# الإثبات في الجرائم المعلوماتية على ضوء القانون 09/04

# Evidence of cybercrimes in the light of the law 04/09

طالبة الدكتوراه/ عبير بعقيقي*
جامعة محمد خيضر بسكرة، الجزائر
bibaabir81@gmail.com
الدكتور/ فيصل نسيغة
جامعة محمد خيضر بسكرة، الجزائر
dr.fayssal_h@yahoo.fr

تاريخ الاستلام: 2018/02/28 تاريخ القبول للنشر: 2018/06/11

❖❖❖❖❖❖❖

**ملخّص:**

إنّ سوء استخدام التكنولوجيا الحديثة أدّى إلى تحوّل الإجرام التقليدي إلى إجرام يعتمد على وسائل تقنية وتكنولوجية، مما تتجسد خطورتها في سهولة ارتكابها ومحو الدليل والتلاعب فيه كما أنها تحتاج إلى خبرة فنية عالية للوصول إلى مرتكبها مما يثير مشكلات في جمع أدلة الإثبات، ولهذا كان لزاما على العدالة الجنائية التسلح بطرق إثبات تتمتع بنفس المواصفات التقنية والعلمية وهذا ما قام به المشرع الجزائري باستحداث قواعد إجرائية لإثبات الجرائم المعلوماتية في ظل القانون 04/09.

**الكلمات المفتاحية:** الجريمة المعلوماتية - الوسط الافتراضي - الدليل الجنائي - الدليل الرقمي - الإجراءات الجنائية - الإثبات.

***abstract:***

*Mishandling of new technology leads to transformation From the traditional crime to the crime of pared on technical means is technological its danger appearing in the easy use is the manual manipulation which requires a technical expertise sofistique to collect evidence it is for that became an obligation to the justice It is a criminal offense to have evidence of scientific technical specification that has been presented by the Algerian legislator as the elaboration of the procedures for proof cyber-crime according to the law 04/09.*

***keywords:*** *Cyber-Crime - Digital Evidence - Criminal Procedure - Evidence.*

* المؤلف المراسل.

**مقدّمة:**

إنّ الجرائم المعلوماتية متنوعة ومتطورة ويصعب اكتشافها وهذا التطور الحاصل في الأنظمة المعلوماتية انعكس بطبيعة الحال على النظام الإثباتي، حيث ظهر ما يدعى بنظام الأدلة العلمية والتي تقوم على الاستعانة بالأساليب العلمية والتكنولوجية الحديثة للكشف عن الجريمة ونسبتها إلى المتهم.

ولما كان نظام الإثبات في الجزائر هو النظام المختلط وفقا لنص المادة 212 من قانون الإجراءات الجزائية "أنه يجوز إثبات الجرائم بأيّ طريق من طرق الإثبات وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي...".

نجد أنّ المشرّع منح القاضي الجزائي السلطة التقديرية في تحديد قيمة دليل الإثبات ومع سكوت المشرّع الجزائري عن النص على الأدلة المستمدة من الكمبيوتر كدليل للإثبات فإنّ القاضي يجد نفسه عاجزا عن إعمال سلطته التقديرية، والسبب ما يتميز به الدليل الرقمي من خصائص إضافة إلى طرق الإثبات المعمول بها لاستخلاصه.

ولهذا تدارك المشرّع هذا النقص وفقا لخطته في مكافحة الجريمة المعلوماتية بتعديل قانون الإجراءات الجزائية بموجب القانون 22/06 المؤرخ في 20-12-2006، وإصدار قانون إجرائي خاص وهو القانون 04/09 والمتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال وهذا من أجل استنباط طرق إجرائية ذات طبيعة تقنية تتلاءم مع هذه الجرائم.

وتتمثل الإشكالية المعالجة في هذه الدراسة: ما هي طبيعة الدليل الرقمي؟ وكيف تعامل المشرّع الجزائري مع هذا الدليل في مجال الإثبات؟

**خطة الدراسة:**

**المبحث الأول:** ماهية الدليل الرقمي.

**المبحث الثاني:** الأحكام الإجرائية لاستخلاص الدليل الرقمي.

## المبحث الأول

## ماهية الدليل الرقمي

إنّ الجرائم المعلوماتية ترتكب في وسط إعلامي افتراضي على عكس الجرائم التقليدية التي تكون في وسط مادي ملموس، وكذلك أدلة الإثبات في الجرائم الإلكترونية تختلف عن الشكل الذي تتواجد عليه في الجرائم العادية مثل القتل، السرقة، التزوير الخ.... وغيرها، حيث نجدها ذات طبيعة فنية وتقنية ناجمة عن النظام المعلوماتي وتتفق مع الوسط الذي ارتكبت فيه الجريمة، وقد عبّرت عنها الاتفاقية الأوربية لمكافحة الجرائم المعلوماتية بالأدلة الرقمية أو الأدلة الإلكترونية وهذا النوع من الأدلة ذو طبيعة خاصة من التعقيد مما جعل التعامل معها يثير مشكلات مهنية وقانونية إمام جهات التحري والتحقيق ولهذا لابدّ من التعرف عليها بوضوح لوضع الحلول المناسبة لمعالجتها، وسنحاول في هذا المبحث التعرض إلى مفهوم الدليل الرقمي، ثم خصوصية الدليل الرقمي من خلال ما يلي:

**المطلب الأول: تعريف الدليل الرقمي وخصائصه**

إنّ ظهور أشكال مستحدثة من الجرائم المعلوماتية أدى بطبيعة الحال إلى ظهور أدلة مستحدثة، وفي إثبات الجاني تختلف عن الأدلة التقليدية وتعرّف "بالدليل الرقمي" وهذا التطور في إثبات الجاني جعل نصوص قانون الإجراءات الجزائية عاجزة عن إثبات هذا النوع من الجرائم الذي يحتاج إلى طرق تقنية وفنية تتناسب مع طبيعته الخاصة بحيث يمكن فك رموزها وشفراتها.

**الفرع الأول: تعريف الدليل الرقمي**

الدكتور محمد رضوان هلال عرف الدليل الرقمي بقوله: "كل ما هو مسجل على وسائط غير ورقية، ويمكن رؤيته عن طريق شاشة جهاز الكمبيوتر أو سماعه ويمكن نقله"[1]، وما يمكننا ملاحظته على هذا التعريف أنه ليس بالكافي إذ أنه لم يحدد ما المقصود بمصطلح "مسجل"؟ كان عليه على الأقل أن يحدده ولو على سبيل المثال، لأنّ هناك العديد من أنواع الملفات والبيانات مسجلة على جهاز الكمبيوتر ويتطلب أمر فرزها وتصنيفها وقتا كبيرًا خاصة إذا كان الجهاز يخص شركة، كما أنه لم يوضح أي الوسائط مقصودةٌ بقوله، فنحن كما نعلم أنّ هناك وسائط إلكترونية خارجة عن الجهاز كال Flash memory والذي قد لا يتوافر في مسرح الجريمة، لذا كان الأحرى أن يحدد بقوله كل ما هو مسجل من بيانات تخص الجريمة على جهاز الكمبيوتر...".

عرّفه البعض كذلك على أنه: "كلّ بيانات يمكن إعدادها، أو تخزينها في شكل رقمي، بحيث تمكن الحاسب الآلي من إنجاز مهمة ما"[2]، وهو تعريف يتماشى مع ما ذكرناه أعلاه بخصوص التعليق على التعريف السابق، فقد حدد أصحاب هذا التعريف نوع البيانات المرادة، وأيضا مكان تخزينها والغاية منها.

عُرِّف الدليل الرقمي على أنه: "المعلومات والبيانات ذات القيمة الاستقصائية، والمخزنة أو المنقولة على جهاز إلكتروني[3]. التعريف من وجهة نظرنا حسن في الشق الأول منه والذي بيّن لنا ماهية البيانات المخزنة والجاري التمحيص فيها من قبل رجال الضبطية القضائية، لكن لم يكن حسنًا في الشق الثاني منه والذي أطلق على محل تلك البيانات والمعلومات بالجهاز الإلكتروني ونحن نعلم سلفًا أنّ هناك مئات الأنواع من تلك الأجهزة، لذا كان الأحرى بأصحاب التعريف أن يخصصوا نوع ذلك الجهاز بالقول "الحاسب الآلي مثلا".

تعريف آخر وهو الذي لفت انتباهنا، وصاحب التعريف هو الدكتور عمر أبو بكر بن يونس، حيث قال: "الدليل الرقمي هو ذلك الدليل الذي يجد له رجال الضبطية القضائية أساسا في العالم الافتراضي ويقود إلى الجريمة"[4]، هذا التعريف أوضح لنا أن تلك البيانات لا يكفي أن تكون مسجلة على الجهاز فحسب وإنما قد تكون كذلك في العالم الافتراضي مثل اتصالات بين الجاني والمجني عليه من خلال مواقع التواصل الاجتماعي ونحوها، والتي أصبح بإمكان مأموري الضبط أن يستخلصوا منها كل كبيرة وصغيرة عن طريق الاتصال بالجهات المعنية في الشركة الأم لتلك المواقع وطلب الترخيص لتنزيل سجل به كل ما قام به المعنيون من نشاطات وغيرها، إلى جانب ذلك فإن الدكتور عمر أبو بكر بن يونس استهل تعريفه

قائلا: "فبعد كل شيء فهو دليل يدفع القاضي بالاقتناع أن الشخص المعني قد ارتكب الجريمة المعلوماتية".

وعُرِّفَ على أنه: "الوسيلة المبحوث عنها في التحقيقات بغرض إثبات صحة واقعة تهم الجريمة أو ظرف من ظروفها المادية أو الشخصية، وهي تلك الواقعة التي يستمد منها القاضي البرهان للنطق بالحكم"[5]، وهذا التعريف في نظرنا أوضح أصحابه الغاية من الدليل الرقمي أو المعلوماتي لكن ليس بتعريف له.

ونحن بدورنا حاولنا تعريف الدليل الرقمي على النحو التالي: "الدليل الرقمي كلّ دليل مأخوذ من جهاز الكمبيوتر محل الجريمة، ويكون على شكل بيانات وملفات مخزنة بداخله وقد يكون عبارة عن ملفات ناجمة عن اتصالات بين الجاني والمجني عليه من خلال مواقع الإنترنت، وهو ما يساعد القاضي على توضيح موقفه من القضية ومنه إصدار الحكم البات في القضية المعروضة أمامه".

**الفرع الثاني: خصائص الدليل الرقمي**

بعد جملة التعريفات المتطرق لها أعلاه اتضح لنا أنه يمتاز عن غيره من الأدلة الأخرى من ناحيتين:

**الناحية الأولى:** طبيعة هذا الدليل المعلوماتية وأنه يتعلق فقط بالحاسوب، الهاتف، والنظم المعلوماتية بشكل عام.

**الناحية الثانية:** القيمة الاستدلالية لهذا الدليل وما يحتويه من معلومات تساعد في إثبات الجرم من عدمه.

لذا على رجال الضبطية القضائية أن يكونوا على دراية كافية بمجال المعلوماتية حتى يمكنهم التعامل مع هذا الدليل، لذا ارتأينا من خلال هذا الفرع التطرق لأهم الخصائص التي جعلت من هذا الدليل مميزًا والدليل الأوحد في إثبات الجرم من عدمه.

**أولًا - الدليل الرقمي دليلٌ علمي:**

المطلع على القواعد التي تضبط الأدلة العلمية يتضح له جليا اتفاق الغاية التي من أجلها وجد الدليل الرقمي مع غاية الدليل العلمي، فكلاهما يصبو من خلالهما رجال الضبطية القضائية لاكتشاف الحقيقة ومنه تحقيق العدالة، تطبيقا للقاعدة: "إن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة"[6]، فالدليل الرقمي يخدم كلتا الغايتين.

ولبيان مدى كون الدليل الرقمي دليلا علميا فقد أورد عمر أبو بكر بن يونس بهذا الصدد: "إذا كان الدليل العلمي له منطقه الخاص والذي يجب ألا يخرج عليه من حيث عدم تعارضه مع القواعد العلمية السليمة، وللدليل الرقمي نفس المنطق، وبهذا فإن الدليل العلمي لا يجب أن يخرج عما توصل إليه العلم الرقمي وإلا فقد معناه"، بعبارة أخرى مواكبة التطور الذي يشهده العلم الرقمي وعدم الاكتفاء بقواعد معينة فقط[7].

لذا فإنّه وعند عرضه كدليل إثبات أمام هيئة المحكمة يأخذ القاضي برأي الخبراء والتقنيين بخصوص تلك المعلومات، وفي الوقت نفسه يقدم له محضرا به كافة الإجراءات المعمولة من قبل رجال الضبطية القضائية، للحرص أكثر على أن التعامل مع هذا الدليل لم يخرج كما أسلفنا عن قواعد العلم الرقمي.

**ثانيًا- الدليل الرقمي ذو طبيعة تقنية:**

كما أشرنا سابقًا فإن طبيعة هذا النوع من الأدلة جعلته مختلفا من ناحية التعامل، إذ لا يمكن التعامل معه كالأدلة المادية عن طريق فحص البصمات وما إلى غير ذلك، وإنما هو دليل يحوي معلومات لا يتم استخراجها إلا بتقنيات تكنولوجية[8]، إذ أن البيئة المتواجد بها تحتوي على كم هائل من الأرقام لا ينتهي ولا يمكن حصره، وهذا العالم يتماشى ورغبات الإنسان والتي يترجمها على شكل برامج وخدمات، فيمكن مباشرة التجارة عبر الإنترنت ويمكن الحصول على خدمات كذلك من خلالها كالحجز في فنادق عالميه والسفر وشراء السلع غير المتوفرة في البلد، بل ويمكن الدخول إلى جامعات من خلال الإنترنت ومزاولة الدراسة من خلالها عن بعد وعليه التخرج والحصول على شهادات جامعية[9]، ويمكن لفئات معينة من الناس (ذوي الخبرة العالية) مباشرة ارتكاب الجرائم من خلالها كما أوضحنا في الباب الأول من دراستنا، لذا فإن الدليل الرقمي والذي يتم تجميع كل بياناته والمعلومات الموجودة فيه عن نشاط المعني لا يتم إلا باستخدام تقنيات عالية كما أسلفنا.

**ثالثًا- صعوبة التخلص من الدليل الرقمي:**

يتميز كذلك الدليل الرقمي بصعوبة التخلص منه عكس الأدلة الأخرى والتي يمكن للجاني فيها مسح بصماته، أو حرق مسرح الجريمة مزيلا بذلك كل الآثار، أو حتى تهديد الشهود بالقتل.

وسبب مميزة الدليل الرقمي يعود إلى أن الكمبيوتر يسجل كذلك نشاط الجاني عند محوه للدليل هذا من جهة، ومن جهة ثانية فإنه وللتخلص النهائي منه على الجاني الرجوع لمسرح الجريمة وتفكيك الجهاز وأخذ القرص الصلب الذي يحتوي على كل شيء وإلا لن يمكنه التخلص منه عن بعد حتى وإن أرسل برمجيات خبيثة لمسح النظام، فرجال الضبطية اليوم على دراية بكيفية استرجاع تلك الملفات حتى وإن تم مسح النظام، ومن أشهر تلك البرامج نذكر برنامج Xtree gold v 3.0 وهو برنامج يساعد المحققين على العثور على أي ملف بالقرص الصلب له علاقة بالجريمة[10].

ومن أشهر القضايا التي أكدت مدى صعوبة التخلص من الدليل الرقمي قضية إيران – كونترا Iran-Contra، وقد خرج من هذه القضية مسؤولون بالحكومة الأمريكية المسؤولة عن التحقيق بعدم وجود توازن بين الأدلة الورقية والرقمية فالأولى يمكن التخلص منها عكس الثانية، فرغم مساعي الجهة المدعى عليه لمسح كل ما به من بيانات استطاع المحققون الاطلاع على نظام الحفظ Backup للبريد الإلكتروني وتأكد لهم مدى تورط بعضٍ من مسؤولي مكتب الرئيس الأمريكي في القضية[11].

**المطلب الثاني: أنواع الدليل الرقمي**

على عكس أدلة الإثبات الجنائية المتعارف عليها كالبصمة، وشهادة الشهود، فإن الدليل الرقمي مختلف تماما إذ لا تعرف له هيئة واحدة، والسبب أنه يختلف باختلاف نوع الجرم المرتكب بوسائل المعلوماتية، فتارة يمكن جمعه فقط من خلال الصور الموجودة بالقرص الصلب، وتارة يكون تسجيلات صوتية أو فيديو لمكالمات بين الجاني والمجني عليه، وتارة أخرى يكون بيانات نسي أن يمسحها الجاني عند اختراقه للنظام وارتكاب جرمه، لذا فإن أنواع الدليل الرقمي مرتبطة بطرق استخلاصه، لذا سنقسم تلك الأنواع حسب طرق التعامل معها.

**الفرع الأول: الدليل الرقمي المستخلص من مركبات الكمبيوتر**

وهذا النوع يتعلق بإحدى مهام رجال الضبطية القضائية عند مداهمة مكان الجريمة على إثر مكالمات من الأعيان مفادها وجود جماعة تتردد على المكان المحدد وأن ذلك المكان لا يعود لملكيتهم، فتنتقل رجال الشرطة القضائية وتداهم المكان وتصادر كل ما يوجد به من أجهزة كمبيوتر وملحقاتها كالطابعات سواء الخاصة بالورق العادي أو الخاصة بصناعة بطاقات الائتمان ونحوها، فيباشر بناءً على ذلك الخبراء مهمة التفتيش الدقيق لعتاد الكمبيوتر Hardware كالأقراص الصلبة التي تحتوي على نظام التشغيل بما يحتوي عليه من برامج خبيثة تم العمل بها ومعلومات تم الاستيلاء عليها، ومحاولة استعادة كل الملفات المحذوفة، ومعالجة الملفات المشوبة بفيروسات وفك شيفرة ملفات أخرى[12].

هذا النوع من وجهة نظرنا الشخصية يعتمد على التفتيش اليدوي وأيضا محاولة رفع بصمات الأصابع إن وجدت فأغلب الهاكرز لا يأخذون الأمر على محمل الجد ظنا منهم أنهم منيعون من الملاحقة، كما يعتمد أيضا على التفتيش التقني والمعلوماتي والذي يتم ببرامج وجدت خصيصًا لهذا الغرض، وسبب تسليطنا الضوء على هذه الطريقة والتي تعد تقليدية مقارنة بالتفتيش عن بعد أن الجاني لا يملك فرصة لمسح الأدلة، بينما في التفتيش عن بعد والذي تخطر فيه السلطات المعني بالأمر بأنهم سيفتشون جهازه سواء عن طريق بريد إلكتروني أو اتصال هاتفي[13]، فإنه سيعمد إلى تغيير القرص الصلب أو وضع برمجيات خبيثة تعرقل عملية التفتيش، كذلك التنصت الذي تنتهجه العديد من الحكومات لن يعمل إن كان المعني هاكرا محترفا، لأن هذه الفئة من المجرمين على دراية تامة بكل الأساليب الحديثة والتي تعتمدها الدولة بل بعضٌ منهم وصل حتى لاختراق مواقع أجهزة الأمن على أعلى مستوياتها والتنصت عليهم وعلى كل عملية سيقومون بتنفيذها، بل وصل الأمر كذلك حتى لتسريبها للغير وفضح تلك الخطط للعلن وهو ما يضع تلك الحكومات أمام مأزق كبير خاصة أمام الرأي العام لانتهاكها خصوصية مواطنيها المكفولة بنصوص الدساتير.

إلى جانب عملية فحص القرص الصلب، فإن ثاني الأمور التي يعمل الخبراء التقنيون التابعون لرجال الضبط القضائي "الشرطة القضائي، مأمور الضبط..." هو فحص البرامج المنزلة على هذا القرص والسبب أن هناك بعضًا من برامج الاختراق تتخذ هيئة برامج رسمية على سبيل المثال يتم برمجة ذلك البرنامج على إدخال شيفرة حتى يفتح وإن لم يتم إدخال تلك الشيفرة فإنه يحولك مباشرة لبرنامج آخر

بشكل عشوائي كأن يفتح برنامج Office word أمامك لتظن أنه برنامج سليم، هنا يفحص الخبراء مصدر البرنامج وكذلك الشهادة الرسمية للبرنامج الملحقة به في ملف التصطيب، فإن اتضح لهم أن البرنامج ليس من تطور شركة مايكروسوفت هنا يصنف كدليل على إدانة الجاني[14].

على كلٍ نحن نرى أن الدليل الرقمي المستند فيه على جهاز الكمبيوتر وما يحتويه من عتاد ملحق به، قد يكون دليلا لإدانة الجاني، وقد لا يكون كذلك، خاصة وإن كانوا يتعاملون مع شبكة من المحترفين الذين لا يتركون خلفهم ولا حتى أثر صغير، فقد طور العديد من الهاكرز أنظمة وهمية يتم تصطيبها على دعامات مادية خارجية كالأقراص الصلبة المحمولة ويمارسون من خلالها نشاطاتهم الإجرامية، ليبقى الكمبيوتر مجرد جهاز عادي بفصل تلك الدعامة ولا يمكن أن يسحب منه أي ملف يخص الجريمة لانعدامها من الأساس.

**الفرع الثاني: الدليل الرقمي المستخلص من فحص نظام الاتصال بالإنترنت**

هذا النوع من الأدلة الرقمية أثار جدلاً كبيرًا حول الأخذ به من قبل هيئة المحكمة من عدم ذلك، والسبب في ذلك الجدل يعود إلى طبيعة الإنترنت التي تعتبر بحرًا رقميًا إذ من الصعب استخلاصه في مدة وجيزة، خاصة وأن البيانات الرقمية سريعة الزوال ويمكن أيضا أن تجعل الجهات المختصة أمام عائق وهو الجريمة العابرة للحدود فطبيعة الإجراءات المتخذة في حالتنا هذه تأخذ كثيرًا من الوقت حسب إمكانات الدولة المعنية، فقد يكون الاعتداء ناجم عن هاكرز ينشطون في دولة لا تربطها بالدولة المتعرضة للهجوم علاقات صداقة، لكن أثبتت بعض الدول مدى فاعلية الدليل الرقمي المستخلص من نظم الاتصال بالإنترنت:

- تساعد بروتوكولات الإنترنت في إدانة الجاني خاصة وأنها كما سبق وأشرنا تحتوي على أربعة خانات بدءًا من اليسار إلى اليمين وإحدى الخانات تدل على المنطقة الجغرافية وأخرى على الجهاز المستعمل في الجريمة وهو ما يساهم في احتمالية إلقاء القبض على الجاني وكما يساعد في تتبع نشاطه والمواقع المتصل بها والجهات الأخرى المشاركة في الجرم وهو ما يساعد كدليل إثبات[15].
- كذلك فحص البريد الإلكتروني وتتبع الإيميلات المشبوهة خاصة وأننا اليوم نشهد أكثر من شركة عملاقة تمنح بريد إلكتروني مقابل ملأ استمارة تحتوي على البيانات الشخصية على الشكل التالي: example@outlook.fr, exmaple@gmail.com، لذا فإن البريد الإلكتروني الذي يخرج عن هكذا نطاقات يعتبر مشبوها، خاصة وإن كان فحوى البريد له علاقة بمنظمات دولية غير معروفة تنشط في مجالات الخير والتي حصدت الكثير من الضحايا وتم الاستيلاء على أرقام حساباتهم المصرفية. مُؤَدَّى كلامنا هذا أن تلك الشركات لديها القدرة على تحديد مكان أي شخص يتم تقديم شكوى عنه، وترسلها للجهات المعنية "الشرطة" والتي تحقق في أمره[16].
- إن استعصى الأمر فإن الطريقة الوحيدة لاستخراج الأدلة تكمن في فحص الخوادم المسؤولة عن توفير الاتصال بالإنترنت "سواء المسؤولة عن ربط الزبائن بالمواقع أو غرف الدردشة"، إذ تحتاج تلك العملية اتخاذ الإجراءات القانونية اللازمة وفق القانون النافذ في النطاق الإقليمي

الذي يوجد به الخادم، ويجب أن يكون المسؤولون عن ذلك على دراية بأنواع الخوادم ووظيفة كل واحد منها وأي الخوادم هو المعني بالتفيش[17].

## المبحث الثاني

## الأحكام الإجرائية لاستخلاص الدليل الرقمي

نظرا للطبيعة التقنية للجريمة المعلوماتية وكذلك الدليل الرقمي و المعوقات التي تواجه رجال الأمن والتحقيق للوصول إلى أدلة الإثبات فإنه لابد من وجود طرق إجرائية مستحدثة تتناسب مع طبيعتها التقنية و التكنولوجية، وهو ما أدى بالتشريعات في مختلف الدول إلى إرساء قواعد جزائية مستحدثة تقوم بتكريس تقنية المعلومات من أجل استخلاص الدليل الرقمي.

والمشرع الجزائري وكغيره من التشريعات قام بإرساء جملة من المقومات التشريعية لمكافحة الجريمة المعلوماتية من خلال ما جاء به في القانون 06-22 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية الأمر(155/66) من خلال إجرائي التسرب واعتراض المراسلات، وكذلك بموجب إصدار قانون إجرائي خاص به القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و لاتصال ومكافحتها، وقام باستخدام إجراء المراقبة الإلكترونية، إلى جانب إجراء التفتيش، وسوف نتعرض في هذا المبحث إلى كل من هذه الإجراءات المستحدثة في مجال المعلوماتية.

### المطلب الأول: المراقبة الإلكترونية

تناول المشرع الجزائري هذا الإجراء من خلال المادة الرابعة من القانون رقم 04/09 المتعلق بالقواعد الخاصة بالرقابة من الجرائم المتصلة بتكنولوجيات الإعلام ولاتصال ومكافحتها بعنوان مراقبة الاتصالات الإلكترونية – الحالات التي تسمح باللجوء إلى الرقابة الإلكترونية[18].

#### الفرع الأول: تعريف المراقبة الإلكترونية

ونجد أن المشرع الجزائري لم يعرّف هذا الإجراء من خلال القانون رقم 09-04، ولهذا سنتطرق إلى التعريف الفقهي الذي وضع له العديد من التعريفات نذكر منها : المراقبة الإلكترونية "تعتمد على الإنصات والتسجيل ومحلها المحادثات الخاصة سواء أكانت مباشرة أو غير مباشرة، أي سواء كانت مما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكية واللاسلكية"، ورأي أخر أن المراقبة هي نوع خاص من استراق السمع يسلط على الأحاديث الشخصية والمحدثات[19].

#### الفرع الثاني: شروط وآليات المراقبة الإلكترونية

يمكن أن نستنتج شروط وآليات المراقبة الإلكترونية في التشريع الجزائري من خلال نص المادة 65 مكرر 5 ق إ ج على أنها:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع ترتيبات تقنية دون موافقة المعنيين من أجل بث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخصية أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص

أو عدة أشخاص يتواجدون في مكان خاص أما المادة 04 من القانون رقم 04/09 من القوانين السالفة الذكر فهي تشير إلى الجرائم الماسة بأمن الدولة.

- في حالة توفير المعلومات عن احتمال الاعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحري والتحقيق القضائي، عندما كان يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

أما بالنسبة لإجراءات تنفيذ المراقبة الإلكترونية وفقا لما جاء في القانون 04/09 فنصت عليه المادة 04 ومنه وهي:

الإذن المكتوب: ويتضمن:

- التعريف و المراقبة.
- طبيعية الجريمة.
- تسليم الإذن.
- كتابة وتحديد المدة التي لا تتجاوز 4 أشهر قابلة لتجديد.

طرق التنفيذ: وتشمل:

- سرية الإجراءات[20].
- **التسيير:** حيث أنه يمكن لوكيل الجمهورية أو قاضي التحقيق أو ضابط الشرطة القضائية أن يسخر عونا مؤهلا لدى هيئة مكلفة بالاتصال (العامة، الخاصة) للقيام بهذا الإجراء.
- **المحاضر:** حيث يحرر الشخص المكلف بالعملية محضرا يحتوي على العناصر الأساسية للعملية.

**المطلب الثاني: التسرب واعتراض المرسلات**

**الفرع الأول: التسرب**

وهو الإجراء المستحدث الذي تنص عليه المواد من 65 مكرر 11 إلى مكرر 18 من قانون الإجراءات الجزائرية.

**أولاً- تعريفه:**

تقنية يسمح بموجبها الدخول إلى وسط مغلق مثل جماعة إجرامية أو شبكة تتاجر في الممنوعات كالأسلحة أو المخدرات، وتتم هذه العملية بعد اختيار ضابط الشرطة القضائية لأحد العناصر التابعة له الذين تتوفر فيهم بعض الصفات الخاصة كالتأقلم والتكيف مع الوسط المستهدف.

**ثانيًا - شروطه:**

- الحصول على إذن مكتوب ومسبق من طرف وكيل الجمهورية أو قاضي التحقيق بعد اخطار وكيل الجمهورية.

- يتضمن الإذن الجريمة التي تبرر اللجوء للتسرب وهوية ضابط الشرطة المنسق للعملية وتحديد المادة إذ لا تتجاوز 4 أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق.
- أن تكون الجريمة ضمن الجرائم المذكورة على سبيل الحصر في المادة 65 مكرر 05 من قانون الإجراءات الجزائية ومن ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

**ثالثًا- مراقبة إجراءات التسرّب:**

يراقب التسرب وكيل الجمهورية المتخصص أو قاضي التحقيق وفقا لنص المادة 65 مكرر11 ق أج ج، ويمكن لهما الأمر بوقف التسرب في أي مرحلة وذلك من أجل تأمين خروج متسلسل من الشبكة الإجرامية أو عدم جدوى التسرب.

**رابعًا- التسرب في مجال الإجرام المعلوماتي:**

تكون عملية التسرب في الجرائم الإلكترونية بدخول ضابط أو عون شرطة إلى العالم الافتراضي وذلك عن طريق اشتراكه في المحادثات كغرف الدردشة، أو اختراق مواقع معينة مستخدما في ذلك أسماء أو صفات وهيئات مستعارة وهمية سعيا منه للاستفادة منهم في كيفية اقتحام الهاكر للموقع، أو القيام بحلقات اتصال مع المشتبه فيهم عن طريق البريد الإلكتروني.

**الفرع الثاني: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور**

يتعلق الأمر بمسألة بالغة الأهمية كونها تشكل انتهاكا لحرمة المراسلات التي كفلها الدستور الجزائري[21]، غير أن المشروع الجزائري قد سمح بموجب المادة 65 مكرر 05 من قانون الإجراءات الجزائية باعتبار المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وذلك إذا اقتضت ضرورة التحري في الجريمة المتلبس بها في جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... الخ، ويلاحظ من نص هذه المادة أن المشرع الجزائري قد يسمح بهذا الإجراء في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حتى تتمكن جهات التحقيق من استخلاص أدلة الإثبات و الوصول إلى الحقيقة.

كما أشار إليه المشرع الجزائري من خلال نص المادة 03 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال مكافحتها على ما يلي: "مع مراعاة القوانين التي تراعي سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحري أو التحقيقات القضائية حماية النظام العام وفق القواعد المنصوص عليها في الإجراءات الجزائية في هذا القانون ووضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة". ولقد كانت وسائل الاتصال في السابق تتمثل في الهاتف أما في الوقت الحاضر فانتقلت إلى البريد الإلكتروني وغرف الدردشة عبر الإنترنت، ونجد أن المشرع الجزائري قد عرف المراسلات في المادة 09 من القانون 03-2000 بأنها: "اتصال مجسد بشكل كتابي عبر مختلف الوسائل المادية التي يتم توصيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه"[22].

وعرف وسائل الاتصال الإلكتروني بأنها الوسائل "ترسل أو إرسال أو استقبال أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"[23]، ولهذا فإن مراقبة الاتصال على الإنترنت أو محتوى البريد الإلكتروني يعتبر جريمة يعاقب عليها القانون لاتصالها بحرمة الحياة الخاصة وهذا ما أشار إليه في المادة 137 من قانون العقوبات الجزائري إلا في الحالات التي أجازها القانون كما سبق الذكر في المادة 03 من قانون 09-04، ولهذا فإن المشرع الجزائري فرض الحماية القانونية على جميع الاتصالات الإلكترونية باعتبارها حق في الخصوصية وأجاز ذلك في الحالات التي يسمح بها القانون من أجل مقتضيات التحري والتحقيق والوصول إلى أدلة الإثبات ووفقا لما تتطلبه العدالة الجنائية.

**المطلب الثالث: إجراء التفتيش**

يعتبر التفتيش أحد أهم إجراءات التحقيق فبواسطته يمكن أن يُغير مسارُ الحقيقة من المجهول وعدم معرفة الجاني، إلى الظفر بأدلة تؤدي به إلى الوقوف أمام العدالة، ومن جهة أخرى وصفه بعضٌ من رجال القانون بأنه كذلك إجراءٌ خطيرٌ لما فيه من مساسٍ بالخصوصية التي تعتبر حقًا من حقوق المواطن مهما كان جانيًا أم مجنيًا عليه أم لا علاقة له من الأساس بالقضية، وإجراءً يتعارض ونصوص الدساتير التي تكفل للفرد حق خصوصيته، لكن من جهة أخرى متى كان بأوامر قضائية فإن ذلك ينتفي.

**الفرع الأول: تعريف التفتيش في الجرائم المعلوماتية**

كما تعودنا فإن مهمة التعريف غير منوطةٍ بالمشرع الجزائري والذي اكتفى في هذه الحالة بالتطرق إلى أنه إجراءٌ من إجراءات التحقيق ولذلك تفصيلٌ فيما بعد، الأمر الذي استلزم منا دراسة أهم ما ورد عن رجال الفقه القانوني وأساتذتنا، فبعضٌ منهم عرف التفتيش بقوله: "التفتيش أحد إجراءات التحقيق والمسعى من اللجوء إليه هو ضبط الأدلة وما يتعلق بالجريمة حتى يتم نسب الجرم لفاعله وإنصاف صاحب الحق، وهو إجراء يمتد كذلك ليطال فئة غير الجاني والمجني عليه كالشهود وفقا لما تمليه القوانين المنظمة لذلك الإجراء"[24]، وهو تعريفٌ في نظرنا يتضمن كل كبيرة وصغيرة بخصوص هذا الإجراء باستثناء ما يتم فيه، وكذلك فعل الدكتور هلالي عبد اللاه أحمد: "التفتيش إجراء من إجراءات التحقيق، هدفه جمع الأدلة المتعلقة بجناية أو جنحة في محل يتمتع بحرمة المسكن، ويسعى المحققون من خلاله نسبة الجرم لمرتكبه"[25]وهو تعريف أدرج عبارة حرمة المسكن وكان الأصح في نظرنا لو كانت العبارة ينتهك خصوصية الشخص ولا يقتصر الأمر فقط على المسكن لأن الجرائم قد ترتكب في محلٍ آخر غير المسكن كمحل العمل، والذي يكون للشخص خصوصيةٌ فيه بعد الغلق ليتصرف بحريته في عد أرباحه والبضائع...الخ، والتعاريف التي جاء بها الفقهاء الغرب مشابهة تمامًا لتعريفات الفقهاء العرب، فالفقه الفرنسي ألحق تعريفه بالتفريق بين تفتيش الأشخاص La fouillé corporelle والذي يطال جسم الإنسان من ملابس وحقائق...الخ، والتفتيش الذي يطال المساكن La perquisition والذي يتم عن طريق زيارة محل السكن وتفتيش غرفه وكل ملاحقه[26]، وهي بطبيعة الحال جملة من التعريفات للتفتيش بشكل عام.

بينما التفتيش في جرائم المعلوماتية يمكن القول بخصوصه أنه: "إجراء من إجراءات التحقيق وتقوم به سلطة مختصة بهذا المجال "مجال المعلوماتية" للدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات ومخرجات بحثًا عن آثار الجرم التي قد يخلفها الفاعل كل هذا لتجميع الأدلة ضده وبالتالي نسبة الجرم له"[27]، التعريف في نظرنا ليس بالكافي للتعريف بهذه المهمة، لذا ارتأينا أن نعرف التفتيش في الجرائم المعلوماتية كالتالي: "التفتيش في الجريمة المعلوماتية هو أحد إجراءات التحقيق التي تقوم بها الهيئات المنصوص عليها حسب تشريع كل دولة، وتُعنى هذه الهيئات بالانتقال إلى محل وقوع هذه الجريمة "الحاسب الآلي"، فيكون التفتيش إما بشكل تقليدي عن طريق تفحص الجهاز ومكوناته وكل ما يحيط به، أو بطريقة تقنية بالدخول إلى النظام الذي يشغله والبحث والتمحيص في كل البيانات، وهي إجراءات تساعد في تقفي آثار الجاني متى وجد لها المحققون سبيلاً ومنه تضييق دائرة الاشتباه إلى تسليم الجاني للمحاكمة".

**الفرع الثاني: إجراءات التفتيش في الجريمة المعلوماتية**

بما أن الجريمة في حالتنا هذه تطال الحاسب ومختلف النظم المعلوماتية، فإننا ارتأينا أن نتطرق لمدى قابلية مكونات الحاسب وشبكاته للتفتيش، وكما هو متعارف عليه وسط مستخدمي الكمبيوتر فإن مكوناته منها ما هو ماديٌ ويطلق عليه Hardware ومنها ما هو ليس بملموس كأنظمة التشغيل والبرمجيات ويطلق عليها على العموم بالـ Software، إلا جانب شبكات الاتصال "الإنترنت" والتي تعرف أشكالا منها السلكية واللاسلكية، ومنها المحلية والدولية.

**أولاً- تفتيش المكونات المادية Hardware:**

للمكونات المادية الخاصة بمحل التفتيش "الجهاز" وجهة نظر مختلفة عند خضوع هذا الأخير للتفتيش، إذ أنها وعلى عكس البرمجيات والأنظمة التشغيل فهي متعلقة بالمكان المتواجد به الجهاز، فمتى كان متواجدا بمسكن أحدهم أو محل عمله الخاص، فإن التفتيش في هذه الحالة يخضع لنفس الإجراءات العادية، تجنبًا لانتهاك حرمة وخصوصية الأخير، ومن جهة أخرى فإن بعضًا من أجهزة الكمبيوتر التي طالتها الجريمة المعلوماتية تكون مرتبطة بمكونات مادية خارجية كما هو الحال في المؤسسات المالية "كالبنوك"، والشركات على مختلف أنواعها، فالهيئة المكلفة بالتفتيش في هذه الحالة تعمد إلى التفتيش اليدوي في بادئ الأمر لكل المكاتب والسجلات التي تحمل أسماء الزوار والعمال المتواجدين بالمكان والمدراء وغيرهم، ومن ثم تفتيش كاميرات المراقبة عن طريق الاطلاع على تسجيلاتها طيلة المدة التي وقعت فيها الجريمة المعلوماتية[28].

ومن مظاهر التفتيش المادي كذلك العملية التي يقوم بها التقنيون لأجهزة الطابعات فيكون هناك تتبع للبيانات ومنه إصدار أمر بالطباعة فيتم الحصول على كافة الملفات المطبوعة سابقًا، ويكون التفتيش للمكونات المادية أيضا يطال الحواسيب المحمولة والهواتف النقالة الحديثة "Smart Phone"، لإمكانية ربطها بأجهزة الكمبيوتر المتعرضة للنصب المعلوماتي أو السرقة ونحوها من الجرائم المعلوماتية الأخرى.

**ثانيًا- تفتيش المكونات المعنوية Software:**

كانت ولا تزال هذه المكونات تؤرق الكثير من المحققين رغم التطور العلمي الذي وصلنا إليه ورغم التدريبات التي تخضع لها هذه الجهة "المكلفة بالتحقيق"، إلا أن التطور في هذا المجال لا يطال فقط رجال الضبط القضائي المكلفين بالتحقيق وإنما يستفيد منها أيضا الهاكرز، ويتم تفتيش المكونات المعنوية Software عن طريق فحص ملفات نظام التشغيل، ولعل إحدى أهم الطرق التي ساهمت فيها شركات صنع معالجات الكمبيوتر بجعل المعالج بمثابة أداة لتسجيل هوية مالك الكمبيوتر إلى جانب أنه محرك هذا الجهاز، فالمحققون يعتمدون عليه لاستيفاء المعلومات التي تمكنهم من تحديد مستخدمه في الجريمة المعلوماتية[29]، وقد يجري كذلك تفتيش الشبكة المعلوماتية رغم أن هذا الإجراء صعبٌ قليلا ويحتاج لوقت وجهد، فيلجأ المحققون إلى الشركات المسؤولة عن تزويد المنطقة بالإنترنت ويضيقون نطاق البحث حول المنطقة التي وقع فيها الاعتداء، ويتفحصون كل نشاطات الأشخاص الذي يقطنون فيها أو الأشخاص الذي لهم صلة بالمجني عليه.

**الفرع الثالث: موقف المشرع الجزائري**

بخصوص تفتيش المكونات المعنوية فقد تناول المشرع الجزائري إجراء التفتيش في نص المادة الثالثة من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: "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 المنظومة المعلوماتية"[30]، بقدر ما بَيَّنَ أن بإمكان رجال الشرطة القضائية تفتيش المنظومة المعلوماتية بقدر ما بَيَّنَ في المادة الرابعة من هذا القانون السالفة الذكر سابقًا أن تلك العملية تتم بإشراف كل من له دراية بهذا المجال عكس تفتيش المكونات المادية التي لا تحتاج لدراية بذلك ويمكن مزاولتها من أي رجل شرطة قضائية عادي.

تعامل كذلك المشرع الجزائري مع مشكلتين: :

- **الأولى:** في حالة كان الجهاز الممارس من خلاله الجريمة متصلا بجهاز المجني عليه، ويكون في هذه الحالة داخل الإقليم الوطني ولكن خارج الاختصاص المكاني للجهات المكلفة بالتحقيق، وقد مدد بذلك المشرع اختصاص قاضي التحقيق المكاني، أو رجال الشرطة القضائية المكلفين من قاضي التحقيق بموجب المادة 40 (معدلة) خاصة وأن الجريمة المعلوماتية من بين تلك الجرائم المعنية بهذا التمديد، حيث نصت الفقرة الثانية: "يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف"[31].

- **الثانية:** في حالة كانت الجهاز الممارس من خلاله الجريمة متصلا بجهاز المجني عليه خارج التراب الوطني أي في بلد أجنبي عن الجزائر بغض النظر عن إن كان عربيا أو أوروبيا...الخ، وبالرغم من أنها مشكلة تؤرق العديد من الأجهزة المكلفة بالتحقيق في بعضٍ من الدول لقصور نصوصها القانونية، إلا أن المشرع الجزائري أوجد لها حلاً حيث نص في القانون رق 09-04 السالف الذكر بإمكانية مساعدة السلطات الأجنبية للبلد المعني بتفتيش الجهاز الموجودة على إقليمه، وإعمالا كذلك لمبدأ المعاملة بالمثل، حيث نصت الفقرة الأولى المادة 16 من هذا القانون: "في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدات القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني"[32]. ورجوعًا منا لشروط هذا الإجراء نجد أن:

**1- الشروط الموضوعية:**

بخصوص محل التفتيش نصوص القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كانت واضحة بذلك الشأن، والمحل هنا يكون الحاسب الآلي سواءٌ المرتكب عليه الجريمة "جهاز الضحية" أو جهاز الجاني في حالة ما وُجدت دلائل على أن شخصًا مشبوهًا عمل به، وكذلك الشبكة المعلوماتية، ولا حاجة لنا للتفصيل أكثر لأننا سبق وأشرنا للنصوص أعلاه، وأيضا يمكن أن يكون المحل كذلك المكان المتواجد به الجهاز لأن الجاني قد يلجأ لتخبئة الدعامات المادية التي تحوي البيانات المستولي عليها على سبيل المثال في المنزل، أو بإحدى غرف الشركة...الخ. وما يجدر بنا كذلك التطرق إليه إلى جانب المحل أن يذكر في مذكرة التفتيش "الأمر القضائي بالتفتيش" أن السبب وراء ذلك التفتيش هو وقوع جريمة معلوماتية على جهاز الضحية، أو على حساب الضحية البنكي...الخ.

**2- الشروط الشكلية:**

حدد المشرع الجزائري في قانون الإجراءات الجزائية الوقت الذي تباشر فيه الجهة المعنية بالتحقيق تفتيش المحل الذي وقعت عليه الجريمة بشكل عام "سواءٌ الجريمة التقليدية أو المعلوماتية بالأخص تفتيش المكونات المادية"، وبيان ذلك كالتالي: التفتيش في الجرائم التقليدية يكون من الساعة الخامسة صباحا إلى الساعة الثامنة مساء ولا يتعدى ذلك، بينما يتعدى الأمر ذلك في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فيمكنهم بذلك التفتيش ليلا ونهارا مهما كانت الساعة، وذلك في الفقرة الثالثة من المادة 47 (معدلة) من قانون الإجراءات الجزائية الجزائري.

ويختتم ضباط الشرطة القضائية التفتيش بتحرير محضر عملا بنص المادة 79 من القانون نفسه، والتي تنص على: "يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها. ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات"[33]، ويتضمن المحضر تاريخ

التفتيش، التوقيع من قبل محرره "الكاتب" وكذلك المحقق وكافة الإجراءات التي عمل بها هذا الأخير واجبٌ تدوينها فيه.

**خاتمة:**

بعد التطرق إلى أهم المواضيع المستحدثة و التي تعالج إثبات أخطر الجرائم الحالية و هي الجرائم المعلوماتية، وبعد التعرض إلى موقف المشرع الجزائري من خلال إدراج جملة من المقومات التشريعية في مجال الإثبات الجنائي، توصلنا إلى جملة من النتائج تتمثل فيما يلي:

- الدليل الرقمي يقوم على أسس علمية و تقنية وبذلك فهو ينتمي إلى الأدلة العلمية.
- يتميز هذا الدليل أنه ذو طبيعة غير مرئية و صعب التخلص منه فهو قابل للنسخ.
- خصوصية الدليل الرقمي من أهم المعوقات والصعوبات التي تواجه سلطات التحري والتحقيق في إثبات الجريمة المعلوماتية.
- الدليل المناسب لإثبات الجرائم المعلوماتية هو الدليل الرقمي.
- لقد تناول المشرع الجزائري من خلال القانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية والقانون 04/09 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام الآلي والاتصال جملة من القواعد الإجرائية المستحدثة في مجال الإثبات لمكافحة الجريمة المعلوماتية بالطرق التقنية التي تتناسب مع طبيعتها.
- إنّ هذا النوع من الأدلة يحتاج إلى خبرة فنية وتقنية يصعب على المحقق التقليدي التعامل معها.

في ختام هذه الدراسة نقترح جملة التوصيات التالية:

- استحداث نص قانوني بخصوص أدلة الإثبات وإضافة الدليل الرقمي ضمنها خاصة وأن الجرائم

المعلوماتية لا يمكن إثباتها بالأدلة التقليدية كالبصمات والشهود...الخ.

- ضرورة تدريب فئات من عناصر الأمن للتعامل مع هذا الدليل لما قد يتسبب فيه أي خطأ من تلف بعض من البيانات التي يحتويها.

## الهوامش:

(1) محمد رضوان هلال، المحكمة الرقمية مفهومها ومقوماتها، دار العلوم، دون بلد نشر، طبعة 2007، ص 91.

(2) Christeine Segarlaa Chung, Dadvid Bayer, The electronic paper trail ‘‘Electronic evidence can be any information created or stored in digital form whenever a computer is used to accomplish a task’’, P. 04.

(3) Panagiotis Kanellis and Others, Digital crime and forensic science in cyberspace, Idea group inc, 2006, P. 272.

(4) عمر أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، أطروحة دكتوراه تخصص القانون الجنائي، كلية الحقوق، جامعة عين شمس، 2004، ص 969.

(5) العربي شحط عبد القادر، نبيل صقر، الإثبات في المواد الجنائية، دار الهدى، الجزائر، طبعة 2006، ص 15.

(6) Robert Adler, Restoring Colorado River Ecosystems: A Troubled Sense of Immensity, Island press, island, 2012, P. 131.

(7) عمر أبو بكر بن يونس، مرجع سابق، ص 977، 978.

(8) مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، مصر، طبعة 2009، ص 217.

(9) Amanda Hoey, Analyse of the police and criminal evidence act see 69, computer generated evidence, UK, 1996, P. 2 .

(10) مصطفى محمود موسى، مرجع سابق، ص 220.

(11) محمد أمين البشري، الحلقة العلمية "الإرهاب والإنترنت" لتأهيل المحققين في جرائم الحاسب الآلي وشبكات الإنترنت، جامعة نايف العربية للعلوم الأمنية، الرياض، طبعة 2008، ص 26.

(12) عمر أبو بكر بن يونس، مرجع سابق، ص 1009-1011.

(13) عمر بن محمد يونس، الدليل الرقمي للمنظمة العربية للتنمية الإدارية، جامعة الدول العربية، القاهرة، طبعة 2006، ص 05.

(14) ممدوح عبد الحميد عبد المطلب، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، 2003، مصر، ص 244، 245.

(15) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، طبعة 2011، ص 234.

(16) المرجع نفسه، ص 235.

(17) عمر أبو بكر بن يونس، مرجع سابق، ص 1007.

(18) القانون رقم 22/06 المؤرخ في 20-12 2006 المعدل المنضم لقانون الإجراءات الجزائية (الأمر 155/66).

(19) احمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة ماجستير ، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013، ص 79.

(20) المادة 04/45 من قانون إجراءات جزائية جزائري التي تتعلق بالسر المهني.

(21) المادة 02/39 من الدستور المتعلقة بسرية المراسلات.

(22) القانون رقم 200-03 المؤرخ في 05 أوت 2000 المتضمن القواعد العالمية المتعلقة بالبريد والموصلات السلكية واللاسلكية، جريدة الرسمية عدد 48.

(23) البند "و" من المادة الثانية من القانون 09-04 سالف الذكر.

(24) عماد محمد ربيع، "حقوق المتهم في مرحلة التحقيق الابتدائي في قانون أصول المحاكمات الجزائية الأردني"، مجلة البلقاء للبحوث والدراسات، عمادة الدراسات العليا والبحث العلمي، جامعة عمان الأهلية، المجلد الثاني عشر، العدد الأول، 2007، ص 140.

(25) هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي "دراسة مقارنة"، دار النهضة العربية، القاهرة، طبعة 1997، ص 47.

(26) علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، عالم الكتاب الحديث، الأردن، طبعة 2004، ص 12.

(27) عبد الناصر محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية "دراسة تطبيقية مقارنة"، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007، ص 20.

(28) عمر محمد أبو بكر بن يونس، مرجع سابق، ص 866.

(29) المرجع نفسه، ص 867.

(30) المادة 03 من الأمر 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف الذكر.

(31) المادة 40 (معدلة) من قانون الإجراءات الجزائية الجزائري السالف الذكر.

(32) الفقرة الأولى من المادة 16 من الأمر 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف الذكر.

(33) المادة 79 من قانون الإجراءات الجزائية الجزائري السالف الذكر.