

جامعة سعد دحلب بالبليدة
كلية الحقوق و العلوم السياسة
قسم القانون العام

مذكرة ماجستير

التخصص: علم العقاب و الإجراءات الجزائية

الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري

من طرف

جبار فطيمة

أمام اللجنة المشكلة من:

رئيساً	جامعة سعد دحلب -البليدة-	أستاذ محاضر(أ)	د.محي الدين جمال
مشرفا ومقررا	جامعة سعد دحلب -البليدة-	أستاذ التعليم العالي	أد.بلقاسم احمد
عضوا مناقشا	جامعة سعد دحلب -البليدة-	أستاذ محاضر (أ)	د.شربال عبد القادر
عضوا مناقشا	جامعة سعد دحلب -البليدة-	أستاذ محاضر (ب)	د.رامي حليم

البليدة ، فيفري 2013

الشكر

الشكر أولاً لله سبحانه وتعالى فله الحمد حمداً طيباً مباركاً فيه

ثم الشكر لأستاذي القدير المشرف الدكتور أحمد بلقاسم لقبوله الإشراف على هذه المذكرة وعلى كافة النصائح والتوجيهات القيمة التي أبدأها لي طيلة إعدادي لهذه المذكرة، والتي لولاها ما أنجز هذا البحث

والشكر موصول لرئيس لجنة المناقشة الدكتور محي الدين جمال

وأعضاء اللجنة على قبولهم مناقشة هذه المذكرة رغم إنشغالهم ووقتهم الثمين

إهداء

إلى من حملتني وهنا على وهن، وقال فيها الحبيب المصطفى الجنة تحت قدميها

إلى من إذا سمعت صوتها لم أجد سوى نبرات الحب، وإذا عانقتها أدركت أنني لا أريد في هذه الدنيا
سوى إرضائها وإسعادها

إلى الذي لم أعهد فيه طول حياتي إلا الحزم والعزم والجد، إلى من أعتبره مثلي الأعلى ومعلمي الأول
في هذه الحياة

إلى من إذا أحسست بالضعف إلتجأت إليه فيمدني قوة، وإذا أحسست بالضياع زادني يقينا

إلى من ضل يشق لي درب المستقبل بنور خافت هو أنيسي كل يوم

إلى من قرن المولى عز وجل طاعتها بطاعته وبرهما ببره

إلى من زرعنا في حب التعلم منذ صباي وعلمانني أن من قال العلم نور والجهل ظلام لم يخطأ

والدي الكريمين

إلى اللاتي قلن لي إنطلق في طلب العلم فأنت تحققين أحلامك وأحلامنا

إلى الذين تألموا لألمي وفرحو لفرحي، إلى اللذين أشد بهم أزمري

إخوتي وأخواتي

إلى من أناروا لي طريق العلم طوال مشواري الدراسي دون كلل أو ملل

أساتذتي الكرام

إلى من مدّ لي يد العون دون تردد

صديقاتي

ملخص

لقد أفرزت الثورة التكنولوجية تطورا هائلا في مجال الإتصالات والمعلومات نتج عنه أن أصبح للمعلومات قيمة إقتصادية عالية في السوق العالمية.

و مع هذا التنامي الهائل للمعلومات وعجز الوسائل التقليدية عن تنظيمها وتسهيل الإستفادة منها أصبح ضروريا البحث عن وسائل أكثر تقدما وفعالية تقوم بحصر هذه المعلومات وجمعها ومعالجتها وإسترجاعها بسرعة فائقة ودقة متناهية، لذلك ظهرت أجهزة جد متطورة تملك هذه الخاصية لإحتوائها على ما يعرف بنظام المعالجة الآلية للمعطيات، وعلى رأسها جهاز الحاسب الآلي.

و ككل تطور في الوجود يحمل بين طياته بذور الخير والشر فإن هذه التكنولوجيا حملت بين طياتها جانبا مظلما أفرزه إستعمالها لأغراض غير مشروعة، وهو ما يطلق عليها بالجريمة المعلوماتية أو كما أثر المشرع الجزائري أن يطلق عليها تسمية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

و رغم أن المشرع الجزائري قد تنبه لهذه الجرائم وبدأ بمكافحتها بوجود العديد من الدول العربية التي لم تنظم هذه المسألة بعد، وذلك بتعديله لقانون العقوبات بالقانون 15/04 بإضافة قسم سابع مكرر عنوانه المساس بأنظمة المعالجة الآلية للمعطيات من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 بالإضافة إلى إصداره للقانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، بحيث تضمن الجانب الإجرائي لتنظيم هذه الجريمة.

إلا أنه تشريع مازال ينقصه الكثير للوقوف أمام هذا المد الإجرامي المدمر، وترجع الصعوبة في مواجهة هذه الجريمة إلى طبيعتها الخاصة من حيث موضوعها وأسلوب إرتكابها ومرتكبيها لهذا على المشرع الجزائري أن ينظم هذه المسألة بتعديل قانون العقوبات حتى تتوافق نصوصه مع هذه الجرائم ولما لا إستحداث نص خاص بها.

الفهرس

الشكر

الاهداء

9مقدمة
16الفصل 1: ماهية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات
171-1: مفهوم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات
171-1-1: تعريف نظام المعالجة الآلية للمعطيات
181-1-1-1: المقصود بنظام المعالجة الآلية للمعطيات
192-1-1-1: عناصر النظام المعلوماتي
233-1-1-1: ضرورة خضوع النظام لحماية فنية
252-1-1: مفهوم المعطيات
251-2-1-1: تعريف المعطيات
262-2-1-1: تمييز المعطيات عما يشابهها
323-2-1-1: عناصر المعطيات محل الحماية
344-2-1-1: الطبيعة القانونية للمعطيات
383-1-1: تعريف الجريمة المعلوماتية
381-3-1-1: المقصود بالجريمة المعلوماتية
412-3-1-1: موضوع الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات
482-1: خصائص الجريمة المعلوماتية

481-2-1: أطراف الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات
481-1-2-1: المجرم المعلوماتي
552-1-2-1: المجني عليه في الجريمة المعلوماتية
572-2-1: صعوبة توقيع الجزاء في الجريمة المعلوماتية
581-2-2-1: صعوبة إكتشاف الجريمة المعلوماتية
602-2-2-1: صعوبة إثبات الجريمة المعلوماتية
623-2-2-1: مشكل الإختصاص القضائي
713-1: المشكلات العملية بشأن الحماية الإجرائية من الجرائم المعلوماتية
711-3-1: التفتيش
721-1-3-1: مفهوم التفتيش
802-1-3-1: مدى قابلية مكونات الحاسوب والشبكة للتفتيش
832-3-1: ضبط مكونات الجريمة
831-2-3-1: ضبط مكونات الكمبيوتر
852-2-3-1: ضبط الرسائل ومراقبة الإتصالات الإلكترونية
892: صور الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات
901-2: الجرائم الماسة بنظام المعالجة الآلية للمعطيات
901-1-2: جريمة الدخول داخل نظام المعالجة الآلية للمعطيات
911-1-1-2: الركن الشرعي
932-1-1-2: الركن المادي
993-1-1-2: الركن المعنوي
4-1-1-2: العقوبات المترتبة على جريمة الدخول داخل نظام المعالجة الآلية
102للمعطيات
1052-1-2: جريمة البقاء داخل نظام المعالجة الآلية للمعطيات
1061-2-1-2: الركن الشرعي

107 2-2-1-2: الركن المادي.
111 3-2-1-2: الركن المعنوي.
	4-2-1-2: العقوبات المترتبة على جريمة البقاء داخل نظام المعالجة الآلية
114 للمعظيات.
118 2-2: الجرائم الماسة بالمعظيات.
119 1-2-2: جريمة التلاعب بالمعظيات.
119 1-1-2-2: الركن الشرعي.
120 2-1-2-2: الركن المادي.
125 3-1-2-2: الركن المعنوي.
126 4-1-2-2: العقوبات المقررة لجريمة التلاعب بالمعظيات.
128 2-2-2: جريمة التعامل في المعظيات.
	1-2-2-2: جريمة التعامل بالمعظيات التي تصلح لأن ترتكب بها جرائم
128 معلوماتية.
135 2-2-2-2: جريمة التعامل في معظيات متحصلة من جريمة.
139 3-2-2-2: الركن المعنوي لجريمة التعامل بالمعظيات بصورتها.
140 4-2-2-2: العقوبة المقررة.
142 3-2: الأحكام المشتركة بين جرائم الإعتداء على أنظمة المعالجة الآلية للمعظيات.....
142 1-3-2: الأحكام المشتركة المتعلقة بالجريمة.
142 1-1-3-2: العقاب على الاتفاق الجنائي المجسد بأعمال مادية.
150 2-1-3-2: العقاب على الشروع.
156 2-3-2: الأحكام المشتركة المتعلقة بالعقوبة.
156 1-2-3-2: العقوبات التكميلية.
161 2-2-3-2: تشديد عقوبة الجريمة المرتكبة من قبل الشخص المعنوي.
166 3-2-3-2: الجرائم المعلوماتية المرتكبة ضد الهيئات والمؤسسات العامة.

173الخاتمة:

177قائمة المراجع

184الملاحق:

مقدمة

لقد أنعم الله على الإنسان بنعمة العقل والعلم، فعن طريقهما بدأ يطور أسلوب معيشتته، فبعد أن كان يعيش عصر الصيد، ويعتمد على الرعي والترحال، بدأ يعرف الزراعة وحياة الاستقرار، ثم دخل عصر الثورة الصناعية التي بدأت باختراع الآلة وظهور الصناعات المختلفة، التي ترتبت عليها آثار ضخمة غيرت خريطة البشرية، كان أبرزها تقسيم دول العالم بين دول متقدمة تزداد تقدما، ودول نامية تحاول التقدم، وأخرى متخلفة ما زالت قابضة في التخلف.

و لم تقف رحلة الإنسان في تطوره عند العيش في ظل الثورة الصناعية، فما إن أوشك القرن الماضي على الزوال حتى بدأ الإنسان يعيش إرهاصات ثورة جديدة قلبت مناحي الحياة المختلفة رأسا على عقب، وهي ثورة تكنولوجيا المعلومات، خاصة بعد أن حدث الاندماج بين المعلوماتية L'INFORMATIQUE وبين الاتصال عن بعد LA TELECOMMUNICATION وظهور ما يسمى بالمعلوماتية عن بعد LA TELEMATIQUE فهذه المعلوماتية الأخيرة قد جعلت العالم كله إلى وحدة سكونية واحدة. [1] ص 1

فكثر الطلب على المعلومات التي زادت غزارتها، وضخامة عدد كتبها ووثائقها لدرجة بات معها أمر حفظها وتخزينها يستلزمان مكتبات كثيرة، وأماكن واسعة، وتصنيفها وتبويبها يتطلبان وقتا وجهدا كبيرين، والرجوع إليها لا يقل عن ذلك جهدا أو وقتا.

كان لابد من التفكير بوسيلة يتم من خلالها تجاوز هذه المشكلات إلى أن ظهر الحاسوب وبدأ بالعمليات الحسابية، ثم تطور ليشمل أعمال التخزين واستيعاب كبير للمعلومات، وتجميعها وترتيبها وإسترجاعها بسرعة فائقة ودقة متناهية، فصارت المعلومات في متناول الأيدي بجهد بسيط. [2] ص 13

وقد ترتب على هذه الثورة الهائلة في مجال تكنولوجيا المعلومات والاتصالات، وفي صناعة الإلكترونيات أن أصبح العالم يعيش حياة زاخرة بالاتصالات السريعة، ونقل المعلومة عبر المسافات والتحاو مع قواعد البيانات المحلية والعالمية، والتعامل مع نظم متقدمة للخبرة والذكاء الاصطناعي، كل

هذا ما كان يمكن أن يتحقق لولا وجود هذا الشيء الرائع المسمى حاسوب Computer والذي تتجلى عظمته في الشبكات الاتصالية المتشعبة "distributed computers networks" [3] ص 7

وككل شيء في الوجود يحمل في طياته بذور الخير والشر، فإن هذا الجهاز العجيب هو الآخر كانت له ايجابيات وسلبيات خاصة في الفرض الذي يكون فيه مرتبط بشبكة للمعلومات كالانترنت، فمن ايجابياته التي جاء بها هي سهولة التحكم في المعلومة بالإضافة إلى سهولة الوصول إليها في أي وقت واسترجاعها ومعالجتها.

كما يمكن للإنسان أن يرصد ما يجري على الطرف الآخر من الكرة الأرضية بالصوت والصورة في لحظة قيام الحدث، وأصبحت عملية تبادل المعلومات والمعارف سهلة وميسورة وهو ما أدى إلى الانتشار السريع للمعلومات عبر وسائل الاتصال المختلفة وتدفق هائل في المعلومات والأخبار والمعارف، والأبحاث، والرسائل الثقافية، يعجز الإنسان بقدراته العادية عن متابعتها والإلمام بها في عمره القصير. [4] ص 2

وهكذا يمكن القول أن عصر الجغرافيا بدأ يتضاءل لعصر بلا حدود، تتلاشى فيه سيادات الدول وتسود اختراقات الأقمار الصناعية، والفاكس، وتزايد مستخدمي شبكة الانترنت، وإذا كانت هذه الأخيرة تعتبر خزينة المعرفة وسيل المعلومات المتدفق، فإنها تعد أيضا أداة رفيعة المستوى لإرتكاب الجريمة.

ففي هذه البيئة الضخمة، المزدحمة تضيق قبضة الأمن والمراقبة والتحكم وتزدهر عمليات التجسس على المعلومات المعالجة إلكترونيا وسرقتها حتى أنها تشكل تهديدا بالغا لسائر المنظمات الحكومية والخاصة التي تعتمد أعمالها على الحاسبات والشبكات الاتصالية. [4] ص 3 ، وحتى بالنسبة للأشخاص العاديين.

وبالفعل فلقد أستغلت هذه التكنولوجيا من قبل من لا ضمائر لهم، وحققوا بذلك جرائم هي من أخطر الجرائم على الإطلاق، نتج عنها أنها توسع نطاق دائرة الجريمة والمجرم، بحيث أن مجرم أمس لم يعد هو نفسه مجرم اليوم، فإن كان من يسرق البارحة لأنه لم يجد ما يأكله في منزله فإن المجرم اليوم هو ميسور الحال، ولا يتطلع في سرقة إلى بعض الدينارات ولكن إلى الملايير منها.

لأن هذه التكنولوجيا تحقق له ذلك، وأصبح بإمكان أي شخص يملك جهاز حاسب آلي مربوط بشبكة عالمية أن يقترف جرائمه، والأكثر من هذا أنها جرائم يرتكبها أشخاص ذووا مهارات عالية في فن الحاسبات الآلية، فتوسعت دائرة الجريمة فلم تعد الجريمة هي التي يمكن إرتكابها في الدولة أو محل

الإقامة، ولكن يمكن للجاني أن يقترب جريمته في أي دولة يريد وفي أي وقت يشاء ما دام يملك هذا الجهاز.

وعليه فالخطر الذي يمكن أن تفرزه هذه التكنولوجيا قد يفوق كل تصور، ولعل تعدد مظاهر الإساءة في استعمال هذه التقنية لدليل على إنسيابها وتشعبها بشكل يصعب السيطرة عليه، وهذا يدل على أنه لا توجد أي نقطة تنتهي فيها الجريمة الإلكترونية، ومن ثم فإن المعلومات -كل المعلومات- التي يحتويها الحاسوب لا يمكنها في النهاية أن تقلت من بصمة هذه الجريمة.

فقد يتم من خلال شبكة الانترنت سرقة المستندات، وتزويرها، وتدمير مواقع المعلومات، ونشر الإشاعات، وتشويه سمعة الدول، والأشخاص، والشركات، والمؤسسات، والإستيلاء على الإنتاج الفكري والعلمي للآخرين، بل ونشر الفتن، والفسوق، والفجور وغيرها من الجرائم الدنيئة. [5] ص 239

إن خطر الجرائم المعلوماتية لا يتعلق بالجانب الموضوعي منها فقط، وإنما يتعلق بالجانب الإجرائي أيضاً، حيث أن طبيعة تلك الجرائم تثير العديد من المشكلات الإجرائية، والتي تقف عقبة أمام جهات التحري والتحقيق والتقاضي.

فهذه الجرائم نظراً ولطابعها الخاص لا يمكن التعامل معها بنفس الطريقة التي يتعامل فيها مع الجرائم التقليدية، وخاصة عندما يتعلق الأمر بالتفتيش، والبحث عن الدليل، وضبطه، وكذا حجية الدليل أو الأدلة المتحصل عليها في الإثبات.

وأمام هذا الشكل الجديد لتلك الجرائم والصعوبات التي تواجه متابعتها وضبط مرتكبيها فقد أصبحت نصوص القوانين التقليدية في شقيها الموضوعي والإجرائي لا تفي بمواجهتها، كون أن هذه النصوص التقليدية تتعامل مع أشياء مادية ملموسة مما يتعذر معه تطبيقها لحماية القيم المتولدة عن المعلوماتية.

ولكون نصوص قانون العقوبات والإجراءات موروثه بعضها من القرن (19) التاسع عشر، حيث لم يكن يوجد آنذاك فنيين وإنما حرفيين وأصحاب مهن، وتطبيق تلك القوانين على الأشكال الجديدة للجرائم المعلوماتية، لا يمكن لها أن تحقق شيئاً، وهذا لأنها في النهاية سوف تصطدم بمجموعة من العراقيل ناتجة عن الطبيعة الخاصة والتقنية التي يتميز بها هذا النوع من الإجرام، ومنها سهولة التخلص من الدليل ومحوه والتلاعب به...

مما يستدعي الأمر إعادة النظر بإصدار تشريعات تتناسب مع أركان الجريمة المعلوماتية والطبيعة الخاصة التي تتميز بها وإستحداث نصوص إجرائية لتمكين سلطات التحقيق، والعدالة من التعامل معها، دون أن تغفل مسألة تدريبهم تدريباً عالي المستوى يمكنهم من التعامل مع هذا النوع من الإجرام، وبالتالي القيام بالمهام المخولة لهم على أحسن وجه.

وإزاء ذلك فقد عقدت المؤتمرات الإقليمية والدولية لمناقشة خطورة هذه الجرائم، ووضعت التوصيات التي تعنى بوضع التشريعات التي تتناسب مع حداثة تلك الجرائم، وأهمية التعاون الدولي في مكافحتها. [6] ص 3

وإن كانت مجتمعاتنا العربية لم تتأثر بعد بشكل ملموس بمخاطر هذا النمط المستجد من الإجرام فإن خطر جرائم الكمبيوتر والانترنت المحتمل في البيئة العربية يمكن أن يكون كبيراً، باعتبار أن الجاهزية التقنية، والتشريعية، والأدائية لمواجهة ليست بالمستوى المطلوب، إن لم تكن غائبة تماماً. [7] ص 4

وبالمقابل فقد أمست جرائم الكمبيوتر والانترنت من أخطر الجرائم التي تقترب في الدول المتقدمة تحديداً الأمريكية والأوروبية، ولهذا تزايدت خطط مكافحة هذه الجرائم، وإنصبت الجهود على دراستها المتعمقة، ومن أهم الإنجازات التي حققها المجتمع الدولي هو إنشاء اتفاقية الإجرام المعلوماتي أو ما يطلق عليها باتفاقية بودابست BUDAPEST لمكافحة جرائم المعلوماتية الموقعة بتاريخ 2001/11/23 في عاصمة المجر من قبل 26 دولة من أعضاء الإتحاد الأوروبي إضافة إلى كندا اليابان، جنوب إفريقيا، الولايات المتحدة الأمريكية.

و تعتبر أول إتفاقية دولية بشأن الأفعال الإجرامية التي تتم ضد شبكات الحاسوب أو باستخدامها
Thebudapest convention on cyber [8] ص 103

و تتضمن هذه الاتفاقية بالإضافة إلى قواعد موضوعية لمكافحة الجريمة قواعد إجرائية، وهي معاهدة مفتوحة لكافة الدول.

أمّا على الصعيد الداخلي فنجد أن هناك من الدول من لم تقم إطلاقاً بسن تشريع خاص بمكافحة هذا النوع من الإجرام، أو على الأقل تعديل قانون العقوبات لديها فأغلب الدول العربية تقوم بمكافحة هذا النوع الجديد من الإجرام وفقاً لقوانينها التقليدية، الدول التي عدلت قوانين العقوبات لديها نجد فرنسا حيث تعتبر فرنسا من ضمن الدول التي كانت تكافح الإجرام المعلوماتي وفقاً لقانون خاص ثم بعد ذلك عاقبت على الجريمة المعلوماتية وفقاً لقانون العقوبات، حيث نجد أن القوانين الفرنسية قد تعاقبت منذ علم

1978، بإصدارها القانون المتعلق بالمعلوماتية والحريات، بعد ذلك القانون (19/88) الصادر بتاريخ 05 جانفي 1988 المتعلق بالغش المعلوماتي ثم التعديلات المتعاقبة لقانون العقوبات من قانون 1992 والذي يعتبر أول تعديل لقانون العقوبات ثم التعديل الثاني عام 2004 بالقانون (575 /2004) الصادر بتاريخ 21 جوان 2004 [9] ص79 ، أمّا عن الدول التي إستحدثت نصوص خاصة بهذا النوع من الإجرام فنجد الإمارات العربية المتحدة.[10]

وبالنسبة للجزائر فقد تدارك المشرع الوطني مؤخرا ولونسبيا الفراغ القانوني في مجال الإجرام المعلوماتي، وذلك باستحداث نصوص قانونية لمكافحة الاعتداءات الواردة على المعلوماتية في الفصل الثالث، من الباب الثاني، من الكتاب الثالث، من القانون 15/04 بإضافة قسم سابع مكرر عنوانه المساس بأنظمة المعالجة الآلية للمعطيات من المادة 394 مكرر إلى غاية المادة 394 مكرر7، حيث أرسى هذا القسم وضع حماية لأنظمة المعالجة الآلية للمعطيات وذلك رغبة منه في مواكبة العصرنة، والسير قدما نحو تطوير منظومته التشريعية تأسيا بغيره من التشريعات، فقد نص على مجموعة من الجرائم وأوجب لها عقوبات.

إضافة إلى القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ويتضمن هذا القانون القواعد الإجرائية لمكافحة هذه الجرائم، والتي تدخل من ضمنها الجرائم المنصوص عليها في قانون العقوبات.[11] ص 5

وتبدو أهمية هذا البحث وسبب إختيارنا للموضوع هو التعريف بجرائم جديدة غزت الساحة العالمية، تقدمت بسرعة مذهلة رغم الجهود الكبيرة التي وضعتها الدول المتقدمة، لمكافحة هذا النوع من الإجرام إلا أنه مازال مستمرا لإعتماده على تكنولوجيات الإتصالات والمعلوماتية.

كذلك ما دفعنا لإختيار هذا الموضوع هو أنه موضوع جديد، لم يحظ بدراسة كافية في العالم العربي، وفي الجزائر لم تصادفنا أثناء البحث إلا القليل من البحوث الأكاديمية في هذا المجال.

أمّا عن الصعوبة التي يثيرها موضوع البحث، فتتمثل في صبغته الفنية، فلا يكفي لمعالجة البحث أن يكون الباحث متخصصا في القانون، بل يجب أن يكون ذا دراية بالجوانب الفنية للحسابات الآلية بالإضافة إلى نقص المراجع المتخصصة في هذا الموضوع، وإن توفرت فإنها تركز على الجانب العام فقط.

وإنطلقت دراستنا للموضوع من إشكالية تتمثل في هل ما إستحدثه المشرع من تشريع سواء تعلق الأمر بالقانون 15/04 أو بالقانون 04/09 كاف وفعال لمواجهة هذه الظاهرة المستجدة أم أنه تشريع مازال ينقصه الكثير للوقوف أمام هذا الزحف الإجرامي المدمر؟

وأثناء دراستنا لهذا الموضوع إعتدنا على المنهج التاريخي وإن كان بصورة ضئيلة، كما إعتدنا على المنهج الوصفي إنطلاقا من وصف الظاهرة، وإتبعنا أيضا المنهج التحليلي بتحليل المواد القانونية التي جاء بها المشرع لدراسة محتواها، في سبيل معرفة إن كانت فعالة أم لا، واعتمدنا أيضا على المنهج المقارن وذلك بمقارنة التشريع الجزائري بغيره من التشريعات حتى يتسنى لنا تبين أوجه القصور التي تعترى النصوص التي جاء بها المشرع من أجل إزالتها، وذلك عن طريق إمّا إستحداث نصوص جديدة، أو تعديل النصوص القائمة.

و في سبيل الإحاطة بمجمل عناصر الموضوع تناولنا هذا البحث من خلال فصلين.

تطرقنا في الفصل الأول لـ: ماهية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حيث إنطلقنا من تحديد المقصود بنظام المعالجة الآلية للمعطيات ، ثم تحديد مفهوم المعطيات وتمييزها عما يشابهها حتى لا تتداخل مع مفاهيم أخرى ، ولقد تعرضنا أيضا إلى التعاريف التي جاء بها الفقهاء لتعريف الجريمة المعلوماتية سواء كانت مضيقّة أو موسعة ، وتطرقنا أيضا إلى موضوع الجريمة وكذا تحديد خصائصها بالإضافة إلى إبراز المشكلات العملية بشأن الحماية الإجرائية من الجرائم المعلوماتية .

وفي الفصل الثاني: تعرضنا إلى صور الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي جاء بها التشريع الجزائري ، حيث تناولنا الجرائم الماسة بالنظام ثم الجرائم الماسة بالمعطيات ، ثم تطرقنا إلى الأحكام المشتركة بين جرائم الإعتداء على أنظمة المعالجة الآلية للمعطيات .

و أنهينا البحث بخاتمة حاولنا أن تكون عامة وشاملة، مستنبطة من البحث حول هذه الجرائم المستحدثة وما يشوب نصوصها من نقص وعيوب، وإقترحنا تعديلات كانت نتيجة لمقارنتها بتشريعات أخرى، رأينا أن تداركها من قبل المشرع ضروري لإعادة صياغتها، ولما لا إستحداث نصوص خاصة تتعلق بالجرائم المعلوماتية.

الفصل 1 ماهية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

إنّ ظاهرة جرائم المساس بأنظمة المعالجة الآلية للمعطيات كما يطلق عليها المشرع الجزائري أو جرائم التقنية العالية، أو الجريمة الإلكترونية كما يطلق عليها البعض، أو الجريمة المعلوماتية كما يرى غالبية الفقه تسميتها هي ظاهرة إجرامية مستجدة نسبيا تفرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر، وهول الخسائر الناجمة عنها باعتبارها تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة من بيانات، معلومات، برامج بكافة أنواعها.

فهي جريمة تقنية، تنشأ في الخفاء، يفترفها مجرمون أذكيايمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومة، وتمس الحياة الخاصة للأفراد وتهدد الأمن القومي والسيادة الوطنية وتشيع فقدان الثقة بالتقنية، وتهدد إبداع العقل البشري. [7] ص 03

ولقد أثبت الواقع العملي أن الجرائم المعلوماتية تشكل تحديا خطيرا سواء بالنسبة للمواطن العادي ولرجال الأعمال، أو لرجال الأمن، والبحث الجنائيين ولرجال القضاء، لما لهذه الجرائم من مخاطر تصل أحيانا لحد الكارثة نظرا للخسائر أو الأضرار أو التهديدات التي تترتب عليها سواء على الجانب الاقتصادي أو الجانب الأمني.

ولمّا كانت هذه الجرائم تتميز بكون مرتكبيها على قدر عالي جدا من العلم، والثقافة، والحرفية للدرجة التي لا يمكن معها مواجهتهم، وضبطهم، والتحقيق معهم ثم محاكمتهم وفقا للفكر الأمني والقضائي التقليدي، وقواعد الإثبات الجنائي التقليدية، لذا كان ضروريا بل وحتما إستحداث طرق وأساليب خاصة قوامها العلم والمعرفة والحرفية، وهذا لا يتأتى إلا بالتدريب والتعليم المستمرين لجميع المعنيين بكشف ومحاكمة هذه الجرائم بكافة صورها وأشكالها، وإستخدام أحدث الوسائل العلمية والتكنولوجية، فضلا عن التعاون الفعال بين الجهات المعنية في الداخل والخارج.

لذا فإن إدراك ماهية هذه الجرائم، واستظهار موضوعها وخصائصها وسمات مرتكبيها ودوافعهم بالإضافة إلى إزالة الستار على الصعوبات التي تعترض توقيع الجزاء في مثل هذا النوع من الإجرام

وكذا إبراز المشكلات الإجرائية التي تعترض سبيل التحري والتحقيق لأجل معاينة مرتكبيها تتخذ أهمية بالغة لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية.

1-1 مفهوم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

في مستهل دراسة هذا النوع الجديد من الإجرام، الذي أفرزه التقدم العلمي والتكنولوجي والتقنيات عالية المستوى، والتي كان من المفترض تسخيرها لخدمة المجتمع ولكن تلقته عقول مريضة وأنفس غير سوية خرجت به من الجانب المفيد إلى الجانب المضر. [12] ص 150

فالجريمة المعلوماتية تعتبر من الظواهر الحديثة، وذلك لإرتباطها بتقنية حديثة هي تكنولوجيا المعلومات والاتصالات والكمبيوتر، فتعتبر بذلك صنف جديد من الجرائم.

وقبل الخوض في مسألة تعريف الجريمة المعلوماتية من الضروري أن نبرز المقصود بنظام المعالجة الآلية للمعطيات في المطلب الأول، لأنه مصطلح جديد في فقه القانون الجنائي، وسوف نركز في المطلب الثاني على المعطيات وذلك بتحديد المقصود منها حتى لا تتداخل مع مفاهيم أخرى، وفي المطلب الثالث سوف نحاول إبراز التعريفات التي قيلت بشأن الجريمة المعلوماتية، والتي لم يتفق الفقهاء إلى حد الساعة على تعريف واحد لها كون أنها مرتبطة بالتطور التكنولوجي فاستمدت منه خاصية المرونة والتغير، أما المطلب الرابع فسوف نتناول فيه موضوع الجريمة المعلوماتية.

1-1-1 تعريف نظام المعالجة الآلية للمعطيات:

يمثل نظام المعالجة الآلية للمعطيات الشرط الأولي الذي يلزم تحققه حتى يمكن القول بأن هذه الجريمة جريمة معلوماتية، وبالتالي يعتبر هو الركن المفترض في جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات التي نص عليها المشرع الجزائري في الفصل السابع مكرر منه من المادة "394 مكرر إلى غاية المادة 394 مكرر 7" بعنوان المساس بأنظمة المعالجة الآلية للمعطيات فإذا تخلف هذا الشرط لا يكون هناك مجال للبحث في مدى توافر أركان أي جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات إذ أن هذا الشرط يعتبر عنصرا لازما فيها.

1-1-1-1 المقصود بنظام المعالجة الآلية للمعطيات:

نشير إلى أن المشرع الجزائري قام بتعريف المنظومة المعلوماتية موافقا بذلك للاتفاقية الدولية للإجرام المعلوماتي التي أوردت تعريفا للنظام المعلوماتي في مادتها الأولى. [13]

أما المشرع الفرنسي فلم يتضمن أي تعريف لهذا النظام، وإنما ترك مهمة تعريفه لكل من الفقه والقضاء، ولقد جاء في نص المادة 2/"ب" من القانون المتضمن قواعد الوقاية من الجرائم الإلكترونية أنه يقصد في مفهوم هذا القانون بالمنظومة المعلوماتية: "كل نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين". [11] ص 05

من خلال نص المادة نلاحظ أن المشرع الجزائري لم يقم بتعريف النظام، وإنما أبرز الخاصية الأساسية لهذا النظام، وهي معالجة المعطيات تنفيذا لبرنامج معين، أما عن التعريف الراجح هو ما جاء به الفقه الفرنسي فنجد أن مجلس الشيوخ الفرنسي أدرج ضمن التعديلات التي أوردتها على إقتراح مشروع النائب "GODIFRAIN" المقصود بهذا النظام وقد حدده على الشكل التالي:

«un ensemble composé d'une ou plusieurs unités de traitement ,des mémoires ,des logiciels, des données, d'organes d'entrées –sorties et de liaisons, qui concourent à un résultat déterminé»

وفقا لهذا المفهوم يتضح أن نظام المعالجة الآلية للمعطيات هو مجموعة مركبة من وحدة أو عدة وحدات للمعالجة سواء كانت متمثلة في ذاكرة الحاسب وبرامجه ووحدات الإدخال والإخراج التي تساهم في نتيجة معينة.

إذا نظام المعالجة الآلية للمعطيات مجموعة من الوحدات المترابطة التي تألفت معا لتشكّل كلا لا يتجزأ وليعمل معا كوحدة واحدة. [14] ص 33

كما هو واضح فإن نظام المعالجة الآلية للمعطيات تعبير فني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة ويسر، فضلا على أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية، ولذلك كان المشرع الفرنسي موقفا جدا حين أسقط من نصوص الجرائم تحديد مفهوم هذا التعبير.

بناء على التعريفات السابقة نخلص إلى أن تعريف نظام المعالجة الآلية للمعطيات يعتمد على عنصرين، العنصر الأول عبارة عن: مركب يتكون من عناصر مادية ومعنوية ترتبط بينها نتيجة علاقات توحيدها نحو تحقيق هدف محدد، والعنصر الثاني: هو ضرورة خضوع النظام لحماية فنية وعلى هذا الأساس سوف نتناول كل عنصر على حدة.

2-1-1-1 عناصر النظام المعلوماتي:

يتمثل أساسا في جهاز الحاسب الآلي، بالإضافة إلى مجموعة من ملحقاته والوسائط التي توصل به، لكي يتلقى من خلالها المعطيات. ونشير إلى أنه لم يتفق الباحثون في مجال الحاسب الآلي على وضع تعريف موحد لهذا المصطلح (الحاسب الآلي) ولعل أنسب التعريفات ما جاءت به الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني حيث جاء فيها "الحاسب الآلي هو جهاز إلكتروني، يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال البيانات Data input أو إخراج المعلومات "Information Out"، وإجراء عمليات حسابية ومنطقية وهو يقوم بالكتابة على أجهزة الإخراج أو التخزين، فالبيانات يتم إدخالها بواسطة مشغل الحاسب عن طريق وحدات الإدخال، مثل لوحة المفاتيح أو إسترجاعها من خلال وحدة المعالجة المركزية التي تقوم بإجراء العمليات الحسابية، وكذلك العمليات المنطقية، وبعد معالجة البيانات تتم كتابتها على أجهزة الإخراج مثل الطابعات أو وسائل التخزين المختلفة". [3] ص 25

1-2-1-1-1 المكونات المادية

تتألف المكونات المادية للحاسب الآلي من ثلاثة عناصر رئيسية هي وحدة التشغيل، وحدات الإدخال والإخراج، ووحدات التخزين.

- وحدة التشغيل "centra processing unit"

تمثل الجزء الرئيسي في الحاسب الآلي، وهناك من الباحثين من يطلق عليها وصف "عقل الحاسب الآلي" وتتكون من الذاكرة الرئيسية للجهاز "MAIN MEMORY"، ووحدة الحساب والمنطق "ARTHMETIC AND LOGIC UNIT"، ووحدة التحكم "CONTROL UNIT"، ويطلق على وحدة الحساب والمنطق ووحدة التحكم معاسم وحدة التشغيل المركزية، كما يطلق عليها البعض إصطلاح وحدة المعالجة العشوائية. [15] ص 18

• الذاكرة الرئيسية للحاسب الآلي "main Memory"

تستخدم هذه الذاكرة لحفظ البيانات والمعلومات والبرامج المدخلة في الحاسب الآلي حفظا دائما أو مؤقتا، وهي تتكون من ذاكرة القراءة فقط، ومن ذاكرة القراءة والكتابة.

* ذاكرة القراءة فقط "Rom":

يمكن القراءة منها فقط دون أي استخدام آخر، وتسمى أيضا بالذاكرة الدائمة، ومن خصائصها أنها لا تكتب برامجها إلا بمعرفة الشركة المنتجة لها، ومن أمثلة البرامج (لغة المترجم، وبرامج بداية التشغيل)، كما أنها تقوم بالاحتفاظ بالبيانات حتى بعد انقطاع التيار الكهربائي لذلك تخزن فيها بعض البيانات اللازمة لبدئ تشغيل الجهاز فيها، ولا يمكن تخزين أي بيانات بعد تصنيعها إلا بمعرفة الجهة الصانعة.

* ذاكرة القراءة والكتابة: RAM

تسمى بالذاكرة المؤقتة أو ذاكرة العمل، وهي التي يستخدمها المستخدم بالفعل على جهاز الحاسب الآلي، ومن خصائصها أنها تستخدم في جميع أغراض تخزين البيانات والمعلومات أثناء تشغيل الجهاز. وهي ذاكرة تتغير حسب البرامج التي يتم تحميلها بالحاسب الآلي، كما أنها تفقد المعلومات والبيانات أثناء انقطاع التيار الكهربائي. [3] ص 36

• وحدة الحساب والمنطق:

هي وحدة تقوم بجميع العمليات الحسابية كالجمع والطرح والقسمة، وتقوم بالمقارنات المنطقية مثل (أكبر من وأصغر من، أو تساوي)... [16] ص 51

تحتوي هذه الوحدة على سجل خاص "REGISTRE" يطلق عليه إسم "مسجلات المرمك" حيث تتراكم وتتجمع بيانات العمليات الوسيطة، وهذا السجل يقوم بتخزين نتائج هذه العمليات أثناء معالجة البيانات، وهذه الوحدة تمثل الجزء الرئيسي في عملية معالجة البيانات. [15] ص 20

• وحدة التحكم:

تقوم هذه الوحدة بالتنسيق بين وحدة التشغيل ووحدات الحاسب الآلي الأخرى، بحيث أنه من خصائصها التحكم في البيانات الداخلة والخارجة من وإلى الذاكرة الرئيسية للحاسب، بتوجيهها إلى القنوات المختلفة، كما أنها تحوي ساعة منطقية تقوم بالتحكم في توقيتات العمليات المختلفة، وتحتوي على مجموعة من وحدات التخزين وتقوم هذه المسجلات بتخزين عنوان الأمر المطلوب مثلاً. [3] ص 37

* وحدات الإدخال:

تقبل بيانات وأوامر في صورة يستطيع الحاسب أن يستخدمها بها، وذلك بإدخالها إلى وحدة التشغيل المركزية وبتوجيه من وحدة التحكم والمراقبة، وتشمل لوحة المفاتيح، والفأرة، والقلم الضوئي والماسح الضوئي .

* وحدات الإخراج:

تظهر البيانات التي أجري عليها التشغيل في صورة مفهومة للمتلقي سواء كان إنسانا أو وسيطا متصلا بالحاسب، وتشمل الشاشة والطابعة والراسم وسماعات الإخراج الصوتي... [17] ص 06

* وحدات التخزين:

إمّا أن تكون داخل الحاسب الآلي، وإمّا أن تكون خارجه، فالوحدات الموجودة داخل الجهاز مثل القرص المرن، القرص الصلب، الأشرطة المغناطيسية. [3] ص 45

2-2-1-1-1 المكونات المنطقية للحاسب الآلي :

بالإضافة إلى أن الحاسب الآلي يتكون من مكونات مادية فهو يتكون أيضا من مكونات منطقية يمكن من خلالها القيام بجميع العمليات المخول له القيام بها، بحيث أن الحاسب الآلي أو أي جهاز يحتوي على نظام للمعالجة الآلية للمعطيات لا يمكن له أن يشتغل إلا بوجود مكونات منطقية، والذي يشمل جميع العناصر غير المادية .

لقد عرفه المنشور الفرنسي الصادر في 22/نوفمبر/1981 بأنه " مجموع البرامج والأساليب والقواعد، وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات"، إذا اختلف الكيان المنطقي عن البرامج فالكيان المنطقي مصطلح أعم وأشمل من البرامج، حيث يضم بالإضافة إلى البرنامج المستندات الملحقة به [17] ص 08 ، وهذه البرامج تشبه إلى حد كبير " العقل من جسم الإنسان" بحيث بدونها لا يعدوا إلا أن يكون مادة صلبة لا منفعة منها، نشير إلى أننا سوف نتناول مفهوم البرامج والمعطيات في مطلب الموالي عند الحديث عن المعطيات ولهذا لا داعي للتكرار.

هذا مع ملاحظة أن هذه الوحدات التي وردت في التعريف إنما وردت على سبيل المثال لا الحصر وهذا يفتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التقدم التقني. [18] ص 121

لذلك لا تقع أي جريمة من جرائم الاعتداء المنصوص عليها إذا وقع الاعتداء على عنصر بمفرده لا يشكل جزء من هذا النظام، كما لو وقع الاعتداء على عناصر معروضة للبيع، أو على جهاز حاسب آلي لم يدخل الخدمة بعد، أو على عنصر مودع بالمخازن، أو على قطع الغيار، أو على الأجهزة التي مازالت في مرحلة التجربة، أو حتى الأنظمة التي خرجت من الخدمة تماما. [19] ص 23

تقع الجريمة إذا وقع الاعتداء على النظام خارج ساعات تشغيله العادية، أو إذا كانت أحد عناصره في حالة عطل، كما تقع الجريمة أيضا إذا وقع الاعتداء على عنصر يشكل جزء من أنظمة متعددة، فإذا تصورنا عدة أنظمة ترتبط فيما بينها بأجهزة اتصال، ووقع الاعتداء على جهاز حاسب آلي في نظام من تلك الأنظمة فإن الجريمة تقع في هذه الحالة، فإذا كان الدخول إلى هذا الجهاز مشروع فإن البحث في توافر الجريمة يتوقف على ما إذا كانت توجد علاقة سببية بين هذا الدخول المشروع والاعتداء المفروض على الأنظمة ككل ومدى حسن نية المتدخل. [20] ص 110

كما تقع الجريمة إذا وقع الاعتداء على شبكة الاتصال التي تربط بين أكثر من نظام، لأن تلك الشبكة تعتبر عنصرا في كل نظام من الأنظمة التي تربط بينها. [21] ص 103

تذهب بعض التشريعات إلى الإشارة أن شبكة المعلومات كمحل ينصب عليه هذا النشاط الإجرامي كقانون العقوبات اليوناني، الذي يشير صراحة إلى شبكات المعلومات كمحل ينصب عليه النشاط الإجرامي في جريمة الاعتداء على نظام المعالجة الآلية للمعطيات. [22] ص 324

وفيما يلي سأعرض في الفرع الموالي إلى مدى ضرورة خضوع النظام لحماية فنية، وهل هي شرط لإسباغ الحماية الجنائية عليه أم لا.

3-1-1-1 ضرورة خضوع النظام المعلوماتي لحماية فنية

يقصد بمصطلح الحماية الفنية ذلك الإجراء الوقائي الذي يتخذه صاحب النظام، أو صانع البرنامج أثناء وضعه له، للحد من الإعتداءات الخارجية التي قد تقع عليه، وفي هذا الصدد هناك طريقتان من الحماية هما أسلوب التشفير والتحقق من شخصية المتعاقدان. [20] ص 111

كما هو معلوم فإن المتخصصين بأمن المعلومات يسعون للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات، وبالأخص حاليا شبكة الانترنت، فهم يسعون لتأمين سرية الرسائل الإلكترونية وسرية البيانات المتناقلة، وخاصة الأعمال التجارية الرقمية، ويمثل أسلوب التشفير حسب الخبراء أفضل وسيلة للحفاظ على سرية البيانات المتناقلة، ولمنع الآخرين من الإطلاع على الرسائل الإلكترونية وهناك شكلين أساسيين للتشفير:

الشكل الأول: " la cryptologie symétrique "

أساسه أن نفس المفتاح ألتشفيري يستعمل للتشفير وفك الشفرة في آن واحد، المشكل الذي تطرحه هذه الطريقة أنه يجب إيجاد وسيلة لإرسال المفتاح بطريقة آمنة للمرسل إليه.

الشكل الثاني: " la cryptologie asymétrique "

هنا ليس نفس المفتاح هو الذي يشفر ويفك الشفرة، فالمستعمل يملك مفتاح خاص ومفتاح عام يوزع المفتاح العام ويحتفظ بسرية المفتاح الخاص، لكل من يريد مراسلته أن يستعمل المفتاح العام لكن المرسل إليه وحده بإمكانه الإطلاع على مضمون الرسالة المشفرة باستعمال المفتاح الخاص. [21]ص104

أما التحقق من شخصية المتعاقدين فيتم عن طريق استخدام " شفرة المفتاح العام " حيث يمكن للطرفين المتعاقدين أن يوقعا على المستندات بطريقة رقمية، ويتأكد كل طرف من توقيع الطرف الآخر بإستخدام المفتاح العام للشفرة. [23] ص ص 89،90

مما سبق نجد أنه بالرغم من تحديد مجلس الشيوخ الفرنسي في تعريفه السابق لمفهوم النظام وذكر عنصر الحماية الفنية ضمن الأعمال التحضيرية للقانون 88/19 إلا أن النص الفرنسي جاء خاليا من أي إشارة إلى هذا الشرط .

لذلك ثار التساؤل حول ضرورة وجود، أو عدم وجود الحماية الفنية كشرط للتمتع بالحماية الجنائية، وللإجابة على هذا التساؤل فقد قسمت أنظمة المعالجة الآلية للمعطيات إلى ثلاثة أنواع: أنظمة مفتوحة للجمهور، أنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية وكذلك أنظمة قاصرة على أصحاب الحق فيها وتتمتع بحماية فنية.

ومقتضى تطبيق هذا العنصر أن النوع الثالث فقط من تلك الأنظمة يتمتع بحماية جنائية أما النوع الأول والثاني فلا يتمتعان بتلك الحماية، وهناك من يصرون عليه لأن الحماية الجزائية في نظرهم يجب أن تقتصر على الأنظمة المحمية فنيا، لأنه من الطبيعي في نظرهم أن من يقوم بالاستغلال يضع الوسائل اللازمة لمنع الغش، وأن القانون لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم، وليس من يهمل منهم في توفير الحد الأدنى لحماية أمواله، ويكون بذلك دور القانون الجنائي في هذه الحالة دور

وقائي. [19] ص 22

يذهب الرأي الغالب في فرنسا إلى عدم ضرورة وجود الحماية الفنية، وذلك لأن نص القانون والأعمال التحضيرية يستفاد منها عكس ذلك، فقد إعتبروا بأن نظام الأمن لا يكون له سوى دور واحد وهو إثبات سوء نية من قام بانتهاك النظام أو الدخول إليه بطريقة غير مشروعة ويدخل ذلك في عداد إثبات القصد الجنائي. [20] ص 112

بينما يذهب رأي آخر إلى ضرورة وجود نظام أمني، ذلك أن القانون يجرم الاعتداء على نظم الأمن المتضمنة في النظام المعلوماتي، ومن أنصار هذا الرأي " M'ALTERNEN ET " BLACHE" ويستند أنصار هذا الرأي لعدة حجج منها أن الاعتداء على النظام الأمني - شرط مفترض- لقيام الجرائم التي تتعلق بالمعلوماتية، والعدالة الجنائية تقتضي عدم العقاب على فعل يعد إعتداء على حق لم يتحوط له صاحبه فضلا على أن التسليم برأي غالبية الفقه يعني توسعا في مجال التجريم، فكل دخول غير مشروع جريمة وذلك أمر غير منطقي. [24] ص 24

كما يذهب أنصار الرأي الأول أن المسألة واضحة ولا تحتاج إلى تفسير ذلك أن النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات صدرت دون أن تتضمن شرط الحماية الفنية، والمبادئ المستقرة في القانون الجنائي أنه لا يجوز تقييد النص المطلق، أو تخصيص النص العام طالما لم ينص المشرع على ذلك، سيما أن عدم ذكر شرط الحماية الفنية يعني أن المشرع قد أراد إستبعاد هذا الشرط صراحة. [20] ص 113

كذلك مجرد توافر فعل الاعتداء على الحق الذي قررت له الحماية كفيل بقيام الجريمة لمجرد توافر فعل الاعتداء. وليس لنا أن نبحت في تحوط صاحبه، فالذي يسير في جانب الطريق ثم تصدمه سيارة لا يطلب منه الامتناع عن السير بحجة وجود سائقين متهورين، كذلك المريض الذي على إثر خطأ طبي لا يطالب بالتحوط بعدم دخول المستشفى بدعوى وجود إهمال من الأطباء في المستشفى. [25] ص 79

بالرجوع إلى المناقشات البرلمانية نجد أنها كانت ضد إشتراط هذه الحماية حتى ولو ورد ذكر النص على هذه الحماية، كشرط ضمن الأعمال التحضيرية للقانون رقم 88/19 حول غش المعلوماتية فإنه لا يكتسب أهمية لعدم إلزامية هذه الأعمال التحضيرية، وإنما يستعان بها في تفسير ما غمض من النصوص أو تعارض مع بعضه البعض. [18] ص 124

وتطبيقا لذلك يمكن القول أنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيد بوجود الحماية الفنية، ولقد وفق المشرع الجزائري عندما استبعد هذا الشرط من النصوص القانونية المتعلقة بهذا النوع من الإجرام.

2-1-1 مفهوم المعطيات:

بعد أن تعرضنا إلى تحديد المقصود بنظام المعالجة الآلية للمعطيات، كان لابد من التعرّيج إلى مسألة في غاية الأهمية وهي مفهوم المعطيات، باعتبار أن هذا المصطلح جاء نتيجة لإستعمال هذه التقنية الجديدة، التي ما فتئت أن جاءت بمصطلحات جديدة لم نعهدها في القواعد العامة للقانون الجنائي، ولذلك لا بد من إيجاد تعريف واحد لها وتمييزها عما يشابهها من معلومات وبرامج.

1-2-1-1 تعريف المعطيات:

المعطيات في اللغة تقابل البيانات [26] ص 92، والبيانات في اللغة مصدرها الفعل بين، والبيان: ما يبين به الشيء من الدلالة، وغيرها، وبان الشيء بيانا: إتضح فهو بين والجمع أبنياء وكذلك أبان الشيء فهو مبين، وإستبان الشيء ظهر. [27] ص 67

ويقابل هذا في اللغة اللاتينية كلمة "DATUM" وتعني شيء معطى أو مسلم به، أو شيء ما معروف أو مسلم به كحقيقة، أو واقعة وجمعها "DATA" وهي التي تستخدم كلاسيكيا في اللغة الإنجليزية، بينما تستخدم اللغة الفرنسية مقابلا لها كلمة معطيات "DONNEES". [28] ص 25 وهو نفس المصطلح الذي استعمله المشرع الجزائري.

أمّا إصطلاحا: فالبيانات تعبر عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام، التي لا علاقة بين بعضها البعض، والتي لم تخضع بعد لعملية تفسير أو تجهيز للإستخدام والخالية – تبعا لذلك - من المعنى الظاهر في أغلب الأحيان. أي أنها بإيجاز "الحقائق أو الرسائل أو الإشارات أو المفاهيم التي تعرض بطريقة صالحة للإبلاغ، أو التوصيل أو التفسير، أو المعالجة بواسطة إنسان أو أدوات ومعدات آلية". [3] ص 72

تجدر الإشارة إلى أنه وبالرجوع إلى قانون العقوبات لكل من الدولتين (الجزائر وفرنسا) نجد أنه لم يورد أي تعريف لمصطلح «معطيات» "DONNEES" كما نجد أنه يخلو من إستعمال مصطلح "INFORMATIONSLES" كون أن هذا المصطلح يتداخل كثيرا مع مصطلح معطيات.

لذلك سوف نتناول في الفرع الثاني تمييز المعطيات عما يشابهها من مصطلحات، والتي يمكن أن تتداخل معها في بعض الأحيان.

2-2-1-1 تمييز المعطيات عما يشابهها

بعد أن حاولنا تعريف المعطيات لا بد لنا في هذا الفرع من تمييزها عما يشابهها من مصطلحات لما لها من ارتباط وثيق يصعب في غالب الأحيان التمييز بينهم.

1-2-2-1-1 تمييز المعطيات عن المعلومات

إن المعلومات على الرغم مما يبدو أن تعريفها لا يثير أي صعوبة، حيث أنها تحيط بنا من كل جانب، إلا أنها وبظهور تكنولوجيات وتقنيات الحاسبات الآلية اكتسبت بعدا جديدا، أضفى عليها أهمية تفوق ما كانت عليه قبل ذلك. فاكتمت بذلك تسمية جديدة .

- تعريف المعلومات

المعلومات في اللغة مشتقة من فعل علم، ودلالاتها فيها تدور حول المعرفة، و المعرفة «knowledge»: تمثل حصيلة أو خبرة إلى جانب معلومات ودراسة طويلة، تتحقق لشخص ما في وقت معين في حين تعمل المعلومات على تزويد الشخص بعناصر هذه المعرفة أو رفع مستواها ، [29] ص 92 والتي يمكن نقلها وإكتسابها، وأعلم فلانا الخبر وبه، أي أخبره به، وأعلم فلانا الأمر حاصلًا جعله يعلمه، [28] ص 23، ويقابل المعلومات في اللغة الفرنسية مصطلح "INFORMATION" وأصلها الكلمة اللاتينية INFORMATIO الدالة بحسب الأصل على شئ قابل للإبلاغ أو التوضيح أو على عملية النقل أو الإبلاغ، أو التوصيل.

أما المعنى الاصطلاحي: للمعلومات فيختلف من إختصاص لآخر ومن ثقافة لأخرى، حتى ليكاد يكون من المستحيل فهم وإدراك معنى المعلومات ومن هذه التعريفات.

مصطلح المعلومات كثيرا ما يترادف مع مصطلح تكنولوجيا المعلومات أو تقنية المعلومات على الرغم من الإختلاف الموجود بينهما، فالمعلومات هي المضمون أو الرسالة الناتجة عن معالجة البيانات التي تم إدخالها، بينما تكنولوجيا المعلومات هي الوسط المستخدم لإقتناء أو حفظ أو نقل المعلومات. [30] ص 227

المعلومات هي " كل نتيجة مبدئية أو نهائية مترتبة على تشغيل البيانات أو تحليلها أو استقراء دلالاتها أو استنتاج ما يمكن استنتاجه منها وحدها أو متداخلة مع غيرها، أو تفسيرها على نحو يثري معرفة متخذي القرار ومساعدتهم على الحكم السديد على الظواهر والمشاهدات أو يسهم في تطوير المعارف النظرية أو التطبيقية ". [16] ص 62

ومن التعاريف الأخرى تقرير الأستاذ "باركر" بأنها " مجموعة من الرموز والحقائق والمفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال والتفسير والتأويل أو للمعالجة بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة، بحيث يمكن تغييرها وتخزينها وجمعها أو نقلها بوسائل وأشكال مختلفة". [31] ص 101

وهناك من يعرف المعلومة أنها "رسالة معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير". [31] ص 102

- تمييز المعطيات عن المعلومات:

هناك من ينطلق في تعريفه للمعلومات من إختلافها عن المعطيات، فيعتبر المعلومات نتاجا لمعالجة البيانات، حيث أن البيانات أي المعطيات هي "مجموعة من الحقائق أو القياسات أو المعطيات التي تتمثل في شكل أرقام، حروف، رموز، تتعلق بفكرة أو موضوع معين، أما المعلومات فهي نتاج معالجة البيانات داخل الحاسب الآلي. [29] ص 92

وقد أخذت التوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية عام 1992 الخاصة بحماية أنظمة الحاسبات الآلية وشبكات المعلومات بالترفة التي سردها هذا الرأي، حيث عرفت البيانات بأنها "مجموعة من الحقائق أو المفاهيم أو المعلومات تتخذ شكلا محددًا يجعلها قابلة للتبادل أو التفسير أو المعالجة بواسطة الأفراد أو بوسائل إلكترونية"، أما المعلومات فهي "المعنى المستقى أو المستخلص من هذه البيانات".

وهناك من يرى أن المعطيات تتداخل مع المعلومات تداخلا كبيرا فقد عرف الباحثين المعطيات بأنها المعطيات الخام والأولية التي تتعلق بقطاع أو نشاط ما وعرف المعلومات بأنها الصورة المحولة للمعطيات وقد تم تنظيمها ومعالجتها بطريقة تسمح باستخلاص النتائج. [16] ص 61، وهناك من يرى أن البيانات (المعطيات) هي مجموعة من الحقائق أو المشاهدات أو القياسات التي تكون عادة في شكل حروف أو أرقام أو أشكال خاصة توصف أو تمثل فكرة أو موضوعا أو هدفا أو شرطا، أو أية عوامل أخرى، وتمثل البيانات المادة الخام التي يتم تجهيزها للحصول على المعلومات فالبيانات تعد مصطلحا عاما لكل الحقائق والأرقام والرموز والحروف، فهي معطيات أولية يمكن معالجتها وإنتاجها عن طريق نظم المعلومات. [32] ص 05

يتضح بذلك أن المعطيات(البيانات) هي المادة الخام للمعلومات، والتي لم يتم معالجتها بعد، أما بعد معالجتها فإنها تحول من بيانات إلى معلومات ، فمثلا إذا قلنا أن عدد الطلبة الحاضرين هو 22 طالب

يعد بيان ، إذا علمنا أن العدد الإجمالي للطلبة هو 25 طالب ، فإن هذا أيضا بيان ، ولكن عند إجراء عمليات رياضية أو منطقية على هذين البيانيين كطرح عدد الحاضرين من العدد الإجمالي يكون الناتج هو 03 يمثل عدد الطلبة الغائبين وهو يشكل معلومة ، ونظرا للتداخل الكبير للمعلومات مع المعطيات فقد عرف بعض الباحثين المعطيات بأنها "المعطيات الخام أو الأولية التي تتعلق بقطاع أو نشاط ما وعرفت المعلومات بأنها الصورة المحولة للمعطيات وقد تم تنظيمها ومعالجتها بطريقة تسمح باستخلاص النتائج.[16] ص 61

وهناك من يرى أن المعطيات هي معلومات في حالة كمون، والمعلومات هي معطيات في حالة حركة وتبلور، وإذا صح هذا التصور فإن المعطيات تعتبر بمثابة " حقائق رقمية أو غير رقمية، أو مشاهدات واقعية لا تصورية، أو قياسات تتم بطريقة منهجية يمكن لأحد الناس قراءتها وفهم دلالتها البسيطة دون دخول في عمليات إستنتاجية، أو إستقرائية لدلالاتها المعقدة سواء من حيث الربط بين أكثر من بيان منها، أو إستخلاص أية نتيجة مترتبة عليها، فإن تم ذلك بدأ دخول منطقة أخرى هي منطقة المعلومات".

فالمعلومات وفقا لذلك هي: " كل نتيجة مبدئية أو نهائية مترتبة على تشغيل المعطيات أو تحليلها أو استقراء دلالتها، أو استنتاج ما يمكن استنتاجه منها وحدها، أو متداخلة مع غيرها أو تفسيرها على نحو يثري معرفة متخذي القرار ومساعدتهم على الحكم السديد على الظواهر والمشاهدات أو يسهم في تطوير المعارف النظرية أو التطبيقية".[16] ص 62

ولا شك أن المعطيات والمعلومات يتفقان في أن كل واحدة تحوي مضمونا معيناً، أي تتضمن فكرة معينة أو معروفة، لكن ما يميز الواحدة عن الأخرى هو الصورة التي توجد عليها في الواقع فالمعطيات المقصودة هنا لا بد أن تأخذ شكلا معيناً، ومكانها هو نظام المعالجة الآلية للمعطيات بينما المعلومات قد تبقى مجرد أفكار ومعرفة داخل ذهن أو فكر الإنسان ولا تأخذ شكلا معيناً[26] ص 95

2-2-2-1-1 تمييز المعطيات عن البرامج:

تعتبر المعطيات من المكونات غير المادية للحاسب الآلي، وهو الأمر نفسه بالنسبة للبرامج وهذه المكونات غير المادية تعتبر بمثابة العقل من جسم الإنسان، فبدونها لا يعدوا إلا أن يكون مجرد آلة، وقيمتها لا تتعدى قيمة المكونات المادية التي صنع منها، فهي التي تمكن الحاسب الآلي من القيام بوظائفه.

- تعريف البرامج:

لقد تعددت التعاريف الخاصة ببرامج الحاسب الآلي سواء من جانب الفقه، أو من جهات أخرى كالجمعية الدولية لحقوق المؤلف والمنظمة العالمية للملكية الفكرية، فقد عرفها جانب من الفقه "تعليمات مكتوبة بلغة ما موجهة إلى جهاز تقني معقد يسمى الحاسب الإلكتروني، بغرض الوصول إلى نتيجة أو مهمة معينة"

أما عن تعريف الجمعية الدولية لحقوق المؤلف فجاء فيه أن برنامج الإعلام الآلي "يشمل كل البرامج والطرق والقواعد، وممكن حتى الوثائق المتعلقة بسير أو تسيير مجموع المعطيات، وبرنامج الإعلام الآلي يمكن أن يعتبر كمجموع غير قابل للتجزئة كما هو،" [33] ص 105

فالبرنامج المعلوماتي: سلسلة من التعليمات (INSTRUCTIONS) المحررة بلغة خاصة والمستعملة من طرف الحاسوب من أجل تنفيذ عملية محددة. [34] ص 12

أما الرأي الراجح فهو الذي يرى أن للبرامج مفهومان أحدهما ضيق والآخر واسع. فالمفهوم الضيق يقتصر على مجموع التعليمات والأوامر الصادرة من الإنسان إلى الآلة أي إلى الكيان المادي للحاسب [35] ص 23، أما المفهوم الواسع فهو يضم إلى جانب تلك التعليمات والأوامر (المفهوم الضيق) التعليمات والأوامر الموجهة إلى العميل مثل بيانات استعمال البرنامج. [35] ص 23

- أنواع البرامج: إن البرامج تنقسم إلى قسمين :

• برامج التشغيل:

ونقصد بها مجموع البرامج التي تعد خصيصا لتنظيم عمل أجهزة الحاسب منذ بدئ تشغيلها وحتى إغلاقها، تخزن هذه البرامج في الذاكرة الداخلية للحاسب باعتبارها تؤدي وظائف أساسية للمتعاملين فهي تشكل القاعدة العامة وجزء لا يتجزأ من أجهزة الحاسب، وتدخل في مكوناتها، ومن أمثلة برامج التشغيل، البرامج الخاصة بحفظ الملفات وإسترجاعها، ومسحها ومن أهم البرامج المعروفة على المستوى العالمي برنامج ماكينتوش الصادر عن شركة آبل كمبيوتر، برنامج windows الصادر عن شركة Microsoft.

• برامج التطبيق:

هي البرامج التي يكون الغرض منها تنفيذ مهام إدارية ووظيفية معينة، غالباً ما تكون محفوظة على دعامة مادية يتم إدخالها في الحاسب، ويتم ابتكار هذا النوع من البرامج لتلبية إحتياجات خاصة للعملاء.

ومن أمثلة برامج التطبيق برامج حسابات العملاء في البنوك، برامج منظمة لحرية الطيران المدني فيما بين الدول ومواعيد الرحلات، برامج خاصة بالأجور الخاصة بالعمال في المؤسسات العمومية. [33]ص 108

- تميز المعطيات عن البرامج:

يكن الفرق بين المعطيات والبرامج في الوظيفة التي يؤديها كل واحد منهما، فالهدف من وجود البرامج ليس في حد ذاتها، وإنما لأن الحاسب الآلي لا يمكنه أن يؤدي الوظيفة المخولة له إلا بوجود هذا البرنامج كما سبق الإشارة له في ذكر أنواع البرامج، فبعدم وجود برامج التشغيل لا يمكن أن يشتغل الحاسب الآلي على الإطلاق، وبعدم وجود برامج التطبيق لا يمكن للعميل أن يقوم بمختلف العمليات التي يريدها ومثال ذلك الكتابة، الرسم، الحساب... وحتى فيما يتعلق الأمر بمعالجة المعطيات سواء بإدخالها أو تخزينها أو استرجاعها عند الطلب، تتطلب برنامج خاص يمكن الحاسب الآلي من القيام بهذه المهام.

أما الغاية من وجود المعطيات فتكمن في حد ذاتها، إذ أن هذه المعطيات ليس لها دور في تشغيل جهاز الحاسب الآلي، وإنما يعتبر الحاسب الآلي بمثابة المستودع الذي يتم فيه معالجة هذه المعطيات وتخزينها، ثم إتاحتها عند الطلب واسترجاعها وذلك للإطلاع عليها، وتكوين معرفة ودراسة توفرها هذه المعطيات. [26] ص 96

لهذا يمكن أن تتداخل المعطيات مع البرامج في الحالة التي تدخل إلى نظام المعالجة الآلية للمعطيات فإن الحماية المقررة لهذه البرامج هي نفس الحماية المقررة للمعطيات أو المعلومات، أما في الحالة التي لم تدخل بعد فيها هذه المعطيات إلى النظام، أو في حالة خروجها منه بعد معالجتها فهنا لا يمكن تطبيق هذه الحماية عليها لأنها انفصلت عن البرنامج.

وعليه لا يدخل في مفهوم البرنامج حتى الواسع منه المعطيات أو المعلومات سواء قبل أو بعد معالجتها، وإن كانت هذه الأخيرة بعد دخولها ومعالجتها آلياً وتخزينها وإسترجاعها لا تنفصل عن البرامج التي تنظمها في كل مرحلة من المراحل السابقة، ولذلك فإن الحماية المقررة لتلك البرامج هي في نفس

الوقت حماية لهذه المعطيات أو المعلومات والعكس ليس بالضرورة صحيحا أي أن حماية البرامج تشمل البرامج في حالتها المجردة أو تلك المطبقة على المعطيات أو المعلومات. [18] ص 695

ونشير إلى أن المشرع الجزائري أقر حماية للبرامج حتى تلك المنفصلة عن المعطيات، وذلك بنص المادة 4 من الأمر (05-03) المتعلق بحقوق الملكية. [36]

3-2-1-1 عناصر المعطيات محل الحماية:

حتى يمكن القول بأن هذه المعطيات تحظى بالحماية التي يوفرها قانون العقوبات، في الفصل السابع مكرر منه، لا بد أن تتوافر على شرطين وهما أن تكون محددة وسرية، ويظهر عنصر التحديد بالنسبة لجريمة التلاعب بالمعطيات، بحيث أن الجاني في جريمة التلاعب عندما يمحي أو يضيف أو يعدل في المعطيات فهو بذلك مس عنصر التحديد لهذه المعطيات المعتدى عليها.

أما عنصر السرية فيتجلى بوضوح بالنسبة لجريمة الدخول أو البقاء غير المصرح به داخل نظام المعالجة الآلية للمعطيات، ولا يتطلب قانون العقوبات أن تكون المعطيات المعتدى عليها مبتكرة أو مستأثرا عليها، لأن الإبتكار والإستأثار هي عناصر تتطلبها قوانين حماية حق المؤلف.

1-3-2-1-1 عنصر التحديد:

من المنطق أنه عند الحديث عن جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات لا بد أن تكون هذه المعطيات موجودة، وأن تكون محددة، لأن المعلومة التي تفنقر لصفة التحديد لا يمكن أن تكون معلومة حقيقية، فإذا كانت المعلومة هي تعبير وصياغة محددة، تجعل رسالة ما قابلة للتبليغ والتداول عن طريق علامات أو إشارات مختارة فينبغي أن تكون محددة. [22] ص 113

بالإضافة إلى أن المعلومة المحددة هي التي يمكن فقط حصرها في دائرة خاصة بها، بيد أن هذا التحديد يبدوا أمرا ملحا في مجال الاعتداء على القيم، لأن هذا التعدي يفترض دائما شيئا محددًا وينبغي على هذا الشيء بدوره أن يكون محلا لحق محدد. [37] ص 75

فالتحديد خاصية تفرض نفسها قبل كل شيء وبإندامها تزول أي معلومة حقيقية، وهكذا أشار الأستاذ catala وبحق أن المعلومة وقبل كل شيء تعبير، وصياغة مخصصة من أجل ذلك وتبلغ أو يمكن تبليغها عن طريق علامات أو إشارات مختارة لكي تحمل الرسالة إلى الغير. [37] ص 75

ويظهر عنصر التحديد جليا في جريمة التلاعب بالمعطيات، حيث لا يمكن القول بالتلاعب في المعطيات إلا إذا كانت هذه المعطيات محددة فقام الجاني بتغيير حالة المعطيات سواء بفعل المحو الكلي أو الجزئي، أو التعديل، أو الإضافة.

1-1-2-3-2 عنصر السرية:

تعتبر السرية صفة لازمة لأنها تحصر حركة الرسالة أو تحمل المعلومة في دائرة محددة من الأشخاص. [37] ص 75

إذ أن المعلومة التي لا تتسم بذلك هي معلومة مكشوفة ومجال حركتها غير محدد بمجموعة من الأشخاص، وتكون قابلة للتداول فلا يمكن الحديث عندئذ عن إعتداء عليها بسرقتها، أو الإطلاع عليها بدون وجه حق، لأنها بمنأى عن أي حيازة. [22] ص 114

وهذا ما ينطبق على المعلومات التي تتعلق بحقيقة معينة كدرجة الحرارة في وقت معين، أو تلك التي ترد على حوادث معينة كالبراكين والفيضانات فهي تبدوا كأنماط قابلة للنقل بسهولة بين كل الأشخاص والوصول إلى المعلومة بسهولة يتعارض والطابع السري لها. [31] ص 104

وتكتسب المعلومة هذه الصفة الأخيرة، إما بإرادة الشخص باكتشاف مجال حديث، أو بحسب طبيعتها كإكتشاف شيء لم يكن معروف من قبل، أو باجتماع الأمرين معا كالرقم السري للبطاقة الائتمانية. [38] ص 40

فالمعطيات تكتسب سريتها من كونها موجودة داخل نظام المعالجة الآلية للمعطيات، وأن هذا النظام مغلق، أي أنه غير مفتوح للجمهور، ولا يتم الدخول إليه إلا بشروط معينة كدفع إشتراك أو الدخول من أشخاص معينين كإشتراط كون الداخل عضو في هيئة أو جهة ما، فمناط السرية هنا هو وجود المعطيات داخل النظام وعدم إتاحة الإطلاع عليها لأي كان. [26] ص 97

ولا عبرة هنا بنوع المعطيات سواء كانت معطيات شخصية أو غير شخصية، معطيات مشفرة أو غير مشفرة وسواء كانت معطيات متاحة، أو مقيدة، أو معطيات ساكنة، أو متحركة فعنصر السرية هنا لا يصاحب معطيات دون أخرى. [26] ص 98، 99

ويظهر جليا عنصر السرية في جريمة الدخول والبقاء داخل نظام المعالجة الآلية للمعطيات فالجريمة هنا تقع عدوان على سرية المعطيات، فهي تقع بغض النظر عن نوع المعطيات، وتقع هذه الجريمة في حالة التعدي على عنصر التحديد أي تغيير المعطيات الموجودة داخل النظام أو عدم التعدي

عليه، أي أن مجرد إنتهاك السرية أي سرية المعطيات من قبل أشخاص غير مخول لهم الإطلاع على هذه المعطيات تقع الجريمة، والوضع هنا يشبه إنتهاك حرمة عقار فهي تتم بالدخول إلى العقار بصرف النظر عما يحويه هذا العقار.

4-2-1-1 الطبيعة القانونية للمعطيات:

المعلومات هي أعلى ما يمتلكه الإنسان في حياته على مر العصور، لذا سعى إلى جمعها وتسجيلها على وسائل مختلفة، بدءا من جدران المقابر والمعابد وأوراق البردى في عصر الفراعنة إلى أن تم اختراع الورق في الصين. [37] ص 71

ومع الوقت بدأت تزداد هذه الأهمية للمعلومات في المجتمعات، لا سيما في الدول المتقدمة وبدت الحاجة ملحة لوجود وسائل أخرى يتم من خلالها تسجيلها، وتخزينها، واسترجاعها عند الطلب، ولذلك أخترع نظام المعالجة الآلية للمعطيات، ويعتبر جهاز الحاسب الآلي النموذج الحقيقي الذي تمارس فيه كل هذه العمليات، فيمكن لنا كتابة وإدخال أي معلومة داخل الجهاز وبإمكاننا الاحتفاظ بهذه المعلومات كما أنه في استطاعتنا إسترجاع المعلومات في أي وقت نريد.

ولكن جهاز الحاسب الآلي عبارة عن آلة، ولا يمكن له التمييز بين مالكة وبين الشخص الأجنبي عن النظام الذي ليس له حق الدخول إليه، والعبث بالمعطيات الموجودة فيه، لذلك كانت الحاجة ملحة لحماية هذه المعطيات وخاصة أن قوانين الملكية تحمي هذه البرامج ولكن وفق شروط صعبة ولا تحمي المعطيات في حالتها المنفصلة عن البرامج أي ما قبل إدخالها إلى النظام أو بعد معالجتها.

ونظرا لأهميتها الواسعة رأى جانب من الفقه ضرورة حمايتها، لأنها تشكل قيمة إقتصادية عالية مخالفا بذلك الإتجاه التقليدي الذي يرى أنه لا يوجد ما إصطلح بتسميته الحماية القانونية للمعلومات (المعطيات)، لأنها عبارة عن أشياء معنوية، والقانون لا يحمي إلا الأشياء المادية كون أنها ملموسة...

وتجدر الإشارة إلى أنه عند الحديث عن المعلومات ليس بمفهومها العام، وإنما نتحدث عنها في الفرض الذي تتطابق فيه بمصطلح المعطيات، فالحديث عن الطبيعة القانونية للمعلومات هو بالضرورة حديث عن الطبيعة القانونية للمعطيات.

لأجل ذلك إنقسم الفقه إلى إتجاهين الأول: يرى أن المعلومة لها طبيعة من نوع خاص، والثاني يرى أن المعلومة ما هي إلا مجموعة من القيم، ولذلك سوف نتعرض لكلا الإتجاهين.

1-1-2-1-4 الاتجاه التقليدي :

يأخذ هذا الاتجاه بمعيار طبيعة الشيء، ويرى أنصار هذا الاتجاه أن المعلومة لها طبيعة من نوع خاص، وذلك انطلاقاً من حقيقة مسلم بها، هي أن وصف القيمة يضاف على الأشياء المادية وحدها. [38] ص 49

يرتكز هذا المبدأ على بديهية مسلمة مؤداها أن الأشياء التي توصف بالقيم هي تلك الأشياء القابلة للإستحواذ المادي، ومؤدى ذلك أن الأشياء التي يمكن الاستئثار المادي بها فقط هي التي تعد وحدها من قبيل القيم التي تكون محلاً للعديد من الإعتداءات القانونية، وبالنظر إلى أن للمعلومات طبيعة معنوية فإنه يكون من غير المقبول أن تكون قابلة للاستئثار والاستحواذ، إلا عن طريق حق الملكية الأدبية أو الذهنية أو الصناعية. [3] ص 75

لذلك فالمعلومات المخترنة التي لا تنتمي إلى المواد الأدبية أو الذهنية أو الصناعية لا تندرج حتماً في مجموعة القيم المحمية، ولا يعني إستبعاد المعلومات من مجموعة القيم رفض كل حماية قانونية لها لأن الفقه والقضاء يعترفان بوجود إعتداء يجب العقاب عليه عند الإستيلاء غير المشروع على معلومات الغير. [37] ص 104

وأياً ما كان الأمر فإنه مستقر بصدد وجود خطأ عند الإستيلاء على معلومات الغير، ولذلك فقد حاول هذا الإتجاه أن يحمي هذه المعلومات بدعوى المنافسة غير المشروعة، وذلك إستناداً إلى حكم محكمة النقض الفرنسية، وأن الغاية من دعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق إستثنائي، لذلك يذهب الأستاذ DEBOIS في وقت مبكر بأن الملكية العلمية ربما ستأتي يوماً ويعترف بها لصاحب فكرة لم تحصل بعد على حق براءة إختراع بإعتبار أن الفكرة السابقة مستبعدة من مجال الملكية الذهنية. [38] ص 49

1-1-2-1-4 الاتجاه الحديث:

يستند أنصار هذا الاتجاه إلى معيار القيمة الاقتصادية للشيء ويرجع الفضل في إضفاء وصف القيمة على المعلومة إلى كل من الأستاذين "VIVANT et CATALA"، ولذلك سوف نحاول دراسة ما جاء به كل واحد منها.

- منهج الأستاذ CATALA:

تعد المعلومة وفقا لـ CATALA قيمة قابلة للإستحواذ حتى في حالة إستقلالها عن المعلومات على اعتبار أن المعلومة تقوم وفقا لسعر السوق، متى كانت غير محظورة تجاريا، وأنها تنتج بصرف النظر عن دعائها المادية عن عمل من قدمها، وأنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه، وهي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما، وهو رأي جانبا من الفقه الحديث الذي يعتبر الشيء مالا ليس بالنظر إلى كيانه المادي وإنما على أساس قيمته ومنفعته الإقتصادية. [8] ص 19

وهكذا استند الأستاذ CATALA إلى حجتين رئيسيتين لإضفاء وصفة القيمة على المعلومات، الأولى قيمتها الإقتصادية، والثانية علاقة التبني التي تجمع بينها وبين مالكيها.

فالنسبة للحجة الأولى: فإذا كان المنطق التقليدي يستبعد المعلومة من مجموعة القيم، فمرد ذلك عدم وجود حق إقامة لها في نطاق حق الملكية المعنوية، حيث يتعارض الطابع المعنوي لها مع وصف القيمة. وأشار أيضا الأستاذ CARBONNIER أن الجوهر على قدر كبير من الأهمية في مجال المنفعة الإقتصادية بالمقارنة بنظيره في مجال البيانات المادية، وأنه من الواضح أن أي قانون يرفض أن يرى قيمة في شيء له أهمية إقتصادية سيبقى حتما بمعزل عن الحقيقة وعليه من المقبول أن ينطبق وصف المال عليها. [3] ص 78

أما بالنسبة للحجة الثانية: فإن رابطة التبني التي تجمع المعلومة بمؤلفها من شأنها أن تشيد الحيادة الأولى لوصف القيمة، وهكذا فإنه إذا وضع في الاعتبار الرابطة التي تجمع المعلومة ومؤلفها فيجوز إذا الإقرار بمكنة حيادة المعلومة، بوصفها قيمة وفقا لهذا التصور. [3] ص 79

- منهج الأستاذ vivant:

إن الأستاذ "VIVANT" أخذ بنفس الرأي الذي أخذ به "CATALA" واستند إلى حجتين هو أيضا.

الحجة الأولى: مستوحاة من أفكار الفقيهين الفرنسيين "RIPERT et PLANIOL" وهي فكرة الشيء أو القيمة لها صورة معنوية، وإنّ نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع إقتصادي، وأن تكون جديرة بحماية القانون. [38] ص 50

أما الحجة الثانية : ف " VIVANT " يرى أن كل الأشياء المملوكة معنوية، والتي يعترف بها القانون، وترتكز على الإقرار بأن للمعلومة قيمة، عندما تكون من قبيل البراءات أو الرسومات أو النماذج أو حق المؤلف. فالإنسان الذي يقدم ويكشف عن معلومة لجماعة بصرف النظر عن الشكل أو الفكرة فهو يقدم لهم معلومة بالمعنى الواسع، فهذه الأخيرة لها قيمة تصبح محلا لحق فلا توجد ملكية معنوية بدون الإقرار بالقيمة المعلوماتية، فهو يرى أن القيمة المعلوماتية ليست بالشيء المستحدث فهي موجودة من قبل مجموعة ما، فالمعلومة حاليا مال قابل للتملك والإستغلال فهي حقيقة لها قيمة اقتصادية مؤكدة، وعلى هذا الأساس تنبني قيمتها وليس على أساس الكيان المادي لذلك فهي تستحق الحماية القانونية. [8] ص 20

لهذا السبب يقرر الأستاذ " VIVANT " أن المعلومة يمكن أن تكون محلا لعقد البيع، طالما أن الإبداع المعنوي يظل ضروريا بوصفه إبداعا يرتبط بصاحبه، بل ويمكن علاوة على ذلك تحويل منفعتها أو استغلالها، وهذا هو ما أشار إليه الأستاذ CATALA، فبعد أن أوضح أن المعلومة تنتمي إلى صاحبها بسبب علاقة التبني التي تجمع بينهما، أضاف أنه يمكن لصاحبها أن يتنازل عنها بموجب عقد، أو أن يفيد استعمالها أو أن يرفضه. [3] ص 80

هذا ويرى الأستاذ محمد سامي الشوا ويؤكد أن المعلومة وبالنظر إلى حقيقتها الذاتية واستقلالها تعد قيمة في ذاتها ولها بالتأكيد مظهر معنوي، ولكنها تملك قيمة اقتصادية مؤكدة، وبحيث يمكن عند الإقتضاء أن ترفعها إلى مصاف القيمة القابلة لأن تحاز حيازة غير مشروعة . بدليل أن الحجة التي ساقها الأستاذ CATALA، والتي تركز على رابطة التبني والأبوة التي تجمع المعلومة بمؤلفها. [38] ص 51

وعلى هذا الأساس يمكن القول أن المعلومات، والمعطيات، والبرامج تعتبر أموال قابلة للتملك والإستغلال ليس على أساس كيانه المادي، وإنما على أساس قيمته الإقتصادية ولذلك فهي تستحق الحماية القانونية.

3-1-1 تعريف الجريمة المعلوماتية:

بداية لابد أن نشير إلى أنه لا يوجد خطأ في تعريف الجريمة المعلوماتية، كون أن المعلوماتية يقصد بها المعالجة الآلية للمعلومات، وهي ترجمة للمصطلح الفرنسي "informatique" وتعني تكنولوجيا تجميع ومعالجة وإرسال المعلومات بواسطة الكمبيوتر، وقد إستعمل مصطلح traitement automatisé de données ويعني المعالجة الآلية للبيانات، ومصطلح "telematique" يعني من الناحية اللغوية تقنيات بث المعلومات عبر شبكة الإتصالات البعدية، وهي تعبير اختصار ناتج عن

إندماج كلا من اللغتين informatique أي المعلوماتية، ولفظ télécommunication أي اتصالات [39] ص 76

1-3-1-1 المقصود بالجريمة المعلوماتية:

لقد أحاط بتعريف الجريمة المعلوماتية الكثير من الغموض، حيث تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها، ولكن الفقه لم يتفق على تعريف محدد، بل أن البعض ذهب، إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الإجرام، ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني والبعض الآخر تأرجح بين مضيق لتعريف الجريمة المعلوماتية وبين موسع لتعريفها.

1-1-3-1-1 المدلول الضيق:

من التعريفات المضيقية للجريمة المعلوماتية ما جاء به الفقيه (Merwe) حيث "يرى أن الجريمة المعلوماتية تتمثل في الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي. [40] ص 08

ويرى الأستاذ (Trédman) أن الجريمة المعلوماتية "تشمل أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات. [41] ص 182

وفي رأي آخر ذهب أنصار الإتجاه المضيق إلى تعريف الجريمة، لمعلوماتية بأنها " كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لإرتكابه من ناحية، وملاحظته من ناحية أخرى" كما عرفها هذا الاتجاه بأنها "هي التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط" أو هي " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر، أو تلك التي يتم تحويلها عن طريقه. [39] ص 74

و يعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها "الجرائم التي تلعب فيها البيانات الكومبيوترية والبرامج المعلوماتية دورا رئيسيا".

وكذلك تعريف "David Tompson" بأنها "أية جريمة يكون متطلبا لإقترافها أن تتوفر لدى فاعلها معرفة تقنية الحاسب" [42] ص 298، وفي دراسة وضعها معهد ستانفورد للأبحاث، وتبنتها وزارة العدل الأمريكية عرفت الجريمة المعلوماتية بأنها "أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها.

وكذلك نجد تعريف Stein schjqtberg بأنها " أي فعل غير مشروع ستكون المعرفة بتقنية الكمبيوتر أساسية لإرتكابها والتحقيق فيه وملاحظته قضائيا. [7] ص 07

وما يأخذ على هذه التعريفات أنها ضيققت إلى حد كبير من تعريف الجريمة المعلوماتية، بحيث تستند في تعريفها إلى جزء أو عنصر دون العناصر الأخرى.

فمثلا نرى أن التعريف الذي جاء به الفقيه (Marwe) كان قاصرا على الإطاحة بأوجه الظاهرة الإجرامية بحيث ركز على وسيلة ارتكاب الجريمة والمتمثلة في الحاسب الآلي.

أما عن التعريف الذي جاء به مكتب التقنية في الولايات المتحدة الأمريكية فيعتبر تعريف منتقد هو الآخر حيث يعرف الجريمة المعلوماتية من خلال تعريف جريمة الحاسب بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا، وهو تعريف منتقد لأنه يعرف الجرائم المعلوماتية بأنها الجرائم وذلك من قبل تعريف الشيء بالشيء.

وهناك من التعريفات من ركزت على سمات شخصية لدى مرتكب الفعل، وهي تحديد سمة الدراية والمعرفة التقنية ومن هذه التعاريف تعريف الفقيه David Thompson وكذلك التعريف الذي جاءت به وزارة العدل الأمريكية.

ويعرف جانب آخر من الفقه الجريمة المعلوماتية بالنظر إلى نتيجة الإعتداء، إذ يرى الأستاذ (Mass) أن المقصود بالجريمة المعلوماتية يتمثل في "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح". [41] ص 182

وكذلك الأستاذ (Parker) الذي يرى في تعريفه للجريمة المعلوماتية بأنها "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ترتبت عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الجاني". [35] ص 18

2-1-3-1-1 المدلول الواسع:

فمع الانتقادات التي وجهت إلى أنصار الاتجاه المضيق لتعريف الجريمة المعلوماتية، إتجه جانب من الفقه إلى تعريف الجريمة المعلوماتية على نحو أوسع في محاولة لتفادي القصور الذي طال تعريفات أصحاب الإتجاه المضيق في التصدي لظاهرة الإجرام المعلوماتي.

فمن التعريفات الموسعة لمفهوم الجريمة المعلوماتية ما ذهب إليه الفقيهان (Michel et credo) من أن جريمة الحاسب تشمل " إستخدام الحاسب كأداة لإرتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحساب المجني عليه، أو بياناته، كما تمتد جريمة الحاسب لتشمل الإعتداءات المادية سواء على جهاز الحاسب ذاته، أو المعدات المتصلة به، وكذلك الإستخدام غير

المشروع لبطاقات الائتمان، وانتهاك ماكينات الحاسب الآلية، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية، وتزييف المكونات المادية والمعنوية للحاسب وسرقة جهاز الحاسب في حد ذاته أو أي مكون من مكوناته". [12] ص 158

وحدثا تبني مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقة المجرمين تعريفا جامعاً لجرائم الحاسب الآلي وشبكات، حيث عرف الجريمة المعلوماتية بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية". [41] ص 183

ويعتبر هذا التعريف من أفضل التعريفات التي تناولت ظاهرة الإجرام المعلوماتي، إذ أنها تشمل كلا الجانبين المادي والمعنوي للحاسب الآلي، وكذا شبكة الإنترنت، ولا يقتصر على كونها محل للاعتداء بل أيضاً بوصفها وسيلة للاعتداء وارتكاب الجرائم.

في حين أن منظمة التعاون الاقتصادي والتنمية "OCDE" وضعت التعريف الحالي للجريمة المعلوماتية من أنها "كل فعل أو امتناع من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"

كما عرفها الفقيه الألماني تيامان (Tiedemann) بأنها تشمل " كل أشكال السلوك غير

المشروع الذي يرتكب باستخدام الحاسب" [42] ص 297، ويرى البعض أنه عند وضع تعريف للجريمة المعلوماتية يجب مراعاة عدة اعتبارات هامة وهي:

- أن يكون هذا التعريف مقبول ومفهوم على المستوى العالمي.

- أن يراعى في وضع التعريف التطور السريع المتلاحق لتكنولوجيا المعلومات والاتصالات.

- أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الإجرامي. [39] ص 75

وما يأخذ على هذا الإتجاه أنه لا يضع تعريف محدد للجريمة المعلوماتية، وإنما أشار إلى المبادئ التي يجب مراعاتها في وضع التعريف.

أمّا المشرع الجزائري فنجد بأنه عرف الجريمة المعلوماتية في نفس المادة 2 "أ" من القانون المتضمن قواعد الوقاية من الجرائم الإلكترونية أنه يقصد في مفهوم هذا القانون بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون

العقوبات، وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية". [11] ص 5

وعليه فالجرائم المعلوماتية هي كل فعل أو إمتناع ينشأ نتيجة الإستخدام غير المشروع لتقنية المعلومات ويهدف للإضرار بالمصالح المادية والمعنوية التي يحميها قانون العقوبات. [30] ص 228

1-1-3-2 موضوع الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات:

يختلف موضوع الجريمة المعلوماتية بحسب اختلاف الزاوية التي ينظر فيها إزاء الإعتداء الموجه ضد أحد مكونات النظام المعلوماتي، فمن ناحية قد يكون هذا الأخير نفسه موضوع للجريمة المعلوماتية ومن ناحية أخرى قد يكون النظام المعلوماتي هو أداة الجريمة ووسيلة تنفيذها. [38] ص 45

وتجدر الإشارة إلى أن الجرائم التي نص عليها المشرع الجزائري وفقا لقانون العقوبات، هي الجرائم التي يكون النظام المعلوماتي بمكوناته (المادية، المعنوية) محلا للجريمة، وعليه سوف نتناول كلا القسمين على النحو التالي:

1-1-3-1 وقوع الجريمة على أحد مكونات النظام المعلوماتي

و في هذه الحالة تكون نظم المعلومات ذاتها محلا لأفعال يعتبرها المشرع الجنائي غير مشروعة ومن المعروف أن أي نظام للمعلوماتية يشتمل على ثلاثة عناصر رئيسية، يمكن أن تكون فردية أو مجتمعة محلا لجرائم المعلوماتية وهذه العناصر هي: المكونات المادية للنظام المعلوماتي، البرامج التي يحتوي عليها النظام وكذا المعلومات المسجلة على نظام المعلوماتية. [03] ص 100

- الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

تتحقق هذه الحالة في الفرض الذي تكون فيه أجهزة الكمبيوتر المادية من أجهزة ومعدات مادية وكابلات وآلات طباعة... محلا للجريمة، ولا تثير هذه الحالات ثمة مشكلة باعتبار أن هذه المكونات المادية محل الاعتداء، تتمتع بالحماية الجنائية للنصوص التقليدية باعتبارها من الأموال المنقولة التي تخضع سرقتها وإتلافها للنصوص الجنائية التقليدية. [43] ص 36

- الجرائم الواقعة على المكونات المنطقية للنظام المعلوماتي:

تتحقق جريمة التعدي على المكونات غير المادية للنظام المعلوماتي، عندما تكون مكونات الكمبيوتر غير المادية مثل البرامج المستخدمة، والبيانات المخزنة في ذاكرة الكمبيوتر محلا أو موضوعا للجريمة. [44] ص 15

وعليه فالإعتداء في هذه الحالة إما أن يقع على البرامج بنوعيتها، وإما أن يقع على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات وذلك بإتلافها أو التلاعب بها إلى غير ذلك من الأفعال التي تهدد السرية والسلامة والموقورية للمعلومات والمعطيات.

إنّ الأساليب المستخدمة للإعتداء على المكونات غير المادية للكمبيوتر قد لا تتطلب معرفة فنية، بل مجرد سلوك مادي قد يقتصر في بعض الحالات على مجرد الإطلاع البصري للمعلومات، وفي حالات أخرى قد يتطلب معرفة فنية يستطيع المجرم المعلوماتي من خلالها القيام بعملية ما يسمى بالسطو المسلح الإلكتروني، ومن هذه الوسائل التقاط المعلومات التي توجد بين الكمبيوتر والنهاية الطرفية terminal والتدخل غير المشروع في نظام معلوماتي بواسطة نهاية طرفية، أو إلتقاط الإشعاعات الصادرة عن الجهاز المعلوماتي، وتسجيل الاتصالات بواسطة خط التليفون. [45] ص 67

ويدخل ضمن هذه الجرائم ما إصطلح الفقه على تسميته بسرقة وقت الماكينة، أو سرقة وقت الحاسب الآلي، وهذه الجريمة تتم عادة من قبل العاملين بنظم المعلوماتية الذين يلجأون في بعض الأحيان إلى استخدام أجهزة النظام المعلوماتي من كمبيوتر، وما إلى ذلك للقيام بأعمال خاصة بهم، وهنا تكون واقعة السرقة منصبة ليس على أشياء مادية بالمعنى المفهوم للكلمة، وإنما على وقت الجهاز، ما دام الوقت يمكن تقويمه بالمال. [03] ص 100.

نظرا للطابع الخاص الذي يميز هذه المكونات عن النصوص التقليدية الحالية لقانون العقوبات فتكون عاجزة عن مواجهة ما قد ينجم عليها من جرائم، نظرا لطبيعتها المختلفة عن المكونات المادية، وعليه فقد استحدث المشرع الجزائري وفقا للقانون 15/04 نصوص قانونية تواجه مثل هذه الاعتداءات.

1-1-3-2 وقوع الجريمة بواسطة النظام المعلوماتي:

في هذه الحالة لا يكون الحاسب الآلي محل أو موضوع للجريمة المعلوماتية، وبالتالي لا يكون محلا للحماية الجنائية، وإنما تقع الجريمة في هذه الحالة بواسطته، أي أنه يستخدم كأداة لإرتكابها.

تتنوع الجرائم التي ترتكب بواسطة النظام المعلوماتي، ما بين جرائم اقتصادية، أو قرصنة المعلومات، أو ذات طابع سياسي، أو متعلقة بالأمن القومي، وقد تقع هذه الجرائم على الأشخاص الطبيعية أو الاعتبارية. [45] ص 68

ومن أمثلة هذه الجرائم، التجسس، التصنت، والتزوير في عمليات سحب جوائز المسابقات وتحويل الأموال من حساب إلى آخر، وجريمة فك شفرة القنوات التلفزيونية الخاصة، وكذلك جريمة تحويل الطائرات والسيارات إلى طرق أخرى، وكذلك جريمة القتل عن طريق برمجة جهاز يقوم بتفجير نفسه عن بعد. [46] ص 47

بالإضافة إلى الجرائم التي ترتكب على شبكة الإنترنت أو بواسطتها، وهي دائما في إزدياد نتيجة التطور التكنولوجي المتواصل، وجرائم الإنترنت إما أن يكون محل الاعتداء فيها هو المال وإما أن يكون هو الأشخاص أو الحقوق التقنية، ومن أمثلتها جريمة النصب عن طريق الإعلان عن بيع سلع وهمية والاستيلاء على أموال العملاء، وكذلك جريمة إنتحال شخصية الغير، وكذا جرائم التحريض على الفتنة الطائفية التي ترتكب في غرف الحوار الموجودة في الشبكة، حيث يدير هذه الغرف في الغالب أشخاص مأجورون من قبل دول أو جماعات إرهابية لها ميولات عدوانية تحض على الكراهية بين الأديان... والجرائم الجنسية التي تدعوا إلى الفجور والدعارة واستغلال الأطفال جنسيا. [17] ص 17

وهذه الجرائم وأخرى تعد في حقيقتها جرائم تقليدية، لولا إتصالها بالنظام المعلوماتي باعتباره وسيلة لإرتكابها، وسنتناول في هذا الفرع أمثلة عن بعض الجرائم التي يمكن أن تقع باستخدام النظام المعلوماتي، أولا: الجرائم الواقعة على الأشخاص الطبيعية ونأخذ جريمة الإعتداء على حرمة الحياة الخاصة كمثال، ثانيا: الجرائم الواقعة على الأنظمة المعلوماتية ونأخذ جريمة الدخول داخل نظام المعالجة الآلية كمثال وسوف نتطرق لها في الفصل الثاني بالتفصيل، ثالثا: الجرائم الواقعة على الأشخاص الاعتبارية ونأخذ الجرائم الواقعة على أسرار الدولة كمثال.

- الجرائم الواقعة على حرمة الحياة الخاصة:

لحياة الأفراد خصوصيتها بما تحويه من أسرار وخصوصيات، والمحافظة عليها من أكثر الأمور التي تحظى بحماية دستورية وقانونية في كافة دساتير العالم. والحق في الخصوصية هو أحد الحقوق اللصيقة التي تثبت للإنسان، والتي غالبا ما يصعب حصر الجوانب المختلفة لها، والتميز

بحدود واضحة بين ما يعد من الحياة الخاصة للإنسان، وما يعد من الحياة العامة له. [40] ص 59

وقد كفل الدستور الجزائري الحقوق والحريات الفردية، حيث جاء في المادة 39 منه أن " حرمة حياة المواطن الخاصة وحرمة شرفه مصونة بمقتضى الدستور".

ونجد كذلك أن المادة 301 قانون العقوبات الجزائري: " تعاقب بالحبس من شهر إلى ستة أشهر وبغرامة من 20.000 دج إلى 100.000 دج أصحاب المهن الاستشفائية، و جميع الأشخاص المؤتمنين على الأسرار إذا ما أفشوها في غير الحالات التي أوجب فيها القانون ذلك". وهذه الأسرار قد تكون مخزنة في أنظمة المعالجة الآلية للمعطيات مما تتحقق معه الجريمة.

أمّا ما تعلق بالقانون 15/04 المؤرخ في 2004/12/10 المعدل والمتمم لقانون العقوبات والذي أضاف قسما خاصا بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، لم يتضمن نص يجرم الاعتداء على البيانات الاسمية، عدا ما ورد في العنصر الثاني من المادة 394 مكرر فقرة 2 التي تنص على أنه "يعاقب بالحبس من شهرين إلى ثلاثة سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي.

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم، وعليه قد تكون هذه البيانات المتحصل عليها هي بيانات إسمية تتعلق بأشخاص، مما تتحقق معه الجريمة، لكن الشرط الوحيد هو أن تكون هذه البيانات متحصل عليها من إحدى جرائم المعلوماتية.

ومن الصعوبة وضع تعريف دقيق وشامل لمفهوم الحياة الخاصة، والسبب في ذلك يعود إلى تبدل هذا المفهوم وتطوره باستمرار تبعا لتبدل المفاهيم الاجتماعية، والاقتصادية، والسياسية والثقافية، والدينية وتطوره وربما يكون من الأسهل تعدد العناصر التي يتكون منها مفهوم الحياة الخاصة من مكان وزمان محددين، فضلا على أنه مفهوم يتبدل بين دولة وأخرى، وبين مجتمع وآخر وأنه يصعب إيجاد تصور عالمي موحد. [04] ص 92

وحماية الحياة الخاصة للأفراد تجد جوهرها في حق الأفراد أن يكون لهم مأمّن لإيداع أسرارهم الخاصة، وحقهم في إبقائها طي الكتمان فلا يعلم بها غيرهم، ولا تمتد لها يد العابثين فيساء استخدامها ولقد ظلت حينا من الزمن حبيسة حتى إنفجار ثورة التكنولوجيا، وظهور الحاسب الآلي وتطوره إلى الحد الذي يملك القدرة على الإحتفاظ بكميات هائلة من المعلومات والبيانات وفق أسس وبرامج تعد لهذه الغاية. [47] ص 215

والنظام المعلوماتي يمكن أن يستخدم في الإعتداء على حرمة الحياة الخاصة، أو على الحرية العامة للفرد، ويتحقق ذلك إذا قام شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه أو إذنه، أو أن يكون تجميع هذه المعلومات بعلم الشخص المعني ولكن قام المكلف بحفظها بإطلاع الغير عليها بدون إذن صاحبها. [37] ص 187

فالحاسبات الآلية بما لها من قدرة فائقة على التخزين، والمعالجة، والإسترجاع، ونقل عدد ضخم من البيانات والمعلومات تكون أقدر في الاعتداء على حريات الأشخاص وحياتهم الخاصة نظرا لعدم وجود الحماية التقنية والفعالة لما يتم تداوله من بيانات، ومعلومات، وأسرار ومراسلات... حيث نجد أن الدول المتقدمة تقوم بجمع المعلومات عن الأفراد وذلك عن طريق إنشاء ما يعرف ببنوك المعلومات، مما يجعلها بعض الفقه أداة للرقابة غير المسبوقه في يد السلطات، أضف إلى ذلك أن كثيرا من المؤسسات الكبرى، والشركات الحكومية، والخاصة تجمع عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي، أو العائلي، أو الأمني، والعادات الاجتماعية...

و تستخدم الحاسبات الآلية وشبكات الاتصالات والمعلومات في خزن تلك البيانات الخاصة ومعالجتها، وهو ما يجعل فرص الوصول إلى هذه البيانات على نحو غير مصرح به أو مأذون به، أو بطريق التحايل أكثر من ذي قبل، ويفتح مجالا أوسع لإساءة استخدامها أو توجيهها توجيها منحرفا أو خاطئا، وتعرية خصوصيات الأفراد، أو الحكم عليهم حكما خفيا من واقع سجلات البيانات الشخصية المخزنة، الأمر الذي حدا بالكثيرين إلى وصف استخدام الحاسبات الآلية كبنوك للبيانات، والمعلومات بأنه تهديد غير مقبول للخصوصية والحريات المدنية [03] ص 188 ، ومن صور الانتهاكات الواقعة على حرمة الحياة الخاصة.

• استخدام بيانات شخصية غير صحيحة

* وذلك إما عن طريق التلاعب ببيانات شخصية، أو محوها، وتتحقق هذه الحالة في أغلب الأحيان لتحقيق مصالح مالية. ومثال ذلك ما حدث في قضية الشركة "TRW Company Crédit Data" حيث كانت تزود عملائها وكان أكثرهم من البنوك والمتاجر الكبرى وشركات تسهيلات الائتمان... من خلال حساباتها وأنظمتها المعلوماتية بمعلومات تتعلق بالمركز الائتماني للأشخاص الذين يرغب هؤلاء العملاء في التعامل معهم، لأنها كانت تنشأ قاعدة بيانات عن هؤلاء الأشخاص، وتخزنها في حساباتها إلى أن قام بعض الجناة بالتلاعب في البيانات وتم توريث المتعاملين في التعامل معهم وهم لا يعلمون أن الأشخاص محل التعامل مركزهم الائتماني سيئ إلى أن فضح أمرهم بالمصادفة.

* و إما عن طريق جمع، أو معالجة، أو نشر بيانات شخصية غير صحيحة من قبل أشخاص مصرح لهم، ونشرها، إلا أن أغلبها يتم عن طريق الإهمال، وإن كان في أحيان أخرى يمكن أن تتم لتحقيق غرض ما لصاحب البيانات والمعلومات.

• جمع أو تخزين بيانات شخصية صحيحة ولكن على نحو غير مشروع جنائياً:

و تكون إما عن طريق:

* الأساليب المستخدمة للحصول على هذه البيانات والمعلومات تكون غير مشروعة، ومن هذه الأساليب إعتراض، وإلتقاط، وتفريغ الرسائل المتبادلة عن طريق البريد الإلكتروني، أو إلتقاط الإرتجاجات التي تحدثها الأصوات في الجدران الإسمنتية...

* عدم مشروعية مضمون البيانات التي يتم منعها أو تخزينها: وهنا تتحقق في الفرض الذي تجمع فيه كافة البيانات عن الأشخاص مما يتحقق معه استنتاج صور تقريبية لشخصياتهم.

• الإفشاء غير المشروع للبيانات الشخصية وإساءة إستخدامها:

سواء كانت هذه البيانات مشمولة بالحماية الجنائية التقليدية أو لا. [03] ص 190

- الإعتداء على أسرار الدولة:

يقصد بالجرائم الواقعة على الحق في الأسرار تلك الجرائم التي تقع باستخدام النظام المعلوماتي في إفشاء الأسرار، سواء ما كان منها متعلقاً بأسرار عامة وهي تخص الدولة ونظام الدفاع عنها ومنها ما تكون أسراراً خاصة وما يطلق عليها الأسرار المهنية. [37] ص 197

فقد تمس الجرائم المعلوماتية المصالح العليا للدولة، عن طريق إفشاء العديد من الأسرار والمعلومات التي تتعلق بالأمن القومي، كما لو كانت تتعلق بالمخابرات العامة، أو بالدفاع الوطني ولا شك في أهمية هذه البيانات والمعلومات المخزنة ألياً، وتأثيرها البالغ على مستقبل الدول والشعوب على حد سواء. [03] ص 200

و جريمة إفشاء الأسرار تقع بأي وسيلة كانت سواء عن طريق سرقة المعلومات، أو عن طريق التجسس بواسطة الأقمار الصناعية، ومن ثم إفشاء ما توصل إليه من معلومات وأخبار وبالتالي لا تهم الوسيلة المهم أنّ هذه الوسيلة تحقق الغاية المرجوة منها وهي إفشاء الأسرار.

كذلك لا تهم الغاية من وراء الاعتداء على أسرار الدولة سواء كان غرض الجاني هو الحصول على مقابل مالي، أو بغرض المساس بسمعة تلك الدولة...، نشير إلى أن المعلوماتية تلعب دورا هاما في هذا المجال، بحيث يمكن أن يصل المعتدي إلى المعلومة في أي وقت يشاء.

يعتبر من قبيل الاعتداء على الأسرار الدولة سواء كانت الأسرار اقتصادية أو مالية، أو عسكرية أو سياسية، المهم في الأمر أن يتم الاعتداء على أسرار الدولة بدون رضاها وبدون إرادتها.

2-1 خصائص الجريمة المعلوماتية:

تتسم الجرائم المعلوماتية بأنها ذات خصائص متفردة خاصة بها، لا توجد في أي من الجرائم التقليدية، سواء في أسلوبها أو في طريقة ارتكابها، فهي تتميز بالطابع الفني كونها جريمة إلكترونية تقنية، ويرتكبها في الغالب مجرم يختلف عن المجرم العادي من عدة جوانب.

كما أنها تقع بنسبة كبيرة على المؤسسات المالية، وتتميز أيضا بصعوبة توقيع الجزاء في مثل هذا النوع من الجرائم لصعوبة اكتشافها، وإن اكتشفت فتبقى عصية على مسألة الإثبات وإن أثبتت قد يقف تنازع الاختصاص القضائي عائقا أمام توقيع الجزاء على مرتكبها.

وعليه سنتطرق في هذا المبحث إلى أشخاص الجريمة في المطلب الأول وفي المطلب الثاني سوف نتطرق إلى صعوبة توقيع الجزاء.

1-2-1 أطراف الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات:

إن إرتباط الجريمة المعلوماتية بالحاسب الآلي لم يكن له أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين، الذين جنحوا إلى السلوك الإجرامي النمطي [12] ص 174.

فالجريمة المعلوماتية تختلف عن بقية الجرائم العادية في كونها ترتكب من قبل مجرم له مجموعة من الخصائص تميزه عن بقية المجرمين العاديين، لأنه مجرم ذكي له دراية بالمعلوماتية، ويتميز بالاحتراف وأنه غير عنيف...

كذلك تختلف عن الجرائم العادية في أنها تقع على الهيئات والمؤسسات المالية، وإن كانت تمس الأنظمة المملوكة للأشخاص الطبيعيين، فالمجني عليه في الجريمة المعلوماتية يكون على الأغلب شخصا معنويا، وعليه سنتناول في الفرع الأول الجاني وفي الفرع الثاني المجني عليه.

1-1-2-1 المجرم المعلوماتي

لا شك أن الشخص الذي يرتكب الفعل غير المشروع، ويعتدي فيه على حق من حقوق الغير بالمعنى الواسع، يعد في نظر القانون مجرماً، ويتعرض للعقاب إذا ما اقتترف جريمته.

لذلك فحتى تحقق العقوبة هدفها في مجال الردع العام أو الخاص، يجب أن ننظر إلى المجرم من حيث الظروف التي دفعته لإرتكاب جريمته، وكذا صفاته وذلك حتى يمكن إعادة تأهيله إجتماعياً حتى ينفع المجتمع ولا يضره، ولقد حظيت أبحاث علم الإجرام بمجموعة من الدراسات القانونية بغرض كشف النقاب عن فكرة المجرم المعلوماتي. [38] ص 61

1-1-1-2-1 سمات المجرم المعلوماتي: يمكن إجمال أهم سمات المجرم المعلوماتي في الآتي:

- المجرم المعلوماتي مجرم ذكي:

يعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتية، لأن ذلك يتطلب منه معرفة تقنية لكيفية الدخول إلى أنظمة الحاسب الآلي، والقدرة على التعديل، والتغيير في البرامج لإرتكاب جرائم السرقة والنصب وغيرها. [39] ص 133

فلا يمكن أن ينتمي المجرم المعلوماتي إلى طائفة المجرمين الأغبياء، فإذا كان من يسرق من منزل أو سيارة محدود الذكاء في كثير من الأحيان، فإن من يستعين بالكمبيوتر في السرقة من أموال بنك أو شركة يتميز بمستوى رفيع من الذكاء، حتى يستطيع أن يتغلب على الكثير من العقبات التي تواجهه في ارتكاب جريمته، فهو أقرب إلى مرتكبي جريمة النصب منه إلى مرتكبي جريمة السرقة. [04] ص 41

- المجرم المعلوماتي مجرم متخصص:

قد ثبت في عديد من القضايا أن عدد من المجرمين لا يرتكبون إلا جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم. [04] ص 40

إلا أن هذا لا يعني بالضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال، أو أن تكون لديه خبرة كبيرة فيه، بل إن الواقع العملي قد أثبت أن جانب من أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لإرتكاب الجريمة عن طريق التعليم، أو الخبرة المكتسبة من العمل في هذا المجال. [12] ص 176

ومعنى ذلك أن المهارة، والخبرة، والتخصص هي التي تحدد نوع الجريمة المرتكبة، بحيث إذا كان الشخص مرتكب الجريمة على قدر ضئيل من مستوى الخبرة، نجد أن الجرائم التي قد يرتكبها لا تتعدى الإتلاف المعلوماتي، إمّا بالمحو، أو الإتلاف، وكذلك بنسخ البيانات والبرامج. أمّا إذا كان الشخص على مستوى عالي من المهارة فإن أسلوب ارتكابه للجرائم يختلف بحيث يقوم عن طريق استخدام الشبكات بالدخول إلى أنظمة الحاسب الآلي وسرقة الأموال، وارتكاب جرائم النصب، والتجسس، وزرع الفيروسات. [39] ص 135

- المجرم المعلوماتي مجرم عائد إلى الإجرام:

يعود كثيرا من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر، إنطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة في المرة السابقة. [04] ص 41

وربما يعودون لإرتكاب هذه الجرائم إعتقادا منهم أن النظام غير القادر على حماية نفسه ليس من الخطأ إقتحامه، فلا يشعرون بأنهم ارتكبوا أفعالا غير مشروعة.

- المجرم المعلوماتي مجرم محترف:

بالإضافة إلى خاصية أو سمة الإختصاص فالمجرم المعلوماتي يتمتع باحترافية كبيرة في

تنفيذ جرائمه، حيث أنه يرتكبها عن طريق الكمبيوتر، الأمر الذي يقتضي الكثير من الدقة والتخصص والإحترافية، حتى يتمكن من التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية....

- المجرم المعلوماتي مجرم غير عنيف:

المجرم المعلوماتي من المجرمين الذين لا يلجأون إلى العنف بتاتا في تنفيذ جرائمهم، وذلك لأنها تنتمي إلى إجرام الحيلة، فهو لا يستلزم قدرا من العنف، وإن صح التعبير فالعنف في مثل هذه الجرائم يتخذ شكلا غير مرئيا للعيان، وغير محسوس به، لأنه يؤدي إلى تخريب الأنظمة والتلاعب بالمعطيات، فهو عنف من نوع خاص.

- المجرم المعلوماتي مجرم إجتماعي بطبيعته:

المجرم المعلوماتي مجرم متكيف مع المجتمع الذي يحيط به، وإنسان ذكي جدا ويساعده ذلك على عملية التكيف. وما الذكاء في رأي الكثيرين سوى القدرة على التكيف، ولا يعني هذا التقليل من شأن المجرم المعلوماتي، بل إن الخطورة الإجرامية قد تزيد إذا زاد تكيفه الإجتماعي مع توافر الشخصية الإجرامية لديه. [04] ص 42

2-1-1-2-1 الأنماط المختلفة للمجرم المعلوماتي:

إنه لمن الصعوبة حصر أنواع المجرم المعلوماتي، ذلك لتعدد تقسيمات المختصين في هذا المجال، كل حسب الزاوية التي ينظر منها إليهم، وعلى هذا الأساس سوف نأخذ بهذا التقسيم.

- القراصنة: "les pirates": وهناك من القراصنة:

الصف الأول: الهواة hackers: وهم من الشباب الفضوليين الذين يسعون للتسلية، ولا يشكلون خطورة على الصناعات وأنظمة المعلومات.

الصف الثاني: المحترفون crackers: وهم أكثر خطورة من الصف الأول، وقد يحدثون أضرار كبيرة وقد يؤلفون أندية لتبادل المعلومات فيما بينهم. [48] ص 01

ومع أن هذا المعيار غير مضبوط، إلا أن الدراسات والمعالجات في حقل جرائم المعلوماتية وبعض التشريعات المحلية في الولايات المتحدة الأمريكية تعتمد هذا التمييز، فإصطلاح الكراكرز مرادف للهجمات الحاقدة والمؤذية، في حين أن إصطلاح الهاكرز مرادف في الغالب لهجمات التحدي، طبعاً دون أن يؤثر هذا التمييز على مسؤولية مرتكبي تلك الأنشطة في كلا الطائفتين ومساءلتهم عما يلحقونه من أضرار بالبيانات المستهدفة. [49] ص 279

- المحترفون:

تتميز هذه الطائفة بسعة الخبرة، والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكبها، ولذلك تعد هذه الفئة الأخطر من بين مجرمي التقنية حيث تهدف إعتداءاتهم إلى تحقيق الكسب المادي لهم، أو للجهات التي كلفتهم وسخرتهم لإرتكاب الجرائم، كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية، والتعبير عن موقف فكري أو نظري أو فلسفي. [42] ص 307

إلى جانب المعرفة التقنية المتميزة، والتنظيم العالي، والتخطيط للأنشطة المقصود إرتكابها، فإن أفراد هذه الطائفة يتسمون بالتكتم خلافا للطائفة الأولى، ولا يتبادلون المعلومات بشأن أنشطتهم ويحاولون ما أمكن عدم كشف طرقهم التقنية لإرتكاب جرائمهم، ولقد أثبتت الدراسات أن أعمارهم على الأغلب من 25-40 عام.

يتم تصنيف أفراد هذه الطائفة إلى فئات متعددة، إما تبعا لتخصصهم، أو تبعا للوسيلة المتبعة من قبلهم في إرتكاب جرائمهم، فمثلا نجد طائفة محترفي التجسس، وطائفة محترفي الإحتيال، وضمن كل طائفة من هذه الطوائف نجد طوائف أخرى. [42] ص 308

- الحاقدون:

تختلف هذه الطائفة عن الطوائف الأخرى من حيث الهدف، والغرض من وراء إرتكاب هذه الجريمة، فالهدف من وراءها هو حب الإنتقام، والثأر كأثر لتصرف صاحب العمل، أو المنشأة المعنية معهم ولهذا فإنهم يكونون إما مستخدمين للنظام بوصفهم موظفين أو مشتركين، أو على علاقة ما بالنظام محل الجريمة، أو إلى غرباء عن النظام تتوفر لديهم أسباب للإنتقام من المنشأة المستهدفة. [49] ص 279

وليس هناك ضوابط محددة بشأن أعمارهم، كما أنه لا تتوافر عناصر التفاعل بين أعضاء هذه الطائفة، ولا يفاخرون بأنشطتهم، بل يعمدون إلى إخفاءها، وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بإرتكابها لتوفر ظروف وعوامل تساعد على ذلك، وبالرغم من أن سمات هذه الطائفة تضعها من حيث الخطورة في مؤخرة الطوائف المتقدمة، إذ هم أقل خطورة من مجرمي التقنية، لكن ذلك لا يمنع أن تكون الأضرار التي نجمت عن أنشطة بعضهم جسمية ألحقت خسائر فادحة بالمؤسسات المستهدفة. [07] ص 173

- صغار السن:

يطلق عليهم البعض إسم صغار نوابغ المعلوماتية، ويصفهم بأنهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية، فإن من بينهم فئة لا تزال دون سن الأهلية، مولعون بالحوسبة والاتصال، وتكون أعمارهم دون الحد الأدنى للمجرمين البالغين أي دون 25 سنة.

وقد تعددت أوصافهم في الدراسات الاستطلاعية، والمسحية وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بمصطلح (المتلثمين) الدال حسب تعبير الأستاذ "توم فوستر" على "الصغار المتحمسين للحاسوب"، بشعور من البهجة دافعهم التحدي لكسر الرموز السرية لتكريبات الحاسوب، ويسميه

البعض كذلك المجانين بمجانين معدلات ومعدلات عكسية لكثرة استخدامهم تقنية المعدل والمعدل العكسي الموديم. [42] ص 309

يثير مجرموا الحوسبة من هذه الطائفة جدلا واسعا بين متحدث عن مخاطر هذه التقنية، وبين مدافع عنها وفقا لمجموعة من المؤلفات والدراسات. [07] ص 173

ولقد إنقسم الفقه إلى 3 إتجاهات تقديرية لطبيعة هذه الفئة.

الإتجاه الأول: يرى أنه لا يجب تصنيفهم ضمن الطوائف الإجرامية لمجرمي الحواسيب إستنادا إلى أن صغار السن (المتلعثمين) لديهم ببساطة ميل إلى المغامرة والاكتشاف، وهم لا يدركون ولا يقدرّون مطلقا نتائج أفعالهم غير المشروعة.

الإتجاه الثاني: هذا الإتجاه يصفهم بالأخيار، وأحيانا بالأبطال الشعبيين ويتمادى في ذلك إذ يطالب بمكافنتهم باعتبارهم لا يسببون ضررا للنظام، ونسب إليهم الفضل في كشف الثغرات الأمنية في تقنية المعلومات وكان " هوجو كورن " أحد أكبر المدافعين عن الهاكرز الصغار.

الإتجاه الثالث: يرى أنهم يصنفون ضمن مجرمي الحاسوب كغيرهم دون تمييز، إستنادا إلى أن التمييز بين العبث بالحواسيب وبين الجريمة أمر عسير، هذا من جهة، ومن جهة أخرى إستنادا إلى خطورة جرائمهم المدمرة. [07] ص 174

3-1-1-2-1 أسباب ارتكاب الجريمة

تتباين أسباب ارتكاب الجرائم المعلوماتية تبعا لطبيعة المجرم، ومدى ثقافته، وخبرته في مجال الحاسب الآلي، لأن المتهم يرتكب جريمته بناء على ما لديه من خبرة، فمن لا تتعدى خبرته تشغيل جهاز الحاسب الآلي لا يمكنه ارتكاب جريمة موافقة تماما لمن له خبرة في مجال البرمجة، ولا يمكن تصور نفس الدافع لهما، فالدوافع تختلف من مجرم إلى آخر، ويمكن إجمال هذه الدوافع في الآتي:

- تحقيق المكسب المادي:

يعد هذا الدافع والذي يمثل في الحقيقة غاية الفاعل من بين أكثر الدوافع تحريكا للجناة لإقتراف جرائم الكمبيوتر، ذلك أن خصائص هذه الجرائم، وحجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الكمبيوتر، أو الاحتيال المرتبط بالكمبيوتر يتيح تعزيز هذا الدافع. [07] ص 177

وعلى هذا الأساس نلاحظ أن أكثر الأنظمة المستهدفة هي الأنظمة التابعة للمؤسسات المالية كالبنوك مثلا، وأكثر الجرائم المقترفة هي جرائم تحويل الأموال، واستخدام بطاقات الائتمان التابعة لأشخاص آخرين... كون أن الربح متحقق في هذه المؤسسات لتوفرها على سيولات نقدية بمبالغ ضخمة.

- إثبات التفوق العلمي:

إن الدافع الثاني لإرتكاب مثل هذا النوع من الإجرام هو إثبات التفوق العلمي، ويعتبر صغار نوابغ المعلوماتية هم أغلب من يحركهم هذا الدافع، لأنهم يسعون إلى اكتشاف ما هو جديد، وفك الشفرات بالإضافة إلى أن دافع تحقيق الكسب المادي ليس دافعهم.

- النزعة إلى الإنتقام:

يعد دافع الإنتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى إرتكاب جريمته، لأنه غالبا ما يصدر من شخص يملك معلومات كثيرة عن المؤسسة، أو الشركة التي يعمل بها نتيجة إما لفصله عن العمل، أو تخطيه في الحوافز والترقية.

وما يزيد الأمر خطورة هو إستعداد الجاني مسبقا لإرتكاب جريمته، إما عن طريق احتفاظه بكلمة السر، وإما بزرع برنامج مسبقا قبل مغادرته المؤسسة [39] ص 140، أو قيامه بإعطاء كلمة السر لشركة منافسة أخرى، أو تزويدها بكل المعلومات التي تساعد على تدمير المعلومات والبيانات للشركة المنافسة.

- أسباب شخصية متفرقة:

يتأثر الإنسان في بعض الأحيان ببعض المؤثرات الخارجية التي تحيط به، ونتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، مع توافر هذه المؤثرات، فإن الأمر يؤول في النهاية إلى إرتكابه لجريمة معلوماتية. [38] ص 66

لأن هذه المؤثرات التي تضغط على الإنسان تجعل له إعتلالا في شخصيته، مما يسبب له أمراضا نفسية، أو ما يعرف بأمراض العصر، وهذه الأمراض تجعل الإنسان غير مبال بما يقوم به، ولا يقدر النتائج مطلقا.

كذلك قد يكون هناك بعض الأشخاص الذين يقعون تحت وطأة الرغبات الجنسية فتصبح هذه الدوافع قائدا لصاحبها في غير هوى منه أو روية، وبحصوله على الوسيلة التي تمكنه من تحقيق رغبته

فيسعى دوماً إلى الإختراق والتجسس للحصول على رغبته، كذلك قد يكون المرض النفسي ناتجا عن التعصب الديني والعقائدي مما يجعل الشخص يقوم بجرائم التشهير والإتلاف... [50] ص 210

3-1-2-1 المجني عليه في الجريمة المعلوماتية:

إن الجرائم المعلوماتية يمكن أن يقع ضحيتها جميع الأشخاص سواء كانوا أشخاصا طبيعيين أو أشخاصا معنوية (خاصة أو عامة)، طالما أنها تستخدم الحاسب الآلي في ممارسة أنشطتها سواء الاقتصادية، أو الاجتماعية، أو حتى الأنشطة السياسية والعسكرية.

يلاحظ أنه من الصعب تحديد نطاق ضحايا هذه الجرائم على وجه الدقة، وذلك يرجع إلى أن هؤلاء الضحايا لا يعلمون شيئا عنها إلا بعد أن تقع بالفعل، وفي هذه الحالة من الحكمة عدم الإبلاغ عنها، وبالتالي لا يحبز أكثرهم أن يعترف بأن نظامه المعلوماتي قد وقع ضده إنتهاك ما، وهذا السلوك السلبي يعتبر مغريا لمرتكبي هذه الجرائم للاستمرار في نشاطهم، ومما هو جدير بالملاحظة أن هذا النوع من الجرائم يوجه بصفة رئيسية إلى البنوك. [35] ص 28

يمكن تقسيم المجني عليهم في مجال الجريمة المعلوماتية إلى فئتين على النحو التالي: إما أن يكونوا أشخاصا طبيعيين وإما أن يكونوا أشخاصا معنويين بقسميهم سواء أشخاص معنوية عامة أو أشخاص معنوية خاصة.

نلاحظ أن طائفة المجني عليهم في الجريمة المعلوماتية قد شملت أغلب الأشخاص لأنها جريمة تقنية، فالإنتشار في الوسائل التقنية هو الذي أدى إلى تعدد فئات المجني عليهم نظرا لسهولة ارتكاب هذه الجريمة، المهم في هذه الجرائم هو أن يكون الجاني والمجني عليهم مالكين لأجهزة تقنية حديثة بها نظام معالجة آلية للمعطيات.

يعتبر جهاز الحاسب الآلي هو الأنسب من بين الأجهزة الأخرى كالهاتف النقال مثلا، لإرتكاب وتسهيل ارتكاب هذا النوع الحديث من الإجرام لقدرته الفائقة على الاستيعاب، والتخزين، وإمكانية معالجة المعطيات الموجودة بداخله بأي طريقة وبسهولة فائقة، بالإضافة إلى إمكانية إستخراج هذه المعطيات واسترجاعها متى أراد ذلك.

وعليه فالجريمة المعلوماتية تقع على جميع الأشخاص الشرط الوحيد هو توافر الوسائل التقنية والتكنولوجية الحديثة.

1-3-1-2-1 الأشخاص الطبيعية:

إن الأشخاص الطبيعية كغيرها من الأشخاص الأخرى قد تكون عرضة للجرائم المعلوماتية، ولكن الملاحظ أن ضررها يكون أقل بكثير من الضرر اللاحق بالأشخاص المعنوية، وهذا نتيجة لأن الذمة المالية للأشخاص الطبيعية أقل بكثير من الذمة المالية للأشخاص المعنوية هذا من جهة .

ومن جهة أخرى فإن أكثر الجرائم التي تقع على الأشخاص الطبيعية هي جرائم تتميز بطابع شخصي، فغالبية الجرائم تكون إما الإعتداء على الحياة الخاصة للأفراد، وذلك عن طريق تجميع المعلومات الخاصة بهم، والبحث على أدق التفاصيل في حياتهم بالإضافة إلى جرائم التشهير، والسب والقذف عبر شبكة الأنترنت، ولكن هذا لا يمنع أن تتعرض الأشخاص الطبيعية لجريمة من جرائم الأموال ومثلها سرقة بطاقات الإنتمان الخاصة بهم ومن ثم الإعتداء على أموالهم بالسرقة.

يتعرض كذلك الأشخاص الطبيعيون لجرائم النصب عبر شبكات الأنترنت، وخير مثال على ذلك وقوع الكثير من الشعب الأمريكي ضحية لجريمة النصب من قبل بعض الأشخاص، مستغلين الحادث الإرهابي الذي حدث في الولايات المتحدة الأمريكية في 2001/09/11، حيث قامت العديد من الجهات بإنشاء عدة مواقع على شبكة الأنترنت بغرض جمع تبرعات للضحايا. [39] ص 153

2-3-1-2-1 الأشخاص المعنوية:

كما سبق الإشارة إليه فإن الأشخاص المعنوية سواء كانت خاصة أو عامة هي أكثر الأشخاص عرضة لوقوع جرائم معلوماتية عليها، وهذا لكون أن الذمة المالية لهذه الأشخاص تقدر بالملايير بالإضافة إلى سهولة ارتكاب هذا النوع من الإجرام، وخاصة إذا كانت هذه الأشخاص مرتبطة بشبكة معلوماتية سواء كانت محلية، أو شبكة الأنترنت الدولية.

وهذه الجرائم تختلف من شخص إلى آخر فمثلاً: فيما يتعلق بالأشخاص المعنوية الخاصة فنجد أن أكثر الجرائم وقوعاً عليها هي جرائم الجوسسة، حيث يعتمد أصحاب الشركات إلى التجسس على الشركات المنافسة، لمعرفة حجم المبيعات وشخصيات العملاء وغيرها من المعلومات التي قد تساهم في تقليل الفرص على الشركات الأخرى المنافسة في مجال الإنتاج. [39] ص 150

أما جرائم النصب، السرقة، الإحتيال، التحويل الإلكتروني للأموال فتعتبر منتشرة لدى المؤسسات المالية كالبنوك، ولم تسلم المؤسسات العسكرية هي الأخرى من هذا النوع المستحدث من الإجرام، بإعتبار أن المعلومة تشكل قيمة إقتصادية في السوق المالية العالمية كما سبق الإشارة إليه، فقد

أصبحت المعلومة بذلك قوة إقتصادية، وعليه فالدولة التي تمتلك المعلومة هي التي تمتلك القوة، وهذا ما أصبح شائعاً في الوقت الحالي.

تتمثل المعلومات العسكرية محل الاعتداء على أسرار الدولة، في المشروعات العامة والمشروعات النووية والتصنيع الحديث للأسلحة المتطورة، وكل ما يمس الأمن القومي لهذه الدول من جراء تسرب هذه المعلومات. [38] ص 67

تعتمد آليات الحرب على شبكات الحسابات الآلية، في تنقل المعلومات عن طريق الشبكات ومن خلال الأقمار الصناعية، حيث يؤدي ذلك بدوره إلى تعاضد دور القوات المسلحة، ونظم المعلومات في أنظمة التسليح، نظراً لاحتمية وأهمية تخزين البيانات، وسرعة معالجتها، وعرضها بصورة مناسبة أمام القادة لإتخاذ القرار المناسب على أساس أهمية المعلومات.

هذا ما جعل الدول تبادر إلى القيام بالتجسس على الدول الأخرى للحصول منها على المعلومات التي تجعلها قادرة على مواجهتها في أي وقت. [39] ص 152

2-2-1 صعوبة توقيع الجزاء في الجريمة المعلوماتية:

لقد سبق الإشارة إلى أن الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات هي جريمة تقنية وتنشأ في وسط مختلف تماماً عن الوسط الذي ترتكب فيه الجرائم التقليدية . فإن كانت الجريمة التقليدية ترتكب في وسط مادي ملموس، ومثال ذلك أن السرقة تتحقق بسرقة شيء مادي ملموس والإتلاف يكون على أشياء مادية فيظهر للعيان أن هذا الشيء قد أتلّف، فإن الجريمة المعلوماتية إمّا أن تقع على النظام، وإمّا أن يكون النظام المعلوماتي وسيلة لإرتكابها.

معنى ذلك أن الجرائم المعلوماتية لا يمكن إطلاقاً أن تنفصل عن هذه التكنولوجيا الحديثة التي أصبغت عليها صفة التقنية.

ونظراً لأن الوسائل الفنية قاصرة عن حماية هذه النظم المعلوماتية بالوجه الفعال، ممّا أدى إلى زيادة انتشار الجرائم من قبل من يمتلكون دراية، ومعرفة بتقنيات قهر وسائل الحماية الفنية التي تنشأ من قبل المبرمجين، أو من مالكي النظام ممّا أدى هذا إلى ضرورة تدخل المشرع بإصباح الحماية الجنائية عليها، وذلك بتوقيع الجزاء على مرتكبي هذا النوع من الإجرام حتى يحقق المشرع غايته من العقوبة وهو تحقيق الردع العام والخاص.

لكن هذه الحماية التي أقرها المشرع تعترضها مجموعة كبيرة جدا من الصعوبات، وعلى رأسها صعوبة إكتشافها وكذا الصعوبة في إثباتها.

1-2-2-1 صعوبة إكتشاف الجريمة المعلوماتية

إن أبرز الصعوبات التي تواجه المختصين في مكافحة هذا النوع المستجد من الإجرام، وكذا الحد من المخاطر الهائلة والخسائر الجمة التي تنشأ عنها، هو الوسط الذي ترتكب فيه هذه الجريمة.

فالجريمة المعلوماتية ترتكب في بيئة للمعالجة الآلية للمعطيات، وتتحقق في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للمعطيات، ففي مرحلة الإدخال حيث تترجم المعلومات إلى لغة مفهومة من قبل الآلة، يكون من السهل إدخال بيانات جديدة لا علاقة لها بالمعطيات، وفي مرحلة المعالجة يمكن التلاعب في برامج النظام المعلوماتي ويمكن أيضا التلاعب بها في مرحلة إخراج المعلومات، وعلى ذلك تتغير وتتبدل المخرجات [39] ص 85 ، مما يؤدي إلى تحقق الجريمة.

وبما أن الوسط الذي ترتكب فيه هذه الجرائم وسط افتراضي، فإنه من الصعوبة ملاحظة الجريمة فهي غير مرئية للعيان، بعكس الجرائم التقليدية فإذا كان مثلا في الجرائم التقليدية تتحقق جريمة السرقة بنقل حيازة المال المملوك للمجني عليه إلى الجاني، فإنه في الجريمة المعلوماتية تبقى الحيازة لدى المالك بالرغم من أنه قد تم سرقة المعلومات مثلا.

فالجرائم التي تقع على الحاسبات أو بواسطتها في أكثر صورها مستترة خفية، لا يلاحظها المجني عليه غالبا أو يدري حتى بوقوعها، وبالإمكان إخفاء السلوك المكون لها ونتاجها عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها، وهذا ليس عسيرا بحكم توافر المعرفة والخبرة الفنية في مجال الحاسبات غالبا لدى مرتكبها. [51] ص 16

ومن الصعوبات التي تواجه المختصين في ملاحقة مجرمي المعلوماتية ليس في عدم إكتشاف هذا النوع من الإجرام فقط، بل تتعدى هذا إلى أنه قد تكتشف الجريمة المعلوماتية بعد زمن سواء كان قصير أو طويل، ولكن الأفراد المجني عليهم سواء كانوا أشخاص طبيعيين أو معنويين لا يريدون التبليغ على وقوع الجريمة، وقد يلجأون في بعض الأحيان إلى حل المسألة مع الجاني والأمثلة على ذلك كثيرة. [32] ص 11

ويحدث ذلك غالبا بالنسبة للجهات المالية كالمصارف والبنوك ومؤسسات السمسرة، إذ أن مجالس إدارتها في الغالب الأعم تفضل كتمان أمر هذه الجرائم تفاديا للأثار السلبية التي قد تنجم عن كشف هذه

الجرائم، أو اتخاذ الإجراءات القضائية اتجاهها، إذ قد يؤدي ذلك إلى تضائل الثقة فيها من جانب المتعاملين معها. [07] ص 216

وحتى في الفرض الذي يبلغ فيه المجني عليه بأن هناك جريمة معلوماتية قد وقعت على أنظمتها أو في حالة ما إذا إكتشفت الجريمة المعلوماتية بمحظ الصدفة، لأنه غالبا ما تكتشف الجرائم المعلوماتية عن طريق الصدفة البحتة، نظرا لعدم وجود أثر كتابي لما يجري خلال تنفيذها من عمليات، حيث يتم بالنبضات الإلكترونية نقل المعلومات، ولذلك يستطيع الجاني تدمير دليل الإدانة في أقل من ثانية.

في الغالب الأعم يحجم المجني عليهم عن مساعدة السلطات المختصة في إثبات الجريمة والكشف عنها، وحتى في حالة الإبلاغ فإن المجني عليهم لا يتعاونون مع جهات التحقيق خوفا مما يترتب عليه من دعاية مضارة وضياع ثقة المساهمين. [52] ص 160

كما أن هذه الجرائم ترتكب غالبا وبصورة منظمة -كما سبق أن ذكرنا- على صعيد أكثر من دولة باستخدام شبكة الإتصالات، والمعلومات ودون تحمل عناء الانتقال. [03] ص 97

وإنطلاقا من كون الجريمة المعلوماتية جريمة عابرة للحدود، بحيث أنه يمكن أن ترتكب الجريمة في دولة وتتحقق النتيجة في دولة أخرى، ومثال ذلك أن تقع الجريمة في الجزائر لكن أثرها يتعدى الحدود الوطنية للدولة ففي هذه الحالة لا يمكن معها التنبؤ بأن هناك جريمة قد وقعت، وإلى جانب هذه الصعوبات توجد صعوبات أخرى تتعلق بمسألة الإثبات.

2-2-2-1 صعوبة إثبات الجريمة المعلوماتية:

إنّ صعوبة توقيع الجزاء في الجرائم المعلوماتية لا تقف عند حد الصعوبة في إكتشافها فحسب، بل تتعدى ذلك، إلى الصعوبة في إثباتها إن إكتشفت، هذا لأنها جريمة تقنية كما سبق القول.

فالجرائم المعلوماتية لا تحتاج إلى أي عنف، أو سفك للدماء، أو آثار اقتحام لسرقة الأموال، وإنما هي أرقام وبيانات تتغير أو تمحى تماما من السجلات المخزونة في ذاكرة الحاسبات الآلية، ولأن هذه الجرائم في أغلب الأحيان لا تترك أي أثر خارجي مرئي لها فهي صعبة الإثبات. [03] ص 97

ونظرا لأنها جريمة تقنية فالدليل سوف يتغير أيضا إلى دليل تقني، أو ما اصطلح على تسميته بالدليل الرقمي وعليه فصعوبة إثبات الجريمة ترجع إلى مجموعة من الأسباب منها الصعوبة الخاصة بالدليل المعلوماتي، وصعوبة الوصول إلى هذا الدليل بالإضافة إلى مشكلة قبول الدليل أمام الجهة القضائية.

1-2-2-2-1 الصعوبة الخاصة بالدليل في الجريمة المعلوماتية:

فالدليل في الجرائم المعلوماتية ليس دليلاً مرئياً يمكن فهمه بمجرد القراءة، ويتمثل حسب ما تتيحه النظم المعلوماتية من أدلة على الجرائم التي تقع عليها، أو بواسطتها في بيانات غير مرئية لا تفصح عن شخصية معينة، وتظهر هذه المشكلة عادة في جرائم الأنترنت. [07] ص 216

مما يزيد من صعوبة إثبات هذه الجرائم أيضاً هو ارتكابها في الخفاء، وعدم وجود أي أثر كتابي لما يجري خلال تنفيذها من عمليات أو أفعال إجرامية. [03] ص 98

كما قلنا أن المعلومة أو البيان عبارة عن نبضات إلكترونية غير مرئية تنساب عبر أجزاء الحاسب الآلي والشبكة كما تنساب الكهرباء عبر الأسلاك فهي غير مرئية. [53] ص 36

ونظراً لأن الدليل في الجريمة المعلوماتية هو دليل غير مادي وغير مرئي للعيان هذا ما استتبع بالضرورة تحقق صعوبات أخرى منها صعوبة الوصول إلى الدليل.

2-2-2-2-1 صعوبة الوصول إلى الدليل:

بعد أن سلمنا أن الجرائم المعلوماتية تستعصم على الإثبات بالطرق التقليدية، وتستلزم طرقاً خاصة للإثبات تتمثل في الدليل الرقمي، إلا أن هذا الدليل تحيط به مجموعة من المشكلات تمنع جهات التحري والتحقيق من الوصول إليه، ومن أبرز هذه المشكلات هي:

- الطبيعة الخاصة بالدليل: ولقد سلمنا أنه دليل غير مرئي.

- سهولة محو الدليل:

من المشكلات التي تتعلق بالدليل الإلكتروني سهولة محوه من قبل الجاني، حيث يستطيع الجاني أن يمحو الدليل الإلكتروني، إما من خلال إدخال برنامج في الجهاز بإمكانه محو آثار الجريمة أو باستعمال أي وسيلة تقنية أخرى.

فالجاني بإمكانه محو الأدلة التي تدينه أو تدمرها في زمن قصير جداً، وحتى لو تم ضبطه فقد يرجعهذه الجريمة إلى خطأ في نظام الحاسب أو الشبكة أو الأجهزة. [53] ص 46

ومن الأمثلة التي أحبط فيها مسعى الجاني لتدمير الأدلة على إدانته بطريقة آلية متطورة حالة شهدتها النمسا تتلخص وقائعها في قيام أحد مهربي الأسلحة بإدخال تعليمات على الأوامر العادية لنظام

تشغيل حاسب صغير يستخدمه في تخزين عناوين عملائه و المتعاملين معه بحيث يترتب على إدخال أمر إلى الحاسب من خلال لوحة مفاتيحه، بالنسخ أو الطبع محو و تدمير البيانات كلها مع أن تعديل نظام تشغيل الحاسب كان قد أجري خصيصا من قبل الفاعل للحيلولة دون نجاح أجهزة الملاحقة في إجراءاتها المتوقعة للبحث عن الأدلة و ضبطها إلا أنه لم تفلح في تحقيق هذا الهدف نتيجة شعور أو حدس راود المتخصصين في معالجة البيانات بالجهاز المركزي لمكافحة الغش بالنمسا بأن شيئا في نظام تشغيل حاسب الفاعل قد جرى تغييره، و قيامهم بناء على ذلك بإستنساخ الأقراص الممغنطة المضغوطة عن طريق أنظمة حاسبه. [51] ص 23

ليس هذا فقط فالجناة في الجرائم المعلوماتية بإمكانهم فرض تدابير أمنية لمنع التفتيش المتوقع عليهم، بحثا عن أدلة إدانة ضدهم، وذلك كإستخدام كلمة السر حول مواقعهم تمنع الوصول إليها، أو ترميزها، أو تشفيرها لإعاقة الإطلاع على أي دليل يخلفه نشاطهم الإجرامي، الأمر الذي يعيق الرقابة على البيانات المخزنة، أو المنقولة عبر حدود الدولة، سيما أنه وبعد تقدم شبكة الأنترنت الدولية لم تعد الحدود الجغرافية عائقا في الإختراق. [53] ص 48

وعليه فإن من معوقات الوصول إلى الدليل يتمثل في حال أن تكون تلك البيانات التي لها علاقة بالجريمة محل البحث مخزنة خارج الدولة عن طريق شبكة الأنترنت، ففي مثل هذه الحالة فإن البحث عن الأدلة يتعارض مع مبدأ السيادة التي تحرص عليها كل دولة، وبالتالي فلن يتم التوصل إلى الدليل ما لم يوجد تعاون دولي بهذا الخصوص. [06] ص 398

كما أنه قد يتردد عدد كبير من الأشخاص على مسرح الجريمة خلال الفترة الزمنية التي تتوسط إرتكابها واكتشافها، مما يهيئ الفرصة لحدوث تغيير، وإتلاف، أو عبث بالأدلة، أو زوالها كلها أو بعضها وذلك ما يثير الشك في الدليل الإلكتروني المتحصل عليه. [15] ص 365

وقد يكون إتلاف الدليل ليس من قبل الجاني، أو الأشخاص الذين يترددون على مسرح الجريمة وإنما قد يكون من قبل جهات التحقيق في حد ذاتها، وذلك يرجع إما لأن ضابط الشرطة القضائية غير متخصص في هذا المجال، وإما يرجع لعدم الحيطة والحذر في التعامل مع هذه الجرائم لأنها وكما سبق القول تختلف عن الجرائم التقليدية، مما يستدعي بالضرورة التعامل مع الأدلة بحذر شديد لأنها قابلة للزوال والتغير لأي مؤثر سواء كان داخل النظام أو خارجه عند تثبيتها على دعامات.

ومن الصعوبات كذلك بالنسبة لضبط الدليل المعلوماتي في جرائم الكمبيوتر ضخامة البيانات التي يجب فحصها من قبل المحقق الجنائي فالكم الهائل للبيانات التي يجري في الأنظمة المعلوماتية، تداولها

أحد مصادر الصعوبات التي تعوق تحقيق الجرائم التي تقع عليها أو بواسطتها، أي ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات التي لا تثبت كلها تقريبا شيئا على الإطلاق. [51] ص 24

بالإضافة إلى أن تقاعس المجني عليهم في هذه الجرائم خاصة في الأعمال التي تتعلق بعدم الإبلاغ، تحاشيا للأضرار المترتبة عن العلانية التي تتسم بها هذه البلاغات. [23] ص ص 214، 215

3-2-2-1 مشكل الإختصاص القضائي:

باعتبار أن الجريمة المعلوماتية جريمة دولية فهي تقع بكاملها في دولة في واحدة، وقد تقع في عدة دول مما يتزامن معها ظهور العديد من المشكلات الخاصة بتحديد القانون الواجب التطبيق والقضاء المختص بنظر تلك الجرائم، سواء على النطاق الداخلي أو الدولي، هذاباعتبار أن الأنترنت ليس لها مالك ولا تعترف بوجود حدود بين الدول، فالمجرم يمكن له ارتكاب جريمته في بضع ثوان أي في وقت قياسي وقد يصل أثرها ومداهها إلى العديد من الدول فهي تتجاوز المجال الجغرافي الموجودة فيه.

تعتبر مشكلة الإختصاص القضائي للجرائم المعلوماتية بوجه عام ذات أهمية كبيرة في عرقلة الإجراءات الخاصة بأجهزة الضبط القضائي، وكذا جهات التحقيق على المستويين المحلي والدولي.

1-3-2-2-1 مشكلة الإختصاص المحلي:

نعالج في هذه المسألة الإختصاص المكاني لضباط الشرطة القضائية، وكذا مشكلة الإختصاص القضائي الداخلي أو المحلي في الجرائم المعلوماتية والتي تعني تنازع الإختصاص بين أكثر من جهة قضائية داخل إقليم الدولة.

- الإختصاص المكاني لضباط الشرطة القضائية:

إن طبيعة الجريمة المعلوماتية تفرض على المشرع الوطني أن يتعامل معها وفقا لطبيعتها الخاصة والتميزة عن الجرائم التقليدية، ففي الجريمة التقليدية تكون إجراءات ضابط الشرطة القضائية محددة بالإختصاص المكاني الذي يمارس فيه عمله، وأي تجاوز له يكون باطلا.

و لقد تنبه المشرع الجزائري إلى هذه المسألة، وذلك عندما نص على إمتداد إختصاص ضباط الشرطة القضائية إلى كامل الإقليم في عدد من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفقا للمادة 16 من قانون الإجراءات الجزائية. [54]

ف نجد أن المشرع الجزائري وفقا لنص المادة 16 فقرة 06 من قانون الإجراءات وسع من إختصاص ضباط الشرطة القضائية ليصبح إختصاصا وطنيا تبعا لصفة منتمي الضبطية القضائية، بحيث نجد أنه وسع من الإختصاص الإقليمي بالنسبة لضباط الشرطة القضائية من مصالح الأمن العسكري في البحث والتحري عن جميع الجرائم دون إستثناء.

أما المادة 16 فقرة 07 فجاء فيها أن توسيع دائرة ضباط الشرطة القضائية يرجع إلى طبيعة الجريمة من ضمنها الجرائم المعلوماتية ففي هذه الحالات وسع المشرع الوطني من اختصاص ضباط الشرطة القضائية ليشمل كامل الإقليم الوطني.

ويتميز هذا الإختصاص بأنه عام يشمل جميع ضباط الشرطة القضائية وأعاونهم مهما كانت الجهة التي يتبعونها سواء كانت درك وطني أم شرطة أو أمن عسكري أم غيرها من الجهات التي ينص عليها القانون. [06] ص 270

كما يمكن لضباط الشرطة القضائية تمديد عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يعمل على الإشتباه فيهم بإرتكاب الجرائم المشار إليها، وكذلك مراقبة نقل أشياء أو أموال أو متحصلات من إرتكاب هذه الجرائم، أو قد تستعمل في إرتكابها منها الجريمة المعلوماتية بشرط عدم إعتراض وكيل الجمهورية المختص على القيام بذلك الإجراء وفقا للمادة 16 مكرر من قانون الإجراءات الجزائية. [54]

و نشير إلى أن هذا الإجراء كان يقتصر على جرائم الإرهاب والتخريب فقط لكن بموجب التعديل الجديد أصبح يضم جرائم أخرى منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما يمكن تمديد إختصاص ضباط الشرطة القضائية في حالة الإستعجال.

وحالة الإستعجال قيدها بعض الفقهاء بحالة الضرورة التي يخشى إن تركزت تسبب في ضياع الدليل، بينما توسع جانب آخر في مدلولها ليشمل ضرورة البحث والتحري، [55] ص 212 ، وتقسم حالة الإستعجال إلى حالتين:

الحالة الأولى: تكون بدون طلب من السلطة القضائية المختصة وهنا يباشر ضابط الشرطة القضائية مهمته على مستوى دائرة إختصاص المجلس القضائي الملحق به.

أما الحالة الثانية: تكون بطلب من السلطة القضائية ويشترط إخطاره مسبقا لكن المشرع لم يبين ضوابط الإختصاص لذا عليه العودة إلى القواعد العامة في المواد 37 و 40 من قانون الإجراءات الجزائية .

- الإختصاص القضائي الداخلي:

تثار مشكلة الإختصاص القضائي المحلي بالنسبة للجرائم المعلوماتية، في حالة أن تكون الجريمة مرتكبة كلها على إقليم الدولة، بحيث لا يوجد قضاء أو قانون لدولة أخرى ينازع قوانين هذه الدولة، كما تثار في الحالة التي تكون مرتكبة في أكثر من نطاق إختصاص محلي داخل إقليمها.

بهذا الخصوص فقد نصت المادة 37 من قانون الإجراءات الجزائية على مايلي: "يتحدد الإختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، أو بمحل إقامة أحد الأشخاص المتشبه في مساهمتهم فيها، أو بالمكان الذي تم فيه القبض على أحد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر" كما نصت المادة 329 قانون الإجراءات الجزائية "تختص محليا بالنظر في الجنحة محكمة محلا لجريمة، أو محل إقامة أحد المتهمين أو شركاءهم، أو محل القبض عليهم، ولو كان هذا القبض قد وقع لسبب آخر" [56]، فمن خلال النصوص السابقة يتحدد الإختصاص المكاني بـ:

- محل الجريمة: بمعنى أن تكون قد إقترفت بكاملها أو أحد عناصر الركن المادي لها في دائرة الإختصاص المكاني لعضو النيابة أو التحقيق، أو أن تتحقق صورة من صور الإستمرار بالنسبة للجريمة المستمرة، أو أي فعل من أفعال الإعتياد أو التتابع بالنسبة للجريمة المركبة، أو أي عمل من أعمال البدء في التنفيذ بالنسبة للشروع في دائرة الإختصاص المكاني لوكيل الجمهورية أو قاضي التحقيق. [55]ص324

- أن تكون إقامة المتهم أو المشتبه به، أو إقامة أحد المشتبه بهم في دائرة إختصاص عضو النيابة العامة أو قاضي التحقيق.

- أن يكون قد ألقى القبض على أحد المتهمين أو المشتبه بهم في نطاق دائرة إختصاص وكيل الجمهورية أو قاضي التحقيق.

و ينعقد الإختصاص وفقا لمعيار من المعايير المشار إليها بحسب السبق للمحكمة التي دخلت الدعوى الجزائية في حوزتها قبل غيرها، فإذا نظرت القضية محكمة محل إقامة المتهم فإنها بالتالي تكون هي المختصة دون غيرها، ويكون من حقها تمديد إختصاصها بشأن إتخاذ أي إجراء من إجراءات المحاكمة بشرط أن يكون ذلك التمديد بموجب نص قانوني. [06] ص 377

و لقد مدد المشرع الجزائري الإختصاص القضائي بالنسبة لعدد من الجرائم منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات وفق للمادة 2/37 و 4/47 و 3/329 من قانون الإجراءات الجزائية. [54]

إن المشرع الجزائري لم يقتصر على تمديد الإختصاص القضائي بمفهومه المادي التقليدي بل ذهب إلى أبعد من ذلك حين أجاز بموجب المادة 05 من القانون 04/09 تمديد الإختصاص القضائي والقيام ببعض الإجراءات عن بعد حيث جاء فيها أنه "إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منضومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها إنطلاقاً من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أجزء منها بعد إعلام السلطة القضائية المختصة مسبقاً بذلك". [11]

2-3-2-2-1 مشكل الإختصاص الدولي:

سوف نعالج هذه المسألة من خلال التطرق إلى إختصاص الضبطية القضائية ثم نتناول مشكل الإختصاص القضائي الدولي.

- مشكل الإختصاص المكاني لضباط الشرطة القضائية :

على الرغم مما أشرنا إليه سابقاً من أن المشرع الجزائري قد عالج مشكل إختصاص الضبطية القضائية، وذلك بتمديد إختصاصها سواء إلى دائرة إختصاص المجلس القضائي الذي تباشر مهامها في نطاق إختصاصه أو تمديد إختصاصها إلى كامل التراب الوطني لتواجه بذلك السرعة التي تتميز بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات .

إلا أن المشرع الجزائري لم يعالج مسألة الإختصاص الدولي لضباط الشرطة القضائية الذي لا يمكن أن يحل إلا عن طريق دخول الجزائر في عدة إتفاقات سواء كانت عربية أو أجنبية، والنص في هذه الإتفاقيات على تمديد إختصاص جهات الضبطية القضائية لأنه حتى وإن كان لا يضره للعيان بأن ضابط الشرطة القضائية قد إنتقل إلى حدود دولة أخرى، بمعنى لم يكن هناك إنتقال مادي مرئي وإنما إنتقال رقمي إن صح القول، إلا أن هذا الإنتقال هو الآخر فيه إعتداء على سيادة الدولة التي تم الإنتقال اللامادي (الرقمي) إلى النظام الموجود فيها.

و نشير فقط إلى أنه لا يمكن معالجة مشكلة تجاوز الإختصاص المكاني بشكل كلي عن طريق التعاون الدولي بسبب أن ما يعد جريمة في دولة معينة قد لا يعد كذلك في دولة أخرى، بالإضافة إلى تجريم بعض الدول لتلك الجرائم بنصوص جديدة بينما لا تزال دول تحاول تطبيق النصوص التقليدية مع أن ذلك يتصادم مع مبدأ الشرعية أحياناً، وإختلاف النصوص بين الدول يعد عائقاً في مجال التعاون الدولي.

أضف إلى ذلك أن الدول المهيمنة في مجال التكنولوجيا الرقمية تحاول السيطرة الكاملة في مجال ملاحقة وضبط تلك الجرائم، لإمتلاكها كل ما يخدم الجوانب التقنية في كشف تلك الجرائم بحيث تقوم باتخاذ الإجراءات دون مراعاة لتجاوز إختصاص ودون إنتظار موافقة الآخرين على قيامها بتلك الإجراءات في نطاق إختصاصهم. [06] ص 267

- مشكل الإختصاص القضائي الدولي:

باعتبار أن الجريمة المعلوماتية جريمة دولية فهي قد تقع بكاملها في دولة واحدة وقد تقع في عدة دول، وفي هذه الحالة يكون الإختصاص دولياً، وتتحقق في حالة الشبكات المفتوحة كالإنترنت.

و بعيدا على أن تكون إنترنت بدون قوانين تنظمها: "no-law-land" فجميع قوانين دول العالم قابلة للتطبيق على شبكة الأنترنت، وهو مكنم الصعوبة في هذه المسألة، لأن الحدود في هذه الجريمة ألغيت مما يسدعي تدخل القانون الجنائي الدولي البارحة كان إستثنائياً واليوم أضحى ذي تطبيق يخص العديد من الدول وليس كالسابق وكل سلوك إجرامي وارد في الشبكة يضع إشكالا كبيرا في التكيف لدى القانون الداخلي وتنازع القوانين. [17] ص 37

وبما أن الجريمة المعلوماتية هي جريمة عابرة للحدود فهي تثير مسألة الإختصاص القضائي الدولي، فمثلا لو قام جزائري بإرتكاب جريمة في تونس وألحق الضرر بدولة ثالثة هي فرنسا مثلا فهنا تخضع الجريمة للإختصاص الجنائي وفقا لتونس إستنادا إلى مبدأ الإقليمية وكذلك تخضع للإختصاص الجزائري وفقا لمبدأ الشخصية لأنه يحمل الجنسية الجزائرية وبما أن الضرر ألحق بفرنسا فتخضع الجريمة لإختصاصها وفقا لمبدأ العينية لأن الجريمة هددت أمن وسلامة فرنسا، وستتناول كل إختصاص على حدة.

• الإختصاص القائم على أساس مبدأ الإقليمية

وفقا لهذا المبدأ فإن المحاكم الجزائرية الجزائرية هي المختصة بنظر الجرائم التي تقع كلها أو جزء منها على إقليمها أيا كان شخص المتهم، أو صفته وبغض النظر عن جنسيته وهذا ما جاء في نص المادة 03 من قانون العقوبات الجزائري. [57]

ووفقا لنص المادة 586 من قانون الإجراءات الجزائرية تكون مرتكبة في الإقليم الجزائري، كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر.

وفي هذا الصدد يكفي أن يرتكب فعلا من الأفعال المكونة للجريمة في الجزائر ينعقد الإختصاص للمحاكم الجزائرية، ونشير إلى أنه يوجد تضامن بين الإختصاص القضائي والتشريع الجزائري سواء كان مبررا أو غير مبرر وعليه فإختصاص القانون الجزائري الجزائري يؤدي آليا لإختصاص قضاء المحاكم الجزائرية [58] ص ص 77،78 ، وعليه تعتبر الجريمة المعلوماتية وفقا لقاعدة إقليمية القوانين من إختصاص المحاكم الجزائرية في حالة:

- وقوع الجريمة المعلوماتية بكامل أركانها في الجزائر وهنا لا إشكال ومثالها أن تتلف معلومات داخل أنظمة معالجة آلية للمعطيات موجودة في الجزائر أي تمت كامل أركان الجريمة في الجزائر.

- وقوع أحد عناصر الركن المادي في الجزائر: بمعنى إما أن يكون الفعل في الجزائر أو أن تتحقق النتيجة في الجزائر ومثالها أن يتم إختراق مؤسسة مالية من الجزائر وتحويل أموالها مع العلم أن المؤسسة المالية خارج الحدود الجزائرية لكن فعل الإختراق وقع في الجزائر.

- وقوع فعل من أفعال الجريمة غير متجزئة في الجزائر: ويدخل تحت هذا الوضع الجريمة المستمرة والجريمة المتتابة وجريمة الإعتياد والجريمة المركبة، ففي هذه الحالة يكفي أن يتحقق في الجزائر حالة من حالات الإستمرار أو فعل من أفعال المتابعة أو الإعتياد أو جزء من الجريمة المركبة من تطبيق القانون الجزائري على الجريمة بأكملها. [17] ص 40

- وقوع فعل الإشتراك بالجزائر: يستخلص من نص المادة 585 من قانون الإجراءات الجزائية أنّ قانون العقوبات الجزائري يطبق على كل من كان في إقليم الجمهورية شريكا في جناية أو جنحة مرتكبة في الخارج وتطبيق هذا الحكم يتوقف على شرطين هما:

- أن يكون الفعل معاقب عليه في الجزائر وفي البلد الذي ارتكب فيه (قاعدة ثنائية التجريم).

- أن تكون الواقعة الموصوفة بأنها جنائية أو جنحة قد ثبت إرتكابها بقرار نهائي من الجهة القضائية الأجنبية. [56]

- وقوع النتيجة في الجزائر وتوقع حصولها فيها: بمعنى أن النتيجة في الجزائر، أما عن النتيجة المتوقع حصولها مثالها وجهة الإعتداء تكون الشبكة الإعلامية الجزائرية، أو حواسيب بالجزائر أثناء تنفيذ سير المعلومات يحدد عن مساره، وهو حال الجريمة الخائبة أو الجريمة المستحيلة المعاقب عليها في التشريع الجزائري. [17] ص 41

• الإختصاص القائم على أساس مبدأ الشخصية:

يقصد بالإختصاص الشخصي صلاحية المحاكم بتطبيق التشريع الجزائري على كل جزائري فاعل كان أو محرض أو شريك، أقدم خارج الإقليم الجزائري على ارتكاب جناية أو جنحة خارج الإقليم الجزائري.

و جرائم المساس بأنظمة المعالجة الآلية للمعطيات هي عبارة عن جنح وبالتالي في حالة ما إذا ارتكب جزائري جنحة من جنح الإعتداء على المساس بأنظمة المعالجة الآلية للمعطيات خارج الإقليم الجزائري يطبق عليه القانون الجزائري، كمن يقوم بالتلاعب ببيانات شخصية لأشخاص خارج الإقليم الجزائري ويعد الإختصاص الشخصي إستثناء على مبدأ الإقليمية وهو ما نصت عليه المادتين 582 و583 من قانون الإجراءات الجزائية الجزائري. [56]، ووفقا لنص المواد يجب تحقق شروط وهي:

- يجب أن تكون الواقعة المرتكبة جنحية أو جنحة في نظر القانون الجزائري وأن تكون الواقعة تشكل جنحية أو جنحة أيضا في نظر تشريع الدولة التي ارتكبت فيها.

- يجب أن يكون المتهم جزائريا وقت ارتكاب الجريمة.

- يجب أن يعود المتهم إلى الجزائر.

- يجب أن تكون الجريمة موصوفة جنحة وكانت قد ارتكبت ضد أحد الأفراد فيجب وفقا لنص المادة 583 قانون الإجراءات الجزائية قرن الإختصاص وولاية النظر فيها بوجود تقديم شكوى من الطرف المضرور، أو بلاغ من سلطات البلد الذي ارتكبت فيه تلك الجريمة.

و تشير إلى أن المشرع الجزائري أخذ بمبدأ الإختصاص الشخصي الإيجابي أي عندما يكون الجاني جزائريا ولم يأخذ بمبدأ الإختصاص الشخصي السلبي إلا في نص المادة 391-2 " بالنسبة للجنايات والجنح المرتكبة ضد جزائريين على متن طائرات أجنبية " و بذلك المشرع الجزائري لم يوافق التشريع الفرنسي الذي يأخذ بمبدأ الإختصاص الشخصي بجانبه الإيجابي والسلبي وفقا لنص المادة 6-113 و7-113 من قانون العقوبات الفرنسي. [59]

• الإختصاص القائم على أساس مبدأ العينة :

وفقا لهذا المبدأ فإن التشريع الجنائي يطبق على الجرائم التي ترتكب في الخارج بغض النظر عن جنسية مرتكبها ولكن على أساس نوع الجريمة بمعنى تختص الدولة بنوع معين من الجرائم التي تمس أمنها ومصالحها.

و قد نص القانون الجزائري عليه في المادة 566 والتي جاء فيها " كل أجنبي إرتكب خارج الإقليم الجزائري بصفة فاعل أصلي أو شريك جناية أو جنحة ضد سلامة الدولة الجزائرية، أو تزييف للنقود أو أوراق مصرفية وطنية متداولة قانونا بالجزائر، تجوز متابعته ومحاكمته وفقا للقانون الجزائري، إذا ألقى القبض عليه في الجزائر أو حصلت الحكومة على تسليمه لها"

كذلك نجد أن المشرع الجزائري نص على مبدأ العينية وفقا لنص المادة 15 من القانون 04/09 والتي جاء فيها " زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني. [11]

و هذا المبدأ صعب التطبيق وذلك لإعتبارات منها:

- الدولة تلقى عناء في الفصل في الدعاوى التي تنشأ عن الجرائم التي تقع على إقليمها فليس في طاقتها إلا إذا كانت من عظام الدول أن تتكبد العناء لملاحقة المجرمين.
- أن مبدأ العالمية يتطلب معرفة القاضي لكافة القوانين وهو أمر صعب التحقيق. [17] ص 43 و عليه توجد العديد من المشكلات التي تتعلق بالإختصاص القضائي العيني منها:
- تعارض الإختصاص وفقا لمبدأ العينية مع الإختصاص وفقا لمبدأ الإقليمية في حالة أن تكون الجريمة المرتكبة وفقا لمبدأ العينية مجرمة في قانون الدولة الأخرى التي أقرت فيها.
- في حالة ما إذا وقع السلوك في بلد ووقعت النتيجة في بلد آخر فإن كل من محاكم مكان النشاط الإجرامي ومكان النتيجة تكون مختصة بنظر الجريمة.
- إن إختصاص القضاء بنظر جرائم الكمبيوتر والقانون المتعين تطبيقه على الفعل لا يحضى دائما بالوضوح أو القبول أمام حقيقة أن غالبية الأفعال ترتكب من قبل أشخاص من خارج الحدود
- كذلك تتعلق بإمتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود وما يحتاجه ذلك إلى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية. [06] ص 393
- وعليه فإن مشكلة الإختصاص القضائي بصفة عامة قد أضحت معقدة في ظل عدم وجود إتفاق دولي ينظم هذه المسألة، وذلك في ظل ما تتمتع به شبكة المعلوماتية من فقدان السيطرة أو الرقابة عليها وهو ما يساهم في إثارة إشكاليات الإختصاص القضائي خاصة في الجوانب المتعلقة بالتفتيش والضبط.

3-1 المشكلات العملية بشأن الحماية الإجرائية من الجرائم المعلوماتية:

إن الثورة الجديدة أدت إلى تشويش قانون العقوبات، وكذا قانون الإجراءات الجزائية، وخاصة إذا تعلق الأمر بالشبكات المعلوماتية لأنها تساهم في تطور الإجرام المعلوماتي.

وفي هذا الصدد لا يكفي أن يكون قانون العقوبات فقط متماشيا مع هذه الجرائم الجديدة، بل يجب أن يشمل التطور أيضا قانون الإجراءات الجزائية، لأن هناك مجموعة كبيرة من المشكلات التي تواجهه وهي مثلا: صعوبة تحديد فاعل الجريمة، إمكانية تعديل وتغيير المعطيات في أي وقت، سهولة إخفاء آثار الجريمة (الدليل المعلوماتي)، لذلك فالسرعة والسرية تعدان في غالب الأحيان من العناصر الجوهرية في نجاح التنقيب والتحري.

ولقد تبنى المشرع الجزائري وسائل إجرائية تقليدية منها التنقيش، والضبط، وأخرى جديدة تتلاءم مع طبيعة هذه الجرائم وهي الحفظ، ولذلك سوف نتناول الإجراءات التي يمكن أن تساعد في كشف وإثبات الجريمة.

1-3-1التفتيش:

يعتبر التفتيش إجراء من إجراءات التحقيق بمقتضاه يتمكن قاضي التحقيق، أو ضابط الشرطة القضائية المنوب عنه البحث عن الأدلة المادية لجريمة تحققت، ولقد نص المشرع الجزائري على التفتيش وفقا لنص المادة 81 من قانون الإجراءات الجزائية وما بعدها.

1-3-1-1 مفهوم التفتيش:

التفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية، فيقصد به إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للمعطيات بما يشمل من مدخلات، وتخزين، ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جنائية، أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها. [32] ص 19

لكن توجد بعض الصعوبات الإجرائية التي تعيق خضوع البيانات المخزنة آليا لقواعد التفتيش التقليدية والتي منها تعدد الأماكن التي يوجد بها النظام المعلوماتي داخل وخارج الدولة، كذلك صعوبة تحديد الأشياء التي يهدف إلى ضبطها من عملية التنقيش، بالإضافة إلى عدم اكتمال المعرفة والتقنية لتنفيذ عملية التفتيش كما ينبغي.

1-1-1-3-1 شروط وضمانات التفتيش:

باعتبار أن التفتيش يتضمن تقييدا للحرية الفردية، ويمثل إعتداء على حرمة الحياة الخاصة فيجب أن يحاط بسياس من الضمانات القانونية اللازمة لصحته، وهي تنقسم إلى ضمانات شكلية وضمانات موضوعية، فالسؤال الذي يتبادر في مجال التحقيق في الجرائم المعلوماتية هو هل تفي هذه الضمانات بتفتيش نظم الحاسوب أم أنها لا تتناسب معها؟، والظاهر للعيان أن هذه الضمانات يمكن أن تعرقل سلطة التحقيق في القيام بمهمتها.

- الشروط الموضوعية:

تتمثل في ضرورة وقوع جريمة ونسبة إرتكابها إلى متهم، إضافة إلى ضرورة أن ينصب التفتيش على محل، وأخيرا حتى يكون التفتيش صحيحا لا بد أن لا يكون غاية في حد ذاته وإنما يجب أن يكون وسيلة لتحقيق غاية تتمثل في العثور على أشياء يمكن أن تفيد في اكتشاف الجريمة.

• سبب التفتيش:

بمعنى أنه حتى يكون التفتيش صحيحا يجب أن يتحقق سببه، وهو وقوع جريمة يتم بموجبها توجيه الإتهام إلى شخص، أو الأشخاص المراد تفتيشهم، وبالتالي لا يجوز التفتيش من أجل فعل لا يعد جريمة، وأنه لا توجد هناك دلائل كافية ينسبها إلى شخص أو مجموعة أشخاص.

وبما أن المشرع الجزائري نص على جرائم المساس بأنظمة المعالجة الآلية للمعطيات وفقا لقانون العقوبات، ونص على الجرائم التي يمكن أن ترتكب بواسطة أنظمة المعلوماتية في المادة 2/ب" من القانون 04/09، فوقوع الجريمة لا يثير إشكال لوجود النصوص القانونية المعاقبة على هذه الجرائم لكن تطلب المشرع توافر أمارات قوية على وجود أشياء تفيد في إكتشاف الجريمة هو ما يخلق إشكالية كبيرة، لأن التوصل إلى قرائن أو أمارات قوية كسبب لقيام التفتيش غالبا ما تسبقها جديّة، والتحريات وفي المجال المعلوماتي تلاقي صعوبات جمة وفقا لما تم الإشارة إليها، ومنها نقص الخبرة لدى سلطة التحريات في مجال التحري في نظم المعلوماتية مقابل ما تتسم به تلك الأدلة من طبيعة معنوية يمكن إخفاؤها ومحوها وتغييرها... [06] ص 318

• محل التفتيش:

يعتبر المحل شرط لصحة التفتيش ومحل التفتيش قد يكون منزلا، وقد يكون شخصا وقد يكون رسائل...، وقد نص المشرع الجزائري على تلك الأحكام بنص المادة 79 من قانون الإجراءات الجزائية.

"يجوز لقاضي التحقيق الإنتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة، أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته".

ونصت المادة 83 قانون الإجراءات الجزائية " إذا حصل التفتيش في مسكن المتهم فعلى قاضي التحقيق أن يلتزم بأحكام المواد 45 إلى 47.

أما ما تعلق بتفتيش الأشخاص فنجد المشرع الجزائري قد نص عليه وفقا للمادة رقم 42 من قانون الجمارك، حيث أجاز لأعوان الجمارك أن يقوموا بتفتيش الأشخاص في حالة الظن بأن الشخص يخفي بنية الغش بضائع، ووسائل الدفع عند اجتياز الحدود إلا أن ذلك لا يمنع من العمل بالقواعد العامة بهذا الشأن وهي قواعد تقوم على وجوب إحترام حقوق الأفراد بعدم التعرض لها، إلا في الحدود التي تقتضيها المصلحة العامة. [55] ص 264

كما يجوز تفتيش الشخص كإجراء قضائي في حالتين: الأولى في حالة إلقاء القبض على المشتبه به، فجواز القبض على الشخص يجيز تفتيشه، لأن إجراء القبض يعد أشد على حريات الأفراد من إجراء التفتيش، والحالة الثانية: تفتيش الشخص كإجراء مكمل لتفتيش المسكن في حالة وجود دلائل تفيد في إخفاء المتواجدين في المنزل ما يفيد في كشف الحقيقة.

أما ما يتعلق بالجرائم المعلوماتية فيجب التمييز بين ما يقع على المكونات المادية وما يقع منها على المكونات المعنوية، ففيما يتعلق بالمكونات المادية لا إشكال يطرح بما أنها عبارة عن أشياء مادية ملموسة، لكن الشرط الوحيد هو أن تذكر في إذن التفتيش، أما ما يتعلق بالأشياء المعنوية للحاسوب فيمكن القول أن المشرع الجزائري، وبموجب القانون 04/09 المتعلق بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، قد عمل على استحداث نصوص قانونية يمكن من خلالها السماح للسلطات المختصة بتفتيش الأنظمة المعلوماتية أو جزء منها، أو المعطيات المخزنة بتلك النظم، وكذلك تفتيش أي منظومة تخزين معلوماتية حيث جعلها محلا للتفتيش المعلوماتي.

ووسع من ذلك المحل ليشمل التفتيش عن بعد داخل النطاق الإقليمي للدولة إلى منظومة معلوماتية أخرى خارج الدولة، لكن يمكن الدخول إليها من هذه المنظومة إذا كانت هناك أسبابا تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة بالمنظومة الأخرى.

كما جعل من صلاحيات سلطة التفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل التفتيش، أو لديه علم بالتدابير المتخذة لحماية المعطيات التي تتضمنها المنظومة، لمساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمة التفتيش وفقا لنص المادة 8 من القانون 04/09. [11]

ويشترط في محل التفتيش أن يكون معيناً، ومحدداً بالإضافة إلى أن يكون المحل مما يجوز تفتيشه
أعلى هذا الأساس يستثنى أجهزة الحواسيب التابعة للدبلوماسيين وأعضاء المجالس النيابية [60]
وكذلك يمنع تفتيش الحواسيب التابعة لمكاتب المحامين وعملائه. [54]

• الغاية من التفتيش:

تضمن المشرع الجزائري الغاية من التفتيش بنص عام وفقاً للمادة 81 ق إ ج حيث جاء فيها
"يأشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيداً لإظهار الحقيقة"
ولقد تضمن النص على الغرض من التفتيش في الجرائم المعلوماتية بنص المادة 05 من القانون 04/09
حيث جاء فيها: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون
الإجراءات الجزائية، وفي الحالات المنصوص عليها في المادة 04 أعلاه، الدخول بغرض التفتيش ولو
عن بعد إلى: منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، منظومة تخزين
معلوماتية.

وعليه إذا ما تحققت الغاية من التفتيش، وفقاً للقواعد العامة في قانون الإجراءات الجزائية، فيحق
للسلطات المختصة بالتحقيق، الدخول إلى النظام المعلوماتي أو جزء منه الدخول إلى نظام معلوماتي آخر
داخل الدولة بغرض التفتيش على المعطيات المخزنة به، وذلك إذا توافرت أسباب تدعو إلى الاعتقاد بأن
المعطيات التي تدل على ارتكاب الجريمة مخزنة بالنظام محل التفتيش.

- الشروط الشكلية:

حدد المشرع الجزائري الشروط التي يتم التقيد بها من قبل قاضي التحقيق، أو من ينوبه حتى لا
يشكل التفتيش مساساً بالحريات والحقوق العامة، وعلى هذا الأساس سوف نحاول دراسة هذه الشروط .

فهل تعد هذه الشروط ضماناً للحقوق والحريات بالنسبة للتفتيش في الجرائم المعلوماتية، أم أنها
تعيق الأشخاص المخول لهم التفتيش للقيام بمهامهم؟

• تحديد أوقات التفتيش:

لقد حدد المشرع الجزائري الوقت المسموح به لتفتيش المنازل من قبل السلطة المختصة من
الساعة " الخامسة صباحاً وحتى الثامنة مساءً " حيث جاء في نص المادة 47 فقرة 1 "لا يجوز البدء
في تفتيش المساكن قبل الخامسة صباحاً ولا بعد الساعة الثامنة مساءً إلا إذا طلب صاحب المنزل ذلك
ووجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة بالقانون".

وهذا الشرط لم يأخذ به على إطلاقه، إنما خضع لبعض الإستثناءات ومن هذه الاستثناءات ما جاءت به المادة 47 ق إ ج وهي إذا طلب صاحب المنزل ذلك، أو وجهت نداءات من الداخل كذلك في حالة التحقيق في جميع الجرائم المعاقب عليها في المواد 342 إلى 348 من قانون العقوبات وذلك في داخل كل فندق، أو منزل مفروش، أو فندق عائلي...

وفي المادة 47 فقرة 3 نص المشرع الجزائي على إستثناء جرائم المساس بأنظمة المعالجة الآلية للمعطيات من ميعاد التفتيش كونها جرائم خطيرة، حيث جاء في المادة 47 فقرة 03 "وعندما يتعلق الأمر بجرائم المخدرات، والجريمة المنظمة عبر الحدود الوطنية، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب، وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني وغير سكني في كل ساعة من ساعات النهار والليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص".

ووفقا للمادة 47 فقرة 04 نصت على أنه: " عندما يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أوحجز ليلا أو نهارا، وفي أي مكان على امتداد التراب الوطني، أو أن يأمر ضباط الشرطة القضائية المختصين للقيام بذلك".

ونلاحظ من خلال المواد السابقة الذكر أن المشرع الجزائي أقر بخطورة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فقد أقر التفتيش في أي وقت ليلا أو نهارا ولم يخضعها إلى مواعيد محددة وبالإضافة إلى هذا فقد أكلها إما إلى قاضي التحقيق أو ضابط الشرطة القضائية بأمر من قاضي التحقيق.

وما يلاحظ وفقا لنص المادة 05 من القانون 04/09 أنه بالرغم من أن المشرع الجزائي، قد مدد من التفتيش سواء إلى منظومة يمكن الدخول إليها من المنظومة الأولى، أنه يمكن تفتيش حتى منظومة خارج إقليم الدولة مع الحصول على مساعدة السلطات الأجنبية، وتطبيق مبدأ المعاملة بالمثل إلا أنه لم ينص على عدم خضوعها للمواعيد المحددة طبقا للمادة 47 من قانون الإجراءات الجزائية.

وبالتالي تصبح جرائم المساس بأنظمة المعالجة الآلية للمعطيات مستثناة من تطبيق المواعيد عليها وفقا لنص المادة 47 فقرة "03"، أما الجرائم التي ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية تخضع للمواعيد، فكان على المشرع الجزائي أن يستبعد هذه الجرائم من مبدأ التقيد بالمواعيد اللازمة للتفتيش لأن ذلك سوف يساهم في ضياع الدليل.

• الأشخاص المطلوب حضورهم:

جاء في نص المادة 45 فقرة "01" من ق.إ.ج تتم عملية التفتيش التي تجري طبقا للمادة 44 أعلاه على الوجه التالي: إذا وقع التفتيش في مسكن شخص يشتبه في أنه يساهم في ارتكاب الجريمة، فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور شاهدين من غير الموظفين الخاضعين لسلطته.

والفقرة الثانية تنص على أنه إذا أجرى التفتيش في منزل آخر يشتبه بأنه يحوز أوراقا، أو أشياء لها علاقة بالأفعال الإجرامية، فإنه يتعين حضوره وقت إجراء التفتيش وإن تعذر ذلك اتبع الإجراء المنصوص عليه في الفقرة السابقة.

وبالرغم من أهمية مثل هذه الضمانات التي تهدف إلى الاطمئنان على سلامة الإجراء وعدم التعسف في استخدامها، إلا أنها قد تتحول إلى مشكلات تحول دون الوصول إلى النتائج المتوقعة من إجراء التفتيش في حالة أن يكون التفتيش يخص إحدى جرائم المعلوماتية، بسبب أن إشعار المطلوب حضورهم للتفتيش قد يتيح لهم التلاعب بالمعطيات، والبرامج المراد تفتيشها وبالتالي إخفاء أدلة الجرائم أو التلاعب بها، ومن ثم صعوبة التوصل إلى مرتكبيها فقد يتم التلاعب بالأدلة وإخفاءها عن بعد في الوقت مابين إجراءات إصدار الإذن بالتفتيش وموافقة المتهم بأن يتم التفتيش بحضوره. [06] ص 336

ولقد كان المشرع الجزائري موقفا جدا حين استبعد جرائم المساس بأنظمة المعالجة الآلية للمعطيات من هذا الأجراء، وفقا لنص المادة 45 فقرة 02 والتي جاء فيها: " لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات، والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال، والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف باستثناء الأحكام المتعلقة بالحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات أعلاه".

وما زال القصور يعتري التشريع الجزائري لأنه لم ينص على هذا الاستثناء بالنسبة للجرائم التي ترتكب، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية، والتي تدخل في صميم الجرائم المنصوص عليها بالقانون 04/09 المتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

• محضر التفتيش:

لقد إشتراط المشرع الجزائري تحرير محضر بالأعمال التي يقوم بها قاضي التحقيق، أو ضابط الشرطة القضائية المنتدب أثناء عملية التفتيش، وجاء هذا وفقا لنص المادة 68 من قانون الإجراءات الجزائية " يقوم قاضي التحقيق وفقا للقانون بإتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة، بالتحري عن أداة الاتهام، وأدلة النفي، وتحرر نسخة عن هذه الإجراءات، وكذلك عن جميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة المنتدب على كل نسخة بمطابقتها للأصل وذلك مع مراعاة ما أشير إليه في الفقرة الخامسة من هذه المادة".

وجاء في المادة 68 فقرة 05 " وإذا كان من المتعذر على قاضي التحقيق أن يقوم بنفسه بجميع إجراءات التحقيق جاز له أن يندب ضابط الشرطة القضائية للقيام بتنفيذ جميع أعمال التحقيق اللازمة ضمن الشروط المنصوص عليها في المواد 138 إلى 142 ".

وهذا الإجراء ليس من النظام العام وعلى هذا الأساس لا يحكم بالبطلان المطلق في حالة مخالفته.

ومحضر التفتيش في مجال الجرائم المعلوماتية إذ يشترط فيه أن يكون مكتوبا من قبل الكاتب الذي يجب اصطحابه مع المحقق، دون إلزامه بالإلمام بالجانب التقني الذي يشكل مشكلة قد تعيق عملية التفتيش.

حيث أن محضر التفتيش بالنسبة للجرائم التقليدية يختلف عن محضر التفتيش بالنسبة للجرائم المعلوماتية، فبالإضافة إلى ما يتطلبه المحضر بالنسبة للجرائم التقليدية من تدوين ما تم من إجراءات وما أسفر عنه التفتيش من أدلة، على أن يكون مكتوبا باللغة الرسمية، وأن يحمل تاريخ تحريره، وتوقيع محرره والاستعانة بكاتب في كل الإجراءات التي تستلزم تحرير محضر فإنه في الجرائم المعلوماتية فضلا عما ذكر لابد من إحاطة قاضي التحقيق أو عضو النيابة بتقنية المعلومات، ثم لابد أن يرافقه شخص متخصص في مجال الحاسب الآلي للاستعانة به في مجال الخبرة الفنية الضرورية، وكذلك المساعدة في صياغة مسودة المحضر بحيث تتم تغطية كل الجوانب الفنية. [06] ص 339

• عدم فض الأوراق المختومة والاطلاع عليها:

لقد جاء وفقا لنص المادة 84 من قانون الإجراءات الجزائية " إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات فإن لقاضي التحقيق، أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الاطلاع عليها قبل ضبطها، مع مراعاة ما تقتضيه ضرورات التحقيق وما توجبه الفقرة الثالثة من المادة 83.

ويجب على الفور إحصاء الأشياء، والوثائق المضبوطة ووضعها في أحرار مختومة.

لا يجوز فتح هذه الأحرار، والوثائق إلا بحضور المتهم مصحوبا بمحاميه، أو بعد استدعاءهما قانونا كما يستدعى أيضا كل من لديه هذه الأشياء لحضور هذا الإجراء...". [57]

يتضح من خلال المادة سالفه الذكر أن المشرع الجزائري قد تضمن حماية قانونية للمستندات المغلقة أثناء التفتيش وهي عدم فضها، أو الاطلاع عليها إلا إذا كان هذا الاطلاع من المحقق الذي هو قاضي التحقيق أو من يندبه وكذلك إحصاء الأشياء أو الوثائق ووضعها في أحرار مختومة.

هذا ما يتعلق بالجرائم التقليدية أما إذا تعلق الأمر بالجرائم المعلوماتية، فهل يمكن تطبيق هذا الإجراء على الجرائم المعلوماتية؟ أو بمعنى آخر هل يكون بالإمكان تطبيق النصوص التقليدية الخاصة بالأوراق المغلقة على البيانات المشفرة الموجودة في النظام المعلوماتي؟.

هناك جانب من الفقه من يرى سريان هذا القيد على ضبط محتوى أنظمة المعالجة الآلية للمعطيات [15] ص 347، لأنه مثلما يضيف الغلق أو التغليف على الأوراق مزيدا من السرية، فكذلك التشفير يضيف سرية بالنسبة للبيانات المعالجة آليا وكذلك على برامج الحاسوب.

لكن هناك رأي آخر يرى انه في الحالة التي لا يمكن الاطلاع فيها على البيانات المشفرة فهي تسمح للمتهم، أو الشخص المراد تفتيش أنظمتها، أو نظامه المعلوماتي بإخفاء تلك المعلومات أو البرامج أو التلاعب بها، مما يتيح أمامه إخفاء أدلة الجريمة، وعلى وجه الخصوص إذا كان القائم بالتفتيش ليس لديه الإلمام الكافي لاتخاذ الإجراءات الفنية أو التقنية المطلوبة لحفظ تلك البرامج، والبيانات وتجميدها من يتم النظر بشأن مدى علاقتها بالجريمة محل التفتيش، ومن ثم القيام بالإجراءات التي تخول فضها والاطلاع عليها. [06] ص 341

ونعتقد أن هذا الرأي هو الذي يجانب الصواب لأن هذه التقنية الجديدة التي ترتكب بها الجرائم المعلوماتية، قد غيرت الكثير من المفاهيم التي كانت سائدة في القوانين التقليدية.

2-1-3-1 مدى قابلية مكونات الحاسوب والشبكة للتفتيش:

لقد سبق لنا تحديد العناصر التي يتكون منها نظام المعالجة الآلية للمعطيات عند تناولنا لمفهوم نظام المعالجة الآلية للمعطيات وقلنا بأنه يتكون من عناصر مادية ملموسة مثل الطابعة، الشاشة، الفأرة... ومن عناصر معنوية وهي تتمثل في البرامج، والبيانات...

فبعد الحديث عن مدى قابلية مكونات الحاسوب والشبكة للتفتيش يقودنا إلى دراسة كل عنصر على حدة.

1-2-1-3-1 مدى خضوع المكونات المادية للحاسب الآلي للتفتيش:

الواقع أن ولوج المكونات المادية للحاسب الآلي بأوعيتها المختلفة بحثاً عن شيء يتصل بجريمة معلوماتية قد وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبيها لا توجد هناك مشكلات تعيق القيام به، مثلها مثل أي مكونات مادية أخرى يتم تفتيشها بالطرق التقليدية، مع الأخذ بعين الاعتبار أن حكم تفتيش الأجهزة يتوقف على طبيعة المكان الموجود فيه، سواء كان مكان عام أو مكان خاص.

2-2-1-3-1 مدى خضوع مكونات الحاسب الآلي المعنوية للتفتيش:

يعد تفتيش المكونات المعنوية للحسابات الآلية إحدى أهم العوائق التي تعيق التحقيق لأن هذه المكونات التي ينصب عليها التفتيش هي عبارة عن مكونات لا ترى بالعين المجردة، ولا يمكن لمسها لهذا انقسم الفقه المقارن إلى فئتين: فئة تحاول تبرير تفتيش المكونات المنطقية للحاسوب انطلاقاً من أن هذه البيانات عبارة عن نبضات، أو ذبذبات إلكترونية، أو موجات كهرومغناطيسية قابلة لأن تسجل وتخزن على وسائط معينة ولها كيان مادي محسوس من خلال إستشعارها، وإمكانية قياسها، ولذلك يمكن إخضاعها لقواعد التفتيش التقليدية.

ومثال ذلك قانون إساءة استخدام الحاسب الآلي في إنجلترا الصادر سنة 1990، حيث نص على أن "إجراءات التفتيش تشمل أنظمة الحاسب الآلي"، وهناك تشريعات أجازت تفتيش أي شيء أو اتخاذ أي إجراء يكون لازماً لجمع أدلة الجريمة وعلى ضوء ذلك فإن تفتيش المكونات المعنوية للحسابات الآلية يدخل في عداد الأشياء التي جاء النص عليها عاماً دون تقييد، وكمثال لهذه التشريعات المادة 251 من قانون الإجراءات الجنائي اليوناني التي تجيز لسلطة التحقيق أن تتخذ أي إجراء أو شيء يكون لازماً لجمع الدليل ويفسر الفقه اليوناني عبارة أي شيء بأنها تشمل جميع بيانات الحاسب الآلية المادية والمعنوية سواء كانت هذه البيانات مخزنة في حملتها أم كانت معالجة آلياً في الذاكرة الداخلية، وعلى هذا النهج نجد المادة 487 من القانون الجنائي الكندي، تعطي للسلطة المختصة الحق في إصدار الإذن يضبط أي شيء ويغير الفقه عبارة "أي شيء" بأنها تشمل المكونات المادية والمعنوية في الحسابات الآلية. [1] ص 43

ولكن يوجد إتجاه آخر من يرى أن التفتيش لا يرد إلا على أشياء مادية ملموسة، ولا يمكن أن تكون الأشياء المعنوية محلا للتفتيش هذا من جهة، وتوجد إلى جانب هذا المشكل مشكلات إجرائية أخرى لتفتيش مكونات الحاسب الآلي غير المادية أهمها.

- نقص الخبرة لدى السلطات التي تقوم بالتفتيش، حيث أن التفتيش هنا يتطلب عملية الولوج وضبط البيانات الموجود بداخله وهذا يحتاج إلى إلمام بالجوانب التقنية.

- صعوبة تحديد محل التفتيش والأشياء المراد ضبطها وذلك لتعلقها بأمر فنية تحتاج إلى أن يكون القائمون بالتفتيش على علم بذلك.

- صعوبة السيطرة على الأجهزة المراد تفتيشها، وخاصة عندما يكون الجهازان في مكانين مختلفين ومتصلين بشبكة عنكبوتية. [06] ص 311

والتشريع الجزائري يعتبر من بين التشريعات التي أجازت تفتيش منظومة معلوماتية وفقا للمادة 05 الخامسة من القانون 04/09.

3-2-1-3-1 مدى خضوع شبكات الحاسب الآلي للتفتيش:

تشير مسألة تفتيش شبكات الحاسب الآلي أي عندما يكون الحاسب الآلي مرتبط بشبكة الإتصال مشكلة أخطر بكثير من مشكلة تفتيش الحاسب الآلي، ويزداد الأمر خطورة عندما يتعلق الأمر بنهاية طرفية موجودة في منزل المتهم ومتصلة بجهاز موجود خارج الدول، وتعد شبكة الأنترنت أهم هذه الشبكات ولذلك سوف نتناول إمكانية تفتيش الحاسب الآلي في الفرض الذي يكون مرتبط فيه بشبكة محلية بمعنى داخل الدولة أو بشبكة عالمية.

- إتصال حاسب المتهم بحاسب آخر موجود داخل الدولة:

من الخصائص التي تتميز بها الحاسبات الآلية أنها قد تتصل مع بعضها البعض داخل الدولة عن طريق الشبكة المحلية، أو قد تتصل مع حاسبات أخرى تقع خارج الدولة عن طريق الربط الشبكي بين أجزاء العالم المختلفة، وفي حالة وقوع جريمة في نظم حاسب آلي يقع داخل الدولة يجوز بالنسبة لها إصدار الإذن بالتفتيش بالنسبة للحاسب الآلي الصادر لصالحه إذن التفتيش فقط، ويترتب على ذلك أنه إذا كان الحاسب المراد تفتيشه يتصل بحاسب آخر لم يصدر بالنسبة له إذن التفتيش، فلا يمكن أن يمتد إليه إذن التفتيش، ويترتب على ذلك أنه إذا كان الحاسب المراد تفتيشه يتصل بحاسب آخر لم يصدر بالنسبة له إذن التفتيش، فلا يمكن أن يمتد إليه حتى ولو كان يحتوي على جريمة. [01] ص 45

أما بالنسبة للتشريع الجزائري فلقد أجاز تفتيش منظومة معلوماتية وفقا للمادة 05 من القانون 04/09 كما أنه أجاز أيضا في الفرض الذي تكون فيه هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة بذلك.

- إتصال حاسب المتهم بحاسب آخر موجود خارج الدولة:

من المشاكل التي تواجه سلطات الإدعاء في جمع الأدلة، وهي قيام مرتكبي الجرائم بتخزين بيانات في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكة الإتصالات البعيدة، بهدف عرقلة التحقيقات، ولمواجهة هذا التكتيك المتطور لتخزين المعلومات بدأت بعض النظم القانونية في التصدي له، من بينها قانون حماية الحاسب الهولندي والذي أجاز لجهات التحقيق تفتيش حتى النظم الموجودة خارج الدولة، بيد أن تقرير المجلس الأوروبي يعتبره انتهاكا لسيادة الدولة، ولذا فإنه مع عدم وجود اتفاقية دولية فإن هذا الاختراق المباشر الذي تضمنته المادة j/125 يفضل عدم تطبيقه. [17] ص 24

لكن المشرع الجزائري ووفقا لنص المادة 05 من القانون 04/09 أقر أنه إذا تبين مسبقا بأن المعطيات المبحوث عنها، والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل.

2-3-1 ضبط مكونات الجريمة:

حتى يحقق التفتيش غايته في جمع الأدلة الجرمية، لا بد من وسيلة لإلتقاط تلك الأدلة وتثبيتها، هذه الوسيلة هي الضبط الذي يعتمد على تحرير أوراق رسمية بكل خطوة تأتينا جهة التفتيش بالإضافة إلى إلتقاط كل دليل معتبر في الإثبات. [47] ص 285

الضبط هو التحفظ على الأشياء وحجزها ووضعها في أختام، فيجيز القانون لقاضي التحقيق أن يقوم بذلك، إذا كانت هذه الأشياء والوثائق تنفع في إظهار الحقيقة، أو تلك التي يضر إفشاؤها بسير التحقيق، والضبط عادة ما يكون مقترنا بالتفتيش الذي يهدف إلى نفس النتيجة.

1-2-3-1 ضبط مكونات الكمبيوتر:

لا يثير ضبط مكونات الحاسب الآلي المادية أية مشكلة تعيق إجراءات لتحقيق، وبالتالي لا يوجد خلاف بين الفقهاء في إمكانيات ضبطها، لأن الغاية من التفتيش هي ضبط المكونات المادية التي تفيد في كشف الحقيقة، ونلاحظ أن النصوص التي تنطبق على الجرائم التقليدية [54]، تنطبق على ضبط الأشياء المادية لجهاز الحاسب الآلي إذا تعلق الأمر بجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

لكن الإشكال يتعلق بضبط المكونات المعنوية للحاسب الآلي، بحيث تعددت الآراء بين الفقهاء فمنهم من يرى بأن الضبط لا يرد إلا على شيء مادي، أما الأشياء المعنوية كبرامج وبيانات الحاسب المعالجة فلا تصلح محلا للضبط، وهناك من يرى أنه ينطبق على الكيانات المعنوية لأن التفتيش لا ينحصر عند مدلوله الضيق في الكيان المادي وإنما يشكل كل ما يدخل في جنسه وفقا للتفسير المنطقي الذي يفسر النص على ضوء المصلحة التي يحققها المشرع من ورائه، ويترتب على ذلك أن الشيء طالما يحقق منفعة أو مصلحة إقتصادية فإنه يكون محلا للحماية سواء كان هذا الشيء من الكيانات المادية أو المعنوية. [01] ص 54

وتجدر الإشارة إلى أن المشرع الجزائري قد نص على ضبط المعطيات المعلوماتية وفقا للقانون 04/09 المتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وفقا للمواد 06 و 07 و 08 و 09.

حيث جاء في نص المادة 06 عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرار وفقا للقواعد المقررة في قانون الإجراءات الجزائية، ويجب في كل الأحوال على السلطة التي تقوم بالتفتيش، والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها إستعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للإستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

وجاء في المادة 07 أنه في حالة إستحالة إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش إستعمال التقنيات المناسبة لمنع الوصول إلى

المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخ المعطيات الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

أما ما جاء في المادة 08 هو إمكانية السلطة التي تباشر التفتيش من الإستعانة بشخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك، وذلك بغرض منع الإطلاع على المعطيات.

أما المادة 09 فقد جاء فيها أنه تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به لا يجوز إستعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

وهذه العقوبات جاءت بها المادة 11 حيث نصت على أنه تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من (06) ستة أشهر إلى (5) خمس سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات وذلك دون الإخلال بالعقوبات الإدارية المترتبة على عدم إحترام الإلتزامات المنصوص عليها في المادة.

كذلك من ضمن المشاكل التي تعترض سبيل الضبط، وهي الطبيعة التقنية للجريمة وللدليل، كذلك مسألة حق المتهم في الصمت والتي تقرها معظم التشريعات والتي تصطدم مع هذا النوع من الجرائم لأنه في بعض الأحيان يكون كلام المتهم مفيد في إجراءات الضبط... [06] ص 346

1-3-2-2 ضبط الرسائل ومراقبة الإتصالات الإلكترونية:

على الرغم من أن ثورة المعلومات قد أسعدت الأفراد بما وفرتهم لهم من سبل الإتصال الحديثة والتي إنعكس أثرها على مختلف مناحي حياتهم، إلا أنها قد سببت لهم الكثير من الأضرار الشخصية ليس فيما يتعلق بالجرائم المستحدثة التي قد ترتكب ضدهم، وإنما كذلك بالنسبة لإنتهاك أسرارهم الشخصية عن طريق الوسائل الإلكترونية المتقدمة.

ونظرا لأن المراسلات والإتصالات الخاصة تعد من الأسرار الشخصية التي لا يجوز الإعتداء عليها، لذلك فقد نصت على حمايتها أغلب التشريعات ومن بينها التشريع الجزائري، الذي وفر لها حماية دستورية لمايشكل الإعتداء عليها مساس بالحياة الخاصة للفرد.

جاء في نص المادة 39 من الدستور الجزائري لسنة 1996 " سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة "، ومن خلال نص المادة 39 نلاحظ أنها شملت كافة أشكال المراسلات بما فيها المراسلات التي تتم عن بعد.

ونلاحظ أن المشرع الجزائري وفقا للتعديل الأخير لقانون الإجراءات الجزائي 06-22 من المادة 65 مكرر 5 إلى 65 مكرر 10 قد أجاز إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، ولكن قيد هذا الإجراء بشروط خاصة، حيث جاء في المادة 65 مكرر 5 أنه:

- لا يجوز إتخاذ هذه الإجراء إلا إذ اقتضت ضرورات التحري ذلك.

- كذلك أن تكون هذه الجريمة متلبس بها أو التحقيق الإبتدائي في الجرائم الخطيرة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

- أن يقدم الإذن من وكيل الجمهورية، وفي حالة فتح تحقيق قضائي تتم العمليات المذكورة بناء على إذن من قاضي التحقيق المباشرة وجاء في المادة 65 مكرر 7 أنه:

- يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5 بكل العناصر التي تسمح بالتعرف على الإتصالات المطلوب التقاطها، والأماكن المقصود سكنية أو غيرها، والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها.

- يسلم الإذن المكتوب لمدة أقصاها 4 أشهر قابلة للتجديد وجاء في المادة 65 مكرر 10 أنه:

ينسخ ضابط الشرطة القضائية المأذون له أو المناب المراسلات أو الصور، أو المحادثات المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف، كما أجازت المادة 65 مكرر 8 لكل من وكيل الجمهورية أو ضابط الشرطة القضائية الذي إذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينييه أن يسخر كل عون مؤهل لدى مصلحة، أو وحدة، أو هيئة عمومية، أو خاصة ومكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر 5 أعلاه.

فالتساؤل الذي يطرح في هذا المجال هل تطل عملية إعتراض المراسلات هنا البريد الإلكتروني بإعتباره وسيلة حديثة للتراسل؟.

يقصد بالبريد الإلكتروني e-mail الرسائل الإلكترونية التي تبعث عن طريق إستخدام شبكات الحاسب كبديل عن الرسائل التقليدية، حيث يخصص لكل شخص صندوق بريد إلكتروني تسجل فيه جميع المراسلات الواردة والصادرة أو المستغنى عنها في سلة المهملات، ويمكن الإطلاع على محتوى

الصندوق والإرسال من أي مكان في العالم باستخدام خطوط التليفون أو الموجات اللاسلكية أو الأقمار الصناعية. [17] ص 27

ومن المسائل الهامة المتعلقة بالبريد الإلكتروني كيفية المحافظة على سرية، وهذا ما حذا بالمبتكرين لبرامجه بابتكار برامج تشفير خاصة بحيث لا يمكن الإطلاع على أي رسالة إلا لمن يعرف هذه الشيفرة، ويمكن حفظ البريد الإلكتروني في صناديق بريد خاصة، أو في ملف أو نسخ الرسالة والإحتفاظ بها ولقد ساعد ظهور التوقيع الإلكتروني في تسيير عملية التراسل عبر البريد الإلكتروني فالبرنامج يقوم بتخزين توقيع المستخدم كرمز أو شيفرة ويضعه تلقائيا على كل رسالة. [01] ص 58

ورغم وجود اختلاف وجهات النظر حول إمكانية ضبطها فالبعض يرى أنه لا يمكن ضبطها وتفتيشها إلا وفقا لنصوص خاصة، والبعض الآخر يرى أنه يمكن ضبطها وفقا للنصوص التقليدية لأنه لا يوجد إختلاف بين هذا المستند والمستند التقليدي، فالمستند وفقا لأصحاب هذا الإتجاه هو: كل أسلوب لتحديد فكر أو فكرة على ورقة مكتوبة أو من خلال صوت أو صورة مسجلة ولذلك يجب الإعتراف بها كمستندات. [06] ص 352

إلا أن المشرع الجزائري لم يترك أي التباس حول ضبطها أم لا. فإنه وإن لم يشر صراحة إلى ضبط الرسائل الإلكترونية في المواد سالفه الذكر من المادة 65 مكرر 5 إلى 65 مكرر 10 وأشار إلى إمكانية أن يكون بوسائل فنية وتقنية فقط، تضمن بلفظ صريح ضبط الرسائل الإلكترونية من خلال نص المادة 03 من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها حيث جاء "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات، يمكن لمقتضيات حماية النظام العام، أو لمستلزمات التحريات، أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، أو القيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

أمّا ما تعلق منها: بمراقبة الإتصالات الإلكترونية فنجد أن المشرع الجزائري قد نص عليه صراحة في الفصل الثاني تحت عنوان مراقبة الإتصالات الإلكترونية ونص على الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية في نص المادة 4 فقرة 01 وهي:

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب، أو التخريب، أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو الدفاع الوطني، أو مؤسسات الدولة، أو الإقتصاد الوطني.

- لمقتضيات التحريات، والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

وتشترط ذات المادة أنه إذا تعلقّت المراقبة الإلكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب، أو التخريب، أو الجرائم الماسة بأمن الدولة وحدها يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية المخولة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إذنا لمدة ستة 06 أشهر قابلة للتجديد، وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

الفصل 2

صور الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

تعرض سير عمل نظم المعالجة الآلية للمعطيات العديد من الأعمال الجرمية، والتي تتميز بكونها ذات طبيعة خاصة كما سنرى، وبفعل ماثيره التطبيق القضائي لنصوص القوانين التقليدية على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من مشكلات، وبغرض عدم إفلات الجناة من العدالة الجنائية لعدم كفاية النصوص، أو عجزها على الانطباق على هذه الجرائم، وإحتراما لمبدأ الشرعية الذي يقضي بأن لا جريمة ولا عقوبة إلا بنص، وفي ظل مبدأ حظر القياس بالنسبة للنصوص الجزائية، ولمواجهة الخسائر الفادحة التي تحدثها هذه الجرائم استدعى كل هذا تدخلا تشريعيا.

فقد تدارك المشرع الوطني الفراغ القانوني في مجال الإجرام المعلوماتي، وذلك باستحداثه لنصوص قانونية بهدف قمع الاعتداءات الواردة على المعلوماتية في الفصل الثالث من الباب الثاني من الكتاب الثالث من القانون 15/04 بإضافة قسم سابع مكرر عنوانه المساس بأنظمة المعالجة الآلية للمعطيات من المادة 394 مكرر إلى غاية المادة 394 مكرر 7، فقد نص على مجموعة من الجرائم، وأوجب لها عقوبات قاسية.

بالإضافة إلى إصداره للقانون 04/09 الصادر في 05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. [11]

وسوف نتناول في هذا الفصل الجرائم الماسة بنظام المعالجة الآلية للمعطيات في المبحث الأول وفي المبحث الثاني سوف نتناول الجرائم الماسة بالمعطيات، أما المبحث الثالث فسوف نتناول فيه الأحكام المشتركة لمختلف الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

1-2 الجرائم الماسة بنظام المعالجة الآلية للمعطيات

يعتبر نظام المعالجة الآلية للمعطيات الشرط الأولي الذي يلزم تحققه للقول بوقوع إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات ولقد تطرقنا إلى مفهوم هذا النظام في الفصل الأول عند تناولنا لمفهوم الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات.

وكما سبق القول فإن الجرائم الموجهة ضد النظام المعلوماتي، قد تقع على المكونات المادية للنظام "le matériel" وتعتبر في هذه الحالة من قبيل الجرائم التقليدية، كما في حالة تحطيم جهاز الكمبيوتر، وقد تقع على المكونات غير المادية.

تتحقق جريمة التعدي على المكونات غير المادية للنظام المعلوماتي عندما تكون مكونات الكمبيوتر المعلوماتية غير المادية مثل البرامج المستخدمة، أو البيانات المخزنة في ذاكرة الحاسب الآلي محل أو موضوع للجريمة. [44] ص 15

ونكون بصدد جرائم المساس بأنظمة المعالجة الآلية للمعطيات عندما يتم الاعتداء على برامج التشغيل، وهي التي تعتبر المسؤولة عن عمل النظام المعلوماتي، من حيث قيامها بتنظيم وضبط التعليمات الخاصة بالنظام. [45] ص 67

وسوف نتناول جريمة الدخول داخل نظام المعالجة الآلية للمعطيات في المطلب الأول ونتناول في المطلب الثاني جريمة البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات باعتبار أن هتين الجريمتين تسمان النظام.

1-1-2 جريمة الدخول داخل نظام المعالجة الآلية للمعطيات:

تعتبر جريمة الدخول داخل نظام المعالجة الآلية للمعطيات من أهم الجرائم، وهذا كونها تعتبر أول جريمة يرتكبها الشخص، ومن خلالها ممكن أن ترتكب جرائم أكثر خطورة.

وكذلك لأن هذه الجريمة شكلية فيقوم الفعل الإجرامي بمجرد الدخول داخل النظام دون أن يتطلب ذلك تحقق نتيجة معينة، ولهذا نجد أن مختلف التشريعات قد نصت على هذه الجريمة منه التشريع الإماراتي في مادته الثانية. [10]، وكذا الإتفاقية الدولية للإجرام المعلوماتي في مادتها الثانية. [13] ولا تقوم جريمة الدخول داخل نظام المعالجة الآلية للمعطيات إلا بتوافر الأركان العامة لأي جريمة بالإضافة إلى العنصر المفترض ألا وهو نظام المعالجة الآلية للمعطيات الذي يجب توافره في كافة الجرائم المعلوماتية، حتى يمكن القول بأنها جرائم معلوماتية وهو الذي سبق تناوله في الفصل الأول، وعلى هذا الأساس لا داعي للتكرار.

1-1-1-2 الركن الشرعي:

جرم المشرع الجزائري جريمة الدخول داخل نظام المعالجة الآلية للمعطيات وفقا لنص المادة 394 مكرر من قانون العقوبات الجزائري، كونها تعتبر جريمة مستحدثة لارتباطها بالتطور التكنولوجي، وبهذا النص فقد وضع المشرع الجزائري حدا لأي خلاف فقهي أو قانوني حول تجريمها عملا بمبدأ الشرعية الذي يقضي بالأجريمة ولا عقوبة إلا بنص، حيث نصت المادة 394 مكرر " يعاقب بالحبس من 3 ثلاثة أشهر إلى سنة وبغرامة من 50.000 إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش، في 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 ستة أشهر إلى 2 سنتين والغرامة من 50.000 إلى 150.000 دج " .

من خلال النص القانوني للمادة سالفة الذكر يتضح بأن المشرع الجزائري قد حذو التشريع الفرنسي في تجريم الدخول داخل النظام المعلوماتي، حيث أعتبر النص نقلا عن النص الفرنسي إلا ما تعلق منه بالعقوبة المقررة، وكذا عدم النص على المحاولة في التشريع الفرنسي وهذا في المادة 323-1 [59] ، حيث نجد أن المشرع الفرنسي قد جعل العقوبة أكثر تشديدا من المشرع الجزائري من خلال النص على عقوبة ذات حد واحد لجريمة الدخول في صورتها البسيطة أو المشددة سواء الغرامة أو الحبس، وبالتالي لا يكون للقاضي سلطة تقديرية في تقدير العقوبة، وإنما يلتزم في حكمه بذات العقوبة المقررة، أما في القانون الجزائري فالقاضي يتمتع بسلطة تقديرية بين الحد الأدنى والأعلى للعقوبة.

1-1-1-2-1 الجريمة في صورتها البسيطة:

تضمنتها المادة 394 مكرر فقرة أولى وتخص جريمة الدخول إلى نظام المعالجة الآلية للمعطيات مجرد عن تحقيق أية نتيجة إجرامية، أي أن الجريمة تتحقق بمجرد الدخول.

1-1-1-2-2 الجريمة في صورتها المشددة:

تضمنتها المادة 394 مكرر فقرة ثانية، وتخص جريمة الدخول إلى النظام المعلوماتي مع تحقيق نتيجة إجرامية تتمثل وفقا لنص المادة 394 مكرر فقرة 2 في حذف أو تغيير لمعطيات المنظومة، أو تخريب نظام اشتغال المنظومة، ولحدوث هذه النتيجة لا يتطلب المشرع الجزائري أن يتم عن طريق العمد وإنما يتم عن طريق الخطأ، وهذا ما جعل جريمة التلاعب التي نص عليها المشرع الجزائري في نص المادة 394 مكرر 1، تختلف عن الصورة المشددة لجريمة الدخول داخل النظام كونها جريمة عمدية، أما عن تخريب نظام اشتغال المنظومة فإن المشرع قد اكتفى بتجريمها كطرف مشدد على

جريمة الدخول أو البقاء، ولم ينص على تجريمها في حالة ارتكابها عن طريق العمد كما فعل التشريع الفرنسي في مادته 2/323 الذي عاقب كل من عطل أو أفسد نشاط أو وظائف المعالجة الآلية للمعطيات وبذلك يكون قد توسع في حماية نظم المعالجة الآلية للمعطيات [59] ، ويقصد بالإفساد هو ذلك الفعل الذي يجعل نظام المعالجة الآلية للمعطيات غير صالح للإستعمال السليم بأن يعطي نتائج غير تلك التي كان من الواجب اعطائها، أو يؤدي النظام لوظائفه في مدة أطول، أمّا فعل الإعاقة فهو الذي يؤدي إلى إرباك نظام المعالجة الآلية للمعطيات [61] ص ص 48، 49 ، ويعد هذا قصور في التشريع الجزائري.

ويلاحظ من خلال نص المادة السابقة بأن المشرع الجزائري قد استخدم لفظ المنظومة وليس النظام، مما يجعل القارئ للنص يستنتج أو يتبادر إلى ذهنه بأن النظام المحمي جزائيا وفقا لنص المادة 394 مكرر، لا بد أن يكون عنصرا من منظومة لمعالجة البيانات مما دفع البعض إلى تحبيذ لفظ النظام على المنظومة [06] ص 180 حتى تكون هناك حماية للنظام في حالته المنفصلة عن الأنظمة الأخرى لكننا نرى أنه لا إشكال فيما يتعلق بمصطلح المنظومة المعلوماتية لأن المشرع الجزائري قد نص في المادة 2 / "ب" من القانون 04/09 المتضمن قواعد الوقاية من الجرائم الإلكترونية المقصود بالمنظومة المعلوماتية. [62] ص 05

ونشير فقط إلى أن المشرع الجزائري قد جرم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات مجرد عن أية غاية أو هدف، وهذا ما أخذ به كذلك كل من التشريع الفرنسي والإماراتي وهناك من التشريعات من جرمت الدخول إلى نظام المعالجة الآلية للمعطيات وجعلته الجريمة الأساسية أمّا ما يعقب ذلك من أفعال فهي لا تشكل سوى ظروف مشددة، وقد أعتبر المشرع الأمريكي في قوانين إساءة استخدام الحاسبات الآلية لعامي 1984 و1986 جريمة الدخول غير المصرح به نقطة البداية لأي جريمة معلوماتية أخرى، وهناك من التشريعات ما أقرت أنه لا يمكن عقاب كل من يقرع على باب الحاسب الآلي، وإنما يجب أن يحاط التجريم بشروط محددة وهو ما تبناه القضاء الإنجليزي، حيث أنّ القانون التركي اشترط نية إيذاء الغير أو الحصول على ربح. [22] ص 320

2-1-1-2 الركن المادي:

يتكون الركن المادي في جريمة الدخول غير المشروع من مجرد سلوك الدخول في الجريمة في صورتها البسيطة، أو الدخول الذي يؤدي إلى نتيجة معينة في صورتها المشددة.

2-1-1-2 السلوك الإجرامي:

يعد السلوك الإجرامي من أهم عناصر الركن المادي، لأنه لا قيام للركن المادي ولا قيام للجريمة بالتالي إذا تخلف هذا السلوك، والسلوك في جريمة الدخول غير المصرح به يتمثل في سلوك إيجابي، أو

ما يطلق عليه بالفعل وهو الذي يمثل فعل الدخول ، وهذا ما جاء في نص المادة 394 مكرر وعليه سنتناول السلوك الإجرامي لهذه الجريمة.

- فعل الدخول accés:

يقصد به الدخول إلى محتويات جهاز الكمبيوتر ذاته، أي إجراء اتصال بالنظام محل الحماية بالطرق الفنية اللازمة لذلك، وليس معنى الدخول، الدخول المادي كالدخول إلى القاعة الموجود بها جهاز الكمبيوتر [46] ص 102، ويرى الفقه الفرنسي أن الدخول له مدلول معنوي، حيث أن الدخول إلى النظام يشبه عملية الدخول إلى ذاكرة الإنسان، كما أن له مدلول مادي يتمثل في أن الشخص يكون قد حاول الدخول أو دخل بالفعل إلى النظام المعلوماتي، وحسب التصور المعنوي فإن عملية الدخول قد تكون مباشرة أو غير مباشرة [24] ص 361، كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصال التلغرافية والطرفيات سواء كانت محلية أو عالمية.

وتجدر الإشارة إلى أن المعنى اللغوي لكلمة " دخول " والتي تقابلها في الفرنسية كلمة "entrée" تعني النفاذ أو الاختراق إلى مكان مادي كالدخول إلى المسكن مثلا، وهذا المعنى لا يمكن تطبيقه بشأن الدخول إلى أنظمة المعالجة الآلية للمعطيات، لأن الدخول إلى تلك الأنظمة هو ظاهرة غير مادية، لذلك نجد أن المشرع الفرنسي قد استعمل مصطلح "accés" بدلا من مصطلح "entrée" وكذلك نجد أن المشرع الإماراتي قد إستعمل مصطلح "التوصل بغير وجه حق" وهو أكثر ملائمة من مصطلح الدخول ولهذا كان على المشرع الجزائري أن يستبدل مصطلح "الدخول" بمصطلح " التوصل بغير وجه حق" لأن الاتصال في معناه لا يثير الإشكال الذي يثيره مصطلح الدخول لأن الدخول إذا كان له مدلول مادي في جانب منه، فإن التوصل أو الاتصال لا يكون له مثل هذا المدلول الأمر الذي ينفي عن النص الغموض أو الإختلاف في التفسير.

أمّا عن تعبير " عن طريق الغش " الذي أورده المشرع الجزائري بنص المادة 394 مكرر والذي أشترط المشرع تحققه لقيام الجريمة، فإن هناك جانبا من الفقه الفرنسي ينتقد هذه العبارة، ذلك لأنها قد توحى بضرورة توفير نوع من الحماية التقنية للنظام حتى يمكن الاستفادة من هذا النص. حيث أن الجاني مع وجود هذه الحماية استطاع أن يدخل إلى البرنامج باستخدامه لأساليب الغش والتضليل، فعن طريق الغش استطاع أن يتغلب على حراسة البرنامج وتمكن من اختراقه والدخول إليه. [63] ص 185

بمعنى أن النظام الذي لا يتمتع بمثل هذه الحماية يعد الاتصال به اتصالا مصحوبا بالغش، بمعنى أن الاتصال به اتصال مشروع، لكن الرأي الراجح هو أن الجريمة تتحقق سواء كان النظام محميا أو غير محمي بأنظمة أمان وهذا كون أن التشريع لم ينص على هذا القيد. [09] ص 79

وننوه إلى أن السلوك أو النشاط الإجرامي لا يمكن أن يتحقق في حالة كون أن النظام مفتوحا للجمهور، إذ يمكن لأي شخص أن يدخل إليه، ولا يوصف هذا الدخول بعدم المشروعية، إلا إذا قيد بشروط أو خصص لأشخاص عندها لا يكون نظاما مفتوحا لاستخدام الجمهور.

ولا يشترط توافر صفة معينة فيمن يقوم بعملية الدخول، وهذا ما جاء في نص المادة 394 مكرر ".....كل من يدخل أو يبقى" وعليه يمكن أن يقوم بهذه الجريمة أي شخص سواء كان ذكر أو أنثى صغير أو كبير، يعمل في مجال الأنظمة أم لا علاقة له بنظم الحاسب الآلي، وقد يكون شخص منبث الصلة عن النظام الداخل فيه، وتوصل إلى النظام عن طريق كمبيوتر آخر موجود في مكان آخر وذلك بواسطة الدخول إلى شبكة المعلومات. [46] ص 103

ولا يشترط كذلك أن يتم الدخول بطريقة معينة، فالمادة 394 مكرر قد جاءت شاملة لكل طرق الدخول، فالدخول إلى النظام يتم بأي وسيلة تقنية حيث تتعدد طرق ووسائل الدخول إلى النظام المعلوماتي وأكثر هذه الوسائل استخداما لإرتكاب جريمة الدخول هي: تشغيل كمبيوتر مغلق أو استعمال كمبيوتر مفتوح، كما تتم أيضا بـ:

* الدخول إلى الكمبيوتر عن طريق استعمال كارت تشغيل ينتمي إلى شخص آخر: قد يتمكن المتهم من الحصول على كارت (بطاقة) للدخول إلى الكمبيوتر إحدى الجهات لكي يحصل على خدمة معينة ذلك إذا كان النظام لا يسمح بالدخول بدون رقم سري، وهذا يحدث عادة في حالة سحب مبالغ مالية *الدخول إلى الكمبيوتر عن طريق خط تليفوني: قد يتمكن المتهم من الوصول إلى نظام الكمبيوتر عن طريق العبث بالخط التليفوني المربوط عليه هذا النظام، فيمكنه هذا من الاتصال بنظام من أنظمة الكمبيوتر، وعادة ما يقوم المتهم بذلك، بغية التوصل إلى إعطاء أوامر النظام للكمبيوتر لتحقيق غاية معينة.

ومن أهم هذه التقنيات:

*المصيدة: المصيدة أو المداخل المميزة تعني أن هناك ممرات خالية متروكة في برنامج ما بمعنى وجود أخطاء وعيوب في البرنامج الأصلي، والتي لا يمكن اكتشافها عند الاستعمال الأول وقد يصل الأمر إلى حد استخدام المعيدة حسب أهوائهم وخطورة هذه الجريمة تتمثل في حقيقة الأمر أنه عن طريقها يمكن الوصول إلى كل المعلومات المخزنة بالحاسب الآلي، أي التوصل إلى التعليمات والشفرات الخاصة بها.

* استخدام برنامج خاص: يكون ذلك بقيام الشخص بإدخال برنامج داخل هذا الجهاز، بحيث يقتصر دوره على التحسس بتسجيل نظام زمني ودخول المشتركين، الأمر الذي ينتج له إمكانية الاحتفاظ بهذه المعلومات.

*استخدام البرامج المخصصة لتخطي أنظمة الأمان في الحالات الطارئة: على الرغم من ضرورة تزويد الحاسبات الآلية ببعض أنظمة الحماية الفنية له دون الاتصال غير المشروع بالبرامج والبيانات المخزنة، إلا أن إدارة وتشغيل بيانات الحاسبات بطريقة آمنة خاضعة للتحكم والسيطرة تقتضي وجود نوع من البرامج يمكن استخدامها لتجنب تخطي حواجز الحماية الفنية لمنظومات الحاسبات في الحالات الطارئة، وحالات إختلال وظائف الحاسب أو توقفها عن العمل، فقد تستعمل هذه البرامج غير المشروعة.

أو استعمال أي وسيلة فنية كاستعمال حسان طروادة مثلا [64] ص 832، ويمكن الدخول كذلك عن طريق استعمال كلمة السر الحقيقية متى كان الجاني غير مخول في استخدامها، أو عن طريق إستخدام برامج أو شفرة خاصة.

ويلاحظ أن تحديد فكرة الدخول غير المشروع من حيث دلالة المكان يمكن أن تعرف بأنها التسلسل في داخل نظم المعلوماتية، أما الدخول من حيث الزمان فيتمثل في تجاوز حدود التصريح أو الترخيص داخل النظام الممنوح لفترة زمنية محددة عن طريق تجاوز هذه الفترة، [39] ص 243، والأصل أن يرتبط تجاوز الفترة الزمنية للدخول بالبقاء وليس بالدخول وإن كان يرتبط به في جانب منه وعلى هذا الأساس سوف نتناول مسألة من له الحق في التصريح عند تناولنا لجريمة البقاء.

ويتحقق فعل الدخول إلى النظام بشكل كلي أو بصورة جزئية، والحكمة من المساواة بين الولوج الكلي والولوج الجزئي هو أن المعتدي في حالة التدخل المقترن بالغش، يمكن أن يدعي بسهولة أن تدخله في مكان محدود بجزء ضيق جدا من النظام، ولا يمكن التحقق من هذا الإدعاء من الناحية العملية. [06] ص 186

وعليه يتحقق فعل الدخول متى كان الدخول يمثل مخالفة لإرادة صاحب النظام أو من له حق السيطرة عليه، أو كان مخالفا لشروط الدخول إذا كان الدخول بناء على عقد مثلا.

وجريمة الدخول تختلف عن بعض الأفعال المتعلقة بالجوانب التقنية في مجال التكنولوجيا الرقمية التي يتم من خلالها سرقة المعلومات، أو الإطلاع عليها أثناء إنتقالها من طرفية نظام إلى طرفية نظام آخر. [06] ص 194، وسيتم إيضاح الخلاف بينهما على النحو التالي بنوع من الإيجاز.

• الفرق بين الدخول والتقاط وإعتراض الرسائل المرسلية:

يتفق كل من الدخول غير المصرح به إلى نظام الحاسب الآلي والاعتراض غير المصرح به لهذا النظام، في أن كل منهما يؤدي إلى نتيجة واحدة، وهي الوصول إلى المعلومات المتواجدة داخل نظام المعالجة الآلية للمعطيات .

بعبارة أخرى يمكن القول أن الوصول إلى المعلومات الكائنة داخل نظام الحاسب الآلي قد يتم مباشرة، وذلك عن طريق الدخول إلى نظام الحاسب الآلي أو بطريقة غير مباشرة عن طريق الاعتراض، [22] ص 350، وتعد الوسيلة الأساسية لاعتراض نظام الحاسب الآلي، هي استخدام الموجات الكهرومغناطية الصادرة عن الحاسب الآلي "ELECTROMAGNETIC RADIATION" اعتراض نظام الحاسب الآلي كما هو معروف في الولايات المتحدة الأمريكية باسم التقاط الموجات الكهرومغناطية "ELECTROMAGNETIC PICKUP" هو جمع للمعلومات عن بعد.

ويختلف إعتراض الرسائل التي ترسل عن طريق جهازي كمبيوتر على شبكة مغلقة، أو عن طريق الانترنت على جريمة الدخول، لكون الإعتراض والإلتقاط لا يتضمن تدخلًا في نظام معين ينتمي إلى كمبيوتر معين، ولكن يمثل نوعًا من التلصص على الرسائل المرسلية بين جهازين من الأجهزة، ولا يعتبر من قبيل النشاط الذي يعاقب عليه القانون بوصفه دخولا، ويتم ارتكاب الفعل عن طريق وسائل سلكية تتصل بالنظام، أو عن طريق التقاط الرسائل بواسطة وسائل حديثة يتم الإلتقاط بواسطتها عن بعد. [06] ص 195

يختلف كذلك الإعتراض عن الدخول غير المصرح به في أنه في حالة الاعتراض غير المصرح به لا يمكن تحديد الجاني للمعلومات التي سوف يقوم بالإلتقاطها، حيث يلتقط الجاني المعلومات التي يتم إرسالها دون أن يكون له دور في تحديدها، مع احتمال أن المعلومات مفيدة جدا له في تحديده للمكان الذي يقوم بالإلتقاط منه، كذلك أن الجاني في هذه الحالة لا يكون له أي دور في تعديل المعلومات، وكذلك تكون عملية تشغيل الحاسب الآلي قد بدأت من قبل شخص غير الجاني بعكس الدخول داخل نظام المعالجة الآلية للمعطيات. [22] ص 351

ولقد حذا المشرع الجزائري حذو المشرع الفرنسي في عدم النص على الاعتراض، ولذا أدى هذا الاختلاف بين الدخول غير المشروع إلى نظام الحاسب الآلي، وبين اعتراض هذا النظام إلى تدارك ذلك في الاتفاقية الدولية للإجرام المعلوماتي في مادتها الثالثة، [13] ، التي أوجبت على الدول الأطراف فيها النص على تجريم فعل الإلتقاط، ونجد النص في بعض قوانين الدول العربية كالقانون الإماراتي في ماته الثامنة . [10]

وبناء على ما تم ذكره فإنه لا يمكن تجريم فعل التقاط البيانات والمعلومات المرسلّة بواسطة نظام معلوماتي من خلال نص المادة 394 مكرر قانون العقوبات الجزائري الخاصة بتجريم الدخول أو البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات فعلى المشرع الجزائري حسم المشكلة القانونية عن طريق إيراد نص خاص يعاقب على إعتراض والتقاط البيانات.

• الفرق بين الدخول والإستعمال غير المصرح به للنظام:

يمكن تعريف الاستعمال غير المصرح به للنظام المعلوماتي بأنه " كل استخدام للحاسوب ولنظامه للاستفادة من الخدمات التي يقدمها دون أن يكون للشخص الذي يستخدم هذا النظام الحق في ذلك". [31] ص 114

ولقد تعددت التسميات التي أطلقت على الاستعمال غير المصرح به لنظام الحاسب الآلي، حيث يستخدم البعض للدلالة عليه سرقة وقت الحاسب الآلي، أو سرقة الخدمات التي يقدمها الحاسب الآلي، أو تشغيل الحاسب الآلي بدون مقابل، أو إساءة استخدام وقت الحاسب الآلي. [45] ص 88، ويتحقق فعل الاستعمال غير المصرح به، كما في حالة استخدام موظف لدى شركة ما الحاسب الآلي الخاص بها في أغراض شخصية، وفي غير ساعات العمل الرسمية، وقد يكون الاستخدام صادر من شخص من الغير. [44] ص 81، وعليه يتم الاستعمال على الأغلب من أشخاص لهم الحق في الدخول إلى النظام، وتختلف فكرة الدخول في النظام عن استعماله، حيث أن تجريم الدخول في النظام لا يعني أن يقوم المتدخل باستعمال الجهاز كون أن دائرة الدخول "The Admission" أضيق من دائرة الاستعمال "USAG" فكل استعمال للنظام دون رضا صاحبه يشكل دخول والعكس غير صحيح فالدخول لا يعني بالضرورة استعمال النظام. [06] ص 197

ومن الحالات العملية قيام عدد من الموظفين التابعين لإحدى المعامل التابعة لمكتب التحقيقات الفدرالية (F,B,I) الخاص بإنتاج الصواريخ النووية باستخدام الكمبيوتر الخاص بالمعمل بشكل غير مشروع لأغراض شخصية. [29] ص 88، وتجدر الإشارة إلى أن المشرع الجزائري لم ينص على هذه الجريمة بعكس التشريع الكندي. [31] ص 120، والتشريع الأمريكي لعام 1986 الذي وضع نصوص صريحة تعاقب عليها.

- محاولة الدخول إلى نظام المعالجة الآلية للمعطيات:

لقد نص المشرع الجزائري على المحاولة بنص المادة 394 مكرر بقوله " ...كل من يدخل أو يبقى عن طريق الغش، في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك..."

فالمحاولة بشكل عام إما أن تكون ناقصة أو كاملة، ففي المحاولة الناقصة لا يقوم الجاني بكل الأفعال التنفيذية اللازمة لإتمام الركن المادي للجريمة، أما المحاولة التامة فهي ما يطلق عليها بالشرع في تنفيذ الجريمة، ويفترض أنّ الجاني قد قام بفعله كاملاً، ولكن النتيجة لم تتحقق. [65] ص 164

ومحاولة الدخول إلى نظام المعالجة الآلية للمعطيات تتحقق بكافة الأعمال التحضيرية التي من شأنها أن تساعده على الدخول إلى النظام، ومثال ذلك البحث عن كلمة السر عن طريق إدخال برنامج في الجهاز الهدف منه التجسس بتسجيل نظام ترميز المشتركين، الأمر الذي يتيح له إمكانية الإحتفاظ بهذه المعلومات.

أو عن طريق شراء البرامج والأجهزة التي تساعده على الاختراق وفك الشفرات، إلى غير ذلك من الوسائل التي تساهم في التحضير لجريمة الدخول داخل النظام، وليس الدخول إلى النظام لأن هذا يتجاوز مجرد المحاولة.

وكما سبق وأشرنا في فعل الدخول فإن جريمة محاولة الدخول إلى النظام المعلوماتي ترتكب من قبل أي شخص بغض النظر عن صفته، فيكفي لتحقيق الجريمة أن يكون الجاني قد حاول الدخول إلى النظام مخالفاً لشروط الدخول، إذا كان الدخول يستلزم شروطاً معينة كدفع مبلغ معين مثلاً، [31] ص 159، وتتحقق المحاولة سواء كان غرض الجاني الدخول إلى كل النظام أو إلى جزء منه وفقاً لما جاء في المادة سالفه الذكر.

ونشير إلى أن جريمة الدخول إلى النظام الآلي بطريق الغش جريمة شكلية، لا يستلزم لتحقيقها تحقق نتيجة معينة له أهميته التي تبنى على التفرقة بين الجرائم المادية والجرائم الشكلية، وأهم هذه الفوارق هو عدم تصور الشروع في الجرائم الشكلية وتصوره في الجرائم المادية. [63] ص 188 وتجدر الإشارة إلى أن المشرع الجزائري قد نص على الشروع أو المحاولة بنص المادة 394 مكرر وبذلك خرج على القواعد العامة للشروع والتي تقضي بأنه لا يتصور الشروع في الجرائم الشكلية التي يقع ركنها المادي بمجرد السلوك، فهي إما أن تقع كاملة وإما أن لا تقع، كذلك لا يمكن تصور الشروع في الجرائم غير العمدية. [65] ص 165، ذات النتيجة، أي يمكن أن تقع بمحض الصدفة وهذه الحالة تنطبق على جريمة الدخول داخل نظام المعالجة الآلية للمعطيات في صورتها المشددة، فهي جريمة غير عمدية، وكذلك نشير إلى مسألة أكثر خطورة وهي مسألة الشروع في الشروع، حيث نجد أن المشرع الجزائري قد نص على الشروع في نص المادة 394 مكرر سالفه الذكر بالنسبة لجريمة الدخول داخل نظام المعالجة الآلية للمعطيات وكذلك نجد أن المادة 394 مكرر 7 جاء فيها أن كافة الجرائم تخضع لنظام الشروع بما فيها جريمة الدخول داخل نظام المعالجة الآلية للمعطيات وهذا ما يفيد بوجود شروع داخل الشروع.

فكان على المشرع الجزائري أن يأخذ بما أخذ به المشرع الإماراتي الذي لم ينص على المحاولة في نص المادة 2 من القانون الاتحادي رقم 02 لسنة 2006، وكذلك بما أخذ به المشرع الفرنسي حيث إنه لم ينص على المحاولة في نص المادة 1-323 وعندما نص على الشروع في نص المادة 4-323 أستبعد جريمة الدخول أو البقاء من هذا النص،[59]، ومن وجهة نظري أن فيه إفقاد لمعنى ظروف التخفيف ولا يشجع الفاعل على العدول على ارتكاب الجريمة إذا ما بدأ بتنفيذها.

3-1-1-2 الركن المعنوي:

كما هو معلوم يقصد بالركن المعنوي الجانب الشخصي أو النفسي للجريمة، فلا تقوم الجريمة بمجرد قيام الواقعة المادية التي تخضع لنص التجريم، ولا تخضع لسبب من أسباب الإباحة، بل لابد من أن تصدر هذه الواقعة عن إرادة فاعلها، وترتبط بها ارتباطاً معنوياً وأدبياً [65] ص 231، ولقد أعتبر المشرع جريمة الدخول داخل نظام المعالجة الآلية للمعطيات جريمة عمدية يجب أن تتم عن طريق الغش، بحيث يتوفر فيها العلم والإرادة، بخلاف الجريمة في صورتها المشددة التي اعتبرت وفقاً لنص المادة 394 مكرر قانون العقوبات، جريمة غير عمدية.

1-3-1-1-2 الركن المعنوي للجريمة في صورتها البسيطة:

كما سبق وأشرنا أن جريمة الدخول في صورتها البسيطة جريمة عمدية يتطلب لتحقيقها القصد الجنائي العام بعنصره العلم والإرادة.

- القصد الجنائي العام:

لقيام القصد الجنائي لا بد أن يتحقق عنصره وهما العلم والإرادة:

• العلم:

لقيام القصد الجنائي لابد أن ينصرف الجاني إلى كل واقعة ذات أهمية قانونية في تكوين الجريمة أي كل واقعة يتطلبها القانون لبناء أركان الجريمة واستكمال عناصرها، وبالإضافة إلى ذلك لابد أن يشمل العلم التكييف الذي تتصف به بعض هذه الوقائع وتكتسب به أهميتها في نظر القانون،[26]ص166، فالفاعل لابد أن يعلم أنه يقوم بفعل الدخول غير المصرح به إلى النظام المعلوماتي، [31] ص160، وبالتالي يجب أن يعلم بأنه ليس له حق دخول النظام، أو أن ذلك يخالف رضا صاحب النظام.[25] ص 86

لكن عنصر العلم ينتفي وينتفي معه القصد الجنائي، في حالة ما إذا وقع الجاني في خطأ يتعلق بحقه في الدخول، أو في مدى نطاق هذا الحق كأن يجهل وجود حظر الدخول، أو كان يعتقد خطأ أنه مسموح له بالدخول. [66] ص 134

• الإرادة:

للإرادة أهمية قصوى في نطاق القانون الجنائي، فالقانون يعنى بالأعمال الإرادية، فإذا تجرد فعل الإنسان من الإرادة فلا يعتد به ولو أصاب المجتمع بأفدح الخسائر، [65] ص 258 ، فبالإضافة إلى توافر العلم لقيام القصد الجنائي، لا بد من توافر الإرادة، ذلك لأنها هي التي تبين الموقف النفسي للفاعل من سلوكه ومن النتيجة المترتبة عليه، وبما أن جريمة الدخول غير المصرح به جريمة شكلية لا يتطلب لقيامها تحقق نتيجة معينة، فإن الإرادة فيها تقتصر على السلوك الإجرامي فتستغرقه بكل مقوماته، ولا تمتد إلى أي نتيجة بغض النظر عن الباعث أو الغاية، سواء كان بغرض إثبات وجود ثغرات أمنية في النظام، أو بقصد الحصول على أموال الغير، أو الانتقام من رب العمل. [06] ص 200

- مدى ضرورة توافر القصد الجنائي الخاص:

لا يبدو من نص المادة 394 مكرر أن المشرع يتطلب وجود نية خاصة لدى الجاني حتى تقوم جريمة الدخول غير المصرح به، وأنه يكفي لقيامها توافر القصد الجنائي العام القائم على العلم والإرادة.

لكن هناك من الفقهاء الفرنسيين من يرون أن لفظ "FRAUDULEUSEMENT" كما هو منصوص عليه في التشريع الفرنسي يختلف عن مصطلح عمدا وإراديا، ويدل على أن جريمة الدخول في تلك المادة لا تقوم بمجرد القصد العام، وإنما لا بد لذلك من قصد خاص هو "الغش". [26] ص 167

لكن الفقه متفق أن الغش هو "كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها. [63] ص 76

وعليه فجريمة الدخول داخل نظام المعالجة الآلية للمعطيات جريمة عمدية، لا يتطلب لتحققها قصدا خاصا.

2-3-1-1-2 الركن المعنوي للجريمة في صورتها المشددة:

لقد شدد المشرع الجزائري عقوبة جريمة الدخول داخل نظام المعالجة الآلية للمعطيات في إحدى حالتين: الأولى: إذا ترتب على الدخول حذف أو تغيير لمعطيات المنظومة، والثانية: إذا ترتب على الدخول تخريب نظام اشتغال المنظومة.

وفي هذه الحالة لا يشترط أن تكون النتيجة المترتبة على الدخول مقصودة، لأن تطلب مثل هذا الشرط غير معقول، كون أن المشرع الجزائري نص على جريمة الاعتداء العمدي على المعطيات بنص المادة 394 مكرر 1، وعلى هذا الأساس لكي تتحقق هذه الجريمة غير العمدية يكفي أن توجد بين الظرف المشدد والجريمة الأساسية علاقة سببية.

فجدير بالذكر أنه لكي يتم المعاقبة على هذا الظرف المشدد، لا بد أن يحدث بعد دخول غير مصرح به [26] ص 170، فإذا كان الأصل أن الفاعل لا يقصد أن يتحقق الظرف المشدد كنتيجة لجريمة الدخول، فإن القصد الجنائي العام هو المفترض في هذه الصورة كأثر على الجريمة، والمسؤولية عن الجريمة المشددة هي مسؤولية غير عمدية تقوم عن طريق الخطأ. [06] ص 202

4-1-1-2 العقوبات المترتبة على جريمة الدخول داخل نظام المعالجة الآلية للمعطيات:

يتضمن قانون العقوبات الجزائري نوعين من العقوبات، إما عقوبات أصلية أو عقوبات تكميلية وفيما يتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات فالمشرع نص على هاذين النوعين من العقوبتين ولأنه سوف يتم تناول العقوبات التكميلية أثناء إيضاح الأحكام المشتركة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فسيتم الاقتصار على العقوبات الأصلية للجريمة سواء في صورتها البسيطة أو المشددة .

1-4-1-1-2 عقوبة جريمة الدخول في صورتها البسيطة:

- وفقا لنص المادة 394 مكرر تكون عقوبة جريمة الدخول عن طريق الغش إلى نظام المعالجة لآلية للمعطيات:

هي "الحبس من ثلاثة 3 أشهر إلى سنة والغرامة من 50.000 إلى 100.000دج" ومن خلال نص المادة نلاحظ أن المشرع الجزائري قد منح القاضي سلطة تقديرية في اختيار العقوبة المناسبة، بحسب الحالة المعروضة عليه.

- عقوبة جريمة الدخول في صورتها البسيطة وفي حالة استهدافها للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام:

طبقا لنص المادة 394 مكرر 3 والتي جاء فيها أنه "تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد".

ونلاحظ من خلال نص المادة أن المشرع الجزائري شدد العقوبة وفي حالة إستهدافها للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، وهذا نظرا للأهمية البالغة لهذه المعطيات، كون أن الاعتداء عليها يشكل مساسا بالاقتصاد الوطني هذا من جهة، ومن جهة ثانية فإن حساسية هذه المعطيات وخاصة المعطيات التابعة لمؤسسة الدفاع الوطني كونها تمس بأمن الدولة ككل تحتاج إلى مثل هذا النص، وعليه تصبح جريمة الدخول داخل نظام المعالجة الآلية للمعطيات في حالة إستهدافها للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام هي "الحبس من (6) ستة أشهر إلى (2) سنتين والغرامة من 100.000 إلى 200.000 دج".

- عقوبة جريمة الدخول المرتكبة من قبل الشخص المعنوي:

وفقا لنص المادة 394 مكرر 4 "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل (5) خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وعليه يعاقب الشخص المعنوي في حالة إرتكابه لجريمة الدخول في صورتها البسيطة بـ"500.000 دج"

- عقوبة جريمة الدخول المرتكبة من قبل الشخص المعنوي وفي حالة استهدافها للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

فوفقا لما جاء في نص المادة 394 مكرر 3 التي تضاعف من العقوبة في حالة ما إذا كانت المعطيات تابعة لمؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، ووفقا أيضا لنص المادة 394 مكرر 4 والتي جاء فيها أنه في الحالة التي ترتكب فيها الجريمة من قبل شخص معنوي فإن العقوبة المقررة له هي مضاعفة الحد الأقصى للغرامة إلى 5 خمسة أضعاف وعليه: تصبح عقوبة جريمة الدخول المرتكبة من قبل الشخص المعنوي وفي حالة استهدافه للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، هي: $5 \times 2 \times 100.000 = 1.000.000$ دج.

2-4-1-1-2 عقوبة جريمة الدخول في صورتها المشددة:

تشدد عقوبة جريمة الدخول وفقا لنص المادة 394 مكرر فقرة 2 في حالتين:

- عندما يترتب على الدخول حذف أو تغيير لمعطيات المنظومة:

- وفقا لنص المادة 394 مكرر فقرة 2". تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة"، وعليه ففي حالة ما إذا نتج عن الدخول حذف أو تغيير لمعطيات المنظومة تكون العقوبة "الحبس من ستة أشهر إلى (2) سنتين والغرامة من 100.000 إلى 200.000 دج".

- في حالة ارتكاب الجريمة من قبل شخص معنوي:

وفقا لنص المادة 394 مكرر 4 والتي تنص صراحة على مضاعفة الحد الأقصى للغرامة إلى (5) خمس مرات العقوبة المطبقة على الشخص الطبيعي في حالة ارتكابه نفس الجريمة وعليه تصبح العقوبة هي: " $1.000.000 = 5 \times 200.000$ دج".

- إذا ترتب على جريمة الدخول حذف أو تغيير لمعطيات منظومة تابعة للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

وفقا لنص المادة 394 مكرر 3 حدد المشرع الجزائري مقدار مضاعفة العقوبة إلى الضعف وعليه يحكم القاضي وفقا لسلطته التقديرية بالعقوبة التالية " الحبس من سنة إلى (4) سنوات والغرامة من 200.000 إلى 400.000 دج"، وهذا وفقا لملاسات القضية وخطورة المجرم.

- إذا ارتكبت الجريمة من قبل الشخص المعنوي وفي حالة استهدافه للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

فوفقا لما جاء في نص المادة 394 مكرر 3 التي تضاعف من العقوبة في حالة ما إذا كانت المعطيات تابعة لمؤسسة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام، ووفقا أيضا لنص المادة 394 مكرر 4 والتي جاء فيها أنه في الحالة التي ترتب فيها الجريمة من قبل شخص معنوي فإن العقوبة المقررة له هي مضاعفة الحد الأقصى للغرامة إلى (5) خمس أضعاف وعليه: تصبح عقوبة جريمة الدخول المرتكبة من قبل الشخص المعنوي وفي حالة استهدافه للدفاع الوطني، أو الهيئات، والمؤسسات، الخاضعة للقانون العام هي: $4.000.000 = 5 \times 2 \times 200.000$ دج.

- عندما يترتب على جريمة الدخول تخريب نظام اشتغال المنظومة:

- وفقا لنص المادة 394 مكرر 3 "وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من (6) ستة أشهر إلى (2) سنتين والغرامة من 50.000 إلى 150.000 دج"

نلاحظ من خلال نص المادة سالفة الذكر أن المشرع الجزائري شدد العقوبة إلى الضعف إذا ترتب على جريمة الدخول تخريب نظام اشتغال المنظومة، أما عن الغرامة المقررة فنلاحظ أنه احتفظ بالحد الأدنى للغرامة هي 50.000 دج ، أما الحد الأقصى فقد شدده .

• في حالة ارتكاب الجريمة من قبل شخص معنوي:

وفقا لنص المادة 394 مكرر 4 والتي تنص صراحة على مضاعفة الحد الأقصى للغرامة إلى 5 خمس مرات فتصبح العقوبة $750.000 = 5 \times 1.500.000$ دج

• إذا ترتب على جريمة الدخول تخريب نظام إشتغال منظومة تابعة للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام .

وفقا لنص المادة 394 مكرر 3 نلاحظ أن المشرع الجزائري قد نص على المضاعفة وعليه تصبح العقوبة "الحبس من سنة إلى 4 سنوات والغرامة من 100.000 إلى 300.000 دج".

• إذا ارتكبت الجريمة من قبل شخص معنوي وإستهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

فوفقا لما جاء في نص المادة 394 مكرر 3 التي تضاعف من العقوبة في حالة ما إذا كانت المعطيات تابعة لمؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، ووفقا أيضا لنص المادة 394 مكرر 4 والتي جاء فيها أنه في الحالة التي ترتكب فيها الجريمة من قبل شخص معنوي فإن العقوبة المقررة له هي مضاعفة الحد الأقصى للغرامة إلى 5 خمس أضعاف وعليه: تصبح عقوبة جريمة الدخول المرتكبة من قبل الشخص المعنوي وفي حالة استهدافها للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، هي $1.500.000 = 5 \times 2 \times 150.000$ دج .

2-1-2 جريمة البقاء داخل نظام المعالجة الآلية للمعطيات:

تعتبر جريمة البقاء داخل نظام المعالجة الآلية للمعطيات ثاني جريمة نص عليها المشرع الجزائري بعد جريمة الدخول داخل النظام المعلوماتي، وهو أمر منطقي كون أن البقاء كفعل يترتب مباشرة بعد الدخول ، بحيث لا يمكن أن يتحقق فعل البقاء إلا بعد أن يتحقق فعل الدخول سواء كان دخولا مشروعا وفي هذا الفرض لا تتحقق جريمة الدخول، أو بعد دخول غير مشروع وفي هذا الفرض تتحقق جريمة الدخول بالموازاة مع جريمة البقاء، وتكتسي هذه الجريمة أهمية بالغة، كون أن البقاء هو الذي يمكن الجاني من القيام بالأفعال الإجرامية المراد اقترافها، فما دام الجاني متصلا بالنظام لفترة أطول فبإمكانه ارتكاب جريمته على أحسن وجه.

إنّ جريمة البقاء داخل نظام المعالجة الآلية للمعطيات كأى جريمة أخرى يتطلب لتحقيقها توافر الأركان العامة الواجب توافرها في أي جريمة بالإضافة إلى العنصر المفترض ألا وهو نظام المعالجة الآلية للمعطيات.

1-2-1-2 الركن الشرعي:

جرم المشرع الجزائري جريمة البقاء داخل نظام المعالجة الآلية للمعطيات بنص المادة 394 مكرر قانون العقوبات الجزائري، كون أنها تعتبر من الجرائم المستحدثة حيث نصت المادة على ما يلي: "يعاقب بالحبس من 3 ثلاثة أشهر إلى سنة وبغرامة من 50.000 إلى 100.000 د ج كل من يدخل أو يبقى عن طريق الغش، في 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 ستة أشهر إلى 2 سنتين والغرامة من 50.000 إلى 150.000 د ج".

من خلال النص القانوني نلاحظ أن المشرع الجزائري سار على النهج الذي اتبعه المشرع الفرنسي في تجريم البقاء داخل النظام المعلوماتي، وما قيل عن الاختلاف بين التشريع الفرنسي والجزائري فيما يتعلق بالمشاولة وتشديد العقوبة من قبل المشرع الفرنسي في جريمة الدخول داخل نظام المعالجة الآلية للمعطيات يقال عن جريمة البقاء داخل نظام المعالجة الآلية للمعطيات لأن المشرع الجزائري قد أخضعهما لنفس النص وبالتالي لنفس الأحكام. ووفقا لنص المادة 394 مكرر سالف الذكر فإن جريمة البقاء داخل نظام المعالجة الآلية للمعطيات تأخذ إحدى صورتين.

1-1-2-1-2 الجريمة في صورتها البسيطة:

وهي التي جاء بها نص المادة 394 مكرر فقرة أولى وتخص جريمة البقاء داخل نظام المعالجة الآلية للمعطيات مجرد عن تحقيق أية نتيجة إجرامية، أي أن الجريمة تتحقق بمجرد التواجد والمكوث داخل نظام المعالجة الآلية للمعطيات، دون أن يتبع هذا البقاء تغيير في حالة المعطيات، أي حتى ولو لم تتحقق أية نتيجة.

2-1-2-1-2 الجريمة في صورتها المشددة:

تضمنتها المادة 394 مكرر فقرة 2 و3، وتخص جريمة البقاء داخل النظام المعلوماتي مع تحقيق نتيجة إجرامية تتمثل وفقا لنص المادة 394 مكرر فقرة ثانية في حذف أو تغيير لمعطيات المنظومة، أو تخريب نظام إشتغال المنظومة وفقا لنص المادة 394 مكرر فقرة ثالثة.

2-2-1-2 الركن المادي:

يتكون الركن المادي لجريمة البقاء داخل نظام المعالجة الآلية للمعطيات في فعل البقاء في الجريمة في صورتها البسيطة، أو في فعل البقاء الذي يؤدي إلى نتيجة معينة في صورتها المشددة، وفقاً لما جاء في نص المادة 394 مكرر.

1-2-2-1-2 السلوك الإجرامي.

إن هذه الجريمة ليست كسابقتها حيث أن الجاني في الجريمة يسعى بنفسه إلى تحقيق الاتصال مما يتطلب منه فعلاً إيجابياً أي القيام بعمل، لذلك هي جريمة إيجابية، أما جريمة البقاء فهي تتطلب الخروج من البرنامج أو النظام الآلي وقطع الاتصال، أو عدم الإبقاء عليه. [63] ص 190

- فعل البقاء (le maintien):

يعتبر فعل البقاء هو السلوك الثاني الذي نصت عليه المادة 394 مكرر ويقصد بالبقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على النظام. [18] ص 133، ومن النص سالف الذكر يتبين أن المشرع يلقي على عاتق من يتحقق الاتصال عنده واجب مضمونه عدم البقاء في النظام الذي حصل به الاتصال، أي أن عليه أن يقوم بفعل إيجابي مضمونه قطع الاتصال، وعليه ففعل البقاء يشكل جريمة امتناع تتحقق بفعل إيجابي. [63] ص 190

وهذه الجريمة ليست كسابقتها، حيث أن الجاني في الجريمة السابقة يسعى بنفسه إلى تحقيق الاتصال، أما في هذه الجريمة فإن المشرع يتطلب قطع الاتصال لمجرد حصوله، وهذا يعني على الأغلب أن الاتصال تم عن طريق الخطأ ولو لم يتبعه إتلاف للمعطيات الموجودة داخل النظام، ويكفي لتحقيق الجريمة البقاء داخل النظام كله أو في جزء منه.

كذلك تتحقق هذه الجريمة في حالة ما إذا كان الدخول إلى النظام مشروعاً. [09] ص 80، ومن صور البقاء استمرار وجود الجاني داخل النظام بعد المدة المحددة له، ومن أمثلة هذا البقاء ما يتعلق بالخدمات التليفونية المفتوحة للجمهور، وحصول الجاني على الخدمة لمدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة.

بينما يرى البعض أن البقاء بعد تجاوز المدة المصرح بها للبقاء في النظام لا تعد جريمة بقاء، لأن الهدف من التجريم هو حماية معلومات وبيانات الحاسب من الإطلاع عليها، وأن البقاء بعد انتهاء المدة المصرح بها لا يحقق ذلك الهدف كون أن المعلومات قد تم الإطلاع عليها بداية من التصريح المحدد

بمدة زمنية معينة، وإنما يمكن أن تكون الجريمة المرتكبة في هذه الحالة هي جريمة الإستعمال غير المصرح به للنظام. [26] ص 155

كذلك يمكن أن تتحقق هذه الجريمة في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي يكون مسموحاً له فيه بالرؤية والإطلاع فقط، ويمكن أن تتحقق هذه الجريمة بالنسبة للخدمات المفتوحة للجمهور بعكس الجريمة الأولى، وقد يتحقق البقاء المعاقب عليه مستقلاً عن الدخول إلى النظام وقد يجتمع، ويكون البقاء معاقب عليه استقلاً حين يكون الدخول إلى النظام مشروعاً وتعتبر جريمة شكلية لا يشترط فيها حدوث نتيجة معينة، فيكفي البقاء داخل النظام المعلوماتي وينطبق عليه في هذه الحالة كل ما قيل على الدخول ليقوم الركن المادي للجريمة. [31] ص 161

وتختلف جريمة الدخول عن جريمة البقاء في كون أن جريمة البقاء جريمة مستمرة يستمر السلوك الإجرامي ومعه يستمر الاعتداء على المصلحة القانونية، بينما جريمة الدخول جريمة وقتية سواء كان دخول مجرد أو أدى إلى نتائج معينة، لأن الجريمة تكتمل في اللحظة التي يتم الدخول فيها إلى النظام وعليه إذا لم ينص المشرع على البقاء فلا يمكن سحب أحكام الدخول إليه. [21] ص 110، وقد يجتمع الدخول غير المشروع والبقاء غير المشروع وذلك في الفرض الذي لا يكون فيه للجاني الحق في الدخول للنظام ويدخل إليه فعلاً ضد إرادة من له الحق في السيطرة على النظام، ثم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الفرض الاجتماع المادي للجرائم بين الجريمتين، ولكن تثار مشكلة متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء.

لقد ذهب رأي من الفقه إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه المتدخل أن بقاءه داخل النظام غير مشروع، وهنا تثار صعوبة تحديد علم المتدخل. وذهب رأي آخر إلى أن جريمة البقاء تبدأ منذ اللحظة التي يتذكر فيها المتدخل بأن تواجه غير مشروع، فإذا لم ينسحب يرتكب منذ تلك اللحظة جريمة البقاء، وقد أنتقد هذا الرأي بحجة أن جهاز الإنذار لا يكون متوفراً إلا بالنسبة للمؤسسات والشركات الكبيرة فقط.

ولذلك فالرأي الراجح في مثل هذه الظروف هو أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي بدأ فيها الجاني التجول داخل النظام، ويستمر في التجول داخله بعد إنتهاء الوقت المحدد، فإذا دخل وظل ساكناً تظل الجريمة جريمة دخول داخل النظام، أما إذا بدأ في التجول فتبدأ هنا جريمة البقاء. [18] ص 134

المهم أن جريمة البقاء تتحقق متى كان فعل البقاء يمثل مخالفة لإرادة صاحب النظام، كتلك الأنظمة التي تتعلق بأسرار الدولة أو الدفاع عنها، أو تتضمن بيانات شخصية تتعلق بحرمة الحياة

لخاصة ولا يجوز الإطلاع عليها. [25] ص 82، وهنا تثار مسألة في غاية الأهمية وهي من له حق التصريح.

إن تحديد الشخص المخول له التصريح أمر بالغ الأهمية، إذ تتوقف الجريمة على إرادة ذلك الشخص أو تلك الهيئة، يسمى الفقه الفرنسي هذا الشخص بصاحب السلطة أو السيطرة على النظام " LE MAÎTRE DU SYSTEME" وقد عرفته المادة الثانية 2 من الإتفاقية الخاصة بحماية الأفراد في مواجهة نظم المعالجة الآلية للمعطيات ذات الطابع الشخصي والتي تبنها المجلس الأوروبي في 28/يناير/1989 عرفته بأنه: "كل شخص طبيعي أو معنوي، أو كل سلطة عامة أوكل مؤسسة أو جهاز يكون له سلطة التصرف في نظام الحاسب الآلي التابع لهم، وتقرير مضمونه أو محتواه وكيفية تنظيمه والهدف منه "[26] ص 145، ولا يثور أي إشكال في حالة ما إذا كان التصريح يعود لشخص واحد ولكن يثور في حالة تعدد المسؤولين كما في حالة تعدد الأنظمة ، ففي هذه الحالة يكون الجميع مسؤولين بمعنى أن التصريح الصادر عن أحد هؤلاء يلزم الباقيين ويعتبر كأنه صادر منهم جميعا. [26] ص 146

ويبقى الإشكال قائما في حالة عدم وجود تصريح إطلاقا، وتحقق في الحالة التي لا يقدم فيها تصريح، أو في الحالة التي يقدم فيها تصريحا لكن المصرح له يقوم بتجاوز حدود هذا التصريح.

• حالة عدم وجود تصريح إطلاقا:

وهي الحالة التي لا يكون فيها للشخص الذي يدخل النظام أية علاقة بهذا الأخير، وذلك لأنه ليس من العاملين لدى الجهة التي يتبعها النظام، أو أنه من العاملين إلا أنه لا توجد له أية علاقة بالنظام، لأن وظيفته لا تخوله الاتصال به، وفي كلتا الحالتين لا يحوز هذا الشخص ترخيص بالدخول للنظام، أو في الحالة التي يكون فيها الدخول إلى النظام ممنوعا إطلاقا، وتحقق هذه الحالة مثلا: في المستشفيات اللاتي تحتوي على قاعدة بيانات، نظم أسماء المرضى وكل المعلومات المتعلقة بهم من بينها نوعية المرض ...، ففي هذه الحالة نجد أن الممرضين وبعض الأطباء مثلا غير مخول لهم صلاحية الإطلاع على هذه البيانات لعدم الاختصاص أو لأي سبب آخر، ففي حالة الإطلاع على هذه البيانات من قبل هؤلاء الأشخاص يعتبر دخولهم غير مصرح به، ويكونون بذلك قد ارتكبوا جريمة دخول داخل النظام حتى وإن كانوا موظفين لدى المستشفى.

ونوه إلى أن المشرع الجزائري قد أغفل النص على معاقبة الموظفين أثناء ارتكابهم لإحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات مثل ما فعلت التشريعات المقارنة، ومنها التشريع الإماراتي في مادته الثالثة. [10]، ويعتبر هذا قصور في التشريع الجزائري.

• حالة تجاوز التصريح:

هذه الحالة تثير العديد من الإشكالات مقارنة بالحالة الأولى، كون أن الشخص في هذه الحالة مرخص أو مصرح له بالدخول إلى النظام، لكن في حدود معينة، ورغم ذلك يتجاوز حدود التصريح المقدم له، ويصعب في كثير من الحالات تحديد ما إذا كان تجاوز اختصاصه بعمد أو بغير عمد، لهذا يكون من الواجب تحديد اختصاصات كل عامل بدقة، والمجالات التي يمكن لكل واحد الدخول فيها. [26]ص 148.

وتجاوز التصريح إما أن يتعلق بالغرض الذي منح من أجله التصريح، أو بالمجال الذي حدده التصريح.

* تجاوز الغرض الذي منح من أجله التصريح.

تنور هذه المسألة في حالة ما إذا تم الدخول إلى النظام لغير الغرض الذي منح من أجله التصريح لقد اختلفت آراء الفقهاء وموقف القضاء بشأن هذه المسألة، فهناك من يرى بأن الدخول كان مشروع وبالتالي فلا جريمة وهو موقف القضاء الأمريكي ويظهر في قضية DPPV BINGELL [22]ص 351، وقد تعرض الحكم السابق المستأنف إلى نقد شديد بحجة أنه يضيق من نطاق تطبيق قانون إساءة استخدام الحاسبات، وأنه يتنافى والمفهوم الصحيح للتصريح بالدخول إلى نظام الحاسب الآلي، لأن الحق في هذا الدخول مقيد بالغرض الذي أعطي من أجله، وهذا النقد تبناه القضاء الأمريكي فهو يرى أن الدخول غير المصرح به يتحقق في حالة استخدام العامل للحاسب الآلي لأسباب تتعارض مع مصلحة رب العمل، يضاف إلى ذلك إذا كان العامل لا يعمل لمصلحة رب العمل، والباعث هنا هو الذي يحدد ما إذا كان الدخول مصرح أو غير مصرح به، وتسمى هذه الحالات في الفقه الأمريكي بسوء إدارة العاملين "EMPLOYEE MISCONDUCT CASES" [26] ص 153، أما الرأي الراجح هو أن جريمة الدخول غير المصرح به لا تتعلق بتجاوز الغرض الذي منح من أجله التصريح لأن المادة 394 مكرر إنما نصت على الدخول غير المصرح به بطريق الغش وليس ما يحصل بعد هذا الدخول من التزام بحدود التصريح أو تجاوزه، وعبارة الغش تنصرف إلى عملية الدخول وليس إلى حدود التصريح وهذا عملاً بالمبادئ التي تقول بعدم التوسع في التفسير بالإضافة إلى حظر القياس [26]ص 153.

* تجاوز المجال الذي حدده التصريح.

في هذه الحالة يملك الشخص الذي يدخل النظام تصريحاً بالدخول إليه، لكن هذا التصريح غير عام وإنما هو قاصر على أجزاء من النظام، وعلى هذا الأساس يكون الدخول إلى الأجزاء المصرح بها مشروع ويكون غير مشروع في المناطق غير المصرح بها.

ويتم هذا التجاوز عادة من قبل العاملين في المؤسسات الصحية لأن هؤلاء هم الذين يملكون في العادة تصريحاً بالدخول، وتثير هذه المسألة إشكالا فيما يتعلق بالأنظمة المشتركة، والتي تتكون إثر ارتباط أكثر من نظام فهل يعتبر العاملين في الأنظمة الأصلية عاملين أيضا في النظام المشترك والإجابة على هذا السؤال تكون بالإيجاب إذا كانت ثمة علاقة بين العامل وبين النظام المشترك، أي أنه يملك تصريحاً بالدخول إلى هذا النظام أو إلى جزء منه، وجدير بالذكر أن تجاوز التصريح إما أن يكون تجاوزا في المكان، أي تجاوز الفاعل للمناطق والمجال المكاني المصرح به إلى غيره من المجالات غير المرخص له بدخولها، وفي هذه الحالة تتحقق جريمة الدخول غير المشروع إلى النظام المعلوماتي، وإما أن ينصب هذا التجاوز في الزمان وليس في المكان، بمعنى البقاء لوقت أطول من البقاء المرخص به وهنا تتحقق جريمة البقاء داخل نظام المعالجة الآلية للمعطيات.

3-2-1-2 الركن المعنوي:

يشترط لتحقيق جريمة البقاء داخل نظام المعالجة الآلية للمعطيات توافر الركن المعنوي، ويتمثل الركن المعنوي لجريمة البقاء في صورتها البسيطة في القصد الجنائي العام بعنصره العلم والإرادة، إذ تعد الجريمة في هذه الحالة جريمة عمدية، أما جريمة البقاء في صورتها المشددة فهي جريمة غير عمدية، كون أن المشرع الجزائري نص على جريمة التلاعب بالمعطيات العمدية بنص المادة 394 مكرر 1 مما يؤكد أن جريمة البقاء في صورتها المشددة جريمة غير عمدية.

1-3-2-1-2 الركن المعنوي للجريمة في صورتها البسيطة:

باعتبار أن الجريمة من الجرائم العمدية وعلى هذا الأساس سوف نتناول مسألة القصد الجنائي العام.

- القصد الجنائي العام:

يتطلب المشرع الجزائري لقيام جريمة البقاء في صورتها البسيطة توافر القصد الجنائي العام بعنصره العلم والإرادة.

• العلم:

يجب أن يعلم المتهم بأنه يقوم بالبقاء داخل نظام المعالجة الآلية للمعطيات ولا يهتم بعد ذلك أن يتحقق البقاء داخل النظام الذي كان يقصده أم إلى نظام آخر. [06] ص 198، وعليه فقيام القصد الجنائي لا بد أن يحيط علم الجاني ما يتطلبه القانون لبناء أركان الجريمة واستكمال كل منها عناصره كي يقال أن عنصر العلم قائم في القصد، والأصل أن يحيط علم الجاني بكل الوقائع التي يتطلبها القانون لقيام الجريمة، فلا يقتصر الأمر على العناصر السابقة على السلوك، وإنما تمتد لتشمل العناصر اللاحقة والمعاصرة للفعل طالما كانت ضرورية للتكوين القانوني للواقعة. [65] ص 250.

لكن عنصر العلم ينتفي وتنتفي معه الجريمة في حالة ما إذا وقع الجاني في خطأ، كأن يعتقد خطأ أن له حق البقاء ويتحقق هذا مثلاً في الحالة التي يكون له حق الدخول إلى النظام ولكن ليس له البقاء ولكن الفاعل يعتقد خطأ أن له حق البقاء لأن له حق الدخول، أو كان مثلاً من الأشخاص الذين لديهم اشتراك في الدخول إلى النظام ولكن الاشتراك انتهى أجله ولم يدفع مبلغ الاشتراك للمرة الثانية ومع ذلك يعتقد خطأ أن له حق الدخول والبقاء داخل النظام.

وكذلك ينتفي القصد الجنائي في الفرض الذي يعتقد فيه الجاني بناء على أسباب معقولة أنه يقوم مثلاً بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلي، ولا يعلم أنه داخل نظام المعالجة الآلية للمعطيات. [22] ص 379، ولكن إذا كان الدخول إلى النظام عن طريق الخطأ ينفي المسؤولية الجنائية العمدية لانقضاء القصد الجنائي الذي لا تقوم بدونه الجريمة، فإن الدخول بطريق الخطأ والاستمرار بذلك والتجوال داخل النظام، وعدم قطع الإتصال ينفي القصد الذي تقوم به هذه الجريمة أيضاً لأنه وطبقاً للقواعد العامة يجب أن يكون القصد الجنائي معاصراً للنشاط الإجرامي. [65] ص 231

غير أن المشرع قد انتبه إلى النتائج التي تترتب على مثل هذه الحالة، إذ من السهل على الجاني أن يدعي أن الاتصال قد تم عن طريق الخطأ، ومن ثم البقاء فيه، مما يعني أن القصد الجنائي إذا كان لا ينهض في الفرض السابق عن جريمة الاتصال (الدخول) غير المشروع فإن الدخول بطريق الخطأ إلى النظام ومن ثم البقاء فيه مع علمه بعدم مشروعية الاتصال بطريق الخطأ يجعل القصد وارداً في الصورة الثانية أي جريمة البقاء. [63] ص 189

• الإرادة:

جريمة البقاء داخل نظام المعالجة الآلية للمعطيات جريمة عمدية يتطلب لتحقيقها اتجاه إرادة الجاني إلى عدم قطع الاتصال، بمعنى أن تتجه إرادة الجاني إلى إبقاء الاتصال مع النظام وهو يعلم بأنه ليس له حق البقاء.

- مدى ضرورة توافر القصد الجنائي الخاص:

لا يبدو من نص المادة 394 مكرر أن المشرع يتطلب وجود نية خاصة حتى تقوم جريمة البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات وأنه يكتفي بقيامها توافر القصد العام بعنصريه العلم والإرادة ويرى غالبية الفقه أن الدخول وكذا البقاء غير المصرح به يتحققان عندما يكونان بدون رضا صاحب النظام، وقد وقفت محكمة باريس في القرار الذي أصدرته في 05/ أفريل / 1994 والمتعلق بالبقاء غير المصرح به في الأنظمة [26] ص 167 بأن البقاء يكون "بدون حق ومع معرفة السبب" وعليه يخلص هذا الرأي إلى أن الغش يكون عند معرفة الشخص بغياب حق الدخول أو البقاء في الأنظمة وعليه فالمشرع الجزائري الذي سار على نهج التشريع الفرنسي، لم يتطلب توافر نية خاصة كما هو عليه الحال في التشريعات الأخرى كالتشريع الأمريكي والبرتغالي والفرنلندي اللذين سبق الإشارة إليهما وعلى هذا الأساس فجريمة البقاء داخل نظام المعالجة الآلية للمعطيات جريمة عمدية لا يتطلب لتحقيقها قصد خاص.

2-3-2-1-2 الركن المعنوي للجريمة في صورتها المشددة.

لقد شدد المشرع الجزائري عقوبة البقاء داخل نظام المعالجة الآلية للمعطيات في إحدى حالتين: الأولى إذا ترتب على الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة، والثانية إذا ترتب على البقاء تخريب نظام اشتغال المنظومة.

وفي هذه الحالة لا يشترط أن تكون النتيجة المترتبة على البقاء مقصودة لأن هذا غير معقول فالمشرع الجزائري نص على جريمة الاعتداء العمدي على المعطيات بنص المادة 394 مكرر 1.

وعلى هذا الأساس لكي تتحقق هذه الجريمة لا يشترط أن تكون عمدية وإنما يشترط أن توجد بين هذا الظرف المشدد والبقاء غير المشروع داخل النظام علاقة سببية، بمعنى أن حذف أو تغيير المعطيات وكذا تخريب نظام اشتغال المنظومة كان نتيجة لوجود إتصال غير مشروع بالنظام دون أن تكون هذه النتيجة مقصودة.

فإذا كان الأصل أن الفاعل لا يقصد أن يتحقق الظرف المشدد كنتيجة لجريمة البقاء، فإن القصد الجنائي العام هو المفترض في هذه الصورة كأثر مترتب على الجريمة، والمسؤولية عن النتيجة المشددة هي مسؤولية غير عمدية تقوم عن طريق الخطأ. [06] ص 202

4-2-1-2 العقوبات المترتبة على جريمة البقاء داخل نظام المعالجة الآلية للمعطيات.

لقد اقر المشرع الجزائري نوعين من العقوبات في هذا القسم وهي عقوبات أصلية وأخرى تكميلية، وبما أنه سوف نتناول العقوبات التكميلية في فرع مستقل فسيتم الاقتصار على العقوبات الأصلية للجريمة سواء في صورتها البسيطة أو المشددة.

1-4-2-1-2 عقوبة جريمة البقاء في صورتها البسيطة:

- وفقا لنص المادة 394 مكرر تكون عقوبة جريمة البقاء عن طريق الغش إلى نظام المعالجة الآلية للمعطيات هي "الحبس من ثلاثة (3) أشهر إلى سنة والغرامة من 50.000 إلى 100.000 دج" ومن خلال نص المادة نلاحظ أن المشرع الجزائري قد منح القاضي سلطة تقديرية في اختيار العقوبة المناسبة، بحسب الحالة المعروضة عليه.

- عقوبة جريمة البقاء في صورتها البسيطة وفي حالة استهدافه للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

طبقا لنص المادة 394 مكرر 3 والتي جاء فيها أنه "تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد".

نلاحظ من خلال نص المادة أن المشرع الجزائري شدد العقوبة وفي حالة إستهدافها للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، وهذا نظرا للأهمية البالغة لهذه المعطيات، كون أن الاعتداء عليها يشكل مساسا بالاقتصاد الوطني هذا من جهة، ومن جهة ثانية فإن حساسية هذه المعطيات وخاصة المعطيات التابعة لمؤسسة الدفاع الوطني كونها تمس بأمن الدولة ككل تحتاج إلى مثل هذا النص، وعليه تصبح جريمة البقاء داخل نظام المعالجة الآلية للمعطيات في حالة استهدافه للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام هي "الحبس من 6 ستة أشهر إلى 2 سنتين والغرامة من 100.000 إلى 200.000 دج

- عقوبة جريمة البقاء المرتكبة من قبل الشخص المعنوي:

وفقا لنص المادة 394 مكرر 4 " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل 5 خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وعليه يعاقب الشخص المعنوي في حالة إرتكابه لجريمة البقاء في صورتها البسيطة بـ $5 \times 100.000 = 500.000$ دج".

- عقوبة جريمة البقاء المرتكبة من قبل الشخص المعنوي وفي حالة استهدافه للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

فوفقا لما جاء في نص المادة 394 مكرر 3 التي تضاعف من العقوبة في حالة ما إذا كانت المعطيات تابعة لمؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، ووفقا أيضا لنص المادة 394 مكرر 4 والتي جاء فيها أنه في الحالة التي ترتكب فيها الجريمة من قبل شخص معنوي فإن العقوبة المقررة له هي مضاعفة الحد الأقصى للغرامة إلى 5 خمس أضعاف وعليه: تصبح عقوبة جريمة البقاء المرتكبة من قبل الشخص المعنوي وفي حالة استهدافه للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، هي $100.000 \times 2 \times 5 = 1.000.000$ دج.

2-1-2-2 عقوبة جريمة البقاء في صورتها المشددة:

تشدد عقوبة جريمة البقاء وفقا لنص المادة 394 مكرر فقرة 2 في حالتين:

- عندما يترتب على البقاء حذف أو تغيير لمعطيات المنظومة:

- وفقا لنص المادة 394 مكرر فقرة 2" تضاعف العقوبة إذا تترتب على ذلك حذف أو تغيير لمعطيات المنظومة"، وعليه ففي حالة ما إذا نتج عن البقاء حذف أو تغيير لمعطيات المنظومة تكون العقوبة" الحبس من 6 ستة أشهر إلى 2 سنتين والغرامة من 100.000 إلى 200.000 دج".
- في حالة ارتكاب الجريمة من قبل شخص معنوي:

وفقا لنص المادة 394 مكرر 4 والتي تنص صراحة على مضاعفة الحد الأقصى للغرامة إلى 5 خمس مرات العقوبة المطبقة على الشخص الطبيعي في حالة ارتكابه نفس الجريمة وعليه تصبح العقوبة هي " $200.000 \times 5 = 1.000.000$ دج"

- إذا تترتب على جريمة البقاء حذف أو تغيير لمعطيات منظومة تابعة للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام:

وفقا لنص المادة 394 مكرر 3 حدد المشرع الجزائي مقدار مضاعفة العقوبة إلى الضعف وعليه يحكم القاضي وفقا لسلطته التقديرية بالعقوبة التالية "الحبس من 1 سنة إلى 4 سنوات والغرامة من 200.000 إلى 400.000 دج"، وهذا وفقا لملاسات القضية وخطورة المجرم.

- إذا ارتكبت الجريمة من قبل الشخص المعنوي وفي حالة استهدافه للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

فوفقا لما جاء في نص المادة 394 مكرر 3 التي تضاعف من العقوبة في حالة ما إذا كانت المعطيات تابعة لمؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، ووفقا أيضا لنص المادة 394 مكرر 4 والتي جاء فيها أنه في الحالة التي ترتكب فيها الجريمة من قبل شخص معنوي فإن العقوبة المقررة له هي مضاعفة الحد الأقصى للغرامة إلى 5 خمس أضعاف وعليه: تصبح عقوبة جريمة البقاء المرتكبة من قبل الشخص المعنوي في حالة استهدافه للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، هي $200.000 \times 5 = 1.000.000$ دج.

- عندما يترتب على جريمة البقاء تخريب نظام اشتغال المنظومة .

- وفقا لنص المادة 394 مكرر 3 "وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 100.000 إلى 150.000 دج".

نلاحظ من خلال نص المادة سالفة الذكر أن المشرع الجزائري شدد العقوبة إلى الضعف إذا ترتب على جريمة البقاء تخريب نظام اشتغال المنظومة، أمّا عن الغرامة المقررة فنلاحظ أنه احتفظ بالحد الأدنى للغرامة هي 50.000 دج و شدد من الحد الأقصى.

- في حالة ارتكاب الجريمة من قبل شخص معنوي :

وفقا لنص المادة 394 مكرر 4 والتي تنص صراحة على مضاعفة الحد الأقصى للغرامة إلى 5 خمس مرات فتصبح العقوبة: $5 \times 1.500.000 = 750.000$ دج.

- إذا ترتب على جريمة الدخول تخريب نظام اشتغال منظومة تابعة للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

وفقا لنص المادة 394 مكرر 3 نلاحظ أن المشرع الجزائري قد نص على المضاعفة وعليه تصبح العقوبة "الحبس من 1 سنة إلى 4 سنوات والغرامة من 100.000 إلى 300.000 دج".

- ذا ارتكبت الجريمة من قبل شخص معنوي وإستهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

فوفقا لما جاء في نص المادة 394 مكرر 3 التي تضاعف من العقوبة في حالة ما إذا كانت المعطيات تابعة لمؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، ووفقا أيضا

لنص المادة 394 مكرر 4 والتي جاء فيها أنه في الحالة التي ترتكب فيها الجريمة من قبل شخص معنوي فإن العقوبة المقررة له هي مضاعفة الحد الأقصى للغرامة إلى 5 خمسة أضعاف وعليه: تصبح عقوبة جريمة الدخول المرتكبة من قبل الشخص المعنوي وفي حالة استهدافه للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام هي: $150.000 \times 5 \times 2 = 3.000.000$ دج.

ولهذا نشير إلى مسألة في غاية الأهمية وهي حالة الاجتماع المادي للجرائم، بمعنى في الحالة التي يرتكب فيها الشخص جريمة الدخول غير المشروع بالإضافة إلى جريمة البقاء غير المشروع.

فهنا طبقا لنص المادة 33 و[57]34 قانون العقوبات الجزائري فإنه يحكم بالعقوبة الأشد بمعنى يحكم بنفس العقوبة في حالة ما إذا قام الشخص بإرتكاب جريمة دخول غير مشروع فقط أو في الحالة التي يرتكب فيها الشخص جريمة البقاء غير المشروع فقط أي في الحالة التي يكون فيها الدخول مشروع.

وعليه كان على المشرع الجزائري أن يحكم في حالة البقاء غير المشروع داخل النظام بعقوبة أشد من عقوبة الدخول غير المشروع داخل نظام المعالجة الآلية للمعطيات، لأن جريمة البقاء يمكن أن يترتب عنها أخطارا أكثر من جريمة الدخول كون أن المشرع طالما أنه متصل بالنظام فهو أقدر على إرتكاب جرائم أخرى أكثر خطورة كالتلاعب بالمعطيات أو تخريب النظام...

2-2 الجرائم الماسة بالمعطيات:

ينصب هذا النوع من الجرائم على المعطيات بإعتبارها المحور الأساسي الذي تدور حوله المعلوماتية، والتي تمثل المعالجة الآلية للبيانات والمعلومات.

وجرائم الإعتداء على المعطيات إما أن تتحقق في الفرض الذي تكون فيه المعطيات متصلة بالنظام وهنا تتحقق جريمة الإعتداء العمدي على المعطيات داخل نظام المعالجة الآلية للمعطيات بمعنى تتحقق الجريمة في الحالة التي تكون فيها المعطيات جزء من نظام المعالجة الآلية للمعطيات وتتحقق أيضا جرائم الإعتداء على المعطيات في الفرض الذي تكون فيه المعطيات قد انفصلت عن النظام، وهنا تتحقق جريمة التعامل بالمعطيات سواء المعطيات المتحصلة من جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، أو المعطيات التي تصلح لأن ترتكب بها جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات .

وعليه سوف نتناول جريمة التلاعب بالمعطيات في المطلب الأول، أما في المطلب الثاني فسوف نتناول جريمة التعامل بالمعطيات بكتا صورتها.

1-2-2 جريمة التلاعب بالمعطيات:

لقد جرم المشرع الجزائري هذه الجريمة حماية للمعطيات المتواجدة داخل النظام المعلوماتي.

1-1-2-2 الركن الشرعي:

لقد نص المشرع الجزائري على جريمة التلاعب بالمعطيات وفقا لنص المادة 394 مكرر 1 "يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام معالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

ونجد بذلك أن المشرع الجزائري قد تأثر بالمشرع الفرنسي الذي نص على جريمة التلاعب بنص المادة 323-3 [59] ، وبعض التشريعات العربية كالنشرع الإماراتي في مادته السادسة [10] ، حيث نجد أن المشرع الفرنسي نص عليها بعد جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات وقد أثرا لمشرع الجزائري عدم النص على هذه الأخيرة نظرا للتشابه الكبير بينها وبين جريمة التلاعب بالمعطيات، ويصعب في كثير من الأحيان التمييز بينهما وقد يعتقد البعض أن نص المادة 394 مكرر 1 المتعلقة بإدخال أو تعديل أو محو البيانات تعالج مسألة تزوير المستندات المعالجة آليا، لأن المادة تتحدث عن التغيير والتعديل في المعطيات وبالتالي في حالة تثبيت هذه المعطيات وإخراجها من الحاسب الآلي تشكل ما يعرف بالمستندات.

وهذا كون أن المستند المعالج آليا قد يكون في داخل النظام وقد يكون خارجه وفي الحالتين يمكن أن يخضع للتزوير، وبالتالي فلا يمكن القول بخضوع المستند إذا كان خارج النظام للنصوص التقليدية لجريمة التزوير، وتطبيق النص المتحدث على تزوير المستندات أو البيانات

المخزنة في النظام [44] ص 124، يترتب على ما سبق عدم إمكانية تطبيق نص المادة 394 مكرر 1 قانون العقوبات الجزائري على جريمة التزوير المعلوماتي.

وعليه فعلى المشرع الجزائري أن يجرم تزوير المعطيات المخزنة في نظام المعالجة الآلية والمستندات المعالجة معلوماتيا شريطة أن يكون من الممكن استخدام المحرر أو الوسيط الذي تم تزويره لممارسة حق أو تصرف، وأن يصلح لإثبات حق أو تصرف له آثار قانونية مثلما جاء فيكل منالنتشريع الفرنسي، [31] ص 150 وكذا التشريع الإماراتي في مادته الرابعة. [10]

فالمشرع الفرنسي قد حسم الجدل في قانون العقوبات الفرنسي لسنة 1992 والمعمول به وذلك في المادة 1/441 منه التي توسعت في مفهوم المحرر الذي يقع عليه التزوير، حيث أصبحت تشمل إلى

جانب المحرر بشكله التقليدي كل وسيط آخر للتعبير عن فكرة ويشمل ذلك بطبيعة الحال الأقراص المغنطة والأسطوانات المدمجة، وغيرها من وسائط تخزين المعلومات، ويشترط القانون أن يكون من الممكن استخدام المحرر أو الوسيط الذي تم تزويره لممارسة حق أو تصرف أو أن يصلح لإثبات حق أو تصرف له آثار قانونه.

2-1-2-2 الركن المادي:

باعتبار أن الركن المادي لأي جريمة من الجرائم المادية يتكون من السلوك الإجرامي والنتيجة الإجرامية والعلاقة السببية بينهما فسوف نتناول السلوك الإجرامي ثم النتيجة الإجرامية.

1-2-1-2-2 السلوك الإجرامي.

يتمثل النشاط الإجرامي لهذه الجريمة في أفعال الإدخال، أو المحو أو التعديل ويكفي توافر إحداها لقيام الجريمة، فلا يشترط اجتماعها معاً، ولذلك فإن السلوك الإجرامي لهذه الجريمة موضوعه محدد وهو الاعتداء على المعطيات في نظام المعالجة الآلية للمعطيات، أي البيانات التي أدخلت لمعالجتها وتحولت إلى معطيات عبارة عن رموز إشارات.

فالجريمة في هذا الفرض تقع على المعطيات أي البيانات التي تمت معالجتها دون المعلومة ذاتها، ولذلك يخرج من نطاق هذه الجريمة، البيانات التي لم تعالج بعد ولم تدخل إلى نظام المعالجة الآلية كذلك البيانات التي دخلت إلى النظام لكن لم تبدأ بعد أي خطوة في معالجتها، وكذلك المعلومات التي انفصلت عن النظام وسجلت على شريط ممغنط. [25] ص 91

وعليه فالنص يحمي المعلومات المعالجة، أو التي في طريقها إلى المعالجة بأن اتخذت خطوة أكثر في مراحل معالجتها وسنوضح هذه الأفعال تباعاً.

– الإدخال: Input:

يقصد به إضافة معطيات جديدة على الدعامة - الشيء المادي- الخاص به سواء كانت خالية أم يوجد عليها معطيات من قبل، وهذه الجريمة تقع عادة بمعرفة المسؤول عن القسم المعلوماتي، والذي يسند إليه وظائف المحاسبة والمعاملات المالية لأنه يكون في أفضل وضع يؤهله لإرتكاب هذا النمط من التلاعب غير المشروع. [24] ص 364

و إدخال بيانات غير معتمدة في نظام معلومات الحاسب أو تحريف البيانات المعتمدة المراد إدخالها هو أكثر أساليب إرتكاب الإحتيال الإعتمادي بساطة وأمناً وأكثر أشكاله وقوعاً، حتى ليشكل ما يقع بإستخدامه أكثر من نصف إجمالي حالات الإحتيال المعلوماتي. [28] ص 58

ومن الصور العملية لإدخال معلومات مصنعة، قيام المسؤول المعلوماتي في المنشأة بضم مستخدمين غير موجودين بالفعل أو قيامه بالإبقاء على مستخدمين تركوا الوظيفة بالفعل .

ومن التطبيقات القضائية في هذا الشأن قيام ميرمج يدعى "THOMSON" و الذي كان يعمل لدى أحد البنوك بالكويت بعمل برنامج ترتب على إثره توافر طرق إحتيالية وإعطائهم أمر بتحويل كميات من حسابات العملاء المسجلة على الحاسب الآلي، والتي لم يقم العملاء بعمليات سحب عليها منذ فترة طويلة، وذلك لصالح حسابات أخرى ثم عاد إلى إنكلترا بعد إنتهاء عمله وقام بفتح حساب له وحول رصيد الحسابات إلى حسابه بإنكلترا وكشف أمره وتمت محاكمته وإدانتته. [4] ص 198

– فعل الإزالة:

الإزالة سلوك إجرامي يقصد به محو جزء من المعطيات المسجلة على دعامة، أو الموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة [66] ص 383، وعملية إزالة المعطيات هي عملية لاحقة على عملية إدخال المعطيات، فالإزالة تقتض الوجود السابق للإدخال. [26] ص 182

– فعل التعديل:

يقصد بتعديل المعطيات تغيير المعطيات الموجودة داخل نظام لمعالجة الآلية للمعطيات أو إستبدالها بمعطيات أخرى، كما يقصد به قيام الغير ممن لا يملك الحق الكافي إحداث تغيير في المعلومات بتعديلها. [25] ص 95

ونشير إلى أن فعل التعديل نصت عليه كل من المادة 394 مكرر 1 قانون العقوبات الجزائري وكذلك المادة 323-3 قانون العقوبات الفرنسي ولم تتناول المادة الرابعة من اتفاقية بودابست السالفة الذكر سلوك التعديل بالتجريم، وإنما تناولت الإضرار بالمعطيات عموماً، وهو ما

يتضمن التعديل المؤدي إلى ضرر إضافة إلى المحو، التعطيل والإتلاف والطمس وفقاً لما جاء في المادة الرابعة [13] ، وتختلف هذه الأفعال الثلاثة عن بعضها البعض، فالتعديل هو النشاط الذي يقوم به الجاني ويكون محددًا بغاية معينة، أو نتيجة محددة فالجاني يسعى من وراء نشاطه تحقيق نتيجة محددة، فيتخذ من الوسائل ما يعتقد أنها توصله إلى غايته، أو من الممكن أن توصله إلى تحقيق غايته، إذا ففي فعل التعديل الهدف محدد وكذلك الوسيلة مدروسة ومحددة والتعديل ممكن أن يكون بالإضافة (الإدخال) أو المحو (الإزالة) وممكن أن يكون بهما معاً ، ومثال ذلك إذا كانت غاية الجاني من التعديل أن يحصل مثلاً على مستند أو محرر يخالف المحرر أو المستند الأصلي المحفوظ في ذاكرة الحاسب الآلي، فإن

ذلك ممكن أن يتحقق إمّا بحذف المعلومات أو البيانات فقط قبل أن يتم إستخراج المحرر أو المستند من وحدة الإخراج، أو أن يتم بالأمرين بمعنى يقوم الجاني بحذف بيانات أو معلومات أو حتى فقرات من برنامج ويستبدلها ببيانات أو معلومات أو فقرات من برنامج آخر وذلك بإضافتها بدلا مما تم حذفه.

أمّا إذا تم فعل الإدخال عن طريق إدخال بيانات إلى نظام خال، فهنا لا يتحقق التعديل. ويختلف فعل التعديل عن المحو رغم أنه قد يبدو لأول وهلة أن التعديل، لا يمكن أن يكون إلا بالمحو، أي محو المعلومات أو البرامج والبيانات لكن الأصح هو أنه إذا كان الجاني قد باشر نشاطه من أجل محو المعلومات أو البيانات فإن الأمر حينئذ يكون مجرد محو، أمّا إذا كان محوا انتقائيا ففي هذه الحالة يتحقق فعل التعديل وليس المحو. [63] ص ص 150 ، 151

وتعديل المعطيات المخزنة في نظام المعالجة الآلية للمعطيات قد يشمل تعديل المعطيات فقط وقد يشمل تعديل البرامج.

فالتلاعب في المعطيات بتعديلها تتحقق إمّا في مرحلة الإدخال [15] ص 104 ، أو في مرحلة الإخراج وهي المرحلة التالية لإعطاء الأمر بإخراج المعطيات والسابقة على عملية الإخراج . [22] ص 442

لأنه في مرحلة الإخراج لا يمكن خلالها تعديل المعطيات لكون المعلومات بعد إعطاء الأمر بإخراجها تخرج عن سيطرة من يريد إجراء التعديل عليها، كون أنها تصبح خارج نظام المعالجة وبالتالي لا يمكن تطبيق النص القانوني عليها.

وعليه فنص المادة 394 مكرر 1 يشمل المعطيات التي يتم تعديلها قبل أو أثناء إدخالها، أو تخزينها في نظام المعالجة الآلية للمعطيات وقبل المرحلة السابقة على إخراجها. [15] ص 101

وكانت التوصية الصادرة عن المجلس الأوروبي والمتعلقة بالجرائم المعلوماتية قد فرقت بين التعديلات التي تؤدي إلى نتائج سلبية تتعلق بحالة المعطيات والبرامج، وبين التعديلات غير المصرح بها والتي لا تؤدي إلى إحداث مثل هذه النتائج، بل قد تساعد على تحسين أي من المكونات المنطقية للحاسب الآلي ولنظامه، وتضمنت التوصية بندا يطالب بإدراج التعديلات الأولى ضمن القائمة الأساسية للجرائم المعلوماتية، بينما تدرج التعديلات الثانية في القائمة الاختيارية، لكن القوانين لم تأخذ هذه التفرقة بعين الاعتبار، وقام معظمها بتجريم التعديل مطلقا، وإن اختلفت التشريعات في العبارات التي استخدمتها في هذا المجال. [26] ص 181

وهذه الأفعال التعديل، المحو، الإضافة وردت في نص المادة 394 مكرر 1 على سبيل الحصر ويترتب على ذلك أنه إذا تحققت النتيجة المتمثلة في التلاعب بالمعطيات نتيجة فعل من غير الأفعال السابقة لا يخضع هذا الفعل إلى نص التجريم سالف الذكر، لأن هذا الفعل خرج عن الأفعال السابقة كفعل التخريب مثلا.

ونشير كذلك إلى أن المشرع الجزائري لم يحدد الوسيلة التي يتم عن طريقها التلاعب، وعليه تتحقق الجريمة بأي وسيلة كانت، سواء عن طريق الإصابات الفيروسية .

حيث شهد العالم في السنوات الأخيرة تصاعدا في الإصابات الفيروسية، خاصة بعد إنتشار إستخدام الانترنت والاعتماد على البريد الإلكتروني الذي يشكل مناخا ملائما لإنتشارها، ومن أبرز الفيروسات التي تستخدم للإعتداءات على معلومات وبرامج الحاسب الآلي فيروس حصان طروادة: TORJAN HORSE وهو برنامج يتمتع بقدرته الفائقة على الانتقال داخل البرنامج الأصلي، ليعمل أثناء التشغيل بحيث يؤدي إلى تعديل البرنامج، أو تغيير ومحو المعلومات وتدميرها وكذلك من أخطر الفيروسات فيروس الحب " love You " انتشر في شهر أيار 2000 عبر البريد الإلكتروني ويعتمد مبدأ عمل هذا الفيروس على الانتشار عبر البريد الإلكتروني إلى سجل العناوين الموجودة في دفتر العناوين في برنامج "OTLOK" من مايكروسوفت مسببا أضرار متعددة ، لتدمير بعض أنواع الملفات ومحاولة تنزيل ملف باب خلفي باسم (VIN . BUGSFISX. EXE) من موضع انترنت محدد إلى جهاز المصاب، وسرقة وإرسال كلمات السر الخاصة ببرنامج البريد الإلكتروني. [29] ص ص 101، 100 ، و الفيروس هو برنامج معلوماتي أعطي تسمية فيروس لتشابهه مع الفيروس البيولوجي من حيث الانتقال والتكاثر ووظائفه التدميرية للأنظمة المعلوماتية والقدرة على تعديل البرامج الأخرى التي يرتبط بها كما يستطيع الفيروس التمييز بين البرامج السليمة وغيرها. [30] ص 234 ، أو عن طريق برامج معدة مسبقا لذلك، أو عن طريق ما يعرف بالقنابل و هي نوعان :

-القنبلة المنطقية: وهي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة، ويتم وضعه في شبكة المعلومات، بهدف تحديد ظروف أو حالة النظام بغرض تسهيل تنفيذ عمل غير مشروع ومن الأمثلة الواقعية على ذلك، قيام احد العاملين في ولاية من الولايات الأمريكية بوضع قنبلة منطقية في نظام الكمبيوتر الخاص بها، الأمر الذي أدى إلى تخريب هذا النظام.

- القنبلة الزمنية: هي قنبلة تنطلق أو تنفجر في زمن وتاريخ محدد من السنة بمعنى أنها مرتبطة بالزمن، فيمكن إدخالها في برنامج وضبطها لكي تنفجر. مثلا يوم 2009/08/15 على الساعة الرابعة، وذلك بغرض تحويل نقود من حساب شخص معين إلى آخر ومثال ذلك، قيام شخص يعمل في نظم المعلومات في فرنسا بوضع قنبلة زمنية بدافع الانتقام بعد فصله بحيث تنفجر بعد 06 أشهر من رحيله ويترتب على ذلك إتلاف كل البيانات المتعلقة بها. [02] ص 53

2-2-1-2-2 النتيجة الإجرامية:

لقد سبق توضيح أن النتيجة الإجرامية بالنسبة لجريمة الدخول أو البقاء داخل نظام معالجة آلية للمعطيات، تقتصر على الخطر، ولا يتطلب المشرع تحقق نتيجة إجرامية كحدوث ضرر ما بمعنى أنها من جرائم الخطر.

لكن من خلال نص المادة 394 مكرر 1، التي تتعلق بجريمة التلاعب بالمعطيات يظهر أنها من جرائم الضرر وليس الخطر، كونها من الجرائم التي يتطلب لتمامها تحقق نتيجة معينة هي الضرر الذي يحدث نتيجة لأحد السلوكات الإجرامية المحددة على سبيل الحصر، إما التعديل أو المحو أو الإضافة. بمعنى أن جريمة التلاعب بالمعطيات هي جريمة مادية .

وهذه النتيجة هي نفسها النتيجة الإجرامية التي يترتب عليها تشديد العقوبة في جريمة الدخول أو البقاء المنصوص عليها في نص المادة 394 مكرر فقرة 2، ووجه الخلاف كما سبق الإشارة إليه هو أن جريمة التلاعب بالمعطيات جريمة عمدية بعكس جريمة الدخول أو البقاء في صورتها المشددة فتكون غير عمدية، وكذلك كون أن جريمة التلاعب تتم بعد دخول أو بقاء مصرح به أو غير مصرح به، أمّا عن جريمة الدخول أو البقاء غير المصرح به فلا تتحقق إلا إذا كان الدخول أو البقاء غير مشروع.

3-1-2-2 الركن المعنوي:

جريمة التلاعب بالمعطيات جريمة عمدية يتطلب لتحقيقها توافر القصد الجنائي العام، دون القصد الجنائي الخاص.

1-3-1-2-2 القصد الجنائي العام:

كما سبق وأشرنا فإن جريمة التلاعب بالمعطيات، جريمة عمدية تقوم على القصد الجنائي العام بعنصريه العلم وإرادة.

- العلم:

يجب أن يعلم الجاني بأنه يقوم بإدخال أو إزالة أو تعديل غير مصرح به على معطيات الحاسب الآلي، حيث يجب أن يعلم بأن المعلومات التي يعتدي عليها هي ملك لغيره، وبالتالي لا تتحقق الجريمة إذا ما قام الشخص بارتكاب أفعال من شأنها محو أو تعديل أو إضافة معلومات هي في حقيقتها تابعة له.

كذلك لا تتحقق الجريمة في الفرض الذي عدل وغير في معطيات خاصة بجهة أخرى، سواء كان شخص طبيعي أو معنوي معتقدا أن المعطيات خاصة به.

- الإرادة:

لا بد أن تتجه إرادة المتهم إلى إقتراف تلك الأفعال المحو، التعديل، الإضافة بغض النظر عن الباعث الذي من أجله اتجهت إرادة المتهم لإرتكاب فعل الاعتداء عن طريق التلاعب بها سواء كان الدافع هو الانتقام أو بغرض الكسب المادي أو بغرض إثبات القدرة والتفوق على النظام.

ولا يشترط أن يكون القصد محددًا، إذ يستوي لقيام الجريمة في القانون الجزائي أن يكون القصد محدد بمعطيات معينة، فلا فرق بين أن يقع القصد على معطيات أو أخرى، فالمعطيات كلها سواء في الحماية

ولا يشترط أن يكون القصد الجنائي مباشرًا أي أن تكون إرادة الجاني قاطعة في اتجاهها لإحداث النتيجة السابقة، بل يكفي لقيام العمد أن تتخذ الإرادة شكل القبول، أي قبول النتيجة وهذا ما يسمى بالقصد غير المباشر. [65] ص 231

2-3-1-2-2 مدى ضرورة توافر القصد الجنائي الخاص:

وفقا لنص المادة 394 مكرر 1 نجد أن المشرع لا يتطلب قصد خاصا لدى الجاني لكي تقوم جريمة التلاعب بالمعطيات، وإنما يكفي بتوافر القصد العام ويستفاد هذا من عدم النص في المادة على نية خاصة، ذلك أن القصد الخاص يتطلب وجود غاية محددة لاكتمال القصد.

وعليه فجريمة التلاعب بالمعطيات المنصوص عليها بنص المادة 394 مكرر 1 هي جريمة عمدية، يتطلب لتوافرها تحقق القصد العام بعنصره العلم والإرادة، ولا يتطلب قصد خاص، غير أن الأمر مختلف في قوانين أخرى، حيث تفرق بعض القوانين بين المعطيات في الحماية فتبسطها على أنواع منها فقط دون أنواع أخرى.

من الأمثلة على ذلك التشريع الفدرالي الأمريكي لسنة 1986 حيث تنص المادة 1030 (أ) التي تجرم الإلتلاف العمدي وغير المصرح به لمعلومات يحتوي عليها حاسب آلي تابع لحكومة الوم.أ وإدارتها، أو حاسب آلي غير تابع للحكومة إلا أنه يستخدم من قبلها أو لصالحها، ووسع قانون حماية بنية المعلومات القومية لعام 1986 من دائرة المعلومات محل الحماية، فأضاف إلى ما سبق المعلومات الموجودة بالحسابات المستخدمة من طرف المؤسسات الاقتصادية التابعة للحكومة وتلك المستخدمة في التجارة والإتصالات بين الولايات أو بين الولايات والدول الأخرى. [26] ص 185

4-1-2-2 العقوبات المقررة لجريمة التلاعب بالمعطيات:

-إن العقوبة المقررة لجريمة التلاعب بالمعطيات وفقا لنص المادة 394 مكرر 1 هي "الحبس من (6) أشهر إلى (3) سنوات وبغرامة مالية من 500.000 دج إلى 2.000.000 دج.

ونلاحظ أن المشرع الجزائري قد جعل من عقوبة جريمة التلاعب تفوق بكثير عقوبة جريمة الدخول أو البقاء في صورتها المشددة، وهذا كون ان جريمة التلاعب بالمعطيات جريمة عمدية.

في حالة ارتكاب الجريمة من قبل شخص معنوي:

وفقا لنص المادة (394 مكرر 4) تضاعف عقوبة الحد الاقصى للغرامة إلى 5 مرات في حالة ارتكاب الجريمة من قبل شخص معنوي على هذا الأساس تكون عقوبة الشخص المعنوي الذي يقوم بالتلاعب بالمعطيات هي $10.000.000 = 5 \times 2.000.000$ دج.

-في حالة إستهداف الجريمة للدفاع الوطني أو المؤسسات والهيئات العامة أي الخاضعة للقانون العام: فوفقا لنص المادة 394 مكرر 3 تضاعف العقوبة إذا إستهدفت الجريمة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام.

وعليه فتكون للقاضي هنا سلطة تقديرية في تقرير العقوبة الملائمة "الحبس من سنة (1) إلى (6) ستة سنوات وبغرامة مالية من 1.000.000 دج إلى 4.000.000 دج".

-في حالة ارتكاب الجريمة من قبل شخص معنوي واستهدف بذلك الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

وفقا لنص المادتين 394 مكرر 3 و394 مكرر 4 فهنا إذا ما عرضت القضية على القاضي فيقوم بتحديد عقوبة ملائمة.

بحيث وفقا لنص المادة 394 مكرر 3 فالقاضي له سلطة في مضاعفة العقوبة ، كما لو أن شخصا طبيعيا قام بإرتكاب الجريمة ضد مؤسسة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام وبعد ذلك ووفقا لنص المادة 394 مكرر (4) تضاعف عقوبة الحد الأقصى للغرامة إلى 5 مرات في حال ارتكاب الجريمة من قبل شخص معنوي.

وعليه يحكم على الشخص المعنوي في حالة ارتكابه لجريمة تلاعب بالمعطيات هي ملك لمؤسسة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام بغرامة تقدر بـ:

$$20.000.000 = 2 \times 5 \times 2.000.000 \text{ دج}$$

2-2-2 جريمة التعامل في المعطيات:

لقد وفر المشرع الجزائري حماية جنائية للمعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات من خلال المادتين 394 مكرر و 394 مكرر 1 كما سبق بيانه، وبالإضافة إلى هذا وفر المشرع الجزائري حماية جنائية للمعطيات خارج النظام، من خلال النص على جريمة التعامل بالمعطيات في كلتا صورتها باعتبار أنها معطيات غير مشروعة.

والغاية أو الغرض من هذا التجريم هو غرض وقائي نظرا لخطورة هذا النوع من التعامل، فالغاية من تجريم التعامل بالمعطيات التي يمكن أن ترتكب بها إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات هي منع وقوع الضرر الذي يترتب عليها.

أما التعامل بالمعطيات الناتجة عن إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات فالغاية من تجريمها هو التخفيف من أثارها قدر الإمكان.

1-2-2-2 جريمة التعامل بالمعطيات التي تصلح لأن ترتكب بها جرائم معلوماتية.

هذه الجريمة تتعلق بالمعطيات التي يتم تجميعها، أو نشرها، أو الاتجار فيها، وغير ذلك من الأفعال التي يتم بها ارتكاب إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

1-1-2-2-2 الركن الشرعي:

تطرق المشرع الجزائري إلى جريمة التعامل في المعطيات التي تصلح لأن ترتكب بها إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات في نص المادة 394 مكرر 2 فقرة 01 وجاء فيها أنه "يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 (مليون) إلى 5.000.000 (خمسة ملايين) دج، كل من يقوم عمدا أو عن طريق الغش بما يأتي.

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

نلاحظ من خلال هذا النص أن المشرع الجزائري قد جرم مجموعة من الأفعال الخطيرة التي بواسطتها يمكن أن تحدث جرائم أخرى يمكن أن تكون أكثر خطورة، وهذه الأفعال تسبق عملية إستعمال هذه المعطيات في ارتكاب الجريمة، ولا يشترط أن تقع هذه الأفعال مجتمعة حتى يمكن القول بوقوع الجريمة، بل يكفي أن تقع إحداها فقط.

والتعامل بالمعطيات هنا يقصد به كل سلوك له علاقة بإعداد وإنتاج المعطيات غير المشروعة وكل سلوك يكشف عن وجود صلة معينة بين شخص ومعطيات غير مشروعة، هذه الصلة تتمثل في القيام بأحد أنواع السلوك التي نصت عليها المادة 394 مكرر 2 والتي يطلق عليها مصطلح التعامل [26] ص 200 ، ونشير إلى أن قانون العقوبات الفرنسي كان أكثر توسعا في ذلك عندما اقر في مادته 323-3-1. [59] ، أن التعاملات المجرمة يمكن أن تقع على تجهيزات أو أدوات أو على برنامج معلوماتي، أو على كل المعطيات المصممة والمعدة لإرتكاب واحدة أو أكثر من الجرائم السابقة سواء الدخول أو البقاء، أو إعاقة أو إفساد النظام، أو التلاعب بالمعطيات.

وعليه فالمشرع الفرنسي توسع ليشمل بذلك كل الوسائل التي يمكن استخدامها في جرائم المعطيات، سواء كانت وسائل مادية وهذا لاستخدامه مصطلح "تجهيزات أو أدوات"، أو استعمال وسائل غير مادية لإستخدامه مصطلح "البرامج والمعطيات"، لكنه قام بالحد من هذا التوسع عندما تطلب أن تكون تلك الوسائل معدة ومصممة لإرتكاب واحدة أو أكثر من جرائم المعطيات، بينما نجد أن المشرع الجزائري الذي لا يشترط أن تكون المعطيات معدة لإرتكاب الجريمة، وإنما يكفي أن تكون صالحة أو قابلة لأن ترتكب بها إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وبذلك يكون قد انتهج المسلك الذي أخذت به إتفاقية بودابست في مادتها السادسة. [13]

وعلى هذا الأساس يمكن القول أن التشريع الجزائري يعمل على التوفيق بين الإتفاقية الدولية للإجرام المعلوماتي والتشريع الفرنسي، مع إستبدال مصطلح "الحصول من أجل الإستخدام" المنصوص عليه في الإتفاقية بمصطلح "التجميع" المنصوص عليه في القانون الفرنسي، ويتضح من خلال نص المادة 394 مكرر 2 بأن محل جريمة التعامل في معطيات صالحة لأن ترتكب بها جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات هي المعطيات المخزنة، أو المعالجة أو المرسله عن طريق منظومة معلوماتية، طالما أن الهدف هو إستعمالها لإرتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

2-1-2-2-2 الركن المادي.

سوف نتناول السلوك الإجرامي الذي بمقتضاه يمكن أن ترتكب جريمة التعامل بالمعطيات التي تصلح لأن ترتكب بها جرائم معلوماتية، وكذا النتيجة الإجرامية المترتبة عنها.

-السلوك الإجرامي:

تضمنت المادة 394 مكرر 2 من قانون العقوبات الأفعال التي يمكن أن تستخدم بها المعطيات لأجل ارتكاب جريمة معلوماتية، وهذه الأفعال التي تسبق إستعمال تلك المعطيات في ارتكاب الجريمة هي:

• التصميم: (Design):

يعتبر أول عملية في سلسلة التعامل في المعطيات وإخراجها إلى الوجود، وهو العمل الذي يقوم به المختصون في هذا المجال كالمبرمجين، ومصممي البرامج كون أنهم المخول لهم القيام بهذه الجريمة بحكم عملهم وإختصاصهم، ومثال هذه الجريمة تصميم برنامج إختراق. [67] ص 62، أو فيروس الحاسب الآلي.

ويوجد هناك من يدافع عن مصممي البرامج التي قد تستخدم لإرتكاب الجرائم المعلوماتية كون أن هذه البرامج تكشف عن الثغرات الأمنية في الأنظمة المعلوماتية، وإمكان إصلاحها إلا أن هذه المبررات غير مقبولة، لأن سلبيات البرامج الخبيثة أكثر من إيجابياتها ، [67] ص 63، ويزداد الأمر خطورة إذا تعلقت الجريمة بالمعطيات المرتبطة بالحياة الخاصة كتلك المتعلقة بالحالة الصحية للشخص أو المتعلقة بوضعه المالي، أو معلومات ذات صلة بانتماءاته السياسية أو الحزبية أو الدينية فمن شأن هذا أن يشكل خرقا للحياة الخاصة.

ولذلك لا يمكن الإحتجاج بتجريب بعض البرامج التي تم تقسيمها بهدف إيجاد أنظمة حماية أمنية قوية، فإن مثل تلك الأعمال تقتصر على المؤسسات الأمنية المتخصصة، والتي تجرب برامجها على أنظمة تتبعها، أو على برامج خبيثة أطلقها القراصنة، وذلك بهدف توفير الحماية منها. [06] ص 227

• بحث: (CONSIDERATION):

يقصد بالبحث، البحث في كيفية تصميم هذه المعطيات وإعدادها، وليس مجرد البحث عن هذه المعطيات، ولذلك جاءت عبارة البحث بعد عبارة التصميم مباشرة، وإن كان النص قد جاء عاما. [26] ص 201

ومن خلال نص المادة 394 مكرر 2 فقرة 1 يتبين أن المشرع الجزائري يجرم البحث في معطيات مخزنة أو معالجة أو مرسله عن طريق منظومة معلوماتية، يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

فمصطلح البحث يشمل كيفية تصميم المعطيات وإعدادها لترتكب بها جريمة، أو البحث عن معطيات وبرامج يمكن أن ترتكب بها جريمة، لكون البحث عن معطيات جاهزة ، يكون أسهل من البحث عن كيفية إعدادها، وذلك في ظل العديد من المواقع التي يمكن أن توفر تلك المعطيات.[06] ص 227

• التجميع: (Collage).

و يقصد به القيام بجمع العديد من المعطيات التي يمكن أن ترتكب بها جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، وخطورة هذا الفعل تكمن في تجميع مجموعة من المعطيات، مما يدل على وجود عدد كبير من المعطيات فلا يكون التجميع بمعطى واحد.

ونشير فقط أن مصطلح التجميع هذا، وعلى الرغم من أنه يظهر للعيان بأنه لا يؤدي إلى أضرار جسيمة مقارنة بالأفعال الأخرى المنصوص عليها في نفس المادة، حيث أن الجاني هنا لا يقوم إلا بتجميع عدد من المعطيات، إلا أن الواقع أثبت جسامه الأضرار الناتجة عن هذا الفعل والأمثلة على ذلك عديدة.[67] ص 63

وتجدر الإشارة إلى أن المشرع الفرنسي إستعمل مصطلح الحيازة، بدلا من التجميع في نص المادة 323-3-1 فالحيازة هنا يمكن أن تكون لعدد من المعطيات، كما يمكن أن تكون لمعطى واحد، بعكس التجميع، وتجدر الإشارة إلى أن مصطلح الحيازة هو الأنسب كون أن الجريمة يمكن أن ترتكب بمعطى واحد، وعلى هذا الأساس إذا ارتكبت الجريمة بمعطى واحد فإن القاضي الفرنسي يمكن له معاقبة الفاعل وتطبيق الجزاء عليه، أما القاضي الجزائري إذا عرضت عليه قضية مشابهة فإنه لا يستطيع تطبيق الجزاء على الجاني لأن المشرع يشترط أن يكون حائزا لمعطين أو أكثر.

ونشير كذلك أن المشرع الجزائري وبإستعماله لمصطلح التجميع لا يشترط أن تكون هناك نية إستخدام المعطيات المتحصل عليها، بعكس الاتفاقية الدولية للإجرام المعلوماتي في نص المادة السادسة منها، والتي تشترط هذا الشرط وبالتالي تضيق من توفير الحماية من جهة كما يصعب إثباته من جهة أخرى وهو أمر منتقد في نظري.

• التوفير Met a disposition:

يعتبر فعل التوفير من الأفعال المجرمة بنص المادة 394 مكرر 2 فقرة 1، فمن يقوم بتوفير معطيات يمكن من خلالها أن ترتكب إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات، يعتبر مقترفا لجريمة تعامل بالمعطيات تصلح لإرتكاب جريمة.

إلا أنه يلاحظ من خلال ترجمة نص المادة 394 مكرر 2 [68] ، باللغة الفرنسية أن معنى العبارة في سياق نص المادة تعني أي إشكال للوضع تحت التصرف، والمراد بذلك هو تقديم المعطيات وإتاحتها لمن يريد، وهو ما يتوافق مع نص المادة السادسة من إتفاقية الإجرام المعلوماتي أي جعلها في متناول الغير ، ووضعها تحت تصرفه، والفرق بين التوفير والتجميع هو أنه في التوفير تتعدى حيازة المعطيات والتصرف فيها الشخص الذي يقوم بتجميعها إلى أشخاص آخرين لهم إمكانية إستخدامها.

يظهر التوفير بشكل جلي في حالة إنشاء مواقع، أو نشر معلومات على الشبكة المعلوماتية بغرض الإتجار في الأشخاص، ترويج أفكار الإرهاب، أو بغرض ترويج المخدرات أو بغرض الاعتداء على الحياة الخاصة، أو إنشاء مواقع تقوم بتحريض القصر على الفسق والدعارة . [04] ص 132

ونشير إلى أن المشرع الجزائري رغم أنه نص على فعل التوفير في المادة سالف الذكر ورغم أنه نص في المادة 394 مكرر 7 على أنه يعتبر محل لجرائم المساس بأنظمة المعالجة الآلية للمعطيات هي نظم المعالجة بالإضافة إلى المواقع ، ورغم خطورة هذه الجرائم إلا أن المشرع الجزائري لم ينص عليها ضمن جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

وعليه فعلى المشرع الجزائري أن يقتدي بالتشريع الإماراتي [10] ، وينص على هذه الجرائم لأنها تتسبب في حدوث أضرار جسيمة خاصة إذا تعلق الأمر بإنشاء مواقع ، والأمثلة على ذلك عديدة، [67] ص 185 ، ولا يهم الغرض من وراء إنشاء الموقع سواء كان بقصد توفير الإختراق أو توفير أرقام بطاقات الائتمان الخاصة بالغير أو عناوين بريدهم الإلكتروني يخضع لنص المادة 394 مكرر 2 فقرة 1 ، لأن برامج الإختراق أو بطاقات الائتمان ...يمكن أن ترتكب بها إحدى جرائم المساس بأنظمة المعالجة كجريمة الدخول أو البقاء داخل نظام المعالجة بصورتها البسيطة أو المشددة ، وكذلك يمكن أن ترتكب بها جريمة التلاعب بالمعطيات، لكن إذا كان الهدف من إنشاء المواقع هو التحريض على الفسق والدعارة ، أو بهدف ترويج المخدرات أو ترويج الأفكار المناهضة للدين.... فنجد أن نص المادة على هذه الأفعال يستدعي البحث في النصوص التقليدية ، لأنّ المشرع قيد التعامل بالمعطيات التي تصلح لأن ترتكب بها جرائم القسم السابع مكرر.

وعليه فالشخص الذي يحوز برامج إختراق، أو برامج تحتوي على كيفية تصميم الفيروسات أو أرقام بطاقات الائتمان...دون أن تتجه نيته إلى بيعها ، أو عرضها على الغير من الجمهور، فهنا يكون مرتكب للجريمة لقيامه بفعل التجميع ، لأنّ الحيازة في يده ولكن إذا قام بإحراز هذه المواد بقصد البيع أو التوزيع أو العرض على الغير ، ففي هذه الحالة يكون مرتكب لجريمة التعامل بالمعطيات لقيامه بفعل التوفير.

• النشر: Diffus.

يعد فعل النشر من الأفعال التي نصت عليها المادة 394 مكرر2، ويعد النشر من أخطر الأفعال التي ترتكب بها جريمة التعامل بكتنا صورتها، سواء جريمة التعامل بالمعطيات التي ترتكب بها إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات، أو جريمة التعامل بالمعطيات الناتجة عن إحدى هذه الجرائم، ففعل النشر: يقصد به إذاعة المعطيات محل الجريمة، وتمكين الغير من الإطلاع عليها، وذلك عن طريق مختلف الوسائل التي يتصور النشر بها، مهما كانت طبيعتها. [26] ص 203

ويقصد به كما جاء في الإتفاقية الدولية للإجرام المعلوماتي التوزيع الإيجابي للمادة المجرمة. [69] ص 124

ويختلف فعل النشر عن فعل التوفير في أن هذا الأخير يتطلب من الشخص البحث عن المعطيات التي يمكن من خلالها ارتكاب إحدى جرائم المعلوماتية، أو تحميلها وتوفيرها للآخرين بخلاف النشر، الذي يفترض فيه أن المعلومات متوفرة لدى الشخص، أو الموقع الذي يتبعه لكنه لا يكتفي بتوفيرها للآخرين إنما يقوم بنشرها بإحدى وسائل النشر. [06] ص 230

ويستمد هذا الفعل خطورته في كون أنه كفيل بأن ينقل المعطيات إلى عدد كبير من الأشخاص، مما يجعل احتمال إستعمال تلك المعطيات في ارتكاب الجرائم بنسبة كبيرة، مقارنة بالأفعال الأخرى من بينها التوفير، لأنه إذا كان التوفير بمقابل فالنشر على الأغلب يكون بدون مقابل، ويعتبر فعل النشر من بين أكثر الأفعال رواجاً في العالم والأمثلة على النشر عديدة. [04] ص 160

و نشير إلى المشرع الجزائري قد وافق بذلك الإتفاقية الدولية للإجرام المعلوماتي التي نصت على النشر في نص المادة 6 سالف الذكر، أما المشرع الفرنسي فلم ينص على النشر.

• الإتجار: (COMMERCIALISATION):

يقصد بالإتجار كل أنواع التعاملات التي تقع على المعطيات الصالحة لإرتكاب جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في القسم السابع مكرر من قانون العقوبات الجزائري .

وما يميز فعل الإتجار عن فعل التوفير والنشر هو أنه إذا كان فعل النشر على الأغلب لا يتم بمقابل، لأنه يتحقق في الحالة التي يوصل فيها الجاني هذه المعطيات بأي وسيلة إلى عدد كبير من الأشخاص ، سواء كان هناك إتفاق سابق بينهم أو لم يوجد.

وفعل التوفير هو تقديم وإتاحة ووضع هذه المعطيات تحت تصرف الغير بمقابل أو بدون مقابل فإن فعل الإتجار يتحقق بتقديم هذه المعطيات للغير بمقابل، ولا يشترط أن يكون هذا المقابل نقديا، بل قد يكون عينيا أو قد يتمثل في خدمات أو غير ذلك.

فالمشرع الجزائري بالنص على الأفعال السابقة أراد أن يجرم كل أنواع التعاملات سواء كانت بمقابل أو بدون مقابل، ونشير إلى أن المشرع الفرنسي في نص المادة 323-3-1 سالف الذكر، لم ينص على هذا الفعل وإنما نص على مصطلح الاستيراد، ونجد أن الإتفاقية الدولية للإجرام المعلوماتي وفقا للمادة (06) المشار إليها أنفا نصت على فعل البيع والاستيراد، أما المشرع الجزائري فقد نص على فعل الإتجار.

ويعتبر هذا الفعل في نظر الكثيرين هو الأنسب لأنه أكثر ملاءمة من مصطلح البيع والاستيراد وبالتالي يكون الاتجار المجرم، هو الاتجار بالمعطيات التي يمكن أن ترتكب بها إحدى جرائم المعلوماتية، ومن ذلك الاتجار ببرامج الاختراق التي تمكن الجناة من الولوج داخل أنظمة المعالجة أو الاتجار بالفيروسات والبرامج التي تمكن من إتلاف المعطيات، أو تساعد على تخريب النظام... ونشير إلى أن الإتجار نص عليه القانون الأمريكي. [06] ص 231

- النتيجة المترتبة:

يبدو من خلال الأفعال السابقة سواء التصميم، أو البحث، أو التجميع، أو التوفير، أو النشر، أو الاتجار، أنها يمكن أن تحقق ضررا فعليا سواء على النظام، أو على المعطيات التي يتضمنها هذا النظام.

والمشرع الجزائري في تجريمه لهذه الأفعال الواردة على سبيل الحصر، لم يجرمها بوصفها أفعالا خطيرة تؤدي إلى نتائج خطيرة، وإنما جرمها لأنه يحتمل أن تؤدي إلى ضرر بمعنى أنه لو تركت الأمور تسير بشكل عادي كما لو ترك الأفراد وشأنهم في تجميع وتصميم هذه البرامج دون حظر قانوني لكان إحتمال إرتكاب هذا النوع من الجرائم وارداً بنسبة كبيرة.

والمشرع الجزائري من منطلق أنه يعتبر المصالح المتعلقة بالمعطيات مصالح هامة، على هذا الأساس وفر هذه الحماية المسبقة للمعطيات، وحتى تتوقف الآثار عند مرحلة الخطر ولا تتعدها إلى مرحلة الضرر.

2-2-2-2 جريمة التعامل في معطيات متحصلة من جريمة:

إضافة إلى تجريم المشرع الجزائري للتعامل بالمعطيات التي يمكن أن ترتكب بها إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات، فقد جرم أيضا التعامل في معطيات متحصلة من جريمة.

1-2-2-2-2 الركن الشرعي:

يتمثل الركن الشرعي للجريمة بنص المادة 394 مكرر 2 فقرة 2 حيث نصت على أنه "يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمداً أو عن طريق الغش بما يأتي.

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

ويلاحظ من خلال نص المادة أن المشرع الجزائري قد تطرق إلى تجريم أفعال الحيازة أو النشر أو الإفساد أو إستعمال المعطيات المتحصل عليها من إحدى جرائم المساس بأنظمة المعالجة، ولقد جرم المشرع الجزائري التعامل بهذه المعطيات لأنها غير مشروعة، كون أنها متحصلة من جريمة فهي إذن ناتج إجرامي هذا من جهة، ومن جهة أخرى كون أن التعامل بها سوف يوسع من دائرة الأشخاص الذين يمكن أن يتعاملوا مع هذه المعطيات، ويستخدمونها إستخداماً غير شرعي لأي غرض كان، سواء كان الغرض هو معاودة إستعمالها لإرتكاب إحدى جرائم المساس بأنظمة المعالجة، أو كان الغرض استعمالها لغرض آخر كمقاطعة الأديان أو إرتكاب إحدى الجرائم السالفة الذكر عند الحديث عن التعامل بالمعطيات الصالحة لإرتكاب جريمة.

ومثال ذلك أن يقوم بعض المجرمين نتيجة اختراقهم للنظام المعلوماتي لبعض الأشخاص بإختراق نظام مملوك لشخصية مهمة ومعروفة داخل المجتمع، كأن يكون سياسياً أو فناناً بالحصول على بعض المعلومات المهمة التي تتعلق بحياته الخاصة، كإنتمائه السياسية أو بعض الصور التي لا يود أن يطلع عليها أحد، ثم يقوم الجناة بحيازة هذه المعطيات بغرض بيعها إلى الغير أو التشهير أو التهديد...

فهنا تقوم الجريمة لأن الغرض غير محدد في نص المادة 394 مكرر 2 فقرة 2، المهم أن تكون المعطيات متحصلة من جريمة وإستعمالها لأي غرض كان.

2-2-2-2-2 الركن المادي.

سوف نتناول السلوك الإجرامي الذي بمقتضاه يمكن أن ترتكب جريمة التعامل بالمعطيات المتحصلة من جريمة معلوماتية، وكذا النتيجة الإجرامية المترتبة عنها.

-السلوك الإجرامي.

يقوم الركن المادي لهذه الجريمة على العديد من الأفعال وهي الحيازة، أو النشر، أو الإفشاء، أو استعمال المعطيات المتحصل عليها من إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في القسم السابع مكرر.

• الحيازة: Possession.

يعتبر فعل الحيازة أول فعل منصوص عليه في نص المادة 394 مكرر 2 فقرة 2، وهذا أمر منطقي كون أن أول فعل يقع بعد ارتكاب إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات هو حيازة المعطيات المتحصلة من الجريمة، وعليه يتحقق فعل الحيازة بسيطرة الجاني على هذه المعطيات.

المقصود بالحيازة كأصل عام هي: السيطرة الفعلية على كل شيء يجوز التعامل فيه مع إنصراف النية إلى استعمال حق عليه، ومن ثم فهي استعمال سلطة فعلية على الشيء فهي تتفق في مظهرها الخارجي مع استعمال حق عليه، وللحيازة عنصران أحدهما مادي قوامه الأعمال المادية التي ينطوي عليها استعمال الحق المحوز، والآخر معنوي قوامه نية الحائز في القيام بهذه الأعمال لحساب نفسه أو في عبارة أخرى نية الإستئثار بالحق الذي يستعمله. [70] ص 15

ويقصد بالحيازة: الاستئثار بالشيء على سبيل التملك والاختصاص دون الحاجة إلى الإستيلاء المادي عليه، وهذه السيطرة إما أن تكون سيطرة مطلقة: ومعها يستطيع الحائز أن يفني المعطيات أو يعدل فيها أو يستعملها.

كما قد تكون سيطرة محدودة: تمكنه فقط من الانتفاع بالمعطيات أو إستغلالها في وجه معين وعليه يكفي القول بتوافر السيطرة مجرد إستطاعة هذه السيطرة دون عقبات واقعية تحول بين الشخص وبين التمتع بها، و الأمثلة على ذلك عديدة.

• الإفشاء:

يعد فعل الإفشاء هو الفعل الثاني الذي نصت عليه المادة 394 مكرر 2 فقرة 2، ويستمد فعل الإفشاء خطورته من كونه يجعل هذه المعطيات المتحصلة عن جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات في متناول أكثر من شخص.

ولا يتطلب قانون العقوبات الجزائري حدوث نتيجة معينة من وراء فعل الإفشاء، بل يجرم هذا الأخير في حد ذاته، والمشرع الجزائري يعاقب كل من يقوم بعملية الإفشاء، ولا يشترط في هذا الشخص أن يكون مؤتمنا على هذه المعطيات دون غيره، سواء بمقتضى وظيفته أو عقد ما، إنما هو

شخص تحصل على هذه المعطيات بطريقة غير مشروعة، وأراد المشرع أن يمنعه من إفشاءها أو نشرها سعياً لتضييق إنتشارها.

وتجدر الإشارة إلى أن المشرع الفرنسي وكذلك الاتفاقية الدولية للإجرام المعلوماتي لم تنص على هذا الفعل عند تجريمها للتعامل بالمعطيات المتحصلة من جريمة.

ولذلك يمكن القول أن المشرع الجزائري بالنص على هذا الفعل قد إنتهج نهج القانون الأمريكي. [26] ص 208 ، وقوانين بعض الدول العربية كالقانون الإماراتي في مادته الثانية. [10]

• النشر:

يعد فعل النشر وفقاً لنص المادة 394 مكرر 2، هو الفعل الوحيد المشترك بين صورتين جريمتين التعامل بالمعطيات فنجد النص في الفقرة الأولى المتعلقة بالتعامل بالمعطيات التي يمكن أن ترتكب بها إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات، والفقرة الثانية المتعلقة بالتعامل بالمعطيات المتحصل عليها من إحدى جرائم المساس بأنظمة المعالجة .

فالمادة 394 مكرر 2 جاءت عامة بحيث لم تشترط عدد معين من المرات التي يتم النشر فيها حتى يقال بالنشر، كما لم تحدد قيد على النشر كأن يكون بمقابل مثلاً، ولم تذكر المادة وسيلة معينة يتم بها النشر، وبالتالي فهو يتم بكل وسيلة يمكن تصورها، سواء كانت تقليدية أو معلوماتية فيستوي إذا أن يكون النشر عن طريق الإنترنت أو الأقراص... أو أن يكون عن طريق الكتابة أو الرسم.

فالنشر يستمد خطورته من كونه سيجعل المعطيات في يد عدد غير محدد من الأشخاص، ومثال ذلك أن فعل النشر يتحقق وتقوم الجريمة بذلك حتى ولو ارتكب الشخص فعل النشر لمرة واحدة، المهم أن تكون هذه المعطيات محل النشر ناتجة عن جريمة، وهذا هو الشرط الذي وضعه المشرع للقول بوقوع الجريمة، ومن قبيل هذا الفعل قيام الكراكرز باختراق مواقع خصومهم والحصول على كلمة المرور أو من ثم القيام بنشرها على الجميع إضراراً بأصحابها. [06] ص 236

• الإستعمال:

يعتبر فعل الإستعمال أخطر سلوك يمكن أن يقع على المعطيات المتحصلة من جريمة، وذلك لأنه إذا كانت أفعال الحيازة والإفشاء والنشر تعتبر أفعال خطيرة ونظراً لخطورتها قام المشرع بتجريمها فإن فعل الإستعمال يعتبر أخطر هذه الأفعال لأن الجاني إنتقل بهذا الفعل من مجرد احتمال إرتكاب الجريمة إذا ما تحققت الأفعال السابقة إلى اقترافها فعلاً إذا تحققت فعل الإستعمال.

و في تحديد المقصود بالإستعمال قيل أنه الفعل الذي يستخدم به الفاعل الشيء إستخداما لا يجوز أن يصدر إلا من مالكه. [28] ص 289

ولم يشترط المشرع الجزائري تكرار الفعل حتى يقال بالاستعمال وإنما يتحقق الفعل ولو إستعمل لمرة واحدة، ومثال ذلك استخدام أرقام بطاقات الائتمان التي تم الحصول عليها نتيجة إرتكاب جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

- النتيجة الإجرامية :

واضح من نص المادة 394 مكرر 2 فقرة 2 أن الأفعال التي جاءت بها هذه المادة، والمتمثلة في الحيازة، والإفشاء، النشر، والاستعمال أنها أفعال يمكن أن يحدث عنها ضرر.

فالمشرع الجزائري عند تجريمه لهذه الأفعال جرمها لأنها أفعالا خطيرة يمكن أن تؤدي إلى ضرر فعلي، فهي تسمح بتوسيع دائرة المتعاملين بهذه المعطيات والتي هي في الأصل عبارة عن ناتج إجرامي فهي غير مشروعة، وعليه فالمشرع الجزائري في نص المادة سألفة الذكر أراد أن يوقف الآثار التي تحدثها هذه الأفعال عند مرحلة الخطر ولا تتعدها إلى مرحلة الضرر .

3-2-2-2 الركن المعنوي لجريمة التعامل بالمعطيات بصورتها.

جريمة التعامل في المعطيات جريمة عمدية، ويستفاد هذا من عبارة عمدا أو عن طريق الغش المنصوص عليها في المادة 394 مكرر 2.

- القصد الجنائي العام:

تعتبر جريمة التعامل في المعطيات جريمة عمدية، يتطلب حدوثها القصد الجنائي العام بعنصريه العلم والإرادة.

• العلم:

لا بد أن يعلم الجاني بأن المعطيات محل التعامل غير مشروعة، ولا بد أن يعلم أن الأفعال التي يقوم بها هي أفعال غير مشروعة وتهدد المصلحة المحمية بالخطر، وبالإضافة إلى هذا يجب أن يعلم في جريمة التعامل بالمعطيات المتحصلة من جريمة، أن هذه المعطيات هي عبارة عن ناتج إجرامي، وأنه لا يجوز له التعامل بها، وأن التعامل بها سوف يؤدي إلى حدوث أضرار وخيمة، وينتفي العلم في الفرض الذي لا يعلم فيه الجاني أن المعطيات ناتج إجرامي أو أنه لا يجوز له التعامل بها.

وفي جريمة التعامل بالمعطيات بغرض ارتكاب جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، يجب حتى تتحقق الجريمة أن يعلم الجاني أن هذه الأفعال محظورة من الناحية القانونية والأكثر من هذا، أن يعلم الجاني أن التعامل بهذه المعطيات ممكن أن ترتكب به إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

• الإرادة:

إضافة إلى عنصر العلم لا بد أن تتوافر الإرادة حتى يتحقق القصد الجنائي العام في جريمة التعامل بالمعطيات، ويجب أن تتجه الإرادة إلى ارتكاب جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، أو أن تتجه إلى التعامل بالمعطيات المتحصلة عن إحدى هذه الجرائم، وكذلك يجب أن تقتصر الإرادة على السلوك فحسب دون النتيجة الإجرامية.

- مدى ضرورة توافر القصد الجنائي الخاص:

كما سبق القول فإن جريمة التعامل بالمعطيات جريمة عمدية يتطلب لتحقيقها القصد الجنائي العام بعنصره العلم والإرادة، وإلى جانب هذا سوف نناقش إمكانية تطلب القصد الجنائي الخاص في كلتا صورتها.

• مدى ضرورة توافر القصد الجنائي الخاص في جريمة التعامل بالمعطيات المتحصلة من جريمة.

يظهر من خلال المادة 394 مكرر 2 أن جريمة التعامل بالمعطيات المتحصلة من جريمة هي جريمة عمدية لا يتطلب لقيامها توافر القصد الجنائي الخاص، كما هو الشأن بالنسبة لجريمة التعامل بالمعطيات الصالحة لإرتكاب جريمة، أمّا بشأن لفظ عن طريق الغش الذي أورده المشرع الجزائري بالإضافة إلى لفظ عمدا لا يعني أن الجريمة تتطلب قصد خاص.

وكان الأولى أن يكتفي بلفظ "عن طريق الغش"، كونه يعبر عن العمدية طالما أنه تم استخدام اللفظ في جريمة الدخول والبقاء وكذا جريمة التلاعب بالمعطيات. [26] ص 217

• مدى ضرورة توافر القصد الجنائي الخاص في جريمة التعامل بالمعطيات الصالحة لإرتكاب جريمة:

لا يكفي لقيام جريمة التعامل في معطيات صالحة لإرتكاب جريمة أن يتوافر لدى الفاعل القصد العام وحده، وإنما يلزم فضلا عن هذا القصد أن يتوافر لدى الفاعل القصد الخاص أي اتجاه العلم والإرادة إلى وقائع معينة لا تدخل في تكوين أركان الجريمة.

ويتحقق القصد الجنائي الخاص في التعامل بالمعطيات التي تصلح لأن ترتكب بها جريمة، ويتحقق ذلك بالتمهيد والإعداد لاستعمالها في ارتكاب الجريمة، وهي مسألة نفسية محضة، أما استعمال المعطيات في ارتكاب الجريمة فليست ركنا في هذه الجريمة، فقد لا يقوم أحد باستعمال هذه المعطيات ومع ذلك تقوم الجريمة. [06] ص 213

4-2-2-2 العقوبة المقررة:

- عقوبة جريمة التعامل بالمعطيات المرتكبة من قبل الشخص الطبيعي:

لقد جاء في نص المادة 394 مكرر 2 أنه "يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 (مليون) إلى 5.000.000 (خمسة ملايين) دج، كل من يقوم عمداً أو عن طريق الغش بما يأتي.

- 1- تصميم أو بحث أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة 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".

- عقوبة جريمة التعامل بالمعطيات المرتكبة من قبل الشخص المعنوي والمستهدفة للجهات العامة:

وفقا لنص المادة 394 مكرر 3 تضاعف العقوبة المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد، وعليه تصبح عقوبة جريمة التعامل بالمعطيات في هذه الحالة هي: الحبس من (4) أربعة أشهر إلى (6) ستة سنوات والغرامة من 2.000.000 (مليونين) إلى 10.000.000 (عشرة ملايين) دج .

$$50.000.000 = 2 \times 5 \times 5.000.000 \text{ دج .}$$

- عقوبة جريمة التعامل بالمعطيات المرتكبة من قبل الشخص المعنوي :

وفقا لنص المادة 394 مكرر 4 يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل (5) خمس مرات الحد الأقصى للغرامة المقررة

للشخص الطبيعي وعليه يعاقب الشخص المعنوي في حالة ارتكابه لجريمة التعامل بالمعطيات بـ $25.000.000 = 5 \times 5.000.000$ دج .

- عقوبة جريمة التعامل بالمعطيات المرتكبة من قبل الشخص المعنوي والمستهدفة للجهات العامة

وفقا لنص المادتين 394 مكرر 3 و 394 مكرر 4 يحكم على الشخص المعنوي في حالة ارتكابه لجريمة التعامل بالمعطيات موجهة ضد مؤسسة الدفاع الوطني أو إحدى الجهات العامة بالعقوبة التالية
 $50.000.000 = 5 \times 10.000.000$ دج .

3-2 الأحكام المشتركة بين جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات

تتشترك هذه الجرائم في أنها تقع على موضوع واحد هو نظام المعالجة الآلية للمعطيات الذي يعتبر الشرط الأساسي الذي يلزم تحققه للبحث في توافر أو عدم توافر الجرائم، ولقد تم شرح مفهوم هذا النظام في المبحث الأول من الفصل الأول أثناء تناول مفهوم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وعلى هذا لا داعي للتكرار.

هذا وقد أقر المشرع الجزائري مبدأ المعاقبة على الاتفاق الجنائي المجسد بأعمال مادية، بالإضافة إلى المعاقبة على الشروع في ارتكاب إحدى الجرائم التي تستهدف الأنظمة المعلوماتية، ولقد جعل المشرع الجزائري العقوبات التكميلية واحدة لكل هذه الجرائم، كما شدد العقوبة في حالة ارتكاب جريمة من هذه الجرائم من قبل شخص معنوي، أو في حالة استهدافها لجهات عامة، وهذا ما سوف نتناوله في المطالب التالية:

1-3-2 الأحكام المشتركة المتعلقة بالجريمة:

تتعلق الأحكام المشتركة المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بالعقاب على الاتفاق الجنائي المجسد بأعمال مادية، والعقاب على الشروع لإرتكاب هذه الجرائم، وسوف نتناول كل عنصر في فرع مستقل.

1-1-3-2 العقاب على الاتفاق الجنائي المجسد بأعمال مادية:

سنتطرق في هذا الفرع إلى أركان الجريمة.

1-1-1-3-2 الركن الشرعي:

لقد تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي المجسد بأعمال مادية بنص المادة 394 مكرر 5 ، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية، ولم يخضعها لأحكام المادة 176 قانون العقوبات والمتعلقة بتكوين جمعية أشرار. [68]

حيث نصت المادة 394 مكرر 5 على أنه "كل من شارك في مجموعة، أو في إتفاق تآلف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسد بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها".

وبهذا يكون المشرع الجزائري قد سار على النهج الذي أخذ به المشرع الفرنسي في مادته 323 / 4 [59]، وبعض التشريعات العربية كالتشريع الإماراتي في مادته (23) [10]، وكذا الاتفاقية الدولية للإجرام المعلوماتي في مادتها (11). [13]

لقد دار جدل كبير بين الفقهاء حول مدى ملازمة تجريم المشرع للاتفاق الجنائي فمنهم من يرى أن الاتفاق الجنائي عزم إجرامي، ومع ذلك لا يعتبر تجريمه إستثناء يرد على قاعدة عدم العقاب على مجرد العزم الإجرامي.

أما أنصار الرأي الثاني فيرون أن العقاب على الاتفاق الجنائي يعتبر خروجاً على القواعد العامة في العقاب، التي تقضي بأن العقاب لا يتقرر إلا بالنسبة للجرائم التامة، أو تلك التي تقف عند حد الشروع أو المحاولة، أي أن مبدأ العقاب يتطلب على الأقل البدء في نشاط إجرامي يرمي مباشرة إلى ارتكاب الجريمة، أما الأعمال التحضيرية فلا عقاب عليها.

ويستند أنصار الرأي الأول إلى أن المشرع لا يعاقب على الاتفاق الجنائي كخطوة للجريمة المتفق عليها، وإنما يعاقب عليه في حد ذاته كجريمة، وهذا يرجع إلى أنه في الاتفاق الجنائي يظهر العزم الجنائي الجماعي بمظهر خارجي مادي، لأن كل عضو فيه يعلن عزمه إلى سائر الأعضاء فتتحد إراداتهم على ارتكاب الجريمة.

كذلك كون أن الاتفاق الجنائي ظاهرة خطيرة تهدد الأمن العام تهديداً فعلياً، وأخيراً يراعي القانون في العقاب على الاتفاق الجنائي وجهة الجزاء لأنه يعاقب على تكوين الاتفاق الجنائي كما يراعي فيه وجهة الوقاية، فتكون نتيجة إحباط الاتفاق الجنائي فيحال بين الجناة وبين تحقيق خططهم الإجرامية. [26] ص 114

وبعبارة أخرى تكون نتيجة العقاب على الاتفاق الجنائي، وهو أن يقضي على الجريمة وهي في المهد وبالتالي يمارس القانون أسلوباً وقائياً من شر الجرائم المتفق عليها، والتي بدورها تمثل مشروعاً إجرامياً وضعت فيه جميع إمكانيات المتفقين.

أما أنصار الرأي الثاني فيستندون إلى أن تجريم الاتفاق سيحث الجناة على الإقدام على ارتكاب الجرائم المتفق عليها، ما دام العقاب واقع لأول بادرة بدت منهم وهي اتفاقهم كذلك في حالة المقارنة بين

خطورة الاتفاق الجنائي وخطورة الأعمال التحضيرية التي تصدر على شخص يسعى إلى ارتكاب الجريمة بمفرده، فالاتفاق الجنائي 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 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. [26] ص 115

وبالرجوع إلى نص المادة 4/323 من قانون العقوبات الفرنسي والمادة 394 مكرر 5 من قانون العقوبات الجزائري نرى أنهما تنبها لهذا النقد، فلم يوقما بتجريم مجرد العزم على الإعداد لجرائم المعطيات، وإنما تطلبا أن يكون هذا العزم مجسد بفعل أو عدة أفعال مادية، أي أنهما خرجا عن تجريم المرحلة النفسية إلى مرحلة تليها وهي التحضير للجريمة بوسائل مادية.

وبالتالي فنص المادتين يعتبر إستثناء على القاعدة العامة، والغرض من هذا النص هو تقرير نوع من الحماية المتقدمة والوقائية لنظم المعالجة الآلية للمعطيات ضد المخاطر التي تنشأ عن النشاط غير المشروع لبعض نوادي المعلوماتية، والتي قد تسهم بمعلوماتها الفنية في التحضير لإرتكاب الجرائم المشار إليها، وكذلك ضد قرصنة المعلوماتية، [18] ص 126، لكن كان على المشرع الجزائري أن يتبع نفس الاتجاه الذي اتخذه المشرع الفرنسي حيث إستبعد من النص بعض الجرائم كجريمة الدخول أو البقاء داخل نظم المعالجة الآلية للمعطيات. [12] ص 206

ولا بد من توافر الركن المادي والركن المعنوي حتى يمكن القول بمعاقبة الأعمال المادية التحضيرية.

2-1-1-3-2 الركن المادي.

إن الركن المادي في الجريمة التامة يقوم على ثلاثة عناصر وهي السلوك والنتيجة المادية غير المشروعة، والعلاقة التي تربط بين الفعل والنتيجة، وهي تتواجد مجتمعة، إلا حيث يعتد المشرع قانونا بالنتائج المادية التي يتسبب فيها السلوك في العالم الخارجي، وهو في بعض الأحيان يكتفي بالسلوك فقط، ويجرمه بغض النظر عما يترتب عليه من نتائج. [71] ص 58

- السلوك الإجرامي:

ولكي يتحقق السلوك الإجرامي في جريمة الاتفاق الجنائي لا بد من توافر ثلاثة عناصر فعل الاتفاق، وموضوع الاتفاق، بالإضافة إلى تعدد المتفقين.

• فعل الاتفاق:

الاتفاق هو إتحاد إرادتين أو أكثر وتكتلهما نحو موضوع معين، [71] ص 58 ، والاتفاق بطبيعته له مظهر مادي ملموس إذ يفترض تعبير كل واحد من أطرافه عن إرادته، بحيث يعلم بها زملاءه في الاتفاق فيتحقق لهم أن إرادتهم تسير في اتجاه واحد، وتتلاقى عند موضوع معين، والتعبير عن الإرادة يفترض ماديات كالقول الشفوي، أو العبارات الشفوية أو الإيماء إن كانت لها دلالة مفهومة، وإن الاتفاق يقوم بغض النظر عما إستغرقه انعقاد الإرادات من وقت قصير كان أم طويلاً، وسواء كان الاتفاق منظماً فيتخذ شكل "جمعية إجرامية" أو كان عارضاً مجملًا اقتصر أعضاؤه على مجرد العزم على جريمة معينة دون تعيين لكيفية تنفيذها، أو تحديد لدور كل واحد فيها. [72] ص 469

وهذا ما نستشفه من نص المادة 176 قانون العقوبات الجزائري "كل جمعية أو إتفاق مهما كانت مادته" فهذه المادة في تجريمها للاتفاق العام بتلاقي الإيرادات على ارتكاب الجريمة، أمّا المادة 394 مكرر 5 ، فتتطلب للعقاب على فعل الإتفاق أن يكون مجسداً بفعل أو عدة أفعال مادية، بمعنى يجب أن تتجسد في أفعال وأعمال مادية يكون القصد منها التحضير والإعداد لإرتكاب الجريمة كأن يقوم المتفقون بإقتناء برامج خبيثة كالفيروسات، أو برامج اختراق يتم من خلالها الدخول غير المشروع لأنظمة الحاسبات الآلية، أو إقتناء كتب تشرح كيفية القيام بتلك الجرائم ويجب التمييز بين الركن المادي لجريمة الإتفاق الجنائي والركن المادي للجريمة المتفق عليها وأن عدولهم عن تنفيذ الجريمة المتفق عليها لا يحول دون العقاب على جريمة الإتفاق الجنائي ، لأن هذا لا يمس الركن المادي الذي توافرت كل عناصره. [72] ص 473

• موضوع الاتفاق:

إن الإتفاق الجنائي يستمد صفته الجنائية في موضوعه، فإذا لم يكن لموضوعه صفة إجرامية فلا يعد الاتفاق جنائياً، فإنه يجب أن ينصب الاتفاق على جريمة هي جنائية أو جنحة أياً كان نوعها ، وبذلك يخرج عن نطاق الاتفاق الجنائي المخالفات بأنواعها. [71] ص 80

ويرى جانب من الفقه أن نص المادة 176 قانون العقوبات الجزائري الذي نص على الاتفاق الجنائي العام في الجنايات ضد الأشخاص والأموال ، يجرم الإتفاق المنصب على ارتكاب الجريمة، أو على الإعداد لها، بينما اقتصر نص المادة 394 مكرر 5 على جعل موضوع الاتفاق الإعداد لتلك الجرائم والتحضير لها فقط ولم ينص على الاتفاق على ارتكابها، وبالتالي وقع المشرع في السهو إذ كان يجب أن يجرم الاتفاق على ارتكاب الجريمة كذلك. [26] ص 117

بينما يري جانب آخر أن نص المادة 394 مكرر 5 قد حددت موضوع الاتفاق بالإعداد للتحضير لإرتكاب جريمة أو أكثر من الجرائم المنصوص عليها، وذلك ما يوحي بأن الاتفاق على الإعداد يشمل الاتفاق على ارتكاب الجريمة، لكون من يتفقون على شراء أو تجهيز برامج يتم من خلالها ارتكاب الجريمة إنما يعد ذلك جزء من اتفاقهم على ارتكاب الجريمة، وتؤكد ذلك الفقرة الأخيرة من النص والمتضمنة "وكان هذا التحضير مجسداً بفعل أو عدة أفعال مادية..."، فالأفعال المادية المشار إليها تدل على الإتفاق المسبق لإرتكاب الجريمة. [06] ص 147

ويجب أن يكون للإتفاق هدف إجرامي منذ البداية، فإذا لم يوجد هدف فلا تتحقق جريمة المساس بأنظمة المعالجة، مثل الاتفاق الذي يقوم على تأسيس ناد للتسلية. [21] ص 131

ونحن نتفق مع أنصار الرأي الأول فمن غير المعقول أن نجزم الاتفاق على الأعمال التحضيرية التي تسبق ارتكاب الجريمة، أي الإعداد لإرتكابها ولا نجزم الاتفاق المنصب على ارتكابها، وهذا ما أخذ به المشرع الفرنسي في نص المادة 4/323 من ق.ع. ف، حيث تجرم المادة مساهمة شخصين أو أكثر في ارتكاب أفعال مادية تحضيرية الهدف من وراءها ارتكاب إحدى الجرائم المنصوص عليها في المواد 1/323 إلى 3/323 من قانون العقوبات، والمختصة في الاعتداء على نظم المعالجة الآلية للبيانات.

ويجب أن يتخذ هذا النص صورة العمل التحضيري المادي ولا يختلط هنا العمل التحضيري مع البدء في التنفيذ الذي يتحقق به الشروع أو المحاولة في ارتكاب الجريمة أو المساهمة في الجريمة والإلما كانت هناك حاجة لمثل هذا النص. [18] ص 127

ومن الأمثلة على الأعمال التحضيرية المادية تبادل المعلومات اللازمة لتنفيذ الجريمة مثل الكشف عن رقم الكود، أو كلمة السر اللازمة للدخول إلى النظام أو شرح كيفية تجاوزها وكذلك كيفية استخدام قنبلة زمنية أو فيروس ما... [14] ص ص 32، 33

ويلاحظ أن المشرع الفرنسي يشدد العقوبة لكونه يبغى ردع مرتكب الجريمة المعلوماتية التي تقدر خسائرها بالملايير، فخروجا على القواعد العامة التي لا تجرم الأعمال التحضيرية المشرع الفرنسي جرم في هذا النص الأعمال التحضيرية المتعلقة بالجرائم المنصوص عليها في القانون. [12] ص 205

ووفقا للمادة 394 مكرر 5 قانون العقوبات الجزائري، إذا كان موضوع الاتفاق أعمال التحضير والإعداد لتلك الجرائم، فإن الاتفاق يكتسب صفته الجنائية ولو كانت الأعمال في ذاتها مشروعة فالإتفاق على كيفية تصميم المعطيات وتجميعها ونشرها هو مشروع في الأصل لكنه يصبح غير مشروع إذا كان الإتفاق على ذلك بنية استعماله في الجرائم التي تنص عليها المادة 394 مكرر 1 و2، والمشرع

الجزائري بمعاقبته على الأعمال التحضيرية التي تسبق البدء في التنفيذ، يعتبر خروج على القواعد العامة التي تقضي بأن العقاب لا يتقرر إلا بالنسبة للجرائم التامة أو تلك التي تقف عند حد الشروع أو المحاولة ، وتبعاً لذلك فإن نص هذه المادة يعتبر استثناء على القاعدة العامة الأمر الذي يؤكد الخطورة التي تتسم بها هذه الجرائم.

• التعدد الضروري للجناة.

جريمة الاتفاق الجنائي تتطلب تعددا ضروريا للجناة، والمشرع الجزائري لم يورد قيد على الحد الأقصى لهذا التعدد ، وإنما يكون شخصين أو أكثر، وهذا طبقاً لنص المادة 176 والمادة 394 مكرر 5، بحيث لا يمكن تصور تجسيد الاتفاق أو الجمعية في شخص واحد فقط، 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. [14] ص 37

ويستوي أن يكون أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي أو جماعة، كما يستوي أن يعرف أشخاص الاتفاق بعضهم كما في العصابة أو تكون مجرد مجموعة من الأشخاص لا يعرف أحدهم الآخر من قبل، ولكن اتفقوا فيما بينهم على القيام بالنشاط الإجرامي المشار إليه، المهم أن يتم الاتفاق بين شخصين على الأقل. [18] ص 128

ويجب أن نميز بين ما إذا كان أحد الطرفين يتمتع بمانع من موانع المسؤولية ، أو مانع من موانع العقاب.

فإذا كان في الإتفاق أحد الأعضاء يتمتع بمانع من موانع المسؤولية، كأن يكون صغير السن أو فاقد للإدراك بسبب جنون، وتناوله لمسكر فإنه يستبعد من الإتفاق لأن هذه الموانع يتمتع مع قيامها أو وجودها قيام المسؤولية الجنائية، ويقتصر أثرها على الشخص الذي يتعلق به المانع فقط، ولا يلحق هذا الأثر باقي المتفقين بمعنى أن الباقيين يسألون مساءلة جنائية عن فعل الاتفاق.

لكن في حالة ما إذا بقي بعد إستبعادهم عضوا واحدا مسؤول جنائيا، فلا عقاب على الاتفاق الجنائي لأن الاتفاق الجنائي هو اتحاد إرادتين فأكثر، ومنه إرادة شخص واحد مسؤول جنائيا غير كافية لتكوين جريمة الاتفاق الجنائي.

أمّا إذا كان في الاتفاق من هم معفون من المسؤولية لمانع من موانع العقاب عوقب الآخرون، حتى ولو بقي في الاتفاق الجنائي عضوا واحدا ذا إرادة، وذلك كون أن موانع العقاب لا تؤثر على قيام المسؤولية الجنائية، إنما يترتب عليه عدم توقيع العقاب على الجاني، لإعتبارات تتعلق به وحده، مثلا: أن

يقوم أحد المتفقين بالإبلاغ عن الجريمة فيستفيد لوحده بالإعفاء من العقاب حتى ولو كان في الاتفاق شخص واحد فقط فهنا الشخص الثاني يساءل مساءلة جزائية عن الفعل الذي قام به. [71] ص 70

ونشير فقط إلى أن جريمة الاتفاق الجنائي تشترك فيها جميع الجرائم الماسة بأنظمة المعالجة، التي نص عليها المشرع الجزائري في الباب السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.

3-1-1-3-2 الركن المعنوي:

جريمة الاتفاق الجنائي جريمة عمدية يجب لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة.

- القصد الجنائي العام:

نتناول كل من العلم والإرادة

• العلم:

يجب أن يعلم كل عضو في الاتفاق بماهية الفعل أو الأفعال موضوع الاتفاق ، وبمالها من خصائص يعتمد عليها المشرع في إضفاء الصفة الإجرامية عليها، أما بخصوص العلم بالصفة الإجرامية ذاتها فهذا مفترض على نحو لا يقبل إثبات العكس. [71] ص ص 87، 88

وبتعبير آخر من يجهل أن الغرض من الاتفاق هو ارتكاب جنائية أو جنحة أو التحضير لهما لا يعد القصد الجنائي متوفرا لديه، فمن يعتقد أن موضوع الاتفاق هو الاتجار في برامج حاسب آلي ومعطيات عادية ، ثم تبين أن الاتجار كان ببرامج خبيثة أو برامج اختراق ففي مثل هذا لا يعد القصد الجنائي متوفرا لديه، وذلك لإنقضاء علمه بموضوعه غير المشروع ومع ذلك بقي في الاتفاق. [26] ص 118

وفي حال قيام الاتفاق الجنائي بين شخصين فقط، فإن انعدام العلم لدى أحدهما، يؤدي إلى عدم قيام جريمة الاتفاق الجنائي وبالتالي انتفاء مسؤوليتهما معا.

• الإرادة:

بمعنى يجب أن تتوافر الإرادة الجادة للدخول في الاتفاق، وللقيام بالدور الذي سيعهد به إليه فالذي يدخل الإتفاق بقصد الوشاية ببقية المتفقين أو الإطلاع على أمرهم أو لمجرد العبث لا يعد القصد الجنائي متوفرا لديه لغياب الإرادة الجادة، ولا بد من توفر هذه الإرادة لدى شخصين على الأقل، وانتفاءها لدى أحدهما ينفي الجريمة عن كليهما. [71] ص 90

وعليه لا بد من توافر القصد الجنائي بعنصره العلم والإرادة حتى تتحقق هذه الجريمة، فيجب أن يتوفر لدى الجاني العلم بأنه عضو في جماعة إجرامية، ولا بد أن تتجه إرادته إلى تحقيق نشاط إجرامي معين، وهو العمل التحضيري وليس من الضروري هنا أن يكون عالما بنشاط الأعضاء الآخرين في المجموعة.

فإذا تحقق كل من الركن المادي والمعنوي يتعرض الجناة لعقوبة الاتفاق الجنائي المجسد بأعمال مادية، وهي حسب المادة 394 مكرر 5 نفس عقوبة الجريمة المراد ارتكابها وإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد، ويستوي في ذلك الأشخاص الطبيعيين والمعنويين. ونشير أيضا أنه إذا ساهم أعضاء الاتفاق في الجريمة التي يتم التحضير لها نكون أمام تعدد مادي للجرائم لأن الجريمة الأولى مستقلة عن الجريمة الثانية.

4-1-1-3-2 العقوبة المقررة للجريمة:

عقوبة الاتفاق الجنائي وفقا لنص المادة 394 مكرر 5 هي نفس العقوبة المقررة للجريمة ذاتها، بخلاف بعض التشريعات التي عاقبت على الاتفاق في جرائم المعلوماتية، بما لا يتجاوز عقوبة الجريمة ذاتها بشرط تحقق الجريمة محل الاتفاق، فإذا لم تتحقق الجريمة فتكون العقوبة بما لا يتجاوز نصف عقوبة الجريمة الأصلية وفقا للمادة 09. [73]

وبعض التشريعات الأخرى لا تعاقب على الاتفاق إلا إذا تحققت الجريمة وتكون العقوبة هي عقوبة الجريمة الأساسية وفقا للمادة 23. [10]

وبناء على ذلك فعقوبة الإتفاق على الإعداد لإرتكاب جريمة الدخول أو البقاء هي نفسها عقوبة جريمة الدخول أو البقاء، والأمر نفسه بالنسبة لباقي الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وذلك تكون.

- عقوبة الاتفاق الجنائي المجسد بأعمال مادية بغرض الإعداد لجريمة الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات هي:

"الحبس من ثلاثة (3) أشهر إلى سنة والغرامة من خمسون ألف (50.000 دج) إلى مائة ألف (100.000 دج)" في حالة إستهدافها لأنظمة الأفراد العاديين .

وتضاعف العقوبة في حالة إستهدافها لأنظمة مؤسسات الدفاع الوطني والمؤسسات الخاضعة للقانون العام لتصبح العقوبة المقررة من " (6) ستة أشهر إلى سنتين والغرامة من مائة ألف (100.000) إلى مائتي ألف (200.000 دج)" وهكذا بالنسبة لباقي الجرائم. [68]

2-1-3-2 العقاب على الشروع:

يهدف المشرع من سياسة التجريم والعقاب حماية الحقوق الأساسية من كل إعتداء يقع عليها وبينما نجد أن غالبية النصوص الجنائية تشترط وجود نتيجة ضارة، كما هو الشأن في جرائم القتل والسرقة أو النصب، فإن المشرع يعاقب في بعض الأحوال لمجرد ارتكاب أفعال تتضمن خطرا يهدد الحق الذي يحميه القانون، كالنصوص التي تعاقب على الاتفاق أو التحريض أو إحراز سلاح بدون ترخيص، فقانون العقوبات لا يهدف فحسب إلى منع الإضرار بتلك الحقوق، وإنما يرمي أيضا إلى حمايتها من الخطر الذي يتهدها. [74] ص 06

فالجرائم إذا على نوعين جرائم ذات ضرر وجرائم ذات خطر، ونظرا لأن الشروع يتنافى بطبيعته مع تحقق الضرر، لذلك فإنه يعتبر من قبيل الجرائم ذات الخطر، والواقع أن مجرد البدء في تنفيذ فعل بقصد ارتكاب جريمة ما يكون من شأنه أن يهدد الحق المعتدى عليه بخطر الجريمة التي شرع الجاني في ارتكابها.

وإذا كانت الجنايات هي المجال الأصلي لنظام الشروع نظرا لخطورتها، طبقا لنص المادة 30 قانون العقوبات فإن هذا النظام في الجرح لا يكون إلا في الخطيرة منها فيقرر ذلك بنص، وهذا ماجاء في نص المادة 31 قانون العقوبات الجزائري "المحاولة في الجنحة لا يعاقب عليها إلا بناء على نص صريح في القانون والمحاولة في المخالفة لا يعاقب عليها إطلاقا". [57]

وعليه سنتناول أركان الشروع ثم نتناول الشروع في الاتفاق الجنائي ثم العقوبة المقررة.

1-2-1-3-2 الركن الشرعي:

يعتبر الشروع في الجريمة مرحلة من مراحل ارتكابها تالية للتحضير لها، وسابقة على تمامها ولقد تعرض المشرع الجزائري للشروع في نص المادة 30 تحت عنوان المحاولة، كما جاء وفقا لنص المادة 31 قانون العقوبات الجزائري أن الشروع لا يكون في الجرح إلا بنص.

وقد قدر المشرع خطورة الجرائم الماسة بأنظمة المعالجة، فقرر خضوعها لنظام الشروع طبقا لنص المادة 394 مكرر 7 حيث جاء فيها "يعاقب على الشروع في ارتكاب الجرح المنصوص عليها في هذا القسم السابع من قانون العقوبات الجزائري بالعقوبات المقررة للجنحة ذاتها" بعدما قرر خضوعها لنظام الاتفاق الجنائي المجسد بأعمال مادية طبقا لنص المادة 394 مكرر 5.

ووفقا لنص المادة 394 مكرر 7 من قانون العقوبات الجزائري، نص على الشروع في جرائم المساس بأنظمة المعالجة الآلية للمعطيات باعتبارها جرح تتطلب هذا النص الخاص.

وبالتالي وضع المشرع الجزائري أي حد للقول بالعقاب على الشروع فيها أم لا، وكان المشرع الجزائري موفق جدا عندما عاقب على الشروع فيها، وهذا نظرا لجسامة الخطر المترتب عنها، وما يمكن أن تؤدي إليه من أضرار في حال تمامها.

2-2-1-3-2 الركن المادي:

يتكون الركن المادي لجريمة الشروع أو المحاولة من عنصرين هما البدء في التنفيذ ، وعدم إتمام هذا التنفيذ لأسباب لا دخل لإرادة الفاعل فيها.[76] ص 376

- البدء في التنفيذ:

لقد اختلف الفقه في تحديد معيار البدء في التنفيذ بين إتجاهين، الأول يأخذ بالمذهب الموضوعي والإتجاه الثاني يأخذ بالمذهب الشخصي.

بالنسبة لأنصار الإتجاه الأول يعتبر البدء في التنفيذ هو الفعل الذي يبدأ فيه الجاني تحقيق الركن المادي للجريمة، ووفقا لهذا الإتجاه تخرج الأفعال التحضيرية السابقة على إقرار الجريمة من جرائم الشروع.

بينما أصحاب الإتجاه الثاني فيهتمون بالنية الإجرامية، فالبدء في التنفيذ في نظرهم هو الفعل الذي يكشف عن نية إجرامية نهائية وقاطعة، بمعنى أنه وفقا لأنصار هذا المذهب يقوم الركن المادي بالنظر إلى شخص الجاني ونفسيته، فيقوم الشروع إذا قام الجاني بوضع كل ما أعده من وسائل موضع التنفيذ حتى ولو كانت من الأعمال التحضيرية. [77] ص 187

ويرجح البعض المذهب المادي على المذهب الشخصي لأنه لا يعاقب على الشروع إلا إذا وضع الجاني يده على الفعل المحقق للنتيجة، وإلا فإنه سيؤخذ على مجرد النية، وبالتالي فيستبعد من الشروع مجرد التفكير فيها أو التصميم عليها، أو إعداد العدة لها قبل البدء في التنفيذ.

- عدم تحقق أو إتمام الجريمة لأسباب لا دخل لإرادة الجاني فيها:

مفادها أنه لا يكفي أن يرتكب الجاني أفعالا ترمي مباشرة إلى ارتكاب الجريمة، أي صالحة لوقوعها حتى يتوافر في حقه الشروع في الجريمة، وإنما يلزم فضلا عن البدء في تنفيذ الجريمة أن يقف التنفيذ أو يخيب أثره لأسباب لا دخل لإرادة الجاني فيها.[76] ص 388

وبالتالي فقد يقوم الجاني بتنفيذ النشاط الذي بواسطته تتحقق النتيجة، إلا أن ذلك النشاط يتوقف بسبب خارج عن إرادة الجاني، كتدخل شخص آخر وتعرف هذه الحالة بالجريمة الموقوفة وفي الجريمة

المعلوماتية قد يقوم الجاني بنشاطه المتمثل في الدخول إلى النظام المعلوماتي، إلا أن ذلك النشاط لا يكتمل بسبب تدخل شخص آخر أوقف ذلك النشاط، وكذلك في حالة ما إذا استعمل برنامج بقصد الدخول إلى النظام والتلاعب بالبيانات الموجودة بداخله، فتتحقق جريمة الدخول لكنه لا يستطيع تحقيق جريمة التلاعب لخلل في البرنامج، وهكذا تتحقق جريمة الدخول وجريمة الشروع في التلاعب بالمعطيات، وفي هذه الحالة تسمى الجريمة بالخائبة. [06] ص 150

وعليه فالركن المادي في جريمة الشروع يقوم على الأفعال المادية التي كانت ستؤدي إلى تحقيق النتيجة الإجرامية، لولا تدخل عوامل خارجية حالت دون وقوعها لأسباب خارجة عن إرادة الجاني وهذا ينطبق على الجرائم التقليدية وكذلك الجرائم المعلوماتية.

3-2-1-3-2 الركن المعنوي:

يتحقق الركن المعنوي في الشروع بتوفر القصد الجنائي الذي تتطلبه الجريمة التامة ألا وهو القصد الجنائي العام
- القصد الجنائي العام.

كما هو معلوم فإن القصد الجنائي العام يقوم على عنصرين العلم والإرادة، وباعتبار أن الشروع لا يكون إلا في الجرائم العمدية، فلا شروع في جريمة غير عمدية، ولا شروع في جريمة تتجاوز قصد الجاني، إذ تنحصر مسؤولية الجاني في الأعمال التي أرادها. [65] ص 168

• العلم:

وعليه يشترط لتحقيق عنصر العلم أن يكون الجاني عالما بكل واقعة ذات أهمية قانونية تدخل في تكوين الجريمة، فكل ما يتطلبه القانون من وقائع لبناء أركان الجريمة وإستكمال عناصرها يتعين أن يكون الجاني عالما به. [65] ص 168

وفي مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ينبغي أن يكون الجاني عالما بكل واقعة ذات أهمية قانونية تدخل في تكوين الجريمة، سواء كانت الجريمة جريمة دخول أو بقاء داخل نظام المعالجة الآلية للمعطيات، أو جريمة التلاعب، أو جريمة التعامل في المعطيات المنصوص عليها في قانون العقوبات الجزائري .

ومثال الشروع في ارتكاب إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات من يضبط وهو يضغط زر الحاسب الآلي بغرض تشغيل الجهاز، أو أن يضبط وهو يدخل إلى أيقونة خاصة بموظف

آخر تحتوي على ملفات خاصة بالموظف... ففي هذه الحالة تتحقق جريمة الدخول إلى النظام إذا لم يكن مسموح له الدخول إلى النظام ، وبالإضافة إلى ذلك تتحقق جريمة الشروع لأنه لم يدخل بعد إلى الملف المراد الاعتداء عليه.

كذلك يتحقق الشروع في الحالة التي يضبط وقد أدخل برنامج إختراق إلى جهاز الكمبيوتر.

• الإرادة:

فإذا ما توافر عنصر العلم على النحو السابق فإنه يتعين توافر العنصر الثاني وهو الإرادة، التي بموجبها يتطلب أن تتجه تلك الإرادة لتحقيق النتيجة.

وقد يثار تساؤل حول سبب تكرار النص على الشروع بالنسبة لجريمة الدخول غير المشروع إلى نظام المعالجة، حيث أن المادة 394 مكرر بعد أن نصت على جريمة الدخول وجرمت المحاولة على الدخول أو البقاء بقولها "...أو يحاول ذلك" وكذلك المادة 394 مكرر وتضمنت الشروع في كافة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بما فيها جريمة الدخول غير المشروع أو المحاولة وهذا ما يستتشف منه ما يعرف بالشروع في الشروع، فهل هذا التكرار يجعل من لفظ أو يحاول ذلك في نص المادة 394 مكرر يختلف عن الشروع.

نجيب على ذلك التساؤل بأن المحاولة لا تختلف عن الشروع في النصين السابقين بدليل أن المشرع الجزائري في نص المادة 30 قانون العقوبات قد نص على الشروع بعنوان المحاولة، مما يجعل مصطلحي الشروع والمحاولة تحمل نفس المعنى.

وبالتالي فإن تكرار اللفظ في جريمة الدخول يجد له تفسير بأهمية هذه الجريمة، لكونها الجريمة الأولى التي يمكن أن تكون بمثابة البوابة لإرتكاب أغلب الجرائم المعلوماتية، وكان يستحسن عدم شمول نص المادة 394 مكرر لفظ المحاولة والإكتفاء بنص المادة 394 مكرر 7 المتضمن تجريم الشروع في جرائم المساس بأنظمة المعالجة الآلية للمعطيات وإستبعاد جريمة الدخول والبقاء داخل نظام المعالجة الآلية للمعطيات من نطاق الشروع ، لأن الشروع غير متصور في هذه الجريمة وهذا ما أخذ به التشريع الفرنسي في مادته 4-323 [59] ، حيث لم ينص على المحاولة بنص المادة 1-323 وعندما نص على الشروع في نص المادة 4-323 استبعد جريمة الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات وكذلك الأمر بالنسبة للتشريع الإماراتي الذي لم ينص في المادة الثانية منه على المحاولة.[10]

الشروع في الإتفاق الجنائي:

يذهب الرأي السائد في الفقه إلى القول بأنه لا يوجد شروع في الإتفاق الجنائي، والحجج التي يستند عليها متعددة، فالإتفاق حالة نفسية تتم بتلاقي الإرادات ولا تحمل بداية ولا نهاية، فهو لا يقع إلا كاملا ولا يحتمل بدءا في التنفيذ. [26] ص 120

وقد تبنى المشرع الجزائري فكرة الشروع في الاتفاق الجنائي، مع أن بعض التشريعات لم تتبنى ذلك كالتشريع الفرنسي، لأن ذلك يؤدي إلى المساس بالنظرية العامة في القانون الجنائي، وهي العقاب على مجرد التحضير أو التفكير في الجريمة.

وهذا المسلك منتقد أيضا لأنه إذا كان تجريم الاتفاق الجنائي في حد ذاته منتقد، وقد 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 وجود الإرادة، الإرادة التي لم تلتق مع إرادات أخرى لأنها لو إلتقت بإرادات أخرى لكان الاتفاق مكتمل، وكان المشرع اقترب من مجرد تجريم النوايا.

أما إتفاقية بودابست في مادتها 11 [13] ، فقد أعطت الدول الموقعة على المعاهدة الخيار في تجريم أو عدم تجريم المحاولة على إرتكاب أي من الجرائم المنصوص عليها في المعاهدة.

4-2-1-3-2 عقوبة جريمة الشروع:

لقد نص المشرع الجزائري على جريمة الشروع بنص المادة 394 مكرر 7 من قانون العقوبات الجزائري، والتي جاء فيها أن الشروع في الجريمة يعاقب عليه بمثل عقوبة الجريمة التامة، وعلى هذا الأساس يصبح الشروع في جريمة الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات في صورتها البسيطة: يعاقب عليه. " بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج أما في صورتها المشددة فيعاقب بـ " ستة أشهر إلى سنتين و الغرامة من 100.000 إلى 200.000 دج في حالة حذف أو تغيير لمعطيات المنظومة، " ويعاقب بـ " ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج "

أما في جريمة التلاعب بالمعطيات فيعاقب عليه " بستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج "

وفي جريمة التعامل بكلتا صورتها يعاقب بالحبس من شهرين إلى ثلاثة سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج "

وفي حالة ما إذا قام بالجريمة شخص معنوي ففي هذه الحالة يضاعف الحد الأقصى للغرامة المطبقة على الشخص الطبيعي إلى خمسة (5) أضعاف وفقا لما جاء في نص المادة 394 مكرر 4 .

وفي حالة ما إذا ارتكبت جريمة الشروع ضد مؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام ، تضاعف العقوبة عما هو مقرر نتيجة للإعتداء على معطيات خاصة بالأشخاص الطبيعيين وفقا لما جاءت به المادة 394 مكرر 3 .

2-3-2 الأحكام المشتركة المتعلقة بالعقوبة.

تتشترك الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في ثلاثة أحكام تتعلق بالعقوبة تتمثل في العقوبات التكميلية لهذه الجرائم، وتشديد عقوبة الشخص المعنوي، والثالثة تتمثل في تشديد عقوبة الجريمة إذا مست الجهات العامة.

1-2-3-2 العقوبات التكميلية.

إضافة إلى العقوبات الأصلية المفروضة على مرتكب جرائم المساس بأنظمة المعالجة الآلية للمعطيات فقد قدر المشرع الجزائري عليه عقوبات تكميلية تتمثل في المصادرة والغلق ، وهذا ما جاء في نص المادة 394 مكرر 6، بخلاف العقوبات التكميلية المطبقة على الأشخاص في حال ارتكابهم للجرائم التقليدية. [68]

العقوبات التكميلية المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

يخضع مرتكب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى عقوبتين تكميليتين يجب على القاضي تطبيقها في حال ارتكاب إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وهذا ما جاء في نص 394 المكرر 6: "مع الإحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها ."

وقد نصت على هذين العقوبتين بعض القوانين العربية الخاصة بمكافحة الجرائم المعلوماتية كالقانون الإماراتي في مادته 24 [10] ، وكذا عدد من التشريعات الأجنبية .

فبالنسبة للتشريع الفرنسي نص عليها في تشريعات متعاقبة 1988 و 1994 و 2004 حيث لم تكن المادة 462 فقرة 9 من قانون 1988 تقرر سوى عقوبة تكميلية واحدة وهي المصادرة، أما المادة 5/322 من قانون العقوبات الفرنسي لسنة 1994 وهي نفسها لسنة 2004 فقد تضمنت قائمة من العقوبات التكميلية لتعطي للقاضي إمكانية تفريد العقوبة. [26] ص 122

2-3-2-1 عقوبة المصادرة:

المصادرة نوعان إمّا أن تكون عامة وإمّا أن تكون خاصة، فالمصادرة العامة هي: نزع سائر أموال المحكوم عليه وإضافتها إلى ملكية الدولة، أمّا المصادرة الخاصة: فهي نزع ملكية مال معين من أموال المحكوم عليه وإضافتها إلى ملكية الدولة وقد نصت على المصادرة الخاصة المادة 15 من قانون العقوبات الجزائي ، فالمصادرة عقوبة مالية مادية أو عينية، تهدف إلى تملك السلطات العامة أشياء ذات صلة بجريمة ما قهرا عن صاحبها وبغير مقابل. [76] ص 868

والمصادرة تشبه إلى حد كبير الغرامة وذلك في أن كليهما من العقوبات المالية، فهما يختلفان من حيث أن المصادرة تتمثل في نقل ملكية شيء من مال المحكوم عليه إلى الدولة، بينما تتمثل الغرامة في تحميل ذمة المحكوم عليه بدين لها.

المصادرة عقوبة تكميلية دائما بمعنى أنها مكملّة لعقوبة أصلية، ولا تنقرر إلا إذا نطق بها القاضي في حكمه الصادر بالعقاب على جنابة أو جنحة. [78] ص 163

ومن نص المادة 394 مكرر 6 يبدوا لنا أن المصادرة عقوبة تكميلية وجوبية، لأنها لم تترك الخيار للقاضي بين الحكم وعدم الحكم بها، وذلك لكون الهدف من هذه العقوبة هو الحد من تلك الجرائم، فأصحاب الأجهزة والوسائل عندما يعلمون مسبقا بأنه سوف تتم المصادرة لكل الأجهزة، والوسائل التي ترتكب بها الجريمة بالإضافة إلى العقوبات الأصلية التي ستوقع عليهم، فإن ذلك سيكون مانعا من الإقدام على ارتكاب الجرائم ولتطبيق عقوبة المصادرة فإنه يتطلب توافر شروط.

- يجب أن تكون عقوبة المصادرة تالية لعقوبة أصلية من العقوبات المنصوص عليها في القانون وهي عقوبة الحبس أو السجن أو الغرامة، وتكون العقوبة وجوبية في الجنايات بشكل عام. [79]

وذلك ما ينطبق على عقوبة المصادرة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حيث نص المشرع على المصادرة بنص خاص، كون أنها جرائم داخلية في نطاق الجرح. [68]

- يجب أن تكون هذه الأشياء التي يحكم بمصادرتها قد استخدمت في ارتكاب الجريمة، فالمادة 394 مكرر 6 جعلت محل للمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة، وهذا ما يؤكد أن المشرع لم يجعل هذه الوسائل محددة على سبيل الحصر، وإنما على سبيل المثال، وهذا ما يستشف من عبارة والوسائل المستخدمة، بمعنى سواء كانت الوسائل تقليدته كالكتب التي توضح وتشرح كيفية ارتكاب الجرائم المعلوماتية، أو كانت الوسائل معلوماتية كاستخدام برنامج معد خصيصا لإرتكاب إحدى جرائم المعلوماتية، أو الاعتماد على أنظمة الحاسب الآلي...

- يجب أن تكون الأشياء التي يحكم بمصادرتها مضبوطة فعلا من قبل الجهات المختصة، سواء السلطات القضائية أو أحد أجهزتها المعاونة ، وسواء قدمها الجاني من تلقاء نفسه أو ضبطتها الشرطة.[26] ص 122

- يجب أن لا تمتد عقوبة المصادرة إلى حقوق الغير حسن النية طبقا للمادة 15 مكرر [79] ، وهذا القيد نابع من طبيعة العقوبة كونها عقوبة مكملة، يترتب عليه أن تكون ذات طبيعة شخصية لا تطال غير من يستحقون العقوبة عن الجريمة، أي كل من لا يسأل عنها ولم يكن قد أدين فيها بوصفه فاعلا أو شريك، وثبتت ملكيته للشيء المضبوط، فهو الغير من الوجهة الجنائية بالنسبة للجريمة ، وهو حسن النية لأنه لا يتوافر لديه قصد أو خطأ بالنسبة لها.[72] ص 843

بمعنى أنه كان يجهل أن هذه الأشياء سوف تستعمل في ارتكاب الجريمة ، أو كان يعلم بذلك وبذل كل ما في وسعه للحيلولة دون استعمالها، إلا أنها استعملت فعلا في ارتكاب الجريمة، ولا تقتصر حقوق الغير حسن النية على حق الملكية فحسب، بل إن الحقوق الأخرى مثل حق الانتفاع وحق الرهن يسري عليها ما يسري على حقوق الملكية، ولا تشملها عقوبة المصادرة بحق حسن النية.

وبتعبير آخر أن الحقوق الشخصية لا تحول دون المصادرة، لأن محلها ذمة المدين، وليس مال معين من أمواله، حتى لو كان الشيء المضبوط هو الضمان الوحيد للمدين، ولا عبرة بما إذا كان حق الغير حسن النية قد نشأ قبل وقوع الجريمة أو بعده، ما دامت نيته كانت حسنة وقت ارتكاب الجريمة أو وقت نشأت حقه حسب الأحوال.

ويترتب على هذا أنه ما دام للغير حق ملكية على الأشياء المضبوطة، فلا يجوز الحكم بمصادرتها حتى ولو كان للمتهم حق عيني عليها كالرهن أو الانتفاع، فإذا كانت هذه الأشياء مملوكة على الشيوخ بين المتهم والغير حسن النية جازت مصادرتها، وتحل الدولة محل المتهم، فتصبح الأشياء مملوكة لها وللغير كل بقدر حصته، فإذا كان حق الغير على الشيء دون حق الملكية، كالرهن أو الانتفاع جازت مصادرتها، إلا أنه ينتقل إلى الدولة محملا بحقوق الغير.[26] ص 124

وفيما يخص العقوبات التكميلية لجرائم المساس بأنظمة المعالجة في القانون الفرنسي فتميز بين وضعين أولا: قانون العقوبات لعام 1988 فالمادة 4-462 لم تكن تقرر إلا عقوبة تكميلية واحدة وهي المصادرة، أما المادة 5-323 من قانون العقوبات لسنة 1994 وهي المادة نفسها من قانون العقوبات لسنة 2004 فقد قدمت قائمة بالعقوبات التكميلية، لتعطى للقاضي إمكانية تحقيق مبدأ تفريد العقوبة، وهذه العقوبات كلها إختيارية، وخاصة بالأشخاص الطبيعيين وهي كالاتي:

- الحرمان لمدة 5 سنوات أو أكثر من ممارسة وظيفة عامة، أو ممارسة نشاط مهني أو إجتماعي في المجال الذي إرتكبت فيه الجريمة.
- مصادرة الأشياء التي إستخدمت في الجريمة أو كانت معدة لإستخدامها فيها، أو نتجت عن الجريمة بإستثناء الأشياء القابلة للإعادة.
- الغلق لمدة 5 سنوات أو أكثر للمؤسسات أو لواحدة أو أكثر من فروع المشروع الذي استخدم في إرتكاب الجريمة.
- الإقصاء لمدة 5 سنوات أو أكثر من إصدار شيكات، ولايمنع هذا من استرداد شيكات السحب الموجودة لدى المسحوب عليه أو الشيكات المعتمدة.
- نشر أو تعليق الحكم المعلن ضمن الشروط التي تنص عليها المادة 131-35 وهي نفس العقوبات التي تحت عليها الاتفاقية الدولية للإجرام المعلوماتي.
- وبالتالي كان على المشرع الجزائري أن ينص على جملة من العقوبات منها المصادرة والغلق، ويترك بذلك السلطة التقديرية للقاضي للحكم بالعقوبة المناسبة.

2-1-2-3-2 الغلق

- نصت المادة 394 مكرر على عقوبة الغلق إلى جانب عقوبة المصادرة كعقوبتين تكميلتين يعاقب بهما كل من ارتكب جريمة من الجرائم الماسة بأنظمة المعالجة وهذه المادة تشمل:
- إغلاق المواقع: ويقصد المشرع بهذا مواقع الانترنت والمواقع الالكترونية بصفة عامة والتي كانت وسيلة لإرتكاب هذا النوع من الجرائم أو ساهمت في إرتكابها.
 - إغلاق المحل (المقهى الالكتروني): ويقوم ذلك في الحالة التي يكون صاحب المحل مشاركا في الجريمة، وذلك إذا تمت الجريمة وهو عالم بها ولم يتصد لها بالإخبار عنها ، أو بمنع مرتكبيها من إرتياد محله لإرتكاب مثل هذه الجرائم. [20] ص 131

ويرى البعض بأن المشرع الجزائري لم يكن موفقا في استعمال عبارة "إغلاق المواقع التي كانت محلا للجريمة" لكون هذا اللفظ يمكن استعماله للتعبير عن المواقع التي تم الاعتداء عليها أو التلاعب بمعطياتها، ومن غير المعقول غلقها كونها ضحية، وكان الأولى أن تكون عبارة النص "المواقع التي تستعمل في إرتكاب الجريمة" بدلا من المواقع التي تعد محل للجريمة. [26] ص 125

بينما يري البعض الآخر أن هذا الرأي قد لا يجانبه الصواب، وذلك لكون المشرع يقصد بالمواقع التي تكون محل لإرتكاب الجرائم، أي التي ترتكب من خلالها تلك الجرائم، فقد تكون محلاً لإرتكاب تلك الجرائم عندما يتم من خلالها إرسال برامج للتدمير والتجسس، أو لأي غرض غير مشروع، ويتسبب في الاعتداء على أنظمة ومواقع الغير، كما قد تكون محلاً للجريمة عندما تكون محتوى للأعمال الضارة والإباحية، وذلك عندما تشتمل على معلومات وبيانات لتعليم الجريمة يستطيع من خلالها من يدخل إلى تلك المواقع من المجرمين، أو من له ميول إجرامي أن يجد ضالته في تلك المواقع، بل إن تأثيرها لا يقتصر على أولئك فحسب، وإنما قد يقع فيها العديد من الأبرياء التي تؤثر عليهم تلك المواقع وقد تجرهم إلى الإنحلال وكافة أشكال الإجرام المعلوماتي.

كما أنّ ما يؤكد صحة تفسير العبارة "مع إغلاق المواقع التي تكون محلاً للجريمة" حسب هذا الرأي بأنها المواقع التي ترتكب منها الجرائم المعلوماتية، أو تكون محتوى للأعمال الضارة أو الإباحية، النص المكمل لها بحيث تكون العبارة بكاملها "مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقاً لهذا القسم"، فهذه العبارة في مقطعها الثاني تؤكد بأن المواقع التي نص المشرع على إغلاقها هي التي ارتكبت من خلالها أو بواسطتها تلك الجرائم.

حيث أن النصوص القانونية الخاصة بكل جريمة من تلك الجرائم المنصوص عليها سواء تعلقت بالدخول أم البقاء أو التلاعب في المعطيات تعاقب من يقوم بالدخول أو البقاء والتلاعب، وكل تلك الألفاظ تشير إلى أن الاعتداء أو الفعل الإجرامي المرتكب قد يتم من موقع أو نظام هو الموقع محل الجريمة أو يستهدف نظام آخر، وهو نظام أو موقع الضحية. [06] ص 173

ونشير فقط إلى أنه يشترط أن تكون الجريمة قد ارتكبت بعلم مالكةا، وعليه إذا انتفي علم مالك المحل أو مكان الاستغلال فلا تطبق العقوبة، وعقوبة الغلق هي الأخرى لا تقع في مواجهة الغير حسن النية للأسباب السالف ذكرها.

وفيما يتعلق بمدة عقوبة الغلق، فلم تحدد المادة 394 مكرر 6 مدة معينة، وعليه فهي قد تكون مؤبدة أو مؤقتة كما نصت على ذلك المادة 26 من الأحكام العامة لقانون العقوبات الجزائري. [57]

ولقد نص المشرع الفرنسي على عقوبة الغلق في المادة 323-5 إلى جانب عقوبات تكميلية أخرى، وقد حددت مدة الغلق بحوالي 5 سنوات أو أكثر للمؤسسات أو لواحدة أو أكثر من فروع المشروع الذي استخدم في إرتكاب الجريمة، وبالتالي فقد حدد المشرع الفرنسي الحد الأدنى للجريمة ولم يحدد الحد الأقصى، وبذلك ترك السلطة التقليدية للقاضي بحسب نوعية كل جريمة.

كما أنّ ما يؤكد صحة تفسير العبارة "مع إغلاق المواقع التي تكون محلا للجريمة" حسب هذا الرأي بأنها المواقع التي ترتكب منها الجرائم المعلوماتية، أو تكون محتوى للأعمال الضارة أو الإباحية.

2-2-3-2 تشديد عقوبة الجريمة المرتكبة من قبل الشخص المعنوي.

لقد شدد المشرع الجزائري عقوبة الشخص المعنوي إلى 05 مرات في حالة ارتكابه إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في الفصل السابع مكرر من قانون العقوبات الجزائري .

وكما هو معلوم أنّ الشخص المعنوي بإمكانه ارتكاب إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات أو جرائم أخرى عن طريق ممثليه، أي عن طريق من لهم الصفة القانونية لتمثيل الشخص المعنوي كمدير المؤسسة مثلا، ولهذا سوف نتناول بنوع من الإيجاز أركان الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي ترتكب من قبل الشخص المعنوي.

1-2-2-3-2 الركن الشرعي.

لقد نص المشرع الجزائري على جريمة المساس بأنظمة المعالجة المرتكبة من قبل الشخص المعنوي في نص المادة 394 مكرر 4، والتي جاء فيها "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل 05 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

هذا وتجدر الإشارة إلى أنّ المشرع الجزائري قد أقر مسؤولية الشخص المعنوي بنص عام وهو نص المادة 18 مكرر من قانون العقوبات ، وذلك بالنسبة لكل الجرائم التي يري المشرع أنها تصلح لأن يسأل عنها الشخص المعنوي.[57]

وقد سار التشريع الجزائري على نهج كل من الاتفاقية الدولية للإجرام المعلوماتي في مادتها (12) [13] ، وكذا التشريع الفرنسي حيث نجد أنّ المشرع الفرنسي لم يستبعد مسؤولية الشخص المعنوي فنص عليها في المادة 6/323 من قانون العقوبات الفرنسي الجديد، وذلك وفقا للشروط التي نصت عليها المادة 2/121، ووفقا لهذه المادة فإن المسؤولية الاعتبارية لا تستبعد مسؤولية الأشخاص الطبيعيين بصفتهم شركاء أو متدخلين أو فاعلين في الجريمة المرتكبة [59] ، وعليه نجد أنّ نص المادة 2/121 من قانون العقوبات الفرنسي يربط إثارة المسؤولية الجزائية للشخص المعنوي باجتماع شرطين هما: من جهة ارتكاب الجريمة من طرف أعضاء أو ممثلي الشخص المعنوي " Les organes ou représentants" ، ومن جهة أخرى ارتكاب الفعل المجرم لحساب الشخص المعنوي.

وهكذا فإن المسؤولية الجزائية للشخص المعنوي متوقفة على صفة الشخص الذي يكون ركيزة أو دعامة لهذه المسؤولية "supportLa qualité de la personnes servant Dou" ، وكذا كفاءاته ومؤهلاته في إظهار إرادة الشخص المعنوي حال ارتكاب الفعل المجرم. [80] ص40

ومن خلال نص المادة 394 مكرر 04 نلاحظ أن المشرع الجزائري قد شدد عقوبة الشخص المعنوي في حالة ارتكابه لإحدى جرائم المساس بأنظمة المعالجة إلى 5 مرات العقوبة المقررة للشخص الطبيعي، وهذا يعود إلى أن المشرع الجزائري قد أخذ بعين الاعتبار ميزانية الشخص المعنوي التي تفوق بكثير ميزانية الشخص الطبيعي، فلو ترك عقوبة الغرامة هي نفسها المقررة للشخص الطبيعي فإن هذه العقوبة قد لا تكون مجدية، فتشديد عقوبة الغرامة في حالة ارتكابها من قبل الشخص المعنوي، قد يكون سببا في الحد من ارتكاب هذه الجرائم، ولكن تجدر الإشارة إلى أن تحديدها بـ 5 مرات الحد الأقصى للغرامة المحكوم بها على الأشخاص الطبيعية قد تؤدي إلى إفلاس الشخص المعنوي.

2-2-2-3-2 الركن المادي:

يتكون الركن المادي في جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في القسم السابع مكرر ، من كافة الأفعال المادية التي يمكن أن ترتكب بها إحدى هذه الجرائم فمثلا في جريمة الدخول أو البقاء في صورتها البسيطة، يقتصر الأمر على الدخول أو البقاء داخل النظام وفي جريمة التلاعب بالمعطيات، الشخص المعنوي هنا لا يكتفي بمجرد الدخول إلى نظام معالجة آلية للغير أو البقاء فيه ضد إرادة من له حق السيطرة عليه وإنما يتعدى ذلك إلى محو أو تغيير أو تعديل في معطيات إشتغال المنظومة حتى تقوم جريمة التلاعب في حقه وهكذا لباقي الجرائم، وما يميز الركن المادي في الجرائم المعلوماتية المرتكبة من قبل الشخص المعنوي هو:

-أن الأفعال المادية للجريمة ترتكب عن طريق شخص يمارس سلطة القيادة داخل الشخص المعنوي.

-أن الجريمة المعلوماتية ترتكب بإسم الشخص المعنوي ولحسابه.

-يجب أن يكون الشخص الذي ارتكب الجريمة يمارس سلطة اتخاذ القرار.

-أن يقوم الشخص المعنوي بإقتراف أي من الأفعال المشار إليها سلفا، وهي فعل الدخول أو البقاء داخل نظام المعالجة للمعطيات، أو التلاعب في المعطيات عن طريق محو أو تغيير أو تعديل معطيات الحاسوب، أو التعامل في المعطيات سواء معطيات يمكن أن ترتكب بها جريمة من جرائم المساس بأنظمة المعالجة، أو معطيات ناتجة عن إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

3-2-2-3-2 الركن المعنوي.

يتحقق الركن المعنوي في الجرائم المعلوماتية المرتكبة من قبل الشخص المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة.

فيشترط لقيام الجريمة المعلوماتية المرتكبة من قبل الشخص المعنوي، أن يكون من ارتكب الجريمة بإسم الشخص المعنوي، أو لحسابه عالما بأنه يرتكب جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى هذا يجب أن تتجه إرادة ممثل الشخص المعنوي لاقتراف إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

وعليه لا يشترط أن يتوافر القصد الجنائي الخاص حتى تقوم الجرائم المعلوماتية المرتكبة من قبل الشخص المعنوي، لأن المشرع الجزائري لم يشر إلى ذلك في نص المادة 394 مكرر 4 ، بالرغم من أن باعث تحقيق الربح، أشد تعلقا بالشخص المعنوي، لأن كثير من الأشخاص المعنوية تنشأ بغرض تحقيق الربح ، فتقوم بالمنافسة غير المشروعة لمنافسيها عن طريق ارتكاب إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، وذلك بالدخول إلى أنظمة حاسبات الشركات المنافسة دخولا غير مصرح به والإطلاع على ملفات وخططها ومنافستها بناء على ذلك، وربما يصل الأمر إلى التلاعب بمعطيات تلك الشركة. [26]ص126

4-2-2-3-2 العقوبات المقررة على الشخص المعنوي:

لقد كانت العقوبة إحدى أهم الحجج التي إستند إليها المعارضون لمبدأ إقرار مسؤولية الشخص المعنوي، حيث رأوا أنه لا يمكن تطبيقها على هذا الأخير خاصة تلك العقوبات السالبة والمقيدة للحرية، لكن وبعد إتساع تطبيق عقوبة الغرامة وإبتكار عقوبات جديدة تتلاءم وطبيعة الشخص المعنوي لم يعد لهذا الاعتراض محل. [26] ص 127

وعليه سوف نشير إلى العقوبات المطبقة على الشخص المعنوي بشكل عام، وكذا العقوبات المطبقة عليه في حالة ارتكابه لإحدى جرائم المساس بأنظمة المعالجة.

- العقوبات المطبقة على الشخص المعنوي بشكل عام:

تضمن المشرع الجزائري في قانون العقوبات عدد من العقوبات المطبقة على الشخص المعنوي في حال ارتكابه لجناية أو جنحة، وهي عقوبة الغرامة كعقوبة أصلية بالإضافة إلى العقوبات التكميلية.

• العقوبة الأصلية:

وتتمثل في الغرامة التي تساوي من مرة إلى 5 مرات العقوبة المقررة على الشخص الطبيعي بمعنى تكون للقاضي السلطة التقديرية بين تطبيق الحد الأدنى أو الحد الأقصى طبقاً للمادة 18 مكرر [79].

• العقوبات التكميلية:

يعاقب الشخص المعنوي بوحدة أو أكثر من العقوبات التكميلية التالية:

- حل الشخص المعنوي.
- غلق المؤسسة أو نوع من فروعها لمدة لا تتجاوز 5 سنوات.
- المنع من ممارسة نشاط أو عدة أنشطة مهنية.
- نشر الحكم وتعليقه.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات.

وهذه العقوبات تطبق على الشخص المعنوي في حالة ارتكابه لأفعال إجرامية وهي ليست خاصة بالجرائم المعلوماتية، وإنما يمكن أن توقع على الشخص المعنوي في حالة ارتكابه للجرائم التقليدية.

- تشديد عقوبة الغرامة في الجرائم المعلوماتية:

يقصد بالغرامة: إلزام المحكوم عليه بدفع مبلغ من المال لصالح خزينة الدولة، وتعتبر من أهم العقوبات التي تطبق على الشخص المعنوي وطبقاً للمادة 394 مكرر 4، والمتعلقة بعقوبة الشخص المعنوي عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، قد ألزمت القاضي بالحكم بالحد الأقصى لهذه الغرامة وهو 5 أضعاف الغرامة المقررة على الشخص الطبيعي وعليه ففي:

- جريمة الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات في صورتها البسيطة :

فتكون العقوبة هي: " $500.000 \text{ دج} = 5 \times 100.000$ "

- عقوبة جريمة الدخول أو البقاء في صورتها المشددة:

تختلف عقوبة جريمة الدخول أو البقاء المرتكبة من قبل الشخص المعنوي بحسب النتيجة المترتبة على الدخول والبقاء.

* فإذا نتج عن الدخول أو البقاء، حذف أو تغيير لمعطيات المنظومة تكون العقوبة: الغرامة المقدرة بـ:
 $1.000.000 = 5 \times 2 \times 100.000$ دج

* أما إذا نتج عن الدخول أو البقاء تخريب نظام اشتغال المنظومة تكون العقوبة: الغرامة المقدرة بـ:
 $750.000 = 5 \times 150.000$ دج"

• عقوبة جريمة التلاعب بالمعطيات:

في حالة ارتكاب جريمة التلاعب من قبل شخص معنوي تصبح العقوبة :

$$10.000.000 = 5 \times 2.000.000 \text{ دج}$$

• عقوبة التعامل في معطيات غير شرعية:

إذا تعلق الأمر بالتعامل بمعطيات متحصلة من جريمة، أو التعامل في معطيات بغرض ارتكاب جريمة معلوماتية تكون العقوبة بـ:
 $25.000.000 = 5 \times 5.000.000$ دج

ونشير إلى أنه في الحالة التي يشرع فيها الشخص المعنوي بإرتكاب أي جريمة من الجرائم سالفة الذكر فإنه وفقا لنص المادة 394 مكرر 7 يحكم عليه بنفس عقوبة الجريمة التامة، وكذلك الأمر بالنسبة للاتفاق الجنائي .

ووفقا لنص المادة 394 مكرر 6 فإنه يحكم على الشخص المعنوي إلى جانب عقوبة الغرامة الحكم عليه بعقوبات تكميلية تتمثل في المصادرة والغلق.

3-2-3-2 الجرائم المعلوماتية المرتكبة ضد الهيئات والمؤسسات العامة:

نظرا للتطور التكنولوجي الذي مس مختلف المجالات والقطاعات منها المؤسسات والهيئات العامة بحيث أصبحت تسير تعاملاتها عن طريق أنظمة معلوماتية، إستدعى تدخل تشريعي للحماية الجنائية من الاعتداءات الموجهة ضد الهيئات والمؤسسات العامة في الدولة، فلم تعد الحماية هنا مقتصرة على القواعد التقليدية فحسب، وإنما أقرتها نصوص خاصة، وعلى وجه الخصوص تلك التي تتعلق بالمعلوماتية حيث تم بواسطتها تشديد هذا النوع من الإجرام.

1-3-2-3-2 الركن الشرعي:

نصت المادة 394 مكرر 3 قانون العقوبات الجزائري على تجريم الدخول إلى بعض الأنظمة الخاصة سواء بالمؤسسات والهيئات الخاضعة للقانون العام، أو الخاصة بالدفاع الوطني حيث ورد النص

كالتالي: "تضاعف العقوبات المنصوص عليها في هذا القسم، إذا إستهدفت الجريمة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد".

وعليه فأى فعل يستهدف الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، إذا تحققت به إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في القسم السابع مكرر من قانون العقوبات الجزائري، يكون خاضعا للمادة 394 مكرر 3.

ونلاحظ أن المشرع الجزائري خص مؤسسة الدفاع الوطني بالذكر نظرا لأهمية هذه المؤسسة من جهة، ومن جهة أخرى لدورها البارز في الحفاظ على سلامة التراب الوطني والأمن العام وكذا حساسية المعطيات المتعلقة بها، والخطورة البالغة للاعتداء عليها، وحكمة التشديد في الجرائم الماسة بالدفاع الوطني عموما هو ما يتطلبه الأمر من وجوب العمل على سلامة وأمن القوة العسكرية، التي في حفظها وسلامتها حفظ وسلام للدولة بأكملها.

فضلا عما يكون عليه الجاني في مثل هذه الجرائم من خسة ونذالة وإجرام في حق نفسه وفي حق وطنه، مما يستدعي أخذه بمنتهى الشدة والقسوة. [26] ص 130

والعقوبة المشددة تتمثل في ضعف العقوبة المقررة على الاعتداء على معطيات وأنظمة الأفراد العاديين وأشخاص القانون الخاص، ولا تقتصر الحماية على مؤسسة الدفاع الوطني بل وسعتها لتشمل الهيئات والمؤسسات الخاضعة للقانون العام.

إنّ هناك من التشريعات من تقصر الحماية على هذه المعطيات دون المعطيات المتعلقة بالأفراد، إلاّ إذا كانت هذه الأخيرة تمس مصالح الدولة، ومثال ذلك القانون الفدرالي الأمريكي لجرائم الحاسب الآلي فالمادة 1030 (أ) (3) منه لا تعاقب على الدخول المجرد، إلاّ إذا كانت هذه الحاسبات ترتبط بها مصالح الدولة، وكذلك الأمر بالنسبة لجريمة إتلاف المعلومات والبرامج. [22] ص 217

لقدأخذ المشرع الجزائري هذا الأمر بعين الإعتبار، فهو و إن بسط حمايته الجنائية على المعطيات بمختلف أنواعها والجهات التي تنتمي إليها حتى وإن كانت معطيات متعلقة بالأفراد، فقد شدد العقوبة إذا كانت تلك المعطيات أو الأنظمة التي تم العدوان عليها تتعلق بالدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام وفقا لنص المادة 394 مكرر من قانون العقوبات الجزائري.

2-3-2-3-2 الركن المادي:

الركن المادي للجرائم المعلوماتية التي تستهدف من خلالها مؤسسة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام، يتمثل بمختلف الأفعال والنتائج الخاصة بكل جريمة من جرائم

المساس بأنظمة المعالجة الآلية للمعطيات سאלفة الذكر، فمثلاً: تقوم جريمة الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات بأي وسيلة سواء عن طريق الإختراق أو عن طريق تصميم فيروس معد مسبقاً للدخول إلى النظام، وهنا تقوم جريمة الدخول أو البقاء في صورتها البسيطة وتشدد العقوبة في حالة ما إذا أدى هذا الدخول إلى نتيجة معنية تتمثل في حذف أو تغيير للمعطيات المخزنة في نظام المعالجة الآلية للمعطيات، أو تخريب نظام إشتغال المنظومة.

فالفارق بين هذه الجريمة وجريمة الدخول أو البقاء سواء في صورتها البسيطة أو المشددة هو أن تلك الأفعال التي يتم بواسطتها إرتكاب جريمة معلوماتية في هذه الجريمة، تكون موجهة ضد مؤسسة الدفاع الوطني أو المؤسسات والهيئات الخاضعة للقانون العام.

ونشير إلى أن هذا الفارق يتعلق بكل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات كجريمة التلاعب بالمعطيات، أو جريمة التعامل في المععطيات سواء التعامل في معطيات متحصلة من جريمة أو التعامل في معطيات يمكن أن ترتكب بها جريمة.

3-3-2-3-2 الركن المعنوي:

إنّ الركن المعنوي للجرائم المعلوماتية التي تستهدف مؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، لا يختلف عن الركن المعنوي لأي جريمة من الجرائم السالفة الذكر، والمتمثل في القصد الجنائي العام بعنصرية العلم والإرادة.

بحيث يجب أن يعلم الجاني بكافة العناصر الداخلة في أركان كل جريمة على حدة، بحيث مثلاً في جريمة الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات يجب أن يعلم الجاني أنه يدخل إلى نظام للمعالجة الآلية للمعطيات، أو أنه باق ضد إرادة من له حق السيطرة عليه وأن إرادته تتجه إلى هذا الدخول أو البقاء.

والجديد في الجرائم التي ترتكب ضد الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، هو أن يعلم الجاني بأنه يرتكب جريمة معلوماتية ضد مؤسسة الدفاع الوطني، أو ضد الهيئات والمؤسسات الخاضعة للقانون العام، وأن تتجه إرادته إلى إقتراف مثل هذا الفعل الإجرامي، وهو ينطبق على كل الجرائم الماسة بنظام المعالجة سواء جريمة التلاعب بالمعطيات أو التعامل بالمعطيات بصورتها.

4-3-2-3-2 العقوبات المقررة:

إن العقوبات المقررة في حالة ارتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تضاعف في حالة ما إذا استهدفت تلك الجريمة مؤسسة الدفاع الوطني، والهيئات والمؤسسات الخاضعة للقانون العام، وعليه سنتناول كل جريمة على حدة، وبيان ذلك لكل جريمة كما يلي:

- عقوبة جريمة الدخول أو البقاء في نظام مؤسسة الدفاع الوطني والمؤسسات والهيئات الخاضعة للقانون العام.

• العقوبات البسيطة:

إن جريمة الدخول أو البقاء في صورتها البسيطة تقتصر على مجرد الدخول أو البقاء إلى أنظمة مؤسسات الدفاع الوطني والهيئات التي تخضع للقانون العام دون تحقق نتيجة معنية فتكون العقوبة "الحبس من ستة أشهر إلى سنتين ، والغرامة من 100.000 دج مائة ألف إلى 200.000 دج مائتي ألف دينار جزائري."

• العقوبات المشددة:

إذا ترتب على جريمة الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة فإن العقوبة هي "الحبس من سنة إلى أربع سنوات ، والغرامة من مائتي ألف 200.000 دج إلى أربعمائة ألف 400.000 دج" ففي هذه الحالة تضاعف العقوبة مرتين.

الأولى: عندما ترتكب ضد الأشخاص والجهات الخاضعة للقانون الخاص، وفقا لنص المادة 394 مكرر ، والثانية إذا تم ارتكابها ضد المؤسسات والجهات الخاضعة للقانون العام، وفقا لنص المادة 394 مكرر 3 ، وليس كما يري البعض أن العقوبة تضاعف مرة واحدة. [26] ص 129

إذا ترتب على جريمة الدخول أو البقاء تخريب نظام اشتغال المنظومة فتصبح عقوبة الحبس من سنة إلى أربع سنوات، والغرامة من ألف 100.000 دج إلى ثلاثة آلاف 300.000 دج.

- عقوبة جريمة التلاعب بالمعطيات:

كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات ، أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها نظام معالجة آلية تابع لوزارة الدفاع الوطني، أو الهيئات أو المؤسسات الخاضعة للقانون العام يعاقب بالحبس "من سنة إلى ستة سنوات والغرامة من مليون 1.000.000 دج إلى أربعة ملايين 4.000.000 دج".

- عقوبة جريمة التعامل في معطيات غير مشروعة:

"يعاقب بالحبس من أربعة أشهر إلى ستة سنوات، والغرامة من مليونين 2.000.000 دج إلى 10.000.000 دج عشرة ملايين" كل من يقوم عمدا وعن طريق الغش بما يأتي:

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسله عن طريق منظومة معلوماتية يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضد مؤسسات وأشخاص القانون العام.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضد هيئات ومؤسسات القانون العام.

- عقوبة الجرائم المرتكبة من شخص معنوي ضد مؤسسة الدفاع الوطني ومؤسسات وهيئات القانون العام.

كما هو معلوم أن العقوبة التي يمكن تطبيقها على الشخص المعنوي في حالة ارتكابه لجريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، هي عقوبة الغرامة مضاعفة إلى خمسة مرات وفقا لنص المادة 394 مكرر 4 ، وهذا في حالة ما إذا استهدفت الأفراد وأشخاص القانون الخاص، بالإضافة إلى أن العقوبة قد تم مضاعفتها وفقا لنص المادة 394 مكرر 3 في حالة إستهدافها لمؤسسة الدفاع الوطني و هيئات القانون العام ، وعليه فعقوبة الجريمة المرتكبة من قبل الشخص المعنوي ضد مؤسسات وهيئات القانون العام ، تكون قد تم مضاعفتها مرتين لتصبح العقوبة مضاعفة إلى عشرة أضعاف ما هو مقرر في حالة ارتكابها من قبل الشخص الطبيعي.

- عقوبة جريمة الدخول أو البقاء:

في صورتها البسيطة: هي $5 \times 200.000 = 1.000.000$ دج مليون دينار جزائري. في صورتها المشددة: وتكون عقوبة جريمة الدخول أو البقاء المرتكبة من الشخص المعنوي ضد إحدى الجهات العامة في صورتها المشددة هي $5 \times 400.000 = 2.000.000$ دج مليونين دينار جزائري هذا في حالة ما إذا ترتب على الجريمة تغير أو حذف لمعطيات المنظومة.

أما في الحالة التي يترتب على الجريمة تخريب نظام اشتغال المنظومة فتكون عقوبة الغرامة هي $5 \times 300.000 = 1.500.000$ دج مليون وخمسمائة ألف دينار جزائري .

هذا بعكس ما يعتقد البعض أن العقوبة تتأرجح بين حدها الأدنى والأقصى ، لأن نص المادة 394 مكرر 04 كان صريحا ، بحيث تضاعف العقوبة إلى 5 مرات الحد الأقصى وليس الحد الأدنى

والأقصى ، وكذلك الأمر بالنسبة لنص المادة 394 مكرر 3 كان المشرع صريح بحيث تضاعف في حال إستهدافها لهيئات ومؤسسات القانون العام.

● عقوبة جرائم التلاعب بالمعطيات المخزنة في أنظمة المعالجة الآلية لإحدى الجهات العامة المرتكبة من قبل الشخص المعنوي.

تضاعف عقوبة الغرامة لجريمة التلاعب بالمعطيات المرتكبة من قبل الشخص المعنوي ضد إحدى الجهات العامة إلى عشرة (10) مرات عقوبة الغرامة ، أمّا جريمة التلاعب بالمعطيات المرتكبة من قبل الشخص المعنوي ضد الأفراد وأشخاص القانون الخاص، فتصبح العقوبة هي $20.000.000 = 5 \times 4.000.000$ دج "عشرون مليون .

● عقوبة جرائم التعامل في معطيات غير مشروعة.

تكون عقوبة جريمة التعامل في معطيات غير شرعية ناتجة أو يمكن أن ترتكب بها إحدى الجرائم المعلوماتية المنصوص عليها في قانون العقوبات الجزائي، عندما ترتكب من قبل الشخص المعنوي وتستهدف مؤسسة الدفاع الوطني والمؤسسات والهيئات الخاضعة للقانون العام تكون عقوبة الغرامة هي $50.000.000 = 5 \times 10.000.000$ دج خمسين مليون دينار جزائري".

ويلاحظ من خلال الغرامات سالفة الذكر وعلى وجه الخصوص الغرامة التي يتحملها الشخص المعنوي في حالة ارتكابه لجريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات أنها كبيرة جدا قد تؤدي إلى إفلاس الشخص المعنوي وإرهاق الذمة المالية للشركاء المساهمين في الشخص المعنوي، لذلك نرى أنه يجب النظر في مسألة تحديد عقوبة الغرامة للشخص المعنوي بالدرجة الأولى ، وكذلك الشخص الطبيعي بما يتناسب مع الذمة المالية للأشخاص وكذا الهدف من وراء إقرار العقوبة.

خاتمة

لقد تناولنا في هذه المذكرة الجرائم المعلوماتية المنصوص عليها في التشريع الجزائري، مستنديين إلى الإتفاقية الدولية للإجرام المعلوماتي، بالإضافة إلى كل من التشريع الفرنسي والتشريع الإماراتي، حتى يمكننا تبيين القصور الذي طال نصوص التشريع الجزائري.

ولقد إتضح من خلال الدراسة أن القوانين التي جاء بها المشرع الجزائري سواء الموضوعية منها، أو الإجرائية مازالت قاصرة عن مواجهة هذا المد الإجرامي، لأن هذه الجرائم تحتاج في مكافحتها إلى تعاون قضائي دولي نظرا لخاصيتها العابرة للحدود.

فعلى الرغم من أن المشرع الجزائري قد نص على مكافحة هذا النوع من الجرائم، وفقا للقانون 15/04 المؤرخ في: 10/نوفمبر/2004 في القسم السابع مكرر منه، بعنوان المساس بأنظمة المعالجة الآلية للمعطيات وكذا القانون 04/09 المؤرخ في: 05/08/2009 المتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهي تستحق الإشادة خاصة مع وجود عدد كبير من الدول العربية التي لم تضع نصوصا لمعاقبة مرتكبي هذا النوع من الإجرام، أو على الأقل تعديل قوانين العقوبات لديها.

إلا أن الدراسة قد بينت قصور التشريع الجزائري في عدد من المسائل، وعليه فقد أظهرت الدراسة مجموعة من النتائج، والتي على ضوءها سيتم تبني مجموعة من المقترحات التي تعالج تلك المشكلات وتتجلى في:

- نص المشرع الجزائري على المحاولة بنص المادة 394 مكرر، وكان الأنسب إستبعاد المحاولة من جريمة الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات والأكثر من هذا نجد أنّ المشرع نص على الشروع بنص المادة 394 مكرر 7 لكافة الجرائم المنصوص عليها في القسم السابع مكرر، وهو ما يستتبع بالضرورة تحقق ما يسمى بالشروع في الشروع، وهذا ما يؤدي بالخروج عن القواعد العامة في القانون الجنائي، والتي تقضي بعدم العقاب على ما يسمى بالشروع في الشروع.

- لم ينص المشرع الجزائري على جريمة الاعتداء العمدي على سير النظام، التي تتحقق إما بتعطيل النظام أو إفساده عن العمل ، حيث أنها تختلف عن كل من جريمة الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات في صورتها المشددة، كون أنها جريمة غير عمدية ، وكذلك تختلف عن جريمة الاعتداء العمدي على المعطيات لأن هذه الجريمة الأخيرة تستهدف المعطيات وليس النظام، وإن كانت في بعض الأحيان تؤدي إلى تعطيل النظام عن العمل.

- عدم تضمين المشرع الجزائري في نصوصه أفعال الإلتقاط، أو الإعتراض، وهي أفعال مستحدثة ينتج عنها إرتكاب إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات وهي تختلف عن الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات.

- لم يتضمن التشريع الجزائري جريمة التزوير المعلوماتي، أو على الأقل تعديل النصوص التقليدية المتعلقة بالتزوير حتى تشمل المستند المعلوماتي، ونشير إلى أن جريمة التلاعب بالمعطيات تختلف عن التزوير، لأن المستند المعالج آليا في جريمة التزوير المعلوماتي قد يكون بداخل النظام وقد يكون خارجه.

- لم يتضمن المشرع الجزائري الجرائم التي ترتكب من قبل الموظف أثناء تأديته لوظيفته أو بمناسبةها كما فعلت بعض التشريعات منها التشريع الإماراتي.

- لقد حدد المشرع الجزائري العقوبات التكميلية التي تطبق على مرتكب إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات بنص المادة 394 مكرر6، وهي إما المصادرة أو الغلق، أما في حالة إرتكاب جريمة تقليدية فالمشرع حدد قائمة بالعقوبات التي تطبق على مرتكب الجريمة منها المصادرة والغلق وبالرغم من أنه توجد عقوبات تكون أجدى في تطبيقها على مرتكب الجريمة المعلوماتية، إلا أن المشرع الجزائري لم يخضعها للقواعد العامة .

- لم ينص المشرع الجزائري على الجرائم التي ترتكب بواسطة المعلوماتية في قانون العقوبات، وإن كان نص عليها في القانون 04/09.

- عدم نص المشرع الجزائري على الجرائم التي ترتبط بالإنترنت، فمع أن نص العقوبات 394 مكرر6 جاء فيه أن المواقع تعتبر محل لجريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات إلا أنه لم ينص على الجرائم التي تتضمن إنشاء مواقع بهدف الترويج لأفكار معادية للدين الإسلامي مثلا أو المواقع المخلة بالحياء، أو المواقع المحرصة على الفسق والدعارة...

- نظرا لخصوصية هذا النوع من الإجرام، قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية بالقانون 22/06 المؤرخ في: ديسمبر 2006، والذي نص على تمديد الإختصاص إلى إختصاص وطني لضباط الشرطة القضائية، وجهات التحقيق، والمحاكمة، إذا تطلب التحقيق ذلك لعدد من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات كذلك أعى تلك الجهات من التقيد ببعض الضمانات منها مواعيد التفتيش، كما جاء القانون 04/09 وعالج مسألة تمديد الإختصاص إلى خارج الدولة الجزائرية إذا تعلق الأمر بالرقابة الإلكترونية، أو تفتيش أنظمة معلوماتية موجودة خارج الدولة عن طريق التعاون والمساعدة القضائية بين الجزائر ودولة أخرى استنادا إلى الإتفاقيات الدولية، ومبدأ المعاملة بالمثل، كذلك تضمن الالتزامات التي تقع على مقدمي الخدمات في مساعدة السلطات، وكذا إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، من ضمن مهامها القيام بأعمال الخبرة، وتبادل المعلومات مع نظيراتها في الخارج.

إلا أننا نجد أن المشرع الجزائري لم يتضمن الإستثناء الخاص بوقت التفتيش، والأشخاص المطلوب حضورهم، ليشمل باقي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال كما فعل بالنسبة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات لأنها تندرج ضمن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

- نظرا لخصوصية هذا النوع من الإجرام فنجد أنه لا يحتاج إلى نصوص قانونية فقط لمكافحته، ولكن يحتاج أيضا إلى تخصص فني من قبل الذين يتعاملون مع هذه الجرائم بغرض مكافحتها.

- تحتاج هذه الجرائم إلى تضافر كافة الجهود الدولية لمكافحتها، وذلك بالنص على تجريم هذه الأفعال من قبل كافة الدول، بالإضافة إلى مشاركة الدول في عدد من الإتفاقيات الدولية حتى تسهل عملية القبض على مرتكبي هذا النمط من الإجرام .

ونتيجة لذلك يتعين إبداء المقترحات التالية:

- يتعين على المشرع الجزائري إستبعاد المحاولة من نص المادة 394 مكرر، وكذا إستبعاد جريمة الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات من نص المادة 394 مكرر 7 التي نصت على تجريم الشروع في كافة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

- أقترح نص المشرع الجزائري على جريمة الاعتداء القسدي على النظام ضمن جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

- أقتراح تضمين المشرع الجزائري في نصوصه أفعال الإلتقاط أو الإعتراض ،لأنه بواسطتها ترتكب جرائم خطيرة جدا.
- ضرورة نص المشرع الجزائري على جريمة التزوير المعلوماتي.
- ضرورة نص المشرع الجزائري على الجرائم التي ترتكب من قبل الموظفين أثناء تأديتهم لمهامهم أو مناسبتها مع تشديد العقوبة المقررة عليهم.
- كان أخرى بالمشرع الجزائري أن يبقي على العقوبات التكميلية المنصوص عليها لمعاقبة مرتكب الجرائم التقليدية، فيترك بذلك المجال واسعا أمام القاضي لتطبيق العقوبة المناسبة وفقا لسلطته التقديرية لأنه توجد عقوبات ملائمة لمعاقبة المجرم من بين هذه العقوبات.
- ضرورة نص المشرع الجزائري على الجرائم التي ترتكب بواسطة المعلوماتية، وتحديد العقوبة المناسبة لكل جريمة.
- ضرورة تدريب شرطة متخصصة لمكافحة هذا النوع من الإجرام، بالإضافة إلى تدريب القضاة حتى يكون هناك قضاة متخصصون بهذا النوع من الإجرام.
- كذلك على الجزائر الإنضمام إلى أي تعاون دولي بغرض مكافحة هذا النوع من الإجرام،ولما لا الإنضمام إلى الإتفاقية الدولية للإجرام المعلوماتي.

قائمة المراجع

- 1/- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مقال منشور على الموقع التالي: www.arablawinfo.com
- 2/- عمرو عيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الآلي والأنترنيت في مصر والدول العربية، المكتب الجامعي الحديث، مصر، 2006.
- 3/- محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والأنترنيت، المكتب العربي الحديث، مصر، 2007
- 4/- شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنيت، دراسة مقارنة، دار النهضة العربية، مصر، 2009
- 5/- راجي أحسن – الجريمة الإلكترونية، النقطة المطلقة بالنسبة للتكنولوجية المعلوماتية وأبحاث، مجموعة أعمال الملتقى الدولي حول التنظيم القانوني للأنترنيت والجريمة الإلكترونية، جامعة الجلفة 27 – 04 – 2009
- 6/- فايز محمد راجح غلاب: الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه قدمت إلى كلية الحقوق، بن عركون، جامعة الجزائر، 2010.
- 7/- د/يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والأنترنيت، دار العدالة، مصر، 2011.
- 8/- مناصرة يوسف: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستير قدمت إلى كلية الحقوق، بن عكنون، جامعة الجزائر، 2009.
- 9/- Myriam Quemener et Joel Ferry, Cyber criminalité- défi mondial et réponce- economica , Paris, 2007.
- 10/- القانون الإماراتي الإتحادي رقم 02 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات.

- 11/- القانون رقم 04/09 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ولإتصال ومكافحتها الجريدة الرسمية رقم العدد 47 الصادرة بتاريخ 2009/18/16.
- 12/- د/طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني لحماية المعلوماتي، دا الجامعة الجديدة للنشر، مصر، 2009 .
- 13/- معاهدة بودابست BUDAPEST الخاصة بالإجراءالمعلوماتي، المبرمة بتاريخ 2001 11/08 منظر فالمجلس الأوروبي والمعتمدة بتاريخ 2001/11/23
- 14/- زينات طلعت شحادة، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، مكتب صادر ناشرون، لبنان، 2001
- 15/- عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، مصر، 2002
- 16/- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، مصر، 2001 .
- 17/- شرقي أحمد، الجرائم المعلوماتية وفقا لقانون العقوبات وقانون حماية حق المؤلف، مذكرة لنيل إدازة المدرسة العليا للقضاء، الجزائر، 2007.
- 18/- د/علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعة الجديدة للطباعة والنشر، مصر، 1999
- 19/- قشار عطا الله – كزاجهة الجريمة في التشريع الجزائري، بحث مقدم إلى المتقى المغربي حول القانون والمعلوماتية، المنعقد بأكاديمية الدراسات العليا بلبيبا 2009.
- 20/- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى، الجزائر، 2010.
- 21/- أمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر، الجزائر، 2006
- 22/- د/نائلة عادل محمد فريد قورة، جرائم الحاسب اللآلي الإقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، لبنان، 2005.
- 23/- د/عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنيت، دار الكتب القانونية، مصر، 2007
- 24/- د/عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، الحماية الجنائية والمعلوماتية لنظام الحكومة الإلكترونية، دار الفكر الجامعي، مصر، 2003
- 25/- د/عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، دار الفكر الجامعي، مصر، 2007

- 26/- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في التشريع الجزائري والمقارن، دار الجامعة الجديدة للنشر، مصر 2007
- 27/- لسان العرب، ابن منظور للإمام العلامة أبي الفضل جمال الدين محمد بن مكرم ابن منظور الإفريقي المصري، المجلد الثالث عشر " 13 "
- 28/- د/هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة، مصر 1994.
- 29/- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الإصدار الثاني، الأردن، 2009 .
- 30/- رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، دراسات وأبحاث، مجموعة أعمال الملتقى الدولي دول التنظيم القانوني للإنترنت والجريمة الإلكترونية، جامعة الجلفة 27-2009/04/28.
- 31/- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن 2008.
- 32/- د/محمد عبيد سعيد المسامري والخبير عبد الناصر محمد محمود فرغلي، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، المنعقد بمدينة الرياض 2-14/11/2007م الموافق لـ 12-14/11/2007م.
- 33/- كوثر مازوني، الشبكة الرقمية وعلاقتها بالملكية الفكرية، دار الجامعة الجديدة للنشر، مصر 2008
- 34/- بن زيطة عبد الهادي- حماية برامج الحاسوب في التشريع الجزائري، الطبعة الأولى، الدار الخالدونية، الجزائر، 2007،
- 35/- أمال قارة، الجريمة المعلوماتية، رسالة ماجستير قدمت إلى كلية الحقوق، بن عكنون، جامعة الجزائر، 2005.
- 36/- الأمر رقم 05/03 المؤرخ في 19/07/2003 المتعلق بحق لمؤلفة والحقوق المجاورة ج.ر.العدد 44 في 23/ جويلية/ 2003.
- 37/- أحمد خليفة الملط، الجرائم المعلوماتية، دراسة مقارنة، دار الفكر الجامعي، مصر 2006.
- 38/- د/محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، مصر، 2004
- 39/- د/خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2009 .
- 40/- محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2004

- 41/- أمينة حمشاشي، ماهية الجريمة المعلوماتية، دراسات وأبحاث، مجموعة أعمال الملتقى الدولي دول التنظيم القانوني للإنترنت والجريمة الإلكترونية، جامعة الجلفة 27-28/04/2009.
- 42/- سمير شعبان، الجريمة الإلكترونية، مقارنة تحليلية لتحديد مفهوم الجريمة والمجرم، دراسات وأبحاث مجموعة أعمال الملتقى الدولي دول التنظيم القانوني للإنترنت والجريمة الإلكترونية، جامعة الجلفة 27-28/04/2009.
- 43/- فتوح الشاذلي وعفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، 2003
- 44/- د/هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، مصر 1992.
- 45/- د/خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، مصر، 2008.
- 46/- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، المكتبة القانونية لدار المطبوعات الجامعية مصر، 2003 .
- 47/- أسامة أحمد المناعسة وجلال محمد الزغبى وصايل فاضل لهواوشة، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة الطبعة الأولى دار وائل للنشر والتوزيع، الأردن، 2001 .
- 48/- وليد عاكوم - التحقيق في جرائم الحاسوب، المؤتمر العلمي حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، 26-28 نيسان الإمارات المتحدة، 2003.
- 49/- حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم والتقليدية، دراسات وأبحاث مجموعة أعمال الملتقى الدولي دول التنظيم القانوني للإنترنت والجريمة الإلكترونية، جامعة الجلفة 27-28/04/2009.
- 50/- حسينة شرون، فعالية التشريعات العقابية في مكافحة الجرائم الإلكترونية، دراسات وأبحاث مجموعة أعمال الملتقى الدولي دول التنظيم القانوني للإنترنت والجريمة الإلكترونية، جامعة الجلفة 27-28/04/2009.
- 51/- د/هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة مكتبة الآلات الحديثة، مصر، 1994 .
- 52/- نبيل صقر، موسوعة الفكر القانوني، جرائم الكمبيوتر والإنترنت في التشريع الجزائري، دار الهلال للخدمات الإعلامية، الجزائر، 2005 .
- 53/- د/عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، مصر، 2005 .

54/- القانون رقم 22/06 المتضمن تعديل قانون الإجراءات الجزائية الجزائري المؤرخ في 20 ديسمبر 2006 جريدة رسمية رقم 43 عدد 84، 24 ديسمبر 2006 .

55/- د/عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومه للطباعة والنشر، الجزائر، 2005.

56/- الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية الجزائري، المعدل والمتمم بعدد من الأوامر والقوانين آخرها، القانون رقم 06-22 المؤرخ في 20/12/2006 ج 43 العدد 84.

57/- الأمر رقم 66 – 156 المؤرخ في 8 يونيو 1966 تتضمن قانون العقوبات المعدل والتمم والتي جاء فيها يطبق قانون العقوبات على طافة الجرائم التي ترتكب في أراضي الجمهورية.

58/- د/أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، الجزء الأول، الطبعة السابعة، دار هومة، الجزائر، 2007

59/- القانون رقم 575- 2004 الصادر بتاريخ 21/جوان/2004 المتضمن تعديل قانون العقوبات الفرنسي.

60/- دستور الجمهورية الجزائرية لسنة 1996

61/- Christiane Peral – Schuhil- Cyber droit , le droit A l'épreuve del'internet , 3^e édition, Dalloz, 2002.

62/- الأزرق بن عبد الله وأ/ أحمد عمراني، نظام المعلوماتية في القانون الجزائري واقع وآفاق، المتمر السادس لجمعية المكتبيات والمعلومات السعودية البيئة العلوم الأمانة، المفاهيم والتشريعات والتطبيقات، المنعقد مدينة الرياض، 21-22 ربيع الثاني 1431 هـ الموافق ب 6 -7 أفريل 2010.

63/- د/محمد حماد مرهج الهيتي، جرائم الحاسوب، دراسة تحليلية، الطبعة الأولى، دار المناهج للنشر والتوزيع، الأردن، 2006.

64/- Christiane Peral – Schuhil- Cyber droit , le droit A l'épreuve del'internet , 5^e édition, Dalloz, 2008.

65/- د/عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول، الجريمة، الطبعة السابعة، ديوان المطبوعات الجامعية، الجزائر، 2009.

66/- د/عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دراسة قانونية متعمقة في القانون المعلومات، يدار الفكر الجامعي، الإسكندرية.

67/- د/مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، دراسة مقارنة، دار الكتب القانونية، مصر، 2005.

- 68/- قانون العقوبات الجزائري رقم 15/04 المؤرخ في 10 نوفمبر 2004. المعدل والمتمم.
- 69/- هلالى عبد اللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية، على ضوء إتفاقية بودابست الموقعة في 23/ 12/ 2001، الطبعة الأولى، دار النهضة العربية، مصر، 2003.
- 70/- مصطفى مجدي هرجة، الحيازة داخل وخارج دائرة التجريم، دار الثقافة للطباعة والنشر، مصر 1989.
- 71/- هشام سعد الدين، جريمة الإتفاق الجنائي، المكتب الفني للإصدارات القانونية، مصر، 1999
- 72/- د/محمود نجيب حسني، شرح قانون العقوبات القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الإحترازي، الطبعة الرابعة، دار النهضة العربية، مصر، 1977.
- 73/- نظام مكافحة الجرائم المعلوماتية السعودي ، الصادر بالمرسوم الملكي (م/17)، المؤرخ في 07 ربيع الأول 1428 هـ الموافق ل 26/03/2007 ، بناء على قرار مجلس الوزراء رقم 79.
- 74/- سمير الشناوي، الشروع في الجريمة، دراسة مقارنة، الطبعة الثالثة، مصر، 1992 .
- 75/- فضيل العيش، قانون العقوبات وفقا للتعديلات الأخيرة، منشورات بغدادى، الجزائر، 2007.
- 76/- د/رؤوف عبيد، مبادئ القسم العام من التشريع العقابي، الطبعة الرابعة، دار الفكر العربي مصر، 1979
- 77/- د/علي عبد القادر القهوجي، شرح قانون العقوبات القسم العام، نظرية الجريمة، الطبعة الأولى منشورات المجلس الحقوقية، لبنان، 2008.
- 78/- د/رمسيس بهنام، النظرية العامة للمرجم والجزاء، منشأة المعارف الإسكندرية (مصر)، 1995.
- 79/- القانون رقم 23/06 المتضمن تعديل قانون العقوبات الجزائري المؤرخ في 20/ديسمبر/2006 الجريدة 43 العدد 84.
- 80/- صمودي سليم، المسؤولية الجزائية للشخص المعنوي، دراسة مقارنة بين التشريع الجزائري والفرنسي، دار الهدى، الجزائر، 2006 .