حول مكافحة الجريمة الالكترونية في التشريع الجزائري

Combating cybercrime in Algerian legislation

الدكتورة/ ناجية شيخ
جامعة مولود معمري تيزي وزو، الجزائر
nadjya.chikh@yahoo.fr

تاريخ الاستلام: 2018/05/23 تاريخ القبول للنشر: 2018/06/10

❖❖❖❖❖❖❖

ملخّص:

تناول البحث الاهتمام الكبير للمشرع الجزائري بأحكام الجريمة الالكترونية، وذلك من خلال سنه لإجراءات وتدابير كثيرة للتصدي لهذا النوع الجديد من الإجرام، وسعيا وراء ذلك، فإنه انتهج سياسة مزدوجة في المكافحة، حيث أدخل تعديلات كثيرة على قانون العقوبات إثر تعديله سنة 2004 بصدور القانون رقم 04-15 وكذا في تعديله الحاصل في سنة 2006، بموجب القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية وكل ذلك تعرفه القواعد العامة للمكافحة. غير أن مشرعنا ذهب إلى أبعد من ذلك، حيث استحدث قوانين خاصة تختص بعملية الوقاية والقمع، ولاسيما منها القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، والمهم في ذلك هو القضاء على هذا الإجرام الخطير أو على الأقل التقليل من حدته. ويتحقق عندها التنظيم الفعال للجريمة.

كلمات مفتاحية: جريمة معلوماتية؛ مكافحة؛ الجريمة؛ حماية قانونية؛ الجزائر.

Abstract:

The study dealt with the great interest of the Algerian legislator in the provisions of cybercrime, through the enactment of many measures and dispositions to deal with this new type of criminality. Thus, it followed a double policy of fight. Many amendments were introduced to the Penal Code after its amendment in 2004, No. 04-15, amended in 2006 by Law No. 06-22, amended and supplemented by the Code of Criminal Procedure. All this is defined by the general rules of control. However, our legislator went further, introducing special laws on prevention and repression, in particular Law No. 90-04 relating to special prevention-related information technology, communication and control rules, why it is important to eliminate this serious crime, or at least reduce its severity.

Keywords: *Crime Information ; Fight ;Crime ;Legal protection ; Algeria*

مقدّمة:

إنّ الأضرار الوخيمة للجرائم الإلكترونية المستحدثة في يومنا هذا، سواء على الأفراد ككل، أو على مؤسسات الدولة، أدّت بالمشرع الجزائري إلى التفكير في ضرورة التصدي لها وقمعها أو على الأقل العمل على الحدّ منها. وهو ما لا يتحقق في نظرنا إلا بالتنظيم القانوني الفعال لهذا الصنف من الجرائم.

وسعيا وراء تحقيق هذا الهدف، فإنّ مشرعنا قد اتجه إلى استحداث نصوص قانونية وطنية كثيرة بهدف التماشي مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال.

تبعا لذلك، عمد المشرع الجزائري إلى تعديل وإعادة النظر في العديد من التشريعات الوطنية وعلى رأسها قانون العقوبات كقانون عام، وأكثر من ذلك، فإنّه استحدث قوانين أخرى خاصة لم تكن معروفة من قبل، وكل ذلك من أجل ضمان الحماية الجنائية للمعاملات الإلكترونية.

والإشكال الذي يمكن طرحه هنا يكمن في: ما هي خصوصية سبل وآليات مواجهة الجرائم الإلكترونية في القانون الجزائري؟

ومن اجل الإجابة عن التساؤل، يتم التعرض إلى إبراز سبل مكافحة الجرائم الإلكترونية في إطار القواعد العامة – أي ضمن قانون العقوبات – (المبحث الأول)، وإظهار تلك الطرق المكرّسة في إطار القوانين الخاصة (المبحث الثاني).

المبحث الأول

مواجهة الجرائم الإلكترونية في إطار القواعد العامة

حاول المشرع الجزائري خلال الفترات الأخيرة من الزمن تدارك الفراغ القانوني الذي عرفه مجال الإجرام الإلكتروني، فقام بتعديل أحكام قانون العقوبات الجزائري، بموجب القانون رقم 04-15[1]، مستحدثا فيه مجموعة من النصوص، التي جرّم من خلالها كل الأفعال والسلوكات المرتبطة بالمعالجة الآلية للمعطيات، وحدّد لكل فعل منها جزاءً.

ويمكن الإشارة قبلها، إلى تعريف الجريمة الالكترونية أو الجريمة السيبرانية أو جريمة الفضاء الالكتروني مثلما يسميها البعض، وهي جريمة يستخدم الحاسوب في ارتكابها، وهي عبارة عن مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي وسواء كان ذلك بطريقة مباشرة أو غير مباشرة، والمهم في ذلك هو استخدام وسائل الاتصال الحديثة بشأنها من كمبيوتر، أو أية آلة ذكية أخرى.

وتتميز الجريمة الالكترونية عن الجريمة التقليدية من حيث تعريفها، وخصائصها، وأركانها، وكذا القانون الواجب التطبيق عليها.

وتبعا لذلك اتسمت الجريمة الالكترونية بخصائص عديدة، أهمها أنها عابرة للحدود، وتمارس داخل النظام ألمعلوماتي، وترتكب من طرف مجرم معلوماتي يوصف بالذكاء والمهارة، وكما أنها صعبة الإثبات مقارنة بالجريمة العادية، وأن مسرح الجريمة فيها غير محدد المعالم، وهي سريعة التنفيذ ومتطورة بتطور الوسائل التكنولوجية، مما أدى إلى ضرورة تنظيمها من المشرع، ويشترط في هذا التنظيم أن يكون محكما.

وعن صور هذه الجريمة، فيمكن أن تأخذ وصف الاعتداء على نظام المعالجة الآلية للمعطيات (المطلب الأول)، أو وصف الاعتداء على معطيات نظام المعالجة الآلية للمعطيات (المطلب الثاني).

المطلب الأول: تجريم الاعتداء على نظام المعالجة الآلية للمعطيات

يقصد بنظام المعالجة الآلية للمعطيات: «كل نظام أو مجموعة من الأنظمة متصلة كانت أم منفصلة عن بعضها البعض أو المرتبطة والتي يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين»[(2)].

والتعريف نفسه جاء في الاتفاقية الدولية للإجرام المعلوماتي المبرمة "ببودابست" في 2001[(3)]، وجعل من وجود نظام المعالجة الآلية للمعطيات شرطا جوهريا للبحث عن مدى تحقق الاعتداء من عدمه.

وتجدر الإشارة إلى أنّ جريمة الاعتداء على نظام المعالجة الآلية للمعطيات تتحقق في صورتين:

تبرز الأولى في جريمتي الدخول والبقاء غير المرخص بهما في النظام (الفرع الأول)، وبينما تظهر الصورة الثانية في تلك النتائج غير المشروعة ضد معطيات النظام المترتبة عن فعل الدخول أو البقاء (الفرع الثاني).

الفرع الأول: الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات:

وذلك في شكل الدخول (أولا) أو البقاء (ثانيا) غير المرخص بهما.

أولاً- الدخول غير المرخص به:

تنص المادة 394 مكرر من قانون العقوبات الجزائري أنّه: «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 المعالجة الآلية للمعطيات أو يحاول ذلك».

يفهم من نص المادة أعلاه، أن الجزاء عن مثل هذه المخالفات يكون بمجرد تحقق الركن المادي للجريمة، والذي يكمن في فعل الدخول، وطبعا هنا يكون الدخول باستعمال الوسائل الفنية والتقنية للنظام المعلوماتي، وبغض النظر إن كان الدخول إلى النظام بأكمله أو إلى جزء منه فقط.

كما يفهم من البند نفسه أن المشرع لا يعاقب على الفعل الكامل، أي على الجريمة التامة، وإنّما يوقع العقاب حتى على مجرد المحاولة أي الشروع في الجريمة بغض النظر عن تحقيق النتيجة الإجرامية، وهو ما أدى بالبعض إلى الإقرار أن هذه الجرائم من قبيل الجرائم الشكلية، التي لا تشترط لقيامها تحقق النتيجة الإجرامية، والشرط الوحيد في البند هو أن يكون الدخول إلى نظام المعالجة الآلية للمعطيات عن طريق الغش، أي لن يكون مشروعا، كالدخول من دون وجه حق أو من دون ترخيص مسبق، بمعنى ألاّ يكون الدخول صدفة أو خطأ.

وتجدر الإشارة هنا، إلى أنّ المشرع الجزائري لم يشترط في البند أعلاه، طبيعة خاصة لهذا النظام، أي أنّ المادة 394 مكرر لم تشترط لتحقق جريمة الدخول غير المرخص به إلى نظام المعالجة أن يكون هذا

النظام محاطا بحماية فنية تمنع الاختراق، بل جاءت عامة ومطلقة وتحمي كل الأنظمة المعلوماتية، وبدون أي استثناء.

وبذلك يكون مشرعنا قد أصاب بشكل كبير في تنظيمه لهذه المسألة، حيث وبتمييز المشرع بين تجريم الدخول غير المرخص به إلى نظام معلوماتية محاط بحماية فنية وعدم التجريم للدخول غير المرخص به إلى نظام غير محاط بحماية فنية، سيؤدي حتما إلى فتح المجال للمجرمين من التهرب من المسؤولية الجزائية عن فعل الاعتداء، بحجة أن النظام المعتدى عليه غير محاط بحماية فنية، وبذلك، فيكون المشرع قد أحسن فعلا عندما لم يفصل بين النظام المحاط بالحماية الفنية، وذلك النظام غير المحاط بها.

ثانياً- البقاء غير المرخص به:

يقصد بالبقاء غير المرخص به هنا، الدخول إلى النظام والاستمرار في التواجد داخله وذلك دون إذن صاحبه، رغم علمه بأن بقاءه فيه غير مرخص[(4)].

ولقد سوّى المشرع الجزائري بموجب المادة 394 مكرر من قانون العقوبات السابق بين كل من جريمة الدخول غير المرخص به والبقاء غير المرخص به، وذلك على غرار ما اتخذه المشرع الفرنسي في منظومته الجزائية، وهو ما تأكد بتطبيق الجزاء نفسه على السلوكين وهي عقوبة الحبس من ثلاثة (03) أشهر إلى سنة، وغرامة مالية من 50.000 دج إلى 100.000 دج.

ويعتبر فعل البقاء مثله مثل فعل الدخول، بمثابة الركن المادي للجريمة، ونضيف هنا ونؤكد أن البقاء قد يحتمل صورتين مختلفتين هما:

- تتمثل الصورة الأولى، في حالة تحقق فعل البقاء غير المرخص به داخل نظام المعالجة الآلية للمعطيات منفصلا عن فعل الدخول ويكون الدخول إلى نظام المعالجة مشروعا، حتى وإن كان خطأ أو صدفة، غير انه وبتفطن الفاعل للوضع وبدلا من الانسحاب أو مغادرة النظام فورا، فإنّه يستمر في استغلال النظام، فهنا يعاقب على جريمة البقاء غير المرخص به.
- بينما تكمن الصورة الثانية، في حالة تحقق فعل البقاء غير المرخص به متصلا ومجتمعا مع فعل الدخول وهي حالة أكثر تشديدا من سابقتها كون فعل الدخول وفعل البقاء مجتمعين وينشآن بصفة غير مشروعة، كأن يتم الدخول دون ترخيص أو إذن سابق، ثم يستمر في البقاء داخله.

والإشكال الذي يمكن أن يثيره هذا الاجتماع والتداخل للسلوكين من دخول إلى النظام والبقاء فيه، هو تحديد النطاق الزمني[(5)] لكل واحدة منها، بمعنى متى تنتهي جريمة الدخول؟ ومتى تبدأ جريمة البقاء؟

ومن أجل الإجابة عن الإشكال، فلقد تضاربت آراء فقهية عن المسألة، إذ هناك من يرى بأن الجريمة المتعلقة بالبقاء داخل النظام تبدأ من اللحظة التي يتم فيها الدخول الفعلي للمجرم إلى النظام، وذلك بتجوّله وتنقله داخل هذا الأخير، وهنا تكون جريمة الدخول مكتملة، وهناك من يرى بأن جريمة

البقاء تكون في الوقت الذي يعلم فيه المتدخل بأن بقاءه في النظام غير مشروع، ولم ينسحب من النظام[6].

ومهما يكن من أمر، فإنّ المشرع الجزائري ومن خلال المادة 394 مكرر قد تطرق إلى الدخول ثمّ إلى البقاء، وكأن المشرع يُصنّف الأولى بجريمة وقتية كون فترة استمرارها قصيرا جدا والأخرى بجريمة مستمرة، مقارنة بالأولى.

الفرع الثاني: الصورة المشدّدة للاعتداء على نظام المعالجة الآلية للمعطيات

يشدد المشرع الجزائري من عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية، وذلك بموجب الفقرة الثانية من المادة 394 مكرر من قانون العقوبات، التي تنص أنّه: «...تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة بعقوبة الحبس من 6 أشهر إلى سنتين والغرامة من50.000 دج الى150.000دج».

تبعا لذلك، فإنّ المادة تُحدد ظرفين لتشديد عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية وهما:

- حالة الدخول أو البقاء مع محو أو تعديل في البيانات التي يحتويها النظام.
- ويتحقق الثاني عندما يترتب عن الدخول أو البقاء تخريب نظام اشتغال المنظومة وإعاقته عن أداء وظيفته.

وتجدر الإشارة هنا، إلى أن الصورة البسيطة للاعتداء على النظام المحددة في المادة 394 مكرر 01 السابقة لم تشترط البحث في النتيجة الإجرامية، بينما وباستقرار الفقرة 02 من المادة 394 مكرر يفهم أنّ النتيجة الإجرامية واجبة الإثبات، فيجب إثبات المحو أو التعديل أو التخريب للإقرار بالصورة المشددة للجريمة[7]، وإلا كنا بصدد الصورة الأولى والبسيطة لا أكثر.

ولقد أصاب المشرع مجددا في تشديده للعقاب هنا، والهدف – طبعا – هو الحدّ من تفاهم الإجرام المعلوماتي وما يرتبه من أضرار بالغة ووخيمة على الفرد والمجتمع والدولة ككل.

المطلب الثاني: تجريم الاعتداء على معطيات نظام المعالجة الآلية

يتحقق الاعتداء على معطيات النظام عند تجاوز مرحلتي الدخول والبقاء في نظام المعالجة، وقد يكون الاعتداء على المعطيات الداخلية للنظام (الفرع الأول)، أو في شكل الاعتداء على معطيات النظام الخارجي (الفرع الثاني).

الفرع الأول: الاعتداء على المعطيات الداخلية للنظام

تنص المادة 394 مكرر 1 من قانون العقوبات أنه: «يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبالغرامة من 500.000 دج وإلى 2000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال أو عدّل بطريقة الغش المعطيات التي يتضمنها».

ويقصد بالمعطيات محل جريمة الاعتداء بمفهوم هذه المادة، تلك المعلومات التي يحتويها النظام وتشكّل جزء منه، ويلاحظ من خلال المادة – دائما – أن المشرع قد حصر ضرر الاعتداء وهي:

- إما الإدخال وذلك بإضافة معطيات جديدة غير صحيحة الى تلك المعطيات الموجودة داخل النظام.

- إمّا المحو، وهي إزالة معطيات مسجلة أو تحطيمها.

- أو التعديل، أي تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى.

وتجدر الإشارة إلى أن توافر إحدى صور الاعتداء يكفي لتحقق الجريمة ويكفي لتحقق الجريمة ودون توافرها مجتمعة، واكتمال الركن المادي.

الفرع الثاني: الاعتداء على المعطيات الخارجية للنظام

تنص المادة 394 مكرر 02 أنه: «يعاقب بالحبس من شهرين إلى 3 سنوات، وبغرامة من 1.000.000 إلى 5000.000 دج كل من يقوم عمدا أو عن طريق الغش بما يلي:

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».

يستخلص من استقراء البند أعلاه أنّ المشرع الجزائري يعمل على تقرير حماية جنائية لكل المعطيات داخلية كانت أو خارجية.

ويقصد المشرع بالمعطيات المخزنة إمّا تلك المفرغة في دعامة مادية خارج النظام كالأقراص، أو تلك المخزنة داخل النظام ذاته كذاكرته أو قرصه الصلب.

ويقصد بالمعطيات المعالجة إمّا تلك التي أصبحت جزءا من النظام بعد أن تحولت إلى إشارات أو رموز تمثل المعطيات المعالجة، أو تلك المعطيات المرسلة عن طريق منظومة معلوماتية مثل تبادل إرسال المعلومات بين أجهزة المنظومة المعلوماتية، فالأولى تعتبر معطيات داخلية للنظام والأخرى معطيات خارجية للنظام[8].

عليه، فأي تلاعب بالمعطيات أعلاه، وبحسب المادة 394 مكرر 02 يعدّ جريمة اعتداء على المعطيات، وبالتالي يعاقب صاحبها طبقا للقانون.

الفرع الثالث: الاعتداء على سير نظام المعالجة الآلية

إنّ مثل هذا النوع من الاعتداء يخلو من أي تفصيل فيه في القانون، حيث أغفل المشرع الجزائري على النص على هذا الصنف من الاعتداء، إلاّ أنه لا يمكن أن نتجاهل أن التفحص في الأنواع السابقة للاعتداءات الواقعة على الأنظمة المعالجة للمعطيات أو على معطيات هذه الأنظمة (داخلية كانت أو خارجية) يؤدي حتما إلى استخلاص ذلك، واستخراج الاعتداءات التي تعرقل سير نظام المعالجة الآلية.

فبالرجوع مثلا إلى نص المادة 393 مكرر، التي نصت على الاعتداء على النظام بتخريبه، من شأنه أن يعيب عملية سير النظام المعلوماتي، ولاسيما باستعمال برامج القنابل المعلوماتية وبرامج الفيروسات.

ومهما يكن من أمر، فإنّ الأفعال الماسة بالسير الحسن لنظام المعالجة قد تتخذ عدة صور، ولاسيما منها أفعال التخريب، التعطيل والإفساد.

إلاّ أنه حبذا لو خصص المشرع الجزائري بندا خاصا ومستقلا لهذا النوع من الاعتداء الذي يقع على سير النظام، ولاسيما أن القاضي الجزائي يكتفي بالتفسير الضيق للنص، فحبذا لو رفع المشرع مثل هذا الحرج على مثل هذا القاضي، وذلك بالنص صراحة على النوع الأخير من الاعتداء وفي نص صريح.

في الأخير، نستخلص أن المشرع الجزائري، وفي إطار قانون العقوبات كقانون عام، قد جرّم الجريمة التامة ومجرد الشروع فيها[9]، وبغض النظر عن تحقق النتيجة الإجرامية من عدمها، كما جرّم أفعال وسلوكات كل من الفاعل والشريك على حدّ سواء، أي أنّ المشرع هنا طبق أحكام المساهمة الجنائية تطبيقا دقيقا، واعتبر الفاعل والشريك على قدم المساواة، والعقوبة المطبقة عليهما نفسها.

ولقد حدّد هذا القانون لمجموعة من العقوبات المقررة لمواجهة هذا الوجه الجديد من الإجرام، وهي إما/

- أصلية وتتمثل في الحبس والغرامات المالية،
- أو عقوبات تكميلية[10] وتكمن في مصادرة الأجهزة والوسائل المستعملة المستخدمة والبرامج.

كما كرّس المشرع وأقرّ بمسؤولية الشخص المعنوي المرتكب لإحدى الجرائم الإلكترونية، ورفع من الحد الأقصى للعقاب إلى 5 مرات عن ذلك السقف المحدد للغرامة المطبقة على الشخص الطبيعي،

كما تم الإقرار في المادة 394 مكرر 04 من قانون العقوبات بمسؤولية الأشخاص الطبيعيين بصفتهم فاعلين أصليين و/أو شركاء في الجريمة نفسها التي اقترفها الشخص المعنوي.

وتجدر الإشارة هنا، إلى أنه في سنة 2006، أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب القانون رقم 06-23[11]، حيث مسّ هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ولقد تمّ تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص الواردة في هذا القسم من القانون رقم 04- 15، ومن المؤكد أن التعديل هنا يعود إلى الوعي الحقيقي للمشرع بخطورة هذا النوع الجديد من الإجرام على جميع ميادين البلاد ولاسيما الاقتصادية منها.

وأكثر من ذلك، ونظرا لخصوصية هذه الجرائم فإنّ مشرعنا خصص لها مجموعة من الإجراءات ذات طبيعة مميزة، تنفرد بها هذه الجرائم مقارنة بتلك الجرائم التقليدية، وهي التي جاءت مفصلة في تعديل قانون الإجراءات الجزائية سنة 2006 بموجب القانون رقم 06-22[12] وتتعلق خصوصا بـ:

- تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الالكترونية طبقا للمادة 37 من قانون الإجراءات الجزائية.
- خصوصية التفتيش المنصب على المنظومة المعلوماتية عن ذلك التفتيش المتعارف عليه عملا بنص المادة 45 فقرة 07 من القانون رقم 06-22 السابق.
- تمديد آجال التوقيف للنظر لمقترف هذه الجرائم طبقا للمادة 51 فقرة 06 من القانون نفسه.

- كما نص على إجراءات خاصة للتحري والتحقيق ولاسيما استحداث أسلوب "اعتراض المراسلات والتقاط الصور وتسجيل الأصوات". طبقا للمواد من 65 مكرر 05 إلى 65 مكرر 10 من القانون رقم 06-22 سالف الذكر.

- وأضاف أيضا أسلوب "التسرب" في المواد من 65 مكرر 11 إلى 65 مكرر 18 من القانون نفسه، وهي أساليب يمارسها ضباط الشرطة القضائية وأعوانهم عند ضرورة التحري أو التحقيق في مجموعة من الجرائم وعددها سبعة، محددة على سبيل الحصر في المادة 65 مكر ر 05 من القانون رقم06 - 22، ومن بينها نجد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بعد إذن من وكيل الجمهورية أو قاضي التحقيق وبحسب الحالة.

- أما بشأن إجراءات المحاكمة والمتابعة فهي نفس الإجراءات المطبقة على الجرائم المألوفة والعادية.

المبحث الثاني

مواجهة الجرائم الإلكترونية في إطار القوانين الخاصة

تتطلب المواجهة الفعالة للجريمة الإلكترونية بمختلف تصنيفاتها إحاطتها بنصوص خاصة إلى جانب تلك القواعد العامة.

وباعتبار مجال الملكية الفكرية والأدبية حقل خصب لوقوع هذه الجرائم، فإنّ المشرع أحاطه بحماية جنائية وذلك من خلال تجريم كل اعتداء على حقوق المؤلف (المطلب الأول)، ولتعزيز جهوده في مكافحة الجريمة الإلكترونية سارع إلى سنّ القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (المطلب الثاني).

المطلب الأول: تقرير حماية جزائية لمعطيات الحاسب في قانون الملكية الفنية والأدبية

إنّ اهتمام المشرع بوضع قوانين الملكية الفكرية، كان بهدف حماية حق الإنسان في الإبداع والابتكار كعاملين جوهريين في تقدم المجتمعات، ولمّا كانت المكونات المنطقية للحاسب الآلي من برامجه وبياناته ثمرة لجهد فكري للإنسان، كان لزاما على المشرع إحاطة هذه المكونات بالحماية المقررة في قانون الملكية الفنية والأدبية، وذلك بتجريم الأفعال التي تشكّل اعتداء عليها (الفرع الأول)، وتكريس ما يقابلها من جزاءات جنائية (الفرع الثاني).

الفرع الأول: الاعتراف بوصف المصنف الفكري لمعطيات الحاسب الآلي

تم الاعتراف بهذا الوصف صراحة من خلال الأمر رقم 03-05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة(13)، بوصف المصنف المحمي لمصنفات الإعلام الآلي.

وأن أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج والبيانات يُشكل فعل من أفعال التقليد المنصوص عليها في المادة 151 من الأمر رقم 03-05 السابق، والتي تقرر العقوبات الجزائية المكرسة في المواد 153-156-157-158 من الأمر نفسه.

وتأخذ جنح التقليد الماسة بمصنف برامج وبيانات الحاسب الآلي ثلاثة صور وهي الجنح المرتبطة بالحق المعنوي للمؤلف(أولا) والجنح المتعلقة بالحق الأدبي للمؤلف(ثانيا) والجنح المرتبطة بالمصنف المقلد(ثالثا).

أولاً- الجنح المرتبطة بالحق المعنوي للمؤلف:

تحددها الفقرة 01 من المادة 151 من الأمر رقم 03-05 السابق، وتتمثل في:

أ- الكشف غير المشروع على المصنف الأدبي والفني، كأن يتم الكشف عن برنامج في الوقت أو بطريقة يرى المؤلف أنها غير مناسبة.

ب- المساس بسلامة المصنف الأدبي أو الفني، كأن يقوم شخص بتعديل أو تغيير أو حذف أو إضافة أو تحويل على البرنامج أو بيانات الحاسب دون إذن من المؤلف.

ثانياً- الجنح المرتبطة بالحق الأدبي للمؤلف:

وتتمثل في:

أ- الاستنساخ غير الشرعي للمصنف مثلما تنص المادة 151 فقرة 01 من الأمر رقم 03-05، وفيها يقوم مثلا شخص باستنساخ برنامج أو بيانات الحاسب بأي أسلوب كان وجعله في شكل نسخ مقلّدة دون إذن المؤلف.

ب- الإبلاغ غير الشرعي للمصنف مثلما تنص عليه المادة 152 من الأمر رقم 03-05، كأن يقوم شخص بإبلاغ وإعلام عموم الجمهور بمصنف برنامج وبيانات الحاسب دون علم وترخيص من المؤلف سواء كان الإبلاغ مباشر أو غير مباشر.

ثالثاً- الجنح المرتبطة بالمصنف المقلد:

وتتعلق هذه الجنح بالتصرفات والتعاملات التي ترد على المصنف المقلّد الذي يمكن أن يكون برنامج أو بيانات الحاسب الآلي وهي كالتالي[(14)]:

- استيراد أو تصدير نسخ مقلدة من المصنف، بيع نسخ مزورة من المصنف، تأجير مصنف مقلد أو عرضه للتداول، الرفض عمدا في دفع المكافأة المستحقة بمقتضى الحقوق المقررة للمؤلف.

وتجدر الإشارة هنا إلى ما صرّحت به المادة 154 من الأمر رقم 03-05 بنصّها على أنه: « يُعدّ مرتكبا للجنحة المنصوص عليها في المادة 151 من هذا الأمر، ويستوجب العقوبة المقررة في المادة 153، كل من شارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة»، ومنها يفهم أن المشرع جرّم الاشتراك بالفعل أو بالوسائل في جرائم التقليد الواقعة على مصنف برامج وقواعد بيانات الحاسب الآلي، وجعل العقوبة عليه هي نفسها تلك المقررة للفاعل الأصلي.

الفرع الثاني: العقوبات المقررة لجنح تقليد معطيات الحاسب الآلي

تكمن هذه العقوبات في تلك الأصلية (أولا)، وتلك التكميلية (ثانيا) على التوالي:

أولاً- العقوبات الأصلية:

لقد حددتها المادة 153 من الأمر رقم 03-05 وهي:

أ- **عقوبة الحبس:** من 6 أشهر إلى 03 سنوات على كل من ارتكب جنحة تقليد مصنف بما فيه المصنفات المعلوماتية.

ب- **عقوبة الغرامة:** علاوة على الحبس، يمكن للقاضي أن يحكم بغرامة مالية تتراوح بين 500.000 دج و1000.000 دج.

ثانياً- العقوبات التكميلية: حيث يمكن للقاضي أن ينطق بواحدة أو أكثر من العقوبات التكميلية المقررة لجنح تقليد المصنفات التالية:

1- مصادرة المبالغ المساوية لأقساط الإيرادات المحصلة من الاستغلال غير المشروع للمصنف طبقا للمادة 157 من القانون السابق،

2- مصادرة وإتلاف كل عتاد أنشأ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة وفقا للمادة 157 فقرة 02 من القانون السابق،

3- الأمر بطلب من المتضرر بتعليق ونشر أحكام الإدانة على نفقة المحكوم عليه عملا بالمادة 158 من القانون السابق،

4- الأمر بتسليم العتاد والنسخ المقلدة أو قيمة ذلك، وكذلك الإيرادات موضوع المصادرة للمؤلف أو أي مالك حقوق أخرى.

لتكون عند الحاجة بمثابة تعويض وفقا للمادة 159 من قانون العقوبات - دائما -.

وأكثر من ذلك كلّه، فإنّ المشرع خوّل للقاضي الجزائي أن يضاعف ويشدد العقوبات الأصلية في حالة توافر ظرف العود، وأن يأمر بغلق المؤسسة التي يستغلها المقلّد أو شريكه لمدة لا تتجاوز ستة أشهر، ويأمر بالغلق النهائي إذا اقتضى الأمر[(15)]، وكلّ ذلك طبقا للقانون.

المطلب الثاني: مكانة القانون رقم 09-04 في الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

يتميز القانون رقم 09-04 السابق الإشارة إليه بأنه القانون الأكثر ملائمة مع الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت.

حيث أتى بتدابير متنوعة بعضها وقائي (الفرع الأول)، وبعضها تدابير إجرائية (الفرع الثاني).

الفرع الأول: التدابير الوقائية

تكمن التدابير الوقائية في مضمون المادة 04 من القانون رقم 09-04 التي حدّدت الحالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات الإلكترونية، وهي أربع حالات:

- الوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب وجرائم ضد أمن الدولة.
- عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام.

- لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

- في إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

الفرع الثاني: التدابير الإجرائية

أضاف المشرع إلى جانب تلك التدابير الوقائية الواردة في القانون الخاص رقم 09-04 إجراءات جديدة تدعم تلك المنصوص عليها في قانون الإجراءات الجزائية، ولاسيما تلك المتعلقة بمكافحة الجريمة الإلكترونية، ويمكن تلخيص هذه الإجراءات في:

- جواز التفتيش ولو عن بعد للمنظومة المعلوماتية أو لجزء منها من طرف الجهات القضائية المختصة وضباط الشرطة القضائية،

- إمكانية تمديد آجال التفتيش بإذن من السلطة المختصة،

- إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، وذلك طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل، طبقا للمادة 05 من القانون رقم 09-04 السابق.

- السماح للسلطات الجزائرية المختصة باللجوء إلى التعاون المتبادل مع السلطات الأجنبية في مجال التحقيق وجمع الأدلة للكشف عن الجرائم المتصلة بتكنولوجية الإعلام والاتصال عبر الوطنية ومرتكبيها، وذلك عن طريق تبادل المعلومات أو اتخاذ تدابير احترازية في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل[16].

تجدر الإشارة أنه أنشئت بموجب القانون رقم 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها هيئة تعرف في صلب القانون بـ : "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال".

اهتمت هذه الهيئة بمهام متعددة، أهمها:

- تفعيل التعاون القضائي والأمني والدولي وإدارة وتنسيق العمليات الوقائية،

- والمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

كما لا يفوتنا الإشارة، إلى أن تعداد هاذين القانونين الخاصين، اللذين تم تحليلهما أعلاه لم يكن أبدا على سبيل الحصر، وإنما على سبيل المثال فقط، وذلك لوجود قوانين خاصة أخرى ربما اسبق في الصدور من هذه الأخيرة.

ونخص بالذكر هنا، قانون البريد والاتصالات السلكية واللاسلكية رقم 2000-03 المؤرخ في05 جويلية 2000[17]، حيث أتت المادة 127 منه، بجزاء لكل من تسول له نفسه وبحكم مهنته، أن يفتح أو

يحول أو يخرب البريد أو ينتهكه، ويعاقب الجاني بالحرمان من كافة الوظائف والخدمات العمومية من 05 الى10 سنوات.

كما تطرق إلى ذلك من خلال قانون التأمينات وبالضبط في المادة 6 مكرر01 والمادة 65 مكرر01 من القانون رقم 08-01، المؤرخ 23 جانفي 2008[18] المعدل والمتمم والمتعلق بالتأمينات كقانون خاص آخر، حيث يتضمن الجريمة الالكترونية من خلال هيئات الضمان الاجتماعي في نصوص قانونية عديدة، تخص البطاقة الالكترونية التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج، وهي صالحة في كل التراب الوطني، وكذلك الجزاءات المقررة في حالة الاستعمال غير المشروع، أو حالة ما يقوم الشخص عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا.

خاتمة:

يستخلص في الأخير، أن الجريمة الإلكترونية حقا جريمة مستحدثة تتمتع بطبيعة قانونية مغايرة ومختلفة تماما عن الجريمة التقليدية، مما جعل القواعد القانونية والإجراءات التقليدية قاصرة وعاجزة عن مكافحة هذا الوجه الجديد من الإجرام، وهو ما أدّى إلى اجتهاد المشرع الجزائري في سبيل التصدي لها، وذلك بتبنيه لسياسة مزدوجة في التصدي للإجرام المستحدث، وبتعديله للقانون العام (قانوني العقوبات والإجراءات الجزائية) من جهة، وإدراجه لنصوص قانونية خاصة كثيرة تُجرّم بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات، ولاسيما القانون رقم 09-04 من جهة أخرى.

ولعل هذا التنوع سيساهم بطريقة أو بأخرى في الحد من الجرائم الإلكترونية أو – على الأقل – التقليل من حدّتها، ولاسيما أن هذه الجرائم تمس بحقوق مكرّسة صراحة في الدستور الذي يعد من أسمى القوانين، وبالضبط في المادة 38 التي تنص انه على أن القانون يحمي حقوق المؤلف، وكذا المادة 39 التي تنص انه لا يجوز انتهاك حرمة الحياة الخاصة.

ومهما يكن من أمر، فلا يخفى عن أحد ما لهذه الجريمة من خطورة، و- هي وللأسف – تتفاقم يوما بعد يوم، وتزداد بشكل سريع ومدهش، مما يؤدي إلى تكييف سبل المكافحة بالقصور وعدم النجاعة.

عليه يمكن تقديم بعض التوصيات والاقتراحات، التي قد يكون تطبيقها مجدي لمكافحة هذه الجرائم الخطيرة ومن ثمة تحقيق التنظيم القانوني الفعال لها:

1- تخصيص قانون خاص ومستقل للجريمة الالكترونية.

2- عقد الدورات التدريبية التي تعتني بمكافحة الجريمة الإلكترونية.

3- ضرورة تأهيل أفراد الضبطية القضائية وكذا النيابة العامة على كيفية التعامل مع هذا النوع من الجرائم.

4- سن إجراءات خاصة لهذا الصنف من الجرائم ليتميز عن الإجرام الكلاسيكي وذلك باستحداث إجراءات محاكمة من نوع خاص- مثلا-.

5- توعية المجتمع وخلق عندهم ثقافة اجتماعية جديدة تبعدهم عن ممارسة تلك الأعمال غير المشروعة.

6- ضرورة التعاون الدولي لمكافحة هذه الجرائم، وذلك من خلال التعامل مع التقنيين وأصحاب الخبرة في هذا المجال.

الهوامش:

(1) قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يتضمن قانون العقوبات، جريدة رسمية عدد 71، لسنة 2004، معدل ومتمم. وذلك من خلال المواد من 394 مكرر إلى 394 مكرر 07، المضافة بموجب القانون نفسه.

(2) عملا بالفقرة الثانية من المادة 02 من القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجية الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47، صادر بتاريخ 07 أوت 2009.

(3) Article 01 a « Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure dans un ou plusieurs élément assurent, en exécution d'un programme, un traitement automatisé de données ».
In www.eastlaw.blogspot.com/2003/03/23-11-2001/htm.

(4) قارة أمال، الجريمة المعلوماتية، مقال مقدم في ملتقى وطني، كلية الحقوق، جامعة الجزائر، 2001، ص 44 (غير منشور).

(5) لما للمسألة من أهمية في تحديد مدة تقادم كل جريمة، وتحديد الاختصاص فيها.

(6) أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2004، ص 28.

(7) خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، 2010، ص 123.

(8) فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي، ملتقى منعقد بليبيا، أكتوبر 2009، ص31.

(9) عملا بالمادتين 394 مكرر 05 و394 مكرر 07 من قانون العقوبات، مرجع سابق.

(10) طبقا للمادة 394 مكرر 6 من القانون نفسه.

(11) قانون رقم 06-23 مؤرخ في 20 ديسمبر 2006، يتضمن قانون العقوبات، جريدة رسمية، عدد 84، صادر بتاريخ 20 ديسمبر 2006، معدل ومتمم.

(12) قانون رقم 06-22 مؤرخ في 20 ديسمبر 2006، يتضمن قانون الإجراءات الجزائية، جريدة رسمية، عدد 84، صادر بتاريخ 20 ديسمبر 2006، معدل ومتمم.

(13) أمر رقم 03-05 مؤرخ في 19 جويلية 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، جريدة رسمية عدد 44، صادر بتاريخ 23 جويلية 2003

(14) وهي جنح مذكورة في المادة 151/3 و4 و5، وكذا في المادة 155 من الأمر رقم 03-05، مرجع سابق.

(15) طبقا للمادة 156 من الأمر رقم 03-05، مرجع سابق.

(16) عملا بالمادتين 16 و17 من القانون رقم 09-04، مرجع سابق.

(17) قانون رقم 2000-03 مؤرخ في 05 جويلية 2000،يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية جريدة رسمية، عدد48 صادر بتاريخ 07 جويلية2000.

(18) قانون رقم 08-01 مؤرخ في 23 جانفي 2008 يتعلق بالتأمينات جريدة رسمية عدد 04 بتاريخ 25 جانفي 2008.

حول مكافحة الجريمة الالكترونية في التشريع الجزائري ـــــــ