الجريمة المعلوماتية

أولا: تعريف الجريمة المعلوماتية : اختلف الفقه في تحديد مفهوم الجريمة المعلوماتية بين اتجاهين رئيسيين:

1. الاتجاه الموسع الذي يرى أنها تشمل كل سلوك إجرامي يتصل بالمعلوماتية اتصالا مباشرا أو غير مباشر، وينتج عنه ضرر أو كسب غير مشروع، ويهدف هذا الاتجاه إلى شمول كافة الأفعال غير المشروعة التي تستعمل التقنية كوسيلة أو كهدف.

2. الاتجاه الضيق الذي يربط الجريمة المعلوماتية بالأفعال التي يكون فيها الحاسب الآلي أو البيانات المعلوماتية محلا أو أداة للجريمة، مثل اختراق الأنظمة أو التلاعب بالبيانات، وهو التعريف الذي تبناه مكتب تقييم التقنية بالولايات المتحدة الأمريكية باعتباره الأقرب للطابع الفني للجريمة المعلوماتية.

اعتمد المشرع الجزائري مصطلح **المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون 15-04 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات**، ثم استعمل لاحقا مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في القانون 09-04 المؤرخ في 5 أوت 2009، المخصص للوقاية من هذه الجرائم ومكافحتها وقد نصت المادة 2 من القانون المذكور على أن الجريمة المعلوماتية هي: **كل جريمة تمس بأنظمة المعالجة الآلية للمعطيات كما هي محددة في قانون العقوبات، أو أي جريمة ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام اتصالات إلكترونية.**

ثانيا: خصائص الجريمة المعلوماتية: تمتاز الجريمة المعلوماتية بعدة خصائص تميزها عن باقي الجرائم التي تصنف في خانة الجرائم الكلاسيكية ، أهمها:

1.جريمة عابرة للأوطان: نظرا للوسيلة المستعملة فيها وهي أجهزة الكمبيوتر ، جعل من هذه الجريمة عابرةللحدود ، لا ترتبط بإقليم جغرافي معين ، تكفي توفر جهاز حاسوب في أي مكان في الكرة الأرضية ، يكون مزودا بالشبكة المعلوماتية لارتكاب جريمة معلوماتية.

هذا الوضع جعل أمام الدول اللجوء إلى حتمية التعاون والتنسيق الدوليين من أجل مكافحة هذه الجرائم بكافة الوسائل المتاحة بداية من خلال **إبرام اتفاقيات ومعاهدات دولية** وفتح المجال واسعا للقيام بإجراءات التحري والتدقيق اللازمين لكشف مرتكبي هذه الجرائم من خلال تحديد القانون الواجب التطبيق في هذه الحالات، وتحديد الدولة صاحبة الاختصاص القضائي.

2.جريمة يصعب إثباتها: ما يميز هذا النوع من الجرائم هو **صعوبة إيجاد الدليل المادي** لإدانة مرتكبيها بسهولة ويسر لأن محو الدليل إجراء بسيط، خاصة مع ما يوفره العالم من مجرمين معلومات يين محترفين برعوا في هذا المجال وتفننوا في علم القرصنة والمعلومات، لذا يصعب معهم إثبات الفعل الجنائي المرتكب على عكس الجرائم العادية المرتكبة.

كما ساهم في صعوبة اكتشاف هذه الجرائم واثبات مرتكبيها هو عدم توفر مختصين لدى رجال الأمن والمحققين، يضاهي مستوى هؤلاء المجرمين المعلوماتيين المحترفين في هذا النوع من الإجرام .

3. جريمة آثارها وخيمة على الصعيد الاقتصادي: نظرا لشمول شبكة الانترنت والكمبيوتر أجهزة اقتصادية حساسة شملت أغلب معاملاتها، حيث تسببت الجرائم المعلوماتية بتكبيد هذه المؤسسات والشركات خسائر مالية ضخمة نتيجة اختراق أنظمتها المعلوماتية من طرف مجرمين مختصين في هذا المجال إضافة إلى سرقة أموال كبيرة من عديد البنوك باختراق حسابات الزبائن ، وتدمير نظام التشغيل أو نشر فيروسات أو إفشاء بيانات.

4.جريمة ناعمة : لا يحتاج هذا النوع من الجرائم إلى بذل مجهود عضلي أو جهد بدني معين المستخدم في الجرائم الأخرى كالقتل أو السرقة مثلا ، بل يحتاج إلى مجهود ذهني يستخدمه المجرم المعلوماتي ، كما لا يحتاج إلى سن محدد، فكثير من هذه الجرائم يرتكبها قصر لم يبلغوا سن الرشد ، ولا تقتصر على جنس الرجال ، فكثير من النساء من تورطن في هذا النوع من الجرائم، لذلك وصفت بالناعمة.

ثالثا: أركان الجريمة المعلوماتية:

الفرع الأول: الركن الشرعي للجريمة المعلوماتية:

يظهر الركن الشرعي للجريمة في وجود نصوص قانونية تواجه الزحف الذي عرفته الجرائم التي مست شبكة الانترنت و الاعتداءات التي شملت خصوصية الأفراد والهيئات ، حيث لجأت أغلب التشريعات الوطنية إلى فرض رقابتها وتجريمها على أوجه مختلفة للجريمة المعلوماتية.

ففي الولايات المتحدة الأمريكية نص قانونها الفدرالي على مكافحة هذه الجرائم ، كما نصت على ذلك أغلبية ولايتها ، و ألحقت كندا تجريمها بقانون العقوبات ، في حين في فرنسا تم إصدار تشريع مستقل لها بموجب القانون رقم 78/17 المؤرخ في1978/01/16المتعلق بقانون الإعلام الآلي والحرياتLoi sur l'informatique et "

La liberté.

بينما في الجزائر فقد نص المشرع على مكافحة الجرائم المعلوماتية من خلال تعديله لقانون العقوبات لسنة 2004، وإضافته للقسم 7 مكرر الموضوع تحت مسمى " المساس بأنظمة المعالجة الآلية للمعطيات Des atteintes aux systèmes de " traitement automatisé des donnes.

تبنى المشرع للدلالة على الجريمة المعلوماتية مصطلح «المساس بأنظمة المعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات محلا للجريمة، وتمثل المعالجة الآلية للمعطيات الشرط الأول الذي لا بد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة.

المشرع الجزائري وضع تعريفا للجريمة المعلوماتية في المادة الثانية من القانون رقم 90/04 الصادر في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والذي دخل حيز التنفيذ بموجب الجريدة الرسمية عدد 47.

جرم المشرع الاعتداء على أنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية وظهور أشكال جديدة من الجرائم وهو ما دفع المشرع إلى تعديل قانون العقوبات بموجب القانون رقم 04/15 الصادر في 10/11/2004 المتمم للأمر رقم 156/66 المتضمن قانون العقوبات والذي أفرد القسم السابع منه تحت عنوان : المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن (8) مواد من المادة 394 مكرر إلى غاية 394 مكرر 7.

الفرع الثاني: الركن المادي للجريمة المعلوماتية

عرفه الفقهاء على انه كل فعل ينتج عنه توقيف نظام المعالجة الآلية للمعطيات عن أدائه الطبيعي ، وبالرغم من الجدل الفقهي الذي صاحب مفهوم النظام المعلوماتي حول شموله جل عناصره من عدمه، إلا أن غالبية الفقه ترى بضرورة عدم الاشتراط أن

يقع فعل التعطيل أو الإضرار للنظام كله بل يكفي أن يؤثر على أحد من عناصره فقط، كجهاز الحاسوب نفسه أو تمتد إلى شبكات الاتصال أو البرامج والمعطيات .

وعليه نكون أمام الركن المادي للجريمة المعلوماتية إذا تم الاعتداء على النظام المعالجة الآلية للمعلومات أو سلامته، كما نكون في حالة الدخول والبقاء غير المشروع في هذا النظام أو الحذف أو التغيير أو في المعطيات، كما يمكن اعتبار التخريب أو أي إتلاف في نظام الاشتغال اعتداءات مادية (المادة 394 مكرر ق ع ج). كل تلك الصور تضمنها المشرع الجزائري من خلال قانون العقوبات المعدل السنة2004، أضاف إليها عديد صور المادية الكافية لقيام الركن المادي للجريمة المعلوماتية كإدخال معلومات في نظام المعالجة الآلية أو إزالتها(المادة 394 مكرر).

يتحقق الركن المادي بكل فعل خارجي ملموس يشكل اعتداء على نظام معلوماتي أو بيانات يتحقق : الكترونية، ويأخذ هذا السلوك صورتين:

- **فعل إيجابي : مثل اختراق نظام معلوماتي أو إدخال بيانات مزورة أو حذفها عمدا.**
- **فعل سلبي : كالامتناع عن حماية الأنظمة رغم الالتزام القانوني بذلك.**

الفرع الثالث: الركن المعنوي للجريمة المعلوماتية

يشترط في الجريمة المعلوماتية توافر القصد الجنائي، أي علم الجاني بعدم مشروعية فعله وإرادته في تحقيق النتيجة الإجرامية، ويختلف هذا القصد باختلاف نوع الجريمة:

ففي جريمة الدخول غير المشروع إلى النظام المعلوماتي، يشترط العلم بعدم الإذن، وتنتفي الجريمة إذا تم الدخول عن طريق الخطأ وغادر الفاعل فور علمه.

أما في جرائم الاحتيال الإلكتروني، او التزوير المعلوماتي فيتطلب المشرع قصدًا جنائيا عاما وخاصا يتمثل في نية تحقيق كسب غير مشروع أو إلحاق ضرر بالغير.

رابعا: الجريمة المعلوماتية في مجال قانون العقوبات الجزائري

خطى المشرع الجزائري خطوات كبيرة في مجال مكافحة الجريمة المعلوماتية، يعتبر القانون الجزائري سباقا في مجال مواكبة التشريعات الخاصة في مثل هذا النوع من التجريم، حيث أقر بتجريم صور الاعتداء على شبكة الانترنت والمساس بالبيانات المعالجة آليا ، في إطار أحكام التعديل الذي شمل قانون العقوبات لسنة 2004 ، بموجب القانون رقم 04-15 المؤرخ في 10/11/612004 ، في إطار أحكام القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات ، هذه المواد هي من 394 مكرر إلى 394 مكرر 7 ، والمتمثلة في الجرائم التالية:

<u>1. جريمة الدخول في كل أو جزء من منظومة للمعالجة الآلية لمعطيات(م 394مكرر1) أو محاولة ذلك:</u>

تنص المادة 394 مكرر على أنه " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الإلية للمعطيات أو يحاول ذلك، لقد جرم المشرع فعل الدخول بطريق غير شرعية إلى أي منظومة معلوماتية وذلك حين عبر عنه بطريق الغش ، كما أن المشرع لم يفرق بين الدخول إلى جزء من المنظومة أوكلها.

وهنا سيتخلص من نص المادة ما يلي:

- التسليم بتوفير القصد الجنائي بمجرد الدخول إلى نظام معلوماتي عن طريق الغش.
- عدم الاعتداد بنتائج هذا الدخول حتى ولو يسبب أي تخريب أو إضرار بالبيانات ، لكون اعتبارها جريمة وقتية
- مجرد المحاولة يعتبر في حد ذاته جريمة حتى وان لم يتحقق فعلا.

2.جريمة البقاء (م 394 مكرر/1): بالرجوع إلى نفس المادة السابقة وفي نفس الفقرة 1 فان المشرع قد فرق بين فعل الدخول غير الشرعي والبقاء فيه، وذلك باعتبار كل فعل يعتبر مجرما ، فالبقاء قرينة على توفر القصد الجنائي ، كما تعتبر جريمة مستمرة على عكس الجريمة الأولى، غير أن المشرع لم يفرق بين البقاء غير الشرعي أو مجرد المحاولة على غرار الجريمة الأولى.

3.جريمة حذف أو تغيير في معطيات المنظومة (م 394 مكرر/ 2) كنتيجة للدخول غير الشرعي أو البقاء واعتبارهما كجريمتين مضاعفتين: تنص المادة 394 مكرر في فقرتها الثانية على أنه تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة وعليه فان المشرع الجزائري فرق بين عملية حذف البيانات وعملية تغييرها ، اللذين يعتبرهما كنتيجة لفعل الدخول غير الشرعي أو البقاء كما اعتبرهما جريمة مضاعفتين وذلك نتيجة لخطورة النتائج المترتبة عنهما.

4.جريمة تخريب نظام الاشتغال كنتيجة للدخول الغير الشرعي أو البقاء (م394 مكرر/3): نصت المادة 394 مكرر 3 على أنه وإذا ترتب على الأفعال المذكورة أعلاه تخريب اشتغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج وعلى أساس ذلك لم يعتبر المشرع الجزائري جريمة تخريب نظام الاشتغال جريمة مستقلة بذاتها على غرار الدخول غير الشرعي أو البقاء ، بل باعتبارها نتيجة للجرائم السابقة، وذلك يرجع إلى أنه من الممكن حدوث تخريب لهذا النظام ابتداء دون توفر القصد الجنائي إلا عندما يكون كنتيجة لجريمة سابقة.

5. جريمة إدخال معطيات في نظام المعالجة الآلية أو إزالتها أو تعديلها عن طريق الغش (م 394 مكرر/1)

نصت المادة 394 مكرر 1 على أنه يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500.000 إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل" ومنه فان المشرع قد اعتبر أن إدخال معطيات مغشوشة في نظام المعالجة الآلية جريمة معلوماتية تستوجب عقوبة ، والتي ضاعفها إذا ما قورنت بالعقوبات السابقة ، وذا كان قد ربط فعل الحذف بالنتيجة المترتبة عن الدخول غير الشرعي أو البقاء ، فقد اعتبر جريمة الإزالة جريمة مستقلة في حد ذاتها تستوجب نفس العقوبة السابقة بالرغم من اتفاقية بودابست وكذا المشرع الفرنسي استعمل مصطلح الحذف" لاستخدامه ضمن نفس المعنى.

وان ذهبنا إلى المعنى اللغوي فان معنى الحذف هو الإسقاط بينما يعني مصطلح الإزالة هو الإبعاد من المكان، ومنه فان المشرع قد يكون فرق في الآثار بين الفعلين، فحذف بيانات الكترونية معينة بكون بإسقاطها من موقعها في النظام المستهدف ولو كان بصفة مؤقتة ، مما يعني ظرفيتها وبذلك تكون قابلة للاسترجاع عن طريق برامج بالرغم من صعوبتها،

ولكن إزالة البرامج تهدف إلى التخلص نهائيا منها وبشكل كامل لذلك يكون المشرع قد فرق بين الفعلين الإجراميين واعتبر الفعل الأخير أشد وطأة لذا فرق بين عقوبة كل فعل مجرم منهما.

6.جريمة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات عمدا وعن طريق الغش (م 394 مكرر(2/1): نصت المادة 394 مكرر 2 في فقرتها الأولى على انه يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا ، وعن طريق الغش "تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو

مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم"، وعليه فإننا نكون أمام توفر عدة شروط القيام هذه الجريمة المعلوماتية ، وهي:

أ- توفر القصد الجنائي لدى الجاني : في هذه الحالة ابتداء لأقر المشرع كشرط أساسي الإقرار هذا الفعل المجرم توفر القصد الجنائي لارتكابه لان علمية تصميم برنامج معين أو بحث في برنامج معين آخر أو نشره وحتى الاتجار فيه لا يعتبر جرما في حد ذاته، إذا لم يسبقها توفر نية مسبقة لارتكاب جريمة معلوماتية تعتمد بالأساس على توفر علم مسبق لدى الجاني بان هذا البرنامج مغشوش.

ب - أن يكون هذا الجرم مرتبطا بأفعال محددة وهي : تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات ، وعليه فان أي فعل آخر يمس هذه المعطيات لا يندرج ضمن هذا الإطار.

ج- أن تكون المعطيات محل الجرم مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية: وهنا يكون المشرع قد اعترف ضمنا بضرورة أن تكون المعطيات تتوفر على قدر كاف من الحماية، لأن المساس بالمعطيات المتاحة والمتوفرة للجمهور لا يمكن أن تكون محل متابعة جزائية ، وبذلك يكون المشرع قد تأثر بالاتفاقيات والقانون المقارن الذي سعى إلى هذا الاتجاه لاسيما اتفاقية بودابست.

كما يمكن إن يكون هذه الجرائم سببا غير مباشرا في ارتكاب الجرائم المعلوماتية السابقة، وعليه فإن المشرع قد قرر لها نفس العقوبة السابقة.

7.جريمة حيازة أو إفشاء أو نشر أو استعمال معطيات المتحصل عليها من الجرائم المذكورة سابقا عمدا وعن طريق الغش (م 394 مكرر(2/2) ان فان حيازة معطيات أو إفشائهاأو نشرها أو استعمالها يعتبر جريمة يعاقب عليها القانون.

8-النصب الالكتروني :تعتبر الجرائم المعلوماتية التي تستهدف المال من أشهر الجرائم وأخطرها خاصة مع انتشار وسائل الانترنت والحواسيب ، فأصبح المجرم المعلوماتي يبحث عن كل الطرق للبحث عن المال المعلوماتي في محاولة منه للوصول إليه مستعملا طرقا غير مشروعة ، وعليه طرح التساؤل بداية عن المال المعلوماتي المعني بالحماية القانونية ؟

يعتبر المال المعلوماتي المعني بالحماية القانونية كل مال الكتروني قابل للنقل والتملك" كما يمكن تعريفه بأنه المال الموجود في الحاسوب سواء في صورة معلومات أو بيانات الكترونية في أي صورة كان عليها سواء كان مخزنا على أقراص صلبة أو دعامات تخزين خارجية ، فهو بذلك كل المدخلات الالكترونية التي لها من القيمة المادية مما يجعلها قابلة للتملك وتكتسي الحماية القانونية .

وبالرجوع إلى تعريف المشرع الجزائري الجريمة النصب من خلال ما تضمنته المادة 372 ق ع فنجده عرفها على صيغة العموم، ولم يحدد جريمة النصب الالكتروني في حد ذاتها ، حيث عرف جريمة النصب على أنها " كل من توصل إلى استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 دينار، وإذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد إصدار أسهم أو سندات أو أذونات أو حصص أو أية سندات مالية سواء لشركات أو مشروعات تجارية أو صناعية فيجوز أن تصل مدة الحبس إلى عشر سنوات والغرامة إلى 200.00 دج.

وعليه فإن كان المشرع لم يربط جريمة النصب بالجريمة المعلوماتية ، ولم يحدد وسيلة بعينها ، ولكن يمكن إسقاطها إذا ما تم توفر شروطها ، والمتمثلة في ما يلي:

أ - تحديد هوية مرتكب جريمة النصب الالكتروني: أن يكون مرتكب الجرم شخصا معينا ، لأنه لا يمكن للبعض تصور أن يقوم بهذه الجريمة جهاز الحاسوب بنفسه لكن الأنظمة الانجلوسكسونية وكذلك جانب من الفقه الفرنسي قبل بفكرة تطبيق العقوبة على الأنظمة المعلوماتية ، في حين طبقت بعض التشريعات الأخرى كالولايات المتحدة الأمريكية القواعد الخاصة بالاحتيال في مجال البريد والتلغراف والبنوك على حالة النصب الالكتروني.

ب -أن نكون أمام تعامل قانوني للمال المعلوماتي : بحيث تشمل تصرفات ومعاملات حددها القانون وهي : استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها ، كما لم يفرق المشرع بين الحصول على هذه المعاملات وبين الشروع فيها.

ج-استعمال وسائل احتيالية : حدد المشرع صور الجرائم الاحتيالية وهي:

- استعمال أسماء أو صفات كاذبة
- استعمال سلطة خيالية
- استخدام الخيال المالي الثقة
- إحداث الأمل في الفوز بأي شيء
- زرع الخوف في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها.

د -ان يكون الهدف منها سلب كل ثروة الغير أو بعضها : وهو ما يعبر عن الركن المعنوي أي القصد الجنائي لدى المجرم المعلوماتي ، كما أن المشرع اعتبر عملية الشروع معاقبا عليها هي كذلك.

هـ-تشديد العقوبة إذا تعلق الأمر بتعاملات تخص شركات أو مشروعات تجارية أو صناعية : نصت المادة 372 ق ع في آخر فقرة 1 على أنه إذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد إصدار أسهم أو سندات أو أذونات أو حصص أو أية سندات مالية سواء الشركات أو مشروعات تجارية أو صناعية فيجوز أن تصل مدة الحبس إلى 10 سنوات والغرامة إلى 200.000 دج.

و أن تتم هذه التصرفات بواسطة استخدام أنظمة معلوماتية : وهو ما يعبر عن توفر الركن الافتراضي للجريمة المعلوماتية ، أي يتم استخدام هذا الجرم بواسطة نظام معلوماتي متوفر على نظام المعالجة الآلية للمعطيات.

ومن أبرز الأمثلة الخاصة بالنصب الالكتروني نجد:

- من أبرز القضايا التي حكمت عليها محكمة النقض الفرنسية حول شخص دخل ساحة انتظار السيارات، ولكنه عوض وضع النقود الأصلية في الآلة الالكترونية وضع قطعة نقدية عديمة القيمة، فترتب عن ذلك تشغيل الآلة وتحرك العقارب ، حيث اعتبرتها جريمةنصب الكتروني، حتى وان كان المعني لم يحصل على أي شيء مادي.
- الاحتيال على الطريقة النيجيرية حيث اشتهرت هذه الطريقة على أساس استعمال رسائل الكترونية توهم الأشخاص أن المعني يحوز على أموال تصل ملايين الدولارات في بلده الأصلي وانه يحكم معاناته من مشاكل سياسية أنه يحتاج إلى فتح حساب باسم الضحية مع تقديم نسبة من 10 إلى 15% من مبلغ العملية، شريطة تقديم تسبيق مبلغ أولي، حيث تعرض الكثير من الضحايا إلى هذه الجريمة.

9-السرقة الالكترونية : إذا كانت تعرف السرقة في مفهومها التقليدي فقها بأنها اختلاس المال منقول بنية تملكه والذي تعود ملكيته للغير فالسرقة الالكترونية أو المعلوماتية لا تختلف في مفهومها التقليدي من حيث توفر عنصري الاختلاس والتملك غير المشروع للمال المملوك للغير، ولكن الاختلاف في الطريقة للحصول على هذا المال وهي استعمال وسائل معلوماتية، حيث عرفها البعض على أنها كل فعل يأخذ صور الاختلاس ويمس ببيانات المجني عليه .

و بالرجوع إلى النص التشريعي الجزائري فالبرغم من تعديله لقانون العقوبات السنة 2004 وتطرقه لنظام المعالجة الآلية للمعطيات كما سبق وان تم التطرق إلى ذلك، إلا انه لم يتعرض إلى جريمة السرقة المعلوماتية أو الالكترونية بشكل صريح ، وعليه فإنها تخضع في أحكامها إلى أحكام وقواعد السرقات بالمفهوم التقليدي ، حالها في ذلك حال جريمة النصب الالكتروني ، وذلك بخضوعها إلى أحكام نص المادة 350 من ق ع التي تنص على أنه " كل من اختلس شيئا غير مملوك له بعد سارقا ويعاقب بالحبس من سنة إلى 5 سنوات وبغرامة من 100.000 دج إلى 500.000 دج

إن عدم تحديد المشرع للشيء المختلس يجعل من إمكانية إدراج المعلومات والبيانات الواردة في الحواسيب طرحا ممكنا، ومنه قبولها كركن مادي لجريمة السرقة المعلوماتية في غياب الركن الشرعي الصريح.

10-استغلال بطاقات الائتمان بطريقة غير شرعية:

حيث يستطيع صاحب هذه البطاقة تسديد التزاماته مباشرة حتى ولو لم يكن يملك حسابا او رصيدا لدى البنك مصدر البطاقة ، ولكن يلتزم بتسديد تلك الالتزامات في اجل معين ، من أشهر هذه البطاقات Visa و Master card ، كما ساهمت هذه البطاقات في تشجيع التسوق عبر شبكة الانترنت في مقابل زيادة حجم التخوف من الجرائم المرتبطة من استغلال هذه البطاقات بطريقة غير شرعية ، ومن صور الاعتداءات التي تطال بطاقات الائتمان : تتمثل هذه الاعتداءات في صورتين:

- الاعتداءات التي تطال البطاقة في حد ذاتها : كسرقتها أو ضياعها واستعمالها على نحو غير مشروع
- الاعتداءات التي تطال البيانات الموجودة في البطاقة وذلك بتزوير البيانات الموجودة في البطاقة.