وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي – برج بوعريريج–
University of Mohamed el Bachir el Ibrahim
كلية الحقوق والعلوم السياسية
Faculty of law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر مهني في الحقوق

تخصص: قانون الإعلام الآلي والإنترنت

الموسومة بـ:

إجراءات التحري والتحقيق في الجريمة الالكترونية

إعداد الطالب:

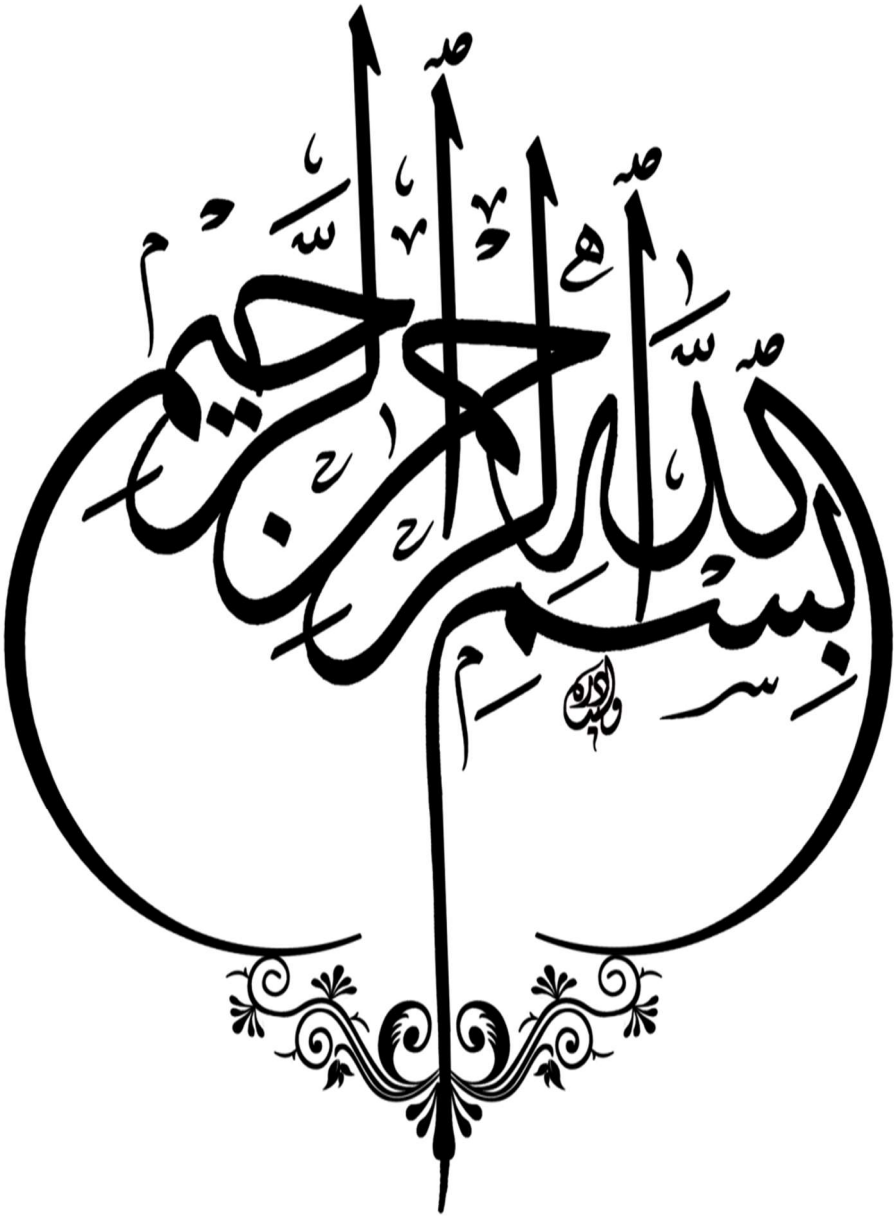
- **مباركية رابح**

إشراف الدكتور:

حمزة عياش

الاسم واللقب	الرتبة	الصفة
أ. د فرشة كمال	أستاذ التعليم العالي	رئيسا
د. حمزة عياش	أستاذ محاضر – أ–	مشرفا
د. خوضري محمد	أستاذ محاضر – أ–	ممتحنا

السنة الجامعية 2021/ 2022


بسم الله الرحمن الرحيم

الشكر و التقدير

الحمد الله الذي بفضله تتم الصالحات نتوجه بالشكر الجزيل الى

الأستاذ الكريم "حمزة عياش" الذي قبل الاشراف على هذه المذكرة

وأنار لنا طريق البحث العلمي والذي لم يدخر أي جهد في سبيل

مساعدتنا.

كما نشكر كل الأساتذة الذين بذلوا الذين بذلوا كل الجهود في سبيل تكويننا

ومساعدتنا على اكتساب العلم والمعرفة.

كما نتقدم بشكرنا الخالص الى كل الزملاء والأصدقاء الذين ساعدونا

في اعداد هذا العمل من قريب أو من بعيد.

نشكر كذلك كل موظفي وعمال كلية الحقوق والعلوم السياسية

جامعة محمد البشير الابراهيمي برج بوعريريج الجزائر.

الاهداء

الحمد لله والصلاة والسلام على الحبيب

محمد صلى الله عليه وسلم

إلى من كللهما الله بالهيبة والوقار ... إلى من علماني العطاء بدون انتظار ... إلى من أحمل اسمهما بكل افتخار...
إلى من كان دعائهما سر نجاحي وحنانهما بلسم جراحي

أمي أبي حفظهما الله وأطال في عمرهما في الخير والصلاح

إلى من كن شموعا متقدمة تنير حياتي ودربي

أخواتي الغاليات رعاهن الله

إلى من بوجودهم أكسب قوة ومحبة لا حدود لها

إخوتي رعاهم الله

إلى كل من علمني حرفا أساتذتي الكرام جزاهم الله كل خير

إلى أصدقائي الذين كانوا عونا لي على مصاعب الحياة الدراسية جزاهم الله خيرا

إلى كل هؤلاء، جزيلا شكرا

الطالب مباركية رابح

.

مقدمة

مما لا شك فيه أنه لا يوجد ما يسمى بالجريمة الكاملة مهما حاول الجاني إخفائها، وذلك استنادا لتبادل المواد التي تنص على أنه عند احتكاك جسمين يبعضهما البعض فإنه لابد أن لقاعدة " لوكارد "[1]ينتقل جزء من الجسم الأول إلى الثاني وبالعكس، وبالتالي ينتج عن هذا الاحتكاك الدليل الجنائي، وفي مجال الجريمة المعلوماتية ينتج لدينا ما يعرف بالدليل الالكتروني أو ما يطلق عليه بالدليل الرقمي.

ونظرا لطبيعة الجرائم المعلوماتية الخاصة فإنها تتطلب إجراءات وأساليب خاصة ونوعية للبحث والتحقيق، لأجل اكتشاف الدليل الرقمي وتحصيله من قبل الفنيين المختصين، وكل ذلك يستدعي اتخاذ إجراءات سريعة.

إن إجراءات البحث والتحقيق في الجنائي العام هي الأساس في البحث والتحقيق في جرائم الالكترونية تماما كما هو الحال في باقي الجرائم الأخرى، أما عناصر البحث والتحقيق الجنائي الأخرى من عملية وفنية وغيرها فإن استخدامها يتوقف على ظروف كل جريمة، فلما اعتمد المشرع الجزائري نصوصا لتجريم الأفعال الواقعة في الوسط الإلكتروني والمستخدم فيها الأجهزة الإلكترونية وكل ما يمس المعالجة الألية للمعطيات بمفهوم الجريمة الإلكترونية مما استدعى المشرع الجزائري الى ادخال مجموعة من التعديلات على كل من قانون العقوبات وقانون الاجراءات الجزائية، كما استحدث القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، اضافة الى

[1]- Le principe d'échange de Locard, énoncé pour la première fois par Edmond Locard en 1920 s'applique au lieu du crime, à l'auteur, à la victime, il peut s'exprimer de la manière suivante: - l'auteur et/ou son matériel abandonnent des indices sur la victime et sur la scène de crime. L'auteur et /ou son matériel emportent des indices appartenant a la victime et a la scène de crime. Plus d'information voir: -Jean Claude martin – investigation de scènes de crimes - fixation de l'état des lieux et traitement des traces d'objet- presse polytechnique et universitaire Romandes- France- 2004. P 08.

القانون 18-04 المتعلق بالقواعد العامة للبريد والاتصالات الالكترونية، والقانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

وصدرت مجموعة من المراسيم الرئاسية سنوات2019و2020 وسنة2021، أخرها المرسوم الرئاسي الذي أعاد سير وتنظيم الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال، والمرسوم الرئاسي المتعلق بوضع منظومة وطنية للأمن الأنظمة المعلوماتية.

فهل كرس المشرع الجزائري فعلا أحكام قانونية تتلاءم مع خصوصية التحري والتحقيق لضمان فاعليته في مواجهة الجرائم الالالكترونية والحد من آثارها والى أي مدى وفق في ذلك؟

فالملاحظ أن إجراءات التحقيق في الجرائم المعلوماتية تتصف بالخصوصية من حيث طريقة كشفها والتبليغ عنها، والعناية بمسرح الجريمة[2]، وكيفية تكوين فريق الضبط والتفتيش، وصولا إلى خصوصية التعامل مع الأدلة الجنائية. إذن كل هذه الإجراءات ذات الطابع الإجرائي يجب أن تتم بالموازاة مع طبيعة الجريمة المعلوماتية وما ينتج عنها من خصوصيات تغيب عن الجرائم الأخرى، وهو ما يتجلى في خصوصيات عمل رجال البحث والتحقيق المنوط بهم مهام البحث والتحقيق المعلوماتي، وهو ما يدفعنا إلى طرح التساؤل حول طبيعتها الإجرائية العملية في مجال البحث والتحقيق المعلوماتي؟ وإلى أي مدى تظهر نجاعة هؤلاء في حل طلاسم الجرائم المعلوماتية بالرغم من تعقيدها وتشعبها؟ وهل الدليل الجنائي يعتبر دليلا على قدم المساواة من حيث قوته الثبوتية وباقي وسائل الإثبات الأخرى؟ إن الإجابة عن هذه الإشكالية الفرعية تستدعي هنا تقسيم هذا العمل إلى فصلين أساسيين هما:

[2]- ضياء علي أحمد النعمان، الغش المعلوماتي الظاهرة والتطبيقات، الطبعة الأولى، المطبعة الوطنية، المملكة المغربية، 2011، ص 363.

• الأول: نستهله لمعالجة إجراءات عملية البحث والتحري في الجريمة الإلكترونية والأساليب المتبعة من قبلهم في هذا الشأن، ومسائل الاختصاص.

• الثاني: فسنخصصه لمعالجة مسألة التحقيق في الجريمة الإلكترونية والدليل الإلكتروني الناتج عن عمل رجال البحث و التحقيق الالكتروني ومدى حجيته في مجال الإثبات الجنائي.

الفصل الأول

إجراءات التحري في الجريمة الالكترونية

تمتاز الإجراءات الجزائية بمجموعة من المراحل بداية من المراحل التي تكون قبل وقوع الجريمة ثم مرحلة التحريات الأولية مما تسمى بمرحلة جمع الاستدلالات أو الحقائق، وتنتهي بتحريك الدعوى والمباشرة فيها وتكون مرحلة جمع الاستدلالات من المراحل المهمة التي تمر بها الدعوى الجزائية، حيث تلعب دورا هاما في مساعدة الجهات المختصة في كشف المستور ومعرفة الحقائق وتقصيها ومن جهة أخرى تخفف العبئ على الجهات القضائية المختصة والتي هي الأخرى خصها المشرع الجزائري من خلال وضعه لقانون الإجراءات الجزائية كل جهة قضائية والاختصاص المستند لها في مجال محاربة الجريمة والحد منها وكشفها بشتى الطرق والأساليب المنصوص عليها في النصوص القانونية، فمن خلال هذا ارتبطت مهمة التحري والبحث بمهام واختصاص الجهات القضائية كالضبطية القضائية (رجال الشرطة القضائية) قاضي التحقيق وكذا وكيل الجمهورية كل واختصاصاته ومهامه في مجال كشف الجريمة والقضاء عليها ولذلك نطرح الإشكال التالي؛

ما هي شروط الإختصاص للتحري والبحث الخاص بالكشف عن الجريمة الالكترونية؟ وما هي الإجراءات الخاصة للتحري والبحث الخاص بالكشف عن الجريمة الالكترونية؟ لهذا الغرض وللإجابة على الإشكال المطروح قسمنا الفصل الأول إلى مبحثين:

الأول نتطرق فيه إلى شروط الإختصاص للتحري والبحث الخاص بالكشف عن الجريمة الالكترونية، أما الثاني: فسنتطرق فيه الى الإجراءات الخاصة بالبحث والتحري في الجرائم الالكترونية.

المبحث الأول: الاختصاص في الجرائم الالكترونية.

التحريات الأولية أو جمع الاستدلالات مصطلح يطلق على نمط سير الإجراءات الجزائية التي ينفذها أعضاء الضبط القضائي عند ارتكاب جريمة ما، تمهيدا لتحريك الدعوى العمومية لاقتضاء المجتمع أو الدولة حقها في العقاب من مرتكب تلك الجريمة.

وما يقصد من التحري كذلك هو البدء بإجراءات تعد تمهيدية تباشرها الضبطية القضائية قبل البدء في تحريك الدعوى العمومية، أي وبمعنى أخر التثبت من وقوع الجريمة، البحث عن القائم بها وجمع الإثباتات والقرائن اللازمة للتحقيق فيها والاستعانة بها للكشف عن الجريمة.

لا تجيز الجريمة المعلوماتية وبحكم خصوصيتها وطبيعتها، لأي كان من جهات الضبطية القضائية أو جهات التحقيق أو النيابة العامة أمر البحث والتحقيق بشأنها، فهي جريمة تستلزم محققا من نوع خاص قادر على التعامل مع مميزاتها بالشكل اللازم الذي يسمح له بمعرفة هوية مرتكبها وتحديد معالمها وآثارها، وذلك من خلال تتبع آثارها الالكترونية ودلائلها، كل ذلك في إطار الشرعية الإجرائية، تجنبا لطائلة البطلان واحتراما لحقوق وحريات الأفراد.

وتعتبر شروط الاختصاص القضائي من مسائل النظام العام التي يمكن إثارتها في أي مرحلة كانت عليها الدعوى فتتعرض الإجراءات برمتها للبطلان في حال عدم استيفائها، وشروط الاختصاص في مسائل البحث والتحقيق نوعان اختصاص نوعي وآخر إقليمي محلي، فلا يمكن لمن يتولى أعمال البحث والتحقيق مباشرة أعماله وهو غير مختص نوعا، كما لا يمكن لمن يتولى الإجراءات نفسها وهو يتمتع بصفة الاختصاص النوعي ممارسة أعماله خارج نطاق اختصاصه الإقليمي.

المطلب الأول: تحديد مفهوم شروط الاختصاص في مسائل الجريمة الالكترونية.

إن المقصود بالاختصاص هو السلطة السيادية للدولة التي تمكنها من تطبيق قوانينها الوطنية داخل أقاليمها، وتعد الجرائم الإلكترونية من أكثر الجرائم التي تطرح مسألة الاختصاص ذلك أن سلوك أو نشاط المجرم فيها لا يعترف بالحدود، فالعالم كله مرهون بمجرد نقرة بسيطة على لوحة المفاتيح جهاز الحاسوب، إذ أن الطبيعة التقنية العالية للنظم المعلوماتية المرتبطة بشبكات الاتصال العالمية يمكن أن تؤدي إلى أن يصبح إقليم أكثر من دولة مسرحا لجريمة واحدة، الأمر الذي قد ينجم عنه تنازع في الإختصاص بين هذه الدول، فقد يحدث أن ترتكب الجريمة الإلكترونية في إقليم دولة معينة وتتحقق النتيجة في دولة أخرى فتتعدد القوانين التي يمكن أن تحكم هذه الجرائم بتعدد الدول المرتبطة بها، وإذا كان الاختصاص على مستوى داخلي وطنيا فيتحدد سلفا بمعايير محددة في قانون الإجراءات الجزائية.

ان التحقيق هو مجموعة القواعد القانونية والفنية التي تباشرها السلطة المختصة لتمحيص الأدلة والكشف عن الحقيقة تتأتى الحقيقة في الجرائم الالكترونية بوجودها كأساس موضوع التحقيق المستحدث، وينبغي التطبيق السليم للقانون من خلال التقدير السليم للدليل المستمد من الجريمة واحترام قواعد الاختصاص وعدم تجاوز حدود الحيز المكاني والزماني خاصة عند عبور الجريمة حدود الدولة الواحدة، واحترام مختلف عناصر التحقيق، مع كفالة حقوق الأفراد لتحقيق توازن عادل بين ما تفرضه السلطة العامة من التزامات عادلة، مع مراعات مبدأ الشرعية الاجرائية والحق فيه؛ اين يخضع الفرد لقيود تحد من حريته الخصوصية تحديا أمام سلطات التحري والتحقيق في الجرائم الالكترونية، كما أن قواعد اثبات الجرائم الالكترونية تعتبر مميزة وتعتبر إجراءات البحث والتحقيق من الإجراءات التي تمس بحقوق وحريات الأفراد، ولذلك فقد حرص المشرع الجزائري على اسنادها لجهة قضائية لأجل ضمان كفالة حقيقية لجملة الحقوق والحريات الفردية، وتتمثل عادة هذه الجهة القضائية في هيئة الضبطية القضائية إذا كانت الإجراءات متعلقة بمرحلة البحث والتحري،

وفي هيئة قضاء التحقيق إذا كانت الإجراءات متعلقة بمرحلة التحقيق القضائي ممثلة في شخص قاضي التحقيق.*

كما أن الاختصاص العملي والفني في مجال أعمال البحث والتحقيق في الجرائم المعلوماتية يعود وبالدرجة الأولى إلى دائرة مكافحة الجرائم المعلوماتية التابعة للمديرية العامة للأمن الوطني، وكذلك الفرق التابعة لمركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها التابعة لسلك الدرك الوطني، وإلى مديرية المراقبة الوقائية واليقظة الإلكترونية التابعة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتحت إشرافها، والتي تم الإعلان عن إنشائها رسميا بموجب صدور المرسوم الرئاسي رقم15-261المؤرخ في08أكتوبر2015وتم تعديلها بصدور المرسوم الرئاسي رقم439/21، مؤرخ في2ربيع الثاني عام1443، الموافق ل7نوفمبر سنة2021، هذه الوحدات الخاصة تتكون أساسا من جملة من المستخدمين يتولى ممن تتوفر لديهم صفة ضباط للشرطة القضائية مباشرة إجراءات البحث والتحقيق في الجرائم المعلوماتية، إما من تلقاء أنفسهم أو بناء على طلبات واوامر تردهم من قبل وكيل الجمهورية أو قاضي التحقيق، مما يجعل منهم العنصر البارز في متابعة هذه الإجراءات بصفة فعلية دون غيرهم.

المطلب الثاني: اختصاص ضباط الشرطة القضائية بالبحث والتحري في مجال الجرائم المعلوماتية.

يتولى عادة ضباط الشرطة القضائية مسائل البحث و التحري في كافة الجرائم ، بما في ذلك الجرائم المعلوماتية فلا يوجد مانع قانوني يحد من ممارسة هؤلاء لأعمالهم المتعلقة بالبحث والتحري ،سوى أن يتوفر فيهم شرط الاختصاص النوعي في مجال الجرائم المعلوماتية بعد

*- تعمل كل من الضبطية القضائية على القيام بأعمال البحث و التحري عن الجرائم ما لم يبدأ فيها بتحقيق قضائي و ذلك من قبل ضباط وأعوان الشرطة القضائية و كذلك بعض الأعوان المنوط بهم مثل هذه المهام و ذلك تحت إدارة وكيل الجمهورية و إشراف النائب العام للمجلس القضائي التابعين له ، و تحت رقابة غرفة الإتهام ، و إذا ما أفتتح تحقيق قضائي بشأن تلك الجرائم تحول دورهم إلى تنفيذ تفويضات جهة التحقيق و تنفيذ طلباتها- راجع نصوص المواد 12 إلى 14 من قانون الإجراءات الجزائية الجزائري.

تبليغهم بوقوعها[3]، و الذي يمكن تحديده في التمتع بصفة ضابط الشرطة القضائية، و ذلك تقيدا بما يفرضه نص المادة 05 من الفصل الثالث المتعلق بالقواعد الإجرائية الخاصة بتفتيش النظم المعلوماتية الوارد في نص القانون09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و سبل مكافحتها و التي تنص على أنه: " يجوز للسلطات القضائية المختصة وكذا ضابط الشرطة القضائية في إطار قانون الإجراءات الجزائية ... الدخول بغرض التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها ." ... وبناء على ذلك فأن الأشخاص المذكورين في نص (المادة 15 ق 02/15 (من قانون الإجراءات الجزائية الجزائري المعدل والمتمم، والتي تحدد قائمة حصرية لصفة الأشخاص المنوط بهم هذه الصفة، هم الأشخاص المخولون قانونا بمباشرة أعمال البحث و تنفيذ أوامر التحقيق بشأن الجرائم المعلوماتية.[4]

إن المتمعن في نص المادة، لايكاد أن يتصور أن يقوم رئيس المجلس الشعبي البلدي بتولي أعمال البحث والتحقيق في الجرائم المعلوماتية، فحسب ما بيناه سالفا فإن هذا الإختصاص يعود وبالدرجة الأولى لضباط الشرطة القضائية المنتمين إلى الفرق المتخصصة في مكافحة الجرائم المعلوماتية، والتي تضم محققين من نوع خاص كما سنبينه لاحقا، ولذلك وجب تخصيص نص منفرد في قانون الإجراءات الجزائية يحدد الإختصاص النوعي في شخص رجال الشرطة والدرك والأمن العسكري الموظفون التابعون للأسلاك الخاصة للمراقبين، ممن يتمتعون بصفة ضباط الشرطة القضائية، حتى يتحقق الإنسجام بين النص

---

[3]- المادة 17 فقرة 01 من قانون الإجراءات الجزائية الجزائري المعدل بموجب الأمر رقم 15-02 المؤرخ في 23جويلية 2015.

[4]- جاء في نص المادة 15 من قانون الإجراءات الجزائية الجزائري المعدلة بموجب الأمر 15-02 المؤرخ في 23 جويلية 1 2015انه:" يتمتع بصفة ضابط الشرطة القضائية: • رؤساء المجالس الشعبية البلدية • .ضباط الدرك الوطني • .الموظفون التابعون للأسلاك الخاصة للمراقبين ومحافظي و ضباط الشرطة للأمن الوطني • .ذوو الرتب في الدرك، و رجال الدرك الذين أمضوا في سلك الدرك ثلاث سنوات غلى الأقل و الذين تم تعينهم بموجب قرار مشترك بين وزير العدل ووزير الدفاع الوطني ، بعد موافقة لجنة خاصة • .الموظفون التابعون للأسلاك الخاصة للمفتشين وحفاظ واعوان الشرطة للأمن الوطني الذين أمضوا ثلاث 03 سنوات على الأقل و عينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية والجماعات المحلية بعد موافقة لجنة خاصة • .ضباط و ضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك صادر بين وزير الدفاع و وزير العدل."

العام والنص الخاص ممثلا في القانون09-04، وذلك تجنبا لتداخل الإختصاصات وتضيع فرص إحراز الأدلة، والتسبب في إفلات الجاني من المتابعة والعقاب.

إذن فالشرط الأساسي من أجل حق ممارسة أعمال البحث والتحري (التحقيق الابتدائي) في الجرائم المعلوماتية، هو التمتع بصفة ضابط الشرطة القضائية وذلك حسب ما هو وارد في هذا الشأن بموجب نص (المادة 63 ق 06-22 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري بقولها:" يقوم ضباط الشرطة القضائية، وتحت رقابتهم أعوان الشرطة القضائية، بالتحقيقات الإبتدائية بمجرد علمهم بوقوع الجريمة إما بناء على تعليمات وكيل الجمهورية او من تلقاء أنفسهم." كما يجوز لضباط الشرطة القضائية القيام بكل أعمال التحقيق القضائي اللازمة لكشف الحقيقة في مجال الجرائم المعلوماتية، إذا ما تعذر على قاضي التحقيق القيام بها بنفسه، وذلك بعد ندبهم من قبل هذا الأخير حسب الشروط القانونية المنصوص عليها في المواد من138إلى142من قانون الإجراءات الجزائية، وعلى قاضي التحقيق عند إنتهاء هؤلاء من أعمالهم مراجعة عناصر التحقيق[5]" ولقد أجاز المشرع حسب مضمون الفقرة الأخيرة من المادة05من قانون04-09المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وسبل مكافحتها، وفي سبيل تخطي عقبات انعدام المعرفة الفنية بالنظم المعلوماتية من قبل ضابط الشرطة القضائية، لهؤلاء أن يقوموا بتسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث بقصد مساعدتهم وتزويدهم بكل المعلومات الضرورية لإنجاز مهامهم دون أن تتعرض الإجراءات المتخذة للبطلان، وهو ما أكدته المادة 65 مكرر 8 قانون06-22 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

[5]- الفقرة 06 و07 – المادة 68 ق 01-08 قانون الإجراءات الجزائية الجزائري

المطلب الثالث: الإختصاص النوعي للجهات القضائية (النيابة العامة – قضاء التحقيق)

- **أولا: جهة النيابة العامة:**

تعتبر النيابة العامة السلطة المختصة بمباشرة الدعوى العمومية باسم المجتمع، ويتولى النائب العام مهمة تمثيل النيابة العامة أمام المجالس القضائية وتتولى مهمة المطالبة بتطبيق القانون[6]، فيما يمثلها لدى المحكمة وكيل الجمهورية أو أحد مساعديه.[7]

وتتولى النيابة العامة ممثلة في شخص وكيل الجمهورية إدارة نشاط الضبطية القضائية كما يتمتع هو نفسه بكافة السلطات والصلاحيات المرتبطة بصفة ضابط شرطة قضائية، فيتولى مباشرة أو الأمر بمباشرة جميع الإجراءات اللازمة للبحث والتحري عن الجرائم بما في ذلك الجرائم المعلوماتية.[8]

وله في حال مباشرة الإجراءات الخاصة بالبحث والتحري في الجرائم المعلوماتية حسب أحكام المادة35مكرر من قانون الإجراءات الجزائية المستحدثة بموجب الأمر 15-02 المؤرخ في23جويلية2015، ومضمون الفقرة الأخيرة من المادة 05 قانون04 – 09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وسبل مكافحتها، أن يستعين بمساعدين متخصصين في مجال المعلوماتية تحت مسؤوليته ،من أجل مساعدته في المسائل الفنية المتعلقة بالجريمة محل المتابعة، وذلك بعد إطلاعهم على ملف الإجراءات المتخذة، وبعد أداءهم القسم المتعلق بالحفاظ على سرية المعلومات، ويقدمون اعمالهم في شكل تقارير تلخيصية او تحليلية تتضمن النتائج المتوصل إليها بناء على إلتماسات النيابة العامة، وهو الإجراء الذي يهدف حسب رأينا إلى تحفيز أعضاء النيابة العامة على التعامل بصفة مباشرة مع الجرائم المعلوماتية من أجل إكتساب الخبرة والمهارات اللازمة في التعامل معها بصفة فورية و سريعة ،ربحا للوقت و عدم تفويت فرصة إحراز الأدلة في الوقت

---

[6]- المادة 29 قانون الإجراءات الجزائية الجزائري

[7]- المادة 34 و 35 قانون الإجراءات الجزائية الجزائري.

[8]- المادة 36 قانون الإجراءات الجزائية الجزائري المعدلة بموجب الأمر 15-02 المؤرخ في 23 جويلية 2015

المناسب قبل إتلافها من قبل الجناة أو ضياعها نظرا لطابعها الإلكتروني، بدل إصدار الأمر بإحالتها على الوحدات الخاصة بمكافحة الجرائم المعلوماتية وما يترتب على ذلك من توفير فرصة للجاني في إتلاف الأدلة ومحوها، بسبب طول المدة بين وقوع الجريمة ووقت إكتشافها وإنطلاق الإجراءات بشأنها.

- **ثانيا: اختصاص جهة التحقيق:**

يختص قاضي التحقيق بإجراءات البحث والتحري اختصاصا أصيلا حسب ما تقضي به المادة38 من الأمر 69–75 قانون الإجراءات الجزائية الجزائري، ويختص بالتحقيق في الجرائم إما بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في (المادتين 67 و 73 من نفس القانون).

ووفق ما تنص عليه المادة 68 ق 01–08 من قانون الإجراءات الجزائية فإن قاضي التحقيق يقوم باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الإقناع و أدلة النفي، وإذا كان من المتعذر عليه القيام بها بنفسه جاز له أن ينيب ويندب ضابط الشرطة القضائية للقيام بتنفيذ جميع أعمال التحقيق اللازمة ضمن الشروط المنصوص عليها قانونا حسب المواد138إلى192 قانون الإجراءات الجزائية، بما في ذلك الجرائم المعلوماتية، بما أن النص كان عاما وشاملا ولم يهدف بالتحديد والتخصيص لنوع الجرائم الجائز التحقيق فيها.[9]

[9]– ما تنص عليه الفقرة الأخيرة من (المادة 05 ق 04 – 09 (المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وسبل مكافحتها فإن قاضي التحقيق وفي حال توليه إجراءات التحقيق بنفسه بشان الجريمة المعلوماتية فله ان يستعين بكل شخص له دراية بعمل المنظومة المعلوماتية محل التفتيش بقصد مساعدته على إنجاز مهمته.

المطلب الرابع: الإختصاص الإقليمي في الجرائم الالكترونية:

أن مبدأ الإقليمية يحدد مبدا مستقر يحدد على أساسه تطبيق السيادة والاختصاص على أساس المكان والذي يعني خضوع الجرائم التي تقع في إقليم الدولة لقانونها الجنائي النافذ وتصبح محاكمها صاحبة الولاية بنظر الدعوى الناشئة عنها ولا تخضع لسلطان أي قانون أجنبي، وفي المقابل فلا مجال لان يمتد سريان القانون خارج نطاق سيادة الدولة الإقليمي وفقا لحدودها المعترف بها. تبرز أهمية تحديد القانون الواجب التطبيق والمحكمة المختصة في مجال الجرائم المرتكبة عبر الانترنت جراء البعد عبر الوطني الذي تتميز به هذه الجريمة، لأن غالبية الأفعال ترتكب من خارج الحدود أو أنها تمر عبر شبكة الانترنت، وهو ما يبرز أهمية اختيار مدى ملائمة قواعد الاختصاص والقانون الواجب التطبيق.

1-تحديد القانون الواجب التطبيق: (في نطاق مبدأ إقليمية النص الجنائي)

تختص المحاكم الجزائرية بالنظر في الجرائم التي تقع كلها أو جزء منها على إقليمها أيا كانت صفة الشخص المتهم وبغض النظر عن جنسيته.[10]

ويرتبط قانون العقوبات في أية دولة ارتباطا وثيقا بسيادتها بل في الحقيقة اهم مظهر للدولة على اقليمها، فيعد مبدأ إقليمية النص الجنائي معتمد في التشريعات الجنائية ومن مبادئ قوانين كل دول العالم. فتبنى القانون الجزائري هذا المبدأ أيضا فتنص المادة3 من قانون العقوبات "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية، كما تطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجزائية" ونصت المادة586من قانون الاجراءات الجزائية " تعتبر الجرائم مرتكبة في الإقليم الجزائري كل جريمة يكون عملا من الأعمال المميزة لأحد أركانها قد تم بالجزائر" كما نصت المادة15من القانون04/09المتضمن للقواعد

[10]- زهية معمش نسمة غانم الثبات الجنائي في الجرائم الالكترونية مذكرة الماستر تخصص قانون الخاص والعلوم الجنائية جامعة عبد الرحمان ميرة بجاية2012-2013.

الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها" وفضلا عن قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية او الدفاع الوطني أو المصالح الاستراتيجية للإقتصاد الوطني". (في نطاق مبدأ العينية للفعل المجرم بالنص الجنائي) يقصد بمبدأ العينية تتبع التشريع الجنائي الوطني للجمهورية ليطبق على بعض الجرائم بعينها والعقاب عليها رغم عدم وقوعها على الإقليم الوطني التي ترتكب في الخارج، بصرف النظر عن جنسية مرتكبها وبالعودة إلى صورة الجريمة الالكترونية واركانها التي نص عليها المشرع الجزائري سواء تعلق الأمر بجريمة الدخول غير المشروع في نظام المعالجة الآلية للمعطيات أو إعاقة أو تحريف تشغيل نظم المعالجة عن طريق التعطيل أو التوقيف لنظم المعالجة الآلية للمعطيات باستخدام فيروسات او عن طريق إدخال أو محو أو تعديل بيانات نظم المعالجة الآلية للمعطيات قد تمت بالجزائر. فالمشرع اعتبرها جرائم مرتكبة بالجزائر وإن كانت النتيجة لم تقع بالجزائر.

المبحث الثاني: الإجراءات الخاصة بالبحث والتحري في الجريمة الالكترونية.

الجريمة المعلوماتية وكغيرها من أنواع الجرائم الأخرى، تمر بذات مرحلتي الإستدلال والتحقيق القضائي، وما يترتب على ذلك من إجراءات قانونية وفنية وشكلية ويعتبر إجراء التحقيق القضائي، هو الأساس في مجال البحث والتحقيق المعلوماتي، وذلك لما يكتسبه هذا الأخير من أهمية قصوى في مجال إستخلاص الحقائق بشأن الجريمة، لكن تبقى الإجراءات الأخرى الخاصة بمرحلة الإستدلال أو التحري الفنية منها خصوصا ضرورية لأجل إستكمال متطلبات التحقيق القضائي في مجال الجريمة المعلوماتية.[11]

يختص ضباط الشرطة القضائية بمسألة التحري بشأن الجرائم التقليدية والمعلوماتية الالكترونية على حد سواء، وتختلف طرق مواجهة كل منها، فالأخيرة تتميز بطبيعة خاصة إذ أن أدلتها غير محسوسة ويحتاج أمر التحري بشأنها إلى خبرات قضائية فنية وتقنية عالية، وذلك على مستويين: الجريمة المعلوماتية وكغيرها من أنواع الجرائم الأخرى، تمر بذات مرحلتي الإستدلال والتحقيق القضائي، وما يترتب على ذلك من إجراءات قانونية وفنية وشكلية ويعتبر إجراء التحقيق القضائي، هو الأساس في مجال البحث والتحقيق المعلوماتي، وذلك لما يكتسبه هذا الأخير من أهمية قصوى في مجال إستخلاص الحقائق بشأن الجريمة، لكن تبقى الإجراءات الأخرى الخاصة بمرحلة الإستدلال أو التحري الفنية منها خصوصا ضرورية لأجل إستكمال متطلبات التحقيق القضائي في مجال الجريمة المعلوماتية ويختص ضباط الشرطة القضائية بمسألة التحري بشأن الجرائم التقليدية والمعلوماتية على حد سواء، وتختلف طرق مواجهة كل منها، فالأخيرة تتميز بطبيعة خاصة إذ أن أدلتها غير محسوسة ويحتاج أمر التحري بشأنها إلى خبرات قضائية فنية وتقنية عالية، وذلك على مستويين:

[11]– عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية، دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية، مرجع سابق– ص 67

• **التحري عن الجرائم المعلوماتية قبل وقوعها؛**

وذلك من خلال تبني تكتيك المراقبة الدورية للشبكات والنظم المعلوماتية، وكذلك مراقبة أعمال مقاهي الأنترنت للحيلولة دون وقوع إعتداءات معلوماتية.

•**التحري عن الجرائم المعلوماتية بعد وقوعها؛**

أي إتخاذ كل الإجراءات التي تخص معاينة مسرح الجريمة من أجل إحراز الدليل الواضح والذي يمكنهم من نسبة الجريمة إلى فاعلها.

تتجلى الصعوبة في هذا الخصوص في حال وقوع الجريمة على برامج الحاسوب أو بواسطة شبكة الأنترنت، ففي هذه الحالة يواجه ضباط الشرطة القضائية إشكالية فقدان الأثار بسبب إمكانية محوها أو تدميرها في مدة قصيرة من قبل أي شخص يتردد على مكان الجريمة، فما هي يا ترى الإجراءات التي تتخذها الجهات الخاصة بمهام البحث والتحري بشأن الجرائم المعلوماتية والتي تسمح لهم بتحصيل الدليل؟ سنحاول الإجابة عن هذه الإشكالية من خلال تعرضنا للمسائل التالية وهي مسائل الكشف عن الجرائم والتبليغ عنها (المطلب الأول)، الإجراءات الخاصة المتبعة التي يجب إتخاذها قبل الإنتقال لمعاينة مسرح الجريمة (المطلب الثاني)، وفي المطلب الثالث إجراءات خاصة بمعاينة مسرح الجريمة الإلكترونية وأخيرا نتعرض للإجراءات خاصة بالتفتيش والضبط للأدلة.

المطلب الأول: آليات الكشف والتبليغ عن الجرائم المعلوماتية.

كما سبق وان فصلنا بشأن خصوصيات الجريمة المعلوماتية، فقد أكدنا على طابعها الخفي فهي نادرا ما تكون تحت وصف حالة التلبس إن لم نقل أن ذلك امر مستحيل، فالمجرم المعلوماتي يبذل كل ما في وسعه للإبقاء على جريمته خفية، و ما يجعل من امر كشفها والتبيلغ لاحقا عنها، فما هي آليات الكشف عن هذه الجرائم، و كيف يتم التبيلغ و التعامل مع التبليغات بشأنها من قبل الجهات المختصة؟

الفرع الأول: آليات الكشف عن الجرائم المعلوماتية.

إن الإشكال الذي يواجه أجهزة الأمن والمحققين من رجال الضبطية القضائية، هو أن الجرائم المعلوماتية–الإلكترونية لا تصل إلى علم السلطات المعنية بالصور العادية، وذلك لصعوبة إكتشافها من قبل الأشخاص العاديين وحتى المؤسسات والشركات لا تكتشف هذه الجرائم فور وقوعها على إعتبار أن أغلبها لا يراجع حساباته بشكل يومي، وحتى وإن تم ذلك بشكل يومي أو شهري فإنه يصعب عليها التأكد من الفوارق في الأرقام التي تبدو عادة خسائر أو ديون أو حتى في حال إكتشافها فإن أغلب تلك الشركات تتردد في التبليغ خوفا على سمعتها.[12]

وهنا تظهر أهمية دور الأجهزة الأمنية في رصد حركة مرتكبي جرائم المعلوماتية واكتشاف هذه الجرائم من خلال الرصد الميداني لحركة المعاملات التجارية ومراقبة المشبوهين داخل المؤسسات المالية وحولها، فالقدرة على الملاحظة وقراءة تصرفات الأشخاص العاملين في مجال المعلوماتية، والمهتمين بالبرامج، وهواة صناعة الأنظمة هي أولى خطوات السيطرة الأمنية على نشاط مرتكبي جرائم الحاسوب ويتعزز كل ذلك من خلال تكثيف المراقبة من قبل الوحدات الخاصة لمكافحة الجريمة المعلوماتية في الأماكن وحول الفئات التالية:

- أسواق أجهزة الحواسيب والبرامج المعلوماتية
- الرصد الدقيق لحركة المترددين على المواقع المذكورة أعلاه .
- الرصد الدقيق لحركة المشبوهين في مجال جرائم الأموال وتجار المخدرات.
- الرصد الدقيق لحركة معتادي جرائم التزوير و الإحتيال و معتادي الإجرام المعلوماتي.

[12]– ضياء علي أحمد النعمان، مرجع سابق– ص364 .

إن هذا القدر من التواجد الميداني المنظم يضمن تغطية أمنية على منافذ المعلومات والحاسوب وله أثر وقائي ورادع في نفس الوقت، كما يسمح بتوفير المعلومات الأولية عن الجرائم المعلوماتية قبل وقوعها كما يضمن سرعة التبليغ عنها واتخاذ الإجراءات بحقها.[13]

الفرع الثاني: كيفية التعامل مع التبليغ بشأن الجرائم المعلوماتية.

البلاغ هو إخطار السلطات المختصة بوقوع جريمة، وهذا الإخطار واجب أدبي يتقيد به المواطن الصالح سواء وقعت الجريمة عليه أو على غيره، إن أهمية التبليغ تعطي للمجني عليه ولغيره من الأفراد في الجرائم المعلوماتية دور لا يستهان به لأنه قد يكون السبيل الوحيد لكشف هذه الجرائم، وهو دور يعطي الفرصة لأجهزة الضبطية القضائية فرصة التحرك بسرعة من أجل مواجهة الجريمة المعلوماتية[14]، ويعتبر عدم الإبلاغ سببا رئيسيا في تفاقم الجرائم المعلوماتية.

فالتبليغ هو المشكلة الحقيقية التي واجهت الجهات المختصة بمواجهة الجريمة المعلوماتية، فغالبية الهيئات فالمؤسسات تخشى الإبلاغ عن الجرائم المعلوماتية خوفا من فقدان عملائها وهو ما ينتج عنه إفلات مرتكب الجريمة بفعلته. [15]

والتبليغ هو إخبار السلطات المختصة عن وقوع جريمة، أو أنها على وشك الوقوع، أو كان هناك إتفاقا جنائيا، أو أدلة أو قرائن أو عزما على إرتكابها، أو وجود شك أو خوف من أنها ارتكبت.[16]

---

[13]- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية، دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية، مرجع سابق- ص 72 – 75.

[14]- عياد الحلبي، مرجع سابق- ص 192.

[15]- سعود بن محمد السراني، مرجع سابق- ص 67.

[16]- نبيلة هبة هروال ، مرجع سابق- ص 177.

وفي هذا الصدد نصت الفقرة الأولى من المادة 17 المعدلة بموجب الأمر 15-02 من قانون الإجراءات الجزائية الجزائري على أنه " يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12و 13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الإستدلالات وإجراء التحقيقات الإبتدائية" تقابلها نص المادة17 من قانون الإجراءات الجزائية الفرنسي والمادة 24 من نظيره المصري و 27 من نظام الإجراءات الجزائية السعودي.

والتبليغ عن الوقائع الجنائية حق لكل شخص بل هو واجب مفروض عليه فلا يصح معاقبته واقتضاء التعويض منه، إلا إذا تعمد الكذب، وتوافرت في شأنه أركان جريمة البلاغ الكاذب. ويتكفل ضباط الشرطة القضائية بتلقي البلاغات ومباشرة الإجراءات المتعلقة بالتحقيقات الإبتدائية، ولهم الحق في سبيل ذلك طلب مساعدة القوة العمومية أثناء تنفيذ مهامهم، وتختم أعمالهم بإعداد محاضر ترسل إلى وكيل الجمهورية لأجل إخطاره بالجنح والجنايات التي تصل إلى عملهم.[17]

ويستحب أن يكون المبلغ في الجريمة المعلوماتية على درجة مقبولة من الإلمام والمعرفة بالجو انب الفنية للحاسوب، حتى يتمكن من تقديم معلومات تصف الحادث بالشكل الذي يمكن معه لضباط الشرطة القضائية من مباشرة البحث والتحري عنها، وهو ما يستلزم أن يكون متلقي البلاغات على قدر من المعرفة بالجوانب المعلوماتية، حتى سيضع مناقشة المبلغ في الكثير من جوانب الجريمة محل البلاغ.[18]

ويتم التبليغ باعتباره أولى خطوات إجراءات البحث والتحقيق المعلوماتي من خلال:

• تلقي جهات الضبطية القضائية معلومات أمنية تشير إلى ممارسته (شخص معروف أو غير معروف) أنشطة معلوماتية محظورة.

[17]- المادة 17 المعدلة بموجب الأمر 15-02 والمادة 18 من قانون الإجراءات الجزائية الجزائري.

[18]- خالد عياد الحلبي، مرجع سابق-ص 193.

• توفر معلومات عن انتشار الفيروسات التخريبية عبر شبكة الإنترنت .

• ضبط شخص بحيازة مستندات أو محررات مزورة أو بطاقات ائتمان مزورة.[19]

الفرع الثالث: كيفية التبليغ عن الجرائم المعلوماتية.

إن التبليغ عن جرائم المعلوماتية لا يختلف عما هو عليه الحال في مجال الجرائم التقليدية، غير أنه يتمتع بنوع من الخصوصية يتماشى و طبيعة هذه الجرائم، فالبلاغ في هذه الحالة قد يتم عن طريق شبكة الأنترنت أو ما يعرف بالبلاغ الإلكتروني، وذلك بإطلاع الهيئات المختصة بالبحث و التحري بواسطة رسالة إلكترونية عن وجود أعمال غير مشروعة، أو عن موقع ينشر صورا جنسية للأطفال هو ما يوفره البريد الإلكتروني للدرك الفرنسي من خلال البريد الإلكتروني: judiciare@gendaremeriedefense.gov.fr بإعتباره الجهة المختصة بالتحري والتحقيق في شأن هذه الجرائم في فرنسا، وكذلك الحال في مصر من خلال الإتصال بموقع شرطة إدارة مكافحة جرائم الحاسب وشبكات المعلومات في مصر.

قد يكون التبليغ من خلال ملئ المبلغ لإستمارة رقمية على الموقع المخصص لتلقي البلاغات والشكاوي كذلك التى يوفرها الموقع الرسمي لأنترنت الأحداث في فرنسا www.intrenet.miners.gov.fr، أو تلك المتوفرة على موقع إدارة مكافحة جرائم الحاسبات و شبكات المعلومات المصري على الرابط التالي: www.ccd.gov.eg .

وهي الإمكانية المتاحة على المستوى الوطني من خلال إمكانية التبليغ التي تتيحها المواقع الخاصة بالجهات الأمنية كجهاز الشرطة والدرك الوطني، هذا الأخير الذي يضع تحت تصرف المواطنين البريد الإلكتروني لأجل التواصل مع هذه الجهات والتبليغ عن كافة

[19]– عبد الله بن سعود محمد السراني، مرجع سابق– ص ص 182 – 183 .

الجرائم والجرائم المعلوماتية، وذلك عبر البريد الإلكتروني من خلال العنوان الإلكتروني: ccom-cgn@mdn_dz، او من خلال الخدمة التي أصبحت متاحة منذ07أفريل2015 المتعلقة بإيداع الشكاوى أو المعلومات المتعلقة بالجرائم عبر الموقع الالكتروني المستحدث من قبل هيئة الدرك الوطني على العنوان التاليhttps://ppgn.mdn.dz ، وهو مايوفره كذلك موقع المديرية العامة للامن الوطني على موقعه www.dgsn.dz الذي يمكن لأي شخص من التبليغ وبصفة تضمن سرية هويته، عن اي جنحة او جناية وذلك بهدف تشجيع الغير على التبليغ عن الجرائم بما فيها المعلوماتية، ويبقى للمبلغ حرية الإختيار في الأخير بين الأسلوب التقليدي أو الإلكتروني.

وتظهر أهمية تلقي البلاغات في أنها تساعد رجال البحث والتحري على تحديد نوع الجريمة المبلغ عنها ان كانت تندرج ضمن الجرائم المعلوماتية، وكذلك وضع تصور مبدئي لخطة العمل المناسبة للبحث والتحري بشأن الجريمة، وبالتالي تحديد نوع الخبرة المطلوبة لأجل المعاينة وتحريز الأدلة وما يجب التأكيد عليه ان جهة تلقي البلاغ يجب عليها ان تحرص على ان يقوم المبلغ بالخطوات التالية :

- تجهيز قائمة بأسماء العاملين في المؤسسة أو المشتبه فيهم.
- تجهيز نسخة إحتياطية من بيانات الأجهزة المتضررة.
- عدم تبليغ أي أحد آخر بالجريمة الواقعة.

المطلب الثاني: الخطوات الأولية لمباشرة أعمال البحث والتحري عن الجرائم الالكترونية.

تعتبر الجريمة المعلوماتية من قبيل الجرائم الخفية، أي أنها عبارة عن أنشطة إجرامية تتم في سرية باعداد تخطيط مسبق وتنفيذ بطريقة مدروسة من قبل مجرمين متمرسين في عالم الجريمة تجمعهم مصلحة عدم إبلاغ السلطات المختصة عن نشاطهم الإجرامي.[20]

وفي حالة الإبلاغ أو تقديم شكوى عن نشاط هؤلاء المجرمين لدى السلطات المختصة ممثلة في المصالح الأمنية والقضائية، فإن هذه الأخيرة تباشر أعمال الإستدلال والتحري بشأن الجرائم محل البلاغ أو الشكوى فيبادر ضباط الشرطة القضائية بدءا وقبل كل شيء بالتأكد من الفرضيات التالية في إطار أداء مهامهم:

الفرع الأول: الإجراءات الأولية لكشف حقيقة الجريمة.

قبل مباشرة إي إجراء وإتقاءا لتضييع الجهد بشأن جريمة لم تقع، أو كانت محل تبليغ كاذب، يباشر ضباط الشرطة القضائية إلى التأكد من؛

أولا: التأكد من وقوع جريمة فعلية:

فلا بد من أجل ضمان صحة الإجراءات الخاصة أن نكون أصلا بصدد جريمة إلكترونية سواء تحت وصف جنحة أو جناية أي استيفاء الركن الشرعي.*

ثانيا: توفر دلائل تشير إلى إتهام شخص معين:

ينبغي أن تتوفر في الشخص المشبه فيه دلائل كافية تدعوا للإعتقاد بأنه ساهم في ارتكاب الجريمة مما يستوجب إتهامه فيها، وفي مجال الجرائم المعلوماتية يمكن القول بأن

[20]- محمد محمد محمد عنب، إستخدام التكنولوجيا الحديثة في الإثبات الجنائي، مصر–2007 – ص 17

*- راجع المواد من394 مكرر إلى 394 مكرر 07 قانون العقوبات الجزائري.

تعبير الدلائل الكافية يقصد به مجموعة من المظاهر والصفات التي تقوم على المضمون المنطقي لملابسات الجريمة وخبرة المحقق.

ثالثا: توفر دلائل كافية وقرائن قوية على حيازة المشتبه فيه لأشياء تفيد في كشف الحقيقة:

فلا يكفي لمباشرة تحريات جدية، الحصول على الإذن القانوني فقط، بل يجب أن تتوفر لدى المحقق أسباب كافية بأنه يوجد في مكان ما أو لدى المشتبه فيه أدوات استخدمت في الجريمة المعلوماتية أو أدلة إلكترونية لها فائدة في إستجلاء الحقيقة.

في حال توفر هذه الشروط جاز لأعضاء فريق التحقيق المعلوماتي مباشرة أعمالهم بشأن الجريمة المعلوماتية من خلال تحديد ملابساتها وهوية مرتكبها من خلال إجراءات تسبق عملية الإنتقال لأجل المعاينة المادية لمسرح الجريمة لسبب وحيد وهو أن غالبية الجرائم المعلوماتية هي جرائم غير ملتبس بها، أي أن أعمال البحث والتحقيق بشأنها عادة ما تنطلق متأخرة بعد وقوعها فهي جرائم خفية تحتاج الى خبرات فنية هائلة للكشف عنها ويتبع فريق التحقيق مجموعة من الإجراءات العملية الخاصة.

الفرع الثانى: إجراء الإرشاد الجنائي.

يعد الإرشاد الجنائي من أهم المصادر التي يعتمد عليها ضباط الشرطة القضائية في عمليات البحث و التحري لجمع المعلومات و خصوصا في مجال الجرائم المعلوماتية فنجد أن هيئات الضبطية أصبحت تجند عناصرها للدخول إلى العالم الافتراضي وبالخصوص إلى مواقع التواصل الإجتماعي و قاعات الدردشة خصوصا تلك المعروف عنها تطرفها وميول العدوانية، وذلك تحت أسماء مستعارة يقصد البحث عن الجرائم ومرتكبيها، فضباط الشرطة القضائية ما عليهم سوى الإتصال بالشبكة واعتماد أسلوب النقاش والدردشة الإلكترونية مع الغير ومختلف الهيئات و بمجرد بروز مؤشرات عن هوية المجرم المعلوماتي أو جرائم

المعلوماتية كالاحتيال أو الإستغلال الجنسي للأطفال، يبادر هؤلاء إلى سؤاله مثلا عن طرق الحصول على بطاقات الإئتمان المزورة أو عن مواعيد استدراج الأطفال وهي المعلومات التي يستعين بها مزود الخدمة بالإنترنت الذي يمكن أن يوفر بواسطة برمجيات خاصة مكان وجود المجرم و مثال ذلك ما قامت به المباحث الفيدرالية الأمريكية FBI التي استطاعت الإطاحة بشبكة(LAND-FAST)التي تمتهن القرصنة المعلوماتية والمتاجرة بها عبر شبكة الأنترنت، و ذلك من خلال دس مرشد معلوماتي ضمن أعضاء هذه الشبكة[1].

وقد أتاح التشريع الجزائري اللجوء إلى هذا الأسلوب حسب ما نصت عليه المادة 65 مكرر 05 ق 06-22 إلى غاية المادة 65 مكرر 18 من قانون الإجراءات الجزائية، وذلك في حالة الجرائم المعلوماتية، بعد الحصول على إذن مسبب من وكيل الجمهورية أو قاضي التحقيق وتحت رقابة الأول لمدة 04 أشهر قابلة للتجديد.

الفرع الثالث: إجراء الوضع تحت المراقبة الإلكترونية.

يجب الإشارة أولا أن المراقبة على أي وسيلة من وسائل الاتصالات تعد بمثابة اعتداء على حرمة الحياة الخاصة فهو حق محمي دستورا.[21]

ومشمول بالحماية القانونية التي تقر بأن الاتصالات مهما كان شكلها مكفولة سرا ولا يجوز مصادرتها أو الاطلاع عليها إلا بأمر قضائي مسبب، ويعد فعل مراقبتها أو تسجيلها أو بثها جريمة معاقب عليها، والمراقبة الإلكترونية هي عملية يقوم فيها المراقب بتتبع المشتبه فيه بواسطة الأجهزة الإلكترونية، و إفراغ ما تسفر عنه في تقارير أمنية، وتلك التقارير تفرغ في ملف إلكتروني يحدد فيه الزمان والمكان الذي تمت فيه والنتيجة التي أسفرت عنها.[22]

[21]- تنص المادة 39 من دستور الجمهورية الديمقراطية الشعبية لسنة 1996 على أنه: " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون ، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

[22]- ناير نبيل عمر، مرجع سابق- ص 149

والحقيقة أن المشتبه فيه المراقب من قبل فريق التحقيق هو شبكة الانترنت أو البريد الالكتروني، إذ يتم من خلالها مراقبة اتصالاته الالكترونية المشتبه فيها، والتقنية المستخدمة في هذا المجال هي التقنية الالكترونية البحتة، والتي تعني مجموعة الأجهزة المتكاملة مع بعضها بغرض تشيكل مجموعة من السمات المتعلقة بالمجرمين أو المشتبه فيهم، وفق برنامج موضوع مسبقا لتحديدهم من أجل ضبطهم وجمع الأدلة قبلهم لإثبات إدانتهم وتقديمهم أمام المحكمة.

وقد نص التشريع الإجرائي الجنائي الجزائري على إمكانية الوضع تحت المراقبة الالكترونية في مجال مكافحة الجرائم المعلوماتية حسب نصوص المواد65مكرر5إلى مكرر10قانون06-22، وذلك تحت الفصل الرابع الموسوم باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، بحيث يجوز لوكيل الجمهورية وكذلك لقاضي التحقيق في حال فتح تحقيق قضائي، منح إذن لضابط الشرطة القضائية المكلفين بالبحث والتحري عن الجرائم المعلوماتية، يتضمن اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية دون موافقة المعنيين بها، ويشترط في الإذن أن يكون مكتوبا ومتضمنا لكافة العناصر الأساسية التي تسمح بالتعرف على الاتصالات المطلوب التقاطها وذلك لمدة أقصاها 04 أشهر قابلة للتجديد، ولصاحب الإذن الحق في تسخير أي عون عمومي أو خاص لدى هيئة الاتصالات السلكية أو اللاسلكية من أجل التكفل بالجوانب التقنية المتعلقة بالعملية، وتختتم العملية بإعداد محضر من قبل ضابط الشرطة القضائية يتضمن مضمون العملية مع توضيح تاريخ وساعة بداية العملية وانتهائها.

وقد تعزز اللجوء إلى هذا الأسلوب سنة2009 بموجب نص كل من المادتين 03 و04 الواردتين ضمن فصول القانون 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها اللتان عبرتا صراحة عن إجازة مباشرة إجراء الرقابة الإلكترونية فيما تعلق بالجرائم المعلوماتية، ولكن دون ذكر الهيئة

المكلفة بتولي ذلك وقد إستمر الوضع كذلك إلى غاية صدور المرسوم الرئاسي 15-261 الذي يحدد تشكلية وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بتاريخ 08 أكتوبر 2015، أصبحت هذه الأخيرة حسب مضمون الفقرة 05 من نص المادة 04 من المرسوم الرئاسي 15-261، الهيئة المختصة بتنفيذ عمليات المراقبة الإلكترونية للإتصالات*.

من خلال إستحداث مديرية المراقبة الوقائية واليقظة الإلكترونية التي يدخل في صميم إختصاصاتها القيام بمهام المراقبة الإلكترونية للإتصالات من أجل الكشف عن الجرائم المعلوماتية بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها، حسب ما تقره المادة 11 من المرسوم الرئاسي 15-261، كما منحها القانون حسب نص المادة 21 من المرسوم السالف الذكر الصفة الحصرية لتولي مهام المراقبة الإلكترونية في حال تصنيف الجريمة المعلوماتية ضمن الجرائم الإرهابية والتخريبية والماسة بأمن الدولة دون سواها من الهيئات الوطنية الأخرى وذلك تحت سلطة قاض مختص.

وتنفذ عادة عملية المراقبة والتتبع الإلكتروني في مجال الجرائم المعلوماتية من خلال الاستعانة ببعض الوسائل التقنية نذكر منها :

أولا: تقنية تتبع عنوان IP- TCP : عنوان IP هو العنصر المسؤول عن تراسل الحزم البيانية عبر شبكة الانترنت وتوجيهها إلى أهدافها، ويعتبر بمثابة عنوان الحاسوب المتصل بالشبكة ويتكون من شفرة رقمية تتكون من أربع 04 أجزاء، يشير الأول إلى المنطقة الجغرافية والثاني لرمز مقدم الخدمة، والثالث لمجموعة الحواسيب المرتبطة والرابع يخص الحاسوب الذي يتم الاتصال منه، ولذلك وفي حالة وجود جريمة معلوماتية فإن ضباط

*- الإلكترونية يقصد بالاتصالات الإلكترونية كل تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية بما في ذلك وسائل الهاتف الثابت والنقال المادة 05 فقرة 01 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

الشرطة القضائية ضمن فريق التحقيق يقومون بتتبع عنوان IP للجهاز مصدر الجريمة وتحديد موقعه.[23]

ثانيا: استخدام تقنية فحص البروكسي (PROXY): البروكسي هو الوسيط العامل بين الشبكة والمستخدم، تستخدمه الشركات المقدمة لخدمة الاتصال لأجل إدارة الشبكة، وضمان أمنها وتوفير حزمة الذاكرة الجاهزة (Memory) يعمل البروكسي على تلقي طلب المستخدم للبحث عن صفحة ما فيتحقق البروكسي ضمن الذاكرة الجاهزة عما إذا جرى تنزيل الطلب من قبل فيقوم بإعادة إرسالها للمستخدم دون الحاجة إلى طلبها من الشبكة العالمية للمعلومات webمن أجل تزويد المستخدم بها، ومن مزاياه أن ذاكرته هذه يمكن أن تحتفظ بتلك المعلومات والعمليات، وهو ما يمنح لضباط الشرطة القضائية فحصها واستخلاص الدلائل ضد المتهم وذلك من خلال تقفي أثاره بمساعدة مزود الخدمات.

ثالثا: استعمال برامج التتبع المعلوماتية: تقوم برامج التتبع على شاكلة برنامج (TRACER–HACK) لاختراق ومن قام بها، واشعار الجهة المتضررة بذلك، وهذه البرامج عادة ما تكون ٍ بالتعرف على محاولات ساكنة في خلفية المكتب، عندما ترصد أي محاولة للقرصنة أو الاختراق وتسارع بغلق منافذ الدخول للمخترق، ثم تبدأ بعملية مطاردته واقتفاء أثره وصولا إلى تحديد عنوانه الإلكتروني (IP)واسم الشركة المزودة بخدمة الانترنت ومعلومات أخرى.

رابعا: الاستعانة بنظام كشف الاختراق(SYSTEM DETECTION INTRUSION): وهو النظام الذي يرمز له ب S.D.I وهو نظام يعتمد على مجموعة من البرامج التي تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب أو الشبكة مع تحليلها بحثا عن أي إشارة قد تدل على وجود مشكلة تهدد أمن الحاسوب والشبكة

[23]– بن محمد السراني– مرجع سابق– ص 51.

من خلال مقارنة نتائج التحليل مع الصفات المشتركة للاعتداءات المعلوماتية، ففي حال استئناف أب منها يبادر لتسجيلها في سجلات حاسوبية خاصة registre) وهي السجلات التي يسعى لها ضباط الشرطة القضائية لتحليل أسلوب ارتكاب الجريمة وربما مصدرها.

خامسا: العمل بنظام جرة العسل: هو نظام حاسوبي مخصص لكي يتعرض للهجمات الإلكترونية عبر الشبكة، من خلال خداع من يقوم بذلك وذلك بإبداء سهولة في الاعتداء عليه وذلك لإغرائه، وذلك حتى يتمكن من جمع أكبر قدر من المعلومات عن أسلوب الهجوم وتحليله وهو ما يسمح باتخاذ الإجراءات الوقائية التي تزود فريق التحقيق بالمعطيات اللازمة التي توضح معالم الجريمة. سادسا: جمع الأدلة من خلال اعتراض رسائل البريد الالكتروني: وذلك من خلال الاستعانة ببرامج مصممة للبحث في مضمون الرسائل الالكترونية المتبادلة على شاكلة برنامج كارنيفور و1000 DCS الذي طورته المباحث الفيدرالية الأمريكية FBI) الذي يتعقب ويفحص رسائل البريد الالكتروني المرسلة والواردة عبر أي حاسوب خادم تستخدمه أي شركة توفر خدمة الانترنت وهو برنامج مستخدم في التحقيق في قضايا الأمن القومي الأمريكي.

كل هذه الأساليب والبرامج والأنظمة هي وسائل تساعد ضباط الشرطة القضائية في أعمال البحث والتحري ولكن يبقى أمر استخلاص نتائجها أمرا مرهونا بمدى التزام مقدم خدمة الانترنت بمد يد العون لأجل تحديد مكان ارتكاب الجريمة وهوية مرتكبها.

الفرع الرابع: التزامات مقدمي خدمات الانترنت في مجال مساعدة أعمال البحث والتحري.

يقصد بمزود الخدمات أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات لأجل التواصل بواسطة تقنية المعلوماتية، ويقوم بتخزين ومعالجة المعطيات بما فيها المعلومات الخاصة بالمشترك كنوع خدمة الاتصالات المستخدمة لديه، هويته، عنوانه البريدي، رقم هاتفه وذلك بناء على اتفاق ترتيب الخدمة القائم بينهما، حسب تعريف المادة

02 الفقرة 02 و09 من الاتفاقية العربية لمكافحة الجرائم المتصلة بالتقنية المعلوماتية كما يعرفه قانون حماية الحياة الخاصة في مجال الاتصالات الالكترونية الأمريكية ECDA) بأنه نوعان :

• **الأول مزودو خدمة الاتصالات الالكترونية؛** وهو كل من يقدم خدمة إلى مستخدمي الشبكة، ويعمل على تسهيل إرسال واستقبال الاتصالات السلكية و اللاسلكية و الالكترونية.

• **الثاني مزودو خدمة معالجة المعلومات عن بعد؛** وهو كل من يقدم للجمهور خدمة معالجة البيانات عن بعد بواسطة وسائل الاتصالات الالكترونية.

وبناء على ذلك فإذا أرسل أي شخص لآخر رسالة عن طريق البريد الإلكتروني فإنها تمر وبالضرورة على مزود الخدمة وتخزن لديه.

إن القانون قد سمح للسلطات المختصة بمتابعة الجرائم المعلوماتية حق طلب التحفظ على البيانات المخزنة لديها وحق كذلك تزويدها بالمعلومات الخاصة بالمشترك ونشاطه في إطار عملها المتعلق بأعمال البحث والتحري عن الجرائم المعلوماتية.

وهو الإجراء و الالتزام الذي نجد له أصلا قانونيا على المستوى الدولي حسب ما تقرره أحكام المادتين 16 و17 من اتفاقية بودابست لمكافحة الجرائم المعلوماتية، تقابلها المواد 23-24-25 من الاتفاقية العربية لمكافحة الجرائم المتصلة بالتقنية المعلوماتية، وقد وردت هذه الالتزامات على المستوى الوطني حسب ما جاء في نص المادة 10 من الفصل 04 من قانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ، التي توجب على مقدمي خدمة الانترنت مساعدة السلطات في إطار التحريات القضائية من خلال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المذكورة وكل ذلك تحت

غطاء السرية ، كما ألزمت المادة 11 من نفس القانون مقدمي الخدمات حفظ المعطيات التالية:

- **المعطيات التي تسمح بالتعرف على مستخدمي الخدمة.**
- **المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.**
- **المعطيات المتعلقة بالخدمات التكميلية المطلوبة.**
- **المعطيات التي تسمح بالتعرف على المرسل إليه وعناوين المواقع المطلع عليها.**

ويلزم حفظ هذه المعطيات لمدة سنة منذ تاريخ تسجيلها، وهي مدة طويلة مقارنة بمقترحات الاتفاقية العربية التي قدرتها ب 90 يوما أو بما يحدده الاتحاد الأوروبي وفق الأمر EC 46/95 بالمدة الضرورية، وهو الأجل الذي يسمح لضباط الشرطة القضائية بالرجوع إليها من أجل تحديد هوية وأماكن ارتكاب الجرائم المعلوماتية وذلك نظرا للاعتبارات التالية:

- **قابلية البيانات المعلوماتية للتلاشي والتلاعب والتغير.**
- **ارتكاب غالبية الجرائم عن طريق نظم الاتصالات وهو ما يساعد على تحديد هوية مرتكبي هذه الجرائم.**

التحفظ على هذه البيانات يعتبر أحد أهم عناصر الإثبات التي يمكن أن تكشف عن هوية مرتكبي هذه الجرائم.

ولضباط الشرطة القضائية إمكانية تقديم طلبات لمزودي الخدمة بالانترنت لأجل تزويدهم بالمعلومات المخزنة ومن ضمن هذه الطلبات:

- **طلب التحفظ المعجل على البيانات المخزنة وذلك حتى يتفادى المزود شطب التسجيلات و القضاء على الدليل.**
- **طلب تقديم بيانات معلوماتية خاصة بالمشترك.**
- **طلب اعتراض الاتصالات الالكترونية.**

إذن تعتبر هذه الإجراءات أهم الإجراءات ذات الطابع الإجرائي الفني والمعلوماتي في مجال أعمال البحث والتحري عن الجرائم المعلوماتية التي يباشرها ضباط الشرطة القضائية تنفيذا لتعليمات وكيل الجمهورية أو قاضي التحقيق أو اختصاصا منهم، وذلك من خلال ممارسة مهامهم بعيدا عن مسرح الجريمة أي في مرحلة تسبق التنقل للمعاينة والتفتيش المادي وضبط الأدلة الالكترونية والمادية وهي الإجراءات التي تختلف نوعا ما من حيث الوسائل والطرق وهي التي ستكون محل بحثنا في المطلب الموالي.

المطلب الثالث: الإجراءات الفنية الخاصة بمعاينة مسرح الجريمة المعلوماتية.

بعد أن تطرقنا إلى المسائل الخاصة بإجراءات البحث و التحري الأولية بشأن الجريمة المعلوماتية و التي يبادر إليها ضباط الشرطة القضائية، بمجرد الوصول إلى علمهم بوقوع الجريمة، تنتقل إلى تفصيل المسائل الخاصة بالإجراءات العملية ذات الطابع الخاص المتعلقة بمرحلة المعاينة والتفتيش والتي يتم عادة على مسرح الجريمة، والتي تقتضي تنقل الجهات المختصة من أجل تحقيق الهدف الرئيسي وهو إحراز ادلة المادية والإلكترونية، والتي من شأنها إثبات الادانة أو براءة المتهم، وعادة ما يتولى مهمة الاتنقل إلى مسرح الجريمة المعلوماتية، الفرقة الخاصة بالبحث والتحقيق في مسائل الجرائم المعلوماتية، نظرا لتوفرهم على معارف تسمح لهم بالتعامل الصحيح مع أدلتها، ولا يتم الانتقال إلى مسرح الجريمة إلا لفرضيتين اثنتان:

- **فرضية مداهمة مسرح الجريمة المتلبس بها**، وهو أمر مستبعد جدا إذا لم نقل نادرا، نظرا لخصوصية الجريمة و المجرم المعلوماتي، اللذان يتميزان بالخفاء و السرية في تنفيذ الجريمة إضافة إلى صعوبة كشفها.

- **فرضية تنفيذ المهام الموكلة لهم** إما من تلقاء أنفسهم بناء على بلاغ أو شكوى بشأن جريمة معلوماتية، أو تنفيذا لأوامر وكيل الجمهورية أو قاضي التحقيق، وهي الفرضية

الأقرب للتجسيد نظرا إلى ضرورة تضافر الجهود الفنية والقانونية لأجل مكافحة الجرائم المعلوماتية.

وعليه فإننا سنحاول أن نضع في هذا المطلب تصورا قانونيا تقنيا وفنيا لجملة الإجراءات الواجب إتباعها عند الانتقال إلى مسرح الجريمة المعلوماتية، بغرض ضبط الأدلة الإلكترونية وذلك حسب تسلسل الفروع التالية:

- الفرع الأول: الإجراءات الخاصة بالانتقال إلى مسرح الجريمة وتأمينه.
- الفرع الثاني: الإجراءات الخاصة بالتفتيش وضبط الأدلة الإلكترونية .
- الفرع الثالث: الأساليب الخاصة في التعامل مع الأشخاص ذو ي العلاقة بالجريمة المعلوماتية.

الفرع الأول: الإجراءات الخاصة بالانتقال إلى مسرح الجريمة وتأمينه .

إذا ثبت بناء على أعمال البحث والتحري الأولية التي قام بها ضباط الشرطة القضائية بشأن صحة فحوى البلاغات الواردة إليهم بشأن وقوع جريمة معلوماتية أو بناء على توفر حالة تلبس بالجريمة، أنه هناك أدلة قوية تشير إلى حيازة المشتبه فيه لأدلة تفيد في استجلاء الحقيقة، مخزنة على حاسوبه أو على وسائط خارجية أو مخبأة في مسكنه أو مقر عمله فإن هذا الأمر يستدعي و بالضرورة الانتقال إلى مسرح الجريمة المفترض لأجل إتمام أعمال البحث و التحري أو القيام بتنفيذ الأوامر القضائية الواردة من قاضي التحقيق كالأمر بالتفتيش، وان كانت الإجراءات الخاصة بالانتقال إلى مسرح الجريمة المعلوم نوعية بعض الشيء إلا أنها تخضع وبالضرورة لمجموعة من الشروط القانونية قبل كل شيء.

الشرط الأول: ضرورة إستيفاء الشروط القانونية لتنفيذ أمر الانتقال.

إن الانتقال إلى مسرح الجريمة وما يصاحبه من ضرورة المعاينة والتفتيش، يقتضي التعدي على حرمة الحياة الشخصية للأفراد ومساكنهم، يستوجب أن يتم في إطار قانوني

لأجل ضمان شرعية الإجراءات وعدم تعريضها للبطلان الذي قد يهدم الدليل ويتسبب في إفلات المتهم من العدالة، إضافة إلى ضمان عدم التعسف في مواجهة الغير من الأفراد بحجة ضرورة التحقيق، وتجنبا لكل ذلك يستوجب القانون على ضابط الشرطة القضائية احترام مجموعة من الشروط القانونية المبنية في قانون الإجراءات الجزائية وأخرى في القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، لأجل إتمام هذه الإجراءات ضمن إطار شرعي وذلك حسب الأحوال التالية:

أولا- حسب أحوال حالة التلبس: توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال أو عقب ارتكابها، كما تعتبر كذلك إذا كان الشخص المشتبه فيه في وقت قريب جدا من وقوعها أو تبعته العامة بالصياح أو كان حائزا لأشياء أو دلائل تدعوا إلى افتراض مساهمته في الجريمة، كما توصف كذلك إذا ما ارتكبت الجناية أو الجنحة في منزل أو كشف صاحب المنزل عنها عقب وقوعها وبادر باستدعاء ضابط الشرطة القضائية لأجل إثباتها.[24]

إن تطبيق هذه الأحوال على الجريمة المعلوماتية يكاد أن يكون أمرا مستحيلا، غير أنه يمكن افتراض وقوعها ولو في نادر الأحوال وهو ما يترتب عنه اتخاذ الإجراءات التالية:

•على ضابط الشرطة القضائية الذي بلغ بجناية أو جنحة متلبس بها مهما كان نوعها، أن يخطر وعلى الفور وكيل الجمهورية، ثم ينتقل وبدون تمهل إلى مسرحها قصد اتخاذ الإجراءات اللازمة للتحري، و التي تسمح بالحفاظ على الآثار التي يخشى اختفائها.[25]

•لا يجوز الانتقال إلى مسكن الأشخاص الذين يظهر أنهم ساهموا في الجريمة المتلبس بها، سواء لتنفيذ إجراءات التحري أو التحقيق بالجرائم المعلوماتية إلا بناء على إذن مكتوب

[24]- المادة: 41 قانون الإجراءات الجزائية الجزائري.

[25]- المادة: 42 قانون الإجراءات الجزائية الجزائري.

من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهاره قبل الدخول إلى مسكن المشتبه فيه، ويترتب على تنفيذ الإجراء في غياب الإذن ،أو غياب أوصاف محل البحث، أو عناوين أماكن البحث، عن مضمون الإذن البطلان المطلق للإجراء برمته.[26]

فبمجرد توفر هذان الشرطان جاز لرجال البحث والتحقيق بناء على حالة التلبس مباشرة أعمالهم المتعلقة بالمعاينة والتفتيش، ولهم الحق في إتمام أعمالهم في أي ساعة من ساعات الليل أو النهار وذلك حسب ما تورده المادة 47 من قانون الإجراءات الجزائية .

ثانيا- حسب ظروف الأحوال العادية: يقصد بها الحالات التي تكون خارج حالة التلبس وهي الظروف التي تميز الجريمة المعلوماتية ، و التي تحتاج إلى تقدير فني كبير لأجل التأكد من مدى صحة وقوعها، واتخاذ تقرير الإجراءات الكفيلة بمتابعة مرتكبيها واثبات الأدلة في مواجهتهم، ويتم الانتقال إلى مسرح الجريمة تنفيذا عادة لأوامر وكيل الجمهورية في إطار إتمام إجراءات البحث و التحري.[27] أو تنفيذا لأوامر قاضي التحقيق. [28]

ويشترط في هذه الحالة احترام جملة الشروط المتعلقة بالإذن المكتوب سواء الصادر من قبل وكيل الجمهورية وقاضي التحقيق حسب الأحكام الواردة في المواد من 44 إلى 47 مكرر من قانون الإجراءات الجزائية تحت طائلة البطلان.

إذن فمن الناحية القانونية فإن الشروط المتعلقة بالمعاينة والتفتيش في إطار الجريمة المعلوماتية هي نفس الشروط المتبعة في باقي الجرائم الأخرى ولا داعي لتكرارها، بحيث ينبغي تركيز البحث حول طبيعة الإجراءات المتبعة والاحتياطات الخاصة التي يطبقها ضباط الشرطة القضائية لأجل معاينة الجرائم المعلوماتية والتي تعرف تحت اسم إجراءات تأمين موقع الجريمة الالكترونية.

---

[26]- المادة 44 ق 06-22 قانون الإجراءات الجزائية الجزائري.

[27]- المادة 36 فقرة 04 -المعدلة بموجب الأمر 15-02 قانون الإجراءات الجزائية الجزائري.

[28]- المادة 68 ق – 01-08 -قانون الإجراءات الجزائية الجزائري.

الشرط الثانى: الإلتزام بإجراءات تأمين موقع الجريمة المعلوماتية .

قد يقوم كل من ضباط الشرطة القضائية أو وكيل الجمهورية أو قاضي التحقيق، عند الانتقال إلى مسرح الجريمة بأعمال المعاينة المادية والميدانية للجريمة في حد ذاتها، و المعاينة هي فحص مكان أو شيء أو شخص له علاقة بالجريمة، وإثبات حالته كمعاينة مكان ارتكاب الجريمة أو أداة ارتكابهما أو محلها أو معاينة جسم أو ملابس الجاني أو المجني عليه لإثبات ما بالجسم من جراح أو ما على الثياب من دماء أو آثار أخرى.[29]

إن الإنتقال من أجل إجراء المعاينة يعتبر أول إجراء من إجراءات البحث والتحري، فهو الإجراء الأكثر أهمية لآنه يسمح بالمعاينة المادية للوقائع المشكلة للجريمة، والإنطلاق بشكل سريع ومباشر في عملية البحث وضبط الأدلة، التي تساعد على معرفة وقت وكيفية إرتكاب الجريمة وهوية فاعلها، وعادة ما تسند هذه المهمة لأفراد الشرطة العلمية والتقنية، نظرا لضرورة التدخل بسرعة وبطريقة مدروسة تتلائم وطبيعة الجريمة محل المعاينة، من خلال القيام بسلسلة من العمليات التي تستلزم خبرة ميدانية ووسائل من نوع خاص.[30]

غير أن دورها يتضاءل في مجال الجرائم المعلوماتية، فهي لا تحقق نفس الأهداف كما هو الحال في الجرائم التقليدية، كما أنها لا ترقى إلى درجة أهميتها كإجراء في تلك الجرائم وذلك راجع إلى:

1.أن الجرائم التي تقع على نظم المعلومات و الشبكات قلما تخلف عقب ارتكابها أثار مادية .

[29]– عبد العال الدريبي، مرجع سابق– ص 294 .

[30]– Charle Diaz, La Police Techenique et Scientifique, 2eme Edition, Edition Presse universitaire de France, France – 2006– p54.

2.إن عددا كبيرا من الأشخاص قد يتردد على مسرح الجريمة خلال الفترة الزمنية التي تتوسط مرحلة ارتكابه او اكتشافها، مما يفسح المجال أمام حدوث تلف أو تغيير أو عبث بالآثار المترتبة عنها.[31]

وحتى تكون للمعاينة في جرائم المعلوماتية فائدة تسهم في كشف الحقائق وجب على المحقق اتباع مجموعة الإرشادات العملية ذات الطابع التأميني نوجزها فيما يلي:

أولا- قبل التنقل إلى إجراء المعاينة:

يجب إتباع الخطوات التالية من قبل رجال البحث والتحقيق قبل التحرك إلى مسرح الجريمة المعلوماتية لإجراء المعاينة وهي :

1 . توفير معلومات مسبقة عن مكان الجريمة، وكذلك عن نوع وعدد الأجهزة المتوقع مداهمتها، ونوع الشبكات المتصلة بها، وذلك لتحديد خطة التعامل معها.

2 . إعداد خريطة الموقع الذي سيتم الانتقال إليه مع ضرورة وضع خطة وتقسيم الأدوار على فريق التحقيق وتحديد المهام واختصاص كل واحد منهم حتى لا تتداخل الاختصاصات

3 . الحصول على الاحتياجات الضرورية من الأجهزة والبرامج الحاسوبية للاستعانة بها في الفحص.

4 . تأمين مصدر التيار الكهربائي حتى لا يتم التلاعب به عن طريق قطعه أو تعديله بهدف تعطيل عمل فريق المعاينة .

5 . مراجعة الخطة واستحضار الإذن القضائي.[32]

[31]- علي عدنان الفيل، مرجع سابق- ص 33.

[32]- نبيلة هبة هروال، مرجع سابق – ص 20.

ثانيا: عند معاينة مسرح الجريمة:

المعاينة إجراء من أهم إجراءات التحقيق الجنائي لأهمية الأدلة المستقاة منها التي تكون غالبا ذات دلالة قاطعة في الإثبات، وقد أكدت المعاينة الفنية في كثير من الأحيان فعاليتها في إظهار حقيقة الجريمة ومعرفة كيفية وأسباب وقوعها وهوية مرتكبيها، لذلك يترتب على المحقق مراعاة الدقة والترتيب وبذل أقصى ما يمكن من العناية والإهتمام عند إجرائها، للحيلولة دون فقدان ما يمكن إستخلاصه من معلومات قيمة قد تفيد في تنوير التحقيق، ويرى الفقه الجنائي ضرورة إتباع ضوابط خاصة لأجل معاينة مسرح الجريمة المعلوماتية هي:[33]

-1تحديد أجهزة الحواسيب الموجودة وتحديد مواقعها بأسرع وقت ممكن، إضافة إلى البحث عن النهاية الطرفية المزود للخدمة بالانترنت(MODEME) من أجل قطع الاتصالات الخارجية التي يمكن أن تخرب الأدلة أو تمحوها من على ذاكرة الحاسوب، كما يراعى ضرورة تصوير الأجهزة الموجودة وخاصة الأجزاء الخلفية التي تحمل الأرقام التعريفية للأجهزة.

-2 ضرورة وضع حراسة كافية على مكان المعاينة ومراقبة التحركات داخل مسرح الجريمة، مع رصد الاتصالات الهاتفية من و إلى مسرح الجريمة مع إبطال مفعول الهواتف النقالة التي تساعد عن طريق تقنية الجيل الثالث في تدمير الأدلة من خلال اتصالها بالأجهزة محل المعاينة.[34]

-3 ملاحظة واثبات الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال وطريقة الولوج

[33]- عبد الفتاح عبد اللطيف الجبارة، إجراءات المعاينة الفنية لمسرح الجريمة، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن،2010 -ص 171.

[34]- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية، دراسة مقارنة 2 على ضوء القواعد العامة للإجراءات الجنائية، مرجع سابق-ص 587- .

للنظام إضافة إلى ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بالنظام حتى يمنح فرصة لإجراء المقارنة حين يعرض الأمر على القضاء.[35]

-4 عدم التسرع في نقل أي "مادة معلوماتية" من مسرح الجريمة وذلك قبل إجراء اختبار اليقين من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي والتي قد تؤدي إلى إتلاف البيانات المخزنة مباشرة في حالة تعرضها لها .

-5 حفظ ما تحتويه سلة المهملات من أوراق ممزقة أو كربون نسخ أو أقراص ممغنطة سليمة أو محطمة مع فحصها ورفع البصمات عنها وكذلك التحفظ على مستندات الإدخال والمخرجات الورقية والتي عادة ما تكون ذات صلة بالجريمة.[36]

-6 حصر عملية المعاينة في فئة المختصين والمحققين الذين يتوافرون على الكفاءة العلمية والخبرة الفنية في مجال النظم المعلوماتية، والذين تلقوا تدريبا فنيا كافيا على التعامل مع الأدلة الإلكترونية، ففي فرنسا مثلا يقوم فريق التحقيق المتكون من ثلاث عشر(13)شرطيا بالإشراف على تنفيذ المهام التي يأمر بها وكيل الجمهورية أو قاضي التحقيق، فيرافقون المحققين أثناء عمليات المعاينة ويعملون على فحص الأجهزة ونسخ محتوياتها والتحقيق واعداد تقارير فنية ترسل إلى قاضي[37]

إذن تعتبر هذه مجموعة من الإجراءات والتدابير العملية الفنية ذات الطابع الخاص بمسائل المعاينة والتي تجري على مسرح الجرائم المعلوماتية والتي تعتبر ضرورية لأجل إتمام أعمال التفتيش والضبط اللاحقة.

[35]- عبد الله حسن علي محمود، مرجع سابق – ص 02.

[36]- فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق ص357.

[37]- علي عدنان الفيل، مرجع سابق ص 35.

المطلب الرابع: الإجراءات الخاصة بالتفتيش وضبط الأدلة

يهدف التفتيش إلى ضبط الأدلة المادية التي تفيد في كشف الحقيقة، و الضبط غاية التفتيش القريبة أي الأثر المباشر الذي يسفر عنه الإجراء، و هدف التفتيش سواء تعلق بالأشخاص أو المساكن هو ضبط الأشياء التي تفيد في كشف الحقيقة أي الأشياء التي تعد في ذاتها دليلا على الجريمة، أو يمكن استخدامها كدليل، وقد تكون هذه الأشياء هي وسيلة الجريمة أو تكون السبب الذي ارتكبت من أجله الجريمة، ولما كان الضبط هو الأثر المباشر للتفتيش، وباعتباره أحد إجراءات التحقيق فتنطبق عليه القواعد التي تنطبق على التفتيش فإذا بطل التفتيش بطل الضبط، و التفتيش يعتبر وسيلة تهدف للوصول إلى الحقيقة وليس غاية في حد ذاته، ولعل أن الشكل الذي يتبادر إلى الذهن في هذه الحالة هو مدى قابلية النظم المعلوماتية للتفتيش باعتبارها بيانات مادية.[38]

لقد سبق وأن فصلنا في الإجابة عن هذا التساؤل، ولقد خلصنا في شأن ذلك بأن أغلب التشريعات قد أقرت بالطبيعة الخاصة للمعلومات وجعلت من موضوعها محل قابلا للتفتيش والضبط شأنها شأن البيانات المادية، وذلك من خلال إقرار النصوص الإجرائية الجزائية بقواعد تنظم عمل جهات التحقيق فيما تعلق بمسألة التفتيش في مجال الجرائم المعلوماتية كما سبق وأن أشرنا إليه، وبالتالي فإننا سنستعرض بالبحث ضوابط التفتيش والضبط القانونية والفنية في مجال الجرائم المعلوماتية

الفرع الأول: الضوابط القانونية للتفتيش والضبط.

إن الحديث عن مسألة الضوابط القانونية للتفتيش والضبط في مجال الجرائم المعلوماتية يقودنا إلى إبرازها وفق التسلسل المنطقي التالي:

أولا: حسب شروط الاختصاص النوعي و المحلي:

[38]– على حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، مرجع سابق–ص 135

على عكس أغلبية التشريعات العربية التي خولت سلطة التحقيق وحق التفتيش للنيابة العامة، فإن التشريع الإجرائي الجزائري ساير نظيره الفرنسي وجعل الاختصاص الأصيل بالتفتيش والضبط لقاضي التحقيق، ولا يحق ذلك للنيابة العامة ممثلة في وكيل الجمهورية إلا وفق حالة التلبس بالجنحة أو الجناية.

فلقاضي التحقيق أن يقوم وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها مناسبة وضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام وأدلة النفي، ويجوز له بناء على ذلك الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويباشر قاضي التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقية (المادة79-80 -81) قانون الإجراءات الجزائية الجزائري. إذا كان من المتعذر على قاضي التحقيق أن يقوم بنفسه بجميع إجراءات التحقيق جاز له أن يندب ضابط الشرطة القضائية للقيام بتنفيذ جميع أعمال التحقيق اللازمة ضمن الشرو ط القانونية المنصوص عليها في المواد من 138 إلى 142 من قانون الإجراءات الجزائية. وباعتبار التفتيش والضبط إجراء يستهدف جرائم عادة ما تقع إما داخل الاختصاص المحلي لقاضي التحقيق أو خارجه، فإن هذا الأخير ملزم بإتباع قواعد الاختصاص الإقليمي فهو مختص ضمن -المادة 68 ق 01 -08 قانون الإجراءات الجزائية الجزائري.

دائرة وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه فيهم، أو بمحل القبض على أحدهم، ويمتد اختصاصه تلقائيا إلى دائرة اختصاص محاكم أخرى فيما يتعلق بالجرائم المعلوماتية فاختصاصه في هذه الحالة وطني حسب ما هو مقرر بالمادة (40 ق 04 -14 ق إ ج) وكذلك الفقرة الأخيرة من نص(المادة 47 ق 06-22 ق إ ج)، وهو نفس الاختصاص المقرر إقليميا المطبق على ضباط الشرطة القضائية في حال تنفيذ أوامر قاضي التحقيق

ثانيا: من حيث المواعيد:

عندما يتعلق الأمر بالجرائم المعلوماتية فإنه يجوز التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل بناء على إذن مسبق من وكيل الجمهورية المختص.

يمكن لقاضي التحقيق أن يقوم بنفسه بعملية التفتيش والضبط ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يندب ضابط الشرطة القضائية المختص بذلك الفقرة 03 و04 المادة 47 من قانون22-06 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

غير أنه إذا ما تعلق الأمر بجناية فلا يجوز سوى لقاضي التحقيق القيام بالتفتيش وبحضور وكيل الجمهورية (المادة 82 ق إ ج)، والملاحظ أن هذا الاستثناء هو بمثابة نص مضاد لما هو وارد في نص المادة 47 الفقرة 03 و04 والتي تمنح الحق لضباط الشرطة القضائية المختصين بالجرائم الالكترونية بالتفتيش في مسرح الجريمة المعلوماتية، فكان من الأولى توسيع مجال اختصاصهم وليس تضييقه من خلال حصر الاختصاص في شخص قاضي التحقيق الذي قد لا يكون على علم بتقنيات التفتيش الخاصة بالجرائم المعلوماتية*.

أما فيما تعلق بمسألة حضور المشتبه فيه عملية التفتيش والضبط سواء في مسكنه أو مسكن شخص آخر فإن الفقرة الأخيرة من نص (المادة 45 ق 22-06 ق إ ج) لا تستوجب حضوره، ففي مجال الجرائم المعلوماتية لقاضي التحقيق أو لضباط الشرطة القضائية مباشرة أعمالهم دون مراعاة هذه المسألة مع ضرورة الالتزام بأحكام ضمان السر المهني والتقيد بقواعد الحجز.

*الفقرة الأخيرة من المادة 16 قانون06-22المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

إذا ما كان الشخص موقوفا للنظر أو محبوسا مؤقتا أو غائبا لسبب آخر وكان من الخطر نقله والمكان التفتيش فإنه يجوز إجراء التفتيش بعد الحصول على الموافقة المسبقة لوكيل الجمهورية، أو لقاضي التحقيق مع ضرورة حضور شاهدين (المادة 47 مكرر قانون 06-22 المعدل والمتمم ق إ ج) .

الفرع الثانى: القواعد الفنية المتبعة عند التفتيش والضبط

إذا ما استنفذت الشروط القانونية لمباشرة إجراء التفتيش، جاز لقاضي التحقيق أو لضباط الشرطة القضائية المختصين، مباشرة عملية التفتيش والضبط، بغرض حجز كل ما من شأنه إظهار الحقيقة المتعلقة بالجريمة المعلوماتية سواء أكانت مادية كالحاسوب وملحقاته أو منطقية كالمعلومات والبيانات المخزنة عليه، أو على الشبكة، ولابد أن يراعى في ذلك القواعد التالية :

أولا: القواعد الاحتياطية قبل بدء التفتيش المعلوماتي:

- 1 .السيطرة على المناطق المحيطة بمسرح الجريمة أو مكان وجود النظام المعلوماتي من خلال غلق المداخل و المخارج.

- 2 .السيطرة على الدائرة المحيطة بمسرح الجريمة بوضع حراسة ملائمة

- 3 .السيطرة على محيط مسرح الجريمة من خلال التحفظ على الأشخاص الموجودين

- 4 .وضع حراسة على الأجهزة حتى لا يتمكن أي كان من لمسها .

- 5 .اختيار مكان لمقابلة المتهمين و الشهود بعيدا عن الأجهزة.

– 6 .توثيق مسرح الجريمة أو محل التفتيش جيدا من خلال جرد محتوياته وذلك لاحتمال توفر إحدى هذه المصادر على الدليل وهي الأوراق التي تم طباعتها، جهاز الحاسوب وملحقاته، أقراص ودعائم البرامج، وسائط التخزين المتحركة، الطابعات.

ثانيا: قواعد تفتيش وضبط ماديات الجريمة المعلوماتية:

يخضع تفتيش المكونات المادية للحاسوب للإجراءات القانونية الخاصة بالتفتيش، أي أنه يجب أن يراعى مكان وجود ذلك الحاسوب أثناء مباشرة الإجراء فيما كان مكانا عاما أو خاصا واستنفاذ الشروط القانونية السالفة الذكر.[39]

ويراعى عند التفتيش لأجل ضبط الأدلة المحتملة القواعد التالية:

. 1 التركيز حول مكان شاشة الحاسوب التي تعتبر الموضع المفضل عند مجرمي المعلوماتية للصق بعض القصاصات التي تحمل المعلومات المهمة كأرقام الهاتف أو فهرس المعلومات داخل الحاسوب كالكلمات السرية والمرور.

. 2 التفتيش بجوانب التوصيلات الهاتفية، فعادة ما يدون مجرمو المعلوماتية محادثاتهم الهاتفية في شكل مخططات يتركونها بجوار الهاتف.

. 3 تفتيش المفكرات الالكترونية، وهي من أهم الأدلة التي يجب التحفظ عليها وضبطها فهي تحمل أرقام الهاتف، وعناوين البريد الإلكتروني والمواعيد والملخصات وغيرها من المعلومات المفيدة في التحقيق.

. 4 تفتيش جيوب المتهم، فمجرمو المعلوماتية معهم عادة أقراص مرنة، أو بطاقات ذاكرة، تحمل معلومات متعلقة بالجريمة عادة ويحق لرجال التحقيق الإطلاع على محل

[39]– حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف للعلوم الأمنية، الرياض، المملكة العربية 3 السعودية سنة 2000 –ص 228.

التفتيش وحجزه أو ضبطه وتوضع عادة الأشياء المحجوزة في وعاء أو كيس، يغلق ويختم عليها بختم قاضي التحقيق أو ضابط الشرطة القضائية.

ثالثا: قواعد تفتيش وضبط المكونات المنطقية:

يجوز للسلطات القضائية المختصة (قاضي التحقيق)، ولضباط الشرطة القضائية حسب ما يجيزه القانون 09-04 المتعلق بمكافحة الجرائم المعلوماتية و في إطار إجراءات التحقيق المعلوماتي، الدخول بغرض التفتيش ولو عن بعد إلى كل منظومة معلوماتية أو جزء منها وإلى كل منظومة تخزين معلوماتية او منظومة اذا كانت هناك أسباب تدعوا للاعتقاد بأن المعطيات المبحوث عنها مخزنة في من معلوماتية أخرى غير تلك الأولى جاز لهم تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا، اذا كانت المعطيات المبحوث عنها مخزنة في منظومة الكترونية خارج الإقليم فإن الحصول على إذن يكون من خلال طلب مساعدة دولية حسب المبادئ والأعراف الدولية في مجال التعاون القضائي[40].

وهي آلية التفتيش عن بعد أو التفتيش المباشر التي تستهدف الكيانات المعنوية والمنطقية إن كانت هذه الأخيرة ضرورية لأجل ولوج النظم المعلوماتية أو الشبكات للحاسوب دون المادية منها، او بهدف التفتيش عن بعد وإلى حجز المعطيات المعلوماتية، فعندما تكتشف السلطة المختصة بالتفتيش المعلوماتي وجود معلومات مهمة من شأنها الكشف عن الجريمة ومرتكبها ويقدر بأنه لا حاجة لضبط وحجز ماديات المنظومة المعلوماتية، فإنه يقوم بنسخ المعطيات والمعلومات الضرورية لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، مع السهر على سلامة المعطيات الأصلية المخزنة على المنظومة المعلوماتية محل التفتيش.[41]

[40]- المادة 05قانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

[41]- المادة 06 قانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

أما إذا استحال أمر حجز هذه المعطيات لأسباب تقنية كان للسلطة المختصة بالتفتيش والحجز أن تستعمل تقنيات المنع من الوصول إلى المعطيات أو نسخها كما يجوز لها أن تأمر باتخاذ جميع الإجراءات اللازمة لمنع الإطلاع عليها وحجبها من خلال تكليف أي شخص مؤهل وذلك باستعمال وسائل تقنية لذلك.

الفرع الثالث: وسائل تحليل الأدلة المحجوزة .

إن عملية التفتيش عادة ما تسفر عن نوعين من المضبوطات مادية ومنطقية، فالأولى في شكل الحاسوب ذاته وملحقاته، والثانية في شكل ملفات وبيانات ومعلومات كانت مخزنة على القرص الصلب للحاسوب أو على الشبكة، وهي المضبوطات التي تحتاج إلى تحليل من أجل استخلاص الدليل منها وذلك من خلال الاستعانة ببرامج ووسائل خاصة نوجزها فيما يلي:

أولا: وسائل استعادة الدليل وفك التشفير:

قد يقدم المتهم على تخريب القرص الصلب لحاسوبه بمجرد علمه باكتشاف أمره، ولذلك يستعين أعضاء فرقة البحث و التحقيق المعلوماتي، في مجال معالجة الأدلة التالفة ببرنامج (DISK VIEW)، أما في مجال فك التشفير الذي قد يعمد الجاني إلى استعماله لمنع الإطلاع على البيانات المخزنة على حاسوبه فتستعمل برامج شركة DATA ACCES CORPORATION تحت اسم(PASS OUT أو PASSWORD RECOVERY)[42].

ثانيا: برامج إذن التفتيش:

هو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة المطلوبة، لترقيم الأدلة وتسجيل البيانات عنها، ويقوم هذا البرنامج بإصدار وصلات استلام الأدلة، والبحث في

[42]- ممدوح عبد الحميد عبد المطلب، مرجع سابق-ص ص 84-85

قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو ظروف ضبط هذا الدليل، وعادة ما يكون بحوزة المحقق على قرص مرن أو قرص صلب محمول.

ثالثا: برنامج بدء تشغيل الحاسوب:

وجود قرص بدء تشغيل الحاسوب مع المحقق، يمكنه من تشغيل الحاسوب المراد تفتيشه إذا كان هذا الأخير محميا بكلمة مرور، ويجب أن يكون مزودا ببرنامج مضاعفة المساحة، فربما قام المتهم باستخدام هذا البرنامج مسبقا لمضاعفة مساحة القرص الصلب.

رابعا: برنامج معالجة الملفات كبرنامج (GOLD XTREE):

وهو برنامج معالجة آلية للملفات، في أي مكان على الشبكة، أو القرص الصلب، ويستخدم لتقسيم محتويات القرص الصلب الخاص بالمتهم، أو الأقراص المرنة المضبوطة ويستخدم لقراءة البرامج والملفات في صورتها الأصلية.

خامسا: برنامج نسخ البيانات كبرنامج(LINK LAP):

هو برنامج يمكن المحقق من نسخ كل البيانات من حاسوب المتهم إلى قرص آخر، من خلال تقنية المنفذ المثالي أو المنفذ الموازي، وهو برنامج مفيد جدا يسمح بنسخ المعطيات بكل أمان ودقة قبل أي محاولة لتدميرها.

سادسا: برامج فحص الشبكة:

هي أدوات تستخدم في فحص البرتوكول **IP/TPC** لمعرفة المشكلات المتعلقة بالشبكات والعمليات التي تعرضت لها، ويرجع فعاليتها إلى قدرتها على دخول الشبكات وتحديد نوع برامج التجسس والفيروسات التي استعملت في عمليات الاختراق وتحديد مصدرها بدقة ومن بين هذه الأدوات:

. **1 أداة(ARP)** وظيفتها تحديد مكان الحاسوب على الشبكة.

. **2 برنامج(ROUTE VISUAL)** وهو برنامج يلتقط أي كلمة لعملية ضد الشبكة فيبين وقت وزمن الهجوم ومصدره.

. **3 أداة (TRACER)** هو برنامج يعمل على رسم مسار بين حاسوب الجاني والعناوين التي زارها والفترات التي قضاها هناك .

. **4 أداة (SAT NAT)** هو برنامج يعرض حالة الاتصال الحالية ومنافذ التصنت في شكل عرض كامل.[43]

إضافة لذلك يستعين المحققون بنوع آخر من البرامج كبرامج عرض الملفات بكل أشكالها وصورها، إضافة إلى إعادة تشكيلها عبر ما يعرف بالاستعانة بتقنيات الذكاء الاصطناعي، فجمع الأدلة في مجال الجرائم المعلوماتية يعتمد على تقنيات خاصة ومدى نجاعتها، فهي السبيل لحصر الاحتمالات والأسباب والفرضيات، وهي تتم عن طريق عمليات حسابية يقوم بها الحاسوب وفق برامج مصممة لذلك، تعمل على حصر الاحتمالات ثم إقصاء الأضعف منها وصولا إلى الاحتمال الأقوى.[44]

سابعا: برامج كشف الفيروسات وتدميرها:

يحب على المحقق أن يحمي أدواته وحاسوبه الخاص بالتحقيق، بواسطة برامج كشف الفيروسات فقد يعمد المتهم إلى تفخيخ حاسوبه بالفيروسات التي تنتقل إلى حاسوب المحقق وتدميره بمجرد ربطه بحاسوب المتهم لنسخ البيانات.[45]

ويبقى أمر استقصاء الوسائل التي تعمل بها الجهات المختصة بالبحث والتحقيق في الجرائم المعلوماتية أمرا مستحيلا نظرا لخصوصية وسائلهم وبرامجهم التي تتميز بطابع السرية، فهي معدة خصيصا لهم ولا يحق ترويجها خارجا، وذلك راجع إلى الخوف عليها من

[43]- علي عدنان الفيل، مرجع سابق- ص ص 75-76.

[44]- خالد عياد الحلبي، مرجع سابق- ص 214.

[45]- حسن طاهر داود، مرجع سابق- ص ص 229-230

مكر المجرمين المعلوماتيين الذين يجتهدون في وضع خطوات استباقية ضد إجراءات البحث والتحقيق المعلوماتي.

الفصل الثاني

إجراءات التحقيق في الجريمة الالكترونية

يخضع الاثبات في المسائل الجنائية لقواعد مخالفة عن تلك المحتكم لها في المسائل المدنية ويعود ذلك لاعتبارات موضوعية ومنها ما يرجع لأهمية الدعوى الجنائية، فالقواعد التي تحكم المسائل الجنائية تدور كلها حول غاية واحدة وهي الكشف عن حقيقة الجريمة، أول هاته القواعد حرية القاضي في تكوين عقيدته وقناعته، فله أن يوجه تحقيقه في الجلسة بالشكل الذي يراه مناسبا وملائما للوصول إلى الحقيقة والكشف عنها دون أن يتقيد في ذلك باتباع وسائل معينة للكشف عن الحقيقة، كما أن له مطلق الحرية في تقدير أدلة الدعوى، وثاني القواعد التي تحكم الإثبات في المسائل الجنائية دور القاضي الإيجابي في البحث عن الحقيقة فإنه ليس مجرد موازنة للأدلة المثبتة للإدانة أو البراءة، وإنما عليه التحري عن الحقيقة للكشف عنها، وآخر القواعد التي تحكم الاثبات في المسائل الجنائية قاعدة عبئ الاثبات.

فالإثبات نشاط إجرائي موجه للوصول الى اليقين القضائي قطعا وفقا لمعيار الحقيقة الواقعية والهدف من الاثبات هو بيان مدى التطابق بين النموذج القانوني للجريمة الالكترونية وبين الواقعة المعروضة، ولتحقق ذلك يستعمل وسائل معينة، ووسيلة الجريمة الالكترونية هي الدليل الإلكتروني، وتعد الجريمة الالكترونية كغيرها من الجرائم لها أركانها وعناصرها وتسري الدعوى الجنائية بالنسبة لها بذات المراحل التي تسري فيها الدعوى في الجرائم التقليدية إلا أن الجرائم الالكترونية تتميز بالطابع الخاص لان محلها أو موضوعها يكون غير مادي فوسائل الاثبات مرت بعدة مراحل وكانت نتيجة تطور طويل تطورت معه هذه الوسائل تدريجيا بتطور الفكر الاجرامي.

دراستنا للفصل الثاني في إجراءات التحقيق في الجريمة الالكترونية في مجال الدعوى العمومية قسمناها الى مبحثين الأول إجراءات استخلاص الدليل في الجريمة الالكترونية والمبحث الثاني حجية الدليل الالكتروني في نطاق الاثبات الجنائي.

المبحث الأول: إجراءات استخلاص الدليل في الجريمة الالكترونية.

إن التطور الحالي الذي لحق ثورة المعلوماتية قد انعكس اثره على الجرائم التي تولدت عنه فانعكس أثره على قانون العقوبات، كما انعكس أثره أيضا على قانون الإجراءات الجزائية خاصة في مجال الإثبات الذي أثر بدوره على التطور الهائل الذي لحق الأدلة الجزائية بسبب تطور طرق ارتكاب الجريمة، وبالنظر إلى الطبيعة الخاصة لتلك الجرائم المتمثلة في صعوبة إثباتها أو صعوبة التوصل إلى مرتكبيها بأدوات البحث الجنائي التقليدية الأمر الذي استوجب على سلطات الضبط القضائي مسايرة هذه الأنماط من الجرائم عن طريق الاستعانة بالتقنيات العلمية الحديثة فالجريمة الإلكترونية تعتبر كأي جريمة من الجرائم المنصوص عليها في قانون العقوبات والقوانين الأخرى، لذلك تتميز الجريمة الإلكترونية عن غيرها في الدعوى العمومية وهذه الدعوى تتم بمراحل لجمع الدليل الالكتروني.

استنادا لما سبق سنتناول في هذا المبحث إجراءات استخلاص الدليل الإلكتروني في الجريمة الالكترونية في مطالب وفقا لتقسيم الإجراءات إلى التقليدية لاستخلاص الدليل الالكتروني ثم الإجراءات الحديثة لاستخلاص الدليل الالكتروني وقبل ذلك نتطرق لمفهوم الدليل الالكتروني وشروط صحة الدليل الالكتروني.

المطلب الأول:مفهوم الدليل الالكتروني وانواعه.

بدأ الحديث منذ شيوع استخدام الحاسب الآلي ومختلف الأجهزة الإلكترونية الأخرى عن بعض الأفعال والسلوكيات المرتبطة بالاستخدام غير المشروع للبيانات المخزنة في أنظمته والتلاعب بهذه البيانات وتدميرها، وقد ارفق ذلك نقاشات وتساؤلات حول كيفية التصدي لهذه السلوكيات الإجرامية المستجدة وما هي الوسائل الملائمة لإثباتها، ولما كان الدليل الالكتروني الناشئ عن البيئة الرقمية لهذه الجرائم الحديثة مرتبطا بتكنولوجيات وسائل الاتصال وشبكات الربط الحديثة، فانه من الضروري أن يكون أي تعريف لهذا النمط من الأدلة متسما بالمرونة بما يسمح باستيعابه وتواكبه مع سائر الجرائم المرتكبة بالتقنيات المبتكرة الراهنة والمستقبلة في تكنولوجيا التعامل مع المعلومات، ولكن التطور المستمر

واللامتناهي لتكنولوجيا المعلومات والاتصالات حال دون وضع تعريف فقهي جامع وشامل لمفهوم الدليل الالكتروني، خشية حصر نطاقه داخل إطارّ تجريمي محدد قد يضر به خاصة في ظل التطور المستمر للتقنية الإلكترونية(الفرع الأول). واذا كان التطور المتجدد والمستمر للبيئة التي يرتبط بها الدليل الالكتروني يمنع إيجاد تعريف موحد لهذا الأخير، فذلك لم يمنع الفقه الجنائي من تحديد السمات والخصائص التي يتميز بها الدليل الالكتروني عن غيره من الأدلة التقليدية، والذي قد يسهم في صياغة المشرع لنصوص قانونية حولها ويساعد القضاء من تفسير هذه النصوص وتقدير الدليل(الفرع الثاني).

الفرع الأول: مقاربة لتعريف الدليل الإلكتروني

لم يتفق الفقه الجنائي حتى الآن حول تعريف موحد للدليل الالكتروني، وذلك ارجع إلى التطور المستمر الذي يطرأ على البيئة التقنية التي ينشأ فيها، وتجعله من الأدلة المتطورة بطبيعتها، لاسيما أن العالم الافتراضي لا يزال في بداية عهده ولم يبلغ بعد ذروته، وأن العالم الالكتروني أو الرقمي من غير الممكن احتوائه. فقد عرفه البعض بأنه " ذلك الدليل المأخوذ من أجهزة الحاسب الآلي، ويكون في شكل ذبذبات رقمية ونبضات مغناطيسية او كهربائية يمكن جمعها او تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة ويتم تقديمها في شكل دليل علمي يمكن اعتماده أمام القضاء الجنائي.[46]

والملاحظ على هذا التعريف أنه يلحق مفهوم الدليل الالكتروني بمفهوم البرنامج رغم وجود فرق كبير في الوظيفة التي يؤديها كل عنصر، فبرنامج الحاسب الآلي له دور في القيام بمختلف العمليات التي يحتويها نظام المعالجة الآلية، أما الدليل الجزائي الالكتروني فيكمن دوره الأساسي في معرفة كيفية حدوث جر ائم الاعتداء على نظم المعالجة الآلية، بهدف إثباتها ونسبتها إلى مرتكبيها.

[46]- ممدوح عبد الحميد عبد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت، دار الفكر القانونية، القاهرة، 2006 ،ص .88

وعرفه البعض الآخر بأنه "معلومات يقبلها المنطق و العقل و يصدقها العلم، يتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الاتصال ويمكن استخدامها في أية مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة[47]" أو انه "يشمل المعطيات الرقمية المشتقة من أو بواسطة النظم و المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الإعلام الآلي أو شبكات الاتصالات وفق إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا وترجمتها الى نصوص مكتوبة أو رسومات أو صور أو أشكال أو أصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة للمتهم وفقها. [48] "يرى أن ما يأخذ على هذا التعريف كذلك هو حصره الأدلة الالكترونية في تلك التي تستخرج من أجهزة الإعلام الآلي وملحقاتها، دون سواها من الوسائل التقنية الالكترونية الأخرى التي تعتمد المعالجة الآلية للمعلومات كالهواتف النقالة والبطاقات الذكية والتي يمكن أن تكون مصدرا مهما للأدلة الالكترونية، وهو ما يعد تضييقا لدائرة هذه الأخيرة. كما عرف الدليل الالكتروني أيضا بأنه "مجموعة البيانات والمعطيات المأخوذة من العالم الافتراضي التي يمكن إعدادها وتجميعها وتخزينها وتحليلها الكترونيا باستخدام ب ارمج وتطبيقات خاصة لتظهر في شكل صور او تسجيلات صوتية أو مرئية"[49] . إلا أن ما يسجل على هذا التعريف هو إضفاؤه صفة الدليل الالكتروني على تلك الأدلة المستخلصة من وسطها الافتراضي المأخوذة من الحاسب مما يعني بمفهوم المخالفة بان تلك المعطيات التي تكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية التي لم تفصل عن الحاسب الآلي لا تصلح لان توصف بالدليل

---

[47]- محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي و شبكات الانترنت، بحث مقدم في الحلقة العلمية بعنوان "الانترنت و الإرهاب"، المنظمة من طرف جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين الشمس، بدبي، في الفترة الممتدة من 15 إلى 11/19 /2008 ،ص 25.

[48]- خالد ممدوح إبراهيم ، الدليل الالكتروني في جر ائم المعلوماتية، بحث منشور في الموقع الالكتروني التالي: http://Kenanaonline.com/users/KhaledMamdouh/posts/79345.

[49]- الدليل الرقمي في مجال الإثبات الجنائي" بحث مقدم إلى المؤتمر ألمغاربي الأول حول 251 المعلوماتية و القانون، المنظم من طرف أكاديمية الد ارسات العليا بط اربلس، في الفترة الممتدة من 29/10/2009-28، ص 06.

الالكتروني، وهذا أمر غير دقيق .ومن التعريفات التي قدمت كذلك للدليل الالكتروني أنه "طريقة خاصة لاظهار الحقيقة والذي يتم فيه اللجوء إلى احد الوسائل الرقمية المتنوعة التي تدرس المحتويات داخل ذاكرة القرص الصلب و الرسائل الالكترونية المخزنة او المنقولة رقميا[50] .استرشادا بالمقاربات السابقة فان التعريف الأكثر شمولا للدليل الالكتروني في نظرنا هو" كل معلومات مخزنة في نظم المعالجة الآلية وملحقاتها أو متنقلة عبرها بواسطة شبكة الاتصالات في شكل مجالات الكترونية او ذبذبات كهربائية او نبضات مغناطيسية، يتم استخلاصها وجمعها وتحليلها وفق إجراءات قانونية وعلمية، وترجمتها لتظهر في شكل مخرجات يقبلها العقل والمنطق ويعتمدها العلم، ويمكن استخدامها في أية مرحلة من م ارحل التحقيق والمحاكمة لإثبات الجريمة وتقرير البراءة أو الإدانة.[51]

الفرع الثاني: مميز ات الدليل الإلكترونـــي

يعتقد البعض أن الأدلة الجنائية الالكتروني ما هي إلا مرحلة متقدمة من الأدلة التقليدية المادية التي يمكن إد اركها بإحدى الحواس الطبيعية للإنسان، إلى الاستعانة بجميع ما يبتكره العلم من وسائل التقنية العالية بما فيها جهاز الحاسب، ولكن الحقيقة تثبت[52] عكس ذلك تماما، لأن الأدلة الالكترونية هي نوع آخر من الأدلة الجنائية الجديدة التي لها من الخصائص العلمية والمواصفات القانونية ما يميزها عن غيرها من وسائل الإثبات التقليدية.

---

[50]- colloque sur « la preuve numérique a l'épreuve du litige. Les acteurs de litige a la preuve numérique » organiser par la compagnie nationale des experts de justice en informatique et associées le 13-04- 2010. Disponible sur le site: www.cnejita.org/.../CNEJTA-ACTES-COLLOQUE10042010-A5-V5.1-pdf وهو تقريبا نفس التعريف الذي استأثرته المنظمة العالمية لدليل الكمبيوتر(IOCE) في تقريرها الصادر في أكتوبر.

[51]- أنظر: مصطفي محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، 2009، ص213.

[52]- عمرو حسين عباس، أدلة الإثبات الجنائي والجرائم الالكترونية، بحث مقدم الى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، المنعقد بمقر الجامعة الدول العربية، القاهرة، خلال الفترة الممتدة من 26-27أفريل 2008 ،ص06. ص07- ،و علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي" مرجع سابق، ص 77 .

وهذه الموصفات والخصائص مرتبطة أساسا بطبيعة البيئة التي يتواجد فيها، وهي البيئة الافتراضية التي انعكست على طبيعة هذه الأدلة وجعلته يتصف بالمميزات التالية :

أولا: الدليل الإلكتروني دليل علمي :يتصف الدليل الالكتروني بأنه علمي لأنه مشّكل من معطيات الكترونية غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات ذات المبنى العلمي، وأن ما يسري على الدليل العلمي يسري على الدليل الالكتروني الدليل ، وذا كان ا 255 العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة " القانون مسعاه العدالة أما العلم فمسعاه الحقيقة " law seek justice, science seeks truth " إذ يستبعد تعارضه مع القواعد العلمية السليمة، فان الدليل الالكتروني له الطبيعة ذاتها، ويجب أن لا يخرج عما توصل إليه العلم الالكتروني الرقمي وإلا فقد معناه.[53]

ثانيا: الدليل الإلكتروني دليل تقني: بمعنى انه مستوحى من البيئة التقنية التي يتواجد فيها، والمتمثلة في مختلف أجهزة تكنولوجية الإعلام والاتصال من أجهزة الحاسب والخوادم والمضيفات والهواتف والشبكات. ولا يمكن تصور وجود الدليل الالكتروني خارج هذا الإطار.[54]

واعتبارا للطبيعة التقنية للدليل الالكتروني فانه اكتسب جملة من مواصفات ميزته عن غيره من الأدلة التقليدية في قابليته للنسخ، إذ يمكن استخراج نسخ من الأدلة الجنائية الالكترونية مطابقة للأصل و تحمل القيمة العلمية نفسها، وهذه الخاصية لا تتوافر في الأدلة الأخرى، مما يشكل ضمانة فعالة للحفاظ على الدليل من التلف أو الفقد أو أي شكل من أشكال التلاعب والتغيير، وذلك لإمكانية مقارنة النسخ مع الأصل باستخدام برامج وتطبيقات خاصة.[55]

[53]– عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، مرجع سابق، ص977 .

[54]– علي محمود علي حمودة، مرجع سابق، ص22.

[55]– خالد ممدوح إبراهيم، الدليل الإلكتروني في جرائم المعلوماتية، مرجع سابق. بدون ترقيم .

وكذا قدرة الدليل الالكتروني على رصد معلومات عن الجاني وتحليلها في الوقت نفسه، اذ يمكنه أن يسجل تحركات الجاني، عاداته وسلوكياته ومختلف المعلومات الشخصية الخاصة به، من ثمة يكون البحث الجنائي فيه أيسر بكثير من الدليل المادي التقليدي[56]. أضف إلى ذلك قابلية الدليل الالكتروني للتطور المتواصل نظرا لارتباطه الوطيد بالطبيعة المتغيرة والمتجددة التي تتمتع بها تكنولوجية الإعلام والاتصال.[57]

ثالثا– صعوبة التخلص من الدليل الالكتروني: تعد هذه الخاصية أهم ميزة يتمتع بها الدليل الالكتروني عن غيره من الأدلة المادية، وإذا كان من اليسير جدا التخلص من الأدلة المادية نهائيا دون إمكانية استعادتها كالوثائق والأشرطة بتمزيقها وحرقها، أو بصمات الأصابع بمسحها من موضعها، أو حتى الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة، فإن الحال غير ذلك بالنسبة للأدلة الالكترونية[58]، إذ يمكن استرجاعها بعد محوها واظهارها بعد إخفائها واصلاحها بعد إتلافها، وذلك باستخدام أدوات وبرمجيات ذات الطبيعة الرقمية صممت خصيصا لهذا الغرض مثل برمجيات(... Recoverpeg, Foremost)[59] photorec . كما أن نشاط الجاني لمحو الدليل الالكتروني بواسطة خصائص التخلص من الملفات في الحاسب الآلي كخاصية(...Erase, Rénove, Delete)يشكل في حد ذاته

[56]– نذكر منها برنامج حساب البصمة الرقمية (Hash)و اللوغارتمية(MD5)وظيفتهما إسناد إلى ملف أو مجموعة ملفات الكترونية سلسلة أحرف أو أرقام متتالية، وأي تعديل ولو طفيف يصيب أحد هذه الملفات ، يؤدي إلى تغيير بصمته الرقمية بصفة آلية ، وبالتالي الكشف عن التغيرات المحتملة في البيانات الرقمية التي يمكن اعتبارها دليلا رقميا لجريمة ما– .

[57]– نذكر منها برنامج حساب البصمة الرقمية (Hash)و اللوغارتمية(MD5)وظيفتهما إسناد إلى ملف أو مجموعة ملفات الكترونية سلسلة أحرف أو أرقام متتالية، وأي تعديل ولو طفيف يصيب أحد هذه الملفات ، يؤدي إلى تغيير بصمته الرقمية بصفة آلية ، وبالتالي الكشف عن التغيرات المحتملة في البيانات الرقمية التي يمكن اعتبارها دليلا رقميا لجريمة ما .

[58]– محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنت، مرجع سابق، ص26.ص27.

[59]– عمر محمد أبو بكر بن يونس، مرجع سابق، ص 982.

دليلا ضد الجاني، لأن هذا النشاط يتم تسجيله وتخزينه بشكل آلي في ذاكرة جهاز الحاسب و يمكن استخلاصه لاحقا كدليل إثبات ضده.[60]

رابعاـ الرقمية الثنائية للدليل الإلكتروني: ومفاد هذا أن الدليل الالكتروني يتكون من تعداد غير محدود لأرقام ثنائية في هيئة الواحد والصفر (1-0) والتي تتميز بعدم التشابه فيما بينها رغم وحدة الرقم الثنائي الذي تتشكل منه، فمثلا المعلومات و البيانات الموجودة داخل الحاسب الآلي سواء كانت في شكل نصوص أو حروف أو أرقام أو صور أو تسجيلات صوتية أو فيديو ليس لها الوجود المادي الذي نعرفه في شكل ورقي، إنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد وهو الرقم الثنائي المذكور أعلاه[61] . فما من شيء في العالم الرقمي إلا ويتكون من معادلة ثنائية قوامها الرقمان (1)و(0)وهما في تكوينهما الحقيقي عبارة عن نبضات وذبذبات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة.[62] مع العلم أن تكوين معطيات هذه المعادلة الثنائية تختلف في الحجم والموضوع، وكمية أو حجم الرقمين (0-1)في ملف يمكن أن يختلف عن كميته في ملفات أخرى. وما يمكن استخلاصه هو أن تمتع الدليل الالكتروني بالخصائص سالفة الذكر جعلته دليلا ذا طابع خاص يختلف عن باقي الأدلة المادية المألوفة، وأصبح على حد تعبير بعض القانونيين المختصين[63] من قبيل الدليل الأحسن والأفضل لإثبات الجرائم الالكترونية لكونه مستمدا من طبيعة الوسط الذي وقعت فيه.

---

[60]- CLEMENT-FONTAINE.Mélanie, op.cit. Article disponible sur ;
www.cnejita.org/.../CNEJTA-ACTES-COLLOQUE10042010-A5-V5.1-pdf

[61]- -عبد الحميد عبد المطلب، استخدام بروتوكول(TCP/IP) في بحث و تحقيق الجرائم على الكمبيوتر، بحث مقدم الى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، المنعقد بدبي، في الفترة الممتدة من 26 -08/28/ 2003 منشور على الموقع الالكتروني التالي: 08 WWW.arablaw.info.com

[62]- عمر محمد أبو بكر بن يونس، مرجع سابق، ص171

[63]- طارق محمد الجملي، مرجع سابق، ص 08

المطلب الثاني: شروط صحة الدليل الالكتروني.

إن الأدلة الالكترونية إما أن تكون مخرجات ورقية يتم إنتاجها بواسطة الطابعة أو غير ورقية أي أن تكون (غير) إلكترونية كالبيانات المخزنة على الأقراص الصلبة أو الأقراص المضغوطة أو غيرها من الأشكال الإلكترونية، وقد تتمكن في شكل عرض على الشاشة الخاصة بالحاسوب، سواء كانت مخزنة على ذاكرة الحاسوب أو على شبكة الانترنت ويكون الدليل الإلكتروني غير قابل للتعامل به إذا ما شابه البطلان فلا يصح الاستناد عليه.

فالمقصود بحجية الدليل الإلكتروني هو قيمة ما يتمتع به هذا الدليل بأنواعه المختلفة من قوة استدلالية على صدق نسبة الفعل الإجرامي إلى شخص معين " و لقبول الدليل الإلكتروني كأساس للحقيقة سواء أكان الحكم الصادر بالإدانة أو البراءة فإنه يجب إن يتوفر في هذا الدليل عدة شروط هي:

الفرع الأول: مشروعية الدليل الالكتروني.

يجب أن يكون الدليل الإلكتروني متحصلا بطريقة مشروعة و يقصد بالشرعية في المقام الأول عدم مخالفة الأحكام التي تهدف إلى صيانة كرامة الإنسان و حماية حقوقه، وذلك ما تتضمنه الدساتير الحديثة، بحيث يتقيد بها المشرع عند وضع قانون الإجراءات الجزائية ، فكل دليل مستمد بصفة مخالفة لهذه الأحكام يعتبر باطلا بطلانا مطلقا.

ويعني مبدأ مشروعية الدليل الجنائي الإلكتروني بما يتضمنه من مفاهيم الإلكترونية، ضرورة إتفاق الإجراء مع القواعد القانونية و الأنظمة المتبعة في وحدات المجتمع المتحضر، أي أن قاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية، بل يجب أن تراعي المبادئ السامية لحقوق الإنسان و قواعد النظام و حسن الآداب في المجتمع، وتفادي الطرق غير المشروعة في تحصيل الدليل الإلكتروني كاستخدام التعذيب، الإكراه المادي أو المعنوي، إطالة التحقيق، استعمال مصل الحقيقة، التنويم المغناطيسي الغش، التدليس تجاه المتهم من أهم ضمانات مشروعية الدليل الإلكتروني.

فإذا كانت المعلومات التي تشكل جريمة مخزنة في ذاكرة الحاسوب أو على الأقراص الصلبة أو المرنة فإن التساؤل الذي يدور حول مدى إمكانية الحصول عليها من المتهم نفسه أو من غيره إذا كان يعلم سبيل الوصول إليها بإرادته أو من خلال إجباره على ذلك؟ إن الإجابة عن هذا التساؤل دفعت بالفقه إلى اتخاذ موقفين:

الاتجاه الأول: يرى أنه لا يجوز إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظامه المعلوماتي، أو إلزامه بالكشف عن الثغرات أو كلمات السر الخاصة بالدخول عملا بمبدأ أنه لا يجوز إلزام الشخص نفسه باتهام نفسه.[64]

أما بالنسبة للشهود فإن أنصار هذا الاتجاه يرون بأن الشاهد غير مجبر على تقديم المساعدة للحصول على الدليل الإلكتروني، أين يتمتع الشاهد بحرية الرفض عن الإجابة أمام المحكمة عن كل ما يعرفه، وبالتالي يصعب إجباره على تقديم بيانات معلوماتية كونه مؤهل للوصول إليها لمعرفته كلمة السر، وإن تعاون من تلقاء نفسه فهو يقترب للخبرة منه للشهادة.[65]

الاتجاه الثاني: يتفق مع الرأي القائل بعدم جواز إجبار المتهم على إدانة نفسه غير أن له موقفا آخر تجاه التزامات الشاهد، فيرى أن من التزامات الشاهد طبع ملفات البيانات و الإفصاح عن كلمة السر، ما عدا الحالات المتعلقة بالمحافظة على سر المهنة فإنه يكون حرا في الالتزام بأداء الشهادة استجابة لسلطات التحقيق عند اصدارها أمر للقائم بتشغيل النظام من أجل تقديم المعلومات اللازمة الخاصة إما بالإفصاح عن كلمات المرور السرية،[3] الشفرات الخاصة بتشغيل البرامج.

[64]- طاهر محمود أبو القاسم، الجرائم المعلوماتية، مرجع سابق، ص 100.

[65]- ضياء علي أحمد النعمان- مرجع سابق- ص 294

أن يكون الدليل الإلكتروني ذا علاقة بموضوع الجريمة المعلوماتية.

نصت على ضرورة توافر هذا الشرط المادة 407 من قانون الإثبات الفدرالي الأمريكي، وأسمته بمبدأ العلاقة الكاشفة حيث يتطلب ضرورة أن تكون هناك علاقة ما بين الدليل و ما بين الواقعة محل الدعوى، و هو مبدأ لا يتحقق إلا بتحقق شرط آخر، و هو مطابقة الدليل الإلكتروني المستخرج للأصل المخزن من الحاسوب بداخله.

عبئ الاثبات في الجرائم الالكترونية:

ان اثبات الركن المادي للجريمة واسنادها لمرتكبها يقع على سلطة الاتهام وهي بصفة اصلية النيابة العامة ولابد ان تبين عند المتابعة الأدلة التي من شأنها اثبات قيام اركان الجريمة وعدم وجود عذر معفي أو أحد اسباب انقضاء الدعوى العمومية، ويمكن للمتهم ان يقدم دفوعا واذا تمسك أو ادعى وجود وسائل الدفاع لصالحه مرتبطة بالدعوى مثل سبب اباحة، موانع العقاب، سبب انقضاء الدعوى العمومية، يتحول المتهم الى مدعي يقع عليه عبئ اثبات ما يدعيه استنادا الى قاعدة البينة على من ادعى. ان دور النيابة العامة هو اظهار الحقيقة بقصد ادانة المذنب او تبرئة البريء، لذلك خول لها قانون الاجراءات الجزائية صلاحيات وامتيازات واسعة تجعل منها طرفا ممتازا في الخصومة الجنائية حيث تعتبر وكالة باسم المجتمع.

وقد تلعب هذه السلطة دورا مهما، في حالة ما اذا كانت الدعوى قد رفعت بواسطته، وفي هذه الحالة لابد من اثبات عناصر الجريمة، و رابطة السببية التي تر بط بين السلوك الاجرامي والنتيجة الاجرامية، فسلطة الاتهام كما يقول الفقيه الفرنسي) PATARIN ليست مجرد مدعي عادي، بل هي تحمي البريء كما تحمي المتهم، ولذلك يجب عليها جمع عناصر الاثبات التي في صالح المتهم اذا ظهرت لها، و تقدمها الى القضاء لأنها باعتبارها نائبة عن المجتمع تهتم ببراءة البريء وادانة المتهم، لذلك على النيابة العامة اثبات جميع

العناصر المكونة للجريمة .كما يقع عبىء الاثبات على الطرف المدني عندما يبادر بتحريك الدعوى العمومية أو عندما يتأسس بعد تحريك الدعوى العمومية.

الفرع الثاني: أن يكون الدليل الإلكتروني يقيني غير قابل للشك .

يشترط في الأدلة الإلكترونية أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ذلك أنه لا مجال لدحض قرينة البراءة و افتراض عكسها إلا عندما يصل القاضي إلى درجة من القناعة تتسم بالجزم و اليقين[66]، واليقين في النظم الإجرائية هو عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة و يتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى و ما يتطبع في ذهنه من تصورات و احتمالات ذات درجة عالية من التأكيد و يمكن الوصول إلى اليقين عن طريق نوعين من المعرفة إحداهما حسية تدرك بالحواس، و الأخرى معرفية تدرك بالعقل[67]، عن طريق التحليل و الاستنتاج .وتأكيدا لمبدأ يقينية الدليل الإلكتروني فقد أكد الفقه في كندا على اعتبار مخرجات الحاسوب من أفضل الأدلة لذا فإنها تحقق اليقين المنشود في الأحكام الجنائية، كما نصت بعض القوانين في الولايات المتحدة الأمريكية على أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تعد من أفضل الأدلة المتاحة لإثبات هذه البيانات و بالتالي يتحقق مبدأ اليقين لهذه الأدلة.

الفرع الثالث: قابلية الدليل الإلكتروني للمناقشة

يقصد بهذا الشرط وجوب مناقشة الدليل الجنائي بصفة عامة أي أن القاضي لا يمكن له أن يؤسس قناعته إلا على العناصر الإثباتية التي طرحت للمناقشة في جلسات المحاكمة، و خضعت لحرية مناقشة أطراف الدعوى و هو ما يعني أن الأدلة الإلكترونية سواء المتحصل عليها من الحاسوب أو من شبكة الأنترنت سواء أكانت مطبوعة أم بيانات

[66]- علي حسن أحمد الطوالبة- التفتيش الجنائي على نظم الحاسوب و الانترنت- دراسة مقارنة- مرجع سابق-ص 186

[67]- علي حسن أحمد الطوالبة-" مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي"- مرجع سابق- ص 5.

معروضة على الشاشة أو مخزنة على دعامة يجب أن تكون محل مناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة و بناءا على ذلك فإن كل دليل تم الحصول عليه من خلال البيئة الرقمية يجب أن يعرض في الجلسة بصفة مباشر ة أمام القاضي، و هذا ما ينطبق على الشهود الذين يجب أن يعيدوا أقوالهم مرة أخرى أمام المحكمة، و كذلك الخبراء و ذلك لأجل مناقشة[2] تقاريرهم التي خلصوا إليها. وما تجدر الإشارة إليه هو أن المشرع الجزائري بموجب المادة 212 من قانون الاجراءات الجزائية في الفقرة الثانية، بنصه: " ولا يسوغ للقاضي أن يبني قراره الا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه" فالقاضي ولكي تكون له السيادة والهيمنة على الدعوى الجنائية فيجب أن يكون متدربا على كيفية التعامل مع تقنية المعلوماتية وتعقيداتها بشكل واف حتى يضمن له هذا التأهيل العلمي لنجاح مهمته[3] إذن فالدليل الإلكتروني و بحسب ما إستعرضناه هو دليل على قدم المساواة مع باقي أنواع الأدلة الجنائية ، بالرغم من مميزاته وخصائصه غير المألوفة في مجال الإثبات الجنائي، و ذلك ما يمكن تفسيره بأنه متناسب والجريمة الناشئ عنها التي تتميز هي الأخرى بمميزات و خصائص تخرج عن ما ألفناه بشأن الجرائم التقليدية المادية.

المطلب الثالث: إجراءات تقليدية لاستخلاص الدليل الالكتروني.

ان طبيعة الوسط الافتراضي، يتطلب اعادة تقييم منهج الاجراءات التقليدية، خاصة وأن الوسائل المستخدمة في ارتكاب الجرائم الالكترونية تختلف عن الوسائل التقليدية، مما يتطلب مواكبة الاجراءات للتطورات الحاصلة في المجال المعلوماتي، لتسهيل التعامل مع الحاسب الآلي وكافة الأجهزة الحديثة والمحافظة على الأدلة المستخلصة منها، مع مراعاة عدم المساس بالحريات وحقوق الانسان، الا لمقتضيات التحري والتحقيق مع مراعاة الضمانات المقررة قانونا بشأنها.

نظم المشرع كيفية استنباط الدليل عن طريق إجراءات تتبع وصولا إلى هذه الغاية. وعليه سنتناول في هذا المطلب الى في فرع أول التفتيش والضبط في الفضاء الالكتروني والفرع الثاني المعاينة والخبرة التقنية وفرع الثالث فقد خصصناه إلى الشهادة وهذه الإجراءات تستخدم بصفة عامة في جميع الجرائم التقليدية منها والمستحدثة.

الفرع الأول: اجراء التفتيش والضبط الإلكتروني –المعلوماتي:

التفتيش بوجه عام هو اجراء قضائي يهدف الى الحصول على أدلة تساعد في كشف الحقيقة، ويتميز بخاصيتي الجبر والاكراه، أي أن الانسان يخضع له مجبرا، إذا لم يوافق على اجرائه برضاه، ويتضمن هذا الاجراء مساسا بمستودع سر الانسان، سواء كان مسكنا، أو في جسمه، وهو اجراء يهدف الى جمع الأدلة التي تساهم في كشف الحقيقة أما فيما يتعلق بالتفتيش الالكتروني: ويمكن تعريفه على أنه[68]: اجراء من اجراءات التحقيق يهدف الى الوصول الى أدلة منبثقة من جناية أو جنحة لإثبات ارتكابها ونسبتها الى المتهم، بشرط أن يكون تحقق وقوعها فعلا داخل نظم المعالجة الآلية للمعطيات.

والضبط لا يخرج من كونه وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، سواء في ذلك أن يكون هذا الشيء عقارا أو منقولا الضبط حسب الأصل لا يراد إلا على أشياء مادية فلا صعوبة بالتالي بضبط الأدلة في الجريمة الواقعة على المكونات المادية للكومبيوتر، كرفع البصمات مثلا عنها وكذلك لا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخة غير مشروع أو إتلافه بوسائل تقليدية كالكسر، الحرق، لكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس وفي ضبط البيانات الكمبيوتر لعدم وجود

[68]– أمدور رجاء خصوصية التحقيق في مواجهة الجرائم المعلوماتية أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث ل.م.د تخصص: القانون الخاص جامعة محمد البشير االبراهيمي برج بوعريريج كلية الحقوق والعلوم السياسية قسم الحقوق السنة الجامعية 2021/2020، ص137.

أي دليل مرئي في هذه الحالات، ولسهولة تدمير الدليل في ثواني معدودات ولعدم معرفة كلمة السر أو ثغرات المرور أو ترميز البيانات .

الضوابط القانونية للتفتيش والضبط.

إن الحديث عن مسألة الضوابط القانونية للتفتيش و الضبط في مجال الجرائم المعلوماتية يستلزم توافر: القواعد الموضوعية لتفتيش أنظمة الحاسوب.[69]

وتلخص هذه القواعد كالآتي: –وقوع جريمة إلكترونية. –ارتكاب شخص أو أشخاص معينين لإحدى الجرائم الإلكترونية أو الاشتراك فيها. –توافر أدلة قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية أو إلكترونية تفيد في كشف الحقيقة. –أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به.

والقواعد الشكلية لتفتيش نظام الحاسوب [70]

وتتضمن عدة قواعد نذكرها كما يلي:–أن يتم بأسلوب آلي إلكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة.–أن يكون أمر التفتيش مسببا.–تكوين فريق تفتيش يتضمن خبراء وفنيين متخصصين بالحاسوب والأنظمة الإلكترونية بالإضافة إلى رجال الشرطة المتخصصين بالحماية والأمن.

شروط الاختصاص النوعي و المحلي: على عكس أغلبية التشريعات العربية التي خولت سلطة التحقيق وحق التفتيش للنيابة العامة، فإن التشريع الإجرائي الجزائري ساير نظيره الفرنسي وجعل الاختصاص الأصيل بالتفتيش و الضبط لقاضي التحقيق، و لا يحق ذلك للنيابة العامة ممثلة في وكيل الجمهورية إلا وفق حالة التلبس بالجنحة أو الجناية . فلقاضي التحقيق أن يقوم وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها مناسبة و

[69]– عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر واالنترنت، الطبعة ألولى، دار الفكر الجامعي، ص 582،583.
[70]– خالد عياد الحلبي، المرجع السابق، ص 132،133.

ضرورية للكشف عن الحقيقة بالتحر ي عن أدلة الاهتمام و أدلة النفي ، ويجوز له بناء على ذلك الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويباشر قاضي التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقية (المادة79-80 -81(قانون الإجراءات الجزائية الجزائري."إذا كان من المتعذر على قاضي التحقيق أن يقوم بنفسه بجميع إجراءات التحقيق جاز له أن يندبوا ضابط الشرطة القضائية للقيام بتنفيذ جميع أعمال التحقيق اللازمة ضمن الشرو ط القانونية المنصوص.عليها في المواد من 138 إلى 142 من قانون الإجراءات الجزائية وباعتبار التفتيش و الضبط إجراء يستهدف جرائم عادة ما تقع إما داخل الاختصاص المحلي لقاضي التحقيق أو خارجه، فإن هذا الأخير ملزم بإتباع قواعد الاختصاص الإقليمي فهو مختص ضمن -المادة 68 ق 01 -08 قانون الإجراءات الجزائية الجزائري. في دائرة وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه فيهم، أو بمحل القبض على أحدهم، ويمتد اختصاصه تلقائيا إلى دائرة اختصاص محاكم أخرى فيما يتعلق بالجرائم المعلوماتية فاختصاصه في هذه الحالة وطني حسب ما هو مقرر بالمادة (40 ق 04 -14 ق إ ج) وكذلك الفقرة الأخيرة من نص (المادة 47 ق 06-22 ق إ ج) ، وهو نفس الاختصاص المقرر إقليميا المطبق على ضباط الشرطة 1القضائية في حال تنفيذ أوامر قاضي التحقيق. [71]

من حيث المواعيد: عندما يتعلق الأمر بالجرائم المعلوماتية فإنه يجوز التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل بناء على إذن مسبق من وكيل الجمهورية المختص .يمكن لقاضي التحقيق أن يقوم بنفسه بعملية التفتيش والضبط ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يندب ضابط الشرطة

[71]- الفقرة الأخيرة من نص (المادة 45 ق 22-06 ق إ ج)

القضائية المختص بذلك (الفقرة 03 و 04 المادة 47 ق) 22-06من قانون الإجراءات الجزائية الجزائري .

غير أنه إذا ما تعلق الأمر بجناية فلا يجوز سوى لقاضي التحقيق القيام بالتفتيش وبحضور وكيل الجمهورية (المادة 82 ق إ ج)، الفقرة الأخيرة المادة 16 ق 06-22 قانون الإجراءات الجزائية الجزائري.

مسألة حضور المشتبه فيه عملية التفتيش والضبط؛ سواء في مسكنه أو مسكن شخص آخر فإن لا تستوجب حضوره، ففي مجال الجرائم المعلوماتية لقاضي التحقيق أو لضباط الشرطة القضائية مباشرة أعمالهم دون مراعاة هذه المسألة مع ضرورة الالتزام بأحكام ضمان السر المهني والتقييد بقواعد الحجز.

إذا ما كان الشخص موقوفا للنظر أو محبوسا مؤقتا أو غائبا لسبب آخر وكان من الخطر نقله لمكان التفتيش فإنه يجوز إجراء التفتيش بعد الحصول على الموافقة المسبقة لوكيل الجمهورية، أو لقاضي التحقيق مع ضرورة حضور شاهدين (المادة 47 مكرر ق 06-22 ق إ ج).

الفرع الثاني: المعاينة والخبرة التقنية

إن التعامل في الجريمة الالكترونية يتطلب إجراءات روتينية متفق عليها وذلك من أجل حماية الدليل، غير أن وسائل حفظ الأدلة واستنتاجها تختلف من الجريمة التقليدية إلى الجريمة الالكترونية الرقمية، ذلك لأن البرامج والبيانات عنصران أساسيان يتحتم على أجهزة تنفيذ القانون وخبراء الأدلة الجنائية جمعها واستخلاصها، وتعد المعاينة والخبرة من بين إجراءات التحقيق، التي تؤدي للوصول إلى الدليل المستمد من الواقعة المجرمة، سوف نتعرض في هذا الفرع لكيفية ذلك في الجريمة الالكترونية.

أولا الانتقال و المعاينة: المعاينة هي اجراء يتضمن وصف مكان الحادث بما فيه من أشياء، اشخاص، مع الفحص الدقيق لكافة المحتويات بهدف كشف المخلفات وآثار الجاني بالمكان، والتي تشير الى شخصيته وشركائه، وما يفيد في اثبات ارتكاب الجريمة وتوضح قدرا من الاستنتاجات 2التي تشكل في حد ذاتها الأساس الذي يقوم عليه التحقيق.[1]

التحقيق.[1]

يعتبر الانتقال عملا كاملا من أعمال التحقيق بقصد جمع الأدلة وإن الانتقال إلى مسرح الجريمة وما يصاحبه من ضرورة المعاينة و التفتيش، يقتضي التعدي على حرمة الحياة الشخصية للأفراد ومساكنهم، يستوجب أن يتم في إطار قانوني لأجل ضمان شرعية الإجراءات وعدم تعريضها للبطلان الذي قد يهدم الدليل ويتسبب في إفلات المتهم من العدالة، إضافة إلى ضمان عدم التعسف في مواجهة الغير من الأفراد بحجة ضرورة التحقيق، وتجنبا لكل ذلك يستوجب القانون احترام مجموعة من الشروط القانونية المبنية في قانون الإجراءات الجزائية وأخرى في القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، لأجل إتمام هذه الإجراءات ضمن إطار شرعي وذلك حسب الأحوال التالية :

1- حسب أحوال حالة التلبس: توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال أو عقب ارتكابها، كما تعتبر كذلك إذا كان الشخص المشتبه فيه في وقت قريب جدا من وقوعها أو تبعته العامة بالصياح أو كان حائزا لأشياء أو دلائل تدعوا إلى افتراض مساهمته في الجريمة، كما توصف كذلك إذا ما ارتكبت الجناية أو الجنحة في منزل أو كشف صاحب المنزل عنها عقب وقوعها وبادر باستدعاء ضابط الشرطة القضائية لأجل[2]، إن تطبيق هذه الأحوال على الجريمة المعلوماتية يكاد أن يكون أمرا مستحيلا، غير

[1]- حازم محمد حنفي، مرجع سابق، ص 11.

[2]- المادة: 41 قانون الإجراءات الجزائية الجزائري.

أنه يمكن افتراض وقوعها ولو في نادر الأحوال و يترتب معه اتخاذ الإجراءات التالية • : إخطار وعلى الفور وكيل الجمهورية، ثم التنقل وبدون تمهل إلى مسرحها قصد اتخاذ الإجراءات اللازمة للتحري، و التي تسمح بالحفاظ على الآثار التي يخشى اختفائها[1]، لا يجوز الانتقال إلا بناء على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهاره قبل الدخول إلى مسكن المشتبه فيه، ويترتب على تنفيذ الإجراء في غياب الإذن، أو غياب أوصاف محل البحث، أو عناوين أماكن البحث، عن مضمون الإذن البطلان المطلق للإجراء برمته.[2]

ولهم حين اذن الحق في إتمام أعمالهم في أي ساعة من ساعات الليل أو النهار وذلك حسب ما تورده المادة 47 من قانون الإجراءات الجزائية.

2- **حسب ظروف الأحوال العادية:** وهي الظروف التي تميز الجريمة المعلوماتية ، و التي تحتاج إلى تقدير فني كبير لأجل التأكد من مدى صحة وقوعها، واتخاذ تقرير الإجراءات الكفيلة بمتابعة مرتكبيها واثبات الأدلة في مواجهتهم، ويتم الانتقال إلى مسرح الجريمة تنفيذا عادة لأوامر وكيل الجمهورية في إطار إتمام إجراءات البحث و التحري، أو تنفيذا لأوامر قاضي التحقيق ويشترط احترام الشروط المتعلقة بالإذن المكتوب سواء الصادر من قبل وكيل الجمهورية وقاضي التحقيق حسب الأحكام الواردة في المواد من 44 إلى 47 مكرر من قانون الإجراءات الجزائية تحت طائلة البطلان.[3]

إذن فمن الناحية القانونية فإن الشروط المتعلقة بالمعاينة والتفتيش في إطار الجريمة المعلوماتية هي نفس الشروط المتبعة في باقي الجرائم الأخرى الا أنه لأجل معاينة الجرائم

[1]- المادة: 42 قانون الإجراءات الجزائية الجزائري.

[2]- المادة 44 ق 06-22 قانون الإجراءات الجزائية

[3]- المادة 36 فقرة 04 -المعدلة بموجب الأمر 15-02 قانون الإجراءات الجزائية الجزائري.و -المادة 68 ق – 01-08 -قانون الإجراءات الجزائية الجزائري.

المعلوماتية وجب اتباع إجراءات واحتياطات خاصة والتي تعرف تحت اسم إجراءات تأمين موقع الجريمة المعلوماتية– .

ثانيا: ندب الخبراء :تعتبر الخبرة من أهم الإجراءات التي تتخذ للتثبيت عن الأدلة التي تساعد عن الكشف عن الجريمة الإلكترونية، كون الجريمة الإلكترونية ترتكب بوسائل مستحدثة ومعقدة يصعب التعامل معها.[1]

الخبرة القضائية عموما هي "الاستشارة الفنية التي يستعين بها القاضي التحقيق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه.[2]

فهي وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية والفنية والتي لا تتوافر سواء لدى المحقق أو القاضي.

فالخبير هو كل شخص له إلمام بأي علم أو فن سواء كان اسمه مقيدا في جدول الخبراء أو على مستوى المحاكم أم لا، وهو كل شخص له دراية بمسألة من المسائل، وقد يستدعي التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه، حتى يخرج التحقيق في صورة موضوعية صادقة.

1: القواعد القانونية التي تحكم الخبرة القضائية: إذا كانت الاستعانة بالخبير في الجرائم التقليدية أمر بالغ الأهمية في إثبات الجريمة، فإن الاستعانة به في مجال إثبات الجرائم الإلكترونية يعد أمرا ضروريا بسبب التطور التقني السريع في مجال تقنية المعلومات، إذ لا يكشف غموض الجريمة إلا شخص على درجة كبيرة من العلم والدراية في مجال تخصصه، حيث قيد الخبراء أو شطبهم بقرار من وزير العدل، و قد ترك المشرع لقاضي التحقيق حرية

[1]– 1ضريفي نادية، سلطات القاضي الجاني في تقدير الدليل الإلكتروني، المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04 ،العدد ، 02 219 ،ص 124.

[2]– 2عادل حافظ غانم، الخبرة في مجال الإثبات الجنائي، بحث بمجلة الأمن العام، العدد43 ،سنة1968 ص19

ندب خبير واحد أو خبراء متعددين بحسب المادة 147 من قانون الإجراءات الجزائية الجزائري، بغرض حل الدعوى المطروحة أمامه، فقد لا يطمئن القاضي الجنائي لرأي خبير فني و تقني واحد فيلجأ لرأي عدة خبراء

كذلك لم يحدد المشرع طبيعة من يقوم بالخبرة سواء كان شخصا طبيعيا، أو معنويا كمؤسسة متخصصة تعمل في مجال الحاسوب الذين يتم اللجوء إليهم خاصة في مجال الدليل الإلكتروني باعتبار أن هذا النوع من المؤسسات يملك موارد مادية من برامج و أجهزة حديثة و موارد بشرية من مهندسين متخصصين في الحاسوب و الانترنت.[1]

2- **واجبات الخبير التقني: له عدة واجبات تتمثل في**

- **:حلف اليمين:** أوجب المشرع الجزائري لضمان صحة تقرير الخبير ونيل ثقة أطراف الدعوى، أن يحلف اليمين قبل البدء في انجاز الخبرة.[2]

إنجاز الخبير لأعمال الخبرة بنفسه: لابد على الخبير أن يقوم بأعمال الخبرة بنفسه وفي حدود ما نص عليه أمر أو حكم الندب، و أن يستجيب للطلبات التي يقدمها أطراف الخصومة مثل: سماع أم شخص قادر على إعطاء معلومات فنية.[3]

الخضوع للرقابة القضائية: يتعين على الخبير أن يتولى مهمته تحت رقابة القاضي الذي عينه و أن يبقى على اتصال دائم به لأجل إحاطته علما بتطورات الأعمال التي يقوم بها، فالخبير مساعد للقاضي و معاون فني لا أكثر. - إيداع الخبرة التقنية: بعد انتهاء الخبير من أعماله التي كلف بها يقوم بإيداع الخبرة التقنية خلال المدة المحددة في أمر أو حكم الندب، وأن يقدم نتائج ما قام به من أبحاث فإن خالف ذلك جاز للقاضي استبداله

[1]- عائشة بن قارة مصطفى، المرجع السابق، ص 101 -100.

[2]- حيث تنص المادة 145 من قانون الإجراءات الجزائية على: "يحلف الخبير المقيد لأول مرة الجدول الخاص بالمجلس"

[3]- المادة 152 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

بغيره، كما يمكن أن يتخذ في حق الخبير الذي ثبت وقوع إهمال منه إجراءات تأديبية قد تصل إلى شطب اسمه من جدول الخبراء بقرار من الوزير.[1]

الفرع الثالث: الشهادة في مجال الجريمة الإلكترونية:

انها من بين الأساليب والإجراءات التقليدية للتحقيق في الجريمة واستخلاص الأدلة عموما فالشهادة بمختلف جوانبها ، وبمختلف فئات الشاهد المعلوماتي وماهي ضمانات استجواب الشاهد وماهي التزاماته ولما لم يتطرق المشرع الجزائري لتعريف الشهادة بل عمد الى تنظيمها وتحديد مجالها وشروط قبولها و حجيتها في الإثبات فالشهادة من إجراءات التحقيق وهي الأقوال التي يدلي بها غير الخصوم أمام سلطة قضاء التحقيق بشأن جريمة وقعت، سواء تعلقت تلك الأقوال بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته منها[2]. ويختلف الشاهد في مجال الجرائم الالكترونية عن الشاهد في سائر الجرائم

1: الشاهد في الجرائم التقليدية: كل شخص تناهت إلى علمه عن طريق حواسه معلومات عن واقعة إجرامية، وعليه الإدلاء للسلطات القضائية بكل ما يفيد في كشف الحقيقة عنها."

2:**الشاهد في الجرائم الالكترونية:** سماع الشاهد إجراء كسائر إجراءات التحقيق في المواد التقليدية و هو أمر متروك لتقدير قاضي التحقيق و مرتبط بظروفه، و الأصل أن يطلب الخصوم سماع شهادة من يرون، و كذلك الحال لقاضي التحقيق الذي له أن يسمع شهادة أي شاهد يتقدم و لو من تلقاء نفسه و لو بدى له أنه لا يتحرى الصدق في أقواله[3].

---

[1]- حيث تنص المادة 103 من قانون الإجراءات الجزائية على: "كل قرار يصدر بندب خبراء يجب أن تحدد فيه مهلة لإنجاز مهمته و يجوز أن تمدد هذه المهلة بناء على طلب الخبراء إذا اقتضت ذلك أسباب خاصة و يكون ذلك بقرار مسبب يصدره القاضي أو الجهة التي ندبتهم، و إذا لم يودع الخبراء تقارير هم في الميعاد المحدد لهم جاز في الحال أن يستبدل بهم غيرهم وعليهم إذ ذلك أن يقدموا نتائج ما قاموا به من أبحاث. كما عليهم أيضا أن يردوا في ظرف ثمان وأربعين ساعة جميع الأشياء والأوراق و الوثائق التي تكون قد عهد بها إليهم على ذمة إنجاز مهمتهم .... و يجوز دائما لقاضي التحقيق أثناء إجراءاته أن يستعين بالخبراء إذا رأى لزاما لذلك."

[2]- علي عدنان الفيل المرجع السابق ص61

[3]- عبد العال الدربي-مرجع سابق-ص 312.

والشاهد في مجال المعلوماتية هو ذلك الشخص صاحب الخبرة والتخصص في تقنيات الحاسوب، والذي له معلومات ومكاسب عن شبكات الحاسوب والاتصال والخدمات الخاصة بذلك، إذا كانت مصلحة التحقيق تقتضي البحث عن الأدلة داخلها، والشاهد الالكتروني عدة أصناف يجوز لقاضي التحقيق استدعاء من شاء منهم لسماعه

1-القائم على تشغيل الحاسوب والمعدات المتصلة به: وهو شخص تتوفر فيه الخبرة الكافية في مجال تشغيل الجهاز واستخدامه.

2-المبرمجون: وهم الأشخاص المختصون في كتابة البرامج المعلوماتية و هم فئتان:

أ. مخططو برامج التطبيقات: يقوم هؤلاء بالحصول على خصائص ومواصفات النظام المعلوماتي المطلوب من محلل النظم ثم تحويلها إلى برامج دقيقة لتحقق هذه المواصفات.

ب. مخططو برامج النظم: يقوم هؤلاء بتصحيح واختبار وتعديل برامج نظم الحاسوب الداخلية أي تلك الخاصة بالوظائف المتعلقة بتجهيز الحاسوب بالبرامج والأجزاء الداخلية منه.

3-المحللون: هم فئة من الأشخاص مهمتهم تحليل الخطوات وجمع ببيانات النظام المعلوماتي ثم تحليلها، أي تقييمه لوحدات منفصلة واستنتاج العلاقات الوظيفية بين هذه الوحدات.

4-مهندسو الصيانة والاتصالات: هم فئة المسؤولين عن أعمال الصيانة الخاصة بالحاسوب و الشبكات المتصلة به.

5-مديرو النظم: وهم من توكل لهم إدارة النظم المعلوماتية. و يبقى قاضي التحقيق الشخص الوحيد الذي له حرية استدعاء أيا كان منهم.

التزامات الشاهد المعلوماتي: يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج إلى أنظمة تشغيل الحواسيب أو

الشبكات، التي تحتوي على الأدلة الإجرامية و تفيد بارتكاب جريمة على سبيل الإلزام، وهو ما يعبر عنه بالالتزام بالإعلام في الجريمة الالكترونية [1]

وقد تدعمت مساهمة الشهود في مجال أعمال مباشرة الدعوى العمومية وإجراءات التحقيق بصفة خاصة ، بما فيها في مجال الجرائم المعلوماتية بموجب التعديل الأخير لقانون الإجراءات الجزائية الجزائري الصادر بتاريخ 23 جويلية 2015 بموجب الأمر 15/02والذي نص في الفصل السادس منه على إجراءات حماية الشهود و الخبراء والضحايا، بموجب نصوص المواد من 65 مكرر 19 إلى 65 مكرر 28 ،على تعزيز دور الشاهد في مسار الإجراءات ، خصوصا إذا كانت المعلومات التي سيقدمها سببا في ظهور الحقيقة في الجرائم المنظمة و الإرهابية و جرائم الفساد ، من خلال منحه الحماية القانونية والإجرائية في حال كان هناك تهديد يمس حياته أو سلامته الجسدية، أو سلامة أحد أفراد عائلته او أقاربه أو مصلحة أساسية له ، و ذلك من خلال إخفاء المعلومات المتعلقة بهويته ، تغيير مكان إقامته ، وضع خط هاتفي تحت تصرفه، تمكينه من نقطة إتصال مع مصالح الأمن ، ضمان حماية جسدية له ، وضع أجهزة تقنية وقائية بمسكنه ...إلخ ، وهي كلها إجراءات تحفيزية تعزز دور الشاهد في الكشف عن ملابسات الجريمة بما فيها المعلوماتية.

الفرع الرابع: الاستجواب في مجال الجريمة الالكترونية.

نعني بالتحقيق مع الأشخاص ذوي العلاقة مع الحاسوب، تلك الإجراءات المتعلقة بتدوين أقوال الشهود، إجراءات مواجهة المتهمين بالأدلة المتوفرة ضدهم وما يتبع ذلك من إجراءات مواجهة واستجواب بين المتهمين والأدلة المتوفرة من جهة، وبين المتهمين والشهود من جهة أخرى، و العودة بالشهود و المتهمين إلى مسرح الجريمة عند الضرورة لمناقشتهم حول أجهزة الحاسوب وملحقاته.

[1]– رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية و المكافحة، يومي 16 ،17نوفمبر 2015 ،كلية الحقوق، جامعة بسكرة، الجزائر، 2015 ،ص5.

ومن أكبر المعوقات التي تقف حائلا في نجاح المحقق في استكمال المتطلبات الإجرائية الخاصة في مواجهة المتهم، هي شخصية المحقق في حد ذاته، والمتمثلة في التهيب من استخدام الحاسوب والانترنت، إضافة إلى عدم اهتمامه بالمستجدات في مجال المعلوماتية.

وحتى تكتمل قدرات الجهات الأمنية و القضائية في هذا الشأن، وجب الاستعانة بخبراء الحاسوب في كل مراحل البحث والتحقيق، كما هو عليه الحال في التحقيق مع المتهمين والشهود، إذ أن أخذ أقوالهم واستجوابهم يعتمد على منهجية معينة، وقدرات ومواهب لا تتوفر إلا لدى المحقق الذي اكتسب خبرة مهنية في مجال التعامل مع المجرمين إضافة إلى المعرفة الفنية للخبير في مجال المعلوماتية.

ضمانات الإستجواب: يتولى عادة وفق التشريع الإجرائي الجزائي الجزائري قاضي التحقيق مهمة استجواب المتهم، وبذلك فهو إجراء ذو طابع قضائي لا يصح إلا من خلال احترام وتوافر الشروط المحددة قانونا و التي يمكننا إيجازها في النقاط التالية :

الاستجواب إجراء من إجراءات التحقيق، يقصد من وراءه التحقق من شخصية المتهم ومناقشته مناقشة تفصيلية في التهمة المنسوبة إليه ومطالبته بالرد على الأدلة القائمة في مواجهته بنفيها أو التسليم بها

وهو بذلك إجراء يحقق وظيفتين الأولى إثبات شخصية المتهم ومناقشته بالأدلة و الثانية تحقيق دفاع المتهم من خلال فتح السبيل أمامه لتفنيذ الأدلة القائمة ضده، وبالتالي مساعدة القضاء على معرفة الحقيقة وكشف ملابسات وشخصية الفاعل الحقيقي.

يختلف استجواب المتهم عن مجرد سؤاله بواسطة أحد ضباط الشرطة القضائية خلال فترة البحث و التحري، ففي هذه الحالة يكون السؤال متعلق بالوقائع المنسوبة للمشتبه فيه فقط دون مناقشة تفصيلية ودون تحقيق لدفاع المشتبه فيه.

يشترط لبدء الاستجواب استيفاء الشروط القانونية المنصوص عليها وفق قانون الإجراءات الجزائية و المقررة حسب نصوص المواد من 100 إلى 105 إضافة إلى التقييد بقواعد الموضوعية واحترام الكرامة الإنسانية للشخص المستجوب، وهي كلها ضمانات قانونية تضمن شرعية الإجراء.

الاستجواب عند الحضور الأول في الجريمة الالكترونية: وهو أن يمثل المتهم أمام المحقق لأول مرة وذلك حتى يتحقق من هويته ويحيطه علما بكل الوقائع المنسوبة إليه وينبهه بأنه حر في الإدلاء بأقواله أو عدم الإدلاء بها، كما يجب على المحقق أن يخير المتهم في أن له الحق في توكيل محام وإن كان غير قادر ماديا يجوز للمحقق أن يعين له محام من تلقاء نفسه، كما يجب على المتهم إذا ما طرا تغير على عنوانه أن يخطر المحقق.

الاستجواب في الموضوع في الجريمة الإلكترونية: ويعني الاستجواب مواجهة المتهم بالتهمة والوقائع المنسوبة إليه ومناقشته فيهما مناقشة تفصيلية ومواجهته بالأدلة القائمة ضده ومطالبته بإبداء رأيه فيها ويكون إجباري كماهو الشأن بالنسبة للجنايات أو اختياري في الجنح.[1]

الاستجواب الإجمالي في الجريمة الإلكترونية: يهدف إلى تلخيص الوقائع وإبراز الأدلة التي سبق جمعها خلال كافة مراحل التحقيق والإشارة إلى الاستعلامات التي وردت في شأن وحياة وسلوك وشخصية والسوابق العدلية للمتهم، ويختم بطرح السؤال التالي: هذا هو استجوابك الأخير فهل لديك ما تدلي به للدفاع عن نفسك؟ ويحتوي الملف الجنائي على الوثائق التالية: شهادة الميلاد المتهم، صحيفة السوابق العدلية، تقرير البحث الاجتماعي ويقصد بهذا الأخير ندب خبير لإجراء بحث اجتماعي عن حياة المتهم، وسلوكه وأخلاقه في

[1]– محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، ط3 ، 2008 ، ص108،109

المحيط الذي كان يعيش فيه وكذا محيط مهنته، وكل ما يتعلق بحياته الاجتماعية، وكذا شهادة جيرانه سواء قام به المحقق بنفسه أو عن طريق إنابة قضائية.

إن استخلاص الدليل قد يكون من خلال استجواب المتهم كما يكون من خلال سماع الشهود، ولذلك كان على من يتولى أمر البحث والتحقيق في الجرائم المعلوماتية، إتباع قواعد خاصة في مجال سماع شهود الجريمة المعلوماتية .

المطلب الثالث: إجراءات حديثة لاستخلاص الدليل الالكتروني.

تطرقنا في المطلب السابق على الإجراءات التقليدية لجمع الدليل الإلكتروني وبالرجوع إلى الأنظمة القانونية الإجرائية الحالية، يلحظ أن هناك قصورا بخصوص أساليب التحري التقليدية في استخلاص الدليل الإلكتروني. فالمشرع أجاز استخلاص الدليل عموما وفق ضوابط إجرائية معينة، كما أن هذه الإجراءات تخص استخلاص الدليل من الجرائم سواء كانت تقليدية أو مستحدثة، و الأكيد أن هذه الإجراءات غير كافية لاستيعاب كافة أشكال الجريمة الالكترونية، فهي تحتاج من المشرع تدعيمها أو استحداث أخرى جديدة لمواكبة التطورات التقنية في مجال مكافحة الجريمة الالكترونية، و ما قام به المشرع الجزائري في التعديلات المتتالية لأحكام قانون الإجراءات الجزائية، بإدر اج قواعد إجرائية جزائية جديدة وفي الوقت نفسه أحاطها بجملة من الضمانات بهدف عدم المساس بحرمة الحياة الخاصة للأفراد.

فنص المشرع الجزائري على إجراءات خاصة تهدف إلى ضبط الأدلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم الأخرى، وتتمثل هذه الإجراءات في التسرب واعتراض المراسلات وكذلك من خلال القانون 01-02 المتضمن القواعد الخاصة

للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، استحداث إجراءين آخرين هما المراقبة الإلكترونية وحفظ المعطيات.[1]

الفرع الأول: الإجراءات الحديثة لجمع الدليل الإلكتروني بموجب المادة65مكرر5إلى65مكرر18.

أولا: التسرب (الاختراق) واعتراض المراسلات. تعتبر الجريمة الإلكترونية من بين الجرائم التي يمكن اللجوء فيها إلى إجراء التسرب واعتراض المراسلات إذا اقتضت ذلك ضرورات التحري والتحقيق بشأنها.

التسرب(الاختراق) استحدث المشرع الجزائري إجراء التسرب بموجب المادة 65 مكرر 11 من قانون الإجراءات الجزائية الجزائري التي تنص على: "عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة65مكرر5أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابة حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبنية في المواد أدناه" و بخلاف إجراءات التحري السابقة الذكر التي لم يعرفها المشرع الجزائري، أورد تعريف التسرب بموجب نص المادة65مكرر12 من قانون الإجراءات الجزائية الجزائري:"يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف، يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة65مكرر14 أدناه، و لا يجوز تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم". كما حدد المشرع

[1]– 1معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2011-2012 ،ص106.

نطاق تطبيق التسرب بموجب المادة65مكرر5 سالفة الذكر والتي من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

يلاحظ من خلال التعريف السابق أن التسرب عملية تتسم بالتعقيد، فهو من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية، وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية وتقديم المتسرب لنفسه على أنه فاعل أو الشريك.

والتسرب كغيره من الإجراءات الحديثة، له ضوابط وشروط شكلية وأخرى موضوعية حتى يعتد به:

أولا: الضوابط الشكلية:

أ- **تحرير التقرير**: يلزم ضابط الشرطة القضائية المكلف بعملية التنسيق بتحرير تقرير كتابي يتضمن بيان مفصل عن جميع العناصر المتعلقة بالعملية، ويجب أن يذكر في التقرير ووفق الترتيب الزمني جميع المعلومات ذات الصلة كالأفعال التي استدعت حدوث عملية التسرب، و كذا تحديد هوية العناصر المشتبه تورطهم في الجريمة (أسمائهم و ألقابهم)، تحديد الكيفيات التي تم بها مخادعة الجناة، فيجب ذكر جميع العمليات منذ بداية التسرب حتى نهايته.

ب-الحصول على إذن بالتسرب :تنص المادة65مكرر11 من ق.إ.ج"عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة65 مكرر 5أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة مباشرة عملية التسرب ضمن الشروط المبينة أدناه"، وعليه فالجهة القضائية المختصة بإصدار الإذن هو وكيل الجمهورية أو قاضي التحقيق، ومنه لا يجوز لضابط أو أعوان الشرطة القضائية القيام به حماية للحقوق المكرسة دستوريا.

كما يجب أن يكون الإذن مكتوبا، وهذا وفق نص المادة(65 مكرر15)التي تنص على: "يجب أن يكون الإذن المسلم تطبيقا للمادة (65 مكرر 11)أعلاه، مكتوبا... وذلك تحت طائلة البطلان" ذلك أن الأصل في العمل الإجرائي الكتابة وفقا لنص المادتين(138-139)من ق.إ.ج.[1]

كما يشترط ذكر اسم الضابط المشرف، وهو ما نصت عليه المادة(65 مكرر15)بقولها: "يجب أن يكون الإذن المسلم تطبيقا للمادة 65مكرر 11 أعلاه، مكتوبا...وذلك تحت طائلة البطلان، تذكر في الإذن الجريمة التي تبرر اللجوء لهذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته ..."

ج- مدة التسرب :حددتها المادة(65 مكرر 3/15) حيث تنص "... ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة4 أربعة أشهر..."، غير أنه ومراعاة لمقتضيات التحقيق الابتدائي يمكن تجديد هذه المدة. ضمن نفس الشروط الشكلية والزمنية السابقة، وحفاظا على حياة العون المتسرب من الخطر إضافة إلى الأشخاص المسخرين، أجازا المشرع للقاضي الذي رخص بعملية التسرب أن يأمر في أي وقت بوقفها قبل انقضاء مدتها، كذلك إذا وصل إلى علمه أن معلومات تفيد باحتمال كشف العملية من طرف المجموعة الإجرامية

د- إبقاء الإذن بالتسرب خارج ملف الإجراءات إلى غاية الانتهاء من العملية: وذلك للحفاظ على السرية المطلوبة لنجاح عملية التسرب كالتي حصرها المشرع بيد القاضي الآمر بها (وكيل الجمهورية أو قاضي التحقيق)، كضابط الشرطة القضائية المشرف على العملية وكذا العون المتسرب، بعد الانتهاء من عملية التسرب، يجب إيداع رخصة التسرب في ملف

[1]- حيث تنص المادة)138 من قانون.إ.ج:"يجوز لقاضي التحقيق أن يكلف بطريق الإنابة القضائية أي قاض من قضاة محكمته أو أي ضابط من ضباط الشرطة القضائية المختصة بالعمل في تلك الدائرة أو أي قاض من قضاة التحقيق بالقيام بما يراه لازما من إجراءات التحقيق في الأماكن الخاضعة للجهة القضائية التي يتبعها كل منهم، ويذكر في الإنابة القضائية نوع من الجريمة موضوع المتابعة وتؤرخ وتوقع من القاضي الذي أصدرها وتمهر بختمه ."...

الإجراءات وهذا وفقا لنص المادة65(مكرر 6/15)التي تنص على:"... تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب."

ثانيا: الضوابط الموضوعية :تتمثل الضوابط الموضوعية لعملية التسرب في شرطين رئيسيين هما :

أ- **التسبيب:** يعتبر التسبيب أساس العمل القضائي، وعليه و يجب على وكيل الجمهورية أو قاضي التحقيق عند إصدار الإذن بالتسرب توضيح الأدلة القانونية والموضوعية بعد تقدير جميع العناصر المعروضة عليه من طرف ضابط الشرطة القضائية[1]. وهذا طبقا لنص المادة (65 مكرر 05)التي تنص على:"يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11أعلاه مكتوبا ومسببا وذلك تحت طائلة البطلان."...

ب-نوع الجريمة: وقد حصرتها المادة (65 مكرر 5)من قانون .إ.ج(في سبعة أنواع الجرائم التالية - :جرائم المخدرات - .الجريمة المنظمة العابرة للحدود الوطنية - .الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات - .جرائم تبييض الأموال - .الجرائم الموصوفة بأفعال إرهابية أو تخريبية - .الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد.[2]

وعليه يجب أن تكون الجريمة جناية أو جنحة.

الفرع الثاني الإجراءات الحديثة لجمع الدليل الإلكتروني بموجب القانون09-04.

تطرقنا سابقا إلى بعض الإجراءات التقليدية المتعلقة بجمع الدليل الإلكتروني وخلصنا إلى عدم كفايتها لاستيعاب كافة أشكال هذا النوع المستحدث من الجرائم، مما دفع بالمشرع الجزائري إلى استحداث أساليب بحث وتحري جديدة تتلائم وخطورة هذه الجرائم. ونظرا للطبيعة الخاصة للجرائم الإلكترونية، لم يكتفي المشرع باستخدام هذه الأساليب حينما تقع الجريمة، ولكن أيضا قبل وقوعها. وعليه صدر القانون رقم: 09-04 المؤرخ في 5 أوت

[1]- سيدهم سيدي محمد، محاضرة حول التسرب حسب تعديل قانون الإجراءات الجزائية، محكمة فرندة، مجلس القضاء تيارت.

[2]- المادة 65 مكرر 12من قانون الإجراءات الجزائية، (أحسن بوسقيعة، التحقيق القضائي، دار هومة، ط6 ،الجزائر،2009 ،ص 114) .

2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي جاء لتكريس إطار قانوني أكثر ملائمة وانسجاما مع خصوصية وخطورة الجريمة الإلكترونية.

نص هذا القانون على جملة من الإجراءات الهامة، وعليه سنتناول مراقبة الاتصالات الإلكترونية و حالات اللجوء إليها في أولا، ثم نتطرق إلى تفتيش المنظومة المعلوماتية ثانيا وحجز المعطيات ثالثا.

أولا: مراقبة الاتصالات الإلكترونية وحالات اللجوء إليها: سنحاول التطرق من خلال هذه الفقرة إلى تعريف مراقبة الاتصالات الإلكترونية وحالات اللجوء إليها وشروطها.

أ/المقصود بمراقبة الاتصالات الإلكترونية: لم يتطرق المشرع الجزائري شأنه شأن أغلب التشريعات المقارنة إلى تعريف مراقبة الاتصالات الإلكترونية، لكنه بالمقابل أوضح لنا مفهوم الاتصالات الإلكترونية بموجب المادة2من القانون رقم: 09- 04 سالف الذكر [177] 177 -يزيد بوحليط، المرجع السابق، ص ص 303 -304) . 1 والتي تنص على: "يقصد في مفهوم هذا القانون ما يأتي...: -الاتصالات الإلكترونية: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية، وبذلك وسع المشرع الجزائري من مفهوم الاتصالات الإلكترونية والتي تتم بأي وسيلة إلكترونية حديثة كجهاز الفاكس والهاتف النقال...الخ." بالرجوع إلى المفهوم الفقهي لمراقبة الاتصالات الإلكترونية الذي يعني: "العمل الذي يقوم به المراقب باستخدام الاتصالات الإلكترونية لجمع معطيات عن المشتبه فيه سواء أكان الخاضع للمراقبة شخصا أو مكانا، أو شيئا ومثال ذلك مراقبة أحد الأشخاص ممن قام باختراق الحاسب الآلي الخاص بالمجني عليه أو القيام بإعداد بريد إلكتروني مستنسخ في مراقبة المشتبه فيه عند إرساله أو

استقبال لصور دعارة الأطفال عبر الانترنت، وإفراغ ما تسفر عنه المراقبة الإلكترونية في تقارير آمنة[1]. أو هي "مراقبة شبكة الاتصالات".[2]

ب/حالات اللجوء للمراقبة الإلكترونية: مما لا شك فيه أن مراقبة الأحاديث والاتصالات الخاصة كالتي تتم بالوسائل الإلكترونية، تمس بحق الإنسان في الخصوصية المكفولة دستوريا في مختلف التشريعات الحديثة، وعليه لم يترك المشرع الجزائري الأمر على إطلاقه استجابة للمواثيق الدولية وحماية لحقوق الإنسان في هذا المجال، حيث نصت المادة04 من القانون 09-04 سالف الذكر على الحالات التي يجوز فيها مراقبة الاتصالات الالكترونية حيث تنص على: "يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 من القانون 09-04 في الحالات الآتية :أ-للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة. ب-في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني. ج-لمقتضيات التحريات كالتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية. د-في إطار تنفيذ طلبات المساعدة القضائية الدولية. لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعبله إلا بإذن مكتوب من السلطة المختصة.

ج/ شروط مراقبة الاتصالات الالكترونية: كما رأينا سلفا، وحفاظا على الحق في سرية المراسلات بكافة أنواعها والمكفولة دستوريا، أحاط المشرع الجزائري إجراء المراقبة الالكترونية تحت طائلة البطلان بشروط قانونية، تتمثل في النقاط الآتية:

1. **وجود إذن قضائي:** أوجب المشرع الجزائري وجود الإذن القضائي الصادر عن السلطة القضائية المختصة وذلك بموجب المادة05/4من القانون 09-04 سالف الذكر التي تنص على:"...لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب

[1]- حجية الدليل ناير نبيل عمر، مرجع سابق، ص149، راجع أيضا: عفيفي كامل عفيفي، مرجع سابق، ص ص474 -475

[2]- نعيم سعيداني، المرجع السابق، ص183.

من السلطة القضائية، عندما يتعلق الأمر بالحالات المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه إذنا لمدة ستة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.[1]

2. **وجود ضرورة:** يتم اللجوء إلى إجراء مراقبة الاتصالات الالكترونية في حالة توفر معومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو لمقتضيات التحريات كالتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

ثانيا: تفتيش المنظومة المعلوماتية: عرفت المادة 2/2من القانون رقم: 09-04 سالف الذكر المنظومة المعلوماتية "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، كما عرف أيضا النظام المعلوماتي على أنه: "جهاز يتكون من مكونات مادية ومكونات منطقية وذلك بغرض المعالجة الآلية للبيانات الرقمية، وهو يشتمل على وسائل الإدخال والإخراج كتخزين البيانات، وهذا قد يكون منفردا أو متصلا بمجموعة من الأجهزة المماثلة عن طريق شبكة ."جعل المشرع الجزائري من إجراء التفتيش مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة الإلكترونية، وذلك من خلال القيام بعمليات المراقبة المسبقة وفق نص المادة 3 من القانون رقم:09-04 السالف الذكر، التي تنص على:"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

[1]- تجيز بعض التشريعات الوطنية كالقانون الأمريكي وضع أجهزة لتسجيل الاتصالات الالكترونية في حالة الضرورة دون إذن من النيابة العامة، إذا توفر خطر على الحياة أو خطر جسيم على السلامة الجسدية، خالد ممدوح إبراهيم، فن التحقيق، المرجع السابق، ص 351

قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش كالحجز داخل منظومة معلوماتية" من جهة أخرى يهدف التفتيش المنصب على المنظومة المعلوماتية إلى استخلاص الدليل الإلكتروني، قبل قيام المجرم المعلوماتي بتدميره أو إخفائه للإفلات من العقوبة. لكن ما هي الجهة القضائية المختصة بمنح الإذن بالتفتيش؟ هذا ما سنجيب عنه.

الجهة القضائية المختصة بذلك :بالرجوع إلى المادة 04/أ من القانون رقم: 09-04 السالف الذكر، يبين لنا المشرع الجهة القضائية المختصة بهذه الحالة في المادة نفسها الفقرة الأخيرة إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضابط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المنصوص عليها بموجب المادة13 من القانون نفسه، إذنا لمدة6 ستة أشهر قابلة للتجديد، وذلك على أساس طبيعة ونوعية الترتيبات التقنية المراد أخذها بخصوص الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية."

ثالثا: حجز المعطيات المعلوماتية .يظل الهدف الأساس لعملية تفتيش المنظومة المعلوماتية، هو وضع اليد على الأدلة الرقمية لإدانة المجرم الإلكتروني، فإذا كان حجز الأشياء المادية كالمعدات(المكونات المادية للحاسوب) و الأوراق والمستندات...الخ، لا يعد مشكلة ويتم وفق القواعد الإجرائية التقليدية، غير أن الأمر يختلف تماما، إذ ليس من السهل توقيع الحجز على المنظومة المعلوماتية التي هي في الأصل شيء معنوي غير ملموس. وطبقا لنص المادة06من القانون رقم:09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تنص على:"عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأن وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية". يجب في كل الأحوال على السلطة التي تقوم

بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي يجري بها العملية.

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

1. **الحجز عن طريق منع الوصول إلى المعطيات.** نص المشرع الجزائري في المادة7 من القانون ر قم:09-04 السالف الذكر "إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة6 أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الدخول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها ."...والملاحظ أن المشرع لم يحدد الأسباب التقنية المانعة للحجز سواء ما تعلق بالمنظومة المعلوماتية نفسيا كاستحالة الدخول لوجود كلمة السر أو نظام حماية يصعب اختراقه، لذلك نص على ضرورة إجراء تدابير احترازية من طرف المختصين باستعمال الوسائل التقنية المناسبة القصد منه عدم تمكين المجرم من الوصول 182 للمعطيات المخزنة في المنظومة المعلوماتية

2. **حدود استعمال المعطيات.** تطرقنا فيما سبق إلى أن إجراء مراقبة الاتصالات الالكترونية يمس بحق الأشخاص في سرية مراسلاتهم ومنها المراسلات الالكترونية، وهو حق مكفول دستوريا، لذا نص المشرع الجزائري تحت طائلة العقوبات على حدود استعمال المعلومات المتحصل عليها من عمليات المراقبة، إلا فيما تتطلبه التحريات والتحقيقات القضائية، وهذا بموجب نص المادة9من القانون رقم: 09-04 السالف الذكر التي تنص على: "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."

المبحث الثاني: حجية الدليل الالكتروني في نطاق الاثبات الجنائي.

إن عملية تقدير الأدلة تعد جوهر الحكم الذي نريد الوصول إليه، ويتم ذلك بممارسة القاضي لسلطته التقديرية على الأدلة التي هي محل الوقائع، و بخصوص الجريمة الإلكترونية يكون الدليل الإلكتروني هو الأوفر، ومن هنا نتساءل هل مشروعية الدليل الالكتروني تعبر عن الحقيقة التي تهدف إليها الدعوى الجنائية، وعلى ذلك تكون الإجابة على هذا الإشكال من خلال تعرضنا لدراسة ما يلي: في المطلب الأول نعرج على دراسة مناقشة الدليل الالكتروني أمام قاضي الحكم والأساس الذي يقبل به الدليل الإلكتروني في الإثبات الجنائي ونتطرق في المطلب الثاني الى مدى تقدير الدليل الإلكتروني والى القيود الواردة على حرية القاضي الجنائي في قبول الدليل الإلكتروني.

أما المطلب الثالث، فندرس حجية الدليل الالكتروني في الأنظمة اللاتينية. والمطلب الرابع حجية الدليل الالكتروني أمام الأنظمة الأنجلو سكسونية.

المطلب الأول: مناقشة الدليل الالكتروني أمام قاضي الحكم.

الدليل الإلكتروني بإعتباره دليل إثبات في الجرائم الالكترونية يخضع للمبدأ العام في الإثبات الجنائي وهو استقلالية القاضي في الاقتناع، ومع تطور دور الإثبات العلمي في ظهور الدليل الإلكتروني كدليل إثبات في الجرائم الإلكترونية، مما ألزم القاضي التعامل مع هذا النوع الجديد من الأدلة لكشف خلفيات جديدة لم تكن مسبقا في الجرائم. والدليل الإلكتروني

وعلى ذلك سنتطرق إلى مبدأ حرية الإثبات الجنائي كأساس لقبول الدليل الإكتروني في الفرع الأول، ثم في الفرع الثاني. عرض الدليل الالكتروني ومناقشته من قبل أطراف الخصومة الجزائية.

الفرع الأول: مبدأ حرية الإثبات الجنائي كأساس لقبول الدليل الإلكتروني:

يملك القاضي سلطة مطلقة في الأخذ بأي دليل يسهم في إثبات وقائع الجريمة، فليس هناك دليل مفروض عليه أن يستعين به في تكوين قناعته منه و بناء عقيدته عليه، حيث أن حرية القاضي في تقدير وسائل الإثبات المطروحة أمامه في الدعوى نتيجة منطقية لمبدأ القناعة الشخصية وهي نتيجة ثانية إلى جانب حرية القاضي في الإستعانة بكل وسائل الإثبات، فالقاضي الجنائي له أن يقبل أي دليل إثبات أي واقعة ذات أهمية في الدعوى الجنائية، أي أنه لا يحتج عليه بأي دليل ما لا يجوز له أن يستمد إقتناعه منه وله السلطة في إستبعاد أي دليل لا يقتنع به.[1]

وتعتبر حرية الإثبات في المسائل الجنائية من المبادئ المستقرة في نظرية الإثبات الجنائي، وذلك بخلاف المسائل المدنية حيث يحدد القانون سافا وسائل الإثبات وقواعد قبولها وقوتها.

ومنه إعتمد المشرع الجزائري في الإثبات على مبدأ حرية الإثبات كأصل ونظام الأدلة القانونية كإستثناء من الأصل.[2]

فتنص المادة 1/212 من قانون الإجراءات الجزائية:" يجوز إثبات الجرائم بأي طريق من طرق 1الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك[3]. وتنص أيضا المادة 213 من قانون الإجراءات الجزائية[4]، شأنه كشأن جميع عناصر الإثبات يترك لحرية القاضي.[5]

---

[1]- نوال شعلال، سلطة القاضي الجنائي في تقدير الأدلة، مذكرة مقدمة لنيل شهادة الماجستير، فرع قانون العقوبات والعلوم الجنائية، جامعة سكيكدة، 2008-2009، ص 84.

[2]- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة للنشر والتوزيع، الجزائر، 2008،ص38.

[3]- المادة 212 من الأمر 66-155 المؤرخ في 18 صفر 1386، الموافق ل 08 يونيو 1966 ،المتضمن قانون الإجراءات الجزائية المعدل والمتمم،الجريدة الرسمية عدد 48 ،الصادرة يتاريخ 28 يونيو 1966 ،ص 644 . ومن الملاحظ أن المشرع الجزائري أدرج نص المادة 212 من قانون الإجراءات الجزائية ضمن الأحكام المشتركة والمتعلقة بطرق الإثبات أمام جهات الحكم مما لا يدع أي شك في تطبيقها أمام كل الجهات القضائية الجزائية

[4]- الإعتراف لغة هوالإقرار، و في معجم الوسيط:" اعترف بالشيء أقر به ،يقال: إعترف بذنبه ".أنظر: نجيمي جمال، إثبات الجريمة على ضوء الإجتهاد القضائي، دار هومة للنشر والتوزيع، الجزائر، 2012 ،ص 157.

[5]- المادة213من الأمر 155/66 المذكور أعلاه ص644

مبدأ حرية الإثبات يعد بمثابة إقرار ضمني من المشرع بعدم قدرة الأدلة التقليدية والتي تم حصرها، كأدلة إثبات في مواجهة الجرائم المستحدثة ومنها الجريمة الإلكترونية، بمعنى فتح الباب لنوع من الأدلة العلمية للإستفادة من الوسائل التي يكشف عنها العلم الحديث كبصمة الصوت والبصمة الوراثية DNA والدليل الإلكتروني. وعلى ذلك نلاحظ أن الدليل الإلكتروني شأنه في ذلك شأن الأدلة الأخرى، التي تم ذكرها على سبيل المثال في القانون مقبول مبدئيا في الإثبات الجزائي بصفة خاصة، إذا ما تم إحترام فيه ضابط المشروعية، ذلك لأن الحرية هنا لا يقصد بها إمكان اللجوء إلى وسائل غير مقبولة قانونا، فحرية الأطراف في مجال الإثبات يجب أن تمارس في إطار ما تفرضه عليه ضوابط المشروعية من قيود يستحيل مخالفتها، وإلا ترتب على ذلك عدم مشروعية ذلك الدليل، ومن ثم عدم قبوله بل بطلانه[6])

إن إعمال مبدأ حرية الإثبات يجعل من دور القاضي الجزائي دور إيجابي[7] في كشف الحقيقة الفعلية في الجرائم التقليدية منها والمستحدثة كالجرائم الالكترونية و يبدو هذا الدور من ثلاث جوانب:

الأول: له الحرية في توفير الدليل المناسب والضروري للفصل في الدعوى بما في ذلك الدليل الإلكتروني،

الثاني: له الحرية في توفير أي دليل يمكن أن تتولد منه قناعته بما في ذي ذلك الدليل الإلكتروني،

الثالث: أنه يتمتع بالحرية نفسها في تقدير قيمتها الإقناعية حسب وجدانه.

---

[6]- عائشة بن قارة، المرجع السابق، ص 188 ص 189.

[7]- يقصد بالدور الإيجابي للقاضي الجزائي في توفير الدليل عدم إلتزامه بما يقدمه إليه أطراف الدعوى من أدلة، و إنما له سلطة بل و واجب عليه أن يبادر من تلقاء نفسه إلى إتخاذ جميع الإجراءات لتحقيق الدعوى، و الكشف عن الحقيقة الفعلية فيها، أنظر: عادل مستاري، "دور القاضي الجزائي في ظل مبدأ الإقتناع القضائي،" مجلة المنتدى القانوني، العدد الخامس، جامعة محمد خيضر، بسكرة، ص 182. و دور القاضي هذا لا يكمن في الموازنة بين الأدلة التي يقدمها الخصوم، ولا يجوز له أن يقنع بفحص الأدلة المقدمة له، إنما يتعين عليه أن يتحرى بنفسه أدلة الدعوى و يدعو الأطراف إلى تقديم أدلتهم، أنظر: محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية،1988،ص417

وتكمن مظاهر الدور الإيجابي للقاضي الجزائي في البحث عن الحقيقة وكشفها من خلال المرحلتين الأساسيتين للدعوى الجزائية(مرحلة التحقيق الإبتدائي و مرحلة المحاكمة)، على إعتبار أن مرحلة التحقيق الإبتدائي هي المرحلة التحضيرية لمرحلة المحاكمة، حيث يتم فيها حشد الأدلة و تمحيصها لتحديد مدى كفايتها لإحالة المتهم على المحكمة المختصة.

.أ/ **مرحلة التحقيق الإبتدائي:** يتحدد الدور الإيجابي للقاضي الجزائي على حسب السلطة المناط بها التحقيق، و مهمة قاضي التحقيق هي القيام بإجراءات البحث و التحري عن الجرائم وهذا ما نصت عليه المادة38من قانون الإجراءات الجزائية، و التي تهدف إلى الكشف عن الحقيقة، و يقوم بالعديد من الإجراءات الهادفة إلى جمع الأدلة و المحافظة عليها (الإنتقال والمعاينة، التفتيش، الخبرة ، ضبط الأشياء، والإستجواب...إلخ)

ب/ مرحلة المحاكمة: هناك العديد من النصوص التي تبين مظاهر الدور الإيجابي للقاضي الجزائي، نذكر منها المادة 286 من قانون الإجراءات الجزائية" ...له سلطة كاملة في ضبط حسن سير الجلسة وفرض الإحترام الكامل لهيئة المحكمة، وإتخاذ أي إجراء يراه مناسبا لإظهار الحقيقة." والمادة235من نفس القانون "يجوز للجهة القضائية إما من تلقاء نفسها أو بناءا على طلب النيابة العامة أو المدعي المدني أو المتهم أن تأمر بإجراء الإنتقالات اللازمة لإظهار الحقيقة ." ... و تطبيقا على الجرائم الإلكترونية، فإن القاضي الجزائي و في سبيل الوصول إلى الحقيقة ، له أن يوجه أمرا إلى مزود الخدمة بتقديم المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم والإتصال وكذا عناوين المواقع المطلع عليها ... إلخ و من أبرز مؤشرات أو دلائل الدور الإيجابي للقاضي الجزائي في البحث عن الدليل الإلكتروني أيضا، أن للقاضي الجزائي سلطة الأمر بإعتراض الاتصالات السلكية واللاسلكية متى ما قدر فائدة الإجراء و جديته و ملائمته لسير الدعوى.

كما للقاضي الجزائي ندب الخبراء ، وكذا إعلانهم ليقدموا إيضاحات عن التقارير المقدمة منهم، لما للخبرة في مجال المساعدة القضائية من دور كبير، فهي تعد من أقوى مظاهر تعامل قاضي الموضوع مع الواقعة الإجرامية المعروضة ، و يمكن القاضي تعيين

الخبراء لاسيما أن الأصل يظل للتحقيق الذي تجريه ا لمحكمة في الجلسة، وهذا ما أكدته المادة 143 من قانون الإجراءات الجزائية حينما نصت "لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناءا على النيابة العامة و إما من تلقاء نفسها أو من الخصوم..." و في مجال البحث عن الدليل الإلكتروني نجد أن الخبرة التقنية في مجال المساعدة القضائية تعد أقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات و الأنترنت خاصة إزاء نقص المعرفة القضائية الشخصية لظاهرة تقنية المعلومات.

الفرع الثاني: عرض الدليل الالكتروني ومناقشته من قبل أطراف الخصومة الجزائية.

تعد مرحلة قبول الدليل الإلكتروني المرحلة أو الخطوة التالية التي تلي البحث عن الدليل و تقديمه من قبل جميع الأطراف(سلطة الإدعاء، المتهم، القاضي) و في هذا الصدد و طبقا لمبدأ الشرعية الإجرائية التي يتحصل من خلالها الدليل الإجرائي بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية كالكمبيوتر المحمول مثلا، لا يكون الدليل مقبولا في عملية الإثبات والتي يتم من خلالها إخضاعها للتقدير، إلا إذا كان مشروعا، ذلك أن القاضي لا يقدر إلا الدليل المقبول ولا يكون ذلك إلا إذا كان مشروعا بأن يتم البحث عنه و الحصول عليه وفقا لطرق مشروعة)[8]. فالقاضي الجنائي ملزم بفحص الدليل الإلكتروني كقاعدة عامة لكي يتوصل إلى تشكيل قناعته على الدليل، انطلاقا من عرض هذا الدليل من جهة، ومن جهة أخرى أن يطرح بالجلسة ويتم مناقشته من طرف الخصوم، لذلك فإن الأمر يتطلب وجوب توافر مجموعة من الشروط في الدليل الرقمي حتى يعبر عن حقيقة علمية ثابتة أولا ومناقشته على الأطراف في الخصومة ثانيا.

[8]- رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012، ص ص 486 ، 487.

ان حرية الدليل الجنائي الرقمي مشروطة بأن يكون الدليل الذي يستند اليه القاضي قد طرحت مناقشته بالجلسة ويكون كذلك متى كان له أصل ثابت في أوراق القضية المطروحة على القاضي، وهو ما يجعل هذه الأدلة متاحة للخصوم لكي يتمكن كل خصم من إعداد دفاعه فإن كان الدليل في صالحه يدافع عنه وإن كان ضده يشك فيه وبضعفهن ويمكن للقاضي حينئذ أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحكمة وخضعت لحرية مناقشة أطراف الدعوى، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال البيئة الالكترونية يجب أن يعرض في جلسة المحكمة ليس من خلال ملف الدعوى في التحقيق الابتدائي وإنما يعرض بصفة مباشرة أمام القاضي وتتمثل في:

-1/وجوب طرح الدليل بالجلسة وحصول مناقشة فيها: ويقصد بمناقشة الأدلة الجنائية بصفة عامة ان القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلست المحاكمة، وخضعت لحرية مناقشة أطراف الدعوى، ولا يختلف الأمر بالنسبة للأدلة الإلكترونية بوصفها أدلة اثبات إذ ينبغي أن تطرح في الجلسة وأن يتم مناقشتها في مواجهة الأطراف، فالعبرة في المحاكمات الجزائية أن يكون باقتناع القاضي بناء على الأدلة المطروحة عليه غما بإدانة المتهم أو براءته ولا يصح مطالبته الأخذ بالدليل، ويجب أن تكون أوراق الدعوى مطروحة أمام القاضي وتحت نظر الخصوم وذلك حتى يتسنى للخصوم الإطلاع عليها والإدلاء برأيهم فيها، وقد نص عليها المشرع الجزائري من خلال المادة2/212من قانون الاجراءات الجزائية"...ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه." وقد قضت المحكمة العلا:"من البادئ الأساسية التي تحكم إجراءات المحاكمة أن يقع التحقيق النهائي شفويا بالجلسة وان يقتنع قاضي الحكم بتكوين اقتناعه على ما دار أمامه من المرافعات طبقا للمادة212من قانون الاجراءات الجزائية " كما قضت المحكمة العليا "من المقرر قانونا أنه لا يسوغ للقاضي أن يبني قراره غلا على الأدلة المقدمة في معرض المرافعات والتي حصلت

المناقشة حضوريا أمامه، ومن ثم فإن القضاء بما يخالف ذلك يعد خرقا للقانون"[9]. ويترتب على قاعدة وجوب طرح الدليل في الجلسة وحصول مناقشة فيه نتيجتين هما:[10]

– أن لا يقضي القاضي بناء على معلوماته الشخصية؛ القاعدة العامة هي أن بمتنع القاضي بعلمه الشخصي، التي يكون قد حصل عليها خارج نطاق الدعوى المطروحة أمامه والتي من الممكن ان تؤثر في تكوين قناعته عند تقدير الأدلة، ويرجع أساس عدم الحكم بعلمه الشخصي إلى أن علم القاضي يكون دليلا في الدعوى ولما كان للخصوم حق مناقشة هذا الدليل يقتضي أن ينزل منزلة الخصوم فيكون خصما وحكما في وقت واحد وهذا لايجوز.[11] ففكرة عدم جواز أن يقضي القاضي في جرائم الأنترنت بناء على معلوماته الشخصية من أهم النتائج المترتبة على قاعدة وجوب مناقشة أو طرح الدليل الجنائي سواء كان دليلا تقليديا أم الكترونيا في الجلسة لأنه لا يسوغ للقاضي أن يحكم بمقتضى معلوماته الشخصية في الدعوى أو على ما رآه بنفسه أو حققه في مجلس القضاء بدون حضور الخصوم، وذلك أن هذه المعلومات لم تعرض في الجلسة والمتمم لمناقشتها وتقيمها ومن ثم يكون الاعتماد عليها مناقضا لقاعدتي الشفوية والمواجهة التي تسود مراحل المحاكمة وتجدر لفت الانتباه الى أن هذه القاعدة لا يجب أن تتعارض مع البحث عن الحقيقة والاستعانة بكافة وسائل الاثبات طالما تطرح هاته الأدلة للمناقشة بين الأطراف.[12]

– أن لا يحكم القاضي بناء على رأي الغير؛ من الآثار التي يتقيد بها القاضي الجنائي في تكوين اقتناعه عدم تعويله على راي الغير بل يجب أن يستمد هذا الاقتناع من مصادر يستقيها بنفسه من التحقيق في الدعوى، وهذه نتيجة هامة من نتائج مناقشة الدليل في

[9]– القرار صادر عن المحكمة العليا الغرفة الجزائية بتاريخ 2005/06/29طعن رقم301387، مجلة المحكمة العليا العدد الأول لسنة 2006ص 583

[10]– نصر الدين مروك محاضرات في الاثبات الجنائي النظرية العامة للإثبات الجنائي الجزء الأول دار هومة الجزائر 2003ص458.

[11]– فاضل زيدان محمد سلطة القاضي الجنائي في تقدير الأدلة دراسة مقارنة دار الثقافة للنشر والتوزيع 2008ص249.

[12]– 1إلياس أبو عيد نظرية الإثبات في أصول المحاكمات المدنية والجزائية بين النص والاجتهاد والفقه، دراسة مقارنة الجزء الثالث لمنشورات زين الحقوقية بيروت لبنان 2005ص406.

الجلسة، فالقاضي لا يجوز له أن يعتد برأي غيره مهما كانت صفتهم وله أن يستأنس برأي خبير ذو كفاءة عالية موثوق في قدراته ونتائجه.

إن قاعدة وجوب احترام مناقشة الدليل الجزائي سواء كان دليلا تقليديا أم الكترونيا هو يشكل ضمانة هامة من ضمانات المحاكمة العادلة، وذلك بوجوب احترام الحق في الدفاع و يترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم الالكترونية بناءا على علمه الشخصي أو استنادا اليه ضمن باقي الأدلة القائمة في أوراق الملف والدعوى العمومية المعروضة عليه.[13]

وعليه فالغرض من التأكيد على وجوب احترام هذا المبدأ هو أنه يشكل ضمانة هامة من ضمانات المحاكمة العادلة، وذلك بموجب احترام الحق في الدفاع، بالإضافة الى تفادي اعتماد القاضي في حكمه على معلوماته الشخصية أو معلومات الغير.[14]

-المواجهة بين الخصوم أثناء المحاكمة:

فالمقصود بحسب المادة2/212من قانون الإجراءات الجزائية هو قاعدة المواجهة، بمعنى مواجهة أدلة كل خصم للآخر بحيث يتاح لكل منهما إبداء أدلته ودفاعاته، وفي النهاية يتسنى للقاضي تكوين اقتناعه من خلال هذه المواجهة، حيث يستند مبدأ مناقشة الأدلة الجنائية عبى قواعد أساسية تتمثل في شفهية المرافعة بحسب المواد300و304و353من قانون الإجراءات الجزائري والتي يقصد بها وجوب أن تجري المرافعة شفويا ، بصوت مسموع، لجميع إجراءات المحاكمة مبدأ العلنية بحسب المواد355،342،285و399من قانون الإجراءات الجزائية فالشهود والخبراء يدلون باقوالهم شفويا امام القاضي ويناقشون فيها أيضا شفويا.

[13]- نعيم سعيداني المرجع السابق، ص219.

[14]- نصر الدين مروك المرجع السابق ص241.

وعليه بترتب الإخلال بمناقشة الأدلة الجنائية بطلان الأدلة وعدم الإعتداد بها، وذلك بسبب أن الإخلال بمبدأ المناقشة يحرم خصوم الدعوى العمومية من الاطلاع على الأدلة المتولدة من الحاسبات الالكترونية وبالنسبة لشهود الجريمة الالكترونية الذين يكون قد سبق أن سمعت أقولهم في التحقيق الابتدائي، فإنه يجب أن بتم إعادة سماعهم مرة أخرى من جديد أمام المحكمة، كذلك بالنسبة لخبراء المعلوماتية على إختلاف تخصصاتهم ينبغي أن يمثلوا أمام المحكمة لمناقشتهم ومناقشة تقاريرهم التي خلصوا اليها[15]. وعلى هذا الأساس فمناقشة الأدلة الجنائية الرقمية قد تتطلب مؤهلات تقنية ومعارف فنية غير التي تتوفر في القاضي، وهو ما يؤدي بنا إلى القول بضرورة التأهيل التقني والفني للقضاة لمواكبة المناقشة العلمية للأدلة الجنائية الرقمية، وذلك بسبب أن هذا النوع من الأدلة أصبح غير مقتصر على إثبات الجريمة الإلكترونية فقط بل اصبح بالإمكان الاعتماد عليه لإثبات الجريمة التقليدية نظرا للتطور الكبير الذي تشهده الجريمة.[16]

المطلب الثاني: تقدير الدليل الالكتروني أمام قاضي الحكم.

ان الوصول إلى الحقيقة في مرحلة التقاضي، هي المرحلة الحاسمة في الدعوى الجنائية، وهذا الأمر يتم عن طريق الأدلة المتوفرة لدى القاضي اجنائي الذي يمارس سلطته التقديرية، وفي مجال الجريمة الإلكترونية يكون الدليل الإلكتروني هو الأوفر، كما أن التطور التكنولوجي الحاصل في الوقت الراهن حتم على القضاء الجنائي أن يأخذ بهذا النوع من الأدلة المستحدثة، بالإضافة إلى أن القاضي الجنائي حر في الأخذ بالأدلة الإلكترونية خاصة فيما يتعلق بالجرائم الإلكترونية، والدليل الإلكتروني من الوجوب ان يكون مقبولا في الإثبات الجنائي، وأمام القضاء الجنائي باعتبار انه ذو مصداقية كبيرة، وهذا راجع لطبيعته العلمية والتقنية، وهذا ما يحتم على القضاء الجنائي أن ينظر في موضوع الأخذ بالدليل

[15]- نعيم سعيداني المرجع السابق ص216.

[16]- 3طاهري عبد المطلب المرجع السابق ص57.

الالكتروني ويعطي له الحجية والقوة الثبوتية اللازمة، آخذا في عين الاعتبار أهمية هذا الدليل في إثبات العديد من الجرائم بصفة عامة، والجرائم الإلكترونية بصفة خاصة فالقاضي الجزائي بالنظر للتطور التكنولوجي الحاصل، يجدنفسه مضطرا إلى النظر في موضوع الدليل الإلكتروني.

فإن اعظم ما يقع على عاتق القاضي هو تقدير أدلة الإثبات والاقتناع بها، وهذا باعتبار أن القاضي لا يقدر إلا الدليل المقبول، وذلك حتى لا يدان بريء ولا يفلت مجرما، فالقاضي قبل أن يصدر حكمه يقوم بالبحث عن الحقيقة، وهو في سبيل ذلك بقوم بفحص الأدلة الجنائية ويطرحها في الجلسة لتناولها الخصوم بالفحص سعيا للوصول إلى الحقيقة التي ترضي ضميره، وتكوين اقتناعه الشخصي لتحقيق العدالة، فقد كان من الضروري وضع ضوابط وقيود يتعين أن تمارس سلطة القاضي في إطار، حتى لا تنحرف عن الهدف المنشود من قبل المشرع، ألا وهو الوصول الى الحقيقة التي تمثل الهدف الاسمى لقانون الإجراءات الجزائية.

ولهذا سيكون من الجدير دراسة مدى سلطة القاضي في قبول الدليل الإ(لكتروني الذي تحكمه مجموعة قيود تحد من حرية القاضي الجزائي في قبوله ثم دراسة ضوابط إقناع القاضي الجزائي بالدليل الالكتتروني.

الفرع الأول: سلطة القاضي الجزائي في تقدير الدليل الرقمي:

إن الأصالة العلمية للدليل الرقمي جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف فقهي، إذا أن هناك من يرى أن الدليل العلمي ومنه الدليل الرقمي له قوته الثبوتية حتى للقاضي، مستندين في رأيهم إلى أن هذا الدليل يتسم بالدقة العلمية التي يبلغ معها إلى درجة اليقين، و هناك من يرى أن مبدأ حرية القاضي في الاقتناع يجب أن يبسط سلطاته

على كل الأدلة دون استثناء حتى على الدليل الرقمي معتبرين أن الدليل الرقمي قوة ثبوتية لا يستطيع القاضي مناقشتها أو تقديرها يعد بمثابة رجوع إلى مذهب الإثبات القانوني (المقيد) .

والمشرع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الجرائم التي قد يتطلب إثباتها دليلا معينا، و منح القاضي الجزائي سلطة تقدير الدليل و الحرية في تكوين اقتناعه من أي دليل يطمئن إليه، فهل تنصرف هذه السلطة التقديرية التي يتمتع بها القاضي الجزائي إلى الدليل الرقمي المستخرج من الوسائل الالكترونية؟

لقد سبق الذكر أن الجريمة الالكترونية في القانون الجزائري تشمل الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات و كذا كل جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية، و هذه الأخيرة قد تنصرف إلى جرائم تقليدية منصوص عليها في قانون العقوبات يمكن حسب طبيعتها أن ترتكب بواسطة الكترونية، و هذا يعني أن الإجرام المعلوماتي قد يأخذ وصف الجناية أو الجنحة أو المخالفة[17].

حسب وصف الجرم المرتكب بواسطة المنظومة المعلوماتية، و إن كان مبدأ الاقتناع القضائي عام النطاق لدى كافة أنواع المحاكم الجزائية سواء كانت محاكم الجنايات أو الجنح أو المخالفات فإن قواعد بيان عناصر تقدير الدليل تختلف حسب اختلاف وصف الفعل للمجرم، فإذا كان الفعل من طبيعة جنائية فإن محكمة الجنايات تتمتع بسلطة تقديرية مطلقة في مواجهة الأدلة المعروضة أمامها و تصدر أحكامها دون أن يكون قضاتها مطالبين بتسبيب أحكامهم و الرقابة لجهات الطعن عليهم، أما إذا أخذ الفعل المجرم وصف الجنحة فإن قاضي الجنح مطالب بعرض و بيان تقديره للدليل المعروض عليه من خلال تسبيب

[17]- إن كان المشرع الجزائري لم يحدد ذلك صراحة في المواد المقررة لهذا المبدأ ارجع المواد307-212 من قانون الإجراءات الجزائية بخلاف المشرع الفرنسي فقد أقر ذلك صراحة حيث خصص المادة353-1 من ق.إ.ج لتطبيق المبدأ أمام محكمة الجنايات كما نصت المادة 427 من ذات القانون على تطبيق هذا المبدأ بالنسبة لمحاكم الجنح

حكمه، والذي يكون محل رقابة[18]، من جهة الطعن، لهذا فهو مطالب باحترام القواعد العامة المنظمة للقوة الثبوتية لكل وسيلة من وسائل الإثبات والتي قد تأخذ شكل محاضر معدة بمناسبة تفتيش أي اعتراض مراسلات أو شكل تقرير خبرة محررة بمناسبة معاينة وفحص الأدلة المضبوطة من جهاز الإعلام الآلي أو دعامات الكترونية.

فأما ما يتعلق بالمحاضر فإن الشرع اعتبر أنها قاعدة عامة مجرد استدلالات ما لم ينص القانون على خالف ذلك، ولا يكون للمحضر أي قوة إثبات إلا إذا كان صحيحا من حيث الشكل، و أنه قد تم إعداده من طرف واضعة أثناء مباشرة أعمال وظيفته، و يكون مضمونه ما يدخل في اختصاصه[19] ، إلا أن المحاضر التي يخول القانون لضباط الشرطة القضائية إعدادها بنص خاص لإثبات جنح معينة فإن هذه المحاضر تكون لها حجتها ما لم يدحضها دليل عكسي[20]

أما بالنسبة لتقارير الخبرة فإن المحكمة العليا ذهبت للقول أن الخبرة شأنها شأن باقي أدلة الإثبات تخضع للسلطة التقديرية لقاضي الموضوع[21]، وهذا المعنى تؤكده المادة 215من ق إ ج التي تنص على أنه:" لا تعتبر التقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات."....لكن الطبيعة العلمية و التقنية للجريمة الالكترونية غالبا ما تفرض على القاضي الاستناد في تكوين اقتناعه على الخبرة الفنية و التقيد بالنتيجة المتوصل إليها الخبير في تقرير خبرته ولا يمكنه طرحها واستبعادها إذا قدر أن ما تحمله من أدلة لا يتوافق مع ظروف و ملابسات الواقعة أو تتناقض مع الحقيقة العلمية، فحسب الاجتهاد القضائي أنه

[18]- انظر المادة 629 من ق إ ج ج و التي تقابلها المادتين 231-196 من ق إ ج فرنسي

[19]- انظر المادة 752 من ق إ ج.

[20]- انظر المادة 753 من ق إ ج.

[21]- ورد في مضمون قرار المحكمة العليا المؤرخ في 5991/02/55 المنشور في نشرة القضاء رقم 13 لسنة 7003 ،ص520

أحيانا ما تكون الخبرة وحدها كافية بالنسبة للقاضي عندما يكون مطالبا للفصل في وقائع ذات طابع تقني دون أن يحتاج إلى مناقشتها.[22]

ويمكن القول أن هناك قيود ترد على قبول الدليل الإلكتروني، ومن الواجب مراعاتها من قبل القاضي الجنائي، لأنها مسائل مهمة من شانها أن تغير في قيمة الدليل الإلكتروني من ناحية الاثبات الجنائي، لأنها مسائل مهمة من شانها أن تغير في قيمة الدليل الالكتروني من ناحية الإثبات الجنائي، في قوة حجيتها، حيث أن قيد مشروعية الدليل الإلكتروني عليه أن يكون خاضعا لمبدأ المشروعية الذي يعد من المبادئ الجوهرية في الإثبات الجنائي وهذا من خلال شرعية الإجراءات التي يتم الحصول على الدليل في سبيل إثبات القضية المطروحة أمام القاضي الجزائي، فمن واجب القاضي الجنائي سواء كان قاضي التحقيق أو غرفة الإتهام أو محكمة جزائية، أن تقيم الدليل على المتهم، ولا يجوز أن يحاكم المتهم ويدان بمجرد وجود قرائن بل لا بد أن تكون هذه الدلائل مكملة لبقية الأدلة المادية الأخرى كما يجب أن تتسم إجراءات جمع الأدلة بالمشروعية وذلك احتراما للحرية الشخصية للمتهم باعتباره بريئا إلى أن تثبت إدانته بحكم بات[23]. والقاعدة أن الإجراء الباطل يمتد بطلانه إلى الإجراءات اللاحقة له مباشرة وهو الرأي الراجح الذي أخذ به المشرع الجزائري بنص المادة191من قانون الإجراءات الجزائية "تنظر غرفة الاتهام في صحة الإجراءات المرفوعة اليها وإذا تكتشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الاقتضاء ببطلان الإجراءات التالية له كلها أو بعضها.

وعليه فالدليل الالكتروني في الوقت الراهن أصبح دليلا لا يمكن الاستغناء عنه خاصة مع التطور التكنولوجي ولهذا كان لازما على المشرع الجزائري هنا أن هذا التطور بداية

[22]– قرار المحكمة العليا الغرفة الجنائية المؤرخ في 2002/06/04 ،نشرة القضاء رقم 58 لسنة 2006 ،ص255 ..

[23]– بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى دار الخلدونية الجزائر ص139

بالنص على الدليل الالكتروني، الذي أصبح لا يقل أهمية عن باقي الأدلة الجنائية، واصبح دوره مهما في مختلف قواعد الإثبات الجنائي.

الفرع الثاني: ضوابط اقتناع القاضي الجزائي بالدليل الإلكتروني-الرقمي:

إن الاثبات في المواد الجزائية نهو نتيجة التي تتحقق باستعمال وسائله وطرقه المختلفة للوصول إلى الدليل الذي يستعين به القاضي لاستخلاص حقيقة الوقائع المعروضة عليه وإعمال حكم القانون عليه ان ويعني ذلك أن موضوع الإثبات هو الوقائع وليس القانون وبالتالي فإن الإثبات الجزائي هو كل ما يؤدي إلى كشف غموض الجريمة وإقامة الدليل على وقوعها والتأكد من أن المتهم هو مرتكب الجريمة بالفعل ووجود الدليل على ذلك، ويعتبر الدليل الوسيلة القانونية التي يستعين بها القاضي للوصول إلى الحقيقة وكشف غموض الجريمة ونسبتها إلى المتهم.

ان موقف المشرع الجزائري من أنظمة الإثبات الجنائي لقد حسم المشرع الجزائري موقفه من أنظمة الإثبات الجنائي بشكل واضح في نصي المادتين(212 و307)من قانون الإجراءات الجزائية، وذلك حينما نص في المادة212 على انه " يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الاحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي" ونص في المادة307 بأن " القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، ويبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة الى المتهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: هل لديكم اقتناع شخصي ". فبالنظر إلى نصي هاتين المادتين يتضح جليا أن المشرع الجزائري تبنى كأصل عام نظام الإثبات الحر أو الاقتناع الشخصي للقاضي الجزائي، والذي منح من خلاله للقاضي الجزائي حرية واسعة

في مجال تقدير الأدلة وفقا لقناعته الذاتية، وفتح أمامه باب الإثبات على مصراعيه كي يستلهم عقيدته من أي موطن يراه[24] دون أن يطالبه بتقديم مبرر لذلك. وفي الوقت نفسه وعلى سبيل الاستثناء نجده أخذ بنظام الإثبات المقيد أو ما يسمى كذلك بنظام الأدلة القانونية في إثبات بعض الجرائم أين اشترط لإثباتها أدلة قانونية محددة مسبقا على سبيل الحصر كما هو الشأن بخصوص جريمة الزنا المنصوص عليها في المادة339من قانون العقوبات. فتنص المادة341من قانون العقوبات على أن " الدليل الذي يقبل في ارتكاب الجريمة المعاقب عليها في المادة339يقوم إما على محضر قضائي يحرره احد رجال الضبط القضائي عن حالة التلبس، و إما بإقرار وارد في رسائل أو مستندات صادرة عن المتهم و إما بإقرار قضائي." كما منع الأخذ ببعض وسائل الإثبات كالمراسلة المتبادلة 374 بين المتهم ومحاميه وان تضمنت اعتراف المتهم بأنه ارتكب الجريمة، المادة217 من القانون الإجراءات الجزائية على انه " لا يستنبط الدليل الكتابي من المراسلة المتبادلة بين المتهم ومحاميه" وقد تأكد الأخذ بمبدأ الإثبات الحر كذلك بطريقة غير مباشرة في عدة نصوص قانون الإجراءات الجزائية، فيما يخص جهات الحكم، نذكر منها الفقرة الأولى من المادة235التي تنص على أنه "يجوز للجهة القضائية إما من تلقاء نفسها أو بناء على طلب النيابة العامة أو المدعي المدني أو المتهم أن تأمر بإجراء الانتقالات اللازمة لإظهار الحقيقة". وكذلك الفقرة الأولى من المادة 286" ... له (اي لرئيس الجلسة) سلطة كاملة في ضبط حسن سير الجلسة وفرض الاحترام الكامل واتخاذ أي إجراء يراه مناسبا لإظهار الحقيقة" ولعل ما يعزز توجه المشرع الجزائري هذا الاتجاه هو عدم سنه نصوصا تملي على القاضي الجزائي مقدما بقبول أو عدم قبول أي دليل من الأدلة المطروحة عليه في الدعوى أو ترسم له طرقا محددة للإثبات يتقيد بها، إنما فسح له المجال لكي يختار بحرية من كل طرقه ما يراه مفيدا وموصلا إلى الكشف عن الحقيقة ويستلهم عقيدته من أية وسيلة أو دليل

[24]– جاء في إحدى قرارات المحكمة العليا الصادر عن الغرفة الجزائية انه " يمكن لقاضي الموضوع تأسيس اقتناعه على أية حجة حصلت مناقشتها حضوريا أمامه" نقلا عن: أحسن بوسقيعة، مرجع سابق.

يطمئن إليه وجدانه ويرتاح إليه ضميره ، ولو تعلق الأمر بالأدلة الالكترونية، خاصة أنه 376 لم يتضمن قانون رقم (09-04)المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أية استثناءات أو أوضاع خاصة بهذا الصدد، مما يوحي بأن الدليل الالكتروني مقبول مبدئيا في الإثبات الجنائي بصفة عامة، والإثبات في مجال جرائم الاعتداء على النظم المعالجة الآلية بصفة خاصة، و يمثل مظهرا من مظاهر اعتناق المشرع لمبدأ حرية الإثبات والاقتناع.

ولم يكتف المشرع الجزائري بالنصوص المذكورة التي أطلقت حرية قاضي الموضوع في إثبات الجريمة بكافة طرق الإثبات وأعطته سلطة تقديرية واسعة في موازنة الدليل، بل خول كذلك لسلطات تنفيذ القانون الأخرى (الاتهام و التحقيق) الحق في البحث عن الأدلة بكل حرية بما فيها الالكترونية، وتجميعها عن طريق وضع الترتيبات التقنية اللازمة لذلك[25]، وكذا تمحيصها وصولا إلى الحقيقة التي سوف تبرر وفقها الاتهام وتؤسس عليها الأوامر التي يصدرها أثناء التحقيق، منها ما تضمنته المادة162الفقرة الثانية من قانون الإجراءات الجزائية " يمحص قاضي التحقيق الأدلة وما إذا كان توجد ضد المتهم دلائل مكونة لجريمة من جرائم قانون العقوبات".

إضافة إلى إمكانية الاستعانة بكل شخص مؤهل أولديه علم وخبرة في الواقعة المراد اتخاذ الإجراء بشأنها[26].

وفي مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وضع المشرع الجزائري على عاتق مقدمي خدمات الانترنت عددا من الالتزامات لمساعدة السلطات المختصة بالتحري والتحقيق[27].

---

[25]- نذكر منها المادة68من قانون الإجراءات الجزائية التي تنص على أن: " يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة، بالتحري عن أدلة الاتهام أو النفي ". والمادة69 من القانون نفسه تنص " يجوز لوكيل الجمهورية سواء في طلبه الافتتاحي لإجراء التحقيق او بطلب اضافي في نهاية مرحلة من مراحل التحقيق أن يطلب من القاضي المحقق كل إجراء يراه لازما لإظهار الحقيقة".

[26]- هذا ما أكدته المادة)143)من قانون الإجراءات الجزائية الجزائري في نصها " لجهات التحقيق أو الحكم عندما تعرض لها مسالة ذات طابع فني أو تأمر بندب خبير إما بناء على طلب النيابة العامة و إما من تلقاء نفسها أو من الخصوم"...

بما من شأنه تسجيل وحفظ المعطيات المتعلقة بمحتوى الاتصال أو المراسلة في حينها، كالمعطيات التي تسمح بالتعرف على مستعملي الخدمة، المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال، خصائصها التقنية، وكذا تاريخ و وقت ومدة الاتصال، والمعطيات التي تسمح بالتعرف على مرسل الاتصال والمرسل إليه، وكذا عناوين المواقع المطلع عليها[28].

وكل ذلك يعد إخبار ا صريحا على أن المشرع الجزائري قد سار على نهج نظام الإثبات الحر وهناك أسباب أخرى عديدة تبرر أخذ المشرع الجزائري بنظام الإثبات والاقتناع الحر، ولعل أهمها ظهور وتفشي الأدلة العلمية بمختلف أنواعها، كتلك المستمدة من الطب الشرعي والتحاليل العلمية الدقيقة (كالبصمات الشخصية والبصمة الوراثية) ومضاهاة الخطوط والأدلة الالكترونية الرقمية، والتي لا تقبل بطبيعتها إخضاع القاضي لأية قيود بشأنها، بل بالعكس فهي تفرض أن يترك أمر تقديرها وتمحيصها لمحض إرادة واقتناع القاضي الجزائي .

المطلب الثالث: حجية الدليل الالكتروني في ظل الأنظمة اللاتينية:

وفقا لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة في شأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلة للاستناد إليها في تكوين قناعته، فله أن يبني هذه القناعة على أي دليل و إن لم يكن منصوصا عليه، وكل الأدلة تتساوى قيمتها في الإثبات في نظر المشرع، والقاضي هو الذي يختار من بين ما يطرح عليه ما يراه صالحا للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية لقبو ل الدليل أو رفضه إذا لم يقتنع به، فالمشرع لا يتدخل في تحديد القيمة الإقناعية للدليل، فعلى الرغم من توفر شرط الصحة في الدليل إلا

---

[27]- أورد المشرع الجزائري في المادة 10من القانون رقم (09/04)أنه في إطار تطبيق أحكام هذا القانون يتعين على مزود الخدمة تقديم المساعدات للسلطات المكلفة بالتحريات القضائية ...بوضع المعطيات التي يتعين عليهم حفظها وفقا لأحكام المادة 11أدناه تحت تصرف هذه السلطات

[28]- أنظر المادة03فقرة11 من القانون رقم 04-09المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها، مرجع سابق.

أن القاضي يملك أن يرده تحت مبرر عدم الاقتناع، ولذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في هذا النظام.

وتأخذ الدول اللاتينية بنظام الإثبات الحر وهو لا يثير صعوبات بشأن حجية الدليل الرقمي، لأن القاضي الجنائي يملك الحرية في تقديره، ومن ثمة الأخذ به من عدمه حيث لا يخضع في ذلك لرقابة المحكمة العليا، وإنما لرقابة موضوعية بخصوص مبر ارت الأخذ به، وأخذت بذلك العديد من التشريعات مثل: فرنسا وتركيا واليونان والبرازيل وسويسرا [1]، في حين حين تشترط بعض الدول أن يكون الدليل الالكتروني مقروءا بعد استخراجه من الحاسوب أو من خلال شاشته .إن أدلة الحاسوب هي تطبيق من تطبيقات الدليل العلمي بما يتصف به من موضوعية وحياد ومشروعية لإقناع القاضي الجنائي الذي يجب عليه قبل الإقناع به أن يميز بين قيمته العلمية أولا عن طريق الاستعانة بالخبراء والمختصين، وثانيا الظروف والملابسات التي وجد فيها الدليل فيمكن أن يرفضه إذا رأى وجوده لا يتناسب منطقيا مع وقائع القضية[2].

يعد مبدأ الاقتناع أحد أهم المبادئ التي تقوم عليها نظرية الإثبات في المواد الجنائية وعنه تتفرع معظم القواعد التي تحكم هذا الاثبات[3]، ولقد تعددت الآراء في بيان مدلوله، ويقصد بمبدأ الاقتناع القضائي هو "أن للقاضي أن يستمد تكوين اعتقاده من أي دليل تطمئن اليه نفسه، ويسكن غليه وجدانه من دون أي قيد يقيده في ذلك، سواء من تلك الأدلة التي طرحت عليه من قبل النيابة العامة أو الخصوم أو التي يرى بنفسه تقديمها وهذه الحرية التي يتمتع بها القاضي الجنائي في هذا المجال ليست مقررة بهدف توسيع الإدانة أو البراءة، وإنما هي مقررة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجنائية" ويعد

[1]- 184هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، النسر الذهبي، القاهرة، مصر،2002 ،ص 43

[2]- سامي جلال فقي حسين، المرجع السابق، ص ص75 -76

[3]- رشيدة بوكر الدليل الالكتروني ومدى حجيته في الاثبات الجزائي في القانون الجزائري مقال منشور مجلة جامعة دمشق للعلوم الاقتصادية المجلد 27العدد الثاني2011. ص155.

التشريع الجزائري في طليعة التشريعات الذي اكد على هذا المبدأ وذلك من خلال المادة307 من قانون الإجراءات الجزائية فتنص "ان القانون لا يطلب من القضاة أن يقدموا حسابا على الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، ويبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة الى المتهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: هل لديكم اقتناع شخصي ". ومن خلال هذا التعريف فإن الإقتناع الشخصي للقاضي الجزائي يتميز بخاصتين هما:

1-مبنية على الاحتمال؛ أنه حالة ذهنية مبنية على الاحتمال وأن العبرة ليست بكثرة الأدلة، وإنما بما تتركه من أثر في نفسية القاضي، لأن هذا التأثير سيلعب دورا في تحديد مصير الدعوى الجزائية بالإدانة أو البراءة.

2 -حرية القاضي في الاقتناع؛ تتمثل في أن القاضي حر في أن يأخذ عقيدته أو اقتناعه من أي دليل لكن يجب التأكيد هنا أن حرية الإثبات في المسائل الجزائية ليست خاصية يتميز بها القاضي الجزائي لتتسع سلطته في الإدانة أو البراءة، ولكنها ترجع إلى أن الإثبات في المسائل الجنائية والوصول إلى الدليل مسألة جد صعبة، وذلك لاختلاف أساليب ارتكاب الجريمة وأن المجرم عادة ما يسعى إلى إخفاء جريمته لذلك فالبحث عن الحقيقة من خلال الأدلة الجزائية لا يكون إلا عن طريق منح القاضي الجزائي هامشا عن الحرية لمناقشة الدليل الذي يراه مناسبا في إثبات الجريمة.

وعليه فهذا الاقتناع ليس نشاطا مجردا من القيود والضوابط فبحكم أنه يمثل خلاصة نشاط القاضي أثناء عملية التقاضي والمحاكمة، حيث وضعت له ضوابط لا تعطي لهذا القاضي الجنائي مطلق الحرية التي يتمتع بها، وعلى تلك ضوابط التي تتعلق بالاقتناع في

حد ذاته ومحل الاقتناع؛1-فالمتعلقة بمحل الاقناع: أن يكون الدليل الإلكتروني مقبولا: وهذا الضابط مكمل لقيد مشروعية الدليل الالكتروني وهو ركيزة في مبدأ حرية القاضي الجنائي في تقدير الدليل الإلكتروني، فالتطبيق الحسن للقانون يفرض على القاضي أن يكون اقتناعه من دليل مقبول ويستبعد في المقابل جميع الأدلة الإلكترونية غير المقبولة، لأنه من غير المعقول ان تكون عنصرا من عناصر اقتناعه وتقديره[1]، فما بني على باطل فهو باطل.

أن يكون الدليل الالكتروني له صلة بملف الدعوى: فيستمد القاضي اقتناعه من الأدلة التي طرحت بالجلسة وخضعت للمناقشة من طرف الخصوم فلا يجوز للقاضي أن يبني حكمه على دليل لا صلة له في الأوراق الدعوى، فالدليل الذي لا يتحقق فيه هذا الشرط يكون منعدما في نظر القانون وذلك استنادا إلى قاعدة وجوب تدوين إجراءات الإستدلال والتحقيق كافة، وغاية ذلك أن يكون الخصوم على بينة مما يقدم ضدهم من أدلة، وأن تتاح لهم إمكانية مناقشتها والرد عليها ولو لم يناقشوها بالفعل، إذ ليس من الضروري أن تحصل مناقشة علنية، كل ما يلزم أن تكون الأدلة في متناول الخصوم فحسب.[2]

2-فالمتعلقة بالإقناع في حد ذاته: عندما يتهيأ القاضي للأخذ بدليل من الملف قد استوفى مشروعية وطرح بجلسة المحاكمة ونوقش فيها فإن على القاضي أن يراعي عند اقتناعه الجزم واليقين وأن يصل الى مرحلة يصبح مقتنعا بالحقيقة لا الاحتمال وأن لا يشك مطلقا وغن احتمال ولو واحد فقط يفيد البراءة فان عليه أن يفسر الشك لصالح المتهم ويحكم ببرائته، فعليه أن يبني اقتناعه من الأدلة مجتمعة لان الأدلة في المواد الجنائية متساندة متماسكة وتكمل بعضها البعض في تكوين اقتناع القاضي، وهو ما يقتضي منه أن يعتمد على أساسين أولهما هو بيان مضمون الأدلة بصفة واضحة لا لبس فيها، بعيدا عن الإبهام والغموض وينعت بالاقتناع اليقيني بالدليل للوصول الى الحقيقة المطلقة وثانيهما هو انعدام

[1]- هلال آمنة المرجع السابق ص 106.

[2]- 23رشيدة بوكر الدليل الالكتروني ومدى حجيته في الاثبات الجزائي في القانون الجزائري مقال منشور مجلة جامعة دمشق للعلوم الاقتصادية المجلد 27العدد الثاني2011.ص323.

التناقض والتخاذل بين هذه الأدلة فيما بينها أو بينها وبين منطوق الحكم ملائمة الاقتناع لمقتضيات العقل والمنطق من عمليات منطقية واستقراء واستنباط ينتهي جميعها لنتيجة يقينية.

المطلب الرابع: حجية الدليل الالكتروني في ظل الأنظمة اللانجلوسكسونية:

تعتمد ما يسمى غلبا نظام الإثبات المقيد أو نظام الأدلة القانونية Système de la preuve légale وفي هذا النظام يقوم المشرع بتحديد أدلة الإثبات حصرا، وكذا القوة الثبوتية لكل دليل من أدلة الإثبات بناء على قناعته، وهو ما يعرف بنظام الأدلة القانونية، إذ لا يكون لقناعة القاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها، إذ تحدد للقاضي الأدلة التي يجوز له قبولها و اللجوء اليها في الإثبات ولا سبيل لإنشاء أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات.[1]

وتعتمد حجية الدليل الإلكتروني في ظل هذا النظام على تحديد أدلة الإثبات من قبل المشرع وليس تقديرها من القاضي، فيقوم المشرع بتحديد سلفا وبشكل حصري الأدلة التي يجوز للقاضي قبولها والاستعانة بها في الإثبات، وكذا تحديد القوة الاستدلالية لكل دليل بناء على قناعته بها، في حين لا يكون للقاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها، وإنما يقتصر دوره على فحص الدليل للتأكد من مدى مشروعيته وتوفره على الشروط التي حددها القانون. وفي حالة انتفاء الشروط التي يتطلبها القانون في الدليل فان القاضي لا يسع له الحكم بالإدانة حتى ولو تكونت لديه قناعة يقينية بارتكاب المتهم للجريمة المنسوبة إليه.[2]

ومن هنا يتضح جليا بأن نظام الإثبات المقيد يقوم على مبدأين أساسيين،

[1]- شيماء عبد الغني، د محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007 ص، .435 ،ص436

[2]- سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب...، مرجع سابق، ص81.

الأول يتمثل في الدور الايجابي للمشرع في عملية الإثبات لكونه الذي ينظم قبول الأدلة سواء عن طريق التعيين المسبق للأدلة المقبولة للحكم بالإدانة، أو باستبعاد أدلة أخرى، أو بإخضاع كل دليل لشروط معينة، ولكونه الذي يحدد القيمة الاقناعية لكل دليل بأن يضفي الحجية الدامغة على بعض الأدلة، والحجية النسبية على بعضها الآخر[1]. وأن يعطي لبعض الأدلة الحجية الأقوى دون الأدلة الأخرى.

أما المبدأ الثاني، فيتمثل في الدور السلبي للقاضي الجزائي في الإثبات الجنائي فيخضع لقواعد شكليه تتضح في سلطة القاضي المقيدة في تقدير عناصر الإثبات التي يستمد منها إقناعه و تقدير قيمة الأدلة المعروضة عليه ، إذ يلتزم التزاما صارما بما يرسمه له المشرع سلفا من أدلة إثبات على نحو يفقده سلطته في الحكم بما يتفق مع الواقع، فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته لنصوص القانون.

ويقوم هذا النظام على مجموعة من الخصائص أهمها أن دور القاضي الجزائي سلبي، ذلك أن الإثبات، كما في الدول التي تأخذ بهذا النظام مثل: بريطانيا وأمريكا تفرض قيودا على هذه الأدلة حتى يمكن الأخذ بها مثل: اعتماد مبدأ تعاضد الأدلة في التشريع البريطاني.[2]

كما يحدد القانون الألماني على سبيل الحصر وسائل الإثبات التي يتعين على القاضي قبولها كسماع أو سؤال المتهم وشهادة الشهود وتقارير الخبراء[3]. في الشأن نفسه و

[1]- هلالي عبد ألاله أحمد، حجية المخرجات الكومبيوترية في المواد الجنائية، مرجع سابق، ص 91.

[2]- 186يقصد بهذا المبدأ: تعزيز دليل بدليل آخر، فمثلا الشهادة لا تكفي وحدها في بعض الحالات، حيث يجب توافر دليل آخر معزز لها كشهادة أخرى مستقلة عنها، أو دليل آخر كخبرة أو مستند، فإذا لم يتوافر هذا الدليل المساند حكم القاضي بالبراءة، راجع سامي جلال فقي حسين، المرجع السابق، ص83.

[3]- عائشة بن قار ة مصطفى، المرجع السابق، ص 181- ص 182.

يستبعد المشرع الأمريكي الأدلة التي يمكن الحصول عليها بالمخالفة للحقوق الدستورية كالحجز والمصادرة والتفتيش غير المشروع[1].

إن دور القاضي في هذا النظام دور سلبي فإذا لم تكن هذه الشروط متوفرة، لا يستطيع الحكم بالإدانة بصرف النظر عن اعتقاده الشخصي حتى ولو كان يميل إلى إدانة المتهم. كما تبرز في ظل هذا النظام صعوبات في مجال إثبات الجرائم الإلكترونية، مما يستوجب إدخال تعديلات تتلائم وطبيعة هذه الجرائم، نظرا للطفرة التكنولوجية الحاصلة في مجال المعلوماتية كشبكة الانترنت، حيث لوحظ بعض التغييرات على حدة هذا النظام. بحيث صار يقبل بمبدأ حرية القاضي في تقدير الأدلة، فقاعدة حرية القاضي الجنائي في الاقتناع معترف بها تقريبيا لدى جميع التشريعات القانونية مع اختلاف الصياغة في القوانين ففي النظام اللاتيني تسمى بمبدأ الاقتناع القضائي، أما في النظام الأنجلوسكسوني فتسمى بالأدلة بدون أي شك معقول، أو الإدانة الخالية في أي شك.[2]

واعتبار لذلك، فقد انتقد الفقه الجنائي هذا النظام بشدة خاصة فيما تعلق منه بتجريد القاضي من وظيفته الطبيعية المتمثلة في فحصه للدليل المعروض أمامه بكل حرية وتقدير قيمته الاقناعية وفقا لضميره المهني، ومن ثم تكوين اقتناعه الشخصي، ومنحها للمشرع ليحل بذلك محل القاضي، بل أكثر من ذلك جعل اقتناع القاضي متوقفا على اقتناع المشرع بما يمليه عليه هذا الأخير من أدلة إدانة على سبيل الحصر .ومن المسائل التي انتقدت في هذا النظام، قيامه بتقنين اليقين بنصوص قانونية سلفا رغم أن اليقين مسالة يطرحها الواقع ترتبط بالظروف الخاصة والمتغيرة لكل قضية وتترك لتقدير قاضي الموضوع.[3]

---

[1]- 188سامي جلال فقي حسين، المرجع السابق، ص81ص83.

[2]- سلامي جلال فقي حسين المرجع السابق ص84.

[3]- ومن النتائج الوخيمة التي تترتب عن تقيد القاضي باليقين القانوني ، والالتزام بحرفية النصوص ما حدث في القضية التي حكم فيها القاضي (Camboوالتي تتلخص وقائعها: بأنه في صبيحة أحد الأيام بينما كان القاضي كامبوا وهو قاضيا في إحدى محاكم مالطا يرتدي ملابسه لاحظ من نافذة غرفته شخصين يتشاجران، وأثناء ذلك قام أحدهما بطعن الأخر بخنجر فأرداه قتيلا ولاذ بالفرار، وسقط منه جراب الخنجر، الذي طعنه في جسم الضحية، وفي الوقت نفسه مر خباز في الجوار، وعثر على جراب الخنجر فأخذه ووضعه في جيبه، ولما شاهد الجثة خاف وهرب، وأثناء ذلك رآه رجال

ونتيجة لهذه الانتقادات وغيرها، تراجع العمل بنظام الإثبات المقيد بشكل سريع في الآونة الأخيرة وتقلص نطاقه حتى في الدول التي تعتبر الأكثر اعتناقاً له، فنجد بريطانيا مثلاً وهي الدولة المؤسسة لهذا النظام قد بدأت تخفف من اعتماده، وظهر فيها ما يعرف بقاعدة "الإدانة دون أدنى شك"، والتي مفادها أن القاضي يستطيع أن يكُّون عقيدته من أي دليل، وإن لم يكن من ضمن الأدلة المنصوص عليها متى كان هذا الدليل قطعياً في دلالته[1]، وهو الاتجاه الذي سايره المشرع الأمريكي من خلال تبنيه في قانون الأدلة الاتحادي لقاعدة "الدليل الأفضل" .[2]

كما ظهر نظام ثالث وهو نظام الإثبات المختلط .يعتبر نظام الإثبات المختلط نظام وسط، أو نظام توفيقي بين نظام الإثبات الحر ونظام الإثبات المقيد، حيث تتراوح أحكامه بين التقييد والإطلاق، كما جاء هذا النظام لتفادي الانتقادات الموجهة للنظامين السابقين فيجنب تعسف القاضي في نظام الإثبات الحر وخروجه عن جادة الصواب، كما يخفف من الدور السلبي المحض للقاضي في النظام المقيد بأن يمنح له الحرية في تقدير ما يعرض عليه من أدلة[3]، كما قد يكون التوفيق بين النظامين عندما يحدد القانون أدلة معينة للإثبات في بعض الوقائع دون الأخرى، أو يطلب شروطا في بعض الحالات، أو يعطي القاضي

الشرطة والقوا القبض عليه، وعند تفتيشه وجدوا بحوزته جراب الخنجر الذي تبين فيما بعد بأنه مطابق للخنجر المطعون في جسم المجني عليه. ورغم مشاهدة القاضي كل تفاصيل القضية بأم عينيه إلا انه عند امتثال الخباز أمامه للمحاكمة لم يدافع عنه، وطبق عليه القانون بكل تفاصيله، بل حمله على الاعتراف بالتعذيب، ولما اعترف الخباز مكرها حكم عليه بالإعدام. نقلا عن: هلالي عبد ألاله أحمد، النظرية العامة للإثبات الجنائي، المجلد الأول، دار النهضة العربية للنشر، القاهرة، بدون سنة، ص.ص 95-96 ،هامش رقم 1.

[1]- STEPHEN . J et autre, la preuve en procédure pénale comparée, rapport de synthèse pour les pays de Common Law, association internationale de droit pénal, 1992, p 33.

[2]- قاعدة الدليل الأفضل، هي القاعدة التي تعطي للقاضي سلطة تقديرية في قبول نسخ أو صور الدليل الأصلي في حالة عدم توافر هذا الأخير (أي الدليل الأصلي) أو فقدانه. أنظر: سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، مرجع سابق، ص303.

[3]- أمام الجمعية التأسيسية الفرنسية سنة 1971 ،حيث كان هذا اقترح النظام المختلط من طرف الأستاذ: robsir روبسيير الاقتراح مكونا مف جزئين: يتمثل الأول في عدم الحكم على المتهم إذا لم تتوفر ضده أدلة حددها القانون، والثاني في عدم الحكم بإدانة المتهم حتى إذا توافرت أدلة قانونية، لكن هذه الأدلة لم تحقق قناعة القاضي. سامي جلال فقي حسين المرجع السابق، ص93

الحرية في تقدير الأدلة كالقانون الياباني الذي يحصر طرق الإثبات المقبولة في أقوال المتهم وشهادة الشهود والخبرة المنجزة من طرف الخبراء.[1]

وفي ختام الفصل الأخير يمكن القول أن إساءة استخدام التقنية المعلوماتية تعد من الموضوعات التي فرضت نفسها على المستوى الوطني والدولي على حد سواء وأجبرت التشريع الجزائي على التدخل من أجل مواجهتها بتشريعات حاسمة لمكافحتها ومعاقبة مرتكبها إلا أن ذلك يبدو غير كاف لتحقيق هذه الهدف، فعلى المستوى الإجرائي تثير الجريمة الالكترونية مشكلات عدة بدءا من مرحلة الاستدلال حتى صدور الحكم الجزائي لاسيما فيما يتعلق بإثبات الجريمة الالكترونية ومدى صالحية الدليل لرقمي للإثبات ومدى شرعية الأدلة المحصل عليها عبر التقنية المعلوماتية وحجيتها أمام القاضي الجزائي، لذلك خصص هذا الفصل لتناول هذه المسائل من خلال تحديد الأجهزة المكلفة بالبحث والتحري عن الجريمة الالكترونية، ثم التعريف الخصائص التي يتميز بها التحقيق والمحققون فيها. ثم بعد ذلك تم البحث في الدليل المناسب لإثبات هذا النوع من الجرائم وهو ما يعرف بالدليل الالكتروني أين تم توضيح مفهومه وتحديد أشكاله ومصادر الحصول عليه، كما تم معالجة القواعد الإجرائية والشروط لصحة الاستدلال به والمستعملة في التحقيق، كما تم تناول إجراءات الحصول على الدليل الرقمي–الالكتروني واستخلاصه التقليدية منها والحديثة ، وأخيرا تم بحث القيمة القانونية للدليل الرقمي في مجال الإثبات الجزائي من مناقشته أمام قضاة الحكم ومدى تقدير قاضة الحكم للدليل الالكتروني لنعرج آخرا لحجية الدليل الالكتروني في الأنظمة اللاتينية وحجيته في الأنظمة الأنجلوسكسونية مع تبيان موقف المشرع الجزائري من هذا الدليل.

[1]– هلالي عبد الإله أحمد، المرجع السابق، ص59.

خاتمة

في الأخير يمكن القول أن إساءة استخدام التقنية المعلوماتية تعد من الموضوعات التي فرضت نفسها على المستوى الوطني والدولي على حد سواء وأجبرت التشريع الجزائي على التدخل من أجل مواجهتها بتشريعات حاسمة لمكافحتها ومعاقبة مرتكبها إلا أن ذلك يبدو غير كاف لتحقيق هذه الهدف، فعلى المستوى الإجرائي تثير الجريمة الالكترونية مشكلات عدة بدءا من مرحلة الاستدلال حتى صدور الحكم الجزائي لاسيما فيما يتعلق بإثبات الجريمة الالكترونية ومدى صالحية الدليل لرقمي للإثبات ومدى شرعية الأدلة المحصل عليها عبر التقنية المعلوماتية وحجيتها أمام القاضي الجزائي، لذلك تتضمن هذه الدراسة في متنها كشفا لرؤية إجرائية تتناول مسألة البحث والتحقيق الجنائي في الجرائم الإلكترونية، والمشكلات الإجرائية المترتبة عليها، وكذا الحلول الممكنة المقترحة لمعالجة تلك المشكلات.

وقد اتضح لنا أن الجرائم الإلكترونية تعد من الأنماط الإجرامية الجديدة التي فجرتها حديثا ثورة تقنية المعلومات والاتصالات عن بعد، والتي تتميز بخصائص مختلفة تماما عن الجرائم التقليدية، من ثمة فأي محاولة للتعامل إجرائيا مع هذا النمط الإجرامي الجديد في إطار عملية البحث والتحقيق سوف يخلق إشكالات إجرائية أمام السلطات المكلفة بهذه العملية وتتجلى أولى هذه الإشكالات في القصور الذي يعتري النصوص الإجرائية القائمة في مواجهة مثل هذه الجرائم، لأن أحكام هذه النصوص إنما وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات في إثباتها أو التحقيق فيها مع خضوعها لمبدأ حرية القاضي الجزائي في الاقتناع.

وقد بينا أن المشرع بادر في الكثير من الدول إلى إعادة النظر في بعض القواعد الإجرائية المتعلقة باستخلاص الدليل كالتفتيش والضبط وجعلها صائغة الاستعمال في مجال البيئة الرقمية الالكترونية.

فضلا عن استحداث قواعد إجرائية أخرى تتلاءم مع الطبيعة الخاصة التي يتميز بها هذا النوع من الجرائم، كالمراقبة الإلكترونية واعتراض المراسلات والتسرب الالكتروني، وهو

ما أقدم عليه المشرع الجزائري من خلال تعديل قانون الإجراءات الجزائية في عام 2006، واصداره القانون رقم (09/04) المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

مما جعل المشرع يحرص على حصر اللجوء إلى هذه الإجراءات في الحالات التي تستدعي ضرورة التحقيق والتحري الى ذلك، كما أحاطها بجملة من الضمانات القانونية التي يتعين على المحقق احترامها عند استعماله لهذه الإجراءات.

كما خصص في هذه الدراسة تناول هذه المسائل من خلال تحديد الأجهزة المكلفة بالبحث والتحري عن الجريمة الالكترونية، ثم تعريف الخصائص التي يتميز بها التحقيق والمحققون فيها ثم بعد ذلك تم البحث في الدليل المناسب لإثبات هذا النوع من الجرائم وهو ما يعرف بالدليل الالكتروني أين تم توضيح مفهومه وتحديد أشكاله ومصادر الحصول عليه، كما تم معالجة القواعد الإجرائية والشروط لصحة الاستدلال به والمستعملة في التحقيق، كما تم تناول إجراءات الحصول على الدليل الرقمي–الالكتروني واستخلاصه التقليدية منها والحديثة،

وأخيرا تم بحث القيمة القانونية للدليل الرقمي في مجال الإثبات الجزائي من مناقشته أمام قضاة الحكم ومدى تقدير قضاة الحكم للدليل الالكتروني لنعرج آخرا لحجية الدليل الالكتروني في الأنظمة اللاتينية وحجيته في الأنظمة الأنجلوسكسونية مع تبيان موقف المشرع الجزائري من هذا الدليل.

من خضم هذه الدراسة توصلنا للنتائج التالية:

– ان التقنية المعلوماتية أصبحت من أساسيات حياة الدول والشعوب ولا يمكن تصور فكرة التخلي عنها، نظرا لتزايد مجالات إستعمالاتها في كافة المجالات، وذلك بالرغم من كافة التهديدات التي تشكلها الجريمة المعلوماتية على أمن وسلامة نظمها ومستعمليها.

– يستحيل القضاء على الظاهرة الإجرامية المعلوماتية بشكل نهائي، وذلك لإتصالها المباشر بتقنية المعلوماتية، ففكرة التخلي عن هذه التقنية هي الحل الوحيد لمشروع القضاء

على الجريمة المعلوماتية وذلك بالرغم من درجة التطور التي آلت إليها المنظومة القانونية العقابية منها والإجرائية في مجال مكافحة الجريمة المعلوماتية.

– تخضع إجراءات البحث والتحقيق المعلوماتي لإختصاص جهات متخصصة في التعامل مع الجرائم المعلوماتية، تعتمد في تكوينها على مجموعة من المختصين في مجال المعلوماتية وكذلك في مجال التحقيق الجنائي، مما يجعل منهم أفضل الأشخاص الذين يستطيعون التكفل بمهام البحث والتحقيق في الجرائم المعلوماتية، نظرا لتقديرهم العلمي والمعرفي بالأساليب الإجرامية المعلوماتية، وكذلك القواعد القانونية للتعامل بالشكل الشرعي مع الجريمة المعلوماتية، إضافة إلى مراعاتهم لجملة من القواعد العملية الإحتياطية منها والأصلية عند مباشرة الإجراءات التي تهدف إلى جمع الأدلة، بشكل يكون الهدف منه ضمان حسن سير الإجراءات والحفاظ على سلامتها من طائلة البطلان، و كذا سلامة الأدلة من مخاطر التلف والفقدان.

– ان قانون الإجراءات الجزائية الجزائري ينص فقط على القواعد العامة التي تطبق على الجرائم التقليدية وكذا على الالكترونية من خلال بعض الإجراءات الخاصة الممثلة في حجز المعطيات أو البيانات وكذا مراقبة الاتصالات الإلكترونية وحفظ البيانات.

– أن بعض الإجراءات تعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الإلكترونية، كالمعانية على المسرح الجريمة وكذا التفتيش الإلكتروني وضبط الدليل الرقمي والمستحدث هو إجراءات جديدة جاء بها تعديل قانون الإجراءات الجزائية الجزائري سنة 2006 واخر تعديل 2015و2021 التي تعرف بأساليب التحري الحديثة حيث جاء بإجراءات لا تطبق إلا على الجرائم الإلكترونية كإجراءات المحاكمة المختص بنظرها الأقطاب الجزائية المتخصصة وبالإضافة إلى إجراءات خاصة جاء بها قانون09-04.

– بالرغم من وجود نصوص قانونية فإن مكافحة الجريمة الإلكترونية رهينة بالمعيقات الإجرائية في مجال المتابعات فإن أول إشكال أو عائق هو غياب القدرات التأهيلية والوسائل التقنية والفنية التي تتيح سرعة إدراك ما حصل، وأن غياب التأهيل قد يؤدي إلى إتلاف

الدليل وافلات مرتكبي هذه الجرائم من العقاب بالإضافة إلى مشكلات في القانون الواجب التطبيق كون الجريمة الإلكترونية عابرة للحدود.

– إن هذه الجريمة ومع تعدد أنماطها واحتراف مرتكبيها، سواء كانت جرائم واقعة على النظام المعلوماتي أو بإستخدامه، فإن لها جوانب سلبية خطيرة تهدد أمن وسلامة الفرد والمجتمع وهو ما يضع مسؤولية كبيرة على ضباط الشرطة والقضاء لاتسامها بالغموض حيث يصعب إتباعها والتحقيق فيها.

كما توصلناالى نتائج هامة أيضا ترتبط بالحجية كنتيجة من نتائج التحري والتحقيق:

– يتمتع الدليل الإلكتروني بمجموعة من الخصائص التي جعلته يتميز عن باقي الأدلة الجزائية، خاصة الخاصية الفنية والتقنية فيه، وأيضا مع إمكانية إسترجاعه بعد إتلافه وإعتبار عملية محاولة إتلافه دليل ضد مرتكبها.

– . قصور من طرف المشرع الجزائري الذي لم ينص على الدليل الإلكتروني في قوانينه، ولم يضع له تعريفا جامعا شاملا.

– .إن محل الدليل الإلكتروني ونطاق العمل به هو الجريمة الإلكترونية غير أنه يصلح كذلك لإثبات الجرائم التقليدية، التي تم إرتكابها عبر تقنية الكترونية.

– . صعوبة جمع الدليل الإلكتروني نظرا لوجوده في وسط إفتراضي.

–. أضاف المشرع الجزائري قسم خاص بعنوان " المساس بأنظمة المعالجة الآلية للمعطيات " في إطار تعديل قانون العقوبات بموجب 15/04 وهذا لمواجهة الجرائم الإلكترونية وأيضا قام بتعديل قانون الإجراءات الجزائية بموجب الأمر 22/06 بغرض ماحقة هذه الجرائم.

– .قصور القواعد الإجرائية المتبعة للحصول على الدليل الإلكتروني، وذلك بإقتصارها على القواعد العامة والإجراءات التقليدية.

– .نقص الثقافة الالكترونية فيما يتعلق بالدليل الإلكتروني، عند رجال الضبط القضائي المكلفين بجمع هذا النوع من الأدلة، وكذلك القضاة الجنائيين، مما يؤدي الآمر إلى إتلافه ونقص قوته الثبوتية.

– . يتمتع الدليل الإلكتروني بيقينية كبيرة، بسبب الحرص على العمل بمبدأ مشروعية الدليل الإلكتروني.

– . إعتبار مبدأ حرية الإثبات الجزائي كأساس في قبول الدليل الإلكتروني.

– . قبول الدليل الإلكتروني أمام القضاء الجزائي، بإعطاء الحرية للقاضي الجزائي في الإقتناع بالدليل الإلكتروني.

وعلى ضوء هذه النتائج المترتبة عن موضوع الدراسة، ارتأي لي أن أبدي بهذه المقترحات أو التوصيات:

– نرجو من المشرع الجزائري التوقف عن استيراد القوانين من البلدان الأجنبية والإهتمام أكثر بالأدمغة الجزائرية والإعتماد على خبرتها في وضع التشريعات الوطنية.

– الاستفادة من التجارب الدولية في هذا المجال لكسب المهارات اللازمة لمكافحتها.

– تعديل قانون الإجراءات الجزائية على وجه الإستعجال من خلال إدراج قسم خاص بأعمال البحث والتحقيق في الجرائم المعلوماتية، وذلك من خلال إفراد نصوص قانونية خاصة بالإجراءات الجزائية المتبعة خلال مرحلة البحث والتحري وكذلك التحقيق بشكل مفصل وواضح، يبين قواعد الإختصاص النوعي والمحلي بدقة ووضوح، إضافة إلى طبيعة الإجراءات المتخذة في هذا الشأن، وذلك للقضاء على كل لبس قد ينشأ جراء المزج بين النصوص العامة والخاصة، وذلك تجسيدا للطبيعة الخاصة للجريمة الالكترونية بفهومها الخاص، ضمن فصول واحكام القانون الإجرائي.

– ضرورة تدريب وتأهيل أفراد الضبطية القضائية على كيفية التعامل مع هذا النوع من الجرائم بعقد دورات تكوينية بشكل دائم.

– لابد أن يكون التفتيش على المكونات المادية للحاسوب الآلي.

– المعاينة في الجريمة الإلكترونية يكون على مستويين وهما المسرح التقليدي والمسرح الافتراضي.

– ضبط الدليل الرقمي إلكترونيا وسماع الشهود المتخصصين والعاملين بالجانب المعلوماتي.

– التسرب الرقمي ومراقبة الاتصالات الإلكترونية وحفظ البيانات.

– وضع سجل أمني إلكتروني يتضمن قائمة بمجرمي المعلوماتية يسمح بوضعهم تحت المراقبة الأمنية، أي رصد نشاطاتهم المعلوماتية المشبوهة عبر الشبكة، والتي تنذر بوقوع جريمة معلوماتية.

في الختام، فإنني لا أزعم من خلال هذا البحث بلوغي جادة الصواب، ولكن أملي أن يحقق قدر من العزم منه، وما أنا إلا بشر اجتهد فأخطئ وأصيب، فان أصبت فأجري على الله وإن أخطأت فأدعوه ألا يحرمني أجر المجتهدين، ولله الأمر من قبل ومن بعد، والحمد الله رب العالمين.

قائمة المصادر والمراجع

المؤلفات:

المراجع باللغة العربية:

- ضياء علي أحمد النعمان، الغش المعلوماتي الظاهرة والتطبيقات، الطبعة الأولى، المطبعة الوطنية، المملكة المغربية، 2011.

- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية، دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية.

- محمد محمد محمد عنب، إستخدام التكنولوجيا الحديثة في الإثبات الجنائي، مصر،2007 .

- عبد الفتاح عبد اللطيف الجبارة، إجراءات المعاينة الفنية لمسرح الجريمة، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن،2010 .

- مصطفي محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، 2009.

-ممدوح عبد الحميد عبد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت، دار الفكر القانونية، القاهرة، 2006 .

- حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف للعلوم الأمنية، الرياض، المملكة العربية 3 السعودية سنة 2000 .

- محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنت.

- علي حسن أحمد الطوالبة- التفتيش الجنائي على نظم الحاسوب و الانترنت- دراسة مقارنة.

- علي حسن أحمد الطوالبة-" مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي".

البحوث الجامعية:

- أمدور رجاء خصوصية التحقيق في مواجهة الجرائم الالكترونية أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث ل.م.د تخصص: القانون الخاص جامعة محمد البشير االبراهيمي برج بوعريريج كلية الحقوق والعلوم السياسية قسم الحقوق السنة الجامعية 2021/2020.

- معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم الالكترونية في التشريع الجزائري و التشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2011-2012 .

- - نوال شعلال، سلطة القاضي الجنائي في تقدير الأدلة، مذكرة مقدمة لنيل شهادة الماجستير، فرع قانون العقوبات والعلوم الجنائية، جامعة سكيكدة، 2008-.

-

- - زهية معمش نسمة غانم الثبات الجنائي في الجرائم الالكترونية مذكرة الماستر تخصص قانون الخاص والعلوم الجنائية جامعة عبد الرحمان ميرة بجاية2012-2013.

المقالات:

- محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي و شبكات الانترنت، بحث مقدم في الحلقة العلمية بعنوان "الانترنت و الإرهاب"، المنظمة من طرف جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين الشمس، بدبي، في الفترة الممتدة من 15 إلى 11/19 /2008.

- الدليل الرقمي في مجال الإثبات الجنائي" بحث مقدم إلى المؤتمر ألمغاربي الأول حول 251 المعلوماتية والقانون، المنظم من طرف أكاديمية الدراسات العليا بطرابلس، في الفترة الممتدة من 28-29/10/2009.

- عمرو حسين عباس، أدلة الإثبات الجنائي والجرائم الالكترونية، بحث مقدم الى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، المنعقد بمقر الجامعة الدول العربية، القاهرة، خلال الفترة الممتدة من 26-27أفريل 2008 ،ص06. ص07- ،و علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي".

- رشيدة بوكر الدليل الالكتروني ومدى حجيته في الاثبات الجزائي في القانون الجزائري مقال منشور مجلة جامعة دمشق للعلوم الاقتصادية المجلد 27العدد الثاني2011.

- ضريفي نادية، سلطات القاضي الجاني في تقدير الدليل الإلكتروني، المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04 ،العدد ، 02 .

- رضا هميسي، أحكام الشاهد في الجريمة الالكترونية، ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة الالكترونية بين الوقاية و المكافحة، يومي 16 ،17نوفمبر 2015 ،كلية الحقوق، جامعة بسكرة، الجزائر، 2015 .

المواقع الإلكترونية:

- خالد ممدوح إبراهيم ، الدليل الالكتروني في جر ائم المعلوماتية، بحث منشور في الموقع الالكتروني التالي:

http://Kenanaonline.com/users/KhaledMamdouh/posts/79345

-colloque sur « la preuve numérique a l'épreuve du litige. Les acteurs de litige a la preuve numérique » organiser par la compagnie nationale des experts de justice en informatique et associées le 13-04- 2010. Disponible sur le site: www.cnejita.org/.../CNEJTA-

وهو تقريبا نفس التعريف الذي ACTES-COLLOQUE10042010-A5-V5.1-pdf
) في تقريرها الصادر في أكتوبر.(IOCE استأثرته المنظمة العالمية لدليل الكمبيوتر

-CLEMENT-FONTAINE.Mélanie, op.cit. Article disponible sur ; www.cnejita.org/…/CNEJTA-ACTES-COLLOQUE10042010-A5-V5.1-pdf

– عبد الحميد عبد المطلب، استخدام بروتوكول(TCP/IP) في بحث و تحقيق الجرائم على الكمبيوتر، بحث مقدم الى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، المنعقد بدبي، في الفترة الممتدة من 26 -28/08/ 2003 منشور على الموقع الالكتروني التالي: WWW.arablaw.info.com08

المراجع باللغة الأجنبية:

-STEPHEN . J et autre, la preuve en procédure pénale comparée, rapport de synthèse pour les pays de Common Law, association internationale de droit pénal, 1992.

- Charle Diaz, La Police Techenique et Scientifique, 2eme Edition, Edition Presse universitaire de France, France , 2006
-Jean Claude martin – investigation de scènes de crimes -fixation de l'état des lieux et traitement des traces d'objet- presse polytechnique et universitaire Romandes- France- 2004.

النصوص التشريعية:

القوانين:

- قانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.
- المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

- الأمر 15-02 قانون الإجراءات الجزائية الجزائري.و -المادة 68 ق - 01-08 -قانون الإجراءات الجزائية الجزائري.

القرارات والأحكام القضائية:

- قرار المحكمة العليا الغرفة الجزائية بتاريخ 2005/06/29طعن رقم301387، مجلة المحكمة العليا العدد الأول لسنة 2006.

- قرار المحكمة العليا المؤرخ في 5991/02/55 المنشور في نشرة القضاء رقم 13 لسنة 2003 .

- قرار المحكمة العليا الغرفة الجنائية المؤرخ في 2002/06/04 ،نشرة القضاء رقم 58 لسنة 2006.

فهرس
المحتويات

فهرس المحتويات.....

شكر وعرفان

إهداءات

مقدمة: 1

الفصل الأول: إجراءات التحري في الجريمة الالكترونية. 5

المبحث الأول: الاختصاص في الجرائم الالكترونية. 6

المطلب الأول: تحديد مفهوم شروط الاختصاص في مسائل الجريمة الالكترونية. 7

المطلب الثاني: اختصاص ضباط الشرطة القضائية بالبحث والتحري في مجال الجرائم المعلوماتية. 8

المطلب الثالث: الإختصاص النوعي للجهات القضائية (النيابة العامة – قضاء التحقيق) 11

المطلب الرابع: الإختصاص الإقليمي في الجرائم الالكترونية: 13

المبحث الثاني: الإجراءات الخاصة بالبحث والتحري في الجريمة الالكترونية. 15

المطلب الأول: آليات الكشف والتبليغ عن الجرائم المعلوماتية. 16

الفرع الأول: آليات الكشف عن الجرائم المعلوماتية..... 17

الفرع الثاني: كيفية التعامل مع التبليغ بشأن الجرائم المعلوماتية. 18

الفرع الثالث: كيفية التبليغ عن الجرائم المعلوماتية. 20

المطلب الثاني: الخطوات الأولية لمباشرة أعمال البحث والتحري عن الجرائم الالكترونية. 22

الفرع الأول: الإجراءات الأولية لكشف حقيقة الجريمة. 22

الفرع الثانى: إجراء الإرشاد الجنائي. 23
الفرع الثالث: إجراء الوضع تحت المراقبة الإلكترونية. 24
الفرع الرابع: التزامات مقدمي خدمات الانترنت في مجال مساعدة أعمال البحث والتحري..... 28
المطلب الثالث: الإجراءات الفنية الخاصة بمعاينة مسرح الجريمة المعلوماتية. 31
الفرع الأول: الإجراءات الخاصة بالانتقال إلى مسرح الجريمة وتأمينه..... 32
المطلب الرابع: الإجراءات الخاصة بالتفتيش وضبط الأدلة 39
الفرع الأول: الضوابط القانونية للتفتيش والضبط. 39
الفرع الثانى: القواعد الفنية المتبعة عند التفتيش والضبط 42
الفرع الثالث: وسائل تحليل الأدلة المحجوزة. 45
الفصل الثاني: إجراءات التحقيق في الجريمة الالكترونية. 50
المبحث الأول: إجراءات استخلاص الدليل في الجريمة الالكترونية. 51
المطلب الأول:مفهوم الدليل الالكتروني وانواعه. 51
الفرع الأول: مقاربة لتعريف الدليل الإلكتروني 52
الفرع الثاني: مميز ات الدليل الإلكترونـي 54
المطلب الثاني:شروط صحة الدليل الالكتروني. 58
الفرع الأول: مشروعية الدليل الالكتروني. 58
الفرع الثاني: أن يكون الدليل الإلكتروني يقيني غير قابل للشك..... 61
الفرع الثالث: قابلية الدليل الإلكتروني للمناقشة..... 61

المطلب الثالث: إجراءات تقليدية لاستخلاص الدليل الالكتروني. 62

الفرع الأول: اجراء التفتيش والضبط الإلكتروني –المعلوماتي:..... 63

الفرع الثاني: المعاينة والخبرة التقنية..... 66

الفرع الثالث: الشهادة في مجال الجريمة الإلكترونية: 71

الفرع الرابع: الاستجواب في مجال الجريمة الالكترونية..... 73

المطلب الثالث: إجراءات حديثة لاستخلاص الدليل الالكتروني..... 76

الفرع الأول: الإجراءات الحديثة لجمع الدليل الإلكتروني بموجب

المادة65مكرر 5إلى65مكرر 18. 77

الفرع الثاني الإجراءات الحديثة لجمع الدليل الإلكتروني بموجب القانون09-04. ... 80

المبحث الثاني: حجية الدليل الالكتروني في نطاق الاثبات الجنائي..... 86

المطلب الأول: مناقشة الدليل الالكتروني أمام قاضي الحكم..... 86

الفرع الأول: مبدأ حرية الإثبات الجنائي كأساس لقبول الدليل الإلكتروني: 87

الفرع الثاني. عرض الدليل الالكتروني ومناقشته من قبل أطراف الخصومة الجزائية. 90

المطلب الثاني: تقدير الدليل الالكتروني أمام قاضي الحكم..... 94

الفرع الأول: سلطة القاضي الجزائي في تقدير الدليل الرقمي: 95

الفرع الثاني: ضوابط اقتناع القاضي الجزائي بالدليل الإلكتروني–الرقمي:..... 99

المطلب الثالث: حجية الدليل الالكتروني في ظل الأنظمة اللاتينية: 102

المطلب الرابع: حجية الدليل الالكتروني في ظل الأنظمة اللانجلوسكسونية: 106

قائمة المصادر والمراجع

فهرس المحتويات

ملخص:

إن إجراءات البحث والتحقيق في الجنائي العام هي الأساس في البحث والتحقيق في جرائم الالكترونية تماما كما هو الحال في باقي الجرائم الأخرى، أما عناصر البحث والتحقيق الجنائي الأخرى من عملية وفنية وغيرها فإن استخدامها يتوقف على ظروف كل جريمة، فلما اعتمد المشرع الجزائري نصوصا لتجريم الأفعال الواقعة في الوسط الإلكتروني والمستخدم فيها الأجهزة الإلكترونية وكل ما يمس المعالجة الألية للمعطيات بمفهوم الجريمة الإلكترونية مما استدعى المشرع الجزائري الى ادخال مجموعة من التعديلات على كل من قانون العقوبات وقانون الاجراءات الجزائية، كما استحدث القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، اضافة الى القانون 18-04 المتعلق بالقواعد العامة للبريد والاتصالات الالكترونية، والقانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الكلمات المفتاحية: إجراءات التحقيق الإلكتروني، الجريمة الإلكترونية، التفتيش، التسرب، الترصد الإلكتروني.

Abstract :

The procedures of research and investigation of the general criminal are the basis for the research and investigation of electronic crimes just as in other crimes, but the elements of research and criminal investigation of the general criminal process and other, its use depends on the circumstances of each crime, when the Algerian legislator adopted texts to criminalize the acts in the electronic environment and the use of electronic devices and all that affects the automated treatment of data in the concept of cybercrime, which necessitated the Algerian legislator to introduce a set of amendments to all amendments to all From the Penal Code and the Penal Procedure Act, Act 09.04 on special rules for the prevention and control of crimes related to information and communication technologies was introduced, in addition to Law 18.04 on the General Rules of Mail and Electronic Communications, and Law 18.07 on the protection of natural persons in the processing of personal data.

Keywords: *electronic investigation procedures, cybercrime, inspection, leakage, electronic surveillance.*