# مكافحة الجرائم الالكترونية في التشريع الجزائري

**برا هيمي جمـــــال، أستاذ مساعد "أ"**

كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو

## مقدمـــة:

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الالكتروني و ما يصاحبها من أضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة، و محاولة منه تدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عمد منذ الألفية الثانية الى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجية الإعلام و الاتصال. و قام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الالكترونية. و مع هذا فيبقى السؤال مطروح حول مدى فعلية و فعالية هذه القوانين في مواجهة الجرائم الالكترونية ؟ وهو الأمر الذي سنحاول الإجابة عليه في هذا البحث من خلال مبحثين، خصصنا الأول لإبراز آليات مكافحة الجرائم الالكترونية في إطار القواعد العامة، و الثاني لإظهار آليات مكافحة هذه الجرائم في أطار النصوص الخاصة.

**المبحث الاول: آليات مكافحة الجرائم الالكترونية في إطار القواعد العامة**

حاول المشرع الجزائري خلال السنوات الأخيرة تدارك الفراغ القانوني الذي عرفه مجال الإجرام الالكتروني فقام بتعديل قانون العقوبات بموجب قانون رقم 04-

15[1] مستحدثا فيه جملة من النصوص جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات، و حدد لكل فعل منها ما يقابله من الجزاء(مطلب 01) . و الى جانب ذلك قام بسن قواعد اجرئية جديدة تتعلق بالتحقيق تتماش مع الطبيعة المميزة للجرائم الالكترونية و ذلك من خلال تعديل قانون الاجراءات الجزائية بموجب قانون رقم06-22.[2] ( مطلب 02)

**المطلب الأول: القواعد الموضوعية المقرر في قانون العقوبات لمكافحة الجرائم الالكترونية**

ركزت إستراتيجية المشرع الجزائري في التصدي لظاهرة الإجرام ألمعلوماتي على سن في القسم السابع مكرر من قانون العقوبات رقم 04-15 تحت عنوان " المساس بانظمة المعالجة الالية للمعطيات" جملة من قواعد قانونية موضوعية حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات و ما يقابلها من جزاء او عقوبة، و تأخذ هذه الأفعال إما وصف الاعتداء على نظام المعالجة الالية ( الفرع 01) أو وصف الاعتداء على معطيات نظام المعالجة الالية (الفرع 02). كما يمكن لها ان تاخذ وصف الاعتداء على سير نظام المعالجة الالية( الفرع 03)

**الفرع الأول: تجريم الاعتداء علي نظام المعالجة الآلية للمعطيات**

[1]- قانون رقم 04-15 مؤرخ في 2004/11/10 يعدل و يتمم الامر رقم 66-156، يتضمن قانون العقوبات، جريدة رسمية عدد 71، صادر بتاريخ 2004/11/10، معدل و متمم.

[2]- قانون رقم 06-22 مؤرخ في 2006/12/20، يعدل و يتمم الامر رقم 66-155، يتضمن قانون الإجراءات الجزائية، جريدة رسمية عدد 84، صادر بتاريخ 2006/12/24.

عرّف المشرع الجزائري نظام المعالجة الالية للمعطيات بانه " كل نظام أو مجموعة من الأنظمة منفصلة كانت أم متصلة بعضها البعض أو المرتبطة والتي يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"[1]، وهو نفس التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي المبرمة ببودابست في 2001 [2]. و جعل من وجود نظام المعالجة الآلية شرطا أساسيا للبحث عن مدى تحقق الاعتداء أم لا.

فجريمة الاعتداء على نظام المعالجة الآلية للمعطيات تتحقق في صورتين هما:

**-أولا: الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات:**

تتضمن جريمتي الدخول و البقاء غير المرخص بهما في النظام .

**1-الدخول غير المرخص (l'intrusion):** يقصد بفعل الدخول هنا وهو الركن المادي لجريمة الاعتداء على نظام المعالجة الآلية للمعطيات، ذلك الدخول المعنوي أو الالكتروني باستعمال الوسائل الفنية و التقنية الى النظام ألمعلوماتي. و لا يعد فعل الدخول بحد ذاته سلوكا غير مشروع و انما يتخذ وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو دون ترخيص[3]، و

---

2 -أنظر المادة 2/02 من القانون رقم 04/09 المؤرخ في 14 شعبان 1430 الموافق ل 05 غشت سنة 2009 ، يتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجية الإعلام و الاتصال و مكافحتها، جريدة رسمية عدد 47، صادر بتاريخ 2009/08/16.

[2] -Article 01 a stipule : « système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou 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.

[3] -أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، طبعة ثانية ، دار هومة للطباعة و النشر و التوزيع، الجزائر، 2007، ص 102

هو ما يستشف من المادة 394 مكرر من قانون العقوبات الجزائري التي تنص على " **يعاقب بالحبس من ثلاثة اشهر الى سنة و بغرامة من 50000دج الى 100000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك**"[1].

يلاحظ من خلال هذه المادة ان المشرع الجزائري اعتبر جريمة الدخول غير المرخص به بمثابة جريمة شكلية التي لا يشترط لقيام الركن المادي فيها تحقق النتيجة الإجرامية، أي انه جرّم مجرد الدخول الى نظام المعالجة الآلية للمعطيات باكمله أو الى جزء منه فقط ، بشرط ان يكون فعل الدخول بدون ترخيص مقصودا و ليس صدفة او خطا .

كما لا تشترط المادة 394 مكرر لتحقق جريمة الدخول غير المرخص به إلى نظام المعالجة أن يكون هذا النظام محاطا بحماية فنية تمنع الاختراق كالتشفير مثلا ، بل جاءت عامة و مطلقة، أي تحمي كل الأنظمة المعلوماتية من الاعتداء سواء كانت محمية فنيا ام لا[2]. وهو ما أكده مرة أخرى المشرع الجزائري في الفقرة "ب" من المادة الثانية (م 2–ب) من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال ومكافحتها. مثمنا بذلك ما نصت عليه الاتفاقية الدولية للإجرام المعلوماتي في المادة الأولي[3]، وكرّسه كذالك القضاء الجزائري من خلال عدة أحكام قضائية[1].

---

[1]– انظر نص المادة 394 مكرر من القانون رقم 15/04، مرجع سابق.

[2] TOUIDJINI Med Kamel Addine « la repense légale et judiciaire a la cybercriminalité » CERIST, Alger ; 2012, p 14.

[3]– أنظر نص المادة في : www.eastlaw.blogspot.com/2003/03/23-11-2001/html

نعتقد ان المشرع الجزائري قد أصاب كثيرا عندما جرم مجرد الدخول إلى نظام المعالجة الآلية للمعطيات عن طريق الغش أي بدون ترخيص و بغض النطر عن ما إذا كان النظام المتعدى عليه محاطا بحماية فنية أم لا، لانه بذلك يكون قد جعل من هذا التدبير بمثابة تدبير تحفظي وقائي سيساهم بشكل كبير في التصدي لظاهرة الإجرام المعلوماتي ، من خلال غلق الباب أمام المجرمين من التهرب من المسؤولية الجزائية عن فعل الاعتداء ، بحجة أن النظام المعتدي عليه لم يكن محاطا بحماية فنية. و في تفادي ارتكاب جرائم أكثرة شدة على نظام المعالجة و معطياته كإتلاف النظام أو محو و تعديل معطيات النظام.[2]

2- **البقاء غير المرخص le maintien frauduleux:**

يقصد بالبقاء غير المرخص به في نظام المعالجة الالية للمعطيات استمرارية التواجد داخل نظام المعالجة دون اذن من صاحبه أو من له السيطرة عليه. بمعني أخر هو بقاء شخص داخل نظام المعالجة ملك الغير بعد الدخول إليه

[1]- يظهر من خلال حكم محكمة الجنح لولاية باتنة المؤيد بقرار مجلس قضاء باتنة ، القاضي بإدانة متهم بجنحة الدخول غير المشروع إلى نظام معلوماتي تابع لمنظمة أمريكية تعرف ب sagonet Works، دون أن يشير في التسبيب إذا كان هذا النظام محمي ام لا. راجع القرار الصادر عن الغرفة الجزائية لمجلس قضاء باتنة بتاريخ 2010/07/04 تحت رقم 10/05805.

[2]-هذا ما أخذ به المشرع الفرنسي من خلال نص المادة 1/323 من قانون العقوبات الفرنسي، و حذا جذوه المشرع الانجليزي في نص المادة الأولى من قانون إساءة استخدام الكمبيوتر لعام 1990. انظر: فايز محمد راجع غلاب، الجرائم المعلوماتية في القانون الجزائري و اليمني، رسالة دكتوراه في القانون، جامعة الجزائر، 2011، ص 186.

خطأ أو صدفة، رغم علمه بأن بقاءه فيه غير مرخص[1].

اعتبر المشرع الجزائري على غرار المشرع الفرنسي فعل البقاء غير المرخص به في نظام المعالجة الالية للمعطيات جريمة مثلها مثل جريمة الدخول الغير المرخص به و ذلك بموجب المادة 394 مكرر من قانون العقوبات و حدد لهاتين الجريمتين نفس العقوبة و هي الحبس من 03 أشهر الى سنة و غرامة مالية من 50000دج الى 100000دج.

تتحقق جريمة البقاء غير المرخص به حسب المادة 394 مكرر السالفة الذكر بتحقق ركنها المادي المتمثل في فعل البقاء دون وجه حق داخل نظام مملوك للغير، و بغض النظر اذا كان هذا البقاء مقصودا من طرف الجاني ام غير مقصود، وهذا الركن المادي يمكن أن يظهر في صورتين هما :

-الصورة الأولى: تتمثل في تحقق فعل البقاء غير المرخص به داخل نظام المعالجة الالية للمعطيات منفصلا عن فعل الدخول، و يتجسد هذا عندما يكون فعل الدخول الى نظام المعالجة مشروعا، كأن يدخل الشخص صدفة او خطا الى نظام ما أي دون قصد ففي هذه الحالة يتعين على المتدخل أن ينسحب ويغادر فورا النظام، أما إذا بقي رغم ذلك فانه يعاقب على جريمة البقاء غير المرخص به.

-الصورة الثانية:تتمثل في تحقق فعل البقاء غير المرخص به مجتمعا مع فعل الدخول، و يتجسد هذا الوضع حينما يكون الدخول غير مشروعا ، كأن يدخل

[1]-أمال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق بجامعة الجزائر، 2001، ص 44.

الجاني نظام ما دون إذن مسبق من صاحب هذا الأخير، ثم يستمر في البقاء داخله، وهنا يتحقق الاجتماع و التداخل المادي بين الجريمتين. [1]

يمكن لهذا التداخل المادي بين جريمتي الدخول إلى و البقاء في نظام المعالجة الآلية للمعطيات بدون ترخيص، أن يثير إشكالا قانونيا حول تحديد الحد الفاصل بين الجريمتين، أو النطاق الزماني لكل واحدة منها ، بمعنى تحديد الوقت الذي تنتهي فيه جريمة الدخول و تبدأ فيه جريمة البقاء.

لقد استقر الفقه الجنائي فيما يخص هذه المسألة على أن بداية سريان جريمة البقاء داخل النظام يكون منذ اللحظة التي يبدأ فيها الجاني التجول و التنقل داخل النظام، أما قبل هذه اللحظة فنكون أمام جريمة الدخول غير المرخص به حتى وان دخل الجاني النظام وبقي فيه ساكنا فترة طويلة من الزمن[2].

إن التفرقة بين الجريمتين المذكورتين من خلال إبراز النطاق الزماني لكل واحدة منهما لها أهمية كبيرة في حساب مدة تقادم كل جريمة و تحديد الاختصاص فيها، خاصة إذا علمنا بان جريمة الدخول إلى النظام هي جريمة

[1]– أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص 110.

[2]–تضاربت أراء الفقهاء في هذه المسالة بين من يري بأن جريمة البقاء داخل نظام المعالجة تبدأ منذ اللحظة التي يتم فيها الدخول الفعلي للمجر إلى النظام و تكتمل فيها جريمة الدخول ، ومن يري بأن بداية جريمة البقاء تكون في الوقت الذي يعلم فيه المتدخل بأن بقاءه داخل النظام غير مشروع ، و ذهب الرأي الثالث الى أن جريمة البقاء تبدأ منذ اللحظة التي يعلم فيها المتدخل بان تواجده في النظام غير مشروع أو أصبح غير مشروع و لم ينسحب من النظام . أنظر : جميل عبد الباقي الصغير" جرائم الكمبيوتر و الجرائم الأخرى في مجال المعلومات" بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، الفترة الممتدة من 25–27 أكتوبر 1993 ، ص 28.

وقتية لان فترة استمرارها قصيرة جدا، في حين أن جريمة البقاء داخل النظام هي جريمة مستمرة. و اعتقد أن هذا ما أراد المشرع الجزائري تحقيقه من خلال نص المادة 394مكرر عندما تطرق أولا للدخول ثم للبقاء .

تجدر الإشارة في الأخير إلى أن المشرع الجزائري اعتبر جريمة البقاء غير المرخص به داخل نظام المعالجة الآلية للمعطيات من الجرائم الشكلية التي لا يستوجب وقوعها تحقق نتيجة إجرامية معينة، فيكفي تحقق فعل البقاء الذي يعتبر الركن المادي للجريمة لنسلّم بوقوع جريمة البقاء تامة و بأركانها.

**ثانيا: الصورة المشددة للاعتداء على نظام المعالجة الآلية للمعطيات:** تتحقق عندما يترتب عن فعل الدخول أو البقاء نتائج غير مشروعة ضد معطيات النظام،و قد نصت المادة 394مكرر في فقرتها الثانية على"....**تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة العقوبة الحبس من 6 أشهر إلى سنتين و الغرامة من 50000دج إلى 150000دج**".

نلاحظ من خلال نص هذه المادة بان المشرع الجزائري أورد ظرفين لتشديد عقوبة الدخول و البقاء بدون ترخيص في نظام المعالجة الآلية ، بحيث يتحقق الظرف الأول إذا نتج عن الدخول أو البقاء محو أو تعديل في البيانات التي يحتويها النظام. و يتحقق الثاني حينما يترتب عن الدخول أو البقاء تخريب نظام اشتغال المنظومة و إعاقته عن أداء وظيفته.

ولكي تتوفر الظروف المشددة المذكورة في المادة 394 مكرر فقرة 2 لا بدمن إثبات وجود علاقة سببية بين فعل الدخول أو البقاء غير المرخص به والنتيجة

الإجرامية التي حددتها المادة في محو او تعديل بيانات النظام أو تخريب تشغيل النظام ذاته، و إلا كنا بصدد جريمة في صورتها البسيطة المذكورة في نص المادة 394مكرر 1 من قانون العقوبات.

تجدر الإشارة إلى أن هذه النتيجة ذاتها هي التي اعتبرها المشرع الجزائري ظرفا مشددا في الجريمة[1] ، أي أنه يكفي أن يترتب عن جريمة الدخول أو البقاء محوا أو تعديلا في بيانات النظام أو تخريب تشغيل هذا النظام كي يتحقق الظرف المشدد و لا يهم أن يكون تحقيقها(أي هذه النتيجة) مقصودا من طرف الجاني أو غير مقصودة.[2]

فمتى تحققت أركان جريمة الدخول أو البقاء في نظام المعالجة الالية للمعطيات في صورتها المشددة عوقب الجاني بالحبس من 6 أشهر الى سنتين وبالغرامة من 50000دج إلى 150000دج. ولعل الغاية من هذا التشديد هو الحدّ من تفاقم الإجرام ألمعلوماتي و ما يصاحبه من أضرار بالغة و تحقيق الائتمان في المعاملات الالكترونية.

**الفرع الثاني: تجريم الاعتداء على معطيات نظام المعالجة الآلية**

يقصد بالاعتداء هنا ذالك الاعتداء الذي يهدف الى الإضرار بمعلومات الكمبيوتر أو وظائفه سواء بالمساس بسريتها أو المساس بسلامتها محتوياتها، تكاملها أو بتعطيل قدرة و كفاءة الأنظمة بشكل يمنعها من أداء وظيفتها بشكل

[1]–خثير مسعود " الحماية الجنائية لبرامج الكمبيوتر أساليب و ثغرات، دار الهدى، عين مليلة، الجزائر، 2010، ص123.

[2]– انظر نص الفقرة الثانية من المادة 394 مكرر من القانون رقم 04–15، مرجع سابق.

سليم. يتحقق الاعتداء على معطيات النظام عادة بعد تجاوز مرحلة الدخول والبقاء في نظام المعالجة، ويتخذ احد الشكلين التاليين :

-**الشكل الأول :الاعتداء على المعطيات الداخلية للنظام:** لقد جرّم المشرع الجزائري أي اعتداء يقع على المعطيات الموجودة داخل نظام المعالجة الآلية من خلال المادة 394مكرر 1 قانون العقوبات التي تنص على "**يعاقب بالحبس من 6 أشهر إلى 3 سنوات و بالغرامة من 500000دج إلى 2000000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها**".

يقصد بالمعطيات محل جريمة الاعتداء بمفهوم هذه المادة، تلك المعطيات والمعلومات التي يحتويها النظام و تشكل جزء منه و التي تمت معالجتها آليا وأصبحت عبارة عن رموز وإشارات تمثل تلك المعلومات، و ليس المعلومات ذاتها باعتبارها أحد عناصر المعرفة.[1]

يلاحظ من خلال أحكام المادة المذكورة أن المشرع حدد صور الاعتداء على معطيات النظام الداخلية على سبيل الحصر و لم يدع أي مجال للاجتهاد فيها، مما يدل على أن أي اعتداء لا يحمل إحدى هذه الصور: الإدخال أو المحو أو التعديل. فهو مستبعد و لا يخضع لأحكام المادة 394مكرر 1.

**فأما الإدخال:** يقصد به إضافة معطيات جديدة غير صحيحة إلى المعطيات الموجودة داخل النظام و التي تمت معالجتها أليا.

[1] Bouder Hadjira « protection des systèmes d'informations : aspects juridiques » centre de recherche sur l'information scientifique et technique, Alger, 2012, p 32.

**وأما المحو**: يعني إزالة من معطيات مسجلة على دعامة موجودة داخل نظام المعالجة الآلية أو تحطيم تلك الدعامة أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة.

**أما التعديل** :يعني تغيير المعطيات الموجودة داخل نظام المعالجة واستبدالها بمعطيات أخرى[1].

تجدر الإشارة إلى ان المادة المذكورة لا تشترط اجتماع هذه الصور الثلاثة، بل يكفي أن يصدر عن الجاني احداها لكي يكتمل الركن المادي لجريمة الاعتداء على معطيات نظام المعالجة. و هو ما ذهب إليه المشرع الفرنسي في نص المادة 323 من قانون العقوبات.[2]

يرجع سبب تجريم المشرع الجزائري للأفعال المذكورة أعلاه بنص مستقل عن جريمتي الدخول و البقاء غير المرخص بهما في نظام المعالجة، و اللتان تمثلان الطريق العادي للوصول إلى المعطيات الموجودة داخل النظام و ارتكاب جريمة محو أو إدخال أو تعديل ضدها، الى وجود طرق أخرى لاقتراف هذه الأفعال عن بعد أي دون الدخول او البقاء في النظام، كاستخدام مثلا القنابل المعلوماتية الخاصة بالمعطيات أو برامج الفيروسات[3]. وأعتقد أن المشرع

---

[1]– انظر: فايز محمد راجح غلاب، مرجع سابق، ص 212 و ما يليها.

[2] -Art 323/2 stipule « le fait d'introduire frauduleusement des données dans un système de traitement automatise ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement » .

[3]–نذكر على سبيل المثال: **برنامج ZAxoon** يظهر في بداية تشغيله كأحد ألعاب التسلية ثم يقوم بعد ذلك بمحو بيانات و معطيات النظام. **برنامج Filer** يبدو في ظاهره كما لو أنه ينظم بيانات

أصاب في ذلك لأنه بوضعه نص المادة 394مكرر 1 يكون قد جرم أفعال المحو والإدخال و التعديل الواقع على معطيات النظام مهما كانت الوسيلة المستعملة والطريقة المتبعة لتحقيق ذلك.

-**الشكل الثاني: الاعتداء على المعطيات الخارجية للنظام:** يقصد بالمعطيات الخارجية لنظام المعالجة تلك المعطيات التي لها دور في تحقيق نتيجة معينة تمثل في المعالجة الالية للمعطيات، وقد نص عليها المشرع الجزائري في المادة 394 مكرر 2 من قانون العقوبات على النحو التالي:"**يعاقب بالحبس من شهرين الى 3سنوات و بغرامة من 1000000دج الى 5000000دج كل من يقوم عمدا أو عن طريق الغش بـ:**

**1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها الجرائم المنصوص عليهافي هذا القسم.**

**2-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم".**[1]

يتبين لنا من نص هذه المادة أنها جاءت عامة و مطلقة، فهي تقرر الحماية الجنائية لكل من المعطيات الداخلية و الخارجية للنظام معا.

---

الملفات و لكن في الحقيقة يقوم بمحوها، **برنامج الدودة** و هي من أخطر البرامج الفيروسية دورها التخريب الفعلي للملفات و البرامج و نظم التشغيل و **حصان طروادة** الذي يرتكز دوره في تعديل غير محسوس في المعطيات و البرامج. أنظر: سناء شوقي ابراهيم "فيروس الحاسب الآلي" مجلة الإدارة، العدد 01، سنة 1994،ص 126 و ما يليها.

[1]- انظر نص المادة 394 مكرر 2 من القانون رقم 04-15، مرجع سابق.

فيقصد المشرع بالمعطيات المخزنة إما تلك المفرغة في دعامة مادية خارج النظام كالأقراص أو تلك المخزنة داخل النظام ذاته كذاكرته أو قرصه الصلب[1].

ويقصد بالمعطيات المعالجة إما تلك التي أصبحت جزءا من النظام بعد أن تحولت إلى إشارات أو رموز تمثل المعطيات المعالجة و إما تلك المعطيات المرسلة عن طريق منظومة معلوماتية مثل تبادل إرسال المعلومات بين أجهزة المنظومة المعلوماتية. فالاولى تعتبر معطيات داخلية للنظام و الثانية هي معطيات النظام الخارجية.[2]

وعليه فأي تلاعب بالمعطيات المذكورة أعلاه، و استعمالها عمدا او عن طريق الغش بإحدى الطرق المحددة في المادة 394مكرر 2 (أي تصميمهاأو بحثها أو تجميعها أو توفيرها أو نشرها أو الاتجار بهاأو حيازتها أو إفشاءها أو نشرها) يعد جريمة اعتداء على المعطيات الخارجية لنظام المعالجة و التالي يعاقب الجاني بالحبس من شهرين الى 3سنوات و بغرامة من 1000000دج الى 5000000دج.

**الفرع الثالث: الاعتداء على سير نظام المعالجة الإلية**

لقد اغفل المشرع الجزائري وضع نص صريح خاص بتجريم الاعتداء على سير نظام المعالجة الآلية للمعطيات، غير أنه يمكن استخلاص ذلك من خلال النصوص التي استحدثها بخصوص تجريم الاعتداءات الواقعة على أنظمة

[1]– فايز محمد راجح غلاب، مرجع سابق، ص 183.

[2] -فشار عطاء الله "مواجهة الجريمة المعلوماتية في التشريع الجزائري " بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية المنعقد بأكاديمية الدراسات العليا، ليبيا، أكتوبر 2009، ص 31.

المعالجة أو على معطيات هذه الأنظمة سواء كانت معطيات داخلية أم خارجية.

فالاعتداء على النظام بتخريبه كما نصت عليه المادة 393مكرر من شأنه أن يعيب عملية سير النظام، والاعتداء على معطيات الداخلية للنظام باستعمال برامج الفيروسات و برامج القنابل المعلوماتية من شانه كذالك التأثير في سير أو حسن سير النظام ألمعلوماتي [1].

يمكن أن تتخذ الأفعال الماسة بسير النظام عدة صور نذكر منها:

**التعطيل:** يمكن أن يصيب التعطيل الأجهزة المادية للنظام كتحطيم الاسطوانات أو قطع شبكة الاتصال أو يصيب الكيانات المنطقية للنظام كالبرامج أو المعطيات باستخدام برنامج فيروسي أو قنبلة منطقية مما يؤدي الى عرقلة سير النظام

**الإفساد:** هو جعل نظام غير صالح للاستعمال بإحداث خلل في نظام سيره وفقدان توازن في أداء وظائفه، كان يعطي نتائج غير تلك التي كان من الواجب الحصول عليها، و مثل هذا الفعل إن لم يؤدي إلى تعطيل نظام المعالجة كلية فانه يحول دون تحقيقه لوظائفه بشكل صحيح.[2]

إذا كان حقيقة يمكن للقاضي الجزائي استخلاص الحماية الجزائية لسير نظام المعالجة الآلية للمعطيات من النصوص القانونية التي تجرم أفعال الاعتداء على أنظمة المعالجة و معطياتها، إلا انه كان الأجدر بالمشرع الجزائري إضافة نص خاص بتجريم الاعتداء على سير النظام لرفع اللبس والحرج

[1] - Bouder Hadjira « protection des systèmes d'informations : aspects juridiques » op cit, p 22 .

[2]– فشار عطاء الله، مرجع سابق، ص 28.

عن القاضي الجزائي الذي تفرضه عليه قاعدة التفسير الضيق للنص الجزائي.

تجدر الإشارة إلى أن المشرع الجزائري جرّم كل من الاشتراك والشروع في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية المذكورة، و جعل العقوبة لهما تساوي العقوبات المقررة للجريمة ذاتها.[1] وقد تشمل هذه العقوبات المذكورة في القسم السابع مكرر من قانون العقوبات، عقوبات أصلية تتمثل في الحبس والغرامة، وعقوبات تكميلية هي مصادرة الأجهزة و البرامج و الوسائل المستخدمة وإغلاق المواقع وأماكن الاستغلال إذا ارتكبت الجريمة بعلم مالكها.[2] كما ان المشرع ضاعف عقوبة الغرامة المقررة للشخص المعنوي الذي يرتكب إحدى الجرائم المعلوماتية إلى 05مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي مع إقراره المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أصليين واو شركاء في نفس الجريمة التي ارتكبها الشخص المعنوي.[3]

**المطلب الثاني: القواعد الإجرائية المقررة في قانون الإجراءات الجزائية لمكافحة الجرائم الالكترونية**

لقد أدرك المشرع الجزائري جيدا بان المواجهة الفعالة للإجرام الالكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية ، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية و تحفظية ، و التي من شانها ان تتفادى وقوع الجريمة الالكترونية أو على الأقل الكشف عنها في وقت مبكر

[1] راجع المادتين 394مكرر5 و 394مكرر7 من قانون العقوبات الجزائري، مرجع سابق.

[2]– راجع العقوبات التكميلية في نص المادة 394مكرر6 من قانون العقوبات الجزائري، المرجع نفسه.

[3]–راجع المادة 394مكرر4 من قانون العقوبات الجزائري، المرجع نفسه.

يسمح بتدارك مخاطرها. و هو ما استدركه المشرع بتضمين القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الالكترونية تتمثل في مراقبة الاتصالات الالكترونية تسجيلها) ( الفرع01) والتسرب ( الفرع 02) .

**الفرع الاول: اعتراض المراسلات وتسجيل الأصوات و التقاط الصور**

يقصد باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج و التوزيع، التخزين، الاستقبال و العرض، التي تتم عن طريق قنوات او وسائل الاتصال السلكية و اللاسلكية في إطار البحث و التحري عن الجريمة و جمع الأدلة عنها.[1]

ولقد أشار المشرع الجزائري إلى ظروف و كيفية اللجوء هذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية على النحو :" **اذا اقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في ...الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... يجوز لوكيل الجمهورية المختص أن يأذن:**

- **باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكي.**
- **وضع الترتيبات التقنية، دون موافقة المعنيين، من اجل التقاط و تثبيت وبث**

[1]-لوجاني نور الدين " أساليب البحث و التحري الخاصة و إجراءاتها وفقا لقانون رقم 06-22 المؤرخ في 20-12-2006" مداخلة في يوم دراسي حول " علاقة النيابة العامة بالشرطة القضائية-احترام حقوق الإنسان و مكافحة الجريمة" وزارة الداخلية، المديرية العامة للأمن الوطني، المنعقد باليزي، الجزائر، يوم 2007/12/12. ص 08

**وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص".**

فموجب هذه المادة فان المشرع الجزائري يسمح لسلطات التحقيق و الاستدلال إذا استدعت ضرورة التحري في الجريمة المتلبس بها، أو التحقيق في الجريمة الالكترونية، اللجوء الى إجراء اعتراض المراسلات السلكية اللاسلكية و تسجيل المحادثات و الأصوات و التقاط الصور، و الاستعانة بكل الترتيبات التقنية اللازمة لذلك من اجل الوصول إلى الكشف عن ملابسات الجريمة و إثباتها دون أن يتقيدوا بقواعد التفتيش و الضبط المألوفة. [1]

ومع هذا فان المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال و التحري و تصون الحقوق و الحريات العامة و الحياة الخاصة للأفراد و التي يمكن ان تتلخص فيما يلي:

**1- ترخيص السلطة القضائية و مراقبتها:**

بمعنى لا يمكن لضابط الشرطة القضائية القيام بإجراء اعتراض المراسلات إلا بعد الحصول على إذن مكتوب و مسبب من طرف وكيل الجمهورية او قاضي التحقيق في حالة فتح تحقيق قضائي، يحدد فيه نوع

[1]- انظر هذه القواعد في المادتين 45 و 47 من قانون الإجراءات الجزائية رقم 06-22 مرجع سابق.

الجريمة التي اقتضت ضرورة التحري أو التحقيق القضائي و طبيعة المراسلة و الاتصال محل

الاعتراض أو التنصت، على إن يتم هذا الإجراء تحت الإشراف المباشر للسلطة المصدرة للاذن.

2-**ضرورة الاعتراض لإظهار الحقيقة** : ويعتبر السند الشرعي المبرر للاعتراض، ذلك لما يمكن أن يحمله هذا الإجراء من اعتداء جسيم على حرمة الحياة الخاصة و سرية الاتصالات، فيباح استثناءا و في حدود ضيقة اعتبارا للفائدة المنتظرة منه، و المتعلقة بكشف اللثام عن الجريمة و ضبط الجناة[1].

3-**مراعاة الجرائم التي يجوز فيها الاعتراض:** أي أن ينصب الاعتراض على إحدى الجرائم التي سمحت فيها المادة 65 مكرر 5 من قانون الإجراءات الجزائية الاستعانة بهذا الإجراء، و حددتها على سبيل الحصر في مقدمتها جرائم الاعتدا على نظم المعالجة الالية .

4- **مراعاة مدة الإجراء:** حددتها الفقرة 2 من المادة 65 مكرر7 ب أربعة أشهر قابلة للتجديد بنفس الشروط الشكلية و الزمنية، حسب تقدير نفس السلطة مصدرة الإذن لمقتضيات التحقيق. [2]

5- **مراعاة السر المهني أثناء الاعتراض:** اي عند القيام باعتراض المراسلات تلتزم سلطات التحقيق بعدم المساس بالسر المهني المتعلق بالتفتيش المنصوص

---

[1]-انظر : لوجاني نور الدين، مرجع سابق، ص10.

[2]- تنص الفقرة 2 من المادة 65 مكرر7 من قانون الإجراءات الجزائية رقم 06-22 على:" يسلم الإذن مكتوبا لمدة أقصاها أربعة أشهر قابلة للتجديد...".

عليه في المادة 45 من قانون الإجراءات الجزائية ، خاصة إذا تعلق الأمر بأماكن يشغلها أشخاص ملزمون بكتمان السر المهني ، مثل مكتب المحامي، مكتب المحضر القضائي، أو تعلق الأمر بأشخاص يحملون اسرار مهنية مثل القضاة، الأطباء، نواب البرلمان، فبرغم ان تلك الأماكن وهؤلاء الأشخاص غير مستثنين من إجراء الاعتراض إلا انه يقتضي الأمر وجوب اتخاذ التدابير اللازمة لضمان احترام السر المهني الذي يخصها .[1]

6-تحرير محضر حول عملية الاعتراض: اي يجب على سلطات التحقيق المختصة تحرير محضرا عن تفصيل كل عملية اعتراض و تسجيل المكالمات و المراسلات و عن عملية الالتقاط و التسجيل الصوتي او السمعي البصري، كما يذكر بالمحضر تاريخ بداية هذه العمليات و نهايتها.[2]

**الفرع الثاني: التسرب**

عرف المشرع الجزائري التسرب بموجب المادة 65 مكرر 12 من قانون الإجراءات الجزائية رقم 06-22 على انه :" **قيام ضابط او عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية او جنحة بإيهامهم انه فاعل معهم أو شريك أو خاف**".

من خلال هذا التعريف يمكن تصور عملية التسرب في نطاق جرائم الاعتداء

[1]- محمد ابو العلاء عقيدة، مراقبة المحادثات التلفونية، دراسة مقارنة، طبعة ثانية، دار النهضة العربية، القاهرة، 2008،ص 192 .

[2]- انظر المادة 65 مكرر 9 من قانون الإجراءات الجزائية رقم 06-22، مرجع سابق.

على أنظمة المعالجة الآلية في ولوج ضابط او عون الشرطة القضائية الى العالم الافتراضي ( الانترنت) و اشتراكه مثلا في محادثات غرف الدردشة او حلقات النقاش و الاتصال المباشر في كيفية قيام احدهم باختراق شبكات او بث الفيروسات، منتحلا في ذلك هوية مستعارة أو باستخدام أسماء و صفات هيئات وهمية ظاهرا فيها بمظهر طبيعي كما لو كان فاعل مثلهم سعيا منه إلى الكشف والإطاحة بالمجرمين. [1]

ولقد سمحت المادة 65 مكرر 14 من قانون الإجراءات الجزائية لضابط أو العون المتسرب من اجل إنجاح العملية، استعمال الوسائل المادية كالأموال أو المنتجات او الوثائق المتحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها، كما يجوز له تسخير وضع تحت تصرف مرتكبي هذه الجرائم كل الوسائل المادية المتاحة لتنفيذ الجريمة كوسائل النقل او التخزين أو الإيواء أو الحفظ أو الاتصال، وكذا الوسائل القانونية كتوفير الوثائق الرسمية إن كان هناك ضرورة لذلك كاستخراج بطاقة التعريف الوطنية او بطاقة رمادية او جواز السفر و لو استدعى الأمر تزويرها ، دون أن يكون الضابط أو العون المتسرب مسئولا جزائيا عن هذه الأعمال.

اعتبارا أن التسرب إجراء غير مألوف عند سلطات الضبط القضائي، و انه من اخطر إجراءات التحقيق انتهاكا لحرمة الخاصة للمتهم، كان لزاما على المشرع إحاطته بجملة من الضمانات و الضوابط التي يتعين مراعاتها عندما

[1]– رشيدة بوكر، مرجع سابق، ص 434.

تقتضي ضرورات التحري او التحقيق في إحدى الجرائم المذكورة اللجوء إليه، و التي يمكن تلخيصها فيما يلي :

1- **صدور إذن قضائي بالتسرب** : نصت على هذا الشرط المادة 65مكرر 11 ومفاده انه لا يجوز لضابط الشرطة القضائية اللجوء إلى التسرب إلا بناءا على إذن مكتوب،[1] صادر من وكيل الجمهورية المختص او قاضي التحقيق بعد إخطار وكيل الجمهورية، على أن يذكر فيه اسم الضابط المشرف على العملية و هويته الكاملة، و تاريخ بداية التسرب.

2- **احترام المدة المقررة للتسرب:** حددت الفقرة الثالثة من المادة 65مكرر 15 من قانون الإجراءات الجزائية مدة التسرب بأربعة أشهر قابلة للتجديد حسب مقتضيات التحري و التحقيق بنفس الشروط ، و يجوز للقاضي الذي رخص بإجراء التسرب أن يأمر في أي وقت بوقفه قبل انقضاء المدة القانونية. و في هذه الحالة و تحسبا للظروف الأمنية للضابط المتسرب أجازت المادة 65 مكرر 17 من نفس القانون لهذا الأخير مواصلة نشاطه لمدة لا تتجاوز أربعة أشهر دون ان يكون مسئولا جزائيا على ذلك، بشرط ان يخطر السلطة مصدرة لإذن في اقرب اجل.[2]

---

[1]-تجدر الإشارة إلى أن الكتابة شرط جوهري لصحة الإذن بالتسرب وهو ما نصت عليه المادة 65 مكرر 15 بأنه " يجب أن يكون الإذن المسلم طبقا للمادة 65 مكرر 11 أعلاه مكتوبا... تحت طائلة البطلان "

[2]- انظر الفقرة الثالثة من المادة 65 مكرر 15 و نص المادة 65 مكرر 17 قانون الإجراءات الجزائية، مرجع سابق.

3- **تسبيب عملية التسرب** : يعتبر التسبيب شرط جوهري لمشروعية عملية التسرب، لذلك اشترط القانون عند إصدار الإذن بالتسرب من السلطات المختصة ذكـر السبب أو الدافع الحقيقي الجاد الذي يبرر اللجوء إلى هذا الإجراء تحت طائلة البطلان.[1]

4- **محل التسرب:** بمعنى أن عملية التسرب يجب أن تنصب على إحدى الجرائم السبعة المنصوص عليها في المادة 65 مكرر 5، و هي: جرائم المحذرات، الجريمة المنظمة، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال و الإرهاب، و جرائم المتعلقة بالتشريع الخاص بالصرف. و فيما عدى ذلك يعتبر التسرب إجراء باطلا.

الجدير بالذكر في الأخير هو أن المشرع الجزائري سمح لسلطات الضبطية القضائية إذا اقتضت ضرورة التحري و التحقيق ممارسة عملية اعتراض المراسلات و تسجيلها و التقاط الأصوات و التسرب و كذا باقي إجراءات التحقيق التي تدخل في اختصاصاتها، عبر كافة الإقليم الوطني إذا تعلق الأمر ببحث و معاينة جرائم الماسة بالمعالجة الآلية للمعطيات. و هذا الإجراء المتمثل في تمديد الاختصاص المحلي لضباط الشرطة القضائية إلى كامل الإقليم الوطني هو من ضمن التدابير غير المألوفة في السابق و التي استحدثها المشرع في المادة 16 الفقرة 7 و 8 و المادة 16 مكرر من قانون الإجراءات الجزائية رقم 06-22 من اجل تحقيق المواجهة الفعالة لظاهرة الإجرام الالكتروني.[1]

[1]- انظر نص المادة 65 مكرر 15 من قانون الإجراءات الجزائية، نفس المرجع.

**المبحث الثاني: آليات مكافحة الجرائم الالكترونية في إطار القوانين الخاصة**

تقتضي المواجهة الفعالة للجريمة الالكترونية بمختلف أنواعها محاصرتها بنصوص خاصة الى جانب القواعد العامة، فلما كان مجال الملكية الفكرية والأدبية حقل خصب لوقوع مثل هذه الجرائم جعل المشرع الجزائري يسارع إلى إحاطته بحماية جنائية و ذلك من خلال تجريم الأفعال التي تشكل اعتداء على حقوق المؤلف (المطلب الاول)، و لتعزيز جهوده في مكافحة الإجرام الالكتروني عمد إلى وضع قواعد أكثر ملائمة مع خصوصيات الجرائم المتعلقة بوسائل الإعلام و الاتصال و ذلك من خلال القانون الخاص بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام و الاتصال و مكافحتها(المطلب الثاني).

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

الهدف من وضع قوانين الملكية الفكرية هو حماية حق الإنسان في التفكير والإبداع والابتكار الذي يعد بمثابة العامل الأساسي لتقدم المجتمعات و تطورها، و لما كانت المكونات المنطقية للحاسب الآلي( برامجه و بياناته) ثمرة جهد فكري للإنسان، كان لزوما على المشرع اشتمال هذه المكونات المنطقية بالحماية المقررة في قانون الملكية الفنية و الأدبية و ذلك بتجريم الافعال التي تشكل اعتداء عليها( الفرع الأول)، و اقرار ما يقابلها من عقوبات جزائية ( الفرع الثاني).

**الفرع الأول: الاعتراف بوصف المصنف الفكري لمعطيات الحاسب الآلي**

[1]– انظر المادة 7/16و8 و المادة 16 مكرر من قانون الإجراءات الجزائية، نفس المرجع .

تجه المشرع الجزائري على غرار معظم التشريعات الغربية[1] إلي الإقرار بالحماية القانونية لبرامج الحاسب الآلي من خلال إخضاعها لقوانين حماية حقوق المؤلف. بحيث اعترف صراحة في الأمر 03-5 المؤرخ في 19-07-2003 المتعلق بحقوق المؤلف و الحقوق المجاورة بوصف المصنف المحمي لمصنفات الإعلام الآلي.[2]

ترتب عن جعل المشرع الجزائري برامج و بيانات الحاسب مصنفا فكريا وإدماجها ضمن المصنفات الأصلية[3]، اعتبار أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج و البيانات يشكل فعلا من أفعال التقليد المنصوص عليها في المادة 151من الأمر 03-5 المذكور سالفا يترتب عليها العقوبات الجزائية المقرر في المواد 153، 156، 157، 158 من نفس الأمر .

وتنقسم جنح التقليد التي تمس مصنف برامج و بيانات الحاسب الآلي إلى ثلاثة أنواع هي:

1-**الجنح المرتبطة بالحق المعنوي للمؤلف:** و هي محددة في المادة 1/151من الامر 03-5 و تتمثل في:

[1]-من بين التشريعات التي توفر الحماية لبرامج الحاسب الالي من خلال القوانين الخاصة بحماية حقوق المؤلف : القانون الفرنسي المؤرخ في 03-07-1985 الخاص بحقوق المؤلف، القانون البريطاني لعام 1985 ، القانون الايطالي لعام 1989، أنظر قارة آمال" الجريمة المعلوماتية" مرجع سابق، 118.

[2]راجع الأمر رقم 03-05 المؤرخ في 19-07-2003، يتضمن حقوق المؤلف و الحقوق المجاورة، جريدة رسمية عدد 44، صادر في 2003/07/23.

[3]- أنظر المادتين 04 و 05 من الأمر رقم 03-05، مرجع سابق .

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

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

**2-الجنح المرتبطة بالحق الأدبي للمؤلف:**تتمثل في:

أ-الاستنساخ غير الشرعي للمصنف(م 1/151 من الامر 03-5): كأن يقوم شخص باستنساخ برنامج أو بيانات الحاسب بأي أسلوب كان و جعله في شكل نسخ مقلدة دون اذن المؤلف.

ب-الإبلاغ غير الشرعي للمصنف(المادة 152 من الأمر 03-5) : كان يقوم شخص بإبلاغ وإعلام عموم الجمهور بمصنف برنامج و بيانات الحاسب دون علم و ترخيص من المؤلف سواء كان الإبلاغ مباشرا كالأداء العلني او البث السمعي البصري او غير مباشرا كاستعمال الاسطوانات و الأقراص الممغنطة .

**3- الجنح المرتبطة بالمصنف المقلد:**

تتعلق هذه الجنح بالتصرفات والتعاملات التي ترد على المصنف المقلد الذي يمكن أن يكون برنامج أو بيانات الحاسب الآلي و هي كالتالي: [1]

[1]- هذه الجنح مذكورة في المادة 3،4،5/151 و المادة 155 من الأمر 03-05 السالف الذكر.

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

تجدر الإشارة في الأخير أن المشرع الجزائري جرّم الاشتراك بالفعل أو بالوسائل في جرائم التقليد الواقعة على مصنف برامج وقواعد بيانات الحاسب الآلي و جعل العقوبة عليه هي نفسها العقوبة المقررة للفاعل الأصلي. [1]

**الفرع الثاني: العقوبات المقررة لجنح تقليد معطيات الحاسب الآلي**

لقد حدد المشرع الجزائري العقوبات التي توقع على جنح تقليد المصنفات المعلوماتية(برامج و قواعد بيانات الحاسب الآلي) في صنفين هما:

**1-العقوبات الأصلية:** حددت هذه العقوبات في نص المادة 153 من الأمر 03-5 على النحو التالي:

أ- **عقوبة الحبس:** للقاضي أن ينطق بعقوبة أصلية تتمثل في الحبس من 06 أشهر إلى 03 سنوات على كل من ارتكب جنحة تقليد مصنف بما فيه المصنفات المعلوماتية.

ب- **عقوبة الغرامة:** علاوة على عقوبة الحبس يمكن للقاضي أن يحكم بغرامة مالية تتراوح بين 500000دج و 1000000دج .

[1]- و هو ما صرحت به المادة 154 من الامر 03-05 بنصها على " يعد مرتكبا الجنحة المنصوص عليها في المادة 151 من هذا الامر و يستوجب العقوبة المقررة في المادة 153 أعلاه، كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة".

**2-العقوبات التكميلية:** لقد أعطى المشرع الجزائري سلطة تقديرية للقاضي للنطق بعقوبة واحدة أو أكثر من العقوبات التكميلية المقررة لجنح تقليد المصنفات التالية:

- مصادرة المبالغ المساوية لإقساط الإيرادات المحصلة من الاستغلال غير المشروع للمصنف (البرنامج) (م157).

- مصادرة و إتلاف كل عتاد انشأ خصيصا لمباشرة المشاط غير المشروع و كل النسخ المقلدة (المادة 2/157).

-الأمر بتسليم العتاد و النسخ المقلدة أو قيمة ذلك و كذلك الإيرادات موضوع المصادرة للمؤلف أو أي مالك حقوق أخرى لتكون عند الحاجة بمثابة تعويض (المادة 159).

- الأمر بطلب من المتضرر بتعليق و نشر أحكام الإدانة على نفقة المحكوم عليه (المادة 158).

-الأمر بحجز الوثائق و النسخ الناتجة عن الاستنساخ غير المشروع أو التقليد أو حجز الدعائم المقلدة و الإيرادات الناتجة عن الاستغلال غير المشروع للمصنفات.

تجدر الإشارة أيضا إلى أنه خول للقاضي الجزائي أن يضاعف و يشدد العقوبات الأصلية في حالة توفر ظرف العود و أن يأمر بغلق المؤسسة التي يستغلها المقلد أو شريكه لمدة لا تتجاوز ستة أشهر، و يأمر بالغلق النهائي إذا اقتضى الأمر. [1]

[1]- أنظر المادة 156 من الأمر 03-05 ، مرجع سابق.

**المطلب الثاني: استحداث تدابير جد يدة في قانون 04/09**[1]

يتميز هذا القانون بأنه الإطار القانوني الأكثر ملائمة مع خصوصيات الجرائم المتعلقة بوسائل الإعلام و الاتصال لا سيما الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت.

باستقراء فحوى هذا القانون يتبين لنا بأن المشرع استحدث تدابير جديدة غير مألـــــوفة في القوانين السابقة للتصدي لجرائم المعلوماتية، تتمثل في تدابير وقائية تساعد على الكشف المبكر للاعتداءات المحتملة و التدخل السريع لتحديد مصدرها و رصد مرتكبيها(الفرع الاول)، و تدابير اخرى إجرائية مكملة لتلك المنصوص عليها في قانون الإجراءات الجزائية(الفرع الثاني).

**الفرع الأول: التدابير الوقائية المستحدثة**

لقد جاء في القانون 09-04 مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها و عن مرتكبيها في وقت مبكر[2]، و هي كالتالي:

1-**مراقبة الاتصالات الالكترونية:** لقد نصت المادة 04 من القانون 09-04 على اربع حالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات والاتصالات الالكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية

[1] قانون رقم 09-04 مؤرخ في 2009/08/5، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، جريدة رسمية عدد 47، صادر بتاريخ 16 اوت 2009.

[2]-تجدر الإشارة إلى أن هذه التدابير هي نفسها المنصوص عليها في المادة 20 الفقرة (ب) و المادة 21 من الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية لعام 2001، مرجع سابق.

المصلحة المحمية وهي:

-للوقاية من الأفعال التي تحمل وصف جرائم الارهاب و التخريب و جرائم ضد امن الدولة .

-عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام.

-لضرورة التحقيقات و المعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية .

- في أطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.[1]

2-**إقحام مزودي خدمات الاتصالات الالكترونية في مسار الوقاية من الجرائم المعلوماتية**[2]:وذلك من خلال فرض عليهم مجموعة من الالتزامات مذكورة في المواد 10، 11 و 12 بالشكل التالي:

-الالتزام بالتعاون مع مصالح الأمن المكلف بالتحقيق القضائي عن طريق جمع أو تسجيل المعطيات المتعلقة بالاتصالات و المراسلات و وضعها تحت تصرفها مع مراعاة سرية هذه الإجراءات و التحقيق.

-الالتزام بحفظ المعطيات المتعلقة بحركة السير و كل المعلومات التي من شانها أن تساهم في الكشف عن الجرائم و مرتكبيها، و هذين الالتزامين موجهين لكل

[1]-انظر نص المادة 04 من القانون 09-04، مرجع سابق.

[2]- عرفت المادة 2 الفقرة (د) من القانون 09-04 مزودي الخدمات بأنه: 1-أي كيان عام او خاص يقدم لمستعملي خدماته، ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام الاتصالات. 2- أي كيان أخر يقوم بمعالجة أو تخزين معطيان معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

مقدمي خدمات الاتصالات الالكترونية (Fournisseurs de services) دون استثناء[1] .

– الالتزام بالتدخل الفوري لسحب المحتويات التي يسمح لهم الاطلاع عليها بمجر العلم طريقة مباشرة او غير مباشرة بمخالفتها للقانون، و تخزينها أو جعل الوصول اليها غير ممكن.

–الالتزام بوضع ترتيبات تقنية للحد من امكانية الدخول الى الموزعات التي تحتوي على معلومات متنافية مع النظام العام و الآداب العامة مع إخطار المشتركين لديهم بوجودها. و نشير إلى ان هذين الالتزامين يخصان فقط مقدمي الدخول إلى الانترنيت (Fournisseurs D'accès a l'internet). [2]

**الفرع الثاني: التدابير الإجرائية**

إضافة الى التدابير الوقائية السالفة الذكر تبنى المشرع في القانون رقم 09-4 إجراءات جديدة يدعم بها تلك المنصوص عليها في قانون الإجراءات الجزائية الخاصة بمكافحة جرائم تكنولوجية الإعلام و الاتصال تتلخص فيما يلي:

–السماح للجهات القضائية المختصة و ضباط الشرطة بالدخول لغرض التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها و المعطيات المعلوماتية المخزنة فيها و استنساخها، مع أمكانية تمديد التفتيش ليشمل المعطيات المخزنة

[1] BOUDER HADJIRA « Quel cadre juridique pour la lutte contre la criminalité liée aux TIC en Algérie » séminaire national sur le cadre juridique des TIC en Algérie ; entre opportunité et contraintes, CERIST, Alger, Algérie du 16 au 17 Mai 2012, p04.

[2]- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري و المقارن، منشورات الحلبي الحقوقية، بيروت، 2012، ص 450.

فـي منظومـة معلوماتيـة أخـرى التـي يمكـن الـدخول إليهـا بواسـطة المنظومـة الأصلية، بشرط إخطار السلطات المختصة مسبقا.

-إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، و ذلك طبقا للاتفاقيات الدولية و مبدأ المعاملة بالمثل.[1]

-توسيع دائرة اختصاص الهيئات القضائية الجزائرية لتشمل النظر في الجرائم المتصلة بتكنولوجية الإعلام و الاتصال المرتكبة من طرف الأجانب خارج الإقليم الوطني، عندما تكون مؤسسات الدولة الجزائرية و الدفاع الوطني و المصالح الإستراتيجية للدولة الجزائرية مستهدفة.

-السماح للسلطات الجزائرية المختصة اللجوء إلى التعاون المتبادل مع السلطات الأجنبية في مجال التحقيق و جمع ألأدلة للكشف عن الجرائم المتصلة بتكنولوجية الإعلام و الاتصال عبر الوطنية و مرتكبيها، و ذلك عن طريق تبادل المعلومات أو اتخاذ تدابير احترازية في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل[2].

يستنتج في الأخير أن أحكام القانون رقم 09-4 جاءت عامة و مطلقة في مجال مكافحة الجرائم المتصلة بتكنولوجية الإعلام و الاتصال، بحيث تجرم كل الأفعال المخالفة للقانون التي ترتكب عبر وسائل الإعلام والاتصال، و يطبق على كافة التكنولوجيات القديمة و الجديدة، بما فيها شبكة الانترنيت و على أي تقنية يمكن

[1]-راجع المادة 05 من القانون 09-04 المؤرخ في 05-02-2009، مرجع سابق .

[2]-راجع المادتين 16 و 17 من القانون 09-04 المؤرخ 05-02-2009، مرجع سابق .

ان تظهر مستقبلا. وهو الأمر الذي يجعله قانونا فعالا و يساير التطور التكنولوجي السريع.

**خاتمة:**

نستنتج مما سبق بان المشرع الجزائري قد تبنى سياسة مزدوجة للتصدي لظاهرة الإجرام المعلوماتية ، بحيث اهتدى من جهة الى تعديل الجوانب الموضوعية و الإجرائية للتشريعات العقابية العامة (قانون العقوبات و قانون الإجراءات الجزائية ) و جعلها تواكب التحديات الجديدة الناتجة عن التطور الهائل للتكنولوجيات الحديثة. و قام من جهة ثانية باستحداث قوانين أخرى خاصة أكثر تجاوبا مع الطبيعة الخاصة للجرائم الالكترونية. وهذا التنوع التشريعي من شانه أن يساهم بشكل فعال على الأقل في الوقت الراهن في الحدّ من تفاقم ظاهرة الإجرام الالكتروني في الدولة الجزائرية.

مع هذا ينبغي الاعتراف بحقيقة و هي انه رغم الجهود الجبارة التي يبذلها المشرع الجزائري في سبيل التصدي لظاهرة الإجرام الالكتروني، إلا أنها غير كافية لبلوغ الهدف الذي يتطلع إليه، نظرا للتطورات السريعة و المستمرة التي تعرفها ظاهرة الإجرام الالكتروني من جهة، و نظرا للطالع العالمي والعابر للحدود الذي تتميز بها هذه الظاهر من جهة أخرى ، لذلك لابد من التفكير في التوجه إلى التعاون التشريعي و القضائي و الأمني مع الدول العربية و لما لا مع الدول الغربية الأكثر دراية بالجرائم الالكترونية والاستفادة من خبراتها في مجال مكافحة هذه الجرائم.