مجلة
البحوث والدراسات القضائية والقانونية

التحقيق الرقمي
«الأدوات والتقنيات المستخدمة في الإثبات الجنائي» *

الباحث / عمرو عبده محمد العماري

* قدمت هذه الدراسة استكمالاً لمتطلبات الحصول على درجة الدبلوم الجنائي - قسم التأهيل المستمر لدى المعهد العالي للقضاء.

الملخص:

هدفت الدراسة إلى التعرف على عملية التحقيق الرقمية والتقنيات المستخدمة في الإثبات الجنائي وبيان موقف المشرع اليمني تجاه هذا النوع من التحقيقات، وتم استخدام المنهج الوصفي التحليلي لدراسة التحقيق الرقمي وخصائصه ووصف الأدوات المستخدمة فيها، وتحليل النصوص التشريعية اليمنية ذات الصلة بموضوع البحث، وأظهرت الدراسة عدة نتائج أهمها: وجود فراغ تشريعي وقانوني يعاني منه التحقيق الرقمي في اليمن، بالإضافة إلى عدم معرفة السلطات القضائية من أعضاء النيابة وقضاة للمعلومات الفنية الأساسية الخاصة بالجرائم الالكترونية والتحقيق فيها، مما يجعلهم في بعض الحالات يستعينون بخبراء في التكنولوجيا من غير السلطة القضائية لتوضيح مدى قوة الدليل الالكتروني في التحقيق، كما قدمت الدراسة عدة توصيات أهمها: إعداد دليل إرشادي يتضمن المبادئ التوجيهية والإجراءات الخاصة بكيفية التحقيق في الجرائم الالكترونية، حتى يكون التحقيق والإثبات يعتمد على أساس علمي سليم غير قابل للطعن.

المقدمة:

الحمد لله العادل في حكمه، القاضي بين عباده بعلمه، أحمده على ما حكم وقضى، وأشكره على ما أبرم وأمضى، وأشهد أن لا إله الا الله وحده لا شريك له وأن محمداً عبده ورسوله، وبعد:

أصبح التقدم التكنولوجي السريع أحد أبرز معالم العصر الحديث، وأضحى المحرك الأساسي لكافة المجالات وقطاعات الحياة، حيث انعكست تطورات التكنولوجيا بشكل ملحوظ على حياتنا اليومية وأساليب العمل فيها، واتسم هذا التقدم بتحسين الكفاءة في شتى مجالات الحياة المختلفة، حيث أدى ظهور الهواتف النقالة والإنترنت والتطبيقات إلى وجود علاقة قوية بين الأفراد والمؤسسات، الأمر الذي أظهر في طياته تحديات وآثاراً سلبية قد تنشأ بسبب هذه العلاقة، منها على سبيل المثال لا الحصر الجرائم الإلكترونية التي طفت على السطح مؤخراً نتيجة هذا التقدم والتي أظهرت تقنيات جديدة للتحقيق بهذه الجرائم تختلف عن التحقيقات التقليدية.

حيث يشكل التحقيق الرقمي أحد أبرز التطورات الحديثة والتي تختص بالتحقيق في الجرائم الإلكترونية التي تمتاز بخصوصية في الأساليب والتقنيات المستخدمة فيها، كما أن مفهوم أدلة الإثبات التقليدية أمام القضاء تغيرت، وما أظهره من انعكاسات على صعوبة إثبات الأدلة في الإثبات الجنائي الإلكتروني لدى سلطات التحقيق المختصة، أصبحت إجراءات التحقيق في الجرائم الإلكترونية والأدلة الإلكترونية تتمتع بطبيعة وخصوصية جعلت تحقيقها وإثباتها مختلفة عن التحقيق الجنائي في الجرائم العادية، إذ يكون التحقيق في الجريمة المعلوماتية تحقيقاً جنائياً معلوماتياً باعتبار مسرح ومحيط هذه الأخيرة هو الفضاء الإلكتروني والبيانات التقنية.

وتأسيساً على ذلك نسلط الضوء في بحثنا هذا على بيان ماهية التحقيق الرقمي والأساليب المستخدمة في الإثبات الجنائي كموضوع مستحدث، وذلك من الناحية الفنية كالأدوات والتقنيات المستخدمة في إجراء التحقيق الرقمي، والناحية القانونية كموقف التشريعات والنظم اليمنية لبيان الإجراءات القانونية الواجب اتباعها من قبل سلطات التحقيق المختصة في كشف وإثبات الجريمة وأدلتها.

مشكلة البحث:

إن الأنشطة الإجرامية التي تتم بواسطة التكنولوجية الرقمية وشبكات الإنترنت بغرض تحقيق مكاسب مالية أو سرقة بيانات أو إلحاق الضرر بالآخرين أو نشر الفوضى

تتسم بأنها تنفذ عن بُعد وبالتالي نواجه صعوبة في التحقيق فيها، لذا فإن مشكلة البحث تكمن في آلية التحقيق المستخدمة في مثل هذه الجرائم، وعليه يتمثل السؤال الرئيس في:

«ماهية التحقيق الرقمي والأساليب والتقنيات المستخدمة في الإثبات الجنائي؟»

ويتفرع منه عدة تساؤلات كالآتي:

١. ماذا يقصد بالتحقيق الرقمي؟
٢. ما هي الأدوات والتقنيات المستخدمة في الإثبات الجنائي؟
٣. كيف تعامل المشرع اليمني تجاه التحقيقات الرقمية في الإثبات الجنائي؟

أهداف البحث:

١ .التعرف على ماهية التحقيق الرقمي.
٢. معرفة الأدوات والتقنيات المستخدمة في الإثبات الجنائي.
٣. تسليط الضوء على موقف المشرع اليمني تجاه التحقيقات الرقمية في الإثبات الجنائي.

أهمية البحث:

توجد أهمية علمية وعملية للبحث أوجزها كالآتي:

الأهمية العلمية:

١. تكمن أهمية البحث في الدور الذي لعبته التكنلوجيا الحديثة من تطورات في مجال التحقيق الجنائي، سواء على مستوى التحقيق الجنائي في الجرائم التقليدية أو الإلكترونية المستحدثة والمتطورة، وإسهاماتها أيضاً في تغيير مفهوم أدلة الإثبات الجنائية، وتطور ضبط الأدلة الرقمية وجمعها، وازدياد الصعوبات العملية الإثباتية نتيجة تدخل الحاسب الآلي وشبكات الإنترنت في كافة المجالات الحياتية وما طرأ عليها من تطورات وتنام للظواهر الإلكترونية الضخمة.
٢. كما تكمن أهمية هذا البحث في أنه يقدم دراسة نظرية عن الإثبات العلمي في التحقيق الجنائي الرقمي من الجوانب الفقهية والقانونية والفنية في مجال الإثبات الجنائي.

الأهمية العملية للبحث:

١. الكشف عن الجرائم الإلكترونية: التحقيق الرقمي يُعد أداة أساسية في مكافحة الجرائم الإلكترونية مثل الاحتيال، القرصنة، والتسلل إلى الشبكات. يُمكن من تتبع الهجمات والتهديدات الرقمية، مما يعزز قدرة الجهات الأمنية على اكتشاف الجناة واتخاذ الإجراءات اللازمة.

٢. التحقيق في الجرائم التقليدية: في العديد من الجرائم التقليدية مثل القتل أو السرقة، يمكن أن يوفر التحقيق الرقمي أدلة حاسوبية تساهم في بناء قضية قوية. على سبيل المثال، يمكن للأدلة الرقمية مثل الرسائل النصية أو بيانات الهاتف المحمول أن تساهم في تحديد المشتبه فيهم أو تقديم أدلة تدعم أو تنفي التهم.

٣. التعامل مع الحوادث الأمنية: في حال حدوث اختراقات للأمن السيبراني أو تسريبات بيانات وتطوير استراتيجيات لتحسين الأمن الوطني.

٤. تحليل الأدلة في قضايا العمل والقانون: يمكن استخدام التحقيق الرقمي في بيئة العمل لتحليل سجلات البريد الإلكتروني أو الأنظمة الرقمية لتحديد المسؤوليات، خاصة في القضايا القانونية أو التأديبية.

أسباب اختيار البحث:

ثمة أسباب شخصية وأسباب موضوعية تكمن وراء اختياري هذا الموضوع وهي كالآتي:

الأسباب الشخصية:

١. التخصص الوظيفي: حيث أن الباحث مهمته الأساسية هي تحقيق العدالة والمساهمة في مكافحة الجريمة، فإن التحقيق الرقمي الجنائي يمكن أن يكون طريقة فعالة لتحقيق ذلك، والعمل في هذا المجال يمكن أن يعزز من مهارات التحليل والتفكير النقدي لدى الباحث، مما يفتح آفاقًا مهنية واسعة.

٢. حب التكنولوجيا والتحديات التقنية: إذ أن الباحث يجد متعة في فهم كيفية عمل الأنظمة الرقمية واكتشاف الأساليب الحديثة في تحليل الأدلة الرقمية.

٣. الرغبة في حماية المجتمع: لدى الباحث دافع قوي لحماية المجتمع والأفراد من الجرائم الرقمية، مثل الاحتيال الإلكتروني والابتزاز الرقمي.

الأسباب الموضوعية:

١. معرفة مدى مواكبة التشريع اليمني للتطورات العلمية الحديثة لاسيما في مجال الأثبات الجنائي في ظل تطور الأساليب الإجرامية بتطور وتنوع الوسائل التكنلوجية الرقمية الحديثة.

٢. حداثة الموضوع وكثرة الإشكاليات التي تواجه مأموري الضبط القضائي والنيابة العامة أثناء التحقيق في الوقائع الجنائية الرقمية وأثباتها.

٣. التطور التكنلوجي المتسارع في عالم التطبيقات الرقمية والحواسيب ووسائل التواصل والمراسلات الرقمية وما يشكل ذلك من خطورة عند استخدامها في ارتكاب الجرائم بواسطتها وعندئذ صعوبة الحصول على الأدلة التي تكشف الوقائع الإجرامية ومعرفة مرتكب تلك الوقائع ومدى مشروعية تلك الأدلة في القانون اليمني.

٤. زيادة الجرائم الإلكترونية: مع تزايد عدد الجرائم الإلكترونية مثل الاحتيال، الهجمات السيبرانية، والابتزاز، أصبح التحقيق الرقمي ضرورة للكشف عن هذه الجرائم ومكافحتها.

مصطلحات البحث:

تضمن البحث العديد من المصطلحات الأساسية التي ترتكز عليها مفاهيم الدراسة، أهمها: التحقيق الرقمي، الأدوات والتقنيات:

التحقيق الرقمي:

التحقيق في اللغة مأخوذ من حقق يحقق تحقيقاً، وحققت الأمر أي تيقنته أو جعلته ثابتاً لازماً[١]، ويقال: حق الأمر على الحق: أي غلبه وأثبته عليه[٢].

ومصطلح الرقمي أو الرقمية (Digital)، هو مصطلح حديث، يرجع أصله إلى استخدام النظام الرقمي الثنائي (١،٠) وهي الصيغة التي تسجل بها كل البيانات (أشكال وحروف ورموز وغيرها) داخل الحاسب الآلي، حيث يمثل (٠) وضع الإغلاق Off، والواحد (١) وضع التشغيل On، ويمثل الرقم صفر أو الرقم واحد ما يعرف بالبيت Bit، ويشكل

(١) الفيومي، أحمد محمد. (بدون تاريخ). قاموس اللغة «كتاب المصباح المنير» الجزء الثاني، مادة «حقق»، دار نوبليس، مصر.

(٢) المعجم الوسيط، مجمع اللغة العربية، الجزء الأول، دار المعارف، مصر، (١٤٠٠هـ).

عدد (٨ بت) ٨ Bits ما يعرف بالبايت[١].

والتعريف الإجرائي لمصطلح التحقيق الرقمي هو: «العملية المنهجية التي يتم من خلالها جمع، حفظ، تحليل، وتقديم الأدلة الرقمية المتعلقة بالجرائم باستخدام الأجهزة الرقمية والأنظمة الإلكترونية. يهدف التحقيق إلى استعادة المعلومات المخزنة على الأجهزة أو الشبكات الإلكترونية، وتحليلها للكشف عن الأنشطة الإجرامية، وتقديم الأدلة في سياق قانوني يمكن استخدامه في المحاكم».

الأدوات والتقنيات:

الأدوات جمع ومفردها أداة، وهي ما يستعان به لإنجاز غرض من الأغراض، آلة القلم أي «القلم أداة عمل»، وأداة رسم جداول» أي أداة تستعمل لطبع حروف بارزة»[٢].

والتقنيات جمع مفردها تقنية، وتعني جملة من المبادئ التي تعين على إنجاز شيء أو تحقيق غاية، وتقوم على أسس علمية دقيقة[٣].

والتعريف الإجرائي لمصطلح الأدوات والتقنيات، فيقصد بها: «الأدوات والوسائل الإلكترونية المستخدمة في التحقيق الرقمي، كالحاسب الآلي وشبكة الإنترنت، والمعاملات الإلكترونية، وتقنيات ومواقع التواصل الاجتماعي، التي تساعد في كشف الأنشطة الإجرامية، وتقديم الأدلة في سياق قانوني يمكن استخدامه في المحاكم».

منهج البحث:

استخدم البحث المنهج الوصفي التحليلي لدراسة التحقيق الرقمي وخصائصه ووصف للأدوات المستخدمة في هذه التحقيقات، وتحليل النصوص التشريعية اليمنية ذات الصلة بموضوع البحث.

صعوبات البحث:

هناك العديد من الصعوبات والتحديات التي تواجه الباحث في هذا المجال، منها:

---

(١) فرغالي، عبد الناصر محمد محمود؛ المسماري، محمد عيج سيف سعيد. (١٢-١٤/١١/٢٠٠٧م). الإثبات الجنائي بالأدلة الرقمية والفنية «دراسة تطبيقية مقارنة». المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف للعلوم الأمنية، ص ٥.

(٢) معلوف، لويس، المنجد في اللغة العربية، الجزء الثاني، دار الشروق، بيروت، ص ١٤.

(٣) مجمع اللغة، المعجم الوسيط، ج٢، مادة «التقنية».

١. نقص الموارد البحثية والمراجع وصعوبة الوصول إلى البيانات والمعلومات اللازمة للبحث.

٢. لا توجد قوانين في الجمهورية اليمنية ذات صلة بموضوع البحث، وإن وجدت بعض النصوص في القوانين النافذة إلا أنها لم تسعف الباحث ليثري موضوع البحث.

٣. كما واجه الباحث عراقيل وصعوبات بسبب شحة الدخل المالي الذي يتطلب أحياناً شراء مراجع حديثة من الإنترنت أو المكتبات، وهذا قد يؤثر سلباً في موضوع البحث.

تقسيمات البحث:

المبحث الأول: التحقيق الرقمي.

المطلب الأول: مفهوم التحقيق الرقمي.

المطلب الثاني: نطاق التحقيق الرقمي ومتطلبات تطبيقه.

المبحث الثاني: آليات التحقيق الرقمي.

المطلب الأول: الأدوات والتقنيات المستخدمة في الإثبات الجنائي.

المطلب الثاني: إجراءات الإثبات الجنائي في التحقيق الرقمي.

المبحث الثالث: موقف المشرع اليمني من التحقيق الرقمي.

المطلب الأول: الأحكام الموضوعية في التحقيق الرقمي في الإثبات الجنائي.

المطلب الثاني: الأحكام الإجرائية في التحقيق الرقمي في الإثبات الجنائي.

الخاتمة:

النتائج

التوصيات

المصادر والمراجع.

المبحث الأول
ماهية التحقيق الرقمي ونطاق تطبيقه

تمهيد:

التحقيق الرقمي يمتاز بخصوصية تميزه عن التحقيق في الجرائم التقليدية، خاصة فيما يتعلق بطبيعة الجريمة ذاتها ومسرحها وأدلتها، التي تقتضي ضرورة تطوير أساليب التحقيق الجنائي بصورة تجعله يتلاءم مع هذا النوع من الجرائم.

وفي هذا المبحث سنتناول مفهوم التحقيق الرقمي، ونطاق ذلك التحقيق ومتطلبات تطبيقه في مطلبين، على النحو التالي:

المطلب الأول
مفهوم التحقيق الرقمي

لتحديد مفهوم التحقيق الرقمي، ينبغي علينا بيان المقصود بمصطلح التحقيق الرقمي في الفرع الأول، ومن ثم بيان أهم المبادئ الأساسية الحاكمة للإثبات الجنائي بشكل عام في الفرع الثاني، والخصائص التي يتميز بها التحقيق الرقمي في الفرع الثالث، وذلك على النحو التالي:

الفرع الأول
المقصود بالتحقيق الرقمي

قد يعتقد البعض أن مصطلح الجريمة الرقمية «Digital Crime» أو الدليل الرقمي «Digital Evidence» يعني أن موضوعهما هو الأرقام، أو ينصب على الأرقام، وهو ما يجافي حقيقة هذا المصطلح، فهذا المصطلح التقني يرجع أصله إلى استخدام النظام الرقمي الثنائي (١،٠) وهي الصيغة التي تسجل بها كل البيانات (أشكال وحروف ورموز وغيرها) داخل الحاسب الآلي، حيث يمثل (٠) وضع الإغلاق Off، والواحد (١) وضع التشغيل On، ويمثل الرقم صفر أو الرقم واحد ما يعرف بالبيت Bit، ويشكل عدد (٨ بت) ٨ Bits ما يعرف بالبايت[١].

(١) فرغالي، عبد الناصر؛ والمسماري، محمد، الإثبات الجنائي بالأدلة الرقمية والفنية، مرجع سابق، ص ٥.
– معلوف، لويس، المنجد في اللغة العربية، الجزء الثاني، دار الشروق، بيروت، ص ١٤.

وبالتالي فإن المقصود بالتحقيق الرقمي في نطاق هذا البحث- كما أوردنا في المقدمة- ظهر من خلال تعريفه بأنه: «العلم الذي يجمع ما بين القانون وعلوم الحاسب الآلي لجمع وتحليل البيانات من الأنظمة والشبكات والاتصالات اللاسلكية ووسائط التخزين بهدف جمع الأدلة بشكل يمكن اعتمادها كدليل مقبول في المحكمة وبشكل يساعد في الوصول لهدف التحقيق»[1].

الفرع الثاني

المبادئ الأساسية الحاكمة للإثبات الجنائي (التقليدي والرقمي)

لا اختلاف بين إجراءات التحقيق في الجرائم التقليدية أو الجرائم الإلكترونية، من حيث الالتزام بالمبادئ الأساسية الحاكمة للإثبات الجنائي، إذ يعتبر قانون الإجراءات الجزائية سياج الأمان للمجتمع والفرد (المتهم) على السواء، إذ أنه يمكن الأول من اقتضاء حقه في العقاب، كما يحقق للثاني الضمانات التي تمكنه من الدفاع عن نفسه، ورد التهمة المنسوبة إليه، انطلاقاً من المبدأ العام القاضي «إن المتهم بريء حتى تثبت إدانته المكرسة دستورا»[2].

وسنوجز في هذا المطلب أهم المبادئ الأساسية التي تحكم الإثبات الجنائي للجرائم التقليدية والرقمية المتمثلة في:

أولاً: مبدأ الأصل في الإنسان البراءة:

نصت المادة (٤٧) من الدستور على أن: المسئولية الجنائية شخصية ولا جريمة ولا عقوبة إلا بناء على نص شرعي أو قانوني وكل متهم برئ حتى تثبت إدانته بحكم قضائي بات، ولا يجوز سن قانون يعاقب على أي أفعال بأثر رجعي لصدوره».

وتأسيساً على هذا النص فإن أصل البراءة يعتبر مبدأ دستورياً لا يجوز بأي حال من الأحوال خرقه، والمقصود به أن المتهم بريء حتى يقوم الدليل القاطع والمقنع على إدانته وإثباتها بحكم قضائي، وعدم توقيع الجزاء إلا بعد صدور حكم من جهة قضائية وصيرورة ذلك الحكم نهائياً وباتاً. ومما ينبغي الإشارة إليه أن الأصل في المتهم البراءة هي قرينة قانونية بسيطة تقبل إثبات العكس، وتبقى هذه القرينة قائمة إلى غاية صدور حكم

(١) اسخيطة، رضوان. التحقيق الجنائي الرقمي في ضوء قوانين حماية البيانات الشخصية، مجلة العلوم السياسية والقانون، العدد (١٧)، المجلد (٠٣)، سبتمبر ٢٠١٩م، ص ٤٦.

(٢) بيراز جمال. (٢٠١٣/٢٠١٤). الدليل العلمي في الإثبات الجنائي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر – باتنة، الجزائر، ص ٢٤.

نهائي يكون عنواناً للحقيقة القضائية[1].

ثانياً: مبدأ شخصية المسؤولية الجزائية:

انطلاقاً من المبدأ الدستوري المنصوص عليه في المادة (٤٧) من الدستور «المسئولية الجنائية شخصية»، نصت المادة (٣) من قانون الإجراءات الجزائية على أن: «المسؤولية الجزائية شخصية فلا يجوز إحضار شخص للمساءلة الجزائية إلا عما ارتكبه هو من أفعال يعاقب عليها القانون».

ثالثاً: مبدأ عبء الإثبات، والمساواة في حق الإثبات:

القاعدة في التشريعات الجزائية أنه على النيابة باعتبارها سلطة الاتهام إثبات العناصر المكونة للجريمة، كما لها أن تقوم بجمع عناصر الإثبات التي هي في صالح المتهم، وتقديمها إلى القضاء باعتبارها نائبة عن المجتمع، إذ يهمها إثبات براءة البريء كما يهمها إدانة المدان، فالنيابة العامة ملزمة بإثبات كافة أركان الجريمة، أي الركن الشرعي، المادي والمعنوي، وهو إجراء تفرضه طبيعة الدعوى الجنائية، وخطورة النتائج التي تترتب عليها، والجزاءات الناشئة عن الحكم فيها[2].

وقد نصت على ذلك المادة (٣/٣٢١) من قانون الجزاءات بقولها: «يقع عبء إثبات أية واقعة على المدعي بقيامها إلا إذا نص القانون على خلاف ذلك». والمادة (٢١) التي نصت على أن: «النيابة العامة هي صاحبة الولاية في تحريك الدعوى الجزائية ورفعها ومباشرتها أمام المحاكم، ولا ترفع من غيرها إلا في الأحوال المبينة في القانون».

كما نصت المادة (٣٢٤) على أن: «يتساوى جميع أطراف القضية في الحقوق والواجبات بما فيهم المتهم وممثل الدفاع والمدعي المدني والمسؤول مدنياً ولهم الحق في تقديم الأدلة ومناقشتها وطلب فحصها عن طريق الخبراء بعد موافقة المحكمة».

أما فيما يخص إثبات سبب الإباحة أو مانع من موانع المسؤولية أو العقاب أو عذر من الأعذار المخففة فقد اختلف الفقه حول هذه المسألة إذ اتجه البعض إلى القول بوجوب إثبات الدفع ممن أثاره كون أن المتهم يكون عند دفعه للتهمة بوضع المدعي بالنسبة إليه؛ فيلزمه إثباتها في حين اتجه البعض الآخر على رأسهم الفقيهان «قارو وقيدال» إلى عكس ذلك على أساس أن النيابة هي المكلفة أصلاً بإثبات الجرائم بجميع

(١) بيراز جمال، مرج سابق،، ص ٣٤.
(٢) نفس المرجع، ص ٤٠.

ظروفها واحتمالاتها أما بونيه «BONNIER» فاقترح حلاً وسطاً وهو أن يكلف المدعى عليه بالإثبات دون أن تفرض عليه القواعد الدقيقة، ودون أن يطلب منه الدليل القاطع، وأنه في حال وجود سبب أو عذر وجب على القاضي الأخذ به، لأن الشك يفسر لمصلحته، وعلى النيابة أن تدلي بما يقوض هذا الدفع بالاستناد إلى الدعوى وظروفها.

وبناء على ما تقدم فإن سلطة الاتهام إذا لم تستطع إقامة الدليل القاطع على وقوع الجريمة ومسؤولية المتهم عنها، فإنه يتعين على المحكمة أن تقضي ببراءة هذا الأخير باعتبارها الأصل وباعتبار أن الحكم بالإدانة يجب أن يبنى على الجزم واليقين بالإدانة لا على الظن والاحتمال وهو ما يعبر عنه بقاعدة «الشك يفسر لصالح المتهم»[1].

رابعاً: مبدأ الاقتناع القضائي:

يقصد بحرية القاضي في تكوين اقتناعه أن تكون له كامل الحرية في أن يستمد اقتناعه من أي دليل يطمئن إليه من الأدلة التي تقدم في الدعوى دون أن يتقيد في تكوين اقتناعه بدليل معين إلا إذا نص القانون على خلاف ذلك[2].

فالقاعدة في الإثبات الجنائي أنه يجوز إثبات الجرائم بكافة الطرق الجائزة قانوناً التي نصت عليها المادة (٢/٣٢١) إجراءات جزائية بقولها: «تقدير الأدلة يكون وفقا لاقتناع المحكمة في ضوء مبدأ تكامل الأدلة فلا يتمتع دليل بقوة مسبقة في الإثبات».

خامساً: مبدأ حرية الإثبات:

يحكم الإثبات الجزائي مبدأ حرية الإثبات الذي لا يقيد أدلة معينة لإثبات الجرائم حتى وإن كان هذا الدليل من صنع أهل الخبرة- الدليل العلمي- وهذا المبدأ أخذ قانون الإجراءات الجزائية في المادة (٣٢٢) إجراءات جزائية بقولها: «لا يجوز إثبات أي واقعة ترتب مسؤولية جزائية على أي شخص إلا عن طريق الأدلة الجائزة قانوناً وبالإجراءات المقررة قانونا».

فللقاضي الجزائي سواء بناء على طلبات الأطراف أو بموجب مقتضيات وظيفته أن يأمر باتخاذ الإجراء الذي يراه مناسباً وضرورياً للفصل في الدعوى، كما أنه يتعين على القاضي أن يتحقق بنفسه من عدم وجود أدلة براءة ظاهرة، ولو لم يدفع المتهم بها، فالقاضي يحكم من تلقاء نفسه بالبراءة إذا تبين له أن المتهم كان في حالة دفاع شرعي أو

(١) بيراز جمال، مرج سابق، ص ٤١.
(٢) نفس المرجع، ص ٤١.

توافر سبب من الأسباب التي تحول دون الإدانة[١].

الفرع الثالث

خصائص التحقيق الرقمي

تعد مرحلة التحقيق؛ مرحلة هامة في سبيل البحث والتحري عن الجرائم، وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة الإلكترونية، لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوة برمتها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبقى متاحاً بعد مرور وقت قصير على ارتكابها والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم، ففي كثير من الجرائم المعلوماتية لم يترك الجاني وراءه سوى ذلك التعبير الذي يعتري وجوه القائمين على تعقبه والممزوج بالإعجاب والإحباط معا[٢].

وفيما يلي سنبين أهم الخصائص التي يمتاز بها التحقيق الرقمي، والخصائص الفنية للمحقق:

أولاً: خصائص التحقيق الرقمي:

التحقيق الجنائي عموماً هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة وراسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة، وهذه القواعد إما قانونية وإما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع والامتثال، أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته[٣]، ذلك أن الفكر البشري المتعلق بالجرم الإلكتروني يجب أن يقابله فكر بشري من قبل المحقق الجنائي، وبالتالي فإن أسلوب التحقيق وفكر المحقق الجنائي يجب أن يكون متغيراً أو متطوراً أيضاً، وذلك كنتيجة طبيعية لمواجهة المجرم الإلكتروني.

وبالتالي فإن من أهم خصائص التحقيق الرقمي أنه يتطلب أسلوباً فنياً خاصاً يتم تنفيذه من خلال إجراءات يقوم بها المحقق وتؤدي إلى اكتشاف الجريمة ومعرفة

(١) الشواربي عبد الحميد، الإثبات الجنائي في ضوء الشريعة والفقه، النظرية والتطبيق، نشأة المعارف، الإسكندرية، طبعة ١٩٩٦م، ص ١٥. أشار إليه في الهامش: بيراز جمال، مرج سابق،، ص ٤٦.

(٢) طارق عبد الرؤوف، محمد. (٢٠١١). جريمة الاحتيال عبر الإنترنت الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، الطبعة الأولى، ص ٢٣٠.

(٣) خالد ممدوح إبراهيم، خالد. (٢٠٠٩). فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، ص ٥٦.

مرتكبيها تمهيداً لتقديمهم للمحاكمة، وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمضاهاة البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام المعلوماتي.

وتتمثل هذه الإجراءات في وضع خطة عمل التحقيق تتضمن الإجراءات الفنية التي يجب مراعاتها قبل البدء في التحقيق وأثناء السير فيه، وتشكيل فريق التحقيق الفني، وغيرها سنبينها في المبحث الثاني من هذا البحث.

ثانياً: الخصائص الفنية للمحقق.

تلعب الأجهزة الفنية دوراً أساسياً في صيانة أمن المجتمع وذلك إما بالقيام بدور وقائي يهدف إلى منع ارتكاب الجرائم والحيلولة دون وقوعها وتقليل فرص اقترافها، وإما القيام بدور قضائي في ضبط الجرائم ومرتكبيها بعد حدوثها.

ولقد أضاف ظهور الجرائم المعلوماتية النابعة من التطور الإلكتروني أعباء جديدة على أجهزة التحقيق لما يتطلب التصدي لهذه الجرائم من قدرات فيه لم يألفها رجال الضبطية القضائية ولم يتعودوا عليها، ما يستلزم ضرورة توفير المهارات المطلوبة في هذا المجال.

والمشكلة الأساسية التي تواجه المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه في مجال الحاسب الآلي، حيث قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دوافع الجريمة وجمع الأدلة التقديم المتهم للمحاكة، وفي كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول الجريمة الإلكترونية، ولكن من الناحية يتضح فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى، بينما المحققون ذوو الخلفية القانونية قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم[1].

وإذا كانت مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق، إلا أنه يلزمه عند مباشرته التحقيق في الجريمة الإلكترونية معرفة العديد من الجوانب الفنية؛ ليقوم بعمله على أحسن وجه، منها: معرفة الجوانب الفنية والتقنية لأجهزة الأجهزة

(١) نعيم سعيداني نعيم. (٢٠١٣). آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر – باتنة، الجزائر، ص ١١٥.

الحاسوب الإنترنت والتي تتعلق بالجريمة المرتكبة ذلك أن افتقار ضابط الشرطة القضائية التأهيل الكافي في الميدان التقني قد يؤدي إلى إتلاف وتدمير الدليل، على اعتبار أن جهله بأساليب ارتكاب الجريمة المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية وتدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن بها البيانات، وبالتالية فإن الكشف عن هذه الجرائم يقتضي أن تكون الأجهزة المعنية على دراية كافية بأساسيات التعامل مع هذه الجرائم وكيفية تقصيها وضبطها وصولاً إلى مرتكبيها[1].

المطلب الثاني

نطاق التحقيق الرقمي ومتطلبات تطبيقه

لا يقتصر نطاق التحقيق الرقمي على الجرائم الإلكترونية وأدلتها فحسب، بل يشمل أيضاً أدلة الإثبات الرقمية التي تثبت الوقائع الإجرامية لإحدى الجرائم التقليدية، كجريمة السرقة مثلاً التي يتم إثباتها بواسطة أدلة إلكترونية (بصمات- تصوير- تسجيل- رصد وتتبع موقع الفاعل). أي أن هناك نوعين رئيسين لأدلة الإثبات، النوع الأول: الأدلة التقليدية كشهادة الشهود والخبرة والأدلة المادية وغيرها؛ والنوع الثاني: الأدلة غير التقليدية وهي الأدلة الرقمية، وكل منهما يختلف عن الآخر في سلامته ودرجة مقبوليته[2].

وسنتطرق في هذا المطلب إلى بيان نطاق التحقيق الرقمي في أدلة الإثبات الرقمية التي تثبت واقعة إجرامية لإحدى الجرائم التقليدية في الفرع الأول، وبيان نطاق التحقيق الرقمي في الجرائم الإلكترونية وأدلتها في الفرع الثاني، وأثر خصوصية الجريمة الإلكترونية على دليل الإثبات الإلكتروني الفرع الثالث، وذلك على النحو التالي:

الفرع الأول

التحقيق الرقمي في الأدلة الرقمية للجرائم التقليدية

نظرا لما أثارته الثورة المعلوماتية على نوعيه الجرائم التي صاحبتها وظهور أنماط مستحدثة من الجرائم عرفت بالجرائم المعلوماتية، وفي المقابل أيضاً أثرت على إثباتها

(١) بن قدوم سوهيل؛ وبسام لديدة، مرجع سابق، ص ٢١.

(٢) عبد الباقي، مصطفى. (٢٠١٨م). التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين «دراسة مقارنة»، مجلة دراسات، علوم الشريعة والقانون، عمادة البحث العلمي وضمان الجودة، الجامعة الأردنية، المجلّد (٤٥) عدد (٤)، ملحق (٢). ص ٢٩٢.

فأصبحت الأدلة التقليدية التي جاءت بها نصوص (قانون الإثبات) وقانون الإجراءات الجزائية غير قادرة على إثبات هذا النوع من الجرائم الذي يحتاج إلى طرق تقنية تتناسب مع طبيعته، بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة، وهو ما يطلق عليه بالدليل الرقمي أو الدليل الإلكتروني[١].

وفي هذا الفرع سنتناول: تعريف دليل الإثبات الرقمي (أولاً)، طبيعة دليل الإثبات الرقمي (ثانياً)، خصائص دليل الإثبات الرقمي (ثالثاً)، نماذج من أدلة الإثبات الرقمية في الجرائم التقليدية (رابعاً)، وذلك على النحو التالي:

أولاً: تعريف دليل الإثبات الرقمي:

يعرف الدليل بصفة عامة بأنه «الوسيلة التي يستعين بها القاضي في تكوين قناعته القضائية للوصول إلى الحقيقة»[٢].

أما الدليل الرقمي فيعرف بأنه «الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطسية أو كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، لتظهر في شكل صور أو تسجيلات صوتية أو مرئية»[٣]. وعرف أيضاً أنه: «الدليل الذي يجد أساساً في العالم الافتراضي ويقود إلى الجريمة»[٤].

كما عرف بأنه: «ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية أجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، تقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور وأشكال وأصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها»[٥].

---

(١) بن قدوم سوهيل؛ وبسام لديدة. (٢٠١٧/٢٠١٨). الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة-بجاية. الجزائر، ص ٥.

(٢) بن قارة، عائشة. (٢٠١٠). حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دون الطبعة، دار الجامعة الجديدة، الإسكندرية، مصر. ص ٥١.

(٣) سوزان نوري علي محمد. (٢٠١٥). الإثبات في جرائم الأنترنت في القانون العراقي المقارن، رسالة دكتوراه حقوق، جامعة المنصورة، ص ٤٤.

(٤) عمر محمد بن يونس. (٢٠٠٦). مذكرات الإثبات الجنائي عبر الانترنت، ندوة الدليل الرقمي بمقر جامعة الدول العربية، مصر، ص ٥.

(٥) محمد فرغلي، عبدالناصر؛ عبيد سيف سعيد السمساري، محمد. (٢٠٠٧). الإثبات الجنائي بالأدلة الرقمية

ثانياً: طبيعة دليل الإثبات الرقمي:

تثير مسألة الطبيعة التي عليها الدليل الرقمي ثلاث مسائل في النقاش، الأولى: الدليل الرقمي والواقعة الافتراضية. والثانية: الدليل الرقمي والواقعة المادية. والثالثة: الدليل الرقمي والواقعة المزدوجة. وكل هذه المسائل تثير جدلاً واسعاً في النقاش، حيث يصعب البحث في طبيعة الدليل الرقمي وأداة التواصل بين سلطات الضبط القضائي والتحقيق وأيضاً المحاكمة وبين الواقعة المعدة في القانون جريمة، وعليه يجب أن تكون العلاقة واضحة في القانون بين الدليل الرقمي وطبيعة الواقعة فيما إذا كانت افتراضية أو مادية أو مزدوجة[1].

والذي يهمنا في هذا الفرع هو الأدلة الرقمية للواقعة المادية أو الجريمة التقليدية، وكذا دليل الإثبات الرقمي في الواقعة المزدوجة (مادية وافتراضية)، ونبين ذلك في الآتي:

١. دليل الإثبات الرقمي في الواقعة المادية أو التقليدية:

يحدث في بعض الأحيان بأن تتم واقعة مادية (جريمة تقليدية) وتتم الاستعانة بالحوسبة والرقمية من أجل الكشف عنها، وفي هذه الحالة فإن الواقعة تسهم بشكل فعال في كشف الواقعة المادية بحيث يصبح الدليل الرقمي دليلاً له وجود في كشف الواقعة المادية.

فمثل هذه القضايا تعتمد على علاقات التخزين الرقمي في الواقع، ولكي يتم الكشف عن الدليل الرقمي ويقدم للقضاء، يجب الاعتماد على ضرورة القيام باتخاذ إجراءات ملائمة ومشروعة، وإلا فقد الدليل مفهومه في القانون وأصبح واقعة مادية صرفة لا تصلح للتقاضي، كما هو الشأن في اتخاذ الإجراءات الملائمة لاستصدار إذن التفتيش أو القيام بأخذ موافقة المالك وحائز الجهاز أو الشبكة كتابة وتصديق شهود على ذلك، وبهذا يصح القول بأنه كلما كانت هناك واقعة مادية غير مشروعة، فإنه من الممكن الاستعانة بإجراءات الكشف عن الدليل الرقمي للتدليل على حدوث الواقعة، ويجب في مثل هذه الحالات التدقيق في الإجراءات (مثلاً: يجب أن يتضمن إذن التفتيش تخصيص بند فيه يسمح بتفتيش مخصص في الحواسيب والشبكات والأقراص ...إلخ)، والتخصيص

من الناحيتين القانونية والفنية «دراسة تطبيقية مقارنة»، المؤتمر العربي للعلوم الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، ص ١٣.

(١) خلف الحمداني، ميسون؛ محمد كاظم الموسوي علي. (٢٠١٦). الدليل الرقمي وعلاقته بالمساس بالحق في الخصومة المعلوماتي أثناء إثبات الجريمة، جمهورية العراق، وزارة التعليم العالي والبحث العلمي، جامعة النهرين، كلية الحقوق، ص ٢٠.

يعني تفصيل هذا البند بدقة متناهية حتى لا يكون إجراء التفتيش باطلاً، بالتالي يتعرض الدليل الرقمي ذات الدفع بالبطلان وهنا تظهر أهمية التمييز بين إجراءات الكشف عن الدليل الرقمي في الواقعة المادية، حيث تبدأ إجراءات الكشف عن الدليل من إجراء استصدار إذن التفتيش مع ملاحظة فرق كبير بين تضمن إذن التفتيش بنداً يسمح بتفتيش الحواسيب والبحث فيها وبين التحفظ على المواد الحاسوبية والرقمية لكي يتم نقلها إلى الحجرة المختصة بإجراء التفتيش واستخراج الدليل الرقمي، والتحفظ عليه تمهيداً لتقديمه وعرضه على الجهات القضائية الفاصلة في النزاع، فمثل هذه المسألة محل دفع أمام القضاء إذ لم يتم مراعاتها، والدفع فيها من الدفوع الموضوعية التي يجب على القضاء التعرض لها، وإلا فقد الحكم تسببيه الصحيح وأصبح عرضه للنقض[1].

٢. دليل الإثبات الرقمي في الواقعة المزدوجة (مادية وافتراضية):

الواقعة المزدوجة التي يكشف عنها الدليل الرقمي في مدى قدرة الاستعانة بالحواسيب للارتكاب جرائم مادية ممزوجة بطابع رقمي، وهنا سوف يكون الدليل شراكة بين المادية والرقمية.

وفي كل الأحوال ليس من السهولة بمكان الحصول على تصنيف متكامل لموضوع العلاقة بين الدليل الرقمي والواقعة المزدوجة، وإنما يتوقف الأمر على مراعاة الطابع المصلحي فيها من حيث مكافحة الإجرام والتبليغ عن الجرائم ومرتكبيها[2].

ثالثاً: خصائص دليل الإثبات الرقمي:

باعتبار أن الدليل الرقمي وليد البيئة الإلكترونية الحديثة في العالم الافتراضي وارتباطه بالجريمة المعلوماتية واختلافها عن الجرائم التقليدية، ولهذا يتميز بجملة من الخصائص تميزه عن الأدلة الأخرى ومنها:

١. الدليل الرقمي دليل علمي وتقني:

الدليل الرقمي هو الواقعة التي تنبئ عن وقوع جريمة أو عمل غير مشروع وهي واقعة مبناها من حيث إن مبنى العالم الرقمي أو الافتراضي هو مبنى علمي يشيده العلماء والتقنيون، وتفيد هذه الخاصية أنه لا يمكن الحصول على الدليل الرقمي أو الاطلاع على فحواه سواء باستخدام الأساليب العلمية وتفيد هذه الخاصية أيضاً حين قيام رجال

(١) الحمداني، ميسون؛ والموسوي، علي. مرجع سابق، ص ٢٠.
(٢) نفس المرجع السابق، ص ٢٠.

الضبط القضائي والاستدلال أو سلطات التحقيق أو المحاكمة بالتعامل مع الدليل الرقمي سعياً وراء إثبات الحقيقة، حيث يجب أن تبنى عملية البحث هنا على أسس علمية فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة[١].

كذلك ما يمكن استخلاصه من هذه الخاصية فيما يخص موضوع حفظه، وجوب حفظ هذا الدليل على أسس عملية، ومنه ضرورة السعي وراء تحديث أسلوب تحرير المحاضر في هذا الشأن، فتحرير محضر يتناول دليلاً علمياً مختلف عن المحضر المتناول اعتراف شخص مثلاً، فالمحضر بالدليل العلمي يعني وجوب توافر طريقة عملية متوافقة مع ظاهرة الدليل العلمي أثناء تحريره، فمن غير المنطقي أن يتخذ صورة المحضر التقليدي[٢].

ومنه نقول إن هذه الخاصية التي يتميز بها الدليل الرقمي ويترتب عنها عدة نتائج مهمة أهمها تحديد طرق وكيفيات التعامل مع هذا الدليل بما يتماشى مع هذه الخاصية، وكذا بما يتماشى مع التطور التكنولوجي الراهن حتى تكون لهذا الدليل حجية أكبر.

وهناك أيضاً خاصية التقنية التي يتمتع بها الدليل الإلكتروني، وجاءت بناء على ميزته العلمية، وهذا على اعتبار أن العلم يبنى على أساس التقنية كما أنه لا يمكن أن تكون هذه التقنية بدون أسس علمية، مفاد هذه الخاصية أنه من الضروري أن يكون التعامل مع الدليل الإلكتروني بصفة خاصة، وهذا راجع إلى أن الدليل الإلكتروني ليس كالدليل العادي، فيما تتجه إليه التقنية هو نبضات إلكترونية، تتشكل قيمتها في إمكانية التعامل مع القطع الصلبة التي تشكل الحاسوب في أي شكل يكون عليه[٣].

كما تظهر أهمية تقنية الدليل الإلكتروني، من خلال الدور الذي تقوم به هذه التقنية في كشف الدليل الإلكتروني، وهذا ما يقتضي الاتهام بهذا الأمر من ناحيتين، الأولى: هي ضرورة الاهتمام بتقنية البرامج التي تتعامل مع الدليل الإلكتروني، وهذا من ناحية اكتسابه، أو التحفظ عليه، وتحليله، وتقديمه، والثانية، هي أن هذه البرامج في حد ذاتها يجب أن تكون مقبولة من مستخدميها في الحصول على هذا الدليل، فإطلاق صفة إلكتروني على دليل ما تعني بالضرورة وجود توافق بينه وبين بيئته، فلا وجود لدليل

(١) عزت، فتحي محمد أنور. (٢٠١٠). الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجاري، دار الفكر والقانون للنشر والتوزيع، الطبعة الأولى، مصر، ص ٦٤٨.

(٢) هلال أمنة. (٢٠١٤/٢٠١٥). الإثبات الجنائي بالدليل الالكتروني. مذكرة محكمة من مقتضيات نيل شهادة الماستر في الحقوق تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر. ص ١١.

(٣) عزت، فتحي محمد أنور، مرجع سابق، ص ٦٤٩.

إلكتروني خارج بيئته التقنية والإلكترونية[١].

٢. الدليل الرقمي دليل يصعب التخلص منه:

حيث تعتبر هذه الخاصية أو الميزة من أهم خصائص الدليل الإلكتروني، ويتمتع بها عن باقي الأدلة التقليدية، فنجد أنه يمكن التخلص بكل سهولة من الأوراق والأشرطة المسجلة إذا كانت تحتوي على اعتراف شخص بارتكابه للجريمة، وذلك بحرقها أو تمزيقها مثلاً، كما أنه من المستطاع التخلص من بصمات الأصابع بمسحها من موضعها، كما أن هناك بعض الدول التي يتم فيها التخلص من الشهود عن طريق قتلهم، أو تهديدهم لعدم الإدلاء بشهادتهم، هذا فيما يتعلق بالأدلة التقليدية.

وبالنسبة للأدلة الإلكترونية فإن الأمر مختلف، حيث أنه يمكن استرجاعها بعد محوها وإصلاحها بعد تلفها أو بعد إخفائها مما يؤدي لصعوبة التخلص منها، وهذا يعود إلى أن هناك العديد من البرامج الحاسوبية تتمثل وظيفتها في استعادة البيانات التي تم إلغاؤها، مثل (Recover lost data) سواء كان هذا الإلغاء عن طريق الأمر، أو إعادة تهيئته، أو تشكيل للقرص الصلب باستخدام الأمر، سواء كانت هذه البيانات في شكل صور أو رسومات أو كتابات أو غيرها، فكل هذا يشكل صعوبة إخفاء الجاني لجريمته، أو التخفي عن أعين العدالة أو غيرها، وهذا بشرط العلم بوقوع الجريمة من رجال البحث و تحقيق الجنائي[٢].

كما يعتبر نشاط الجاني في سبيل محو الدليل الذي يدينه دليلاً أيضاً، وهذا لأن فعله هذا أي محاولته لإخفاء الدليل يتم تسجيله في الكمبيوتر، ويمكن استخلاصه كدليل إدانة ضده، بمعنى أن الإلغاء أو الحذف للدليل الإلكتروني، هو في الحقيقة واقعة إخفاء له مادام أن القاعدة المشار إليها ثابتة[٣].

فهذه الخاصية في حقيقة الأمر تعد حافزاً لمواصلة البحث في الجريمة الإلكترونية، ومنه تعد دافعاً لاتخاذ الحيطة. ومن هذه الخاصية تجدر الإشارة لأمر مهم، هو إمكانية استفادة مرتكب الجريمة من الضمانات الممنوحة له بمقتضى القانون، وبالتالي فإن خاصية صعوبة التخلص من الدليل الإلكتروني تقابلها مسألة أخرى هي أن هذا الدليل نتيجة لمرونته وضعفه، فإن يسهل إتلافه أو فقدانه، وبالنظر في هذه المسألة أي إمكانية

(١) عزت، فتحي محمد أنور، مرجع سابق، ص ٦٤٩.
(٢) انظر نفس المرجع، ص ٦٥٠.
(٣) انظر نفس المرجع، ص ٦٥١.

إتلاف الدليل الإلكتروني، هي في الواقع ليست حقيقة، وإنما القول بإمكانية إتلاف معناه أنه يوجد قصور في القدرات التكنولوجية لدى مؤسسات العدالة، مما ينبغي وجود العمل على التطور المستمر لنظم العدالة، بالإضافة لتطور قدرات القائمين على مهامها وأعمالها[١].

٣. الدليل الرقمي دليل متنوع ومتطور وقابل للفسخ:

على الرغم من أن الدليل الإلكتروني في أساسه يعتبر متحداً في تكوينه، أي في مجال الحوسبة الرقمية، إلا أنه يتخذ أشكالاً مختلفة، فمصطلح الدليل الإلكتروني يشمل كافة أنواع البيانات الإلكترونية الممكن تداولها رقمياً، ويكون بينها وبين الجريمة رابط من نوع ما، بالإضافة إلى أنها تكون متصلة بالضحية مما يتحقق معه وجود رابطة بينها وبين الجاني[٢].

ففيما يخص التنوع المتعلق بالدليل الإلكتروني، نجد أنه يظهر بطريقة علنية في هيئات مختلفة الأشكال، كأن يكون بيانات غير مقروءة، كما هو الأمر في حالة المراقبة عبر الشبكات أو الخوادم، وقد يكون الدليل الإلكتروني مفهوماً للأشخاص كما كان وثيقة معدة بنظام المعالجة الآلية للكلمات بأي نظام، كما يمكن أن يكون صورة ثابتة أو متحركة، أو معدة بنظام التسجيل السمعي المرئي، أو أن تكون مخزنة في نظام البريد الإلكتروني، وهذه الخاصية تستوجب مواكبة التطور في عالم التكنولوجيات[٣].

أيضاً الدليل الإلكتروني يعتبر دليلاً قابلاً للفسخ، وهذا مرده لإمكانية استخراج نسخ من الأدلة الجنائية الإلكترونية مطابقة للأصل، ولها نفس القيمة العلمية، وهذه الخاصية لا تتوافر في باقي الأدلة الجنائية التقليدية، وهذا يأتي معه بالضرورة وجود ضمانة شديدة الفعالية للحفاظ على هذا النوع من الأدلة ضد الفقد والتلف والتغيير، عن طريق النسخ المطابق للأصل من الدليل[٤].

كما نجد أن الدليل الإلكتروني يمتاز بالسعة التخزينية العالية، فآلة الفيديو الرقمية يمكنها تخزين مئات الصور، ودسك صغير يمكنه تخزين مكتبة صغيرة، بالإضافة إلى أن الدليل الإلكتروني له خاصية رصد معلومات عن الجاني وتحليلها في ذات الوقت،

(١) هلال أمنة، مرجع سابق، ص ١٣.
(٢) عزت، فتحي محمد أنور، مرجع سابق، ص ٦٥١ – ٦٥٢.
(٣) بن قدوم سوهيل؛ وبسام لديدة، مرجع سابق، ص ١٣.
(٤) ممدوح عبد المطلب. (٢٠٠٦). البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ص ٨٠.

ومن خلال إمكانية تسجيله لتحركات الفرد، وتسجيل عاداته وسلوكياته وبعض الأمور الشخصية، ولذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي ومنه نقول إن الدليل الإلكتروني يتمتع بمجموعة من الخصائص والمميزات التي جعلته يتميز عن باقي الأدلة الجنائية التقليدية، ويفرض نفسه في مجال الإثبات الجنائي[١].

وبالنظر إلى كل هذه الخصائص نجد أنه يجب العمل على تطوير كل ما يتعلق بهذا الدليل، باعتبار أنه دليل علمي، عن طريق المواكبة الحديثة، وأيضاً فيما يخص إجراءات جمعه ودراسته وتحليليه، ليتماشى مع طبيعة الدليل الإلكتروني، وأيضاً أنه نوع من الأدلة له مميزات خاصة تستوجب التعامل معه بطريقة خاصة[٢].

رابعاً: نماذج من أدلة الإثبات الرقمية في الجرائم التقليدية:

تضمن قانون الجرائم والعقوبات رقم (١٢) لسنة ١٩٩٤م بعض أحكام الجرائم التقليدية التي يكون محلها ودليل إثباتها دليل إلكتروني، وذلك في الباب العاشر (الجرائم الواقعة على الأشخاص والأسرة)، الفصل الثاني (الاعتداء على الحرية الشخصية)، ضمن المواد (٢٥٥ - ٢٥٧)، نوردها في الآتي:

١. جريمة انتهاك حرمة المراسلات:

نصت على ذلك المادة (٢٥٥) من قانون العقوبات، بقولها: يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة من فتح بغير حق خطاباً مرسلاً إلى الغير أو احتجز رسالة برقية أو هاتفية ويعاقب بالعقوبة ذاتها من اختلس أو أتلف إحدى هذه المراسلات أو أفضى بمحتوياتها إلى الغير ولو كانت الرسالة قد أرسلت مفتوحة أو فتحت خطأ أو مصادفة ويقضي بالحبس مدة لا تزيد على سنتين أو بالغرامة إذا ارتكب الجريمة موظف عام إخلالاً بواجبات وظيفته.

٤. الاعتداء على حرمة الحياة الخاصة:

نصت على ذلك المادة (٢٥٦) بقولها: يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة كل من اعتدى على حرمة الحياة الخاصة وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه:

أ. استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات

(١) بن قارة مصطفى عائشة، مرجع سابق، ص ٦٤.

(٢) بن قدوم سوهيل؛ وبسام لديدة، مرجع سابق، ١٤.

جرت في مكان خاص أو عن طريق الهاتف.

ب. التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص.

فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع فإن رضاء هؤلاء يكون مفترضاً.

ويعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بالغرامة الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته.

ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة كما يحكم بمحو التسجيلات المتحصلة عنها أو إعدامها.

١. التهديد بإذاعة الأسرار الخاصة:

نصت على ذلك المادة (٢٥٧) بقولها: «يعاقب بالحبس مدة لا تزيد على سنتين أو بالغرامة كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلاً أو مستنداً متحصلاً عليه بإحدى الطرق المبينة بالمادة السابقة أو كان ذلك بغير رضاء صاحب الشأن ويعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من هدد بإفشاء أمر من الأمور التي تم الحصول عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه ويعاقب بالحبس مدة لا تزيد على خمس سنوات الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل منها كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها».

الفرع الثاني

التحقيق الرقمي في الجرائم الإلكترونية وأدلتها

سنتناول في هذا الفرع: تعريف الجريمة الإلكترونية وخصائصها، وأثر خصوصية الجريمة الإلكترونية على دليل الإثبات الإلكتروني، وذلك على النحو التالي:

أولاً: تعريف الجريمة الإلكترونية:

الجريمة الإلكترونية كظاهرة لا توجد تسمية موحدة للدلالة على هذه الظاهرة الإجرامية «الجريمة، فهناك تباين في التسميات التي أطلقت عليها، وقد يكون مراد هذا الأمر إلى نشأة وتاريخ وتطور تكنولوجيا المعلومات، وكذا اختلاف وجهات النظر بين

المختصين في مجال الإعلام، وأيضاً بين رجال القانون وعلماء النفس والاجتماع، ومن بين تسميات هذه الظاهرة جرائم الكمبيوتر والإنترنت، جرائم التقنية العالية، الجريمة الإلكترونية، الاحتمال المعلوماتية (cyber crime) جرائم أصحاب الياقات البيضاء، وغيرها من التسميات»[١].

حيث يرى جانب من الفقه إلى أن تعريف الجريمة الإلكترونية يجب أن يكون من الناحية الفنية والتقنية، فالتعريف الفني لها هو: «نشاط إجرامي تستخدم فيه تقنية الحاسوب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود»[٢].

أما من الناحية القانونية، فقد عرفها الفقيه الألماني تدمان أنها: «كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب»، وعرفها R.Tott،A. Hard Castl بأنها: «تلك الجرائم التي يكون قد حدث في مراحل ارتكابها بعض عمليات فعلية داخل الحاسوب».

وهناك أيضاً تعريفات تسند إلى السمات الشخصية للجاني، ومن هذه التعريفات: «الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسوب، ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها على الجريمة»[٣].

ونستخلص مما سبق أن هناك غياباً مفهوماً عاماً متفقاً عليه بين الدول حول نموذج النشاط المكون للجريمة المتعلقة بالنظام المعلوماتي والإنترنت، فليس هناك اتفاق حول التعريف القانوني للنشاط الإجرامي المتعلق بهذا النوع من الإجرام[٤].

ثانياً: خصائص الجريمة الإلكترونية:

إن ارتباط الجرائم الإلكترونية بجهاز الحاسوب وشبكة الإنترنت أضفى عليها مجموعة من الخصائص، ومن هذه الخصائص المميزة عن باقي الجرائم التقليدية فهي كالتالي.

(١) الطائي جعفر حسن جاسم. (٢٠١٠). جرائم تكنولوجينا المعلومات، ط ١، دار البداية، الأردن، ص ١٠٧.
(٢) حجازي عبد الفتاح بيومي. (٢٠٠٩). الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت «دراسة معمقة في جرائم الحاسب الآلي والإنترنت»، بهجت للطباعة والتجليد، مصر، ص ١٠٠.
(٣) الملط أحمد خليفة. (٢٠٠٦). الجرائم المعلوماتية، ط ٢، دار الفكر الجامعي، مصر، ص ٨٤. أشار إليه: بن قدوم سوهيل؛ وبسام لديدة ص ١٨.
(٤) بن قدوم سوهيل؛ وبسام لديدة. (٢٠١٧/٢٠١٨). الدليل الرقمي في الإثبات الجنائي، مرجع سابق، ص ١٨.

١. ازدواجية محل الجريمة الإلكترونية:

باعتبار أن النظام المعلوماتي ليس من طبيعة واحدة فهو يتكون من عناصر مادية أخرى وأخرى غير مادية، فهذا الأمر يسمح بإمكانية أن يكون موضوع الجريمة ذا طبيعتين مختلفتين، إحداهما تتمثل في الجانب المادي والآخر غير مادي أي ظهور المحل الواحد بمظهرين أحدهما مادي والآخر غير مادي، وقد تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة معلوماتية، حتى أن المعلومات بطبيعتها غير المادية أو المادية يمكن أن تخضع لأكثر من نص قانوني، مما يولد مشكلة تعدد الأوصاف القانونية على نفس المحل[١].

٢. صعوبة اكتشاف الجريمة الإلكترونية وإثباتها:

فالجريمة الإلكترونية تتميز بأنها لا تترك آثاراً مادية عند القيام بها، وبالتالي من الصعب اكتشافها، فكل ما يحدث فيها هو مجرد تحرك وانتقال لذبذبات ونبضات إلكترونية من خلال استخدام النظم المعلوماتية وشبكات الاتصال[٢]. وتعود خاصية صعوبة اكتشاف الجريمة الإلكترونية وإثباتها، إلى الأسباب التالية:

أ- الدليل الرقمي غير مرئي: فمن مميزات الدليل الرقمي أنه دليل غير مرئي، وهو عبارة عن نبضات مغناطيسية أي إلكترونية تتكون من سلسلة طويلة من الأرقام أي أنه ذو طبيعة ثنائية لا تفصح عن الشخصية المعنوية، ودائما ما يكون الدليل في الجريمة التقليدية ذا طبيعة مادية مرئية بحيث يمكن للمختصين في عملية التحقيق بمعاينة مسرح الجريمة، وضبط أي دليل يفيد الكشف عن الجريمة، ولكن الجريمة الإلكترونية تقع في بيئة تختلف عن البيئة التقليدية، وذلك لأن الأدلة فيها عبارة عن نبضات مغناطيسية تشكل بيانات رقمية في العالم الافتراضي، ومنه فعدم رؤية الدليل الرقمي يشكل العديد من المعوقات خلال جمعة وتحليلية مما يستوجب توفر لدى المحققين الفنيين دراية كافية في التعامل مع هذا النوع من الأدلة[٣].

ب- سهولة محو وتعديل الدليل الرقمي: بعد محو وتعديل الدليل الرقمي من أهم

(١) بن قدوم سوهيل؛ وبسام لديدة، مرجع سابق، ص ٢٠.

(٢) بن فردية محمد. (٢٠١٥). الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم الجنائية، كلية الحقوق، الجزائري، ص ٢١٤. وبن قدوم سوهيل؛ وبسام لديدة، مرجع سابق، ص ٢٠.

(٣) حجازي عبد الفتاح بيومي، مرجع سابق، ص ٧٩.

الصعوبات التي تواجهها عملية الحصول على الدليل، وذلك يعود لسهولة هذه العملية من محو الأدلة في فترة وجيزة، فمرتكبو الجرائم الإلكترونية يتميزون بالذكاء في العمل الذي يقومون به، وذلك أن الجاني يسعى دائماً إلى محو وتدمير الدليل الذي يؤدي إلى إدانته[١]. بحيث يستطيع الجاني تغيير بيانات تؤدي إلى إدانة أو تبرئة شخص، ولذلك فإن القاضي يجد صعوبة في إدانة شخص دون أن يتأكد من أنه هو المذنب، مما أدى بالفقهاء إلى القول بضرورة تدخل المشرع في حالة ارتكاب الجرائم الإلكترونية بالسماح لرجال السلطات المختصة كاستثناء بضبط الأدلة عند حدوث الجريمة دون الحصول على إذن مسبق من وكيل الجمهورية، وذلك تفادياً للدفوعات والتأكد من أن الدليل لم يتغير[٢].

ج- صعوبة الحصول على الدليل الرقمي: كثيراً ما يلجأ مرتكبو الجريمة الإلكترونية إلى أهم الوسائل لعرقلة جمع أدلة الإدانة، ومن بين أهم هذه الوسائل نجد مسألة استخدام تقنية التشفير. أو لاستخدامهم لمسألة التدابير الأمنية لمنع مشكلة التفتيش والاطلاع على الأدلة أو ضبطها، وذلك لاستخدام لكلمة السر أو لجوئهم إلى إخفاء هويتهم، وخاصة عند استخدامهم لشبكة الإنترنت وذلك باستعمالهم للعديد من البرامج والتطبيقات التي تعمل على طمس هويته في شبكة الإنترنت[٣].

د- الصعوبات المتعلقة بالخبرة: التطور الحديث وما صاحب ذلك، جعل الواقع الإلكتروني يحتوي على مجرمين محترفين، وقد تكون خبراتهم في كثير من الدول تفوق خبرة الجهات الرسمية والتي يوكل لهم مواجهة هذا النوع من الجرائم، مما أدى إلى نقص الخبرة لدى هذه الجهات وهي من معيقات اكتشاف الأدلة، وذلك نظراً لافتقاد أو النقص الفاحش للخبراء سواءً أمام النيابة أو القضاء، وذلك نظراً للقدرات الكبيرة التي يتميز بها المجرمون تفوق القدرات التي تتمتع بها الجهات القضائية[٤].

---

(١) هشام فريد رستم. (٢٠٠٠). أصول التحقيق الجنائي الفني في بحوث مؤتمر القانون والكمبيوتر والإنترنت، المجلد الثاني، ط الثالثة، الامارات العربية المتحدة، ص ٢٠.

(٢) حسن محمد إبراهيم. (٢٠١١). الحماية الجنائية لحق المؤلف عبر الإنترنت، رسالة الدكتوراه في الحقوق، كلية الحقوق، جامعة عين شمس، مصر. ص ١٤٤.

(٣) حجازي عبد الفتاح بيومي، مرجع سابق، ص ٨٩.

(٤) بن قدوم سوهيل؛ وبسام لديدة، مرجع سابق، ص ٢٢.

٣. الجريمة الإلكترونية جريمة عابرة للحدود:

فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية فالشبكات تخترق الزمان والمكان، خاصة بعد ظهور شبكات المعلومات الدولية أي الإنترنت، حيث أن القائم على النظام المعلوماتي في أي دولة يمكنه أن يحول مبلغاً من المال لأي مكان في العالم مضيفاً له صفر أو بعض الأصفار لحسابه الخاص، بل يستطيع أي شخص أن يعرف كلمة السر لأي شبكة في العالم ويتصل بها ويغير ما بها من معلومات[١].

الفرع الثالث

أثر خصوصية الجريمة الإلكترونية على دليل الإثبات الجنائي

تتميز الجريمة الإلكترونية بطبيعة خاصة جعلتها تثير العديد من المشكلات، و هذا الأمر صعب إلى درجة كبيرة إثبات الجريمة الإلكترونية، و ترجع هذه الصعوبة إلى العديد من الأمور منها أن الجريمة الإلكترونية تتم في بيئة غير تقليدية فهي تقع خارج إطار الواقع المادي الملموس وأركانها تقوم في بيئة الحاسوب والإنترنت، وهذا الأمر يجعل إمكانية محو وطمس الدليل سهلة، ومن ثم يكون من الصعب ملاحقة المجرم أو كشف شخصيته، لذلك يرى جانب من الفقه ضرورة تدخل المشرع بإضافة حالة ارتكاب الجريمة الإلكترونية كظرف استثناء يسمح لرجال السلطة العامة بالقيام بضبط الأدلة عند وقوع الجريمة، وبدون إذن مسبق من النيابة العامة، وهذا حماية للأدلة من المحو وتعديل من قبل الفاعل[٢].

وكما أن للمجني عليه دوراً في هذه الصعوبة بسبب دوره السلبي وعدم إبلاغه عن وقوع هذا النوع من الجرائم، فالكثير من الجهات التي تتعرض أنظمتها للانتهاك تعمد إلى عدم الكشف عنها تجنباً لعدم الإضرار بسمعتها وتكتفي بالإجراءات الإدارية، ويمكن القول إن الجريمة الإلكترونية تنشأ عنها عدة معوقات تعيق إثباتها في إطار الإثبات الجنائي، كصعوبة جمع أدلتها نظراً لسهولة محوها وتغييرها بعد ارتكاب الجريمة مباشرة، وأيضاً يترتب عليها صعوبة الوصول إلى الفاعل ومرتكب الجريمة، والعائق الكبير هو نقص الخبرة الفنية والتقنية خاصة في هذا النوع والصعب والمعقد من الجرائم ألا وهو الجريمة الإلكترونية[٣].

---

(١) انظر: الملط أحمد خلفي، مرجع سابق، ص ٩٤. وبن قدوم سوهيل؛ وبسام لديدة، مرجع سابق، ص ٢٣.

(٢) بن قارة مصطفى عائشة، مرجع سابق، ص ٤٦.

(٣) بن قدوم سوهيل؛ وبسام لديدة، مرجع سابق، ص ٢٣.

المبحث الثاني
آليات التحقيق الرقمي ومعوقاته

تمهيد:

بقدر ما حققته تكنولوجيا المعلومات من آثار إيجابية وإنجازات وتطورات في المجال الرقمي من خلال الاعتماد عليها في الكثير من قطاعات الحياة، فإنها في الوقت نفسه مهدت لظهور أنواع جديدة من الجرائم بالغة الخطورة، شكلت اعتداءات على الحياة الخاصة للأفراد وتسببت في خسائر كبيرة لاقتصاد الدولة ألا وهي الجرائم المعلوماتية بشتى أنواعها، ذلك أن المجرم اليوم وجد تقنية عالية وأساليب حديثة تساعده في ارتكاب الجرائم دون أن يترك أثراً للكشف عنها ومعرفة مصدرها، وكما يستطيع أيضاً أن يقترف جريمته ضد مجموعة من المجني عليهم في أي مكان يرغب فيه وفي نفس الوقت بعد أن تم الربط بين الحاسب الآلي والشبكة العالمية للإنترنت[1].

وفي هذا المبحث سنتناول أهم الأدوات والتقنيات المستخدمة في الإثبات الجنائي، والنظام الإجرائي لإثباتها وذلك في مطلبين على النحو التالي:

المطلب الأول
الأدوات والتقنيات المستخدمة في الإثبات الجنائي

أضحت الأدوات والتقنيات الإلكترونية غير قابلة للحصر نتيجة تعدد مجالات استخداماتها المختلفة، وهذا بلا شك ما يصعب حصرها أو حتى تصنيفها، لذلك سنقتصر في هذا المطلب على بيان بعض نماذج من الأدوات والتقنيات الرقمية المستخدمة في الإثبات الجنائي، بداية بالأدلة المتحصلة من الحاسب الآلي وشبكة الإنترنت في الفرع الأول، وأدوات وتقنيات الإثبات في المعاملات الإلكترونية في الفرع الثاني، والأدلة المتحصلة من أدوات وتقنيات ومواقع التواصل الاجتماعي في الفرع الثالث، وذلك على النحو التالي:

(١) معمش، زهية؛ غانم، نسيمة. (٢٠١٢/٢٠١٣). الإثبات الجنائي في الجرائم المعلوماتية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة – بجاية –، الجزائر، ص ١.

الفرع الأول

الأدلة المتحصلة من الحاسب الآلي وشبكة الإنترنت

يعتبر الحاسب الآلي وشبكة الإنترنت من أهم ما أنتجته الثورة المعلوماتية وما صاحبها من تطورات في شتي المجالات، ونظراً للأهمية الكبيرة لشبكة الإنترنت والخطورة الناتجة عن سوء استخدامها، وكذا نظراً لحاجة مجرم الإنترنت إلى جهاز حاسب آلي للدخول إلى شبكة الإنترنت لارتكاب الجريمة من خلاله.

وفيما يلي سنبين بشكل موجز ماهية كل من الحاسب الآلي وشبكة الإنترنت (أولاً) وطبيعتها القانونية (ثانياً)، وحجيتها في الإثبات (ثالثاً)، وذلك على النحو التالي:

أولاً: ماهية الحاسب الآلي وشبكة الإنترنت:

١. تعريف الحاسب الآلي:

توجد العديد من التعريفات التي أطلقت على الحاسب الآلي، حيث لم يكن هناك إجماع فقهي على إيجاد تسمية موحدة لجهاز الحاسب الآلي فالبعض توسع في تعريفه والبعض ضيق في تعريفه، وقد اعتمد المجمع اللغوي المصري تسميته بالحاسب الإلكتروني، وأُطلق عليه في الإنجليزية كمبيوتر (computer) وهو مشتق من الفعل (comput) والذي يعنى في اللغة العربية يحسب أو حاسب، وقد اعتمدت المنظمة العربية للمواصفات والقياس مصطلح الحاسوب[١].

ومن أهم التعريفات الموسعة للحاسب الآلي، تعريفه بأنه: «جهاز إليكتروني يتكون من مجموعة من العناصر المتداخلة والمتشابكة فيما بينها والتي تتعلق بإدخال واستخراج البيانات والمعلومات وتخزينها، فهو ينقسم إلى شقين، الشق الأول: الشق المادي الملموس (hardwar) والشق الثاني: غير الملموس (software) ويعمل وفق أوامر وتعليمات محددة لاستقبال وتخزين البيانات وإجراء المعالجات الممكنة لتحقيق النتائج المطلوبة بسرعة ودقة ضمن ترتيب معين وبتسلسل منطقي مما يسهل على المستخدم الحصول على ما يريد من معلومات ونتائج وبيانات، بشرط أن تكون تلك المدخلات صحيحة للوصول إلى نتائج صحيحة وحقيقية، بالإضافة إلى قيامه بمجموعة من العمليات الحسابية والمنطقية وفقاً للتعليمات المدخلة والمختزنة به ثم يقوم

(١) بطيخ، حاتم أحمد محمد. (٢٠١٧م). «دور الإنترنت في الإثبات أمام القاضي الجنائي والإداري – دراسة مقارنة»، أطروحة دكتوراه، قسم القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر. ص ٣٠.

بإخراجها في شكل نتائج حسابية »[١].

٢. تعريف شبكة الإنترنت:

تعددت وتنوعت التعريفات الفقهية لشبكة الإنترنت بتعدد وتنوع الاتجاهات التي يستند إليها كل فريق، ولم يتفقوا فيما بينهم على وضع تعريف محدد لها، فمنهم من اعتمد على الجانب التقني فقط، ومنهم من اعتمد على الجانب التقني الإنساني وذلك على النحو التالي:

الاتجاه الأول: ويري أنصاره ضرورة الاعتماد على الجانب التقني فقط لتعريف شبكة الإنترنت باعتبار أن الإنترنت ظاهرة تقنية بحتة، ويتزعم هذا الاتجاه العالمان الأمريكيان Vint Serf، و ob khan اللذان عملا على تصميم بروتوكول (TCP/IP) للتعامل عبر الإنترنت، ويعرف أنصار هذا الاتجاه شبكة الإنترنت بأنها «شبكة تتألف من عدد من الحاسبات الآلية التي ترتبط فيما بينها، إما عن طريق الخطوط التليفونية أو الأقمار الصناعية لتكون شبكة كبيرة تتيح لمستخدميها الدخول في أي وقت متى كان جهاز الحاسب الآلي الخاص به مزوداً بجهاز مودم »[٢].

الاتجاه الثاني: وهو يمثل غالبية الفقه، وقد اعتمد في تعريف شبكة الإنترنت على الجانب الإنساني، بالإضافة إلى الجانب التقني، ويري أنصاره ضرورة أن يوضع في الاعتبار القيمة الإنسانية للإنترنت إلى جانب القيمة التقنية عند البحث عن تعريف للإنترنت، على أساس أن الإنترنت يجمع بين الإنسانية إلى جانب التقنية معاً[٣].

وقد عرفت شبكة الإنترنت لدى البعض من أنصار هذا الاتجاه بأنها «شبكة دولية فسيحة تسمح لكافة أنواع الحاسوب بالمشاركة في الخدمات والاتصالات بشكل مباشر كما لو كانت كلها جهاز حاسوب واحد »[٤]، وعرفت أيضاً بأنها: «شبكة اتصالات دولية متصلة ببنوك المعلومات، ومراكز البحث العلمي ومراكز المعلومات المفتوحة والخاصة، والتي يتم الاتصال بها للحصول على معلومات من قبل المشتركين بالشبكة، ولكل منهم كلمة المرور الخاصة به password، وصندوق البريد الالكتروني (E-Mail) وموقع مخصص له »[٥].

(١) بطيخ، حاتم أحمد محمد. مرجع سابق، ص ٣٠.
(٢) – بطيخ، حاتم أحمد محمد. مرجع سابق، ص ٦٠.
(٣) – بطيخ، حاتم أحمد محمد. مرجع سابق، ص ٦١.
(٤) بطيخ، حاتم أحمد محمد. مرجع سابق، ص ٦٢.
(٥) تمام، أحمد حسام طه. (٢٠٠٠م). الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، ص ٢٧.

ثانياً: طبيعة الدليل الرقمي المستخرج من الحاسب الآلي وشبكة الإنترنت:

باعتبار أن الدليل الرقمي ينتمي إلى بيئة إليكترونية تتكون من نبضات إليكترونية يتم معالجتها باستخدام لغات برمجة رقمية وتقوم بتحويلها إلى أشكال متنوعة من المعلومات تعرض في شكل نصوص أو صور أو جداول، كما أنها تمكن المستخدم من اختيار اللغات الحية في تعامله مع الجهاز الرقمي، وتنتقل هذه الأشكال المبرمجة من خلال وسائل الاتصال الرقمي لشبكات النظم الرقمية، لذا يتميز الدليل الرقمي بطبيعة مركبة بحيث يرتبط الدليل بالجانب التقني للعالم الرقمي والمعلومة التي يتم بناؤها وحفظها بالتقنية الرقمية، وتتداول هذه المعلومة الرقمية عبر شبكات اتصال الإنترنت والحاسب الآلي[1].

ولما كان ذلك فإنه تواجهنا مشكلة في التعامل مع الكيان المنطقي وتكمن هذه المشكلة في البيانات والمعلومات المخزنة في صفحات القضاء الإلكتروني، فإن ما تتضمنه من المعلومات وبيانات قد تكون مستمدة بطريقة غير مشروعة أو تكون دليلاً على حصول تحريف أو دخول غير مشروع إلى الأنظمة المختلفة من أجل الحصول على الدليل، فكيف يقبلها القضاء وهي ليست دليلاً مادياً[2].

ولتجاوز هذه الإشكالية يلجأ القضاء إلى انتداب الخبراء المتخصصين لإجراء عمليات التثبت من محتوى البيانات الإلكترونية، ومن ثم تقديم التقرير الذي يعد هو الدليل وليس البيانات الإلكترونية، لكنه مسلك تأباه بعض النظم القانونية، عوضاً عن معارضته لأسس وأغراض إجراء الخبرة وطبيعتها كبينة تخضع للمناقشة لدى المحكمة.

وهنا تجدر الإشارة إلى أن الفكر القانوني اختلف حول حماية المعلومات والبيانات، فيرى البعض أن المعلومات لها طبيعة خاصة ولا يطبق عليها الشرط الضروري لتعريف الجريمة (لا يوجد تكييف قانوني لها) فهي تتسم بأنها جريمة خفية، وبالتالي فالدليل ليس محسوساً أو مرئياً[3]، ويرى البعض الآخر أن البيانات والمعلومات تأخذ قيمة مادية، بصفتها حقاً خاصاً ينسب إلى شخص محدد، وبالتالي تعد الأدلة الرقمية ما هي إلا مرحلة متقدمة من الأدلة المادية الملموسة التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان والاستعانة بجميع ما يبتكره العلم من أجهزه ووسائل التقنية الحديثة

(١) بطيخ، حاتم، مرجع سابق، ص ٣٩٥.

(٢) رستم، هشام فريد. (١٩٩٤م). الجوانب الإجرائية في الجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، مصر، ص. ٢٧.

(٣) عرب، يونس. (١٩٩٩). جرائم الكمبيوتر، مجلة البنوك، الأردن، العدد الخامس، ص ٣٧.

ومنها الحاسب الآلي وشبكة الإنترنت محور الأدلة الرقمية، فالأدلة الرقمية من منظور هذا الاتجاه لا تختلف من حيث المفهوم عن بصمات الأصابع أو بصمات الحمض النووي أو آثار الأسلحة وغيرها من الأدلة العلمية[١]، مؤدى ذلك: أن هنالك من يتجه إلى اعتبار الأدلة الجنائية الرقمية نوعاً من أنواع الأدلة المادية.

ثالثاً: حجية الدليل المتحصل من الحاسب الآلي وشبكة الإنترنت في الإثبات:

اختلفت أنظمة الإثبات التشريعية في تقديرها لمدى حجية تلك المخرجات وقوتها الثبوتية على النحو التالي:

ففي القوانين ذات الصياغة اللاتينية، ومنها القانون الأردني والفرنسي والمصري والسوري واللبناني، لا تثير حجية تلك الأدلة الإلكترونية أية صعوبات بالنسبة لحرية الأفراد في تقديم الأدلة لإثبات جرائم الإنترنت والحاسب الآلي، ولا تؤثر على حرية القاضي في تقدير هذه الأدلة ذات الطبيعة الخاصة باعتبارها أدلة إثبات في المواد الجنائية والإدارية، ففي فرنسا مثلاً لم تكن مشكلة حجية المخرجات المتحصلة من الإنترنت والحاسب الآلي على مستوى القانون الجنائي أمراً ملحاً أو عاجلاً في نظر الفقهاء، فالأساس هو حرية القاضي في تقدير هذه الأدلة، ويدرس الفقه الفرنسي هذه الحجية تحت نطاق قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل أجهزة التصوير وأشرطة التسجيل وأجهزة التنصت، وقد قضت محكمة النقض الفرنسية بأن أشرطة التسجيل الممغنطة تكون لها قيمة دلائل الإثبات ويمكن أن تكون صالحة للتقديم أمام القضاء الجنائي[٢]، وقد سارت على هذا النهج كل من ألمانيا وتركيا ولوكسمبورج واليونان والبرازيل، وأخضعت هذه الدول الأدلة الإلكترونية لحرية القاضي في تكوين قناعته الذاتية، بحيث يكون بمقدوره أن يطرح مثل هذه الأدلة- رغم قطعيتها من الناحية العلمية- عندما يجد أنها لا تتسق منطقياً مع ظروف الواقعة وملابساتها[٣].

وبالنسبة للدول التي يحدد فيها المشرع أدلة الإثبات ويقدر قيمتها الإقناعية، كما في نظام الدول الأنجلوسكسونية، فقد تضمنت قوانينها أدلة الإنترنت والحاسب الآلي ومنها، بريطانيا، التي أصدرت قانون إساءة استخدام الحاسوب في عام ١٩٩٠م، الذي لم يتناول الأدلة الناتجة عن الحاسوب، وربما كان السبب هو وجود قانون البوليس والإثبات

(١) Eoghan Casy: Digital Evidence Forensics Science Computer and The Internet Computer Crime, OP-CIT, P.٥.

(٢) - هلالي عبد الله أحمد، مرجع سابق، ص ٤٢. بطيخ، حاتم، ص ٥١٨.

(٣) بطيخ، حاتم، مرجع سابق، ص ٥١٧.

الجنائي لسنة ١٩٨٤م، الذي حوى تنظيماً محدداً لمسألة قبول مخرجات الإنترنت والحاسب الآلي، كأدلة إثبات في المواد الجنائية، ومنها أيضاً الولايات المتحدة الأمريكية التي تناولت في بعض القوانين حجية الأدلة الإلكترونية(١).

الفرع الثاني

أدوات وتقنيات المعاملات الإلكترونية

من الأدوات والتقنيات التي قد تستخدم كأدلة إثبات جنائية إلكترونية؛ أدوات وأنظمة المعاملات، وفيما يلي بيان أبرز تلك الأدوات والتقنيات:

أولاً: التوقيع الإلكتروني في التصرفات:

لقد توصل الفريق العامل الرابع التابع للجنة الأمم المتحدة للقانون التجاري الدولي؛ المكلف بالعمل التحضيري بشأن التجارة الإلكترونية؛ بعد وضعها الدليل القانوني الخاص بقبول التحويلات الإلكترونية للأموال سنة (١٩٧٨م) وتوصية (١٩٨٥م) المتعلقة بالقيمة القانونية للسجلات الحاسوبية؛ إلى وضع قانونين سمي الأول: بقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية والمعتمد رسمياً من قبل اللجنة العامة للأمم المتحدة بموجب القرار (٥١/١٦٢) الصادر بتاريخ: ١٦ ديسمبر ١٩٩٦م، أما الثاني فهو قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية الصادر عن الجمعية العامة للأمم المتحدة بموجب القرار رقم (٥٦/٨٠) المؤرخ: ١٢ ديسمبر ٢٠٠١م، تلتهما اتفاقية الأمم المتحدة المتعلقة بالخطابات الإلكترونية في العقود الدولية سنة (٢٠٠٥م)(٢).

ويعرف التوقيع الإلكتروني عند فقهاء القانون: «بأنه كل إشارة أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع ومرتبطة ارتباطاً وثيقاً بالتصرف الإلكتروني، وتتم بتمييز شخص صاحبها وتحديد هويته، وتتم دون غموض عن رضائه

(١) بطيخ، حاتم، ص ٥١٧.

(٢) هي لجنة أنشئت بموجب القرار رقم (٢٢٥) (د -٢١) المؤرخ في ١٧ ديسمبر ١٩٦٦م الصادر عن الجمعية العامة للأمم المتحدة، تتشكل من ستين دولة منتخبة في الجمعية العامة مع مراعاة تنظيم الأقاليم الجغرافية والأنظمة الاقتصادية والقانونية المختلفة، أما العضوية فتكون لمدة ست سنوات مع تجديد نصفي كل ثلاث سنوات. يقع مقر أمانتها في فينيا، ومهمتها: عصرنة ومواءمة القواعد المتعلقة بالأعمال التجارية الدولية بصياغة اتفاقيات وقوانين نموذجية وقواعد وتوصيات مقبولة عالمياً بالإضافة إلى إعطاء معلومات محدثة عن السوابق القضائية وتقديم مساعدة تقنية في مشاريع إصلاح القوانين وتنظيم حلقات دراسية إقليمية ووطنية في مجال القوانين التجارية الموحدة.

بهذا التصرف القانوني»[١].

وحتى يكتسب التوقيع الإلكتروني قيمته القانونية؛ فلا بد فيه من توافر شروط معينة نوردها في الآتي:

أ- تحديد هوية الموقع: يعتبر التوقيع عنصراً جوهرياً في المحرر، وهو عنصر لا غنى عنه؛ لإضفاء الحجية عليه، حيث يتضمن إقرار الموقع بالرضاء عما هو في المدون، وهو بهذه المثابة يعتبر تصرفاً إرادياً يكشف عن هوية صاحبه ويميزه عن غيره[٢].

ب- التعبير عن إرادة صاحب التوقيع: حتى يستوفي التوقيع الإلكتروني الشروط القانونية، وتكون له حجية في الإثبات لابد أن يكون توقيع المحرر الإلكتروني صادراً عن إرادة الموقع برضائه بمضمون التصرف القانوني وإقراره له[٣].

ج- اتصال التوقيع بالمحرر: يشترط في التوقيع لكي يؤدي وظيفته القانونية إقرار الموقع بما ورد في مضمون المحرر، وأن يكون التوقيع متصلاً بالمحرر على نحو لا يمكن فصله عنه، وأن يكون هذا الاتصال مستمراً ويمكن حفظه واسترجاعه بطريقة معلوماتية آمنة طوال الفترة الزمنية الكافية لاستخدامه في الإثبات، ويضع الموقع توقيعه في نهاية المحرر بحيث ينسحب التوقيع على كافة البيانات الواردة في المحرر الإلكتروني، ويلزم أن يكون التوقيع متصلاً اتصالاً مادياً ومباشراً بالمحرر. وبالرغم من أن العرف قد استقر على وضع التوقيع في نهاية المحرر إلا أن ذلك ليس شرطاً لوجود العقد وصحته[٤].

أما بالنسبة لحجية التوقيع الإلكتروني فإنها تعتمد على قيمة التوقيع الإلكتروني ومحتوى البيانات الواردة على المحرر الإلكتروني يرتبط بمدى الثقة التي تحيط به، وهي ثقة تعتمد على مدى إمكانية التلاعب في التوقيع الإلكتروني والبيانات المرتبطة به، فهي مسألة مرتبطة بالأمان التقني الإلكتروني[٥].

(١) فهمي، خالد مصطفى. النظام القانوني للتوقيع الإلكتروني، في ضوء الاتفاقيات الدولية التشريعات العربية والقانون رقم (١٥) لسنة ٢٠٠٤م، بدون طبعة، دار الجامعة الجديد، الإسكندرية. (٢٠٠٧م). ص٣٨.

(٢) بلعيد، يحيى محمد السعيدي عبيد. (٢٠٠٧/٢٠٠٨). التوقيع الإلكتروني وحجيته في الإثبات في القانون المدني اليمني والمصري «دراسة مقارنة»، دبلوم تمهيدي، المعهد العالي للقضاء. ص. ١٠.

(٣) فهمي، خالد مصطفى. (٢٠٠٤م). النظام القانوني للتوقيع الإلكتروني في ضوء الاتفاقيات الدولية والتشريعات العربية والقانون رقم ١٥لسنة ٢٠٠٤م.

(٤) الجمالي، سمير حامد عبد العزيز، مرجع سابق، ص ٢٢٤-٢٢٥.

(٥) بلعيد، يحيى محمد السعيدي عبيد، مرجع سابق، ص. ١٣.

فإذا تم تأمين الطابع المتفرد لبيانات إنشاء التوقيع الإلكتروني، وعدم قابلية التوقيع ومفرداته لبيانات الاستنساخ وحمايته، مما قد يؤثر في سلامة وصحة نسبته لطرف ما، أو تأكيد عدم تعرضه لتقليد أو تزوير أو تحريف أو اصطناع بما يعكس علم الموقع، المنسوب إليه التوقيع الذي يتحمل بالتزامات ناشئة بمضمون المحرر الإلكتروني قبل التوقيع، فإنه ينتج أثره القانوني مثل الأثر المترتب على التوقيع العادي[١].

وقد أضحى التوقيع التقليدي لا يتفق مع المعاملات التي تتم بواسطة المعلومات أو معالجة المعلومات بطريقة آلية، جعلت التعامل يتم عن طريق كتابة المعلومات أو البيانات بطريقة رمزية أو أرقام، ويتم التوقيع عليها بما يسمى التوقيع الرقمي، وكذلك ما يدعو الشكل في قيمة التوقيع الإلكتروني يرجع إلى انفصال هذا النوع من التوقيع عن شخصية صاحبه وإمكانية تكراره دون موافقته أو علمه، لذا يتم استخدام تقنيات تكنولوجية معتمدة من أجل تأمينه[٢].

ثانياً: السجلات الإلكترونية:

السجل الإلكتروني هو: «القيد أو العقد الإلكتروني أو رسالة البيانات التي يتم إنشاؤها أو إرسالها أو تسليمها أو تخزينها بوسائل إلكترونية[٣].

وبالنسبة لحجية السجلات الإلكترونية فكما في التوقيع الإلكتروني؛ فإن قيمة السجل الإلكتروني ومحتوى البيانات الواردة على المحرر الإلكتروني ترتبط بمدى الثقة التي تحيط به، وهي ثقة تعتمد على مدى إمكانية التلاعب في التوقيع الإلكتروني والبيانات المرتبطة به، فهي مسألة مرتبطة بالأمان التقني الإلكتروني. فإذا تم تأمين بيانات السجل الإلكتروني، وتأكيد عدم قابليته لتقليد أو تزوير أو تحريف أو اصطناع سجل مشابه، فإنه ينتج أثره القانوني مثل الأثر المترتب على السجل العادي[٤].

ثالثاً: رسائل المعلومات والوسائط الإلكترونية:

تعتبر رسالة المعلومات وسيلة من وسائل التعبير عن الإرادة المقبولة قانوناً لإبداء الإيجاب أو القبول بقصد إنشاء التزام تعاقدي في المعاملات التجارية والمدنية، وهذا

(١) عبدالرحمن، خالد حمدي. (٢٠٠٦م)، التعبير عن الإرادة في العقد الإلكتروني، (ب ط)، دار النهضة العربية – والقاهرة، ص ٢٤.

(٢) بلعيد، يحيى محمد السعيدي عبيد، مرجع سابق، ص. ١٣.

(٣) عبدالرحمن، خالد حمدي، مرجع سابق، ص ٢٤.

(٤) بلعيد، يحيى محمد السعيدي عبيد، المرجع السابق، ص ١٤.

بلا شك ينعكس عليها في اعتبارها أدلة إثبات جنائية إلكترونية، أما حجيتها وآثارها، فهي تتمتع بذات الحجية والآثار القانونية التي تتمتع بها الوثائق والمستندات والتوقيعات الخطية، من حيث إلزامها لأطرافها وحجتها في الإثبات(١).

الفرع الثالث

الأدلة المتحصلة من أدوات وتقنيات ومواقع التواصل الاجتماعي

تعد المعلومات التي تتوفر على مواقع التواصل الاجتماعي مذهلة؛ فمواقع التواصل الاجتماعي مثل فيسبوك قادرة- استجابةً لطلبات قضائية أو مذكرات تفتيش- على تزويد أجهزة الشرطة والنيابة العامة والقضاء بمعلومات كاملة عن صاحب الحساب، إضافة إلى المراسلات الموجودة على واجهة الموقع، والصور التي تم تحميلها على الموقع، والصور التي تم التأشير عليها من قبل المستخدم، وقائمة شاملة بالأصدقاء، وعمليات تسجيل الدخول، ومعلومات تحديد الموقع بدقة(٢).

ولم يعد سراً القول إن أجهزة العدالة الجنائية تقوم «بتفتيش» مواقع التواصل الاجتماعي بحثاً عن أدلة، وبدون الحاجة للحصول على تفويض من المحكمة أو طلب إحضار، هناك الكثير من المعلومات المهمة المتمثلة في الأدلة المتوفرة للعامة على مواقع التواصل الاجتماعي، على سبيل المثال: إدارة الشرطة في ولاية نيويورك في الولايات المتحدة تملك وحدة خاصة لمواقع التواصل الاجتماعي، تقوم بالبحث في مواقع التواصل الاجتماعي مثل فيسبوك وتويتر وغيرهما، من أجل الحصول على أدلة أو ضبط أي نشاط إجرامي محتمل الوقوع(٣).

وغالبية الهيئات الحكومية مشاركون فاعلون، حيث يساهمون في المحتوى وفي الحث على نشر المعلومات من خلال مواقع التواصل الاجتماعي ولا تحتاج الأجهزة المختصة إلى الحصول على إذن بالتفتيش، أو أمر من المحكمة، للحصول على الدليل بالنظر إلى حجم المعلومات المتوفرة للعامة على مواقع التواصل الاجتماعي، والطرق

(١) للمزيد انظر: عبدالرحمن، خالد حمدي، مرجع سابق، ص ٢٤ - ٢٦.

(٢) حمدان الرواشده، سامي. الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي «دراسة في القانونين الإنجليزي والأمريكي». International Review of Law: Vol ٣, ٢٠١٧. ١٤. dx.doi.org/١٠,٥٣٣٩/irl.١٤,٢٠١٧

(٣) Rocco Parascandola, NYPD forms new social media unit to mine Facebook and Twitter for mayhem, n.Y. DaiLY news, Aug ١٠, ٢٠١١, http://www.nydailynews.com/new-york/nypd-forms-new-social-media-unit-facebooktwitter-mayhem-article-١,٩٤٥٢٤٢.

التي تملكها في سبيل البحث عن هذه المعلومات.

ففي أقصى الحدود، تشكل بعض الاتصالات في مواقع التواصل الاجتماعي جريمة يعاقب عليها القانون وفي حالات أخرى، يستند الادعاء العام على أشياء تجريمية لإثبات الإدانة بصورة مباشرة أو غير مباشرة، ويستخدم محامو الدفاع عن المتهم الرسائل المرسلة عن طريق مواقع التواصل الاجتماعي لمهاجمة مصداقية الشهود، ودحض أدلة «تحديد الهوية» المقدمة من قبل النيابة العامة[١].

وفي هذا الفرع سنتناول ماهية مواقع التواصل الاجتماعي من حيث تعريفها (أولاً)، وأهمية مواقع التواصل الاجتماعي في الإثبات الجنائي (ثانياً)، وحجية مواقع التواصل الاجتماعي في الإثبات (ثالثاً)، وذلك على النحو التالي:

أولاً: تعريف مواقع التواصل:

تعرف مواقع التواصل الاجتماعي بأنها: تقنيات موجودة على شبكة الإنترنت يستخدمها الناس للتواصل والتفاعل مع بعضهم البعض[٢].

كما يشار في بعض الأحيان، إلى مواقع التواصل الاجتماعي على أنها: المحتوى الذي يتم إنشاؤه باستخدام أدوات مواقع التواصل الاجتماعي، لا سيما «المحتوى الذي يقدمه المستخدم»، والذي يتم إنشاؤه بواسطة الأفراد على المواقع الإلكترونية التي تشجع على إنشاء وتبادل المحتوى، ويتراوح المحتوى ما بين رسائل نصية، إلى صور يتم تبادلها، ومقاطع فيديو تحظى بمشاهدات عديدة[٣].

وعلى الرغم من ذلك، فإن مفهوم مواقع التواصل الاجتماعي عادة ما يشير إلى واحدة من الصفات الأكثر أهمية بين جميع وسائل الإعلام الموجودة على الإنترنت وهي: القدرة على التبادل الحيوي للمعلومات بين الأفراد، أو المجموعات[٤].

ثانياً: أهمية مواقع التواصل الاجتماعي في الإثبات الجنائي:

مما لا شك فيه أن مواقع التواصل الاجتماعي تقدم خدمات ذات أهمية بالغة؛

(١) See, e.g., Haque & Nuth [٢٠٠٩] (EWCA (Crim ١٤٥٣؛ Johnson [٢٠٠٨] (EWCA (Crim ٣٣٢١؛ Mullen [٢٠١١] (EWCA (Crim ١٧٤٤؛ Eglen [٢٠١١] ٧ (EWCA (Crim ١٤٣٧؛ Hothi [٢٠١١] (EWCA (Crim ١٠٣٩؛ O'Brien [٢٠١١] (EWCA (Crim ٧٦٨.

(٢) حمدان الرواشده، سامي، مرجع سابق، ص. ٥.

(٣) نفس المرجع، ص. ٥.

(٤) نفس المرجع، ص. ٥.

فالمهمة الأساسية لها هي المحافظة على التواصل الفعال مع الأصدقاء لتقديم النصيحة في مجالات الصحة وغيرها، ومشاركة الخبرات العلمية ومبادرات الأعمال[١].

والأدلة المتحصلة من هذه الاتصالات قد تكون ذات علاقة بالمحاكمة الجنائية، ويمكن أيضاً لأجهزة الشرطة أن تستخدم مواقع التواصل الاجتماعي في التحقيقات التي تجريها من خلال إنشاء حسابات على مواقع التواصل الاجتماعي للحصول على معلومات من الجمهور، أو من خلال استخدام الإعلانات على مواقع التواصل الاجتماعي، كما يمكن في الوقت نفسه أن يساء استخدام مواقع التواصل الاجتماعي لتحقيق أهداف إجرامية مثل: الانتحال، والغش، وسرقة الهوية، وبدء وتطوير علاقات إجرامية، ومشاركة مواد غير مشروعة، والتنمر الإلكتروني، وتعنيف الضحايا، وإقامة وإدارة الشبكات الإجرامية[٢].

ثالثاً: حجية مواقع التواصل الاجتماعي في الإثبات:

من السهل التلاعب في الاتصالات الإلكترونية مثل البريد الإلكتروني، حيث تتوفر تعليمات واضحة على شبكة الإنترنت يمكن الاستفادة منها في كيفية التلاعب بالبريد الإلكتروني، ومن السهل أيضاً التلاعب بالرسائل الصادرة عن مواقع التواصل الاجتماعي من خلال نسخ الرسالة في برامج أخرى، إذاً مادامت تلك المواقع سهلة التلاعب والانتحال فما مدى حجيتها في الإثبات الجنائي؟

اختلف الفقه القانوني في ذلك، فشراح القانون الأمريكي أبدوا تشدداً واضحاً في معرض بحث هذا الموضوع[٣]، حيث يرى الفقيه « Schwartz» أنه يتوجب على الطرف الذي يسعى إلى تقديم الدليل أن يقنع قاضي الموضوع بأن المسألة محل البحث المراد إثباتها «من المحتمل أن تكون صحيحة على الأغلب»[٤].

ويرى الفقيه « Mason» أن التحقق من أصالة الدليل يتعين أن يتم وفقاً للمعايير المنصوص عليها في القانون الجنائي[٥]، وقد أفصح صراحة عن دعمه فكرة أن يتم التعامل مع أصالة الدليل من خلال «معيار القبول» (admissibility test) من حيث المبدأ.

---

(١) نفس المرجع، ص.٦.

(٢) حمدان الرواشده، سامي، مرجع سابق، ص.٦.

(٣) حمدان الرواشده، سامي، مرجع سابق، ص.٢٠.

(٤) O'Floinn & Ormerod, Social Networking Material, supra note ٧١ at ,٥٠٤; see also O'Floinn & Ormerod, Social Networking Sites, supra note ٣١١٧٧ at ,٤٩٠.

(٥) eLecTRonic eviDence ١٠,٢٨٢-١٠,٢٨٣ (Stephen Mason & Daniel Seng, eds ٢٠١٠).

ومما لا شك فيه أن هناك غموضاً كبيراً يتعلق بتحديد معنى هذا المعيار ضمن هذا السياق في قضية (R v. Robson)[١] قضت المحكمة بقبول تسجيلات الفيديو في عداد الأدلة بعد أن تم التحقق من أصالتها، وقد فصلت المحكمة في موضوع أصالة الفيديو بناء على «موازنة الاحتمالات» (balance of probabilities) وهو أمر يتساوى مع دليل المصداقية من حيث المبدأ[٢].

كما قضت محكمة الاستئناف في أيرلندا الشمالية في قضية (R v. Murphy)[٣] بقبول الدليل المتمثل في تسجيلات الفيديو طالما كان موثوقاً بها من حيث المبدأ، وقد سعت المحكمة في هذه القضية إلى تطبيق هذا المعيار، وأشارت إلى قضية (Robson) ولكن لم تتم الإشارة إلى فكرة موازنة الاحتمالات.

وهناك أحكام قضائية أخرى نظرت إلى الموضوع على اعتبار أنه مسألة تتعلق بالعلاقة؛ أي أن الوقائع المراد إثباتها تتعلق بالدعوى أو مرتبطة بها. في قضية (The Queen v. Aidan Quinn) يبدو أن محكمة الاستئناف في أيرلندا الشمالية تبنت التفسير الذي قالت به في قضية (Murphy) حيث قضت بأن تحديد ما إذا كانت تسجيلات الفيديو موثوقاً بها من حيث المبدأ هو أمر يتعلق بالعلاقة المحتملة للوقائع المراد إثباتها بالدعوى المنظورة (test of potential relevance).

وأيد جانب من الفقه الإنجليزي هذا الاجتهاد القضائي، فالأستاذة «Pattenden» ترى أن مسألة العلاقة يتعين تقريرها في ضوء ارتباط الوقائع المراد إثباتها بالدعوى بشكل عام، إضافة إلى وجود دليل على المصداقية، ويصف الفقه هذا المنهج بأنه منهج «متعدد الطبقات» (multi-layered test) وهذا المنهج يتطلب الآتي:

١. يجب أن يكون الدليل المتحصل من مواقع التواصل الاجتماعي له علاقة منطقية بالوقائع محل البحث. ويتحقق ذلك عندما يتمتع هذا الدليل بالأصالة، ويؤخذ في الاعتبار كل الاحتمالات المتعلقة بالمسألة محل النزاع.

٢. يجب أن يكون الدليل المستخلص من مواقع التواصل الاجتماعي متعلقاً قانوناً بالدعوى؛ ويكون ذلك عندما يتبين وجود دليل مقبول ذي مصدر يتمتع بالثبات والنزاهة[٤].

---

(١) WLR ٦٥١؛ [١٩٧٢] ٢ All ER ٦٩٩؛ [١٩٧٢] ٥٦ Cr. App. R ٤٥٠؛ [١٩٧٢] Crim. LR ٣١٦؛ [١٩٧٢] ١١٦ SJ ٣١٣. ١ [١٩٧٢]

(٢) حمدان الرواشده، سامي، مرجع سابق، ص. ٢٠.

(٣) نفس المرجع السابق، ص ٢١.

(٤) حمدان الرواشده، سامي، مرجع سابق، ص. ٢٢.

ويهدف هذا المنهج إلى توفير متطلب سهل؛ لأنه من مهام هيئة المحلفين تقرير أصالة الدليل المقدم محل النزاع في نهاية المطاف. وقد دافعت الأستاذة «Pattenden» عن معيار «وجود دليل على المصداقية» (أي حد أدنى من الأدلة التي تثبت المصداقية،) وأعربت عن مخاوفها من أن تطبيق المعيار من حيث المبدأ سيفسر على أنه يفرض المعايير المبدئية في الإثبات الجنائي(١).

وعلى الرغم من أن جانباً من الفقه الجنائي يؤيد تطبيق متطلب سهل لمعيار الأصالة، فإن تبني هذا المنهج سوف يواجه تطبيقه صعوبات في الواقع العملي.

وتطبيق مبدأ الارتباط المنطقي والقانوني (أي أن تكون الوقائع المراد إثباتها مرتبطة بالدعوى ارتباطاً منطقياً وقانونياً) يؤدي إلى حلقة مفرغة. فإذا كان يجب أن يكون الدليل المستخلص من مواقع التواصل الاجتماعي أصيلاً بصورة محتملة لاستيفاء معيار الارتباط المنطقي، فلا بد إذن من وجود «بعض الدليل» يؤكد المصداقية والأصالة، كما يتطلب ذلك مبدأ الارتباط القانوني(٢).

ويرى جانب من الفقه الإنجليزي أن الغموض في موقف القانون الإنجليزي ينبثق من أن التعامل مع موضوع أصالة الدليل ينظر إليه على أنه مظهر للارتباط، ويضاف إلى ذلك وجود التباس حول المعيار الذي يجب أن يستند إليه القاضي فيما يتعلق بأصالة الدليل، فيتعين على كل طرف أن يقدم دليلاً تم الحصول عليه من مواقع التواصل الاجتماعي، وأن يستوفي متطلبات عبء الإثبات.

كما يذهب هذا الجانب من الفقه- بحق- إلى أن عبء الإثبات لا يعني إثبات أي شيء، خلافاً لعبء الإثبات، فإن عبء تقديم الدليل لا يتطلب من الخصم أن يخلق أي درجة من الثقة لدى القاضي بصحة الدليل، بل يكفي من الخصم أن يقنع محكمة الموضوع بأن المسألة محل البحث تستحق أن تؤخذ بعين الاعتبار للحكم في الدعوى(٣).

وقد عبر عن هذه الفكرة بعض الفقهاء منهم « Bingham»(٤) حيث يرى أن عبء الإثبات لا يقصد به وجوب تقديم دليل حاسم في الدعوى، أو وجوب تقديم بينة

---

(١) نفس المرجع السابق، ص. ٢٢.

(٢) O'Floinn & Ormerod, Social Networking Material, supra note ٧١, at ٤٩١.

(٣) PauL RoBeRTs & aDRian ZucKeRman, cRiminaL eviDence ٢٧-٢٨ (٢d ed ٢٠١٠).

(٤) أستاذ فخري (Emeritus Professor) في القانون الجنائي، في كلية القانون، جامعة « »Oxford البريطانية. أشار إليه: حمدان الرواشده، سامي، مرجع سابق، ص. ٢٢.

على صحة الادعاء، بل يعني عبء أن يجعل الخصم مسألة ما صالحة لتكون محل تقدير من قبل محكمة الموضوع.

ويرى الأستاذ « Tapper » أن موضوع التحقق من أصالة الدليل يعادل استيفاء عبء تقديم الدليل فلا توجد «واقعة أساسية» تتطلب الإثبات، لا يعد التحقق من أصالة الدليل مسألة تتعلق بتقرير الارتباط(١).

كما يذهب الفقه الأمريكي إلى أنه يتعين ألا يكون موضوع التحقق من أصالة الدليل متطلباً صعباً بصورة مبالغ فيها(٢).

وفي القانون الإنجليزي يكفي لاستيفاء متطلبات التحقق من أصالة الدليل أن يترك الأمر لهيئة المحلفين. على سبيل المثال: شهادة الشاهدة التي تقر فيها بوجود علاقة صداقة سابقة على موقع التواصل الاجتماعي مع شخص، وأنها استقبلت وشاهدت الاتصالات ذات العلاقة التي أرسلت من ذلك الشخص؛ فالدليل الظرفي قد يكون كافياً أيضاً، على الرغم من أن الدليل الظرفي الضعيف لا يمكن التعويل عليه لاستيفاء المتطلبات المبدئية للأصالة(٣).

المطلب الثاني

إجراءات الإثبات الجنائي في التحقيق الرقمي

شهد التحقيق الإلكتروني تطوراً لافتاً في الآونة الأخيرة، حيث أنشئت دوائر وأقسام مستقلة في مؤسسات إنفاذ القانون، كما تم رفدها بفرق عمل متخصصة للتعامل مع الأدلة الرقمية، مثل فرق عمل مسرح الجريمة، وجمع الأدلة الرقمية، وتحليل الأدلة الرقمية وفحصها(٤).

وسنبين في هذا المطلب، الاختصاص القضائي في الجرائم الإلكترونية في الفرع الأول، ومراحل إجراء التحقيق الرقمي ومتطلباته في الفرع الثاني، ووسائل الإثبات الإلكترونية في التحقيق الرقمي في الفرع الثالث، وذلك على النحو التالي:

(١) نفس المرجع السابق، ص ٢٢.
(٢) نفس المرجع السابق، ص ٢٢.
(٣) حمدان الرواشده، سامي، مرجع سابق، ص. ٢٢.
(٤) عبد الباقي، مصطفى. مرجع سابق، ص ٢٨٦.

الفرع الأول

الاختصاص القضائي في التحقيق الرقمي

إذا كان الاختصاص في الجرائم التقليدية الداخلية يؤول إلى قضاء دولة واحدة، فإن الاختصاص القضائي في الجريمة الإلكترونية يثير العديد من الإشكالات كتحديد القانون الواجب التطبيق والقضاء المختص بنظر تلك الجرائم سواء على الصعيد الداخلي أو الخارجي، ويرجع ذلك إلى صفتها الممتدة في أكثر من إقليم دولة، إما من حيث ارتكاب هذه الجريمة أو من حيث الآثار المترتبة عليها[1].

وقد نظم المشرع اليمني القواعد العامة للاختصاص القضائي في نظر الجرائم، ضمن الكتاب الثالث (في المحاكمة)، الباب الأول (اختصاص المحاكم)، الفصل الأول والثاني والثالث، ضمن المواد من (٢٣١) إلى (٢٥٠)، حيث تنطبق هذه الأحكام على جميع الجرائم سواء كانت تقليدية أو إلكترونية، وسنتناول ذلك تفصيلاً في المبحث الثالث الخاص بموقف المشرع اليمني من التحقيق الرقمي.

الفرع الثاني

مراحل إجراء التحقيق الرقمي ومتطلباته

يمر التحقيق في الجرائم الإلكترونية بمراحل إجرائية مختلفة، منها ما هو فني، ومنها ما هو إجرائي تنفيذي، فالمراحل الفنية تتمثل في وضع خطة عمل التحقيق، والثانية تشكيل فريق التحقيق، أما المراحل التنفيذية تتمثل في: الإجراءات التي يتم تنفيذها في مسرح الجريمة، والإجراءات التالية التي ينبغي على فريق التحقيق القيام بها في مسرح الجريمة، وسنتناول ذلك تفصيلاً في البنود التالية:

أولاً: الإجراءات الفنية السابقة على مباشرة التحقيق:

في الجرائم الإلكترونية يتم اتباع منهج تحقيقي فني يختلف عن غيره بالنسبة للجرائم الأخرى، وهذا المنهج يتمثل في وضع خطة عمل التحقيق أولاً، وتشكيل فريق التحقيق ثانياً، ونسبين ذلك تفصيلاً فيما يلي:

(١) بوحزمة نصيرة. (٢٠٢١/٢٠٢٢). التحقيق الجنائي في الجرائم الإلكترونية «دراسة مقارنة». أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس – سيدي بلعباس، الجزائر. ص ٢١٢.

١. وضع خطة عمل التحقيق:

يبدأ المحقق عند تجميع الاستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللازمة على ضوء المعلومات المتوفرة لديه، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك على النحو الآتي[١]:

- وضع الخطة المناسبة والتي لا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة.
- التخطيط الفني للتحقيق وذلك من أجل الوصول إلى أفضل الطرق والأساليب التعامل مع هذه الجرائم.
- عمل دراسة جادة لكافة الإجراءات التحقيق خطة مسبقة التي يتم وضعها ومناقشتها من طرف العاملين في فريق التحقيق[٢].
- تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في إنجاز العمل من أجل ضمان مستوى جيد من الأداء.
- تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطار الفردية التي قد تنتج عن قلة الخبرة أو نقص المعرفة، والتي تساعد في التقيد بالمستوى المطلوب والتي تضمن الخطوات التي يقوم بها المحقق خلال مراحل التحقيق.

٢. تشكيل فريق التحقيق:

إن التحقيق الابتدائي في الجرائم المعلوماتية يكون غالباً أكبر من أن يتولاه شخص واحد بمفرده، حتى ولو كانت المضبوطات هي مجرد حاسب شخصي واحد، ولذلك فإنه يفضل أن يتعاون عدة محققين في إنجاز مهمة التحقيق والعثور على الأدلة، ويجب أن يتشكل فريق التحقيق من فنيين أخصائيين ذوي خبرة في مجال الحاسوب الإنترنت، ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الإلكتروني بشكل خاص، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والإنترنت ليتمكنوا من فك التعقيدات التي تفرقها ظروف وملابسات كل جريمة[٣].

---

(١) بن قدوم سوهيل؛ وبسام لديدة، مرجع سابق، ص ٢١.

(٢) السرحاني، محمد نصير. (٢٠٠٤). مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، ص ٧٢.

(٣) عبد الله حسين محمود. (٢٠٠٣). إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، ص ٦١٢.

وإن كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلا أنه يأخذ أهمية خاصة في الجرائم المعلوماتية لما يتطلبه من مهارات وخبرات متنوعة قد لا تتوافر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمراً ضرورياً ومن الناحية العملية غالباً ما يتكون فريق التحقيق من:

- خبراء الحاسوب وشبكات الإنترنت الذين يعرفون ظروف الحادثة وكيفية التعامل مع هذه الجرائم.
- خبراء ضبط وتحرير الأدلة الرقمية العارفون بأمور تفتيش الحاسوب.
- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.
- خبراء التصوير والبصمات والرسم التخطيطي[١].

ثانياً: المراحل الإجرائية التنفيذية:

يقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبيها، وهناك إجراءات واحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الابتدائي وإجراءات أخرى يجب على الضبطية القضائية مراعاتها أثناء التحقيق الابتدائي[٢].

وتمر هذه الإجراءات بمرحلتين رئيستين: المرحلة الأولى تمثل الإجراءات التي يتم تنفيذها في مسرح الجريمة، والمرحلة الثانية تشتمل على الإجراءات التالية التي ينبغي على فريق مسرح الجريمة من مأموري الضبط القضائي، ذوي الاختصاص، القيام بها[٣]، وسنتناول هاتين المرحلتين تفصيلاً في الفقرات التالية:

١. الإجراءات التي يتم تنفيذها في مسرح الجريمة:

تتمثل الإجراءات التي يتم تنفيذها في مسرح الجريمة في: إغلاق أو تجميد مسرح الجريمة لمنع فقدان أو تلف أو تلوث الأدلة، والحفاظ على مسرح الجريمة وتأمينه ومنع العبث به[٤]، ومراعاة ما يلي[٥]:

(١) عبد الله حسين محمود، مرجع سابق، ص٦١٣.
(٢) حجازي عبد الفتاح بيومي، مرجع سابق، ص ٨٤.
(٣) عبد الباقي، مصطفى. مرجع سابق، ص ٢٨٦.
(٤) عبد الباقي، مصطفى. مرجع سابق، ص ٢٨٦.
(٥) بن قدوم سوهيل؛ وبسام لديدة، مرجع سابق، ص ٢١.

- تحديد نوع نظام المعالجة الأولية للمعطيات فهل هو كمبيوتر معزول أم متصل بشبكة معلومات.
- وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.
- إذا وقعت الجريمة على شبكة فإنه يجب حصر طرفيات الاتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الاختراق من عدمه.
- مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.
- مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.
- يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار الجريمة.
- فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيئون استخدامها لطمس البيانات.
- التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنه من الخدع التي يستعملها الجاني عند الاختراق أن يتم ذلك بخط هاتفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتقليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك.
- إبعاد الموظفين عن أجهزة الحاسوب الآلي بعد الحصول منهم على كلمة السر وكذا الثغرات في حالة وجودها.
- تصوير الأجهزة المستهدفة من أمام والخلف لإثبات بأنها كانت تعمل.

٢. الإجراءات التالية التي ينبغي على الفريق القيام بها في مسرح الجريمة أثناء التحقيق:

في هذه المرحلة ينبغي على فريق مسرح الجريمة من مأموري الضبط القضائي، ذوي الاختصاص[١] القيام بما يلي:

- توثيق حالة مسرح الجريمة، أي تسجيل كافة التفاصيل المتعلقة بحالة الكمبيوتر،

(١) عبد الباقي، مصطفى. مرجع سابق، ص ٢٨٦.

مثل تحديد ما إذا كان في وضع التشغيل (مفتوحا) وقت ضبطه أم لا، وما إذا كان موصولاً بالإنترنت أم لا.

- تحديد هوية وتوثيق جهاز الكمبيوتر والأجهزة الملحقة به التي يعثر عليها في مسرح الجريمة، حيث أن رمز بروتوكول الإنترنت يلعب دوراً كبيراً في تحديد موقع ومكان المشتبه به.
- تحديد هوية وتوثيق أجهزة التخزين مثل (CDs) و (DVDs) التي يعثر عليها في مسرح الجريمة.
- تصوير مسرح الجريمة.
- حفظ الأدلة والمواد الرقمية.
- حفظ الوثائق المطبوعة.
- حفظ الأجهزة.
- إجراء استرجاع للوثائق العالقة، من قبيل طباعة الأوراق العالقة في ماكينة الطباعة.
- إجراء استرجاع للوثائق الملغاة أو التي تم مسحها[1].
- نقل الأدلة التي يتم ضبطها.
- عمل نسخة احتياطية من الأقراص الصلبة قبل استخدامها والتأكد فنياً من دقة النسخ.
- نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.
- العمل على فحص العلاقة بين برامج التطبيق والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.
- حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة.
- العمل على فحص برامج الأجهزة وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلومات.
- أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص وتحليل المعلومات

(١) عبد الباقي، مصطفى. مرجع سابق، ص ٢٨٧.

الموجودة بها بغرض التوصل إلى معرفة المعلومات والملفات الممسوحة، وكذلك معرفة الملفات المخفية المخزنة في ذاكرة الحاسوب[١].

الفرع الثالث

وسائل الإثبات الإلكترونية في التحقيق الرقمي

إن التعامل في الجريمة المعلوماتية يتطلب إجراءات روتينية متفقاً عليها وذلك من أجل حماية الدليل، غير أن وسائل حفظ الأدلة واستنتاجها تختلف من الجريمة التقليدية إلى الجريمة المعلوماتية الرقمية، ذلك لأن البرامج والبيانات عنصران أساسيان يتحتم على أجهزة تنفيذ القانون وخبراء الأدلة الجنائية جمعها واستخلاصها، وتعد المعاينة والتفتيش من بين الإجراءات التي تباشرها سلطات التحقيق والتي تؤدي للوصول إلى الدليل المستمد من الواقعة الإجرامية، عن طريق التنقيب عن الحقيقة من حيث ثبوت التهمة ونسبتها إلى المتهم من عدمه، وكل هذا سواء تعلق بالمجرم المعلوماتي أو التقليدي ما دام أن إجراءات الحصول على الدليل نفسها[٢].

أولاً: التفتيش والحجز على الأجهزة الرقمية:

يحق للجهات المعنية مثل النيابة العامة أو مأموري الضبط القضائي إجراء التفتيش على الأجهزة الرقمية في حالة الاشتباه بارتكاب جريمة، ويجب أن يتم ذلك وفقًا لإذن قضائي أو في حالات الطوارئ التي تقتضي التدخل السريع.

في الإذن القضائي: يتطلب القانون الحصول على إذن من المحكمة أو النيابة العامة قبل التفتيش والحجز على الأجهزة الرقمية، وذلك لضمان عدم المساس بالحقوق الشخصية [٣].

ثانياً: الحفاظ على سرية الأدلة الرقمية:

عند ضبط الأجهزة الرقمية مثل الحواسيب أو الهواتف المحمولة، يجب على الجهات المعنية اتخاذ التدابير اللازمة لحفظ الأدلة الرقمية من التلاعب أو التدمير، وتتمثل تلك الإجراءات في الآتي[٤]:

(١) بن قدوم سوهيل؛ وبسام لديدة، مرجع سابق، ص ٢١.
(٢) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٦.
(٣) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٦ – ٧.
(٤) بوحزمة نصيرة، مرجع سابق، ص ٢١٢ وما بعدها.

١. عدم فتح الأجهزة: يجب عدم التفاعل مع الجهاز أو فتح الملفات عليه إلا بحضور مختصين في التحقيق الرقمي.

٢. إجراء النسخ الاحتياطي: ينبغي أخذ نسخة من البيانات المخزنة على الأجهزة لضمان إمكانية استخدامها كدليل في المستقبل.

ثالثاً: التحقيق الرقمي والتفريغ:

بعد حجز الأجهزة الرقمية، يجب على فرق التحقيق الرقمي المتخصصة القيام بإجراءات تفريغ البيانات الرقمية، وتتم هذه الإجراءات بحذر وبدقة لضمان أن الأدلة لا تتعرض للتعديل أو التلف، وتتطلب مهارة التحليل الرقمي التي تتضمن فحص جميع الملفات والمعلومات المخزنة على الأجهزة لاستخراج الأدلة التي قد تكون ذات صلة بالقضية[١].

رابعاً: الاعتماد على الخبراء الفنيين:

في معظم الحالات، يكون من الضروري الاستعانة بالخبراء الفنيين المتخصصين في التحقيق الرقمي لضمان صحة الأدلة المستخلصة من الأجهزة، فهؤلاء الخبراء يجب أن يكونوا مؤهلين وقادرين على تقديم تقرير شامل وواضح للمحكمة حول كيفية استخراج الأدلة[٢].

خامساً: إجراءات التوثيق:

من المهم أن يتم توثيق كل خطوة من خطوات التحقيق الرقمي بدقة، بما في ذلك توقيت التفتيش، وحجز الأجهزة، وتحليل البيانات، وذلك لضمان أن هذه الأدلة يمكن تقديمها في المحكمة وتكون قابلة للإثبات. التوثيق يشمل أيضًا تصوير الأدلة الرقمية باستخدام أدوات موثوقة للحفاظ على صحتها[٣].

سادساً: الالتزام بالقواعد القانونية والشرعية في جمع الأدلة:

يجب أن يتم جمع الأدلة الرقمية بطريقة قانونية وشرعية بحيث لا يتم انتهاك حقوق

(١) للمزيد انظر: معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٦. عبد الباقي، مصطفى. مرجع سابق، ص ٢٨٨.
(٢) الحمداني، ميسون؛ والموسوي، علي. مرجع سابق، ص ٢١.
(٣) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٧.

المتهم أو التلاعب بالأدلة. يشمل ذلك احترام حقوق الخصوصية والأمن المعلوماتي[1].

سابعاً: عرض الأدلة في المحكمة:

عند تقديم الأدلة الرقمية في المحكمة، يجب أن تكون هذه الأدلة قابلة للفهم من قبل القاضي وأطراف الدعوى. وهذا يتطلب تحويل الأدلة إلى نسخ قابلة للعرض، كتحويل البيانات إلى مستندات نصية أو صور لعرضها أمام المحكمة، وكذا يتطلب الإجابة على استفسارات القاضي، إذ يمكن للخبير أو محامي الدفاع استجواب الخبراء حول الطريقة التي تم بها جمع وتحليل البيانات[2].

المبحث الثالث
موقف المشرع اليمني من التحقيق الرقمي

يواجه النظام القانوني اليمني تحديات في التعامل مع الجرائم الإلكترونية بسبب عدم وجود تشريع خاص ينظم الاستدلالات والتحقيق في هذه الجرائم وطرق إثباتها، وهذا القصور يؤدي إلى صعوبات في جمع الأدلة الرقمية وتقديمها أمام المحاكم، حيث يتطلب التحقيق الرقمي في الإثبات الجنائي باليمن تطويرًا تشريعيًا وتدريبًا متخصصًا لضمان فعالية مكافحة الجرائم الإلكترونية وحماية المجتمع.

وفي هذا المبحث نتناول موقف المشرع اليمني من تنظيم الأحكام الموضوعية والإجرائية للتحقيق الرقمي في الإثبات الجنائي، وذلك في المطلبين التاليين:

المطلب الأول
الأحكام الموضوعية في التحقيق الرقمي في الإثبات الجنائي

يُعَد التحقيق الرقمي جزءًا أساسيًا من عملية الإثبات الجنائي، خاصةً مع تزايد الجرائم الإلكترونية، وفي النظام القانوني اليمني على الرغم من عدم وجود تشريع خاص بالجرائم الإلكترونية في اليمن، إلا أن القوانين الحالية تُطبَّق على هذه الجرائم بقدر الإمكان.

---

(١) للمزيد انظر: فرغالي، عبد الناصر؛ والمسماري، محمد، مرجع سابق، ص ٥. واسخيطة، رضوان، مرجع سابق، ص ٤٦.

(٢) رستم، هشام فريد. (١٩٩٤م). الجوانب الإجرائية في الجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، مصر، ص. ٢٧ وما بعدها. وعرب، يونس، جرائم الكمبيوتر، مرجع سابق، ص ٣٧.

وفي هذا المطلب نتناول الأدوات والتقنيات الرقمية المنصوص عليها في التشريع اليمني في الفرع الأول، وقيمة الأدلة الرقمية في التشريع اليمني في الفرع الثاني، والتحديات والقصور التشريعي اليمني في مواجهة التحقيق الرقمي في الفرع الثالث، وذلك على النحو التالي:

الفرع الأول

الأدوات والتقنيات الرقمية المنصوص عليها في القانون اليمني

في سياق التوجه العالمي الجديد في الاعتراف الرسمي بمدى تحقيق المستخرجات الإلكترونية من ائتمان وموثوقية لتكون دليلاً كاملاً في الإثبات؛ أصدر المشرع اليمني القانون رقم (٤٠) لسنة ٢٠٠٦م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية.

ومن أهم الأدوات والتقنيات التي قد تستخدم كأدلة إثبات جنائية إلكترونية؛ أدوات وأنظمة المعاملات المنصوص عليها في قانون أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، في المادة (٤/أ): «يسري هذا القانون (أي قانون أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية) على جميع المعاملات التي تتناولها أحكامه وعلى وجه الخصوص ما يلي: ١. أنظمة الدفع الإلكترونية، وسائر العمليات المالية والمصرفية التي تنفذ بوسائل إلكترونية. ٢. رسائل البيانات والمعلومات الإلكترونية وتبادلها، والسجلات الإلكترونية. ٣. التوقيع الإلكتروني، والترميز والتوثيق الإلكتروني. ٤. المعاملات التي يتفق أطرافها صراحةً أوضمناً على تنفيذها بوسائل إلكترونية ما لم يرد فيه نص صريح يقضي بغير ذلك».

وقد عرفت المادة (٢) من هذا القانون، العقد الإلكتروني بأنه: «الاتفاق الذي يتم إبرامه بوسائل إلكترونية كلياً أو جزئياً».

والعقد الإلكتروني وفقاً للقانون يعد من قبيل السجلات الإلكترونية، التي اشترط لصحتها القانونية في المادة (١١) منه، فيما يلي:

أ- أن تكون البيانات والمعلومات الواردة في ذلك السجل قابلة للاحتفاظ بها وتخزينها بحيث يمكن في أي وقت الرجوع إليها.

ب- إمكانية الاحتفاظ بالسجل الإلكتروني بالشكل الذي تم به إنشاؤه أو إرساله أو تسلمه أو بأي شكل يسهل به إثبات دقة البيانات والمعلومات التي وردت فيه عند إنشائه أو إرساله أو تسلمه.

ج- دلالة البيانات والمعلومات الواردة في السجل على من ينشئه أو يتسلمه وتاريخ ووقت إرساله وتسلمه.

كما نصت المادة (٢/١١) على أنه: لا تطبق الشروط الواردة في الفقرة (١) من هذه المادة على المعلومات المرافقة للسجل التي يكون القصد منها تسهيل إرساله وتسلمه.

وأما حجية العقد الإلكتروني في الإثبات فقد حسم المشرع اليمني هذا الأمر، حيث جعل له من الحجية ما للعقد التقليدي من الحجية، وفق ما نصت عليه المادة (١٠) من قانون أنظمة الدفع والعمليات المالية والمصرفية الإلكتروني، التي نصت على أنه: «يكون للسجل الإلكتروني والعقد الإلكتروني ورسالة البيانات والمعلومات الإلكترونية والتوقيع الإلكتروني نفس الآثار القانونية على الوثائق والمستندات والتوقيعات الخطية، من حيث إلزامها لأطرافها أو حجيتها في الإثبات».

وكذلك الأمر بالنسبة للسجل الإلكتروني، فهو يتمتع بالحجية التي يتمتع بها السجل العادي، وفق ما نصت عليه المادة (١٠) من قانون أنظمة الدفع والعمليات المالية والمصرفية الإلكتروني، التي نصت على أنه: «يكون للسجل الإلكتروني والعقد الإلكتروني ورسالة البيانات والمعلومات الإلكترونية والتوقيع الإلكتروني نفس الآثار القانونية على الوثائق والمستندات والتوقيعات الخطية، من حيث إلزامها لأطرافها أو حجيتها في الإثبات».

إضافة إلى ذلك بينت المادة (٢/١٣) من القانون، آلية إثبات صحة التوقيع الإلكتروني ونسبته إلى صاحبه، حيث نصت على: «يتم إثبات صحة التوقيع الإلكتروني ونسبته إلى صاحبه إذا توافرت طريقة لتحديد هويته والدلالة على موافقته على المعلومات الواردة في السجل الإلكتروني الذي يحمل توقيعه إذا كانت تلك الطريقة مما يعول عليها لهذه الغاية في ضوء الظروف المتعلقة بالمعاملة بما في ذلك اتفاق الأطراف على استخدام تلك الطريقة».

وعرف المشرع اليمني التوقيع الإلكتروني أيضاً في المادة (٢/ف٨) من قانون أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية؛ بأنه: «عبارة عن جزء مشفر في رسالة البيانات أو مضاف إليها أو مرتبط بها، ويتخذ هيئة حرف أو أرقام أو رموز أو إشارات أو غيرها، ويكون مرتبطاً بشكل إلكتروني أو رقمي أو ضوئي، أو أي وسيلة أخرى مماثلة، بحيث يمكن من خلاله التعرف على المنشئ وتمييزه وتحديد هويته والتأكيد على موافقته على محتوياتها».

ومن حيث حجية التوقيع الإلكتروني، فقد حسم المشرع اليمني الأمر، حيث جعل له من الحجية ما للتوقيع التقليدي من الحجية، وفق ما نصت عليه المادة (١٠) من قانون

أنظمة الدفع والعمليات المالية والمصرفية الإلكتروني، التي نصت على أنه: «يكون للسجل الإلكتروني والعقد الإلكتروني ورسالة البيانات والمعلومات الإلكترونية والتوقيع الإلكتروني نفس الآثار القانونية على الوثائق والمستندات والتوقيعات الخطية، من حيث إلزامها لأطرافها أو حجيتها في الإثبات».

كما عرفت المادة (٢) من قانون أنظمة الدفع، رسالة المعلومات، بأنها: «عبارة عن بيانات تمت معالجتها بواسطة نظام معالجة المعلومات فأخذت شكلاً مفهوماً...». كما عرفت هذه المادة الوسيط الإلكتروني بأنه: برنامج الحاسب الآلي أو أي وسيلة إلكترونية أخرى تستعمل من أجل تنفيذ إجراء أو الاستجابة لإجراء بقصد إنشاء أو إرسال أو تسلم رسالة البيانات...».

وأما بالنسبة لحجيتها وآثارها، فهي تتمتع بذات الحجية والآثار القانونية التي تتمتع بها الوثائق والمستندات والتوقيعات الخطية، من حيث إلزامها لأطرافها وحجيتها في الإثبات. مادة (١٠) من قانون أنظمة الدفع.

الفرع الثاني

قيمة الأدلة الرقمية في التشريع اليمني

تختلف نظم الإثبات أو طريقة الاعتراف بالدليل الرقمي وقبوله كدليل إثبات من دولة إلى أخرى بحسب طبيعة نظام الإثبات السائد فيها، والذي لا يمكن أن يخرج عن الأنظمة التالية:

أولاً: نظام الإثبات الحر:

وفقاً لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة في شأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلة للاستناد إليها في تكوين قناعته، فله أن يبني هذه القناعة على أي دليل وإن لم يكن منصوصاً عليه، وكل الأدلة تتساوى قيمتها في الإثبات في نظر المشرع، والقاضي هو الذي يختار من بين ما يطرح عليه ما يراه صالحاً للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا لم يقتنع به[١].

(١) عز الدين بن أمين الأموي. (٢٠٢٤). القيمة القانونية والقضائية للأدلة الرقمية طبقاً للقانون اليمني. تم الاسترداد من القضائية – عدن:
utm-source=chatgpt.com&٢٩٩٩=https://alqadaeya-ye.net/?p

ثانياً: نظام الأدلة القانونية أو المقيد:

في ظل هذا النظام لا يكون الدليل الرقمي مقبولاً أمام القاضي الجنائي ما لم يتم النص عليه من قبل المشرع، حيث يتوجب عليه تحديد هذا النوع من الأدلة سلفاً وبدقة، والقاضي الجنائي يتوجب عليه الأخذ بهذه الأدلة متى توافرت فيها شروط الدليل الصحيح، لذلك ففي حالة توافر شروط الدليل الصحيح يلزم القاضي الجنائي أن يؤسس حكمه على أساس هذا الدليل حتى وإن لم يكن مقتنعاً به، كما أنه إذا لم تتوافر الشروط المطلوبة قانوناً يكون القاضي ملزماً ببناء اقتناعه وتأسيس حكمه على أساس عدم قيام الدليل على الادعاء، حتى لو كان القاضي مقتنعاً بثبوت الادعاء.

ثالثاً: نظام الإثبات المختلط:

تقوم فكرة هذا النظام أنه يأخذ بملامح كل من نظام أدلة الإثبات الحر ونظام الأدلة القانونية وحاول التوفيق بينهما، فلكي يتسنى للقاضي إصدار حكمه ينبغي عليه أن يكون مقتنعًا اقتناعاً شخصيًا، وفي نفس الوقت يجوز القناعة القانونية كما أقرها القانون، ويقوم هذا النظام بالجمع بين النظامين، وذلك عن طريق تحديد القانون لأدلة معينة للإثبات في بعض الجرائم دون البعض الآخر أو يشترط في الدليل شروطاً في بعض الأحوال أو يعطي القاضي الحرية في تقدير القيمة الإثباتية للأدلة القانونية.

رابعاً: موقف المشرع والقضاء اليمني:

يمكن للقاضي الجنائي اليمني- بخلاف القاضي المدني- أن يلعب دوراً إيجابياً في استثمار مبدأ الإثبات الحر، ولاسيما إذا اتخذ المبادرة في البحث عن الوسائل الناجعة التي تؤدي به إلى إظهار الحقيقة، ففي ظل القانون اليمني لا وجود لأدلة يحظر المشرع مقدماً على القاضي الجنائي قبولها، وكل دليل يمكن أن يتولد معه اقتناعه، يكون من حيث المبدأ مقبولاً أمامه، فحرية الإثبات في الميدان الجنائي تبقى ضرورية ومنطقية في آن واحد، إذ أن الأصل العام هو أن الجرائم على اختلاف أنواعها يجوز إثباتها بكافة الطرق القانونية، ما عدا ما استثني منها بنص خاص في القانون.

وفي التشريع اليمني نصت المادة (٣٢١) من قانون الإجراءات الجزائية النافذ على: «...٢- تقدير الأدلة يكون وفقاً لاقتناع المحكمة في ضوء مبدأ تكامل الأدلة فلا يتمتع دليل بقوة مسبقة في الإثبات».

ونصت المادة (٣٢٢) على أنه: «لا يجوز إثبات أي واقعة ترتب مسؤولية جزائية على

أي شخص إلا عن طريق الأدلة الجائزة قانوناً وبالإجراءات المقررة قانونا».

وبالنظر إلى المادة ٣٢٣ من نفس القانون، نجد أنه جاء في صدر المادة: «تعد من أدلة الإثبات...» وجاء في نهايتها عبارة: «أو وقائع الجريمة والقرائن والأدلة الأخرى»، مما يتبين لنا أن المشرع اليمني لم يحصر أدلة الإثبات الجنائي بل ذكرها على سبيل المثال.

وتنص المادة (٣٦٧) من نفس القانون على أنه: «يحكم القاضي في الدعوى بمقتضى العقيدة التي تكونت لدية بكامل حريته من خلال المحاكمة».

إذا ومن خلال نصوص المواد المذكورة يتضح جلياً بأن المشرع اليمني لم يحصر أدلة الإثبات بأدلة معينة، بل ترك حرية الإثبات للخصوم في الدعوى، وكذلك للقاضي كمبدأ عام في الاثبات، وعمد إلى تحديد بعض طرق الإثبات في جرائم معينة فقط دون البعض الآخر ويتعلق الأمر بجرائم الحدود والقصاص. لقد جعل المشرع للقاضي دوراً في تقدير الأدلة وفي التحرك الذاتي والاقتناع الموصل إلى الحكم العادل والحسم السريع، مما يمكن معه القول أن القانون اليمني تبنى نظام الإثبات المختلط، كما أن في عمومية نصوص الإثبات الجنائي الواردة أعلاه تستوعب الإثبات بالأدلة الرقمية، شريطة أن يتم استخلاصها بطرق مشروعة، والتي تنتهي بقناعة القاضي بها.

وما يعزز توجه المشرع اليمني للأخذ بالأدلة الرقمية ما أخذ به قانون أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية رقم (٤٠) لسنة ٢٠٠٦، حيث تنص المادة (٤١) على أنه: «يعاقب كل من يرتكب فعلاً يشكل جريمةً بموجب أحكام القوانين النافذة بواسطة استخدام الوسائل الإلكترونية...».

وهكذا فإن الإثبات الجنائي في اليمن يسيطر عليه مبدأ حرية الإثبات في المواد الجنائية- مع الإشارة إلى تحديده لبعض طرق الإثبات في جرائم معينة- ولا فرق بين دليل نجم عن إجراء علمي أم غيره، والقاضي يستطيع أن يستمد من أي دليل يرتاح له وجدانه، وهذه الحرية مقررة بالنظر إلى ظروف وملابسات القضية.

وبتحليل موقف المشرع اليمني من خلال النصوص المذكورة أعلاه نجدها تكرس قاعدتين تكمل إحداهما الأخرى، قاعدة الاقتناع الحر للقاضي الجنائي من جهة، وقاعدة حرية اختيار وسائل الإثبات الجنائي من جهة أخرى.

ونشير إلى أنه تظهر أهمية الإثبات الجنائي في الدور الإيجابي الممنوح للقاضي في البحث عن الحقيقة، فالقاضي الجنائي لا يكتفي بمجرد موازنة الأدلة التي يقدمها الخصوم

والترجيح بينهما، إنما له دور إيجابي يفرض عليه التحري والبحث عن الحقيقة والكشف عنها، كما تكمن أهميته في أنه يتطلب في الحصول على الدليل اتباع القواعد التي تحدد كيفية الحصول عليه، والشروط التي يتعين عليه تطبيقها فيه والتي توفر الثقة في الدليل الذي يقدمه، ومخالفة هذه القواعد والشروط قد تهدر الدليل ويشوب الحكم البطلان.

إذا يملك القاضي سلطة تقديرية واسعة، فإذا ما طرحت عليه مجموعة من الأدلة يوازي بينها مفضلاً بعضها على البعض الآخر ويأخذ من بينها ما يطمئن إليه، ويطرح ما سواه مما لم يطمئن إليه، وما يمكن أن نخلص إليه في الأخير أن الأدلة الرقمية بمختلف نظم الإثبات لها الحجية والقيمة القانونية، حيث قبلت الأنظمة الثلاثة الأدلة الرقمية كأدلة إثبات، إلا أنها في نظام الأدلة القانونية تتطلب شروطاً عديدة لقبولها.

الفرع الثالث

التحديات الموضوعية في مواجهة التحقيق الرقمي

على الرغم من انتشار الجرائم الإلكترونية في المجتمع اليمني في الآونة الأخيرة بشكل كبير، إلا أنه لا يوجد حتى اللحظة - ضمن المنظومة التشريعية اليمنية - أي قانون خاص بالجرائم الإلكترونية، حيث لم يواكب المشرع اليمني المتغيرات التكنولوجية[1]، مع أن غالبية الدول العربية بادرت بإصدار قوانين خاصة بالجرائم الإلكترونية، منها: قانون الجرائم الإلكترونية الفلسطيني رقم (١٧) لسنة ٢٠١٧م/ وقانون جرائم أنظمة المعلومات الأردني رقم (٣٠) لسنة ٢٠١٠م.

كما يوجد عدد من الاتفاقيات الدولية والإقليمية بهذا الشأن منها: معاهدة مجلس أوروبا لمكافحة الجرائم الإلكترونية «معاهدة بودابست» لسنة ٢٠٠١م، والاتفاقية العربية لمكافحة جرائم المعلوماتية لسنة ٢٠١٠م (اليمن وقع عليها - ٢٠١٠/١٢م - ولم يصادق عليها بعد).

الأمر الذي يشكل تحدياً أمام الجهات الأمنية التي كانت منهكة في متابعة الجرائم التقليدية على مدار الأعوام الماضية[2].

---

(١) عدا وجود قانون خاص بأنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، الصادر برقم (٤٠) لسنة ٢٠٠٦م، المنشور في الجريدة الرسمية العدد الرابع والعشرون الصادر بتاريخ ١١/ ذي الحجة/١٤٢٧هـ الموافق ٣١ / ديسمبر/٢٠٠٦م. ونطاق سريانه مقصور على: جميع المعاملات التي تتناولها أحكامه، كالعمليات المالية والمصرفية التي تنفذ بوسائل إلكترونية، ورسائل البيانات والمعلومات الإلكترونية وتبادلها والسجلات الإلكترونية، المتصلة بالمصارف.

(٢) تحقيق صحفي حول الورقة المقدمة في المؤتمر الوطني الأول في اليمن بعنوان: «مخاطر الجريمة

وفي هذا الشأن أقيمت في الآونة الأخيرة العديد من المؤتمرات والندوات العلمية حول مخاطر الجرائم الإلكترونية في المجتمع اليمني، منها: المؤتمر العلمي الأول للأمن السيبراني، الذي عقدته وزارة الاتصالات وتقنية المعلومات بتاريخ: ٧-٩/ يونيو/ ٢٠٢١م[١].

وكذا الندوة التي عقدتها الأمانة العامة بمجلس الشورى بالتعاون مع عدد من الجهات ذات العلاقة، في تاريخ: ١٦ يوليو ٢٠٢٤م، بعنوان: «مخاطر الجرائم الإلكترونية في المجتمع اليمني»[٢]، التي خرجت جميعها بعدد من التوصيات والمعالجات المقترحة للحد من الجريمة الإلكترونية، منها سرعة إصدار التشريعات اللازمة والقوانين الرادعة، والاهتمام بأمن المعلومات (الأمن السيبراني) عند بناء الأنظمة في المؤسسات، وبناء وتحديث إدارة مكافحة الجرائم الإلكترونية وتجهيزها بالمواد التقنية والفنية والتأهيلية والتشغيلية للازمة، وتكثيف التوعية الأمنية ضد الجريمة الإلكترونية في مراحل التعليم المختلفة.

وبالتالي فإنه يتوجب على السلطات المختصة التعجيل بإصدار قانون خاص بشأن الجرائم الإلكترونية؛ لمسايرة التطورات الراهنة أولا، ومواجهة التحديات التي تواجه المجتمع اليمني بشأن انتشار الجرائم الإلكترونية.

الإلكترونية وأضرارها على الفرد والمجتمع» للعقيد أحمد يحيى السراجي. (٧-٩/ يونيو/ ٢٠٢١م). « صحيفة الثورة، العدد (٢٠٧٣٣)، تاريخ الأربعاء ١٧ محرم ١٤٤٣هـ الموافق ٢٥ أغسطس ٢٠٢١م.

(١) للمزيد راجع: السراجي، أحمد يحيى. (٧-٩/ يونيو/ ٢٠٢١م). مخاطر الجريمة الإلكترونية وأضرارها على الفرد والمجتمع، المؤتمر العلمي الأول للأمن السيبراني، وزارة الاتصالات وتقنية المعلومات، اليمن. وتحقيق صحفي حول الورقة المقدمة في المؤتمر الوطني الأول في اليمن، صحيفة الثورة، العدد (٢٠٧٣٣)، تاريخ الأربعاء ١٧ محرم ١٤٤٣هـ الموافق ٢٥ أغسطس ٢٠٢١م.

(٢) ناقشت الندوة ست أوراق عمل، تمحورت الأولى حول واقع الجريمة الالكترونية في اليمن قدمها عن مجلس الشورى الدكتور فهمي النعامي، أشار فيها إلى أن نسبة انتشار الجريمة الإلكترونية في المجتمع اليمني بلغت ٤٧ بالمائة وفقاً للدراسة المسحية المنفذة.. لافتاً إلى أهمية حل إشكالية تداخل الصلاحيات بين الجهات ذات العلاقة والتي حالت دون إصدار مشروع قانون مكافحة جرائم تقنية المعلومات. للمزيد راجع: مخاطر الجرائم الإلكترونية في المجتمع اليمني، ندوة علمية عقدتها الأمانة العامة بمجلس الشورى بالتعاون مع عدد من الجهات ذات العلاقة، بتاريخ: الثلاثاء، ١٠ محرم ١٤٤٦هـ الموافق ١٦ يوليو ٢٠٢٤م. متوفرة على الرابط التالي: https://www.saba.ye/ar/news٣٣٤٩٥٣٨

المطلب الثاني

الأحكام الإجرائية في التحقيق الرقمي في الإثبات الجنائي

يقصد بالأحكام الإجرائية للتحقيق الرقمي في الإثبات الجنائي اليمني: «القواعد والضوابط التي يجب اتباعها خلال التحقيقات الجنائية التي تشمل الأدلة الرقمية».

وفي هذا المطلب نسلط الضوء على الأحكام الإجرائية للتحقيق الرقمي في الإثبات الجنائي اليمني، من خلال بيان قواعد الاختصاص القضائي اليمني في التحقيق الرقمي في الفرع الأول، وإجراءات التحقيق الرقمي في الفرع الثاني، والتحديات الإجرائية في مواجهة التحقيق الرقمي في الفرع الثالث، وذلك على النحو التالي:

الفرع الأول

قواعد الاختصاص القضائي اليمني في التحقيق الرقمي

نظم المشرع اليمني القواعد العامة للاختصاص القضائي في نظر الجرائم، ضمن الكتاب الثالث (في المحاكمة)، الباب الأول (اختصاص المحاكم)، الفصل الأول والثاني والثالث، ضمن المواد من (٢٣١) إلى (٢٥٠)، حيث تنطبق هذه الأحكام على جميع الجرائم سواء كانت تقليدية أو إلكترونية، وفيما يلي نتناول أهم تلك القواعد:

١. قواعد الاختصاص النوعي:

نصت المادة (٢٣١) إجراءات جزائية على اختصاص المحاكم الابتدائية بالفصل في جميع الجرائم التي تقع في دائرة اختصاصها المحلي.

وتختص محاكم الاستئناف بالفصل في استئناف الأحكام والقرارات الصادرة من المحاكم الابتدائية الواقعة في دائرة اختصاصها. المادة (٢٣٢) إجراءات.

وتختص المحكمة العليا بالفصل في الطعون بالنقض في الأحكام والقرارات الصادرة من محاكم الاستئناف والأحكام والقرارات النهائية الصادرة من المحاكم الابتدائية في الأحوال التي يحددها القانون. مادة (٢٣٣).

٢. الاختصاص المحلي (المكاني):

نصت المادة (١/٢٣٤) إجراءات على انه يتعين الاختصاص محلياً بالمكان الذي وقعت فيه الجريمة أو المكان الذي يقيم فيه المتهم أو المكان الذي يقبض عليه فيه،

ويثبت الاختصاص للمحكمة التي رفعت فيها الدعوى أولاً. وفي حالة الشروع تعد الجريمة مرتكبة في كل محل وقع فيه عمل من أعمال البدء في التنفيذ، وفي الجرائم المتتابعة ومتعددة الأفعال يعتبر مكاناً للجريمة كل محل يقع فيه أحد الأفعال الداخلة فيها، وفي الجرائم المستمرة يعتبر مكاناً للجريمة كل محل تقوم فيه حالة الاستمرار. مادة (٢٣٥) إجراءات.

٣. الاختصاص في الجرائم المرتكبة خارج الإقليم:

نصت المادة (١/٢٣٦) إجراءات على أنه إذا وقعت جريمة في الخارج مما يسري عليها أحكام القانون اليمني ولم يكن لمرتكبها محل إقامة معروف في الجمهورية ولم يضبط فيها، ترفع عليه الدعوى الجزائية أمام محاكم العاصمة. أما إذا ارتكبت الجريمة جزئياً خارج الجمهورية وجزئياً داخلها اختصت محلياً المحكمة الواقع في دائرتها مكان ارتكاب أفعال الجريمة داخل الجمهورية.

٤. الاختصاص بالجرائم التي تقع على السفن والطائرات والجرائم التي تقع خارج الإقليم:

نصت المادة (٢٤٤) إجراءات على اختصاص المحاكم اليمنية بالفصل في الجرائم التي تقع في عرض البحر على متن بواخر تحمل العلم اليمني أياً كانت جنسية مرتكبي هذه الجريمة وفي الجرائم التي تقع على متن باخرة تجارية أجنبية متى كان وجودها داخل ميناء بحري يمني أو المياه الإقليمية اليمنية ينعقد الاختصاص لمحكمة أول ميناء يمني ترسو فيه الباخرة.

كما نصت المادة (٢٤٥) على اختصاص المحاكم اليمنية بالفصل في الجرائم التي تقع على متن الطائرات اليمنية أياً كانت جنسية مقترف الجريمة، كما تختص بالفصل بالجرائم التي تقع على متن طائرات أجنبية إذا كان الجاني أو المجني عليه يمني الجنسية، وإذا هبطت طائرة في اليمن بعد وقوع الجريمة وينعقد الاختصاص عندئذ للمحكمة التي يقع في دائرتها مكان هبوط الطائرة إن ألقي القبض عليه وقت الهبوط أو للمحكمة التي ألقي القبض على المتهم في دائرتها إذا تم القبض في اليمن أما إذا قبض على المتهم خارج إقليم الدولة فيجوز للمحاكم اليمنية أن تنظر الدعوى.

كما تختص أيضاً المحاكم اليمنية بمحاكمة كل يمني ارتكب خارج إقليم الدولة فعلاً يعد بمقتضى القانون جريمة إذا عاد إلى الجمهورية وكان الفعل معاقباً عليه بمقتضى قانون الدولة الذي ارتكبت فيه. مادة (٢٤٦) إجراءات.

وتختص المحاكم اليمنية أيضاً بمحاكمة كل يمني ارتكب خارج إقليم الدولة جريمة مخلة بأمن الدولة مما نص عليه في (الباب الأول من الكتاب الثاني) من قانون العقوبات أو جريمة تقليد أو تزييف أختام الدولة أو إحدى الهيئات العامة أو تزوير عمله وطنية متداولة قانوناً أو إخراجها أو ترويجها أو حيازتها بقصد الترويج أو التعامل بها. مادة (٢٤٧) إجراءات.

وعليه ينبغي على السلطات القضائية أن تتثبت قبل كل شيء من مدى دخول النظر في الدعوى ومن ضمنها التحقيق فيها على الصعيد الدولي ضمن ولايتها كقضاء وطني، فإذا ظهر لها عدم ولايتها من الناحية الدولية فلا يجوز لها النظر في الدعوى ولا التحقيق فيها، ومثل هذا الأمر وارد كثيراً في مجال التحقيق في الجرائم الإلكترونية باعتبارها من الجرائم العابرة للدول والقارات[١].

الفرع الثاني
إجراءات التحقيق الرقمي

أولاً: إجراءات المعاينة والتفتيش في التحقيق الرقمي:

١. المعاينة في التحقيق الرقمي:

تعتبر المعاينة من أهم إجراءات التحقيق والتي يمكن من خلالها الحصول على الدليل الجنائي بحيث يجوز للنيابة العامة أن تقوم به في غيبة المتهم إذا لم يتيسر له حضوره[٢]، وفي هذا البند سنتناول بإيجاز المعاينة من حيث ماهيتها وأهميتها والسلطة المختصة بها وشروط صحتها، وذلك على النحو التالي:

أ- تعريف المعاينة وأهميتها:

يقصد بالمعاينة الانتقال إلى الأماكن التي وقعت فيها الجريمة لإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن الجريمة وعن مرتكبها.

المعاينة كإجراء تحقيق أو استدلال، يستهدف إلى إظهار الحقيقة في واقعة يبلغ أمرها إلى السلطات المختصة، بحيث لا تتوقف طبيعتها على صفة من يجريها، بل على ما يقتضيه إجراؤها من مساس بحقوق الأشخاص[٣].

(١) بوحزمة نصيرة، مرجع سابق، ص ٢١٢.
(٢) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٧.
(٣) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٧.

ب- أهمية المعاينة في الجرائم الإلكترونية:

تظهر أهمية المعاينة في كونها تقوم بإحاطة صورة شاملة لموقع الجريمة لجهة التحقيق والمحاكمة، وبكل ما يحتويه من تفصيلات سواء تعلقت بمكانه أو وصفه من الداخل أو الآثار الموجودة به، وهذا حتى يتسنى لضباط الشرطة القضائية والقضاة وضع تصور لكيفية وقوع الجريمة واستخلاص بعض الأدلة من المادة التي تم جمعها[١].

وباعتبار المعاينة من أهم إجراءات التحقيق الجنائي فإن أهميتها تتجسد سواء من الناحية القانونية أو العملية، فمن الناحية القانونية تبدو أهميتها من عدة اتجاهات منها تأكيد وقوع الجريمة أو نفيها، صدق أقوال الواقعة، ركن الخطأ أو العمد فيها، تحديد الوصف القانوني لها، كما تساعد القاضي في تكوين قناعته؛ أما من الناحية العملية فهي تساعد المحقق على تحديد وقت ارتكاب الواقعة الإجرامية، ومعرفة علاقة الجاني بالمجني عليه، وتحديد الأسلوب الإجرامي الذي استعان به الجاني[٢].

والمعاينة في مجال كشف غموض الجريمة الإلكترونية لا تتمتع بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية[٣]، ومرد ذلك أن هناك تقريباً مسرحاً للجريمة التقليدية، والتي يتمكن من خلالها الباحث والمحقق الجنائي التنقيب عن الواقعة عن طريق معاينة الآثار المادية التي خلفها ارتكاب الجريمة والتحفظ على الأشياء التي لها علاقة بالواقعة الإجرامية، بينما لا يوجد عادة مسرح للجريمة المعلوماتية باعتبار مكان الإغارة هو العالم الافتراضي أو عالم الفضاء الإلكتروني Cyber Space والذي يكون عادة الموقع أو المكتب الذي توجد فيه مكونات الحاسب الآلي المادية والمعنوية، والتي تكون محلاً للجريمة أو أدلتها وهي تتمثل في الأجهزة والأنظمة والبرامج[٤].

فالانتقال للمعاينة في الجريمة المعلوماتية لا يكون إلى العالم المادي، بل إلى العالم الافتراضي، حيث تقل فرص الإفصاح والكشف عن الحقيقة المراد التوصل إليها من وراء معاينة الجريمة المعلوماتية لأسباب عدة منها[٥]:

---

(١) خالد ممدوح، مرجع سابق، ص ١٥٠.

(٢) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٧.

(٣) خالد ممدوح إبراهيم، خالد، مرجع سابق، ص ١٥٣.

(٤) هبه هروال، نبيلة. الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، ٢٠٠٧، ص ٢١٧.

(٥) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٩.

- أن الجرائم التي تقع على نظم المعلوماتية والشبكات أو بواسطتها قلَّما ينجم عن ارتكابها آثار مادية.
- أن عدداً كبيراً من الأفراد يكونون قد ترددوا على مسرح الجريمة خلال الفترة التي تتوسط عادة بين ارتكاب الجريمة واكتشافها وهذا ما يفتح المجال لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو محو بعضها وهو ما يثير الشك على الدليل المستنبط من المعاينة[1].
- استطاعة الجاني التلاعب في البيانات عن بعد أو محوها عن طريق قيام الجاني بالتدخل من خلال وحدة طرفية.

ج- السلطة المختصة بإجراء المعاينة لمسرح الجريمة الإلكترونية:

الأصل أن انتقال المحقق الجنائي لإجراء المعاينة أو لمباشرة أي إجراء آخر من إجراءات التحقيق أمر متروك للسلطة التقديرية له، فلا يقوم به إلا إذا كانت هناك مصلحة من ورائه، لذلك جرى أن المعاينة هي من إجراءات التحقيق التي يترك أمر تقدير لزوم القيام بها إلى السلطة التي تباشر التحقيق[2].

وهذا ما نصت عليه المادة (١٣٠) من قانون الإجراءات الجزائية، بقولها: «ينتقل المحقق إلى محل الحادث أو إلى أي مكان لمعاينته كلما رأى ذلك مفيداً للتحقيق لإثبات حالة الأماكن والأشياء والأشخاص ووجود الجريمة مادياً وآثارها وكل ما يلزم إثبات حالته وله استدعاء الخبراء لإجراء المعاينة ويحرر محضراً بالمعاينة يكون صورة كاملة ومطابقاً للشيء محل المعاينة ويجوز لهذا الغرض تكملة المحضر عن طريق الصور الفوتوغرافية والرسوم».

ويتم إجراء معاينة الجريمة الإلكترونية المرتكبة كأي جريمة أخرى، عن طريق الانتقال إلى مكان الجريمة، غير أن الانتقال لا يكون إلى العالم المادي وإنما إلى الفضاء الإلكتروني، وبالتالي يتم الانتقال إلى العالم الافتراضي لمعاينة الجريمة من قبل المحقق.

يتولى المحقق معاينة الآثار التي خلفها مستخدم شبكة الإنترنت والتي تتمثل في الرسائل المرسلة منه أو التي يستقبلها وكل الاتصالات التي قام بها من خلال الكمبيوتر والشبكة العالمية، وكما أن الآثار الرقمية المستمدة من أجهزة الكمبيوتر قد تكون ثرية

(١) حسين على محمود، عبدالله. سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، ٢٠٠١م، ص ٢٦٥.

(٢) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٩.

فيما تحتويه من معلومات مثل صفحات المواقع Web pages، والبريد الإلكتروني Email، والملفات المخزنة في الكمبيوتر الشخصي files stared ...إلخ.

ومعظم التشريعات الجنائية الحديثة لم تهتم بتعريف مسرح الجريمة ولم تقم بتحديد النطاق المكاني له كما هو الحال بالنسبة للتفتيش، وبالتالي فإن معظم التشريعات تعبر عنه بمحل الحادث أو إلى أي مكان لمعاينته، مادة (١٣٠) إجراءات جزائية.

ولا توجد صعوبة مادية لتقرير صلاحية مسرح الجريمة المعلوماتية الذي يضم المكونات المادية، كأشرطة الحاسب، مفاتيح التشغيل، والأقراص وغيرها لمعاينتها من طرف المحقق، وكذا وضع الأختام في الأماكن التي تمت معاينتها، وضبط كل ما استعمل في ارتكاب الجريمة والتحفظ عليها، وفقاً لنص المادة (١٤٥) إجراءات: «لأعضاء النيابة أن يضعوا الأختام على الأماكن التي بها آثار أو أشياء تفيد في كشف الحقيقة ولهم أن يقيموا حراساً عليها وإذا قام بذلك أحد مأموري الضبط القضائي وجب عليه إخطار النيابة العامة فوراً».

د- شروط صحة معاينة مسرح الجرائم الإلكترونية:

حتى تحقق المعاينة الغرض المرجو منها في كشف غموض الحادث ومعرفة الفاعل يجب التقيد بعدة شروط[١]:

١. سرعة الانتقال إلى مكان وقوع الجريمة المعلوماتية، على السلطة المختصة بالتحقيق الانتقال فور وصول خبر وقوع الجريمة إلى علمها إلى مكان الواقعة[٢].

٢. السيطرة والتحكم على مكان وقوع الجريمة المعلوماتية، عند وصول سلطة التحقيق لمكان الحادث لمعاينته ويجب أن تقوم بالسيطرة عليه وذلك:

- بمنع أي شخص من مبارحة مكان الواقعة ريثما تنتهي الضبطية القضائية من تحرياتها[٣].
- منع تواجد أي شخص بداخل مسرح الجريمة حتى لا يؤدي إلى تغيير الآثار والأدلة المستمدة من الواقعة سواء بقصد أو بخطأ.
- حماية كل ما له علاقة بالحادث من وسائل وأشياء وأشخاص.
- قيام الخبراء كل حسب اختصاصه برفع الآثار بمسرح الجريمة.

(١) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ١٠.
(٢) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ١٠.
(٣) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ١٠.

٣. الترتيب في المعاينة، ولضمان إجراء معاينة بصورة مرتبة ومتسلسلة ينبغي على السلطة المختصة الالتزام بالطرق التالية:

- تحديد نقاط البدء في المعاينة.
- عدم الانتقال من مكان لآخر إلا بعد التأكد من معاينته تماماً[١].

٤. الدقة والعناية الفائقة في معاينة مسرح الجرائم المعلوماتية، وذلك بوصف المنطقة التي ارتكبت فيه الجريمة، وإذا كانت هذه الأخيرة داخل مبنى فيجب معاينة كل منافذ الدخول والخروج، وكذا وصف المحتويات فيما هو مرتبط بالجريمة، كأجهزة الكمبيوتر والماسح الضوئي (السكانر والطابعة) والأسطوانات المدمجة، وغير ذلك من الوسائل المستخدمة في اقتراف الجريمة المعلوماتية.

٥. التحفظ على مسرح الجرائم المعلوماتية بعد المعاينة، لأن الهدف من الحفاظ على آثار الجريمة بعد الانتهاء من المعاينة هو من أجل إمكانية العودة إليه كلّما أراد المحقق أو القاضي كشف غموض أو التأكد من آثار معينة.

٦. تدوين المعاينة، ويكون ذلك كتابياً ورسمياً وتصويرياً.

١. التفتيش في التحقيق الرقمي:

يعتبر إجراء التفتيش من أخطر الحقوق الممنوحة للمحقق، كونه يمس بالحريات التي تكفلها وتصونها الدساتير والقوانين، وقد نظم المشرع اليمني أحكامها الخاصة في قانون الإجراءات ضمن الباب الثالث (في التحقيق)، الفصل الثالث (في التفتيش وضبط الأشياء والتصرف فيها)، ضمن المواد من (١٣١ - ١٦٤)، حيث نصت المادة (١٣١) على: للأشخاص والمساكن والمراسلات البريدية والمحادثات السلكية واللاسلكية والمحادثات الشخصية حرمة. كما نصت المادة (١٣٢) على أنه: لا يجوز تفتيش الأشخاص أو دخول المساكن أو الاطلاع على المراسلات البريدية أو تسجيل المحادثات السلكية أو اللاسلكية أو الشخصية وكذا ضبط الأشياء إلا بأمر من النيابة العامة أثناء التحقيق ومن القاضي أثناء المحاكمة».

وفي هذا البند سنتناول بإيجاز ماهية التفتيش وخصائصه ومدى قابلية جرائم الحاسوب والشبكات الإلكترونية للتفتيش عن أدلتها، وشروط تفتيش الجرائم الإلكترونية، وذلك على النحو التالي:

(١) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ١٠.

أ- تعريف التفتيش:

لا يختلف معنى التفتيش في الجريمة التقليدية عن الجريمة المعلوماتية، وبالتالي يقصد به إجراء من إجراءات التحقيق الذي يهدف الوصول إلى أدلة تفيد إظهار الحقيقة وإسنادها إلى المتهم المنسوبة إليه التهمة، حيث تباشر السلطة المختصة بالدخول إلى نظم المعالجة الآلية للمعطيات بما تحتويه من مدخلات وتخزين ومخرجات، وذلك من أجل البحث عن الأفعال والسلوكيات المرتكبة وغير المشروعة[١].

ب- خصائص التفتيش:

يتميز التفتيش بناء على التعريف السالف الذكر بعدة خصائص[٢]:

- أنه إجراء من إجراءات التحقيق: يعتبر التفتيش من أوامر التحقيق الابتدائي والذي يدخل ضمن الاختصاصات العادية لقاضي التحقيق وهذا ما قضت به نص المادة (١٥٠) إجراءات جزائية.
- إن الهدف من التفتيش هو الوصول إلى الأدلة المادية للجريمة والتي تؤثر في اقتناع القاضي لأنه في الغالب يترك الجاني في مسرح الجريمة بعض الوسائل والأدوات التي يكون قد استخدمها في ارتكاب الجريمة، أو بصمات الأصبع إلى غير ذلك من الأدلة التي يستعين القاضي بها في الإثبات.
- أن يقع التفتيش على محل يتمتع بحرمة المسكن أو الشخص: يقع التفتيش على حرمة المسكن أو الشخص، ذلك أن قيام ضابط الشرطة القضائية بالبحث والتحري في الطرق العامة أو في الغابات...الخ، لا يعد تفتيشاً لانتفاء حرمة المكان، وعليه فهو إجراء من إجراءات الاستدلال والذي يدخل في اختصاصاتهم العادية[٣].
- أن يتم التفتيش وفقاً للإجراءات القانونية المقررة: يتم القيام بإجراء التفتيش وفقاً للشروط القانونية، بحيث يجب مباشرته طبقاً لإجراءات صحيحة فإذا شاب التفتيش الواقع على نظم الحاسوب عيب فإنه باطل[٤].

(١) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ١٥.
(٢) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ١٥
(٣) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ١٦.
(٤) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ١٦.

ج- مدى قابلية جرائم الحاسوب والشبكات الإلكترونية للتفتيش عن أدلتها:

قد يرد محل التفتيش في البيئة المعلوماتية على المكونات المادية أو المعنوية للحاسب الآلي والتي نتعرض إليها فيما يلي:

١. خضوع مكونات الحاسوب المادية والمعنوية للتفتيش عن أدلة الجريمة:

تشمل مكونات الحاسوب المادية على الأشياء الملموسة وملحقاته[١]، والتي تتمثل في شكل وحدات كوحدة الذاكرة، لوحة المفاتيح والشاشة ووحدة التحكم، وكل واحدة لها مهمة محددة، فهي لا تواجه صعوبات تعيق إجراءات التفتيش باعتبارها من المكونات المادية، والتي يمكن إيجادها في مسكن المتهم أو مسكن غير المتهم، والتي قد تتواجد أيضاً في مكان عام، فهي بذلك تخضع للقواعد التي تحكم ذلك المكان، كما قد تتواجد هذه المكونات في حيازة شخص خارج مسكنه، فهي بذلك تخضع لقواعد تفتيش الأشخاص بوصف المكونات المادية للحاسوب أحد ملحقاته، وسواء كان الشخص الحائز المالك أو الغير، أما بالنسبة لمكونات الحاسوب المعنوية والمتمثلة في المعلومات والبيانات المعالجة آلياً، فهي محل خلاف باعتبارها غير مادية[٢].

٢. خضوع شبكات الحاسب الآلي للتفتيش:

قد يكون حاسب المتهم متصلاً بغيره من الحواسيب عبر الشبكة الإلكترونية، وهنا يجب التمييز بين ما إذا كان حاسوب المتهم متصلاً بآخر داخل إقليم الدولة، أو كان متصلاً بحاسوب يقع في نطاق إقليم دولة أخرى.

وتكمن المسألة في الحالة الأولى في تجاوز الاختصاص المكاني للسلطة المختصة بالتفتيش، كما أنه يعتبر بمثابة العدوان على حقوق الأفراد وحرياتهم، ذلك عند قيام سلطة التحقيق بتفتيش جهاز له علاقة بجهاز المتهم داخل الدولة.

وقد أجازت بعض التشريعات للأشخاص القائمين على التفتيش امتداد هذا الأخير على سجلات البيانات المتصلة في النهاية الطرفية للحاسوب في منزل المتهم مع جهاز أو نهاية طرفية في مكان آخر، حيث أنه يمكن امتداد الحق في تفتيش المساكن إلى نظم المعلومات الموجودة في موقع آخر حينما يهدف ذلك إلى إظهار الحقيقة دون وجوب

(١) موسى مسعود، ارحومة. (٢٠٠٩). «الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ص ٧.

(٢) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ١٧.

صدور إذن مسبق من قاضي التحقيق وذلك بشرطين هما: أن تكون النهاية الطرفية المتصلة بالحاسب الآلي موجودة داخل الدولة المعنية، وأن تتضمن النهاية الطرفية المتصلة بالحاسب الآلي بيانات مخزنة تستهدف إظهار الحقيقة[١].

أما حالة وجود جهاز متصل بجهاز المتهم خارج الدولة، فتعد هذه المسألة من المشكلات التي تواجه إجراء التحقيق وبالخصوص مسألة التفتيش، ذلك لما توصلت إليه الدول من خلال برمجيات يمكنها القيام بإجراء التفتيش والذي لا يستند إلى مبرر قانوني من جهة، وباعتباره اعتداء على خصوصيات الأفراد وأجهزة حواسبهم من جهة أخرى[٢].

د- شروط التفتيش:

يعتبر التفتيش انتهاكاً للحق في الخصوصية الفردية، ومن ثم يعد التفتيش أحد مظاهر تقييد الحريات الإنسانية، لذا عمدت الدول إلى إحاطته بالضمانات القانونية حتى لا يتم إساءة استخدامه وسوف نتناول في هذا الإطار ما يلي:

د.١- الشروط الموضوعية للتفتيش الرقمي:

يشترط أن يتوافر في التفتيش سبب له، وأن يكون محله الحاسوب بكل مكوناته المادية والمنطقية والشبكة الإلكترونية، بالإضافة إلى وجود سلطة مختصة للقيام به، وعلى ضوء ما سبق فإن القواعد الموضوعية لتفتيش نظم المعلوماتية تتمثل فيما يلي:

الشرط الأول: أسباب تفتيش النظم المعلوماتية:

ترتب على إجراء التفتيش خلاف فقهي حول مدى مشروعية التفتيش في الجرائم المعلوماتية بين الذين يرون قابلية النصوص التقليدية لتطبيق هذا الإجراء في الجرائم المعلوماتية، مع الذين يتجهون إلى وجوب استحداث نصوص تشريعية جديدة تجرم الأفعال، وأثناء غياب تشريعات جديدة فلا مجال للحديث عن سبب تفتيش الحاسب الآلي، غير أن هذه المشكلة لا يمكن أن تثير سبب التفتيش في الجرائم المعلوماتية في الدول التي تضمنت نصوص قانونية للتجريم والعقاب على مثل هذه الجرائم [٣].

وعليه لكي يعتبر التفتيش في مجال الجريمة المعلوماتية مشروعاً لابد من توافر شروط والتي نوردها فيما يلي:

(١) خالد ممدوح إبراهيم، خالد، مرجع سابق، ص ٢١٠. ومعمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٢١.
(٢) موسى مسعود، ارحومة، مرجع سابق، ص. ٧. وخالد ممدوح إبراهيم، خالد، مرجع سابق، ص ٢١٠.
(٣) غلاب، فايز محمد راجح. (٢٠١٠/٢٠١١). الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، ص ٢١٩.

- وجوب وقوع جريمة معلوماتية سواء كانت جناية أو جنحة، وبالتالي تستبعد المخالفات نظراً لقلة أهميتها باعتبارها لا تصل إلى درجة المساس بحريات الأشخاص أو انتهاك لحرمات منازلهم[١].
- اتهام شخص أو أشخاص معينين بارتكاب الجريمة أو المشاركة فيها.
- توافر أمارات قوية أو قرائن على وجود أجهزة معلوماتية تفيد في كشف الحقيقة لدى المتهم أو غيره[٢].

ولذلك لا يجرى التفتيش إلا إذا توافرت لدى قاضي التحقيق أسباب كافية مقنعة، أي تواجد أدوات أو أشياء استعملت في ارتكاب الجريمة أو متحصلة منها، أو مستندات إلكترونية يحتمل أن يكون لها فائدة في التفتيش عن الحقيقة سواء لدى المتهم المعلوماتي أو غيره والتي تتواجد في المكان أو عند الشخص المراد تفتيشه[٣].

الشرط الثاني: محل تفتيش النظم المعلوماتية:

لكي يكون التفتيش صحيحاً يجب أن يرد على المحل الذي قد يكون الشخص أو المكان، وهذا المحل يجب أن يكون محدداً أو قابلاً للتحديد وجائزاً قانوناً[٤]، وبالتالي فالشخص الذي يقوم بتفتيش نظم المعلوماتية، قد يكون من خبراء البرامج سواء كانت برامج نظام أو برامج تطبيقات، أو من مشغلي، أو مستخدمي الحاسب، أو مقدمي الخدمة، أو من مهندسي الصيانة والاتصالات، أو من مديري نظم المعلوماتية، أما الأشخاص الذين يقوم عليهم التفتيش هم أي أشخاص آخرون تكون بحوزتهم معدات أو أجهزة معلوماتية أو أجهزة حاسب آلي محمول أو تلفونات متصلة بجهاز المودم أو مستندات، وفي كل الأحوال يقصد بالشخص كمحل قابل للتفتيش كل ما يتعلق بكيانه المادي وما يتصل به[٥].

(١) خالد ممدوح إبراهيم، خالد، مرجع سابق، ٢١٠.
(٢) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٢١.
(٣) عطية، طارق إبراهيم الدسوقي. الأمن المعلوماتي، النظام القانوني للحماية المعلوماتي، (بدون طبعة)، دار الجامعة الجديدة، الإسكندرية، ص ٤٠٥. أشار إليه في الهامش: معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٢١.
(٤) فرغلي، عبدالناصر؛ السمساري، محمد، مرجع سابق، ص ١٩.
(٥) هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، ١٩٩٧، ص ١٣٦.

الشرط الثالث: السلطة المختصة بتفتيش النظم المعلوماتية:

الأصل أن تقوم بإجراء تفتيش نظم الحاسب الآلي سلطة التحقيق الأصلية المتمثلة في قاضي التحقيق لدى النيابة العامة وقضاة المحكمة، إلا أنه يجوز لضباط الشرطة القضائية أن يقوموا بهذا الإجراء بناء على تفويض صادر من السلطة المختصة، وهذا ما سنبينه في الآتي:

إجراء تفتيش نظام المعلوماتية بمعرفة سلطة التحقيق الأصلية:

إن المشرع الإجرائي أناط الاختصاص بالتفتيش كإجراء تحقيق للنيابة العامة كسلطة أصلية ولقاضي التحقيق في حالات خاصة[1]، واستثناءً يجوز تخويل بعض سلطة التحقيق للمنتدب، مع بقاء الأصل في أن الاختصاص الأصيل مباشرته يعود لقاضي التحقيق وحده دون سواه.

ولا يكفي توافر صفة قاضي التحقيق لكي يقوم بإجراء التفتيش، بل لابد أن يكون مختصاً سواء من ناحية الاختصاص المكاني، وبالإضافة إلى الاختصاص المكاني يجب أن يتوافر الاختصاص النوعي المتمثل في نوع الجريمة التي يختص بها المحقق بالتفتيش[2].

إجراء تفتيش النظم المعلوماتية بمعرفة ضباط الشرطة القضائية:

يتمتع قاضي التحقيق وحده بالاختصاص الأصيل لإجراء التحقيق، ونظراً لكثرة هذه الإجراءات وتنوعها أجاز له القانون أن يندب غيره للقيام ببعضها وفقاً لشروط يجب توافرها وتطبيقها بحذافيرها[3].

وبالتالي فإن المنتدب الذي يختص في الجريمة التقليدية هو نفسه الذي يختص في الجريمة المعلوماتية، ويتحقق إجراء تفتيش نظم المعلوماتية بمعرفة المنتدب، في الحالات التالية[4]:

- **التفتيش بناء على إذن قضائي بإجرائه:**

باعتبار أن قاضي التحقيق غير ملزم في كل الحالات بمباشرة التفتيش، فإنه يجوز

(١) هلالي عبد اللاه أحمد، المرجع السابق، ص. ١٣٣.
(٢) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٢٣.
(٣) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٢٤.
(٤) طارق إبراهيم الدسوقي عطية، مرجع سابق، ص ٤٢٨.

له أن يندب أحد ضباط الشرطة القضائية للقيام بهذا الإجراء وهذا ما يسمى بالإنابة القضائية، لذلك فلا يجوز لضباط الشرطة القضائية القيام بإجراء التفتيش إلا بعد حصولهم على إذن من السلطة المختصة[١].

- **التفتيش بناء على حالة التلبس بالجريمة (الجريمة المشهودة):**

لا يختلف التفتيش في حالة التلبس في نظم الحاسب الآلي عن الجريمة التقليدية، لذلك يجوز للمنتدب في أحوال التلبس بالجرائم المعلوماتية تفتيش نظم الحاسب الآلي[٢]، وهذا ما تضمنته المواد من (٩٩) إلى (١٠٢) إجراءات جزائية يمني:

- **التفتيش بناء على موافقة المتهم:**

يجب أن تكون الموافقة من طرف صاحب الشأن بالتفتيش صريحة ومكتوبة بخط يده، فإذا كان لا يعرف الكتابة يذكر ذلك في المحضر ويذكر فيه هذه الموافقة؛ أما بخصوص جرائم الحاسب الآلي فإنه لا توجد نصوص قانونية مشابهة تخص تفتيش نظم المعلوماتية بناء على موافقة المتهم سواء في مصر أو في القانون المقارن، لذلك فإن هذا الفراغ يمكن تغطيته بالقواعد التقليدية[٣].

د.٢- الشروط الشكلية للتفتيش الرقمي:

إلى جانب الضوابط الموضوعية لتفتيش نظم الحاسب الآلي، هناك ضوابط أخرى ذات طابع شكلي يجب مراعاتها والأخذ بها أثناء القيام بالتفتيش، والتي تتمثل فيما يلي:

الشرط الأول: الأشخاص المطلوب حضورهم أثناء التفتيش:

يشترط لقيام التفتيش كضمانة حضور صاحب المكان المراد تفتيشه، حيث اعتبر غالبية الفقه أن حضور المتهم للتفتيش من الأحكام الأساسية التي يجب الالتزام بها ويترتب على مخالفتها بطلان إجراء التفتيش[٤].

الشرط الثاني: أسلوب تنفيذ التفتيش:

لا يوجد نص قانوني في المنظومة التشريعية اليمنية يبين أسلوب التفتيش في الجرائم المعلوماتية، وبالاطلاع على التشريعات العالمية المنظمة لهذا الموضوع؛ قام

(١) معمش، زهية؛ غانم، نسيمة، مرجع سابق، ص ٢٤.
(٢) طارق إبراهيم الدسوقي عطية، مرجع سابق، ص ٤٣٧.
(٣) هلالي عبد اللاه أحمد، مرجع سابق، ص. ١٦٢.
(٤) غلاب، فايز محمد راجح، مرجع سابق، ص ٣٣٤.

القانون الأمريكي بتنظيم أسلوب تنفيذ التفتيش في نظم الحاسب الآلي، حيث يبدأ رجال الشرطة بالهجوم في الوقت نفسه وبشكل سريع على جميع منافذ المكان، باعتبار أن هذه الخطة تقلل من وقوع إصابات بين فرق رجال الشرطة، وبعد ذلك يقومون بسرعة فائقة باستبعاد الأشخاص المشتبهين فيهم على الحواسب الموجودة في المكان حتى لا يتم تغيير أو حذف أو تدمير الأدلة التي تثبت إدانتهم، حيث يوضع المتشبه فيهم في غرفة مع حراسة أمنية، وتفتيشهم في نفس الوقت مع إعلامهم أن كل أقوالهم ستؤخذ بعين الاعتبار ويمكن أن تكون دليل إدانتهم، حيث يوجد مكان في المنزل يعتبر النقطة الساخنة والتي يكون فيها جهاز حاسب آلي متصل بخط هاتفي أو أكثر من ذلك[١].

الشرط الثالث: تحديد ميعاد التفتيش:

يعتبر ميعاد التفتيش أحد أهم الضمانات الشكلية، بحيث لا يجوز إجراؤه خارج الأوقات المحددة قانوناً ما عدا في الأحوال الاستثنائية المقررة قانوناً[٢].

فلا يجوز البدء في التفتيش قبل الساعة الخامسة صباحاً ولا بعد الساعة الثامنة مساءاً، إلا إذا طلب صاحب المنزل ذلك، أو وجهت نداءات من الداخل، أو في الحالات الاستثنائية التي أقرها القانون[٣]، منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي يجوز إجراء التفتيش فيها في كل ساعة من ساعات الليل والنهار بناء على إذن مسبق من وكيل الجمهورية المختص، ذلك لأن المكونات المعنوية للحاسب الآلي وشبكة الاتصال قد تكون عرضة لإخفاء أو تغيير أو تدمير أو تلاعب بالبيانات المخزنة والتي تعتبر أدلة إلكترونية لإظهار الحقيقة، مما قد يؤدي بالجاني في ظرف ثوان إلى إفساد هذه الأدلة وعرقلة عمل التحقيق، لذلك استوجب هذا الأمر على التشريعات الحديثة إضافة الجريمة المعلوماتية كاستثناء عن أوقات التفتيش نظراً لطبيعة أدلتها الخاصة[٤].

الفرع الثالث

التحديات الإجرائية في مواجهة التحقيق الرقمي

إضافة إلى التحديات القانونية والموضوعية، يواجه النظام القضائي اليمني في مجال التحقيق الرقمي العديد من التحديات الإجرائية، وفيما يلي بيان بأهم تلك التحديات:

(١) غلاب، فايز محمد راجح، المرجع السابق، ص ٣٣٨.
(٢) غلاب، فايز محمد راجح، المرجع السابق، ص ٣٢٨.
(٣) غلاب، فايز محمد راجح، المرجع السابق، ص ٣٢٨.
(٤) غلاب، فايز محمد راجح، مرجع سابق، ص ٣٣٠.

أولاً: القصور الإجرائي التشريعي:

تعاني التشريعات الإجرائية في اليمن- وعلى وجه الخصوص قانون الإجراءات الجزائية- جموداً تشريعياً مستفحلاً، حال دون مواكبة التطورات على الساحة العالمية وتحديداً في مجال التكنلوجيا والتحول الرقمي[1]، وفيما يلي نوجز أهم التحديات الإجرائية أو القصور الإجرائي، وذلك في الآتي:

١. اقتصار القوانين الإجرائية على تنظيم أحكام التحقيق العادي، دون استحداث التعديلات المناسبة مع التغيرات التكنلوجية.

٢. عدم تطوير آليات التحقيق، وذلك جاء نتيجة عدم وجود التشريعات الحديثة التي تساير الجوانب التكنلوجية.

٣. نقص الكوادر المؤهلة، حيث يواجه النظام القضائي اليمني تحديات في توافر الخبرات المتخصصة في مجال التحقيق الرقمي.

ثانياً: عدم الاستفادة من الخبرات الدولية في مجال التحقيق الرقمي نتيجة الظروف السياسية والأمنية:

يعد تفعيل التعاون الدولي في الجرائم الرقمية، ركيزة أساسية في اكتساب العنصر المحلي لخبرات التحقيق الرقمي، إلا أن اليمن خلال العقد الماضي مرت بالكثير من الأزمات والنزاعات التي حالت دون وجود أية اتفاقات أو تفاهمات أو مؤتمرات مع دول العالم بشأن التحقيق في الجرائم الرقمية، وهذا بحد ذاته شكل تحدياً كبيراً- على المستوى الموضوعي والإجرائي- حال دون استفادة الكادر القضائي اليمني من خبرات التحقيق في هذا المجال.

وبالتالي يستلزم لتجاوز تلك التحديات، العمل على تطوير آليات التحقيق الرقمي من خلال تطوير ووضع قوانين بإجراءات أكثر تحديدًا لتنظيم التحقيقات الرقمية، وتدريب القضاة وأعضاء النيابة ومأموري الضبط، من خلال توفير برامج تدريبية متخصصة لتعاملهم مع الأدلة الرقمية، بالإضافة إلى تفعيل التعاون الدولي لتبادل الخبرات في مجال التحقيق الرقمي.

(١) السراجي، أحمد يحيى، مخاطر الجريمة الإلكترونية وأضرارها على الفرد والمجتمع، مرجع سابق، ص ٨.

الخاتمة

بعد أن استعرضنا في متن البحث بيان ماهية التحقيق الرقمي ونطاق تطبيقه، وبيان أهم الأدوات والتقنيات المستخدمة في الإثبات الجنائي وإجراءاته؛ خلصنا إلى الخروج بالنتائج والتوصيات التالية:

أولاً: النتائج:

١. وجود فراغ تشريعي وقانوني يعاني منه التحقيق الرقمي في اليمن، فلا يوجد نص تشريعي أو قانوني يحدد المبادئ الإجرائية والتوجيهية لكيفية التحقيق الرقمي، مما يضعف أداء الجهات المختصة بالتحقيق.

٢. عدم وجود قانون يختص بالجرائم المعلوماتية أو الالكترونية في اليمن جعل عملية التحقيق في هذه الجرائم تواجه صعوبة في الاثبات الجنائي.

٣. عدم معرفة السلطات القضائية من أعضاء النيابة وقضاة في اليمن للمعلومات الفنية الأساسية الخاصة بالجرائم الالكترونية والتحقيق فيها، مما يجعلهم في بعض الحالات يستعينون بخبراء في التكنولوجيا من غير السلطة القضائية لتوضيح مدى قوة الدليل الالكتروني في الإثبات الجنائي.

٤. تكييف التحقيق الرقمي بالتحقيق التقليدي في اليمن، مما يجعل عملية التحقيق في الجريمة الالكترونية تعود بشكل كبير لقناعة القاضي في حجية الدليل الالكتروني في الإثبات الجنائي.

ثانياً: التوصيات:

١. إصدار قانون خاص بالجرائم والإلكترونية؛ لمسايرة التطورات الراهنة أولاً، ومواجهة التحديات التي تواجه المجتمع اليمني بشأن انتشار الجرائم الإلكترونية.

٢. إعداد دليل إرشادي يتضمن المبادئ التوجيهية والإجراءات الخاصة بكيفية التحقيق في الجرائم الالكترونية، حتى يكون التحقيق والإثبات يعتمد على أساس علمي سليم غير قابل للطعن.

٣. إقامة دورات وبرامج تدريبية وورشات عمل للقضاة وأعضاء النيابة ومأموري الضبط القضائي في مجال الجرائم الإلكترونية والتحقيق فيها والتعامل مع الأدلة الرقمية

وجمعها وتحليلها بشكل صحيح.

٤. تجهيز قسم خاص بالجرائم الالكترونية والتحقيق فيها يتبع النيابة العامة مكون من اختصاصيين فنيين وقانونين.

٥. كما نوصي أيضاً الجامعات والمعاهد ومراكز البحوث الرسمية والخاصة، بتشجيع وتوجيه الأكاديميين والباحثين إلى تركيز البحوث والدراسات المتعلقة بالجرائم الإلكترونية بمختلف تفاصيلها وتقنياتها مسايرة للتطور التكنلوجي الخطير على أمن الدولة والمجتمع معاً.

قائمة المصادر والمراجع

المصادر والمراجع العربية:

أولاً: المصادر العامة:

١. القرآن الكريم.

٢. دستور الجمهورية اليمنية النافذ.

٣. القرار الجمهوري بالقانون رقم (٢١) لسنة ١٩٩٢م بشأن الإثبات وتعديلاته.

٤. القرار الجمهوري بالقانون رقم (١٢) لسنة ١٩٩٤م بشأن الجرائم والعقوبات وتعديلاته.

٥. القرار الجمهوري بالقانون رقم (١٣) لسنة ١٩٩٤م بشأن الإجراءات الجزائية.

٦. القرار الجمهوري بالقانون رقم (٤٠) لسنة ٢٠٠٦م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، المنشور في الجريدة الرسمية العدد الرابع والعشرون الصادر بتاريخ ١١/ ذو الحجة /١٤٢٧هـ الموافق ٣١ / ديسمبر/٢٠٠٦م.

٧. الاتفاقية العربية لمكافحة جرائم المعلوماتية لسنة ٢٠١٠م.

٨. الرازي، محمد بن أبي بكر. مختار الصحاح، الهيئة المصرية العامة للكتاب، ط١، ١٩٧٦م.

٩. المعجم الوسيط، مجمع اللغة العربية، الجزء الأول، دار المعارف، مصر، (١٤٠٠هـ).

١٠. قاموس اللغة «كتاب المصباح المنير». الفيومي، أحمد محمد. (بدون تاريخ)، الجزء الثاني، نوبليس، مصر.

ثانياً: الكتب:

١. الأودن، سمير عبد السميع. (٢٠٠٥م). العقد الإلكتروني، (ب ط)، منشأة المعارف بالإسكندرية، مصر.

٢. الجوخندار حسن. (٢٠٠٨). التحقيق الابتدائي في قانون الأصول المحاكمات الجزائية، دار الثقافة عمان، الطبعة الأولى، الأردن.

٣. حجازي عبد الفتاح بيومي. (٢٠٠٩). الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت «دراسة معمقة في جرائم الحاسب الالي والانترنت»، بهجت للطباعة والتجليد، مصر.

٤. حجازي، عبد الفتاح بيومي. التجارة الإلكترونية وحمايته القانونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٥م.

٥. حسين على محمود، عبدالله. سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر. ٢٠٠١م.

٦. رستم، هشام فريد. (١٩٩٤م). الجوانب الإجرائية في الجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، مصر.

٧. طارق عبد الرؤوف، محمد. (٢٠١١). جريمة الاحتيال عبر الإنترنت الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، الطبعة الأولى، ٢٠١١م.

٨. الطائي جعفر حسن جاسم. (٢٠١٠). جرائم تكنولوجينا المعلومات، ط ١، دار البداية، الأردن.

٩. عبد الرحمن، خالد حمدي. (٢٠٠٦م)، التعبير عن الإرادة في العقد الإلكتروني، (ب ط)، دار النهضة العربية – والقاهرة، مصر.

١٠. عزت، فتحي محمد أنور. (٢٠١٠). الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجاري، دار الفكر والقانون للنشر والتوزيع، الطبعة الأولى، مصر.

١١. فهمي، خالد مصطفى. النظام القانوني للتوقيع الإلكتروني، في ضوء الاتفاقيات الدولية التشريعات العربية والقانون رقم (١٥) لسنة ٢٠٠٤م، بدون طبعة، دار الجامعة الجديد، الإسكندرية. (٢٠٠٧م).

١٢. قنديل، سعيد السيد. (٢٠٠٤م). التوقيع الإلكتروني بين التدوين والاقتباس، (ب ط)، دار الجامعة الجديد، الإسكندرية، مصر.

١٣. ممدوح عبد المطلب. (٢٠٠٦). البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر.

١٤. هبه هروال، نبيلة. الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٧م.

١٥. هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، ١٩٩٧م.

ثالثاً: الرسائل العلمية:

١. بطيخ، حاتم أحمد محمد. (٢٠١٧م). «دور الإنترنت في الإثبات أمام القاضي الجنائي والإداري – دراسة مقارنة»، أطروحة دكتوراه، قسم القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر.

٢. بن إبراهيم بن حماد العمر، عمر. (٢٠٠٧). إجراءات الشهادة في مرحلة الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمينة.

٣. بن فردية محمد. (٢٠١٥). الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم الجنائية، كلية الحقوق، الجزائري.

٤. بوحزمة نصيرة. (٢٠٢١/٢٠٢٢). التحقيق الجنائي في الجرائم الإلكترونية «دراسة مقارنة». أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس – سيدي بلعباس، الجزائر.

٥. بيراز جمال. (٢٠١٣/٢٠١٤). الدليل العلمي في الإثبات الجنائي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر – باتنة، الجزائر.

٦. تمام، أحمد حسام طه. (٢٠٠٠م). الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر.

٧. جستينه، محمد أحمد أحمد. (بدون تاريخ). مدى حجية التوقيع الإلكتروني في عقود التجارب الإلكترونية، أطروحة دكتوراه، الحقوق كلية الحقوق، جامعة القاهرة، مصر.

٨. الجمالي، سمير حامد عبد العزيز. (٢٠٠٥م). التعاقد عبر تقنيات الاتصالات الحديثة، رسالة دكتوراه في الحقوق، كلية الحقوق جامعة القاهرة، مصر.

٩. حسن محمد إبراهيم. (٢٠١١). الحماية الجنائية لحق المؤلف عبر الانترنت، رسالة الدكتوراه في الحقوق، كلية الحقوق، جامعة عين شمس، مصر.

١٠. عدلي دحمان؛ وسعد الدين ثامر البشير. (٢٠٢٠/٢٠٢١). التحقيق الجنائي في الجرائم الإلكترونية، مذكرة ماستر، قسم الحقوق، كلية الحقوق والعلوم السياسي، جامعة زيان عاشور – الجلفة –، الجزائر.

١١. هلال أمنة. (٢٠١٤/٢٠١٥). الإثبات الجنائي بالدليل الالكتروني. مذكرة محكمة من مقتضيات نيل شهادة الماستر في الحقوق تخصص القانون الجنائي، كلية الحقوق

والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر.

رابعاً: المجلات العلمية:

١. الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي «دراسة في القانونين الإنجليزي والأمريكي». International Review of Law: Vol. ٢٠١٧ ,٣ ,١٤. dx.doi.org/١٠,٥٣٣٩/irl.٢٠١٧,١٤

٢. اسخيطة، رضوان. التحقيق الجنائي الرقمي في ضوء قوانين حماية البيانات الشخصية، مجلة العلوم السياسية والقانون، العدد (١٧)، المجلد (٠٣)، سبتمبر ٢٠١٩م.

٣. عبد الباقي، مصطفى. (٢٠١٨م). التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين «دراسة مقارنة»، مجلة دراسات، علوم الشريعة والقانون، عمادة البحث العلمي وضمان الجودة، الجامعة الأردنية، المجلّد (٤٥) عدد (٤)، ملحق (٢).

٤. عرب، يونس. (١٩٩٩). جرائم الكمبيوتر، مجلة البنوك، العدد الخامس، الأردن.

خامساً: المؤتمرات والندوات:

١. «مخاطر الجرائم الإلكترونية في المجتمع اليمني». (١٦ يوليو ٢٠٢٤م). ندوة عقدتها الأمانة العامة بمجلس الشورى بالتعاون مع عدد من الجهات ذات العلاقة، اليمن.

٢. عبد الله حسين محمود. (٢٠٠٣). إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات.

٣. فرغالي، عبد الناصر محمد محمود؛ المسماري، محمد عيج سيف سعيد. (١٢-١٤/١١/٢٠٠٧م). الإثبات الجنائي بالأدلة الرقمية والفنية «دراسة تطبيقية مقارنة». المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف للعلوم الأمنية.

٤. المؤتمر العلمي الأول للأمن السيبراني، الذي عقدته وزارة الاتصالات وتقنية المعلومات بتاريخ: ٧-٩/ يونيو/ ٢٠٢١م، اليمن.

٥. موسى مسعود، ارحومة. (٢٠٠٩). «الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون،

أكاديمية الدراسات العليا، طرابلس، المغرب.

٦. هشام فريد رستم. (٢٠٠٠). أصول التحقيق الجنائي الفني في بحوث مؤتمر القانون والكمبيوتر والانترنت، المجلد الثاني، ط الثالثة، الامارات العربية المتحدة.

سادساً: الصحف:

١. تحقيق صحفي حول الورقة المقدمة في المؤتمر الوطني الأول في اليمن بعنوان: «مخاطر الجريمة الإلكترونية وأضرارها على الفرد والمجتمع» للعقيد أحمد يحيى السراجي. (٧-٩/ يونيو/ ٢٠٢١م). صحيفة الثورة، العدد (٢٠٧٣٣)، تاريخ الأربعاء ١٧ محرم ١٤٤٣هـ الموافق ٢٥ أغسطس ٢٠٢١م.

English References

1. eLecTRonic eviDence 10.282–10.283 (Stephen Mason & Daniel Seng, eds. 2010).
2. Eoghan Casy: Digital Evidence Forensics Science Computer and The Internet Computer Crime, OP–CIT, P.5.
3. Hothi [2011] EWCA (Crim) 1039; O'Brien [2011] EWCA (Crim) 768.
4. O'Floinn & Ormerod, Social Networking Material, supra note 71, at 504; see also O'Floinn & Ormerod, Social Networking 177Sites, supra note 31, at 490.
5. PauL RoBeRTs & aDRian ZucKeRman, cRiminaL eviDence 227–28 (2d ed. 2010).
6. Rocco Parascandola, NYPD forms new social media unit to mine Facebook and Twitter for mayhem, n.Y. DaiLY news, Aug. 10, 5.
7. See, e.g., Haque & Nuth [2009] EWCA (Crim) 1453; Johnson [2008] EWCA (Crim) 3321; Mullen [2011] EWCA (Crim) 1744; Eglen 7 [2011] EWCA (Crim) 1437.
8. WLR 651; [1972] 2 All ER 699; [1972] 56 Cr. App. R. 450; [1972] Crim. LR 316; [1972] 116 SJ 313. 1 [1972].