تاريخ الإرسال: 2021/11/07 تاريخ القبول:2022/03/25

الإجراءات التقنية للإثبات الجنائي في جرائم الاتصالات الالكترونية

Technical Procedures for CriminalEvidence inElectronic Communications Crimes

صحراوي مصطفى[1*]

جامعة وهران2محمد بن احمد(الجزائر)sahraoui.mustapha@univ-oran2.dz

الملخص:

يُعتبر الإثبات الجنائي تقنية قانونية ترمي إلى مطابقة ما توصل إليه القضاء من حقيقة مع حقيقة الوقائع المجرمة، ولمّا كانت المطابقة بين الحقيقتين تشكل جوهر مبدأ المحاكمة العادلة، فإن الإثبات في القانون قد تحّول من شكل من أشكال المعرفة إلى وسيلة من وسائل تحقيق العدالة، فكلما كان نظام الإثبات ملما بتطورات الحقيقة الواقعية كلما كانت المحاكمة عادلة.

ونظرا لأهمية الإثبات في تحقيق مبدأ المحاكمة العادلة فإنه من الضروري أن يكون مسايرا للتطورات العلمية والتقنية التي من شأنها أن تساعد على كشف الجرائم، ولعلنا من خلال هذا البحث نقف على مدى ملائمة نظام الإثبات لجرائم الاتصالات الالكترونية ومدى خصوصيته في التشريع الجزائري والمقارن.

الكلمات المفتاحية:

الاثبات الجنائي، الدليل الرقمي، الاتصالات الالكترونية، التحقيق الجنائي

Abstract:

Criminal evidence is a legal technique that aims to match the truth that the judiciary has found with the truth of the criminal facts. The evidentiary system is aware of factual developments whenever a trial is fair.

Given the importance of evidence in achieving the principle of a fair trial, it is necessary to keep pace with scientific and technical developments that would help detect crimes, and perhaps through this research we stand on the suitability of the evidence system for electronic communications crimes and the extent of its privacy in Algerian and comparative law.

Keywords:criminal evidence, digital evidence, electronic communication, criminal investigation.

*صحراوي مصطفى

مقدمة:

يخضع التحقيق الجنائي في الجرائم المعلوماتية إلى قواعد علمية ثابتة، تحكمه إجراءات قانونية تستلزم الامتثال والتطبيق الحرفي، وقواعد تقنية متزنة تحتم على المحقق إضفاء خبرته ومهاراته، مواكبا في ذلك التطور السريع للجريمة الإلكترونية وتطور أساليب ارتكابها.

وبإعتبار جرائم الاتصالات من الجرائم المستحدثة التي تتطلب إعمال إجراءات تقنية يتطلبها التحقيق الجنائي حتى يتحقق الدليل اللازم للإثبات، وجب التعرض إلى الإجراءات التقنية للإثبات الجنائي في هذه الجرائم و ذلك قصد معالجة الإشكالية الآتية : فيما تتمثل الإجراءات التقنية للإثبات الجنائي في جرائم الاتصالات الالكترونية ؟ و للإجابة عن هذه الإشكالية نعالج موضوع دراستنا من خلال مبحثين، يتناول المبحث الأول مبادئ وإجراءات جمع الدليل الجنائي في جرائم الاتصالات، بينما يعالج المبحث الثاني وسائل الإثبات التقنية في جرائم الاتصالات.

المبحث الأول:مبادئ وإجراءات جمع الدليل الجنائي في جرائم الاتصالات

تتسم إجراءات الاستدلال في مجال جرائم الاتصالات بذاتية خاصة، ويبدو ذلك من خلال الطابع الخاص لهذه الجرائم وتطور أساليب ارتكابها، مما يضع سلطة التحقيق أمام تحدي مواكبة تطور وسائل التحقيق والإثبات الجنائي وضرورة الاستعانة بالأساليب العلمية الحديثة وإستخدام الحاسب الآلي وشبكة الانترنت، سواء عند المعاينة الأولية للظروف المحيطة بالجريمة الإلكترونية المرتكبة، أو ما يتبع ذلك من تحفظ فوري على الدليل الإلكتروني المستمد من بيانات المستند الالكتروني في هذه المرحلة من التحقيق.

وفيما يلي نعرض لكيفية جمع الاستدلالات في جرائم الاتصالات من خلال التعرف على العناصر الأساسية لجمع الاستدلالات في جرائم الاتصالات في المطلب الأول، ثم تتناول إجراءات المعاينة التقنية في هذه المرحلة في المطلب الثاني.

المطلب الأول: العناصر الأساسية لجمع الاستدلالات في جرائم الاتصالات

يتعين قبل مباشرة أي تحقيق جنائي يتعلق بمختلف الإعتداءات الإجرامية الواقعة على وسائل الاتصال الإلكتروني مراعاة جهات التحقيق لإجراءات وقواعد أساسية قبل أو أثناء هذا التحقيق[1]، تتمثل في جمع اكبر قدر من المعلومات عن السلوك المكون للجريمة وأسلوب وظروف ارتكابها.

ووسيلة الحصول على تلك المعلومات يمكن أن يتم عن طريق مقابلات مع المجني عليه، وبناء على طبيعة السلوك الإجرامي المرتكب يتحدد نطاق وتوقيت هذا التحري والوقت الذي يستلزمه.

الفرع الأول: الطبيعة الخاصة للدليل المتحصل من الجريمة

بالنظر إلى الطابع الخاص للجريمة من جهة والدليل الرقمي المتحصل منها من جهة أخرى هناك من الاعتبارات ما يتعين وضعها في الحسبان عند إجراء عملية التحري من أهمها[2]:

- أن الدليل المستند إلى المعالجة الآلية للبيانات يمكن أن يكون متاحا لفترة قصيرة من الزمن .
- أن الجريمة التي يجرى التحري بشأنها يمكن أن تكون مستمرة من حيث نتائجها أو تنفيذها.
- أن الجريمة التي يجرى التحري بشأنها يمكن أن تكون تغطية لفعل إجرامي آخر.

وإذا ما توافرت أدلة أن هذا هو الوضع، فقد يكون من الضروري البدء على الفور في إجراء تحقيق أكثر دقة حول الواقعة والحقائق المفترض إسهام التحري الأول في إظهارها وهي:

- التثبت من وقوع الجريمة.
- نمط وطبيعة الجريمة المرتكبة.
- التقنيات المستخدمة في ارتكابها.
- الجاني (أو الجناة) المحتملون أو المشتبه فيهم.
- الأسباب والدوافع المحتملة لارتكاب الجريمة.
- الاستدلال على الشهود في حالة وجودهم.
- طبيعة الأدلة الجنائية ومصادرها.

وعند بدء التحقيق مع الأشخاص ذوي العلاقة بجرائم الاتصالات تتبع الخطوات التالية: (3)

- قبل البدء في اخذ أقوال الشهود والمشتبه فيهم أو استجواب المتهمين يقوم ضابط الشرطة القضائية وخبير الحاسب الآلي بتبادل المعلومات فيما بينهم بحيث يشرح الضابط للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم.
- يتم حصر النقاط المطلوب استيضاحها من قبل الخبير والضابط المحقق ومن ثم يتولى الضابط ترتيب تلك النقاط.
- يقوم ضابط الشرطة القضائية بالحصول على كافة المصطلحات التي يمكن إستخدامها مع بيان لمعاني تلك المصطلحات للاستفادة منها عند الضرورة.
- يضع الضابط خطة التحقيق على ضوء المعطيات الأخرى التي يراها.
- مباشرة إجراءات اخذ أقوال الشهود واستجواب المتهمين من قبل الضبطية القضائية، وبحضور الخبير والذي يجوز له توجيه الأسئلة التقنية أثناء الاستجواب وذلك وفق كيفية تم الإتفاق عليها ويفضل أن يكتب الخبير السؤال التقني على ورقة يضعها أمام ضابط الشرطة القضائية ليحدد الأخير الوقت

الذي يوجه فيه ذلك السؤال، كما أنه من الممكن إتاحة الفرصة للخبير بعد انتهاء الضبطية القضائية من إستجوابه.

- مراعاة القوانين الوطنية فيما يتصل بسلطة التحقيق، والمدى المسموح به للخبير في مشاركة الضبطية القضائية وحضور الاستجواب، ومن الأنسب في حالة الدول التي لا تسمح قوانينها بمثل هذه المشاركة إستصدار قرارات بتشكيل لجان تحقيق تضم في عضويتها الخبرات الفنية المطلوبة في كل حالة .
- مراعاة التنسيق بين الضابط المحقق والخبير في الحصول على البيانات المخزنة في الحاسب الآلي وملحقاته الخاصة بالمتهم أو الشاهد الذي يتم التحقيق معه إذ أنّ المجرم المتخصص في جرائم الحاسب الآلي يحتفظ بمعلوماته وخططه في الحاسب الآلي أو على أقراص مدمجة أو اسطوانة مرنة، ويمكن للمحقق والخبير أن يتوصلا إلى تلك البيانات وأساليب فتحها من خلال التحقيق مع الأشخاص ذوي العلاقة بجرائم التوقيع الإلكتروني، علما بان اقل خطا في مثل هذه الحالات يقضي على كافة البيانات المخزنة في الحاسب الإلكتروني. (4)

الفرع الثاني: القواعد العامة للتحقيق الجنائي الالكتروني

هناك قواعد عامة ينبغي مراعاتها لضمان نجاح التحقيق مع الأشخاص ذوي العلاقة بالحاسب الآلي وهي:

- مراعاة التعامل بين ضابط الشرطة القضائية وخبراء الحاسب الآلي العاملين في المؤسسة المتضررة من الجريمة فقد يكون خبراء المؤسسة شهود، أو متهمين، أو مساهمين في الجريمة عن قصد، أو جهل، أو إهمال .
- التركيز في البحث عن البرامج اللازمة لكشف البيانات المخزنة ووضع تدابير للمحافظة عليها وحسن إستخدامها .
- مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البريد الإلكتروني وغير ذلك من الحقوق الخاصة تفاديا لأي طعن بعدم مشروعية الأدلة التي يحصل عليها المحقق.

- العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط أجهزة الحاسب الآلي وملحقاتها (Softwear) وبرامجها.
- مراعاة حفظ الأدلة الجنائية بالطرق المناسبة لكل حالة وذلك حتى يتم تقديمها للمحكمة وهي على حالتها التي ضبطت عليها إذ أن أي تأثير أو تعديل للأدلة قد ينهي القضية لصالح المتهم الذي يفسر الشك لصالحه كقاعدة عامة. (5)

المطلب الثاني: المعاينة التقنية في مرحلة جمع الاستدلالات

لم يحدد المشرع الجزائري المقصود بالمعاينة مكتفيا بالنص عليها في العديد من مواد قانون الإجراءات الجزائية(6)، وبالرجوع إلى تعريفات الفقه الجنائي تعتبر المعاينة :" إثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة(7)"، أو هي: " إثبات حالة الأشياء والأشخاص وغيرها وهي تستلزم الانتقال إلى محل وجود الشيء أو الشخص الذي ينبغي معاينته".(8)

فالمعاينة إجراء من إجراءات التحقيق، يتم بقصد جمع الأدلة وفحصها لكشف حقيقة الجريمة، ويتطلب ذلك أن ينتقل المحقق من مقر عمله إلى مكان محدد قد يشكل مسرحا للجريمة.

وتكمن أهمية المعاينة وفعاليتها في التيسير على سلطة التحقيق في الأحوال التي تقتضيها الضرورة، ذلك أن المبادرة بالإنتقال إلى مكان الجريمة لمعاينته وضبط ما قد يوجد به من أشخاص أو أشياء، من شأنها أن تؤدي إلى المساعدة في جمع الأدلة المترتبة على ارتكاب الجاني لجريمته قبل أن تمتد إليها يد العبث أو قبل زوال معالمها .

ويثار التساؤل حول كيفية الانتقال إلى مسرح جرائم الإعتداء على وسائل الاتصال الالكتروني؟ وكيف يمكن معاينتها؟ في ظل انصراف أغلب النصوص المنظمة لإجراء المعاينة والانتقال إلى الجرائم التقليدية وإمكانية تطبيقها بخصوص معاينة مكونات الحاسب الآلي ذات الطابع المادي، والتي بإمكان ضابط الشرطة القضائية التحفظ على

الأشياء التي تعد أدلة مادية على ارتكاب الجريمة وضبطها ونسبتها إلى الفاعل مع إخطار النيابة العامة بذلك[9]. وهو ما سيتم التعرف عليه فيما يلي:

الفرع الأول: القواعد التقنية لإجراء المعاينة في جرائم الاتصالات

تقوم المعاينة على الملاحظة واثبات الحالة[10]، ويستطيع المحقق أن يقوم بذلك بنفسه أو عن طريق من يندبه لذلك من ضباط الشرطة القضائية المختصين قانونا، وأهم ما يميز المعاينة كإجراء من إجراءات التحقيق في جرائم الاتصالات هو معاينة مسرح الجريمة واثبات الحالة فيه، وليس هناك ما يمنع من استعانة ضابط الشرطة القضائية بخبير في ذلك كما في إستعانته لرفع البصمات مثلا[11]، غير أن الإنتقال لا يتم بالضرورة عبر العالم المادي، إنما عبر العالم الافتراضي (Cyber Space). وعليه يستطيع ضابط الشرطة القضائية الانتقال إلى العالم الافتراضي لمعاينة الإعتداءات سواء من مكتبه أو من مقهى الأنترنت أو اللجوء إلى مؤدي الخدمات الالكترونية أو الطرف الثالث الموثوق أو لمزود خدمة الأنترنت (Intrnet Server Provider).[12]

- **إجراءات المعاينة والتحفظ على مسرح الجريمة في جرائم الاتصالات:**

يختلف الأمر بالنسبة إلى المسرح الافتراضي عن ما هو متعارف عليه في عملية الإنتقال إلى المسرح التقليدي التي تتم بطريقة مادية، حيث يستطيع عضو النيابة أو قاضي التحقيق أو ضابط الشرطة القضائية أن يقوم بهذه المعاينة وهو جالس في مكتبه من خلال جهاز الكمبيوتر الموضوع على مكتبه[13]، أو من خلال الاستعانة بالخبراء المتخصصين في المعلوماتية، على نحو ما سيتم تفصيله لاحقا في إجراء الخبرة التقنية بالنسبة لجرائم الاتصالات.

ونتيجة لإختلاف مسرح الجريمة في جرائم الاتصالات الإلكترونية عن غيره من الجرائم، لكون هذا النوع من الجرائم يتميز بوجود الأدلة الإلكترونية ذات الطبيعة غير المرئية، وحتى تصبح معاينة مسرح الجريمة في مجال هذه الجرائم لها فائدة في كشف الحقيقة عنها وعن مرتكبها، ينبغي إتباع قواعد وإرشادات فنية أهمها[14]:

- تحديد نقطة البدء في المعاينة ونقطة الانتهاء منها بحيث تجرى المعاينة بصورةمرئية يلم فيها المحقق بكافة الجوانب التي يريد الوصول إليها من المعاينة.
- تصوير شاشة الحاسب الآلي[15]، والأجهزة الطرفية المتصلة به والمحتويات صور شمسية مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته لكي تظهر المعلومات أو الصور المطلوب معاينتها.
- ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة .
- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام، والآثار الإلكترونية التي يخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الإتصال ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام أو الموقع أو الدخول معه في حوار. [16]
- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بوسيلة الاتصال الإلكتروني محل الجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات.
- التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة القريبة من الحاسب والشرائط والأقراص الممغنطة غير السليمة أو المحطمة، وفحصها ورفع البصمات التي قد تؤدي إلى التعرف على المتهم مرتكب الواقعة.
- الإستعانة عند مباشرة المعاينة بالخبراء والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات واسترجاع المعلومات، والذين تلقوا

تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يمكن أن يحويها مسرح الجرائم المعلوماتية. (17)

- عدم نقل أية محررات إلكترونية وأية معلومات مسجلة على الحاسب من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أية مجالات لقوى مغناطيسية يمكن إن تتسبب في محو البيانات المسجلة على الوسيط المادي.
- الحصول على الاحتياجات الضرورية من أجهزة وبرامج للاستعانة بها في الفحص والتشغيل مثل برنامج معالجة الملفات (Xtree pro Gold)، وبرنامج (Encase) الذي ينتج صورا مطابقة من القرص الصلب، ويستخدم بصفة خاصة لأغراض التحقيقات الجنائية في المباحث الفدرالية الأمريكية ويسميها الخبراء "حقيبة الأدلة الرقمية".(18)
- السيطرة على الدائرة المحيطة بمكان المعاينة بوضع حراسات كافية لمراقبة التحركات داخل الدائرة أو لإمكان العودة لإجراء معاينة أخرى فيما بعد حتى يتم الانتهاء من التحقيق.

الفرع الثاني: تصنيف بيانات المستند الالكتروني:

يحتفظ مؤدوا خدمات الاتصالات الالكترونية في إطار تأدية خدماتهم بالمستندات الالكترونية وما تتضمنه من بيانات ومعلومات سرية، ونظرا لتعدد وتنوع هذه البيانات فقد بات من الضروري تصنيفها من قبل رجال الضبط القضائي عند التنقيب على الدليل الإلكتروني في جرائم الاتصالات. وقد تضمن القسم الثاني عشر من قانون الإجراءات الجنائية الإلكترونية الأمريكي لسنة 2000 تقسيما لأنواع المعلومات والبيانات محل البحث حيث قسمها إلى نوعين:

- بيانات تتعلق بمضمون المستند الإلكتروني

- بيانات تتعلق بالمشترك والمستهلك في المستند الإلكتروني.

ونصـــــــــتالفقرة 8 منالقسمالثانيعشرمنقانونا لإجراءاتالجنائيةالإلكترونيةالأمريكيلســــــــــنة 2000،علىتعريفتلكالبياناتبأنها:"البياناتأوالمحتوىأوالمضمونالذييتضمنهالإتصالالإلكتروني". علىذلكيمكنناالقولانجميعالبياناتالجوهريةالتييتضمنهاالمســتندالإلكترونيوالتيتكونمحلاللإعتداءأوتستخدمفيالتزويرالإلكترونيأوإعدادبرنامجلإتلاف مســـــــــــــــتند الكترونيأوتعييبهيبياناتجوهريةيتعينعلىرجالالضبطإلزاممقدميخدماتالاتصـــــــــــــــالات الالكترونية،ومقدميخدماتالحاسبالاليبتقديمهاحتيتسنىتحليلهاوالوصولمنخلالهاللدليلالإلكترونيال مؤديلإدانةالمتهمفيتلكالجرائم.

المبحث الثاني:أدلة الإثبات التقنية في جرائم الاتصالات

بالنظر إلى الطبيعة الخاصة لجرائم الإعتداء على وسائل الاتصال الالكترونية، صارت عملية الكشف عن هذه الجرائم تتطلب إتباع استراتيجيات خاصة تتعلق بإكساب القائمين بجمع الدليل مهارات خاصة على نحو يساعدهم على مواجهة تقنيات الحاسب الآلي وشبكاته، بحيث تتعقد وتتنوع التقنيات المرتبطة بارتكاب تلك الجرائم، استخدام تقنيات تحقيق جديدة ومبتكرة لتحديد نوع الجريمة المرتكبة وشخصية مرتكبها وكيفية ارتكابها مع الاستعانة بوسائل جديدة أيضا لضبط الجاني والحصول على أدلة إدانة .

على ذلك سيتم تقسيم المبحث إلى مطلبين على النحو التالي:

- المطلب الأول:التفتيش واستخلاص الدليل الرقمي
- المطلب الثاني: الدليل الرقمي ومجاله في الإثبات الجنائي

المطلب الأول: التفتيش واستخلاص الدليل الرقمي

يعتبر إجراء التفتيش الخطوة الأولى في مباشرة التحقيق الذي يتولاه قاضي التحقيق أو ضابط الشرطة القضائية المنوب.

الفرع الأول: موقف المشرع الجزائري

نصت المادة (84) من قانون الإجراءات الجزائية الجزائري في فقرتها الأولى على انه: " إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات فان لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الاطلاع عليها قبل ضبطها مع ما تقتضيه ضرورات التحقيق وما توجبه الفقرة الثالثة من المادة83...".[19]

وفي هذا الصدد نص القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، على جملة من القواعد الإجرائية المتعلقة بتفتيش المنظومة المعلوماتية وحجز المعطيات، منسجما في ذلك مع نصوص الإتفاقية الأوربية لمكافحة الإجرام المعلوماتي والإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وينصب التفتيش على المكونات المادية للحاسب بأوعيتها المختلفة للوصول إلى دليل يتصل بارتكاب جريمة من جرائم الاتصالات الالكترونية وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبيها. [20]

الفرع الثاني: تفتيش المنظومة المعلوماتية

نصت المادة (05) من القانون 04/09 تحت عنوان " تفتيش المنظومات المعلوماتية " على: " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه، الدخول بغرض التفتيش ولو على بعد إلى:

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

من خلال هذه المادة يجيز المشرع الدخول إلى المنظومة المعلوماتية دون إذن صاحبها ولو عن بعد بغرض التفتيش، ونظرا لصعوبة تنفيذ هذا الإجراء من الجانب التقني، انجاز المشرع بنص المادة (6/05) من القانون رقم: 04/09 سالف الذكر الاستعانة بكل

شخص له دراية بعمل المنظومة المعلوماتية محل البحث والتفتيش أو بالتدابير المتخذة لحماية المعطيات المعلوماتية.

وخلافالإجراء تفتيش المكونات المادية للحاسوب الذي يتطلب إذنا مكتوبا من طرف وكيل الجمهورية أو قاضي التحقيق وفقا لأحكام المادة (44) من (ق.ا.ج.ج)، فان إجراء تفتيش المنظومة المعلوماتية لوسيلة الاتصال الالكترونية كلها أو جزء منها تنصب حول الكيان المنطقي للحاسوب، أي أنّ التفتيش يستهدف أشياء غير مادية. [21]

المطلب الثاني: الدليل الرقمي ومجاله في الإثبات الجنائي

نتيجة للتطور العلمي وانتشار التقنية الرقمية في التعاملات اليومية، أصبحت تستعمل تلك التقنية كوسيلة لارتكاب الجرائم تارة، وكموضوع للجريمة تارة أخرى، وبذلك اختلف الوسط الذي ترتكب فيه الجريمة، من وسط مادي إلى وسط معنوي أو ما يعرف بالوسط الافتراضي، وهو ما استتبع ظهور طائفة جديدة من الأدلة تتفق وطبيعة الوسط الذي ارتكبت فيه الجريمة، وهي الأدلة الرقمية أو ما يسمى بالأدلة الإلكترونية.

الفرع الأول : التعريف بالدليل الرقمي

نظرا لحداثة وأهمية الدليل الرقمي، تعددت التعريفات وإختلفت بخصوص وضع تعريف شامل له لعل من أبرزها أنه: " تلك الأدلة التي يمكن الحصول عليها بإحدى وسائل الإخراج"[22]، أو هو: " الدليل المأخوذ من أجهزة الكمبيوتر، يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها بإستخدام برامج تطبيقات وتكنولوجيا، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الإشكال والرسوم، وذلك من أجل إعتماده أمام أجهزة إنفاذ وتطبيق القانون".[23]

وترجع تسمية الدليل الرقمي إلى أن البيانات داخل الوسط الإفتراضي سواء كانت صورا أو تسجيلات أو نصوص تأخذ شكل أرقام على هيئة الرقمين(1 أو 0) ويتم تحويل هذه الأرقام عند عرضها لتكون في شكل صورة أو مستند أو تسجيل.[24]

الفرع الثاني: مجالات إعمال الدليل الرقمي في الإثبات الجنائي

أدى إنتشار استخدام تقنية المعلومات الرقمية وتعاظم دورها مع دخول الانترنت شتى مجالات الحياة إلى الاهتمام بالدليل الرقمي قياسا بغيره من الأدلة الأخرى المستمدة من الآلة، وأصبح بذلك هذا الوسط مرتعا لطائفة من الجناة يطلق عليهم اسم المجرمين المعلوماتيين، فالجرائم التي يرتكبها هؤلاء تقع في الوسط الافتراضي أو ما يمكن تسميته بالعالم الرقمي[25]، ولذا كان الدليل الرقمي هو الدليل الأفضل لإثبات هذا النوع من الجرائم، لأنه من طبيعة الوسط الذي ارتكبت فيه، ومن هنا بدت أهمية هذا النوع من الأدلة، ذلك أن الدليل الرقمي كدليل إثبات لا ينحصر مجاله فقط على جرائم المعلوماتية التي من ضمنها جرائم التوقيع الإلكتروني، إنما يصلح في ذات الوقت لإثبات الجرائم التقليدية، مثلما يعتبر الدليل الأفضل لإثبات الجرائم المعلوماتية.

خاتمة:

أخيرا، مما لا ريب فيه أن الإجراءات التقنية التي تعتمد على الدليل الرقمي أصبحت جزءا لا يتجزأ من البحث الجنائي الذي يستهدف الكشف عن الجرائم ذات العلاقة بعالم الإتصالات وهو ما تناوله البحث الذي انتهى إلى النتائج والتوصيات التالية:

أولا: النتائج

- إن جرائم الإتصالات تعتمد على آليات متطورة في تنفيذ السلوك الاجرامي لذا كان من الضروري ظهور ما يسمى الإثبات العلمي في المجال الجنائي للكشف عن هذه الجرائم.
- أجازت أغلب التشريعات اعتماد الوسائل العلمية الحديثة للحصول على الأدلة الرقمية سواء للكشف عن المجرمين أم للإثبات الجنائي.

ثانيا: التوصيات

- ضرورة إلمام القاضي الجنائي بتقنية وعلوم المعالجة الآلية للمعلومات لمواكبة المناقشة العلمية للمخرجات الإلكترونية ذات الصلة بجرائم الاتصالات.

- تعديل قانون الإجراءات الجزائية وغيره من التشريعات ذات الصلة بما يتوافق مع طبيعة جرائم الاتصالات.
- زيادة العناية بأعمال الخبرة الفنية القضائية المتخصصة بالإثبات العلمي التقني لجرائم الاتصالات والاستفادة من الخبرات الأجنبية.

الهوامش:

[1]–جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002، ص119.

[2]– هشام محمد فريد رستم، الجوانب الإجرائية للجريمة المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط 1994 ص 106، 105 .

[3]– محمد الأمين البشرى، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر "القانون والكمبيوتر والأنترنت، جامعة الإمارات العربية المتحدة، العين في الفترة ما بين 1 و3 ماي 2000، " ص358 وما بعدها.

[4]–بن قارة مصطفى عائشة، الحماية الجنائية للحكومة الإلكترونية، رسالة دكتوراه، جامعة ابو بكر بلقايد، تلمسان، 2018، ص215.

[5]–ياسر محمد أبو حطب، الحماية الجنائية والأمنية للتوقيع الإلكتروني، الحماية الجنائية والامنية للتوقيع الإلكتروني ،منشأة المعارف، الاسكندرية، مصر،2014، ص240.

[6]– حيث تنص المادة 79 من (ق.ا.ج.ج) على: " يجوز لمقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها.."

– وفي نفس السياق نصت المادة 42 من (ق.ا.ج.ج) على: " يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية ويتخذ جميع التحريات اللازمة وعليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي وأن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة..." .

– كما نصت المادة 235 (ق.إ.ج.ج) على أنه: " يجوز للجهة القضائية إما من تلقاء نفسها أو بناء على طلب النيابة العامة والمدعي المدني أو المتهم أن تأمر بإجراء الانتقالات اللازمة لإظهار الحقيقة..." .

– راجع في هذا الإطار المواد: (47) و(50) و(62)من(ق.ا.ج.ج)

[7]–فؤاد حسن العزيزي، الجرائم المعلوماتية، دراسة مقارنة، دار الفكر الجامعي الإسكندرية، مصر، 2015، ص 195 .

[8]– نصر شومان، التكنولوجيا الجرمية الحديثة، وأهميتها في الإثبات الجنائي، شركة المؤسسة الحديثة في الكتاب، طرابلس، لبنان، ط1، 2011، ص 151.

[9]–عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، ط1، 2003.

[10]– عمر سالم، الوجيز في شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2011–2012، ص219.

[11]–مأمون سلامة، قانون الإجراءات الجنائية معلقا عليه بالفقه وأحكام النقض، الجزء الأول، مكتبة رجال القضاء، الطبعة الثانية، 2005، ص 643.

[12]– نبيلة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، 2013، ص218.

[13]–عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2004، ص 895.

[14]– احمد عاصم عجيلة، الحماية الجنائية للمحررات الإلكترونية، الحماية الجنائية للمحررات الإلكترونية، دار النهضة العربية،القاهرة،2014، ص438.

[15]–جميل عبد الباقي الصغير، جرائم الأنترنت، الأحكام الموضوعية والجوانب الإجرائية، طبعة نادي القضاة، 2010، ص 24.

[16]–عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 104.

[17]–هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الالات الحديثة، اسيوط، مصر،1994، ص60.

[18]–عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الاسكندرية، مصر،2010، ص 85.

[19]–أضاف المشرع الفرنسي البحث عن البيانات المعلوماتية (Données informatiques) إلى البحث عن المستندات.

[20]–إبراهيم حامد مرسي، سلطات مأمور الضبط القضائي، دراسة مقارنة، رسالة دكتوراه، الطبعة الثانية، 1997، ص743، ص743 .

[21]–Chaque partie adopte les mesures législative et autre qui se révèlent nécessaire pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du

système informatique ou les mesures appliquées pour protéger les donner informatique qui contient de fournir toutes les information raisonnablement nécessaire , pour permettre l'application des mesures visées par les paragraphes 1 et 2 convention européenne de la cybercriminalité, Op.Cit,p.10.

[22]–سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الاثبات الجنائي، دراسة مقارنة، دار الكتب القانونية، مصر، 2011، ص55.

[23]–ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006، ص77.

[24]–ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشورضمن أعمال مؤتمر "الأعمال المصرفية والإلكترونية"، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، في الفترة من: 10 إلى 12 ماي لسنة 2004، المجلد الخامس، ص2238 .

[25]–ياسر الكومي، مرجع سابق، ص266

المراجع:

الكتب:

- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002.
- فؤاد حسن العزيزي، الجرائم المعلوماتية، دراسة مقارنة، دار الفكر الجامعي الإسكندرية، مصر، 2015.
- نصر شومان، التكنولوجيا الجرمية الحديثة، وأهميتها في الإثبات الجنائي، شركة المؤسسة الحديثة في الكتاب، طرابلس، لبنان، ط1، 2011.

- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، ط1، 2003.
- عمر سالم، الوجيز في شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2011-2012.
- مأمون سلامة، قانون الإجراءات الجنائية معلقا عليه بالفقه وأحكام النقض، الجزء الأول، مكتبة رجال القضاء، الطبعة الثانية، 2005.
- نبيلة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، 2013.
- احمد عاصم عجيلة، الحماية الجنائية للمحررات الإلكترونية، دار النهضة العربية،القاهرة،2014.
- جميل عبد الباقي الصغير، جرائم الأنترنت، الأحكام الموضوعية والجوانب الإجرائية، طبعة نادي القضاة، 2010.
- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.
- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة،مكتبة الالات الحديثة، مصر،1994.
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الاسكندرية، مصر،2010.
- سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الاثبات الجنائي، دراسة مقارنة، دار الكتب القانونية، مصر، 2011.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006.
- ياسر محمد الكومي، الحماية الجنائية والامنية للتوقيع الإلكتروني ،منشأة المعارف، الاسكندرية، مصر،2014.
- خالد ممدوح إبراهيم، حجية البريد الالكتروني في الاثبات، دراسة مقارنة، دار الفكر الجامعي، الاسكندرية،2008.

- عبد الفتاح بيومي حجازي، الدليل الرقمي والتزوير في جرائم الكمبيوتر والأنترنت، دراسة معمقة في جرائم الحاسب الآلي والأنترنت.
- ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، مركز شرطة دبي، 2005.
- حسن إبراهيم، الحماية الجنائية لحق المؤلف عبر الأنترنت، رسالة دكتوراه، دار النهضة العربية.
- ابوبكر يونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي، دار الفكر العربي، مصر 2005.
- عمر ابوبكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت(الاحكام الموضوعية والجوانب الاجرائية)، دار النهضة العربية،مصر،2004.
- احمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الاثبات الجنائي، دراسة مقارنة، دار النهضة العربية، مصر، 2015
- **الملتقيات:**
- هشام محمد فريد رستم، الجوانب الإجرائية للجريمة المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط 1994 .
- محمد الأمين البشرى، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر "القانون والكمبيوتر والأنترنت، جامعة الإمارات العربية المتحدة، العين في الفترة ما بين 1 و3 ماي 2000.
- ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر "الأعمال المصرفية والإلكترونية"، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، في الفترة من: 10 إلى 12 ماي لسنة 2004، المجلد الخامس.
- راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، بحث مقدم للمؤتمر الدولي الأول حول حماية المعلومات والخصوصية في قانون الأنترنت، الفترة: 2-4/يونيو 2008، منشور على الأنترنت، ص5 وما بعدها، على الموقع:
- http: //www.f-law.net تاريخ الزيارة 2019/8/22
- **رسائل الدكتوراه:**

- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2004.
- إبراهيم حامد مرسي، سلطات مأمور الضبط القضائي، دراسة مقارنة، رسالة دكتوراه، الطبعة الثانية، 1997.
- بن قارة مصطفى عائشة، الحماية الجنائية للحكومة الإلكترونية، رسالة دكتوراه، جامعة ابو بكر بلقايد، تلمسان، 2015.

القوانين:

- الأمر 155/66 المؤرخ في 08 يونيو عام 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.
- القانون 09-04 المؤرخ في:2009/08/05، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنلوجيا الاعلام والاتصال ومكافحتها (ج ر) عدد:07