

ثانيا: من خلال النصوص القانونية المستحدثة (قانون 15/04)

لما كانت الحاجة ملحة و ضرورية لحماية المال المعلوماتي، فقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة لهذا الغرض، و قد استجابت عدة دول لهذا الاتجاه منها الولايات المتحدة الأمريكية، كندا، ألمانيا، النرويج و فرنسا... الخ .

و بالنسبة للتشريع الجزائري، فقد تدارك المشرع الجزائري مؤخرا - ولو نسبيا- الفراغ القانوني في مجال الإجرام المعلوماتي و ذلك باستحداث نصوص تجريبية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون رقم 15/04 المتضمن تعديل قانون العقوبات ، لكن تجدر الإشارة إلى أن المشرع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية، و أغفل الاعتداءات الماسة بمنتجات الإعلام الآلي و المتمثلة في التزوير المعلوماتي، و لذلك ارتأينا و حتى لا تكون دراستنا لموضوع الحماية الجزائية ناقصة أن نتعرض للاعتداءات الواردة على المعلوماتية من خلال الفرعين التاليين :

الفرع الأول : الاعتداءات الماسة بالأنظمة المعلوماتية

الفرع الثاني : الاعتداءات الماسة بمنتجات الإعلام الآلي

الفرع 01 : الاعتداءات الماسة بالأنظمة المعلوماتية

تشير الإحصائيات إلى وقوع ما بين 200 إلى 250 اعتداء يوميا على الأنظمة المعلوماتية في الجزائر¹.

إن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية ، استدعى تدخلا تشريعيًا صريحا سواء على المستوى الدولي أو الداخلي فدوليا وضعت أول اتفاقية حول الإجرام المعلوماتي بتاريخ 2001/11/08 تضمنت مختلف أشكال الإجرام المعلوماتي² أما على المستوى الوطني، فقد استدرك المشرع الجزائري الفراغ القانوني من خلال التعديل الأخير لقانون العقوبات الذي تم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 156/66 بقسم سابع مكرر عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات " ويشمل المواد من 394 مكرر إلى 394 مكرر 7.

الجرائم الماسة بالأنظمة المعلوماتية وان كانت تختلف في أركانها و عقوباتها إلا أن ما يجمعها أنهما تحقق حماية جزائية تنظم المعالجة الآلية للمعطيات ، أي أن القاسم المشترك بينهما هو نظام المعالجة الآلية ، ولذلك فان دراسة تلك الجرائم تقتضي منا أولا توضيح وبيان مفهوم نظام المعالجة الآلية للمعطيات.

أولا : مفهوم نظام المعالجة الآلية للمعطيات

يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أية جريمة من جرائم الاعتداء على هذا النظام . فان ثبت تخلف هذا الشرط الأولي ، لا يكون هناك مجال لهذا البحث، ويؤدي توافر هذا الشرط إلى الانتقال إلى المرحلة التالية وهي بحث توافر أركان أية جريمة من الجرائم السابقة ، إذ أن هذا

¹ - آمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة و النشر، الجزائر .

2006 .

² - الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ: 2001/11/08 من طرف المجلس الأوروبي و تم وضعها للتوقيع منذ تاريخ: 2001/11/23.

الشرط يعتبر عنصر لازما لكل منها , ولذلك يكون من الضروري تحديد مفهوم نظام الآلية للمعطيات .

نظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا عن انه تعبير متطور يخضع للتطورات السريعة و المتلاحقة في مجال فن الحاسبات الآلية³.

ولذلك فالمشرع الجزائري على غرار التشريع الفرنسي لم يعرف نظام المعالجة الآلية للمعطيات فأوكل بذلك مهمة تعريفه كل من الفقه و القضاء.

➤ تعريف نظام المعالجة الآلية للمعطيات⁴

الاتفاقية الدولية للإجرام المعلوماتي قدمت تعريف للنظام المعلوماتي في مادتها الثانية على النحو التالي:

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

أما الفقه الفرنسي فقد عرفه كما يلي:

كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة البرامج والمصطلحات وأجهزة الإدخال والإخراج وأجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهما معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية .

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

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

- العنصر الثاني: ضرورة خضوع النظام لحماية فنية.

➤ مكونات نظام المعالجة الآلية للمعطيات :

العناصر المادية والمعنوية التي يتكون منها المركب ومثال ذلك:الذاكرة، البرامج، المعطيات, أجهزة الربط... الخ. هذه العناصر واردة على سبيل المثال لا الحصر.

وهذا يفتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال , وعلى ذلك لا يتوافر نظام المعالجة الآلية للمعطيات ,ولا تقع بالتالي أي جريمة من جرائم الاعتداء عليه المنصوص عليها إذا وقع الاعتداء على برامج معروضة للبيع , أو على جهاز حاسب لم يدخل الخدمة أو على عنصر مودع بالمخازن، أو على قطع الغيار، أو على الأجهزة التي مازالت في حالة التجربة، أو حتى الأنظمة التي خرجت من الخدمة تماما و لكن على العكس من ذلك، تقع الجريمة إذا وقع الاعتداء على النظام خارج ساعات تشغيله العادية، أو إذا كانت أحد عناصره في حالة عطل أو حتى لو كان النظام كله في حالة عطل تام، و كان يمكن إصلاحه.

³ - د. علي عبد القادر القهوجي، المرجع السابق، ص 119-120.

⁴ - أنظر المادة 01 من الاتفاقية الدولية للإجرام المعلوماتي.

و تقع الجريمة أيضا إذا وقع الاعتداء على عنصر يشكل جزءا من أنظمة متعددة، فإذا تصورنا عدة أنظمة ترتبط فيما بينها بأجهزة اتصال و وقع اعتداء على جهاز حاسب آلي في نظام من تلك الأنظمة المرتبطة، فإن الجريمة تقع في هذه الحالة. و إذا كان الدخول إلى هذا الجهاز مشروع، فإن البحث في توافر الجريمة يتوقف على ما إذا كانت توجد علاقة سببية بين هذا الدخول المشروع و الاعتداء المفروض على الأنظمة ككل، و ومدى حسن اوسوء نية المتدخل كما تقع الجريمة إذا وقع الاعتداء على شبكة الاتصال التي تربط بين أكثر من نظام، لان تلك الشبكة تعتبر عنصر في كل نظام من الأنظمة التي تربط بينهما⁵.

➤ ضرورة خضوع النظام لحماية فنية⁶:

يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات وبالأخص حاليا شبكة الانترنت فهم يسعون لتأمين سرية الرسائل الالكترونية وسرية البيانات المتناقلة وخاصة بالأعمال التجارية الرقمية . ويمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة ، ويرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الاطلاع على الرسائل الالكترونية .

و تنقسم الأنظمة إلى ثلاثة أنواع :

- أنظمة مفتوحة للجمهور.
- أنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية.
- أنظمة قاصرة على أصحاب الحق فيها و تتمتع بحماية فنية.

و مقتضى تطبيق هذا العنصر أن النوع الثالث فقط من تلك الأنظمة هو الذي يتمتع بالحماية الجنائية أما النوع الأول و الثاني فلا يتمتعان بتلك الحماية، و هناك من يصرون عليه لأن الحماية الجزائية في نظرهم يجب أن تقتصر على الأنظمة المحمية. فنيا لأنه من الطبيعي في نظرهم، أن ما يقوم بالاستغلال يضع الوسائل الفنية اللازمة لمنع الغش و أن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم، و ليس من يهمل منهم في توفير الحد الأدنى لحماية أمواله ، و يكون دور القانون الجنائي في هذه الحالة دور وقائي و هذا أيضا هو ما يتفق و سياسة المشرع الجنائي و ما نلاحظه من المفهوم العام للحماية الجزائية للملكية.

بالرجوع إلى النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات لا تتضمن شرط الحماية الفنية و خرجت تلك النصوص الخالية منه تماما. و من المبادئ العامة المستقرة في تفسير القانون الجنائي أنه لا يجوز تقييد النص المطلق، أو تخصيص النص العام، إلا إذا وجد نص يجيز ذلك. و لا يوجد في حالتنا نص خاص يقيد إطلاق النص أو يخصص عمومه، و لذلك فإن عدم ذكر المشرع لشرط الحماية الفنية يعني أن المشرع أراد استبعاده. هذا بالإضافة إلى أن الحماية الجزائية يجب أن تمتد لتغطي كل أنظمة المعالجة الآلية للمعطيات سواء كانت تتمتع بحماية فنية أم لا.

و تطبيقا لذلك، فإنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيدا بوجود حماية فنية و لكن إذا نظرنا للوقائع ، نلاحظ أن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية

⁵ - د. علي عبد القادر القهوجي، المرجع السابق، ص 121.

⁶ - أمال قارة، المرجع السابق، ص 103.

فنية، بالإضافة إلى أن وجود مثل تلك الحماية يساعد على إثبات أركان الجريمة و بصفة خاصة الركن المعنوي⁷.

ثانيا: الأركان الأساسية

و تتمثل هذه الأركان فيما يلي :

1- الركن المادي :

يتمثل الركن المادي في أشكال الاعتداء على نظم المعالجة الآلية للمعطيات و التي هي:

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

هذه الاعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات كشرط مسبق بخلاف الاعتداءات على منتوجات النظام و سنتعرض إليها بالتفصيل فيما يلي:

➤ الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

نصت عليه المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 إلى 150000 دج".

كما نصت عليه المادة 02 من الاتفاقية الدولية للإجرام المعلوماتية.

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

* الصورة البسيطة:

أ- **فعل الدخول** : لا يقصد بالدخول هنا الدخول بالمعنى المادي، أي الدخول إلى مكان أو منزل أو حديقة، و في نفس الاتجاه إلى جهاز الحاسب الآلي و إنما يجب أن ينظر إليه كظاهرة معنوية، تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات. و لم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، و لذلك تقع الجريمة بأية وسيلة أو طريقة و يستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر⁸.

ب- **فعل البقاء Le maintien**⁹ :

قد يتخذ النشاط الإجرامي الذي يتكون منه الركن المادي في الجريمة محل الدراسة صورة البقاء داخل النظام، و يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام و قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول على النظام، و قد يجتمعان. و يكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى

7- د. علي عبد القادر القهوجي، المرجع السابق، ص 123.

8- د. علي عبد القادر القهوجي، المرجع السابق، ص 121.

9- د. علي عبد القادر القهوجي، المرجع السابق، ص 133.

النظام مشروعاً. و من أمثلة ذلك: إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده و ينسحب فوراً، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي. و يكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحاً له فيه الرؤية و الإطلاع فقط و يتحقق ذلك أيضاً بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، و التي يستطيع فيها الجاني الحصول على الخدمة التلفونية دون أن يدفع المقابل الواجب دفعه أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة، و قد يجتمع الدخول غير المشروع و البقاء غير المشروع معا و ذلك في الفرض الذي لا يكون فيه الجاني الحق في الدخول إلى النظام، و يدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، و يتحقق في هذا الفرض الاجتماع المادي للجرائم و إذا كانت تلك الجريمة على هذه الصورة تهدف أساساً إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق أيضاً و بصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها بل يمكن من خلالها تجريم سرقة وقت الآلة، و ذلك بالنسبة للموظف أو العامل أو غيرهما حين يسرق وقت الآلة ضد إرادة من له الحق السيطرة على النظام، و يقوم بطبع أو نسخ بعض المعلومات أو المعطيات أو البرامج¹⁰.

كما يمكن أن تطبق على الاستخدام غير المشروع البطاقات الممغنطة إما لسرقتها أو التزوير ثم استخدامها أو حتى إذا استخدمها صاحبها في سحب مبالغ دون أن يكون لديه رصيد كاف، أو عند عدم وجود الرصيد و تكون الجريمة في هذه الحالة هي جريمة البقاء غير المشروع داخل النظام بشرط أن يكون صاحب البطاقة يعلم مقدماً بأنه ليس له رصيد كاف و يمكن أيضاً تطبيقها على التصنت على المحادثات الهاتفية طالما أن أرقام الهواتف معالجة آلياً في نظام خاص بها. هذه الجريمة تعد جريمة سلوك مجرد، أي أنها تقع و تكتمل بمجرد الانتهاء من السلوك المكون لها و هو الدخول أو البقاء دون أن يطلب المشرع في نموذجها القانوني حسب نصوص التجريم أية نتيجة إجرامية¹¹.

* الصورة المشددة:

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

نصت المادة 394 مكرر 3/2 قانون العقوبات على طرفين تشدد بهما عقوبة جريمة الدخول و البقاء داخل النظام، و يتحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام و إما عدم صلاحية النظام لأداء وظائفه، و يكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع و تلك النتيجة الضارة، و لا يشترط أن تكون تلك النتيجة الضارة مقصودة، لأن تطلب مثل هذا الشرط يكون غير معقول، حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام عن طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة. كما لا يشترط أن تكون تلك النتيجة

10 - آمال قارة، المرجع السابق، ص 111.

11 - د. جميل عبد الباقي الصغير، جرائم التكنولوجيا الحديثة، دار النهضة العربية، ص 28.

مقصودة، أي على سبيل الخطأ غير أعمدي، فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة العمدية الأساسية و هي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره إلا إذا أثبت الجاني انتفاء تلك العلاقة، كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ.

➤ الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات:

نصت عليه المادتين 05 و 08 من الاتفاقية الدولية للإجرام المعلوماتي¹². لم يورد المشرع الجزائري نصا خاصا بالاعتداء العمدي على سير النظام و اكتفى بالنص على الاعتداء العمدي على المعطيات الموجودة بداخل النظام و ربما يجد ذلك تفسيره في أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه، و قد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات و الاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية. فإذا كان الاعتداء الذي وقع على المعطيات مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء العمدي على النظام، أما إذا كان الاعتداء الذي وقع على المعطيات غاية فإن الفعل يشكل جريمة الاعتداء العمدي على المعطيات.

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

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

➤ الاعتداءات العمدية على المعطيات:

نصت عليها المادة 03،04،08 من الاتفاقية الدولية للإجرام المعلوماتي ، كما نص المشرع الجزائري عليها في المادة 394 مكرر 2 في قانون العقوبات «يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريقة الغش المعطيات التي تتضمنها».

- الصورة الأولى: الاعتداءات العمدية على المعطيات الموجودة داخل النظام
النشاط الإجرامي في جريمة الاعتداء العمدي على المعطيات يتجسد في إحدى الصور الثلاث التالية¹³:

* الإدخال L'intrusion.

* المحو L'effacement.

* التعديل Modification.

لا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوافر الركن المادي. و أفعال الإدخال و المحو و التعديل تنطوي على التلاعب في المعطيات التي يحتويها

12 - أمال قارة، المرجع السابق، ص 114.

13 - أمال قارة، المرجع السابق، ص 120.

نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل و هذا يعني أن النشاط الإجرامي في هذه الجريمة إنما يرد على محل أو موضوع محدد و هو المعطيات أو المعلومات التي تمت معالجتها آليا و التي أصبحت مجرد إشارات أو رموزا تمثل تلك المعلومات، و ليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام، أي التي يحتويها النظام و تشكل جزءا منه.

لا تقع الجريمة على مجرد المعلومات التي لم يتم إدخالها بعد إلى النظام أو تلك التي دخلت، و لم يتخذ حيالها إجراءات المعالجة الآلية، أما تلك التي في طريقها إلى المعالجة حتى و لو لم تكن المعالجة قد بدأت بالفعل تتمتع بالحماية الجنائية، و يكون هناك مجال للقول بتوافر الجريمة التامة أو الشروع على حسب الأحوال.

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

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

- الإدخال L'intrusion:

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل، و يتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة، هاته الأخيرة ليسحب بمقتضاها النقود من أجهزة السحب الآلي و ذلك حين يستخدم رقمه الخاص و السري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه، و كذلك الحامل الشرعي لبطاقة الائتمان و التي يسدد عن طريقها مبلغ أكثر من المبلغ المحدد له و بصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب « فيروس... الخ» يضيف معطيات جديدة .

- المحو L'effacement :

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

- التعديل Modification:

يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام و استبدالها بمعطيات أخرى، و يتحقق فعل المحو و التعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها و ذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات و برنامج المحاة Gomme

d'effacement أو برنامج الفيروسات بصفة عامة¹⁴، و هذه الأفعال المتمثلة في الإدخال و المحو و التعديل و ردت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى و لو تضمن الاعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينهما، لأن كل تلك الأفعال لا تنطوي لا على إدخال و لا على تعديل بالمعنى السابق.

- الصورة الثانية: المساس العمدي بالمعطيات خارج النظام

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

1- نص المادة 394 مكرر 2 يستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم معالجتها آلياً، فمحل الجريمة هو المعطيات سواء كانت مخزنة كأن تكون مخزنة على أشرطة أو أقراص أو تلك المعالجة آلياً أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

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

2- الركن المعنوي

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

➤ الدخول و البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات:

الولوج و التجول و البقاء داخل نظام المعالجة الآلية للمعطيات لا يجرمان إلا تما عمداً. المادة 02 من الاتفاقية الدولية للإجرام المعلوماتي تسمح للدولة العضو أن تشترط بأن ترتكب الجريمة عن طريق خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة بداخله. جريمة الدخول أو البقاء داخل النظام جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم و الإرادة.

فيلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء و أن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام و البقاء فيه، و عليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاءه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، فإذا توافر القصد الجنائي بعنصريه العلم و الإرادة فإنه لا يتأثر بالبائع على الدخول أو البقاء فيظل القصد قائماً حتى و لو كان البائع هو الفضول أو إثبات القدرة على المهارة و الانتصار على النظام¹⁵.

14 - آمال قارة، المرجع السابق، ص 122.

15 - د. علي عبد القادر القهوجي، المرجع السابق، ص 136-137.

بالنسبة لنية الغش تبدو من خلال الغش الذي يتم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام، بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام. في الحقيقة أن الدخول و البقاء بالغش لا يتضمن معنى خرق الجهاز الرقابي للنظام، إنما يظهر من خلال الولوج دون وجه حق إلى النظام إلا أن الجهاز الرقابي ما هو إلا وسيلة لإثبات أن الدخول للنظام غير مرخص به.

➤ الاعتداءات على سير نظام المعالجة الآلية للمعطيات :

إن هذه الجريمة جريمة عمدية ، إذ أن من المفترض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية وهذا ما يميزه عن الاعتداء غير العمدى لسير النظام الذي يشكل طرفاً مشدداً لجريمة الدخول والبقاء الغير مشروع داخل النظام وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة¹⁶.

➤ الاعتداءات العمدية على المعطيات:

جريمة الاعتداء العمدى على المعطيات جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يعلم الجاني بان نشاطه الجرمي يترتب عليه التلاعب في المعطيات، ويعلم أيضاً أن ليس له الحق في القيام بذلك وانه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته¹⁷.

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

3 - استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية :

وذلك إما بالتصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسله عن طريق منظومة معلوماتية.

حياسة أو إفشاء أو نشر أو استعمال لأي غرض كان للمعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية .فان هذا الاستخدام يجب أن يكون عمداً وبطريق الغش أي بتوافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش.

ثالثاً : الجزاءات المقررة

وستتناول فيما يلي الجزاءات التي قررها المشرع الجزائري لهذا النوع من الإجرام الحديث . طبقاً للمادة 13 من الاتفاقية الدولية للإجرام المعلوماتي فإن العقوبات المقررة للإجرام المعلوماتي يجب أن تكون رادعة وتتضمن عقوبات مالية للحرية ، والتي تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي ، كما توجد عقوبات تطبق على الشخص المعنوي بناءً على تبني مبدأ مسالة الشخص المعنوي الواردة في المادة 12 من الاتفاقية.

1- العقوبات المطبقة على الشخص الطبيعي :

➤ العقوبات الأصلية :

16 - د. علي عبد القادر القهوجي، المرجع السابق، ص142.

17 د - علي عبد القادر القهوجي، المرجع السابق، ص145.

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

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

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

ج/ الاعتداء العمدي على المعطيات : طبقا لنص المادة 394 مكرر 2 فالعقوبة المقررة للاعتداء العمدي على المعطيات الموجودة داخل النظام هي الحبس من ستة أشهر إلى ثلاث سنوات و غرامة من 500000 دج إلى 2000000 دج أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، العقوبة المقررة هي الحبس من شهرين إلى ثلاث سنوات و غرامة من 1000000 دج إلى 5000000 دج .

➤ العقوبات التكميلية:

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

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

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

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

➤ الظروف المشددة:

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

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

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

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

2- العقوبات المطبقة على الشخص المعنوي :

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

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

كما تجدر الإشارة إلى أن المشرع الجزائري قد اقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي وذلك في نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات الذي ينص على أن: " العقوبات المطبقة على الشخص المعنوي في مواد الجنايات و الجنج هي :

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

ب/ واحدة أو أكثر من العقوبات الآتية:

- حل الشخص المعنوي
 - غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات
 - الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات
 - المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات.
 - مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
 - نشر أو تعليق حكم الإدانة.
 - الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات ، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبةه .
- بالنسبة لعقوبات الغرامة المطبقة على الشخص المعنوي عند ارتكابه أحد الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة 394 مكرر 4 قانون العقوبات 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

3- عقوبة الاتفاق الجنائي:

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتية وقد تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر 5 ، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ولم يخضعها لأحكام المادة 176 من قانون العقوبات المتعلقة بجمعية الأشرار ، حيث تنص المادة 394 مكرر 5 من قانون العقوبات : " كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية ، يعاقب بالعقوبات المقررة بالجريمة ذاتها " .

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

ويعاقب المشرع الجزائي على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد. وشروط المعاقبة على الاتفاق الجنائي بمن استخلصها من نص المادة 394 مكرر 5 م قانون العقوبات، والتي هي:

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

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

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

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

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

فعل المشاركة في الاتفاق إذ أن المجرم بنص المادة 394 مكرر 5 ليس الاتفاق وإنما المشاركة من طرف شخص طبيعي أو معنوي فبمجرد الانضمام إلى الاتفاق غير كافي بل يجب توافر فعل إيجابي للمشاركة.

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

4- عقوبة الشروع في الجريمة :

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

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

يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، إذ جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب بنفس عقوبة الجريمة التامة، ومن خلال استقراء نص المادة نستنتج أن الجنحة الواردة بنص المادة 394 مكرر 5 من قانون العقوبات مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي .

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

الفرع 02: الاعتداءات على منتوجات الإعلام الآلي – التزوير المعلوماتي-

إن الدعائم المادية للحاسب الآلي قد احتلت مكانة المحررات والصكوك ونظرا لأهمية وخطورة ما تحتويه من بيانات والتي قد تكون محلا للاعتداء بتغيير حقيقتها بقصد الغش في مضمونها، والذي من شأنه إحداث أضرار مادية أو معنوية¹⁸. كتزوير المستخرجات الإلكترونية كالأوراق المالية أو السحب على الجوائز.

جريمة التزوير في المجال المعلوماتي من أخطر صور غش المعلوماتية نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسب الآلي الآن والذي اقتحم كافة المجالات وأصبحت تجري من خلال كم هائل من العمليات ذات الآثار القانونية الهامة والخطيرة والتي لا يصدق عليها وصف " المكتوب" في القانونين المدني والجنائي، وقد أثار هذا الوضع الشك حول دلالتها في الإثبات وحول إمكانية وقوع جريمة التزوير العادية ولهذا كان التدخل التشريعي ذو أهمية بالغة. تجدر الإشارة إلى أن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي، ربما إقتداء بما فعله المشرع الفرنسي الذي أخضع أفعال التزوير المعلوماتي للنصوص العامة للتزوير وذلك بعد أن قام بتعديله بجعل موضوع التزوير أي دعامة مادية وليس محررا، الفرق أن النصوص الواردة في قانون العقوبات الجزائري الخاصة بالتزوير تجعل التزوير يرد على محرر وعليه لا يمكن إخضاع أفعال التزوير المعلوماتي للنصوص العامة للتزوير كما هو عليه الحال في التشريع الفرنسي مما يستدعي تدخلا تشريعا، إما بتعديل نصوص التزوير التقليدية أو بإدراج نص خاص بالتزوير المعلوماتي

أولا: مفهوم منتوجات الإعلام الآلي

سنعرض من خلال هذا العنوان التفرقة بين مفهومين هما المستند المعالج أليا والمستند المعلوماتي ➤ **المستند المعالج أليا¹⁹ :**

18 - أمال قارة، المرجع السابق، ص 193.

19 - أمال قارة، المرجع السابق، ص 134

يقصد بالمستند في الاصطلاح القانوني كل دعامة مادية (مكتوب أو أي شيء) تصلح لأن تكون عليها معلومات أو أراء والتي هي غير مادية، 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 خلافة) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام معالجة آلية، ويستوي بعد ذلك أن يكون هذا الشيء قد خرج من الآلة و تم تصنيفه أو تخزينه أو أنه مازال بداخلها انتظارا لاستخراجه أو تعديله

المستند المعالج أليا هو كل دعامة مادية مهيأة لاستقبال المعلومات والتي تسجل المعطيات عليها من خلال تطبيق إجراءات المعالجة الآلية للمعلوماتية أي من خلال نظام المعالجة الآلية للمعلومات، بعبارة أخرى يقصد بالمستند المعالج أليا الدعامة المادية التي تم تحويل المعطيات المسجلة عليها لغة الآلة²⁰.

➤ **المستند المعلوماتي :**

وهو ذلك المستند غير المعالج أليا وتعتبر مستندات معلوماتية 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 البرامج، وكذلك أيضا البطاقات البنكية التي لم تدخل الخدمة بعد وهذه إن كان مسجلا عليها معلومات مكتوبة بخط اليد أو مطبوعة أو محفورة، إلا أنه لم يتم معالجتها بعد، إذ أنها مازالت في مرحلة الإعداد فقط .

ثانيا : مدى خضوع منتوجات الإعلام الآلي لنصوص التزوير

الاعتداء على منتوجات الإعلام الآلي يتجسد في فعل التزوير المعلوماتي الذي نصت عليه المادة 7 من الاتفاقية الدولية للإجرام المعلوماتي إذ أن التلاعب في المعطيات الذي ينتج عنه معطيات غير أصلية يعد تزويرا .

الإشكال المطروح هو هل يمكن تطبيق نصوص التزوير الواردة في قانون العقوبات الجزائري على الاعتداءات الماسة بمنتوجات الإعلام الآلي ؟
للإجابة على هذا التساؤل وجب التطرق إلى مدى انطباق وصف المحرر على البيانات المعالجة أليا ومدى خضوعها لفعل تغيير الحقيقة.

➤ **مدى انطباق وصف المحرر على منتوجات الإعلام الآلي:**

موضوع جريمة التزوير هو المحرر والمحرر في مضمونه كتابة مركبة من حروف أو علامات تدل على معنى أو فكرة معينة، وإمكانية القراءة البصرية لمحتواه، وهو ما تفرضه نصوص التزوير التقليدية، وعليه يمكن إجمال خصائص المحرر في ثلاث نقاط:

- أن يتخذ المحرر شكلا كتابيا ويجب إدراك مضمون المحرر بالنظر إليه أو لمسه وإذا استحالت قرأته فلا يصلح وسيلة للإثبات و لا عقاب على ماحتواه من تغيير.
- أن تكون الكتابة منسوبة لشخص معين .
- أن يحدث المحرر أثارا قانونية.

فهل يعتبر البيان المعالج أليا من قبيل المحررات التقليدية التي يسري عليها النص الجنائي الخاص بالتزوير ؟

بإسقاط المفهوم التقليدي للمحرر على مجال المعالجة الآلية للبيانات ، نجد أن تغيير الحقيقة الذي يكون محله الأشرطة الممغنطة لا تقع به جريمة التزوير في المحررات وذلك لعدم وجود عنصر

الكتابة ف جريمة التزوير تشترط الكتابة بأي تغيير في الوعاء أ معلوماتي لا يعتبر تزويرا لانقفاء هذا الشرط .

الفقيه (DEVEY) يقرر أن الكتابة مطلب تقليدي في جرائم التزوير، لكن تجدر الإشارة إلى أن بعض الفقه الفرنسي يرى إمكانية تغليب روح النصوص واعتبار ما يظهر على شاشة الحاسب شكلا مستحدثا للمحرر²¹ .

الفقه البلجيكي يرى أن نصوص التزوير في المحررات يمكن أن تنطبق في حالة ظهور المعلومات التي تم تزويرها في المستخرجات الورقية . كما أن جانبا من الفقه السوري يرى تطبيق نصوص التزوير عندما تكون البيانات قد سجلت على أسطوانة أو شريط ممغنط بحيث يعتبر محررا .

وتغيير الحقيقة فيه يعد تزويرا وذلك بسبب انتقال المعلومات و المعطيات المخزنة إلى جسم مادي له سمات المحرر المكتوب و الذي يمكن قراءته بالعين باستخدام الحاسب للكشف على محتواه من قبل الغير فالعبارة بالمادة التي دُون عليها.

و قد ذهبت بعض التشريعات كمصر (المادة 211) إيطاليا (المادة 485) بلجيكا (المادة 190) فنلندا وسويسرا إلى اشتراط وجود المحرر بمفهومه التقليدي لتطبيق جريمة التزوير، بان يكون محتوى الوثيقة أو الوعاء قابلا للمشاهدة البصرية، فلا يشمل ذلك البيانات المخزنة الكترونيا .

وقد عمدت بعض التشريعات الحديثة لمواجهة القصور في النصوص التقليدية، إلى استحداث نصوص تجرime جديدة أو إدخال تعديلات على التشريعات التقليدية، من أجل المعاقبة على جريمة التزوير الواقعة على المستندات المعلوماتية، حفاظا على الثقة الواجب توافرها في المستندات المعلوماتية . ومن أمثلة هذه التشريعات التشريع الفرنسي الذي استحدث نصوصا خاصا بالتزوير أ معلوماتي و هو المادة 9/462 من قانون العقوبات وذلك بموجب تعديل 1988، غير أنه و بموجب تعديل 1994 تراجع المشرع الفرنسي عن موقفه وألغى النص الخاص بالتزوير أ معلوماتي، و أخضعه لنصوص التزوير التقليدية.

وكان السبب الذي أدى إلى إلغاء النص الخاص بالتزوير أ معلوماتي هو أن أفراد جرائم التزوير الواقعة على المستندات المعلوماتية سوف يكون من غير جدوى مادام مفهوم التزوير غير واضح، وهو ما دفع بالمشرع الفرنسي إلى إدراج تعريف للتزوير في نص المادة 441 من قانون العقوبات التي أصبحت تشمل كل صور التزوير الحديثة التي تنشأ عن استخدام الحاسب الآلي، كما أن الغاية من تجريم أفعال التزوير هو حماية الثقة العامة، التي تنشأ من تعامل الأفراد بالمحدرات بمفهومها التقليدي، ووضع نص خاص بالتزوير أ معلوماتي يحقق حماية للنظام أ معلوماتي فقط دون الحفاظ على الثقة العامة، وعن طريق وضع نص خاص بالتزوير أ معلوماتي تخرج المحررات المعلوماتية من المفهوم التقليدي للمحرر مما ينقص من ثقة المتعاملين بها، لذلك فإن إلغاء النص يخضع المحررات المعلوماتية إلى النصوص التقليدية الخاصة بالتزوير، بالمفهوم الجديد للمحدرات .

أما بالنسبة للتشريع الجزائري فيعد من التشريعات التقليدية، حيث أدرج النصوص الخاصة بتزوير المحررات في الأقسام الثالث والرابع و الخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات في المواد 124 إلى 229 التي تشترط المحرر لتطبيق جريمة التزوير، ولم يتخذ أي موقف لتوسيع مفهوم المحرر من أجل إدماج المستندات المعلوماتية ضمن

21 - أمال قارة، المرجع السابق، ص137.

المحركات محل جريمة التزوير ، وكان من الأفضل لو أضاف المشرع الجزائري في باب التزوير في المحركات نصا يعرف فيه التزوير .

وعليه نقترح إضافة نص إلى باب التزوير في المحركات يعرف فيه التزوير على النحو التالي: كل تغيير للحقيقة بطريق الغش في مكتوب أو في أي دعامة أخرى تحتوي تعبيراً عن الفكر. وهذا النص قد يكون أشمل حيث يمكن أن تدرج فيه جميع المستندات المعلوماتية حتى وإن كانت غير معالجة آلياً، وهو ما يتضمن حماية جزائية فعالة لكافة المنتجات المعلوماتية.

➤ مدى خضوع منتوجات الإعلام الآلي للنشاط الإجرامي لجريمة التزوير:

النشاط الإجرامي لجريمة التزوير يتمثل في فعل تغيير الحقيقة و يعني استبدالها بما يخالفها وإذا انتفى هذا التغيير انتفى التزوير و المقصود هو تغيير الحقيقة القانونية النسبية وليس تغيير الحقيقة الواقعية المطلقة، إذ يكفي لتغيير الحقيقة الذي تتطلبه جريمة التزوير أن يكون هناك مساس بحقوق الغير، أو مراكزهم القانونية الثابتة في تلك المحركات، وعليه يمكن تصور تغيير الحقيقة في نطاق المعالجة المعلوماتية بالتلاعب في المعطيات مما يؤثر على أصالتها²².

و تجدر الإشارة إلى أن تحويل البرامج أو قواعد البيانات لا يعد تزوير و إنما يقع تحت طائلة نصوص التقليد الواردة في قانون حق المؤلف و الحقوق المجاورة.

لا يتصور وقوع فعل تغيير الحقيقة من خلال طرق التزوير المعنوية - و التي كما هو معروف- لا تتحقق إلا أثناء تكوين المستند بالنسبة إلى للجريمة محل البحث.

بينما من المتصور وقوع فعل تغيير الحقيقة بالنسبة لهذه الجريمة من خلال طرق التزوير المادية، ولكن بشرط أن يكون التزوير لاحقاً على نشأة المستند الأصلي و الحقيقي المعالج آلياً فلا تتحقق تلك الجريمة من خلال فعل تغيير الحقيقة باستخدام طريقة التزوير المادية أثناء نشأة المستند على خلاف جريمة التزوير العادية²³.

نخلص إلى أن المشرع الجزائري رغم تداركه من خلال القانون 15/04 و المتضمن قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على الأنظمة المعلوماتية باستحداث نصوص خاصة، إلا أنه أغفل تجريم الاعتداءات الواردة على منتوجات الإعلام الآلي، فلم يستحدث نصاً خاصاً بالتزوير المعلوماتي، و لم يتبنى الاتجاه الذي تبنته التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث.

22 - أمال قارة، المرجع السابق، ص 139.

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