صور الركن المادي في الجرائم الماسة بـأنظمة المعالجة الآلـية للمعطيات

The forms of Actus reus in the crimes related to data automated processing systems

الدكتور/ عزالدين عثماني

جامعة العربي التبسي تبسة، الجزائر

azdineatmani@yahoo.fr

تاريخ الاستلام: 2018/09/06 تاريخ القبول للنشر: 2018/10/30

❖❖❖❖❖❖❖

ملخّص:

يثير تحديد الركن المادي في الجرائم الماسة بأنظمة المعالجة الآلية المعطيات أو الجرائم المرتكبة عبر الإنترنت جملة من الصعوبات التي تفرضها طبيعة الوسط الذي تتم فيه الجريمة والمتمثل في الجانب التقني، وهذا ما يميز ركنها المادي الذي يجب أن يتم باستخدام أجهزة الحاسب الآلي أو الشبكة العالمية للإنترنت و من هنا تبدأ التساؤلات التي تتعلق بصور هذا النشاط التقني؟

وقد نص المشرع الجزائري على صور هذا النشاط من خلال نص المادة 394 مكرر من قانون العقوبات، واعتبر أن الركن المادي لهذه الجريمة يقوم من خلال الدخول والبقاء غير المشروعين، بالإضافة إلى فعل الغش والإتلاف المعلوماتي الذي يتحقق من خلال مجموعة من الأفعال تتمثل أساسا في تزوير المعلومات، بالإضافة إلى إتلافها من خلال القيام بسلوكات معينة تؤدي إلى استحالة الاستفادة من المعلومة المعالجة آليا.

الكلمات المفتاحية: الركن المادي؛ الجريمة؛ الإتلاف؛ البيانات؛ المعلوماتية.

Abstract:

The identification of the physical element, in the crimes against the data automated processing systems or crimes committed through the Internet, raises a number of difficulties imposed by the nature of the environment in which the crime is committed, which is the technical aspect, and this is what distinguishes their physical element that should be done using computers or the World Wide Web. From here questions related to the forms of this technical activity begin?

The Algerian legislator provided a description of the forms of this activity through the text of article 394 bis of the Penal Code. He considered that the physical element of this crime is through the illegal entry and stay, in addition to the act of fraud and information damage achieved through a series of acts consisting mainly of forging information, in addition to their destruction through the conduct of certain behaviors leading to the impossibility to benefit from information the processed automatically.

مقدّمة:

تأصيل للموضوع:

يعد الركن المادي للجريمة الجانب المادي الذي يدخل في تكوينها، ويبرز هذا الجانب إلى العالم الخارجي بمظهر مادي يعبر عن سلوك ونتيجة، ويتكون الركن المادي من ثلاث عناصر هي السلوك الإجرامي والنتيجة التي تحققت والعلاقة السببية التي تربط بين السلوك والنتيجة، وقد لا يتوفر الركن المادي دائما على هذه العناصر في جميع الجرائم، فقد يكتفي المشرع بالسلوك وحده للقول بقيام الركن المادي للجريمة دون اشتراطه أن تتحقق النتيجة وصور ذلك ما يسمى بالجرائم الشكلية.

أهمية الموضوع:

في الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فحتى لو كان القانون لا يعاقب على الأعمال التحضيرية في الجرائم العادية إلا أن الأمر يختلف بعض الشيء في جرائم تكنولوجيا المعلومات، فشراء برنامج الاختراق أو تصميمه أو شراء معدات لفك الشفرات وكلمات المرور، وحيازة صور مخلة بالحياء لأطفال صغار في السن كلها أشياء تشكل جريمة في حد ذاتها، لذلك نجد أن المشرع الفرنسي قد وسع من مفهوم الشروع في الجرائم المعلوماتية باعتبار أن هذه الأفعال هي مقدمة الفعل غير المشروع وبالتالي فإن الجزء الأكبر من الأعمال التحضيرية يدخل في نطاق الشروع في السلوك المجرم ويعاقب عليه بنفس عقوبة الجريمة التامة.

إشكالية الموضوع:

يثير تحديد الركن المادي في الجرائم الماسة بأنظمة المعالجة الآلية المعطيات أو الجرائم المرتكبة عبر الإنترنت جملة من الصعوبات التي تفرضها طبيعة الوسط الذي تتم فيه الجريمة والمتمثل في الجانب التقني، وهذا ما يميز ركنها المادي الذي يجب أن يتم باستخدام أجهزة الحاسب الآلي أو الشبكة العالمية للإنترنت وتبدأ التساؤلات التي تتعلق ببداية النشاط التقني أو الشروع فيه، ومكان البداية واكتمال الركن المادي، وأجهزة السلوك الإجرامي المرتكب في العالم المادي، أو العالم الافتراضي وغيرها من التساؤلات التي تتعلق بطبيعة الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات، وبالتالي يثور التساؤل حول أهم عنصر تقوم على أساسه الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات، ألا وهو الركن المادي، فما هي صوره وما هي الإشكاليات القانونية التي يثيرها؟

المبحث الأول

صور الركن المادي في جريمتي الدخول والبقاء غير المصرح بهما

يرجع البعض الاختلاف بين جريمتي الدخول والبقاء غير المصرح لهما إلى أن جريمة الدخول جريمة إيجابية تقتضي إتيان فعل الدخول، في حين تقوم جريمة البقاء بسلوك سلبي، فرغم دخول الجاني صدفة أو خطأ، ورغم علمه بأن ذلك غير مشروع فهو يرفض الخروج من النظام وبمعنى آخر يمتنع عن الخروج، لذلك فالنشاط الإجرامي – حسب رأي هذا الجانب – يمثل في هذه الصورة سلوكا سلبيا من الجاني.

إلا أن هناك جانبا آخر يرى أن الامتناع عن الخروج من النظام الذي تم الدخول إليه ليس مناط التجريم بل أن السلوك المجرم هو البقاء داخل هذا النظام بعد الدخول إليه مع العلم بأن هذا البقاء غير مصرح به وهو ما يشكل سلوكا إيجابيا.

وذهب بعض الفقه إلى القول بأن طبيعة البقاء هي طبيعة الدخول ذاتها وينطبق عليها كل ما ينطبق على الدخول، لكن ما يميز بينهما هو وقوع الجريمة في وقت واحد أو استمرارها، فيذهب رأي إلى اعتبار كل من جريمتي الدخول والبقاء من الجرائم المستمرة، بينما يعتبر رأي آخر جريمة الدخول جريمة متتابعة الأفعال وجريمة البقاء مستمرة، ورأي آخر يجد جريمة الدخول جريمة وقتية ذات أثر ممتد، وجريمة البقاء جريمة مستمرة[1].

وبالنسبة للنصوص التي تجرم مجرد الدخول إلى النظام، فإنه لا يمكن العقاب على البقاء غير المصرح به ما لم ينص على ذلك صراحة، وهو ما فعله المشرع الفرنسي حيث نص صراحة على تجريم البقاء داخل النظام إثر تجريمه للدخول المجرد غير المصرح به، وقد حذا حذوه المشرع الجزائري[2].

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

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

المطلب الأول: صور الركن المادي في جريمة الدخول غير المصرح به

إن السلوك الذي تنهض به الجريمة متعدد ومتنوع، والجريمة المعلوماتية لا تخرج عن هذه القاعدة، فكثير من السلوكيات التي تنهض بها الجريمة المعلوماتية ترتكب عن طريق الكمبيوتر، إلا أن قسما منها والتي تستخدم فيها التقنيات والمخترعات العلمية الحديثة قد تخضع لقواعد القانون الجنائي التقليدي.

وتجدر الإشارة إلى أن الدخول الاحتيالي في نظام معلوماتي على عكس البقاء الاحتيالي يعد من الجرائم الآنية كمعظم الجرائم الأخرى إذ يتحقق في فترة زمنية محددة أي في لحظة الدخول غير مشروع إلى النظام المعلوماتي[3].

وبالرجوع إلى قانون العقوبات الجزائري نجده أنه يعاقب كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك[4].

ومن خلال ذلك نجد أن المشرع نص على فعل مادي وهو الدخول عن طريق الغش، إلا أنه لم يقدم تعريفا له، وبالرجوع إلى بعض التشريعات العربية نجدها تعرف هذا الفعل على أنه دخول شخص بطريقة

معقدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها[5]، لذلك يعد فعل الدخول غير المصرح به أو المخول به من الأنشطة الجرمية الأكثر انتشارا من بين جرائم الكمبيوتر أو المعطيات، ويقوم التوصل غير المصرح به بالأساس على الدخول إلى نظام الحاسوب أو شبكة المعلومات، ويكون ذلك عادة من خلال استخدام وسيلة اتصال عن بعد كالموديم ومن خلال التواصل عبر نقاط الاتصال والموجات الموجودة على الشبكة إلى نظام كمبيوتر معين بغرض الوصول إلى البيانات أو البرامج المخزنة في النظام ويتطلب هذا النشاط غالبا تجاوز أو كسر إجراءات الحماية التقنية للنظام كتجاوز كلمة السر وإجراءات التعريف والجدران النارية وغيرها أو التوصل لنقطة ضعف في نظام حماية البرامج والنفاذ منها[6].

ويتبين لنا أن المشرع الجزائري اكتفى بذكر فعل الدخول فنص على ذلك" ... كل من يدخل أو يبقى عن طريق الغش" ولم يذكر الأفعال المادية لفعل الدخول ولم يحدد الوسيلة أو الطريقة التي يتم بها الدخول إلى النظام، لذلك جرم أي وسيلة أو طريقة للدخول سواء تم الدخول بطريقة مباشرة أو غير مباشرة على عكس بعض التشريعات الأخرى التي وسعت من دائرة التجريم وذكرت مجموعة كبيرة من الأفعال التي قد تحدث نتيجة فعل الدخول[7]، وقد تم تجريم تلك الأفعال لعدم وجود حماية قانونية صريحة للبيانات والمعلومات الإلكترونية في التشريعات العقابية العامة إضافة إلى لزوم معاملتها معاملة المال والوثائق والحقوق الأخرى التي يحظر القانون المساس بها، فالمعلومات والبيانات الإلكترونية لها قيمة مادية ومعنوية لا تقل عن قيمة الوثائق والأموال والحقوق الأخرى المحمية بموجب التشريعات النافذة، ولا إمكانية لتصور وقوع إتلاف إلكتروني لا يكون محله مال إلكتروني معنوي وهو أمر لا يتوفر إلا في بيئة إلكترونية قوامها تقنين نظم المعلومات، كما قد تحتوي هذه البيانات على دراسات ومعلومات خاصة أو أنها برامج تتحكم بأنظمة أو مؤسسات وتسيرها مما يترتب على ما تقدم أن أي من تلك الأفعال قد ينجم عنها تعطيل خدمات مثل الكهرباء ...إلخ، وقد ينجم عنها تعطيل الأجهزة ووقوع خسائر مادية أخرى، مما يتطلب وجود حماية تشريعية خاصة للمعلومات والبيانات المخزنة في نظام معلومات أو شبكة معلومات لسهولة الوصول إليها وإلغائها وحذفها وإضافتها وتدميرها وإتلافها[8].

ويرى الفقه الفرنسي أن الدخول له مدلول معنوي، حيث يعتبر الدخول إلى نظام معالجة البيانات أو النظام المعلوماتي أو النظام الإلكتروني يشبه الدخول إلى ذاكرة الإنسان، كما أن له مدلولا ماديا يتمثل في أن الشخص يكون متى دخل الجاني إلى النظام كله أو جزء منه وكذلك يتحقق الدخول غير المشروع متى كان مسموحا للجاني بالدخول لجزء معين في النظام وتجاوز ذلك إلى جزء آخر غير مسموح له بالدخول، وحتى نكون بصدد جريمة الدخول غير المصرح به يجب أن يكون النظام غير مفتوح أمام الجمهور، لأنه لو كان كذلك لما اعتبر جريمة و معظم الذين يدخلون، يستخدمون طرق غير مشروعة من خلال التوصل إلى الأرقام والكلمات أو الشفرات أو الحروف أو المعلومات السرية التي تكون بمثابة النظام الأمني لجهاز الحاسب الآلي أو البرامج والنظم المعلوماتية[9].

وقد لا يكون هدفهم في الغالب الإضرار بالبيانات والملفات أو تدميرها، وقد يسعى مقترفو هذه الأنشطة إلى الاطلاع على المعلومات المحمية، غير أن حماية المعلومات من أخطار هذه الأنشطة أو احتمال تطور هذه الأنشطة من مجرد هدف للاطلاع إلى أهداف أكثر خطورة كالتلاعب بالمعطيات أو إتلافها أو ارتكاب غير ذلك من جرائم الحاسوب أو استخدام الدخول لارتكاب جرائم أخرى بواسطة الكمبيوتر، دفعت غالبية دول العالم إلى تجريم هذه الأنشطة كما هو الشأن في قوانين كل الدول الأوربية، وحتى أمريكا، واليابان إذ تقع الجريمة من كل إنسان أيا كانت صفته، سواء كان يستطيع أن يستفيد من الدخول أولا فيكفي أن يكون الجاني ليس ممن لهم الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، حيث تتوافر الجريمة في كل حالة يكون فيها الدخول مخالفا لشروط الدخول التي نص عليها القانون أو الاتفاقيات، كما هو الحال إذا كان القانون يفرض سرية معينة بالنسبة لبعض الأنظمة مثل أسرار الدولة أو السرية المتعلقة بالمعلومات الذاتية أو الإسمية أو أسرار الأشخاص مثل أسرار الحياة الخاصة المهنية أو أي معلومات[10] يجمعها الإنسان في نظام ولا يترك أمر الاطلاع عليها لأي إنسان[11]، ويكون الدخول غير مشروع إذا كان من له حق السيطرة على النظام قد وضع بعض القيود للدخول إليه ولم يحترم الجاني تلك القيود، وإذا كان يتطلب ضرورة دفع مبلغ من النقود، وتم الدخول دون دفع ذلك المبلغ وترتكب الجريمة من يعمل على الحاسب ولكن بنظام معين، فيدخل في نظام آخر كما تقع الجريمة سواء تم الدخول إلى النظام كله أو إلى جزء منه فقط، أي يكفي لتوافر الجريمة أن يتم الدخول على بعض عناصر النظام، أو على عنصر واحد منه، أو منطقة منه بشرط أن يكون العنصر الذي تم الدخول إليه فقط يدخل في برنامج متكامل قابل للتشغيل[12].

كما أن عملية الدخول إلى نظام المعلوماتي باعتبارها مسألة تقنية بحتة قد تتم بعدة طرق هي:

- الاتصال المادي المباشر بالنظام المعلوماتي:

ويقصد به الدخول في النظام دون الحاجة إلى شبكة اتصال معلوماتي أو إلكتروني لتحقيق الجريمة، أي الجاني موجود في نفس المكان الذي يوجد فيه النظام محل الجريمة وما عليه في هذه الحالة إلا إجراء عمليات مادية مثل إدخال دعامة مادية كالقرص المضغوط تحتوى على برنامج فك الرموز للدخول في النظام المعلوماتي المحمي تقنيا أو إزالة أو حذف عنصر مادي من الكمبيوتر محل الجريمة لتسهيل عملية الدخول في النظام، كما قد يتم الدخول في النظام بإجراء عمليات إلكترونية كالتلاعب في عين المكان بنظام معطيات أو برامجه أو إجراء تعديلات فيها بهدف تسهيل عملية الدخول.

- الاتصال المعنوي عن بعد بالنظام المعلوماتي:

ويقصد به الدخول في النظام المعلوماتي محل الجريمة باستعمال وسائل الاتصال عن بعد المستحدثة (الشبكات المعلوماتية أو الإلكترونية السلكية أو اللاسلكية)، وفي هذه الحالة لا يشترط حتى تقوم الجريمة أن يكون الجاني موجود في نفس مكان وجود الكمبيوتر محل الجريمة.

وتهدف كل من حالتي الاتصال بالنظام محل الجريمة إلى القيام بتصرفات غير مشروعة من بينها حالة استعمال أو مناداة برنامج عن بعد أو داخل النظام دون أي ترخيص أو من دون أي صلاحية.

- حالة استجواب أو الاطلاع على محتوى معطيات معلومات موجودة في النظام من دون أي ترخيص أو صلاحية[13].

وفي النهاية فإن الجريمة تقوم بمجرد فعل الدخول إلى النظام دون ضرورة حدوث أية نتيجة أخرى، فلا يشترط لقيامها التقاط المتدخل للمعلومات التي يحتويها النظام أو بعضها أو استعمال تلك المعلومات، بل أن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات الموجودة على النظام[14].

وبالنسبة للتصريح بالدخول هناك حالتين لعدم التصريح تتمثل الأولى في حالة عدم وجود تصريح إطلاقا حيث لا يملك الشخص هنا ترخيص بالدخول للنظام سواء كان هذا الترخيص يتوقف على سداد مبلغ معين أو يتوقف على العضوية في جهة معينة أو على غير ذلك من الشروط أو كان الدخول إلى النظام ممنوعا على الإطلاق.

أما الحالة الثانية فتتمثل في تجاوز التصريح حيث يكون الفاعل مصرحا له بالدخول في حدود معينة ولكنه يتجاوز هذه الحدود، التي تعتبر تجاوزا في المكان لا في الزمان، أي تجاوز الفاعل للمناطق والمجال المكاني المصرح به لغيره من المجالات غير المصرح له بدخولها.

المطلب الثاني: صور الركن المادي في جريمة في جريمة البقاء الاحتيالي

البقاء الاحتيالي هو المرحلة التي تلي الدخول إلى النظام، ونصت عليها كلا من المادة 323-1فقرة.1 ق. ع فرنسي والمادة394 مكرر فقرة 1.ق.ع جزائري.

اعتبر المشرع أن البقاء الاحتيالي جريمة، حيث نص عليها في قانون العقوبات بقوله، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات ...[15] لذلك عرف البقاء الاحتيالي بأنه كل تواجد غير عادي كالاتصال بواسطة الشبكة المعلوماتية بالنظام المعلوماتي أي الدخول والنظر فيه، أي في المعطيات التي يتضمنها وغيرها من التصرفات غير مسموح بها والتي تشكل بدورها بقاءً احتياليا[16]، فيتحقق الركن المادي في جريمة البقاء الاحتيالي إذا اتخذ صورة البقاء داخل النظام ويقصد بفعل البقاء" التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام"[17].

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الفرض الذي لا يكون فيه الجاني له الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له الحق في السيطرة عليه، ثم يبقى داخل النظام بعد ذلك ويتحقق في هذا الفرض الاجتماع المادي لجريمتي الدخول والبقاء غير المشروع في النظام[18].

لذلك تعد هذه الجريمة من الجرائم المستمرة، فالجريمة تستمر كلما زادت مدة البقاء غير المشروع داخل النظام المعلوماتي[19]، كما أن جريمة البقاء الاحتيالي لم يشترط فيها القضاء الفرنسي أن تتوافر لدى المجرم نية الإضرار بالنظام المعلوماتي بل يكفي أن يقوم بمجرد البقاء فقط إذا كان غير مشروع، وقد يتسبب المجرم زيادة عن بقائه غير المشروع في النظام إلى الإضرار بهذا الأخير[20].

وقد نص قانون العقوبات على أنه، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ...[21].

ويتبين أن المادة نصت على ظرفي تشديد لعقوبة الدخول أو البقاء داخل النظام، ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام، أو عدم قدرة النظام على تأدية وضيفته، ويكفي لتوافر هذا الظرف المشدد أن تكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت، وهي محو النظام أو عدم قدرته على أداء وظيفته، أو تعديل البيانات.

المبحث الثاني

صور الركن المادي في جريمتي الغش والإتلاف المعلوماتي

التزوير المعلوماتي هو أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة وكانت مرسومة عن طريق الرسم ويستوي في المحرر المعلوماتي أن يكون مدوناً باللغة العربية أو بلغة أخرى محفوظة على دعامة لبرنامج منسوخ على أسطوانة شرط أن يكون المحرر المعلوماتي ذو أثر قانوني معين.

وقد عرف المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بالبرازيل لعام 1994 في مقرراته وتوصياته بشأن جرائم الكومبيوتر والتزوير المعلوماتي بأنه المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الكومبيوتر وتعد فيما لو ارتكبت بغير هذه الطرق من قبيل أفعال التزوير المنصوص عليها في القانون الوطني.

ويفهم مما سبق بأن مفهوم التزوير لا يثير صعوبة حيث ورد في كافة القوانين والتشريعات العقابية التقليدية، ولكن التزوير بظهور تكنولوجيا وتقنية الحاسبات الآلية قد اكتسب بعد جديداً أضفى عليه أهمية تفوق ما كان عليه قبل ذلك كما أكسبه شكلاً جديداً بل تسمية جديدة حيث أصبح يشار إليه بالمعلوماتية إشارة يرتبط بها بتقنية تكنولوجيا الحاسبات.

ويبدو مما تقدم أن التزوير المعلوماتي يرد على بيانات في وثائق في أصلها معلوماتية وهي تلك الوثائق التي يتم الحصول عليها بوسائل معلوماتية، بعبارة أدق تلك الوثائق التي يتم الحصول عليها بواسطة جهاز إليكتروني أو كهرومغناطيسي أو أشرطة ممغنطة، وإن كان هنالك جانب من الفقه يرى ضرورة عدم الخلط بين الوثائق المبرمجة والوثائق المعلوماتية، وعلى الرغم مما ذكر فإن التزوير المعلوماتي يعادل في خطورته التزوير التقليدي وعليه فإن التزوير المعلوماتي هو أي تغيير للحقيقة في محرر بكل الطرق التي يقرها القانون المادية والمعنوية تغيراً من شأنه إحداث ضرر للغير بواسطة استخدام الحاسب الآلي[22].

المطلب الأول: صور الركن المادي في جريمة الغش المعلوماتي

يتجسد الركن المادي في جريمة الغش المعلوماتي من خلال نص المادة 394 مكرر 01 من قانون العقوبات عملية إدخال وبطريقة الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريقة الغش المعطيات التي يتضمنها، ومضمون هذه المادة يصطلح عليه بتسمية المساس بالمنظومة المعلوماتية.

وتعد جريمة الغش المعلوماتي في مجال المعالجة الآلية للمعطيات من أخطر طرق الغش التي تقع في هذا المجال ولاسيما بعد تراجع المحررات والمستندات والوثائق والصكوك الورقية في حين غزت المحررات الإلكترونية كل المجالات مما زاد صعوبة اكتشاف وإثبات الغش في هذا المجال، أو هو تغيير الحقيقة في

مستند رسمي ولكن المستند هنا ليس مستندا عاديا بل هي عبارة عن تسجيلات إلكترونية أو محررات إلكترونية.

وقد أشار المشرع بخصوص الغش بقوله:... عن طريق الغش ....خاصة مع تزايد حجم الاعتداءات الواقعة على المعطيات المخزنة داخل الحاسب الآلي التي تمس الأفراد في حقوقهم وأموالهم وحياتهم الخاصة وأمام تزايد فرص الأشخاص للعبث والتلاعب في معطيات الحاسب بتبديلها وتحويرها بالشكل الذي يفقد الثقة بالتقنية ويمس مراكز الأفراد بات من الواجب بسط الحماية لهذه المعلومات وضمان أمنها وسلامتها من كل تبديل وغش[23].

ويتمثل الركن المادي لجريمة الغش المعلوماتي في تغيير الحقيقة في محرر معلوماتي بإحدى الطرق التي نص عليها القانون وهو تغيير من شأنه أن يسبب ضررا ومن هنا ولقيام هاته الجريمة لا بد من توافر ثلاثة عناصر أساسية:

- وجود محرر.
- تغيير الحقيقة بإحدى الطرق المنصوص عليها قانونا.
- أن يترتب على ذلك ضرر.

1- وجود محرر:

المحررات الإلكترونية عبارة عن سجل أو مستند إلكتروني يتم إنشاءه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس أو على أي وسيط إلكتروني آخر ويكون قابلاً للاسترجاع بشكل يمكن فهمه وإبراز مضمون هذه المحررات الإلكترونية (الأقراص اللينة والمضغوطة أو أية وسائط الكترونية أخرى).

ولعل من أهم العقبات التي واجهت تطبيق النص الخاص بالغش المعلوماتي هي وجود محرر، فمستند المعلومات ينتج عن إصدار أمر من مشغل الجهاز إلى الطابعة وذلك بطبع المعلومات التي تم معالجتها آليا داخل جهاز الكمبيوتر، حيث أن البيانات بإدخالها تتم معالجتها وتتحول إلى معلومات مفيدة، ويشترط أن يظهر مستند المعلومات لحيز الوجود، ولا يشترط أن يتم الغش على المستندات المطبوعة على أوراق بواسطة طابعة، فيمكن أن يتم التزوير على المعلومات المعالجة آليا داخل جهاز الكمبيوتر والمسجلة على قرص صلب أو قرص مرن ومن هنا يمكن القول بتطبيق ذلك على برنامج الكمبيوتر، عندما يكون هذا البرنامج قد دون على أسطوانة أو شريط ممغنط محرر، ومن ثم فإن تغيير الحقيقة فيه يعد غشا أو تزوير لانتقال المعطيات المخزنة إلى جسم مادي، يأخذ صفات المحرر المكتوب، الذي يمكن قراءته بالعين عن طريق الكمبيوتر والكشف عن مضمونه من قبل الغير[24].

2- تغيير الحقيقة:

يقصد بتغيير الحقيقة هو إبدالها بما يغايرها، وبالتالي فلا يعتبر تغييرا للحقيقة أي إضافة لمضمون المحرر طالما ظل مضمون المحرر على حالته قبل الإضافة أو الحذف، ويقوم ذلك بصدد المستندات

المعلوماتية في حالة حذفها أو إضافتها أو التلاعب فيها بأي صورة سواء كانت البيانات مخزنة في ذاكرة الآلة أم كانت تمثل جزءا من برنامج التشغيل أو برنامج التطبيق ويجب في هذه الحالة أن تكون محلا للتجريم.

وعليه يكون تغيير الحقيقة في نطاق المعالجة الآلية للمعطيات عن طريق الحذف أو بإزالة كلمة أو رمز معين أو عن طريق الإضافة بزيادة عبارات أو بيانات غير صحيحة، أو بتغيير محتوى الرسائل المنقولة، فقد يستولي الفاعل على أمر دفع موجه من بنك لآخر ويزيف أو يزور الرسالة بحيث يتم الدفع لحسابه.

أو أن يلجأ الجاني إلى أحد طرق التزوير المعنوي لتحقيق جريمة بالتدخل في نظام الحاسب الآلي لتسجيل بيانات لم تصدر عن المتعاقدين أو إثبات واقعة كاذبة أو غير معترف بها أو إهمال وإغفال معلومة بما يسبب تحريفا للحقيقة في محررات الحاسب الآلي.

3- الضرر:

وهو عنصر أساسي في جريمة الغش المعلوماتي، فإذا تخلف الضرر انتفى التزوير ولو توافرت كل أركانه، فالضرر عنصر جوهري في جريمة الغش المعلوماتي، ولا يشترط القانون وقوع ضرر بالفعل بل يكفي احتمال وقوعه، ويكفي لقيام التزوير أن يكون الضرر ماديا أو أدبيا أو فرديا أو اجتماعيا، والبحث في توافر الضرر من عدمه مسألة تتعلق بالوقائع يفصل فيها قاضي الموضوع، ونظرا لعدم كفاية النصوص المتعلقة بالغش في المحررات لمواجهة الغش المعلوماتي الذي يقع في مجال المعالجة الآلية للمعطيات، فقد عاقب المشرع الفرنسي على الغش المعلوماتي الذي يقع في المستندات المعالجة آليا، سواء كانت داخل الجهاز أو خارجه[25].

فلا 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 عنصرا جوهريا لقيام الجريمة ويستوي في الضرر أن يكون ماديا أو أدبيا أو فرديا أو اجتماعيا، ومسألة توافر الضرر من المسائل الموضوعية التي تقدرها المحكمة حسب ظروف كل دعوى.

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 أو على سبيل المصادفة.

وقد نص المشرع الفرنسي في المادة 441-1 من قانون العقوبات أنه: "يعد تزويرا كل تغيير بطريق الغش في الحقيقة من شأنه أن يحدث ضررا....."، أما بالنسبة للمشرع الجزائري فإنه لم ينص صراحة على ضرورة أن يؤدي التزوير إلى إحداث الضرر حتى تقوم هذه الجريمة إلا أن التطبيقات القضائية تتطلب ذلك، فقد استقر الاجتهاد القضائي للمحكمة العليا على أنه لا تزوير بدون ضرر، وعلى ذلك فإنه بانعدام الضرر لا يمكن تطبيق العقوبات الواردة بالنص[26].

ويكون الشخص مرتكبا لجريمة الغش المعلوماتي إذا قام بما يلي:

1- يدخل أو يسبب الدخول في الحاسب الآلي أو أي جزء منه، أو إلى برنامج أو بيانات الحاسب بقصد ابتكار أو تنفيذ أي مشروع، و يضع حيلة للغش أو جزء من مخادعة.

2- يحصل على الاستعمال أو يتلف، أو يحطم حاسب آلي أو أي جزء منه أو يعدل أو يمحو أو يسحب أي برنامج أو بيانات موجودة في الحاسب الآلي بأي مشروع، عن طريق صلة أو غش أو جزء من مخادعة.

3- يدخل أو يسبب الدخول في حاسب آلي أو جزء منه، أو برنامج بيانات ويحصل على مال أو يسيطر على مال، أو ممتلكات، أو خدمات ذات صلة بأي مشروع.

المطلب الثاني: صور الركن المادي في جريمة الإتلاف المعلوماتي

قد يتخذ الركن المادي لجريمة إتلاف المعلومات إما صورة إجراء تعديلات غير مشروعة لها، أو تدميرها أو الإدخال غير المشروع للمعلومات داخل أنظمة الحاسبات الآلية:

1- التعديل غير المشروع للمعلومات:

يشكل التعديل غير المشروع للمعلومات المبرمجة آليا واحد من أكثر صور إتلاف المعلومات شيوعا، ويمكن تعريفه بأنه كل تغيير غير مشروع للمعلومات والبرامج يتم عن طريق استخدام إحدى وظائف الحاسب الآلي.

وقد فرقت التوصية الصادرة عن المجلس الأوروبي المتعلق بجرائم المعلوماتية بين التعديلات التي تؤدي إلى نتائج سلبية تتعلق بحالة المعلومات والبرامج وبين التعديلات غير المصرح بها والتي لا تؤدي إلى إحداث هذه النتائج بل قد تساعد على تحسين أي من المكونات المنطقية للحاسب الآلي ونظامه[27].

2- تدمير المعلومات:

يعد تدمير المعلومات بدوره صورة من صور الإتلاف وإن كان أبعد أثرا من مجرد إجراء بعض التعديلات للمعلومات، وقد أوصى التقرير الصادر عن المجلس الأوروبي بخصوص جرائم المعلوماتية بتجريم الأفعال التي تؤدي إلى تدمير المعلومات، ولقد ميزت التوصية الصادرة عن المجلس الأوروبي بين شكلين من أشكال التدمير الذي يلحق بالمعلومات، الأول يتعلق بمحو المعلومات تماما، والثاني بإخفاء المعلومات بحيث لا يمكن الوصول إليها دون أن يترتب على ذلك محو تماما، ويذهب البعض إلى أن إخفاء المعلومات دون محوها لا يمكن أن يشكل تدميرا لها، ومؤدى ذلك أن إخفاء أحد الملفات على سبيل المثال لا يترتب عليه محو المعلومات التي يحتوى عليها من ذاكرة الكمبيوتر وإنما يؤدي فقط إلى تعديل في قائمة الملفات وهو ما يعني أن إخفاء المعلومات في هذه الحالة لا يعدو أن يكون تعديلا وليس تدميرا[28].

ولإتلاف المعلومات صور وأشكال متعددة منها:

أولاً- الاعتداء على المعلومات مما يؤدي إلى إعاقة وتعطيل النظام عن العمل:

وينجم ذلك عن فعل يسبب تباطؤ أو ارتباك في عمل نظام المعالجة الآلية للمعلومات ويترتب على ذلك تغيير في حالة عمل النظام، ويسوي بعضهم بين عرقلة النظام عن العمل ومحو أو تعديل أو إلغاء المعلومات وحتى يمكن أن تتحقق الفاعلية في الإتلاف، ينبغي أن يوجه الفعل إلى برامج تشغيل النظام المعلوماتي وليس على المعلومات بالمعنى الضيق.

ثانياً. العدوان على المعلومات المخزنة بالنظام المعلوماتي:

تقع صورة الإتلاف المعلوماتي بتدمير وتخريب المعلومات المخزنة بالنظام المعلوماتي حيث تصير بلا معنى ولا يمكن الاستفادة منها وهو يسري على النظام المعلوماتي ككل وعلى التعاملات الإلكترونية عامة.

ثالثاً. تضخيم البريد الإلكتروني:

أن يتم إرسال نسخ مكررة بعدد كبير من الرسائل بما يترتب عليه من إعاقة سير النظام التقني المعلوماتي بشكل يؤدي إلى إعاقة استخدام تلك الخدمة أو توقفها وفي الغالب يتم هذا الأمر من خلال فيروسات معلوماتية يتم بثها ونشرها عن طريق الإنترنت.

رابعاً- بث الفيروسات المعلوماتية عبر شبكة المعلومات لتعطيل الاتصالات:

تعد جريمة بث الفيروسات من أخطر التهديدات التي تضر شبكة المعلومات فهذه الجريمة لا تقع ضد المعلومات أو البرامج بل تتم ضد تعديل أو إيقاف شبكة الاتصالات من خلال تدمير أو تخريب برامج الاتصال وتتحقق صورة الإتلاف المعلوماتي تلك من خلال القيام بإدخال أو تعديل أو محو المعلومات أو البرامج[29].

الخاتمة:

بعد التطرق لموضع صور الركن المادي للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، نجد أن المشرع الجزائري وعلى غرار باقي التشريعات الأخرى قد نص على مجموعة من الأفعال اعتبرها صورا للركن المادي لهذه الجرائم، وخصوصية هذه الصور تجد أساسها في خصوصية الجريمة الإلكترونية ذاتها، إلا أنه يلاحظ أن المشرع الجزائري لم يقدم تعريفا للأفعال التي اعتبرها صورا للركن المادي لهذه الجرائم، مما فتح الباب أمام إثارة مسألة تطبيق مبدأ الشرعية فيما يتعلق بالجرائم الإلكترونية، ذلك أن القواعد العامة لا تكفي وحدها للإحاطة القانونية بهذا النوع المستحدث من الإجرام والذي يعرف نشاطا متناميا نظرا للانتشار الرهيب لوسائل الاتصال والمعلوماتية، والتي أصبح معها الولوج إلى المعلومات المعالجة إلكترونيا أمر متاحا للجميع تقريبا.

وقد عمل المشرع الجزائري على إصدار مجموعة من النصوص القانونية تضمنت جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، إلا أن أهم النصوص القانونية التي تناولت مسألة الركن المادي لهذه الجرائم تضمنها قانون العقوبات من خلال نص المادة 394 مكرر، الذي جاء فيه النص على مجموعة من الأفعال التي ترتكب في الوسط الإلكتروني تشكل صورا للركن المادي للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي تتمثل في فعل الدخول والبقاء غير المصرح بهما، بالإضافة إلى جريمة الغش المعلوماتي وإتلاف المعلومات.

وبناءً على ما تقدم فقد توصلنا لجملة من النتائج التي تتعلق بموضوع البحث نوردها على النحو التالي:

- نص المشرع الجزائري على صور الركن المادي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من خلال نص المادة 394 مكرر من قانون العقوبات.

- اكتفى المشرع الجزائري بذكر فعل الدخول فنص على ذلك" ... كل من يدخل أو يبقى عن طريق الغش" ولم يذكر الأفعال المادية لفعل الدخول ولم يحدد الوسيلة أو الطريقة التي يتم بها الدخول إلى النظام، لذلك جرم أي وسيلة أو طريقة للدخول سواء تم الدخول بطريقة مباشرة أو غير مباشرة على عكس بعض التشريعات الأخرى التي وسعت من دائرة التجريم وذكرت مجموعة كبيرة من الأفعال التي قد تحدث نتيجة فعل الدخول.

- تقوم الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات بمجرد فعل الدخول إلى النظام دون ضرورة حدوث أية نتيجة أخرى، فلا يشترط لقيامها التقاط المتدخل للمعلومات التي يحتويها النظام أو بعضها أو استعمال تلك المعلومات، بل أن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات الموجودة على النظام.

- اعتبر المشرع أن البقاء الاحتيالي جريمة، حيث نص عليها في قانون العقوبات بقوله، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات... لذلك عرف البقاء الاحتيالي بأنه كل تواجد غير عادي كالاتصال بواسطة الشبكة المعلوماتية بالنظام المعلوماتي أي الدخول والنظر فيه، أي في المعطيات التي يتضمنها وغيرها من التصرفات غير مسموح بها والتي تشكل بدورها بقاءً احتياليا، فيتحقق الركن المادي في جريمة البقاء الاحتيالي إذا اتخذ صورة البقاء داخل النظام ويقصد بفعل البقاء" التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام.

الهوامش:

(1) عباوي نجاة، الإشكاليات القانونية في تجريم الاعتداء على أنظمة المعلومات، مجلة دفاتر السياسة والقانون، العدد 16، ورقلة، الجزائر، 2017، ص283.

(2) المادة 394مكرر من الأمر رقم 150/66 المؤرخ في 8 جوان المتضمن قانون العقوبات الجزائري المعدل و المتمم.

(3) دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة ماجستير، تخصص قانون جنائي، جامعة قسنطينة، كلية الحقوق، 2013، ص24.

(4) أنظر المادة 394 مكرر من الأمر رقم 150/66 المؤرخ في 8 جوان المتضمن قانون العقوبات الجزائري المعدل و المتمم.

(5) أنظر المادة الأولى من المرسوم الملكي السعودي المتعلق بنظام مكافحة الجرائم المعلوماتية السعودية، الصادر في 27،4،2008.

(6) تم الاطلاع على الموقع بتاريخ 59149.11،6،2016. http// www- assakina. com ./book .

(7) وقد حاولت بعض التشريعات معالجة فعل الدخول غير المصرح به، ومن بين هذه التشريعات ما نص عليه قانون جرائم أنظمة المعلومات الأردني في المادة (03): كل من دخل قصدا إلى موقع إلكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح يعاقب بالحبس ...وإذا كان الدخول بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالك فيعاقب الفاعل....

(8) بهاء فهمي الكبيجي، مدى توافق أحكام جرائم أنظم المعلومات في القانون الأردني، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، 2013، ص26.

(9) بهاء فهمي الكبيجي، المرجع السابق، ص29.

(10) قارة أمال، الجريمة المعلوماتية، رسالة ماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر، سنة 2002، ص42.

(11) المادة الأولى من القانون رقم 18-07 المؤرخ في 25 رمضان من عام 1439، الموافق لـ 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الصادر بالجريدة الرسمية عدد 2018/34.

(12) قارة أمال، المرجع السابق، ص43.

(13) دردور وسيم، المرجع السابق، 2013، ص30،31.

(14) قارة أمال، الجريمة المعلوماتية، ص43.

(15) أنظر المادة 394 مكرر فقرة الأولى من قانون العقوبات الجزائري.

(16). Bensoussan Alain (sous la direction de), Internet: aspect Juridique, édition Hèmes, Juin 1996 (France), page 109.

(17) لي عبد القادر قهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، 1999، ص133.

(18) علي عبد القادر قهوجي، المرجع نفسه، ص133.

(19) أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة الأولى، الديوان الوطني للأشغال التربوية، الجزائر، 2002، ص 85، 68.

(20) André Lucas ,jean Devréze jean Frayssinent , Droit de L'informatique et de l'internet edition Dallas ,collection thémis (Droit Privé) November 2001 (France) de la page 683 à 684.

(21) أنظر المادة 394 مكرر 3.2 قانون العقوبات الجزائري.

(22) نهاد كريدلي، بحث بعنوان الجريمة والاحتيال في البيئة الإلكترونية، كلية إدارة الأعمال الإسلامية، جامعة الإمام الأوزاعي، بيروت لبنان، 2008.

(23) محمود أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية، دار الثقافة للنشر و التوزيع الأردن، 2009، ص107.

(24) خثير مسعود، الحماية الجنائية لبرامج الكومبيوتر أساليب و ثغرات، دار الهدى، الجزائر طبعة 2010،ص134،135.

(25) خثير مسعود، المرجع نفسه، ص137.

(26) أمين طعباش، الحماية الجنائية للمعاملات الإلكترونية، مذكرة ماجستير في علم الإجرام والعقاب، كلية الحقوق، جامعة باتنة، 2013، ص70.

(27) خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، 2010، ص418.

(28) خالد ممدوح إبراهيم، المرجع نفسه، ص419.

(29) محمد نصر محمد، مركز الدراسات العربية للنشر والتوزيع، الوسيط في الجرائم المعلوماتية، الطبعة الأولى، 2015، ص53-54.