

تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري

يزيد بوحليط

كلية الحقوق والعلوم السياسية

جامعة باجي مختار-عناينة

ملخص

حققت الثورة التكنولوجية قفزة هائلة في مجال تقنية المعلومات، وبالمقابل أدى سوء استخدامها إلى ظهور جرائم مستحدثة عرفت بالجرائم المعلوماتية، مما صعب من مكافحتها نظرا لطبيعتها وخصوصية إجراءات التحقيق فيها، عبر هذه البيئة الافتراضية لتعقب المجرم المعلوماتي. في هذا الصدد، يتضمن نص القانون رقم: 04-09 المؤرخ في: 05 أوت 2009 القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على جملة من القواعد الإجرائية المتعلقة بتفتيش المنظومة المعلوماتية وحجز المعطيات. لكن تبقى هذه الإجراءات مقصورة في الكشف عن هذه الجرائم أمام التطورات التقنية المذهلة في مجال المعلوماتية، مما يستوجب مراجعتها بما يتماشى وهذا التطور.

الكلمات المفتاحية: منظومة معلوماتية، معطيات معلوماتية، معالجة آلية للمعطيات، تفتيش.

*Perquisition du système informatique et saisie des données dans la législation algérienne***Résumé**

La révolution technologique a fait un saut considérable dans la technologie de l'information. En contrepartie, l'utilisation abusive de cette technologie a fait apparaître un nouveau genre de crime dit "la cyber criminalité". Cela a engendré des difficultés pour la combattre, vu sa nature et la spécificité des procédures investigatrices afin de poursuivre "le criminel informatique", dans cet environnement virtuel. Dans ce contexte, la loi n°09-04 du 05 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication, a édicté un ensemble de règles procédurales concernant l'inspection du système informatique, et la saisie de ses données. Mais cela reste insuffisant devant l'hallucinant progrès technique dans le domaine de l'informatique, d'où la nécessité de revoir ces règles, et les adapter selon l'évaluation de cette technologie.

Mots-clés: Système informatique, données informatiques, traitement automatisés des données, perquisition.

*Search of the information system and data entry in the Algerian legislation***Abstract**

The Progressing technological revolution has realized a huge area of information, In return, negative effects has esmerged among them is "cybercrimes", which creates enorunus difficulties, that are hard to fight them by all means. For this purpose, the law n°, 09-04 of August 05 Th 2009 includes special rules relating to the search of the information system and data entry. But, in spite of that, legal texts remain insufficient to detect the crimes. This is time to be reviewed and updated with this revolution.

Key words: Information system, computer data, automated data processing, search.

مقدمة

عرف القرن العشرون تطورا مذهلا في مجال تكنولوجيات الإعلام والاتصال، حيث انتشرت الحواسيب وأضحت حاجة أساسية في إدارة الشؤون العامة والخاصة، وشكلت شبكة الإنترنت أعجوبة القرن الحالي فأصبحت وسيلة التعامل اليومي مما أفرز أنماطا مستحدثة من الجرائم لم يكن للبشرية سابق عهد بها. فهي معقدة في طرق ارتكابها ووسائل كشفها. كما تشكل هاجسا أمنيا للأفراد والدول على حد سواء، مستغلة في ذلك أحدث التكنولوجيات في مجال تقنيات الحوسبة والاتصال تعرف بالجرائم المعلوماتية (Cybercrimes) فهي جرائم يصعب حصرها، وتستهدف الاعتداء على البيانات والمعلومات والبرامج ونظم التشغيل والأنظمة المعلوماتية، وشبكات الاتصال وقواعد البيانات⁽¹⁾، مما يتطلب ضرورة توفير وسائل حديثة وإجراءات خاصة للجهات القضائية لمحاربة هذه النوع من الجرائم.

في هذا الشأن، يعتبر إجراء التفتيش وفقا للضوابط التقليدية "عملية بحث في مستودع السر عن أدلة الجريمة وكل ما يفيد في كشف الحقيقة"⁽²⁾. لكن يثور التساؤل حينما نكون أمام إجراء التفتيش والحجز في مجال الجرائم المرتكبة على منظومة معلوماتية تخزن بيانات ومعلومات معالجة إلكترونيا. فحينما ينصب التفتيش على الكيان المادي للحاسوب (Hardware) وهي الأشياء الملموسة من أجزائه التي تعمل بشكل متكامل لأداء مهمة في معالجة البيانات آليا لا مشكلة في ذلك، إذ يمكن ضبطها وحجزها وفقا للقواعد التقليدية للتفتيش، ولكن تبرز الصعوبة حينما نكون بصدد تفتيش وحجز المكونات المعنوية أو المنطقية للحاسوب (Software) كالبرامج والمنظومات المعلوماتية وقواعد البيانات... إلخ، من هنا تكمن أهمية الموضوع، وهذا ما عالجه المشرع الجزائري بموجب نصوص القانون رقم: 09-04 الصادر في: 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها⁽³⁾. كما عزز هذا الاتجاه بالتصديق بتاريخ: 08 سبتمبر 2014 على نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ: 21 ديسمبر 2010⁽⁴⁾.

وعليه يمكن طرح الإشكالية الآتية: ما هي القواعد الإجرائية الخاصة التي أقرها المشرع الجزائري في مجال تفتيش المنظومة المعلوماتية وحجز المعطيات؟ وهل تعتبر كافية لمكافحة هذا النوع المستحدث من الجرائم الذي يتم في بيئة افتراضية تخلق صعوبات جمة؟ للإجابة على هذه الإشكالية قسمنا موضوعنا الى مبحثين نتناول في المبحث الأول: تفتيش المنظومة المعلوماتية والجهة القضائية المختصة بذلك. أما في المبحث الثاني فننتطرق فيه لإجراء تمديد التفتيش إلى منظومات معلوماتية تقع داخل إقليم الوطن أو خارجه إضافة الى حجز المعطيات المعلوماتية، لنخلص في الأخير إلى وضع خاتمة تتضمن النتائج والاقتراحات.

المبحث الأول: تفتيش المنظومة المعلوماتية والجهة المختصة بذلك:

يعتبر التفتيش من أخطر الحقوق التي منحت للمحقق، وذلك لمساسها بالحقوق المكفولة دستوريا لذا يحيطها المشرع بجملة من الضوابط تكون ضمانا للحرية الفردية أو حرمة المسكن⁽⁵⁾. سنتطرق إلى ماهية التفتيش في (المطلب الأول) ثم إلى تفتيش المنظومة المعلوماتية والجهة القضائية المختصة بذلك في (المطلب الثاني).

المطلب الأول: ماهية التفتيش: تحولت الجريمة المعلوماتية إلى ظاهرة عالمية يصعب معها الكشف عن مرتكبيها نظرا لطبيعتها الخاصة واستخدامها لأحدث تكنولوجيات الكمبيوتر والأنظمة المعلوماتية، مما يتطلب ضرورة

توفير وسائل وإجراءات حديثة للجهات القضائية المختصة لمحاربة هذه النوع من الجرائم خاصة ما تعلق بإجراء التفتيش الذي يهدف إلى استخراج أدلة معلوماتية من نظام حاسوبي⁽⁶⁾. وعموما يمكن تعريف جرائم نظم المعلومات على أنها: "السلوك السيئ المتعمد الذي يستخدم نظم المعلومات لإتلاف المعلومات أو إساءة استخدامها"⁽⁷⁾. فما المقصود بالتفتيش؟ وما هي خصوصية هذا الإجراء، حينما نكون بصدد تفتيش المنظومة المعلوماتية؟.

أولاً: تعريف التفتيش: لم يضع المشرع الجزائري تعريفاً للتفتيش. فقد اعتبره إجراء من إجراءات التحقيق الهدف منه الحصول على الأدلة لإثبات الجريمة للوصول للجاني، لكن بالمقابل أحاطه بجملة من الضوابط الصارمة لما يترتب عنه من مساس بحرية الأشخاص وكرامتهم وحرمة ممتلكاتهم⁽⁸⁾، فلقد نصت المادة 40 من الدستور الجزائري لسنة 1996: "تضمن الدولة عدم انتهاك حرمة المسكن. فلا تفتيش إلا بمقتضى القانون. وفي إطار احترامه. ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة"⁽⁹⁾. كما نص عليه المشرع في المواد من 44 إلى 47 والمادة 64 إضافة إلى المادة 79 وما بعدها من قانون الإجراءات الجزائية⁽¹⁰⁾. ونظرا لخطورة هذا الإجراء تكفل الفقه بمحاولة إعطاء تعريفات للتفتيش منها أنه: "إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه"⁽¹¹⁾، أو هو: "تفتيش شخص المتهم للبحث معه في مستودع سره عن أشياء تفيد في الكشف عن الجريمة و نسبتها إلى المتهم"⁽¹²⁾ كما عرف المجلس الأوروبي هذا النوع من التفتيش المتعلق بمكافحة الجرائم المعلوماتية بأنه: "إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني"⁽¹³⁾. يقودنا هذا للحديث عن خصوصية التفتيش الواقع على المنظومة المعلوماتية، فماذا نعني به؟

ثانياً: خصوصية التفتيش الواقع على المنظومة المعلوماتية: قد يتطلب التحقيق تفتيش شخص المتهم أو منزله قصد ضبط الأشياء المحصلة من الجريمة وبالتالي فإجراء التفتيش هو أصلاً من اختصاص سلطة التحقيق، يهتم بالبحث في مستودع السر عن أدلة الجريمة⁽¹⁴⁾. فالتفتيش المنصب على الكيان المادي للحاسوب لا يمثل مشكلة، إذ يتم تطبيقه وفقاً للضوابط التقليدية. لكن يثور التساؤل حينما نكون بصدد تفتيش المكونات المعنوية (المنطقية) للحاسوب بكل مكوناته خاصة ما تعلق بالمنظومات المعلوماتية. فما المقصود بالمكونات المادية والمعنوية للحاسوب؟

أ- المكونات المادية للحاسوب (Hardware): يقصد بالمكونات المادية للحاسوب: "الأشياء الملموسة من أجزائه و أدواته التي تعمل بشكل متكامل لأداء مهمة في معالجة البيانات آلياً"⁽¹⁵⁾، وعليه يتكون الحاسوب من عدة وحدات مثل وحدات الإدخال كلوحة المفاتيح والقلم الضوئي وشاشات اللمس، ووحدة الذاكرة الرئيسية التي تستخدم في الحفظ الدائم أو المؤقت للبيانات والبرامج، إضافة إلى وحدة المعالجة المركزية التي تقوم بالتنسيق بين الوحدات الأخرى وضبط التعليمات. وأخيراً وسائط إظهار نتائج التشغيل كالشاشة والطابعة والسماعات والراسم والأقراص المرنة والصلبة والذاكرة الوميضية التي تعتبر من أشهر تخزين البيانات والمحافظة عليها⁽¹⁶⁾. وعليه ليس هناك خلاف في أن الدخول إلى المكونات المادية للحاسوب بحثاً عن دليل الجريمة يخضع للإجراءات التقليدية للتفتيش كتحديد طبيعة المكان الموجودة فيه تلك المكونات سواء كان عاماً أو خاصاً إضافة إلى حضور المعني أو من ينوب عنه.

ب- المكونات المعنوية للحاسوب (Software): يطلق أيضا على المكونات المعنوية للحاسوب بالبرمجيات، فهي بمثابة عصب عمل الكمبيوتر إذ توفر إمكانيات وسرعة فائقة في إنجاز المهام المطلوبة. كما يعرف الكيان المنطقي للحاسوب لغة بأنه كلمة تستخدم للدلالة على جميع المكونات غير المادية لنظام الحاسوب كنظم التشغيل و برامج التطبيقات. كما عرف التوجيه الأوروبي الصادر في 14 ماي 1991 برامج الحاسب الآلي بأنها: "مجموعة من الأوامر التي تؤدي إلى إنجاز المهام المستهدفة من خلال نظام معالجة المعلومات، ويطلق عليه اسم الحاسب"⁽¹⁷⁾ كما يمكن تقسيم برامج الحاسوب إلى نوعين: يسمى الأول برامج النظام (System Programs) الذي دونه لا يمكن استغلال الحاسوب، والثاني برامج التطبيقات (Application Programs) التي تقوم بمهام محددة، مثل برامج معالجة النصوص، أو برامج توجه لخدمة وظيفة معينة كبرامج إدارة الموارد البشرية... إلخ⁽¹⁸⁾.

وعليه فإجراء التفتيش على المكونات المنطقية للحاسوب، ومنها تفتيش المنظومة المعلوماتية سواء كانت في حاسوب واحد، أو مرتبطة عن طريق شبكة اتصال سلكي أو لاسلكي كالإنترنت مثلا بمنظومة معلوماتية أخرى تتواجد في حاسوب آخر داخل الإقليم الوطني أو خارجه -كما سنرى لاحقا- سيكون من الصعوبة بمكان، نظرا للطبيعة المعنوية الخاصة لهذه المعطيات المخزنة إلكترونيا ناهيك على أنها تتم في بيئة افتراضية يتطلب الكشف عنها وسائل تقنية وبشرية خاصة، إذ يتطلب مثلا الكشف عن الرقم السري أو الكود (Code)، أو كلمة السر (Password)⁽¹⁹⁾، أو نظام التشفير أو ترميز البيانات للولوج إلى مختلف الملفات لتقديمها دليلا ضد المتهم.

المطلب الثاني: تفتيش المنظومة المعلوماتية والجهة المختصة بذلك:

تكمّن وظيفة نظم المعلومات في معالجة واسترجاع وتخزين ونشر المعلومات سواء داخل منظومة معلوماتية واحدة أو متصلة بأخرى، وسواء داخل الإقليم الوطني أو خارجه. فما المقصود بتفتيش المنظومة المعلوماتية؟ وما هي الجهة القضائية المختصة بذلك؟

أولا: تفتيش المنظومة المعلوماتية: إن تقاوم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، تتطلب تدخلا تشريعا صريحا سواء على المستوى الدولي أو الداخلي، حيث تضمنت الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت في: 08/11/2001 من طرف المجلس الأوروبي مختلف أشكال الإجرام المعلوماتي⁽²⁰⁾. كما قام المشرع الجزائري ولنفس السبب بتعديل قانون العقوبات بإضافة قسم سابع مكرر عنوانه: "المساس بأنظمة المعالجة الآلية للمعطيات" بموجب القانون رقم: 04-15 المؤرخ في: 10/11/2004⁽²¹⁾، حيث يهدف المشرع الى حماية نظام المعالجة الآلية للمعطيات الذي يخضع لتطورات متلاحقة في مجال صناعة الكمبيوتر وملحقاته وبرامجه⁽²²⁾ حيث عرفت المادة 2 الفقرة 2 من القانون رقم: 09-04 مؤرخ في: 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المنظومة المعلوماتية: "أي نظام منفصل أو مجموعة من الأنظمة المتصل أو المرتبط بعضها ببعض؛ يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين" مترجما بذلك نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 2 الفقرة 5 التي عرفت النظام المعلوماتي على أنه: "مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات"⁽²³⁾، كما عرفت الاتفاقية الدولية للإجرام المعلوماتي النظام المعلوماتي على أنه:

«Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données»⁽²⁴⁾.

وفي تعريف آخر بأنه: "مجموعة من الإجراءات التي يتم من خلالها تجميع واسترجاع أو تشغيل وتخزين ونشر المعلومات بغرض دعم عمليات صنع القرار وتحقيق الرقابة داخل الجهة الإدارية أو أيا كان شكل تلك المنظمة"⁽²⁵⁾. كما عُرِف أيضا النظام المعلوماتي على أنه: "جهاز يتكون من مكونات مادية ومكونات منطقية وذلك بغرض المعالجة الآلية للبيانات الرقمية، وهو يشتمل على وسائل الإدخال والإخراج وتخزين البيانات"⁽²⁶⁾. وهذا الجهاز قد يكون منفردا أو متصلا بمجموعة من الأجهزة المماثلة عن طريق شبكة، وعليه تقوم المنظومة المعلوماتية على وجود نظام تشغيل حاسوبي سواء كان منفصلا أو متصلا سلكيا أو لا سلكيا يقوم واحد منها بالمعالجة الآلية للمعطيات تنفيذا لبرنامج معين، حيث نجد أن التعريفات المختلفة لنظم المعلوماتية تطابقت مع تعريف المشرع الجزائري مما يمكن من تحديد أدق للعناصر المكونة للجريمة الواقعة على الأنظمة المعلوماتية.

هناك صعوبات جمة يصادفها رجال الضبطية القضائية والمحققين في ضبط الجرائم المعلوماتية بسبب طبيعتها الخاصة، فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود⁽²⁷⁾. غير أن المشرع الجزائري خرج عن هذا المبدأ واستبق الأحداث، فجعل من إجراء التفتيش مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة المعلوماتية، من خلال القيام بعمليات المراقبة المسبقة وفق نص المادة 03 من القانون 04-09 السالف الذكر: "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 الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية"، كما نصت المادة 04 الفقرة 02 من نفس القانون على أنه: "في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني..⁽²⁸⁾. وعليه تسمح هذه الإجراءات بتسهيل مكافحة الجرائم المعلوماتية.

إن الهدف من التفتيش المنصب على المنظومة المعلوماتية هو منع المجرم المعلوماتي من تدمير أو إخفاء الدليل للإفلات من العقوبة، وذلك بموجب نصوص القانون 04-09 السالف الذكر وتطبيقا لنصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات خاصة المادتين 26 و 27 المتعلقةتين بتفتيش المعلومات المخزنة وضبطها⁽²⁹⁾. لذا أدرج المشرع إجراء التفتيش في مجال الجرائم المعلوماتية في قانون الإجراءات الجزائية. فالتفتيش في هذه الحالة يختلف عن التفتيش العادي. فهو يتوقف أساسا على طبيعة المكان الذي يحتوي على أجهزة الكمبيوتر ومكوناته وفيما إذا كان خاصا أو عاما ناهيك عن تحديد الإقليم إذا كان وطنيا أو أجنبيا، فلقد نصت المادة 5 من القانون رقم: 04-09 السابق ذكره على أنه: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه، الدخول بغرض التفتيش ولو عن بعد إلى:

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

ب- منظومة تخزين معلوماتية..."

من خلال هذه المادة أجاز المشرع الدخول بغرض التفتيش ولو عن بعد إلى المنظومة المعلوماتية دون إذن صاحبها، وهذا برغم اعتبار برامج الحاسوب من بين المصنفات الأدبية المحمية بموجب مجموعة من النصوص الخاصة⁽³⁰⁾. كما رأينا سالفاً يتبين بوضوح أن التفتيش إذا تعلق بالمكونات المادية للحاسوب لا مشكلة في ذلك ويتم وفقاً لأحكام المادة 44 من قانون الإجراءات الجزائية⁽³¹⁾، وعليه يجب الانتقال إلى مكان تواجد الحاسوب أو أحد مكوناته المادية مثل الأقراص الصلبة والمرنة، فمن السهولة هنا ضبط جهاز الحاسوب ومكوناته وملحقاته وحجزها وتقديمها كدليل لإدانة المتهم، لكننا هنا بصدد التفتيش الذي يستهدف الكيان المنطقي للحاسوب وسواء استهدف المنظومة المعلوماتية كلها أو جزءاً منها، أو منظومة تخزين معلوماتية⁽³²⁾. فالتفتيش في كلتا الحالتين يستهدف في مفهومه أشياء غير مادية.

ونظراً لما تتطلبه العملية من جانب تقني معقد أجاز المشرع نسخ وإفراغ المعطيات على دعامة تخزين إلكترونية تكون قابلة للحجز مثل الأقراص المرنة والأقراص المضغوطة والذاكرة الوضعية... إلخ وهذا بموجب نص المادة 6 من القانون 04-09: "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 لفهما على دعامة تخزين إلكترونية تكون قابلة للوضع والحجز في أحرار وفقاً للقواعد المقررة في قانون الإجراءات الجزائية..." مع إمكانية الاستعانة بكل شخص له دراية بعمل المنظومة المعلوماتية محل البحث. كما ينبغي أن تتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية سواء بوصفه فاعلاً أو شريكاً فيها⁽³³⁾.

ثانياً: الجهة القضائية المختصة:

بالرجوع إلى نص المادة 4 الفقرة أ من القانون رقم: 04-09 السالف الذكر التي تبين كيفية المراقبة للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، يبين لنا المشرع الجهة القضائية المختصة بهذه الحالة في نفس المادة الفقرة الأخيرة، إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المنصوص عليها بموجب المادة 13 من نفس القانون إننا لمدة ستة أشهر قابلة للتجديد، وذلك على أساس طبيعة ونوعية الترتيبات التقنية المراد أخذها⁽³⁴⁾. فيما عدا هذه الحالة الخاصة وبموجب نص المادة 05 من القانون 04-09 التي تنص على أنه: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش..." إذ يتعين الرجوع إلى التدابير التي نص عليها قانون الإجراءات الجزائية في مجال التحري والتفتيش بالنسبة للجرائم الإلكترونية، وبالضرورة في مجال الاختصاص بالنسبة لوكيل الجمهورية وقاضي التحقيق الذي يحدده المرسوم التنفيذي رقم: 06-348 المؤرخ في: 05/10/2006 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق⁽³⁵⁾ وباعتبارهما أيضاً الجهة المؤهلة بمنح الإذن بالتفتيش وفقاً للشروط المنصوص عليها بموجب نص المادة 44 من قانون الإجراءات الجزائية. وفي نفس الصدد أشارت المادتان 37 و40 من قانون الإجراءات الجزائية بتمديد الاختصاص لكل من وكيل الجمهورية وقاضي التحقيق في جرائم معينة من بينها الجرائم الماسة بالمعالجة الآلية للمعطيات.

وعليه يمكن القول بأن المشرع الجزائري حدد بوضوح الجهة القضائية المختصة سواء في مجال الإذن بوضع ترتيبات للمراقبة الالكترونية للحيلولة دون الاعتداء على منظومة معلوماتية، أو في مجال الدخول بغرض التفتيش ولو عن بعد لمنظومة معلوماتية أو جزء منها أو منظومة تخزين معلوماتية سواء تقع داخل الإقليم الوطني أو خارجه، فكيف يتم ذلك؟

المبحث الثاني: تمديد التفتيش وحجز المعطيات المعلوماتية:

تعرّف الشبكة العنكبوتية العالمية بأنها "الوسيلة التواصلية بين الشبكات المعلوماتية دون ما اعتبار للحدود الوطنية"⁽³⁶⁾. إذ يشكل هذا مكانا خصبا للجرائم المعلوماتية، فماذا نعني بتمديد التفتيش؟ وكيف يتم حجز المعطيات المعلوماتية؟

أولاً: تمديد التفتيش إلى منظومة معلوماتية أو جزء منها:

نظرا لخطورة هذه الجريمة المستحدثة، ويقصد ملاحقة المجرم المعلوماتي، نص المشرع على تمديد إجراء التفتيش سواء داخل الإقليم الوطني أو خارجه. سنوضح هذا فيما يأتي:

أ- تمديد التفتيش داخل الإقليم الوطني:

أدى سوء استخدام الفضاء السبراني (cyberspace)⁽³⁷⁾، إلى بروز جرائم مستحدثة تسمى بالجرائم المعلوماتية (Cybercrimes)، إذ يمكن للمجرم الدخول والانتقال من منظومة معلوماتية لأخرى بما يسمح له بتغيير أو تدمير المعطيات ناهيك عن صعوبة تتبعه وإيجاد دليل ضده. لذا نص المشرع الجزائري في المادة 5 من القانون 09-04 على أنه: "يجوز للسلطات القضائية المختصة... 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 السلطات القضائية المختصة مسبقا... فتمديد التفتيش إلى منظومة معلوماتية أخرى مشكوك فيها يتطلب إجراءات خاصة، فهو يتم عن بعد وبشكل سريع تماشيا مع السرعة الهائلة في نقل المعلومات وأيضا متى توفر الشك في وجود معطيات مبحوث عنها مخزنة في منظومة معلوماتية أخرى. ولكن يتم الوصول إليها عن طريق الدخول من منظومة معلوماتية أولى. كما نؤكد أن هذه الإجراءات تكتسي طابع الرسمية. وبذلك حاول المشرع غلق منافذ إفلات المجرم في هذا النوع من الجرائم الذي يتسم بالتعقيد والتطور الدائم في استخدام تقنية الحوسبة والاتصال، مما أجاز معه للسلطات المكلفة بالتفتيش تسخير كل شخص مختص في مجال عمل المنظومة المعلوماتية قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهامها.

في هذا الشأن تنص المادة 5 الفقرة الأخيرة من القانون 09-04 السالف الذكر، على أنه: "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"، لذا

يجب على السلطات القضائية المختصة العمل على تكوين وتدريب أعضائها في مجال البحث والتحري عن الجرائم المعلوماتية.

ب- تمديد التفتيش خارج الإقليم وشروط المساعدة القضائية:

تتصف الجرائم المعلوماتية بأنها جرائم عابرة للحدود يمكن للمجرم المعلوماتي من أي مكان في العالم يملك جهاز حاسوب متصل بشبكة الإنترنت الإضرار بمصالح الوطن، كاستهداف أمن الدولة واستقرار مؤسساتها أو الدفاع الوطني أو سلامة الاقتصاد الوطني، في هذا الصدد نصت المادة 15 من القانون 04-09 على أنه: "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائية 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".

وبذلك أقر المشرع إجراءات صارمة لملاحقة هذا النوع من الجرائم خارج الإقليم الوطني وذلك حينما وسع من نطاق التفتيش بموجب نص المادة 05 الفقرة 04 من القانون 04-09: "...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..."، غير أن المشرع الجزائري لم يترك الأمر على إطلاقه، ونظرا لمقتضيات تتعلق بالسيادة الوطنية، وضع شروطا وقيودا للمساعدة القضائية في مجال مكافحة هذا النوع من الجرائم المستحدثة نوضحها كالآتي:

• شروط المساعدة القضائية الدولية:

نصت المادة 16 من القانون 04-09 على أنه: "في إطار التحريات أو التحقيقات القضائية الجارية لمعينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني..."، وتعرف المساعدة القضائية الدولية بأنها: "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"⁽³⁸⁾. ونظرا لحالة الاستعجال والسرعة التي تتطلبها إجراءات التحقيق في مثل هذه الجرائم التي تستعمل التقنيات المتطورة في مجال الحاسوب والانترنت ونظم الاتصالات ولضمان عدم إفلات المجرم المعلوماتي من العقاب نصت المادة 16 الفقرة 02 على قبول طلبات المساعدة القضائية حتى وإن جاءت عن طريق وسائل الاتصال السريعة كالبريد الإلكتروني أو الفاكس بشرط التأكد من صحتها فقط.

بناء على ما سبق وضع المشرع شروطا للمساعدة القضائية طبقا لنصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المادة 04 الفقرة 01 التي تنص على أنه: "تلتزم كل دولة طرف وفقا لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى" وهذا ما ترجمته فحوى المادة 17 من القانون 04-09 المذكور سلفا، حيث تتمثل هذه الشروط أساسا فيما يأتي:

- تكون وفقا للاتفاقيات الدولية المبرمة في مجال مكافحة الجرائم المعلوماتية وما يرتبط بها كتبادل المعلومات وتسليم المجرمين والإنابة القضائية...إلخ.

- خضوعها لمبدأ المعاملة بالمثل الذي يؤكد سيادة الدولة.
- توفر شروط أمن كافية للتأكد من صحة المعلومات الواردة عن طريق وسائل الاتصال الحديثة مثل: البريد الإلكتروني، والفاكس، وعموما ترك المشرع المجال مفتوحا لأي وسيلة اتصال حديثة تظهر مستقبلا.
- القيود الواردة عليها:

قلنا سلفا إن هناك صعوبات تقنية بالغة لملاحقة الجرائم المعلوماتية، مما استوجب اتفاق الدول على ضرورة التنسيق فيما بينها وطلب المساعدة القضائية الدولية بخصوص إجراءات التحقيق والتحري وتسليم المجرمين... إلخ، لكن برغم ذلك وضع المشرع الجزائري قيودا نظرا لحساسية التعامل في المعلومات وقواعد البيانات وما تشكله من خطر على أمن الأشخاص والدول على حد سواء في حالة إساءة استغلالها. لذا نصت المادة 18 من القانون 04-09 على أنه: "يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام يمكن أن تكون الاستجابة لطلبات المساعدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب". فحسب هذه المادة وضع المشرع احتمالين هما:

أ: يمكن رفض تنفيذ طلبات المساعدة القضائية إذا كانت تمس أولا بالسيادة الوطنية وما تثيره هذه المسألة من حساسية بين الدول، وثانيا بالنظام العام والآداب العامة.

ب: إن الاستجابة للمساعدة القضائية، مقيدة بشرط المحافظة على سرية المعلومات المبلغة وأيضا عدم استعمالها في غير ما هو مقدم في الطلب. وهذا كما قلنا بسبب أهمية المعطيات والبيانات التي قد تحتويها منظومة معلوماتية خاصة ما تعلق بأمن الدولة أو الأفراد.

المطلب الثاني: حجز المعطيات المعلوماتية:

يظل الهدف الأساس لعملية تفتيش المنظومة المعلوماتية هو وضع اليد على الأدلة المادية التي تساعد على كشف المجرم، وما يتطلب ذلك من تدابير حجز معينة، خاصة وأن التقنية المعلوماتية تتيح له محو أو تعديل الدليل بكبسة زر وفي جزء من الثانية. أما إذا استحال حجز المعطيات المعلوماتية لأسباب تقنية أجاز المشرع للسلطات المختصة القيام بالإجراءات اللازمة لمنع الوصول إليها وكذا حدود استعمالها. فما هي هذه التدابير؟

أولاً: تدابير الحجز: يمكن تخزين المعطيات في ذاكرة الحاسوب أو في برامجه إذ تعتبر كيانات غير مادية مما شكل اختلافا في التشريعات العالمية حول مدى اعتبارها قابلة للحجز، حيث اعتبر المشرع الفرنسي برامج الحاسوب كيانا ماديا ملموسا فهو عبارة عن نبضات أو إشارات إلكترونية ممغنطة⁽³⁹⁾. في حين أضفى المشرع الجزائري حماية قانونية لقواعد البيانات بموجب نص المادة 5 الفقرة 2 من الأمر رقم: 03-05 المؤرخ في: 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، واعتبرها من المصنفات المحمية سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى. وطبقا لنص المادة 6 الفقرة 1 من القانون 04-09 التي تنص: "... يتم نسخ كل المعطيات اللازمة على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرار وفقا للقواعد المقررة في قانون الإجراءات الجزائية"، حيث استعمل المشرع مصطلح دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرار مثل: القرص المرن والقرص الصلب والقرص المضغوط والذاكرة الويضية والأشرطة المغناطيسية... إلخ، كما ترك المجال مفتوحا أمام ظهور تقنيات تخزين جديدة بناء على التطورات التقنية المذهلة في مجال صناعة الحواسيب وملحقاتها، إذ أنه لا يمكن التعامل مع تلك

المعطيات في شكلها الأولى المعنوي وهي عبارة عن نبضات أو ذبذبات إلكترونية أو إشارة ممغنطة⁽⁴⁰⁾، إلا بعد نسخها على هذه الدعامات.

كما تتم عملية الحجز وفقا للقواعد المقررة في نص المادة 84 من قانون الإجراءات الجزائية كاحترام إجراءات التحقيق وخاصة احترام سر المهنة وحقوق الدفاع بما يكفل أمن وسرية وسلامة المعطيات في المنظومة المعلوماتية⁽⁴¹⁾. ووفقا لنص المادة 6 الفقرة 2 من القانون 04-09 وأيضا إعادة تشكيل هذه المعطيات بما يخدم التحقيق بشرط عدم المساس بمحتواها وفقا لنص المادة 6 الفقرة 3 من نفس القانون، وهذا تحت طائلة العقوبات وفقا لنص المادة 85 من قانون الإجراءات الجزائية، وهو نفس ما نصت عليه المادتان 07 و 09 من القانون 04-09 كما سنرى لاحقا. إضافة إلى إجراء الحجز، نص قانون العقوبات في المادة 394 مكرر 6 على تدابير أخرى كمصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع الإلكترونية التي تكون محلا للجريمة⁽⁴²⁾.

ثانيا: الحجز عن طريق منع الوصول إلى المعطيات وحدود استعمالها: يخلق تتبع المجرم المعلوماتي صعوبات تقنية بالغة تحول في كثير من الأحيان دون الكشف عنه وبالتالي إفلاته من العقاب، لذلك نص المشرع في المادة 7 من القانون 04-09: "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 الدخول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة". إن الملاحظ في هذه المسألة، هو عدم تحديد المشرع للأسباب التقنية المانعة للحجز سواء ما تعلق بالمنظومة المعلوماتية نفسها كاستحالة الدخول لوجود كلمة السر أو نظام حماية يصعب اختراقه، أو ما تعلق بعملية نسخ المعطيات بسبب التطور الدائم في هذه التقنيات وما يتطلبه ذلك من توفير الوسائل التقنية اللازمة، إضافة إلى ضمان تكوين دوري بقصد اكتساب أعضاء الأجهزة القضائية المختصة في مجال التحقيق والكشف عن الجرائم المعلوماتية المهارات المطلوبة لمكافحتها.

ويبقى الهدف عدم تمكين المجرم من الوصول للمعطيات المخزنة في المنظومة المعلوماتية لاستعمالها أو نسخها أو الاطلاع عليها، لأنها تشكل محل الجريمة إذ تحتوي على أدلة قد يتمكن المجرم من تهريبها أو تدميرها أو تعديلها. كما نص المشرع تحت طائلة العقوبات على حدود استعمال المعلومات المتحصل عليها من عمليات المراقبة إلا فيما تتطلبه التحريات والتحقيقات القضائية وهذا بموجب نص المادة 09 من القانون 04-09 السالف الذكر⁽⁴³⁾.

خاتمة

تصدى المشرع الجزائري للجرائم المعلوماتية سواء من خلال تعديل قانون العقوبات أو من خلال تعديل قانون الإجراءات الجزائية، وذلك بالنص على جملة من القواعد الإجرائية خاصة ما تعلق بتفتيش المنظومة المعلوماتية وحجز المعطيات وحدود استعمالها، وهذا تماشيا مع التشريعات الحديثة والاتفاقيات المبرمة في هذا المجال وبرغم ذلك لازالت هذه القوانين تتسم بالنقصان وعدم القدرة على مواكبة التطورات المتلاحقة وذلك راجع لعدة أسباب نذكر منها:

- التطورات التقنية المذهلة الحاصلة في مجال الحوسبة ونظم الاتصالات، مما يخلق معه صورا وأنماطا مستحدثة لجرائم جديدة.
- الطبيعة الخاصة للجرائم المعلوماتية، فهي جرائم حديثة تقع في بيئة افتراضية يصعب اكتشافها والتحقيق فيها وبالتالي يسهل على المجرم المعلوماتي الإفلات من العقوبة.
- تباطؤ المشرع في إصدار تشريعات لمكافحة هذا النوع من الجرائم، وهذا رغم الانتشار الواسع للحاسوب وشبكة الإنترنت في الجزائر.
- ولكن برغم هذه الأسباب نقترح ما يأتي:
- الإسراع في تنصيب أعضاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته نظرا لأهمية دورها خاصة ما تعلق برسم الاستراتيجية الوطنية للوقاية من هذه الجرائم، ومساعدة السلطات القضائية في التحقيقات والتحريات.
- وضع آليات قانونية لضبط خدمة مقاهي الانترنت كتسجيل بيانات مستخدميها واستعمال كاميرات المراقبة بما لا يضر بحرية الحياة الخاصة قصد المساعدة في أعمال التحريات والتحقيقات القضائية للكشف عن المجرم المعلوماتي.
- تحيين نصوص القانون رقم: 04-09 السالف الذكر، بما يتماشى والتطورات المذهلة في مجال تقنية المعلومات وشبكة الانترنت مثلما بات يعرف حاليا، بعالم الانترنت المظلم (The Dark Internet).
- الاهتمام بالتكوين النظري والتدريب العملي للمكلفين من السلطة القضائية المختصة بالتحقيق في الجرائم المعلوماتية قصد اكتساب المهارات التقنية اللازمة والاستفادة من خبرات الدول الرائدة في مجال مكافحة الجرائم المعلوماتية بكافة صورها وتوفير الوسائل الحديثة في مجال الحوسبة والاتصال.

المراجع:

- 1- خالد ممدوح إبراهيم: "الجرائم المعلوماتية"، دار الفكر الجامعي، الإسكندرية، 2009، الطبعة الأولى، ص 5-6.
- 2- علي حسن محمد الطوالة: "التفتيش الجنائي عن نظم الحاسوب والانترنت"، عالم الكتب الحديث الأردن 2004، ص 10.
- 3- انظر نصوص القانون رقم: 04-09 مؤرخ في: 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم: 47 الصادرة بتاريخ: 16 أوت 2009، ص 5-8.
- 4- انظر نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات محررة بالقاهرة في: 21/12/2010 صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم: 14-252 المؤرخ في: 08/09/2014، الجريدة الرسمية رقم: 57، الصادرة بتاريخ: 28/09/2014، ص 4-14.
- 5- خالد ممدوح إبراهيم: "فن التحقيق الجنائي في الجرائم الالكترونية"، دار الفكر الجامعي، الإسكندرية 2009، الطبعة الأولى، ص 180.
- 6- سامي جلال فقي حسن: "التفتيش في الجرائم المعلوماتية"، دار الكتب القانونية، مصر، 2010، ص 55.
- 7- حسن طاهر داود: "جرائم نظم المعلومات"، أكاديمية نايف للعلوم الأمنية، الرياض، 2000، الطبعة الأولى ص 23.
- 8- زيدان زبيحة: "الجريمة المعلوماتية في التشريع الجزائري والدولي"، دار الهدى، عين مليلة، الجزائر، 2011 ص 130.
- 9- انظر المادتين 39 و 40 من المرسوم الرئاسي رقم: 96-438 المؤرخ في: 07/12/1996 المتضمن التعديل الدستوري باستفتاء شعبي ليوم 28 نوفمبر 1996، الجريدة الرسمية رقم: 76 المؤرخة في: 08/12/1996، ص 12.
- 10- انظر المواد من 44 إلى 47، و المادتان 64 و 79 وما بعدها من الأمر رقم: 66-155 المؤرخ في 8 يونيو سنة 1966، الذي يتضمن قانون الإجراءات الجزائية، المعدل والمتمم.

- 11- منى جاسم الكواري: "التفتيش، شروطه وحالات بطلانه، دراسة مقارنة"، منشورات الحلبي الحقوقية، بيروت 2008 الطبعة الأولى، ص 23.
- 12- أحمد عبد الحكيم عثمان: "تفتيش الأشخاص وحالات بطلانه"، منشأة المعارف، الإسكندرية، 2002، ص 13.
- 13- علي عدنان الفيل: "إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية"، المكتب الجامعي الحديث، مصر، 2012، ص 39.
- 14- نبيلة هبة هروال: "الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات"، دار الفكر الجامعي الإسكندرية، 2006، ص 221.
- 15- بلال أمين زين الدين: "جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن"، دار الفكر الجامعي، الإسكندرية 2008، ص 22.
- 16- طارق إبراهيم الدسوقي عطية: "الأمن المعلوماتي"، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص 88-89.
- 17- خالد ممدوح إبراهيم: "أمن الجريمة الالكترونية"، الدار الجامعية، مصر، 2008، ص 66.
- 18- طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 100.
- 19- كلمة السر: كلمة يحتفظ بها المستخدم سرا للتأكد من شخصية المستخدم، انظر نبيلة هبة هروال، مرجع سابق ص 355.
- 20- انظر نصوص الاتفاقية الدولية للإجرام المعلوماتي المؤرخة في: 2001/11/23 المنجزة من طرف المجلس الأوروبي، المنشورة في موقعه على شبكة الانترنت على الرابط الآتي: <http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm> بتاريخ: 2015/03/20 على الساعة 09:22.
- 21- انظر المواد من 394 مكرر إلى 394 مكرر 7 من القانون رقم: 04-15 المؤرخ في: 2004/11/10 يعدل ويتم الأمر رقم: 66-156 المؤرخ في: 8 يونيو 1966 والمتضمن قانون العقوبات، الجريدة الرسمية رقم: 71، المؤرخة في: 10 نوفمبر 2004، ص 11-12.
- 22- آمال قارة: "الحماية الجزائية للمعلوماتية في التشريع الجزائري"، دار هومة، الجزائر، 2006، الطبعة الأولى ص 100.
- 23- انظر المادة 02 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مرجع سابق، ص 4.
- 24- انظر المادة الأولى من الاتفاقية الدولية للإجرام المعلوماتي، مرجع سابق، منشور على شبكة الانترنت: <http://conventions.coe.int>
- 25- أيمن عبد الله فكري: "جرائم نظم المعلومات، دراسة مقارنة"، رسالة دكتوراه، جامعة المنصورة، مصر 2006 ص 11.
- 26- عرفت المادة 02 الفقرة 03 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات مصطلح البيانات: "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات كالأرقام والحروف والرموز وما إليها"، مرجع سابق ص 4-5.
- 27- يوسف المصري: "الجرائم المعلوماتية والرقمية للحاسوب والانترنت"، دار العدالة، القاهرة، 2011، الطبعة الأولى، ص 217.
- 28- انظر المادة 04 من القانون رقم: 09-04، مرجع سابق، ص 6.
- 29- انظر نصوص المادتين 26 و 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مرجع سابق، ص 8.
- 30- عبدالهادي بن زيطة: "حماية برامج الحاسوب في التشريع الجزائري"، دار الخلدونية، الجزائر، 2007، الطبعة الأولى، ص 34-35.
- 31- انظر المادة 44 من قانون الإجراءات الجزائية المعدل والمتمم.
- 32- يقصد بمنظومة تخزين معلوماتية: المنظومة التي تحتوي على بيانات تأخذ شكلا إلكترونيا أو أي شكل آخر يسمح بمعالجتها مباشرة، أنظر، نبيلة هبة هروال، مرجع سابق، ص 355.
- 33- الشحات إبراهيم محمد منصور: "الجرائم الالكترونية في الشريعة الاسلامية والقوانين الوضعية"، دار الفكر الجامعي الإسكندرية، 2011، ص 197.
- 34- انظر نص المادة 04 الفقرة الأخيرة من القانون رقم: 09-04، مرجع سابق، ص 6.
- 35- انظر المرسوم التنفيذي رقم: 06-348 المؤرخ في: 2006/10/05 والمتضمن تمديد الاختصاص المحلي، الجريدة الرسمية رقم: 63 الصادرة في: 2006/10/08، ص 29-30.

- 36- حسين بن سعيد الغافري: "السياسة الجنائية في مواجهة جرائم الانترنت"، دار النهضة العربية، القاهرة، 2009، ص 15.
- 37- يقصد بالفضاء السبراني: العوالم الافتراضية التي تخلقها الشبكات المعلوماتية، انظر حسين بن سعيد الغافري مرجع سابق، ص 14.
- 38- خالد ممدوح ابراهيم، الجرائم المعلوماتية، مرجع سابق، ص 407.
- 39- هشام محمد فريد رستم: "الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة"، (بدون دار النشر)، (بدون سنة النشر)، ص 596.
- 40- أمير فرج يوسف المحامي: "الجرائم المعلوماتية على شبكة الانترنت"، دار المطبوعات الجامعية الإسكندرية، (بدون سنة النشر)، ص 237.
- 41- تنص المادة 84 من قانون الإجراءات الجزائية المعدل والمتمم على أنه: "إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات، فإن لقاضي التحقيق أو ضباط الشرطة القضائية أو المنوب عنه وحدهما الحق في الاطلاع عليها... ويجوز على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحرار مختومة، ولا يجوز فتح هذه الأحرار والوثائق إلا بحضور المتهم مصحوبا بمحاميه...".
- 42- تنص المادة 394 مكرر 6 من قانون العقوبات المعدل والمتمم على أنه: "مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم صاحبها".
- 43- تنص المادة 09 من القانون رقم: 04-09 على أنه: "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"، مرجع سابق، ص 7.