الأحكام الموضوعية والإجرائية لمكافحة الجريمة الالكترونية في التشريع الجزائري

Objective and Procedural Rules Against Cybercrime in Algerian Legislation

خاليدة بن بعلاش*
جامعة تيارت – الجزائر
khalida.benbaalach@univ-tiaret.dz

علي عثماني
المركز الجامعي أفلو –الجزائر
otmani.ali1@gmail.com

تاريخ الارسال:2021/06/20 تاريخ القبول:2021 /10/14 تاريخ النشر:2021/12/31

ملخص:

يهدف هذا المقال إلى تحليل توجه المشرّع الجزائري نحو القضاء على الجريمة الالكترونية، وفي نفس الوقت مُحاولة إبراز كيف تسعى الجزائر جاهدة إلى وضع رصيد تشريعي عقابي؛ موضوعي وإجرائي في سبيل مكافحة الجريمة الالكترونية بشتى مظاهرها ووسائل ارتكابها، ومقاربته قدر الإمكان مع التطور السريع والخطير لهذا النوع من الإجرام المعاصر.

كلمات مفتاحية: الجريمة الالكترونية. أنظمة المعالجة الآلية للمعطيات. العقاب. موضوعيا. إجرائيا.

Abstract:

This article aims to analyze the direction of the Algerian legislator towards the elimination of cybercrime, while trying to highlight how Algeria is trying to achieve a legal arsenal put; from the side substantive and procedural in order to fight against cybercrime in all its manifestations and the means of its perpetration, withe format that corresponds toas possible with the rapid and dangerous development of this type of contemporary crime.

Keywords: Cybercrime. Automated Data Processing Systems. Punishment.Substantive. Procedural.

*المؤلف المرسل

مقدمة

باتت الجريمة الالكترونية كنقطة مظلمة بالنسبة للتكنولوجيا المعلوماتية، حيث صاحب تطور وسائل الاتصال الإلكتروني بمُختلف أنواعه تطور في الجريمة يتماشى وهذا التطور التكنولوجي، وبذلك أصبحت الجريمة الإلكترونية لا تقل خطورة عن الجريمة التقليدية.

وتُعد الجريمة الالكترونية من الجرائم المستحدثة، التي يمكن وصفها بالجرائم الناعمة غير الدامية أو العنيفة التي تستخدم فيها شبكة الانترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها. والتي تكمن خطورتها في أنها لا تعرف الحدود ولا المكان ولا توجد لها أدالة مادية تدل عليها أو على من يرتكبها.

بالتالي تهدف هذه الدراسة إلى الوقوف على مفهوم الجريمة الالكترونية، وإبراز أهم خصائصها و مظاهرها، مع بيان الإطار القانوني لمكافحة الجريمة الالكترونية من الناحيتين الموضوعية والإجرائية؛ الأمر الذي من شأنه تبيان جهد المشرع الجزائري من خلال التشريع العقابي لمواجهة هذا النوع من الجرائم، سواء كان ذلك من خلال القواعد الواردة في قانون العقوبات رقم 66-156 المعدل والمتمم أو القانون رقم 09-04 المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلى جانب قانون الإجراءات الجزائية رقم 66-155 المعدل والمتمم.

على هذا الأساس نطرح الإشكالية الآتية: كيف تصدى المشرع الجزائري للجريمة الالكترونية من الناحية القانونية الموضوعية منها و الإجرائية ؟

للإجابة على هذه الإشكالية يتم تقسيم الدراسة إلى محورين، يعالج أولهما: الأحكام الموضوعية لمكافحة الجريمة الالكترونية والثاني: الأحكام الإجرائية المقررة لمكافحة الجريمة الالكترونية.

أولا: الأحكام الموضوعية لمكافحة الجريمة الالكترونية

لابد من بيان مفهوم الجريمة الالكترونية (**أولا)** قبل التطرق للأحكام الموضوعية لمكافحتها(**ثانيا)**.

1. مفهوم الجريمة الالكترونية

تتم الإشارة فيه لأهم التعاريف التي تطرقت للجريمة الالكترونية، ثم بيان خصائصها، ونماذج هذا النوع من الإجرام.

1.1. تعريف الجريمة الإلكترونية

تعريف الجريمة الالكترونية يقتضي بيان التعريف الفقهي، ثم التعريف التشريعي.

1-1-1: التعريف الفقهي للجريمة الالكترونية

أعطى الفقه القانوني تعاريف مُختلفة للجريمة الالكترونية، سواء بالنظر إلى وسيلة ارتكاب الجريمة أو محلها أو مرتكبها أو حتى غرض الجريمة، ذلك على النحو التالي:

– الجريمة الالكترونية: عبارة عن اعتداء يطال معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت؛ فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات[1].

– كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الالكترونية.

– الاعتداءات القانونية التي يمكن أن ترتكب بواسطة الوسائل الالكترونية بغرض تحقيق الربح[2].

-نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود[3].

ومن التعاريف التي تستند إلى موضوع الجريمة أو أحيانا أنماط السلوك محل التجريم، تعرف الجريمة الالكترونية بأنها: نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه أو هي كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات، أوهي أي نمط من أنماط الجرائم المعروفة في قانون العقوبات، طالما كان مرتبطا بتقنية المعلومات. أو هي الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة أو إساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر[4].

1-1-2: التعريف التشريعي للجريمة الالكترونية

يُمكن تحديد المقصود من الجريمة الالكترونية من خلال السلوكيات المكونة لها والمحددة في المواد من 394 مكرر إلى 394 مكرر 07 من قانون العقوبات في القسم السابع مكرر من الفصل الثالث بعنوان الجنايات والجنح ضد الأموال(ما يتم التفصيل فيه في المحور الثاني من الدراسة).

كما يمكن الاعتماد على ما جاء في القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[5]، حين عرفت المادة الثانية فقرة "أ" منه الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بكونها: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

كما عرّفت نفس المادة في فقرتيها "ب " و "ج" كلا من المنظومة المعلوماتية والمعطيات المعلوماتية على النحو الآتي:

– **المنظومة المعلوماتية:** أي نظام منفصل أو مجموعة من الأنظمة المتصلة يبعضها البعض أو المرتبطة، يقوم واحد منه أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

- **معطيات معلوماتية:** أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

2.1. خصوصيّة الجريمة الالكترونية

تظهر خصوصية الجريمة الالكترونية من عدة نواحي أهمها:

1-1-1: من حيث التجريم

فهي نابعة من وقوع غالبية هذه الجرائم على العالم الافتراضي دون المادي، وذلك حتى مع ملامسة بعضها للعالم المادي، فإنّها تبقى من الخصوصية بما يجعلها متمايزة عن غيرها من الجرائم والتي تتطلب خصوصيّة في التجريم لئلا يفلت مقترفها من العقاب.

1-1-2: من ناحية خصوصية الإثبات في هذا النوع من الجرائم

فإنّها لا تخلو من الصعاب الجمة، والتي تكتنف رصد واحتواء الدليل المتحصل من مسرح الجريمة سواء المادي أو الافتراضي، وذلك كون الأدلة الرقمية صعبة الاحتواء وسهلة الاختفاء والمحو . وكذلك أنّه يمكن التضليل بشأن كشفها أو الاطلاع على مضمونها[6].

1-1-3: من ناحية الفاعل في جرائم المعلوماتية

يتميز عن غيره من الجناة الآخرين في الجرائم التقليدية بالعديد من الصفات أهمها أن يكون على درجة كبيرة من العلم والحرفية في مجال الحواسيب وشبكة المعلومات، كما يجب أن تكون له رغبة جامحة في تحدي كل ما هو جديد ومبتكر، حيث أن الإحصائيات العملية أفادت أنّ العديد ممن تم القبض عليهم من المجرمين المعلوماتيين، أفادوا بمحاضر التحقيقات أنّهم قاموا بتلك الجرائم رغبة منهم في تحدي وقهر الأنظمة المحوسبة أو يكون ذلك الجاني في الجريمة المعلوماتية(لديه طمع مادي مبالغ فيه).

فهؤلاء الجناة من هذا الصنف لا يرضون بالكسب غير المشروع القليل بل عيونهم دائما تكون مصوبة شطر الكسب الكبير جدًا ولهذا نراهم لا يستهدفون إلاّ المؤسسات المالية الكبيرة وبنوك المال والمعلومات أيضا[7].

1-1-4: خصوصية الملاحقة

فإنّها تنبع من الجانب التقني لهذه الجرائم، والتي تتطلب قدرات خاصة لدى الأشخاص المختصين بالمتابعة والملاحقة لمثل هذا النوع من الجرائم ، وكذلك الآليات القانونية التي يجب إقرارها للمساعدة في التنقيب عن الأدلة الالكترونية، ومشروعية الإجراء الذي يمكن إتباعه للكشف عن الدليل وهذا عوضا عن مشروعية الدليل نفسه[8].

1-1-5: المجني عليه في الجرائم الالكترونية

على الرغم من إمكانية تعرض الجميع للجريمة المعلوماتية سواء أكانوا أشخاصًا معنوية أو طبيعية إلاّ أنّه يمكن الجزم بأنّ مُعظم الجرائم المعلوماتية ترتكب من أجل أمرين لا ثالث لهما وهما: المال والمعلومات، وبالتالي يمكن الجزم أيضا بأن الغالبية العظمى من المجني عليهم في الجرائم المعلوماتية هم إما مؤسسات مالية كالبنوك والمصارف وشركات الصرافة وإما شركات المعلومات يصرف النظر عن نوع هذه المعلومات وقيمتها، إذ قد تكون بالغة الأهمية كالمعلومات العسكرية و المخابراتية وقد تكون معلومات رياضية أو اجتماعية بسيطة[9].

هذا وتجدر الإشارة إلى أنّ المشرّع الجزائري ضاعف عقوبة الجريمة المعلوماتية التي تستهدف الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد بموجب المادة 394 مكرر 3 من قانون العقوبات.

1-1-6: يمكن للجريمة الالكترونية أن تمتد من دولة إلى دولة أخرى، أو ترتكب في دولة لتصيب دولة أخرى

باستخدام الشبكات المعلوماتية، وهنا تطرح مشكلة الاختصاص القضائي وكذا قانون العقوبات الواجب التطبيق.[10]

3.1. أنواع الجرائم الالكترونية

تتنوع الجريمة الالكترونية وتأخذ أشكالا متعددة، ولكنّها بصفة عامة تشمل الجرائم الجنسية وجرائم ترويج المخدرات، وتعليم الإجرام أو الإرهاب كصنع المتفجرات، إضافة إلى جرائم الفيروسات واقتحام المواقع، إضافة إلى سرقة المعلومات أو حتى البيانات الشخصية، وتتعدى ذلك لتشمل تحويل الأرصدة في البنوك عبر الشبكة...[11].

هذا ومن النماذج الخطيرة للجريمة الالكترونية نجد جرائم التجسس الالكتروني، وجرائم القرصنة، جرائم الإرهاب الالكتروني، والجرائم المنظمة وجرائم الابتزاز الجنسي.

2. القواعد الموضوعية المقررة لمكافحة الجريمة الالكترونية

يمكن إجمال القواعد الموضوعية المقررة لمكافحة الجريمة الالكترونية في تلك الواردة في قانون العقوبات أو بموجب قوانين خاصة على النحو التالي:

1.2. القواعد الموضوعية المقررة لمكافحة الجريمة الالكترونية في ظل قانون العقوبات

أول نص تشريعي جزائري في مجال الإجرام الالكتروني، كان سنة 2001، بصدور القانون رقم 01-09 المؤرخ في 26 جويلية 2001 [12] المعدّل والمتمم لقانون العقوبات، في المواد من 144 مكرر و144 مكرر 1و 144مكرر 2 و146 من قانون العقوبات، والمتعلق بجريمة القذف و السب و الإهانة إزاء رئيس الجمهورية أو فيما يخص دين الإسلام (الرسول وباقي الأنبياء أو ما هو معلوم من الدين) أو ضد الهيئات والمؤسسات أو الهيئات العمومية، ومن خصوصيات المادة 144 مكرر أنها أدرجت لأول مرة مصطلح:

(...وسيلة الكترونية أو معلوماتية ...) التي تسمح بتجريم الأفعال السالفة الذكر في محيط المعلوماتية والانترنت.

فيما بعد أحدث قسم في قانون العقوبات(القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الأموال) تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04-15 المؤرخ في10 نوفمبر2004[13].حدد المشرّع الجزائري من خلاله كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة، وتأخذ هذه الأفعال إما وصف الاعتداء على نظام المعالجة الآلية للمعطيات أو وصف الاعتداء على معطيات نظام المعالجة الآلية، كما يمكن لها أن تأخذ وصف الاعتداء على سير نظام المعالجة الآلية[14]. مع عدم إغفال النص على عقوبات الأشخاص المعنوية المرتكبة للجرائم الالكترونية وكذا عقوبات الشروع والاشتراك في الإجرام الالكتروني.

2-1-1: تجريم الاعتداء على نظام المعالجة الآلية

ذلك من خلال الدخول أو البقاء في نظام المعالجة الآلية للمعطيات، حيث نصت المادة394 مكرر من قانون العقوبات: " يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من خمسين ألف دينار جزائري إلى مائة ألف دينار جزائري كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظمة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من06 أشهر إلى سنتين و غرامة من خمسين ألف دينار جزائري إلى مائة و خمسون ألف دينار جزائري".

بالتالي فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع فيما الصورة المشددة، تتحقق بتوافر الظرف المشدد لها، و يكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة[15].

2-1-2: تجريم الاعتداء على معطيات نظام المعالجة الآلية

ويكون ذلك بإحدى الصورتين:

أ: الاعتداء على المعطيات الداخلية للنظام: جاء في المادة394 مكرر1:" يعاقب بالحبس من06 أشهر الى03 سنوات و بغرامة من500.000 دج الى2000.000 كل من ادخل بطريقة الغش معطيات في نظام أو أزال أو عدل بطريقة الغش المعطيات التي يتضمنها"،بالتالي فالنشاط الإجرامي في جريمة الاعتداء العمدي على المعطيات يتجسد في إحدى الصور الثلاث التالية[16]: الإدخال L'intrusion، المحـــو L'effacement، التعديل Modification.

لا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقــط لكي يتوافر الركــن المــادي. 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، و

هذا يعني أن النشاط الإجرامي في هذه الجريمة إنّما يرد على محل أو موضوع محدد و هو المعطيات أو المعلومات التي تمت معالجتها آليا و التي أصبحت مجرد إشارات أو رُموزًا تمثل تلك المعلومات، و ليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام، أي التي يحتويها النظام و تشكل جزءا منه.

ب: الاعتداء على المعطيات الخارجية للنظام: نصت عليه المادة394 مكرر2:" يعاقب بالحبس من شهرين الى03 سنوات و بغرامة من1000.000 دج الى5000.000 دج كل من يقوم عمدا و عن طريق الغش بما يلي:

01- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

02- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

ج: الاعتداء على سير نظام المعالجة الآلية: لقد أغفل المشرّع الجزائري وضع نص صريح خاص بتجريم الاعتداء على سير نظام المعالجة الآلية للمعطيات، غير أنّه يمكن استخلاص ذلك من خلال النصوص التي استحدثها بخصوص تجريم الاعتداءات الواقعة على أنظمة 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 شأنه كذلك التأثير في سير أو حسن سير النظام المعلوماتي[17].

د: عقوبة الشخص المعنوي: تم إقرار إمكانية معاقبة الشخص المعنوي المرتكب لجرائم المساس بأنظمة المعالجة الآلية للمعطيات في المادة394 مكرر4.وذلك بغرامة تعادل خمس مرات الحد الأقصى المقرر للشخص الطبيعي المرتكب لهذه الجرائم.

ه: عقوبة الشروع والاشتراك في الجريمة الالكترونية: الجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي، وباعتبار أنّه لا عقاب على الشروع في الجنح إلاّ بنص، فقد أقرّت المادة394 مكرر7 من قانون العقوبات بأن" يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها. "بالتالي يبدوا من خلال هذا النص رغبة المشرّع الجزائري في توسيع نطاق العقوبة لتشمل اكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية[18].

هذا وقد نصت المادة394 مكرر5:" كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان هذا التحضير مجسد أو عدّة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها.

بالتالي قد تشمل العقوبات المنصوص عليها في هذا القسم عقوبات أصلية، تتمثل في الحبس والغرامة أو عقوبات تكميلية مثل مصادرة الأجهزة و البرامج و الوسائل المستخدمة، مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها.

2.2. القواعد الموضوعية المقررة لمكافحة الجريمة الالكترونية في ظل قوانين خاصة

حدد المشرّع الجزائري العقوبات التي توقع على جنح تقليد المصنفات لاسيما منها المعلوماتية،[19] في صنفين هما: العقوبات الأصلية في نص المادة 153 من الأمر رقم 03-05 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف والحقوق المجاورة،[20] والعقوبات التكميلية في المواد 157 و158 و159.

كذلك في ظل قانون الملكية الصناعية سواء ما تعلق منها بتقليد العلامة التجارية حسب ما جاء في الأمر رقم 03-06 [21] أو قانون براءة الاختراع وفقا للأمر رقم 03-07 المؤرخ في 19 يوليو 2003[22].

ثانيا: القواعد الإجرائية لمكافحة الجريمة الالكترونية

هناك الكثير من التحديات الإجرائية لجرائم الكمبيوتر والانترنت والتي تواجه سلطات الضبط القضائي، وذلك لكونها تتمتع بطبيعة افتراضية تجعلها متمايزة عن غيرها من الجرائم التقليدية، حيث أن هذه الجرائم لا تترك أثرا ماديا في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية، كما أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة، وأهم الصعوبات التي تواجه الملاحقة الإجرائية هو ما يتعلق بإجراءات التفتيش ومحله، ومدى قانونية الإجراء في الأصل وكذلك مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش[23].

ومواجهة لما سبق سارع المشرّع الجزائري إلى مواكبة التطور بإصدار تشريع جديد؛ ألا وهو القانون المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها رقم 09-04الصادر في 05 أوت 2009، بحيث تضمن قواعد إجرائية جديدة تكمل القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية، بخصوص التفتيش والحجز وكذلك المراقبة أو التسرب الذي يقع على هذه الجرائم.

هذا و يُعتبر القانون رقم 09-04 المنظم لفضاء المعلوماتية بصفة عامة و مكافحة المجال الإجرامي المتصل بها من خلال قواعد تسمح بمتابعة هذا النوع من الجرائم ومرتكبيها بشكل يضمن شرعية الإجراءات المتخذة[24].

كما أنّ صدور هذا القانون كان نتيجة القصور الذي عرفه القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004الذي نص على الحماية الموضوعية، وذلك في قانون العقوبات الجزائري أما بخصوص الجانب الإجرائي الخاص بمكافحة هذه الجرائم فلم يتضمن النصوص التي سبقت القانون رقم 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

عموما تكمن خصوصية إجراءات المتابعة والبحث والاستدلال في الجريمة الالكترونية فيما يلي:

1. تمديد قواعد الاختصاص المحلي والقضائي

اتجه المشرّع الجزائري قصد تفعيل عمليات التصدي و المتابعة للجرائم ذات الخطورة البالغة لإصدار كل من القانون رقم 04-14 وكذا القانون رقم 06-22 [25]المتضمنان تعديل قانون الإجراءات الجزائية[26] والذي من خلالهما وجدت إمكانية توسيع الاختصاص المحلي لكل من وكيل الجمهورية[27] وقاضي التحقيق[28]و ضباط الشرطة القضائية[29] و المحكمة[30]إلى دائرة اختصاص محاكم أخرى تحدد عن طريق التنظيم[31]ويتعلق الأمر بجريمة تبييض الأموال إلى جانب جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنشطة المعالجة الآلية للمعطيات والجرائم المتعلقة بمخالفة التشريع الخاص بالصرف وحركة رؤوس الأموال وتمويل الإرهاب.

كما نظم المشرّع الجزائري في القانون رقم 09-04 أحكاما جديدة خاصة بالاختصاص في مجال الجريمة الالكترونية تتماشى والتطور الذي لحق الجريمة، من هذه القواعد ما نصت عليه المادة الثالثة منه، بالإضافة إلى ذلك قررت المادة 15 من نفس القانون بأنّه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

2. تطوير إجراءات التحري والكشف عن الجريمة الالكترونية

عرّف الفقه أساليب التحري الخاصة بكونها: تلك العمليات أو الإجراءات أو التقنيات التي تستخدمها الضبطية القضائية تحت مراقبة وإشراف السلطة القضائية، بغية البحث والتحري عن الجرائم الخطيرة المقررة في قانون العقوبات، وجمع الأدلة عنها والكشف عن مرتكبيها، وذلك دون علم ورضا الأشخاص المعنيين، وهي الأساليب التي نصت عليها المادة 14 من تعديل قانون الإجراءات الجزائية، (التي تتمم الباب الثاني من الكتاب الأول بفصل رابع تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وفصلا خامسا بعنوان التسرب) وكذا ما نصت عليه المادة 16 مكرر من نفس القانون[32].

1.2. اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

أقرّ المشرّع الجزائري اللجوء إلى هذه الوسائل في المواد من 65 مكرر 05 إلى 65 مكرر 10 من قانون الإجراءات الجزائية، التي سمحت بها استثناء كإجراءات تحقيق، إذا ما دعت إلى ذلك مُقتضيات البحث والتحري والتحقيق الابتدائي في الجرائم المتلبس بها، أو في جرائم عدة من بينها الجريمة المعلوماتية، هذا كله مع ضرورة الحصول على الإذن من وكيل الجمهورية.

حيث نصت المادة65مكرر5من قانون الإجراءات الجزائية على أنه: "إذا اقتضت ضرورة التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو في الجريمة المنظمة العابرة للحدود الوطنية

أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جريمة تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية أن يأذن بما يلي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

- وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث 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.

- يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47من قانون الإجراءات الجزائية وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن...".

كذلك نصت المادة 03 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:" مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام، أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائيّة وفي هذا القانون وضع الترتيبات التقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية". وبخصوص مراقبة الاتصالات الالكترونية فقد أقرته المادة 04 من القانون رقم 09-04 .

2.2. التفتيش

نص المشرّع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنّه: "إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك..." .

كما تم النص على إجراءات التفتيش والحجز[33] داخل المنظومة المعلوماتية وذلك بالرجوع إلى المادة 05 من القانون 09-04حيث نجد أن المشرّع الجزائري أجاز للسلطات القضائية المختصة، وكذا ضابط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04منه، الدخول بغرض التفتيش ولو عن بعد إلى:"-منظومة معلوماتية أو جزء منها وكذلك المعطيات المخزنة فيها ومنظومة تخزين معلوماتية.

-في الحالة المنصوص عليها في الفقرة/ أ من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

3.2. التسرب

نصت عليه المواد من 65 مكرر 11 إلى 65 مكرر 18 من قانون الإجراءات الجزائية، وقد عرّفه المشرع الجزائري في نص المادة 65 مكرر 18 من نفس القانون بكونه:" قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

وأجاز المشرّع الجزائري اللجوء إلى هذه الوسيلة، التي تعد أسلوبا من أساليب التحري الخاصة، في بعض الجرائم المنصوص عليها على سبيل الحصر في المادة 65 مكرر 05، وهي: الجرائم المتلبس بها ، جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية، والجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب وجرائم الصرف، إضافة إلى جرائم الفساد.

ويتم التسرب بعد الحصول على إذن قضائي من وكيل الجمهورية أو قاضي التحقيق، لضمان شرعيته وعدم مساسه بخصوصية الأفراد المكفولة دستوريا. ويكون عبر استعمال العون المتسرب هوية مستعارة في مواقع الانترنت، التي يشتبه قيام أصحابها بعمليات النصب والاحتيال[34].

4.2. التوقيف تحت النظر

بغية مواجهة الجريمة الالكترونية، تم تمديد التوقيف تحت النظر الممنوح لضباط الشرطة القضائية مرة واحدة إذا تعلق الأمر بالجريمة الالكترونية، وذلك بموجب المادة 5/51 من الأمر رقم 15-02 المؤرخ في 23جويلية 2015 المعدل والمتمم لقانون الإجراءات الجزائية.

الخاتمة

من خلال الدراسة السابقة توصلنا إلى جملة من الاستنتاجات والتوصيات، نجملها فيما يلي:

أولا: الاستنتاجات

-توجد فعلا حلول تشريعية ردعية في الجزائر يمكن الاعتماد عليها بغية التصدي لمخاطر الجرائم الالكترونية إلاّ أنّها لا ترقى لدرجة القضاء النهائي على هذا النوع من الإجرام، بالنظر للصعوبات والتحديات التي تطرحها الجريمة الالكترونية التي تمتاز بالتطور و التحور السريع يوما بعد يوم .

-صدور القانون رقم 09-04 لتكملة الترسانة القانونية لمواجهة الجرائم الالكترونية الواردة في قانون العقوبات.

-خصوصية الجرائم الالكترونية انعكست على الإجراءات الجزائية المطبقة عليها، سواء من حيث البحث والتحري أو الضبط والتفتيش أو من حيث وسائل الإثبات.

-تمديد قواعد الاختصاص المحلي أو القضائي في مجال مكافحة الجريمة الالكترونية.

ثانيا: التوصيات

-تطوير التعاون التشريعي والقضائي والأمني على مختلف المستويات الوطنية والدولية والإقليمية لمكافحة وحصر الجريمة الالكترونية.

-تطوير الدراسات الميدانية والأكاديمية للكشف عن الباعث إلى ارتكاب هذا النوع من الجرائم، والذي يحتل أهمية بالغة باعتباره السبب الأساسي في وجودها وتفاقمها.

-توفير كوادر بشرية متخصصة في الخبرة الجنائية للجرائم الالكترونية.

-التنظيم التشريعي لمسألة قيمة الدليل المستمد من الجرائم الالكترونية وقيمته الثبوتية.

-توسيع نطاق التجريم في الجرائم الالكترونية ليشمل كذلك **التزوير الالكتروني** إلى جانب الجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات.

في الأخير يجب التأكيد على أن الجريمة الإلكترونية هي جريمة فعلية وأنه ينبغي حملها على محمل الجد أسوة بسائر الجرائم التقليدية.

الهوامش:

[1] يونس عرب، جرائم الكمبيوتر والانترنت، اتحاد المصارف ،2001، ص19.

[2] عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية- دراسة مقارنة، مذكرة ماجستير في القانون العام، جامعة الشرق الأوسط، 2014، ص 13.

[3] ليندة شرا بشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية، الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة دراسات وأبحاث، المجلد الأول ، العدد الأول، 2009، ص242.

[4] محمود مدين، الجريمة الالكترونية وتحديات الأمن القومي، الطبعة الثانية، المصرية للنشر والتوزيع، سنة 2019، ص 30.

[5] القانون رقم 09-04 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد: 47 لسنة 2009.

[6] عبد اللطيف محمود ربايعة، الجرائم الالكترونية، التجريم والملاحقة والإثبات، مقدم إلى المؤتمر الأول للجرائم الالكترونية في فلسطين، المنعقد في جامعة النجاح الوطنية، نابلس، 17نيسان 2016م، ص04.

[7] رابحي عزيزة، الأسرار المعلوماتية، وحمايتها الجزائية، أطروحة دكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبى بكر بلقايد، تلمسان، 2018/2017، هامش الصفحة 102.

[8] عبد اللطيف محمود ربايعة، المرجع السابق، ص 04.

[9] رابحي عزيزة، المرجع السابق، ص 103.

[10] دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة قسنطينة، 2013/2012، ص 14.

[11] لينا جمال محمد، الجرائم الالكترونية، دار خالد اللحياني للنشر والتوزيع، 2016، ص 05.

[12] الجريدة الرسمية العدد: 34 لسنة 2001.

[13] القانون رقم 04-15 المؤرخ في 10نوفمبر 2004 الجريدة الرسمية العدد: 71 لسنة 2004.

[14] براهيمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، المجلد 11، العدد:02، نوفمبر سنة 2016، ص 125.

[15] فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون والمعلوماتية المنعقد بأكاديمية الدراسات العليا بليبيا ، أكتوبر 2009، ص 26.

[16] المرجع نفسه، ص 29.

[17] براهيمي جمال، المرجع السابق، ص 137.

[18] فشار عطاء الله، المرجع السابق، ص 34-35.

[19] تنص المادة 152 من الأمر رقم 03-05 المتعلق بحقوق المؤلف و الحقوق المجاورة بأنه: يعد مرتكبا لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الأداء ....أو بأي منظومة معالجة معلوماتية .

[20] الأمر رقم 03-05 المؤرخ في 19 يوليو 2003 يتعلق بحقوق المؤلف والحقوق المجاورة ، الجريدة الرسمية العدد: 44 لسنة 2003.

[21] الأمر رقم 03-06 المؤرخ في 19 يوليو 2003 يتعلق بالعلامات، الجريدة الرسمية العدد: 44 لسنة 2003.

[22] الأمر رقم 03-07 المؤرخ في 19 يوليو 2003 يتعلق ببراءات الاختراع، الجريدة الرسمية العدد: 44 لسنة 2003.

[23]عبد اللطيف محمود ربايعة، المرجع السابق ، ص 23.

[24]سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة الإخوةمنتوري، العدد52، ديسمبر 2019، ص 50.

[25] القانون رقم 06-22 المؤرخ في 20 ديسمبر سنة 2006 الجريدة الرسمية العدد 84 لسنة 2006

[26] القانون رقم 04-14 المؤرخ في 10 نوفمبر سنة 2004، الجريدة الرسمية العدد 71 لسنة 2004.

[27] المادة 37 الفقرة 02 من قانون الإجراءات الجزائية .

[28] المادة 40 الفقرة 02 من قانون الإجراءات الجزائية.

[29] المادة 16 فقرة 07 من قانون الإجراءات الجزائية .

[30] المادة 329 من قانون الإجراءات الجزائية .

[31] صدر المرسوم التنفيذي رقم 06-348 تطبيقا لأحكام المواد 37، 329،40 من قانون الإجراءات الجزائية الذي حصر الجهات القضائية ذات الاختصاص الإقليمي الموسع في أربعة محاكم على المستوى الوطني وهي: محكمة سيدي أمحمد بالجزائر العاصمة، محكمة قسنطينة، محكمة وهران ومحكمة ورقلة. ينظر: المرسوم التنفيذي رقم 06-348 المؤرخ في : 12 رمضان عام 1427 الموافق 05 اكتوبر سنة 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق(الجريدة الرسمية العدد: 63 لسنة 2006). المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 اكتوبر 2016(الجريدة الرسمية العدد: 62 لسنة 2016).

[32] فريدة بن يونس، الإطار الناظم لاختصاص الشرطة القضائية في مواجهة الجريمة المعلوماتية في التشريع الجزائري، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، ، المجلد 12، افريل 2020، ص 130.

[33] المواد 06 و07 و08 من القانون رقم 09-04 .

[34] ياسين بن عمر، المعالجة القانونية للجرائم الالكترونية في القانون الجزائري والتشريعات المقارنة، – التشريع المغربي والاماراتي نموذجا)، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الوادي، المجلد 10، العدد03، ديسمبر 2019، ص 719.