الدكتور/ رامى متولى القاضى
أستاذ ورئيس قسم القانون الجنائى المساعد بكلية الشرطة

الدليل الجنائى الرقمى فى التشريع المصرى

فى ضوء أحكام القانون رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية

المراسلة: د. رامي متولي القاضي
أستاذ ورئيس قسم القانون الجنائي المساعد، كلية الشرطة، مصر

معرف الوثيقة الرقمي (DOI): https://doi.org/10.54873/jolets.v2i1.9

البريد الإلكتروني: ramy_elkady@alumini.cu.edu.eg

نسق توثيق البحث:
رامي متولي القاضي، الدليل الجنائي الرقمي في التشريع المصري في ضوء أحكام القانون رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية والتشريعات المقارنة والمواثيق الدولية، مجلة القانون والتكنولوجيا، المجلد ٢، العدد ١، أبريل ٢٠٢٢، صفحات ١٧٧-٢٤٦

الدليل الجنائي الرقمي في التشريع المصري في ضوء أحكام القانون رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية والتشريعات المقارنة والمواثيق الدولية

الدكتور/ رامى متولى القاضى

الملخص:

يهدف البحث إلى التعريف بالدليل الرقمي وبيان خصائصه وبحث الحجية القانونية للدليل الرقمي في التشريع المصري وإلقاء الضوء على الشروط الخاصة بطرق جمع الأدلة الرقمية ومقبوليتها أمام القضاء الجنائي وتسليط الضوء على الحماية الجنائية للأدلة الرقمية وإجراءات جمعها وتوثيقها في التشريع المصري، ويمكن تأصيل أهمية موضوع البحث في أن ذيوع استخدام التكنولوجيا في مناحي الحياة، وانتشار الأجهزة الكهربائية والتكنولوجية وشبكة الإنترنت أدى إلى استنتاج، نراه من جانبنا منطقياً، مؤداه أنه من غير المتصور وقوع جريمة تقليدية أو مستحدثة، دونما أن يتخلف عنها أدلة رقمية يمكن التوصل من خلالها إلى تحديد مرتكب الجريمة، مثل: الرسائل النصية، ورسائل البريد الإلكتروني، وبيانات تصفح الإنترنت، وإنه مع شيوع استخدام التطورات التكنولوجية الجديدة، مثل: إنترنت الأشياء وشبكات الإنترنت المظلم، والتشفير العالي الدرجة والعملات الافتراضية في ارتكاب الجرائم، فمن المتوقع ازدياد أهمية الدليل الرقمي في الحقل الجنائي، وهو ما سيتطلب من جهات إنفاذ القانون إجراء تغييرات جذرية في طرق جمع الأدلة وآليات التعاون الدولي في المسائل الجنائية، تتناسب وطبيعة هذه النوعية المستحدثة من الأدلة الجنائية.

وقد انتهى البحث إلى وجوب تعزيز التعاون مع المنظمات الدولية العاملة في مجال تبادل المعلومات ذات الصلة بجرائم تقنية المعلومات والأدلة الرقمية، والاستفادة من التسهيلات التي تقدمها للدول للتعامل مع هذه الطائفة من الجرائم، ووجوب تعزيز التعاون الدولي القضائي عبر الاتفاقيات الثنائية ومتعددة الأطراف لتسهيل مهمة القائمين على إنفاذ القانون في عمليات جمع واستخراج الأدلة الرقمية، وبصفة خاصة الدول التي توجد بها الخوادم الرئيسية لشبكات المعلومات، والمضي قدماً في صقل قدرات العنصر البشري المتعامل مع الأدلة الرقمية من رجال إنفاذ القانون تمكيناً لهم من التعامل الأمثل مع الأدلة الرقمية.

الكلمات الرئيسية: الدليل الرقمي- علم الأدلة الجنائية الرقمية- حجية الدليل الرقمي- مقبولية الدليل الرقمي- توثيق الدليل الرقمي.

Digital Forensic Evidence in the Egyptian Legislation in light of the provisions of Law No. 175 of 2018 and its Executive Regulations, Comparative Legislation and International Covenants

Dr. Ramy Metwally Elkady

Abstract:

The research aims to introduce the digital evidence, explain its characteristics, examine the legal authenticity of the digital evidence in the Egyptian legislation, shed light on the conditions for the methods of collecting digital evidence and its admissibility before the criminal judiciary, and highlight the criminal protection of digital evidence and the procedures for collecting and documenting it in the Egyptian legislation. The importance of the research topic can be rooted in the widespread use of technology in all walks of life, the spread of electrical and technological devices and the Internet has led to a conclusion, which we see logical from our side, that it is inconceivable that a traditional or a new crime will occur, without leaving behind digital evidence through which to identify the perpetrator of the crime.

The research concluded that cooperation with international organizations working in the field of information exchange related to information technology crimes and digital evidence should be strengthened, and the facilities they provide to countries to deal with this category of crimes should be strengthened, and international judicial cooperation should be strengthened through bilateral and multilateral agreements to facilitate the task of those responsible for the crime. Law enforcement in the processes of collecting and extracting digital evidence, especially in countries where the main servers of information networks are located, and moving forward in refining the capabilities of the human element dealing with digital evidence from law enforcement officers to enable them to optimally deal with digital evidence.

Kewords: digital evidence - digital forensics - authenticity of digital evidence - admissibility of digital evidence - documentation of digital evidence.

مقدمة:

١- التعريف بموضوع البحث وأهميته: يباشر الدليل دوراً مهماً فى عملية الإثبات الجنائي، بالنظر إلى أن هذه العملية تهدف إلى إثبات الصلة بين المتهم والجريمة وإسنادها إليه، توصلاً للحكم بإدانته أو تقرير براءته، فالدليل الجنائى هو الوسيلة التى يستعين بها القاضى للوصول إلى اليقين القضائى الذى يقيم عليه حكمه فى ثبوت الاتهام المعروض عليه[١].

وترجع أهمية الدليل الرقمى فى مجال الإثبات الجنائى باعتباره الأثر المترتب على جريمة تقنية المعلومات، وهو الوسيلة التى يعتمد عليها القاضى فى تكوين عقيدته القضائية بالإدانة أو بالبراءة، فمبدأ قضاء القاضى باقتناعه من المبادئ الأساسية فى الإثبات الجنائي، ومؤداه أن القاضى يحكم فى الدعوى بناءً على الأدلة التى تطرح أمامه فى الجلسة، فهى الوسيلة التى ينظر من خلالها القاضى للواقعة ليبنى قناعته[٢]، وقد ورد نص على المبدأ المشار إليه فى المادة (٣٠٢) إجراءات جنائية، التى تقضى بأنه: «يحكم القاضى فى الدعوى حسب العقيدة التى تكونت لديه بكامل حريته، ومع ذلك لا يجوز له أن يبنى حكمه على أى دليل لم يطرح أمامه فى الجلسة».

ويمكن تأصيل أهمية الدليل الرقمى فى أن ذيوع استخدام التكنولوجيا فى مناحى الحياة، وانتشار الأجهزة الكهربائية والتكنولوجية وشبكة الإنترنت أدى إلى استنتاج، نراه من جانبنا منطقياً، مؤداه أنه من غير المتصور وقوع جريمة تقليدية أو مستحدثة، دونما أن يتخلف عنها أدلة رقمية يمكن التوصل من خلالها إلى تحديد مرتكب الجريمة، مثل: الرسائل النصية، ورسائل البريد الإلكتروني، وبيانات تصفح الإنترنت.

وإنه مع شيوع استخدام التطورات التكنولوجية الجديدة، مثل: إنترنت الأشياء وشبكات الإنترنت المظلم، والتشفير العالى الدرجة والعملات الافتراضية فى ارتكاب

---

(١) د. عبد الرءوف مهدي، شرح القواعد العامة للإجراءات الجنائية، القاهرة، دار النهضة العربية، ٢٠٠٣، ص١٢٧٧؛ د. أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، القاهرة، دار النهضة العربية، ١٩٩٦، ص٤٩٢؛ د. مأمون سلامة، الإجراءات الجنائية فى التشريع المصري، ج٢، القاهرة، دار النهضة العربية، ١٩٩٦، ص٢٠٠.

(٢) د. وهيبة لعوارم، الدليل الرقمى فى مجال الإثبات الجنائى وفقاً للتشريع الجزائري، المجلة الجنائية القومية، المركز القومى للبحوث الاجتماعية والجنائية، المجلد ٥٧، العدد٢، يوليو ٢٠١٤، القاهرة، ص٦٧.

الجرائـم[١]، فمـن المتوقع ازديـاد أهمية الدليـل الرقمى فى الحقل الجنائـي، وهو ما سيتطلـب من جهات إنفاذ القانون إجراء تغيـيرات جذرية فى طرق جمع الأدلة وآليات التعاون الدولى فى المسائل الجنائية، تتناسب وطبيعة هذه النوعية المستحدثة من الأدلة الجنائية، والتى تتسـم بطابع خاص، وهو طبيعتها المعنوية المتغيرة، فالمعلومات المخزنة علـى أجهزة الحاسب الآلى أو على خوادم الحوسبة السحابية عبر شبكة الإنترنت، هى معلومـات متقلبة[٢]، ويسهل العبث بها وتغييرها أثنـاء التحقيقات[٣]، بل إن هذه الأدلة ذات طبيعة هشة وقابلة للإتلاف من خلال سوء المناولة أو الفحص بطريقة غير سليمة.

ومن ثَمَّ تبدو أهمية الدليل الرقمى جلية، باعتباره الوسيلة التى تمكن سلطات إنفاذ القانـون من معرفة كيفية وقوع جريمة تقنية المعلومـات وإثباتها ونسبتها إلى مرتكبها، لا سيمـا أنهـا ترتكب فى بيئـة افتراضية غير مادية [٤]، وكان مـن الواجب وضع قواعد وشـروط محـددة للتعامل مع هذه الأدلـة الرقمية للتأكـد من مقبوليتها أمـام القضاء الجنائي، فضـلاً عن اتخاذ احتياطات خاصة من أجل توثيقها وجمعها والحفاظ عليها وفحصها.

٢- **أهـداف البحث:** يهدف البحث إلى تحقيق هـدف رئيسى يتمثل فى إلقاء الضوء على الأحكام التى تنظم استخدام الدليل الرقمى فى التشريع المصرى فى ضوء القانون رقـم ١٧٥ لسنـة ٢٠١٨ ولائحتـه التنفيذيـة، وينبثق عن هـذا الهـدف الرئيسى بعض الأهداف الفرعية، من أبرزها ما يلي:

أ- التعريف بالدليل الرقمى وبيان خصائصه.

ب- بحث الحجية القانونية للدليل الرقمى فى التشريع المصري.

ج- إلقـاء الضوء على الشـروط الخاصة بطرق جمع الأدلة الرقمية ومقبوليتها أمام القضاء الجنائي.

(1) Sarah Meiklejohn and others, "A fistful of bitcoins: characterizing payments among men with no names", in Proceedings of the 2013 ACM SIGCOMM conference on Internet measurement conference (New York, ACM, 2013).

(2) Myriam Quéméner, Magistrat, Les spécificités juridiques de la prevue numérique AJ Pénal (1), 2014, p.63.

(٣) انظر: دراسة مكتب الأمم المتحدة بعنوان: «دراسة شاملة عن الجريمة السيبرانية»، مرجع سابق، ص٢٣٠.

(٤) د. جميـل عبـد الباقى الصغير، أدلة الإثبات الجنائـى والتكنولوجيا الحديثة، القاهرة، دار النهضـة العربية، ٢٠٠٢، ص١١؛ د.هنـد نجيب، حجية الدليـل الإلكترونى فى الإثبات الجنائي، المجلـة الجنائية القومية، المركز القومـى للبحوث الاجتماعية والجنائيـة، القاهـرة، المجلد ٥٧، العـدد الأول، مارس ٢٠١٤، صـ٤٩؛ د. أحمد سعد الحسيني، الجوانـب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، رسالة دكتوراه، جامعة عين شمس، ٢٠١٣، ص١٥٠.

د- تسليـط الضوء على الحماية الجنائية للأدلة الرقمية وإجراءات جمعها وتوثيقها فى التشريع المصري.

٣- أدوات ومنهـج البحث: سيستخدم الباحث المنهـج الوصفى التحليلي، والذى يعد أنسـب المناهج لدراسـة الموضوعـات القانونية، ويعـرف المنهج الوصفـى بأنه:«دراسة الظاهرة كما توجد فى الواقع ووصفها وصفاً وثيقاً ويعبر عنها تعبيراً كيفياً أو كمياً بغية الوصول إلى استنتاجات تسهم فى فهم هذا الواقع وتطويره»[١].

٤- خطـة البحث: نتناول موضوع البحث فى مبحثين: نعرض فى الأول ماهية الدليل الرقمـى وحجيته، ونتناول فى الثانى الحصول على الدليل الرقمى وحمايته، **وذلك على النحو التالي:**

المبحث الأول

ماهية الدليل الرقمى وحجيته

نتنـاول فى هذا المبحث التعريف بالدليل الرقمى فـى مطلب أول، ومشروعية الدليل الرقمى ومقبوليته أمام القضاء الجنائى فى مطلب ثانٍ، وحجيته فى مطلب ثالث، وذلك على النحو التالي:

المطلب الأول

التعريف بالدليل الرقمي

أولاً- تعريـف الدليل الجنائى الرقمي: قبل أن نتنـاول تعريف الدليل الرقمي، تجدر الإشـارة إلى بيان المقصود بالدليل الجنائي، حيـث إن المقصود فى الأساس من الدليل الرقمـى هـو الدليـل الجنائى الرقمـى الموجود فى الفضـاء الافتراضـي، والناجم عن استخدام تقنية المعلومات.

١- تعريـف الدليـل الجنائي: يقصد بالأدلـة الجنائية الوسائل التـى تربط الوقائع بإدانـة أو براءة الأفراد أثنـاء المحاكمات الجنائية، وهى مجموعة مـن القرائن، والتى مـن خلالها يمكن إثبات مجموعة مـن الحقائق التى تدور حول الجريمة، بالإضافة إلى

(١) ذوقان عبيدات وآخرون، مناهج وأساليب البحث العلمي، عمان، الأردن، دار صنعاء للنشر، ١٩٩٦، ص٢٢٠.

القدرة على نسبتها إلى فاعل معين، أو هي: مجموعة من البراهين مقبولة بحكم القانون لا يمكن أن يتم إثبات وقائع الجريمة إلّا بواسطتها أمام الجهات القضائية، سواء أكانت المحاكم أم دور النيابة العامة، وهى تتنوع تبعًا لتنوع الجرائم، ومن ثَمَّ فالدليل الجنائى هـو: كل إجراء معـترف به قانوناً لإقنـاع القاضى بحقيقة الواقعة محـل الاتهام، وهذا الدليل إما أن يكون أثراً منطبعاً فى نفس أو فى شيء أو يتجسم فى شيء يدل على وقوع جريمـة مـن جانب شخص معـين[١]، والدليل يتم الحصول عليه مـن مسرح الجريمة، والـذى يعرف بأنـه: «المكان الذى وقعت أو نفـذت فيه الجريمة»، كمـا يُمكن الحصول عليهـا من خـلال أشخاص شاهدوا هـذه الجريمة أو سمعوا بهـا أو عن طريق اعتراف

(١) الدليل الجنائى قد يكون عبارة عن أثر منطبع فى نفس؛ كأقوال شاهد أو اعتراف المتهم، ومن ثم يكون الدليل نفسياً، وقد يكون الدليل أثراً منطبعاً فى شيء؛ كبصمة الجاني، أو أثراً يتجسم فيه كالمخدر، أو النقود المزيفة التى وجدت فى جيب الشخص، ومـن ثـم يكون الدليل مادياً، وقد يكـون الدليل كاملاً يدل على وقوع الجريمة وعلى نسبتهـا إلى شخص معين، وقد يكون دليل جريمـة فقـط؛ أى دليل وقوع جريمة دون نسبتهـا إلى شخص معين؛ كرؤية شخص مذبوح أو التقاريـر الطبية وتقرير الصفة التشريحيـة ومعاينـة المعمل الجنائـي، والدليل فى النهاية كما قد يكـون بسيطاً أى دال بذاته وبمفـرده للقطع بوقوع الجريمة مـن جانـب المتهم، وقد يكون مركباً أى خليط أو مزيج من عدة آثار تتراكم بحيـث تقطع فى النهاية بوقوع الجريمة من جانب الجـاني، وهـو ما تطلق عليه محكمة النقض الأدلـة المباشرة وغير المباشرة، والأخيرة اصطلح الفقـه على تسميتها بالقرائن، أى استخلاص واقعـة مجهولـة – ارتكاب المتهم الجريمة- من واقعـة معلومة وثابتة، كاستخلاص ارتكـاب المتهم للسرقة من واقع ضبط المسروقات فى حوزته أو وجود بصماته على المكان محل السرقة دون مبرر أو استنتاج قتل المتهم للمجنى عليه من واقـع ضبـط السلاح المستخدم فى الحادث فى منزلـه وعليه بصماته أو ضبط ملابسه وعليها بقع دم من فصيلة دم القتيل أو وجود أجزاء من جثة القتيل فى منزل المتهم، وكذا استخلاص هتك عرض المتهم للمجنى عليه من وجود آثار لمنى يخصه على ملابس المجنى عليه، وكلما كانت القرينة قوية كان استدلال القاضى بها مقبولاً، وكلما كانت ضعيفة كان استدلال القاضى بها فاسـداً، وتكـون القرينة ضعيفة كلما كانت لا تؤدى حتماً ووفقا لطبائع الأمـور إلى ارتكاب المتهم للجريمة، ومن أمثلة القرائن الضعيفـة استنتاج الحكـم ارتكاب المتهم للتزوير من واقع كونه صاحب المصلحة من التزويـر أو من استعمال المحرر المزور أو توافـر نيـة القتل من مطلق الضغينة أو الخلافات السابقة أو القتـل للحصول على الميراث أو لقبض وثيقة التأمين التى عقدها القتيـل حـال حياتـه لصالح المتهـم، وهنا تظهر رقابة النقض على قاضى الموضـوع؛ إذ لا تتردد فى نقض حكمـه للفساد فى الاستـدلال طالمـا استخلص ارتكـاب المتهم للجريمة من قرينة ضعيفـة لا تودى وفقاً للزوم العقلى لما رتبـه الحكم عليها، وقد قضـت محكمـة النقض فى أحد أحكامهـا الحديثة بأنه: «لما كان ذلـك، وكان من المقرر أن العبرة فـى المحاكمة الجنائية هى باقتنـاع القاضـى بناءً على الأدلة المطروحـة عليه، ولا يصح مطالبته بالأخـذ بدليل بعينه فيما عدا الأحـوال التى قيده فيها القانـون بذلـك، فقد جعل القانون من سلطته أن يزن قوة الإثبات وأن يأخذ من أى دليل أو قرينة يرتاح إليها دليلاً لحكمه، ولا يلـزم أن تكـون الأدلة التى اعتمد عليها الحكم بحيث ينبـئ كل دليل منها ويقطع فى كل جزئية من جزئيات الدعوى، إذ الأدلة فـى المـواد الجنائية متساندة يكمل بعضها بعضاً، ومنها مجتمعة تتكون عقيدة القاضى فلا ينظر إلى دليل بعينه لمناقشته على حـدة دون باقـى الأدلـة، بل يكفى أن تكـون الأدلة فى مجموعها كوحـدة مؤدية إلى ما قصده الحكم منهـا ومنتجة فى اكتمال اقتناع المحكمة واطمئنانها إلى ما انتهت إليه، كما لا يشترط فى الدليل أن يكون صريحاً دالاً بنفسه على الواقعة المراد إثباتها، بـل يكفى أن يكـون استخلاص ثبوتها عن طريق الاستنتـاج مما تكشف للمحكمة من الظروف والقرائـن وترتيب النتائج على المقدمات». انظر: نقض١٣/٤/ ٢٠٢١، الطعن رقم ١٤٥٤٤ سنة ٨٨ ق.

مرتكبيهـا[١]؛ ونظراً لمـا للأدلة من أهمية كبـيرة عند الجهات القضائيـة للوصول إلى الحقيقـة، فقـد تم تقييدها بمجموعة من القيـود والضوابط، وذلك يعنـى أنه يجب أن تقوم هذه الأدلة على البرهان والمنطق، وأن يقتنع بها العقل.

٢- **تعريف الدليل الرقمي:** نتناول فيما يلى تعريف الدليل الجنائى الرقمى من خلال الإشارة إلى كلٍ من التعريفين التشريعى والفقهي، وذلك على النحو التالي:

أ- التعريـف التشريعي: عـرف المشرع المصـرى الدليل الرقمى بأنـه:«أى معلومات إلكترونيـة لها قـوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسـب أو الشبكـات المعلوماتية وما فى حكمها، ويمكـن تجميعها وتحليلها باستخدام أجهـزة أو برامـج أو تطبيقات تكنولوجيـة خاصة»[٢]، ويلاحـظ أن التعريف التشريعى حرص على إبراز جوهر الدليل الرقمي، وهى المعلومات المستخرجة من الأجهزة التقنية سواء أكانت أجهزة الحاسب الآلى أم شبكات المعلومات وما فى حكمها.

ومـن الجديـر بالذكـر أن تعريف الدليـل الرقمى قد جـاء فى صياغـة موسعة، بما يسمـح إجرائيًـا بالتوسع فيما يُمكـن اعتباره دليـلا رقميًا، فلم يضـع التعريف الوارد بالقانون سوى ضابطين يتعلقان بالمعلومات التى يتم جمعها أو استخراجها من الأجهزة والشبكـات، ويـرى الباحث أن هذين العنصرين اللذيـن تم ذكرهما أساسيين يُكمل كل منهمـا الآخر؛ لذا يجب توافرهما معًا، ويجب أيضًا أن يستمر توافرهما فى الدليل على الأقـل فى المرحلة الخاصـة بجمع واستخراج الدليـل ومرحلة توثيـق وتوصيف الدليل، وهذان العنصران هما:

العنصـر الأول: القـوة الثبوتيـة للمعلومـات المُستخرجـة: يرتبـط العنصـر الأول الـذى تضمنه تعريف الدليل الجنائـى الرقمى بثبوتية المعلومات المخزنـة أو المنقولة أو

---

(١) تعـددت تعاريـف الدليل الجنائى لـدى الفقه، فمنهم من عرفه بأنه: الوسيلة التى يستعين بهـا القاضى للوصول إلى الحقيقة، ومنهـم مـن عرفـه بأنه: الواقعـة التى يستمد منهـا القاضى الرهان علـى إثبات اقتناعـه بالحكم الذى ينتهى إليـه، والدليل يختلـف عـن الدلائل والأمارات، والتى توضع فى مرتبة إثباتية أقل من الدليل، حيث تحتمل أكثر من وجه، ولا ينعقد بها اليقين القضائي. د. أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، مرجع سابق، ص٤١٨؛ د. مأمون سلامة، الإجراءات الجنائية فى التشريع المصري، مرجع سابق، ص١٩١؛ د. هند نجيب، حجية الدليل الإلكتروني، مرجع سابق، ص٤٨.

(٢) ومن التشريعات العربية التى عرفت الدليل الرقمي، التشريع السورى الذى عرفه بأنه: «البيانات الرقمية المخزنة فى الأجهزة الحاسوبية أو المنظومات المعلوماتية، أو المنقولة بواسطتها، والتى يمكن استخدامها فى إثبات جريمة معلوماتية أو نفيها»(م١ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧ لسنة ٢٠١٢)، الصادر بتاريخ ٢٠١٢/٢/٨م.

المستخرجة أو المأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية، ويفهم ضمنيًا من القوة الثبوتية، أن المقصود هو قدرة المعلومات التى تم الحصول عليها فى إثبات ارتكاب الجريمة أمام الجهات القضائية، كما يُفهم من التعريف أن استخراج الدليل وجمعه لا يقتصر على أجهزة الحاسب فقط، حيث استخدم التعريف عبارة: «وما فى حكمها»، وهو ما يعنى أن التعريف يعتبر أن أى أجهزة أو شبكات، يمكن الاعتداد بها كدليل جنائى رقمي، مادام لدى هذه الاجهزة والشبكات القدرة على تخزين البيانات والمعلومات.

العنصر الثاني: إمكانية جمع وتحليل المعلومات المُستخرجة: أما عن العنصر الثانى الذى يجب توافره بجانب قوة ثبوتية المعلومات المستخرجة فهو إمكانية تجميع وتحليل هذه المعلومات باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة، وقد حددت اللائحة التنفيذية لقانون مُكافحة جرائم تقنية المعلومات الخواص التى يجب أن تتمتع بها البرامج التى يُمكن استخدامها فى عملية جمع أو الحصول أو استخراج المعلومات، ومن أهمها: الخواص أو الإمكانيات التى تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات، وقد حددت اللائحة نوعين من البرامج تم ذكرهما على سبيل المثال، هما:Write Blocker ، Digital Images HashK.

ومن الجدير بالذكر أن السياق الذى أتى خلاله تعريف الدليل الرقمى يُفهم منه -حسب ظاهر النص- أن مفهوم الدليل الجنائى الرقمى وما يجب أن يتوافر فيه من ضوابط وشروط تحقُّقه، تقتصر فقط على ما يتعلق بنطاق تطبيق قانون مكافحة جرائم تقنية المعلومات، فالتعاريف التى وردت بالمادة الأولى من القانون ترتبط بتطبيق أحكامه فقط، لكن من الوارد أن نجد فى التطبيقات العملية، أن المحاكم المصرية قد تتوسع فى استخدام تعريف الدليل الرقمى الوارد بقانون مكافحة جرائم تقنية المعلومات [١].

(١) قضت المحكمة الإدارية العليا فى أحد أحكامها الحديثة بأنه:«ولما كان الثابت بالأوراق أن سبب قرار الجزاء الموقع على الطاعن بخصم أجر عشرة أيام من راتبه كان بركيزة من أنه بوصفه مأمور ضرائب شبرا الخيمة بمصلحة الضرائب المصرية أساء استخدام مواقع التواصل الاجتماعى بما نشره على صفحته الخاصة على الفيسبوك يوم ٢٠١٧/٦/٤ من إساءة إلى قيادات مصلحة الضرائب واتهامه لرئيس المصلحة بأنه يردع الشرفاء ويستعين بالفاسدين والعناصر الإخوانية كرؤساء مأموريات والإساءة لوكيل الوزارة بأنه فاسد وغير شريف، والثابت من الأوراق أن تلك المنشورات كانت على صفحة (اتحاد ضرائب مصر ٢٠١٤ علم وشرف ومهنية) على الفيسبوك، وقد أنكر الطاعن صلته بهذه الصفحة ودفع اتهامه بأن طلب فى التحقيقات تتبع حساب الصفحة المذكورة لأنها لا تخصه، وأنه كان يتعين على الجهة الإدارية أن تحيل الأمر إلى الجهات الفنية =

ب- التعريف الفقهي: اهتم الفقه بوضع تعريف للدليل الرقمي، وقد تعددت تعاريفه فـى هذا السياق، حيث عرفـه البعض[١] بأنه: «أية مواد موجودة فـى شكل إلكترونى أو رقمـي»، أو هو: «أيـة بيانات مولدة أو مخزنـة فى شكل رقمي، كلمـا استخدم الحاسب الآلي، فهـى تشمل أية معلومات مدرَجة أو مولَّـدة أو محفوظة فى قواعد بيانات أو نظم تشغيلية أو برامج تطبيقات أو نماذج مولَّدة حاسوبياً، بل وحتى تعليمات محتَفظًا بها فى صورة خامدة ضمن ذاكرة حاسوبية»، كما عرفه البعض الآخر[٢] بأنه: «الدليل المأخوذ من أجهزة الكمبيوتر، ويكون فى شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعهـا وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، ويتم تقديمها فى شكل دليل يمكن اعتماده أمام القضاء، وهو مكون رقمى لتقديم معلومات فى أشكال متنوعة، مثل: النصوص المكتوبة أو الصـور أو الأصوات أو الأشكال والرسوم، وذلك من أجل اعتماده أمام الجهات القضائية لاستعماله فى الإثبات».

بينمـا عرفـه رأى آخـر[٣] بأنه: «الدليـل المشتق مـن أو بواسطة النظـم البرامجية المعلوماتية الحاسوبية، وأجهـزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصالات

= التـى تؤكـد مدى ملكيته لحساب الصفحة من عدمه رغم طلبه ذلك فـى التحقيقات وإنكاره ذلك الاتهام، وقد جانب التحقيق الـذى أجرى مع الطاعن الصواب بإغفالـه تناول أوجه دفاع الطاعن فى وجود الدليل الرقمى الذى يفيد ملكية الصفحة التى تناولـت مخالفـات الإساءة والتشهير والتجريح لقيادات مصلحة الضرائب، مما يصـم التحقيق بالقصور الجسيم لخلوه من الدليل الرقمى على ما نشر بالفيسبوك دون تمحيص لدفاعه الجوهرى وصولاً للحقيقة بدقائق تفاصيلها وحقيقة كنهتها وهو مـا خلا التحقيق من بحثـه والتيقن منه، مما يصم التحقيق بإهدار ضمانات جوهرية للطاعن بعدم تحقيق أوجه دفاعه حتى تتجلى وقائع المخالفة ويصمها بالعوار ويقوض أساسها وما ترتب عليها من الجزاء الطعين بناءً على تلك التحقيقات المبتسرة المعيبـة، مما يكون معـه القرار الطعين صدر مخالفًا مبـادئ المحاكمة العادلة المنصفة، ويستوجـب القضاء ببطلان التحقيق وبطـلان قـرار الجزاء المطعون عليه كأثر مترتب على ذلك العوار، ويتعـين القضاء بإلغاء الحكم المطعون فيه والقضاء ببراءة الطاعـن ممـا هو منسوب إليـه». أنظر: حكم المحكمة الإدارية العليا، جلسة ٢٠٢١/٥/٢٢ فـى الطعن رقم ٩٦٨٤٥ لسنة ٦٤ ق عليا، الصادر فى الدعوى التأديبية رقم ٤٠ لسنة ٥٢ ق.

(1) Ireland Law Reform Commission, "Documentary and Electronic Evidence", Consultation paper, December 2009, p. 8.

(2) Casey Eoghan (2004), Digital Evidence and Computer Crime, Third Edition, Published by Elsevier Inc, London, 2011, p.7.

ومـن الفقـه العربي، انظـر: د. ممدوح عبـد الحميد عبد المطلب، البحـث والتحقيق الجنائـى الرقمى فى جرائـم الحاسب الآلى والإنترنت، القاهرة، دار الكتب القانونية، ٢٠٠٦، ص٨٨.

(٣) د. أحمـد محمد العمر، الدليل الرقمى وحجيته فى الإثبات الجنائي، مجلة الدراسات الفقهية والقانونية، العدد الثالث، يناير ٢٠٢٠، المعهـد العـالى للقضـاء، سلطنة عمان، صـ١٣٢؛ عبد الناصر محمد محمـود فرغلى وآخر، الإثبـات الجنائى بالأدلة الرقميـة من الناحيتين القانونية والفنية- دراسة تطبيقية مقارنة، المؤتمر العربى الأول لعلوم الأدلة الجنائية والطب الشرعى الذى نظمته جامعة نايف العربية للعلوم الأمنية خلال الفترة (١٢-١٤/١١/٢٠٠٧)، الرياض، ص١٣.

مـن خلال إجـراءات قانونية وفنية، لتقديمهـا للقضاء بعد تحليلها علميـاً أو تفسيرها فـى شكل نصوص مكتوبـة، أو رسومات أو صور وأشكال وأصوات، لإثبات وقوع الجريمة ولتقريـر البراءة أو الإدانة فيها»، ويعرفه البعض الآخر[١] بأنه:«معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابيـة المخزنـة فى أجهـزة الحاسـب الآلى وملحقاتها وشبكـات الاتصال، ويمكن استخدامهـا فى أى مرحلة من مراحل التحقيـق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جانٍ أو مجنى عليه»، بينما عرفته المنظمة الدولية لأدلة الحاسـب IOCE بأنه: «المعلومـات المخزنة أو المتنقلة فى شـكل ثنائي، ويمكن أن تعتمد عليها المحكمة»[٢].

ويتضـح لنا مـن التعاريف السابقـة أنه بينما ركـز التعريف التشريعـى على جوهر الدليل ومضمونه، بينما نجد التعاريف الفقهية ركزت على عدة جوانب موضوعية وفنية وقانونيـة فى تعريف الدليـل الرقمي، وهو نهج محمود، حيث يحسـب له تصديه لمسألة التعريـف بالدليل الرقمى فى وقت تأخر فيه المشـرع المصرى عن إصدار هذا القانون، ومـن ثَمَّ تأخره فـى بيان ماهيـة وطبيعة هذه النوعيـة المستحدثة مـن الأدلة الجنائية وحجيتها القانونية.

ثانيـاً- الأثر الرقمـى والدليل الرقمي: يقصد بالأثر الرقمـى كل ما ينتج عن تفاعل المستخـدم مـع وسائل تقنيـة المعلومـات وأجهزة الحاسـب الآلي، حيث ينتـج عن هذا التفاعـل مجموعـة كبيرة من الآثـار الرقمية (يطلق عليهـا أحياناً البصمـات الرقمية أو الأشيـاء الاصطناعيـة)، إلا أن هذا الأثـر يتحول إلى دليل رقمـى إذا نجح الخبراء التقنيـون باستخـدام الأجهزة والتطبيقـات التكنولوجية الخاصة فـى الربط بينه وبين الجريمـة المرتكبة، ومن ثَمَّ إثبات الصلة بينه وبين مرتكب الجريمة، ويذهب البعض[٣]

---

(١) د. محمـد الأمـين البشري، التحقيق فى الجرائـم المستحدثة، الرياض، مطبوعات جامعة نايـف العربية للعلوم الأمنية، ط١، ٢٠٠٤، ص٢٣٤.

(2) Casey Eoghan (2004), Digital Evidence and Computer Crime, op. cit., p.7.

ومن الفقه العربي، انظر: د. هند نجيب، حجية الدليل الإلكتروني، مرجع سابق، ص٤٩؛ عبد المطلب طارهي، الإثبات الجنائى بالأدلة الرقمية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر، ٢٠١٤، ص١٤.

(٣) د. أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، ج١، طبعة مطبعة جامعة القاهرة، ١٩٧٩، ص٣٧٥.

إلى وجوب التزام مأمورى الضبط القضائى أو الخبراء بالضمانات التى توفر الثقة فى الأدلة المادية، بمعنى الالتزام بالشرعية فى كل إجراء يتخذه أو كل خطوة يخطوها، وإلا كان البطلان للإجراء، وعدم الأخذ بالدليل المستمد من ذلك الإجراء الباطل[١].

ثالثـاً- خصائص الدليل الرقمي: يتسم الدليل الرقمـى بعدد من الخصائص التى تميـزه عن الدليـل الجنائى التقليدي، ومن أبـرز خصائص الدليـل الرقمى التى يتفق عليها الفقه ما يلي:

١- الطابـع العلمى للدليل الرقمي: فالتعامل مع الدليـل الرقمى يتطلب دراية علمية وفنيـة فـى التعامل معه، فلا يمكن استخراجه أو حتى اكتشافـه، إلا من خلال دراسات علمية حول كيفية ذلك[٢].

٢- الطابـع التقنى للدليـل الرقمي: إن الدليل الرقمى ذو طابـع تقنى وفني، ويتكون من معلومات تتجسد فى صورة إلكترونية، لا يتم إدراكها إلا باستخدام أجهزة الحاسب الآلي، أو الاعتمـاد علـى تقنية المعلومات[٣]، ومن ثَمَّ فالدليل الرقمى لا يكون إلا فى بيئة رقمية[٤].

٣- الطابـع المعنوى الافتراضـى للدليل الرقمـي: يتكون الدليل الرقمـى من بيانات ومعلومـات ذات هيئـة إلكترونية غير ملموسـة، لا تدرك بالحواس العاديـة، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية HARDWARE، واستخدام نظم برامجية حاسوبية SOFTWARE [٥]، فالأدلة الرقمية ليست أقل مادية من الدليل

---

(١) د. حسين إبراهيم، الإثبات الجنائي، القاهرة، مطبعة كلية الشرطة، ٢٠٠٢، ص٢١.

(٢) د. عمـر محمـد بـن يونـس، الجرائم الناشئة عـن استخدام الإنترنـت، رسالة دكتـوراه، جامعة عين شمـس، ٢٠٠٤، ص٩٧٧؛ د. هنـد نجيب، حجية الدليـل الإلكتروني، مرجع سابق، ص٥١؛ د. وليد المعـداوي، دور الشرطة فى حماية الحياة الخاصة من أخطار المعلوماتية، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، ٢٠١١، ص٣٥٢؛ د. أحمد سعد الحسيني، الجوانب الإجرائية، مرجع سابق، ص١٥٣؛ د. وهيبة لعوارم، الدليل الرقمى فى مجال الإثبات الجنائي، مرجع سابق، ص٧٢.

(٣) د. هنـد نجيـب، حجية الدليل الإلكـتروني، مرجع سابق، ص٥٢؛ د. سامح أحمد بلتاجى موسـى، الجوانب الإجرائية للحماية الجنائية لشبكة الإنترنت، رسالة دكتوراه، جامعة الإسكندرية، ٢٠١٠، ص٣٠٨؛ د. أحمد سعد الحسيني، الجوانب الإجرائية، مرجع سابق، ص١٥٣؛ د. وهيبة لعوارم، الدليل الرقمى فى مجال الإثبات الجنائي، مرجع سابق، ص٧٢.

(٤) د. خالـد ممـدوح إبراهيم، الإثبـات الإلكترونى فى المواد الجنائية والمدنيـة، الإسكندرية، دار الفكـر الجامعي، ٢٠٢٠، ط١، ص٤٠.

(٥) عبـد الناصـر محمد محمود فرغلى وآخـر، الإثبات الجنائي، مرجع سابق، ص١٤؛ د. هند نجيـب، حجية الدليل الإلكتروني، مرجع سابق، ص٥١؛ د. عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص٩٧٧.

المـادى فحسـب، بل تصل إلى درجـة التخيلية فى شكلها وحجمهـا ومكان وجودها غير المعلـن، فالدليل الرقمـى يشمل كافة أشكال وأنـواع البيانات الرقميـة الممكن تداولها، بحيـث يكـون بينها وبين الجريمة رابطة من نوع ما، وتتصـل بالضحية على النحو الذى يحقق هذه الرابطة بينها وبين الجاني[١].

٤- **الطابـع الديناميكـى للدليل الرقمـي:** الأدلة الرقمية ذات طابـع ديناميكى فائق السرعة، تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان [٢].

٥- **إمكانيـة نسـخ الدليل الرقمـى بشكل مطابق:** يمكـن استخراج نسـخ من الأدلة الرقميـة مطابقة للأصل ولهـا القيمة العلميـة والحجية الثبوتية ذاتهـا، وهذا الأمر لا يتوافر فى الأدلة التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير، عن طريق نسخ طبق الأصل من الدليل[٣].

٦- **صعوبـة التخلص من الدليـل الرقمـي:** إن الأدلـة الرقمية يمكـن استرجاعها بعـد محوهـا، وإصلاحها بعد إتلافهـا، وإظهارها بعد إخفائها، مما يـؤدى إلى صعوبة الخلاص منها، وهى خصيصـة من أهم خصائص الدليل الرقمـي، بالمقارنة بالدليل التقليدي، ويتم ذلك من خـلال استخدام العديد من البرامج الحاسوبية التى وظيفتها استعادة البيانات التى تم حذفها أو إلغاؤها، سواء تم ذلك عن طريق حذف البيانات أو المعلومـات، أو تم عمـل إعادة تهيئة أو تشكيل للقرص الصلب، مما يعنى صعوبة إخفاء الجانى لجريمته عن أعين رجال العدالة الجنائية [٤].

٧- **الدليـل الرقمـى يكشف عن شخصيـة المجرم:** يمكن من خـلال الدليل الرقمى

---

(١) د. عمر محمد بن يونس، مذكرات فى الإثبات الجنائى عبر الإنترنت، ندوة الدليل الرقمى التى نظمتها جامعة الدول العربية، خلال الفترة (٥-٨ مارس٢٠٠٦)، القاهرة، ص١٤.

(٢) عبـد الناصـر محمد محمود فرغلى وآخـر، الإثبات الجنائي، مرجع سابق، ص١٥؛ د. هند نجيـب، حجية الدليل الإلكتروني، مرجع سابق، ص ص٥٢ و٥٥.

(٣) عبـد الناصـر محمد محمود فرغلى وآخـر، الإثبات الجنائي، مرجع سابق، ص١٥؛ د. هند نجيـب، حجية الدليل الإلكتروني، مرجع سابق، ص٥٤.

(٤) عبـد الناصـر محمد محمود فرغلى وآخـر، الإثبات الجنائي، مرجع سابق، ص١٥؛ د. هند نجيـب، حجية الدليل الإلكتروني، مرجع سابق، ص٥٢؛ د. أحمد سعد الحسيني، الجوانب الإجرائية، مرجع سابق، ص١٥٧؛ د. وهيبة لعوارم، الدليل الرقمى فى مجال الإثبات الجنائي، مرجع سابق، ص٧٢.

رصـد المعلومات عن الجانى وتحليلها فى الوقت ذاته، كما يمكن للدليل الرقمى تسجيل تحركات الفرد وعاداته وسلوكياته وبعض الأمور الشخصية عنه[١].

رابعـاً – تقسيم الأدلة وتصنيـف الدليل الرقمي: يمكن تقسيـم الأدلة الجنائية إلى أربعـة أنـواع رئيسية، هـي: الأدلـة القانونية، وهى التـى حددها المشـرع، وعين حالات استخدامهـا، ومدى حجية كل منهـا، والأدلة الفنية، وهى التـى تنبعث من رأى الخبير الفنـى حـول تقدير أو تقـديم دليل مادى أو قولى وفـق معايير ووسائـل علمية معتمدة، والأدلة المادية، وهى الناتجة عن عناصر مادية ناطقة بنفسها، وتؤثر فى اقتناع القاضى بطريـق مباشـر، والأدلة القوليـة، والتى تنبعث مـن أشخاص أدركـوا معلومات مفيدة للإثبات بإحدى حواسهم كالاعتراف وأقوال الشهود[٢]، وقد اختلف الفقه حول تصنيف الدليـل الرقمى بـين اتجاهين: **الأول:** يـرى الدليل الرقمى مرحلـة متقدمة من الدليل المادي[٣]، **والثاني:** يرى أن الدليل الرقمى له طبيعة خاصة، ويشكل إضافة جديدة لأنواع الأدلة الأخرى[٤]، ويعتقد الباحث أن الرأى الأخير هو الأولى بالتأييد بالنظر إلى الفروق الواضحة بين الدليل المادى التقليدى والدليل الرقمي.

خامساً– أوجـه التمييز بين الدليل التقليدى والدليل الرقمـي: يتسم الدليل الرقمى بعـدد من السمات التـى تميزه عن غيره من الأدلـة التقليدية، ومن أبرزهـا: أنه سريع الـزوال والتغيير، وهو ما يثير إشكالية حفظ الدليل والحصول عليه، علاوة على صعوبة الوصـول إليه حينما يستخدم المشتبه فيهم نظامـاً للتشفير، مما يجعل الحصول عليه بـدون رمـز التشفير أمـراً صعباً ويستغـرق وقتاً طويـلاً، فضلاً عن وجـوده فى أماكن جغرافية متعددة، ومن ثَـمَّ صعوبة الحصول عليه خارج نطاق الولاية القضائية للدول،

---

(١) د. ممـدوح عبـد الحميد عبد المطلب، استخدام بروتوكول TCP IP فى بحـث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمى الأول حـول الجوانـب القانونية والأمنية للعمليـات الإلكترونية، الذى نظمه مركز البحوث والدراسـات بأكاديمية شرطة دبي، خلال الفترة (٢٦-٢٠٠٣/٤/٢٨)، إمارة دبي، دولة الإمارات العربية المتحدة، ص ص٦٤٩، ٦٥٠؛ د. هند نجيب، حجية الدليل الإلكتروني، مرجع سابق، ص٥٤؛ د. وهيبة لعوارم، الدليل الرقمى فى مجال الإثبات الجنائي، مرجع سابق، ص٧٣.

(٢) د. وهيبة لعوارم، الدليل الرقمى فى مجال الإثبات الجنائي، مرجع سابق، ص٧٤.

(٣) د. هـلالى عبـد اللاه أحمد، حجيـة المخرجات الكمبيوترية فى الإثبات الجنائي، القاهـرة، دار النهضة العربية، ١٩٩٧، ط١، ص ص١٤-٢٢.

(٤) د. عمـر محمـد بـن يونس، الإجراءات الجنائية عبر الإنترنـت فى القانون الأمريكي، بدون ناشـر، ٢٠٠٦، ص٩٧٧؛ د. محمد الأمين البشري، التحقيق فى الجرائم المستحدثة، مرجع سابق، ص٢٣٥؛ د. محمد أحمد منشاوي، سلطة القاضى الجنائى فى تقدير الدليل الإلكتروني، مجلة الحقوق، جامعة الكويت، المجلد ٣٦، العدد٢، يونيو ٢٠١٢، ص٥٢٩.

بالإضافة إلى العديد من الإشكاليات التى تخص مدى مقبوليته أمام القضاء الجنائي، وتتبلور أبرز ملامح التمييز بين كل من الدليلين، فيما يلي:

١- الدليل التقليدى دعامته ورق ملموس، بعكس الدليل الرقمي، فإن دعامته برامج الحاسب الآلي، أو أى وسائط تقنية حديثة، ومن ثَمَّ يحتاج الدليل الرقمى إلى وسائط تقنية لقراءته، بينما يمكن قراءة الدليل المادى بسهولة ومباشرة من دعامته الورقية.

٢- الدليل الرقمى يسهل البحث عنه وإدارته، والتعديل فيه، وتخزينه واسترجاعه، وتبويبه، باستعمال بعض خصائص البرمجة الإلكترونية، بعكس الدليل المادى الذى يثبت على حالته التى أعد بها.

٣- الدليل الرقمى ووفقاً لدعامته الإلكترونية التى تستوعب معلومات كبيرة تبعاً لحجم الوسيط ومقدار المعلومة، فإن ذلك يتيح الفرصة لعرض عدد غير محدود من المستندات، فى مساحة صغيرة من الوسيط الإلكتروني.

سادساً - تقسيمات الدليل الرقمى: تتباين صور الدليل الرقمي، وقد قسمها البعض[١] إلى ثلاثة أقسام رئيسية: **(الأول)**:

أدلة رقمية تخص أجهزة الحاسب الآلى وشبكاتها، **و(الثاني)**: أدلة رقمية تخص شبكة المعلومات الدولية «الإنترنت»، **و(الثالث)**: أدلة رقمية تخص بروتوكولات تبادل المعلومات بين أجهزة شبكة الإنترنت.

بينما يشير البعض الآخر إلى تقسيم ثان قررته وزارة العدل الأمريكية سنة ٢٠٠٢، إلى ثلاث مجموعات، تشمل[٢]: (الأولى): السجلات المحفوظة فى الحاسب الآلي، كالوثائق المكتوبة والمحفوظة، مثل: رسائل البريد الإلكتروني، وملفات النصوص المكتوبة كالوورد، ورسائل غرف المحادثات عبر الإنترنت، و(الثانية): السجلات التى تم إنشاؤها بواسطة الحاسب الآلي، وتعتبر مخرجات برامج الحاسب الآلى التى لم يتدخل فيها الإنسان، كسجلات الهاتف، وفواتير السحب الآلى ATM، و(الثالثة): السجلات التى

(١) د. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائى الرقمي، مرجع سابق، ص٨٨؛ د. وهيبة لعوارم، الدليل الرقمى فى مجال الإثبات الجنائي، مرجع سابق، ص٨٣.

(٢) عبد الناصر محمد محمود فرغلى وآخر، الإثبات الجنائي، مرجع سابق، ص١٤؛ د. هند نجيب، حجية الدليل الإلكتروني، مرجع سابق، ص٥٠؛ د. أحمد سعد الحسيني، الجوانب الإجرائية، مرجع سابق، ص١٥٦؛ د. وهيبة لعوارم، الدليل الرقمى فى مجال الإثبات الجنائي، مرجع سابق، ص٨٣.

جـزء منها تم حفظه بالإدخـال والجزء الآخر تم إنشاؤه بواسطـة الحاسب الآلي، ومن أمثلتهـا أوراق العمـل المالية التى تحتـوى على مدخلات تم معالجتهـا من خلال برامج أوراق العمل، مثل EXCEL بإجراء العمليات الحسابية عليها.

ومن ثَـمَّ يفترض التنوع فى صور الدليل الرقمي، تنـوع وتعدد وسائل الحصول عليه مـن أجهزة الحاسـب الآلى والشبكات المعلوماتية، ومـن ثَمَّ يرى البعض [١] أن مسألة استخلاص الدليل الرقمى من مخرجات الحاسب الآلى والشبكات المعلوماتية أن الدليل المستمـد منهـا يظل رقميـاً، حتى وإن اتخذ هيئـة أخرى، ويكون اعـتراف القانون بهذه الهيئة الأخرى مؤسساً على طابع افتراضى مبناه أهمية الدليل الرقمى ذاته، وضرورته فـى عمليـة الإثبات الجنائى فـى جرائم تقنية المعلومـات، ومن ثَمَّ يلـزم اتخاذ مسلك الافتراض من حيث اعتباره دليلاً أصلياً.

سابعـاً- الدليل الرقمى وعلم الأدلة الجنائية الرقميـة: يقصد بالدليل الرقمي، أى محتـوى فى شـكل إلكترونى أو رقمـي، ناجم عن استخـدام الحاسـب الآلى أو الشبكة المعلوماتيـة أو أية وسيلة من وسائل تقنية المعلومـات، بينما يقصد بعلم الأدلة الجنائية الرقمية، أحد فروع علوم الأدلة الجنائية، والذى يتناول البحث عن البيانات المخزنة فى أجهـزة إلكترونية، والحصول عليها ومعاملتها وتحليلها والإبلاغ بها، ومن ثَمَّ يعنى علم الأدلة الجنائية الرقمية أو التحليل الجنائى الرقمى باسترجاع الآثار الرقمية الحاسوبية والتحقيق فيها، ولتعقب هـذه الآثار، يستفيد خبراء الأدلة الجنائية الرقمية من قابلية الحواسيب لتخزين وتسجيل وحفـظ بيانات عن أغلب الأنشطة التى تقوم بها، وبالتالى التـى يقـوم بها مستخدموهـا[٢]، ومن ثَمَّ تتمثـل مهمة خبراء الأدلـة الجنائية الرقمية فـى إيجاد نسخ مطابقة تماماً للدليل الرقمـي، أو صور غير مضطربة منه، تحتوى على نسخـة مفصلة بقدر الإمكان، وفحص البيانات وتحليلها، دون إلحاق أى اضطراب بها، بالإضافة إلى القدرة على استرجاع الملفات المحذوفة أو التالفة[٣].

---

(١) د. عمـر محمد بن يونس، مذكرات فـى الإثبات الجنائى عبر الإنترنت، مرجع سابق، ص١٢؛ د. وهيبة لعوارم، الدليل الرقمى فى مجال الإثبات الجنائي، مرجع سابق، ص٨٤.

(٢) انظر: دراسة مكتب الأمم المتحدة حول الجريمة السيبرانية، مرجع سابق، ص٢٣٠.

(٣) غوتمـان بي، الحـذف الآمن للبيانات من الذاكرة المغناطيسية وذاكرة الحالة الصلبـة، وقائع الندوة الأمنية السادسة لاتحاد الحوسبة التقنية المتقدمة، ١٩٩٦، مشار إليه: دراسة مكتب الأمم المتحدة، المرجع السابق، ص٢٣١.

ثامناً- الإطار الـدولى والإقليمى لمكافحة جرائم تقنية المعلومات والتعامل مع الأدلة الرقميـة: يمكن القول إن الإطار الدولى والإقليمى للتعامـل مع الأدلة الرقمية هو بذاته الإطار لمكافحة جرائم تقنية المعلومات، ومن أبرز الصكوك الدولية والإقليمية:

على الصعيد الأوروبي: الاتفاقيـة الأوروبية (اتفاقية مجلس أوروبا) بشأن الجريمة السيبرانية لعـام٢٠٠١، والتى تعرف باسم اتفاقية بودابست [١]، والبروتوكول الإضافى للاتفاقية المعنى بتجريم أفعال ذات طبيعة عنصرية أو كراهية الأجانب المرتكبة بواسطة النظم الحاسوبية، ومن الجدير بالذكر أن المفوضية الأوروبية فى سبيلها لطرح مشروع مسـودة بروتوكول إضافى ملحق باتفاقيـة بودابست فى مجال تأمين الأدلة الإلكترونية، والـذى يهدف إلى تعزيز التعاون بـين الأطراف فى مجالى تعقـب الجرائم السيبرانية وتأمين الأدلة الرقمية.

أضـف إلى ذلك قـرارى الاتحاد الأوروبى لعـام ٢٠٠١ بشأن الاحتيـال والتزوير فى وسائـط الدفع غير النقدية، ولعام ٢٠٠٥ بشأن الهجمات ضد نظم المعلومات، والمشروع التوجيهـى للاتحاد الأوروبى لعـام ٢٠١٠ بشأن الهجمات ضد نظـم المعلومات، وتوجيه الاتحـاد الأوروبى لعـام ٢٠١١ بشأن مكافحـة الاعتداء الجنسـى والاستغلال الجنسى للأطفال واستغلال الأطفال فى المواد الإباحية.

علـى الصعيد العربي: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، والقانـون العربى النموذجى لمكافحة جرائـم تقنية أنظمة المعلومات لعام ٢٠٠٤ (قانون الإمارات النموذجي).

على الصعيد الإفريقي: مشروع اتفاقيـة الاتحاد الإفريقى بشأن إنشاء إطار قانونى للمساعدة فى الأمن السيبرانى فى إفريقيا لعام ٢٠١٢ [٢]، ومشروع القانون النموذجى للكوميسا (السوق المشتركة لشرق وجنوب إفريقيا) لعام ٢٠١١ بشأن الأمن السيبراني [٣]،

---

(١) على الرغم من أن اتفاقية بودابست هى اتفاقية إقليمية، وهى فى الأصل أوروبية المنشأ، إلا أنها اتفاقية ذات طابع دولي، فهى مفتوحة للدول الأخرى لطلب الانضمام إليها من خارج أوروبا، ويبلغ عدد الدول الأطراف فى هذه الاتفاقية ٦٣ بلداً، وقد وقعت هذه الاتفاقية بتاريخ ٢٠٠١/١١/٢٣، من ٢٦ دولة أوروبية وكل من الولايات المتحدة الأمريكية وكندا واليابان وجنوب إفريقيا.

(٢) تتضمن الاتفاقية المادة (١/٢٤) والخاصة بمقبولية الأدلة والسجلات الإلكترونية.

(٣) تتضمن الاتفاقية المادة (٥/أ) والخاصة بمقبولية الأدلة والسجلات الإلكترونية.

والمشروع التوجيهى للإيكواس (الجماعة الاقتصادية لدول غرب إفريقيا) لعام ٢٠٠٩ بشأن مكافحة الجريمة السيبرانية داخل دول غرب إفريقيا[١].

أضف إلى هذه المواثيق الإقليمية، اتفاقية كومنولث الدول المستقلة بشأن التعاون فى مكافحة الجرائم المتعلقة بالمعلومات الحاسوبية[٢]، واتفاقية منظمة شنغهاى للتعاون فى مجال أمن المعلومات الدولية.

على الصعيد الدولي: علاوة على البروتوكول الاختيارى الملحق باتفاقية حقوق الطفل لعام ٢٠٠٠ بشأن بيع الأطفال وبغاء الأطفال واستغلال الأطفال فى المواد الإباحية، والنصوص التشريعية النموذجية لعام ٢٠١٠ بشأن الجرائم السيبرانية والأدلة الإلكترونية للاتحاد الدولى للاتصالات والجماعة الكاريبية والاتحاد الكاريبى للاتصالات [٣].

المطلب الثاني

مشروعية الدليل الرقمى ومقبوليته أمام القضاء الجنائي

أولاً- مشروعية الدليل الرقمي: يستلزم الدليل الرقمى أن تكون وسيلة الحصول عليه مشروعة، وهو ما يتحقق من خلال ما يلي:

١- إجراءات الحصول على الدليل تمت وفق القانون: أى ضرورة ارتكان الدليل على إجراءات مشروعة، سواء كانت تلك الإجراءات قد صدرت من قبل القاضى بصورة مباشرة أو غير مباشرة، أو من قبل المتهم واعترافه واستجوابه، أو من قبل الغير بعد القيام بالقبض عليه أو تفتيشه أو تفتيش مسكنه، أو ممارسة أى عمل من أعمال الخبرة الفنية [٤].

---

(١) تتضمن الاتفاقية المادة (٣٤) الخاصة بمقبولية الأدلة والسجلات الإلكترونية.

(٢) تتضمن الاتفاقية أحكاماً تخص الأدلة الرقمية، نذكر منها المادتين (٣/٢٠) و (١١) الخاصتين بمقبولية الأدلة، والمادة (٥) الخاصة بعبء الإثبات فى جرائم تقنية المعلومات، والمادة (٦) الخاصة بقاعدة أفضل دليل، والمادة (٧) الخاصة بافتراض سلامة الدليل، والمادة (٨) بشأن معايير التسجيل والتحفظ على الأدلة، والمادة ١٢ الخاصة بمقبولية التوقيع الإلكتروني.

(٣) تعد هذه الاتفاقية أكثر الاتفاقيات الدولية تنظيماً لموضوع الأدلة الرقمية، حيث تتضمن الاتفاقية المواد (٥) و (١/٧) و (١٢) الخاصة بمقبولية الأدلة، والمادة (٦) الخاصة بقاعدة أفضل دليل، والمادة (٢/٧) الخاصة بافتراض سلامة الدليل، والمادة (٨) الخاصة باعتبار المطبوعات أفضل دليل، والمادة (٩) الخاصة بعبء الإثبات فى جرائم تقنية المعلومات، والمادة (١٠) بشأن معايير التسجيل والتحفظ على الأدلة، والمادة (١٤) الخاصة بمقبولية التوقيع الإلكتروني، والمادتين (١٦) و (١٧) الخاصتين بالأدلة والسجلات الإلكترونية والوثائق الأجنبية من دول أخرى.

(٤) د. هند نجيب، حجية الدليل الإلكتروني، مرجع سابق، ص٥٦.

٢- التوصل إلى الدليل عن طريق إرادة حرة: بمعنى أن الحصول عليه قد تم دون أى اعتداء على إرادة المتهم أو إرادة الغير، بحيث يكون طريقة العثور عليه خالية من أى عيب يشوب تلك الإرادة، ومن أمثلة ذلك: استخدام التعذيب أو الإكراه المادى أو المعنوى مع المشتبه به من أجل فك شفرة نظام معلوماتي، أو الوصول إلى دائرة حل التشفير، أو الوصول إلى ملفات البيانات المخزنة[١].

ومن التطبيقات القضائية حول مشروعية إجراءات الحصول على الدليل، ما قررته إحدى المحاكم الأمريكية بشأن مشروعية قيام أجهزة إنفاذ القانون بجمع معلومات بشأن وقوع جريمة ما، من بين المعلومات والبيانات التى يتشاركها المتهم مع أصدقائه على مواقع التواصل الاجتماعي، حيث دفع المتهم ببطلان الدليل الذى تم الحصول عليه من حسابه الشخصى على فيسبوك، على سند من القول إن أجهزة الشرطة قد انتهكت حقوقه المنصوص عليها فى التعديل الرابع على الدستور الأمريكي، وكان المتهم قد قام بضبط إعدادات الخصوصية الخاصة بحسابه الشخصى على موقع التواصل الاجتماعى (فيسبوك) بصورة يمكن معها «للأصدقاء» فقط رؤية ما يقوم بإرساله على حسابه من مراسلات.

وتمكنت أجهزة الشرطة من الحصول على دليل يجرم المتهم من خلال أحد الأشخاص (الشهود)، وقد صادف أن يكون هذا الشاهد أحد (أصدقاء) المتهم على موقع التواصل الاجتماعي، وقد رفضت المحكمة الدفع وقضت بأنه: «إذا كانت إعدادات الضبط المتعلقة بالخصوصية على موقع التواصل الاجتماعى (فيسبوك) تسمح برؤية المراسلات من قبل (الأصدقاء)، فتستطيع أجهزة الدولة الولوج إلى هذه المعلومات من خلال تعاون أحد الأشخاص من «أصدقاء» المتهم على موقع التواصل الاجتماعى دون أن يُشكِّل ذلك انتهاكًا للتعديل الرابع، بينما يعتقد المتهم -بدون أدنى شك- أن حسابه لن تتم مشاركته من قبل سلطات إنفاذ القانون، ليس هناك أى مبرر للتوقع بأن (الأصدقاء) سيحافظون على سرية الحساب، وكلما اتسعت دائرة (الأصدقاء)، زاد الاحتمال بأن مراسلات المتّهم ستتم رؤيتها من قبل شخص غير متوقع أن يراها، وأن توقعات المتهم المشروعة فى الحفاظ على خصوصيته تنتهى عندما ينشر مراسلاته إلى

(١) المرجع السابق، ص٥٦.

«أصدقائـه»؛ لأن هؤلاء (الأصدقاء) يملكون الحرية فى استخدام هذه المعلومات كيفما يشاءون بما فى ذلك مشاركة هذه المعلومات مع أجهزة الدولة»[١].

بينمـا فى قضية أخرى، قـررت إحدى المحاكم الأمريكية رفضـ الدليل المستمد من المراقبـة الإلكترونيـة لأحد الأشخاصـ؛ لكونها تمت بشكل ينم عن عـدوان على الحياة الخاصة، وكانت المباحث الفيدرالية الأمريكية فى هذه القضية قد قدمت طلباً للمحكمة لـلإذن بمراقبة حسـاب أحد الأشخاص لكونه يستخدم الإنترنـت فى أنشطة إجرامية، وتمكنت من التوصل إلى أدلة تثبت ذلك[٢].

وفـى قضية ثالثـة، قضت محكمة النقضـ الفرنسية فـى حكم لها بـأن: «التسجيل الهاتفى الذى يجريه أحد الأطراف بدون علم صاحب الأقوال المسجلة يشكل طريقة غير مشروعة تؤدى إلى عدم قبوله برهاناً، وقد نقضت بذلك حكم محكمة الاستئناف بباريس الذى أخذ بالتسجيل»، حيث ذهبت محكمة النقض الفرنسية (الغرفة التجارية) إلى أن تسجيـل مكالمـة هاتفية من قبل أحد الأطـراف دون علم صاحب الأقـوال يشكل وسيلة ماكـرة، ممـا يمنع قبول تقديمه كدليل، حيث بنت محكمـة النقض حكمها بنقض حكم محكمـة استئنـاف باريس الصادر فى ٢٠٠٧/٦/١٩ على مخالفـة ذلك لأحكام الفقرة الأولى مـن المادة السادسة من الاتفاقية الأوروبية لحقـوق الإنسان وحرياته الأساسية، وكانت محكمة الاستئناف بباريس قد قررت أن تسجيلات المكالمات الهاتفية المقدمة من الطـرف الرافـع للدعوى وليس من المحققين أو من المقـرر، لا يمكن رفضها بمجرد علة الحصـول عليها بصورة ماكرة، وبأنها تعتبر مقبولة متى خضعت للمناقضة، حيث يعود للمحكمة تقدير قيمتها الثبوتية[٣].

ومن الجدير بالذكر أن الفقه والقضاء الجنائى يتوسعان فى تحديد نطاق مشروعية الدليـل الرقمـي، بحيث لا تقتصر مشروعية إجراءات الحصـول عليه على مجرد اتباع

---

(١) انظـر: حكـم صادر من محكمة المقاطعـة الجنوبية بنيويورك بالولايات المتحدة الأمريكيـة بتاريخ ١٠ من أغسطس عام ٢٠١٢ فى قضية:
United States v. Meregildo, No. 11 Cr. 576(WHP), 2012 WL 3264501, at *2 (S.D.N.Y. Aug. 10, 2012).

(٢) د. عمـر محمـد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص٩٧٧؛ د. أحمد سعد الحسيني، الجوانب الإجرائية، مرجع سابق، ص١٥٢.

(3) انظر: Cass. Com. 3 Juin 2008, No. 07-1714707-17196, bull. 4, 2008, no.112.

قارن كذلك: حكم محكمة النقض الفرنسية (الدائرة الجنائية)
Cass. Crim. 31 Jan 2007, No. 383-82-06, bull. Crim., 2007, no.27.

القواعـد القانونيـة المقررة، وإنما يجـب أن تتفق كذلك مع القواعـد الثابتة فى وجدان المجتمع [١].

ثانياً- مقبوليـة الدليل الرقمى أمام القضاء الجنائي: سبق أن أشرنا إلى أن الدليل الرقمـى هو أية مادة تتخذ الشكل الإلكترونى أو الرقمي، ونظراً للخصائص التى يتمتع بها الدليل الرقمي، والتى من أبرزها الطابع المعنوى المتغير لهذا الدليل وقابليته للتغيير والتعديـل، وأهميته فى الإثبات الجنائـى والارتكان عليه فى تقريـر المسئولية الجنائية للأشخاص وإدانتهـم بنـاءً على هـذه الأدلـة، فقد اتجـه القضاء الجنائـى فى بعض الـدول إلى وضـع بعض القواعـد أو المعايير لتقدير مـدى قبول الأدلـة الرقمية والتأكد مـن موثوقيتها، وبحث مـدى إمكان الارتكان عليهـا فى الإجـراءات القضائية، وتتبلور أبـرز القواعد لتقرير مقبوليـة الدليل الرقمى أمام القضـاء الجنائى فى ضرورة تيقن المحكمـة من سلامة الدليل الرقمى وصحتـه، وعدم تعرضه لأى محاولة للعبث به، ومن ثَمَّ يقع على عاتق سلطة الاتهام إثبات أن هذا الدليل بداءةً قد تم الحصول عليه بطريق مشروع، وثانياً إثبات ما يسمى باستمرارية الدليل؛ أى إن حالة المعلومات الرقمية كدليل لم يطرأ عليها أى تعديل أو تغيير يشكك فى مصداقيتها فى كشف وقائع الجريمة طوال فترة الإجراءات القضائية منذ تاريخ التحفظ عليه وحتى صدور حكم فى الدعوى.

وتمثـل إمكانية تعديل الأشيـاء الاصطناعية الخاصة بالحاسـب أو الكتابة فوقها أو حذفهـا بسهولـة تحدياً يتعلـق بمصداقية هذا الدليـل أمام المحكمـة، ووجوب التحقق مـن مصـادر المعلومـات الرقمية، ومن ثَـمَّ تتطلب عمليـة جمع الآثـار الرقمية بمسرح جريمـة تقنيـة المعلومات خبراء متخصصين فى مجـال المعلوماتية، وهم من يناط بهم استخلاص وجمع الأدلة الرقمية من أجهزة الحاسب الآلى والنظم المعلوماتية والشبكات المعلوماتيـة، ومن وسائل تقنية المعلومـات المختلفة، ويقع على عاتقهم مهمة جمع الدليل وحفظه بالصورة التى عليها، وبما يمنع أى محاولة للعبث به أو تعديله أو تغييره.

---

(١) د. محمد زكى أبو عامر، القيود القضائية على حرية القاضى الجنائى فى الاقتناع، مجلة القانون والاقتصاد، جامعة القاهرة، السنـة ٥١، ١٩٧١، صـ١٢٠؛ د. محمـد أحمد منشاوي، سلطة القاضـى الجنائى فى تقدير الدليل الإلكـتروني، مرجع سابق، صـ٥٥٢، ومـن القضاء المقارن، انظر موقف محكمة النقض البلجيكية التى قضت بـأن: «وصف الفعل غير المشروع لا يقتصر فقـط علـى الفعل الذى يحظره القانـون صراحةً، بل يشمل كل فعـل يتعارض مع القواعد الجوهرية للإجـراءات الجنائية، أو المبـادئ القانونيـة»، مشـار إليه: د. جميل عبد الباقـى الصغير، أدلة الإثبـات الجنائى والتكنولوجيا الحديثـة، مرجع سابق، ص١١٠.

ويجـب على القائمين على جمع الأدلة الرقمية من مسرح الجريمة اتخاذ الإجراءات اللازمـة للحفـاظ على سلامة الدليل الرقمـي، بدءاً من لحظة إنشائـه ووصولاً لمرحلة تقديمـه أمام المحكمـة، وهو ما يعـرف باستمرارية الدليل وثبات حالتـه وعدم تعرضه للتعديل أو التحريف أو العبث به، حيث يجب عليهم الحفاظ على استمرارية الأدلة على كل مـن الأجهـزة المادية التى تحتوى علـى البيانات (عند تلقيهـا أو الاستيلاء عليها)، والبيانات المخزنة الموجودة على الأجهزة [١].

ويجـب على سلطة التحقيق أن تعرض على المحكمة الإجراءات المطبقة للحفاظ على سلامـة الدليل الرقمي، وتبيان الآلية المطبقة لحفـظ الدليل وتوثيق التاريخ الزمنى له، وأنـه لم يطـرأ عليه أى تغيير، ولم يتـم العبث به، فيجب على النيابـة العامة أن تعرض على المحكمة أن المعلومات الرقمية التى تم الحصول عليها من الجهاز هى بمثابة تمثيل حقيقى وسليم للبيانات الأصلية التى يتضمنها الجهاز (الصحة)، وأن الجهاز والبيانات المراد تقديمها كأدلة هى ذاتها التى تم اكتشافها فى الأصل، وتم حفظها وتوثيق التاريخ الزمنـى لهـا (السلامة)، لما فى ذلك مـن تأثير مباشر على المحكمـة فى ترجيح فكرة موثوقيـة الدليل الرقمى وجدارته بالثقة من جانبهـا[٢]، ومن ثَمَّ مقبوليته أمام القضاء الجنائي، وللمحكمة فـى تحقيقها للدعوى بالجلسة سماع الشهود والخبراء ممن قاموا بجمع واستخلاص الأدلة الرقمية ومناقشتهم فيما أثبتوه بتقاريرهم للتثبت من صحتها وسلامتها وأن الوصول إليها قد تم بطريق مشروع.

وخلاصـة القـول: إنه ينبغى لقبـول الأدلة الرقميـة أمام القضاء الجنائـي، أن تتم إجراءات جمع الأدلة بالشكل الذى يضمن صحة إجراءات جمعها من الناحية القانونية، والحفاظ على سلامة الدليل، وعدم تغير شكله، واستمرارية حالته طوال الفترة الزمنية الكاملة التى تفصل بين ضبطها واستخدامها فى المحاكمة.

وتبرز أهمية تناول موضوع موثوقية الدليل الرقمى أمام القضاء الجنائي، فى سابقة

---

(١) انظر: الأدلة الرقمية الموجودة فى حجرة المحكمة، دليل لإنفاذ القانون والمدعين العامين، وزارة العدل الأمريكية، معهد العدالة الوطني، ٢٠٠٧، ص١٦، مشار إليه: دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٢٨.

(٢) مارسيـلا الإبن أيه جيه، غرينفيلد أر أس (محرران)، الأدلة الجنائية الإلكترونية، الدليل الميدانى لجمع ودراسة وحفظ أدلة جرائم الحاسب، بوكا راتون، مطبعة سى أر سي، ط٢، ٢٠٠٢، ص١٣٦، مشار إليه: دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٢٩.

الطعـن أمام إحدى المحاكم الأمريكية فى موثوقية المعلومات المتولدة من الحاسب الآلى وتلـك المخزنة على الحاسب، على أساس الثغرات الأمنيـة الموجودة فى أنظمة التشغيل والبرامـج التى يمكن أن تـؤدى إلى طرح تهديدات على سلامة المعلومات الرقمية، حيث نظـرت المحكمـة فى مسألـة قابلية المعلومـات الرقميـة للتعرض للتلاعـب أثناء تقديم الدلائـل الإلكترونية، وتم تسليط الضوء علـى الحاجة لتبيان صحة الحاسب الآلى فيما يخصـ قدرته علـى الاحتفاظ بالمعلومات موضـوع القضية واستعادتهـا[١]، حيث قضى بأن: مقبولية المعلومات المتولدة من الحاسب الآلى (مثل سجلات ملف التسجيل) تعطى تفاصيل عن الأنشطة الخاصة بالحاسب الآلى والشبكة وغيرها من الأجهزة التى يمكن أن تكـون عرضة للطعن فى حال كـان النظام الذى يقوم بتوليد المعلومات لا يحتوى على ضوابط أمنية قوية[٢].

وأخـيراً يشير البعض [٣] إلى اعتماد القضاء الأمريكـى على خمسة شروط أساسية لقبـول الدليـل الرقمى أمامها، أيـاً كان نوعه، وهذه الشروط هـي: ١- أن يكون له صلة بالواقعـة المراد إثباتها، سـواء بشكل مباشر أو غير مباشر. ٢- أن يكـون أصلياً؛ أى أن يكـون الدليـل المستخرج هو نفسه أصل البيانات التى ضبطـت، دون أن يلحقه أى تغيير منذ ضبطه وتجميعه. ٣- أن يكون موثوقاً فيه، وألا يكون قد تعرض للعبث به أو تغييره. ٤- أن يكـون الدليـل الأفضل، بأن يكون الدليل المقدم نسخة أصلية، باعتباره من أفضل البيانـات والمعلومـات المتاحة التـى يمكن للمحاكـم أن تستند عليها فـى قضائها، وهى قاعدة مقررة بالمادة (١٠٠٢) من القواعد الفيدرالية الأمريكية للإثبات، والتى تقضى بأن: الأصل يكون مطلوباً عند إثبات محتوى الرسائل أو السجلات أو الصور. كما تقضى المـادة (١٠٠٣/٣) من القـواعد المشـار إليهـا بأنه: إذا كانت المعلومات مخزنـة على الحاسـب الآلى أو جهـاز مماثل، فـإن أى مطبوع أو مستخرج منهـا مقروء بالبصر

---

(١) رى فيى فينهي، قضية شركة ديبتور أمريكان إكسبريس ترافلريلاند سيرفيس ضد شركة فيى فينهي، جلسة١٦/١٢/٢٠٠٦، ص١٨، مشار إليه: دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٢٩.

(٢) تشايكـين دي، تحقيقـات الشبكة حـول الهجمات الإلكترونية- حدود الأدلـة الرقمية، الجريمة والقانـون والتغير الاجتماعي، ٢٠٠٦، ص ص ٢٣٩-٢٦٥، مشار إليه: دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٢٩.

(٣) يرجـع إقـرار هذه الشـروط لما قررته إحـدى المحاكم الأمريكية فـى إحدى القضايا بـين شركـة Lorrinace وشركة Markel American Insurance، حيث يعد هذا الحكم سابقة قضائية مهمة؛ لتناوله بشكل مفصل متطلبات مقبولية الأدلة المستخرجة مـن الأجهزة الإلكترونيـة؛ كالبريد الإلكترونى ومواقع الإنترنـت، ومحتويات غرف الدردشة والتسجيـلات المخزنة والمنقولة. د. سالم محمد الأوجلي، مقبولية الدليل الرقمى فى المحاكم الجنائية، مجلة دراسات قانونية، جامعة بنى غازي، ليبيا، العدد ١٩، يناير ٢٠١٦، ص ص٣١-٤٠. ومن الفقه المقارن، انظر:
Keiko. L. Sugisaka, Admissibility of evidence in Minnesota: New problems or evidence as usual, p.1458.

يظهـر البيانـات بدقة يعد نسخـة أصلية. ٥- ألا يكـون شهادة سماعيـة؛ أى إن الدليل الرقمى لا يمكن قبوله إ ذا كان قولاً مرسلاً أو مجرد شائعة.

ثالثـاً- القواعـد الواجب مُراعاتها فـى إثبات الأدلة الرقمية: يتسـم الدليل الرقمى بطبيعـة خاصة، وهـى قابليته للتعديل، ومن ثم فإن هذا الدليـل غالباً ما يتسم بطبيعة مُتقلبة[١]، وهو ما يتطلب سرعة التحقيق فى جرائم تقنية المعلومات، واتخاذ الإجراءات القانونيـة اللازمة لضبط وتفتيش أو التحفظ على هذه الأدلـة الرقمية، ولذلك ترتكز خطة التحقيق فى هذه الفئة من الجرائم على عدة عوامل من أبرزها:

١- **فحـص طبيعـة بيئة المعالجة الآليـة للبيانات** التى سيمارس المحقق فى إطارها عمله، وتحديد نوعية وكيفية تعامله معها وتأثيرها فى طبيعة ونطاق إجراءاته وتوقيتها.

٢- **حصـر المواقع والأماكن الحساسة** بمبنى معالجة أو نقل البيانات كمكتبة الوثائق وأماكن تخزين الأشرطة والأقراص المغنطة، وتحديد المسئولين عن أمنها.

٣- **الوقـوف علـى قواعـد تشغيـل نظـام الحاسـب**، وكيفيـة تنظيـم دورة المعالجة الإلكترونية للبيانات ومدى مركزية المهام والمعرفة فى هذا الصدد.

٤- **تحديد أساليب التدقيق والمعالجة** وغيرها من العمليات الممكن إجراؤها بمساعدة الجهة المجنى عليها، وتلك التى يلزم إجراؤها عن طريق حاسب آخر غيره.

٥- **مراعـاة أمـن المعلومـات** التى قـد يستلزم التحقيـق الحصول عليهـا من نظام المعالجـة الإلكترونية للبيانات، يمكن أن تكون متاحـة فقط لفترة زمنية محدودة داخل دائـرة معالجـة البيانات، ويقتضى ذلك أن يبادر المحقق بتقييـم البيانات التى يتطلبها التحقيق والحصول عليها فوراً لتخزينها فى دعائم مأمونة.

٦- **فحص الاحتمالات المختلفة لنمط الدعامة أو الوعاء المتبقى** استخدامه للحصول على الدليل وصيانته (ورق، ميكروفيش، أوعية أو وسائط ممغنطة).

٧- **إعداد قائمة بالأشخاص المتعين سؤالهم**، وتحديد النقاط التى يجب استيضاحهم بشأنها[٢].

---

(١) كينجى ميانيشي، شبكة الربط بين النقاط المرجعية الوطنية، المؤتمر الدولى السادس للجرائم المعلوماتية،١٣-١٥/٤/٢٠٠٥، إصدار مركز بحوث الشرطة، القاهرة، ص ص٩٥-٩٨.

(٢) د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ١٩٩٤، ص٣٤ ومابعدها.

المطلب الثالث

حجية الدليل الرقمي

أولاً- حجية الدليل الرقمى فى الإثبات الجنائي: تحتوى بيانات الحاسب الآلى والاتصالات الإلكترونية -التى يحتمل أن تكون ذات صلة بجرم ما- على العديد من الصور والفيديوهات ورسائل البريد الإلكترونى وسجلات المحادثات وبيانات النظام، ويواجه المحققون فى سبيل جمع الأدلة الرقمية ذات الصلة بجرم ما بعض التحديات المتمثلة فى كبر حجم هذه البيانات، والتى يستغرق فحصها وقتاً طويلاً، فضلاً عن تباين أشكال الملفات المحتملة ونظام التشغيل والبرمجيات التطبيقية وتفاصيل الأجهزة، وهو ما قد يشكل تعقيدات عملية بشأن تحديد المعلومات ذات الصلة بالجريمة، ولا شك فى أن هذه البيانات والمعلومات تشكل بنسبة كبيرة أدلة رقمية، إذا ما تم التعامل معها من جانب الخبراء التقنيين، إلا أنه فى إطار القانون الجنائي، فقد ثار التساؤل عما إذا كانت هذه الأدلة الرقمية المستحدثة تتمتع بالحجية القانونية ذاتها التى تتمتع بها الأدلة التقليدية فى إثبات الجريمة، على الرغم من الطبيعة المعنوية لهذه الأدلة والتى تختلف عن الأدلة التقليدية ذات الطبيعة المادية؟

وقد أجاب المشرع عن هذا التساؤل فى قانون مكافحة جرائم تقنية المعلومات، من خلال إضفائه الحجية القانونية المقررة للدليل المادى التقليدى على الدليل الرقمى ذى الطابع المعنوى فى الإثبات الجنائي، حينما قرر فى المادة (١١) من القانون رقم ١٧٥ لسنة ٢٠١٨ أنه: «يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتى أو من برامج الحاسب، أو من أى وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية فى الإثبات الجنائى متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون»[(١)].

ثانياً- العلة من تقرير الحجية القانونية للدليل الرقمي: ترجع أهمية هذا النص

(١) أخذ القضاء السعودى بهذا النهج، حيث أصدرت الهيئة العامة للمحكمة العليا بالمملكة العربية السعودية القرار رقم ٣٤ المؤرخ فى ١٤٣٩/٤/٢٤هـ بخصوص الأدلة الرقمية وحجيتها، والذى ينص على أنه: «الدليل الرقمى حجة معتبرة فى الإثبات متى سلم من العوارض ويختلف قوة وضعفاً حسب الواقعة وملابساتها وما يحتف بها من قرائن»، والسلامة من العوارض تعنى أن يكون الدليل سليماً من التعديل والتغيير، وأن يكون موثوقاً. انظر: موقع جريدة عكاظ السعودية على الرابط: https://www.okaz.com.sa/articles/na/١٦٩٧١٨٣، تاريخ الاطلاع ٢٠٢١/٤/١٧م.

فيما يقرره من قيمة ثبوتية وحجية قانونية فى الإثبات الجنائى للدليل الرقمى كتلك المقررة للدليل التقليدي، وهو من الأهمية بمكان فى مجال الإثبات الجنائي، بغية الاستفادة من هذه الطائفة من الأدلة فى إثبات الجرائم ونسبتها إلى مرتكبيها، فمن المعلوم أن وثائق الحاسب الآلى ورسائل البريد الإلكترونى والرسائل النصية والفورية، والمعاملات، والصور وتواريخ الإنترنت، هى أمثلة على المعلومات التى يمكن جمعها من الأجهزة الإلكترونية واستخدامها بشكل فعال جداً كدليل جنائي.

والدليل الرقمى قد يكون من الوضوح، حينما يتخذ صوراً معينة، مثل مطبوعات رسائل البريد الإلكترونى المتوافرة بسهولة التى يرسلها مرتكب الجريمة، أو سجلات اتصال بروتوكول الإنترنت التى يبلغ عنها مباشرة من قبل موفر خدمة الإنترنت، وقد يتطلب فى أحوال أخرى استعمال تقنيات متطورة من أجل التوصل إليه، عن طريق استخدام تقنيات أو أدوات لاستعادة الآثار أو البيانات التى يتم الحصول عليها من الحاسب الآلى والنظم المعلوماتية والشبكات، والتى من شأنها أن تقدم أدلة على وقوع جرم ما، ومن ثَمَّ يأتى دور خبراء وتقنيات الأدلة الجنائية الرقمية فى استعادة وتحليل المواد التى تم الحصول عليها من أجهزة الحاسب والشبكات والنظم المعلوماتية، والاستفادة من قابلية الحواسب لتخزين وتسجيل وحفظ البيانات عن أغلب أنشطة مستخدميها، فى جمع وتعقب الآثار الرقمية[1].

ويرى البعض أن نص المادة (١١) من القانون يثير إشكالية حول طبيعة الدليل الرقمى من جهة، وقوته فى الإثبات من جهة أخري، لا سيما فى ضوء مبدأ حرية القاضى الجنائى فى الإثبات، حيث يرى الرأى السابق أن هذا النص قد أضفى على الدليل الرقمى حجية مطلقة فى الإثبات، يصح للقاضى أن يؤسس حكمه عليه بمفرده، ولو لم يعزز بأى قرينة أخرى، وهو ما يرى فيه البعض الآخر مغالطة؛ إذ يذهب الرأى الأخير إلى أنه من الثوابت أنه ولئن كان القاضى الجنائى حراً فى الإثبات وفقاً لمبدأ قضاء القاضى باقتناعه، إلا أن هذه الحرية ليست مطلقة؛ إذ ثمة ضوابط تحكم عمله، أولها: أنه لا يصح أن يبنى حكمه إلا على – دليل- أما ما دون الدليل أو القرائن البسيطة أو بالأحرى الدلائل، فلا يصح أن يستمد منها القاضى اقتناعه، ويؤسس عليها بمفردها حكم الإدانة، وعلة ذلك أن الأحكام الجنائية تبنى على الجزم واليقين من الواقع الذى

(١) انظر: دراسة مكتب الأمم المتحدة بعنوان: «دراسة شاملة عن الجريمة السيبرانية»، مرجع سابق، ص٢٣٠.

يثبت بالدليل المعتبر لا على الظن والتخمين[١]، حال أن الدلائل تقوم على الاحتمال[٢]، ولما كان الدليل الرقمى لا يدل رأساً ومباشرةً على وقوع الجريمة ونسبتها إلى الجاني، بل استخلص ذلك من واقع استخدام جهاز حاسب آلى يخصه مرتبط بخط تليفون باسمه، لذا كان الدليل الرقمى دليل جريمة، ولكنه فى الوقت ذاته قرينة مادية ضعيفة على إسناد الجريمة إلى الجاني، أو بالأحرى مجرد دلائل لا يصح بناء حكم الإدانة عليها بمفردها ما لم تعزز بأدلة أخرى؛ إذ لا تقطع بارتكاب المتهم للجريمة، إذ قد يكون حساب المتهم الإلكترونى قد تم اختراقه، أو أن خط الهاتف المرتبط بالحساب استخدمه غيره فى غيبته، وكان الأصل عدم جواز الركون إلى تلك القرينة فى الإثبات لأنها مجرد دلائل لا تقطع بنسبة الجريمة إلى صاحب الحساب أو الخط، إلا أن بعض الآراء ذهبت إلى أن المشرع رغب فى أن يخرج على هذا الأصل فى المادة (١١) من قانون جرائم تقنية المعلومات، بحجة أنه اعتبر الدليل الرقمى من الأدلة المادية وله قيمتها نفسها؛ إذ يعنى لديهم أن يكون له قيمة قاطعة فى الإثبات تغنى عن تعزيزه بأى قرينة أو دليل آخر.

ويرى البعض أن الرأى السابق محل نظر؛ إذ الدليل أى كان نوعه، أى سواء كان مادياً أو نفسياً لا يكون له قيمة دامغة فى الإثبات، إلا إذا كان قاطعًا فى وقوع الجريمة من شخص بعينه، وهو ما تفتقر إليه الأدلة الرقمية، بل إنه طبقاً لمبدأ حرية الإثبات الجنائى لم تحصر الأدلة، ولا يحظى الدليل المادي، ومن ثَمَّ الرقمى بحجية أمام القاضى الجنائي، فله أن يأخذ به أو يطرحه تبعاً لاطمئنانه له من عدمه، ومن ثَمَّ فإن ما جاءت به المادة (١١) من قانون جرائم تقنية المعلومات من اعتبار الدليل الرقمى دليلاً ماديًا له ذات قيمة الأدلة المادية من جانب هذا الرأى هو تحصيل حاصل وذكر لمعلوم.

---

(١) انظر: نقض١٣/٣/٢٠١٦، الطعن رقم ٢٠٠٣١ سنة ٨٤ ق؛ نقض٢٦/١/٢٠١٤، الطعن رقم ٦٥٠٥ سنة ٤ ق، جنح النقض، مجموعة المكتب الفني، س٦٥؛ نقض٧/٤/٢٠١١، الطعن رقم ٧٥٣٣ سنة ٧٩ ق؛ نقض١/٢/١٩٩٠، الطعن رقم ٢٢٤٣٢ لسنة ٥٩ق، مجموعة أحكام محكمة النقض، المكتب الفني، س٤١، ص٢٥٩؛ نقض١٣/٦/١٩٨٥، الطعن رقم ٦٣٣٥ لسنة ٥٥ق، مجموعة أحكام محكمة النقض، المكتب الفني، س٣٦، ص٧٨٢.

(٢) ومن أمثلة الدلائل: التحريات التى يستقيها الضابط من مصادره السرية، ويرفض الإفصاح عنها تحقيقاً للصالح العام، أو المعلومات التى يجمعها من جمهور الناس عند انتقاله لمحل الواقعة لفحص البلاغ، مادام لم يحدد شخص بعينه نقل إليه هذه المعلومات، ومن أمثلة الدلائل أيضاً التسجيلات الصوتية واستعراف الكلب البوليسي.

ويضيف الرأى السابق إلى ذلك أن الدليل الرقمى يعد دليلاً فنيًا، لا يصح للمحكمة عند المنازعة فيه أن تدلى بدلوها فيه، وإنما يتعين عليها الاستعانة بأهل الخبرة المختصين ولا يقدح قالة إن المحكمة هى الخبير الأعلى، إذ شرط ذلك ألا تكون المسألة المطروحة على بساط البحث من المسائل الفنية البحتة التى تستعصى على المحكمة أن تستجليها بنفسها دون الركون إلى أهل الخبرة، فهنا لا مجال للقول بأن محكمة الموضوع هى الخبير الأعلى، وأن تحل نفسها محل الخبير[1].

ثالثاً- مدى الحجية القانونية للدليل الرقمى فى الإثبات الجنائي: يتمثل جوهر العملية الإثباتية فى تحويل تلك الواقعة المتنازع عليها إلى أمر مقبول للكافة ومسلم به دون تنازع فيه، أى تحويل حالة الشك فى الواقعة التى يراد إثباتها إلى حالة من التيقن بحدوثها، وذلك من خلال التوصل إلى إقناع القاضى بحقيقة ذلك عن طريق ما يقدم فى الدعوى من وسائل قادرة على ذلك.

ويتبع التشريع المصرى نظام الإثبات الحر أو نظام الأدلة المعنوية، وفى هذا النظام لا يرسم القانون طرقاً محددة للإثبات يتقيد بها القاضى الجنائي، بل ترك حرية الإثبات لأطراف الخصومة فى أن يقدموا ما يرون أنه مناسب لاقتناع القاضى الذى يتلمس تكوين عقيدته أى دليل يطرح أمامه، وله أن يقدر القيمة الإقناعية لكل منها، حسبما تتكشف لوجدانه، حيث لا سلطان عليه فى ذلك إلا ضميره، وهو ما يعرف بمبدأ قضاء القاضى باقتناعه.

وهكذا يتضح أن القاضى له مطلق الحرية فى أن يستعين بكافة طرق الإثبات للبحث عن الحقيقة والكشف عنها طالما كانت هذه الطرق مشروعة، ويقوم بتقدير كل دليل طرح أمامه؛ لأن مبدأ الحرية والاقتناع لدى القاضى فى تقدير قيمة الأدلة قائم، وله أن

---

(١) طبقت محكمة النقض هذه القاعدة على مسألة تحقيق ما إذا كانت الحيوانات المنوية التى وجدت على سروال المجنى عليها من فصيلة مادة المتهم المنوية من عدمه عن طريق المختص فنياً وهو الطبيب الشرعي، أما وهى لم تفعل، فإن حكمها يكون معيبًا، انظر: الطعن رقم ٥٧٧٩ لسنة ٥٢ ق، وطبقتها كذلك على مدى تأثير السكر على إدراك المتهم المعترف، انظر: الطعن رقم ١٥٦٥ لسنة ٨١ ق، وكذلك على تحديد ما إذا كانت الدماء البشرية تُعد من الأعضاء والأنسجة البشرية التى جُرّم الاتجار فيها بالمادة الثانية من القانون رقم ٦٤ لسنة ٢٠١٠ من عدمه، انظر: الطعن رقم ١٤٧٦٤ لسنة ٨٣ ق، وأيضاً على الاضطراب النفسى كسبب للإعفاء من العقاب؛ إذ رأت أنه يجب على محكمة الموضوع تحقيقه من خلال خبير للبت فيها إثباتاً أو نفياً، ولا يجوز للمحكمة أن تحل محل الخبير فيه؛ لأن كونها الخبير الأعلى؛ لأن ذلك لا يكون إلا عند تقدير رأى الخبير لا قبله، انظر: الطعن رقم ٢٧١٥٨ لسنة ٨٦ ق.

يستمدهـا مـن أى مصدر يطمئن إليه، دون أن يملى عليـه المشرع حجية معينة أو يلزمه باتباع وسائل محددة للكشف عن الحقيقة كقاعدة عامة (م٢٩ إجراءات مصري) [١].

وقـد استقر قضاء محكمة النقض على أن ما تحويه الأوراق إن هى إلا عناصر إثبات تخضـع فى جميع الأحـوال لتقدير القاضى الجنائى وتحتمل الجـدال والمناقشة كسائر الأدلة، وللخصـوم أن يفندوها دون أن يكونوا ملزمين بسلوك سبيل الطعن بالتزوير [٢]، ويبـين القاضـى الأدلة التى اعتمـد عليها وكانت مصـدراً لاقتناعه، فـإذا كان تقديره لا يخضـع لرقابـة محكمة النقض، إذ ليس لها أن تراقبه فى تقديره إلا أن لها أن تراقب صحة الأسباب التى استدل بها على هذا الاقتناع [٣]، ويُرجع الفقه الجنائى إقرار القانون الجنائى لهذا المبدأ فى استخدام الدليل العلمى فى الإثبات مثل تلك الأدلة المستمدة من الطـب الشرعى والتحاليل، وتحقيـق الشخصية ومضاهاة الخطوط، وغيرها من الأدلة العمليـة، وهى أمـور لا تقبل أى قيود لدى تعويل القاضى عليهـا لتكوين عقيدته، ولذلك ترك القانون للقاضى الحرية فى تقدير تلك الأدلة وملاءمتها.

فالقانون لم يرسم فى المواد الجنائية طريقاً يسلكه القاضى فى تحرى الأدلة [٤]، ولا يخـرج عن هذه القاعـدة إلا ما استثناه القانون وجعل له قوة إثبات خاصة، بحيث يعتبر المحضر حجة بما ورد فيه إلى أن يثبت ما ينفيه تارة بالطعن بالتزوير، كما هى الحال فى محاضـر الجلسات والأحكام، وتارة أخرى بالطعن بالطرق العادية كمحاضر المخالفات بالنسبة إلى الوقائع التى يثبتها المأمورون المختصون إلى أن يثبت ما ينفيها [٥].

ويذهـب البعض [٦] – بحـق – إلى أن تطبيق القواعد العامـة فى الإثبات الجنائى تفترض أن تكـون الأدلة الرقمية مطروحة علـى بساط البحث أمـام المحكمة، فإذا ما اطمأنـت إليهـا عولت عليهـا، وإذا لم ترتح لها طرحتها ولا تعتد بهـا، فملاك الأمر إلى وجدانها وعقيدتها، كما هو الحال فى سائر الأدلة الأخرى.

---

(١) تقضـى المـادة (٢٩١) إجراءات جنائية بأنه: «للمحكمة أن تأمر ولو من تلقـاء نفسها أثناء نظر الدعوى، بتقديم أى دليل تراه لازماً لظهور الحقيقة».

(٢) انظر: نقض ٢٠١٢/١٢/٢٣، مجموعة أحكام محكمة النقض، س٦٣، ص٨٦٤.

(٣) د. محمود نجيب حسنى، شرح قانون الإجراءات الجنائية، القاهرة، دار النهضة العربية، ط٢، ١٩٨٨، ص٤٠٥ وما بعدها.

(٤) انظر: نقض ٢٠١٥/٤/١٤، الطعن رقم (١٨٦٣٧) لسنة ٨٤ق.

(٥) انظر: نقض ١٩٦٧/٦/١٢، مجموعة أحكام محكمة النقض، س١٨، ص٧٩٧.

(٦) المستشار/ د. محمد سمير، قانون العقوبات الاقتصادي، طبعة نادى القضاة، ٢٠١٩، ص٢٥١.

كمـا أن الوقائع الجنائية لا يمكن تحديدها مسبقاً كما فى القانون المدني؛ فهى ليس مما يحرر بها عقود أو يمكن الحصول من الجانى على اعتراف مكتوب بها، ولذلك كان الدليـل المستمد مـن أجهزة الحاسب الآلى ما هو إلا أحد تطبيقـات الدليل العلمي، بما يتميز به من موضوعية وحياد وكفاءة فى إقناع القاضى الجنائي.

رابعـاً- الشـروط الواجب توافرها لتقرير حجية الدليـل الرقمي: تُثير حجية الدليل الرقمي، أهمية كبيرة فيما يتعلق بالدور الذى يلعبه الدليل الرقمى فى إثبات الجريمة، لذلك يجب أن يتوافر فى الدليل عناصر مهمة؛ لكى يُمكن الاستناد إليه فى عملية إثبات الجريمـة، وقد تناول قانون مكافحة جرائم تقنيـة المعلومات، المُحددات المتعلقة بحجية الدليـل الجنائى المُرتبـط بالجرائم المنصوص عليها بالقانـون، حيث يشترط القانون، للأخـذ بالدليـل الرقمى واعتبـاره ذا حُجية فى عمليـة الإثبات، توافـر بعض الشروط الفنيـة فى هذا الدليل، وقد أحال القانون توضيح هذه الضوابط والشروط إلى اللائحة التنفيذيـة للقانـون، وقد حـددت المادة (٩) مـن اللائحة التنفيذيـة للقانون الجوانب والشـروط الفنية بشأن التعامل مع هذه النوعية من الأدلة الجنائية، حيث تقضى المادة المشار إليها بأنه:«تحوز الأدلة الرقمية ذات القيمة والحجية للأدلة الجنائية المادية فى الإثبات الجنائى إذا توافرت فيها الشروط والضوابط الآتية:-

١- أن تتـم عمليـة جمع أو الحصـول أو استخراج أو استنبـاط الأدلة الرقمية محل الواقعة باستخدام التقنيات التى تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات، أو أى تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات، أو أنظمة المعلومات أو البرامج أو الدعامات الإلكترونية وغيرها. ومنها على الأخص تقنيةDigital Images Hash، Write Blocker، وغيرها من التقنيات المماثلة.

٢- أن تكون الأدلة الرقمية ذات صلة بالواقعة وفى إطـار الموضوع المطلوب إثباته أو نفيه وفقًا لنطاق قرار جهة التحقيق أو المحكمة المختصة.

٣- أن يتم جمع الدليل الرقمى واستخراجه وحفظه وتحريزه بمعرفة مأمورى الضبط القضائـى المخـول لهم التعامل فى هذه النوعية من الأدلـة، أو الخبراء أو المتخصصين المنتدبين من جهات التحقيق أو المحاكمة، على أن يبين فى محاضر الضبط، أو التقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهـزة والمعـدات التى تم استخـدامها،

مـع توثيق كود وخـوارزم Hash الناتج عن استخراج نسخ مماثلـة ومطابقة للأصل من الدليـل الرقمى بمحضر الضبـط أو تقرير الفحص الفني، مع ضمان استمرار الحفاظ على الأصل دون عبث به.

٤- فى حالة تعذر فحص نسخة الدليل الرقمى وعدم إمكانية التحفظ على الأجهزة محل الفحص لأى سبب يتم فحص الأصل ويثبت ذلك كله فى محضر الضبط أو تقرير الفحص والتحليل.

٥- أن يتم توثيق الأدلة الرقمية بمحضر إجراءات من قبل المختص قبل عمليات الفحص والتحليل له، وكذا توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته».

ويتضح من النص السابق أن اللائحة تطلبت اشتراطات خاصة تتمثل فى استخدام برامج تقنية تعنى بالحفاظ على حالة الدليل الرقمى وقت استخراجه، فضلاً عن تحديد القائمين على جمع واستخراج الدليل فى مأمورى الضبط القضائى المختصين والخبراء المنتدبـين من جهات التحقيـق أو المحكمة للتعامل مع هذه الأدلـة الرقمية، كما قصرت اللائحـة عملية جمع الأدلة على الأدلة الرقمية ذات الصلة بالواقعة -دون غيرها- وفق الإطـار المحـدد فى هذا الشأن من جهـات التحقيق أو المحكمـة المختصة، كما حرصت اللائحة على وجوب توثيق الأدلة الرقمية قبل عملية فحصها، وتوثيق مكان حفظها، بما يحقـق الثقـة المتطلبة فى إجراءات استخراجها وجمعها، مـع التأكيد على وجوب إثبات حالة تعذر فحص الأدلة الرقمية، وإثبات ذلك فى محضر الضبط أو تقرير الفحص.

كمـا يجـب الإشـارة إلى أن الشـروط والضوابط التـى حددتها اللائحـة التنفيذية لقانـون مُكافحة جرائـم تقنية المعلومات، يجـب أن تتوافر جميعها فـى الدليل الرقمى حتـى يكتسـب حجية فى عملية الإثبـات الجنائي، وأن تخلف أحد هـذه العناصر، يُفقد الدليل قوته اللازمة للاحتجاج به واستخدامه فى عملية الإثبات، ويجب هنا الإشارة أن فقدان هذه الشروط، تُفقد الدليل قدرته الكاملة فى عملية الإثبات، إلا أن ذلك لا يعنى استبعـاد ما أفضت إليه هذه العملية بالكامل، حيث يُمكن الأخذ بما أفضى إليه الدليل، تحـت توصيفات قانونيـة أخرى، ولكنها ليست بقـوة الدليل الذى ألـزم قانون مكافحة جرائم تقنية المعلومات توافره.

خامساً- تساؤل- هل ضبط جهاز الحاسب الآلى وما به من أدلة رقمية- يتطلب قراراً من القاضى الجزئى كما هو الوضع فى ضبط الخطابات أو الرسائل أو المطبوعات لدى مكاتب البريد؟ أجابت محكمة جنح مستأنف القاهرة الاقتصادية عن هذا التساؤل، حينما قضت فى أحد أحكامها بأن: ضبط جهاز الحاسب الآلى المستخدم فى ارتكاب الجريمة لا يستلزم إذناً من القاضى الجزئى لكون محل الجريمة هو جهاز الحاسب الآلى وليس ضبط خطابات أو رسائل أو مطبوعات لدى مكتب البريد[١]، وهو ما أيده البعض[٢] مستنداً فى ذلك إلى حكم المادة (٢٠٦) من قانون الإجراءات الجنائية التى لم تتطلب إذن القاضى الجزئى إلا فى حالة ضبط الطرود والرسائل والمطبوعات لدى مكاتب البريد أو البرق، دون غيرها، وأن حالة الضبط من خلال الحاسب الآلى تختلف عن ضبط الرسائل والطرود بمكاتب البريد، فالأخيرة تفترض أن الخطابات المرسلة لم تصل للمرسل إليه، بخلاف حالة الضبط من خلال جهاز الحاسب الآلي، يكون الخطاب فى حوزة المرسل للخطاب أو المرسل إليه حسب الأحوال، فضلاً عن عدم وجود نص تشريعى ينظم هذه المسألة، ومن ثَمَّ فإن ضبط الرسائل الإلكترونية المرسلة أو المستلمة من بريد إلكترونى إلى آخر لا يستلزم إذناً من القاضى الجزئي، باعتبار أنها تعد من قبيل الرسائل، وطالما أنها لم تكن موجودة لدى مكاتب البريد أو البرق، فإنه يكفى للاطلاع عليها أو ضبطها صدور إذن من النيابة العامة.

ويضيف الرأى السابق أن بعض الرسائل الإلكترونية قد تكون فى حوزة المتهم كما لو كان حائزاً لهاتفه الذكى الذى يحتوى على الرسائل المذكورة، أو قد يكون فى مسكنه، ومن ثَمَّ فإنه يتعين صدور الإذن الملائم الذى بموجبه يكون التفتيش صحيحاً، وهو ما ينطبق كذلك على حالات ذاكرات الهواتف النقالة والكاميرات ووسائط التخزين والأقراص المدمجة، ويتفق الرأى السابق مع قضاء محكمة النقض، والتى ترى أن تفتيش جهاز الحاسب الآلى يدخل فى اختصاص النيابة العامة التى تختص بإصدار الإذن بتفتيش الأشخاص والمنازل، دونما الاختصاص بتفتيش غير مسكن المتهم، أو

---

(١) انظر: حكم محكمة جنح مستأنف القاهرة الاقتصادية، جلسة ٢٠١٠/١١/٣، الدعوى رقم ٧٨٩ لسنة ٢٠١٠ جنح مستأنف والمقيدة برقم ١٥١٧ جنح القاهرة الاقتصادية (غير منشور)، مشار إليها: المستشار/ د. محمد سمير، قانون العقوبات الاقتصادي، مرجع سابق، ص٢٢٤.

(٢) المستشار/ د. محمد سمير، قانون العقوبات الاقتصادي، مرجع سابق، ص ص٢٢٤، ٢٢٥.

التنصت على المكالمات الإلكترونية أو مراقبة المحادثات السلكية واللاسلكية، أو تسجيل محادثات تجرى فى مكان خاص، والتى تتطلب صدور إذن من القاضى الجزئي[١].

سادساً- موقف القضاء المصرى من الاعتداد بالدليل الرقمي: تبرز الإشارة إلى أن القضاء المصرى قد اعتد بالدليل الرقمى المتحصل من جرائم تقنية المعلومات، إذ عولت إحدى دوائر الجنايات على الإثبات الناتج عن دليل مستمد من محادثة إلكترونية عبر شبكة الإنترنت، وأقرتها محكمة النقض على ذلك [٢]، كما اعتد القضاء بتقديم الدليل من المجنى عليه، سواء كان هاتفه المحمول، أو جهاز الحاسب الخاص به، أو من خلال ضبطه من جهاز المتهم، وذلك على النحو التالي:

(الفرض الأول): تقديم الدليل من جهاز المجنى عليه: بالنسبة للفرض الأول، فقد اعتد به القضاء فى حالة تقديمه من المجنى عليه، واعتد به دون إذن، لأنه هاتف المجنى عليه الذى قدمه برضائه الكامل، حتى ولو كان به تسجيل للمتهم، حيث قضت محكمة النقض بأن: «المشرع تطلب مباشرة الإجراءات المبينة بالمادة المراد ذكرها، كى يوضع تحت المراقبة التليفون الذى استعان به الجانى فى توجيه ألفاظ السب والقذف إلى المجنى عليه، بحسب أن تلك الإجراءات فرضت ضمانة لحماية الحياة الخاصة والأحاديث الشخصية للمتهم.

ومن ثَمَّ فلا تسرى تلك الإجراءات على تسجيل ألفاظ السب والقذف من تليفون المجنى عليه الذى يكون له بإرادته وحدها، ودون حاجة إلى الحصول على إذن من رئيس المحكمة الابتدائية لتسجيلها، بغير أن يعد ذلك اعتداء على الحياة الخاصة لأحد، ومن ثَمَّ فلا جناح على المدعين بالحقوق المدنية إذا وضعا على خط التليفون الخاص بهما

---

(١) انظر: نقض ٢٠١٣/٧/٣، الطعن رقم ١٥٤٢ لسنة ٨٢ ق.

(٢) قضت محكمة النقض فى أحد أحكامها الحديثة بأنه: «لما كان ذلك، وكان ما أثبته الحكم فى بيانه للواقعة ومضمون ما شهد به ضابطها من أنه إذ سمع مضمون نسخة المحادثة التى أجراها المتهم الطاعن على شبكة المعلومات الدولية وتبينه ما احتوت عليه من عبارات تثبت حيازته لمواد مفرقعة وقنابل وأسلحة نارية وذخائر دون ترخيص، وإقراره له باعتناقه لأفكار «جهادية» متطرفة بتكفير مؤسسات الدولة وبحيازة المضبوطات التى أشار إليها الحكم، وكان من المقرر أن القول بتوافر حالة التلبس أو عدم توافرها من المسائل الموضوعية التى تستقل بتقديرها محكمة الموضوع بغير معقب، ما دامت قد أقامت قضاءها على أسباب سائغة، وكان ما أورده الحكم تدليلا على قيام حالة التلبس وردا على دفع الطاعن كافيا وسائغا ويتفق وصحيح القانون، فإن ما أثاره الطاعن ينحل إلى جدل موضوعى لا تجوز إثارته أمام محكمة النقض». انظر: نقض ٢٠١٥/٥/٥، الطعن رقم (٣١٣٣٠) لسنة ٨٣ ق.

جهـاز تسجيل، لضبط ألفاظ السبـاب الموجهة إليهما، توصلاً إلى التعرف على شخص من اعتاد على توجيه ألفاظ السباب والقذف إليهما عن طريق الهاتف.

ولمـا كـان ذلك، وكان الحكم المطعـون فيه قد انتهى إلى بطـلان الدليل المستمد من الشريط المسجل بمعرفة المدعين بالحقوق المدنية من جهاز التليفون الخاص بهما، فإنه يكون قد أخطا فى تطبيق القانون بما يعيبه ويوجب نقضه والإعادة» [1].

(الفرض الثاني): الحصـول على الدليل من جهـاز المتهم: أما الفرض الثانى أن تتـم المطالبة بالتحصل على الدليـل بضبطه من جهاز المتهم أو مراقبته، وهو ما يحتاج إلى إذن مـن الجهـات القضائية المختصة لعمل ذلك، ولقد كـان قانون العقوبات يحوى عددًا كبيرًا من قرائن الإثبات ضد المتهم، إلى أن قضت المحكمة الدستورية العليا بعدم دستوريتهـا لإخلالها بمبدأ الأصل فى المتهم الـبراءة، ومنها القرينة التى كانت تضعها المـادة (١٩٥) عقوبات، والتـى افترضت علم رئيس التحرير بكافـة ما تنشره الجريدة التـى يشـرف عليها، وعدم جواز نفـى هذه القرينة إلا من خـلال وسائل محددة نصت عليهـا المادة (١٩٥) عقوبـات ذاتها، لذلك، فإنه يجب إثبـات وقوع الجريمة من المتهم دون افتراض ذلك، أو إقامة قرينة ضده.

ولقـد صدرت أحكام عديدة من القضاء المصرى تفيد بأنه قد اعتد بالدليل الرقمى دون الوقوف فى موقف متحجر، وتطلب أن يتم فى شكل تقليدى كمحرر أو شهادة شاهد، ومـن القضايا الشهيرة قضية حرق المجمـع العلمي، حيث اعتدت المحكمة بالأسطوانات المدمجـة والتسجيلات المثبتة لمرتكـب الجريمة والتى اطمأنت إليهـا، وكذلك فى واقعة رشـوة عرضـت على القضاء استنادًا لتسجيلات، حيث قضـت محكمة النقض بأن: «لما كـان الثابت من مدونـات الحكم المطعون فيه أن المحكمة عولت فـى إدانة الطاعن على تسجيلات اللقاءين اللذين تما بين المبلغ والطاعن يومى ٢٦ و٢٨ نوفمبر ١٩٩٦، وأفصح الحكـم عن اطمئنانه إليهـا ثم أردف بقولـه، إنه على فرض بطـلان التسجيلات، فلا يوجـد ما يمنع المحكمة من اعتبارها عنصرًا من عناصر الإثبات فى الدعوى فى منزلة تظاهر الأدلة.

(١) نقض ٢٠٠٠/٥/١٨، الطعن رقم (٢٢٣٤٠) لسنة ٦٢ ق، مجموعة أحكام محكمة النقض، س٥١، ص٤٨١.

ويبين مما أورده الحكم أن المحكمة لم تبن قضاءها بصفة أصلية على تلك التسجيلات، وإنما استندت إليها كقرينة تعزز بها أدلة الثبوت التى أوردتها، ولا يعد ذلك منها تناقضًا أو اضطرابًا فى الحكم» [١]، ومن ثَمَّ يتضح أن القضاء قد سبق أن اعتد بالدليل الرقمى فى عدد من القضايا فى تاريخ سابق على صدور قانون مكافحة جرائم تقنية المعلومات، وهذا نهج محمود للقضاء المصرى الذى أرسى هذه القواعد فى وقت غاب فيه التنظيم القانونى لهذه المسألة.

سابعاً- حجية التصوير بكاميرات المراقبة التليفزيونية: انتشر استخدام كاميرات المراقبة التليفزيونية فى كافة مناحى الحياة، نتيجة لانتشار الجرائم، حيث عملت الكثير من الدول على تزويد الطرق العامة والميادين وغيرها من الأماكن العامة والمؤسسات والأسواق الكبرى والفنادق والمدارس وبعض المساكن بكاميرات المراقبة التليفزيونية الحديثة، وتلعب هذه الكاميرات دوراً فاعلاً فى كشف غموض الكثير من الجرائم، حيث تتمكن من تسجيل وتصوير ما يدور فى المكان على مدار اليوم، وقد يتصادف أن تسجل الكاميرات المذكورة وقائع إجرامية أو يبين منها شخص المشتبه به أو أن الجريمة قد ارتكبت على نحو معين.

ويقر البعض [٢] بمشروعية الدليل المتحصل من الكاميرات المذكورة؛ شريطة وجود هذه الكاميرات فى أماكن عامة، وتسجيلها وقائع الجريمة فى هذه الأماكن أيضاً، وكذلك إذا كانت موضوعة فى مكان خاص كمسكن وكانت تسجل ما يحدث فى مكان عام، فإذا التقطت شخصاً يرتكب جريمة، فلا تثريب فى التعويل على الدليل المستمد منها، أما إذا كانت الكاميرات مثبتة فى مكان خاص كمسكن، وسجلت الكاميرات ما يحدث بهذا المكان من جرائم، فإن الدليل المتحصل فى هذه الحالة يفتقر إلى المشروعية، ومع ذلك فإن الدليل غير المشروع المذكور قد يقود مأمور الضبط القضائى إلى أدلة أخرى مشروعة.

ويرى الرأى السابق أن المحاكم الجنائية لم تتردد فى التعويل على الأدلة المتحصلة من الكاميرات، كما أن محكمة النقض لم تجد حرجاً فى ذلك [٣]، على الرغم من وجود

(١) نقض ١٩٩٨/٣/١٤، الطعن رقم (١٦١٣٧) لسنة ٦٧ ق، مجموعة أحكام محكمة النقض، س٤٩، ص٥٦٣.

(٢) المستشار/ د. محمد سمير، قانون العقوبات الاقتصادي، مرجع سابق، ص٢٣١.

(٣) نقض ٢٠١٥/١٢/٣، الطعن رقم (٢١٨١٩) لسنة ٨٥ق؛ نقض ٢٠١٠/٣/٤، مجموعة أحكام محكمة النقض، س٦١، ص٢١٥.

أعطـال فـى كاميرات المراقبة فى بعض الأحيان، مما يـؤدى إلى التأثير على وضوح أو جودة بعض مقاطع الصورة والصوت المسجل عليها [١].

خلاصـة القول: إن الباحث يرى أنه كان ينبغى أن تتناول اللائحة التنفيذية للقانون إجـراءات وتقنيات وأدوات جمع الأدلة الرقميـة بشكل أكثر تفصيلاً، بما يحقق تنظيماً تفصيلياً متكاملاً لإجراءات جمع وتوثيق الأدلة الرقمية، وهى من الأدلة المستحدثة التى تتطلب ضرورة تنظيم أحكام التعامل معها بشكل مفصل، بالشكل الذى يحقق موثوقيتها أمام القضاء الجنائي، ومن ثَمَّ تعزيز الاستفادة منها فى مجال الإثبات الجنائي، حيث لم تتحدث اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات عن الآثار المترتبة علـى تخلف الشروط التى يجب توافرهـا فى الدليل الجنائى الرقمي، أو الضوابط ذات الصلة بالإجراءات المرتبطة بعملية جمع وتوثيق الدليل فى المراحل المختلفة، بجانب غياب الضوابـط المُتعلقة بحالات تلف الدليل فى أى مرحلة مـن مراحل التحقيق أو المُحاكمة، لذلـك سوف يكـون للاجتهادات القضائية جانب كبير فى سد الثغـرات التشريعية، إما من خلال تطبيق القواعد المعمول بها فى القواعد الخاصة بالدليل الجنائى بشكل عام، أو مـن خلال إرساء سوابق قضائية جديدة، هـذا بجانب المساحة التقديرية التى يتمتع بها القضاء فى تحديد ثبوتية وحجية الأدلة الجنائية الرقمية المُقدمة.

(١) سبـق لمحكمـة النقض التصدى لهذه المسألة، فقضـت بأنه: «لما كان الطاعـن لم يدفع أمام محكمة الموضـوع ببطلان الدليل المستمـد مـن كاميرات المراقبة على الأساس الذى يتحدث عنه فـى وجه طعنه – أى لوجود أعطـال بأجزاء فى بعض مقاطع الصـورة والصـوت المسجل عليها – فإن هذا الوجه من النعى غير مقبول، لما هو مقرر أن الدفع ببطلان إجراء من الإجراءات السابقـة على المحكمة مـن الأخذ بهذه التسجيلات – على فرض بطلانها– على أنها عنصر من عناصر الاستدلال مادام أنه كان مطروحاً على بساط البحث وتناوله الدفاع بالمناقشة». انظر: نقض٢٠١٧/٧/٣١، الطعن رقم (٣٢٤١٨) لسنة ٨٥ ق.

المبحث الثاني

الحصول على الدليل الرقمى وحمايته

نتناول فى هذا المبحث الحماية الجنائية للدليل الرقمي، وإجراءات جمع وتوثيق الأدلة الرقمية والجهات المعنية بذلك، والتعاون الدولى فى جمع الأدلة الرقمية، وذلك فى ثلاثة مطالب على النحو التالي:

المطلب الأول

الحماية الجنائية للدليل الرقمي

نتناول فى هذا المطلب الحماية الجنائية للدليل الرقمي، والتى قررها المشرع المصري، من خلال تجريم العبث بالأدلة الرقمية، وذلك على النحو التالي:

أولاً- نص التجريم:

تنص المادة (٢٨) من القانون على أنه:«يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين، كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكترونى أو نظام معلوماتى إذا أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها فى هذا القانون والتى وقعت على موقع أو حساب أو بريد إلكترونى بقصد إعاقة عمل الجهات الرسمية المختصة».

ثانياً- العلة من التجريم: تتمثل علة التجريم فى مجابهة كل من تسول له نفسه تضليل العدالة عن طريق العبث فى أدلة الجريمة من جانب المسئولين عن إدارة المواقع الإلكترونية، فى ضوء ما يشكله هذا السلوك من مساعدة لهم للهروب من المساءلة، فضلاً عما يمثله الدليل الرقمى من أهمية فى عملية الإثبات الجنائى للجرائم المعلوماتية باعتباره الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم[١]، ومن ثَمَّ يشكل هذا العبث فى الأدلة الرقمية تقويضاً لجهود رجال العدالة الجنائية وتضليلاً لهم فى ضبط مثل هذه الجرائم الخطيرة والوصول إلى الحقيقة التى تتغياها العدالة الجنائية.

(١) عبد الناصر محمد محمود فرغلى وآخر، الإثبات الجنائى بالأدلة الرقمية، مرجع سابق، ص١١.

ثالثـاً- محـل الجريمة: يتمثل محل الجريمة فى الدليل الرقمـي، وقد عرفه القانون بأنـه: «أى معلومات إلكترونية لها قوة أو قيمـة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخـوذة من أجهزة الحاسـب أو الشبكات المعلوماتية وما فـى حكمها، ويمكن تجميعها وتحليلهـا باستخدام أجهـزة أو برامج أو تطبيقات تكنولوجيـة خاصة»، ومن ثم يقصد بالدليـل الرقمى أى أثـر أو دليل يخلفه الجانى فى النظام المعلوماتى أو شبكة المعلومات وتتصل بارتكاب الجريمة.

رابعـاً- صفة الجاني: تطلـب القانون فى فاعل الجريمة أن يكـون مسئولاً عن إدارة موقع أو حساب خاص أو بريد إلكترونى أو نظام معلوماتي، وكان القانون قد عرف مدير الموقـع بأنـه:«كل شخص مسئول عن تنظيم أو إدارة أو متابعـة أو الحفاظ على موقع أو أكـثر على الشبكة المعلوماتيـة، بما فيها حقوق الوصول لمختلـف المستخدمين على ذلك الموقع، أو تصميمه، أو توليد وتنظيم صفحاته أو محتواه، أو المسئول عنه».

خامسـاً- الركن المـادي: يتكون الركن المـادى فى هذه الجريمة مـن أفعال الإخفاء والعبث بالأدلة الرقمية، وذلك على النحو التالي:

١- الإخفاء: يقصد بالإخفاء ستر الشيء عن أعين الناس وعدم إظهاره لهم، ويجب أن ينصـب هـذا الإخفاء على دليل رقمى يخص جريمة وقعت بالفعل، وهو ما تتحقق به جريمـة إعاقة سـير العدالة المنصوص عليها فى غالبيـة التشريعات الجنائية، ويستوى لـدى القانـون الوسيلة المستخدمة فى تحقيق الإخفاء، فقد تكـون برنامجاً أو أية وسيلة تقنيـة، كمـا يستوى لدى القانون أن يكون هذا الدليل هـو الدليل الوحيد فى الدعوى، أو أنه أحد الأدلة المرتبطة بها، ومن ثَمَّ قد يتخذ فعل الإخفاء صورة مسح الدليل أو إلغائه.

٢- العبـث بالأدلـة الرقمية: يقصد بالعبـث بالدليل الرقمى قيـام الجانى بأى فعل إيجابـى مـن شأنه تغيير طبيعـة هذا الدليـل أو عناصره، ومن ثَـمَّ التشكيك فى نسبته إلى الجانـى بما تتحقـق به كذلك إعاقة العدالة، ومن ثَمَّ قـد يتخذ العبث صورة تعديل معطيـات الدليل الرقمـي، بالشكل الذى يغير من شكل الدليـل أو طبيعته، أو موقعه، أو تعديـل مساره، وتـبرز الإشارة إلى أن المشرع قصر العبث علـى الأدلة الرقمية الناجمة عن إحدى الجرائم الواقعة على المواقع أو الحسابات الخاصة أو البريد الإلكتروني.

ويتحقـق هذا العبث من خلال استخدام الجانى لأية تقنية كالبرمجيات أو التقنيات

أو الأدوات التـى من شأنها تعديل المعطيـات والبيانات، أو تغيير الطبيعة المعنوية للدليل الرقمـي، حيث يستـوى لدى القانون الوسيلة التى يستخدمهـا الجانى فى تحقيق العبث بالدليل الرقمي، سواء كانت هذه البرامج أو التقنيات قد استخدمت عبر شبكة معلوماتية أو باستخـدام برمجيات خبيثة تقوم بتغيـير أو تعديل أو محو المعلومات أو البيانات التى تشكل الدليل الرقمي.

سادسـاً- الركن المعنـوي- من جرائم القصد الخاص: هـذه الجريمة من الجرائم العمدية التى يتحقق فيها الركن المعنوى بتوافر القصد الجنائى العام بعنصريه: العلم، والإرادة، فضـلاً عـن توافـر قصد جنائى خاصـ يتمثل فى قصد إعاقـة عمل الجهات الرسمية المختصة، حيث يجب أن تتجه إرادة الجانى إلى الإخفاء أو العبث بغرض إعاقة سير السلطات الرسمية، ويقصد بالسلطات الرسمية فى هذه الجريمة السلطات العامة المعنية بمكافحة الجرائم المعلوماتية، من جهات الضبط أو التحقيق أو المحاكمة.

سابعـاً- العقوبة: عاقب القانـون على هذه الجريمة بعقوبـة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتـين العقوبتين، ومن ثَمَّ يجـوز للقاضى توقيع عقوبة الحبـس أو الغرامة أو العقوبتين معـاً، ويجوز للقاضـى فى هذه الجريمة أن يحكـم بإيقاف التنفيذ وفقـاً لأحكام المادة (٥٥) عقوبـات، والخطأ فى الجرائم غير العمدية هو الركـن المميز لها، ومن ثَمَّ يجب على المحكمة بيان عنصر الخطأ المرتكب والدليل عليه [١].

(١) نقضـ ٢٠١٣/٣/٢٥، الطعـن رقم (٢١٣٣٥) لسنة ٧٧ق، المستحدث من المبادئ الصادرة عن الدوائر الجنائية من أول أكتوبر ٢٠١٢ لغاية آخر سبتمبر ٢٠١٣، الصادرة عن المكتب الفنى لمحكمة النقض، المجموعة الجنائية، ص ص٥٣، ٥٤.

المطلب الثاني

إجراءات جمع وتوثيق الأدلة الرقمية

نتناول فيما يلى إجراءات جمع وتوثيق الأدلة الرقمية فى ثلاثة أفرع، وذلك على النحو التالي:

الفرع الأول

إجراءات جمع الأدلة الرقمية

اتجهت العديد من التشريعات المُقارنة والاتفاقيات الدولية إلى النص على إجراءات مُستحدثة تتوافق مع النظام المعلوماتي، والتى تهدف إلى تسهيل مُهمة جمع الأدلة فى مجال جرائم تقنية المعلومات، فغالبية هذه الإجراءات مستحدثة وغير مألوفة فى القواعد الإجرائية التقليدية المستخدمة فى جمع الأدلة، ويعبر عنها بمصطلحات بيئة التقنية، ولا شك فى أن هذه الإجراءات تتلاءم مع طبيعة جرائم تقنية المعلومات، ولها دور مهم فى تحديد مرتكبى هذه الجرائم وجمع الأدلة ضدهم، ولهذا تلاقى قبولاً لدى الكافة، إلا أنها يجب أن تتم وفقاً للقانون، وفى إطار التوازن بين استخدام الوسائل الحديثة فى كشف الجرائم وجمع أدلتها وبين الحرية الشخصية للأفراد[1]، ويمكن تقسيم الإجراءات الجديدة لجمع الأدلة إلى قسمين: (الإجراءات المهدة لجمع الأدلة- إجراءات جمع الأدلة)، وذلك على النحو التالي:

أولاً- الإجراءات المهدة لجمع الأدلة: الإجراءات المهدة لجمع الأدلة هى عبارة عن نوع من المراقبة والمتابعة لاستخدام وسائل تقنية الاتصالات الحديثة، وتسجيل كافة البيانات المخزنة بالأجهزة المستخدمة فى هذه الاتصالات (الحاسب الآلى والإنترنت)، وهذه إجراءات تتخذ فى الغالب قبل التحقيق فى الجريمة، ولا يعد اتخاذها تحريكاً للدعوى ضد أى شخص، ويتولى القيام بها مقدمو الخدمة بتكليف من السلطة المختصة باعتبارها إجراءات لازمة وضرورية لتسهيل مهمة سلطة التحقيق فى كشف جرائم تقنية المعلومات والبحث عن أدلتها وضبطها.

---

(١) د. وليد نبيل طه، الجرائم الإلكترونية طبقاً لاتفاقية بودابست، ورقة عمل مقدمة لندوة (الواقع الأمنى «مسئوليات- إنجازات») والتى انعقدت بتاريخ ٢٠١١/١/٩، مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة، ص٢٤.

وقد نصت اتفاقية بودابست على نوعين من هذه الإجراءات هي: (إجراءات التحفظ السريع على مضمون البيانات المخزنة - إجراءات التحفظ على البيانات المتعلقة بخط سير البيانات).

١- إجراءات التحفظ السريع على مضمون البيانات المخزنة: تتمثل إجراءات التحفظ السريع على مضمون البيانات المخزنة فى إصدار أوامر إلى مقدمى الخدمة بالحفاظ على البيانات المخزنة بالنظم المعلوماتية والإنترنت لفترة زمنية معينة، وقد نصت المادة (١٦) من الاتفاقية على أنه: «يجب على كل دولة طرف أن تتبنى الإجراءات التشريعية وأية إجراءات أخرى ترى أنها ضرورية لتخويل سلطاتها المختصة أن تأمر بالتحفظ العاجل على البيانات المخزنة»، والغرض من ذلك هو تمكين السلطة المختصة بالتحقيق فى جرائم تقنية المعلومات من معرفة مضمون البيانات التى أرسلها المشترك أو استقبلها سواء عن طريق طلبها من مقدمى الخدمة أو خلال القيام بالتفتيش[(١)]، وعلى ذلك فإن الأمر الذى تصدره السلطة المختصة فى الدولة يلتزم بمقتضاه مقدمو الخدمة بالحفاظ على البيانات وحمايتها من الضياع أو التعديل أو المحو، وبالحفاظ على سريتها ومنع الغير من الحصول أو الوصول إليها، وتختلف مدة التحفظ على البيانات من تشريع لآخر، وإن كانت الاتفاقية قد حددتها بمدة لا تتجاوز ٩٠ يوماً (م ١٦/٣ من الاتفاقية) [(٢)]، ويختص

(١) د. وليد نبيل طه، المرجع السابق، ص٢٥.

(٢) نصت المادة الثانية من القانون رقم (١٧٥) لسنة ٢٠١٨ المعنونة بالتزامات وواجبات مقدم الخدمة، على التزام مقدم الخدمة بحفظ وتخزين سجل النظام المعلوماتى أو أى وسيلة لتقنية المعلومات، لمدة مائة وثمانين يوماً متصلة، حيث تقضى المادة المشار إليها بأنه: «(أولاً): مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ المشار إليه، يلتزم مقدمو الخدمة بما يأتي: - (١) حفظ وتخزين سجل النظام المعلوماتى أو أى وسيلة لتقنية المعلومات، لمدة مائة وثمانين يوماً متصلة. وتتمثل البيانات الواجب حفظها وتخزينها فيما يلي: - أ - البيانات التى تمكن من التعرف على مستخدم الخدمة. ب- البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتى المتعامل فيه متى كانت تحت سيطرته. ج- البيانات المتعلقة بحركة الاتصال. د - البيانات المتعلقة بالأجهزة الطرفية للاتصال. هـ- أى بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز. (٢) المحافظة على سرية البيانات التى تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة – ويشمل ذلك البيانات الشخصية لأى من مستخدمى خدمته، أو أية بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التى يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التى يتواصلون معها. (٣) تأمين البيانات والمعلومات بما يحافظ على سريتها. عدم اختراقها أو تلفها. (ثانياً): مع عدم الإخلال بأحكام قانون حماية المستهلك، يجب على مقدم الخدمة أن يوفر لمستخدمى خدماته ولأى جهة حكومية مختصة، فى الشكل وبالطريقة التى يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية: (١) اسم مقدم الخدمة وعنوانه. (٢) معلومات الاتصال المتعلقة بمقدم الخدمة، بما فى ذلك عنوان الاتصال الإلكتروني. (٣) بيانات الترخيص =

بإصدار أمر التحفظ السلطة التى يحددها التشريع الداخل لكل دولة [١].

٢- إجراءات التحفظ السريع على البيانات المتعلقة بخط سير البيانات: يقصد بالتحفظ على البيانات المتعلقة بخط سير البيانات إلزام مقدمى الخدمة بالحفاظ على البيانات والمعلومات المخزنة عن مصدر الاتصالات، ووقتها ومقدمى الخدمة الذين ساهموا فى نقل البيانات، ويرجع السبب فى اتخاذ هذا الإجراء إلى أنه يسهم فى التعرف على مرتكبى جرائم تقنية المعلومات والمساهمين معهم، إلا أن تنفيذ هذا الإجراء يتطلب سعة تخزينية كبيرة، وغالباً ما يتم تحديد مراقبة خط سير بيانات معينة السلطات المختصة بالتحرى عنها ومتابعة أصحابها.

ويختلف إجراء التحفظ على البيانات المتعلقة بخط سير البيانات، عن التحفظ السريع على مضمون البيانات الذى نصت عليه المادة ١/١٦ من الاتفاقية، فى أن التحفظ يقتصر على البيانات المتعلقة بالاتصال من حيث مصدرها ووقتها ومرسلها ومستقبلها، ومن ساهم فى نقلها، ولا يشمل محتوى البيانات، وما تتضمنه من معلومات، وهذا الإجراء كسابقه يحتاج إلى تقنية عالية، تساعد مقدم الخدمة فى القيام به فى وقت سريع، بغية إعطاء السلطة المختصة فرصة اتخاذ الإجراء اللازم لكشف مرتكب الجريمة وضبط أدلتها[٢]، وقد نصت المادة (١/١٧) من الاتفاقية على ضرورة تبنى الدول تشريعات تكفل قيام مقدمى الخدمات بالتحفظ السريع على البيانات المتعلقة بخط سير البيانات، كما نصت الفقرة الثانية من المادة ذاتها على ضرورة أن تتبنى الدول الإجراءات التى تتضمن قيام مقدم الخدمة بالإفشاء السريع لتلك البيانات للسلطة المختصة[٣].

= لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التى يخضع لإشرافها. (٤) أية معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمى الخدمة، ويحددها قرار يصدره الوزير المختص. (ثالثاً): مع مراعاة حرمة الحياة الخاصة التى يكفلها الدستور يلتزم مقدمو الخدمة، أن يوفروا حال طلب أجهزة الأمن القومى ووفقاً لاحتياجاتها كافة الإمكانيات الفنية من معدات ونظم وبرامج والتى تتيح لتلك الجهات ممارسة اختصاصاتها وفقاً للقانون. (رابعاً): يلتزم مقدمو خدمات تقنية المعلومات ووكلاؤهم وموزعوهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، ويحظر على غير هؤلاء القيام بذلك».

(١) نظم المشرع الأمريكى فى القانون الخاص بمكافحة جرائم الكمبيوتر والإنترنت الصادر تنفيذاً لاتفاقية بودابست إجراءات التحفظ على مضمون البيانات بأن نص عليه فى المادة (USC ١٨ ٢٧٠٣)، ونص عليه المشرع الفرنسى فى المادة (٥٦) إجراءات فرنسي. انظر: د. وليد نبيل طه، الموضع السابق.

(٢) د. وليد نبيل طه، مرجع سابق، ص٢٦.

(٣) نص المشرع الأمريكى على هذا الإجراء بمقتضى المادة (USC ١٨ ٢٧٠٣)، كما نص قانون الإجراءات الفرنسى على هذا الإجراء كذلك فى المادة (٣/٩٩) إجراءات فرنسي. انظر: د. وليد نبيل طه، الموضع السابق.

٣- إجراءات التحفظ العاجل على بيانات الحاسب الآلى المخزنة: فيما يتعلق بالتحفظ العاجل على بيانات الحاسب الآلى المخزنة، فيجوز لأطراف هذه الاتفاقية الطلب من الأطراف الأخرى التحفظ العاجل على بيانات كومبيوتر يقع فى إقليم الطرف الآخر، وقد بينت المادة (٢٩) الإجراءات المتبعة، ويجوز للطرف الآخر اشتراط ازدواجية الجريمة، وله حق الرفض إذا ما تعلق الطلب بجريمة سياسية أو أن تنفيذ الطلب يمس السيادة أو الأمن أو النظام العام، وفيما يتعلق بالدخول على بيانات الحاسب الآلى فى إقليم دولة أخرى، فيجوز الدخول عن طريق الموافقة، أو إذا ما كانت متاحة علناً، وعلى الدول الأعضاء تعيين نقطة اتصال ٢٤/٧ لضمان توافر المساعدة الفورية.

ثانياً- الإجراءات الخاصة بجمع واستخراج الأدلة الرقمية المتعارف عليها دولياً: نصت اتفاقية بودابست فى المواد (١٨-٢١) على مجموعة من القواعد الإجرائية، بقصد التثبت من وقوع الجريمة والبحث عن مرتكبها وجمع أدلتها، وأغلبها إجراءات جديدة ذات مسميات غير مألوفة فى إجراءات التحقيق التقليدية، وهى وإن كانت لا تتضمن أى حجر أو قيد على حرية الأشخاص، إلا أن اتخاذها يحتاج إلى تشريع خاص يسمح بمباشرتها لمساسها بحقوق الإنسان، وتتمثل أهم إجراءات جمع الأدلة الرقمية فيما يلي:

١- إصدار أمر بتقديم بيانات محددة: يقصد بإصدار أمر بتقديم بيانات محددة تخويل السلطة المختصة بإصدار أمر إلى مقدم الخدمة، أو أى شخص فى حيازته أو تحت سيطرته بيانات معينة بتقديم تلك البيانات، سواء أكانت هذه البيانات تتعلق بالمحتوى أم بخط السير، وهذا الإجراء كغيره من الإجراءات السابقة يصدر عن جهة مختصة، وينفذه أشخاص لا يتبعون هذه السلطة؛ إذ هم عبارة عن أشخاص فى حيازتهم أو تحت سيطرتهم بيانات مخزنة داخل النظام المعلوماتي، أو فى دعامة تخزين المعلومات؛ بمعنى أن الأمر يصدر لصاحب الحيازة المادية للبيانات ولصاحب السيطرة ولو لم يحزها حيازة مادية، وقد نصت المادة (١٨) من الاتفاقية الأوروبية على ضرورة أن تتبنى الدول تشريعات تلزم مقدم الخدمة وغيره من الأشخاص بتقديم بيانات معينة تكون فى حيازتهم أو تحت سيطرتهم ومخزنة فى النظام المعلوماتى أو دعامة التخزين، وهو ما سار عليه المشرع الأمريكى بالنص على هذا الإجراء فى المادة (١٨ usc٢٧٠٣).

٢- تفتيش وضبط البيانات المخزنة: نصت المادة (١٩) من الاتفاقية على ضرورة أن تتبنى الدول الأطراف تشريعات إجرائية تخول سلطة معينة اختصاصات تكفل البحث عن أدلة الجريمة وضبطها، وترد إجراءات التفتيش والضبط على البيانات المخزنة فى النظام المعلوماتي، أو فى دعامة تخزين المعلومات، سواء أكانت هذه البيانات مخزنة فى جهاز واحد أم فى منظومة اتصالات، وقد حددت هذه المادة الإجراءات الخاصة بجمع الأدلة فى الآتي:

أ- التفتيش أو الدخول المشابه: نصت المادة (١/١٩) من اتفاقية بودابست على وجوب أن تتبنى كل دولة طرف تشريعات تخول السلطة المختصة اختصاص التفتيش أو الدخول المشابه، وتحديد مصطلح التفتيش لا يثير أية صعوبة؛ إذ يقصد به البحث والتنقيب عن أدلة الجريمة بفحص البيانات ومحاولة معرفة محتواها أو خط سيرها، أما مصطلح الدخول وما يعبر عنه أحياناً بالولوج فهو مصطلح خاص بنظم التكنولوجيا والاتصال، يحقق الوصول إلى البيانات المخزنة، ويقتضيه بطبيعة الحال إجراء التفتيش والحصول على الأدلة، ولهذا ثمة فرق بين الاثنين، فالدخول إجراء للتفتيش، والتفتيش وسيلة لجمع الأدلة، ورغم هذه التفرقة فإنهما يعتبران من إجراءات التحقيق الماسة بحقوق الأفراد؛ لذا يجب أن يستند اتخاذها إلى نص قانوني، وهذا ما نصت عليه المادة (٢/١٩) من الاتفاقية[(١)].

ب- الضبط أو الحصول: نصت المادة (٣/١٩) من الاتفاقية على وجوب أن تتبنى كل دولة طرف تشريعات تخول السلطة المختصة اختصاص الضبط أو الحصول على البيانات المخزنة، ويشمل هذا الاختصاص الإجراءات الآتية: (الضبط أو الوصول إلى البيانات - التحقق والتحفظ على نسخة من البيانات - المحافظة على سلامة البيانات - منع الوصول إلى هذه البيانات أو رفعها من النظام المعلوماتي).

ويمكن تقسيم الإجراءات التى نصت عليها المادة (٣/١٩) إلى نوعين: **(الأول)**: إجراءات تحفظية، تهدف إلى الحفاظ على البيانات المخزنة التى ترى الجهة المختصة أهميتها فى التحقيق ببقائها فى أمكنتها فى النظام المعلوماتى أو فى دعامة التخزين، ومنع الوصول إليها أو إلغائها أو التصرف فيها، **(والثاني)**: إجراءات ضبط، وهى

(١) نص المشرع الأمريكى على هذا الإجراء فى المادة (USC ٢٧٠٣ ١٨)، ونص عليه قانون الإجراءات الجنائية الفرنسى فى المادتين (٥٦) و (٩٧) إجراءات جنائية. د. وليد نبيل طه، مرجع سابق، ص٢٩.

إجراءات لاحقة للتفتيش والدخول، ويقصد بها جمع البيانات سواء بأخذ دعامة تخزين المعلومـات ذاتها، أو بعمل نسخة من البيانات المخزنة بها أو بالنظام المعلوماتى فى ورق أو أقراص، وهو ما نص عليه القانون الأمريكى (usc ٢٧٠٣ ١٨).

ثالثـاً- التجميـع فى الوقت الفعلى لبيانـات خط سير البيانـات: نصت المادة (٢٠) مـن الاتفاقية علـى التجميع فى الوقـت الفعلى لخط سـير البيانات، وذلك بـأن تتبنى الدول الأطـراف تشريعات تخول سلطة معينة القيام بجمع أو تسجيل عن طريق وسائل معينة موجودة على أرضها البيانات المتعلقة بخط سير البيانات فى الوقت الصحيح، أو إلـزام مقدم الخدمة فى حدود قدرته الفنية بجمع وتسجيل البيانات المتعلقة بخط سير البيانات فى الوقت الصحيح.

ويهدف هذا الإجراء الخاص بالتجميع فى الوقت الفعلى للبيانات المتعلقة بخط سير البيانـات الذى قد تقـوم به السلطة المختصة فى الدولـة، أو ينفذه مقدمو الخدمة بناء علـى أوامر صادرة إليهم من السلطة المختصة بهذا الإجراء، إلى تسهيل مهمة الجهات القائمـة بجمع الأدلة، ويختلف إجـراء التجميع فى الوقت الفعلي للبيانات المتعلقة بخط سـير البيانات، عن إجراء التحفـظ السريع على البيانات المتعلقـة بخط سير البيانات الذى نصـت عليه المادة (١٦) من الاتفاقية، فى أن البيانات فى حالة التحفظ موجودة لدى الجهة مقدمة الخدمة؛ أى مخزنة بالنظام المعلوماتى أو فى دعامة التخزين، بينما فـى حالة التجميـع أو التسجيل فالبيانـات ليست مخزنة، وتهدف هـذه الإجراءات إلى جمعها أو تسجيلها وقت مباشرة الاتصال، وهذا ما عبرت عنه الاتفاقية بالوقت الفعلى أو الصحيـح، ولهـذا فهو يحتـاج إلى وسائل تقنيـة حديثة قد لا تتوافـر لدى السلطة المختصـة، أو قـد لا يكون بمقـدورهـا القيام به، وعلـى ذلك أسنـدت الاتفاقية القيام بإجراء التجميع أو التسجيل للسلطة المختصـة فى الدول لتقوم به بنفسها أو تنفذه من خـلال مقدم الخدمة أو بمساعدته، وهو ما نص عليه القانون الأمريكى فى المادة (usc ٢٧٠٣ ١٨)، وكذلك القانون الفرنسى فى مادته (٢/٦٠ إجراءات فرنسي).

رابعـاً- اعتراض مضمون البيانـات: نصت المادة (٢١) مـن الاتفاقية على ضرورة تبنـى كل دولـة طرف تشريعات تخول سلطـة معينة القيام باعتراض محتوى البيانات المتعلقـة بجرائـم خطيرة، ويتـم الاعتراض بأحـد إجراءيـن: (الأول): قيـام السلطة المختصة بإجـراءات التجميع أو التسجيـل لمضمون البيانات، (والثـاني): إلزام مقدم

الخدمة بتجميع أو تسجيل محتوى البيانات، والمقصود باعتراض مضمون البيانات جمع أو تسجيل مضمون البيانات التى تنقل عبر وسائل الاتصال فى حينها، حتى تتمكن السلطات المختصة فى الدولة من التعرف على الاستخدامات غير المشروعة لأنظمة الاتصالات، بما يكفل منع ارتكاب الجرائم، والأصل أن إجراء اعتراض مضمون البيانات تباشره سلطة معينة بالدولة، إلا أن الاتفاقية أجازت إلزام مقدم الخدمة بالقيام به على أساس أنه قد تتوافر لديه الإمكانيات الفنية اللازمة لذلك، ويلاحظ أن هذا الإجراء يختلف عن إجراء التحفظ السريع على مضمون البيانات الذى نصت عليه المادة (١٦) من الاتفاقية، فى أن البيانات المطلوب التعرف على مضمونها مخزنة، ويلتزم مقدم الخدمة بالتحفظ عليها، بينما يعد الاعتراض على مضمون البيانات نوعاً من المراقبة المعاصرة للاتصال، وتجميع وتسجيل مضمون أية اتصالات تتعلق بمسائل غير مشروعة[١].

الفرع الثاني

إجراءات توثيق الدليل الرقمي

أولاً- توثيق الدليل الرقمي: تأتى مرحلة توثيق وتوصيف الدليل الجنائى الرقمى فى مرحلة لاحقة على عملية الجمع واستخراج الدليل، وهى مرحلة يتم فيها إنتاج المعلومات المُخزنة على أحد الأجهزة أو الشبكات إلى معلومات فى صورة نسخ مطبوعة، وذلك من خلال طباعة نسخ من الملفات المخزن عليها أو تصويرها بأى وسيلة مرئية أو رقمية، وقد حددت المادة (١٠) من اللائحة التنفيذية للقانون كيفية توثيق الدليل الرقمي، حيث نصت المادة المشار إليها على أنه:«يتم توصيف وتوثيق الدليل الرقمى من خلال طباعة نسخ من الملفات المخزن عليها أو تصويرها بأى وسيلة مرئية أو رقمية، واعتمادها من الأشخاص القائمين على جمع أو استخراج أو الحصول أو التحليل للأدلة الرقمية، مع تدوين البيانات التالية على كل منها:

١ - تاريخ ووقت الطباعة والتصوير.

(١) نص المشرع الأمريكى على هذا الإجراء فى المادة (USC ٢٧٠٣ ١٨)، وقد أشارت المادة بضرورة أن يصدر الأمر باتخاذ هذا الإجراء من المحكمة أو من الإدارة العليا للعدل على ألا تزيد مدة الاعتراض على ٣٠ يوماً، كما نص على هذا الإجراء قانون الإجراءات الفرنسى فى المادة (٩٥/٧٠٦) إجراءات جنائية.انظر: د. وليد نبيل طه، مرجع سابق، ص٣١.

٢ – اسم وتوقيع الشخص الذى قام بالطباعة والتصوير.

٣ – اسم أو نوع نظام التشغيل ورقم الإصدار الخاص به.

٤ – اسم البرنامج ونوع الإصدار أو الأوامر المستعملة لإعداد النسخ.

٥ – البيانات والمعلومات الخاصة بمحتوى الدليل المضبوط.

٦ – بيانات الأجهزة والمعدات والبرامج والأدوات المستخدمة».

ولا شك فى كفاية هذه البيانات التى تطلبتها اللائحة للاستيثاق من عملية جمع الدليل الرقمى وتوثيقه.

ثانياً– أدوات توثيق الدليل الرقمي: يستعين خبراء الأدلة الجنائية الرقمية –فى إطار عملهم التقني– بأدوات أو برمجيات أو أجهزة تقنية تساعد على إيجاد صورة للدليل الرقمي، من أبرز هذه الأجهزة جهاز مانع الكتابة والذى من شأنه منع إلحاق أى تغييرات على البيانات الأصلية[١]، وبرامج «نحت البيانات أو الملفات» والتى من شأنها استعادة الملفات المحذوفة أو التالفة من بقايا البيانات الأولية التى تبقى على أجهزة التخزين حتى بعد زوال الملف الأصلي[٢]، والعمل على إيجاد نسخة «خطوة بخطوة» للمعلومات المخزنة، وفى بعض الأحيان يستعين خبراء الأدلة الجنائية الرقمية بأدوات تحليل تجزئات التشفير للتعامل مع الملفات المشفرة؛ إذ إن أى تغيير بسيط للبيانات، ينتج عنه حدوث تشفير مختلف.

ومن الجدير بالذكر أن الأجهزة والبرمجيات والأدوات التقنية المستخدمة من قبل الخبراء لجمع الأدلة الرقمية تختلف بحسب نوعية الوسائط التقنية المستخدمة، كما أنها تتطلب تقنيات مختلفة لتحقيق هذه الأدلة الرقمية، فأجهزة المحمول تختلف أدوات فحصها عن تلك المستخدمة فى فحص جهاز حاسب مكتبى أو خادم شبكة، فقد تشتمل عملية جمع الأدلة الرقمية على إجراء فحص وتحليل الأجهزة الإلكترونية وأجهزة الحاسب المكتبى والمحمول الكائنة فى المنازل وأماكن العمل، والتى عادةً ما تحتوى على أقراص صلبة ذات سعة كبيرة من شأنها تخزين كمية كبيرة من المعلومات، بما فى ذلك

(١) انظر: المعهد الأمريكى الوطنى للمعايير والتكنولوجيا، ٢٠٠٤، جهاز مانع الكتابة (HWB) مواصفات، الإصدار ٢,٠، مشار إليه: دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٣١.

(٢) غوتمان بي، الحذف الآمن للبيانات، مرجع سابق، مشار إليه: دراسة مكتب الأمم المتحدة، الموضع السابق.

الصـور ومقاطع الفيديو، فضلاً عن تواريخ تصفـح المواقع الإلكترونية، ورسائل البريد الإلكترونـى ومعلومـات التراسل الفوري، والتى عـادةً ما تقوم بتشغيـل عدد صغير من أنظمـة التشغيل؛ كالوينـدوز والماك أو إس ولينوكس، بينمـا تشمل عملية فحص أجهزة المحمول أجهزة محمولة صغيرة الحجم تعمل بطاقة منخفضة، وذات سعة تخزين أقل، وببرامج أبسط لتسهيل المكالمات الهاتفية وتصفح الإنترنت[١].

وتبرز الإشارة إلى أن أجهزة المحمول والأجهزة اللوحية – والتى غالباً ما تكون بمثابة نسخ مطورة من أجهزة المحمول– قد تشكل بالنسبة للمحققين كنزاً هائلاً من المعلومات ذات الصلـة بارتكاب الجرائم، بالنظر لما تتسم به من سمات مميزة، أبرزها: قابليتها علـى التنقـل، ووجودها بصحبـة مالكها فى كل الأوقـات، واتصالهـا المستمر بشبكات الاتصـالات، ممـا يساعد فى الحصول علـى مراقبة دقيقة للموقـع الجغرافى إلى حد معقول، علاوة على ما تحتويه من قائمة جهات الاتصال وسجلات المكالمات، فضلاً عن تدفق جميع المعلومات والبيانات عبر شبكات مقدمى خدمات الإنترنت المحمول[٢].

كما تحظى تقنيات الأدلة الجنائية الخاصة بالشبكات المعلوماتية بأهمية كبيرة، من خـلال ارتباطها بالهواتـف المحمولة وأجهزة الحاسـب الآلي، واستخدامها فى خدمات الإنترنـت والتخزيـن السحابـي، حيث يتـم تخزين البيانـات على الإنترنـت من خلال مراكز بيانـات، بدلاً من تخزينها على جهاز المستخدم، الأمر الذى يدعو إلى استخدام نظـم لتحليل المعلومات على هـذه الشبكات للتوصل إلى كمية مـن المعلومات التى يمكن تجميعهـا، ويتعين للحصول علـى معلومات مفصلة بخصوص الأنشطة التى تجرى فى الشبكـة وتخزينهـا، أن يكون جمـع البيانات بصـورة نشطة وتخزينهـا للتحليل لاحقاً، ويمكـن أن تشمل هذه العملية تحليلاً لملفات السجلات من أجهزة الشبكة، مثل: جدران الحمايـة وكشـف التسلل، فضـلاً عن نظم الوقايـة، وكذلك تحليل محتـوى نقل بيانات الشبكة المسجلة فى حال توافرها[٣].

غنـى عن البيان أنه فى الحالات التى يتمكـن فيها الجانى من الدخول غير المشروع والتسلل لأحد نظـم الحاسب، فإن البيانات الموجودة على هذا الحاسب تصبح معرضة

(١) انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٣٢.

(٢) الموضع السابق.

(3) Chappell, L., 2012. Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide. Laura Chappell University.

للخطـر من طرف المهاجم، ولا يعتد بملفات السجـلات لنشاط هذا النظام، ومن ثَمَّ لا تمثل التحقيقات الجنائية للشبكة الصيغة الوحيدة المتاحة لأى محلل؛ إذ يكمن التحدى الأساسـى فى هـذه الحالة فى إعـادة القيام بالإجـراءات التى اتخذت علـى أى شبكة مـن بيانات السجلات المحـدودة المتاحة، واستخدام ذلك فى تحديـد محاولات التسلل والدخـول غير المشروع للنظم المعلوماتية ومحـاولات قطع الخدمة، إضافة إلى البيانات الخاصة بأى الموارد التى وصل إليها الأفراد فى أى وقت[١].

الفرع الثالث

الجهات المعنية بجمع واستخلاص الدليل الرقمى

يمر الحصول على الدليل الجنائى الرقمى بمراحل مُتعددة، من بينها (جمع الدليل الرقمي- استخراجه- حفظه- تحريـزه- توثيقـه وتوصيفـه)، لذلك حـددت اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات الأشخاص المعنيين بجمع واستخلاص الدليل الرقمى فى طائفتين: الأولى: مأمورو الضبط القضائي، والثانية: الخبراء، وذلك على النحو التالي:

أولاً- مأمـورو الضبط القضائي: عنيت المادة الخامسة من القانون بتحديد مأمورى الضبط القضائى فى جرائم تقنية المعلومات؛ إذ تقضى المادة المذكورة بأنه:«يجوز بقرار مـن وزير العدل بالاتفـاق مع الوزير المختص منح صفة الضبطيـة القضائية للعاملين بالجهـاز أو غيرهم ممن تحددهـم جهات الأمن القومى بالنسبة إلى الجرائم التى تقع بالمخالفـة لأحكام هذا القانون والمتعلقـة بأعمال وظائفهم»، ومن ثَـمَّ يتضح أن المشرع المصـرى أجاز لوزيـر العدل بالاتفاق مع الوزيـر المعنى بشئون الاتصـالات وتكنولوجيا المعلومات منح صفة الضبطية القضائية للعاملين بالجهاز القومى لتنظيم الاتصالات أو غيرهم ممن تحددهم جهات الأمن القومى المحددة بالقانون، وهي: رئاسة الجمهورية، ووزارة الدفـاع، ووزارة الداخليـة، والمخابـرات العامـة، وهيئـة الرقابـة الإداريـة[٢]، بالنسبـة للجرائم التى تقـع بالمخالفة لأحكام هذا القانون والمتعلقـة بأعمال وظائفهم،

(١) انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٣٣.

(٢) تبرز الإشارة إلى اقتراح أحد أعضاء البرلمان إضافة وزارة المالية ضمن جهات الأمن القومي، إلا أن هذا المقترح لم يلق قبولاً مـن أعضـاء البرلمان. انظر: مضبطة مجلس النواب المصري، الفصل التشريعى الأول، دور الانعقـاد العادى الثالث، الجلسة السادسة والخمسين، المعقودة فى ٢٠١٨/٥/١٤، ص٨٦.

وجديـر بالذكـر أن وزارة الداخلية فى مصر كان لها السبق فـى استحداث إدارة أمنية متخصصة، سُميت بإدارة مكافحة جرائم تقنية المعلومات، تعنى بضبط ومكافحة هذه الطائفـة مـن الجرائم، ومن ثَمَّ يمكن التمييز فى هـذا الشأن بين طائفتين من مأمورى الضبط القضائي: الأولى: من مأمورى الضبط من رجال الشرطة، والثانية: من مأمورى الضبـط الفنيين أو المتخصصين من العاملين بـوزارة الاتصالات وتكنولوجيا المعلومات ممن خولهم القانون صفة الضبطية القضائية.

وقـد أشارت اللائحـة بشكل عـام إلى ضرورة أن يكـون مأمورو الضبـط القضائى الذيـن يقومون بأى من الإجراءات المُتعلقة بالدليـل الرقمى من المخول لهم التعامل فى هـذه النوعيـة من الأدلة، ويفهم من ذلـك أنه فيما عدا مأمـورى الضبط المُختصين أو الصـادر لهم قرار بالضبطيـة القضائية فى الجرائم المُنصوص عليها بقانون جرائم تقنيـة المعلومات لا يحـق لأى مأمور قضائى جمع الدليل الرقمى أو استخراجه أو حفظه أو تحريزه، ومن ثَمَّ تحرير محاضر الضبط المتعلقة بالأدلة.

وتقضـى المـادة (٦) من القانون رقـم ١٧٥ لسنة ٢٠١٨ المعنونـة بالأوامر القضائية المؤقتـة بأنه: «لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأمورى الضبـط القضائى المختصين، لمدة لا تزيد على ثلاثـين يوماً قابلة للتجديد لمرة واحدة، متـى كان لذلـك فائدة فى ظهور الحقيقـة على ارتكاب جريمة معاقـب عليها بمقتضى أحكام هذا القانون، بواحد أو أكثر مما يأتي:

١- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها فى أى مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه. ويتـم تسليـم أدلتها الرقمية للجهة مصـدرة الأمر، على ألا يؤثر ذلـك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتضٍ.

٢- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط.

٣- أن تأمـر مقـدم الخدمة بتسليـم ما لديه من بيانـات أو معلومـات تتعلق بنظام معلوماتى أو جهاز تقنى موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمى خدمتـه وحركـة الاتصـالات التى تمت على ذلـك النظـام أو النظام التقنـي. وفى كل الأحوال، يجب أن يكون أمر جهة التحقيق المختصة مسبباً.

ويكـون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة فى غرفة المشورة، فى المواعيد ووفقاً للإجراءات المقررة بقانون الإجراءات الجنائية»[(١)].

ثانياً- الخبراء: تضمنت المادة (١٠) من القانون رقم (١٧٥) لسنة ٢٠١٨م المعنونة بـ «الخبراء»، النص على إنشاء سجلين: الأول: لقيد الخبراء التقنيين العاملين بالجهاز القومـى لتنظيـم الاتصالات، والثاني: للخـبراء التقنيين من خارج الجهـاز؛ إذ تقضى المـادة المذكـورة بأنه: «يُنشـأ بالجهاز سجـلان لقيد الخـبراء، يقيد بأولهمـا الفنيون والتقنيـون العاملـون بالجهـاز، ويقيد بالآخر الخـبراء من الفنيـين والتقنيين من غير العاملـين بـه. وتطبق على الخبراء فـى ممارسة عملهم وتحديـد التزاماتهم وحقوقهم القواعـد والأحكـام الخاصة بقواعد تنظيم الخبرة أمام جهـات القضاء. واستثناء من تلـك القواعد، تسرى على الخبراء المقيديـن بالسجل الثانى القواعد والأحكام الخاصة بالمساءلـة الإدارية والتأديبية الواردة بالقانـون المنظم لعملهم إن وجد. وتحدد اللائحة التنفيذية لهذا القانون قواعد وشروط وإجراءات القيد فى كل من السجلين».

وقد أشارت المـادة (٦) من اللائحة التنفيذية للقانون الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠ إلى أنه:«يقوم الخبراء وفقًا للمادتين رقمى (١)، (١٠) مـن القانـون بتنفيذ المهام الفنية والتقنية التى يتم تكليفهـم بها من جهات التحقيق أو

---

(١) ومـن أبـرز هـذه الصكوك الدولية متعـددة الأطراف المعنيـة بمكافحة جرائم تقنيـة المعلومات التى تضمنـت أحكاماً تتعلق بالأوامـر الخاصـة بجمع الأدلـة الرقمية والحصول علـى البيانات المخزنـة، الاتفاقية العربيـة بشأن مكافحـة جرائم تقنية المعلومـات (م١/٢٥)، واتفاقية بودابست (الاتفاقية الأوروبية) بشأن الجريمة الإلكترونية (م١٨/١/أ)، والتى تنص على أن: «نطـاق الأحكـام الإجرائية الواردة فى الاتفاقية ينطبق على الصلاحيات والإجـراءات لأغراض جمع الأدلة الإثباتية فى شكل إلكترونـى لفعل إجرامـي» انظر: دراسة مكتب الأمم المتحـدة المعنى بالمخدرات والجريمة بشأن الجريمـة السيبرانية، مرجع سابق، ص١٨٦.

ومـن التشريعـات المقارنة التـى سمحت بضبط الأدلة الرقميـة التشريعين الفرنسى والبلجيكي، حيث نظـم قانون الإجراءات الجنائيـة الفرنسـى ضبط كافة المعلومات المدونة على الحاسب الآلى أو الإنترنت، وذلك بوضع جهاز دون علم المتهم فى جميع الأماكـن الخاصة للاطلاع على المعلومات الإلكترونية وتسجيلها والاحتفـاظ بها ونقلها، حيث يتم ذلك بمعرفة مأمور الضبط القضائـى المختص بعـد ندبه من قاضى التحقيق (المـواد ٧٠٦-١٠٢-١ إلى ٧٠٦-١٠٢-٩ من القانـون رقم ٢٦٧ الصادر فى ٢٠١١/٣/١٤)، كمـا أجـازت المـادة (٣٩مكرراً) من قانون تحقيـق الجنايات البلجيكى نسخ المـواد المخزنة فى نظم المعالجة الآليـة للبيانات بقصد عرضها على الجهات القضائية. ومـن التشريعات العربية التى أجازت لمأمورى الضبط ضبط الأجهزة والأدوات المستخدمـة فى ارتكـاب الجرائم المعلوماتية التشريع الأردنى (م١٣). المستشـار/ د. محمد سمير، قانون العقوبات الاقتصـادي، مرجـع سابق، ص ص٢٢٨، ٢٢٩؛ د. عمر محمد بن يونس، مذكرات فى الإثبـات الجنائى عبر الإنترنت، مرجع سابق، ص١٢.

الجهـات القضائيـة المختصة أو من الجهـات المعنية بمكافحة جرائـم تقنية المعلومات بشأن الجرائم موضوع هذا القانون».

فقد أعطت اللائحة للخبراء المتخصصين الحق فى جمع الدليل الرقمى واستخراجه وحفظه وتحريزه، وتحرير التقارير الفنيـة المُرتبطة بهذه الإجراءات، وتجدر المُلاحظة أن الأصـل فى عمل الخـبراء المُتخصصين فى عملية جمع الدليـل الرقمى واستخراجه وحفظـه وتحريـزه، يتم بُناء على انتـداب هؤلاء الخبراء للقيام بهـذه المهام من جهات التحقيـق أو المحاكمة فقط، بينما تعطى اللائحة التنفيذية للخبراء المُتخصصين بعض المهـام الفنيـة والتقنية الأخرى، مثل: أعمـال التوصيف والتوثيق للأدلـة الرقمية، وفى هذه الحالة يقوم الخبراء بأداء مهام التوثيق والتوصيف وفقًا للتكليفات التى قد تصدر مـن جهات التحقيق أو الجهات القضائية المُختصـة أو الجهات المعنية بمكافحة جرائم تقنية المعلومات، وفى هذه الحالة قد يقوم أحد مأمورى الضبط القضائى بعملية جمع أو استخراج الدليل أو تحريزها، بينما يترك للخبراء مهام توثيق وتوصيف الدليل الرقمي، إذا رأت الجهات المعنية بمكافحة جرائم تقنية المعلومات أن هناك حاجة لذلك.

أ- قواعد قيد الخبراء فى السجل الأول: حددت المـادة الرابعة من اللائحة التنفيذية قواعد قيد الخبراء بالسجل الأول للخبراء، حيث تنص المادة المشار إليها على أنه: «يُنشأ بالجهـاز سجلان لقيد الخـبراء، يقيد بأولهمـا الفنيون والتقنيـون العاملون بالجهاز، ويقيد بالآخر الخبراء من الفنيين والتقنيين من غير العاملين به. ويتم القيد فى السجل الأول الخاص بالعاملين بالجهاز بناءً على القواعد والشروط والإجراءات الآتية:

١- أن يكون حاصلاً على مؤهل علمى أو فنى أو تقنى يتناسب ومجال الخبرة.

٢- أن يكون قد أمضى عام على الأقل فى عمله بالجهاز.

٣- أن يجتاز الاختبارات الفنية التى يجريها الجهاز للمتقدم».

ب- قواعـد قيد الخبراء فـى السجل الثاني: حـددت المـادة الخامسـة من اللائحة التنفيذيـة قواعد قيد الخبراء بالسجـل الأول للخبراء، حيث تنص المـادة المشار إليها علـى أنه:«يُقيد الخبراء من الفنيين والتقنيين من غير العاملين بالجهاز بالسجل الثانى للخبراء طبقًا للقواعد والشروط الآتية:

١- أن يكـون مصريًـا متمتعًا بالأهليـة المدنية الكاملة. ويجوز قيـد الأجنبى على أن يتعهد كتابة بخضوعه للقوانين المصرية.

٢- أن يكون محمود السيرة حسن السمعة.

٣- ألا يكون قد سبق الحكم عليه بحكم نهائى بالإدانة فى جريمة مخلة بالشرف.

٤- أن يكون لديه سيرة ذاتية تتضمن خبرة عملية مناسبة.

٥- موافقة الجهات المعنية من جهات الأمن القومى على القيد بالسجل. ويترتب على تخلف أى شرط من الشروط السابقة الشطب من السجل بقرار من الجهاز».

وقـد أشـارت المـادة السابعـة من اللائحـة التنفيذيـة إلى التزام الجهـاز القومى لتنظيـم الاتصالات بالحفاظ على سرية بيانات الخبراء، وعـدم الإفصاح عنها، حيث نصت المـادة المشار إليها على أنه: «يُراعى الجهاز الحفاظ على سرية البيانات الواردة بسجلات قيد الخبراء وعدم الإفصاح عنها إلا بموجب أمر قضائي».

ج- التمييز بين خبراء الجهاز القومى لتنظيم الاتصالات وغيرهم من الخبراء: ميز المشـرع المصرى بين خـبراء الجهاز القومى لتنظيم الاتصـالات وغيرهم من الخبراء، حيث أشـار إلى سريان القواعد والأحكام الخاصة بالمساءلة الإدارية والتأديبية الواردة بالقانـون المنظـم لعملهم إن وجـد، وذلك اتساقاً مـع القواعد العامة فى هـذا الشأن، وبالنظـر إلى أن هـؤلاء الخبراء قد ينظم عملهـم ومساءلتهم إداريـاً أو تأديبياً قوانين خاصة تنظم عملهم.

د- تقديـر موقـف المشـرع المصـرى بشـأن الخـبراء: حسناً فعـل المشـرع المصرى باستحداث سجلين للخبراء الذيـن يمكن لجهات التحقيق والمحاكمة الاستعانة بهم فى الجرائم المعلوماتية، حيث يجوز للمحكمة أو جهات التحقيق أن تندب أحد خبراء الجهاز القومى لتنظيم الاتصالات أو أحد خبراء المعلوماتية من المشهود لهم بالكفاءة والخبرة فـى هذا المجـال المستحدث، وبما يواجه مشكلة عدم توافـر العدد المناسب من الخبراء لـدى الجهاز القومى لتنظيـم الاتصالات فى ضوء ضخامة الأعـداد المتوقع نظرها من هذه القضايا أمام القضاء الجنائي.

هـ- إجراءات قيد الخبراء فى السجلات: أشارت المـادة (٨) من اللائحة التنفيذية

إلى إجـراءات قيد الخـبراء، حيث نصت المـادة المشار إليها على أنـه: «يتعين على من يرغـب فى قيد اسمه فـى السجل الثانى للخـبراء أن يتقدم للرئيـس التنفيذى للجهاز بطلـب كتابـى بذلك موضحًا فيه التخصص الذى يرغب العمـل فيه كخبير، وأن يرفق بالطلـب صور الشهادات والمستندات المؤيـدة لطلبه. ويمكن للجهاز أن يطلب منه خلال ثلاثـين يومًا من تاريخ تقديم الطلب معلومات إضافية قبـل الفصل فى الطلب، ويعتبر عدم الرد على الطلب لمدة ستين يومًا من تاريخ تقديمه رفضًا له. وفى حال رفض الجهاز الطلب، يحق للمتقدم التظلم بالإجراءات المقررة قانونًا».

و- قواعـد تنظيم الخبرة أمام القضاء: تـبرز الإشارة إلى أن قانون مكافحة جرائم تقنيـة المعلومـات قد أشـار إلى أنه تطبـق على الخبراء فـى ممارسـة عملهم وتحديد التزاماتهـم وحقوقهم القواعـد والأحكام الخاصة بقواعد تنظيـم الخبرة أمام جهات القضـاء، وهـذه القواعد أوردها المرسـوم بقانون رقم (٩٦) لسنـة ١٩٥٢ بشأن تنظيم الخبرة أمام جهات القضاء، والذى تضمن قواعد اختيار وعمل وتأديب الخبراء المقيدين فى جـداول المحاكم وخبراء وزارة العـدل ومصلحة الطب الشرعـى والمصالح الأخرى التـى يعهد إليها بأعمال الخبرة، وكل من ترى جهـات القضاء عند الضرورة الاستعانة برأيهـم الفنـى من غير من ذكروا، ومن ثم ينطبق هذا القانـون على خبراء المعلوماتية الذين تنتدبهم المحكمة أو سلطات التحقيق لإبداء الرأى الفنى فى مثل هذه الجرائم.

ثالثـاً- التحديات التى تواجه جهـات إنفاذ القانون فى التعامل مـع الدليل الرقمي: تتبلـور أبرز التحديـات التى تواجه جهات إنفاذ القانون فـى التعامل مع الدليل الرقمى فيما يلي:

١- ضخامـة كم البيانـات والمعلومات: يعتـبر التوسع فى استخـدام شبكة الإنترنت والتدفقـات الواسعة من البيانـات والمعلومات عبر الشبكة الدوليـة، واستخدام الجناة للحوسبة السحابية، ونشر المعلومات على خوادم خارجية، وقواعد البيانات الضخمة من التحديات التى تواجه جهات إنفاذ القانون، بالشكل الذى دفعها إلى تطوير أدوات تقنية تعتمد على خوارزميات الذكاء الاصطناعى لتحليل الكم الهائل من البيانات والمعلومات، توصـلاً إلى البيانـات والمعلومات المطلوبـة لإثبات الصلة بين الجانـى والجريمة، والتى تشكل بلا أدنى شك دليلاً جنائياً رقمياً.

٢- استخدام التشفير [١] وغيره من أساليب التشويش على البيانات: يعمد الجناة المعلوماتيون إلى إخفاء أية صلة بينهم وبين الجريمة، منعاً لتعقبهم من جانب جهات إنفاذ القانون، وهو ما يدفعهم إلى استخدام تقنيات التشفير لتجهيل الهوية والتشويش على البيانات، وهو ما أظهر انتشار استخدام شبكات الإنترنت المظلم التى ينتشر عليها الأنشطة الإجرامية المختلفة، ولا شك فى أن استخدام تقنيات التشفير يشكل عقبة حقيقية فى تعقب الأنشطة الإجرامية من جانب سلطات إنفاذ القانون[٢]، وقد يستخدم الجناة تقنيات لإخفاء المعلومات داخل الملفات والصور والتطبيقات، وتمثل ملفات الوسائط مضيفات مثلى لإخفاء المعلومات، وقد يجرى التعرف على البيانات المخفية بمقارنة تدفقات ملفات وبيانات المشتبه به مع الأصول المعروفة[٣].

٣- تخزين البيانات على خوادم خارجية أو على السحابة الإلكترونية: كما يعمد الجناة المعلوماتيون إلى تخزين ونشر البيانات والمعلومات على خوادم خارج دولهم وخوادم الحوسبة السحابية، بهدف تسهيل ارتكابهم لجرائهم، وفى الوقت ذاته تأمين أنفسهم من ملاحقة جهات إنفاذ القانون التى تواجه الصعوبات القانونية فى تتبع الأدلة الرقمية المخزنة على هذه الخوادم خارج ولايتها القضائية، حيث يعقد تخزين البيانات السحابية عملية التعرف على المعلومات المخزنة إلكترونياً وتجميعها وتحليلها[٤].

---

(١) عرفت المادة الأولى من اللائحة التنفيذية للقانون رقم (١٧٥) لسنة ٢٠١٨ كلاً من التشفير ومفتاح التشفير، بأن التشفير Encryption: منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيًا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة، بينما مفتاح التشفير Encryption Key: أرقام أو رموز أو حروف ذات طول محدد تستخدم فى عمليات التشفير وفك التشفير. ويستخدم نفس المفتاح فى التشفير وفك التشفير ويسمى التشفير المتماثل، ويجب الحفاظ على سرية المفتاح. ويستخدم زوج من المفاتيح مترابطين بعلاقة رياضية بحيث يستخدم أحدهما فى التشفير والآخر فى فك التشفير ويسمى التشفير غير المتماثل، ويجب الحفاظ على سرية أحد المفاتيح بينما يعلن عن الآخر بشروط ومعايير محددة.

(٢) أشارت دراسة مكتب الأمم المتحدة حول الجريمة السيبرانية إلى أن الأدلة الرقمية كثيراً ما تشفر بمعرفة المشتبه بهم فى غالبية البلدان (٦٠-٨٠٪)، وأن التشفير قد يتطلب مساعدة وقدرة فنية متخصصة، وأن بعض البلدان لا يكون لها سبيل للتعامل مع مشكلة التشفير دون الحصول على المفاتيح من المشتبه به، أو الاستحواذ عليها، وأن المشتبه به إذا لم يفصح عن مفاتيح فك الشفرة، فللمحققين الاستعانة بالخبرة الفنية وبرامج فك التشفير. انظر: دراسة مكتب الأمم المتحدة حول الجريمة السيبرانية، مرجع سابق، ص ص٢٣٦، ٢٣٧.

(٣) المرجع السابق، ص٢٣٧.

(4) Reilly, D., Wren, C., and Berry, T., 2011. Cloud computing: Pros and Cons for Computer Forensic Investigators. International Journal Multimedia and Image Processing, 1(1):26-34, 33.

المطلب الثالث

التعاون الدولى فى جمع الأدلة الرقمية

تبرز أهمية التعاون الدولى فى المسائل الجنائية ذات الصلة بالأدلة الرقمية وجرائم تقنيــة المعلومات، بالنظــر إلى الطابع عبر الوطنى الذى تتسم بــه هذه الجرائم، والتى تستخــدم فى ارتكابها فى أغلب الأحوال شبكة الإنترنــت، ومن ثَمَّ توجد الأدلة الرقمية الناجمــة عن هذه الجرائم خارج حــدود الولاية القانونية لجهات إنفاذ القانون، وهو ما يتطلــب ضرورة وجود قواعد قانونية تنظم مسائــل التعاون بين الدول، مع وجوب الأخذ بعين الاعتبار الطبيعة غير المستقرة للدليل الرقمي، والتى تستوجب استجابة سريعة من جانــب جهات التحقيــق، وقدرة على طلب إجراءات تحقيقيــة متخصصة تتطلب تعزيز آليات التعاون الدولى على نطاق واسع بين مختلف الدول.

وقد بينت المادة الرابعة من القانون رقم (١٧٥) لسنة ٢٠١٨ أحوال وشروط التعاون الدولى فى مجال مكافحــة الجرائم المعلوماتية، وقد جاءت هذه الأحكام فى نص عام، تضمن آليات تبادل المعلومات والمساعدة القضائية، حيث أشارت المادة المذكورة إلى أنه: **«تعمــل السلطــات المصرية المختصة على تيسير التعاون مــع نظيراتها بالبلاد الأجنبية فى إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقاً لمبدأ المعاملة بالمثــل، بتبادل المعلومات بما من شأنه أن يكفل تفــادى ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها. على أن يكون المركز الوطنى للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة فى هذا الشأن»**[(١)].

(١) وكانــت المــادة الثالثة من القانون رقــم (١٧٥) لسنة ٢٠١٨ المعنونة:«نطــاق تطبيق القانون من حيث المكــان» تقضى بأنه:«مع عــدم الإخــلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبــات، تسرى أحكام هذا القانون على كل من ارتكب خارج جمهوريــة مصــر العربية من غير المصريين جريمــة من الجرائم المنصوص عليهــا من هذا القانون، متى كــان الفعل معاقبًا عليــه فــى الدولــة التى وقع فيها تحت أى وصف قانوني، وذلك فى أى من الأحوال الآتية: ١ - إذا ارتكبت الجريمة على متن أى وسيلــة مــن وسائل النقل الجوى أو البرى أو المائي، وكانت مسجلــة لدى جمهوريــة مصــر العربية أو تحمــل علمها.٢ - إذا كــان المجنــى عليهم أو أحدهم مصــريًا.٣ - إذا تم الإعداد للجريمة أو التخطيط أو التوجيــه أو الإشراف عليها أو تمويلها فــى جمهورية مصر العربية.٤ - إذا ارتكبــت الجريمة بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية فى أكثر من دولة من بينها جمهورية مصر العربية.٥ - إذا كان من شأن الجريمة إلحاق ضرر بأى من مواطنى جمهورية مصر العربية أو المقيمين فيها، أو بأمنها أو بأى من مصالحها، فى الداخل أو الخارج.٦ - إذا وُجد مرتكب جريمة فى جمهورية مصر العربية، بعد ارتكابها ولم يتم تسليمه».

وقد أشار القانون إلى اعتبار المركز الوطنى للاستعداد لطوارئ الحاسب والشبكات بالجهاز القومى لتنظيم الاتصالات هو النقطة الفنية المعتمدة فى هذا الشأن، ويكون ذلك فى إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو تطبيق مبدأ المعاملة بالمثل.

ويرى الباحث أنه كان من الأولى بالمشرع أن يتضمن تفصيلاً أكثر فيما يتصل بمسائل التعاون الدولى فى مكافحة جرائم تقنية المعلومات، من خلال تقرير نصوص بشأن تسليم المجرمين والمساعدة القضائية، وبالشكل الذى يحدد شروط وإجراءات التسليم وشروط وإجراءات المساعدة القضائية المتبادلة..، إلى غير ذلك من آليات التعاون القضائى الدولي.

وفى هذا الإطار، تبرز الإشارة إلى أن مكتب الأمم المتحدة المعنى بالمخدرات والجريمة – فى إحدى دراساته حول الجريمة السيبرانية- يرى -بحق- أن الاعتماد على الوسائل التقليدية للتعاون الدولى الرسمى فى مسائل جرائم تقنية المعلومات، لا يكفى حالياً للاستجابة فى الوقت المناسب لمقتضيات الحصول على أدلة رقمية سريعة الزوال والتغير، توجد فى أماكن جغرافية متعددة، وهو ما سيشكل مشكلة إجرائية بشأن كافة الجرائم، وليس جرائم تقنية المعلومات فحسب[١]، وقد أشارت الدراسة – آنفة الذكر- إلى أن غالبية البلدان (ما يزيد على ٧٠٪) تستخدم آلية طلبات المساعدة القانونية المتبادلة الرسمية، والتى عادةً ما تستغرق نحو ١٥٠ يومًا، للاستجابة لهذه الطلبات، وأنه فى كثير من الأحيان قد تتجاوز هذه المدد الزمنية مدة احتفاظ مقدم الخدمات بالبيانات، أو قد يتمكن مرتكبو الجريمة خلالها من إتلاف الأدلة الرقمية.

وترجع أهمية التعاون الدولى فى مكافحة جرائم تقنية المعلومات إلى الطبيعة الخاصة لجريمة تقنية المعلومات كجريمة عبر وطنية، والتى تتطلب تحقيقات سريعة تتسم بالخبرة والتعاون غير المسبوق، وهو ما يتطلب ضرورة تعاون أجهزة إنفاذ القانون بصورة سريعة وفعالة عبر الحدود الوطنية[٢]، فضلاً عما تطرحه الحوسبة السحابية

(١) انظر: دراسة مكتب الأمم المتحدة المعنى بالمخدرات والجريمة بعنوان: «دراسة شاملة عن الجريمة السيبرانية»، نيويورك، ٢٠١٣، صXV.

(٢) كريستوفر بينتر، التهديد الذى تفرضه الجريمة المعلوماتية والحاجة إلى التعاون الدولي، ورقة عمل مقدمة للمؤتمر الدولى السادس للجرائم المعلوماتية الذى نظمته المنظمة الدولية للشرطة الجنائية «الإنتربول»، القاهرة، ١٣-٢٠٠٥/٤/١٥، ترجمة مركز بحوث الشرطة بأكاديمية الشرطة، القاهرة، ص٦٦.

مـن تحد متزايـد أمام التعاون الـدولى بسبب نقل الخدمات الحاسوبيـة بشكل متزايد إلى خـوادم ومراكز بيانات موزعة جغرافياً، مما يجعل من الصعب تحديد موقع الأدلة الرقمية[١].

علاوة على اقتصار نطاق انطباق القواعد الجنائية على إقليم الدولة (مبدأ إقليمية القاعـدة الجنائيـة)، وهو ما يترتب عليه صعوبات إجرائيـة فى مواجهة هذه الجرائم، تتمثـل فى عدم إمكانية السلطـات القضائية بالدولة مباشرة بعض الأعمال القضائية الإجرائية داخل أقاليـم الدول الأخرى، كإجراءات التفتيش والضبط إلى غير ذلك من الإجراءات الجنائية [٢]، فغالباً ما تتضمن معظم الاتفاقيات الثنائية والإقليمية والدولية نصوصاً تقتضى ضرورة اللجوء إلى المُساعدة القضائية المُتبادلة، بهدف تحقيق السرعة والفعالية فى إجراءات الملاحقة للجناة، وجمع الأدلة الرقمية[٣].

ويعد تبادل المعلومات فى مجال جرائم تقنية المعلومات من أبرز صور التعاون الدولى فـى مواجهتها، وهو قد يتم بشكل ثنائـى أو متعدد الأطراف، من خلال المنظمة الدولية للشرطـة الجنائية أو غيرهـا من الأجهزة النظيرة على الصعيـد الإقليمى كاليوروبول، والأفريبول، والمكتب العربى لمكافحة الجريمة، ويقصد بتبادل المعلومات التعاون الدولى الأمنـي، والـذى يتم من خلال تبـادل المعلومـات بين الأجهـزة الأمنية حـول الأنشطة الإجراميـة التـى يباشرها مجرمـو المعلوماتيـة، بهدف تحقيـق تعاون أمنـى فعال فى مواجهتها.

وبالنظر إلى الطبيعة الخاصة للجرائم المعلوماتية، فإن التعاون الدولى فى مكافحتها لا ينبغى أن يقتصر على التعاون الدولى الأمنى فى مجال تبادل المعلومات، والتعاون الدولى القضائى فى مجال الإنابة القضائية وتسليم المجرمين، وإنما يتطلب الأمر التعاون الدولى فى مجال تدريب الكوادر الأمنية والقضائية على كشف وتحقيق جرائم تقنية المعلومات، وقـد اهتـم المجتمع الدولى بتفعيل التعـاون الدولى فى مجال مكافحة هـذه الطائفة من الجرائـم من خلال عدة حلـول، أبرزها: اتفاقيـة بودابست، والقـرار الإطارى الخاص

(١) انظر: دراسة مكتب الأمم المتحدة حول الجريمة السيبرانية، مرجع سابق، ص٢١٦.

(٢) المستشـار/ البشـرى الشوربجي، آفاق وآليات التعاون الدولى ضد الجريمة، مجلـة القضاة الفصلية، نادى القضاة المصري، السنة ٥٣، ٢٠٠٣، القاهرة، ص١٠.

(٣) د. جميل عبد الباقى الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، القاهرة، دار النهضة العربية، ١٩٩٩، ص٧٩.

بالاتحاد الأوروبي، والأنشطة التشريعية وأنشطة بناء القدرات فى مجال المكافحة، والتى تدعمها بعض المنظمات الدولية الإقليمية كمنظمة الدول الأمريكية، ومجموعة دول آسيا والباسيفيك، فضلاً عن جهود مجموعة العمل الدولية المعنية بالتدريب على الجريمة المعلوماتية، وجهود المنظمة الدولية للشرطة الجنائية «الإنتربول»[١].

دور الإنتربول فى التعامل مع الأدلة الرقمية: تعمل منظمة الإنتربول على تعزيز التعاون الدولى الشرطى بين أعضائها -والذين يبلغ عددهم ١٩٤ دولة-، وذلك من خلال تقديم الخدمات التالية:

- **الدعم الميداني:** يمكن تقديم مساعدة متخصصة فى مجال الأدلة الجنائية فى مختبر الإنتربول للأدلة الجنائية الرقمية، وفى الميدان خلال إيفاد أفرقة التحرك إزاء الأحداث.
- **الإرشاد:** تساعد منظمة الإنتربول البلدان الأعضاء فى إقامة أحدث المختبرات وصيانتها، بما ينسجم مع الإجراءات المعتمدة على الصعيد الدولى لدعم التحقيقات والملاحقات القضائية على نحو أفضل.
- **بناء القدرات:** تضع منظمة الإنتربول برامج تدريب تركز على مناهج وحلول موحدة فى مجال الأدلة الجنائية الرقمية، بالتعاون الوثيق مع وحدة الإنتربول لبناء القدرات وشركائها من أجهزة إنفاذ القانون والقطاع الخاص والأوساط الجامعية.
- **تحقيق الاتصال بين الخبراء المختصين:** يؤمِّن مختبر الإنتربول للأدلة الجنائية الوصل بين الخبراء فى جميع أنحاء العالم من أجل تبادل ما يحوزونه من معارف ومناقشة سبل تحسين عملهم اليومي.

وتعمل منظمة الإنتربول فى سياق دورها فى مكافحة جرائم تقنية المعلومات بإعداد المنشورات والإصدارات ذات الصلة بالتعامل مع الأدلة الرقمية، ومن أبرزها:

- **المبادئ التوجيهية العالمية الخاصة بمختبرات الأدلة الجنائية الرقمية:** تعرض هذه الوثيقة الإجراءات المتبعة لإنشاء وإدارة مختبر للأدلة الجنائية الرقمية، وتوفر أساليب تقنية لتدبّر الأدلة الإلكترونية ومعاملتها.

(١) كريستوفر بينتر، مرجع سابق، ص٦٦.

- **إطـار مواجهـة حوادث الطائرات المسـيّرة:** يزود أوائلَ المتدخلـين وخبراءَ الأدلة الجنائيـة الرقميـة بالإرشـادات التقنية ذات الصلـة بإدارة حـوادث الطائرات المسيّرة والتعامل معها.
- **Digital 4N6 Pulse (إصدار فصلي):** هى رسالة إخبارية تتضمن مقالات وجيزة بقلـم إخصائيين فى مجال الأدلـة الجنائية الرقمية، ولا سيما خبراء من أجهزة إنفاذ القانون والقطاع الخاص والأوساط الجامعية.
- **المبـادئ التوجيهية الموجهة لأوائل المتدخلين فى مجـال الأدلة الجنائية الرقمية:** تتيح هذه الوثيقة إسداء المشورة فيما يتعلق بالبحث عن الأدلة الرقمية وضبطها وتحديدها ومعاملتها باستخـدام أساليب تكفل سلامتها لتكون مقبولة فى سياق الإجراءات القضائية.

كما تعنى منظمة الإنتربول فى السياق ذاته بتنظيم العديد من المنتديات ذات الصلة بالتعامل مع الأدلة الرقمية، ومن أبرزها:-

- **اجتماع فريق خـبراء الإنتربول للأدلة الجنائيـة الرقمية (اجتماع سنوي):** وهو مفتـوح للأخصائيـين والمديرين من أجهزة إنفاذ القانـون والوكالات الحكومية، وشركات الأدلة الجنائيـة الرقمية والمؤسسات الجامعية التى تُدعى إليه، ويشكل الاجتمـاع مكاناً مؤاتيـاً لإقامة العلاقات وتبادل الاطـلاع على الخبرات، وتقديم معلومـات محدثة عن التكنولوجيا والتقنيـات الجديدة فى مجال الأدلة الجنائية الرقمية.
- **منتـدى الإنتربول للخـبراء المعنيين بالطائـرات المسيّرة (منتـدى سنوي):** وهو إطـار للتحليـل المعمق لوضـع الطائرات المسـيّرة وما تطرحه مـن تحديات على أجهـزة إنفاذ القانون، وتتناول المناقشات فى إطـاره ثلاثة مجالات محددة هي: التهديدات، والأدوات، والأدلة.
- **اجتمـاع فريق خـبراء الإنتربول المعنى بالتهديدات السيبرانيـة لقطاع السيارات وبالأدلـة الجنائيـة المتصلـة بالمركبات (اجتماع سنـوي):** يوفر منـبراً لمناقشة الصعوبـات الراهنـة وأمثلـة على فائـدة البيانـات المتصلة بالمركبـات فى إطار

التحقيقات، ويتوجه هذا الاجتماع إلى المديرين والمتخصصين العاملين فى مجالى مكافحة التهديدات السيبرانية لقطاع السيارات والأدلة الجنائية الرقمية.

- **منتـدى الإنتربول للأدلة الجنائيـة الرقمية المتعلقة بالمعـدات المحمولة على متن السفن (منتدى سنوي):** هذا المنتدى الذى ينظَّم بمشاركة فريق الإنتربول العالمى المعنـى بإنفـاذ القوانين فـى قطاع صيد الأسمـاك، يجمع أجهزة إنفـاذ القانون والشركـاء من القطاع الخاص فى إطـار نهج عملى لتطبيق أفضل الممارسات فى مجال الأدلة الجنائية الرقمية المتعلقة بالمعدات المحمولة على متن السفن.

الخاتمة

استعرضنا خلال السطور السابقة موضوع الدليل الجنائى الرقمى فى ضوء أحكام القانون رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية، حيث تناول الباحث التعريف بالدليل الرقمى وخصائصه، وأوجه التمييز بينه وبين الدليل المادى التقليدي، وحجيته أمام القضاء الجنائي، وشروط صحته وإجراءات وأدوات توثيقه، والحماية الجنائية المقررة له، وقد تمخض البحث عن مجموعة من النتائج والتوصيات، وذلك على النحو التالي:

النتائج: من أبرزها:

١- تزايد أهمية الأدلة الرقمية فى الوقت الراهن بسبب ثورة الاتصالات والمعلومات وانتشار استخدام شبكة الإنترنت والحاسب الآلي، بشكل أصبحت فيه الأدلة الرقمية من المتصور وجودها فى كافة صور الجرائم التقليدية والمستحدثة.

٢- تأثير طبيعة الأدلة الجنائية المعنوية المتغيرة على موثوقيتها أمام القضاء الجنائي، بالشكل الذى تطلب تنظيماً قانونياً دقيقاً لهذه المسألة.

٣- اضطلاع المشرع بتحديد مجموعة من الشروط الخاصة بإجراءات جمع وتوثيق الأدلة الرقمية لتحقيق فكرة الموثوقية فيها، ومن ثم تنتج أثرها فى تكوين عقيدة القاضى الجنائي.

التوصيات: من أبرزها:

١- توجيه نظر المشرع المصرى إلى تعديل اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات الصادرة بقرار رئيس مجلس الوزراء رقم (١٦٩٩) لسنة ٢٠٢٠، وذلك بإضافة مادة باللائحة برقم (٦) التى كانت موجودة بمشروع اللائحة، والتى كانت تنظم إجراءات جمع الدليل الرقمى من جانب مأمورى الضبط القضائي، وكانت تنص المادة المشار إليها (وفق مسودة اللائحة) على أنه:«على مأمورى الضبط القضائى المختصين وفقاً للأمر المسبب من جهة التحقيق المختصة القيام بالإجراءات الواردة فى المادة رقم (٦) من القانون، وفق الضوابط التالية: أن تتم عملية ضبط أو جمع أو الحصول أو استخراج أو التحفظ على الأدلة الرقمية محل الواقعة، واستخراج النسخ الرقمية Digital Forensic Images من هذه

الأدلــة بأجهزة أو معدات أو برامج أو بأدوات البحــث الجنائى الرقمى وبأساليب تقنية مثـل Write Blocker أو مــا يماثلها بما يضمن عدم تغيــير أو تحديث أو محو أو تحريف للكتابــة أو البيانات والمعلومات، أو أى تغيــير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانــات والمعلومات، أو أنظمة المعلومــات أو البرامج أو الدعامات الإلكترونية وغيرها. ويجب أن تُثبت الإجراءات بمحضر الضبط وتقرير الفحص المبدئى وفقاً لما يلي: ١- أن تكــون عملية البحث والتفتيش والدخول والنفاذ إلى برامج الحاســب وقواعد البيانات والأجهــزة والنظم المعلوماتيــة، وفقاً للنطاق المحــدد بقرار جهة التحقيــق المختصة أو المحكمــة، أو بتصريــح مكتوب مــن صاحب الشــأن، وأن تكون مرتبطة فقــط بالواقعة. ٢- معاينــة وتوصيــف وتصوير عملية الضبط ومسرح الجريمــة أو الواقعة قبل عمليات الفحــص والتحليل، وتوثيق مكان الضبط. ٣-توثيق وتسجيل الأرقام المسلسلة للأجهزة والمعدات المضبوطة مع تحديد أنواعها ومواصفاتها وأى ملحقات أخرى. مع بيان النظم والبرامــج والتطبيقــات وبياناتهــا إن أمكــن. ٤- توصيف كيفية وأسلــوب التحفظ على الأدلة وتحريزها ومكان حفظها لحين تسليمها لجهات الفحص والتحليل، مع توثيق كود وخوارزم Hash النــاتج عن استخراج نسخ مماثلة ومطابقة للأصل من الأدلة الرقمية. ٥- فى حالات الضبط التى يتضح فيها وجود تشفير مستخدم على الأجهزة أو المعدات أو البيانــات أو المعلومــات أو النظم المعلوماتية، يتم الفحص أثناء عملية الضبط وتوثيق وإثبــات ذلك بمحضر الضبــط والفحص المبدئي. ويتم الاسترشــاد بمعيار الأيزو ISO ٢٧٠٣٧ كنموذج مرجعى للتعامل مع الأدلة الرقمية».

٢- وجــوب تعزيــز التعاون مع المنظمــات الدولية العاملة فى مجــال تبادل المعلومات ذات الصلــة بجرائــم تقنية المعلومــات والأدلة الرقمية كمنظمة الإنتربــول واليوروبول، والاستفادة من التسهيلات التى تقدمها للدول للتعامل مع هذه الطائفة من الجرائم.

٣- وجوب تعزيز التعاون الدولى القضائى عبر الاتفاقيات الثنائية ومتعددة الأطراف لتسهيل مهمة القائمين علــى إنفاذ القانون فى عمليات جمع واستخراج الأدلة الرقمية، وبصفة خاصة الدول التى توجد بها الخوادم الرئيسية Servers لشبكات المعلومات.

٤- المضــى قدماً فى صقــل قدرات العنصر البشرى المتعامل مــع الأدلة الرقمية من رجــال إنفاذ القانــون ومعاونيهم (شرطة- نيابة- قضاء- خــبراء) تمكيناً من التعامل الأمثل مع جرائم تقنية المعلومات والأدلة الرقمية الناجمة عنها.

المراجـع

المراجع العربية

المراجع العامة:

- **أحمد فتحى سرور:** الوسيط فى قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٩٦.

– الوسيـط فى قانون الإجـراءات الجنائية، ج١، طبعة مطبعـة جامعة القاهرة، ١٩٧٩.

- **عبـد الـرءوف مهدي،** شرح القواعـد العامة للإجراءات الجنائيـة، دار النهضة العربية، القاهرة، ٢٠٠٣.
- **مأمون سلامـة،** الإجراءات الجنائية فى التشريع المصري، دار النهضة العربية، القاهرة، ١٩٩٦، ج٢.
- **محمـود نجيب حسنى،** شـرح قانون الإجراءات الجنائيـة، دار النهضة العربية، القاهرة، الطبعة الثانية، ١٩٨٨.

المراجع المتخصصة:

- **تشايكين دي،** تحقيقات الشبكة حول الهجمات الإلكترونية– حدود الأدلة الرقمية، الجريمة والقانون والتغير الاجتماعي، ٢٠٠٦.
- **حسين إبراهيم،** الإثبات الجنائي، مطبعة كلية الشرطة، القاهرة، ٢٠٠٢.
- **جميل عبد الباقى الصغـير:** الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ١٩٩٩.

– أدلـة الإثبات الجنائـى والتكنولوجيا الحديثة، دار النهضـة العربية، القاهرة، ٢٠٠٢.

- **سـالم محمـد الأوجلـي،** مقبولية الدليـل الرقمى فـى المحاكـم الجنائية، مجلة دراسات قانونية، جامعة بنى غازي، ليبيا، العدد ١٩، يناير ٢٠١٦.

- **عمر محمد بن يونس**، الإجراءات الجنائية عبر الإنترنت فى القانون الأمريكي، بدون ناشر، ٢٠٠٦.
- **غوتمان بي**، الحذف الآمن للبيانات من الذاكرة المغناطيسية وذاكرة الحالة الصلبة، وقائع الندوة الأمنية السادسة لاتحاد الحوسبة التقنية المتقدمة، ١٩٩٦.
- **كينجى ميانيشي**، شبكة الربط بين النقاط المرجعية الوطنية، المؤتمر الدولى السادس للجرائم المعلوماتية،١٣-١٥/٤/٢٠٠٥، إصدار مركز بحوث الشرطة، القاهرة.
- **مارسيلا الإبن أيه جيه، غرينفيلد أر أس (محرران)**، الأدلة الجنائية الإلكترونية، الدليل الميدانى لجمع ودراسة وحفظ أدلة جرائم الحاسب، بوكا راتون، مطبعة سى أر سي، ط٢، ٢٠٠٢.
- **محمد الأمين البشري**، التحقيق فى الجرائم المستحدثة، مطبوعات جامعة نايف العربية للعلوم الأمنية، الرياض، ط١، ٢٠٠٤.
- **محمد سمير**، قانون العقوبات الاقتصادي، طبعة نادى القضاة،٢٠١٩.
- **ممدوح عبد الحميد عبد المطلب**، البحث والتحقيق الجنائى الرقمى فى جرائم الحاسب الآلى والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٦.
- **هشام محمد فريد رستم**، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ١٩٩٤.
- **هلالى عبد اللاه أحمد**، حجية المخرجات الكمبيوترية فى الإثبات الجنائي، القاهرة، دار النهضة العربية، ١٩٩٧، ط١.

رسائل الدكتوراه:

- **أحمد سعد الحسيني**، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، رسالة دكتوراه، جامعة عين شمس، ٢٠١٣.
- **سامح أحمد بلتاجى موسى**، الجوانب الإجرائية للحماية الجنائية لشبكة الإنترنت، رسالة دكتوراه، جامعة الإسكندرية، ٢٠١٠.

- **عمـر محمد بن يونس،** الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة عين شمس، ٢٠٠٤.
- **وليـد المعـداوي،** دور الشرطة فى حماية الحياة الخاصة مـن أخطار المعلوماتية، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، ٢٠١١.

المقالات وأوراق العمل:

- **البشـرى الشوربجي،** آفـاق وآليات التعاون الدولى ضـد الجريمة، مجلة القضاة الفصلية، نادى القضاة المصري، السنة ٥٣، ٢٠٠٣، القاهرة.
- **عبـد الناصر محمد محمود فرغلى وآخر،** الإثبـات الجنائى بالأدلة الرقمية من الناحيتـين القانونية والفنية- دراسة تطبيقية مقارنة، المؤتمر العربى الأول لعلوم الأدلـة الجنائية والطب الشرعى الذى نظمته جامعة نايف العربية للعلوم الأمنية خلال الفترة (١٢-١٤/١١/٢٠٠٧)، الرياض.
- **عمر محمد بن يونس،** مذكـرات فى الإثبات الجنائى عبر الإنترنت، ندوة الدليل الرقمـى التـى نظمتهـا جامعـة الـدول العربية، القاهـرة، خلال الفـترة (٥-٨ مارس٢٠٠٦).
- **كريستوفـر بينـتر،** التهديد الـذى تفرضـه الجريمـة المعلوماتيـة والحاجة إلى التعاون الدولي، ورقة عمل مقدمـة للمؤتمر الدولى السادس للجرائم المعلوماتية الـذى نظمته المنظمـة الدولية للشرطة الجنائيـة "الإنتربـول"، القاهرة، ١٣-١٥/٤/٢٠٠٥، ترجمة مركز بحوث الشرطة بأكاديمية الشرطة، القاهرة.
- **محمد أحمـد منشاوي،** سلطة القاضـى الجنائى فى تقديـر الدليل الإلكتروني، مجلة الحقوق، جامعة الكويت، المجلد ٣٦، العدد٢، يونيو ٢٠١٢.
- **محمد زكى أبو عامر،** القيود القضائية على حرية القاضى الجنائى فى الاقتناع، مجلة القانون والاقتصاد، جامعة القاهرة، السنة٥١، ١٩٧١.
- **ممدوح عبد الحميد عبد المطلب،** استخدام بروتوكول TCP IP فى بحث وتحقيق الجرائم علـى الكمبيوتر، المؤتمر العلمى الأول حـول الجوانب القانونية والأمنية للعمليـات الإلكترونية، الذى نظمه، مركـز البحوث والدراسات بأكاديمية شرطة

دبـي، خـلال الفـترة (٢٦-٢٨/٤/٢٠٠٣)، إمارة دبـي، دولة الإمـارات العربية المتحدة.

- **هنـد نجيب،** حجيـة الدليل الإلكترونـى فى الإثبـات الجنائي، المجلـة الجنائية القوميـة، المركـز القومى للبحـوث الاجتماعية والجنائية، القاهـرة، المجلد ٥٧، العدد الأول، مارس ٢٠١٤.
- **وليـد نبيل طه،** الجرائم الإلكترونية طبقاً لاتفاقيـة بودابست، ورقة عمل مقدمة لندوة (الواقع الأمنى «مسئوليات- إنجازات») والتى انعقدت بتاريخ ٢٠١١/١/٩، مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة.
- **وهيبة لعوارم،** الدليل الرقمى فى مجال الإثبات الجنائى وفقاً للتشريع الجزائري، المجلة الجنائية القومية، المركز القومى للبحوث الاجتماعية والجنائية، القاهرة، المجلد ٥٧، العدد٢، يوليو ٢٠١٤.

الوثائق والدراسات:

- دراسـة مكتـب الأمم المتحدة حول الجريمـة السيبرانية، وثائـق الأمم المتحدة، نيويورك، ٢٠١٣.
- دليـل «الأدلة الرقمية الموجودة فى حجرة المحكمة»، دليل لإنفاذ القانون والمدعين العامين، وزارة العدل الأمريكية، معهد العدالة الوطني، ٢٠٠٧.
- المعهـد الأمريكـى الوطنـى للمعايـير والتكنولوجيـا، ٢٠٠٤، جهاز مانـع الكتابة (HWB) مواصفات، الإصدار ٢,٠.
- مضبطـة مجلس النواب المصري، الفصل التشريعـى الأول، دور الانعقاد العادى الثالث، الجلسة السادسة والخمسون، المنعقدة فى ٢٠١٨/٥/١٤.

المراجع الأجنبية:

- Chappell, L., 2012. Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network AnalystStudy Guide. Laura Chappell University.

أحكام القضاء الأمريكي:

- United States v. Meregildo, No. 11 Cr. 576(WHP), 2012 WL 3264501, at *2 (S.D.N.Y. Aug. 10, 2012).

أحكام القضاء الفرنسي:

- Cass. Com. 3 Juin 2008, No. 0717196-1714707-, bull. 4, 2008, no.112.
- Cass. Crim. 31 Jan 2007, No. 38306-82-, bull. Crim., 2007, no.27.

أحكام القضاء المصري:

المستحدث من المبادئ الصادرة عن الدوائر الجنائية من أول أكتوبر ٢٠١٢ لغاية آخر سبتمبر ٢٠١٣، الصادرة عن المكتب الفنى لمحكمة النقض، المجموعة الجنائية.

مواقع إلكترونية:

موقع جريدة عكاظ السعودية على الرابط: https://www.okaz.com.sa/articles/na/١٦٩٧١٨٣.