المعالجة القانونية للجرائم الالكترونية في القانون الجزائري والتشريعات المقارنة
(التشريع المغربي والإماراتي نموذجا)

Legal Treatment of Cybercrime in Algerian Law and Comparative Legislation (Moroccan and UAE Legislation Model)

طالب الدكتوراه/ ياسين بن عمر [1،2]

[1] **جامعة باتنة، (الجزائر)**

[2] **المؤلف المراسل:** ostadyacine@gmail.com

تاريخ الاستلام: 2019/03/07 تاريخ القبول للنشر: 2019/09/23 تاريخ النشر: 2019/12/28

❖❖❖❖❖❖❖

مراجعة المقال: اللغة العربية: أ./ عفاف طريلي (جامعة الوادي) اللغة الإنجليزية: د./ محمد أكرم عربات (جامعة قسنطينة)

ملخّص:

تعدّدت أضرار ومخاطر الجرائم الالكترونية، وباتت تهدد أمن المجتمعات والمؤسسات والأفراد على حد سواء، وأصبح الحفاظ على أمن المجتمع والأفراد تحديا كبيرا لرجال التشريع والقضاء، في مواجهة هذا الإجرام المتطور. وقد بات من الضروري أن تواكب التشريعات المختلفة هذا التطور الملحوظ في الجرائم الإلكترونية، والتي يأتي في مقدمتها إنتاج ونشر برامج الفيروسات، والدخول غير المشروع لأنظمة الشبكات والمعطيات والتعديل والتغيير في البيانات، والتحايل على النظام، وإتلاف البرامج وتزوير المستندات...

ولقد سارع المشرع الوطني في تعديل نصوص قانون العقوبات بإدراجه مواد تحت مسمى المساس بأنظمة المعالجة الآلية للمعطيات، وعلى غرار المشرع الوطني فقد سارت التشريعات المقارنة في اعتماد مواجهة الجرائم الالكترونية، على غرار التشريع الجنائي المغربي والتشريع الإماراتي، مع اختلاف سياسة المواجهة بين التشريعات.

وتتناول هذه الورقة البحثية السياسة التي انتهجها المشرع الوطني في مواجهة صور الجرائم الالكترونية وتقييمها، من خلال قراءة في النصوص المعتمدة ومقابلتها بالتشريعات المقارنة المغربية والإماراتية على وجه الخصوص.

الكلمات المفتاحية: الجرائم الالكترونية؛ المعالجة الآلية للأنظمة المعلوماتية؛ المشروعية؛ الدليل الالكتروني؛ أنظمة المعطيات؛ المعالجة الإجرائية؛ المعالجة الموضوعية.

Abstract:

Cybercrime has become more and more dangerous and has threatened the security of communities, institutions and also individuals. It has become a serious challenge for the legislators and judiciaries to confront this ever-developing crime. It has also become necessary for legislations to keep up with the remarkable development in cybercrimes led by the production and dissemination of virus software, illegal access to network systems and data, modification and change in data, system circumvention, the destruction of programs and falsification of documents.

The national legislator has reacted quickly to amend the provisions of the Penal Code by inserting articles under the name of prejudice to the automated data processing systems. Like the national legislator, the comparative legislations have undertaken confronting cybercrime, such as the Moroccan criminal legislation and the UAE legislation, with a different policy of confrontation between legislations.

This paper discusses the policy adopted by the national legislator in confronting the forms of cybercrime and evaluating them through reading the adopted texts and comparing them with the Moroccan and Emirati legislations in particular.

Keys words: *Cybercrimes; Automated Processing of Information Systems; Legitimacy; Electronic Evidence; Data Systems; Procedural Processing; Objective Processing.*

مقدّمة:

أثارت الجريمة الالكترونية نقاشا كبيرا بين فقهاء القانون في التعامل معها، خاصة بعد أن أصبحت واقعا ملموسا ووسيلة للتعدي على الأموال أوالبيانات الشخصية للأفراد، ولأن التشريع يأتي متأخرا عن تطور الجريمة، فقد سبب هذا الفراغ القانوني مشكلة ما يسمى بأزمة الشرعية الجزائية في القانون الجزائي، وهي عدم إمكانية مواجهة الجرائم المرتكبة لعدم وجود نص قانوني ينظمها، مع تضارب الإتجاهات حول مدى إمكانية التعامل معها بالنصوص الموجودة، وقد استحدث المشرع الجزائري نصوصا لمواجهة الصور الجديدة للجرائم الالكترونية، لسد الفراغ القانوني ابتداء من قانون 04-15 المعدل والمتمم لقانون العقوبات، والذي عني بتجريم الاعتداءات على أنظمة المعطيات ثم لحقها بقانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاتصال والإعلام ومكافحته، وتعديل قانون العقوبات رقم 02/16، وبعد هذا كله يثار تساؤل مفاده:

- هل وفق المشرع الجزائري في معالجته للصور الجديدة للجرائم الالكترونية؟

وللإجابة على هذا السؤال سنتناول الموضوع من جانبين:

المبحث الأول: المعالجة القانونية من الناحية الموضوعية.

المبحث الثاني: المعالجة القانونية من الناحية الإجرائية.

المبحث الأول

المعالجة القانونية للجرائم الالكترونية من الناحية الموضوعية

أفرز التطور السريع للتكنولوجيا صورا جديدة للجريمة، جعل شراح القانون في مأزق حيال التعامل مع هذه الصور الجديدة، حيث أن طبيعة النص الجنائي وماله من خصوصية تحظر القياس الذي يؤدي إلى خلق جرائم لم ينص القانون عليها، تمنع القاضي من الاجتهاد عند التعامل مع الوقائع الجديدة، وبالمقابل فإن إفلات الجاني من العقوبة رغم الضرر الواقع بحجة تطبيق هذا المبدأ لا يستقيم وغاية القانون الجنائي التي تحمي المجتمع قبل أن تحمي الفرد.

- فكيف تعاملت التشريعات المقارنة تجاه تجريم هذه الصور الجديدة للجرائم الالكترونية؟

المطلب الأول: المعالجة القانونية في التشريعات المقارنة

اختلفت التشريعات المقارنة في طريقة تعاملها مع صور الجريمة المستحدثة، حيث اتجهت اتجاهات مختلفة، بخصوص تطبيق النص على صور الجريمة المرتكبة عبر الانترنت، وتفرعت إلى اتجاهين:

الفرع الأول: وضع نصوص جديدة للجريمة المعلوماتية

ذهب فريق إلى عدم تفسير النصوص القانونية في القانون الجنائي لتجنب خلق جرائم جديدة لم ينص عليها المشرع، وهو تطبيق لمبدأ الشرعية الجنائية، إذ يعد تفسير النصوص الجنائية خروجا عن مبدأ الشرعية، وليس من شأن الفقهاء أوالقضاة خلق جرائم جديدة، بل هو عمل السلطة التشريعية التي تسن القوانين، إذا رأت ضرورة لذلك، ويدعو هذا الاتجاه إلى وضع نصوص جديدة تجرم الصور الحديثة للجريمة المعلوماتية، إذ يعتبر هذا الإتجاه أن النصوص التقليدية لا تحيط بالصور المستحدثة للجريمة. وقد اختلف هذا الاتجاه في طريقة وضع النصوص الجديدة إلى فريقين:

01- فريق يرى بإدراج النصوص الجديدة في إطار قانون العقوبات العام على غرار المشرع الفرنسي الذي أدرج نصوص تجرم التلاعب بالمعطيات، من خلال إصدار قانون 88-19 الصادر في 1988/01/05 المتعلق بالغش المعلوماتي ضمن الفصل الثالث من قانون العقوبات الفرنسي، وقد أدرجه في قانون العقوبات لسنة 1992[(1)]. وكذلك فعل المشرع المغربي الذي أدرج باب تحت مسمى المس بنظام المعالجة الآلية للمعطيات احتوى على 08 فصول من 03-607إلى 11-607 ضمن تعديل قانون العقوبات لسنة 2003[(2)].

02- فريق آخر يرى بوضع قانون خاص بالجرائم الالكترونية مستقل عن قانون العقوبات، على غرار المملكة المتحدة التي سنت قانون الاحتيال 2006، والولايات المتحدة الأمريكية التي سنت قانون غش الحاسب وإساءة استخدامه 1986[(3)]، والمشرع الإماراتي في القانون الاتحادي الإماراتي للجريمة الالكترونية لسنة 2012[(4)].

الفرع الثاني: اتجاه تفسير النصوص الموجودة

على خلاف الاتجاه الأول، هناك من الفقه من ذهب إلى أن تفسير النص الجنائي لا يخالف مبدأ الشرعية إذا كانت عبارات النص تشمل وقائع ينطبق عليها النص الجنائي، طالما أن هذا النص بإمكانه الإحاطة بالصور المستحدثة للجرائم الالكترونية، ويعتبر هذا الاتجاه أن وضع نص جديد يعني تغيير النص في كل مرة يتطور فيها الفعل المجرم، وهو الأمر الذي يؤدي إلى عدم استقرار النصوص، فالأخذ بالتفسير المطابق للتطورات لا يعد خروجا عن مبدأ الشرعية، وما على أجهزة تنفيذ القانون إلا أن يقوموا بتفسير النص حسب التطورات الحاصلة في مجال الجريمة، وتطور وسائل ارتكاب الجريمة لا يعني عدم صلاحية النص الجنائي لتطبيقه على السلوك الإجرامي، وإنما هو صورة متطورة للجريمة التقليدية، ومن ذلك بعض الولايات الفيدرالية في الو.م.أ (ألاسكا) وفرجينيا، وكذلك اعتمدت كندا التفسير الموسع للنصوص التقليدية من أجل تجريم الصور الجديدة للجرائم الالكترونية[5].

المطلب الثاني: المعالجة القانونية في التشريع الجزائري

على غرار التشريعات المقارنة التي تصدت للجريمة المعلوماتية، فقد وجد المشرع الجزائري نفسه أمام صور جديدة للجريمة تختلف عن الجرائم التقليدية، من حيث الوسائل المستخدمة وتتطلب تدخلا تشريعيا لمواجهتها لهذا سن تعديلا في قانون العقوبات رقم 04/ 15،الذي أدرج فيه مواد تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

الفرع الأول: نطاق المعالجة القانونية للجرائم الالكترونية في التشريع الجزائري

اعتمد تدخل المشرع الجزائري في مواجهته للجرائم الالكترونية على أسلوبين حسب طبيعة هذه الجرائم التي تأخذ شكلين:

1- شكل يتجسد في صور جرائم تقليدية، يتم ارتكابها بوسائل الكترونية، وفي هذه الحالة فإن النصوص التقليدية يتم تطبيقها على الجرائم الالكترونية، ولا تعتبر إلا صور متطورة للجرائم التقليدية، فالجرائم التي تمس الأموال مثل النصب والاحتيال عبر الانترنت تعد من قبيل الجرائم التقليدية، التي تتم باستخدام وسائل تكنولوجية، ومن ثم تنطبق عليها النصوص التقليدية، وجرائم الاعتداء على الأشخاص مثل: السب والقذف عبر الشبكات الاجتماعية وتعد من قبيل الجرائم التقليدية التي تتم باستخدام التكنولوجيا، وبالتالي فالنصوص الموجودة في مواجهة هذه الأفعال كفيلة لتلائم الأفعال المرتكبة بوسائل تكنولوجية، ولا يوجد داع لإعادة صياغة نصوص جديدة لتجريم الأفعال المرتكبة بوسائل متطورة، فالأمر لا يتطلب سن تشريعات جديدة.

2- شكل يأخذ صور جديدة لجرائم حديثة تتميز كلية عن الجرائم التقليدية، وفي هذا الشكل لا يمكن بأي حال الاعتماد على النصوص التقليدية لتجريم هذه الأفعال، وبالتالي فإنه يتوقف على نصوص جديدة تجرم أفعال التعدي على المعلوماتية، والتي تتخذ شكل التعدي على البيانات المخزنة في ذاكرة الحاسوب، مثل: جرائم تدمير البيانات وإتلافها، التي يعاقب عليها القانون في المادة 394 مكرر فقرة 02.

وقد اعتمد المشرع الجزائري إصدار قوانين جديدة، لتجريم أفعال تمس الاعتداء على أنظمة المعالجة الآلية للمعطيات، ليس في قانون جديد وإنما أدرجها ضمن قانون العقوبات ضمن الفصل الثالث القسم السابع مكرر، بعنوان: المساس بأنظمة المعالجة الآلية للمعطيات[6]، وبالتالي فإن هذا القانون لا ينطبق على الجرائم التقليدية التي يتم ارتكابها بواسطة التكنولوجيا، إذ أن القانون الذي يضبطها هو النصوص التقليدية لقانون العقوبات، ونلاحظ أن المشرع لم يشر إلى النصوص التي تطبق في حال ارتكاب أفعال تشكل جرائم تقليدية عن طريق أنظمة المعلوماتية، فلا يوجد إشارة تدل على تشديد العقوبة أو اعتبارها ظرف تشديد، بشأن الجرائم المرتكبة بوسائل تكنولوجية، إن هذا الفراغ يؤدي إلى حالة من التخبط في تكييف الأفعال التي تشكل جرائم تقليدية بوسائل أنظمة المعلوماتية المتطورة. فهي من جهة تعد من أشكال الجرائم التي تم ارتكابها من خلال التغيير والتعديل في أنظمة المعلوماتية، مثل: الاحتيال والتزوير وانتحال الصفة والسب والقذف..، والتي لها صور وتصنيف ضمن الجرائم التقليدية، ومن جهة أخرى فإنها تعد من الجرائم التي تمس بأنظمة المعلوماتية وقد جاءت النصوص الجديدة لتجريمها، مما يؤدي إلى تعارض النصوص الجزائية في تكييفها وتطبيق العقوبة على مرتكبيها.

وبخلاف ذلك فقد نص المشرع الإماراتي في قانونه الاتحادي رقم (5) لسنة 2012 المتعلق بمكافحة جرائم تقنية المعلومات في المادة 48 منه على اعتبار استخدام شبكة المعلومات أو الانترنت أو أي نظام معلوماتي أو موقع الكتروني، أو أي وسيلة تقنية للمعلومات ظرفا مشددا عند ارتكاب جرائم أخرى لم ترد في القانون[7].

الفرع الثاني: تحليل لنصوص مواد تجريم المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري

جاءت مواد قانون العقوبات بعنوان القسم السابع مكرر1 تحت الفصل الثالث المتعلق بالجنايات والجنح ضد الأموال، وإدراج هذه المواد في هذا الفصل دليل على أن موضوع الاعتداء هو الأموال، أو بالأحرى البيانات والمعطيات التي تأخذ صفة المال.

إن الدراسة القانونية لمواد قانون العقوبات المتعلقة بمعالجة الأنظمة الآلية للمعطيات، وهي المواد من 394 مكرر إلى غاية 394 مكرر08[8] تعتبر إضافة جاء بها المشرع في سبيل مكافحة الجرائم الالكترونية، إلا أن هذه النصوص بالرغم من إضافتها في مكافحتها الجرائم الالكترونية حملت غموضا كبيرا من حيث الصياغة، وبعد قراءة النصوص المتعلقة بتجريم الأفعال التي تمس نظام المعالجة الآلية للمعطيات، ومقارنتها بنصوص تشريعية على غرار المشرع المغربي والمشرع الإماراتي، يمكن أن نخلص إلى عدة أوجه مقارنة:

1- من ناحية المصطلحات المستعملة:

نلاحظ غياب الكلمات المفتاحية في نصوص القانون، فقد جاءت نصوص مواد التجريم المتعلق بمعالجة الأنظمة الآلية للمعطيات غامضة، إذ لا يوجد في نصوص القانون ما يشرح الكلمات الدالة التي تبين كيفية قيام الركن المادي للجريمة، فهناك نقص فيما يخص كيفية ارتكاب الجريمة، وهذا يسبب

إشكالا عند تطبيق النصوص، ومثاله المادة 394 مكرر 02 حيث جاءت عبارات النص مقتضبة وغامضة في تبيان السلوك المادي للجريمة، مثل: عبارات: بحث، تصميم، توفير، تجميع...أين يصعب تصور وقوع الجريمة من خلال هذه العبارات.

وعلى خلاف ذلك، فإن المشرع الإماراتي في القانون الاتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، مهد في المادة الأولى منه بوضع تعريفات للمصطلحات المستعملة في نص القانون من قبيل: البرنامج المعلوماتي – نظام المعلومات الالكتروني – المستند الالكتروني – العنوان البروتوكولي وغيرها والتي من شأنها أن تزيل اللبس على المصطلحات التقنية، التي تبتعد عن اللغة القانونية المعروفة سابقا في النصوص التقليدية.

ويلاحظ أن المشرع تدارك الأمر في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها رقم 04/09 حين أفرد مادة تشرح المصطلحات المستخدمة في القانون، وحسنا فعل المشرع.

كما أن المشرع المغربي في صياغته لنصوص المواد المتعلقة بالمس بنظام المعالجة الآلية للمعطيات ابتعد عن استعمال العبارات التقنية، التي يصعب فهمها في مجال المعلوماتية في غالب المواد، وتميز بالبساطة في الأسلوب.

2- من ناحية التجريم:

تختلف النصوص التجريمية بين القوانين المقارنة من ناحية ذكر أوإغفال بعض الصور من الجرائم، حيث نسجل أن المشرع المغربي لم يستثن أفعال البقاء في نظام للمعالجة الآلية للمعطيات، حتى ولو كان الدخول إليه عن طريق الخطأ[9] وهذا ما يلاحظ في الفصل 03-607. كما أضاف التشريع الجنائي المغربي جريمة عرقلة سير نظام المعالجة الآلية للمعطيات في الفصل رقم 5-607، في حين لا نجد النص على هذه الجريمة في قانون العقوبات الجزائري.كما عاقب على إدخال معطيات فيه أو إتلافها أو حذفها أو تغيير المعطيات المدرجة فيه، أو تغيير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال، وهوما ينطبق على المادة 394 مكرر 01 إلا أن المشرع المغربي استخدم لفظ الاحتيال بدل الغش، ولفظ الاحتيال أقرب لأن لفظ الغش عادة ما يرتبط بالمواد والسلع.[10]

ومن حيث نطاق التجريم نسجل أن المشرع الجزائري لم يعمم صور الجرائم التقليدية، التي ترتكب بواسطة نظام معلوماتية، بل اقتصر على الجرائم التي تمس بالأنظمة المعلوماتية للمعطيات، بمعنى أن يكون محل الجريمة هو النظام المعلوماتي في حد ذاته، وهذا الأمر يجعل بعض النصوص التقليدية لا تنطبق على الجرائم التي ترتكب بواسطة التكنولوجيا، مثل: جريمة التزوير الالكتروني[11]، وخلافا لذلك فقد أفرد المشرع المغربي نصوصا خاصة بتزوير المعطيات واستعمالها، ونص على تجريم عملية تزوير وتزييف وثائق المعلومات أيا كان شكلها، إذا كان من شأن التزوير أو التزييف إلحاق الضرر بالغير[12].

ومن حيث التكرار في صور الجرائم وعدم توحيد المصطلحات: فالمادة 394 مكرر فقرة 01 والمادة 394 مكرر 1 تتشابهان لدرجة التطابق، حيث تناولت المادة الأولى تجريم الدخول أوالبقاء عن طريق الغش في جزء من منظومة المعالجة الآلية للمعطيات، وتكلمت عن مضاعفة العقوبة، إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة، في حين نصت المادة 394 مكرر 01 على عقوبة من 06 أشهر إلى 03 سنوات والغرامة لكل من أدخل عن طريق الغش معطيات في نظام المعالجة الآلية، أو أزال أو عدل عن طريق الغش المعطيات التي يتضمنها.

فالمشرع مرة يتكلم عن نظام (المادة 394 مكرر 01) ومرة يتكلم عن منظومة (المادة 394 مكرر) ومرة يتكلم عن حذف أو تغيير (المادة 394 مكرر) ومرة يتكلم عن إزالة أوتعديل (394 مكرر 01) وهو اختلاف في المفردات فقط مع اشتراكها في المعنى.

3- من ناحية العقاب:

تميزت عقوبات التشريع الجزائري بتشديد العقوبات المالية مقارنة بالحبس، إذ تصل الغرامة إلى 4.000.000دج في جرائم إدخال أو تعديل أو إزالة معطيات عن طريق الغش (المادة 394 مكرر01) وتصل الغرامة حدها الأقصى إلى 10.000.000دج في الجرائم التي تناولتها المادة 394 مكرر 02، ورفع المشرع الجزائري من عقوبة الحبس في حالة واحدة، وهي الجرائم المتعلقة بتقديم المساعدة لارتكاب أفعال إرهابية، وهي المنصوص عليها في المادتين 87 مكرر 11 و12 المعدلتين بموجب القانون رقم 02/16 أين يبلغ حدها الأقصى 10سنوات سجنا[13] في حين نسجل أن المشرع المغربي تميز بعقوبات أخف، مقارنة بما نص عليه المشرع الجزائري، إذ جعل للقاضي سلطة الاختيار بين عقوبة الحبس أو الغرامة في أغلب الجرائم بينما كان المشرع الإماراتي أكثر تشديدا من ناحية العقوبة، إذ اعتبر بعض صور الجرائم من قبيل الجنايات التي تنطبق عليها عقوبة السجن المؤقت والغرامة معا، على غرار المادة 28 من القانون[14]، إذا تعلق الأمر المساس بأمن الدولة والنظام العام، كما نجد في بعض الجرائم، أين تصل العقوبة إلى السجن المؤبد، وذلك في حالة محاولة تغيير نظام الحكم بأي وسيلة إلكترونية مستعملة (المادة 30).

وبشأن تشديد العقوبة في صفة الموظف فقد اتفق المشرع المغربي مع التشريع الإماراتي في تشديد العقوبة، إذا تعلق الأمر بممارسة هذه الأفعال من قبل الموظف أثناء ممارسة وظيفته أو بمناسبتها، وهو ما نقرأه في القانون الجنائي المغربي في الفقرة 02 من الفصل 04 -607، كما نلاحظ في القانون الاتحادي الإماراتي في المادة 03 منه[15] في حين لم يشر المشرع الجزائري إلى ظرف التشديد بشأن الموظف عند ارتكابه لأحد الجرائم التي نص عليها القانون رقم 15/04.

وقد أحال كل من التشريع الإماراتي والتشريع المغربي تطبيق عقوبات أشد من العقوبات التي ينص عليها القانون سواء من قانون العقوبات أو القوانين الأخرى الخاصة، حيث جاء النص عليها في التشريع المغربي من خلال عبارة (دون الإخلال بالمقتضيات الجنائية الأشد)، كما أفرد لها المشرع الإماراتي مادة مستقلة هي المادة 48 من القانون، وذهب المشرع الإماراتي أكثر من ذلك، حينما اعتبر استخدام وسيلة تقنية معلوماتية، أو شبكة معلومات، أو نظام معلوماتي الكتروني في حد ذاته ظرف تشديد، إذا

كان بغرض استخدام جرائم أخرى غير منصوص عليها في قانون مكافحة جرائم تقنية المعلومات، في حين أننا نجد أن المشرع الجزائري حصر حالة اللجوء إلى نصوص عقابية أشد، إذا تعلق الأمر باستهداف جريمة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام (المادة 394 مكرر 03).

تضمن القانون الإماراتي لمكافحة جرائم تقنية المعلومات، تدابير احترازية ضد المحكوم عليهم بارتكاب جرائم الكترونية؛ تتمثل في الوضع تحت المراقبة أوالحرمان من استخدام أي شبكة معلوماتية أو وسيلة تقنية معلوماتية يجوز للمحكمة النطق بها إذا رأت ضرورة لذلك، وغرض التدابير الاحترازية تأهيل المحكوم عليهم وإصلاحهم، وهو مسلك ندعو المشرع الوطني للاقتداء به، إذ الحاجة لإصلاح المحكوم عليهم في هذا النوع من الجرائم وتأهيلهم أكبر من تطبيق العقوبة السالبة للحرية التي لا تجدي مع هذا النوع من مجرمي المعلوماتية، كما أن المشرع الإماراتي انفرد دون غيره بالنص على ظروف التخفيف أو الإعفاء من العقوبة في حالة التبليغ عن الجرائم المرتكبة، أو المساعدة على الكشف عن هوية مرتكبيها وهو عامل مساعد على تحفيز الجناة للتبليغ عن الجرائم، والإدلاء بمعلومات تساعد السلطات العامة في الكشف عن الجرائم قبل ارتكابها.

وبالتالي يمكن القول أن التشريع الإماراتي والمغربي وسع في نطاق الحماية، من خلال إمكانية تطبيق عقوبات غير الواردة في النص، وبالمقابل فإن العقوبات التي أقرها المشرع الجزائري تميزت بمضاعفة العقوبة في جانبها المالي أكثر من جانبها البدني، وهوما يفقد من ميزة الردع، ويحد من سياسة مواجهة الجريمة الالكترونية، ونخلص إلى أن السياسة الجنائية للمشرع الإماراتي أفضل من نظيرتها المغربية والجزائرية. في مجال مكافحة الجرائم الالكترونية.

المبحث الثاني

المعالجة الإجرائية للجرائم الالكترونية

إنّ الإشكال الذي يواجه أجهزة القضاء والشرطة القضائية لا يتمثل في الفراغ التشريعي للنصوص التجريمية بقدر ما هي كامنة في طرق ضبطها وإثباتها، وهوما يرجع إلى افتقاد الآثار التقليدية التي قد تتركها أي جريمة ذات طبيعة معلوماتية، وإذا كان البحث في مسألة قدرة القواعد الإجرائية التقليدية في ضبط جريمة الكترونية أمرا صعبا، فهذا ما جعل مسألة ملاءمة الإجراءات الجنائية في البحث والتحري مع خصوصية هذا النوع من الجرائم تستأثر باهتمام المشرعين.

وقد استحدث المشرع الجزائري نصوصا تنظم الإجراءات المتعلقة بالبحث والتحري في الجريمة الالكترونية، وهو ما عرفه بصدور القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال رقم 04/09، وهو مسلك انفرد به المشرع الجزائري دون غيره من التشريعات العربية، التي لم تورد قانونا خاصا إجرائيا في البحث والتحري على الجرائم الالكترونية، وعلى هذا الأساس ستكون المقارنة مع التشريعات الأجنبية، التي أدخلت تعديلات في قوانينها الإجرائية لمواجهة الجريمة الالكترونية، وأبرزها التشريع الفرنسي.

وتعكس النصوص الإجرائية مدى الضمانات المتوفرة في مراحل الدعوى العمومية، من خلال حماية الحريات والضمانات التي توفرها للأشخاص المتابعين، وحدود تدخل السلطات القضائية في البحث والتحري ومتابعة الأشخاص وفق القانون، وفي هذا الجزء نناقش مجال حماية الحريات والضمانات التي كفلها المشرع الجزائري، من خلال النصوص الإجرائية التي وضعها لمواجهة الجريمة الالكترونية.

المطلب الأول: المعالجة الإجرائية واحترام مبدأ المشروعية

يشترط في إجراءات البحث والتحري في الجريمة عموما سلامتها ومشروعيتها، وموافقتها للقانون حتى تحقق العدالة منها، وفي الجرائم الالكترونية بالخصوص، لذا فإن الخصوصية التي تتميز بها تجعل من احترام مبدأ المشروعية والموافقة للقانون، تحديا للمشرعين بالنظر إلى أن القانون لم يعرف مثل هذه الإجراءات سابقا، إضافة إلى أن طبيعة آثار الجريمة تجعل التعامل معها وفق مبدأ المشروعية، والموافقة صعبا نوعا ما في ما يخص استخلاص الدليل الجنائي، وتتناول مسألة المشروعية عنصرين: مشروعية الإجراءات المتخذة في حد ذاتها ومشروعية استخلاص الدليل.

الفرع الأول: المشروعية في الإجراءات

أقر المشرع الجزائري مجموعة من الإجراءات لمواجهة الجريمة الالكترونية، منها ذات طابع تقليدي على غرار التفتيش، ومنها ما هو مستحدث على غرار التسرب الالكتروني.

1- المشروعية في إجراء التفتيش:

إن سهولة محو آثار الجريمة في جرائم المعلوماتية بصفة عامة، يتطلب السرعة في اتخاذ إجراءات التفتيش للحفاظ على أدلة الجريمة، إذ أن إتباع الإجراءات التقليدية المتمثلة في الحصول على الترخيص من السلطة القضائية قد يؤدي إلى ضياع دليل الجريمة هذا من جهة، ومن جهة أخرى فإن القفز على الضمانات القانونية لمشروعية التفتيش تؤدي إلى انتهاك الحريات، بدعوى خصوصية الجريمة الالكترونية وإجراءاتها، ولذلك ينبغي إيجاد توازن بين خصوصية البحث والتحري في الجرائم الالكترونية، مع الحفاظ على الحريات الأساسية، وقد حافظ المشرع على ضوابط التفتيش المنصوص عليها في قانون الإجراءات الجزائية، وأعاد التذكير بها في قانون 04/09 في المادة 05 القيام بالتفتيش بناء على أمر من السلطة القضائية، وعليه فإن القانون 04/09 أحال على قانون الإجراءات الجزائية في مسألة تطبيق قواعد التفتيش، وأحاط إجراء التفتيش بضمانات؛ وهي أن يظل القائم بالتفتيش مقيدا إلى غاية صدور أمر بالتفتيش من القاضي المختص، وتراعى في عملية صدور الإذن استخدام أي وسيلة اتصال لإعلام المكلف بالتفتيش السماح له القيام بالتفتيش، خلافا لما هو معمول به في قانون الإجراءات الجزائية في الجرائم التقليدية، حيث يمكن الاستعانة بالفاكس أو رسالة نصية أو أي وسيلة الكترونية للتبليغ.

وبشأن مسألة تمديد التفتيش فقد نظم المشرع الجزائري مسألة تمديد التفتيش لمنظومة معلوماتية أخرى، غير التي يقع عليها التفتيش في القانون 04/09، وجاء النص عليها في المادة 05 الفقرة 02[16] في ما يخص بتفتيش المنظومات المعلوماتية، وعلى خلاف التفتيش في الجرائم التقليدية التي

ينظمها قانون الإجراءات الجزائية، فإن المشرع الجزائري في حالة تطلب الأمر تمديد التفتيش لمحل آخر اقتصر على مجرد إعلام السلطات القضائية بتمديد التفتيش، لضرورة سرعة الإجراءات والحيلولة دون محو البيانات والمعطيات التي تشكل دليلا للتجريم، في حين يشترط في الجرائم التقليدية ضرورة الحصول على إذن من السلطات القضائية، ويختلف الإذن عن الإعلام في كون الإذن عمل قضائي من السلطة القضائية يتطلب شكليات لصدوره، بينما لا يشترط الإعلام ذلك، فهو مجرد إشعار للسلطة المختصة بتمديد التفتيش.

كما نظم المشرع الجزائري مسالة تمديد التفتيش في الجرائم الالكترونية في المادة 05 فقرة 03، إذ أجاز تمديد التفتيش لأنظمة معلوماتية خارج الإقليم الوطني، إذا دعت الضرورة ذلك، حيث تخول المادة للجهات المختصة توسيع نطاق التفتيش، ليشمل المعطيات المخزنة في منظومة معلوماتية تقع خارج القطر الوطني، وقد يشكل هذا الجواز انتهاكا لسيادة الدول، وتحسبا لذلك فقد ربط المشرع الجزائري اتخاذ هذه الإجراءات بوجود اتفاقيات بين الدول، في نطاق المساعدة القضائية المتبادلة ووفقا لمبدأ المعاملة بالمثل.

وقد سبق المشرع الفرنسي النص على هذا الإجراء، الذي أجاز تمديد التفتيش خارج الإقليم الفرنسي كلما كان ذلك ممكنا، حيث نص عليه في المادة 1/57 من قانون الإجراءات الجزائية الفرنسي المضافة بموجب قانون الأمن الداخلي رقم 239-2003، والتي تنص: "إذا تبين مسبقا أن هذه المعطيات مخزنة في نظام معلوماتي موجود خارج الإقليم الوطني أو أنها متاحة انطلاقا من النظام الرئيسي، يمكن الحصول عليها من طرف ضابط الشرطة على وجه السرعة كلما دعت ضرورة التحقيق ذلك، على أن يتم إبلاغ السلطات المختصة في الدولة التي تتواجد هذه المعطيات على إقليمها، فيما بعد وفقا للضوابط المنصوص عليها في المعاهدات الدولية "[17].

2- التسرب الالكتروني:

عرف قانون الإجراءات الجزائية الجزائري التسرب في المادة 65 مكرر 12 بالقول: "يقصد بالتسرب 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"[18].

وأجاز المشرع اللجوء إلى هذه الوسيلة، التي تعد أسلوبا من أساليب التحري الخاصة، في جرائم ذكرها المشرع على سبيل الحصر، 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.[19]، ويتم اتخاذ الإجراءات بعد الحصول على إذن قضائي من وكيل الجمهورية أو قاضي التحقيق، ويعد هذا ضابطا لوقوع هذه الإجراءات التي تمس بخصوصية الأفراد وتقع باطلا الإجراءات التي لم تتوفر فيها إذن من السلطة القضائية.

يخول القانون للمتسرب انتحال هوية مستعارة، كما يسمح له بارتكاب أعمال تعد جريمة في نظر القانون تحت ظرف الضرورة وهي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم، أو مستعملة في ارتكابها.

-استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي، وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ والاتصال[20].

ويتم التسرب من خلال استعمال العون المتسرب هوية مستعارة في مواقع الانترنت، يشتبه قيام أصحابها بعمليات النصب والاحتيال، وفي إحدى العمليات تمكنت الشرطة القضائية الفرنسية عن طريق إجراء التسرب لأحد أعوانها، والذي قام بالدخول في موقع الكتروني، عبارة عن منتدى مخصص للحديث عن تقنيات تزوير البطاقات البنكية، وعن طريق هذا الموقع تمكنت الضبطية من الكشف عن هوية المحتالين على البطاقات البنكية، واستخدام محادثات الدردشة كدليل إثبات ضد الفاعلين[21].

الفرع الثاني: المشروعية في استخلاص الدليل (نحو التخلي عن التمسك بمشروعية الدليل الجنائي في الجرائم الالكترونية)

أمام التحديات التي تطرحها الجرائم الالكترونية عامة، قد يصعب على الأجهزة المكلفة بالبحث والتحري التقيد ببعض المبادئ الإجرائية، التي تقتضيها عملية استيفاء الدليل الالكتروني، الذي يقود إلى كشف الفاعل، مما دعى بعضهم إلى إعادة النظر في التمسك بمبدأ مشروعية الدليل، ومدى إمكانية ترجيح متطلبات العدالة على فكرة شرعية الدليل.

إن الملاحظ أن معظم التوجهات القضائية وعلى وجه الخصوص الفرنسية، بعدما كانت حريصة على مسألة الشرعية في الحصول على الدليل الجنائي، وذلك استنادا على بعض القرارات الصادرة عنها، بدأت تتخذ اتجاهات أخرى نحو الوصول إلى الحقيقة، حتى ولو كانت طريقة تحقيق ذلك غير مشروعة، ومن الأمثلة على ذلك القرار الصادر عن الغرفة الجنائية بمحكمة النقض الفرنسية، بتاريخ 2012/01/31 والذي جاء فيه "إن التسجيلات المتحصل عليها بشكل سري لا تنسجم مع مقتضيات المادة 170 من قانون الإجراءات، ومن ثم يجب الحكم بإلغائها لكن من الممكن أن يتم مناقشتها أثناء الخصومة"[22] مما يفيد أن القضاء الفرنسي لم يرفض الدليل المأخوذ بصفة غير مشروعة، بل سمح بالاعتماد عليه ومناقشته أثناء الجلسة، ويفهم منه اتجاه القضاء إلى التخلي عن فكرة رفض الدليل غير المشروع دون مناقشته[23].

وفي هذا الصدد قررت محكمة النقض الفرنسية في قرارها المؤرخ في 2014/04/30 بعدم وجود افتعال لجرائم معلوماتية متمثلة في النصب والاحتيال، وتزوير بطاقات بنكية من خلال قيام مكتب التحقيقات الفيدرالي FBI بإنشاء موقع الكتروني عبارة عن منتدى مخصص للحديث حول تزوير البطاقات البنكية، تم وضعه شهر جوان 2010 تحت اسم "carderprofit" وبواسطته تم التسرب وتسجيل هوية، ومكان تواجد المحتالين على البطاقات البنكية.

وبفضل هذا المنتدى تمكنت الضبطية الفرنسية من توقيف وتفتيش المتهم بناء على معلومات من FBI ، تثبت تورط المعني في أعمال احتيال باستعمال بطاقات بنكية مزورة، وتمت إدانته على أساسها.

ولجأ المحكوم عليه إلى الطعن ضد الحكم بالنقض لدى محكمة النقض، مستندا إلى عدم مشروعية استخلاص الدليل المستمد، لكون الشرطة القضائية ساهمت في استدراج الطاعن لارتكابه الأفعال المنسوبة إليه، في حين اعتبرت محكمة النقض أن الموقع الالكتروني للمراقبة وتسجيل الرسائل المتبادلة بالمنتدى سمحت فقط؛ من تجميع الإثباتات لارتكاب جريمة الاحتيال في البطاقات البنكية، ومن تحديد مرتكبيها، ولا يوجد أي عنصر يثبت أن الغرض منه كان تشجيع الأشخاص المتصفحين للمنتدى من الانتقال إلى مرحلة الفعل والاحتيال[24].

وأكدت محكمة النقض الفرنسية على ضرورة التمييز بين رفض محكمة الموضوع، قبول دليل متحصل عليه بطريق غير مشروع من ناحية، وبناء المحكمة لاقتناعها الشخصي على مثل ذلك الدليل من ناحية أخرى، فالقاعدة أن القاضي الجنائي (قاضي الجنايات) يتعين عليه أن لا يحرم خصما من تقديم دليل، ولو كان قد حصل عليه بطريقة غير مشروعة، لتمكنه من التوصل إلى الحقيقة، ولكن تقديم هذا الدليل لا يعني قبوله في تكوين عقيدة القاضي، فالقاضي له الحرية في بيان قوة الدليل في الإثبات تبعا لاقتناعه الذاتي، ويعد هذا الحكم تراجعا عن التمسك بالتطبيق الصارم لقاعدة المشروعية في استخلاص الدليل، وقبول مناقشته وطرحه في الجلسة والأخذ به إذا اقتنع القاضي بقوته الإثباتية، بغض النظر عن مشروعية الحصول عليه، وهو تكريس للوصول إلى الحقيقة بدل المشروعية في الوصول إلى الدليل[25].

ولقد نظم قانون الإثبات الأمريكي مسألة الدليل الالكتروني، فقد نصت المادة 3/1001 على أنه: "إذا كانت البيانات مخزنة في حاسب أو آلة مشابهة، فإن أي مخرجات طابعة منها أومخرجات مقروءة برؤية العين تبرز انعكاسا دقيقا للبيانات تعد بيانات أصلية"[26]، وبناء عليه فقد لجأ القضاء الأمريكي إلى إعطاء الدليل الالكتروني حجية في الإثبات لا تدحض إلا بدليل قاطع، معتبرا أن الدليل المتحصل عليه يعد حجة ما لم يوجد دليل يثبت تغيير في مضمونه، وبهذا يكون قد أرسى مبدأ يفيد بأن وجود احتمال بتعديل البيانات الموجودة في الحاسوب غير كاف للقول بعدم جدارة الدليل[27].

وبالمقابل فإنّ المشرع الوطني لم يتناول مسألة الدليل الالكتروني بالخصوص مقارنة بالأدلة الأخرى، إذ جميعها تخضع للمادة 212 من قانون الإجراءات الجزائية في مسألة الإثبات، بالرغم من أن المشرع الوطني نظم إجراءات المتابعة في الجرائم الالكترونية، من خلال القانون 04/09 إلا أنه لا يوجد ما ينظم مسألة قيمة الدليل المستمد من الجرائم الالكترونية، ونطاق المشروعية في الحصول عليه.

إن خصوصية الدليل غير المادي في الجريمة الالكترونية، يحتم علينا إعادة النظر في التمسك بفكرة مشروعية الدليل، إذ أن إقصاء أي دليل لا يتوفر على المشروعية من شأنه أن ينجي الفاعل من العقوبة، ويسقط التهمة الموجهة إليه بناء على عدم وجود دليل مشروع، و هذا القول مناف لمتطلبات العدالة، التي تسعى إلى متابعة الجاني، والتمسك بالمشروعية في الجرائم التقليدية، إلا أن خصوصية الجريمة الالكترونية تتطلب الأخذ بمبدأ المشروعية، بصورة نسبية وليست مطلقة، وتتمثل في قبول الدليل غير المشروع في حالة مناقشته وعدم استبعاده.

المطلب الثاني: المعالجة الإجرائية واحترام الحريات الأساسية

تصطدم إجراءات البحث والتحري بمسألة تتعلق بالحريات الأساسية للأشخاص، وهي الضمانة التي كفلها الدستور إذ أن الحياة الخاصة تتعلق بحرمة السكن – والاستئثار بالبيانات الشخصية والاسمية – وسرية الاتصالات والمكالمات – والحق في حماية الصورة الشخصية، كل هذه العناصر تشكل الخصوصية للحياة الشخصية، ولا شك أن إجراءات التفتيش والبحث في البيانات وأدلة الجريمة المرتكبة بواسطة الكمبيوتر سيطال أحد عناصر هذه الخصوصية، مما أوقع التشريعات المقارنة في تضارب تجاه تقييد أو منع التعدي على الخصوصية، وعليه كان لزاما توافر ضمانات لحماية خصوصية الأفراد.

الفرع الأول: ضمانات حماية المعطيات الخاصة

تعتبر قضية انتهاك الخصوصية من بين أهم القضايا المطروحة في مجال التحقيق في الجرائم المتعلقة بالانترنت، خاصة فيما يتعلق بالتفتيش والمعاينة عبر الانترنت، حيث يتطلب فحص مختلف المعاينات عبرها، بما في ذلك تفتيش البريد الالكتروني مثلا الأمر الذي يجعل خصوصيات الأفراد على المحك، خاصة إذا كان التفتيش والمعاينة متعلق بحسابات متصلة بالحاسوب محل التحقيق، فالحق في الخصوصية بمثابة عائق دون إجراء تحقيق على أكمل وجه، فيما يخص الجرائم المرتكبة عبر الانترنت.

إن حيز الاعتبار بالخصوصية في الجرائم الالكترونية والحياة الخاصة، أصبح ضيّقا نظرا لصعوبة مكافحة الجريمة، دون الكشف عن سرية الاتصالات والبيانات المتعلقة بالمشتبه به، أو حتى ضمن دائرة الأشخاص الذين يتعاملون معه، وهي من دواعي البحث والتحقيق في الجريمة، إذ أنّ المعلومات التي يتم الكشف عنها ستظلّ سرية في التحقيق، ويضمن القانون عدم نشرها وكتمها، الأمر الذي يجعل الحياة الخاصة في هذه الحالة فقط مكشوفة من قبل رجال القضاء، ومزوّدي الخدمة (Les Opèrateurs) الملزمون بكتمان العمليات التي ينجزونها بناء على طلب المحققين، وكذا المعطيات التي يتحصلون عليها تحت طائلة العقوبة والمتابعة بتهمة إفشاء سرية التحقيق[28]، وقد حدد القانون مدة حفظ البيانات والتسجيلات المتعلقة بالأشخاص، والتي يلزم مقدمو الخدمات الاحتفاظ بها سنة واحدة ابتداء من تاريخ التسجيل، وهي نفس المدة في القانون الفرنسي التي تعتبر معقولة، ولا تمس بالحياة الخاصة، خاصة إذا ما تم مقارنتها بما ينص عليه القانون الألماني والتي تصل إلى 05 سنوات.

ورتب المشرع الجزائري المسؤولية الجزائية لمن يقوم باستخدام المعلومات المتحصل عليها في غير الغرض الذي خصصت له، وقد أشار إلى ذلك في المادة 09 من القانون رقم 09-04، ولكن تبقى مسألة تجريم إفشاء الأسرار والبيانات المتحصل عليها غير كاف، مقارنة بما تسببه من أضرار نفسية على الأشخاص عند تداول معلوماتهم، ونظرا لما تمتلكه السلطات العامة من إمكانيات وأجهزة اتصالات تتيح لها التوصل إلى معلومات الأفراد والبيانات الشخصية، مما يشكل في بعض الأحيان تجاوزا لها من خلال الوصول بدون إذن لمعطيات خاصة، ونعتقد أن إنشاء هيئة إدارية مستقلة تعمل على مراقبة مدى احترام السلطات العامة لخصوصية الأفراد، يشكل ضمانا من تعدي أجهزة القضاء والشرطة عند البحث والتحري في الوقائع التي من المحتمل أن تشكل جرائم، وفي هذا السياق صدر مؤخرا قانون رقم 07/18

الذي يهدف إلى تحديد قواعد حماية الأشخاص الطبيعيين، في مجال معالجة المعطيات ذات الطابع الشخصي، والذي نص على إنشاء سلطة وطنية لحماية المعطيات ذات الطابع الشخصي في انتظار تنصيبها[29] على غرار ما هو معمول به في المغرب، الذي استحدث ما يسمى باللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي بموجب القانون 09/08[30].

الفرع الثاني: ضمانات المراقبة الالكترونية

تعرف المراقبة الالكترونية (surveillance électronique) بأنها عملية مراقبة شبكة الاتصالات باستخدام التقنية الالكترونية، تجمع بواسطتها بيانات ومعلومات حول المشتبه فيه لتحقيق غرض أمني يقوم بها مراقب ذوكفاءة تتماشى مع نوع الجريمة التي يحقق فيها [31]، وهوإجراء وقائي يمكن أن تلجأ إليه السلطة القضائية حتى قبل وقوع الجريمة، في حالة اشتباه بارتكاب أفعال تمس بالنظام العام والأمن كما نصت عليه المادة 04 فقرة أ و ب من القانون رقم 04/09 المتعلق بالوقاية من جرائم الاتصالات ومكافحتها.

لقد قيد المشرع الجزائري في قانون 04/09 عمليات إجراء ومراقبة الاتصالات الالكترونية[32] بأمر من السلطة القضائية، لما لهذه الإجراءات من مساس بحقوق وحريات الأشخاص، وبالتالي لا يمكن إتخاذ إجراءات مراقبة الاتصالات الالكترونية، وتسجيلها وتجميعها دون الحصول على إذن من السلطة القضائية، وهذا ما نصت عليه الفقرة 02 من المادة 04 من القانون سالف الذكر، لكن ما يلاحظ على هذه المادة أن المشرع لم يضع جزاء على مخالفة هذا الإجراء، واقتصر على عبارة "لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية"، وعلى خلاف ما هو موجود في قانون الإجراءات الجزائية، حيث رتب البطلان عند مخالفة الإجراءات الخاصة في متابعة الجرائم المذكورة. وعلى سبيل الحصر في المادة 65 مكرر 05 والتي من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، ونجد النص على البطلان في المادة 65 مكرر 15، و نهيب بالمشرع أن يستدرك هاته النقطة ويشير إليها، إضافة إلى ذلك فإن المشرع أغفل ترتيب المسؤولية الجزائية في حالة القيام بإجراءات مراقبة الاتصالات الالكترونية دون إذن من السلطة القضائية، إذ أنه يعد انتهاكا لحق الحياة الخاصة وهو حق دستوري كفله الدستور في المادة 46 منه والتي تنص: "لا يجوز انتهاك حرمة الحياة الخاصة وحرمة شرفه، يحميهما القانون، وسرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم".

فالدستور يحيل على القانون المعاقبة على انتهاك الحقوق والحريات، في حالة مخالفتها للإجراءات ونحن نهيب بالمشرع النص عليها حماية لحقوق الأفراد من المساس بالحريات والحياة الخاصة.

وقد سبق قانون الإجراءات الجزائية أن نص على مشروعية إجراء تسجيل الأصوات واعتراض المراسلات والتقاط الصور، في تعديل لقانون الإجراءات الجزائية رقم 22/06 في المواد 65 مكرر 05 وما يليها، وهي إجراءات ترتبط بجرائم محددة على سبيل الحصر، وهي جرائم المخدرات – الجريمة المنظمة العابرة للحدود الوطنية – جرائم المساس بأنظمة المعالجة الآلية للمعطيات – تبييض الأموال – الإرهاب

– الجرائم المتعلقة بالتشريع الخاص بالصرف –جرائم الفساد، وقد أدرج المشرع الجزائري جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضمن هذه الجرائم، وهي ذات طبيعة الكترونية، وهي إجراءات تتفق مع الإجراءات المتخذة في قانون 04/09، وكان بإمكان المشرع الجزائري تفادي تكرار هذه الإجراءات في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ومكافحتها وإحالتها إلى قانون الإجراءات الجزائية.

الخاتمة:

تعد الجرائم الالكترونية ظاهرة عالمية تعاني منها جميع التشريعات الوطنية، مما يدعونا إلى التعاون المتبادل بين الدول، سواء على الصعيد الثنائي أو الجماعي، لمواجهة الصور المختلفة الجرائم الالكترونية، ولقد استفاد المشرع الجزائري من تطور النصوص القانونية في التشريعات المقارنة، التي كانت سباقة في مواجهة هذا النوع من الجرائم وأخذ منها، غير أن الواقع يفرض ضرورة تنقيح وتحيين النصوص، مما يعزز فعالية المواجهة وتحقيق الردع العام تجاه الإجرام الحديث.

وفي الختام نسجل أهم النتائج المتوصل إليها وأهم التوصيات التي ندعو لها:

- النتائج:

1- تصدى المشرع الجزائري للجرائم الالكترونية بإدراج مواد ضمن قانون العقوبات، طبع عليها الغموض والتشابه في صور الجرائم، وتكرار في المصطلحات بمفردات مختلفة.

2- لم يشر المشرع إلى إمكانية تطبيق عقوبات أشد في حالة تعدد صور الجريمة، أو التكييف في النصوص الأخرى التقليدية، بخلاف ما نجده عند المشرع المغربي.

3- أغفل المشرع الوطني ذكر الجرائم الأخرى المرتكبة بوسائل تكنولوجية، والتي لم ترد في نص القانون بخلاف المشرع الإماراتي، الذي اعتبرها ظرف تشديد عند تطبيق العقوبة.

4- لم يشر المشرع إلى مسألة تقدير قيمة الدليل الالكتروني بين أدلة الإثبات.

5- انفرد المشرع الجزائري دون غيره من التشريعات العربية بوضع قانون إجرائي لمواجهة الجرائم الالكترونية.

6- إن خصوصية الجريمة الالكترونية تتطلب الأخذ بمبدأ المشروعية، بصورة نسبية وليست مطلقة في الشق الإجرائي، مع قبول الدليل غير المشروع، وطرحه للمناقشة وعدم استبعاده.

7- أغفل المشرع توقيع جزاء البطلان على إجراءات مراقبة الاتصالات الالكترونية من دون إذن بخلاف ما هو منصوص عليه في قانون الإجراءات الجزائية.

- التوصيات:

1- وضع إطار مفاهيمي للمصطلحات يفسر المقصود منها، ويقطع الشك والتأويل.

2- الإشارة إلى إمكانية تطبيق عقوبات النصوص التقليدية على الجرائم الالكترونية في حالة التشديد لضمان العقوبة والردع، وملاءمة النصوص التقليدية لهذه الجرائم.

3- النص على توقيع جزاء البطلان في حالة مخالفة إجراءات مراقبة الاتصالات الالكترونية في قانون 04/09، بالإضافة إلى ترتيب المسؤولية، والمتابعة الجزائية لانتهاك حرمة الحياة الخاصة.

4- إنشاء هيئات إدارية مستقلة، تعمل على مراقبة ومنع التجاوزات في مسائل التعدي على خصوصية الأفراد التي يمكن أن ترتكبها السلطات العامة.

الهوامش:

(1) Voir : L323-1jusqu323-8 de code pénal français sous titre : des atteintes aux systèmes de traitements automatisée de données.

(2) انظر: قانون 07/03 الصادر بتاريخ 2003/11/11 المتمم لمجموعة القانون الجنائي المتعلق بنظم المعالجة الآلية للمعطيات.

(3) محمد طارق الخن : جريمة الاحتيال عبر الانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2011 ص104.

(4) انظر: قانون الاتحادي الإماراتي رقم (5) لسنة 2012 بشأن مكافحة جرام تقنية المعلومات.

(5) يونس عرب : الاتجاهات التشريعية للجرائم الالكترونية ، ورقة بحث مقدم بمناسبة ورشة عمل (تطوير التشريعات في مكافحة الجرائم الالكترونية) مسقط- عمان ، 02إلى 04 أفريل 2006.

(6) ينظر: المواد من 394 مكرر إلى غاية 394 مكرر 07 من قانون العقوبات المعدل و المتمم بالقانون 04-15، ج ررقم 71.

(7) تنص المادة 48 من القانون رقم (5) لسنة 2012 على ما يلي: "لا يخل تطبيق العقوبات المنصوص عليها في هذا المرسوم بقانون بأي عقوبة أشد ينص عليها قانون العقوبات أو أي قانون آخر ".

(8) أضيفت المادة 394 مكرر 08 وفق قانون 16-02 المؤرخ في 19 يونيو 2016 المتمم للأمر 66-156 و المتضمن قانون العقوبات، ج رعدد 37 بتاريخ 22يونيو 2016.

(9) ينظر الفصل 3-607 من الباب العاشر تحت عنوان :المس بنظم المعالجة الآلية للمعطيات أضيف هذا الباب بمقتضى القانون رقم 07/03 الصادر بتاريخ 2003/11/11 ، الجريدة الرسمية عدد 5171 بتاريخ 2003/12/22.

(10) انظر المواد 429 إلى 432 من قانون العقوبات المتعلقة بالغش في السلع والتدليس في المواد الغذائية والطبية.

(11) أمال قارة : الحماية الجزائية للمعلوماتية في التشريع الجزائري دار هومة ، الجزائر، ط2 ، 2007 ، ص136،137

(12) نص الفصل 07 -607 : (دون الإخلال بالمقتضيات الجنائية الأشد يعاقب بالحبس من سنة إلى خس سنوات و الغرامة من 10.000إلى 1.000.000 درهم كل من زور أو زيف وثائق المعلوميات أيا كان شكلها إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير) .

(13) ينظر: المادتين 87 مكرر 11 و12 من القانون رقم 16/02 مؤرخ في 19 يونيو 2016 المتمم للأمر 156/66 المتضمن قانون العقوبات ، ج رعدد 37 بتاريخ 22 يونيو 2016.

(14) تنص المادة 28 " يعاقب بالسجن المؤقت و الغرامة كل من أنشأ أو أدار موقعا إلكترونيا أو أشرف عليه أو استخدم معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات بقصد التحريض على أفعال أو نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى من شأنها تعريض الدولة أو مصالحها العليا للخطر أو المساس بالنظام العام".

(15) تنص المادة 03 : "يعاقب بالحبس مدة لا تقل عن سنة واحدة و الغرامة التي لا تقل عن 250.000 درهم ولا تجاوز 1.000.000 درهم أو بإحدى هاتين العقوبتين كل من ارتكب الجرائم المنصوص عليها في البندين (1) و (2) من المادة 02 بمناسبة أو بسبب تأدية عمله ."

(16) تنص الفقرة 02 من المادة 05 من القانون 04/09 : (إذا كانت هناك أسباب تدعو إلى الاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك).

(17) article 57/1 LOI n° 75-1426 du 31 Decembre 1957 de code de procedure penale français.

(18) المادة 65 مكرر 12 من قانون الإجراءات الجزائية رقم 22/06 المعدل والمتمم.

(19) ينظر المادة 65 مكرر 05 من قانون 06-22 المعدل و المتمم لقانون الإجراءات الجزائية.

(20) ينظر: المادة 65 مكرر 14 من قانون الإجراءات الجزائية 06-22 المعدل والمتمم .

(21) مناصرة يوسف: الدليل الالكتروني في القانون الجزائي، دار الخلدونية، الجزائر، 2018، ص، ص 101،99.

(22) Cass.Crim,31Janvier 2012,n11-85-464,Bulletin Des Arrêts , Chambre criminelle, N1 janvier 2012.

(23) ياسين زوباير إثبات الجريمة الالكترونية بين قيود الشرعية ومتطلبات العدالة، مقال منشور بمجلة الفقه والقانون، العدد 31، ماي 2015.

(24) مناصرة يوسف : الدليل الالكتروني في القانون الجزائي، دار الخلدونية، الجزائر ، 2018، ص، ص 101،100.

(25) Voir :crim 11Juin 2002 , Bull.crim 131.

"لا يسمح أي حكم قانوني لقضاة الجزائي استبعاد الأدلة التي قدمها الطرفان فقط على أساس أنه تم الحصول عليها بصورة غير مشروعة أو غير منصفة، والأمر متروك لهم لتقدير قيمتها الثبوتية بعد تقديمها للمناقشة الحضورية"، مشار إليه مناصرة يوسف: مرجع سابق، صن 133.

(26) Rule 1001of Federal Rules of Evidence .(usa) (d) An "original" of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, "original" means any printout — or other output readable by sight — if it accurately reflects the information. An "original" of a photograph includes the négative or a print from it" .

(27) محمد طارق عبد الرؤوف الخن: مرجع سابق، 358.

(28) ينظر: الفقرة الأخيرة من المادة 10 من القانون 04/09. والمادة 301 من قانون العقوبات.

(29) ينظر: المادة 22 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر عدد 34، الصادرة بتاريخ 10يونيو 2018.

(30) لمزيد من المعلومات يرجى زيارة الموقع الرسمي للجنة على صفحة الانترنت: https://www.cndp.ma/a

(31) بن شهرة شول، مرجع سابق، الحماية الجنائية للتجارة الالكترونية، أطروحة مقدمة لنيل شهادة دكتوراه في الحقوق، جامعة محمد خيضر بسكرة، 2011/2010 ص219.

(32) يقصد بالاتصالات الالكترونية حسب المادة 02 من قانون 04/09 : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

المعالجة القانونية للجرائم الالكترونية في القانون الجزائري والتشريعات المقارنة
(التشريع المغربي والإماراتي نموذجا) ـــــــ