جامعة قاصدي مرباح – ورقلة–

كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير

قسم علوم التسيير

مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني

الميدان: العلوم الاقتصادية والعلوم التجارية وعلوم التسيير

تخصص: إدارة التحقيقات الاقتصادية والمالية

بعنوان:

الجريمة المعلوماتية في التشريع الجزائري

من اعداد الطالب: عمار حشمان

نوقشت وأجيزت بتاريخ: 02 جويلية 2019

أمام اللجنة المكونة من السادة الاعضاء:

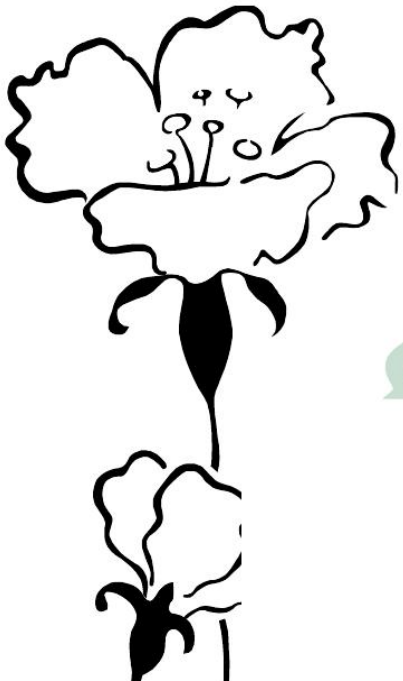
د/ رجـــم خـــالـــد (أستاذ "أ" جامعة ورقلة) – رئيسا.

د/ طواهير عبد الجليل (أستاذ محاضر"ب" جامعة ورقلة) – مشرفا ومقررا.

د/ بوخلة باديس (أستاذ محاضر"أ" جامعة ورقلة) – مناقشا.

السنة الجامعية: 2019/2018


بسم الله الرحمن الرحيم



إهداء

إلى من لا يمكن للكلمات

أن توفي حقهما، الوالدين الكريمين

إلى من لا أستطيع الاستغناء عنهم،

زوجتي وإلى كل الأهل و الأقارب

وجميع الأصدقاء والزملاء

عمار.

شكر وعرفان

أشكر أولا وأخيرا الله تعالى الذي أسبغ علينا نعمه ظاهرة وباطنة، وأمدني بالصبر لتذلل الصعوبات أمامي وأعانني كل العون على إنجاز هذه المذكرة، ثم أشكر أستاذي الكريم عبد الجليل طواهير الذي قبل الإشراف على مذكرتي وساعدني خطوة بخطوة لبلوغ نهاية البحث.

وأشكر كل من ساهم وبذل جهدا ولو بالقليل في إنجاز هذه المذكرة، كما أشكر الأساتذة الكرام أعضاء لجنة المناقشة على تفضلهم بقبول المناقشة.

عمار حشمان

الملخص

تطرح الجريمة المعلوماتية العديد من المشاكل من ناحية القانون الإجرائي، إذ يصعب على المحققين إجراء تحقيق وجمع الأدلة الرقمية، بإتباع الإجراءات التقليدية للتحقيق: كالمعاينة، التفتيش، الضبط، ... الخ. في هذا السياق ورغبة منها في مكافحة فعالة للجريمة المعلوماتية، تبنت الجزائر أساليب جديدة للتحري، من خلال: تعديل قانون العقوبات بموجب القانون رقم 06-22 بتاريخ 20 ديسمبر 2006 عن طريق إضافة إجراءات جديدة تطبق على جرائم المساس بأنظمة المعالجة الآلية للمعطيات. وفي 2009 أصدر المشرع الجزائري القانون رقم 09-04 المؤرخ في 05 أوت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، في هذا القانون خلق المشرع آليات جديدة خاصة للتحري من أجل مكافحة الجريمة المعلوماتية، إلا أن هذه الأساليب الحديثة للتحري أثارت مشكلة مدى مشروعيتها، خاصة وأنها تمس بالحقوق والحريات الأساسية للفرد والمعترف بها في الاتفاقيات الدولية، ولحل هذا الإشكال فقد وضعت شروط وضمانات يقتضي على السلطات القضائية مراعاتها عند الإذن بهذه الأساليب.

Résumé:

La cybercriminalité pose de nombreux problèmes juridiques au niveau du droit processuel, car il est Difficile pour les enquêteurs de mener une enquête et la collecte de preuves numériques, conformément aux procédures traditionnelles d'enquête: constatations matérielles, perquisitions, saisies, etc . Dans ce contexte et animé par le souci de lutte contre la cybercriminalité, l'Algérie a adaptées des nouvelles méthodes d'investigation. Cela se traduit par : La modification du code de procédure pénale par la loi N ° 06-22 du 20 Décembre 2006 en ajutant des Novelles dispositions qui s'appliquent sur les infractions relatives aux atteintes aux systèmes de traitement automatisés de données .Et en 2009 le législateur Algérien a promulgué la loi N° 09-04 du 05 Aout 2009 contenant les règles particulières relatives à la préventions et à la lutte contre les infractions liées au technologies de l'information et de la communication, dans cette loi le législateur a crée des novelles procédures spécifiques d'investigation pour lutter contre la cybercriminalité.

Cependant, ces méthodes modernes d'investigation soulèvent la problématique de leur légitimation surtout parce qu'elles affectent les droits et libertés fondamentaux de l'individu reconnus à l'échelle des conventions internationales .Et dans le but de résoudre cette confusion, des conditions des garanties on été imposées aux autorités judiciaires lors de l'autorisation de ces méthodes.

قائمة المحتويات

القائمة المحتويات

المقدمة

شهد العالم ثورة مذهلة في مجال التكنولوجيا والاتصالات وتقنية المعلومات، حتى أن مقولة أن العالم أصبح قرية صغيرة، مقولة شارفت الصواب في معظمها، وهذه الثورة في التقنية، كان من أهم أوجه انتفاضتها، التقدم المذهل في مجال الحواسيب الآلية وملحقاتها، والبرامج التي تلحق بها، كما بات الاعتماد على هذه التكنولوجيا واضحا جليا في كل الجهات الرسمية وغير الرسمية، حتى بات العنصر البشري يشكو من إحلال الأجهزة الذكية من حواسيب وبرامج محل الجهد البشري، حتى حل الذكاء الاصطناعي محل الذكاء البشري، على الرغم من أن هذه التكنولوجيا هي صناعة بشرية في الأساس، وأصبحت الدول تقاس مدى تقدمها بقدرتها على امتلاك والتعامل مع التكنولوجيا الحديثة في شتى مناحي الحياة، وبالرغم من هذه النعمة الكبيرة التي حلت بالجنس البشري، إلا أن هذه النعمة صاحبتها نقمة، تمثلت في الاستخدام الغير قانوني لهذه التكنولوجيا، حتى أصبحت هذه التكنولوجيا تستخدم كمعول هدم لا للبناء، في ايدي الخارجين عن القانون، ذوو الصفات الخاصة، صاحبو الاجرام الناعم، الذي لا يراق فيه نقطة دماء، وبالرغم من خطورة هذه الجرائم، نجد صعيد آخر أنه نظرا لأن هذه الجريمة عابرة للحدود، فإن هذا السلوك الاجرامي الذي يستخدم شبكات المعلومات والتكنولوجيا الحديثة، يسهل التهرب من العقاب، حيث ترتكب كثير من هذه الجرائم من على بُعد دولي.

وقد انتشرت في الآونة الأخيرة وأصبحت ظاهرة جديرة بالنظر والاعتبار، الاجرام المستحدث، الذي يتم عن طريق التكنولوجيا، فهي الجريمة المعلوماتية، والتي أصبحت ظاهرة تخترق المجتمع وتهدد دعائمه، ولعله الجوهر والسبب الرئيسي لتجريم هذه الجريمة، وهو ما دعا المشرع الجزائري إلى سن تشريعات تتماشى مع المستجدات على الساحة الاجرامية، ووضع نصوصا واضحة فيها عقوبة الجاني واهتم شُراح القانون بتفسير هذه التشريعات وشرحها، وبيان أركان الجريمة التي تقوم عليها.

مشكلة الدراسة:

ساهم التقدم الهائل الذي أضحى واضحا في المجال التكنولوجي، والزيادة في عدد مستخدمي التكنولوجيا والأجهزة الحديثة، من اشخاص طبيعية، أو هيئات واشخاص معنوية، كل ذلك أسهم في ظهور فئة جديدة من الاجرام، مرتبطة بالتكنولوجيا، ومنها جرائم المعلوماتية، ونظرا لتزايد نسب ارتكاب هذه الجريمة في الآونة الأخيرة، الأمر الذي أدى إلى انعكاسها على مضمون الأنظمة والقوانين، حتى تتماشى مع طبيعة الجريمة ومعطياتها، وآثارها.

وبناء عليه كانت الحاجة ملحة لوضع هذا الموضوع موضع الدراسة والتحليل، ولتعريف بالجريمة المعلوماتية، وأسس قيام المسؤولية الجنائي لفاعل الجريمة، وذلك في التشريع الجزائري، وبناء على كل ذلك، نطرح اشكالية الدراسة المحورية:

ما هي آليات واجراءات الكشف عن الجريمة المعلوماتية في التشريع الجزائري؟

تساؤلات الدراسة:

ومن هذه الاشكالية الرئيسية، يتفرع عدة تساؤلا فرعية، تقف مع الاشكالية الرئيسية لتقيم بنيان البحث وهي كالتالي:

- ما هي الجريمة المعلوماتية؟
- هل للجريمة المعلوماتية أنواع وأهدافها؟
- هل للجريمة المعلوماتية أركان؟
- هل يوجد آليات المؤسساتية المختصة للكشف عن الجريمة المعلوماتية؟
- ما هي إجراءات التحقيق في الجريمة المعلوماتية؟

فرضيات البحث:

- الجريمة المعلوماتية أحد صور الجرائم التقليدية.
- للجريمة المعلوماتية أنواع وأهداف.
- للجريمة المعلوماتية نفس الأركان الجريمة التقليدية.
- للجريمة المعلوماتية هيئات وآليات قانونية للكشف عنها في التشريع الجزائري.

أسباب اختيار الموضوع:

من بين الأسباب التي دفعتني إلى اختياري لهذا الموضوع:

- استفحال وانتشار ما أصبح يعرف بالجرائم المعلوماتية مما جعلها هاجسا وخطرا على المستوى العالمي، لما تلحقه هذه الجرائم من أضرار على اقتصاديات الدول، ما يستوجب إقامة أجهزة كفيلة بالإشراف على مكافحة هذه الجريمة وآليات التحقيق فيها.
- إن الجريمة المعلوماتية ورغم أهميتها في نطاق الدراسة والبحث فإنها لم تحظ بالعناية الكافية من قبل الباحثين في بحوثهم وعولجت بطريقة عامة سطحية وصنفت كباقي الجرائم الأخرى، لذا فإنه من الضروري إعطاء توضيح شامل لهذه الجريمة، سواء بالنسبة للدارسين أو أولئك الذين يعملون على تطبيق النص الإجرامي الخاص المساس الانظمة المعلوماتية في الميدان العملي.
- محاولة المزاوجة بين ما هو نظري وما هو تطبيقي، كون كل الدراسات السابقة لم تتطرق لهذا.

أهداف الدراسة:

- تهدف الدراسة إلى التعرف ودراسة العديد من النقاط وهي:
- التعرف على الجريمة المعلوماتية.

- التعرف على أهداف ارتكاب الجريمة المعلوماتية.
- دراسة أركان الجريمة المعلوماتية في التشريع الجزائري.
- التعرف على الهيئات المختصة لمكافحة الجريمة المعلوماتية.
- التعرف على إجراءات التحقيق للكشف عن الجريمة المعلوماتية.

أهمية الدراسة:

أولاً: الأهمية العلمية:

تظهر الأهمية العلمية للدراسة في تسليط الضوء على المسؤولية الجنائية لمرتكب جريمة المعلوماتية في التشريع الجزائري، حيث أن تفشي هذه الجريمة أصبح يشكل خطرا كبيراً، لذا ارتأينا أن نقوم بدراسة مستفيضة لمسؤولية فاعل الجريمة، ولعل في هذا العمل ما يكون نواة يستند إليها الباحثين ورواد القانون والعاملين في المجال القانوني.

ثانيا: الأهمية العملية:

تظهر الأهمية العملية لهذه الدراسة لاستيعاب هذا النوع من المخاطر المستحدثة، والحد منها داخل المجتمع، والتقليل من آثارها، وزيادة الوعي لدى مستخدمي الأجهزة الحديثة بمخاطر هذه الجريمة، وبأخذ الحذر والحيطة في الاستخدام.

حدود الدراسة:

الحدود الموضوعية: تتناول هذه الدراسة القانونية العلمية للجريمة المعلوماتية، والمسؤولية الجنائية اتجاه هذا النوع من الإجرام، وإجراء دراسة على التشريع الجزائري، وحتى يتأتى ذلك نعرض لماهية الجريمة المعلوماتية وأنواعها، وأركان هذه الجريمة، والعقوبات المقررة بشأنها للقضاء عليها.

منهج الدراسة:

استخدم الباحث في هذا البحث المنهج الوصفي التحليلي، الذي يقوم على أساس تحديد خصائص المشكلة محل البحث، ووصف ماهيتها وأسبابها، ثم تحليل هذه المشكلة والتعرف على أنواعها وأهدافها، وذلك للوصول لمعالجة المسؤولية الجنائية عن الجريمة المعلوماتية، في التشريع الجزائري، وهو المنهج الذي ساعدتنا في الوصول إلى مجموعة من النتائج الدقيقة.

الدراسات السابقة:

- رسالة ماجستير: "**اليات مكافحة جرائم تكنولوجيات الاعلام والاتصال على ضوء قانون 04/09**" بجامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية قسم الحقوق، أحمد مسعود مريم سنة 2013/2012 تناول فيها الباحث الجرائم المتصلة بالتكنولوجيات العلام والاتصال وآليات مكافحتها التي جاء بها القانون 04/09.
- رسالة ماجستير: "**جرائم الماسة بالأنظمة المعالجة الالية للمعطيات**" بجامعة وهران، كلية الحقوق، نسيمة جدي، سنة 2014/2013 التي تناول الباحث الجرائم الماسة بالأنظمة المعالجة للمعطيات الواردة في القانون العقوبات.
- رسالة ماجستير: "**الاطار لقانوني لمكافحة الجريمة المعلوماتية في التشريع الجزائري والتشريع المقارن**" جامعة باتنة، كلية الحقوق والعلوم السياسية قسم الحقوق، عبد اللطيف معتوق، سنة 2013/2011، تناول في الباحث نظرة المشرع الجزائري ومقارنته بموقف التشريع الفرنسي والتشريعات العربية وتناول التعاون الدولي في مجال مكافحة الجريمة المعلوماتية.

صعوبات الدراسة:

الصعوبات التي واجهتني في إعداده والمتمثلة أساسا في:

– قصر الوقت المخصص لتحضير المذكرة، خاصة وأن تحديد موضوع المذكرة والأستاذ المشرف كانا متأخرين.

– صعوبة الاتصال بالأستاذ المشرف بسبب ارتباطات العمل.

– صعوبة التنقل بين مكان العمل والمؤسسة الخارجية وكذا مكتبة الجامعة.

– طبيعة الموضوع في حد ذاته وعدم معالجته من قبل بالتحديد وتداخل مفهومه وتعدد استعمالاته بين عدة تخصصات، علم الاقتصاد، القانون والإدارة ... إلخ.

للإجابة على الإشكالية الرئيسية للموضوع، مع ما ينبثق عنها من إشكالات فرعية، قمنا بتقسيم الدراسة إلى: مقدمة، وفصلين، وخاتمة.

خصصنا **الفصل الأول** لدراسة كل ما يتعلق بالجريمة المعلوماتية من خلال مبحثين، بينا تناولنا في **المبحث الأول** ماهية الجريمة المعلوماتية، تعريف، أنواع، الطبيعة القانونية، كما درسنا في **المبحث الثاني** الحماية الجنائية من خلال النصوص القانونية.

أما **الفصل الثاني** تطرقنا فيه **آليات وإجراءات التحري في مجال الجريمة المعلوماتية** وذلك في مبحثين، في **المبحث الأول** الوحدات المختصة في مكافحة الجريمة المعلوماتية، **والمبحث الثاني** إجراءات التحري للكشف عن الجريمة المعلوماتية.

الفصل الأول
الإطار المفاهيمي
للجريمة المعلوماتية

تمهيد:

تعد الجريمة المعلوماتية، من أكبر التحديات التي نواجهها في عالمنا المعاصر، إن لم تكن أكبرها على الإطلاق، والحديث عن هذه التحديات يتطلب أولاً إعطاء صورة عامة عن تحديد ماهيتها، قبل التعرض إلى بحث المسؤولية الجنائية الناتجة عنها، وهو ما يدعونا إلى التعرض إلى ماهية الجريمة المعلوماتية بتعريفها، أنواعها، أهدافها في المبحث الأول قبل التعرض إلى بحث إشكاليات المسؤولية الجنائية وتحدي المعلوماتية للقواعد العامة للمسؤولية الجنائية في المبحث الثاني.

المبحث الأول: ماهية الجريمة المعلوماتية

سوف نتطرق في هذا المبحث إلى مفهوم أنواع وأهداف الجريمة المعلوماتية (المطلب الأول)، وتحديد طبيعتها القانونية وخصائصها وأركانها (المطلب الثاني).

المطلب الأول: مفهوم، أنواع، أهداف الجريمة المعلوماتية

عددت تعريفات الجريمة المعلوماتية وتباينت فيما بينها ضيقا واتساعا وقد أسفر ذلك على تعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية، وما سيتبع ذلك للوصول إلى إيجاد الحلول المناسبة لمواجهتها.

الفرع الأول: تعريف الجريمة المعلوماتية

مع دخول الحاسوب والانترنت إلى مجتمعاتنا وفي كافة جوانب حياتنا بدأ يظهر نوع جديد من الجرائم تسمى الجرائم المعلوماتية وبالتالي أصبح هناك حاجة لتعريف هذه الجرائم والتوعية حولها، حيث سنقوم بتعريفها قانونيا وفقهيا.

أولا: التعريف الفقهي

لقد أعطى الفقهاء والدارسون عددا ليس قليلا من التعريفات تتميز وتباين تبعا لموضع العالم المنتمية إليه وتبعا لمعيار التعريف ذاته، وقد اجتهدنا في جمع غالبية التعريفات التي وضعت في هذا الحقل.

فمن التعريفات التي تستند إلى موضوع الجريمة أو أحيانا إلى أنماط السلوك محل التجرم، تعريف الأستاذ ROSENBALT بأنه نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقة أو هي كما عرفها الفقيه سولا رز أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات.

أما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة فان أصحابها ينطلقون من أن الجرائم المعلوماتية تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة، ومن هذه التعريفات:

تعريف الأستاذ جون فور ستر " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية وبعرفها تادمان بأنها كل أشكال السلوك غير المشروع الذي يرتكب بواسطة الحاسب[1].

ونشير أيضا إلى أن جانبا من الفقه والمؤسسات ذات العلاقة بهذا الموضوع وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل تعرف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979 حيث عرفت الجريمة المعلوماتية أي جريمة لفاعلها معرفة فنية بالحاسبات تمكن من ارتكابها.

كما عرفها الأستاذ" دافيد تومسن "أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها المعرفة بتقنية الحاسب الآلي[2].

ثانيا: التعريف القانوني

عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة 02-الفقرة – أ –من القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بالقول بأن " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي: **جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية**"

إذن وعملا بالتعاريف المقترحة للجريمة المعلوماتية، فإنه يمكننا اقتراح تعريف خاص يشمل كافة الجوانب "**المتعلقة بالجريمة هذه فنعرفها بأنها " كل السلوكات المجرمة التي يشكل الحاسوب وشبكات الاتصال الخاصة به وسيلة لارتكابها أو محلا لوقوعها، أي الجرائم التي ترتكب في البيئة الرقمية الإلكترونية**".

(1) – هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص 120.

(2) – هشام محمد فريد رستم، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة ،2000، ص 20.

الفرع الثاني: أنواع وأهداف الجريمة المعلوماتية

أولا: أنواع الجريمة المعلوماتية

أ/ الجرائم التي تقع على الأشخاص: هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع الشخصي البحث، أي الحقوق اللصيقة بالشخص والتي تعتبر من بين المقومات الشخصية وتخرج عن دائرة التعامل الاقتصادي، ومن أهم هذه الحقوق الحق في الحياة والحق في سلامة الجسم وفي الحرية والحق في صيانة الشرف.

1- الجريمة انتحال الشخصية: هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلا أنه ومع انتشار شبكة الانترنت فقد أخذ هذا النوع شكلا جديدا وهي انتحال شخصية الفرد على الشبكة الالكترونية واستغلالها أسوء استغلال وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شابهها من أجل الحصول على بطاقات ائتمانية وغيره، ومن خلال هذه المعلومات يستطيع المحرم إخفاء شخصيته الحقيقية والتصرف بحرية تحت اسم مستعار، وغالبا ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت[1].

2-جريمة المضايقة والملاحقة: وهو نوع حديث من الجرائم المتزايدة باستمرار مع كل إضفاء وتحديث يطال برامج الحوارات المتبادلة والدردشة، وهي عبارة عن مساحات معروفة في الفضاء الالكتروني تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض.

(1)- منير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص 42 43.

وجرائم الملاحقة تشمل رسائل تهديد وتخويف ومضايقة وقد شبه القضاة هذه الجريمة خارج الشبكات بجرائم التهديد العلني، ولا تتطلب الجريمة المرتكبة عبر الإنترنت أي اتصال مادي بين المجرم والضحية مما يدل أن لها تأثيرات سلبية نفسية فهي لا تؤدي إلى أي تصرفات عنف مادية[1].

3-جرائم التغرير والاستدراج: هي من أشهر جرائم الانترنت ومن أكثرها انتشارا خاصة بين أواسط صغار السن ومن مستخدمي الشبكة، وهي تقوم على عنصر الإمام حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة أو زواج على الانترنت والجريمة المعلوماتية التي قد تتطور إلى لقاء مادي بين الطرفين، وهذه الجرائم لا تعرف الحدود ولا يمكن حصرها، وهي دون حدود سياسية أو اجتماعية اذ يستطيع كل مراسل عبر الشبكة ارتكابها بكل سهولة وكذلك يقع ضحيتها أي مستخدم حسن النية[2].

4-جرائم التشهير وتشويه السمعة: مع انتشار الشائعات والأخبار الكاذبة التي تطول وتمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية أو حتى دينية، وقد ظهرت على شبكة الانترنت بعض المواقع والتي جندت نفسها لهدف واحد هو خدمة تلك الشائعات والأخبار الكاذبة وذلك بهدف تشهير وتشويه سمعة تلك الرموز، وكذلك لتسميم أفكار الناس أو محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم.

وأبرز وسائل ارتكاب هذه الجريمة إنشاء مواقع على الشبكة تحتوي المعلومات المطلوب إدراجها ونشرها أو إرسالها عبر المواقع الالكترونية، ومن أمثلتها إرسال الصور الغير اللائقة أو معلومات غير صحيحة[3].

5-الجرائم المخلة بالأخلاق والآداب العامة: إذا كانت شبكة الانترنت تتسم بالعالمية ولا تقتصر على مستخدم دون الآخر، فإن ما يتم عرضه من مواد تعد مخلة بالآداب والأخلاق العامة في بلد معين قد تشكل

(1) – محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004، ص 45.

(2) – عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السايسية، جامعة د. الطاهر مولاي، سعيدة ، سنة 2016/2015، ص 19.

(3) – منير محمد الحنبيهى، ممدوح محمد الجنبيهي، المرجع السابق، ص 34.

جريمة يعاقب عليها القانون في حين أنها لا تكون كذلك في أي بلد آخر، وتشمل هذه الجرائم تحريض القاصرين على أنشطة جنسية غير مشروعة وإفسادهم عبر الوسائل الالكترونية أو محاولة إغوائهم لإرتكاب هذه الأنشطة، أو نشر معلومات عنهم عبر الحاسب الآلي ودعوتهم إلى القيام بالأعمال الفاحشة، وتصوير قاصرين ضمن أنشطة للجنس.

والأعمال الإباحية هي من أشهر الأعمال الحالية وأكثرها رواجا خاصة في الدول العربية وأوروبا والدول الآسيوية، وتشمل الجرائم المخلة بالأخلاق والآداب العامة على الانترنت كافة الإشكال سواء كانت صور أو فيديو أو حوارات أو أرقام هاتفية مما خول هذه الشبكة أن تكون في متناول أيدي الجميع ودون أي حواجز[1].

ب/ الجرائم التي تقع على الأموال: هي جرائم الاعتداء على الأموال والتي تهدد الحقوق ذات القيمة المالية ويدخل في نطاق هاته الحقوق الحق ذو قيمة اقتصادية.

فإذا كان موضوع الاعتداء على الأموال في نطاق ما ينصب على الحاسب الآلي ذاته وما يرتبط به من أسلاك وما يتصل به من ملحقات فأنه هنا لا يثير أي صعوبة في تطبيق النصوص الجزائية التقليدية كون الأمر يتعلق بمال عادي منقول، أما إذا وقع الاعتداء على ما يتعلق بفن الحاسب الآلي من برمحيات ونظم فإن النصوص التشريعية التقليدية قاصرة عن حمايتها لما لهذا المجال من طابع خاص غير تقليدي[2].

1-جرائم صناعة ونشر الفيروسات: الفيروس هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي، ولكنها مصممة بحيث يمكنها التأثير على كافة البرامج الأخرى الموجودة على الجهاز بأن تجعل تلك البرامج نسخة منها أو أن تعمل على مسح كافة البرامج الأخرى وبالتالي تعطلها عن العمل.

(1) – انظر محمد امين احمد الشوابكة، المرجع أعلاه، ص 114.

(2) – انظر محمد امين احمد الشوابكة، المرجع السابق، ص 136.

وأما عن مبدأ عملها فيتحدد طبقا لأسلوب تصميمها، فقد تبدأ بالعمل بمجرد فتح الرسالة الموجودة بها، وقد تبدأ بمجرد تشغيل البرنامج الموجودة عليه، وتعتبر هذه الصناعة من أهم جرائم الانترنت وأكثرها اتساعا وانتشار، ويعود تاريخ الفيروسات لأول مرة في أربعينيات القرن الماضي حين تحدث عنها العالم الرياضي "فون نيو مان" على صعيد الحاسب الآلي دون الانترنت، ومن أشهرها فيروس رسائل الحب، فيروس الدودة الحمراء، وقد أحدث هذا الأخير أعطالا في أكثر من ربع مليون جهاز كمبيوتر في اقل من 9 ساعات عام 2001[1].

2-جرائم الاختراقات: الاختراق هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الغير والشبكات الالكترونية، ويتم هذا الاختراق بواسطة برامج متطورة يستخدمها كل من يملك الخبرة وله القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت لحماية تلك الحاسبات أو الشبكات.

وتختلف أسباب الاختراق باختلاف أهداف المخترق، فمنهم من يخترق أجهزة البعض أو مواقعهم لمجرد الفضول والبعض الأخر لسرقتها، وهذا هو السبب الأبرز الذي يدفع المخترقين إلى الدخول إلى مواقع الحواسيب الأخرى لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل مبلغ مالي للاطلاع عليها.

وقد يكون السبب تبديل أو تحريف أو تعطيل المعلومات في أجهزة الغير، وهو أخطر أنواع الاختراق، ومن أبرز ضحايا الاختراق فهي مواقع الانترنت التي يقوم المخترقون بتحريف تصاميمها ومعلوماتها وهذه العملية تسمى تغيير وجه الموقع[2].

3-جريمة تعطيل الأجهزة والشبكات: يطال التعطيل أجهزة الحاسب الآلي عبر برابحها، كما قد يؤدي تعطيل البرامج إلى أعطال فنية تقع على القطع الالكترونية للجهاز والهدف من التعطيل منع الحواسيب والشبكات من تأدية عملها دون أن تتم عملية اختراق فعلية لتلك الأجهزة وتتم عملية تعطيل الأجهزة عن

(1) – منير محمد الجنبيهى ممدوح محمد الجنبيهى، المرجع السابق، ص36.

(2) – منير محمد الجنبيهي ممدوح محمد الجنبيهي، المرجع أعلاه، ص 37.

طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطلها وهو الأمر الذي يعيقها عن تأدية عملها[1].

4-جريمة النصب والاحتيال[2]: أصبح التعاقد عبر الانترنت حاجة وضرورة نظرا لسرعة وسهولة التعامل عبرها، لكن هذه الميزة ما لبثت أن شابتها سلبيات عديدة هي عبارة عن أفعال إجرامية تعرف النصب والاحتيال ومن بينها:

- خرق التعاملات عبر طرق احتيال جديدة تم ابتكارها، وكذلك زادت من وقوع جرائم النصب التي لا يزال يقع فيها عدد كبير من مستخدمي الانترنت.

- إما المظهر الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية واستخدام هذه المعلومات لسرقة المبالغ الموجودة داخل حسابات الضحايا، ومرتكبو الجرائم عبر تلك الوسائل يسهل هروبهم وتواريهم لذلك من الصعب جدا ملاحقتهم والقبض عليهم.

ثانيا: أهداف الجريمة المعلوماتية

وتتمثل أهداف الجريمة المعلوماتية في التمكن من الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الإطلاع عليها أو حذفها أو تغييرها بما يحقق هدف المجرم، والتمكن من الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها أو التلاعب بمعطياته، كما يتم الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم من خلالها دافع مادي أو سياسي، وتحقق الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات اختراق وهدم المواقع على الشبكة العنكوبتية وتزوير وسرقة الحسابات المصرفية.

(1) – منير محمد الجنبيهي ممدوح محمد الجنبيهي، المرجع أعلاه، ص 38.

(2) – عبد الكريم شيباني ، مرجع سابق، ص23.

المطلب الثاني: الطبيعة القانونية للجريمة المعلوماتية

قبل التطرق الى أركان الجريمة المعلوماتية يجب معرفة خصائص هذه الجريمة المعلوماتية وهذا ما سنطرق إليه في الفرع الأول وإلى أركانها في الفرع الثاني.

الفرع الأول: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواحي، سواء كان هذا التميز في السمات العامة لها أو في الباعث على تنفيذها أو في طريقة هذا التنفيذ ومن أهم خصائصها:

أولا: صعوبة اكتشاف الجريمة المعلوماتية

تتسم الجرائم الناشئة عن استخدام الانترنت بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة مثلا عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وسرقة المكالمات وغيرها من الجرائم[1].

كما أن وسيلة تنفيذها تتميز في أغلب الأحيان بالطابع التقني الذي يضفي عليها الكثير من التعقيد بالإضافة إلى الأحجام عن التبليغ عنها في حالة اكتشافها لخشية المجني عليهم فقدان عملائهم فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل إثبات في مدة تقل عن الثانية[2].

ثانيا: صعوبة إثبات الجريمة المعلوماتية

فالجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق

(1) – محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، ص32.

(2) – نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2 ، دار الثقافة للنشر والتوزيع، ص.56

والملاحقة، ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلبها لاكتشافها والبحث عنها، وتستلزم أسلوب خاص في التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، نظرا لنقص المعارف وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي ضد هذه الظاهرة، حيث لم تعد القوانين التقليدية قادرة على مواجهة تطور الجريمة المعلوماتية في ظل السرعة الهائلة للتطورات التكنولوجية[1].

ثالثا: أسلوب ارتكاب الجريمة المعلوماتية

الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها، فإذا كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة الخلع أو الكسر كما هو الحال في جريمة السرقة[2]، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت مع وجود مجرم يوظف خبرته التوجه النظري والإطار المنهجي للدراسة أو اختراق خصوصيات الغير للتغرير وقدراته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس بالقاصرين كل ذلك دون الحاجة لسفك الدماء).

رابعا: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص

تتميز الجريمة المعلوماتية عادة أنها تتم بتعاون أكثر من شخص على ارتكابها للإضرار بالجهة المجني عليها، وغالبا ما يشترك في إخراج الجريمة المعلوماتية إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت، يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه[3].

(1) – محمد عبيد الكعبي، مرجع سابق، ص40.

(2) – نهلا عبد القادر المومني، مرجع سابق، ص 57–58.

(3) – محمد عبيد الكعيبي، المرجع السابق، ص 42.

خامسا: خصوصية مجرمي المعلوماتية

المجرم الذي يرتكب الجريمة المعلوماتية يطلق عليه تسمية المجرم الالكتروني أو المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (المجرم التقليدي)، فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الانترنت[1].

سادسا: الجريمة المعلوماتية جريمة عابرة للحدود

بعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها ألاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد.

الفرع الثاني: أركان الجريمة المعلوماتية

تتخذ الجريمة المرتكبة عبر الانترنت من الفضاء الافتراضي مسرحا لها، مما يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي، فهي تشترك بوجود الفعل غير المشروع، والمجرم يقوم بهذا الفعل، من خلال هذا التشابه سوف نتطرق إلى تبيان الأركان التي تقوم عليها هذه الجريمة.

(1) – نهلا عبد القادر المومني، مرجع سابق، ص 58–57.

أولا: الركن الشرعي

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضع العقاب المترتب عليه وقت وقوع هذا الفعل، يبني على ذلك عدم جواز ملاحظة الشخص عن فعل ارتكبه قبل صدور نص التجريم، وعن فعل ارتكبه بعد إلغاء نص التجريم كما لا يجوز قياس أفعال لم ينص المشرع على تجريمها وأفعال أخرى ورد نص التجريم عليها مهما يكن بينها من تشابه من حيث الدوافع أو الفاعلية أو النتائج أو العناصر، ذلك أنه لا يجوز أيضا التوسع في تفسير النصوص الجزائية، وعلى القضاة التقيد بمدلول النص والالتزام بمضامينه[1].

يترتب على إهمال قاعدة شرعية الجرائم والعقوبة نتيجة مهمة، تتمثل في عدم رجعية القاعدة الجنائية، أي بمفهوم المخالفة تنطبق القواعد الجنائية بأثر فوري ولا مجال لإهمالها بأثر رجعي، إلا إذا نص القانون على ذلك صراحة في النص القانوني أو إذا ما أعملت قاعدة تطبيق القانون الأصلح للمتهم[2].

إن الركن الشرعي للجريمة الذي هو الصفة غير المشروعة للفعل الذي يقوم به الجاني له ركنين أساسين:

- مطابقة الفعل لنص التجريم.
- ألا يخضع الفعل المرتكب لسبب من أسباب الإباحة.

يقصد بمطابقة الفعل لنص التجريم هو تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة، أما بالنسبة لخضوع الفعل لسبب من أسباب الإباحة فقد ذهب اجتهاد المحكمة العليا إلى أنه لتطبيق نظرية العقوبة المبررة أن يكون النص الواجب التطبيق يقرر نفس العقوبة[3].

(1)- أسامة احمد المناعة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان 2014، ص45.
(2)- حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الاولى، منشورات الحلبي الحقوقية، ب يروت2014، ص57.
(3) - بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007، ص94-95.

ثانيا: الركن المادي

يقصد بالركن المادي للجريمة كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، يؤدي إلى نتيجة تمس حقا من الحقوق، التي يكفلها الدستور والقانون وقد ذهب الدكتور رضا فرح إلى تقسيم الركن المادي في حد ذاته إلى ثلاث عناصر:

- السلوك الإجرامي.
- النتيجة الإجرامية.
- العلاقة السببية بين الفعل والنتيجة.

أ-**السلوك الإجرامي:** هذا السلوك يوجد بصورتين فقد يكون بفعل إيجابي، إذ يفترض في هذه الصورة قيام الجاني بفعل إرادي بغية إحداث نتيجة معينة، كما يمكن أن يكون بفعل سلبي يأخذ وصف الامتناع عن إتيان أمر يوجبه المشرع، وفي الجريمة المعلوماتية يمكن أن نجده بنوعيه السلوك الإيجابي او السلبي. لا ننسى التطور الكبير في محتوى وطبيعة هذا السلوك الإجرامي الذي تطور بتطور الوسائل التي وجدت بين يدي الفاعل، وهذا السلوك الذي طورته أيضا عقلية الفاعل الذكية، والتي استطاعت أن تخرج من تقليدية السلوك الجرمي إلى مساحات أكثر تعقيدا أوجدت بلا شك صعوبات كثيرة[1].

ب- **النتيجة الإجرامية:** يقصد بالنتيجة الإجرامية الأثر المادي الذي يحدث، فالسلوك قد أحدث تغييرا ملموسا، ومفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج، بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى[2].

ج- **العلاقة السببية بين الفعل والنتيجة:** تتمثل العلاقة السببية في الصلة التي تربط بين الفعل والنتيجة، وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة وأهمية الرابطة السببية ترجح إلى إسناد

(1) - أسامة احمد المناعة، جلال محمد الزغبي، المرجع السابق، ص51 -52.

(2) - بلعلبات إبراهيم، المرجع السابق، ص 18.

النتيجة الى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتحقق الرابطة السببية تلازما ماديا بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حد الشروع، إذ لا يعد مسؤولا عن النتيجة التي تحققت، أما إذا كانت غير عمدية فإن نفي رابطة سببية يؤدي إلى انتفاء المسؤولية كلية عنها ذلك أنه لا شروع في الجرائم غير العمدية[1].

ثالثا: الركن المعنوي

يقوم الركن المعنوي للجريمة المرتكبة عبر الانترنت على أساس مجسد في توافر الإرادة الجرمية لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون كانتحال شخصية المزود عبر الانترنت، وسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر النتيجة الجريمة المترتبة على الأفعال السابقة، فتكتسب إرادة الجاني الصفة المجرمة من العمل غير المشروع الذي يبين الشبه في ارتكابه وهو عالم بالآثار الضارة الناشئة عنه[2].

يختلف الركن المعنوي في الجرائم المعلوماتية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع لمحل الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله إلى نظام الحاسب الآلي خطأ أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي[3].

(1)- أسامة احمد المناعة، جلال محمد الزغبي، المرجع السابق، ص 58-59.

(2)- خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنات، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان2011، ص73-74.

(3)- حنان ريحان مبارك المضحاكي، المرجع السابق، ص 107.

وفي جريمة الاحتيال الإلكتروني التي بدورها جريمة عمدية، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعية العام والخاص، فالمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص أخر من ممتلكاته على نحو غير مشروع[1].

(1)- احمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الاسك ندرية2006، ص112-113.

المبحث الثاني: الحماية الجنائية من خلال النصوص القانونية

في هذا المبحث سوف نتطرق إلى موقف المشرع الجزائري من الجريمة المعلوماتية (المطلب الأول)، جرائم الاعتداء الماسة بالأنظمة المعلوماتية (المطلب الثاني).

المطلب الاول: موقف المشرع الجزائري من الجريمة المعلوماتية

لم يجد المشرع الجزائري بدا من تعديل قانون العقوبات لما كان فراغ قانوني في هذا المجال، وكان ذلك بموجب القانون رقم 15/04 المؤرخ في 2004/11/10 المتمم والمعادل للأمر 156/66 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات، ولقد جاء في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام.

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحول إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة.

لذلك فقد آثار المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات، وينصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج بذلك من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة لارتكابها، وحصرها فقط في صور الأفعال التي تشكل إعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها (الفرع الأول). ثم في مرحلة لاحقة اختار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بموجب القانون رقم 04/09 المتضمن الوقاية من هذه الجرائم ومكافحتها (الفرع الثاني).

الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات

تبنى المشرع الجزائري للدلالة على الجريمة المعلوماتية مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته أي المحتوى (Le contenant) وما يحتويه من مكونات غير مادية (Le contenu) محلا للجريمة المعلوماتية، ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أي جريمة من جرائم الاعتداء على هذا النظام، فإن ثبت تخلف هذا الشرط الأولي، فلا يكون هناك محال لهذا البحث إذ أن هذا الشرط يعتبر عنصرا لازما لكل منها.

ولما كانت مكونات النظام المعلوماتي غير المادية لا تظهر على حالة واحدة إذ قد تكون مخزنة به أو منقولة منه أو عليه، فإن الأمر يتوجب التطرق لدراسة المقصود بنظام المعالجة الآلية للمعطيات.

أولا: المقصود بنظام المعالجة الآلية للمعطيات[1]

إن عملية معالجة المعطيات تحتاج إلى آلية منظمة تتولى عمليات جمع وتوفير المعلومات اللازمة ومعالجتها، وهو الأمر الذي ولد الحاجة إلى إجراءات ووسائل تساعد على القيام بذلك فظهر بالنتيجة مصطلح نظم المعلومات المبنية على الحاسبات الآلية، أو ما يسمى بنظام المعلومات المحوسبة، وهو نظام يعتمد على المكونات والأجهزة البرمجية للحاسوب في معالجة المعطيات واسترجاع المعلومات.

فالتطور التقني الحاصل في عالم تكنولوجيا المعلومات وما يتطلبه من ضرورة القيام بمهام توفير وجمع ومعالجة وتبادل المعلومات في نفس الوقت أدى إلى ابتكار نظام المعالجة الآلية، والذي نشأ في الحقيقة بهدف وصف الحالة التي انبثقت عن اندماج تقنية نظم المعلومات وتقنية الاتصالات عن بعد.

(1)- سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، مذكرة مقدة لنيل شهادة الماجيستر في العلوم القانونية، جامعة الحاج لخضر باتنة، سنة دراسية 2013/2102، ص 42-43.

وقد تم تعريفه على أنه عبارة عن آلية وإجراءات منظمة تسمح بتجميع وتصنيف وفرز البيانات ومعالجتها ومن ثم تحويلها إلى معلومات يسترجعها الإنسان عند الحاجة ليتمكن من إنجاز عمل أو اتخاذ قرار أو القيام بأي وظيفة عن طريق المعرفة التي يحصل عليها من المعلومات المسترجعة من النظام.

والظاهر أن المشرع الجزائري عند تعديله لقانون العقوبات وإضافته للقسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات عارضا من خلاله صور هذه الاعتداءات لم يعرف نظام المعالجة الآلية للمعطيات، وأوكل بذلك مهمة تعريفه للفقه وقد حذا في ذلك موقف المشرع الفرنسي عندما لم تحتفظ الجمعية الوطنية الفرنسية بالتعريف الذي تقدم به مجلس الشيوخ الفرنسي النظام المعالجة الآلية بمناسبة تعديل قانون العقوبات وحذف من النص النهائي.

وإذا كان تعريف مجلس الشيوخ الفرنسي النظام المعالجة الآلية للمعلومات غير ملزم إلا انه يعتبر من الأعمال التحضيرية التي يمكن الاستعانة بما في تفسير غموض النص، كما يمكن للقضاء أن يستهدي به فيما يعرض عليه من منازعات في هذا الخصوص.

ونرى أن المشرع حسنا فعل حينما تجنب التقيد بتعريف محدد لنظام المعالجة الآلية للمعطيات، ذلك أن العناصر التي يتكون منها هذا النظام في حالة تطور تكنولوجي مستمر يخضع للتطورات السريعة والمتلاحقة التي تطرأ على البيئة التقنية التي يمثلها والتي تتسع لإمكانية شمول وسائل تقنية جديدة، لاسيما وأن العالم الافتراضي لا يزال في بدايته ولن يكون من السهولة احتواؤه، ومن جهة أخرى فإن نظام المعالجة الآلية للمعطيات يعاد تعبيرا فنيا يصعب على المشتغل بالقانون إدراك طبيعته.

أما على المستوى الدولي فإن الاتفاقية الدولية الإجرام تقنية المعلومات وقفت عند حد هذا المفهوم عندما عرفت نظام المعالجة الآلية للمعطيات بموجب الفقرة أمن المادة الأولى من الفصل الأول بعنوان

المصطلحات على "أنه كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معين بأداء معالجة آلية للبيانات.

كما أورد قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية في مادته الثانية تعريفا للنظام المعلوماتي باعتباره النظام الذي يستخدم لإنشاء رسائل البيانات وإرسالها واستلامها أو تخزينها أو لتجهيزها على أي وجه آخر.

كما عرفته الاتفاقية الأوروبية المبرمة في بوداسبت بشأن مكافحة جرائم الفضاء المعلوماتي بأنه "كل جهاز بمفرده أو مع غيره من الأجهزة المتواصلة بينيا أو المتصلة والتي يمكن أن يقوم واحد منها أو أكثر تنفيذا لبرنامج معين بأداء المعالجة الآلية للبيانات.

وفي مشروع القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات في صيغته المعادلة نجد في مادته الأولى تعريفا لنظام المعالجة الآلية للمعطيات على أنه كل مجموعة مركبة من وحدة أو عدة وحدات المعالجة سواء كانت متمثلة في ذاكرة الحاسوب وبرامجه أو وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة."

ومن خلال التعريفات التي تم ذكرها فإننا نستنتج أن مصطلح نظام المعالجة الآلية يستخدم في الحقل القانوني للدلالة على المعنى المقصود نفسه بهذا الاصطلاح وفقا لمفهومه العلمي، فهو إذن مصطلح ينطبق على أي نظام مهما كان مسماه يتوافر له عدة عناصر مرتبطة ببعضها بعدد معين من الروابط لتحقيق المعالجة الآلية للمعلومات من تجميعها وتخزينها ومعالجتها ونقلها وتبادلها وذلك من خلال برنامج معلوماتي.

وتبعا لذلك فإن حدود فكرة نظام المعالجة الآلية للمعطيات تقوم على أساس الروابط بين مختلف أجزاء هذا النظام والوجود المتزامن للأجهزة والبرامج، فالدخول إلى برنامج من أجل تعديله أو تحويله إلى استعمال غير الاستعمال المخصص له لا يشكل جريمة معلوماتية إلا إذا كان هذا البرنامج يشارك في

تطبيق فعلي داخل نظام كامل، ذلك أن البرنامج المعزول لا يأخذ تكييف النظام، وكذلك الشأن بالنسبة لأي من المكونات التي لا تشكل جزءا من النظام كما لو وقع الاعتداء على برامج معروضة للبيع، ولا يدخل أيضا في مفهوم نظام المعالجة الآلية للمعلومات المخزنة والتي لا توجد بالمعالجة، أي التي تعتبر كالأرشيف فالدخول عليها لا يمثل دخولا إلى نظام المعالجة الآلية للمعطيات، ذلك أن الأموال المعلوماتية المعزولة لا تطبق عليها عموما إلا القواعد التقليدية.

ثانيا: مدى اشتراط الحماية التقنية للنظام المعلوماتي[1]

لقد طرح الفقه القانوني مسألة هامة في شأن جرائم التعدي على نظام المعالجة الآلية للمعطيات، تتعلق بمدى اشتراط أن يكون النظام المعلوماتي متوفرا على الحماية التقنية حتى يحظى بالحماية الجزائية.

فقد ذهب الرأي الغالب في الفقه الفرنسي إلى عدم اشتراط الحماية التقنية للنظام حتى تقوم الجريمة المعلوماتية فبحسب هذا الرأي فإن نظام الأمن والحماية التقنية لا يكون سوى دور إيجابي وإثبات سوء نية من قام بانتهاك النظام والدخول إليه بطريقة غير شرعية، ويدخل في عداد إثبات القصد الجنائي وهذه مسألة أخرى، في حين ذهب الرأي الثاني في المسألة إلى القول بضرورة وجود نظام أمني لحماية النظام المعلوماتي حتى يعترف بتجريم الاعتداء على نظم معالجة البيانات، ويستند أنصار هذا الرأي إلى عدة حجج منها أن الاعتداء على النظام الأمني شرط مفترض لقيام الجريمة المعلوماتية، وأن القضاء يقضي بعدم العقاب على فعل يعاد اعتداء على حق لم يتحوط له صاحبه، بالإضافة إلى أن تغيب هذا الشرط يعد توسعا في التجريم فكل دخول إذن غير مشروع يعد جريمة وهو أمر غير منطقي.

إلا أن هذا الشرط أصبح في الوقت الراهن بدون موضوع، ذلك أن غالبية النظم المعلوماتية تتمتع بحماية فنية على درجة عالية من الكفاءة، بل إن هناك شركات متخصصة لتقديم هذه الخدمة في ظل تقدم

(1)- سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، المرجع السابق، ص45.

المعلوماتية، وأن الحماية الفنية وإن كانت هامة ولازمة فهي غير كافية للحد من الجرائم الماسة بنظم المعالجة الآلية للمعطيات فيلزم أن تكفلها حماية جزائية.

والمناقشات البرلمانية في فرنسا تؤكد أنها كانت ضد اشتراط الحماية الفنية بعد رفض وضع تعريف النظام المعالجة الآلية للمعطيات والذي اقترحه مجلس الشيوخ الفرنسي مشيرا فيه إلى أن النظام لابد أن يكون محميا بجهاز للأمان وأن الأنظمة المحمية تقنيا هي وحدها التي تحضى بالحماية الجنائية.

الفرع الثاني: المقصود بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1]

إنه وقبل صدور القانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كانت الجريمة المعلوماتية في النظام العقابي الجزائري تقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وهي وفقا لدلالة الكلمة تنصرف إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكة المعلومات وهذه الأفعال في الحقيقة ما هي إلا جزء من الظاهرة الإجرامية.

هذا فقد تبنى المشرع الجزائري حديثا بموجب القانون04/09 تعريفا موسعا للجرائم المعلوماتية واعتبر أنما تشمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر 07 أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية وبذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء بل توسع نطاقها لتشمل إضافة إلى ذلك تلك الأفعال التي تكون المنظومة المعلوماتية وسيلة الارتكاب.

(1) – سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، المرجع السابق، ص 42-43.

ويذهب بعض الفقه الجنائي إلى القول بأن هذه الطائفة الأخيرة تشكل أهم الجرائم التي تتصل بالمعلوماتية وأكثرها إثارة للمشكلات القانونية، فهي تتكون بصفة عامة من بعض الجرائم التقليدية التي يتم ارتكابها بواسطة المعلوماتية فتكتسب داخل هذا الإطار خصائص جديدة لارتباطها بالحاسب الآلي والنظم المعلوماتية تتميز عن الصورة التقليدية لها وتؤدي بالتالي إلى صعوبة تطبيق النصوص التقليدية عليها وهي في ثوبها الجديد، ومن هذه الجرائم على سبيل المثال يمكن أن نتصور ارتكاب جرائم إرهابية، جرائم التزوير أو جرائم أخلاقية ... بواسطة منظومة معلوماتية.

لذلك فالسؤال المطروح في هذا الصدد هو مدى قابلية وكفاية التشريعات العقابية القائمة والمنظمة للجرائم التقليدية للانطباق على هذه الأنماط الجديدة من الجرائم.

إن الدراسة التحليلية لمختلف الاتجاهات الفقهية والقضائية أظهرت قصور نصوص التجريم التقليدية السائدة وعجزها عن الإحاطة بهذه الجرائم ومرد ذلك إلى حقيقتين قانونيتين أساسيتين:

الأولى تتعلق بمبادئ الشرعية الذي يمنع المساءلة الجزائية ما لم يتوفر النص القانوني، فلا جريمة ولا عقوبة إلا بنص ومن انت فى النص على تحريم مثل هذه الأفعال التي لا تطالها النصوص القائمة امتنعت المسؤولية وتحقق القصور في مكافحة هكذا جرائم.

والثانية تتعلق بمسألة القياس في النصوص الجزائية الموضوعية أين يكون محظورا وغير جائز ويكاد ينحصر في الحقل الجزائي على النصوص الإجرائية كلما كانت أصلح للمتهم ومؤدى ذلك امتناع قياس أنماط الجرائم المرتكبة بواسطة منظومة معلوماتية أو عن طريق وسيلة اتصال إلكترونية على أنماط هذه الجرائم في صورتها التقليدية.

لذلك قام المشرع الجزائري بنص المادة 02 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال غير كاف وحده لتجريم الأفعال التي ترتكب بواسطة

المنظومة المعلوماتية أو يسهل ارتكابها عن طريق هذه المنظومة طالما أنه لا توجد نصوص قانونية موضوعية تحرم كل فعل بعينه وتحدد أركانه والعقوبة المقررة له، وهو الأمر الذي يخالف مبدأ شرعية التجريم والعقاب، فعبارة "أي جريمة أخرى" التي استعملها المشرع في المادة الثانية من القانون 04/09 نعتقد أنه لا يمكن القياس عليها لمتابعة أي شخص جزائيا حتى ولو ارتكب جريمة تقليدية بواسطة منظومة معلوماتية في ظل غياب النص الجزائي الذي يجرم هذا الفعل إذا ارتكب بواسطة منظومة معلوماتية صراحة.

لذلك ندعو المشرع الجزائري لتعديل النصوص القائمة لتستوعب الصور المتطورة للجرائم التقليدية والتي يمكن حسب طبيعتها أن ترتكب بواسطة منظومة معلوماتية.

المطلب الثاني: جرائم الاعتداء الماسة بالأنظمة المعلوماتية

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

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

(1) – قانون رقم 04-15 مؤرخ في 10 نوفمبر2004، يتضمن قانون العقوبات، جريدة رسمية عدد 71، لسنة 2004، معدل ومتمم. وذلك من خلال المواد من 394 مكرر إلى 394 مكرر 07، المضافة بموجب القانون نفسه.

وتتميز الجريمة المعلوماتية عن الجريمة التقليدية من حيث تعريفها، وخصائصها، وأركانها، وكذا القانون وجب تطبيقه عليها.

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

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

الفرع الأول: الصور البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات

تتمثل الصورة البسيطة للاعتداء على نظام المعالجة الالية للمعطيات في شكل الدخول (أولا) أو البقاء (ثانيا) غير المرخص بهما.

أولا: الدخول غير المرخص به

تنص المادة 394 مكرر من قانون العقوبات الجزائري أنه: «**يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 500000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك**».

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

كما يفهم من البند نفسه أن المشرع لا يعاقب على الفعل الكامل، أي على الجريمة التامة، وإنما يوقع العقاب حتى على مجرد المحاولة أي الشروع في الجريمة بغض النظر عن تحقيق النتيجة الإجرامية، وهو ما أدى بالبعض إلى الإقرار أن هذه الجرائم من قبيل الجرائم الشكلية، التي لا تشترط لقيامها تحقق النتيجة

الإجرامية، والشرط الوحيد في البند هو أن يكون الدخول إلى نظام المعالجة الآلية للمعطيات عن طريق الغش، أي لن يكون مشروعا، كالدخول من دون وجه حق أو من دون ترخيص مسبق، بمعنى ألا يكون الدخول صدفة أو خطأ.

وتجدر الإشارة هنا، إلى أن المشرع الجزائري لم يشترط في البند أعلاه، طبيعة خاصة لهذا النظام، أي أن المادة 394 مكرر لم تشترط لتحقق جريمة الدخول غير المرخص به إلى نظام المعالجة أن يكون هذا النظام محاطا بحماية فنية تمنع الاختراق، بل جاءت عامة ومطلقة وتحمي كل الأنظمة المعلوماتية، وبدون أي استثناء.

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

ثانيا: البقاء غير المرخص به

يقصد بالبقاء غير المرخص به هنا، الدخول إلى النظام والاستمرار في التواجد داخله وذلك دون إذن صاحبه، رغم علمه بأن بقاءه فيه غير مرخص[1].

ولقد سوى المشرع الجزائري بموجب المادة 394 مكرر من قانون العقوبات السابق بين كل من جريمة الدخول غير المرخص به والبقاء غير المرخص به، وذلك على غرار ما اتخذه المشرع الفرنسي في منظومته

(1) – آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر 2007، ص102

الجزائية، وهو ما تأكد بتطبيق الجزاء نفسه على السلوكين وهي عقوبة الحبس من ثلاثة (03) أشهر إلى سنة، وغرامة مالية من 50000 دج إلى 100000 دج ويعتبر فعل البقاء مثله مثل فعل الدخول، بمثابة الركن المادي للجريمة، ونضيف هنا ونؤكد أن البقاء قد يحتمل صورتين مختلفتين هما:

– تتمثل الصورة الأولى، في حالة تحقق فعل البقاء غير المرخص به داخل نظام المعالجة الآلية للمعطيات منفصلا عن فعل الدخول ويكون الدخول إلى نظام المعالجة مشروعا، حتى وإن كان خطأ أو صدفة، غير انه وبتفطن الفاعل للوضع وبدلا من الانسحاب أو مغادرة النظام فورا، فإنه يستمر في استغلال النظام، فهنا يعاقب على جريمة البقاء غير المرخص به.

– بينما تكمن الصورة الثانية، في حالة تحقق فعل البقاء غير المرخص به متصلا ومجتمعا مع فعل الدخول وهي حالة أكثر تشديدا من سابقتها كون فعل الدخول وفعل البقاء مجتمعين وينشأن بصفة غير مشروعة، كأن يتم الدخول دون ترخيص أو إذن سابق، ثم يستمر في البقاء داخله.

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

ومن أجل الإجابة عن الإشكال، فلقد تضاربت آراء فقهية عن المسألة، إذ هناك من يرى بأن الجريمة المتعلقة بالبقاء داخل النظام تبدأ من اللحظة التي يتم فيها الدخول الفعلي للمجرم إلى النظام، وذلك بتجوله وتنقله داخل هذا الأخير، وهنا تكون جريمة الدخول مكتملة، وهناك من يرى بأن جريمة البقاء تكون في الوقت الذي يعلم فيه المتدخل بأن بقاءه في النظام غير مشروع، ولم ينسحب من النظام[1].

(1) – أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2004، ص28

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

الفرع الثاني: الصور المشددة للاعتداء على نظام المعالجة الآلية للمعطيات

يشدد المشرع الجزائري من عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية، وذلك بموجب الفقرة الثانية من المادة 394 مكرر من قانون العقوبات، التي تنص أنه: «... تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة بعقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50000 دج الى 150000 دج».

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

– حالة الدخول أو البقاء مع محو أو تعديل في البيانات التي يحتويها النظام.

– ويتحقق الثاني عندما يترتب عن الدخول أو البقاء تخريب نظام اشتغال المنظومة وإعاقته عن أداء وظيفته.

وتجدر الإشارة هنا، إلى أن الصورة البسيطة للاعتداء على النظام المحددة في المادة 394 مكرر 01 السابقة لم تشترط البحث في النتيجة الإجرامية، بينما وباستقرار الفقرة 02 من المادة 394 مكرر يفهم أن النتيجة الإجرامية واجبة الإثبات، فيجب إثبات المحو أو التعديل أو التخريب للإقرار بالصورة المشددة للجريمة[1]، وإلا كنا بصدد الصورة الأولى والبسيطة لا أكثر.

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

(1) – خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، 2010، ص123.

خلاصة الفصل:

ما سبق فإن الجريمة المعلوماتية جريمة مستحدثة تستهدف للإعتداء على المعطيات بدلالتها التقنية الواسعة أو الاستعانة بها لإرتكاب جرائم تحاكي الجرائم التقليدية في العالم الافتراضي، وفي هذا الفصل تم تناول تعريف الجريمة المعلوماتية وذلك حسب الإتجاهات القانونية، ثم بعد ذلك تم تحديد الطبيعة القانونية لها ثم تبيان خصائصها، بالإضافة إلى الهدف من ارتكابها، ثم تم التعريج بعد ذلك إلى استيضاح موقف التشريع الجزائري من الجريمة المعلوماتية من خلال النصوص القانونية الموضوعة لمواجهة هذه الجريمة، والصور التي جاءت هذه النصوص القانونية ، وفي الأخير إبراز أهم صور هذه الجريمة.

الفصل الثاني
آليات وإجراءات التحري
في مجال الجريمة

تمهيد:

الجريمة المعلوماتية يرتكبها جناة ذوي صفات معينة أهمها الدراية الفنية بعمل الحاسب الآلي، وكلها تقدم الجاني في فهم تكتيك العمل في الحسابات الآلية، وكيفية تصميم البرامج كلما استطاع أن يرتكب جريمته دون أن يتم الاهتداء إليه، لأنه لا يترك أي آثار يمكن أن يستدل عليه من خلالها، هذا ما يصعب على المحققين الكشف عن هاته الجرائم وإلقاء القبض على مرتكبيها وللتعرف أكثر على الاليات والإجراءات التي تتخذ للكشف عن هذه الجريمة، تم التطرق الوحدات المختصة التي تتولي اجراءات البحث و التحقيق في الجرائم المعلوماتية على المستوى الوطني في المبحث الاول، وإجراءات القانونية التحري للكشف عن الجريمة المعلوماتية في المبحث الثاني.

المبحث الأول: الوحدات المختصة التي تتولي اجراءات البحث والتحقيق في الجريمة المعلوماتية

سنحاول من خلال هذا المبحث استعراض أبرز الهيئات والوحدات المتخصصة في مجال مكافحة الجرائم المعلوماتية، والتي ما تسند إليها عادة مهام الوقاية ومكافحة الجرائم المعلوماتية، نظرا لتشكيلتها البشرية الخاصة والتي تضم محققين من نوع خاص تجتمع لديهم صفة ضابط شرطة قضائية إضافة إلى المعرفة الواسعة بمجال النظم المعلوماتية والإجرام المعلوماتي، مما يسمح لهم ويؤهلهم لتولي مهام البحث والتحقيق في ميدان الجرائم المعلوماتية، سواء تمثلت في شخص وكيل الجمهورية او قاضي التحقيق نظرا لقلة خبرتهم بميدان النظم المعلوماتية وعلم تحكمهم في تقنيات البحث والتحقيق بواسطة وسائل معلوماتية خاصة تتطلب المعرفة والدقة في مجال إستخدامها، ولعل أن أبرز هذه الهيئات والوحدات هي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال (المطلب الأول)، إضافة إلى تلك الاجهزة الامنية (المطلب الثاني) سواء التابعة لسلك الأمن الوطني او التابعة لقيادة الدرك الوطني.

المطلب الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

تعود فكرة إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال إلى سنة 2009 وبالضبط منذ تاريخ 05 أوت 2009 تاريخ صدور القانون 09-04 المتعلق بتحديد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، بحيث جاء في نص المادة 13 من القانون على أنه تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، تحدد تشكيلة الهيئة وتنظيمها وكيفية سيرها عن طريق التنظيم.

وقد إستلزم الأمر لصدور التنظيم الذي طرحته نص المادة 13 السالفة الذكر الإنتظار لمدة 06 سنوات كاملة، أين صدر المرسوم الرئاسي رقم 15-268 بتاريخ 08 أكتوبر 2015 ضمن العدد الثالث

والخمسين 53 للجريدة الرسمية، والذي تضمن في فصوله تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[1].

الفرع الأول: التعريف بالهيئة وإختصاصاتها

أولا : التعريف بالهيئة

تعتبر " الهيئة " كما يصطلح عليها في صلب نصوص المرسوم الرئاسي حسب أحكام المواد من 01 إلى 04 منه بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والإستقلال المالي توضع لدى الوزير المكلف بالعدل، ويقع مقرها بالجزائر العاصمة، تتولى الهيئة المهام المنصوص عليها في المادة 14 من القانون 09-04 وذلك تحت رقابة السلطة القضائية وطبقا لأحكام قانون الإجراءات الجزائية[2].

ثانيا : إختصاصات الهيئة

بينت الفقرة الثانية 02 من المادة 04 من المرسوم الرئاسي 15-261 المهام الأساسية التي تكلف بها الهيئة وهي وعلى سبيل الحصر مهام الهدف منها هو الوقاية من الجرائم المعلوماتية ومكافحتها من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون المصالح الشرطة القضائية وأبرز مهام هذه الهيئة هي :

1- اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

---

(1)- حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدّمة لنيل شهادة دكتوراه العلوم في الحقوق تخصّص- قانون العقوبات و العلوم الجنائية، جامعة باتنة1، السنة الجامعية 2016/2015

(2)-تنص المادة 14 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال على انه "تتولى الهيئة المذكورة في المادة 13 خصوصا المهام التالية :

أ- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته.

ب- مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، بما في ذلك تجميع المعلومات و انجاز الخبرات القضائية.

ج- تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال وتحديد مكان تواجدهم

2- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها .

3- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية.

4- ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالاعمال الارهابية والتخريبية والماسة بأمن الدولة وذلك تحت قاضي مختص وذلك كاختصاص حصري.

5- تجمع وتسجيل وحفظ المعطيات الرقمية وتحديد مسارها من أجل استعمالها في الاجراءات القضائية.

6- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات المعلومات.

7- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المعلوماتية.

8- تنفيذ الطلبات الصادرة عن الدول الأجنبية وتطوير سبل التبادل معها.

9- المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

الفرع الثاني: تشكيلة الهيئة وطبيعة عملها

أولا: تشكيلية الهيئة الادارية

تتشكل الهيئة من لجنة التي تدير إضافة الى مديرية عامة، تتشكل اللجنة التي تدير من الوزير المكلف بالعدل رئيسا اضافة الى الوزير المكلف بالداخلية والوزير المكلف بالتكنولوجيات الاعلام والاتصال وقائد الدرك الوطني وكذلك مدير العام للأمن الوطني، وممثلين أحدهما عن رئاسة الجمهورية وآخر عن وزارة الدفاع يكملها قاضيان من المحكمة العليا، أما المديرية العامة فيرأسها مدير عام معين بموجب مرسوم رئاسي، وتتجلى مهام هذه المديريات في ضبط برامج عمل الهيئة ودراسة مشروع الميزانية وتقديم تقارير

خاصة بنشاط الهيئة، والتالي فهي لا تساهم في الاجراءات الخاصة بالوقاية أو بمكافحة الجرائم المعلوماتية[1].

ثانيا : تشكيلية الهيئة التقنية

إضافة إلى اللجان الإدارية تضم الهيئة مديريات تتقسم من حيث مهامها وتشكيلتها بالطابع التقني، بإعتبارها المختصة بإنجاز المهام التقنية المتعلقة بالوقاية وبمكافحة الجرائم المعلوماتية وهذه المديريات هي:

1 – مديرية المراقبة الوقائية واليقظة الإلكترونية : لم يشر الأمر الرئاسي 15-261 إلى تشكيلة هذه المديرية، غير أنه ومن خلال تحليل نص المادة 18 منه يمكن لنا تحديد تشكيلتها في مجموعة من ضباط وأعوان الشرطة القضائية المختصين في مجال مكافحة الجرائم المعلوماتية، من سلك الأمن الوطني وكذلك الدرك الوطني والمصالح العسكرية للإستعلام والأمن، يعينون بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل والدفاع والداخلية، يساعدهم مستخدمي الدعم التقني والإداري من نفس الأسلاك .

تعمل هذه المديرية على إنجاز المهام التالية:

1- تنفيذ عمليات المراقبة الوقائية للإتصالات الإلكترونية والقيام بإجراءات التفتيش والحجز داخل الأنظمة المعلوماتية إذا ما تعلق الأمر جرائم الإرهاب أو التخريب والجرائم الماسة بأمن الدولة بناء على رخصة مكتوبة من السلطة القضائية وتحت رقابة القاضي المختص.

2-إرسال المعلومات المحصل عليها إلى السلطات القضائية ومصالح الشرطة القضائية.

3- تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات التي تسمح بتحديد مكان تواجد مرتكبي الجرائم المعلوماتية والتعرف عليهم.

(1)- المواد 06 الى 10 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

4- جمع كل المعلومات وإستغلالها من أجل الكشف عن الجرائم المعلوماتية.

5- المشاركة في حملات التوعية حول مخاطر تكنولوجيا الإعلام والإتصال.

6- تزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المعلوماتية.

إذن وبالنظر إلى تشكيلة والمهام الملحقة بهذه المديرية فإنه يمكن وصفها بأنها المركز العملياتي للهيئة بما أنها تتولى الجانب التقني الخاص بإنجاز الأعمال المتعلقة بالبحث والتحقيق في الجرائم المعلوماتية، ولعل أن ما يزيد من دورها الفعال هو تنصيبها على رأس مركز العمليات التقنية وكذلك الملحقات مما يبرز دورها الفعال في تسيير وتأطير الأعمال المتعلقة بالوقاية أو بمكافحة الجرائم المعلوماتية[1].

2- مديرية التنسيق التقني: لم ينص المرسوم الرئاسي 15-261 على تشكيلة مديرية التنسيق التقني مما يترك المجال للقول بأنها تشكيلتها تكون بناء على قرارات مشتركة بين وزراء العدل والدفاع والداخلية على شاكلة مديرية المراقبة الوقائية واليقظة الإلكترونية، غير أنها تختلف عنها من حيث المهام الموكلة إليها، فتتمثل مهامها أكثر في الدور الوقائي والإعلامي من خلال توليها :

1- إنجاز الخبرات القضائية في مجال إختصاص الهيئة.

2- تكوين قاعدة معطيات تحليلية للإجرام المعلوماتي .

3- إعداد الإحصائيات الوطنية للإجرام المعلوماتي.

(1)- المواد 11-13-14- 18-21 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

4- تسيير المنظومة المعلوماتية و إدارتها[1].

إذن فمن خلال إستعراض الهيكل العام للهيئة ومجمل إختصاصاتها، يتضح لنا جليا مدى إقتناع الهيئة التشريعية بضرورة تفعيل دور الهيئة في مجال الوقاية ومكافحة الجرائم المعلوماتية ولو بشكل متأخر، نظرا لتوسع تطبيقات تقنية المعلوماتية في المجتمع الجزائري على الصعيدين الحكومي والإجتماعي، وهو ما ينبئ بتنامي الإجرام المعلوماتي وإزدياد حجم التهديدات التي يشكلها على سلامة الأنظمة المعلوماتية وأمن المعطيات المخزنة والمتداولة عبرها.

المطلب الثاني: الأجهزة الأمنية

تضم الأجهزة الأمنية كل من جهاز الأمن الوطني والذي سنتطرق له في الفرع الأول، وجهاز الدرك الوطني في الفرع الثاني.

الفرع الأول: الوحدات التابعة لسلك الأمن الوطني

تضع مديرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديها لأجل التصدي لكل أنواع الجرائم وبالخصوص تلك المستحدثة منها كالجرائم المعلوماتية، والتي تعتبر نتاج التطور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والإتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة بإستعمال هذا النوع من التكنولوجيات.

(1)- المادة 12 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة و تنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

أولا: على مستوى المركزي

بادرت المديرية العامة للأمن الوطني إلى تحديث بنيتها الهيكلية بغية خلق وحدات متخصصة تعمل كل منها على مكافحة نوع معين من الجرائم دون سواها، ولذلك قامت المديرية العامة للشرطة القضائية بإستحداث مصلحة مختصة في لمكافحة الجريمة المعلوماتية سميت بنيابة مديرية مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، بالإضافة الى نيابة مديرية الشرطة العلمية والتقنية، هذه الأخيرة التي تضع لخدمة هذا الهدف مصالح عملية مختصة بذلك، تتولى أعمال البحث والتحري والتحقيق بشأن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وهذه الوحدة هي المخبر المركزي للشرطة العلمية و الكائن مقره بالجزائر العاصمة.

يتولى كل المخبر المركزي، مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها، ولأجل ذلك يضم المخبر دائرة تقنية وتتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها الأسلحة والقذائف بمختلف أنواعها، وكذلك جرائم التزوير، إضافة إلى الجرائم المعلوماتية، وتباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الأخرى[1].

ثانيا:على المستوى الجهوي

قامت بانشاء مخابر جهوية للشرطة العلمية في كل من ولايتي قسنطينة ووهران، بالإضافة إلى ثلاث 03 مخابر أخرى قيد الإنجاز على مستوى – ورقلة – بشار – تمنراست ينتظر تسليمها قريبا لأجل تعميم هذا النوع من النشاط على كافة ربوع الوطن.

(1)– مساهمة المخبر الجهوي للشرطة العلمية في كل من قسنطينة ووهران في إدارة الدليل ضمن التقنيات الخاصة للتحقيق – وثيقة خاصة صادرة عن نيابة مديرية الشرطة العلمية و التقنية – مديرية الشرطة القضائية– المديرية العامة للأمن الوطني – ص 02–03.

على مستوى كل مخبر مصلحة تسمى دائرة الأدلة الرقمية والآثار التكنولوجية التابعة لمخبر الأدلة الجنائية ، تتولي هذه المصلحة أعمال البحث والتحقيق القائمة بشأن الجرائم المعلوماتية، وذلك تحت تسمية دائرة الأدلة الرقمية والأثار التكنولوجية" والتي لم تكن عند إستحداثها سنة 2004 سوى قسم، غير أن الإرتفاع الملحوظ لعدد القضايا الناتجة عن الجرائم المعلوماتية، بسبب الإنتشار المتزايد لتقنية المعلوماتية عجل بترقيتها إلى دائرة تضم ثلاث 03 أقسام فرعية هي:

1- قسم إستغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.

2- قسم إستغلال الأدلة الناتجة عن الهواتف النقالة.

3- قسم تحليل الأصوات

تضم الدائرة في صفوفها ثمانية 08 أعضاء محققين أربع 04 منهم عناصر شرطيون رسميون يتمتعون بصفة ضابط شرطة قضائية، والبقية هم أعوان شبيهون، يحمل كل منهم شهادة جامعية في تخصص الإعلام الآلي، إضافة إلى إلمامهم بالجانب القانوني، ومما يزيد من فعاليتهم في مجال مباشرتهم لمختلف إجراءات البحث والتحقيق في الجرائم المعلوماتية هو خضوعهم بصفة دورية لدورات تكوينية لأجل الإطلاع على كل المستجدات القانونية منها والتقنية في مجال الإجرام المعلومات[1].

ومن مهام هذه المخابر ضمان الدعم التقني لمختلف مصالح الشرطة والأجهزة القضائية في مجال التحريات الالكترونية، وذلك من خلال القيام بعمليات البحث عن المعطيات المشبوهة والمعلومات الرقمية على مختلف أشكالها: ملفات، رسائل الكترونية، برامج، صور،... هذا البحث يتم عن طريق استعمال برامج ووسائل خاصة تمكن من استرجاع كل المعطيات المحذوفة، والإطلاع على محتوى كل الوسائط الرقمية[2].

(1)-حسين سعيداني، اليات التحقيق في الجرائم المعلوماتية، مرجع سابق، ص180.

(2)- مساهمة الشرطة العلمية والتقنية في مجال التحقيقات الجنائية- وثيقة خاصة صادرة عن مديرية الشرطة القضائية- المديرية العامة للأمن الوطني - ص46.

تلعب الدائرة دورا مهما للغاية في الكشف عن أسرار الجرائم المعلوماتية، من خلال مختلف الإجراءات التي تباشرها إما أثناء مرحلة البحث والإستدلال، أو أثناء مرحلة التحقيق القضائي.

فأما أثناء مرحلة البحث والتحري فإن أعضاء الدائرة عادة ما يستجيبون للطلبات التي يقدمها لهم عناصر الشرطة التابعون لفرق مكـافحة الجرائم المعلوماتية الموزعة على كـل مديريات الأمن الوطني، أو الطلبات وكيل الجمهورية أو قاضي التحقيق التي تردهم في شكل إنابة قضائية، من أجل دعمهم ومساعدتهم أثناء مرحلة المعاينة لمسرح الجريمة وكذلك لحجز الأدلة المتواجدة عليها.

أما أثناء مرحلة التحقيق القضائي فإن دور الدائرة لا يتعدى لأن يكون دور خبير، وذلك من خلال إعداد تقارير خبرة بناء على طلبات وكيل الجمهورية وبالخصوص قاضي التحقيق، كنتيجة لقيام المحققين بأعمال تحليل الأدلة المحجوزة والعمل على إستخراج الأدلة الإلكترونية منها، كتحليل محتوى الأقراص الصلبة للحواسيب المستعملة في الجريمة، أو حواسيب الضحايا، وكذلك كل دعامات التخزين الإلكترونية بمختلف أنواعها وأشكالها، وكذلك المواقع التي تم إختراقها وإستهدافها وصولا إلى تحديد المواقع الجغرافي وعناوين المجرمين، وذلك بالإستعانة بوسائل مادية خاصة متطورة ذات جودة عالية[1].

وفي الأخير فإن ما يمكن قوله بهذا الخصوص أن المديرية العامة للأمن الوطني تولي أهمية بالغة في مجال مكافحة الإجرام المعلوماتي.

ثالثا: على المستوى المحلي

في سبيل تدعيم المصالح الولائية للشرطة القضائية في مجال مكافحة الجرائم المعلوماتية، خلقت المديرية العامة للأمن الوطني سنة 2016 ما يقارب 48 فرقة لمكافحة الجرائم المعلوماتية على مستوى

(1)–حسين سعيداني، اليات التحقيق في الجرائم المعلوماتية، مرجع سابق، ص181.

مصالحها بأمن والولايات ، يتمثل دورها في تلقي الشكوى والبحث والحقيق في الجرائم المعلوماتية وتقريب الإدارة من المواطن.

الفرع الثاني: الوحدات التابعة للدرك الوطني

تضع قيادة الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية وهي تباعا:

1. قيادة الدرك الوطنية.
2. الوحدات الإقليمية.
3. الوحدات المشكلة.
4. الوحدات المتخصصة وحدات الإسناد.
5. هياكل التكوين.
6. المعهد الوطني للأدلة الجنائية وعلم الإجرام.
7. المصالح والمراكز العلمية والتقنية.
8. المصلحة المركزية للتحريات الجنائية .
9. المفرزة الخاصة للتدخل[1].

تعمل مؤسسة الدرك الوطني جادة إلى التطلع بمختلف الجرائم المرتكبة على شبكة الإنترنت وهذا لتسهيل مهمة البحث والمعاينة والتفتيش في أنظمة الحواسيب والعمل على مراقبة مختلف الشبكات وبالتالي

(1)- الموقع الرسمي لقيادة الدرك الوطني – تاريخ التصفح 31 مارس 2019 – الرابط الإلكتروني:
http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined

فقد تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني في خدمة هذه الأهداف، وذلك حسب الإختصاص والصلاحيات وطبيعة الجريمة إلى ثلاث 03 مستويات مركزية، جهوية، محلية.

أولا: على المستوى المركزي:

تعمل مصالح الدرك الوطني من خلال أجهزتها المركزية على مكافحة الجرائم المعلوماتية ودعم أعمال البحث والتحقيق بشأنها من خلال الهيئات التالية:

1 – مديرية الأمن العمومي والإستغلال: وهي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي، في مجال أعمال البحث والتحري في الجرائم المعلوماتية.

2 – المصلحة المركزية للتحريات الجنائية: وهي هيئة ذات إختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الإعلام والإتصال[1].

3 – المعهد الوطني للأدلة الجنائية وعلم الإجرام: يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاءه بمرسوم رئاسي رقم 183–04 بتاريخ: 26 جوان 2004، في إطار عصرنة قطاع الدرك الوطني، وهو يشكل كذلك أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة، يعد المعهد بمثابة هيئة مختصة في إجراء الخبرات والمعاينة وذلك بمختلف دوائره، بما فيها دائرة الإعلام الآلي والإلكترونيك، التي أوكلت لها مهام تحليل الأدلة الخاصة بالجرائم المعلوماتية، وإن الخدمة الأساسية التي يقدمها هذا المعهد في هذا الشأن:

– القيام بالخبرات العملية أو الخبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة بما فيها تلك المتعلقة بالجرائم المعلوماتية.

– مساعدة المحققين للسير الحسن للمعاينات، عن طريق دعمهم الأفراد المؤهلين أثناء الحاجة.

(1)– معلومات مقدمة من قبل الفرقة الإقليمية للدرك الوطني – البيض – الجزائر.

– تنفيذ مناهج الشرطة العلمية والتقنية لجمع وتحليل الأدلة المأخوذة من مسرح الجريمة.

– ضمان المساعدة العلمية في التحريات المعقدة كحال التحريات الخاصة بالجرائم المعلوماتية.

– المشاركة في الأبحاث والتحاليل المتعلقة بالوقاية للتقليل من جميع أشكال الإجرام بما فيها المعلوماتي.

تعتبر مشاركة ومساهمة المعهد الوطني للأدلة الجنائية وعلم الإجرام بصفته الهيئة المكلفة بالتحاليل والخبرات في ميدان علم الإجرام في وضع سياسة مكافحة الإجرام[1].

4– مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية: أنشأ هذا المركز حديثا ويعتبر بمثابة نقطة وصل وطنية في مجال دعم أعمال البحث والتحقيق في الجرائم المعلوماتية[2]، إذ يوفر المساعدة التقنية للمحققين ويساهم في توجيه التحقيقات المرتبطة بتكنولوجيا الإعلام والإتصال، فهو هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي والإستغلال لقيادة الدرك الوطني ويحقق المهام التالية:

1. ضمان المراقبة الدائمة والمستمرة على شبكة الإنترنت.

2.القيام بمراقبة الإتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.

3. مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والإتصال والبحث عن الأدلة في شبكة الأنترنت.

4. المشاركة في عمليات التحري والتسرب عبر شبكة الأنترنت الفائدة وحدات الدرك الوطني والسلطات القضائية.

---

(1)– الموقع الرسمي لقيادة الدرك الوطني – تاريخ التصفح 31 مارس 2019 – الرابط الإلكتروني :

http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined

(2)– بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة 16 و17 نوفمبر 2015، كلية الحقوق جامعة بسكرة ص29.

5. المشاركة في قمع الجرائم المعلوماتية، من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.

إذن تعتبر هذه الهيئات التابعة للدرك الوطني مسؤولة عن تنفيذ إجراءات البحث والتحقيق بشأن الجرائم المعلوماتية، وذلك على نطاق وطني بحيث تعتبر هيئات دعم وإسناد ونقاط وصل بين مختلف الوحدات الأخرى المتخصصة والتي توجد كذلك على مستويات أدنى منها الجهوية والمحلية .

ثانيا: على المستوى الجهوي

تختص المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني بمهمة تنسيق النشاطات بين مختلف الوحدات التابعة للشرطة القضائية وكذلك دعمها بالوسائل الخاصة للتحريات والأبحاث المعقدة كالجرائم المعلوماتية.

يلعب الدرك الوطني دورا هاما في ميدان الشرطة القضائية نظرا لانتشار وحداته على مستوى كامل التراب الوطني، ونظرا للوسائل المادية الموضوعة تحت تصرفه وعدد أفراده الهائل، والصلاحيات التي خولها لهم القانون، وهم في الواقع حسب الرتب والوظائف ضباط وأعوان الشرطة القضائية.

ثالثا: على المستوى المحلي

يحوز الدرك الوطني على فصائل للأبحاث التي ينتمي إليها أفراد ذوو خبرة وإختصاص واسعين في ميدان الشرطة القضائية، هذه الفصائل مكلفة خصوصا بمكافحة الأشكال الخطيرة للإجرام المنظم كالجرائم المعلوماتية، وذلك عن طريق القيام بتحقيقات تتطلب تحريات معقدة، هذه الوحدات المختصة تساهم في تدعيم نشاط الأبحاث والتحريات التي تقوم بها الفرق الإقليمية للدرك الوطني، وهو ما سمح بإنشاء خلية متخصصة لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال في كل مجموعة ولائية، وهو ما يسمح

بتطبيق سياسة فعالة في مكافحة الجرائم المعلوماتية من خلال توفير الخلايا المتخصصة في مجال أعمال البحث والتحقيق في هذا النوع من الجرائم[1].

(1)- معلومات مقدمة من قبل الفرقة الإقليمية للدرك الوطني – البيض – الجزائر.

المبحث الثاني: إجراءات القانونية التحري للكشف عن الجريمة المعلوماتية

تنقسم الإجراءات القانونية من أجل الكشف عن الجريمة المعلوماتية الى إجراءات كلاسيكية وهذا ما سنتطرق إيه في المطلب الأول، وإجراءات حديثة للكشف عن الجريمة المعلوماتية في المطلب الثاني.

المطلب الأول: إجراءات التحري الكلاسيكية للكشف عن الجريمة المعلوماتية

تتمثل إجراءات التحري الكلاسيكية للكشف عن الجريمة المعلوماتية في جميع الإجراءات التي يمكن ايجادها في الجرائم التقليدية وهي المعاينة والتفتيش، وعليه سوف نبرز هذه إجراءات فيما يلي:

الفرع الأول: معاينة مسرح جرائم الماسة بأنظمة المعلوماتية

عند التكلم عن إجراءات التحري كلاسيكية للكشف عن الجريمة المعلوماتية، أول ما يجب دراسته هو معاينة مسرح الجريمة المعلوماتية ويقصد بهذه الأخيرة رؤية العين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة[1]، أو هي إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة وهي تتطلب أن ينتقل ضابط الشرطة القضائية إلى عين مكان ما لمباشرتها لإثبات حالته وحالة ما قد يوجد فيه من أشخاص أو أشياء تفيد في إظهار الحقيقة للكشف عن الجريمة محل الإجراء."

وهي إجراء جائز في كافة الجرائم، إلا أن غالبية التشريعات بما فيها التشريع الجزائري في المادة 61 من قانون الإجراءات الجزائية الجزائري، تقصرها على الجنايات والجنح الهامة، بحيث تعد إجراء وجوبيا في الجنايات وجوازيا في الجنح، وهي قد تتم في مكان عام أو مكان خاص، فإذا كانت في مكان عام؛ الضابط الشرطة القضائية لا يحتاج إلى إذن من النيابة العامة بإجرائها، أما إذا كانت بمكان خاص؛ فلابد لصحتها، من رضا صاحب المكان أو وجود إذن مسبق من سلطة التحقيق بإجرائها.

(1)- محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة الثامنة، دار الجامعة الجديدة، 2008، ص 123 وما بعدها.

ولمعاينة مسرح الجرائم المعلوماتية، يجب التفرقة بين حالتين:

أولا: معاينة الجرائم الواقعة على المكونات المادية للحاسوب(Hardware)

كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي المحسوس، فهي لا تثير أية مشكلة بحيث يمكن لضابط الشرطة القضائية معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.

ثانيا: معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها(Software)

كتلك الواقعة على برامج الحاسوب وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينة أو فائدته، وهذه الصعوبات، تتلخص فيما يلي:

- قلة الآثار المادية المترتبة عن الجرائم التي تقع على المكونات غير المادية للحاسوب.
- الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبا ما تكون طويلة، وذلك بين اقتراف الجريمة والكشف عنها، الأمر الذي يمنح فرصة لإحداث تغييرات أو العبث بالآثار المادية أو زوال بعضها، مما يؤدي إلى غموض الدليل المستقى من المعاينة.

ولنجاح المعاينة في الجرائم المعلوماتية يوصي الخبراء بوجوب إتباع ومراعاة قواعد وإرشادات فنية أبرزها ما يلي:

- القيام بتصوير الحاسوب وما قد يتصل به من أجهزة ظرفية ومحتوياته، وأوضاع المكان الذي يوجد به بصفة عامة مع التركيز على تصوير أجزائه الخلفية وملحقاته، ومراعاة تسجيل الزمان والتاريخ والمكان الذي التقطت فيه كل صورة.

- يجب ملاحظة واثبات الحالة التي تكون عليها توصيلات الكابلات (الخيوط الكهربائية للحاسوب)، والتي تكون متصلة بمكونات النظام، حتى يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة.
- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الاختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو للبيانات المسجلة.
- وضع مخطط تفصيلي للمنشأة الواقعة بها الجريمة مع كشف تفصيلي بالمسؤولين بها ودور كل واحد منهم.
- ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء.
- التحفظ على ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة، والأشرطة والأقراص الممغنطة غير السليمة أو المحطمة وفحصها، ورفع البصمات التي قد تكون لها صلة بمرتكبي الجريمة.
- القيام بحفظ المستندات الخاصة بالإدخال، وكذا مخرجات الحاسوب الورقية التي قد تكون ذات صلة بالجريمة، وذلك من أجل رفع البصمات التي قد تكون موجودة عليها[1].

(1)- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011-2012، ص 131.

الفرع الثاني: تفتيش الأنظمة المعالجة الالية للمعطيات وضبطها

إن الهدف من التفتيش هو ضبط الأدلة المادية للكشف عن الجريمة، فكل ما يضبطه الضابط الشرطة القضائية بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الأثر المباشر للتفتيش، فالضبط إذن يعد أيضا إجراء من إجراءات التحقيق في الجرائم المعلوماتية؛ بوضع اليد على الشيء وحبسه والمحافظة عليه، للحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة[1]، وهو ما سنبرزه فيما يلي:

أولا: تفتيش نظم المعلوماتية

عملية تفتيش تنصب على المكونات المادية بأوعيتها المختلفة، للبحث في أي شيء يتصل بجريمة معلوماتية ما للكشف عنها، يدخل في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات، هي:

الحالة الأولى :في حالة ما إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات.

الحالة الثانية :إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة، لذلك حتى تتم

(1)- يمثل الحاسوب الآلي المحل الرئيسي للتفتيش في نظم المعلوماتية، وينصب التفتيش على المكونات المادية: وهي مجموعة من الوحدات لكل منها وظيفة محددة وتتصل مع بعضها البعض بشكل يجعلها تعمل كنظام متكامل، وتسمى بمعدات الحاسوب وهي: وحدات الإدخال، وحدة الذاكرة الرئيسية، وحدة ذاكرة القراءة، وحدة الحاسوب والمنطق، الشاشة، وحدة التحكم، وحدة الذاكرة المساعدة، وحدة الإخراج، الطابعة، أنظر: طارق إبراهيم الدسوقي عطية، الامن المعلوماتي ، دار الشر الجديدة الاسكندرية، سنة 2009، ص 441.

عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن[1].

وقد حذا المشرع الجزائري حذو معظم التشريعات المعاصرة، بأن قرر المادة 65 مكرر 5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا اقتضت ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بإعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور.

الحالة الثالثة :إذا وجدت مكونات الحاسوب المادية **(**في حالة الحاسوبات الآلية المحمولة**)** في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة ...الخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات[2].

ثانيا :تفتيش نظم الحاسوب المنطقية أو المعنوية

يعرف الكيان المنطقي للحاسوب بأنه: "مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات[3]".

وقد حذا المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري حذو التشريعات السابقة بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه: "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."

(1)- طرشي نورة، المرجع السابق، ص 115.

(2)- طارق إبراهيم الدسوقي عطية، الامن المعلوماتي ، دار الشر الجديدة الاسكندرية، سنة 2009، ص 385.

(3)- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، 2007.

ثالثا :القواعد الشكلية لتفتيش نظم المعلوماتية

تتلخص هذه القواعد كما يلي:

أ- **إجراء التفتيش بحضور أشخاص معينين بالقانون:** من بين هذه الأشخاص: المتهم والقائم بالتفتيش وشاهدين طبقا للمادة 45 من قانون الإجراءات الجزائية الجزائري، تنص على أن: أن التفتيش يتم بحضور المتهم أو من يجوز أن يمثله وضابط الشرطة القضائية-القائم بالتفتيش-، وإذا تعذر حضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته، غير أنه كاستثناء على هذه القواعد نص المشرع الجزائري في الفقرة الأخيرة من المادة45 من قانون الإجراءات الجزائية الجزائري، على أنه: "لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات".

ب- **إعداد محضر خاص بالتفتيش:** ويكون بتكليف القائم بالتفتيش باصطحاب كاتب يحرر محضرا خاصا بالتفتيش والضبط، تسجل فيه جميع وقائع التحقيق بالتفصيل، وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل أمانة ودقة وحرص.

ت- **إجراءات تنفيذ تفتيش نظم الحاسوب الآلي وميعاده:** لهذه الإجراءات خصوصية تتميز بها، وذلك لدقة التعامل مع الأجهزة والبرامج الموجودة عليها، ولكي تتم على أكمل وجه، يجب تحديد نوع النظام المراد تفتيشه، وبالتالي يجب أن يكون القائم بالتفتيش على علم بقدر كبير بعلوم الإعلام الآلي حتى يتسنى له معرفة نظم الحاسوب المراد تفتيشها، والاستعانة بخبراء النظام للاستعانة بهم في عملية إجراء التفتيش،

ومعرفة إمكانية الحصول على كلمة السر والدخول للنظام المراد تفتيشه، ومعرفة مكان القيام بتحليل نظم الحاسوب الآلي[1].

بالإضافة إلى تحديد هوية أعضاء فريق التفتيش يجب على القائم بالتفتيش اتخاذ الخطوات التالية عند تنفيذ إذن التفتيش والتي تتلخص في ما يلي:

- تأمين حماية مسرح الجريمة، بضمان فصل القوة الكهربائية عن موقع المعاينة وأجهزة خادمة شبكة الانترنت، لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير على أثار الجريمة.
- إبعاد المتهم عن مكان النظام إن كان قريبا منه.
- أخذ الحيطة لمنع تمكن المتهم من الدخول عن بعد للنظام المعلوماتي.
- الدخول إلى الموقع ببطء، لكي لا يتم تشويه أو إتلاف الدليل.
- عدم لمس لوحة المفاتيح، لأن ذلك قد يستلزم استخدام برامج أخرى احتيالية أو صعبة.
- يجب العناية بالملاحظات وكلمات السر ورموز الشفرة إلى غيرها من العمليات والإجراءات الفنية التي تساعد على الكشف عن الجريمة المراد إثباتها[2].

وفي نطاق تفتيش نظم الحاسوب، نجد أن المشرع الجزائري لم تحدد مدة معينة لتنفيذ إجراء التفتيش، غير أن الرأي الغالب في مجال تفتيش النظم المعلوماتية هو عدم تقييد المحقق بمدة زمنية معينة، بل يجب تركها للسلطة التقديرية له، لأن الوقت الذي تكثر فيه الجرائم المعلوماتية هو ليلا، لسهولة الاتصال ومجانيته في ذلك الوقت في بعض الحالات، وأيضا لسهولة الدخول إلى المواقع المستهدفة بالفعل الإجرامي لقلة

(1)- طرشي نورة، المرجع السابق، 125.

(2)- عفيفي كامل عفيفي، المرجع السابق، ص 65.

المستخدمين في هذا الوقت، كما نص عليها في الفقرة الثالثة من المادة 47 من قانون الإجراءات الجزائية الجزائري[1] .

المطلب الثاني :إجراءات التحري المستحدثة للكشف عن الجرائم المعلوماتية

في إطار تعديل من قانون الإجراءات الجزائية الجزائري بالقانون 22/06 المؤرخ في 2006/12/20 الذي جاء فيه إجراءات مستحدثة للكشف عن للجرائم الماسة بأنظمة المعالجة للمعطيات وهي :

الفرع الأول: الكشف بواسطة أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

مكن المشرع الجزائري ضابط الشرطة القضائية من صلاحية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور للكشف عن الجرائم المعلوماتية، وهي إجراءات تباشر بشكل خفي، على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة[2].

والتقاط الصور يكون بالتقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص، ويتم استخدام هذه الوسائل في المحلات السكنية والأماكن العامة والخاصة.

أما تسجيل الأصوات، فيتم عن طريق وضع رقابة على الهواتف وتسجيل الأحاديث التي تتم عن طريقها، كما يتم أيضا عن طريق وضع ميكروفونات حساسة تستطيع إلتقاط الأصوات وتسجيلها على أجهزة خاصة، وقد يتم أيضا عن طريق التقاط إشارات لاسلكية أو إذاعية[3].

(1)- طرشي نورة، المرجع السابق، ص 126.

(2)- خلفي عبد الرحمن، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة، الجزائر، 2010، ص 72- 73.

(3)- حسن صادق المرصفاوي، المرصفاوي في التحقيق الجنائي، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر، 1990، ص78.

إن ما يهم هو أن مثل هذا الإجراءات يمكن له المساس بالحرية الشخصية، خصوصا إذا علمنا أن سرية المراسلات هي حق دستوري، فقد جاء في المادة 03 من القانون رقم 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، أنه: "مع مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية[2].

بالإضافة إلى أن كل متهم بريء حتى تثبت إدانته[3]، لذلك هل يجوز إثبات أو نفي الاتهام عن المشتبه فيه، باللجوء إلى وسيلة التسجيل الصوتي أو اعتراض المراسلات أو التقاط الصور في الأماكن العامة والخاصة، وخصوصا أن مثل هذه الإجراءات أو الوسائل قد لا تمس بشخص المتهم فقط، وإنما كذلك بمن يحيطون به من أقاربه أو معارفه؟.

يفرق الفقه بين مصطلح اعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة، فبينما يكون الأول دون رضا المعني، يكون الثاني برضا أو بطلب من صاحب الشأن، ويخضع لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك.

(1)- يقصد بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال في إطار المادة 2 /أ من القانون رقم 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

(2)- يقصد بالمعطيات المعلوماتية في إطار المادة 2 / ج من القانون رقم 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، 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.

(3)- تنص المادة (45) من دستور عام 1996 على أنه: "كل شخص يعتبر بريئا حتى تثبت جهة قضائية نظامية إدانته مع كل الضمانات التي يتطلبها القانون".

ويعد هذا الإجراء الحديث من أهم إجراءات التحقيق، مكن المشرع ضابط الشرطة القضائية ممارسته للكشف عن الجرائم التي حددها على سبيل الحصر في المادة 65 مكرر 5 بموجب قانون الإجراءات الجزائية، تباشره الجهة القضائية في بعض الجنايات والجنح التي وقعت أو التي قد تقع في القريب العاجل، بمعنى أنها إجراء للتحري والتحقيق، وكل ما يتمخض عنها كدليل ضد كل شخص قامت تحريات جدية على أنه ضالع في ارتكاب هذه الجريمة أو لديه أدلة تتعلق بها، وأن في مراقبة أحاديثه الهاتفية ما يفيد في إظهار الحقيقة، بعد أن صعب الوصول إليها بوسائل البحث العادية.

لكن مع ذلك، نجد المشرع حاول يوفق بين هذه المتعارضات، بأن أجاز هذه الأساليب، ولكن بضوابط وهي مباشرة التحري بإذن من وكيل الجمهورية المختص، وإلتزام أعوان وضباط الشرطة القضائية القائمين بالإجراء السر المهني، وفيما يلي نتولى شرح كلا الضابطين، فالمشرع على الرغم من إقراره أساليب تحري خاصة قد تمس بحرمة الحياة الخاصة إلا أنه يعاقب على اللجوء لاستعمالها بطرق غير مشروعة[1]، وهو ما سنشير إليه على النحو التالي:

أولا: مباشرة التحري بإذن من وكيل الجمهورية

لم يسمح المشرع بإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بقصد التحري والتحقيق عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، إلا بإذن من وكيل الجمهورية المختص، وتباشر هذه العمليات تحت مراقبته، وهذا ما قررته المادة 04 من القانون 04/09 التي جاء فيها أنه: " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة."

(1)–المادة (303 مكرر) من الأمر رقم 156/66 معدلة ومتممة بموجب المادة (33) من القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006.

ويجب أن يتضمن الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سواء أكانت سكنية أو غير سكنية، كما يجب أن يتضمن نوع الجريمة التي تبرر اللجوء إلى هذه التدابير ومدة هذه التدابير[1]، لذلك فإن الإذن المسلم من قبل وكيل الجمهورية للتحقيق في جريمة ما لا يصلح للتحقيق في جريمة أخرى، إلا بإذن جديد، كذلك يجب أن يتضمن الإذن كل الأماكن التي توضع فيها الترتيبات التقنية من أجل التقاط وتسجيل وتثبيت الكلام المتفوه به بصفة خاصة من شخص أو عدة أشخاص[2].

وعند مباشرة التحريات والتحقيقات، يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص، محضر عن كل عملية اعتراض للمراسلات وتسجيل الأصوات والتقاط للصور، وحتى عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتسجيل الصوتي أو السمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها[3]، بحيث يشتمل المحضر على كل البيانات المذكورة سابقا وتكون محددة تحديدا نافيا للجهالة، ويجب أن يشتمل المحضر على توقيع محرره في نهايته[4]، بعد أن يصنف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب، المراسلات أو الصور أو المحادثات المسجلة أو المفيدة في إظهار الحقيقة في محضر يودع بملف المتهم، وتنسخ وتترجم المكالمات التي تتم باللغات الأجنبية عند الاقتضاء، بمساعدة مترجم يسخر لهذا الغرض[5].

(1)- المادة (65 مكرر 7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

(2)- المادة (65 مكرر 7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

(3)- المادة (65 مكرر 9) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

(4)- كمال كمال الرخاوي، إذن التفتيش فقها وقضاء، الطبعة الأولى، دار الفكر والقانون، المنصورة، مصر، 2000، ص 271.

(5)- المادة (65 مكرر 10) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

ثانيا: إلتزام السر المهني

تكون إجراءات التحري والتحقيق سرية، ومن ثم فإن بحثها ضمن الضمانات الممنوحة للمتهم[1] ، والسرية تعني القيام قدر الإمكان ممن هو قائم بالتحري أو كلف بإجراء من إجراءاته أو ساهم فيه بالمحافظة على السر المهني، وبالتالي صارت السرية ليس هدفها كما كان عليه من قبل هو تسهيل قمع المتهم، بل صارت وسيلة لضمان الحريات الشخصية[2].

فقد نص المشرع صراحة على أن هذه العمليات تتم بمراعاة السر المهني ودون المساس به[3]، فالضابط المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ملزم قانونا بكتمان السر المهني ويجب أن يتخذ مقدما التدابير اللازمة لضمان احترام ذلك السر[4]، وقد نص قانون الإجراءات الجزائية على أن تكون إجراءات التحري والتحقيق سرية[5]، ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع، وكل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها فيه، لذلك فعملية التحري عن جرائم المساس بأنظمة المعالجة الألية للمعطيات تتم بسرية مطلقة، فيمنع منعا باتا أن يخبر المشتبه فيه بهذه التحريات أو أي شخص آخر، كذلك يمنع على ضابط الشرطة المأذون له أو المناب أن يفصح عن مضمون محضر التحريات لأي شخص كان، وإلا وقع تحت طائلة الجزاء الجنائي بتهمة إفشاء السر المهني، فيجب على ضباط الشرطة القضائية ومرؤوسيهم عدم إفشاء الأسرار التي جمعوها أثناء التحريات، لأن سمعة المواطنين لا يجوز أن تظل مهددة ببيانات غير مؤكدة.

(1)- المادة (11) من الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

(2)- سهيلة بوزيرة، مواجهة الصفقات العمومية المشبوهة، مذكرة ماجستير في القانون الخاص، كلية الحقوق جامعة جيجل، 2008، ص 127.

(3)- المادة (65 مكرر 7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

(4)- المادة (45 /3) من الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

(5)- المادة (11) الأمر رقم 155/66 معدل ومتمم.

الفرع الثاني: أسلوب التسرب أو الاختراق

يعتبر التسرب تقنية جديدة أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة 2006، عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر 5)، كما يجوز لوكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن شروط محددة[1] ويشترط حصول الضابط المكلف بالتسرب على الإذن من وكيل الجمهورية المختص، ويجب أن تتم العملية تحت أشرافه ومراقبته، فإن قرر ضابط الشرطة القضائية مباشرة هذا الإجراء وجب عليه أولا إخطار وكيل الجمهورية بذلك، ثم يقوم بمنح الإذن مكتوب لضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، على أن يتم ذكر هويته فيه[2]، وهذا تحت طائلة البطلان المطلق، فيجب أن يكون الإذن مكتوبا يتضمن كل ما يتعلق بعملية التسرب وكذلك هوية ضباط وأعوان الشرطة المأذون لهم بالتسرب.

والتسرب هو قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيهم، بإيهامهم أنه فاعل معهم أو شريك لهم[3]، فالتسرب إذن هو قيام المأذون له بالتحقيق في الجريمة بمراقبة الأشخاص المشتبه في ارتكابهم جريمة، أو التوغل داخل جماعة إجرامية بإيهامهم أنه شريك لهم، ويسمح لضباط وأعوان الشرطة القضائية بأن يستعملوا لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة بعض الجرائم، دون أن يكون مسؤولا جزائيا[4]، وذلك بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، بإخفاء الهوية الحقيقية.

(1)- المادة (65 مكرر11) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

(2)- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثانية، الجزائر، 2009، ص 115.

(3)- المادة (65 مكرر12) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

(4)- عيساوي نبيلة، المرجع السابق، ص 02.

ولهذا يجوز لضابط أو عون الشرطة القضائية المرخص له بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض، دون أن يكونوا مسؤولين جزائيا القيام بما يلي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات 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 التخزيب أو الإيواء أو الحفظ أو الاتصال.

ويحظر على المتسرب إظهار الهوية الحقيقية في أي مرحلة من مراحل الإجراءات مهما كانت الأسباب إلا لرؤسائهم السلميين، لأن هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم وتعريض العضو المكشوف عن هويته للخطر، وهو ما أكده المشرع بموجب المادة (65 مكرر 16) بأن نصت صراحة أنه:" لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات."

كما عاقب المشرع كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وبغرامة من 50000 دج إلى 2000000 دج، وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين، فتكون العقوبة الحبس من خمس سنوات إلى 10 سنوات والغرامة من 200000 دج إلى 500000 دج، وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من 10 إلى 20 سنة والغرامة من 500000 إلى 1000000 دج[1].

(1)- المادة (3/65 – 4 مكرر) من الأمر رقم 155/66 المعدل والمتمم ومعدل بموجب المادة (14) من القانون رقم 22/06.

ورغم أن المشرع أجاز مثل هذه الأفعال التي تعتبر في حقيقة الأمر جرائم من أجل خلق الثقة وتعزيزها في ضباط الشرطة القضائية وأعوانهم المرخص لهم بإجراء عملية التسرب من قبل المشتبه فيهم والنجاح في إيهامهم بأنهم شركاء أو فاعلون، مع ذلك منع المشرع هؤلاء الضباط أو الأعوان من أن يحرّضوا المشتبه فيهم على ارتكاب الجريمة، بمعنى أنه يمنع على الضباط والأعوان المتسربين أن يخلقوا الفكرة الإجرامية للشخص الموضوع تحت المراقبة ودفعه لارتكاب الجريمة، فهذا الفعل ممنوع تحت طائلة بطلان الإجراء.

خلاصة الفصل

ما سبق تم التطرق في هذا الفصل الى الأجهزة المختصة المكافحة للجريمة المعلوماتية متمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام والاتصال، الأجهزة الأمنية سواء الامن الوطني أو الدرك الوطني سواء على المستوى الوطني أو الجهوي أو المحلي، ثم بعد ذلك تم التطرق الى الإجراءات القانونية للتحري من أجل الكشف ومكافحة الجريمة المعلوماتية، التي تكمن المحقق من التعرف على الجاني وتوقيفه وتقديمه أمام النيابة العامة لأخذ جزاءه.

الخاتمة

نستخلص من خلال ما قد سبق دراسته نجد أن موضوع الجريمة المعلوماتية يعد من المواضيع البالغة في الأهمية نظرا لخطورتها، مما يتطلب دراسة دقيقة وعميقة حولها، الأمر الذي جعلنا نلاحظ وجود آليات معتمدة لمكافحة هذه الجريمة في التشريع الجزائري وفقا لمجهودات قد قامت بها أجهزة الدولة من جهة.

فنرى أن المشرع سعيا منه لتدارك الفراغ التشريعي الذي وقع فيه بخصوص مجال مكافحة الجرائم المعلوماتية، قد قام بإدراج تعديلات خاصة على قانون العقوبات الجزائري، واستحداث قانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، محاولة منه للتقليص من هذه الجرائم المستحدثة و العابرة للحدود.

من بين النتائج التي توصلنا إليها نجد:

1- الجرائم المعلوماتية من بين الجرائم المستحدثة و العابرة للحدود.

2- هي من الجرائم المختلفة من حيث خصائصها عن الجريمة التقليدية، كما أنها صعبة الإثبات والإكتشاف كما يقل الإبلاغ فيها.

3- الجرائم المعلوماتية من بين الجرائم التي لا يتطلب فيها العنف على الإطلاق ويتصف المجرم المعلوماتي فيها بالذكاء والسرعة كذلك يكون متميزا بالدقة والتخصص في مسائل تكنولوجيا المعلومات.

4- هي من بين الجرائم التي تتوافق مع غيرها من الجرائم في مدى توفر القصد الجنائي العام.

5- إسراع الدولة إلى إيجاد حلول قانونية ردعية للحد من انتشار هذه الجريمة، كذلك تسخير الكفاءات البشرية للوقاية من تأثير هذه الجرائم على الأمن العام وكذا حماية المواطنين من خطورتها.

6- تفطن المشرع الجزائري لهذا النوع من الجرائم بواسطة إحداثه التعديلات في القانون العقوبات وقانون الإجراءات الجزائية واستحداث قانون 04/09 لمكافحة هذه الجريمة إلا أن ذلك لا يعتبر كافيا مع حداثة هذا النوع المستحدث من الجرائم الذي هو في تزايد مستمر.

أما بالنسبة للاقتراحات التي يمكن تقديمها هي كالآتي:

1- نقترح من وجهة نظرنا أنه على المشرع استحداث تعريف قانوني خاص لهذا النوع المستجد من الجرائم، نظرا لازدیادهم وخطورته، الأمر الذي يستوجب إضفاء تعريف يبين نوعية الجريمة لعدم الوقوع في الخطأ خاصة من ناحية التكييف.

2- على المشرع أن يقوم بتطوير بنيته التشريعية تماشيا مع التطور السريع والملحوظ لهذه الجريمة.

3- إنشاء أقسام متخصصة بالجرائم المعلوماتية.

4- ضرورة تخصيص شرطة جنائية خاصة وخبراء من ذوي الكفاءة العالية في مجال الأنترنت.

5- حبذا لو سار المشرع توفير الوسائل والأجهزة المسخرة والمتنوعة لقمع الجريمة من جهة مغايرة.

6- ضرورة إبرام معاهدات وإتفاقيات دولية لردع الجريمة المعلوماتية.

7- على السلطات المختصة الإكثار من الحملات التوعوية للمواطنين من أجل وضعهم في الصورة لتوخي الحيطة والحذر من هذه الجرائم التي تتزايد أكثر فأكثر.

مما سبق ذكره أن هذه الجريمة عابرة للحدود وصعبة الاثبات، لذلك أقترح ان تكون دراسات في المستقبل، تتضمن نظرة المشرع الجزائري لهذه الجريمة المعلوماتية مقارنة بتشريعات الدول العربية أو بتشريعات الدول الغربية، ومدى الجهود الدولية المبذولة لمكافحة هذه الجريمة.

أرجوا أن أكون قد وقفت في معالجة هذا الموضوع، وإن لم أوفق فإنني اجتهدت ولكل مجتهد نصيب.

قائمة المصادر
والمراجع

1. أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية 2006.

2. أسامة احمد المناعة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان 2014.

3. آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر 2007.

4. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2004.

5. بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007.

6. حسن صادق المرصفاوي، المرصفاوي في التحقيق الجنائي، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر، 1990.

7. حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الاولى، منشورات الحلبي الحقوقية، بيروت 2014.

8. خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنات، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان2011.

9. خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، 2010.

10. خلفي عبد الرحمن، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة، الجزائر، 2010.

11. طارق إبراهيم الدسوقي عطية، الامن المعلوماتي ، دار الشر الجديدة الاسكندرية، سنة 2009.

12. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، 2007.

13. كمال كمال الرخاوي، إذن التفتيش فقها وقضاء، الطبعة الأولى، دار الفكر والقانون، المنصورة، مصر، 2000.

14. محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004.

15. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثانية، الجزائر، 2009.

16. محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة الثامنة، دار الجامعة الجديدة، 2008.

17. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، سنة 2008.

18. منير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005.

19. نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2 ، دار الثقافة للنشر والتوزيع.

20. هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.

21. هشام محمد فريد رستم، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة، 2000.

القوانين والأوامر

1. دستور 1996.
2. القانون رقم 04-15 مؤرخ في 10 نوفمبر2004، يتضمن تعديل قانون العقوبات.
3. القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية
4. القانون رقم 09-04 المؤرخ في 05 اوت 2009، يتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.
5. المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المطويات الخاصة

1. مساهمة الشرطة العلمية والتقنية في مجال التحقيقات الجنائية- وثيقة خاصة صادرة عن مديرية الشرطة القضائية- المديرية العامة للأمن الوطني.
2. مساهمة المخبر الجهوي للشرطة العلمية –وهران- في إدارة الدليل ضمن التقنيات الخاصة للتحقيق – وثيقة خاصة صادرة عن المخبر الجهوي للشرطة العلمية – وهران – نيابة مديرية الشرطة العلمية و التقنية – مديرية الشرطة القضائية- المديرية العامة للأمن الوطني.

مذكرات الجامعية

1. بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة 16 و17 نوفمبر 2015، كلية الحقوق جامعة بسكرة.
2. حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدّمة لنيل شهادة دكتوراه العلوم في الحقوق تخصّص- قانون العقوبات العلوم الجنائية، جامعة باتنة1، السنة الجامعية 2016/2015

3. سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماجيستر في العلوم القانونية، جامعة الحاج لخضر باتنة، سنة دراسية 2013/2102.

4. سهيلة بوزبرة، مواجهة الصفقات العمومية المشبوهة، مذكرة ماجستير في القانون الخاص، كلية الحقوق جامعة جيجل، 2008.

5. طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، السنة 2011-2012.

6. عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة د. الطاهر مولاي، سعيدة، سنة 2016/2015.

<u>المواقع الانترنات</u>

1. الموقع الرسمي لقيادة الدرك الوطني - تاريخ التصفح 31 مارس 2019 - الرابط الإلكتروني:http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined

الملاحق

الملحق 01:

25 شعبان عام 1430 هـ
16 غشت سنة 2009 م

الجريدة الرّسميّة للجمهوريّة الجزائريّة / العدد 47

5

قوانين

قانون رقم 09 – 04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إن رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 119 و120 و122 – 7 و126 منه،

– وبمقتضى الأمر رقم 66 – 155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 66 – 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 58 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدّل والمتمّم،

– وبمقتضى القانون رقم 2000 – 03 المؤرّخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدّد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 03 – 05 المؤرّخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة،

– وبمقتضى القانون رقم 08 – 09 المؤرّخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبعد رأي مجلس الدولة،

– وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

الفصل الأول
أحكام عامة
الهدف

المادّة الأولى : يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المصطلحات

المادّة 2 : يقصد في مفهوم هذا القانون بما يأتي :

أ – الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية،

ب – منظومة معلوماتية : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،

ج – 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،

د – مقدمو الخدمات :

1 – أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

2 – وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها،

هـ – المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة،

و – الاتصالات الإلكترونية : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

مجال التطبيق

المادّة 3 : 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 الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الفصل الثاني

مراقبة الاتصالات الإلكترونية

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

المادّة 4 : يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

أ – للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة،

ب – في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج – لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

د – في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

الفصل الثالث

القواعد الإجرائية

تفتيش المنظومات المعلوماتية

المادّة 5 : يجوز للسلطات القضائية المختصة وكذا ضبّاط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى :

أ – منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب – منظومة 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.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

حجز المعطيات المعلوماتية

المادّة 6 : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة

تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

الحجز عن طريق منع الوصول إلى المعطيات

المادّة 7 : إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

المعطيات المحجوزة ذات المحتوى المجرم

المادّة 8 : يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

حدود استعمال المعطيات المتحصل عليها

المادّة 9 : تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

الفصل الرابع

التزامات مقدمي الخدمات

مساعدة السلطات

المادّة 10 : في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

حفظ المعطيات المتعلقة بحركة السير

المادّة 11 : مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ :

أ – المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب – المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج – الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د – المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ – 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 وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

تحدد كيفيات تطبيق الفقرات 1 و2 و3 من هذه المادة، عند الحاجة، عن طريق التنظيم.

الالتزامات الخاصة بمقدمي خدمة "الإنترنت"

المادّة 12 : زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الإنترنت" ما يأتي :

أ – التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

ب – وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

إنشاء الهيئة

المادّة 13 : تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

مهام الهيئة

المادّة 14 : تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية :

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،

ب – مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

الفصل السادس

التعاون والمساعدة القضائية الدولية

الاختصاص القضائي

المادّة 15 : 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 الاستراتيجية للاقتصاد الوطني.

المساعدة القضائية الدولية المتبادلة

المادّة 16 : في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

تبادل المعلومات واتخاذ الإجراءات التحفظية

المادّة 17 : تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل.

القيود الواردة على طلبات المساعدة القضائية الدولية

المادّة 18 : يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

المادّة 19 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009.

عبد العزيز بوتفليقة

الملحق 02:

مراسيم تنظيميّة

مرسوم رئاسي رقم 15-261 مؤرّخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إنّ رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 39 و77 (1 و2 و8) و125 (الفقرة الأولى) منه،

– وبمقتضى القانون العضوي رقم 04-11 المؤرخ في 21 رجب عام 1425 الموافق 6 سبتمبر سنة 2004 والمتضمن القانون الأساسي للقضاء،

– وبمقتضى الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية ، المعدل والمتمم،

– وبمقتضى الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم،

– وبمقتضى القانون رقم 90-21 المؤرخ في 24 محرم عام 1411 الموافق 15 غشت سنة 1990 والمتعلق بالمحاسبة العمومية، المعدل والمتمم،

– وبمقتضى القانون رقم 2000-03 المؤرخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدل والمتمم،

– وبمقتضى القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

يرسم ما يأتي :

الفصل الأول

أحكام عامة – تعاريف

المادّة الأولى : تطبيقا لأحكام المادة 13 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه، يهدف هذا المرسوم إلى تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تدعى في صلب النص "الهيئة".

المادّة 2 : الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل.

المادّة 3 : يحدد مقر الهيئة بمدينة الجزائر.

المادّة 4 : تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، تحت رقابة السلطة القضائية، طبقا لأحكام التشريع الساري المفعول، لا سيما منها قانون الإجراءات الجزائية والقانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه.

تكلف الهيئة، في ظل احترام الأحكام التشريعية المبينة أعلاه على الخصوص، بما يأتي :

– اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية،

– ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وبلستثناء أي هيئات وطنية أخرى،

– تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية،

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها،

– تطوير التعاون مع المؤسسات و الهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

– المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال،

– المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

المادّة 5 : يقصد في مفهوم هذا المرسوم ما يأتي :

– "**الاتصالات الإلكترونية**" : كل ترا سل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها من طريق أي وسيلة إلكترونية، بما في ذلك وسائل الهاتف الثابت والنقال.

– "**مستخدمو الهيئة**" : المستخدمون الذين يمارسون عملهم بالتوقيت الكامل في الهيئة مهما كان وضعهم القانوني الأصلي.

الفصل الثاني

تشكيلة الهيئة وتنظيمها

المادّة 6 : تضم الهيئة :

– لجنة مديرة،

– مديرية عامة،

– مديرية للمراقبة الوقائية واليقظة الإلكترونية،

– مديرية للتنسيق التقني،

– مركز للعمليات التقنية،

– ملحقات جهوية.

المادّة 7 : يرأس اللجنة المديرة الوزير المكلف بالعدل، وتتشكل من الأعضاء الآتي ذكرهم :

– الوزير المكلف بالداخلية،

– الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال،

– قائد الدرك الوطني،

– المدير العام للأمن الوطني،

– ممثل عن رئاسة الجمهورية،

– ممثل عن وزارة الدفاع الوطني،

– قاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

يعين ممثلا رئاسة الجمهورية ووزارة الدفاع الوطني بموجب مرسوم رئاسي.

المادّة 8 : تكلف اللجنة المديرة على الخصوص، بما يأتي :

– توجيه عمل الهيئة والإشراف عليه ومراقبته،

– دراسة كل مسألة تخضع لمجال اختصاص الهيئة، لا سيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية المنصوص عليها في المادة 4 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه،

– ضبط برنامج عمل الهيئة وتحديد شروط وكيفيات تنفيذه،

– القيام دوريا بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة، للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة ،

– اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– دراسة مشروع النظام الداخلي للهيئة والموافقة عليه،

– دراسة مشروع ميزانية الهيئة والموافقة عليه،

– دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه،

– إبداء رأيها في كل مسألة تتصل بمهام الهيئة،

– تقديم كل اقتراح مفيد يتصل بمجال اختصاص الهيئة.

المادّة 9 : يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي. وتنهى مهامه حسب الأشكال نفسها.

المادّة 10 : يتولى المدير العام الصلاحيات الآتية على الخصوص :

– السهر على حسن سير الهيئة،

– السهر على تنفيذ برنامج عمل الهيئة،

– تنشيط نشاطات هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها،

- تحضير اجتماعات اللجنة المديرة،

- تمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية،

- تمثيل الهيئة لدى القضاء وفي جميع أعمال الحياة المدنية،

- ممارسة السلطة السلّمية على مستخدمي الهيئة،

- السهر على احترام قواعد حماية السر في الهيئة،

- السهر على القيام بإجراءات التأهيل وأداء اليمين قبما يخص المستخدمين المعنيين في الهيئة،

- إعداد التقرير السنوي لنشاطات الهيئة وعرضه على اللجنة المديرة للمصادقة عليه،

- ضمان التسيير الإداري والمالي للهيئة.

المادّة 11 : تكلف مديرية المراقبة الوقائية واليقظة الإلكترونية على الخصوص، بما يأتي :

- تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول،

- إرسال المعلومات المحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة،

- تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم،

- جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

- تنظيم و/أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والاتصال، وحول المخاطر المتصلة بها،

- تنفيذ توجيهات اللجنة المديرة،

- تزويد السلطات القضائية ومصالح الشرطة القضائية، تلقائيا أو بناء على طلبها، بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

- وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة والسهر على حسن سيرها وكذا الحفاظ على الحالة الجيدة لمنشآتها وتجهيزاتها ووسائلها التقنية،

- تطبيق قواعد الحفاظ على السر في نشاطاتها.

المادّة 12 : تكلف مديرية التنسيق التقني على الخصوص، بما يأتي :

- إنجاز الخبرات القضائية في مجال اختصاص الهيئة،

- تكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها،

- إعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

- القيام بمبادرة منها أو بناء على طلب اللجنة المديرة، بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها،

- تسيير منظومة الإعلام للهيئة وإدارتها.

المادّة 13 : يزود مركز العمليات التقنية بالمنشآت والتجهيزات والوسائل المادية وكذا بالمستخدمين التقنيين الضروريين لتنفيذ العمليات التقنية لمراقبة الاتصالات الإلكترونية.

ويتبع هذا المركز مديرية المراقبة الوقائية واليقظة الإلكترونية ويتم تشغيله من طرفها.

المادّة 14 : يتم تشغيل الملحقات الجهوية من طرف مديرية المراقبة الوقائية واليقظة الإلكترونية التي تتبعها.

المادّة 15 : يحدد التنظيم الداخلي لهياكل الهيئة بموجب قرار مشترك بين الوزراء المكلفين بالعدل، والدفاع الوطني، والداخلية.

الفصل الثالث

كيفيات سير الهيئة

المادّة 16 : تجتمع الهيئة المديرة بناء على استدعاء من رئيسها أو بناء على طلب أحد أعضائها.

المادّة 17 : تعد الهيئة نظامها الداخلي وتصادق عليه.

المادّة 18 : تزود الهيئة بقضاة وفقا للشروط والكيفيات المنصوص عليها بموجب التشريع الساري المفعول.

كما تزود بضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني، يحدد عددهم بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل، والدفاع الوطني، والداخلية.

وتزود أيضا بمستخدمي الدعم التقني والإداري، ويجلب هؤلاء المستخدمون من ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني.

المادة 19 : يمكن أن تستعين الهيئة بأي خبير أو أي شخص يمكن أن يعينها في أعمالها.

المادة 20 : تؤهل الهيئة لكي تطلب من أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة ضرورية لإنجاز المهام المسندة إليها.

المادة 21 : قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة، تكلف الهيئة حصريا بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية تحت سلطة قاض مختص، ووفقا للأحكام المنصوص عليها في المادة 4 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه.

المادة 22 : يمكن الهيئة لتنفيذ عملية المراقبة الاتصالات الإلكترونية، أن تضع وحدة مراقبة واحدة أو أكثر، تزود بالوسائل والتجهيزات التقنية الضرورية.

تتشكل الوحدة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاض يساعده ضابط واحد من الشرطة القضائية أو أكثر ينتمي للهيئة.

تمتثل الوحدة في عملها إلى أحكام التشريع الساري المفعول وشروط الرخصة المسلّمة من الشرطة القضائية.

وتحرر أشغالها في محضر يعد طبقا لأحكام قانون الإجراءات الجزائية.

المادة 23 : لا يمكن أن يشارك في عملية المراقبة الاتصالات الإلكترونية إلا أعضاء الوحدة أو الوحدات التي أوكلت لها السلطة القضائية هذه المهمة.

يتخذ مسؤول الوحدة أثناء سير العملية كل التدابير اللازمة، بالاتصال مع المسؤولين المعنيين في الهيئة، من أجل ضمان سرية العملية وحماية المعلومات المستقاة من المراقبة.

المادة 24 : تحفظ المعلومات المستقاة أثناء عمليات المراقبة، خلال حيازتها من الهيئة، وفقا للقواعد المطبقة على حماية المعلومات المصنفة.

المادة 25 : تسجل الاتصالات الإلكترونية التي تكون موضوع مراقبة، وتحرر وفقا للشروط والأشكال المنصوص عليها في قانون الإجراءات الجزائية.

تسلّم التسجيلات والمحررات إلى السلطات القضائية وإلى مصالح الشرطة القضائية المختصة وتحفظ السلطات القضائية، دون سواها بهذه العمليات أثناء المدة القانونية المنصوص عليها في التشريع الساري المفعول.

المادة 26 : يجب، تحت طائلة العقوبات الجزائية المنصوص عليها في التشريع الساري المفعول، ألا تستخدم المعلومات والمعطيات التي تستلمها أو تجمعها الهيئة، لأغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وذلك وفقا للأحكام المنصوص عليها في القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه.

المادة 27 : يلزم مستخدمو الهيئة بالسرّ المهني وواجب التحفظ.

ويخضع المستخدمون من بينهم الذين يدعون إلى الاطلاع على معلومات سرّية إلى إجراءات التأهيل.

المادة 28 : يؤدي مستخدمو الهيئة الذين يدعون إلى الاطلاع على المعلومات السرّية، اليمين أمام المجلس القضائي، قبل تنصيبهم، الآتي نصه :

"أقسم بالله العليّ العظيم أن أقوم بعملي أحسن قيام، وأن أخلص في تأدية مهمتي، وأن أكتم الأسرار والمعلومات أيا كانت التي أطلع عليها أثناء قيامي بعملي أو بمناسبته، وأن أسلك في كل الظروف سلوكا شريفا".

المادة 29 : يوضع مستخدمو الهيئة تحت سلطة المدير العام.

المادة 30 : يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعون للهيئة أثناء ممارستهم لوظائفهم أو بمناسبتها، طبقا للشروط والكيفيات المنصوص عليها في التشريع الساري المفعول، ولا سيما قانون الإجراءات الجزائية، بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم أنه يحوز و/أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية.

وفي حالة معاينة أفعال يمكن وصفها جزائيا، تخطر الهيئة النائب العام المختص للقيام بالمتابعات المحتملة.

المادّة 31 : يمكن أن تطلب الهيئة مساعدة موظفين مختصين من الوزارات المعنية في مجال تكنولوجيات الإعلام والاتصال، طبقا للشروط والكيفيات المحددة في التنظيم الساري المفعول.

المادّة 32 : يرفع رئيس اللجنة المديرة للهيئة إلى رئيس الجمهورية تقارير فصلية عن نشاطات الهيئة.

الفصل الرابع

أحكام مالية

المادّة 33 : يعد المدير العام ميزانية الهيئة ويعرضها على اللجنة المديرة للموافقة عليها.

تسجل ميزانية الهيئة في الميزانية العامة للدولة طبقا للتشريع والتنظيم الساريين المفعول.

ويكون المدير العام هو الآمر بصرف ميزانية الهيئة.

المادّة 34 : تشتمل ميزانية الهيئة على باب للإيرادات وباب للنفقات.

في باب الإيرادات :

- إعانات الدولة.

في باب النفقات :

- نفقات التسيير،
- نفقات التجهيز.

المادّة 35 : تمسك محاسبة الهيئة وفق قواعد المحاسبة العمومية.

يتولى مسك المحاسبة عون محاسبة يعينه أو يعتمده الوزير المكلف بالمالية.

المادّة 36 : يمارس المراقبة المالية للهيئة مراقب مالي يعينه الوزير المكلف بالمالية.

الفصل الخامس

أحكام قانونية أساسية

المادّة 37 : يعيّن مدير المراقبة الوقائية واليقظة الإلكترونية ومدير التنسيق التقني بموجب مرسوم رئاسي. وتنهى مهامهما حسب الأشكال نفسها.

المادّة 38 : يبقى ضباط وأعوان الشرطة القضائية وكذا المستخدمون المدنيون للوزارات المعنية والممارسون وظائفهم في الهيئة خاضعين للأحكام التشريعية والتنظيمية والقانونية الأساسية المطبقة عليهم.

المادّة 39 : يستفيد مستخدمو الهيئة، طبقا للتشريع الساري المفعول، من حماية الدولة من التهديدات أو الضغوط أو الإهانات، مهما تكن طبيعتها، التي قد يتعرضون لها بسبب أو بمناسبة قيامهم بمهامهم.

المادّة 40 : تحدد طريقة صرف الرواتب والنظام التعويضي المطبقين على مستخدمي الهيئة بموجب نص خاص يحدد تصنيف الوظائف في الهيئة.

الفصل السادس

أحكام ختامية ونهائية

المادّة 41 : تمارس الهيئة الحصرية في مجال مراقبة الاتصالات الإلكترونية تحت مراقبة قاض مختص، باستثناء الحالات المنصوص عليها في قانون الإجراءات الجزائية.

وزيادة على ذلك، وما عدا الحالات المبيّنة في الفقرة السابقة، لا يمكن أن تستورد أو تقتني أو تحوز أو تستعمل الوسائل والتجهيزات التقنية لمراقبة الاتصالات الإلكترونية إلا الهيئة، أو عند الاقتضاء، سلطة ضبط الاتصالات السلكية واللاسلكية وكذا المؤسسة العمومية المكلفة بشبكات الاتصالات، وذلك باستثناء أي هيئة أو مؤسسة أو شخص.

يتولى الأعوان المؤهلون في الهيئة ووحداتها المكلفة بالمراقبة، لصالح ضباط الشرطة القضائية، الجوانب التقنية للعمليات المنصوص عليها في قانون الإجراءات الجزائية.

المادّة 42 : تحول إلى الهيئة نشاطات مراقبة الاتصالات الإلكترونية التي كانت تمارسها في السابق هيئات وطنية أخرى.

تحدد كيفيات تطبيق هذه المادة بموجب نص خاص.

المادّة 43 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015.

عبد العزيز بوتفليقة

الفهرس