الجزء الثالث

مجلة الدراسات القانونية المقارنة

EISSN:2600-6154 المجلد 07/ العـــدد01 (2021)، ص.ص. 1542-1560 ISSN:2478-0022

الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الاتصال ودورها في تفتيش نظم المعلوماتية

The National Authority for the Prevention of Media Crime and Communication Technology and its role in inspecting information systems

الدكتورة: حكيمة بوكحيل

Dr. Hakima BOUKEHIL

كلية الحقوق والعلوم السياسية، أستاذة محاضرة ب، جامعة محمد الشريف مساعدية، سوق اهراس

Faculty of Law and Political Science, University of Mohamed-ChérifMessaadia Souk Ahras

Email:hakimaboukehil23@gmail.com

الأستاذة: سامية بن عديد

Assistant Professor: Samia BEN ADID

كلية الحقوق والعلوم السياسية، أستاذة مساعدة أ، جامعة محمد الشريف مساعدية، سوق اهراس

Faculty of Law and Political Science, University of Mohamed-ChérifMessaadia Souk Ahras

Email: samiabenadid@gmail.com

تاريخ إرسال المقال: 2020/12/02 تاريخ القبول:2021/05/04 تاريخ النشر:2021/06/28

ملخص:

تشهد الحياة اليومية تطوّرا متسارعا في مجال التقنية المعلوماتية وأجهزة الاتصال الحديثة، فأصبحت الحواسيب والأنترنت تحتل مكانة هامّة في حياة المواطن، لكن في المقابل ساهمت هذه الأخيرة في بروز العديد من الجرائم الإلكترونية التي تباينت صورها وتشعّبت أنواعها، والتي أصبحت تشكّل خطرا حقيقيا على الكثير من الدول، باعتبارها جريمة عابرة للحدود، والأمر الذي دفعها إلى العمل على مكافحتها.

والجزائر كغيرها من الدول عملت على وضع منظومة قانونية متكاملة ترتكز في الأساس على قانون العقوبات والإجراءات الجزائية، كما دعّمتها سنة 2009 بالقانون 09-04 المتضمّن قواعد خاصة للوقاية من الجرائم المتّصلة بتكنولوجيا الاعلام والاتصال والحدّ منها، أي قواعد خاصة بمكافحة الجرائم الماسّة بأنظمة المعلوماتية الآلية للمعطيات،

Email :hakimaboukehil23@gmail.com المؤلف المرسل:بوكحيل حكيمة

ورغم كافة الجهود المبذولة في هذا الإطار، إلا أنّها تبقى غير كافية في ظلّ الوتيرة المتسارعة للابتكارات التكنولوجية، ما يدفعنا لتقديم جملة من الاقتراحات ضمن هذه الدراسة لاحتواء معيقات مواجهة الجرائم الالكترونية.

كلمات مفتاحية:

الهيئة الوطنية، جرائم الإعلام والاتصال، الجريمة الإلكترونية، التفتيش، نظم المعلوماتية، آليات الوقاية.

Abstract:

Daily life isexperiencingacceleratteddevelopment in the field of information technologies and modern means of communication. Computers and the Internet nowoccupy an important place in the lives of citizens.On the other hand, the latter have contributed to the emergence of numerouscybercrimes, whoseforms have varied and diverged in their types, which have become a real threat for many countries, becauseitis a transnational crime.

Algeria, likeother countries, has strived to put in place an integratedlegal system basedmainly on the penal code and criminalprocedures, and in 2009 itsupporteditwith Law 09-04 whichincludesspecialrules for the prevention and reduction of crimes related to media and communication technologies, iespecialrules to fightagainst crimes related to automatic data and information systems.Despite all the efforts made in this regard, itremainsinsufficient in view of the rapid pace of technological innovation, which prompts us to present a set of proposalswithin the framework of thisstudy to contain the obstacles to the fightagainstcybercrime.

Keywords:

The National Authority, Media and Communication Crimes, Electronic Crime, Inspection, Information Systems, Prevention Mechanisms.

مقدمة

إنّ التطور الكبير الذي عرفه عالم التكنولوجيا المعلوماتية وأجهزة الاتصال، واستعمال الأنترنت، أدّى إلى تعاظم دورها بشكل كبير، بحيث أصبحت هذه الأخيرة تمثّل روح العصر ومحرك عملية التنمية، ووسيلة الرقي والتقدم في كافة العلوم، كما أنّها تعتبر كاتمة أسرار قطاعات واسعة من شرائح المجتمع، ووسيلة التواصل الرئيسية عبر العالم. فرغم فوائدها الكثيرة إلا أنّها وللأسف أصبحت وسيلة ارتكاب جرائم خطيرة عابرة للحدود، والمتمّثلة في الجريمة الإلكترونية، التي يصعب اكتشافها ومكافحتها، وذلك نتيجة الاستعمال الواسع للحواسيب والأنترنت، ووسائل الاتصال المختلفة وإتاحة استعمال التقنيات الحديثة دون ضوابط صارمة.

إنّ هذه الجرائم أصبحت تشكل خطرا كبيرا على جميع دول العالم، نظرا لخطورتها، الأمر الذي دفع الدول إلى بحث ووضع قواعد مستحدثة، بالإضافة إلى القواعد التقليدية لحماية النظم المعلوماتية وقواعد البيانات، والاستخدام المشروع لها، ومنه حماية حرمة الحياة الخاصة للأشخاص وسرية البيانات المخزّنة في هذه الأنظمة.

وقد كان القانون 09-04 الذي يتضّمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، أحد تلك القوانين التي وضعت آليات وضوابط تتيح ضبط وكشف الجريمة المعلوماتية.

بناء على ما تقدّم فإنه يمكن طرح إشكالية هذه الدراسة في التساؤل التالي:

ما مدى فعالية دور الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال في المكافحة والوقاية من هذه الجرائم؟

وبذلك تهدف هذه الدراسة إلى تقديم دراسة قانونية حول هذه الجريمة الخطيرة وكيفية مكافحتها في ظلّ القانون 09-04 السالف ذكره من خلال إظهار أهمّ الآليات التي جاء بها هذا القانون.

وفي سبيل الإجابة عن الإشكالية المطروحة وتحقيق أهداف الدراسة، تمّ الاعتماد على كلّ من المنهج الوصفي والتحليلي المناسبين لطبيعة الموضوع، حيث تمّ تقسيم الدراسة إلى ثلاث مباحث بحيث يتناول المبحث الأول كل ما يتعلق بالهيئة المكلفة بالوقاية من جرائم النظم المعالجة الآلية للمعطيات (نظم الدفع الإلكترونية)، ليتم في المبحث الثاني التطرق لقواعد الاختصاص القضائي للهيئة، أما المبحث الثالث فقد خصصّ لدراسة إجراءات التحري الخاصة بنظم المعالجة الآلية للمعطيات.

المبحث الأول: الهيئة المكلفة بالوقاية من جرائم نظم المعالجة الآلية للمعطيات

نصّ القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لمكافحتها، في الفصل الخامس منه على إنشاء هيئة وطنية للوقاية من الجرائم المعلوماتية أو كما تعرف عامة بالجرائم الإلكترونية.

ويعتبر هذا التشريع نقلة نوعية في النصوص الإجرائية الجزائية بالنظر إلى نوعية الإجراءات التي نصّ عليها كمراقبة الاتصالات السلكية واللاسلكية والمراسلات الإلكترونية والاتصالات الهاتفية، وكذا مراقبة كل المعطيات الشخصية على الإنترنت، وهو ما قد يتخذ أحيانا بقصد أو دون قصد كطريق للمساس بحرمة حياة الأشخاص وأمن اتصالاتهم وبياناتهم الشخصية المالية والصحية والاجتماعية، لذلك تمّ إنشاء الهيئة الوطنية للوقاية من جرائم تكنولوجيا المعلومات ومكافحتها، لتكون هذه الهيئة هي الجهة الرقابية الخاصة بهذا النوع من الجرائم، حتى تضمن الحق الدستوري لكل مواطن في حرمة حياته ومراسلاته من المساس بها بداعي مكافحة الجرائم، وبقصد تفعيل نص المادة 13من القانون 09-04 فقد صدر في البداية المرسوم الرئاسي 15-261[1] المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا ت الإعلام والاتصال ومكافحتها والذي سوف نتناوله في هذه الدراسة باختصار نظرا لنوعية القواعد المستحدثة التي أتى بها آنذاك، غير أنه في 2019 صدر مرسوم رئاسي[2] 19-172 المعدل بالإلغاء للأحكام المرسوم الرئاسي 15-261 وذلك نتيجة الظروف السياسية والأمنية التي عرفتها البلاد في تلك الفترة مما أفضى إلى ظهور مخاطر فعلية لتعرض الأمن العمومي وكذا المؤسسات الدستورية للخطر فجاء هذا المرسوم ليغير من الطبيعة القانونية للهيئة حيث نقل الإشراف عليها من وزارة العدل إلى وزارة الدفاع[3]مما حولها إلى هيئة ذات طابع أمني، وعليه نتحدث عن تشكيلة الهيئة وتنظيمها في المطلب الأول، ثم مهامها وكيفية سيرها في المطلب الثاني.

المطلب الأول: تشكيل الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال وتنظيمها

لم ينصّ القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من جرائم تكنولوجيا الإعلام والاتصال على الهيئة ولا تشكيلها ولا آليات عملها ونطاقه بشكل مفصل، حيث نصّت المادة 13 منه على أن **" تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته... تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم"**.

تحت سلطة وزارة الدفاع الوطني حدد مقرها تعدّ الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي بالجزائر العاصمة مع إمكانية نقلها إلى أي مكان آخر بموجب قرار من وزارة الدفاع الوطني، ويتضمن المرسوم الرئاسي 19-172 تعديلا في الهيكل التنظيمي للهيئة، حيث أصبحت تضم مجلس توجيه والذي ندرسه في الفرع الأول ومديرية عامة في الفرع الثاني.

الفرع الأول: مجلس التوجيه

بعد وضع الهيئة تحت إشراف وسلطة وزارة الدفاع الوطني بعد أن كانت في ظل المرسوم الرئاسي 15-261 الملغى تخضع لسلطة وزارة العدل، أصبحت تشكيلة مجلس التوجيه الذي حل محل اللجنة المديرة كالتالي:

يترأس هذا المجلس وزير الدفاع الوطني القائد الأعلى للقوات المسلحة أي رئيس الجمهورية ومن الناحية العملية فإن نائب وزير الدفاع هو من ينوبه في رئاسة المجلس وهو ما نصت عليه المادة 5 من المرسوم الرئاسي 19-172كما يتشكل من ممثلي الوزارات التالية: وزارة الدفاع الوطني ووزارة الداخلية، وزارة العدل، وزارة المواصلات السلكية واللاسلكية كما أسندت مهمة أمانة المجلس للمديرية العامة.

الفرع الثاني: المديرية العامة

بموجب المادة 9 من المرسوم الرئاسي 19-172 السالف الذكر فإنه تنشأ مديرية عامة يترأسها مدير عام يعين طبقا للتنظيم المعمول به في وزارة الدفاع الوطني وهو ما نصت عليه المادة 19 من ذات المرسوم ويتضح لنا الطابع الأمني للهيئة من خلال التشكيلة التي يغلب عليها عامل الانتساب للمؤسسة العسكرية كما أن المديرية من الناحية التنظيمية تضم بموجب المادة 10 من ذات المرسوم مديريتان هما المديرية التقنية ومديرية للإدارة والوسائل.

أولا: المديرية التقنية

تتكفل المديرية التقنية على وجه الخصوص بمهمة المراقبة الوقائية للاتصالات الالكترونية من أجل الوقاية من الجرائم الموصوفة بالأفعال الإرهابية وأي اعتداء على أمن الدولة، هذا بالإضافة إلى مساعدة السلطات القضائية ومصالح الشرطة بما في ذلك في مجال الخبرات القضائية في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[4]

ثانيا: مديرية الإدارة والوسائل

وضعت مديرية الإدارة والوسائل على الخصوص للقيام بمهمة التسيير الإداري والمالي اليومي لمختلف الموارد البشرية للهيئة، كما تتولى تسيير إنفاق ميزانية الهيئة سواء في مجال التموين أو صيانة العتاد والوسائل والمنشآت القاعدية[5]

المطلب الثاني: كيفيات سير الهيئة ومهامها

لقد طال مهام الهيئة بعض التغيرات وذلك على مستوى مجلس التوجيه أو المديرية العامة وعليه نورد مهام الهيئة في الفرع الأول وكيفية تسييرها في الفرع الثاني.

الفرع الأول: مهام الهيئة

رغم أن القانون المتضمن القواعد الخاصة المتصلة بجرائم الإعلام والاتصال ومكافحتها قد نص في المادة 14 منه على مهام الهيئة بصفة واضحة، إلا أنه في المرسوم الرئاسي السالف الذكر فصل في هذه المهام ووزعها على مجلس التوجيه والمديرية العامة.

أولا: مهام مجلس التوجيه

يكلف المجلس على الخصوص بالتداول حول الاستراتيجية الوطنية للوقاية من الجرائم المعلوماتية وتكنولوجيات الاتصال ومكافحتها، وكذا يتداول ويناقش مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إجراء تقييم دوري لحالة التهديد في مجال الجرائم والأهداف المرجوة منها،كما يقترح أي نشاط يراه مناسبا يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المعلوماتية ومكافحتها،كما يقدم كل اقتراح في مجال اختصاص الهيئة وكذا يساهم في ضبط المعايير القانونية في مجال اختصاصه، ويدرس ميزانية الهيئة و يوافق عليه[6]

أما فيما يتعلق بتسييره فإنه يجتمع في دورتين عاديتين بناء على استدعاء من رئيسه كما يمكن أن يجتمع في دورة غير عادية بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة كلما كان لذلك ضرورة عملية وهو ما نصت عليه المادة 6من المرسوم السالف الذكر، أما المادة 8 فقد حددت قواعد وكيفيات سير مجلس التوجيه بناء على قرار من وزير الدفاع الوطني.

ثانيا: مهام المديرية العامة

تتولى المديرية السهر على حسن سير الهيئة وذلك من خلال تنشيط و تنسيق عمليات الوقاية المتصلة بجرائم تكنولوجيات الإعلام والاتصال ومكافحتها،وكذا تبادل المعلومات مع الهيئات الأجنبية التي تعمل في نفس المجال في إطار التعاون الأمني بغرض تجميع المعطيات المتعلقة بمرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك للتعرف عليهم وتحديد مكان تواجدهم بالإضافة إلى القيام بمهام إدارية بحتة كإعداد مشروع ميزانية الهيئة، إعداد وتنفيذ برامج عمل الهيئة وكذا العمل تنسيق ومتابعة ومراقبة أنشطة هياكل الهيئة، تحضير اجتماعات مجلس التوجيه كون المديرية العامة تتولى مهام الأمانة العامة لمجلس التوجيه بموجب المادة 5 الفقرة الأخيرة من المرسوم السالف الذكر كما تقوم بإعداد التقرير السنوي لنشاطات الهيئة حيث يمسك محاسبة الهيئة حسب قواعد المحاسبة العمومية وهو ما نصت عليه المادة 17 من المرسوم السالف الذكر.

الفرع الثاني: كيفيات تسيير الهيئة

لم يحدد المرسوم الرئاسي 19-172كيفيات تسيير الهيئة خاصة فيما يتعلق بالمديرية العامة ولا الأشخاص المستخدمين فيها رغم أهميتها، حيث أن هذه المديرية تعتبر المحرك الفعلي لهذه الهيئة حيث تلعب دور مزدوج فهي تمارس مهام الأمانة العامة لمجلس التوجيه المادة 5 من المرسوم الرئاسي 19-172 بالإضافة إلى إلى أنها تمارس العمليات التقنية من خلال المديرية التقنية المادة 11من المرسوم السالف الذكر، كما تقوم بالعمل الإداري بموجب المادتين 15،9 من ذات المرسوم، هذا بالإضافة للمادة 21من ذات المرسوم التي تحدد تنظيم وكيفيات سير مكونات المديرية العامة وصلاحياتها ويكون ذلك عن طريق تنظيم يصدر بموجب قرار من وزير الدفاع كما أن المادة 19من ذات المرسوم التي تص على أن تعيين المدير العام و مستخدمو هذه الهيئة طبقا للتنظيم المعمول به في وزارة الدفاع الوطني.

وبالرجوع الى هذا التنظيم المتمثل في القانون18-14 المتضمن قانون القضاء العسكري فإنه يمكننا أن نستشف القواعد العامة لتسيير الهيئة، كونها تخضع بموجب المادة 22 من ذات المرسوم لمجموع الأحكام التشريعية و التنظيمية المطبقة في وزارة الدفاع الوطني، وعليه فبموجب المادة 43 من القانون 18-14 المتضمن القضاء العسكري " **يكلف ضباطالشرطة القضائية العسكرية بالتحقيق في الجرائم وجمع الأدلة و البحث عن الفاعلين طالما لم يفتح التحقيق القضائي... وعند فتح متابعة قضائية ينفذ ضباط الشرطة القضائية العسكرية تفويضات الجهة القضائية العسكرية ويحيلونها حسب طلبها** "

كما أن المادة 45 من ذات القانون حددت من له صفة ضباط شرطة قضائية عسكرية في مجموعتين:

1-كل العسكريين التابعين للدرك الوطني والضباط وضباط الصف التابعين للمصالح العسكرية للأمن الحائزين لصفة ضباط شرطة قضائية وفقا لأحكام المادة 15مكررمن قانون الإجراءات الجزائية.

2-كل ضباط القطاع العسكري أو المصلحة والمعينين خصيصا لهذا الغرض بموجب قرار من وزير الدفاع الوطني ويتبع ضباط الشرطة القضائية العسكرية في ممارسة صلاحياتهم لسلطة النيابة العامة العسكرية... "

أما فيما يتعلق بالتفتيش في حالة الجناية أو الجرائم المتلبس بها خارج المؤسسة العسكرية فيتعين عليهم إخبار وكيل الجمهورية لدى المحكمة المدنية المختصة، كما أنه بموجب المادة 51 من القانون 18-14 فإنه يمكن لضباط الشرطة القضائية العسكرية أن يبادر ضمن الحالات المنصوص عليها في المادة 14" **أوإذا طلب منه ذلك طبقا للمادة 47 من القانون بالانتقال فورا إلى مكان الجناية أو الجنحة فيشرع في جميع التحقيقات الضرورية وإجراءات التفتيش اللازمة لجمع الأدلة والكشف عن مرتكبي تلك الجرائم** ".

نلاحظ أن ضباط الشرطة القضائية العسكرية يمارسون مهامهم في حالات الجرائم العسكرية تحت إشراف النائب العسكري العام والوكيل العسكري للجمهورية أمام القضاء العسكري وضمن ضوابط قانون القضاء العسكري، كما أنه يقوم بمهام الضبطية القضائية العادية فيما يتعلق بجرائم القانون العام حيث يخضع لوكيل الجمهورية لدى المحكمة المدنية المختصة، كما أنه يخضع لأحكام قانون الإجراءات الجزائية.

وعليه فإنه إلى حين تفعيل نص المادة 21من المرسوم الرئاسي يبقى سير الهيئة وتنظيمها وآليات تطبيق أو تنفيذ صلاحيات المديرية العامة يخضع لهذه الازدواجية.

المبحث الثاني: قواعد الاختصاص القضائي للهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال

نصّت المادة 15 من القانون 09-04 على الإحالة إلى أحكام قانون الإجراءات الجزائية لتحديد الاختصاص النوعي والإقليمي الوطني للهيئة ممثلة في المديرية التقنية، وكذا قواعد التعاون الدولي القضائي لمكافحة الجرائم المعلوماتية بوصفها جرائم عبر وطنية.

وعليه بالرجوع إلى المادة 15 يتحدد الاختصاص كما يلي:

المطلب الأول: الاختصاص الوطني بنوعيه (المحلي والنوعي)

بالإحالة على أحكام المادة 37 فقرة 1 و2 نجدها تنص على أن: **" يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال وتمويل الإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف"**أما عند معاينة الجرائم الماسة بأنظمة المعالجة الألية للمعطيات فإن إصلاحات الضبطية القضائية تؤول بموجب المادة 13من المرسوم الرئاسي 19 -172 إلى المديرية التقنية تمارس مهامها في التحري و الضبط وفقا للأحكام التشريع المعمول به، أي قانون القضاء العسكري[7]، كذلك الأمر عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات لصلاحيات الضبطية القضائية توسع من حالات عديدة أهمها:

الفرع الأول: تمديد الاختصاص المحلي

تكلف المديرية التقنية بمهمة التحقيق والتحري وجمع الأدلة والبحث عن الفاعلين لأي جريمة موصوفة للأعمال الإرهابية والتخريبية والاعتداء على أمن الدولة بموجب المادة 11 من المرسوم الرئاسي 19-172، كما أنها بموجب المادة 13 من ذات المرسوم تمارس المهام المرتبطة بالشرطة القضائية كون أعضاء هذه المديرية من المستخدمين الخاضعين لقانون القضاء العسكري، كما نصّت على ذلك المادة 19 من ذات المرسوم والذين يخضعون في إطار أداء مهامهم للقانون 18-14 المعدل لقانون القضاء العسكري خاصة المادة 26 منه التي حددت مفهوم المستخدمين الخاضعين لقانون القضاء العسكري واللذين يمارسون مهم وفق أحكام المواد 43، 45، كما أنّ المديرية التقنية تمارس أعمال الضبط القضائي وفق أحكام المواد 15و 15 مكرر من قانون الإجراءات الجزائية، وعليه فإنهم يخضعون للإلزام بإخبار وكيل الجمهورية لدى المحكمة المدنية المختصة عندما يقومون بأعمال التفتيش الخاصة بالجنايات أو الجنح المتلبس بها خارج المؤسسة العسكرية وهو ما نصت عليه المادة 45 من القانون 18-14 سالف الذكر.

الفرع الثاني: تمديد صلاحيات التفتيش

حيث وسعّ إجراء التفتيش ليشمل المحلات السكنية وغير السكنية في كل ساعة عن ساعات الليل والنهار بإذن من وكيل الجمهورية، على خلاف القواعد العامة المتضمنة حرمة المنازل ومنع تفتيش للمنازل بعد الساعة الثامنة ليلا والخامسة

صباحا، حيث نصّت المادة 47 فقرة 3 على أنّ: **"عندما يتعلق الأمر بجرائم... أو الجرائم الماسة بأنظمة المعالجة الآلة للمعطيات، وكذا تبييض الأموال وتمويل الإرهاب... فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من النهار أو الليل، وذلك بناء على إذن مسبق من وكيل الجمهورية المختص"**.

المطلب الثاني: قواعد التعاون القضائي الدولي

إنّ فكرة الاعتماد على القدرات الوطنية لوحدها للتصدي لهذا النوع من الجرائم، وكذا التحري والتفتيش وحجز الأدلة من طرف القضاء الوطني لوحده أمر غير واقعي، بالنظر للتقنية المستخدمة وكفاءة مرتكبي هذه الجرائم، واتساع رقعة عمليات الإجرام من تزييف[8]، واختراق وتحويلات غير مشروعة للأموال.[9]

الفرع الأول: تعريف المساعدة القضائية الدولية

وهي كل إجراء قضائي أو أمني في مرحلة التحريات البوليسية، قبل المتابعة والمحاكمة تقوم به الدولة من أجل تسهيل إتمام التحريات والاستعلام وجمع الأدلة لفائدة دولة أخرى، بغية محاكمة مجرم أو منع ارتكاب جريمة –إجراء وقائي–أو تسليم مجرم لمحاكمته بعد القبض عليه،فلقد نصّ المشرع الجزائري في القانون 09-04 على مبدأ المساعدة القضائية الدولية المتبادلة في المادة 16 وذلك في مرحلة التحريات الأولية، حيث يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة الإلكترونية.

الفرع الثاني: صور المساعدة القضائية والتعاون الدوليين

تأخذ صورة تبادل المعلومات وطلبات اتخاذ إجراءات التحفظية

أولا: تبادل المعلومات

يشمل عملية تبادل المعلومات تقديم البيانات والوثائق والمواد الاستدلالية، ومحاضر حجز الأدلة، وتقارير الشرطة العلمية عن الأدلة، ومحاضر تسجيل السمعية و/أو البصرية، التي تطلبها السلطات الأجنبية في إطار تحريها وتحقيقها عن جريمة ما بصفة عامة.

وتعدّ آلية تبادل المعلومات من الآليات الأكثر شيوعا في مختلف الاتفاقيات الجماعية أو الثنائية، أهمها الفقرة 02 من المادة الأولى: لمعاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية[10]، وكذلك المادة 08 البند 3، 4، 5 لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود، إذا ألزمت الأطراف الموقعة عليها على وضع آليات تسيير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي.[11]

وعلى المستوى الوطني أقرّ المشرع الجزائري مبدأ التعاون والمساعدة القضائية الدوليين في عدة نصوص منها قانون 09-04 موضوع الدراسة في المادة 17 منه، حيث أوجب الاستجابة من السلطات القضائية والوقائية الوطنية أي المحاكم والمجالس، وكذا الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيات الاتصال، وذلك عن تبادل المعلومات واتخاذ

الإجراءات التحفظية في إطار مبدأ المعاملة بالمثل أساسا، واستجابة للاتفاقيات الدولية، وكذا الاتفاقيات الثنائية التي صادقت عليها الجزائر.[12]

ثانيا: طلبات اتخاذ الإجراءات التحفظية

تتميّز هذه الإجراءات بأنها ذات طابع جزائي كانتقال للمعاينة لدليل، أو حجز دليل، أو تفتيش منظومة معلوماتية، ويتم طلب اتخاذ هذه الإجراءات أو الإجراءات التحفظية كحجز دليل، أو نظام الإنابات القضائية الدولية، **"وهو إجراء بموجبه تمنح الدولة لقرينتها سلطة اتخاذ بعض الإجراءات نيابة عنها، وفي حدود هذه النيابة.**

المبحث الثالث: إجراءات التحري الخاصة بنظم المعالجة الآلية للمعطيات

نظرا لأنّ جرائم الاعتداء على بوصفها نظم معالجة آلية للمعطيات تقع ضمن بيئة افتراضية، ظهرت الحاجة إلى تعديل هذا القانون لتكريس قواعد تتماشى ونوعية هذه الجرائم، وذلك بوضع قواعد تتعلق بطرق التحري عن هذه الجرائم وهي آلية المراقبة الالكترونية، ثم طرق تفتيش نظم المعالجة الآلية، آليات حجز الأهم حفظهما من التدمير أو المحو، وكذا الأساليب التقنية اللازمة، وإقحام مزودي خدمات الانترنت في إجراءات حجز الأدلة، وتقديم المساعدة الضرورية للمديرية التقنية بموجب المادة 14 الفقرة الأخيرة من المرسوم الرئاسي 19-172، والأهم هو حفظ حرمة الحياة الخاصة للأفراد وسلامة وحرمة اتصالاتهم الخاصة من الاستغلال عن طريق الانحراف في تنفيذ إجراءات التفتيش أو حجز الأدلة، وتبيان طرق حفظ الدليل المعلوماتي الناتج عن التفتيش والحجز، وضمان سلامته وصحته ودقته ومنه إضفاء المشروعية عليه، ومدى إلزامية هذا الدليل للقاضي في الموضوع في إطار مبدأ حرية القاضي الجزائي في الاقتناع.

المشرع الجزائري نظم آليات وإجراءات التفتيش لنظم المعالجة الآلية للمعطيات بموجب القانون رقم 06-22 في المواد 65 مكرر 5 إلى المكرر 10 من ذات القانون حيث نصّ على أساليب تحري خاصة تتمثل أساسا في إجراء الاعتراض على المراسلات وتسجيل الأصوات والتقاط الصور.[13]

ثم توج عمله بالقانون 09-04 المتعلق بإجراءات مراقبة وتفتيش نظم المعالجة الآلية للمعطيات وحجز الدليل التقني وحفظه، والطرق المستخدمة للمراقبة والتفتيش وحجز الأدلة، وكذا الأشخاص المخولين بتنفيذ تلك الإجراءات، وعليه نقسم دراستنا في هذا المبحث إلى: الأجهزة المكلفة بالتحري والتفتيش في المطلب الأول، ثم القواعد الإجرائية الخاصة بالتحري والتفتيش في المطلب الثاني.

المطلب الأول: الأجهزة المكلفة بالتحري والتفتيش

الأصل أنّ السلطة القضائية هي المكلفة ممثلة في القضاء الجزائري باتخاذ تدابير للتحري والتحقيق في مختلف الجرائم من خلال الأجهزة المقرّرة لذلك عبر مختلف المراحل التي تمر بها القضية الجنائية من مرحلة جمع الاستدلالات لدى الضبطية القضائية تحت إشراف ورقابة وكيل الجمهورية[14]، إلى القرار الذي سيتخذه بصدد إبلاغه على محاضر الضبطية القضائية[15]، من خلال تفعيل مبدأ الملائمة، فإنّ قرار تحريك الدعوى العمومية من أجل تكييف الجريمة جناية أو جنحة يطلب فتح تحقيق لدى قاضي التحقيق المختص نوعيا ومحليا، وإلا قرر حفظ المحضر.

غير أنّ قانون 09-04 نصّ على استحداث هيئة وطنية مستقلة ذات طابع إداري هي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته في الفصل 5، المادة 13 وما يليها.

الفرع الأول: الدور المساعد للهيئة

تحت رقابة السلطة القضائية تلعب الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لمكافحته بمساعدة السلطة القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وذلك بوضع المديرية التقنية بموجب المادة 12 الفقرة 02 من المرسوم السالف الذكر تحت تصرف السلطة القضائية، حيث تقوم بتقديم المساعدة لها بناء على طلبها سواء في مجال الخبرات القضائية في إطار مكافحة الجريمة المتصلة بتكنولوجيات الإعلام والاتصال التي تتطلب اللجوء إلى إجراءات خاصة للتحري،كاعتراض المراسلات السلكية واللاسلكية، تفتيش نظم المعالجة الآلية للمعطيات، وحجز المعطيات عن طريق منع الوصول إليها، وحجز المعطيات ذات المحتوى المجرم، وحفظ المعطيات المتعلقة بحركة السير للمعطيات، وكذلك تنفيذ إجراءات التعاون والمساعدة الدوليين وتأخذ المساعدة عدة صور منها:

أولا: المراقبة الوقائية الاستباقية

حيث نصّت المادة 4 من القانون 09-04 على أنّ الهيئة ممثلة في مديرية المراقبة الإلكترونية واليقظة الإلكترونية، يقوم بالمراقبة الاستباقية، أي مراقبة ورصد تحركات واتصالات أشخاص أو جماعات مشبوهة تحضّر أو تجتمع أو تجهز للقيام بعمليات إرهابية، وذلك لمنعها قبل وقوعها وذلك عن طريق إخطار السلطات القضائية المختصة[16]، وهو ما أكدّه المرسوم الرئاسي 19-172 في المادة 11 منه.

كما نصّت المادة 4 من القانون 09-04 على حالة ثانية لتفعيل المراقبة الوقائية الاستباقية في الفقرة "ب" منها وذلك في حالة توفر معلومات عن احتمال[17]اعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.[18]

ثانيا: المراقبة كإجراء قانوني في تحقيقات جارية

حيث نصّت المادة 4 فقرة "ج" من القانون 09-04 على حالة وجود تحريات أو تحقيقات قضائية مفتوحة مسبقا، إلا أنّ هذه التحريات على مستوى القضاء أمام قاضي التحقيق، تواجه صعوبات في الوصول إلى نتائج[19] أي أدلة جنائية بالنظر إلى طبيعة الجريمة ممّا يتطلب اللجوء إلى المراقبة الإلكترونية ويبررها علما وأنّ هذا الإجراء يتخذ في جرائم المنظومة المعلوماتية –ليس الإرهاب–مهما كان موضوع الجريمة المرتكبة.[20]

ثالثا: الدور التنفيذي لإجراءات المراقبة

كذلك تعدّ الهيئة منفذ لأوامر جهات التحقيق في جرائم تتطلب اتخاذ تدابير المراقبة الإلكترونية، حيث تصرف بناء على طلب من جهات التحري أو أوامر النيابة العامة أو جهات التحقيق، كذلك تعمل تحت إشراف القاضي المختص نوعيا ومحليا، وذلك بناء على إذن مكتوب من القضاء، وتشمل اختصاصها في تنفيذ أوامر جهات القضاء:

-تزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا (دور مساعد) وبناء على طلب المعلومات والمعلومات المتعلقة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال؛

-إرسال المعلومات المحصل عليها خلال المراقبة الوقائية إلى السلطات المختصة؛

-تسجيل وتجميع محتوى عمليات المراقبة السمعية البصرية والالكترونية في الحين؛

-القيام بتنفيذ التفتيش والحجز داخل المنظومة المعلوماتية؛

-وضع الوسائل والتجهيزات التقنية الضرورية لتنفيذ مهام المديرية التقنية على مستوى المنشآت القاعدية للمتعاملين ومقدمو الخدمات وهو ما نصت عليه المادة 14 من المرسوم الرئاسي 19-172.

كذلك يمكن هنا ضباط الشرطة القضائية التابعون للهيئة الوارد تحديدهم في المادة 19 من المرسوم الرئاسي 19-172وكذلك المواد 43، 45 من القانون 18-14 المتضمن قانون القضاء العسكري عند تنفيذهم لمهامهم، ولمقتضيات قانون الإجراءات الجزائية، أن يقوموا بتفتيش أي مكان أو جهاز بلغ إلى علمهم ويستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية، أي أنّ المرسوم هنا مدّ اختصاصهم ليشمل بالإضافة إلى تفتيش المنظومة المعلوماتية والمعطيات والبيانات بوصفها كيان منطقي، يشمل اختصاصها هنا تفتيش الأماكن بصفة عامة، بما في ذلك السكن، ودور مقاهي الإنترنت وغيرها، وذلك مع مراعاة القواعد الخاصة بتفتيش السكنات كما نصّت المادة سابقا وكذلك أي هيكل، أي هياكل أبراج الاتصالات لشبكة الهاتف النقال في اعتقادي الخاص هذا هو المقصود بالهياكل، وكذلك الجهاز ويقصد به الكيان المادي لأي جهاز إلكتروني كان كمبيوتر أو هاتف محمول أو لوح إلكتروني أو غيره.

المطلب الثاني: الإجراءات الخاصة بالتحري عن جرائم المساس بنظم المعالجة الآلية

باعتبار نظم معالجة آلية للمعطيات فإنها من ناحية الحماية الموضوعية تخضع لقواعد تجريم المساس بنظم المعالجة الآلية للمعطيات في قانون العقوبات في المواد 394 مكرر إلى غاية 394 مكرر 7، أما من الناحية الإجرائية فنجد المشرع الجزائري قد عمل بعد تعديل قانون العقوبات في سنة 2004 إلى تعديل قانون الإجراءات الجزائية بموجب القانون رقم 06-22 لسنة 2006 المعدل بذلك الأمر رقم 66-155 المتضمن القانون، وأهمية هذا التعديل تكمن في إدراج إجراءات جديدة تتوافق مع طلبات التطور التكنولوجي وتطور أساليب ارتكاب الجريمة، فنجد المواد 65 مكرر 5 إلى غاية المادة 65 مكرر 10 التي تضمنت أحكام تنظيم إجراء اعتراض المراسلات وتسجيل الأصوات، والتقاط الصور، ثم نجد القانون 09-04 والمرسوم الرئاسي 19-172 المتضمن إجراءات المراقبة الوقائية الإلكترونية، وكذا إجراءات التفتيش لنظم المعالجة الآلية للمعطيات وحجز الأدلة (المعطيات أو منع الوصول إليها).

الفرع الأول: إجراء المراقبة الإلكترونية

سبق وأن شرحنا الهيئة المسؤولة عن تنفيذ هذا الإجراء الذي يكون في حالتين الأولى كتدبير وقائي استباقي لارتكاب الجريمة وتكون غايته منع ارتكاب الجريمة والقبض على الفاعلين أو المخططين قبل الشروع في تنفيذ الجريمة أو عند بدء التنفيذ وذلك بقطعه ومنع تحقق النتيجة الإجرامية.[21]

وأمّا الحالة الثانية فيكون بموجب إذن من السلطة القضائية كإجراء من إجراءات التحري عن جرائم وجدت السلطة القضائية صعوبة في الوصول إلى أدلة قطعية لإدانة مرتكبها.

وتعتبر آلية المراقبة الإلكترونية أداة فعالة في مكافحة خاصة جرائم الاعتداء على نظم المعالجة الآلية في مجال الخدمات البنكية الإلكترونية المجال الأكثر خصوبة لأفعال الاعتداء، وقد كانت اتفاقية **"بودابست"** الخطوة الأولى لتفعيل هذا الإجراء.[22]

وقد قسمّ المشرع الجزائري متأثرا باتفاقية **"بودابست"** المعطيات محل المراقبة إلى نوعين: الأول هو المعطيات المتعلقة بالمرور وهي[23]: **" كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي أي يتم إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الاتصال، مع تعيين المعلومات التالية: أصل الاتصال، مقصد الاتصال أو الوجهة المقصودة بالاتصال، خط السير، ساعة وتاريخ الاتصال، حجم وفترة الاتصال أو نوع الخدمة"**، وأما النوع الثاني فيتعلق بالمحتوى أي معطيات المحتوى، لم تعرفه الاتفاقية.

المشرّع الجزائري حددّ المعطيات المتعلقة بحركة السير في المادة 11 من قانون 09-04، وحددّ شروطها مع مراعاة طبيعة ونوعية الخدمات يلتزم مقدمو الخدمات بحفظ:

-المعطيات التي تسمح بالتعرف على مستعملي الخدمة؛

-المعطيات التقنية بالتجهيزات الطرفية المستعملة للاتصال؛

-الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال؛

-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها؛

-المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ " من هذه المادة بسنة وابتداء من تاريخ التسجيل.

أمّا معطيات المحتوى فنصّ عليها المادة 4 من ذات القانون وهي:

-أن يكون محتوى الاتصال الإعداد أو الاتفاق الجنائي لارتكاب أفعال إرهابية أو التخريب أو الجرائم الماسة بأمن الدولة.[24]

-أن يكون محتوى الاتصال يتضمن إشارات لاحتمال ارتكاب جريمة اعتداء على منظومة معلوماتية بما يهدد النظام العام، أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

-أن يكون محتوى الاتصال يتضمن دلائل من الصعب الوصول إليها بغير هذا الاعتراض لإتمام مقتضيات تحريات أو تحقيقات جارية، سواء كانت التحقيقات وطنية أو لتلبية طلبات المساعدة القضائية الأجنبية في إطار التعاون الدولي.

ويقصد بالاتصالات الإلكترونية كما عرفّها المشرع الجزائري في قانون 09-04 في المادة 2 فقرة "و": **"أي تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي أدلة إلكترونية".**[25]

أما المراقبة الإلكترونية فهي **"مراقبة شبكة الاتصالات باستخدام التقنية الإلكترونية لجمع المعطيات ومعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا مرتبط بالزمن (التاريخ والوقت) لتحقيق أمني أو لأي غرض آخر"**.[26]

فهي إجراء ماس بحرمة الحياة الخاصة للأفراد وحرمة مراسلاتهم واتصالاتهم المحمية دستوريا، لذلك فقد أحاطه المشرع بمجموعة من الضمانات منها أساسا أن تقع المراقبة على الاتصالات الخاصة، لا تحتوي على تهديد أمني كما في ذلك من مخاطر تمس كرامة الأفراد، وحقهم في حماية حرياتهم في الاتصال وغيره.

الفرع الثاني: إجراءات التفتيش لنظم المعالجة الآلية للمعطيات وما ينتج عنه من حجز

لقد نظمّ المشرع الجزائري إجراء التفتيش في قانون الإجراءات الجزائية [27]وأحاطه بمجموعة من الضمانات لما فيه من خطورة ومساس لحرمة الأشخاص وحرمة مساكنهم المضمونة دستوريا، إلا أنّ ظهور الإجرام الإلكتروني واستخدام التقنيات الحديثة لارتكاب الجرائم المختلفة خاصة على خدمات الدفع الإلكتروني، ممّا يستدعي إدخال تعديلات بإضافة قواعد تنظيم إجراء التفتيش على نظم المعالجة الآلية أياستخدام نظم معالجة إلكترونية لإجراء التفتيش في نظم معلوماتية أو نظم تخزين المعلوماتية.

فالتفتيش ما هو إلا إجراء من إجراءات التحقيق يقوم به قاضي التحقيق أو ينوب عنه ضابط الشرطة القضائية أو يأذن بإجرائه[28] إلى حين الوصول إلى مسرح الجريمة بهدف البحث عن أدلة عن الجريمة محل البحث أو مشبوه أو متهم في مسكن أو مكان ما، وذلك لاستيفاء واستكمال مقتضيات التحقيق ثم المحاكمة.

الهدف من التفتيش هو ضبط حجز الأدلة عن الجريمة محل التحقيق وتفتيش الحاسب الآلي بكيانه المادي باتباع القواعد التقليدية للتفتيش من حيث المبدأ، أما الكيان المنطقي له ولنظم المعالجة الآلية والبرمجيات المختلفة، فإنه يخضع لقواعد أكثر صرامة بالنظر إلى خصوصية الدليل المرغوب التحصّل عليه وحساسيته وهشاشته وسهولة ضياعه [29]بذبذبة كهرومغناطيسية، أو نقرة بالخطأ تفعل برنامج للتدمير الذاتي أو محو البيانات عن المنظومة المعلوماتية ولو تمّ ذلك عن بعد.

لذلك يشترط في التفتيش لنظم المعالجة الآلية للمعطيات شروط موضوعية السبب والمحل والسلطة المختصة، فسبب التفتيش هو لتحصيل وحجز أدلة داخل النظام المعلوماتي أو منظومة تخزين بغية الوصول إلى الحقيقة عن جريمة الاعتداء على منظومة معلوماتية كنظام آرتس[30] أو آتس[31]، ثم تحديد المنظومة المعلوماتية التي سيرد عليها التفتيش وقد تكون فردية خاصة بشخص واحد ككمبيوتر منزلي موصول أو مفصول عن الشبكة أو عمومية مفتوحة للجمهور كمقهى الانترنت.

أمّا محل التفتيش فهو نظام المعالجة الآلية للمعطيات [32]بكل مكوناته المنطقية والمادية، وشبكة الاتصال والخوادم والمزود الآلي والمصنف والملحقات التقنية سواء كانت متصلة بالشبكة أو منفصلة، أو كانت منظومة تخزين المعطيات دون معالجتها [33]كالأقراص المضغوطة أو الفلاشة (الوصلة)، أو بطاقة ذاكرة أو شريحة أو هاتف نقال.

إجراء التفتيش من السلطات القضائية المختصة عن طريق الهيئة الوطنية للوقاية من جرائم تكنولوجيا الاتصال والإعلام ممثلة في المديرية التقنية، بإشراف قضائي بموجب إذن مكتوب ومؤرخ وموقع ليتم إفراغ محتوى الإجراء في محاضر

رسمية تحترم الإجراءات والشروط الواردة من قانون الإجراءات الجزائية[34] حيث تنص المادة 95 منه على أنه **" لا يجوز أن تتضمن المحاضر تحشيرا بين السطور ويصادق قاضي التحقيق والكاتب والشاهد على كل شطب أو تخريج فيها ومن المترجم أيضا، إن كان محل لذلك، وبغير هذه المصادقة تعتبر هذه الشطوبات أو التخريجات ملغاة، وكذلك الشأن في المحضر الذي لم يوقع عليه توقيعا صحيحا أو في الصفحات التي تتضمن توقيع الشاهد"**.

في مجال تفتيش نظم المعالجة الآلية للمعطيات فإنّ نتيجة التفتيش يجب أن تنتهي بالوصول إلى المعطيات المعلومات التي لأجلها تم التفتيش، ولذا يجب ضبط هذه الأدلة بموجب المادة 6 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وحددت طرق ضبط الدليل المعلوماتي كالتالي:

-إذا لم يكن ضروريا ضبط أي حجز كل المنظومة المعلوماتية، فيتم نسخ المعطيات محل البحث، وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية، تكون قابلة للحجز والوضع في أحراز وفقا لمقتضيات 84 فقرة 2 من قانون الإجراءات الجزائية، وعليه أي سلطات التفتيش السهر على سلامة المعلومات محل الحجز، فإذا كانت هذه المعطيات قد تعرضت لتلف أو محو أو محاولة محو غيرت من معالمها أو بعثرت محتواها، جاز لجهات التفتيش استخدام كل الوسائل التقنية الضرورية؛

-برمجيات الترميم قصد تشكيل هذه المعطيات أو إعادة تشكيلها بغرض استغلالها لفائدة التحقيق بشرط عدم الإضرار بالمحتوى أو إتلافه أو محوه؛[35]

-الحجز عن طريق منع الوصول إلى المعطيات: وهو إجراء يهدف إلى حظر الوصول إلى المعطيات ذات المحتوى بالأساس، وذلك في حالة استحالة تنفيذ إجراءات الحجز وفقا للمادة 6 سابقة الذكر، ويكون منع الوصول إلى هذه المعطيات عن طريق الحجب بالترميز التقييد، التشفير، وباستخدام أي وسيلة إلكترونية أخرى[36]، ويتم اللجوء إلى إجراء المنع من الوصول إذا كانت المعطيات تتضمن خطرا مبررا؛

-منع الاطّلاع على المعطيات المخزنة في منظومة معلوماتية ذات محتوى مجرم بموجب المادة 4 من القانون 09-04 وإجراء منع الاطلاع يكون بتكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك[37].

الخاتمة

إنّ الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الاتصال بمخلف مديرياتها تعدّ دعامة فعالة لتطبيق أحكام القانون 06-22 الذي أرسى إجراءات تحري وتفتيش جديدة، لكن بقيت غير مقنعة كليا بسبب محدودية التقنيات المستخدمة من طرف الضبطية القضائية، وسرعة تطور تكنولوجيا الإعلام والاتصال، كما نجد إجراءات جديدة كتفتيش نظم المعلومات، حجز المعطيات، إجراءات منح الوصول، إجراءات الرقابة الاستباقية (اليقظة الإلكترونية)، تنفيذ مختلف الأوامر المتعلقة بالتفتيش والتحري عن جرائم محل تحقيق، وذلك ضمن ضوابط القواعد العامة في قانون الإجراءات الجزائية المتمثلة في إذن السلطة القضائية المختصة واحترام إجراءات وآجال تفتيش المساكن وضبط الأدلة، واحترام حرمة الحياة الخاصة.

ورغم كل المحاولات التي بذلها المشرع الجزائري في محاربة هذه الجريمة إلا أنها تعتبر غير كافية وذلك بسبب التطور الكبير في مختلف الأجهزة الإلكترونية.

ويمكن تلخيص النتيجة التالية:

-إنّ تغيير طبيعة الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال من طبيعة قضائية، حيث كانت تخضع لإشراف القضاء ومراقبته من خلال القضاة المشرفين والمترأسين لمديرية اليقظة الوقائية وكذا ترأس قاض لوحدة المراقبة، وكذا تنوع تشكيلة الضبطية القضائية التي تقوم بإجراءات التحري وتحول هذه الهيئة إلى إشراف السلطة العسكرية ممثلة في وزارة الدفاع لا يؤثر في الحقيقة على عملها حيث أنها تبقى في صميمها تعمل تحت رقابة القضاء بموجب المادة 13 من المرسوم 19-172، حيث يتطلب الامر إذن قضائي مكتوب للقيام بإجراءات المراقبة والتفتيش، كما أنّ ضباط الأمن العسكري الذين يمارسون مهامهم بوصفهم ضباط شرطة قضائية ملزمون قانونا بأداء مهامهم ضمن ما نصّ عليه قانون الإجراءات الجزائية، وهو نفس القانون الذي يقدم ضمانات احترام حرمة الحياة الخاصة وحرمة البيانات الخاصة وكذا يضمن احترام قواعد استخلاص الدليل الجزائي.

ومن خلال ما سبق يمكن تقديم الاقتراحات التالية:

-العمل على وضع بروتوكولات تعاون مشترك بين الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال وباقي الهيئات المتخصصة، كالهيئة الوطنية للوقاية ومكافحة جرائم الفساد، الديوان الوطني لقمع الفساد، المجلس الوطني لحقوق الإنسان؛

-التأكيد على وجوب الحصول على إذن مسبق من طرف القاضي المكلف بإجراءات المراقبة عند تحديد المراقبة؛

-توفير الإمكانات البشرية والمادية والتقنية الحديثة للمراكز والأجهزة المتخصصة في مكافحة الجرائم الإلكترونية؛

-وضع قواعد واضحة حول سرية البيانات المتحصل عليها أثناء التفتيش وحجز الأدلة.

قائمة المصادر والمراجع

أولا: النصوص القانونية

أ-المعاهدات

1.اتفاقية بودابست لمكافحة الجرائم المعلوماتية الخاصة بالاتحاد الأوروبي الموقعة بتاريخ 2001/11/23.

2. معاهدة الأمم المتحدة النموذجية حول نقل الإجراءات في المسائل الجنائية، اعتمدت بقرار رقم 118-45 في 14 ديسمبر 1990.
3. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت للتوقيع والتصديق والانضمام بموجب الجمعية العامة المؤرخة في 15 نوفمبر 200، صادقت عليها الجزائر بالمرسوم رقم 02-55 المؤرخ في 05 فيفري 2002، الجريدة الرسمية، العدد 09.

ب-القوانين

1. القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
2. القانون رقم 18-14المؤرخ في 16 ذي القعدة 1439الموافق لـ 29 يوليو 2018، المعدل والمتمم للأمر رقم71-28 المتضمن قانون القضاء العسكري، الجريدة الرسمية، عدد 47.
3. قانون الإجراءات الجزائية.
4. قانون عقوبات جزائري.

ج-الأوامر

1. أمر رقم 12-02 مؤرخ في 20 ربيع الأول عام 1433 الموافق لـ 13 فبراير سنة 2012، المعدل والمتمم للقانون رقم 05-01 المؤرخ في 27 ذي الحجة عام 1425 الموافق لـ 6 فبراير سنة 2005، والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها، ج ر ع 08، 2012.
2. الأمر رقم 66-155 المعدل والمتمم بالقانون رقم 06-22 المتضمن قانون الإجراءات الجزائية.

د-المراسيم الرئاسية

1. المرسوم الرئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436 الموافق لـ 8 أكتوبر سنة 2015، المحدد لتشكيلة وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ع 53.
2. المرسوم التنفيذي رقم 06-05 مؤرخ في 2006/1/9 المتضمن شكل الإخطار بالشبهة ونموذجه ومحتواه وصل استلامه، ج ر ع 02، سنة 2006.
3. النظام 05-04 المؤرخ في 13-10-2005 المتعلق بنظام التسوية الفورية الإجمالية والدفع المستعجل ج ر ع 02.
4. النظام 05-07 المتعلق بأمن أنظمة الدفع بتاريخ 28-12-2005 ج ر ع 37.
5. النظام 12-03 مؤرخ في 14 محرم عام 1434 الموافق لـ 28 نوفمبر 2012 المتعلق بالوقاية منتبييض الأموال وتمويل الإرهاب ومكافحتها، ج ر ع 12 لسنة 2013.
6. النظام 05-06 المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى، الجريدة الرسمية رقم 26 المؤرخة في 23 أفريل 2006.

ثانيا: الكتب

1. رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، طبعة 1، سنة 2012.
2. عبد العزيز شافي، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، طرابلس 2007.
3. عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائرية، التحري والتحقيق، دار هومة للنشر والتوزيع، الجزائر، 2009.
4. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، طبعة 2، القاهرة، 2000.
5. عبد الهادي بن زيطة، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية، طبعة 1، 2007.
6. محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، منشورات الحلبي الحقوقية، طبعة 1، 2009.
7. منير محمد الجنبيهي، ممدوح الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2004.

ثالثا: المقالات

1. جودة حسين جهاد، المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، مؤتمر القانون والكمبيوتر والانترنت، الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد 3، طبعة 3، 1-3 ماي 2000، 2004.
2. صفوت عبد السلام، الآثار الاقتصادية لعمليات غسيل الأموال ودور البنوك في مكافحة هذه العملية، مجلة الحقوق، جامعة الكويت، عدد 2، سنة 29، يونيو 2005.
3. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، المجلة العربية للدراسات الأمنية والتدريب، علمية، دورية، محكمة، عدد 30، نوفمبر2000.

رابعا: رسائل الدكتوراه والماجستير

1. عمر عبيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان وفقا للمعطيات التكنولوجية المعاصرة، أطروحة دكتوراه في القانون الجنائي، كلية الحقوف، جامعة القاهرة، 2006.
2. أحمد بن زايد وجوهر الحسن المهندي، تفتيش الحاسب الآلي وضمانات المتهم، رسالة ماجستير، كلية الحقوق، جامعة القاهرة، 2009.

خامسا: المواقع الالكترونية

1. http://rm.coeexplonatory

الهوامش والإحالات:

[1]: المرسوم الرئاسي 15-261 المؤرخ في 24 ذي الحجة عام 1436 الموافق لـ 8 أكتوبر 2015 المحدد لتشكيلة وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الجريدة الرسمية عدد 53 الصادرة سنة 2015.

[2]: المرسوم الرئاسي 19-172 المؤرخ في 3 شوال 1440الموافق لـ 6 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتنظيمها وكيفيات سيرها، الجريدة الرسمية عدد 37 الصادرة في 9 يونيو 2019.

[3]: المادة 2 من المرسوم الرئاسي 19-172 السالف الذكر.

[4]: جاء ذكر المديرية التقنية في المواد 11،12،13،14، من المرسوم الرئاسي 19-172السالف الذكر.

[5]: جاء ذكر مديرية الإدارة والوسائل في المادة 15 من المرسوم الرئاسي 19-172السالف الذكر.

[6]: المادة 6 من المرسوم الرئاسي 19-172 السالف الذكر.

[7]:القانون رقم 18-14المؤرخ في 16 ذي القعدة 1439الموافق لـ 29 يوليو 2018، المعدل والمتمم للأمر رقم71-28 المتضمن قانون القضاء العسكري، الجريدة الرسمية، عدد 47.

[8]: المادة 197 من قانون العقوبات.

[9]: المادة 17 من النظام 12-03 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها والتي نصت على " يتعين على المصارف والمؤسسات المالية والمصالح المالية لبريد الجزائر في إطار التحويلات الإلكترونية مهما كانت الوسيلة المستعملة (SWIFT, ATCI, ARTS)و/أو وضع الأموال تحت التصرف، أن تسهر على التحقق بدقة من هوية الأمر بالعملية والمستفيد بالإضافة إلى عنوانيهما.

[10]: معاهدة الأمم المتحدة النموذجية حول نقل الإجراءات في المسائل الجنائية، اعتمدت بقرار رقم 118-45 في 14 ديسمبر 1990.

[11]: جودة حسين جهاد، المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، مؤتمر القانون والكمبيوتر والانترنت، الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد 3، طبعة 3، 1-3 ماي 2000، 2004، ص. 1109

[12]: المادة 17 من القانون 09-04.

[13]: محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، المجلة العربية للدراسات الأمنية والتدريب، علمية، دورية، محكمة، عدد 30، نوفمبر 2000، ص.ص. 349، 353

[14]: المواد 15-16 من قانون الإجراءات الجزائية.

[15]: المادة 18 من قانون الإجراءات الجزائية.

[16]: رشيدة بوكر، المرجع السابق، ص. 374، -كذلك انظر جودة حسين جهاد، المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد 3، طبعة 3، من 1-3 ماي 2000، سنة 2004، ص. 111.

[17]: رشيدة بوكر، المرجع السابق، ص. 374

[18]: منير محمد الجنبيهي، ممدوح الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2004، ص. 18

[19]: المادة 4 فقرة "ج" من القانون 09-04.

[20]: المادة 3 من القانون 09-04.

[21]: المواد 31-32 من قانون العقوبات والمادة 4 من القانون 09-04.

[22]: اتفاقية بودابست لمكافحة الجرائم المعلوماتية الخاصة بالاتحاد الأوروبي الموقعة بتاريخ 2001/11/23، تاريخ الاطلاع على الموقع 2021/03/03 http://rm.coeexplonatory على الساعة 12:00.

[23]: المادة 21، 22 من المرسوم الرئاسي 15-261 السالف الذكر.

[24]: المادة الأولى من اتفاقية بودابست، المرجع السابق.

[25]: المادة 87 مكرر من قانون العقوبات، كذلك راجع المادة 4 من قانون 09-04، -هناك عدة تعريفات للاتصالات الإلكترونية في العديد من القوانين والأنظمة منها: قانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، نظام 05-06 المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى، الجريدة الرسمية رقم 26 المؤرخة في 23 أفريل 2006. نظام 05-07 المتضمن أمن أنظمة الدفع.

[26]: رشيد بوبكر، المرجع السابق، ص. 370

[27]: المواد 81، 82، 83 من قانون الإجراءات الجزائية.

[28]: عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائرية، التحري والتحقيق، دار هومة للنشر والتوزيع، الجزائر، 2009، ص. 266، –كذلك: أحمد بن زايد وجوهر الحسن المهندي، تفتيش الحاسب الآلي وضمانات المتهم، رسالة ماجستير، كلية الحقوق، جامعة القاهرة، 2009، دون صفحة.

[29]: عبد الله حسين علي محمود، المرجع السابق، صص. 107، 109، 122. – كذلك راجع: محمد أمين الشوايكة، المرجع السابق، ص 169، 170، 238، 239، 219.

[30]: النظام 05-04 المؤرخ في 13-10-2005 المتعلق بنظام التسوية الفورية الإجمالية والدفع المستعجل.

[31]: النظام 05-06 المتعلق بالمقاصة الإلكترونية للصكوك ووسائل الدفع الأخرى الموجهة للجمهور العريض، المرجع السابق.

[32]: عبد العزيز شافي، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، طرابلس 2007، ص.ص. 142، 147.

[33]: عبد العزيز شافي، المرجع السابق، ص.ص. 142، 147، كذلك راجع: محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، منشورات الحلبي الحقوقية، طبعة 1، 2009، ص.ص. 54 إلى 62.

[34]: عبد الله حسين علي محمود، المرجع السابق، ص 369. – كذلك: عبد الهادي بن زيطة، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية، طبعة 1، 2007، ص 10 إلى 19. –كذلك: محمد أمين البشري المرجع السابق، ص.ص. 322، 323.

[35]: رشيدة بوكر، المرجع السابق، ص 418.

[36]: المادة 6 من القانون 09-04 السالف الذكر.

[37]: المادة 7 من القانون 09-04 السالف الذكر،كذلك: رشيدة بوكر، المرجع السابق، ص. 422