

## إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الإتصال والمعلوماتية

د. عزالدين عثمانى

جامعة تبسة

### ملخص:

لا شك أن ظهور أنماط جديدة من الجرائم لم تكن مألوفة في السابق ونحن لا نزال في بداية عصر الانفجار المعلوماتي، يعنى توقع ظهور المزيد و المزيد من هذه الأنماط الجديدة، التي يتوجب معها تحديث الأنظمة و التعليمات و الجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة، وهو ما يستتبع تطوير أسلوب التحقيق والتفتيش فيها.

كما أن التحقيق بشكل عام يعتمد على ذكاء المحقق و فطنته و قوة ملاحظته و سرعة البديهة لديه، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق و البحث فيها و متابعتها، والبحث في الأدلة والتنقيب عنها وصولا إلى إظهار الحقيقة.

وتتميز الجريمة الإلكترونية بخصائص وصفات تميزها عن الجرائم الأخرى تجعلها صعبة الإثبات لعدم وجود الآثار المادية التقليدية مثل بقع الدم والبصمات، مما يؤدي إلى ضرورة البحث عن أدلة أخرى لإثباتها ودون أدنى شك فإن مسألة الحصول على هذه الأدلة يتطلب منظومة قانونية وقضائية فعالة تتولى مسألة التحقيق والتفتيش في هذا النوع من الجرائم.

### Abstract:

There is no doubt that the emergence of new types of non-common crimes in the past and we are still at the beginning of the era of information explosion, means the expectation of the emergence of more and more of these new patterns, which urge to update regulations and instructions and the competent security authorities to address the issues resulting from the emergence of these new patterns, which entails the development of investigation and inspection manners.

The investigation in general depends on the intelligence of the investigator and his intuition, the strength of his observation and the speed of his intuition, and he must try with all possible effort to investigate and search and follow-up, and search for evidence and their exploration to show the truth.

The e-crime is characterized by characteristics and qualities distinguish it from other crimes which make it difficult to be proven due to the absence of traditional physical effects such as blood stains and fingerprints, this leads to the need to search for other evidence of improve, and without doubt, the issue of obtaining this evidence requires an effective legal and judicial system handles the matter of investigation and inspection in this type of crimes.

مقدمة:

### التعريف بالموضوع :

تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تطورا ملموسا يواكب حركة الجريمة و تطور أساليب ارتكابها، فبعد أن كان الطابع المميز لوسائل التحقيق العنف والتعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية الحديثة القائمة على الإستعانة بالأساليب العلمية و استخدام شبكة الإنترنت هي الصفة المميزة و الغالبة، ومرد ذلك هو حدوث طفرة علمية في مجال تكنولوجيا المعلومات و الإتصالات و استخدام الوسائط الإلكترونية في شتى مجالات الحياة، فكلما اكتشف العلم شيئا حديثا وجد الإكتشاف طريقه إلى مجال الإثبات الجنائي و التدليل.

وقد اصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال وعرفها بموجب القانون 09-04 المؤرخ في 05 غشت 2009 على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات و أية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

### - أهمية الموضوع :

لا شك أن ظهور أنماط جديدة من الجرائم لم تكن مألوفة في السابق ونحن لا نزال في بداية عصر الانفجار المعلوماتي، يعنى توقع ظهور المزيد و المزيد من هذه الأنماط الجديدة، التي يتوجب معها تحديث الأنظمة و التعليمات و الجهات الأمنية المختصة بمعالجة القضايا

الناجمة عن ظهور هذه الأنماط الجديدة، وهو ما يستتبع تطوير أسلوب التحقيق والتفتيش فيها.

كما أن التحقيق بشكل عام يعتمد على ذكاء المحقق و فطنته و قوة ملاحظته وسرعة البديهة لديه، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق و البحث فيها و متابعتها، والبحث في الأدلة و التنقيب عنها وصولا إلى إظهار الحقيقة.

وتتميز الجريمة الإلكترونية بخصائص وصفات تميزها عن الجرائم الأخرى تجعلها صعبة الإثبات لعدم وجود الآثار المادية التقليدية مثل بقع الدم والبصمات، مما يؤدي إلى ضرورة البحث عن أدلة أخرى لإثباتها ودون أدنى شك فإن مسألة الحصول على هذه الأدلة يتطلب منظومة قانونية وقضائية فعالة تتولى مسألة التحقيق والتفتيش في هذا النوع من الجرائم .

#### - أهداف الدراسة:

الهدف من هذه الدراسة هو تسليط الضوء على إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الإتصال والمعلوماتية، وإبراز خصوصيتها بالنسبة للجرائم التقليدية.

#### إشكالية الدراسة:

الإشكالية التي يمكن طرحها لهذا الموضوع ومن ثمة معالجتها تتمثل أساسا في مدى فعالية إجراءات التحقيق والتفتيش في الكشف عن الجرائم الماسة بأنظمة الإتصال والمعلوماتية في التشريع الجزائري؟.

وسنجيب عن هذه الإشكالية من خلال الإعتماد على خطة مكونة من مبحثين:

الأول بعنوان: التحقيق في الجرائم الماسة بأنظمة الإتصال والمعلوماتية.

والثاني بعنوان: التفتيش في الجرائم الماسة بالمعطيات الرقمية.

#### المبحث الأول : التحقيق في الجرائم الماسة بأنظمة الإتصال والمعلوماتية.

إن مقتضيات تطبيق مبدأ الشرعية تقتضي إرساء مجموعة قواعد إجرائية تخضع لها السلطة القضائية وأعاونها، حتى يستطيع رجال الضبط القضائي ممارسة إجراءات خاصة

تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية<sup>(1)</sup>

ونظرا لأهمية التحقيق في هذا النوع من الجرائم قسمنا هذا المبحث إلى مطلبين تناولنا في المطلب الأول الأجهزة المكلفة بالتحقيق في الجرائم الماسة بأنظمة الإتصال والمعلوماتية، وفي المطلب الثاني التفتيش في الجرائم الماسة بأنظمة الإتصال والمعلوماتية. المطلب الأول : الأجهزة المكلفة بالتحقيق في الجرائم الماسة بأنظمة الإتصال والمعلوماتية.

منح القانون 04-09 دورا ايجابيا لمقدمي الخدمات من خلال مساعدة السلطات العمومية في مواجهة الجرائم الماسة بأنظمة الإتصال والمعلوماتية وكشف مرتكبيها حيث تنص المادة الثالثة منه على وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية .

ونص ذات القانون في مادته الرابعة على أربعة حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والإتصالات الإلكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة، وكذلك في حال توفر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام، ولمقتضيات التحريات والتحقيقات القضائية، عندما يصعب الوصول إلى نتيجة تم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وفي إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

وعلى هذا الأساس، يجوز للجهات القضائية وضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي، ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن

الجرائم أو مرتكبيها ذلك أن ملاحقة الجناة وكشف جرائمهم عبر الحدود يقتضي من الناحية العملية أن يتم هذا الإجراء في نطاق إقليم دولة أخرى<sup>(2)</sup>

الفرع الأول: الأعوان المكلفون بالتحري وجمع الأدلة في الجرائم الماسة بأنظمة الإتصال والمعلوماتية.

يعتبر جهاز الضبطية القضائية صاحب الولاية العامة في البحث والتحري عن الجرائم بمختلف أنواعها وأشكالها، غير أن ذلك لا يمنع أن تعهد بعض القوانين الخاصة بهذا الدور على سبيل الإستثناء إلى بعض الجهات والهيئات الخاصة بحكم خبرتها في مجال معين وباعتبارها الأقدر من غيرها على كشف الجرائم الواقعة ضمن حدود اختصاصها الفني أو التقني، والواقع أن ذلك لا يحول دون ضرورة تنسيق الجهود مع جهاز الضبطية القضائية التقليدي من أجل ضمان تحقيق أكبر قدر من الفعالية في مجال ضبط الجرائم والتحري بشأنها .

ومن أجل إشراك مزودي خدمات الإنترنت والاتصالات الثابتة والمتنقلة في محاربة الجرائم التكنولوجية، يلزم القانون 09-04 هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات الملزمين بحفظها، وتشمل هذه المساعدة المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وتلك المتعلقة بالتجهيزات المستعملة في الإتصال، والخصائص التقنية وتاريخ وزمن ومدة كل اتصال، والمعطيات المتصلة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، بالإضافة إلى المعلومات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم وعناوين المواقع المطلع عليها.

ويتضمن القانون أيضا إجراءات عقابية حيث أنه ولتفادي أي تهرب من إلتزامات القانون 09-04، يسلط هذا الأخير على الأشخاص الطبيعيين الذين يعرفون سير التحريات القضائية عقوبة السجن من خمس إلى ستة سنوات وغرامة مالية تتراوح ما بين

خمسة ملايين إلى خمسين مليون سنتيم، مع معاقبة المؤسسات المخالفة بالغرامات المالية المنصوص عليها في قانون العقوبات<sup>(3)</sup>

### أولاً: جهاز الضبطية القضائية.

يعتبر أعضاء الشرطة القضائية موظفون منحهم القانون صفة الضبطية القضائية وخولهم بموجبها حقوق و فرض عليهم واجبات في إطار البحث عن الجرائم و مرتكبيها وجمع الإستدلالات عنها فيبدأ دورهم بعد وقوع الجريمة و ينتهي عند فتح التحقيق القضائي أو إحالة المتهم إلى جهة الحكم و تتميز الشرطة القضائية عن الشرطة الإدارية في أن المهمة الرئيسية لهذه الأخيرة تتمثل في تنفيذ تدابير الشرطة العامة الصادرة من السلطات المختصة ومراقبة نشاط الأفراد و الجماعات قبل وقوع الجريمة قصد المحافظة على الأمن العمومي ومنع أسباب الإضطرابات و إزالتها إذا وقعت فأعمال الشرطة الإدارية إجراءات وقائية ومانعة في حين أن أعمال الشرطة القضائية عبارة عن إجراءات رادعة .

ثانياً: دور مقدمي الخدمات في التحري والتحقيق في الجرائم الماسة بأنظمة

### الإتصال والمعلوماتية.

إن تكنولوجيات الإعلام والإتصال متنوعة خاصة ما يتعلق منها بخدمات الإتصال السلكية واللاسلكية، كالهواتف النقالة والشبكات الرقمية المتمثلة في الإنترنت، وهو ما يجعل عملية توصيل الخدمات المتنوعة لهذه التكنولوجيا إلى مستعمليها يتطلب توافر مجموعة من الفاعلين على رأسهم مقدمي الخدمات، المنصوص عليهم في القانون 09-04 الذي يعرفهم على أنهم:

1. أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات.
2. وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها<sup>(4)</sup>

## الفرع الثاني: الوسائل المستخدمة في التحري وجمع الأدلة.

عند القيام بالتحقيق في جريمة ما، فإنه يجب على المحقق الإلتزام بقوانين وتشريعات ولوائح مفسرة، و قواعد فنية تحقق الشرعية، و سهولة الوصول إلى الجاني، وحيث أن للجرائم المعلوماتية طابعها الخاص المميز لها، فإن التحقيق فيها يحتاج إلى معرفة تامة وإدراك لوسائل وقوع الجريمة و بالتالي حل لغرها و الوصول إلى الجاني، وفي سبيل ذلك يعتمد المحقق على مجموعة من الوسائل المختلفة.

### أولاً: الوسائل المادية.

وهي الأدوات الفنية التي غالباً ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها:

- عناوين IP ، والبريد الإلكتروني، وبرامج المحادثة.
- البروكسي (proxy) حيث يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الإتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة.(CacheMemory)
- برامج التتبع: حيث تقوم هذه البرامج بالتعرف على محاولات الإختراق التي تتم مع تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على إسم الحدث وتاريخ حدوثه وعنوان (IP) الذي تمت من خلاله عملية الإختراق، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى، ومن الأمثلة على هذه البرامج برنامج (Hack Tracer vl,2)
- نظام كشف الإختراق (Intrusion Détection System)، ويرمز له اختصاراً بالأحرف (IDS) وهذه الفئة من البرنامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسبة الإلكترونية أو الشبكة مع تحليلها بحثاً عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسبة الإلكترونية أو الشبكة.

ويتم ذلك من خلال تحليل رموز البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاص بتسجيل الأحداث فور وقوعها في جهاز الحاسبة الإلكترونية أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للإعتداءات على الأنظمة الحاسوبية والتي يطلق عليها أهل الاختصاص مصطلح التوقيع، وفي حال إكتشف النظام وجود أحد هذه التوقيعات يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الإعتداء في سجلات حاسوبية خاصة، والتي يمكن أن تقدم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها.

- أدوات تدقيق ومراجعة العمليات الحاسوبية.

- أدوات فحص ومراقبة الشبكات: هذه الأدوات تستخدم في فحص بروتوكول ما وذلك لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها ومن هذه الأدوات أدوات (ARP) وظيفتها تحديد مكان الحاسبة الإلكترونية فيزيائيا على الشبكة.

### ثانيا: الوسائل الإجرائية.

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة والغير محددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها.

1- إقتفاء الأثر: يمكن تفصي الأثر بطرق عدة سواء عن طريق بريد إلكتروني تم استقباله، أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الإختراق.

2- الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته.

3- الإستعانة بالذكاء الإصطناعي، من خلال إستنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الإلكترونية، وفق برامج صممت خصيصا لهذا الغرض.

4- مراقبة الإتصالات الإلكترونية: لم يعرف المشرع الجزائري على غرار العديد من المشرعين عملية مراقبة الإتصالات الإلكترونية، على عكس بعض التشريعات التي عرفتها مثل التشريع الأمريكي والكندي.<sup>(5)</sup>



### الفرع الثالث: صعوبات ومعوقات جمع الأدلة.

من الصعوبات التي قد تواجه عملية استخلاص الدليل في الجريمة الماسة بأنظمة الإتصال والمعلوماتية مسألة نقص الخبرة لدى رجل الضبط القضائي أو أجهزة الأمن بصفة عامة، وكذلك لدى أجهزة العدالة الجنائية متمثلة في سلطات الإتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي وأنظمة الإتصال والإلمام بعناصر الجرائم المعلوماتية وكيفية التعامل معها وذلك على الأقل في البلدان العربية بشكل عام، نظرا لأن تجربة الإعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاءت متأخرة عن أوروبا وكندا والولايات المتحدة، كما أن أجهزة العدالة المقاومة للجرائم المرتبطة بهذه التقنية تبدأ في التكوّن والتشكل عقب ظهور هذه الجرائم، وهو أمر يستغرق وقتا أطول من وقت إنباش الجريمة، لأن الجريمة الماسة بأنظمة الإتصال والمعلوماتية - كما سبق - تتقدم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها، وحتى الآن فإن الحركة التشريعية أو الثقافة الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بذات المعدل، وهذا الفارق في التقدم أو التطور ينعكس سلبا على فئة إجراءات الإستدلالات والتحقيقات في الدعوى الجنائية في الجريمة الماسة بأنظمة الإتصال والمعلوماتية، ومن هنا تأتي الدعوة إلى وجوب تأهيل سلطات الأمن وجهات التحقيق والإدعاء والحكم في شأن هذه الجرائم.<sup>(6)</sup>

### المبحث الثاني: التفتيش في الجرائم الماسة بالمعطيات الرقمية.

يعتبر التفتيش من أخطر الحقوق التي منحت للمحقق و ذلك لمساسه بالحريات التي تكفلها الدساتير عادة، ولذا نجد المشرع يضع لها ضوابط عديدة سواء فيما يتعلق بالسلطة التي تباشره أو تأذن بمباشرته و الأحوال التي تجوز فيها مباشرته و شروط إتخاذ هذا الإجراء بما يمثل ضمانات الحرية الفردية أو حرمة المسكن<sup>(7)</sup>

## المطلب الأول: شروط التفتيش في الجرائم الماسة بالمعطيات الرقمية.

هناك عدة شروط يجب توافرها لإجراء التفتيش منها ما هو موضوعي، و منها ما هو شكلي لذلك سنتطرق في الفرع الأول: للشروط الموضوعية، وفي الفرع الثاني: للشروط الشكلية .

### الفرع الأول: الشروط الشكلية.

المقصود بالشروط الشكلية تلك الإجراءات التي أوجب المشرع مراعاتها عند إجراء عملية التفتيش و الهدف من وضع هذه الشروط من قبل المشرع هو إحاطة عملية التفتيش بإجراءات و شكليات تضمن صحة ودقة النتائج التي يصل إليها القائم بالتفتيش و إحاطة المتهم بضمانات كافية للحفاظ على حرته الفردية فالشكالية في الإجراءات الجنائية هي ضمانة لعدم تعسف الجهات القائمة بالتفتيش لذلك سنتطرق إلى القواعد الشكلية لإجراء التفتيش:

#### 1- وقت إجراء التفتيش:

حدد المشرع الجزائري أوقات التفتيش من الساعة الخامسة صباحا إلى الساعة الثامنة مساء و قد نص على ذلك في قانون الإجراءات الجزائية " لا يجوز البدء في التفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا و لا بعد الساعة الثامنة مساء..."<sup>(8)</sup>

إلا أنه و في حالات استثنائية يجوز الخروج عن تلك القاعدة فعند ما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم الأموال و الإرهاب و كذلك الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناء على إذن مسبق من وكيل الجمهورية المختص<sup>(9)</sup>.

ويتبين من النص أعلاه أن المشرع الجزائري أجاز إجراء التفتيش في أي وقت من أوقات النهار و الليل في جرائم معينة حددها المشرع ومن بينها الجرائم المتعلقة بالمعالجة الآلية للمعطيات<sup>(10)</sup>

## 2- حضور الأشخاص المعنيين أثناء التفتيش:

كذلك المشرع الجزائري هو الآخر اشترط أن يتم تفتيش المنازل في حضور المتهم، و في حالة إذا ما تعذر عليه الحضور وقت الإجراء، كان على ضابط الشرطة القضائية أن يكلفه بتعيين ممثل له و إذا امتنع عن ذلك أو كان هاربا كان من الواجب أن ينوبه عنه شاهدين من غير الموظفين الخاضعين له .

## 3- محضر التفتيش في الجرائم الماسة بالمعطيات الرقمية:

تسمى محاضر الشرطة القضائية محاضر البحث الابتدائي و تكمن أهميتها في قيمتها الممنوحة لها كوسيلة إثبات على وقوع الجريمة و نسبتها إلى فاعلها من جهة، ومن خطورة الصلاحيات الواسعة الممنوحة بموجبها لضابط الشرطة القضائية لذلك عرف المشرع الجزائري محاضر الشرطة القضائية بأنها الوثائق المكتوبة التي يحررها ضابط الشرطة القضائية أثناء ممارسته لمهامه و يضمنها ما عاينه أو تلقاه من صلاحيات أو قام به من عمليات تدخل في اختصاصه(11).

## الفرع الثاني: الشروط الموضوعية.

يقصد بالشروط الموضوعية للتفتيش بصفة عامة في الجرائم التقليدية و بصفة خاصة في الجرائم الماسة بالمعطيات الرقمية الشروط اللازمة لإجراء تفتيش صحيح، ويمكن حصرها في الشروط الأساسية وهي سبب التفتيش، محل التفتيش، السلطة المختصة بالقيام بالتفتيش، وبالنسبة لسبب التفتيش فهو بالنسبة للجرائم الماسة بأنظمة الإتصال والمعلوماتية هو ارتكاب الجريمة المعلوماتية بشكل عام.

أما محل التفتيش فيقصد به بشكل عام مستودع سر الإنسان، و هذا المستودع إما أن يكون في محل له حرمة خاصة كالمسكن أو قد يكون الشخص أو رسائله، هذا بالنسبة للجرائم التقليدية(12)، أما بالنسبة للجرائم الماسة بأنظمة الإتصال والمعلوماتية فمحل التفتيش هو الحاسب الآلي الذي يعتبر النافذة التي تطل بها الإنترنت على العالم .

ويعد التفتيش إجراء من إجراءات التحقيق الابتدائي التي تمس حقوق و حريات الأفراد، لذا حرص المشرع على إسنادها لجهة قضائية تكفل تلك الحقوق و الحريات، وتتمثل هذه الجهة القضائية في قاضي التحقيق أو النيابة العامة بإختلاف التشريعات كسلطة أصلية، أو استثناء في رجال الضبط القضائي.

وقد منح قانون الإجراءات الجزائية صلاحية إصدار الإذن استثناء إلى سلطات أخرى غير السلطات المختصة، ففي حالة وقوع جريمة من نوع الجنائيات أو الجنح و لم يكن قاضي التحقيق المختص موجودا فإن على المسؤول عن التحقيق عندما تقتضي الضرورة إصدار قرار أو إجراء فوري في التحقيق عرض الأمر على أي قاضي في منطقة إختصاص قاضي التحقيق أو أي منطقة قريبة لإتخاذ ما يلزم على أن تعرض الأوراق على قاضي التحقيق المختص في أقرب وقت.<sup>(13)</sup>

ولم يشترط المشرع الجزائري شكلا معيناً لأمر التفتيش، ولكن بالرجوع إلى القواعد الأساسية للتحقيق الابتدائي، فإنه يجب أن تكون الإجراءات مدونة في محاضر وموقعة عليها من القاضي .

ومن المتعارف عليه في معظم التشريعات الإجرائية أن حالة التلبس تعتبر إحدى الحالات التي تتسع فيها سلطات الضبطية القضائية، حيث تباشر اختصاصات هي أصلا من اختصاص سلطة التحقيق ومنها تحديدا التفتيش بحثا عن أدلة الجريمة و تحديد فاعلها، سواء تعلق الأمر بتفتيش المساكن أو الأشخاص، ولما كانت الجرائم الماسة بأنظمة الإتصال والمعلوماتية كغيرها من الجرائم يمكن أن تتوفر فيها شروط الجريمة المتلبس بها كان من الجائز إجراء تفتيش شخص المشتبه به وما قد يحمله من حاسوب نقال أو هاتف نقال أو حاسوب صغير أو مسكنه وما يتضمنه من موجودات ومن بينها الحاسوب ومن مظاهر التفتيش في حالة التلبس أن يكون رجل الضبط القضائي في إحدى مقاهي الإنترنت يمارس هوايته في الإبحار عبر شبكة الإنترنت، و يلاحظ وجود شخص آخر يقوم بالإبحار عبر تلك الشبكة

في المواقع الإباحية، ويقوم بطباعة الصور المتواجدة فيها بواسطة طباعة ففي هذه الحالة تحقق شروط التلبس. (14)

### المطلب الثاني: إجراءات التفتيش في الجرائم الماسة بالمعطيات الرقمية.

تعد إجراءات التفتيش و الضبط من إجراءات التحقيق التي تختص بها سلطة التحقيق و يناط لضابط الشرط القضائية القيام بهما في حالات إستثنائية و يعتبر التفتيش وسيلة للحصول من خلاله على أدلة في بيان و ظهور الحقيقة، و لا يكفي في التفتيش مجرد توافر شروطه سواء الموضوعية أو الشكلية، بل يلزم أيضا ضرورة مراعاة حدوده الداخلية و التي يتمثل أهمها في ضرورة التقييد بالغرض من التفتيش أثناء تنفيذه وفقا لما نص عليه قانون الإجراءات الجزائية و الذي يقضي بأن الأصل في التفتيش هو البحث عن الأشياء المتعلقة بالجريمة موضوع التحقيق، و يلاحظ أنه في الحالات التي يجوز فيها لضابط الشرط القضائية القيام بإجراء التفتيش و الضبط فإن مشروعية هذا الإجراء تتوقف على محل ارتكاب الجريمة ومدى تبعيته للمعني عليه (15)

ويعد حضور أشخاص معينين في أثناء إجراء التفتيش من قبل الشخص المكلف بذلك قانونا من الضمانات المهمة التي تكفل إجراءه بشكل صحيح، و يبعد الشك حول إمكانية إخفاء الدليل من قبل القائمين به، و يعد ضمانة للقائم بالتفتيش به، و يقوم المفتش في إطار البحث عن الجرائم الماسة بأنظمة الإتصال والمعلوماتية بمجموعة من الإجراءات منها:

#### 1- إجراءات تفتيش النظام المعلوماتي الخاص بالمتهم:

إذا كان محل ارتكاب الجريمة ينصب على نظام المعلومات الخاص بالمتهم دون لزوم التدخل في نظام معلوماتي لشخص آخر، و في هذا الفرض إذا كانت الشروط الإجرائية للتفتيش صحيحة وفقا لما نص عليه القانون فإن التفتيش و ما يسفر عنه من ضبط أي من الأدلة، سواء أكانت هذه الأدلة هي أجهزة الكمبيوتر أم أحد الوسائط المتعددة، يكون مشروعاً، وهذا الحال يكثر في جرائم التزوير و التزييف حيث يتم التفتيش و ملحقاته من

طباعات ملونة أو أجهزة ماسح ضوئي، و يتم نقل البرنامج الداخلي الذي يوجد عن طريق إتمام عملية التزوير أو التزييف في أي من الوسائط المتعددة و بذلك يتم الحصول على دليل ارتكاب الجريمة، وهذا ما يتم أيضا في الجرائم النسخ و التقليد حيث يتم ضبط الوسائط المتعددة المحملة بالبرنامج المنسوخة و الأجهزة المستخدمة في ذلك<sup>(16)</sup>

## 2- إجراءات تفتيش في نظام معلوماتي غير خاص بالمتهم:

يظهر هذا الفرض في الجرائم التي ترتكب باستخدام الشبكات بحيث يتم ارتكاب الجريمة من أي جهاز من أجهزة الحاسبات الآلية الأخرى المتصلة بالحاسب الذي ارتكبت في نظامه المعلوماتي الجريمة و في هذا الفرض فإن إجراءات التفتيش و الضبط تتطلب الدخول في نظام معلوماتي لشخص آخر. ويلاحظ أن قانون الإجراءات الجزائية نص على أنه لا يجوز لرجال الشرطة القضائية الدخول في أي محل مسكون إلا في الأحوال المبينة في القانون، أو في حالة طلب المساعدة من الداخل..... وهو ما دعا المشرع إلى مد تلك الحماية إلى المحل الخاص بحيث أقر له ذات الحماية الخاصة بالمسكن و كذلك السيارة الخاصة إذا كانت توجد في مسكن المتهم، أما إذا وجدت في الطريق العام فلها نفس حرمة الشخص بحيث لا يجوز تفتيشها إلا إذا جاز تفتيش الشخص قانونا.

## 3- تطبيقات في إجراءات تفتيش نظم الحاسبات الآلية الخاصة بالأشخاص :

طبقا لمعيار الخصوصية التي يحميها المشرع يتبين أنه قد تناول المسكن و السيارة والمحل و كل ما يتعلق بالشخص و يمثل خصوصياته، و لذلك فإن نضام المعلومات وما يحويه من خصوصيات للأشخاص تخضع أيضا و بالتبعية لمعيار الخصوصية من حيث عدم جواز التدخل فيها بدون إذن من وكيل الجمهورية.<sup>(17)</sup>

ورغم أن المشرع و في جل القوانين التي نصها حاول حماية خصوصية الأفراد بما فيها البيانات و المعلومات الشخصية و كذلك السجلات و الدفاتر أو الحاسبات الآلية والملحقات السرية بعدم جواز الإطلاع عليها أو الحصول على بياناتها إلا في الأحوال التي نص عليها القانون، وهذا ما أكده أيضا بامتداد الحق في التفتيش إلى سجلات البيانات التي

تكون في موقع إلكتروني آخر عندما يكون التخزين الفعلي خارج المكان الذي يتم فيه التفتيش.

و كذلك ذهب جانب آخر من الفقه بأن البيانات لها طابع مادي على أساس أنها نبضات أوذبذبات إلكترونية و إرشادات أو موجات كهرومغناطيسية قابلة لأن تسجل وتخزين على وسائط متعددة و يمكن قياسها<sup>(18)</sup>.

و لأن البحث عن الدليل على ارتكاب الجريمة، من حيث كونه وسيلة للإثبات ومحلا للإقتناع وفقا لنظرية الإثبات الجنائي يتطلب الإقرار بإمكانية أن تكون المعلومات محلا للتفتيش و ضبط الأدلة المتحصل عليها، يلاحظ أن الأمر يختلف من حيث صدور إذن بالتفتيش في النظام المعلوماتي لأحد الأشخاص عنه في الإذن بالتفتيش في الجرائم التقليدية الأخرى، لأن الإذن قد يصدر في حق شخص ارتكب جناية أو جنحة و قامت قرائن قوية على ارتكابه للجريمة و عند القيام بتنفيذ إذن التفتيش، فإن الأمر قد يقتضي امتداد حق التفتيش إلى نظام معلوماتي آخر إما تابع للمتهم، أو أن للمتهم أكثر من جهاز في أماكن مختلفة كأن يكون المتهم مالكا لجهاز في منزله و جهاز آخر في عمله، أو أن يكون الشخص له شريك في الأجهزة مما يتطلب الحصول على إذن آخر من وكيل الجمهورية.

و يتم ذلك عن طريق تحديد مجال هذا التفتيش وما يستتبعه بالضرورة من تتبع لشبكات المعلومات، و يخضع ذلك للسلطة التقديرية للقاضي من حيث توافر حالة الضرورة أو عدم توافرها، و هذا النظام إتبعته بعض الدول مثل الولايات المتحدة الأمريكية و كندا، حيث نصتا على أن يكون إذن التفتيش متضمنا ما يلي:

- البحث عن أدلة محصلة من كيان الحساب المنطقي و التي يدخل فيها برامج التطبيق ونظم التشغيل.

- البيانات المستخدمة بواسطة برنامج الكمبيوتر أو كيانه المنطقي.

- السجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات<sup>(19)</sup>.

- السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات.

#### 4- التعاون الدولي في مواجهة امتداد إجراءات التفتيش والضبط خارج حدود الدولة:

يعد التفتيش بوصفه إجراء تحقيقيا تنص عليه التشريعات لأن فيه مساسا بحرية الأفراد و حرية أماكنهم و التي تكفل القانون بحمايتها من أي انتهاك، فالتفتيش يشكل انتهاكا قانونيا لهذه الحرية و الجريمة التي كفلها المشرع و ذلك بهدف تحقيق مصلحة أهم و أعم من مصلحة الأفراد و هي المصلحة العليا للمجتمع، التي تتمثل في كشف الحقيقة في جريمة وقعت، حيث أنه بهدف إيصال الجاني إلى العدالة قد تستدعي مصلحة التحقيق اتخاذ هذا الإجراء للحصول على الأدلة التي تفيد في كشف الجريمة(20).

ولكون الجرائم الماسة بأنظمة الإتصال والمعلوماتية ظاهرة مستحدثة على الساحة الإجرامية داخل الجزائر لم ينص قانون العقوبات عليها صراحة بل ذكرها في القسم السابع مكرر 03 تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وبين كذلك أن تعقب مرتكب الجريمة و تتبع آثاره و ضبط الأدلة المعلوماتية الدالة على ارتكابه للجريمة قد لا يتقيد بحدود الدولة وإنما يمتد إلى خارجها و هذا مرجعه إلى قوة إنتشار شبكات الإنترنت التي ربطت جميع الدول ببعضها البعض و أصبح لا يحدّها فاصل.

وأمام هذا التطور التكنولوجي بات ارتكاب الجرائم من دولة إلى أخرى من السهولة بمكان، و لذلك أصبح من ضروري البحث في مشروعية القيام بإجراء التفتيش و الضبط من قبل من الضبطية القضائية لمتهم في دولة أخرى، و تعرف الجريمة بهذا الوصف بالجريمة المنظمة نتيجة مزاولة الأنشطة الإجرامية عبر حدود الدول، مما دعا الدول لإقرار أن الجريمة المنظمة هي في حقيقتها جريمة داخلية مضافا إليها البعد الدولي، أي بارتكابها خارج حدود الدولة و حدوث النتيجة في الداخل(21).

و إذا كان الإختصاص بنظر تلك الجرائم ينعقد للإختصاص المكاني للدولة التي ارتكبت الجريمة على أرضها تبعا لمبدأ السيادة الدولة، فإن للضبطية القضائية القيام بإجراء التفتيش و الضبط على أرضها، ومن هنا يثور البحث في حالة امتداد إجراءات التفتيش والضبط خارج حدود الدولة و الدخول في سيادة دولة أخرى.



ومن هنا يثور البحث في حالة امتداد إجراءات التفتيش و الضبط خارج حدود الدولة و الدخول في سيادة دولة أخرى، لذلك فإن الدولة حرصا منها على مراعاة مصلحتين هامتين هما احترام الخصوصية للأشخاص ومواجهة الجرائم المرتكبة لتحقيق الصالح العام أبرمت العديد من الإتفاقيات الدولية لمكافحة هذه الظاهرة، هذا إلى جانب الضمانات التي أقرتها المواثيق الدولية في هذا الإطار<sup>(22)</sup>.

### الخاتمة:

إن تنامي ظاهرة الجرائم المعلوماتية، وتخطي آثارها حدود الدول، أفرز جملة من التحديات القانونية على الصعيد الإجرائي تجسدت في المقام الأول في بعض الصعوبات التي تكتنف عملية التحقيق وإثبات هذه الجرائم وقبول الدليل بشأها باعتبارها لا تترك أثراً مادياً ملموساً، كما هو الحال في الجرائم التقليدية .

فضلاً عما يثيره ذلك من عقبات تواجه الأجهزة القضائية والأمنية في سبيل مباشرة بعض إجراءات التحقيق كالمعينة والتفتيش والضبط في نطاق البيئة الافتراضية،.

ورغم الجهود التي بذلت ولا تزال تبذل، فإن هذه التحديات تبقى عضية على الحل في كثير من الأحيان في غياب استراتيجية واضحة للتعامل مع هذه الطائفة من الجرائم ومرتكبيها .

وبناءً على ما تقدم، توصلنا إلى بعض التوصيات التي نراها قد تسهم في حل بعض الإشكاليات المتعلقة بمسألة التحقيق، ومنها :

1. ضرورة مراجعة وتطوير القوانين القائمة وإصدار المزيد من القوانين لتقوية الترسانة القانونية في مجال التحقيق والتفتيش، وعدم الاقتصار على القوانين التي تم سنها لمواجهة بعض الصعوبات الطارئة المتعلقة بالأنشطة الماسة بنظم المعالجة الآلية للمعطيات والإعتداءات الإرهابية التي تستخدم هذه الأنظمة .

2. الإهتمام بالتأهيل المناسب لكوادر الأجهزة القضائية بما يجعلها قادرة على التعامل مع هذه الجرائم بكفاءة واقتدار .

3. العمل على استحداث ضبطينة قضائية متخصصة في مجال الجرائم المعلوماتية أسوة بالدول المتقدمة.
4. إعادة النظر في مقررات كليات الشرطة ومعاهد القضاء وكليات القانون بحيث يفرد مقرر مستقل للجرائم المعلوماتية .

#### الهوامش:

1. أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيايات الإعلام والاتصال في ضوء القانون رقم 04-09، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة ورقلة، السنة الجامعية 2012-2013، ص66.
2. موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مقال مقدم إلى المؤتمر المغربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص02.
3. المادة 11 من القانون رقم 04-09، المؤرخ في 05 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيايات الإعلام والإتصال.
4. المادة 02 فقرة د من القانون رقم 04-09.
5. فقد عرف المشرع الأمريكي مراقبة الإتصالات الإلكترونية بأنها: عملية الإستماع لمحتويات أسلاك أو أي إتصالات شفوية عن طريق إستخدام جهاز إلكتروني أو جهاز آخر، المادة 2510 الفقرة الرابعة من قانون الإتصالات الفدرالي الأمريكي لسنة 1968، وطبقا لقانون الإتصالات الإلكترونية لسنة 1986 أصبح التعريف المذكور يتسع ليشمل الإتصالات الإلكترونية الأخرى.
6. خيرت علي محرز، خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، 2012، ص81.
7. خالد ممدوح إبراهيم، خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الاللكترونية، دار الفكر الجامعي، الإسكندرية، 2010، ص108.
8. أنظر المادة 47 من الأمر رقم 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية قانون الإجراءات الجزائية الجزائري المعدل والمتمم.
9. أنظر المادة 47 من قانون الإجراءات الجزائية.

10. نبيلة هبة هروال، نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2007، ص 262
11. أنظر المادة 23 من قانون الإجراءات الجزائية الجزائري.
12. قدرې عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري و المقارن، منشأة المعارف، الإسكندرية، 2005، ص 111
13. سعيد حسب الله عبد الله، شرح قانون أصول المحاكمات الجزائية، دارين الأثير للطباعة، الموصل، 1998، ص 177
14. نبيلة هبة هروال، المرجع السابق، ص 248
15. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية المرجع السابق، ص 228
16. خالد ممدوح إبراهيم، المرجع نفسه، ص 229
17. خالد ممدوح إبراهيم، المرجع نفسه، ص 230
18. خالد ممدوح إبراهيم، المرجع السابق، ص 331
19. خالد ممدوح إبراهيم، المرجع السابق، ص 232
20. سامي جلال فقي حسين، سامي جلال فقي، التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار الكتب القانونية، مصر، 2011، ص 09
21. خالد ممدوح إبراهيم، المرجع السابق، ص 234
22. خالد ممدوح إبراهيم، المرجع السابق، ص 235.