الحماية الجنائية للمعطيات الإلكترونية في إطار القانون الجزائري
(دراسة تحليلية لقانوني العقوبات وحقوق المؤلف)

الدكتورة أمحمدي بوزينة أمنة
أستاذة محاضرة قسم (ب) كلية الحقوق والعلوم السياسية
جامعة حسيبة بن بوعلي– الشلف.

ملخص باللغة العربية:

لا شك أن الحاسوب أصبح ضرورة لا يمكن الإستغناء عنها في حياة الأفراد والمؤسسات الخاصة والعامة على حد سواء فقد ساعد على القيام بالأعمال الإدارية والفنية والخدمية التي لا حصر لها، ولكنه في المقابل ساهم بشكل غير مباشر في فتح المجال نحو وجود سلوكيات جديدة وأساليب مختلفة لإرتكاب أفعال غير سوية وجرائم مختلفة، من هذا المنطلق استدرك المشرع الجزائري الفراغ القانوني في مجال الحماية الجنائية للنظم المعلوماتية من خلال استحداث القسم السابع مكرر ضمن قانون العقوبات عنوانه المساس بأنظمة المعالجة الآلية للمعطيات، وكذلك تقررت عقوبات للاعتداء على أنظمة المعلومات في قانون حماية حقوق المؤلف الجزائري.

Résumé :

Les décisions du conseil de la concurrence ne sont pas considérées comme des décisions finales possèdent la force de la chose jugée. Elles sont susceptibles d'être un objet de recours devant les tribunaux ordinaires, en règle générale, mais par exception la juridiction administrative est compétente en cas de manquement à informer les obligations de publicité ou de la concurrence régissantes la conclusion du processus de passation des marchés publics. Aussi les décisions de rejet de groupement, émis par le Conseil de la concurrence, sont soumises au contrôle du Conseil d'Etat. Vu que le conseil de la concurrence est une autorité administrative indépendante est censée de contester ses décisions devant le tribunal administratif, comme un principe général et non une exception, alors quelle est la raison pour le législateur de sortir de cette règle générale dans les litiges de la concurrence?

مقدمة

لا شك أن الحاسوب أصبح ضرورة لا يمكن الإستغناء عنها في حياة الأفراد والمؤسسات الخاصة والعامة على حد سواء، فقد ساعد على القيام بالأعمال الإدارية والفنية والخدمية التي لا حصر لها، ولكنه في المقابل ساهم بشكل غير مباشر في

فتح المجال نحو وجود سلوكيات جديدة وأساليب مختلفة لإرتكاب أفعال غير سوية وجرائم مختلفة، ولاشك أن المجرمين يحاولون الإستفادة من هذا التقدم التقني خاصة وأننا في عصر ثورة المعلومات وتقدم العلوم الحديثة والتكنولوجيا المتطورة، وتبعاً لذلك، فإنه من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق، وهذا ليس قاصراً على أسباب التقدم التقني فقط، بل يحدث دوما وبصفة مستمرة، فالمجرم والجريمة في تقدم وتجدد مستمر، فمجرم الأمس ليس كمجرم اليوم، حيث أن هذه التقنيات شجعت وساعدت المجرمين على زيادة عدد وحجم جرائمهم، بل مع انخفاض احتمالات انكشاف أمرهم، مما أدى إلى تزايد حجم الخسائر المادية لجرائم الحاسوب، فبات من الضروري تحديد حجم وأنماط هذه الجرائم، وهو ما سيبرز من خلال الوقوف على جريمة المساس بأنظمة المعالجة الآلية للمعطيات على أن نتعرف قبل ذلك على نظام المعالجة الآلية للمعطيات.

وإن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، استدعى تدخلاً تشريعياً صريحاً سواء على المستوى الدولي أو الداخلي، فدولياً وضعت أول اتفاقية حول الإجرام المعلوماتي بتاريخ: 2001/11/08 تضمنت مختلف أشكال الإجرام المعلوماتي، أما على المستوى الوطني، فقد استدرك المشرع الجزائري الفراغ القانوني من خلال تعديل قانون العقوبات بموجب القانون 15/04 باستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات"، ويشمل المواد من (394 مكرر) إلى (394 مكرر7)، وكذلك تقررت عقوبات للاعتداء على أنظمة المعلومات في قانون حماية حقوق المؤلف رقم 05/03.

هذه الاعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات كشرط مسبق بخلاف الاعتداءات على منتجات النظام، وتكشف عن أهم التحديات القانونية التي

تفرضها جرائم المساس بأنظمة الكومبيوتر على النظام المعلوماتي الجزائري بشكل خاص والعالمي بشكل عام، ولتحقيق هذا الهدف يحاول هذا البحث بشكل مجمل تقديم صورة عامة لأبرز التحديات المصاحبة لشبكة الإنترنت، من هذا المنطلق نتساءل: ما هي أبرز الأنماط الإجرامية في مجال المساس بأنظمة الكومبيوتر والإنترنت؟، وما هي الجهود المتخذة من قبل المشرع الجزائري في مجال مكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات؟

وللإجابة على هذه التساؤلات وحل الإشكال المطروح، نقدم تحليلا يقوم على المحورين التاليين:

المبحث الأول: الحماية الجنائية للمعطيات الإلكترونية في إطار قانون العقوبات.

المبحث الثاني: الحماية الجنائية للمعطيات الإلكترونية بموجب قانون حقوق المؤلف.

وتفصيل ذلك على النحو التالي:

المبحث الأول: الحماية الجنائية للمعطيات الإلكترونية في إطار قانون العقوبات.

الجرائم الماسة بالأنظمة المعلوماتية وإن كانت تختلف في أركانها وعقوباتها، إلا أن ما يجمعها أنها تحقق حماية جزائية تنظم المعالجة الآلية للمعطيات أي أن القاسم المشترك بينهما هو نظام المعالجة الآلية، وهو ما سنبرزه نشئ من التفصيل على النحو التالي:

المطلب الأول: صور الجرائم الواردة في إطار قانون العقوبات الجزائري.

نص المشرع الجزائري من خلال نصوص قانون العقوبات على مجموعة من الأفعال من خلال المواد (394 مكرر) إلى (394 مكرر7)، التي يمكن تلخيصها فيما يلي:

- الدخول أو البقاء داخل منظومة معلوماتية عن طريق الغش أو في جزء منها (المادة 394 مكرر/1).

- إتلاف أو حذف أو تغيير لمعطيات المنظومة أو تخريب أشغال المنظومة (المادة 394 مكرر/2).
- إدخال بطريق الغش معطيات في نظم المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها (المادة 394 مكرر1).
- 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 (المادة 394 مكرر1/2).
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر2/2).

وعليه انطلاقاً من هذا التقسيم، سوف نعرض لهذه الجرائم بشيء من التفصيل على النحو التالي:

الفرع الأول: جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

نص المشرع الجزائري على جريمة الدخول أو البقاء داخل منظومة معلوماتية عن طريق الغش أو في جزء منها في المادة (394 مكرر/1)، ويمكن القول وانطلاقاً من نص المادة، أنه ولقيام هذه الجريمة لابد من اشتمالها على ركنين هما المادي والمعنوي، إذْ لا يتحقق المفهوم القانوني للجريمة إلا بوجود نص تشريعي وارتكاب فعل أو إمتناع، إذْ لا جريمة ولا عقوبة إلا بنص، كما تستلزم بالإضافة إلى ذلك عدم مساءلة الشخص عن الفعل أو الترك إلا إذا قام به بإرادته واختياره، وهو ما سيتضح من خلال النقطتين التاليتين المواليين كالتالي:

الواضح من خلال صياغة هذا النص، أنه تضمن صورتين لهذه الجريمة، فهناك:

- الصورة البسيطة لفعل الدخول أو البقاء غير المشروع.
- الصورة المشددة لجريمة الدخول إلى النظام أو البقاء غير المشروع.

أولا: الصورة البسيطة لفعل الدخول أو البقاء غير المشروع.

1. الركن المادي في الصورة البسيطة لفعل الدخول أو البقاء غير المشروع:

أ- فعل الدخول[1]:

بما أن المشرع لم يحدد وسيلة الدخول إلى النظام، فإنه يمكن الدخول بأية وسيلة كانت، وذلك عن طريق كلمة السر الحقيقية متى كان الجاني غير مخول باستخدامها أو باستخدام برنامج أو شفرة خاصة أو عن طريق استخدام الرقم الكودي لشخص آخر أو الدخول من خلال شخص مسموح له بالدخول[2].

وتقع هذه الجريمة من أي إنسان أيا كانت صفته سواء كان يعمل في مجال الأنظمة أم لا علاقة له بنظم الكمبيوتر وسواء كان يستطيع الاستفادة من النظام أم لا، إنما يشترط ألا يكون من أولئك الذين لهم حق الدخول إلى النظام، ويتحقق الدخول غير المشروع كذلك متى كان مخالفاً لإرادة صاحب النظام أو من له حق السيطرة عليه، كتلك الأنظمة المتعلقة بأسرار الدولة أو دفاعها أو تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة بحيث لا يجوز الإطلاع عليها[3].

---

[1] علي عبد القادر القهوجي، **الحماية الجنائية لبرامج الكمبيوتر**، المكتبة القانونية، القاهرة، 1999، ص: 121.

[2] عبد الفتاح بيومي حجازي، **النظام القانوني لحماية التجارة الإلكترونية**، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، 2002، ص ص: 28-29.

[3] علي عبد القادر القهوجي، **الحماية الجنائية لبرامج الكمبيوتر**، المرجع السابق، ص: 123.

ويتحقق فعل الدخول غير المشروع إلى النظام، متى دخل الجاني إلى النظام كله أو جزء منه كالدخول إلى شبكة الاتصال أو البرنامج، وكذلك يتحقق الدخول غير المشروع متى كان مسموحا بالدخول لجزء معين في البرنامج وآخر غير مسموح له بالدخول فيه، فلو فرضنا أن الجاني دخل إلى موقع – أمازون دوت كوم – وهو موقع للبيع الإلكتروني معد للجمهور، لكنه تجاوز الموقع إلى البيانات الخاصة بإعداد الموقع وتنظيمه في صفحة (Home Page) وتنطوي على معلومات لا يجوز للجمهور الدخول إليها، وبالتالي يكون فعل الجاني مكونا لجريمة الدخول غير المشروع، رغم أن الموقع في ذاته مفتوحا للجمهور[1]، لذلك يخرج من نطاق الدخول غير المشروع، الدخول إلى برنامج منعزل عن نظام المعلومات الذي حظر عليه الدخول فيه، كما لا تتوفر الجريمة إن اقتصر دور الجاني على مجرد قراءة الشاشة دون الولوج إلى داخل النظام، إذْ بهذه الأفعال لا تقوم جريمة الدخول غير المشروع للنظام معلوماتي[2].

ب– فعل البقاء:

ويتحقق الركن المادي في جريمة البقاء في النظام كذلك إذا اتخذ صورة البقاء داخل النظام، ويقصد بفعل البقاء: "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام"[3]، ومما لا شك فيه أن البقاء داخل نظام الكمبيوتر بعد دخوله عن طريق الخطأ لا يختلف عن الدخول غير

---

[1] ختير مسعود، **الحماية الجنائية لبرامج الكمبيوتر**، دار الهدى، عين مليلة، الجزائر، 2010، ص: 115–116.

[2] عبد الفتاح بومي حجازي، **النظام القانوني لحماية التجارة الإلكترونية**، المرجع السابق، ص: 30.

[3] علي عبد القادر القهوجي، **الحماية الجنائية لبرامج الكمبيوتر**، المرجع السابق، ص: 133.

المصرح به من حيث وجوب التجريم، فاتجاه إرادة الفاعل إلى البقاء داخل هذا النظام على الرغم من معرفته أنه غير مصرح له بالدخول، لا يختلف في جوهره عن الدخول غير المصرح به إلى نظام الكمبيوتر، فالنتيجة الإجرامية في الحالتين واحدة وهي الوصول إلى نظام غير مصرح للدخول إليه، فالمصلحة التي يحميها القانون هي حماية نظام الكمبيوتر في الحالتين[1]، وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا، وذلك في الفرض الذي لا يكون فيه الجاني له الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الفرض الاجتماع المادي لجريمتي الدخول والبقاء غير المشروع في النظام.

والإشكالية التي تثور في هذا الصدد: متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء؟

ذهب رأي من الفقه إلى أن جريمة الدخول تتحقق منذ اللحظة التي يتم الدخول فيها فعلا إلى البرنامج، ويبقى مدة من الزمن داخله، وبعد تلك اللحظة تبدأ جريمة البقاء وتنتهي بانتهاء حالة البقاء، ويذهب رأي آخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه أن بقاءه داخل النظام غير مشروع[2].

بينما يذهب رأي راجح من الفقه إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجوال داخل النظام أو يستمر في التجوال داخله بعد انتهاء الوقت المحدد، أي منذ علم الجاني أنه ليس له حق الدخول، فإذا دخل وظل ساكناً تظل الجريمة جريمة دخول إلى النظام، أما إذا بدأ في التجوال حتى مع علمه

---

[1] نائلة عادل محمد فريد قروة، **جرائم الكمبيوتر الاقتصادية**، منشورات حلبي، الطبعة الأولى، بيروت، 2005، ص: 346.

[2] خثير مسعود، المرجع السابق، ص: 117.

بأن بقاءه ممنوع في النظام، فإن جريمة البقاء داخل النظام تبدأ من اللحظة لأنه من يتجول في النظام يعلم مسبقا أن مبدأ دخوله واستمراره فيه غير مشروع، ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام [1].

2. الركن المعنوي:

تعتبر جريمة الدخول أو البقاء من الجرائم العمدية، بحيث يكفي فيها القصد العام، فيكفي لتوافر هذه الجريمة أن يعلم الجاني أنه قد دخل إلى نظام ليس له حق الدخول فيه أو تعمد البقاء فيه رغم انتهاء مدة حقه في البقاء ولو كان الدخول مشروعا، أما إذا إنتفى علمه فإنها لا تتوافر الجريمة، كأن يجهل وجود حظر الدخول، أو أنه مسموح له الدخول فيه، ولا يتأثر القصد الإجرامي بالباعث على الدخول أو البقاء، فيظل القصد الإجرامي قائما حتى ولو كان الباعث من الدخول أو البقاء للفضول أو التنزه أو إثبات القدرة على الإنتصار على النظام[2].

ثانياً: الصورة المشددة لجريمة الدخول إلى النظام أو البقاء غير المشروع:

نصت المادة (394 مكرر/2 و3) من قانون العقوبات على أنه: "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 ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج".

وباستقراء نص المادة (394 مكرر/2 و3) من قانون العقوبات، نجد أنها قد نصت على ظرفين مشددين تشدد بهما عقوبة الدخول أو البقاء داخل النظام، ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع محو أو

---

[1] علي عبد القادر قهوجي، الحماية الجنائية لبرامج الكمبيوتر، المرجع السابق، ص: 135.

[2] علي عبد القادر قهوجي، نفس المرجع، ص: 137.

تعديل البيانات التي يحتويها النظام أو عدم قدرة النظام على تأدية وظيفته ويكفي لتوافر هذا الظرف المشدد أن تكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت، وهي محو النظام أو عدم قدرته على أداء وظيفته أو تعديل البيانات[1]، وبذلك فالهدف الأساسي من هذا النص هو التعرض لكل محاولة لإعاقة أو تحريف قد تلحق بهذا النظام، ولذلك فإنه لتحقق هذه الجريمة يستلزم توافر الركن المادي والركن المعنوي.

أولا: الركن المادي:

يتمثل الركن المادي، إما في فعل توقيف أو تعطيل نظام المعالجة الآلية للمعطيات عن أداء نشاطه ولا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام، بل يكفي أن يؤثر على هذه العناصر فقط سواء المادية (جهاز الكمبيوتر نفسه، شبكات الاتصال، أجهزة النقل) أم المعنوية (البرامج والمعطيات).

1- التعطيل أو التوقيف:

تعتبر عملية إعاقة سير عمل نظام المعالجة الآلية للمعطيات بأنها:" فعل يتسبب في تباطؤ أو ارتباك عمل نظام المعالجة، ومن ثم ينتج عن ذلك تغيير في حالة عمل النظام، وهذا الارتباك الناجم عن الإعاقة تتأثر به أجهزة الكمبيوتر والبرامج على السواء"[2]، ومن أمثلة التخريب أو التعطيل الواقع على أنظمة المعالجة قضية روبير موريس (Rober Morris) ، وهي أحد أول الهجمات الكبرى والخطرة في بيئة الشبكات، ففي مارس عام 1988 تمكن طالب يبلغ من العمر 23 عاما ويدعى روبير موريس من إطلاق فيروس عرف باسم "دودة مورس" عبر الانترنت

[1] ختير مسعود، المرجع السابق، ص: 119.

[2] نفس المرجع، ص: 121.

أدى إلى إصابة 6 ألاف جهاز يرتبط معها حوالي 60000 نظام عبر الانترنت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مئة مليون دولار، إضافة إلى مبلغ أكثر من ذلك تمثل في الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة[1].

ويحصل فعل التعطيل أو التوقيف بأي وسيلة كانت، فالمشرع لم يشترط وسيلة معينة، وبالتالي فيستوي أن يكون بوسيلة مادية أو معنوية، ومن أمثلة وسائل التعطيل المادية استعمال العنف لمنع الوصول إلى الأجهزة ككسرها أو تحطيمها أو تحطيم أسطوانة أو قطع شبكات الاتصال أو سكب كوب شاي أو أي مادة أخرى أو منع العاملين من الوصول إلى النظام، أما الإعاقة أو التعطيل بوسيلة معنوية، فقد تتحقق بإدخال فيروس عن البرنامج أو تعديل كلمة السر أو كيفية أداء النظام لوظيفته، بوسيلة تؤدي إلى أن يتباطئ في أدائه لوظيفته المعلوماتية داخل النظام المعلوماتي[2].

2- الإفساد أو التعييب:

يقصد بالإفساد أو التعييب كل فعل؛ وإن كان لا يعطل نظام معالجة البيانات؛ لكنه يجعل هذا النظام غير قادر على الاستعمال السليم، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها، ويذهب جانب من الفقه إلى أن الإفساد من هذه الزاوية يقترب من التعييب الذي صادفناه عند دراسة الظرف المشدد لجريمة الدخول أو البقاء غير المشروع، ولعل الفارق بينهما يكمن فقط في أن الإفساد في

---

[1] يونس عرب، **جرائم الكمبيوتر والانترنت**، بحث مقدم إلى مؤتمر الأمن العربي تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 2002.

[2] علي عبد القادر قهوجي، **الحماية الجنائية لبرامج الكمبيوتر**، المرجع السابق، ص: 139.

حال الظرف المشدد لا يشترط فيه أن يكون قصديا، بينما يتطلب فيه هذا الشرط بالنسبة لجريمة الاعتداء القصدي على نظام المعالجة.

وتتنوع وسائل التعييب أو الإفساد كاستخدام القنبلة المعلوماتية، بحيث يدخل من خلالها مجموعة من المعطيات تتكاثر داخل النظام بحيث تجعله غير صالح للإستعمال[1]، أو استخدام فيروس يطلق عليه "حصان طروادة"، وغير ذلك من الفيروسات التي توقف أو تفسد أو تعطل النظام[2].

ثانياً: الركن المعنوي:

جريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات جريمة عمدية، بحيث يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصرية العلم والإرادة؛ على اعتبار إتجاه إرادة الجاني إلى فعل الإفساد مع علمه بأن نشاطه الإجرامي من شأنه أن يوصله إلى تلك النتيجة، فإذا قام شخص يتعامل مع النظام بصورة مشروعة بإعاقة أو إفساد النظام نتيجة لخطأ في التشغيل أو التعامل مع البيانات ينتفي القصد الجنائي لديه ولا يسأل عن هذه الجريمة[3]، فإذا أثبت الجاني إنتفاء العلاقة السببية بين السلوك الإجرامي– الدخول أو البقاء غير المشروع – والنتيجة الإجرامية التي

---

[1] في سنة 1996 قام مصمم ومبرمج شبكات كمبيوتر ورئيس سابق لشركة أوميغا (Omega) بإطلاق قنبلة الكترونية بعد عشرين يوما من فصله من العمل استطاعت أن تلغي كافة التصاميم وبرامج الإنتاج لإحدى كبرى مصانع التقنية العالية في نيوجرسي والمرتبطة والمؤثرة على نظم التحكم المستخدمة في (Nasa) والبحرية الأمريكية ملحقا خسائر بلغت 10 ملايين دولار.

[2] ضياء مصطفى عثمان، **السرقة الإلكترونية (دراسة فقهية)**، الطبعة الأولى، دار النفائس للنشر والتوزيع، عمان، 2011، ص ص: 73 –75.

[3] عبد الفتاح بيومي حجازي، **النظام القانوني لحماية التجارة الإلكترونية**، المرجع السابق، ص: 43.

هي ذات الظرف المشدد في الجريمة، كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ؛ انتفى السلوك الإجرامي؛ وانتفى بذلك معه القصد الجنائي، ومن الأمثلة على جرائم الدخول أو البقاء لنظام معلوماتي مما أدى إلى محو النظام أو تدميره، قيام مجموعة إرهابية يطبق عليها بإتلاف برامج وملفات تخص شركة كبيرة متخصصة في بيع الحاسبات الآلية[1].

الفرع الثاني: الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام[2].

النشاط الإجرامي في هذه الجريمة ينحصر في أفعال الإدخال والمحو والتعديل، ويكفي توافر إحداها لقيام الجريمة فلا يشترط اجتماعها معا، ومن ثم يقوم الركن في الجريمة، لكن القاسم المشترك في هذه الأفعال جميعا هو انطوائها على تلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل آخر قائمة[3].

من هنا يمكن القول أن النشاط الإجرامي لهذه الجريمة، إنما ينصب على المعطيات أي المعلومات المعالجة آليا التي أصبحت رموزا وإشارات وليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام التي تشكل جزءا منه، وبناء عليه

---

[1] ختير مسعود، المرجع السابق، ص: 119.

[2] نصت عليها المادة 08،04،03 من الاتفاقية الدولية للإجرام المعلوماتي، كما نص المشرع الجزائري عليها في المادة 394 مكرر2 من قانون العقوبات: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريقة الغش المعطيات التي تتضمنها".

[3] علي عبد القادر قهوجي، **الحماية الجنائية لبرامج الكمبيوتر**، المرجع السابق، ص: 143.

فالجريمة لا تتحقق إذا وقع النشاط الإجرامي على المعطيات خارج النظام سواء قبل دخولها أم خروجها، أما المعلومات غير المعالجة التي لم تدخل إلى النظام؛ فهي خارج نطاق الحماية المشمولة بهذا النص؛ وإن كان يجوز حمايتها وفقا لنصوص جنائية أخرى[1]، وتقوم هذه الجريمة على صورتين هما:

أولاً: الاعتداءات العمدية على المعطيات الموجودة داخل النظام.

النشاط الإجرامي في جريمة الاعتداء العمدي على المعطيات يتجسد في إحدى الصور الثلاث التالية[2]:

1. فعل الإدخال **(L'intrusion)**
2. فعل المحو **(L'effacement)**
3. فعل التعديل **(Modification)**

لا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط؛ لكي يتوافر الركن المادي؛ وأفعال الإدخال والمحو والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة أو محو أو تعديل معطيات موجودة من قبل؛ وهذا يعني أن النشاط الإجرامي في هذه الجريمة؛ إنما يرد على محل أو موضوع محدد وهو المعطيات أو المعلومات التي تمت معالجتها آليا التي أصبحت مجرد إشارات أو رموزا تمثل تلك المعلومات، وليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام، أي التي يحتويها النظام وتشكل جزءا منه[3].

---

[1] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص: 43.

[2] آمال قارة، المرجع السابق، ص: 120.

[3] فشار عطاء الله، المرجع السابق، ص: 30.

عمومًا التلاعب في المعطيات الموجودة داخل النظام؛ يتخذ إحدى الأشكال التالية:

- الإدخال (L'intrusion):

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بالمعلومات المعالجة آليا سواء كانت خالية أم كان يوجد عليها معطيات من قبل بقصد التشويش على صحة البيانات القائمة؛ ولعل اصطناع المعلومات هو الأكثر سهولة في التنفيذ ولاسيما في المنشآت ذات الأموال حيث يعد المسؤول في القسم المعلوماتي في أفضل وضع يؤهله لارتكاب هذا النمط غير المشروع من التلاعب[1].

ويتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة، هذه الأخيرة ليسحب بمقتضاها النقود من أجهزة السحب الآلي، وذلك حين يستخدم رقمه الخاص والسري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه، وكذلك الحامل الشرعي لبطاقة الائتمان التي يسدد عن طريقها مبلغ أكثر من المبلغ المحدد له وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب « فيروس» يضيف معطيات جديدة.

- المحـو (L'effacement):

يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة، ومثالها قيام بعض المسؤولين بالاستيلاء على مبلغ قدره 61 ألف

---

[1] نبيل صقر، **جرائم الكمبيوتر والانترنت**، موسوعة الفكر القانوني، دار الهلال للخدمات الإعلامية، الجزائر، 2005، ص: 141.

دولار كانت قد أرسلته إحدى شركات التأمين لصالح أحد المراكز الطبية وقاموا بفتح حسابات وهمية وضعوا المبلغ بها وحتى تتم هذه العملية بنجاح قاموا بمحو حسابات من سجلات الحاسب الآلي للمركز الطبي وهي حسابات المتوفين، وذلك إما لجعلها غير قابلة للتحصيل وإما بحذفها من الملفات[1].

- التعديل (Modification):

يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها، وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة **(Gomme d'effacement)** أو برنامج الفيروسات بصفة عامة[2].

وهذه الأفعال المتمثلة في الإدخال والمحو والتعديل وردت على سبيل الحصر، فلا يقع أي فعل آخر غيرها تحت طائلة التجريم حتى ولو تضمن الاعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات، فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينهما، لأن كل تلك الأفعال لا تنطوي لا على إدخال ولا على تعديل بالمعنى السابق[3].

الفرع الثالث: المساس العمدي بالمعطيات خارج النظام.

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

---

[1] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص: 49.

[2] آمال قارة، المرجع السابق، ص: 122.

[3] فشار عطاء الله، المرجع السابق، ص ص: 30 -31.

فنص المادة (394 مكرر2) يستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة أم لا كأن تكون مخزنة على أشرطة أو أقراص أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

1. الركن المادي:

الواضح من خلال صياغة هذا النص، أنه تضمن صورتين للركن المادي لهذه الجريمة، فهناك:

الصورة الأولى:

نصت المادة (394 مكرر1/2) على تجريم تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم، أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق...الخ.

الصورة الثانية:

جرمت الفقرة الثانية من (394 مكرر2/2) حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

2. الركن المعنوي:

تتحقق هذه الجريمة بمجرد توافر النية بكافة عناصرها– العلم، الإرادة–وبالتالي يكفي أن يعلم الجاني أنه يصمم أو يصنع أو يحوز أو ينشر أو يستعمل أو أي فعل منها، مع إرادته القيام بهذا الفعل، وبالتالي لا يشترط لقيامها نية الإضرار بالشخص مالك البرنامج أو صاحب النظام، وإن كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي إلا أنه ليس عنصرا في الجريمة.

المطلب الثاني: عقوبة جرائم الإعتداء على نظام المعالجة الآلية للمعطيات.

طبقا للمادة (13) من الاتفاقية الدولية للإجرام المعلوماتي؛ فإن العقوبات المقررة للإجرام المعلوماتي يجب أن تكون رادعة وتتضمن عقوبات مالية وسالبة للحرية، تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي، كما توجد عقوبات تطبق على الشخص المعنوي بناءا على تبني مبدأ مساءلة الشخص المعنوي الواردة في المادة (12) من الاتفاقية، كما نص المشرع الجزائري على مجموعة من العقوبات عن الجرائم الماسة بالنظام والمتمثلة في عقوبات أصلية وأخرى تكميلية بموجب المواد من 394 مكرر إلى 394 مكرر 5، كما نص على عقوبة الأشخاص المعنوية والأشخاص الطبيعية، وأيضا عقوبة المساهمة والشريك في الجريمة.

واعتمد المشرع أثناء وضعه لهاته الجرائم على معيار أساسه الخطورة الإجرامية لكل جريمة على حدا، بحيث إتبع مبدأ الهرمية في التدرج في سلم العقوبات، فنص على جريمة الدخول أو البقاء في الصورة البسيطة والمشددة، ثم نص على جريمة الاعتداء العمدي على المعطيات باعتبارها أشد خطورة من سابقتها، ذلك أنها تستهدف المعطيات الموجودة داخل النظام بما فيها البيانات، والبرامج، المعطيات، وأي اعتداء عليها سيؤدي لا محالة إلى وقف النظام أو تعطيله أو تغيير سير وجهة هذا النظام.

الفرع الأول: العقوبات المقررة للشخص الطبيعي.

أولاً: العقوبات الأصلية:

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

- الدخول والبقاء بالغش (الجريمة البسيطة): العقوبة المقررة هي 3 أشهر إلى سنة حبس و50000 دج إلى 100000 دج غرامة (المادة 394 مكرر).
- الدخول والبقاء بالغش (الجريمة المشددة): تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة، وتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة (المادة 394 مكرر/ 2و3).
- الاعتداء العمدي على المعطيات: طبقا لنص المادة (394 مكرر 1)، فالعقوبة المقررة للاعتداء العمدي على المعطيات الموجودة داخل النظام هي الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500000 دج إلى 2000000 دج.

أما العقوبة المقررة لاستخدام المعطيات وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، العقوبة المقررة هي الحبس من شهرين إلى ثلاث سنوات وغرامة من 1000000 دج إلى 5000000 دج (394 مكرر 2).

ثانياً: العقوبات التكميلية:

نصت المادة (394 مكرر 3) من قانون العقوبات على العقوبات التكميلية والمتمثلة في:

- المصادرة: وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية.
- إغلاق المواقع: والأمر يتعلق بالمواقع **(les sites)** التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- إغلاق المحل أو مكان الاستغلال: إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق المقهى الإلكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكها[1].

الفرع الثاني: العقوبات المقررة للشخص المعنوي.

أقر المشرع الجزائري مبدأ مساءلة الشخص المعنوي في القانون 15/04 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 156/66، وذلك بنص المادة (51 مكرر) من هذا التعديل[2]، كما تجدر الإشارة إلى أن المشرع الجزائري، قد أقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي، وذلك في نص المادة (18 مكرر) من القانون رقم 15/04 المتضمن قانون العقوبات[3].

---

[1] نفس المرجع، ص ص: 33-34.

[2] محمد مزاولي، **نطاق المسؤولية الجنائية لمسيري المؤسسات الاقتصادية في القانون الجزائري (دراسة مقارنة)**، رسالة ماجستير، المركز الجامعي بشار، 2006، ص: 310.

[3] نصت المادة 18 مكرر على أن: "العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح هي:

أما بالنسبة لعقوبات الغرامة المطبقة على الشخص المعنوي عند ارتكابه أحد الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة (394 مكرر 4) من قانون العقوبات 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

الفرع الثالث: عقوبة الإشتراك والشروع في الإعتداء على نظام المعالجة الآلية للمعطيات.

1. عقوبة الإشتراك:

نصت عليه المادة (11) من الاتفاقية الدولية للإجرام المعلوماتي، وقد تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة (394 مكرر 5)، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ولم يخضعها لأحكام المادة (176) من قانون العقوبات المتعلقة بجمعية الأشرار[1].

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

ب/ واحدة أو أكثر من العقوبات الآتية:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات.

[1] حيث تنص المادة (394 مكرر5) من قانون العقوبات: "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية، يعاقب بالعقوبات المقررة بالجريمة ذاتها".

من خلال استقراء نص المادة أعلاه، نجد أن المشرع الجزائري لم يخرج عن القواعد العامة لعقوبة الشريك، حيث رصد لها نفس عقوبة الجريمة التامة، ذلك أن جرائم الاعتداء على نظم المعالجة الآلية للمعلومات، أغلبها تتم في شكل مجموعات، وإن لم يسبق اتفاق بين المجموعة على ارتكاب هذه ولكن النتيجة الإجرامية تبين اتفاق ضمني بين أفراد المجموعة، إذْ أن هذه الجرائم لا تتطلب اجتماع حقيقي فيما بين شخصين أو أكثر، وإنما يتصور الاتفاق الجنائي بمجرد انتقال كلمة السر من شخص إلى آخر؛ وإن لم يكن بينها معرفة سابقة، ويستوي أن يكون أفراد الاتفاق مجموعة أشخاص طبيعية أو معنوية.

كما أن المشرع ولرغبته في توسيع نطاق العقوبة أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي، بمعنى أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص، ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها، فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد.

وشروط العقاب على الاتفاق الجنائي بعد استخلاصها من نص المادة (394 مكرر5) من قانون العقوبات، التي هي: "مجموعة أو اتفاق بهدف تحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية، تجسيد هذا التحضير بفعل مادي، فعل المشاركة في هذا الاتفاق، القصد الجنائي".

فبالنسبة لمجموعة أو الاتفاق يستوي أن يكون أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي، كما يستوي أن يعرف أشخاص الاتفاق بعضهم بعضا كما في العصابة أم تكون مجرد مجموعة من الأشخاص، لا يعرف أحدهم الأخر من قبل ولكن اتفقوا فيما بينهم على القيام بالنشاط الإجرامي، المهم أن يتم الاتفاق بين

شخصين على الأقل، فإذا ارتكب الشخص العمل التحضيري المادي شخص واحد بمفرده أو بمعزل عن غيره، فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر؛ إذْ أن المجرم بنص المادة (394 مكرر5) ليس الاتفاق، وإنما المشاركة من طرف شخص طبيعي أو معنوي في الاتفاق، فبمجرد الانضمام إلى الاتفاق غير كافي، بل يجب توافر فعل إيجابي للمشاركة[1].

2. عقوبة الشروع في الإعتداء على نظام المعالجة الآلية للمعطيات:

الجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص، وقد نصت عليه المادة (11) من الاتفاقية الدولية للإجرام المعلوماتي، كما تبنى المشرع الجزائري فكرة العقوبة على الشروع في ارتكاب الجنح الماسة بنظام المعالجة الآلية للمعطيات المشرع الجزائري بموجب المادة (394 مكرر 7) من قانون العقوبات[2]، وذلك رغبة منه في توفير حماية فعالة لهذا النظام[3].

المبحث الثاني: الحماية الجنائية لبرامج الكمبيوتر من خلال نصوص الملكية الفكرية.

نظراً لنسبية الحماية المقررة من خلال النصوص التقليدية في قانون العقوبات الجزائري، ارتأينا البحث في مدى إمكانية الحماية من خلال نصوص قانون الملكية الفكرية وبالتحديد قانون حقوق المؤلف، باعتبار أن المشرع الجزائري مثله مثل معظم التشريعات، قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءات الاختراع، وذلك طبقا للمادة (07) من الأمر 07/03 المتضمن براءة الاختراع: "لا

---

[1] فشار عطاء الله، المرجع السابق، ص ص: 36-37.

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

[3] أمال قارة، المرجع السابق، ص: 133.

تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب"[1]، وعليه سنفصل في حماية أنظمة المعالجة الآلية للمعطيات في إطار قانون حق المؤلف، من خلال:

المطلب الأول: الحماية الجنائية في نطاق قانون حق المؤلف.

نجد أن المشرع حسم كل خلاف قد ينشأ من جراء الاعتداء على هذه البرامج وذلك بإدخالها ضمن نطاق حماية حق المؤلف وفي سبيل تقرير حماية جنائية فعالة في هذا المجال، وقد عدد المشرع هذه الأفعال هي تلك المكونة لجريمة التقليد والجرائم الملحقة بها، بالإضافة إلى أهم العقوبات التي جاءت في الأمر رقم 05/03 الصادر بتاريخ 2003/07/19 المتعلق بحق المؤلف.

الفرع الأول: الحماية عن طريق تجريم تقليد برامج الكمبيوتر.

عرفت جريمة التقليد بأنها: "نقل مصنف لم يسقط في الملك العام من غير إذن مؤلفه"، وعرفت كذلك بأنها: "القيام بعمل لا يقوم به سوى المؤلف أو يرخص به".

أما قانون حق المؤلف، فلم يتعرض لتعريف جريمة التقليد، وإنما اكتفى بتعداد الأفعال المشكلة للجرائم الموصوفة بالتقليد في المادتين (151) و(152) من الأمر رقم 05/03 الصادر بتاريخ 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر رقم 14/73 بقوله: "يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية:

- الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف.
- استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة"[2].

---

[1] الأمر رقم 07/03 المؤرخ في 2003/07/19 المتعلق ببراءات الاختراع.

[2] خثير مسعود، المرجع السابق، ص ص: 88- 89.

من هذا المنطلق، يمكن القول أنه لقيام جريمة التقليد لابد من توافر ركنيين أساسيين: الركن المادي والركن المعنوي، وذلك على النحو التالي:

أولا: الركن المادي.

لقيام الركن المادي، لابد من توافر سلوك ونتيجة وعلاقة سببية بينهما، والنشاط الإجرامي في جريمة التقليد يأخذ صورة من إحدى الصورتين السابقتا الذكر في المادتين (151) و(152)، وذلك على النحو التالي:

1. الكشف غير المشروع عن البرمجية:

إن الكشف عن البرمجيات، أي إظهارها للعلن يكون غير مشروع إذا خالف الطرق المشروعة أو القانونية لذلك، ويعتبر الكشف غير مشروع عن البرمجيات فعلاً مكونا لجنحة التقليد طبقا للمادتين (151) و(152) ، وبالرجوع إلى أحكام الأمر رقم 05/03، نجد أن المادة (22) منه، قد نصت على أن للمؤلف الحق في الكشف عنه باسمه أو باسم مستعار، ويمكنه تحويل هذا الحق إلى الغير، كما يعود هذا الحق إلى ورثته بعد وفاته، فلهم الحق في الكشف عن البرمجية[1]، وبالتالي فإن أي عملية للكشف عن البرمجية وإظهار من قبل الغير الذي لم يحال له هذا الحق يعد اعتداء غير مشروع ويدخل نطاق التجريم، وعليه فإن للمؤلف وحده الحق في اختيار الوقت والطريقة التي يتم بها إذاعة أو نشر برنامجه، وبالتالي فإن أي نشر لهذا البرنامج في غير الوقت أو بغير الطريقة التي أرادها المؤلف يعد اعتداء.

كما أن طرق الكشف عن البرمجيات أصبحت كثيرة ومتنوعة، وذلك بسبب تطور تكنولوجيات كسر الحماية بالموازاة مع تطور طرق حماية البرمجيات، ومن بين طرق الكشف غير المشروع عن البرمجيات كسر حمايتها عن طريق الحصول على

[1] راجع المادة (22) من الأمر رقم 05/03.

الشفرة السرية التي تسمح بالدخول للبرمجة واستغلالها كمستعمل مرخص له، أو صاحب حق عليها، ومن الطرق أيضا قرصنة الرقم التسلسلي للنسخة من البرمجة، وهو رقم تضعه الشركة المصنعة للبرمجة من أجل ضمان عدم تقليد برمجياتها أو استنساخها بطريقة ما على حد سواء، وفي هذا الشأن أدانت المحكمة الإصلاحية لمدينة ميتز الفرنسية شابين قرصانين، بسبب قيامها بالهندسة العكسية والنسخ لبرمجيات ألعاب والكشف عنها في ذات اليوم الذي قررت فيه الشركة المنتجة الإطلاق التجاري لها[1].

2. المساس بسلامة البرمجية:

للمؤلف وحده الحق في تعديل أو تحوير أو تغيير أو حذف أو إضافة في برنامجه، ولا يمكن للغير الاعتراض على ذلك ما لم يكن فيه إخلال أو مساس بمصالحهم، فمؤلف البرنامج له حق التعديل دون التغيير في هذه الحالة بنوع المصنف، وإدخال ما يراه ملائما أثناء عملية صنع الدعامة[2].

كما أنه لا يمكن لأي كان أن يدخل تعديلات على المصنف بتصحيح أو إضافة أو تعديل أو حذف إلا بموافقة من المؤلف، وهذا ما يظهر من خلال استقراء نص المادة (90) من الأمر رقم 05/03، إلا أنه يرد استثناء على هذه المادة المنصوص عليه بالمادة (25) من هذا الأمر التي نصت على أنه: "يحق للمؤلف إشتراط احترام سلامة مصنفه والاعتراض على أي تعديل يدخل عليه أو تشويهه أو إفساده، إذا كان ذلك من شأنه المساس بسمعته كمؤلف أو بمصالحه المشروعة".

---

[1] بن زيطة عبد الهادي، **حماية برامج الحاسوب في التشريع الجزائري وفقا لأحكام قانون حقوق المؤلف الجديد الأمر رقم 05/03**، دار الخلدونية، الطبعة الأولى، الجزائر، 2007، ص ص: 78-79.

[2] انظر المادة (89) من الأمر رقم: 05/03.

بمفهوم المخالفة أنه إذا لم يكن من شأن هذه التعديلات المساس بسمعة المؤلف أو بشرفه أو بمصالحه المشروعة، فإنه لا يمكن الاعتراض عليها من طرف المؤلف، ومثال ذلك تعديل معدل ضريبة القيمة المضافة في أحد البرامج المصممة لمأموري الضرائب العقارية.

وقد ذهبت التوجيهات الأوروبية الصادرة في: 1991/05/14 إلى هذا، حيث نصت المادة (1-5)، على أن المؤلف لا يستطيع أن يمنع تعديل أو تحوير البرنامج طالما كان ذلك ضروريا لتمكن الحائز الشرعي من استغلال هذا البرنامج على النحو التالي الذي يتلائم مع الغرض المعد له، وعلى ذلك فإنه لا يوجد ما يمنع من ليتلائم مع المتطلبات الشخصية للحائز الشرعي لهذا البرنامج بما يساير المستجدات التشريعية أو الشخصية أو اللائحية أو أي نوع آخر من المستجدات أو المتغيرات، طالما كان هذا التعديل لازما للحفاظ على القيمة الاقتصادية والعلمية لهذا البرنامج في حدود الحقوق المتنازع عنها أو الممنوحة لمستغل البرنامج[1].

3. استنساخ البرنامج بأي أسلوب من الأساليب في شكل نسخ مقلدة:

يعد هذا السلوك الإجرامي من أشهر وأخطر عمليات التقليد والقرصنة المعلوماتية لسهولة القيام بها وقلة تكاليفها وارتفاع مداخليها، واستنساخ البرمجيات قد يتم في عدة صور باختلاف الدعامة، والمصدر المتواجد فيه هذه البرمجيات.

غير أن التساؤل المطروح هو: هل الاستنساخ المقصود يتمثل فقط في إجراء نسخة طبق الأصل للبرمجة من مصدرها إلى وسيلة أو دعامة مشابهة (كمثال: نسخ

[1] خالد مصطفي فهمي، **الحماية القانونية لبرامج الكمبيوتر**، دار الجامعة الجديدة للنشر، الإسكندرية، 2005، ص: 119.

قرص مضغوط CD إلى آخر بواسطة **(Gravure du CD)**، أم كل استنساخ يعتبر غير مشروع كيفما كان سواء من دعامة إلى أخرى أو غيرها ؟

والجواب هو أن المقصود من الاستنساخ هو كل عملية الهدف منها الاعتداء على البرامج محل الحماية بأي طريقة كانت، وتبقى مسألة توسيع نطاق هذه السلوكيات أو تصنيفها من اختصاص المصالح الأساسية للشركات أو الأفراد المعنيين بها، وعلى سبيل المثال تقرر شركة **(Microsoft)** بأن المستعمل يجري نسخة عن برنامج الكمبيوتر، كلما قام بما يلي:

- تحميل البرنامج إلى الذاكرة المؤقتة **(RAM)** تشغيله في قرص أو ثابت أو مضغوط أو وسيلة تخزين أخرى.
- نسخ البرنامج إلى وسائط أخرى مثل القرص المرن أو القرص الثابت للجهاز.
- تشغيل البرنامج على الكمبيوتر من ملقم شبكة الاتصال حيث يوجد البرنامج أو حيث يتم تخزينه. واعتبرت أن النسخ يكون غير مشروع إذا تم دون إذن مالك الحقوق.

هذا وغالبا ما تحدد إتفاقية الترخيص التي ترافق معظم البرمجيات ذات الانتشار العالمي شروط لاستخدام ما يعد مشروعا وما لا يعد مشروعا بالنسبة للاستنساخ، ويدخل في حكم الاستنساخ تثبيت البرمجية على القرص الصلب للحاسوب، باعتبار أن عملية التثبيت تستدعي بالضرورة نقل الملفات الموجودة في المصدر الأصلي للبرمجة إلى موقع التثبيت، ويدخل تثبيت البرمجة في جهاز آخر غير مرخص به للتثبيت في حكم الاستنساخ غير المشروع، حيث قضت المحكمة الإصلاحية لمدينة **Cusset** الفرنسية في قضية شركة قام رئيسها رفقة أحد مديريه بتثبيت برمجية مرخص بها لجهاز واحد في باقي أجهزة المؤسسة، وتمت إدانته بناء على تفتيش من فرقة درك فرنسية مختصة.

وبالنسبة للمشرع الجزائري، فقد اعتبرت المادة (2/27) من الأمر رقم 10/97 المؤرخ في 1997/03/06 المتعلق بحق المؤلف والحقوق المجاورة، أن المؤلف أو مالك الحقوق المادية على المصنف هو الوحيد المخول دون غيره بإجراء نسخ من الصنف وبأي وسيلة كانت، غير أن التخويل ليس على إطلاقه، فقد أورد الأمر السابق عدة استثناءات في أكثر من موضع تمكن من استنساخ المصنفات بدون إذن صاحبها أو مؤلفها[1]، وتتعلق جل هذه الاستثناءات بأغراض تعليمية أو إعلامية غير هادفة لتحقيق الربح، ومن هذه الاستثناءات نورد الاستثناء الذي نصت عليه المادة (52) من قانون حماية حقوق المؤلف، بأنه: "يعد عملا مشروعا كل استنساخ بدون ترخيص من المؤلف أو من أي مالك آخر من هذا البرنامج أو اقتباسه شريطة أن يكون كل من النسخة أو الاقتباس ضروري لما يأتي:

- استعمال برنامج الحاسوب للغرض الذي اكتسب من أجله ووفقا للشروط التي كانت قائمة عند اكتسابه.
- تعويض نسخة مشروعة الحيازة من برنامج الحاسوب لغرض التوثيق في حالة ضياعه أو تلفه أو عدم صلاحيته للاستعمال[2].

كما نصت المادة (53) من نفس الأمر على أنه: "ينبغي أن تقتصر الاستعمالات على استنساخ نسخة واحدة من برنامج الحاسوب أو اقتباسه على الأوجه المنصوص عليها في المادة (52) أعلاه، يجب تدمير كل نسخة مستنسخة من برنامج الحاسوب منه عند انقضاء مشروعية حيازتها".

بهذا يكون المشرع الجزائري، قد فصل جيدا الاستنساخ بالنسبة للبرمجيات وحددها في حالات استثنائية معينة، إضافة إلى ضرورة توافر سلوك من السلوكيات

---

[1] بن زيطة عبد الهادي، المرجع السابق، ص ص: 81-80.

[2] فشار عطا الله، المرجع السابق، ص: 36.

السابقة الذكر، لابد كذلك وأن يصحب هذا السلوك عدم موافقة المؤلف، فكما سبق الذكر أن للمؤلف حق التنازل عن برنامجه أو عن حق من الحقوق المادية المخولة له المادة (27) من الأمر السابق، كما أن هذا الإذن يعد بمثابة عنصر أساسي لقيام هذه الجريمة، فبتخلفه تقوم الجريمة وبوجوده تنتفي الجريمة[1]، وقد اشترط المشرع ضرورة وجود إذن كتابي من المؤلف يتنازل به عن حقوقه المادية (المادة 62) من الأمر رقم 05/03 المتعلق بحق المؤلف والحقوق المجاورة الصادر بتاريخ 2003/07/19 المعدل والمتمم للأمر رقم 14/73، وبالتالي فالكتابة هنا تعتبر شرط وجود لا شرط إثبات، كما أن الإذن اللاحق لا يمكن أن يأخذ حكم الإذن السابق، وبالتالي فالموافقة بعد تمام الجريمة لا تحول دون المتابعة.

ثانياً: الركن المعنوي.

لا يكفي لقيام جريمة التقليد وجود الركن المادي وحده بل لابد من توافر عنصري العلم والإرادة لدى الجاني أثناء قيامه بأي اعتداء في صورة من الصور السابقة، والقصد المتطلب في هذه الحالة هو القصد العام وليس الخاص، فليس بالضرورة أن يقصد المعتدي إلحاق الضرر بمؤلف البرنامج، وبالتالي فيكفي أن يعلم الجاني أنه يعتدي على برنامج لشخص أخر وأن ذلك الفعل يعد جريمة.

الفرع الثاني: الجرائم الملحقة بجريمة التقليد.

نصت على هذه الجرائم الفقرات الثالثة والرابعة والخامسة من الأمر رقم 05/03 الصادر بتاريخ 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر رقم 14/73، وهي كالتالي:

[1] ختير مسعود، المرجع السابق، ص ص: 94- 95.

أولاً: الركن المادي.

لتوافر الركن المادي للجرائم الملحقة بجريمة التقليد، لابد وأن يقع سلوك من السلوكيات التالية: استيراد أو تصدير نسخ مقلدة من مصنف أو أداء، بيع نسخ مقلدة من مصنف أو أداء، تأجير أو وضع رهن التداول نسخ مقلدة لمصنف أو أداء، كما أضافت المادتين 154 و155 جريمتي: المشاركة في التقليد والرفض عمدا دفع المكافأة المستحقة للمؤلف.

1. استيراد أو تصدير برامج مقلدة من مصنف أو أداء:

بسط المشرع الجزائري حمايته على جميع البرامج المحمية سواء بالقانون الجزائري أو بقانون دولة أجنبية بشرط أن يكون متمتعا بالحماية في دولته، فيستوي بذلك أن يكون مؤلف البرنامج جزائري أم أجنبي، كما يستوي أن يكون الجاني جزائري الجنسية أم أجنبي وهو خروج عن مبدأ الإقليمية، كما يشترط لقيام هذه الجريمة عدم موافقة المؤلف وهي بذلك تشترك مع جرائم التقليد في التداول كون أن الموافقة المطلوبة في هذه الحالة هي موافقة كتابية، بمعنى أن الموافقة الضمنية أو الشفوية أو الموافقة اللاحقة لا تغني عن المتابعة.

2. المشاركة في تقليد برنامج من مصنف أو أداء:

تعد هذه الصورة من التقليد تطبيقا للقواعد العامة بمعاقبة الشريك وهو الشخص الذي يساهم في هذه الجريمة سواء بعمله لمدة محدودة أو غير محدودة.

3. رفض دفع المكافأة المستحقة عمدا لمؤلف البرنامج:

يقوم الركن المادي لهذه الجريمة في حالة إمتناع الشخص المكلف بدفع المكافأة المستحقة لمؤلف البرنامج عمدا، ومثال ذلك ما نصت عليه المادة (95) من قانون حماية حق المؤلف، وتكون في أغلب الأحوال من جراء تنازل مؤلف عن حق من حقوقه المادية سواء كلية أو بصفة مؤقتة.

4. بيع برامج أو تأجير أو وضع رهن التداول لبرامج مقلدة من مصنف أو أداء:

يظهر الركن المادي لهذه الجريمة في حالة التعامل في البرامج المقلدة سواء بالبيع أو التداول، ويكون البرنامج مقلدا إذا كان مشابها للبرنامج الأصلي المحمي من طرف القانون، والعبرة في ذلك بأوجه الشبه لا بأوجه الاختلاف بحيث يكون من شأنه أن ينخدع به الجمهور في المعاملات[1]، وكما ذكرت أن المشرع قد نص على ثلاثة حالات رئيسية للتعامل في البرنامج المقلد وذلك بالبيع، والمقصود من ذلك نقل حق استغلال البرنامج إلى الغير مقابل ثمن معين، وسواء كان هذا الاستغلال ينطوي على نشر أم استعمال أم ترجمة للبرنامج المقلد. أما بالنسبة للتأجير، فيقصد منه وضع البرنامج المقلد أو نسخ منه لدى الغير – المستأجر– قصد تمكينه من استعمال لمدة معينة مقابل دفع أجر مالي محدد. أما التداول، فيقصد به وضع البرنامج بين يدي الغير لاستعمالها سواء بمقابل أو بغير مقابل أو الانتفاع بها سواء لمدة محدودة أو غير محدودة[2].

ثانياً: الركن المعنوي.

القصد الجنائي بالنسبة لهذه الجرائم مفترض، بحيث يقوم الركن المعنوي بمجرد اتجاه إرادة الجاني إلى القيام بسلوك من السلوكيات السابقة فهو مرتبط بتوافر الركن المادي، والشروع متصور في أغلب هذه الجرائم، وبالتالي فالقصد المتطلب في هذه الجرائم هو القصد العام فقط، وتجب الإشارة إلى أن جريمة التصدير والاستيراد للبرامج المقلدة التي تتطلب إلى جانب القصد العام توافر القصد الخاص، إذْ لابد منّ أن تتجه إرادة الجاني إلى فعل من الفعلين المذكورين "الاستيراد والتصدير"[3].

---

[1] نفس المرجع، ص: 34.

[2] بن زيطة عبد الهادي، المرجع السابق، ص: 82.

[3] ختير مسعود، المرجع السابق، ص: 98.

المطلب الثاني: العقوبات المقررة لجريمة التقليد.

قبل صدور قانون حماية المؤلف كان التعدي على الملكية الأدبية والفنية تحكمه المواد (390) إلى (394) من قانون العقوبات الجزائري، إلا أن أحكام هذه المواد ألغيت بمقتضى المادة (151) من الأمر رقم 10/97 المؤرخ في 6 مارس 1997، كما ألغي هذا الأمر بموجب الأمر 05/03، حيث تضمنت المواد (153)، (156)، (157)، (158)، (159) العقوبات المقررة لجريمة التقليد وهي على قسمين: عقوبات أصلية وتكميلية.

الفرع الأول: العقوبات الأصلية.

نصت المادة (153) من الأمر رقم 05/03، على عقوبة التقليد بقولها: "يعاقب مرتكب جنحة تقليد مصنف أو أداء كما هو منصوص عليه في المادتين (151) و(152) أعلاه، بالحبس من ستة أشهر إلى ثلاثة سنوات وبغرامة مالية من خمسمائة ألف دينار إلى مليون دينار سواء كان النشر قد حصل في الجزائر أو في الخارج"، كما نصت المادة (154) من الأمر رقم 05/03، بقولها: "يعد مرتكبا الجنحة المنصوص عليها في المادة (151) من هذا الأمر ويستوجب العقوبة المقررة في المادة 153 أعلاه، كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة"، ونصت المادة (155) من الأمر رقم 05/03، بقولها: "يعد مرتكبا لجنحة التقليد ويستوجب نفس العقوبة المقررة في المادة 153 أعلاه كل من يرفض عمدا دفع المكافأة المستحقة للمؤلف أو لأي مالك حقوق مجاورة....."، ونصت المادة (156) من الأمر رقم 05/03، بقولها: "تضاعف في حالة العود العقوبة المنصوص عليها في المادة 153 من هذا الأمر"[1].

[1] ختير مسعود، نفس المرجع، ص ص: 99-100.

ومما تجدر الإشارة إليه أن هذه العقوبات تسري على جميع صور التقليد السابقة.

الفرع الثاني: العقوبات التكميلية.

تتلخص هذه العقوبات في الغلق والمصادرة ونشر ملخص الحكم الصادر في الدعوى.

1. الغلق:

نصت المادة (156) من الأمر رقم 05/03، بقولها: "يمكن للجهة القضائية المختصة أن تقرر الغلق المؤقت لمدة لا تتعدى ستة أشهر للمؤسسة التي يستغلها المقلد أو شريكه أو أن تقرر الغلق النهائي".

بناء على هذه المادة، فإن للمحكمة الحكم بغلق المؤسسة التي يستغلها المقلد سواء كانت مملوكة لهم أم مستأجرة، ويجوز كذلك الحكم بالغلق المؤقت أو النهائي لهذه المؤسسة وذلك بالموازاة مع حجم الخسائر أو نوع الجريمة القائمة ويرجع الفصل فيها لمحكمة الموضوع.

2. المصادرة:

نصت المادة (159) من الأمر رقم 05/03، بقولها: "يمكن للجهة القضائية المختصة مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي مصادرة، وإتلاف كل عتاد أنشأ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة".

يتضح من خلال نص المادة أن المصادرة وجوبية، فالقاضي ملزم بأن يحكم بمصادرة وإتلاف جميع الوسائل والعتاد المستخدم في النسخ والتقليد، كما وأن المادة (159) حددت الجهة التي يمكن أن تؤول إليها هذه الأموال والوسائل محل

المصادرة، بحيث قررت تسليمها للمؤلف أو مالك الحقوق أو ذوي حقوقها، وهي بذلك تعتبر بمثابة تعويض عن الضرر اللاحق بهم.

3. نشر ملخص الحكم:

نصت على هذه العقوبة المادة (158) من الأمر رقم 05/03، على أنه للمحكمة بطلب من الطرف المدني أن تأمر بنشر أحكام الإدانة كاملة أو مجزأة في الصحف التي تعينها وتعليق هذه الأحكام في الأماكن التي تحددها، ومن ضمن ذلك على باب مسكن المحكوم عليه على نفقة هذا الأخير شريطة أن لا تتعدى هذه المصاريف الغرامة المحكوم بها[1].

ويقصد بهذه العقوبة التشهير بالمحكوم عليه والتأثير على شخصيته الأدبية والمالية، فهي ماسة بالشرف والاعتبار وهي عقوبة تكميلية وجوبية يجب الحكم بها دائما في حال صدور حكم بالإدانة حتى ولو وقف تنفيذ الحكم[2].

الخاتمـــة

في الأخير نخلص إلى أنه، بالرغم من ما للثورة المعلوماتية من ايجابياتها وقدرتها على تغيير أوجه الحياة إلى الأحسن والأفضل، إلا أن هذه الثورة المعلوماتية ذاتها تحمل في طياتها أيضا العديد من السلبيات التي تتمثل في الاستخدام غير المشروع لنظم الحاسب الآلي، ومن هذا المنطلق استطاع الجناة تطوير طرق الإجرام على نحو عال من التقنية في بيئة تكنولوجيا المعلومات.

رأينا كيف أن المشرع الجزائري لا يتوفر على آليات قادرة على الاضطلاع بالآثار الخطيرة التي ترتبها جرائم المساس بأنظمة المعالجة الآلية للمعطيات سواء

---

[1] بن زيطة عبد الهادي، المرجع السابق، ص: 87.

[2] ختير مسعود، المرجع السابق، ص ص: 101- 102.

على مستوى النصوص التشريعية أو على مستوى طبيعة الكوادر والأجهزة المتخصصة لمواجهة هذا النوع من الإجرام، ومن ثم كان لابد أن يبادر إلى تبني سياسة موسعة ومحكمة، تستهدف إيقاف كل التحديات التي يطرحها هذا الإجرام، وإيمانا بأهمية الوقوف أمام التحديات التي تفرضها هذه الجريمة، ارتأينا ختام هذا البحث ببعض الاقتراحات والتوصيات التي قد تساهم في التقليل من الآثار السلبية لكثير من التحديات المصاحبة لوسائل الاتصال الجديدة، وتندرج هذه التوصيات تحت النقاط الآتية :

1. خلق ثقافة اجتماعية جديدة تصور جرائم الإنترنت على أنها أعمال غير مشروعة تمس أو تضر بالمجتمع الدولي ككل مثلها مثل أنماط الجريمة العالمية الأخرى، والتأكيد على أن مجرم الإنترنت يستهدف الإضرار بالآخرين، ويستحق العقوبة بدل عبارات الإعجاب التي تبرز كل ما تتم جريمة جديدة.
2. إعطاء جرائم التقنية حقها من الأهمية في مؤسسات التشريع الوطنية والدولية على السواء، مع التركيز على أهمية إدراج نصوص هذه الأخيرة ضمن التشريعات الوطنية المختلفة، باعتبار أن جرائم الإنترنت ذات بعد دولي تتطلب الانخراط في اتفاقيات دولية، والاهتمام بالتعاون الدولي في مجال المكافحة لضمان الحماية العالمية الفعالة لبرامج المعطيات الآلية والكمبيوتر وشبكة الانترنت ككل.
3. تعديل بعض التشريعات الحالية بما يتلاءم مع طبيعة جرائم الإنترنت، والتقنية، وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات، وشرحها لهم بشكل واضح، وخاصة وانفي مجال الملكية الفكرية فالتشريع الوحيد الذي تقع برامج المعالجة الآلية للمعطيات تحت حمايته هو قانون حقوق المؤلف وحتى في هذا إطار هذا القانون لا تتعدى الحماية شكل البرنامج فقط، لهذا السبب تبرز أهمية

البحث عن إطار أكبر وأوسع لبرامج الكمبيوتر يتعدى النصوص التقليدية لجريمة التقليد المنصوص عليها في قانون حقوق المؤلف والحقوق المجاورة.

4. تشجيع الباحثين بالدعم المعنوي والمادي، لإجراء المزيد من البحوث والدراسات حول الجرائم المستحدثة.
5. عقد دورات مكثفة للعاملين في حقل التحري والتحقيق، والمحاكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسبات، والجرائم المرتبطة بها، والنظر في تضمين مناهج التحقيق الجنائي في كليات، ومعاهد تدريب الشرطة موضوعات عن جرائم الإنترنت.
6. مساعدة شركات التقنية، والإنترنت العربية في اتخاذ إجراءات أمنية مناسبة سواء من حيث سلامة المنشآت، أو ما يختص بقواعد حماية الأجهزة، والبرامج.
7. التنسيق لإنشاء مركز معلومات عربي مشترك يهتم برصد وتحليل جرائم الحاسوب، يضم معلومات مكتملة عن أي واقعة ومعلومات عن المدانين والمشتبه بهم، حيث أن جريمة الإنترنت لا تحدها حدود وطنية، أو قومية.

قائمة المراجع

أ- الكتب:

- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، 2006.
- بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري وفقا لأحكام قانون حقوق المؤلف الجديد الأمر رقم 05/03، دار الخلدونية، الطبعة الأولى، الجزائر، 2007.
- خالد مصطفي فهمي، الحماية القانونية لبرامج الكمبيوتر، دار الجامعة الجديدة للنشر، الإسكندرية، 2005.

- ختير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، 2010.
- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، 2002.
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، 1999.
- ضياء مصطفى عثمان، السرقة الإلكترونية (دراسة فقهية)، الطبعة الأولى، دار النفائس للنشر والتوزيع، عمان، 2011.
- نائلة عادل محمد فريد قروة، جرائم الكمبيوتر الاقتصادية، منشورات حلبي، الطبعة الأولى، بيروت، 2005.
- نبيل صقر، جرائم الكمبيوتر والانترنت، موسوعة الفكر القانوني، دار الهلال للخدمات الإعلامية، الجزائر، 2005.

ب- المذكرات والرسائل:

- محمد مزاولي، نطاق المسؤولية الجنائية لمسيري المؤسسات الاقتصادية في القانون الجزائري (دراسة مقارنة)، رسالة ماجستير، المركز الجامعي بشار، 2006.

ج- الندوات والملتقيات:

- فشار عطاء الله، "مواجهة الجريمة المعلوماتية في التشريع الجزائري"، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية المزمع عقده بأكاديمية الدراسات العليا بليبيا في أكتوبر 2009.
- يونس عرب، "جرائم الكمبيوتر والانترنت"، بحث مقدم إلى مؤتمر الأمن العربي، تنظيم المركز العربي للدراسات والبحوث الجنائية أبو ظبي 2002.

د- الاتفاقيات والقوانين:

- الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ 2001/11/08.

- القانون رقم 14/04 المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية العدد (71) لسنة 2004.
- القانون رقم 15/04 المؤرخ في 27 رمضان 1425 هـ الموافق لـ10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات رقم 156/66 المؤرخ في 18 صفر 1386 هـ الموافق لـ 8 يوليو 1966، الجديدة الرسمية العدد (71) لسنة 2004.
- القانون رقم 06-22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، والمتضمن قانون الإجراءات الجزائية، المنشور في الجريدة الرسمية رقم84 الصادرة سنة 2006.
- الأمر رقم 07/03 المؤرخ في 2003/07/19 المتعلق ببراءات الاختراع المعدل للأمر رقم 17/93 المؤرخ في 1993/12/07 المتعلق بحماية الاختراعات المعدل للأمر 54/66 في 1963/03/03 المتعلق بشهادات المخترعين وإجازات الاختراع.
- الأمر رقم 05/03 الصادر بتاريخ 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة.