المكافحة الإجرائية للجرائم الإلكترونية
دراسة حالة الجزائر

الدكتور: حاحة عبد العالي
أستاذ محاضر "أ"

قلات سمية
باحثة دكتوراه

كلية الحقوق و العلوم السياسية
جامعة محمد خيضر - بسكرة

الملخص:

إن أخطر ما أنجبته ثورة تقنية المعلومات التي من خلالها تم الانتقال من العالم الواقعي إلى العالم الإفتراضي هو سلوك إجرامي مستحدث يتمثل في الجرائم الإلكترونية التي تجاوزت كل الحدود الجغرافية و السياسية ، منبهة عن خطر يهدد الأمن الدولي و الوطني و هذا نتيجة حتمية لكل تطور علمي.

و نتيجة لما يتسم به هذا النوع من الإجرام الإلكتروني من حيث خصائصه و سمات مرتكبيه و الذي ينتج مختلف العوائق التي تقف أمام تطبيق الإجراءات التقليدية في سبيل الكشف و إثبات الجرائم الإلكترونية فقد استرعت اهتمام الدولة الجزائرية لوضع إستراتيجية إجرائية لمكافحتها.

Résumé :

La révolution de la technologie marque le passage du monde réel au monde virtuel ce qui a engendrer des comportements criminels nouveaux appelés la cybercriminalité qui ont traversé toutes les frontières géographiques et politiques, menaçant la sécurité internationale et nationale comme étant le résultat inévitable du progrès scientifique.

En conséquence ce type de criminalité électronique se caractérise en fonction des attributs des auteurs, qui produit divers obstacles à l'application des procédures traditionnelles afin de détecter et de prouver les crimes électroniques, poussant l'Etat algérien à élaborer une stratégie procédurale pour la combattre.

مقدمة:

مما لاشك فيه أن الجريمة الإلكترونية تعبير عن صورة من صور الإجرام المستحدث، الذي يمثل الجانب السلبي للتطور التكنولوجي الذي أثر على أمن المجتمعات والدول معا، إذ عرفت انتشارا واسعا في مختلف المجالات والميادين، جعل الكل يتفق على خطورتها التي تتزايد يوميا بفعل التطور السريع في وسائل المعلوماتية التي أصبحت تعتمد عليها الدول والحكومات إلى حد بعيد باعتبارها إحدى مؤشرات تحسين الخدمة العمومية والرقي بها.

والجزائر لم تكن بمنئ عن هذه الجريمة الإلكترونية التي أصبحت ظاهرة مثيرة للانتباه، تستدعي التشخيص والدراسة، إذ بلغت حدا من الخطورة، بحيث جعلت كل المجتمع الدولي يقف بالمرصاد لها، وذلك من خلال وضع الإستراتيجيات والخطط المختلفة لمواجهتها.

وتعد الآليات القانونية الموضوعية والإجرائية الوسيلة الأساسية ضمن استراتيجية مواجهة هذه الآفة، ويقصد بالآليات الموضوعية هو التجريم بصفة عامة، أي التنصيص على أفعال تمثل جريمة إلكترونية وتقرير عقوبات لها، وفي المقابل نجد آليات المكافحة الاجرائية الخاصة بهذه الجريمة وهي محل الدراسة.

ونظرا لما تتميز به الجريمة الإلكترونية من سمات تنفرد بها نذكر منها: أنها جرائم ناعمة وتتخطى حدود الدولة الواحدة وصعوبة الحصول على الدليل وإثباتها... كل هذا جعلها تنعكس على الأحكام الإجرائية التقليدية لمكافحتها وتتجاوزها من خلال عالمها التقني والافتراضي، مما استوجب على المشرع الجزائري التدخل والعمل على مواكبة الإجراءات التقليدية للجريمة الإلكترونية من ناحية مكافحتها وكذا استحداث إجراءات خاصة تتلاءم وطبيعة هذه الجريمة.

ولعل أهم الإجراءات التقليدية التي اصطدمت مع خصوصية الجريمة الإلكترونية مما أدى إلى تطويعها حسب هذه الخصوصية نجد المعاينة والتفتيش والضبط، وبالنسبة لوسائل الإثبات نجد الشهادة والخبرة، وبالنسبة للإجراءات المستحدثة التي واكبت الخصوصية نجد التسرب والمراقبة الإلكترونية، لكن في سبيل ذلك كان لزاما تحديد أشخاص وهيئات معينة تتعامل مع هذه الجريمة من الناحية الإجرائية في إطار الإقليم الجزائري كله، مع مراعاة الاختصاص الداخلي والخارجي، كما أنه من أجل المكافحة الفعالة للجريمة الإلكترونية ومحاصرتها، لجأ المشرع الجزائري إلى تبني إجراء المساعدة القضائية الدولية.

من خلال ما سبق نطرح الإشكالية التالية:

- **إلى أي مدى وفق المشرع الجزائري في إيجاد إطار قانوني إجرائي شامل وفعال لمكافحة الجرائم الإلكترونية؟**

و للإجابة عن هذه الإشكالية نقترح التقسيم الثنائي التالي:

المبحث الأول: القواعد الإجرائية التقليدية لمكافحة الجرائم الإلكترونية.

المبحث الثاني: القواعد الإجرائية المستحدثة لمكافحة الجرائم الإلكترونية.

المبحث الأول: القواعد الإجرائية التقليدية لمكافحة الجرائم الإلكترونية

تقوم مختلف الأجهزة المرصودة من قبل المشرع الجزائري بعملية التحري والتحقيق عن الجرائم الإلكترونية في إطار نطاق اختصاصها [1] ولقد نظم المشرع الجزائري عملية الكشف عن الجريمة الإلكترونية بقواعد إجرائية

تقليدية تواكب مكافحة هذا النوع من الإجرام المستحدث مما يجعلنان طرح سؤال حول مدى إمكانية إسقاط إجراءات التحري والتحقيق الكلاسيكية على الجرائم الإلكترونية؟

وللإجابة عن هذا السؤال نتناول بالدراسة الإجراءات المادية للمجابهة الجريمة الإلكترونية (المطلب الأول)، ثم وسائل الإثبات في الجريمة الإلكترونية(المطلب الثاني)، وهذا كله في ظل مراعاة مبادئ تطبيق القانون الجزائي.[2]

المطلب الأول: الإجراءات المادية لمجابهة الجريمة الإلكترونية

تقتصر دراستنا في هذا المقام على الإطار الإجرائي التقليدي الذي يتميز بخصوصية و هذا تبعية بديهية لما تتميز به الجريمة الإلكترونية من سمات تجعلها تنفرد بخصوصيات إجرائية لمكافحتها وتتمثل هذه الإجراءات في كيفية تلقي البلاغات و الشكاوى والمعاينة والتفتيش والضبط.

الفرع الأول: تلقي البلاغات و الشكاوى إلكترونيا

الإبلاغ هو إعلام السلطات المختصة عن وقوع جريمة سواء من الضحية أو من شخص آخر شهدها أو علم بها... وبالنسبة للجريمة المعلوماتية فإنه يتم التبليغ عنها سواء بالشكل التقليدي أو من خلال التبليغ الإلكتروني و هذا متاح على المستوى الوطني من خلال: جهاز الدرك الوطني:(الذي يضع تحت تصرف المواطنين بريد إلكتروني للتبليغ عن الجرائم الإلكترونية عنوانه : cgn@mdn_dzccom

أو من خلال الخدمة التي أصبحت متاحة منذ 7 أفريل2015 المتعلقة بإيداع الشكاوى أو المعلومات المتعلقة بالجرائم منها: www.ppgn.mdn.dz

و بالنسبة للمديرية العامة للأمن الوطني فإنها تضع هي كذلك تحت تصرف المواطنين للتبليغ عن أي جريمة مع ضمان سرية هويتهم الموقع التالي: www.dgsn.dz[3]

الفرع الثاني: المعاينة الإلكترونية

تعد من أهم الإجراءات الأولية اللازمة لكشف ملابسات الجريمة حيث تعرف على أنها(إثبات لحالة الأماكن و الأشخاص، وكل ما يفيد في كشف الحقيقة عن الجريمة و مرتكبها [4])، نستنتج من هذا التعريف أن إجراء المعاينة عبارة عن مسح حسي و مادي لمكان وقوع الجريمة...و بالتالي ضبط كل الدلائل التي تسمح بكشف الجريمة و قد نص المشرع الجزائري على أحكامها في المواد 42 و 43 و 49 من قانون الإجراءات الجزائية، و أمام الجريمة الإلكترونية فإننا نواجه مسرحين و هما:

أولا-مسرح تقليدي:

ويقع خارج البيئة الإلكترونية، يتكون من مكونات مادية ملموسة فهو في هذه الحالة مثل مسرح أي جريمة تقليدية أخرى.

ثانيا-مسرح افتراضي:

(و يقع داخل البيئة الإلكترونية، يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الأنترنت، في ذاكرة الأقراص الصلبة الموجودة بداخله [5]) ، أي من خلال هذا الطرح تنصب المعاينة على الكيانات المعنوية للحاسوب و كل ما هو إلكتروني وذلك من خلال اتباع اجراءات تتمثل في: القيام بتصوير جهاز الحاسب الآلي و كل ما يتصل به من أجزاء طرفية... وعدم نقل المواد المعلوماتية خارج مسرح الجريمة حماية لها من قوى مغناطيسية قد تتسبب في محوها [6] ، ملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها الولوج إليه [7] ، التحفظ على محتويات سلة المهملات.. [8] وكذا الإستعانة بأهل الخبرة عند الضرورة.

الفرع الثالث:التفتيش والضبط الإلكترونيان

يمثل إجراء التفتيش أهم الإجراءات التي تؤدي إلى الحصول على الدليل الالكتروني ومن ثم يتم ضبطه

أولا- التفتيش الإلكتروني:

أجمع الفقه على أن التفتيش:"هو إجراء من إجراءات التحقيق، يقوم به موظف مختص طبقا للإجراءات المقررة قانونا، في محل يتمتع بحرمة، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم". [9]

والتفتيش يعتبر وسيلة لتحقيق غاية و هي ضبط كافة الدلائل التي تشير لارتكاب الجريمة،حيث نص المشرع الجزائري على مجمل أحكامه في المواد من 44 إلى 48 و المادة 64 والمادتين

82 و 83 من قانون الإجراءات الجزائية المعدل و المتمم بالقانون رقم 06/ 22 وبالتالي فهو يعتبر إجراء يضطلع به كل من قاضي التحقيق وضباط الشرطة القضائية في حالة التلبس أو الإنابة القضائية.

ولما كان الحاسوب يتكون من مكونات مادية و معنوية **فالإشكال يثور حول مدى إمكانية خضوع هذه المكونات للتفتيش؟**

1-المكونات المادية:

هذه المكونات لا تثير أي إشكال فيما يخص تفتيشها فهي تخضع للقواعد القانونية المنصوص عليها في المادة44، وفي نطاق الجريمة الإلكترونية فإن مختلف الضمانات المقررة عند إجراء عملية التفتيش لا يؤخذ بها من احترام للميقات القانوني للتفتيش حيث يكون في أي ساعة من ساعات النهار أو الليل... و حضور المعني لعملية التفتيش لا يكون إجباري و عدم الأخذ برضاه...الخ.

2- المكونات المعنوية:

أثارت مسألة تفتيش المكونات المنطقية خلافا فقهيا ، إلا أنه في الأخير تم الأخذ بالرأي القائل بإمكانية تفتيشها وهذا ما جسده المشرع الجزائري بموجب المادة 5 من القانون رقم 09/ 04 و التي أجازت للسلطات القضائية المختصة وكذا لضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة 4 من نفس القانون نذكر منها حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أو في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام... وفي إطار تنفيذ طلبات المساعدة القضائية...الخ من الحالات التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها و كذا منظومة تخزين معلوماتية.

3-التفتيش عن بعد:

قد يكون حاسوب المتهم متصلا بغيره من الحواسيب عبر الشبكة ، سواء كان هذا الاتصال داخل إقليم الدولة أو خارجها و قد أخذ المشرع الجزائري بكلتا الحالتين حيث أجاز تمديد التفتيش بسرعة إلى منظومة معلوماتية غير منظومة المتهم متصلة بها بعد إعلام السلطات القضائية المختصة مسبقا، و إذا كان الاتصال بمنظومة معلوماتية خارج الإقليم فإنه يجوز تفتيشها و الحصول على المعطيات المبحوث عنها بمساعدة السلطات الأجنبية وفقا للاتفاقيات الدولية و مبدأ المعاملة بالمثل، كما يمكن للسلطات المكلفة بالتفتيش بتسخير أهل الخبرة لهم دراية بعمل المنظومة المعلوماتية(المادة 5 الفقرة 2 و 3 و 4).

و يخضع التفتيش لمجموعة من الشروط نذكر منها: توافر سبب التفتيش ونقصد به وقوع جريمة إلكترونية فعلا... ومحل التفتيش وكذلك السلطة المختصة به والتي سبق تناولهما وحصول إذن من عند وكيل الجمهورية أو قاضي التحقيق المختص...الخ وحضور أشخاص معينين لعملية التفتيش والميعاد الزمني له.

ثانيا- الضبط أو الحجز الإلكتروني

يقصد عموما بالضبط السيطرة المادية على الأشياء و وضعها تحت تصرف القضاء، وبشكل دقيق فإنه يقصد به (التحفظ على الأشياء و حجزها و وضعها في أختام ... ، إذا كانت الأشياء والوثائق تدفع إلى إظهار الحقيقة أو تلك التي يضر إفشائها بسير التحقيق) [10].

1-مدى إمكانية ضبط المكونات المنطقية: بعد أن ثار خلاف فقهي حول هذا الإشكال فقد أخذ المشرع الجزائري بإمكانية ضبط المكونات المعنوية من خلال المادة 6 من القانون رقم 04/09.

2-محل الضبط في الجريمة الإلكترونية: بالإضافة للمكونات المادية و المعنوية تضبط كذلك: البرمجيات و المعطيات التي يجري تبادلها في نطاق شبكة المعلومات التي تربط الحواسيب و ما يتصل بها. [11].

3-أسلوب ضبط المعطيات الإلكترونية: ويكون إما من خلال الحجز المادي حيث تنسخ المعطيات على دعائم التخزين تكون قابلة للحجز و تسهر السلطة المكلفة بالحجز على الحفاظ على سلامة المعطيات في المنظومة المعلوماتية و استعمال الوسائل التقنية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق(المادة 6) أو إتباع أسلوب الحجز عن طريق منع الوصول إلى المعطيات و هذا ما أقره المشرع الجزائري في نص المادة 7 من القانون رقم 04/09 بنصها على:" إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه،لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة".

كما يجوز بالنسبة للمعطيات المحجوزة ذات المحتوى المجرم أن تأمر السلطة المكلفة بالتفتيش بإجراءات منع الإطلاع عليها، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك و هذا ما نصت عليه المادة 8 من القانون رقم 04/09، و مثال ذلك حجب المواقع التي تحمل شعارات ضد الدولة.

من خلال ما سبق نلاحظ أن المشرع الجزائري تدخل لسد الفراغ التشريعي فيما يخص إجراء الضبط الإلكتروني حيث أنه في حال استحالة الحجز المادي للمعطيات يتم اللجوء إلى أسلوب منع

الوصول للمعطيات أو عدم الإطلاع على المعطيات وهذا كله في إطار تكريس مكافحة شاملة للجريمة الإلكترونية.

4- قواعد ضبط المعطيات الإلكترونية: في عملية ضبط الأدلة الجنائية سواء كانت أدلة إثبات أو نفي وجب إتباع قواعد خاصة ترجع لخصوصية المادة الواجب تحريزها للحفاظ عليها و تتمثل في: [12]

- ضبط الدعائم الأصلية للمعطيات و عدم الاقتصار على ضبط نسختها.
- عدم ثني القرص لمنع إتلافه، و كذا عدم تعريضه هو و الأشرطة الممغنطة لدرجات الحرارة العالية و لا إلى الرطوبة.
- منع الوصول إلى المعطيات التي تم ضبطها و ذلك عن طريق تشفيرها كما سبق القول.

المطلب الثاني: اجراءات إثبات الجريمة الإلكترونية

تعد الجريمة الإلكترونية جريمة تقنية تحتاج للدقة في التعامل معها سواء من ناحية الإجراءات المتبعة بشأنها أو من ناحية وسائل إثباتها والتي يجب مواكبتها وإعطاء خصوصيات لها، ويمكن حصر أهمها في: الاستجواب والشهادة و الخبرة.

الفرع الأول: الاستجواب الإلكتروني

يعتبر الاستجواب الإلكتروني أحد إجراءات التحقيق في الجريمة الإلكترونية للكشف عن هوية المتهم وعلاقته بالجريمة...، كما أنه محاط بجملة من الشروط و الضمانات التي تكفل تحقيق عادل.

أولا: المقصود بالاستجواب الإلكتروني

يعتبر إجراء قضائي يقوم به قاضي التحقيق وهو على أربع مستويات استجواب عند الحضور الأول و استجواب في الموضوع و استجواب اجمالي و استجواب في حالة الإستعجال، حيث يقوم قاضي التحقيق من خلال الإستجواب الأولي من التأكد من هوية المتهم و إحاطته بالوقائع المجرمة المنسوبة إليه و تعيين محامي له إذا لم يختر المتهم محامي له بشرط أن يكون قد طلب ذلك ...و بالنسبة للإستجواب في الموضوع فإنه يؤخذ كقرينة ضد المتهم و يتم بصيغة سين و جيم ... ، وهذا كله في ظل استيفاء الشروط القانونية و احترام الضمانات المقررة عند الإستجواب وهو ما نصت عليه المواد من 100إلى 105 من قانون الإجراءات الجزائية المعدل و المتمم.

ثانيا: قواعد استجواب المجرم الإلكتروني:

يتبع في ذلك أسلوب قبلي و يتمثل في تبادل المعلومات بين قاضي التحقيق والخبير الإلكتروني حيث يقوم هذا الأخير بشرح كافة الأبعاد التقنية والمصطلحات الإلكترونية لقاضي التحقيق والتي

يمكن استخدامها أثناء الاستجواب وفي الأخير وضع خطة الاستجواب بناء على المعطيات السابقة [13] ، وأسلوب بعدي أي عند بدء الاستجواب حيث يتم إتاحة الفرصة للخبير لحضور جلسة الاستجواب مع إمكانية توجيه أسئلة فرعية للمتهم و في حال الدول التي لا تسمح بذلك يستحب تكوين لجان تحقيق لحضور الخبير في عضويتها،تفادي إضاعة الوقت في استجواب المتهم حول جريمة لا يمكن اكتشافها مع تحرير محضر الإستجواب بكل دقة و وضوح [14] .

الفرع الثاني: الشهادة الإلكترونية

تعرف الشهادة عموما على أنها أقوال يدلي بها غير الخصوم أمام الجهات القضائية و إسنادها للمتهم بالنفي أو الإثبات وهي على أنواع شهادة مباشرة و نقصد بها كل شخص شهد وقوع الجريمة بحواسه ... شهادة سماعية حيث نقلها شخص لشخص آخر.. و شهادة بالتسامع وهي التي سمعها شخص من ما يتداوله الناس من أقوال و تختلف القيمة الثبوتية لهذه الأنواع من الشهادة حسب تدرجها، نص المشرع الجزائري على مختلف أحكامها في المواد من 220 إلى 238 من قانون الإجراءات الجزائية المعدل و المتمم.

أولا:تعريف الشاهد الإلكتروني:

يقصد به صاحب الخبرة و التخصص في المجال الإلكتروني حيث تكون له معلومات عن شبكة الانترنت و شبكات الاتصال ... حيث تشمل فئات الشهادة بهذا المفهوم عدة طوائف منها مستخدموا الحاسب الآلي و خبراء البرمجة و المحللون و مهندسو الصيانة و الخبراء التقنيين ومقدمي الخدمات الوسيطة [15] .

ثانيا:مدى إلزام الشاهد بتقديم معلومات عن الجريمة الإلكترونية:

بالرغم من اختلاف الفقه والقانون بخصوص هذا الشأن إلا أن موقف المشرع الجزائري محدد من خلال المادة 10 من القانون رقم 04/09 إذ ألزمت مقدمي الخدمات بالتعاون مع السلطات المكلفة بالتحريات القضائية من أجل تزويدهم بكافة المعطيات المتعلقة بمحتوى الإتصالات وفي هذا الإطار نجد أن المشرع الجزائري ألقى مجموعة من الالتزامات على عاتق مقدمي الخدمات منها حفظ المعطيات المتعلقة بحركة سير أي حمايتها و منع إتلافها و قد تم تحديد أنواع هذه المعطيات و هذا كله في (المادة11) و كذلك ما نصت عليه المادة 12 من التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين و تخزينها أو جعل الدخول إليها غير ممكن و كذا وضع الترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة و إخبار المشتركين لديهم بوجودها، من خلال هذا يحاول المشرع الجزائري حصر الجريمة الإلكترونية و تطويقها من مختلف الجوانب .

ثالثا:التزامات الشاهد في الجريمة الإلكترونية:

نذكر منها طبع ملفات البيانات المخزنة...و تسليمها للسلطات القضائية و الإفصاح عن كلمات المرور و الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة [16] ...الخ.

الفرع الثالث:الخبرة الإلكترونية

عادة ما تعترض القاضي الجزائي أمور فنية تحتاج لذوي الاختصاص كل في مجاله منها الجريمة الإلكترونية، لذا تسند مهام الخبرة لرجال خارج القضاء في نطاق الشروط الواجب احترامها.

أولا: المقصود بالخبرة الإلكترونية

يقصد بها عموما استخدام قدرات شخص الفنية أو العلمية والتي لا تتوافر لدى رجل القضاء أو المحقق من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع الجريمة أو نسبتها إلى المتهم... [17].

من خلال التعريف أعلاه نستنتج أن الخبرة وسيلة من وسائل الإثبات الفنية التي تتطلب الاستعانة بذوي التخصص من غير رجال القضاء و قد نظم المشرع مختلف أحكامها من اختيار الخبراء وواجباتهم منها حلف اليمين و خضوعهم للرقابة القضائية و قيامهم بأداء مهامهم بأنفسهم و إيداع التقارير في المدة المحددة..الخ في المواد من 143 إلى 156 من قانون الإجراءات الجزائية المعدل و المتمم بالقانون رقم 22/06، و لقد أشار المشرع الجزائري للخبرة في مجال الجريمة الإلكترونية أيضا من خلال الفقرة الأخيرة من المادة5 من القانون رقم 04/09 عندما نصت على أنه يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية...قصد مساعدتها وتزويدها بكل المعلومات الضرورية و كذلك المادة 19 من المرسوم261/15 السابق ذكره حيث سمحت للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال الإستعانة بأي خبير قصد مساعدتها في أعمالها.

ثانيا: القواعد الفنية التي تحكم الخبرة الإلكترونية [18]

وتتجسد في خطوات ما قبل التشغيل نذكر منها التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدون عليها و كذلك من صلاحية وحدات النظام للتشغيل، وفي خطوات التشغيل و الفحص والتي تتجلى في استكمال تسجيل باقي معطيات الوحدات من خلال قراءات الجهاز وعمل نسخة من كل وسائط التخزين المضبوطة لإجراء الفحص المبدئي على هذه النسخة لحماية الأصل... تحديد أنواع وأسماء المجموعات البرامجية، إظهار الملفات المخبأة...الخ ، والقاعدة الثالثة تحديد مدى ترابط بين الدليل المادي والتقني وفي الأخير تدون النتائج وإعداد التقارير.

المبحث الثاني: القواعد الإجرائية المستحدثة لمكافحة الجرائم الإلكترونية

في حين عمل المشرع الجزائري على مواكبة الإجراءات التقليدية للجريمة الإلكترونية قام باستحداث إجراءات تعمل على مجابهة الإجرام الخطير نظرا لتطور الجريمة بمختلف أنواعها منها الجريمة الإلكترونية تتماشى وطبيعتها الخاصة ، حيث نص عليها في قانون الإجراءات الجزائية خاصة المعدل والمتمم بالقانون رقم 22/06 و إجراءات أخرى في القانون رقم04/09 و تتمثل هذه الإجراءات في إجراء التسرب أولا وإجراء المراقبة الإلكترونية(ثانيا).

المطلب الأول: التسرب

عالج المشرع هذا الإجراء في ثمانية مواد وهي من المادة 65 مكرر 11إلى المادة 65 مكرر18 من قانون الإجراءات الجزائية تناولت جل الأحكام المتعلقة بالتسرب من تحديد المقصود بعملية التسرب وكل ما يدور في فلكها من شروط..الخ.

الفرع الأول: تعريف التسرب

تصدى المشرع الجزائري هذه المرة بتحديد المقصود من عملية التسرب بالرغم من أن هذا من عمل الفقه فنصت المادة 65 مكرر12 على أنه :"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 أو خاف"، يستنتج من هذه المادة أن هذا الإجراء جد خطير بوضع ضابط أو عون ضمن مجموعة إجرامية لذا يجب أن تساق هذه العملية بجملة من الضوابط و الشروط.

الفرع الثاني: شروط عملية التسرب:

نذكر منها الإذن الذي يجب أن يتحصل عليه المتسرب من الجهة القضائية المختصة ممثلة في وكيل الجمهورية أو قاضي التحقيق ، على أن يكون هذا الإذن مكتوب و مسببا تحت طائلة البطلان و الذي يجب أن يتضمن هوية الضابط الذي تتم عملية التسرب تحت مسؤوليته و المدة المحددة لعملية التسرب هي 4 أشهر قابلة للتجديد حسب مقتضيات التحري و التحقيق في الجريمة الإلكترونية، و يمكن للقاضي الذي أمر بهذا الإجراء أن يأمر بتوقيفه قبل انقضاء المدة المحددة(المواد 65 مكرر11 و مكرر15 و مكرر17)،و كذلك تحديد نوع الجريمة على أن تكون من الجرائم التي حددتها المادة 65 مكرر5 و بطبيعة الحال نجد من بينها الجريمة الإلكترونية...الخ من الأحكام التي تضبط عملية التسرب خاصة فيما يخص مسؤولية القائمين بها[19].

ومثال ذلك في الجريمة الإلكترونية أن يقوم المتسرب و هو ضابط أو عون الشرطة القضائية بالدردشة مع المشتبه فيهم و إخبارهم بأنه قام مثلا بإختراق موقع وهمي ما مع تجسيد ذلك فيصدقونه و يتعودوا الحديث معه و إخباره بمختلف أنشطتهم الإجرامية الإلكترونية.

المطلب الثاني: المراقبة الإلكترونية

نص المشرع الجزائري على هذا الإجراء في قانون الإجراءات الجزائية في صورة الترصد الإلكتروني في المواد من 65 مكرر5 إلى 65 مكرر10 متمثل في الأعمال التالية: اعتراض المراسلات و تسجيل الأصوات و التقاط الصور و يلجأ لهذا الإجراء متى اقتضت ضرورات التحري و التحقيق في الجرائم الخطيرة منها الجريمة الإلكترونية وذلك مع مراعاة جملة من الشروط منها الحصول على الإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق الذي تجرى عملية اعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية و وضع الترتيبات التقنية من أجل تسجيل الكلام و التقاط الصور... تحت رقابته لمدة 4 أشهر..الخ [20].

الفرع الأول :تعريف مراقبة الإتصالات الإلكترونية

نحدد المقصود بإجراء المراقبة أولا ثم محل المراقبة أي الإتصالات الإلكترونية ثانيا.

أولا:المقصود بإجراء مراقبة الإتصالات الإلكترونية

تعرف على أنها (مراقبة شبكة الإتصالات، أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع المعطيات و المعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته، مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر[21]) يشبه لحد بعيد ما تضمنته المواد السالفة الذكر في قانون الإجراءات الجزائية.

ثانيا- المقصود بالإتصالات الإلكترونية:

يقصد بها أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو معلومات مختلفة بواسطة أي وسيلة إلكترونية(المادة 2 من الفقرة و) من القانون رقم 04/09.

الفرع الثاني: حالات اللجوء للمراقبة الإلكترونية و ضوابطها:

لا يمكن اللجوء لإجراء المراقبة الإلكترونية إلا إذا توفرت حالتها و ضوابطها.

أولا:حالات اللجوء للمراقبة الإلكترونية

نصت عليها المادة 4 من القانون رقم 04/09 و تتمثل في الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة فهنا طبق المشرع الجزائري مستوى من مستويات

السياسة الجنائية على غرار المستوى التجريمي والعقابي نجد المستوى الوقائي، وفي حالة توافر معلومات عن احتمال اعتداء على المنظومة على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني أو في حالة مقتضيات التحريات و التحقيقات القضائية أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

ثانيا: ضوابط المراقبة الإلكترونية من خلال القانون رقم 04/09

تتمثل في تقديم الإذن من قبل النائب العام لدى مجلس قضاء الجزائر، بناء على تقرير يبين طبيعة الترتيبات التقنية المستعملة و الأغراض الموجهة لها ، و يكون القائمون بعملية المراقبة ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها دون غيرهم .

و بالنسبة للمدة تم تحديدها بستة أشهر قابلة للتجديد و هذا عندما يتعلق الأمر بالحالة الأولى المتمثلة في الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ونود أن نشير في الأخير أنه لتطبيق مبادئ سريان القانون الجزائي **لابد من التعاون الدولي لمكافحة الجرائم الإلكترونية** لأن الدول خاصة غير المتطورة لا تقدر وحدها على مجابهتها، وفي إطار ذلك نص القانون رقم 09 /04 على المساعدة القضائية الدولية المتبادلة في المادة 16 منه حيث يمكن أن تتم في حالة الاستعجال عن طريق وسائل الإتصال السريعة مثل الفاكس أو البريد الإلكتروني، لكن هذه المساعدة ترد عليها قيود نصت عليها المادة 18 من نفس القانون تتمثل في عدم المساس بالسيادة الوطنية و كذا وجوبية المحافظة على سرية المعلومات المبلغة وعدم استعمالها في غير ما هو موضح في الطلب، و تتجسد مظاهر التعاون الدولي في تبادل المعلومات أي تقديم البيانات و الوثائق التي تطلبها سلطة قضائية لدولة أجنبية و هي بصدد النظر في جريمة إلكترونية(المادة17 من القانون04/09)

ونقل الإجراءات إذ يقصد به قيام دولة بمقتضى اتفاقية أو معاهدة باتخاذ إجراءات جزائية وهي بصدد التحقيق في جريمة إلكترونية

ارتكبت في إقليم دولة أخرى و لمصلحة هذه الدولة مع احترام مجموعة من الشروط [22] ، والإنابة القضائية(المواد من 721 إلى725 من قانون الإجراءات الجزائية) و التي نعني بها قيام دولة بطلب من دولة أخرى القيام بإجراء جزائي محدد تعذر القيام به بنفسها في إطار النظر في مسألة معروضة عليها متعلقة بالجريمة الإلكترونية... [23] و تسليم المجرمين إذ أصبح المجرم الإلكتروني مجرم دولي و بالرجوع لمبدأ السيادة فلا يصح لدولة ما متابعته و إلقاء القبض عليه خارج نطاق إقليمها، فكان من اللازم الأخذ بهذه الآلية و هو ما تجسد من قبل المشرع الجزائري في المواد694 و ما يليها من قانون الإجراءات الجزائية، لكن لابد من تدعيم التعاون الدولي القضائي بتعاون دولي فني من خلال التدريب التقني و

نقل الخبرات من الدول المتقدمة للدول الغير متطورة في مجال مفاهيم و أساليب الجريمة الإلكترونية...الخ.

و بالنسبة للتوقيف للنظر: فإنه في حالة تم توقيف المشتبه في ضلوعهم في الجريمة الإلكترونية للنظر فلضابط الشرطة القضائية تمديد مدة التوقيف و هي 48 ساعة مرة واحدة في هذه الجريمة ، إذا رأى أن ذلك ملائما لمقتضيات التحري و التحقيق شريطة أن يطلع فورا وكيل الجمهورية و يكون ذلك بإذن مكتوب(المادة 51 من قانون الإجراءات الجزائية المعدل و المتمم).

الخاتمة:

نخلص في الأخير أنه بالرغم من أن الجريمة الإلكترونية ترتكب بوسائل و أساليب تقنية و متطورة و لعل هذا ما يعطيها طابع التميز، إلا أنه نجد في المقابل الهيئة التشريعية الجزائرية تحاول جاهدة مواكبة هذا التطور الإجرامي ومكافحته من خلال العديد من الإجراءات المنصوص عليها في القانون العام و نقصد بذلك قانون الإجراءات الجزائية أو في قوانين خاصة منها القانون رقم 09-04.

ولعل ما أقره المشرع الجزائري من إجراءات للتصدي لهذه الظاهرة الإجرامية التي أصبحت في إنتشار واسع و سريع نجد إجراءات تقليدية بلباس إلكتروني وهي : إجراء تلقي البلاغات و الشكاوى الذي أصبح يتم بطريقة إلكترونية من خلال إيداع الشكاوى و التبليغ عن الجرائم في المواقع التي تتيحها السلطات المختصة و إجراء المعاينة التي تصطدم بمسرحين للجريمة الإلكترونية مسرح تقليدي و مسرح افتراضي، و كذلك إجراء التفتيش الذي تحكمه مجموعة من الضمانات و الشروط و الذي يتم في بيئة إلكترونية من قبل المختصين و هو ما ينطبق على الضبط أيضا حيث يتم نسخ ما تم العثور عليه من عملية التفتيش من مكونات معنوية و تحريزها...الخ.

وفيما يخص وسائل الإثبات فقد تطرقنا للاستجواب الذي يتم في حالة حضور شخص له دراية تقنية و يعرف مصطلحات الجريمة الإلكترونية لكن هذا لم يأخذ به بعد في التشريع الجزائري ... و كذلك الشهادة التي عرفت فئات جديدة غير الشاهد التقليدي و إلزام الشاهد المعلوماتي بتقديم شهادته وكما يساعد في فك لغز الجريمة... وبالنسبة للخبرة فهي توكل لأصحاب الإختصاص في المجال التكنولوجي و تخضع لمجموعة من القواعد كما أسلفنا.

وبالرجوع للأحكام الإجرائية الجديدة فإننا نتحدث عن عملية التسرب و إن كانت من الإجراءات الشخصية التي يضطلع بها ضابط الشرطة القضائية في ظل احترام الضمانات و الشروط المحددة قانونا، و أيضا المراقبة الإلكترونية التي نجدها زاوجت في التنصيص عليها بين قانون الإجراءات الجزائية و قانون رقم09-04 الذي أعطى لها أحكام خاصة من حيث شروط القيام بها و الحالات التي يتم اللجوء فيها لهذا الإجراء.

والقيام بمختلف هذه الإجراءات يحتم على القائمين بها احترام نطاق اختصاصهم سواء النوعي أو المحلي حيث تعرف مكافحة الجريمة الإلكترونية امتداد على كافة الإقليم الوطني، كما أنه و في إطار المكافحة الفعالة لهذه الجريمة استحدث المشرع الجزائري هيئة وطنية تتكون من أشخاص مؤهلين لهذا الغرض و وحدات مختصة على مستوى جهاز الدرك الوطني و المديرية العامة للأمن الوطني، و كل هذا مع مراعاة قواعد و مبادئ تطبيق القانون الجزائي و كذلك القيام بإجراءات المساعدة القضائية الدولية المتبادلة تحت لواء الاتفاقيات والمعاهدات أو مبدأ المعاملة بالمثل.

وفي الأخير يمكن القول أن المشرع حاول جاهدا من خلال نصوص قانون الإجراءات الجزائية والقوانين المكملة له إيجاد إطار تشريعي إجرائي لا بأس به من أجل مكافحة الجريمة الإلكترونية، ما يتبقى سوى تفعيل حقيقي ومادي للنصوص القانونية وتكوين متخصصين في مجال الإلكترونيك بشكل جدي الذين يقومون بالتحري والتحقيق واكتساب مهارات الدول التي قطعت شوطا في مكافحة هذه الجريمة.

و من خلال ما سبق نقدم الاقتراحات التالية:

1- سن قانون إجرائي جزائي خاص وموحد تجمع وتحدد فيه مختلف الإجراءات بدقة و وضوح لمكافحة الجريمة الإلكترونية ، بغية تجنب تعارض الإجراءات العامة و الخاصة سواء في الأحكام أو المصطلحات.

2- إنشاء هياكل متخصصة في مكافحة هذا النوع من الإجرام المستحدث، و هذا ما تم تجسيده و العمل به من قبل المشرع الجزائري كإنشاء الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال...الخ، لكن هذا لا يزال يحتاج لتفعيل حقيقي لعمل الهيئة و المراكز المتخصصة الأخرى و إعطائها كامل الحرية و الاستقلالية في إنجاز مهامها بشرط عدم تعارض ذلك مع الحريات الخاصة...الخ، و حبذا لو تم وضع هذه الهيئات تحت يد القضاء الذي يستطيع أن يوازن بين المصالح العامة و الخاصة...

3- تشجيع على خدمة تلقي الشكاوى و البلاغات إلكترونيا و العمل بها و نشر ثقافتها... من خلال تحسيس الأشخاص بصفة عامة و الضحايا بصفة خاصة على التبليغ على مثل هذه الجرائم بسرعة من أجل ضمان سهولة الكشف عن الجريمة الإلكترونية وسرعة اتخاذ الإجراءات بشأنها.

4- حبذا لو أخذت الجزائر بالاستعانة بخبير الكتروني بجانب قاضي التحقيق إذا كان غير عارف بالأمور التقنية أثناء التحقيق مع المجرم الإلكتروني في سبيل سهولة التعامل مع مفردات الجريمة الإلكترونية...الخ.

5- تزويد الجهات الأمنية و القضائية بوسائل تعزز عملها و تأهيل أفرادها من خلال دورات تكوينية و تدريبية في المجال الإلكتروني و بالتالي جاهزيتها لمواكبة تطور الجريمة الإلكترونية.

6- التوعية من خطورة الجريمة الإلكترونية سواء توعية مادية واقعية من خلال عقد مختلف الندوات و الملتقيات و تدخل الإعلام بكل أنواعه أو توعية رقمية افتراضية من خلال الحث على عدم إعطاء معلومات شخصية الكترونيا و كلمات المرور ...الخ.

7- تحديد حالات اللجوء لإجراء المراقبة الإلكترونية بشكل ضيق وخاص، فالمادة 4 من القانون 04/09 حددت الحالات على سبيل الحصر لكن من بين الحالات نجد اللجوء للمراقبة الإلكترونية حسب مقتضيات التحري و التحقيق و هذا يجعل اللجوء لمثل هذا الإجراء عام في كل الجرائم .

8- أن يكون إجراء التسرب من قبل ضباط الشرطة القضائية أو أعوانهم مختصين في الجانب التقني والفني فضلا عن الجانب الإجرائي القانوني ... لسهولة التعامل مع المجرمين الإلكترونيين وصعوبة كشف المتسرب.

9- تطبيق حقيقي لتزويد الجهات القضائية بمعلومات تفيد الكشف عن الجريمة الإلكترونية ...الخ، وأيضا وضع كاميرات في مقاهي الانترنت وغلق مواقع لها علاقة بارتكاب الجريمة الإلكترونية أو تعطيل الإطلاع عليها من خلال برامج معينة.

10- نصت المادة 19 من المرسوم الرئاسي رقم261/15 على أنه يمكن للهيئة الإستعانة بخبير... يعينها على أداء عملها، في حين نجد أنه من بين تشكيلتها كما أسلفنا تشكيلة تقنية، لذا حبذا توضيح ما المقصود بخبير هنا فلو كان خبير تقني في المجال الإلكتروني فهذا لا يستقيم مع تشكيلتها...الخ.

11- تشجيع التعاون الدولي فيما يخص مكافحة الجريمة الإلكترونية من خلال إبرام اتفاقيات ثنائية و جماعية و من ثم التغلب على إشكالات و صعوبات التي تعترض هذا الإجراء و تجاوزها، و بالتالي تكون مكافحة دولية لمجرمي الجريمة الإلكترونية و محاصرتهم.

الهوامش :

1- يتحدد اختصاص الهيئات القضائية أو الأمنية في مكافحة الجرائم الإلكترونية بثلاث أنواع نتطرق إليها كما يلي:
اختصاص شخصي و يقصد به الجهات المعنية بالبحث عن الجرائم الإلكترونية و تتمثل حسب التشريع الجزائري في: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها التي أنشئت بموجب القانون رقم 04/09 المؤرخ في 5 أوت 2009، **المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**، جريدة رسمية عدد 47، المؤرخة في 16 أوت 2009 وذلك من خلال المادة 13 والتي أحالت كيفية تنظيمها وسيرها إلى المرسوم الرئاسي رقم 261/15 المؤرخ في 8 أكتوبر 2015، **المتعلق بتحديد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها**، جريدة رسمية. عدد 53، المؤرخة في 8 أكتوبر 2015.
إذ تعتبر هذه الهيئة من خلال مضامين المواد من 1 إلى 4 سلطة إدارية تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل و مقرها الجزائر العاصمة، وتتولى المهام المنصوص عليها في المادة 14 من القانون رقم 04/09 وهي تنشيط و تنسيق عمليات الوقاية من الجرائم الإلكترونية ومساعدة السلطات القضائية ومصالح الشرطة القضائية في عملية التحري بخصوص هذا النوع من الجريمة وكذلك تبادل المعلومات مع نظيرتها في الخارج قصد تتبع مرتكبي الجريمة الإلكترونية (بتصرف من الباحثين)، و ذلك تحت رقابة السلطة القضائية و طبقا لأحكام قانون الإجراءات الجزائية و هي نفس المهام المتضمنة في المادة 4 من المرسوم السالف الذكر و التي حددت المهام على سبيل الحصر وبشكل موسع و مرد ذلك أي تكرار المهام المنصوص عليها في المادة 14 في المرسوم رقم 261/15 هو أن هذا الأخير صدر بشكل متأخر تقريبا 6 سنوات لذا حددت المهام في القانون رقم 04/09 أولا، وبالنسبة لتشكيلتها فقد نصت عليها المادة 6 من المرسوم إذ تتكون من تشكيلة إدارية تتمثل في لجنة مديرة ومديرية عامة(أنظر المواد رقم 7 و 8 و 9 و 10 من المرسوم) ومن تشكيلة تقنية تتمثل في مديرية المراقبة الوقائية و اليقظة الإلكترونية يتبعها مركز للعمليات وملحقات

جهوية(أنظر المواد 11 و 13 و14 من المرسوم) و مديرية التنسيق التقني(أنظر المادة12)، هذا فيما يخص الهيئة و كذلك تم إنشاء وحدات تابعة لسلك الأمن الوطني يوجد على مستواها مصلحة نيابة مديرية الشرطة العلمية و التقنية والتي بدورها تنقسم إلى المخبر المركزي للشرطة العلمية مقره الجزائر العاصمة و مخبران جهويان مقرهما قسنطينة و وهران حيث توجد على مستوى هذه المخابر دائرتان علمية و تقنية و هذه الأخيرة هي التي تتولى مهمة التحري و التحقيق وتحليل الأدلة الجنائية المتحصل عليها من ارتكاب الجرائم الإلكترونية، أنظر: عبد الرحمان حملاوي، **دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق، جامعة محمد خيضر، بسكرة،16 و17 نوفمبر2015، ص8.

وبالرجوع للوحدات التابعة للدرك الوطني فإننا نجد على المستوى المركزي مديرية الأمن العمومي و الاستغلال و المصلحة المركزية للتحريات الجنائية والمعهد الوطني للأدلة الجنائية وعلم الإجرام الذي تم إنشائه بموجب المرسوم الرئاسي رقم 04 / 183 المؤرخ في 26 جوان2004،**المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني** ،جريدة رسمية.عدد41، المؤرخة في 27 جوان 2004.، مركز الوقاية من جرائم المعلوماتية، أما على المستوى الجهوي نجد المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني، و بالنسبة للمستوى المحلي نجد فصائل ذات خبرة تساعد في التحري عن الجريمة الإلكترونية و كذلك خلايا الشرطة العلمية و التقنية.

كما نجد المادة 15 من الأمر رقم 155/66 المؤرخ في 8 جوان 1966، **المتعلق بقانون الإجراءات الجزائية**، جريدة رسمية .عدد49، المؤرخة في 11 جوان1966، المعدل والمتمم بالأمر رقم 02/15 المؤرخ في 23 جويلية2015، المتعلق بتعديل وتتميم قانون الإجراءات الجزائية، جريدة رسمية.عدد40، المؤرخة في 23 جويلية2015، قد حددت الأشخاص الذين لهم صفة الضبطية القضائية لمكافحة الجرائم ومنها الجريمة الإلكترونية والذين نجد بعضهم ينتمي للوحدات السابقة الذكر لكن ما يشار إليه إلى أن من بين هؤلاء الأشخاص المحددين نجد رئيس المجلس الشعبي البلدي وهو الأمر الذي لا نجده منطقي لأنه لا يكون غالبا له دراية تقنية بالجريمة الإلكترونية.

اختصاص نوعي: حيث نجد أن الأشخاص السالف ذكرهم توكل لهم مهمة التحري عن الجريمة الإلكترونية و الذين يعملون تحت إشراف و مراقبة الجهات القضائية، ونقصد بذلك النيابة العامة وقضاء التحقيق، كما أن المحكمة المختصة في الفصل في القضايا المتعلقة بالجرائم الإلكترونية هي الأقطاب الجزائية(مرسوم تنفيذي رقم 348/06 المؤرخ في 5 أكتوبر 2006،**المتعلق بتمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق**، جريدة رسمية.عدد63،المؤرخة في 5 أكتوبر 2006.)التي تم استحداثها للنظر في الجرائم الخطيرة.

اختصاص محلي: يتحدد الاختصاص المحلي لضباط الشرطة القضائية في الحدود التي يمارسون فيها وظائفهم المعتادة و في حالة الاستعجال يمتد هذا الاختصاص إلى كافة دائرة المجلس القضائي و إلى كافة الإقليم الوطني وكذلك في حالة التحري عن الجرائم الخطيرة منها الجريمة الإلكترونية(المادة 16 من قانون الإجراءات الجزائية المعدلة بالقانون رقم 22/06 المؤرخ في 20 ديسمبر2006،المتعلق **بتعديل و تتميم قانون الإجراءات الجزائية**، جريدة رسمية.عدد84،المؤرخة في 24 ديسمبر2006.)

2- تتمثل هذه المبادئ في:**مبدأ الإقليمية** والذي يقصد به تطبيق القانون الجزائي داخل نطاق حدود الدولة إذ يستند لعدة مبررات منها فكرة سيادة الدولة، إذ نصت عليه المادة 3 من الأمر رقم 66 /156 المؤرخ في 8جوان1966، **المتعلق بقانون العقوبات**، جريدة رسمية.عدد49،المؤرخة في 11جوان1966. كما تنص المادة586 من قانون الإجراءات الجزائية على أنه يكفي وقوع عمل من الأعمال المميزة للجريمة على إقليم الجزائر لتطبيق القانون الجزائي الجزائري، ونصت كل من المادتين590 و 591 من قانون الإجراءات الجزائية على الإقليم الاعتباري. و تطبيقا لهذا المبدأ نقوم بإعطاء مثال : شخص يقوم بجريمة الدخول الغير مشروع لنظام المعالجة الآلية للمعطيات و يقوم بتعديلها...سواء ارتكب السلوك الإجرامي أو تحققت النتيجة في الجزائر...الخ.

مبدأ الشخصية: نصت عليه المادتين 582 و 583 من قانون الإجراءات الجزائية و مفاده تطبيق القانون الجزائي على كل جزائري ارتكب جناية أو جنحة خارج الإقليم لكن بشروط أن تكون الجريمة الموصوفة جناية أو جنحة و بالتالي لا يتم الأخذ بالمخالفات مجرمة في كلا القانونين أي قانون الدولة الجزائرية و قانون الدولة التي ارتكبت فيها الجريمة، عودة المتهم إلى الجزائر و ألا يكون قد حكم عليه بحكم نهائي ... و هذا مبدأ الشخصية الإيجابي و بالنسبة للسلبي و الذي يقصد به تطبيق القانون الجزائي في حالة إذا ما كان المجني عليه جزائري فالمشرع الجزائري لم يأخذ به إلا من خلال المادة591 من قانون الإجراءات الجزائية. مثال قيام جزائري في الخارج باختراق مواقع إلكترونية لشركات كبرى هذا بالنسبة لمبدأ الشخصية الإيجابي أما السلبي فمثاله قيام أجنبي بالاعتداء على البريد الإلكتروني لجزائري في دولة أجنبية أخرى فالقانون الجزائي الجزائري يبقى مختص في حالة ما تم القبض على الجاني أو تم تسليمه للسلطات الجزائرية.

مبدأ العينية: و مفاده تطبيق القانون الجزائي الجزائري على كل شخص سواء جزائري أو أجنبي ارتكب جريمة خارج الجزائر لكن تضر بمصالحها الإستراتيجية ، حيث نصت عليه المادة 588 من قانون الإجراءات الجزائية و كذا المادة 15 من القانون رقم 04/09السالف الذكر. و مثاله قيام شخص بإرسال فيروسات للنظام المعلوماتي لوزارة الدفاع الوطني لتعطيل عمله متى ألقي القبض على الجاني أو تم تسليمه وفقا لإجراءات تسليم المجرمين.

مبدأ الصلاحية الشاملة: حيث تنص المادة 585 قانون الإجراءات الجزائية على:« كل من كان في إقليم الجمهورية شريكا في جناية أو جنحة مرتكبة في الخارج يجوز أن يتابع من أجلها و يحكم عليه فيها بمعرفة جهات القضاء الجزائرية إذا كانت الواقعة معاقبا عليها في كلا القانونين الأجنبي و الجزائري بشرط أن تكون تلك الواقعة الموصوفة بأنها جناية أو جنحة قد ثبت ارتكابها بقرار نهائي من الجهة القضائية الأجنبية » . مثاله قيام فرنسي بمساعدة شخص ألماني للقيام بعملية الاحتيال

على مصرف في إسبانيا، ثم حضر الفرنسي إلى الجزائر و تم القبض عليه هنا ينعقد الإختصاص الجزائي للدولة الجزائرية ما لم يكن قد طلب استرداده أو قبل طلب الاسترداد.

3- ربيعي حسين، **آليات البحث والتحقيق في الجرائم المعلوماتية**، رسالة دكتوراه، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2016، ص.227.

4- محمد سعيد نمور، **أصول الإجراءات الجزائية شرح لقانون أصول المحاكمات الجزائية**، الطبعة الأولى، الأردن: دار الثقافة، 2005، ص.345.

5- عائشة بن قارة مصطفى، **حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن**، دون طبعة، الأزاريطة: دار الجامعة الجديدة، 2010، ص 84.

6- المرجع نفسه، ص ص: 86، 87.

7- حكيم سياب، **الإعلام الآلي والقانون**، الطبعة الأولى، الأردن: دار وائل، 2014، ص 144.

8- علي عدنان الفيل، **إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية – دراسة مقارنة-**، دون طبعة، الأردن: المكتب الجامعي الحديث، 2012، ص 43.

9- أحمد شوقي الشلقاني، **مبادئ الإجراءات الجزائية في التشريع الجزائري**، الجزء الثاني، الطبعة الثانية، الجزائر: ديوان المطبوعات الجامعية، 1999، ص40.

10- عبد الله أوهايبية، **شرح قانون الإجراءات الجزائية الجزائري- التحري و التحقيق-**، دون طبعة، الجزائر:دار هومة،2008،ص 366.

11- لد عياد الحلبي، **إجراءات التحري و التحقيق في جرائم الحاسوب و الأنترنت**، الطبعة الأولى،عمان:دار الثقافة ،2011،ص169.

12- شيدة بوكر، **جرائم الإعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري والمقارن**، الطبعة الأولى، بيروت: منشورات الحلبي الحقوقية،2012، ص422.

13- ضياء علي أحمد النعمان،**الغش المعلوماتي الظاهرة و التطبيق**، الطبعة الأولى، مراكش : المطبعة الوطنية،2011، ص 380.

14- محمد أمين البشري، **التحقيق في الجرائم المستحدثة**، الطبعة الأولى،الأردن: دار الحامد،2014،ص ص :123، 124.

15- نزيهة مكاري، **وسائل الإثبات في جرائم الإعتداء على حق المؤلف عبر الأنترنت**،مجلة المناهج القانونية، دون ذكر هيئة النشر،عدد مزدوج 13-14 ،المملكة المغربية،2009،ص75.

16- حكيم سياب، المرجع السابق،ص152.

17- أحمد شوقي الشلقاني، المرجع السابق، ص 259.

18- أنظر أكثر تفصيلا: رشيدة بوكر، المرجع السابق، ص .330 وما بعدها.

19- أنظر : حاحة عبد العالي، **الاليات القانونية لمكافحة الفساد الاداري في الجزائر**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة بسكرة، 2013/2012، ص.268 وما بعدها

20- حاحة عبد العالي، المرجع السابق، ص.259.

21- رشيدة بوكر، المرجع السابق، ص370.

22- سعيداني نعيم،**آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري**، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر-باتنة-،2013، ص90.

23- يوسف حسن يوسف، **الجرائم الدولية للانترنت**، الطبعة الأولى:القاهرة:المركز القومي للإصدارات القانونية،2011،ص152.