وزارة التعليم العالي والبحث العلمي
جامعة الحاج لخضر- باتنة -

كلية الحقوق والعلوم السياسية
قسم الحقوق

الحمـاية الجنـــائية للمعـــاملات الإلكترونـــية

بحث مقدم لنيل شهادة الماجستير في العلوم القانونية تخصص علم الإجرام وعلم العقاب

إعداد الطالب :
طعبـــاش أميـــن

تحت إشراف الأستاذة الدكتورة :
مزيـــاني فريـــدة

أعضـــــــاء لجنة المنـــــــاقشة

لقب واسم الأستاذ	الرتبة العلمية	الجامعة الأصلية	الصفة
أ.د/ بريكي لحبيب	أستاذ التعليم العالي	جامعة أم البواقي	رئيسا
أ.د/ مزياني فريدة	أستاذة التعليم العالي	جامعة باتنة	مشرفة ومقررة
د/ بلفراق فريدة	أستاذة محاضرة	جامعة باتنة	عضوا مناقشا
د/ مباركي دليلة	أستاذة محاضرة	جامعة باتنة	عضوا مناقشا

السنة الجامعيـــــــة

2013/2012



الإهـداء

شكـــــــــــر و عـــــــــــرفان

اللهم ربنا لك الحمد حمدا كثيرا طيبا مباركا فيه ملء السماء والأرض، وصلاة وسلام على صفوتك من خلقك وخاتم أنبيائك ورسلك سيدنا وإمامنا محمد"صلى الله عليه وسلم" وعلى آله وصحبه ومن دعا بدعوته إلى يوم الدين، ونحمده سبحانه وتعالى أن وفقنا إلى أفضل مهنة في الوجود : جمع العلم ونشره، وكل موفق لما خلق .

ومن منطلق قوله صلى الله عليه وسلم " من لم يشكر الناس لم يشكر الله "

فإننا نتوجه بعد شكرنا لله عز وجل ، بالشكر الجزيل إلى الأستاذة الدكتورة مزياني فريدة التي كانت لنا وستبقى إن شاء الله نورا نقتبس منه ما يضيء لنا درب العلم، والتي لم تبخل علينا بجهدها وتوجيهها في هذا العمل العلمي، زادها الله علما وأدامها لنا ذخرا وسندا.

الإهـــــــــــــداء

- إلى من وفر علي عناء الحياة ، إلى من منحني العزة و الرفعة ،إليك أبي العزيز
- إليك يا من نزعت عني روح العياء، إليك يا من منبع الحب والحنان إليك أمي الغالية

"حفظهما الله من كل سوء"

- إلى كل إخوتي و أخواتي
- إلى كل أصدقائي الأعزاء
- إلى كل أسرة كلية الحقوق
- إلى من كان لي قدوة وسندا في هذا المشوار العلمي، إلى الأستاذ الدكتور "شعبان حسان" أهدي هذا العمل.

أمين طعباش

مقدمـــة

لكل عصر ميزة يمتاز بها وميزة هذا العصر هي الإنترنت، والتي ظهرت نتيجة تلاحم بين تكنولوجيا المعلوماتية وأدوات الاتصال السلكية واللاسلكية، و قد نشأت هذه الأخيرة من شبكتي اتصال أمريكيتين مستقلتين إحداهما تابعة لوزارة الدفاع والأخرى تابعة للجامعات الأمريكية، وكان الهدف منها هو خلق شبكة اتصالات غير قابلة للتخريب والخرق تتمثل في شبكات المعلومات العالمية، والتي تتيح فرصة تبادل المعلومات وإبرام العقود، حيث أصبحت أداة فعالة في تسهيل المعاملات سواء بين الأفراد أو الشركات أو المؤسسات، وانعكس ذلك إيجابا على الشركات التجارية حيث ساهمت هذه الشبكة في تسهيل المعاملات الإلكترونية ، فعند استخدامها يتم توفير وقت وجهد كبيرين فلا يشترط في الشراء التنقل لمعاينة المبيع بل يكفي إبداء الموافقة آليا عبر الحاسوب، و تسهل الشبكة عملية التسويق و الدفع التي أصبحت إلكترونيا و تمكن من استخدام البيانات والوسائل الإلكترونية لإبرام العقد دون الحضور الشخصي لطرفيه، كما أن العلاقة القانونية الناشئة عنها غير مقيدة جغرافيا .

ونظرا لكل هذه الميزات الخاصة بالشبكة فقد أصبحت الكثير من المعاملات تبرم عبر الإنترنت ذلك ما جعل هذه المعاملات عرضة لأن تكون محل اختراق وسرقة وقرصنة ، فالإعلام الآلي الذي يستخدمه الأفراد في مجال المعلوماتية هو نفسه الذي يستخدمه المجرمون لتحقيق مآربهم الشخصية .

فالإجرام لم يعد يقتصر على من يشهر سلاحه في وجه ضحيته بل أصبح هناك ما يعرف بالمجرم المعلوماتي و الذي يقتنص المعلومات الإلكترونية بغية التخريب أو المساومة أو السرقة، ومن ثم أصبح من الضروري وضع نظام قانوني متكامل بغية حماية هذه المعاملات، دون إغفال ما قد يعترض وضع ذلك النظام من صعوبات في الواقع العملي نظرا لما تتمتع به الجرائم المعلوماتية من خصائص تختلف عن الجرائم التقليدية، ذلك ما دفع بالفقه الجنائي في بلدان عدة كفرنسا و إيطاليا وألمانيا إلى التكفل بإبراز الصعوبات التي تعترض تطبيق النصوص العقابية للتشريعات التقليدية القائمة على الجرائم الجديدة التي أفرزتها التكنولوجيا المعلوماتية، وسعى إلى إبراز مجموعة من

المبادئ و الآراء الفقهية التي تكفل تحقيق التوازن بين ضرورة حماية المعاملات الإلكترونية و كيفية تكييف النصوص العقابية بشكل يخدمها.

فبتوفير الحماية الجنائية للمعاملات الإلكترونية تصبح هذه الأخيرة أكثر انتشارا واستعمالا نظرا لوجود قواعد قانونية تكفل الحماية لها، وذلك باحتواء هذه القواعد لعقوبات صارمة تجعلها في منأى من الاختراق.

وذلك ما نلمسه من خلال الاهتمام المتزايد للحكومات وحتى العديد من المنظمات الدولية لمكافحة الجرم المعلوماتي فضلا عن رجال الاختصاص الذين يعملون من خلال تجاربهم على سد ثغرات الأنظمة المعلوماتية وتطوير أساليب الحماية، إلا أن ذلك لن يأتي بثماره ما لم تصاحبه حماية قانونية تسبغ صفة عدم المشروعية على انتهاك امن المعلومات تكون بمثابة حاجز ردعي وسببا في التقليل من الإجرام المعلوماتي وتكفل الحماية الجنائية للمعاملات الإلكترونية.

الإشكالية :

نحاول في بحثنا هذا إيجاد حلول لإشكاليته الأساسية و المتمثلة في:

ما مدى مواكبة التشريعات الجزائية للتطور التكنولوجي و المعلوماتي على نحو يجعلها فعالة في تحقيق الحماية الجنائية للمعاملات الإلكترونية ؟

ومن الإشكالية الأساسية هناك تساؤلات فرعية والتي نجمل أهمها في ما يلي:

- ما دواعي إقرار الحماية الجنائية للمعاملات الإلكترونية ؟

- هل النصوص الخاصة أو المستحدثة تكفي لحماية هذه المعاملات ؟

- إلى أي مدى يمكن للنصوص الخاصة بجرائم الأموال أن تحقق الحماية الجنائية للمعاملات الإلكترونية ؟

وبعبارة أخرى هل الأموال المتداولة في نطاق المعاملات الإلكترونية تصلح لأن تكون محلا أو أن تخضع لنشاط جرائم السرقة أو النصب أو خيانة الأمانة ؟

أهمية الموضوع :

من خلال طرح هذه الإشكالية تتضح لنا الأهمية البالغة التي يكتسبها هذا الموضوع حيث أن كثرة المعاملات الإلكترونية واتساعها أصبح يستوجب الحماية كي تكون الشبكة المعلوماتية مكانا خصبا لتلك المعاملات، فيكتسب موضوع الحماية الجنائية أهمية كبيرة بسبب انتشار المعاملات الإلكترونية وتزايد التجارة الإلكترونية، بحيث يشهد العالم اليوم ثورة كبيرة في مجال المعلوماتية خصوصا بعد فتح المجال أمام المعاملات المدنية والتجارية بأن أصبحت تتم بوسائل الكترونية الأمر الذي دفع بالقوانين المقارنة إلى اعتبار حماية تلك المعاملات مصلحة اجتماعية تستحق التدخل لتحقيقها فقامت العديد من التشريعات الأجنبية بإدخال قوانين خاصة بجرائم الكمبيوتر، وما يزيد من أهمية البحث أن نسبة كبيرة من الأفراد والشركات قد لحقتها أضرار كبيرة نتيجة معاملاتهم الإلكترونية. فكيف يمكنهم مباشرة هذه المعاملات في ظل وجود نصوص قليلة تكاد تكون غير كافية لحمايتها؟

الأهداف:

نظرا للأهمية التي يكتسبها هذا الموضوع فقد أردنا تقديم دراسة له لتحقيق جملة من الأهداف التي قد تساعد في فهم ما تم استحداثه في هذا المجال و الإحاطة ببعض جوانبه السلبية ومن بين تلك الاهداف:

الأهداف النظرية :نهدف من خلال بحثنا إلى دراسة موضوع دخل الساحة القانونية وأصبح واقعا مفروضا يستوجب الإلمام بشتى جوانبه والتركيز على تحديات القانون الجنائي في مواجهة تطورات الإعلام الآلي، حيث أن ظهور المعاملات الإلكترونية أدى إلى ظهور مشاكل قانونية في نطاق القانون الجنائي كون القانون بذاته لا يتطور بالسرعة التي تتطور بها التكنولوجيا.

الأهداف العملية: فيما يتعلق بالجانب العملي فإننا نهدف إلى تحقيق الحماية الجنائية للمعاملات الإلكترونية مسبقا لأن الإجرام المعلوماتي في الجزائر والبلدان العربية لم يتخذ الأبعاد التي اتخذها في الدول الغربية، ومن ثم فبإمكان المشرع الجزائري إحاطة المعاملات الإلكترونية بالحماية الكافية قبل استفحال ظاهرة الإجرام المعلوماتي و الذي قد يخلق انتهاكا لحرمة البيانات الشخصية والمساس بالأمن القومي للدولة، كما أنه قد يسهم موضوعنا في الإفادة ببعض المقترحات بعد عرض ما توصلت إليه بعض الدول وتحليله بهدف أن تكون لهذه المقترحات دور في توجيه المشرع الجزائري بغية مسايرة قانون العقوبات للتطورات التكنولوجية وما تطرحه من مشاكل قانونية .

ونظرا لخصوصية الموضوع وطبيعته فقد اضطررنا إلى التعامل معه وفقا للمنهج التحليلي، والذي يعتبر الأنسب لهذا الموضوع وذلك بتحليل النصوص القانونية وإبداء وجهات نظر رجال القانون لانتقاء الحلول البديلة لحماية المتعاملين على الشبكة الإلكترونية.

و للإحاطة بشتى جوانب هذه الدراسة قسمنا الموضوع إلى فصلين خصصنا الأول لماهية الجرائم الواقعة على المعاملات الالكترونية والحماية الجنائية المقررة لها بنصوص خاصة، حيث تناولنا في المبحث الأول ماهية الجرائم الواقعة على المعاملات الإلكترونية ودواعي الحماية الجنائية المقررة لها ، و في المبحث الثاني الحماية الجنائية للمعاملات الالكترونية بنصوص خاصة ، أما الفصل الثاني فتعرضنا فيه للحماية الجنائية للمعاملات الالكترونية وفقا للقواعد العامة في قانون العقوبات، حيث قسمناه إلى مبحثين تناولنا في الأول الحماية الجنائية للمعاملات الالكترونية وفقا للقواعد العامة المقررة في جرائم الأموال، وفي المبحث الثاني تناولنا الحماية الجنائية للمعاملات

الالكترونية من خلال تجريم الاتفاق أو الشروع في الجرائم المعلوماتية، ثم خاتمة تطرقنا فيها لأهم النتائج والاقتراحات التي تم التوصل إليها .

الفصـــل الأول:

ماهية الجرائم الواقعة على المعاملات الالكترونية والحماية الجنائية المقررة لها بنصوص خاصة.

ظهرت المبتكرات الحديثة في نهاية القرن الماضي والتي وقف الكثيرون مبهورين أمامها في حين تكيف معها الآخرون، بحيث حرصوا على تطويرها والاستفادة من وجودها بما لا يخل بالنسيج السياسي والاجتماعي والاقتصادي.

وتمثلت بعض تلك المبتكرات الحديثة في ظهور ما يعرف بالمعاملات الالكترونية أي المعاملات التي يتم تنفيذها بوسائل إلكترونية.[1]

إلا أن ظهور هذه المعاملات أدى إلى ظهور مشاكل في مجالات القانون المختلفة وخاصة القانون الجنائي، وذلك نظرا للجرائم التي أصبحت تعترضها ، ومن ذلك ولدت الحاجة الملحة لتوفير الأمن والموثوقية اللازمة عن طريق وضع نظام قانوني متكامل يضمن الحماية للمعاملات الإلكترونية، ذلك دون إغفال الصعوبات التي قد تعترض وضع ذلك النظام ، ومن ثم استند الفكر العقابي الحديث إلى ربط العدالة الجنائية في مراحلها المتعاقبة بما أحرزته البشرية من تقدم ملموس على صعيد التكنولوجيا ومعطيات العلم الحديث[2] .

وذلك ما تحقق عمليا لدى بعض التشريعات حيث واكبت هذا التطور التكنولوجي باستحداث قوانين تعالج الإجرام المعلوماتي والتي سنتكلم عنها بعد التطرق لماهية هذه الجرائم كون الحديث في هذا المجال يستوجب الإلمام بطبيعة هذه الجرائم وخصائصها ثم الأسباب التي دفعت بنا للبحث عن وجوب إقرار الحماية الجنائية لهذه المعاملات، وبعد ذلك نتطرق للنصوص الخاصة التي تم استحداثها في هذا الفرض من حيث البحث في مدى كفايتها لحماية المعاملات الإلكترونية متبعين في ذلك التقسيم التالي:

المبحث الأول: ماهية الجرائم الواقعة على المعاملات الإلكترونية ودواعي الحماية الجنائية لها

المبحث الثاني: الحماية الجنائية للمعاملات الالكترونية بنصوص خاصة.

1 - د/ محمود الكيلاني، الموسوعة التجارية والمصرفية، المجلد الثاني التشريعات التجارية والالكترونية دراسة مقارنة، دار الثقافة للنشر والتوزيع،عمان 2007،ص439.

2- د/ أسامة حسنين عبيد، المراقبة الجنائية الإلكترونية (دراسة مقارنة) ، دار النهضة العربية، القاهرة 2009 ، ص03.

المبحث الأول

ماهية الجرائم الواقعة على المعاملات الإلكترونية ودواعي الحماية الجنائية المقررة لهـــا

تعتبر تكنولوجيا المعلومات وقود الثورة الصناعية الثالثة وأن المعلومات هي المادة الخام الأساسية للإنتاج التي يعتمد المجتمع على إنتاجها وإيجادها والاستفادة منها إلا أن هذا الجانب المشرق لتقنية المعلومات يتخلله جانب مظلم يتمثل في الإجرام المعلوماتي [1] .

فهاته التكنولوجيا التي ارتقت بمستوى الإنسان إلى العصر المعلوماتي هي ذاتها التي يستعملها مجرمو المعلوماتية وذلك بالاستعانة بنظم المعلومات و الاتصالات في الأنشطة الإجرامية فالتكنولوجيا المعلوماتية تعتبر كغيرها من التطورات حيث تحمل في طياتها جانبا مظلما يتجسد في ظاهرة الإجرام المعلوماتي[2]

ذلك ما يجعل الحاجة ملحة لحماية المعلوماتية من الجرائم التي قد تقع عليها بغرض تحقيق العديد من الأهداف كالتوجه نحو الحكومة الالكترونية ، وحماية الاقتصاد الوطني من الخسائر التي قد تلحق به جراء الجرائم المعلوماتية وفرض الحماية الجنائية للمعلوماتية نظرا لعدم كفاية التشريعات الجنائية القائمة.

وذلك ما سنتطرق إليه في هذا المبحث من خلال تقسيمه لمطلبين، نتناول في الأول ماهية الجرائم الواقعة على المعاملات الالكترونية ونتناول في المطلب الثاني دواعي الحماية الجنائية للمعاملات الالكترونية.

1– نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 2008، ص64.
2- د/ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدر الجامعية للطباعة والنشر، بيروت 1999 ، ص07.

المطلب الأول

ماهية الجرائم الواقعة على المعاملات الالكترونية

ساهمت الثورة المعلوماتية التي يشهدها العالم في عصرنا هذا في تطوير معاملات الأفراد وتسهيلها وذلك في شتى مجالات الحياة المختلفة خاصة بظهور الانترنت والتي وضعت العالم كله في قرية صغيرة نظرا لما تمتاز به من سرعة في تبادل المعلومات والبيانات ما أدى إلى تكثيف المعاملات بواسطتها بين الأفراد، إلا أن هاته المعاملات لم تكن في منأى عن الإجرام حيث ظهر ما يعرف بالجريمة المعلوماتية والتي سنتطرق لها في هذا العنصر من خلال إعطاء تعريف للجرائم الواقعة على المعاملات الالكترونية، مع إدراج تعريف نسبي للمعاملات الإلكترونية معرجين بذلك على محل الجريمة المعلوماتية وذلك في فرع أول، ثم نتناول في الفرع الثاني خصائص الجرائم الواقعة على المعاملات الالكترونية.

الفرع الأول:تعريف الجرائم الواقعة على المعاملات الإلكترونية

لتناول الجرائم الواقعة على المعاملات الالكترونية يجب الحديث أولا عن الجريمة المعلوماتية[1]، ثم المحل الذي تنصب عليه هذه الجرائم .

أولا: تعريف الجريمة المعلوماتية:

ما يلاحظ في مجال الجريمة المعلوماتية أنه لا يوجد مصطلح موحد للدلالة على هذه الظاهرة، فهناك من يطلق عليها ظاهرة الغش المعلوماتي أو الاختلاس المعلوماتي أو الجريمة المعلوماتي وعلة هته

1- "المعلوماتية" مصطلح استعمله أول مرة البروفيسور "A.I.MIKHAILOV" مدير المعهد الاتحادي للمعلومات العلمية والتقنية بالإتحاد السوفياتي سابقا وذلك تعريفا لعلم المعلومات العلمية science of scientific information وذاع استخدامه بعد ذلك على مستوى واسع، وأخذته بعض الأكاديميات الفرنسية على أنه علم التعامل العقلاني بواسطة آلات أوتوماتيكية مع المعلومات باعتبارها دعامة للمعارف الإنسانية وعماد الاتصالات في الميادين التقنية والاقتصادية والاجتماعية، وقام بعد ذلك مجلس الوزراء الفرنسي بتكريس الاستخدام الرسمي لكلمة المعلوماتية حيث أخذت به جل الأكاديميات الفرنسية عام 1967.راجع في ذلك : مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة مقدمة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، قسم العلوم القانونية، جامعة الجزائر، السنة الجامعية 2009/2008،ص9.
وميلاد تقنية المعلوماتية جاء نتيجة اندماج فرعين تقنيين هما الحوسبة والاتصال أما الحوسبة فنقوم على استخدام التقنية لإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محددة فتصل بعملي الحاسب والمنطق أما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها ، باندماج هذين الفرعين أصبح يطلق عليهما التقنية العالية أو تقنية المعلومات، أنظر الموقع:
www.djetfa.info/Vb/showthread.php?t=204052 .

الاختلافات هو خشية حصر هذه الجريمة في مجال ضيق [1]

ومن ثم ظهرت تعريفات عديدة للجريمة المعلوماتية تختلف بحسب ضيقها واتساعها.

1- التعريف الواسع:

هناك العديد من التعريفات الواسعة والتي من بينها:

أن الجريمة المعلوماتية تتمثل في: " كل عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد نصوص قانون العقوبات لحمايتها [2]، ويتبنى الخبير الأمريكي**(Parker)** مفهوما واسعا للجريمة المعلوماتية حيث يعرفها بأنها" كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو كسبا يحققه الفاعل[3] "

يتبين من هذا التعريف أنه ربط الفعل الإجرامي بالخسارة أو الربح أيا كانت الصلة التي تربطه بالمعلوماتية، في حين عرفها الفقيه D. Ball بأنها: "كل أشكال الفعل الغير مشروع الذي يستخدم الحاسب في ارتكابه كأداة رئيسية" [4]

إن الأخذ بالتعريف الواسع للجريمة المعلوماتية سيدخل في نطاقها كل التصرفات غير المشروعة والتي لها علاقة بالحاسوب أيا كانت هاته العلاقة وأيا كان دور الحاسوب فيها، سواء كان وسيلة أو مناسبة لارتكاب التصرفات غير المشروعة أو كان موضوعا لها.

فالاعتماد في تعريف الجريمة المعلوماتية على الوسيلة المستخدمة في ارتكابها أو المناسبة التي ارتكبت في إطارها منتقد لأنه لتعريفها وجب الرجوع إلى العمل الأساسي المكون لها وليس الوسائل المستخدمة لارتكابها وليس لمجرد أن الحاسب قد أستخدم في جريمة أن نعتبرها من الجرائم المعلوماتية وذلك ما دفع بالبعض إلى الأخذ بتعريف أضيق للجريمة المعلوماتية.

1- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية 2004، ص43.
2- محمد أمين الشوابكة، جرائم الحاسوب والإنترنت(الجريمة المعلوماتية)، دار الثقافة، عمان 2009، ص 9.
3- نهلا عبد القادر المومني، المرجع السابق، ص 49.
4 - leslie d. ball, cumputer crime " the information technology revolution" , 1985, p,543

2- التعريف الضيق:

من بين التعريفات الضيقة للجريمة المعلوماتية بأنها تلك التي يكون الغرض منها موجه ضد الأموال المعلوماتية متى كانت مرتبطة باستخدام نظام المعالجة الالية للمعطيات، مع إقصاء تلك الأفعال المتمثلة في استخدام الإعلام الآلي كوسيلة للاعتداء على الغير، سواء الأشخاص أو الثقة العامة[1]، وتبنى الفقه الفرنسي تعريفا أضيق من ذلك حيث عرفها بأنها كل الأفعال الغير مشروعة الموجهة ضد نظام المعالجة الآلية للمعطيات[2]

في حين يرى الأستاذ Massa أن المقصود منها هو الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح [3] .

لكن الأخذ بأحد هذه التعريفات يجعلنا نحصر الجرم المعلوماتي في الاعتداءات الواقعة على المال المتداولة في هذا النطاق أو على الاعتداءات الموجهة ضد النظام المعلوماتي، متجاهلين بذلك الجرائم الماسة بالحياة الخاصة للأفراد كالسب أو القذف ...

من خلال ما سبق يتضح لنا أن التعريفات الواسعة جاءت فضفاضة و تتسم بالعموم، أما التعريفات الضيقة فتنظر إلى الجريمة من زاوية دون الأخرى، و على ذلك يمكن تعريف الجرائم المعلوماتية بأنها تلك الجرائم الناتجة عن استخدام المعلوماتية و التقنية الحديثة المتمثلة بالكمبيوتر والإنترنت في أعمال وأنشطة إجرامية متى مست تلك الأعمال والأنشطة المكونات المادية أو المعنوية للنظام المعلوماتي أو ألحقت أضرارا بالأشخاص.

هذا فيما يتعلق بتعريف الجرائم المعلوماتية أما المعاملات الإلكترونية[4] فهي تلك المعاملات المشتملة على المعلومات، والتي يتم تبادل بياناتها إلكترونيا على شكل رسائل لتلك المعلومات و يمكن تقييد تلك المعلومات في سجل إلكتروني لتعد أداة إثبات عقد يعرف بأنه عقد إلكتروني و

1- مناصرة يوسف،المرجع السابق، ص 10

2 - Andre lucas , le droit de l'informatique, P.U.F, ed 1987, p496.

3- محمد علي العريان، المرجع السابق، ص 44

4- عرفت المعاملات الإلكترونية في القانون الأردني بأنها " المعاملات التي تنفذ بوسائل إلكترونية و أوضحت بأن مصطلح إلكتروني يعني تقنية استخدام وسائل كهربائية أو مغناطيسية أو ضوئية أو إلكترومغناطيسية أو أي وسائل مشابهة في تبادل المعلومات وتخزينها"
راجع في ذلك: للمادة الأولى من قانون المعاملات الإلكترونية الأردني، رقم 85 لسنة 2001.

ذلك بعد أن تكون الرسالة قد تم توقيعها إلكترونيا ، وجاءت معالجة تلك المعلومات بواسطة نظام إلكتروني يستخدم لإرسالها أو تسلمها من مرسلها أو تخزينها أو تجهيزها على أي وجه، وهذه المعلومات الواردة ضمن الرسالة في عملية تبادل البيانات يطلق عليها المعاملات الإلكترونية [1]، ولتكون هذه المعاملات في منأى من التخريب والسطو يجب إحاطتها بالحماية اللازمة سواء كانت تقنية كوضع رموز مشفرة لحماية الأنظمة والتعاملات أو حماية قانونية بوضع قوانين صارمة وصريحة تحمي تلك المعاملات.

ثانيا:المقصود بمحل الجريمة المعلوماتية

محل الجريمة المعلوماتية هو المال المعلوماتي تمييزا لماليته المغايرة للمال التقليدي فالمال المعلوماتي هو الحاسب بكل مكوناته، والحاسب اصطلاحا لا يخرج عن كونه آلة إلكترونية تستقبل البيانات ثم تقوم عن طريق الاستعانة ببرنامج معين بعملية تشغيل هذه البيانات للوصول إلى النتائج المطلوبة، والحاسبات تنقسم من حيث أغراض استخداماتها إلى حاسبات عامة الأغراض وأخرى متخصصة الأغراض، كما لها انقسامات أخرى من حيث النوعية، والحاسبات بأنواعها وتقسيماتها المختلفة تجمعها خاصية واحدة فهي تتكون من عنصرين أساسيين هما: الكيان المادي والكيان المعنوي.

فالكيان المادي يتمثل في المكونات المادية للحاسب وهي جهاز الإدخال، جهاز الإخراج، وحدة التشغيل المركزية التي يتم من خلالها معالجة المعلومات وتخزينها وإخراجها.

أما الكيان المعنوي أو ما يطلق عليه بالكيان المنطقي يشمل البرامج التي يتحقق من خلالها قيام الحاسوب بوظائفه المختلفة بالإضافة إلى المعلومات المطلوب معالجتها أو التي تمت معالجتها بالفعل[2]، فمعطيات الكمبيوتر بدلالتها الواسعة تتمثل في البيانات المدخلة والبيانات والمعلومات المعالجة والمخزنة والبرامج بأنواعها والمعلومات المستخرجة والمتبادلة بين النظم[3].

1- د/ محمود الكيلاني، المرجع السابق، ص 440-441.
2- أمال قارة، الجريمة المعلوماتية، رسالة مقدمة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، قسم العلوم القانونية، جامعة الجزائر، السنة الجامعية 2006/2005، ص 15
3- د/ علي جبار الحسناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، الأردن 2009، ص32.

وتشمل الجرائم المعلوماتية في حالة الاعتداء على الكيان المنطقي كل من أفعال السرقة أو التغيير أو حذف المعلومات ، مثل حالة النشاط الجرمي الذي يستهدف اختراق بريد إلكتروني والعبث بمحتوياته أو سرقة المعلومات المخزنة في موقع ما والاستفادة منها بما يحمل في طياته بعضا من انتهاك الخصوصية وحقوق الملكية الفكرية وأنماط جرمية أخرى[1]، كتزوير المستخرجات الإلكترونية و إفشاء محتوياتها أو ما اصطلح على تسميته بسرقة ساعات عمل الحاسب [2]

الفرع الثاني:خصائص الجرائم الواقعة على المعاملات الالكترونية

يمكن إجمال أهم خصائص الجرائم المعلوماتية في النقاط التالية:

أولا: الجريمة المعلوماتية متعدية الحدود أو جريمة عابرة للدول

بعد ظهور شبكة الإنترنت لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد[3] ، ونظرا لامتداد هذه الجريمة لخارج حدود مرتكبيها فإنها تثير مشاكل الاختصاص والإجراءات والتحري والتفتيش والضبط [4]

ثانيا: الحاسب الآلي هو أداة ارتكاب جرائم الإنترنت

تعتبر هذه الخاصية من أهم الخصائص التي تميز جرائم الإنترنت عن غيرها من الجرائم الأخرى التقليدية، ذلك لأن شبكة الإنترنت هي إحدى التقنيات الحديثة التي أفرزها تطور الحوسبة ولذلك فإن ارتباطها بالحاسب الآلي هو أمر لا مفر منه باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي[5]

1- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت(الجرائم الالكترونية) دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان 2007، ص18

2- محمد علي العريان، المرجع السابق، ص 46

3- نهلا عبد القادر المومني، المرجع السابق، ص 50.

4- عبد الله عبد الكريم عبد الله، ص32.

5- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2006، ص35.

ثالثا: صعوبة إثبات الجريمة المعلوماتية

اكتشاف الجريمة المعلوماتية أمر ليس بالسهل ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب، فالجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة [1]

وتعود صعوبة إثبات جرائم الإنترنت إلى:

- صعوبة الاحتفاظ الفني لآثارها إن وجدت.

- الحرفية الفنية العالية التي تتطلبها من أجل الكشف عنها وهذا ما يعرقل عمل المحقق الذي تعود التعامل مع الجرائم التقليدية.

- أنها تعتمد على الخداع في إركابها والتضليل في التعرف على مرتكبيها فهؤلاء يعتمدون على التخفي عبر دروب الإنترنت تحت قناع فني.

- يلعب البعد الزمني(اختلاف المواقيت بين الدول) والمكاني (إمكانية تنفيذ الجريمة عن بعد) والقانوني (أي قانون يطبق) دورا مهما في تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم [2]

رابعا: خصوصية مجرمي المعلوماتية

مرتكبو هذه الجرائم لهم صفات مميزة من حيث الثقافة والعلم التكنولوجي، فالمجرم في هذا النوع من الجرائم ليس عاديا فهو يرتكب جريمة متخصصة خاصة إذا ما تمثلت هذه الجريمة في سرقة معلومات مشفرة ما سيتبع معه خبرة تقنية عالية في هذا المجال.[3]

1- نهلا عبد القادر المومني، المرجع السابق، ص 56.
2- نبيلة هبة هروال، المرجع السابق، ص40.
3- عبد الله عبد الكريم عبد الله، المرجع السابق، ص33.

فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتباكها، فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم ، ومن يرتكبها عادة ما يكون من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت.

فعلى سبيل المثال فإن الجرائم المعلوماتية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية عالية جدا من قبل مرتكبها [1] .

كما يتميز المجرم المعلوماتي أيضا بفئاته وأنماطه المختلفة[2] و أساس التمييز بين تلك الأنماط هو الباعث أو الدافع إلى ارتكاب الجريمة بينما هو ساذج لدى البعض لا يتعدى الرغبة في الاستطلاع و الاستكشاف، فهو خبيث لدى البعض الآخر و الذي قد يكون ماليا أو سياسيا أو غيره[3]

1- نهلا عبد القادر المومني، المرجع السابق ، ص59.

2- من بين أهم تصنيفات مجرمي المعلوماتية التصنيف القائم على أساس أغراض الإعتداء الذي أورده كل من :
Davide icove, Paul serger,willian vontrach في مؤلفهم جرائم الكمبوتر الصادر عام 1995 حيث تم تصنيف مجرمي المعلوماتية إلى ثلاث طوائف: المخترقون ، المحترفون والحاقدون.
ا- المخترقون : وفي هذه الطائفة يوجد نوعين وهما: الهاكرز والكراكز.
- الهاكرز (HACKER) أو المتسلل هو شخص بارع في استخدام الحاسب الآلي وبرامجه ولديه فضول في استكشاف حسابات الآخرين وبطرق غير مشروعة.
- الكراكرز (CRACKER) : أو المقتحم وهو شخص يقوم بإقتحام نظام الحاسوب لإلحاق الضرر أو العبث بمحتوياته أو سرقتها، والسمة المميزة للمقتحمين هي تبادلهم المعلومات فيما بينهم .
ب- المحترفون : هذه الطائفة تعد الأخطر من بين مجرمي الكمبيوتر والأنترنت حيث تهدف إعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لإرتكاب جرائم الحاسوب ويتسم أفراد هذه الطائفة بالتكتم خلافا للطائفة الأولى فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة ، والأعمار الغلبة لهذه الطائفة تتراوح بين 25 و40 سنة
ج- الحاقدون : هذه الطائفة يغلب عليها عدم توافر أهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين فهم لا يسعون إلى إثبات القدرات التقنية والمهارية وفي نفس الوقت لا يسعون إلى مكاسب مادية أو سياسية إنما يحرك نشاطهم الرغبة في الإنتقام والثأر كأثر لتصرف صاحب العمل معهم، أو لتصرف المنشأة المعينة معهم عندما لا يكونون موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوضعهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الإنتقام من المنشأة المستهدفة في نشاطهم ، وتغلب على أنشطتهم من الناحية التقنية إستخدام تقنيات الفيروسات والبرامج الضارة وتخريب النظم وإتلاف كل أو بعض معطياته ، وليس هناك ضوابط محددة بشأن أعمار هذه الطائفة. أنظر الموقع:
www.djetfa.info/Vb/showthread.php?t=204052 .

3- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن، دار الجامعة الجديدة، الإسكندرية2007، ص33

المطلب الثاني:

دواعي الحماية الجنائية للمعاملات الالكترونية

هناك العديد من الأسباب التي تجعل الحاجة ملحة لحماية المعاملات الالكترونية من الجرائم التي قد تقع عليها وتتمثل أهم هذه الأسباب في:

- العمل من أجل التوجه نحو الحكومة الإلكترونية.

- الخسائر الفادحة التي قد تلحقها هذه الجرائم بالاقتصاد الوطني.

- عدم كفاية التشريعات الجنائية القائمة لمواجهة الاعتداءات التي قد تنصب على المعاملات الإلكترونية.

ونظرا لما تتمتع به هذه الأسباب من أهمية وتشعب، فإننا سنتناول كل واحد منها في فرع مستقل. وذلك على الشكل التالي :

الفرع الأول:التوجه نحو الحكومة الإلكترونية.

الفرع الثاني :أضرار الجرائم المعلوماتية على الاقتصاد الوطني.

الفرع الثالث: عدم كفاية القوانين القائمة.

الفرع الأول:التوجه نحو الحكومة الإلكترونية

التوجه نحو إقامة حكومة إلكترونية كأحد أهم الأسباب التي توجب الحماية الجنائية للمعلوماتية تتطلب الحديث عن ماهية الحكومة الإلكترونية وأهدافها ومراحل تطبيقها.

أولا: ماهية الحكومة الإلكترونية

ظهور شبكة الإنترنت بخدماتها المتعددة كان له دور بارز في أن توجه كثير من الدول طاقاتها وإمكاناتها للاستفادة من هذه الشبكة وكانت فكرة الحكومة الإلكترونية هي الثمرة التي خرجت بها بعض الدول باعتبارها وسيلة لتسهيل معاملاتها الإلكترونية والارتقاء بمستوى المواطن وتخفيف العبء على المؤسسات الحكومية المختلفة مما يؤدي إلى زيادة كفاءاتها.

و الحكومة الالكترونية هي النسخة الافتراضية للحكومة الحقيقية الكلاسيكية مع فارق أن الأولى تعيش في الشبكات و أنظمة المعلوماتية و التكنولوجيا، أما الثانية فتتواجد بشكل مادي في أجهزة الدول[1]

وقد عرفت الحكومة الإلكترونية بأنها البيئة التي تتحقق فيها خدمات المواطنين واستعلاماتهم وتتحقق فيها الأنشطة الحكومية للدائرة المعنية من دوائر الحكومة بذاتها أو فيما بين الدوائر المختلفة باستخدام شبكات المعلومات والاتصال عن بعد، كما عرفت بأنها استخدام للأنترنيت والشبكة العالمية العريضة لإرسال معلومات وخدمات الحكومة للمواطنين[2]

وبتعريف أكثر دقة فالحكومة الإلكترونية هي قدرة قطاعاتها المختلفة على توفير الخدمات الحكومية التقليدية للمواطنين، وذلك بوسائل إلكترونية وبسرعة وقدرة متناهيتين وبتكاليف ومجهود أقل من خلال موقع واحد لكل قطاع على شبكة الإنترنيت[3].

وبناءا على ما سبق فإن فكرة الحكومة الإلكترونية تقوم على عدة ركائز منها:

1- www.egovconcepts.com/channels/basics/62-2009-05-26-06-29-05.html. le : 15/02/2011 à : 10h 30mn.

2- د/ خالد ممدوح إبراهيم، أمن الحكومة الالكترونية، الدار الجامعية، الإسكندرية 2008، ص64.

3- د/ خالد ممدوح إبراهيم، ص65

- تجميع كافة الأنشطة والخدمات المعلوماتية والتفاعلية والتبادلية كلها في موقع الحكومة الرسمي على شبكة الإنترنيت.

- تحقيق حالة اتصال دائم بالجمهور مع القدرة على تأمين الاحتياجات الاستعلامية والخدماتية كلها للمواطن[1]

- تحقيق سرعة وفعالية الربط والتنسيق والأداء والانجاز بين دوائر الحكومة ذاتها ولكل منها على حدى[2]

- تحقيق التواصل العلمي بمعنى الاطلاع على التطورات العلمية المتنوعة في مجالات العمل المختلفة والاستفادة المتبادلة منها.

- تحقيق قدر مناسب من الاستقرار لأفراد المجتمع بتوفير احتياجاتهم من المعلومات المنوعة عن طريق شبكة المعلومات الحكومية[3]

ولتحقيق جل هذه الأهداف وجب الاعتماد على محاور أساسية للعمل بها بشكل متكامل ومتناسق وتتمثل هذه المحاور في: التشريعات القانونية ، التعليم ، البنية التحتية، الخدمات الالكترونية، وما يهمنا في دراستنا هذه هو المحور ألا وهو محور التشريعات القانونية.

ثانيا: مراحل الحكومة الالكترونية

تجدر الإشارة إلى أن التطبيق الفوري للحكومة الالكترونية يتطلب موارد مالية كبيرة، وكذلك وجود موارد بشرية ذات تدريب وتأهيل عالي المستوى وهما أمران لا يتوفران لمعظم البلدان وتحديدا بلدان المنطقة العربية، لذلك فالتدرج في أسلوب تنفيذ هذا المشروع الرائد هو وسيلة تضمن استمرارية الحكومة الالكترونية على أرض الواقع وتأديتها لوظائفها على أكمل وجه[4].

1- نهلا عبد القادر المومني، المرجع السابق، ص61.
2- د/ خالد ممدوح إبراهيم، المرجع السابق ص54
3- أحمد الصم النقبي، فوائد تأسيس شبكة أنظمة المعلومات الحكومية، مجلة الشرطة، العدد 343، السنة 29، يوليو 1999، ص 56.
4- نهلا عبد القادر المومني، ص 63.

فما نلمسه في أسلوب التدرج من الناحية العملية وفي شتى المجالات أنه يؤدي إلى تقبل المواطنين لأي فكرة تأتي عن طريق هذا الأسلوب، ويمكن توعيتهم بمضمون الفكرة شيئا فشيئا وأسلوب التنفيذ التدريجي للحكومة الالكترونية يمكن أن يتم وفق أربع مراحل.

المرحلة الأولى: التواجد

تقوم الحكومة في هذه المرحلة بتوفير المعلومات والبيانات للمستخدمين من المواقع المختلفة للوزارات والوحدات الحكومية دون الحاجة إلى الذهاب الفعلي لتلك الوزارات[1]

فبذلك يستطيع المواطن البسيط أو الموظف من مكتبه أو المستثمر من دولة أخرى الاطلاع على القوانين أو على الوثائق الإدارية اللازمة في بعض الملفات على سبيل المثال، من خلال الاطلاع على المواقع الحكومية عبر شبكة الانترنت دون تكبد عناء التنقل إلى الجهة الإدارية كما كان عليه الحال سابقا.

المرحلة الثانية: التفاعل

وهي المرحلة التي تلي التواجد حيث يستطيع المواطن أو رجل الأعمال الاتصال المباشر عن طريق البريد الالكتروني وتبادل الآراء والملاحظات حول القضايا المختلفة [2]، كما تمكن هذه المرحلة من إعطاء المواطن إمكانية إبداء رأيه في السياسات المطروحة ومشاركته في عملية إتخاذ القرار، وذلك ما يعرف بالمشاركة الفعالة[3]

المرحلة الثالثة: تنفيذ المعلومات إلكترونيا :

وهذه المرحلة من أكثر مراحل الحكومة الالكترونية تعقيدا حيث تتم المعاملات المختلفة مع الوحدات الحكومية مباشرة من خلال المواقع الالكترونية للحكومة ووحداتها بما في ذلك السداد الالكتروني للرسوم و المدفوعات المتنوعة.

1- نهلا عبد القادر المومني،المرجع السابق ، ص 63.
2- نهلا عبد القادر المومني، ص63.
3 - www.egovconcepts.com/channels/basics/62-2009-05-26-06-29-05.html . le : 15/02/2011 à : 10h 30mn.

ومن شأن هذه المرحلة توفير أمرين في غاية الأهمية وهما : الوقت والمال فربما تحتاج معاملة ما ثلاثة أو أربعة أيام من التنقل من دائرة إلى أخرى، بالإضافة إلى أجور المواصلات وتعطل المواطن عن العمل خلال هذه الفترة، على عكس من ذلك عندما تنفذ المعاملات إلكترونيا فربما تكفيه عشر دقائق من العمل على الإنترنت لإنهاء معاملته[1]

المرحلة الرابعة: التحول النهائي

وهي آخر مراحل تنفيذ الحكومة الالكترونية حيث يصبح استخدام تقنية المعلومات والاتصالات في المعاملات كلها عبارة عن ممارسة يومية عادية ومتوفرة في المناطق كلها، حيث يستطيع المواطن أو المؤسسات الإستفادة من خدمات الحكومة الإلكترونية عبر الأنترنيت [2]

وفي الواقع أن معظم تحديات الحكومة الالكترونية ومشاكلها قد تطفو على السطح في المرحلة الثالثة وهذه التحديات تتطلب التدخل التشريعي الجنائي لحماية الأفراد وكذلك الحكومة من بعض الذين يستغلون هذه التقنيات الحديثة بما يحقق مصالحهم الشخصية ومطامعهم الاقتصادية[3]، حيث يستغل مخترقوا الأنظمة المعلوماتية حداثة التعامل الإلكتروني خاصة في الدول العربية وضعف الحماية الفنية والجنائية لتلك المعاملات وبذلك تسهل عليهم عملية السرقة أو الاختلاس المعلوماتي.

وهناك نماذج إجرامية كثيرة تقع في مرحلة المعاملات الإلكترونية مثل الدخول إلى الشبكة الإلكترونية ومحاولة تدمير قاعدة البيانات والمعلومات بها أو تعويق عمل نظام هذه الحكومة بل قد يصل الأمر إلى تزوير المحررات المعلوماتية الخاصة بهذه الحكومة الإلكترونية[4]

ثالثا: متطلبات الحكومة الالكترونية:

إن السعي إلى استخدام تقنية المعلومات والاتصالات والتقدم العلمي في تقديم الخدمات وتوفير البيانات في القطاعين العام والخاص وجعل الخدمة الآلية أو الإلكترونية المحرك الأساسي لتوفير هذه

1- د/ خالد ممدوح إبراهيم، أمن الحكومة الإلكترونية،المرجع السابق ،ص58

2 -www.egovconcepts.com/channels/basics/62-2009-05-26-06-29-05.html. le : 15/02/2011 à : 10h 30mn.

3- نهلا عبد القادر المومني، المرجع السابق، ص64.

4- د/ عبد الفتاح بيومي حجازي، الحكومة الالكترونية ونظامها القانوني، دار الفكر الجامعي، الإسكندرية، 2004، ص173.

الخدمات وتقديمها وإتاحتها للجميع يتطلب وجود عدد من المعطيات والعناصر التي يمكن القول أنه في حال تخلف أحدها سيكون مشروع الحكومة الالكترونية عاجزا عن تحقيق غاياته التي وضع ابتداء من أجلها، وأنفقت الدولة في سبيل إتمامه مبالغ كبيرة، ومن ثم فالمعطيات المطلوبة لقيام الحكومة الالكترونية تشمل عددا من الأمور أهمها:

المعطيات البشرية:

السعي لإقامة حكومة إلكترونية يستدعي العمل على تقليص الفجوة الرقمية لدى المواطنين وذلك بمحو الأمية المعلوماتية لديهم وتوفير الكفاءات القادرة على التعامل مع أنظمة المعلومات ومع الخدمات الالكترونية التي تتضمنها الحكومة الالكترونية[1]، و بما أن شبكة المعلومات الحكومية تعتبر مجالا جديدا للمعلومات المشتركة فهي تعاني نقصا كبيرا في مجال الخبرة العملية و الأخصائيين في الشبكة الموضوعية و إدارة الشبكة الواسعة.

المتطلبات الإدارية:

إن الحاجة إلى إدارة وتنظيم المعلومات هي أحد المتطلبات الأساسية لتطوير قواعد البيانات وتوفير المعلومات التي هي بمثابة وثائق وتصنيف النظام والحصول على البيانات الالكترونية، وبما أن شبكة أنظمة المعلومات الحكومية هي بصورة أساسية ربط إلكتروني بين الوزارات في الحكومة المحلية والحكومة الاتحادية فإن اعتماد التنظيم في إدارة المعلومات يؤدي إلى نجاح تأسيس شبكة أنظمة المعلومات الحكومية [2].

ومن ثم تبرز الحاجة إلى الهندسة الحكومية و التي تأخذ على عاتقها عملية تركيب مكونات الحكومة الإلكترونية مع بعضها البعض، بالموازاة مع عملية تطوير هيكل الإدارة الإلكترونية [3]

كما أن من سمات الإدارة الالكترونية عدم وجود علاقات مباشرة بين طرفي المعاملة وعدم وجود دعائم ورقية ووجود تفاعل جماعي أو متوازي بين عدة أطراف في وقت واحد و إمكانية

1- نهلا عبد القادر المومني، المرجع السابق، ص64.
2- أحمد الصم النقبي، المرجع السابق، ص56
3 -www.egovconcepts.com/channels/basics/62-2009-05-26-06-29-05.html le : 15/02/2011 à : 10h 30mn.

تنفيذ كافة المعاملات إلكترونيا والاستخدام المكثف لتكنولوجيا المعلومات وتحويلها لتكون الوسط الأساسي للعمل.[1]

ذلك ما يستوجب تأهيل الكفاءات الإدارية على وجه التحديد وتدريب الموظفين جميعهم وتوعيتهم بمفهوم وأهمية الحكومة الالكترونية، حتى يكونوا قادرين على نشر ثقافتها وترويجها لدى المتعاملين معهم.

المتطلبات القانونية والتشريعية:

هي المتطلبات الأكثر أهمية وخطورة، وتنبع أهمية المتطلبات القانونية من كونها تشكل الإطار التنظيمي الوقائي الرادع الذي يحيط بكل متعلقات الحكومة الالكترونية الأمر الذي يجعل التفكير في التلاعب بمحتوى هذه الحكومة من قبل العابثين أمرا في غاية الصعوبة، وكذلك يضمن أمن المعلومات وسريتها وخصوصيتها خاصة للأفراد الذين يتملكهم الخوف من أن تصبح بياناتهم الخاصة ووثائقهم عرضة لاختراقها، وبالتالي تفقد حرمتها وخصوصيتها[2]

لكن الذي نلحظه في هذا السياق أن هنالك غيابا تشريعيا واضحا في عدد من القوانين الحالية القائمة، كما أن العديد من رجال القانون والقضاء تنقصهم الدراية و الخبرة اللازمة لاستخدام الكمبيوتر والانترنت، ناهيك عن ضرورة توافر العلم القانوني بالتعاملات الحكومية[3] ولهذه الاعتبارات يجب على الحكومات التي تقوم بأعمالها عن طريق الحاسب الآلي والإنترنت أن تسارع بإصدار تشريعاتها التي تنظم عملية استخدام الأعمال الإلكترونيةن وأن تجرم كافة صور التعديات التي تقع على هذه الأعمال في صورة جنائية [4]، فالغياب التشريعي في هذه الحالة سيجعل الباب مفتوحا على مصراعيه أمام المتطفلين والقراصنة ومجرمي المعلوماتية بكل أطيافهم للتطاول على محتوى الحكومة الالكترونية بكل ما تشتمله، وقد يصل الأمر إلى حد التلاعب في الأرقام والبيانات وخاصة في النواحي الاقتصادية المالية، كما هو الحال في حالات الدفع الالكتروني

1- د/ خالد ممدوح إبراهيم، المرجع السابق، ص 61.
2- نهلا عبد القادر المومني، المرجع السابق، ص 65.
3- د/ خالد ممدوح إبراهيم، ص72.
4- د/ عبد الفتاح بيومي حجازي، المرجع السابق، ص 173.

عبر بوابة الحكومة الالكترونية دون وجود إمكانية لمعاقبتهم لعدم وجود نصوص قانونية تسمح بذلك.

وتجدر الإشارة إلى أن تطبيق مفهوم الحكومة الالكترونية في الولايات المتحدة الأمريكية ودول الاتحاد الأوربي وغيرها من الدول الغربية كان متزامنا مع حملة لتعديل التشريعات القانونية القائمة خاصة الجنائية منها، في خطوة الهدف منها هو الحماية القانونية الشاملة لهذا المفهوم وتخطي الثغرات القانونية التي قد يستفيد منها العابثون بأمن المعلومات وأنظمتها، فالعملية وحدة متكاملة فلا يمكن إيجاد حكومة إلكترونية دون وجود تشريعات تحكم هذه العملية من الناحية المدنية وكذلك من الناحية الجنائية [1]

ففي الجزائر على سبيل المثال بدأت بوادر الاتجاه نحو الحكومة الالكترونية في الظهور وذلك ما يتضح من خلال عمل الهيئات الحكومية في التدرج نحو استبدال المعاملات الإدارية العادية بالمعاملات الالكترونية، لكن ذلك يقابله بطء تشريعي واضح من حيث أن المشرع الجزائري أغفل هذا الجانب بالرغم من تعديله الأخير لقانون العقوبات الذي تمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم:156/66[2]

وذلك بقسم سابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، إلا أن ذلك غير كاف لعدم إحاطة هذه النصوص بكافة حيثيات المعاملات الالكترونية.

وفي الواقع فإن الحماية المتكاملة للمعلوماتية من الجرائم التي قد تكون عرضة لها تتطلب تشريعات متناسقة يكمل بعضها بعضا وتشمل جوانب الحياة الالكترونية كلها، ولهذه الاعتبارات يجب على الدول التي تريد الاتجاه نحو الحكومة الالكترونية أن تسارع بإصدار تشريعات تنظم عملية استخدام الأعمال الالكترونية وتجرم كافة صور التعديات الواقعة على هذه الأعمال

1- نهلا عبد القادر المومني، المرجع السابق، ص 66،67
2- القانون 04/ 05 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 156/66 المؤرخ في 08 جوان 1966 المتضمن قانون الغقوبات، ج ر، 71 في 2004/11/10

الفرع الثاني :أضرار الجرائم المعلوماتية على الاقتصاد الوطني:

"مالم نستطع تأمين بنيتنا التحتية الالكترونية فإن كل ما يحتاجه المجرم لتعطيل اقتصادنا ووضع حياتنا موضع الخطر هو نقرات بسيطة على جهاز الحاسوب والاتصال عن طريق الإنترنت، فالفأرة يمكن أن تكون الآن أكثر خطورة من الرصاص والقنبلة"، هذا ما أدلى به (**لامار سميث**) رئيس اللجنة الفرعية المسؤولة عن الجريمة في الكونغرس الأمريكي للتدليل على الخسائر الاقتصادية التي قد تلحق بالولايات المتحدة الأمريكية جراء الجرائم المعلوماتية[1].

ففي أحدث التقارير السنوية لمركز شكاوى احتيال الإنترنت الأمريكي، اظهر التحليل الشامل للشكاوى التي قدمت للمركز أن عددها تضاعف سنة 2002 لتصل 48252 شكوى مقارنة بما تم تسجيله سنة 2000 وسنة 2001[2]، وذلك ما يعكس الضرر التي تلحقه هذه الجرائم بالأفراد والدول، وللبحث في ذلك قام معهد الحاسوب في سان فرانسيسكو الخاص بمكتب التحقيق الفدرالي فرع جرائم الحاسوب عام 2003 على 520 مؤسسة أمريكية ووكالة حكومية بدراسة تضع أمام أعيننا حجم الأضرار المالية التي تسببها الجرائم المعلوماتية، فقد وجدت الدراسة أن 88٪ من العينة التي أجريت عليها كانوا ضحية للجريمة المعلوماتية، إذ أكد 64٪ من الذين شملهم البحث أنهم تعرضوا لسرقات معلوماتية، إضافة إلى 24٪ عانوا من الأضرار التي لحقت بأجهزتهم بسبب الفيروسات ومن بين الذين أدلوا بحجم خسارتهم أوردوا أنهم خلال عام 1997 فقدوا (137) مليون دولار،وتقدر خسائر الاقتصاد الأمريكي بسبب الجرائم المعلوماتية بـــ 250 مليار دولار هذا بالإضافة إلى تعرض نظم المعلومات بوزارة الدفاع الأمريكي لمحاولات اختراق عديدة[3]

1- مناسبة هذا الحديث الذي أدلى به لامارسميث هو موافقة مجلس النواب الأمريكي بأغلبية ساحقة على قانون يسمح بتطبيق عقوبة السجن مدى الحياة على مرتكبي الجرائم المعلوماتية الخطيرة و كان الكونجرس الأمريكي قد وافق على ما يعرف بقانون الجرائم الالكترونية بغالبية 385 صوت مقابل ثلاث أصوات رافضة،حيث يوسع هذا القانون ن قدرات الشرطة في التصنت على الاتصالات عبر الإنترنت دون الحصول على إذن مسبق من المحكمة وكانت إدارة الرئيس الأمريكي بوش الابن قد طلبت من الكونغرس الموافقة على تحسين قانون الأمن الإلكتروني كطريقة للتعامل مع مشكلات القرصنة الإلكترونية والإرهاب الإلكتروني وكان هذا القانون قد تم إعداده قبل هجمات 11 أيلول إلا أن الهجمات دعت الكونغرس إلى الإسراع بالموافقة عليه . راجع في ذلك: نهلا عبد القادر المومني، المرجع السابق،ص 67.

2- نبيلة هبة هروال، المرجع السابق، ص32.

3- نهلا عبد القادر المومني،المرجع السابق، ص67.

والدول العربية لم تكن بمنأى عن الجرائم المعلوماتية والخسائر الاقتصادية التي تسببها، وإن كانت خسائرها ليست بمقدار الخسائر التي تتكبدها الدول الغربية، وتجدر الإشارة أن الخبراء الاقتصاديين أكدوا أن المنطقة العربية ستتعرض إلى أزمة خطيرة في السنوات القليلة القادمة وذلك بسبب البطء في اتخاذ التدابير الوقائية اللازمة والذي يقابله تطور كبير في الإجرام المعلوماتي.

وفي هذا الصدد أجريت عدة دراسات في بعض دول الشرق الأوسط كالتي أجرتها منظمة Soft ware Alliance business والتي تبين من خلالها وجود تباين بين دول تلك المنطقة في حجم الخسائر، حيث تراوحت بين ثلاثة ملايين دولار أمريكي في المملكة العربية السعودية والإمارات العربية المتحدة، ومليون وأربع مائة ألف دولار أمريكي في لبنان [1]، ومن أمثلة تلك الأضرار ما يقع منها على بطاقات الائتمان وذلك لاعتبارها من أهم مقومات المعاملات الالكترونية، حيث أن هناك جانب من هذه المعاملات وهي الواقعة بين العميل والمستهلك تكون بطاقة الائتمان هي الرابط بينهما فعند وقوع احتيال في بطاقات الائتمان فإنها تؤثر ماديا على العميل كما أنها تفقد الثقة في بطاقة الائتمان التي صممت لحماية وتسهيل معاملاته عوضا عن النقد، فزيادة التلاعب والاحتيال في بطاقات الائتمان يؤثر سلبا على النمو الاقتصادي بحيث يقلل عدد مصدري حاملي هذه البطاقات وبالتالي يقل قبولها في الأسواق العالمية مما يؤثر سلبا على قطاع الفنادق والسفريات والمحلات التجارية أيضا[2].

الفرع الثالث: عدم كفاية القوانين القائمة

إذا كانت التشريعات العقابية التقليدية قد تناولت الجرائم التقليدية التي تقع على الأموال والأشخاص وغيرها بالتجريم، فإن هذه القوانين قد لا تطال غالبية الجرائم التقنية المعلوماتية وذلك لاختلاف هذه الأخيرة عن سابقتها في الطبيعة أو في الأركان أو في المحل.

وفي الواقع فإن القانون الجزائي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا أو مهارة الذهن البشري في تسخير المبتكرات للاستخدام السيئ، فالأشكال المستجدة للجريمة لم

1- نبيلة هبة هروال ، المرجع السابق ص33.
2- هشام مفيد حمود ، عمليات الاحتيال في بطاقات الائتمان، مجلة الأمن والحياة، العدد 217، السنة 19 سبتمبر/أكتوبر 2000، ص15

يقتصر اعتداؤها على القيم المادية التي كانت محمية بقانون العقوبات ، بل امتد هذا الاعتداء إلى القيم المعنوية مثل المعلومات والمعطيات وغير ذلك فأصبحت النصوص التقليدية في قانون العقوبات عاجزة عن مواكبة هذه الأشكال المستحدثة من الإجرام المعلوماتي[1].

ومن هنا فلا بد للمشرع الجنائي أن يتدخل ليتناول بالتجريم والعقاب ما يستجد من هذه الأشكال الإجرامية المعلوماتية التي لا تقع تحت سلطانه، وذلك إعمالا لمبدأ شرعية الجريمة والعقوبة والتي تعني حصر مصادر التجريم والعقاب في نصوص القانون.

ولمبدأ شرعية الجريمة والعقوبة شقان:

الأول: شرعية أو قانونية الجرائم ويعني أن كل واقعة لا يمكن أن تعد جريمة ما لم يقرر القانون ذلك.

الثاني: شرعية أو قانونية العقوبات ويعني أن المتهم لا يمكن أن يخضع لعقوبة تختلف عما يقرره المشرع، فالمشرع دون القاضي هو المختص بتحديد الأفعال التي تعد جرائم وبيان أركانها وعناصرها،وكذلك العقوبات المقررة لها من حيث نوعها أو مقدارها[2] .

فمبدأ شرعية الجريمة والعقوبة يضع نصوص القانون الجنائي في قالب ضيق ليتقيد بها القاضي عند التفسير، فلا يجوز للقاضي الجنائي التوسع في تفسير النصوص أو قياس جريمة ورد فيها نص على جريمة لم يرد فيها نص مستندا على أوجه التشابه بين الجريمتين، ومبدأ شرعية الجريمة والعقوبة وضع أساسا ليشعر الفرد بالأمان تجاه السلطة، بحيث يكون على علم مسبق بالعقوبات المقررة عليه حال ارتكابه لبعض الجرائم على العكس عند إغفال هذا المبدأ فقد يقع الفرد ضحية في يد القاضي الجنائي على اثر تفسيره الواسع لبعض نصوص القانون أو ضحية القياس بين جريمتين، ومن هذا المنطلق فإنه يتوجب على المشرع وضع نصوص مباشرة تحمي المعاملات الالكترونية من الجرائم المعلوماتية، وذلك لغلق باب الإفلات عن المساءلة الجنائية بحجة عدم وجود نصوص صريحة تحمي تلك المعاملات ووضع حد للذين يتحججون بمبدأ شرعية الجريمة والعقوبة.

1- نهلا عبد القادر المومني، المرجع السابق ، ص72 .
2- نهلا عبد القادر المومني، ص73.

المبحث الثاني

الحماية الجنائية للمعاملات الإلكترونية بنصوص خاصة

نظرا للأضرار الكبيرة التي ألحقتها الجرائم المعلوماتية بالأفراد و الدول استدعت الضرورة إلى استحداث نصوص خاصة لمواجهة هذه الجرائم كي تتحقق بها الحماية التشريعية للمعاملات الإلكترونية، ذلك ما دفع بالفكر القانوني لدى المشرعين إلى الاستقرار على ضرورة وجود نصوص خاصة بالمال المعلوماتي، وصدرت بالفعل تشريعات فدرالية ومحلية في الولايات المتحدة الأمريكية وألمانيا والدانمارك وفرنسا ...الخ.

وفي نفس السياق سار المشرع الجزائري حيث استحدث نصوصا تجريمية في تعديله الأخير لقانون العقوبات بموجب القانون رقم 15/04، حيث تناول فيه جملة من النصوص لمواجهة الإجرام المعلوماتي خصصها لحماية أنظمة المعالجة الآلية للمعطيات، فهل هذه النصوص كافية لضمان الحماية الجنائية للمعاملات الإلكترونية؟

للإحاطة بفحوى النصوص التي استحدثتها التشريعات المختلفة نتطرق في هذا المبحث إلى ثلاثة مطالب .

المطلب الأول: الحماية الجنائية لأنظمة المعالجة الآلية للمعطيات.

المطلب الثاني: الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد المقررة في جرائم الإتلاف.

المطلب الثالث: الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد المقررة في جرائم التزوير.

المطلب الأول

الحماية الجنائية لأنظمة المعالجة الآلية للمعطيات

يعد نظام معالجة البيانات أو نظم المعالجة الآلية للمعطيات بمثابة الشرط الأول الذي يلزم تحققه لكي نبحث بعد ذلك ما إذا كان هناك اعتداء على هذا النظام أو لا، ولذلك فلكي نتأكد من وجود اعتداء على قواعد بيانات المعاملات الإلكترونية في دولة ما أو مشروع ما لابد أن يكون هناك بالطبع قاعدة معالجة آلية للمعطيات التي تتعلق بهذه المعاملات الإلكترونية[1]، ونظام المعالجة الآلية للمعطيات تعبير فني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا عن أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية[2].

ونظرا لهذه الخصائص التي يتمتع بها هذا النظام فسنحاول إلقاء الضوء عليه في هذا المطلب من خلال التطرق لتعريف نظام المعالجة الآلية للمعطيات ثم نتطرق لأركان جريمة الإعتداء على هذا النظام وذلك على الشكل التالي :

الفرع الأول:تعريف نظام المعالجة لآلية المعطيات

الفرع الثاني:أركان جريمة الاعتداء على نظام المعالجة الآلية للمعطيات

1- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية 2004، ص 21.
2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية دار هومة للطباعة والنشر والتوزيع الجزائر 2007، ص 101.

الفرع الأول:تعريف نظام المعالجة لآلية المعطيات

في البداية استعمل المشرع الفرنسي مصطلح "معالجة آلية" لتنظيم حماية المعلومات الاسمية ولم يورد المشرع الفرنسي تعريف رسمي لنظام المعالجة الآلية للمعطيات في القرار المتعلق بإثراء المصطلحات المعلوماتية، رغم أنه يمثل أساس النظرية العامة للقانون المعلوماتي[1].

والمشرع الجزائري أغفل ذلك عند تناوله للمواد المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، حيث اكتفى بتقرير عقوبات للشخص الطبيعي والمعنوي حال المساس بهذه الأنظمة أو حتى الشروع في ارتكاب هذه الجنح وذلك في المواد 394 مكرر إلى غاية 394 مكرر7 ، لكنه تدارك ذلك بالقانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـــ 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث نصت المادة 2 على:

" يقصد في مفهوم هذا القانون بما يأتي:

أ- الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

ب- منظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين

ج- معطيات معلوماتية: أي عملية عرض للوقائع المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها ... " [2]

1- Raymond Gassin, Froude Informatique. Dalloz, 1995 n066 p11.

2- القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت سنة 2009 والمتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ومن ثم فإن المشرع الجزائري عرف المنظومة المعلوماتية بأنها أي نظام أو مجموعة من الأنظمة منفصلة كانت أم متصلة ببعضها البعض أو المرتبطة والتي يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، وبذلك يكون المشرع الجزائري قد أخذ بالتعريف الذي جاءت به الإتفاقية الدولية للإجرام المعلوماتي " إتفاقية بودابست " [1] .

أما الفقه الفرنسي[2] فقد عرف نظام المعالجة الآلية للمعطيات بأنه "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة أو البرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة، وهي معالجة المعطيات على أن يكون هذا الركب خاضعا لنظام الحماية الفنية[3].

من هذا التعريف يتبين لنا أن نظام المعالجة الآلية للمعطيات يقوم على عنصرين:

أولهما وهو مجموعة المركبات المادية والمعنوية التي يتم بترابطها تحقيق نتيجة معينة وهي معالجة المعطيات، وتتمثل المركبات المادية والمعنوية في كل من الذاكرة والمعطيات والبرامج وأجهزة الإدخال والإخراج وكل عنصر يمكن أن يدخل في هذه المجموعة، شرط أن يكون له دور في تحقيق نتيجة معينة وهي معالجة المعطيات.

---

1 - Art1 : a « system informatique : désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données » de : www.eastlaw.blogspot.com/2010/03/23-11-2001.html le : 16/09/2010 à 20h30mn.

2 - أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 102

3- المقصود بنظام الحماية الفنية هو إخضاع النظام المعلوماتي إلى نظام التشفير (encryptions) حيث يعمل هذا النظام على تأمين سرية البيانات المتناقلة وخاصة أعمال التجارة الرقمية والرسائل الإلكترونية والتشفير المستخدم في حماية النظام المعلوماتي له شكلين أساسيين :

La cryptalogie symétrique : أساسها أن نفس المفتاح التشفيري يستعمل للتشفير وفك الشفرة في آن واحد والمشكل الذي تطرحه هذه الطريقة أنه يجب إيجاد وسيلة لإرسال المفتاح بطريقة آمنة للمرسل إليه

cryptologie, asymétrique : ليس نفس المفتاح هو الذي يشفر ويفك الشيفرة فالمستعمل يملك مفتاحا خاصا ومفتاحا عاما فهو يوزع المفتاح العام ويحتفظ بسرية المفتاح الخاص ، ويكون لكل من يريد المراسلة أن يستعمل المفتاح العام لكن المرسل إليه وحده بإمكانه الإطلاع على مضمون الرسالة المشفرة باستعمال المفتاح الخاص .

تجدر الإشارة أن أسلوب le cryptage يواجه معارضة من قبل الحكومتين الأمريكية والبريطانية بدعوى أن المعلومات المتناقلة عبر شبكة الانترنت لا بد أن تكون مكشوفة لشركة الشبكات وتقترح الجهات الحكومية ضرورة إيداع مفتاح البيانات المشفرة لدى طرف ثالث موثوق trusted thrd party ويلقى هذا الاقتراح اعتراضا من قبل العديد من الجهات المهتمة بموضوع الأمن ومن قبل مستخدمي الشبكة. راجع في ذلك: أمال قارة، الجريمة المعلوماتية ، المرجع السابق ص 29 .

أما العنصر الثاني الذي اقترحه مجلس الشيوخ فهو ضرورة خضوع النظام لحماية فنية أي إحاطة المعلومات والنظام ككل ببرامج حماية تقيها من الاختراق الخارجي، وإن كانت هذه النقطة قد أثارت جدلا قانونيا في الفقه الفرنسي ودار التساؤل حول مدى ضرورة وجود الحماية الفنية لنظام معالجة البيانات حتى يمكن العقاب على عملية التعدي على ذلك النظام من عدمه.

فذهب الرأي الغالب إلى القول بأن الحماية الفنية ليست شرطا حتى تسبغ الحماية الجنائية على النظام الآلي لمعالجة البيانات أو المعطيات، وذلك أن القانون فضلا عن الأعمال التحضيرية لنصوص القانون يستفاد منها رفض اشتراط الحماية الفنية حتى تسبغ الحماية الجنائية[1].

ولكن يتعين ملاحظة أنه بوجود الحماية الفنية وبالرغم من ذلك يتم اختراقها فذلك دليل على سوء نية الجاني.

ومن ثم ذهب رأي آخر إلى القول بضرورة وجود نظام أمني للحماية الفنية لنظم المعالجة الآلية للمعطيات حتى يمكن تجريم التعدي على ذلك النظام، وذلك لأن كسر الحماية الفنية لهذا النظام شرط لقيام الجريمة الجنائية، كما أن اعتبارات العدالة تقتضي عدم العقاب على فعل يمثل اعتداء على حق لم يتحوط له صاحبه[2].

لكن بالرغم من اعتبار اختراق الحماية الفنية للنظام المعلوماتي دليل على سوء نية الجاني إلا أننا نرى بأن التسليم بضرورة وجود الحماية لكي يمكن العقاب على عملية التعدي سيفتح باب التهرب للمجرمين من المساءلة الجنائية، بحجة أن النظام المتعدى عليه لم يكن محاطا بحماية فنية تمنع الاختراق، ومن ثم فالحماية الجنائية في نظرنا واجبة سواء تم إحاطة النظام المعلوماتي بحماية فنية أولا، أضف إلى ذلك فالمشرع الجزائري على سبيل المثال لا الحصر لم يشترط في النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات أن يكون النظام محاطا بحماية فنية، فقد جاءت تلك النصوص مطلقة أي تحمي الأنظمة المعلوماتية سواء كانت محمية فنيا أولا ومن ثم فإنه لا يجوز تقييد تلك النصوص.

1- د/ عبد الفتاح بيومي حجازي، الحكومة الالكترونية ونظامها القانوني،المرجع السابق، ص 359.
2- د/ عبد الفتاح بيومي حجازي،ص 359.

كما أن المشرع الجزائري في نص المادة الثانية من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لم يشترط في الفقرة "ب" والمتضمنة تعريف المنظومة المعلوماتية أن تكون هذه المنظومة محاطة بحماية فنية حتى يتم تجريم الاعتداء عليها، وذلك ما يستنتج أيضا من نص الاتفاقية الدولية للإجرام المعلوماتي، حيث جاء في مادتها الأولى :" نظام الكمبيوتر عبارة عن جهاز أو مجموعة من الأجهزة المترابطة ذات الصلة فيما بينها والتي يحقق واحد منها أو أكثر تنفيذ برنامج لتجهيز البيانات آليا[1].

ومما سبق يمكن القول أن نظام المعالجة الآلية للمعطيات هو كل مجموعة مكونة من وحدة أو عدة وحدات للمعالجة أيا كانت تلك الوحدات، شرط أن تساهم في الحصول على نتيجة محددة وهي معالجة البيانات.

الفرع الثاني:أركان جريمة الاعتداء على نظام المعالجة الآلية للمعطيات

إن من أبرز صور الاعتداء على نظام المعالجة الآلية للمعطيات هو الدخول إلى النظام والبقاء فيه بدون إذن، وتبدأ هذه الجريمة بالفضول للدخول إلى النظام ثم بعد ذلك تتطور لتمتد إلى جرائم أخرى كإتلاف البيانات أو سرقتها أو غير ذلك من الجرائم، أو تبدأ بنية الجاني في ارتكاب بعض الجرائم وذلك قبل اختراقه للنظام.

ولذلك سنتطرق في هذا العنصر للركن المادي والمعنوي لجريمة الدخول والبقاء دون إذن في نظام المعالجة الآلية للمعطيات.

أولا: الركن المادي لجريمة الاعتداء على نظام المعالجة الآلية للمعطيات

يتمثل الركن المادي فيما تبدو عليه الجريمة في شكلها الخارجي، ويمكن تناولها هذا العنصر من خلال التعرض لجريمة الدخول والبقاء دون إذن في نظام المعالجة الآلية للمعطيات ثم بعد ذلك نتعرض للاعتداء العمدي على معطيات النظام.

1- www.eastlaws.blogspot.com/2010/03/23_11_2001.html le : 16/09/2010 à 20h30mn

1/ الدخول والبقاء دون اذن في نظام المعالجة الآلية للمعطيات:

قبل التطرق لمعنى الدخول والبقاء دون إذن في النظام المعلوماتي نتعرض أولا للجدل الفقهي الذي ثار حول مدى انطباق وصف الجريمة المعلوماتية على الشخص الذي يدخل النظام المعلوماتي ويبقى فيه، وبالتالي هل تستوجب الحماية الجنائية لذلك النظام أم لا وكان في هذا الخلاف اتجاهين:

الاتجاه الأول: يرى أنه لا توجد ضرورة تستدعي تجريم مجرد الدخول أو البقاء غير المصرح بهما على النظام المعلوماتي وخاصة إذا لم يكن لدى الفاعل نية لارتكاب جريمة لاحقة على هذا الدخول أو البقاء، ويبرر هذا الاتجاه رأيه أن هذا السلوك لا يخرج عن كونه طريقة لعرض القدرات التقنية والذهنية التي يتمتع بها الشخص الذي قام بهذا الفعل وهذا الأمر لا يشكل بحد ذاته جريمة تستدعي معاقبة الفاعل[1].

الاتجاه الثاني: يذهب هذا الاتجاه إلى ضرورة تجريم الدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي حتى ولو لم يكن ذلك بقصد ارتكاب جريمة لاحقة فيما بعد[2]، فالقول بعدم تجريم الدخول والبقاء في النظام المعلوماتي الذي لا تتبعه نية من قبل الجاني في ارتكاب جرائم أخرى قد يفتح الباب بمصرعيه للمتطفلين بغرض التجسس على المعلومات والتحجج بعد ذلك بعدم ارتكاب جرائم أخرى ملموسة كالسرقة أو الإتلاف.

ويعزز هذا الاتجاه رأيه بالإشارة إلى أن هناك خسائر مادية قد تترتب على حالات الدخول غير المصرح به على النظام المعلوماتي و التي قد تكون نتيجة مجرد محاولة وقف هذا الدخول، حيث تشير التقديرات إلى أن هناك الآن ما يزيد عن مئة ألف خبير استشاري في المجال المعلوماتي يعملون في أكثر من 20 ألف شركة في العالم وبلغ مجموع ما أنفقته الشركات على خدمات الاستشارة المعلوماتية 4.5 بليون دولار وكل ذلك من أجل ضمان أمن المبادلات الالكترونية[3]

1- نهلا عبد القادر المومني، المرجع السابق، ص 156.
2- نهلا عبد القادر المومني، ص 156.
3- محمود أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية، دار الثقافة للنشر و التوزيع، عمان 2005 ص81.

مما سبق تبدو الحاجة ملحة للأخذ بالرأي الثاني، لما قد يلحقه الدخول والبقاء غير المصرح به من ضرر بالنظام المعلوماتي.

وذلك ما أخذ به المشرع الفرنسي في نص المادة 323-1 من قانون العقوبات[1]، وحذا حذوه المشرع الجزائري حيث نص في المادة 394 مكرر من قانون العقوبات على: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 دج إلى 100000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك .

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج".

كما أصدر المشرع الإنجليزي قانون إساءة استخدام الكمبيوتر عام 1990، وجاء في مادته الأولى تجريم فعل الدخول الغير المشروع إلى النظام المعلوماتي، سواء قصد الجاني تدبير الدخول إلى أي برنامج أو بيانات موضوعة في أي كمبيوتر فقط أو نتج عن دخوله أضرار بعمل المنظومة [2].

وكلاهما يمثلان الركن المادي لجريمة الدخول والبقاء دون إذن في نظام المعالجة الآلية، ففعل الدخول أو البقاء بغش دون إحداث إتلاف أو تخريب للنظام يمثل الصورة البسيطة للجريمة، أما الصورة المشددة فتتحقق بتوافر نتيجة عن فعل الدخول أو البقاء [3] وذلك ما سنتناوله بتفصيل أكثر بتناول كل صورة على حدة .

1- Art 323-1 « le fait d'accéder ou de se maintenir frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement, et de 30 000 euros d'amende . Lorsqu'il en est résulté soit la suppression ou la modification de données, continues dons le système , soit une altération de fonctionnement de ce système, la peine est de 3ans d' emprisonnement et de 45 000 euros d'amende ». code pénal français, date de derrière modification le : 01/12/2011, édition 2011.

2 - Smith and Hogan criminal law (seventh edition). Butter worths London 1992 .p.715

3- مناصرة يوسف ،المرجع السابق، ص57 .

-الصورة البسيطة لجريمة الدخول والبقاء دون إذن في نظام المعالجة الآلية للمعطيات:

نتطرق في هذه الصورة لكل من فعل الدخول و فعل البقاء:

أ- فعل الدخول بدون إذن لنظام المعالجة الآلية للمعطيات:

فعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي أي الدخول المعنوي أو الإلكتروني[1].

ويرى الفقه الفرنسي أن الدخول له مدلول معنوي، حيث يشبه الدخول إلى النظام الدخول في ذاكرة الإنسان، كما أن له مدلول مادي يتمثل في أن الشخص قد يكون حاول الدخول

أو دخل بالفعل إلى النظام المعلوماتي، ووفقا للتصور المعنوي لفكرة الدخول فإنه يتحقق بأي صورة من صور التعدي أي يستوي أن يكون التعدي مباشرا أو غير مباشر[2].

وفعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكا غير مشروع وإنما يتخذ هذا الفعل وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق، أو بمعنى آخر دون تصريح، ومن الحالات التي يكون فيها الدخول غير مشروع إلى النظام المعلوماتي:

- دخول الفاعل إلى النظام المعلوماتي دون الحصول على تصريح من المسئول عن النظام أو مالكه، وقد يكون الفاعل مصرحا له بالدخول إلى جزء من النظام إلا أنه يتجاوز التصريح الممنوح له ويدخل إلى كامل النظام المعلوماتي أو إلى أجزاء أخرى يحظر عليه للدخول إليها، وهذا الفرض في الغالب يتم من قبل العاملين في المؤسسات التي يوجد بها النظام المعلوماتي

- يمكن أن يحصل الدخول دون إذن باختراق النظام المعلوماتي عن طريق الحصول على شفرات خاصة أو استخدام فيروس يتم دمجه في إحدى البرامج الأصلية للحاسب الآلي كي يعمل

1- نهلا عبد القادر المومني، المرجع السابق، ص 158.
2- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق،ص 28.

كجزء منه، ثم يقوم بتسجيل الشفرات التي يستعملها المستخدمون الشرعيون للدخول إلى الكمبيوتر[1].

وتعتبر هذه الطريقة من بين أحد التقنيات الأكثر استخداما لارتكاب جريمة الدخول دون إذن للنظام، وهناك طرق أخرى يتم استخدامها لارتكاب هذه الجريمة مثل:

- استخدام البرامج المخصصة لتخطي أنظمة الحماية الفنية للحيلولة دون الاتصال غير المشروع بالبرامج والبيانات المخزنة، حيث أن إدارة وتشغيل البيانات والحاسبات بطريقة آمنة خاضعة للتحكم والسيطرة بوجود نوع من البرامج، حيث يمكن استخدام هذا الأخير من تخطي حواجز الحماية الفنية لمنظومات الحاسب في الحالات الطارئة وحالات اختلال وظائف الحاسب أو توقفه عن العمل[2].

- طريقة القناع وذلك بأن يقوم القرصان بإقناع الحاسوب بأنه شخص مرخص له بالدخول وهناك طريقة أخرى تتمثل في استعمال نقاط الضعف الموجودة على مستوى نظام الاستغلال وتقع هذه الجريمة من كل شخص أيا كانت صفته، أي أنها ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة وإنما ترتكب من أي شخص سواء كان يعمل في مجال الأنظمة أو لا وسواء كان يستطيع أن يستفيد من الدخول أو لا، فيكفي أن يكون الجاني ليس ممن يكون لهم الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، فتتوافر الجريمة في كل حالة يكون فيها الدخول مخالفا لشروط الدخول التي نص عليها القانون أو الاتفاق أو مخالفا لإرادة من له الحق في السيطرة على النظام[3].

وأيا كانت الطريقة التي تم بها الدخول إلى النظام المعلوماتي فالتعمد في اختراق نظام المعالجة الآلية للمعطيات يحقق جريمة الدخول دون إذن.

1- د/ نعيم مغبغب، حماية برامج الكمبيوتر، (الأساليب والثغرات)، منشورات الحلبي الحقوقية، لبنان 2006، ص 235.
2- أمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 108
3- أمال قارة، ص 109.

وذلك ما حكمت به محكمة جنح ولاية باتنة، حيث قضت في أحد أحكامها بإدانة متهم لدخوله الغير مشروع لأحد الأنظمة المعلوماتية التابعة لمنظمة أمريكية واعتبرت أن ذلك فعل مجرم طبقا للمادة 394 مكرر من قانون العقوبات[1] .

كما عالجت الإتفاقية الدولية للإجرام المعلوماتي "اتفاقية بودابست" هذا الفرض وذلك في مادتها الثانية [2] حيث أنها جرمت مجرد الدخول إلى نظام المعالجة الآلية للمعطيات سواء أكان الدخول لجزء فقط من المنظومة أو لكاملها، كما أعطت الإتفاقية الحرية للدول الأطراف أن تشترط في قوانينها بأن يكون تجريم الدخول للنظام المعلوماتي مرتبط بإختراق التدابير الأمنية أو لا، أي الحرية في اشتراط وجود حماية فنية للنظام حتى يتم تجريم الدخول إليه، وقد تم التطرق في بداية هذا العنصر للاتجاهات المختلفة حول مدى وجوب الحماية الفنية لإسباغ الحماية الجنائية على النظام المعلوماتي، و أعطت الإتفاقية حرية الإختيار للدول الإعضاء في تجريم فعل الدخول فقط أو اشتراط أن يكون الغرض هو الحصول على بعض البيانات أو غرض آخر غير أمين كالسرقة أو الإتلاف مثلا أي البحث في مدى توافر القصد الجنائي من عدمه، وذلك ما سنتطرق له في الركن المعنوي لجريمة الدخول والبقاء دون إذن في النظام المعلوماتي.

1- وذلك في حكم لها صدر بتاريخ 1-6-2010 في قضية قام فيها أحد الأشخاص من ولاية باتنة بالدخول عن طريق الغش إلى منظومة معلوماتية لمؤسسة أمريكية تعرف باسم Sagonet works والتي تعتبر بنك معلوماتية كبير بولاية فلوردا الأمريكية حيث أن المتهم أبلغ المؤسسة الأمريكية بأنه أكتشف طريقة للدخول عن طريق الغش إلى المعطيات الإلكترونية المخزنة لديها وذلك عبر نظام المشغل logiciel والمسمى Ubersmith وذلك ما تم التأكد منه فعلا على موقع Unknown.wn ما يثبت صحة الدخول عن طريق الغش إلى منظومة المؤسسة الأمريكية. وعلى ذلك قضت المحكمة بإدانة المتهم بجريمتي الدخول عن طريق الغش في منظومة معلوماتية طبقا للمواد 394 مكرر و394 مكرر 2 و394 مكرر 06 من ق.ع والحكم عليه بعام حبسا نافذا و50.000 دج غرامة نافذة مع مصادرة المحجوزات وباستئناف الحكم من طرف المتهم والنيابة جاء في حيثيات قرار مجلس قضاء باتنة أن دفع المتهم بأنه دخل عن طريق الخطأ غير مؤسس وتعين رفضه لأنه دخل متعمدا وباع المعلومات المتحصل عليها وتحصل مقابل ذلك على مبالغ مالية وأن سوء النية ثابت بالدخول والاختراق للمنظومة المعلوماتية للغير وأن أركان جنحتي الدخول عن طريق الغش في منظومة للمعالجة الآلية، والبحث والتجميع والنشر والاتجار في معطيات مخزنة معالجة ومرسلة عن طريق منظومة معلوماتية ثابتة في حقه مما يتعين إدانته والحكم عليه طبقا للمواد 394 مكرر و394 مكرر2 و394 مكرر 6 من ق.ع وعلى ذلك فقد ثبت للمجلس بأن الحكم المستأنف قد أصاب وطبق صحيح القانون مما يتعين تأييده مبدئيا وتعديله بعد إسعاف المتهم بظروف التخفيف طبقا للمادة 53 من ق.إ.ج لأنه لم يسبق الحكم عليه من قبل بأية عقوبة سالبة للحرية بجعل ستة أشهر حبس نافذة في حقه وستة أشهر حبس موقوفة التنفيذ. أنظر مجلس قضاء باتنة، الغرفة الجزائية، بتاريخ: 2010/07/04 قرار رقم :10/05805

2- Art 2 « chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale conformément à sont, droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique, une partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention délictueuses ou soit en relation avec un système informatique connecté à un autre système informatique » de : www.eastlaw.blogspot.com/2011/03/23- 11-2001.html le: 16/09/2010 à : 20h30mn.

كما نصت المادة 3 من قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات على أن "كل من دخل عمدا وبغير وجه حق موقعا أو نظاما معلوماتيا يعاقب بالحبس ..، والغرامة .... أو بإحدى هاتين العقوبتين"[1].

فنص المادة جاء واضحا في شروط توقيع إحدى العقوبتين السابقتين، فيستثنى من توقيع العقوبة من يجد نفسه بطريق الخطأ أو الصدفة داخل نظام المعالجة الآلية للمعطيات وتقع على من اخترق النظام دون وجه حق.

وتجدر الإشارة في الأخير إلى أن جريمة الدخول بدون إذن على النظام المعلوماتي تعد من الجرائم الشكلية التي لا يتطلب لقيام الركن المادي فيها نتيجة ما، فبالرغم من إمكانية حدوث أضرار معينة بالمعلومات سواء بمحوها أو بتعديلها أو إفساد نظام التشغيل نتيجة عملية الدخول غير المصرح به إلا أن ذلك لا يغير من طبيعة الجريمة باعتبارها جريمة شكلية[2].

ب- البقاء دون إذن في نظام المعالجة الآلية للمعطيات:

قد يجد شخص نفسه داخل نظام لحاسب آلي عن طريق الخطأ كما لو كان في طريقه للدخول إلى نظام له الحق في الدخول إليه ثم وجد نفسه بسبب خطأ ما كاستخدام شفرة خاطئة على سبيل المثال داخل نظام آخر، وفي هذه الحالة قد يقوم هذا الشخص بالخروج من هذا النظام بمجرد تبينه للخطأ الذي وقع فيه، وقد يستمر في البقاء داخل النظام على الرغم من معرفته أن هذا النظام غير مصرح له بالدخول إليه[3].

وهذا الفرض الأخير هو محل الدراسة فالمقصود بالبقاء دون إذن في النظام المعلوماتي هو التواجد داخل هذا النظام بالمخالفة لإرادة الشخص صاحب النظام أو من له السيطرة عليه.

1- تم اعتماد قانون اللإمارات العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات في الدورة التاسعة عشرة لمجلس وزراء العدل ومجلس وزراء الداخلية العرب و ذلك بالقرار رقم:495 بتاريخ 2003/10/08. أنظر الوقع:
www.arabic.mjustice.dz. Le 09/11/2010 a:11h00mn

2- نهلا عبد القادر المومني، المرجع السابق، ص 159..

3- د/ محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة 2010، ص 459

ويتحقق الركن المادي لجريمة البقاء غير المصرح به داخل النظام المعلوماتي في الحالة التي يجد فيها الشخص نفسه داخل النظام عن طريق الخطأ أو الصدفة إلا أنه يقرر البقاء داخل النظام وعدم قطع الاتصال به [1]، و البقاء المعاقب عليه قد يتحقق مستقلا عن الدخول إلى النظام وقد يجتمعان، ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو إذ يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي، ويكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح له بالبقاء فيها داخل النظام أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها بالرؤية والإطلاع فقط، وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الفرض الذي لا يكون فيه للجاني الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه ثم يبقى داخل النظام بعد ذلك ويتحقق في هذا الفرض الاجتماع المادي للجرائم[2].

و جريمة البقاء دون إذن داخل النظام المعلوماتي بشكل عام تعتبر من الجرائم التي يصعب تقديم دليل على إثباتها، حيث يزعم المتهم في حالة القبض عليه أنه كان على وشك الانفصال عن النظام المتعدى عليه[3]، ذلك ما يدفعنا للتساؤل عن الوقت الذي تنتهي به جريمة الدخول وتبدأ فيه جريمة البقاء وبصيغة أخرى ما هو الحيز الزماني الذي تستغرقه كل جريمة على حدا ؟

ذهب جانب من الفقه إلى القول بأن جريمة الدخول تتحقق منذ اللحظة التي يتم الدخول فيها فعلا إلى البرنامج 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[4].

2- نهلا عبد القادر المومني، المرجع السابق ، ص 161
2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 110.
3- نهلا عبد القادر المومني، ص 161.
4- أمال قارة، ص112

ما يؤخذ على هذا الاتجاه 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 هذا الرأي صعوبة إثبات علم المتدخل.

في حين ذهب رأي ثالث إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع وأصبح غير مشروع، فإذا لم ينسحب فهو يرتكب منذ تلك اللحظة جريمة البقاء داخل النظام، ولكن إذا أمكن توفير هذا الرأي فنيا فإنه لن يكون متاحا إلا بالنسبة للشركات أو المؤسسات الكبيرة فقط[1].

ومن جانبنا يمكننا القول بأن جريمة الدخول تنتهي في الوقت الذي يجد فيه الفاعل نفسه داخل النظام، أي عند إتمام كل الطرق الفنية للدخول لأننا في فرض يكون فيه الجاني على علم بأنه غير مخول لدخول النظام، وبتحقق جريمة الدخول تبدأ جريمة البقاء أي منذ علم الجاني بأنه داخل النظام سواء كان داخل النظام ككل أو في جزء منه فقط.

ومما لا شك فيه أن سبب التفرقة بين الجريمتين يعود لكون جريمة الدخول إلى النظام تعتبر جريمة وقتية في حين أن جريمة البقاء تعد جريمة مستمرة، لذلك جاء نص المشرع الجزائري و الفرنسي صريحا في التطرق للدخول ثم البقاء ذلك ما يعني اختلاف الجريمتين .

وفي هذا الصدد ذهبت محكمة استئناف باريس في حكم صادر لها بتاريخ 5 أبريل 1999 إلى أن القانون يجرم البقاء غير المشروع داخل نظام الحاسب الآلي، سواء أكان الدخول قد تم بطريق الخطأ أو تم بطريقة مشروعة، إلا أنه اكتسب بعد ذلك صفة عدم المشروعية كما لو فقد الفاعل صفة البقاء نتيجة لخطأ من جانبه[2].

إن جريمة البقاء تعد من الجرائم الشكلية التي لا يشترط فيها حدوث نتيجة جرمية معينة فيكفي البقاء غير المصرح به ليقوم الركن المادي لهذه الجريمة[3].

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 112.
2- د/ محمد عبد الكعبي، المرجع السابق، ص 463.
3- نهلا عبد القادر المومني، المرجع السابق، ص 161.

-الصورة المشددة لجريمة الدخول أو البقاء دون إذن في نظام المعالجة الآلية للمعطيات:

تنص المادة 323/ 1 من قانون العقوبات الفرنسي في فقرتها الثانية[1]: "إذا نجم عن الدخول محو أو تعديل في المعطيات المخزنة في هذا النظام أو إتلاف تشغيل هذا النظام تكون العقوبة لمدة ثلاث سنوات وغرامة مقدارها 45000 يورو".

و تنص المادة 394 مكرر من قانون العقوبات الجزائري: "يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 50000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50000 إلى 150000دج".

جاء نص المشرع الفرنسي في فقرته الثانية والمشرع الجزائري في فقرتيه الثانية والثالثة لتبيان الصورة المشددة لجريمة الدخول والبقاء غير المصرح بهما، حيث تتحقق الجريمة في ظرفها المشدد إذا نتج عن الدخول أو البقاء محو أو تعديل في البيانات التي يحتويها النظام أو إعاقة النظام عن أداء مهامه.

ويكفي لتوافر الظروف المشددة أن تكون هناك علاقة سببية ما بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت وهي محو في النظام أو عدم قدرته على أداء وظيفته أو تعديل البيانات، وهذه النتيجة ذاتها هي التي اعتبرها المشرع ظرفا مشددا في هذه الجريمة[2].

كما لا يشترط أن تكون النتيجة الضارة مقصودة أي على سبيل الخطأ غير العمدي، فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة العمدية وهي جريمة الدخول أو

1- Art 323/1 : «… Lorsqu'il en est résulté soit la suppression ou la modification de données, continues dons le système , soit une altération de fonctionnement de ce système, la peine est de 3ans d' emprisonnement et de 45 000 euros d'amende ». code pénal français, édition 2011,

2- د/ عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، المرجع السابق، ص 362.

البقاء غير المشروع العلاقة السببية السابقة الذكر 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[1].

فمتى تحققت أركان جريمة الدخول أو البقاء غير المشروع في صورتها المشددة عوقب الجاني بالعقوبة المقررة لها وهي الحبس لمدة 6 أشهر إلى سنتين والغرامة من 50000 دج إلى 150000دج في القانون الجزائري، وعقوبة الحبس لمدة ثلاث سنوات وغرامة تقدر بـــ 45000 يورو في القانون الفرنسي، والعلة من هذا التشديد هو ما آلت إليه المعاملات الإلكترونية اليوم من أضرار بالغة نتيجة تطور تقنيات الإجرام المعلوماتي، ما استوجب على المشرع التدخل لتشديد العقوبة قصد درء بعض مفاسد هذه الجرائم.

2- الاعتداء العمدي على معطيات النظام:

يقصد بالاعتداء العمدي على معطيات النظام أن توجه هجمات إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المساس بالسلامة والمحتوى والتكاملية أو تعطيل القدرة والكفاءة للأنظمة التي تحول دون القيام بأعمالها[2].

وهدف هذا النمط الإجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات، وذلك بهدف السيطرة على النظام دون تصريح أو المساس بسلامة المعلومات وتعطيل القدرة لخدمات الكمبيوتر، ويلاحظ أن غالبية محاولات الاعتداء على النظم المعلوماتية تتم من خلال برامج متوفرة على الانترنيت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير.

ومن ضمن جرائم الاعتداء على الأنظمة المعلوماتية أنشطة الاقتحام أو الدخول أو التواصل غير المصرح به مع نظام الكمبيوتر، وقد يكون إما مجردا أو بغرض ارتكاب فعل آخر ضد البيانات

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 114.
2- د/ خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، ، الدار الجامعية الإسكندرية، ، ص84

والبرامج والمخرجات وتخريب المعطيات والنظم والممتلكات وإيذاء الكمبيوتر واغتصاب الملكية وخلق البرمجيات الخبيثة والضارة ونقلها عبر النظم وشبكات الاتصال[1].

والاعتداء العمدي على معطيات النظام يتخذ صورتين إما الاعتداء على المعطيات الموجودة داخل النظام أو على التي تكون خارجه.

الصورة الأولى: الاعتداء العمدي على المعطيات الموجودة داخل النظام

جرمت المادة 03 من اتفاقية الإجرام المعلوماتي اتفاقية "بودابست "واقعة الاعتراض العمدي وبدون حق وذلك باستخدام وسائل فنية للإرسال الغير العلني لبيانات الحاسب في مكان الوصول وفي المنشئ أو في داخل نظام المعلوماتي [2].

نص الاتفاقية يجرم الاعتداء العمدي للبيانات داخل النظام، وذلك ما نص عليه أيضا المشرع الجزائري في المادة 394 مكرر 1 من قانون العقوبات: "يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500000دج إلى 2000000دج كل من أخل بطريق الغش معطيات في نظام المعالجة الآلية وأزال أو عدل بطريق الغش المعطيات التي يتضمنها".

كما تنص المادة 01/323 من قانون العقوبات الفرنسي في الفقرة الثانية على تشديد العقوبة إذا نجم عن الدخول غير المشروع محو أو تعديل في المعطيات أو إتلاف تشغيل النظام.

ما يلاحظ في المواد السابقة الذكر اتفاقها في صور الاعتداء العمدي على المعطيات الموجودة داخل النظام، والتي يمكن حصرها في: الإدخال والمحو والتعديل، وما تجدر الإشارة إليه أنه لا يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوفر الركن المادي، والنشاط الإجرامي هنا يجب أن يقع على المعطيات أو المعلومات التي تمت معالجتها آليا

1- د/ خالد ممدوح إبراهيم، المرجع السابق، ص 85.

2- Art 3 : « interception illégale . chaque partie adopte les mesures législatives et autres qui se révélant nécessaires l'interception intentionnelle et sans droit , éffectuée par des moyens technique , de données informatiques , lors de transmissions non publiques, à destination en provenance ou à l'intérieur d'un système informatique » de : www.eastlaws.blogspot.com le : 16/09/2010 à : 20h30mn.

والتي أصبحت عبارة عن إشارات أو رموز تمثل تلك المعلومات، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام أي التي يحتويها النظام وتشكل جزءا منه.

والاعتداء العمدي على المعطيات الموجودة داخل النظام يتخذ احد الصور التالية:

الإدخال: يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة به سواء كانت خالية أم يوجد عليها معطيات من قبل، وهذه الجريمة تقع غالبا بمعرفة المسئول عن القسم المعلوماتي والذي يسند إليه وظائف المحاسبة والمعاملات المالية لأنه يكون في أفضل وضع يؤهله لارتكاب هذا النمط من التلاعب غير المشروع[1].

المحـــو: يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة[2].

التعديل: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى ويتحقق فعل المحو والتعديل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها، وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات أو برامج الفيروسات بصفة عامة وهذه الأفعال المتمثلة في الإدخال والمحو والتعديل وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى ولو تضمن اعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات، فلا يخضع لتلك الجريمة فعل نقل البيانات أو التنسيق أو التقريب بينها، لأن كل تلك الأفعال لا تنطوي على إدخال ولا تعديل بالمعنى السابق[3].

الصورة الثانية: الاعتداء العمدي على المعطيات الموجودة خارج النظام

يقصد بالمعطيات الموجودة خارج النظام تلك التي لها دور في تحقيق نتيجة معينة تتمثل في المعالجة الآلية للمعطيات وقد نص المشرع الجزائري في المادة 394 مكرر 2 من قانون العقوبات

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 120.
2- د/ عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، المرجع السابق، ص 365.
3- أمال قارة، ص 122.

على أن "يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة من 1000000دج إلى 5000000دج كل من يقوم عمدا أو عن طريق الغش بما يأتي:

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

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

بتحليل نص المادة يتضح لنا أن المشرع الجزائري يحمي المعطيات سواء أكانت داخل النظام المعلوماتي أو خارجه، فالمشرع يقصد بالمعطيات المخزنة تلك تكون على دعامة خارجية كالأقراص أو تكون مخزنة داخل النظام ذاته في الذاكرة مثلا، أما المعطيات المعالجة هي التي أصبحت جزءا من النظام أي أصبحت عبارة عن إشارة أو رموز تمثل معلومات معالجة آليا، وقد تكون تلك المعطيات مرسلة عن طريق منظومة معلوماتية كتبادل وإرسال المعلومات بين أجهزة المنظومة المعلوماتية،كما يجرم المشرع في الفقرة الثانية أفعال الحيازة أو لإفشاء أو النشر أو الاستعمال للمعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم السابع من قانون العقوبات، فنص المادة 394 مكرر 2 جاء مطلقا، فلم يشترط أن تكون المعطيات داخل نظام معالجة آلية ومن ثم فإنه لا يجوز تقييد النص بحمايته للمعطيات الموجودة داخل النظام فقط، هذا فيما يتعلق بالاعتداء العمدي على المعطيات الموجودة خارج النظام، لكن ما تجدر الإشارة إليه أن المشرع الجزائري أغفل استحداث نص يتعلق بالاعتداء العمدي على سير النظام، وربما يكون مرد ذلك أن المشرع باستحداثه النصوص التي تجرم الاعتداء على المعطيات المعالجة آليا سواء أكانت داخل النظام المعلوماتي أو خارجه يكون بذلك قد تناول جانبا من تجريم الاعتداء على سير النظام، فالاعتداء على النظام بتخريبه من شأنه أن يعيب عملية سير النظام ومن ذلك يبدو أن المشرع الجزائري جرم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات والتي من شأنها التأثير على عملية سير النظام المعلوماتي، وقد تتخذ الأفعال الماسة بسير النظام عدة صور مثل:

التعطيل أو العرقلة: قد تكون عملية التعطيل مادية أو معنوية، فتكون مادية متى وقعت على الأجهزة المادية للنظام كتحطيم الأسطوانة أو قطع شبكة الاتصال، وقد تكون وسيلة التعطيل معنوية إذا وقعت على الكيانات المنطقية للنظام مثل البرامج والمعطيات وذلك بإتباع التقنيات التالية:

- إدخال برنامج فيروسي[1].
- استخدام قنابل منطقية.
- جعل النظام يتباطأ في أدائه لوظائفه.

الإفساد: يقصد بالإفساد كل فعل وإن كان لا يؤدي إلى التعطيل بل الى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال، ذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها[2]، وأيا كانت الطريقة المتبعة في الاعتداء على سير نظام المعالجة الآلية للمعطيات فهي في الأخير تحول دون تحقيقه لوظائفه، وكان الأولى بالمشرع الجزائري إضافة نص يجرم المساس بسير نظام المعالجة الآلية للمعطيات ما يحول دون استنتاج ذلك التجريم من نصوص أخرى.

ثانيا: الركن المعنوي لجريمة الاعتداء على نظام المعالجة الآلية للمعطيات

يمثل الركن المعنوي الأصول النفسية لماديات الجريمة والسيطرة النفسية عليها، فهو في جوهره قوة نفسية وهذه القوة هي الإرادة وتعد هذه الإرادة الإجرامية دليلا على خطورة شخصية الجاني، وتعد كذلك جوهر الركن المعنوي، هذا الأخير الذي يمثل ركن المسئولية الجنائية فإذا انتفى الركن المعنوي كنا بصدد مانع من موانع المسئولية الجنائية، ويتطلب الركن المعنوي في الفاعل توافر الأهلية الجنائية، كما يتطلب عنصرين: وجود إرادة معتبرة قانونا واتجاه هذه الإرادة إلى نحو مخالف للقانون[3].

1-اشتق مصطلح الفيروس من العلوم البيولوجية وهو يعني بالاتينية " سم " وقد أصابت الفيروسات الحاسب الآلي قبل تسميتها بهذا الإسم وأول من أطلق عليها هذا الإسم هو Fredcohen في عام 1983 ويرجع الفضل إليه في إيضاح سهولة كتابة برامجها وسهولة إخفائها وأشار إلى قدرتها الإنتشارية السريعة في شبكات الإتصال وبعد معرفة هذه الحقيقة أمكن وضع البرامج التي تكشف وجود الفيروس والقضاء عليه، وقد سجل أول اكتشاف للفيروس في مدينة "لاهور" في باكستان عام 1987 وأطلق عليه إسم "Brain" اشتقاقا من الاسم الموقع على الأسطوانة المرنة التي يسكنها الفيروس. مشار إليه لدى : محمد علي العريان ، المرجع السابق ، ص 83.
2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 116- 119.
3- د/ محمد عبيد الكعبي، المرجع السابق، ص 480.

فالركن المعنوي هو القصد الجرمي أي القيام بالعمل عن علم وإرادة، فأغلب التشريعات الدولية تتطلب توفر هذا القصد لاكتمال الجرم[1].

وفي هذا العنصر سنتطرق للركن المعنوي لكل من جريمة الدخول والبقاء دون إذن في نظام المعالجة الآلية للمعطيات وجريمة الاعتداء العمدي على معطيات النظام.

1- الركن المعنوي لجريمة الدخول والبقاء دون إذن في نظام المعالجة الآلية للمعطيات

جريمة الدخول أو البقاء داخل النظام جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصرية العلم والإرادة، فيلزم لكي يتوافر هذا الركن أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء داخل نظام المعالجة الآلية، وأن يعلم الجاني بأنه غير مخول للدخول إلى النظام أو البقاء فيه [2]، أما إذا اعتقد الفاعل بناءا على أسباب معقولة انه يقوم بإجراء بعض العمليات عن طريق الحاسب الآلي دون أن يتجه علمه إلى أنه يقوم بالدخول إلى نظام الحاسب بما يحتوي عليه من معلومات وبيانات، فإن القصد الجنائي العام في جريمة الدخول لا يتوافر لديه وعلى الرغم من الأهمية القانونية لذلك، إلا أنه من الناحية العملية يفقد هذه الأهمية لأنه نادرا ما يدخل الفاعل على نظام الحاسب الآلي وهو غير عالم بذلك نظرا للخبرة التي يتمتع بها المجرم المعلوماتي في اغلب الأحوال والتي تمنع التسليم بهذا الفرض، ومع ذلك إذا ثبت انتفاء هذا العلم وجب أن ينتفي القصد الجنائي بدوره. [3]

وقد جاء في نص المادة 394 مكرر من قانون العقوبات الجزائري: "كل من يدخل أو يبقى عن طريق الغش.." فالدخول أو البقاء في النظام عن طريق الغش يحقق صورة القصد الجنائي فالجاني تبدو نيته في اختراق النظام واضحة، وذلك من خلال تتبعه للمراحل الفنية للاختراق، فنظام الحماية الفنية كما سبق وأن ذكرنا ليس شرطا لتحقق الحماية الجنائية بل تسبغ هذه الأخيرة حتى ولو لم يكن النظام محاطا بحماية فنية، لكن الدور الأساسي الذي تلعبه الحماية الفنية أنها وسيلة لإثبات أن دخول الجاني كان بطريق غير مشروع، فعند إقدام الجاني لدخول النظام واصطدامه

1- د/ نعيم مغبغب، المرجع السابق، ص 238.
2- مناصرة يوسف ، المرجع السابق ، ص64.
3- د/ محمد عبيد الكعبي، المرجع السابق، ص 482.

بحماية فنية فهنا يتحقق عنصر العلم، أي علم الجاني بأنه غير مرخص له بالدخول وبإقدامه على اختراق النظام بتتبع الخطوات الفنية يتحقق عنصر الإرادة.

2- الركن المعنوي لجريمة الاعتداء العمدي على معطيات النظام:

يتحقق الاعتداء العمدي على معطيات النظام سواء على تلك التي توجد بداخله أو المعطيات الموجودة خارج النظام، والاعتداء العمدي عليها هو جريمة يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة، ويتطلب القصد الجنائي في هذا الفرض أن يتوقع الجاني حين يأتي فعله النتيجة الإجرامية التي سوف تترتب على الفعل، ويمثل توقع النتيجة الأساس النفسي الذي تقوم عليه إرادته، والنتيجة التي يجب أن يتوقعها الجاني هي تلك التي يحددها القانون وفي النطاق الذي يرسمه لها، فلا يشترط أن يتجه التوقع إلى عناصر أو حدود أو آثار لا يدخلها المشرع في فكرة النتيجة ولو كان من شأنها أن تعطيها مزيدا من التحديد، وهي في هذا المقام الدخول غير المصرح به إلى النظام لذا لا يلزم أن يتجه التوقع إلى الآثار غير المباشرة التي لا يدخلها القانون في تحديد النتيجة[1]، وأغلب لتشريعات تتفق في أن صور الاعتداء العمدي على المعطيات داخل النظام تتلخص في فعل الإدخال أو المحو أو التعديل، فمتى تم الدخول أو البقاء دون إذن في النظام وترتب عليه إدخال أو محو أو تعديل يتحقق عنصر العلم والإرادة معا،أما المعطيات الموجودة خارج النظام فقد سبق وأشرنا إلى أن نص المادة 394 مكرر 2 من قانون العقوبات الجزائري قد جاء مطلقا أي يشمل حتى المعطيات الموجودة خارج النظام فهي جزء من النظام متى كانت تؤدي دورا فيه، حيث يلاحظ أن استخدام تلك المعطيات كوسيلة لارتكاب جرائم تمس بالأنظمة المعلوماتية وفق الحالات التي حددها المشرع من تصميم أو بحث أو تجميع أو توفير أو نشر أو إتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، أو حيازة أو إفساد أو نشر أو استعمالها لأي غرض معاقب عليه، فهذا الاستخدام يتطلب قصدا خاصا نص عليه المشرع وهو الغش أي نية الاستخدام بغرض الإساءة ويفترض لتوافر القصد الخاص ثبوت توافر القصد العام.

1- د/ محمد عبيد الكعبي، المرجع السابق، ص 384

المطلب الثاني

الحماية الجنائية للمعاملات الالكترونية وفقا للقواعد المقررة في جرائم الإتلاف

عند تحقيق المجرم المعلوماتي لغايته باختراق النظام المعلوماتي أو البقاء فيه دون إذن يدفعه ذلك البقاء في غالب الأحيان إلى الإطلاع على المعطيات أو البيانات الموجودة داخل النظام، ما قد يدفعه في النهاية لإتلاف تلك البيانات أو المكونات المعنوية لنظام المعالجة الآلية للمعطيات.

ذلك ما دفع ببعض التشريعات لاستحداث نصوص خاصة تمس هدا الفرض، مثل ما استحدثه كل من المشرع الفرنسي والجزائري من نصوص تتعلق بالإتلاف المعلوماتي.

للإحاطة بجريمة الإتلاف في نطاق المعاملات الالكترونية نتطرق في هذا المطلب إلى:

الفرع الأول: محل جريمة الإتلاف في نطاق المعاملات الالكترونية

الفرع الثاني: أركان جريمة الإتلاف في نطاق المعاملات الالكترونية.

الفرع الأول:محل جريمة الإتلاف في نطاق المعاملات الالكترونية

محل جريمة الإتلاف وفق القواعد العامة هو الأموال الثابتة والمنقولة، وقد تعددت النصوص في سن التشريعات التي تحكم وتجرم الإتلاف كل على حسب القيمة المادية أوالمعنوية للشيء محل الإتلاف، والأهم في ذلك أن يكون الشيء محل الإتلاف أو التخريب هو ملك للغير حتى يدخل الفعل في دائرة التجريم، ولذلك سنتناول في هذا الفرع قسمين يتعلق الأول بالأموال الثابتة والمنقولة في نطاق المعاملات الالكترونية، أما الثاني فيتناول ملكية الغير للمال محل الإتلاف في نطاق المعاملات الالكترونية.

1/ الأموال الثابتة والمنقولة في المعاملات الالكترونية:

يقصد بالأموال الثابتة والمنقولة في نطاق المعاملات الالكترونية كل من الكيان المادي والمعنوي للمال المعلوماتي.

أ- الكيان المادي:

يقصد بالكيان المادي للمال المعلوماتي المكونات المادية للنظام كجهاز الإدخال والإخراج وشاشات العرض ووحدات التشغيل التي يتم بها معالجة المعلومات والأسطوانات والأقراص المغنطة، والاعتداء على هذه المكونات لا يثير أي إشكال ذلك لخضوعها لنصوص التجريم الكلاسيكية، في حين ذهب البعض إلى المساواة بين إتلاف البرنامج كعنصر معنوي من العناصر المعنوية للنظام المعلوماتي وبين الإتلاف الحاصل للإطار المسجل عليه البرنامج، وفي هذا خلط بين البرنامج المعلوماتي الذي هو عبارة عن مجموعة متوافقة من المعلومات المعالجة آليا وبين الإطار المادي الذي يحتوي البرنامج كالشريط المغنط[1].

ومن ثم فإن القول أن أفعال الإتلاف الواقعة على الإطار المادي الخام الذي يسجل عليه البرنامج أو المعطيات هي نفسها أفعال الإتلاف الواقعة على البرنامج المعلوماتي أو المعلومات المسجلة إلكترونيا على شريط أو أسطوانة هو أمر مخالف للواقع، ذلك أن فعل الإتلاف قد وقع على المكونات المعنوية للنظام المعلوماتي ومن الصعب دخول أو إدخال هذه العناصر تحت طائفة المكونات المادية للنظام المعلوماتي، ذلك لأنه في هذه الحالة يستهدف أساسا البرنامج ذاته أو معلومات ذاتها لا الشريط أو الأسطوانة فما قيمة الأسطوانة أو الشريط بجانب ما يحمله كل منهما من معلومات قد تكون على قدر كبير من الأهمية[2].

ب- الكيان المعنوي:

يقصد بالكيان المعنوي المكونات المنطقية للنظام المعلوماتي فهي تشمل البرامج المختلفة التي من خلالها تتم المعالجة الآلية للمعطيات.

وقد ظهر خلاف فقهي في الدول التي لم تستحدث نصوصا لمعالجة الإتلاف المعلوماتي حيث ذهب اتجاه إلى القول بصلاحية تطبيق نصوص التجريم الكلاسيكية المتعلقة بالإتلاف على

1- د/عمر أبوالفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا(دراسة مقارنة)، دار النهضة العربية، القاهرة 2010، ص 963.
2- د/عمر أبوالفتوح عبد العظيم الحمامي، ص 963.

المكونات المعنوية للنظام المعلوماتي، في حين ذهب اتجاه آخر إلى القول بعدم صلاحية تطبيقها على المال المعلوماتي.

في حين حسمت بعض التشريعات الموقف باستحداث نصوص خاصة، فقد وضع المشرع الفرنسي حدا للخلاف الفقهي الذي ثار في هذا الشأن، فعالج في المادة 03/323 من قانون العقوبات[1]، الاعتداءات الماسة بنظام المعالجة الآلية للمعطيات والواقعة على البيانات والمعلومات، وسار المشرع الجزائري في نفس السياق وذلك في نص المادة 394 مكرر من قانون العقوبات حيث عاقب على الدخول أو البقاء بطريق الغش في كل أو جزء من المنظومة المعلوماتية، وضاعف العقوبة إذا ترتب عن الدخول أو البقاء غير المشروع تخريب نظام اشتغال المنظومة.

ونص المشرع الكندي في المادة 387 من قانون العقوبات المعدل بالقانون رقم 218 لسنة 1985 والتي تعالج الإتلاف المعنوي "يعد مرتكبا لجريمة كل من قام عمدا بـــ:

1/ إتلاف أو تعديل البيانات.
2/ تجريد البيانات من معناها وجعلها غير صالحة.
3/ أعاق أو عطل الاستخدام المشروع للبيانات.
4/ أعاق أو عطل شخص في ممارسة حقه المشروع في استخدام البيانات".

وقد ذهبت المحكمة العليا "Ontario" الكندية سنة 1984 إلى إدانة متهم لقيامه بتعديل برامج النظام المعلوماتي على نحو أضر بأداء وظيفتها بشكل طبيعي، وجاء في حيثيات حكمها: "إذا كان تعديل أو إتلاف البيانات المعنوية لا يشكل في ذاته جريمة اعتداء، إلا أن إعاقتها عن أداء وظيفتها الطبيعية يعد جريمة"[2].

كما أن المشرع الإنجليزي أيضا عاقب على إتلاف المكونات المعنوية للنظام المعلوماتي وذلك في نص المادة الثالثة من قانون إساءة استخدام الكمبيوتر الصادر سنة 1990 ،حيث عاقبت المادة على نتيجة الدخول إلى النظام إذا تمثلت في تعديل محتوى النظام أو إتلاف عمله أو إعاقة

1 -Art 323/03 « le fait d'entraver ou de Fausser le fonctionnement d'un système de traitement automatisé de donnés est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende », code pénale français.

2- د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 978.

الدخول لأي برنامج أو بيانات في النظام المعلوماتي أو إتلاف عمل أو صحة أي برنامج أو بيانات.[1]

2/ ملكية الغير للمال محل الإتلاف في نطاق المعاملات الإلكترونية:

يجب أن يكون المال محل الإتلاف ملك للغير وهو شرط لوقوع جريمة الإتلاف، فمالك الشيء له الحرية التامة في التصرف في ملكه حتى ولو قام بإتلافه فلا عقاب على ما فعله إلا في بعض الحالات التي حددها المشرع كإتلاف الأوراق النقدية مثلا، فبالرغم من أنها ملك لصاحبها إلى أن إتلافها يلحق ضررا بالاقتصاد الوطني.

وللمالك أن يتلف ملكه ولو فعل ذلك إضرارا بالغير ممن له على المال حق عيني كحق امتياز أو رهن تأمينا لدين، ولكن يشترط أن تكون ملكية الشيء خالصة لمتلفه فإذا كان يملكه بالاشتراك مع الغير يعد متلفا لأن ضرر الإتلاف لا يعود عليه وحده وإنما يعود على غيره أيضا[2].

أما في نطاق المعاملات الالكترونية فنكون بصدد جريمة الإتلاف إذا كان الفاعل ليس المالك الحقيقي للنظام المعلوماتي، فقد يكون مسيرا للنظام فقط أو مخترق له، وفي حال وقع الإتلاف المعلوماتي من طرف صاحب النظام أو البرنامج ذاته فلا تتحقق جريمة الإتلاف هنا.

فملك الغير شرط من شروط جريمة الإتلاف في الجرائم العادية هو نفسه في الجرائم المعلوماتية، فمتى تحقق الإتلاف من غير المالك الأصلي للنظام المعلوماتي اكتملت بذلك جريمة الإتلاف في نطاق المعاملات الالكترونية.

إذن فمحل جريمة الإتلاف في نطاق المعاملات الالكترونية هو كل من المكونات المادية والمتمثلة في الأجهزة كشاشات العرض وأجهزة الإدخال و الإخراج والقرص الصلب... إضافة إلى المكونات المعنوية والمتمثلة في البرامج والبيانات والتي تحقق المعالجة الآلية للمعطيات شرط أن تكون ملكا للغير.

1- Smith and Hogan ,op,cit,p719

2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 979.

الفرع الثاني:أركان جريمة الإتلاف في نطاق المعاملات الالكترونية

قد تقع جريمة الإتلاف عن طريق شبكة الانترنيت وذلك بالاعتداء على الوظائف الطبيعية للحاسب الآلي أو عن طريق التعدي على البرامج والبيانات المخزنة والمتبادلة عن طريق شبكة الانترنيت أو التلاعب بالبيانات وإتلاف المعلومات المخزنة بالحواسيب ومحوها أو تعديلها أو تغيير نتائجها أو التشويش على النظام المعلوماتي وإعاقة سير عمل النظام.

وبالتالي يكون الإتلاف العمدي للبرامج والبيانات بمحوها كلية أو تدميرها إلكترونيا أو تشويشها على نحو فيه إتلاف بما يجعلها غير صالحة للاستعمال[1].

و باعتبار الجريمة من الجرائم العمدية سنتطرق في هذا الفرع لكل من الركن المادي والذي يمكن أن تتم فيه الجريمة على الكيانات المادية للنظام المعلوماتي أو المنطقية، ثم نتطرق للركن المعنوي لها.

أولا: الركن المادي لجريمة الإتلاف في نطاق المعاملات الالكترونية

فعل الإتلاف في نطاق المعاملات الالكترونية يمكن أن يمتد إلى المكونات المادية للنظام المعلوماتي أو المكونات المعنوية، وفي كلتا الحالتين يتمثل الركن المادي في تخريب الأموال بجعلها غير صالحة للاستخدام والاستعمال ولا يشترط القانون أن يكون الإتلاف تاما بل تقوم الجريمة ولو كان جزئيا، ويشترط القانون في حالة الإتلاف الجزئي أن يكون فعل الإتلاف من شأنه جعل المال غير صالح للاستعمال، أو تعطيله بأي طريقة[2]، وحتى لو لم يترتب على فعل الإتلاف تأثير على مادة الشيء أو لا تزال بعد الفعل مثلما كانت عليه قبله متكاملة الحجم والوزن متماسكة الجزئيات ولكن قيمتها زادت أو نقصت فإن هذا الفعل يتعين اعتباره إتلافا أو تعييبا وذلك لأن محل الحماية الحقيقة في جريمة الإتلاف هو قيمة الشيء فإذا كان فعل الإتلاف قد افقد الشيء قيمته أو انقص منها فقد وقع الاعتداء المجرم والمعاقب عليه بمقتضى القانون[3].

1- د/ محمد عبيد الكعبي، المرجع السابق، ص 495.
2- د/ محمد عبيد الكعبي، ص 496
3- د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 985.

1- إتلاف المكونات المادية للنظام المعلوماتي:

تعاقب كل التشريعات على إتلاف المكونات المادية للنظام المعلوماتي كإتلاف أجهزة الحاسب الآلي ككل أو لجزء منها فقط،وهذه المكونات تدخل في نطاق المنظومة المعلوماتية التي أسبغ لها المشرع الجزائري حماية جزائية في نص المادة 394 والمشرع الفرنسي في نص المادة 323 من قانون العقوبات.

وحتى لو لم يتم استحداث تلك النصوص فهي تدخل ضمن الأشياء التي تحميها النصوص التقليدية، فالمكونات المادية للنظام المعلوماتي لا تثير أي إشكال قانوني حال إتلافها، وقد تتعد أشكال وصور الاعتداء المادي على النظام المعلوماتي ومن بين بعض الأمثلة على ذلك ما قامت به مجموعة من المجرمين تطلق على نفسها منظمة تدمير الحاسبات أو نظم المعلومات، حيث كبدت هذه الجماعة الشركات الفرنسية التي تقوم بصناعة معدات وأجهزة الأنظمة المعلوماتية خسائر مادية كبيرة بلغت عشرات الملايين من الفرنكات الفرنسية نتيجة أفعال التعدي والإتلاف[1].

فمصادر الاعتداء على المعدات المعلوماتية المادية وإتلافها عديدة ومتنوعة وكذلك بواعث هذا الاعتداء حيث تختلف من شخص لآخر، فمن جهة قد تكون مصادر هذا الاعتداء هي الطبيعة حال الفيضانات والزلازل وقد يكون الإنسان ذاته، كما تتعدد بواعث الإتلاف وتتنوع كعدم رضاء المستخدمين عن أصحاب أعمالهم مثلما حدث في النرويج حيث أتلفت حاسبات آلية لشركة عقب فصل عشرين مستخدما كانوا يعملون بها[2].

2- إتلاف المكونات المعنوية للنظام المعلوماتي: المقصود بإتلاف المكونات المعنوية للنظام المعلوماتي(l'altération) [3] هو محو أو تعديل بالإضافة أو النقصان للمكونات الداخلية للنظام المعلوماتي كالبرامج والبيانات، بحيث يكون هذا الإتلاف معيبا لكل أو لجزء من النظام المعلوماتي.

1-Rose (ph), la criminalité informatique , Pars PUF,2eme édition 1995, p62.

2- د/ محمد عبيد الكعبي،المرجع السابق، ص 504.

3- يستخدم الفقه الفرنسي مصطلح Altération للإشارة للإتلاف المعنوي الذي يتمثل في العناصر المعنوية أو المنطقية للنظام المعلوماتي ومصطلح Dégradation للتعبير عن الاختلاف المادي الذي يلحق بالمعدات المادية للنظم المعلوماتية: راجع في ذلك، عمر أبو عبد الفتوح عبد العظيم الحمامي، المرجع السابق، ص963

وقد حدد المشرع الجزائري صور الإتلاف المعلوماتي فقد تكون إما بالإدخال أو الحذف أو التعديل، والتي قد ينجر عن أحدها تخريب المنظومة المعلوماتية ككل.

وإتلاف المكونات المعنوية للنظام المعلوماتي يتخذ صورتين:

الصورة الأولى: إتلاف المعلومات المنسوخة على الدعامات والشرائط المغنطة

قد يقع الاعتداء بالإتلاف على المعلومات والبرامج المنسوخة على دعامات مادية كالأسطوانات أو الشرائط الممغنطة، بأي طريقة من طرق الإتلاف الأمر الذي يخرجها من نطاق الصلاحية للاستعمال[1]

وفي هذا الفرض يثور الإشكال حول مدى دخول البرامج المنسوخة على دعامات مادية في دائرة الحماية الجنائية التي أقرتها بعض التشريعات للنظام المعلوماتي؟

بالرجوع لنص المادة 394 مكرر قانون العقوبات الجزائري و المادة 323 قانون العقوبات الفرنسي نجد أن هذه المواد أقرت حماية جنائية واضحة لكل المكونات المعنوية أو المنطقية للنظام المعلوماتي، وبالرجوع أيضا لتعريف نظام المعالجة الآلية للمعطيات حيث قلنا بأنه مجموعة مركبة من وحدة أو عدة وحدات للمعالجة والتي تساهم في الحصول على نتيجة محددة وهي معالجة البيانات فإنه يمكن القول في هذا الصدد بأن إتلاف الدعامة المادية التي تحتوي على برنامج أو بيانات يدخل في نطاق التجريم، متى كانت تلك البرامج أو البيانات جزء من المنظومة المعلوماتية ويتحقق لنا هذا الفرض في بعض الحالات التي يكون فيها برنامج خارجي هو مفتاح المنظومة المعلوماتية، أي يحتوي على رموز خاصة بسير المنظومة ومن ثم فإنه لا يمكن إغفال هذا الجزء من الحماية الجنائية المقررة للمكونات المعنوية للنظام المعلوماتي، أضف إلى ذلك أن الاعتداء على تلك الأسطوانات الغرض منه في أغلب الأحيان هو المعلومات الموجودة داخلها و ليس الأسطوانة في شكلها الخارجي، حيث أن القول بغير ذلك يجعلنا نساوي بين القيمة المادية للدعامة وقيمتها المعنوية أي المعلومات التي تحتويها.

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 988.

الصورة الثانية: إتلاف المعلومات الموجودة داخل النظام المعلوماتي

السمة الغالبة في إتلاف العناصر المعنوية للنظام المعلومات أن يتم الإتلاف ومحله المعلومات الموجودة بداخل النظام، وهذا النمط من الإجرام يستلزم في مرتكبيه صفات خاصة مثل الذكاء والتآلف الشديد مع الأنظمة المعلوماتية، فهذه الصورة هي التي تميز الإتلاف التقليدي الذي يميل في غالبه إلى العنف والتحطيم والتكسير... عن الإتلاف الحاصل للمكونات المعنوية الذي لا ينشأ باستخدام العنف التقليدي ولكن عن طريق ما يسمى بتقنيات التدمير الناعمة[1].

فالغرض من الاعتداء على معطيات النظام هو المعلومات الموجودة بداخله وذلك ما عاقب عليه المشرع الجزائري في المادة 394 مكرر1 من ق.ع التي تنص على أن: "يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"

يعالج النص المعطيات الموجودة داخل النظام المعلوماتي، فمتى تم الاعتداء عليها سواء بالإدخال أو التعديل أو الحذف نكون بصدد جريمة الإتلاف المعلوماتي والتي حدد لها المشرع العقوبات السالفة الذكر.

و نص المشرع الجزائري في المادة 394 مكرر على أن الجاني عند قيامه بفعل الدخول أو البقاء غير المشروع و يقوم بالحذف أو التغيير في معطيات المنظومة وينجر على هذه الأفعال السابقة تخريب نظام اشتغال المنظومة تسلط عليه عقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج.

كما عالجت الاتفاقية الدولية للإجرام المعلوماتي هذا الفرض في المادة 4 و جرمت فعل الدخول عمدا ودون وجه حق إلى النظام و إلحاق أي أضرار أو محو أو تعطيل أو إتلاف أو طمس لبيانات الحاسب"[2].

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 989.

2- Art4: « atteinte à l'intégralité des données chaque parie adopte les meures législatives et autres qui se révèlent nécessaires pour ériger en information pénale, conformément à sont droit interne le fait,

فالهدف من نص الاتفاقية هو ضمان حماية البيانات والبرامج المعلوماتية من الإتلاف.

وتجدر الإشارة إلى أن هناك العديد من القضايا التي تم معالجتها في هذا الفرض مثل ما ذهبت إليه محكمة النقض الفرنسية في حكم لها سنة عام 1996 حيث ذهبت إلى أن إدخال البرامج الخبيثة إلى نظام الحاسب الآلي هو سلوك معاقب عليه طبقا للفقرة الثانية من المادة 01/323 والتي تنص: "وإذا نجم عن هذا الدخول محو أو تعديل في المعطيات المخزنة في هذا النظام أو إتلاف تشغيل هذا النظام تكون العقوبة الحبس لمدة ثلاث سنوات وغرامة مقدارها 45000 يورو".

كما ذهبت نفس المحكمة أيضا في حكم لها صادر عام 1999 إلى أن إدخال بيانات والتي يترتب عليها إتلاف لأي من المكونات المنطقية لنظام الحاسب الآلي هو سلوك معاقب عليه ولو كان للجاني حق الدخول إلى هذا النظام[1].

ما يلاحظ على حكم محكمة النقض الفرنسية أنها لم تشترط الدخول غير المشروع للقول بوجود جريمة الإتلاف، فمتى كانت النتيجة إتلاف البيانات بالصورة التي حددها القانون تحققت الجريمة، فالدخول غير المشروع يحقق لنا القصد الجنائي بعنصريه العلم والإرادة كما سبق التفصيل في ذلك وبتوفر القصد الجنائي لا يستطيع الجاني الفرار من العقوبة بحجة أن الإتلاف كان عن غير قصد، كما هو الحال بالنسبة للعامل المخول له الدخول إلى النظام حيث يستطيع هذا الأخير حال قيامه بإتلاف البيانات القول بان الإتلاف كان عن غير قصد أو أثناء تأديته لمهامه العادية ولقاضي الموضوع السلطة التقديرية في ذلك.

وجريمة الإتلاف من شأنها أن تجعل الفعل المجرم داخلا في نطاق جريمة الإتلاف ونطاق جريمة أخرى لذا يجب على سلطة التحقيق ومن بعدها المحكمة التي تنظر الموضوع التأكد من صحة الوصف القانوني على الواقعة وذلك بأن تنزلها منزلها الصحيح وفقا للوقائع والقانون.

=intentionnel et sont droit, d'endommager d'effacer, de détériorer, d'altérer ou de supprimer des données informatique » www.eastlaws.blogspot.com le : 16/09/2010 à : 20h30mn

1- د/ محمد عبيد الكعبي، المرجع السابق، ص 506.

ومن التطبيقات القضائية على ذلك حالة تكييف فعل على أنه نصب معلوماتي عندما قام محاسب بمحو بيانات ومعلومات معالجة آليا تخص إحدى الشركات وذلك بعد مرور 6 شهور من بداية العمل، وهذا يعني أن أفعال المحو التي وقعت على البيانات الموجودة بالبرنامج المحاسبي قد كيفت جنائيا على أنها جريمة نصب معلوماتي بالرغم من أن المحو من وسائل الإتلاف، و قد يكيف التزوير بتغيير أو تعديل بيانات إلكترونية على أنه إختلاس مثل التزوير الحاصل في الطلبات التي تصدر عن طريق الشركات في طلب البضائع، فالتكييف القانوني يجب أن يتم وفق الغاية التي هدف إليها المجرم المعلوماتي[1].

أما عن الأساليب والوسائل الفنية المستخدمة في إتلاف المعلومات والبرامج الموجودة داخل النظام المعلوماتي فهي كثيرة ومتنوعة نذكر أهمها:

1/ التلاعب في المدخلات:

وذلك بإدخال بيانات محرفة في نظام معلومات الحاسب أو تغيير مسار البيانات الصحيحة المدخلة أو الجمع بين الأمرين معا وهذه الأمور يسهل القيام بها في أولى مراحل تشغيل النظام المعلوماتي وذلك في مرحلة إدخال البيانات لمعالجتها، حيث تجهز البيانات وتحول إلى لغة مقروءة من قبل الآلة المستخدمة في المعالجة ويكون سهلا تغذية الحاسب ببيانات مغلوطة أو زائفة أو منع إدخال بيانات أووثائق معينة[2]، وأكثر من نصف الجرائم المعلوماتية تقع باستخدام هذه الطريقة.

2/ التلاعب في البرامج: يتحقق التلاعب في البرامج بإصابة أحد أجزاء المكونات الصلبة للجهاز ما ينتج عنه حذف الملفات وذلك بحذف جميع المعطيات الموجودة داخل القرص الصلب أو مسح الملفات التنفيذية سواء المثبتة داخل نظام التشغيل أو الموجودة داخل الحاسب[3]

ومن أخطر تلك البرامج تلك التي تتيح إدخال أوامر إلى الحاسب لتحقيق أغراضه الإجرامية كبرنامج حصان طروادة أو القنابل المنطقية أو برامج الدودة أو الفيروسات.

1- د/ محمد عبيد الكعبي، المرجع السابق، ص 514.
2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 116
3- محمد خليفة، المرجع السابق، ص52.

أ- برنامج حصان طروادة:

سميت هذه البرامج هكذا كنية بالأسطورة القديمة عندما اختفى الجنود داخل الحصان الخشبي ليدخلوا مدينة طروادة ويهزموا جيشها، هكذا فإن أحصنة طروادة هي برامج خبيثة تختفي بداخل برامج مفيدة وغرضها الأساسي هو جمع المعلومات مثل الاسم وكلمة السر ثم يبعث بهذه المعلومات لصاحبه أثناء اتصال الجهاز بالشبكة، والأسوأ من ذلك أنه يسمح للهاكر بتصفح الجهاز والتحكم في الملفات تحكما كاملا[1]، وانتشر هذا النوع من البرامج في العصور الوسطى خاصة في أربع دول أروبية وهي إنجلترا والنرويج والسويد والدا نمارك[2]

ب- برنامج الدودة:

هي عبارة عن برامج تستغل أية فجوة في نظم التشغيل كي تنتقل من حاسب إلى آخر ومن شبكة إلى أخرى عبر الوصلات التي تربط بينهما و تتكاثر أثناء عملية إنتقالها كالبكتيريا بإنتاج نسخ منها[3]

ج- القنابل المنطقية أو الموقوتة:

هي برامج محمية بحيث تبقى ساكنة وغير فعالة وغير مكتشفة لمدة قد تصل إلى أشهر أو أعوام، ويحتوي هذا البرنامج على تاريخ معين بحيث ينشط هذا البرنامج عند حلول تاريخه ويؤدي مهامه الهدامة، وقد لا يرتبط مؤشر التفجير بالزمن وإنما بشروط منطقية معينة تكون داخل برنامج أو ملف أو النظام وذلك حسب ما يحدده برنامج القنبلة[4].

1- د/ محمد عبيد الكعبي، المرجع السابق، ص527.

2- ومن نماذج فيروسات حصان طروادة التي تم اكتشافها فيروس أطلق عليه اسم فيروس الإيدز والذي ظهر خلال النصف الأول من عام 1990 وتعرض له الآلاف من المستخدمين في شتى أنحاء العالم وبدأ بإرسال أسطوانة ممغنطة Magnetie disk تحمل عنوان Aids information عن طريق البريد إلى العديد من مستخدمي الحاسبات بهذه القارات مع التنويه بأنها تحوي برنامجا يتعلق بعرض الإيدز واحتمالات تعرض الشخص للإصابة به وكان فيروس حصان طروادة يختفي وراء هذا البرنامج فبمجرد تحميله يظهر للمستخدم رسالة تخطر المستخدم بأن بياناته سيتم محوها إذا لم يرسل على عنوان شركة معينة في بنما 179 دولار لتزويده ببرنامج يتيح له استخدام الجهاز لمدة سنة بدون محو ما بداخله من بيانات وفعلا بدأت البيانات والبرامج تتعرض لمحو مع ظهور تهديد آخر بإرسال المبلغ وإلا تعرضت كل البيانات للمحو وقد أسفرت التحقيقات الأولية لجهاز (FBI) أن المسؤول عن هذا الفيروس هو الدكتور Joseph.lowispopp البالغ من العمر 39 سنة والحاصل على الدكتوراه في علم Anthropology راجع في ذلك : محمد علي العريان ، المرجع السابق، ص90 .

3- محمود أحمد عبابنة، المرجع السابق، ص103

4 - آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 117.

د- الفيروس المعلوماتي: هو برنامج مكتوب بإحدى لغات البرمجة بطريقة خاصة و يستطيع أن يخلق نسخ تنفيذية من نفسه في برامج أخرى تصبح بدورها قادرة على إلحاق نسخ من الفيروس في أجزاء محددة في برامج أخرى[1]، ومن أهم خصائصه:

-القدرة على التخفي

-القدرة على العدوى

-الاختراق والتدمير

ثانيا: الركن المعنوي لجريمة الإتلاف في نطاق المعاملات الالكترونية

الإتلاف من الجرائم العمدية ويتحقق متى تعمد الجاني ارتكاب الفعل المنهي عنه بالصورة التي حددها القانون واتجاه إرادته إلى إحداث ذلك الفعل بأي صورة من الصور التي أوردها قانون مكافحة الجرائم المعلوماتية [2]، أي أن يكون الجاني عالما وقت اقترافه لفعل الإتلاف بأنه يتلف عناصر معنوية أو مادية للأنظمة الآلية لمعالجة المعلومات [3].

وهي في قانون العقوبات الجزائري إما إدخال معلومات لم تكن موجودة في نظام المعالجة الآلية للمعطيات أو تعديل المعلومات الموجودة داخل النظام أو حذفها أو إفساد النظام ككل ومتى تحقق أحد هذه الصور مع علم الجاني بأنه يقوم بالاعتداء على مال معنوي أو مادي يتعلق بالأنظمة الآلية لمعالجة البيانات وأن تكون إرادته متجهة لهذا الإتلاف مع علمه بملكية الغير لتلك الأشياء فباكتمال هذه العناصر نكون بصدد الركن المعنوي لجريمة الإتلاف في نطاق المعاملات الالكترونية فإذا نقص عنصر العلم أو الإرادة لا تتحقق الجريمة.

1- آمال قارة، المرجع السابق، ص 117.
2- د/ محمد عبيد الكعبي، المرجع السابق، ص 514.
3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 999.

المطلب الثالث

الحماية الجنائية للمعاملات الالكترونية وفقا للقواعد المقررة في جرائم التزوير

احتلت اليوم الدعامات المادية للحاسب الآلي مكانة لمحررات والصكوك ونظرا لأهمية وخطورة ما تحتويه من بيانات فقد تكون محلا للاعتداء بتغيير حقيقتها بقصد الغش في مضمونها والذي من شأنه إحداث أضرار مادية أو معنوية[1]، فقد أصبح التزوير في مجال نظم المعلومات بوصفه أحد أنماط الغش المعلوماتي يشهد تزايدا سريعا في الآونة الأخيرة كتزوير المستخرجات الإلكترونية وإفشاء أسرارها وتزوير المعلومات المخزنة بداخل الأنظمة المعلوماتية، والضمانة الأبرز لحماية هذه المعلومات هي التشريعات، لكن ما يلاحظ على التشريعات العربية أنه بالرغم من بسطها للحماية على المحررات التقليدية إلا أنها أغفلت فرض الحماية على المعلومات الإلكترونية، وهنا يأتي دور الفقه في البحث عن مدى كفاية نصوص التزوير التقليدية في معالجة حالات التزوير المعلوماتي.

و لمعالجة ذلك سنتطرق في هذا المطلب لفرعين نتناول في الأول محل جريمة التزوير في نطاق المعاملات الالكترونية، أما الثاني فنفرده لأركان هذه الجريمة وذلك على الشكل التالي :

الفرع الأول: محل جريمة التزوير في نطاق المعاملات الالكترونية

الفرع الثاني: أركان جريمة التزوير في نطاق المعاملات الالكترونية

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 133.

الفرع الأول:محل جريمة التزوير في نطاق المعاملات الالكترونية

محل جريمة التزوير في ضوء القواعد العامة هو المحرر وذلك ما نصت عليه العديد من التشريعات وحصرته في ذلك السياق كالمشرع المصري، الجزائري .. ويعتبر التشريع الجزائري من التشريعات التقليدية التي تشترط المحرر لتطبيق جريمة التزوير، وذلك ما تناوله كل من القسم الثالث والرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات وذلك في المواد من 214 إلى 229.

وما يؤخذ على المشرع الجزائري وبعض التشريعات العربية كالمشرع المصري أيضا أنها لم تعط تعريفا للتزوير وإنما يستخلص ذلك من نصوص تلك التشريعات، إلا أن المشرع الأردني أعطى تعريفا له في نص المادة 260 قانون العقوبات، حيث نص على أنه "تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي"، وقد طابق القانون اللبناني في مادته 453 نص المادة السابقة والمشرع السوري في نص المادة 440[1].

كما عرفه الفقيه Garcon بأنه "تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه إحداث ضرر ومقترن بنية استخدام المحرر المزور فيما أعد له"[2].

والملاحظ في جميع التشريعات سواء التي أوردت تعريفا للتزوير أو التي يستخلص من نصوص تشريعاتها أنها تتفق في أن محل التزوير في ضوء القواعد العامة هو المحرر.

والمحرر في مفهوم جريمة التزوير هوعبارة عن كتابة منسوب صدورها إلى شخص أو جهة معينة من شأنها أن تولد مركز قانوني معين أو ترتب نتائج معينة، وإذا كان المحرر في شكله التقليدي يتم تحريره على ورق إلا أنه ليس في القانون ما يستلزم هذا الشرط [3].

1- محمد أحمد عابنة، المرجع السابق، ص 107.
2- محمد أحمد عابنة، ص 107.
3 - د/ محمد حسام محمود لطفي ، الإطار القانوني للمعاملات الإلكترونية ، دار النهضة العربية 2002 ، ص40

وللمحرر التقليدي العديد من الخصائص أهمها:

1- أن يتخذ المحرر شكلا كتابيا ويجب إدراك مضمون المحرر بالنظر إليه أو لمسه وإذا استحالت قراءته فلا يصلح وسيلة للإثبات ولا عقاب على ما احتواه من تعبير.

2- أن تكون الكتابة منسوبة لشخص معين

3- أن يحدث المحرر آثارا قانونية[1].

من هذه الخصائص التي يتسم بها المحرر نتساءل: هل يمكن القول بتطابق هذا الوصف على المستندات المعالجة آليا؟ وبصيغة أخرى ما مدى اعتبار المحرر المعلوماتي من قبيل المحررات التقليدية؟ وذلك ما سنتناوله من خلال التطرق للجدل الذي دار حول مدى اعتبار المحرر المعلوماتي من قبيل المحررات التقليدية، ثم نتناول محل التزوير في نطاق المعاملات الالكترونية وفقا لما يلي:

أولا: ما مدى اعتبار المحرر المعلوماتي من قبل المحررات التقليدية

ذهب جانب من الفقه الفرنسي إلى القول بعدم إمكانية اعتبار المحرر المعلوماتي من قبيل المحررات التقليدية، لأن جريمة التزوير تستلزم الكتابة وذلك ما لا يتحقق في الأشرطة الممغنطة[2].

أضف إلى ذلك أن جريمة التزوير تفترض على وجه العموم إمكانية استخدام الوثيقة المزورة كوسيلة إثبات، وذلك ما لا يتحقق في الوثائق المعلوماتية.

و ذهب جانب آخر إلى القول بعكس ذلك مستندا على تفسير القضاء للمحررات الخاصة تفسيرا واسعا فصار يندرج تحتها الدفاتر التجارية وكافة المحررات المتعلقة بالتجارة، وطبقا لمبدأ الإثبات الحرفي مجال المعاملات التجارية والذي يسري على الفواتير وبطاقات العمال وغالبية الوثائق المحاسبية فإن هذه الأخيرة تشهد الآن عمليات المعالجة المحاسبية والتي تتم معالجتها إلكترونيا طالما أن لها قيمة تصلح في الإثبات، وأصبح القضاء يعاقب على أي تزوير في محرر له قيمة تصلح

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 136.
2- محمود أحمد عبابنة، المرجع السابق، ص 109.

في الإثبات[1]، كما ذهب هذا الاتجاه للقول بإمكانية تغليب روح النصوص واعتبار ما يظهر على شاشة الحاسب شكلا مستحدثا للمحرر[2]

بينما يرى جانب آخر من الفقه البلجيكي ضرورة التمييز بين البيانات التي يمكن إدراكها بالبصر وتلك المخزنة في ذاكرة النظام المعلوماتي، ويترتب على ذلك سريان جريمة التزوير في المحررات على الأولى دون الثانية، أما الفقه الأمريكي فقد استقر على أن البيانات سواء أكانت مخزنة في ذاكرة النظام المعلوماتي أو متضمنة في برامجه أو في أشرطة الإدخال أو الإخراج الممغنطة لا يمكن اعتبارها محررا [3]

في حين ذهب جانب من الفقه السوري إلى القول بتطبيق نصوص التزوير وذلك عندما تكون البيانات قد سجلت على أسطوانة أو شريط ممغنط، بحيث يعتبر محررا وتغيير الحقيقة فيه يعد تزويرا وذلك بسبب انتقال المعلومات والمعطيات المخزنة إلى جسم مادي له سمات المحرر المكتوب، والذي يمكن قراءته بالعين وذلك باستخدام الحاسب للكشف عن محتواه من قبل الغير فالعبرة بالمادة التي دون عليها[4].

من وجهات النظر الفقهية هذه نرى أن الاتجاه المعارض لفكرة تطبيق نصوص قانون العقوبات على المحرر المعلوماتي هو الاتجاه الغالب والأقوى حججا، كما أن أغلب التشريعات حصرت صورة المحرر في ضرورة إدراك مضمونه بالنظر أو اللمس، وذلك ما لا يتوافر في المحرر المعلوماتي، أضف إلى ذلك أن العديد من التشريعات استحدثت نصوصا خاصة بالتزوير المعلوماتي وذلك ما يوجب على باقي التشريعات مسايرة ذلك.

أما على صعيد التشريعات فقد ذهبت بعضها كمصر (المادة 211) إيطاليا (المادة 485) بلجيكا (المادة 190) إلى اشتراط وجود المحرر بمفهومه التقليدي لتطبيق جريمة التزوير بأن يكون محتوى

1- د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 883.
2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 137.
3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 886.
4- أمال قارة، ص 137.

الوثيقة أو الوعاء قابلا للمشاهدة البصرية فلا يشمل بذلك البيانات المخزنة إلكترونيا[1]

وهو ما عمل به المشرع الجزائري، فبالرغم من استحداثه لنصوص تعاقب الاعتداء على نظام المعالجة الآلية للمعطيات والتي تضمنت بعض طرق التزوير كالتعديل والمحو والإدخال إلا أن المشرع اغفل التطرق للتزوير الحاصل في المجال المعلوماتي.

ولذلك نقترح إضافة نص إلى باب التزوير في المحررات، بحيث يتناول هذا النص تعريف موضوع جريمة التزوير وأساسها ألا وهو المحرر وذلك على الشكل التالي: "المحرر هو كل مركب يتكون من حروف أو علامات تدل على فكرة معينة بالنظر إليها مباشرة أو بالاستعانة بتقنية أخر"، وبذلك يشمل هذا النص المحررات التقليدية والمعلوماتية معا كالمستندات الموجودة على الأقراص والأشرطة، هذا فيما يتعلق بالتشريعات التي لم تستحدث نصوصا خاصة لمواجهة التزوير المعلوماتي.

وعلى الجانب الآخر ذهب المشرع في العديد من الدول إلى استحداث نصوص خاصة بالتزوير المعلوماتي ومن بين تلك التشريعات:

التشريع الفرنسي حيث نصت المادة 462-5 من قانون الغش المعلوماتي لسنة 1988 على: "كل من يقوم بتزوير مستندات معالجة آليا ..." فنص المشرع تناول المستندات المعالجة آليا أي تلك التي تم صياغتها في صورة إحدى لغات الحاسب وبذلك يكون المشرع قد حسم الجدل القائم في هذا الفرض وبصدور قانون العقوبات الفرنسي لسنة 1994 أورد المشرع نصا جديدا في المادة 441-1 التي عرفت التزوير بأنه: "كل تغيير للحقيقة في محرر أو أي وعاء آخر بأي طريقة"[2] وطبقا لهذا النص لم تعد طرق تغيير الحقيقة محددة على سبيل الحصر بل إن المشرع بهذا النص قد أطلق طرق تغيير الحقيقة بغير قيد[3].

1- أمال قارة،الحماية الجزائرية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 137.

2 -Art441-1 : « constitue un faux toute altération frauduleuse de la vérité, de nature a causer un préjudice et accomplie par quelque molène que ce soit dans un écrit au tout autre support d'expression de la pensée qui a pour objet au qui peut avoir pour effet d'établir la preuve. D'un droit au d'un fait ayant des conséquences juridiques » code pénale français.

3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 891.

ويعود السبب في قيام المشرع الفرنسي بإلغاء المادة 5/462 السابقة الذكر والمادة 6/462 والتي جرمت استعمال تلك المحررات، والسبب في ذلك حسب وجهة نظر بعض الفقه المصري هو اختلاف المصلحة التي يحميها القانون في هاتين المجموعتين من الجرائم، فالمصلحة التي يحميها المشرع من تجريم الاعتداء على نظام المعالجة الآلية للمعطيات هي هذا النظام ذاته، أو بمعنى أدق هي مصلحة صاحب الحق في هذا النظام أو مصلحة من له السيطرة عليه بينما المصلحة التي يحيها القانون بصدد جريمة التزوير هي الثقة العامة في المستندات ذات القيمة القانونية أيا كان شكلها[1].

كما أن المشرع الألماني استحدث نصا جديدا "269" من قانون العقوبات يجرم فيها التزوير الذي يقع على "البيانات ذات الأهمية القانونية"، فالمشرع الألماني لم يتطلب أن يكون المستند الذي يقع عليه التزوير قابلا للإدراك المرئي أي بالعين المجردة، حيث قرر عقوبة الحبس لمدة تزيد على خمس سنوات أو الغرامة على "كل من يقوم بقصد الخداع في تعامل قانوني بتخزين أو تغيير بيانات إذا ما استنسخت بهذا الشكل وأنتجت مستندا غير أصلي أو مزور وكذا كل من يستخدم هذه البيانات المخزنة أو المحرفة"[2].

أما في أستراليا فقد تم إضافة مادة جديدة تحت رقم 276 لسنة 1983 إلى قانون العقوبات و تنص الفقرة الأولى من هذه المادة على أنه: "يعاقب بالحبس كل من حرف أو زور أو محا أو أتلف بطريقة غير مشروعة وبأي قصد كان للغش أية مادة لمعالجة البيانات"، وبالتالي فقد أصبح مفهوم المحرر يتسع ليشمل ما يطلق عليه المحررات الإلكترونية [3]

ومن جهته تناول القانون العربي الاسترشادي التزوير المعلوماتي في نص المادة الرابعة حيث نصت على :

"كل من ارتكب تزويرا في احد المستندات المعالجة في نظام معلوماتي يعاقب بالحبس مدة لا تقل عن... ويعاقب بذات العقوبة كل من استعمل المستند المزور مع علمه بالتزوير"[4]

1- د/ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، الإسكندرية 1999، ص 153.
2- د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 893.
3- د/ شيماء عبد الغني محمد عطا الله، الحماية الجنائية لتعاملات الالكترونية، دار الجامعة الجديدة الإسكندرية2007، ص85
4- www.arabic.mjustice.dz le : 09/11/2010 11h00mn

فمجمل النصوص السابقة جاءت قاطعة وصريحة بما لا يدع مجالا للشك حول كيفية المعالجة القانونية للتزوير المعلوماتي.

وبعد التطرق للإشكالية السابقة حول مدى اعتبار المحرر المعلوماتي من قبيل المحررات التقليدية وموقف التشريعات المختلفة منها يسهل علينا التكلم الآن عن محل جريمة التزوير في نطاق المعلوماتية.

ثانيا:محل التزوير في نطاق المعاملات الالكترونية

كان محل التزوير مقتصرا على المحرر أو المكتوب الذي يتخذ شكل الكتابة، أي العبارات الخطية أو العلامات أو الرموز التي تصلح لسرد واقعة أو للتعبير عن إرادة، أي تلك التي تصلح لنقل المعنى من شخص لآخر وكان يستبعد استنادا لهذا التحديد الأسطوانات وأشرطة التسجيل وغيرها من الدعامات التي لا تتخذ شكل الكتابة، ولكن المشرع الفرنسي في تعديله الأخير لمحل التزويرفي المادة 01/441 ق.ع أصبح لا يقتصر على ما يصدق عليه وصف المكتوب فقط وإنما يمتد ليشمل أي دعامة أخرى تحتوي على الفكر، وتعبير دعامة أخرى تعبير مطلق من أي قيد ويدخل فيه بلا جدال كل الدعامات المستخدمة في مجال الحاسب الآلي والتي يسجل عليها أي تعبير عن الفكر يصلح لأن يرد عليه التزوير بأن يكون ليس مجرد سرد لوقائع أو بيانات تعبر عن إرادة وإنما يلزم فوق ذلك أن تكون تلك الوقائع أو البيانات مما يصلح للتمسك به أو للاحتجاج به، وهي لا تكون كذلك إلا إذا كانت تقرر حق سواء بإنشائه أو بتعديله أو بإلغائه أو تثبيته وهذا يصدق على المستندات المعالجة آليا وغير المعالجة[1].

والمستند في الإصلاح القانوني هو كل دعامة مادية تصلح لأن تدون عليها المعلومات أو الآراء أو هي الشيء المادي الذي يمكن أن يدون عليه شيء معنوي، ويقصد بالمستند في مجال المعلوماتية كل شيء مادي متميز قرص أو شريط ممغنط أو خلاف ذلك يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام المعالجة الآلية.

1- د/ علي عبد القادر القهوجي، المرجع السابق، ص 155.

والمستند المعالج آليا هو كل دعامة مادية مهيأة لاستقبال المعلومات والتي تسجل المعطيات عليها من خلال تطبيق إجراءات المعالجة الآلية المعلوماتية، وبعبارة أخرى يقصد بالمستند المعالج آليا الدعامة المادية التي تم تحويل المعطيات المسجلة عليها إلى لغة الآلة.

أما المستند غير المعالج آليا فهو مجموعة الأوراق المعدة لتسطير المعلومات عليها والأقراص الممغنطة التي لم يسجل عليها أي شيء بعد والملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة استخدام البرنامج وكذلك أيضا البطاقات البنكية التي لم تدخل الخدمة بعد وإن كان مسجلا عليها معلومات مكتوبة بخط اليد أو محظورة إلا أنه لم يتم معالجتها بعد [1].

ومن جانب آخر أقر القضاء المصري أنه لا يدخل في مدلول المحررات الآلات الحاسبة مثل عدادات المياه أو الكهرباء، حيث قضت محكمة النقض بأنه يخرج عن معنى المحرر في صحيح القانون العدادات والآلات واللوحات والصور، حتى ولو تضمنت بعض أجزائها كتابات أو علامات أو أرقام أيا كان نوعها [2].

الفرع الثاني:أركان جريمة التزوير في نطاق المعاملات الالكترونية

بعد التطرق لمحل جريمة التزوير في نطاق المعاملات الالكترونية ألا وهو المستند المعلوماتي نتطرق في هذا الفرع للأركان التي يتم بها الاعتداء على هذا المستند فلكي تتحقق جريمة التزوير لابد من توافر الركنين المادي والمعنوي.

أولا:الركن المادي لجريمة التزوير في نطاق المعاملات الالكترونية

يتكون الركن المادي لجريمة التزوير من عدة عناصر يمكن إجمالها في: تغيير الحقيقة، واتباع طرق لتحقيق ذلك وإحداث ضرر.

1- تغيير الحقيقة في نطاق المعاملات الالكترونية: تغيير الحقيقة هو جوهر جريمة التزوير، والسلوك الإجرامي فيها هو الفعل الواقع على المحرر والذي يتمثل في تغيير الكتابة على نحو مخالف

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 134- 135.
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 901.

للحقيقة، وبغير تغيير الحقيقة لا تقوم جريمة التزوير[1] والمحرر في مجال المعاملات الالكترونية يراد به المستند المعلوماتي وهو كل شيء مادي متميز (قرص أو شريط ممغنط أو خلافه) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات ويستوي بعد ذلك أن يكون هذا الشيء قد خرج من الماكينة وتم تصنيفه أو تخزينه أم أنه مازال بداخلها انتظار لاستخراجه أو تعديله[2].

وقد عالج المشرع الفرنسي هذا الفرض في نص المادة 441-1ق.ع وهو نص أحكم المشرع صياغته من ناحيتين:

- **الأولى:** أنه قد حسم الخلاف حول المحرر المعلوماتي حيث قرر أن تغيير الحقيقة قد يتم في محرر أو في وعاء آخر والمعنى أي دعامة أخرى غير المحرر.
- **الثانية:** أن نص المادة 441-1 قد أطلق طرق تغيير الحقيقة فلم تعد محدودة قانونا على سبيل الحصر كما كان عليه الحال في القانون الفرنسي القديم حيث جاءت عبارة نص المادة 441-1 كما يلي: "يعد تزويرا كل تغيير بطريق الغش في الحقيقة من شأنه أن يحدث ضررا وأيا ما كانت الطريقة التي اجري بها في محرر أو في دعامة (وعاء) أخرى تعبر عن فكر يهدف أو يمكن أن يترتب عليه إقامة الدليل على ثبوت حق أو واقعة ذات آثار قانونية"[3].

فمتى تم تغيير الحقيقة التي يحتويها المستند المعلوماتي وبأي طريقة شرط أن يكون محتوى ذلك المستند يثبت حقا أو واقعة ذات آثار قانونية يتحقق لنا بذلك جوهر جريمة التزوير وهو فعل تغيير الحقيقة.

2- طرق التزوير في نطاق المعاملات الالكترونية:

طرق التزوير في نطاق المعاملات الالكترونية أو المحررات التقليدية قد تكون مادية أو معنوية، وقبل التطرق لطرق التزوير المادي في نطاق المعاملات الالكترونية تجدر الإشارة إلى أن الطرق المادية يجب أن تتم على مستند أصلي حقيقي، وهذا يعني أنه لا يتصور وقوع فعل تغيير

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 921.
2- د/ علي عبد القادر القهوجي، المرجع السابق، ص 150.
3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 923.

الحقيقة من خلال طرق التزوير المعنوية والتي لا تتحقق إلى أثناء تكوين المستند بل يقع هذا التغيير عن طريق الاستعانة بطرق التزوير المادية اللاحقة[1]، ومن أهم طرق التزوير المادية:

1. **الحذف**: وذلك بإزالة كلمة أو رقم أو رمز من شأنه التغيير في مضمون المستند.
2. **الإدخال**: وذلك بإضافة أشياء إلى المستند تغير محتواه.
3. **التعديل**: وذلك بحذف شيء من المحرر وإضافة شيء آخر مكانه.

وهذه الطرق عاقب عليها المشرع الجزائري في نص المادة 394 مكرر 1 وهي من أهم الطرق المستخدمة في التزوير المادي، و يحدث هذا الفرض كثيرا في نطاق المعاملات الالكترونية، خاصة في مجال المعاملات المالية حيث أنه في ظل انتشار التحويل الإلكتروني للأموال من بنك لآخر قد يلجأ المجرم إلى احتجاز أمر الدفع الموجه من بنك إلى آخر وتحريف الرسالة بحيث يتم الدفع لحسابه هو، أو ما يقوم به الجاني من استبدال رقم القيد الخاص به برقم القيد الخاص بأحد الأشخاص[2].

أما أهم طرق التزوير المعنوي في نطاق المعاملات الالكترونية تتمثل في:

1. **تغيير إقرار أولي الشأن:**

ويحدث هذا الفرض كما لو أن الموظف الذي يدون البيانات على النظام المعلوماتي يقوم بتغيير ما يملي عليه صاحب الشأن.

2. **جعل واقعة مزورة في صورة واقعة صحيحة:**

تتمثل هذه الطريقة في إثبات واقعة على غير حقيقتها بمعرفة كاتب المحرر، وعلى ذلك فكل تشويه أو تحريف يدخله كاتب المحرر على الوقائع التي يثبتها فيه عند تدوينه للمحرر يعد تزويرا معنويا بهذه الطريق[3].

1- د/ علي عبد القادر القهوجي، المرجع السابق، ص 156.
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 926.
3- د/ محمد عبيد الكعبي، المرجع السابق، ص 563.

3. جعل واقعة غير معترف بها في صورة واقعة معترف بها:

ويتمثل ذلك في إثبات واقعة مزورة في صورة واقعة صحيحة، كما لو قام محرر محضر بإثبات اعتراف متهم بارتكاب جريمة لم يرتكبها[1].

3- الضرر في نطاق المعاملات الالكترونية:

لا يكفي لقيام جريمة التزوير قيام الركن المادي بتغيير الحقيقة في محرر وأن يتم ذلك التغيير بإحدى الطرق التي يبينها القانون وإنما يجب أن يكون من شأن ذلك إحداث ضرر للغير فحصول ضرر أو احتمال حصوله شرط للعقاب على جرائم التزوير، وبالتالي فإن مجرد قراءة المعلومات على شاشة الحاسب الآلي لا يشكل ضررا، لذلك يعد عنصر الضرر عنصرا جوهريا لقيام الجريمة، ويستوي في الضرر أن يكون ماديا أو أدبيا فرديا أو اجتماعيا، ومسألة توافر الضرر من المسائل الموضوعية التي يقدرها قاضي الموضوع حسب ظروف كل دعوى[2].

ويقاس ضابط الضرر على أساس ما للمستند المعالج آليا من قيمة قانونية في الإثبات، أي مدى صلاحيته لأن يحتج به في مواجهة الغير أو للتمسك به في مواجهته ويستوي بعد ذلك أن يكون هذا المستند قد أعد منذ البداية لهذا الغرض أم أنه يتمتع بتلك القيمة على نحو عارض أوعلى سبيل المصادفة[3].

وقد نص المشرع الفرنسي في المادة 441-1 قانون العقوبات: "يعد تزويرا كل تغيير بطريق الغش قي الحقيقة من شأنه أن يحدث ضررا ..."، فالمشرع تطلب ضرورة أن يؤدي التزوير إلى إحداث الضرر حتى تقوم هذه الجريمة وعلى ذلك فإنه بانعدام الضرر لا يمكن تطبيق العقوبات التي الواردة بالنص.

ثانيا: الركن المعنوي لجريمة التزوير في نطاق المعاملات الالكترونية

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص929
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 930.
3- د/ علي عبد القادر القهوجي، المرجع السابق، ص 151.

التزوير في المحررات جريمة مقصودة ومن ثم يتخذ ركنها المعنوي صورة القصد الجنائي المتمثل في إرادة تغيير الحقيقة في محرر تغييرا من شأنه أن يسبب ضررا حين استعمال المحرر فيما غيرت الحقيقة من أجله، وهو أمر مسلم به في الفقه والقضاء.

كما استقر الفقه والقضاء الجنائي على أنه لا يكفي للعقاب على التزوير أن يكون تغيير الحقيقة قد أرتكب عن علم وإرادة، بل يجب أن يكون بسوء نية أي إضافة للقصد العام يستلزم وجود القصد الخاص أيضا[1].

ويسري التفصيل السابق سواء على المحررات العادية أو المستندات المعلوماتية، وذلك ما سنفصله من خلال التطرق لكل من القصد العام والقصد الخاص.

1- القصد العام:

لتوافر القصد العام يجب أن ينصرف علم الجاني إلى أنه يغير الحقيقة في مستند معلوماتي بإحدى الطرق المحددة في القانون، وأن تتجه إرادته إلى فعل تغيير الحقيقة وكذلك إلى أثره والمتمثل في اشتمال المستند على معطيات مخالفة للحقيقة[2].

فيشترط أن يثبت علم المتهم على وجه اليقين بأنه يغير الحقيقة فإذا لم يكن علمه بتغيير الحقيقة ثابتا بالفعل فإن مجرد إهماله في تحريرها لا يتحقق به هذا الشرط، ويفترض علم الجاني بأن ما حصل من تغيير الحقيقة فيه يعتبر محررا في نظر القانون وأن هذا التغيير قد حصل بطريقة من الطرق التي نص عليها القانون، فالاعتذار بالجهل في هذه الحالة ليس له محل، أما عن الضرر فيجب أن يكون الجاني مدركا وقت تغيير الحقيقة أن من شأن هذا التغيير أن يحدث ضررا ماديا أو أدبيا حال أو محتمل الوقوع يلحق بالأفراد أو بالصالح العام.

وفي إطار المعلوماتية يجب أن يكون الجاني عالما بأنه يقوم بعملية تزوير لمستندات معلوماتية كما يجب أن تتجه إرادته إلى إحداث فعل التزوير[1].

1- د/ كامل السعيد، شرح قانون العقوبات، الجرائم المضرة بالمصلحة العامة، دار الثقافة للنشر والتوزيع، عمان 2008، ص 121.
2- د/ علي عبد القادر القهوجي، المرجع السابق، ص 152.

2- القصد الخاص:

هو نية إضافية أو قصد إضافي يتمثل في اتجاه نية الجاني إلى استعمال المستند المزور فيما زور من أجله[2]، فإذا تخلفت هذه النية انتفى القصد الجنائي، ومتى توافر للقصد الجنائي عناصره فلا عبرة بالبواعث التي قد تدفع الجاني على ارتكاب التزوير، فقد يكون الباعث شريفا في ذاته ولكنه لا يحول مع ذلك دون توافر القصد الجنائي و مثال ذلك حالة من يصطنع مستندا لإثبات حق متنازع عليه ولا سبيل لإثباته إلا بالدليل الكتابي.

فجريمة التزوير المعلوماتية شأنها شأن جريمة التزوير التقليدية من ناحية اشتراط اتجاه نية الجاني إلى إحداث ضرر للغير احتماليا أو فعليا[3].

ومما سبق نخلص إلى أن الركن المعنوي لجريمة التزوير في نطاق المعاملات الالكترونية هو اتجاه إرادة الجاني إلى تزوير مستندات معلوماتية مع نية مسبقة في استعمال المستندات المزورة في الغرض الذي تم تزويرها من أجله، وأن يؤدي هذا الفعل إلى حصول ضرر فعلي أو احتمالي لمن ارتكب ضده فمتى توافر الركن المادي والمعنوي قامت جريمة التزوير واستحق مرتكبها العقوبة .

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 940.
2- د/ علي عبد القادر القهوجي، ص 152.
3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص941.

- خلاصة:

وفقا لما تم تناوله في هذا الفصل يمكن الوقوف على جملة من النقاط اهمها:

أن الجرائم المعلوماتية تتميز بجملة من الخصائص التي تجعلها مختلفة عن الجرائم التقليدية وذلك ما يوجب على التشريعات المختلفة أن تعمل للتصدي لها بغية حماية المعاملات الإلكترونية منها، كون هذا التصدي يحقق جملة من الأهداف والتي يعتبر أهمها التوجه نحو الحكومة الإلكترونية والتي تمثل الحماية التشريعية بالنسبة لها الأرضية الخصبة لتجسيدها.

أن المشرع الجزائري على خلاف أغلب التشريعات العربية يكون قد أغلق باب الاجتهاد الفقهي ولو نسبيا، وذلك باستحداثه للنصوص السالفة الذكر والمتعلقة بحماية أنظمة المعالجة الآلية للمعطيات، حيث أحاط النظام المعلوماتي بالعديد من النصوص لحمايته فاعتبر مجرد الدخول جريمة سواء أدى ذلك الدخول إلى نتيجة أخرى أو لا، مع عدم إغفال أن هذه النصوص المستحدثة تتخللها بعض النقائص والتي نفرد الحديث عنها في خاتمة هذه الرسالة .

أما في مجال الإتلاف المعلوماتي فقد أحاط المشرع المعلومات المتبادلة في مجال المعاملات الالكترونية بنصوص عقابية كفيلة بحمايتها من الاعتداءات التي قد تطال تلك المعاملات أو المنظومة المعلوماتية ككل.

وفيما يتعلق بالتزوير الحاصل في نطاق المعاملات الالكترونية نجد أن المشرع الجزائري وجل التشريعات العربية لا تزال تعاني من الفراغ التشريعي في هذا المجال على غرار التشريعات الغربية التي استحدثت نصوصا خاصة أو عدلت النصوص التقليدية القائمة، وذلك قصد مواكبة القانون الجنائي للتطورات الحاصلة في مجال المعاملات الالكترونية. وذلك ما يوجب على التشريعات العربية أن تسير نحوه.

الفصل الثاني:

الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد العامة في قانون العقوبات

اعتنى القانون الجنائي بحماية حق الملكية عناية كبيرة وحاز المنقول من هذه العناية بنصيب أوفر حيث أن المشرع الجنائي يعاقب على السرقة والنصب وخيانة الأمانة، وكل هذه الجرائم لا تقع إلا على منقول ويكون الغرض منها دائما الاستيلاء على مال الغير.

وبما أننا نتناول موضوع المعاملات الإلكترونية فلا مجال لدينا لإغفال الحديث عن جرائم الأموال و التي لا يمكن أن تكون تلك المعاملات في منأى عنها، مع عدم إغفال صعوبة تكييف هذه الجرائم على المعاملات الإلكترونية نظرا لإشكالية كيفية مواجهة القانون الجنائي لهذا الواقع حيث انعكس ذلك سلبا على رجال القانون في مواجهة هذا النمط المستحدث من الجرائم والتي لم تكن في ذهن المشرع عند سنه للنصوص العقابية، ما يجعل القاضي الجزائي مقيدا بمبدأ شرعية الجرائم والذي يمنعه من تجريم أفعال لم ينص عليها القانون، وخاصة بعدما رأينا في الفصل الأول نسبية النصوص المستحدثة في حماية هذه المعاملات.

فإلى أي مدى يمكن للقواعد العامة لقانون العقوبات أن تحمي المعاملات الإلكترونية ؟

وهل يمكن أن يصلح ما يتم تداوله في هذه المعاملات أن يكون محلا لجريمة السرقة أو النصب أو خيانة الأمانة ؟

وسواء اعتنى التشريع الجنائي بحماية المعاملات الإلكترونية من هذه الجرائم أو لا، هل يمكن القول بأن العقاب على الاتفاق أو الشروع في جرائم المعلوماتية كإجراء وقائي كفيل بحماية المعاملات الإلكترونية ؟

للإجابة عن هذه الأسئلة سنتطرق في هذا الفصل إلى مبحثين على الشكل التالي:

المبحث الأول: الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد العامة المقررة في جرائم الأموال.

المبحث الثاني: الحماية الجنائية للمعاملات الإلكترونية من خلال تجريم الاتفاق أو الشروع في الجرائم المعلوماتية.

المبحث الأول

الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد العامة المقررة في جرائم الأموال

تنقسم الجرائم التي تمثل اعتداء على ملكية المنقول إلى طائفتين رئيسيتين، إحداهما تضم جرائم تكون الغاية منها الإستلاء على مال الغير، والأخرى تشمل جرائم تكون غايتها إتلاف مال الغير ويدخل ضمن الطائفة الأولى كل من جرائم السرقة والنصب وخيانة الأمانة [1]

و الحديث عن حماية المعاملات الإلكترونية وفقا للقواعد العامة المقررة في جرائم الأموال هو أمر محسوم فيه ومحقق سلفا، وذلك حال الاعتداء على المكونات المادية للنظام المعلوماتي فلا يقوم الإشكال حال الاعتداء على المعلومات المخزنة على أدوات التخزين ذات الكيان المادي المحسوس كالدعامات والأشرطة ...

فمتى كانت المعلومات داخل دعامات مادية وتم الاعتداء على هذه الأخيرة كالاعتداء على قرص أو ذاكرة الحاسب الآلي في شكلها المادي أو الخارجي فلا يثور لدينا إشكال، ذلك أن هذه الجرائم تعد تقليدية وتلك المكونات تعتبر مالا ماديا منقولا يخضع للحماية الجنائية بموجب نصوص قانون العقوبات.

لكن الإشكال الذي يعترضنا هو حال وقوع هذه الجرائم على المكونات المنطقية أي المعلومات المخزنة داخل الجهاز أو التابعة للنظام المعلوماتي وذلك في شكلها المعنوي، أو تلك التي يتم تبادلها في مجال المعاملات الإلكترونية.

فهل تصلح هذه المعلومات لأن تكون محلا لجرائم الأموال كالسرقة والنصب وخيانة أو أن تخضع لنشاطها الإجرامي، وبصيغة أخرى هل تطبق القواعد العامة التي تحكم كل من جرائم السرقة والنصب وخيانة الأمانة على الجرائم الواقعة في مجال المعاملات الإلكترونية؟ [2]

أم أن المكونات المعنوية للنظام المعلوماتي تقتضي وجود نصوص خاصة لحمايتها؟

1- د/ عمر السعيد رمضان ، شرح قانون العقوبات القسم الخاص، دار النهضة العربية ، القاهرة 1986، ص408
2- د/ عبد الحق حميش، حماية المستهلك الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي، 10-12 ماي 2003، ص 1267 .

للإجابة على هذه الأسئلة سنتطرق في هذا المبحث إلى ثلاثة مطالب على الشكل التالي:

المطلب الأول: مدى تحقق الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد العامة لجريمة السرقة.

المطلب الثاني: مدى تحقق الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد العامة لجريمة النصب.

المطلب الثالث: مدى تحقق الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد العامة لجريمة خيانة الأمانة.

المطلب الأول

مدى تحقق الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد العامة المقررة لجريمة السرقة

نص المشرع الجزائري على جريمة السرقة والجرائم الملحقة بها تحت عنوان "السرقات وابتزاز الأموال" في المواد من 350 إلى 369 من قانون العقوبات، وقد عرف المشرع الجزائري السرقة من خلال تعريفه للسارق في نص المادة 350 قانون العقوبات حيث نص على "كل من اختلس شيئا غير مملوك له يعد سارقا" وعليه يمكننا القول أن السرقة هي اختلاس مال منقول مملوك للغير بنية تملكه، ومن ثم يمكن القول أن جريمة السرقة تقوم على ثلاثة أركان وهي:

1. محل الاعتداء وهو المال المنقول المملوك للغير.
2. النشاط المادي وهو فعل الاختلاس.
3. الركن المعنوي وهو القصد الجنائي.[1]

فقيام جريمة السرقة يستلزم توافر هذه الأركان مجتمعة فإذا تخلف أحدها انتفت الجريمة.

والمقصود بمحل الاعتداء أي المال المنقول المملوك للغير هو كل شيء قابل أن يكون محلا للسرقة شرط أن يكون للشيء قيمة سواء كانت تجارية أو مادية أو أدبية،[2] ويجب أن يكون هذا المال منقولا أي توافر إمكانية نقله من مكان لآخر أو من شخص لآخر، أضف إلى ذلك أن يكون هذا المال ملكا للغير فلا تتحقق جريمة السرقة على من يستولي على ماله الذي يعتبر مالكا له ملكا تاما، وبتوفر هذه الشروط يكون محل الاعتداء متوافرا.

أما النشاط المادي أي فعل الاختلاس هو الذي تتم به جريمة السرقة أي إخراج المال من حيازة المجني عليه إلى حيازة الجاني أو أي شخص ليس له الحق في ذلك[3].

1- حسين فريجة، شرح قانون العقوبات الجزائري، ديوان المطبوعات الجامعية بن عكنون، الجزائر 2006، ص 188.
2- د/ أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ط 10، دار هومة للنشر والتوزيع، الجزائر 2009، ص268،267
3- حسين فريجة، ص202

وبتحقق الركنين السابقين لا يبقى لنا سوى البحث عن توافر الركن المعنوي لاكتمال جريمة السرقة والذي يتمثل في القصد الجنائي العام والخاص، حيث يتحقق القصد العام بتوافر ركنيه العلم والإرادة أي علم الجاني بأن المال المستولى عليه مملوك للغير، فإذا استطاع الجاني إثبات عدم علمه بأن المال ليس ملكا له انتفى لديه عنصر العلم، أما الإرادة فتتمثل في أن تتجه إرادة الجاني بنقل الحيازة من صاحبها إلى شخص آخر.

إضافة إلى توفر القصد العام يجب توافر القصد الخاص والمتمثل في نية تملك المال من طرف المتهم، فلا يعد سارقا من يستولي على مال الغير بقصد الإطلاع عليه أو معاينته أو الانتفاع به ورده إلى صاحبه أو بقصد المزاح مع المجني عليه، وعلى هذا لا يعد سارقا من قام بتجريد شخص من سلاحه بقصد منعه من ارتكاب جريمة[1].

فمتى تحققت كل هذه الأركان مجتمعة كنا بصدد جريمة السرقة وفقا للقواعد العامة، لكن الإشكال الذي يصادفنا هو ما مدى تحقق هذه الأركان في نطاق المعاملات الإلكترونية ؟ أي هل تتحقق جريمة السرقة بمفهومها التقليدي على المكونات المعنوية للنظام المعلوماتي؟

للإجابة على هذا السؤال ارتأينا الطرق لكل من محل وأركان جريمة السرقة في ظل القواعد العامة وتطبيقها في مجال المعاملات الإلكترونية وذلك على النحو التالي:

الفرع الأول: محل جريمة السرقة في نطاق المعاملات الإلكترونية

أولا: مدى انطباق وصف المال والمنقول على المعلومات.

ثانيا: ملكية الغير للمال المعلوماتي.

الفرع الثاني: أركان جريمة السرقة في نطاق المعاملات الإلكترونية.

أولا: الركن المادي لجريمة السرقة في نطاق المعاملات الإلكترونية.

ثانيا: الركن المعنوي لجريمة السرقة في نطاق المعاملات الإلكترونية.

1- حسين فريجة، المرجع السابق، ص 202.

الفرع الأول: محل جريمة السرقة في نطاق المعاملات الإلكترونية

تنص المادة 1/311 من قانون العقوبات الفرنسي[1] على أن السرقة هي اختلاس شيء مملوك للغير بطريق الغش، وقد استقر القضاء والفقه في تفسيره للنص السابق على أن فعل الأخذ والاختلاس في السرقة يجب أن يرد على شيء مادي أو مال مادي وهذا يعني أن السرقة لا تقع إلا على شيء ذي كيان مادي ملموس[2]

فالجرائم الواقعة على المكونات المادية للنظام المعلوماتي تعد من قبيل الجرائم الواقعة في نطاق الجرائم التقليدية فهي تقع ضمن الجرائم العادية التي تستهدف المال و ذلك كون المكونات المادية للحاسوب تصنف ضمن الأموال المنقولة ومن ومن ثم فهي تصلح محلا للجرائم التقليدية، وعلى ذلك الأساس إصطلح الفقه سرقة الأجهزة المادية المعلوماتية على الإعتداءات التي تتعرض لها هذه المكونات [3]

أما السرقة في مجال المعاملات الإلكترونية فهي لا تستهدف الشريط الممغنط أو الأسطوانة أو الذاكرة أو الأسلاك التي تنقل الشارة لأن السارق لا يستهدف سرقتها للحصول على القيمة المادية لها بل ليسرق ما هو مسجل عليها[4]

فهل يمكن أن تقع جريمة السرقة على كيان معنوي غير ملموس؟ أي هل ينطبق وصف المال على المعلومات أم لا ؟

لذلك سنتطرق للجدل الذي ثار حول مدى انطباق وصف المال على المعلومات ثم نستكمل محل جريمة السرقة من خلال التعرض لملكية الغير للمال المعلوماتي.

1- Art311/1 « le vol est la soustraction frauduleuse de la chose d'autrui » code pénale français.
2- د/ علي عبد القادر القهوجي، المرجع السابق، ص 86.
3 - Henri croze et yves Bismuth ;le droit de l'informatique . paris expertise . 1984.P151
4- د/ رياض سليمان عواد، أمن المعلومات وضرورة وضع تشريع الجرائم الحاسب الآلي، مجلة الشرطة العدد 359، نوفمبر 2000، ص47

أولا : مدى انطباق وصف المال على المعلومات

المعلومة في اللغة اللاتينية لها مدلولان يتمثل الأول في الإعلام والذي يعني فعل الصياغة أو الوضع في هيئة أو شكل معين، أما المدلول الثاني فيعني التصور، وبجمع المدلولين معا يتجسد لدينا الجانب الحركي والوصفي للمعلومة [1]

وقد عرف الأستاذ Parker المعلومات بأنها "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو التفسير والتأويل أو للمعالجة بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة" [2].

كما عرفت المادة الأولى من القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات البيانات أو المعلومات انها: "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الآلي كالأرقام والحروف والرموز وما إليها" [3]، ومن ثم فلكي يتحقق للمعلومة هذا الوصف السابق فيجب أن تتوافر فيها العديد من الشروط و التي من بينها:

-التحديد والابتكار: فلكي تكون الرسالة مخصصة للتبليغ يجب أن تكون المعلومة محددة لان التبليغ الحقيقي يفترض التحديد ذلك أن الاعتداءات على الأموال تفترض دائما وجود شيء محدد طالما أن هذا الشيء يجب أن يكون لحق محدد، أما الابتكار فهو أمر ضروري ذلك أن المعلومة غير المبتكرة هي معلومة شائعة يسهل الوصول إليها من قبل الكافة وليس من شأنها أن ترتبط بشخص أو بمجموعة من الأشخاص.

- أن تكون المعلومة سرية ومستأثرة: الطابع السري يحصر المعلومة في دائرة محددة من الأشخاص والمعلومة غير السرية لديها ميل إلى الحركة ويمكن أن تحاز بحرية، أما الاستئثار فهو أمر ضروري قد يخص بعض الأشخاص أو لشخص واحد فقط كالمؤلف أو صاحب المعلومة.[4]

1 - Daragon elise . etude sur le statut juridique de l'informatique . Dalloz 1998 , P64

2 - نهلا عبد القادر المومني ، المرجع السابق ، ص 102

3- www.arabic.Mjustice.dz le :09/11/2010 à 11h00mn

4- د/ عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2001، ص 156- 156 نقلا عن =

والاستئثار هو الحصر أي أن تكون هذه المعلومة محصورة لدى صاحبها أو أشخاص محددين، وإذا لم تتوفر هذه الخصائص في المعلومة فلا نكون بصدد إشكال حال التعدي عليها ذلك أن المعلومة الشائعة لا يعتبر الإطلاع عليها انتهاكا لسريتها.

وبعد التطرق لهذه الخصائص التي تمتاز بها المعلومة، تدفعنا طبيعتها المعنوية للبحث في مدى انطباق وصف المال عليها؟

ظهر حول هذا التساؤل اتجاهان، حيث ذهب جانب من الفقه إلى القول بذاتية المكونات المعنوية للنظام المعلوماتي أي لا يمكن اعتبارها مالا ومن ثم فلا يمكن أن تكون محلا لجريمة السرقة.

في حين ذهب جانب آخر للقول بأن المكونات المعنوية للنظام هي مجموعة مستحدثة من الأموال، أي يمكن أن تكون محلا لجريمة السرقة.

الاتجاه الأول: المعلومات ليست مال

تعددت الآراء الفقهية التي ترى أن المعلومات لا يمكن أن تكون محلا لجريمة السرقة لأنها ليست مالا، أي التسليم بالطبيعة الذاتية للمعلومة.

وهذا الوصف هو نتيجة لتطبيق المنهج التقليدي الذي يضفي وصف المال على الشيء المادي وحده، وينطلق هذا المنهج من الحقيقة التي مؤداها أن الأشياء التي تعد من قبيل الأموال هي الأشياء القابلة للتملك، ويستخلص من هذه الحقيقة أن الأشياء التي تكون قابلة وحدها لأن تكون محل للحق الاستئثاري هي التي تعد من قبيل الأموال.[1]

وبالتالي فالمعلومة لا تصلح لان تكون محلا لجريمة السرقة إلا إذا اقترنت بالمادية، فالمعلومات المسجلة إلكترونيا والمخزنة داخل النظام المعلوماتي أو على وسائط التخزين الخارجية وكذلك الحال

=P. Catala les transformation de droit par l'informatique in émergence du droit de l'informatique et des parques 1983, p 264.

1- د/ عبد الله حسين علي محمود، المرجع السابق، ص 163.

بالنسبة للبرامج المعلوماتية لا يعد الاعتداء عليها جريمة سرقة إلا إذا كانت مسجلة على دعامات أو أسطوانات فهي بذلك تصبح أموال ومن ثم تصلح محلا لجريمة السرقة.[1]

ومما سبق يتبين أنه لا خلاف في الفقه حول سرقة الكيان المادي للأنظمة المعلوماتية وكذلك البرامج والمعلومات إذا تم إفراغها على أية وسيلة مادية كالأسطوانات [2]

لكننا نرى أن الأخذ بالحجة القائلة أن الأشياء التي تكون محل للحق الاستئثاري فقط هي التي تعد من قبيل الأموال والاستناد على هذه الحجة لاستبعاد وصف المال على المعلومة هو في الحقيقة إغفال لخاصية أساسية للمعلومة ألا وهي الاستئثار، فقد سبق وأشرنا أن من بين أهم خصائصها هو الاستئثار، أي أن تكون محصورة عند شخص أو بضع أشخاص فمتى فقدت المعلومة هذه الخاصية تصبح شائعة وبالتالي تخرج من نطاق دراستنا لأننا بصدد البحث عن الجرم الذي يترتب عن انتهاك المعلومات السرية وليست المعلومات التي يكون للجميع الحق في الإطلاع عليها.

و ذهب رأي آخر إلى اعتبار المعلومات ليست مالا بحجة أن المعلومات التي نقابلها افتراضا هي من قبيل الأشياء المعنوية، وأن الحق الاستئثاري الذي من شأنه أن يتقدم بالنسبة لها لا يمكن من خلال التحليل التقليدي إلا أن يكون من قبيل حقوق الملكية الأدبية أو الفنية أو الصناعية، إلا أن المعلومات المخزنة لا تنتمي إلى المعلومات الأدبية أو الفنية أو الصناعية الأمر الذي يؤدي إلى رفض منحها حق الإقامة في هذه المجالات، وهكذا تستبعد بالضرورة من نطاق مجموعة الأموال[3]

كما ذهب رأي إلى القول بأن مقومات الجانب غير المادي من النظم الآلية لمعالجة المعلومات من برامج ومعلومات ليست بمال، ولكن هذه المقومات يمكن أن تستغل ماليا، وآية ذلك أن البرنامج هو إبداع فكري وذهني قابل للاستغلال المالي وحقيقة دوره انه أسلوب لمعالجة المعلومات، وعلى ذلك فإن الاعتداء على البرنامج ونسخه هو اعتداء على حقوق المؤلف وذلك في استغلال مؤلفه استغلالا ماليا، ومن ثم يرد عليه أحكام حماية حق المؤلف وليس السرقة أما بالنسبة للمعلومة فلا يخلو الأمر من أحد الفرضين:

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 527.
2 -Bertrand(A) . la criminalité informatique . les débits relatifs ou matriel . expertisés. Juin 1984.P150
3- د/ عبد الله حسين علي محمود، المرجع السابق، ص 164.

- **الأول:** أن تكون المعلومة سرية حيث يكون الإطلاع عليها أو حيازتها محظورا على غير ذي الصفة في ذلك، وفي هذه الحالة فإن الحصول عليها في الواقع لمن لا صفة له في ذلك يمثل انتهاكا لسرية المعلومات وليس سرقة لها.

- **أما الفرض الثاني:** فيتمثل في أن تكون المعلومة غير سرية فهي إما أن تكون مجانية ومن ثم فلا جريمة في الحصول عليها، وإما أن تكون بمقابل وهنا يشكل الأمر جريمة سرقة منفعة، وينتهي هذا الرأي إلى أن مكونات الجانب غير المادي من النظام المعلوماتي لا يتحقق فيها وصف المال بالمعنى المتداول وأن تسميتها مجازا بالأموال المعلوماتية يتعين فهمه على أنه يعني القابلية للاستغلال المالي.[1]

لكن القول بأن جريمة السرقة لا تتحقق إلا إذا كانت المعلومة بمقابل فنكون بصدد جريمة سرقة منفعة، فالأخذ بهذه الحجة هو أمر منافي لطبيعة المعلومة ذاتها فالمعلومة يمكن أن تكون تجارية وبالتالي يشترط لها صاحبها مقابلا ماديا للحصول عليها، وقد تكون تلك المعلومة تشكل خصوصية لصاحبها و من ثم فلا يمكن تقييمها بمقابل مادي، وعليه يمكن القول أنه متى تحققت للمعلومة خصائصها من تحديد وابتكار وسرية واستئثار وجب اعتبارها مالا معنويا ومن ثم حمايتها من الاعتداء أي سواء فرض لها صاحبها مقابلا ماديا أو لا.

الاتجاه الثاني: المعلومات عبارة عن مال

ذهب جانب من الفقه الحديث إلى اعتبار الشئ مالا ليس بالنظر إلى كيانه المادي وإنما على أساس ما له من قيمة أو منفعة اقتصادية، وذلك ما يتجسد في المعلومة[2]

ومن ثم يرى الأستاذ Catala أن المعلومة واستقلالا عن دعامتها المادية تعد من قبيل المال للحيازة، ولتدعيم هذا الوصف فقد أشار بأن المعلومة قابلة للحيازة، وهي قيمة تقوم وفقا لسعر السوق وأنها منتج بصرف النظر عن دعامتها المادية وعن عمل من قدمها وأن المعلومة ترتبط بصاحبها عن طريق علاقة قانونية، وهي علاقة المالك بالشيء الذي يملكه وأنها تنتمي إلى مؤلفها

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 529.

2 - Roger Merle : traite de droit criminal . édition cujus 1998 . p182

بسبب علاقة التبني التي تربط بينهما، وهكذا اعتمد الأستاذ Catala من أجل إضفاء وصف المال على المعلومة على قيمتها الاقتصادية من ناحية وعلاقة التبني التي تربط بينها وبين المؤلف، وأيده في ذلك الأستاذ Carbonnier حيث يرى أن القانون الذي يرفض بذاته إضفاء وصف المال على شيء له قيمة اقتصادية سيبقى حتما على خلاف الحقيقة.[1]

إذن يمكن القول أنه إذا ما وضعنا في الاعتبار العلاقة التي تربط المعلومة بمؤلفها فمن الممكن الاعتراف بإمكانية حيازة المعلومة ومن ثم إضفاء وصف المال عليها.

هذا ويذهب الأستاذ Vivant أن المعلومة مال مستندا في ذلك على حجتين:

- **الأولى:** أن قيمة الشيء "المال" ليست قاصرة على الصورة المادية فقط وإنما لها أيضا صورة معنوية، وأن صفة محل الحق يجوز أن تنتمي لمال معنوي ذي طابع اقتصادي.

- **الثانية:** أن المعلومة محمية من قبل بنصوص الملكية الأدبية المخصصة من أجل إجازة الأشياء المملوكة ملكية معنوية.[2]

ويضيف الأستاذ Vivant أن لصاحب المعلومة الحق في أن يتنازل عنها بموجب عقد أو يقيد استخدامها أو أن يرفضه، وذلك ما يعزز من اعتبارها مالا[3].

وذهب جانب آخر إلى الربط بين الطبيعة المالية للمعلومة وبين الإطار المادي الذي يحتويها مؤكدا أن المال المعلوماتي "البرامج والمعلومات" لا يمكن أن يكون شيئا ملموسا أو محسوسا ولكن يمكن أن يكون له كيان مادي يمكن رؤيته على الشاشة مترجم إلى أفكار، وأن المعلومة المتنقلة عبر الأسلاك عن طريق انتقال نبضات أو رموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل ومولد صادرة عنه يمكن سرقته وبالتالي لها كيان مادي.[4]

1- د/ عبد الله حسين علي محمود، المرجع السابق، ص 168- 169.
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 526.
3- د/ عبد الله حسين علي محمود، ص 171.
4- نهلا عبد القادر المومني، المرجع السابق، ص 110.

ويعزز هذا الاتجاه رأيه بتفسيره لنص المادة 379 عقوبات فرنسي قديم والتي تقابلها المادة 311 قانون العقوبات الفرنسي الجديد، حيث اعتبروا أن كلمة "شيء" الواردة في المادة تشمل الأشياء المادية وغير المادية، وطالما أمكن حيازة الأشياء غير المادية مثل حق الارتفاق والدين وحق الانتفاع، فإنه من الممكن حيازة المعلومات وفي المقابل سلب هذه الحيازة .

كما أن المعلومة منفصلة عن دعامتها المادية هي مال يمكن تملكه لما له من قيمة اقتصادية إذ يمكن للجاني استغلال المعلومات بأن يبرم عقودا مع الغير، بحيث تكون هذه المعلومات سواء المخزنة أو المنقولة محلا لها وبالتالي حرمان صاحبها من عائدها المادي، وكذلك يمكن أن تقوم المعلومة باعتبارها خدمة [1]

فالمعلومات تصنف إذن ضمن الأموال المعنوية أو اللامادية، وعلى ذلك فهي تصلح لأن تكون محلا للاختلاس المعلوماتي أو السرقة المعلوماتية، كما أن نقل حيازة هذه المعلومات يتفق وطبيعتها فهو نقل معنوي وليس مادي ولا يشترط أن تضمن هذه المعلومات ضمن دعامة مادية أو شريط تسجيل حتى يمكن القول باختلاسها ماديا.[2]

و في هذا الصدد يرى بعض الفقه المصري أن ما استقر عليه بعض الفقه في اعتبار المكونات المعنوية للنظام لا تصلح لأن تكون محلا لجريمة السرقة، هو اعتبار يفسره الظروف والوقت الذي وضعت فيه نصوص السرقة، حيث كانت الأموال المعنوية قليلة العدد والقيمة، وان الحماية الجنائية وقتها كانت مركزة على حماية الأموال المنقولة المادية، في حين أن الأشياء المعنوية الآن زاد عددها مع التطور وازدادت قيمتها الاقتصادية، حتى أن بعضها فاق الأموال المادية المنقولة والعقارية على السواء فهذه الأشياء لم تكن في ذهن المشرع وقت وضع النصوص السابقة[3].

ونحن من وجهة نظرنا نؤيد الاتجاه القائل بإمكانية اعتبار المكونات المعنوية للنظام المعلوماتي محل لجريمة السرقة ذلك أن المشرع الفرنسي أو الجزائري على حد السواء قد نص في المادة 350 من قانون العقوبات على: "كل من اختلس شيئا غير مملوك له يعد سارقا ويعاقب بالحبس من سنة

1- محمد أمين الشوابكة، المرجع السابق، ص151،152
2- د/ عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، المرجع السابق، ص 272.
3- د/ علي عبد القادر القهوجي، المرجع السابق، ص 86

إلى 5 سنوات وبغرامة من 100.000 دج إلى 500.000 دج، وتطبق نفس العقوبة على اختلاس المياه والغاز والكهرباء..."، فكلمة شيء التي جاء بها المشرع الجزائري هي كلمة فضفاضة تحتمل أن يكون ذلك الشيء ماديا أو معنويا، فمحل السرقة يشمل مطلق الأموال متى قبلت هذه الأخيرة الأخذ أو الاختلاس.

أضف إلى ذلك أن المشرع نص في الفقرة الثانية على أن تطبق نفس العقوبة على اختلاس المياه والغاز والكهرباء، فطبيعة التيار الكهربائي ليست مادية وبالرغم من ذلك قام المشرع بحمايته وذلك لما له من قيمة اقتصادية، وهو ما يتطابق مع طبيعة المعلومة وقيمتها الاقتصادية، وبالتالي يمكن القول أن تطبيق هذا النص على المكونات المعنوية للنظام المعلوماتي لا يمثل خروجا على مبدأ شرعية الجرائم والعقوبات، ذلك أن هذا النص مطلق يستوي أن يكون عنده الشيء ماديا أو معنويا ومن ثم فلا يجوز تقييده، ولتجنب هذا الخلاف الفقهي نقترح إضافة مصطلح شيء مادي أو معنوي لنصوص تجريم السرقة وبذلك يحسم هذا الجدل الفقهي.

ثانيا: ملكية الغير للمال المعلوماتي

نص المشرع الجزائري في المادة 350 من قانون العقوبات على ضرورة أن يكون المال محل السرقة ليس ملكا للجاني، أي مملوكا للغير فمتى كان المال ملكا للجاني فلا تقوم جريمة السرقة حتى ولو كان المال المسروق محل نزاع ثم عادت ملكيته للجاني فلا تقوم الجريمة، والعبرة في الملكية هو وقت ارتكاب فعل الاختلاس، وكما سبق وأن أشرنا فالمكونات المادية للنظام المعلوماتي لا تثير إشكالا نظرا لخضوعها للقواعد العامة التي تحكم جريمة السرقة.

وبالنسبة للبرامج المعلوماتية والتي تشكل أو تحمل طابعا ابتكاريا أو تمثل محتوى فكريا، فإن تلك البرامج تكون محمية بقانون حماية حقوق الملكية الفكرية وحقوق المؤلف فالبرنامج ملكا لمن ابتكره.[1]، أما عن المعلومة المجسدة في أفكار داخل النظام المعلوماتي فاختلاسها يشكل جريمة سرقة متى توافرت أركان الجريمة، حيث يشترط أن تكون تلك الأفكار الموجودة داخل النظام ليست ملكا للجاني وملكا للغير كالمعلومات التي تعبر عن أفكار صاحبها والتي جسدها داخل النظام

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 542.

المعلوماتي وأعطى لها صفة المعلومة من تحديد أي أن لا تكون فضفاضة، وابتكار أي أن تكون مستحدثة، وأن تكون سرية أي إحاطتها بنظام مشفر لكي لا يتم الإطلاع عليها، وأن تكون مستأثرة أي حصرية لشخص أو لمجموعة أشخاص فقط، فإذا لم تتوفر هذه الشروط تكون المعلومة شائعة، أي يحق لأي شخص الإطلاع عليها ومن ثم تملكها وبالتالي فهي ليست ملكا للغير، ومن ثم إذا تم الاعتداء عليها فلا يصح لصاحب المعلومة الإدعاء بوقوع جريمة السرقة على معلوماته.

الفرع الثاني:أركان جريمة السرقة في نطاق المعاملات الإلكترونية

نتطرق في هذا العنصر لكل من الركن المادي والمعنوي لهذه لجريمة:

أولا: الركن المادي لجريمة السرقة في نطاق المعاملات الإلكترونية

البحث في مدى تحقق الركن المادي لجريمة السرقة في نطاق المعاملات الالكترونية هو مراعاة لمدى تحقق فعل الأخذ أو الاختلاس في هذه الجريمة

ويستوي فعل الاختلاس في أن يكون الجاني قد استولى على المال خلسة أو عنوة أو تسلمه بناءا على يد عارضة فغير نيته واستولى عليه، ومن ثم فإن فعل الاختلاس يقتضي نقل حيازة المال موضوع الاختلاس أو السرقة من حيازة المجني عليه إلى الجاني، بمعنى أن يظهر الجاني بوصفه صاحب السلطة والسيطرة الفعلية[1]

والاستيلاء بهذا المعنى ينتج عليه خروج الشيء المستولى عليه من ذمة ودخوله في ذمة أخرى، وبعبارة أخرى إفراغ ذمة وإشغال ذمة أخرى بحيث لا يوجد مجال لتزاحم الذمتين في الاستيلاء على الشيء، وبتطبيق المعنى السابق للاختلاس على برامج الحاسب الآلي أو المعلومات المعالجة بصفة عامة تصادفنا العديد من العقبات، حيث تتمثل الأولى في أن الجاني وإن كان يدخل في ذمته ما استولى عليه من برامج إلا أنه في نفس الوقت لم يخرج هذه البرامج من ذمة صاحبها الشرعي إذ تظل رغم مباشرة أفعال الاختلاس عليها تحت سيطرة هذا الأخير دون أدنى انتقاص من محتواها كما يلاحظ أن الاستيلاء على البرامج باعتبارها معلومات لا يتصور إلا على أنه انتقال لهذه المعلومات من ذهن إلى ذهن أو من ذاكرة إلى ذاكرة وهذه عقبة ثانية، أما العقبة الثالثة فتتمثل في

1- د/ خالد ممدوح إبراهيم، أمن الحكومة الإلكترونية، المرجع السابق، ص 164.

أن المعلومات التي تحويها البرامج من طبيعة غير مادية أي أنها شيء معنوي فكيف يتصور فعل الأخذ والاختلاس الذي هو من طبيعة مادية على شيء معنوي.[1]

ولتفصيل هذه العقبات يجدر بنا التطرق لأهم الصور التي يتم بها فعل الاختلاس في مجال المعاملات الالكترونية:

الصورة الأولى: الالتقاط الذهني للبيانات

يتحقق هذا الالتقاط بالاختزان أو الحفظ الواعي أو العرضي للمعلومات في ذاكرة الإنسان إثر مطالعتها بالبصر إن كانت قد ظهرت على شاشة الحاسب في شكل مرئي، أو بعد وصولها إلى الأذن إن تمثلت في صورة صوتية صادرة من الأجهزة[2].

والاختزان الواعي للمعلومة في الذاكرة إثر التقاطها ذهنيا سواء عن طريق البصر أو السمع هو محل خلاف فقهي حيث ظهر فيه اتجاهين:

الاتجاه الأول:

يرى هذا الاتجاه أن الاختزان الواعي للمعلومة في الذاكرة إثر التقاطها ذهنيا لا يصلح أن يكون محلا للاختلاس، والسبب في ذلك هو عدم وجود نشاط مادي في هذه الحالة وقع تحت سيطرة الجاني، كما أن سلوك الشخص في هذه الحالة لا يتوافر فيه مقومات النشاط المادي ذو المظاهر الخارجية الملموسة الذي يقتصر التجريم عليه في الشرائع الحديثة، وإن وجود جرائم تتمثل مادياتها في محض النشاط الذهني تفتح مجالا لتجريم ما يدور في العقول والأذهان وهذا غير معقول، كما أن القول بأن مجرد الإطلاع على المعلومات دون علم ورضاء صاحبها يمثل جريمة سرقة يؤدي إلى نتائج غير معقولة ومبالغ فيها، فلا يمكن عقاب الجاني في حالة سماعه للمعلومات التي تهمه من خلال مكبر الصوت أو قراءة المعلومات التي يبحث عنها من خلال شاشة الجهاز، فالجاني اطلع على المعلومات عن طريق السمع أو المشاهدة دون علم وعلى غير إرادة صاحبها الشرعي، إلا انه لا يوجد أي شيء مادي بين يدي الجاني.[3]

1- د/ علي عبد القادر القهوجي، المرجع السابق، ص 95.
2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 23.
3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 571.

الاتجاه الثاني:

يرى هذا الاتجاه أن الاختزان الواعي للمعلومة في الذاكرة اثر التقاطها ذهنيا يصلح أن يكون محلا للاختلاس، وقد علل أحد أنصار هذا الرأي ذلك بقوله أنه "مع التحفظ بشأن صعوبة الإثبات فليس ثمة عقبة نظرية هامة تحول دون تقبل وقوع سرقة المعلومة من قبل من يقوم بدلا من النسخ بقراءة مستند وتسجيله وحفظ فحواه في ذاكرته[1].

كما استند هذا الاتجاه أن المعلومات المعالجة آليا طالما تم وضعها والتعامل معها، فطبيعتها تصبح مادية ومالية وبالتالي تصلح لأن تكون موضوعا للاختلاس سواء تم نقلها أو نسخها أو الإطلاع عليها بالبصر أو السمع أي عن طريق الالتقاط الذهني، لأنه يمكن أن يترتب على ذلك أضرار بمالكها وبقيمتها الاقتصادية إذا قام الجاني باستخدامها وترجمتها على أي مخرجات سواء كانت أسطوانات أو شرائط أو أوراق وعرضها للبيع.[2]

الصورة الثانية: الالتقاط الهوائي للبيانات المعالجة أو المنقولة

معروف أن الحاسبات الإلكترونية وكوابلها ودائرتها الكهربائية وما يتصل بها من توابع تصدر أثناء تشغيلها إشعاعات كهرومغناطيسية يمكن التقاطها وترجمتها إلى بيانات مرئية على شاشة تلفزيونية، وأن ثمة إمكانية لاعتراض والتقاط البيانات أثناء نقلها بالموجات القصيرة من نهاية طرفيه إلى نهاية أخرى، ومثل هذا الالتقاط الذي ثبت إمكانيته عمليا يثير تساؤلا عن مدى صلاحية الإشعاعات والموجات لأن تكون موضوعا للسرقة[3]

وفي هذا الصدد قضت محكمة باريس فيما يتعلق بالاختلاس الناتج عن الالتقاط غير المشروع الوارد بقضية قناة تلفزيونية في فرنسا "Canal+" أن فكرة الاختلاس الناتج لا يوجد فيها اعتداء على العنصر المادي للشبكة المنتجة للبرامج التي تبث بوضوح وتلك التي تبث مشوشة، فقد اعتبرت المحكمة في هذا الحكم أن جريمة السرقة لا تتوافر عناصرها كون التوصيل غير المشروع لالتقاط برامج هذه القناة لم يكن من شأنه أن يغل يد المالك أي صاحب البرنامج، وبذلك تنتفي جريمة السرقة.[4].

1- أمال قارة: الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق ، ص 23.
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق ، ص 573.
3- أمال قارة، ص 26.
4- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 570.

ويلتقي هذا القضاء في نتيجته مع فقه إيطالي راجح يؤيده جانب من الفقه المصري، يرى أن التقاط الموجات الإذاعية والتلفزيونية لا يشكل اعتداءا على الحيازة ولا تقوم به جريمة السرقة وبالتالي فهذه الموجات إذا توافرت لها الصفة المادية بوصفها موجات كهرومغناطيسية إلا أنها لا تصلح لأن تكون محلا للاختلاس لأن ملتقطها لا يستطيع حيازتها، إذ لا تتحقق هذه الحيازة إلا بحرمان جميع أجهزة الاستقبال من استقبالها وهذا الأمر لا يستطيع جهاز عادي تحقيقه، في حين لو حدث واستخدم شخص جهازا يحول كل الإرسال لديه بحيث يحرم من عداه فإن الحيازة تكون في هذه الحالة متحققة وبها تقوم جريمة السرقة.[1]

الصورة الثالثة: نسخ ونقل المعلومة من النظام المعلوماتي

تخزن البيانات المعالجة إلكترونيا على هيئة نبضات كهربائية في دوائر إلكترونية مجمعة أو على أشرطة وأسطوانات ممغنطة وفي الحالتين يمكن نسخها على دعامات أخرى، وبسط أحكام السرقة على عملية الاستنساخ هذه تثير تردد الفقه والقضاء حيال صلاحية خضوع نسخ ونقل المعلومات من النظام المعلوماتي لفعل الاختلاس، وظهر في ذلك اتجاهين:

الاتجاه الأول:

يذهب هذا الرأي إلى نفي قابلية المعلومة للسرقة استنادا على انتفاء الصفة المادية عن المعلومة، وهي صفة يتعين توافرها في المحل الذي تنصب عليه السرقة[2]، وبالتالي لا يمكن أن يتحقق لها ذلك إلا إذا تم إفراغها أو تثبيتها داخل إطار أو دعامة مادية.

كما يرى هذا الاتجاه أن عدم اعتبار نسخ ونقل المعلوماتية اختلاسا مرده أن الجاني لم يستولي على أصل المعلومة ولكنه نقل صورة منها فقط، وبالتالي لا ينطبق عليها وصف السرقة، ومما لا شك فيه أن عدم مشروعية هذا الفعل قد تكيف على أنها تقليد أو سرقة منفعة بشرط وجود نص خاص بذلك، أما بعدم وجود هذا النص فلا يمكن الإقرار بوجود سرقة.[3]

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 27.
2- أمال قارة، ص 25.
3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 568.

وفي هذا السياق ترى الأستاذة Lucas de Leyssac أن محكمة النقض الفرنسية في أحد أحكامها قد أدانت المتهم بالسرقة ليس لقيامه بالتصوير وإنما لاستيلائه على المستند الأصلي أثناء المدة اللازمة لاستنساخه، وبذلك حافظت على شرط توافر الصفة المادية في محل السرقة[1]، أي أن فعل الاختلاس يتمثل في الاعتداء على الأصل مدة الوقت اللازم لتصويره.

الاتجاه الثاني:

يرى أنصار هذا الاتجاه صلاحية نسخ ونقل المعلوماتية من النظام المعلوماتي لأن تكون محلا للاختلاس، و استندوا في ذلك على اعتناق القضاء لمفهوم واسع لجريمة السرقة بحيث يمكن امتداد هذا المفهوم ليشمل بين طياته التجريم والعقاب على سرقة المعلومات وفقا لهذه الصورة، واعتمد أصحاب هذا الرأي في حجتهم على الحكم الصادر من محكمة مونبيليه في قضية بوركان في 26 ماي عام 1978، والذي تتلخص وقائعه في أن أحد المبرمجين قدم استقالته من الشركة التي يعمل بها وانتقل لوظيفة في شركة أخرى أكثر دخلا، وقام بنسخ بعض البرامج التي سبق وأن أعدها في الشركة الأولى، فحكم عليه بجريمة السرقة استنادا على أنه استحوذ على تسجيلات للمعلومات التي أصبحت ملكا للشركة الأولى، وعوقب بالحبس شهرا مع إيقاف التنفيذ وفقا لنص المادة 379 عقوبات فرنسي، ويبرر أصحاب هذا الرأي ذلك أن مفهوم النقل يمكن أن ينطبق على المعلومات واستنساخها وفقا للمفهوم الواسع للنقل، حيث لا يشترط أن يكون مفهوم النقل مرتبط بمادية الجسم، فبالرغم من أن المعلومات ليست ذات جسم مادي محسوس إلا أنه يمكن نقلها وبالتالي فإن الأخذ بالمفهوم الواسع للنقل يتيح تجريمها كوقائع سرقة.[2]

كما يستند هذا الاتجاه في حججه على أن غاية المجرم من اختلاس المعلومة ليس إطارها المادي بل قيمتها الاقتصادية، أضف إلى ذلك فهو يظهر عليها بمظهر المالك الأصلي شرط أن يتبعها بنشاط مادي كبيعها مثلا [3]

2 - Lucas d. leyssac . une information seule est elle suxeptible de vol Dalloz 1988, P34
2- André Lucas , Op.cit., P 530
3 - Lucas d. leyssac . Op.cit. P 43.

وبعد التطرق لأهم الصور التي يتم بها الاختلاس في نطاق المعاملات الالكترونية والتعرض للجدل الفقهي الذي دار في كل صورة من صوره، يمكن جمل ذلك الجدل من خلال طرح إشكال جوهري يتمثل في البحث في مدى خضوع البرامج أو المعلومات بصفة عامة لفعل الاختلاس بغض النظر عن الصورة التي تم بها الجرم.

كان القضاء الفرنسي السباق في التصدي لهذه الإشكالية من خلال تقديمه حلولا عملية يحاول الفقه من خلالها الوصول إلى التأصيل النظري لمواجهة الإشكالية الجوهرية، وأول حكم أصدرته محكمة النقض الفرنسية في هذا الشأن هو حكم لوجاباكس Logabax والذي تتلخص وقائعه في أن أحد مهندسي شركة لوجاباكس فصل من عمله، وفي الدعوى المرفوعة منه ضد رب العمل قدم للمحكمة تأييدا لدعواه صورتين كان قد نسخهما لمستندين من مستندات الشركة أمكنه الحصول عليهما بمناسبة وظيفته السابقة قبل فصله من العمل، وقدم للمحاكمة بتهمة سرقة هذه المستندات، وبرأته محكمة أول درجة وتأيد حكم البراءة في الاستئناف على أساس أن المتهم لم يحمل هذه المستندات إلى منزله على سبيل التملك، ولكن محكمة النقض الفرنسية نقضت الحكم السابق لمخالفته صحيح القانون لان القانون لم يشترط لتحقق الأخذ أو الاختلاس في جريمة السرقة أخذ أو انتزاع الشيء، وأن الاختلاس يمكن أن يتحقق ولو كان الشيء بين يدي الجاني قبل الاستيلاء عليه على سبيل اليد العارضة، ولأن الجاني استولى على المستندين التابعين للشركة المذكورة التي كان يعمل فيها لمصلحته الشخصية بدون علم وبدون رضاء رب العمل المالك لهما أثناء الوقت اللازم لتصويرهما.[1]

وعلى خلاف ذلك ذهبت محكمة استئناف باريس في 1992/11/27 برفض تكييف السرقة على واقعة تتعلق باعتماد المتهم فيها على التصوير لنقل المعلومات، وجاء في حيثيات الحكم أن النقل الذي ينصب على المعلومات فقط دون دعامتها الخارجية ومهما كانت قيمة تلك المعلومات فإنه لا يمكن تطبيق نص المادة 379 عقوبات عليها لأن الاختلاس لا ينصب إلا على الشيء المادي

1 -www.djetfa.info/Vb/showthread.php?t=204052. Le :05/02/2011 à : 15h40mn.

وأن الفعل الواقع في هذه القضية لم يؤدي إلى نقل الحيازة، وأن المعلومات وحدها لا يمكن أن تشكل اختلاسا[1].

وقد انقسم الفقه الفرنسي بمناسبة تعليقه على الأحكام السابقة إلى مؤيد ومعارض لصلاحية الشيء الذي يقع عليه فعل الاختلاس لأن تطبق عليه القواعد التي تحكم جريمة السرقة.

1- الاتجاه القائل بصلاحية المعلومات للاختلاس أو الأخذ:

يذهب أنصار هذا الاتجاه إلى القول بصلاحية المعلومات للاختلاس مستندين على عدة حجج تتلخص في:

- أن المعلومات تصنف ضمن الأموال المعنوية أو اللامادية مثلها في ذلك مثل الكهرباء أو المكالمات الهاتفية، وعلى ذلك فهي تصلح للأخذ أو الاختلاس.[2]

- المعلومات تمثل مال منقول قياسا على سرقة الكهرباء[3] والتي تمثلها النبضات الكهربائية من خلال الأسلاك، حيث يمكن تحديد قيمة وكمية المعلومات المختلفة من خلال الشريط أو الأسطوانة وبالتالي فهي صالحة لأن يرد عليها فعل الاختلاس وبالتالي صالحة كمحل لجريمة السرقة.

- تبدو صلاحية وقوع فعل الاختلاس في حالة البرامج المعلوماتية حيث أنها تشكل خلق فكري وأن ركن الاختلاس سيكون من نفس طبيعة الشيء أي الحيازة الفكرية لهذا الشيء المعلوماتي "البرامج" وبالتالي فإن ورود فعل الاختلاس عليها صحيح.[4]

فالأشياء المعنوية يمكن اختلاسها باختلاس الدعامة التي تحملها كما يمكن اختلاسها استقلالا عن تلك الدعامة حيث يمكن للجاني التقاط بعض المعلومات أو البرامج دون الاستعانة بوساطة مادية، أي من خلال النظر أو السمع، لكن القول بتحقق جريمة السرقة في هذا الفرض

1- Claude Garcin, Lamy droit Pénal des affaires, la fraude informatique, ed 2003, no 502, 204.
2- د/ عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، المرجع السابق، ص 272.
3- ذلك ما قضت به محكمة النقض المصرية من أن وصف المنقول لا يقتصر على ماكان جسما متميزا قابلا للوزن طبقا لنظريات الطبيعة بل هو طبقا لأحكام القانون المدني كل شيء ذي قيمة يمكن تملكه وحيازته ونقله وهذه الخصائص متوافرة في الكهرباء إذ لتيارها قيمة مالية يمكن ضبطه وحيازته ونقله من حيز إلى آخر ومن ثم فلا مجال لإخراج غختلاس الكهرباء من حكم السرقة .راجع في ذلك: د/علي عبد القادر قهوجي، المرجع السابق ، ص87.
4- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 563.

الأخير يؤدي إلى العقاب على ما يدور في الأذهان وذلك ما لا يتماشى مع طبيعة القانون الجنائي[1].

لذلك يذهب أنصار هذا الاتجاه إلى القول بأن الاختلاس يجب أن يتم بنشاط مادي كعملية النسخ أو التصوير التي عن طريقها تنتقل المعلومات من الأصل إلى الصورة، فتشغيل الجهاز يحقق النشاط المادي، فالجاني ليس في حاجة لاستعمال الشيء، فمجرد التشغيل يحقق له النتيجة بالحصول على المعلومةن فرابطة السببية متوافرة بين نشاطه المادي و نتيجته الإجرامية[2]، وبالنسبة للمعلومات التي تم التقاطها ذهنيا فإن الاختلاس لا يتحقق بالنسبة لها إلا إذا وضعت موضع التنفيذ أو تم بيعها أو نقلها إلى الغير على دعامة مادية أو إذاعتها لأن هذا النشاط المادي هو الذي ينتج عنه انتقال المعلومات من ذمة إلى أخرى ويقوم بها الاختلاس.[3]

ويستنتج أنصار هذا الاتجاه القائل بإمكانية وقوع فعل الاختلاس على المعلومة هذه الفكرة من التطور في مفهوم الاختلاس الذي أحدثته نظرية الفقيه Garcon، فجريمة السرقة تقع في كل حالة يحرم فيها مالك أو حائز الشيء ولو لفترة قصيرة من مميزات حق الملكية التي له على الشيء حتى ولو لم يتحرك هذا الشيء من مكانه، ويرون أن الاختلاس ماهو إلا انتقاص لذمة، فإذا كان الشيء المختلس ماديا فإن انتقاص ذمة المجني عليه لا يكون إلا بخروج الشيء من ذمته بنقله أو تحريكه، أما إذا كان الشيء يحتوي على قيمة اقتصادية معنوية مثل البطارية الجافة التي تحتوي على طاقة فإننا لا نكون بحاجة إلى نقل للشيء (البطارية) فسحب الطاقة من هذه البطارية يعني انتقاص الذمة دون نقل الشيء، وقد يقال هنا أن السرقة هي سرقة استعمال [4]، ولكن هذا غير صحيح لأنها لو كانت كذلك لوقعت على البطارية كلها أي على هيكل البطارية وما بداخله من كهرباء وفي حالتنا لم يحدث شيء من ذلك فالبطارية مازالت في مكانها لم تتعرض لأي اعتداء، أي لا يوجد أي انتقاص لها، وبالتالي لا يوجد اختلاس لهيكل البطارية، وإنما الاختلاس وقع على الطاقة فهي التي خرجت من ذمة مالكها، وهذا هو الذي اتجهت إليه محكمة النقض الفرنسية للقول بتوافر

1- د/ علي عبد القادر القهوجي، المرجع السابق، ص 98.
2 -www.djetfa.info/Vb/showthread.php?t=204052. Le :05/02/2011 à : 15h40mn.
3- د/ علي عبد القادر القهوجي، ص 98.
4- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 40.

جريمة السرقة بالنسبة للشرائط وسرقة المحتوى المعلوماتي وذلك من خلال المدة اللازمة لنسخ هذه المعلومة.[1]

وبنقل ذلك المعنى إلى مجال البرامج أو المعلومات فإن نسخ البرنامج من دعامته دون نقل لها ودون خروجها من المكان الذي توجد فيه دون رضاء صاحب الحق عليها لا يعني بأن فعل الاختلاس في هذه الحالة قد وقع على الدعامة أو الأصل، إذ الفرض أنه لم ينتقل و لم ينقص منه شيء، وإنما يكون هذا الفعل قد وقع من خلال عملية التصوير أو النسخ على المعلومات التي يحتويها الأصل أو الدعامة وأدى إلى انتقالها من خلال الأصل أو تلك الدعامة إلى الصورة، أي من ذمة إلى ذمة أخرى، ولكن يلاحظ هنا على عكس الطاقة أن المعلومات مازالت بين يدي مالكها وتحت سيطرته إلا أن قيمتها قد نقصت بفعل الاختلاس لأن صاحبها يكون في هذه الحالة قد فقد حقه في احتكار استغلالها[2].

وهكذا ينتهي أصحاب هذا الاتجاه إلى القول بصلاحية وقوع الأخذ أو الاختلاس على برامج الحاسب والمعلومات بصفة عامة مستقلة عن دعامتها الأصلية، حيث يتم نسخها وهي في مكانها، واستطرادا مع هذا الاتجاه فإن جريمة السرقة تقع على المعلومات فقط سواء تم النسخ مباشرة أم عن بعد وذلك عن طريق طرفيه متصلة بالحاسب المركزي وسواء كانت هذه الطرفية سلكية أو لاسلكية.

2- الاتجاه القائل بعدم صلاحية المعلومات للاختلاس أو الأخذ

يستبعد هذا الاتجاه أن تقع جريمة السرقة على البرامج والمعلومات مستقلة عن دعامتها نظرا للطبيعة غير المادية للمعلومات على خلاف الاختلاس الذي يعتبر ذو طبيعة مادية، كما أن المعلومات على خلاف الطاقة تبقى بين يدي صاحبها على الرغم من حصول الجاني عليها في حالة نسخها، فعلى الرغم من أن المعلومات مال إلا أنها مال يتميز عن غيره من الأموال بالخصائص الثلاثة التالية:

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 40.
2- د/ علي عبد القادر القهوجي، المرجع السابق، ص 101.

- أنها مال يمكن استعماله بواسطة أطراف عديدة في نفس الوقت دون أن يفقد قيمته فالمعلومات لا تتغير باتساع نطاق استخدامها.
- أنها مال غير قابل للنفاذ بمعنى أنه لا ينفذ بالاستعمال ولا يفقد قيمته إلا بالنسيان أو بظهور معارف جديدة.
- نفقة نقل هذا المال من طرف لآخر ضئيلة للغاية ولا تقارن بنفقة إنتاجه[1].

ونظرا لهذه الخصائص التي يتسم بها المال المعلوماتي فإنه لا يستطيع أن يكون محلا لجريمة الاختلاس على حسب رأي هذا الاتجاه مستندين في ذلك على حجج رئيسية تتمثل في:

- عدم توفر صفة المنقول في المعلومة: ذلك أن الاختلاس في مجال المعاملات الالكترونية لا يتم إلا إذا كانت المعلومات مدونة على دعامة مادية، وإن لم يكن كذلك فالأمر يتعلق بخدمات وليس بأموال، وعليه فإذا قام صاحب المعلومة ببثها عبر شبكة معينة وقام شخص آخر باعتراضها بوسيلة أو بأخرى كاستعمال كلمة السر مثلا بطريق الغش فإن الأمر لا يتعلق بسرقة أو نصب، ويرجع ذلك إلى عدم توفر صفة المنقول في المعلومات محل البث [2]، فالمعلومات المخزنة في النظام المعلوماتي لا تعتبر منقولا لأنه لا يتصور انتزاعها وحيازتها[3]

أي لا يمكن انتزاعها من صاحبها بشكل يفقده تملكها كما في الأشياء المادية.

- وقوع فعل الاختلاس لا يتم على المعلومة بل على الأصل: حيث أن هذا الفعل يتمثل في الاستيلاء على الأصل مدة الوقت اللازم لتصويره، وأن الجاني في هذه الحالة يتوافر في حقه سرقة استعمال لهذا الأصل حتى ولو كان هذا الاستيلاء لم يستمر فترة طويلة من الزمن، ويستند أنصار هذا الرأي إلى ما استقر عليه التطور القضائي بشأن سرقة الاستعمال وبصفة خاصة استعمال السيارات، ففي هذا النوع من السرقة لا يشترط قضاء محكمة النقض الفرنسية أن يكون الاستيلاء على السيارة قد تم على سبيل التملك وإنما يكتفي بأن يكون لهذا الاستيلاء أحد مظاهر الملكية على الشيء، حتى ولو كان لفترة قصيرة ثم عاد الشيء بعدها إلى مالكه لأن الجاني في تلك الفترة

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 42.
2- د/ عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، المرجع السابق، ص 271.
3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 532.

كان يبدو مثل المالك الذي يستعمل سيارته، وقد اضطر القضاء الفرنسي أمام انتشار ظاهرة الاستيلاء على السيارات لاستعمالها ثم إعادتها إلى مكانها أو أي مكان آخر أن يعطي مفهوما موسعا للاختلاس والقصد الجنائي في جريمة السرقة، حيث يستطيع ملاحقة هذه الأفعال التي لم يتدخل المشرع لتجريمها بنص خاص وانتهى به هذا التطور إلى التسليم بوقوع هذه السرقة (سرقة الاستعمال) على الدعامة التي تحتوي على البرامج والمعلومات على الوقت اللازم لتصويرها مهما كان قصيرا، وإن لم يصل به هذا التطور إلى درجة القول بوقوع السرقة على المعلومات وحدها واستقلالا.[1]

- وقوع فعل الاختلاس لا يتم على المعلومة بل على الآلة: ذهب بعض الفقه المناهض لفكرة خضوع المعلومة لفعل الاختلاس إلى القول أن هذا الأخير يتم على الآلة التي توجد بها المعلومة، فالسرقة لا تقع على الأصل بل على وقت الآلة أي أن هذا الرأي يعتبر أن فعل الاختلاس وقع على آلة الحاسوب ذاتها وأن هذا الفعل يتمثل في الاستيلاء عليها ولو لوقت قصير جدا وهو الوقت اللازم لنسخ صور للبرامج أو المعلومات الأصلية من خلالها [2]، فسرقة وقت الحاسوب تعد بمثابة سرقة عادية قياسا على سرقة السيارة واستعمالها دون إذن صاحبها وكذلك سرقة التيار الكهربائي[3]

وحسب هذا الاتجاه فجريمة السرقة لا تقع في الحالات السابقة لأن طبيعة البرنامج والمعلومات تأبى تحقق الأخذ أو الاختلاس لمعناه الدقيق المسلم به في جريمة السرقة والذي يعني الاستيلاء على الحيازة الكاملة للشيء دون رضا صاحبه أو حائزه السابق.[4]

بتحليل الحجج التي جاء بها هذا الاتجاه يمكن القول أنها حجج غير كافية للقول بعدم صلاحية المعلومة للاختلاس، فهي لا تقر ذلك صراحة حيث تعترف بوقوع الاختلاس لكن ليس على المكونات المنطقية للنظام بل إما على الأصل أو على الآلة أو وقتها.

1- د/ علي عبد القادر القهوجي، المرجع السابق، ص 102.
2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 43.
3- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها الإلكترونية، المرجع السابق، ص 177.
4- أمال قارة، ص 44.

فالقول أن الاختلاس يقع على الأصل لا على المعلومة هو في الحقيقة تهرب من الإقرار بوقوعه على المعلومة، ذلك أن الاعتماد في هذه الحجة على القياس بسرقة السيارات لاستعمالها في أغراض غير مشروعة ثم إعادتها هو قياس غير مقبول في نظرنا لأن سرقة السيارة ثم إعادتها يكون الغرض منه دائما هو غرض مادي كاستعمالها في سرقة أخرى... بينما سرقة المستند الأصلي الغرض منه هو غرض معنوي يتعلق باختلاس المعلومة، وعلى ذلك فإنه لا يمكن قياس سرقة السيارات بسرقة المستندات الأصلية.

أما القول أن الاختلاس لا يتم على المعلومة بل على الآلة أو وقتها فهو أمر محسوم في نظرنا ذلك أن الاعتداء على الآلة من خلال سرقة وقتها لا يتأتى في أغلب الأحيان إلا من خلال الدخول أو البقاء غير المشروع داخل النظام المعلوماتي وبالتالي فهو يخضع لنص المادة 394 مكرر من قانون العقوبات الجزائري أو المادة 323 من قانون العقوبات الفرنسي، ومن ثم فإنه لا مفر من ضرورة التسليم بأن الاختلاس لا يكون إلا على المعلومة وبالتالي فهي تخضع للنشاط الإجرامي لجريمة السرقة.

وبتحقق النشاط الإجرامي أي الركن المادي لجريمة السرقة تجدر الإشارة إلى عنصر مهم يعد ميزة لجريمة السرقة عن الجرائم الأخرى ألا وهو عنصر التسليم، حيث لا يتحقق الاختلاس إذا استلم الجاني المال من مالكه صاحب الحيازة الكاملة أو تسلمه من حائزه أي صاحب الحيازة الناقصة تسليما تتحقق به الحيازة وليس مجرد اليد العارضة، فإذا صدر التسليم من غير ذي صفة أي من غير المالك أو الحائز فلا قيمة لهذا التسليم في نفي الاختلاس وكذلك إذا استعان الجاني بآلة للحصول على الشيء، ولما كانت الحيازة هي ملكية أو سلطة مباشرة للحائز على الشيء فإن التسليم الذي يقع ممن له اليد العارضة على الشيء لا ينفي الاختلاس باعتبار أنه يكون في حكم الآلة[1]، فمتى تحقق النشاط الإجرامي أي انتقال المال المعلوماتي إلى الجاني دون رضا صاحبه يكون الركن المادي قد اكتمل ووجب بعدها البحث فيما مدى توافر الركن المعنوي للقول باكتمال جريمة السرقة في نطاق المعاملات الالكترونية من عدمه.

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 584.

ثانيا/ الركن المعنوي لجريمة السرقة في نطاق المعاملات الإلكترونية :

الركن المعنوي لجريمة السرقة في ضوء القواعد العامة يتخذ صورة القصد الجنائي، هذا الأخير الذي يتكون من عنصري العلم والإرادة، أي أن يعلم الجاني بأنه يستولي على منقول مملوك للغير بدون رضاه وأن تتجه إرادته إلى فعل الاختلاس.[1]

ولا يكفي هذا فقط أي إلى جانب العلم والإرادة (القصد العام) يجب توافر القصد الخاص و الذي لا يتوافر في حق المتهم بهذه الجريمة إلا إذا توافرت لديه نية السرقة [2] أي نية تملك الشئ والذي لا يتحقق إلا بتوفر القصد العام

أي أن هناك علاقة ترابط بين القصد العام والقصد الخاص حيث لا يكتمل عنصر إلا بتوافر الآخر، كما يجب في الركن المعنوي أن يعاصر القصد الجنائي السلوك الإجرامي، ولا أثر للباعث أو الغاية على توافر القصد الجنائي، فيقوم هذا الاخير بغض النظر عن الباعث من وراء السرقة، وكذلك لا أثر للغاية على نفي القصد الجنائي وبالتالي تقوم جريمة السرقة إذا توافرت بقية أركانها حتى ولو كان الباعث على الاختلاس شريفا في ذاته وعلى سلطة الاتهام عبء إثبات توافر القصد الجنائي العام والخاص لدى الجاني.

هذا فيما يتعلق بالركن المعنوي لجريمة السرقة في ظل القواعد العامة وهو نفسه في نطاق المعاملات الإلكترونية وفقا للتفصيل الآتي:

1/ القصد العام:

يقوم القصد العام في جريمة السرقة في نطاق المعاملات الإلكترونية على عنصرين شأنه في ذلك شأن القصد العام في ضوء القواعد العامة وهما العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى الاستيلاء على المعلومات المسجلة إلكترونيا سواء المعلومات المخزنة داخل النظام المعلوماتي أو

1- د/ علي عبد القادر القهوجي، شرح قانون العقوبات، القسم الخاص، الكتاب الثاني، دار المطبوعات الجامعية، الإسكندرية1999، ص 277.
2- حسين فريجة، المرجع السابق، ص 200.

المعلومات المسجلة إلكترونيا والمخزنة على دعامة خارجية مثل الأسطوانات والشرائط الممغنطة مع علمه بأن المعلومات محل السرقة ليست ملكا له[1]

فإذا قام شخص بأخذ قرص ممغنط يحتوي على برامج معلوماتية واختلسه من صاحبه، ثم قام بتشغيله لمعرفة محتواه ثم رده فإن إرادة الاختلاس تنتفي لديه ويتخلف القصد العام عنده[2].

أما العلم فيتجسد عند معرفة الجاني بأنه يستولي على معلومات ليست ملكا له، أما حال الخطأ بالاعتقاد أن المعلومات أو البرنامج أو الدعامة هي ملك له ثم تبين له العكس وقام بإرجاعها فلا يتحقق هذا العنصر، فالقصد العام يتوافر بعنصريه العلم والإرادة في مجال المعاملات الالكترونية عند اتجاه إرادة الجاني إلى الاستيلاء على المعلومات مع علمه بملكية الغير لها.

2/ القصد الخاص:

كما سبق القول فالسرقة جريمة عمدية يفترض لإثباتها توافر قصد جنائي خاص وهو الذي يعبر عن نية التملك لأنها هي التي تكشف عن نية الجاني في حيازة الشيء المعلوماتي ويستدل على توافر القصد من القرائن والظروف، ونية التملك التي تتجه إليها إرادة الجاني هي عنصر يضاف إلى عنصري القصد العام (العلم والإرادة) فبالإضافة إلى ضرورة اتجاه الإرادة إلى اختلاس الشيء المعلوماتي مع علم الجاني أنه يختلس شيئا مملوكا للغير يضاف إليهما نية الاستحواذ على الشيء المسروق [3] ، فانتفاء نية التملك ينفي جريمة السرقة لذلك يرى بعض الفقهاء أنه يتعين عدم الخلط ين مجرد الانتفاع بالشيء دون حق وبين سلب قيمته، ويقصد بسلب قيمة الشيء الحالة التي يستولي بها الشخص على شيء مملوك لغيره بنية استعماله على نحو يجرده من قيمته كلها أو بعضها ثم رده بعد ذلك إلى صاحبه، فقصد الجاني هنا هو استتراف قيمة الشيء كلها أو بعضها بحيث إذا أعيدت بعد ذلك كان عديم القيمة أو ناقصها فينبغي أن يعد فعله سرقة لأن القانون إنما يحمي الأشياء لأنها تمثل قيمة معينة فتكون العبرة في نظره بقيمة الشيء لا مادته، بحيث إذا استولى

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 609.
2- د/ خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، المرجع السابق، ص 105.
3- د/ خالد ممدوح إبراهيم، ص 167.

الشخص على شيء مملوك لغيره بغير رضائه أو استتراف قيمته كلها أو بعضها فإن اتجاه نيته وقت الاستيلاء عليها إلى رده لصاحبه لا يحول دون اعتبار فعله اختلاسا محققا لجريمة السرقة.[1]

والقول بهذا الرأي الأخير يتجسد تماما في مجال المعاملات الالكترونية حيث أن نية التملك لا تخرج الشيء كلية من عند صاحبه بل تنقص قيمته المعنوية أو الاقتصادية حيث يفقد صاحب المعلومة حق الاستئثار بها، والقصد الخاص في أغلب جرائم المعلوماتية يسهل إثباته لأن نية التملك في نطاق المعاملات الالكترونية في أغلب الجرائم يسبقها الدخول أو البقاء داخل النظام المعلوماتي وهو جرم معاقب عليه بنص المادة 323 عقوبات فرنسي ونص المادة 394 عقوبات جزائري، فمتى تحقق اختراق النظام المعلوماتي أو البقاء فيه فما ذلك إلا تفسير لسوء نية الجاني ويعتبر كدليل إثبات، ذلك أن الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه هو بوابة لوقوع جرائم أخرى كالسرقة والنصب وخيانة الأمانة.

بعد هذا التفصيل لجريمة السرقة في نطاق المعاملات الالكترونية يجدر بنا الوقوف على النقاط الرئيسية التي كانت موضوع جدل في هذه الجريمة، ذلك أن جريمة السرقة تثير مشاكل أكثر من غيرها من الجرائم، فضلا عن أن الحلول بشأنها تعتبر القاعدة العامة بالنسبة للجرائم الأخرى فمن بين الإشكالات الرئيسية التي اعترضت تطبيق نصوص التجريم الكلاسيكية على السرقة المعلوماتية القول بأن تطبيقها مخالف لمبادئ التفسير ومخالف لمبدأ المشروعية، لكن الأخذ بذلك يصطدم بالتطور الهائل في مجال المعاملات الالكترونية الذي خلق أنواع جديدة من الجرائم والتي يصعب أن تطالها النصوص الحالية، ولكن حفاظا على المصلحة العامة والخاصة ولكي لا يفلت المجرم من العقاب يجب تطبيق القواعد العامة التي تحكم جريمة السرقة إلى أن يصدر تشريع خاص بها.

كما أن تطبيق القواعد العامة ليس خروجا على مبدأ المشروعية، ذلك أن نص المشرع الجزائري أو الفرنسي جاء موسعا حيث أن كلمة "شيء" يدخل في مدلولها الشيء المادي أو المعنوي فمن باب أولى فهمها فهما واسعا أو فهما إيجابيا ذلك أن هذا الفهم يدخل في دائرته

1- جهاد رضا الحباشنة، الحماية الجزائية لبطاقات الوفاء، دار الثقافة، عمان 2008، ص .100

العقاب على أي اختلاس، كما أن القول بعدم صلاحية تطبيق القواعد العامة التي تحكم جريمة السرقة لأنها تشترط أن يكون محل السرقة منقولا وإن هذا الأخير لا يتوفر في المعلومة هي حجة لا يمكن التسليم بها في نظرنا لأن المعلومات سلعة لها قيمة تباع وتشترى فالكهرباء ليست منقولا ماديا لكن الاعتداء عليها مجرم قانونا والمعلومة والكهرباء ينتهيان إلى نتيجة واحدة وهي التجسد في شيء مادي.

كما أن التحجج بأن المال المعلوماتي غير قابل للحيازة وبالتالي غير قابل للسرقة، هي حجة تجافي المنطق ذلك أن التسليم بها يعني تجريد المال المعلوماتي من الحماية الجنائية ما يجعله عرضة للاعتداء، فالملاحظ على كل الحجج التي جاء بها الاتجاه المناهض لإضفاء وصف المال على المكونات المعنوية للنظام المعلوماتي سواء بعدم قابليته للحيازة أو عدم اعتباره منقولا أو القول أن إضفاء وصف المال على المعلوماتية فيه إهدار لمبدأ المشروعية أو لمبادئ التفسير التي تحكم النصوص العقابية، هي حجج مقبولة نسبيا لكن الأقرب للمنطق ألا يتم الأخذ بها كونها حجج يؤدي العمل بها إلى إعاقة المعاملات الإلكترونية التي تحقق لها الحماية القانونية الأرضية الخصبة لتجسيد نتائجها الإيجابية، أضف إلى ذلك فإن استعانة القاضي الجنائي بالنصوص التقليدية فيه حماية للصالح العام والقول بعكس ذلك فيه حماية لمجرمي المعلوماتية.

ومما سبق يمك القول بضرورة تطبيق القواعد العامة التي تحكم السرقة على تلك التي تقع في مجال المعاملات الإلكترونية دون أن يكون في ذلك أي إخلال بالمبادئ العامة التي تحكم القانون الجنائي.

المطلب الثاني

مدى تحقق الحماية الجنائية للمعاملات الالكترونية وفقا للقواعد العامة المقررة لجريمة النصب

تعرض قانون العقوبات الجزائري لجريمة النصب في المادة 372 حيث نص على:" كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو الحصول على أي منها أو شرع في 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 في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 دج.

وإذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد إصدار أسهم أو سندات أو أذونات أو حصص أو أية سندات مالية سواء لشركات أو مشروعات تجارية أو صناعية فيجوز أن تصل مدة الحبس إلى عشر سنوات والغرامة إلى 200.000 دج وفي جميع الحالات يجوز أن يحكم علاوة على ذلك على الجاني بالحرمان من جميع الحقوق الواردة في المادة 14 أو من بعضها بالمنع من الإقامة وذلك لمدة سنة على الأقل وخمس سنوات على الأكثر"[1]

فالنصب هو الاستيلاء على الحيازة الكاملة عمدا بطريق الحيلة أو الخداع على مال مملوك للغير.

ويظهر من هذا التعريف أن جريمة النصب تتفق مع جريمة السرقة في أن كلا منهما تنطوي على اعتداء على ملكية الغير وأن هذا الاعتداء يهدف إلى تملك المال المستولى عليه إلا أنهما يفترقان من حيث النشاط الإجرامي، إذ يتمثل هذا النشاط في جريمة النصب في فعل الاحتيال أو الخداع الذي يؤثر على إرادة المجني عليه فيوقعه في غلط يدفعه إلى تسليم المال إلى النصاب بينما في جريمة السرقة هو الاستيلاء على المنقول بدون رضاء المالك أو الحائز السابق، وبعبارة أخرى فإن النصاب

1- حسين فريجة، المرجع السابق، ص251

يتسلم المال من المجني عليه برضا هذا الأخير وإن كانت إرادته مشوبة بغلط بينما يستولي السارق على المال خلسة أو بدون رضا مالكه أو حائزه السابق[1] .

وما تجدر الإشارة إليه أن المشرع الجزائري لم يتطرق إلى النصب الواقع في مجالات المعاملات الإلكترونية مثله في ذلك مثل المشرع الفرنسي، إلا أن هذا الأخير كان تعريفه لجريمة النصب أوسع حيث نص في المادة 313- 1 قانون العقوبات[2] بأنه " واقعة خداع شخص طبيعي أو معنوي سواء باستعمال اسم كاذب أو صفة كاذبة أو التعسف في صفة غير صحيحة أو باستعمال حيلة تدليسية من شأنها حمل الغير على تسليم أموال أو قيمة أو مال ما أو تقديم خدمة أو الموافقة على عمل ينتج عنه التزام أو تحرر من التزام"[3].

فنص المشرع الفرنسي جاء أوسع من حيث محل جريمة النصب حيث جعل الخدمات مساوية للمال الذي يمكن تسليمه في هذه الجريمة، بمعنى أن الخدمات قد تكون موضوعا للتسليم في جريمة النصب، كما أن المشرع الفرنسي على خلاف المشرع الجزائري جاء بمصطلح قيمة والتي تستوي في نظرنا أن تكون قيمة مادية أو معنوية ذلك أن نص المادة 313 جاء على الشكل التالي: "... أموال أو قيمة ..."، فبغض النظر عن الجدل الذي تطرقنا له عن الأموال في مدى اعتبارها مادية أو معنوية فتبدو رغبة المشرع الفرنسي واضحة من خلال اتباع مصطلح الأموال بمصطلح قيمة فلا تخرج هذه الأخيرة من اعتبارها قيمة معنوية لأن الأشياء ذات القيمة المادية تدخل في نطاق مصطلح الأموال .

وقبل التطرق لمدى تحقق الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد العامة المقررة في جريمة النصب يجدر بنا التطرق أولا لتعريف النصب المعلوماتي كي يمكن الحديث عن محل

1- د/ علي عبد القادر القهوجي، شرح قانون العقوبات، القسم الخاص، المرجع السابق ص 323

2- art 313/ « l'escroquerie est le fait; soit par l'usage d'un faux nom ou d'un fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, a son préjudice d'un tiers, a remettre des fonds, des valeurs ou un bien quelconque a fournir un service ou consentir un acte apérant obligation ou décharge
l'escroquerie est puni de cinq ans d'emprisonnement et de 75000 euros d'amande ». code pénale français.

3- د/ محمد عبيد الكعبي، المرجع السابق، ص 611.

وأركان هذه الجريمة في مجال المعاملات الإلكترونية، والذي عرفه بعض الفقه بأنه " كل سلوك احتيالي يرتبط بعملية التحسب الإلكتروني بهدف كسب فائدة أو مصلحة مالية "[1].

وهذا التعريف يشمل كل ضروب غش الحاسوب والمتمثلة في الاعتداء على المعطيات المخزنة في النظام المعلوماتي والمتبادلة عبر قنوات النظام بما تمثلها من أموال وخدمات بغرض الحصول على منفعة مادية .

وبعد إعطاء تعريف للاحتيال المعلوماتي يمكننا الآن البحث في ما مدى تحقق حماية المعاملات الإلكترونية وفقا للقواعد العامة لجريمة النصب، وذلك من خلال التطرق لكل من محل وأركان هذه الجريمة وذلك على الشكل التالي:

الفرع الأول: محل جريمة النصب في نطاق المعاملات الإلكترونية.

الفرع الثاني: أركان جريمة النصب في نطاق المعاملات الإلكترونية.

1- محمد أمين الشوابكة، المرجع السابق ،ص180

الفرع الأول: محل جريمة النصب في نطاق المعاملات الإلكترونية

محل النصب هو ما يتوصل الجاني إلى الاستيلاء عليه من المجني عليه عن طريق الاحتيال، وقد حدد المشرع الجزائري المحل بأنه "نقود أو منقولات أو سندات دين أو سندات مخالصة أو أي متاع آخر"، فمحل النصب هو مال منقول [1]

ويشترط في المال موضوع الاحتيال أن يكون شيئا له صفة المال ويكون للشيء صفة المال متى كان صالحا لأن يكون محلا لحق الملكية، كما يشترط في المال موضوع الاستيلاء أن يكون ماديا لأن الشيء المادي هو الذي يقبل الحيازة والتسليم والاستيلاء[2].

كما يشترط في المال محل النصب أن يكون مملوكا لغير المتهم، فالنصب اعتداء على ملكية الغير وبالتالي لا يعد نصبا من أخذ مالا مملوكا له أو كان مالا مباحا أو متروكا، وذلك ما أشار إليه المشرع الجزائري في نص المادة 372 عقوبات بقوله أن الاحتيال الصادر عن المتهم يكون بهدف سلب ثروة الغير أو بعضها[3].

هذا فيما يتعلق بمحل جريمة النصب وفق القواعد العامة، وبتطبيقه في مجال المعاملات الالكترونية فإنه ينصرف إلى المكونات المادية للنظام المعلوماتي والتي لا تثير أي إشكال في مدى صلاحيتها لأن تكون محلا لهذه الجريمة، فالمكونات المادية للنظام المعلوماتي كشاشات العرض ولوحة المفاتيح وأجهزة الإدخال والإخراج ماهي إلا مال منقول مملوك للغير، كما أن المعلومات يمكن أن تكون محلا لجريمة النصب وفق القواعد العامة شريطة أن تكون مثبتة على دعامة مادية حيث ينصرف محل الجريمة إلى هذه الدعامة.

وبالتسليم أن محل جريمة النصب في نطاق المعاملات الالكترونية هو المكونات المعنوية للنظام المعلوماتي وهو نفسه محل جريمة السرقة المعلوماتية فإننا نكون بصدد إشكال جوهري في هذا الفرض، وهو كيفية تكييف التلاعب في المعلومات والبرامج والأموال التي يتم تداولها في نطاق المعاملات الإلكترونية والتي تعتبر محلا لهذه الجريمة وتكون دائما عرضة للاحتيال المعلوماتي خاصة

1- حسين فريجة، المرجع السابق، ص 252.
2- د/ علي عبد القادر القهوجي، شرح قانون العقوبات القسم الخاص، المرجع السابق، ص 353.
3- حسين فريجة، ص 255.

المتعلقة منها بالمستحقات المالية وبطاقات الائتمان وأوامر الدفع إلى غير ذلك من التعاملات الإلكترونية.

فهل يمكن القول أن المكونات المعنوية للنظام المعلوماتي باعتبارها محلا لجريمة النصب في نطاق المعاملات الإلكترونية تصلح لأن تكون محل لهذه الجريمة وفقا للقواعد العامة؟ وبصيغة أكثر دقة ما مدى إمكانية تطبيق القواعد العامة لجريمة النصب على النصب المعلوماتي؟

للإجابة على هذه الإشكالية يستوجب علينا التطرق للاتجاهات الفقهية التي ظهرت في هذا الفرض:

الاتجاه الأول:

يرى هذا الاتجاه صلاحية المعلومات والبرامج المعالجة آليا لأن تكون محلا أو موضوعا لجريمة النصب وفقا للقواعد العامة، وتبنى هذا الاتجاه بعض من الفقه الفرنسي والدول الأنجلوساكسونية منها بريطانيا واستراليا وكندا، وهذا الاتجاه يوسع من نطاق تطبيق النصوص المتعلقة بالعقاب على جريمة النصب ويسمح بتطبيق هذه النصوص على النصب المعلوماتي[1]، ولقد تدخل المشرع الإنجليزي عام 1983 واعتبر خداع الآلة بنية ارتكاب غش مالي هو من قبيل الاحتيال الذي يجب العقاب عليه جنائيا، وبذلك تطبق نصوص تجريم النصب على ذلك الغش أو الاحتيال بطرق معلوماتية، وقد سار على ذلك النهج كل من القضاء الكندي والأسترالي[2]

كما يرى هذا الاتجاه أن خداع النظام المعلوماتي لسلب مال الغير تتحقق به الطرق الاحتيالية المشار إليها في القواعد العامة لقانون العقوبات ككذب تدعمه أعمال مادية أو وقائع خارجية، حيث يتوافر بالإضافة إلى الكذب واقعة خارجية تسانده وهي إبراز أو تقديم المستندات المعلوماتية التي تدخل النظام المعلوماتي.

وزيادة على ذلك فالمعيار الأساسي لجريمة النصب يتمثل في المحاولة التدليسية، وذلك باستخدام أساليب فنية من قبل الجاني أثناء تشغيل، الجهاز ويرجع ذلك إلى الطبيعية الذاتية الخاصة لهذه الجريمة في نطاق المعاملات الالكترونية، ففي النصب المعلوماتي تتوافر الخبرة الفنية وتتنوع

1- د/ محمد عبيد الكعي، المرجع السابق، ص 603.

2 -www.djetfa.info/Vb/showthread.php?t=204052. Le :05/02/2011 à : 15h40mn.

الأساليب التكنولوجية في خداع النظام المعلوماتي وكيفية الحصول على الهوية واختلاسها وانتحال صفة صاحبها للحلول محله في العمليات الإلكترونية، وباختلاس الهوية يمكن الحصول على المستخرجات ونتائج العمليات الأولية، و يضيف أن الطبيعة المعلوماتية لجرائم الحاسب الالي لا تضيف جديدا في مجال النصب التقليدي إلا مجرد الوسيلة المستخدمة،[1] كما يدعم هذا الاتجاه رأيه بحكم محكمة النقض الفرنسية حيث طبقت عقوبة النصب على شخص وضع قطعا معدنية بدل قطعة النقود في عداد أماكن الانتظار وترتب على ذلك تشغيل الماكينة، واعتبرت المحكمة هذا الفعل من قبيل الطرق الاحتيالية[2]

وتجدر الإشارة إلى أن موقف هذا الاتجاه مرده أن البلدان التي تتبنى النظم القانونية ذات الاتجاه الأنجلوساكسوني توسع من نطاق نصوص جريمة النصب حتى تتسع وتطبق على عمليات النصب المعلوماتي، مثل بريطانيا واستراليا وكندا، ولعل القضاء في هذه البلدان لم يحاول الخروج على نصوص القانون التي وضعت بذاتها لتجريم النصب المعلوماتي[3].

الاتجاه الثاني: يرى أنصار هذا الاتجاه أن جريمة النصب لا تقوم إلا إذا خدع شخص شخصا مثله وأن يكون الشخص المخدوع مكلفا بمراقبة البيانات، وعلى ذلك لا يتصور خداع الحاسب الآلي بوصفه آلة ومن ثم لا يطبق النص الجنائي الخاص بالنصب والاحتيال لافتقاره أحد العناصر اللازمة لتطبيقه، وهذا الاتجاه تتبناه تشريعات: مصر وألمانيا والدانمرك وفنلندا واليابان والنرويج والسويد ولكسمبورغ وإيطاليا[4].

وذلك ما يمكن استنتاجه من نصوص المشرع الجزائري كونه لم يستحدث نصوصا تتعلق بالنصب المعلوماتي وبالتالي فهو يساير هذا الاتجاه التقليدي.

الاتجاه الثالث: وتمثله الولايات المتحدة الأمريكية، حيث تطبق النصوص المتعلقة بالغش في مجال البنوك والبريد والتلغراف والاتفاق الإجرامي لغرض الغش على حالات النصب المعلوماتي.

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 645.
2- د/ شيماء عبد الغني محمد عطا الله ، المرجع السابق ص 61
3- د/ عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، المرجع السابق، ص 309- 310.
4- د/ محمد عبيد الكعبي، المرجع السابق، ص 602.

بل إن بعض القوانين المحلية في بعض الولايات الأمريكية أصدرت قوانين في هذا الخصوص وأضافت تعريفا موسعا للأموال بأنها "كل شيء ينطوي على قيمة" ومن ثم يندرج تحت تعريف الأموال المذكور كل من الأموال المعنوية والبيانات المعالجة، حيث تعاقب هذه القوانين على الاستخدام غير المسموح به للحاسب الآلي بغرض اقتراف أفعال الغش أو الاستيلاء على الأموال[1]

ومما سبق نخلص إلى أن محل جريمة النصب في مجال المعاملات الالكترونية هو المكونات المعنوية للنظام المعلوماتي، أو كل ما يتم تبادله في تلك المعاملات من معلومات وبيانات وأموال.... هذا من جهة، أما عن إمكانية خضوع المكونات المعنوية للنظام المعلوماتي للقواعد العامة التي تحكم جريمة النصب فيلاحظ أن الاتجاهات الفقهية السابقة جاءت موافقة لتشريعاتها الداخلية فليس هناك خلاف حول تفسير النصوص التي جاءت بها تشريعاتها .

الفرع الثاني:أركان جريمة النصب في نطاق المعاملات الإلكترونية

لتناول أركان جريمة النصب في نطاق المعاملات الإلكترونية نتطرق لمدى خضوع المكونات المعنوية للنظام المعلوماتي للنشاط الإجرامي في جريمة النصب، أي الركن المادي لهذه الجريمة ثم نتناول بعد ذلك الركن المعنوي لها.

أولا: مدى خضوع المكونات المعنوية للنظام المعلوماتي للنشاط الإجرامي في جريمة النصب

النشاط الإجرامي في جريمة النصب هو الاستيلاء على الحيازة الكاملة لمال مملوك للغير عن طريق إحدى وسائل الاحتيال المحددة في القانون على سبيل الحصر[2]

وفي نطاق المعاملات الإلكترونية يمكن القول أنه متى توصل الجاني إلى الاستيلاء على دعامات مادية تحتوي على معلومات تخص صاحبها، وكان ذلك الاستيلاء بالطرق المنصوص عليها قانونا، فإن جريمة النصب في نطاق المعاملات الالكترونية تتحقق وتخضع للقواعد العامة.

1- www.Arablawinfo.com . Le ;20/01/2011, a; 21h00mnt
2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 45.

وطرق التدليس التي جاء بها المشرع الجزائري هي:

1. استعمال طرق احتيالية.
2. أن تتخذ الأكاذيب نطاق معين يؤدي إلى التصرف في مال أو منقول ليس ملكا للجاني.
3. اتخاذ اسم كاذب أو صفة غير صحيحة[1]

والطرق الاحتيالية تكاد لا تدخل تحت حصر لكن المهم فيه أن يكون من شأنها خداع المجني عليه وحمله على تسليم المال.

ويكفي لتكوين جريمة النصب أن يتسمى الجاني باسم كاذب يتوصل به إلى تحقيق غرضه دون حاجة إلى الاستعانة لإتمام جريمته بأساليب احتيالية أخرى[2].

فهل يمكن تحقق جريمة النصب وفقا للوصف السابق على المكونات المنطقية للنظام المعلوماتي؟

هذا الإشكال يتمخض عنه سؤالين رئيسيين يتمثل الأول فيما مدى صلاحية النظام المعلوماتي لأن يكون محلا للطرق التدليسية المنصوص عليه قانونا؟ وقد تم التفصيل في هذا الإشكال عند التطرق لمحل جريمة النصب في نطاق المعاملات الإلكترونية.

أما الإشكال الثاني فيتمحور حول مدى إمكانية تطبيق فكرة الاستيلاء في مجال المعاملات الإلكترونية ؟ ذلك أن هذه الجريمة تتم ماديا بحصول الاستيلاء على المال المنقول المملوك للغير وذلك بإحدى طرق الاحتيال، فالاستيلاء على مال الغير هو النتيجة اللازمة قانونا لاكتمال تكوين الواقعة في الجريمة[3].

وقبل التطرق لفكرة الاستيلاء في نطاق المعاملات الإلكترونية نتناول أولا الأشكال التي يمكن أن تتخذها هذه الجريمة باعتبارها أحد أهم الجرائم الواقعة في هذا المجال حيث نذكر من بين أهم الطرق التدليسية الواقعة في مجال المعلوماتية ما يلي:

1- حسين فريجة، المرجع السابق، ص 256.

2 -www.algeriedroit. Fb.bz. le ; 22/01/2011 a ; 14h20mn

3- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 48.

- إعداد مزادات خادعة حيث أن ما يتم عبر شبكة الانترنيت ليس ماديات يتم الإطلاع عليها واقتناؤها فورا مثل المزاد التقليدي وإنما مجرد صور لتلك المواد بما يزيد من فرص النصب ويجعلها تعد الأكثر انتشارا في العالم الافتراضي.

- الاحتيال باستخدام أساليب الاستثمار، كالإعلان عن بيع أسهم شركات عبر شبكة الانترنيت والقيام بتحويل قيمتها إلى أحد المصارف، وذلك بقصد الإعلان المزيف عن الوضع المالي للشركة وذلك برفع قيمة أسهمها ثم القيام ببيع هذه الأسهم بمجرد بروز الأثر الإيجابي للخديعة.

- النصب بأسلوب انتحال الشخصية فيقوم المجرم عن عمد بالحصول على منفعة اقتصادية كحيازة مال أو تحويله أو استخدامه بموجب وثائق إثبات شخصية تخص آخرين.

- الاستيلاء على متعلقات الهوية مثل أرقام كروت الائتمان وذلك بعرض مواقع خادعة يتم من خلالها الاستيلاء على هذه الأرقام بأن يرتاد المجني عليه هذه المواقع بما يؤدي إلى وقوعه ضحية للاحتيال[1].

وهذا الشكل الأخير للاعتداء على المعاملات الإلكترونية يمثل الصيغة الثانية للإشكال الذي طرحناه حول مدى إمكانية تطبيق فكرة الاستيلاء في المجال المعلوماتي، ذلك أن هذه الفكرة الأخيرة يكون الهدف منها في أغلب الأحيان هو الحصول على الأموال، ومن ثم يستوجب علينا للتطرق لمدى إمكانية تطبيق فكرة الاستيلاء في مجال المعاملات الإلكترونية أن نتعرض للمسالتين التاليتين:

1- المسألة الأولى: مدى تحقق جريمة النصب من خلال الاستيلاء على النقود الكتابية أو البنكية عن طريق القيد الكتابي.

2- المسألة الثانية: مدى تحقق جريمة النصب من خلال الاستيلاء على النقود الكتابية أو البنكية عن طريق بطاقات الائتمان.

1- د/ محمد عبيد الكعيبي، المرجع السابق، ص 606.

والإجابة عن هاتين المسألتين تقودنا لمعرفة مدى خضوع المكونات المعنوية للنظام المعلوماتي للنشاط الإجرامي في جريمة النصب.

المسألة الأولى:

مدى تحقق جريمة النصب من خلال الاستيلاء على النقود الكتابية أو البنكية عن طريق القيد الكتابي

تقتضي جريمة النصب أن يقوم الجاني بحيازة المال محل الجريمة حيازة مادية وهو ما يستلزم كذلك أن يكون الاستيلاء ماديا من قبل هذا الجاني، و يتحقق هذا الفرض في مجال المعاملات الإلكترونية في حالة الشخص الذي يقوم بالتلاعب في البيانات الموجودة داخل الحاسوب ثم يتحصل على مستخرجات مادية تتجسد في شكل فواتير و شيكات أو أقراص صلبة ثم يستولي عليها وهذا الفرض يخضع للقواعد العامة لقانون العقوبات[1] و لا يخلق أي إشكال لكننا نكون بصدده في حالة ما إذا كان محل الإستلاء ما يعرف بالنقود الكتابية أو البنكية[2] وذلك إذا تحقق هذا الإستلاء عن طريق إجراء ما يعرف بالقيد الكتابي وذلك بالتلاعب في البرامج والبيانات الذي يترتب عليه تحويل بعض أو كل أرصدة أصحابها الشرعيين أو فوائدها إلى حساب الجاني[3]

فهل يعد هذا من قبيل الاستيلاء المادي الذي تتطلبه جريمة النصب؟ وتكون الإجابة بالإيجاب وذلك حال الاعتراف لهذه النقود بصفة المال.

باستقراء الموقف في التشريعات لمقارنة نجد أن بعض هذه التشريعات مثل التشريع الألماني في المادتين 242، 246 عقوبات وتشريعات اليابان ولكسمبورغ، تنظر إلى النقود الكتابية بوصفها من قبيل الديون ولا تعتبرها بمثابة مال مادي وبالتالي يستحيل أن تكون محلا لجريمتي النصب أو السرقة[4].

1-Raymons gassin, le droit penale de l'informatique, dalloz1986 , p38.

2 - المقصود بالأموال الكتابية أو البنكية تلك الأموال التي يتم تبادلها إلكترونيا وذلك بالاستعانة بأنظمة المعالجة الآلية للمعطيات والتي تسهل عملية التحويل الإلكتروني للأموال وفقا لبرامج معدة سلفا لهذا الغرض وتمتاز طريقة تحويل هذه الأموال بالسرعة في التنفيذ، راجع في ذلك: عفيفي كامل، جرائم الكمبيوتر وحفوف المؤلف والمصنفات الفنية، دار الثقافة للطباعة والنشر، 2000، ص151.

3- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 48

4 -www.djetfa.info/Vb/showthread.php?t=204052. Le :05/02/2011 à : 15h40mn.

في حين هناك بعض التشريعات تعتبر النقود الكتابية بمثابة أموال مادية، مثل كل من كندا "المادة 2/282 عقوبات" وهولندا "310، 311، 322 عقوبات" وسويسرا في المواد "137، 140، 141 عقوبات" وفي معظم الولايات الأمريكية وانجلترا، كما قضت المحكمة العليا في النمسا مؤخرا بأن تعبير المال الوارد بالمادتين 133 عقوبات الخاصة بجريمة خيانة الأمانة، و"134 عقوبات الخاصة بجريمة النصب يشمل النقود الكتابية[1].

وذلك ما قضت به ايضا محكمة النقض الفرنسية من أن التسليم المقصود للأموال في جريمة النصب المعلوماتي يستوي فيه التسليم المادي أو ما يعادله، فقد أدانت محكمة النقض الفرنسية تاجرا عن جريمة نصب لأنه تقدم بفواتير بيع مزورة وحصل في مقابل ذلك على استرداد قيمة ضرائب المبيعات في الدولة، إلا أن التاجر لم يسترد هذا المبلغ نقدا ولكن تم خصمه من قيمة الضرائب المستحقة عليه للخزينة العامة نظير المبيعات الحقيقية التي تمت في فترات سابقة، وقد اعتبرت محكمة النقض أن الدفع الذي تم عن طريق القيد الكتابي يعادل تسليم الأموال ماديا، فالائتمان الذي حصل عليه الجاني وهو قيمة الضرائب المستحقة عليه للخزينة العامة ومن ثم تكون محكمة النقض قد أخذت بالأشكال الجديدة للعملات الكتابية[2]

وعلى ذلك الاساس ابتكر القضاء الفرنسي نظرية جديدة تعرف بنظرية "التسليم المعادل" وقد لاقت هذه النظرية ترحيبا واسعا من قبل الفقه الفرنسي، وذلك لمواجهة حالات الاحتيال الواقع باستعمال الحاسب، فعلى الرغم من الطبيعة غير المادية للنقود الكتابية، فإن الدفع يتم بواسطة القيد كتابة وهو ما يعادل التسليم المادي للأموال-[3].

كما اعتبرت محكمة النقض الفرنسية أن الإبراء من دفع الأجرة يقوم مقام التسليم على الرغم من أن الجاني لم يتسلم أي شيء مادي، وذلك في قضية الشخص الذي دخل بسيارته إلى ساحة انتظار السيارات ولكنه بدلا من وضع النقود الأصلية المطلوبة في أماكن الانتظار إلا أنه وضع فيه قطعة معدنية عديمة القيمة، فقضت محكمة النقض بتطبيق عقوبة النصب على هذا

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 702.
2- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 223.
3- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 49.

الشخص لأنه بوضعه لهذه القطعة في العداد يكون قد استخدم طرقا احتيالية من أجل نقل عقارب العداد للإيهام بأنه دفع أجرة التوقف في أماكن الانتظار[1].

كذلك قضت محكمة "Douai" بتطبيق عقوبة النصب على الشخص الذي وضع قطعة معدنية عديمة القيمة داخل جهاز هاتف عام وذلك بقصد التحدث مع الغير دون دفع قيمة المكالمة[2]

ومما سبق يمكن القول أن الأموال التي يتم تداولها في نطاق المعاملات الإلكترونية يمكن أن يشملها النشاط الإجرامي المنصوص عليه في المادة 372 من قانون العقوبات الجزائري، كون التلاعب بالمعلومات أو البيانات المحيطة بتلك الأموال يؤدي في النهاية إلى تسليم المال للجاني، حيث يمكن تصنيف فعل التلاعب بالبيانات بأنه من قبيل الطرق الاحتيالية التي عالجتها المادة 372 وذلك حال تسليمنا بنظرية التسليم المعادل.

المسألة الثانية: مدى تحقق جريمة النصب من خلال الاستيلاء على النقود الكتابية عن طريق بطاقات الائتمان؟[3] .

قد يحدث وأن يتم استخدام بطاقة الائتمان بطريق الغش بغرض الحصول على الأموال ويكون ذلك من قبل مالكها الأصلي أو من الغير، ولذلك نفرق بين الحالتين لبحث مدى توافر الاستيلاء على النقود الكتابية عن طريق بطاقات الائتمان، وبصيغة أكثر دقة إلى أي مدى يمكن أن تستخدم بطاقات الائتمان كوسيلة لقيام فعل الاحتيال ومن ثم قيام جريمة النصب؟

أولا: حالة استخدام البطاقة من مالكها الشرعي:

وفي هذا الفرض نفرق بين ثلاث حالات:

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 49.
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 704.
3- بطاقة الائتمان هي بطاقة مستطيلة من البلاستيك تحمل المؤسسة المصدرة لها وشعارها وتوقيع حاملها وبشكل بارز على وجه الخصوص رقمها واسم حاملها ورقم حسابه وتاريخ انتهاء صلاحيتها وبفضل هذه البطاقة يستطيع حاملها أن يسحب مبالغ نقدية من أجهزة التوزيع الأوتوماتيكي ويستطيع أن يحصل المتعاملون بهذه البطاقة على ما يحتاجونه من سلع وخدمات من التاجر دون أن يضطر حاملها إلى الوفاء بثمن الخدمات فورا بل يكتفي بتقديم هذه البطاقة إلى التاجر الذي يدون بياناتها عادة باستخدام آلة طباعة إلكترونية أو يدوية في فاتورة من عدة نسخ يوقعها العميل حيث يرسل التاجر نسخة من هذه الفاتورة إلى الجهة المصدرة في نهاية كل شهر وذلك لسداد قيمتها إلى التاجر وخصمها في نفس الوقت من الحساب الجاري للعميل لديها، راجع في ذلك : د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص680.

1- **بطاقة الائتمان الصحيحة:** يقوم الإشكال في هذا الفرض حال استخدامها من قبل صاحبها في سحب النقود من منافذ السحب الآلي، وذلك بما يتجاوز رصيده، فهناك من اعتبر هذا السلوك سرقة وهناك من اعتبره نصبا[1]، لكن القضاء كانت له وجهة نظر مغايرة فقد رفضت محكمة النقض الفرنسية التسوية في مجال النصب بين استعمال صفة غير صحيحة ومجرد الكذب الخاص بصفة المتهم كدائن، وأن المبالغة في استخدام صفة حقيقية لا تعد من قبيل الوسائل الاحتيالية إلا إذا كان من شأن هذه الصفة أن ترسخ وتدعم الإدعاءات الكاذبة وتخلق نوعا من الثقة لدى المجني عليه، وغني عن البيان أن كل ذلك غير متوافر في الواقعة محل البحث، وانتهت هذه المحكمة إلى القضاء بأن هذا التصرف ليس نصبا أو سرقة ولا ينطبق عليه أي نص أو وصف جنائي، وإنما هو مجرد إخلال بالتزام تعاقدي وذلك ما سار عليه القضاء المصري [2].

2- بطاقة الائتمان الملغاة: إذا كان الاستعمال التعسفي لبطاقة السحب من جانب الحامل الشرعي لا يشكل جريمة جنائية في حال السحب الزائد عن الرصيد، فإن للبنك مصلحة مشروعة في أن يتوقف هذا الحامل غير الأمين عن هذا الاستعمال، وذلك عن طريق إلغاء البطاقة بالنسبة للمستقبل، لان إلغاء هذه البطاقة يعد سلاحا رادعا ضد العميل سيء النية الذي يستمر في استعمال البطاقة رغم طلب الرد المعلن من البنك، وقد اجمع الفقه في هذه الحالة أن الشخص إذا قام باستخدام بطاقته رغم إلغائها في سحب النقود فإن فعله يشكل جريمة نصب حيث يشكل فعله وسيلة احتيالية تتجه إل إقناع المجني عليه بوجود ائتمان وهمي، بالإضافة إلى سوء نية الحامل الذي لا يمكن إنكاره في هذه الحالة حيث يتحقق في النهاية ركن التسليم، فاحتفاظ الحامل بالبطاقة رغم إلغائها وعدم ردها والاستمرار في استعمالها فالهدف منه هو محاولة إقناع الغير بوجود ائتمان وذلك بغرض الاستيلاء على المال وهو ما تتوافر به الطرق الاحتيالية[3].

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ص51.

2- وذلك من خلال حكمه في الدعوى التي أقامها أحد البنوك ضد أحد الأفراد بتهمة النصب ذلك أن المدعي عليه تمكن من استخدام طرق احتيالية للاستيلاء على مبالغ مالية تتجاوز دخله السنوي، لكن المحكمة قضت ببراءة المتهم لأن أركان جريمة النصب غير متوافرة وجاء في حيثيات الحكم "حيث أن المدعي عليه قام باستخدام الفيزا كارد وحصل على مشتريات من التاجر وقام البنك بسداد ثمنها وتبين أن رصيد المدعي عليه لم يسمح بسداد مديونيته ومن ثم فإن المسئولية تكون مسئولية البنك وحيث أن العلاقة بينهما علاقة مدنية بحتة فلا يكون المدعي عليه مرتكبا لجريمة النصب" راجع في ذلك: د/عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص689 .

3- د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 691.

3- بطاقة الائتمان المنتهية الصلاحية: قد يحدث وأن يستخدم الحامل الشرعي بطاقته رغم علمه بنهاية صلاحيتها، وفي هذا الصدد ذهب جانب من الفقه إلى القول بأن هذا السلوك مكون لجريمة خيانة الأمانة وذلك على أساس أن البطاقة بمثابة محرر يتم تسليمها للعميل على سبيل عارية الاستعمال[1].

لكن البعض اعتبرها جريمة نصب، فمتى نجح حامل البطاقة المنتهية الصلاحية في إدخالها إلى الماكينة التي من المفروض أن تبتلعها أو ترفضها، واستخدم في سبيل ذلك رقم سري خاص ببطاقة أخرى، فإنه يرتكب جريمة النصب باستعمال الطرق الاحتيالية[2].

ثانيا: حالة استخدام البطاقة من قبل الغير: وفي هذه الحالة نفرق بين فرضين:

1- بطاقة الائتمان المفقودة أو المسروقة:

يرى بعض الفقه أن استغلال الغير للبطاقة التي قام بسرقتها أو العثور عليها في إجراء عملية سحب للنقود بموجبها أن هذا السلوك الذي قام به الجاني مكونا لجريمة النصب على أساس أن الجاني اتخذ اسما كاذبا بما يسوغ القول معه أنه استخدم وسيلة احتيالية يريد من ورائها إقناع المجني عليه بأن هناك ائتمانا موجودا[3].

وذلك ما قضت به بعض المحاكم الفرنسية، بان يسأل عن جريمة النصب الجاني الذي يستخدم البطاقة المفقودة أو المسروقة في سحب أوراق البنكنوت من أجهزة التوزيع الآلي للنقود وتم التعرف عليه عن طريق كاميرات المراقبة، وذلك لان الجاني يكون قد اتخذ اسما كاذبا وهو اسم العميل صاحب الرصيد في البنك أو اسم الحامل الشرعي للبطاقة، فالجاني عندما يضع البطاقة الممغنطة في جهاز التوزيع الآلي للنقود يدعي لنفسه اسما كاذبا وهو أنه يحق له أن يسحب من ذلك الرصيد، كما تتحقق جريمة النصب حال السرقة الصورية للبطاقة حيث يقوم صاحبها في هذه الحالة بالتبليغ بضياعها والفرض أنها مازالت في حوزته وبعد ذلك الإخطار الكاذب يقوم باستخدامها، ويعد هذا الحامل في هذه الحالة من الغير بالنسبة للبطاقة لأن الإعلان عن سرقتها أو

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 51.
2- د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 689.
3- أمال قارة، ص51.

فقدها يكون قد جرده من صفته كحامل شرعي لها ويدخله في طائفة الغير، وذلك ما قضت به محكمة النقض الفرنسية بتوافر أركان جريمة النصب في مواجهة حامل البطاقة إذا استعمل البطاقة بعد الإعلان الكاذب عن سرقتها[1].

2- بطاقة الائتمان المزورة: قد يحدث وان يتم تزوير بطاقة الائتمان سواء بتقليدها أو اصطناعها ومن ثم استخدامها، وقد ثار خلاف حول تكييف هذا الفعل قانونيا، فقد ذهب جانب من الفقه انه في حالة قيام الغير بتزوير بطاقة الائتمان واستغلالها في سحب مبالغ من أجهزة السحب الآلي للنقود يعتبر جريمة سرقة بمفتاح مصطنع، كما استبعد بعض الفقه تطبيق جريمة التزوير على أساس أن بطاقة الائتمان لا تعتبر محررا كتابيا[2].

أما بالنسبة لموقف القضاء فقد قضت محكمة جنح RENNES سنة 1981 أن استخدام البطاقة المزورة في السحب من جهاز التوزيع الآلي للنقود يعد من قبيل الطرق الاحتيالية التي تقوم بها جريمة النصب، في حين ذهبت محكمة جنح LILLE إلى عدم انطباق جريمة النصب في حالة بطاقة الائتمان المزورة لأن الطرق الاحتيالية يجب أن ترتبط بين شخصين[3].

لكن المشرع الفرنسي حسم الجدل الذي كان قائما حول استخدام بطاقة ائتمان مزورة وذلك بإصداره لقانون رقم 91-1382 في 30 ديسمبر 1991 والذي عدل قانون 30 أكتوبر 1935، وقد بدأ سريان قانون العقوبات الجديد اعتبارا من 01 مارس 1994 و لم يلغي قانون سنة 1991 الخاص بالبطاقات والذي نصت فيه المادة 67 على "عقوبة الحبس من سنة إلى سبع سنوات والغرامة من 3600 فرنك حتى 500000 فرنك أو بإحدى هاتين العقوبتين على:

1. كل من قلد أو زور بطاقة من بطاقات الوفاء أو السحب.
2. كل من استعمل أو حاول استعمال بطاقات مقلدة أو مزورة وهو عالم بذلك.
3. كل من قبل الدفع ببطاقة الوفاء على الرغم من علمه بتقليد البطاقة أو تزويرها"[4].

1- د/ عمر أبو الفتوح عبد العظيم الحمامي،المرجع السابق، ص 691- 695.
2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 52.
3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 697.
4- د/ إيهاب فوزي السقا، الحنائية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية 2007، ص 328.

وبذلك يكون المشرع الفرنسي قد حسم الجدل القائم حول تكييف استخدام بطاقة الائتمان المزورة، وباستقراء الاتجاهات الفقهية والقضائية السابقة حول مدى خضوع المكونات المعنوية للنظام المعلوماتي للنشاط الإجرامي في جريمة النصب بغض النظر عن التشريعات التي عالجت هذا الفرض، فإننا نرى إمكانية تحقق ذلك أي تحقق الركن المادي لجريمة النصب على المكونات المعنوية للنظام المعلوماتي وذلك للأسباب التالية:

- إمكانية خداع النظام المعلوماتي ذلك أن هذا الأخير مبرمج سلفا وفقا لرغبة صاحبه، ومن ثم فإن خداع النظام المعلوماتي يمكن أن يتحقق بإحدى الطرق التي نص عليها المشرع الجزائري في نص المادة 372 كاستعمال أسماء أو صفات كاذبة كما يمكن تدعيم ذلك الكذب أو الخداع بأعمال مادية ، وتحقق الاحتيال على النظام المعلوماتي يعني تحققه على صاحب النظام.

- باعتبار جريمة النصب جريمة مركبة وليست بسيطة أي يشترط لقيامها بالإضافة إلى فعل الاحتيال أن يكون هناك تسليم ويترتب عليه ضرر وعليه يمكن القول :

- التسليم المنصوص عليه في القواعد العامة ينصرف محله أيضا إلى النقود الكتابية فالتلاعب في البيانات المدخلة أو المخزنة في النظام المعلوماتي من شأنه تحويل الأرصدة المالية ما يؤدي إلى تسليم المال للجاني، فالتلاعب في البيانات هنا يعد من قبيل الطرق الاحتيالية، أما المال الذي يتم استلامه فهو يعادل التسليم المادي وفق نظرية التسليم المعادل.

- أما التسليم الواقع بواسطة بطاقة الائتمان ففي حال بطاقة الائتمان الصحيحة التي يستخدمها صاحبها في الحصول على مشتريات تفوق رصيده في البنك، فإننا نكون بصدد جريمة نصب حال علم الجاني بذلك أي توافر القصد الجنائي لديه ويمكن إثبات ذلك عن طريق التأكد من المعطيات التي قدمها العميل للبنك والتي قد تكون مخالفة للحقيقة، كما يمكن التحقق من توافر القصد الجنائي في هذه الحالة عند إقدام الجاني على استلام أموال أو سلع تفوق رصيده ثم يقوم بإلغاء تلك البطاقة، وبذلك يمكن إثبات سوء نيته، كما أن الأموال أو السلع التي يستلمها هي أشياء مادية وبالتالي يمكن القول أن التسليم الحاصل في هذا الفرض يدخل في نطاق نص المادة 372 عقوبات جزائري.

- أما في حالة استخدام بطاقة ائتمان ملغاة أو منتهية الصلاحية، فلا تقوم جريمة النصب إلا إذا كان حامل البطاقة لا ينوي تجديدها، ويتحقق التسليم في هذا الفرض على المشتريات أو الخدمات فقط دون الأموال، ذلك أن البنك عند إلغاء البطاقة يقوم بسحب رقمها من نظامه المعلوماتي وبإقدام الجاني على إظهار البطاقة الملغاة للتاجر يتحقق هنا القصد الجنائي ويكون الجاني قد استخدم طرقا احتيالية على التاجر بإيهامه بوجود مبالغ مالية في البنك.

- أما في حالة التسليم الواقع بواسطة بطاقة ائتمان مسروقة أو مزورة فهو تسليم مادي يدخل في نطاق المادة 372 عقوبات جزائري، واستخدام البطاقة في هذه الحالة يمثل جريمة نصب نظرا لتوفر القصد الجنائي لدى مستخدمها وإتباعه طرقا احتيالية للحصول على المال.

أما الضرر في جريمة النصب فتطلبه المشرع الجزائري في نص المادة 372 "لسلب كل ثروة الغير أو بعضها" ويتحقق الضرر هنا عند استيلاء الجاني على مال المجني عليه عن طريق الطرق الاحتيالية التي سبق الإشارة إليها.

ويرى بعض الفقهاء أن مدلول الضرر في جريمة النصب ليس بالضرورة الانتقاص من ثروة المجني عليه وبالتالي لا يلزم وضع الضرر المادي فقط وإنما يجب إضافة الضرر المعنوي الذي ينتج عن تسليم المال إلى الجاني بناء على طرق احتيالية[1]

وذلك ما ينطبق تماما في مجال المعاملات الالكترونية، فالحصول على المعلومات لا ينقص من ثروة المجني عليه أي لا ينقص من تلك المعلومات وإنما يحدث له ضررا معنويا على عكس الأموال النقدية.

كما يشترط لاكتمال جريمة النصب أن تكون علاقة سببية بين فعل الاحتيال وسلب مال الغير وذلك ما يتحقق في نطاق المعاملات الالكترونية، حيث أن الغش وخداع الأنظمة المعلوماتية لسلب مال الغير يتحقق باستعمال الطرق الاحتيالية بالكذب الذي تدعمه مظاهر مادية وخارجية تؤيده، مثل تقديم مستندات مستخرجة من النظام المعلوماتي أو معلومات مدخلة للنظام للتلاعب

1- حسين فريجة، المرجع السابق، ص 275.

فيها ليستولي الجاني على أموال لا حق له فيها، فالطرق الاحتيالية التي اتخذها الجاني تربط بينها وبين المال الذي حصل عليه علاقة هي السبب في هذه الجريمة ولولا هذه الطرق الاحتيالية لما تمت الجريمة التي أوقعت المجني عليه في الخطأ نتيجة لها وجعلته يسلم ماله سواء أكان الشخص ذاته أو النظام المعلوماتي، أو جهاز التوزيع الآلي للنقود[1] ، أي أن يكون الاحتيال هو السبب الفعلي والدافع على التسليم وأن يكون التسليم نتيجة لانخداع المجني عليه، وأن يكون لاحقا على فعل الاحتيال.

أما فيما يتعلق بالمعلومات المعالجة آليا والتي يتم تداولها في نطاق المعاملات الإلكترونية فإنها تخضع للقواعد العامة لجريمة النصب وفق التعديل الذي أجراه المشرع الفرنسي لنص المادة 405 من القانون القديم، حيث حذف لفظ أشياء واستخدم في المادة 313-1 من قانون العقوبات الجديد عبارة " أموال أو قيمة " حيث يستوي في الشيء ذو القيمة أن يكون ماديا أو معنويا، وما يعزز ذلك أن بعض القوانين المحلية في الولايات المتحدة الأمريكية عند تعريفها للمال في قوانين الغش المعلوماتي عرفته بأنه " كل شيء ينطوي على قيمة " [2]ومن ثم فالأموال المعنوية تدخل في هذا الوصف، كذلك تقوم جريمة النصب المعلوماتي حسب النص الفرنسي متى كان محلها تقديم خدمة بناءا على النشاط الإجرامي الصادر من الجاني، ولذلك فاختلاس الخدمات ليس سرقة حسب القانون الفرنسي، ولكن استعمال طرق احتيالية للحصول على هذه الخدمة يعود نصبا حسب هذا القانون[3] لذلك لو قام أحد الأشخاص بطلب استشارة من طبيب أو محام عبر شبكة الانترنيت وأوهمه بسداد أتعابه من خلال بطاقة الائتمان و لم يسددها فإنه يرتكب جريمة نصب حسب قانون العقوبات الفرنسي، فهذا الأخير يجعل الخدمات مساوية للمال الذي يمكن تسليمه في جريمة النصب، فالنص الجديد تكلم عن تسليم المال والخدمات وليس الأشياء ولذلك فإن الفقه الفرنسي يرى في تخلي المشرع الفرنسي عن لفظ الأشياء يقابله أن التسليم قد يكون محله مالا معنويا إلى جانب المال المادي[4].

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 710.
2 -www.djetfa.info/Vb/showthread.php?t=204052. Le :05/02/2011 à : 15h40mn.
3- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 225.
4- د/ محمد عبيد الكعبي، المرجع السابق، ص 611.

ومما سبق التطرق إليه يمكن القول أن الأموال المتداولة في نطاق المعاملات الإلكترونية تدخل في نص المادة 372 عقوبات جزائري، أما البيانات أو المعلومات المعالجة آليا فإننا نرى ضرورة تدخل المشرع لحسم الجدل وذلك بإضافة عبارة " خدمات أو قيمة " لأن الخدمات في مجال المعاملات الإلكترونية لا تتم إلا بتبادل المعلومات، أما لفظ القيمة فيستوي فيه أن تكون مادية أو معنوية مثلما سبق التفصيل في ذلك، أو أن يقوم المشرع بالنص صراحة على جريمة النصب المعلوماتي مثل ما هو منصوص عليه في نظام مكافحة جرائم المعلوماتية السعودي، حيث ينص في المادة الرابعة: "يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليون ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة [1]

وبقيام المشرع الجزائري أو أي من التشريعات العربية بالنص صراحة على النصب المعلوماتي يحسم الجدل القائم حول تفسير مدلول المال بين المال المادي والمعنوي.

وقد عالجت الاتفاقية الأوروبية للإجرام المعلوماتي "اتفاقية بودابست" جريمة النصب المعلوماتي وذلك في المادة الثامنة[2] حيث جرمت فعل الاعتداء العمدي على وظيفة منظومة كمبيوتر و إلحاق خسائر لملكية شخص آخر عن طريق أي تدخل في بقصد احتيالي أوغير أمين للحصول وبدون وجه حق على منفعة اقتصادية لصالح الشخص ذاته أو لصالح الغير.

كما تنص المادة 10 من قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها على: "كل من توصل عن طريق الشبكة المعلوماتية أو أحد أجهزة

---

1 -www.lawyers-gate.co;/vb/therads/8371 le:02/01/2011à 10h40mn

2- Art8 : «Fraude informatique : ……a- l'introduction ,l'altération , l'effacement ou la suppression de données informatique .

b-toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui » de : www.eastlas.blogspot.com/2010/03/23.11.2001/htm le:16/09/2010 à 20h30mn

ومن باب الحرص على أن تكون كل أنواع التلاعب المتصورة قذ أخذت بالإعتبار فإن العناصر المكونة للإدخال introduction أو الإتلاف l'altération أو المحو l'effacement أم الطمس la supppression المبينة في الفقرة (1) يتم تكملتها بالإجرام العام للإعتداء على وظيفة الحاسب المنصوص عليها في الفقرة "ب" والمتمثلة في التلاعب في المكونات المادية للحاسب والأفعال التي تمنع الخرجات والأفعال التي تؤثر على تسجيل أو تدفق البيانات أو التسلسل الذي يتم تحميل البرامج ، راجع في ذلك د/هلالي عبد الله أحمد إتفاقية بودباست لمكافحة جرائم المعلوماتية ، دار النهضة العربية، القاهرة 2007، ص101.

الحاسب الآلي وما في حكمها على الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية، أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس... ، وبالغرامة... ، أو بإحدى هاتين العقوبتين"[1].

كما عالج قانون العقوبات الياباني النصب المعلوماتي وذلك في المادة 2/246 حيث يعاقب على الإستعانة بمعلومات مبرمجة كاذبة أو إدخال هذا النوع من المعلومات في نظام كمبيوتر لشخص آخر [2]

فالنصوص السابقة الذكر ذات مدلول واسع وتعالج الإشكال محل الدراسة بصيغة أكثر دقة فهي تحمي المال المادي والمعنوي من جريمة النصب.

ثانيا: الركن المعنوي لجريمة النصب في نطاق المعاملات الإلكترونية

نص المشرع الجزائري في المادة 372: "...وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها..." أي أن يكون سبب الاحتيال هو سلب ثروة الغير كلها أو بعضها بغية تملكها أي توافر القصد العام ثم القصد الخاص.

1/ القصد العام:

يتمثل القصد العام في توافر عنصري العلم والإرادة.

أ- العلم: يتطلب القصد العام علم الجاني بالعناصر المتمثلة في ماديات الجريمة، وانصراف إرادته إلى تحقيق هذه العناصر، وذلك بأن ينصرف الجاني إلى القيام بالتدليس ليحمل المجني عليه على تسليم ماله، وذلك بأن يكون الجاني على علم ويدرك كذب المعلومات التي يدلي بها[3].

1- www.Arabic.Mjustice.dz/ligve.arabe/loiemir-ar-crim-tech-info.htm. le ; 09/11/2010 à 11h00mn
2- د/ شيماء عبد الغني عطا الله ، المرجع السابق ص 67 .
3- حسين فريجة، المرجع السابق، ص 277.

وفي جرائم النصب المعلوماتي يستخدم الجاني أسلوبا للإيهام بوجود ائتمان كاذب أو مشروع كاذب[1].

ب- الإرادة: يجب أن تتجه إرادة الجاني إلى تحقيق الواقعة الإجرامية وهي سلب مال الغير، وأن من شأن فعله خداع المجني عليه وإيقاعه في الخطأ الذي يحمله على تسليم المال، ومن البديهي أنه يجب توافر عنصر الإرادة بجانب العلم.

وبخصوص القصد العام لجريمة النصب في نطاق المعاملات الإلكترونية، فقد أشار بعض الفقه إلى أن القصد العام بالمفهوم السابق ينطبق على جريمة النصب في النطاق المعلوماتي وذلك بالنسبة للجرائم الناشئة عن استخدام الجهاز و ذلك بعلم الجاني أن قيامه بالتلاعب في المعلومات والبيانات المخزنة داخل النظام المعلوماتي، أو التلاعب في المعطيات المدخلة من شأنه خداع النظام، ومن ثم تسلم البيانات أوالمعلومات بناءا على طرق إحتيالية .

ويبدو ذلك القصد جليا في حالة اتخاذ الجاني اسم كاذب من أجل تحويل الأموال من حساب لآخر، وفي حالة استخراجه لفواتير مزورة أي بحساب غير حقيقي، وكذلك في حالة تزوير أوامر الدفع ففي كل هذه الحالات فإن إرادة الجاني متجهة إلى خداع النظام المعلوماتي من أجل سلب مال الغير[2].

2/ القصد الخاص: القصد الخاص هو نية التملك، ويقوم متى كان هدف الجاني هو الاحتيال والاستيلاء على مال مملوك لغيره، علما أنه لا عبرة بالبواعث في ارتكاب جريمة النصب سواء كان الباعث نبيلا أم غير ذلك، ويتوفر القصد الخاص في النصب المعلوماتي متى قام الجاني باستخدام البطاقة وهو عالم أن رصيده ليس به ما يكفي أوأن بطاقته منتهية أو موقوفة ويستخدمها[3]، ففعل الجاني في هذه الحالة يعد مناورة هدفها الاستيلاء على جزء من مال البنك ذلك أن الجاني يعلم أنه لا يحق له استخدام هذه البطاقة ولكنه رغم ذلك يوجه إرادته لاستخدامها لسلب مال المجني عليه[4].

1- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 226.
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 716.
3- د/ عبد الفتاح بيومي حجازي ، ص 226.
4- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 718

المطلب الثالث:

مدى تحقق الحماية الجنائية للمعاملات الالكترونية وفقا للقواعد العامة المقررة لجريمة خيانة الأمانة

تنص المادة 376 من قانون العقوبات الجزائري: "كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقود 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 أجر 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 ويعاقب بالحبس من ثلاثة أشهر الى ثلاث سنوات وبغرامة من 500 إلى 20000 دينار.

ويجوز علاوة على ذلك أن يحكم على الجاني بالحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 وبالمنع من الإقامة وذلك لمدة سنة على الأقل وخمس سنوات على الأكثر، وكل ذلك دون الإخلال بما نصت عليه المادتان 158 و159 المتعلقتان بسرقة النقود والأوراق التجارية والمستندات والاستيلاء عليها من المستودعات العمومية".

وهذه المادة يقابلها نص المادة 341 عقوبات مصري والمادة (1/314)[1] عقوبات فرنسي التي حلت محل المادة 408 من قانون العقوبات الفرنسي القديم.

وقد عرف الفقه خيانة الأمانة بأنها استيلاء شخص على منقول يحوزه بناء على عقد مما حدده القانون عن طريق خيانة الثقة التي أودعت فيه بمقتضى هذا العقد وذلك بتحويل صفته من حائز لحساب مالكه إلى مدع لملكيته"[2].

1 - art 314/1 « *L'abus de confiance est le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenterou d'en faire un usage déterminé.*
L'abus de confiance est puni de trois ans d'emprisonnement et de 375000 euros d'amende. » code pénal français, édition 2011.

2- د/ مجدي محب حافظ، خيانة الأمانة والجرائم الملحقة بها، النسر الذهبي للطباعة، القاهرة 2002، ص 06.

كما عرفها البعض بأنها استيلاء الأمين عمدا على الحيازة الكاملة لمال سلم إليه بمقتضى سند من سندات الأمانة التي نص عليها القانون.

والجريمة على هذا النحو وإن كانت تتفق مع السرقة والنصب في أنها تمثل اعتداء على ملكية الغير وأنها تقع على منقول إلا أنها تختلف عنهما من حيث النشاط الإجرامي، فهو في السرقة الاستيلاء على الحيازة الكاملة دون الرضاء أي دون أن يسبقه تسليم ناقل للحيازة وفي النصب يوجد مثل هذا التسليم الناقل للحيازة ولكنه تم بناء على إرادة مشوبة بالغلط بسبب الاحتيال الذي لجأ إليه الجاني، أما في خيانة الأمانة فالتسليم الإرادي عنصر أولي فيها، فالأمين يتسلم المال تسلما قانونيا ينقل إليه الحيازة الناقصة على هذا المال ثم يغير نيته بعد ذلك إلى حائز حيازة كاملة ويعبر عن هذا التغيير بأحد الأفعال التي نص عليها المشرع وهي الاختلاس أو التبديد أو الاستعمال[1] .

وسنتطرق لهذه الأفعال في الركن المادي لهذه الجريمة، أما عقود الأمانة المحددة في نص المادة 376 على سبيل الحصر فسنتعرض إليها عند التطرق لمحل هذه الجريمة.

والمشرع الجزائري لم يتطرق لجريمة الخيانة في مجال المعاملات الإلكترونية مثله في ذلك مثل المشرع المصري في نص المادة 341 أو الفرنسي في نص المادة (1/314) من قانون العقوبات الجديد فعلى الرغم من استحداث هذا الأخير لنصوص تعالج الغش المعلوماتي بشكل مباشر أو بإجرائه لتعديلات مثل النصوص التي تعالج جريمة التزوير أو النصب إلا أنه أغفل ذلك فيما يتعلق بجريمة خيانة الأمانة.

ولبحث مدى تحقق جريمة خيانة الأمانة في نطاق المعاملات الإلكترونية ارتأينا الإحاطة بهذا العنصر على الشكل التالي:

- **الفرع الأول:** محل جريمة خيانة الأمانة في نطاق المعاملات الإلكترونية.
- **الفرع الثاني:** أركان جريمة خيانة الأمانة في نطاق المعاملات الإلكترونية.

1- د/ علي عبد القادر القهوجي، شرح قانون العقوبات القسم الخاص، المرجع السابق، ص 365.

الفرع الأول: محل جريمة خيانة الأمانة في نطاق المعاملات الإلكترونية

بالنظر لنص المادة 376 عقوبات جزائري يتبين أن محل جريمة خيانة الأمانة هو المال المنقول المملوك للغير والذي تم تسليمه للجاني قبل وقوع الجريمة وذلك بناءا على عقد من عقود الأمانة الواردة على سبيل الحصر ويجب أن يكون المال الذي تسلمه الجاني من المجني عليه بقصد نقل الحيازة الناقصة.

لذلك سنبحث في هذا الفرع عن مدى تحقق هذه الشروط اللازمة في محل هذه الجريمة ومدى انطباقها في مجال المعاملات الإلكترونية وذلك على النحو التالي:

- **أولا:** ماهية المال المنقول المملوك للغير في نطاق المعاملات الإلكترونية.
- **ثانيا:** واقعة التسليم نطاق المعاملات الإلكترونية.
- **ثالثا:** عقود الأمانة في نطاق المعاملات الإلكترونية.

وبالتطرق لهذه العناصر الثلاث نكون قد أحطنا بمحل هذه الجريمة في مجال المعاملات الإلكترونية.

أولا/ ماهية المال المنقول المملوك للغير في نطاق المعاملات الإلكترونية:

تعد جريمة خيانة الأمانة من جرائم الاعتداء على الأموال، لذا كان من الطبيعي أن يكون محلها مال منقول معقود له جميع الخصائص المطلوبة سواء في السرقة أو النصب، وذلك لأن هذه الجرائم يجمع بينها جامع من حيث وقوعها على المال سواء كانت له قيمة مادية أو معنوية عند صاحبه وأن يكون ذو طبيعة مادية أي قابلا للحيازة[1].

كما يشترط في المال موضوع التسليم أن يكون منقولا، أي توافر إمكانية نقله من مكان لآخر حتى ولو أدى ذلك النقل إلى تلفه وهو ذات المعنى في جريمة السرقة والنصب، فيشمل المنقول بطبيعته والعقار بالتخصيص أو بالاتصال.

1- د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 758.

ويشترط أخيرا أن يكون المال موضوع التسليم مملوكا للغير وهذا شرط بديهي لأن العلة من العقاب على خيانة الأمانة هي الاعتداء على مال الغير[1]، كما لا يشترط أن يكون مالك الشيء معلوما بل يكفي أن يثبت أن للشيء مالكا آخر غير الجاني حتى ولو كان هذا المالك مجهولا أو غير معين[2].

وبالتعرض لهذه الصفات الواجب توافرها في المال محل جريمة خيانة الأمانة، فهل يمكن القول بتطابقها على المال محل الجريمة في نطاق المعاملات الإلكترونية؟

قبل التطرق للآراء الفقهية التي جاءت في هذا السياق يمكن القول بأن المكونات المادية للنظام المعلوماتي أو التي تقوم عليها المعاملات الإلكترونية لا تثير أي إشكال قانوني مثلما سبق التفصيـــل في ذلك عند التطرق لجريمة السرقة والنصب، ذلك أن المكونات المادية للنظام المعلوماتي كالشاشة وأجهزة الإدخال والإخراج ولوحة المفاتيح والدعامات المادية كالأشرطة والأقراص .. في شكلها الخام تدخل في نطاق نصوص القواعد العامة، أي يتضمنها نص المادة 376 عقوبات جزائري والمادة 341 عقوبات مصري والمادة 314 عقوبات فرنسي.

- فهل يمكن القول بخضوع المكونات المعنوية للأنظمة المعلوماتية كالمعلومات التي يتم تداولها إلكترونيا للقواعد العامة التي تحكم جريمة خيانة الأمانة؟

في البداية يتعين تصور إمكانية وقوع جريمة خيانة الأمانة بالطريق المعلوماتي كما لو تسلم الجاني من المجني عليه مجموعة برامج خاصة بالحاسب الآلي موجودة على دعامة على أن يردها إليه وذلك بمقتضى عقد من عقود الأمانة، ثم قام الجاني بتغيير نيته وحول الحيازة الناقصة إلى حيازة تامة وتصرف في هذه البرامج المعلوماتية كما لو كان مالكا أو استعملها بطريقة أدت إلى هلاكها أو قام بتبديدها أو إعارتها إلى آخر دون أن يكون متفقا على ذلك في عقد الأمانة المبرم بينه وبين صاحب هذه البرامج [3]

1- د/ علي عبد القادر القهوجي، شرح قانون العقوبات القسم الخاص، المرجع السابق، ص 368.
2- مجدي محب حافظ، المرجع السابق، ص 41.
3- د/ عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، المرجع السابق، ص 318.

- في هذا الصدد يرى جانب من الفقه أن الطبيعة المعنوية أو غير المادية للقيم "المعلومات" في المجال المعلوماتي تثير بعض الصعوبات نظرا لأن هذه القيم ذات طبيعة معنوية من جهة، ولان جريمة خيانة الأمانة لا ترد إلا على منقول مادي من جهة أخرى، وعلى الرغم من ذلك فإن هذه القيم المعنوية مثل المعلومات والبرامج تصلح لأن تكون محلا لجريمة خيانة الأمانة إما لأنها تعتبر بمثابة بضائع، وإما لأنها تدخل في مفهوم المكاتيب التي ترتب التزاما أو تحوي مخالصة.

فالمعلومات وإن لم تعتبر أوراقا أو نقودا مالية أو بضائع كما حددها المشرع واتجه إلى ذلك غالب الفقه، فإن الرأي السابق قد استند في تبرير رأيه على التوسع من جانب القضاء الفرنسي في تعريفه لفكرة البضائع بحيث يمكن تطبيقها على الجرائم الناشئة عن استخدام النظام المعلوماتي[1] وفكرة البضائع تشمل كل شيء ناتج عن الطبيعة أو من صنع الإنسان ذاته يمكن أن يكون محلا للتجارة أو أن يستخدم في عمليات تجارية، لذلك استقر القضاء الفرنسي على أن المحرر حتى ولو لم يشتمل على تمسك أو مخالصة إلا أن له قيمة كبيرة في ذاته فهو من قبيل البضائع [2]

أما بالنسبة للمكاتيب فقد قضت المحاكم الفرنسية بأن كل الأوراق التي لها قيمة يمكن تقديرها بالنقود تعتبر بمثابة بضائع، وذلك مثل التصميمات الهندسية والخطابات الخطية والمستندات المتعلقة بعملاء مكتب متخصص في الخبرة المحاسبية، أو أي أوراق أخرى حتى إن لم تحتوي أو ترتب التزاما أو مخالصة [3]ولذلك فالكيانات المنطقية والبيانات تعد من قبيل المعلومات المعالجة والتي لها قيمة تجارية ولذا يجب النظر إليها بوصفها أموال، ومن ثم فهي تصلح لأن تكون محلا لجريمة خيانة الأمانة.

وقد لاقى هذا الرأي تأييدا في الفقه المصري من حيث اعتبار البيانات والمعلومات أموالا منقولة مملوكة للغير، ومن ثم فهي تصلح لأن تكون محلا لجريمة خيانة الأمانة[4].

ومما سبق نستنتج أن المعلومات التي يتم تداولها في مجال المعاملات الإلكترونية تصلح لأن تكون محلا لجريمة خيانة الأمانة وفقا للقواعد العامة متى تمتعت تلك المعلومات بطابع الاستئثار أي

1- د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 760.
2- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 241.
3- د/ جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة 1992،ص 111
4- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 764.

أنها تخص صاحبها فقط أو أشخاص محددين، ومتى تجسدت تلك المعلومات في شكل مرئي سواء على شاشة الحاسب الآلي أو على دعامات خارجية كالأوراق والأقراص، فهي تعد من قبيل الأموال لما لها من قيمة اقتصادية وبالتالي تقابلها قيمة مادية، فهي إما أن تكون ذات قيمة اقتصادية أي تدخل في مدلول البضائع، أو تكون عبارة عن بيانات ترتب التزما أو تحوي مخالصة، وبالتالي تدخل في مفهوم المكاتيب

كما أن المعلومات بهذا الوصف يمكن نقلها من شخص إلى آخر وبالتالي يمكن أن تنطوي تحت عقد من عقود الأمانة.

أما إذا كانت تلك المعلومات عبارة عن أفكار مجردة لم يتم تجسيدها في الواقع أي معالجتها آليا فإنه لا يمكن اعتبارها من قبيل الأموال، وبالتالي لا يمكن أن تكون محلا لجريمة خيانة الأمانة.

ثانيا/ واقعة التسليم في نطاق المعاملات الإلكترونية:

رأينا مما سبق أن التسليم في القواعد العامة شرط ثاني بعد تحقق شرط المال المنقول المملوك للغير وهذا الشرط هو جوهر هذه الجريمة، كونه يمثل نقطة الخلاف بينه وبين الجرائم الأخرى كالسرقة والنصب، ففي السرقة يتم الاستيلاء على الحيازة الكاملة دون أن يسبقه تسليم، أما في جريمة النصب فيكون التسليم بناءا على غلط، أما في خيانة الأمانة فيتم تسليم الحيازة الناقصة تسليما قانونيا ثم يحول الجاني الحيازة الناقصة إلى حيازة كاملة، فهل تطبق القواعد العامة لجريمة خيانة الأمانة فيما يتعلق بالتسليم على ذلك الذي يقع في مجال المعاملات الإلكترونية؟

في هذا الصدد ذهب جانب من الفقه الفرنسي إلى القول بإمكانية تطبيق القواعد العامة لجريمة خيانة الأمانة على تلك التي تقع في المجال المعلوماتي، واستند في ذلك على عبارة التسليم لأداء عمل بأجر أو بدون أجر الواردة في نص المادة 314 عقوبات فرنسي ذلك أن هذا النص يمكن تطبيقه في كل عقود العمل بأجر أو بدون أجر سواء في المعاملات العادية أو الإلكترونية

فالعبارة السابقة تعني أي شيء يتسلمه الأمين بغية ترميمه أو تعديله أو صنعه أو أن يباشر تصرفا قانونيا فيه وكل ذلك يتحقق بسهولة في المجال المعلوماتي[1]

وقد حدث وأن نسب القضاء الفرنسي تهمة خيانة الأمانة إلى مندوب شركة متخصصة في بيع اللوحات الشهيرة لقيامه بتغيير مسار بطاقات عملاء الشركات بأن سلمها لأحد المنافسين كي ينسخها بالتصوير و ذلك بصرف النظر عن إعادتها سليمة فيما بعد[2] فيكفي لوقوع جريمة خيانة الأمانة أن يكون المال المسلم قد خصصه صاحبه لإستعمال معين فيخرجه الأمين عن ذلك الإستعمال مستوليا على مال الغير[3]

في حين يرى جانب آخر أنه لا يتصور قيام عنصر التسليم في حالة المعلومات المسجلة إلكترونيا والمخزنة بداخل النظام المعلوماتي لعدم إمكان حيازتها في حد ذاتها، ولكن إذا أفرغت هذه المعلومات على دعامة مادية كشريط أو أسطوانة، وفي حالة تسليم الشريط أو الأسطوانة المتضمنة للمعلومات من المجني عليه بقصد نقل الحيازة الناقصة إلى الجاني بناء على عقد من عقود الأمانة المحددة قانونا على سبيل الحصر ثم قام الجاني بإختلاس الاسطوانة أو إستعملها أو بددها إضرارا بصاحبها فإن فعل الجاني هذا يشكل جريمة خيانة الأمانة[4].

ونحن من جهتنا نشاطر الرأي الأول القائل بإمكانية تطبيق القواعد العامة الواردة بشأن التسليم في خيانة الأمانة على التسليم الحاصل في المجال المعلوماتي، ونعيب على الرأي الثاني حجته الأولى القائلة بعدم إمكانية تصور قيام عنصر التسليم في حالة المعلومات المسجلة الكترونيا والمخزنة بداخل النظام المعلوماتي لعدم إمكانية حيازتها في حد ذاتها، فهذه الحجة في نظرنا مجافية للواقع العملي، صحيح أن المعلومات لا يمكن حيازتها في حد ذاتها لكن عمليا وفي مجال المعاملات الإلكترونية لا يتم تسليم تلك المعلومات ماديا أي في شكل دعامات مادية وإنما يتم تبادلها إلكترونيا من جهاز إلى جهاز، فيمكن أن يتم عقد من عقود خيانة الأمانة عن طريق تسليم المعلومات "بقصد نقل الحيازة الناقصة أو المؤقتة" إلكترونيا أي بدون الاستعانة بوسائل مادية

1- André vitu, traité de droit pénale spécial, éd cujas1989 p1950
2- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 242.
3- د/ شيماء عبد الغني عطا الله ، المرجع السابق ص 71 .
4- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 768.

كتسليم برامج على أقراص مثلا، ومن ثم فإنه يمكن القول أنه في ضوء المعاملات العادية يتم التسليم ماديا أما في مجال المعاملات الإلكترونية فإن التسليم يتم إلكترونيا، فالتسليم هنا يتفق مع طبيعة المعلومة والتي هي عبارة عن كيان معنوي، وبالتالي لا يكون التسليم مادي بل معنوي، ونظرا للتطورات الهائلة في مجال المعاملات الاقتصادية فقد بات من الضروري الاعتراف بفكرة التسليم الإلكتروني.

ثالثا/ عقود الأمانة في نطاق المعلوماتية:

جاءت عقود الأمانة سواء في القانون المصري أو القانون الفرنسي أو القانون الجزائري على سبيل الحصر وهي وفقا لنص المادة 341 عقوبات مصري "الوديعة، والإجازة، وعارية الاستعمال والرهن، والوكالة، وعقد الخدمات المجانية" أما في قانون العقوبات الفرنسي وفق نص المادة 314 هي "الوديعة، الإجارة، وعارية الاستعمال، الرهن، الوكالة، والعمل بأجر أو بدون أجر" والمادة 376 عقوبات جزائري هي نفسها المادة 314 عقوبات فرنسي من حيث تحديد هذه العقود، إذن فالعقود المحددة على سبيل الحصر هي:

1. **عقد الوديعة**:هي عقد يسلم بمقتضاه المودع شيئا منقولا إلى المودع إليه على أن يحافظ عليه لمدة وعلى أن يرده عينا (المادة 590 ق.م.ج) .
2. **عقد الإيجار**: هو عقد يمكن المؤجر بمقتضاه المستأجر من الإنتفاع بشيء لمدة محددة مقابل بدل إيجار معلوم (المادة 467 ق.م.ج).
3. **عارية الاستعمال**: هو عقد يلتزم به المعير أن يسلم المستعير شيئا غير قابل للاستهلاك ليستعمله بلا عوض لمدة معينة، أو في غرض معين على أن يرده بعد الاستعمال (المادة 538 ق.م.ج)[1].
4. **عقد الرهن**: الرهن المقصود هنا هو الرهن الحيازي لأنه هو الذي يتضمن نقل حيازة الشيء مؤقتا إلى الدائن المرتضي وهو عقد به يلتزم شخص ضمانا لدين عليه أو على غيره أن يسلم إلى الدائن أو إلى أجنبي يعينه المتعاقدان شيئا يترتب عليه للدائن حقا عينيا يخوله

1- أمر رقم 58/75 المؤرخ في 20 رمضان عام 1395 الموافق لـ: 26 سبتمبر1975 والمتضمن القانون المدني.

حبس الشيء إلى حين استيفاء الدين وأن يتقدم الدائنين العاديين والدائنين التالين له في المرتبة في اقتضاء حقه من ثمن هذا الشيء في أي يد يكون.

5. **عقد الوكالة**: وهو عقد بمقتضاه يلتزم الوكيل بأن يقوم بعمل قانوني لحساب الموكل[1].
6. **عقد العمل بأجر أو بدون أجر:** وهو العقد الذي أضافه كل من المشرع الفرنسي والجزائري والذي يستوي فيه أن يكون الالتزام بأداء العمل بمقابل أو بدون مقابل، ويقصد به من يتسلم شيئا للقيام بعمل مادي لمصلحة مالك الشيء أو غيره وقد يكون العمل بمقابل كعقد المقاولة أو بدون مقابل كمن يتطوع لعمل ما[2]

ومما سبق يمكننا التساؤل فيما مدى إمكانية تطبيق هذه العقود في مجال المعاملات الإلكترونية؟

انقسم الفقه في هذا الإشكال إلى اتجاهين:

الاتجاه الأول:

يرى هذا الاتجاه أن هذه العقود لا تمثل سوى قدر ضئيل من الأهمية في حالات الغش المعلوماتي وذلك باستثناء عقد القيام بعمل سواء بأجر أو بدون أجر حيث أن هذا العقد يتيح تجريم حالات قيام شخص يعمل على النظام المعلوماتي بحكم وظيفته في الحصول على المعلومات والتلاعب بها متى كانت تقع في نطاق حيازته الناقصة.

كما ذهب هذا الإتجاه للقول بتوافر جريمة خيانة الأمانة على العميل الذي يمتنع عن رد بطاقة الائتمان إلى البنك ذلك أن العلاقة بين العميل والبنك هي " عقد عارية الإستعمال " وبذلك يمكن إعمال هذا العقد في المجال المعلوماتي دون أي إشكال، كون بطاقة الإئتمان ملك للبنك فمتى قام بإلغائها وإخطار العميل بذلك أو انتهت صلاحيتها ورفض العميل إرجاع البطاقة فتتحقق فيه جريمة خيانة الأمانة [3].

1- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها الإلكترونية، المرجع السابق، ص 233- 235.
2- د/ أحسن بوسقيعة، المرجع السابق، ص 366.
3- د/ جميل عبد الباقي الصغير، المرجع السابق، ص 114.

ونحن من جهتنا نرى أن حصر العقود التي تتم في مجال المعاملات الإلكترونية في عقدي العمل وعارية الاستعمال فقط هو أمر مغاير للواقع، فباتساع شبكة الاتصالات أصبحت جل المعاملات تتم إلكترونيا حيث أصبح من السهولة إبرام العقود إلكترونيا، فقد يحدث وأن يرسل شخص معلومات سرية أو برنامج معلوماتي خاص بشركة ما عن طريق الشبكة المعلوماتية ويوكل شخص آخر بالتصرف في تلك المعلومات مثلا ثم يقوم الوكيل بعمل مغاير لما تم الاتفاق عليه فيجرم ذلك العمل بأنه خيانة أمانة، والأمثلة على التصرفات القانونية التي تتم إلكترونيا كثيرة ومتنوعة، لذلك نشاطر في الرأي ما ذهب إليه الاتجاه الثاني والذي توسع في نطاق العقود التي يمكن إدخالها في المجال المعلوماتي والتي تدخل في نطاق عقود خيانة الأمانة.

الاتجاه الثاني:

ذهب جانب من الفقه إلى إمكانية توسيع مجال تطبيق النصوص السابقة من استخدام لفظ "عمل مأجور أو غير مأجور" في عقود المقاولة والخدمات المجانية وعارية الاستعمال و عقد الوكالة، أي أن جريمة خيانة الأمانة يمكن تصورها بالنسبة للمخالفات المرتكبة في المؤسسات العاملة في المجال المعلوماتي، وانتهى هذا الرأي إلى أن العقود المهمة في هذا المجال هي عقود الخدمات المجانية والوكالة وعارية الاستعمال والعمل، لذلك يعد مرتكبا لجريمة خيانة الأمانة العامل الذي يختلس الأشياء المسلمة إليه بسبب عمله سواء كان بأجر أو بدون أجر فالعامل يدخل بحكم عمله على جهاز الحاسب الآلي أو النظام المعلوماتي ويمكنه ذلك بتجاوز المهام المعهود بها إليه، فيسأل عن خيانة الأمانة العامل الذي يختلس البرنامج المعهود به إليه بحكم عمله[1].

كما ذهب بعض الفقه الفرنسي إلى أن عقد العمل سواء بأجر أو بدون أجر يمكن أن يتسع ليشمل عقود عديدة ومتنوعة، منها عقد العمل وعقد تأجير الأشخاص وعقد المقاولة فإذا كان من قبيل خيانة الأمانة "اختلاس مدير أحد فروع شركة تجارية كبرى لأموالها إضرارا بها لقيامه بوصفه أجيرا لديها بتحصيل الرواتب الشهرية للعاملين بها لنفسه" فإنه يمكن بالمثل تطبيق ذلك على الجرائم

1- د/ جميل عبد الباقي الصغير، المرجع السابق، ص 113.

المعلوماتية التي يستغل فيها الفاعل مهنته في الولوج للنظام المعلوماتي ثم يتجاوز الحقوق التي منحت له.

أما القضاء الفرنسي فقد توسع في تطبيق هذه الجريمة في المجال المعلوماتي، حيث نسبت محكمة جنح باريس في حكم صادر لها في 12 أكتوبر سنة 1988 جريمة خيانة الأمانة إلى أحد المستخدمين الذين يعملون بشركة توظيف أموال والذي وضع تحت تصرفه بعض الأساليب المعلوماتية الخاصة بنظام المعالجة الآلية للبيانات المكلف بها وقام العامل بسبب وظيفته هذه بالاستيلاء على الأموال المجمدة للعملاء عن طريق تحويلها إلى حسابات أخرى[1].

ومما سبق يمكن القول أن "معظم العقود المنصوص عليها على سبيل الحصر في جريمة خيانة الأمانة يمكن أن تتم في مجال المعاملات الإلكترونية مثل عقود الوكالة وعارية الاستعمال والعمل و الخدمات المجانية وحتى وإن كانت بعض العقود الأخرى تصلح لأن تكون كذلك مثل عقد الوديعة إلا أنها نادرة التطبيق في مجال المعاملات الإلكترونية.

وما يمكن استنتاجه من الاتجاهات السابقة هو عدم وجود فقه معارض معارضة مطلقة لفكرة تطبيق العقود المنصوص عليها في جريمة خيانة الأمانة على المجال المعلوماتي فتلك المعارضة نسبية فقط كونها تستبعد عقود دون أخرى، ومن ثم فالتسليم بفكرة خيانة الأمانة في مجال المعاملات الإلكترونية هو أمر ضروري نظرا لإمكانية تجسيد جل تلك العقود في المجال المعلوماتي.

الفرع الثاني:أركان جريمة خيانة الأمانة في نطاق المعاملات الإلكترونية

للإحاطة بجريمة خيانة الأمانة في نطاق المعاملات الإلكترونية نتناول كل من الركن المادي والمعنوي لهذه الجريمة وفقا للقواعد العامة ومدى تحققه على المعاملات الإلكترونية.

أولا/ الركن المادي لجريمة خيانة الأمانة في نطاق المعاملات الإلكترونية:

تنص المادة 376 عقوبات جزائري على أن:"كل من اختلس أو بدد بسوء نية ...وذلك إضرارا بمالكيها أو واضعي اليد عليها أو حائزيها ...".

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 770.

فالمشرع الجزائري حصر النشاط أو السلوك الإجرامي في صورتين تتمثلان في الاختلاس والتبديد، أما المشرع المصري فقد نص في المادة 341 عقوبات على: "كل من اختلس أو استعمل أو بدد ...إضرارا بمالكيها أو أصحابها أو واضعي اليد عليها..."، فقد أضاف صورة الاستعمال للسلوك الإجرامي لهذه الجريمة، وهذه الصورة نجدها بشكل كبير في مجال المعاملات الإلكترونية، ولذلك يمكن القول أن صور السلوك الإجرامي في جريمة خيانة الأمانة هي الاختلاس، التبديد، الاستعمال، ويشترط في هذه الصور أن تحقق ضررا لمالك الأشياء المحددة في المادة على سبيل الحصر.

ولذلك سنتطرق للركن المادي لجريمة خيانة الأمانة في مجال المعاملات الإلكترونية من خلال تناول العنصرين التاليين:

1. مدى تحقق صور النشاط الإجرامي لجريمة خيانة الأمانة في مجال المعاملات الإلكترونية.
2. الضرر الناتج عن السلوك الإجرامي.

1- مدى تحقق صور النشاط الإجرامي لجريمة خيانة الأمانة في مجال المعاملات الإلكترونية:

السلوك الإجرامي في جريمة خيانة الأمانة له صور ثلاث وهي الاختلاس والاستعمال والتبديد وذلك على التفصيل التالي:

أ- الاختلاس:

يتحقق الاختلاس معلوماتيا في جريمة خيانة الأمانة بكل فعل يفصح عن طريقه "الأمين" عن اتجاه نيته إلى إضافة المال إلى ملكه والحلول محل صاحبه دون أن يترتب على ذلك خروج المال من حيازته، وعلى ذلك يتحقق فعل الاختلاس في خيانة الأمانة متى توافرت النية لدى الجاني في تغيير حيازته الناقصة على المال المسلم إليه من حيازة ناقصة إلى حيازة كاملة ومن ثم نيته في تملك هذا المال[1] وفي هذا الصدد ذهب بعض الفقه للقول بأن الاختلاس الحاصل في نطاق المعاملات الالكترونية يتحقق في الحالة التي يمتنع فيها العميل عن رد بطاقة الائتمان إلى البنك في حالة طلبها

1- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 244.

من جانب هذا الأخير سواء لانتهاء مدة صلاحيتها أو لإلغائها أثناء مدة صلاحيتها كجزاء لسوء استعمالها من جانب العميل، ذلك أن البنك هو مالك البطاقة وأنها موجودة لدى العميل على سبيل عارية الاستعمال[1].

وكيف البعض الاختلاس المعلوماتي في أفعال الغش المحاسبية والتي يستخدم فيها الحاسب الآلي من أجل إخفائها، ومن أمثلة ذلك قيام عضو مجلس الإدارة بصرف منح لنفسه بدون وجه حق وعن طريق حسابات غير منتظمة، أو ذلك الذي يزور في حسابات التحصيل والمدفوعات المسجلة في بطاقات الخزينة كي يتمكن من اختلاس الرصيد، وكذلك مندوب عامل التأمين الذي يستغل صفته حتى يقوم بتحصيل تبرعات يحتفظ بها لنفسه، وكلها أمثلة لفعل الاختلاس في خيانة الأمانة[2].

أما عن موقف القضاء فقد ذهبت محكمة النقض الفرنسية إلى أنه عندما يكون الحديث عن تسليم دعامات التي هي عبارة عن شرائط أو أسطوانات مسجل عليها معلومات فهي بمثابة أموال منقولة، ومن ثم فهي تصلح لأن تكون موضوعا لجريمة خيانة الأمانة، وهذا الحكم دعا البعض إلى القول بصلاحية تطبيق نص المادة 341 عقوبات مصري والمادة 314 عقوبات فرنسي جديد على الاختلاس الحاصل في النطاق المعلوماتي سواء الواقع على العناصر المادية للأنظمة المعلوماتية أو على العناصر المنطقية أو المعنوية للأنظمة المعلوماتية مثل البرامج المعلوماتية والمعلومات المسجلة إلكترونيا[3].

ب- التبديد: هو تصرف الأمين في المال الذي اؤتمن عليه شرط أن يؤدي هذا التصرف إلى خروج المال من حيازته، وقد اختلف الفقه حول الإتلاف ومدى اعتباره تبديدا، فذهب البعض إلى أن الإتلاف لا يعد تبديدا لأنه لا ينطوي على تغيير الحيازة وبالتالي فإن الجاني لا يهدف إلى تملك الشيء وإنما إلى تدميره، أما أغلب الفقه فيرون أن الإتلاف يعد تبديدا لأنه مظهر من مظاهر التصرف في المال لا يثبت إلا لمالكه وهو يتنافى تماما مع واجب الرد الذي يلتزم به الأمين[4].

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 782.
2- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 322.783.
3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 783.
4- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري،المرجع السابق ص 55.

وفي هذا الصدد ذهب بعض الفقه للقول بأن التبديد بمعناه الضيق غير متصور حصوله في حالات الغش المعلوماتي، ذلك أن التبديد سلوك إيجابي أو سلبي يخرج به الأمين المال من حيازته ويضيعه على صاحبه دون أن تكون نيته قد اتجهت إلى تملكه[1].

في حين ذهب البعض الاخر أن التبديد متصور حدوثه في النطاق المعلوماتي سواء الحاصل على المكونات المادية أو المعنوية مثل المعلومات التي تعد في وجهة نظر هذا الرأي من قبيل الأموال المنقولة، فإذا تسلم المؤتمن أي من نوعي المكونات المادية أو المعنوية بناء على عقد من عقود الأمانة فيمكن أن يسأل عن جريمة خيانة الأمانة في حال تبديدها أو إتلافها[2].

وذلك ما نؤيده شرط أن تكون تلك المعلومات معالجة آليا أي ليست معلومات مجردة فمتى تم تسليمها سواء ماديا عن طريق دعامة خارجية أو إلكترونيا بإرسالها عبر الشبكة المعلوماتية وذلك بناءا على عقد من عقود الأمانة وقام الأمين بتبديدها فإن سلوكه هذا يدخل في إطار القواعد العامة التي تحكم هذه الجريمة.

ج- الاستعمال:

وهو ذلك الاستعمال الذي يعدم المال من قيمته كلها أو جزء منها مع بقاء مادة المال كما هي ويتحقق ذلك الاستعمال عندما يكون استعمال الشيء مخالفا للغاية التي خصصت من أجله والمرتهنة بإرادة الأطراف، والاستعمال في جريمة خيانة الأمانة قد يكون إما استعمال متعسف للشيء المسلم للأمين، وقد يتعلق الاستعمال بالآلة أو قد يكون لبطاقات الائتمان[3].

- الاستعمال المتعسف للشيء المسلم للأمين:

خيانة الأمانة لا تقوم بمجرد الإخلال المدني بتنفيذ العقد من جانب الأمين، وإنما يجب لقيامها أن يثبت أن هذا الإخلال كان نتيجة ظهور الأمين على الشيء بمظهر المالك، وتطبيقا لذلك رفض القضاء الفرنسي تطبيق النص الخاص بخيانة الأمانة على حالات الاستخدام التعسفي للشيء من

1- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 247.
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق ص 770- 785.
3- د/ عمر أبوا الفتوح عبد العظيم الحمامي ، ص 786.

قبيل الأمين استخداما يتعارض مع الالتزامات التي يفرضها عليه العقد الذي تسلم الشيء بمقتضاه وذلك لأن مخالفة هذه الالتزامات لا تشكل بالضرورة اختلاسا، فقد قضت محكمة Dijon بأنه لا يرتكب خيانة الأمانة العامل الذي يتسلم البرنامج لمعالجة المعطيات الخاصة بالمشروع الذي يعمل به إذا ما استخدم هذا البرنامج في معالجة المعطيات الخاصة بالغير[1].

و يرى البعض أن الاستعمال المتعسف للشيء يعتبر مكونا لجريمة خيانة الأمانة متى كان الاستعمال مخالفا للتخصيص المتفق عليه، وذلك ما أقرته محكمة النقض الفرنسية بوجود خيانة أمانة ناشئة عن الاستخدام المتعسف لسلعة في أغراض مغايرة عن تلك المشترطة في العقد وهو ما ينطبق على محلل نظم المعلومات الذي يستغل فرصة إطلاعه على المعلومات المخزنة في بطاقات أو على شرائط ممغنطة ويستعملها بشكل يخالف ما هو متفق عليه، وذلك بنقلها إلى الغير أو تصوير بعضها تمهيدا لنقلها، كما يعتبر مرتكبا لجريمة خيانة الأمانة الشخص الذي يستعمل الشيء على نحو يخالف الغاية من الحق، وذلك كالشخص الذي يمارس سلطات وظيفته من الناحية المادية ولكن في الحقيقة يقوم باختلاس أشياء لمصلحته الشخصية[2]

- استعمال الآلة:

يرى البعض أن اغتصاب جهد الآلة لا يقع تحت طائلة خيانة الأمانة، كالعامل الذي يغتصب جهد جهاز الحاسب الآلي بدون مقابل أو لتحقيق غايات شخصية خاصة به طالما أن الأمين لم يغير حيازته على الجهاز أو نظامه من حيازة ناقصة إلى حيازة كاملة، وطالما لم يؤدي استعمال العامل للجهاز أو النظام إلى إتلافه كليا أو جزئيا و لم ينقص من قيمته، فمجرد الاستخدام التعسفي للجهاز لا تقوم به خيانة الأمانة[3]

في حين يرى البعض أن استعمال الآلة بدون رضا صاحبها وفي غير الغرض المخصص لها يعد سرقة استخدام قياسا على سرقة استخدام السيارة وسرقة الصورة ونسخها[4].

1- د جميل عبد الباقي الصغير، المرجع السابق، ص129
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 787- 788.
3- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 569.
4- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 790.

و من جانبنا نرى أن استخدام الجهاز بشكل غير مشروع يدخل في نص المادة 394 مكرر عقوبات جزائري والتي تعاقب كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات، فمتى انتهت ساعات عمل العامل المحددة في العقد فإن دخوله إلى النظام المعلوماتي أو بقاءه فيه بدون إذن صاحب النظام فإنه يعد مرتكبا لجريمة الدخول والبقاء دون إذن في النظام المعلوماتي.

- **استعمال بطاقات الائتمان:** يرى جانب من الفقه أن الاستخدام التعسفي لبطاقات الائتمان في سحب أوراق نقدية من أجهزة التوزيع الآلي للنقود تزيد عن الرصيد يشكل خيانة أمانة، ويبرر هذا الرأي وجهة نظره على أساس أن تسليم البنك للبطاقة الائتمانية للعميل مشروط بوجود رصيد كافي في حسابه وقت السحب وبمفهوم المخالفة عدم سحب مبالغ تزيد عن رصيده الموجود في البنك، وبالتالي إذا استخدم العميل البطاقة في السحب مع عدم وجود رصيد كافي يكون قد تعسف في استخدامها بما يتعارض مع ما جاء في العقد ومن ثم يكون محلا للمساءلة الجنائية، ويرى البعض أن العميل الذي يسحب بمقتضى بطاقته من أجهزة التوزيع الآلي للنقود مبالغ تجاوز رصيده في البنك يقع تحت طائلة المادة 462-4 من القانون الفرنسي رقم 19 لسنة 1988 وهي الخاصة بالإدخال العمدي لمعلومات إلى نظام معلوماتي معين أو تعديل أو إلغاء بث المعلومات التي يحتويها هذا النظام سواء تم ذلك بطريقة مباشرة أو غير مباشرة، وذلك لأن البنك بإعطائه بطاقة الائتمان إلى العميل ليسحب بمقتضاها من أجهزة التوزيع الآلي للنقود يكون قد سمح له بالولوج إلى النظام أو الجهاز و إذا ما دخل العميل إلى النظام وأعطى له أمرا بأن يصرف مبالغ تجاوز رصيده في البنك يكون بذلك قد أدخل إلى النظام معطيات يترتب عليها الإضرار بحقوق البنك، وبالتالي يكون العميل قد أساء إستعمال التصريح الممنوح له بالدخول إلى النظام بموجب بطاقة الائتمان[1].

والراجح فقها أنه إذا قام حامل البطاقة بالإستلاء على مبالغ مالية نتيجة استخدام البطاقة أثناء فترة صلاحيتها ولو بالمخالفة لشروط العقد فإن الفعل الذي وقع منه لا يعد خيانة أمانة، وذلك لأن قيام هذه الجريمة يتطلب أن تكون المبالغ التي إستولى عليها العميل قد سلمت إليه بمقتض عقد من عقود الأمانة [2]

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 791.

2 - Carillac et Mouly . droit Pénal de la Banque et du cridit . éd Masson 1982

أما عن موقف القضاء فقد استقرت محكمة النقض الفرنسية على أنه لا يمكن عقاب العميل الذي يسحب بمقتضى بطاقته مبالغ تتجاوز رصيده في البنك عن خيانة الأمانة، حتى ولو كان السحب الذي تم قد وقع بالمخالفة لشروط العقد المبرم بين العميل والبنك[1].

أما عن بطاقة الائتمان المنتهية الصلاحية والتي ثبت امتناع صاحبها عن ردها إلى الجهة المصدرة لها واستمراره في استخدامها فقد رأى غالبية الفقه أن هذا الفعل مشكل لجريمة خيانة الأمانة، ذلك أن البطاقة مملوكة للبنك وفي حالة عدم ردها عند انتهاء صلاحيتها أو إلغائها فإن حامل البطاقة يعد مختلسا لها، وذلك ما حكمت به محكمة جنح Certiel في حكمها الصادر في 15 يناير سنة 1985 من اعتبار عدم رد البطاقة الملغاة أو المنتهية الصلاحية فعل مشكل لجريمة خيانة الأمانة، حيث أن القضاء أسس تكييفه للفعل بأنه خيانة أمانة على أساس أن البطاقة تعد عقد من عقود عارية الاستعمال[2].

ومما سبق التطرق إليه من صور السلوك الإجرامي لجريمة خيانة الأمانة فإنه يمكن القول بإمكانية تحقق النشاط الإجرامي لهذه الجريمة في مجال المعاملات الإلكترونية وذلك سواء على المعلومات الموجودة في دعامات وأشرطة مادية أو المعلومات الموجودة داخل النظام والتي تمت معالجتها آليا، فمتى تم تسليمها بناءا على عقد من عقود الأمانة فهي تعتبر محلا لهذه الجريمة وتخضع لنشاطها الإجرامي.

2- الضرر الناتج عن خيانة الأمانة في نطاق المعاملات الإلكترونية:

اشترطت جل التشريعات أن يترتب على النشاط الإجرامي لجريمة خيانة الأمانة "الاختلاس الاستعمال والتبديد" ضررا، فهذا الأخير عنصر من عناصر الركن المادي للجريمة ومن ثم يجب توافره، ويستوي في الضرر أن يكون محقق الوقوع أو محتمل[3] أو أن يكون ماديا أو أدبيا، ولو انتفى الضرر ولو في شكله المحتمل فإن الجريمة تنتفي لانتفاء الإضرار بالمصلحة محل الحماية الجنائية والضرر المشترط لخيانة الأمانة قد يلحق مالك الشيء أو صاحبه أو حتى واضع اليد عليه، والضرر

1- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 57.
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 792.
3- د/ عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، المرجع السابق، ص 328.

على النحو السابق يمكن تحققه في نطاق المعاملات الإلكترونية مثل حالة امتناع العميل عن رد البطاقة الائتمانية بعد إلغائها أو انتهاء صلاحيتها ونجاحه في استعمالها في سحب أوراق نقدية فاستعماله هذا يكون قد حقق ضررا ماديا للبنك يتمثل في خسارته لأمواله التي سحبها العميل بدون وجه حق، كما أن اختلاس دعامات مادية مسجل عليها معلومات أو برامج يكون الضرر فيها متوافرا في حق صاحب المعلومات أو البرامج [1]

كما يمكن أن يحدث الضرر في نطاق المعاملات الإلكترونية في حالة الشخص الذي يقوم بتبديد برنامج أو معلومات داخل النظام المعلوماتي والتي كانت تحت تصرفه بموجب عقد من عقود الأمانة.

ثانيا/ الركن المعنوي لجريمة خيانة الأمانة في مجال المعاملات الإلكترونية:

جريمة خيانة الأمانة جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي أي علم بعناصر الجريمة وتوافر إرادة تتجه نحو تحقيق السلوك الإجرامي ونتيجته، وفي جريمة خيانة الأمانة كي يتوافر القصد الجنائي يجب أن يعلم الجاني أن ما يستولي عليه هو مال منقول مملوك للغير، وأن تتجه إرادته إلى الاستيلاء على الحيازة الكاملة للشيء والظهور عليه بمظهر المالك أو صاحب الحق عليه[2].

هذا فيما يتعلق بالقصد العام أما القصد الخاص فقد ثار بشأنه خلاف فقهي حول مدى ضرورة توافره لذلك سنتناول هذا الركن من خلال التطرق للقصد العام ثم الخلاف الفقهي الذي دار بشأن القصد الخاص.

1- القصد العام:

أ- العلم: علم الجاني بصفة المال مفترض في جانبه لأنه علم بفكرة قانونية جنائية، أما العلم بملكية الغير وبأنه سلم إليه على وجه الأمانة وعلى سبيل الحيازة الناقصة فيقبل الاعتذار بالجهل بشأنها مما ينفي القصد الجنائي إذا ثبت فعلا[3]

1- د/ جميل عبد الباقي الصغير، المرجع السابق، ص115 .
2- د/ علي عبد القادر القهوجي، شرح قانون العقوبات القسم الخاص، المرجع السابق، ص 390.
3- د/ عبد القادر القهوجي، ص 390.

لذلك يجب أن يكون الجاني على علم بأنه تسلم الشيء تسليما ناقلا للحيازة الناقصة، فإذا اعتقد أنه تسلمه على سبيل الحيازة الكاملة فإن القصد الجنائي ينتفي، كما يجب أن يكون الجاني على علم أن التسليم قد تم بناءا على عقد من عقود الأمانة، وكذلك أن من شأن فعله ترتيب ضرر سواء محققا أو محتملا، فمن يستعمل الشيء و لم يدر بخاطره أن من شأن هذا الاستعمال الإضرار بصاحبه ويكون هذا الاستعمال بدون إذن ويتعرض الشيء لظروف شاذة تؤدي إلى هلاكه كمن يستعمل النظام المعلوماتي ويحدث ارتفاع مفاجئ في التيار الكهربائي يؤدي إلى هلاك النظام فهو لا يسأل عن خيانة الأمانة. [1]

كما يمكن أن يتحقق هذا العنصر في الشخص الذي يتسلم بطاقة الائتمان ثم يرفض إرجاعها للبنك، فالتسليم هنا هو ناقل للحيازة الناقصة بناء على عقد من عقود خيانة الأمانة ألا وهو عقد عارية الاستعمال، فالجاني هنا يعلم أن التسليم تم بناء على عقد من عقود الأمانة ويعلم أيضا أن عدم إرجاعه للبطاقة فيه ضرر للبنك وبالتالي يتحقق عنصر العلم لدى الجاني.

ب- الإرادة: لاكتمال القصد العام يجب أن تتجه نية الجاني إلى الاستيلاء على المال والظهور عليه بمظهر المالك، فلا ينفي هذا القصد اتجاه نية الجاني إلى رد المال بعد ذلك أو يكون قد رده فعلا أو يحرر على نفسه إقرارا يلتزم فيه الرد[2] فالإرادة تتحقق متى اتجهت نية الجاني إلى تغيير صفة الحيازة من حيازة ناقصة إلى حيازة كاملة عن طريق القيام بإحدى الصور الثلاث للسلوك الإجرامي، والمتمثلة في الاختلاس أو الاستعمال أو التبديد، وأن تتجه هذه الإرادة إلى ترتيب ضرر محقق أو محتمل الوقوع نتيجة لهذا الفعل.

فالقصد الجنائي يتوافر في حق الجاني الذي يعطي للغير اسطوانات مسجل عليها برامج أو معلومات لينسخها ويعيدها فيحتفظ بها لنفسه ويحول حيازتها من حيازة مؤقتة إلى حيازة كاملة ذلك أن هذه الأشياء سلمت إلى الجاني لممارسة نشاط محدد لحساب صاحب المشروع او لحساب صاحب الحق عليها، وكذلك يتحقق القصد الجنائي في حق الجاني الذي يعلم بالضرر الذي ينجم عن تلاعبه في البرامج أو المعلومات التي يكون له حق الدخول إليها والتعامل معها بحكم عمله خاصة فيما يتعلق بإفشاء المعلومات السرية أو في حالة الاستيلاء على أموال الغير[3].

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 802.
2- د/ علي عبد القادر القهوجي، شرح قانون العقوبات القسم الخاص، المرجع السابق، ص 391.
3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 802.

2- القصد الخاص:

ثار خلاف في الفقه حول مدى ضرورة وجود قصد خاص بجانب القصد العام في جريمة خيانة الأمانة، فذهب بعض الفقه إلى ضرورة تطلب قصد خاص و الذي يتمثل في انصراف نية الجاني إلى تملك المال وإضافته إلى ملكه، فإذا كان قصد الجاني منصرف إلى مجرد استعمال المال فقط فلا جريمة في الأمر، أضاف هذا الاتجاه أن القصد الخاص يتمثل في نية التملك وحرمان صاحب المال من التصرف فيه وظهور الجاني عليه بمظهر المالك، لذلك فهذه النية شرط ضروري ولازم في هذه الجريمة، كما أن خيانة الأمانة تعد من جرائم الأموال مثل السرقة والنصب فكلها ترجع إلى أصل واحد ويجمعها قصد واحد وهو إرادة تملك المال وحرمان صاحبه منه[1].

في حين ذهب جانب آخر من الفقه مع تسليمه بأهمية توافر نية التملك لكن يبقى مع ذلك أن القصد المطلوب هو القصد العام فقط، رغم اشتراط توافر النية، فالركن المادي للجريمة في صوره الثلاث لا يتوافر إلا إذا كان نشاط الجاني معبرا عن نية تغيير الحيازة على الشيء من حيازة ناقصة إلى حيازة كاملة، فنية التملك متصلة تماما بالركن المادي للجريمة ولا يتوافر بها القصد الجنائي[2]

وذلك ما نؤيده كون اشتراط نية التملك سينفي قيام الجريمة في حالة ما إذا قام الجاني باستخدام المال لمصلحته ثم إعادته إلى صاحبه، لذلك نرى أنه في مجال المعاملات الإلكترونية يشترط توفر القصد العام دون الخاص ذلك أن النشاط الإجرامي في هذه الجريمة يكون دائما متبوع بنية تغيير الحيازة، ففعل الاختلاس على سبيل المثال لا يتجسد إلا بتوفر نية التملك لذلك فهذه النية نجدها دائما متبوعة بالركن المادي لهذه الجريمة، فمن يقوم باختلاس برنامج معلوماتي الذي حصل عليه بمقتضى عقد من عقود الأمانة فإن نيته في تملك ذلك البرنامج يمثلها النشاط الإجرامي ذاته والمتمثل في فعل الاختلاس.

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص799
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 800.

المبحث الثاني

الحماية الجنائية للمعاملات الإلكترونية من خلال تجريم الاتفاق أو الشروع في الجرائم المعلوماتية

تطرقنا في كل من الفصل الأول والثاني لهذه الرسالة لأهم الجرائم التي يمكن أن تقع في مجال المعاملات الإلكترونية ويمكن القول أن جل الجرائم يمكن أن نجدها في المجال المعلوماتي فبغض النظر عن الجرائم المعلوماتية الواقعة على أموال الأشخاص فقد اتسعت تلك الجرائم لتهدد حريات الناس وحياتهم الخاصة والسبب في ذلك يرجع لاتساع نطاق المعاملات الإلكترونية حيث أصبحت في الدول المتقدمة شيء بديل للمعاملات العادية.

ولم تكتف بعض الدول من تجريم أفعال قد تقع على النظام المعلوماتي أو المعاملات الإلكترونية بصفة عامة بل عاقبت حتى على الاتفاق السابق لتلك الجرائم أو الشروع فيها وذلك لزرع الرهبة والردع في نفوس مجرمي المعلوماتية والحيلولة دون ارتكاب تلك الجرائم، فقام المشرع الفرنسي على سبيل المثال بتجريم الشروع في جرائم المعطيات، وذلك ما سار عليه المشرع الجزائري وإن كان هذا الأخير لا يعاقب على الشروع إلا في الجنح التي يقدر خطورتها، ومن ثم فإننا نلمس مدى رغبة المشرع الجزائري في مكافحة هذه الجرائم.

فالعقاب على الاتفاق الجنائي أو الشروع يغلق باب كل الجرائم سواء الماسة بأنظمة المعالجة الآلية للمعطيات أو الإتلاف أو التزوير أو السرقة... لذا ارتأينا تناول كل من الاتفاق والشروع على الشكل التالي:

المطلب الأول: الحماية الجنائية للمعاملات الإلكترونية من خلال تجريم الاتفاق على ارتكاب الجرائم المعلوماتية.

المطلب الثاني: الحماية الجنائية للمعاملات الإلكترونية من خلال تجريم الشروع في الجرائم المعلوماتية

المطلب الأول

الحماية الجنائية للمعاملات الإلكترونية من خلال تجريم الاتفاق على ارتكاب الجرائم المعلوماتية

قبل التفصيل في هذا العنصر نتطرق أولا للجدل الفقهي الذي دار حول مدى ملائمة تجريم المشرع للاتفاق الجنائي من عدمه، حيث ظهر هناك اتجاهان:

فذهب اتجاه إلى القول أن الاتفاق الجنائي عزم إجرامي، وتجريمه لا يعتبر استثناء يرد على قاعدة عدم العقاب على مجرد العزم الإجرامي، ويستند هذا الرأي إلى أن المشرع لا يعاقب على الاتفاق الجنائي كخطوة للجريمة المتفق عليها وإنما يعاقب عليه في حد ذاته كجريمة خاصة تامة وتبرير المعاقبة عليه أنه في الاتفاق الجنائي يظهر العزم الجنائي الجماعي بمظهر خارجي مادي لأن كل عضو فيه يعلن عزمه إلى سائر الأعضاء فتتحد إرادتهم على ارتكاب الجريمة، وبذلك يكون الاتفاق معلوما ويمكن إثباته، ومن جهة ثانية الاتفاق الجنائي ظاهرة خطرة تهدد الأمن العام تهديدا فعليا، كما أن هدف المشرع من العقاب على الاتفاق هي الوقاية حيث أن إحباط الاتفاق الجنائي نتيجته هي الحيلولة بين الجناة وتحقيق خططهم الإجرامية[1].

في حين يرى اتجاه آخر أن تجريم مجرد الاتفاق فقط ستكون له انعكاسات سلبية، ذلك لما يخلقه من دفع للمجرمين بإتمام ما تم الاتفاق عليه نظرا لأن اتفاقهم قد تم تجريمه حيث أن العدل عن هذا الاتفاق وفقا للرأي السابق لا يمنع من تقرير العقوبة، لأن الاتفاق حسبهم جريمة مستقلة بذاتها لذلك ذهب هذا الاتجاه للقول بأن حجج الرأي السابق غير قويمة ويكفي لدحضها جميعا المقارنة بين خطورة الاتفاق الجنائي على نحو ما صوره أصحاب الاتجاه السابق، وبين خطورة الأعمال التحضيرية التي تصدر عن شخص يسعى إلى ارتكاب الجريمة بمفرده، فالاتفاق الجنائي في مرحلة مبكرة بالنسبة للتحضير للجريمة إذ أنها ترد إلى المرحلة النفسية أي إلى مرحلة اتخاذ القرار وعقد العزم على ارتكاب الجريمة، بينما يعقب التحضير للجريمة هذه المرحلة النفسية لهذا لو صحت

1- محمد خليفة، المرجع السابق، ص 112.

خطورة الاتفاق الجنائي تبريرا لمعاقبة المتفقين في هذه المرحلة المبكرة من المراحل التي تمر بها الجريمة لوجب على المشرع أن يجرم مرحلة التحضير للجريمة من باب أولى[1].

وذلك ما سار عليه المشرع الجزائري والفرنسي من خلال اشتراطهما أن يكون التحضير مجسدا بأفعال مادية، أي تجنب المشرع العقاب على المرحلة النفسية، وذلك ما نص عليه في جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات.

وللإحاطة أكثر بجريمة الاتفاق الجنائي في مجال المعاملات الإلكترونية نتناولها من خلال التطرق لكل من الركنين المادي والمعنوي لهذه الجريمة.

الفرع الأول: الركن المادي للاتفاق الجنائي

لتناول الركن المادي لهذه الجريمة نتطرق لثلاث عناصر تتمثل في فعل الاتفاق وموضوع الاتفاق وتعدد المتفقين.

أولا: فعل الاتفاق:

تنص المادة 176 عقوبات جزائري "كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه تشكل وتؤلف بغرض الإعداد لجناية أو أكثر، أو لجنحة أو أكثر معاقب عليها بخمس سنوات حبس على الأقل ضد الأشخاص أو الأملاك تكون جمعية أشرار وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل" والمشرع الجزائري لم يخضع فعل الاتفاق في مجال المعاملات الإلكترونية لنص المادة السابقة الذكر وإنما أخضع الفعل لنص المادة 394 مكرر 5 عقوبات[2].

وعلى كل يستشف من نص المادة 176 عقوبات جزائري أن فعل الاتفاق هو انعقاد إرادتين أو أكثر واجتماعهما على موضوع معين، والاتفاق بطبيعته له مظهر مادي ملموس إذ يفترض تعبير كل واحد من أطرافه عن إرادته بحيث يعلم بها زملاؤه في الاتفاق فيتحقق لهم أن إرادتهم تسير في اتجاه واحد وتتلاقى عند موضوع معين، والتعبير عن الإرادة يفترض ماديات

1- محمد خليفة، المرجع السابق، ص 113.
2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 130.

كالقول الشفوي أو العبارات المكتوبة أو الإيماء إن كانت لها دلالة مفهومة، والاتفاق يقوم بغض النظر عما استغرقه انعقاد الإيرادات من وقت قصيرا كان أم طويل وسواء كان الاتفاق منظما مفصلا فيتخذ شكل الجمعية الإجرامية، أو كان عارضا مجملا اقتصر أعضاؤه على مجرد العزم على جريمة معينة دون تعيين لكيفية تنفيذها أو تحديد لكل دور منهم فيها[1].

هذا فيما يتعلق بفعل الاتفاق حسب نص المادة 176 عقوبات جزائري، لكن المادة 394 مكرر 5 لم تكتف بمجرد الاتفاق بل اشترطت أن يكون التحضير أو الاتفاق مجسدا بفعل أو عدة أفعال مادية، حيث تنص المادة 394 مكرر 5 قانون العقوبات على: "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 عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها" وهذه المادة تقابل المادة 4/323 عقوبات فرنسي[2] فنص المادة يشترط ضرورة توافر أعمال مادية تحضيرية تعقب الاتفاق، أي أن تتجسد المرحلة النفسية المتمثلة في الاتفاق في شكل مادي يتمثل في أعمال تحضيرية.

ونظرا لأن مفهوم المادية يثير صعوبة في جرائم الغش المعلوماتي فقد حدث بشأنها خلاف فقهي في ما مدى إعتبار الأعمال المادية قد تتحقق فقط في صورة بدء تنفيذ الأعمال التحضيرية؟

يرى بعض الفقه أنه من الواجب إعطاء مفهوم أوسع للمادية حيث أن مجرد تبادل المعلومات في صورة مناسبة يعد كافيا لتحقيق هذه الجرائم[3]

ومن أمثلة الأعمال التحضيرية في مجال المعلوماتية تبادل المعلومات الهامة لارتكاب الجريمة كالإعلان عن كلمة المرور Mot de Passe أو رمز الدخول Code d'accès ...الخ[4]

1- محمد خليفة، المرجع السابق، ص 114.

2- Art323/4 :« la participation à un groupement formé ou à une entente, établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée » code pénale français .

3- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 1021.

4- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 132.

ومن جانبنا نرى ضرورة تأييد الرأي الفقهي القائل بتوسيع نطاق المادة ليدخل في نطاقه مجرد تبادل المعلومات متى كان لها دور في الجريمة.

كما أن فعل الاتفاق يمكن أن يمتد ليشمل كل من يساهم في المساعدة أو الاتفاق، الأمر الذي يجعل من الممكن أن تكون هناك جماعة مساهمة في تحقيق هذه الجرائم شرط أن تمارس نشاط إيجابي، وفي هذه الحالة فإن العقاب لن يشمل رئيس الجماعة فقط بل الجماعة ككل[1].

ومن خلال ما سبق تجدر الإشارة إلى انه يجب التمييز بين الركن المادي لجريمة الاتفاق والركن المادي للجريمة المتفق عليها، لأن الركن المادي للأولى يستكمل عناصره بتوافر الإرادات ولو لم تنفذ الجريمة المتفق عليها، وأن عدولهم عن تنفيذ الجريمة المتفق عليها لا يحول دون العقاب على جريمة الاتفاق الجنائي، لأن هذا العدول لا يمس الركن المادي الذي توافرت كل عناصره.

ثانيا/ موضوع الاتفاق:

يستمد الاتفاق صفته الجنائية من موضوعه فإذا لم تكن لموضوعه صفة إجرامية أي كان فعلا مشروعا و لم تكن له صلة بجريمة ما، فليس الاتفاق جنائيا والملاحظ أن نص المادة 176 في قانون العقوبات الجزائري، الذي نص على الاتفاق الجنائي العام في الجنايات ضد الأشخاص و الأموال يجرم الاتفاق المنصب على ارتكاب جريمة أو الإعداد لها، بينما اقتصر نص المادة 394 مكرر 5 المجرم للاتفاق في جرائم المعطيات على جعل موضوع الاتفاق الإعداد لتلك الجرائم والتحضير لها فقط و لم ينص على الاتفاق على ارتكابها[2]

والجنح التي يشكل تحضيرها هدف الاتفاق المنصوص عليه بالمادة 394 مكرر 5 قانون العقوبات هي الجنح الماسة بالأنظمة المعلوماتية، وعليه لا يعاقب استناد لهذا النص الاتفاق بهدف ارتكاب جنحة تقليدا لبرامج المعاقب عليها بنصوص حق المؤلف والحقوق المجاورة[3]

1- د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 1021.
2- محمد خليفة، المرجع السابق، ص 115.
3- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 132.

ووفقا للمادة 394 مكرر 5 فإنه إذا كان موضوع الاتفاق أعمال التحضير والإعداد لتلك الجرائم فإن الاتفاق يكتسب صفته الجنائية ولو كانت الأعمال في ذاتها مشروعة، فالاتفاق على تعليم كيفية تصميم المعطيات وتجميعها ونشرها هو مشروع في الأصل، لكنه يصبح غير مشروع إذا كان الاتفاق على تعليم ذلك بغية استعماله في الجرائم التي تنص عليها المادة 394 مكرر(01/02) [1].

وموضوع الاتفاق أو محله الذي نصت عليه المادة 394 مكرر 05 هو الإعداد لأي من الجرائم التي نصت عليها المواد 394 مكرر والخاصة بالدخول والبقاء غير المصرح بهما والمادة 394 مكرر 01 والخاصة بالتلاعب بالمعطيات و394 مكرر 02 المتعلقة بالمساس بحقوق الأشخاص عن طريق المعلوماتية، كجمع المعلومات أو نشرها أو الاتجار فيها أو إفشائها.

فالاتفاق يكون بهدف التحضير لارتكاب إحدى الجرائم المنصوص عليها والمتعلقة بالمعلوماتية، ويترتب على ذلك أنه يخرج من إطار تطبيق هذا النص حالة النوادي المعلوماتية، حيث أن هذه النوادي يمارس داخلها الأعضاء هواياتهم المتصلة بالمعلومات بطريقة قد توحي في بعض الأحيان بأنها تنم عن الاتفاق لارتكاب جريمة أو المساعدة على ارتكابها، ويرجع عدم تطبيق هذا النص عليها لأن هذا الاتفاق لا يتم بقصد ارتكاب أحد هذه الجرائم، ومن جهة أخرى فإنه لا مجال لتطبيق هذا النص إذا كان الاتفاق قد تم بغرض ارتكاب جريمة معلوماتية غير واردة بالنصوص المعنية في قانون العقوبات الفرنسي (المواد من 323-1 حتى 323-3)[2]

والمواد السابقة الذكر تقابلها المواد "394 مكرر إلى 394 مكرر 2" من قانون العقوبات الجزائري.

ثالثا/ تعدد الجناة:

جريمة الاتفاق تتطلب تعددا ضروريا للجناة والحد الأدنى لهذه التعداد هو شخصان بينما لا يرد قيد على الحد الأقصى حسب نص المادة 176 عقوبات جزائري، ومن القوانين من يتطلب

1- محمد خليفة، المرجع السابق،ص 115.
2- د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 1020

ثلاثة أشخاص كالقانون الإيطالي ويشدد العقوبة إذا بلغ عشرة فأكثر[1]، ويستوي أن يكون أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي أو جماعة، كما يستوي أن يعرف أشخاص الاتفاق بعضهم البعض كما في العصابة أم تكون مجرد مجموعة من الأشخاص لا يعرف أحدهم الآخر من قبل ولكن اتفقوا فيما بينهم على القيام بالنشاط الإجرامي، والمهم في ذلك أن يتم الاتفاق بين شخصين على الأقل، فإذا ارتكب العمل التحضيري المادي شخص واحد بمفرده وبمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر[2]

ويجب أن يكون الشخصان المتفقان مسئولين جنائيا، فإذا كان أحدهما غير مسئول جنائيا كأن يكون صغيرا أو فاقدا للإدراك والتمييز لتعاطيه مسكرا دون علم منه أو مجنونا فالاتفاق لا يقوم، أما العذر المحل من العقاب الذي يتمتع به أحد الشخصين المتفقين فلا يحول دون قيام الاتفاق لأن هذا العذر لا ينفي المسئولية الجنائية لهذا يبقى المتفق الآخر معاقبا وحده على اتفاقه[3]

الفرع الثاني: الركن المعنوي للاتفاق الجنائي

جريمة الاتفاق جريمة عمدية لابد لقيامها من توافر القصد الجنائي وهذا الأخير يقوم على العلم والإرادة.

أولا/ العلم:

يجب أن يعلم كل عضو في الاتفاق بماهية الفعل أو الأفعال موضوع الاتفاق وبما لها من خصائص التي يعتمد عليها المشرع في إضفاء الصفة الإجرامية عليها، ولا يتطلب العلم بالصفة الإجرامية ذاتها للفعل لأن ذلك أمر مفترض على نحو لا يقبل إثبات العكس، ويترتب على ذلك أن من يجهل الغرض من الاتفاق وهو ارتكاب جناية أو جنحة أو التحضير لهما لا يعد القصد الجنائي متوافرا لديه، فمن ينضم إلى اتفاق معتقدا أنه للاتجار في برامج حاسب آلي ومعطيات عادية ثم

1- محمد خليفة، المرجع السابق، ص 115.
2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 131.
3- محمد خليفة، ص 116.

يتبين أن الاتجار كان ببرامج خبيثة أو برامج اختراق فمثل هذا لا يعد القصد الجنائي متوافرا لديه وذلك لانتفاء علمه بموضوع الاتفاق الجنائي لكن القصد الجنائي يتوافر لدى هذا الشخص إذا علم بعد دخوله الاتفاق بموضوعه الغير مشروع ومع ذلك بقي في الاتفاق[1] فيجب أن يكون الشخص على وعي بأنه يساهم في مساعدة ما بغرض ارتكاب إحدى الجرائم المنصوص عليها[2].

ثانيا - الإرادة:

لابد أن تتوافر الإرادة الجادة لشخصين على الأقل للدخول في الاتفاق أي إرادة كل واحد أن يكون طرفا في هذا الاتفاق وأن يقوم بالدور الذي سيعهد به إليه فلابد أن تكون هذه الإرادة جادة، فالذي يدخل الاتفاق بقصد الوشاية ببقية المتفقين أو للإطلاع على أمرهم أو لمجرد العبث لا يعد القصد الجنائي متوفر لديه لغياب الإرادة الجادة ولابد من توافر هذه الإرادة لدى شخصين على الأقل[3].

إذن يجب أن تتجه إرادة كل عضو إلى تحقيق نشاط إجرامي معين يتمثل في العمل التحضيري لتلك الجريمة أي النشاط المادي لفعل الاتفاق، ومما سبق تناوله في الركن المادي أو الركن المعنوي يتبين أن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية، هو أن مثل هذه الجرائم تتم عادة في إطار مجموعات كما أن المشرع ورغبة في توسيع نطاق العقوبة أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي، بمعنى آخر 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[4]، كما أن

1- محمد خليفة، المرجع السابق، ص 117.
2- د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 122.
3- محمد خليفة، ص 117.
4- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص 130.

العقوبة تطبق في حالة عدم إتمام الجريمة التي تم الإعداد لها وذلك استنادا إلى أن جريمة الاتفاق تعد جريمة مستقلة بذاتها عن الجرائم الأخرى وتقوم من مجرد الاتفاق دون الإتمام[1].

ومما سبق يمكن القول أن شروط العقاب على الاتفاق الجنائي تتمثل في:

1. تطلب الاتفاق المنشئ وذلك بتوفر شخصين أو أكثر.
2. أن يكون الاتفاق بهدف التحضير لإحدى الجرائم المنصوص عليها على سبيل الحصر.
3. يجب تجسيد الاتفاق في شكل مادي.
4. ضرورة مشاركة الأعضاء في الاتفاق.
5. توفر القصد الجنائي.

فإذا توافرت الشروط السابقة الذكر فإن المتهم يعاقب بذات العقوبة المقررة للجريمة التي تم الإعداد لها.

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 122.

المطلب الثاني

الحماية الجنائية للمعاملات الإلكترونية من خلال تجريم الشروع في الجرائم المعلوماتية

إذا كانت العلة من العقاب على أية جريمة هي أنها تحقق عدوانا على المصالح محل الحماية القانونية فإن العلة من العقاب على الشروع بوصفه جريمة لابد أن تتمثل في تحقيق ذلك العدوان وكل ما هنالك أن العدوان يأخذ في الشروع صورة الخطر الذي يهدد المصالح القانونية، ذلك أن الشارع لا يحمي المصالح القانونية من الضرر الذي يترل بها فيقضي عليها جزءا أو كلا فحسب وإنما يوفر لها حماية لإزالة الخطر الذي يهدد المصلحة لاحتمال القضاء عليها كلها، فلقد ثبت أن خطر الجريمة لا يقتصر على ما تحدثه من ضرر مادي بالفرد بل يتعدى ذلك إلى ما تحدثه من قلق واضطراب في الجماعة أيضا[1].

ومن المعلوم أن نظام الشروع مجاله الأصلي هو الجنايات أما في الجنح فلا يكون إلا في الخطيرة منها، وقد تعرض المشرع الجزائري للشروع تحت عنوان المحاولة، وذلك في المادة 30 قانون العقوبات حيث نص على: "كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها"

ونصت المادة 31 عقوبات على "المحاولة في الجنحة لا يعاقب عليها إلا بناء على نص صريح في القانون والمحاولة في المخالفة لا يعاقب عليها إطلاقا" ونظرا لخطورة الجرائم المعلوماتية فقد أخضعها المشرع لنظام الشروع وذلك في نص المادة 394 مكرر 7 حيث نصت على: "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقرر للجنحة ذاتها" وهذه المادة تقابل المادة 323-7 عقوبات فرنسي [2]

1- محمد خليفة، المرجع السابق، ص 117.

2 - Art323/7 : « la tentative des débits prévus par les articles232/1à323-3-1 est punie des mêmes peines » . code pénale français

ونظرا لما تتمتع به الجرائم المعلوماتية من خطورة فقد أخضعها المشرع الجزائري لنظام الاتفاق الجنائي المجسد بأعمال مادية ثم أخضعها لنظام الشروع أيضا.

لذلك سنتطرق في هذا المطلب لأركان الشروع ثم للشروع في الاتفاق الجنائي وذلك على الشكل التالي:

- **الفرع الأول**: أركان الشروع
- **الفرع الثاني**: الشروع في الاتفاق

الفرع الأول: أركان الشروع

نتناول في هذا الفرع كل من الركن المادي والركن المعنوي لهذه الجريمة.

أولا/ الركن المادي:

يتمثل الركن المادي للشروع في الأفعال المادية التي تمر بها هذه الجريمة، أي المراحل المجسدة في نشاط مادي دون المعنوي فمرحلة التفكير في الجريمة لا عقاب عليها، فمن يفكر في ارتكاب جريمة من الجرائم المعلوماتية سواء بالإتلاف أو التزوير أو أي جريمة معلوماتية أخرى، وكانت هذه الجريمة في مرحلة التفكير وطي الكتمان دون أن تتخذ مظهرا خارجيا بارتكاب أي فعل يقع تحت طائلة القانون كالبدء في التنفيذ أو غير ذلك من الأعمال الخارجية فإن الفعل يخرج عن دائرة التجريم والعقاب، وهو ما ينطبق أيضا على مرحلة التحضير للجريمة فهي كمرحلة التفكير لا عقاب عليها ما لم تشكل هذه الأعمال جريمة قائمة بذاتها مستقلة، كمن يحوز سلاحا ناريا بدون ترخيص للتحضير لجريمة قتل، فالعقاب هنا يستند على جريمة حيازة سلاح ناري بدون ترخيص، وفي نطاق المعلوماتية قد يقوم الجاني بإعداد تجهيزات لارتكاب جريمة من جرائم الاعتداء على نظم المعلوماتية، كإعداد البرامج المستخدمة كالفيروس أو برامج معدة للقرصنة المعلوماتية أو لسرقة المعلومات بطريقة النسخ غير المشروع عن طريق النهايات الطرفية للشبكة المعلوماتية، أو إعداد مادة حامضة لوضعها على الشرائط الممغنطة لتلفها، والقاعدة العامة هنا أنه لا عقاب على هذه الأعمال لأنها لا تعد شروعا[1].

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 1012.

لكن الأفعال السابقة الذكر متى تجسدت في شكل مادي، أي أن يكون ذلك التحضير متبوعا بأعمال مادية فإنه يدخل في نص المادة 394 مكرر 5 حيث يتخذ ذلك التحضير صورة الاتفاق الجنائي، ويجد الركن المادي للشروع ضالته في مرحلة البدء في التنفيذ ففي هذه المرحلة يبدأ الجاني في تنفيذ الجريمة بالقيام بفعل مادي في سبيل تنفيذ الجريمة، فإذا تمكن الجاني من تحقيق النتيجة الإجرامية فإن الجريمة تكون قد وقعت تامة، وإذا لم يتمكن من تحقيق النتيجة لظرف طارئ خارج عن إرادته فإن الشروع يكون متحققا في هذه الحالة، وإذا عدل الجاني عن نشاطه الإجرامي بإرادته فإن هذا يعد عدولا اختياريا ولا عقاب على ذلك، وقد يحدث العدول الاختياري في نطاق المعاملات الالكترونية كما لو قام الجاني بإعداد الأجهزة التي سوف يستخدمها في جريمة تزوير مستند معالج آليا أو برنامج محضر للاعتداء على شبكة معلوماتية، وقبل أن يدخل بفعله حيز التنفيذ يعدل عن الجريمة بإرادته الحرة فلا عقاب في هذه الحالة[1].

ومعيار البدء في تنفيذ الجريمة وفقا للمذهب الموضوعي هو البدء في ارتكاب الفعل المادي الذي يقوم به الركن المادي للجريمة، فمثلا في جريمة السرقة في نطاق المعاملات الالكترونية فإن معيار البدء في التنفيذ بالنسبة لسرقة الدعامات أو البرامج يكون بالبدء بفعل الاختلاس للبرامج أو الدعامات وكذلك في الإتلاف فإن البدء في التنفيذ يبدأ بإدخال برنامج الفيروس على الشبكة المعلوماتية المراد إتلافها.

أما معيار البدء في التنفيذ في نطاق المعاملات الالكترونية وفقا للمذهب الشخصي فإنه يعتد بإرادة الجاني، فالخطورة نابعة من شخص الجاني لإتمام الجريمة كما لو وضع الجاني برنامج فيروسي لتدمير شبكة معلوماتية مرتبطة بالانترنيت فيجب البحث عن الغرض من فعله واتجاه نيته[2]

فالشروع جريمة ناقصة وهذا النقصان لا يعتري الركن المعنوي فيها لأن القصد ثابت لدى الفاعل وإنما يعتري الركن المادي لأن الفاعل يقدم على أفعال تعتبر بدءا في التنفيذ لكنه لا يتمكن من تحقيق النتيجة لأسباب خارجة عن إرادته[3].

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص114
2- د/ عمر أبوا الفتوح عبد العظيم الحمامي، ص 114.
3- محمد خليفة، المرجع السابق، ص 118.

ثانيا/ الركن المعنوي:

يتمثل القصد الجنائي في الشروع في ارتكاب جريمة تامة بركنيها المادي والمعنوي وعلى ذلك لا يكفي في هذا المقام توافر الركن المادي فقط وإنما يلزم مع ذلك توافر الإرادة التي تنصرف إلى ارتكاب الجريمة، ويشترط في هذا القصد أن يكون معاصرا للبدء في التنفيذ فلا يعتد بالقصد السابق أو اللاحق على هذه المرحلة[1]

ويشترط في الركن المعنوي للشروع أن تكون نية الجاني قد اتجهت إلى تحقيق جريمة معينة وفي مجال المعاملات الإلكترونية أن تتجه نيته إلى إحداث جريمة من الجرائم المنصوص عليها في قانون العقوبات الجزائري على سبيل المثال، والتي وردت على سبيل الحصر في المواد 394 مكرر إلى 394 مكرر 2" عقوبات جزائري، وعلى ذلك فإنه لا يتصور الشروع في حالة قيام عامل بإتلاف بعض البيانات عن طريق الخطأ وذلك أثناء أدائه لوظيفته والعلة في ذلك أن النتيجة المتحققة لم يكن يريدها العامل المتسبب فيها.

وبعد التطرق للركن المادي والمعنوي للشروع تجدر الإشارة لنقطة مهمة لهذه الجريمة وذلك أثناء وقوعها على الجرائم المعلوماتية، فالشروع وفقا للقواعد العامة غير متصور في الجرائم الشكلية، والمعلوم أن جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي هي جريمة شكلية حيث لا يتطلب لتمامها نتيجة معينة فمجرد الدخول أو البقاء يعد جريمة، أما الجرائم الواقعة بعد الدخول أو البقاء كتغيير المعطيات أو حذفها فقد اعتبرها المشرع كظرف مشدد فبالرغم من أن هذه الجرائم جرائم شكلية إلا أن المشرع وضع للشروع فيها عقوبة تساوي عقوبة الجريمة ذاتها، والسبب في ذلك هو رغبة المشرع في توسيع نطاق العقوبة لتشمل العديد من الأفعال الماسة بالأنظمة المعلوماتية، ورغبة من المشرع أيضا في حماية المعاملات الإلكترونية نظرا لما تمتاز به من خصائص تختلف عن المعاملات العادية وذلك لما قد تلحقه من أضرار اقتصادية كبيرة نتيجة التعدي عليها، فالمشرع لا يقرر نظام الشروع في جنحة إلا إذا لمس خطورتها وما يمكن أن تؤدي إليه من أضرار حال تمامها، وتبدو رغبة المشرع كبيرة في حماية المعاملات الإلكترونية وذلك في خروجه عن المبدأ العام لنظام الشروع حيث تكون عقوبته أقل في مقدراها عن عقوبة الجريمة التامة إلا أنه

1- د/ عمر أبوا الفتوح عبد العظيم الحمامي، المرجع السابق، ص 117.

في مجال المعاملات الإلكترونية ساوى بين عقوبة الشروع وجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

الفرع الثاني: الشروع في الاتفاق

تكلم المشرع الجزائري عن جرائم المعطيات وتناول معها جريمة الاتفاق الجنائي ثم أنهى النصوص العقابية بالنص على تجريم الشروع في الجرائم السابقة، فهل يمكن القول بوجود شروع في الاتفاق الجنائي؟

يذهب الرأي السائد في الفقه بالقول بأنه لا يوجد شروع في الاتفاق الجنائي مستندا في ذلك على:

- أن الاتفاق حالة نفسية تتم بتلاقي الإرادات ولا تحمل بداية ولا نهاية فهو لا يقع إلا كلاما ولا يحتمل بدءا في التنفيذ.
- ذهب بعض الفقه المصري للقول بأن الدعوة إلى الاتفاق لا تعد شروعا وإنما يعاقب عليها كجريمة قائمة بذاته[1].

وهناك رأي مخالف يرى غير ذلك متحججا بأنه طالما كانت أركان الشروع متصورة و لم يكن القانون متضمنا نصا خاصا يقضي بعدم العقاب عليه فلا وجه للقول بالرأي السابق، وأنه ليس صحيحا أن الشروع في الاتفاق غير متصور إذ الدعوة إليه أو الحمل عليه بدء في التنفيذ وفقا للمذهب الشخصي، فإذا توافر القصد الجنائي و لم يتم الاتفاق لأسباب لا دخل لإرادة الجاني فيها فالعقاب على الشروع متعين إذا كان الاتفاق جناية إذ لا يتطلب العقاب نصا خاصا وإذا كان الاتفاق جنحة فلابد من وجود هذا النص[2].

ومن خلال استقراء نص المادة 394 مكرر 7 عقوبات جزائري نستنتج أن الجنحة الواردة بنص المادة 394 مكرر 5 عقوبات جزائري يشملها نص المادة 394 مكرر 7 أي أن المشرع الجزائري أخذ بفكرة الشروع في الاتفاق الجنائي، أي تصور قيام الشروع في جنحة الاتفاق الجنائي، وهذا المسلك منتقد لدى البعض فإذا كان تجريم الاتفاق الجنائي في حد ذاته منتقدا وقد

1- محمد خليفة، المرجع السابق، ص118
2- محمد خليفة، ص 118.

حكم بعدم دستوريته في مصر وأنه يعاقب على مجرد العزم، فإن العقاب على مجرد الشروع في هذا الاتفاق أو العزم على العزم إن صح التعبير هو منتقد بصورة أشد لأن المشرع بهذا يقوم بالتجريم في مرحلة متقدمة جدا وهي الإرادة، هذه الإرادة التي لم تلتق مع إرادات أخرى لأنها لو التقت بإرادات أخرى لكان الاتفاق مكتملا وكأن المشرع بهذا قد اقترب من تجريم مجرد النوايا[1].

لكن ما تجدر الإشارة إليه أن المشرع الجزائري لم يعاقب على الاتفاق في المرحلة الأولى وإنما عاقب على الاتفاق المجسد بأعمال مادية حسب نص المادة 394 مكرر 5 لكن بتبنيه لنظام الشروع بعد الحديث عن الاتفاق الجنائي يمكن القول أن المشرع تبنى فكرة الشروع في الشروع ومن ثم فإننا نقترح أن يخرج المشرع جنحة الاتفاق الجنائي المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات من نطاق الشروع وذلك من خلال تغيير نص المادة 394 مكرر 7 بأن يصبح نصها كالآتي: "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في المواد 394 مكرر إلى 394 مكرر 2 بالعقوبات المقررة للجنحة ذاتها".

ونقترح أيضا أن يتم نفس التعديل على المادة 394 مكرر 5 والتي تتناول الاتفاق الجنائي وذلك لحصر الاتفاق الجنائي على الجرائم الواردة في المواد 394 مكرر إلى 394 مكرر 2.

وفي خاتمة هذا المبحث تجدر الإشارة أن العلة من تناولنا لكل من الاتفاق الجنائي والشروع في الفصل المخصص لجرائم الأموال على الرغم من أن المشرع الجزائري قد تناولهما بنصوص خاصة والمتعلقة بالمساس بأنظمة المعالجة للمعطيات، هي أن كل من الاتفاق الجنائي والشروع يعدان بوابة لكل الجرائم فلا يتصور قيام جريمة في مجال المعلوماتية من دون تخطيط مسبق سواء أكانت تلك الجرائم تتعلق بأنظمة المعالجة الآلية للمعطيات، أو جرائم تمس الأموال المعلوماتية وذلك من خلال التعدي عليها سواء بالسرقة أو النصب.

فالشروع نجده في كل الجرائم سواء الجرائم العادية أو المعلوماتية، لذلك ارتأينا أن نتكلم عن أهم الجرائم الواقعة في مجال المعاملات الإلكترونية ثم نختم الحديث عنها بالتطرق لكل من الاتفاق الجنائي والشروع.

1- محمد خليفة، المرجع السابق، ص 119.

- **خلاصة:**

بالرغم من الفراغ التشريعي الواضح فيما يتعلق بجرائم الأموال فإننا نستطيع القول بإمكانية اعتبار المكونات المعنوية للنظام المعلوماتي محلا لجريمة السرقة وفقا للقواعد العامة، كما يمكن أن تخضع المعلومات المتبادلة إلكترونيا للنشاط الإجرامي لجريمة السرقة، فالإختلاس لا يستهدف الدعامة الخارجية بل المعلومة ذاتها، كما أن الإعتداء على المعاملات الإلكترونية لا يمكن تكييفه اعتداء على وقت الآلة كون القصد الجنائي متجه نحو ما يتم تبادله في هذه المعاملات وليس الآلة التي تحقق ذلك التبادل، وحتى لو تم الإقرار بذلك فهو أمر محسوم كونه لا يتحقق إلا بالدخول في أنظمة المعالجة الآلية للمعطيات وهو فعل مجرم وفق قانون العقوبات الجزائري .

أما فيما يتعلق بجريمة النصب فما يتم تبادله في مجال المعاملاي الإلكترونية من أموال دون المعلومات و البيانات فهو يصلح أن يكون محلا لهذه الجريمة ويخضع لنشاطها الإجرامي، ذلك أن التلاعب في البيانات تتحقق به الطرق الإحتيالية التي من شأنها أن تدفع المجني عليه لتسليم ماله حيث أن خداع النظام المعلوماتي يعتبر خداع لصاحب النظام كون هذا الأخير مبرمج وفقا لرغبة صاحبه.

أما في جريمة خيانة الأمانة فباعتبار أن المعلومات و البيانات محلا لها و تدخل في إطار أغلب العقود المنصوص عليها حصرا في هذه الجريمة فإن التسليم المشترط لتحققها متوافر إعمالا لفكرة التسليم الإلكتروني وهو ما يسمح بتحقق الركن المادي لهذه الجريمة.

وفيما يتعلق بالإتفاق أو الشروع في الجرائم المعلوماتية فقد عالجه المشرع الجزائري و كفل بذلك الحماية للمعاملات الإلكترونية من خلال تجريمه لمجرد البدء في هذه الجرائم، إلا أنه لم يراعي في تلك النصوص أخذه بفكرة الشروع في الإتفاق الجنائي.

خاتمة

بعد أن تناولنا المحاور الرئيسية لهذه الدراسة والمتعلقة بالحماية الجنائية للمعاملات الإلكترونية وقبل التطرق لما توصلنا إليه من نتائج وتوصيات يجدر بنا الحديث عن الصعوبات التي واجهتنا، وفي مقامها الأول طبيعة الموضوع ذاته كونه موضوع فني أكثر منه قانوني.

ذلك ما أدى بالكثير من الباحثين في المجال القانوني للعزوف عن الحديث في هذا المجال، أضف إلى ذلك أن صلب الموضوع ليس تحليلا لتشريعات قائمة بل أكثره عبارة عن اتجاهات فقهية ما يؤدي في النهاية للوقوف على نتائج ذات طبيعة فقهية لا تشريعية وعلى كل فإنه يمكن الوقوف على النتائج والتوصيات التالية:

النتائج:

من موضوع دراستنا تبينت لنا العديد من النتائج والتي من أهمها:

1- أن الجرائم المعلوماتية هي تلك الناتجة عن استخدام المعلوماتية و التقنية الحديثة في أعمال وأنشطة إجرامية، متى مست تلك الأعمال والأنشطة المكونات المادية أو المعنوية للنظام المعلوماتي أو ألحقت أضرارا بالأشخاص.

2- أن توفير الحماية الجنائية للمعاملات الإلكترونية هي الركيزة الأساسية التي تقوم عليها فكرة الحكومة الإلكترونية، هذه الأخيرة التي يكون الهدف من إنشائها هو ربط المواطن بأجهزة الحكومة للحصول على الخدمات بشكل آلي، كما أن إنشاء الحكومة الإلكترونية يخفض كلفة المعاملات الإدارية ويسرع في وتيرتها ويحسن أداءها ولن يتأتى ذلك ما لم تكن هناك حماية قانونية تجرم الاعتداء على تلك المعاملات.

3- فيما يتعلق بالنصوص المستحدثة في هذا المجال فإن أهم نتيجة تتمخض عنها هو أن إدراج المشرع الجزائري أو الفرنسي لحماية أنظمة المعالجة الآلية للمعطيات، وذلك في القسم المخصص لجرائم الأموال ما هو إلا اعتراف ضمني للمشرع على مالية المكونات المعنوية للنظام المعلوماتي، هذه النقطة التي كانت محل جدل فقهي حول إضفاء وصف المال من عدمه على ما يتم تبادله في

نطاق المعاملات الإلكترونية وبنص المشرع الفرنسي والجزائري عليها في قسم جرائم الأموال هو حسم لذلك الجدل.

4- جريمة الإتلاف تعد من جرائم الأموال وبالرغم من ذلك فقد تناولها المشرع الجزائري والفرنسي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهو ما يعزز رأينا السابق باعتبار المعلوماتية مال مستحدث وجبت حمايته.

5- بتعديل المشرع الجزائري لقانون العقوبات ونصه على تجريم الدخول والبقاء دون إذن في نظام المعالجة الآلية للمعطيات وذلك دون التطرق لبعض الجرائم الأخرى كالسرقة أو النصب ... مرده أن جريمة الدخول والبقاء غير المشروع هي بوابة أغلب الجرائم الواقعة في مجال المعاملات الالكترونية، فاختلاس المعلومات أو إتلافها أو الاحتيال للحصول عليها لا يتم إلا بالدخول في النظام المعلوماتي وبتجريم الدخول الغير مشروع للنظام المعلوماتي يكون المشرع قد غلق باب وقوع جرائم أخرى ولو نسبيا .

6- تبين لنا من خلال الدراسة وجود قصور في النصوص التي إستحدثها المشرع الجزائري والمتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، حيث أنها لا تكفل المعاملات الالكترونية بحماية جنائية من كل الجوانب بل تحميها من بعض الاعتداءات دون الأخرى .

7- فيما يتعلق بنصوص التجريم الكلاسيكية فإننا نسجل عجز أغلب التشريعات العربية في التصدي لهذا النمط المستحدث من الجرائم، ذلك أن الوقت الذي وضعت فيه هذه النصوص لم يكن فيه الإجرام المعلوماتي متفشيا مثلما هو عليه الآن و بالرجوع لما تم تناوله في الموضوع محل البحث فإننا نلحظ أن الحماية التي تقرها نصوص التجريم الكلاسيكية للمعاملات الإلكترونية هي حماية نسبية لا مطلقة، والعلة في ذلك أن تطبيق هذه النصوص على الجرائم المعلوماتية تتعارض في أغلب الأحيان مع مبدأ الشرعية لكننا رأينا في تحليلنا للموضوع أن الاتجاهات المؤيدة لتطبيق تلك النصوص على الجرائم المعلوماتية هي التي تمثل غالبية الفقه والقضاء وسايرنا ذلك لاعتبار أن القول بعدم صلاحية المكونات المعنوية للنظام المعلوماتي أن تخضع لنصوص التجريم الكلاسيكية هو قول يستغله في الغالب مجرموا المعلوماتية بغية الإفلات من العقاب، مستغلين بذلك الفراغ التشريعي

الموجود ، فنصوص التجريم جاءت مطلقة فالأصح أن يتم استغلالها إيجابيا قصد حماية مصالح الأفراد والدول لأن الأخذ بعكس ذلك يؤدي إلى التهرب من العقاب ولا يخدم إلا مجرمي المعلوماتية.

8- إمكانية اعتبار المكونات المعنوية للنظام المعلوماتي كمحل لجرائم الأموال كالسرقة والنصب وخيانة الأمانة، لأن ما يتم تبادله في نطاق المعاملات الإلكترونية هو من قبيل الأموال المستحدثة والتي تنطوي على قيمة أو قد تكون عبارة عن بيانات تثبت التزاما أو إبراء وبالتالي تدخل في نطاق المكاتيب.

9- أن كل من المشرع الجزائري والفرنسي قاما بوضع النصوص المستحدثة في المجال المعلوماتي في القسم المخصص لجرائم الأموال ، وهذا ما يعزز من اعتبار المكونات المعنوية مال في نظر المشرع، وما يدعم وجهة نظرنا هو التعريف الذي جاء به المشرع الأمريكي للمال حيث اعتبره كل شيء ينطوي على قيمة وذلك هو التعريف الأدق لأنه يشمل كل الأموال سواء مادية أو معنوية .

الإقتراحات:

بعد التطرق للنتائج التي تم التوصل إليها في هذه الدراسة فإننا نخرج بجملة من الاقتراحات و المتمثلة فيما يلي:

1- من خلال النصوص الخاصة :

لقد تدارك المشرع الجزائري على غرار جل التشريعات العربية الفراغ الوارد في مجال المعاملات الإلكترونية من خلال استحداثه لنصوص حماية أنظمة المعالجة الآلية للمعطيات، إلا أن ذلك تتخلله بعض النقائص والتي نفرد بعض الاقتراحات لتداركها.

ا- نقترح تشديد عقوبة الدخول إلى نظام المعالجة الآلية للمعطيات متى كان ذلك النظام محاطا بحماية فنية، لأن اختراق تلك الحماية يعكس توفر القصد الخاص لدى الجاني ويثبت أن تواجده داخل النظام المعلوماتي لم يكن وليد الصدفة.

ب- نقترح تشديد العقوبة إذا ترتب على الدخول الغير المشروع جريمة أخرى من الجرائم الغير منصوص عليها في هذا القسم.

ج- ضرورة تجريم الاعتداء على سير النظام المعلوماتي فبالرغم من أن المشرع جرم هذا الفعل نتيجة الدخول أو البقاء الغير مشروع في نظام المعالجة الآلية للمعطيات إلا أن الاعتداء على سير النظام المعلوماتي قد يحدث حال الدخول أو البقاء المشروع في النظام المعلوماتي محل الاعتداء.

د- بالرغم من تطرق المشرع الجزائري لطرق التزوير المعلوماتي " الإدخال، المحو، التعديل " إلا أنه أغفل محله في مجال المعاملات الإلكترونية، ومن ثم نقترح إضافة نص يتعلق بالتزوير المعلوماتي وذلك في القسم المخصص لحماية أنظمة المعالجة الآلية للمعطيات أو أن يستهل المشرع باب التزوير في المحررات بنص يعرف فيه المحرر على أنه " كل مركب يتكون من حروف أو علامات تدل على فكرة معينة بالنظر إليها مباشرة أو بالاستعانة بتقنية أخرى "، ومن ثم يمتد هذا النص ليشمل كل المحررات التقليدية والمحررات المعلوماتية معا كالمستندات المعالجة آليا والموجودة داخل النظام أو على دعامات خارجية كالأقراص الممغنطة والأشرطة.

ه- فيما يتعلق بالشروع في الجرائم المعلوماتية نرى ضرورة تعديل نص المادة 394 مكرر 7 وذلك تجنبا للأخذ بفكرة" الشروع في الاتفاق " بإخراج نص الاتفاق الجنائي من المواد التي يتناولها نص الشروع وذلك على الشكل التالي:

" يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في المواد 394 مكرر إلى 394 مكرر 2 بالعقوبات المقررة للجنحة ذاتها ".

كما نقترح تعديل المادة 394 مكرر 5 والمتعلقة بالاتفاق الجنائي وذلك بحصر المواد التي يشملها هذا الاتفاق من المادة 394 مكرر إلى 394 مكرر2

2- من خلال نصوص جرائم الأموال :

نظرا لأن كل الجدل الفقهي الذي دار في البحث محل الدراسة كان محله جرائم الأموال فإننا نرى ضرورة تدخل المشرع الجزائري و التشريعات العربية بنصوص صريحة تعالج الإشكال محل الدراسة وتقطع دابر البحث عن مدى صلاحية نصوص التجريم الكلاسيكية لتطبيقها في مجال المعاملات الإلكترونية، وعلى ذلك نقترح تعديل النصوص العقابية القائمة لتشمل في مضمونها كلا من المعاملات العادية والإلكترونية وذلك على النحو التالي :

ا- نقترح تعديل النصوص المتعلقة بجريمة السرقة وذلك بإضافة مصطلح شيء مادي أو معنوي على الشكل التالي " كل من اختلس شيئا ماديا أو معنويا غير مملوك له يعد سارقا " فبالرغم من تسليمنا في الموضوع محل الدراسة بإمكانية خضوع المكونات المعنوية للنظام المعلوماتي لنص السرقة وفقا للمدلول العام على اعتبار أن كلمة " شيء" يستوي أن يكون فيها الشيء ماديا أو معنويا، إلا أن هذا التعديل سيكف عناء الجدل الفقهي السابق.

ب- فيما يتعلق بجريمة النصب فإننا نقترح إضافة عبارة " خدمات أو قيمة " وبذلك يكون النص أكثر ملاءمة للتطبيق في مجال المعلوماتية، أو النص صراحة على النصب المعلوماتي وذلك على الشكل التالي: "كل من توصل لنفسه أو لغيره للاستيلاء على مال مادي أو معنوي بطرق احتيالية من شأنها خداع المجني عليه متى كان الحاسوب فيها وسيلة أو بيئة للجريمة يعاقب بالحبس لمدة ... والغرامة... أو بإحدى هاتين العقوبتين ".

ج- ضرورة الأخذ بفكرة التسليم المعادل التي ابتكرها الفقه الفرنسي وذلك لإدخال الأموال المتداولة في نطاق المعاملات الإلكترونية في مجال النصوص المتعلقة بجريمة النصب.

د- ضرورة استحداث نصوص عقابية تعالج الاعتداءات التي قد تقع على المعاملات التي تتم بواسطة بطاقات الائتمان ذلك ما يكفينا صعوبة تكييف ذلك الجرم.

ه- ضرورة الاعتراف بفكرة التسليم الإلكتروني في جريمة خيانة الأمانة، ذلك أن التسليم في مجال المعاملات العادية يكون ماديا في حين أن التسليم في مجال المعاملات الإلكترونية يعكس طبيعة المعلومة والتي تتجسد في شكل معنوي ما يستوجب معه أن يكون التسليم معنويا.

و- نقترح استحداث قانون موحد تتبناه كل الدول يجرم كل الأفعال التي تشكل جرما في القوانين العقابية القائمة، كما يتناول قواعد جديدة تخص الإجراءات الجزائية في هذا المجال وذلك لاختلاف الجرائم المعلوماتية عن الجرائم العادية وباستحداث هذا القانون وتبنيه من قبل التشريعات المختلفة نتجاوز إشكاليات كثيرة تصادفنا في هذا المجال كالاختصاص القضائي والإجراءات المتبعة في ذلك.

وفي ختام هذه الدراسة لا يسعنا إلا أن نأمل أن يكون موضوع بحثنا أرضية خصبة لدراسات أخرى لاحقة حيث لا ندعي من خلاله أننا أحطنا بكل جوانب الموضوع بل نأمل أن نكون قد وفقنا لإثارة إشكالية جديدة تكون بمثابة انطلاقة لدراسات أخرى أكثر تعمقا.

وفي الأخير ليس لنا إلا أن نحمد الله الذي وفقنا لإتمام هذه الدراسة .

" اللهم لك الحمد والشكر كما ينبغي لجلال وجهك وعظيم سلطانك "

قائمة
المراجع

قائمـة المراجـع :

أولا: مراجع باللغة العربية

1- المؤلفات العامة :

- د/ أحسن بوسقيعة الوجيز في القانون الجزائري الخاص، ط10، دار هومة للنشـــر والتوزيـــع الجزائر 2009 .

- حسين فريجة، شرح قانون العقوبات الجزائري، ديوان المطبوعات الجامعية، بن عكنون الجزائـــر 2006.

- د/ عمر السعيد رمضان ، شرح قانون العقوبات القسم الخاص ، دار النهضة العربية ، القـــاهرة 1986.

- د/ علي عبد القادر القهوجي، شرح قانون العقوبات القسم الخـــاص، الكتـــاب الثـــاني، دار المطبوعات الجامعية، الإسكندرية 1999 .

- د/ غنام محمد غنام ، شرح قانون العقوبات القسم الخاص ، جامعة المنصورة 2004 .

- د/ كامل السعيد، شرح قانون العقوبات الجرائم المضرة بالمصلحة العامة، دار الثقافـــة للنشـــر والتوزيع، عمان 2008.

- د/ مجدي محب حافظ، خيانة الأمانة والجرائم الملحقة بها، النسر الـــذهبي للطباعـــة، القـــاهرة 2002.

2- المؤلفات المتخصصة:

- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومة للطباعة والنشر والتوزيع، الجزائر 2007.

- د/ أسامة حسنين عبيد ، المراقبة الجنائية الإلكترونية ، دار النهضة العربية ، القاهرة 2009 .

- د/ إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية 2007.

- د/جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية 1992 .

- جهاد رضا الحبشانة، الحماية الجزائية لبطاقات الوفاء، دار الثقافة، عمان 2008 .

- د/ خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية الإسكندرية 2008.

- د/ خالد ممدوح إبراهيم، أمن الحكومة الإلكترونية، الدار الجامعية الإسكندرية 2008.

- د/ شيماء عبد الغني عطا الله، الحماية الجنائية للتعاملات الإلكترونية ، دار الجامعة الجديدة ، الإسكندرية 2007 .

- د/ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية 2004.

- د/ عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، دار الفكر الجامعي، الإسكندرية 2004.

- د/ عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية القاهرة 2001.

- د/ عفيفي كامل، جرائم الكمبيوتر وحقوق الؤلف و المصنفات الفنية، دار الثقافة للطباعة و النشر 2000.

- د/ علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية للنشر والتوزيع، الأردن 2009.

- د/ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، الإسكندرية 1999.

- د/ عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، دار النهضة العربية، القاهرة 2010 .

- محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان 2005.

- محمد أمين الشوابكة، جرائم الحاسوب والانترنت الجريمة المعلوماتية، دار الثقافة، عمان 2009.

- د/ محمد حسام محمود لطفي ، الإطار القانوني للمعاملات الإلكترونية ، دار النهضة العربية ، القاهرة 2002.

- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة الإسكندرية 2007 .

- د/ محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة 2010.

- د/ محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية 2004.

- د/ محمود الكيلاني، الموسوعة التجارية والمصرفية المجلد الثاني، التشريعات التجارية والإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان 2007 .

- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية 2006.

- د/ نعيم مغبغب، حماية برامج الكمبيوتر الأساليب والثغرات، منشورات الحلبي الحقوقية، لبنان 2006 .

- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان 2008.

-د/ هلالي عبد الله أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة 2007.

3- الرسائل العلمية:

- آمال قارة، الجريمة المعلوماتية، رسالة مقدمة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، قسم العلوم القانونية، جامعة الجزائر، السنة الجامعية 2005 / 2006 .

- مناصرة يوسف ، جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، رسالة مقدمة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية ، قسم العلوم القانونية ، جامعة الجزائر ، السنة الجامعية 2008-2009 .

4- المقالات والأبحاث والدوريات:

- أحمد الصم النقبي، فوائد تأسيس شبكة أنظمة المعلومات الحكومية، مجلة الشرطة الإماراتية، العدد 343، يوليو 1999 .

- د/ رياض سليمان عواد، أمن المعلومات وضرورة وضع تشريع لجرائم الحاسب الآلي، مجلة الشرطة الإماراتية العدد 395، نوفمبر 2000 .

- هشام مفيد محمود، عمليات الاحتيال في بطاقات الائتمان، مجلة الأمن والحياة، العـــدد 217، سبتمبر / أكتوبر 2000.

- د/ عبد الحق حميش ، حماية المستهلك الإلكتروني ، بحث مقدم إلى مؤتمر الأعمـــال المصـــرفية الإلكترونية بين الشريعة والقانون ، دبي من 1 إلى 3 ماي 2003 .

5- أحكام قضائية:

- مجلس قضاء باتنة، الغرفة الجنائية، تاريخ 2010/7/4 ، قرار رقم 10/05805 .

6- النصوص التشريعية:

- أمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافـــق ل 26 ســـبتمبر ســـنة 1975 المتضمن القانون المدني

- قانون المعاملات الإلكترونية الأردني ، رقم 85 لسنة 2001.

-القانون رقم 15/04 المؤرخ في 2004/11/10 المعدل والمتمم للأمـــر 156/66 المـــؤرخ في 1966/06/08 المتضمن قانون العقوبات (ج.ر 71 في 2004/11/10)

-القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق ل 5 غشت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

ثانيا: مراجع باللغة الأجنبية:

1- مراجع باللغة الفرنسية:

-ANDRE LUCAS, le droit de l'informatique, P.U.F 1 Ed 1987.

-ANDRE VITU, Traité droit pénal spécial, édition cujas, 1989

-BERTRAND (A) : la criminalité informatique , les débits relatifs au matériel ,Paris expertisés , 1984 .

-CARILLAC ET MOULY , droit pénal de la banque et du cridit , édition Masson, 1982.

-CLAUD GARCIN, Lamy droit pénal dés affaires,(la froude informatique) éd 2003

-DARAGON ELISE , étude sur le statut juridique de l'informatique , Dalloz 1998 .

-HENRI CROZE ET YVES BISMUTH , le droit de l'informatique . paris expertise 1984.

-LUCAS D LEYSSAC , une Information seule est elle seuxeptitible de vol .Dalloz 19883.

-RAYMONS GASSIN la fraude informatique, Dalloz 1995.

- RAYMONS GASSIN, le droit pénal de l'informatique, Dalloz 1986.

- ROGER MERLE , traite de droit criminel , édition Cujas 1988 .

-Rose (PH), la criminalité informatique, PUF 2eme édition 1995.

2- مراجع باللغة الإنجليزية:

- LESLIE D. BALL, computer crime " the information technologie révolution, 1985

- SMITH AND HOGAN , criminal Law 7th ed , butter Worths London 1992

3- مواقع الانترنيت:

- www. Algeriedroit .fb.bz. le 22/01/2011 à 14h 20mn

- www.arabic.Mjustice.Dz/ligue.Arabe/loi_emir_ar_crim_tech_info/loi_emir_ar_crim_tech_info.htm. le 09/11/2010 à 11h00mn

- www. Arablawinfo.com. le 20/01/2011 à 21h00mn

-www.djetfa.info/Vb/showthread.php?t=204052. Le :05/02/2011 à : 15h40mn.

- www. Eastlaws.blogspot.com /2010/03/23-11-2001.html le 16/09/2010 à 20h30mn

-www.egovconcepts.com/channels/basics/62-2009-05-26-06-29-05.html le: 15/02/2011 à :10h 30mn.

- www. Lawyers-gate.com/ub/threads/8371 le 02/01/2011 à 10h 00mn

الفهـــرس

الفهرس:

مقدمة

الفصل الأول :

ماهية الجرائم الواقعة على المعاملات الإلكترونية والحماية الجنائية المقررة لها بنصوص خاصة

المبحث الأول : ماهية الجرائم الواقعة على المعاملات الالكترونية ودواعي الحماية الجنائية المقررة لها 07

المطلب الأول : ماهية الجرائم الواقعة على المعاملات الالكترونية.....08

الفرع الأول : تعريف الجرائم الواقعة على المعاملات الالكترونية 08

الفرع الثاني : خصائص الجرائم الواقعة على المعاملات الالكترونية 12

المطلب الثاني : دواعي الحماية الجنائية للمعاملات الالكترونية 15

الفرع الأول : التوجه نحو الحكومة الالكترونية 16

الفرع الثاني : أضرار الجرائم المعلوماتية على الاقتصاد الوطني 23

الفرع الثالث : عدم كفاية القوانين القائمة 24

المبحث الثاني : الحماية الجنائية للمعاملات الإلكترونية بنصوص خاصة 26

المطلب الأول : الحماية الجنائية لأنظمة المعالجة الآلية للمعطيات 27

الفرع الأول : تعريف نظام المعالجة الآلية للمعطيات 28

الفرع الثاني :أركان جريمة الإعتداء على نظام المعالجة للمعطيات 31

المطلب الثاني : الحماية الجنائية للمعاملات الالكترونية وفقا للقواعد المقررة في جرائم الإتلاف.....48

الفرع الأول : مجل جريمة الإتلاف في نطاق المعاملات الالكترونية 48

الفرع الثاني : أركان الجريمة الإتلاف في نطاق المعاملات الالكترونية 52

المطلب الثالث : الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد المقررة في جرائم التزوير 60

الفرع الأول : محل جريمة التزوير في نطاق المعاملات الالكترونية 61

الفرع الثاني : أركان جريمة التزوير في نطاق المعاملات الالكترونية 67

الفصل الثاني :

الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد العامة في قانون العقوبات

المبحث الأول : الحماية الجنائية للمعاملات الالكترونية وفقا للقواعد العامة المقررة في جرائم الأموال 75

المطلب الأول : مدى تحقق الحماية الجنائية للمعاملات الإلكترونية وفقا للقواعد العامة المقررة لجريمة السرقة 77

الفرع الأول: محل جريمة السرقة في نطاق المعاملات الالكترونية 79

الفرع الثاني: أركان جريمة السرقة في نطاق المعاملات الالكترونية 87

المطلب الثاني: مدى تحقق الحماية الجنائية للمعاملات الالكترونية وفقا للقواعد العامة المقررة لجريمة النصب.....103

الفرع الأول: محل جريمة النصب في نطاق المعاملات الالكترونية.....106

الفرع الثاني: أركان جريمة النصب في نطاق المعاملات الالكترونية.....109

المطلب الثالث: مدى تحقق الحماية الجنائية للمعاملات الالكترونية وفقا للقواعد العامة المقررة لجريمة خيانة الأمانة124

الفرع الأول: محل جريمة خيانة الأمانة في نطاق المعاملات الالكترونية 126

الفرع الثاني: أركان جريمة خيانة الأمانة في نطاق المعاملات الالكترونية.....134

المبحث الثاني: الحماية الجنائية للمعاملات الالكترونية من خلال تجريم الاتفاق أو الشروع في الجرائم المعلوماتية 144

المطلب الأول: الحماية الجنائية للمعاملات الالكترونية من خلال تجريم الاتفاق على ارتكاب الجرائم المعلوماتية..145

الفرع الأول: الركن المادي للاتفاق الجنائي.....146

الفرع الثاني: الركن المعنوي للاتفاق الجنائي.....150

المطلب الثاني: الحماية الجنائية للمعاملات الالكترونية من خلال تجريم الشروع في الجرائم المعلوماتية.....153

الفرع الأول: اركان جريمة الشروع في نطاق المعاملات الالكترونية.....154

الفرع الثاني: جريمة الشروع في الاتفاق الجنائي.....157

خاتمـــــــة.....160