جامعة الشرقية
A' SHARQIYAH UNIVERSITY

كلية الحقوق

قسم القانون العام

إجراءات التحقيق الابتدائي والمحاكمة في الجرائم الإلكترونية وفق التشريع العُماني
(دراسة قانونية تحليلية)

إعداد الباحث

سلطان بن أحمد بن علي الحارثي

رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام

تخصص: القانون الجزائي

إشراف

الدكتور/ أحمد بن صالح البرواني

لجنة المناقشة:

اسم عضو اللجنة	رتبته الأكاديمية - جهة العمل	الصفة
د. أحمد بن صالح البرواني	أستاذ مساعد - جامعة الشرقية	مشرفًا ورئيسًا
د. نزار حمدي قشطة	أستاذ مشارك - جامعة الشرقية	مناقشًا داخليًا
د. تامر حامد جابر القاضي	أستاذ مشارك - جامعة الأقصى	مناقشًا خارجيًا

سلطنة عُمان

2025م / 1446هـ

قرار لجنة المناقشة بإجازة الرسالة

اجراءات التحقيق والمحاكمة في الجرائم الاليكترونية وفق التشريع العماني

(دراسة قانونية تحليلية)

إعداد الباحث: سلطان بن احمد بن علي الحارثي

الرقم الجامعي:**2212404**

نوقشت هذه الرسالة وأجيزت بتاريخ 30 جمادى الأولى 1446هـ

الموافق 2 ديسمبر 2024م

المشرف

د. احمد بن صالح البرواني

أعضاء لجنة المناقشة

م	صفته في اللجنة	الاسم	الرتبة الأكاديمية	التخصص	الكلية/ المؤسسة	التوقيع
1	رئيس اللجنة	د. أحمد بن صالح البرواني	أستاذ مساعد	القانون الجزائي	كلية الحقوق جامعة الشرقية	
2	المناقش الخارجي	د. تامر حامد جابر القاضي	أستاذ مشارك	القانون الجزائي	كلية الحقوق جامعة الأقصى	الدكتور تامر حامد القاضي
3	المناقش الداخلي	د. نزار حمدي قشطه	أستاذ مشارك	القانون الجزائي	كلية الحقوق جامعة الشرقية	

إقـــــرار الباحـــــث

الإقـــــرار

أقـر بـأن المـادة العلميـة الـواردة فـي هـذه الرسـالة تـم تحديـد مصـدرها العلمـي، وأن محتـوى الرسـالة غيـر مقـدم للحصـول علـى أي درجـة علميـة أخـرى، وأن مضـمون هـذه الرسـالة يعكـس آراء الباحـث الخاصـة، وهـي ليسـت بالضـرورة الآراء التي تتبناها الجهة المانحة.

الباحث: سلطـان بـن أحمـد بـن علـي الحارثـي الرقم الجامعي: 2212404

التوقيع:

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

قَالَ تَعَالَىٰ:

﴿ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُوٓاْ إِن جَآءَكُمْ فَاسِقُۢ بِنَبَإٖ فَتَبَيَّنُوٓاْ أَن تُصِيبُواْ قَوْمَۢا

بِجَهَٰلَةٖ فَتُصْبِحُواْ عَلَىٰ مَا فَعَلْتُمْ نَٰدِمِينَ ﴾

صَدَقَ اللهُ العَظِيمُ

سـورة الحجرات الآية: 6

إهداء

إلى والديّ العزيزين، الذَيّنِ منحهما الله القوة والحكمة ليكونا سندا وملاذًا لي طوال رحلتي

إلى زوجتي الحبيبة، رفيقة الدرب وصاحبة الصبر والدعم الذي لا ينضب

إلى أبنائي الأعزاء الذين هم مصدر إلهامي وسبب طموحي المستمر

إلى كل من ساهم في هذا العمل، بجهد أو فكرة أو دعم

أهديكم هذا العمل تقديرًا ومحبة فأنتم القوة التي تدفعني دائما نحو الأفضل.

الباحث

أتقدم بخالص الشكر والتقدير إلى الدكتور أحمد بن صالح البرواني لتفضله بقبول الإشراف على رسالتي، والذي كان له الفضل الكبير في توجيهي ودعمي خلال هذه الرحلة العلمية.

كما أعبر عن أمتناني لجميع الأساتذة الكرام الذين كانوا سندًا وداعمين لي في مسيرتي التعليمية.

ولزملائي الأعزاء الذين شاركوني هذه الرحلة وساهموا في إلهامي ودعمي.

وفي الختام أوجه شكري وتقديري العميق لكلية الحقوق في جامعة الشرقية التي وفرت لي بيئة علمية متميزة ساعدتني في تحقيق أهدافي.

الباحث

إجراءات التحقيق الابتدائي والمحاكمة في الجرائم الإلكترونية وفق التشريع العُماني (دراسة قانونية تحليلية)

إعداد: سلطان بن أحمد بن علي الحارثي

إشراف: الدكتور أحمد بن صالح البرواني

الملخص

تواجه سلطات إنفاذ القانون في جميع أنحاء العالم بما في ذلك سلطنة عُمان، تحديات متزايدة في التصدي للجرائم الإلكترونية التي تتسم بسرعة تطورها وتعقيدها المستمر، مما يتطلب استجابة قانونية فعالة تواكب هذا التطور وتكافح الجرائم الناشئة عنه. ومن هنا تأتي أهمية هذه الدراسة التي تهدف إلى تطوير الإطار القانوني الإجرائي في سلطنة عُمان لمواجهة الجرائم الإلكترونية بفعالية، في ظل تزايد استخدام التكنولوجيا الرقمية والإنترنت، وسد الفجوات القانونية القائمة، وتقديم توصيات عملية للتعامل القانوني مع هذه الجرائم.

سعت الدراسة إلى تحليل النص الإجرائي الجزائي المتعلق بالجريمة الإلكترونية وتقييم مدى كفايته للتصدي لهذه الجرائم، حيث ركزت الإشكالية الرئيسية على مدى قدرة التشريع العُماني على مواكبة التطورات السريعة في الجرائم الإلكترونية ومدى تناسب الإجراءات القانونية الحالية للتصدي لها، إضافةً إلى التحديات الموضوعية والإجرائية المصاحبة لهذا التطور، مع تقديم مجموعة من التوصيات لتعزيز فعاليتها وتحسين قدرتها على التصدي لهذه الجرائم بفاعلية أكبر.

اعتمدت الدراسة على المنهج التحليلي القانوني من خلال تحليل النصوص والقواعد القانونية ذات الصلة، وخلصت إلى أن التشريعات الجزائية العُمانية بحاجة إلى تحديث شامل ومتكامل بين القوانين المختلفة لتوفير حماية قانونية شاملة وفعالة ضد الجرائم الإلكترونية، وأوصت بضرورة إصدار قانون خاص بالإجراءات الجزائية لمواجهة الجرائم الإلكترونية.

الكلمات المفتاحية: الجرائم الإلكترونية – الجرائم السيبرانية – التحقيق والمحاكمة، الإجراءات الجزائية، الأدلة الإلكترونية، التعاون القضائي الدولي، الخبرة الفنية.

Abstract

In many parts of the world, including the Sultanate of Oman, the challenges in enforcing laws in various areas have become prominent, especially with the increasing prevalence of electronic crimes that evolve continuously in terms of deception and sophistication. This requires an effective legal response that can keep pace with these developments and combat emerging crimes. This study focuses on the Sultanate of Oman efforts to develop a legal framework for electronic crimes, addressing the growing use of digital technology and the internet, while presenting legal gaps and practical recommendations to aid in the legal handling of these crimes.

The study aims to analyze and assess the effectiveness of current legal responses to electronic crimes, examining the extent to which these responses meet the growing needs for combating these offenses. The main issue highlighted is the extent of the authorities' ability to keep up with the rapid developments in electronic crimes and the adequacy of legal procedures to monitor these changes, as well as the challenges associated with enhancing the efficiency of these responses.

The study relied on the comparative legal approach by analyzing laws and regulations, concluding that Omani countries need a comprehensive update to their legal frameworks. It found that current procedures lack coordination across different legal entities to achieve an integrated and effective legal approach against electronic crimes. The study recommended issuing a dedicated law for legal procedures aimed at addressing electronic crimes.

Keywords: Electronic crimes - Cybercrimes - Investigation and trial.

مقدمـــــــه

مع انتشار استخدام شبكة الإنترنت في بداياتها، لم يكن هناك قلق بشأن الجرائم الممكنة على الشبكة، نظرًا للقيود الواضحة لاستخدامها، كانت تقتصر أساسًا على الأغراض البحثية والعلمية، وكانت محصورة بشكل رئيسي في فئة محددة من المستخدمين، وهم الباحثون والعلماء وطلاب الجامعات، كما كانت تُدير شبكة الإنترنت أنشطتها في إطار حدود الفضاء الافتراضي، المعروف أيضًا بـ"Cyberspace"، كبيئة خصبة ومهيئة لنقل المعلومات بين المواقع الإلكترونية، التي كانت تقع ضمن الحواسب المنتشرة التابعة للأفراد في القرية الإلكترونية الكونية الجديدة.

وقد تميزت هذه المرحلة بانسيابية تدفق المعلومات عبر الشبكات الحاسوبية العالمية، مما أتاح انتقال البيانات بسلاسة بين المواقع ووثائقها، مع اعتماد بنية تقنية معقدة تضمن تفرعات متعددة وعلاقات ترابطية تعزز التكامل بين المستخدمين. كانت هذه البنية بمثابة نسيج رمزي مترابط، يخدم هدفًا رئيسيًا هو تحقيق أقصى استفادة من موارد الشبكة في بيئة آمنة ومحددة المعالم.

إلا أنه مع بزوغ فجر الثورة المعلوماتية وتوسع استخدام شبكة الإنترنت، ومع بداية دخولها في المعاملات التجارية وانضمام جميع فئات المجتمع إلى مجموعة المستخدمين، بدأت جرائم على الشبكة تظهر بشكل متزايد، متنوعة في أشكالها ومظاهرها، تُعرف هذه الجرائم باسم "الجريمة الإلكترونية"، وهي تشير إلى الجرائم التي يتم ارتكابها عن طريق الكمبيوتر والإنترنت، تعد هذه الظاهرة من بين أهم وأخطر المعوقات التي تواجه المعاملات الإلكترونية في الوقت الحالي.

لهذا أصبح الإنترنت يشكل حاليًا ساحة إجرامية نموذجية تعتبر تحديًا للأجهزة الأمنية والقضائية نظرًا لتواجد ثغرات قانونية وفراغات تشريعية.

ربما يكون التطور المستمر للشبكة المعلوماتية وتوفر السرية التامة هما اللذين جعلا منها وسيلة مثالية لتنفيذ العديد من الجرائم بعيدًا عن رصد الجهات الأمنية، فقد فتحت شبكة الإنترنت أبوابًا واسعة لمافيا الجرائم، مما يمكنها من تنظيم وتنفيذ أنشطتها بكفاءة[1].

---

[1] محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري 175 لسنة 2018. دراسة تحليلية مقارنة، دار الجامعة الجديدة، الإسكندرية، 2019. ص547.

وتُعبِّر دوافع ارتكاب الجريمة الإلكترونية إما عن رغبة في تحقيق الربح المالي، أو عن رغبة في الانتقام من رؤساء العمل أو تكوين ضرر لهم، وقد تنطوي أيضًا على الرغبة في إثبات الذات وإبراز المهارات الفردية والقدرات المعلوماتية والتقنية بهدف التغلب على مُقدِّمي برامج التأمين والحماية، يجدر بالذكر أن المجرم الإلكتروني يتسم بالمعرفة والذكاء، فضلًا عن التخصص والمهارة، إلا أنه يستغل هذه الصفات بشكل غير قانوني، ويمكن لذلك أن يتجاوز في بعض الأحيان حدود التجسس أو يتسبب في أفعال كالقتل أو الإرهاب.

وشبكة المعلومات الدولية عبارة عن أداة للربط والاتصال بين مختلف شعوب العالم، فإذا تم إساءة استخدام هذه الشبكة أو استغلالها بشكل غير مشروع، يؤدي ذلك إلى ظهور طائفة جديدة من الجرائم، وهي الجرائم المعلوماتية.

تتنوع جرائم الحاسوب إلى عدة أنواع رئيسية، منها **الجرائم الاقتصادية** التي تستهدف تحقيق مكاسب مالية غير مشروعة عبر الإنترنت، مثل **الاحتيال الإلكتروني**، حيث يتم خداع الأفراد أو المؤسسات للحصول على أموال بطرق غير قانونية، و**سرقة الهوية الإلكترونية** التي تشمل سرقة معلومات شخصية لاستخدامها في عمليات احتيالية، كما تشمل **القرصنة الإلكترونية** التي تهدف إلى اختراق الأنظمة للحصول على بيانات حساسة أو تدميرها، و**التجارة غير القانونية عبر الإنترنت** التي تشمل بيع وشراء سلع أو خدمات غير قانونية.

أما **الجرائم غير الاقتصادية** فتشمل **الجرائم ضد الخصوصية** مثل التجسس الرقمي، حيث يتم اختراق حسابات الأفراد للوصول إلى معلومات حساسة، و**الابتزاز الإلكتروني** الذي يعتمد على تهديد الضحية بنشر معلومات شخصية في حال عدم دفع أموال، إضافة إلى **التحرش الإلكتروني** الذي يتم عبر الإنترنت، وتشمل هذه الجرائم أيضًا **الجرائم المتعلقة بحقوق الملكية الفكرية** مثل القرصنة على البرمجيات والمحتوى الإعلامي، و**الإرهاب الإلكتروني** الذي يهدف إلى نشر أفكار متطرفة أو تنفيذ هجمات على البنية التحتية الحيوية.

وبناءً على أهمية هذا الموضوع، يظهر بوضوح أن هناك حاجة ملحة للتعمق في دراسته من خلال استكشاف الجوانب الإجرائية والتشغيلية المتعلقة بتحقيق وإثبات جرائم المعلومات، تتمحور هذه الدراسة حول استكشاف المسائل القانونية والتقنية المتعلقة بسلطة مأمور الضبط القضائي في مواجهة الجريمة بشكل عام، وتركز بشكل خاص على جرائم المعلومات، وتهدف الدراسة إلى توضيح مفهوم هذه الجرائم، وتحليل أنماطها وخصائصها، بالإضافة إلى إلقاء الضوء على الأسس الإجرائية والتشغيلية لإجراءات الاستدلال في بيئة رقمية.

أهمية البحث:

تتمثل أهمية مرحلة التحقيق في الجرائم الإلكترونية في أنها الأساس الذي تقوم عليه عملية التصدي لهذه الجرائم، وتحقيق العدالة في هذه القضايا، ونظرًا لطبيعة الجرائم الإلكترونية التي تتميز بسرعتها وسهولة ارتكابها، والصعوبة في جمع الأدلة لإثباتها، فإن مرحلة التحقيق تلعب دورًا هاما في مكافحة هذه الجرائم.

كذلك تُعتبر مرحلة المحاكمة من بين أهم المراحل القانونية، حيث تقوم على قناعة قائمة على الدلائل والأدلة العلمية بدلًا من الحدس والتخمين، يتم في هذه المرحلة إثبات التهمة أو براءة المتهم، وشهدت مجال الإثبات الجنائي تطورات كبيرة بفضل التقدم العلمي الهائل في وسائل جمع الأدلة.

وسلطة القاضي في تقدير الأدلة تعد أمرًا هاما لضمان تحقيق العدالة، ويتمثل دوره في الاقتناع بقيمة الأدلة المقدمة، وتشير التسميات المتعددة لهذه السلطة إلى حريته في تحديد مدى أهمية الأدلة والاعتماد على معاييره وقناعاته الشخصية.

كما يجسد مبدأ حرية الإثبات الجنائي حقيقة القاضي الذي يُكلَّف بتحقيق التوازن بين مصالح المجتمع وحقوق الأفراد، وتُبرز التحديات الحديثة في استخدام الأدلة العلمية، مثل التحاليل الجينية وتسجيلات الفيديو، الحاجة إلى وضع إطار قانوني وأخلاقي للتحقق من القوانين والتشريعات المتعلقة بها.

تكمن أهمية هذا البحث في تسليطه الضوء على موضوع حيوي يتناول إجراءات التحقيق والمحاكمة في الجرائم الإلكترونية بسلطنة عُمان، حيث يعكس هذا الموضوع التحولات التي طرأت على طبيعة الجريمة في العصر الرقمي الحديث، إذ أصبحت الجرائم الإلكترونية تمثل تحديًا جديدًا للنظم العقابية التقليدية، من هنا تبرز أهمية البحث في مساهمته الفاعلة لتطوير الإطار القانوني والإجراءات المعتمدة للتحقيق والمحاكمة، وذلك من خلال تقديم مقترحات تهدف إلى رفع كفاءة هذه الإجراءات وضمان تحقيق العدالة في التصدي للجرائم الإلكترونية، بما يتماشى مع التحديات التي يفرضها هذا النوع المستجد من الجرائم.

فبشكل عام يُعتبر هذا البحث ذا أهمية لأنه يتناول موضوعًا حديثًا وجذابًا، حيث يقدم تحليلًا قانونيًا دقيقًا للتحديات التي يفرضها التطور التكنولوجي على أنظمة العقوبات في سلطنة عُمان، كما يوفر مقترحات عملية لتحسين إجراءات التحقيق والمحاكمة في الجرائم الإلكترونية.

أهداف البحث

يهدف البحث إلى تحقيق الأهداف التالية:

1. تحديد اختصاصات وصلاحيات مأموري الضبط القضائي في التحقيق بالجرائم الإلكترونية، مع توضيح الفروق بينها وبين الجرائم التقليدية.
2. تحليل الوسائل المستخدمة في التحري عن الجرائم الإلكترونية واستكشاف التحديات التي تواجه هذه الوسائل.
3. تحديد أنواع الأدلة الإلكترونية الممكن الاعتماد عليها في التحقيقات الجنائية، مع توضيح كيفية جمعها وتحليلها وفقًا للأصول القانونية.
4. تحديد معايير الاختصاص الجنائي في القضايا ذات العلاقة بالجرائم الإلكترونية، وبيان الآليات التي يتم اتباعها في هذا السياق.
5. توضيح الأسس القانونية للتعاون الدولي في مكافحة الجرائم الإلكترونية، مع بيان آليات تبادل المعلومات والأدلة بين الدول لتحقيق العدالة.

6. تقييم فعالية الإجراءات القضائية الحالية في التعامل مع الجرائم الإلكترونية، وتقديم توصيات لتعزيز كفاءة هذه الإجراءات.
7. إلقاء الضوء على إجراءات التحقيق والمحاكمة في سلطنة عُمان بهدف تحليل التحديات التي تواجه التحقيقات والمحاكمات المتعلقة بالجرائم الإلكترونية، من أجل تقديم حلول فعّالة لتجاوز هذه العقبات في ظل التكنولوجيا الحديثة.

إشكالية البحث:

أصبحت الجرائم الإلكترونية تشكل تهديدًا حقيقيًا يؤثر على الأفراد والمجتمعات على حدٍ سواء، حيث تشمل هذه الجرائم اختراقات الأنظمة، والاحتيال الإلكتروني، وسرقة الهوية، والتجسس الإلكتروني، وغيرها من الأفعال الإجرامية التي تتزايد باستمرار، وتزداد الحاجة إلى تطوير آليات وإجراءات دقيقة للتحقيق في هذه الجرائم لضمان حفظ الحقوق وردع المجرمين، ومع ذلك تبرز العديد من التحديات التشريعية والفنية التي تعوق تحقيق العدالة في مواجهة الجرائم الإلكترونية، من بينها اختلاف طبيعة الأدلة الرقمية وصعوبة تعقب المجرمين في فضاء إلكتروني لا يخضع لحدود جغرافية واضحة، وفي هذا السياق، يثار التساؤل حول مدى كفاءة وجاهزية الأجهزة القضائية والأمنية للتعاطي مع هذا النوع الحديث من الجرائم، وكذلك كيفية تطوير وسائل التحري والتحقيق لتتناسب مع تطور هذه الجرائم.

وبالإضافة إلى ذلك، تواجه الجهات القضائية تحديًا كبيرًا يتمثل في كيفية التحقق من حجية الأدلة الرقمية وجمعها بشكل قانوني، وكيفية التعاون الدولي الضروري في التصدي للجرائم الإلكترونية العابرة للحدود، فالجرائم الإلكترونية تتسم بطبيعتها العابرة للحدود، مما يستدعي تعاونًا وتنسيقًا دوليًا في جمع الأدلة وتقديمها للمحاكم، هذه الإشكالية تتناول دراسة الإجراءات المتعلقة بالتحقيق والمحاكمة في الجرائم الإلكترونية، بدءًا من اختصاصات مأموري الضبط القضائي، ومرورًا بالأساليب المستخدمة في جمع وتحليل الأدلة الرقمية، وصولًا إلى دور القضاء في تقدير هذه الأدلة والتعاون الدولي في معالجتها، وبالتالي تهدف هذه الدراسة إلى تحليل أوجه القصور والتحديات التي تعترض الإجراءات القضائية في الجرائم الإلكترونية، مع التركيز على الأدوات والاستراتيجيات التي يمكن من خلالها

تعزيز فعالية هذه الإجراءات وتطويرها لضمان العدالة.

وفيما يلي التحديات التي يفرضها التطور المعلوماتي على أنظمة التحقيق والمحاكمة في سلطنة عُمان تتجسد هذه التحديات في:

- سهولة ارتكاب الجرائم الإلكترونية، حيث يمكن للمرتكب تنفيذ جريمته في غضون دقائق معدودة.
- صعوبة جمع الأدلة لإثبات الجرائم الإلكترونية، حيث يمكن للمرتكب محو آثار جريمته بسهولة.
- صعوبة تحديد هوية مرتكب الجرائم الإلكترونية، حيث يمكن للمرتكب ارتكاب جريمته من أي مكان في العالم.
- كيفية مواجهة هذه التحديات من خلال تطوير الإطار القانوني والإجراءات التي يتم اتباعها في التحقيق والمحاكمة في الجرائم الإلكترونية.

تساؤلات البحث

بناءً على إشكالية البحث وأهدافه، يمكن طرح الأسئلة التالية:

1. ما هي اختصاصات وصلاحيات مأمور الضبط القضائي أثناء التحقيق في الجرائم الإلكترونية؟ وكيف تختلف وظائفهم عن التحقيق في الجرائم التقليدية؟
2. ما هي الوسائل المتبعة في التحري عن الجرائم الإلكترونية؟ وما هي التحديات التي تواجها هذه الوسائل؟
3. ما هي أنواع الأدلة الإلكترونية التي يمكن الاعتماد عليها في التحقيقات الجنائية؟ وكيف يتم جمع وتحليل هذه الأدلة؟
4. كيف يتم تحديد الاختصاص الجنائي في القضايا المتعلقة بالجرائم الإلكترونية؟ وهل هناك معايير معينة يتم اتباعها في هذا المجال؟
5. ما هي الأسس القانونية للتعاون الدولي في التصدي للجرائم الإلكترونية؟ وكيف يتم تسهيل تبادل المعلومات والأدلة بين الدول في هذه القضايا؟

منهجية البحث:

يعتمد البحث على المنهج القانوني التحليلي، والذي يهدف إلى تحليل وتفسير النصوص القانونية، وتحديد الأحكام والقواعد التي تنظم موضوع البحث، ويشمل هذا المنهج دراسة النصوص القانونية المتعلقة بالجرائم الإلكترونية، وإجراءات التحقيق والمحاكمة في هذه الجرائم، وذلك في ضوء التطور التكنولوجي.

وفيما يلي الخطوات التي سيتم اتباعها في البحث:

- **الخطوة الأولى:** جمع البيانات والمعلومات المتعلقة بموضوع البحث، وذلك من خلال مصادر مختلفة، مثل:
  - الكتب والمراجع القانونية: تتضمن هذه المصادر مجموعة واسعة من المعلومات المتعلقة بالجرائم الإلكترونية، وإجراءات التحقيق والمحاكمة في هذه الجرائم.
  - القوانين واللوائح: تتضمن هذه المصادر النصوص القانونية التي تنظم موضوع البحث.
  - الأحكام القضائية: تتضمن هذه المصادر تطبيقات القضاء لأحكام القوانين المتعلقة بالجرائم الإلكترونية.
  - الدراسات والبحوث السابقة: تتضمن هذه الدراسات والبحوث نتائج البحوث السابقة التي أجريت حول موضوع البحث.
- **الخطوة الثانية:** تحليل البيانات والمعلومات التي تم جمعها، وذلك من خلال استخدام المنهج القانوني التحليلي، ويشمل هذا المنهج الخطوات التالية:
  - قراءة البيانات والمعلومات بعناية ودقة.
  - تحديد المفاهيم والمصطلحات الأساسية المتعلقة بموضوع البحث.
  - تحليل العلاقة بين المفاهيم والمصطلحات الأساسية.
  - تحليل النصوص القانونية المتعلقة بموضوع البحث.
  - تفسير النصوص القانونية وتحديد الأحكام والقواعد التي تنظم موضوع البحث.

- **الخطوة الثالثة:** تقديم النتائج والتوصيات التي تم التوصل إليها في البحث، ويجب أن تكون هذه النتائج والتوصيات قابلة للتطبيق، وذات فائدة للجهات المعنية.

وبناءً على هذه المنهجية، من المتوقع أن يساهم البحث في تحقيق الأهداف التالية:

- التعرف على التحديات التي يفرضها التطور التكنولوجي على إجراءات التحقيق والمحاكمة في الجرائم الإلكترونية في سلطنة عُمان.
- تحليل هذه التحديات من الناحية القانونية، وتحديد أسبابها وآثارها.
- تقديم مقترحات قابلة للتطبيق لتحسين إجراءات التحقيق والمحاكمة في الجرائم الإلكترونية في سلطنة عُمان.

الدراسات السابقة:

الدراسة الأولى:

عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، بحث متطلب رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، 2014م.

يشمل موضوع هذا البحث دراسة للمشكلات الموضوعية والإجرائية التي تثيرها الجرائم الإلكترونية على الصعيدين التشريعي والعملي في النظاميين الكويتي والأردني، حيث تناول البحث كيفية تقديم دليل رقمي إلكتروني مقبول ويحوز على حجية أمام القاضي الجزائي، كما تناول القواعد التقليدية في التشريع الكويتي ومدى كفايتها لمواجهة المشكلات الناجمة عن الجرائم الإلكترونية في ظل عدم وجود تنظيم قانوني خاص بهذا النوع من الجرائم في التشريع الكويتي.

وتهدف هذه الدراسة إلى إيصال توصيات للمشرع الكويتي على أمل الأخذ بها ووضع تشريع خاص لمجابهة الجرائم الإلكترونية.

المقارنة بين الدراستين:

الدراسة الحالية تركز بشكل أساسي على **إجراءات التحقيق والمحاكمة في الجرائم الإلكترونية** ضمن إطار التشريع العُماني، وتهدف إلى تسليط الضوء على التحديات التي تواجه سلطنة عُمان في

هذا المجال، سواء من حيث **القوانين الحالية** أو من خلال **الأساليب الإجرائية** المعتمدة في التحقيقات، وتبحث الدراسة في مدى كفاءة النظام القضائي العُماني في التعامل مع الجرائم الإلكترونية، خاصة في ظل تزايد هذه الجرائم وظهور تقنيات جديدة قد تجعل من الصعب تحديد مرتكبي هذه الجرائم أو جمع الأدلة، بالإضافة إلى ذلك، تسعى الدراسة إلى تقديم **حلول عملية** لتحسين النظام القضائي العُماني، مثل تحديث القوانين المعمول بها، وتدريب الكوادر القضائية والأمنية على التعامل مع الأدلة الرقمية.

في المقابل، **الدراسة السابقة** تركز على **المشكلات القانونية والعملية** التي تنشأ نتيجة للجرائم الإلكترونية في النظامين القانونيين الكويتي والأردني، وتلقي الدراسة الضوء على **غياب التشريعات الخاصة** لمكافحة هذا النوع من الجرائم، مما يسبب صعوبات في التحقيقات ومحاكمة القضايا المرتبطة بالأدلة الرقمية، كما تستعرض الدراسة الطرق الحالية المتبعة في تقديم الأدلة الرقمية أمام المحاكم وكيفية قبولها في غياب تنظيم قانوني ملائم، وفي هذا السياق، سعت الدراسة إلى تقديم **توصيات للمشرع الكويتي** من أجل وضع تشريعات خاصة لمعالجة القضايا المتعلقة بالجرائم الإلكترونية وتحسين آلية التعامل مع الأدلة الرقمية في النظام القضائي.

الدراسة الثانية:

سعيد سالم المزروعي، عزمان عبد الرحمن، إجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقا للتشريع الإماراتي، مجلة العلوم الاقتصادية والإدارية والقانونية، 2018م.

هدفت هذه الدراسة إلى استكشاف التشريع الإماراتي في سياق إجراءات التحقيق الجزائي في جرائم تقنية المعلومات، قامت الدراسة بتحليل إجراءات رجال الشرطة، المأمورين بالضبط القضائي، خلال مرحلة جمع الأدلة، وكذلك إجراءات التحقيق الابتدائي التي تتخذها النيابة العامة في مكافحة جرائم تقنية المعلومات.

كانت المشكلة الرئيسية التي تناولتها الدراسة تسليط الضوء على التحديات والمشكلات القانونية والتقنية التي يواجهها التحقيق في جرائم تقنية المعلومات، كما سعت الدراسة إلى تحديد مدى ملاءمة وفاعلية وسائل التحقيق الجزائي التقليدية في مجال جرائم تقنية المعلومات.

اعتمدت الدراسة على منهج الوصف التحليلي للنصوص القانونية والأحكام الصادرة عن المحاكم العليا في دولة الإمارات العربية المتحدة، وتوصلت الدراسة إلى نتائج مهمة، حيث أظهرت أن جرائم تقنية المعلومات تتطلب من رجال الشرطة المأمورين بالضبط القضائي أن يكونوا ملمين بالثقافة الفنية في مجال نظم المعلومات لتمكينهم من تنفيذ إجراءات جمع الأدلة، وأشارت الدراسة إلى أن قانون الإجراءات الجزائية الإماراتي لم يتناول بشكل كافٍ قواعد الضبط في جرائم تقنية المعلومات، واكتفى بالقواعد العامة للضبط في الجرائم.

توصلت الدراسة أيضًا إلى مجموعة من التوصيات، منها ضرورة تدريب جهات التحقيق المختصة في مكافحة جرائم المعلومات، لضمان فهمهم للمفاهيم المتقدمة المتعلقة بجرائم تقنية المعلومات والتعامل الفعّال مع الأدلة الإلكترونية.

المقارنة بين الدراستين:

تتناول الدراسة السابقة موضوعًا مهمًا وهو إجراءات جمع الاستدلالات والتحقيق الابتدائي في الجرائم الإلكترونية، وتُقدم تحليلًا شاملًا لهذه الإجراءات في التشريع الإماراتي، وتُوصي الدراسة بضرورة تطوير مهارات وقدرات المحققين الجنائيين في الجرائم الإلكترونية.

أما الدراسة الحالية التي تناولها الباحث فقد اختلفت عن الدراسة السابقة في كونها تناولت موضوعًا مهمًا وهو إجراءات التحقيق في الجرائم الإلكترونية بجميع مراحله سواء جمع الاستدلالات والتحقيق الابتدائي والتحقيق النهائي، وتركز على التحديات التي تواجه التحقيق والمحاكمة في الجرائم الإلكترونية في سلطنة عُمان، وتستعرض الدراسة الإجراءات القانونية في التحقيق والمحاكمة ومن خلالها سوف تتوصل إلى مجموعة من الحلول القانونية للتحديات التي تواجه التحقيق والمحاكمة في الجرائم الإلكترونية.

الدراسة الثالثة:

عبد الله بن علي بن سالم الشبلي، الجريمة الإلكترونية في سلطنة عُمان: التحديات والحلول القانونية، مجلة العلوم الاقتصادية والإدارية والقانونية، المركز القومي للبحوث، غزة، 2019.

هدفت الدراسة إلى تحديد مفهوم الجريمة الإلكترونية وخصائصها، وتقييم التشريع العُماني في إيجاد الحلول المناسبة لها، وقد تم استخدام المنهج القانوني الوصفي لتحقيق هدف الدراسة.

وتوصلت الدراسة إلى أن التشريع العُماني استطاع مواكبة التطور الحضاري من خلال تطوير القوانين التي تكافح الجرائم بصورة عامة، والجرائم الإلكترونية وتقنية المعلومات على وجه الخصوص من خلال منظومة قانونية متكاملة، وتتراوح العقوبات المقررة لهذه الجرائم بين الغرامة المالية والعقوبات السالبة للحرية.

كما توصلت الدراسة إلى جملة من التوصيات، منها:

- أهمية القيام بدراسات معتمدة على المسوح الميدانية تتناول أنواع الجرائم الإلكترونية المرتكبة، وأعداد مرتكبيها، ودوافعهم الإجرامية، وجنسياتهم، وفئاتهم العمرية؛ من أجل تطوير القوانين المعمول بها حاليًا لتتواكب مع القوانين الدولية الحديثة في ذات المجال.
- توعية المجتمع بخطورة الجرائم الإلكترونية، وأساليب ارتكابها، وآثارها الأخلاقية على الفرد والمجتمع، وطرق الوقاية منها.

المقارنة بين الدراستين:

تتناول الدراسة السابقة موضوع الجريمة الإلكترونية بشكل عام والتحديات التي تواجه إجراءات مكافحة الجريمة الإلكترونية، وتركز على تقديم حلول قانونية لهذه التحديات، أما هذه الدراسة فتتناول إجراءات التحقيق والمحاكمة في الجرائم الإلكترونية، وتركز على مدى كفاية هذه الإجراءات في تحقيق العدالة في الجرائم الإلكترونية.

تناولت الدراسة السابقة موضوع التحديات التي تواجه إجراءات مكافحة الجرائم الإلكترونية بشكل عام، وقدمت مجموعة من الحلول القانونية التي يمكن أن تساعد في مواجهة هذه التحديات.

أما هذه الدراسة تتناول موضوعًا مهما وهو إجراءات التحقيق والمحاكمة، وقدمت تحليلًا مفصلًا لهذا الموضوع، وتُوصي بضرورة تطوير أنظمة العقوبات بما يتناسب مع التطور التكنولوجي.

خطة البحث

- **الفصل الأول: إجراءات التحقيق في الجرائم الإلكترونية**
  - **المبحث الأول:** الجهات المختصة بالتحقيق في الجرائم الإلكترونية
    - المطلب الأول: دور الادعاء العام في جمع إجراءات الأدلة الإلكترونية وتحليلها.
    - المطلب الثاني: مأموري الضبط القضائي في الجرائم الإلكترونية ووظائفهم.
  - **المبحث الثاني:** الأدلة الإلكترونية وإجراءات جمعها وتحليلها
    - المطلب الأول: مفهوم الدليل الإلكتروني وخصائصه.
    - المطلب الثاني: الوسائل المتبعة في التحري عن الجريمة الإلكترونية ومعوقاتها.
- **الفصل الثاني: إجراءات المحاكمة في الجرائم الإلكترونية**
  - **المبحث الأول:** الاختصاص الجزائي في الجرائم الإلكترونية
    - المطلب الأول: مبادئ التحقيق الجزائي في الجرائم الإلكترونية
    - المطلب الثاني: التعاون القضائي الدولي في مواجهة الجرائم الإلكترونية
  - **المبحث الثاني:** حجية الإثبات في الجرائم الإلكترونية
    - المطلب الأول: حجية الدليل الرقمي أمام القضاء
    - المطلب الثاني سلطة القاضي في تقدير الخبرة الفنية في الجرائم الإلكترونية
- **الخاتمـــــــة**

الفصل الأول

إجراءات التحقيق في الجرائم الإلكترونية

شهدت التكنولوجيا الرقمية ثورة هائلة أحدثت تحولًا محوريًا في نمط الحياة والعمل والتواصل، ومع تزايد الاعتماد على الإنترنت والتكنولوجيا الرقمية، جاءت تحديات جديدة تتعلق بالجريمة والتحرش الإلكتروني، والاختراقات السيبرانية، وغيرها من الأنشطة الإجرامية التي تتم عبر الشبكة المعلوماتية.

حيث تتطلب الجرائم الإلكترونية معالجة فعالة تمثل تحديات قانونية وتقنية متعددة الأبعاد، ويجب على السلطات القانونية والمحققين أن يكونوا على دراية بأحدث التقنيات والممارسات للتحقيق في هذه الجرائم بفعالية ودقة، لذلك يأتي هذا الفصل لاستكشاف إجراءات التحقيق في الجرائم الإلكترونية، وفهم التحديات التي تواجه المحققين في هذا المجال، بالإضافة إلى استكشاف الأساليب والأدوات التي يمكن استخدامها للتحري وجمع الأدلة الرقمية وتحليلها بشكل فعال.

سيتم تناول مجموعة متنوعة من المواضيع في هذا الفصل، بما في ذلك الجهات المعنية بإجراءات التحقيق في الجرائم الإلكترونية، وتحليل التحديات القانونية والتقنية التي تواجه عمليات التحقيق في هذه الجرائم، واستكشاف الأساليب والأدوات الحديثة المستخدمة في جمع الأدلة الرقمية وتحليلها.

يهدف هذا الفصل إلى توضيح أهمية فهم إجراءات التحقيق في الجرائم الإلكترونية وتوفير التدريب اللازم للمحققين لمواجهة هذه التحديات بفعالية، كما يهدف إلى توفير نظرة شاملة حول أدوات التحقيق الرقمية المتاحة وكيفية استخدامها بشكل فعال في جمع الأدلة وتحليلها، بهدف تعزيز القدرة على التحقيق في جرائم الإنترنت وتحقيق العدالة.

المبحث الأول

الجهات المختصة بالتحقيق في الجرائم الإلكترونية

في عصر الرقمنة الذي نعيش فيه، تشهد الجريمة تحولًا متسارعًا نحو العالم الرقمي، حيث أصبحت الجرائم الإلكترونية مصدر تهديد خطير على الأمن الإلكتروني والاقتصاد الرقمي، لمواجهة هذا التحدي المتنامي، وتتدخل جهات إنفاذ القانون المختصة للتحقيق في هذه الجرائم ومعاقبة مرتكبيها.

يُعد فهم الجهات المعنية بالتحقيق في الجرائم الإلكترونية أمرًا بالغ الأهمية، حيث يلعب هذا الجانب دورًا هاما في تأمين البيئة الرقمية وحماية المجتمع من التهديدات السيبرانية[1]، وسلطنة عُمان كغيرها من الدول تواجه تهديدات كبيرة من هذه الجرائم، مما يستدعي وجود جهات مختصة وفعالة للتحقيق ومكافحة هذه الجرائم.

يهدف هذا المبحث إلى تسليط الضوء على الجهات المعنية بالتحقيق في الجرائم الإلكترونية في سلطنة عُمان، وتحليل دور كل جهة واختصاصاتها وتحدياتها في هذا المجال، كما يهدف إلى استكشاف كيفية تعاون هذه الجهات في مجال التحقيقات الرقمية وتبادل المعلومات، بهدف تحسين كفاءة التحقيق وتعزيز التعاون الدولي في مكافحة الجرائم الإلكترونية، وذلك من خلال المطلبين التاليين.

المطلب الأول

دور الادعاء العام في التحقيق في الجرائم الإلكترونية

إن الإثبات يعد من أهم وأخطر المسائل التي تواجه العدالة القضائية عند النظر في الدعوى المتنازع فيها والمعروضة أمام القضاء، حيث أن وسائل الإثبات تهدف إلى كشف الحقيقة والتي يتمخض عنها الحكم الذي يصدره القاضي، ويكون ذلك بتكوين قناعته نتيجة الأدلة المتحصل عليها والتي تؤكد على الحقيقة.

---

[1] د. طه السيد أحمد الرشيدي، الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق في النظام الجنائي المصري والسعودي، دار الكتب والدراسات العربية، الإسكندرية، ط1، 2016، ص51.

ولتحقق الدليل لإثبات الجريمة فإنه لا بد من جمع كافة عناصر التحقيق والدعوى، وتقديم هذه العناصر إلى الجهة المعنية بالتحقيق الابتدائي، فإذا أسفر هذا الحقيق عن دليل أو أدلة ترجح معها إدانة المتهم قدمته إلى المحكمة لبدأ إجراءات المحاكمة، ومرحلة المحاكمة هي أهم المراحل لأنها مرحلة الجزم بتوافر دليل أو أدلة يقتنع بها القاضي بإدانة المتهم وإلا قضى ببراءته[1].

وقد رتب الاستخدام غير المشروع لتقنية الحاسب الآلي والإنترنت العديد من الإشكاليات الإجرائية في مجال إجراءات الملاحقة الجزائية التي يتم إتباعها من أجل الكشف عن الجريمة وإيجاد الدليل على وقوعها ونسبتها إلى مرتكبيها الذين يستخدمون التقنية المتطورة في ارتكابها وفي إخفاء معالمها وعدم تركهم أية آثار مادية تدل عليها، وهذه أحد الصعوبات التي تواجه الحصول على الدليل أدت إلى تدخل مشرعي بعض الدول لمواجهة هذا النوع من الجرائم، وذلك بإصدار قوانين خاصة بملاحقتها وتنظيم الإجراءات التي تناسبها دون مساس بحقوق الأفراد وحرياتهم إلا في حدود القانون، حيث يتجلى دور الادعاء العام في اتخاذه الإجراءات المناسبة التي من خلالها يتم ملاحقة المجرمين وتقديمهم إلى عدالة المحكمة.

فمن هنا تأتي أهمية الموضوع في بيان الجهة المختصة في التحقيق الابتدائي والإجراءات المتبعة في التعامل مع الجرائم الإلكترونية.

الفرع الأول

المحقق الجزائي في الجرائم الإلكترونية

يعد المحقق في الجرائم الإلكترونية أحد أفراد سلطة إنفاذ القانون، وهو المكلف باتخاذ كافة الإجراءات اللازمة القانونية والإدارية والفنية للكشف عن الجريمة، والتعرف على الأشخاص الذين ارتكبوها، وإلقاء القبض عليهم، بالإضافة إلى جمع الأدلة وتقديم المساعدة للضحايا لمساعدتهم على تخطي الأزمات التي تعرضوا لها، ويمكن أن يكون المحقق فردا بمفرده، أو يعمل كجزء من فريق أو

[1] د. حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، دار النهضة العربية، القاهرة، ط1، 2017م، ص37.

لجنة متخصصة حسب طبيعة الجريمة وظروف ارتكابها[1].

قبل التطرق إلى موضوع مأموري الضبط القضائي المعنيين بالتحقيق في الجرائم الإلكترونية، سيتم أولا بيان تعريف المحقق وتوضيح دوره في عملية التحقيق الإلكتروني.

أولًا: تعريف المحقق الجزائي:

في إطار فقه القانون الجزائي توجد عدة تعريفات للمحقق الجزائي؛ إذ يعتبره البعض أنه "الشخص أو الموظف المكلف بخدمة عامة، والمختص والمؤهل بإتباع سلسلة من الإجراءات والوسائل القانونية المشروعة بهدف كشف الحقيقة، ويقوم بجمع الأدلة التي تبث وقوع الجريمة وتوضح كيفية ارتكابها وأسبابها، مما يسهم في تحديد هوية مرتكبها".[2]

كما عرفه البعض بأنه: "الشخص الذي يكلفه القانون بالتحقيق في الجرائم، وذلك بموجب الصلاحيات الممنوحة له من خلال أحكام القوانين الشكلية"[3].

وأحد التعريفات الأخرى للمحقق هو أنه "كل من يُعهد إليه بتحري الحقيقة في الحوادث الجزائية، ويتولى التحقيق وكشف غموضها، وجمع الأدلة ضد الجاني استعدادًا لمحاكمته"[4].

ويُعرّف المحقق في الجرائم عبر الكمبيوتر وشبكاته بأنه "الشخص المكلف بالتحقيق في الجرائم التي تتعلق بالأنظمة الإلكترونية وشبكات الكمبيوتر، حيث يقوم بالبحث وجمع الأدلة المتعلقة بتلك الجرائم، وذلك بهدف كشف المتورطين وتحديد مسؤوليتهم، يتمتع بالخبرة والمعرفة الفنية اللازمة لفحص الأنظمة وتحليل البيانات الإلكترونية المتعلقة بالتحقيق، ويتولى تنفيذ إجراءات التحقيق وفقًا للأنظمة والإجراءات المعتمدة في مجال التحقيق الجزائي في الأنظمة الإلكترونية"[5].

---

[1] د. محمد الأمين البشري، التحقيق الجنائي المتكامل، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، ط1، 1998، ص15.

[2] د. برهم محمد ظاهر، تنظيم التحقيق الابتدائي في الجرائم، ط1، دار وائل للنشر، عمان،2013، ص53.

[3] د. مجيد خضر أحمد السبعاوي، مولان قادر أحمد، الضرورة الإجرائية في مرحلة التحقيق الابتدائي – دراسة تحليلية مقارنة، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2017، ص148.

[4] د. محمد أنور عاشور، المبادئ الاساسية في التحقيق الجنائي العملي، عالم الكتب، القاهرة، 1969. ص15.

[5] د. مصطفي محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مكتبة الكونجرس، القاهرة، 2009. ص253.

تأكيدًا لما سبق المحقق الجزائي هو الشخص المكلف بأعمال إجراءات التحقيق الجزائي سواء في الجرائم التقليدية أو الجرائم الإلكترونية، والفرق الرئيسي بين تعريف المحقق في كل من هذين النوعين من الجرائم يعود فقط إلى نوعية الجريمة التي يتعامل معها، وليس في الدور أو التعريف الأساسي للمحقق نفسه.

ومن التعريفات السابقة يمكن استنتاج أن الاختلاف يتمحور حول النطاق التطبيقي لعمل المحقق وطريقة تحديد وتنفيذ الإجراءات والوسائل التي يستخدمها في كل نوع من الجرائم، وعلى سبيل المثال في حالات الجرائم الإلكترونية، قد يتطلب التحقيق استخدام تقنيات خاصة بالحوسبة الرقمية والأدلة الإلكترونية، بينما في الجرائم التقليدية قد يكون التركيز أكثر على جمع الأدلة المادية واستجواب الشهود.

وبالتالي، على الرغم من الاختلافات الظاهرة في النوعية والتقنيات المستخدمة، فإن دور المحقق يظل ثابتًا في كلا النوعين من الجرائم، وهو البحث عن الحقيقة وجمع الأدلة التي تدعم الإدانة أو البراءة، والتعاون مع الادعاء العام والقضاء لضمان تحقيق العدالة.

بذلك يتضح أن المحقق الجزائي هو الفرد الذي يؤدي دوره بموجب القانون للتحقيق في الجرائم، سواء كانت تقليدية أو إلكترونية، ويختلف التركيز بين التعريفات في النظر إلى تفاصيل الإجراءات أو المهام التي يقوم بها، ولكن الهدف الأساسي يبقى هو تحقيق العدالة وتطبيق القانون بنزاهة وفعالية.

والتحقيق في الجرائم الإلكترونية، يتم تكليف مهمة التحقيق إلى نوعين من المحققين[1]:

- **النوع الأول: خبراء متخصصون في الأنظمة الإلكترونية وأجهزة الحاسب الآلي:** يتمتع هؤلاء المحققون بخبرة في استخدام التقنيات الرقمية والأجهزة الإلكترونية، ويستعان بهم في جميع مراحل ضبط الجرائم الإلكترونية والتحقيق فيها وكشفها، ويقدمون الأدلة الجزائية للجهات

[1] د. يوسف بن سعيد الكلبانى، الحماية الجنائية للبيانات الإلكترونية في التشريعين العُماني والمصري دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، دار النهضة العربية 2017، ط1، ص349.

المختصة، موضحين كيفية ارتكاب الجريمة وأسلوبها، مستهدفين من معرفتهم الفنية المتقدمة في هذا المجال[1].

- **النوع الثاني: المحققون ذوو الكفاءة المهنية في التحقيق الجنائي:** حيث يتميز هؤلاء بمهاراتهم وكفاءتهم العالية في استنباط الحقائق وجمع الأدلة التي تدعم إقامة الدعوى الجزائية، ويعتمدون على خبراتهم الشخصية والمهنية في توجيه مسارات التحقيق مع الحرص على تحقيق العدالة ضمن إطار القوانين الجزائية السارية.

باختلاف دور كل من النوعين، يضمن الاستخدام المتزن للخبراء الفنيين والمحققين الجنائيين المهنيين تحقيق نتائج فعالة في مكافحة الجرائم الإلكترونية وتقديم المتهمين إلى العدالة بشكل صحيح ومنصف.

إن جهات إنفاذ القانون المعنية بالتعامل مع الجرائم الإلكترونية تسعى إلى تكليف خبراء متخصصين وأصحاب الكفاءة المهنية لأداء مهمة التحقيق الجنائي، هذا الاختصاص يهدف إلى الوصول إلى تحقيق نتائج دقيقة وذات قيمة، تساهم في سير الدعوى الجنائية بشكل فعّال ومنصف، استخدام المحققين ذوي الخبرات المتقدمة في أنظمة الكمبيوتر والتحقيق الجنائي يساعد على ضبط الجرائم الإلكترونية، وجمع الأدلة اللازمة لتقديمها أمام السلطات القضائية بطريقة تضمن تحقيق العدالة واحترام حقوق المتهمين.

ثانيًا: الإطار القانوني لإجراءات الادعاء العام في التحقيق في الجرائم الإلكترونية:

يعد الادعاء العام جزء من السلطة القضائية، يتولى الدعوى العمومية ويشرف على شؤون الضبط القضائي وتطبيق القوانين الجزائية وهذا ما أكدت عليه المادة (86) من النظام الأساسي للدولة الصادر بالمرسوم السلطاني رقم 2021/6. وكذلك أكدت على ذلك المادة (1) من قانون الادعاء العام والتي نصت: "أن الادعاء العام يتولى الدعوى العمومية باسم المجتمع، ويشرف على شؤون الضبط القضائي، ويسهر على تطبيق القوانين الجزائية وملاحقة المذنبين وتنفيذ الأحكام...".

---

[1] د. محمد الأمين البشري، مرجع سابق، ص122.

بموجب هذا النظام، يقوم الادعاء العام بإجراءات التحقيق الابتدائي، بما في ذلك جمع الأدلة وسماع الشهود، وذلك بغرض تحديد ما إذا كان هناك أساس لتقديم الاتهام أم لا، ويحظى الادعاء العام بسلطات واسعة في إدارة القضايا الجنائية والتحقيقات المتعلقة بها، مما يساعدها في تنفيذ وظائفه بشكل شامل وفعال.

وتجدر الإشارة إلى أن المادة الرابعة من قانون الإجراءات الجزائية تؤكد أن الادعاء العام يختص بشكل أساسي بتحريك الدعوى العمومية ومباشرتها أمام المحكمة المختصة، فهذه الإجراءات تمس حقوق وحريات الأفراد، ولذلك حرص المشرع الإجرائي على تفويضها لجهة قضائية، وهي الادعاء العام كقاعدة عامة.

لذلك فإن الادعاء العام يمثل المجتمع، ويسعى جاهد لتحقيق مبادئ العدالة والقانون، وحرصا منه في تطوير النظام القانوني والتنظيمي لمواكبة تزايد الجرائم المرتبطة بالتكنولوجيا ووسائل الاتصالات الحديثة تم إنشاء مختبر الأدلة الجنائية بالادعاء العام في سبتمبر 2015م، ويختص هذا المختبر بفحص وتحليل الأدلة الرقمية المحالة إليه، وقد تم تدريب وتأهيل الموظفين في هذا المختبر بما يتماشى مع التطورات التكنولوجية، لضمان مواكبة التحديات الجديدة التي تفرضها الجرائم الإلكترونية.

ثالثا: صلاحيات مأمورو الضبط القضائي في التحقيق في الجرائم الإلكترونية:

وفقًا لقانون الإجراءات الجزائية العُماني يعد التحقيق الابتدائي اختصاصًا أصيلًا للادعاء العام، ومع ذلك فقد أجاز المشرع في بعض الحالات وضمن شروط محددة لمأموري الضبط القضائي مباشرة أعمال التحقيق في بعض الحالات وذلك وفق التالي:

1. **التلبس:** فقد نصت المادة (38) من قانون الإجراءات الجزائية الحالات التي تعتبر الجريمة متلبسا بها، ومثال على الجرائم الإلكترونية المتلبس بها، كأن يقوم أحد الأفراد باختراق موقع حكومي أو مصرفي وتم ضبطه متلبسًا أثناء تنفيذ الهجوم والاختراق، في هذه الحالة يجوز لمأمور الضبط القضائي التدخل فورًا والتحفظ على الأدلة الإلكترونية، والقبض على المشتبه به، وإخطار الادعاء العام لاتخاذ الإجراءات القانونية اللازمة.

2. **الندب:** كذلك نصت المادة (75) من ذات القانون أنه يجوز للادعاء العام تكليف أحد مأموري الضبط القضائي القيام بأعمال التحقيق عدا استجواب المتهم، بشرط ألا يتجاوز حدود تكليفه، كما أعطى المشرع الصلاحية للادعاء العام لندب أحد مأموري الضبط القضائي من أصحاب الخبرة أو غيرهم من الذين يمكن أن يستعين بهم إذا اقتضت مصلحة التحقيق ذلك، وهذا ما أكدت عليه المادة (116) من قانون الإجراءات الجزائية العُماني[1]، حيث تهدف هذه الصلاحيات الممنوحة إلى دعم الادعاء العام في إدارة التحقيقات الجزائية بشكل فعال ومنظم مما يسهم في تسريع وتنظيم إجراءات التحقيق مع الحفاظ على الإجراءات القانونية وضمان حقوق الأفراد.

كما تجدر الإشارة إلى أن المشرع الجزائي العُماني أعطى صفة الضبطية القضائية إلى عدة جهات وفق طبيعة اختصاصاتها، ومن ضمنها شرطة عمان السلطانية، حيث نصت المادة (31) من قانون الإجراءات الجزائية بأنه: "مأمورو الضبط القضائي في دوائر اختصاصهم:...2- ضباط الشرطة والرتب النظامية الأخرى بدءا من رتبة شرطي..."، فمن هذا المنطلق واهتمامًا من شرطة عمان السلطانية فقد أنشأت المختبر الرقمي التابع للمختبر الجنائي في الإدارة العامة للتحريات والبحث الجنائي وكذلك أنشأت إدارة متخصصة لمتابعة الجرائم الإلكترونية تحت مسمى إدارة الجرائم الاقتصادية تتبع الإدارة العامة للتحريات والبحث الجنائي.

وقد نصت المادة (34) من قانون مكافحة جرائم تقنية المعلومات العُماني على إعطاء موظفي هيئة تقنية المعلومات صفة الضبطية القضائية في نطاق تطبيق أحكام قانون مكافحة جرائم تقنية المعلومات.

وتعزيزا للجهود الرامية إلى مكافحة الجرائم الإلكترونية فقد تم إنشاء مركز الدفاع الإلكتروني بموجب المرسوم السلطاني رقم (64/ 2020) ويتبع جهاز الأمن الداخلي، فقد أوكل لهذا المركز دورا مهما ومحوريا في حماية الفضاء الإلكتروني في سلطنة عُمان[2]، فقد أعطي المركز مجموعة من الاختصاصات يمارس بموجبها صفة الضبطية القضائية في الجرائم الداخلة في هذه الاختصاصات.

---

[1] المادة (116) من المرسوم السلطاني رقم 99/97 بإصدار قانون الإجراءات الجزائية.

[2] المادة الأولى من المرسوم السلطاني رقم 2020/64 بإنشاء مكز الدفاع الإلكتروني وإصدار نظامه.

فمن خلال ما تقدم يتضح بأن المشرع قد أعطى صفة الضبطية القضائية في الجرائم الإلكترونية إلى عدة جهات والتي جاء ذكرها أعلاه، ويجد الباحث أن ممارسة هذه الصلاحيات من قبل كل هذه الجهات رغم تحديد اختصاصات كل منها قد يسبب تداخل وتنازع في الاختصاص، فعلى سبيل المثال فيما يتعلق بتلقي بلاغات حدوث اختراق أو تهديد أمني إلكتروني، فقد نصت المادة (4) من نظام مركز الدفاع الإلكتروني على التزام الجهات المعنية بإخطار المركز بشكل فوري عن أي خطر أو تهديد لاختراق إلكتروني، وكذلك نصت المادة (19) من قانون حماية البيانات الشخصية على إلزام المتحكم عند حدوث اختراق للبيانات الشخصية، إبلاغ وزارة النقل والاتصالات وتقنية المعلومات وصاحب البيانات الشخصية عن الاختراق.

بناءً على ما تقدم يتضح جليًا أهمية دور مأموري الضبط القضائي في قدرتهم على تحليل البيانات الرقمية وتتبع الأنشطة الإلكترونية لتقديم الأدلة اللازمة في محاكمة الجناة، وإن تعاونهم مع السلطة القضائية يسهم في تعزيز التحقيقات الجنائية وتحقيق العدالة، فمن هذا المنطلق يرى الباحث ضرورة وضع نصوص قانونية إجرائية خاصة لتوضح جميع الأدوار والإجراءات المتخذة من قبل الجهات المعنية بالتعامل مع الجرائم الإلكترونية.

الفرع الثاني

دور الادعاء العام في جمع الدليل الإلكتروني

إن وجود تشابه في إجراءات التحقيق في الجرائم الإلكترونية والجرائم التقليدية، يتطلب اتخاذ إجراءات متشابهة فيما بينها قد تتخذ على جميع أنواع الجرائم مثل المعاينة والتفتيش والشهادة والخبرة، والتي سوف نتناولها في هذا الفرع.

أولًا: المعاينـــــــة:

يختلف شكل المعاينة في الجرائم الإلكترونية باختلاف نوعية الجريمة المرتكبة، وذلك لاختلاف مسرح الجريمة، حيث أن مسرح الجريمة في الجريمة الإلكترونية يتمثل في المعدات والنظم المعلوماتية التي تم ارتكاب الجريمة بها أو استخدمت كأداة لارتكابها، فلعضو الادعاء العام أن ينتقل

إلى مكان وقوع الجريمة أو أي مكان متعلق بالجريمة المرتكبة وذلك لإثبات حالة الأمكنة والأشياء والأشخاص وهذا ما أكدت عليه المادة (76) من قانون الإجراءات الجزائية[1]، فالمعاينة تحتمل أن تكون إجراء من إجراءات التحقيق الابتدائي، أو قد تكون أحد إجراءات جمع الاستدلالات، كما أنه لا يعتمد ذلك على طبيعة القائم بها، بل على مدى مساس إجراءها بحقوق الأفراد، فإذا تمت المعاينة في مكان عام فإن ذلك يعد من قبيل إجراءات جمع الاستدلالات، أما إذا تطلب الإجراء دخول منزل أو أي مكان خاص له حرمة خاصة فيعد ذلك ضمن إجراءات التحقيق التي لا يمكن اتخاذها إلا بعد الحصول على إذن من الادعاء العام[2].

ثانيًا: التفتيـــــــش:

التفتيش بمفهومه القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مفهوم التفتيش المنصوص عليه في قانون الإجراءات الجزائية، حيث لم يضع المشرع العُماني إجراءات خاصة تتعلق بالتفتيش في الجرائم الإلكترونية وإنما تطبق نفس الإجراءات التقليدية فيما يتعلق بالتفتيش المنصوص عليها في ذات القانون، فهو إجراء من إجراءات التحقيق الابتدائي تقوم به جهة مختص خولها القانون بذلك، ويكون ذلك بعد الحصول على إذن كتابي مسبب من الادعاء العام، وتتم عملية التفتيش بالدخول إلى أنظمة المعالجة الآلية للبيانات بجميع ما تشمله من ملحقات وبرامج، وذلك من أجل الحصول على الدليل على ارتكاب أعمال غير مشروعة يتم ارتكابها باستخدام هذه الأنظمة[3].

كما تجدر الإشارة إلى أن أمر التفتيش يجب ألا يتعدى الغرض منه، وإلا حكم ببطلان هذا الإجراء، وأكدت المحكمة العليا العُمانية على هذا الأمر حيث نصت على أنه: " اقتصار أمر التفتيش على حدود الغرض منه مبدأ قانون هام مقرر لحماية حق الخصوصية، فيجب أن يستهدف الأشياء المتعلقة بالجريمة، لأنه إذا كان التفتيش هو حقيقته انتهاكًا لخصوصية شخص اقتضته ظروف الواقعة

---

[1] المادة (76) من المرسوم السلطاني رقم 99/97 بإصدار قانون الإجراءات الجزائية.

[2] لطيفة الخلفي، سارة اليزيد، سناء المخوض، عثمان السفياني، المعاينة في الجرائم الإلكترونية، جامعة محمد الخامس بالرباط، كلية العلوم القانونية والاقتصادية والاجتماعية، السنة الجامعية 2018/2019، ص5.

[3] أحمد يوسف الطحاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2015، ص137.

قانونية معينة فإنه يجب أن يبقى في الحدود التي اقتضت إجراءه، مؤدى ذلك بطلان ما يتم ضبطه خارج نطاق أمر التفتيش ما دام لم يتعلق به شبهه معقولة"[1].

ثالثًا: الخبـــــــرة:

الخبرة هي أن يتم الاستعانة بمختصين للبحث في مسائل مادية أو فنية تصعب على الادعاء العام أن يقوم بها بنفسه لجمع أدلة الإثبات، فقد أجاز له المشرع بأن يستعين بخبير للوقوف على الحقائق في هذه المسائل[2]، فهو إجراء من إجراءات التحقيق نص عليها قانون الإجراءات الجزائية في المادة (116)، حيث نصت على أنه: "إذا اقتضى التحقيق الاستعانة بطبيب أو غيره من الخبراء لإثبات حالة من الحالات كان لعضو الادعاء العام أن يصدر أمرا بندبه ليقدم تقريرا عن المهمة التي يكلف بها وما يراد إثبات حالته".

فإن جرائم تقنية المعلومات ذات طبيعة فنية وعلمية معقدة يحتاج فيها لجمع الأدلة إلى إجراءات فنيه، فقد تكون الأدلة فيها غير مرئية بحيث يحتاج للكشف عنها إلى مختصين وخبراء في هذا المجال.

فالغلبة في الإثبات الجنائي بالأدلة الرقمية ستكون للقرائن والخبرة، وهو ما يزيد من أهمية دور القاضي الجنائي من خلال السلطة التقديرية التي يتمتع بها، وهو ما أكدته محكمة النقض المصرية، فقد بينت أن "تقدير آراء الخبراء والفصل فيما يوجه إلى تقاريرهم من مطاعن مرجعه إلى محكمة الموضوع التي لها كامل الحرية في تقدير القوة الدليلية لتقرير الخبير شأنه في هذا شأن سائر الأدلة فلها مطلق الحرية في الأخذ بما تطمئن إليه"[3]، فندب الخبير لا يسلب المحكمة سلطتها في تقدير الوقائع وما بها من أدلة[4].

---

[1] الطعن رقم 2017/619م، جلسة 2018/1/9م، مجموعة الاحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها، ص319.

[2] د. علي محمود علي حمودة، أدلة إثبات الجرائم الإلكترونية وتقديرها في إطار نظرية الاثبات الجنائي، مجلة الأمن القومي، أكاديمية شرطة دبي، مجلد17، عدد 1، يناير2009، ص51.

[3] الطعن رقم (24806)، لسنة قضائية رقم (67) بتاريخ جلسة 6/ 2/ 2000م.

[4] الطعن رقم (37456)، لسنة القضائية رقم (77)، بتاريخ جلسة 21/ 4/ 2009م.

رابعًا: الشهـــــــادة:

الشهادة هي "التعبير عن المضمون الحسي للشاهد بما رآه أو سمعه بنفسه من معلومات عن الغير مطابقة لحقيقة الواقعة التي شهد عليها في القضاء بعد أداء اليمين ممن تقبل شهادتهم وممن يسمح لهم بها ومن غير الخصوم في الدعوى"[1]، فتعد الشهادة أحد أدلة الإثبات، فالشاهد في الجرائم الإلكترونية وفق هذا التعريف يجب أن يكون ذا خبرة فنية في المجال التقني، لهذا فإن الشاهد في الجرائم الإلكترونية ليس كالشاهد في الجرائم التقليدية، حيث أن الشاهد هنا صاحب خبرة في المجال التقني وعلوم الحاسب الآلي، تمكنه هذه الخبرة من الحصول على معلومات جوهرية تساعد في دخوله إلى نظم المعالجة للوصول إلى البيانات اللازمة للحصول على الأدلة والحقائق[2].

---

[1] د. سليمان مرقص، أصول الاثبات واجراءاته، الأدلة المقيدة، الجزء الثالث، دار الحلبي للمنشورات الحقوقية، بيروت، 1998، ص11.

[2] نبيه قنعود، فوزي عمارة، أحكام الشاهد في الجريمة الإلكترونية، كلية الحقوق، جامعة قسطنطينية، الجزائر، 2024، ص193.

المطلب الثاني

مأموري الضبط القضائي في الجرائم الإلكترونية ووظائفهم

يشهد التطور التكنولوجي زيادة ملحوظة في حجم الجرائم الإلكترونية وتعقيداتها، تصبح الحاجة إلى تحقيق فعال وكشف الجرائم الإلكترونية أمرًا ضروريًا لضمان الأمن السيبراني وحماية المجتمع من التهديدات الرقمية.

ويعتبر مأمورو الضبط القضائي أحد أهم الجهات المختصة في التحقيق وكشف الجرائم الإلكترونية، فهم يمتلكون المعرفة والمهارات الفنية اللازمة لتتبع الأنشطة الإلكترونية وجمع الأدلة الرقمية الضرورية لتقديمها للسلطات المختصة لملاحقة المجرمين، لهذا قسمنا هذا المطلب إلى فرعين؛ الأول سوف يكون عن وظائف مأموري الضبط القضائي في الجرائم الإلكترونية وفقا للتشريع العُماني، والثاني سوف يتضمن وظائفهم.

الفرع الأول

وظائف مأموري الضبط القضائي في الجرائم الإلكترونية

مأموري الضبط القضائي يلعبون دورًا محوريًا في مكافحة الجرائم الإلكترونية، التي باتت تشكل تحديًا كبيرًا للأنظمة القانونية حول العالم، ومع تطور التكنولوجيا وانتشار الإنترنت ظهرت أنواع جديدة من الجرائم التي تستهدف الأفراد والمؤسسات الخاصة والحكومية، مثل الاختراقات الإلكترونية، والاحتيال الإلكتروني، وسرقة البيانات، ويكلف مأمور الضبط القضائي بمتابعة هذه الجرائم من خلال تلقي البلاغات والشكاوى، والانتقال إلى مسارح الجرائم والمعاينة وجمع الأدلة الرقمية وتعقب الجناة وضبطهم، تعتبر مهامهم بالغة الأهمية حيث تتطلب معرفة تقنية متقدمة إلى جانب فهم دقيق للإجراءات القانونية المتعلقة بالتعامل مع الأدلة الرقمية.

أولًا: قبول البلاغات والشكاوى: تعد من أهم وظائف مأموري الضبط القضائي قبول البلاغات عن وقوع الجرائم الإلكترونية ويتطلب عليهم فحصها والتأكد من صحتها وإثباتها في محضر معد

لذلك[1]، حيث يعرف البلاغ على أنه إخطار تقدمه جهة أو فرد إلى السلطات المختصة، يعلمها فيه بوقوع جريمة، سواء كانت هذه الجريمة وقعت بالفعل أو كانت على وشك الحدوث، ويتم تقديم البلاغ بهدف تحريك الجهات المختصة لاتخاذ الإجراءات القانونية المناسبة للبحث والتحري لمعرفة ملابسات الجريمة وتفاصيلها وضبط مرتكبيها أو منعهم من ارتكابها.[2]

ثانيًا: الانتقال إلى مسرح الجريمة: عند العلم بوقوع الجريمة فإن أول خطوة يقوم بها مأمور الضبط القضائي هو الانتقال إلى مسرح الجريمة؛ لأن هذا الأخير حجر الزاوية في التحقيق الجنائي، ومكمن الآثار والأدلة المادية، وينبغي التعامل في هذا الإطار مع مسرح الجريمة الإلكترونية على أنه مسرحان هما:

1. المسرح تقليدي: يقع هذا المسرح خارج نطاق بيئة الحاسوب والشبكة المعلوماتية، ويتألف بشكل رئيسي من العناصر المادية الملموسة في المكان الذي حدثت فيه الجريمة، ويشبه مسرح الجريمة التقليدية حيث قد يترك الجاني آثارًا متنوعة مثل البصمات أو بعض مقتنياته الشخصية أو وسائط التخزين الرقمية.
2. المسرح افتراضي: يقع هذا المسرح داخل البيئة الإلكترونية، ويشمل البيانات الرقمية المخزنة على الحاسوب والشبكة المعلوماتية، وخاصة في ذاكرة الأقراص الصلبة، ولا ينبغي التعامل مع الأدلة الموجودة في هذا المسرح إلا بواسطة خبير مختص في معالجة الأدلة الرقمية من هذا النوع[3].

وإذا كانت عملية الانتقال إلى المسرح التقليدي تتم بطريقة مادية، فالأمر يختلف بالنسبة إلى المسرح الافتراضي؛ فلا يكون بالضرورة عبر العالم المادي، وإنما عبر العالم الافتراضي، حيث يستطيع عضو الادعاء العام أو مأمور الضبط القضائي أن يقوم بهذه المعاينة وهو جالس في مكتبه من خلال الحاسوب الموضوع في المحكمة، كما يمكنه الاستعانة ببيت الخبرة القضائية

---

[1] المادة (33) من المرسوم السلطاني رقم 99/97 بإصدار قانون الإجراءات الجزائية.

[2] د. عبد الله ذيب محمود، د، أسامة إسماعيل دراج، الوجيز في الجرائم الإلكترونية القواعد الموضوعية والإجرائية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1. 2022م، ص162.

[3] د. محمود نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسب الآلي والأنترنت، رسالة دكتوراه للعلوم الشرطية، تخصص القيادة الأمنية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض، 2004م، ص77.

أو الخبراء الاستشاريين، وأيضا يمكنه التوجه إلى مقر مزود خدمة الإنترنت الذ يعد المكان الأنسب لإجراء المعاينة[1].

ونظرًا لاختلاف مسرح الجريمة الإلكترونية عن مسارح الجرائم الأخرى، حيث يتميز بوجود أدلة إلكترونية ذات طبيعة غير مرئية؛ فإن ذلك يتطلب تعاملا خاص، ويتم ذلك من خلال اتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة من أبرزها ما يلي:

1. جمع معلومات مسبقة عن موقع الجريمة، وتشمل نوع الأجهزة وعددها المتوقع مداهمته بالإضافة إلى شبكات الاتصال المرتبطة بها.
2. إعداد خريطة للموقع الذي تتم الإغارة عليه، وإعداد خطة للهجوم على ذلك المكان، وتكون موضحة بالرسومات.
3. إعداد فريق التفتيش من المتخصصين، على أن يكون هذا الفريق مرفقا بالأمر القضائي اللازم للقيام بالتفتيش؛ لأن أغلب الجرائم الإلكترونية تكون داخل أمكنة لها خصوصياتها[2].
4. تأمين الأجهزة والبرامج الضرورية التي يمكن الاستعانة بها في عمليات الفحص والتشغيل؛ مثل: برنامج معالجة الملفات Xtree Pro Gold، وبرنامج النسخ (Lap Link)، وبرنامج (Encase) الذي ينتح صورا مطابقة من القرص الصلب، ويستخدم بصفة خاصة لأغراض التحقيقات الجنائية في المباحث الفدرالية الأمريكية، ويسميها الخبراء حقيبة الأدلة الرقمية.
5. تأمين التيار الكهربائي من الانقطاع المفاجئ لأن ذلك يسبب العديد من المخاطر تتمثل في محو المعلومات من الذاكرة من جراء غلق جهاز الكمبيوتر، وبالتالي فقدان كافة العمليات التي كان يتم تشغيلها، واتصالات الشبكة وأنظمة الملفات الثابتة[3].

وفي كل الأحوال عند تلقي بلاغ عن وقوع جريمة إلكترونية وبعد التحقق من صحة البيانات

---

[1] د. عمر أبو بكر بن يونس، الجريم الناشئة عن استخدام الانترنت، كلية الحقوق، جامعة المنصورة، 2004. ص895.

[2] د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من 1-3 مايو 2000م، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ط3، 2004م، المجلد الثالث، ص357.

[3] د. ممدوح عبد الحميد عبد المطلب، البحث الجنائي الرقمي (في جرائم الكمبيوتر والإنترنت)، المكتبة القانونية، القاهرة، 2000، ط1، ص115.

الواردة في البلاغ؛ يتم الانتقال إلى مسرح الجريمة لمعاينته، ويختلف مسرح الجريمة الإلكترونية عن مسرح الجريمة التقليدية كجرائم القتل أو السرقة، إذ قد تكون الجريمة الإلكترونية جريمة مستمرة كما في الجرائم الاقتصادية كالسرقة والاحتيال، وفي بعض الحالات قد يكون مسرح الجريمة الإلكترونية مشابها للجرائم الأخرى مثل التزوير أو إتلاف البرامج أو تفجير المباني والمنشآت.

في حالة الجريمة المستمرة ذات الأهداف الاقتصادية تهدف المعاينة إلى المداهمة وضبط الأدلة المادية على أرض الواقع، أما في الحالة الثانية بعد وقوع الجريمة يعتمد التحقيق على اعترافات المتهمين عن القبض عليهم وكذلك شهادات الشهود والقرائن المتاحة، ويتم توثيق مسرح الجريمة بالكامل ووصف محتوياته بدقة مع توثيق كل دليل بشكل مفصل بما في ذلك الأدلة الرقمية، بحيث يوضح مكان ضبطها وحالتها ووقت الضبط والشخص الذي قام بجمعها وتحريزها وكيفية وتوقيت ذلك، وهناك رأي يقترح أن يشمل التوثيق جميع المصادر المتاحة على شبكة المرتبطة بالأجهزة محل التحقيق، ومن أبرز المواقع التي يحتمل العثور فيها على أدلة جنائية مرتبطة بالجرائم الإلكترونية ما يلي[1]:

- **الـورق:** فحص سلة المهملات للبحث عن أي أوراق مطبوعة ذات صلة بالحاسوب محل الفحص، إذ قد تكون ذات قيمة خاصة إذا تطابقت مع النسخ الرقمية لبعض المعلومات الرقمية الموجودة على الحاسوب، وبذلك تعد هذه الأوراق من الأدلة المهمة التي يجب مراعاتها في البحث عن الحقيقة.
- **المكونات المادية (Hardware):** تشمل أجهزة الحاسب الآلي بمختلف أنواعها والأقراص الصلبة الخارجية والملحقات المرتبطة بالحواسيب والمتعلقة بالجريمة، مثل الطابعات والماسحات الضوئية والكاميرات الرقمية وغيرها من الأجهزة..
- **البرامج (Software):** إذا كان الدليل الرقمي قد تم إنشاءه باستخدام برنامج خاص أو غير شائع، فإن الحصول على الأقراص المستخدمة لتثبيت هذا البرنامج أمرا بالغ الأهمية عند فحص الدليل.
- **وسائط التخزين المتحركة:** كالأقراص المدمجة أقراص الليزر"، والأقراص المرنة والشرائط

---

[1] د. محمد الأمين البشري، مرجع سابق، ص158.

المغناطيسية وغيرها، وأي شكل من الأشكال المختلفة لأشرطة تخزين البيانات الخارجية مثل Flash Memory"، وتعد هذه الوسائط جزءا من الجريمة المرتكبة عبر الإنترنت متى كانت محتوياتها عنصرا من عناصر الجريمة.

- **دليل الاستخدام Manuals:** وهو الدليل الخاص بالمكونات المادية والبرمجية للحاسوب والتي تساعد في فهم التفاصيل الدقيقة لآلية عملها، وتشمل أيضا مجلات الحاسب الآلي والأوراق المطبوعة التي قد تكون مفيدة في التحقيق[1].
- **كلمات السر أو أرقام الهاتف:** قد تكون مدونة على أوراق لاصقة بالحواسيب أو على مقربة منها، وقد تتعلق بحسابات الاتصال بشبكة الإنترنت أو بعض خدمات الإنترنت الأخرى، كما قد تكون هذه البيانات مفيدة لفك تشفير بعض المعلومات التي قد تحتوي على أدلة مهمة للقضية.

ثالثًا: المعاينة: فبداية تعد المعاينة من أهم الأدلة في المسائل المادية، وقد تكون في بعض الأحوال الدليل القاطع الذي لا يغني عنه دليل سواها، فهي إجراء منتج للدليل[2]، وأكد المشرع الإجرائي العُماني بضرورة إجراءها من قبل مأموري الضبط القضائي فور تلقيه أو علمه بارتكاب الجريمة[3].

فالمعاينة هي الانتقال إلى موقع محدد لفحصه وتوثيق حالته؛ أي تسجيل الحالة الفعلية لمسرح الجريمة والأشياء المرتبطة بها بهدف كشف الحقيقة وتوثيق حالة الأشخاص المرتبطين بها مثل المجني عليه، وبعبارة أخرى تهدف المعاينة إلى توثيق جميع الآثار المادية المرتبطة بالجريمة مما يشكل إثباتًا مباشرًا ماديا لحالة شيء أو شخص معين، ويجري ذلك عبر الملاحظة أو الفحص المباشر للشيء أو الشخص من قبل القائم بالإجراء[4].

ويقتضي إجراء المعاينة إثباتها في محضر يعد من قبل مأمور الضبط القضائي وموقعًا منه؛

---

[1] د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت: دراسة مقارنة، دار النهضة العربية، القاهرة، 2009. ص10.

[2] د. هشام زوين، الموسوعة الشاملة التقادم "المدني، الجنائي، الإداري والنظم القانونية الشبيهة بالتقادم "المنظومة المتكاملة لأحكام التقادم والسقوط والانقضاء وعدم السماع في ضوء الفقه والقضاء والتشريع والمحاماة"، مركز المحمود للنشر وتوزيع الكتب القانونية، 2008. ص159.

[3] المادة (33) بالمرسوم السلطاني رقم 99/97 بإصدار قانون الإجراءات الجزائية.

[4] د. عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، 1999. بدون ناشر، ص704.

لأنها من الإجراءات التي تستلزم من المحقق حضورًا ذهنيا، وتتبعا في شأنها أيضًا في جميع القواعد التي تحكم إجراءات المحاكمة، من إخطار الخصوم بمكان المعاينة وزمانها؛ ليتمكنوا من الحضور أثناء إجراءها[1].

وتكمن أهمية المعاينة في أنها من أهم الإجراءات في التحقيقات الجنائية، وهي عصب التحقيق ودعامته، فهي تعبر عن الواقع تعبيرا أمينا صادقا لا تعرف الكذب والخداع ولا المحاباة، وتعطي المحقق صورة صحيحة واقعية لمكان الجريمة وما فيها من ماديات وآثار للجاني أو الجناة، وتكشف عن كيفية ارتكاب الجريمة منذ بدايتها حتى نهايتها[2].

فالمعاينة وسيلة يتمكن القاضي بواسطتها من الإدراك المباشر للجريمة ومرتكبها، وقد تشمل إثبات النتائج المادية التي تخلفت عنها، أو إثبات حالة الأماكن أو الأشياء أو الأشخاص التي لها علاقة بالجريمة، أو إثبات الوسيلة التي استخدمت في ارتكابها أو المكان الذي وقعت فيه[3].

تعد المعاينة ذات أهمية كبيرة في كشف غموض العديد من الجرائم التقليدية، ولكن دورها في كشف غموض الجرائم الإلكترونية وضبط الأشياء التي قد تساعد في إثبات وقوعها ونسبتها إلى مرتكبها لا يصل إلى نفس المستوى من الأهمية، ويعود ذلك إلى الاعتبارات التالية[4]:

1. الجرائم الإلكترونية نادرًا ما تترك آثار مادية واضحة عند ارتكابها، حيث تكون الأدلة الناتجة عنها عبارة عن بيانات غير مرئية.
2. قد يتردد العديد من الأشخاص على مسرح الجريمة خلال الفترة الزمنية الممتدة من ارتكابها واكتشافها مما يزيد من احتمالية إتلاف أو تغيير أو العبث بالآثار المادية، وهو ما قد يضعف الثقة في الدليل المستمد من المعاينة.
3. إمكانية تلاعب الجاني في البيانات عن بعد، أو محوها عن طريق التدخل من خلال وحدة

---

[1] د. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002. ص27.

[2] محمد أنور عاشور: الموسوعة في التحقيق الجنائي العملي، ط3، عالم الكتب، 1998. ص114.

[3] د. امال عبد الرحيم عثمان، شرح قانون الإجراءات الجنائية، الهيئة المصرية العامة للكتاب، القاهرة، ط2، 1991، ص406.

[4] د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة، دار النهضة العربية، القاهرة، 1998. ص59.

طرفية؛ لذلك ينبغي على المشرع أن يقرر جزاءات جنائية على كل من يقوم بإجراء أي تغيير أو تعديل في المعلومات المسجلة في ذاكرة الحاسوب، أو وسائط التخزين، أو في بنك المعلومات، أو قاعدة البيانات، قبل قيام سلطة التحقيق بإجراء المعاينة، وهو ما نص عليه المشرع الجزائي العُماني[1]، وذلك حرصا منه على المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأولية للتحقيق الجنائي، والملاحظ أن النص وإن كانت ينصرف إلى أغلب الجرائم التقليدية، إلا أنه يمكن تطبيقه عند معاينة مكونات الحاسوب ذات الطابع المادي؛ كأشرطة الحاسوب، وكابلاته، وشاشة العرض الخاصة به، والأقراص وغيرها، بخلاف معاينة المكونات غير المادية؛ لأنها تتطلب إجراءات خاصة.

4. مشكلة تبخر الدليل الإلكتروني الذي يمكن تعديله أو تغييره أو محوه في بضع ثواني؛ لذلك أوجب المشرع الجزائي العُماني لمأمور الضبط القضائي أن يعجل بإجراء المعاينة؛ خشية ضياع الأدلة.

ونظرًا لما تتميز به الجريمة الإلكترونية من خصائص، فبإمكان المحقق أو مأمور الضبط القضائي أن يستعين بالخبراء للفحص، وإبداء الرأي الفني في الأمور التي تستعصى على هؤلاء فهمها وتفسيرها، وهذا ما أكدته المادة (30) من قانون الإجراءات الجزائية، حيث نصت: "... ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة..."[2].

تتضمن المعاينة التقنية لمسرح الجريمة الإلكترونية إجراءات متعددة تختلف باختلاف نوع الجريمة المرتكبة، فعلى سبيل المثال في حالات جرائم الاعتداء على الملكية الفكرية تجري عملية تنزيل أو حفظ نسخة من المحتوى أو المصنف الذي تم الاعتداء عليه، ويتم التحفظ على هذه النسخة كدليل رقمي يمكن استخدامه في التحقيقات لاحقا، وذلك بطباعتها واستخراجها في هيئة ورقية أو صلبة، وحديثا تستعمل تقنية الطباعة على خشب أو بلاستيك خاص، إلا أن هناك طرقا عامة تتوافق مع طبيعة النظام المعلوماتي، مثل وسيلة تصوير شاشة وذلك بواسطة آلة تصوير الحاسوب تقليدية، أو عن طريق استخدام برمجيات حاسوب متخصصة في أخذ صورة لما يظهر على الشاشة، وهو ما

---

[1] المادة (232) بالمرسوم السلطاني رقم 2018/7 بإصدار قانون الجزاء العُماني.

[2] انظر المادة (30) بالمرسوم السلطاني رقم 99/97 بإصدار قانون الإجراءات الجزائية.

يعرف بـ طريقة تجميد مخرجات الشاشة Frozen"، أو أن يكون ذلك عن طريق حفظ الموقع باستخدام خاصية الحفظ (Save as) المتوافرة في نظام التشغيل.

ومن الإجراءات التي يتعين اتباعها عند إجراء المعاينة ما يلي:

1. القيام بتصوير جهاز الحاسب الآلي الذي ترتكب عن طريقه الجرائم، وجميع ما يتصل به من أجهزة طرفية ومحتوياته، ووضع المكان الذي يوجد به بصفة عامة مع العناية بتصوير أجزاءه الخلفية وملحقاته الأخرى[1].
2. الاهتمام الكبير بتركيز الملاحظة على كيفية إعداد النظام، وتتبع الآثار الإلكترونية الناتجة عن الوصول إليه أو زيارة المواقع على الشبكة المعلوماتية، وخاصة السجلات الإلكترونية التي توفرها الشبكات لمعرفة موقع الاتصال ونوع الجهاز الذي يتم استخدامه للوصول إلى النظام أو التفاعل معه[2].
3. تجنب الإسراع في نقل أي بيانات أو معلومات من موقع الجريمة قبل التأكد من إجراء الاختبارات اللازمة للتحقق من عدم وجود مجالات مغناطيسية في المحيط الخارجي، لتجنب إتلاف البيانات المخزنة.
4. الحفاظ على المستندات الخاصة بعملية الإدخال ومخرجات الحاسوب الورقية ذات العلاقة بالجريمة، مع رفع أي بصمات أو آثار مادية قد تكون موجودة عليها.
5. توصيل الأقراص الحاسوبية التي قد تحتوي على أدلة بجهاز يمنع الكتابة أو التسجيل عليها، مما يسمح للمحققين بقراءة بياناتها دون تعديلها.
6. التحفظ على محتويات سلة المهملات، مع فحص الأوراق والأشرطة والأقراص الممغنطة المحطمة فيها، ورفع أي بصمات قد تكون ذات صلة بالجريمة.

ولا شك أن الهدف من التفتيش هو الضبط فإن تخلفت هذه الغاية فقد أحد شروط

---

[1] د. هشام محمد فريد رستم، المرجع السابق. ص60.

[2] د. سليمان احمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، القاهرة 2007. ص290، وانظر أيضا: د، عبد الفتاح بيومي حجاري، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، ط1، الإسكندرية، 2006، ص104.

صحته الموضوعية[1].

رابعًا: ضبط الأشياء: وتكون بوضع اليد على الأشياء المرتبطة بالجريمة بهدف كشف الحقيقة وتحديد مرتكبها، وتقليديا يقتصر الضبط على الأشياء المادية دون القيم المعنوية نظرًا لان الأخيرة تفتقر للوجود المادي المباشر، لذلك يرى بعض الفقهاء أن الضبط لا يمكن أن يرد على الأدلة الرقمية إلا إذا تجسدت في وسائط مادية مثل الطباعة من مخرجات الحاسوب أو تخزين البيانات على أسطوانات ليزرية أو مدمجة أو ذاكرة فلاشيه، حيث تتيح هذه الوسائط التعامل مع الأدلة الرقمية ككيانات مادية قابلة للضبط، في حين يرى البعض الآخر أنه لا مانع من ورود الضبط على البيانات الإلكترونية في حد ذاتها[2].

أما الاتجاه الثالث فيدعو المشرع للتدخل لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط؛ لتشمل أيضا إلى جانب الأشياء المادية البيانات الإلكترونية، وعلى ذلك يمكن تعريف الضبط في البيئة المعلوماتية بأنه: وضع اليد على الدعائم المادية المحزنة فيها البيانات الإلكترونية التي تتصل بالجريمة المعلوماتية[3]، وإن كانت الصعوبة تتمثل في عدم إمكانية وضع اليد على شبكات المعلومات الدولية؛ لأنها لا تخضع لسيطرة شخص معين، ولا تعمل في إطار دولة معينة، ولكن ضبط البيانات الإلكترونية المتحصل عليها من التفتيش يطرح عدة إشكاليات.

والضبط، بحسب الأصل لا يرد إلا على أشياء مادية، فلا صعوبة بالتالي بضبط أدلة الجريمة الواقعة على المكونات المادية للكمبيوتر؛ كرفع البصمات مثلا عنها، وكذلك لا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخ غير المشروع، أو إتلافه بوسائل تقليدية كالكسر أو الحرق.

---

[1] د. أحمد عوض بلال، الإجراءات الجنائية المقارنة والنظام الإجرائي في المملكة العربية السعودية، دار النهضة العربية للنشر والتوزيع، القاهرة، 2017. ص423.

[2] د. هشام محمد فريد رستم، مرجع سابق، ص95- 96.

[3] رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم الإلكترونية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، ط2، 2017، ص142.

ولكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس، وفي ضبط بيانات الكمبيوتر Data؛ لعدم وجود أي دليل مرئي في هذه الحالات، ولسهولة تدمير الدليل في ثوان معدودة، ولعدم معرفة كلمات السر، أو شفرات المرور، أو ترميز البيانات.

فالدليل الإلكتروني: عبارة عن معطيات مخزنة في نظام إلكتروني يمكن استخدامها في قضية ما، والنتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها.

وبذلك يُسمح لمأموري الضبط القضائي بتفتيش المتهم في الأحوال التي يسمح فيها القانون بالقبض عليه، هذا يعني أنه يمكن تفتيش المتهم وجسمه وملابسه وأمتعته بما يتفق مع الإجراءات القانونية المعمول بها.

خامسا: التفتيش: تظهر أهمية التفتيش في كيفية إجراءه في الجرائم الإلكترونية من قبل الجهات المختصة، وذلك كون الجرائم الإلكترونية من الجرائم المستحدثة التي تحتاج إلى إتباع إجراءات خاصة في التعامل معها.

1. تعريف التفتيش:

التفتيش "هو إجراء قانوني يهدف إلى البحث عن أدلة مادية قد تكون مخفية وتساهم في كشف حقيقة الجريمة أو الوقائع المتورط فيها الأشخاص"[1]. يتم التفتيش بناءً على إذن قضائي أو وفقًا لضوابط قانونية محددة تتعلق بالأمارات أو الشكوك المعقولة.

2. حالات التفتيش:

يُسمح أيضًا بتفتيش أي شخص غير متهم إذا كانت هناك أمارات قوية تشير إلى أنه يخفي أشياء تساهم في كشف الحقيقة، هذا التفتيش يمكن أن يشمل جسمه وملابسه وأمتعته[2]، **وتتمثل تلك الحالات في:**

---

[1] أحمد فقيه فهد الطويلة، بطلان إجراءات التفتيش في القانونين الأردني والكويتي، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2011، ص15.

[2] انظر المواد (77– 97) من المرسوم السلطاني رقم 99/97 بإصدار قانون الإجراءات الجزائية.

- **التفتيش في حال وجود أمارات قوية:** يمكن لمأموري الضبط القضائي تفتيش أي شخص حتى لو لم يكن متهمًا، إذا كانت هناك أمارات قوية تشير إلى احتمال إخفائه أشياء قد تساهم في كشف الجريمة أو التحقيق. يشمل ذلك تفتيش الجسم، الملابس، والأمتعة. لكن يجب أن يتم هذا التفتيش بناءً على دلائل معقولة تدعم الشكوك.
- **التفتيش في الجرائم المتلبس بها:** يسمح لمأموري الضبط القضائي بتفتيش الأشخاص أو الأماكن في حال التلبس بالجريمة دون الحاجة إلى إذن مسبق من النيابة العامة أو القضاء، شريطة أن يكون هناك دليل ملموس أو تصرف مريب يشير إلى حدوث الجريمة في تلك اللحظة.
- **التفتيش على أساس إذن قضائي:** في حالات أخرى، يتطلب التفتيش الحصول على إذن قضائي محدد، حيث لا يجوز تفتيش الأشخاص أو الأماكن إلا بعد استصدار أمر قضائي يبرر التفتيش استنادًا إلى أدلة وشكوك معقولة تتعلق بالجريمة.
- **التفتيش في حالات الطوارئ:** في بعض الحالات الاستثنائية، مثل الخوف من تهريب الأدلة أو تهديد حياة الأشخاص، قد يُسمح بتفتيش الأشخاص أو الأماكن دون الحاجة لإذن قضائي فوري، ولكن تحت مراقبة دقيقة من قبل القضاء بعد ذلك.

3. ضمانات التفتيش:

- **احترام الحقوق الفردية:** يجب على مأموري الضبط القضائي أن يلتزموا بكافة الإجراءات القانونية المنصوص عليها لضمان أن التفتيش لا يمس كرامة الأفراد أو حقوقهم الأساسية، مثل احترام خصوصية الأفراد أثناء التفتيش.
- **الشفافية والمصداقية:** يجب أن يتم التفتيش بشفافية تامة وأن يتم تسجيل جميع الإجراءات بشكل دقيق في محاضر رسمية، مع تحديد الوقت والمكان والظروف التي تمت فيها عملية التفتيش.
- **التوازن بين حقوق الأفراد وضرورة التحقيق:** يكمن التحدي في ضرورة تحقيق العدالة وكشف الحقيقة من خلال التفتيش، مع ضمان الحفاظ على التوازن بين حماية الحقوق الفردية للأشخاص المتورطين في التحقيقات.

الفرع الثاني

الإجراءات الحديثة للحصول على الدليل الإلكتروني

إن إثبات الجرائم الإلكترونية يعد من أهم الصعوبات التي تواجه سلطتي جمع الاستدلالات والتحقيق، حيث أن إثباتها لا يمكن أن يتم بدون الدليل الذي يثبت وقوعها، ويرجع سبب هذه الصعوبات إلى التطور الإلكتروني والرقمي الذي يشهده العالم الأمر الذي أدى إلى ابتكار أساليب حديثه لارتكاب الجريمة نتيجة للاستخدام السيء لهذه الوسائل الحديثة، لهذا سوف نتطرق في هذا المطلب إلى بيان الإجراءات الحديثة التي تعين في جمع الأدلة الإلكترونية.

أولًا: الإجراءات المتعلقة بنظم التشغيل والبيانات الساكنة:

من أوائل الاتفاقيات الدولية المختصة بمكافحة الجرائم الإلكترونية هي الاتفاقية الأوروبية لمكافحة الجرائم الإلكترونية والتي تم التوقيع عليها من قبل ثلاثون دولة بتاريخ 23 نوفمبر 2001 بالعاصمة المجرية بودابست، حيث يشرف عليها المجلس الأوروبي، وقد دخلت الاتفاقية حيز التنفيذ في يوليو 2004م، فقد كانت النواة الأولى لمواجهة مشكلة تزايد الجرائم الإلكترونية.

فقد تضمنت هذه الاتفاقية النص على التفريق بين نوعين من البيانات وهي البيانات المخزنة أو الساكنة، والبيانات المتحركة أو البيانات المتعلقة بخط سير المعلومات، وبقراءة نصوص هذه الاتفاقية نجد أنها تضمنت إجراءات جديدة لجمع الأدلة الإلكترونية[1].

ويقصد بالبيانات الساكنة أنها البيانات الثابتة على الحاسب الآلي أيًا كان نوعها، سواء كان برنامج أو تطبيق، كان قد أنشأ بواسطة مستخدم معرف أو أنها أنشئت بواسطة البرامج نفسها أو بالاشتراك بينهما، وقد تكون هذه البيانات على هيئة صور أو أفلام أو ملفات كتابية أو حسابية، فجميعها لديها صفة الثبات على هذه الأجهزة، ولا تنتقل من جهاز إلى آخر إلا عن طريق صاحب الجهاز أو بمعرفته، فهو المتحكم

---

[1] انظر مجلس أوروبا، مجموعة المعاهدات الأوروبية رقم 185، الاتفاقية المتعلقة بالجريمة الإلكترونية، بودابست، 2001/11/23م.

فيه والذي يقوم بأي عملية نسخ أو نقل لها من هذا الجهاز إلى أخر[1].

فلا بد من مأمور الضبط القضائي عندما يحصل على أذن سواء لضبط أو تفتيش لاستخلاص المعلومات من أحد أجهزة الحاسب الآلي أن يحرص على مراعاة مجموعة من الإجراءات، ومن هذه الإجراءات أن يتحفظ على البيانات ويمنع أي شخص من الوصول إليها وخاصة صاحب الجهاز، استخدام برامج خاصة لاستخلاص كافة البيانات من الجهاز، ويكون ذلك بمعرفة خبير في هذا المجال.

ثانيًا: جمع المعلومات من خلال شبكة المعلومات:

إن انتشار الأجهزة المحمولة والمتصلة بالشبكات اللاسلكية يعد نقلة نوعية في عصر الحاسب الآلي، ويعتبر من أهم التحديات التي تواجه عمليات البحث والتحقيق في جرائم تقنية المعلومات، وتكمن هذا التحدي في كيفية الحصول على الأدلة من هذه الأجهزة عند وقوع جرائم بواسطتها.

فقد يواجه مأمور الضبط القضائي إشكاليات تشريعية عن البحث على الأدلة وذلك بأنه من الممكن أن ترتكب الجريمة في دولة وتحقق النتيجة في دولة أخرى فيصعب ملاحقة الجناة في هذه الحالة، وكذلك القوانين المطبقة في هذه الدول قد تختلف.

كذلك من الصعوبات التي قد يوجهها في البيانات الإلكترونية نفسها التي من السهولة أو تغييرها بسهولة، لهذا يتوجب على المحقق أن يكون سريعًا في اتخاذ إجراءات المحافظة عليها، كذلك أحد التحديات المهمة هيه مدى توفر الخبرات الكافية لمواجهة هذه الجرائم، وذلك بسبب تنوع الأساليب واختلافها بحيث يصعب أن يوجد خبير واحد يلم بجميع هذه الأساليب، كما أنه تدر الإشارة إلى ضخامة المعلومات على شبكة المعلومات التي تصعب عمليات البحث فيها للوصول إلى البيانات المطلوبة[2].

---

[1] د. حازم محمد حنفي، مرجع سابق، ص75.

[2] د. ممدوح عبد المطلب عبد الحميد مرجع سابق، ص120.

رابعًا: الحصول على الدليل الإلكتروني عن طريق بروتوكول العنوان الإلكتروني:

يرتفع عدد مستخدمي الشبكة العالمية للمعلومات، فبلا شك أنه من الطبيعي أن يرتفع عدد الذين يستخدمونها بشكل خاطئ أو إجرامي، فالجريمة الإلكترونية يمكن أن تقع على الشبكة الإلكترونية نفسها أو تنفذ الجريمة بواسطتها، لهذا كان لزاما أن يتم وضع وسائل حماية لهذه الشبكة لمنع أي شخص من اختراقها أو التعدي عليها أو على أي معلومات بها، فقد تم وضع قواعد وبروتوكولات أمنية وإدارية لاستخدام الشبكة، وذلك حتى يتسنى لها معرفة جميع مستخدميها.

ومن أهم هذه القواعد والأسس التي يتوجب أن يقوم بها مستخدم الشبكة، وضع عنوان رقمي خاص بكل جهاز يتم استخدام الشبكة بواسطته بمجرد اتصاله بالشبكة، بحيث لا يمكن أن يتكرر هذا العنوان الرقم أبدًا على أي جهاز أخر مطلقًا، فيعد هذا العنوان من أهم الأدلة الإلكترونية التي تساعد المحقق للوصول إلى مرتكب الجريمة والتحقق من ارتكابها من عدمه[1].

[1] د. حازم محمد حنفي، مرجع سابق، ص87.

المبحث الثاني

الأدلة الإلكترونية وإجراءات جمعها وتحليلها

فتحت التكنولوجيا بابًا جديدًا لأنواع لم تكن معهودة من الجرائم، جرائم قد يغيب عن العيان مشهد مرتكبيها، بل ويغيب حتى الجاني عن مكان الضحية، جرائم عابرة للقارات، سلاح المجرم فيها خبرة تكنولوجية عالية يوظفها في خدمة أهداف غير مشروعة، مستغلًا قدرته على إتلاف الأدلة للإفلات من العقاب، ومستغلًا عدم وسمه بسمات المجرم التقليدي ليبقى متخفيًا حتى عن أقرب الناس إليه[1].

ولما كانت الدعوى الجنائية لا تصل للمحاكم المختصة إلا بعد أن تتهيأ لذلك عن طريق القيام بإجراءات معينة بغية الحصول على الأدلة التي تثبت ارتكاب الجريمة وكيفية وقوعها وبيان أسبابها، وإثبات ارتكابها أو نفيها ممن أسندت إليه[2].

فلا شك أن الجوانب الإجرائية المتعلقة بالإنترنت هي أهم محور من محاور البحث في كافة الموضوعات ذات الصلة بالعالم الافتراضي، الذي تولد عن تشابك الحاسبات، فالقاعدة الموضوعية وحدها لا تكفي للتفاعل مع الوقائع والأفعال المرتكبة عبر الإنترنت، ما لم يكن هناك تتبع إجرائي قانوني يكفل صحة وسلامة الإجراءات المتبعة[3].

ولذلك تبدو خطورة الإثبات هنا في كون الدليل ليس دليلًا ماديا مع ما قد يحيط به من عدم الوضوح، مما قد يضعف من ثقة جهات التحقيق والمحاكمة فيه[4].

فإبراز الدليل الرقمي وحمايته هو المهمة الشاقة لنظم العدالة الجنائية، وهذه المهمة تحتاج إلى مزيد من الوعي بموضوعات تكنولوجيا المعلومات وتطوراتها، فالحوسبة الرقمية أداة تضع الحلول، بل انه ليس هناك أفضل من الحوسبة الرقمية تحديدًا في وضع الحلول لمعضلات الدليل، بحيث لا يكون

---

[1] د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992م، ص8.

[2] د. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، مطبعة جامعة عين شمس، القاهرة، 1978م، ص37.

[3] د. سالم مبارك سليم، الحماية الجنائية للأدلة المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة،2019م، ص1.

[4] المرجع السابق، ص3.

على المشرع سوى البحث في الضمانات التي تشكل القدر اللازم من حقوق الإنسان[1]، وسوف نتناول هذا المبحث من خلال المطلبين التاليين.

المطلب الأول

مفهوم الدليل الإلكتروني وخصائصه

يعد الدليل الإلكتروني من المفاهيم الحديثة في مجال القانون، وهو الذي برز مع التطور السريع في التكنولوجيا واعتماد الأفراد والمؤسسات على الوسائل الرقمية في التفاعل والتواصل، ويتمثل الدليل الإلكتروني في البيانات أو المعلومات التي يتم استرجاعها من الأجهزة الرقمية مثل الحواسيب والهواتف الذكية وشبكات الإنترنت، والتي تستخدم في الإثبات القانوني.

يتميز الدليل الإلكتروني بمجموعة من الخصائص الفريدة التي تجعله مختلفًا عن الأدلة التقليدية من حيث كيفية جمعه وتخزينه وتحليله.

الفرع الأول

تعريف الدليل الإلكتروني

الدليل لغة المرشد، وهو ما يُستدل به[2]، والدليل الدال أيضًا[3]، والدال قريب المعنى من الهدى وهما في السكينة والوقار في الهيئة والمنظر والشمائل وغير ذلك، وفى الحديث "كان أصحاب عبد الله يرحلون إلى عمر – رضى الله عنه – فينظرون إلى سمته وهديه ودلًه فيتشبهون به[4].

والدليل في اصطلاح الشرعيين هو ما يلزم من العلم به العلم بشيء آخر، كالنهى عن التأفيف في قوله تعالى: "فَلَا تَقُل لَّهُمَا أُفٍّ"[5] يستدل به على حرامة الضرب وغيره مما فيه نوع من الأذى[6].

---

[1] د. عمر محمد أبوبكر بن يونس، الدليل الرقمي، الجمعية العربية لقانون الإنترنت، ط1. 2007م، ص13 – 14.

[2] المعجم الوسيط، مجمع اللغة العربية، ط4. مكتبة الشروق الدولية، 1425هـ – 2004م، ص294.

[3] محمد بن أبى بكر عبد القادر الرازي، مختار الصحاح، ص209.

[4] د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، ط2. دار النهضة العربية، القاهرة، 2008. هامش ص69.

[5] سورة الإسراء، من الآية 23.

[6] على محمد السيد الشريف الجرجاني، معجم التعريفات، دار الفضيلة، ص91. 92.

أما في الاصطلاح القانوني فقد تعددت التعريفات التي أعطيت للدليل، فقد قيل بأنه: "الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها، والمقصود بالحقيقة في هذا الصدد هو كل ما يتعلق بالوقائع المعروضة عليه لتطبيق حكم القانون عليها"[1]،

وقيل هو الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهى إليه، وذلك لأن مرحلة الحكم هي المرحلة الضرورية التي تقرر المصير النهائي في الدعوى الجنائية، وتفصل بين الإدانة والبراءة، وذلك إما بتحقيق حالة اليقين لدى القاضي فيحكم بالإدانة، أو ترجيح موقف الشك لديه فيحكم بالبراءة[2].

ويخلط البعض – أحيانًا – بين الدليل الجنائي والإثبات لما بينهما من علاقة في الإجراءات القضائية، ولكن عند التمحيص نجد أن الإثبات عملية متكاملة تهدف إلى البحث عن الأدلة التي تثبت حدوث الواقعة الجنائية وظروف ارتكابها وأسبابها ونسبتها إلى مرتكبيها وتقديمهم للعدالة، ولكن دور الدليل ينحصر في إقناع المحقق والقاضي بتورط الجاني في اقتراف الجريمة أو براءة ساحته منها[3].

وبذلك فإن مفهوم الإثبات أوسع نطاقًا من مفهوم الدليل، فكلمة الإثبات تشمل جميع الإجراءات الشكلية والموضوعية اللازمة لكشف الحقائق، وتبدأ بتلقي البلاغ أو الشكوى، وتمر بمرحلة المعاينة وجمع الأدلة والتفتيش والضبط والاستجواب والمحاكمة.

وقد أدى استخدام وسائل التقنية الحديثة إلى ثورة علمية في مجال الإثبات الجنائي، نتج على إثرها إمكانية الاستعانة بالأدلة الرقمية في عملية الإثبات الجنائي بوسائل التقنية الحديثة، مع ما يثيره هذا الأمر من تساؤلات حو إمكانية وضع تعريف جامع مانع له، مع بيان خصائصه وأنواعه.

وفى إطار المحاولات للوصول إلى تعريف لدليل الإثبات الجنائي الرقمي صنف البعض الأدلة الرقمية إلى نوعين، الأول منها أدلة أعدت لتكون وسيلة إثبات، كالسجلات التي تم إنشاؤها بواسطة

---

[1] د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2016م، ص507.

[2] د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، ط2. دار النهضة العربية، القاهرة، 2008. هامش ص70.

[3] د. محمد محمد عنب، استخدام التكنولوجيا الحديثة في الإثبات الجنائية، 2007م، ص9.

الآلة تلقائيًا مثل سجلات الهاتف، والسجلات التي تم حفظ جزء منها بالإدخال وجزء تم إنشاؤه بواسطة الآلة، كالبيانات التي إدخالها إلى الآلة وتتم معالجتها من خلال برنامج خاص، وثانيها أدلة لم تعد لتكون وسيلة إثبات، وهذا النوع من الأدلة الرقمية عبارة عن أثر يتركه الجاني دون أن يكون راغبًا في وجوده، ويسمى "بالبصمة الرقمية"، والتي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل أو استقبال الرسائل المرسلة منه أو إليه، وكذلك كافة الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العنكبوتية، ومن الجدير بالذكر أن الوسائل التقنية الخاصة والحديثة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من وقت نشوئها[1].

ويؤخذ على هذا التصنيف أنه تجاهل التطور السريع الحادث في مجال تكنولوجيا المعلومات، وما ترتب على ذلك من وجود أدلة رقمية أخرى، كالأدلة الرقمية التي يتم إعدادها للربط بين أجهزة الحواسب المتعددة، وكذلك تلك التي تتولى الربط بين الخوادم عبر الشبكات الخاصة، وكذلك شبكات الإنترنت، فالأمر لم يعد يقتصر على الحاسب فقط.

وفى محاولة أخرى عرفت المنظمة العالمية لدليل الكمبيوتر IOCE في مارس 2000م الدليل الرقمي بأنه المعلومات المخزنة أو المنقولة والتي يمكن الاعتماد عليها أمام المحكمة، ثم عرفته في أكتوبر 2001م بأنه المعلومات ذات القيمة المحملة والمخزنة أو المنقولة في صورة رقمية، ويؤخذ على التعريفين تجاهل الأول الصيغة التي تم بها تخزين المعلومات، في حين أن الثاني تجاهل الجهة التي سيقدم إليها الدليل الرقمي[2].

وعلى الجانب الآخر تعددت الاجتهادات الفقهية لتعريف الدليل الرقمي، وقد تنوعت تلك الاتجاهات على النحو التالي:

---

[1] حنان محمد الحسيني، سحر على عبد الله، التحقيق الجنائي الرقمي، مجلة جامعة الملك سعود، كلية الحقوق والعلوم السياسية، المجلد 33. العدد2. 2021م، ص136.

[2] د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1. مطبعة الشرطة، 1430هـ – 2009م، ص214. 215.

الاتجاه الأول: ربط التعريف بفكرة المعلومة:

حيث ذهب هذا الاتجاه إلى القول بأن الدليل الجنائي الرقمي هو:" معلومات مستندة إلى المنطق والعلم، يتم الحصول عليها من خلال إجراءات قانونية وعلمية عبر تحليل البيانات الرقمية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الاتصال، ويمكن استخدام هذه المعلومات في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة تتعلق بفعل أو شيء أو شخص يرتبط بالجريمة أو الجاني أو الضحية"[1].

الاتجاه الثاني: ربط التعريف بالبيئة الرقمية:

حيث عرف الدليل الجنائي الرقمي بأنه:" الدليل المستخرج من أجهزة الحاسب الآلي يأتي في صورة مجالات أو نبضات مغناطيسية أو كهربائية، ويمكن تجميعه وتحليله باستخدام برامج وتطبيقات وتقنيات متخصصة، ليُقدم كدليل يُعتمد عليه أمام القضاء، ويتكون هذا الدليل الرقمي من معلومات متنوعة تشمل النصوص المكتوبة والصور والأصوات والأشكال والرسوم، مما يسهم في الربط بين الجريمة والمجرم والضحية، ويُعتبر مستندًا قانونيًا قابلًا للاستخدام أمام جهات إنفاذ القانون"[2].

الاتجاه الثالث: ربط التعريف بالواقعة الرقمية:

حيث ذهب إلى تعريف الدليل الجنائي الرقمي بأنه:" الدليل المستند إلى العالم الافتراضي، والذي يمكن أن يكشف عن صلة بالجريمة، فهو يستند إلى استخدام تقنيات معالجة المعلومات الرقمية، ويقنع قاضي الموضوع بثبوت ارتكاب شخص ما للجريمة عبر الإنترنت."[3].

وبذلك يمكن اعتبار الدليل الرقمي دليلًا مستخرجًا من أو بواسطة النظم البرمجية المعلوماتية وأجهزة الحاسوب ومعداتها، أو من خلال شبكات الاتصال، ويجمع وفق إجراءات قانونية وفنية ليُقدَّم

---

[1] د. محمد الأمين البشري، الأدلة الجنائية الرقمية: مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد 17. العدد 33. 2002م، ص109.

[2] د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1. مطبعة الشرطة، 1430هـ – 2009م، ص217.

[3] د. خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية، 2014م، ص98.

للقضاء بعد تحليله علميًا أو تفسيره. ويأتي هذا الدليل في شكل نصوص مكتوبة أو رسومات أو صور أو أشكال أو أصوات لإثبات وقوع الجريمة والمساعدة في تقرير الإدانة أو البراءة[1].

الفرع الثاني

خصائص وأنواع الدليل الإلكتروني

ان كان الدليل الجنائي يتميز بعدة خصائص عامة أهمها ضرورة اتسامه بالوضوح والعقلانية والإقناع والمشروعية، فهي سمات تدخل بالضرورة في خصائص الدليل الإلكتروني، ويبقى للدليل الإلكتروني خصائصه التي تميزه كونه جزءً من البيئة الرقمية بجميع مكوناتها من برمجيات وقطع صلبة وغيرها، والتي تحكمها قواعد علمية تحكم التعامل خلالها والولوج عبر أرجائها[2]، ولذلك يتميز الدليل الرقمي بعدة خصائص من أهمها:

1. **الطابع التقني للدليل الرقمي:** إن الطبيعة العلمية للدليل الرقمي تقتضي التعامل مع هذا النوع من الأدلة الجنائية العلمية من قبل تقنيين في البيئة الافتراضية، فالطبيعة التقنية تقتضي أن يكون هناك توافق بين الدليل المستخلص والبيئة التي يكون فيها، لأن التقنية لا تنتج لنا سكين يتم به الكشف عن القاتل وإنما تنتج نبضات أو مجالات مغناطيسية أو كهربائية[3].
2. **استخلاص الدليل بأساليب علمية:** يخضع الدليل الرقمي لكافة القواعد المطبقة على الأدلة العلمية، مما يتطلب عدم تعارضه مع المبادئ العلمية السليمة. وقد نتج عن ذلك ظهور قواعد علمية مخصصة لاستخلاص الدليل الرقمي في الوقائع المجرمة قانونًا، والتي تُعرف بعلم الحاسب الجنائي، ويختص هذا العلم بوضع القواعد التي يجب أن يلتزم بها المحققون أثناء

---

[1] د. أنيس حسيب السيد المحلاوي، الخبرة القضائية في الجرائم المعلوماتية أو الرقمية، دار الفكر الجامعي، الإسكندرية، 2016م، ص56.

[2] د. خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية، 2014م، ص117.

[3] د. أحمد مالك، د. إبراهيم الخال، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، المركز الجامعي، الجزائر، المجلد5. العدد1. 2021م، ص109.

فحص الوقائع التي تمت باستخدام أجهزة التقنيات الرقمية والاتصال بالإنترنت[1].

نظرًا لأن الدليل الرقمي يُستمد من أنظمة معلوماتية، فهو يتمتع بطبيعة فنية بحتة تعتمد على استخدام تقنيات علمية، ولذلك يتوجب على المحكمة تعيين خبير في القضية للحصول على هذا الدليل، كي يتمكن القضاء من تقييم مدى صلاحية الدليل الرقمي المقدم، يجب على الخبير أن يعيد بناء كيفية استخلاصه والطريقة التي تم بها معالجة الدليل. ويتطلب ذلك أن يكون القاضي ملمًا بالقدر الكافي من المعلومات التي تمكنه من تقييم صحة الدليل المستخلص والتأكد من عدم التلاعب به[2].

3. **الدليل الرقمي دليل متطور:** تتميز علوم النظام الرقمي بكونها ليست من العلوم التقليدية الجامدة ولكن المتطورة بصورة سريعة جدًا، كما أن هذا التطور ليس مقصورًا على المؤسسة العلمية المختصة أو الوكالات المتخصصة في هذا المجال ولكن أيضًا تساهم به الافراد ذوو الخبرة من شتى بقاع الأرض[3].

وخاصية التطور التي يتمتع بها الدليل الرقمي ناتجة عن تزايد استخدام تقنية المعلومات الرقمية، بعد ان اصبحت اجهزة الحاسب الالي وشبكة الانترنت تشكل مستودعا هاما للمعلومات والبيانات الرقمية[4].

4. **صعوبة التخلص من الدليل الرقمي:** تعد هذه الخاصية من أهم خصائص الدليل الرقمي، ويشترك مع الدليل الرقمي في هذه الميزة الدليل الجيني أو دليل DNA، فيتحد كل منهما في صعوبة التخلص منها بالمقارنة بالأدلة التقليدية، فيجب على القائمين على العمل بقانون الإجراءات الجنائية بسرعة الوصول الى مسرح الجريمة حتى لا تضيع آثار ارتكاب الجريمة،

---

[1] د. خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية، 2014م، ص119.

[2] Ralph Clifford, Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime, Carolina Academic Press, USA, 2001, p، 113.

[3] د. خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية، 2014م، ص123.

[4] د. أحمد مالك، د، إبراهيم الخال، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، المركز الجامعي، الجزائر، المجلد5. العدد1. 2021م، ص109.

فمن الطبيعي أن يسعى المتهم إلى التخلص من أدلة ارتكابه للجريمة كما يمكن العبث بطريق الخطأ في مسرح ارتكاب الجريمة وأن يفسد أو يضيع أدلة ارتكاب الجريمة، وعلى سبيل المثال فإن بصمات الأصابع بمسرح الجريمة تصبح محل شك إذا طالت المدة بين ساعة ارتكاب الجريمة وبين الحصول عليها[1].

ويتميز العالم الرقمي بأن المعلومات التي يتم تخزينها في وسائط التخزين الثابتة والمتحركة، يمكن التعامل معها بالمحو أو مسحها من خلال خواص نظام التشغيل، ولكن هذا الأمر لا يعني أنه لا يمكن استرجاع هذه المعلومات، حيث إن برامج التشغيل مثل الويندوز تعمل من خلال DOS والذي يحتفظ بالمعلومات التي تم حذفها من نظام التشغيل، فيمكن من خلال استخدام بعض البرامج استرجاع هذه المعلومات[2]، فهو ليس مثل الدليل المادي يمكن تحريفه، أو حتي طمسه، وهو ما سهل إثبات الجريمة أو نفيها بدرجة كبيرة من اليقين والجزم، ذلك الجزم الذي يجب أن تقوم عليه الأحكام بالإدانة في الجرائم، وليس مجرد الظن والاحتمال[3].

ففي حالة محاولة إصدار أمر بإزالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الالة التي تحتوي على ذلك الدليل، بل إن محاولة محو الدليل تعد في حد ذاتها دليل، لأنه في حالة القيام بتلك العملية يتم تسجيلها في ذاكرة الالة استخراجه كدليل ضد من قام بالفعل، ويمكن أيضًا عرض الدليل الرقمي على برامج وتطبيقات لمعرفة اذا كان قد تعرض للعبث أو التحريف[4]، كذلك يمكن التعرف على تاريخ نشأة الملف وآخر تعديل عليه وآخر مرة تم فتحه فيها[5].

---

[1] د. خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية، 2014م، ص124. 125.

[2] Kenneth Rosenblatt, High-Technology Crime: Investigating Cases Involving Computers, KSK Publications, USA, 1995, p ،260.

[3] Stephan Caidi, La prevue et la conservation de l'ecrit dans la societe d' information, Ph D Thesis, Universite de Monteral, 2002, p.24.

[4] د. أحمد مالك، د. إبراهيم الخال، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، المركز الجامعي، الجزائر، المجلد5. العدد1. 2021م، ص109.

[5] Ricordel, I., L'expertise en police scientifique, Dalloz, 2015, p.398.

وبذلك يتبين لنا أن الدليل الرقمي بصفة عامة له خصائصه التي تميزه عن غيره من أدلة الإثبات الأخرى، فبالإضافة إلى ما تم إقراره من خصائص يمكن لهذا الدليل الرقمي أن يسجل تحركات الفرد وعاداته وسلوكياته، كما يمكن أيضًا أن يمس بحريته الشخصية.

فقد وضعت أجهزة التقنيات الرقمية المعلومات في قالب جديد، فاستحدثت العديد من الوسائل التي يتم بها عرض وتداول المعلومات وفقًا للمفهوم الرقمي، وذلك أضفى عليها بعدًا جديدًا في مفهومها وطريقة التعامل معها على الصعيد القانوني[1].

ويتداول الفقه ثلاثة مصطلحات للمعلومات كمصدر للدليل الرقمي هي: البيانات والمعلومات والمعلوماتية، فيرى البعض أن **البيانات** هي مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض، ولم تخضع بعد للتفسير أو التجهيز للاستخدام والتي تخلو من المعنى الظاهر في أغلب الأحيان، وقد بينت التوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية عام 1992م، الخاصة بحماية أنظمة الحاسبات الآلية وشبكة المعلومات في تعريفها للبيانات عن أنها: "مجموعة من الحقائق أو المفاهيم أو التعليمات تتخذ شكلًا محددًا يجعلها قابلة للتداول أو التفسير أو للمعالجة بواسطه الأفراد أو بوسائل إلكترونية"[2].

أما **المعلومات** هي المعنى الذي يستخلص من هذه البيانات، وأما **المعلوماتية** فهي تشمل الحواسيب الآلية ووسائل الاتصال وشبكة المعلومات والبيانات والمعلومات، التي يمكن تخزينها ومعالجتها واسترجاعها ونقلها بواسطة هذه الحواسيب أو وسائل الاتصال أو شبكات المعلومات بما في ذلك برامج الحواسيب الآلية وجميع القواعد اللازمة لتشغيل هذه الأنظمة والحفاظ عليها[3].

---

[1] د. خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية، 2014م، ص109.

[2] د. هشام فريد رستم، الجوانب الإجرائية في الجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، 1994م، ص28.

[3] David O'Connor, Andrea Goldstein, E-commerce for Development: Prospects and Policy Issues, OECD Development Centre, 2000, p.23،

ويتضح من ذلك أن النظرة للمعلومات تأخذ في الاعتبار مختلف الحقائق التي تتفق مع طبيعة المعلومة ونظامها فتشمل تبعًا لذلك: المناظرة والأصوات، الأشكال المختلفة للأشياء، الرسوم، الأفكار، وكل ناتج غير مادي لصناعة الإنسان[1].

وتشمل الأدلة الجنائية الإلكترونية جميع البيانات الرقمية التي يمكن أن تثبت بأن هناك جريمة تم ارتكابها، أو توجد علاقة تربط بين الجريمة والجاني أو توجد علاقة بين الجريمة والمتضرر منها، والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت أو الصورة[2].

وبناءً عليه ثار جدل فقهي حول مكانة الأدلة الرقمية من بين الأدلة المادية، فهل تُعد نوعًا متطورًا من الأدلة المادية لكونها ناتجة من عناصر مادية ملموسة، أم أنها أدلة فنية لانبعاثها من رأي خبير فني ووفق معايير علمية معتمدة، وفي إطار هذا الأمر هناك اتجاهين فقهيين:

حيث يرى أنصار الاتجاه الأول أن الأدلة الجنائية الإلكترونية مرحلة متقدمة من الأدلة المادية الملموسة، التي تدرك بالحواس، سواء كانت على شكل مطبوعات مستخرجة من الحاسوب باعتباره مصدر لها، فهي بمفهوم هذا الاتجاه لا تختلف عن مفهوم الأدلة العلمية كآثار الأسلحة والبصمة الوراثية[3]،

والاتجاه الثاني فهو عكس الاتجاه الأول، حيث يذهب أنصاره إلى القول بأن الأدلة الرقمية نوع متميز من وسائل الإثبات، ما يؤهلها لتقوم كإضافة جديدة إلى باقي الأدلة الجنائية، ومنه نخلص إلى القول إن الرأي الأول غير صائب ولا يمكن الأخذ به، باعتبار أن الأدلة الإلكترونية ليست مادية فقط، والرأي الراجح هو الرأي الثاني باعتبار أن الأدلة الإلكترونية تتمتع بخصائص جعلتها مختلفة عن الأدلة الجنائية التقليدية[4]،

---

[1] د. بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، ط1. دار الفكر الجامعي، الإسكندرية، 2011م، ص15.

[2] Eoghan Casey, Digital Evidence and Computer Crime, Academic Press, London, 2000, p.260.

[3] د. سامي جلال، الأدلة المتحصلة من الحاسب وحجيتها في الإثبات، دار الكتب القانونية، القاهرة، 2011م، ص59.

[4] أنظر د. أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، القاهرة، 2015م، ص21.

وفي هذا الصدد، سوف نقوم بالتعرض لأنواع الدليل الرقمي، وذلك بدءً بالحديث عن التقسيمات الفقهية للدليل الرقمي، ثم التقسيمات التشريعية والقضائية لذلك الدليل.

أولًا: التقسيمات الفقهية للدليل الرقمي:

لم يتطرق فقهاء القانون الجنائي إلى دراسة الدليل الرقمي بشكل واسع، وهذا راجع إلى الحداثة النسبية لهذا الدليل من جهة، والتطور المتلاحق من جهة أخرى، وقد قسم البعض الدليل الرقمي إلى الأقسام الرئيسية التالية[1]:

1. أدلة رقمية خاصة بأجهزة الحاسب الآلي وشبكاتها:

وهي سلوك غير إنساني يشكل فعل غير مشروع على أجهزة الكمبيوتر، سواء وقع هذا الأمر على المكونات المادية له أو المكونات المعنوية، أو قواعد البيانات الرئيسية، مثل تخريب مكونات الكمبيوتر كالطابعة.

2. أدلة رقمية خاصة بالإنترنت:

وهي سلوك إنساني يشكل فعلًا غير مشروع قانونًا، يقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات، مثل جرائم الدخول غير المشروع لمواقع يمنع الدخول إليها، واستخدام عناوين IP غير حقيقية للولوج إلى الشبكة العالمية للمعلومات وغيرها[2].

3. أدلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات:

وهي متعلقة بالجرائم التي ترتكب باستخدام الكمبيوتر، بحيث لا يعتبر استخدام الكمبيوتر أو الشبكة العالمية للمعلومات أو الإنترنت في هذه الجرائم من طبيعة الفعل الجرمي، بل تستخدم كوسيلة

---

[1] د. وهيبة لعوارم، الدليل الرقمي في مجال الإثبات الجنائي وفقًا للتشريع الجزائري، المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، مجلد57. العدد2. 2014م، ص83.

[2] د. أسامة حسين محيي الدين، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية (دراسة تحليلية مقارنة)، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 76. 2021م، ص656.

مساعدة لارتكاب الجريمة مثل غسيل الأموال أو نقل المخدرات من مكان لآخر، وجهاز الكمبيوتر في هذه الحالة يحتفظ بآثار إلكترونية يمكن أن تستخدم للإرشاد عن الفاعل[1].

وإن هذا التقسيم للدليل الإلكتروني، وإن كان يتناسب مع تقسيم الفقه للجرائم عبر الكمبيوتر إلا أنه غير متناسب مع مفهوم التقنية الحديثة، فكل هذه التقسيمات تدور حول موضوع واحد ألا وهو الدليل الإلكتروني، إلا أنها ميزت بين شبكات الكمبيوتر والإنترنت وبروتوكول تبادل المعلومات والشبكة العالمية للمعلومات التي هي في الأصل واحد، لكنها تختلف في المصطلحات.

ومنه نخلص إلى القول إن هذا التقسيم لم يشمل كل ما يتعلق بالدليل الإلكتروني، إذ أنه لم يأخذ بعين الاعتبار التقنية الحديثة التي ظهر بظهورها هذا الدليل.

ثانيًا: التقسيمات التشريعية والقضائية لتقسيم الدليل الرقمي:

برزت عدة تشريعات حاولت تقسيم الدليل الرقمي، وإحاطة كل ما يتعلق به، والقضاء أيضًا كان له دور في معالجة موضوع الدليل الرقمي، إلا أن تشريع الولايات المتحدة الأمريكية كان من السباقين الذين تطرقوا للدليل الرقمي[2].

ففي عام 2002م قررت وزارة العدل الأمريكية تقسيم الدليل الرقمي إلى ثلاث مجموعات هي[3]:

1. السجلات المحفوظة في الحاسوب: وهي عبارة عن وثائق مكتوبة ومحفوظة، كالبريد الإلكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الإنترنت.
2. السجلات المحفوظة جزئيًا في الحاسوب: يتم إنشاء هذا النوع من السجلات بواسطة الحاسوب، فهي تعتبر مخرجات برامج الحاسوب، أي أنه لم يتم لمسها من قبل الأشخاص مثل log, files، وسجلات الهاتف، وكذا فواتير أجهزة السحب الآلي ATM .

---

[1] د. أسامة حسين محيي الدين، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية (دراسة تحليلية مقارنة)، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 76. 2021م، ص656.

[2] د. أسامة حسين محيي الدين، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية (دراسة تحليلية مقارنة)، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 76. 2021م، ص657.

[3] د. وهيبة لعوارم، الدليل الرقمي في مجال الإثبات الجنائي وفقًا للتشريع الجزائري، المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، مجلد57. العدد2. 2014م، ص82. 83.

3. السجلات المحفوظة للإدخال والمنشأة بواسطة الحاسوب: ومن أمثلتها أوراق العمل المالية التي تحتوي على مدخلات تم تلقيمها إلى برامج أوراق العمل مثل (EXCEL)، ثم تمت معالجتها بإجراء العمليات الحسابية.

وهذا التقسيم هو نفس التقسيم الذي أخذ به القضاء الأمريكي، فسجلات الحاسوب المقبولة أمام القضاء الأمريكي، هي التي تكون في شكل نصوص، وهذا إما في هيئة سجلات الحاسوب المتوالدة، أو سجلات الحاسوب المخزنة، والفرق بينهما يكمن فيما إذا كان الشخص هو المنشئ لمحتوى هذه السجلات أو الآلة، فسجلات الحاسوب المخزنة تشير إلى الوثائق التي تحتوي على كتابات شخص، أو بعض الأشخاص في شكل إلكتروني مثل رسائل البريد الإلكتروني، أما فيما يخص سجلات الحاسوب المتوالدة فالكمبيوتر هو الذي يصدرها، فهي تحتوي على مخرجات برامج الحاسوب مثل سجلات الدخول على الإنترنت ومصدرها مزود خدمة الإنترنت، بالإضافة إلى نوع ثالث من السجلات الذي يجمع بين التدخل الإنساني ومعالجة الكمبيوتر، مثلًا كما لو أدخل متهم بيانات معينة ويطلب من الكمبيوتر معالجتها للوصول إلى نتائج يسمح بها البرنامج المستخدم، كالشخص الذي يتهرب من الضرائب فيسجل بيانات غير صحيحة عن دخله وربحه، طالبًا من الكمبيوتر حساب الضريبة المستحقة[1].

إلا أن ما يؤخذ على هذه التقسيمات أنها ليست شاملة للدليل الرقمي، بل اقتصرت على نوع واحد، وهو سجلات الحاسوب المحتوية على نص، بالرغم من أن الدليل الإلكتروني يشمل كافة البيانات الإلكترونية الممكن تداولها إلكترونيا، كالصور والأصوات والرسوم وغيرها، فنجد حاليًا بروتوكولات الاتصالات والتطبيقات المعلوماتية التي تستخدم في تحقيق الجرائم الإلكترونية ويعتبر نظام TCP / IP من أكثر البروتوكولات المستخدمة في شبكة الإنترنت، فهي جزء أساسي منه فهي تدل بصفة يقينية عن مصدر الجهاز الذي استخدم في الجريمة، كما تحدد الأجهزة التي أصابها الضرر من هذا الفعل الإجرامي[2].

---

[1] د. أسامة حسين محيي الدين، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية (دراسة تحليلية مقارنة)، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 76. 2021م، ص659.

[2] المرجع السابق. ص659.

فالتنوع في الدليل الرقمي مفاده أنه لا توجد وسيلة واحدة للحصول عليه، وإنما هي متعددة وفي كل الأحوال يبقى الدليل إلكترونيا حتى وإن اتخذ هيئة أخرى، وفي هذه الحالة فإن اعتراف القانون لهذا النوع من الأدلة يكون مؤسسًا على طابع افتراضي بيني على أساس الدليل الإلكتروني، فإنه لابد من اتخاذ مسلك الافتراضي باعتبار هذا الدليل دليلًا أصليًا، نتيجة إلى نقص توافر الإمكانيات الإلكترونية في المحاكم الجنائية التي تنظر في هذا النوع من الأدلة[1].

ثالثًا: تقسيمات أخرى للدليل الرقمي:

تتخذ المعلومات المعالجة رقميًا من أجهزه الحاسب شكل مجالات مغناطيسية أو نبضات كهربائية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة، وتقديمها في شكل دليل معتمدة أمام القضاء[2]، وذلك على النحو التالي:

1. الأشرطة المغناطيسية Magnetic tape: هذا الشريط هو عبارة عن شريط بلاستيكي مغطى بمادة قابلة للمغنطة. قد يكون ملفوفًا على بكرة، كما في أجهزة التسجيل الصوتي، أو داخل علبة على هيئة شريط فيديو أو شريط كاسيت. تحتوي جميع الأشرطة المغناطيسية على رأس للقراءة والكتابة، الذي يسجل البيانات على الشريط في شكل نقاط مغناطيسية باستخدام شفرة خاصة تمثل البيانات المستخرجة من الحاسوب. يستطيع هذا الرأس اكتشاف وجود هذه النقاط وإرسال النبضات الكهربائية المقابلة لشفرة البيانات إلى داخل الحاسوب. يتم استخدام الشريط المغناطيسي لتخزين البرامج والملفات المتتالية، التي تتطلب قراءة الشريط من بدايته. يتم تنظيم المعلومات على الشريط في شكل وحدات خاصة تُسمى "حزم"، ويحدد المستخدم حجم كل حزمة. تُعامل الحزمة كوحدة متكاملة عند تخزينها أو إخراجها من الشريط[3].
2. الأقراص المغناطيسية disk Magnetic: تعتبر الأقراص المغناطيسية من أفضل وسائط التخزين نظرًا لقدرتها العالية على التخزين المباشر والعشوائي. من أهم خصائصها أنها تسمح بالقراءة أو التسجيل على

---

[1] د. سامي جلال، الأدلة المتحصلة من الحاسب وحجيتها في الإثبات، دار الكتب القانونية، القاهرة، 2011م، ص59.

[2] د. خالد مصطفى الجسمي، الإثبات الجنائي بالأدلة الرقمية، دار السلام للطباعة والنشر، العدد34. 2017م، ص26.

[3] د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 1997م، ص27.

أي قطاع من السطح، كما يمكن تعديل أو تغيير أي ملف عليها دون الحاجة إلى إنشاء ملف جديد، حيث يتم تعديل السجل وهو في مكانه. هناك عدة أنواع من الأقراص المغناطيسية، من بينها:

أ. القرص المرن Floppy disk: يعتبر القرص المرن أحد أشهر وسائط تخزين البيانات، وينتشر استخدامه في الحواسيب الصغيرة والمتوسطة، وذلك لسهولة استخدامه وتداوله، ويمكن مسح البيانات من القرص وإعادة تخزينها عدة مرات دون أن يفقد القرص المرن كفائته[1].

ب. القرص الصلب Hard disk: هو عبارة عن قرص معدني رقيق، ومغطى بمادة قابلة للمغنطة، ويتميز بالسعة التخزينية وكذلك سرعة تسجيل واسترجاع البيانات، وبعدم إمكانية تحريكه من مكانه، لذا يطلق عليه أحيانًا اسم القرص الثابت Fixed disk ويكون عادة داخل جهاز الحاسوب[2].

ج. قرص الخرطوش أو قرص الكارتريدج Cartridge disk: وهو قرص هجيني يجمع بين خصائص القرص الصلب من حيث كبر حجم السعة التخزينية وبين القرص المرن في إمكانية تغييره من مكانه بقرص آخر[3].

د. المصغرات الفيلمية Computer out Microfilm (COM): تعتبر هذه الأدلة أحد الأشكال المختلفة في تكنولوجيا المخرجات، والتي تسجل فيها المعلومات والبيانات، بدلًا من تسجيلها على الورق، وهي عبارة عن أفلام فوتوغرافية يتم استخدامها في تصوير صفحات البيانات مع تصغيرها لدرجة متناهية عن طريق جهاز تحويل للبيانات المسجلة على الأشرطة والأقراص الممغنطة تتراوح سرعته من عشرة الآف إلى أربعين ألف سطر في الدقيقة الواحدة[4].

ويلاحظ أن هذه التقسيمات قد ألمت بجانب كبير ومهم من الأدلة الرقمية، وأن هذا النوع في الدليل يفيد أنه ليس هناك وسيلة واحدة للحصول عليه وإنما تتعدد هذه الوسائل أيضا[5].

---

[1] د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 1999. ص18. 19.

[2] د. هلالي عبد اللاه أحمد، قانون العقوبات وأزمة الحاسبات، دار النهضة العربية، القاهرة، 1998. ص64.

[3] د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 1997م، ص26.

[4] د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق. ص19. 20.

[5] د. أسامة حسين محيي الدين، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية (دراسة تحليلية مقارنة)، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 76. 2021م، ص662.

المطلب الثاني

الوسائل المتبعة في التحري عن الجريمة الإلكترونية ومعوقاتها

منذ اعتداءات الحادي عشر من سبتمبر 2001م في الولايات المتحدة الأمريكية، أصبحت العلاقة بين جرائم الإرهاب والجريمة المنظمة من جهة، واستخدام الشبكة المعلوماتية من جهة أخرى، دافعًا نحو سن تشريعات جديدة تهدف إلى تعزيز فاعلية العدالة الجنائية في كشف وملاحقة ومعاقبة مرتكبي الجرائم عبر الشبكة المعلوماتية، وقد زادت الحاجة إلى البحث تشريعات جزائية أكثر فاعلية، عبر توفير إجراءات تحقيق حديثة يمكن لجهات التحقيق في الجرائم الإلكترونية استخدامها، حتى وإن أدى ذلك إلى التضحية ببعض المبادئ الأساسية والحقوق الجوهرية.

وتجدر الإشارة إلى أن هذه الإجراءات لا تقتصر على نوع محدد من الجرائم، بل تمتد لتشمل التحقيق في كافة الجرائم الإلكترونية التي تتم عبر أنظمة الحاسوب وغيرها من تقنيات الاتصالات.

الفرع الأول

إجراءات البحث والتحري في الجرائم الإلكترونية

أولًا: صلاحيات مأموري الضبط القضائي في مرحلة الاستدلال:

1. قبول البلاغات والشكاوى

يجب على مأموري الضبط القضائي قبول البلاغات والشكاوى التي ترد إليهم بشأن الجرائم الإلكترونية وإثباتها في محضر رسمي، والبلاغات التي يتم تقديمها من قبل أي شخص علم بوقوع الجريمة يجب أن تُعرض على النيابة العامة دون تأخير، ويختلف البلاغ عن الشكوى في أن البلاغ هو إخطار عام بالحادثة بينما الشكوى يقدمها المجني عليه أو المتضرر نفسه، ويتعين على مأموري الضبط القضائي تسجيل جميع البلاغات والشكاوى بشكل رسمي وإرسالها للنيابة العامة للتصرف.

2. جمع الاستدلالات:

يبدأ مأمور الضبط القضائي في جمع الاستدلالات بمجرد علمه بوقوع الجريمة الإلكترونية، سواء كان ذلك عبر بلاغ، شكوى، أو تحريات. الاستدلالات تشمل الأدلة والشهادات والقرائن التي تساعد في التحقيق، مثل المعاينة، الاستماع لشهادات الشهود، والاستعانة بالخبراء المتخصصين في الجرائم الإلكترونية، إضافة إلى ذلك، يمكن لمأمور الضبط القضائي إجراء المعاينات للأماكن المتورطة في الجريمة، مثل أجهزة الكمبيوتر أو الخوادم التي قد تحتوي على أدلة رقمية. كل هذه الاستدلالات تساهم في جمع الأدلة الضرورية لتحقيق العدالة.

3. إجراء المعاينات:

تتضمن المعاينة التي يقوم بها مأمور الضبط القضائي زيارة المكان الذي يشتبه في وجود أدلة تتعلق بالجريمة الإلكترونية، مثل غرفة الكمبيوتر أو مقر تخزين البيانات، ويتم فحص الأجهزة والأماكن بعناية لتوثيق الحالة المبدئية للأدلة، وفي حال كانت المعاينة تتطلب دخول مكان خاص مثل منزل أو مكتب، يجب الحصول على إذن قانوني من قبل الجهات المختصة. في حالة عدم الحصول على إذن، يعتبر الإجراء بمثابة تفتيش ويخضع لرقابة المحكمة.

4. التحفظ على أدلة الجريمة:

من أهم واجبات مأموري الضبط القضائي هو اتخاذ الإجراءات اللازمة لحماية الأدلة التي يتم جمعها، مثل وضع حراسة على الأجهزة الإلكترونية أو تخزين البيانات، ويجب التأكد من عدم العبث بالأدلة الرقمية التي قد تكون حاسمة في إثبات الجريمة. يشمل ذلك أيضًا تأمين الوثائق الإلكترونية أو سجلات الإنترنت التي قد تتضمن أدلة قد تساهم في كشف الجريمة.

5. سماع أقوال الشهود والخبراء:

يعد سماع أقوال الشهود من أبرز مهام مأموري الضبط القضائي في مرحلة الاستدلال، ويمكن لهم سماع شهادات الأشخاص الذين قد تكون لديهم معلومات هامة حول الجريمة الإلكترونية، مثل من شهد وقوع الجريمة أو من يملك معرفة فنية حول الأدلة الرقمية، كما يحق لمأموري الضبط القضائي

الاستعانة بالخبراء في مجالات مثل تحليل البيانات الرقمية أو الأمن السيبراني للحصول على تقارير تساعد في فهم الجريمة بشكل أعمق.

6. تحرير محضر الاستدلالات:

من الضروري أن يقوم مأمور الضبط القضائي بتوثيق جميع الإجراءات التي يتم اتخاذها أثناء جمع الاستدلالات في محاضر رسمية، وهذه المحاضر تشمل توقيع الضابط المعني بالأمر وكذلك توقيع الأشخاص المتورطين في الإجراءات مثل الشهود أو الخبراء، وينبغي أن تحتوي المحاضر على كافة التفاصيل المتعلقة بالتاريخ والوقت والمكان والفعاليات التي تمت في سبيل التحقيق.

7. إجراءات الاستدلال في حالة التلبس:

في حالات التلبس بالجريمة، يكون مأمور الضبط القضائي ملزمًا بالانتقال فورًا إلى مكان الجريمة الإلكترونية، وعليه أن يقوم بالمعاينة الفورية للأدلة الإلكترونية المتاحة وتحفظها بشكل صحيح، ويمكن لمأمور الضبط القضائي أن يستمع إلى أقوال الشهود أو الأشخاص المتواجدين في مكان الجريمة لتوثيق تفاصيل الواقعة بسرعة، كما أنه يجب أن يخطر النيابة العامة فورًا بكل التطورات.

8. القبض على المتهم

يمكن لمأموري الضبط القضائي في الجرائم الإلكترونية القبض على المشتبه بهم في حال وجود دلائل قوية على ارتكابهم الجريمة، وإذا كان هناك اشتباه في أن الشخص متورط في الجريمة الإلكترونية أو إذا تم ضبطه متلبسًا بها، يمكن للضابط اتخاذ إجراء القبض، ويجب أن يتم هذا الإجراء وفقًا للقانون مع احترام حقوق المشتبه به وحرياته الشخصية.

ثانيًا: دور السلطات القضائية في إصدار أوامر الحصول على البيانات الإلكترونية:

تتمثل الإجراءات الجديدة لجمع الأدلة في تمكين المحقق من إصدار أمر لمزود الخدمة للاحتفاظ بالبيانات المخزنة، وتقديم معلومات تتعلق بالمشترك في الخدمة[1].

1. الأمر بالتحفظ على بيانات مخزنة:

يهدف هذا الإجراء إلى منح السلطات المختصة بالتحقيق القدرة على إصدار أمر عاجل لمزود الخدمة للاحتفاظ ببيانات إلكترونية مخزنة لديه أو تحت سيطرته، وذلك بانتظار اتخاذ إجراءات أخرى مثل التفتيش أو طلب تقديم البيانات المخزنة. وتكمن أهمية هذا الإجراء في أن البيانات في البيئة الإلكترونية قابلة للمحو أو التعديل بسرعة، وقد يكون ذلك بنية إجرامية لإخفاء أدلة الجريمة أو هوية مرتكبها، مما يجعل أمر التحفظ إجراءً ضروريًا للحفاظ على البيانات قبل ضياعها. ومع ذلك، تظل هذه البيانات مرتبطة بالحق في الخصوصية، مما يعني أن التعرض لها يعد انتهاكًا لهذا الحق.

2. الأمر بتقديم بيانات مخزنه:

يتيح هذا الأمر للسلطات المختصة بالتحقيق إلزام مزودي الخدمة بتقديم بيانات بحوزتهم وتحت سيطرتهم تتعلق بالمستخدم، باستثناء البيانات المتاحة للجمهور، إذ ترتبط هذه البيانات بالحق في الخصوصية. ويشمل هذا الأمر نوعين من البيانات المتعلقة بالمستخدم:

- البيانات المتعلقة بالمرور التي تكون في الغالب في حيازة مزود الخدمة فقط:

هذه البيانات، التي تكون غالبًا بحوزة مزود الخدمة وحده، تعالج الاتصالات التي تمر عبر النظام المعلوماتي، وتشمل مصدرها ووجهتها ومسارها وتاريخها ووقتها ومدتها. وتتيح هذه البيانات إمكانية تتبع مسار الاتصال، مما يسهم في تحديد هوية المشاركين في ارتكاب الجريمة قيد التحقيق.[2]

---

[1] د. علي حسن محمد الطوالبة، مرجع سابق. ص205.

[2] حددت المادة (1) فقرة (د) من اتفاقية بودابست بيانات المرور على أنها أي بيانات كمبيوتر متعلقة باتصال عن طريق منظومة كمبيوتر، والتي تنشأ عن منظومة كمبيوتر تشكل جزءًا في سلسلة الاتصالات توضح مصدر الاتصال، والوجهة المرسلة إليها والطريق الذي تسلكه ووقت وتاريخ وحجم ومدة، وقوع الخدمة المذكورة"

– البيانات المتعلقة بالمحتوي، أي المعلومات المنقولة عن الطريق الإلكتروني:

هذه البيانات تتضمن المعلومات المنقولة إلكترونيًا، ورغم عدم وجود فرق جوهري في المضمون بين نوعي البيانات، إلا أن البيانات المتعلقة بالمحتوى تحمل أهمية أكبر للحق في الخصوصية، مما يستدعي حماية أكبر لها، ينبغي على سبيل المثال، أن يكون إصدار الأوامر المتعلقة بها من قبل سلطة قضائية وليس من مأموري الضبط القضائي، كما ينبغي تقييد هذه الأوامر بالجرائم الأكثر خطورة فقط.

الفرع الثاني

معوقات التحري وجمع الاستدلالات في الجرائم الإلكترونية

مما لا شك فيه التحري وجمع الاستدلالات في الجرائم الإلكترونية عملية معقدة وصعبة، نظرًا لطبيعتها الرقمية والتقنية المتطورة، وفي هذا السياق يواجه مأموري الضبط القضائي عدة معوقات في عدة جوانب، منها التقني، والقانوني، أحيانا الاجتماعي، والتي سوف نوجزها فيما يلي[1]:

أولًا: سهولة إخفاء الجريمة:

الجريمة المعلوماتية في أغلب الأحوال تكون مستترة خفية، فعلى سبيل المثال نجد أن اختلاس المال بواسطة التلاعب غير الشرعي، غالبا ما يحاول المختلس تغطيته وستره والتجسس على ملفات البيانات المختزنة، الأمر الذي يضعف إلى حد كبير فرصة المجني عليه في إثبات هذا الاختلاس بالنسبة لاختراق قواعد البيانات لتغير بعض محتوياتها والتخريب المنطقي للأنظمة باستخدام الفيروسات.

ثانيًا: نقص المعرفة الفنية لدى سلطات التحقيق ومأموري الضبط.

من التحديات التي تواجه عملية استخلاص الأدلة في الجرائم المعلوماتية هو نقص الخبرة لدى رجال الضبط القضائي وأجهزة الأمن بشكل عام، بالإضافة إلى سلطات الاتهام والتحقيق الجنائي في

---

[1] د. محمود صلاح العادلي، الفراغ التشريعي في مجال مكافحة الجرائم الإلكترونية، 2009، ص89.

العدالة الجنائية، هذا النقص يتعلق بفقدان ثقافة الحاسب الآلي وفهم كيفية التعامل مع التكنولوجيا.

بينت الوقائع أن بعض أفراد الضبط القضائي قد يقعون في حالات مساعدة مجرمي المعلوماتية عن طريق الخطأ، بسبب عدم امتلاكهم المعرفة اللازمة للتعرف على هذه الجرائم وطرق ارتكابها، هذا الوضع ينطوي على حاجة ملحة لتحسين التدريب والتأهيل لرجال الضبط القضائي، وتعزيز فهمهم للتقنيات المتقدمة المستخدمة في الجرائم المعلوماتية[1].

بالتالي، ينبغي على البلدان العربية الاستثمار في تطوير برامج تعليمية وتدريبية متخصصة لرجال الضبط القضائي، بهدف تعزيز قدراتهم في مجالات ثقافة الحاسب الآلي وأمن المعلومات، وذلك لضمان فاعلية وكفاءة أعمالهم في مجال مكافحة الجرائم الإلكترونية وضبط المجرمين المتورطين فيها.

التحديات التي تعترض عملية استخلاص الدليل في الجرائم المعلوماتية تتمثل في نقص الخبرة لدى المحققين وأجهزة العدالة الجنائية، وذلك فيما يتعلق بثقافة الحاسب الآلي وفهم عناصر الجرائم المعلوماتية وكيفية التعامل معها، خاصة في البلدان العربية حيث تأتي تجربة الاعتماد على التكنولوجيا وتقنياتها متأخرة مقارنة بالدول الأخرى مثل أوروبا وكندا والولايات المتحدة، بالإضافة إلى ذلك، تشير الوقائع إلى أن أجهزة العدالة تكون غالبًا غير مجهزة لمواجهة الجرائم المتقدمة هذه إلا بعد وقوعها، مما يستغرق وقتًا أطول من انتشار الجرائم نفسها[2].

تتقدم التكنولوجيا بشكل سريع وهذا يعكس الفجوة في التطور بين القانون والتشريعات المتعلقة بالجرائم المعلوماتية والتقنيات المستخدمة في ارتكابها، هذا الفارق يؤثر سلبًا على كفاءة إجراءات التحقيق الجنائي والاستدلال في الجرائم المعلوماتية عن طريق الحاسب الآلي.

لذا، تتطلب هذه الظروف التأهيل المناسب والتدريب المستمر للمحققين والمختصين في جهات التحقيق والادعاء، لضمان فاعلية استخدام التكنولوجيا في مكافحة وتحقيق الجرائم المعلوماتية بشكل ملائم وفعال.

---

[1] د. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2004، ص107.

[2] د. ممدوح عبد الحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، دار الحقوق، الشارقة، 2001، ص17.

جهات الضبط القضائي التقليدية غالبًا ما تفتقر إلى الثقافة القانونية الكافية للتعامل مع الجرائم المعلوماتية وفهم خطورتها، هذه المشكلة تتفاقم بشكل كبير في الدول التي لا تمتلك تشريعات خاصة لمكافحة الجرائم المعلوماتية، حيث يعد وجود تلك التشريعات ضرورة لا غنى عنها، فإنها تساهم في توعية المجتمع بشكل عام وتثقيف جهات الضبط القضائي على وجوب التعرف على خطورة هذه الجرائم، وتساعد أيضًا في تحديد الأفعال التي تشكل الجرائم المعلوماتية والتي يمكن ألا تشملها التشريعات التقليدية.

تلاحظ العديد من خبراء الفقه الجنائي أهمية وصعوبة التحقيق في الجرائم المعلوماتية، خاصة نظرًا للمتطلبات العلمية والتدريبية، والخبرات المكتسبة التي يجب أن يتمتع بها رجال الضبط القضائي وسلطات التحقيق الجنائي، حيث تتطلب حداثة هذه الجرائم وتقنياتها المتقدمة من الباحثين والمحققين إلمامًا كافيًا بها، لذا، لا يكفي أن يكون لديهم الخلفية القانونية أو الخبرة في العمل الشرطي فقط، بل يجب أن يتمتعوا بمعرفة تقنية تساعدهم في فهم الجرائم المعلوماتية التي تتم عبر الحاسوب الشخصي[1].

تزداد تحديات أجهزة العدالة الجنائية في التعامل مع جرائم الحاسوب والإنترنت بسبب المصطلحات واللغات الخاصة التي يستخدمها الجناة في هذا المجال، يعتبر الجناة أنفسهم "النخبة" نظرًا لمعرفتهم العميقة بأسرار الحاسوب ولغاته المتقدمة، بينما يُشار إلى رجال الشرطة والنيابة والقضاء بأنهم "الضعفاء"[2].

يبدو أن هذا القصور الفني والمعرفي لدى سلطات التحقيق يتطلب ابتداء تفعيل عدة أمور لمكافحة الجرائم المعلوماتية وإمكانية ضبط الأدلة الجنائية أن وجدت ويمكن أن نورد أهمها:

1. تفعيل دور الضبط الإداري:

الضبط الإداري يُعَدُّ أحد أهمِّ وظائف الإدارة، حيث يهدف إلى الحفاظ على النظام العام في الأماكن العامة من خلال إصدار القرارات التنظيمية، واستخدام القوة الجسمانية إذا لزم الأمر،

---

[1] د. ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص20.

[2] د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت، دار الفكر الجامعي، 2006. ص124.

مما يترتب عليه فرض قيود على الحريات الفردية التي تُعتبر ضرورية لضمان سلامة الحياة المشتركة في المجتمع[1].

بعض المشغلين في بيئة الإنترنت يتمتعون بصفة ضبطية إدارية، مثل مزودي الخدمات والوصول إلى الإنترنت، بموجب أعمالهم وتنصيبهم بالقانون، يحظون بالصلاحيات للرقابة على سير حركة العمل والامتثال للأنظمة والقوانين من قِبل مستخدمي الإنترنت، وعندما يتم اكتشاف جريمة بهذه الطريقة، يقتصر دور المشغل الضبطي الإداري عادة على الاحتفاظ بأدلة الجريمة حتى يحضر رجال الضبط القضائي[2].

بالإضافة إلى الإجراءات التي يتخذها رجال الضبط الإداري للتصدي لجرائم الإنترنت مبكرًا ومنع وقوعها، هناك إجراءات ينتهجها العاملون في المنشآت الحيوية تُعرف بأمن المعلومات، تشمل هذه الإجراءات التدابير والسياسات التي تتبناها الإدارات الحديثة لمنع الجريمة، بدءًا من تحديد المعلومات الحساسة، ومن ثم تحليل المخاطر والتهديدات، وتقييم قابلية التعرض للهجمات، وتنفيذ الإجراءات الوقائية المناسبة حتى يتسنى تقييم فعالية هذه الإجراءات[3].

2. التدريب التخصصي لجهات التحقيق:

يتطلب التحقيق في جرائم الإنترنت والمعلوماتية خبرة ومهارات خاصة تتطلب تدريبًا متخصصًا يراعي عدة جوانب مهمة، مثل شخصية المتدرب، ومنهج التدريب، وصفته الرسمية أو غير الرسمية، بالإضافة إلى أسلوب التدريب وجهته، يجب أن يكون المتدرب مؤهلًا للتدريب، سواء كان ضابط شرطة أو محقق جنائي، مما يتطلب قدرات ذهنية ونفسية خاصة لاستيعاب هذا التدريب[4].

---

[1] د. ماجد راغب الحلو، القانون الإداري، دار المطبوعات الجامعية، الإسكندرية، 1994، ص471.

[2] د. عمر محمد بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، 2004، ص809.

[3] د. ايمن عبد الحفيظ عبد الحميد، استراتيجية مكافحة جرائم الحاسب الآلي، دراسة مقارنه، رسالة دكتوراه، أكاديمية الشرطة، بدون سنة طبع، ص374 وما بعدها.

[4] د. محمد الأمين البشري، مرجع سابق، ص52.

عادةً ما يظهر أن تدريب المختصين في معالجة البيانات وأنظمة التشغيل يكون أكثر فعالية وسرعة من التدريب الذي يتلقاه أفراد أجهزة العدالة مثل الشرطة والتحقيق الجنائي، ينبغي أن يكون لدى متلقي برنامج التدريب الخبرة اللازمة لتحقيق أقصى استفادة منه.

التدريب يمكن أن يكون رسميًا أو غير رسمي، حيث يتم التدريب غير الرسمي عندما يُكلَّف المتدرب بالعمل مع شخص ذو خبرة في تحقيق الجرائم المعلوماتية، أما التدريب الرسمي فيتم من خلال حلقات دراسية أو حلقات نقاش، ويُعرف غالبًا بورشة العمل، حيث يتم التركيز فيه على جرائم الحاسب الآلي وشبكات المعلومات وسوء استخدامها[1].

ثالثًا: صعوبة الإثبات وذلك يرجع إلى:

1. الطبيعة الخاصة للدليل في الجرائم المعلوماتية: فهو ليس دليل مرئي يمكن فهمه بمجرد القراءة، ويتمثل حسب ما تتيحه النظم المعلوماتية من أدلة على الجرائم التي تقع عليها أو بواسطتها في بيانات غير مرئية لا تفصح عن شخصية معينه عاده، وتظهر هذه المشكلة بصفة خاصة بالنسبة لجرائم الإنترنت مثل الجرائم التي ترتكز على البريد الإلكتروني في ارتكابها، إذ يكون من الصعب على جهات التحري تحديد مصدر المرسل[2].
2. صعوبة الوصول إلى الدليل: وذلك نتيجة قيام كبرى المواقع العالمية على الإنترنت بإحاطة البيانات المخزنة على صفحتها بسياج من الحماية الفنية لمنع التسلل للوصول غير المشروع إليها، لتدميرها أو تبديلها أو الاطلاع عليها أو نسخها، هذا من جهة، ومن جهة أخرى يمكن للمجرم زيادة صعوبة عملية ضبط أي دليل يدينه، وذلك من خلال استخدامه كلمات مرور بعد تخريب الموقع مثلا، أو استخدامه تقنيات التشفير.
3. سهولة محو الدليل: فالجاني يستطيع أن يتوجه إلى أي مقهى للإنترنت"، والدخول على أحد المواقع وإرسال رسالة على البريد الإلكتروني لأخر تحوي عبارات سب وقذف، ثم يقوم بمحو الدليل، وإعادة كل شيء كما كان عليه والانصراف إلى حال سبيله.

---

[1] د. عبد الفتاح بيومي حجازي، مرجع سابق. ص130.

[2] علي محمود على حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد 1. 2003. ص116.

4. أدلة الإدانة ذات نوعية مختلفة: فهي معنوية الطبيعة، وذلك مثل سجلات الكمبيوتر، ومعلومات الدخول والاشتراك والنفاذ والبرمجيات، ولذا فهذه الأدلة تثير أمام القضاء مشكلات عديدة، ولاسيما فيما يتصل بمدى قبولها وحجيتها والمعايير اللازمة لذلك[1].

خامسًا: إحجام الجهات والأشخاص المجني عليهم عن الإبلاغ عن الجرائم المعلوماتية:

ويحدث ذلك غالبا بالنسبة للجهات المالية كالمصارف والبنوك وجهات السمسرة، إذ أن مجالس إدارتها في الغالب الأعم – تفضل كتمان هذه الجرائم، تفاديا للآثار السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية تجاهها، إذ قد يؤدى ذلك إلى تضاؤل الثقة فيها من جانب المتعاملين معها.

سادسًا: صعوبات شديدة في ضبط وتوصيف جرائم المعلومات:

لا مراء في أن رجال الضبطية القضائية والمحققين والقضاة يصادفون صعوبات جمة فيما يتعلق بإجراءات ضبط الجرائم المعلوماتية، وإضفاء الوصف القانوني المناسب على الوقائع المتعلقة بهذه الجرائم، ولعل مرد ذلك يرجع إلى الطبيعة الخاصة لهذه الجرائم، فهي تتم في قضاء إلكتروني، يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود.

سابعًا: يتعارض التفتيش عن الأدلة في الجرائم المعلوماتية مع الحق في الخصوصية المعلوماتية:

حيث يتم هذا التفتيش غالبًا على أنظمة الكمبيوتر وقواعد البيانات وشبكات المعلومات، مما قد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة. ويرجع ذلك إلى انتشار الربط بين الحواسب والشبكات الداخلية على مستوى المنشآت، والشبكات المحلية والإقليمية والدولية على مستوى الدول. ولا شك أن امتداد التفتيش إلى أنظمة أخرى غير النظام المشتبه به قد يؤثر على حقوق الخصوصية المعلوماتية لأصحاب الأنظمة التي يشملها التفتيش[2].

---

[1] د. سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية للنشر والتوزيع، القاهرة، 1999. ص132.

[2] د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت/ دراسة مقارنة، عالم الكتب الحديث، 2004. ص207.

ثامنًا: فكرة الاختصاص والطبيعة الدولية للجرائم الإلكترونية:

الجرائم الإلكترونية تتم في الغالب بأفعال يرتكبها أشخاص من خارج الحدود، كما أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود، الأمر الذي يثير تساؤلات حول الاختصاص القضائي بهذه الجرائم، علاوة على أن امتداد أنشطة الملاحظة والتحري والضبط والتفتيش خارج الحدود، أمرٌ يحتاج إلى تظافر وتعاون دولي شامل، يحقق أهدافه في مكافحة هذه الجرائم، مع احترام السيادة الداخلية للدول المعنية.

الفصل الثاني

إجراءات المحاكمة في الجرائم الإلكترونية

في ظل التطورات التكنولوجية المتسارعة وانتشار وسائل الاتصال الحديثة، أصبحت الجرائم الإلكترونية ظاهرة تتزايد يومًا بعد يوم، الأمر الذي أوجب على المشرع العُماني تبني إجراءات خاصة للتعامل مع هذا النوع من الجرائم.

يهدف هذا الفصل إلى تسليط الضوء على إجراءات المحاكمة في الجرائم الإلكترونية وفق التشريع العُماني، بما يتلاءم مع خصوصية هذه الجرائم وطبيعتها الفنية التي تختلف عن الجرائم التقليدية، وسوف يتناول الفصل مبحثين أساسيين، يتطرق الأول إلى الاختصاص الجنائي في الجرائم الإلكترونية، حيث يتناول مبادئ التحقيق الجنائي في هذا المجال، ويسلط الضوء على أهمية التعاون الدولي لمواجهة الجرائم الإلكترونية العابرة للحدود، نظرًا لما تفرضه من تحديات تتطلب تكاتف الجهود الدولية.

أما المبحث الثاني فيركز على حجية الإثبات في الجرائم الإلكترونية، حيث يبحث في قيمة الدليل الإلكتروني أما القضاء، ودور القاضي في تقدير الخبرة الفنية المقدمة في هذه الجرائم، ويوضح هذا المبحث كيفية استناد المحاكم إلى الأدلة الإلكترونية، مع مراعاة الضمانات القانونية اللازمة، وكذلك سلطة القاضي في تقييم الدليل الفني بموضوعية وعدالة.

بهذا يسعى هذا الفصل إلى تقديم فهم شامل لإجراءات المحاكمة في الجرائم الإلكترونية وفق التشريع العُماني، مشددًا على أهمية هذه الإجراءات في إرساء العدالة وحماية المجتمع من أخطار الجرائم الإلكترونية.

المبحث الأول

الاختصاص الجنائي في الجرائم الإلكترونية

يعتبر الاختصاص الجنائي في الجرائم الإلكترونية من الموضوعات المؤثرة في عصر المعلومات والتكنولوجيا، حيث تتيح البيئة الرقمية ظهور أنواع جديدة من الجرائم التي تتسم بعالميتها وتعقيدها، يهدف هذا المبحث إلى دراسة الأسس القانونية والإجرائية للاختصاص الجنائي في الجرائم الإلكترونية، مع التركيز على المبادئ الأساسية التي تحكم التحقيقات الجنائية في هذا المجال.

المطلب الأول

سلطة القاضي في تقدير توافر أركان الجريمة

التحقيق في الجرائم الإلكترونية يتطلب أدوات ومهارات تختلف عن تلك المستخدمة في التحقيقات الجنائية التقليدية. تحقيق العدالة في هذا النوع من الجرائم يعتمد بشكل كبير على سرعة ودقة جمع الأدلة الرقمية وتحليلها، وذلك لان القاضي الجزائي يعتمد على هذه المبادئ في تكوين قناعته.

وتعد السلطة القضائية إحدى الدعائم الأساسية لتحقيق العدالة في أي نظام قانوني، إذ يتولى القاضي دورًا محوريًا في تحديد ما إذا كانت الجريمة قد ارتكبت وفقًا للقانون أم لا، ومن بين المهام التي تقع على عاتق القاضي هو تقدير توافر أركان الجريمة، التي تشمل الركن المادي والركن المعنوي والركن القانوني. ولتنفيذ هذه المهمة، يعتمد القاضي على فحص الأدلة المقدمة في القضية، وتحليل تصرفات الجاني، ودراسة النية وراء الفعل المرتكب، إضافة إلى ذلك، يتطلب من القاضي أن يوازن بين تطبيق النصوص القانونية وتفسيرها بما يضمن الحفاظ على حقوق المتهم مع تحقيق العدالة، وعليه، تعتبر هذه السلطة جزءًا أساسيًا من العملية القضائية، حيث يلتزم القاضي بتحقيق الإنصاف بناءً على المعطيات القانونية والواقعية المتاحة له، وهو ما نود بيانه من خلال الفرعين التاليين:

الفرع الأول

أركان الجرائم الإلكترونية

تعد عملية تحقق القاضي من توافر أركان الجريمة من أهم مراحل المحاكمة، إذ إنها تضمن تحقيق العدالة وعدم إدانة شخص دون وجود أدلة قاطعة على ارتكابه الفعل الإجرامي، فالقانون الجزائي يشترط لقيام الجريمة ثلاثة أركان رئيسية وهي الركن القانوني، والذي يتمثل بوجود نص يجرم الفعل، والركن المادي الذي يشمل السلوك والنتيجة والعلاقة السببية بينهما، والركن المعنوي الذي يعبر عن القصد الجنائي أو الخطأ غير العمدي[1]، فمن دون هذه الأركان لا يمكن مساءلة المتهم جنائيًا، مما يجعل دور القاضي في هذا التحقق ضروريًا لحماية الحقوق وضمان تطبيق القانون بعدالة وإنصاف، فمن هنا تأتي أهمية الحديث في هذا الفرع عن ركني الجريمة المادي والمعنوي.

أولًا: الركن المادي للجرائم الإلكترونية

في سياق الجرائم الإلكترونية، يعد الركن المادي عاملًا أساسيًا في إثبات مادية الجريمة، يشير هذا الركن إلى الأفعال الملموسة التي يقوم بها الجاني والتي تظهر في العالم الخارجي كنتيجة لنيته الإجرامية، على عكس الجرائم التقليدية التي تعتمد على الأدلة المادية، مثل المسروقات أو الأسلحة، فإن الجرائم الإلكترونية تنفذ في الفضاء الرقمي، وبالتالي، يشير الركن المادي في الجرائم الإلكترونية إلى استخدام الأدوات الرقمية والشبكات والأجهزة لارتكاب أفعال غير قانونية، هذا الركن يشكل أساسًا لتحديد هوية المجرمين الإلكترونيين وملاحقتهم في التحقيقات الجنائية. [2]

1. تعريف الركن المادي في الجرائم الإلكترونية

في القانون الجنائي التقليدي، يتضمن الركن المادي الجوانب الملموسة للجريمة، مثل السرقة أو الاعتداء، ولكن في الجرائم الإلكترونية، يشمل الركن المادي الأفعال الرقمية التي تؤدي إلى نتائج

---

[1] معهد الكويت للدراسات القضائية والقانونية، أركان الجريمة والشروع فيه، 2018–2019، ص7.

[2] جمال زين العابدين أمين أحمد، الاختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية "دراسة مقارنة، مجلة مستقبل العلوم الاجتماعية، جامعة عبد الملك السعدي، المغرب، العدد الرابع، يناير 2021م، ص76.

إجرامية، مثل اختراق الأنظمة، نشر البرمجيات الخبيثة، أو سرقة البيانات، غالبًا ما تكون هذه الأفعال معقدة وتتطلب مهارات تكنولوجية متقدمة، مما يجعلها مختلفة عن الجرائم التي ترتكب في الفضاء الفيزيائي، البيئة الرقمية التي تقع فيها هذه الجرائم تخلق تحديات جديدة للمحققين، حيث أن الأدلة غالبًا ما تكون غير ملموسة وموزعة عبر أنظمة متعددة.[1]

الركن المادي للجريمة الإلكترونية يرتكب في بيئة تكنولوجيا المعلومات، ويعتمد على المعرفة التقنية المتقدمة، تشمل الأمثلة على هذه الأفعال زراعة الفيروسات، الانخراط في عمليات الاحتيال عبر التصيد الإلكتروني، أو استغلال الثغرات في الشبكات، تترك هذه الأفعال عادة آثارًا رقمية، مثل عناوين بروتوكول الإنترنت (IP)، أو ملفات السجلات، أو توقيعات البرمجيات الخبيثة، والتي يستخدمها المحققون لتتبع مصدر الجريمة.

2. الجرائم الإلكترونية كجرائم "السلوك الإجرامي"

تعتبر الجرائم الإلكترونية في كثير من الأحيان جرائم "السلوك المحض" أو الجرائم الشكلية، مما يعني أن مجرد القيام بالسلوك غير القانوني يكون كافيًا للملاحقة القانونية، بغض النظر عن حجم الضرر أو نتيجته الفورية، في العديد من الحالات، يعتبر استخدام الوصول غير المصرح به أو نشر البرمجيات الضارة جريمة بحد ذاتها، حتى لو لم يحدث ضرر مادي مباشر في الحال، هذا المفهوم مهم بشكل خاص في قوانين الجرائم الإلكترونية، حيث يُعترف بالتهديد المحتمل كافيًا لتبرير العقاب.[2]

على سبيل المثال، تعترف القوانين الأمريكية بالخطر المحتمل الذي تشكله الجرائم الإلكترونية، وقامت بتوسيع تعريف النتائج الإجرامية ليشمل النتائج المحتملة، يسمح هذا التفسير الواسع بمتابعة القضايا حتى عندما لا يوجد ضحية مباشرة، ومن الأمثلة البارزة على ذلك القضية الشهيرة في الولايات

---

[1] د. عبد الله ذيب محمود، د أسامة إسماعيل دراج، الوجيز في الجرائم الإلكترونية القواعد الموضوعية والإجرائية، دار الثقافة، الأردن، عمّان، ط1، 2022م، ص43.

[2] Curtis, Joanna, and Gavin Oxburgh. "Understanding Cybercrime in 'Real World' Policing and Law Enforcement." The Police Journal Theory Practice and Principles, vol. 96, no. 4, December 2023, pp. 573–592, journals.sagepub.com.

المتحدة ضد روتس[1]، حيث اعترفت المحاكم بإمكانية الضرر كنتيجة معتبرة في قضايا الجرائم الإلكترونية، يوضح هذا الموقف القانوني أهمية الاعتراف بطبيعة التهديدات الرقمية في المجتمع الحديث، حيث يمكن إلحاق الضرر دون الحاجة إلى وجود مادي.

ونجد أن المشرع العُماني قد اعتنق المذهب الشخصي في مجال الجرائم الإلكترونية، حيث يركز على الفعل المادي للجاني ونيته في ارتكاب الجريمة بغض النظر عن النتيجة النهائية، ويتضح ذلك من خلال النصوص القانونية الواردة في قانون مكافحة جرائم تقنية المعلومات، حيث يعتبر المشرع العُماني أن الدخول غير المشروع إلى المواقع الإلكترونية أو النظم المعلوماتية أو وسائل تقنية المعلومات يُعد جريمة حتى وإن لم تحدث أضرار فعلية.

ومن أمثلة ذلك ما نصت عليه المادة (3) من قانون مكافحة جرائم تقنية المعلومات، والتي تجرم التعدي على سلامة وسرية وتوافر البيانات والمعلومات الإلكترونية، وبموجب هذه المادة، يعد كل من يدخل إلى موقع إلكتروني أو نظام معلوماتي أو أي وسيلة تقنية معلوماتية دون وجه حق، أو يتجاوز صلاحياته الممنوحة له، أو يستمر في الدخول بعد علمه بذلك، مرتكبًا لجريمة[2]، وبالتالي، يُظهر المشرع العُماني التزامًا بمبدأ المذهب الشخصي، حيث يُعاقب الشخص على فعل الدخول غير المشروع بحد ذاته بغض النظر عن الضرر المترتب على ذلك.

3. التحديات التحقيقية في إثبات الركن المادي

إحدى التحديات الرئيسية التي يواجهها المحققون في قضايا الجرائم الإلكترونية هي تحديد وإثبات الركن المادي في بيئة رقمية، على عكس الأدلة المادية التقليدية، تكون الأدلة الرقمية غالبًا

---

[1] قضية تتعلق بجرائم الإنترنت قام شخص يدعى "Roots" بمحادثة عبر الدردشة مع من أعتقد أنها فتاة قاصر لم تتجاوز 14 عامًا، تضمنت المحادثة أمورا ذات طابع جنسي وعرض فيها مقابلة الفتاة بغرض ممارسة أفعال غير أخلاقية، وعند الموعد المحدد في مكان عام تم إلقاء القبض عليه، ليكتشف لاحقا أن الفتاة كانت في الحقيقة عضوة في فريق مكافحة الجرائم الإلكترونية، قد قامت بدور فتاة قاصر كجزء من عملية سرية، وخلال المحاكمة دفع Roots بعدم وجود ضحية، إلا أن المحكمة رفضت الدفع بالاستناد إلى المادة (2422) من قانون الولايات المتحدة، التي تعتبر مجرد النية أو محاولة ارتكاب الجريمة كافية دون الحاجة إلى وجود ضحية فعلية، وأكدت محكمة الاستئناف في الدائرة الحادية عشرة هذا المبدأ موضحة أن احتمال ارتكاب الجريمة يكفي لإثبات التهمة وفقًا للمادة المذكورة.

[2] قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم 2011/11.

مخفية تحت طبقات من التشفير، وأدوات إخفاء الهوية، والشبكات المعقدة، على سبيل المثال، قد يستخدم الجناة شبكات افتراضية خاصة (VPN) أو تقنيات تشفير لإخفاء أنشطتهم، مما يجعل من الصعب على المحققين تتبع تصرفاتهم.[1]

ورغم هذه التحديات، فإن وجود أدوات القرصنة، والبرمجيات الخبيثة، والوصول غير المصرح به إلى الأنظمة يشكل دليلًا ماديًا قويًا على الركن المادي في الجرائم الإلكترونية، وتسمح الأدوات والتقنيات الجنائية المتقدمة للمحققين بتتبع الأعمال التي يقوم بها المجرمون الإلكترونيون، حتى في حال محاولتهم محو أو إخفاء آثارهم.

إن الركن المادي في الجرائم الإلكترونية حجر الزاوية في التحقيقات الجنائية، حيث يحدد الأفعال التي تشكل السلوك غير القانوني في العالم الرقمي، يتطلب فهم وإثبات هذا الركن معرفة عميقة بالنظم الرقمية والتكنولوجيا، يجب على المحققين أن يكيفوا أساليبهم مع تعقيدات البيئة الرقمية، مستخدمين أدوات جنائية متقدمة لكشف وتتبع الآثار الرقمية التي يتركها المجرمون الإلكترونيون، هذا المجال المتطور من القانون الجنائي يبرز الحاجة إلى نهج قوي ومتقن تقنيًا لمكافحة الجرائم الإلكترونية بفعالية وملاحقتها قانونيًا.

وسلطة القاضي في تقدير الركن المادي للجريمة تكمن في قدرته على تحديد ما إذا كان الفعل الذي ارتكبه الجاني يشكل جريمة وفقًا للقانون، حيث يتعين عليه فحص الأدلة المتاحة وتقييمها بعناية. لهذا يقوم القاضي بتحليل سلوك الجاني لتحديد ما إذا كان الفعل المادي قد تحقق وفقًا للوصف القانوني للجريمة، كما يقدّر إذا كانت النتيجة الجرمية قد حدثت نتيجة مباشرة لهذا الفعل. بالإضافة إلى ذلك، يتحقق القاضي من وجود علاقة سببية بين الفعل والنتيجة، مما يساعده على تحديد ما إذا كان الجاني مسؤولًا عن الجريمة، وفي حالة وجود غموض أو لبس في الأدلة، يملك القاضي السلطة لتفسير النصوص القانونية بما يتناسب مع الواقعة المعروضة أمامه.

---

[1] خالد على نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، بحث مقدم لاستيفاء متطلبات الحصول على درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة المنصورة، 2022، ص9.

وقد أيدت محكمة النقض المصرية هذا الاتجاه، حيث قضت بأن "يكفى في المحاكمات الجنائية أن تتشكك محكمة الموضوع في صحة إسناد التهمة الى المتهم لكى تقضى بالبراءة ما دام حكمها يشتمل على ما يفيد أنها محصت الدعوى وأحاطت بظروفها وبأدلة الثبوت التي قام الاتهام عليها عن بصر بصيرة ووازنت بينها وبين أدلة النفي فرجحت دفاع المتهم أو داخلتها الريبة في صحة عناصر الاتهام، وكانت المحكمة، قد خلصت الى ارتيابها في أقوال شاهدي الإثبات وعدم الاطمئنان إليها ورجحت دفاع المتهم وهو ما يدخل في سلطتها بغير معقب عليها لدى محكمة النقض"[1]

ثانيًا: الركن المعنوي للجرائم الإلكترونية

إن الركن المعنوي في الجرائم الإلكترونية يمثل مكونًا جوهريًا من مكونات المسؤولية الجنائية، ولا يكفي توافر الركن المادي وحده لتحقيق المسؤولية القانونية، يتطلب القانون الجنائي وجود الإرادة الإجرامية لتكوين الركن المعنوي، الذي يتجسد في صورتين: القصد الجنائي أو الخطأ غير العمدي[2].

فيمكن أن تقع بعض الجرائم الإلكترونية بطريق الخطأ، ولكن هذا لا يعني بالضرورة أن المسؤولية الجنائية تنتفي في هذه الحالات، ففي القانون الجنائي بشكل عام، يتم التمييز بين الجرائم التي تُرتكب عن عمد (القصد الجنائي) والجرائم التي تحدث عن غير قصد (الخطأ).

وفيما يتعلق بالجرائم الإلكترونية، يمكن أن تحدث نتيجة للإهمال أو الخطأ غير المقصود، مثل الخطأ في التعامل مع الأنظمة، حيث قد يرتكب شخص فعلًا غير قانوني عن غير قصد، كإرسال بريد إلكتروني يحتوي على معلومات حساسة أو فتح روابط تحتوي على فيروسات نتيجة لعدم الحذر أو الجهل، كما قد تُصاب الأنظمة بفيروسات أو برمجيات ضارة عن طريق الخطأ أثناء تصفح الإنترنت، مما يؤدي إلى أضرار أو سرقة بيانات، أيضًا، في بعض الحالات قد يتم نشر معلومات أو بيانات بشكل غير مقصود بسبب أخطاء في البرمجة أو الإعدادات الأمنية في الأنظمة الإلكترونية.

---

[1] الطعن رقم (6763)، لسنة القضائية رقم (59)، بتاريخ جلسة 7/ 11/ 1991م، محكمة النقض المصرية.

[2] حسين محمد فلاح البرايسه، الركن المعنوي للجرائم الإلكترونية وفقًا لقانون العقوبات الأردني، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2021، ص44.

ومع ذلك، حتى في حالة وقوع الجرائم الإلكترونية عن طريق الخطأ، قد يتحمل الجاني المسؤولية الجنائية إذا ثبت أن هناك إهمالًا أو تقصيرًا في اتخاذ الاحتياطات اللازمة لحماية البيانات أو الأنظمة، مثل إرسال معلومات سرية عبر البريد الإلكتروني عن غير قصد دون اتخاذ تدابير كافية لمنع ذلك، وبالتالي، بينما يمكن أن تحدث الجرائم الإلكترونية عن غير قصد، فإن المسؤولية الجنائية قد تتفاوت بناءً على وجود الإهمال أو التقصير في اتخاذ التدابير الوقائية المناسبة.

وهذا ما أكدت عليه المادة (33) من قانون الجزاء والتي نصت على أن الركن المعنوي وهو: "العمد في الجرائم المقصودة، والخطأ في الجرائم غير المقصودة، ويتوفر العمد باتجاه إرادة الجاني إلى ارتكاب فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرمًا قانونًا، وذلك بقصد أحداث نتيجة مباشرة أو أي نتيجة أخرى مجرمة قانونًا يكون الجاني قد توقعها وقبل المخاطرة بها، وتكون الجريمة عمدية كذلك إذا وقعت على غير الشخص المقصود بها، ويتوفر الخطأ إذا وقعت النتيجة الإجرامية بسبب خطأ الفاعل، أو عدم مراعاة القوانين أو الأنظمة"[1]، ويعد الركن المعنوي في الجرائم الإلكترونية تحديًا خاصًا نظرًا للطبيعة الرقمية للجريمة وطبيعة الأدلة المتعلقة بها[2].

1. القصد الجنائي في الجرائم الإلكترونية

القصد الجنائي هو أساس الركن المعنوي، ويعني علم الجاني بالعناصر المكونة للجريمة واتجاه إرادته لتحقيق تلك العناصر أو قبول حدوثها، في الجرائم الإلكترونية، يتمثل القصد الجنائي العام في علم الجاني بأنه يقوم بفعل غير قانوني يتضمن اختراقًا أو إساءة استخدام للتكنولوجيا أو النظام الرقمي، على سبيل المثال، الشخص الذي يقوم باختراق نظام حماية الشبكات عن قصد أو ينشر فيروسات تدميرية يكون لديه علم مسبق بالعواقب المحتملة لهذه الأفعال، ويتجه بفعله نحو تحقيق تلك النتائج، ما يُعرف بالقصد الجنائي.[3]

---

[1] قانون الجزاء الصادر بالمرسوم السلطاني رقم 2018/7، الباب الثالث تقسيم الجرائم وأركان الجريمة، الفصل الثالث، الركن المعنوي، المادة (33).

[2] د. عبد الله ذيب محمود، د. أسامة إسماعيل دراج، مرجع سابق، ص51.

[3] خالد على نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، كلية الحقوق – جامعة المنصورة، 2022

ولكن في الجرائم الإلكترونية، لا يكتفي القانون بوجود القصد الجنائي العام، بل يشترط في بعض الحالات توافر القصد الجنائي الخاص، القصد الخاص يتطلب أن يكون لدى الجاني نية تحقيق غاية معينة، مثل نية التملك، أو نية الإضرار بسمعة مؤسسة أو شخص، على سبيل المثال، في حالات اختراق البريد الإلكتروني أو سرقة البيانات الشخصية، يجب أن يكون لدى الجاني نية استخدام هذه المعلومات بطريقة غير مشروعة لتحقيق غايات مادية أو معنوية محددة[1]، وفي هذا السياق قالت المحكمة العليا:" إن الركن المعنوي يتمثل في القصد الجنائي العام في جريمة السب والقذف وليس الخاص، كون المشرع لم يتطلب القصد الخاص وبالتالي يكفي لتوافر القصد الجنائي أن تتجه إرادة الجاني إلى استخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات في نشر عبارات تحمل معنى السب والقذف حتى لو لم تتجه إرادته إلى الإهانة أو تشويه السمعة أو المساس بالغير طالما أقدم على الفعل بإرادة صحيحة مختارة غير مشوبة بإكراه"[2].

2. الفرق بين الإرادة والعلم في الركن المعنوي

في إطار تحديد الركن المعنوي، يتنقل المشرعون بين مبدأ الإرادة ومبدأ العلم، الإرادة تعني أن الجاني ليس فقط على علم بما يقوم به، ولكن إرادته تتجه نحو تحقيق الأفعال الإجرامية، أما العلم، فيرتبط بمعرفة الجاني بأن فعله غير قانوني أو يؤدي إلى نتائج إجرامية، ولكنه قد لا يكون بالضرورة مهتمًا بتحقيق تلك النتائج.[3]

في القانون الفيدرالي الأمريكي، نجد أن المشرع يستخدم مفهوم الإرادة في قوانين العلامات التجارية عندما يتطلب وجود نية واضحة لانتهاك حقوق العلامة التجارية، في المقابل، في حالات مثل النسخ الإلكتروني أو انتهاك حقوق الملكية الفكرية، يعتمد المشرع على مبدأ العلم، حيث يكفي أن يكون الجاني على علم بأن أفعاله تنتهك حقوق الملكية دون الحاجة إلى إثبات نية محددة لتحقيق ضرر.[4]

---

[1] محمد سعيد نمور أصول الإجراءات الجنائية، شرح لقانون أصول المحاكمات الجنائية، دار الثقافة للنشر والتوزيع، ط1، عمان 2011، ص397.

[2] الطعن رقم 2016/611 الصادر عن الدائرة الجزائية جلسة 7/3/ 2017، مجموعة الاحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها للسنتين القضائيتين السابعة عشر والثامنة عشر.

[3] خالد على نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، كلية الحقوق – جامعة المنصورة، 2022.

[4] علي عدنان الفيل، اجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، المكتب الجامعي الحديث الإسكندرية، ط1، 2012، ص67.

3. الإرادة الإجرامية في الجرائم الإلكترونية

الإرادة الإجرامية، أو ما يعرف بالحالة النفسية للجاني، تلعب دورًا محوريًا في تحديد الركن المعنوي، تعني هذه الإرادة أن الجاني لم يكن فقط على علم بما يقوم به، بل كان يوجه أفعاله نحو تحقيق غايات غير قانونية، في الجرائم الإلكترونية، قد تكون الإرادة الإجرامية أكثر تعقيدًا نظرًا للطبيعة الرقمية للجريمة، على سبيل المثال، الشخص الذي يقوم بإرسال برامج ضارة بهدف تدمير الأنظمة أو تعطيل الخدمات يكون قد وجه إرادته نحو تحقيق تلك الأضرار.

في حالة الجرائم الإلكترونية التي تنطوي على انتهاكات للخصوصية، مثل التجسس على البريد الإلكتروني أو سرقة البيانات الشخصية، يجب أن يتم إثبات أن الجاني كان يهدف إلى انتهاك حق الشخص في الخصوصية، وبالتالي، يجب أن يكون لدى الجاني نية واضحة للقيام بهذا الانتهاك، وأنه كان يعلم بأن فعله غير قانوني وأنه يهدف إلى إحداث ضرر بالضحية. [1]

إن الركن المعنوي في الجرائم الإلكترونية يشكل عنصرًا مهمًا في المسؤولية الجنائية، ويشمل توافر الإرادة الإجرامية سواء كانت بشكل قصد جنائي عام أو خاص، تختلف طبيعة القصد المطلوب وفقًا لنوع الجريمة والمشرع الذي ينظر في القضية، حيث قد يُطلب إثبات نية واضحة لتحقيق ضرر أو انتهاك خصوصية، ويعد تحديد هذا الركن تحديًا خاصًا في الجرائم الإلكترونية نظرًا للتعقيد التكنولوجي والبيئة الرقمية التي تقع فيها هذه الجرائم.

وسلطة القاضي في تقدير الركن المعنوي للجريمة تعد من الجوانب الأساسية في عمله القضائي، حيث يختص القاضي بتحديد ما إذا كان الجاني قد ارتكب الجريمة بنية إجرامية أو بقصد جنائي، ويعتمد القاضي على تحليل الأدلة والقرائن المتاحة له، مثل تصرفات الجاني قبل أو بعد ارتكاب الجريمة، لتحديد ما إذا كانت الجريمة قد تمت عن عمد أو نتيجة إهمال، وقد ينظر القاضي أيضًا في الظروف المحيطة بالجريمة مثل توقيت الفعل وطريقة ارتكابه، بالإضافة إلى الحالة النفسية والعقلية للجاني، ما يساعده في تحديد ما إذا كان القصد الجنائي متوفرًا أم لا، وفي بعض الحالات،

---

[1] د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2019م، ص105.

يمكن للقاضي الاستفادة من الظروف المخففة أو التخفيفات القانونية، مثل الدفاع عن النفس أو التأثيرات النفسية التي قد تؤثر على سلوك الجاني وتخفف من مسؤوليته.

الفرع الثاني

أهمية التحقيق النهائي في الجرائم الإلكترونية

إجراءات المحاكمة في الجرائم الإلكترونية تمثل تحديًا كبيرًا للنظام القضائي بسبب طبيعة هذه الجرائم التي تعتمد على التكنولوجيا والبيانات الرقمية. الجرائم الإلكترونية تشمل مجموعة واسعة من الأنشطة غير القانونية التي تتم عبر الإنترنت أو باستخدام الأجهزة الإلكترونية، مثل اختراق الأنظمة، الاحتيال الإلكتروني، سرقة الهوية، توزيع البرمجيات الضارة، وغيرها. تتطلب المحاكمة في هذه القضايا إجراءات دقيقة ومعقدة لضمان تحقيق العدالة وحماية حقوق الأفراد.[1]

وتحقق التحقيقات الجزائية في جميع مراحلها في الجرائم الإلكترونية أهدافًا متعددة تتعلق بإثبات وقوع الجريمة، كيفية ارتكابها، وأسبابها، ومعرفة الجاني من خلال أقوال الشهود وخبراء التحليل الجنائي، تتطلب هذه التحقيقات أساليب خاصة وفهمًا عميقًا لطبيعة الجرائم الرقمية، والتي تختلف عن الجرائم التقليدية، مما يستدعي استراتيجيات وأدلة جديدة للوصول إلى النتائج التالية:

1. إثبات وقوع الجريمة

أول غرض من أغراض التحقيق الجنائي في الجرائم الإلكترونية هو إثبات وقوع الجريمة، يتعين على المحقق أن يتأكد من أن هناك جريمة حدثت بالفعل، وهذا يتطلب جمع الأدلة المادية التي تدعم وقوع الجريمة، إن طبيعة الجرائم الإلكترونية تجعلها أكثر تعقيدًا، إذ لا تتواجد الأدلة المادية كما هو الحال في الجرائم التقليدية، فالأدلة في الجرائم الإلكترونية تشمل البيانات المخزنة على أجهزة الكمبيوتر، السجلات الرقمية، والمعلومات التي قد تكون مخفية داخل البرامج.[2]

---

[1] حميد قادري، لحسن إمعلي، محمد الحبيب اعمير، إجراءات المحاكمة في الجريمة الإلكترونية، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الخامس، الرباط، السنة الجامعية 2018-2019، ص2.

[2] خالد على نزال الشعار، مرجع سابق، ص11.

يجب أن يتفحص المحقق كافة البيانات ذات الصلة، بما في ذلك سجلات الدخول، وملفات الولوج، وأي تغييرات تم إجراؤها على النظام، إن الاعتماد على الأدلة التقليدية في هذه الحالة قد لا يكفي، مما يستدعي توظيف مهارات جديدة تتعلق بتحليل البيانات وفهم طبيعة الأدلة الرقمية، يُعتبر استخدام أساليب التحقيق التقليدية غير كافٍ نظرًا لطبيعة الجرائم الإلكترونية المعقدة، مما يتطلب تطوير تقنيات وأساليب جديدة لجمع وتحليل الأدلة.

2. تحديد أسلوب ارتكاب الجريمة

تتطلب التحقيقات الجنائية أيضًا تحديد أسلوب ارتكاب الجريمة، يختلف كل مجرم في الطرق التي يتبعها لتنفيذ جريمته، وفهم هذه الأساليب يساعد المحققين في تضييق دائرة المشتبه بهم، فعلى سبيل المثال، إذا كانت الجريمة تتعلق بزرع برامج اختراق أو تجسس، فإن معرفة أسلوب الجاني في الوصول إلى الهدف تكون ضرورية.[1]

عند وقوع جريمة إلكترونية، يتعين على المحققين تحليل جميع الأدلة المتاحة لفهم كيفية تنفيذ الجريمة، على سبيل المثال، إذا كانت الجريمة تتعلق بزرع برامج اختراق أو تجسس، فإن معرفة الأسلوب الذي استخدمه الجاني للوصول إلى الهدف تعتبر ضرورية، تشمل هذه الأساليب استخدام تقنيات محددة أو استراتيجيات تلاعب بالنظام، لذا، فإن تحليل البيانات المستخرجة من النظام يلعب دورًا محوريًا في هذا السياق.

تتطلب عملية التحليل فحص الأدوات والتقنيات المستخدمة في الجريمة، قد يقوم المجرمون بتعديل إعدادات النظام أو استخدام أجهزة معينة لاختراق الأنظمة، مما يجعل من الضروري تحديد هذه الأدوات لفهم كيفية تنفيذ الجريمة، على سبيل المثال، يتضمن ذلك استخدام أدوات متخصصة مثل "البرامج الضارة" أو "الفيروسات"، والتي تتيح لهم الوصول غير المصرح به إلى البيانات.[2]

---

[1] عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، منشورات الحلبي الحقوقية، لبنان، ط1، 2015، ص20.

[2] خالد على نزال الشعار، مرجع سابق، ص12.

من جانب آخر الخلفية الفنية للجاني جزءًا أساسيًا من التحقيق، على سبيل المثال، قد يشير نمط سلوك الجاني إلى مستوى معرفته التقنية، مما يساعد المحققين في تحديد نوع الجاني المحتمل، إذا كان الجاني يمتلك مهارات تقنية عالية، فقد يُظهر ذلك أنه متورط في أنشطة إجرامية معقدة، مثل القرصنة، بينما قد يشير أسلوب آخر أكثر بساطة إلى وجود جاني أقل خبرة، مما يفتح مجالات مختلفة للبحث والتحقيق.

حيث يساعد تحديد أسلوب الجريمة المحققين في فهم الدوافع وراء ارتكاب الجريمة، إذا تم التعرف على أنماط سلوك معينة مرتبطة بجريمة محددة، تساهم هذه المعلومات في تحديد النوايا والدوافع المحتملة للجاني، فالأشخاص الذين يرتكبون الجرائم من أجل الربح المالي قد يتبعون أساليب مختلفة تمامًا عن أولئك الذين يسعون لتحقيق أهداف سياسية أو اجتماعية.

3. معرفة أسباب وقوع الجريمة

تُعتبر دراسة أسباب وقوع الجريمة عنصرًا مؤثرا في التحقيق الجنائي، حيث تسهم في فهم أعمق للدوافع التي تقف وراء ارتكاب الجرائم، وخاصة الجرائم الإلكترونية، يتطلب ذلك تحليلًا دقيقًا لمجموعة من العوامل النفسية والاجتماعية التي قد تدفع الأفراد إلى اتخاذ قرار ارتكاب جريمة، تشمل هذه الدوافع مجموعة متنوعة من الأسباب، مثل الرغبة في الربح المالي، الانتقام من شخص أو جهة معينة، أو حتى الفضول الشخصي الذي يدفع الفرد لاستكشاف الأنظمة والبيانات المحمية.

تحليل الدوافع لا يوفر فقط رؤى قيمة حول كيفية تطور الجريمة، بل يسهم أيضًا في توجيه مسار التحقيقات، على سبيل المثال، إذا كان الجاني موظفًا سابقًا لديه معرفة عميقة بالأنظمة الداخلية لشركة معينة، فإن ذلك قد يفسر دوافعه لاختراق النظام، إن فهم هذه الظواهر يسهل التعرف على المشتبه بهم، كما يوجه المحققين إلى أماكن محددة للبحث عن الأدلة.[1]

علاوة على ذلك، تُعَد معرفة الدوافع بمثابة مفتاح لفهم سلوكيات الجناة، فالأفراد الذين يسعون إلى الربح المالي قد يستخدمون استراتيجيات معقدة للوصول إلى معلومات حساسة، بينما

[1] علي عدنان الفيل، مرجع سابق، ص67.

قد يكون الانتقام دافعًا قويًا يحفز بعض الأشخاص على ارتكاب الجرائم، مثل استخدام تقنيات الاختراق لتسريب معلومات شخصية عن خصومهم، لذلك، يعتبر التعرف على هذه الدوافع جزءًا أساسيًا من عملية التحقيق.

أيضًا، تكشف دراسة السياق الاجتماعي والاقتصادي للجاني عن عوامل إضافية تسهم في ارتكاب الجريمة، فقد تلعب الظروف المعيشية الصعبة أو ضغوط العمل دورًا في دفع الأفراد نحو اتخاذ قرارات غير قانونية، من خلال هذا الفهم المتكامل للدوافع والسياق، يمكن للمحققين تطوير استراتيجيات فعالة لاكتشاف الجرائم ومنعها، مما يسهم في تعزيز الأمن المعلوماتي وتقليل معدلات الجرائم الإلكترونية.

4. تحديد معرفة الجاني

إن معرفة الجاني الهدف النهائي للتحقيق الجنائي، حيث يتطلب ذلك التحقق من شخصية المجرم عبر تحليل خصائصه النفسية والسلوكية، يعتمد المحققون في هذا السياق على مجموعة من العوامل، مثل الذكاء والمعرفة بالتقنيات الحديثة، إلى جانب الدوافع المحتملة مثل حب المال، الانتقام، أو حتى التسلية، هذه الخصائص تعزز من فهم سلوك الجاني وتساعد في تحديد الأنماط المرتبطة بأنواع معينة من الجرائم، مما يساهم في رسم صورة دقيقة له، ومع ذلك، تظل الصورة المرسومة عنه غير قاطعة، بل تشكل نقطة انطلاق للبحث عن الأدلة.[1]

وتتضمن عملية تحديد الجاني أيضًا دور الشهود، الذين يقدموا معلومات قيمة حول ظروف الجريمة وتفاصيلها، فإذا أحسن المحقق مناقشة الشهود، فإنه يستطيع استخراج رؤى متعددة حول الحادثة، مما يسهم في تشكيل فهم شامل للوقائع، هذا التفاعل مع الشهود يعكس أهمية البيانات الشخصية والتجريبية في رسم صورة الجاني، ويُعزز من فرص الوصول إلى الأدلة المادية.

كما أن معاينة مسرح الجريمة واستشارة الخبراء من العناصر الجوهرية في تحديد هوية الجاني، فمسرح الجريمة يتيح للمحققين جمع الأدلة المادية وتحليل آثار المجرم والأدوات المستخدمة،

---

[1] محمد صلاح محمد عبد المنعم، الجرائم الإلكترونية وتحدياتها دراسة مقارنة، مرجع سابق، ص247.

مما يعزز الفهم العام للجريمة، كما أن الخبراء يمكنهم تقديم تفسيرات متخصصة حول سلوكيات الجناة، مما يسهم في توضيح الأسباب المحتملة وراء وقوع الحادث، بالتالي، يُشكل تفاعل هذه العوامل الثلاثة: خصائص الجاني، الشهادات، والأدلة المادية، أساسًا قويًا لتحقيق العدالة وكشف ملابسات الجرائم.[1]

5. تحديد وقت ومكان ارتكاب الجرائم الإلكترونية

إن تحديد وقت ومكان ارتكاب الجرائم الإلكترونية يعد من العناصر الأساسية في التحقيقات الجنائية، حيث يسهم بشكل كبير في توضيح الأركان المادية والمعنوية للجريمة، على عكس الجرائم التقليدية، التي غالبًا ما تُحدد فيها الأطر الزمنية والمكانية بشكل واضح، فإن الجرائم الإلكترونية تتسم بالتعقيد نظرًا لطبيعة الإنترنت التي تتجاوز الحدود الجغرافية، هذا يعكس ضرورة تفهم هذه العناصر بدقة عند إجراء التحقيقات الجنائية.[2]

كما تعتبر دقة تحديد وقت ومكان وقوع الجريمة الإلكترونية من الأمور المؤثرة لبناء ملف قانوني قوي، حيث يتطلب الأمر إثبات وقوع الجريمة بشكل قاطع، يعتمد نجاح الادعاء العام في إقامة الدعوى على القدرة على تحديد موقع الجريمة والزمن الذي وقعت فيه، فكلما كانت المعلومات دقيقة، كانت احتمالات التوصل إلى أدلة قاطعة أكبر، مما يسهل عملية المحاكمة ويزيد من فرص الإدانة.[3]

فإن تحديد المكان يرتبط مباشرةً بسلطة الولاية القضائية، حيث تختلف القوانين والعقوبات بين الدول، وقد ينشأ تساؤل حول كيفية تحديد مكان الجريمة في الحالات التي تُرتكب فيها الجرائم عبر الإنترنت، حيث يتم تنفيذها من مكان معين بينما تُسجل النتائج في مكان آخر، مما يزيد من التعقيد في تحديد الاختصاص القانوني.

تمتاز الجرائم الإلكترونية بأنها جرائم عابرة للحدود، مما يثير العديد من الإشكاليات القانونية المتعلقة بتحديد الوقت والمكان[4]، على سبيل المثال، إذا قام هاكر في بلد معين باختراق نظام

---

[1] عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، منشورات الحلبي الحقوقية، لبنان، 2015، ص20.

[2] خالد على نزال الشعار، مرجع سابق، ص10.

[3] علي عدنان الفيل، مرجع سابق، ص67.

[4] عراب مريم، الاختصاص القضائي في الجرائم المعلوماتية، كلية الحقوق والعلوم السياسية، جامعة وهران، بدون ناشر، ص276.

مصرفي في بلد آخر، فإن ذلك يطرح تساؤلات حول كيفية تحديد وقت حدوث الجريمة، هل ينبغي اعتبار توقيت الجريمة وفقًا للوقت المحلي للهاكر، أم الوقت المحلي للمصرف، أم الوقت الخاص بالخادم المستخدم في الهجوم؟ هذا النوع من التعقيد يبرز ضرورة وجود آليات قانونية مرنة للتعامل مع الجرائم الإلكترونية التي لا تعترف بالحدود.

وتُظهر طبيعة الجرائم الإلكترونية الحاجة إلى تطوير قوانين أكثر شمولية تأخذ بعين الاعتبار البعد الدولي لهذه الجرائم، فعندما تتداخل الجرائم بين دول متعددة، يصبح من الضروري تحديد القانون الذي ينبغي تطبيقه في كل حالة، في هذا السياق، يتطلب الأمر وجود تعاون دولي وتوقيع اتفاقيات قانونية تضمن تيسير التحقيقات والمحاكمات.

كما أن الاتفاقيات الدولية في هذا المجال وسيلة هامة لتسهيل تبادل المعلومات والأدلة بين الدول، مما يعزز من قدرة الأجهزة الأمنية على تتبع الجناة، على سبيل المثال، قد يتطلب التحقيق تنسيقًا بين السلطات القضائية في الدول المختلفة لتحديد مكان الجريمة بدقة، وتبادل الأدلة التي قد تكون متاحة في دول مختلفة.[1]

ولتحديد الوقت والمكان بدقة في الجرائم الإلكترونية، يتعين على المحققين استخدام تقنيات متقدمة وأدوات تحليل البيانات، يُعتبر تحليل سجلات الخوادم ومراقبة حركة البيانات من الاستراتيجيات الأساسية التي تساعد في رسم خريطة زمنية للمؤشرات والأدلة الرقمية، إضافةً إلى ذلك، يمكن استخدام التكنولوجيا المتقدمة مثل الذكاء الاصطناعي والتعلم الآلي لتحليل البيانات بشكل أسرع وأكثر دقة.

وتعتبر مرحلة المحاكمة آخر مرحلة من مراحل إجراءات الدعوى الجنائية فعندما تقدم الدعوى الجنائية إلى المحكمة تبدأ عملية طرح الأدلة في الجلسات التي تعقدها المحكمة لنظر القضية الجنائية سواء تمثلت هذه الأدلة بأدلة مباشرة كشهادة الشهود أو الإقرار أو بأدلة غير مباشرة مستمدة من استخدام الوسائل العلمية والتقنية الحديثة حيث نجد أن البينات المستقاة من وسائل التقنية الحديثة والتي تعتبر أساسا من أعمال الخبرة لا تأخذ بها المحكمة ولا القاضي على علاتها بل تخضع لتقييم القاضي فيأخذ

[1] علي عدنان الفيل، مرجع سابق، ص67.

بما اطمأن إليه وبالتالي ليست ملزمة للقاضي، ففي الشريعة الإسلامية تنضم سلطة القاضي في تقدير الوسائل الحديثة منذ الوهلة الأولى فينظر القاضي لها بفهم وإدراك ويقرر صلاحيتها للحكم أو عدم صلاحيتها حيث قال: ابن قيم الجوزيه بهذا الشأن "والحاكم إذا لم يكن فقيه النفس في الأمارات ودلائل الحال ومعرفة شواهده وفي القرائن الحالية والمقالية أضاع حقوقا كثيرة على أصحابها[1].

وبناء عليه فكل ما يقتنع به القاضي وتطمئن إليه نفسه يحكم به على أن يكون المقياس الذي يعول عليه هو مدى ارتباط الواقعة التي اعتبرها قرينة للإثبات، وقد أكدت المحكمة العليا العُمانية حرية القاضي في تكوين عقيدته حيث نصت بأنه: " لئن كان للقاضي الجزائي يملك سلطة واسعة وحرية كاملة في سبيل تقصي ثبوت الجرائم أو عدم ثبوتها، ويكون عقيدته من جميع العناصر المطروحة ما لم يقيده القانون بأدلة معينة إلا أن ذلك مقيد بسلامة التقدير والاستدلال فإن كانا غير سليمين أو كانا قائمين على أسس تخالف الثابت في الأوراق ولا تتفق مع العقل أو المنطق كان الحكم الصادر بنتيجة ذلك خاضعًا لرقابة المحكمة العليا.[2]

الأدلة الجنائية الرقمية مثل غيرها من الأدلة المادية تحتاج إلى التوثيق والتأمين بالقدر الذي يكفل لها المصداقية ويُبعد عنها العيوب وذلك لأسباب عدة منها:

1. التوثيق الذي يحفظ الأدلة الرقمية في شكلها الأصلي يستعمل لعرض وتأكيد مصداقية الدليل وعدم تعرضه لتحريف أو تعديل الصورة المسجلة بالفيديو – مثلًا – يمكن الاستعانة بها في تأكيد مدى صحة المناقشة الحية بين طرفين عن طريق مطابقة النص الرقمي مع النص المصور على الشاشة.
2. الأشخاص الذين يقومون بجمع الأدلة عليهم الإدلاء بشهاداتهم حول مطابقة الأدلة التي قاموا بجمعها مع تلك المقدمة أمام المحكمة والتوثيق هو الأسلوب الوحيد الذي يمكن المحققين من

---

[1] محمد بن أبي بكر بن أيوب بن سعد شمس الدين ابن قيم الجوزية (ت 751هـ)، الطرق الحكيمة في السياسة الشرعية، مكتبة دار البيان، بدون طبعة وبدون تاريخ، ص10.

[2] الطعن رقم 2017/1234، مجموعة المبادئ والقواعد القانونية التي قررتها المحكمة العليا، الدائرة الجزائية، 2018م، ص29.

القيام بهذا الدور أمام القضاء، ويُعتبر فشل المحقق في التمييز بين أصل الدليل وصورته أمام القضاء سببًا في بطلان الدليل.

3. من المهم توثيق مكان ضبط الدليل الرقمي في حالة إعادة تكوين الجريمة إذ أن تشابه أجهزة الحاسوب وملحقاتها يجعل من الصعب إعادة ترتيبها دون وجود توثيق سليم ومفصل يحدد الأجزاء والملحقات وأوضاعها الأصلية بدقة.

4. يشكل التوثيق جزءًا من عمليات حفظ الأدلة الرقمية حتى انتهاء إجراءات التحقيق والمحاكمة، إذ أن التوثيق يشمل تحديدًا دقيقًا للجهات التي تحتفظ بالأدلة وقنوات تداولها والتي ينبغي حصرها في نطاق محدود قدر الإمكان[1].

عند توثيق الدليل الرقمي يجب التأكد من أين؟ كيف؟ متى؟ وبواسطة من تم ضبط الدليل وتأمينه؟ كما أنه من الضروري توثيق الأدلة الرقمية بعدة طرق كالتصوير الفوتوغرافي التصوير بالفيديو، وطباعة نسخ من الملفات المخزنة في جهاز الحاسوب أو المحفوظة في الأقراص، وعند حفظ الأدلة الرقمية على الأقراص والشرائط يجب تدوين البيانات التالية على كل منها التاريخ والوقت، توقيع الشخص الذي قام بإعداد النسخة، اسم أو نوع نظام التشغيل، اسم البرنامج أو الأوامر المستعملة لإعداد النسخ، المعلومات المضمنة في الملف المحفوظ.

ورسالة التصنيف الحسابي Massage Digest Algorithm هي مجموعة من الأحرف والأرقام المركبة بطريقة حسابية خاصة تمثل أي نوع من البيانات الرقمية، ويمكن ترجمة جميع محتويات أي ملف إلى كود محدد من الأحرف والأرقام أشبه بقراءة بصمات الأصابع، إن إعداد التصنيف السليم ينتج دائمًا قراءة خاصة ومميزة لكل ملف، تختلف تمامًا عن قراءة الملفات الأخرى إلا أنها مطابقة لقراءة النسخ الصحيحة لنفس الملف.

تستخدم رسالة التصنيف الحسابي لمضاهاة الأدلة الرقمية الأصلية مع النسخ للتأكد من صحتها وعدم تعرضها لأي تلاعب أو تحريف، وعند إدخال ملف الدليل الرقمي على رسالة التصنيف

---

[1] Richard Saferstein. Criminalistics: An Introduction to Forensic Science, Upper Saddle River, NJ: Prentice, Hall, 1998, P. 34

(MD) تظهر قراءة الملف بالحروف والأرقام مطابقة لقراءة النسخ الصحيحة لنفس الملف، ولكن في حالة حدوث أي تعديل في النسخة فإن الناتج يكون قراءة مختلفة، ولذا توصيف رسالة التصنيف الحسابي بالبصمة الرقمية Digital Fingerprint[1].

وتعد عملية الحصول على الأدلة الجنائية الرقمية أمرا صعب الوصول إليه، لما تتطلبه من خبرة ومهارة كبيرة في مجال الحاسب الآلي[2]، ويرجع ذلك لتعدد صور وأشكال الجرائم المعلوماتية، ما بين مهاجمة المعلومات بغرض تدميرها، أو الاستيلاء عليها، أو قد يكون المقصود بالهجوم هو الأجهزة، كنشر فيروس يعمل على إتلاف وحداته الرئيسية مثلًا. أو قد يكون الأمر مجرد اختراق لكلمة السر الخاصة ببنك أو مؤسسة كبري، بغرض الاحتيال والحصول على الأموال، وقد تكون لمجرد إثبات الذات وإظهار المقدرة العليا في مجال الحاسب الآلي.

ولما كانت عملية تجميع الأدلة العلمية الجنائية في الجرائم المعلوماتية أو الرقمية تعد من أهم وأصعب الأمور التي تواجه عملية الإثبات الجنائي، لذا كان لزامًا أن يتم اللجوء إلى الخبير القضائي المعلوماتي أو الرقمي، ويكون متخصص لاشتقاق الدليل العلمي الفني الجنائي.

والخبير المعلوماتي هو الخبير المتخصص والمدرب على معالجة جميع أنواع الأدلة الرقمية وحصرها وتحليلها[3].

ويري بعض المتخصصين أن عملية تجميع الأدلة الرقمية في الجرائم الرقمية التي تتم عبر الشبكة العالمية (الإنترنت) تتم عبر ثلاثة مراحل المرحلة الأولي مرحلة تجميع المعلومات المخزنة لدي الطرف مقدم الخدمة، والمرحلة الثانية مرحلة المراقبة، والمرحلة الثالثة ضبط الأجهزة المشتبه فيها وفحصها فحصًا فنيًا وشرعيًا[4].

---

(1) Bruce Schneier, Applied Cryptography: protocols and source Code. New York: john wiley, 1996, P. 231.

(2) Luther G., Les Preuves en droit pénal allemand, Faculté international pour l'enseignement du droit compare, Strasbourg, session de printemps,1966, p.42.

(3) د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من 1-3 مايو 2000م، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ط3، 2004م، المجلد الثالث، ص162.

(4) Orin S. Kerr, Digital Evidence and the New Criminal Procedure, Columbia Law Review 105(1), January 2005, pp. 279-318.

وفي المرحلة الأخيرة يبدأ عمل الخبير المعلوماتي في فحص النظام الحاسوبي المشتبه فيه بمكوناته المادية ومكوناته البرمجية، سعيًا لاشتقاق الدليل المادي لتقديمه لجهة التحقيق أو المحكمة، لتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه، ولتقرير إدانة المتهم أو تأكيد براءته، وذلك جميعه وفق الأسس والقواعد الفنية المتعارف عليها والمتبعة في مجال الخبرة المعلوماتية، مع مراعاة القواعد القانونية إعلاء لمبدأ المشروعية.

المطلب الثاني

التعاون القضائي الدولي في مواجهة الجرائم الإلكترونية

تُعد الجرائم الإلكترونية من أخطر التحديات التي تواجه الأنظمة القانونية في العصر الحديث، حيث تتميز هذه الجرائم بقدرتها على التعدي على الحدود الجغرافية والتأثير على دول متعددة في وقت واحد، ولذلك، فإن التصدي لهذه الجرائم يتطلب تعاونًا دوليًا منظمًا بين الأنظمة القضائية في مختلف الدول، وهذا التعاون يساهم في تسهيل تبادل الأدلة والمعلومات، وضمان تنفيذ الإجراءات القانونية عبر الحدود، مما يعزز قدرة السلطات القضائية على التحقيق والملاحقة بشكل فعال، وبالإضافة إلى ذلك، فإن وجود اتفاقيات دولية متخصصة، مثل اتفاقية بودابست لمكافحة الجرائم الإلكترونية، يعد خطوة هامة في بناء إطار قانوني موحد يسمح بمكافحة هذه الجرائم بشكل منسق وفعّال، ومن هنا، تبرز أهمية التعاون القضائي الدولي كأداة أساسية لمواجهة التحديات التي تطرحها الجرائم الإلكترونية في عالم مترابط تقنيًا.

إن التعاون القضائي الدولي في مواجهة الجرائم الإلكترونية ضرورة ملحة في عالم يزداد فيه الترابط، مع تزايد استخدام الإنترنت وتكنولوجيا المعلومات، أصبحت الجرائم الإلكترونية تهديدًا عالميًا يتجاوز الحدود الوطنية، مما يستدعي استجابة متكاملة تتضمن تنسيق الجهود بين الأنظمة، يتطلب هذا النوع من التعاون تطوير استراتيجيات مشتركة وتبادل المعلومات والموارد لمكافحة هذه الظاهرة بفعالية.

تتسم الجرائم الإلكترونية بخصائص معقدة، حيث تُرتكب من أي مكان في العالم وتؤثر على ضحايا في أماكن مختلفة، على سبيل المثال، يمكن للمجرمين استخدام أدوات وتقنيات متقدمة لشن هجمات على المؤسسات المالية أو الحكومية، مما يسبب خسائر مالية جسيمة، لذا، فإن التعاون القضائي يُعتبر أمرًا مؤثرا، حيث يمكن للدول تبادل المعلومات حول الأساليب المستخدمة في الجرائم، وتحليل الأنماط السلوكية للجناة، يعزز هذا التعاون من القدرة على التصدي للجريمة بشكل أكثر فعالية، مما يمكن الدول من اتخاذ إجراءات سريعة وفعّالة.

الفرع الأول

وسائل التعاون القضائي الدولي

يعد التعاون القضائي الدولي أداة حيوية في مواجهة التحديات المتزايدة التي تفرضها الجرائم الإلكترونية، والتي تمتد عبر الحدود الوطنية وتستهدف الأفراد والمؤسسات على نطاق عالمي، ومع تعقيد هذه الجرائم وتنوع أساليب ارتكابها أصبح من الضروري توحيد الجهود بين الدول لتعزيز تبادل المعلومات والأدلة، وتنسيق الإجراءات القانونية اللازمة لملاحقة الجناة، ويعتمد هذا التعاون على مجموعة من المعاهدات والاتفاقيات الدولية التي تنظم المساعدة القضائية المتبادلة بين الدول، فالمساعد القضائية بين الدول هي كافة الإجراءات القانونية التي تتخذها دولة بهدف تسهيل سير المحاكمة في دولة أخرى بشأن جريمة معينة[1]، ويتخذ التعاون القضائي عدة صور والتي سوف نوجزها في التالي:

أولًا: تبادل المعلومات

تبادل المعلومات يُعدّ أحد الركائز الأساسية للتعاون القضائي الدولي في مواجهة الجرائم الإلكترونية، نظرًا للطبيعة العابرة للحدود لهذه الجرائم، فإن الدول بحاجة إلى تبادل المعلومات بسرعة وكفاءة لضمان ملاحقة الجناة ومنع توسع الأضرار، يشمل هذا التعاون تبادل المعلومات حول الأساليب المستخدمة في ارتكاب الجرائم، والبيانات المتعلقة بالتحقيقات الجارية، إضافة إلى تبادل الأدلة الرقمية التي قد تكون حاسمة في تحديد هوية الجناة وملاحقتهم قضائيًا[2].

سلطنة عُمان انضمت إلى عدة معاهدات واتفاقيات دولية وإقليمية تسهم في تعزيز التعاون القضائي، بما في ذلك تبادل المعلومات في إطار مكافحة الجرائم الإلكترونية، ومن أبرز هذه المعاهدات:

---

[1] د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، ط2، 2019، ص407.

[2] د. خالد علي الشعار، التحقيق الجنائي في الجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2024م، ص124.

1. اتفاقية الرياض العربية للتعاون القضائي: سلطنة عُمان عضو في هذه الاتفاقية، والتي تعد واحدة من أهم الاتفاقيات العربية للتعاون القضائي، وتشمل بنودًا تتعلق بتبادل المعلومات بين الدول الأعضاء، بما في ذلك تبادل المعلومات المتعلقة بالجرائم الإلكترونية وذلك وفق ما نصت عليه المادة (1) من هذه الاتفاقية[1].
2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: تركز على تعزيز التعاون بين الدول العربية في مواجهة الجرائم الإلكترونية، وتتضمن نصوصًا تتعلق بتبادل المعلومات بين الدول الأعضاء لمكافحة هذه الجرائم بفعالية أكبر[2].
3. المنظمة الدولية للشرطة الجنائية: كعضو في المنظمة الدولية للشرطة الجنائية (الإنتربول)، سلطنة عُمان تستفيد من شبكات تبادل المعلومات بين الدول الأعضاء في الإنتربول فيما يخص الجرائم العابرة للحدود، بما في ذلك الجرائم الإلكترونية، حيث أنظمت سلطنة عُمان إلى هذه المنظمة عام 1972م، حيث أن أحد مهامها هي تبادل المعلومات المتعلقة بالجريمة والمتهمين المطلوبين للعدال، وذلك من خلال نشرات يصدرها الإنتربول، أو من خلال التواصل بين ضباط الارتباط [3]، تُمثل منظمة الإنتربول مثالًا مؤثرا على كيفية يمكن للدول التعاون لمواجهة التحديات المعاصرة، من خلال تبادل المعلومات، وتنسيق العمليات، وبناء قدرات المحققين، يمكن للدول أن تعمل معًا لبناء بيئة أكثر أمانًا وتحقيق العدالة في عصر تحكمه التكنولوجيا.[4]
4. اتفاقيات التعاون القضائي الثنائية: عمان أبرمت عددًا من الاتفاقيات الثنائية مع دول أخرى تشمل تبادل المعلومات في إطار مكافحة الجرائم الإلكترونية وتقديم المساعدة القانونية المتبادلة.

---

[1] المرسوم السلطاني رقم 34/ 99 بشأن التصديق على اتفاقية الرياض العربية للتعاون القضائي.

[2] المرسوم السلطاني رقم 5/ 2015 بشأن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] العميد راشد بن سالم البادي، إنتربول مسقط ضمانة شرطية لحفظ الأمن ومكافحة الجرائم وملاحقة المجرمين، صحيفة الرؤيا، نشر بتاريخ 13 مايو 2025، تم استيراده بتاريخ 22 أكتوبر 2024م، https://alroya.om/p/132947

[4] جمال محمد خلفان محمد النقبي، التعاون الوطني والدولي في الجرائم الإلكترونية المشكلات والحلول، مجلة المعهد العالي للدراسات النوعية، مجلد 3 عدد 16 يوليو، 2023.

هذه المعاهدات تسهم في تعزيز التعاون الدولي بين سلطنة عُمان والدول الأخرى في مجال تبادل المعلومات حول الجرائم الإلكترونية، مما يسهل التعرف على مرتكبي الجرائم وجمع الأدلة التي تساعد في ملاحقتهم، فهي تعد جزءً من التشريع الوطني وذلك وفق ما أكد عليه النظام الأساسي للدولة في المادة (97)، والتي أكدت بأن لا يجوز إصدار أية قرارات أو لوائح أو تعليمات مخالفة للمعاهدات والاتفاقيات الدولية.

ثانيًا: نقل الإجراءات:

يعد نقل الإجراءات من العناصر الأساسية في التعاون القضائي الدولي، حيث يهدف إلى تقديم الدعم بين الدول في تحقيق العدالة وخاصة في مجال الجرائم الإلكترونية، حيث يقصدها أن تقوم الدولة بناءً على اتفاقية أو معاهدة باتخاذ إجراء من إجراءات التحقيق الجزائي لجريمة ارتكبت في إقليم دولة أخرى أو العكس من ذلك، بأن تطلب السلطة المختصة الحصول على إجراء تحقيق جزائي في إقليم دولة أخرى[1]، فإن نقل الإجراءات يتطلب لإجرائه مجموعة من الشروط لا بد من تحققها، كأن يكون الفعل المرتكب يشكل جريمة في كلتا الدولتين، كذلك أن لا يكون الإجراء المطلوب يتعارض مع السيادة الوطنية أو النظام العام للدولة المطلوب منها الإجراء، أن يتم التعامل مع المعلومات المطلوبة بسرية وذلك للمحافظة الأدلة المتحصلة[2].

ثالثًا: الإنابة القضائية الدولية:

الإنابة القضائية هي طلب تتقدم به جهة أو دولة للقيام بإجراء أو أكثر من إجراءات الدعوى الجزائية، حيث تقوم الدولة المطلوبة بتنفيذ هذا الإجراء لتمكين السلطات القضائية في الدولة الطالبة من متابعة قضية معينة، يتم اللجوء إلى هذا الطلب عندما يتعذر على الدولة الطالبة إجراء التحقيق بنفسها، وتكم أهمية الإنابة القضائية في تيسير الإجراءات الجزائية بين الدول وتوفير الأدلة المطلوبة لمحاكمة المتهمين، إلى جانب تجاوز عقبة السيادة الإقليمية التي تحول دون ممارسة الدولة الأجنبية

---

[1] د. خالد علي الشعار، مرجع سابق، ص125.

[2] الدليل التطبيقي للتعاون القضائي والقانوني الدولي في السائل الجنائية، المجلس الأعلى للقضاء، الادعاء العام، ط1، 2018، ص18.

لبعض الإجراءات القضائية داخل دولة أخرى[1]، مثل سماع الشهود أو إجراء التفتيش وغيرها، تأتي الإجراءات القضائية أيضا نتيجة الالتزامات التي يفرضها القانون الدولي العام، بحيث يتم تكليف السلطات القضائية في الدولة المطلوبة بالتحقيق لصالح السلطات المختصة في الدولة الطالبة، مع ضمان احترام حقوق الأفراد وحرياتهم، وفي المقابل تتعهد الدولة الطالبة بتقديم مبدأ المعاملة بالمثل[2].

بناءً على ما سبق، يتضح أن التعاون القضائي الدولي في مواجهة الجرائم الإلكترونية ليس مجرد خيار، بل هو ضرورة ملحة لضمان الأمن والسلامة على المستوى العالمي، يتطلب ذلك التزامًا من الدول لتفعيل الاتفاقيات الدولية وتطوير استراتيجيات شاملة تسهم في حماية المجتمعات من مخاطر الجرائم الإلكترونية، مما يعزز من استقرار العالم في وجه تحديات العصر الرقمي.

الفرع الثاني

التحديات التي تواجه التعاون القضائي الدولي

على الرغم من أهمية التعاون القضائي الدولي، إلا أن هناك العديد من التحديات التي تعوق فعاليته، تشمل هذه التحديات اختلاف القوانين بين الدول، حيث قد يكون هناك تباين كبير في التعريفات القانونية للجريمة الإلكترونية وطرق التعامل معها، هذا الاختلاف يؤدي إلى تأخير في الإجراءات القانونية، مما يسهل على المجرمين الهروب من العدالة. [3]

أيضًا، تواجه الدول صعوبة في تبادل المعلومات الحساسة، حيث تخشى بعض الدول من تسريب المعلومات أو استغلالها لأغراض غير قانونية، تبرز الحاجة إلى إنشاء آليات واضحة وآمنة لتبادل المعلومات، تضمن حماية البيانات وتحقيق التعاون الفعال في الوقت ذاته، ونجمع اهم تلك المعوقات في السطور التالية:

---

[1] د. جمال محمد خلفان النقبي، د. سلطان محمد سالم عوض هيسان المصعبي، التعاون والوطني والدولي في الجرائم الإلكترونية (المشكلات والحلول)، مجلة المعهد العالي للدراسات النوعية، مجلد 3 عدد 16، يوليو 2023، ص5485.

[2] د. خالد علي الشعار، مرجع سابق، ص126.

[3] منصور فهيد سعيد الحارثي. "معوقات إثبات الجرائم المتعلقة بتقنية المعلومات". المجلة القانونية، العدد 1051، فبراير 2023، ص90.

1. تباين التشريعات القانونية

تعتبر التشريعات القانونية أحد العوامل الأساسية التي تؤثر على فعالية التعاون الدولي في مكافحة الجرائم الإلكترونية، ففي العالم العربي، تختلف القوانين من دولة لأخرى، حيث تتمتع بعض الدول بتشريعات متطورة تشمل جوانب متعددة من الجرائم الإلكترونية، بينما تفتقر دول أخرى إلى قوانين شاملة تلبي الاحتياجات المتغيرة لمواجهة هذه الجرائم، هذا التباين يؤدي إلى صعوبات في التنسيق بين الدول، حيث لا تستطيع الدول التي تملك تشريعات صارمة إجراء تحقيقات فعالة مع دول أخرى ذات تشريعات متساهلة.[1]

فيسبب هذا الاختلاف في التشريعات تعقيدات في إجراءات تسليم المجرمين، إذ قد تُعاقب الجرائم في دولة ما بشكل مختلف تمامًا عن دولة أخرى، هذا الأمر يؤثر سلبًا على تنفيذ العدالة، حيث يتمكن المجرمون من الاستفادة من الثغرات القانونية للهروب من العقوبات، في العديد من الحالات، يكون هناك ارتباك حول كيفية تطبيق القانون الدولي عندما يتداخل مع القوانين المحلية، مما يجعل من الصعب تحقيق الأهداف المشتركة لمكافحة الجرائم الإلكترونية.

كما أن ضعف التعاون في تطوير تشريعات موحدة يعزز من الفجوات القائمة بين الدول، فعدم وجود معايير قانونية متسقة يؤدي إلى حدوث تضارب في الأحكام وتفسيرات متفاوتة، مما يعوق عمليات التنسيق اللازمة بين الأجهزة الأمنية، وبذلك، يصبح من المهم أن تسعى الدول العربية إلى التنسيق وتبادل التجارب من أجل تطوير إطار قانوني مشترك يساعد على مواجهة الجرائم الإلكترونية بشكل أكثر فعالية.

2. نقص الموارد التقنية

نقص الموارد التقنية من المعوقات الرئيسية التي تواجه الدول العربية في مجال مكافحة الجرائم الإلكترونية، تعاني العديد من الدول من نقص في البنية التحتية اللازمة لرصد وتحليل التهديدات

[1] د. هدية أحمد محمد زعتر، الإشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسُبل مواجهتها، مجلة البحوث القانونية والاقتصادية (المنصورة)، العدد 84، يونيو 2023، ص110.

الإلكترونية، مما يحد من قدرتها على التعامل مع هذه الجرائم بشكل فعال، تشمل هذه الموارد التقنية الأجهزة والبرمجيات اللازمة لمراقبة الشبكات وتحليل البيانات، وهو ما يتطلب استثمارات كبيرة قد تكون خارج نطاق العديد من الدول.[1]

تعاني هذه الدول من قلة الكوادر المدربة على استخدام التقنيات الحديثة وفهم كيفية تطبيقها في سياق الأمن السيبراني، تحتاج الأجهزة الأمنية إلى تدريب مستمر لتعزيز مهارات العاملين فيها، وتزويدهم بالمعرفة اللازمة للتعامل مع التهديدات المتزايدة، غياب التدريب المناسب يؤدي إلى ضعف الأداء في مواجهة الجرائم الإلكترونية، وبالتالي يتعذر على الدول تحقيق الأهداف المرجوة من التعاون الدولي.

حيث يؤدي نقص الموارد التقنية إلى اعتماد الدول على تقنيات قديمة وغير فعالة، مما يجعلها عرضة للهجمات الإلكترونية المتطورة، هذا الأمر لا يؤثر فقط على سلامة البيانات والمعلومات، بل يهدد أيضًا الثقة بين الدول في جهود التعاون، في ظل التهديدات المتزايدة، يصبح من الضروري أن تستثمر الدول في تعزيز بنيتها التحتية التقنية وتدريب الكوادر البشرية لمواجهة التحديات الأمنية بشكل أكثر فعالية.

3. تفاوت مستويات الوعي

تعتبر مستويات الوعي بأهمية الأمن السيبراني عاملًا محوريًا في مواجهة الجرائم الإلكترونية، إذ يختلف هذا الوعي بين الدول العربية بشكل كبير، في بعض الدول، توجد استراتيجيات متقدمة للحماية من الهجمات الإلكترونية، ويكون هناك دعم حكومي واسع النطاق لزيادة الوعي حول هذه القضايا، بينما تعاني دول أخرى من نقص في الوعي مما يجعل مواطنيها عرضة لمخاطر الجرائم الإلكترونية، مثل الاحتيال أو الابتزاز.[2]

---

[1] منصور فهيد سعيد الحارثي، معوقات إثبات الجرائم المتعلقة بتقنية المعلومات، *المجلة القانونية*، مجلة علمية محكمة، المجلد15، العدد4، فبراير 2023، ص1081.

[2] مجمع البحوث والدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، نزوى – سلطنة عُمان، 2016

هذا التفاوت في الوعي ينعكس سلبًا على قدرة المجتمعات على التصدي للجرائم الإلكترونية، فعندما يكون المواطنون غير مدركين لأساليب الاحتيال وكيفية حماية بياناتهم الشخصية، يصبحون أهدافًا سهلة للمجرمين، وبالتالي، فإن تعزيز الوعي العام يعتبر خطوة أساسية في بناء مجتمع آمن يستطيع مواجهة التهديدات الإلكترونية.

فإن غياب الوعي المناسب يؤثر أيضًا على قدرة الحكومات في تنفيذ استراتيجيات فعالة لمكافحة الجرائم الإلكترونية، ففي بعض الحالات، قد تعجز الحكومات عن اتخاذ تدابير وقائية مناسبة بسبب عدم فهم المخاطر المرتبطة بتكنولوجيا المعلومات، من هنا، يصبح من الضروري أن تتبنى الدول العربية برامج توعية مستمرة تشمل جميع فئات المجتمع، بهدف تعزيز الفهم العام حول الأمن السيبراني وأهمية حماية المعلومات.

4. الاعتبارات السياسية

تُعتبر التوترات السياسية بين الدول العربية عائقًا رئيسيًا أمام التعاون في مجال مكافحة الجرائم الإلكترونية، حيث تُؤثر العلاقات المتوترة بين الدول على تبادل المعلومات والبيانات الضرورية للتصدي للجرائم، فالدول التي تعاني من قلة الثقة قد تتردد في مشاركة المعلومات، مما يعيق جهود التحقيق والملاحقة.[1]

هذا الوضع السياسي يُعقد الأمور أكثر عندما يتعلق الأمر بالجرائم العابرة للحدود، حيث قد يكون لدى الدول مصلحة في حماية معلوماتها أو تجنب التعاون مع دول تعتبرها خصومًا، هذا يُعزز من قدرة المجرمين على الاستفادة من الفراغات في التعاون الأمني، مما يؤدي إلى تفشي الجرائم الإلكترونية بشكل أكبر.

للتغلب على هذه المعوقات، من الضروري تعزيز الحوار والتفاهم بين الدول، يُساهم إنشاء منصات للتعاون الأمني، حتى في ظل التوترات السياسية، في تسهيل تبادل المعلومات وتعزيز

---

[1] خالد علي الجنيبي، الجريمة الإلكترونية بين تحديات الواقع واستشراف المستقبل، في المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية– ICACC المملكة العربية السعودية، الرياض: جامعة الإمام محمد بن سعود الإسلامية. كلية علوم الحاسب والمعلومات، (2015)، ص81 – 86.

الثقة، ذلك يتطلب إرادة سياسية قوية من الدول المعنية لتحقيق التوازن بين المصالح الوطنية والتعاون الأمني الدولي.

5. تحديات التنسيق

يمثل غياب التنسيق الفعّال بين الجهات المعنية في الدول العربية عقبة كبيرة أمام جهود مكافحة الجرائم الإلكترونية، عدم وجود آليات واضحة للتنسيق بين الوزارات والهيئات الأمنية يُفضي إلى عمل كل جهة بشكل منفصل، مما يُعقد من عمليات تبادل المعلومات والتعاون في التحقيقات، هذا الوضع يضعف من قدرة الدول على التنسيق السريع والفعال في مواجهة التهديدات.

فإن ضعف قنوات الاتصال بين مختلف الجهات يُؤدي إلى عدم فعالية الاستجابة للجرائم الإلكترونية، عندما تعمل كل جهة بمعزل عن الأخرى، قد تتأخر الإجراءات القانونية والتحقيقات بسبب عدم تبادل المعلومات المؤثرة في الوقت المناسب، هذه الفجوات تؤدي إلى تفشي الجرائم الإلكترونية وتعقيد جهود مكافحة المجرمين.

لتجاوز هذه التحديات، يجب أن تسعى الدول إلى إنشاء آليات تنسيق فعالة تُعزز من التعاون بين جميع الجهات المعنية، ينبغي تطوير بروتوكولات واضحة لتبادل المعلومات وتحديد الأدوار والمسؤوليات لكل جهة، هذا التعاون يُعزز من فعالية الإجراءات الأمنية ويُسهم في بناء استجابة شاملة للتحديات المرتبطة بالجرائم الإلكترونية.

6. غياب التنسيق الإقليمي

تفتقر الدول العربية إلى منظمات إقليمية قوية تعمل على تعزيز التعاون في مجال الأمن السيبراني، مما يُعقد من جهود التصدي للجرائم الإلكترونية، غياب هذه المنظمات يُعني أن هناك نقصًا في التوجيه والإشراف على المبادرات المشتركة، مما يقلل من فعالية التعاون الأمني، بدون وجود إطار عمل إقليمي، تظل كل دولة تعمل بشكل مستقل، مما يؤدي إلى عدم التنسيق والتكامل في الجهود.[1]

[1] د. جمال محمد خلفان محمد النقبي، د. سلطان محمد سالم عوض هيسان المصعبي، مرجع سابق، ص5498.

هذا الوضع يُعزز من الفجوات في القدرات الأمنية بين الدول، فالدول التي تفتقر إلى الدعم الإقليمي قد تجد صعوبة في الوصول إلى الموارد اللازمة أو تبادل المعرفة والخبرات الضرورية لمكافحة الجرائم الإلكترونية، هذا يخلق بيئة تُستغل من قِبل المجرمين، مما يزيد من المخاطر التي تواجهها الدول.

لذا، يُعتبر إنشاء منظمات إقليمية فعّالة أمرًا مؤثرا لتعزيز التعاون في مجال الأمن السيبراني، يجب أن تشمل هذه المنظمات تنسيق الجهود، وتبادل المعلومات، وتطوير استراتيجيات مشتركة للتصدي للتهديدات، من خلال تعزيز التنسيق الإقليمي، يمكن للدول العربية تعزيز قدراتها على مكافحة الجرائم الإلكترونية وتحقيق أهدافها الأمنية بشكل أكثر فعالية.[1]

[1] مارية بوجداين، ومريم ءال سيدي الغازي، تحديات مواجهة الجرائم المعلوماتية وآليات الحماية.، مجلة العلوم الجنائية، المركز المغربي للدراسات والاستشارات القانونية وحل المنازعات، ع7، 2021، ص93 – 127.

المبحث الثاني

الإثبات في الجرائم الإلكترونية

تُعد وسائل الإثبات في الجرائم الإلكترونية من العناصر الأساسية التي يعتمد عليها القضاء في الوصول إلى الحقيقة وإثبات وقوع الجريمة. ونظرًا للطبيعة الفريدة لهذه الجرائم، التي تتسم بالاعتماد على الأدوات الرقمية والشبكات الإلكترونية، فإن طرق جمع الأدلة وتحليلها تختلف بشكل كبير عن الجرائم التقليدية. في هذا السياق، يعتبر الدليل الرقمي هو العمود الفقري لإثبات الجرائم الإلكترونية، سواء كانت هذه الأدلة في صورة بيانات محفوظة على الأجهزة الإلكترونية أو في شكل سجلات الشبكات الرقمية[1].

يهدف هذا المبحث إلى استعراض وسائل الإثبات المتاحة في الجرائم الإلكترونية وفقًا للتشريع العُماني، مع التركيز على حجية الدليل الرقمي أمام القضاء ودوره الحاسم في تحديد المسؤولية الجنائية. كما سيتم تسليط الضوء على أهمية الخبرة الفنية ودورها في تحليل وتفسير الأدلة الرقمية، خاصةً في ظل تعقيد هذه الجرائم واعتمادها على تقنيات متقدمة تتطلب فهمًا عميقًا من قبل الخبراء المختصين.

المطلب الأول

حجية الدليل الرقمي أمام القضاء

هدفت التشريعات الجزائية إلى تنظيم العلاقات بين الأفراد داخل المجتمع وكذلك تنظيم العلاقات بين السلطات المختلفة، حيث يسعى القانون إلى تحقيق العدالة والوصول إلى الحقيقة من خلال إصدار أحكام عادلة، لذلك تُمنح القاضي مساحة من الحرية لممارسة دوره في الوصول الى الحقيقة، وهو ما اعتمدت عليه معظم التشريعات الجزائية، التي تتيح للقاضي حرية الاقتناع بالأدلة وتكوين قناعته منها، وقد أصبحت هذه الحرية قاعدة أساسية في عملية الإثبات الجنائي، فبقبول الأدلة

---

[1] د. مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، مقالة علمية، ملحق خاص، العدد3، الجزء الثاني، أكتوبر 2018، ص190.

والاقتناع بها يعتبر الخطوة الأولى التي يقوم بها القاضي فيما يتعلق بالأدلة الجزائية[1]؛ بناءً على ذلك فإن الأدلة الإلكترونية التي تم توضيح تعريفها وخصائصها في الفصل الأول، يجب الحصول عليها بشكل قانوني وصحيح تمامًا مثل الأدلة التقليدية، خاصة وأن القاضي الجزائي يسعى أثناء المحاكمة للتأكد من شرعية الإجراءات المتعلقة بالأدلة، لذا اعترفت معظم التشريعات ومن ضمنها المشرع العُماني وكذلك أحكام القضاء بحجية مخرجات أجهزة الحاسب الآلي كأدلة إثبات أمام القاضي الجزائي، وذلك في ظل مجموعة من الشروط التي ستتناولها الدراسة.

الفرع الأول

الحجية القانونية للأدلة الرقمية

تعد الحجية القانونية للأدلة الإلكترونية موضوعًا معقدًا يتطلب دراسة دقيقة للمسائل المتعلقة بمشروعية هذه الأدلة وقبولها في الأنظمة القضائية المختلفة، يعتبر الاختلاف في الآراء حول مشروعية الدليل الإلكتروني انعكاسًا لتنوع الأنظمة القانونية والإجراءات الجنائية في مختلف البلدان، وهذا يعكس الأوضاع الاجتماعية والسياسية التي تؤثر على كل نظام قانوني.

تختلف نظم الإجراءات الجنائية باختلاف الأوضاع الاجتماعية والسياسية للشعوب، مما يفرض على التشريعات الجنائية اتباع نظام إجرائي معين، يمكن تقسيم هذه الأنظمة إلى ثلاث فئات رئيسية: النظام الحر، والنظام المقيد، والنظام المختلط، يعكس كل من هذه الأنظمة طريقة مختلفة في تقييم الأدلة وتحديد حجيتها.[2]

في النظام الحر، يتمتع القاضي بسلطة مطلقة في تقدير الأدلة المعروضة عليه، حيث لا يلزمه القانون بأنواع معينة من الأدلة، تعزز هذه الحرية قدرة القاضي على الوصول إلى الحقيقة بناءً على القناعة الشخصية، مما يمنحه قدرة على استخدام الأدلة الإلكترونية كمصدر موثوق، لكن هذا

---

[1] د. خالد علي الشعار، التحقيق الجنائي في الجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2024م، ص345.

[2] حمد سالم العلوي، حجية الأدلة الإلكترونية في القانون العُماني، مجلة العلوم الاقتصادية والإدارية والقانونية، مجلد 7، العدد العاشر، 2023, ص37–53. https://doi.org/10.26389/AJSRP.L030923

النظام يعاني من عيب أساسي، وهو اختلاف تقييم الأدلة من قاضي لآخر، مما يخلق عدم استقرار قانوني للمتقاضين.

على الجانب الآخر، يعكس النظام المقيد موقفًا مختلفًا، حيث يحدد المشرع الجزائي الوسائل التي يمكن اعتمادها لإقامة الدليل، ولا يُسمح للقاضي بتوظيف قناعته الشخصية في تقدير الأدلة، يتطلب هذا النظام من القضاة الالتزام بالنصوص القانونية المحددة، مما قد يعيق العدالة إذا لم تكن الأدلة المتاحة تلبي الشروط المقررة، على الرغم من ذلك، قد يعزز هذا النظام الثقة في عملية التقاضي نظرًا لوضوح القواعد والإجراءات المتبعة.[1]

النظام المختلط هو مزيج من النظامين السابقين، حيث يجمع بين إيجابيات النظام الحر والقيود المفروضة في النظام المقيد، يسمح هذا النظام للقاضي بتقدير الأدلة مع تحديد طرق الإثبات القانونية، مما يخلق توازنًا بين حرية القاضي ومتطلبات القوانين المعمول بها، يعد هذا النظام من الأنظمة الأكثر فائدة، حيث يمكن للقاضي توجيه الأطراف واستكمال الأدلة الناقصة، مما يسهم في تحقيق العدالة بشكل أفضل.[2]

في السياق العُماني، اعتمد المشرع مذهب الإثبات الحر، مما يعكس توجهًا نحو تعزيز كفاءة النظام القضائي، وهذا ما أكدت عليه المادة (215) من قانون الإجراءات الجزائية حيث نصت بأنه: "يحكم القاضي في الدعوى حسب القناعة التي تكونت لديه بكامل حريته، ومع ذلك لا يجوز له أن يبني حكمه على دليل لم يطرح على الخصوم أمامه في الجلسة أو على معلوماته الشخصية"، يسمح هذا النظام للقاضي باستكمال الأدلة الغير مكتملة واستيضاح النقاط الغامضة في القضية، شرط أن لا تتعارض مع نصوص القانون، يعد هذا النهج خطوة إيجابية نحو تطوير نظام قانوني يتسم بالمرونة والفعالية، فيرجع قبول الأدلة لدى القاضي إلى مدى اقتناعه بها، إلا أن المشرع العُماني قيد هذه القناعة بعدة شروط يجب أن يتقيد بها القاضي، حيث يجب أن تكون هذه الأدلة مستمدة وتم الحصول

---

[1] د. مزهر جعفر عبيد شرح قانون الإجراءات الجنائية العُماني الجزء الأول، ط1، أكاديمية السلطان قابوس العلوم الشرطة، مسقط، 2008، ص209-211.

[2] حمد سالم العلوي، مرجع سابق، ص37.

عليها بطرق مشروعة[1]، وكذلك يتوجب عليه مناقشتها مع الخصوم مناقشة تفصيليه، وكذلك يجب عليه الالتزام بطرق الإثبات الخاصة بالمسائل غير الجزائية.

ومما لا شك فيه أن الأدلة الإلكترونية تعتبر جزءًا متزايد الأهمية من القضايا الجنائية، حيث تساهم التكنولوجيا في تسهيل عمليات الجريمة وتعقيد جهود المكافحة، لذا، فإن تطوير الأطر القانونية التي تعترف بهذه الأدلة وتحدد كيفية تقييمها يعد أمرًا مؤثرا لضمان العدالة، تحتاج التشريعات إلى أن تكون ديناميكية بما يكفي للتكيف مع التغيرات التكنولوجية السريعة.

لذلك تتطلب الحجية القانونية للأدلة الإلكترونية استراتيجيات فعالة لضمان قبولها في المحاكم، يجب أن تتضمن هذه الاستراتيجيات تعزيز الوعي حول كيفية جمع وتحليل الأدلة الإلكترونية، إضافة إلى ضرورة التدريب المستمر للمحققين والقضاة حول التعامل مع هذه الأدلة، كما يجب أن يكون هناك تعاون دولي لتوحيد المعايير القانونية والإجرائية المرتبطة بالأدلة الإلكترونية.

وقد أخذت أحكام القضاء الجنائي الفرنسي بحجية الدليل الإليكتروني في الإثبات، إذ قضت في حكميها الصادرين بتاريخ 29 يناير 2014، و25 مارس 2014 بأن الصور التي التقطتها الكاميرات المثبتة علي قارعة الطريق يمكن أن تشكل أساسًا لتحرير محضرًا ضد مخالف إشارات المرور[2]. من ناحية أخري، فقد أقرت محكمة النقض الفرنسية بحجية الصور الفوتوغرافية كدليل إثبات لتقديم السائق إلي المحاكمة لمخالفته قانون الطرق[3].

وقد مُنحت الفرصة لمحكمة النقض الفرنسية مرة أخرى أن تدلي بدلوها حول حجية الدليل الرقمي في الإثبات، إذ قضت في حكم حديث لها بأن الدليل الكتابي يتساوى في حجيته أمام القضاء مع ذلك الدليل الذي يتم الحصول عليه بالوسائل التكنولوجية، وأضافت المحكمة أنه إذا كانت محكمة

---

[1] د. لورنس سعيد الحوامدة، حجية الأدلة الرقمية في الاثبات الجنائي، مجلة البحوث الفقهية، العدد 36، أكتوبر 2021، ص907.

[2] **Géraldine Vial, Étienne Vergès et Vincent Gautrais,** Preuves scientifiques et technologiques, Le procès pénal à l'épreuve de la génétique Chroniques, 9, 2019, p. 179-197; Cass. crim., 29 janv. 2014, n° 13-83.283; Cass. crim., 13 déc. 2006, n° 06-82.047; 11 mai 2011, n° 10-87; Cass. crim. 25 mars 2014, n° 13-81.559; 21 mars 2017, n° 16-82.404 ; 20 mars 2018, n° 17-83.765.

[3] Cass. crim., 11 mars 2014, n° 13-82.550; 26 mars 2014, n° 13-87.099.

الموضوع قد أدانت الطاعن بتهمة تجاوز السرعة المقررة علي الطريق استنادا إلي ما أورده جهاز الرادار من بيانات فإنها تكون قد استندت إلي دليل له أصله الثابت في الأوراق، وأن النعي ببطلان هذا الدليل لعدم النص عليه في المادة (537) من قانون الإجراءات الجنائية يكون قائمًا علي غير أساس متعينًا رفضه[1].

وفي 30 أكتوبر 2018، استند القاضي في محكمة المخالفات إلى قراءة عداد السيارة في القضاء بإدانة سائق السيارة لتجاوز السرعة المقررة، وقالت المحكمة أنه إذا سجل جهاز الرادار السرعة للسائق المخالف ب 106 كم/ساعة في حين أن أقصي سرعة مسموح بها هي90 كم/ساعة، وأردفت المحكمة أن ما تم تسجيله على عداد السيارة هو بمثابة دليل كتابي له حجيته في الإثبات أمام القضاء ما لم ينازع المتهم بحدوث غش أو تلاعب في جهاز الرادار أو عديد السيارة[2].

وفي موضع آخر، فقد قضت محكمة النقض الفرنسية بإدانة أحد أصحاب الأعمال لتشغيله ليلًا عمال محظور تشغيلهم ليلًا من النساء والأطفال والكبار خلال الفترة من الأول من يونيه 2013 وحتي 5 فبراير 2104 استنادًا إلي ما أورده تقرير مفتش العمل بتشغيل هؤلاء العمال المحظور تشغيلهم بما أستخلصه من جهاز البصمة الذي تم تركيبه في مكان العمل لتوقيع العمال من خلاله بالحضور والانصراف، تحديد عدد العمال وهويتهم وساعات العمل، ومن ثم فإن هذا المستخرج من جهاز البصمة بما يفيد عمل هؤلاء الأشخاص المحظور تشغيلهم ليلًا يرتقي إلي مرتبة الدليل الكتابي الوارد في المادة (537) من قانون الإجراءات الجنائية، له حجيته في الإثبات حتي تقديم دليل يخالف ذلك، وأن الدليل الإليكتروني هو ثمرة التقدم العلمي والتكنولوجي[3].

---

(1) Cass. crim., 8 mars 2016, n° 15-83.019.
(2) Cass. Crim., 30 Oct. 2018, Bull. Crim., 8, pourvoi No 18-81.318, p.587.
(3) Cass. Crim., 30 Oct. 2018, Bull. Crim., 8, pourvoi No 17-87.520, p.588.

الفرع الثاني

القواعد الإجرائية ومشروعية الدليل الإلكتروني[1]

القواعد الإجرائية ومشروعية الدليل الإلكتروني تعتبر من المواضيع الحديثة التي تثير اهتمامًا متزايدًا في مجال القانون، خصوصًا في ظل التطور التكنولوجي المتسارع واعتماد العديد من الدول على الوسائل الإلكترونية في جمع الأدلة وتقديمها أمام المحاكم، وتهدف القواعد الإجرائية إلى تنظيم كيفية التعامل مع الأدلة الإلكترونية وضمان احترام الحقوق والحريات الأساسية للأفراد أثناء جمعها واستخدامها، مما يطرح تساؤلات حول مدى مشروعية الأدلة المستمدة من الوسائل الرقمية[2].

أولًا: القواعد الإجرائية للدليل الإلكتروني:

تتطلب طبيعة الجرائم المرتبطة بتقنية المعلومات والأدلة الإلكترونية المترتبة عليها وضع قواعد إجرائية دقيقة تضمن سلامة العملية القانونية، لقد أوجب ظهور فئات جديدة من الجرائم التقنية على جميع المشاركين في النظام القانوني فهم الأشكال المتعددة للدليل الإلكتروني، في ظل التطور العلمي المستمر، يتطور شكل الجريمة، مما يستلزم تحديث الأساليب المستخدمة لجمع الأدلة، تعتمد القواعد الإجرائية للدليل الإلكتروني على تحديد ما إذا كان الدليل علميًا أو فنيًا أو إلكترونيًا، بينما تبقى بعض الأدلة التقليدية، مثل الأدلة القولية، بدون تغيير يذكر، مما يزيد من أهمية تطوير الأساليب المستخدمة لجمع الأدلة الإلكترونية.

تتطلب القوانين المعمول بها توافر شروط معينة للاعتراف بالدليل الرقمي واعتباره ذي حجية قانونية في إجراءات الإثبات، من أبرز هذه الشروط هو الحصول على الدليل بشكل مشروع، وعدم مخالفته للدستور أو القوانين المعمول بها، إن الدساتير الحديثة تهدف بشكل رئيسي إلى صيانة كرامة الإنسان وحماية حقوقه، وبالتالي تتضمن نصوصًا تنظم القواعد الأساسية المتعلقة بالاستجواب،

---

[1] د. مزهر جعفر عبيد، مرجع سابق، ص209-211.

[2] د. أسامة حسين محي الدين عبدالعال، حجية الدليل الرقمي في الاثبات الجنائي للجرائم المعلوماتية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 76، يونيو 2021، ص675.

والتوقيف، والحبس، والتفتيش، على سبيل المثال، ينص النظام الأساسي للدولة في سلطنة عُمان في المادة (33) على أن "للمساكن حرمة، فلا يجوز دخولها بغير إذن أهلها، إلا في الأحوال التي يبينها القانون وبالكيفية المنصوص عليها فيه"، كما تؤكد المادة (36) على حماية الحياة الخاصة وسرية المراسلات بجميع أنواعها، مما يستدعي الالتزام بالإجراءات القانونية المحددة عند جمع الأدلة.[1]

تتطلب الإجراءات الجنائية احترام الحقوق والحريات للأفراد، وأي مخالفة لهذه القوانين تؤدي إلى بطلان الأدلة المتحصل عليها، تتمثل الطرق غير المشروعة للحصول على الدليل في أساليب مثل إكراه المتهم لفك تشفير كلمة السر للوصول إلى البيانات المخزنة، أو استخدام التحريض على ارتكاب الجرائم الإلكترونية، كما يشمل ذلك التجسس المعلوماتي، والاستخدام غير المصرح به للحاسوب، والتنصت أو المراقبة الإلكترونية للحصول على الأدلة الرقمية، من الضروري أيضًا تجنب أساليب التدليس أو الغش في جمع الأدلة، إذ أن أي استخدام لهذه الطرق يعرض الأدلة للخطر ويؤثر سلبًا على مصداقية العملية القانونية برمتها.

تتجلى أهمية القواعد الإجرائية للدليل الإلكتروني في تحديد معايير قبول الأدلة في المحكمة، يجب أن تتم عملية جمع الأدلة الإلكترونية وفقًا لإجراءات محددة تحترم الحقوق القانونية للأفراد، حيث يتوجب على السلطات القانونية أن تتبع خطوات دقيقة لضمان أن الأدلة قد تم جمعها بطريقة قانونية وغير متجاوزة، يجب أن يتم توثيق كل خطوة من خطوات جمع الأدلة، بما في ذلك كيفية الوصول إلى الأجهزة أو الأنظمة المستخدمة، وتفاصيل حول كيفية معالجة البيانات المستخرجة، مما يعزز من موثوقية الدليل المقدم في المحكمة.

علاوة على ذلك، تتطلب القواعد الإجرائية للدليل الإلكتروني تطوير مهارات وكفاءات الكوادر القانونية والجنائية، يجب أن يكون المحققون، القضاة، والمحامون على دراية كافية بالتقنيات المستخدمة في جمع وتحليل الأدلة الرقمية، هذا يتضمن فهم كيفية عمل الأنظمة المعلوماتية، وكيفية حماية الأدلة من العبث، وأهمية استخدام الأدوات التقنية الحديثة في التحقيقات الجنائية، التدريب

[1] حمد سالم العلوي، مرجع سابق، ص37.

المستمر في هذا المجال يعتبر ضروريًا لضمان أن جميع المعنيين قادرون على التعامل بفاعلية مع التحديات المرتبطة بالجرائم الإلكترونية. [1]

في هذا السياق، تلعب التكنولوجيا الحديثة دورًا كبيرًا في تسهيل عمليات جمع وتحليل الأدلة، التقنيات مثل تحليل البيانات الكبيرة، والذكاء الاصطناعي، وأدوات الكشف عن التلاعب تساهم في تعزيز دقة وفعالية جمع الأدلة الرقمية، ومع ذلك، يجب مراعاة القواعد القانونية والأخلاقية عند استخدام هذه التقنيات، لضمان عدم انتهاك حقوق الأفراد أو المساس بسلامة الإجراءات القانونية.

تتطلب التعاملات القانونية المتعلقة بالأدلة الرقمية التوازن بين الابتكار في استخدام التكنولوجيا والالتزام بالقيم القانونية الأساسية، إن غياب هذا التوازن يؤدي إلى انتهاكات خطيرة للحقوق الشخصية، ويؤثر على مصداقية النظام القانوني ككل، لذلك، يجب على المشرعين، المحققين، والجهات القضائية العمل معًا لوضع إطار قانوني وإجرائي متكامل، يضمن التعامل مع الأدلة الإلكترونية بشكل يحترم حقوق الأفراد ويعزز من كفاءة النظام القانوني.[2]

يشترط في الأدلة الجنائية أن تكون مشروعة، مما يعني أنها يجب أن تُجمع وفقًا للإجراءات القانونية المعمول بها، مع مراعاة الحقوق التي تنص عليها المواثيق الدولية والإعلانات المتعلقة بحقوق الإنسان، وبالمثل قرر المشرع العُماني البطلان في المادة (208) من قانون الإجراءات الجزائية على عدم مراعاة أحكام القانون المتعلقة بأي إجراء جوهري[3]، ويعد الحصول على إذن رسمي من الجهة المختصة بالتحقيق شرطًا أساسيًا للتفتيش وجمع الأدلة، ولا يجوز اتخاذ أي إجراء دون ذلك، يتعين أن يكون هذا الإذن مكتوبًا، محدد التاريخ، وموقعًا من الجهة المختصة، كما يجب أن يتضمن تفاصيل دقيقة حول نوع الجريمة المراد التحقيق فيها، ومكان التفتيش، سواء كان شخصًا، منزلًا، أو مؤسسة.

وفي إطار الحماية القانونية للخصوصية، أكدت المحكمة العليا في سلطنة عُمان على أهمية التقيد بمبدأ اقتصار التفتيش على حدود الغرض منه، يعني ذلك أن التفتيش يجب أن يقتصر على

---

[1] د. مزهر جعفر عبيد، مرجع سابق، ص209-211.

[2] حمد سالم العلوي، مرجع سابق، ص43.

[3] المادة (208) من المرسوم السلطاني رقم 99/97 بشأن اصدار قانون الإجراءات الجزائية.

الأشياء المتعلقة بالجريمة المعنية، وفي حال تم ضبط أشياء خارج نطاق أمر التفتيش، فإن ذلك يعد انتهاكًا للخصوصية وقد يؤدي إلى بطلان تلك الأدلة، يشدد هذا المبدأ على ضرورة حماية حقوق الأفراد وضمان عدم التعدي على خصوصياتهم، مما يعكس التوازن المطلوب بين تحقيق العدالة وحماية الحقوق الشخصية في سياق الجرائم الإلكترونية.[1]

يتضح من استقراء نصوص المشرع العُماني أن النظام القانوني القائم يأخذ بنظام الإثبات الحر، مما يمنح القاضي القدرة على قبول الأدلة الإلكترونية كجزء من الأدلة المعروضة في الدعوى، في هذا السياق، يبقى تقدير القاضي للدليل المعروض عليه هو الأساس، حيث يملك الحرية الكاملة في قبول أو رد هذه الأدلة وفقًا لاقتناعه الشخصي، ومع ذلك، فإن هذه الحرية ليست مطلقة، بل تحكمها ضوابط قانونية تضمن حسن سير العدالة، فعلى القاضي أن يستند إلى أدلة صحيحة تتوافر فيها القوة القانونية للإثبات، مما يعزز من مصداقية القرارات القضائية.[2]

كما أن المشرع العُماني قد وضع استثناءات على حرية القاضي في مجال الإثبات، تتضمن ضرورة طرح الأدلة على بساط البحث وإتاحة الفرصة للمناقشة خلال المحاكمة، يتعين على القاضي الالتزام بطرق الإثبات المحددة في المسائل غير الجزائية، وهذا يمثل قيدًا إضافيًا على سلطته التقديرية، يُعتبر هذا التوجه القانوني خطوة نحو تحقيق توازن بين حرية القاضي في تكوين قناعته وضمان حقوق الأفراد ومبدأ المحاكمة العادلة، مما يعكس الرغبة في تحقيق العدالة بشكل فعّال ومنظم.

ثانيًا: مشروعية الدليل الرقمي:

تُظهر مشروعية الدليل الإلكتروني في التشريع العُماني التزام النظام القانوني بمبدأ الإثبات الحر، حيث تُتيح للقاضي حرية واسعة في قبول الأدلة أو ردها، بناءً على قناعته الشخصية، ينص قانون الإجراءات الجزائية العُماني، وتحديدًا في المادة (215)، على أن القاضي يحكم حسب القناعة التي تتكون لديه، مما يعكس قدرة القاضي على تقييم الأدلة بشكل مستقل، ومع ذلك، هناك قيود على

---

[1] د. مزهر جعفر عبيد، مرجع سابق، ص209-211

[2] حمد سالم العلوي مرجع سابق، ص43.

هذه الحرية، حيث يتعين على القاضي عدم الاعتماد على أدلة لم تُطرح أمام الخصوم، وهو ما يضمن حقوق الدفاع ويعزز مبدأ العدالة.

حيث تجدر الإشارة إلى أنه عند النظر إلى الدليل الإلكتروني، نجد أن التشريع العُماني قد تفاعل مع الجرائم الإلكترونية منذ عام 2001، عندما تم تجريم جرائم الحاسب الآلي بموجب المرسوم السلطاني رقم 72/2001 بتعديل بعض أحكام قانون الجزاء، وقد تم تطوير هذا الإطار التشريعي لاحقًا بإصدار قانون خاص بمكافحة جرائم تقنية المعلومات في عام 2011، مما يعكس التقدير المتزايد لأهمية الأدلة الرقمية في القضايا الجنائية.

على الرغم من وجود قوانين متخصصة، إلا أن نظام الإثبات الحر يبقى هو السائد، هذا يعني أن الدليل الإلكتروني يُعتبر مشروعًا وذو قيمة قانونية، شريطة أن يكون مقبولًا من قبل القاضي، الذي يُقدر مصداقيته وفقًا لقناعته الشخصية، بالتالي، يمكن للقاضي أن يعتمد على الأدلة الإلكترونية، مثل الرسائل الإلكترونية أو السجلات الرقمية، في بناء حكمه.

ومع ذلك، يجب أن يمارس القاضي هذه الحرية بطريقة مدروسة، حيث يتعين عليه التأكد من أن الأدلة المعروضة صحيحة وموثوقة، إذا كانت الأدلة تحتوي على نقاط ضعف أو تعارض مع المعايير القانونية، فقد يتعرض الحكم للنقض من قبل المحكمة العليا، لذلك، هناك استثناءات محددة تتطلب من القاضي التمسك بأدلة صحيحة ومناسبة، وإتاحة الفرصة للمناقشة خلال المحاكمة، لضمان تحقيق العدالة.[1]

من المهم أيضًا أن يلتزم القاضي بطرق الإثبات المقررة في المسائل غير الجزائية، بالإضافة إلى ضرورة تسبيب الحكم، مما يُعزز من شرعية القرارات القضائية، هذه القيود تعمل على حماية حقوق المتقاضين وتضمن عدم تعسف القضاة في استخدام سلطاتهم.

إن الحاجة إلى إطار قانوني قوي يدعم الحجية القانونية للأدلة الإلكترونية أصبحت ملحة، يجب أن يجمع هذا الإطار بين الاعتراف بالتقدم التكنولوجي والامتثال لمبادئ العدالة وضمان حقوق المتقاضين، إن تحقيق هذا التوازن يمثل تحديًا كبيرًا، ولكنه ضروري لمواجهة الجرائم الإلكترونية في العصر الحديث.

---

[1] د. مزهر جعفر عبيد، مرجع سابق، ص209-211.

المطلب الثاني

الخبرة الفنية في الجرائم الإلكترونية وسلطة القاضي في تقديرها

في ظل التطور التكنولوجي الهائل، أصبح العالم الرقمي جزءًا أساسيًا من حياتنا اليومية، مما أدى إلى نشوء الجرائم الإلكترونية وانتشارها بأساليب متعددة ومعقدة. لمواجهة هذا النوع من الجرائم، تعتمد السلطات القضائية بشكل كبير على الخبرة الفنية لتفسير الأدلة التقنية والكشف عن الأدلة الرقمية، يتناول هذا المطلب دور الخبرة الفنية في كشف وتحليل الجرائم الإلكترونية، وكيفية تقييم القاضي لهذه الخبرة في ضوء القوانين والإجراءات المعمول بها، ويُسلط الضوء على أهمية الخبرة الفنية في تحقيق العدالة، ومسؤولية القاضي في تقديرها وفقًا للمعايير الموضوعية، مما يضمن استناد الأحكام إلى أسس علمية دقيقة تتماشى مع تطورات العصر الرقمي[1].

الفرع الأول

الخبرة في مجال الجريمة الإلكترونية

الخبير في مجال الجريمة الإلكترونية يعد عنصرًا أساسيًا في عملية التحقيق والمحاكمة في القضايا المتعلقة بالجرائم الإلكترونية، ونظرًا لأن الجرائم الإلكترونية تعتمد بشكل كبير على التكنولوجيا والبيانات الرقمية، فإن دور الخبير يتسم بأهمية خاصة لضمان دقة وسلامة الإجراءات القانونية[2].

وتُعَدُّ الخبرة في مجال الجريمة الإلكترونية عنصرًا أساسيًا للكشف عن الجرائم ذات الصلة بالتقنية والحاسب الآلي، منذ بداية ظهور هذه الجرائم، بدأت جهات الاستدلال والتحقيق في الاستعانة بالخبراء الفنيين المتخصصين، الذين يمتلكون المهارات والمعرفة اللازمة لفهم طبيعة الجرائم الإلكترونية وجمع الأدلة المرتبطة بها.

---

[1] تقي مباركية، د فاطمة الزهراء غريبي، دور الخبرة في إثبات المعاملات الإلكترونية والقواعد الفنية التي تحكمها في اكتشاف الدليل الرقمي، مجلة العلوم الإنسانية، جامعة الأخوة منتوري قسطنطينية، المجلد 33، العدد2، 2022، ص130.

[2] راشد محمد حمد المري، ضرورة الاستعانة بالخبير الإلكتروني أمام المحاكم الجنائية، مجلة كلية الشريعة والقانون بتهفنا الإشراف، دقهلية، العدد 25، 2022، الإصدار الثاني، الجزء الرابع، ص3273.

تتضح أهمية الاستعانة بالخبراء في الجريمة الإلكترونية بشكل خاص عند غيابهم، ففي حالة عدم وجود خبراء، تفتقر جهات التحقيق إلى القدرة على تحليل شفرات الجريمة وكشف غموضها، كما أن غياب الخبرة قد يؤدي إلى تدمير الأدلة المهمة أو محوها أثناء التعامل معها، بسبب عدم الفهم الكافي للتقنيات المستخدمة، لذا، يجب أن يكون الخبير في الجريمة الإلكترونية مؤهلًا علميًا ومتمرسًا في هذا المجال، مما يمكنه من تقديم تقييم دقيق وموثوق للأدلة.

القواعد القانونية المتعلقة بالخبرة الإلكترونية تشمل إجراءات اختيار الخبراء وواجباتهم، غالبًا ما تحدد التشريعات الطريقة التي يتم بها اختيار الخبراء، من خلال التسجيل في جداول خاصة تُعدها وزارة العدل أو المجالس القضائية المختصة، وفقًا لقانون الإجراءات الجزائية العُماني، يتطلب الاستعانة بخبير تحديد طبيعة الخبير سواء كان شخصًا طبيعيًا أو معنويًا، يتم اختيار الخبير بناءً على أمر يُصدره عضو الادعاء العام، سواء كان الخبير مسجلًا في جدول الخبراء أو لم يكن، مما يضمن مرونة في الاختيار.[1]

في مجال الجريمة الإلكترونية، غالبًا ما تُفضل شركات أو مؤسسات متخصصة في تقنية المعلومات، نظرًا لما تمتلكه من خبرات متعمقة، يمكن لهذه المؤسسات تقديم مجموعة متنوعة من الخبرات التي تتعلق بأبعاد متعددة من التقنيات المعلوماتية، يجادل بعض الفقهاء بأن الخبرة في المجال ليست محصورة فقط على الخريجين من الجامعات أو الكليات المتخصصة في تقنية المعلومات، بل يكفي أن يمتلك الخبير مهارات عملية ومعرفة كافية بالأنظمة والأدوات المستخدمة في هذا المجال.[2]

القواعد الفنية التي تحكم عمل الخبير الإلكتروني تختلف عن تلك التي تحكم الخبرة التقليدية، يتطلب عمل الخبير الإلكتروني مستوى عالٍ من المعرفة التقنية، بالإضافة إلى القدرة على تطبيق تلك المعرفة في سياق قانوني، يجب أن يكون الخبير قادرًا على توضيح المعلومات الفنية بطريقة تفهمها المحكمة، مما يعزز من مصداقية الأدلة التي يقدمها.[3]

---

[1] فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية،2016، ص598.

[2] د. مزهر جعفر عبيد، مرجع سابق، ص209-211.

[3] ميمون حنان، سلطة القاضي في تقدير الدليل الرقمي، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماجستير في الحقوق، جامعة محمد البشير الإبراهيمي، 2023، ص229.

الفرع الثاني

سلطة القاضي في تقدير الخبرة الفنية في الجرائم الإلكترونية

تُعد سلطة القاضي في تقدير الخبرة الفنية في الجرائم الإلكترونية عنصرًا أساسيًا لضمان تحقيق العدالة في القضايا المعقدة التي تتطلب فهمًا دقيقًا للتكنولوجيا، مع تطور التكنولوجيا وانتشار الجرائم الإلكترونية، برزت الحاجة الملحة لوجود خبراء فنيين يمكنهم تقديم رؤى متخصصة تساهم في توضيح ملابسات الجرائم، ومع ذلك، تبقى السلطة النهائية في تقدير هذه الخبرة بيد القاضي، الذي يلعب دورًا محوريًا في تحديد مدى صلاحية الأدلة الفنية وتأثيرها على سير الدعوى، وفيما يلي سوف نتطرق لصلاحيات القاضي في تقدير الخبرة ومدى قوة الإثبات وسلطة القاضي في قبولها أو ردها:

أولًا: صلاحيات القاضي في تقدير الخبرة:

1. **تقييم الخبرة:** يبدأ دور القاضي في تقدير الخبرة الفنية بتقييم كفاءة الخبير الذي يتم الاستعانة به، يتعين على القاضي النظر في المؤهلات الأكاديمية والخبرة العملية للخبير، بما في ذلك سنوات العمل في المجال ومجالات تخصصه، يعتمد القاضي على مجموعة من المعايير لتحديد ما إذا كان الخبير مؤهلًا لتقديم شهادة موثوقة، يُعتبر التقييم الدقيق لهذه المعايير أمرًا حيويًا، حيث أن عدم كفاءة الخبير يمكن أن يؤدي إلى قرارات قضائية خاطئة.[1]

في حالة الجرائم الإلكترونية، يجب أن يكون الخبير متمرسًا في الأدوات والتقنيات المستخدمة في الفضاء الرقمي، بالإضافة إلى فهم عميق للجوانب القانونية المرتبطة بتلك الجرائم، لذلك، يُسهم تقييم كفاءة الخبير في توفير ضمانات حول جودة الأدلة المقدمة.

---

[1] صكصك محمد، الإثبات الجنائي في الجرائم الإلكترونية، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية بالجزائر، 2022، ص45.

2. **قبول الأدلة:** بمجرد أن يقيّم القاضي الخبير، تأتي مرحلة أخرى تتعلق بقبول الأدلة، يمتلك القاضي السلطة المطلقة لتحديد ما إذا كانت الأدلة التي تم جمعها وتحليلها من قبل الخبير مقبولة أم لا، إذا كانت الأدلة غير موثوقة أو تم جمعها بطريقة تثير الشكوك، يمكن للقاضي أن يستبعدها.[1]

هذا الاستبعاد قد يعتمد على عدة عوامل، منها طريقة جمع الأدلة، صحة الإجراءات المتبعة، ومدى مطابقة الأدلة للمعايير القانونية المعمول بها، إن استبعاد الأدلة غير الموثوقة يحمي حقوق الدفاع ويضمن عدم استخدام معلومات قد تؤدي إلى حكم غير عادل.

3. **الاستقلالية:** تُعتبر استقلالية القاضي في تقدير الخبرة الفنية من العوامل المهمة التي تضمن نزاهة العملية القضائية، يجب أن يكون القاضي غير متحيز، وأن يتخذ قراراته بناءً على وقائع القضية والأدلة المقدمة، وفي حالة تباين الآراء بين الخبير والقاضي، يمكن للقاضي أن يختار عدم الاعتماد على رأي الخبير إذا كان لديه أسباب موضوعية تدعمه، كما تعتبر هذه الاستقلالية ضرورية لخلق توازن بين الخبرة الفنية والقرارات القضائية، مما يعزز من مصداقية النظام القضائي.

4. **التوجيه للمحكمة:** يمكن للقاضي أن يطلب من الخبير تقديم توضيحات إضافية أو إجابات على أسئلة محددة تتعلق بالأدلة المقدمة، هذا يسمح للقاضي بفهم أعمق للموضوع ومساعدته في اتخاذ قرار مستنير، في بعض الحالات، قد يحتاج القاضي إلى استشارة خبراء آخرين أو طلب آراء متعددة لضمان تقييم شامل للأدلة، تتطلب الجرائم الإلكترونية فهمًا معقدًا، ولذلك يعتبر التواصل الفعّال بين القاضي والخبير ضروريًا للوصول إلى الحقائق الكاملة[2].

5. **تسبيب الحكم:** عندما يصدر القاضي حكمه، يتعين عليه تسبيبه بناءً على الأدلة المتاحة، بما في ذلك رأي الخبير، يجب أن يكون التسبيب منطقيًا وموثقًا بشكل جيد، مما يسمح للخصوم بفهم الأسباب التي أدت إلى الحكم، إذا كانت هناك ثغرات في التسبيب، قد يؤدي ذلك إلى

---

[1] د. مزهر جعفر عبيد، مرجع سابق، ص209-211.

[2] د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، ط2، دار النهضة العربية، القاهرة، 2008، ص104، 105.

نقض الحكم من قبل المحكمة العليا، حيث أن التسبيب الجيد يعكس التزام القاضي بمعايير العدالة، كما يُعزز من ثقة الجمهور في النظام القضائي.

6. **توازن بين الخبرة الفنية والقانون:** يتطلب تقدير الخبرة الفنية في الجرائم الإلكترونية من القاضي تحقيق توازن دقيق بين المعايير الفنية والأنظمة القانونية، ينبغي أن يكون لدى القاضي معرفة بأساسيات التقنية المستخدمة، ولكنه أيضًا يجب أن يحترم الأطر القانونية التي تحكم العملية القضائية.

هذا التوازن يُعزز من قدرة القاضي على اتخاذ قرارات مستندة إلى تحليل موضوعي وشامل للأدلة، مما يساهم في حماية حقوق المتقاضين وضمان تحقيق العدالة.

ثانيًا: القوة الإثباتية للدليل الرقمي، وسلطة القاضي في قبوله أو رده

تتعلق القوة الإثباتية للدليل الرقمي بالقدرة على استخدام هذا النوع من الأدلة كقرينة قانونية يعتمد عليها القاضي في اتخاذ القرارات القضائية، يتطلب قبول الدليل الرقمي تحقيق شرطين أساسيين: الأول هو المصداقية، والثاني هو الصلة المنطقية أو الدلالة الصحيحة التي تربط الدليل بالنتيجة المراد إثباتها.

المصداقية تعني أن الدليل يجب أن يكون موثوقًا، وأن يثبت خلوه من التلاعب أو الشكوك حول أصله، يتولى خبراء مختصون فحص الأدلة الرقمية للتأكد من صحتها وسلامتها، يقوم هؤلاء الخبراء بإجراء تحليل دقيق للأدلة، مستندين إلى تقنيات علمية وأساليب متقدمة، ثم يقدمون تقريرًا يوضح درجة ثبات الدليل ومصداقيته، يُعتبر هذا التقرير عنصرًا مؤثرا، حيث يعتمد عليه القاضي في تقييم مدى قبول الدليل.[1]

من جهة أخرى، تعتمد الصلة المنطقية على قدرة الدليل الرقمي على إظهار العلاقة بين الوقائع المدعاة والنتيجة المطلوبة، يتولى القاضي مسؤولية دراسة الدليل بعناية، وتحديد ما إذا كان

---

[1] محمد الأمين البشرى، الأدلة الجنائية الرقمية مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية، مجلد17، العدد33، أبريل (2002)، ص129.

يوفر دليلًا واضحًا على الفرضيات المعروضة، في هذا السياق، يقوم القاضي بمقارنة الدليل الرقمي مع الأدلة الأخرى المقدمة، وهذا يساعده في بناء صورة شاملة حول القضية، ويعزز من قدرته على اتخاذ قرار مستنير[1].

إذا تم التحقق من أن الدليل الإلكتروني يتسم بالثبوت القطعي، ويظهر دلالة قوية على النتيجة، فإنه يعتبر بمثابة قرينة قطعية، في هذه الحالة، يمكن استخدامه كدليل نهائي يُعتمد عليه في إصدار الحكم، مثال على ذلك هو تسجيلات مرئية توثق حدثًا معينًا، حيث تُعتبر دليلًا قويًا إذا كانت قد جُمعت بواسطة جهات حكومية أو محايدة، وكان الخبراء قد أكدوا على سلامتها.[2]

على النقيض، إذا كان الدليل الإلكتروني مشكوكًا في صحته أو مصدره، فإنه يُعتبر قرينة ضعيفة، ولا يُؤخذ بها في الاعتبار، أمثلة على ذلك تشمل الملفات النصية التي لا تحمل توثيقًا واضحًا أو التي يمكن تعديلها بسهولة، مما يثير شكوكًا حول مصداقيتها، في هذه الحالات، يُنظر إلى الدليل على أنه غير قادر على دعم الدعوى أو الدفاع بشكل فعّال.

كما يظهر الدليل الإلكتروني كمرجح في بعض الحالات، خصوصًا إذا كانت الأدلة تشير إلى ظن غالب، مثل التسجيلات الصوتية أو المرئية التي قد تدعم أحد الجانبين، ومع ذلك، يتطلب الأمر من القاضي أن يكون مقتنعًا بمصداقية هذا الدليل، وألا تكون هناك أدلة أخرى تُعارضه بشكل قوي.

---

[1] د. سليمان محمد المعلم، بدور بنت خالد الكربي، تأثير التقنية على وسائل الاثبات الرقمية في النظام السعودي، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بدمهور، جامعة الازهر، العدد 46، يوليو 2024، ص3297.

[2] محمود صبحي محمد محمود زايد، حجية الدليل الإلكتروني في الإثبات الجنائي وسلطة القاضي في تقديره، *مجلة بنها*، للعلوم الإنسانية، العدد 1، الجزء 2،2022، ص39.

الخاتمـــــة

في ختام هذه الدراسة التي تناولت بشكل واسع موضوع إجراءات التحقيق والمحاكمة في الجرائم الإلكترونية وفق التشريع العُماني، وتم التأكيد على الأهمية المتزايدة لدراسة هذا الموضوع في ظل التوسع الانتشار السريع لتقنية المعلومات، وتزايد الاعتماد على الإنترنت والتقنيات الإلكترونية في شتى مجالات الحياة، وقد تم التركيز على الاطار القانوني الإجرائي لمواجهة الجرائم الإلكترونية، ومدى الحاجة الملحة في لتطوير هذه الإجراءات القانونية لتواكب هذا التطور الرقمي، وتوفير الأدوات الضرورية لجهات إنفاذ القانون لمواجهة الجرائم الإلكترونية، وحماية المجتمع والأفراد من المخاطر التي قد تنشأ في الفضاء الإلكتروني.

سعت الدراسة إلى تحليل النصوص القانونية ذات الصلة، وتبين أن سلطنة عُمان بذلت جهودًا كبيرة سواء من حيث سن التشريعات أو تطوير التقنيات اللازمة، إلا أنه نتيجة للتطور المستمر للفضاء الإلكتروني والتقنيات الحديثة التي تستخدم في الجرائم الإلكترونية، بات من الضروري على المشرع العُماني أن يواكب هذا التطور وأن يكون أكثر مرونة لمواجهة هذه التحديات التي تفرضها الطبيعة المتغيرة لهذه الجرائم.

أظهرت الدراسة أن الإجراءات التقليدية المتبعة وفق المنصوص عليها في قانون الإجراءات الجزائية العُماني قد لا تتناسب وطبيعة الجرائم الإلكترونية، وهذا ما يعزز من الحاجة إلى إصدار قانون خاص للإجراءات الجزائية في الجرائم الإلكترونية، ومن جانب آخر تؤكد الدراسة على ضرورة استمرار تأهيل وتدريب الكوادر القضائية التي تتعامل مع قضايا الجرائم الإلكترونية بما يتماشى مع التحديات المستقبلية.

ويبقى الأمل في أن تساهم هذه الدراسة في تعزيز الجهود الوطنية الرامية إلى تعزيز الأمن في سلطنة عُمان بشتى مجالاته، وتساهم في تطوير السياسات والتشريعات والإجراءات القانونية في مكافحة الجرائم الإلكترونية، وقد خلصت الدراسة إلى مجموعة من النتائج والتوصيات نذكرها في التالي:

أولًا: النتـــائج

خلصت هذه الدراسة إلى الوصول لمجموعة من النتائج تتمثل في التالي:

1. تطور التشريعات العُمانية: تبين أن التشريع العُماني قد واكب التطورات التقنية، وذلك من خلال إصدار قوانين مثل قانون مكافحة جرائم تقنية المعلومات، والذي يهدف إلى التصدي للجرائم الإلكترونية وحماية المجتمع من تأثيراتها السلبية.
2. حدد المشرع العُماني عدة جهات مختصة بالتعامل مع الجرائم الإلكترونية في مرحلة جمع الاستدلالات والتحقيق الابتدائي، والتي ورد تحديدها في عدة مواضع تشريعية، وهي شرطة عمان السلطانية وفق ما نصت عليه المادة (31) من قانون الإجراءات الجزائية، وكذلك وزارة النقل والاتصالات وتقنية المعلومات، وذلك وفق القوانين واللوائح المنظمة لاختصاصاتها، وكذلك مركز الدفاع الإلكتروني وفق الصلاحيات الممنوحة له بموجب المرسوم السلطاني رقم **2020/64** بإنشاء مركز الدفاع الإلكتروني وتحديد اختصاصاته، وقد يتخفف الادعاء العام من القيود الإجرائية ويقوم بإجراء جمع الاستدلالات في بعض الحالات التي تطلب ذلك.
3. مأموري الضبط القضائي في الجرائم الإلكترونية على دراية كافية وتأهيل جيد في كيفية التعامل مع الجرائم الإلكترونية، بدأ من تلقي البلاغات والشكاوى والانتقال إلى موقع مسرح الجريمة وكيفية التعامل معه بالمعاينة وفق خطوات عملية تحافظ على الأدلة الإلكترونية، إلا أنه نتيجة للتطور المستمر في الفضاء الإلكتروني يتطلب الأمر استمرارهم في التأهيل والتدريب.
4. قد يحدث تنازع في الاختصاص بين مأموري الضبط القضائي عندما تتداخل اختصاصاتهم في تنفيذ بعض الإجراءات، مما يستدعي تحديد الجهة المختصة قانونًا لتنفيذ تلك الإجراءات وذلك كما أسلفنا من خلال هذا البحث فيما يتعلق بتلقي بلاغات حدوث اختراق او تهديد امني إلكتروني والتي نص عليها نظام مركز الدفاع الإلكتروني بضرورة إخطاره فورا عن أي خطر إلكتروني، وكذلك نصت المادة (19) من قانون الحماية البيانات الشخصية على الزام المتحكم عند حدوث اختراق للبيانات الشخصية إبلاغ وزارة النقل والاتصالات وتقنية المعلومات وصاحب البيانات الشخصية عن الاختراق.

5. إن مسرح الجريمة في الجرائم الإلكترونية يختلف عن مسرح الجريمة في الجرائم التقليدية الأمر الذي يتطلب معه إجراءات خاصة تختلف عن الإجراءات التقليدية المنصوص عليها في قانون الإجراءات الجزائية.
6. تحديات جمع الأدلة الإلكترونية: يواجه المحققون تحديات تقنية وإجرائية في جمع الأدلة الإلكترونية بسبب تعقيدات الجرائم الإلكترونية واعتمادها على وسائل تكنولوجية متطورة، مما يستدعي خبرات خاصة وإجراءات دقيقة لضمان سلامة الأدلة وصحتها.
7. الخصوصية وحقوق المتهمين: تبرز مخاوف بشأن حماية حقوق المتهمين وخصوصياتهم أثناء التحقيقات الإلكترونية، حيث قد تؤدي بعض الإجراءات إلى انتهاك هذه الحقوق إذا لم تُنفذ وفقًا للضوابط القانونية المعتمدة.
8. الدعم الفني والتقني: يتطلب التحقيق في الجرائم الإلكترونية وجود دعم فني متطور وأدوات تقنية متقدمة لضمان جمع الأدلة وحفظها وتحليلها بشكل ملائم.

ثانيًا: التوصيـــــــات:

1. تطوير تشريعات داعمة: دعوة المشرع العُماني بمراجعة وتحديث قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم2011/12 بشكل دوري لمواكبة التطورات السريعة في مجال الجرائم الإلكترونية، وضمان شموليته لمختلف أنواع هذه الجرائم الإلكترونية وأساليبها المتغيرة.
2. تُشير نتائج الدراسة إلى أن قانون الإجراءات الجزائية العُماني الصادر بالمرسوم السلطاني رقم 99/97 يفتقر إلى أحكام خاصة بإجراءات التحقيق في الجرائم الإلكترونية بشكل خاص، مما يقلل من فعاليته في التعامل مع التعقيدات التقنية لهذه الجرائم، ويستلزم تعديل القانون لتضمين إجراءات خاصة بالاستدلال، والتحقيق الابتدائي، والمحاكمة بما يتناسب مع طبيعة هذه الجرائم.
3. التدريب والتأهيل: ضرورة تدريب القضاة والمحققين والمتخصصين على كيفية التعامل مع الأدلة الإلكترونية وإجراءات التحقيق والمحاكمة في الجرائم الإلكترونية، لضمان الكفاءة والاحترافية في المعالجة.

4. يوصي الباحث بدراسة إنشاء قضاء متخصص ومدرب ومحققين مؤهلين، للنظر في الجرائم الإلكترونية، نظرًا لصعوبة الكشف عن هذه الجرائم وإثباتها والتحقيق فيها، كما أن هذه الجرائم تتطلب خبرات ومعطيات خاصة قد لا تكون متوفرة في القضاء التقليدي.
5. حماية حقوق الأفراد: التأكيد على أهمية حماية حقوق المتهمين وخصوصيتهم عند التعامل مع الأدلة الإلكترونية، وضمان اتخاذ جميع الإجراءات القانونية التي تمنع أي انتهاك لهذه الحقوق.
6. تعزيز التعاون الدولي: دعم التعاون الدولي مع الجهات المختصة في الدول الأخرى في التحقيقات المرتبطة بالجرائم الإلكترونية العابرة للحدود، حيث تعتبر هذه الجرائم ذات طبيعة دولية وتتطلب تعاونا دوليا فعالا.
7. توفير تقنيات متقدمة: ينصح بتوفير أحدث الأدوات والتقنيات اللازمة لجمع وتحليل الأدلة الرقمية بما يتماشى مع التطورات الحديثة، وذلك لضمان دقة وسرعة التحقيقات.
8. توحيد الجهود الوطنية في التعامل مع الأدلة الرقمية: يكون ذلك بإنشاء مختبر رقمي وطني يعنى بالتعامل مع الأدلة الإلكترونية، فإن من شأن ذلك أن يساهم في توحيد الإجراءات في التعامل مع الأدلة الرقمية وذلك بأن تنصب في جهة واحد مختصة ومؤهلة.

هذه النتائج والتوصيات تعزز من قدرة النظام القانوني العُماني على مواجهة التحديات التي تفرضها الجرائم الإلكترونية، وتؤكد الحاجة إلى استجابة شاملة ومستدامة للتطورات التقنية المتسارعة.

قائمة المراجع والمصادر

أولًا: المراجع العامة

1. د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2016م.
2. د. أحمد عوض بلال، الإجراءات الجنائية المقارنة والنظام الإجرائي في المملكة العربية السعودية، دار النهضة العربية للنشر والتوزيع، القاهرة، 2017.
3. الدليل التطبيقي للتعاون القضائي والقانوني الدولي في السائل الجزائية، المجلس الأعلى للقضاء، الادعاء العام، ط1، 2018.
4. المعجم الوسيط، مجمع اللغة العربية، ط4. مكتبة الشروق الدولية، 1425هـ – 2004م.
5. د. أمال عبد الرحيم عثمان، شرح قانون الإجراءات الجنائية، الهيئة المصرية العامة للكتاب، القاهرة، ط2، 1991.
6. د. برهم محمد ظاهر، تنظيم التحقيق الابتدائي في الجرائم، ط1، دار وائل للنشر، عمان،2013.
7. د. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، مطبعة جامعة عين شمس، القاهرة، 1978م.
8. د. سليمان مرقص، أصول الإثبات وإجراءاته، الأدلة المقيدة، الجزء الثالث، دار الحلبي للمنشورات الحقوقية، بيروت، 1998.
9. على محمد السيد الشريف الجرجاني، معجم التعريفات، دار الفضيلة.
10. د. عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، 1999. بدون ناشر.
11. د. فوزية عبد الستار، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ط1، 1986م.
12. د. ماجد راغب الحلو، القانون الإداري، دار المطبوعات الجامعية، الإسكندرية، 1994.
13. د. مجيد خضر أحمد السبعاوي، مولان قادر أحمد، الضرورة الإجرائية في مرحلة التحقيق الابتدائي – دراسة تحليلية مقارنة، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2017.

14.محمد بن أبى بكر عبد القادر الرازي، مختار الصحاح.

15.د. محمد الأمين البشري، التحقيق الجنائي المتكامل، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، ط1، 1998.

16. محمد سعيد نمور أصول الإجراءات الجزائية، شرح لقانون أصول المحاكمات الجزائية، دار الثقافة للنشر والتوزيع، ط2، عمان 2011.

17.د. مزهر جعفر عبيد شرح قانون الإجراءات الجزائية العُماني الجزء الأول، ط1، أكاديمية السلطان قابوس العلوم الشرطة، مسقط، 2008.

18.د. مزهر جعفر عبيد، الوسيط في شرح قانون الإجراءات الجزائية العُماني (المحاكمة والحكم وطرق الطعن في الأحكام)، الجزء الثاني، دار الثقافة للنشر والتوزيع، عمّان، 2020م.

19.د. هشام زوين، الموسوعة الشاملة التقادم "المدني، الجنائي، الإداري والنظم القانونية الشبيهة بالتقادم "المنظومة المتكاملة لأحكام التقادم والسقوط والانقضاء وعدم السماع في ضوء الفقه والقضاء والتشريع والمحاماة"، مركز المحمود للنشر وتوزيع الكتب القانونية، 2008.

ثانيًا: المراجع المتخصصة

1.د. أحمد يوسف الطحاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، القاهرة، 2015م.

2.د. أنيس حسيب السيد المحلاوي، الخبرة القضائية في الجرائم المعلوماتية أو الرقمية، دار الفكر الجامعي، الإسكندرية، 2016م.

3.د. بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، ط1. دار الفكر الجامعي، الإسكندرية، 2011م.

4.د. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002.

5.د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت: دراسة مقارنة، دار النهضة العربية، القاهرة، 2009.

6.د. خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية، 2014م.

7.د. خالد علي الشعار، التحقيق الجنائي في الجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2024م، ص124.

8.د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2019م.

9.رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم الإلكترونية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، ط2، 2017.

10.د. سليمان احمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة 2007.

11.د. سامي جلال، الأدلة المتحصلة من الحاسب وحجيتها في الإثبات، دار الكتب القانونية، القاهرة، 2011م.

12.د. سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية للنشر والتوزيع، القاهرة، 1999.

13.د. طه السيد أحمد الرشيدي، الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق في النظام الجزائي المصري والسعودي، دار الكتب والدراسات العربية، الإسكندرية، ط1، 2016.

14.د. عبد الفتاح بيومي حجاري، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، ط1، الإسكندرية، 2006.

15.د. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2004.

16.د عبد الله ذيب محمود، د أسامة إسماعيل دراج، الوجيز في الجرائم الإلكترونية القواعد الموضوعية والإجرائية، دار الثقافة، الأردن، عمّان، ط1، 2022م.

17.عراب مريم، الاختصاص القضائي في الجرائم المعلوماتية، كلية الحقوق والعلوم السياسية، جامعة وهران، بدون ناشر.

18.د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت/ دراسة مقارنة، عالم الكتب الحديث، 2004.

19.علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، المكتب الجامعي الحديث الإسكندرية، ط1، 2012.

20.د. عمر أبو بكر بن يونس، الجريم الناشئة عن استخدام الإنترنت، كلية الحقوق، جامعة المنصورة، 2004.

21.د. عمر محمد أبوبكر بن يونس، الدليل الرقمي، الجمعية العربية لقانون الإنترنت، ط1. 2007م.

22.د. عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، 2004.

23.عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، منشورات الحلبي الحقوقية، لبنان، ط1، 2015.

24.عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، منشورات الحلبي الحقوقية، لبنان، 2015.

25.فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية،2016.

26.د. محمد أنور عاشور، المبادئ الأساسية في التحقيق الجنائي العملي، عالم الكتب، القاهرة، 1969.

27.محمد أنور عاشور: الموسوعة في التحقيق الجنائي العملي، ط3، عالم الكتب، 1998.

28.د. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2004.

29.د. محمد محمد عنب، استخدام التكنولوجيا الحديثة في الإثبات الجنائي، 2007م.

30.محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري 175 لسنة 2018. دراسة تحليلية مقارنة، دار الجامعة الجديدة، الإسكندرية، 2019.

31.د. محمود صلاح العادلي، الفراغ التشريعي في مجال مكافحة الجرائم الإلكترونية، 2009.

32.د. محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة (جرائم نظم الاتصالات والمعلومات)، المكتب الجامعي الحديث، الكتاب الثاني، الإسكندرية، 2017.

33.د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1. مطبعة الشرطة، 1430هـ - 2009م.

34.د. ممدوح عبد الحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، دار الحقوق، الشارقة، 2001.

35.د، ممدوح عبد الحميد عبد المطلب، البحث الجنائي الرقمي (في جرائم الكمبيوتر والإنترنت)، المكتبة القانونية، القاهرة، ط1، 2000.

36.د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992م.

37.د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة، دار النهضة العربية، القاهرة، 1998.

38.د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، ط2. دار النهضة العربية، القاهرة، 2008.

39.د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 1997م.

40.د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 1999.

41.د. هلالي عبد اللاه أحمد، قانون العقوبات وأزمة الحاسبات، دار النهضة العربية، القاهرة، 1998.

ثالثًا: الرسائل والبحوث

1. أحمد فقيه فهد الطويلة، بطلان إجراءات التفتيش في القانونين الأردني والكويتي، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2011.

2. د. ايمن عبد الحفيظ عبد الحميد، استراتيجية مكافحة جرائم الحاسب الألى، دراسة مقارنه، رسالة دكتوراه، أكاديمية الشرطة، بدون سنة طبع.

3. حسين محمد فلاح البرايسه، الركن المعنوي للجرائم الإلكترونية وفقًا لقانون العقوبات الأردني، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2021.

4. خالد على نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، بحث مقدم لاستيفاء متطلبات الحصول على درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة المنصورة، 2022.

5. د. سالم مبارك سليم، الحماية الجنائية للأدلة المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة،2019.

6. صكصك محمد، الإثبات الجنائي في الجرائم الإلكترونية، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية بالجزائر، 2022.

7. ميمون حنان، سلطة القاضي في تقدير الدليل الرقمي، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماجستير في الحقوق، جامعة محمد البشير الإبراهيمي، 2023.

8. د. يوسف بن سعيد الكلبانى، الحماية الجزائية للبيانات الإلكترونية في التشريعين العُماني والمصري دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، دار النهضة العربية 2017، ط1.

رابعًا: الأبحاث والمقالات والدوريات

1. د. أحمد مالك، د، إبراهيم الخال، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، المركز الجامعي، الجزائر، المجلد5. العدد1. 2021م.

2. د. أسامة حسين محيي الدين، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية (دراسة تحليلية مقارنة)، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 76. 2021م.

3. تقي مباركية، د فاطمة الزهراء غريبي، دور الخبرة في إثبات المعاملات الإلكترونية والقواعد الفنية التي تحكمها في اكتشاف الدليل الرقمي، مجلة العلوم الإنسانية، جامعة الأخوة منتوري قسطنطينية، المجلد 33، العدد2، 2022.

4. جمال زين العابدين أمين أحمد، الاختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية "دراسة مقارنة، مجلة مستقبل العلوم الاجتماعية، جامعة عبد الملك السعدي، المغرب، العدد الرابع، يناير 2021م.

5. د جمال محمد خلفان النقبي، د. سلطان محمد سالم عوض هيسان المصعبي، التعاون والوطني والدولي في الجرائم الإلكترونية (المشكلات والحلول)، مجلة المعهد العالي للدراسات النوعية، مجلد 3 عدد 16، يوليو 2023.

6. خالد علي الجنيبي، الجريمة الإلكترونية بين تحديات الواقع واستشراف المستقبل، في المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية– ICACC المملكة العربية السعودية، الرياض: جامعة الإمام محمد بن سعود الإسلامية. كلية علوم الحاسب والمعلومات، (2015).

7. حمد سالم العلوي، حجية الأدلة الإلكترونية في القانون العُماني، مجلة العلوم الاقتصادية والإدارية والقانونية، مجلد 7، العدد العاشر.

8. حنان محمد الحسيني، سحر على عبد الله، التحقيق الجنائي الرقمي، مجلة جامعة الملك سعود، كلية الحقوق والعلوم السياسية، المجلد 33. العدد2. 2021م.

9. حميد قادري، لحسن إمعلي، محمد الحبيب اعمیار، إجراءات المحاكمة في الجريمة الإلكترونية، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الخامس، الرباط، السنة الجامعية 2018-2019.

10. د. خالد مصطفى الجسمي، الإثبات الجنائي بالأدلة الرقمية، دار السلام للطباعة والنشر، العدد34. 2017م، ص26.

11. راشد محمد حمد المري، ضرورة الاستعانة بالخبير الإلكتروني أمام المحاكم الجنائية، مجلة كلية الشريعة والقانون بتهفنا الإشراف، دقهلية، العدد 25، 2022، الإصدار الثاني، الجزء الرابع.

12. د. سليمان محمد المعلم، بدور بنت خالد الكربي، تأثير التقنية على وسائل الإثبات الرقمية في النظام السعودي، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بدمهور، جامعة الأزهر، العدد 46، يوليو 2024.

13. د. عزالدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية – مخبر المؤسسات الدستورية والنظم السياسية، مجلة محكمة، الجزائر العدد الرابع، 2018.

14. د. علي محمود علي حمودة، أدلة إثبات الجرائم الإلكترونية وتقديرها في إطار نظرية الإثبات الجنائي، مجلة الأمن القومي، أكاديمية شرطة دبي، مجلد17، عدد 1، يناير 2009.

15. مارية بوجداين، ومريم ءال سيدي الغازي، تحديات مواجهة الجرائم المعلوماتية وآليات الحماية.، مجلة العلوم الجنائية، المركز المغربي للدراسات والاستشارات القانونية وحل المنازعات، ع7، 2021.

16. مجمع البحوث والدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، نزوى – سلطنة عُمان، 2016

17. مجموعة الأحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها للسنتين القضائيتين السابعة عشر والثامنة عشر، المكتب الفني مجلس الشؤون الإدارية للقضاء، 2019.

18.د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من 1-3 مايو 2000م، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ط3، 2004م، المجلد الثالث.

19.د. محمد الأمين البشري، الأدلة الجنائية الرقمية: مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد 17. العدد 33. 2002م.

20.محمد الأمين البشرى، الأدلة الجنائية الرقمية مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية، مجلد17، العدد33، أبريل (2002).

21.منصور فهيد سعيد الحارثي، معوقات إثبات الجرائم المتعلقة بتقنية المعلومات، المجلة القانونية، مجلة علمية محكمة، المجلد15، العدد4، فبراير 2023.

22.محمود صبحي محمد محمود زايد، حجية الدليل الإلكتروني في الإثبات الجنائي وسلطة القاضي في تقديره، مجلة بنها، للعلوم الإنسانية، العدد 1، الجزء2، 2022م.

23.د. محمود نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسب الآلي والأنترنت، رسالة دكتوراه للعلوم الشرطية، تخصص القيادة الأمنية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض، 2004م.

24.د. مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، مقالة علمية، ملحق خاص، العدد3، الجزء الثاني، أكتوبر 2018.

25. لطيفة الخلفي، سارة اليزيد، سناء المخوض، عثمان السفياني، المعاينة في الجرائم الإلكترونية، جامعة محمد الخامس بالرباط، كلية العلوم القانونية والاقتصادية والاجتماعية، السنة الجامعية 2018/2019.

26.د. لورنس سعيد الحوامدة، حجية الأدلة الرقمية في الإثبات الجنائي، مجلة البحوث الفقهية، العدد 36، أكتوبر 2021.

27.د. هدية أحمد محمد زعتر، الإشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسُبل مواجهتها، مجلة البحوث القانونية والاقتصادية (المنصورة)، العدد 84، يونيو 2023.

28.د. وهيبة لعوارم، الدليل الرقمي في مجال الإثبات الجنائي وفقًا للتشريع الجزائري، المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، مجلد57. العدد2. 2014م.

خامسًا: المواقع الإلكترونية

1. مختبر الأدلة الجنائية يتجه لإضافة "الوسائط المتعددة"، صحيفة الوطن العُمانية، العدد 11942. تاريخ النشر 25 أبريل 2016م، الموقع الإلكتروني (http://alwatan.om).

2. العميد راشد بن سالم البادي، إنتربول مسقط ضمانة شرطية لحفظ الأمن ومكافحة الجرائم وملاحقة المجرمين، صحيفة الرؤيا، نشر بتاريخ 13 مايو 2021، https://alroya.om/p/132947

3. الموقع الإلكتروني الرسمي لمركز الدفاع الإلكتروني. https://cdc.gov.om/

سادسًا: القوانين والمعاهدات الدولية:

1. النظام الأساسي للدولة الصادر بالمرسوم السلطاني رقم (2021/6) بتاريخ 2021/1/12م، نشر في الجريدة الرسمية رقم (1374).

2. قانون الجزاء الصادر بالمرسوم السلطاني رقم (2018/7) بتاريخ 2018/1/14م، نشر في الجريدة الرسمية العدد رقم (1226).

3. قانون الإجراءات الجزائية الصادر بالمرسوم السلطاني رقم (99/97) بتاريخ 1999/12/15م، نشر في الجريدة الرسمية العدد رقم (661).

4. قانون الادعاء العام الصادر بالمرسوم السلطاني رقم (99/92) بتاريخ 1999/11/21م، نشر في الجريدة الرسمية العدد رقم (660).

5. قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2011/12) بتاريخ 2011/2/15م، نشر في الجريدة الرسمية العدد رقم (929).

6. قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم (2022/6) بتاريخ 2022/2/13م، نشر في الجريمة الرسمية العدد رقم (1429).

7. قانون تنظيم الاتصالات الصادر بالمرسوم السلطاني رقم (2020/30) بتاريخ 2002/3/17م، نشر في الجريدة الرسمية العدد رقم (715).

8. المرسوم السلطاني رقم (2020/64) بإنشاء مركز الدفاع الإلكتروني الصادر بتاريخ 2020/6/14م، نشر في الجريدة الرسمية العدد رقم (1345).

9. مجلس أوروبا، مجموعة المعاهدات الأوروبية رقم 185، الاتفاقية المتعلقة بالجريمة الإلكترونية، بودابست، 2001/11/23م.

10. المرسوم السلطاني رقم 34/ 99 بشأن التصديق على اتفاقية الرياض العربية للتعاون القضائي.

11. المرسوم السلطاني رقم 5/ 2015 بشأن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

سابعًا: المصادر باللغة الأجنبية

1. Ralph Clifford, Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime, Carolina Academic Press, USA, 2001.
2. Kenneth Rosenblatt, High-Technology Crime: Investigating Cases Involving Computers, KSK Publications, USA, 1995
3. Stephan Caidi, La prevue et la conservation de l'ecrit dans la societe d' information, Ph D Thesis, Universite de Monteral, 2002.
4. Ricordel, I., L'expertise en police scientifique, Dalloz, 2015.
5. Curtis, Joanna, and Gavin Oxburgh. "Understanding Cybercrime in 'Real World' Policing and Law Enforcement." The Police Journal Theory Practice and Principles, vol. 96, no. 4, December 2023, journals.sagepub.com.
6. Eoghan Casey, Digital Evidence and Computer Crime, Academic Press, London, 2000.
7. David O'Connor, Andrea Goldstein, E-commerce for Development: Prospects and Policy Issues, OECD Development Centre, 2000.

قائمة المحتويات