وزارة التعليم العالي والبحث العلمي
جامعة قاصدي مرباح ورقلة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة بعنوان:

الـــــــــــدليل الرقمي و الإثبـــــــــــات الجنائي

مقدمة لاستكمال متطلبات الحصول على شهادة الماستر في الحقوق

تخصص قانون جنائي وعلوم جنائية

من اعداد الطلبة:

جليلة بلعلمي

صالح مزري

اشراف الأستاذ:

أ.د محمد عمران بوليفة

أعضاء لجنة المناقشة

اسم ولقب الأستاذ	الرتبة العلمية	الجامعة	الصفة
أحمد خديجي	أستاذ محاضر أ	جامعة ورقلة	رئيساً
محمد عمران بوليفة	أستاذ محاضر أ	جامعة ورقلة	مشرفاً ومقرراً
محمد بكرار شوش	أستاذ محاضر أ	جامعة ورقلة	مناقشاً

السنة الجامعية: 2022/2021

وزارة التعليم العالي والبحث العلمي
جامعة قاصدي مرباح ورقلة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة بعنوان:

الـــــــــــدليل الرقمي و الإثبـــــــــــات الجنائي

مقدمة لاستكمال متطلبات الحصول على شهادة الماستر في الحقوق

تخصص قانون جنائي وعلوم جنائية

من إعداد الطلبة:

جليلة بلعلمي

صالح مزري

اشراف الأستاذ:

أ.د. محمدعمران بوليفة

أعضاء لجنة المناقشة

اسم ولقب الأستاذ	الرتبة العلمية	الجامعة	الصفة
أحمد خديجي	أستاذ محاضر أ	جامعة ورقلة	رئيساً
محمد عمران بوليفة	أستاذ محاضر أ	جامعة ورقلة	مشرفاً ومقرراً
محمد بكرار شوش	أستاذ محاضر أ	جامعة ورقلة	مناقشاً

السنة الجامعية: 2022/2021

كلمة شكر

الحمد لله حمدا كثيرا

والصلاة والسلام على سيدنا محمد خاتم الأنبياء والمرسلين

نتقدم بأسمى عبارات الشكر والاحترام لأستاذنا الفاضل

الأستاذ محمد عمران بوليفة على ما قدمه لنا من حسن

توجيه وارشاد وعلى ملاحظاته القيمة لإنجاز هذا العمل

كما نتقدم بجزيل الشكر والتقدير لأعضاء لجنة المناقشة

كما نشكر كل من ساعدنا في إنجاز هذا العمل من قريب أو بعيد

إهداء

إلى الوالدين العزيزين

إلى كل الأهل والأقارب والأصدقاء

إلى كل من ساعدني في إنجاز هذا العمل المتواضع

سواء كان من قريب أو من بعيد

بلعلمي جليلة

إهداء

إلى الوالدين العزيزين

إلى كل الأهل والأقارب والأصدقاء

إلى كل من ساعدني في إنجاز هذا العمل المتواضع

سواء كان من قريب أو من بعيد

مزري صالح

قائمة المختصرات

باللغة العربية

- ج. ر.ج.ج: الجريدة الرسمية للجمهورية الجزائرية
- ص: الصفحة
- ص. ن: الصفحة نفسها
- ف: الفقرة
- ع: العدد
- م: المجلد
- د.ط: دون طبعة
- د.د.ن: دون دار النشر
- د.س.ن: دون سنة النشر
- ق. إ. ج: قانون الاجراءات الجزائية
- ق. ع: قانون العقوبات
- ق.ن: القانون نفسه

مقدمة

دخلت البشرية منذ مطلع الألفية الثالثة مرحلة جديدة من مراحل تطور العلم والتكنولوجيا في كل مجالات الحياة، وكان التطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات والاتصال، والاندماج المذهل الذي حدث بينهما فيما بعد، المحور الأساسي الذي قامت عليه الثورة المعلوماتية.

تلك الثورة العلمية بقدر ما كانت مفيدة للبشرية بفضل ما حققته الشبكات المعلوماتية من مزايا لا يمكن إنكارها على مستوى جميع الأصعدة، من حيث توفير الجهد والوقت وحتى المال، جعلت حياة الإنسان أكثر سهولة ويسر، إلا أنها فتحت مجال آخر لمخاطر لا يمكن الاستهانة بها، فانعكست بصورة سلبية على البشرية، من خلال ظهور أنماط جديدة من الجرائم، لم يكن متعارف عليها من قبل اصطلح على تسميتها بالجرائم معلوماتية، أو ما يسمى بالجرائم الإلكترونية.

إن الجرائم الإلكترونية المستحدثة خرجت عن المألوف في الجرائم التقليدية، كون أن مسرح ارتكابها ليس كبقية مسارح ارتكاب الجريمة التقليدية، فهو غير ملموس وغامض يحتاج لمعرفة كبيرة بواقعه، بالإضافة إلى أن مرتكبي الجرائم المعلوماتية ليسوا كغيرهم من المجرمين، فهم أشخاص متميزين متفوقين ذو مستوى علمي وثقافي مرموق في الغالب، يمتلكون تكوينا عاليا ولا ربما شهادات جامعية مميزة فهم من نخبة المجتمع، زد على ذلك أن الإجرام المعلوماتي لا تحده حدود ولا تأثر عليه بعد المسافات.

ونظرا لخطورة الجرائم الالكترونية وتنوعها وخصوصيتها جعلت من الإجراءات التقليدية لمكافحة الجريمة بصفة عامة عاجزة عن اكتشاف هذا النوع المستحدث من الجرائم، وملاحقة مرتكبيها في حالة اكتشافها، فهي إجراءات لا تتوافق مع مسرح الجريمة الإلكترونية، ولا مع دهاء وفطنة مرتكبها، الأمر جعل مختلف التشريعات من بينهم المشرع الجزائري يستحدثون إجراءات استثنائية ووسائل اثبات حديثة تواكب التطور الذي شهدته الجريمة الإلكترونية، مما استوجب تحول الدليل الجنائي من صورته التقليدية إلى الرقمية الحديثة.

فأصبح من الضروري على جهات التحقيق الاعتماد على النوع الجديد من الأدلة الجنائية في مجال الإثبات الجنائي، والتي تعرف بالأدلة الجنائية الرقمية التي تكشف ستر هذا النوع من الجرائم، بطرق ووسائل علمية حديثة يمكنها فك رموزه، وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة، تصلح أن تكون أدلة إثبات لهذه الجرائم، ذات الطبيعة الفنية والعلمية، ومن ثم نسبتها إلى فاعليها ومرتكبيها.

ويعد موضوع الأدلة الجنائية من المواضيع ذات الأهمية البالغة في الإثبات الجنائي، ووسيلة لإسناد الواقعة الإجرامية للمتهم أو نفيها عنه، فهو يكتسي أهمية في جميع مراحل الدعوى العمومية وبه تعرف الحقيقة.

من هنا تبرز قيمة هذا الموضوع من خلال أن له صلة وثيقة بطائفة جديدة من الجرائم ظهرت مع التطور التكنولوجي بغرض اكتشاف ومكافحة هذا النوع المستحدث من الجرائم، فالقضاء الجنائي وجد نفسه أمام هذا الدليل المستحدث، بما يفرضه من تحديات جديدة على القاضي الجنائي، بالإضافة إلى أن موضوع الدليل الرقمي في الإثبات الجنائي يعالج نوعا جديدا من الأدلة الجنائية من ناحيتين الفنية والقانونية، ومن جهة أحرى تناول هذا الموضوع أحد الوسائل العلمية التي جاءت لتواكب الفكر الاجرامي الحديث، وكان على المشرع حتميا أن يستحدث ما يلائم هذا النوع من الجرائم، فضلا عن انشاء أجهزة فنية يناط بها عملية الإثبات العلمي والفني.

ومن الأسباب التي دفعت للبحث في هذا الموضوع كون أن ظاهرة الجريمة الإلكترونية ظاهرة جديدة، بدأت في الانتشار في الآونة الأخيرة بشكل ملفت للانتباه وتعتبر من المواضيع الشائكة والمعقدة التي تشغل فقهاء القانون، الأمر الذي أدى إلى الرغبة في إثراء الدراسات الجامعية. بالإضافة إلى معرفة مدى مواكبة القانون للتطور التكنولوجي، وكيفية التعامل مع الأدلة الحديثة، لاسيما الدليل الرقمي من طرف جهات التحقيق والقاضي الجنائي، والكشف عن مدى حجيته وقوته الثبوتية في مجال الاثبات الجنائي.

ويقتضي موضوع الدراسة بالنظر الى الطبيعة الخاصة التي يتميز بها الدليل الرقمي وما قد يصاحب الحصول عليه من تعقيدات، والاخذ به وقبوله في الاثبات الجنائي، الوقوف على كيفية التعامل مع الدليل الالكتروني بالدقة المطلوبة من الناحية التقنية والقانونية والاجرائية، التي يجب اتباعها للحصول على الدليل الالكتروني، وفحص مدى مشروعية الاخذ به كوسيلة اثبات جنائية، وتأثيره على قناعة القاضي الجنائي خاصة في غياب النصوص التشريعية التي تنظمه، والكشف عن مدى حجيته وقوته الثبوتية في مجال الاثبات الجنائي.

ولعل اهم الصعوبات التي واجهتنا في إعداد هذا البحث هو أن الموضوع حديث لم تسبق دراسته على نطاق واسع، رغم وجود مجموعة من المقالات والمراجع التي عالجت هذا الموضوع ولكن بشكل جزئي، أي دون تناول كل جوانبه، ونقص المراجع التي تتناوله وبالأخص الجزائرية منها

ومما سبق ذكره، تهدف دراستنا لهذا الموضوع إلى معرفة الأدلة الجنائية، وإبراز دورها في عملية الإثبات الجنائي، ومدى فعاليتها في إثبات الجريمة الالكترونية المستحدثة، وتأثيرها على قناعة القاضي الجنائي ومدى قبوله كدليل علمي يفرض نفسه بقوة حجيته وقطعيته في الاثبات.

هذا ما يقود إلى التساؤل حول طرق استخلاص الدليل الرقمي في مجال الإثبات الجنائي وتأثيره على حرية اقتناع القاضي؟

إن الإشكالية المطروحة أعلاه تدل على مدى عمق الموضوع وتشعبه كونه يجمع بين مجالين متباعدين نظريا وهما موضوع التكنولوجيا المعلوماتية ومجال القانون ونظرية الاثبات الجنائي.

ومن أجل الإحاطة بكل جوانب الموضوع اعتمدنا على المنهج الوصفي من خلال إبراز إجراءات الحصول عليه واستخلاصه من البيئة الرقمية، كذا شروط قبوله، بالإضافة

إلى المنهج التحليلي بمناقشة ما يحتاجه الدليل الرقمي لجمع الحقائق والبيانات، والتعرض إلى مدى تأثيره على اقتناع القاضي الجنائي، وفي بعض الأحيان يتدخل المنهج المقارن من أجل المقارنة بين مختلف النظم والتشريعات.

إن الإحاطة بكل جوانب الموضوع والإجابة على إشكالية بإعمال المناهج المذكور آنفا تفرض تقسيم البحث إلى فصلين:

(الفصل الأول) إجراءات الاستخلاص الدليل الرقمي وشروط قبوله

(الفصل الثاني) حجية الدليل الرقمي في الإثبات الجنائي

الفصل الأول

إجراءات استخلاص الدليل الرقمي وشروط قبوله

نظرا لخطورة الجريمة الالكترونية في حد ذاتها، لكون محلها مجموعة معطيات هي عبارة عن ذبذبات الكترونية يصعب على الجاني القيام بعمل اجرامي دون ترك آثار، ودون ان يستغرق هذا العمل وقتا طويلا، وهو ما يجعلها صعبة الاكتشاف والاثبات، الأمر الذي أدى الى ظهور مشكلات إجرائية أثناء التحقيق، وأمام القاضي الجزائي عند الفصل في الدعوى المعروضة أمامه كونها حديثة النشأة، ولا يمكن تطبيق النصوص التقليدية عليها، لذلك عمد المشرع إلى وضع قواعد إجرائية لاستخلاص جميع الأدلة التي يمكن بها إدانة المتهم أو تبرأته من الجرم المنسوب اليه.

إن صعوبة إثبات الجرائم الالكترونية يرجع إلى الطبيعة الخاصة للدليل الرقمي، فهو ليس بدليل مرئي يمكن فهمه من بمجرد القراءة، إلى جانب صعوبة الوصول إليه واستخلاصه، وهذا نتيجة قيام كبرى المواقع العالمية الإلكترونية بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية الفنية، لمنع التسلل والوصول إليها، لتدميرها أو تبديلها أو الاطلاع عليها أو نسخها، كما يمكن للمجرم زيادة صعوبة عملية ضبط أي دليل يدينه من خلال استخدامه كلمات المرور بعد تخريب الموقع مثلا، أو استخدامه لتقنيات التشفير...إلخ.

لذلك لم تكتف التشريعات الحديثة بحماية معطيات الحاسب الآلي بصفة عامة من خلال تجريم صور الاعتداء عليها أي الحماية الموضوعية، إنما وضعت مجموعة من الإجراءات الاستثنائية الخاصة باستنباط واستخلاص الأدلة الرقمية منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الخاصة بالمعطيات ومنها لا يطبق الا على الجريمة المعلوماتية ولذلك سنحاول التطرق في هذا الفصل لإجراءات لاستخلاص الدليل الرقمي (المبحث الأول) ثم شروط قبوله (المبحث الثاني).

المبحث الأول: إجراءات استخلاص الدليل الرقمي

انتهجت السياسة الجنائية الحديثة عدة طرق وأساليب إجرائية للوقاية من الجريمة وقمعها والجريمة الرقمية من بين هذه الجرائم التي يتطلب التحقيق فيها من حيث ثبوت التهمة، ونسبتها إلى المتهم من عدمه واستخلاص الدليل إلى إجراءات يخرج تنفيذها عن نطاق مكتب التحقيق أو ما تستخلصه محاضر الضبطية القضائية، بل يستلزم الأمر في

بعض الجرائم الانتقال لإجراء معاينات مادية وعمليات تفتيش وضبط، وهي نفس الإجراءات المتبعة في الجرائم التقليدية.

كما أن عملية الحصول على الدليل الرقمي أمر صعب الوصول إليه لما يتطلب من خبرة ومهارة كبيرة في مجال التكنولوجيا الرقمية، بالإضافة إلى تعدد صور وأشكال الجريمة المعلوماتية وسرعة تنفيذها، وللحصول على هذا النوع من الأدلة الجنائية يجب إتباع طرق ووسائل فنية وإجرائية حديثة رسمها القانون لاستخلاصها.

المطلب الأول: الإجراءات التقليدية لاستخلاص الدليل الرقمي

إن عملية البحث والتحري والتحقيق في الجرائم بصورتها التقليدية يختلف اختلافا جذريا عن الجرائم التي ترتكب في العالم الافتراضي أو الرقمي، لأنها لا تخلف آثار مادية محسوسة في مسرح الجريمة لذلك سنبين في هذا المطلب صلاحية الإجراءات التقليدية في استخلاص الأدلة الجنائية الرقمية التي أثارت جدلا فقهيا كبيرا، وسنكتفي بدراسة الإجراءات التقليدية المتمثلة في المعاينة والتفتيش والخبرة لعلاقتها المباشرة بالدليل الجنائي الرقمي.

الفرع الأول: الانتقال والمعاينة في الجرائم الرقمية

تعتبر المعاينة من أهم إجراءات التحقيق في اثبات الواقعة الاجرامية فهي تعبر على الوقائع والحقيقة تعبيرا صادقا، إذ تمكن المحقق من تصور كيفية وقوع الجريمة وظروفها وملابسات ارتكابها.

لم تعرف أغلب التشريعات المقصود بالانتقال والمعاينة وترك ذلك للفقه لتعريفهما فعرفها البعض على أنها اجراء بمقتضاه ينتقل المحقق الى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة، وكيفية وقوعها وكذلك جميع الأشياء الأخرى التي تفيد في كشف الحقيقة واتخاذ ما يلزم من إجراءات كضبط بعض الاشياء[1].

كما عرف جانب آخر من الفقه على أنها " الكشف الحسي المباشر والمادي لإثبات حالة الشيء أو المكان او الشخص وكل ما يفيد في كشف الحقيقة "[2].

1مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، ج1، دار النهضة العربية، القاهرة، 2000، ص 642.

(2)نفس المرجع، ص 643.

وللمعاينة هدفين اثنين الأول جمع الأدلة الناتجة عن الجريمة (الأثار) والثاني إتاحة الفرصة للمحقق لكي يشاهد بنفسه مكان وقوع الجريمة حتى تكون لديه فكرة واضحة لا لبس فيها ولا غموض عن كيفية وقوع الجريمة[1].

ولقد أشارت القوانين الجنائية إلى إجراء المعاينة باعتبارها إجراء من إجراءات التي تمتلكها سلطات التحقيق، وهذا ما ورد في نص المادة 79 من ق إ ج التي تنص يجوز لقاضي التحقيق الانتقال إلى مكان وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها...[2]

والمعاينة في الجرائم المعلوماتية هي معاينة الآثار التي يخلفها مستخدم الشبكة المعلوماتية أو الانترنيت وتشمل الرسائل المرسلة منه أو التي استقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر والشبكة العالمية.

أولا/ محل المعاينة في الجريمة الرقمية:

يعتبر مكان ارتكاب الجريمة الوعاء الأساسي الذي يحتوي على أخطر الأدلة الجنائية التي يخلفها الجاني وراءه اثناء ارتكابه للجريمة، والمعاينة في الجرائم التقليدية تتم على مسرح الجريمة المادي فإن المعاينة في الجريمة المعلوماتية تتم على مستويين:

أ. المسرح التقليدي: وهو المسرح الذي يقع عادة خارج بيئة الحاسوب ويتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة وهو قريب من مسرح الجريمة التقليدية ومن أمثلة هذه الجرائم الواقعة على أشرطة الحاسب والكابلات الخاصة به ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسب الآلي ذات الطابع المادي المحسوس.

ب. المسرح الافتراضي: ويقع عادة داخل البيئة الالكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله، وفي

1 محمد حماد مرهج الهيتي، جرائم الحاسوب، دار المناهج، عمان، ط 1، 2006، ص 256.

2 أنظر المادة 79 من الأمر رقم 66 . 155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية الجزائري، ج ر ج ج ، ع 48 صادرة بتاريخ 11 جوان 1966 المعدل والمتمم.

مقدمتها الجرائم الواقعة على برامج الحاسب الآلي أو بياناته أو التي تتم بواسطتها، وكذلك الجرائم التي تتم بطريق الانترنيت ومنها جرائم التزوير المعلوماتي والتخريب[1].

وتختلف أشكال المعاينة في الجرائم المعلوماتية بحسب نوعية الجريمة المرتكبة، على أن هناك طرق عامة تتوافق مع طبيعة الاتصال بالأنترنيت أو الوسيلة المستخدمة مثلا: وسيلة تصوير شاشة الحاسوب التي تكون بواسطة آلة تصوير تقليدية عن طريق استخدام برمجة حاسوب متخصصة في أخذ صورة لما يظهر على الشاشة، وهذا ما يصطلح عليه تجميد مخرجات الشاشة وغيرها[2].

ثانيا/ إجراءات معاينة مسرح الجريمة الرقمية

تختلف إجراءات المعاينة في الجرائم الرقمية عن الجرائم التقليدية بالنظر لخصوصية الجريمة، ويقوم المحقق باتباع بعض القواعد والارشادات الفنية عند معاينة مسرح الجريمة المعلوماتية وتتمثل هذه الإجراءات في:

عند العثور على حاسبات آلية أو أجهزة أخرى داخل مسرح الجريمة يجب عدم العبث بها وتدوين الحالة التي هي عليها إذا كانت مطفأة، أو في حالة تشغيل موصولة بالكهرباء أو بجهاز لاحق آخر، كما ينبغي ترقيم لواحقها بشكل متسلسل.

يجب تحرير الأوراق المطبوعة على الحاسب الآلي والتي عثر عليها في مسرح الجريمة ووضعها في أكياس حسب حالتها ويمكن إعادة الطباعة إذا كان الجهاز في حالة تشغيل وتحرير الأوراق التي تمت طباعتها بالإضافة الى تفقد الجهاز وتسجيل ما إذا كانت هناك برامج تم استخدامها لحظة دخول مسرح الجريمة[3].

وعند العثور على دعائم التخزين (أسطوانات، أقراص، حوامل مغناطيسية) يجب ترقيمها وتسجيل الحالة التي هي عليها والمكان الذي وجدت فيه (داخل الحاسب الآلي أو خارجه) ثم يتم تصوير الأجهزة وملحقاتها في الحالة التي هي عليها.

1 عبد الفتاح بيومي حجازي، المرجع السابق، ص 164.

2 نبيلة هبة هروال، الجوانب الإجرائية لجوانب الانترنيت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2013، ص 212.

3 محمد امين احمد الشوابكة، جرائم الحاسوب والانترنيت، ط 1، دار الثقافة للنشر والتوزيع، عمان، 2004، ص 122.

وفي الأخير تقوم فرقة البحث والتحري بتحرير جميع العينات التي عثر عليها من أجهزة ودعائم داخل أكياس خاصة (بلاستيكية أو ورقية) كما ينبغي حمايتها من الكسر وتأثير العوامل الجوية وابعادها عن أي مجال مغناطيسي لتفادي فقدان المعلومات وارسالها الى المخبر لإجراء الخبرة.

وتقتضي القاعدة العامة أن تكون هناك استعانة بالخبراء في المسائل العلمية والتقنية التي تحتاج إلى إجراء خبرة، ويحتاج خبراء الأدلة الجنائية الرقمية لتأدية أعمالهم التقنية واكتشاف المعلومات التي يحتويها كل دليل، أخذه الأجهزة والأنظمة والبرمجيات ما يلي:

أجهزة بقدرة عالية على التحليل وتخزين المعطيات.

نسخ من مختلف أنظمة التشغيل المستعملة لدى الافراد والمؤسسات، نسخ من برامج حذف وكسر كلمات المرور لمختلف الحاسبات، برامج نسخ الأقراص المدمجة والمحمولة، برامج الضغط وفك الضغط، برامج التشفير وفك التشفير، برامج حماية الأنظمة والشبكات من الاختراق، برامج كشف الأجهزة المخفية من الأقراص الصلبة، برامج استعادة الملفات المحذوفة وبرامج البحث عن الانترنيت.

قصر المعاينة على الباحثين والمحققين الذين لديهم كفاءة علمية وخبرة فنية في مجال الحاسوب والشبكات واسترجاع المعلومات، ولن يكونوا قد تلقوا تدريبا جيدا على التعامل مع نوعية الآثار والأدلة التي يتضمنها مسرح الجريمة المعلوماتية[1].

ويحرر محضر المعاينة عن طريق كاتب، ويجب عند اجرائها اخطار الخصوم بمكان المعاينة وزمانها ويتم توثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد مع توثيق كل دليل على حدى بما فيها الأدلة الرقمية بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها ومن قام برفعه وتحريزه.

1 حسين بن سعيد الغافري، التحقيق، جمع الأدلة في الجرائم المتعلقة بشبكات الانترنيت، موقع المنشاوي للدراسات والبحوث على الموقع WWW.minshawi.com اطلع عليه بتاريخ 11-02-2018، ص 10.

وقد أجاز المشرع الجزائري المعاينة في الجرائم المعلوماتية المتلبس فيها بنص المادة 3/47 من قانون الإجراءات الجزائية والتي تنص على أنه عندما يتعلق الأمر بالجرائم الخاصة بأنظمة المعالجة الآلية للمعطيات يجوز اجراء المعاينة في كل محل سكني أو غير سكني وفي كل ساعة من ساعات النهار والليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص[1].

الفرع الثاني: التفتيش في الجرائم الرقمية

يعتبر إجراء التفتيش من أهم إجراءات التحقيق التي تفيد في الكشف عن الحقيقة، ومن أخطرها على الحياة الخاصة، وبالرجوع للمشرع الجزائري نص على ذلك بمقتضى قواعد دستورية[(2)]، ولعدم انتهاك حرمة منزل فلا تفتيش الا بمقتضى القانون وفي إطار احترامه فلا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة، هذا وبالإضافة إلى نصوص قانون الإجراءات الجزائية والقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

ويعرف الفقه التفتيش على أنه البحث المادي في مكان ما بهدف البحث عن الأشياء المتعلقة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها[3].

ويمكن أن نعرفه بأنه إجراء من إجراءات التحقيق تقوم به سلطة خول لها القانون ذلك بالبحث الدقيق عن أدلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة. إلا أن ذلك يتنافى مع الطبيعة المادية للدليل الجنائي الرقمي وهذا ما يجعلنا نطرح التساؤل حول إمكانية تطبيق القواعد العامة للتفتيش على صور التفتيش في الجريمة المعلوماتية.

1 صالح شنين، الحماية الجنائية للتجارة الالكترونية، أطروحة لنيل شهادة الدكنوراه في القانون الخاص، جامعة أبو بكر بلقايد تلمسان، كلية الحقوق، الجزائر، 2013.

2 المادة 40 من الدستور الجزائري لسنة 1996

3 محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة للطباعة والنشر، 2009، ص 91.

أولا: خضوع أنظمة الحاسب الآلي للتفتيش

إن الغرض من التفتيش هو البحث عن الأدلة المتعلقة بالجريمة التي تساعد في كشفها والتفتيش في الجريمة الالكترونية، ينقسم إلى تفتيش ماديات الجريمة الملموسة، والتفتيش في نظم الحاسوب غير الملموسة والتي تخضع لقواعد شكلية وأخرى موضوعية

ومن أهم القواعد الشكلية لتفتيش في نظم الحاسوب والانترنيت هو أن يخضع التفتيش في هذه الحالة للخصائص العامة لكافة إجراءات التحقيق المتمثلة في وجوب التدوين بمعرفة كاتب والسرية عن الجمهور وحضور الخصوم ووكلائهم إذا أمكن ذلك.

غير أن التفتيش في الجريمة المعلوماتية يختلف عن غيرها من الجرائم الأخرى، إذ يجب أن تتوفر الخبرة الفنية لدى القائم بالتفتيش من خلال تلقي المحقق تدريبات فنية خاصة تعرفه كيفية التعامل مع التقنية الحديثة وكيفية ضبط الأدلة والحفاظ عليها، كذلك يجب ان يتم التفتيش بصورة صحيحة من الناحيتين الموضوعية والشكلية[1].

ومن بين القواعد الشكلية التي تحكم إجراءات التفتيش عدم التجاوز في التفتيش وذلك بمنع التفتيش عندما لا توجد تحريات جدية تنبئ عن وجود دلائل قوية عن معلومات تفيد في كشف الحقيقة مع وجوب ان يكون التفتيش في حدود الاذن المكتوب المؤرخ والموقع من الجهة التي أصدرته وإلا كان التفتيش باطلا.

ويجب ان يكون إذن التفتيش محدد المدة التي تحتسب من يوم الإذن إلى الجهة المأذون لها إجراء التفتيش[2].

والمشرع الجزائري لم يوضح بدقة هذه الإجراءات الشكلية، وترك ذلك لأحكام القانون 09-04 والذي بدوره اخضعها للقواعد العامة المنصوص عليها في المادة 44 وما يليها من قانون الإجراءات الجزائية ومن بينها:

1 بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية ط 1، 2011، ص 105

2 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، ط 1، 2009، ص 223.

الحصول على اذن مكتوب صادر عن السلطات القضائية المختصة المتمثلة في وكيل الجمهورية أو قاضي التحقيق، حسب الحالة وضرورة استظهاره قبل الدخول إلى المسكن والقيام بعملية التفتيش.

غير أن القانون 09 -04 نص بضفة عامة على ضرورة إعلام جهات التحقيق السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة حاسوبية أخرى، ونص على أن تفتيش رجال الضبطية القضائية لنظم الحواسيب يكون بناء على قواعد ق ا ج التي تفرض عليهم عند الانتقال لتفتيش مساكن الأشخاص المشتبه في ارتكابهم أفعال جنائية أن يكون مصحوبين بإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهاره قبل الدخول إلى المنزل والشروع في التفتيش طبقا للمادة 05 من القانون 09-04.

ويجب أن يكون إذن التفتيش مسببا أي أن يتضمن سبب إصداره وتظهر أهمية ذلك في تقييد سلطة الجهة القضائية المختصة التي وجب عليها إثبات مبررات اللجوء إلى إجراء التفتيش لما فيه من مساس بحريات الأشخاص وتمكين الجهة القضائية من بسط رقابتها على المبررات التي استندت إليها السلطة المختصة في إصدار الأمر[1].

كما يجب أن يتضمن الإذن بالتفتيش وصف الجرم الذي يجري التفتيش بشأنه من أجل البحث عن دليل فيه، وكذا عنوان المسكن الذي سيتم فيه عملية التفتيش تحت طائلة البطلان.

وينص قانون الإجراءات الجزائية في المادة 1/45 على وجوب حضور صاحب المسكن عملية التفتيش أو تعيين من يمثله أو حضور شاهدين يتم تسخيرهما من طرف ضابط الشرطة القضائية، ونظرا للطابع الخاص بالجريمة المعلوماتية أجاز المشرع التفتيش دون حضور صاحب الحق على المسكن أو من ينوبه ودون تسخير شاهدين في حال ما إذا كان هاربا، وذلك بفرض الإسراع في استخلاصه، أما إذا كان المشتبه فيه محجوز للنظر أو محبوس في مكان آخر ويتعذر نقله لأسباب أمنية أو لمقتضيات النظام العام أو وجود خطر اختفاء الأدلة خلال مدة نقله لمكان إجراء التفتيش فإنه في هذه الحالات يجوز إجراء التفتيش

1 ثابت دنيازاد، مراقبة الاتصالات الالكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والانسانية جامعة تبسة، العدد 6، 2012، ص 87.

من دونه ولكن بحضور شاهدين خاضعين لسلطة ضابط الشرطة القضائية[1] ، وهذا من أجل الحصول على الدليل المستهدف من عملية التفتيش في الوقت المناسب.

ولعملية التفتيش وقت قانوني حدده المشرع الجزائري في قانون الإجراءات الجزائية من الساعة الخامسة صباحا الى الساعة الثامنة مساء غير أنه ونظرا لطبيعة الجرائم المعلوماتية وسرعة إتلاف وتعديل المعطيات خاصة إذا علم الجاني بوجود تفتيش قد يؤدي إلى محو الأدلة أجاز المشرع في المادة 47 فقرة 03 من ق ا ج التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في أي ساعة من ساعات النهار أو الليل بناء على إذن مسبق من وكيل الجمهورية، وهنا فإن المشرع غلب المصلحة العامة على المصلحة الشخصية للأفراد نظرا لذاتية الجريمة المعلوماتية المتمثلة في إمكانية اختفائها بسرعة ومن جهة أخرى افتراض كون الدليل الرقمي هو الدليل الوحيد في الدعوى الجزائية ومن ثم ارتكاز كل العملية الاثباتية على وجوده[2] .

ومن أهم القواعد الموضوعية التي يجب مراعاتها أثناء مباشرة عملية التفتيش في نظم الحاسوب هو ضرورة وجود سبب للتفتيش، فلا يصح إصداره إلا لضبط ماديات الجريمة الواقعة بالفعل وإتهام شخص أو عدة أشخاص بارتكابها أو المشاركة فيها، سواء كانت جنحة أو جناية فمن غير الممكن القيام بالتفتيش دون وقوع جريمة، وذلك مع توافر دلالات وامارات قوية على وجود أجهزة وأدلة معلوماتية تفيد في كشف الحقيقة.

وبالرجوع إلى محل التفتيش في الجريمة التقليدية نجد أنه ينصب على شخص المتهم أو غير المتهم وعلى مسكنه وما في حكمه وملحقاته، غير أن المحل التفتيش في الجريمة المعلوماتية هو جهاز الحاسوب وشبكة الانترنيت محلا للاعتداء، وليس وسيلة لارتكاب الجريمة فحسب، فيقع التفتيش على الأشياء المادية وبرامج الحاسب الآلي و بياناته أي كل ما يحتويه وكل ماله علاقة بالجريمة من أجهزة الحاسوب و الآلات والنظم والبرامج والأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش، ونظرا لإمكانية قيام الجاني

1 احسن بوسقيعة، التحقيق القضائي، دار هومة للطباعة والنشر، الجزائر، ط 10، 2013.

2 جولحي عبد الستار، جرائم الحاسوب – دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري–مذكرة تخرج تدخل ضمن متطلبات الحصول على شهاد الماستر في العلوم الإسلامية، جامعة الشهيد حمه لخضر، كلية العلوم الاجتماعية والإنسانية، قسم العلوم الإنسانية الجزائر، 2015، ص 64.

بالتخلص من البيانات التي يستهدفها التفتيش عبر ارسالها من خلال نظام معلوماتي من مكان إلى آخر ارتباط شبكة الحواسيب ببعضها البعض فقد أجاز المشرع في المادة 05 من القانون 09-04 تمديد التفتيش بسرعة إلى منظومة معلوماتية أخرى أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك، وبالتالي فالتفتيش قد يقع على الأشخاص أو المساكن التي تحتوي على تلك الأجهزة أو الشبكات المعلوماتية[1]. ويحرر محضر يثبت فيه إجراءات التفتيش.

ثانيا: تفتيش المنظومة المعلوماتية

وتضم المنظومة المعلوماتية المكونات المادية للحاسب الآلي والمكونات المعنوية والشبكات المتصلة بالحاسوب عن بعد.

وتخضع المكونات المادية لنظام المعالجة الآلية للمعطيات لإجراءات التفتيش المنصوص عليها في المادة 44 من قانون الإجراءات الجزائية، أي أنه يجب مراعاة مكان وجود ذلك الحاسوب اثناء مباشرة الإجراء فيما إذا كان مكانا عاما أو خاصا، لأن تحديد المكان له أهمية خاصة في مجال التفتيش، فاذا كان موجودا في مكان خاص كمسكن المتهم فلا يجوز تفتيشه إلا في الحالات التي يجوز فيها تفتيش مسكنه، وبنفس الضمانات المقررة قانونا كما سبق بيانه، ويرد التفتيش على المكونات المادية للحاسب الآلي وملحقاته بما في ذلك البيانات المخزنة أو وسائل مادية كالأشرطة الممغنطة والأقراص الصلبة والضوئية.

أما عن التفتيش في المكونات المعنوية للحاسب الآلي التي تتمثل في أنظمة الكمبيوتر والبيانات المخزنة فيه والتي جرى التلاعب فيها أو تغييرها، وكذا الوسائط التي تساعد على تخزين المعلومات[2]، فالتفتيش في هذه المكونات أمر تفرضه طبيعة الجريمة المرتكبة للبحث عن الأدلة الجرمية وضبطها لأن الغاية من التفتيش هو الحصول على دليل خاص بالجريمة وكشف الغموض الذي أحاط بها[3].

1 خالد ممدوح إبراهيم، المرجع السابق، ص 222.

2 خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، ط 1، 2011، ص159.

3 عبد الفتاح بيومي حجازي، مرجع سابق، ص 159.

ويتضح موقف المشرع الجزائري من خلال النص في المادة 05 من القانون 09-04 على إجازة تفتيش المنظومات المعلوماتية وقد نصت على أنه " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المحزنة فيها وكذا منظومة تخزين معلوماتية.

أما عن تفتيش الشبكات المعلوماتية المتصلة بالحاسوب والتي تعرف بانها مجموعة مكونة من اثنين فأكثر من أجهزة الحاسوب والمتصلة ببعضها اتصالا سلكيا أو لا سلكيا وقد تكون الأجهزة موجودة في نفس الموقع، وتسمى بالشبكة المحلية أو قد تكون موزعة في أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف وتسمى بالشبكة بعيدة المدى[1]

والتفتيش في هذه الحالة على درجة من الخطورة تتعلق بالتفتيش عن بعد، نتيجة للطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أداة عبر شبكات حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش، وهو ما يزيد المسألة تعقيدا باعتبار أن الشبكة المعلوماتية ممتدة في أنحاء العالم.

ثالثا: بطلان التفتيش في الجرائم الرقمية

راعى المشرع في شأن قواعد التفتيش الموازنة بين حماية حريات الاشخاص وعدم المساس بحقهم في الخصوصية وعدم افشاء الأسرار[2]، وحصانة مساكنهم وبين المصلحة العامة في الكشف عن الحقيقة ولذلك على جهة التحقيق مراعاة القواعد الموضوعية والشكلية للقيام بالتفتيش حتى لا يترتب على ذلك البطلان.

وقد اختلف الفقه الجنائي في جعل قواعد البطلان من النظام العام من عدمه غير أن الراجح هو جعلها قواعد جوهرية يترتب على مخالفتها البطلان وهذا البطلان لا يتعلق بالنظام العام.

---

1 يتم الاتصال ونقل المعلومات بواسطة الشبكية بأشكال ثلاث هي:

احادي الجانب ويام بين جهاز الحاسوب المستفيد مع جهاز مركزي

اتصال ثنائي غير متكامل المعلومات و يتم بين جهازين يرسل الأول المعلومات و الثاني يستقبلها و بعد انتهاء الأول يقوم الثاني بإرسال المعلومات و يستقبلها الأول و هكذا، واتصال تنائي كامل المعلومات ويتم بين جهازي الارسال والاستقبال في نفس الوقت.

2 بكري يوسف بكري، مرجع سابق، ص 60.

الفرع الثالث: الضبط في الجرائم الرقمية

ان الأشياء المضبوطة في الجرائم المعلوماتية تكون ذات طبيعة معنوية فقد يرد ضبط الأشياء على عناصر معلوماتية منفصلة مثل الأسطوانات الممغنطة، وهنا لا يثور أي اشكال عند القيام بالضبط لكن الصعوبة تكون عندما يلزم ضبط النظام كله أو الشبكة كلها لأنها تحتوي على عناصر لا يمكن فصلها، إما بالنسبة للمكونات المادية للحاسوب فيمكن ضبط الوحدات المعلوماتية الآتية: وحدات الادخال (لوحة المفاتيح، الفأرة، نظام القلم الضوئي) وضبط وحدة الإخراج (الشاشة، الطابعة الرسم، المصغرات الفيلمية) وكل ما يتم ضبطه من بيانات الكترونية يتعين تحريرها و تأمينها فنيا[1].

ولقد نصت المادة 06 من القانون رقم 09-04 على أنه "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية..." و بالتالي فقد كان اتجاهه هو امكانية حجز المنظومة المعلوماتية برمتها بشروط كما حرص المشرع على جعل المعلومات محل البحث في مأمن باستخدام التقنيات اللازمة لمنع الوصول أليها، وذلك في حالة استحالة حجزها لأسباب تقنية كما لو كانت المعطيات مخزنة بأنظمة التشغيل التي لا يمكن نسخها وهو ما نصت عليه المادة 07 من القانون 09-04 وذلك لمنع تهريبها وتدميرها.

ومن خلال ما سبق نستخلص أن هناك نوعين من إجراءات الضبط تسمى الأولى بإجراءات مبدئية تحفظية الهدف منها هو الحفاظ على البيانات المخزنة التي تكون لها أهميتها في التحقيق ببقائها في مكانها في النظام المعلوماتي للكمبيوتر أو في دعامة التخزين ومنع الوصول إليها أو إلغائها أو التصرف فيها، وذلك للكشف عن مرتكب الجريمة وسهولة اثباتها، الثانية هي عبارة عن إجراءات لاحقة بالضبط ويقصد بها جميع البيانات

1 بوعناد فاطمة زهرة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، سيدي بلعباس، 2013، العدد 01.

سواء بأحد دعامة تخزين المعلومات أو أخذ نسخة من البيانات المخزنة بها أو بالنظام المعلوماتي للكمبيوتر في ورق أو أقراص.

وحدد المشرع الجزائري ضوابط حجز الأدلة في أحكام المادة 84 من قانون الإجراءات الجزائية التي تنص على أن الأحراز والوثائق المحجوزة لا يتم فتحها إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا، وبالتالي فالمشرع حافظ على مبدأين أساسين هما السرية وحقوق الدفاع، وهذا ما أكدته المادة 09 من القانون 09-04، كما أكدت على أن الاطلاع على المستندات المراد حجزها مخول فقط لقاضي التحقيق أو ضابط الشرطة القضائية الذي اناب عته قبل حجزها ووضعها في أحراز مختومة وحرر محضرا بضبطها

الفرع الرابع: الخبرة في الجرائم الرقمية

ترتكب الجريمة الالكترونية بوسائل مستحدثة ومعقدة صعب التعامل معها، فهي عبارة على قضايا ذات طابع فني وتقني تتطلب في غالب الأحيان إلى خبرة خاصة من ذوي الاختصاص، فلا يمكن تصور أن يرفض القاضي اللجوء الى نذب خبير في مثل هذا النوع من القضايا. ويكون حكمة مجانبا للمنطق العلمي ومعيبا إذا لم يستند إلى الخبرة التقنية في هذا المجال[1] تحقيقا لمبدأ عام يسمى مبدأ التخصص.

والخبرة ليست دليلا مستقلا عن الدليل المادي وإنما هي تقييم فني لهذا الدليل والعنصر المميز للخبرة عن غيرها من إجراءات الاثبات كالمعاينة والشهادة والتفتيش[2]

والخبرة في مجال المعلوماتية تكون بتحري الحقيقة عن طريق جمع المعلومات من الأدلة الرقمية وتحصيلها من خوادم الموقع ومن الجهاز المعتدى عليه بعد التوصل إلى تحديده ثم يقوم الخبير بعملية تحليل رقمي لها بمعرفة كيفية إعدادها البرمجي ونسبتها إلى

1 عادل عزام سقف الحيط، جرائم الدم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع، ط 1، 2011.

2 عبد الفتاح بيومي الحجازي، المرجع السابق، ص 321.

مسارها الذي أعدت فيه وتحديد عناصر حركتها ثم التوصل إلى معرفة بروتوكول الانترنيت للحاسوب الذي صدرت منه الرسائل والنبضات الالكترونية[1]

إن التحقيق في الجرائم الإلكترونية يستدعي في غالب الأحيان اللجوء إلى ذوي الخبرة من الفنيين والتقنيين لتقديم المساعدة اللازمة للقضاة أو المحققين في مجال الإثبات الجنائي لتكوين عقيدتهم نحو المسائل التي يحتاج تقريرها إلى معرفة فنية تقنية أو دراية علمية لا تتوفر لديهم.

فلا يمكن للقاضي الجزائي الاستغناء على تقرير الخبير عند التحقيق في الجرائم الإلكترونية فهو في حاجة دائمة إلى خبراء، ويمتد عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات، وكذلك إعداد البرمجيات وتشغيل الحاسب الآلي وعلومه، ونجاح أعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء، ويجب على المحقق الجنائي أن يحدد للخبير الالكتروني دوره في المسألة التي أنتدب من أجلها على وجه الدقة.

وهناك اسلوبان لعمل الخبير أولهما القيام بتجميع وتحصيل مجموعة المواقع التي تشكل جريمة في ذاتها كجريمة التهديد أو النصب وجرائم النسخ ...الخ، ثم يقوم الخبير بعملية تحليل رقمي لها، وذلك لمعرفة كيفية اعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها، وكيف تم التوصل إلى معرفتها وأخيرا التوصل لمعرفة برتوكول الانترنيت الذي ينسب إلى جهاز الحاسوب الذي صدرت عنه هذه المواقع[2].

أما الأسلوب الثاني يتمثل في القيام بتجميع وتحصيل مجموعة المواقع التي لا تشكل موضوعها جريمة في ذاته، ولكن الجرائم تقع من جراء تتبع موضوعات هاته المواقع، مثل المواقع التي تساعد الغير على معرفة جرعات المخدرات والمؤثرات العقلية حسب وزن الانسان بإيهامه أنه إذا تم تتبع التعليمات الواردة فيها لن يصل الشخص إلى حالة ادمان،

1 سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2012-2013، ص 171.

2 خالد ممدوح إبراهيم، مرجع سابق، ص 301.

كذلك الشأن بالنسبة لكيفية إعداد القنابل وتخزينها أو كيفية التعامل مع القنابل الزمنية... الخ[1] .

نظم المشرع الجزائري أعمال الخبرة في قانون الإجراءات الجزائية في المواد من 143 إلى 156 واعتبرها من إجراءات البحث عن الدليل بحيث نصت المادة 143 على أنه" لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة، أو من تلقاء نفسها أو من الخصوم "

كما أشارت المادة 05 منٌ قانون 04/09 الذي يتضمن القواعد الخاصة بالوقاية من جرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها. قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

المطلب الثاني: الإجراءات الحديثة لاستخلاص الدليل الرقمي

نتيجة التطور الحاصل في مجال التكنولوجيات الرقمية أصبح المجرمين أكثر ذكاء باستعمالهم لوسائل تقنية حديثة في مختلف الجرائم التي سهلت تنقلاتهم الإجرامية، والتي امتدت إلى خارج الحدود الوطنية لتشمل دول أخرى وتهدد أمنها واستقرارها، فأصبح من الصعب تتبع تحركات هاته الشبكات الإجرامية، الأمر الذي استوجب مواكبة التطور التكنولوجي، من خلال وضع وسائل وطرق إجرائية حديثة تتناسب مع الطبيعة التقنية للدليل الرقمي. مما استدعى المشرع الى التدخل لمكافحة هذا النوع من الجرائم عن طريق تعديل القانون رقم 06-22 المؤرخ في 2006/07/20 المتضمن قانون الاجراءات الجزائية، إذ أدخل أساليب البحث والتحري الخاصة التي تقوم بها جهات متخصصة بغية التحري في جرائم خطيرة مقررة في قانون العقوبات، كما استحدث المشرع القانون رقم 04/09 المؤرخ في 2008/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، وهذا ما سنتطرق اليه في دراستنا إلى صلاحية الإجراءات الحديثة في استخلاص الدليل الجنائي الرقمي فيما يلي:

1 خالد ممدوح إبراهيم، مرجع سابق، ص 301

الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

سعيا من المشرع لمكافحة الجرائم الخطيرة ومراقبة نشاطات الشبكات الاجرامية الذين يستعملون تقنيات حديثة تتسم بالسرعة والفعالية قام بإدخال الوسائل التقنية في مجال البحث والتحري في التحقيقات الجنائية الخاصة بهذه الجرائم، ولقد نظم المشرع الجزائري كل من اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في المواد من 65 مكرر 5 إلى غاية 65 مكرر 10ق ا ج ج بحيث يجوز لضباط الشرطة القضائية وأعوانهم القيام بهذه الاعمال إذا اقتضت ضرورة التحري في الجرائم المتلبس بها وفي بعض الجرائم الأخرى عن طريق إذن من وكيل الجمهورية أو قاضي التحقيق.

أولا: اعتراض المراسلات

لم يعرف قانون الإجراءات الجزائية اعتراض المراسلات واكتفى بتنظيمها في المواد المذكورة أعلاه، فقد عرفها الباب الثالث من القانون الفدرالي الامريكي لسنة 1968 انها الاكتساب السمعي عن طريق السمع لمحتويات أية أسلاك أو أية اتصالات شفوية عن طريق استخدام جهاز الكتروني أو ميكانيكي أو جهاز آخر وبصفة عامة فإن أي جهاز يمكن استعماله لتسجيل اتصالات يقع ضمن ما يقصده القانون[1].

وعرفها اجتماع لجنة الخبراء للبرلمان الاوربي بستراسبورغ بتاريخ 2006/10/06 المتعلق بأساليب التحري التقنية وعلاقتها بالأفعال الارهابية بأنها عملية مراقبة سرية للمراسلات السلكية واللاسلكية، في إطار البحث والتحري عن الجريمة وجمع الادلة والمعلومات حول الاشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجرائم.

ويمكن اعتراض المراسلات عن طريق وسائل الاتصال السلكية واللاسلكية ويقصد به التصنت التلفوني[2] ، أو ما يعرف بالتصنت على المكالمات وهو تقنية يتم من خلالها الاعتراض عن طريق ربط خط هاتفي لشخص ما مع اللجوء الى تسجيل المكالمات في أشرطة مغناطيسية.

1 حمزة قريشي، الوسائل الحديثة للبحث و التحري في ضوء القانون الجزائري، منشورات لسائحي، الجزائر، ط 1 ، 2017، ص 36.

2 احسن بوسقيعة، مرجع سابق، ص 113.

ويراد بها أيضا تلقي أية مراسلة مهما كان نوعها مكتوبة أو مقروءة أو مسموعة وبغض النظر عن وسيلة ارسالها وتلقيها سواء كانت سلكية أو لاسلكية من الشخص الموجه إليه أو الذي أرسلها[1] .

واعتراض المراسلات هو اجراء من إجراءات التحقيق يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطات القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها، ويتضمن استراق السمع وحفظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض.

وهنا يفرق الفقه بين مصطلح اعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة، الأول يكون دون رضا المعني والثاني بطلب أو برضا صاحب الشأن ويخضع لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك.

وحدد المشرع الجزائري في نص المادة 65 مكرر 05 الفقرة 02 ق إ ج نوع المراسلات محل الاعتراض وهي المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

كثيرا ما تتطلب إجراءات التحري والتحقيق اللجوء الى مراقبة المحادثات الهاتفية، ونجد أن وسائل الاتصال الحديثة ساهمت بشكل كبير في تسهيل ارتكاب جرائم منظمة، سواء عن طريق المكالمات الهاتفية أو المراسلات الإلكترونية المتبادلة عبر الشبكات المعلوماتية.

وفي هذا الإطار أجازت اتفاقية بودابست للجرائم الالكترونية الاعتراض الشرعي لكل أشكال النقل الإلكتروني للبيانات سواء تمت عبر التلفون أو الفاكس أو البريد الإلكتروني ...إلخ.

وتشمل الاتصالات محل الاعتراض محتوى غير مشروع أو دليل على الأفعال الإجرامية الخطيرة التي يعرفها القانون الداخلي لكل دولة طرف في الاتفاقية مما يستوجب

1 ياسر الأمير فاروق، مراقبة الأحاديث الخاصة دراسة تأصيلية تحليلية و مقارنة للتنصت على المحادثات التلفونية و التي تجرى عبر الأنترنت و الاحاديث الشخصية نظريا و علميا، دار المطبوعات الجامعية،الإسكندرية، ط 1، 2019، ص 150 .

ضرورة اعتراض المراسلات الالكترونية المتبادلة عبر الحاسب الآلي أيضا لدرء خطر الجريمة وملاحقة الجناة، وبالرجوع للقانون الجزائري فإنه نص صراحة على اعتراض المراسلات السلكية واللاسلكية وفقا لأحكام القانون 04/09 حيث أجاز وضع الترتيبات التقنية لمراقبة الاتصالات الالكترونية والقيام بالتفتيش والحجز داخل المنظومة المعلوماتية.[1]

كما نص على ذلك قانون 03/00 المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية حيث أجاز اعتراض المراسلات المتبادلة عن طريق التلغراف والفاكس والبريد الالكتروني (الايميل) الرسائل القصيرة و sms،[2]عن طريق الهاتف المحمول والاتصالات المرئية.....الخ. وإذا كان الحال كذلك وكل إشارة أو كتابة أو صورة مطلوب التقاطها أو مكالمة هاتفية يجوز أن تكون محل للاعتراض.

وأسلوب اعتراض المراسلات يتميز بخصائص معينة تساعد في تحديد مضمونها وطبيعة العمل به، وهو أن يتم خلسة دون علم ورضا صاحب الشأن، ويمس بالحق الشخصي في سرية الحديث من أجل الحصول على دليل غير مادي، وذلك باستخدام أجهزة قادرة على التقاط الأحاديث.

ثانيا: تسجيل الأصوات والتقاط الصور

لم يرف المشرع الجزائري تسجيل الأصوات وبالرجوع الى المادة 65 مكرر 05 ق إ ج نستشف أن المقصود من تسجيل الأصوات هو وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به، بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية[3].

1 القانون رقم 09 . 04 مؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج ر ج ج، عدد 47، صادر بتاريخ 16 أوت 2009

2 قانون رقم 2000 . 03 المؤرخ في 05 عشت 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، ج ر ج ج، عدد 48، صادرة بتاريخ 06 أوت 2000.

3 احسن بوسقيعة، مرجع سابق، ص 113.

ويقصد به كذلك حفظ الحديث على جهاز معد لذلك بهدف الاستماع إليه مرة أخرى والتسجيل الصوتي الذي يهمنا في هذه الدراسة هو الذي يجريه رجال الضبطية القضائية من أجل التحري والتحقيق عن الجرائم الخطيرة.

أما بالنسبة لالتقاط الصور كذلك لم يعرف المشرع الجزائري هذه العملية صراحة، إلا أنه أشار إليها بلفظ "بالالتقاط" وتعرف على أنها تلك العملية التقنية التي تتم دون موافقة المعنيين من اجل التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

وتجدر الإشارة أن المشرع عندما جمع بين اعتراض المراسلات وتسجيل الاصوات والتقاط الصور في عنوان واحد بحكم أن هذه التقنيات تؤدي نفس الغرض متى توافرت الضمانات المنصوص عليها في المواد من 65 مكرر5 إلى غاية 65 مكرر10 ق إ ج.

ثالثا: إجراءات وشروط اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

حق الانسان في الخصوصية وأن يعيش حياة هادئة من المبادئ القدسية التي كرسها الدستور في المادة 39 منه، إلا أن المشرع الجزائري ولضرورة التحقيق في بعض الجرائم الحساسة سمح بالقيام بمثل هذه العمليات، إذ فضل مصلحة التحقيق وكشف المجرمين عن حرمة المساس الحياة الخاصة، وفقا لأحكام المواد من 65 مكرر5 الى غاية 65 مكرر 10 ق إ ج. كما أتاح للضبطية القضائية حق استعمال الأساليب والوسائل التقنية في إطار البحث والتحري في الجرائم المستحدثة وفقا للشروط والإجراءات التالية:

01/ طبيعة الجريمة: نصت المادة 65 مكرر 5 ق إ ج على اجراءات التحري والتحقيق الخاصة بحالة التلبس أو التحقيق الابتدائي في جرائم المخدرات، والجريمة المنظمة العابرة للحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الالية، وجرائم تبييض الأموال، والجرائم الإرهابية، وجرائم الصرف والفساد إذا اكتشفت اثناء التحريات الخاصة جرائم أخرى غير مذكورة في الاذن فهذا لا يكون سببا لبطلان الإجراءات العارضة وفقا لأحكام المادة 65 مكرر 2/6 ق.إ.ج.

02/ أن يكون الإذن صادر من وكيل الجمهورية أو قاضي التحقيق: وهو شرط أساسي لمباشرة عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ويشترط لصحته أن

يكون مكتوبا ويتضمن جميع المعلومات المكونة للجريمة، مع تحديد المدة الزمنية للعملية بأربعة أشهر قابلة للتجديد حسب مقتضيات التحري[1].

03/ الرقابة القضائية: يجب خضوع هذه العمليات المسموح بها قانونا الى رقابة واشراف وكيل الجمهورية المختص، وفي حالة فتح تحقيق قضائي فإن هذه العمليات يكون قاضي التحقيق صاحب السلطة لإصدار الإذن وتحت رقابته.

04/ وضع التقنية: بعد الحصول على الإذن يسمح لضباط الشرطة القضائية بوضع الترتيبات التقنية في الأماكن الخاصة والعمومية وغيرها دون موافقة وعلم الأشخاص المعنيين، وهذا للمحافظة على سرية العملية، كما أجاز المشرع أن تكون هذه الترتيبات خارج الميقات القانوني، أي خارج المواعيد المحددة في نص المادة 47 ق. إ.ج

05/ الإطار المكاني للأساليب التقنية في التحري عن الجرائم: بالرجوع إلى المادة 65 مكرر 5 ق.إ.ج حددت الأماكن التي يتم فيها استعمال الوسائل التقنية وهي الاماكن العمومية والأماكن الخاصة والمحلات السكنية[2] .

06/ المحافظة على السر المهني يلزم على الضبطية القضائية أثناء أداء مهامهم أو وظيفتهم بكتمان السر المهني الذي إطلعوا عليه سواء كان عن طريق تسجيل الاصوات او التقاط الصور خاصة إذا تعلق الأمر بأماكن يشغلها أشخاص ملزمون بكتمان السر المهني مثل مكاتب المحامين أو الموثقين أو إذا تعلق الأمر بأشخاص يحملون أسرار مهنية مثل القضاة والأطباء.

07/ تسخير الأعوان المؤهلين والمكلفين بالمواصلات السلكية واللاسلكية: أجاز المشرع لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له باستعمال الوسائل الخاصة في البحث والتحري ولقاضي التحقيق أو ضباط الشرطة القضائية الذي ينوبه أن يكلف عون مؤهل وصاحب خبرة وكفاءة في مجال المواصلات السلكية واللاسلكية بالتكفل

1 المادة 18 فقرة 01 من قانون الإجراءات الجزائية " يتعين على ضباط الشرطة القضائية أن يحرروا محاضر بأعمالهم وان يبادروا بغير تمهل الى اخطار وكيل الجمهورية بالجنايات او الجنح التي تصل الى علمهم".

2 الأماكن العامة: و هي التي يتم الدخول اليها و الخروج منها بحراسة تامة كالأسواق – الأماكن الخاصة وهي الأماكن او المحلات المعدة لنشاطات معينة كالفنادق و العيادات، المحلات السكنية عرفتها المادة 355 من قانون العقوبات.

بالجوانب التقنية لعمليات اعتراض المراسلات وتسجيل الأصوات، وهذا ما جاء في نص المادة 65 مكرر 8 ق إ ج[1].

08/ تحرير محضر عن العملية: كمبدأ عام يجب على ضباط الشرطة القضائية تدوين وتحرير تقارير عن كل عملية تطبيقا لنص المادة 65 مكرر 09 ق إ ج التي جاء فيها أنه يجب تحرير محضر يذكر فيه جميع التفاصيل العملية من بدايتها الى نهايتها وكذلك يذكر فيه تاريخ وساعة بداية العملية وتاريخ الانتهاء منها[2] .

أما بخصوص نتائج التحريات التي تتعلق بمضمون المراسلات المسجلة والصور الملتقطة فعلى المأذون له بهذه العملية أو المناب أن ينسخ أو يصف المحتوى الضروري والمهم لإظهار الحقيقة في محضر ليودع بالملف أما إذا كانت المكالمات باللغة الأجنبية فإنه يتم الاستعانة بمترجم لترجمة محتوى المكالمات ونسخها.

09/ ضبط التسجيلات ووضعها في أحراز: بما أن التسجيلات أو الأشرطة المصورة تعتبر أدلة اثبات مادية أصلية تقتضي الشرعية الإجرائية حفظها بطريقة خاصة، وذلك بوضعها في أحراز مختمة يضمن عدم التلاعب بها أو العبث في الحديث المسجل سواء بالحذف أو الإضافة، وضمها إلى المحضر وهذا ما نستنتجه من خلال استقراء نصوص المواد 18 و45 ق.إ.ج، وتجدر الاشارة هنا الى ان المشرع الجزائري لم يشر الى عرض هذه التسجيلات والصور على المشتبه فيهم في مرحلة جمع التسجيلات ويرجع ذلك الى الطابع السري الذي تتميز به هذه الجرائم الخطيرة على عكس ما نجده في المادة 42 من نفس القانون حيث اوجب عرض الاشياء المضبوطة على المشتبه فيهم لتميزها بطابع العلنية.

الفرع الثاني: مراقبة الاتصالات الالكترونية

من المؤكد قانونا أنه لا يجوز انتهاك حرمة المواطن وحرمة شرفه وسرية مراسلاته واتصالاته الخاصة بأي شكل من الأشكال، ولكن نظرا للظروف الأمنية التي يعيشها المجتمع الدولي وخاصة مع التطور التكنولوجي الذي سهل عمل الشبكات الاجرامية،

1 انظر المادة 65 مكرر 8 من قانون الإجراءات الجزائية.

2 عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة و النشر الجزائر، ط 2 ، 2011 ، ص 280.

وحفاظا على الأمن والنظام العام تدخل المشرع بموجب أحكام قانون 04/09 السالف الذكر الذي أجاز بصفة استثنائية للسلطات القضائية وفي إطار قرار معلل بمراقبة الاتصالات الالكترونية.

عرف المشرع الجزائري الاتصالات الالكترونية بموجب الفقرة (و) من المادة 02من القانون 04/09 السالف الذكر على انها اي تراسل أو ارسال او استقبال علامات أو اشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية وتعرف الاتصالات الالكترونية في الفقه المقارن بأنها الاتصالات التي تتم عن طريق جهاز الحاسب الالي والتي تتخذ شكل البريد الالكتروني email أو شكل محادثة فورية message instanyt والتي تتم عن طريق شبكة الانترنت.

ومما سبق يمكن تعريف مراقبة الاتصالات الالكترونية أنها عملية تتمثل في ترصد الرسائل الالكترونية وإجراء فحوصات تقنية وذلك بغية الوصول إلى مصدرها ومعرفة صاحبها[1].

وبالرجوع لأحكام المادة 04 من قانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها نجدها تتضمن حالات تطبيق الإجراء الجديد في مراقبة الاتصالات الالكترونية وقد جاءت على سبيل الحصر، كالوقاية من الافعال الموصوفة بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو في حالة توافر معلومات على احتمال وقوع اعتداء على منظومة حاسوبية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو في حالة صعوبة الوصول إلى نتيجة تفيد التحقيقات والأبحاث الجارية دون اللجوء إلى مراقبة الاتصالات الالكترونية، وكذا في إطار تنفيذ طلبات المساعدة القضائية الدولية.

1 قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة لنيل شهادة الماستر اكاديمي في القانون ، تخصص قانون عام للأعمال جامعة قاصدي مرباح ورقلة ن 2014 ، ص 56 .

المبحث الثاني: شروط قبول الدليل الجنائي الرقمي أمام القضاء

إن مجرد وجود دليل يثبت وقوع جريمة وينسبها للمتهم لا يكفي لبناء وتسبيب حكم الإدانة، إذ يجب أن يكون لهذا الدليل قيمة قانونية[1]، تتوقف على خضوعه للقواعد المقرر في الإثبات الجنائي، بما فيها الأدلة الرقمية التي لا تكون مقبولة ومشروعة إلا إذا أجريت عملية البحث والكشف والحصول عليها وتقديمها أمام القضاء في إطار أحكام القانون والإجراءات التي رسمها، وقيم العدالة وأخلاقياتها التي يحرص على حمايتها، وفي حالة الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد به مهما كانت دلالته الحقيقية، وحجيته في الاثبات وذلك لعدم مشروعيته[2] .

ويشترط أيضا في الدليل أن يكون يقينيا في دلالته على الوقائع المراد اثباتها سواء كانت هذه الأدلة تقليدية أو حديثة، فالدليل الرقمي يجب أن يكون غير قابل للشك، ويجب أن يخضع هذا الدليل للمناقشة ومواجهته بين الخصوم.

هذا ما سنحاول دراسته في هذا المبحث وعليه خصصنا المطلب الأول مشروعية الدليل الرقمي، وفي المطلب الثاني يقينية الدليل الرقمي، وفي المطلب الثالث مناقشة الدليل الرقمي.

المطلب الأول: مشروعية الدليل الجنائي الرقمي

إن كل قاعدة إجرائية يكون جزائها البطلان إذا ما كانت ماسة بالحقوق والحريات التي يتمتع بها أطراف الخصومة الجنائية، ويستوي في ذلك أن يكون الدستور أو التشريع مصدرا لهذه الحقوق والحريات.

وأثير الكثير من الجدل حول موضوع انتهاك الحياة الخاصة في إطار الحصول على دليل إدانة متهم في الجرائم المعلوماتية أثناء استخلاصه عن طريق استعمال الوسائل الحديثة الأمر الذي أدى إلى ظهور العديد من الاجتهادات القضائية التي تقرر عدم مشروعيته على أساس أن الحصول عليها واستخلاصها تطلب خرق مجال الخصوصية

1خالد عياد الحلبي، مرجع سابق، ص 235.

2 ميسون خلف الحمداني على محمد كاظم الموسوي، الدليل الرقمي وعلاقته بالمساس بالحق في الخصومة المعلوماتية أثناء اثبات الجريمة، جمهورية العراق، وزارة التعليم العالي والبحث العلمي، جامعة النهرين، كلية الحقوق،2016،ص37.

المعلوماتية كأحد مظاهر الحق في حرمة الحياة الخاصة للفرد وما تحويه من معلومات عنه في الوسط الواقعي والتي تحولت بفضل التكنولوجيا إلى الوسط الافتراضي المجرد، ومع وجود اختلاف بين الوسطين ينبغي أن نحاط بنوع من الحرمة والقداسة.

ومن أجل الحفاظ على الخصوصية المعلوماتية، وعدم انتهاك حرمة الحياة الخاصة للفرد وضعت الاتفاقيات دولية، والدساتير وطنية، والقوانين الإجرائية نصوصا تتضمن ضوابط لشرعية الإجراءات الماسة بالحريات الفردية، ومن ثم فإن مخالفة هذه النصوص يضفي عليه عدم المشروعية، غير أن ذلك لا يعني حصر حالات عدم المشروعية في نطاق مخالفة النصوص المقررة لضمان الحريات الشخصية، وبعيدا عن هذه النصوص يتجه الفقه والقضاء إلى الحاق الدليل بعدم المشروعية متى كانت طريقة الحصول عليه تتعارض مع القواعد القانونية العامة [1].

ويتضح بأن قيد مشروعية الحصول على الدليل بصفة عامة يمثل بالمقابل لحرية القاضي في قبول جميع أدلة الإثبات، بما فيها تلك التي ينظمها المشرع خاصة أمام ما قد يستجد من وسائل أخرى يكون من شأنها تيسير الوصول للحقيقة[2]

الفرع الأول: المقصود بمشروعية الحصول على الدليل الجنائي الرقمي

المقصود بمشروعية الحصول على الدليل الرقمي الجنائي يتمثل في الإجراء الذي استنبط منه القاضي الدليل يتفق مع القواعد القانونية التي تحكمه غير مخالف لأحكام الدستور أو قانون الإجراءات الجزائية، ويكون الدليل مشروعا متى كان من يباشره يستند إلى قواعد قانونية دون تعسف أو تجاوز، والهدف من ذلك هو حماية الحريات والحقوق الشخصية من تعسف سلطة التحقيق في غير الحالات التي رخص فيها بذلك[3]

كما أن قاعدة مشروعية الحصول على الدليل الجنائي الرقمي لا تقتصر فقط على مجرد مطابقة القاعدة القانونية التي ينص عليها المشرع، بل يجب أيضا مراعاة إعلان حقوق

1 ميسون خلف الحمداني، مرجع سابق، ص 38

2 عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، د ط، دار الجامعة الجديدة الإسكندرية، 2010، ص 213.

3 كمال محمد عواد، الضوابط الشرعية والقانونية للأدلة الجنائية في الفقه الإسلامي والقانون الوضعي الطبعة الأولى، دار الفكر الجامعي، مصر، 2011، ص 165

الإنسان والمواثيق والاتفاقيات الدولية وقواعد النظام العام، ومثال ذلك ما نصت عنه المادة 12 من الإعلان العالمي لحقوق الإنسان "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته. ولكل شخص حماية القانون من مثل هذا التدخل أو تلك الحملات "[1] .

ومشروعية الدليل هي إحدى أهم ما وصى به المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات، المنعقد في عاصمة البرازيل في الفترة 9/4 سبتمبر 1994 في مجال اصلاح حركة الإجراءات الجنائية بالتوصية رقم 18 التي تنص على " كل الأدلة التي يتم الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة ولا يمكن التمسك بها أو مراعاتها" كما أشارت إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في جرائم الحاسب الآلي والجرائم التقليدية في بيئة تكنولوجيا المعلومات وإلا ترتب عليها بطلان الإجراء فضلا عن تقرير المسؤولية لرجل السلطة العامة الذي انتهك القانون[2] .

ومن قبيل الأدلة غير المشروعة تلك المتحصل عليها من خلال إجراء مراقبة الاتصالات دون أن تكون محل لإذن من سلطة قضائية مختصة، أو اتخاذ ترتيبات تقنية من أجل تفتيش منظومة معلوماتية تؤدي بالمساس بالحياة الخاصة للغير، أو ممارسة أي إكراه معنوي على المشتبه فيه لفك شفرة نظام من نظم المعلوماتية، ويعد من الطرق غير المشروعة استخدام التدليس والخداع في الحصول على الأدلة الإلكترونية[3]

الفرع الثاني: مشروعية الحصول على الدليل الجنائي الرقمي

أكد المشرع الجزائري على ضرورة حماية الحياة الخاصة وعدم المساس بها وهذا الحق مكفول دستوريا من خلال نص المادة 39 من الدستور الجزائري والتي تنص: لا يجوز انتهاك حرمة المواطن الخاصة، وحرمة شرفه، ويحميها القانون، وأضافت نفس المادة في فقرتها الثانية على أن: سرية المراسلات والاتصالات الخاصة مضمونة بكل أشكالها.

1 معتصم خميس مشعشع، مرجع سابق، ص 34.

2 سامية بلجراف، سلطة القاضي الجنائي في قبول وتقدير الدليل الرقمي، ورقة بحثية مقدمة إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر بسكرة، الجزائر، يومي 16 و17 نوفمبر 2015.

3 عائشة بن قارة مصطفى، مرجع سابق، ص 218.

وتأتي الحماية القانونية لهذا الحق الدستوري من خلال نص المادة 303 مكرر من قانون العقوبات إذ يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دينار جزائري إلى 300.000 دينار جزائري كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص وبأي تقنية كانت وذلك بالتقاط الصور أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

كما نص قانون الإجراءات الجزائية الجزائري على تقرير البطلان في حالة الحصول على دليل بطريقة غير مشروعة بما فيها الأدلة الرقمية وفقا لأحكام المادة 1/157 و 105 والمادة 191 وهذا الأمر يثير مسألة مهمة هي المعيار الذي يبين العلاقة التي تربط بين العمل الإجرائي والأعمال التالية له، حتى يمتد إليها البطلان، وقد تعددت المعايير التي جاء بها الفقه إلا أن المعيار السائد في الجزائر هو أن العمل اللاحق يعتبر مرتبطا بالإجراء السابق إذا كان هذا الإجراء ضروريا لصحة العمل الاحق، فإذا أوجب القانون مباشرة اجراء معين قبل الآخر بحيث يصبح الأول بمثابة السبب الوحيد للإجراء الذي تلاه كان الإجراء الأول شرطا لإجراء التالي له، فإذا بطل ترتب عليه بطلان الإجراء الذي بني عليه [1]

وأما فيما يخص المشرع الفرنسي فقد كان السباق في حماية الحياة الخاصة وذلك بموجب إصداره لقانون رقم 643/70 المؤرخ في 1970/07/17 بالإضافة إلى القانون رقم 17/78 الصادر في سنة 1978 والمتعلق بالمعالجة الالكترونية للبيانات الرسمية والذي تضمن حماية البيانات الشخصية المرتبطة بحياة الخاصة للأفراد[2].

زيادة على ذلك ما نص عليه قانون العقوبات الفرنسي بتجريم العديد من الأفعال التي تمس البيانات الإلكترونية الشخصية، مثل ما نصت عليه المادة 226 مكرر 1 التي تعاقب كل من يقوم بمعالجة الكترونية للبيانات الشخصية دون ترخيص، وكذلك ما نصت عليه المادة 226 مكرر 21 والتي عاقبت على الانحراف على الغرض من المعالجة الإلكترونية للبيانات الشخصية.

1 شهرزاد حداد، الدليل الالكتروني في مجال الاثبات الجنائي، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة العربي بن مهيدي أم البواقي،2016،2017، ص91.

2 سوزان عدنان، انتهاك حياة حرمة الحياة الخاصة عبر الإنترنت، دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانون، العدد 03 المجلد 29، سوريا، 2013، ص 437.

بناء على ما سبق ذكره فقد حرص كل من المشرعين الجزائري والفرنسي على حماية الحياة الخاصة للأفراد، وذلك بالرفع من مكانة هذا الحق، وجعله في مصاف الحقوق الدستورية، بالإضافة إلى تقرير عقوبات على كل الأفعال التي تخل به، ولكن هذا لا يعني أنه لا يمكن المساس بهذا الحق بتاتا، إذ وضع القانون استثناءات على هذه القاعدة الدستورية وذلك بإمكانية المساس بهذا الحق إذا اقتضت الضرورة, على نحو ما سار عليه المشرع الجزائري في المادة 03 من قانون 04/09 والتي 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 قانونا الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية، لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها، في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

من خلال القيام بإجراءات التفتيش أنظمة الحاسوب الآلي أو مراقبة الاتصالات الإلكترونية بغية استخلاص الأدلة الجنائية الرقمية، وذلك بشرط احترام الإجراءات الخاصة بها والمنصوص عليها قانونا.

وعلى هذا الأساس وفي إطار مشروعية الحصول على الدليل الجنائي الرقمي فالمشرع الفرنسي وبالرغم من أنه لم يتضمن نصوص تتعلق بمبدأ الأمانة والنزاهة في البحث عن الحقيقة، إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال البحث والتحري والتحقيق في الجرائم العادية أو في الجرائم الإلكترونية بحيث تم قبول استخدام الوسائل العلمية الحديثة في بحث واستخلاص الأدلة الجنائية والتي من بينها الأدلة الرقمية تحت التحفظ وهو أن يتم الحصول عليها بطريقة مشروعة ونزيهة [1].

1 أحمد عبد اللاه هلالي، مرجع سابق، ص 353.

المطلب الثاني: يقينية الدليل الجنائي الرقمي ومناقشته

إن الهدف الذي تسعى إليه كافة التشريعات الإجرائية هو أن يصيب القاضي الحقيقة في حكمه، سواء بالبراءة أو الإدانة، والحقيقة لا يمكن الوصول إليها إلا باليقين، فالقاضي لا يبني حكمه ويؤسس اقتناعه إلا بناء على الأدلة طرحت أمامه وخضعت للمناقشة أمام الخصوم. ومنه تكمن أهمية يقينية الأدلة الجنائية ومناقشتها من أهم المبادئ التي تحقق المحاكمة العادلة التي ينشدها الجميع.

لذا وجب علينا في هذا المطلب أن نبين مفهوم يقينية الأدلة الجنائية الرقمية بالإضافة إلى بيان القواعد التي تحكمه في الفرع الأول ونتطرق في الفرع الثاني مناقشة الأدلة الجنائية الرقمية.

الفرع الأول: يقينية الدليل الجنائي الرقمي

اليقين بصفة عامة هو عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة، ويتم الوصول إليها عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة عالية من التوكيد[1] لذا عندما يصل القاضي إلى درجة اليقين فإنه يصبح في هذه المرحلة مقتنعا بالحقيقة لأن اليقين هو الأصل ووسيلة لاقتناع القاضي بالحقيقة، هو ثمرة اليقين وليس اليقين ذاته. [2]

ويتضح من خلال ما سبق أن الوصول إلى اليقين يكون عن طريق نوعين من المعرفة، الأولى تتمثل في المعرفة الحسية التي تدركها الحواس، والثانية تتمثل في المعرفة العقلية التي يقوم بها العقل عن طريق التحليل والاستنتاج

وأما اليقين في مجال الأدلة الجنائية الرقمية، فإنه يشترط في هذا النوع من الأدلة مثل باقي الأدلة الجنائية الأخرى، بحيث تكون يجب أن تكون غير قابلة للشك حتى

1 مبروك نصر الدين، محاضرات في الإثبات الجنائي، النظرية العامة للإثبات الجنائي، طبعة 2، دار الهدى، الجزائر، 2010، ص 491

2 نفس المرجع، ص 491

يمكن الحكم بالإدانة، لأنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين[1].

ويمكن الوصول إلى اليقين في هذه الحالة من خلال ما يعرض من أدلة رقمية بمختلف أنواعها وأشكالها، وما ينطبع في ذهن القاضي من تصورات واحتمالات تحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه[2].

وفي حالة عدم قدرة أدلة الإدانة على إحداث اليقين يترتب عليه استمرار حالة البراءة التي يكفي لتأكيد وجودها مجرد الشك في ثبوت الإدانة. وذلك لأنها إثبات على خلاف الأصل الذي لا يمكن إثبات عكسه إلا بمقتضى حالة من اليقين في نتائجها مع تلك المسلم بوجودها نتيجة لمبدأ افتراض البراءة[3].

نظرا لطبيعة التقنية التي يتميز بها الدليل الرقمي الجنائي حدد المختصين عدة قواعد تحكم يقينيتها، وذلك بواسطة استعمال وسائل فنية من طبيعة هذا الدليل تمكن في فحصه والتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه.

إن مضمون عملية تقييم الدليل الجنائي الرقمي هو التأكد من سلامته من العبث عبر اتباع مجموعة من الطرق أهمها استعمال عملية التحليل النظري الرقمي، التي تعتبر من بين الوسائل المهمة للكشف عن مصداقية الدليل الرقمي، من خلال القيام بعملية مقارنة الدليل الجنائي الرقمي (الأصلي) المقدم للقضاء بالنسخة المستخرجة.

وفي حالة عدم الحصول على النسخة الأصلية للدليل الجنائي الرقمي أو في حالة وقوع تعديل أو إتلاف للنسخة الأصلية، في هذه الحالة للتأكد من سلامة هذا الدليل من العبث يتم استخدام عمليات حسابية خاصة تسمى بالخورزميات، أو باللجوء إلى نوع آخر

1 أحمد عبد اللاه هلالي، مرجع سابق، ص 739.

2 علي حسن أحمد الطوالبة، التفتيش الجنائي على نظم الحاسوب، دراسة مقارنة، ط1، عالم الكتب الحديث للنشر والتوزيع، الأردن، 2004، ص 190.

3 نفس المرجع، ص 191.

من الأدلة الرقمية، والذي يطلق عليه اسم الدليل الرقمي المحايدة، وهو دليل لا علاقة له بموضوع الجريمة، ولكنه يساهم في التأكد من سلامة الدليل الجنائي الرقمي[1] .

لذا وتفاديا لحصول أي اتلاف أو تعديل للدليل الجنائي الرقمي، يوصي المختصون دائما بالحفاظ على الدليل الجنائي الرقمي الأصلي، واستغلال الميزة التي يتمتع بها وهي استخراج العديد من النسخ المطابقة له.

وعند اتباع جملة من الأساليب والإجراءات التقنية للحصول على الأدلة الجنائية الرقمية يمكن أن تعتري هذه الإجراءات أخطاء قد تشكك في سلامة النتائج، لذا يجب في هذه الحالة الاعتماد على اختبارات محددة كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الجنائي الرقمي، ويتمثل مضمونها في نقطتين أساسيتين تتعلق الأولى بالتأكد من دقة الأدوات المستخدمة في استخلاص الدليل الجنائي الرقمي بالتحقق من مدى قدرة هذه الأدوات على عرض كافة البيانات المتعلقة بالدليل الجنائي الرقمي، بالإضافة إلى خضوع هذه الأدوات لاختبار فني يمكن من خلاله التأكد من انها لا تعرض بيانات إضافية جديدة[2]

والنقطة الثانية في الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل، إذ تبين الدراسات العلمية في مجال تقنية المعلومات على الطرق السليمة التي يجب اتباعها في الحصول على الدليل الرقمي، لذا فالاعتماد على الأدوات التي أثبتت الدراسات العلمية عدم كفاءتها، تؤثر بصفة مباشرة على مصداقية الأدلة الجنائية الرقمية المستمدة منها[3]، وبالتالي يتعدى التأثير حتى على يقين القاضي الذي يقوم باستبعاد هذه الأدلة.

1 خالد عياد الحلبي، مرجع سابق، ص249.

2 عائشة بن قارة مصطفى، مرجع سابق، ص 271

3 خالد عباد الحلبي, مرجع سابق، ص 251

الفرع الثاني: مناقشة الأدلة الجنائية الرقمية

يقصد بمناقشة الأدلة الجنائية أن القاضي لا يمكن أن يبني حكمه ويؤسس اقتناعه الشخصي إلا على العناصر الإثباتية والأدلة التي طرحت أمامه بجلسة المحاكمة وأثناء التحقيق النهائي للدعوى المنشورة أمامه، وهذا ما أقر به المشرع الجزائري وفقا لمنظور المادة 212 من قانون الإجراءات الجزائية والتي تنص على أنه " لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه"

من الأسس التي تقوم عليها الأدلة أن القاضي لا يمكن أن يباشر سلطته في تقدير هذه الأدلة ما لم تطرح في الجلسة وبحضور الخصوم وتتم مناقشتها، وغاية ذلك أن يتاح لكل طرف في الدعوى أن يواجه خصمه بما لديه من أدلة إزاءه ويبين موقفه منها، ومن مقتضيات هذا الضابط أن تعرض أدلة الدعوى جميعا في جلسة المحاكمة وتطرح للمناقشات فالشاهد يدلي بشهادته، والمتهم يدلي بأقواله ويقرأ تقرير الخبرة.

وضابط وضعية الدليل الرقمي يقوم على عنصرين أساسين حيث يتمثل العنصر الأول في اتاحة الفرسة للخصوم للاطلاع على الدليل الالكتروني والرد عليه، أما العنصر الثاني يتمثل في أن يكون الدليل الالكتروني أصلا في أوراق الدعوى.

بالنسبة للعنصر الأول ففحواه أنه على القاضي مبدئيا أن يطرح كل دليل مقدم في الدعوى للمناقشة أمام الخصوم، حتى يكونوا على بينة مما يقدم ضدهم من أدلة ليتمكنوا من مواجهة هذه الأدلة والرد عليها، وهذا احتراما لحقوق الدفاع. والذي يعد أحد المظاهر الأساسية في دولة القانون والنظم الديمقراطية[1].

ويتيح مبدأ المواجهة تجسيد هذا الأخير، حيث يقضي مبدأ حق الدفاع حضور كل الخصوم في الدعوى وأن يطلع خصومه على ما لديهم من أدلة، ويواجه بها وأن يناقش كل واحد منهما أدلة الطرف الآخر ومبدأ المواجهة يجب أن تتوفر فيه نوعين من الضمانات.

1 أشرف عبد القادر قنديل، مرجع سابق ص237

حيث أن الضمانة الأولى تكون سابقة على عملية المواجهة الأولى ذاتها بين طرفي الدعوى وهو يتضمن ضرورة إحاطة المتهم بالتهم المنسوبة اليه وأن يمنح الوقت والوسائل اللازمة لتحضير دفاعه وأن يسمح له بالاستعانة عند الاقتضاء بمترجم.

أما النوع الثاني من الضمانات فيتم أثناء عملية المواجهة ذاتها وهي الأكثر تأثيرا في الدعوى العمومية إذ يلزم أن يسمح لكل طرف بتقديم ما لديه من سندات وسؤال الشهود والخبراء وأن يطالب باتخاذ أي اجراء يقدر فائدته وإثارة أي دفع أو إيداع مذكرات ثم حق كل طرف من مناقشة تقارير الخبرة والبحث ما ورد فيه.

ولهذا فإنه لا يجوز للقاضي الجنائي أن يبني اقتناعه قدمه أحد أطراف الدعوى إلا إذا عرض هذا الدليل في جلسة المحاكمة، إذ أن العدالة تقتضي أن حكم القاضي يأتي بعد مناقشة هادئة ومجادلة حرة ومتكافئة لكل صاحب حق مشروع في الدعوى[1].

أما بالنسبة للعنصر الثاني من ضبط وضعية الدليل الإلكتروني يتمثل في أن يكون الدليل الالكتروني أصل في أوراق الدعوى حتى يكون اقتناع القاضي الجنائي مبني على أساس ومن أجل ذلك أوجب المشرع تحرير محضر الجلسة لإثبات وقائع الدعوى الجزائية وأدلتها لكي يتمكن قاضي الموضوع أو أي شخص من الخصوم للرجوع إلى هذا المحضر إذا ما رغبوا في استيضاح أين من الوقائع الثابتة به بهدف منع التحكم من طرف القاضي الجنائي وتحقيق العدالة بالإضافة إلى ذلك فإن الغرض أيضا تمكين المحكمة المطعون أمامها من مراجعة الحكم المطعون فيه وتقديره من حيث الخطأ والصواب [2]

وضابط وضعية الدليل الالكتروني ترتب عليه نتائج من أهمها عدم جواز أن يقضي القاضي الجنائي بناءا على علمه الشخصي، أي عدم استناده على معلوماته الشخصية التي يكون قد حصل عليها من خارج نطاق الدعوى المطروحة أمامه، والتي من الممكن أن تؤثر في تكوين قناعته عند تقديره لأدلتها

وهذا يعني أن المعلومات الشخصية والتي يحوزها القاضي والتي يمنع عليه القضاء لاستناد اليها هي معلومات تتصل بصورة أو بأخرى بالدعوى التي ينظر فيها ومن الممكن

1 عائشة بن قارة مصطفى، مرجع سابق، ص 272

2 أشرف عبد القادر قنديل، مرجع سابق، ص 237

أن تؤثر على تقديره لأدلتها ذلك لأنها لم تحصل بالطريقة التي رسمها القانون، وهو أن يكون لها أصل في الأوراق.

ويرى البعض أن أساس هذه القاعدة، إلى أنه يترتب على حق الخصوم في مناقشة الأدلة التي تقدم في الدعوى أنه لا يجوز للقاضي أن يقضي بعلمه وهذا لأن علم القاضي يكون دليلا في الدعوى، ولما كان للخصوم حق مناقشة هذا الدليل يقتضي أن ينزل القاضي من منزلة الخصوم فيكون خصما وحكما وهذا لا يجوز.

ويرجع البعض الآخر أساس هذه القاعدة إلى ضرورة احترام حق الدفاع إذ أن المعلومات الشخصية التي يستند عليها القاضي تعد في الحقيقة مفاجأة للخصوم أن لم تناقش بمعرفتهم، ولم يتم اثباتها في إطار إجراءات الخصومة، ويذهب رأي ثالث من أن منع القاضي الجزائي من الحكم برأيه الشخصي بعلمه الشخصي لا يرجع إلى حق الخصم في مناقشة الأدلة التي تقدم في الدعوى، وإنما يرجع إلى ما شاهده القاضي أو علمه أو سمعه مما يتصل بوقائع الدعوى، سوف يؤثر حتما في تقدير القاضي للأدلة بل أنه قد يشمل هذا التقدير وهو في هذه الحالة لا يصلح أن يكون قاضيا وإلا أعتبر قاضيا شاهدا في آن واحد. ولهذا نص القانون على أن القاضي الذي سبق له أن شهد في قضية ما لا يصلح أن يكون قاضيا فيها[1]

ولهذا فإنه ضمانة لنزاهته وحياده فإذا ما توفرت لديه معلومات شخصية حول الدعوى المطروحة أمامه فعليه في هذه الحال أن يتنحى عن الفصل فيها تاركا الفرصة للخصوم لمناقشة المعلومات التي حصل عليها.

ولكن يجوز له أن يستند إلى معلومات عامة التي يفترض الكل أن يعلم بها والتي يكتسبها القاضي من خبرته أو ثقافته العامة، مما لا تلتزم المحكمة قانونا ببيان الدليل عليه فهي لا تعد من قبيل المعلومات الشخصية المحضورة على القاضي أن يبني حكمه عليها، إلا أن ما ينبغي الإشارة إليه أن هذه القاعدة يجب أن لا تتعارض مع الدور الإيجابي للقاضي في البحث عن الحقيقة أو عن حريته في الاستعانة بكافة وسائل الإثبات، طالما أنه يطرح الأدلة المتحصل عليها للمناقشة بين أطراف الدعوى فالحضر يقع على المعلومات

1 عائشة بن قارة مصطفى، مرجع سابق، ص 272

التي يستقيها بصفة شخصية وليس بصفته القضائية وهذه القاعدة ورد عليه استثناء أنه يجوز للقاضي أن يحكم بما رآه وسمعه بنفسه في حالة ارتكاب جريمة في الجلسة أي جرائم الجلسات وهو ما نصت عليه المادة 569 من ق ا ج.

الفصل الثاني

حجية الدليل الرقمي

في الإثبات الجنائي

يعتبر الدليل الجنائي العنصر الأهم والأساسي لتحديد مصير المتهم بين الحكم بالإدانة أو البراءة، وهذا بالنظر إلى مدى حجيته في الإثبات الجنائي، ومدى اعتماد القانون على هذه الحجية، أو ما تعلق بسلطة القاضي في تقدير هذا الدليل، أو بسلطته بقبوله الدليل الرقمي والتي تخضع لنفس القواعد والضوابط المقررة لباقي الأدلة.

إن مجرد وجود دليل يثبت الجريمة وينسبها إلى شخص معين لا يمكن التعويل عليه لإصدار الحكم بالإدانة، فلا بد أن يكون لهذا الدليل قيمة قانونية، تتوقف على مشروعية وجوده أي أن يكون معترف به ويجيز للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة كما سبق وأن أشرنا إلى ذلك في الفصل الأول.

والدليل الرقمي كباقي الأدلة الجنائية يخضع للقواعد المقررة لباقي الأدلة سواء كانت هذه القواعد تتعلق بنظام الإثبات الحر أو المقيد أو المختلط، وبما أنه يعتبر من الأدلة المستحدثة

قد يواجه بعض الصعوبات أثناء تقييمه، أو تقديره من طرف القاضي الجنائي وهو ما يثير العديد من الإشكالات حول مدى قابلية القضاء للتعامل مع هذا النوع من الأدلة.

إن الطبيعة الخاصة التي يتميز بها الدليل الإلكتروني، وكذا حجيته في الإثبات الجنائي ومدى قبوله والأخذ به، يقتضي أن نقسم هذا الفصل إلى مبحثين:

المبحث الأول: حجية الدليل الرقمي في أنظمة الإثبات.

المبحث الثاني: حجية الدليل الرقمي أمام القضاء الجنائي.

المبحث الأول: حجية الدليل الرقمي في أنظمة الإثبات

إن موقف القوانين المقارنة فيما يتعلق بسلطة القاضي الجنائي في قبول الدليل الرقمي تخضع إلى طبيعة نظام الإثبات السائد في كل دولة، وهذا الأخير يختلف من دولة لأخرى حيث تتعامل هذه الأنظمة مع الأدلة الجنائية بشكل متباين، بين التضييق والتقييد، إلى التوسع والإطلاق، وتنقسم هذه النظم القانونية في هذا المجال إلى قسمين، نظام الإثبات الحر ونظام الإثبات المقيد، وفضلا عن ذلك برز نظام ثالث يجمع بين النظامين وهو نظام الاثبات المختلط.

سنحاول في هذا المبحث اسقاط قواعد أنظمة الإثبات الجنائي على الدليل الرقمي بصفته من الأدلة المستحدثة وسنتناول في المطلب الأول الدليل الإلكتروني في نظام الإثبات الحر وفي المطلب الثاني نظام الإثبات في نظام الإثبات المقيد، وفي المطلب الثالث الدليل الرقمي في نظام الإثبات المختلط.

المطلب الأول: الدليل الرقمي في نظام الإثبات الحر

يعتمد هذا النظام على مبدأ حرية الإثبات، يتمتع القاضي الجنائي بسلطة واسعة في اختيار وقبول الأدلة وتقييم مدى اعتماده على تلك الأدلة، لتكوين اقتناعه الشخصي، أي أن يحكم في الدعوى المنشورة أمامه حسب العقيدة التي تكونت لديه بكامل حرية، وبالتالي يكون حرا في اختيار الدليل، ويستعين بكل طرق الإثبات للبحث عن الحقيقة هذا من جهة، ومن جهة ثانية يكون حرا في تقييم هذا الدليل دون أن يفرض عليه شرط أو قيد.

بصفة عامة أن نظام الإثبات الحر يكرس مبدأ حرية القاضي في الاقتناع بمعنى أن القاضي حر في تكوين عقيدته من أي دليل يراه يقينيا ويقتنع به[1].

ومما سبق ذكره يتضح أنه يجوز للقاضي الجنائي الاستناد إلى الدليل الرقمي لإثبات الفعل المجرم بصفة عامة، والجرائم الإلكترونية على وجه الخصوص.

ولم تفرد التشريعات التي أخذت بنظام الإثبات الحر نصوصا خاصة، فيما يتعلق بقبول الدليل الالكتروني، وذلك على أساس أن هذه الدول تستند لمبدأ حرية الإثبات في

1 محمد مروان، المرجع السابق، ص 39

المسائل الجنائية، والذي تتمثل خصائصه في عدم تحديد الأدلة، بمعنى أن للخصوم الحرية في تقديم أي دليل يمكنهم من اثبات أدائهم. والقاضي حر في تقييم الأدلة وتقديرها وقبولها بدون أي شرط أو قيد.

الفرع الأول: مبدأ حرية الإثبات الجنائي للدليل الرقمي

ويقصد بهذا المبدأ حرية جميع الأطراف في اللجوء إلى كافة وسائل الإثبات، للاستدلال بها على ما يدعونه، فلسلطة الاتهام أن تلجأ إلى لأي وسيلة لإثبات وقوع الجريمة واسنادها للمتهم، وعلى هذا الأخير أن يدافع عن نفسه ويدرأ التهم الموجهة إليه بكافة طرق الإثبات ويستظهر القاضي الحقيقة، ويفصل في الدعوى الجنائية المعروضة عليه بكل دليل يراه مناسبا في ذلك، أي أن جميع الأدلة متساوية فيما بينها، ولا مفاضلة بين دليل وآخر في الإثبات إلا بمقدار ما تحدثه من أثر في نفس القاضي من ارتياح واطمئنان[1] .

كما أن الأدلة في ظل هذا النظام لا تكون محددة مسبقا، ولا وجود لأدلة تفرض على القاضي قبولها، وتحدد الشروط اللازمة لصحة الدليل من طرف المشرع وكيفية تقديمه ضمانا للحرية الفردية، وكفالة لحسن سير العدالة، وللقاضي أن يتخذ أي إجراء يراه ضروريا ومناسبا للفصل في الدعوى، فله أن ينتقل إلى عين المكان للمعاينة أو يدونأقوال المتهم بعد سماعه واحاطته بكافة الضمانات المكفولة له قانونا، واستدعاء الشهود وسماعهم، وغيرها من الإجراءات الأخرى[2].

لقد أخذ المشرع الجزائري بهذا النظام على غرار بقية الدول اللاتينية، فأقر مبدأ حرية الإثبات الجنائي في المادة 212 من قانون الإجراءات الجزائية التي تنص على أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدى الأحوال التي ينص القانون على خلاف ذلك، وللقاض أن يبني حكمه بناء على اقتناعه الخاص.

ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا.

1 ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 128.

2 سامي جلال فقي حسين، المرجع السابق، ص 75.

وهناك عدة أسباب تجعل من الضروري العمل بهذا المبدأ في مجال الاثبات الجنائي

كحرية الإثبات التي تعد نتيجة منطقية لقضاء القاضي بمحض اقتناعه، وهذا الأمر يترتب عليه السماح للقاضي بالاستعانة بجميع وسائل الإثبات التي يقتنع ويطمأن اليها ليتمكن من أداء رسالته في إرساء العدالة بين المتقاضين.

كما أن الإثبات في الدعوى الجنائية يرد على وقائع قانونية، سواء كانت مادية أو معنوية مما يصعب بل يستحيل الحصول على دليل مسبق لهذه الوقائع، بعكس الدعوى المدنية التي يسهل الحصول على دليل مسبق لوقائعها، بالإضافة إلى طبيعة المصلحة التي تحميها الدعوى الجنائية، التي تختلف عن المصلحة التي تحميها الدعوى المدنية، فغالبا ما تتعلق الأدلة بمصلحة المجتمع في أمنه واستقراره، أما المصلحة في الدعوى المدنية تتعلق بأفرادها.

من المسلم به أن قرينة البراءة تلقي عبء الإثبات كلية على عاتق سلطة الاتهام، مما جعل صعوبة في مهمة هذه السلطة، لذلك كان من الضروري، تسهيل مهمتها بإقرار مبدأ حرية الإثبات، والذي يعد بمثابة إقرار ضمني من المشرع بعدم قدرة الأدلة التقليدية في مواجهة الجرائم المستحدثة، ومنها الجريمة الالكترونية[1].

وعليه فإن الدليل الرقمي شأنه شأن الأدلة الأخرى، فهو مقبول مبدئيا في الإثبات الجنائي بصفة عامة، والاثبات في الجرائم الالكترونية بصفة خاصة، بشرط احترام ضابط المشروعية.

فالحرية في هذا النظام مقيدة بضوابط المشروعية التي يجب احترامها وعدم مخالفته، وعدم الاعتماد على وسائل غير قانونية، وإلا ترتب على هذه المخالفة عدم مشروعية الدليل، ومنه عدم قبول الدليل وبطلانه.

1 عائشة بن قارة مصطفى، المرجع السابق، ص 187.

الفرع الثاني: النتائج المترتبة عن تطبيق مبدأ حرية الإثبات الجنائي

إن إعمال مبدأ حرية الإثبات الجنائي يجعل القاضي يتمتع بدور إيجابي في توفير وقبول وتقدير الدليل الجنائي، بما في ذلك الدليل الرقمي ومنه تقتضي الدراسة التطرق إلى الدور الإيجابي للقاضي الجنائي في توفير الدليل الالكتروني ودوره الإيجابي في قبول هذه الأدلة من خلال ما يلي:

أولا/ الدور الإيجابي للقاضي الجنائي في توفير الدليل الرقمي

أن اعتناق المشرع لمبدأ حرية الإثبات الجنائي، منح للقاضي الجزائي دورا هاما في الدعوى الجنائية، خاصة فيما يتعلق بالإثبات[1]، والمقصود بالدور الإيجابي للقاضي الجنائي هو عدم التزام القاضي بما يقدمه أطراف الدعوى من أدلة، وإنما له سلطة فيها، ويجب عليه أن يبادر من تلقاء نفسه إلى اتخاذ إجراءات المناسبة للتحقيق في الدعوى، والكشف عن الحقيقة[2] .

وهذه الأخير لا تظهر وحدها وإنما تحتاج إلى من يبحث عنها، والقاضي غير ملزم بأن يقنع بما يقدمه اليه أطراف الدعوى، وإنما عليه أن يبحث بنفسه عن الأدلة اللازمة لتكوين قناعته من واجبه أن يتحرى ويبحث عن الحقيقة بجميع الوسائل، سواء نص عليها القانون أو لم ينص كالدليل الرقمي مثلا، وهو ما أكدته المادة 212 من قانون الإجراءات الجزائية.

ويتحدد الدور الإيجابي للقاضي من خلال النظام الإجرائي السائد في الدول التي تأخذ بنظام الإثبات الحر، فإذا كان النظام المتبنى هو النظام الاتهامي، فمن الطبيعي أن يكون دور القاضي الجنائي سلبي، لأن هذا النظام ينظر إلى الدعوى الجنائية على أنها ملك للطرفين، أحدهما هو الادعاء الذي يمثله المضرور من الجريمة والآخر هو مرتكب الجريمة، ولا شأن للسلطات العامة بجمع الأدلة وينحصر دور القاضي في فحص الأدلة المقدمة من قبل الأطراف.

---

1 أشرف عبد القادر قنديل، المرجع السابق، ص 198.

2 عادل مختاري، دور القاضي الجزائي في ظل مبدأ الاقتناع القضائي، مجلة المنتدى القانوني، العدد الخاص، مارس 2008، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة ص 182.

أما النظام التنقيبي هو المهيمن على الإجراءات الجنائية، كالقانون الجزائري عندما يكون دور القاضي إيجابي على أساس أن الضرر الذي تحدثه الجريمة ليس ضررا فرديا فحسب، وإنما هو ضرر يهدد مصلحة المجتمع في أمنه واستقراره وسلامته.[1]

ويظهر الدور الإيجابي للقاضي الجنائي في توفير الدليل الالكتروني من خلال مهمة البحث عن الأدلة وتقديمها في مرحلة المحاكمة تقع بصفة أساسية على عاتق الادعاء والدفاع كما أن القاضي يتحمل جزء من هذه المسؤولية.

وفيما يتعلق بالجرائم الالكترونية فإن دور القاضي الجنائي يظهر من خلال توفير الأدلة الرقمية التي يستند اليها من أجل الوصول إلى الحقيقة، وله عدة طرق ووسائل إجرائية خولت له قانون للاستعانة بها في هذا المجال، كأن يوجه امر إلى مزود خدمة الأنترنت لتقديم البيانات المعلوماتية تخص مستخدم الإنترنت كمواقع الأنترنت التي زارها ووقت الزيارة والصفحات التي اطلع عليها والملفات التي جلبها والحوارات التي قام بها وشارك فيها والرسائل الالكترونية التي أرسلها واستقبلها، وغيرها من المعلومات المتعلقة بكل أفعال المستخدم عندما يتصل بالشبكة.

كما أن القاضي الجنائي يمكنه أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إلى داخله، كالإفصاح عن كلمة المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة، والتكليف بحل رموز البيانات المشفرة داخل ذاكرة الحاسوب والقاضي الجنائي يملك سلطة الأمر بتفتيش نظام الحاسوب بمكوناته المادية والمعنوية، وشبكات الاتصال متى رأى ضرورة لهذا الإجراء وله أن يتخذ أي إجراء ما إجراءات استخلاص الأدلة الرقمية المذكورة في الفصل السابق، لا سيما الإجراءات الحديثة.

ثانيا/ الدور الإيجابي للقاضي الجنائي في قبول الدليل الرقمي

بعد مرحلة البحث عن الدليل وتقديمه للمحكمة يأتي دور القاضي الجنائي للبحث عن الحقيقة من خلال التحقيق الذي يقوم به باستعمال كافة الصلاحيات المخول له قانونا، فلا يجوز له أن يقتنع بما يقدم له أطراف الدعوى من أدلة كل حسب مركزه القانوني، سواء

1 عائشة بن قارة مصطفى، المرجع السابق، ص 191.

كانت سلطة اتهام أو ضحية أو متهم، وإنما عليه أن يبحث بنفسه عن الأدلة التي تأثر في تكوين عقيدته واقتناعه وأن يستشير الأطراف إلى تقديم ما لديهم من أدلة، وتعد مرحلة قبول الدليل االرقمي الخطوة الثاني بعد البحث عن الدليل وتقديمه من سلطة الادعاء والمتهم والقاضي في حال ما إذا تطلب الفصل في الدعوى تحقيق الدليل بعينه وبهذا بهدف خلق حالة اليقين المطلوبة لدى القاضي كأساس لإصدار حكمه بالإدانة أو البراءة.

وتجدر الإشارة في هذا الشأن أن القاضي الجنائي يجب عليه في البداية مرحلة قبول الدليل التأكد من مدى مشروعية الدليل الالكتروني، وذلك قبل الوصول إلى المرحلة الأخيرة وهي مرحلة تقدير الدليل، لأن القاضي الجنائي لا يقدر إلا الدليل المقبول، والذي لا يكون كذلك إلا إذا كان مشروعا[1].

الفرع الثالث: حجية الدليل في نظام الإثبات الحر

إن نظام الإثبات الحر لا يحدد طرفا معينا في الاثبات، وإنما يترك الحرية للأطراف الدعوى لتقديم أدلة اثبات دعواهم، ويقوم القاضي الجنائي بتقييم تلك الأدلة ووزنها ومن ثم التوصل إلى قناعة معينة بخصوص تلك الأدلة، وإصدار حكمه في ظل القناعة التي توصل إليها، وإذا كان هذا الأمر ينطبق على الأدلة التقليدية فإن ذلك لا يثير أي اشكال إذا ما طبق على الأدلة الإلكترونية حيث يقدم أطراف الدعوى أدلتهم وتقدم سلطة الاتهام الأدلة، ومن ثم اصدار حكمه حسب القناعة التي توصل إليها بما يتميز به من موضوعية وحياد وكفاءة في اقناع القاضي الجنائي.

هذه الصفات التي يتميز بها دفاع البعض إلى اعتقاد أنه كلما اتسعت مساحة الأدلة العلمية ومنها الأدلة الالكترونية كلما تضاءل دور القاضي الجنائي في التقدير، لكن هذا الأمر يجب أن يكون مستبعدا، وذلك لأنه أثناء مناقشة الدليل العلمي، ومنه الدليل الالكتروني يجب التمييز بين أمرين مهمين، يتمثل الأول في القيمة العلمية القاطعة للدليل، والأمر الثاني هو الظروف والملابسات التي وجد فيها الدليل.

1 عائشة بن قارة مصطفى، المرجع السابق ص 195

فالقاضي الجنائي عند تقدير الدليل الرقمي لا يتطرق إلى القيمة العلمية للدليل، لأنها ثابتة وليس من اختصاصه مناقشة الأمور العلمية، وإذا استدعى الأمر ذلك في بعض القضايا المعقدة التي تحتاج إلى توضيح أو تفسير يستعين القاضي بذوي الخبرة والاختصاص، ويختار أحد الخبراء من قائمة الخبراء المحلفين والمعتمدين لدى المحاكم والمجالس القضائية لمعرفة حقيقة الدليل العلمي، وبإمكان القاضي أن لا يأخذ بهذا الدليل ويرفضه إذا كان لا يتناسب مع وقائع الدعوى المعروضة عليه وملابساتها، أما إذا اقتنع أن هذا الدليل وجد في ظروف تتلاءم مع وقائع الدعوى وملابساتها فإنه يستند عليه في تسبيب حكمه ويعتمد عليه كدليل اثبات في القضية المنشورة أمامه[1].

وعليه فإن حجية الأدلة الرقمية لا تثير صعوبات في حرية تقديم الأدلة لإثبات الجرائم الإلكترونية وفي حرية القاضي الجنائي أثناء تقديره لهذه الأدلة المستحدثة وذات الطبيعة الخاصة عن غيرها.

إن نظام الأثبات الحر أخذ بالأدلة الرقمية في الإثبات الجنائي تطبيقا للمبدأ الأساسي في هذا النظام المتمثل في حرية الاثبات، الذي يقوم على عدم تحديد طرق معينة للإثبات الجنائي مع الأخذ بعين الاعتبار الدور الإيجابي للقاضي الجنائي في تمحيص أي الأدلة المقدمة إليه ليأخذ بالدليل الذي يستقر في وجدانه ويبني على أساسه اقتناعه، ومنه يصدر حكمه بالبراءة أو الإدانة.

المطلب الثاني: الدليل الرقمي في نظام الإثبات المقيد

يقوم نظام الإثبات المقيد على مبدأين رئيسيين، مبدأ تحديد أدلة الإثبات من قبل المشرع ومبدأ اقتناع المشرع بدلا من اقتناع القاضي، فالمشرع هو الذي يحدد أدلة الإثبات مسبقا وبصفة حصرية ولا يجوز لقاضي الخروج عن تلك الأدلة المحددة له، ويقتصر دوره على مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون، ولا سبيل لأي دليل لم ينص عليه القانون صراحة ضمن الأدلة المحدد حصرا[2].

1 سامي جلال فقي حسين، المرجع السابق، 79، 80.

2 عائشة بن قارة مصطفى، مرجع سابق، ص 204.

وتكون أدلة الاثبات في نظام الإثبات المقيد محددة مسبقا بقواعد قانونية ثابتة تبين للقاضي وسائل الإثبات المقبولة، ويقتصر دوره على مراعاة توفر دليل الاثبات، فإذا لم يتوفر الدليل فإنه لا يجوز أن يحكم بالإدانة، حتى وإن كان لديه اقتناع شخصي بأن المتهم الماثل أمامه هو الشخص الذي ارتكب الجريمة، أي أن هذا النظام يحدد طرق الإثبات الجائز قبولها أمام القضاء، كالكتابة والبينة والقرائن، وهذا النظام متبع من طرف الدول الاجلوساكسونية.

إن المشرع في النظام المقيد يحدد الطريقة التي يتم بها إثبات الحق كما أنه لا يجوز للخصم إثبات الحق الذي يدعيه بأي طريقة أخرى، وعلى القاضي أن يتقيد بطرق الإثبات التي يفرضها عليه القانون، ويلتزم بها وبالقيمة التي يعطيها القانون لكل دليل من أدلة الإثبات فالقاضي في ظل هذا النظام دوره سلبي تماما، يقتصر على تقدير ما يقدمه الخصوم من أدلة قانونية وليس له أن يكمل الأدلة إذا كانت ناقصة[1].

أما فيما يخص الدليل الرقمي في ظل النظام المقيد فإنه يجب توضيح مشكلة قبول الدليل وكذا القواعد التي تحكم الإثبات في ظل هذا النظام.

الفرع الأول: أساس مشكلة قبول الدليل الرقمي في ظل النظام المقيد

يطرح على مستوى النظام المقيد إشكالية مدى قبول الدليل الرقمي في مجال الإثبات الجنائي لتعارضه مع أحد أهم مبادئ الإثبات التي تحكم هذا النظام، والمتمثلة في تعارض الدليل الرقمي وقاعدة استبعاد شهادة السماع، وتعارض الدليل الرقمي وقاعدة المحرر الأصلي، ومادام الدليل الرقمي في أصله يمثل شهادة سماع، على أساس أنه يتكون من جمل وكلمات أدخلها شخص إلى جهاز الكمبيوتر سواء تمت معالجة تلك البيانات أم لا، ومن شأن ذلك أن يثير اعتراض على قبول مستندات المطبوعة التي يخرجها الحاسوب في الإثبات أمام القضاء الجنائي.

1 سامي جلال فقي حسين، نفس المرجع، ص 91.

أما بالنسبة للقواعد المتعلقة بكيفية تقديم الأدلة للقضاء وتحديد مدى قبولها، كأدلة الإثبات في المواد الجنائية، هناك قاعدة الدليل الأفضل والمحرر الأصلي ولو تم تطبيق هذه القاعدة من حيث المبدأ على الدليل الإلكتروني لكان مستبعد كوسيلة اثبات في هذا النظام.

والدليل الرقمي في هذه الحالة على أنه مجرد مخرجات طابعة ملف الكتروني مخزن على حاسوب لا يعد أصليا، وسبب ذلك هو الطريقة التي يعرض بها الدليل الرقمي أمام القضاء في شكل مستندات مطبوعة أو كبيانات معروضة على شبكة الكمبيوتر، إلا أن وأصل الدليل الإلكتروني هو عبارة إشارات إلكترونية ونبضات ممغنطة، وما يقدم إليهم من وثائق أخرجها الحاسوب إلا نسخة على الأصل مما يجعله دليل ثانوي لا أصلي، وهذه النسخ لا تظهر جميع البيانات المتضمنة في الدليل الأصلي، مثل الوثيقة المطبوعة من وثائق الميكرو سوفت لا تظهر جميع التعديلات والملاحظات في حالة تغيير الوثيقة الأصلية، كما أن الدليل الأصلي في بعض العمليات التي تجرى عن طريق الحاسوب، يمكن أن ينعدم وجودها كما هو الحال في التحليلات، أو الإسقاطات المعالجة[1]، مما يؤدي إلى طرح العديد من التساؤلات حول موقع الدليل الرقمي في ظل هذا النظام.

الفرع الثاني: موقع الدليل الرقمي في نظام الإثبات المقيد

ولمعرفة موقع الدليل الرقمي ضمن أهم قواعد نظام الإثبات المقيد وما إذا كان هذا الدليل متماشيا مع هذه القواعد مقبولا أو مستبعدا كدليل اثبات جنائي من خلال الآتي:

أولا/ تعارض الدليل الرقمي وقاعدة استبعاد شهادة السماع

ويقصد بشهادة السماع أو كما تسمى التسامع عن الغير بأنها بيان أو تقرير شفوي أو كتابي يحدث خارج المحكمة الذي يقدم أمامها بهدف اثبات واقعة حدثت خارج الجلسة.

ويرى بعض الفقهاء أن شهادة السماع نوع من الشهادة غير المباشرة، وانقسمت هذه الأخيرة إلى نوعين الشهادة السماعية، والشهادة بالتسامع، وتعني الأولى أن شخص سمع من الآخر معلومات عن الواقعة محل التحقيق. أما الشهادة الثانية فهي مجرد ترديد لإشاعة

1 عائشة بن قارة مصطفى، مرجع سابق، ص 197.

متداولة بين الناس دون الجزم بصحتها، ويرجع السبب في التمييز بين النوعين في أن النوع الأول من الشهادة له القوة في الإثبات[1].

وما يهم في نطاق الدليل الالكتروني هو شهادة السماع التي عرفت في الغالب على أنها الشهادة التي أدلى بها شاهد قد سمعها ولم يشارك في وضعها بإحدى حواسه، أي هي دليل شفوي يقدمه شخص ما إلى المحكمة، محمول على أنه عبارات أو سلوك صدر من آخر خارج المحكمة، حيث يتوقف قبوله أو استبعاده على مقدار الثقة التي تتوفر لدى المحكمة في الشخص الذي أدلى بها، والأصل في شهادات السماع أنها لا يعتمد عليها كدليل اثبات يستند عليه القاضي للفصل في الدعوى المطروحة امامه ويعود السبب في ذلك لعدم الثقة في الشخص الذي يدلي بها باعتباره لا يؤدي اليمين القانونية أمام المحكمة إلا أن هذه القاعدة لها حالات استثنائية يتم فيها قبول شهادة السماع كدليل اثبات[2].

وتتمثل أهم هذه الحالات في أقوال المجني عليه التي نطق بها قبل وفاته، اخبار أحد أعضاء الاتفاق الجنائي، التسجيلات الرسمية، البيانات والمعلومات التي يتم الحصول عليها من الكمبيوتر التقرير التلقائي.

ويتبن من خلال ما سبق أن الدليل الرقمي يدخل ضمن طائفة الحالات الاستثنائية عن قاعدة شهادة السماع، ليصبح هذا الدليل مقبولا في الإثبات الجنائي، إلا أن هذا الأمر لا ينطبق على جميع أنواع سجلات الحاسوب، كما معلوم أن تقسيمات الأدلة الالكترونية إلى ثلاث أنواع يتمثل النوع الأول في سجلات الحاسوب المخزنة على بيانات بشرية مثل المخرجات وبرنامج الكتابة من الكمبيوتر وهذا النوع يعتبر شهادة سماع ككل التقارير التي يسجلها الإنسان على الأجهزة المتعلقة بالكتابة.

أما النوع الثاني فهي سجلات الحاسوب المتوالدة وهذا النوع فإن الجهاز فيها هو الذي يدون البيانات التي تصلح أن تقدم مباشرة إلى المحكمة، وبالتالي فهي لا تعتبر شهادة سماع وتحدد قيمتها الثبوتية على أساس طريقة عمل جهاز الكمبيوتر.

1 العربي شحط عبد القادر، نبيل صقر،الإثبات في المواد الجزائية، دار هدى للطباعة والنشر والتوزيع، الجزائر، ص101.

2 بن فردية محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي، مقال في المجلة الأكاديمية للبحث القانوني الصادرة عن كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة عبد الرحمان ميرة، بجاية، الجزائر، جانفي 2014 ص 287.

أما بالنسبة للنوع الثالث فهو يجمع بين التدخل الإنساني ومعالجة الكمبيوتر فهي لا تعتبر من شهادة السماع رغم أن فيها جزءا يعد شهادة سماع.

ثانيا/ تعارض الدليل الرقمي وقاعدة الدليل الأفضل:

ويقصد بهذه القاعدة اثبات محتويات كتابة أو سجل أو صورة، فإن أصل الكتابة أو السجل أو الصورة يكون مطلوبا، بمعنى لا يجوز تقديم الصورة لإثبات محتوى الأصل بصفة عامة حين يقدم أحد الأطراف، تأييدا لدعواه، دليلا يستند إلى عدة دعائم يجب عليه أن يقدم أفضل نموذج، وهو ما يعني أن تكون الأدلة الواجب تقديمها أولية وليست ثانوية لا بديلة، وأن يكون الدليل المقدم هو الأفضل وما يتاح الحصول عليه بالنسبة لطبيعة القضية وظروفها وملابساتها[1].

بالنسبة لكيفية تقديم الأدلة الالكترونية وعرضها على القضاة تحكم قاعدة الدليل الأفضل للنظم الإنجلوساكسونية" أي عدم الأخذ بالنسخ المطابقة للأصل" وإذا ما طابقنا هذه القاعدة على الدليل الالكتروني فإنها ستؤدي حتما الى استبعاده عن النطاق الجنائي، باعتبار مخرجات الحاسوب نسخ غير أصلية، وذلك لأن عرض الدليل الالكتروني أمام القضاء يكون في شكل مستندات مطبوعة أو بيانات معروضة على الشاشة، والأصل أن بيانات الحاسوب هي مجرد إشارات ونبضات ممغنطة غير مرئية للعين البشرية، مما لا يتيح للقضاة وضع اليد عليها ومعاينتها، وهو ما يجعل منها نسخا أي أدلة ثانوية لا أصلية[2].

الفرع الثالث: حجية الدليل الرقمي في نظام الإثبات المقيد

في ظل نطام الإثبات المقيد فإن الدليل الرقمي لا يكون مقبولا أمام القضاء ما لم ينص عليه القانون حيث يتوجب عليه تحديد هذا النوع من الأدلة سلفا وبدقة، ويتوجب على القاضي الجنائي أن يأخذ بهذه الأدلة متى توفرت فيها شروط الدليل الصحيح، وقد نظمت العديد من التشريعات التي تأخذ بها النظام هذه الأدلة " الأدلة الالكتروني " وحددتها بدقة

1 محمد بن فردية، مرجع سابق، ص 288.

2 عائشة بن قارة مصطفى، المرجع السابق، ص 207.

فالمشرع لعب دورا هاما في تحديدها، ويقتصر دور القاضي الجنائي على تفحص الأدلة لمعرفة ما إذا كانت صحيحة من الناحية القانونية[1].

وقبول الدليل الرقمي في هذا النظام له شروط نص عليها المشرع الإنجليزي حيث تعاقبت القوانين، في إنجلترا التي أصبحت تسمح بالدليل الالكتروني كقانون الاثبات الجنائي سنة 1968 وكذا القانون الصادر في سنة 1988 المتعلق بقانون العدالة الجنائية وكذا قانون الشرطة والإثبات الجنائي الصادر سنة 1984 وترتب على ذلك قبول المشرع الإنجليزي للدليل الالكتروني كدليل في الإثبات الجنائي، وهو ما يعد خروجا عن الأصل العام الذي تبناه القانون الإنجليزي في عدم قبول الشهادة السماعية، إلا أن هذا القبول مقيد بشروط معينة تمنتها المادة 69 من قانون 1984 والتي تنص عدم وجود أسباب معقولة للاعتقاد بأن البيان يفتقر إلى الدقة بسبب الاستخدام غير مناسب أو الخاطئ للحاسوب، التأكد من أن الحاسوب يعمل بصفة سليمة وإذا لم يكن كذلك فإن أي جزء لم يعمل فيه بصورة سليمة أو كان عاطلا عن العمل لم يكن ليأثر في إخراج مستندات أو دقة محتوياته[2].

الوفاء بأي شروط متعلقة بالمستند محددة طبقا لقواعد المحاكمة المتعلقة بالطريقة أو الكيفية التي يجب أن يقوم بها المعلومات البيان المستخرج عن طريق الحاسوب.

تجدر الإشارة إلى أن صحة الدليل الالكتروني تتوقف على صحة برنامج التشغيل الذي يعمل الكمبيوتر بحسب تعليماته من حق المتهم الدفع بكون أن برنامج التشغيل لا يعمل بشكل صحيح أو منتظم إذا ما تأكد من إثبات ذلك.

كما أن القانون الإنجليزي لسنة 1984 تضمن توجيهات لكيفية تقدير قيمة أو وزن البيان المستخرج عن طريق الحاسوب فأوصت المادة 11 من الجزء 02 من الملحق الثالث من القانون المذكور بمراعاة كل الظروف عند تقديم البيانات الصادرة عن الحاسوب والمقبولة في الإثبات طبقا للمادة 69 من هذا القانون.

وعليه فإن الدليل الالكتروني في ظل النظام المقيد مقبول ويأخذ به باعتباره دليل اثبات جنائي وله قوة ثبوتية أيضا، إلا أن الأخذ بالدليل الالكتروني في هذا النظام تعترضه

1 أشرف عبد القادر قنديل، المرجع السابق، 204.

2 سامي جلال فقي حسين، المرجع السابق، ص 91.

عدة مشاكل، خاصة فيما يتعلق بقواعد هذا الأخير وأهمها قاعدة استبعاد شهادة السماع، إلا أنه يعتبر شهادة سماع كما سبق بيانه، قاعدة الدليل الأفضل كذلك.

إلا أن غالبية التشريعات وحتى تتماشى مع هذا النوع الجديد والمستحدث من الأدلة أوردت استثناءات على هذه القواعد وتم قبول الدليل الالكتروني والأخذ به في ظل هذا النظام مع وضع شروط الواجب توفرها.

ومما سبق ذكره يمكن القول أن الدليل الالكتروني له حجية وقو ثبوتية بالنسبة للتشريعات التي تأخذ بنظام الإثبات المقيد، وقد حاولت بشكل كبير إعطاء القوة الثبوتية لهذا النوع من الأدلة، بالرغم من أن الدليل الالكتروني تتعارض طبيعته مع أهم قواعد نظام الاثبات الجنائي المقيد، إلا أنه من الضروري الخروج عن الأصل العام في هذه القواعد وذلك بوضع استثناءات عليها حتى يكون في الإمكان الأخذ به، وهذا ما تفرضه التكنولوجيات الحديثة في إثبات الجريمة الالكترونية الامر الذي يستوجب مواكبتها[1].

المطلب الثالث: الدليل الرقمي في نظام الإثبات المختلط

نظام الاثبات المختلط هو نظام وسط ما بين نظام الاثبات الحر ونظام الاثبات المقيد وتتراوح أحكامه بين التقييد والاطلاق. إذ يسعى للجمع بين مفهومي النظامين للوصول إلى الحقيقة، ولكي يتسنى للقاضي اصدار حكمه لابد عليه أن يكون مقتنعا اقتناعا شخصيا، وأن يحوز القناعة القانونية كما أقرها المشرع[2].

فهذا النظام يتجنب ما وجه من انتقاد للنظام الحر خشية من تعسف القاضي الجنائي وخروجه عن جادة الصواب، وذلك بتحديد طرق الاثبات التي يلجأ اليها، ويتجنب ما وجه من انتقادات لنظام الإثبات المقيد، والذي جعل دور القاضي سلبي محضا في عملية الاثبات وذلك عن طريق إعطاء القاضي الحرية في تقدير ما يعرض عليه من أدلة ثبوتية في الدعوى المطروحة أمامه.

أبرز نموذج لنظام الاثبات المختلط هو الذي روبسيير في اجتماع الجمعية التأسيسية الفرنسية عام 1791 المتكون من جزئين يتمثل الجزء الأول في عدم الحكم

1 ربيعي حسين، المرجع السابق، ص 275.

2 سامي جلال فقي حسين، المرجع السابق، ص 81.

بالإدانة على المتهم إذا لم تتوفر ضده أدلة حددها القانون، أما الجزء الثاني يكمن في عدم الحكم بإدانة المتهم حتى إذا توفرت أدلة قانونية، لكن هذه الأدلة لم تحقق قناعة القاضي[1].

ومن التشريعات التي أخذت بهذا النظام القانون الاجرائي الياباني الذي حدد سلفا أدلة ووسائل الاثبات من جهة وأخذ بقاعدة الاقتناع الذاتي للقاضي من جهة أخرى.

الفرع الأول: مبدأ نظام الاثبات المختلط بالنسبة للدليل الرقمي

إن هذا النظام يقوم على تحديد أدلة الاثبات سلفا من قبل المشرع بحيث يتقيد بها القاضي ويحدد قيمتها وحجيتها وله كامل الحرية في تقدير الدليل المناسب في القضية المعروضة أمامه.

وفيما يتعلق بالدليل الرقمي من ناحية تحديد الأدلة مسبقا فقد سبقت الإشارة إلى عدم نص التشريعات عليه باعتباره دليل مستحدث لجريمة مستحدثة، إلا أن هذه التشريعات وفي إطار مواكبة التكنولوجيا وتماشيا مع هذا النوع المستحدث من الأدلة والجرائم، فقد قامت بوضع استثناءات حتى تشمل هذا الدليل في تشريعاتها، وبالنسبة لمبدأ حرية القاضي الجنائي لا يثير اشكال باعتبار أن كل الأدلة الجنائية خاضعة لتقدير وحرية القاضي الجنائي والدليل الالكتروني دليلا من أدلة الاثبات الجنائي، فهو خاضع لحرية القاضي وتقديره واقتناعه كغيره من الأدلة بمعنى أن له دور إيجابي في ظل هذا النظام[2].

ونظام الاثبات المختلط في إطار التوفيق بين نظام الاثبات المقيد والحر أخذ صورتين تتمثل الصورة الأولى في الجمع بين الحقيقتين في كل الحالات سواء في الإدانة أو البراءة، ولكن في هذه الحالة تطرح مشكلة تطابق قناعة القانون مع قناعة القاضي والحال كذلك فإن القاضي لا يمكنه الفصل في القضية لا بالإدانة ولا بالبراءة، وفي إطار هذا المشكل اقترح نظام الاثبات المختلط حلا وسطا ومؤقت مفاده أن القاضي ما عليه إلا أن يحكم بعدم ثبوت التهم حتى تتوقف المحاكمة ويستعيد المتهم حريته، وإلا يحكم بالبراءة في نفس الوقت ولكن يؤجل الحكم مع بقاء الدعوى أمام القضاء معلقة.

1 نفس المرجع، ص 93.

2 سامي جلال فقي حسين، المرجع السابق، ص 93.

أما الصورة الثانية: فتتمثل في وجوب الجمع بين القناعة القانونية وقناعة القاضي في حالة الإدانة فقط، وقد دافع البعض عن إمكانية توافق هذه الصورة في الجمعية التأسيسية الفرنسية في القول: " أن المتهم لا يمكنه اعتباره مدان مادامت الأدلة القانونية لم تتوافر أو إذا وجدت ولكنها تخالف اقتناع القاضي الشخصي، أي أن نظام الاثبات المقيد في هذه الصورة يكون له دور سلبي أكثر[1].

الفرع الثاني: حجية الدليل الرقمي في نظام الإثبات المختلط

في ظل نظام الإثبات المختلط يحدد المشرع الأدلة الالكترونية سلفا عن طريق اصدار تشريع بهذه الأدلة يحدد فيه الأدلة المقبولة ومن ثم فإنه يمنح القاضي الحق في تقدير هذه الأدلة المعروضة أمامه في القضية التي ينظرها، له الحق في استبعاد أي دليل لا يقتنع به والأخذ بدليل آخر يقتنع به، فعلى سبيل المثال لو حدد التشريع المنظم للأدلة الالكترونية أن الأدلة المقبولة هي الأقراص المغناطيسية والمخرجات الورقية، وكان هذان الدليلان معروضين أمام القاضي الجنائي في قضية ما فيحق له الأخذ بأحدهما، والذي يقتنع به ويطمأن له، ويستبعد دليل آخر[2].

فالقانون الإجرائي الياباني مثلا حصر طرق الإثبات المقبولة في أقوال متهم وأقوال الشهود والقرائن والخبرة، أما بالنسبة للأدلة الالكترونية، فقد قرر الفقه الياباني أن السجلات الالكترومغناطيسية تكون غير مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة إلا إذا تم تحويلها إلى صور مرئية ومقروءة عن طريق مخرجات الطابعة لمثل هذه السجلات، وفي مثل هذه الحالة يتم قبول هذه الأدلة، وهي الأدلة الالكترونية سواء كانت هي الأصل أو كانت نسخة من هذا الأصل.

كما نص قانون الإجراءات الجنائية التشيلي من خلال نص المادة 113، على امكاني استخدام الأفلام السينمائية والفوتوغراف والنظم الأخرى بإنتاج الصور والصوت والاختزال وبصفة عامة أي وسيلة أخرى قد تكون ملائمة وثيقة الصلة، تؤدي إلى استخلاص المصداقية، يمكن أن تكون مقبولة كدليل إثبات، ويرى الفقه التشيلي أن الدليل الناتج عن

1 مبروك نصر الدين، محاضرات في الاثبات الجنائي، الجزء الأول، الطبعة الثالثة، دار هومة للطباعة النشر والتوزيع، الجزائر، 2009، ص 64

2 سامي جلال فقي حسين، المرجع السابق ص 97.

الحاسوب والأنترنت أو الدليل الالكتروني يمكن أن يكون مقبولا في المحكمة كدليل كتابي أو مستندي كالنظم الحديثة الأخرى لجمع وتسجيل المعلومات، وحجية الفقه التشيلي تستهدف توسيع نطاق الوسائل العلمية الحديثة في الاثبات لتغطي العناصر الاثباتية الناتجة عن الجرائم المعلوماتية[1].

ومنه نقول أن الدليل الالكتروني في ظل نظام الاثبات المختلط يعمل على تحديد نظام أدلة الإثبات الجنائية من جهة، والدليل الالكتروني حدد كاستثناء على هذه القاعدة، كما أنه يولي أهمية كبيرة في سلطة القاضي الجنائي في الأخذ بالأدلة وتقديرها، الأمر الذي يسهل الأخذ بالدليل الإلكتروني على أساس حرية القاضي الجنائي في قبول أي دليل يراه مناسبا استبعاد الدليل الذي لا يراه مناسبا.

المبحث الثاني: حجية الدليل الرقمي أمام القضاء الجنائي

مما لا شك فيه أن التطورات التكنولوجية الحديثة قد أحدثت تغيرات جذرية في وسائل الاثبات الجنائي، وأصبحت الأدلة الالكترونية حجة يعول عليها القضاء كأدلة يؤسس عليها الأحكام بالبراءة أو الإدانة في العديد من القضايا خاصة في الجرائم الالكترونية، ومرد ذلك لطبيعتها العلمية والتقنية، إذ يعد قبول الدليل الخطوة الإجرائية الأولية التي يمارسها القاضي تجاه الدليل الجنائي بصفة عامة والدليل الالكتروني بصفة خاصة، بالإضافة إلى أن القاضي الجنائي حر بالأخذ بالأدلة الالكترونية.

لدراسة الدليل الالكتروني من حيث حجيته أمام القضاء الجنائي، المتمثل بدوره في القاضي الجنائي قسمنا هذا المبحث إلى مطلبين المطلب الأول السلطة التقديرية للقاضي الجنائي في القبول والاقتناع بالدليل الالكتروني، والمطلب الثاني ضوابط قبول واقتناع القاضي الجنائي بالدليل الالكتروني.

1 علي حسين محمد الطوالبة، المرجع السابق ص 198.

المطلب الأول: السلطة التقديرية للقاضي الجنائي في قبول الدليل الرقمي

يخضع الدليل الرقمي لمبدأ عام في الإثبات الجنائي وهو حرية القاضي الجنائي في الاقتناع الشخصي، وحريته في هذا المقام بالغة السعة فهو وحده الذي يقر قيمة الدليل الرقمي بحسب ما تحدثه من أثر في وجدانه من ارتياح واطمئنان، وتعاظم دور الاثبات العلمي مع ظهور الدليل الرقمي المطلوب للأثبات في الجرائم الالكترونية، مما جعل القاضي يضطر للتعامل مع هذا النوع المستحدث من الأدلة الضرورية لكشف أنماط جديدة من الجرائم، في مقابل نقص الثقافة المعلوماتية من جهة، والقيمة العلمية التي يتمتع بها هذا الدليل من جهة أخرى، وهذا الأمر تنجر عنه عدة مشاكل، خاصة فيما يتعلق بالدليل الرقمي، مما يؤدي إلى نقص قيمته الأمر الذي يؤدي إلى نقص الاعتماد عليه في الجرائم الالكترونية

وعلى ضوء ذلك سنتطرق إلى الطبيعة العلمية للدليل الالكتروني وأثرها على اقتناع القاضي الجنائي، كما سيكون الحديث على مشكلات الدليل الالكتروني وتأثيرها على اقتناع القاضي الجنائي.

الفرع الأول: الطبيعة العلمية للدليل الرقمي وأثرها على اقتناع القاضي

يعد الدليل الرقمي السلطة التقديرية للقاضي الجنائي في القبول والاقتناع من تطبيقات الأدلة العلمية الجنائية الموثوقة بسبب احتلاله مراتب أفضل دليل لإثبات الجرائم الالكترونية، وهو ما فرض على القاضي الجزائي التعامل معه رغم نقص ثقافته المعلوماتية من جهة والقيمة العلمية التي يتمتع بها الدليل العلمي من جهة أخرى.

وهذا الأمر ينتج عنه عدة مشاكل يثيرها هذا الدليل مما يؤدي إلى نقص قيمته ونقص الاستناد عليه في اثبات الجرائم الالكترونية.

إن الطبيعة العلمية للدليل الالكتروني لها أهمية بالغة في الإثبات الجنائي ولذلك لا بد من معرفة معنى الاقتناع القضائي، ثم بيان قيمة الدليل الالكتروني في الإثبات الجنائي[1].

1 أشرف عبد القادر قنديل، المرجع السابق ص 221.

فبالنسبة لمعنى الاقتناع القضائي فهو الايمان العميق والركون إلى صحة الوقائع التي يقدمها الأطراف المتنازعة والتي اعتمدها القاضي وتنتج عنها آثار عميقة في نفسيه تتركه يصدر حكمه عن قناعة وحرية، واحساس كبير بإصابته في حكمه[1] .

أما نطاق تطبيق مبدأ الاقتناع القضائي فقد ثار خلاف حوله فهناك من يرى أنه يمتد إلى كافة أنواع المحاكم الجنائية سواء كانت محاكم جنح مخالفات أو جنايات والمشرع الجزائري لم ينص على هذا الأمر بخلاف المشرع الفرنسي.

وهناك من يرى أن هذا المبدأ وجد أصلا ليطبق أمام قضاة الحكم بل يشمل مراحل التحقيق الابتدائي وقضاة التحقيق والإحالة فهم أيضا يقدرون مدى كفاية الأدلة ويخضعون في ذلك لضمائرهم واقتناعهم الذاتي فحسب[2].

أولا/ قيمة الدليل الرقمي كدليل علمي

إن الدليل الالكتروني لا تختلف قيمته ولا تزيد حجيته عن غيره من الأدلة، وعليه قد يؤسس القاضي اقتناعه على الدليل الرقمي، كما يستطيع إبعاده، وبالتالي لا يجوز مطالبه القاضي أو الزامه بالاقتناع بالدليل الإلكتروني حتى ولم يكن في الدعوى دليل غيره.

وتجدر الإشارة إلى أن الفقه الفرنسي، تناول حجية ومخرجات الكمبيوتر في المواد الجنائية في مسألة قبول الأدلة المتحصلة من الأدلة العلمية، وأقر بأن لها قيمة الأدلة الأخرى ويمكن الاطمئنان اليها وتكون صالحة في الإثبات أمام القضاء الجنائي.

كما أن أغلب التشريعات اللاتينية وإن كانت تجمع على قبول الدليل الرقمي فإنها تختلف على كيفية وطريقة تقديمه أمام المحكمة، ويبقى ما يتميز به الدليل العلمي من موضوعية وحياد وكفاءة يجعل اقتناع القاضي الجنائي أكثر حزما ويقينا ويساعد في تقدير الأخطاء القضائية والتوصل بدرجة كبيرة نحو الحقيقة.

هذه سمات التي يتمتع بها تدفع إلى الاعتقاد بأنه بقدر اتساع مساحة الأدلة العلمية بما فيها الدليل الالكتروني بقدر يتضاءل دور القاضي الجنائي في التقدير لاسيما في

1 سامي جلال فقهي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر، 2014، ص 280.
2 عائشة بن قارة مصطفى، المرجع السابق، ص 245.

ظل نقص الثقافة الفنية، حيث يصبح الخبير هو المسيطر على العملية الإثباتية، وهذا الأمر لا يثير أي مشكل إذا سلمنا بأن نظام الإثبات يقوم على التوازن بين الإثبات العلمي والإثبات القضائي.[1]

ثانيا/ تقدير القضاء للدليل العلمي.

من أهم النتائج التي تترتب على مبدأ حرية القاضي في تقدير الأدلة بما في ذلك الدليل الرقمي وموازنتها وفقا لما يمليه عليه وجدانه، دون أن يخضع في ذلك لرقابة المحكمة العليا غير أنه يبقى مقيد بضرورة تأسيس قناعته على الجزم واليقين دون الضن والاحتمال وأن يكون متوائما مع مقتضيات العقل والمنطق إن سلطة القاضي الجزائي في تقدير الدليل الرقمي يحكمه مبدأ الاقتناع القضائي والذي يؤدي إلى نتيجتين هما:

حرية القاضي في قبول الأدلة وحريته في تقديرها، إذ يجوز له الاستناد إلى الدليل الرقمي لإثبات الجرائم خاصة ما تعلق منها بالجرائم المعلوماتية، حيث أن المشرع حسم هذه المسألة بتحديد النموذج القانوني للدليل الخاضع لتقدير القاضي، فمتى توافرت شروط هذا النموذج طبقا لمبدأ الشرعية الإجرائية، وجب للقاضي إخضاعه لعملية تقديره وهي مسألة موضوعية بحتة، وله أن يمارس سلطته التقديرية فيها، بل هي المجال الطبيعي لهذه السلطة، إذ أنها تتعلق بقيمة الدليل في الإثبات وصولا للحقيقة.

وللقاضي الجنائي أن يستبعد في مجال تقديره للدليل ما لم يطمأن اليه عندما يمارس سلطته في الدعوى موضوعيا[2] .

فالدليل العلمي ليس آلية معدة لتقرير اقتناع القاضي لمسألة غير مؤكدة بل هو دليل اثبات قائم على أساس من العلم والمعرفة وللقاضي أنظر اليه على ضوء الظروف والملابسات المحيطة[3].

1 هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتب اللالات الحديثة، أسيوط، 1994 ص 58

2 جابري عبد المجيد، دراسة قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دون طبعة، دار هومة الجزائر، 2012، ص 122

3 عائشة بن قارة مصطفى، المرجع السابق، ص 246.

الفرع الثاني: إشكالات الدليل الرقمي وأثرها على اقتناع القاضي

يثير الدليل الرقمي العديد من الإشكالات وهي في الحقيقة تتعلق بطبيعته التكوينية من جهة وبإجراءات استخلاصه من جهة أخرى، وهذه المشكلات تضعف من قيمته في مجال الإثبات الجنائي . إن لم يتم وجود حلول بشأنها . وفي هذا الإطار يمكن تقسيمها إلى مشكلات موضوعية وأخرى إجرائية.

أولا/ المشكلات الموضوعية للدليل الرقمي

وهي غالبا ما تتعلق بطبيعة الدليل الرقمي في حد ذاته، وذلك بسبب الخصائص التي يتميز بها والتي يمكننا حصرها فيما يلي:

إن اختلاف الدليل الرقمي عن الآثار المادية الناتجة عن الجرائم التقليدية التي يسهل على رجال العدالة اثباتها، وطبيعته كونه عبارة عن نبضات الكترونية غير مرئي مخزن في نظام الحاسوب، وإضافة إلى أنه غالبا ما يكون مرمزا أو مشفر ويمكن تعديله أو التلاعب به، مما يقطع الصلة بين المجرم وجريمته، هذا ما يشكل عائقا أمام رجال التحري والتحقيق خاصة وأنهم اعتدوا على الاثبات المادي للجرائم[1].

إن مشكلة الأصالة في الدليل الالكتروني وما لها من طابع افتراضي لا يرقى إلى مستوى الأصالة في الدليل المادي، التي تعبر عن وضعية مادية ملموسة أثارت العديد من المشكلات من حيث مدى الاعتداد بنسخة التي تشكل دليلا كاملا، ونجد أن موضوع الأصالة على مستوى القانون جعل المشرع يعتمد على منطق افتراض أصالة الدليل الرقمي وقد تضمن القانون الفيدرالي للولايات المتحدة الأمريكية نصا صريحا على قبول الدليل الالكتروني، باعتباره مستندا أصليا وهذا استثناء مادام أن البيانات صادرة عن الكمبيوتر أو جهاز مماثل له، سواء كانت هذه البيانات مطبوعة أو مسجلة على دعامات أخرى تعبر عن البيانات الأصلية بشكل دقيق ومنه تتساوى الكتابة المادية من حيث الأصالة مع مخرجات الحاسوب رغم أن هذه الأخيرة مجرد نسخ من أصل موجود رقميا في الحاسوب أو الأنترنت[2]

1 عائشة بن قارة مصطفي، مرجع سابق، ص 252.

2 المرجع نفسه، ص 252، 253

كما أن مشكلة الطبيعة الديناميكية للدليل الرقمي الذي يتنقل عبر شبكات الاتصال بسرعة فائقة، مع إمكانية تخزين المعلومات أو البيانات في الخارج بواسطة شبكة الاتصال عن بعد يؤدي إلى صعوبة ضبط الأدلة الالكترونية وتعقبها، الأمر الذي يستوجب القيام بأعمال إجرائية خارج حدود الدولة التي ارتكبت فيها الجريمة، كتفتيش نظام الحاسوب أو معاينة مواقع الأنترنت المخالفة، وهذا يصطدم كله مع مشكل الحدود والولايات القضائية[1]

وهذا راجع إلى أن هذه الإجراءات فيها مساس بسيادة الدول المقصودة، وهو ما ترفضه غالبية الدول، لذلك أبرمت العديد من الاتفاقيات والمعاهدات الدولية في مجال التعاون الدولي بهدف التقارب بين القوانين الجنائية، خاصة في إطار مكافحة الجرائم العالمية ومنها الجريمة الإلكترونية[2].

ثانيا/ المشكلات الإجرائية للدليل الرقمي

وتتمثل في ارتفاع تكاليف الحصول على هذا الدليل ونقص الخبرة الفنية والتقنية لدى سلطات الاستدلال والتحقيق والقضاء في مجال تقنية المعلومات.

أن من أهم المشكلات الإجرائية للدليل الرقمي ارتفاع تكاليف الحصول عليه واستخلاصه في أغلب الأحيان يتم اللجوء إلى الخبرة للتعامل مع هذا الدليل الفني المتواجد في مجال التكنولوجيا المعلوماتية والإنترنت، فالخبرة لها دور لا يستهان به خاصة مع نقص معرفة رجال القانون للجوانب التقنية في الجرائم الالكترونية، ولكن هذه الخبرة في المقابل تشكل عبء بسبب حجم وضخامة المصاريف التي يتم إنفاقها في سبيل الحصول على الدليل الإلكتروني فالإشكال الأساسي هنا يتعلق بطبيعة الدليل الرقمي وما يتطلب اثباته من تكاليف باهضه خاصة أمام غياب مؤسسات متخصصة في هذا الشأن لاسيما في الدول العربية التي تضطر للجوء للمؤسسات الأجنبية مما يجعل التكاليف خاضعة للسعر العالمي المقرر في اللوائح المالية لتلك المؤسسات[3].

1 أشرف عبد القادر قنديل، المرجع السابق، ص 227.

2 عائشة بن قارة مصطفى، نفس المرجع، 253، 254

3 أشرف عبد القادر قنديل مرجع سابق، 227.

كما تعد نقص المعرفة التقنية عند رجال القانون من المشكلات الإجرائية للدليل الرقمي نظرا للطبيعة الخاصة التي يتمتع بها، أثر على عمل الجهات المكلفة بالتحقيق والمحاكمة كون أن الكشف عن الجرائم الإلكترونية وإثباتها يستلزم اتباع استراتيجيات ومهرات خاصة في سبيل مواجهة تقنية الحاسوب وشبكاته، بحيث تتعقد التقنيات المرتبطة بارتكاب تلك الجرائم، الأمر الذي يستوجب معه الاعتماد على تقنيات جديدة، تتماشى مع طبيعة هذه الجرائم وهذا بهدف معرفة نوع الجريمة المرتكبة، وشخصية مرتكبيها وكيفية ارتكابها وضبط الجاني والحصول على أدلة إدانته[1].

وبسبب هذا الأمر فإن الجهات المكلفة بالقبض والتحقيق تجد صعوبة كبيرة في التعامل مع هذه الجرائم عن طريق الوسائل الاستدلالية والإجراءات التقليدية، ولهذا كثيرا ما تفشل جهات التحقيق في جمع الأدلة الالكترونية، كما أنه قد يتم تدمير الدليل عن غير قصد بسبب نقص المعرفة التقنية ولهذا كان من الضروري انشاء إدارة متخصصة لهذا النوع من الجرائم والأدلة وهو ما حدث فعلا، وهذا على المستوى الدولي وكذا المحلي فعلى المستوى الدولي أنشأت شرطة خاصة لمكافحة هذه الأنشطة الإجرامية المستحدثة.

ويعد التعاون الدولي الشرطي من أهم صور التعاون الدولي في مكافحة الإجرام بصفة عامة والإجرام الالكتروني العابر للحدود بصفة خاصة، ولقد أنشأت عدة أجهزة لتحقيق هذا التعاون، أهمها المنظمة الدولية للشرطة الجنائية[2].

كما أنه توجد منظمات دولية أخرى لا تقل أهمية عن الأنتربول تهدف أيضا لمواجهة هذا النوع المستهدف من الجرائم، نذكر منها على سبيل المثال منظمة التعاون الاقتصادي والتنمية، وكذا مجموعة الثمانية الاقتصادية، هذا بالاضافة إلى انشاء المجلس الأوربي لشرطة أوربية التي كان لها دورا فعالا في مكافحة جرائم الانترنت.

1 نفس المرجع، ص 228

2 أنشأ هذا الجهاز سنة 1923 تحت اسم اللجنة الدولية للبوليس الجنائي ويظم 160 دولة من بينها الجزائر وللمزيد من التفاصيل راجع كتاب سراج الدين الروبي الأنتربول وملاحقة المجرمين، دار المصرية البنانية، 1998.

أما على المستوى العربي نجد أن مجلس الوزراء العرب أنشأ المكتب العربي للشرطة الجنائية[1] والتي تهدف إلى توطيد جهود التعاون بين أجهزة الشرطة في الدول المشاركة بهدف تطبيق القانون وملاحقة المجرمين.

وعلى المستوى الداخلي بادرت العديد من الدول إلى إنشاء وحدات متخصصة لمكافحة الإجرام الإلكتروني على المستوى الوطني نذكر على سبيل المثال مكتب التحقيق الفيدرالي في الولايات المتحدة، كما أسست هونكونغ قوة لمكافحة قرصنة الأنترنت سنة 1999، وفي الصين القوة المضادة للهاكر سنة 2000، كما قامت وزارة الداخلية المصرية بإنشاء إدارة مكافحة الحاسوب وشبكات الانترنت[2].

أما بالنسبة للجزائر لم يتم إنشاء أي هيئة لمكافحة الجرائم الإلكترونية واكتفت بتعديل قانون الإجراءات الجزائية بموجب القانون 22/06 والذي استحدث فيه فصلين هما الفصل الرابع والخامس من الباب الثاني من الكتاب الأول. ومن حيث التكوين والتأهيل في مجال مكافحة الجريمة الإلكترونية فقد قامت الجزائر بدورات تكوينية على المستوى الدولي لإطارات الدرك الوطني للتكوين والتخصص والبحث والتنقيب وملاحقة المجرمين، كما تم استحداث شبكة اتصالات وطنية موحدة لمع البيانات المتعلقة بالشبكات الإجرامية

المطلب الثاني: الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الرقمي

إن تقدير قيمة الدليل الجنائي بما في ذلك الدليل الرقمي يعود إلى قناعة القاضي، الذي يتمتع بسلطة واسعة في تقدير الأدلة، حيث ترك له المشرع الحرية في هذا المجال، يظهر ذلك جليا من خلال سلطته التقديرية، على أن يتحرى الحقيقة بكافة الأدلة دون إلزام مسبق بقيمة دليل ما، غير أن المشرع لم يترك حرية القاضي مطلقة بل وضع لها ضوابط تكون لها بمثابة صمام الأمان الذي يضمن عدم انحرافه عند ممارسة سلطته[3].

1 هذا المكتب هو أحد المكاتب الخمسة التابع للأمانة العامة لمجلس الوزراء الداخلية العرب ومقره بسوريا

2 عائشة بن قارة مصطفى، المرجع السابق، ص 267.

3 زبدة مسعود، المرجع السابق، ص 131، 132.

ولقد حددت أغلب التشريعات المقارنة الأدلة التي تقبل الإثبات بنصوص خاصة كجريمة الزنا، كما تدخل المشرع أحيانا لإلزام القاضي الجنائي لإتباع طرق خاصة في بعض المسائل مراعاة لطبيعتها.

وتناولت أغلب التشريعات المقارنة موضوع الاقتناع الشخصي للقاضي الجزائي وجسدته في قوانينها الإجرائية كما تم الأخذ به في أحكامها ومحاكمها، وعلى هذا الأساس ستكون دراستنا في الأول حول القيود الواردة على حرية القاضي الجنائي في قبول الدليل الكتروني ثم يكون الحديث عن الضوابط التي تحكم القاضي الجنائي بالدليل الالكتروني.

الفرع الأول: قيود قبول الدليل الرقمي من القاضي الجنائي

تتخذ الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الرقمي صور متباينة منها ما يتعلق بمصدر الاقتناع ومنها ما يرد على اقتناع القاضي الجنائي في حد ذاته.

أولا/ القيود المتعلق بالدليل الرقمي نفسه

سبق وأن تناولنا في الفصل الأول شروط قبول الدليل الالكتروني، فالقاضي الجنائي لا يمكن أن يؤسس حكمه ويفصل في الدعوى المعروضة عليه إلا بناء على أدلة مقبولة تتوفر فيها جميع الشروط، والمتمثلة في مشروعية الدليل الرقمي وأن يكون هذا الدليل مبني على الجزم واليقين وأن يتم مناقشته في الجلسة وأمام جميع أطراف الدعوى.

إن القاضي الجزائي ليس حرا في تقدير الدليل الرقمي أي كان، إذ أن هذه الحرية تقتصر على تقدير الدليل المقبول في الدعوى وفقا للشروط المحددة في القانون، وتختلف هذه الشروط من تشريع لأخر، إلا أنه متفق ضمنيا على أهم هذه الشروط بموجب العديد من الاتفاقيات الدولية المناهضة من أجل مكافحة ومحاربة الجريمة الإلكترونية بشتى صورها وأشكالها.

وفي هذا الإطار نجد أن المنظمة الدولية لدليل الحاسوب وضعت المعايير المطلوبة في الدليل الرقمي المصادقة عليها خلال المؤتمر الدولي للبحث المعلوماتي، أو الجريمة التقنية المنعقد في نوفمبر عام 1999.

حددت التشريعات المختلفة وسائل وإجراءات لتحصيل أدلة الإثبات لتجعل منها إجراءات أو وسائل خاضعة لمبدأ الشرعية، يرجع إليها القاضي أثناء تكوين اقتناعه الشخصي كمعيار لتحديد مدى مشروعية الدليل المستند عليه في ذلك، في حد ذاته.

إن الارتباط الوثيق بين مشروعية الدليل كمبدأ، وبين شرعية الإجراء الموصل اليه فوجود الأول متوقف أساسا على وجود الثاني، فهدف الإثبات أولا وأخيرا، بغض النظر عن وسيلة، هو الوصول إلى الحقيقة لا غير ولا يمكن بأي حال من الأحوال أن يبرر هذا الهدف استعمال أي وسيلة عن الإطار الذي رسمته لها الشرعية التي أوجدها المشرع والمجتمع في آن واحد، بغية ضمان عدم خروج هذا الأخير أثناء تأديته لوظائفه عن قواعد العدالة، وبالتالي ضمان حق الدفاع المكفول لشخص المتهم.

فالعبرة بنزاهة الأدلة وشرعية تحصيلها وليس بحشدها وتوافرها وهذا ما اتفق عليه في أغلب الدساتير والقوانين، وإذا كان القاضي لا يجد أي اشكال في تطبيق الدليل التقليدي كون أن التشريعات وضعت طرق معينة، يجب احترامها للوصول اليه، فإن الإشكالات تظهر وبقوة إذا كنا بصدد دليل رقمي يفترض فيه قوة حجيته، وهو بذلك يفرض نفسه على اقتناع القاضي الجنائي، ولم يكن المشرع قد وضع قواعد محدد لتنظيم أو تقنين إجراءات الحصول عليه ليجد القاضي نفسه أمام خيارين إما عدم الأخذ بهذا الدليل لعدم وجود نص قانوني يحدد مدى شرعية إجراءات الحصول عليه أو لمساسه بالحريات الفردية من جهة أخرى وبين خيار الأخذ به معتمدا على المادة 212 من قانون الإجراءات الجزائية والتي تفتح المجال واسعا باستعمال كل الطرق التي من شأنها أن تمكنه من الوصول إلى الحقيقة، وبذلك تكون قد أعطته كل الحرية في اختيار كل وسيلة أو الأخذ بأي دليل من شأنه أن يكون قناعة شخصية لديه.

ونظرا لكون شرعية الحصول على دليل ما تستلزم شرعية الإجراء الموصل اليه فوجود الأول متوقف أساسا على مدى وجود الثاني، ولا غنى لأي منهما عن الآخر.

وفي حالة سكوت المشرع عن إجراءات تحصيل أدلة الإثبات يتعين استبعاد جميع الوسائل التي من شأنها أن تهدد سلامة الإنسان الجسدية والذهنية أو تلك التي قد تشكل انتهاك لحقوق الإنسان أو تمس بالحريات الفردية.

ثانيا/ الضوابط التي يخضع لها اقتناع القاضي:

إن القاعدة العامة في الإثبات الجزائي أن تبنى الأحكام على الجزم واليقين لا على الضن والاحتمال، حيث تنص القاعدة القانونية بأن الشك يفسر لصالح المتهم وهو ما يعني أنه وفي حال عدم ثبوت التهمة بصورة يقينية يلزم القاضي أن يحكم ببراءة المتهم وهو ما يجسد إحدى النتائج الإيجابية لقرينة البراءة[1].

إن اليقين في أحكام الإدانة هو شرط عام حيث أنه سواء كانت الأدلة التي يستنتج منها تقليدية أو مستحدثة للدليل الرقمي، لذلك لا بد أن يكون للدليل الرقمي غير قابل للشك إذ أن هذا الأخير يفسر لصالح المتهم استناد إلى مبدأ الأصل في الإنسان البراءة، فيكفي الشك في صحة اسناد التهمة إلى المتهم، حتى يقضى بالبراءة[2].

وإذا كان القاضي الجنائي يستطيع الوصول إلى اليقين بالمعرفة الحسية أو العقلية عن طريق التحليل والاستنتاج فإن الجزم بوقوع الجريمة المعلوماتية، تستلزم من القاضي نوعا آخر من المعرفة، كونه يلعب دور إيجابي في الإثبات وهي المعرفة العلمية والإحاطة بالأمور المعلوماتية.

فعدم إحاطة القاضي الجنائي بالأمور المعلوماتية وجهله بها يؤدي حتما إلى التشكيك بالدليل الرقمي، وهو ما يوجب القضاء بالبراءة، ويستفيد من هذا الشك المتهم المعلوماتي وهو ما يؤدي إلى إفلات المجرمين المعلوماتيين من العدالة والقانون، ومن ثم يترتب على ثبوت التهمة بلوغ الاقتناع، بالإدانة درجة اليقين من طرف القاضي الجنائي لأن الاقتناع ثمرة اليقين[3] .

أن الأصل أن تكون الأدلة في المواد الجنائية مساندة ومتماسكة وتكمل بعضها البعض حتى يمكن اعتمادها فيتكون اقتناع لا لبس فيه، من مجمل الأدلة دون تناقض أو تخاذل فيما بينها تؤدي وفق قواعد العقل والمنطق، إلى النتيجة التي وصلت اليها المحكمة. فحتى يكون اقتناع القاضي صحيح يجب أن يكون مبني على أدلى غير متعارضة تؤدي

1 بلوهالي مراد، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مرجع سابق، ص 118.

2 عائشة بن قارة مصطفى، مرجع سابق، ص 277.

3 معمش زهية وغانم نسيمة، مرجع سابق، ص 75.

مجتمعة للضرورة إلى النتيجة المستخلصة فإذا لحقها تناقض أو تخاذل فإن ذلك يؤدي إلى فسادها، ويترتب عنه بطلان الحكم وأيضا إذا أخطأ الحكم المطعون فيه في الاستدلال ولو بدليل واحد فقد كان للطعن مصلحة محققة في التوصل إلى ابطاله، لا ينفيها توافر أدلة صحيحة غيرها، وذلك لتعذر التعرف على مبلغ الأثر الذي كان للدليل الباطل في الرأي الذي انتهت اليه المحكمة أو الوقوف على ما إذا كانت تنتهي إليه لو أنها فطنت إلى هذا الدليل غير القائم بما يتعين معه إعادة النظر، في كفاية باقي الأدلة لدعم الإدانة[1].

الفرع الثاني: مدى الأخذ بالدليل الرقمي مراعاة للمصلحة الأولى

وهي الحالة التي يكون فيها الدليل الإلكتروني غير مشروع كأثر للتعدي على الحياة الخاصة وفي نفس الوقت يعد وسيلة اثبات لجرائم تهدد أمن الدولة أو نظام المجتمع الأخلاقي، وهنا تثور مشكلة أي المصلحتين أولى.

هنا يشكك البعض في مشروعية الدليل الكتروني باعتباره طريقة للتدخل في الحياة الخاصة للأفراد خاصة في مجال الجرائم الجنسية، التي تكون برضا المشتركين فيها، إلا أن الاستعانة بالوسائل الحديثة كالإنترنت، واستخدامها كدليل على وقوع جريمة الإعلان على البغاء ونشر المطبوعات الفاضحة يستهدف المصلحة العامة، وحتى تتمكن الدولة من حماية النظام الاجتماعي حتى لا ينهار هذا النظام بسبب احترام مبالغ فيه للحقوق والحريات الخاصة، ولا يمكن الاعتراض عليه بحجة عدم مشروعية الدليل الالكتروني، فكل ما يتولد عن العلم الحديث يجب أن يستخدم في أمن المجتمع، ولا شك في مشروعيته.

وإذا سلمنا بالقول بأن هناك تعد على حريات الأفراد، فإنه تعدي ضئيل للغاية، وبالتالي ما يتعين الاعتداد به هو مدى خطورة العدوان أو المساس بالنظام الاجتماعي، فلا يمكن استبعاد كل وسيلة لمجرد منافاتها للقواعد العامة دون دراسة أو تعمق لآثارها في المجتمع

1 فاضل زيدان، مرجع سابق، ص 136.

الفرع الثالث: قيمة الدليل الرقمي غير المشروع

انطلاقا من قاعدة أن الأصل في الإنسان البراءة، فإن المتهم يجب أن يعامل على أساس أنه بريء في مختلف مراحل الدعوى إلى ان يصدر حكم بات، ومما سبق ذكره فإنه يستلزم أن تكون أدلة الإثبات متحصل عليها بطريقة مشروعة حتى يستند ويؤسس عليها القاضي الجنائي حكمه ويبني قناعته في ذلك، وبالتالي فإن أي دليل يتم الحصول عليه بطريقة غير مشروعة لا تكون له قيمة في الإثبات ذلك بأنه ما سمح بقبول الأدلة التي تكون وليدة إجراءات باطلة، فإن الضمانات التي كفلها المشرع بلا أهمية متى أمكن اهدارها وعدم الالتزام بها.

فشرعية الإثبات الجنائي تستلزم عدم قبول أي دليل كان الحصول عليه قد تم بطريقة غير مشروعة، وتعد باطلة كل الإجراءات التي بنيت أو استندت على دليل تم الحصول عليه بطرق ووسائل تخرج عن إطار الشرعية، وإذا تقرر بطلان إجراء ما يجب استبعاد ما ينتج عنه من أدلة وإجراءات لاحقة له، تطبيقا لقاعدة ما بني على باطل فهو باطل[1].

وهذه القاعدة مطبقة في النظم اللاتينية ، فالأدلة التي يؤسس عليها حكم الإدانة يجب أن تكون مشروعة، سواء كانت أدلة تقليدية أو ناتجة عن الوسائل الإلكترونية بصفة عامة ومن أمثلة الطرق غير المشروعة التي يمكن أن تستعمل في الحصول على الدليل الإلكتروني، إكراه المتهم المعلوماتي على فك الشفرة المعلوماتية أو ارغامه للحصول على كلمة السر اللازمة للدخول إلى ملفات البيانات المخزنة، وأيضا أعمال التحريض على ارتكاب الجريمة الإلكترونية من قبل رجال الضبطية القضائية كالتجسس المعلوماتي أو المراقبة الإلكترونية عن بعد وبدون إذن قانوني[2].

أما عن اشتراط مشروعية الدليل الرقمي في أدلة البراءة ثار جدل واختلاف فقهي في هذه المسألة وبرزت ثلاث آراء مختلفة:

1 بلولهي مراد، مرجع سابق، ص 105، 106

2 عائشة بن قارة مصطفى، مرجع سابق، ص 217.

يرى الاتجاه الأول أن المشروعية دليل لازم لكل دليل سواء كان دليل الإدانة أو البراءة باعتبار أن قصر مبدأ المشروعية على دليل الإدانة فقط فيه ضرر على الفرد والمجتمع كما أن هذا الاتجاه يرى أن اثبات البراءة من قيد المشروعية الذي هو شرط أساسي في أي تشريع بكل اقتناع سليم[1].

بينما يرى الاتجاه الثاني بأنه ليس ثم ما يمنع من تأسيس حكم البراءة على دليل غير مشروع وهذا انطلاقا من مبدأ افتراض البراءة باعتبارها هي الأصل، وبالتالي المحكمة ليست بحاجة إلى اثباتها، كما أن الدليل المستمد من وسيلة غير مشروعة شرع أساس لحماية حرية المتهم ومن ثم فإنه من غير المعقول أن ينقلب عليه، ولو تم التمسك بعدم قبول دليل البراءة بحجة أنه غير مشروع فستكون النتيجة خطيرة وهي إدانة بريء، بالإضافة إلى أن القاضي يحكم بالبراءة لمجرد الشك تطبيقا لمبدأ الشك يفسر لصالح المتهم. ومن باب أولى أن يحكم ببراءة الشخص الذي توفر دليل براءته حتى وأن لم يتم الحصول على هذا الدليل بطريقة غير مشروعة وهو ما ذهب اليه المشرع المصري[2].

وأخيرا يرى الاتجاه الثالث إلى ضرورة التفرقة بين ما إذا كان دليل البراءة قد تم الحصول عليه نتيجة جريمة جنائية، أو كان الحصول عليه نتيجة سلوك يشكل مخالفة لقاعدة إجرائية، فإذا كانت الطريقة الأولى هي التي تم الحصول بها على الدليل وجب اهدار هذا الدليل لأنه يجعل البعض يفلت من العقاب، أم إذا كان الحصول على هذا عن طريق مخالفة إجرائية فحسب يصلح للاستناد إلى هذا الدليل وتبرأة المتهم تحقيق للغاية من تشريع البطلان، لأن البطلان الذي شاب وسيلة الوصول إلى هذا الدليل يرجع إلى الشخص الذي قام بالإجراء الباطل، وبالتالي لا يصح أن يضار المتهم بسبب فعل لا دخل له فيه.

1 أشرف عبد القادر قنديل، مرجع سابق، ص 210.

2 بلوهلي مراد، مرجع سابق، 107.

خاتمة

لقد فرض الدليل الالكتروني نفسه في مجال الإثبات الجنائي، كضرورة حتمية تمخضت عن ظهور نوع مستحدث من الجرائم، وقفت جميع طرق الإثبات التقليدية عاجزة في مواجهتها، فما شهده العالم من تطور علمي في مجال الثورة المعلوماتية غير الكثير من المفاهيم التقليدية الأمر الذي أدى إلى ظهور العديد من التقنيات والتكنولوجيات التي لم تعرفها البشرية من قبل، فبدأ الحديث عن النقود الإلكترونية، والمستندات الإلكترونية...إلخ.

وبظهور هذه التكنولوجيا الحديثة والعمل بها كان لزاما حمايتها جنائيا ومن هنا تبين قصور التشريعات العقابية في مواجهة الجريمة الالكترونية، نظرا لما تكتسيه الأخيرة من خصوصية وطبيعة فنية وعلمية معقدة من جهة، وما يتصف به مرتكبوها عادة من سمات وطبيعة ذكية ماكرة. وهو ما يترتب عنه إفلات مرتكبي هذا النوع من الجرائم رغم ثبوت اقترافهم للجريمة في الواقع.

ومن هنا ظهر الدليل الرقمي الذي اتسم بقوة ثبوتية وحجية كافية في مجال الإثبات الجنائي اذ يجب على القضاء والقوانين الأخذ به وبإلقاء الضوء على طبيعة اثبات الجرائم الإلكترونية وإجراءات الحصول على أدلتها وقيمتها في مجال الإثبات الجنائي وصلنا إلى مجموعة من النتائج يمكن تلخيصها فيما يلي:

- التطور الهائل في مجال التكنولوجيا المعلوماتية استحدث عدة طرق وأساليب جديدة ومتطورة لارتكاب الجريم، وخلق جرائم جديدة لم تكن معروفة في السابق.
- تتمتع الأدلة الرقمية بخصائص جعلتها تتميز عن الأدلة الرقمية، وله أهمية بالغة في مجال الإثبات الجنائي، لاسيما في إثبات الجرائم الالكترونية المستحدثة.
- إن الجرائم الإلكترونية المستحدثة لها طبيعة خاصة ومعقدة، ولاستخلاص أدلة إثباتها والبحث عن مرتكبيها والكشف عنها يحتاج ذلك إلى ذوي الكفاءة ويتمتعون بخبرة فنية وتقنية العالية في مجال تكنولوجيات المعلوماتية.
- تتسم إجراءات جمع الأدلة الرقمية والحصول عليها وتقديمها أمام للقضاء الجنائي بالمشروعية مما يستوجب اتباع الطرق والأساليب القانونية التي رسمها المشرع.

- الدليل الرقمي المستمد من إجراءات باطلة يعد باطل، ويؤدي ذلك إلى فقدان قوته الثبوتية وحجيته أمام القضاء.
- إن تقدير قيمة الدليل الرقمي المقدم في الدعوى العمومية يرجع الاختصاص في ذلك إلى القاضي الجنائي، وفقا لما خول له من سلطة تقديرية قانونا، بحسب قناعته وحجية الدليل الرقمي في الاثبات.
- تبنى المشرع الجزائري نظام الإثبات الحر في مجال الإثبات الجنائي بالأدلة الجنائية الرقمية.
- لا يقتصر دور الدليل الرقمي في إثبات الجرائم الالكترونية فحسب، بل يصلح أيضا أن يكون دليلا لجرائم أخرى استعمل فيها الحاسوب أو شبكة الأنترنت لارتكابها.

وبعد عرض النتائج التي توصلنا اليها نقترح بعض التوصيات التي ينبغي الأخذ بها في مجال الإثبات الجنائي بالأدلة الرقمية وتتجلى في:

1. يتضح من خلال الإجراءات التقليدية لاستخلاص الدليل الرقمي أنها غير كافية الأمر الذي يستلزم أن تصاحبها إجراءات حديثة كإجراء التسرب واعتراض المراسلات والتصنت.
2. ضرورة تعديل قانون الإجراءات الجزائية بما يتماشى ويساير طبيعة الأدلة الرقمية وخصوصيتها، والحالة التي يكون عليها لإثبات الجريمة الالكترونية، مع وضع قواعد تبين طرق وأساليب الحصول على الدليل الرقمي وكيفية التعامل معه.
3. وضع تشريعات خاصة بمكافحة الجرائم الالكتروني وردعها، والوقاية منها، ولحماية المساس بالحياة الخاصة للأفراد، تكون مواكبة للتطور العلمي في مجال تكنولوجيا المعلومات.
4. إنشاء أو إحداث مخابر للأدلة الجنائية الرقمية، لفحص الأدلة واكتشافها وتقييمها تقنيا وفنيا وتقديمها للعدالة بصورة سليمة، والمحافظة عليها من أي عبث أو تشويه أو تغيير أو تلف مع الاحتفاظ بنسخها الأصلية للرجوع اليها عند الحاجة.

5. المشاركة والانضمام إلى كل الفعاليات الدولية المناهضة لمكافحة الجريمة الالكترونية مع العمل على تحقيق كل الجهود الدولية والمحلية والإقليمية في مجال القضاء على الإجرام بشتى صورها.
6. استحداث فرق خاصة من الشرطة لمكافحة الجريمة الالكترونية، تتميز بتكوين خاص في مجال تكنولوجيا المعلوماتية.
7. برمجة دورات تكوينية لتأهيل وتدريب القضاة، ورجال الضبطية الفضائية، وكل سلطات البحث والتحري عن الجريمة الالكترونية، لمواكبة كل التطورات العلمية لاسيما في مجال المعلوماتية.

قائمة المراجع

Les References

باللغة العربية

أولا- النصوص القانونية

1. دستور الجزائر لسنة 1996 الصادر بموجب مرسوم رئاسي رقم 96-438 مؤرخ في
2. 07-12-1996، جريدة الرسمية، العدد 76، الصادرة بتاريخ 08-12-1996.
3. أمر رقم 66-155 مؤرخ في 08-06-1966 المتضمن قانون الإجراءات الجزائية الجزائري جريدة رسمية عدد 48، الصادرة بتاريخ 10-06-1966.
4. أمر رقم 66-156 المؤرخ في 08-06-1966 المتضمن قانون العقوبات منشور في الجريدة الرسمية عدد 49 بتاريخ 11-06-1966.
5. قانون رقم 03/2000 المؤرخ في 2000/08/05 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، جريدة رسمية عدد 48 الصادر بتاريخ 2000/08/06.
6. القانون رقم 09-04 المؤرخ في 05-08-2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتعلقة بتكنولوجيا الاعلام والاتصال ومكافحتها منشور في الجريدة الرسمية عدد 47 الصادرة بتاريخ 06-08-2009.
7. القانون رقم 06-22 مؤرخ في 20-12-2006 معدل ومتمم لقانون الإجراءات الجزائية جريدة رسمية عدد 84 الصادرة بتاريخ 27-12-2006.
8. مرسوم رئاسي رقم 15-261 مؤرخ في 08-10-2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها جريدة رسمية عدد 53 الصادرة في 08-10-2015.

ثانيا: الفقه

الرسائل والاطروحات

1. روميصاء بوطبة، صلاحيات الضبطية القضائية في ضوء القانون رقم 06-22 مذكرة لاستقبال متطلبات شهادة الماستر، قانون جنائي، جامعة قاصدي مرباح ورقلة، 2015.
2. سارة قادري، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة لنيل شهادة الماستر اكاديمي في القانون، تخصص قانون عام للأعمال جامعة قاصدي مرباح ورقلة 2014.
3. شهرزاد حداد، الدليل الالكتروني في مجال الاثبات الجنائي، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة العربي بن مهيدي أم البواقي، 2016. 2017.
4. عبد الستار جولحي، جرائم الحاسوب، دراسة مقارنة، بين الشريعة الإسلامية والقانون الجزائري، مذكرة تخرج تدخل ضمن متطلبات الحصول على شهاد الماستر في العلوم الإسلامية، جامعة الشهيد حمه لخضر، كلية العلوم الاجتماعية والإنسانية، قسم العلوم الإنسانية الجزائر، 2015.
5. مراد بلولهي، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مذكرة لنيل شهادة ماجيستر، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة الحاج الأخضر باتنة، 2010.2011.

نعيم سعيداني، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية ، تخصص علوم جنائية ، جامعة الحاج لخضر ، باتنة ، 2012-2013.

الكتب المتخصصة

1. أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة الإسكندرية، مصر، 2015.
2. بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، ط 1، 2011.
3. خالد ممدوح إبراهيم، خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية دار الفكر الجامعي، الإسكندرية، ط 1، 2009.
4. سامي جلال فقهي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي دار الكتب القانونية، مصر، 2014.
5. عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، د ط، دار الجامعة الجديدة الإسكندرية، 2010.
6. عادل عزام سقف الحيط، جرائم الدم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع، ط 1 ،2011.
7. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2014.
8. علي حسن أحمد الطوالبة، التفتيش الجنائي على نظم الحاسوب، دراسة مقارنة، ط1، عالم الكتب الحديث للنشر والتوزيع، الأردن، 2004.
9. ياسر الأمير فاروق، مراقبة الأحاديث الخاصة دراسة تأصيلية تحليلية ومقارنة للتنصت على المحادثات التلفونية والتي تجرى عبر الأنترنت والاحاديث الشخصية نظريا و علميا، دار المطبوعات الجامعية، الإسكندرية، ط 1، 2019.
10. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتب اللالات الحديثة، أسيوط، 1994.

الكتب العامة

1. احسن بوسقيعة، التحقيق القضائي، دار هومة للطباعة والنشر، الجزائر، ط 10، 2013.
2. جابري عبد المجيد، دراسة قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة دون طبعة، دار هومة الجزائر، 2012.
3. خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، دار الثقافة، الأردن، ط 1، 2011.
4. عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة والنشر الجزائر، ط 2، 2011.
5. كمال محمد عواد، الضوابط الشرعية والقانونية للأدلة الجنائية في الفقه الإسلامي والقانون الوضعي الطبعة الأولى، دار الفكر الجامعي، مصر، 2011.
6. مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، ج1، دار النهضة العربية، القاهرة، 2000.
7. محمد امين احمد الشوابكة، جرائم الحاسوب والانترنيت، ط 1، دار الثقافة للنشر والتوزيع، عمان، 2004.
8. محمد حماد مرهج الهيتي، جرائم الحاسوب، دار المناهج، عمان، ط 1، 2006.
9. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة للطباعة والنشر، 2009.
10. نبيلة هبة هروال، الجوانب الإجرائية لجوانب الانترنيت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2013.

ثالثا: المقالات

1. سامية بلجراف، سلطة القاضي الجنائي في قبول وتقدير الدليل الرقمي، ورقة بحثية مقدمة إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر بسكرة، الجزائر، يومي 16 و17 نوفمبر 2015.

2. سوزان عدنان، انتهاك حياة حرمة الحياة الخاصة عبر الإنترنت، دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانون، العدد 03 المجلد 29، سوريا، 2013.

3. دنيازاد ثابت، مراقبة الاتصالات الالكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والانسانية جامعة تبسة،العدد 6، 2012.

4. عادل مختاري، دور القاضي الجزائي في ظل مبدأ الاقتناع القضائي، مجلة المنتدى القانوني، العدد الخاص، مارس 2008، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة.

5. بوعناد فاطمة زهرة، مكافحة الجريمة الالكترونية في التسريع الجزائري، مجلة الندوة للدراسات القانونية، سيدي بلعباس، 2013،العدد 01 .

رابعا: المواقع الالكترونية

1. حسين بن سعيد الغافري، التحقيق، جمع الأدلة في الجرائم المتعلقة بشبكات الانترنيت، موقع المنشاوي للدراسات والبحوث على الموقع WWW.minshawi.com اطلع عليه بتاريخ 11-02-2018.

الفهرس

مقدمة.....1

الفصل الأول: إجراءات استخلاص الدليل الرقمي وشروط قبوله.....5

المبحث الأول: إجراءات استخلاص الدليل الرقمي.....6

المطلب الأول: الإجراءات التقليدية لاستخلاص الدليل الرقمي.....7

فرع الأول: لانتقال والمعاينة..... 7

الفرع الثاني: التفتيش الأدلة الجنائية الرقمية.....11

الفرع الثالث: الضبط في الجرائم الرقمية..... 16

الفرع الرابع: الخبرة في الجرائم الرقمية.....18

المطلب الثاني: الإجراءات التقليدية لاستخلاص الدليل الرقمي.....20

الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور..... 21

الفرع الثاني: مراقبة الاتصالات الالكترونية.....26

المبحث الثاني: شروط قبول الدليل الجنائي الرقمي أمام القضاء الجنائي.....28

المطلب الأول: مشروعية الدليل الجنائي الرقمي.....28

الفرع الأول: المقصود بمشروعية الحصول على الدليل الجنائي الرقمي.....29

الفرع الثاني: مشروعية الحصول على الدليل الجنائي الرقمي في التشريعين الجزائري والفرنسي.....30

المطلب الثاني: يقينية الدليل الجنائي الرقمي ومناقشته..... 33

الفرع الأول: يقينية الدليل الجنائي الرقمي.....33

الفرع الثاني: مناقشة الأدلة الجنائية الرقمية.....36

الفصل الثاني: حجية الدليل الجنائي الرقمي في الإثبات الجنائي.....40

المبحث الأول: حجية الدليل الرقمي في أنظمة الإثبات..... 42
المطلب الأول: الدليل الرقمي في نظام الإثبات الحر..... 42
الفرع الأول: مبدأ حرية الإثبات الجنائي للدليل الرقمي.....43
الفرع الثاني: النتائج المترتبة على تطبيق مبدأ حرية الإثبات الجنائي..... 45
الفرع الثالث: حجية الدليل في نظام الإثبات الحر.....47
المطلب الثاني: الدليل الرقمي في نظام الإثبات المقيد..... 48
الفرع الأول: أساس مشكلة قبول الدليل الرقمي في ظل النظام المقيد..... 49
الفرع الثاني: موقع الدليل الرقمي في نظام الإثبات المقيد.....50
الفرع الثالث: حجية الدليل الرقمي في نظام الإثبات المقيد.....52
المطلب الثالث: الدليل الرقمي في نظام الإثبات المختلط.....54
الفرع الأول: مبدأ نظام الاثبات المختلط بالنسبة للدليل الرقمي.....55
الفرع الثاني: حجية الدليل الرقمي في نظام الإثبات المختلط.....56
المبحث الثاني: حجية الدليل الرقمي أمام القضاء الجنائي.....57
المطلب الأول:السلطة التقديرية للقاضي الجنائي في القبول والاقتناع بالدليل الرقمي.....58
الفرع الأول: الطبيعة العلمية للدليل الرقمي وأثرها على اقتناع القاضي.....58
الفرع الثاني: إشكالات الدليل الرقمي وأثرها على اقتناع القاضي.....61
المطلب الثاني: ضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الالكتروني..... 64
الفرع الأول: قيود قبول الدليل الرقمي من القاضي الجنائي.....65
الفرع الثاني: مدى الأخذ بالدليل الإلكتروني مراعاة للمصلحة الأولى 68
الفرع الثالث: قيمة الدليل الإلكتروني غير المشروع:..... 69
خاتمة..... 73

قائمة المراجع.....77

الفهرس..... 83

الملخص:

تقتضي الجريمة الإلكترونية على غرار بقية الجرائم التقليدية أساليب خاصة للبحث والتحري عنها لطبيعتها الخاصة، الأمر الذي أدى بالمشرع إلى إستحداث إجراءات وأساليب إستثنائية لإثبات هاته الأخيرة

بالإظافة إلى أنه يتوجب مع انتهاج هذه السياسة المغايرة في الإثبات معرفة مدى حجية هذا الدليل في الإثبات وتكوين قناعة القضاة لأن هذا الدليل يواجه صعوبات اثناء تقييمه كونه مستحدث.

الكلمات المفتاحية:

الجريمة الإلكترونية، حجية الدليل الرقمي، أساليب البحث، قناعة القاضي، إجراءات إستخلاص الدليل الرقمي، طبيعة الدليل الرقمي.

Résumé:

Comme d'autres crimes traditionnels, la cybercriminalité nécessite des méthodes particulières de recherche et d'investigation en raison de sa nature particulière, ce qui a conduit le législateur à développer des procédures et des méthodes exceptionnelles pour prouver cette dernière,De plus, avec l'adoption de cette politique différente de la preuve, il est nécessaire de connaître l'étendue de l'autorité de cette preuve dans la preuve et de former la conviction des juges, car cette preuve rencontre des difficultés lors de son évaluation car elle est nouvelle

Mots clés:

Cyber criminaliti ,Guide numèrique authentique,Mèthodes de recherche,Condamnation du juge,Procèdures d’extraction de preuves numèriques,La nature des preuves numèriques.

Abstract:

Like other traditional crimes, cybercrime requires special methods of research and investigation due to its special nature, which has led the legislator to develop exceptional procedures and methods to prove the latter. adopting this different policy of evidence, it is necessary to know the extent of the authority of this evidence in the evidence and to form the conviction of the judges, because this evidence encounters difficulties during its evaluation because it is new

Keywords:

Cyber crime, Authentic digital guide, Research methods, Judge's conviction, Digital evidence, extraction procedures,The nature of digital evidence.