

الضمانات الإجرائية للدليل الرقمي - دراسة مقارنة

Procedural Safeguards for Digital Evidence in Criminal Proceedings: A Comparative Study

الدكتور: إبراهيم عبد الصمد صالح البلوشي

عضو هيئة التدريس بكلية الشرطة - دولة الإمارات العربية المتحدة

ملخص:

تجدُر الإشارةُ إلى توسُّع الدليل الرقمي والعمل به في الواقع العمليّ، وهذا التوسُّع استوجب أن تكون هناك ضرورةً لحماية هذا النوع من الأدلة، وهذه الحماية تتجلى في الحماية الجزائية الإجرائية، وقد اقتصرنا على هذه الحماية دون غيرها من صور الحماية الأخرى، لذلك تجلّت الإشكالية الحقيقية في مدى فاعلية هذا النوع من الحماية في تفعيل حماية متكاملة للدليل الرقمي، وهذا ما دعانا إلى بيان الأحكام الإجرائية التي عليّ ضوئها يتعيّن استخلاص الدليل الرقمي، كذلك بيان وجوه التّحقيق في الجرائم المتّصلة من المساس بهذا النوع من الأدلة، وعملاً بأصول المنهج التحليلي المُقارن، توصّلنا إلى عددٍ من النتائج والتوصيات، أهمّها: خلُو التنظيم الاتحاديّ الإماراتيّ من نصّ يُنظّم إجراءات الضبط، وتنظيم أعمال الخبرة في البيئة التقنية، وهذا ما دعانا إلى الاقتراح بشأن معالجة هذه النتائج وإيضاء المُشرّع بإعمال التدخّل التشريعيّ الملائم. الكلمات المفتاحية: الدليل الرقمي - الحماية الإجرائية - المعاينة التقنية - التفتيش التقني.

Abstract

It is worth noting the expansion of digital evidence and its implementation in practice, and this expansion has become necessary to protect this type of evidence, and this protection is manifested in procedural criminal protection, and we have limited ourselves to this protection without other forms of protection, so the real problem was It is evident in the effectiveness of this type of protection in activating integrated protection for digital evidence, and this is what prompted us to clarify the procedural provisions according to which the digital evidence must be extracted, as well as explaining the aspects of investigating crimes related to harming this type of evidence, and in accordance with the principles of the comparative analytical approach, We reached a number of results and recommendations, the most important of which is that the UAE federal regulation lacks a text regulating control procedures and regulating the work of expertise in the technical environment. This is what prompted us to propose addressing these results and recommending that the legislator implement appropriate legislative intervention.

Keywords: Digital evidence - procedural protection - technical inspection - technical inspection.

أولاً: المقدّمة:

لا شكّ أنّ الدليل الرقمي هو إحدى صور الأدلة المستحدثة والتي نشأت في نطاق النظم القانونية المختلفة، ممّا كان ذلك وكان الدليل الرقمي محلّ اهتمامٍ وحمايةٍ من جانب المُشرّع، فإنّ هذا الأخير نظّم صورتين من الحماية: الصورة الأولى تتجلى في الحماية الموضوعية، أمّا الصورة الثانية فهي الحماية الإجرائية، لذلك فإننا في هذا النطاق نتناول الحماية الجزائية الإجرائية، ونظراً لأهمية هذه الأخيرة واعتبارها جانباً مكماً للحماية الموضوعية، فسوف نُقسم حديثنا بصدها إلى جانبين، بحيث نستعرض في الجانب الأول الأحكام الإجرائية لاستخلاص الدليل الرقمي، وفي إطارها سوف نتناول الوسائل المادية التي من شأنها الحصول على الدليل الرقمي، وكذلك خصوصية التعامل مع هذا النوع من الأدلة، أمّا الجانب الثاني فسوف نعرض فيه التّحقيق في جرائم التّعدي

والمساس بهذا النوع من الأدلة، وبصدده نفس هذا الجانب، بحيث نعرض أولاً التَّحَقُّق والتَّحْقِيق من سلامة الدليل الرقمي، ثم في الأخير نعرض لإجراءات التَّحْقِيق في هذه الجرائم، وذلك على النحو الذي سنعرض له في متن الدِّراسة.

ثانياً: نطاق الدِّراسة:

يعدُّ نطاق الدِّراسة ضابطاً جوهرياً ومنشوداً، وفي هذا المقام يتحدّد هذا النطاق في ثلاثة جوانب جوهريّة:

➤ **الجانب الأول:** يتمثّل في النّظر إلى فكرة الحماية ذاتها، ونقتصر في هذا الصدد على بيان إحدى صور الحماية، وهي الحماية الجزائيّة، دون غيرها من صور الحماية الأخرى، لذلك يخرج عن نطاق الدِّراسة كافّة صور الحماية الأخرى كالحماية الدستوريّة والإداريّة والمدنيّة وغيرها.

➤ **الجانب الثاني:** يتمثّل في النّظر إلى طبيعة الحماية الجزائيّة ذاتها، بحيث نعرض في هذا النطاق الحماية الإجرائيّة على وجه الحصر، دون النّظر إلى الحماية الموضوعيّة، وإلا بات إعمال غير ذلك خروجاً عن نطاق الدِّراسة.

➤ **الجانب الثالث:** يتمثّل في النّظر إلى الدليل الرقميّ دون غيره من صور الأدلة الأخرى التّقليديّة ذات الطابع الماديّ.

ثالثاً: مُشكلة البحث:

تتجلّى المُشكلة الحقيقيّة للبحث في مدى فاعليّة الحماية الجزائيّة الإجرائيّة للأدلة الرقميّة، وإلى جانب هذه المُشكلة المُتقدّمة، نعرض لعدّة إشكاليات فرعيّة هي على النحو الآتي:

- هل الحماية الإجرائيّة التي نظمها المُشرّع الجزائيّ الإماراتيّ كافيةٌ لحماية الأدلة الرقميّة؟
- هل يختلف موقف المُشرّع المُقارن عن موقف المُشرّع الإماراتيّ في إقرار الحماية الجزائيّة للأدلة الرقميّة؟
- هل توجد خصوصيّة حقيقيّة في تنظيم الحماية الجزائيّة الإجرائيّة للدليل الرقميّ، وهل هذه الخصوصية تختلف عمّا هو مُقرّرٌ بعد الأدلة الرقميّة؟

رابعاً: منهجيّة البحث:

يعتمد الباحث في إطار الدِّراسة المُتقدّمة على المنهج التحليليّ المُقارن؛ كونه أقرب المناهج إلى روح الدِّراسة؛ نظراً لما يتضمّنه من تحليل موقف المُشرّع، وما يستتبعه ذلك من بيانٍ لموقف الفقه واجتهادات القضاء بصدد موضوع الدِّراسة، هذا بالإضافة إلى استعراض تنظيم الدِّراسة في ضوء النظام القانونيّ المُقارن، بحيث نتناول موقف النظام الإماراتيّ وكلّ من نظيره المصريّ والفرنسيّ؛ لأجل التوصل إلى نتائج إجابيّة سليمة وتوصيات صالحة للأخذ بها.

خامساً: خطة البحث:

➤ **المبحث الأول: الأحكام الإجرائيّة لاستخلاص الدليل الرقميّ.**

• **المطلب الأول: الوسائل الماديّة للحصول على الدليل الرقميّ.**

- **الفرع الأول: المُعاينة التّقنيّة.**

- **الفرع الثاني: التّفتيش التّقنيّ.**

• **المطلب الثاني: خصوصيّة التعامل مع الدليل الرقميّ.**

- **الفرع الأول: خصوصيّة ضبط الدليل الرقميّ.**

- **الفرع الثاني: خصوصيّة المُحافظة على الدليل الرقميّ.**

➤ **المبحث الثاني: التَّحْقِيق في جرائم التّعديّ على الدليل الرقميّ.**

• **المطلب الأول: التَّحْقِيق من سلامة الدليل الرقميّ.**

- الفرع الأول: كيفية التَّحَقُّق من سلامة الدليل الرقمي.
- الفرع الثاني: استبعاد الدليل الرقمي محلّ التلاعب أو العبث.
- المطلب الثاني: إجراءات التَّحْقِيق في جرائم التَّعْدِي على الدليل الرقمي.
- الفرع الأول: الاستعانة بالخبرة التقنية.
- الفرع الثاني: دور النيابة العامة في تقدير التلاعب والعبث بالدليل الرقمي.

المبحث الأول

الأحكام الإجرائية لاستخلاص الدليل الرقمي

تمهيد وتقسيم:

تعدُّ الأحكام الإجرائية التي تستهدف استخلاص الحصول على الدليل الرقمي، والتي نظَّمها كلُّ من المشرِّع الإماراتي ونظيره المصري، جانباً من الحماية الإجرائية الجزائية لهذه الأدلة الرقمية، والأحكام الإجرائية لها طابعها المهمُّ في هذا الصدد؛ نظراً إلى إتصالها الوثيق بالحماية الجزائية الموضوعية لهذه الأدلة الرقمية، وفي إطار الحديث عن هذه الأحكام الإجرائية، نُقسِّم هذا المبحث إلى مطلبين، وذلك على النحو الآتي:

المطلب الأول: الوسائل المادية للحصول على الدليل الرقمي.

المطلب الثاني: خصوصية التعامل مع الدليل الرقمي.

المطلب الأول

الوسائل المادية للحصول على الدليل الرقمي

يعدُّ الحصول على الدليل الرقمي من المسائل الجوهرية في البيئة الرقمية، لا سيَّما وأنَّ الحداثة التي تتميز بها هذه الأدلة الرقمية خلقت لها نوعاً من الخصوصية المعلوماتية، هذه الخصوصية أثَّرت بطبيعة الحال على الوسائل؛ أي الوسائل المادية التي من شأنها الحصول على هذه الأدلة الرقمية، وإزاء بيان هذه الوسائل المشروعة التي على ضوئها يتمُّ الحصول على الدليل الرقمي، نُقسِّم هذا المطلب إلى فرعين رئيسيين، وذلك على النحو التالي ببيان.

الفرع الأول

المُعَايَنَةُ التَّقْنِيَّةُ

يُقصد بالمُعَايَنَةُ عملية إثبات الحالة، سواءً تعلَّق الأمر بالأشخاص أو الأشياء؛ وذلك من أجل الكشف عن الحقيقة الخفية التي ترغبُ السُّلطات المعنية في الكشف عنها، وحتى تتمَّ المُعَايَنَةُ - وبخاصَّة في البيئة الرقمية - يتعيَّن توافُّر شرطين جوهريَّين، هما:

أ. الشرط الأول: يتمثَّل هذا الشرط في الجهة أو السُّلطة المعنية القائمة على أمر المُعَايَنَةُ، إذ يتعيَّن أن تكون لهذه السُّلطة شرعية مباشرة هذا العمل، وهذه السُّلطة في التشريع الإماراتي تتمثَّل في مأمور الضبط القضائي؛ عملاً بما نصَّت عليه المادَّة (35) من قانون الإجراءات الجزائية الاتِّحادي والتي نصَّت على أنه "يجبُ على مأموري الضبط القضائي أن يقبلوا التَّبليغات والشكاوى التي تَرِدُ إليهم في شأن الجرائم، ويجبُ عليهم وعلى مرؤوسهم أن يحصلوا على الإيضاحات وإجراء المُعَايَنَةُ اللازمة لتسهيل تحقيق الوقائع التي تُبلِّغ إليهم أو التي يعلمون بها بأيَّة كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحقُّطية اللازمة للمُحافظة على أدلة الجريمة"، وتعدُّ السُّلطة المُتقدِّمة هي ذاتها المُعوَّل عليها في المادَّة (1/24) من قانون الإجراءات الجنائية المصري.

ب. الشرط الثاني: يعدُّ هذا الشرط بَدْهِيًّا بالنظر إلى البيئة التي ينتمي إليها الدليل الرقمي، وهذا الشرط يتمثل في ضرورة الاستعانة بأهل الخبرة من الإعلام الرقمي؛ كونهم الأجدر على إجراء المعاينة؛ نظرًا لأنَّ المعاينة في البيئة الرقمية تختلف بطبيعة الحال عن المعاينة التقليدية.

وعلى ضوء ما تقدّم، يثور التساؤل من جانبنا حول صفة مأموري الضبط القضائي، وهل توجد خصوصية في تحديدهم إذا ما تعلّق الأمر بالأدلة الرقمية؟ هذا ما نوّدُ إيضاحه من خلال التفرقة بين موقف المُشرّع الإماراتي، ونظيره المصري، وذلك على النحو الآتي:

- موقف المُشرّع الإماراتي:

أصدر المُشرّع الاتحاديّ الإماراتي المرسوم بقانون رقم (34) لسنة 2021م في شأن مكافحة الشائعات والجرائم الإلكترونية، لما كان ذلك وكان الدليل الرقمي وثيق الاتصال بهذا القانون، فقد نظم المُشرّع تنظيمًا خاصًا لمأموري الضبط القضائي بالمادة (70) من القانون سالف الذكر.

مفاد ذلك أنّ المُشرّع الإماراتي نظم خصوصية مأموري الضبط القضائي في إطار القانون المتقدّم، بالمادة (70) من قانون مكافحة الشائعات والجرائم الإلكترونية والتي نصّت على أنه "يكونُ للموظّفين الذين يصدرُ بتحديدهم قرارٌ من وزير العدل أو رئيس الجهة القضائية المحلية بحسب الأحوال - صفةُ مأموري الضبط القضائي في إثبات الأفعال التي تقعُ بالمخالفة لأحكام هذا المرسوم بقانون، وعلى السُّلطات المحلية بالإمارات تقديمُ التسهيلات اللازمة لهؤلاء الموظّفين؛ لتمكينهم من القيام بعملهم"، بحيث إنّ صفة مأموري الضبط القضائي تثبت لطائفتين:

الطائفة الأولى: الموظّفون الذي يصدرُ بتحديدهم قرارٌ من وزير العدل.

الطائفة الثانية: رئيس الجهة القضائية المحلية.

- موقف المُشرّع المصري:

أصدر المُشرّع المصري قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018م، وبموجبه عوّل على تنظيم خاصٍ لمأموري الضبط القضائي؛ عملاً بما نصّت عليه المادة (5) من هذا القانون والتي نصّت على أنه "يجوزُ بقرارٍ من وزير العدل بالاتفاق مع الوزير المختصّ منحُ صفة الضبطية القضائية للعاملين بالجهاز أو غيرهم ممّن تُحددهم جهات الأمن القومي بالنسبة إلى الجرائم التي تقعُ بالمخالفة لأحكام هذا القانون والمتعلّقة بأعمال وظائفهم"، أي إنّ موقف المُشرّع المصري جاء متفقاً مع موقف المُشرّع الاتحاديّ الإماراتي في هذا الصدد، وقد أشرنا سلفاً لما نقصده في هذا النطاق بصدد موقف المُشرّع الإماراتي، ونُحيل إليه؛ منعاً للتكرار.

وتتخذ المعاينة في الجرائم الإلكترونية عدّة أشكال، وذلك حسب نوعية الجريمة المرتكبة، فعند العلم بوقوع الجريمة، فإنَّ أول خطوة يقوم بها مأمور الضبط القضائي هي الانتقال إلى مسرح الجريمة؛ فهو محلُّ آثار الجريمة والأدلة المادية لها، وفي الجريمة الإلكترونية ينبغي التفرقة بين مسرحين، هما: المسرح التقليدي والمسرح الافتراضي، وهما على النحو الآتي (المعمري، 2018م، ص 210).

- مسرح تقليدي: وهو ما يقعُ خارج بيئة الحاسب الآلي والإنترنت، ويتكوّن من المكوّنات المادية المحسوسة في المكان الذي وقعت فيه الجريمة، وهو كمسرح أية جريمة تقليدية، يتركُ فيها الجاني عدّة آثار، كال بصمات أو المتعلّقات الشخصية أو وسائل تخزينية رقمية.

- مسرح افتراضي (إلكتروني): وهو ما يقعُ داخل البيئة الإلكترونية، ويتكوّن من البيانات الرقمية التي تتواجد أو تنتقل داخل الحاسب الآلي وشبكة الإنترنت، وفي ذاكرة الأقراص الصلبة الموجودة بداخلها، والتعامل مع الأدلة الموجودة في هذا المسرح،

لا بُدَّ أن تتمَّ على أيدي مُختصِّين وذوي خبرةٍ في التعامل مع الأدلة الإلكترونية (حنفي، 2017م، ص 55 – 56)، وتتعدَّد الصعوباتُ بصدد المعاينة في نطاق مسرح الجريمة الإلكترونية، نذكر منها الآتي (المعمري، ص 211).
إنَّ المعاينة في مسرح الجريمة الإلكترونية تُظهر عدَّة صعوباتٍ في مجال كشف الجريمة وضبط الأشياء التي تفيد في وقوعها ومعرفة فاعلها، ويمكنُ تلخيصُ تلك الصعوباتِ وفُقِّ التَّالي:

- 1- قلة الآثار الماديَّة التي تترتَّب عن الجرائم الإلكترونية.
 - 2- تردُّد العديد من الأشخاص على مسرح الجريمة خلال الفترة الزمنيَّة الطويلة نسبياً ما بين وقوع الجريمة والكشف عنها، وهو ما يُتيح الفرصة للعبث وإتلاف وتغيير الآثار الماديَّة، وهو ما يُدخل الشكَّ في الأدلة المُستمدَّة من المعاينة.
 - 3- إمكانية تلاعب الجاني في البيانات والمعلومات عن بُعد أو مَحْوُها أو إتلافها عن طريق التدخُّل من خلال وحدة طرفيَّة خارجيَّة، لذا ينبغي على المُشرِّع أن يضع جزاءاتٍ جنائيَّةً على من يقوم بإجراء أيِّ تغييرٍ أو تعديلٍ في المعلومات والبيانات المُخزَّنة والمتوقِّرة في الجهاز الإلكتروني قبل قيام مأموري الضبط القضائيِّ بإجراء المعاينة.
 - 4- زوال الأدلة الإلكترونية التي يمكنُ مَحْوُها أو تعديلها أو تغييرها في ثوانٍ معدودة، لذا أجازت بعضُ التَّشريعات لأعضاء النيابة العامَّة تعجيل إجراء المعاينة خشية ضياع الأدلة، من خلال إرسال رسالةٍ إلى مُزوِّد الخدمة بتتبع السجلات المطلوبة، وذلك إلى حين أن تُصدر المحكمة المعنيَّة قرارها باتِّخاذ الإجراء. (عمر، 2013م، ص 125 – 128).
- ونتيجة الاختلاف في مسرح الجريمة الإلكترونية عن غيره في الجرائم التَّقليديَّة الأخرى؛ فإنَّ هذا المسرح يميَّز بوجود أدلة ذات طبيعةٍ غير مرئيَّة، تقتضي التعامل معه بحرصٍ وبشكلٍ خاصٍّ، وذلك من خلال اتِّباع بعض القواعد الفنيَّة والإرشادات قبل الانتقال إلى مسرح الجريمة الإلكترونية، ومن أهمِّها ما يلي (المعمري، ص 211):

- 1- الإعداد الجيِّد قبل المعاينة: لعدم تسرُّب الأدلة أو إتلافها.
 - 2- إعداد فريق المعاينة من المُختصِّين بتقنيَّة المعلومات وشبكات الإنترنت.
 - 3- إعداد خريطةٍ للموقع الذي تتمُّ المعاينة فيه وتحديد معلوماتٍ مُسبقَةٍ عنه.
 - 4- الحصول على الاحتياجات الضَّروريَّة من أجهزة وبرامجٍ للاستعانة بها في الفحص والتَّشغيل.
 - 5- تأمين تيارٍ كهربائيٍّ احتياطيٍّ؛ تجنباً للانقطاع المفاجئ أثناء الفحص وإتلاف مُكوِّنات الحاسوب.
- ويتمُّ توثيقُ مسرح الجريمة بالكامل من خلال وصف مُحتوياته بشكلٍ جيِّد، وتوثيق كلِّ دليلٍ على حدة، بما فيها الأدلة الإلكترونية، بحيث يتمُّ توضيح مكان الضبط والهيئة التي كان عليها، وما قام برفعه وتحريزه، وكيف ومتى تم ذلك، وهناك البعض ممَّن يرى بأنَّ التوثيق يجبُ أن يشملَ كافة المصادر المُتاحة على الشبكة التي ترتبطُ بها الأجهزة محلُّ المعاينة، ولعلَّ أبرز الأماكن التي يحتملُ تواجد الأدلة الجنائيَّة فيها والمتعلِّقة بالجرائم الإلكترونية فيها، ما يلي (المعمري، ص 213):
- الورق: ويتمُّ الحصول عليه من خلال البحث في سلة المُهملات عن أوراق مطبوعة ذات علاقةٍ بالحاسب الآليِّ محلِّ المعاينة، ويعدُّ من الأدلة التي ينبغي الاهتمامُ بها عند البحث عن الحقيقة.
 - المُكوِّنات الماديَّة: كأجهزة الحاسب الآليِّ بأنواعها المُختلفة، والأقراص الصَّلبة الخارجيّة، والملحقات المُرتبطة بأجهزة الحواسيب ذات الصَّلة بالجريمة، كالطابعات والمساحات الضوئيَّة والكاميرا الرقميَّة وغيرها من الأجهزة الماديَّة الأخرى.
 - البرامج: إذا كان الدليلُ الإلكترونيُّ نشأ نتيجة برنامجٍ خاصٍّ أو أنه ليس واسع الانتشار، فإنَّ أخذ الأقراص الخاصَّة بتثبيت وتنصيب هذا البرنامج يعدُّ أمراً في غاية الأهميَّة عند فحص الدليل.
 - وسائط التخزين المُتحرِّكة: كالأقراص المُدمجة والأقراص المرنة والشرائط المغناطيسيَّة، وأيِّ من أشكال أشرطة التخزين الخارجيّة المُختلفة، مثل (فلاش ميموري).

- دليل الاستخدام الخاص بالمكونات المادية والتقنية للجهاز الإلكتروني، والذي يفيد في معرفة التفاصيل الدقيقة لكيفية عمله.

- كلمات السرّ أو أرقام الهاتف، والتي قد تكون مكتوبة على أوراق ملصقة بالحاسب الآلي أو بقرتها، وقد تكون خاصة بحسابات الاتصال بشبكة الإنترنت.

وعلى ضوء ما سبق، ولكي تُؤتي المعاينة ثمارها عند القيام بها من قبل مأموري الضبط القضائي، فإنه لا بدّ من تأهيلهم وتعليمهم علوم الحاسب الآلي وتقنية المعلومات، وكيفية التعامل مع الأجهزة الإلكترونية المختلفة، والتي أصبح لها الدور المهم في مختلف مجالات الحياة، ومنها المجال الأمني، للكشف عن الجرائم وضبطها وتحليلها والحصول على الأدلة منها، ويرى جانب من الفقه الجنائي أنّ مأموري الضبط القضائي عند قيامه بالمعاينة من أجل الاستدلالات وجمع التحريات، يلزمه القيام بالآتي **(المعمري، ص 214):**

- 1- تحديد نوع نظام المعالجة الآلي للمعلومات؛ هل هو متصل بالشبكة أو لا؟ وذلك لأنّ عملية البحث والتحري تكون صعبة في حالة وجود ملحقات طرفية أو شبكات أخرى متصلة بالجهاز الإلكتروني محل المعاينة.
- 2- وضع خطة شاملة للمنشأة ككلّ، وإعداد كشف بأسماء المسؤولين عنها ودور كلّ منهم، فهناك من يقوم بالمعالجة الآلية للمعلومات، وهناك من يقوم بإدارة الدراسات والتطوير وإدارة وتشغيل نظم المعلومات.
- 3- إذا كان الأمر يتعلق بشبكة، فيجب إحصاء الطرفيات وتحديد طبيعة الروابط الموجودة بينها؛ لمعرفة الطريقة التي يتم بها نقل المعلومات من موقع لآخر.
- 4- مراعاة أنّ الدليل في مجال المعالجة الآلية للبيانات يمكن أن يختفي خلال وقت قصير جداً، إذ يمكن للجاني أن يتدخل من خلال وحدة طرفية لإتلاف المعلومات المخزنة في الجهاز، عن طريق ساعة في معصم اليد أو هاتفه المحمول، وغيرها من وسائل تقنية المعلومات.
- 5- ضرورة فصل التيار الكهربائي من مكان خارج الموقع قبل دخوله، وهذا الإجراء يمنع المستخدم من التلاعب في المعلومات أو محوها، وإن كان لذلك أثره في فقد المعلومات المخزنة في الذاكرة العشوائية لأجهزة الحاسبات الآلية، وللضضاء على تدخل المجالات المغناطيسية مع بعضها على نحو يؤدي إلى إتلاف البيانات.
- 6- فصل خطوط الهاتف؛ تحسباً لاستعمال "المودم" في جهاز المعالجة الآلية للمعلومات، والمُراد ضبطه.
- 7- التأكد من عدم استخدام خاصية تحويل المكالمات، والتأكد من أنّ رقم الهاتف يخصّ جهاز الحاسب الآلي محلّ المعاينة.

الفرع الثاني

التفتيش التقني

يُقصد بالتفتيش المساس بحرية الفرد الشخصية في حماية أسراره، لذلك يتعيّن أن يكون مشروعاً **(أبو عامر، 2010م، ص 200)**، ويختلف التفتيش باختلاف نوعه والغرض منه، وهو ما يعكس بصورة واضحة وجه الاختلاف بين التفتيش في البيئة الرقمية والتفتيش التقليدي؛ نظراً لأنّ التفتيش في البيئة الرقمية يتناول محلاً معيّناً، ألا وهو الحاسوب الآلي وما يتصل به من أجهزة ملحقة لها طابع تقني ومزود بخدمة التخزين الإلكتروني.

وفي هذا المقام يثور التساؤل من جانبنا: هل نظم المشرع التفتيش في البيئة الرقمية بصورة صريحة، ونعرض في هذا الصدد وجه التفرقة بين موقف المشرع الإماراتي وما عليه الحال بصدد المشرع المصري، على النحو الآتي:

أ) موقف المشرع الاتحادي الإماراتي:

لم يُنظم المشرع الاتحادي الإماراتي بصورة صريحة مسألة التفتيش في البيئة الرقمية؛ أي إنّ قانون مكافحة الشائعات والجرائم الإلكترونية جاء خالياً من تنظيم هذا الأمر، وذلك على غرار المَعوّل عليه بصدد التشريع المصري كما سنرى.

ويعُدُّ التفتيش في الجرائم الإلكترونية ذا طبيعة خاصة ومتميزة عن التفتيش التقليدي للمساكن والأشخاص (حكم المحكمة الاتحادية العليا، الطعن رقم 287 لسنة 27 قضائية، 37 لسنة 2019 قضائية).

(ب) موقف المشرع المصري:

تناول المشرع بالتنظيم مسألة التفتيش في البيئة الرقمية على النحو الذي نظمته المادة (2/6) من قانون مكافحة جرائم تقنية المعلومات والتي نصت على أنه "الجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين، لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، بوحدة أو أكثر ممّا يأتي: 2- البحث والتفتيش والدخول والنفوذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية؛ تحقيقاً لغرض الضبط ..."، إذ يعدُّ موقفه على هذا النحو أفضل ممّا عليه الحال بصدد المشرع الإماراتي.

(ج) موقف المشرع الفرنسي:

في إطار إيضاح موقف المشرع الفرنسي بصدد مسألة التفتيش التقني، يتعين إدراك ما نظمته المشرع بالمادة [17\أ] من قانون الأمن الداخلي رقم [٤٣٩] لسنة ٢٠٠٣ م، إذ نصت هذه الأخيرة على أنه "يجوز لرجال الضبط القضائي من درجة ضابط وغيرهم من رجال الضبط القضائي أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي تمّ التفتيش فيها على البيانات التي تمّ التحقيق في النظام المذكور أو في نظام معلومات آخر ما دامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيسي أو يتمّ الدخول إليها أو تكون متاحة ابتداءً من النظام الرئيسي.

[Loi 2003 - 239, 2003 - 03 - 18 art. 17.1 Jorf. 19 mars, 2003]

وفي إطار هذه الطبيعة الخاصة للتفتيش في البيئة الرقمية، تتكوّن تلك الأجهزة وجهاز الحاسب الآلي من مكونات مادية ومكونات أخرى معنوية، ونعرض لكيفية تفتيشها على النحو الآتي (المعمري، ص 217):

أ. تفتيش مكونات الجهاز الإلكتروني المادية:

إنّ تفتيش المكونات المادية للجهاز الإلكتروني بحثاً عن الأدلة أو أي شيء يتصل بالجريمة الإلكترونية يُفيد في كشف الحقيقة عنها أو مرتكبها، يخضع للإجراءات القانونية والقواعد العامة لإجراء التفتيش، كالإجراءات التي يُقام بها عند التفتيش في الجريمة التقليدية؛ نظراً لأنّ الغاية هنا هي تفتيش أجزاء ومكونات مادية، ويعني ذلك أنّ حكم التفتيش للمكونات المادية للجهاز الإلكتروني يعتمد في ذلك على طبيعة المكان الذي تتواجد فيه تلك المكونات المادية، سواء أكان مكاناً عاماً أم مكاناً خاصاً، فإذا كان مكان تواجد المكونات المادية مع الشخص في مكان عام وهو حائز لها، سواء أكان المكان عاماً بطبيعته كالطرق العامة والميادين، أم كان مكاناً عاماً بالتخصيص كالمقاهي والحافلات العامة، فإنّ التفتيش هنا يخضع للحالات التي يجوز فيها تفتيش الأشخاص بذات الضمانات والقيود المنصوص عليها في هذا الشأن (هروال، 2013 م، ص 237).

أمّا إذا كان مكان تواجد المكونات المادية للجهاز الإلكتروني في مكان خاص كمسكن المتهم أو أحد ملحقاته، كان لذلك المكان حكمه كذلك، أي إنه لا يجوز تفتيش المكونات المادية إلا في الحالات التي يجوز فيها تفتيش المساكن، وبذات الضمانات والإجراءات المقررة قانوناً في هذا المجال.

وتفتيش المكونات المادية للجهاز الإلكتروني لا يعني البحث عن البصمات والآثار المادية الأخرى مثلما هو حاصل في الجرائم الجنائية التقليدية الأخرى، وإنما يكون بالبحث عن الأجهزة والملحقات المرتبطة بها، كالبحث عن طابعة أو جهاز ماسح ضوئي؛ لقيامه بجريمة تزوير، أو البحث عن جهاز الوصول للإنترنت (مودم)؛ لقيامه بجريمة اختراق مواقع إلكترونية (المعمري، ص 218)، وذلك يعدّ موطناً من مواطن الخصوصية الرقمية في الجرائم المعلوماتية.

ب. تفتيش مكونات الجهاز الإلكتروني المعنوية:

تنقسم المكوّنات المعنويّة للأجهزة الإلكترونيّة بشكلٍ عامٍّ وللحاسب الآليّ بشكلٍ خاصٍّ، إلى نوعين رئيسيين: الأول منهما يختصُّ بتشغيل الجهاز ذاته وتحسين أدائه ببرامج تكون ثابتةً في الجهاز تعملُ على ذلك، مثل عرض الشاشة الرئيسيّة للجهاز ونظام تشغيله، والنوع الثاني منهما يُساعد المُستخدم على القيام بأداء أعماله وتسهيل استخدامه للجهاز مثل البرامج المكتبيّة، فعند استخدام هذه البرامج وحفظها يتمُّ إضافة ملفٍ ومُحتوى جديدين بالجهاز غير موجودين مُسبقًا، وهو نتيجة استخدام المُستخدم للجهاز، وهناك نوعٌ آخرٌ من المُحتويات المعنويّة، وهي المُحتويات المُتعلّقة بشبكة المعلومات والإنترنت (حسين، 2011م، ص 217 – 218).

فإذا ما قام أحدُ المُستخدمين لمواقع التواصل الاجتماعيّ بسبِّ أو قذف أحد الأشخاص في ذات الموقع، فلمعرفة المُتهم في هذه الجريمة لا بدُّ أن تقوم سلطات التحريّ والتّحقيق بالتواصل مع المُختصّين بذات الموقع للحصول على العنوان الإلكترونيّ الخاصّ بالمُتهم الذي قام بالسبِّ أو القذف، وهي من الإجراءات الحديثة التي سيتمُّ بيانها تفصيلًا عند معرض الحديث عن الإجراءات الحديثة لجمع الدليل الإلكترونيّ (المعمري، ص 218).

ثالثًا: شروط التفتيش في البيئة الإلكترونيّة:

نقسم شروط التفتيش في هذا المقام إلى طائفتين: الطائفة الأولى هي طائفة الشروط الشكلية أو الإجرائية، أمّا الطائفة الثانية فهي طائفة الشروط الموضوعية، ونعرض لكلّهما على النّحو الآتي (المعمري، ص 222 وما بعدها):

1- الشروط الشكلية لتفتيش الأجهزة الإلكترونيّة:

أ. حضور بعض الأشخاص أثناء إجراء التفتيش في البيئة الإلكترونيّة:

عند إجراء التفتيش على الأشخاص لم تشترط أغلب التشريعات وجود شهود أو حضور أشخاص عند القيام بهذا الإجراء، أمّا فيما يتعلّق بتفتيش المساكن والأماكن عمومًا، فالأمر مُختلف، فنصّت غالبية التشريعات على وجود شهود عند القيام بالتفتيش، ومنها ما نصّ عليه المشرّع المصريّ من اشتراط حضور شاهدين عند إجراء التفتيش بمعرفة أحد مأموري الضبط القضائيّ، كما اشترط أن يكون الشاهدان بقدر الإمكان من أقارب المُتهم البالغين أو القاطنين معه بالمسكن أو من الجيران (م 59 إجراءات جزائية إماراتي)، (م 51 إجراءات جنائية مصرية).

ب. الزمن المُتعيّن لإجراء التفتيش في الجرائم الإلكترونيّة:

يعدُّ الزمن المُتعيّن حصول التفتيش خلاله أمرًا متروكًا إلى حكم القواعد العامة الوارد النصُّ عليها في قانون الإجراءات الجزائية، أمّا زمن التفتيش وفق المنظور الضيق فهو أمرٌ تقتضيه الطبيعة التقنية، على النّحو الذي يتولاه المُختصّون من التقنين، لكن يتعيّن كذلك أن يكون إجراء هذا التفتيش في الأوقات النهارية من اليوم، بحيث لا يكون بعد مُنتصف الليل على ضوء المثال.

ج. محضر التفتيش في الجرائم الإلكترونيّة:

يعدُّ محضر التفتيش إجراءً ثبوتيًا لازمًا في الجرائم الإلكترونيّة، هذا بالإضافة إلى ضرورة وجود مُتخصّصين أثناء إجراء هذا التفتيش على النّحو الذي أسلفناه في هذا الصّدّد، وفي هذا المقام قضت المحكمة الاتّحادية العليا الإماراتيّة بأنّ "المحاضر التي يُحرّرها مأمور الضبط القضائيّ في حدود اختصاصه هي أوراقٌ لها حجّية في الإثبات ولا يمكن دحض ما ورد فيها إلا بالطعن بالتزوير" (المحكمة الاتّحادية العليا، الطعن رقم 460 لسنة 2014 قضائية).

2- الشروط الموضوعية لتفتيش الأجهزة الإلكترونيّة:

وهي الضوابط اللازمة لإجراء تفتيش صحيح، وتكون في الغالب سابقة له؛ أي إنه لا بدُّ من توافرها قبل إجراء عملية التفتيش، وتتمثّل هذه الشروط الموضوعية في الآتي (المعمري، ص 224):

- سبب التفتيش في البيئة الإلكترونيّة:

إنَّ سبب التفتيش في الجرائم الإلكترونية يجب أن يكون مُستنداً إلى ثلاثة شروط فرعية، الأول: هو وقوع جريمة من الجرائم الإلكترونية بالفعل من نوع الجنائية أو الجنحة، وذلك يكون وفقاً للأفعال التي يُحددها المُشرع في هذا المجال، والثاني: هو اتهام شخص أو أشخاص مُعَيَّنِينَ بارتكاب الجريمة أو الاشتراك فيها، وذلك يكون وفقاً لدلائل كافية ومظاهر وأمارات قائمة على العقل والمنطق والخبرة الفنية تدلُّ على أنَّ الشخص هو مَنْ قام بارتكاب الجريمة، والثالث: هو توافر قرائن قوية على وجود معلومات أو بيانات أو معدات مادية تفيد في كشف الحقيقة لدى المُتهم المعلوماتي أو غيره (المعمري، ص 225).

- السُّلطة المُختصة بالتفتيش:

تتمثل السُّلطة المُختصة بالتفتيش وفقاً لأصل العام في النيابة العامة أو مَنْ تعهد إليه من مأموري الضبط القضائي، إذ تمنحه هذه السُّلطة باعتباره نائباً عنها في إتمامه، وهذا أمرٌ معمولٌ به في نطاق الجرائم والأدلة التقليدية، وكذلك الرقمية. والتساؤل الذي يثور في هذا المقام هو: هل السُّلطة المعنية بإجراء التفتيش في التشريع الفرنسي في هذا المقام هي ذات السُّلطة المقررة أعلاه، أو أنها سُلطة مُختلفة، وهذا ما يتعين معه الرجوع إلى ما نظمته القواعد العامة الواردة في قانون الإجراءات الجنائية والتي تجعل قاضي التحقيق هو السُّلطة الأصلية في مباشرة أعمال التفتيش، على خلاف ما هو مُقررٌ للنيابة العامة واختصاصها بالتفتيش في بعض الآونة كحالات التلبس، أمّا موقف المُشرع الأمريكي فجاء متفقاً مع الأصل العام الذي يقضي بأغلبية مباشرة غالبية الإجراءات من قِبَل النيابة العامة (عبد اللاه، ٢٠٠٨م، ص ١٣٣ وما بعدها).

المطلب الثاني

خصوصية التعامل على الدليل الرقمي

تمهيد وتقسيم:

في إطار الحديث عن خصوصية التعامل مع الأدلة الرقمية، نعرض لجانبين من أحكام هذه الخصوصية، بحيث نعرض في الجانب الأول لخصوصية ضبط الدليل الرقمي، وذلك مُقارنتاً بما عليه الحال بصدد ضبط الأدلة المادية التقليدية، إضافةً إلى استعراض الحديث في الجانب الثاني عن الخصوصية التي تمتاز بها المحافظة على الدليل الرقمي، وعلى كلٍّ يتعين أن يكون التعامل على هذا الدليل الرقمي بالطرق المشروعة التي نظمها المُشرع، وعلى ضوء التمهيد البسيط المُتقدم نتناول هذا المطلب في فرعين رئيسيين على النحو التالي بيانه.

الفرع الأول

خصوصية ضبط الدليل الرقمي

يعدُّ الضبط من قبيل الإجراءات المترتبة كأثرٍ على المعاينة والتفتيش (المصفاوي، 1998م، ص 402) في البيئة الرقمية، ونظراً لخصوصية البيئة الرقمية - كما أسلفنا البيان - فإنَّ الضبط يقع على دعامة إلكترونية، حركات اتصال، شبكة معلوماتية، أو بيانات ومعلومات إلكترونية بصفة عامة (قارة، 2010م، ص 114)، والتساؤل في هذا الصدد يثور حول تنظيم المُشرع لإجراءات الضبط في البيئة الرقمية، وهل تمَّ تنظيمها من عدمه؟ وهذا ما سنعرض له بصورة مُفصلة في نطاق التشريع الإماراتي ونظيره المصري، وذلك على النحو الآتي:

(أ) موقف المُشرع الإماراتي:

لم يُنظم المُشرع الاتحادي الإماراتي طي قانون مكافحة الشائعات والجرائم الإلكترونية مسألة إجراءات الضبط في نطاق البيئة الرقمية، بل ترك أمر تنظيمها للقواعد العامة في قانون الإجراءات الجزائية، وهذا أمرٌ لا يراه الباحث مُوفقاً؛ نظراً لأنه يطمس معالم الخصوصية والتُمييز بين البيئة الرقمية ونظيرتها التقليدية، هذا بالإضافة إلى أنَّ القواعد المُعول عليها بصدد الضبط في

نطاق قانون الإجراءات الجزائية نراها لا تتماشى مع ما عوّلت عليه المادة (61) من قانون الإجراءات الجزائية الإماراتي بقولها: "للمأموري الضبط القضائي أن يضبطوا الأشياء التي يُحتمل أن تكون قد استعملت في ارتكاب الجريمة أو نتجت عن ارتكابها أو يُحتمل أن تكون قد وقعت عليها الجريمة، وكذلك كل ما يفيد في كشف الحقيقة. وتُوصف هذه الأشياء وتُعرض على المتهم، ويُطلب منه إبداء ملاحظاته عليها، ويُحرر بذلك محضر يُوقعه المتهم أو يذكر فيه امتناعه عن التوقيع. وتوضع الأشياء والأوراق المضبوطة في حرز مغلق مختوم بالشمع الأحمر ويكتب على الحرز تاريخ المحضر المُحرر بضبط تلك الأشياء، ويُشار إلى الموضوع الذي حصل الضبط من أجله".

ب) موقف المُشرع المصري:

نظم المُشرع المصري مسألة إجراءات الضبط في المادة (1/6) من قانون مكافحة جرائم تقنية المعلومات والتي نصّت على أنه "لجهة التحقيق المختصة - بحسب الأحوال - أن تُصدر أمراً مسبباً لمأموري الضبط القضائي المُختصين، لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة مُعاقب عليها بمقتضى أحكام هذا القانون، بواحدة أو أكثر ممّا يأتي: 1- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه. ويتم تسليم أدلتها الرقمية للجهة مُصدرة الأمر، على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مُقتضى..."، وبذلك يكون إجراء الضبط في البيئة الرقمية كإجراء تقليديّ أمراً مُعولاً عليه بصدد الحصول على الدليل الرقمي بصورة مشروعة، وهذا على غرار ما أقامه المُشرع الإماراتي في هذا الصدد.

ج- موقف المُشرع الفرنسي:

تعدّ الجهة المعنية بالتفتيش هي ذاتها المعنية بالضبط على النحو الذي نظّمته المادة (17/أ) من قانون الأمن الداخلي رقم (239) لسنة 2003م، وهي في هذا المقام لها طابع من الخصوصية تتفق مع ما هو مُعول عليه من جانب المُشرع المصري.

الفرع الثاني

خصوصية المحافظة على الدليل الرقمي

في إطار الحديث عن مناهج الخصوصية بصدد المحافظة على الأدلة الرقمية، يتعين القول: إنّ المحافظة على هذا النوع من الأدلة أمر ذو طبيعة تقنية؛ أي إنّ أصحاب الخبرة التقنية هم من يتولّون القيام بهذه المهمة، وعلى ضوء ذلك يتعين النظر بدايةً فيما إذا كان المُشرع قد نظم الطرق التي من شأنها المحافظة على هذه الأدلة الرقمية من عدمه، وبالرجوع إلى موقف المُشرع في هذا الصدد نراه جاء خالياً من النصّ على هذه الطرق، سواء تعلّق الأمر بموقف المُشرع الاتحاديّ الإماراتي أم نظيره المصري، لذلك يتعين الرجوع إلى ما عرّضه الفقه من مهام للخبير الإلكتروني في ضوء المحافظة على الأدلة الرقمية.

إذ عند استخراج الخبير الإلكتروني لتلك الأدلة وتجميعها، عليه الالتزام ببعض القواعد الفنية والخطوات في هذا المجال، وتتمثل هذه الخطوات والقواعد الفنية في المراحل التالية (المعمري، ص 231 - 232):

- أ. خطوات ما قبل التّشغيل والفحص:
 - التأكد من مطابقة محتويات إحراز المضبوطات لما هو مكتوب عليها.
 - التأكد من صلاحية وحدات نظام التّشغيل.
 - تسجيل بيانات وحدات المُكوّنات المضبوطة، كنوعها وطرازها والرقم المُتسلسل لها.
- ب. خطوات التّشغيل والفحص:
 - عمل نسخة من كلّ وسائط التّخزين المضبوطة وأهمّها القرص الصلب؛ لإجراء عملية الفحص المبدئيّ على هذه النسخة؛ لحماية الأصل من أيّ فقد أو تلف أو تدمير، سواء من سوء الاستخدام أو لوجود فيروسات أو قنابل برمجية.
 - استكمال تسجيل باقي بيانات الوحدات من خلال القراءات التي يوفّرها الجهاز.

- تحديد أنواع وأسماء المجموعات البرمجية، كبرامج النظام، وبرامج التطبيقات، وبرامج الاتصالات.
- إظهار الملفات المخبأة والنصوص المخفية داخل الملفات.
- استرجاع الملفات التي تم محوها من الأصل؛ وذلك باستخدام برامج استعادة البيانات، وكذلك بالنسبة للملفات المعطلة أو التالفة من خلال إعادة تشغيلها وإصلاحها، وتخزين هذه الملفات بعد ذلك ويعمل لها نسخة طبق الأصل من الأسطوانة أو القرص محل الفحص.
- إعداد قائمة يُجرّد فيها الخبير الإلكتروني كلّ الأدلة الإلكترونية التي تم الحصول عليها في وعاء خاص، مع إجراء مراجعة لكلّ الملفات المُحتفظ بها في الوعاء في جهاز آخر للتأكد من سلامة القائمة.
- تحويل الدليل الإلكتروني إلى هيئة مادية؛ وذلك عن طريق طباعة الملفات أو تصوير محتوياتها إذا كانت صوراً أو نصوصاً، أو وضعها في أي وعاء آخر حسب نوع المعلومات والبيانات المكونة للدليل.
- ج. تحديد مدى الترابط بين الدليل المادي والدليل الإلكتروني:
- في هذه المرحلة يتم فحص كلّ من الدليل المادي المضبوط والدليل الإلكتروني في شكله المادي، ومن ثم الربط بينهما؛ لإكساب الدليل الموثوقية واليقينية، ممّا يؤدي لقبوله لدى جهة التحقيق والمحاكمة.
- د. مرحلة تدوين النتائج وإعداد التقارير:
- تعدّ هذه المرحلة هي النهائية في هذا الصدد، وعلى ضوءها يتم جمع كافة الأدلة وإرفاقها بغيرها من الملاحق وتقديمها إلى الجهات المعنية.

المبحث الثاني

التحقيق في جرائم التعدي على الدليل الرقمي

تمهيد وتقسيم:

يعدّ التحقيق والتحقّق مُصطلحين لازمين، وثيقيّ الصلة في العمل القضائي، لا سيّما إذا تعلّق الأمر بالأدلة الرقمية، حيث إنّ جرائم التعدي على الدليل الرقمي إذا ما نظرنا إلى الجانب الإجرائي الخاص بها، نرى أنه يتعيّن التحقّق من سلامة هذا الدليل الرقمي، إضافة إلى استعراض إجراءات التحقيق، وفي إطار تفصيل مُفردات هذا المبحث المُتقدّم، نقسّمه إلى مطلبين، وذلك على النحو الآتي:

المطلب الأول: التحقّق من سلامة الدليل الرقمي.

المطلب الثاني: إجراءات التحقيق في جرائم التعدي على الدليل الرقمي.

المطلب الأول

التحقّق من سلامة الدليل الرقمي

تمهيد وتقسيم:

يعدّ التحقّق من سلامة الدليل الرقمي مسألة مهمّة؛ نظراً لأنّ هذا الدليل الرقمي يعدّ حجة في الإثبات ومعمولاً به، ولمّا كان ذلك وكان يتطلّب في الدليل الرقمي الصحة والمشروعية، فإنّ التحقّق من سلامته بات أمراً لازماً في هذا الخصوص، لذلك يمكننا القول بضرورة استعراض هذا المطلب في فرعين رئيسيين، نعزّض لهما على النحو التالي بيانه.

الفرع الأول

كيفية التحقّق من سلامة الدليل الرقمي

في إطار الحديث عن كيفية التحقّق من سلامة الدليل الرقمي، نعزّض لبعض المواطن الإجرائية في هذا الصدد، والتي على ضوءها يسلم الدليل الرقمي من أيّ عوارٍ قد يلحق به ممّا يفقد جوهريه، لذلك نعزّض لهذه المواطن على النحو الآتي:

أولاً: التأكد من طرق الحصول عليه:

يعدُّ هذا المواطنُ أهمَّ المواطن على الإطلاق إذا ما تعلَّق بالتأكد من طرق الحصول على الدليل الرقمي، مفاد ذلك أنَّ كافة الإجراءات المتعلقة بالمعينة أو الضبط أو التفتيش أو شهادة الشهود يتعيَّن أن يكون قد تمَّ الحصول عليها بالطريق المشروع الذي نصَّ عليه القانون، ولا فرق في هذه المسألة بين ما إذا كانت هذه الأدلة تقنية أو رقمية، أو كونها تقليدية مادية، وتعدُّ هذه المسألة قد أفصح عنها القضاء مراراً وتكراراً، وعلى سبيل المثال: قضت محكمة النقض المصرية في هذا المقام بأنه "من مهمة مأمور الضبط القضائي بمقتضى المادة (21) من قانون الإجراءات الجنائية الكشف عن الجرائم والتوصل إلى مرتكبيها، وكلُّ إجراء يقوم به في هذا السبيل يُعتبر صحيحاً مُنتجاً لأثره ما دام لم يتدخل بفعله في خلق الجريمة أو التحريض على مقارفتها وطالما بقيت إرادة الجاني حرة غير معدومة" (حكم محكمة النقض المصرية، الطعن رقم 3536 لسنة 52 قضائية).

ثانياً: التقارير الخاصة بأهل الخبرة:

يعدُّ التقرير الصادر من أهل الخبرة من قبيل المواطن الموعول عليها بصدد سلامة الدليل الرقمي، وقد أكدَّ المُشرع في ضوء القواعد العامة بالمادة (98) من قانون الإجراءات الجزائية الاتحادية الإماراتية والتي نصَّت على أنه "يُقدِّم الخبير تقريره كتابةً، ويُحدِّد عضو النيابة العامة للخبير ميعاداً لتقديمه، وله أن يستبدل به خبيراً آخر إذا لم يُقدِّم التقرير في الميعاد أو استدعى التحقيق ذلك"، على أهميَّة التقرير الكتابي الذي يخلص إليه الخبير فور الانتهاء من أداء عمله، لذلك يتعيَّن في هذا الخبير أن يكون من أهل الثقة والأمانة في سبيل إتمام هذا العمل كما أشرنا لا سيَّما وأنَّ الخبرة التقنية من قبيل المسائل الفنية، وبعض النقاط لا يمكن للغير - حتى ولو كان من قبيل المختصين - أن يدرك ما يقوم بفعله بعض أهل الخبرة التقنية، لذلك تعدُّ مسألة العلم بالخبرة التقنية في هذا المقام مسألة نسبية.

ويثور التساؤل في هذا المقام؛ هل للشاهد دور ملموس إزاء مُساندة الجهات المعنية في الكشف عن الجريمة المعلوماتية وتشكيل الدليل الرقمي؟ وإزاء الإجابة عن هذا التساؤل نتناول موقف الفقه الفرنسي، إذ يتجَّه جانب منه إلى أن المُشرع لم يُنظِّم هذه المسألة، وإنما يُحيلها إلى تنظيم القواعد العامة، وبالرجوع إلى المواد [١٠٩]، [٤٣٨] من قانون الإجراءات الجنائية الفرنسي نرى أنَّ الشاهد مُكلَّف بالكشف عن كلمات المرور ذات الطابع السريِّ حال معرفتهم لها، هذا بالإضافة إلى شفرات تشغيل البرامج، ويُستثنى من ذلك حالات المحافظة على الأسرار المهنية. [Francillon, 1993, p.309]

ثالثاً: الدور الجوهرى لقضاء الموضوع:

يقع في هذا المقام على عاتق المحكمة ودورها الأصيل مسألة التأكد من سلامة الدليل الرقمي، لا سيَّما وأنَّ المسألة متروكة إلى تقديرها في هذا الخصوص، وهذا ما أكَّدته المحكمة الاتحادية العليا الإماراتية (المحكمة الاتحادية العليا الإماراتية، الطعن رقم 10 لسنة 23 قضائية).

الفرع الثاني

استبعاد الدليل الرقمي محل التلاعب أو العبث

إذا كان الدليل الرقمي في حال العبث أو التلاعب به، تصدَّى المُشرع الجزائي له وعده جريمة يستوجب معها العقاب، فإنَّ هذا مفاده ضرورة استبعاد هذا الدليل من نطاق الأدلة الموعول عليها في الدَّعوى الجزائية، وإزاء ذلك يثور التساؤل بصدد مفهوم الاستبعاد، وهل يعدُّ المقصود منه الاستبعاد الكلي أم الاستبعاد الجزئي؟ فالأمر في بداية المقام بحاجة إلى بيان في هذا الصدد، وهذا ما سنعرض له.

نرى - في هذا المقام - أنَّ الأدلة الرقمية قد تكون أكثر من دليل، وفي حالة ذلك قد يتمُّ العبث ببعض هذه الأدلة دون البعض الآخر، وعليه يكون استبعاد هذه الأدلة جملة واحدة، أمراً نراه غير مرغوب فيه، ففي هذه الحالة يكون الاستبعاد جزئياً، ونقصد من هذا القول بأنَّ الاستبعاد يشمل الأدلة التالفة، ويمكنها تصوير هذا الفرض بجسد الإنسان، إذ يتمُّ بتر العضو التالف على الرَّغم من

أن هذه الحالة تعدُّ صورةً من صور القياس مع الفارق، أمّا إذا كان الدليل الرقمي الذي تقوم عليه الجريمة يعدُّ دليلاً واحداً في هذا الصدد فإنَّ العبث به يُؤدّي إلى استبعاده تماماً، فلا جدوى من دليل فقد قيمته، ويأخذ حكم الدليل الرقمي المعبوث به أو محل التلاعب ذات قيمة الأدلة التي أخفيت من مسرح الجريمة، وهذا يعدُّ مناطاً للتفرقة بين الوجود والعدم، فالأدلة المتلاعب بها، وكذلك المفقودة، نراها كالعدم لا يُمكن أن تُبنى عليها حجة.

ولكن يثور التساؤل، هل يُمكن التعويل على أدلة رقمية تمَّ العبث بها أو التلاعب بها، وهل من الممكن التعويل على ذلك دون قصد؟ في هذا المقام يتعيّن القول بدايةً: إنَّ الخطأ من قِبَل السلطات المعنية على أمر تقدير الأدلة أمرٌ نراه غير مقبول، إذ نُعده في هذا الخصوص بمثابة خطأ جسيم قد لا يُغتفر لا سيما وأنَّ الجهل بقواعد القانون الجزائي أمرٌ كذلك غير مقبول، فتقدير الأدلة الرقمية يعدُّ بمثابة قاعدة جزائية يتعيّن أن تقوم على أسسٍ مُنضبطة، وألا تكون واعيةً بغير حجة (العتيبي، 2020م، ص 24 وما بعدها).

وإلى جانب التساؤلات المُتقدّمة يثور تساؤل آخر في هذا المقام، ألا وهو: هل الاستبعادُ بحاجةٍ إلى تقديم طلب؟ أم أنَّ السلطات المعنية لها استبعادُ هذه الأدلة الرقمية محل التلاعب من ذاتها دون طلب؟ في هذا المقام نفرّق بين فرضين:

- **الفرض الأول:** سلطة الدفاع أو صاحب المصلحة في دحض الدليل الرقمي بالنظر إلى أنه لا يستقيم وقواعد العدالة والمشروعية الجنائية، فلا مانع من تقديم هذا الطلب، لا سيما في الحالات التي لم يكشف عنها أهل الخبرة التقنية أنَّ هذه الأدلة الرقمية تمَّ العبث بها.
- **الفرض الثاني:** أنَّ السلطات العامة المعنية يُمكنها من تلقاء نفسها دَرء الدليل الرقمي محلّ التلاعب من تلقاء نفسها وإبعادها عن الدَّعوى الجزائية: نظراً لارتباط الأمر في نطاق هذه المسألة بالنظام العام، الأمر الذي لا يحقُّ معه الاتفاق على خلافه، مفاد ذلك أنه يعدُّ ارتصاص الأمر في هذا الصدد بالنظام العام راجعاً إلى أنَّ كافة القواعد المتعلقة بالقوانين الجزائية هي محلُّ ارتصاص بالنظام العام، لا سيما إذا تعلّق الأمر بقواعد الأدلة الجنائية والعدالة.

المطلب الثاني

إجراءات التحقيق في جرائم التعدي على الدليل الرقمي

نستعرض في تفصيل المطلب الحالي الاستعانة بالخبرة التقنية (أهل الخبرة)، وذلك في الفرع الأول، ثم نتناول بعد ذلك دور النيابة العامة في تقدير التلاعب والعبث بالدليل الرقمي، وذلك على النحو التالي بيانه.

الفرع الأول

الاستعانة بالخبرة التقنية

المقصود بها: ضرورة الاستعانة بأهل الخبرة التقنية على النحو الذي تتطلبه التحقيقات، لا سيما وأنَّ الأدلة الرقمية في الجرائم الإلكترونية أو المعلوماتية هي بحاجة دائمة لأشخاص تتوافر فيهم هذه الخبرة؛ حتى يتمَّ التمكين من كشف دقائق الأمور لسلطات التحقيق؛ من أجل إتمام أعمالها على أفضل وجه، وفي ذلك نستعرض الأحكام المنظمة للاستعانة بأهل الخبرة التقنية بين كلٍّ من المشرع الاتحادي الإماراتي، ونظيره المصري، وذلك على النحو الآتي:

أولاً: موقف المشرع الإماراتي:

يعدُّ موقف المشرع الاتحادي الإماراتي في هذا الصدد منظوراً إليه من جانب قانون مكافحة الشائعات والجرائم الإلكترونية، لا سيما وأنه هو القانون المنظم لجرائم الدليل الرقمي في البيئة التقنية، لمّا كان ذلك، وكانت الاستعانة بأهل الخبرة التقنية، وهم الخبراء المختصون في المجال التقني؛ فإنَّ الأمر - بطبيعة الحال - يستتبُّ معه الحيلولة والرجوع إلى الأحكام الواردة في ضوء القواعد

العامة، وعلى ضوء ذلك يمكننا التساؤل: هل نظم المشرع الإماراتي كفاءة الاستعانة بالخبرة التقنية في نطاق قانون مكافحة الشائعات والجرائم الإلكترونية من عدمه؟

ندرك من جانبنا؛ أنه بعد الرجوع إلى أحكام قانون مكافحة الشائعات والجرائم الإلكترونية الاتحادي الإماراتي، تبين أن المشرع لم ينظم الأحكام والقواعد المتعلقة بأهل الخبرة التقنية، وهذا أمر نرى أنه قد أغفله، لا سيما وأن الخبرة وأعمالها تم تنظيمها في ضوء القواعد العامة، وقد أكدت على أهميتها المحكمة الاتحادية العليا، إذ قضت هذه الأخيرة بأنه "لمحكمة الموضوع - سواء من تلقاء نفسها أو بناءً على طلب الخصوم - أن تُعَيِّنَ خبيرًا أو أكثر في الدعوى؛ عملاً بالمادة 180 من قانون الإجراءات الجزائية ...". (المحكمة الاتحادية العليا الإماراتية، الطعن رقم 104 لسنة 23 قضائية).

ثانيًا: موقف المشرع المصري:

في هذا المقام تجدر الإشارة إلى أن موقف المشرع المصري جاء أكثر إلمامًا وتنظيمًا لأعمال الخبرة التقنية، إذ جاء مُتفادياً ما أغفله المشرع الإماراتي في هذا الصدد، لذلك يتعين إعمال المعالجة اللازمة من قبل المشرع الإماراتي؛ لسدّ النقص والخلل الذي أصاب قانون مكافحة الشائعات والجرائم الإلكترونية، وإزاء ما تقدّم نعرض موقف المشرع المصري في تنظيم الاستعانة بالخبرة التقنية، في نطاق قانون مكافحة جرائم تقنية المعلومات بصدد الخبرة التقنية، وبالرجوع إلى أحكام هذا القانون، نجد المادة (10) منه نصت على أنه "ينشأ بالجهاز سجلان لقيد الخبراء، يُقَيَّدُ بأولهما الفنيون والتقنيون العاملون بالجهاز، ويُقَيَّدُ بالآخر الخبراء من الفنيين والتقنيين من غير العاملين به. وتطبق على الخبراء في ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء. واستثناءً من تلك القواعد، تسري على الخبراء المُقَيَّدِينَ بالسجل الثاني القواعد والأحكام الخاصة بالمسألة الإدارية والتأديبية الواردة بالقانون المنظم لعملهم إن وُجد. وتُحدّد اللائحة التنفيذية لهذا القانون قواعد وشروط وإجراءات القيد في كلٍّ من السجلين".

ثالثًا: موقف المشرع الفرنسي:

لا نرى ثمة إشكالية في هذا المقام إزاء اعتراف المشرع الفرنسي بمسائل الخبرة التقنية، وإذا كان الخبير التقليدي في النظام الفرنسي معمولًا به مُحَقَّقًا جدواه في ضوء القواعد العامة، فإن الخبير التقني بات معمولًا به أيضًا لا سيما بعد إقرار المشرع الفرنسي لقانون حماية البيانات الشخصية [CHASSIGNEUX, 2001, P5 et es]، وكذلك قانون تكنولوجيا المعلومات والبيانات والحريات [loi n° 78-17 du 6 janvier 1978].

وعلى ضوء ما سبق نخلص إلى الواجبات المتعين على الخبير الإلكتروني/ التقني إتباعها، ثم نعرض للقواعد الفنية التي تحكم طبيعة عمله التقني، وذلك على النحو الآتي:

أولًا: واجبات الخبير الإلكتروني:

يمكن بيان هذه الواجبات من الناحية القانونية وفق ما يلي (المعمرى، ص 228-229):

1- أداء اليمين:

إن من أهم الواجبات القانونية التي تقع على الخبير الإلكتروني هي أداء اليمين، فقد أوجب المشرع عليه أداء اليمين قبل أداء أعماله، وإلا اعتبر ما يقوم به باطلاً، إلا أن المشرع الإماراتي لم يتطلب حلف اليمين إلا إذا كان الخبير غير مُقَيَّدٍ اسمه في الجداول؛ عملاً بما نصت عليه المادة (97) من قانون الإجراءات الجزائية الاتحادي الإماراتي بنصها على أنه "إذا كان الخبير غير مُقَيَّدٍ اسمه في الجدول وجب أن يحلف أمام عضو النيابة العامة يميناً بأن يؤدي عمله بالصدق والأمانة".

2- أن يؤدي الخبير أعماله ومهامه بنفسه:

وذلك وفق حدود القانون ووفق حدود الأمر الذي يصدرُ بنذبه للقيام بأعمال الخبرة، فعليه القيام بعمله وفق ما يُحدّد له في أمر النّدب من الأعمال المطلوب منه إبداء رأيه الفنيّ فيها دون الدخول في وقائع أخرى خارج نطاق الأمر الصّادر.

3- خضوع الخبير الإلكتروني لرقابة وإشراف عضو سلطة التحقيق أو مأمور الضبط القضائي:

على الخبير أن يبقى على اتّصالٍ دائمٍ مع عضو سلطة التحقيق أو مأمور الضبط القضائي، ويخضع لتوجيهه من أجل إحاطته بالتطوّرات والأعمال التي يقومُ بها، فهو مُساعد فنيّ له.

4- الاستعانة بأطراف الخصومة والسّماع إلى أقوالهم وما يُقدّمون من طلباتٍ كإجراء أبحاثٍ مُعيّنة أو سماع شهود.

5- تقديم تقريرٍ فنيّ بعد انتهاء أعمال الخبرة:

وذلك وفق الوقت المُحدّد في أمر النّدب، ويحقُّ استبداله إذا لم يقم بتقديم تقريره في الوقت المُحدّد، مع إلزامه برّد جميع الأشياء والأوراق والوثائق التي تكون قد مُنحت إليه بمُوجب أمر النّدب.

ثانياً: القواعدُ الفنيّةُ التي تحكم عمل الخبير الإلكتروني:

تتعدّد القواعدُ الفنيّةُ التي تحكم عمل الخبير الإلكتروني، ونعرضُ منها الآتي (المعمرى، ص 229 وما بعدها):

1- الإمام بوصف وتركيب وصناعة الجهاز الإلكتروني وطرازه ونوع نظام التّشغيل الذي يعملُ عليه، وأهمّ الأنظمة والبرامج الفرعيّة التي تُستخدم بالجهاز، والأجهزة والنهايات الطرفيّة المُلحقة بها، إضافةً لكلمات المرور والسرّ لنظام التّشفير وغيرها من الأمور المُماثلة.

2- الإمام بوصف الموضوع المُحتمل لأدلة الإثبات الماديّة والمعنويّة وشكلها ونوعها والهيئة التي تكونُ عليها.

3- الإمام بوصف طبيعة بيئة الجهاز الإلكتروني وشبكاته، من حيث تنظيمها ومُدّة تركيز وعمل المُعالجة الآليّة، ونمط وسائل الاتّصالات وتردّدات موجات البثّ وأماكن تخزينها.

4- التمكن من نقل أدلة الإثبات غير المرنّية وتحويلها إلى أدلةٍ مرنّيةٍ مقروءة، بحيث يُتاح لمأمور الضبط القضائيّ أو عضو سلطة التحقيق الاطّلاعُ عليها وفهمها، مع إثبات أن الدليل مُطابقٌ لصورته غير المرنّية.

5- عزّل النظام المعلوماتيّ دون إتلافٍ للأدلة أو تدميرها أو إلحاق الضّرر بالجهاز، وبيان كيفية إجراء ذلك.

6- نقل أدلة الإثبات إلى أوعيةٍ ووسائطٍ تقنيّةٍ مُلائمةٍ دون أن يلحقها تلفٌ أو تغييرٌ، وبيان طريقة إجراء ذلك (رستم، 1994م، ص 142-143).

ويتجهُ جانبٌ من الفقه في هذا المقام إلى أن القيام بعملية تجميع الأدلة الرقمية في الجريمة الإلكترونيّة من خلال شبكة الإنترنت تتمُّ عبر ثلاث مراحلٍ رئيسيّةٍ (حنفي، ص 69-70)، وهي:

المرحلة الأولى: تجميع المعلومات المُخزّنة لدى طرفٍ مُقدّم خدمة الاتّصال والوصول إلى شبكة المعلومات، من خلال تتبّع الخوادم التي دخلَ الفاعلُ منها، ومُحاولة إيجاد أي أثرٍ إلكترونيّ له.

المرحلة الثانية: وهي مرحلة المراقبة، وتقومُ على فرضيّة أن الفاعل لا بدّ من أن يعودَ لمسرح جريمته سواءً بالدخول إليه مرّةً أخرى أو بمُشاهدته والاطّلاع عليه عن قُرب، وتتعدّد طرقُ مراقبة هذه الأجهزة وتنوّعٌ وفق ما تُنتجه التقنيّة من تحديثاتٍ وبرامجٍ خاصّةٍ لهذه المراقبة.

المرحلة الثالثة: وهي مرحلة ضبط الأجهزة المُشتبه بها وفحصها فحصاً فنياً وقانونياً، ويبدأ في هذه المرحلة عملُ الخبير الإلكترونيّ في فحص نظام الجهاز المُشتبه فيه بجميع مُكوّناته الماديّة والمعنويّة والشبكيّة؛ من أجل استخراج دليل أدائه الفاعل وتحديد مدى قدرة الأدلة على ذلك، أو الوصول إلى براءة النظام والأجهزة المُشتبه بها من استخدامها في الجريمة.

الفرع الثاني

دور النيابة العامّة في تقدير التلاعب والعبث بالدليل الرقميّ

قبل الحديث عن الدور الذي تتولاه النيابة العامة في هذا الشأن يتعين النظر إلى بيان ماهيتها وخصائصها في هذا الصدد، ثم الإجابة عن التساؤل الجوهرى المتعلق بمدى وجود نيابة عامة معلوماتية مختصة ومختصة في هذا الصدد؟
تتسم النيابة العامة بوصفها جهازاً من أجهزة الدولة بعدة خصائص تميزها عن غيرها من أجهزة الدولة وتحكم تصرفاتها بوجه عام. وهذه الخصائص هي (سرور، 2016م، ص 260 وما بعدها)، (بهنام، 1977م، ص 195 وما بعدها).

1- مبدأ استقلال النيابة العامة.

2- مبدأ التبعية التدريجية.

3- مبدأ عدم تجزئة النيابة العامة.

4- عدم مسئولية النيابة العامة.

أما بصدد الحديث عن دور النيابة العامة في تقدير التلاعب والعبث بالدليل الرقعى، فنقسم هذا الحديث إلى جانبين، بحيث نعرض في الجانب الأول لموقف المشرع الإماراتي، ثم نعرض لموقف المشرع المصري، وذلك على النحو الآتي:
أولاً: موقف المشرع الإماراتي:

في هذا المقام نقصد موقف المشرع الاتحادي الإماراتي من تنظيم الدور الذي تتولاه النيابة العامة بصدد تقدير التلاعب والعبث بالأدلة الرقمية، والتساؤل: هل نظم المشرع هذا الدور أو لا؟ وهذا ما نود تفصيله من خلال الرجوع إلى نصوص قانون مكافحة الشائعات والجرائم الإلكترونية.

وبالرجوع إلى هذه الأخيرة نرى أن المشرع الإماراتي تناول في إطلالة بسيطة سلطة النيابة العامة في كونها لها إتخاذ ما تراه مناسباً بشأن الدعوى الجزائية في نطاق هذا القانون، وذلك على النحو الذي نظمته المادة (62) في فقرتها الأخيرة من قانون مكافحة الشائعات والجرائم الإلكترونية.

لذلك؛ وإن كان المشرع لم يعرض للدور الذي تتولاه النيابة العامة في تقدير التلاعب والعبث بالدليل الرقعى، يمكننا القول: إن النيابة العامة وما لها من سلطة التحقيق والادعاء وتقدير ما يعرض عليها في نطاق التحقيقات تحت رقابة محكمة الموضوع، يمكنها التعويل على الأدلة المقدمة إليها عدمه، لا سيما وأن العبث بالدليل الرقعى والتلاعب به يفقده جوهريته، وبالتالي فلا جدوى منه، مفاد ذلك أن النيابة العامة وكونها ممثلة للادعاء في الدعوى الجزائية يمكنها تقييم العبث والتلاعب الحاصل بصدد الأدلة الرقمية، باعتبارها السلطة المعنية بإجراءات التحقيق، إلا أن ذلك في الوقت ذاته لا يحول وسلطتها في الاستعانة بالخبراء التقنيين إذا لزم الأمر ذلك.

ثانياً: موقف المشرع المصري:

لم يعرض المشرع المصري في نطاق قانون مكافحة جرائم تقنية المعلومات ما إذا كانت النيابة العامة تملك في هذا المقام سلطات واسعة بصدد تقدير العبث أو التلاعب بالأدلة الرقمية، إلا أن ذلك لا يحول - بطبيعة الحال - أن تتخذ النيابة العامة وفي نطاق سلطة ورقابة محكمة الموضوع عليها ما نشاء من قرارات بصدد الدليل الرقعى، لا سيما إذا كشفت لها التحقيقات أن هذه الأدلة تم العبث والتلاعب بها.

ونخلص مما تقدم إلى أنه كان من الأجدر على المشرع، سواء الاتحادي الإماراتي أو نظيره المصري، أن ينص على الدور الجوهرى الذي يمكن للنيابة العامة أن تتولاه بصدد مسألة التلاعب أو العبث بالأدلة الرقمية، لا سيما وأن الأمر بحاجة إلى إيضاح؛ نظراً لأن مسألة التقدير في هذا الصدد تعد ذات طابع فني؛ أي إن النيابة بحاجة إلى أهل الخبرة للاستعانة بهم لتقدير الأمور.
أما بصدد الإجابة عن التساؤل الذي طرحناه في الأعلى فيمكننا القول: إنه لا توجد نيابة تقنية أو معلوماتية؛ نظراً لأن الهدف من عمل النيابة العامة يتجسد في وجود بعض الوظائف المعاونة لها، كما هو الحال بصدد الخبراء على النحو الذي أسلفناه، لذلك

فلا داعي أن تُفَرَّغَ نفسها من مهامها الأعلى والأقيم إلى أن تبحث مسألة التقنية حتى ولو كان الواقع التقني المعول عليه في البيئة الرقمية يتطلب ذلك.

ثالثاً: موقف المشرع الفرنسي:

تعد النيابة العامة هي الجهة المعنية بمباشرة التحقيقات، مثلها في هذا المقام مثل المشرع المصري، ولا يمكن الخروج عن هذا الأصل طالما أن قانوناً خاصاً لم يُعَيَّنْ جهةً بعينها بمباشرة هذا العمل، وذلك على النحو الذي أسلفناه.

الخاتمة:

للمحماية الجزائية الإجرائية طابع ملموس، لا سيما أهمية الشكل، وفي هذا النطاق وبصدد حماية الدليل الرقمي حماية إجرائية لها طابعها الجزائي، قسّمنا دراستنا إلى مبحثين، استعرضنا في المبحث الأول الحديث عن الأحكام الإجرائية لاستخلاص الدليل الرقمي، أما المبحث الثاني فعرضنا بصدد الحديث عن التحقيق في جرائم التعدي على هذا الدليل، وفي ضوء إعمال المنهج التحليلي المقارن توصلنا إلى عددٍ من النتائج والتوصيات، نعرض لها على النحو الآتي:

أولاً- النتائج:

- 1- جاء قانون مكافحة الشائعات والجرائم الإلكترونية خالياً من تنظيم مسألة التفتيش في البيئة الرقمية؛ باعتباره من قبيل الإجراءات التقليدية المعول عليها في الحصول على الدليل الرقمي، وذلك على خلاف ما هو معول عليه من قبل المشرع المصري.
- 2- لم يُنظَم المشرع الاتحادي الإماراتي في قانون مكافحة الشائعات والجرائم الإلكترونية مسألة إجراءات الضبط باعتبارها إحدى الطرق التي من شأنها التحصل على الدليل الرقمي بالشكل المشروع، وهو في ذلك يُخالف - وبصورة قاطعة - ما عول عليه المشرع المصري في هذا الخصوص.
- 3- جاء قانون الإجراءات الجزائية الاتحادي الإماراتي خالياً من نص قانوني يؤكد سلطة القاضي الجزائي تجاه الأدلة بوجه عامٍ واتّباعه في ذلك منهج الإثبات الحر.
- 4- جاء قانون مكافحة الشائعات والجرائم الإلكترونية الاتحادي الإماراتي خالياً من النص على تنظيم قواعد وأحكام العمل بالخبرة التقنية؛ أي إن أهل الخبرة التقنية لم يلقوا الاهتمام الكافي من جانب المشرع في إطار القانون المتقدم، وذلك على خلاف ما هو عليه الحال بصدد التشريع المصري.
- 5- جاء قانون مكافحة الشائعات والجرائم الإلكترونية الاتحادي خالياً من النص على دور النيابة العامة في تقدير الأدلة الرقمية إذا ما تمّ العبث أو التلاعب بها.

ثانياً- التوصيات:

- 1- نقترح على المشرع الاتحادي الإماراتي تنظيم نص خاص يُنظَم مسألة التفتيش في البيئة الرقمية كما فعل نظيره المصري، وذلك من خلال تعديل قانون مكافحة الشائعات والجرائم الإلكترونية باعتباره القانون ذا الصلة بالأدلة الرقمية.
- 2- نقترح على المشرع الاتحادي الإماراتي تعديل قانون مكافحة الشائعات والجرائم الإلكترونية، وذلك عن طريق إضافة نص قانوني مُستحدث يتضمّن تنظيم إجراءات الضبط؛ كونها طريقاً للحصول على الدليل الرقمي بصورة مشروعة، ولكن في نطاق ووفق طبيعة البيئة الرقمية.
- 3- نقترح على المشرع الاتحادي الإماراتي تعديل قانون الإجراءات الجزائية وإضافة نص قانوني يؤكد سلطة القاضي التقديرية تجاه الأدلة بصفة عامة وإعمالها لدوره في ظلّ نظام الإثبات الجزائي الحر.
- 4- نقترح على المشرع الاتحادي الإماراتي تعديل قانون مكافحة الشائعات والجرائم الإلكترونية وإدراج نص يتضمّن أهل الخبرة التقنية، وذلك كما فعل نظيره المصري في المادة (10) من قانون مكافحة جرائم تقنية المعلومات.

5- نقتزح على المُشَرِّع الاتِّحاديّ الإماراتيّ النصَّ بصورة واضحة على الدور المهمّ الذي تتولاه النيابة العامّة بصدد تقدير مسألة العبث أو التلاعب بالدليل الرقعيّ، وذلك من خلال تعديل قانون مكافحة الشائعات والجرائم الإلكترونيّة. قائمة المراجع أولاً- الكتب القانونيّة:

- (1) أبو عامر، محمد زكي [٢٠١٠م]، الإجراءات الجنائيّة، دار الجامعة الجديدة.
- (2) بهنام، رمسيس [١٩٧٧م]، الإجراءات الجنائيّة تأصيلًا وتحليلًا، منشأة المعارف.
- (3) حسين، سامي جلال فقي [٢٠١١م]، التفتيش في الجرائم المعلوماتيّة: دراسة تحليليّة، دار الكتب القانونيّة ودار شتات للنشر والبرمجيات.
- (4) حنفي، حازم محمد [٢٠١٧م]، الدليل الإلكتروني ودوره في المجال الجنائيّ، دار النهضة العربيّة.
- (5) رستم، هشام فريد [١٩٩٤م]، الجوانب الإجرائيّة للجرائم المعلوماتيّة، دار النهضة العربيّة.
- (6) سرور، أحمد فتحي [٢٠١٦م] الوسيط في قانون الإجراءات الجنائيّة، ط10، دار النهضة العربيّة.
- (7) عبد الله، هلاي [2008م]، تفتيش نظم الحاسب الآليّ وضمانات المتهم المعلوماتيّة: دراسة مقارنة، دار النهضة العربيّة.
- (8) عمر، رشاد خالد [٢٠١٣م]، المشاكل القانونيّة والفنيّة للتحقيق في الجرائم المعلوماتيّة: دراسة تحليليّة مقارنة، المكتب الجامعي الحديث.
- (9) قارة، عائشة بن [٢٠١٠م]، حجّة الدليل الإلكترونيّ في مجال الإثبات الجنائيّ، دار الجامعة الجديدة.
- (10) المرصفاوي، حسن صادق [١٩٩٨م]، المرصفاوي في أصول الإجراءات الجنائيّة، منشأة المعارف.
- (11) هروال، نبيلة هبة [٢٠١٣م]، الجوانب الإجرائيّة لجرائم الإنترنت في مرحلة جمع الاستدلالات: دراسة مقارنة، دار الفكر الجامعي.

ثانيًا- الأبحاث العلميّة والمقالات:

- (1) العتيبي، زياد بن محمد هادي [٢٠٢٠م]، دراسة استطلاعيّة حول حجّة الأدلة الرقمية في إثبات الجرائم المعلوماتيّة، المجلة الإلكترونيّة الشاملة متعدّدة التخصصات، العدد [29].
- (2) المعمري، مسعود بن حميد [٢٠١٨م]، الدليل الإلكتروني لإثبات الجريمة الإلكترونيّة، مجلة القانون الكويتيّة العالميّة، ملحق خاص، العدد [٣]، الجزء الثاني.

ثالثًا- الأحكام القضائيّة:

- (1) أحكام القضاء الاتِّحادي الإماراتي [المحكمة الاتِّحادية العليا]:
 - الطعن رقم ٢٨٧ لسنة ٢٧ قضائيّة، الأحكام الجزائيّة، بتاريخ 2006/10/16م.
 - الطعن رقم ٣٧ لسنة ٢٠١٩ قضائيّة، الأحكام الجزائيّة، بتاريخ 2019/10/21م.
 - الطعن رقم ٤٦٠ لسنة ٢٠١٤ قضائيّة، الأحكام الجزائيّة، بتاريخ 2015/1/20م.
 - الطعن رقم 10 لسنة ٢٣ قضائيّة، الأحكام الجزائيّة، بتاريخ 2001/5/21م، مكتب في [23]، الجزء [١]، ص [٣٤٧].
 - الطعن رقم ١٠٤ لسنة ٢٣ قضائيّة، الأحكام الجزائيّة، بتاريخ 2002/2/2م، مكتب في [24]، الجزء [١]، ص [١٣٨].
- (2) أحكام القضاء المصريّ [محكمة النقض]:
 - الطعن رقم ٣٥٣٦ لسنة ٥٢ قضائيّة، الدوائر الجنائيّة، بتاريخ 1982/12/8م، مكتب في [33] - الجزء [١]، ص [٩٦٢].
 - الطعن رقم ١١١٥٥ لسنة ٨٣ قضائيّة، الدوائر الجنائيّة، بتاريخ 2016/2/25م، مكتب في [٦]، ص [٢٦٧].

رابعاً- القوانين:

(1) القوانين الإماراتية:

- المرسوم بقانون اتّحادي رقم [٣٤] لسنة ٢٠٢١ م بشأن مكافحة الشائعات والجرائم الإلكترونية.
- قانون الإجراءات الجزائية الاتّحادي.

(2) القوانين المصرية:

- قانون مكافحة جرائم تقنية المعلومات رقم [١٧٥] لسنة ٢٠١٨ م.
- قانون الإجراءات الجنائية.

خامساً- المراجع الفرنسية:

Jacques": Les Crimes informatiques d'autres Crimes dans Le domaine de la technologie [ran Cillon]"-

informatiqueen France . R. I.D.P. 1993 . P. 309.

2, ° CYNTHIA (CHASSIGNEUX) , la protection des donnees personnelles en france , lex Electronica , vol.6 , n - Hiver/ winter 2001 .

سادساً- القوانين الفرنسية:

1. قانون الإجراءات الجنائية.
2. قانون الأمن الداخلي.
3. قانون حماية البيانات الشخصية الفرنسي.
4. قانون تكنولوجيا المعلومات والبيانات والحريات.

Kaymt elmarageea

Awln elkotop:

- 1- hanafe, hazem Mohamed (2017) , aldalel elelkrone we dawroh fe elmagal elgenae, dar elnahda elarabia.
- 2- Omar , rashad khaled (2013) , elmashakel elqanonia we alfania lltahqeq fe elgaraemelmalomatia:drasa tahlelia moqarna,elmaktab elgamee elhades.
- 3- abo amer, mohamed zaki (2010) , elegraat elgenaea, dar elgamaa elgdeda.
- 4- hrwal,nabila (2013) , algawanb elegraea lgaraym elenternt fe marhlet gamea elestdlalat: drasa moqarna, dar elfkr elgamee .
- 5- hussin, sami galal feke (2011) , eltaftesh fe elgaraym elmalomatia: drasa tahlelia, dar elkotop elqanonia , we dar shtat llnashr we elparmagiat .
- 6- almarsafawe , hassan sadeq (1998) , almarsafawe fe osol elegraat algebra ' monshaet elmaaref .
- 7- qara, aisha bn (2010) , hoget eldalel elelkrone fe magal elesbat elgenae, dar elgamaa elgdeda .
- 8- rostom hesham farid (1994) , algawanb elegraea lgaraym elmalomatia , dar elnahda elarabia .
- 9- srer, ahmed fathi (2016) , elwaset fe qanon elegraat elgenaia , t 10 , dar elnahda elarabia .
- 10 - bahnam , ramsis (1977) , elegraat elgenaia taseln we tahleln , monshaet elmaaref.
- 11-Abdelah, helale [2008], Tartesh Nozm elhaseb elale we damanat elmotaham el malomate: drasa moqarnas 42 dar elnahda elarabia.

Sanian: elabhas Elelmea we elmaqalat:

- 1- almemare, mswood bn hmed (2018) , aldalel elelektroni lesbat algaraym elelektronia , maglet elqanon elkwetia elalamia, molhaq khas, add (3) , gozea (2) .
- 2- aletabe, ziad bn mohamed hade (2020) , drasa estetlaea haol hoget aladela alraqmia fe esbat alargaem almalomatia , almagla alelektroina alshamla motaddt altakhsosat , add (29) .

Salthn: alahkam elqdaea:

1- ahkam elqdaa elethade elemarate (elmahkma elethadia elolia)

- altaan rkm 287 lsnt 27 qdaaea, elahkam elgazaea, btarekh 16/10/2006 .
- Altaan rkm 37 lsnt 2019 qdaaea, elahkam elgazaea, btarekh 21/10/2019 .
- Altaan rkm 460 lsnt 2014 qdaaea, elahkam elgazaea , btarekh 20/1/2015 .
- Altaan rkm 10 lsnt 23 qdaaea , elahkam elgazaea, btarekh 21/5/2001 , maktab fne (23) , gozea (1) , sad (347) .
- Altaan rkm 104 lsnt 23 qdaaea. elahkam elgazaea , btarekh 2/2/2002 , mktab fne (24) , gozea (1) , sad (138) .

2- ahkam elqadaa elmasry (mahkmet elnaqd):

- altaan rkm 3536 lsnt 52 qdaaea , eldawaer elgenaya , btaerh 8/12/1982 , mktab fne (33) , gozea (1) , sad (962) .
- altaan rkm 11155 lsnt 83 qdaaea , eldawaer elgenaya, btarekh 25/2/2016 .

Rabeen: alqwanen:

1- alqwanen alemaratia:

- marsom beqanon etahade rkm (34) lsnt 2021 bshaan mokafhet elshaeaat we elgaraym elelektronia .
- Qanon elegraat elgazaea eletahade.

2- alqwanen almasrea:

- qanon mokafhet garaym tqnet elmalomat rkm (175) lsnt 2018 .
- Qanon elegraat elgenaya .

Khamasn: Al marageaa elfrnsia:

-[ran Cillon]" Jacques": Les Crimes informatiques d'autres Crimes dans Le domaine de la technologie informatiqueen France . R. I.D.P. 1993 . P. 309.

Sadesn: AL qawanen elfrnsia:

- qanon elegraat elgenaea.
- qanon elamn eldakhle.
- qanon hemaye elpyanat elshakhsea .
- qanin tekmlagea elmalomat we elbayanat we elhoreat .