ASJP
Algerian Scientific Journal Platform

مجلة افاق للعلوم
Issn: 2507-7228 – Eissn: 2602-5345
https://www.asjp.cerist.dz/en/PresentationRevue/351

المجلد:07 العدد: 01(2022) ص457-468

الحماية الجنائية للمعلوماتية في التشريع الجزائري

Criminal protection for informatics in Algerian legislation

عمري فيصل
جامعة الجزائر 01 (الجزائر)
sissi.mmh@gmail.com

معلومات المقال

تاريخ الارسال:
28 ماي 2021
تاريخ القبول:
11 سبتمبر 2021

الكلمات المفتاحية:
- ✓ التجديد
- ✓ البنية التركيبية
- ✓ الإيقاعية

الملخص:

يبدو أن هناك محاولات لتطوير المنظومة القانونية وتكييفها مع المعطيات الدولية من خلال اصدار تشريعات تواكب التطور الحاصل في المجال المعلوماتي، ومن أبرز تلك التعديلات ما أورده في 03-05 الصادر في 2003/07/19 والمتعلق بحقوق المؤلف والحقوق المجاورة والتي أدرجت برنامج الحاسوب ضمن المؤلفات مضمونة الحماية، بالإضافة إلى النصوص الخاصّة التي تبنّاها المشرّع في تعديله الأخير للقانون (04–15) المؤرخ في 2004/11/10 المعدّل والمتمّم للأمر (66–156) المؤرخ في 1966/06/08، المتضمّن قانون العقوبات، ويشمل المواد من 394 إلى 394 مكرر 7، فتعتبر مكافحة فعالة نظرا لما تمتاز به من شمولية، بحيث جاءت لتشمل أغلب الجرائم التي قد تمس نظام المعالجة الآلية للمعطيات بصفة عامة، وكذا تضمنت أغلب الجرائم التي قد تمس البيانات والمعطيات المكونة لهذا النظام.

Article info

Received
28 May 2021
Accepted
11 September 2021

Keywords:
- ✓ *Synthetic structure*
- ✓ *Rythmic*
- ✓ *structure Semantic*

Abstract :

It seems that there are attempts to develop the legal system and adapt it to international data through the issuance of legislation that keeps pace with the development in the information field, and among the most prominent of these amendments is what was mentioned in 03-05 issued on 07/19/2003 related to copyright and related rights, which included the computer program among the literature Guaranteed protection, in addition to the special provisions adopted by the legislator in his last amendment to Law (04-15) of 10/11/2004 amending and supplementing Ordinance (66-156) of 06/08/1966, containing the Penal Code, and including articles 394 to 394 bis 7, which is considered an effective fight due to its comprehensiveness, as it came to include most crimes that may affect the automated data processing system in general, as well as most crimes that may affect the data and data that make up this system.

مقدمة:

لقد احتلت المعلومات المرتبة الأولى في جميع الدول المتقدمة، واكتسبت الأهمية القصوى في مختلف المجالات، واعتبرت معيارا لقياس مدى تحضر الأمم، ولقد صاحب هذا الاهتمام تطورا ملحوظا في نظم المعلومات الآلية أفرزته التكنولوجيا فائقة السرعة القائمة على الحاسب الآلي كوسيلة رئيسية لحفظ ومعالجة وتشغيل البيانات أو المعلومات داخل معظم المؤسسات الحكومية بل وبين الأفراد في حياتهم اليومية وكان من الطبيعي أن يصحب هذا التطور التكنولوجي المذهل تصاعد السلوك الإجرامي واتخاذه أبعادا جديدة لم يعدها الفقه القانوني من قبل، وبات عليه مواكبة هذه الأنماط الإجرامية الجديدة بالمنع والقمع.

الجريمة المعلوماتية le délit informatique هي كل نشاط إجرامي يؤدي نظام الحاسب الآلي دورا فيه، سواء تمثل هذا الدور في إتمام النشاط الإجرامي أو في كونه محلا له[1]، فهي ذات طابع تقني، كما أنه من السهل إخفاء معالمها وصعوبة تتبع مرتكبيها، ويصعب على المحقق التقليدي التعامل مع هذه الجرائم، فهي تتسم بالغموض والتعقيد والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية، وكل هذا بسبب الطابع التقني الصرف الذي تتميز به عن الجرائم العادية الأخرى.

من هذا المنطلق كان لزاما أن يواكب هذا التقدم فهم ودراية كاملين بالجريمة المعلوماتية ووسائل مكافحتها سواء من الناحية التقنية وهو عمل المتخصصين في مجال تكنولوجيا المعلومات، أو من الناحية القانونية وهو عمل رجال الفقه والقانون، حيث وضعت مختلف التشريعات نظما حمائية مختلفة تتراوح بين البعد الوقائي بوضع أنظمة مراقبة، وكذا وضع قوانين ردعية كقوانين المسؤولية المدنية والمسؤولية الجزائية في حالة حدوث أي مخالفة مجرمة أو تحقق أي ضرر، هذه الأخيرة التي ينحصر فيها موضوع الحماية الجنائية للمعلوماتية، اعتبارا لما قد يقع عليها من اعتداء يمس مباشرة مؤلف البرنامج ونظرا لما يلحقه من أضرار مادية أو معنوية لهذا الأخير، مما سيفتح مجالا واسعا لتدخل المشرع لتجريم كل المخالفات الواقعة على هذه البرامج.

بناء على ماسبق نطرح الإشكالية التالية: ما مدى فعالية النصوص التشريعية التي أقرها المشرع لمواجهة الجريمة المعلوماتية؟

المبحث الأول: ماهية الجريمة المعلوماتية

لقد أسهبت بعض التعريفات في التعامل مع الجريمة المعلوماتية كجريمة خاصة دون الإجابة مسبقا على مفهوم هذه الجريمة وموضوعها باعتبارها ظاهرة إجرامية مستجدة متميزة من حيث خصائصها وسمات مرتكبيها وتصنيف السلوك الإجرامي المجسد لها، وهذا ما حاولنا التطرق له من خلال هذا المبحث.

المطلب الأول: مفهوم الجرائم المعلوماتية

سنتناول بالدراسة مفهوم الجريمة المعلوماتية وتبيين أهدافها في الفرع الأول، ثم نتطرق إلى خصائص هذه الجرائم وأهم سمات مرتكبيها في الفرع الثاني.

الفرع الأول: التعريف والأهداف

إن الجريمة المعلوماتية باعتبارها ظاهرة جديدة تثير الكثير من التساؤلات التي تتعلق بتحديد مفهومها، وأهدافها، بالإضافة إلى البحث عن خصائصها وسمات مرتكبيها ومن ثمة كيفية التعامل معها.

أولا: تعريف الجريمة المعلوماتية

يمكن تقسيم هذه التعريفات إلى طائفتين رئيسيتين[2]:

1/ طائفة تقوم على معيار واحد، وتشمل تعريفات قائمة على معيار قانوني كتعريفها بدلالة موضوع الجريمة أو السلوك محل التجريم أو الوسيلة المستخدمة[3].

2/ طائفة التعريفات القائمة على تعدد المعايير، وتشمل التعريفات التي تبرز موضوع الجريمة وأنماطها، وبعض العناصر المتصلة بآليات ارتكابها أو سمات مرتكبيها.

أما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة، فإن أصحابها ينطلقون من أن جريمة الحاسب الآلي تتحقق باستخدام الحاسب وسيلة لارتكاب الجريمة، ومن هذه التعريفات أنها "فعل إجرامي يستخدم الحاسوب في ارتكابه كأداة أساسية"[4].

ثانيا: أهداف الجرائم المعلوماتية

تهدفُ الجرائم المعلوماتية لجملةٍ من الغايات، منها:

1/ تحصيل مكسب سياسي أو مادي أو معنوي غير مشروع عبر تقنيات المعلومات كعمليّات تزوير بطاقات الائتمان، والاختراق، وتدمير المواقع على الإنترنت وسرقة الحسابات المالية[5].

2/ تحصيل معلومات ووثائق سريّة للمؤسسات والجهات الحكوميّة والمصرفية والشخصية لابتزازهم من خلالها[6].

3/ الوصول لمعلوماتٍ غير مُخوّل للعامّة الاطلاع عليها بشكلٍ غير مشروع، وسرقتها أو حذفها أو تعطيلها أو التعديل عليها لتحقيق مصالح مرتكب الجريمة[7].

الفرع الثاني: خصائص الجرائم المعلوماتية وسمات مرتكبيها

تتميز الجرائم المعلوماتية بعدّة خصائص تميزها عن غيرها من الجرائم التقليدية، وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عددا من السمات والخصائص.

أولا: خصائص الجرائم المعلوماتية

تتميّز الجرائم المعلوماتية بعدّة خصائص منها:

1/ صعوبة معرفة مرتكب الجريمة، إلّا باستخدام وسائل أمنيّة ذات تقنية عالية[8].

2/ صعوبة قياس الضّرر المترتّب عليها، كونه ضرراً يمسّ الكيانات المعنوية ذات القيم المعنوية أو القيم الماديّة أو كلاهما[9].

3/ سهولة الوقوع فيها؛ بسبب غياب الرّقابة الأمنية.

4/ سهولة إخفاء وطمس مَعالم الجريمة وآثارها والدّلائل التي تُدلّ على مرتكبها.

5/ هي أقلّ جهداً وعُنفاً جسديّاً من الجرائم التّقليدية.

6/ سلوكٌ غير أخلاقيّ في المجتمع.

7/ جريمةٌ لا تتقيّد بمكانٍ أو زمانٍ مُحدّدين.

ثانيا: خصائص المجرم المعلوماتي

1/ المجرم المعلوماتي مجرم متخصص: تبين في عديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يبين أن المجرم الذي يرتكب الجريمة المعلوماتية هو مجرم في الغالب متخصص في هذا النوع من الإجرام[10].

2/ المجرم المعلوماتي مجرم عائد إلى الإجرام: يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة في المرة السابقة، ويؤدى ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلى تقديمهم إلى المحاكمة .

3/ المجرم المعلوماتي مجرم محترف: يتمتع المجرم المعلوماتي باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر الذي يقتضى الكثير من الدقة والتخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية.

4/ المجرم المعلوماتي مجرم غير عنيف: المجرم المعلوماتي من المجرمين الذين لا يلجؤون إلى العنف بتاتا في تنفيذ جرائمهم وذلك لأنه ينتمي إلى إجرام – الحيلة – فهو لا يلجأ إلى العنف في ارتكاب جرائمه، وهذا النوع من الجرائم لا يستلزم أي قدر من العنف للقيام به، وإلى جانب ما تقدم فالمجرم المعلوماتي مجرم ذكي، فضلاً عن أنه متكيف اجتماعيا.

5/ المجرم المعلوماتي على قدر كبير من المعرفة التقنية: تميز المعرفة مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتي أن يكوّن تصورا كاملا لجريمته، ويرجع ذلك

إلى أن المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة وذلك قبل تنفيذ الجريمة[11].

6/ المجرم المعلوماتي لديه الباعث: الباعث وهو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة ويظل هو الباعث الأول وراء ارتكاب الجريمة المعلوماتية، ويمكن أن يكون الباعث هو الانتقام من رب العمل، وأيضا مجرد الرغبة في قهر نظام الحاسب

واختراق حاجزه الأمني، فالمجرم المعلوماتي قد يكون شخص مزدر من القانون أو لديه شعور بأنه فوق القانون[12].

7/ يتمتع المجرم المعلوماتي بقدر من المهارة: يتطلب تنفيذ الجريمة المعلوماتية قدراً من المهارة يتمتع بها الفاعل، وهذه ليست قاعدة ثابتة ذلك أن هناك الكثير من أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الجرائم[13].

8/ المجرم المعلوماتي يمتلك خيال نشط وحب انتحال الشخصيات

9/ المجرم المعلوماتي لديه حب المخاطرة والتلاعب

المطلب الثاني: تصنيف الجرائم المعلوماتية

إذا كانت الجريمة المعلوماتية تعرف بأنها:" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"، فإنه انطلاقا من هذا التعريف يمكن تصور الجريمة المعلوماتية من جانبين كونها وسيلة لارتكاب الاعتداءات.

الفرع الأول: المعلوماتية كوسيلة لارتكاب الاعتداءات

يتعلق الأمر في هذا الإطار باستخدام المعلوماتية كوسيلة لارتكاب الفعل الجرمي، ويمكن تقسيم الجرائم المعلوماتية إلى مجموعات فرعية كما هو الحال في الجرائم التقليدية والتي غالبا ما تنقسم إلى جرائم الأشخاص وجرائم الأموال.

أولا: جرائم المعلوماتية ضد الأشخاص

الجرائم ضد النفس أو الأشخاص هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع الشخصي البحت، أي الحقوق اللصيقة بالشخص المجني عليه والتي تعتبر من بين المقومات الشخصية لأهميتها الاجتماعية.

1/ جرائم الشرف والاعتبار: في هذا الإطار غالبا ما يقوم المجرم بنشر معلومات في الإنترنت، قد تكون سرية أو مضللة عن ضحيته والذي قد يكون فردا أو مؤسسة، وتتعدد الوسائل المستخدمة في هذا النوع من الاعتداءات ولعل أهمها الدخول إلى الملفات المخزونة وأخذ المعلومات الخاصة والسرية للأفراد، مما يفسح المجال لإيقاع الأضرار بهم عند طريق نشر هذه المعلومات أو استخدامها في غير الغاية المحددة لها[14].

2/ الجرائم الجنسية : إن الاستخدام اللاقانوني واللاأخلاقي لشبكة الإنترنت غالبا ما يؤثر على آلاف المستخدمين خاصة من فئة الأحداث حيث يقع البعض منهم عرضة لاستغلال الجنسي بعد إيهامهم بالرغبة في تكوين علاقات صداقة، هذه العلاقات التي يسعى المجرمون إلى تطويرها لغايات إجرامية في نفوسهم، من هذه الجرائم: تحريض القاصرين على أنشطة جنسية، التحرش الجنسي، ترويج الدعارة[15].

ثانيا: جرائم المعلوماتية ضد الأموال

تشمل جرائم السطو على أرقام البطاقات الائتمانية، لعب القمار، التزوير، الجريمة المنظمة والمخدرات وغسيل الأموال، ولعل جرائم هذا القسم أوضح كونها مجرمة، حيث لا تختلف في نتيجتها عن الجرائم التقليدية إلا أنه توجد اختلافات في تصنيف هذه الجرائم:

1/ جرائم السطو على أرقام البطاقات الائتمانية : بدأ مفهوم التجارة الإلكترونية ينشر منذ السبعينات، وذلك لسهولة الاتصال بين الطرفين ولإمكانية اختزال العمليات الورقية والبشرية، فضلا عن السرعة في إرسال البيانات وتخفيض تكلفة التشغيل والأهم هو إيجاد أسواق أكثر أتساعا .

2/ القمار عبر الانترنت : ويمكن تقسيم الطرق التي تتم ممارسة القمار على الإنترنت من خلالها إلى ثلاث فئات: اليانصيب، المراهنات، وألعاب الكازينو، حيث يمكن لأي مستخدم أن يبدأ لعب القمار بعد قيامه بالخطوات التالية : تحميل البرنامج المجاني من موقع القمار.[16].

3/ تزوير البيانات: تعد من أكثر الجرائم إنتشارا، فلا تكاد تخلوا جريمة من جرائم نظم المعلومات من شكل من أشكال تزوير البيانات، وتتم عملية التزوير بالدخول إلى قاعدة البيانات وتعديل البيانات الموجودة بها أو إضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك[17].

4/ الجرائم المنظمة : يتبادر إلى الذهن عند التحدث عن الجريمة المنظمة عصابات المافيا لأنها من أشهر المؤسسات الإجرامية المنظمة والتي تبادر بالأخذ بوسائل التقنية الحديثة سواء في تنظيم أو تنفيذ أعمالها ومن ذلك إنشاء مواقع خاصة

بها على شبكة الإنترنت لمساعدتها في إدارة العمليات، وتلقي المراسلات واصطياد الضحايا، وتوسيع أعمالها وغسيل الأموال.

5/ تجارة المخدرات عبر الانترنت : في عصر الإنترنت أضيف إلى أولياء الأمور مخاوف جديدة لا تقتصر على رفقاء السوء فقط بل يضاف إليها مواقع السوء التي لا تتعلق بترويج المخدرات وتشويق النشء لاستخدامها فقط بل تتعداه إلى تعليمهم كيفية زراعة وصناعة المخدرات بكافة أصنافها وأنواعها وبأبسط الوسائل المتاحة .

6/ غسيل الأموال يعرف غسل الأموال بأنه أي عملية من شأنها إخفاء المصدر غير المشروع الذي اكتسب منه الأموال" وتلعب التجارة الإلكترونية دورا مهما في عقد الصفقات عبر الإنترنت كصفقات السيارات والعقارات أو المعادن الثمينة، كما يمكن للأنظمة الحاسوبية التي تعمل في البنوك في مساعدة المجرمين على إيداع أموالهم ذات المصدر المشبوه، ومن ثم إعادة سحبها في الخارج بعملات صعبة كالدولار.

7/ الإرهاب السيبراني : "cyber terrorism " لا يوجد اتفاق عالمي على ماهية الأفعال الجرمية التي يمكن أن يطلق عليها إرهابا إلا أنه يشترط أن يكون للفعل الإجرامي أهدافا وأغراضا سياسية حتى يمكن اعتباره إرهابا، ومجال الإرهاب بواسطة الحاسوب والإنترنت واسع وكبير خاصة مع تنامي انتشار الحواسيب حول العالم وزيادة الحرص على ربطها بالإنترنت.[18]

الفرع الثاني: المعلوماتية محل لارتكاب الاعتداءات

بالنظر إلى الطبيعة الخاصة للأنظمة المعلوماتية الموصولة بشبكة الإنترنت فإن الأفعال الجرمية المرتكبة تعد مستحدثة لارتباطها في أغلب الأحيان إما بأمن الأنظمة المعلوماتية وسلامتها أو بسرية البيانات والمعلومات التي تحتويها تلك الأنظمة.

أولا: التدمير المتعمد للأنظمة المعلوماتية

نعني بالأنظمة المعلوماتية في شبكة الإنترنت المعدات، الآلات والمعلوماتية، الكمبيوتر والبرامج وقواعد وبنوك المعلومات ومواقع الويب ومنتديات المناقشة، والمجموعات الإخبارية وكل وسيلة معلوماتية أخرى مخصصة لصناعة أو لمعالجة أو لتخزين أو لاسترجاع أو لعرض أو لنقل أو لتبادل المعلومات[19].

ثانيا: انتهاك سرية البيانات

رغم أن وسائل المعلوماتية وبخاصة الإنترنت قد تسهل على الفرد تجميع البيانات وتخزينها ومعالجتها في أوقات قياسية إلا أنها قد تمثل تهديدا مباشرا وجديا للحياة الخاصة والحريات الفردية، لاسيما إذا أدركنا أن كل اتصال بالإنترنت يمكن أن يترك أثرا ما، حتى وإن لم يدرك مستخدم الشبكة ذلك .

ثالثا: قرصنة البرامج

أصل مصطلح قرصنة يرجع إلى عمليات السلب والنهب وكل ما يؤخذ بطريق السرقة والنصب في البحر، إلا أنه استخدم لاحقا للدلالة على قيام البعض بالسطو على مؤلفات الآخرين واستخدامها بغير وجه حق[20].

المبحث الثاني: النظام القانوني للجريمة المعلوماتية

لقد حاول المشرع الجزائري أن يساير الركب المعلوماتي على غرار التشريعات الأخرى ودلك سواء من خلال إخضاع أفعال الاعتداء على المعلوماتية لنصوص الملكية الفكرية باعتبار المعلوماتية نتاج فكر وإبداع، وكذا حماية المال المعلوماتي من خلال نصوص القانون العقوبات، كما حاول تدارك الفراغ التشريعي في مجال مكافحة الجريمة المعلوماتية من خلال قانون القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لعام 2009.

المطلب الأول: الحماية الجنائية للمعلوماتية من خلال نصوص الملكية الفكرية

تبنى المشرع الجزائري نظام الحماية وفقا لحقوق المؤلف والحقوق المجاورة وهو ما سارت عليه غالبية التشريعات والاتفاقيات الدولية، وتتمثل الحماية بالنصوص المعدلة لحقوق المؤلف في الاعتراف صراحة بوصف المصنف المحمي لمصنفات الإعلام الآلي وتجريم عملية تقليده.

الفرع الأول: تجريم عملية التقليد

نص المشرع الجزائري في الأمر 05/03 على جريمة التقليد والجرائم المشابهة لها، حيث تنص المادة 151 منه عن وجود جنحة التقليد في الحالات التالية :

- الكشف غير المشروع عن مصنف أو أداء فني.

- المساس بسلامة مصنف أو أداء فني.
- استنساخ مصنف أو أداء فني بأي أسلوب من الأساليب في شكل نسخ مقلدة أو مزورة.
- استيراد نسخ مقلدة أو تصديرها.
- بيع نسخ مزورة من مصنف أو أداء فني.
- تأجير مصنف أو أداء فني أو عرضه للتداول.

الفرع الثاني: الجزاءات المقررة لجرائم التقليد

لقد ربط المشرع الجزائري الحماية بتاريخ الانتهاء من الابتكار أو تاريخ النشر أو التوزيع لأول مرة، حيث أصبحت الدعوى الجزائية أو المدنية مقبولة حتى ولو لم يتم الإيداع.

تجدر الإشارة إلى أنه بالإضافة إلى الطرق التقليدية لتحريك الدعوى العمومية، فإن المادة 160 الأمر 05/03 تنص على حق مالك الحقوق المحمية ومن يمثله بتقديم شكوى للجهة القضائية المختصة محليا في حالة ما إذا كان ضحية الأفعال المنصوص والمعاقب عليها في الأمر 05/03.

نشير إلى أن المشرع قد خول لصاحب المصنف المعتدى عليه إجراء تحفظيا يتمثل في عملية حجز التقليد وهو إجراء يسهل إثبات عملية التقليد.

هذا الإجراء تحفظي يمكن بواسطته حجز الوثائق والنسخ الناتجة عن الاستنساخ غير المشروع أو التقليد وذلك حتى في غياب ترخيص قضائي مسبق.

للقاضي سلطة اتخاذ إحدى التدابير الآتية المادة 147 الأمر 05/03:

- إيقاف كل عملية صنع جارية ترمي إلى الاستنساخ غير المشروع للمصنف أو للأداء المحمي أو تسويق دعائم مصنوعة بما يخالف حقوق المؤلفين والحقوق المجاورة.
- القيام ولو خارج الأوقات القانونية بحجز الدعائم المقلدة والإيرادات المتولدة من الاستغلال غير المشروع للمصنفات والأداءات.
- حجز كل عتاد استخدم أساسا لصنع الدعائم المقلدة.

لقد نصت المادة 165 الأمر 10/97 المعدل والمتمم بالأمر 05/03 المتعلق بحقوق المؤلف على العقوبات على النحو التالي :

للقاضي أن يطبق كعقوبة أصلية: الحبس من 06 أشهر إلى 03 سنوات والغرامة من 500.000 دج إلى 1.000.000 دج وذلك سواء تمت عملية النشر داخل الجزائر أو خارجها.

للقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية لمبلغ الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو آداء محمي، ومصادرة وإتلاف كل عتاد أنشئ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة، والمصادرة هنا وجوبية.

كما تأمر الجهة القضائية بتسليم العتاد أو النسخ المقلدة أو قيمة ذلك وكذلك الإيرادات موضوع المصادرة للمؤلف أو أي مالك حقوق آخر لتكون عند الحاجة بمثابة تعويض.

يمكن للقاضي بناءا على طلب الطرف المدني الأمر بنشر أحكام الإدانة على نفقة المحكوم عليه على ألا تتعدى المصاريف قيمة الغرامة المحكوم بها.

للقاضي أن يضاعف العقوبات المقررة وذلك في حالة العود مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة أشهر.

المطلب الثاني: الحماية الجزائية للمعلوماتية من خلال نصوص قانون العقوبات

تدارك المشرع الفراغ القانوني في مجال الجريمة المعلوماتية، وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون رقم 15/04 المتضمن تعديل قانون العقوبات مركزا على الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات .

الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات

قدمت الاتفاقية الدولية للإجرام المعلوماتي (السيبيري) تعريفا للنظام المعلوماتي في مادتها الثانية على النحو التالي : « يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة

ببعضها البعض أو التي ذات صلة بذلك، ويقوم أحدها أو أكثر من واحد منها، تبعا للبرنامج بعمل معالجة آلية للبيانات"[21].

أولا: مكونات نظام المعالجة الآلية للمعطيات

يتكون نظام المعالجة الآلية للمعطيات من العناصر المادية والمعنوية التي يتكون منها المركب ومثال ذلك: الذاكرة، البرامج، المعطيات، أجهزة الربط...الخ وعليه فإن هذه العناصر واردة على سبيل المثال لا الحصر مما يفتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يستوحيه التطور التقني في هذا المجال[22].

ثانيا: ضرورة خضوع النظام لحماية فنية

يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات، وبالأخص حاليا شبكة الإنترنت، لتأمين سرية الرسائل الالكترونية وسرية البيانات المتناقلة. وخاصة منها المتعلقة بالأعمال التجارية الرقمية. ويمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة، و عليه فان الخبراء يؤكدون على ضرورة استخدام أسلوب التشفير لمنع الآخرين من الإطلاع على الرسائل الالكترونية.

الفرع الثاني: الأركان الأساسية لهده الجريمة

أولا: الركن المادي

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

- الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات
- الاعتداءات العمدية على المعطيات: نص عليها المشرع الجزائري في المادة 394 مكرر 2 من قانون العقوبات وهي:

1. تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
2. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

ثانيا: الركن المعنوي

يشترط لتوفر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء وأن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به، أي مشروع، أو إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق كأن يجهل بوجود حظر للدخول أو البقاء أو كان يعتقد خطآ أنه مسموح له بالدخول، فإذا توافر القصد الجنائي بعنصرية العلم والإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيضل القصد قائما حتى ولو كان الباعث هو الفضول أو إثبات القدرة على المهارة والانتصار على النظام.

الفرع الثالث: عقوبات جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات

نصّ المشرّع على مجموعة من العقوبات لهاته الجرائم الماسّة بالنظام والمتمثّلة في:

أولا: العقوبات الأصلية

1/ عقوبة الدخول أو البقاء داخل النظام

أ. **الصورة البسيطة للجريمة:** حدّد المشرّع عقوبة هذه الجريمة بالحبس من ثلاثة أشهر إلى سنة والغرامة من 50000 دج إلى 100000 دج (المادة 394 مكرر).

ب. **الصورة المشدّدة للجريمة:** نصّ المشرّع في المادة (394 مكرر فقرة 2 و3) على مضاعفة العقوبة إذ ترتّب على هذا الدخول أو البقاء حذف أو تغيير معطيات النظام، أمّا إذا أنجرّ على هذا الدخول أو البقاء تخريب لنظام عمل المنظومة، فإنّ العقوبة تكون الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج.

2/ عقوبة الاعتداء العمدي على المعطيات

حدّد المشرّع عقوبة الاعتداء العمدي على المعطيات الموجودة داخل النظام في المادة 394 مكرر 1 بالحبس من ستة أشهر

إلى ثلاث سنوات وبغرامة من 500000 دج إلى 2000000 دج، كما عاقب على استخدام هذه المعطيات في ارتكاب الجرائم الماسّة بالأنظمة المعلوماتية، وكذا حيازة أو إنشاء أو نشر أو استعمال المعطيات المتحصّل عليها من إحدى الجرائم الماسّة بالأنظمة المعلوماتية بنصّ المادّة (394 مكرر 2) بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000 دج إلى 5000000 دج.

ثانيا: العقوبات المُقرّرة للشخص المعنوي

أقرّ المشرّع مبدأ مُساءلة الشخص المعنوي في القانون 04-15 المؤرخ في 2004/11/10 وذلك بموجب نصّ المادّة 51 مكرر منه، كما حدّد ثلاثة شروط لإمكان مساءلة الشخص المعنوي جنائيا وهي كالتالي:

1. أن تُرتكب إحدى الجرائم المنصوص عليها قانونا.
2. أن تكون بواسطة أحد أعضاء أو مُمثّلي الشخص المعنوي.
3. أن تُرتكب الجريمة لحساب الشخص المعنوي.

كما حدّد في المادّة 18 مكرر من نفس القانون، العقوبات المطبّقة على الأشخاص المعنوية، حيث جاء فيها ما يلي: "العقوبات التي تُطبّق على الشخص المعنوي في مواد الجناية والجنح هي:

- الغرامة التي تساوي من مرّة إلى خمس مرات الحدّ الأقصى للغرامة المقرّرة للشخص الطبيعي في القانون الذي يُعاقب على الجريمة.
- واحدة أو أكثر من العقوبات الآتية:
- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدّة لا تتجاوز خمس سنوات.
- الإقصاء من الصفقات العمومية لمدّة لا تتجاوز خمس سنوات.
- المنع من مزاولة نشاط أو عدّة أنشطة مهنية أو اجتماعية بشكل مباشر، نهائيا لمدّة لا تتجاوز خمس سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر وتعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدّة لا تتجاوز خمس سنوات، وتنصبّ الحراسة على ممارسة النشاط الذي أدّى إلى الجريمة أو الذي ارتُكبت الجريمة بمناسبته.

من هذا المنطلق، فقد عاقب المشرّع في المادّة 394 مكرر 4 الشخص المعنوي في حالة ارتكابه لإحدى جرائم الاعتداء على نظام المعالجة الآلية للبيانات بغرامة تعادل خمس مرّات الحدّ الأقصى للغرامة المقرّرة للشخص الطبيعي.[23]

ثالثا: عقوبة الاشتراك والشروع في الجريمة

1/ عقوبة الاشتراك

يُعاقب المشرّع على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تمّ التحضير لها، فإذا تعدّدت الجرائم التي يتمّ التحضير لها تكون العقوبة هي عقوبة الجريمة الأشدّ[24].

وشروط المعاقبة على الاتفاق الجنائي يمكن استخلاصها من نفس المادّة 394 مكرر 5 من قانون العقوبات، وهي كالآتي:

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

2/ عقوبة الشروع

نصّت المادّة 11 من الاتفاقية الدولية للإجرام المعلوماتي على عقوبة الشروع وتبنّاها المشرّع في المادّة 394 مكرر 7 من قانون العقوبات. فالجرائم الماسّة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنصّ.

تنصّ المادّة 394 مكرر 7 من قانون العقوبات على: "يُعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقرّرة للجنحة ذاتها".

يبدو من خلال هذا النصّ رغبة المشرّع في توسيع نطاق العقوبة بحيث تشمل أكبر قدر من الأفعال الماسّة بالأنظمة المعلوماتية،

إذ جعل الشروع في إحداها مُعاقب عليه بنفس عقوبة الجريمة التامة.

رابعا: العقوبات التكميلية

1/ المصادرة:

هي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسّة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية.

2/ إغلاق المواقع:

الأمر يتعلّق بالمواقع (les sites) التي تكون محلاّ لجريمة من الجرائم الماسّة بالأنظمة المعلوماتية.

3/ إغلاق المحلّ أو مكان الاستغلال

إذا كانت الجريمة قد ارتُكبت بعلم مالكها، ومثال ذلك إغلاق مقهى الأنترنت الذي تُرتكب فيه مثل هذه الجرائم بشرط توفّر عنصر العلم لدى مالكها.

المطلب الثالث: القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

تضمنها القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق 05 غشت سنة 2009م، حيث تدارك المشرع الجزائري الفراغ التشريعي في مجال مكافحة الجريمة المعلوماتية من خلال قانون القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لعام 2009 في الوقت الذي استحدثت فيه معظم الدول العربية أنظمة خاصة بهذه الظاهرة[25].

الفرع الأول: مراقبة الاتصالات الالكترونية

نصت المادة 04 من هذا القانون على الحالات التي تسمح باللجوء إلى المراقبة الالكترونية وهي على النحو التالي:

1- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والجرائم الماسة بأمن الدولة.

2- حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام.

3- أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

4- مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

5- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

يتم هذا الإجراء بإذن مكتوب من السلطة القضائية المختصة، إلا أن النائب العام لدى مجلس قضاء الجزائر يمنح هذا الإذن لمدة 6 أشهر قابلة للتجديد لضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

الفرع الثاني: تفتيش المنظومة المعلوماتية

حسب هذا القانون يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في الحالات الضرورية اللجوء إلى المراقبة الالكترونية والدخول إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها ولو عن بعد لغرض التفتيش.

كما أن القانون أشار إلى أنه في حالة ما إذا كانت المعطيات المبحوث عنها يمكن الدخول إليها انطلاقا من منظومة معلوماتية تقع خارج الإقليم الوطني يكون الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل، كما أنه أجاز تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها وهذا للسلطات المكلفة بالتفتيش.

الفرع الثالث: حجز المعطيات المعلوماتية

حسب هذا القانون يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على داعمة تخزين الكترونية تكون قابلة للحجز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، ويجوز استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض

التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات، كما أنه نص على إمكانية الحجز عن طريق منع الوصول إلى المعطيات وذلك بأمر من السلطة التي تباشر التفتيش عن طريق تكليف أي شخص مؤهل مع استعمال وسائل تقنية مناسبة لذلك.

الفرع الرابع: حفظ المعطيات المتعلقة بحركة السير

يلزم القانون 04/09 مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها.

بوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المذكورة مع كتمان سرية هذه العمليات إذ يقوم مقدمو الخدمات بحفظ ما يلي:

1- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
2- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
3- الخصائص التقنية وكذا تاريخ ومدة كل اتصال.
4- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة أو مقدميها.
5- المعطيات التي تسمح بالتعرف على المرسل إليه الاتصال وكذا عنوان المواقع المطلع عليها.

تحدد مدة هذه المعطيات بسنة واحدة ابتداء من تاريخ التسجيل مع الإشارة إلى قيام المسؤولية الجزائية على الأشخاص الطبيعيين والمعنويين، إذ يعاقب الشخص الطبيعي بالحبس من ستة أشهر إلى خمس سنوات وبغرامة من 50 ألف إلى 500 ألف دينار جزائري أما الشخص المعنوي فيعاقب بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

كما يتعين على مقدمي خدمات الانترنيت التدخل الفوري وسحب المحتويات التي يسمح الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفة هذه القوانين وتخزينها أو جعل الدخول إليها غير ممكن، وقد ألزمهم هذا القانون بوضع ترتيبات تقنية تسمح بحصر إمكانيات الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

أكد ذات النظام على إجراءات التفتيش والمعاينة والحجز طبقا لنص المادة 47 من قانون الإجراءات الجزائية، إذ يمكن لعناصر الضبطية القضائية أثناء عملية البحث والتحري عن هذه الجرائم العمل بهذه الإجراءات بناء على إذن مسبق من وكيل الجمهورية في كل ساعة من ساعة الليل أو النهار، ويمكن ذلك لقاضي التحقيق في أي مكان على مستوى الإقليم الوطني طبقا لأحكام المادة 65 مكرر وما يليها من قانون الإجراءات الجزائية، كما تضمن الإجراءات المتبعة لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور وكذا إجراءات التسريب في هذا النوع من الجرائم بناء على إذن من وكيل الجمهورية أثناء مرحلة التحقيق الابتدائي وبناء على إذن من قاضي التحقيق في مرحلة التحقيق القضائي.

إضافة لذلك، كرس القانون مبدأ التعاون والمساعدة القضائية الدولية من خلال المادة 15 في حالة ما إذا كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني وأسند مهام الرقابة على هذه الجرائم لهيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته بمقتضى المادة 13 منه.

الخاتمة:

من المعلوم أن الإجرام المعلوماتي في بلادنا لم يتخذ نفس الأبعاد المحققة في الدول المتقدمة، لكن هذا لا ينفي ضرورة التصدي لبوادره التي بدأت تتجلى للعيان، وهذا حتى لا تستفحل هذه الوضعية مع وتيرة النمو المتسارع في استخدام النظم المعلوماتية، فضلا عن العولمة والتطور التكنولوجي الهائل، ما يوفر مناخا ملائما لانتهاك حرمة البيانات الشخصية والمساس بالأمن الوطني.

وبالفعل فإن المشرع سارع لتدارك هذا الأمر مؤخرا، فاستحدث أحكاما قانونية لحماية البرامج وهذا ضمن الأمر رقم 97-10 المؤرخ في 1997/03/06 المتعلق بحق المؤلف والحقوق المجاورة[26]، وتم تعديله بموجب الأمر 03-05 الصادر بتاريخ

2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر 73-14[27]، وكذا التعديل الأخير لقانون العقوبات 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 66-156 المؤرخ في 1966/06/08 المتضمن قانون العقوبات[28]، الذي عالج فيه المساس بأنظمة المعالجة الآلية للبيانات.

بالرغم من أن المشرع قد ساير الركب المعلوماتي في هذا المجال بأن تبنى نصوصا تشريعية حديثة جسد من خلالها أغلب الأحكام الواردة في الاتفاقية الدولية للإجرام المعلوماتي، إلا أنها تبقى دائما كمادة خام غير قابلة للتطبيق، ذلك أنها تحتاج إلى نصوص إجرائية تلازمها نظرا لما تمتاز به الجريمة المعلوماتية من خصوصية تختلف عن باقي الجرائم، وهو ما دفع بالمشرع الجزائري إلى إصدار سلسلة من التشريعات لمواجهة الجريمة المعلوماتية على اختلافها منها المباشرة ومنها غير المباشرة، نذكر منها القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لعام 2009 في الوقت الذي استحدثت فيه معظم الدول العربية أنظمة خاصة بهذه الظاهرة.

حيث وجهت لهذا القانون العديد من الانتقادات من أهل الاختصاص كان أهمها أن مصطلحاته التقنية غير واضحة ماعدا البعض منها أين أعطى المشرع بعض المفاهيم من خلال المادة الثانية منه، إلا أن توضيح هذه المفاهيم يستدعي وضع نص قانوني يحدد بدقة جميع المصطلحات المستعملة في مجال الجريمة الالكترونية وكذا إبراز الحقوق والواجبات المرتبطة بالمتعاملين بأجهزة الإعلام الآلي أو شبكة الانترنت أو شبكات الانترانت وحتى باقي الأجهزة الالكترونية على غرار الهواتف الذكية، مع وضع قانون مستقل لتحديد المفاهيم من شأنه أن يجنب جميع محاولات التملص من المسؤولية الجزائية والمدنية ومن شأنه مساعدة رجال القضاء ورجال القانون وحتى الباحثين في هذا الميدان في عملهم من خلال تحديد المسؤوليات وتبيان الحقوق والواجبات الخاصة بمستعملي أجهزة الإعلام الآلي أو شبكات الانترنت، الأمر الذي يجعل من غياب مثل هذه القواعد القانونية في نظام مستقل يشكل أحد أبرز إشكالات الجريمة الالكترونية في التشريع الجزائري.

الهوامش

1 أبو الوفا محمد أبو الوفا، المواجهة الإجرائية للجرائم المعلوماتية، ندوة حول جرائم تقنية المعلومات في ظل القانون الاتحادي رقم (2)، الإمارات العربية المتحدة، 2006، ص 64.

2 نائلة عادل محمد فريد قورة -جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية- منشورات الحاتي الحقوقية 2005 ص32.

3 هشام فريد رستم، جريمة الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، بحث مقدم لمؤتمر الأمم المتحدة التاسع لمنع الجريمة و معاملة المجرمين –مجلة الأمن العام العدد 151-1995- ص38

4 هشام رستم، المرجع السابق، ص29 و30

5 جميل عبد الباقي الصغير الإنترنت والقانون الجنائي دار الفكر العربي القاهرة لسنة 2001 ص 92

6 محمد بن عبد الله بن على المنشاوي، جرائم الكمبيوتر في المجتمع السعودي، رسالة ماجستير في العلوم الشرطية أكاديمية نايف للعلوم الأمنية, الرياض ,2003، ص 125.

7 عبد الواحد العلمي، القانون الجنائي المغربي القسم الخاص، الطبعة الثانية 2000/ص 337.

8 تي عفاف, محاضرة حول الجريمة الإلكترونية, معدة من طرف ضابط الشرطة لدى أمن ولاية غرداية , 17-07-2003، ص 11.

9 أحمد فتحي سرور، الوسيط في قانون العقوبات، ط 4، القاهرة، 1991, ص 15.

10 سب دراسة قام بها المكتب الفدرالي الأمريكي (federal bureau of investigation FBI) غالبية الهاكرز الأكثر خطورة هم الشباب المتراوحة أعمارهم بين 18- 35 سنة.

11 Bouchaib RMAIL, la criminalité informatique, criminalité a double dimension :internationale, thèse pour l'obtention du grade de ducteur en droit privé-option : droit des affaires, faculté des sciences juridiques, économiques et sociales- fés, 2005, p : 82.

12 هشام فريد، مرجع سابق، ص38.

13 علي عبد القادر القهوجي الحماية الجنائية لبرامج الحاسب الآلي-الدار الجامعية للطباعة و النشر بيروت 1999، ص 136-137.

14 محمد بن عبد الله بن على المنشاوي، مرجع سابق، ص 96.

15 محمد بن عبد الله بن على المنشاوي، مرجع سابق، ص97

16 علاء الدين محمد شحاتة, رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي, بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي –القاهرة من 25- 26 أكتوبر 2014، ص 03

17 أنيس المومني، قانون العقوبات في مواجهة مخاطر الإنترنت، مذكرة ماجيستير، جامعة باجي مختار، عنابة، الجزائر ص 123.

18 سعيداني نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجيستير، جامعة باتنة، 2013، ص 188.

19 حنان ريحان مبارك ماجد المضحكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014، ص 356.

20 منير محمد الجنبيهي وممدوح محمد الجنبيهي، جرائم الانترنت والحساب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص 206.

21 Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparents, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé des données.

22 Gassin : droit pénal de l'informatique les systèmes traitement des données commentaire de la loi n° 88/18 du **03/01/88** relative à la fraude informatique DALLOZ 1988 – p 05.

23 خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر في التشريع الجزائري، دار الهدى، الجزائر، 2010.، ص 129.

24 آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، 2006، ص 131.

25 Dahmane M et bouder H: l'équipe de recherche en droit des TIC genése ،par cours et ambitions ، séminaire national sur le cadre juridique des TIC en Algérie entre opportunités et contraintes ،cerist ، Alger ،Algérie ،2012 .

26 الأمر رقم 97-10 المؤرخ في 1997/03/06 المتعلق بحق المؤلف والحقوق المجاورة (ج.ر 13 في 1997/03/12).

28 الأمر رقم 05/03 المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة (ج.ر 44 في 2003/07/23).

29 القانون 15/04 المؤرخ في 2004/11/10 المعدل والمتمم للأمر رقم 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات (ج.ر 71 في 2004/11/10).