الجامعة العربية الأمريكية
كلية الدراسات العليا

الأدلة الرقمية ودورها في الإثبات الجزائي في ضوء المواثيق الدولية والتشريعات الفلسطينية

إعداد
معتز إدريس عبد الله حمودة

إشراف
د. عصام عابدين

تم تقديم هذه الرسالة استكمالا لمتطلبات درجة الماجستير في تخصص العلوم الجنائية

07/ 2024

إجازة الرسالة

الأدلة الرقمية ودورها في الإثبات الجزائي في ضوء المواثيق الدولية والتشريعات الفلسطينية

إعداد

معتز إدريس عبد الله حمودة

نوقشت هذه الرسالة بتاريخ 2024/06/08 وأجيزت.

أعضاء لجنة المناقشة:		التوقيع
1. د. عصام عابدين	مُشرفاً ورئيساً	
2. د. رائد أبو بدوية	ممتحناً داخلياً	
3. د. رائد عصفور	ممتحناً خارجياً	

الإقرار

أنا الموقع أدناه معتز إدريس عبد الله حمودة أفوض/ الجامعة العربية الأمريكية بتزويد نسخ من رسالتي للمكتبات أو المؤسسات أو الهيئات أو الأشخاص، عند طلبهم بحسب التعليمات النافذة في الجامعة.

وأقر بأنني قد ألتزمت بقوانين الجامعة العربية الأمريكية وأنظمتها وتعليماتها وقراراتها السارية المعمول بها والمتعلقة بإعداد أطروحات الدكتوراه عندما قمت شخصياً بإعداد رسالتي الموسومة ب الأدلة الرقمية ودورها في الإثبات الجزائي في ضوء المواثيق الدولية والتشريعات الفلسطينية". وذلك بما ينسجم مع الأمانة العلمية المتعارف عليها في كتابة الرسائل العلمية.

الاسم: معتز إدريس عبد الله حمودة

الرقم الجامعي: 202012181

التوقيع:

التاريخ: 2024/08/15م

الإهداء

إلى ثمرة جهدي إلى من تنحني له جبهتي خجلاً المعلم الأول "أبـي"

إلى من حملتني وهناً على وهن "أمـــي"

إلــى التي تبعث بِنورها من خَلف الظِلال ويضيءُ لي ظُلــمتي

إلى أهلي وكل الأصدقاء والزملاء

الباحــث

الشكر والتقدير

احمد الله حمداً يليق بجلال وجهه وعظيم سلطانه، ربنا رب العرش العظيم، ويسرني أن أقدم أرقى وأسمى عبارات الشكر والتقدير،إلى كل من أضاء بعلمه عقلي، وهدى بالجواب الصحيح حيرة أسئلتي، وأظهر بسماحته، تواضعه في العلم، ليمده إلي لأنتفع به وأفيد به غيري إلى كادر الجامعة العربية الأمريكية العريقة ممثلة بإدارتها وأساتذتها الأجلاء الأفاضل.

وأخص بجزيل الشكر مشرف رسالتي الفاضل **الدكتور عصام عابدين** من تتناثر كلماته منه لتغرس في عقلي وكان لي نعم المشرف والمرشد والموجه، له جزيل الشكر والامتنان والتقدير، كما يدعوني واجب العرفان إلى أن أتقدم بالشكر إلى جميع أعضاء لجنة المناقشة الأساتذة الأجلاء الأفاضل، الذي تفضلوا بالموافقة على مناقشة هذه الرسالة.

الباحث

ملخص الرسالة

تُعالج هذه الرسالة مجال الأدلة الرقمية ودورها في الإثبات الجزائي في ضوء المواثيق الدولية والتشريعات الفلسطينية. تكمن الإشكالية البحثية في أنه وعلى الرغم من التحول المُتسارع من المجتمع التقليدي إلى المجتمع الرقمي واتساع الجرائم الإلكترونية إلا أن المشرع الفلسطيني اكتفى باعتبار الأدلة الرقمية من أدلة الإثبات ولم يعالج الجوانب التنظيمية والإجرائية المرتبطة بالأدلة الرقمية في المجال الجزائي، وما يتصل بها في المجال المدني والتجاري، علاوة على تجاهل قواعد الاختصاص في الجرائم الإلكترونية العابرة للحدود، مما ينعكس سلباً على القناعة الوجدانية للقاضي، والعدالة الناجزة، والحقوق والحريات العامة، ويتعارض مع القانون الأساسي (الدستور) والاتفاقيات والمعايير الدولية.

اتبع الباحث المنهج الوصفي التحليلي، مع التوسع في مجال المواثيق الدولية كأدوات معيارية وقد شملت الاتفاقيات الأساسية لحقوق الإنسان التي انضمت إليها دولة فلسطين، ونظام المراقبة على حقوق الإنسان فيما يتصل بالأدلة الرقمية (الآليات التعاقدية وغير التعاقدية) والاتفاقيات الأوروبية وبخاصة اتفاقية بودابست (مجلس أوروبا) بشأن الجرائم الإلكترونية وتعديلاتها وشروحاتها، والمعايير الدولية بشأن المراقبة على الاتصالات الرقمية. وأجرى الباحث مقابلات شخصية هامة في الجانب التطبيقي شملت وحدة الجرائم الإلكترونية في الشرطة ونيابة الجرائم الإلكترونية وقضاة سابقين وأساتذة جامعات، ومؤسسات مجتمع مدني متخصصة، علاوة على المؤسسة الوطنية لحقوق الإنسان.

جرى تقسيم الرسالة إلى فصلين، ومبحثين ومطلبين لكل فصل، الفصل الأول تناول مفهوم الدليل الرقمي وخصائصه وإجراءاته، والفصل الثاني تناول قيمة الأدلة الرقمية في التشريعات والمواثيق الدولية وصولا إلى النتائج والتوصيات.

خلصت الرسالة للعديد من النتائج أبرزها: وجود تطور تشريعي نسبي ومحدود بشأن الأدلة الرقمية في المجال الجزائي (قرار بقانون الجرائم الإلكترونية وتعديلاته وقانون الإجراءات الجزائية وتعديلاته) على مستوى الاعتراف بالدليل الرقمي كدليل في الإثبات، رغم الإشكاليات التي يثيرها الاعتراف في الصياغة التشريعية، وقد امتدت أيضاً إلى المجال المدني والتجاري (قانون البينات وتعديلاته) مما يدلل على التطور المحدود الحاصل في المجال المدني والتجاري في الأدلة الرقمية. اقتصرت القرارات بقوانين على الاعتراف بالدليل الرقمي، وتجاهلت اجراءات التعامل معه في

المجال الجزائي،مقابل التركيز على تجريم حرية التعبير بعد اقتحام تخومها من خلال قرار بقانون الجرائم الالكترونية. ورغم أن الجرائم الالكترونية وما يتصل بها من أدلة رقمية عابرة للحدود إلا أن المشرع لم يعالج أيضاً مشكلة الاختصاص التي تعتبر من أبرز الإشكاليات التي تواجه مثل هذا النوع من الجرائم.القصور التشريعي في التعامل مع الأدلة الرقمية من شأنه أن يمس بالحقوق والحريات وضمانات المحاكمة العادلة المكفولة في القانون الأساسي والمعايير الدولية.القرارات بقوانين بذاتها، بما يشمل التي صدرت بشأن الأدلة الرقمية في غياب المجلس التشريعي، ساهمت في المساس بحرية التعبير واقتصرت على التجريم في غياب التنظيم الإجرائي.وهناك قصور في المعالجة المتكاملة للأدلة الرقمية.

خرجت الرسالة بالعديد من التوصيات أبرزها: ضرورة إلغاء كافة النصوص الواردة في القرار بقانون بشأن الجرائم الالكترونية التي تنال من حرية التعبير وبما ينسجم مع الحقوق والحريات الدستورية والمعايير الدولية.وإجراء تعديلات جوهرية على قرار بقانون الجرائم الإلكترونية بما يضمن تحري الرقابة القضائية في جميع الجوانب المتعلقة بالأدلة الرقمية وينسجم مع المعايير الدولية (المبادئ الدولية لتطبيق حقوق الإنسان فيما يتعلق بالاتصالات 2013). ومعالجة النقص التشريعي المتعلق بالجوانب الإجرائية في التعامل مع الأدلة الرقمية في مراحلها كافة، وعدم الاكتفاء باعتبار الأدلة الرقمية مقبولة في الإثبات الجنائي، ضماناً لجودة الدليل الرقمي، وبما يشمل الأدلة الرقمية في مجال الإثبات المدني والتجاري، للارتباط القائم بينهما.وتعزيز قدرات مؤسسات العدالة (أجهزة إنفاذ القانون، النيابة العامة، القضاء) عبر برامج تدريبية في مجال التعامل مع الأدلة الرقمية. والعمل على إدراج الأدلة الرقمية ودورها في الإثبات ضمن مساقات متخصصة في الجامعات، وإدراجها ضمن برامج المعهد القضائي،مواكبة للمُستجدات.ووقف العمل بالقرارات بقوانين، التي لعبت دوراً كبيراً في انتهاك الحقوق والحريات، واعترفت بالدليل الرقمي لغايات التجريم فقط وليس لغايات المأسسة والتنظيم.واستعادة الدور الأصيل للمجلس التشريعي في التشريع،واحترام الدستور، والفصل بين السلطات، والتحول الديمقراطي، واضطلاع"التشريعي" بمهامه الدستورية في تنظيم كافة جوانب الأدلة الرقمية.

فهرس المحتويات

إجازة الرسالة.....أ
الإقرار.....ب
الإهداء.....ج
الشكر والتقدير..... د
ملخص الرسالة.....ه
المقدمة..... ط
إشكالية البحث ..... ي
أسئلة البحث..... ك
أهمية البحث ..... ك
أهداف البحث .....ل
نطاق البحث .....ل
منهجية البحث ..... م
خطة الدراسة .....ن
الفصل الأول: مفهوم الدليل الرقمي وإجراءاته 1
المبحث الأول: ماهية الدليل الرقمي باعتباره وسيلة إثبات.....1
المطلب الأول: تعريف وسائل الإثبات الرقمي وأنواعه 1
الفرع الأول: تعريف وسائل الإثبات الرقمية.....2
الفرع الثاني: أنواع وتقسيمات الأدلة الإثبات الرقمية.....6
المطلب الثاني: خصائص وسائل الإثبات الرقمية وميزاتها 8
الفرع الأول: خصائص وسائل الإثبات الرقمية.....9
الفرع الثاني : ميزات وسائل الإثبات الرقمية.....13
المبحث الثاني: آليات ضبط الأدلة الرقمية وإجراءات الحصول عليها 15
المطلب الأول: مفهوم ضبط الأدلة الرقمية وإجراءات الحصول عليها وتحليلها.....15
الفرع الأول: وسائل ضبط وجمع الأدلة الرقمية.....15
الفرع الثاني: الإجراءات الخاصة لحيازة الأدلة الرقمية وتحليلها.....25
المطلب الثاني: آليات التعامل مع الأدلة الرقمية 33
الفرع الأول: موقف الفقه الدولي والتشريع الوطني في تفتيش وضبط الأدلة الرقمية.....33
الفرع الثاني: الإشكاليات المترتبة على تفتيش الدليل الرقمي وضبطه 39
الفصل الثاني: الأدلة الرقمية وضوابطها القانونية 45
المبحث الأول: القيمة القانونية للأدلة الرقمية 46
المطلب الأول: حجية الأدلة الرقمية أمام القاضي الجزائي ومدى مشروعيتها.....46

الفرع الأول: حجية الأدلة الرقمية أمام القاضي الجزائي.....46
الفرع الثاني: سلطة القاضي في الإثبات الجنائي 59
المطلب الثاني: القيود الواردة على حرية القاضي الجزائي في قبول الدليل الرقمي.....64
الفرع الأول: قيود متعلقة بطريقة الحصول على الدليل الرقمي.....64
الفرع الثاني: القيود الواردة بموجب نصوص قانونية خاصة.....69
المبحث الثاني: التشريعات الوطنية الخاصة بالأدلة الرقمية ومدى مواءمتها والمواثيق الدولية ..74
المطلب الأول: مواءمة التشريعات الوطنية الخاصة بالأدلة الرقمية مع المواثيق الدولية وأحكام الدستور.....74
الفرع الأول : مواءمة تطبيق التشريعات الرقمية في تقرير دولة فلسطين (العهد المدني والسياسي) 74
الفرع الثاني: الممارسات العملية للتشريعات الرقمية 77
المطلب الثاني: التشريعات المقارنة والمواثيق الدولية المتعلقة بالأدلة الرقمية ودورها في الإثبات الجنائي.....87
الفرع الأول: أهم التشريعات المقارنة ذات الصلة بالأدلة الرقمية.....87
الفرع الثاني: أهم المواثيق الدولية المتعلقة بالأدلة الرقمية 93
الخاتمة.....111
النتائج.....112
التوصيات 114
قائمة المصادر والمراجع 116
الملاحق 137
Abstract 143

المقدمة:

استخدام الحواسيب والشبكات الإلكترونية وتقنيات الذكاء الاصطناعي أنتج منافع متعددة في مجالات البحث العلمي وتوثيق المعلومات وتخزينها والحصول على المعلومات تيسيراً لأعمال القطاعين الخاص والعام، وما لبث الأمر أنْ تحولت هذه المنفعة إلى سيف ذي حدين؛ فقد أحدثت تغيرات جذرية ونوعية بمختلف مناحي الحياة، في نهاية القرن العشرين، من خلال استغلال هذه التقنيات المتطورة في ارتكاب العديد من الجرائم سواء على الصعيد الوطني أو الدولي محدثة آثاراً سلبية ومباشرة وخطيرة.

وقد لوحظ ازدياد كبير في استعمال هذه التقنيات الرقمية والتي زادت من ارتفاع معدلات المخاطر المرتبطة بسوء استخدامها، حتى ظهر الحديث عن مخاطر الجرائم الإلكترونية، أو الجرائم الرقمية، وهو نوع جديد من الجرائم التي شكلت مأزقاً لكيفية التعامل معها وللسياسة التشريعية الجنائية في العصر الحديث، وذلك للصعوبات التي قد تتعرض لها أثناء جمع أدلة وقوعها وملاحقة مرتكبيها، وكذلك بالنظر إلى خصوصية أركانها وحداثة أساليب ارتكاب ها، وطبيعة البيئة التي ترتكب من خلالها، ونوعية مرتكبيها، والوسائل التي تستدعي معرفة كاملة من قبل خبراء مؤهلين ليتسنى كشفها.

كما تستمد هذه الجرائم طبيعتها الخاصة من قدرة الشبكة المعلوماتية على نقل وتبادل المعلومات العامة والخاصة في آن واحد، وهذا كله جاء نتيجة لتطور العالم الافتراضي الذي أصبح جزءاً من حياة الإنسان والذي رافقه وجود الحواسيب والإنترنت والتطور التكنولوجي الهائل، والتعامل مع هذه التقنيات المتطورة سواء في القطاعين العام والخاص. ففي وقتنا الحاضر أصبحت الدول تعتمد على حوسبة وأتمتة أعمالها ونشاطاتها واتصالاتها وتنظيم إدارتها والإشراف على حسن سير أعمالها من خلال نظام إلكتروني، وأصبحت هذه التكنولوجيا المتمثلة بالحواسيب والشبكة العالمية جزءاً من الحياة اليومية للأفراد ونشاطه الاجتماعي وتعامله، بحيث أنه لا يمكن الاستغناء عنها لتسهيل تسيير الحياة بشكل عام.

ونظراً لتميز الأدلة الرقمية، بطبيعة خاصة، أصبح هناك ضرورة لوجود تشريع خاص ينظمها، لاتصالها ببيانات وكلمات ورموز وأرقام سواء من حيث تجميعها وتخزينها وتجهيزها واسترجاعها وتصحيحها وتعديلها ومحوها وطباعتها ونسخها، فهي تتم من خلال المعالجة الآلية للبيانات بهدف الحصول على المعلومات المرجوة، ومن خلال الطبيعة الخاصة بالأدلة الرقمية من حيث طريقة التحقيق وتحليلها وربطها والحصول عليها ومتابعتها من خبراء تكنولوجيا المعلومات، فهي تمتاز بطبيعة مزدوجة ما بين الحصول على الدليل وتحليله واتصاله بالنص القانوني، فإثبات الأدلة الرقمية

بحاجة إلى إجراءات خاصة لمتابعتها بشكل يتواءم مع التقنيات المستخدمة والمستحدثة ليتوافق مع الخصوصية التي تتميز بها، ومن الصعب، إنْ لم يكن من المستحيل، معالجتها بطرق الإثبات التقليدية، الأمر الذي يُبرز أهمية البحث في مجال الأدلة الرقمية ومواكبة مُستجداتها من مختلف جوانبها في ميزان الأدلة وبما ينسجم مع الاتفاقيات والمعايير الدولية ذات الصلة والممارسات الفضلى ويحقق بذات الوقت العدالة الناجزة.

إشكالية البحث

تتمثل إشكالية البحث في عدم النص صراحةً على وجوب اعتبار الأدلة الرقمية دليلاً في إثبات الجرائم الإلكترونية، وفي مدى جواز إثبات الجريمة الإلكترونية دون دليل رقمي وعلاقة ذلك بقاعدة " الشك يفسر لمصلحة المتهم "، حيث نصت المادة 37 من القرار بقانون رقم 10 لسنة 2018، على اعتبار الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية **من أدلة الإثبات .**

فعلى الرغم من تأكيد قانون الجرائم الإلكترونية 2018 على الاعتراف بالأدلة الرقمية في الإثبات الجزائي إلا أنه لم ينظم إجراءات التعامل معها، واقتحم تخوم حرية التعبير، ما أدى بالنتيجة إلى جعل الاعتراف يخدم غايات التجريم على حرية التعبير.

وعلى الرغم من تأكيد التعديلات التي جرت على قانون الإجراءات الجزائية في العام 2022 على الأدلة الرقمية إلا أنها لم تنظم أيضاً كيفية التعامل معها وجعلت استخدامها وجوبياً في جرائم العرض وشهادة الأطفال تحت سن (15) سنة وجوازياً للنيابة والقضاء في جميع الجرائم الأخرى، ودون تحديد أية أسس ومعايير وضوابط لهذه السلطة الجوازية، ما أدى بالنتيجة إلى حالة من الفوضى التشريعية في التعامل مع الأدلة الرقمية.

وكذلك فعلى الرغم من تأكيد قانون البينات في التعديلات التي جرت في العام 2022 على الأدلة الرقمية في المجال المدني، وفي الدفاتر التجارية، إلا أنه لم يعالج أيضاً الجوانب الإجرائية في التعامل مع الأدلة الرقمية. وهي ذات الإشكاليات التي تعاني منها التشريعات الجزائية.

بالنتيجة نحن أمام قصور تشريعي في بتنظيم إجراءات البحث والتحري والتفتيش وضبط الدليل الرقمي والحفاظ عليه، ليكون دليلا مقبولاً يعتد بحجيته أمام القاضي الجزائي. أدى بالنتيجة إلى استغلال الاعتراف المجرد بالدليل الرقمي من أجل النيل من حرية التعبير المُجرمة في الجرائم الإلكترونية!

أسئلة البحث

جاءت هذه الدراسة للإجابة عن تساؤل رئيسي يكمن في «المغزى» من الاقتصار على الاعتراف بالدليل الرقمي في الإثبات دون تنظيم كيفية التعامل معه؟ وكيفية التعامل مع الأدلة الرقمية في ظل هشاشة المعرفة والإلمام بمفهوم الدليل الرقمي وأنواعه وخصائصه وإشكالاته وأهميته في إثبات الجرائم الالكترونية الرقمية، والذي يقودنا إلى أسئلة فرعية أهمها :

- هل يوجد تنظيم قانوني خاص يبين ماهية الأدلة الرقمية وتنظيمها وكيفية التعامل معها في فلسطين؟
- هل هناك تنظيم قانوني متكامل يعالج مختلف الجوانب الفنية والإجرائية في التعامل مع الأدلة الرقمية ؟
- مدى القدرة المعرفية والفنية لدى أجهزة العدالة (ضابطة عدلية ، نيابة عامة ، قضاة)، ومدى توفر التقنية اللازمة للتعامل مع الأدلة الرقمية؟
- مدى مواكبة ومواءمة التشريعات الخاصة بالأدلة الرقمية مع المواثيق الدولية ؟
- مدى حجية الأدلة الرقمية أمام القاضي الجزائي ومقبولتيها وابرز القيود الواردة عليها ؟
- هل يمكن الفصل بين مفهوم الأدلة الرقمية في الإثبات الجزائي والأدلة الرقمية في الإثبات في القانون المدني ؟.

أهمية البحث

تكمن أهمية هذا البحث في فهم التحول المُتسارع من المجتمع التقليدي إلى المجتمع الرقمي الذي يعتمد بشكل أساسي على قوة وسرعة المعرفة المعلوماتية الرقمية، ودور الأدلة الرقية وارتباطها بمنظومة الحقوق والحريات بأكملها سواء في المجال الجزائي أو المدني.

وبالتناوب معرفة المخاطر والآثار التي قد تترتب على الاعتماد المتزايد على هذا التحول الرقمي، وكيفية التعامل معها بشكل يضمن حماية الحقوق والحريات والسلامة الرقمية والأمن الرقمي وفحص أوجه الخلل ومعالجته بما يكفل الحفاظ على سلامة وقوة الأدلة الرقمية.

وبالنتيجة، إنشاء نظام متكامل للأدلة الرقمية في المجال الجنائي وما يتصل به في المجال المدني قائم على حماية الحقوق والحريات الدستورية والمعايير الدولية لحقوق الإنسان.

أهداف البحث

يهدف هذا البحث إلى ما يلي :

- تقديم رؤية قانونية متكاملة حول أدلة الإثبات الرقمي في الجرائم الإلكترونية من حيث مفهومها. أنواعها، خصائصها، مشروعيتها، ووفق الاتفاقيات والمعايير الدولية والممارسات الفضلى للدول.
- التعمق في مفهوم الدليل الرقمي وكيفية التعامل معه في العصر الرقمي.
- بيان الإجراءات القانونية الخاصة بالأدلة الرقمية وأهم مبادئها وآليات تنظيمها.
- معرفة طرق جمع واستخلاص أدلة الإثبات الرقمية في ضوء القانون الوطني والمعايير الدولية.
- بيان المشكلات وأهم الثغرات التي لم تعالجها التشريعات الوطنية في مجال الإثبات الرقمي ومعالجتها.
- إيضاح مدى حجية الأدلة الرقمية أمام القضاء الفلسطيني وأبرز التحديات وسُبل التعامل معها.

نطاق البحث

تكمن الحدود الزمانية لنطاق البحث في مناقشة قانون الجرائم الإلكترونية رقم 10 لسنة 2018 وتعديلاته وقانون الإجراءات الجزائية رقم (3) لسنة 2001 وتعديلاته، والقرار بقانون بشأن مكافحة غسل الأموال وتمويل الإرهاب رقم (39) لسنة 2022، وما يتصل بها في مجال الأدلة الرقمية المدنية في ضوء قانون البينات رقم (4) لسنة 2001، وما جرى عليه من تعديلات من خلال القرار بقانون رقم (9) لسنة 2022 بشأن تعديل قانون البينات في المواد المدنية والتجارية رقم (4) لسنة 2001، وقانون أصول المحاكمات المدنية والتجارية رقم (2) لسنة (2001)، والتشريعات العربية والغربية ذات الصلة، أهم والاتفاقيات الدولية التي انضمت إليها دولة فلسطين المتعلقة بالمجال الرقمي والتعامل مع الأدلة الرقمية، والمعايير الدولية ذات الصلة.

وأمّا بخصوص الحدود المكانية فتتمثل في استعراض ومناقشة وتحليل التشريعات السارية في فلسطين، والتشريعات العربية بما ينسجم مع الاتفاقيات والمعايير الدولية ومتطلبات انضمام فلسطين للاتفاقيات الدولية واستحقاقاتها على المستوى التشريعي وفي الممارسات.

منهجية البحث

قمت في هذه الدراسة بإتباع المنهج الوصفي التحليلي لغايات تحليل أهم النصوص القانونية الوطنية الناظمة للجرائم الإلكترونية، والتشريعات ذات الصلة، وابرز التعديلات التي جرت عليها وتأثيرها على الأدلة الرقمية ودورها في الإثبات الجزائي، وكذلك أهم الاتفاقيات الدولية ذات الصلة بالأدلة الرقمية، كما قمنا بإجراء العديد من المقابلات مع مؤسسات العدالة متمثلة بالقضاة والنيابة العامة والمحامين وأساتذة جامعيين، لتعزيز الجانب التطبيقي والتحليلي في الرسالة، علاوة على تناول معايير الأمم المتحدة في هذا المجال المتخصص بآلياتها التعاقدية وغير التعاقدية، ومقارنتها ببعضها البعض، والتركيز على أهم المعوقات التي قد تواجه ذوي الاختصاص أثناء الكشف عن الأدلة الرقمية واستخلاصها واستخراجها ونقلها والتعامل معها، والبناء على الايجابيات للخروج بدراسة بحثية أصيلة تساهم في منع التلاعب بالدليل الرقمي والحفاظ عليه من اجل تقديمه كدليل إثبات أثناء وقوع الجريمة الإلكترونية، ليتسنى محاسبة الجناة بما يتفق وصحيح القانون، وكذلك مساعدة منظومة العدالة في معرفة كيفية التعامل مع الدليل الرقمي عند وقوع أية جريمة الكترونية، علاوة على نشر الوعي والمعرفة بأهمية الأدلة الرقمية وتطورها ودورها في مجال الإثبات الجزائي. إنها منهجية تُركز على التحليل والمقابلات العملية والمعايير الدولية في المعالجة.

خطة الدراسة:

سنقوم بتقسيم هذه الدراسة إلى فصلين كل فصل يتكون من مبحثين وذلك على النحو التالي:

الفصل الأول: مفهوم الدليل الرقمي وخصائصه وإجراءاته

المبحث الأول: ماهية الدليل الرقمي كوسيلة إثبات

المطلب الأول: تعريف وسائل الإثبات الرقمي وأنواعها

المطلب الثاني: خصائص وسائل الإثبات وميزاتها

المبحث الثاني: آليات ضبط الأدلة الرقمية في العصر الرقمي

المطلب الأول: ضبط الأدلة الرقمية وإجراءاتها وتحليلها

المطلب الثاني: آليات التعامل مع الأدلة الرقمية

الفصل الثاني: قيمة الأدلة الرقمية في التشريعات والمواثيق الدولية

المبحث الأول: القيمة القانونية للأدلة الرقمية

المطلب الأول: حجية الأدلة الرقمية أمام القاضي الجزائي ومدى مشروعيتها

المطلب الثاني: القيود الواردة على حرية القاضي الجزائي في قبول الدليل الرقمي

المبحث الثاني: التشريعات الوطنية الخاصة بالأدلة الرقمية ومدى مواءمتها والمواثيق الدولية

المطلب الأول: مواءمة التشريعات الوطنية الخاصة بالأدلة الرقمية مع المواثيق الدولية وأحكام الدستور

المطلب الثاني: أهم التشريعات الدولية والمواثيق الدولية المتعلقة بالأدلة الرقمية ودورها في الإثبات الجزائي

الفصل الأول

مفهوم الدليل الرقمي وإجراءاته

يتحتم على القائمين بإنفاذ القانون الإلمام الدائم بالتقنية العلمية المتطورة والحرص الدائم على تطوير معارفهم ومهاراتهم في هذا المجال سريع التطور والتعقيد، وتطبيقاً لذلك جاءت وسائل الإثبات الرقمية لتكون نتاجاً للتطور الحاصل في جميع المجالات العلمية والتقنية، إذ يصح القول أنها انعكاس لما بلغه العلمُ واكتسبته الخبرة، ولها من الممارسات القضائية ما يشهد لها بالدور المهم والفعال في عملية الإثبات .

وفي هذا الشأن سنقسم هذا إلى مبحثين، الأول نناقش فيه مفهوم الدليل الرقمي كوسيلة إثبات، والثاني نخصصه لدراسة الإجراءات الخاصة بأدلة الإثبات الرقمية.

المبحث الأول

ماهية الدليل الرقمي باعتباره وسيلة إثبات

إن تعدد مفاهيم الدليل الرقمي والتباسه بمفهوم الدليل الإلكتروني، يعد من الأمور التي لا بد من الوقوف عندها ومناقشتها.

وانطلاقاً مما تقدم سنقوم بتقسيم هذا المبحث إلى مطلبين، نتناول في المطلب الأول تعريف وسائل الإثبات الرقمي وأنواعه، ونخصص المطلب الثاني للحديث في خصائص وسائل الإثبات الرقمية.

المطلب الأول

تعريف وسائل الإثبات الرقمي وأنواعه

سنتناول في هذا المطلب التعريفات العلمية واللغوية وكذلك التعريفات الاصطلاحية والفقهية الشرعية للدليل كدليل إثبات والأدلة الرقمية، وكذلك وسنقوم بتبيان موقعها.

الفرع الأول

تعريف وسائل الإثبات الرقمية

- **(التعريف العلمي).**

خلال المراجعة يتضح أن المصطلح مترجم من كلمة (Digital) باللغة الانجليزية، وقد عرفها قاموس كامبردج أنها: **"تسجيل أو تخزين المعلومات كسلسلة من الأرقام (0،1) من خلال إظهار أو إخفاء الإشارة"**[1]، ويسمى هذان الرقمان (0،1) بالأرقام الثنائية أو بالنظام الثنائي، وهي الصيغة التي تسجل فيها البيانات كافة من حروف ورموز وأشكال وغيرها داخل الحاسوب، إذ يطلق على الواحد أو الصفر بالـ (بايت،Bit)، وبعبارة أخرى تحويل المعلومات إلى أرقام لكي يتم تخزينها في جهاز الحاسوب، مثال على ذلك، الرقم 65 يمثل الحرف (A)، ويمثل الرقم (66) الحرف (B)، فيرمز للرقم 65 بهذا الشكل (01000001) والرقم 66 يرمز له (01000010)، ويمثل أمر المسافة أو الفراغ (Space) بين كلمتين الرقم 32 ويرمز له (00100000)، وهكذا تتحول الأرقام إلى معلومات يمكن تخزينها بجهاز الحاسوب أو ما شابه ذلك، من خلال النظام الثنائي الذي يعد كشِفرة تترجم جميع المعلومات[2] وتخزنها[3].

- **(التعريف اللغوي).**

الدليل في اللغة هو المرشد وما يستدل به وجمعه أدلة، كما يقصد به كذلك تأكيد الحق بالبينة، والبينة هي الدليل والحجة أو البرهان.[4]

وجاء في معنى "الرقمي" فهي اسم منسوب للدليل واصلها "رقم" وهي علامات الأعداد المعروفة، وينصب معناها أيضا إلى كلمة عدد، وجمعها أعداد.[5]

- **(التعريف الفقهي الشرعي).**

الدليل في اصطلاح فقهاء الشريعة هو: ما يلزم من العلم به العلم بشيء أخر، فإذا قدم المدعي حجته للقاضي واقتنع الأخير بتلك الحجة لزم عليه الحكم للمدعي فيما ادعاه،[6] وتستعمل كلمة الدليل في الشريعة بمعنى البينة أي الحجة أو البرهان، فالبينة اسم لكل ما يبين الحق.

---

[1]. قاموس كامبردج، (2003)، معنى الدليل الرقمي، (تاريخ الدخول : 2023/09/12)، انظر الموقع الالكتروني:
-.https://dictionary.cambridge.org/dictionary/english/digital

[2]. المناعسة، أسامة والزعبي، جلال (2014)، جرائم تقنية نظم المعلومات، دراسة مقارنة، ط1، دار الثقافة للنشر والتوزيع، عمان، ص 290.

[3]. جيتس، بيل (1998)، المعلوماتية بعد الإنترنت – طريق المستقبل، ترجمة عبد السلام رضوان، مجلة عالم المعرفة، العدد 231، الكويت، ص40-46.

[4]. صليبا جميل، المعجم الفلسفي المصطلحات القانونية، الجزء الأول، دار الكتاب اللبناني، بيروت ، الطبعة الأولى، 1982، ص 564.

[5]. طاهري عبد المطلب، (2014 – 2015)، الإثبات الجنائي بالأدلة الرقمية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة المسيلة، ص 2.

[6]. الجوزية، ابن القيم، أعلام الموقعين عند رب العالمين، القاهرة، الطبعة الأولى، 1955، ص 450.

ومعنى الدليل كما جاء في قوله تعالى: **﴿أَلَمْ تَرَ إِلَىٰ رَبِّكَ كَيْفَ مَدَّ الظِّلَّ وَلَوْ شَاءَ لَجَعَلَهُ سَاكِنًا ثُمَّ جَعَلْنَا الشَّمْسَ عَلَيْهِ دَلِيلًا﴾**[1].

وهناك رأيان في الفقه الإسلامي في معنى الدليل أو البينة.

- الرأي الأول هو رأي جمهور الفقهاء الذي يقوم على ضرورة حصر الأدلة أو البينة والتقيد بها حسبما جاءت قرينة كل جرم بما لا يخرج عن : الإقرار، اليمين، الشهادة، علم القاضي، النكول، القرائن والقسامة.
- الرأي الثاني فهو رأي ابن تيمية وابن القيم الجوزية اللذين أطلقا للخصوم حرية تقديم الأدلة التي يرونها، كما أطلقا للقاضي حرية اعتماد ما يراه مفيداً للدعوى ومثبتاً للواقعة.[2]

(التعريف اصطلاحاً).

الدليل اصطلاحاً هو ما يلزم من العلم به علم شيء أخر، وغايته أن يتوصل العقل إلى التصديق اليقيني فيما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة.[3]

أما الدليل في الاصطلاح القانوني فهو الحجة أو البرهان وما يستدل به على صحة الواقعة، ويعرف بعض فقهاء القانون الدليل بأنه "الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها، والمقصود بالحقيقة في هذا السياق هو كل ما يتعلق بالوقائع المعروضة على القاضي لإعمال حكم القانون عليها.[4]

- **إذن يمكن القول بأن معظم التعريفات الاصطلاحية تدور حول معرفة الحقيقة من خلال المنطق العقلي والقانوني السليم، فالدليل هو وسيلة القاضي للوصول إلى الحقيقة، سواء ارتكاب الشخص للجريمة أو عدم ارتكاب ه لها.**

أما الأدلة الرقمية فتعد من الناحية النظرية كأي دليل أخر، فهي عبارة عن معلومات تجمع لإيجاد العلاقة السببية بين الوقائع والأشخاص لإثبات المسؤولية القانونية[5]. وقد عرفها قانون الشرطة والأدلة الجنائية في المملكة المتحدة بأنها **"جميع المعلومات الموجودة على جهاز الحاسوب"**[6].

---

[1]. القران الكريم، الآية 45 من سورة الفرقان.

[2]. احمد، أبو القاسم احمد، (1994)، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، أكاديمية نايف للعلوم العربية والأمنية، الرياض، ص 183.

[3]. د. البشرى، محمد الأمين، (2002)، الأدلة الجنائية الرقمية، المجلة العربية للدراسات الأمنية والتدريب، الرياض، المجلد 17، العدد 33، ص 104.

[4]. د. سرور، احمد فتحي، الوسيط في قانون الإجراءات الجنائية، القاهرة، دار النهضة العربية، الطبعة الثانية، 1981، ص 418.

[5]Goodison, Sean E. and Others (2015), Digital Evidence and the U.S. Criminal Justice System, RAND Corporation, US, P.2.

[6]Gercke, Marco (2012), Understanding cybercrime: Phenomena, challenges and legal response, ITU publication, Switzerland – Geneva, P.227.

ونلاحظ أن هذا التعريف، قد حصر الأدلة الرقمية في جهاز الحاسوب، في حين عرفتها المجموعة العلمية للعمل بالأدلة الرقمية (SWGDEScientific Working Group Digital Evidence) المكونة من دائرة مختبرات الجريمة الفيدرالية في واشنطن في عام 1998 على أنها: **"أي معلومات ذات قيمة إثباتيه يتم تخزينها في شكل ثنائي - وفي وقت لاحق تغير المصطلح من "ثنائي" إلى "رقمي"-. وتشمل هذه الأدلة، أدلة أجهزة الحاسوب، الفيديو الرقمي، والصوت الرقمي، وأجهزة الفاكس الرقمية، والهواتف المحمولة، والمواقع الإلكترونية وغيرها"**[1]، ونلاحظ أن هذا التعريف جاء أوسع من سابقه.

وهناك من يعرفها بأنها **"معلومات وبيانات ذات قيمة للتحقيق، يتم تخزينها على جهاز إلكتروني، أو استلامها أو إرسالها بواسطة جهاز إلكتروني، يتم الحصول عليها من خلال الحجز على الأجهزة الإلكترونية وتأمين بياناتها للفحص"**[2]. وقد عرفها آخرون بأنها **"البيانات الرقمية التي يمكن أن تثبت ارتكاب جريمة ما، وتعزز الصلة بين الجريمة وضحاياها، أو بين الجريمة ومرتكبها، ومن بين ألأمثلة على هذه الأدلة هي البيانات الموجودة في ذاكرة الحاسوب أو القرص الصلب أو الهاتف المحمول"**[3].

وفي الصدد نفسه قد تطرح تساؤلات منها: لما كان هناك مسميات كالأدلة الإلكترونية أو أدلة الحاسوب، فهل يقصد بهذه الأدلة المعنى ذاته المتجسد بالأدلة الرقمية؟ وهل يدخل الدليل الناتج عن المواقع الإلكترونية في إطار الأدلة الإلكترونية أم الرقمية؟

للإجابة يمكن القول إن دليل الحاسوب يعرف أحياناً بالدليل الإلكتروني، والأدلة الإلكترونية تشمل الأدلة التي يتم إنشاؤها وإنتاجها بواسطة الحاسوب، ومخرجاته، والأدلة المستندة إليه، والأدلة المرتبطة به، وجميع البيانات والمستندات الإلكترونية، وبشكل عام يمكن أن تشمل الأدلة الإلكترونية أي بيانات يتم إنشاؤها أو تخزينها في شكل رقمي باستعمال جهاز الحاسوب[4]. وفضلاً عما سبق تعرف الأدلة الرقمية بأنها: **"عبارة عن معلومات مرسلة أو مخزنة كبيانات رقمية يمكن أن يستعملها أحد أطراف الدعوى، وقد تكون هذه الأدلة على شكل صور فوتوغرافية أو صور الأقمار**

[1]Whitcomb, Carrie Morgan (2002), An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vo1.1, no pages number.
[2]Dutelle, Airc W (2017), An Introduction to crime scene Investigation, thired Edition, Jones & Bartleff learning, USA, P.374.
[3]Carrier, Brian and Spafford Eugene H. (2003), Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence, Vo1.2, P.6.
[4]Law Reform Commission (2009), Documentary and Electronic Evidence, First Published, Dublin, P.1.

الاصطناعية أو فيديو أو تسجيل صوتي أو بريد إلكتروني، أو تكون على شكل موقع إلكتروني أو أحد مواقع التواصل الاجتماعي مثل (Facebook أو Twitter)"[1].

وفي هذا السياق يصح القول أن الأدلة الرقمية هي أوسع نطاقاً من الأدلة الإلكترونية، إذ أنها تشتمل فضلاً عن الأخيرة على ما ذكر في تعريف الأدلة الرقمية المذكورة آنفاً.

ويتضح مما تقدم، أنه لم يكن هناك اتفاق على تعريف موحد سواء كان ما تعلق بالأدلة الإلكترونية أم بالأدلة الرقمية، وخصوصاً بعد المحاولة التي جرت في المؤتمر الذي عقد في مدريد في 14 كانون الأول 2006 من قبل الجمعية الأوروبية لخبراء الطاقة (Associated European Energy Consultant–AEEC)، بشأن مشروع قبول الأدلة الإلكترونية في إجراءات المحاكم، إذ لم يستطع هذا المشروع التوصل إلى تعريف موحد للأدلة الإلكترونية أو الرقمية، وبالرغم من ذلك لا يعد هذا التعريف ضرورياً في الإجراءات القانونية، لأن معظم السلطات القضائية في أغلب الدول تتعامل مع الأدلة الإلكترونية أو الرقمية كشكل من أشكال المستند، ويقصد بهذا الأخير: **"أي شيء يسجل بأي شكل كان، ومُسْتَوفٍ لشروط المقبولية"**[2].

وفي سياق متصل فقد عرفت المحكمة الجنائية الدولية الخاصة لرواندا (المستند) على نطاق واسع في قضية المدعي العام ضد ألفرد موسيما (Alfred Musema) إذ قالت: **"يقصد بالمستند أي شيء يتم تسجيل المعلومات فيه، من أي وصف كان"**. وهذا التعريف واسع بما يكفي ليشمل فضلاً عن الوثائق الخطية، الخرائط والرسومات والخطط والرسوم البيانية والسجلات الحاسوبية والمواقع الإلكترونية والسجلات الكهرومغناطيسية والسجلات الرقمية وقواعد البيانات والمسارات الصوتية والأشرطة الصوتية وأشرطة الفيديو والشرائح والصور الفوتوغرافية وصور الأقمار الاصطناعية[3].

وتبعاً لكل تلك التعريفات يمكن القول بأن الوسائل الرقمية هي أدلة ذات طبيعة خاصة وتقنية خاصة لأنها تعيش وتتكون في بيئة مرتبطة بالحاسوب وشبكات الإنترنت المتصلة بها، وهي أدلة متنوعة تشمل كافة أشكال وأنواع البيانات الإلكترونية الممكن تداولها الكترونياً من نصوص أو صور أو سمعيات أو بصريات لو مرئيات، كما أنها أدلة متطورة يصعب إن لم يكن من المستحيل حصرها لان العالم الإلكتروني في تطور مستمر، وبالتالي تشهد بين كل فترة وأخرى ظهور أشكال جديدة من الوسائل الرقمية التي يمكن ان يعتد بها كأدلة إثبات رقمية[4].

---

[1]Ashouri, Aida and Others (2013), An Overview of the Use of digital Evidence in International Criminal Courts, Working Paper, Salzburg Workshop on Cyber Investigation, P.1.

[2]Mason, Stephan (2008), International Electronic Evidence, British Institute of International and Comparative law, London, P.xxxiv.

[3]Prosecutor v. Alfred Musema (2000), ICTR, Trial Chamber I, Case No. ICTR-96-13-T, 27,parper 53, P.24.

[4]. الحراق، اسيا، الإثبات بالوسائل الإلكترونية، 2017، ص 8.

ويعرف "كيسي" الأدلة الجنائية الرقمية بأنها تشمل جميع البيانات الرقمية التي يمكن ان تثبت ان هناك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني أو توجد علاقة بين الجريمة والمتضرر منها، والبيانات الرقمية هي مجموعة من الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت أو الصورة.[1]

ونستنتج مما تقدم، أن وسائل الإثبات الرقمية، ما هي إلا امتداد واستمرار للأدلة الخطية أو الكتابية لكن بوجهٍ متطور، لذا من المفترض أن تستجيب المحاكم الوطنية بشكل جيد ومستمر لما يطرأ من تطورات في جميع المجالات، من أجل توضيح ذلك لأغراض العدالة.

الفرع الثاني

أنواع وتقسيمات الأدلة الإثبات الرقمية

استناداً إلى التعريفات التي قمنا بالتطرق إليها يتضح بان الأدلة الرقمية هي إحدى أنواع الأدلة الجنائية والتي تتشارك معها في ذات الخصائص والشروط والاستخدامات، إلا أنها تتميز بخصائص استثنائية كونها أدلة مستحدثة ومتطورة باستمرار تجعل منها نوع خاص متميزا عن باقي أنواع الأدلة الجنائية التقليدية، ولمعرفة ما يميزها عن الأدلة الجنائية التقليدية لا بد من ذكر أنواع الأدلة بصفة عامة.

تنقسم الأدلة بصفة عامة إلى أربعة أنواع هي :

1. **الدليل القانوني،** ويقصد به الأدلة التي حددها المشرع وعن حالات استخدامها ومدى حجية كل منها.
2. **الدليل الفني،** ويقصد به الذي ينبعث من رأي الخبير الفني حول تقدير أو تقييم دليل مادي أو قولي وفق معايير وسائل علمية معتمدة.
3. **الأدلة القولية،** وهي الأدلة التي تنبعث ممن أدركوا معلومات مفيدة للإثبات بإحدى حواسهم كالاعتراف وأقوال الشهود.
4. **الأدلة المادية،** وهي الدليل الناتج من عناصر مادية ناطقة بنفسها، وتؤثر في اقتناع القاضي بطريق مباشر.[2]

---

[1] . Eoghan Casey, Digital Evidence and Computer Crime, London: Aca- demic Press , 2000, P.260.

[2]. البشرى، محمد الأمين، مرجع سابق، ص 110.

- **والسؤال هنا** ما هو موقع الأدلة الرقمية بين أنواع الأدلة الجنائية سالفة الذكر؟ وهل تعتبر مادية كونها قد تكون أحيانا ملموسة على شكل ديسك أو فلاشه مستندة على نظريات علمية؟ أم هي أدلة فنية كونها تدعم برأي خبير فني وفق معايير علمية معتمدة؟

يرى جانب من الفقه أن الأدلة الجنائية الرقمية ما هي إلا مرحلة متقدمة من الأدلة المادية الملموسة التي يمكن ادراكها بإحدى الحواس الطبيعية للإنسان والتي تقودنا إلى الاستعانة بجميع وما يبتكره العلم من أجهزة مخبريه ووسائل التقنية العالية ومنها الحاسوب محور الأدلة الرقمية، فالأدلة الجنائية الرقمية في منظور أنصار هذا الاتجاه لا تختلف عن آثار الأسلحة والبصمات أو البصمة الوراثية (DNA).[1]

ولكن الباحث يرى غير ذلك، كون أن الأدلة الرقمية لها خصائص علمية تتميز بها عن الأدلة الجنائية أنفة الذكر، وينعى ذلك كونها تتكون من موجات مغناطيسية وبيانات غير ملموسة، ولا تدركها الحواس البشرية، إضافة إلى أنها قد تكون في بعض الأحيان خيالية في شكلها وحجمها ومكان وجودها غير المعروف ابتداءً، أي أنها اقل مادية من الأدلة المادية التقليدية، كما ويمكن للخبراء استخراج نسخ طبق الأصل عن النسخ الأصلية والتي لها ذات الحجية القانونية أمام القاضي الجزائي، وهو الشيء الذي لا يمكن تصوره في الأدلة الجنائية التقليدية، وكذلك يمكن من خلال الخبراء معرفة ما إذا تم تعديلها أو تزويرها أو حذف بعض بياناتها أو تحريفها وذلك بمضاهاتها مع الأدلة الرقمية الأصلية بما لا يدع مجالا للشك.

ولا بد لنا من ذكر مدى صعوبة إتلاف الأدلة الرقمية أو القضاء عليها بشكل نهائي، بحيث يمكن استرجاعها بعد حذفها من خلال تطبيقات مختصة لمثل هذه الحالات، علاوة على إمكانية وجودها في مسرح جريمة تقليدي ومسرح أو مكان افتراضي عبر الفضاء الإلكتروني والتي يمكن لها التحرك بسرعة فائقة عبرها.

أي أنه لا يمكن إدراك الدليل الرقمي بالحواس، فهو مجرد بيانات أو معلومات ذات هيئة الكترونية غير ملموسة، وهذا على عكس الأدلة التقليدية التي إدراكها بالحواس كما هو الحال بالنسبة للمحررات المزورة والنقود والطوابع المزيفة والمخدرات والأسلحة المضبوطة والشعر والدماء.[2]

[1] . Eoghan Casey, Digital Evidence Op. Cit, P.5.

[2]. لميس، بوناب، الأدلة الجنائية وحجيتها أمام القضاء الجنائي، رسالة ماجستير، 2021، ص 11.

والسبب في ذلك يرجع إلى البيئة التي يمكن أن يستخلص منها الدليل فبينما يستخلص الدليل التقليدي من البيئة المادية المحسوسة، يستخلص الدليل الرقمي من البيئة الافتراضية أو غير المحسوسة.[1]

وقد قضت المحاكم بإمكانية اعتماد مثل تلك الأدلة غير الملموسة لأنها تتميز عن غيرها من أنواع الأدلة المادية الأخرى بما يلي:

1. يمكن استخراج نسخ منها مماثلة ومطابقة للأصل ولها ذات الحجية.
2. يمكن بالأساليب العلمية الملائمة تحديد وتأكيد ما إذا كانت الأدلة الرقمية قد تعرضت للتعديل أو التحريف.
3. من الصعب إتلاف الأدلة الرقمية، وفي حالة محوها أو إتلافها يمكن استرجاعها من ذاكرة الحاسوب.
4. إذا المتهمون إتلاف الأدلة الرقمية يمكن الاحتفاظ بنسخ منها في أماكن آمنة، علماً بأن للنسخ قيمة الأصل.[2]

المطلب الثاني

خصائص وسائل الإثبات الرقمية وميزاتها

استناداً إلى الطبيعة الخاصة لمفهوم وسائل أدلة الإثبات الرقمية والتي تميزها عن الأدلة التقليدية كما وضحنا في المطلب الأول، فلا بد أن يكون لها خصائص وميزات تميزها عن خصائص الأدلة الأخرى التقليدية وميزاتها، وعليه سنتناول أهم الخصائص التي تميز الأدلة الرقمية عن الأدلة التقليدية ومميزاتها من خلال فرعين، الفرع الأول سنتحدث فيه عن أهم الخصائص العامة للأدلة الرقمية، والفرع الثاني سنعرض فيه أهم الميزات التي تتميز بها وسائل الإثبات الرقمية وهي الأكثر خصوصية من الناحية العلمية البحتة.

---

[1]. العربي، مصطفى إبراهيم، دور الدليل الجنائي الرقمي في الإثبات الجنائي، مجلة البحوث القانونية، ص 74.
[2]. البشرى، محمد الأمين، مرجع سابق، ص 112.

الفرع الأول

خصائص وسائل الإثبات الرقمية

البيئة التي تتواجد فيها الأدلة الرقمية والمرتبطة بالحاسوب وشبكات الإنترنت تشمل وسائل الحاسوب المختلفة والشبكات العنكبوتية والهاتف أو عبر مواقع التواصل الاجتماعي والتي ساهمت في صقل طبيعة خصائصها ألاستثنائية التي تميزها عن باقي وسائل الإثبات التقليدية، وهي كالتالي:

1. **الأدلة الرقمية أدلة علمية :** في حال ظهور الدليل الرقمي إلى حيز الوجود فإنه ينبئ عن ارتكاب جريمة الكترونية، والتي لا يمكن الكشف عن أدلة ارتكابها واستخدامها والاطلاع عليها إلا من خلال الوسائل والأساليب العلمية، وعند قيام أي جهة كانت سواء الخبراء أو الضابطة القضائية أو جهات التحقيق الابتدائي أو المحاكمة باستخدام هذه الأدلة سعياً منهم لإثبات الحقيقة فإنه لا يمكن لهم ذلك إلا من خلال اللجوء إلى الوسائل العلمية، **فالدليل العلمي يخضع لقاعدة لزوم اتفاقه مع الحقيقة كاملةً وفقاً للقاعدة التي تنص على أن" القانون مسعاه العدالة أما العلم فمسعاه الحقيقة".**

وتفيد هذه الخاصية مسألة حفظ الدليل الرقمي، حيث يجب أن تبنى عملية حفظ الدليل الرقمي على أسس علمية، ثم أنها كذلك في ضرورة الحث على تحديث أسلوب تحرير المحاضر في هذا الشأن، فتحرير محضر يتناول دليلاً علمياً يختلف عنه في تحرير محضر يتناول اعتراف شخص بجريمة قتل أو سرقة عادية، أو انتهاك حرمة منزل، فتحرير محضر يتناول دليلاً علمياً يعني في الحقيقة ضرورة توافر مسلك علمي في تحريره يتوافق مع ظاهر الدليل العلمي تحديداً، بحيث يجب أن لا يتخذ المحضر المظهر التقليدي فقط، فيجب التذكير بضرورة الارتباط بالخبرة وتحديد الخبرة في محضر ضبط الدليل العلمي.[1]

وعليه فإنه يتحتم على المختصين الباحثين عن الدليل الرقمي فهم طبيعة الفضاء الرقمي، والمحتوى الرقمي، والولوج إلى جغرافيا العالم الافتراضي ضمن اطر تنظيمية معينة، خاضعين للقوانين الرقمية المعلوماتية المعتمدة، التي حددتها التشريعات الوطنية، وبما لا يتعارض مع الاتفاقيات والمعايير الدولية.

2. **تقنية الأدلة الرقمية:** التقنية بنت العلم، ولا يمكن ان تتواجد تقنية بدون أسس علمية، وإذا تم التأكيد على أن الدليل الرقمي هو دليل علمي فإن ذلك يثبت بالضرورة أن التقنية هي الخاصية الثانية التي يتمتع بها الدليل الرقمي، ولكي يتم التعامل مع الدليل الرقمي يجب أن يكون ذلك

---

1. حمودة، علي محمود، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ونظمته شرطة دبي، في الفترة 26 – 4 إلى 28-4-2003 ، دبي، ص 22.

من قبل تقنيين مختصين في الدليل الرقمي والعالم الافتراضي ككل، فالدليل الرقمي ليس مثل الدليل العادي، فلا تنتج التقنية سكيناً يتم به اكتشاف القاتل أو اعترافاً مكتوباً أو مالاً في جريمة الرشوة أو بصمة إصبع،[1] وإنما ما تنتجه التقنية هي نبضات رقمية تتشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب على أية شاكلة يكون عليها.

ومثل هذا الأمر لاحظه المشرع البلجيكي فقام بمقتضى قانون 8 نوفمبر 2000 بتعديل قانون التحقيق الجنائي بإضافة المادة 39 التي سمحت بضبط الأدلة الرقمية، مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية.[2]ما يؤدي لوضوح الرؤية بشأن دورها في الإثبات الجزائي.

ويمكن أن تكون هذه الخاصية دعوة إلى سلطات الضبط القضائي والتحقيق لكي يمكنهما الشروع في بناء منطق لا ينسب إلى الخبرة كما هو الدارج في هذا الإطار، فمثلاً إن سلطات التحقيق الجنائي في العديد من الدول وعلى رأسها الولايات المتحدة لديها مقومات الاستدلال والتحقيق والتقنية الكاملة، وهو أمر يستفاد منه الفصل بين الخبرة وبين السلطات الأخرى كسلطات الاستدلال والتحقيق، وذلك نتيجة لما تحظى به مؤسساتهم من هيكلة تقنية كبيرة، بل انه يمكن القول إن مؤسسات الضبط القضائي وسلطات التحقيق في الولايات المتحدة الأمريكية وألمانيا ساهمت بشكل كبير في تطوير تكنولوجيا المعلومات من خلال البحث المستمر.[3]

وفي المقابل، نجد أن قرار بقانون الجرائم الإلكترونية الفلسطيني، الذي جرى نقاشه وإقراره دون مشاورات مجتمعية تشمل المختصين في المجال الرقمي، يُركز على الجانب الموضوعي ألتجريمي ويتجاهل الجانب الإجرائي المتعلق بالأدلة الرقمية وكيفية التعامل معها، والحال كذلك في قانون العقوبات القديم 1960 النفاذ في الضفة الغربية وقانون العقوبات الأكثر قدماً 1936 الذي لا زال نافذا في قطاع غزة. وفيما يبدو، أن الفلسفة التشريعية في قرار بقانون الجرائم الإلكترونية انصبت على التوسع في التجريم ليطال حرية التعبير عن الرأي تحت ستار الجرائم الإلكترونية ولم تكترث بتنظيم الأدلة الرقمية في مجال الجرائم الإلكترونية.

3. الدليل الرقمي ذات طبيعة مزدوجة: تعتبر هذه الطبيعة المزدوجة التي يختص بها الدليل الرقمي امتداداً للطبيعة العلمية والتقنية التي يتمتع بها، وأيضا امتداداً للبيئة الافتراضية التي تكَوَنَ فيها كما سبق ذكره، لذا فالمعلومات والبيانات التي تشكل لنا دليلاً جنائياً رقمياً تكون في الأصل شكلاً

---

[1] . Brian Caeeier – Open Source Digital Forensics Tools: The Legal Argument -1- Oct. 2002, S T A.

[2]. منصور، محمد حسين، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، مصر، 2006، ص 272.

[3]. يونس، عمر محمد، الدليل الرقمي، ندوة لجامعة الدول العربية للتنمية الإدارية، القاهرة، 2006، ص 8 – 39.

ثنائياً أو رقمياً، ومردَ ذلك أن الحاسب الآلي أو أي جهاز أخر له نفس خصائصه، يقوم باستقبال هذه البيانات والمعلومات وتحويلها إلى أرقام ثم معالجتها.[1]

فمضمون الطبيعة المزدوجة للدليل الرقمي، هو اختزال البيانات أو المعلومات كالنصوص أو الصور أو الصوت أو أي معلومة أخرى إلى رموز ثنائية، وهذه الرموز الثنائية تتكون من سلسلة من رقم (0) ورقم (1)، ومثال ذلك أن الحرف (أ) يقابله في البيئة الافتراضية (11000110)، وهكذا يتم من خلال طرق الترميز نقل وتمثيل البيانات المختلفة لتكون صالحة للتعامل معها داخل الحاسب الآلي وكذلك الأجهزة الرقمية، بحيث إن لغة التعامل بين الأجهزة هي النظام الثنائي الرقمي، والتي تسمى في الأصل لغة الأدلة.[2]

4. **الدليل الرقمي متنوع ومتطور:** وتعني هذه الخاصية انه على الرغم من أن الدليل الرقمي في أساسه متحد التكوين بلغة الحوسبة والرقمية، فإنه مع ذلك قد يتخذ أشكالاً مختلفة، فمصطلح الدليل الرقمي يشمل كافة إشكال وأنواع البيانات الرقمية الممكن تداولها رقمياً، بحيث يكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني.[3]

ولا بد من الإشارة إلى أن الدليل الرقمي متنوع في شكله، فقد يكون على شكل بيانات مشفرة غير مقروءة عبر المصدر أو الخادم، وقد يكون معداً بنظام المعالجة الآلية للكلمات الرقمي مفهوماً للبشر كما لو كان وثيقة بأي نظام، كما من الممكن أن تكون صورة ثابتة أو متحركة أفلام رقمية أو مدة بنظام تسجيل السمعي المرئي أو تكون مخزنة من نظام البريد الإلكتروني، وقد يكون ذلك أيضا مرتبطاً بالتشفير للحفاظ على حقوق المؤلف، حيث تعد مسألة حقوق المؤلف من المسائل الشرسة التي تكتسح العالم الافتراضي والإنترنت.[4]

وعليه فإن الدليل الرقمي عبارة عن نبضات مغناطيسية يتم معالجتها لتتحول إلى لغات برمجة رقمية تشمل جميع البيانات والمعلومات الرقمية التي يمكن تداولها رقمياً بأشكال مختلفة، سواء كانت متعلقة بالحاسب الآلي أو شبكات الإنترنت والاتصالات السلكية واللاسلكية، لهذا تكون المعلومات المتحصلة

---

[1]. العتيبي، غازي سليمان، (2019 – 2020)، درجة توافر كفايات البحث عن الدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، السعودية.

[2] . Personal Education , File system Analysis , Brain Carrier –,United states of America, 2005, p22.

[3]. المعايطة، منصور عمر، (2009)، الأدلة الجنائية والتحقيق الجنائي، دار الثقافة للتوزيع والنشر، عمان ، الأردن ، ص 27 – 28.، ص 35.

[4]. حمودة، علي محمود، مرجع سابق، ص 24.

من الفضاء الإلكتروني أو العالم الافتراضي قيمة وتنذر بقيام جريمة الكترونية آم لا، وما إذا كانت تصلح أن تكون أدلة إدانة أو براءة.

ومنه، فهذا التنوع إن دل على شيء، فإنما يدل على اتساع قاعدة الدليل الرقمي، بحيث يمكنه أن يشمل أنواعاً متعددة من المعلومات والبيانات الرقمية التي تصلح لان تكون دليلاً جنائياً ببراءة المتهم أو إدانته.[1]

5. **صعوبة التخلص من الدليل الرقمي:** الأدلة الرقمية يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفاءها، مما يؤدي إلى صعوبة التخلص منها، وهي خاصية من أهم خصائص الدليل الرقمي بالمقارنة مع الدليل التقليدي، فهنالك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغاؤها سواء تم ذلك الأمر (Delete) أو حتى عمل إعادة تهيئة للقرص الصلب باستخدام الأمر (Format)، والبرامج التي تم إتلافها أو إخفاؤها سواء كانت كذلك صوراً أو رسوماً أم كتابات أم غيرها، فإن الملف الذي تم حذفه يمكن استرداده بواسطة برامج استردادية للملفات المحذوفة، مما يعني صعوبة إخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن والعدالة.[2]

ولقد كانت قضية إيران – كونترا من أولى القضايا التي برزت فيها طبيعة صعوبة إزالة الدليل الرقمي وما يتمتع به من صلابة، ففي هذه القضية أدرك المسئولون في الحكومة الأمريكية،[3] عدم وجود اتزان في مقارنة الدليل الورقي في الدليل الرقمي، فالدليل الورقي يمكن التخلص منه بتمزيق الورقة التي تحمله في حين أن الدليل الرقمي يمكن إعادته إلى الحياة، حتى وان كان قد تعرض للإزالة ولقد ترتب على هذا الأمر أن قامت الإدارة الأمريكية بالاطلاع على نظام الحفظ للبريد الإلكتروني فتبين تورط بعض المسؤولين في مكتب الرئيس الأمريكي.[4]

---

[1]. سعيداني، نعيم، (2012 – 2013)، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، الجزائر، ص 124.

[2]. الحمداني، ميسون خلف، (2016)، مشروعية الأدلة الإلكترونية، معهد البحوث و الدراسات العربية، مجلة جامعة النهرين، العدد 2، المجلد 18، مصر.

[3] . Christine Sqarlata & David J. Byer – The Electronic Paper Trail . At 6.

[4]. حمودة، علي محمود، مرجع سابق، ص 30.

الفرع الثاني

ميزات وسائل الإثبات الرقمية

نظراً للطبيعة الخاصة التي تميز الأدلة الرقمية عن الأدلة الجنائية التقليدية والتي أشار إليها الباحث في الفرع الأول من هذا المطلب، فإنه لا بد من ذكر بعض أهم مميزات الأدلة الرقمية عن الأدلة الجنائية التقليدية والتي سنقوم بعرضها كالتالي:

أ. يمكن للمختصين في المجال الرقمي أن يستعيدوا الملفات ورسائل البريد ومعلومات المواقع الإلكترونية المفقودة أو المحذوفة والعثور على المعلومات المخفية منها بالاعتماد على برامج إلكترونية معدة لهذا الغرض[1].

ب. للأدلة الرقمية مجال أوسع في الإثبات لتعدد وانتشار أدواتها، وقد تتعامل مع معلومات حساسة وأكثر شخصية من الأدلة التقليدية[2].

ج. يمكن عمل نسخ احتياطية للأدلة الرقمية مطابقة للأصل، وتكون لها ذات القيمة في الإثبات ، وهو الأمر الذي لا يتوافر في الأدلة التقليدية، وهذا ما يشكل ضمانة مهمة للحفاظ على الدليل ضد التلف أو التغيير أو الفقد[3].

د. لا يعد الدليل الرقمي دليلاً مادياً فهو غير ملموس بطبيعته، حتى وإن استخرج في شكل مادي فإنه لا يفقد صفته، وهذا لأن عملية الاستخراج لا تعدو أن تكون عملية نقل من الطبيعة الرقمية غير الملموسة (Software) إلى الهيئة الصلبة أو الملموسة (Hardware) التي يمكن أن يستدل بها على معلومة معينة[4]، فالدليل الرقمي لا يمكن إدراكه بالحواس العادية وإنما يتطلب الاستعانة بخبراء وأجهزة كالحاسوب وأدوات خاصة كالطابعة والكاميرا الرقمية وغيرها، وقد يتطلب بعض البرامج الحاسوبية المعقدة[5].

ه. الطبيعة الثنائية للدليل الرقمي، وهو ما يقوم به من عملية اختزال للمعلومات والبيانات كالصوت أو الصور أو النصوص وتحويلها إلى رموز ثنائية، كما أوضحنا ذلك مسبقاً[6].

---

1. Grobler, Marthie (2012), The Need for Digital Evidence Standardisation, International Journal of Digital Crime and Forensics, 4(2), p.2.

2. Goodison, Sean E. and Others, op.cit, P.3

3. فرغلي، عبد الناصر محمد والمسماري، محمد عبيد، (2007)، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، جامعة نايف العربية للعلوم الأمنية، الرياض ، ص15.

4. تقرير صادر عن مركز هردو لدعم التعبير الرقمي (2014)، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، ص23.

5. الحمداني، ميسون خلف، مرجع سابق، ص200.

6. المطلب، طاهري عبد (2014-2015)، الإثبات الجنائي بالأدلة الرقمية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر، ص9.

و. تعد الأدلة الرقمية ذات طبيعة متطورة ديناميكية فهي تنتقل بسرعة فائقة عبر شبكات الاتصال أو برامج معدة لهذا الغرض، ويمكنها رصد تحركات الأشخاص وتحليلها وتسجيل المعلومات عنها، فضلاً عن تسجيل عادات وسلوكيات الفرد وأموره الشخصية، لذا فقد تجد المحكمة وأطراف الدعوى، ضالتها عند الاستعانة بالأدلة الرقمية ذات الصلة بالجاني أو بالواقعة الإجرامية محل نظر المحكمة[1].

وعليه فإنه يمكننا الاستفادة مما سبق والقول بأن الدليل الرقمي لا يمكن رده أو التشكيك في قيمته كونه بحكم طبيعته الفنية يمثل إخبارا صادقاً عن الوقائع وحقيقة علمية ثابتة إلا إذا كان هذا الدليل ليس له أي صلة بالجريمة موضوع الإثبات. كما أن التخلص من الأدلة الرقمية عسيرٌ خلافاً لما هو الحال في الأدلة التقليدية. ولا يُعقل أن يشهد العصر الرقمي تطوراً هائلاً في الأدلة الرقمية في حين يبقى الإثبات رهيئة الأدلة التقليدية.

[1]. سوهيل، بن قدوم، ليدية، بسام (2017-2018)، الدليل الرقمي في الإثبات الجنائي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة- بجاية، الجزائر، ص14.

المبحث الثاني

آليات ضبط الأدلة الرقمية وإجراءات الحصول عليها

إن ضبط الدليل الرقمي من شأنه أن يُكوِن نظرة واضحة عن الجريمة الإلكترونية عموماً، ويمنح إمكانية تقديم هذا الدليل أمام القضاء لإثبات التهم الموجهة إلى مرتكبي مثل هذه الجرائم. كما أن عملية ضبط هذا الدليل من شأنها أن تضفي الصفة الشرعية للملاحقة الجزائية أمام القضاء، الأمر الذي يستدعي لغايات هذا البحث تحديد مفهوم ضبط الأدلة الرقمية وإجراءات الحصول عليها وتحليلها في المطلب الأول، وبيان آليات التعامل مع الأدلة الرقمية في المطلب الثاني.

المطلب الأول

مفهوم ضبط الأدلة الرقمية وإجراءات الحصول عليها وتحليلها

يكمن مفهوم الضبط في وضع اليد على شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها ونسبتها لفاعلها، ولكن الصعوبة تكمن في ضبط الأدلة غير المرئية في الجرائم الرقمية، كضبط الوسائل الفنية المستخدمة في إتلاف البيانات، أو مسببات حذفها أو استرجاعها، وذلك لسهولة التلاعب بها من قبل مختصين، وكذلك فإن ضبط الأدلة الجنائية الرقمية أهمية كبيرة تتمثل باستخراج البيانات منها ومعاملتها وتحويلها إلى بيانات استخباراتية يمكن التحرك على أساسها، وتقديم النتائج في سياق الملاحقات القضائية، وتُستخدم في إطار جميع هذه العمليات تقنيات سليمة في مجال الأدلة الجنائية الرقمية لضمان قبول النتائج في المحكمة، ومن هنا فإننا سوف نتناول هذه الإجراءات من خلال تقسيم هذا المطلب إلى فرعين، نعالج في الفرع الأول وسائل جمع الأدلة الرقمية، ونتناول في الفرع الثاني سلسلة الإجراءات الخاصة لحيازة الأدلة الرقمية.

الفرع الأول

وسائل ضبط وجمع الأدلة الرقمية

عملية الحصول على الأدلة الجنائية الرقمية أمر صعب الوصول إليه، وذلك لما تتطلبه من خبرة ومهارة كبيرة في مجال التكنولوجيا الرقمية، إضافة إلى تعدد صور وأشكال الجريمة المعلوماتية، وللحصول على هذا النوع من الأدلة الجنائية يجب إتباع طرق ووسائل فنية معقدة، جرى تقسيمها إلى وسائل مادية إجرائية.[1]

---

[1]. عبد المطلب، ممدوح عبد الحميد، (2000)، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، دار الفتح للطباعة والنشر، الإمارات، (الشارقة)، ص 29.

أولا: الوسائل المادية الحديثة في جمع الأدلة الرقمية

يقصد بالوسائل المادية تلك الأدوات الفنية التي تستخدم غالباً في بيئة نظم معلوماتية، والتي يمكن باستخدامها يتم تنفيذ إجراءات وأساليب التحقيق المختلفة، والتي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، والوسائل المادية عبارة عن أدوات أو برامج ذات طبيعة تقنية يتم استخدامها في التحقيق بغرض إثبات وقوع الجريمة وتحديد مرتكبها، أو بالأحرى وسائل فنية الهدف منها جمع مختلف الأدلة الجناية الرقمية التي يمكن من خلالها الكشف عن ملابسات الجريمة المعلوماتية، ومنه عندما يستعمل المستخدم شبكة الإنترنت، فإنه يترك اثأرا وراءه عن كل موقع يزوره، إذ يفتح هذا الأخير سجلاً خاصاً يحتوي على معلومات كثيرة من بينها الحاسب الآلي والمتصفح، وعنوان IP، وكل هذه البيانات تعتبر من قبيل معلومات جد هامة في التحقيق.[1]

وهنا لا بد من التطرق إلى بعض الوسائل المادية العلمية التي يتم اللجوء إليها لإثبات وقوع الجريمة وتحديد من هو مرتكبها، ومن بين هذه الوسائل والبرامج المستخدمة في جمع الأدلة:

- **استخدام بروتوكول IP/ TCP**

يعتبر من أهم وأشهر البروتوكولات المستخدمة في شبكة الإنترنت ويتكون من بروتوكول (User Datagram Protocol / UDP)، بروتوكول Transmission Control Protocol / TCP ( )، وبروتوكول (Internet Protocol / IP)، ومن مميزات هذه البروتوكولات أنها تقوم بالتعاون فيما بينها بنقل المعلومات الخاصة بالمستخدم وفقاً لنظام هيكلة تبادل المعلومات المعروف باسمTCP/ IP with OSI.[2]

ويعتبر بروتوكول IP/ TCP من أكثر البروتوكولات المستخدمة في شبكة الإنترنت لأنه يعتبر جزء أساسي منه، والمسؤول عن تراسل حزم البيانات عبره وتوجيهها إلى أهدافها، فهو يوجد بكل جهاز مرتبط بالإنترنت، ويتكون من أربعة أجزاء، يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والجزء الثالث لمجموعة الحاسبات الآلية المترابطة، وأما الرابع فيحدد الحاسب الآلي الذي تم الاتصال[3] منه.[4]

---

[1]. العنزي، سليمان بن مهجعة، (2003)، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، ص 98.

[2]. البشير، سيدي محمد، (2010) دور الدليل الرقمي في إثبات الجرائم المعلوماتية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، السعودية، ص 73.

[3]. إبراهيم، خالد ممدوح، (2009)، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، ص 304.

[4]. دأود، حسن طاهر، (2000)، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، ص 288.

وعليه يعتبر رقم الجهاز المتصل بالفضاء الإلكتروني أيا كان نوعه هو الجهاز الذي تم من خلاله ارتكاب الجريمة الإلكترونية، وبالتالي تحديد الجاني مرتكب الجريمة.

زيادة على ذلك يعمل عنوان IP بشكل متزامن مع بروتوكول أخر وهو بروتوكول التحكم بالنقل TCP، والذي تكمن وظيفته في تقسيم المعلومات إلى حزم معلوماتية، ويقوم بروتوكول IP بعنونة كل حزمة مع إضافة معلومات أخرى إليها، ومنه يتم استخدام عنوان IP من خلال البحث عن رقم الجهاز وتحديد موقعه الجغرافي، بالإضافة إلى إمكانية مراقبة المستخدم من طرف مزود الإنترنت وتقديم المعلومات التي تفيد في التحقيق، بناء على أن لكل جهاز حاسب إلي يتصل بالإنترنت عنوان IP خاص به.[1]

وبناء على ما سبق ذكره، وبالرغم من المعلومات المهمة التي يحتويها بروتوكول IP/TCP، إلا انه تثار العديد من الصعوبات في استخدامه، إذ انه يحتوي على معلومات عن جهاز الحاسب الآلي وليس الأشخاص، لذلك فمن الصعوبة إثبات أن شخصاً قد ارتكب جريمة ومعلوماتية، ومع ذلك يمكن أن يستخدم كقرينة ضد مالك أو صاحب هذا الجهاز إلى أن يثبت العكس، ومن جهة أخرى إمكانية استعمال عناوين مزيفة وذلك بوضع معلومات غير صحيحة من اجل تجنب التعرف إليهم، أو حتى استخدام برامج معينة تؤمن لهم سرية تحركاتهم عبر الشبكة، وذلك بإخفاء عنوان IP عن المواقع التي يزورها.[2]

- **استخدام معلومات كوكيز - Cookies**

عند زيارة مستخدم الإنترنت أي موقع من مواقع ويب، تفتح الأخيرة ملفاً صغيراً على القرص الصلب يسمى **"كوكيز – Cookies"** بهدف جمع بعض المعلومات عنه وتحسين عملية تصفح الموقع، ومنه فهو يسجل العديد من المعلومات التي يكن أن تساعد في التحقيق من بينها تاريخ زيارة الموقع الإلكتروني، أو تاريخ إجراء التعديلات عليه أو الانتهاء منه، وزيادة على ذلك الاحتفاظ بكلمات السر الخاصة بالمستخدم عند زيارته للموقع،[3] كما تعتبر الكوكيز أداة يتم من خلالها جمع البيانات التعريفية الخاصة بالمستخدم عن طريق الاتصال بالخادم (Server) والقرص الصلب

---

[1] . Debra Littlejohn Shinder, Scene Of The cyber crime (Computer Forensic Handbook), Publishing (Inc), United stat Of America, 2002, p 240.

[2]. د. داوود، حارث عاصم، (2013)، المخاطر الأمنية في بروتوكول الإنترنت، الإصدار السادس، المجلة العربية الدولية للمعلومات، المجلد الثاني، العدد الرابع، السعودية، ص4 .

[3]. Steve Bunting And William Wei, Encase Computer Forensic, Wiley Publishing (inc), United stat Of America, 2006, p 371.

لحاسب المستخدم.[1] وهي تُسمى "ملفات تعريف الإرتباط" كونها ملفات نصيّة تحتوي على حزم من المعلومات حول المواقع التي قام الشخص بتصفحها. وهي تساعد مواقع الويب على التعرف على جهاز الحاسوب الخاص بهذا الشخص المتصفح حتى تتمكن من تقديم المحتوى بشكل أسرع.

- **استخدام معلومات البروكسي Proxy**

يعمل البروكسي كوسيط بين المستخدم والشبكة، وتقوم فكرته على أساس تلقيه طلباً من المستخدم للبحث عن صفحة ما ضمن ذاكرة (Cache) المحلية المتوفرة لديه، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فيقوم بإرسالها دون الرجوع إلى الشبكة، أما في حالة عدم تنزيلها من قبل فإنه يعمل كمزود زبون ويقوم بإرسال الطلب إلى الشبكة العالمية حيث يستخدم احد عناوين (IP) ، ومن أهم مزاياه أن ذاكرة (Cache) المتوفرة لديه تحفظ تلك المعلومات التي تم تنزيلها، وفي حالة وجود أي أشكال يتم فحص تلك العمليات المحفوظة والتي تخص المتهم والموجودة عند مزود الخدمة.[2]

في بادي الأمر تم تطوير تقنية البروكسي **Proxy** لاستخدامها كحواجز نارية لشبكة الإنترنت Firewalls، والحاجز الناري عبارة عن نظام أمني يفرض توليد جميع الرزم المرسلة أو الواردة من خلال جهاز وحيد، وتمريرها من خلال الحاجز الناري، ومنه فإن الدور الاساسي الذي تقوم به هو قيامها بدور الوسيط بين مستخدم شبكة الإنترنت وبين مواقعها، وذلك بطلب المعلومات من تلك المواقع وتقديمها للمستخدم.[3]

وبالرغم من المميزات التي تتمتع بها مزودات البروكسي **Proxy** إلا أنها تحتوي على عدة مساوئ قد تشكل عائقاً في التحقيق، من بينها منع الوصول إلى صفحات مواقع الكترونية معينة، أو الحصول على صفحات قديمة أو ناقصة أحيانا، إلا أن هذا كله لا يمنع كونها وسيلة هامة ومفيدة في التحقيق.[4]

- **استخدام برامج التتبع وكشف الاختراق**

تقوم برامج التتبع بالتعرف على محاولات الاختراق وتقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ومثاله برامج Hack Tracer وهو مصمم للعمل في الأجهزة المكتبية، وعندما

---

1. البشير، سيدي محمد، مرجع سابق، ص 37.
2. إبراهيم، خالد ممدوح، مرجع سابق، ص 306.
3. فراحتيه، خلود، (2021)، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير،جامعة محمد البشير الإبراهيمي، ص 27.
4. نظام البروكسي، ويكيبيديا، (تاريخ الدخول: 2023/10/06)، انظر الموقع الالكتروني: :
-www.+Proxy/wiki/org.wikipidia.m.en//:https

يرصد محاولة للاختراق يسارع بإغلاق منافذ الدخول أمام المخترق ثم يبدأ بعملية مطاردة تستهدف اقتفاء اثر مرتكب عملية الاختراق، حتى الوصول إلى الجهاز المرتكب منه العملية.[1]

فعندما يرصد أي محاولة للقرصنة أو اختراق جهاز الحاسب الآلي، يسارع بإغلاق منافذ الدخول امام المخترق، ثم يبدأ في عملية اقتفاء أثره حتى يصل إلى جهاز الحاسوب الذي حدثت العملية من خلاله، ويستعرض هذا البرنامج مجموعة شاملة من بيانات المخترق من حيث عنوان IP الخاص به، وتاريخ حدوث الاختراق باليوم والساعة، وفي الأخير المعلومات الخاصة بمزود الخدمة.[2]

ثانياً: الوسائل الإجرائية الحديثة في جمع الأدلة الرقمية

يقصد بالوسائل الإجرائية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية، تلك الإجراءات التي تستعمل أثناء تنفيذ طرق التحقيق الثابتة والمحددة والأساليب المتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، ومنه فالوسائل الإجرائية عبارة عن أساليب محددة قانوناً تهدف إلى إثبات وقوع الجريمة وتحديد شخصية مرتكبها، وذلك باستخدام تقنيات وبرامج الكترونية مختلفة، تماشياً مع إرادة المشرع في مكافحة الجرائم المعلوماتية، أو الجرائم التقليدية التي تتطلب استخدام هذه الوسائل.[3]

- **ضبط الأدلة**

أجاز المشرع الفلسطيني في القرار بقانون رقم 10 لسنة 2018 في مادته (32) بشأن مكافحة الجرائم الإلكترونية لجهات التحقيق المختصة، أن تصدر أمراً مسبباً ومحدداً لمأموري الضبط القضائي المختصين بضبط الأدلة الرقمية المستخدمة في ارتكاب جريمة الكترونية معاقب عليها بمقتضى القرار بقانون سالف الذكر.[4]

وإذا أسفر التفتيش عن ضبط أجهزة وأدوات ذات صلة بالجريمة يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات وعرضها على النيابة لاتخاذ المقتضى القانوني،[5] كما أجاز

---

[1]. إبراهيم، خالد ممدوح، مرجع سابق، 304.

[2]. برنامج المخبر لنظام التشغيلWindows ،(تاريخ الدخول: 2023/10/06)، انظر الموقع الالكتروني :
- www.informer.software.tracer-hack//:https

[3]. د.عبد العال، أسامة حسين، (2021)، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، المجلد 11، العدد 76، مصر، ص670.

[4]. انظر المادة (52) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م المعدل بالقرارين بقانون ذوات الأرقام (28) لسنة 2020، و (38) لسنة 2021.

[5]. انظر المادة (32) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م المعدل بالقرارين بقانون ذوات الأرقام (28) لسنة 2020، و (38) لسنة 2021.

المشرع لجهات الاختصاص القضائي الحصول على الأجهزة والأدوات والوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو البيانات ذات الصلة، وكذلك الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة، كما يمكن لها أن تقوم بنسخ هذه البيانات أو المعلومات التي لها علاقة بالجريمة في حال تعذر ضبطها، ولها أن تستعين بكافة الوسائل المناسبة لمنع الوصول إلى البيانات المخزنة بنظام المعلومات التي استحال ضبطها والتحفظ عليها بصفة فعلية، وذلك حفاظاً على هذه الأدلة، على أن تقوم بتحرير قائمة بالمضبوطات المتحفظ عليها حسب الحالة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية.[1]

- **المراقبة الإلكترونية**

لا بد من الإشارة إلى أن المشرع الفلسطيني قد أجاز لقاضي الصلح أن يأذن للنائب العام أو احد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها، والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يعاقب عليها بالحبس مدة لا تقل عن سنة، وذلك لمدة خمسة عشر يوماً قابلة للتجديد لمرة واحدة بناء على توافر دلائل جديدة، كما أجاز للنيابة العامة أن تأمر بالجمع والتزويد الفوري لأي بيانات بما فيها حركة الاتصالات أو المعلومات الإلكترونية أو بيانات مرور أو معلومات المشترك التي يراها لازمة لمصلحة التحقيقات، وذلك باستعمال الوسائل الفنية المناسبة.[2]

وقد سمح قانون الإجراءات الجزائية الفرنسي بالاستعانة بتقنية المراقبة الإلكترونية عندما تستدعي ضرورة الاستعلام عن جناية أو جنحة من الجرائم الخطيرة التي تدخل تحت نطاق تطبيق المادة (706 – 73)،[3]إذ أجاز لقاضي التحقيق بعد استطلاع رأي النائب العام، أن يسمح لعناصر الضابطة القضائية المتصرفين وفق إنابة قضائية بأن يضعوا أداة تقنية بهدف الوصول إلى المعطيات المعلوماتية من غير رضا المشتبه فيه، كما يحق لهم أيضا تخزين هذه المعطيات وحفظها ونقلها بما فيها المعلومات الظاهرة على شاشة المستخدم، وتلك المدخلة من جهته، من خلال كتابة النصوص، وهذه الرقابة تكون لمدة (4) أشهر قابلة للتجديد مرة واحدة فقط.[4]

---

[1]. المادة (53) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م المعدل بالقرارين بقانون ذوات الأرقام (28) لسنة 2020، و (38) لسنة 2021.

[2]. انظر المادة (54) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م المعدل بالقرارين بقانون ذوات الأرقام (28) لسنة 2020، و(38) لسنة 2021.

[3]. عبد المطلب، طاهري، مرجع سابق، ص 10.

[4]. كويمينر، مريم ، الخصائص القانونية للإثبات الرقمي الجزائي، 2014، ص 63.

وقد اعتبرت محكمة النقض الفرنسية في أحدث قراراتها أن مثل هذا الإجراء يعد انتهاكاً للحياة الخاصة، وانه لا يمكن أن يتم إلا تحت رقابة القاضي – الضامن للحرية الفردية – وبأمر منه ومن ثم لا يمكن إجراؤه من غير قاض يتبع للقضاء الجالس.[1]

نخلص مما تقدم إلى نشوء اتجاه فقهي وقضائي حديث هاجسه الوصول إلى الحقيقة، ولو على حساب نزاهة الدليل الجزائي، وهو ما يظهر جلياً في السماح لأطراف الدعوى بجلب الأدلة ومناقشتها، وان كانت طريقة الحصول عليها غير مشروعة، ما يستتبع أحياناً قبول القاضي الجزائي الدليل الذي تم الحصول عليه من خلال إجراء يفقد النزاهة أو الشرعية، ويبدو من هذه الأحكام أن القضاء الفرنسي بدأ ينحو إلى تكريس الاتجاه الفقهي الذي يعطي الدليل قوة وقيمة إثباتيه بصرف النظر عن قيمته القانونية،[2]

- **اعتراض المراسلات**

بالعودة إلى القرار بقانون بشأن مكافحة الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم 10 لسنة 2018 وتعديلاته، حيث جاء بالآتي (كل من التقط ما هو مرسل عن طريق الشبكة أو إحدى وسائل تكنولوجيا المعلومات أو سجله أو اعترضه أو تنصت عمداً دون وجه حق، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين).[3]

إن أي شخص يستخدم وسائل تقنية وفنية ليقوم باعتراض بيانات مرسلة عن طريق الشبكة المعلوماتية أو إحدى شبكات تكنولوجيا المعلومات لا تخصه ولا تخص أي شخص أو جهة أخرى بشكل غير قانوني سواء كان هذا الاعتراض على شخص أو منشأة خاصة أو عامة، سواء كانت البينات المراد اعتراض مشفرة أم لا، فإن القانون قد جرم ذلك ويستدعي الملاحقة الجزائية ويترتب على مرتكبيه العقوبة، إلا إذا كان الاعتراض قد وقع على بيانات عامة متاحة لعامة الناس، فإن القانون لا يعاقب على ذلك، كما ان الاعتراض يكون فقط من خلال الجهات المختصة وسلطات التحقيق المخولة لعملية الاعتراض شريطة ان يكون قرار الاعتراض صادر عن المحكمة أي بناءً

---

1. انظر قرار محكمة النقض الفرنسية رقم 13-81. .945 جنائي، الصادر بتاريخ 2013/10/22.

2.من الجدير بالذكر أن لمحكمة النقض السورية، منذ أكثر من نصف قرن موقفاً منفرداً خالفت فيه الأصل القانوني الذي يقضي بضرورة ان يكون البحث والتنقيب عن الدليل قد تم بوسائل مشروع، وأقرت فيه الاستناد إلى دليل تم الحصول عليه بصورة مخالفة للقانون، واعتبرت الدليل لا يمكن التغاضي عنه، ولا إلغاءه، لأنه أمر واقع، ولا سبيل لإنكاره، ويصح أن يكون مستنداً للحكم، نقض سوري رقم 1186 ، ص 630 ، بتاريخ 1963/11/14، مجموعة القواعد القانونية، ونقض في 1965/4/20، مجلة المحامون، السنة 1965، ص 224.

3. انظر المادة (7) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م المعدل بالقرارين بقانون ذوات الأرقام (28) لسنة 2020، و (38) لسنة 2021.

على قرار قضائي لضمان حسن سير الإجراءات حسب الأصول والقانون، وهذا حتى يصار إلى ضبط الأدلة الرقمية المتحصلة عن الجريمة الرقمية في حال الاشتباه بوقوعها، كي لا يتم استبعادها للحصول عليها بطريقة غير مشروعة.

وبالتناوب فقد منح المشرع الفلسطيني للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات وتسجيلها أو نسخها بناء على طلب من قبل النائب العام أو احد مساعديه، متضمناً موضوع طلب الاعتراض والأفعال ألموجبه له، ومدته، على أن لا تزيد مدة الاعتراض على ثلاثة أشهر من بداية تاريخ الشروع الفعلي في انجازه، قابلة للتمديد مرة واحدة فقط.[1]

- **الحجب**

وأمّا فيما يتعلق بحجب المواقع الإلكترونية؛ فهي تتم بالاستناد إلى المادة (39) من قرار بقانون الجرائم الإلكترونية، حيث يتم رفع محاضر التحريات (الاستدلالات) من قبل الأجهزة الأمنية بالمواقع التي يُراد حجبها إلى النائب العام أو أحد مساعديه، تحت عبارات فضفاضة واردة في النص المذكور (تهديد الأمن القومي أو النظام العام أو الآداب العامة) ومن ثم يقوم النائب العام أو أحد مساعديه بطلب الإذن من محكمة الصلح خلال (24) ساعة بحجب المواقع الإلكترونية وبذلك تتم عملية حجب المواقع.[2]

كما نص القرار بقانون بشأن مكافحة الجرائم الإلكترونية في مادته 39 على أنه "لجهات التحري والضبط المختصة، إذا ما رصدت قيام مواقع الكترونية مستضافة داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو غيرها، من شأنها تهديد الأمن القومي أو النظام العام أو الآداب العامة، أن تعرض محضراً بذلك على النائب العام أو احد مساعديه،

1. انظر المادة (56) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م المعدل بالقرارين بقانون ذوات الأرقام (28) لسنة 2020، و (38) لسنة 2021.
2. د. عابدين، عصام، (2022)، واقع تطبيق الجرائم الإلكترونية في الضفة الغربية بميزان المواثيق الدولية وأحكام الدستور، معهد الحقوق، جامعة بير زيت، ص 10.

وتطلب الإذن بحجب المواقع الإلكترونية[1] أو حجب[2] بعض روابطها من العرض".[3]وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة خلال 24 ساعة، مشفوعاً بمذكرة برأيها، وتصدر المحكمة قرارها في الطلب في ذات يوم عرضه عليها بالقبول أو الرفض، على أن لا تزيد مدة الحجب على ستة أشهر، ما لم تجدد المدة وفقاً للإجراءات المنصوص عليها في هذه المادة.[4]وهذا النص يدلل على الغياب الواضح لضمانات المحاكمة العادلة في التعامل مع الأدلة الرقمية.

رغم أهمية مراجعة قانون العقوبات وقانون المطبوعات والنشر إلا أنها لا تبدو كافية في مواجهة المادة (45) من قرار بقانون الجرائم الإلكترونية، كون النص المذكور (الخزّان) أوسع من القرار بقانون بأكمله عشرات المرات، كونه يعتبر كل من ارتكب فعلاً يُشكل جرُماً، في المنظومة التشريعية الفلسطينية بأكملها، باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات، أو اشترك فيها بأي شكل من أشكال الاشتراك ألجرمي فإنه يكون قد ارتكب "جريمة إلكترونية" ويعاقب بالعقوبة الواردة في ذلك التشريع.

وبتعبير أوضح فإنَّ النص المذكور يُسيطر على جميع النصوص العقابية وبخاصة القديمة التي تستخدم كمّاً هائلاً من "المصطلحات الفضفاضة" لغايات التجريم في المنظومة التشريعية لتحويلها

---

[1]. أصدرت محكمة صلح رام الله بتاريخ 2019/10/17 قراراً صدر تدقيقاً "باسم الشعب العربي الفلسطيني" بناءً على طلب مقدم من النائب العام بحجب (59) موقعاً إلكترونياً دفعة واحدة، استناداً للمادة (39) من قرار بقانون الجرائم الإلكترونية رقم (10) لسنة 2018، وقد جاء قرار المحكمة على النحو التالي"بالتدقيق في هذا الطلب تجد المحكمة أن النيابة العامة قد أسست هذا الطلب سنداً لنص المادة 2/39 من القرار بقانون بشأن الجرائم الإلكترونية رقم "10" لسنة 2018، على سند من القول إن الجهة المستدعى ضدهم، قد أقدمت على نشر ووضع عبارات وصور ومقالات عبر الشبكة العنكبوتية من شأنها تهديد الأمن القومي والسلم الأهلي والإخلال بالنظام العام والآداب العامة وإثارة الرأي العام الفلسطيني، طالبة بالنتيجة حجب هذه المواقع ومن حيث الموضوع ظاهر الأدلة المقدمة في هذا الطلب فإننا نجد أن نص المادة 2/39 من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، قد أجازت حجب المواقع الإلكترونية، ولذلك وسنداً لما تقدم فإن المحكمة تقرر إجابة طلب النائب العام وحجب المواقع الإلكترونية المذكورة أعلاه، قرار صدر تدقيقاً باسم الشعب العربي الفلسطيني بتاريخ 2019/10/17".

[2]. وكانت محكمة صلح رام الله قد أصدرت قراراً مماثلاً "باسم الشعب العربي الفلسطيني" بحجب (29) موقعاً إلكترونياً دفعة واحدة بناءً على طلب النائب العام في 12 /2017/6، قبل صدور قرار بقانون الجرائم الإلكترونية رقم (16) لسنة 2017 الذي قام مجلس الوزراء بتنسيبه للرئيس في 2017/6/20 بعد أن أقرته الحكومة في جلستها التي انعقدت في ذات اليوم وصادق عليه الرئيس محمود عباس يوم السبت 2017/6/24 (عطلة رسمية – عيد الفطر) ونُشر في الجريدة الرسمية في عدد خاص (عدد ممتاز 14) بتاريخ 2017/7/9 ونص هذا القرار بقانون في المادة (61) على أن يُعمل به من تاريخ نشره في الجريدة الرسمية.

[3]. وهذا ما أكد عليه تقرير الأمم المتحدة حول تعزيز وحماية الحقوق المدنية والسياسية المقدم إلى مجلس حقوق الإنسان في العام 2022 وثيقة رقم (A/HRC/50/55) حول حجب الإنترنت في بند "الاستنتاجات والتوصيات" التي خرج بها التقرير وتحديداً في البند (64) على أنه " تتحمل الدول المسؤولية الرئيسية عن ضمان ابتاع نهج تمتثل لحقوق الإنسان في عمليات الحجب، وفي الأساس، ينبغي لها ان تمتنع عن فرض عمليات الحجب، وان تعزز الوصول إلى الإنترنت إلى أقصى حد، وتزيل العقبات المتعددة التي تعيق الاتصال، ويقع على الشركات والمنظمات الدولية ووكالات التنمية والمجتمع المدني دور يمكن أن يؤديه في إنهاء عمليات الحجب والتقليل من تأثيرها، وينبغي للشركات أن تتفادى التعطيل إلى أقصى حد ممكن وان تبذل العناية الواجبة لتقييم المخاطر التي يتسبب فيها الحجب في مجال حقوق الإنسان ، وأن تتخذ إجراءات بشأنها، ومن الأهمية بمكان أن تدمج الوكالات الائتمانية والجهات المانحة في سبيل سعيها إلى توسيع شبكة الاتصالات وسد الفجوة الرقمية العالمية، اعتبارات حقوق الإنسان في جهودها، وأن تضع في اعتبارها إمكانية تعطيل الخدمات الرقمية بناء على أمر صادر عن الدولة، وينبغي للمجتمع المدني والمؤسسات الوطنية لحقوق الإنسان والأوساط الأكاديمية أن تواصل جهودها في الدعوة إلى مناهضة عمليات الحجب".

[4]. انظر المادة (59) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م المعدل بالقرارين بقانون ذوات الأرقام (28) لسنة 2020، و (38) لسنة 2021.

لجرائم إلكترونية وعقوبات، كما أن العقوبات بأشكالها المختلفة ترد في التشريعات داخل وخارج نصوص قانون العقوبات وقانون المطبوعات والنشر؛ كحجب المواقع الإلكترونية مثلاً الواردة في قرار بقانون الجرائم الإلكترونية ذاته أو وقف بث المحطات الإذاعية والتلفزيونية الأرضية والفضائية وشركات خدمات البث الفضائي ومكاتب المحطات الفضائية والإنتاج الإعلامي في حال لم تحصل على الموافقات الأمنية المُسبقة كشرط للتراخيص وتجديد التراخيص بموجب نظام 2018 الصادر بشأن تراخيصها .. وغيرها الكثير.[1]

لذلك نجد أن الاعتقالات على خلفية المحتوى الرقمي تستند بشكل رئيس إلى المادة (45) من قرار بقانون الجرائم الإلكترونية، فيما يستند حجب المواقع بشكل رئيس للمادة (39) من قرار بقانون الجرائم الإلكترونية. ولذلك قلنا، ونكرر، بأن اهتمام هذا القرار بقانون ينصب على "التجريم" ولا يهتم بتنظيم مجال الأدلة الرقمية.[2]

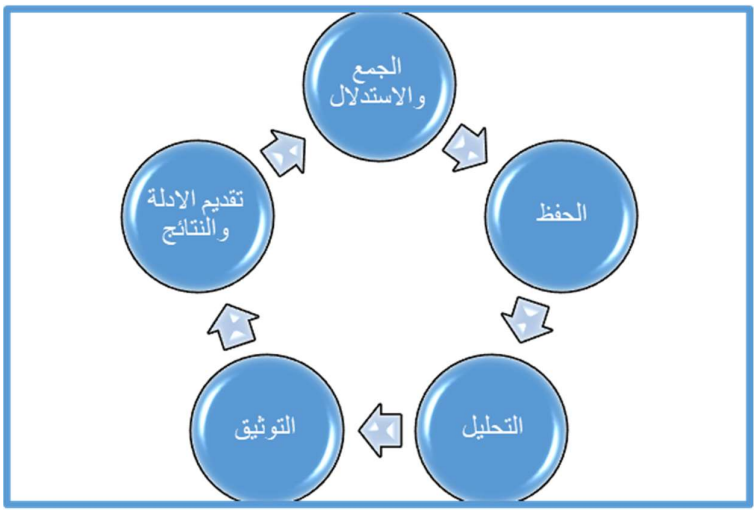
[1]. د. عابدين، عصام ، مرجع سابق، ص 18 – 19.

[2] . أعرب المقرر الخاص في الأمم المتحدة المعني بتعزيز وحماية الحق في حرية الرأي والتعبير في مذكرته الموجهة للحكومة الفلسطينية بتاريخ 16 آب/أغسطس (OL PSE 2/2017) بشأن قرار بقانون الجرائم الإلكترونية عن "قلقه العميق من أن قرار بقانون الجرائم الإلكترونية الفلسطيني يَستخدم مصطلحات فضفاضة وعلى نحو مُبالغ فيه، ويفتقر إلى تعريفات تتسم بقدر كاف من الوضوح، ويُجيز للسلطات العامة أن تُجرّم التعبير عن الرأي على شبكة الإنترنت ويفرض عقوبات بالغة القسوة على مَن يخالف أحكامه، وفي ظل غياب قانون بشأن الحق في الحصول على المعلومات، فقد يُفضي هذا الواقع إلى مأسسة الانتهاكات التي تمس الحقوق الأساسية، وقد يُفضي هذا القرار بقانون إلى فرض قدر هائل من الرقابة والرقابة الذاتية التي تُمارسها وسائل الإعلام على نفسها والأفراد على أنفسهم، ولا سيما أولئك الذين يوجهون الانتقادات للسلطة التنفيذية، ويثور قلق أخر من الإشارات المتعددة للعقوبات القاسية التي ينص عليها القرار بقانون، والتي لا تتماشى مع أحكام المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية ... وإنَّ هذه العقوبات المفروضة في القرار بقانون لا تستوفي شرط التناسب الذي توجبه المادة (3/19) من العهد الدولي الخاص بالحقوق المدنية والسياسية أنها لا تتناسب مع الأعمال التي ترمي إلى المعاقبة عليها" (نص المذكرة التفصيلية للمقرر الخاص في الأمم المتحدة المعني بتعزيز وحماية الحق في حرية الرأي والتعبير منشور كاملاً في كتاب د. عابدين عصام، (2018)، جهود مؤسسة الحق في مواجهة قرار بقانون الجرائم الإلكترونية، مؤسسة الحق، فلسطين، ص (55) وما بعدها).

الفرع الثاني

الإجراءات الخاصة لحيازة الأدلة الرقمية وتحليلها

إن سلسلة حيازة الدليل (Chain of Custody)[1]ما هي إلا وسيلة تبين من حصل على الأدلة، وأين ومتى تم الحصول على هذه الأدلة، ومن قام بتأمين الأدلة والتعامل معها، والشكل التالي يوضح مراحل وفترة الحياة التي يمر بها الدليل الرقمي:



1. **الجمع والاستدلال:** ويمكن تسمية هذه المرحلة البحث والضبط، وتتم هذه المرحلة من خلال ضباط مدربين للقيام بهذه المهمة، ومن المهم أيضا عند القيام بهذه المهمة مراعاة عدة أمور أثناء التواجد في مسرح الجريمة الإلكترونية:

- تأمين المشهد ماديا وإلكترونياً.
- فصل اتصالات البيانات الخارجية.
- تحديد الأجهزة والبيانات التي نود حفظها.
- يمكن أن تتضمن أي شكل من أشكال البيانات أو الأجهزة الإلكترونية مثل: ملفات محملة من موقع الكتروني، رسائل البريد الإلكتروني، أنشطة الإنترنت، أجهزة الكمبيوتر الشخصية وأجهزة الكمبيوتر المحمولة ومحركات الأقراص الثابتة، الهواتف المحمولة وأجهزة المساعد الرقمي الشخصي والكاميرات الرقمية.

[1]. International Bar Association (2016), Evidence Matters in ICC Trials, The Global Voice of Legal Profession, United Kingdom, P.19-20.

بخصوص الأجهزة المحمولة فينبغي إيقاف تشغيلها على الفور وإزالة البطاريات، إذا كان ذلك ممكناً حيث ان إيقاف تشغيل الهاتف المحمول يحافظ على معلومات مواقع تنقل الهاتف وسجل المكالمات، ويوقف عملية استغلال الهاتف، والتي يمكن أن تغير البيانات الموجودة على الهاتف، بالإضافة إلى انه إذا كان الجهاز مضبوطاً على أمر التدمير عن بعد يمكن استخدامه دون معرفة المحقق بذلك، وهذا من شأنه أن يضر البيانات، وبالتالي إزالة البطارية هو الحل الأمثل، ويجب وضع الأجهزة الرقمية في أكياس مقاومة للكهرباء الساكنة مثل أكياس الورق أو مغلفات البطاقات البريدية والورق المقوى، وينبغي تجنب الأكياس البلاستيكية لأنها يمكن أن تنقل الكهرباء الساكنة، أو تسمح بحدوث التكاثف أو تسرب الرطوبة.[1]

عند إرسال الأجهزة الرقمية إلى المختبر يجب على المحقق ان يشير إلى نوع المعلومات المطلوبة، على سبيل المثال أرقام الهواتف وسجلات المكالمات من الهاتف الخلوي أو البريد الإلكتروني والوثائق ورسائل الكمبيوتر والصور التي على الأقراص.[2]

وكذلك بخصوص جمع أجهزة الكمبيوتر والمعدات ولمنع تغيير الأدلة الرقمية خلال عملية الجمع يجب على فريق الاستجابة توثيق أي نشاط على جهاز الكمبيوتر أو المكونات والأجهزة على طريق التقاط صور وتسجيل أية معلومات على الشاشة، يمكن للمختص تحريك الفارة دون الضغط على الأزرار لتحديد إذا كان هناك شيء على الشاشة، إذا كان الكمبيوتر في وضع التشغيل فينصح وبشدة استدعاء خبير بالجنايات الإلكترونية حيث انه يمكن فقدان الاتصال بالنشاط الإجرامي إذا تم إيقاف تشغيل جهاز الكمبيوتر في وضع التشغيل ولكنه بدأ في تشغيل برنامج تخريبي، فيجب فصل الطاقة الكهربائية عن جهاز الكمبيوتر على الفور للحفاظ على ما تبقى على الجهاز.[3]

2. **حفظ الدليل الرقمي[4]:** في هذه المرحلة يتم عزل الأدلة الرقمية وحمايتها تماماً كما وجدت دون تغيير، بحيث يمكن تحليلها لاحقاً، ومن المهم اتخاذ تدابير وقائية مهمة من أجل الحفاظ على الدليل الرقمي:

- اتخاذ جميع التدابير اللازمة لتجنب تغيير الأدلة أو إتلافها.
- النقل إلى خزانة الأدلة إن أمكن.

---

1. هجيرة سلامة، (2017)، الإثبات الجنائي بالأدلة الرقمية، رسالة ماجستير، ص 28.
2. سعيداني، نعيم، مرجع سابق، ص 139.
3. بوعناد، فاطمة زهرة، (2013)، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة والدراسات القانونية الجزائرية، كلية الحقوق والعلوم السياسية بجامعة سيدي بلعباس، ص 68.
4. الفيل، علي عدنان (2012)، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، ط1، المكتب الجامعي الحديث، بغداد، ص 54.

- إنتاج نسخة طبق الأصل من القرص الصلب (صورة) وأحياناً في مسرح الجريمة إن كان هذا ضرورياً.

3. **التحليل:** تتم في هذه المرحلة تحليل الأدلة الرقمية والعمل على النسخ المطابقة التي تم الحصول عليها من خلال الأدلة الرقمية، ومن المهم في هذه المرحلة التعامل مع العديد من الأمور والملفات، ومنها:

- استكشاف واستخراج كل الملفات .
- استعادة كل (أو قدر الإمكان) من الملفات المحذوفة.
- الكشف عن محتويات الملفات المخفية وكذلك الملفات المؤقتة منها المستخدمة في كل من برامج التطبيق ونظام التشغيل.
- الوصول إلى محتويات الملفات المحمية والمشفرة.
- العثور على الملفات التي تم استخدامها للجريمة.

وكذلك فإنه وبمجرد إرسال الأدلة الرقمية إلى المختبر فإن الخبراء المختصين يشرعون بتحليلها وذلك بإتباعهم خطوات فينة منها:

- منع التلوث : من السهل ان نفهم حدوث التلوث في مختبر الحمض النووي أو في مسرح الجريمة، ولكن الأدلة الرقمية لديها مشاكل مماثلة والتي يجب منعها من قبل ضابط جمع الأدلة، قبل تحليل الأدلة الرقمية، يتم إنشاء صورة أو نسخة من العمل من جهاز التخزين الأصلي، وعند جمع البيانات من جهاز المشتبه به يجب ان يتم تخزين نسخة على شكل أخر من أشكال الوسائط للحفاظ على النسخة الأصلية، كما يجب على المحللين استخدام وسائط التخزين "النظيفة" لمنع التلوث أو إدخال بيانات مصدر أخر على سبيل المثال، إذا قام المحلل بوضع نسخة من الجهاز المشتبه به على قرص مضغوط يحتوي بالفعل على المعلومات، يمكن تحليل تلك المعلومات كما كانت على جهاز المشتبه به، على الرغم من أن وسائط التخزين الرقمية مثل وسائط التخزين المتنقلة وبطاقات البيانات قابلة لإعادة الاستدامة، إلا أن محو تلك البيانات ببساطة واستبدالها بأدلة جديدة ليس كافياً، فإن وحدة التخزين المستهدفة يجب ان تكون جديدة، أو إذا كانت مستخدمة، يجب أن يتم "محو" محتواها بشكل جنائي قبل استخدامها، وهذا يزيل كل المحتويات المعروفة وغير المعروفة من الوسائط.[1]

[1]. حجازي، عبد الفتاح، (2002)، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ص 31.

- عزل الأجهزة اللاسلكية: ينبغي أن يتم دراسة الهواتف المحمولة والأجهزة اللاسلكية الأخرى في البداية في غرفة العزل، إذا كانت متوفرة، هذا من شأنه ان يمنع الاتصال بالشبكات ويحافظ على الأدلة الأصلية قدر الإمكان، يمكن فتح حقيبة داخل الغرفة وبعدها يستخدم الجهاز، بما في ذلك معلومات الهاتف ومعلومات لجنة الاتصالات الفيدرالية (FCC) وبطاقات SIM وما إلى ذلك، يمكن توصيل الجهاز ببرامج التحليل من داخل الغرفة، إذا لم يكن لدى الوكالة غرفة معزولة، فإن المحققين عادةً يضعون الجهاز في حقيبة فاراداي ويقومون بضبط الهاتف على وضع الطيران لمنع الاستقبال.[1]
- تثبيت برامج حظر الكتابة: لمنع أي تغيير في البيانات الموجودة على الجهاز أو الوسائط، فإن المحلل يقوم بتثبيت برامج يحظر الكتابة على نسخة العمل بحيث يمكن الاطلاع على البيانات ولكن لا يمكن تغير أو إضافة أي شيء.[2]
- اختيار طرق الاستخراج: حالما يتم إنشاء نسخة العمل، سوف يقوم المحلل بتحديد نوع واستخدام الجهاز ومن ثم يحدد برمجيات الاستخراج المصممة بهدف تحليل البيانات أو عرض محتوياته.[3]
- إرسال الأجهزة أو الوسائط الأصلية لفحص الأدلة التقليدي: عندما تتم إزالة البيانات، يتم إرسال الجهاز مرة أخرى إلى الأدلة، قد يكون هناك حمض نووي أو اثر أو بصمة أو غيرها من الأدلة التي يمكن الحصول عليها من ذلك، ويمكن للمحلل الرقمي الآن العمل بدونها.[4]
- المضي قدماً في التحقيق: عند هذه النقطة يقوم المحلل في باستخدام البرامج التي يتم اختيارها لعرض البيانات ليكون قادراً تعلى رؤية كل الملفات الموجودة على القرص، ومعرفة ما إذا كان هناك مناطق مخفية، وحتى يكون قادراً على استعادة تنظيم الملفات والسماح بعرض المناطق المخفية وحذف الملفات المرئية أيضا طالما انه لم يتم كتابة بيانات جديدة عليها.[5]

أن الملفات على جهاز كمبيوتر أو أي جهاز أخر ليست هي الأدلة الوحيدة التي يمكن جمعها، قد يعمل المحلل على نطاق أوسع من الجهاز لإيجاد الأدلة التي تتواجد على شبكة الإنترنت بما في ذلك غرفة الدردشة، والرسائل الفورية، والمواقع والشبكات الأخرى من المشاركين أو

[1]. عريان، محمد علي، (2011)، الجرائم المعلوماتية، دار الجامعة الجديدة لطباعة والنشر والتوزيع، مصر، الإسكندرية، ص 31.
[2]. هجيرة سلامة، مرجع سابق، ص 28.
[3]. هجيرة سلامة، مرجع سابق، ص 28.
[4]. المويشر، تركي بن عبد الرحمن، (2009)، بناء نموذج أمني لمكافحة الجرائم المعلوماتية، أطروحة دكتوراه، الفلسفة الأمنية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، السعودية، ص 20.
[5]. هجيرة سلامة، مرجع سابق، ص 31.

المعلومات باستخدام نظام عناوين الإنترنت والمعلومات في عناوين البريد الإلكتروني،[1] أوقات الطوابع على الرسائل والبيانات المشفرة الأخرى ويمكن للمحلل جمع سلاسل التفاعلات معاً لتقديم صورة عن النشاط.[2]

4. **التوثيق وتقديم الأدلة:** وتعتبر هذه المرحلة هي المرحلة النهائية للتعامل مع الدليل الرقمي حيث يتم خلال هذه المرحلة:
   - تقرير رسمي نهائي (يذكر الخبير ما فعله وما وجده).
   - ملفات صور النظام.
   - الأدلة المستخرجة.
   - تقارير أدوات التحليل الرقمي المستخدمة للتحليل .
   - تقديم النتائج والشهادة عليها.

كما يجب الإشارة هنا إلى أن هنالك أربعة مبادئ أساسية للأدلة الرقمية صادرة عن رابطة كبار ضباط الشرطة في المملكة المتحدة (Association of Chief Police Officers – ACPO) ويمكن الاسترشاد بها عند إعمال وسائل الإثبات الرقمية[3] وغيرها من الأدلة الناتجة بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو البيانات والمعلومات الإلكترونية.

1. لا يجوز لأي سلطة من سلطات إنفاذ القانون تغيير البيانات الموجودة في جهاز الحاسوب أو أية وسائط تخزين يمكن الاعتماد عليها في إجراءات التقاضي.
2. يجب أن يكون الشخص الذي يتعامل مع الأدلة الموجودة في جهاز الحاسوب أو وسائط التخزين شخصاً مختصاً وقادراً على تقويمها، ويجب أن يقدم أسباباً تبين أهمية الوصول والحصول على تلك الأدلة وما يترتب عليها من نتائج ذات صلة بالتحقيق.
3. يجب إنشاء سجل لتوثيق كل ما جمع من الأدلة الرقمية وما جرى من عمليات في سبيل جمعها، وذلك من أجل تدقيقها والحفاظ عليها.

---

1. إبراهيم، خالد ممدوح، مرجع سابق، ص 32.
2. بوعناد فاطمة، المرجع السابق، ص 71.
3. Aljneibi, Khaled Ali (2014), The Regulation of Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform, PHD Thesis, Bangor University, Wales, UK, P.103

4. يتحمل القائم بالتحقيق المسؤولية الكاملة عن ضمان تطبيق القانون وهذه المبادئ خصوصاً[1].

إن هذه المبادئ تُعد تدابير أساسية يجب أن لا تنتهك، وينبغي على المحققين المختصين في الأدلة الرقمية وضعها دائماً بعين الاعتبار، ومع ذلك قد تؤدي بعض طرق الحصول على الأدلة الرقمية إلى الإضرار بالبيانات الرقمية الأصلية رغم أنها تمت بصورة سليمة، مما يؤدي إلى انتهاك المبدأ الأول المذكور آنفاً، في هذه الحالة يمكن التغاضي عن هذا الانتهاك إذا كان ضرورياً للتوصل إلى كشف الحقيقة، مع التأكد من تحقق باقي المبادئ[2].

ويجب على المحقق المختص اتخاذ كافة الاحتياطات اللازمة لتخزين وحفظ الأدلة الرقمية والتعامل معها بحذر للمحافظة على ما تحتوي من بيانات، بمعنى يجب أن تكون هذه البيانات محمية مؤمنة بصورة جيدة لكي يتم استعمالها كأدلة[3]، من خلال إزالة كل ما يؤثر على سلامتها فور استلامها والمحافظة عليها بعد تخزينها بعيداً عن المجالات المغناطيسية، وختمها وترقيمها وعمل نسخ احتياطية كلما أمكن ذلك، واستعمال النسخ الاحتياطية أولاً بدلاً من النسخ الأصلية[4].

كما ان أهمية وسائل الإثبات الرقمية تنطلق من كونها مستحدثة ومتطورة، خصوصاً إذا كانت الواقعة محل الإثبات خارجة عن الإدراك البشري المجرد، ناهيك عن الدقة التي تتمتع بها في نقل المعلومة، إذا توافرت شروطها القانونية والعلمية.

ومع ذلك لا يمكن عد وسائل الإثبات الرقمية محصنة ضد الخطأ، فهي تعتمد على دقة وسلامة الأجهزة المستخدمة وعلى درجة كفاءة المختص القائم عليها، وهي لا تخلو من العيوب، فقد تكون عملية تحديد مصدر المعلومات أمر يصعب التحقق منه، مقارنة بالشاهد الذي يرى المجرم بأم عينه، أو يسمع الصوت بأذنه، فضلاً عن ذلك من المحتمل أن يتم إصدار المعلومات عن طريق برنامج إلكتروني أو إنسان آلي (Robot)، وهذا ما يجعل عملية الإثبات تحتاج إلى إسناد أو دعم من أدلة أخرى، كأن تكون شهادة أو خبرة، أو تكون وسيلة إثبات رقمية أخرى[5].

---

[1]Wilkinson, Sue, Association of Chief Police Officers (ACPO), Good Practice Guide for Computer-Based Electronic Evidence, published by 7safe, Official release version 4.0, United Kingdom, no date of issue, P.4.

[2]Casey, Eoghan (2011), Digital evidence and computer crime – Forensic Science, computer and the Internet, Published by Elsevier Inc, USA, P.232.

[3]Dutelle, Airc W. (2014), An Introduction to crime scene Investigation, second Edition, Jones & Bartleff learning, USA, P.412.

[4]Petit, Robert and Warren, Maria and Akerson, David (2012), Prosecution Mass Atrocities Lessons from the International Tribunals, open society Foundation, Bangkok – Thailand, P.137.

[5]Outerbridge, David and Siller, Ezra, The Admissibility of Electronic Evidence, Torys LLP, Toronto.

ومن أكثر التحديات هي تلك الناشئة عن محو آثار الجريمة أو تعقب مرتكبها، وهنا تكمن الصعوبة، ففي الغالب يقوم المجرم الإلكتروني بمحو آثار الجريمة (الماديات) من خلال إتلاف الموقع أو البرامج أو التضليل مما يصعب التحقيق، وكذلك قيام شركات خاصة ببرمجة وتنفيذ تلك المواقع، وقد تكون في مناطق غير تابعة لسيطرة الدولة الفعلية أو القانونية، خصوصاً إذا كان الموقع يعمل وفقاً لبرنامج روبوت (إنسان آلي). أو أن يكون الجناة والضحايا من ولايات قضائية مختلفة، وصعوبة تعقب البيانات في "السحاب"وهي البيانات التي يتم نقلها باستمرار من خادم إلى أخر، وتتنقل داخل عدة بلدان أو تصل إليها في أي وقت، وقد تظهر البيانات الموجودة في "السحابة"لأسباب تتعلق بالأمان والتوافر، وبالتالي يمكن العثور عليها في مواقع متعددة داخل بلد واحد أو في عدة بلدان، لدرجة أنه حتى مزود الخدمة "الحوسبة السحابية" قد لا يعرف بالضبط مكان البيانات المطلوبة[1].

لا بد لنا من الإشارة إلى أن قرار بقانون الجرائم الإلكترونية الفلسطيني قد أعطى للنيابة العامة في المادة (1/3) من القرار بقانون الإشراف القضائي على أعمال وحدة الجرائم الالكترونية في جهاز الشرطة وقوى الأمن من مأموري الضابطة القضائية، كما تتولى النيابة العامة وفقاً لاختصاصها وكونها ممثلة الحق العام النظر في دعوى الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات كما نصت عليها المادة (2/3) من القرار بقانون ذاته.[2]

وإذا كان دور النيابة العامة في الإشراف على وحدة الجرائم الإلكترونية في جهاز الشرطة، باعتباره جهاز الضبط القضائي الأصيل، يُمكن تصوره في الحالة الفلسطينية، في أعمال الاستدلال وإجراءات حيازة وتحليل الأدلة الرقمية، بما يتفق وأحكام القانون الأساسي وحقوق الإنسان وضمانات المحاكمة العادلة والمعايير الدولية، فإن ما ورد في النص المذكور بشأن إنشاء وحدات للجرائم الإلكترونية في "قوى الأمن الفلسطينية" يجعل من الصعب إنْ لم يكن من المستحيل قيام النيابة العامة بالإشراف على وحدات الجرائم الإلكترونية المتعددة لدى الأجهزة الأمنية ومدى احترام الدستور والقانون وحقوق الإنسان والمعايير الدولية في التعامل الأدلة الرقمية، الأمر الذي يطرح تساؤلات بشأن المغزى من تعدد وحدات الجرائم الإلكترونية داخل قوى الأمن الفلسطينية؟

النيابة الالكترونية هي نيابة متخصصة بموجب أحكام القرار بقانون رقم (10) لسنة (2018) وتعديلاته، والتي نص في المادة (٣ /١) منه على إنشاء وحدة متخصصة من الأجهزة المتخصصة

[1]INTERPOL (2011), European Working Party on Information Technology Crime (EWPITC) – Project on cloud computing.

[2]. انظر المواد (1/3) و (2/3) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م المعدل بالقرارين بقانون ذوات الأرقام (28) لسنة 2020، و (38) لسنة 2021.

تحت إشراف النيابة العامة، وكذلك المادة (٣/ ٢) حيث أوكلت للنيابة العامة وفقاً لاختصاصها النظر في دعاوى الجرائم الإلكترونية، والتي بموجبها أنشأت نيابة الجرائم الالكترونية كنيابة متخصصة بهذا النوع من الجرائم ومنذ إنشائها والعمل جاري على تطوير أداء عمل وكلاء النيابة العامة المكلفين بالتحقيق فيها حيث شمل ذلك عقد العديد من الدورات التدريبية وتنظيم عدة زيارات خارجية للاطلاع على تجارب الدول المجاورة بالإضافة للمشاركة بورشات عمل مع الشركاء بهدف الوصول إلى توحيد العمل بكافة النيابات وهذا ما نتج عنه بالفعل إنشاء دليل الاجراءات الموحد لنيابة الجرائم الالكترونية مما سهل عمل أعضاء النيابة المكلفين والموظفين الإداريين المساندين.

كما قامت النيابة العامة في العام 2019 بعقد المؤتمر السنوي التاسع الفلسطيني التركي المشترك، بمشاركة وحضور 630 شخصا منهم 160 عضو نيابة عامة فلسطينية، و42 مشاركا من الوفد التركي، و45 وفدا دوليا، بمشاركة 22 دولة من بينهم تركيا، والذي كان بعنوان (الأدلة الرقمية بين مقتضيات التحقيق وحقوق الإنسان) والذي تناول أهمية الدليل الإلكتروني والذي يشكل الدليل الوحيد في إثبات هذا النوع من الجرائم، واتخاذ الإجراءات القانونية المتفق عليها بنصوص القانون ضمانا لصحة الدليل ومواءمته مع الاتفاقيات المتعلقة بحقوق الإنسان والحق في الخصوصية وضمان حرية الرأي والتعبير الذي كفلته أيضا دساتير الدول بما فيها فلسطين.

ومن أهم مخرجات المؤتمر ضرورة سن التشريعات اللازمة في مجال اعتماد الأدلة الرقمية كوسيلة من وسائل الإثبات أمام المحاكم، بما يسهل عمل النيابة العامة والقضاة في معالجة القضايا التي يباشرونها.

ومع ذلك، ورغم مرور خمس سنوات على فعاليات وتوصيات المؤتمر بشأن الأدلة الرقمية فإنه لم يتم تنظيمها على المستوى التشريعي بما يضمن الحفاظ على قوة وفعالية الدليل الرقمي، وينظم إجراءات الحصول عليه، بما ينسجم وأحكام الدستور والقانون والمعايير الدولية ويحترم حقوق الإنسان وضمانات المحاكمة العادلة، وما زال قرار بقانون الجرائم الإلكترونية لسنة 2018 وتعديلاته يركز على الجانب الموضوعي المتعلق "بالتجريم" ويمتد ليطال حرية التعبير تحت ستار الجرائم الإلكترونية خلافاً للقانون الأساسي والاتفاقيات والمعايير الدولية، ويهمل الجانب التنظيمي الإجرائي المتعلق بالأدلة الرقمية وكيفية التعامل معها في مجال الإثبات الرقمي. وما زالت التشريعات العقابية في الضفة الغربية وغزة قديمة وبعيدة كل البعد عن مأسسة وتنظيم الأدلة الرقمية.

ومن جهتها، تؤكد النيابة العامة بهذا الخصوص على أهمية حماية البيانات والبيئة القضائية مع الأخذ بعين الاعتبار حماية الحقوق الشخصية، بوضع قائمة للدليل الإلكتروني مرتبط بالإجراءات الجنائية

الرقمية ويتضمن آلية تخزين البيانات والمعلومات القضائية وحمايتها وإنشاء منتج يتيح للسلطات القضائية الحصول على المعلومات الإلكترونية في مدة قصيرة، ما ينعكس إيجابا على حماية حقوق الإنسان. ومع أهمية تلك الجهود، فإنها لا تغني عن المعالجات التشريعية اللازمة لمأسسة وتنظيم التعامل مع الأدلة الرقمية في فلسطين.

كما أن ما يميز الجريمة الالكترونية عن باقي الجرائم أنها جريمة متطورة عابرة للحدود وسريعة الوقوع وكذلك من السهل على مرتكبيها محو آثارها بسرعة الأمر الذي يتطلب من عضو النيابة مواكبة هذا التطور ومراجعة ما يستجد من جرائم الكترونية ووسائل مستخدمة بارتكابها، حيث لا يجب على عضو النيابة الاكتفاء بالجانب النظري من نصوص قانونية جامدة بل يجب العمل على تطوير قدراته الفنية التي تمكنه بالحد الأدنى من فهم التقارير المعدة من جهات الضبط القضائي المختصين وبالتالي توضيحها بالشكل المطلوب للمحكمة المختصة.[1] وهذا بتطلب وجود "برامج مُستدامة" من أجل بناء وتعزيز القدرات في التعامل مع الأدلة الرقمية.

المطلب الثاني

آليات التعامل مع الأدلة الرقمية

تتمثل آليات التعامل مع الدليل الرقمي بشكل خاص في التفتيش والضبط لما لهما من خصوصية، باعتبار أن تنفيذهما يتم في العالم الافتراضي للجريمة الرقمية وليس العالم التقليدي للجريمة، وفي هذا المطلب سنتطرق لموقف الفقه والتشريع الوطني من التفتيش والضبط الرقمي في الفرع الأول وفي الفرع الثاني أهم الإشكاليات المترتبة على تفتيش الدليل الرقمي وضبطه.

الفرع الأول

موقف الفقه الدولي والتشريع الوطني في تفتيش وضبط الأدلة الرقمية

أود أن أشير بداية إلى اتفاق معظم الاتجاهات الفقيه بخصوص آليات التعامل مع الأدلة الرقمية الجنائية ولا يوجد أي خلاف حول إمكانية التعامل معها لا سيما عندما يتعلق الأمر بإجراء التفتيش والضبط عندما يكون محل التفتيش والضبط المكونات المادية للحاسب الآلي وما يلحق به، ويخضع التفتيش والضبط في مثل هذه الحالة للقواعد العامة التي تحكم التفتيش التقليدي كتفتيش الأماكن والأشخاص، ويكون التفتيش بصرف النظر عن مكان الحاسب الآلي ما إذا كان موجوداً في منزل

1. مقابلة شخصية - أ. ناصر جرار، تاريخ المقابلة 2023/09/20، رئيس نيابة مكافحة الجرائم الإلكترونية في دولة فلسطين، مكان إجراء المقابلة – مكتب النائب العام لدولة فلسطين، 2023.

المتهم أو خارجه، ومن الشخص الذي قام باستخدامه، إذ انه يمكن إجراء التفتيش التقليدي للحاسب الآلي أو من قام باستخدامه بواسطة القواعد العامة لتفتيش الأماكن أو الأشخاص مع مراعاة شروطه، وذلك إذا كان الدليل من الأدلة المادية المرئية الملموسة، ولكن السؤال هنا حول إمكانية إجراء التفتيش عندما يكون محل التفتيش شيئاً معنوياً وغير مرئي أو غير ملموس، والمتمثل في البيانات الرقمية والنبضات المغناطيسية التي تثبت قيام الجريمة الرقمية.

وقد اختلف الفقهاء حول مسألة إمكانية إعمال قاعدة تفتيش الأماكن والأشخاص في الأشياء الغير مرئية والغير ملموسة وانقسموا إلى اتجاهين:

- **الاتجاه الأول : الاتجاه الرافض لإمكانية تفتيش الدليل الرقمي وضبطه**

تتلخص حجة هذا الاتجاه في القول بأن البيانات أو المعلومات الإلكترونية لا تصلح لان تكون محلاً للتفتيش والضبط، على اعتبار أنها أشياء معنوية والتفتيش والضبط لا يرد إلا على الأشياء المادية.[1] كما يذهب هذا الاتجاه إلى القول بأن التشريعات الناظمة لعملية الضبط والتفتيش حينما صيغت، كانت من اجل آليات تفتيش وضبط الأدلة الملموسة التقليدية، ويعزو ذلك إلى أنه وقت صياغة وإصدار هذه التشريعات لم يكن للأدلة المعنوية غير الملموسة وجود يذكر.

- **الاتجاه الثاني : الاتجاه المؤيد لإمكانية تفتيش الدليل الرقمي وضبطه**

تعتمد حجة هذا الرأي على الانطلاق من التفسير الغائي للنصوص وإهمال التفسير الحرفي، لأنه هو الذي يساعد على الكشف عن الإرادة الحقيقية للمشرع من وراء إصدار النص، ولا شك أن الإرادة الحقيقية للمشرع من وراء إصدار النصوص المتعلقة بإصدار بإجراءات جمع الأدلة هي الكشف عن الحقيقة، وبالتالي فإن تلك الإجراءات إذا ما أدت إلى هذه الغاية فإنه ينبغي عدم تقييدها دون مبرر أو مسوغ قانوني إذا كان محلها البيانات أو المعلومات الإلكترونية.[2]

---

[1]. د. ارحومه، موسى مسعود، (2009)، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، كلية القانون ـ جامعة قاريونس، طرابلس، ليبيا، ص 7.

[2]. د. حمودة، محمود علي، مرجع سابق، ص 17 .

ويرى الباحث هنا أن الاتجاه الثاني كان اقرب وأصوب في تحليله لمعنى النصوص القانونية والأخذ بالمفهوم الواسع للتفتيش والضبط والذي ينسجم مع السياسة المشرع الفلسطيني حينما حدد في نصوصه تفتيش الأدلة المعنوية وغير المرئية بشكل أدق، شريطة أن يكون التفتيش مراعيا للأصول والضمانات القانونية للشخص المراد تفتيشه الكترونياً وآن يكون منسجماً وأحكام الدستور والقانون والمعايير الدولية ذات الصلة.

- **التفتيش كما يراه المشرع الفلسطيني**

لما كان الضبط بحسب الأصل لا يرد إلا على الأشياء المادية، فليس هناك صعوبة في ضبط أدلة الجريمة الواقعة على المكونات المادية للحاسوب كرفع البصمات مثلاً، وكذلك لا صعوبة أيضا في ضبط الدعامة المادية للبرامج أو الوسائل المستخدمة في إتلاف البرامج. ولكن في ضبط بيانات الحاسوب ولعدم وجود أي دليل مرئي في هذه الحالات، ولسهولة تدمير الدليل في ثوان معدودة ولعدم معرفة كلمات السر أو شيفرات المرور أو ترميز البيانات فلا بد أن يتم إتباع قواعد فنية لحماية البيانات وتجنيبها خطر الإتلاف[1]، مما حدا بالمشرع الفلسطيني[2] توسيع صلاحيات سلطة التحقيق في ضبط ما يحويه الحاسوب من بيانات دون الحاجة إلى إخطار مسبق بعملية التفتيش والضبط.

فالمادتان (52) و(53) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م وتعديلاته (القرار بقانون رقم (10) لسنة 2018م[3] بشأن الجرائم الإلكترونية المعدل بالقرارين بقانون ذوات الأرقام (28) لسنة 2020م[4]، و(38) لسنة 2021م[5])، تمنح الصلاحية للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي، ودون أمر من المحكمة المختصة، بتفتيش وسائل تكنولوجيا المعلومات ذات الصلة بالجريمة وضبط الأجهزة والأدوات والبيانات والمعلومات الإلكترونية والتحفظ على كامل نظام المعلومات أو أي وسيلة من وسائل تكنولوجيا المعلومات من شأنها أن تساعد على كشف الحقيقة، ودون حضور المتهم أو حائز الأجهزة لإجراءات التفتيش والضبط، ودون تحديد لمدة أمر التفتيش في النص المذكور.

---

[1] قنديل، أشرف عبد القادر (2018)، الوسائل الإلكترونية ودورها في الإثبات الجنائي، دراسة مقارنة ، ط1، دار الجامعة الجديدة للنشر، الإسكندرية، ص 149.

[2] المادتان (52) و(53) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م وتعديلاته.

[3] منشور على الصفحة (8) من عدد الوقائع الفلسطينية (عدد ممتاز) رقم (16) بتاريخ: 2018/05/03.

[4] منشور على الصفحة (9) من عدد الوقائع الفلسطينية رقم (171) بتاريخ: 2020/09/24.

[5] منشور على الصفحة (30) من عدد الوقائع الفلسطينية رقم (186) بتاريخ: 2021/12/23.

ينبغي أن تكون تشريعات الجرائم الإلكترونية (قرار بقانون الجرائم الإلكترونية رقم 10 لسنة 2018 وتعديلاته) منسجمة مع اتفاقية بودابست،[1] المتعلقة بالجرائم الإلكترونية في جوانبها الموضوعية والإجرائية. ما يهمنا حالياً هو الجوانب الموضوعية من اتفاقية بودابست؛ أي "التصنيف الرباعي للجرائم الإلكترونية" وهو كالتالي" جرائم تمس خصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر، والجرائم المتعلقة في الحاسوب والتي استخدمت الحاسوب كأداة لارتكاب الجريمة، والجرائم المتعلقة بالمحتوى، وأخيراً جرائم انتهاكات حقوق النشر والتأليف والحقوق ذات الصلة"، وفقاً للاتفاقية، كون الخروج على هذا التصنيف في قرار بقانون الجرائم الإلكترونية الفلسطيني يعني حتماً اتخاذ الجرائم الإلكترونية "ستاراً" للنيل من حرية التعبير عن الرأي، وفي تلك الأحوال، نكون أمام خروج مؤكد على الاختبار ثُلاثي الأجزاء (فشل في مستويات الفحص) وأمام انتهاك مؤكد طال حرية التعبير.[2]

ونعتقد بأن هذا الخروج في القرار بقانون رقم 10 لسنة 2018 في المواد 39 بشأن حجب المواقع وكذلك المادة 45 بشأن الاحتجاز التعسفي على خلفية الرأي والتعبير، ينتقص من ضمانات المتهم في مرحلة التحقيق، ويمس بالحقوق والحريات الدستورية، إذ ينبغي أن تتم تلك الإجراءات بناء على طلب من النيابة العامة، وقرار من المحكمة المختصة (الرقابة القضائية)، وأن تتم في حضور المتهم أو حائز الأجهزة وضمان توقيعه على محضر التفتيش، وأن يكون القرار الصادر عن المحكمة المختصة بالتفتيش محدداً زمنياً، وذلك حفاظاً على ضمانات المتهم في مرحلة التحقيق الابتدائي، وانسجاماً مع الاتفاقيات والمعايير الدولية على هذا الصعيد[3].

وفيما يبدو، أن الدور الأساسي الذي لعبته النيابة العامة في "صياغة" قرار بقانون الجرائم الإلكترونية وتعديلاته هو الذي يُفسّر الصلاحيات الواسعة للنيابة العامة في هذا القرار بقانون مقابل تراجع دور الرقابة القضائية، في التعامل مع الأدلة الرقمية، خلافاً لأحكام القانون الأساسي (الدستور) والمعايير الدولية. وهذا يتعارض مع السياسية التشريعية كون النيابة العامة مخاطبة

---

[1]. الإتفاقية المتعلقة بالجرائم الإلكترونية (بودابست) 2001 وتعديلاتها، مجلس أوروبا، مجموعة المعاهدات الأوروبية رقم (185)، ويُراجع أيضا التقرير التفسيري لاتفاقية بودابست الصادر عن مجلس أوروبا في 23 نوفمبر/ تشرين الثاني 2001، مجموعة المعاهدات الأوروبية رقم (185).

[2]. د.عصام عابدين، مرجع سابق، ص 14.

[3]وهذا ما أكد عليه المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير في تقريره المقدم إلى مجلس حقوق الإنسان في العام 2013 وثيقة رقم (A/HRC/23/40) في بند "الاستنتاجات والتوصيات" التي خرج بها التقرير وتحديداً في البند (81) على أنه "ينبغي على الدول أن تنظر إلى مراقبة الاتصالات ووسائل تكنولوجيا المعلومات كعمل تطفلي بدرجة كبيرة ربما يتعارض مع الحق في حرية التعبير والحق في الخصوصية ويهدد دعائم المجتمع الديمقراطي. ويجب على التشريعات أن تنص على وجوب إلا تقوم الدولة بالمراقبة إلا في ظروف استثنائية جداً، وأن يكون ذلك حصراً تحت إشراف سلطة قضائية مستقلة، ويجب أن يتضمن القانون ضمانات واضحة عن طبيعة التدابير الممكنة ونطاقها ومدتها الزمنية والأسس اللازمة للأمر بها ونوع الانتصاف الذي تتضمنه التشريعات الوطنية". وهذا ما أكدت عليه أيضا المبادئ الدولية لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات للعام 2014 وذلك في المبدأ السادس الذي شدد على أن القرارات المتعلقة بمراقبة الاتصالات يجب أن تضطلع بها سلطة قضائية كفؤ نزيهة ومستقلة منفصلة عن الجهات التي تضطلع بمراقبة الاتصالات، علماً بأن تفتيش وسائل تكنولوجيا المعلومات يندرج في تعريف "مراقبة الاتصالات" بموجب تلك المبادئ الدولية.

بأحكام هذا القرار بقانون ولا ينبغي أن تكون هي من يُصيف نصوصه وأحكامه، ونكون أمام حالة تضارب مصالح، كما أن النيابة العامة ليست جهة تشريع. علماً أن المبادئ الدولية لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات 2013 تؤكد وتشدد على الدور الحاسم للرقابة القضائية النزيهة والمستقلة في كل ما يتعلق بالتعامل مع الأدلة الرقمية كدليل في مجال الإثبات.

ومن جانب آخر، فإن قواعد الإثبات الجنائية التقليدية المعمول بها لا تصلح لإثبات الجرائم الإلكترونية بشكل مباشر، بل يحتاج ذلك لجهات إنفاذ قانون متخصصة وقضاة ووكلاء نيابة متخصصين بالشأن. وحتى يصبح الدليل الرقمي بشكل عام وذلك المتحصل من الموقع الإلكتروني على وجه الخصوص دليلاً يعتمد عليه في كشف وتتبع أثر الجريمة الإلكترونية تقوم جهات إنفاذ القانون المتخصصة بمكافحة الجرائم الإلكترونية باستخدام برامج الكشف والتتبع[1]، واتخاذ إجراءات التفتيش الإلكتروني التي تشكل في مجملها وسائل لضبط أدلة يمكن التحرز عليها وضبطها والاستعانة بأهل الفن والدراسة والخبرة لمعرفة أماكن تخزين المعلومات وإجراءات إرسالها، ويبقى الحذر مطلوباً في هذا النوع من الجرائم وذلك من خلال خلق آلية متطورة لا يكلفها إلا التعاون الدولي وتبادل الخبرات والممارسات الفضلى في هذا المجال.

مما حدا بالمشرع الفلسطيني وعلى غرار قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018 للنص في المادة (57) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م وتعديلاته على أنه: **"يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات "**[2]، فيما نصت المادة (58) من ذات القانون على أنه:**"تعتبر الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، من أدلة الإثبات ، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي"**[3]. وقد تميز المشرع الفلسطيني بهذه النصوص والتي لم يرد لها نظير في قانون الجرائم الإلكترونية الأردني رقم (24) لسنة 2015 وتعديلاته. كونها اعتبرت بشكل صريح الأدلة

---

1. Law Reform Commission (2009), Documentary and Electronic Evidence, First Published, Dublin, P.1.

2. نصت المادة (11) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018 على أنه: "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام ألمعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون".

3. نصت المادة (4) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018 على أنه: "تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقا لمبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادي ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها، على أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة في هذا الشأن".

الناتجة بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات الجنائي.

نصت المادة 19 من قانون البينات رقم 4 لسنة 2001 على ما يلي (1- تكون للرسائل الموقع عليها قيمة السند العرفي من حيث الإثبات ما لم يثبت موقعها انه لم يرسلها، ولم يكلف أحداً بإرسالها. 2- تكون للبرقيات ومكاتبات التلكس والفاكس والبريد الإلكتروني هذه القوة أيضا إذا كان أصلها المودع في مكتب التصدير موقعاً عليها من مرسلها، وتعتبر البرقيات مطابقة لأصلها حتى يقوم الدليل على عكس ذلك).[1]

وكذلك فإنه وبالرجوع إلى القرار بقانون رقم (39) لسنة 2022 بشأن مكافحة غسل الأموال وتمويل الإرهاب فقد نص في المادة (45) فقرة (3) على أنه "للنيابة العامة أو من تنتدبه، الوصول إلى الأجهزة الإلكترونية وأنظمة وشبكات الحاسوب، وذلك وفقاً للقوانين النافذة في الدولة". ما يعزز القيمة القانونية للأدلة الرقمية في الإثبات في التشريعات الفلسطينية من خلال قرار بقانون الجرائم الإلكترونية ومن خلال قرار بقانون مكافحة غسل الأموال وتمويل الإرهاب 2022 وهو التشريع الفلسطيني النافذ حالياً بهذا المجال.

وعلى الرغم من تأكيد التشريعات الفلسطينية المذكورة على القيمة القانونية للأدلة الرقمية في الإثبات الجزائي إلا أنها لم تنظم لغاية الآن إجراءات التعامل مع الأدلة الرقمية بما يكفل اتباع الطرق العلمية في حيازة الدليل الرقمي وتحليله والتعامل معه ويضمن مراعاة تلك الإجراءات لحقوق الإنسان والضمانات المكفولة في أحكام القانون الأساسي المعدل (الدستور) وفي الاتفاقيات والمعايير الدولية لحقوق الإنسان.

[1]. المادة (19) قانون البينات الفلسطيني رقم 4 لسنة 2001 الصادر بتاريخ 2001/05/12 .

الفرع الثاني

الإشكاليات المترتبة على تفتيش الدليل الرقمي وضبطه

أثيرت بعض الإشكاليات حول كيفية تنفيذ التفتيش عن الدليل الرقمي وضبطه أهمها إشكاليات متعلقة بكيفية إجراء التفتيش حينما يكون جهاز المتهم متصلاً بغيره من الأجهزة الأخرى، وكذلك الإشكاليات المتعلقة بكيفية إجراء التفتيش والضبط للدليل الرقمي إذا كان جهز المتهم المراد تفتيشه محمياً بواسطة كلمة سر تمنع الولوج إلى البيانات والمعلومات الرقمية، وإشكاليات تتعلق بكيفية التحرز على الدليل الرقمي بعد تفتيشه وضبطه، إضافة إلى الصعوبات العملية التي تتعلق بالتفتيش عن الدليل الرقمي وضبطه.

أولا: الإشكاليات المتعلقة بتفتيش الدليل الرقمي وضبطه

1- الاتصال بجهاز المتهم محل التفتيش والضبط بغيره من الأجهزة

في بعض الأحيان يكون جهاز المتهم عند قيامه بجريمة رقمية ما متصلاً بأجهزة أخرى سواء داخل حدود الدولة أو خارجها، وعند تفتيشه وضبطه قد يشكل مساس بحقوق غير المتهم إذا ما امتد التفتيش إلى جهاز الغير إذا كان داخل حدود الدولة ومساساً بسيادة الدولة في حال امتد التفتيش إلى خارج حدود دولة المتهم مرتكب الجريمة الرقمية، فهل يمكن إجراء التفتيش في كلتا الحالتين دون المساس بحقوق غير المتهم وسيادة الدولة؟

في حالة الاتصال بنظام المتهم بنظام أخر موجود في مكان أخر داخل الدولة جاز لجهات الاختصاص بالمباشرة في عملية التفتيش والضبط للعالم الافتراضي للجريمة بعد إعلام السلطات القضائية واخذ الإذن كما اشرنا آنفاً في النصوص القانونية بموجب القرار بقانون بشأن الجرائم الإلكترونية النافذ، أما في حالة كان نظام المتهم الإلكتروني متصل بنظام أخر الكتروني موجود خارج حدود الدولة فإنه قد أجازت بعض التشريعات الوطنية تفتيش وضبط الأدلة الرقمية المتحصلة من الجريمة حتى وان كانت خارج حدود الدولة لا سيما المواد (62) و (63) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م وتعديلاته، وذلك بموجب تقديم العون للجهات النظيرة في الدول الأخرى وذلك في إطار الاتفاقيات الدولية والإقليمية، أو من مبدأ المعاملة بالمثل والذي من شأنه أن يكفل بالإنذار المبكر بالجرائم المعلوماتية وتفادي ارتكابها وأيضا المساعدة على التحقيق فيها وملاحقة مرتكبها،[1] ولغايات تقديم المساعدة القانونية

[1]. (62) و (63) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م وتعديلاته.

المتبادلة، وتسليم المجرمين لاستكمال التحقيقات والإجراءات الجنائية المرتبطة بالجرائم وفقاً للقوانين الوطنية والمعاهدات والاتفاقيات الدولية التي تكون الدولة طرفاً فيها.

كما أشارت الإتفاقية الأوروبية بشأن الجرائم الإلكترونية الصادرة عن مجلس الإتحاد الأوروبي عام 2001 (**اتفاقية بودابست**) لنظام المساعدة القانونية المتبادلة بين الدول في مجال تفتيش الدليل الرقمي وضبطه، حيث ألزمت المادة (1/25) بتبادل المساعدة القانونية بين الدول الأطراف بأقصى قدر ممكن للتحقيق في الجرائم الرقمية وجمع الأدلة المتحصلة منها.[1]

وكذلك الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي وقعت بين دول مجلسي الداخلية والعدل العرب بتاريخ 2010/12/21 بمقر الأمانة العامة لجامعة الدول العربية في القاهرة والتي أقرت في المادة (32/ 1) بضرورة تبادل المساعدة القانونية المتعلقة بجمع الأدلة الرقمية لإثبات الجرائم الواقعة خارج حدود الدولة.[2]

كما أجازت الاتفاقيتان ودون الحصول على إذن مسبق أو تفويض من دولة طرف ان تصل إلى البيانات والمعلومات الرقمية أينما كان موقعها الجغرافي بشرط أن تكون هذه البيانات والمعلومات متاحة للعامة، وهو ما يسمى بالمصدر المفتوح للمعلومات.

2- حماية جهاز المتهم محل التفتيش والضبط بكلمة سر

من الممكن أن يكون الجهاز أو التطبيق المراد تفتيشه للولوج للمعلومات أو البيانات والتي قد تشكل دليل رقمي يثبت وقوع الجريمة ويعتد به أمام الجهات القضائية محمي بموجب كلمة سر تحول دون عملية التفتيش، فهل بالإمكان إجبار المتهم على الإفصاح عن كلمة السر حتى يتسنى تفتيش الجهاز أو المتصفح؟؟

في حال كان المتهم هو المراد منه الإفصاح عن كلمة السر، فيرى جانب من الفقه انه لا يجوز إجبار المتهم في مثل هذه الحالة على الإفصاح عن كلمة السر بهدف الولوج إلى المعلومات محل التفتيش أو الضبط، لأن في ذلك إخلالاً بحق الدفاع وإهدارا لمبدأ افتراض البراءة الذي يعطي للمتهم الحق في عدم تقديم دليل ضد نفسه، بل والحق في التزام الصمت.[3]

---

[1]. انظر المادة (25 /1) من اتفاقية بودابست بشأن الجرائم الإلكترونية الصادرة عن مجلس الإتحاد الأوروبي بتاريخ 2001/11/23 .
[2]. الإتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن مجلس الداخلية والعدل العرب بتاريخ 2010/12/21 في القاهرة.
[3]. د حمودة، علي محمود، مرجع سابق، ص 19.

ويرى الباحث هنا أن إجبار المتهم على الإفصاح عن كلمة السر بلا أدنى شك فيه أي إهدار لحق المتهم في الدفاع أو مساساً بقرينة البراءة، مثله مثل تفتيش المنازل والحقائب، كأن يكون المنزل المراد تفتيشه مقفل بمفاتيح بحوزة المتهم وهو مالك المنزل، أو أن تكون الحقيبة المشتبه بها مقفلة بأرقام سرية لا يعلمها إلا المتهم صاحب الحقيبة ولا يعلمها غيره، فإجبار المتهم على إعطاء مفتاح المنزل أو فتح حقيبته المغلقة بكلمة سر يعتبر انتهاكاً لحق الدفاع ومساساً بقرينة البراءة ويندرج تحت طائلة الإكراه، والتي لم تجيزها القوانين والقواعد الإجرائية المتعلقة بتفتيش المنازل والأشخاص.

أما في حال كان المراد منه الإفصاح عن كلمة السر هو غير المتهم، فيرى جانب من الفقه بأنه بالإمكان إجبار غير المتهم على الإفصاح عن كلمة السر لتيسير الدخول إلى المصدر الإلكتروني للمعلومة محل التفتيش أو الضبط، لأن الإكراه الواقع على غير المتهم لا يمس حقوق الدفاع، خلافاً للوضع بالنسبة للمتهم.[1]

3- مدى إمكانية تحريز الدليل الرقمي بعد ضبطه

هناك من الوسائل الإلكترونية ما يمكنه تحقيق فكرة التحريز بالنسبة للدليل الإلكتروني، والتي تعتمد في مجملها على فصل المعلومات الإلكترونية عن مصدرها ونقلها إلى أداة تخزين خارجية (USB, CD) أو طباعتها على ورق إذا كانت في شكل نصوص مكتوبة، ثم تحرز تلك الأداة التخزينية أو الورق المطبوع بالطريقة التي حددها النص.[2]

ولا شك أن الغاية من ضوابط التحريز التي أشار إليها النص هي المحافظة على الدليل الرقمي وتوقي احتمال العبث به، حتى لا تضعف قوته الإثباتية أمام القضاء.

وقد تدخل المشرع الفرنسي بموجب تعديله لقانون الإجراءات الجزائية من خلال القانون رقم 239-2003 أين أسندت الفقرة الثالثة من المادة 57، والتي نصت على نسخ جميع المعلومات والبيانات الرقمية الناتجة عن التفتيش على دعامات التخزين الإلكترونية وتحريزها، وإذا كان الدليل الجنائي يخضع إلى قواعد تحريز الأدلة الجنائية، إلا انه وبالنظر إلى الطبيعة التقنية والفنية التي يختص بها، فإن عملية ضبطه تستوجب بعض الإجراءات الخاصة لحمايته والحفاظ عليه من العبث.[3]

---

1. د. ارحومة، موسى محمود، مرجع سابق، ص 9.
2. الجملي، طارق محمد (2009)، الدليل الرقمي في مجال الإثبات الجنائي، ورقة مقدمة إلى ألمغاربي الأول حول المعلوماتية والقانون، ليبيا، ص 39.
3. هروال، آية نور الهدى، (2021)، الأدلة الرقمية في إثبات الجريمة الإلكترونية، رسالة ماجستير، جامعة ابن خلدون، ص 35 -36.

ثانياً: الصعوبات العملية المتعلقة بالتفتيش عن الدليل الرقمي وضبطه

أثناء عملية التفتيش عن الدليل الرقمي وضبطه وكيفية التحرز عليه لا بد من مواجهة بعض الصعوبات والتي يمكن تلخصيها على النحو التالي:

1 – نقص الخبرة لدى جهات التحقيق والمحاكمة

يتطلب البحث عن الدليل الرقمي في مختلف الجرائم مهارات فنية في إدارة التحقيق وإجراء المحاسبة، تتمثل في الإلمام بتقنيات الحاسب الآلي وشبكات الاتصال ولغة التخاطب بين مستخدمي تلك التقنيات، فعن طريق الإلمام بهذه الأصول الفنية تستطيع جهات التحقيق والمحاكمة أن تناقش المتهمين والشهود والخبراء وأن تبحث عن الدليل الفني وتستخلصه من الوقائع وتقدر مدى كفايته للإدانة، خصوصاً الإلكترونية منها.[1]

وكذلك من أهم الصعوبات التي تؤثر على أعمال التفتيش الرقمي وضبطه النقص الكبير في خبرات رجال الشرطة وجهات الاختصاص بسبب الطبيعة الخاصة لمثل هذه الجرائم، حيث يتطلب إجراء التفتيش الرقمي وضبط الأدلة الرقمية خبرة متميزة للكشف عن الجرائم محل البحث والاهتداء إلى مرتكبيها إخضاع رجال الاختصاص إلى تدريب خاص يسمح لهم بفهم ومواجهة تقنيات الحاسب الآلي المتطورة وأساليب التلاعب المعقدة التي تستخدم عادةً في ارتكاب مثل هذه الجرائم، لذلك وجدت سلطات البحث الجنائي والتحقيق نفسها غير قادرة على التعامل بالوسائل التقليدية مع هذه النوعية من الجرائم ولنقص الخبرة والتدريب كثيراً ما تخفق أجهزة الشرطة في تقدير أهمية الجريمة محل البحث فلا تبذل لكشف غموضها وضبط مرتكبيها جهوداً خاصة تناسب مع هذه الأهمية.[2]

2- الإحجام عن التبليغ عن الجرائم الرقمية أو التأخر فيه

من الممكن أن يكون المجني عليه في الجريمة الرقمية هو شخصية اعتبارية كأن يكون بنك أو مؤسسة خاصة أو شركة تجارية تخشى من فقدان زبائن وذلك بسبب انعدام ثقتهم في الجانب الأمني لحفظ البيانات أو المعلومات بهذه المؤسسة أو الشركة، وقد تتأخر في اكتشاف أن الجريمة قد وقعت وبناء عليه تتأخر في الإبلاغ عنها والتي يخشى معه فقدان الدليل الرقمي أو تم العبث به، أو أن

---

1. مجلة البحوث القانونية، (2016)، كلية مصراتة، العدد الأول، ليبيا، بنغازي، ص 102.
2. نجيب، هند (2016)، التعاون القضائي الدولي في مجال الجرائم الإلكترونية، المجلة الجنائية القومية، المجلد التاسع والخمسون، العدد الثاني، ص 155.

تكون هذه المؤسسات تعاني من فقدان الثقة الفنية مع الجهات القضائية المختصة في قدرتها على التعامل مع مثل هذه الجرائم والتي قد تؤثر سلباً على عمل تلك المؤسسات.

3 – اختلاف السياسات التشريعية للدول

لا تزال بعض الدول تعتمد في تشريعاتها الوطنية في التعامل مع الجرائم الإلكترونية الرقمية على التشريعات التقليدية التي تتعامل بها في مواجهة الجرائم التقليدية، والبعض إلاخر قام بسن تشريعات خاصة للتعامل مع الجرائم المعلوماتية، ومما لا شك فيه ان اختلاف السياسات التشريعية للدول في مواجهة الجرائم المعلوماتية ستؤثر سلباً على مكافحة مثل هذه الجرائم.

وبنظرة متأنية للأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المتعلقة بشبكة الإنترنت، يتضح لنا عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحاً في احد الأنظمة قد يكون مجرماً وغير مباح في نظام أخر مما يؤدي إلى اختلاف عناصر الجريمة الإلكترونية من دولة أخرى،[1]ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لأخر، وبالتالي اختلاف السياسة الجنائية من مجتمع لأخر.[2]

كما أن الدول التي أفردت تشريعات خاصة في مجال الجرائم الإلكترونية، ولا سيما الدول العربية، تُركّز على الجانب الموضوعي المتعلق "بالتجريم" ولا تُفرد فصولاً تشريعية إجرائية للأدلة الرقمية والبحث والتحري الرقمي والضبط والتحريز والتحليل للمحتوى الرقمي والحماية والمحافظة على الأدلة الرقمية، بما يؤثر سلباً على جودة الدليل الرقمي في الإثبات، ويؤثر سلباً على حقوق وضمانات المتهم في المجال الرقمي دون شك.

4 – تواضع مستوى التعاون الدولي في مجال البحث والتفتيش عن الأدلة الرقمية

تم التطرق إلى تدني مستوى التعاون الدولي في مجال التحقيق في الجرائم الرقمية في مؤتمر الأمم المتحدة والذي عقد في البرازيل في شهر 4 من العام 2010، حول منع الجريمة والعدالة الجنائية، حيث قد تبين وجود صعوبات كبيرة أثناء تطبيق عدد كبير من الاتفاقيات الموقعة بين الدول والتي

---

1. حجازي، عبد الفتاح بيومي ، مرجع سابق، ص 102.
2. عبد اللطيف، براء منذر كمال ، منديل، ناظر احمد (2009)، التعاون القضائي الدولي في مواجهة جرائم الإنترنت، المؤتمر العلمي الأول حول تحولات العام في مطلع الألفية الثالثة، كلية القانون، جامعة تكريت، العراق، ص 11.

تعنى بالمساعدة القانونية، وذلك بسبب استنادها إلى إجراءات رسمية معقدة تحتاج إلى وقت طويل لتنفيذها.

ومن جانب أخر لا بد من التطرق إلى إشكالية عدم وجود نظام الاتصال يسمح بتبادل المعلومات والبيانات الإلكترونية بين الدول لجمع أدلة معينة أو معلومات مهمة، وعدم وجود قواعد بيانات رقمية مشتركة، فعدم وجود نظام الاتصال وقواعد للبيانات المشتركة يسمح بالمساعدة القانونية لاستكمال التحقيق وإجراء التفتيش وضبط الأدلة الرقمية بشكل سريع وسلس، يعني عدم القدرة على التصدي لمثل هذه الجرائم المرتكبة التي تتسع وتتطور باستمرار وتأخذ منحنيات على درجة عالية من التعقيد، وبالتالي إفلات المجرمين من العقاب.

وهنا يرى الباحث بضرورة وضع قواعد قانونية خاصة تنظم "الجانب الإجرائي" في التعامل مع الأدلة الرقمية على مستوى البحث والتحري والضبط والتحريز والتحليل والخبرة اللازمة والحماية الواجبة للدليل الرقمي والمحافظة عليه، وليس فقط الاكتفاء بالنص على مقبوليته في الإثبات الجزائي، ونصوص صريحة تسمح بالتعاون القضائي بين الدول لا سيما إجراءات الولوج إلى أنظمة حاسوب قد تكون موجودة خارج نطاق الدولة، استكمالا لما جاء في توصية المجلس الأوروبي رقم 95/ 13 حتى لا تمثل اعتداء على سيادة الدولة. أي بمعنى أننا بحاجة إلى تنظيم تشريعي "متكامل" في التعامل مع الأدلة الرقمية على المستوى الإجرائي والموضوعي والمساعدة القضائية ويحمي الحقوق والضمانات الدستورية وفي القانون الدولي.

الفصل الثاني

الأدلة الرقمية وضوابطها القانونية

إن وسائل وإجراءات جمع الأدلة الجنائية لإثبات الجرائم قد وردت في مواد قانون الإجراءات الجزائية رقم (3) لسنة 2001[1] وتعديلاته[2]، ولأجل ذلك يعمل المحقق الجنائي على استخدام الطرق المشروعة لجمع وتحليل ما توفر لديه من الأدلة التي يرى أنها ملائمة للكشف عن حقيقة الجريمة، فيجوز له أن يباشر أي إجراء يرى فيه فائدة للإثبات[3].

كما أن استخلاص الدليل الرقمي في الجرائم الإلكترونية الناجمة عن الاستخدام غير المشروع لتقنية الحاسوب والإنترنت من أجل الاعتداء على الحقوق التي يحميها القانون، قد يخلق عدة صعوبات عملية بالنظر إلى خصوصيته التقنية المتطورة وطبيعته الرقمية، بالإضافة إلى الفضاء الواسع والمتاح الذي ترتكب فيه الجريمة، فإن هذه الميزات تجعل من إمكانية إخفاء ومحو آثار الجريمة ممكنة. وهذا ما يؤكد أهمية المعالجة التشريعية الخاصة للجوانب الإجرائية في مجال الأدلة الرقمية وعدم الاكتفاء بالنصوص العامة الواردة في الإجراءات الجزائية، نظراً للطبيعة المتطورة والمعقدة للأدلة الرقمية بالمقارنة مع الأدلة التقليدية وإجراءاتها.

لذلك سوف نبحث في الوسائل الممكنة والمتاحة لاستخلاص الأدلة الرقمية في إثبات الجرائم الإلكترونية التي تمثل ضرباً من ضروب الذكاء الإجرامي الجديد، التي باتت تتخذ أنماطاً جديدة لا يجدي معها إتباع الإجراءات التقليدية، لما تثيره طبيعتها غير المادية من إشكاليات وما تؤديه التقنية الحديثة من دور في ارتكاب ها، وما توفره لها من مسرح غالباً ما يكون أقل إظهاراً للأدلة محل التحقيق، وذلك لوقوعها في عالم افتراضي وبأدلة غير ملموسة، وتعتبر مسألة جمع الأدلة من المسائل الأساسية في تكوين الجريمة وإعادة ملامحها وكيفية حدوثها.

وفي هذا الشأن سنقسم هذا الفصل إلى مبحثين، الأول نناقش فيه القيمة القانونية للأدلة الرقمية في الإثبات، والثاني نخصصه لدراسة دور التشريعات الوطنية والمواثيق الدولية في ضبط الأدلة الرقمية وإثباتها.

---

1. منشور على الصفحة (94) من عدد الوقائع الفلسطينية رقم (38) بتاريخ: 2001/09/05.
2. القرار بقانون رقم (17) لسنة 2014 بشأن تعديل قانون الإجراءات الجزائية رقم (3) لسنة 2001، والقرار بقانون رقم (13) لسنة 2018 بشأن تعديل القرار بقانون رقم (17) لسنة 2014 م بشأن تعديل قانون الإجراءات الجزائية رقم (3) لسنة 2001.
3. مطردي، مفتلح بوبكر (2012)، الجريمة الإلكترونية والتغلب على تحدياتها، مؤتمر رؤساء المحاكم العليا في الدول العربية، السودان، ص52.

المبحث الأول

القيمة القانونية للأدلة الرقمية

تمثل القيمة القانونية للأدلة الرقمية أساسًا للنظام القانوني الحديث، وتشكل تحولًا نوعيًا في طبيعة الأدلة المقدمة للمحكمة، وفيما يتعلق بقيمتها القانونية، فأنها تأتي من قدرتها على إثبات الحقائق والأحداث بشكل دقيق وموثوق، كما أن مجرد وجود دليل جنائي يثبت وقوع الجريمة وينسبها لشخص معين لا يكفي للتعويل عليه لإصدار الحكم بالإدانة، إذ يجب أن يكون لهذا الدليل قيمة قانونية، وهذه القيمة للدليل الجنائي تتوقف على مسألتين رئيستين، الأولى المشروعية، والثانية اليقينية في دلالته على الوقائع المراد إثباتها[1]، مما يوجب إبراز أهم الأسس التي يستند عليها الدليل حتى يكون مشروعاً، وإلى أي درجة من اليقين يجب أن يحققها، وعليه فقد كان لزاماً علينا أن نبين حجية الأدلة الرقمية أمام القاضي الجزائي ومدى مشروعيتها في المطلب الأول، ونستعرض القيود الواردة على حرية القاضي الجزائي قبول الدليل الرقمي.

المطلب الأول

حجية الأدلة الرقمية أمام القاضي الجزائي ومدى مشروعيتها

لما كان الدليل الرقمي يختلف في إثبات الجرائم الإلكترونية عن الأدلة التقليدية، فقد كان لزاماً علينا وقبل أن نبدأ ببسط بحثنا بشأن شرعية الأدلة الرقمية أن نسعى لدراسة مدى حجية هذه الأدلة أمام القاضي الجزائي.

الفرع الأول

حجية الأدلة الرقمية أمام القاضي الجزائي

يعد الأخذ بالدليل الرقمي وأن يكون دليلاً صالحة للحكم من أولى الخطوات التي يستند إليها القاضي وذلك قبل البدء في تقديره وذلك للتأكد من صحته وملاءمته لتحقيق الغاية التي قدم الدليل الرقمي من اجلها، وكي يؤخذ به لا بد ان يستند على أساس قانوني علمي سليم، وهذا الأخير يختلف كمن نظام قانوني إلى آخر، وذلك نظراً لوجود عدة اختلافات بين النظم الإجرائية للإثبات الجنائي، فمنها ما يأخذ بنظام الإثبات الحر، ومنها ما يأخذ بنظام الإثبات المقيد، ومنها ما يأخذ بالنظامين معاً، وسوف نحاول التطرق إلى هذه الأنظمة الإجرائية باختصار على النحو التالي:

[1] الهيتي، محمد حماد (2010)، التحقيق الجنائي والأدلة الجرمية، ط 1، دار المناهج للنشر والتوزيع، عمان، ص22 وما بعدها.

أولاً: الحجية في نظم الإثبات حول الدليل الرقمي

1. **الحجية في نظام الإثبات الحر (النظام اللاتيني):** وقد أخذ بهذا النظام العديد من الدول مثل (فرنسا، الأردن ، مصر، سوريا، لبنان)، ويعتمد هذا النظام على منح القاضي الحرية في تقدير الدليل سواء كانت الأدلة تقليدية أو علمية حديثة كالأدلة الرقمية، وقد أكد المشرع الفرنسي عندما نص في المادة (427) من قانون الإجراءات الفرنسي على ما يلي:" ما لم يرد نص مخالف، يجوز إثبات الجرائم بجميع الطرق ويحكم القاضي بناءً على اقتناعه الشخصي"، وتأكيداً على ذلك قضت محكمة النقض الفرنسية في احد قراراتها بصلاحية القضاء بالأخذ بأشرطة التسجيل الممغنطة والمدمجة، واعتبارها صالحة للتقديم أمامها.[1]

وهنا يثار التساؤل حول التسجيلات الممغنطة والمسجلة الكترونياً (رقمياً) ومدى حجيتها في الإثبات الجنائي ؟

يرى جانب من الفقه أنه من الصعوبة التلاعب بهذه التسجيلات، ويمكن لخبراء الأدلة الرقمية اكتشاف التلاعب فيها إن وجد وبكفاءة فنية وتقنية عالية، وبالتالي فإن التسجيل الممغنط له الحجية الكاملة في الإثبات الجزائي باعتباره من الأدلة التي لا تحتمل الخطأ والتلاعب.[2]

يسود نظام الإثبات الحر في القوانين الإجرائية اللاتينية بحيث يتمتع القاضي بموجب هذا النظام بالحرية المطلقة في إثبات الوقائع المعروضة عليه ولا يلزمه القانون بأدلة معينة للاستناد عليها في تكوين قناعته الشخصية، وإن حجية الدليل الرقمي المتحصل من الموقع الإلكتروني لا تثير أي صعوبات متعلقة بمدى حرية تقديم الأدلة لإثبات الجريمة، ولا بمدى حرية القاضي الجنائي في تقدير هذه الأدلة ذات الطبيعة الخاصة باعتبارها أدلة إثبات في المواد الجنائية أم لا، بل إن العنصر الاساسي وفق هذا المذهب هو مدى حرية قاضي الموضوع في تقدير هذه الأدلة، ومدى قبول هذه الأدلة، كدليل قائم بذاته وكافٍ لإثبات الإدانة أو البراءة[3].

وقد سارت الأخذ بهذا الاتجاه معظم الدول الأوروبية مثل (ألمانيا، اليونان، ودول أمريكا اللاتينية كالبرازيل)، وقد اعتمدت هذه الدول على الأخذ بنظام الإثبات الحر من حيث خضوع

---

1. د. أحمد، هلالي، عبد الإله، (2000)، التزام الشاهد بالإعلام في الجريمة المعلوماتية، دراسة مقارنة، دار النهضة العربية، القاهرة، ص 27.
2. د. عرفة، محمد عبد الحميد (2018)، مدى حجية الأدلة الإلكترونية الرقمية في الإثبات الجنائي – دراسة مقارنة – مجلة كلية الحقوق لبحوث القانونية والاقتصادية، جامعة الإسكندرية، العدد1 ، ص 493 – 513.
3. د . أحمد، هلالي عبد الإله (1997)، حجية المخرجات الكمبيوترية، ط1، دار النهضة العربية، القاهرة، ص 23.

الأدلة الرقمية لسلطان القاضي وقناعته الوجدانية، فله قبول الدليل أو رفضه، سيما إذا وجد أن هذه الأدلة لا تنسجم مع العقل والمنطق ووقائع الدعوى المطروحة عليه.[1]

فالقاضي في هذا النظام يتمتع بدور إيجابي في مجال الإثبات وبالمقابل تقييد دور المشرع، وعليه ففي هذا الاتجاه لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود على اعتبار أن المشرع لم يعهد إليه مهمة تحديد قائمة أدلة الإثبات، فمسألة قبول الأدلة لا ينال منها سوى مدى اقتناع القاضي بها. وفي المقابل، فإن تنظيم الجوانب الإجرائية للأدلة الرقمية يلعب دوراً هاماً في القناعة الوجدانية للقاضي في التعامل مع الأدلة الرقمية وفقاً للخطة التي يرسمها المشرّع للحفاظ على جودة الدليل الرقمي، كما أن مأسسة التعامل مع الأدلة الرقمية ووضوحها هام في مسار جودة الدليل.

2. **الحجية في نظام الإثبات المقيد (إلانجلوسكسوني):** يستند هذا النظام على عدم منح القاضي السلطة التقديرية للدليل مهما كان نوع الدليل تقليدياً أم رقمياً، بمعنى ان القاضي لا يملك حجية الدليل بالمطلق، فالقانون هو الذي يحدد للقاضي ماهية الدليل ونوعه، وقيمته القانونية وحجيته في الإثبات، وخلاصة ذلك أن الدليل لا يكون له القيمة القانونية إلا إذا نص القانون عليه واعتبره ضمن القائمة، فعدم وجود النص يعني انه لا قيمة للدليل، وليس له الحجية في الإثبات الجزائي.[2]

كما يقوم نظام الإثبات المقيد على مبدأ أساسي في أن المشرع الجنائي يحدد سلفاً الوسائل والطرق التي يعتمدها في إقامة الدليل الجنائي على مرتكبي الجرائم، فوفقاً لهذا الاتجاه فإن المشرع هو الذي يحدد الأدلة التي يجوز للقاضي اللجوء إليها ويقدر قيمتها الاقناعية، بحيث يقتصر دور القاضي في هذا النظام على مجرد فحص الدليل والتأكد من توافر الشروط التي حددها القانون، فلا سبيل للاستناد على دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات، كما لا دور للقاضي في تقدير القيمة ألاستدلالية للدليل، حيث أن القانون يقيد القاضي بقائمة الأدلة التي حددت قيمتها الإثباتية[3].

ومن الدول التي أخذت بهذا النظام بريطانيا، حيث حدد المشرع البريطاني أدلة الإثبات في قانون الشرطة والإثبات الجنائي الصادر عام 1984م، متناولاً المشرع البريطاني في هذا القانون أدلة الإثبات في القضايا الجنائية بصورة دقيقة، سيما أن المشرع لم يمنح القاضي صلاحية تقدير الدليل من حيث قبوله أو رفضه، وقد سارت على نهج الأخذ بنظام الإثبات المقيد العديد من الدول

---

1. د. فتوح الشاذلي، عفيف كامل، (2003)، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة – منشورات الحلبي الحقوقية، بيروت، ص 373 وما بعدها.
2. د. عرفة، محمد عبد الحميد ، مرجع سابق، ص 513.
3. د. أحمد، هلالي عبد الإله، مرجع سابق، ص22.

كالولايات المتحدة الأمريكية، وكندا، وفي أمريكا صدر قانون الحاسب الآلي عام 1984م، متمخضاً عنه اعتبار مخرجات الحاسوب الإلكترونية أدلة لها قيمتها وحجيتها القانونية.[1]

3. **الحجية في نظام الإثبات المختلط:** أخذ هذا النظام بالجمع بين النظام اللاتيني والانجلوسكسوني، بمعنى أن نظام الإثبات المختلط منح القاضي السلطة التقديرية لقبول الدليل في بعض أدلة الإثبات الرقمية.

وفي أدلة أخرى لم يكن له إلا الالتزام بالنص القانوني والذي يحدد القيمة والحجية للدليل هو القانون وليس القاضي، ففي بعض الدول كاليابان التي أخذت بنظام الإثبات المختلط اعتبرت أن الأدلة الجنائية التقليدية (كالشهادة، وأقوال المتهم، والقرائن، والخبرة)، هي أدلة قانونية، وليس للقاضي سلطة تقديرية فيها، لان القانون هو الذي يمنح هذه الأدلة والحجة القانونية، بينما استقر الفقه الجنائي الياباني على أن الأدلة الإلكترونية تخضع للسلطة التقديرية للقاضي، فمثلاً: المجالات الالكترومغناطيسية إذا كانت غير ملموسة أو مرئية لا تعد دليلاً يستند عليه القاضي المختص، أما إذا تحولت المجالات الالكترومغناطيسية إلى أدلة مقروءة ومرئية فيمكن اعتبارها دليلاً في الإثبات الجنائي، وهذه تخضع للسلطة التقديرية للقاضي بحكم طبيعة الدليل ووقائع الدعوى.[2]

يقوم النظام المختلط على أساس الجمع بين خصائص النظام المختلط ونظام الإثبات الحر، إذ يعتمد أساساً أن القانون يحدد أدلة معينة لإثبات وقائع دون بعضها الآخر، وقد يحدد قبول الدليل بشروط معينة في بعض الحالات، كما يعطي للقاضي الحرية في تقدير الأدلة القانونية على غرار القانون الفلسطيني فقد نصت المادة (1/206) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 وتعديلاته على أنه" تقام البينة في الدعاوى الجزائية بجميع طرق الإثبات ، إلا إذا نص القانون على طريقة معينة للإثبات .."[3].

---

[1]. د. عرفة، محمد عبد الحميد ، مرجع سابق، ص 490.

[2]. د. عبد الفتاح بيومي حجازي، (2007)، الإثبات في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ص 46.

[3]وفي ذلك تقول محكمة النقض الفلسطينية بأنه: "أما عن أسباب الطعن في مجملها نجد أنها بنيت على أن المحكمة أخطأت في تطبيق القانون وعدم بناء حكمها على الخبرة الفنية. ولما كانت البينة من طرق الإثبات الجزائي في الدعوى أن المادة 206 من قانون الإجراءات الجزائية رقم 3 لسنة 2001 تفيد ((1/206 تقام البينة في الدعاوى الجزائية بجميع طرق الإثبات إلا إذا نص القانون على طريقة معينة للإثبات)). خاصة وأن الأدلة في الدعوى الجزائية تخضع لمبدأ القناعة الوجدانية للمحكمة، ومحكمة الاستئناف كمحكمة موضوع لها صلاحية وزن البينة حيث أن القاعدة في الأحكام الجزائية وجوب اشتمالها على الأدلة والأسباب الموجبة للتجريم أي استظهار أركان الجريمة وعناصرها وفقاً للتعريف الذي نص عليه القانون، ولمحكمة الموضوع الصلاحية في الأخذ بما تقتنع به من البينة المقدمة والخبرة من عداد البينات وهي مسألة موضوعية يترخص قاضي الموضوع بتقديرها وما دام أن محكمة الموضوع لم ترى جدوى بإحداث خبرة خلاف من ثم سماع شهادته كخبير في الدعوى وهو موظف البنك بكر العمري فأنها تكون قد استعملت خيارها في هذه المسألة ما دام أنها ثبتت حكمها على الوقائع الثابتة في الدعوى والمستمدة من الأدلة المقدمة إليها والتي عالجت هذه الواقعة محكمة الاستئناف أيضاً كما أن هذا لم يكن مدار طعن أمام محكمة الاستئناف مما يجعل من هذه الأسباب أسباباً جديدة لا يستقيم طرحها أمام محكمة النقض مما يستوجب ردها"، حكم محكمة النقض الفلسطينية المنعقدة في رام الله في الدعوى الجزائية رقم 77 لسنة 2016 بتاريخ 2016/04/04. وقضت محكمة النقض الفلسطينية في حكم أخر بأنه: "ترى هذه المحكمة أن المحكمة الإستئنافية حينما عدلت حكم محكمة أول درجة وأدانت الطاعن بالتهمة الأولى المسندة إليه قد أعملت وظيفتها الأساسية وهي إعادة النظر في الحكم المستأنف

ثانياً: شرعية الأدلة الرقمية

أصبحت الأدلة الرقمية ذات أهمية كبيرة في ميدان القضاء الجنائي، حيث تشكل عنصراً أساسياً يسهم في توجيه القرارات القانونية أمام القاضي. ما يجعل التحكيم في هذه الأدلة يتطلب فهمًا دقيقًا للطرق والمعايير التي تحكم قبولها واستخدامها في عملية اتخاذ القرارات القانونية. وكنتيجة لتسارع التكنولوجيا بشكل كبير، توسع نطاق الأدلة الرقمية لتشمل مجموعة واسعة من المعلومات، مثل البيانات الإلكترونية، سجلات الاتصالات، وملفات الوسائط المتعددة. ونتيجة لذلك ظهر تحدي اكبر أمام القضاء الجنائي في تحديد مدى حجيتها وقبولها أمام المحكمة؛ بالتالي يجب على القاضي الجنائي أن يكون على دراية بأساليب جمع وتحليل الأدلة الرقمية، وكذلك فهم التقنيات المستخدمة في إنتاج هذه الأدلة، كما ينبغي أن يكون لديه إطلاع على المعايير القانونية المتعلقة بحجية الأدلة الرقمية وكيفية تقييمها.

من المهم أيضا التأكيد على ضرورة احترام حقوق الأفراد خلال جمع واستخدام الأدلة الرقمية، مع مراعاة القوانين والمعايير الدولية ذات الصلة. يتعين على القاضي أن يكون حذرًا في التعامل مع هذه الأدلة لضمان نزاهة العملية القانونية والحفاظ على حقوق الأطراف المعنية.

- **مشروعية الأدلة الرقمية**

يقصد بمشروعية الأدلة الرقمية ضرورة اتفاق الإجراء مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر، فقاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع، بل يجب مراعاة إعلانات حقوق الإنسان والمواثيق الدولية، وكذلك قواعد النظام العام وحسن الآداب السائدة في المجتمع، والمبادئ التي محكمة النقض.[1]

وقد نص القانون الاساسي الفلسطيني في المادة (10) على ضمان احترام حقوق الإنسان وحرياته "حقوق الإنسان وحرياته الأساسية ملزمة وواجبة الاحترام"،[2]ونص في البند الثاني من

من الناحيتين القانونية والموضوعية وأعملت صلاحيتها في الرقابة على محكمة أول درجة في تقدير الشهود وأنزلت صحيح حكم القانون والسوابق القضائية بالنسبة للبينة التي ساقتها النيابة العامة ذلك أنه من المقرر قانوناً في المواد الجزائية جواز إثباتها بكافة طرق الإثبات المقررة ما لم ينص القانون على غير ذلك (م 206 من قانون الإجراءات الجزائية رقم 3 لسنة 2001) وأن من ضمن هذه الطرق حسبما نصت عليه المواد106 ،108 ،109 من قانون البينات رقم 4 لسنة 2001 القرائن القضائية كما أن ما استقر عليه قضاء هذه المحكمة من أن البينة الظرفية كافية لإثبات التهمة قبل فاعلها الأمر الذي يكون معه النعي على الحكم المطعون فيه بمخالفته للقانون على غير أساس متعيناً رفضه أما عن النعي على الحكم بإجحافه بحقوق الطاعن فإن هذا النعي مردود كذلك لكون هذا السبب ليس من الأسباب الموجبة للطعن بالنقض طبقاً لنص المادة 251 من قانون الإجراءات الجنائية الأمر الذي يتعين معه رفض الطعن"، حكم محكمة النقض الفلسطينية المنعقدة في غزة في الدعوى الجزائية رقم 205 لسنة 2003 بتاريخ 2005/10/25.

[1]. هلالي احمد، حجية المواد الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2008، ص 118.

[2]. المادة (10) من القانون الاساسي الفلسطيني لسنة 2005 .

ذات النص الدستوري على وجوب أن "تعمل السلطة الوطنية الفلسطينية دون إبطاء على الانضمام إلى الإعلانات والمواثيق الإقليمية والدولية التي تحمي حقوق الإنسان".

كما ونصت المادة (17) من القانون الأساسي على أنه " للمساكن حرمة، فلا تجوز مراقبتها أو دخولها أو تفتيشها إلا بأمر قضائي مسبب ووفقاً لأحكام القانون. يقع باطلاً كل ما يترتب على مخالفة أحكام هذه المادة، ولمن تضرر من جراء ذلك الحق في تعويض عادل تضمنه السلطة الوطنية الفلسطينية".[1]

فيما أكدت المادة (32) من القانون الأساسي على أن "كل اعتداء على أي من الحريات الشخصية أو حرمة الحياة الخاصة للإنسان وغيرها من الحقوق والحريات العامة التي يكفلها القانون الأساسي أو القانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم وتضمن السلطة الوطنية تعويضاً عادلاً لمن وقع عليه الضرر".

ما يعني ان انتهاك الحقوق والضمانات الدستورية في التعامل مع الأدلة الرقمية في الممارسات العملية يشكل "جريمة دستورية" موصوفة بموجب القانون الأساسي المعدل (الدستور) علاوة على انتهاكها للاتفاقيات الأساسية لحقوق الإنسان التي انضمت إليها دولة فلسطين بدون تحفظات وللمعايير الدولية ذات الصلة.

وكذلك فقد نصت المادة (273) من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 "تحكم المحكمة في الدعوى حسب قناعتها التي تكون لديها بكامل حريتها، ولا يجوز لها أن تبني حكمها على أي دليل لم يطرح أمامها في الجلسة أو تم التوصل إليه بطريق غير مشروع"،[2] وبالتالي فقد منع القانون أي مساس بالحقوق والحريات الخاصة بالأفراد سواء من خلال القبض أو التفتيش أو التوقيف إلا بأمر قضائي، وأوجب عقوبات على خلاف ذلك.

ولحسن تطبيق مبدأ الشرعية الجنائية على الجرائم فإنه يتوجب على القاضي احترام مبدأ الشرعية الإجرائية، أو ما يعرف بشرعية الدليل الجنائي، فلا يسوغ له بناء حكمه على دليل جنائي غير شرعي، أو تحصل عليه المحقق بطرق غير شرعية، حتى يكتسي الدليل القضائي الحجية في إسناد واقعة الاتهام إلى المتهم أو نفيها عنه.

وانطلاقاً من مبدأ ضرورة أن يكون القضاء نزيهاً فإنه يتوجب عليه أن يبني أحكامه وقراراته على أدلة مشروعة، إذ يشترط في الدليل الجنائي عموماً لقبوله كدليل إثبات أن يتم الحصول عليه بطرق مشروعة، وذلك يقتضي أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي

---

1. المادة (17) من القانون الاساسي الفلسطيني لسنة 2005. .
2. المادة (273) من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

يحددها القانون. كما أن الحديث عن مدى مشروعية الدليل الرقمي يجرنا حتماً للحديث عن مدى مشروعية طرق ووسائل الحصول عليه، مثل اللجوء إلى ممارسة إجراءات التفتيش في مختلف الوسائط التقنية الرقمية والوسط الافتراضي، الذي استعملت في الجريمة الإلكترونية، بالإضافة إلى أن هذا الإجراء ينبغي أن يمارس من سلطة التحقيق المختصة، وهي النيابة العامة[1]. علماً أن الرقابة القضائية على أداء النيابة العامة وإجراءاتها معيار أساسي للحكم على مشروعية الإجراءات وفقاً لما تؤكده المبادئ الدولية لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات لسنة 2013.

إن مجرد الحصول على الدليل الرقمي وتقديمه أمام القضاء لا يكفي لاعتماده كدليل للإدانة، إذ أن الطبيعة الفنية الخاصة لهذا الأخير يمكن العبث بمضمونها على نحو يحرف الحقيقة، فضلاً عن ذلك فإن نسبة الخطأ في إجراءات الحصول على الدليل للوصول إلى الحقيقة عالية في مثل هذا النوع من الأدلة، ولذلك تثور فكرة الشك في مصداقيتها كأدلة إثبات جنائي.

وفي ظل النظم القانونية التي تعتمد النظام اللاتيني فإن للقاضي السلطة الواسعة في تقييم الدليل من حيث قيمته التدليلية، فله أن يقبل بالدليل أو أن يرفضه، وهو يعتمد في ذلك على مدى اقتناعه الشخصي، وبذلك يكون للقاضي في هذا النظام أن يستعمل سلطته في تقرير الدليل، بحيث تمتد لتشمل الأدلة العلمية، لأن هذه الأخيرة لها قيمتها الاستدلالية في الإثبات ، قد تصل إلى درجة اليقين كالأدلة العلمية.

فالدليل الرقمي - من حيث تدليله على الوقائع- تتوفر فيه شروط اليقين، مما لا يمكن قبول ممارسة القاضي لسلطته في التأكد من ثبوت تلك الوقائع أو نفيها، ولكن هذا لا يناقض القول بأن هذا الدليل موضع شك من حيث سلامته والعبث به وصحة الإجراءات المتبعة للحصول عليه، بحيث يمكن أن يثار الشك في سلامة الدليل الرقمي لسببين اثنين[2]، نذكرهما فيما يلي:

- إمكانية العبث بالدليل على نحو يصبح مخالفاً للحقيقة، ومن ثمة يكون هذا الدليل معبراً عن واقعة معينة صنعت أساساً لأجل التعبير عنها خلافاً للحقيقة، وذلك دون أن يكون لغير الخبراء في هذا المجال إدراك هذا التحريف أو التدمير الذي لحق بتلك الأدلة.
- كما أن احتمال حدوث الخطأ الفني في جمع وتحليل الدليل الرقمي ممكن جداً، بالنظر إلى الأجهزة المعقدة التي تستعمل في ارتكاب الجريمة.

[1]. سرور، احمد فتحي (1981)، الوسيط في قانون الإجراءات الجنائية، ط4، المجلد الأول، دار النهضة العربية، القاهرة، ص506.
[2]أحمد، هلالي عبد الإله، المرجع السابق، ص43.

- **شرعية الأدلة الرقمية**

فيما يتعلق بمبدأ "مشروعية الدليل الجنائي الإلكتروني"، يقصد به قبول الأدلة الرقمية في النظام القانوني والشروط التي يجب أن تتوافر لجعل هذه الأدلة مقبولة أمام القضاء. لقبول الدليل الرقمي يشترط أن يتم الحصول عليه بطرق مشروعة، مع احترام القواعد والإجراءات الموضوعية والشكلية المحددة قانونًا. وعدم الامتثال لهذه القواعد يؤدي إلى عدم مقبولية الدليل وبالتالي لا يمكن استخدامه لدعم حكم قضائي بالإدانة أو البراءة[1].

بمعنى أخر، مشروعية وجود الدليل الرقمي تعتمد على اعتراف المشرع به كجزء من الأدلة الجنائية، حيث يُسمح للقاضي باستخدامه للوصول إلى قناعته بالإدانة . يختلف موقف التشريعات حول مشروعية الدليل الرقمي بحسب طبيعة النظام القانوني، حيث يتنوع بين نظام الإثبات المحدد الذي يُحدد المشرع فيه الأدلة المسموح استخدامها، ونظام الإثبات الحر الذي يتيح للقاضي حرية التقرير بناءً على أي دليل يراه مناسباً للوصول إلى الحقيقة، دون الحاجة إلى تحديد أدلة محددة في القانون، وهناك أيضا نظام الإثبات المختلط هو وسط بين النظامين، حيث يوفر وسائل محددة للاستناد إليها في تأسيس حكم القاضي، مما يعالج المخاوف المتعلقة بتعسف القاضي في الإثبات[2].

اعتمد القضاء الجنائي الفلسطيني نظام الإثبات الحر، إذ يُتاح للقاضي، وفقًا لقناعته الشخصية والوجدانية، اعتماد أي وسيلة من الوسائل التي يُطرحها أمامه، شريطة أن يكون قد تم التحصل عليها بطريقة قانونية. في هذا السياق يتم التشديد على أهمية احترام الإجراءات القانونية في جمع الأدلة، مع التأكيد على أن عدم الامتثال لمبدأ المشروعية يمكن أن يعتبر عملية التفتيش أو وسيلة الضبط للدليل باطلة. كما يتيح هذا النظام للقاضي التحقق من الأدلة بمرونة وفقًا لتقديره الشخصي، ولكن يتعين على النظام القانوني ضبط هذا التحقق وفقًا للمعايير القانونية وضمان احترام حقوق الأفراد. من خلال هذا النهج، يُشدد على أهمية الشرعية ولامتثال للقوانين في جمع الأدلة، مما يعزز مبدأ العدالة ويحفظ حقوق الأفراد خلال الإجراءات الجنائية[3].

وجود دليل يثبت وقوع الجريمة الرقمية لا يكفي بمفرده للاعتماد عليه وإصدار حكم بالإدانة . يتعين على هذا الدليل أن يحمل قيمة قانونية، تمامًا كما هو الحال مع الأدلة الأخرى، حيث يعتمد ذلك على مدى توافر شروط الإثبات الجنائي. إضافة إلى ذلك، يجب أن تلتزم إجراءات الحصول

---

[1]. بن عزة، أسامة، (2018 – 2019)، سلطة القاضي الجنائي في تقدير الدليل الإلكتروني، رسالة ماجستير، جامعة العربي التبسي- تبسة، الجزائر، ص41-42

[2]. بوبعاية، ابتسام (2021 – 2022)، التحقيق في الجريمة الإلكترونية، رسالة ماجستير، جامعة محمد البشير الإبراهيمي – برج بوعريريج، الجزائر، ص 56.

[3] أحمد حمو، علاء عواد، ولاء عبد الله (2015)، الأدلة الإلكترونية (الجوانب القانونية والتقنية)، أوراق بحثية في القانون ومكافحة الفساد، جامعة بيرزيت- معهد الحقوق، ، ص39 -40.

على الأدلة الرقمية بحقوق الإنسان والمواثيق الدولية، بالإضافة إلى النظام العام والأخلاق العامة في المجتمع. وينبغي أن تتوافق هذه الإجراءات مع ما استقرت عليه محكمة النقض الفلسطينية في قراراتها[1].

بمعنى أخر، لا يقتصر التحقق من الدليل الرقمي على مجرد التأكد من وقوع الجريمة، بل يجب أيضا التحقق من مدى صحة وقانونية ذاك الدليل. حيث يجب أن تتم جمع الأدلة الرقمية واستخراجها بما تشترطه المعايير القانونية لجمع الأدلة مع ضرورة احترام حقوق الأفراد، وهو يضمن عدم انتهاك حقوق الأفراد في عمليات الجمع والتحليل ويعزز النزاهة والعدالة في النظام القضائي.

إن مشروعية الدليل تستند على هدفين قانونيين أساسيين. الهدف الأول هو الحفاظ على نزاهة وسير الإجراءات الجزائية، مع التأكيد على التزامها بالمعايير والقواعد القانونية. يهدف ذلك إلى ضمان أن تتم العمليات القانونية بشكل عادل وفقًا للقوانين واللوائح. الهدف الثاني هو حماية حقوق الأفراد والحريات الفردية، مع التركيز على ضمان توازن عدالة العقوبات بين الأطراف المتنازع عليها. وبناءً على ذلك، يأخذ مبدأ المشروعية دورًا حيويًا في ضمان التوازن بين مصلحة المجتمع وحقوق الفرد، مما يسهم في حماية الحقوق وتحقيق التناغم بين المصلحتين وفقًا للأحكام القانونية[2].

- **يقينية الدليل الرقمي**

اليقين يعبر عن درجة عالية من الاقتناع بالحقيقة دون وجود شك أو تردد. وفي سياق الأدلة الجنائية الرقمية، فإنه يشير إلى مستوى التأكد العالي من صحة أو دقة الأدلة المقدمة لدعم حالة معينة، وهذا يعني أن هناك تأكيد قوي وقاطع بأن الأدلة تشير بوضوح إلى وجود جريمة معينة أو مسؤولية شخص معين. يعتمد اليقين على تحليل الأدلة الرقمية والقوة الاستدلالية لها ومدى قدرتها على إثبات الجريمة بشكل مؤكد، وإلا فإن الشك يبقى قائمًا، ولا يمكن الحكم بالإدانة بناءً على تلك الأدلة. وعليه لضمان اليقين في الأدلة الجنائية الرقمية، يتعين تطبيق قواعد وإجراءات من قبل

1. شهاب، أحمد عبد الحكيم، د. بن مارني نور عزم الميل (2018)، شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني، مجلة العلوم السياسية والقانون- العدد 07 فبراير2018، المجلد02، المركز الديمقراطي العربي ألمانيا- برلين، ص 128-130

2 بقدار، عبد القادر كامل ، عبد السلام، محمد نور الدين (2017)، أثر مبدأ المشروعية في حجية الدليل الجزائي في القانون الجزائري، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 14 ، العدد 1، ص269-272

المختصين في تقييم سلامة الدليل الجنائي الرقمي وضمان عدم تلاعبه أو تزويره، وأن يتم استخراجه واستخدامه بطريقة تلبي المعايير التقنية والقانونية المحددة[1].

يعد مبدأ اليقين أساسيًا في القضاء، لكنه يتسم بالنسبية، حيث يمكن أن يتغير تفسيره وتطبيقه باختلاف القضاة عند مواجهتهم لنفس القضية. ينبع هذا التباين من اختلاف الشخصيات والتجارب والقيم بين القضاة، الأمر الذي يؤدي إلى تباين في طريقة فهمهم وتقديرهم للحقائق والأدلة واختلاف مدى اليقين في قراراتهم. فمبدأ اليقين يعتمد بشكل كبير على كيفية تفاعل الوقائع مع شخصية القاضي.

في ظل التطورات الحديثة، خاصة في مجال تكنولوجيا المعلومات والجرائم الإلكترونية، تزداد التحديات التي يواجهها القضاة، إذ أن هذه التقنيات يمكن أن يؤثر بشكل كبير في قدرته على فهم وتقدير الأمور التقنية؛ هذا قد يؤثر سلبًا على درجة اليقين في قراراته، وهي ما تعد تحديًا كبيرًا للقضاة، ليجدون أنفسهم أمام صعوبة في التكيف مع هذه التقنيات الجديدة وفهم الأمور التقنية، ما قد يؤثر سلبًا على قدرتهم على تقدير الأدلة واتخاذ قرارات قائمة على مبدأ اليقين[2].

وهنا يرى الباحث أن التوازن بين مبدأ اليقين والتطورات التكنولوجية تعبر عن تحديات حديثة يواجهها القضاء، ويتطلب من القضاة تطوير قدراتهم لفهم التقنيات الحديثة وضمان استمرارية تحقيق اليقين في قراراتهم.

عندما يتعلق الأمر بالدليل الإلكتروني، يُعتبر استخدامه نموذجًا للدليل العلمي، إذ يبرز بقوة إثباتيه ويتسم بالموضوعية والحياد والكفاءة. يتبع هذا الدليل قواعد علمية صارمة تستبعد التأويل، مما يزيد من القناعة به، ويسهم في تقليل الأخطاء وتحقيق الحقيقة. ورغم أن الدليل الإلكتروني قد يثير الشك بسبب احتمالية التلاعب أو التزوير، يعتمد تحقيق اليقين على سلامته من التلاعب وصحة الإجراءات المستخدمة في الحصول عليه. يمكن أن يكون الدليل الإلكتروني عرضة للشك بسبب إمكانية التلاعب به لتحريف الحقيقة بسهولة، وخطأ في الحصول عليه أو استنتاجات غير صحيحة بسبب خلل في الأدوات المستخدمة. يتطلب تحقيق اليقين بالدليل الإلكتروني تقييمه باستخدام أدوات فنية خاصة للتأكد من سلامته وصحة الإجراءات المستخدمة للحصول عليه. يعتمد هذا التقييم على

---

1. المطلب، طاهري عبد ، مرجع سابق، ص51-54.

2 موقع محاماة نت، بحث قانوني حول يقينية الدليل الرقمي كقيد للقاضي الجنائي، مقالة منشورة، تاريخ النشر: 2023/05/24، تاريخ الاطلاع: 2023/11/13، ساعة الاطلاع: 14:50.

الشروط الفنية لضمان قبوله كدليل موثوق به في المحاكم[1]، وهو ما سيتم التطرق إليه في المبحث التالي.

تقييم اليقين في الأدلة الجنائية الرقمية يشكل جانبًا حيويًا لضمان قوة الإدانة والعدالة في النظام القضائي. هذا الأمر، يتطلب عملية تحليل دقيقة للأدلة الرقمية والتحقق من سلامتها وصحة الإجراءات المتبعة في استخراجها. يتمثل اليقين في مدى قدرة قاضي المسائل الرقمية على فهم وتقييم الأدلة المقدمة، وضمان تأثيرها الاستدلالي وتوافقها مع معايير اليقين.

يمكن تحديد القواعد التي تحكم مبدأ اليقينية فيما يتعلق بالأدلة الرقمية، إذ تتعلق بشرطين أساسين، أولهما هو تقييم الدليل الجنائي الرقمي من حيث سلامته من العبث، إذ تكمن أهمية صلاحية الأدلة الجنائية الرقمية وسلامتها من التلاعب في التحقيقات الجنائية. يتطلب ذلك التأكد من موثوقية الأدلة واستخدام عمليات مثل التحليل التناظري الرقمي لمقارنة النسخ المستخرجة بالأصل. في حالة عدم توفر النسخة الأصلية أو التلاعب بها، يُستخدم الحساب الرقمي للتحقق من سلامة الأدلة وتجنب التلاعب. يُعزز اللجوء إلى الدليل الرقمي المحايد فحص السلامة بشكل مستقل. يُنصح بالحفاظ على الدليل الجنائي الرقمي الأصلي واستخدام النسخ المتطابقة لتجنب أي تلاعب أو إتلاف محتمل. أما الشرط الثاني فيتمثل بتقييم الدليل الجنائي الرقمي من حيث السلامة الفنية لإجراءات استخلاصه، إذ خلال سير عملية الحصول على الأدلة الجنائية الرقمية باستخدام سلسلة من الأساليب والإجراءات التقنية، قد تظهر أخطاء قد تثير الشك حول مدى سلامة النتائج المحققة. لهذا، يتطلب الأمر اعتماد اختبارات محددة كوسيلة للتحقق من سلامة الإجراءات المتبعة في عملية الحصول على الأدلة الجنائية الرقمية، مما يتيح تقديم ضمانات إضافية بشأن صحة النتائج وتأكيد جودة العملية الفنية المستخدمة، وبالتالي تعزيز الثقة في الأدلة المستخدمة أمام القضاء[2].

لتحقيق اليقين، يعتمد القاضي على استخدام خوارزميات التحليل التناظري والدين الرقمي المحايدة. وهو ما يتطلب التركيز على أهمية الحفاظ على النسخ الأصلية للأدلة وتجنب التلاعب بها، مما يمكن من تقييم السلامة الفنية لإجراءات استخراج الأدلة والتحقق من صحتها. من خلال استخدام الأدوات الفنية المعتمدة، يمكن بناءً على ذلك تعزيز مصداقية الأدلة الرقمية أمام القضاء. كما يعتبر التحقق من السلامة الفنية لعمليات استخراج الأدلة واستخدام الأدوات الفنية المتقدمة في تلك العملية،

[1] مرجع سابق، بن عزة أسامة، ص 42-44

[2] . أوساسي، فؤاد (2019-2020)، دور الدليل الرقمي في الإثبات الجنائي، رسالة ماجستير، جامعة زيان عاشور- الزلفة، ص41-42.

خطوة مهمة وذات تأثير في التأكيد على صحة الأدلة الرقمية وجعلها قاعدة قوية للإدانة. هذا الأمر يعطي قوة ثبوتية ومكانة للأدلة الرقمية كأداة قانونية قوية وموثوقة في سياق القضاء الرقمي[1].

- **الاقتناع اليقيني والجازم بالدليل الرقمي كما يراها المشرع الفلسطيني في المادة 57 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته.**

إن ومبدأ القناعة الوجدانية يخول القاضي الجزائي حرية كاملة وسلطة واسعة في تقدير الأدلة التي تطرح أمامه في الدعوى، بما فيها الأدلة الرقمية، واستخلاص اقتناعه من هذا الدليل أو ذاك، وبأية وسيلة يراها موصلة إلى الحقيقة، شرط ان يصدر القاضي حكمه عن اقتناع يقيني بالأدلة، وبخاصة الأدلة المتحصلة من الحاسب الآلي ومخرجاته الإلكترونية، فسلطة القاضي الجزائي في تقدير الأدلة مقيدة بضرورة أن يؤسس قناعته على أدلة قاطعة وحاسمة، لأن الأحكام الجزائية لا تبنى على الشك والتخمين بل على الجزم واليقين،[2] والوصول إلى يقينية الدليل الرقمي يتم عن طريق ما يستنتجه القاضي بمختلف وسائل إدراكه من خلال معاينته لهذا الدليل، وما ينطبع في ذهنه من تصورات ذات درجة عالية من التوكيد عن طريق التحليل والاستنتاج والربط بين الواقع.[3]

وإذ كانت سلطة القاضي الجزائي في تقدير الدليل تتسع لتشمل الأدلة العلمية، إلا أن تطور العلوم وتشعب فروعها ومقتضيات المنطق والعقل والعدالة توجب على القاضي، (وهو ذو تكوين قانوني غير قادر على إدراك الحقائق المتعلقة بأصالة الدليل الرقمي)، أن يؤسس اقتناعه بالدليل الرقمي على رأي الخبرة الفنية في هذا المجال،[4] فيجعل من هذا الرأي سنداً له في تمتع الدليل الرقمي بقيمة اثباتية قد تصل إلى حد اليقين، فتحديد القيمة العلمية للدليل أمر لا يملك القاضي أية سلطة في تقديرها، لأنها حقيقة ثابتة، وليس من اختصاصه مناقشة الأمور العلمية البحتة، وإنما هي من اختصاص ذوي الخبرة في هذا الشأن،[5] وليس للمحكمة الجزائية أن تبت فيها من تلقاء ذاتها، كما أنها لا تستطيع أن

---

[1] مرجع سابق، طاهري عبد المطلب، ص51-54.

[2] هذا ما أكدت عليه محكمة النقض السورية في العددي من أحكامها، إذ تقول " إن القضاء مؤسسة مهمتها الحكم بالعدل والقسط، ولا يكون ذلك إلا بالعمل على إبراز الوقائع واضحة جلية لا لبس فيها ولا غموض،تدعمها أدلة قاطعة وحاسمة لا يتطرق إليها الشك والشبهة، ولا يلتبس فيها الاحتمال، وكل دليل يحمل في طياته شكاً أو شبهة أو احتمالا يجب أن يكون مصيره الإهمال، لان في ذلك فقط يسود الحق ويقوم العدل"، نقض في 1968/5/23، مجموعة القواعد القانونية، رقم 15، ص 14، ونقض سوري في 1964/4/26، مجموعة القواعد القانونية، رقم 13، ص 12.

[3] زغلول، طارق احمد ماهر (2016)، شرح قانون الإجراءات الجزائية العماني، الجزء الثاني، المحاكمة وطرق الطعن في الأحكام، الطبعة الأولى، دار الكتاب الجامعي، ص 222.

[4] الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، بحث منشور على موقع كلية القانون، جامعة كربلاء، ص 29.

[5] هذا ما استقر عليه الاجتهاد القضائي، انظر قرار محكمة النقض السوري في 1964/11/31، مجموعة القواعد القانونية، رقم 52، ص 31، وفي 1967/11/12، رقم 53، ص 31، ونقض سوري في 1977/6/22، مجموعة المحامون، س 42، رقك 759، ص 583، ونص مصري في 1973/5/23، مجموعة أحكام النقض، س 23، ق 26، ص 97، وفي 1984/11/25، مجموعة أحكام النقض، س 35، ق 185، ص 821.

تحل نفسها محل الخبير الفني في المسائل الفنية البحتة، وعليها الاستعانة بخبير تخضع خبرته ورأيه لتقديرها.

أما بالنسبة إلى الظروف والملابسات التي وجد فيها الدليل، فالقاضي الجزائي يستطيع أن يرفض هذا الدليل إذا تبين له إن وجوده لا يتناسب منطقياً مع ظروف الواقعة، لان القاضي يتمتع بسلطة تقدير الأدلة، والتحقق من سلامة إجراءات الحصول عليها ومشروعيتها.[1]

وبالرجوع إلى المادة (37) من القرار بقانون رقم 10 لسنة 2018 بشأن مكافحة الجريمة الإلكترونية حيث يتبادر للذهن التساؤل التالي: هل يجوز للقاضي الجزائي أن يبني حكم الإدانة على المتهم بارتكابه جريمة الكترونية بناءً على أدلة تقليدية أي إن يقوم بربط المتهم بالتهمة المسندة إليه دون الاعتماد على الأدلة الرقمية سواء كان السبب عدم توافر أدلة رقمية أو انه قام باستبعاد الدليل الرقمي من وزن البينة المقدمة..؟

لا يمكن ربط المتهم بالتهمة المسندة إليه دون الاعتماد على الأدلة الرقمية، إذ بالنظر إلى طبيعة هذه التهمة فإن عدم وجود أدلة رقمية وفنية يُبقي الشك حول قيام المتهم بالجريمة الإلكترونية قائما، ولا يمكن بدون الأدلة الرقمية والفنية التيقن من ربط المتهم بالتهمة المسندة إليه، لاحتمالية اختراق حساب المستدعي مثلا أو استعماله من شخص أخر أو غيرها من الشكوك التي لا تزول إلا بوجود دليل رقمي مقنع يمكن من خلاله التيقن من قيام المتهم بالركن المادي للجريمة الإلكترونية، لذلك اعتبرت المادة 37 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية الدليل الناتج بأي وسيلة تكنولوجية من أدلة الإثبات ، لأن طبيعة هذه الجرائم لا يمكن التيقن من وقوعها من قبل الشخص المتهم وإزالة الشكوك حول قيامه بها إلا بهذه الأدلة، وإن إدانة المتهم دون وجود هذه الأدلة يعني إدانته بالتهمة المسندة إليه والشك ما زال قائما حول قيامه بها، وهو ما يعتبر خروجا عن القاعدة القاضية بأن الشك يفسر لمصلحة المتهم.

ويشترط في الدليل الرقمي أن يتمتع بالمصداقية الكافية بحيث يؤدي فعلا إلى الوصول إلى الحقيقة التي يفترض بالقاضي الجزائي أنه يسعى إليها، ويكون كذلك عندما يكون هذا الدليل مشروعا، بحيث يتم الحصول عليه بطريقة مشروعة وفقا لأحكام القانون، وأن يكون يقينيا بحيث يدلل فعلا على الوقائع المراد إثباتها، فإن تخلف أي من هذين الشرطين فإن الدليل الرقمي تنتفي عنه صفة المصداقية، ولا يصلح عندها الاعتماد عليه كدليل لإثبات الجريمة الإلكترونية ويبقى الشك حول قيام المتهم بالجريمة قائما.

---

1. د. العمر، احمد محمد (2020)، الدليل الرقمي وحجيته في الإثبات ، مجلة الدراسات الفقهية والقانونية، المعهد العالي للقضاء، العدد الثالث، ص 164.

ويفترض عند إثبات الجريمة الإلكترونية كما هو الحال في أية جريمة أخرى أن يتم إثبات عناصر هذه الجريمة بشكل يقيني من خلال الأدلة الرقمية، لاسيما الركن المادي للجريمة بكافة عناصره، فيجب إثبات السلوك والنتيجة والعلاقة السببية بين السلوك والنتيجة.

والدليل الرقمي كغيره من وسائل الإثبات يجب أن يكون خاضعا للنقاش أمام القضاء، وذلك ليصار إلى تحقق القاضي من توافر الشروط السابق ذكرها فيه، فيكون من حق المتهم مناقشة الدليل الرقمي والتشكيك بمشروعيته أو التشكيك بكونه يقينيا.

وما يبنى على ما سبق أنه يجب على المحكمة عند الاعتماد على الدليل الرقمي أن تظهر في حكمها أسباب قناعتها بالدليل الرقمي، وأن تظهر في حكمها الأسباب التي توصلت من خلالها إلى مشروعية الدليل وأنه يقينيا، وكذلك الحال فيما لو قررت المحكمة عدم الاعتماد على الدليل الرقمي فيكون على المحكمة أن تظهر في حكمها الأسباب التي دعتها إلى عدم الأخذ بهذا الدليل.

ونظرا لخصوصية الأدلة الرقمية، ولأن هذه الأدلة قابلة للنقاش، فإن ذلك يستدعي أن يكون القاضي الذي ينظر بالجرائم الإلكترونية على دراية ومعرفة جيدة بطبيعة هذه الأدلة وكيفية الحصول عليها، لأن التحقق من مصداقية هذه الأدلة لا يتأتى واقعا إلا من خلال تخصيص قاضي يكون قادرا على التحقق من توافر شروط الأدلة الرقمية من عدمه.[1]

الفرع الثاني

سلطة القاضي في الإثبات الجنائي

مع منح المشرع الفلسطيني للقاضي الجنائي صلاحيات تقدير وقبول الأدلة المقدمة أمامه، يظهر أهمية دور القاضي في اتخاذ القرارات النهائية في المسائل الجنائية. يعني هذا أن القاضي أو المحكمة يتحملون المسؤولية الكاملة لاتخاذ القرارات استنادًا إلى قناعاتهم، ويتم ذلك على أساس الأدلة المقدمة والمناقشات التي تجري خلال الجلسات. ولا يُسمح للمحكمة بالاعتماد على دليل أو معلومة لم تُقدم أمامها خلال الجلسة القضائية، أو التي تم الوصول إليها بطرق غير قانونية أو غير مشروعة. ينص قانون الإجراءات الجزائية في المادة 1/273 على أن "تحكم المحكمة في الدعوى حسب قناعتها التي تكونت لديها بكامل حريتها ولا يجوز لها أن تبني حكمها على أي دليل لم يطرح أمامها في الجلسة أو تم التوصل إليه بطريق غير مشروع"[2].

---

[1]. مقابلة شخصية، د. فاتح حمارشة، تاريخ المقابلة 2024/3/20، أستاذ القانون في جامعة بيرزيت، محامي وقاضي سابق، مكان إجراء المقابلة جامعة بيرزيت، 2024.

[2]. قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

أولا: القناعة بالأدلة القانونية

أكدت محكمة النقض الفلسطينية حول سلطة القاضي في قبول الدليل بناء على قناعته، في القرار رقم 599 لسنة 2019: "من المقرر أن وزن البينات وتقييم أقوال الشهود وتقدير الظروف التي يؤدون فيها شهادتهم وفهم وتعويل القاضي على أقوالهم مهما وجه إليه من المطاعن وحام حولها من شبهات كل ذلك مرجعه إلى محكمة الموضوع تنزله المنزلة التي تراها وتقدره التقدير الذي تطمئن إليه ومتى أخذت بشهادته فإن ذلك يعتبر أنها طرحت جميع الاعتبارات التي ساقها الدفاع لحملها على عدم الأخذ بها وان تناقض الشاهد أو تضاربه في أقواله لا يعيب الحكم ولا يقدح في سلامته ما دام قد استخلصت محكمة الموضوع الحقيقة من أقوال الشهود حتى لو كانت شهادة فرديه متى قنعت بها المحكمة لان الحكم هو وجدان الحاكم ولا رقابة لمحكمة النقض على قناعة المحكمة في الأدلة المقدمة إليها إذا استخلصت النتيجة استخلاصاً سائغاً لا تناقض فيه مما يجعل ما ينعاه الطاعن في هذا الشأن في غير محله مما يستوجب رد هذه الأسباب"[1].

وهو الأمر ذاته التي اتفقت عليه محكمة النقض المصرية في الطعن رقم ٢٥٠٠٦ لسنة ٨٨ قضائية، أن قصد المحكمة من تقدير القاضي في المحاكمات الجنائية يتم على أساس الأدلة المقدمة، حيث يحظى القاضي بحرية التقدير والاعتماد على الأدلة التي تدعم قراره دون الحاجة لتقديم دليل معين. الأدلة المقدمة تتعاون معًا وتكمل بعضها البعض، حيث تشكل مجموعًا مؤثرًا ومقنعًا لقرار المحكمة. ليس من الضرورة أن تثبت كل جزئية بشكل مفصل، فالدليل يمكن استخلاص ثبوته من خلال الاستنتاجات المنطقية المستمدة من الظروف والقرائن المقدمة. الاعتراض على كفاية الأدلة ظنية لا يُعتبر جدلاً موضوعيًا قابلاً للمراجعة أمام محكمة النقض[2].

كما جاء أيضا في قرار محكمة النقض الفلسطينية في القضية رقم 2019/140 على: "... ولما كان من المبادئ القانونية التي انعقد عليها إجماع الفقه والقضاء وبأن قاضي الموضوع حر في تقدير الدليل المقدم إليه في المسائل الجزائية وله أن يأخذ بالدليل إذا اقتنع به، وليس لمحكمة النقض أن تستأنف النظر في موازنة الدليل والترجيح بين الأدلة، حيث أن البينات تأتي في الجانب الواقعي من الحكم والذي يدخل في سلطة محكمة الموضوع، حيث أن فهم الواقع والتقرير بشأنه وتقدير قيمة البينة ووزنها يدخل في صميم سلطة محكمة الموضوع متى أقيم الحكم على أسباب سائغة تكفي لحمله ولها أصل في الأوراق. ولمحكمة الموضوع إن تبين حقيقة الواقعة وتردها لصورتها الصحيحة

1. قرار نقض،القضية رقم 2018/599 المنعقدة في محكمة النقض الفلسطينية بتاريخ 5-3-2019
2 . أشرف زهران، «النقض» توضح سلطة القاضي الجنائي في تقدير الأدلة، مقال منشور عبر الموقع الإلكتروني الخاص لنقابة المحامين المصريين، تاريخ أخر تحديث: 2023/09/18، تاريخ الاطلاع: 2023/11/08.

التي تستخلصها من جماع الأدلة المطروحة عليها، وهي ليست مطالبة بأن لا تأخذ إلا بالأدلة المباشرة، بل لها أن تستخلص الحقائق القانونية من كل ما يقدم إليها من أدلة ولو كانت غير مباشرة ما دام أن ما حصله الحكم من هذه الأدلة لا يخرج عن استخلاصه السليم ومتفق والمنطق العقلي. ولا يشترط في الدليل أن يكون صريحا دل بنفسه على الواقعة المراد إثباتها، بل يكفي أن يكون استخلاص ثبوتها عن طريق الاستنتاج، مما ينكشف للمحكمة من الظروف والقرائن وترتيب النتائج على المقدمات. وهذا ما نجده في الحكم حيث ان النتائج جاءت مرتبة على المقدمات والاستخلاص منطقي ومقبول والحكم قائم على حجج وأدلة كافية لحمله، خاصة وان الأدلة في المواد الجنائية ضمان متساندة يكمل بعضها بعضا مجتمعة، ومناقشتها فردي غير جائز، ومنها جميعا تتكون عقيدة المحكمة. ولا ينظر لدليل بعينة لمناقشته على حده بل يكفي ان تكون الأدلة في مجموعها كوحدة مؤدية إلى ما قصده الحكم فيها، وهذا ما نجده في الحكم حيث جاء الوزن متفق والاستنتاج الصحيح واستخلاص النتائج بشكل سائغ ومقبول..."[1].

من خلال إعادة قراءة قرار محكمة النقض الفلسطينية السابق، والذي اتفق أيضا مع قرار محكمة النقض المصرية، يتضح أن مهمة محكمة الموضوع هي توضيح حقائق الواقعة وإعادتها لصورتها الصحيحة، باستناد إلى تقدير الأدلة المقدمة أمامها، فالأدلة يمكن أن تكون مباشرة أو غير مباشرة؛ وعليه، يمكن للمحكمة استخدام جميع الأدلة المتاحة لاستنتاج الحقائق، وذلك بناءً على الظروف والقرائن وترتيب النتائج. مع التأكيد على أهمية أن تكون الأدلة متساندة ومجتمعة، ومناقشتها بشكل فردي غير جائز في المواد الجنائية. يتسق الحكم مع المبادئ القانونية والمنطق العقلي، مما يجعله قائمًا على حجج وأدلة كافية ومؤدية للحكم.

للقاضي الحرية في بناء قناعته من خلال النظر في موازنة الدليل والترجيح بين الأدلة وبناء قناعته عليها، ولا رقابة لمحكمة النقض على قناعة المحكمة في الأدلة المقدمة إليه إذا استخلص النتيجة استخلاصاً سائغاً لا تناقض فيه، إلا ان تلك الحرية ليست مطلقة بشكل تام، حيث نصت محكمة النقض الفلسطينية في إحدى قراراتها على: ".. إلا ان قاضي الموضوع وان كان حراً في تقدير الدليل ووزن وبناء قناعته من أي دليل يراه في الدعوى إلا ان هذه الحرية ليست مطلقه وغير محدده اذ أنها مقيده بضوابط وتقوم محكمة النقض بمراقبة كفاية الأسباب التي تحمل الحكم وعلى صحة اقتناع محكمة الموضوع من حيث مصدر الاقتناع ومنطقية الاقتناع..."[2].

[1] قرار نقض،القضية رقم 2019/140 المنعقدة في محكمة النقض الفلسطينية بتاريخ 17-06-2019.
[2]. قرار نقض،القضية رقم 2019/173 المنعقدة في محكمة النقض الفلسطينية بتاريخ 01-07-2019.

ثانيا: مناقشة الأدلة الرقمية

يقتضي قبول القاضي للدليل بأن يتبع ذلك مناقشة شاملة للأدلة أمام المحكمة بشكل علني، كما يتعين على الأطراف المشاركة في الجلسة وتقديم الحقائق ومناقشة الأدلة بشكل علني وواضح ومفصل.

يشدد القانون الفلسطيني، وتحديداً المادة 207 من قانون الإجراءات الجزائية، على أن الحكم لا يمكن أن يستند إلا إلى الأدلة التي قُدمت خلال المحكمة وتمت مناقشتها بشكل علني أمام الخصوم. حيث نصت المادة المذكورة على: "لا يبنى الحكم إلا على الأدلة التي قدمت أثناء المحاكمة والتي تمت مناقشتها في الجلسة بصورة علنية، أمام الخصوم"[1]، فهذا النهج يعزز مبدأ العدالة والشفافية في النظام القضائي.

تهدف هذه الضوابط إلى ضمان أن يتم تقديم الأدلة بشكل دقيق وأن يتم التأكيد على قوتها وصحتها. يُعتبر النقاش العلني فرصة لتوضيح وتفسير الحقائق والأدلة المقدمة، ويتيح للأطراف التعبير عن آرائها والتعليق على الأدلة بطريقة تساعد في تحقيق إجراءات قانونية عادلة وشافية. بالتالي، يتيح هذا النهج تحقيق التوازن بين حقوق الدفاع والحاجة إلى تحقيق العدالة، ويسهم في بناء نظام قضائي يعكس مبادئ الشفافية والنزاهة.

تتسم حرية القاضي في اتخاذ القرارات القضائية بميزة السلطة التقديرية، حيث يحق له تقدير واعتبار الأدلة المقدمة أمامه، سواء كان ذلك خلال مرحلة التحقيق أو المحاكمة. يتسنى للقاضي قبول الأدلة وتقديرها دون وجود ضوابط قانونية صارمة تلزمه في هذا الصدد. يمتلك القاضي أيضا حرية قبول الأدلة المقدمة دون ضرورة شرح الأسباب المحددة لقراراته، وهو يتخذ قراراته بناءً على تقديره الشخصي وفقًا للظروف الأمور المعروضة عليه[2]. لكن القاضي في ذات الوقت لم يطلق العنان للقاضي في هذا الأمر، فالمشرع الفلسطيني في المادة 1/275 أكد على عدم جواز صدور قرار القاضي بحسب قناعته في حالتين:

1. صدور القرار على دليل لم يطرح أمامها في الجلسة ولم يتم مناقشته.
2. كان الدليل الذي يبنى عليه القرار، قد تم التوصل إليه بطريق غير مشروع.

نص قانون الإجراءات الجزائية الفلسطيني في المادة 474 منه على: "يعتبر الإجراء باطلا إذا نص القانون صراحة على بطلانه، أو إذا شابه عيب أدى إلى عدم تحقيق الغاية منه". حيث جاء في منطوق قرار محكمة النقض في الدعوى رقم 140\2019 على: "... وبهذا لا يكون بطلان بغير

[1] . انظر المادة (207) من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.
[2]. مرجع سابق، بن عزة أسامة، ص54-58

نص. وبمقتضى ذلك ان المشرع هو الذي يتولى تحديد أسباب البطلان. كما انه يجب التمييز بين شروط صحة العمل الإجرائي وبين القواعد الإرشادية التنظيمية التي تنطوي على قواعد لتنظيم الأمور وحسن تسييرها ولا يترتب عليها بطلان لأنها تتعلق بتنظيم الدليل لا بقبوله ومشروعيته وكذلك إرشادات للجهة القائمة على إدارة الدليل، وبالتالي هذه لا تعتبر من أسباب البطلان حيث لم يرد نص على بطلانها مما يستوجب معه رد هذا السبب.."[1].

فيما يتعلق بالدليل الإلكتروني، أكد المشرع الفلسطيني أنه يُعامل على نحو مماثل للأدلة الأخرى، ويتم التعامل معه بموجب قرار بقانون رقم (10) بشأن الجرائم الرقمية، والذي نص على: "يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الرقمية أو البيانات والمعلومات الرقمية من أدلة الإثبات"[2]. تشير هذه المادة إلى أن الدليل الرقمي يتمتع بنفس الاعتبارات القانونية التي يحظى بها الدليل التقليدي، إذ يُعتبر وسيلة فعالة وقانونية في سياق القضاء الرقمي. وهو ما يجسد توجه المشرع لتحديث الأنظمة من اجل مواكبة التطورات التكنولوجية، من خلال مراعاته أن يتم التعامل مع الدليل الرقمي بنفس القيمة والثقة التي تُمنح للأدلة التقليدية. كما أن نص المادة السابقة الذكر، أكدت أيضا على أن هذا الدليل يخضع لشروط وإجراءات محددة، بهدف ضمان صحة وجوازية الحصول عليه. يعتبر هذا النهج جزءًا من جهود السلطات القانونية للتأكيد على سلامة جمع وتحليل البيانات الرقمية وضمان النزاهة في استخدامها كدليل أمام المحكمة.

كما تم التطرق إليها سابقا وفقًا لمبدأ حرية الإثبات والاقتناع، فإن القاضي الجنائي يتمتع بحرية تقدير الأدلة، بما في ذلك الأدلة الرقمية. ومع ذلك، هذه الحرية لا تعني أن القاضي يمكنه الحكم بالإدانة بدون وجود يقين قوي، إذ إن حالات فساد الاستدلال قد تحدث عندما يتسرع القاضي في الجلب بالإدانة بناءً على دليل غير مباشر أو قرينة من القرائن، مما يؤكد على خطورة هذا التسرع في الاستنتاج. كما أن التأكيد على الإدانة يتطلب وجود يقين بوجود هذه الإدانة ، وهذا يتماشى مع مبدأ افتراض البراءة الذي يعتبر المتهم بريئًا حتى يُثبت خلاف ذلك بشكل قاطع. بالمعنى الأخر، على القاضي أن يكون حذرًا ومتأكدا قبل أن يصدر حكمه ويلتزم بمبدأ افتراض البراءة، مع ضرورة التوازن في تقييم الأدلة لضمان عدالة القرارات القضائية[3].

---

[1] مصدر سابق، القضية رقم 2019/140 المنعقدة في محكمة النقض الفلسطينية.

[2] . انظر المادة (37) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018م المعدل بالقرارين بقانون ذوات الأرقام (28) لسنة 2020، و (38) لسنة 2021.

[3] . حجال، صادق (2018)، شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني، مجلة العلوم السياسية والقانون، تصدر عن المركز الديمقراطي العربي ألمانيا-برلين، العدد 70 فبراير 2018-المجلد 78، ص 131-132.

المطلب الثاني

القيود الواردة على حرية القاضي الجزائي في قبول الدليل الرقمي

لا يمكن للقاضي الجزائي أن تطلق يده في قبول الأدلة الرقمية، فلا بد ان تكون هناك قيود معينة تجعل قناعة القاضي لا تنحرف عن الهدف الأسمى في الوصول للحقيقة المرجوة وبناء حكم سليم، ومن هذه القيود ما يتعلق بمشروعية الدليل الرقمي والتي سنتطرق إليها في الفرع الأول من هذا المطلب، ومنها ما يتعلق ومنها ما ورد في نصوص قانونية خاصة سنقوم بذكرها في الفرع الثاني.

الفرع الأول

قيود متعلقة بطريقة الحصول على الدليل الرقمي

المقصود بمبدأ المشروعية في هذه الحالة أن الدليل الجنائي بما تضمنه من أدلة مستخرجة من وسائل الكترونية كالكمبيوتر مثلاً، لا يكون مشروعاً ومن ثم مقبولاً في الإثبات، إلا إذا جرت عملية البحث عنه والحصول عليه وإقامته أمام القضاء في إطار أحكام القانون واحترام قيم العدالة،[1]ومن هنا فإنه لا يجوز للقاضي أن يقبل في إثبات إدانة المتهم دليلاً رقمياً تم الحصول عليه من تفتيش لنظام معلوماتي باطل،[2] وذلك إثر على صدور إذن من جهة غير مختصة مثلاً، أو لم تكن الجريمة الإلكترونية محل الإذن قد وقعت بعد.

والواقع أن هذا القيد يمثل المقابل لحرية القاضي الجنائي في قبول جميع أدلة الإثبات ،[3] بما فيها تلك التي لم ينظمها المشرع، وهذا القيد يكتسب أهمية كبرى نتيجة التقدم الهائل الذي تحقق في السنوات الأخيرة في شأن الوسائل الفنية للبحث والتحقيق والتي تسمح أكثر فأكثر باختراق مجال الحياة الخاصة للأفراد، وان كان في مقابل ذلك يرضي أو يلبي مقتضيات العدالة الجنائي على مكافحة الجريمة بصفة عامة والجريمة الإلكترونية بصفة خاصة.[4]

ويرى الباحث أن ما يثار حول هذا القيد هو مسألة الأخذ بالدليل الرقمي غير المشروع مراعاة للمصلحة العامة، وقيمة الدليل الرقمي الذي تم الحصول عليه بطريقة غير مشروعة في الإثبات الجزائي لا سيما أن هناك بعض التشريعات التي أخذت به وقبلته في الإثبات.

---

1. خولة عباسي (2014)، الوسائل الحديثة للإثبات الجنائي في القانون الجزائر، مذكرة استر، جامعة محمد خيضر، الجزائر.
2. مصطفى، (2010)، عائشة بن قارة، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن، دار الجامعة، الإسكندرية، ص 211.
3. آمنة، هلال، (2015)، الإثبات الجنائي بالدليل الإلكتروني، مذكرة ماستر، جامعة محمد خيضر، الجزائر، ص 97.
4. هجيرة، سلامة ياسين رجال ، (20156- 2017)، الإثبات الجنائي بالأدلة الرقمية، جامعة العربي التبسي، رسالة ماجستير، الجزائر، ص 72.

وللإجابة عن هذه التساؤلات سنتطرق إلى هاتين المسألتين وهي الأخذ بالدليل الرقمي مراعاةً للمصلحة الأولى فالأولى وهي (المصلحة العامة)، وقيمة الدليل غير المشروع بالنسبة كدليل إدانة وكدليل براءة.

1- مدى الأخذ بالدليل الرقمي مراعاة للمصلحة المجتمعية الفضلى: وهي الحالة التي يكون فيها الدليل الرقمي غير المشروع فيه اعتداء على الحياة الخاصة لأحدهم، ولكن في نفس الوقت يعتبر وسيلة إثبات لجرائم تهدد أمن ونظام المجتمع الأخلاقي، هوا تثور مشكلة أي المصلحتين أولى.[1]

فإذا كان البعض يشكك في مشروعية الدليل الإلكتروني، باعتباره طريقة للتدخل في الحياة الخاصة للإفراد، لا سيما في مجال الجرائم الجنسية، حيث يكون السلوك الجنسي برضاء المشتركين فيه، إلا أن الاستعانة بالوسائل العلمية الحديثة مثل الإنترنت، واستخدامه كدليل على وقوع جريمة الإعلان عن البغاء ونشر المطبوعات الفاضحة يستهدف المصلحة العامة وحتى تتمكن الدولة من حماية النظام الاجتماعي حتى لا ينهار هذا النظام بسبب احترام مبالغ فيه للحقوق والحريات الخاصة ولا يمكن الاعتراض عليه بحجة عدم مشروعة الدليل الرقمي، فكل ما يسفر عنه العلم الحديث يجب أن يستخدم في تحقيق امن المجتمع ولا شك في مشروعيته.[2]

2- قيمة الدليل غير المشروع[3]: من الضروري التمييز بين نوعين من الأدلة، أدلة الإدانة وكذلك أدلة البراءة.[4]

- **بالنسبة لدليل الإدانة :** انطلاقا من قاعدة أن الأصل في الإنسان البراءة فإن المتهم يجب أن يعامل على أساس انه بريء في مختلف مراحل الدعوى إلا أن يصدر بحقه حكم نهائي، وهذا بمقتضى أن تكون الأدلة التي أسس عليها حكم الإدانة مشروعة سواء كانت أدلة تقليدية أو ناتجة عن الوسائل الإلكترونية بصفة عامة، ومن أمثلة الطرق لغير المشروعة التي يمكن أن تستخدم في الحصول على الدليل الإلكتروني إكراه المتهم ألمعلوماتي من اجل فك شفرة الدخول إلى النظم المعلوماتية، أو كلمة السر اللازمة للدخول إلى ملفات البيانات المخزنة.

---

1. مصطفى، عائشة بن قارة، مرجع سابق، ص 216.
2. هجيرة، سلامة ياسين رجال، مرجع سابق، ص 72.
3. بن طايه، عبد الرزاق، (2014)، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مذكرة ماستر، جامعة محمد خيضر، الجزائر، ص 222.
4. آمنة، هلال، مرجع سابق، ص 98.

وهذا ما نص عليه قانون الإجراءات الجزائية الجزائري في المواد (1 / 157 ، 105 ، 191)، وهذا الأمر يثير مسألة مهمة في المعيار الذي يبين العلاقة التي تربط بين العمل الإجرائي والأعمال التالية له حتى يمتد إليها البطلان، وقد تعددت المعايير التي جاء بها الفقه إلا أن المعيار السائد في الجزائر هو أن العمل اللاحق يعتبر مرتبطاً بالإجراء السابق، إذا كان هذا الإجراء ضرورياً لحصة العمل اللاحق، فإذا أوجب القانون مباشرة إجراء معين قبل الآخر بحيث يصبح الأول بمثابة السبب الوحيد للإجراء الذي تلاه، كان الإجراء الأول شرطاً لصحة الإجراء التالي له، أي اللاحق، فإذا بطل ترتب عليه بطلان الإجراء الذي بني عليه.[1]

وإذا كانت القاعدة أن الإجراء الباطل يمتد بطلانه إلى الإجراء والإجراءات اللاحقة له مباشرةَ، غير أن هذه القاعدة تثير مسألة في غاية الأهمية تتعلق بماهية المعيار الذي يبين مدى العلاقة التي تربط بين العمل الإجرائي والأعمال التالية له حتى يمتد إليها البطلان، وقد تعددت المعاير التي قال بها الفقه المقارن، والمعيار السائد والراجح في مصر والجزائر هو أن العمل اللاحق يعتبر مرتبطاً بالإجراء السابق، إذا كان هذا الأخير مقدمةً ضروريةً لصحة العمل اللاحق فإذا أوجب القانون مباشرة إجراء معين قبل أخر بحيث يصبح الأول بمثابة السبب الوحيد للإجراء الذي تلاه، كان الإجراء الأول شرطاً لصحة الإجراء التالي له، فإذا بطل ترتب عليه بطلان الإجراء الذي بني عليه.[2]

- **بالنسبة لدليل البراءة:** بخصوص قيد قيمة الدليل الرقمي غير المشروع بالنسبة لدليل البراءة فظهرت ثلاثة اتجاهات مختلفة حول هذه المسألة.

أ. **الاتجاه الأول:** يرى أن مشروعية الدليل لازمة في كل دليل، سواء كان دليل إدانة أو براءة، باعتبار أن قصر مبدأ المشروعية على الدليل فقط فيه ضرر على الفرد والمجتمع، كما أن هذا الاتجاه يرى بأن إثبات البراءة كالإدانة، لا يكون إلا من خلال طرق مشروعة، ومن غير الصحيح أن يفلت إثبات البراءة من قيد المشروعية الذي هو أساس في أي تشريع لكل اقتناع سليم.[3]

ب. **الاتجاه الثاني:** يرى بأنه ليس ثمة ما يمنع من تأسيس حكم البراءة على دليل غير مشروع، وهذا انطلاقاً من مبدأ افتراض البراءة باعتبارها هي الأصل، وبالتالي فالمحكمة ليست في حاجة إلى إثباتها، كما أن بطلان الدليل المستمد من وسيلة غير مشروعة شرع أصلا لحماية حرية المتهم، ولهذا من غير المعقول أن ينقلب عليه، ولو تم التمسك بفكرة عدم قبول دليل البراءة لأنه غير

---

1. هجيرة، سلامة ياسين رجال، مرجع سابق، ص 73.
2. هجيرة، سلامة ياسين رجال، مرجع سابق، ص 73.
3. آمنة، هلال، مرجع سابق، ص 99.

مشروع فستكون النتيجة خطيرة، وهي إدانة شخص بريء، بالإضافة إلا أن القاضي بمجرد الشخص الذي توفر دليل براءته حتى وان تم الحصول عليه بطريقة غير مشروعة، وهذا الاتجاه تبنته محكمة النقض المصرية.[1]

ت. **الاتجاه الثالث:** يرى ضرورة التفرقة بين ما إذا كان دليل البراءة قد تم الحصول عليه نتيجة جريمة جنائية، أم كان الحصول عليه نتيجة سلوك يشكل مخالفة لقاعدة إجرائية، فإذا كانت الطريقة الأولى هي التي تم بها الحصول على الدليل وجب إهدار هذا الدليل، لأنه يجعل بعض الجرائم تفلت من العقاب.[2]

بالتالي فإنه إذا ما تم الحصول على الدليل الرقمي بطريق غير مشروع بناء على مخالفة قاعدة مسلكية إجرائية تكون البراءة مستحقة للمتهم استناداً لصحة الاستناد لطبيعة الحصول على هذا الدليل.

- **قيمة الدليل غير المشروع في بعض قوانين بعض الدول:**

من القوانين البارزة التي تناولت موضوع الدليل الجنائي غير المشروع بصفة عامة القانون الانجليزي، حيث أن القاعدة الأساسية في نظام القانون العام أنه متى يكون الدليل ذو فائدة في الإثبات فهو مقبول، بغض النظر عن الطريقة التي تم الحصول بها على هذا الدليل، حتى وان كانت هذه الطريقة غير مشروعة، إلا انه وفي إطار هذا الأمر ظهر اتجاه كان صارماً في طريقة الحصول على الدليل، إلا انه وبسرعة أعيد تكريس مبدأ عدم استبعاد الدليل غير المشروع، والأخذ بنظرية الضبط ألجرمي.[3]

في عام 1984 صدر قانون الشرطة والإثبات الجنائي الذي عالج اختصاص الشرطة وقواعد الإثبات الجنائي، وقد تضمن هذا القانون أحكاماً تنظم استبعاد الأدلة غير المشروعة، ومنها الأدلة التي تستخرج عن طريق إرغام المتهم، أو الحصول على الدليل من شخص أخر غير المتهم، كما نظم السلطة التقديرية للقاضي في استبعاد الدليل غير المشروع.، بحيث يجب ان لا تؤثر هذه الأدلة على نزاهة الإجراءات حتى لا تقضي المحكمة بعدم قبولها.[4]

---

[1]. مصطفى، عائشة بن قارة، مرجع سابق، ص 219.
[2]. بلولهي، مراد (2011)، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مذكرة ماستر، جامعة محمد خيضر، الجزائر، ص 106.
[3]. مصطفى، عائشة بن قارة، مرجع سابق، ص 224.
[4]. آمنة، هلال، مرجع سابق، ص 100.

- **من القضايا التي حدثت في انجلترا والتي على أساسها قام القاضي باستبعاد الأدلة الرقمية المتحصلة من هذه القضية هي قيام الشرطة بمراقبة مكالمات هاتفية بين المشتكية والشخص المشتبه به بناء على موافقة المشتكية بعد أن قامت بتركيب أجهزة تنصت، تضمنت هذه المكالمات مواضيع تدين المشتبه به، والتي اعتبرها القاضي أدلة رقمية غير مشروعة تم استبعادها من وزن البينة.**

كذلك في التشريع الأمريكي الذي تبنى قاعدة عدم استبعاد الأدلة الرقمية التي تم الحصول عليها بطريقة غير مشروعة، والتي قامت المحكمة الفدرالية العليا بحظر إدانة الأفراد المشتبه بهم بناء على أدلة مستمدة منه أو من مسكنه دون موافقته وتم الحصول عليها دون سبب معقول

- **من القضايا التي حدثت في الولايات المتحدة الأمريكية والتي كانت مؤثرة في صياغة التشريعات الجنائية بشأن استبعاد الأدلة الرقمية المتحصلة بطريقة غير مشروعة هي القضية التي جرت أحداثها في عام 1914، والتي قررت فيها المحكمة الاتحادية بإجماع أعضائها مبدأ عدم قبول الدليل المتحصل بالمخالفة، وهذا بهدف حماية الفرد من التعسف السلطات الدستوري، إلا ان هذه المحكمة قد أوردت بعض الاستثناءات ويمكن اختزالها في أربعة حالات، أولها حسن النية لدى رجال الشرطة أثناء عملهم الإجرائي ويستند على أساس قانوني صحيح، والاستثناء الثاني عندما تكون الصلة بين العمل الإجرائي المخالف والدليل المتحصل من ذاك الإجراء ضعيف، بحيث لا يتم إدراك الخطأ في الإجراء، والثالث عندما يتم الحصول على الدليل بصورة مستقلة عن العمل الإجرائي الضعيف، والرابع عندما تكون الأدلة لا يتم اكتشافها والحصول عليها إلا من خلال إجراء القانوني السليم.**

وعليه قام المشرع الأمريكي بتخصيص مبحث خاص بتفتيش وضبط الحواسيب وصولاً إلى الدليل الرقمي، وهو المبحث الخامس في المرشد الفدرالي الأمريكي، والذي يتعلق بمعالجة الانتهاكات التي قد تحدث أثناء عملية التفتيش والمراقبة وقانون التسجيل والتقصي، كي لا يقع أي بطلان إجرائي يؤثر على القيمة القانونية للدليل الرقمي فيما إذا تم الحصول عليه بشكل غير مشروع.

الفرع الثاني

القيود الواردة بموجب نصوص قانونية خاصة

الأصل العام أن القاضي الجنائي يقوم بحرية بالاستناد إلى أية أدلة يطمئن إليها دون أن يتقيد بدليل معين، لان القاعدة تنص على اقتناع القاضي بالأدلة المطروحة أمامه، إلا أن هذا الأصل يرد عليه استثناءات تقيد القاضي في الاستناد إلى هذه الأدلة، حيث يتقيد فيها قاضي المحكمة الجزائية بتكوين قناعته. يرجع ذلك إلى طبيعة الجرائم المعنية ذاتها، حيث تكون بعض الأفعال الجرمية ذات طبيعة خاصة، ويكون على القاضي الالتزام بأدلة محددة حددها المشرع. هذا يقيد حريته في اعتماد هذه الأدلة، حيث لا يمكن للقاضي أن يأخذ بأدلة أخرى حتى لو اقتنع بها.

وجاءت هذه القيود في بعض النصوص القانونية الجنائية التي تختص في بعض الجرائم، حيث انه لا يجوز للقاضي إثبات وقوع الجريمة وإدانة مرتكبها إلا من خلالها، أو إلزامه بأدلة إثبات خاصة في بعض المسائل غير الجنائية، والتي يملك اختصاص النظر فيها بصفة تبعية للدعوى الجنائية الأصلية، والتي أدلة إثباتها قانونية، وهذه القيود تتمثل فيما يلي :

1- حصر أدلة الإثبات في بعض الجرائم

المبدأ العام في الإثبات الجزائي هو عدم حصر الأدلة في نوع معين من الجرائم، وهناك بعض التشريعات التي خرجت من هذا الأصل عن طريق تحديدها الأدلة التي تقبل في إثبات بعض الجرائم، ومن بين هذه التشريعات والقضايا التي لا يُسمح بإثباتها بحرية القانون الأردني والمصري وكذلك الجزائري، حيث يتقيد فيها قاضي المحكمة الجزائية بتكوين قناعته، يرجع ذلك إلى طبيعة الجرائم المعنية ذاتها، حيث تكون بعض الأفعال الجرمية ذات طبيعة خاصة، ويكون على القاضي الالتزام بأدلة محددة حددها المشرع. هذا يقيد حريته في اعتماد هذه الأدلة، حيث لا يمكن للقاضي أن يأخذ بأدلة أخرى حتى لو اقتنع بها. ومن بين أهم هذه المسائل التي يتجلى فيها تقييد حرية القاضي الجزائي في اعتماد الدليل الرقمي هي جريمة الزنا.

في هذا الأمر، حدد قانون العقوبات الأردن ي رقم 16 لسنة 1960 في المادة (282) والساري في فلسطين قيود فيما يتعلق بإثبات وقوع جريمة الزنا، والذي نص على: "الأدلة التي تقبل وتكون حجة على شريك الزانية هي القبض عليهما حين تلبسهما بالفعل أو اعتراف المتهم لدى قاضي التحقيق أو في المحكمة أو وجود مكاتيب أو أوراق أخرى مكتوبة"[1]، أما فيما يتعلق بالإثبات على الزوج الزاني أو الزوجة الزانية فهي تخضع لكافة وسائل الإثبات الجنائي.

[1]. انظر المادة (282) من قانون العقوبات رقم 16 لسنة 60 وتعديلاته.

وكذلك من التشريعات السباقة التي تقيد الأدلة الرقمية في جريمة الزنا القانون المصري من خلال المادة (276) من قانون العقوبات المصري النافذ، والتي حددت من خلال هذه المادة أدلة معينة لإثبات شريك الزوجة الزانية، وبهذا قيد القاضي البحث عن الحقيقة عن أدلة أخرى غير ما نصت عليه المادة سالفة الذكر،[1] وحصر هذه الأدلة في التلبس بالزنا و الاعتراف وإقرار الشريك والأوراق والمكاتيب التي حررها الشريك، ووجود شريك في منزل مسلم في المكان المخصص للحريم.

أما المشرع الجزائري فقد حدد ثلاثة أنواع من الأدلة لإثبات جريمة الزنا المعاقب عليها في نص المادة (33) من قانون العقوبات الجزائري، وهذه الأدلة تم تحديدها في نص المادة (341) من القانون ذاته، وهي إما المحضر الذي يحرره إحدى عناصر مأموري الضبط القضائي أو إقرار وارد في رسائل أو مستندات صادرة عن المتهم، إقرار قضائي.[2]

ويذهب الرأي الغالب في الفقه والقضاء إلا أن هذه الأدلة لازمة فقط لإثبات زنا شريك الزوجة، لان إثبات زنا أي منهما يخضع لمبدأ حرية الإثبات الجزائي، ولهذا لا يجوز للقاضي الجنائي أن يقبل في سبيل إثبات زنا الشريك إلا الأدلة التي تم إقرارها، حتى وان كان دليلاً الكترونياً، سواء كان عبارة عن صور فيديو أو رسالة مرسلة من الشريك إلى الزوجة أو غيرها عن طريق الهاتف النقال، أو عن طريق الإنترنت، وسواء تضمنت هذه الرسالة اعترافاً صريحاً أو ضمنياً من الشريك بوقوع الزنا، أو فيها نوع من الكلام الذي يوحي بممارسة علاقة غير شرعية للزوجة.

- **وعليه يرى الباحث أن من الضروري أن تعامل الأدلة الرقمية مثل الصور الرقمية والفيديوهات الرقمية والرسائل النصية المرسلة بواسطة إحدى أجهزة شبكات الفضاء الإلكتروني في جريمة الزنا أن تعامل معاملة الأدلة التقليدية كالصور الفوتوغرافية والمكاتب والرسائل المكتوبة والتي حددها المشرع لإثبات جريمة الزنا على سبيل الحصر، وذلك لسد القصور التشريعي في قوانين معظم الدول العربية ذات الخصوص.**

ولا بد من التذكير، مُجدداً، بنص المادة (45) من قرار بقانون الجرائم الإلكترونية الفلسطيني رقم (10) لسنة 2018 والتي نصت صراحة على أن كل مَن ارتكب فعلاً جُرمياً بموجب "أي تشريع نافذ" باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات أو اشترك فيها يُعاقب بذات العقوبة المقررة في ذلك "التشريع النافذ". مما يعني أن الأفعال الجُرمية الواردة في

---

1. انظر المادة (276) من قانون العقوبات المصري رقم 58 لسنة 1937 وتعديلاته.
2. انظر المواد (339)، (341) قانون العقوبات الجزائري المعدل والمتمم، الصادر بالأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو عام 1966، وتعديلاته.

النصوص والتشريعات النافذة في مجال الأدلة التقليدية مُعاقب عليها إذا ارتكبت في المجال الرقمي وبالعقوبة الواردة في تلك التشريعات. وبذلك فإن كل ما يسري على الأدلة التقليدية في المجال التجريمي يسري على الادلة الرقمية بالاستناد لهذا النص. وقد سبق القول بأن هذا النص أوسع من القرار بقانون بأكمله ويطال كافة التشريعات النافذة ذات الصلة.

2- قيد الإثبات الخاص في بعض المسائل غير الجزائية

قد تعرض على القاضي الجنائي أثناء نظره الدعوى الجنائية مسألة مدنية أو تجارية أو إدارية، وفي هذه الحالة يتوجب على القاضي الجنائي إتباع طرق الإثبات الخاصة بتلك المسائل، كما هو الحال في عقود الأمانة كالوديعة والعارية والرهن والوكالة.[1]

وهذه المسائل غير الجنائية أو كما تسمى بالمسائل الأولية تعرف على أنها، "تلك المسائل العارضة التي تثار أثناء نظر الدعوى الجزائية، والتي يلزم ويتعين الفصل فيها أولاً من قبل القاضي الجزائي، لكونها تدخل في البناء القانوني للفعل ألجرمي موضوع الدعوى، إذ أن الفصل في الدعوى الجنائية يتوقف على الفصل فيها أو لاً، وان قيام الجريمة من عدمه واقف على ذلك، فالعلة من الأمر تمكين القاضي الجزائي من فحص مجموعة المشروعات الإجرامية التي ترتبط فيما بينها بحيث يفسر بعضها بعضاً، فيتمكن القاضي الجنائي من فحص جريمة كاملة متكاملة بجميع أركانها وعناصرها، ولو كانت من بين هذه العناصر ما يخرج عن اختصاص القاضي الجنائي.[2]

وعليه فإنه يستفاد مما سبق أن القاضي الجزائي قد يضطر أحيانا في بعض القضايا الجنائية المرتبط الفصل فيها على الفصل في مسائل أولية سابقة ومقترنة فيها، فجريمة الاختلاس على سبيل المثال تفرض وجود عقد مدني بين الجاني والمجني عليه، ويتعين على القاضي الفصل في عقد الأمانة إذا كان موجود أم لا قبل الفصل في جريمة الاختلاس التي لم تكن لولا وجود عقد أمانة مبرم بين المشتكي والمتهم، وهنا يتعين على القاضي الجزائي أن يقوم بإعمال قواعد إثبات القانون المدني، وفيما يتعلق بالأدلة الرقمية وإمكانية إثباته فيما يتعلق بإثبات عقد الأمانة الإلكتروني الذي تم إبرامه بين الجاني والمجني عليه الكترونياً، أي عن طريق إحدى شبكات الإنترنت، مثل السند أو المحرر الإلكتروني، فعلى القاضي هنا لإثبات وقوع العقد بينهما أن يستبعد أدلة الإثبات الرقمية الجنائية وان يقوم بإعمال نصوص قواعد القانون المدني الكترونياً لإثبات المسائل الأولية السابقة للجريمة

[1]. مصطفى، عائشة بن قارة، مرجع سابق، ص 231.
[2]؟ هجيرة، سلامة ياسين رجال، مرجع سابق، ص 80.

الإلكترونية كالنصب والاحتيال أو الاختلاس التي تمت عن طريق الإنترنت الكترونياً، كونه مقيد حسب القاعدة أنفة الذكر.

وعليه فقد أقر التشابه والتماثل بين الكتابة على الورق والكتابة الإلكترونية كمن حيث الحجية في الإثبات، حيث نصت المادة (1316 – 1) من القانون المدني الفرنسي على انه (تقبل الكتابة في شكل الكتروني كدليل في الإثبات مثلها في ذلك مثل الكتابة على دعامة ورقية، ما دام أن الشخص المنسوب إليه هذه الكتابة قد تم تحديده على وجه صحيح وقد تم إثبات هذه الكتابة والاحتفاظ بها في ظروف من شأنها أن تضمن سلامتها).

وتدخل المشرع الفرنسي بتعديل بعض مواد القانون المدني لتتفق مع التوقيع على العقود والمحررات الإلكترونية، فعرف التوقيع بشكل عام والتوقيع الإلكتروني بشكل خاص، وقد ركز على آثاره القانونية، من خلال المادة (4) من القانون رقم (2000/230) المعدلة والمتممة للمادة (1316 – 1) من القانون المدني الفرنسي، حيث تنص:" إن التوقيع ضروري لاكتمال التصرف القانوني، وهو يحدد هوية من يحتج به عليه ويعبر عن رضا الأطراف بالالتزامات الناشئة عن هذا التصرف، وعندما يتم بواسطة موظف عام يكتسب التصرف صفته الرسمية، وعندما يكون التوقيع الإلكتروني يقتضي استخدام وسيلة آمنة لتحديد الشخص بحيث تضمن صفته بالتصرف الذي وقع عليه. ويفترض أمان هذه الوسيلة ما لم يوجد دليل مخالف بمجرد وضع التوقيع الإلكتروني الذي يجري بموجبه تحديد الشخص الموقع، ويضمن سلامة التصرف وذلك بالشروط التي يتم تحديدها بمرسوم يصدر عن مجلس الدولة.[1]

وهنا يمكن لنا القول بان الأدلة الرقمية في الوقت الحالي أصبحت أدلة لا يمكن الاستغناء عنها خاصة مع التطور التكنولوجي الهائل، والذي كان منوط بالمشرعين مواكبة هذه التطور من خلال تشريعاتهم سواء بالنص صراحة على الدليل الرقمي الذي لا يقل أهمية عن الأدلة التقليدية في الإثبات الجنائي، إعمالا للقواعد العامة التي نصت على حرية الإثبات في المسائل الجنائية والذي هو الأساس في مقبولية الأدلة الرقمية الجنائية، إلا انه قد ورد بعض الاستثناءات التي تندرج تحت نظام الإثبات المقيد، والتي من شأنها أيضا أن تقود القاضي الجزائي للوصول إلى الحقيقة وبناء أحكام جزائية سليمة.

وهنا لا بد وأن نشير إلى التطور الذي جرى على مستوى قانون البينات في المواد المدنية والتجارية الفلسطيني رقم (4) لسنة 2001 من خلال القرار بقانون رقم (9) لسنة 2022 بشأن تعديل

[1]. انظر المواد (1316- 1) والمادة (4) من القانون الفرنسي المدني من القانون رقم (2000/230).

قانون البينات في المواد المدنية والتجارية رقم (4) لسنة 2001، في مجال الأدلة الرقمية المدنية، حيث أكد القرار بقانون المذكور لسنة 2022 في المادة (4) على إضافة فقرة جديدة للمادة (19) من قانون البينات الأصلي تحمل الرقم (3) وقد جاءت الإضافة على النحو التالي "3.أ تكون لرسائل الفاكس والتلكس والبريد الإلكتروني وما يماثلها من وسائل الاتصال الحديثة، قوة السندات العرفية إذا اقترنت بشهادة من أرسلها لتأييد صدورها عنه أو بشهادة من وصلت إليه لتأييد تسلمه لها، ما لم يثبت خلاف ذلك ب. تكون لرسائل البريد الإلكتروني قوة السندات العرفية في الإثبات دون اقترانها بالشهادة إذا تحققت فيها الشروط التي يقتضيها قانون المعاملات الإلكترونية النافذ ج. يجوز الاتفاق على أن تكون البينات المنقولة أو المحفوظة باستخدام التقنيات الحديثة من خلال رقم سري متفق عليه فيما بين الطرفين حجة على كل منهما لإثبات المعاملات التي تمت بمقتضى تلك البيانات د. تكون لمستخرجات الحاسوب الآلي المصدقة أو الموقعة قوة الإسناد العادية في الإثبات، ما لم يثبت من نسبت إليه أنه لم يستخرجها أو لم يصدقها أو لم يوقعها أو لم يكلف أحداً بذلك".

ولم يقتصر التطور في التعامل مع الأدلة الرقمية في المجال المدني على ذلك، بل وشمل أيضاً الأدلة الرقمية في المجال التجاري (الدفاتر التجارية) حيث حمل قانون البينات المعدل في العام 2022 "نصاً مستحدثاً" على قانون البينات الأصلي تمثل في المادة (5) المستحدثة والتي جاءت على النحو التالي "تُعتبر مستخرجات الحاسوب الآلي أو غيره من أجهزة التقنية الحديثة التي يستخرجها التجار في تنظيم عملياتهم المالية وقيودهم المحاسبية بمثابة دفاتر تجارية". ما يدلل على التطور الحاصل في المجال المدني والتجاري في التعامل مع الأدلة الرقمية. إذ لم يعد بالإمكان الركون على الأدلة التقليدية المدنية أيضاً في العصر الرقمي.

وبالنتيجة، فإن التطور في مجال التعامل مع الأدلة الرقمية لا يقتصر فقط على المجال الجنائي والمسائل الأولية المتصلة بالدعاوى الجنائية، وإنما يشمل أيضاً المجال المدني والتجاري من خلال قانون البينات في المواد المدنية والتجارية والتعديلات التي جرت عليه وبخاصة في العام 2022. وهذا من البديهيات في العصر الرقمي الحديث لأنه لا يمكن تخيل الفصل في الأدلة الرقمية بين المجال الجنائي والمجال المدني والتجاري.

وهذا ما يدفعنا إلى التأكيد، مجدداً، على أن مجال"الأدلة الرقمية عموماً" ما زال يحتاج إلى تدخل متكامل على المستوى التشريعي ينظم التفاصيل التقنية للجوانب الإجرائية، جنباً إلى جنب، مع الجوانب الموضوعية.

المبحث الثاني

التشريعات الوطنية الخاصة بالأدلة الرقمية ومدى مواءمتها والمواثيق الدولية

ستبقى التشريعات الوطنية الناظمة للجرائم المعلوماتية الرقمية وإجراءات التعامل مع الأدلة الرقمية محل شك إذا ما كانت هذه التشريعات كافية وقادرة على معالجة المشكلات التي تطرأ على مثل هذه الجرائم نتيجة التغير المستمر في طبيعتها والحداثة، إذا ما تم مواءمتها مع المواثيق والاتفاقيات الدولية ومدى فاعليتها في ظل نقص التعاون الدولي لخلق بيئة قانونية إجرائية سليمة تمكن الدول من محاربة مثل هذا النوع من الجرائم وملاحقة مرتكبيها، وعليه فقد كان لزاماً علينا أن نبين مدى انسجام التشريعات الوطنية مع المواثيق الدولية وأحكام الدستور في المطلب الأول، ونستعرض أهم الاتفاقيات والمعايير الدولية المتعلقة بالأدلة الرقمية ودورها في الإثبات الجنائي في المطلب الثاني.

المطلب الأول

مواءمة التشريعات الوطنية الخاصة بالأدلة الرقمية مع المواثيق الدولية وأحكام الدستور

بعد انضمام دولة فلسطين إلى العهد الدولي الخاص بالحقوق المدنية والسياسية عام (2014) بموجب هذا الانضمام كان لزاماً عليها مواءمة تشريعاتها الوطنية وسياساتها وممارساتها العملية مع أحكام العهد الدولي. لا سيما وأنه قد تم "إدماج" العهد الدولي المذكور في التشريع الداخلي الفلسطيني وذلك من خلال القرار بقانون رقم (18) لسنة (2023) بشأن نشر العهد الدولي الخاص بالحقوق المدنية والسياسية في الجريدة الرسمية. والقرار بقانون المذكور منشور في الوقائع الفلسطينية في العدد رقم (204) الصادر بتاريخ 2023/07/26.

الفرع الأول

مواءمة تطبيق التشريعات الرقمية في تقرير دولة فلسطين (العهد المدني والسياسي)

بتبيان كيفية تعاطي التقرير الرسمي لدولة فلسطين بشأن العهد الدولي الخاص بالحقوق المدنية والسياسية - التقرير الأولي الشامل- الذي انضمت إليه دولة فلسطين، والمقدم إلى الجنة المَعنية بحقوق الإنسان في الأمم المتحدة (لجنة العهد المدني والسياسي)، مع واقع تطبيق قرار بقانون الجرائم الإلكترونية رقم (10) لسنة 2018 وتعديلاته من خلال المادة (19) من العهد الدولي المذكور المتعلقة بالحق في حرية الرأي والتعبير.

بالرجوع إلى التقرير الأولي[1] المُقدَّم من دولة فلسطين إلى اللجنة المعنية بحقوق الإنسان في الأمم المتحدة بشأن العهد الدولي الخاص بالحقوق المدنية والسياسية في 16 تشرين الثاني/نوفمبر 2020 (موعد تقديمه 2015) فقد تناول المادة (19) المتعلقة بحرية الرأي والتعبير في البنود (333 – 358) منه، وبفحص قرار بقانون الجرائم الإلكترونية تحديداً وواقع تطبيقه فقد جاء في "فقرة واحدة" من تقرير دولة فلسطين هي الفقرة (344) وقد وردت على النحو التالي "صدر قرار بقانون الجرائم الإلكترونية رقم (16) لسنة 2017، وأثار القرار بقانون منذ صدوره موجة من الانتقادات، وإثر ذلك تم عرض القرار بقانون لنقاش مجتمعي بمشاركة مؤسسات المجتمع المدني واعتماد مجموعة من التعديلات التي قُدمَت من خلال لجنة مواءمة التشريعات، وبالتالي تم استبداله بقرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، حيث تم إلغاء النصوص الفضفاضة وتخفيف العقوبات الجزائية والوصول إلى تعديلات جوهرية. ولا زال النقاش البنّاء ما بين الجهات الحكومية ومؤسسات المجتمع المدني قائماً لغايات التوصل إلى الإطار الناظم الأفضل فيما يتعلق بالجرائم الإلكترونية ما يدل على توجه الإرادة السياسية لدولة فلسطين نحو ضمان حرية الرأي والتعبير وإشراك المجتمع المدني في تحقيق المواءمة مع المعايير الدولية".[2]

من الواضح أن دولة فلسطين قد تجاهلت الممارسات العملية الناجمة عن تطبيق قرار بقانون الجرائم الإلكترونية رقم (16) لسنة 2017 ومن ثم قرار بقانون الجرائم الإلكترونية رقم (10) لسنة 2018 الذي ألغى بموجبه قرار بقانون 2017 في التقرير المُقدم إلى اللجنة الدولية. ولعل هذا ما دفع اللجنة المَعنِية بحقوق الإنسان - كما سنرى لاحقاً - أن تطلب "قائمة مسائل"[3] من دولة فلسطين بتاريخ 2022/9/19 في هذا الجانب (حرية الرأي والتعبير) وغيره من الجوانب الواردة في التقرير؛ والتي تعني وجود "نواقص جوهرية"تحتاج إلى إجابات من دولة فلسطين كي يكون تقريرها الرسمي "ناضجاً" للمناقشة المُرتقبة بشأنه أمام اللجنة الدولية في مقر الأمم المتحدة بجنيف. وطلبت اللجنة، من دولة فلسطين، تزويدها بمعلومات وشروحات وإحصائيات بشأن الأفراد المحتجزين والذين جرى محاكمتهم بسبب منشوراتهم على مواقع التواصل الاجتماعي خلال السنوات الخمس الماضية.[4]

جدير بالذكر، أنه قد جرت ثلاث جلسات للحوار بين المجتمع المدني والحكومة بشان قرار بقانون الجرائم الإلكترونية، أخرها كان جلسة الحوار في "لجنة مواءمة التشريعات" داخل مقر مجلس

---

[1]. التقرير الأولي المُقدم من دولة فلسطين إلى اللجنة المعنية بحقوق الإنسان في الأمم المتحدة بموجب المادة (40) من العهد (CCPR/C/PSE/1).

[2]. د. عابدين، عصام ، مرجع سابق، ص 10.

[3]. قائمة المسائل المقدمة من اللجنة المعنية بحقوق الإنسان في الأمم المتحدة إلى دولة فلسطين في 19/9/2022 (CCPR/C/PSE/Q/1) فقرة (19).

[4]. د. عابدين، عصام ، مرجع سابق، ص 11.

الوزراء الفلسطيني في 19-2017/11/22، ورغم إدخال بعض التعديلات المهمة على قرار بقانون الجرائم الإلكترونية 2017 وتحديداً في جلسة الحوار الثالثة (لجنة مواءمة التشريعات) بعد فشل جلستي الحوار السابقتين، إلا أن لجنة مواءمة التشريعات رفضت تعديل "النصوص الحاسمة" التي تُشكل "الخزان" لانتهاكات حرية التعبير والحقوق الرقمية في الممارسات العملية من خلال قرار بقانون الجرائم الإلكترونية وتحديداً المادة(39) بشأن (حجب المواقع الإلكترونية) والمادة (45) بشأن (الاعتقالات التعسفية) وغيرها. ورفض ممثل المجتمع المدني[1] طرح الأمر على التصويت داخل اللجنة مع بقاء تلك النصوص التي تشكل انتهاكات صارخة للحقوق والحريات وتُفرغ أي تقدم من مضمونه مع بقاء تلك النصوص، ولكون أعضاء لجنة مواءمة التشريعات من الجهات الرسمية إلى جانب الهيئة المستقلة، ولا يمكن القبول بطرح مواد على التصويت تنطوي على مخالفات صارخة للاتفاقيات الدولية. ومع إصرار لجنة مواءمة التشريعات على اللجوء للتصويت بما يشمل المواد المذكورة أعلن ممثل المجتمع المدني تجميد المشاركة في الحوار مع اللجنة على الفور والانسحاب من الاجتماع، فيما استمرت اللجنة في عملها مع وجود العضو الممثل عن الهيئة المستقلة بعد التواصل مع إدارة الهيئة وتأكيد استمراره في اللجنة، وجرى إقرار المواد المذكورة وغيرها، وخرج قرار بقانون الجرائم الإلكترونية 2018 النافذ[2]. وقد شكلت تلك المواد (39، 45) النصوص الأبرز لانتهاكات حرية التعبير في الممارسات العملية.

- التقارير فاعلة ومؤثرة إلى حد ما، وذلك عبر مساعدة المقررين الخواص والهيئات التعاقدية في تحديد المشاكل التي تعتري التشريعات وتمثل انتهاكاً لحقوق الإنسان، الأمر الذي يؤدي بالنتيجة إلى تبني المقررين الخواص والهيئات التعاقدية لتوصيات أكثر فاعلية ومفيدة من أجل تقديمها إلى السلطة الفلسطينية وحثها على اعتمادها وإجراء التعديلات اللازمة. وقد حصل تطور من هذا القبيل فيما يتصل بقانون الجرائم الالكترونية 2017، وفي القرارات بقانون المعدلة لقوانين إجراءات التقاضي سنة 2022، حيث إنه وبناءً على بيانات صحفية ومذكرات قانونية صادرة عن مؤسسات المجتمع المدني والهيئة المستقلة بخصوص تلك التشريعات، وبناءً على مخاطبة من بعض المؤسسات (مؤسسة الحق) للآليات الدولية في الأمم المتحدة بشأن قرار بقانون الجرائم الإلكترونية 2017، دعا المقرر الخاص لدى الأمم المتحدة المَعني بحرية التعبير، "ديفيد كاي"، بمذكرة شاملة، الحكومة

[1] ممثل المجتمع المدني في جلسات الحوار مع الحكومة بشأن قرار بقانون الجرائم الدولية ومواءمته مع الاتفاقيات الدولية هو د. عصام عابدين.

[2]. د. عابدين، عصام ، ملاحظات مؤسسة الحق على مشروع القرار بقانون المعدل للجرائم الإلكترونية، 25 يناير 2018، منشورة على موقع مؤسسة الحق على الرابط:

. https://www.alhaq.org/ar/advocacy/2291.html

الفلسطينية إلى تعديل قانون الجرائم الالكترونية، وفعلاً تم تعديله. وفي العام 2022، دعت لجنة مناهضة التعذيب في الأمم المتحدة السلطات الفلسطينية إلى إلغاء قانون الإجراءات القضائية وفعلاً تم إلغائها.

طبعاً هناك وجه آخر لدور مؤسسات المجتمع المدني وللمؤسسة الوطنية لحقوق الإنسان (الهيئة المستقلة) في مساندة ودعم آليات الأمم المتحدة فيما يتعلق بالحق في الخصوصية وانعدام الأمن الرقمي، وذلك عبر الإشارة إلى هذه المسائل في تقارير الظل أو بحسب تسمية أخرى "التقارير الموازية" التي تتقدم بها تلك المؤسسات إلى الهيئات التعاقدية، وتستعرض فيها مدى التزام السلطة الفلسطينية بتنفيذ التزاماتها بموجب الاتفاقية التي انضمت إليها، وتساعد هذه التقارير تلك الهيئات (مجموعة الخبراء) في إعداد قوائم المسائل، والتوصيات أو الملاحظات الختامية التي تقدمها للسلطات الفلسطينية وتحثها فيها على إجراء التعديلات اللازمة.[1]

الفرع الثاني

الممارسات العملية للتشريعات الرقمية

سنتناول التحليل القانوني للممارسات المتعلقة بقرار بقانون الجرائم الإلكترونية رقم (10) لسنة 2018 النافذ في الضفة الغربية في ضوء المواثيق والمعايير الدولية ذات الصلة وأحكام القانون الاساسي الفلسطيني المعدل (الدستور) والقرار بقانون الجرائم الإلكترونية وتعديلاته وبخاصة الانتهاكات الأكثر انتشاراً في الممارسات العملية المرتبطة بالقرار بقانون وتحديداً الاعتقالات التعسفية وحجب المواقع الإلكترونية المرتبطة بقرار بقانون الجرائم الإلكترونية المخالف للدستور والمواثيق والمعايير الدولية ذات الصلة.

1- في المواثيق الدولية لحقوق الإنسان

انضمت دولة فلسطين إلى العهد الدولي الخاص بالحقوق المدنية والسياسية بدون تحفظات مطلع نيسان 2014 وبموجب هذا الانضمام فإنه يتوجب عليها مواءمة تشريعاتها وسياساتها وممارساتها العملية مع أحكام العهد الدولي المذكور بدون تحفظات وبيان التقدُّم المُحرَز على هذا الصعيد أمام اللجنة المَعنِية بحقوق الإنسان في الأمم المتحدة، أكد العهد الدولي على احترام حرية الرأي والتعبير في المادة (19) والحقوق الرقمية ونقيضها الجرائم الإلكترونية يتم معالجتها في تلك الإتفاقية الدولية

1. أ. عمار جاموس، تاريخ المقابلة 2024/05/28، باحث قانوني، الهيئة المستقلة لحقوق الإنسان، مكان إجراء المقابلة – مكتب الهيئة المستقلة لحقوق الإنسان، 2024.

تحت المادة (19) المتعلقة بحرية الرأي والتعبير والتعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان بشأن المادة (19) المذكورة.[1]

وحيث أن التعليق العام (34) الصادر عن اللجنة المَعنِية يُمثل شرح اللجنة للمادة (19) من العهد بحصيلة نقاشاتها البنّاء مع الدول الأطراف في العهد، فقد أكد التعليق العام على أن حرية الرأي والتعبير شرطان لا غنى عنهما لتحقيق النمو الكامل للفرد، وهما عنصران أساسيان من عناصر أي مجتمع، ويشكلان حجز الزاوية لكل مجتمع تسوده الحرية والديمقراطية، وحرية التعبير شرط ضروري لإرساء مبادئ الشفافية والمساءلة التي تمثل بدورها عاملاً أساسياً لتعزيز وحماية حقوق الإنسان [2].

وفي مجال الحقوق الرقمية، أكدت اللجنة على أنه ينبغي على الدول الأطراف أن تأخذ بالحسبان مدى تأثير التطورات التي طرأت على تكنولوجيا المعلومات والاتصالات، مثل نظم نشر المعلومات الإلكترونية القائمة على خدمات الإنترنت والهاتف النقال، في إحداث تغيير كبير في ممارسة الاتصالات حول العالم. توجد اليوم شبكة عالمية لتبادل الأفكار والآراء لا تعتمد بالضرورة على الوسطاء التقليديين لوسائط الإعلام الجماهيري. ينبغي على الدول الأطراف أن تتخذ جميع التدابير الضرورية لتعزيز استقلالية هذه الوسائط الإعلامية الجديدة وأن تضمن سُبل وصول الأفراد إليها[3].

وأكدت اللجنة على أن الحق في الوصول إلى المعلومات التي تكون بحوزة السلطات والهيئات العامة مشمولة بحرية التعبير عن الرأي في المادة (19) من العهد[4].

واستعرضت اللجنة في البنود (21) وما بعدها من التعليق العام (34) ما نُسَميه **"الاختبار ثُلاثي الأجزاء"** للحُكم صحة وسلامة أيّ قيد أو ضابط يتم وضعه على الحق في حرية التعبير عن الرأي بالاستناد لأحكام المادة (19) من العهد والتعليق العام المذكور، وجوهر هذا الفحص الثلاثي، الصارم والمُتشدد، حِماية لحرية التعبير، المحمية بالعهد، يقوم على أنه لا يجوز لأي قيد أن يُعرّض الحق نفسه (حرية التعبير) للخطر وأن لا يقلب هذا القيد العلاقة بين "الحق والقيد" وبين "القاعدة والاستثناء"[5].

يعني الاختبار ثُلاثي الأجزاء؛ اجتياز القيد أو الضابط الوارد على حرية التعبير ثلاث مستويات "بنجاح" للقولِ بانسجامه مع أحكام العهد الدولي للحقوق المدنية والسياسية والمعايير الدولية ذات

---

1. د.عصام عابدين، مرجع سابق، ص 11.
2. اللجنة المعنية بحقوق الإنسان ، التعليق العام رقم (34)، CCPR/C/GC/34، البنود رقم (2) و (3) من التعليق العام المذكور.
3. البند (15) من التعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة.
4. البنود (18) و (19) من التعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة.
5. البند (21) من التعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة.

الصلة[1] وهذا الاختبار"الصارم والمتشدد" يسري على باقي الحقوق التي يُمكن تقييدها في العهد الدولي الخاص بالحقوق المدنية والسياسية[2].

المستوى الأول من الفحص يتناول"القانونية" ويجب اجتيازه بنجاح؛ أي أن يكون القيد الوارد على حرية التعبير منصوصاً عليه في القانون بنص واضح وصريح ولا يستخدم مصطلحات فضفاضة ويمكن للأفراد الحُكم على تصرفاتهم من خلاله. والمستوى الثاني من الفحص يتناول "الضرورة" ويتعلق بمشروعية الغرض من القيد (حماية الحق في الخصوصية مثلاً) وعلى قاعدة إذا كان هناك إمكانية لتوفير تلك الحماية بطرق أخرى لا تحد من حرية التعبير فلا يُصار إلى إعمال هذا القيد (أي يفشل في المستوى الثاني للفحص) ونكون أمام انتهاك لحرية التعبير حال وضع هذا القيد. والمستوى الثالث من الفحص يتناول "التناسب" أي أن يكون القيد مناسباً لتحقيق الوظيفة الحِمائية ويجب أن يكون أقل الوسائل تدخلاً مقارنة بغيره لتحقيق الهدف المنشود؛ فإذا كان بالإمكان حذف الأخبار التي تتضمن خطاب كراهية مثلاً فلا يُصار إلى حجب الموقع الإلكتروني بأكمله لأن المصلحة المراد حمايتها قد تحققت.[3]

المبادئ الدولية تتقاطع مع " الاختبار ثُلاثي الأجزاء" وإنْ كانت تعرضها على نحو أكثر شمولاً وتفصيلاً، وحيث تؤكد **المبادئ الدولية لتطبيق حقوق الإنسان فيما يتعلق بالاتصالات الرقمية 2013** بشكل واضح وصريح على وجوب أن تطلع **"سلطة قضائية كفؤة ونزيهة ومستقلة"** في كل ما يتصل بالجوانب والإجراءات والأدلة الرقمية (الرقابة القضائية)، ولا يجوز أن تُترك إلى "النيابة العامة" وحدها مثلاً كما هو الحال في نصوص قرار بقانون الجرائم الإلكترونية الفلسطيني. مع الأخذ بالاعتبار أن النيابة العامة ليست سلطة قضائية إذ لا يتوفر فيها ونظراً لطبيعة عملها "الحياد" الذي يعد من أبرز عناصر استقلال القضاء[4].

وهذا ما أكدت عليه صراحة المبادئ التوجيهية الدولية بشأن دور أعضاء النيابة العامة 1990،[5]التي أكدت صراحة بالبند (10)على أن "تكون مناصب أعضاء النيابة العامة منفصلة تماماً عن الوظائف القضائية".

---

[1]. مبادئ جوهانسبرغ بشأن الأمن القومي وحرية التعبير والوصول للمعلومات، ومبادئ سيراكوزا بشأن القيود المتعلقة بالعهد الدولي الخاص بالحقوق المدنية والسياسية، والمبادئ العالمية للأمن القومي والحق في المعلومات (مبادئ تشواني).

[2]. تنص المادة (4) من العهد الدولي للحقوق المدنية والسياسية على الحقوق المطلقة التي لا يجوز تقييدها كالحق في حرية الفكر والوجدان والدين.

[3]. د. عابدين، عصام ، مرجع سابق، ص 13.

[4] . الكيلاني فاروق (1999) ، استقلال القضاء، المركز العربي للمطبوعات، بيروت، دار المؤلف للنشر والطباعة والتوزيع، الطبعة الثانية ، ص (30) وما بعدها.

[5]. المبادئ التوجيهية بشأن دور أعضاء النيابة العامة، اعتمدها مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين المعقود في هافانا من 27 آب/أغسطس إلى 7 أيلول/ سبتمبر 1990.

كما وينبغي وفقاً للمبادئ الدولية 2013 إخطار المُستخدم الذي جرى مراقبة نشاطه الرقمي بعملية المراقبة ما لم يؤدي الإخطار لإفشال الغرض الذي من أجله مُنِح الإذن القضائي بالمراقبة أو لخطر حال وشيك على حياة الإنسان، وفي جميع الأحوال، يتوجب إخطار المستخدم بأمر المراقبة فور انتهاء المبرر أو الخطر، حتى يتمكن المستخدم من استخدام حقه بالمراجعة القضائية والمساءلة والتعويض حال التعسُّف في استخدام السلطة.

وبالنتيجة، فإنه ينبغي إجراء تعديلات جوهرية على قرار بقانون الجرائم الإلكترونية بما يضمن تحري الرقابة القضائية في جميع الجوانب المتعلقة بالأدلة الرقمية والتعامل معها، بما ينسجم مع المعايير الدولية ولا سيما المبادئ الدولية لتطبيق حقوق الإنسان فيما يتعلق بالاتصالات الرقمية 2013 إلى جانب اتفاقية بودابست. وبيان الجوانب الإجرائية في التعامل مع الأدلة الرقمية كما سبق القول. وبما يضمن احترام الحقوق والحريات.

ولا ينبغي أن تقتصر التعديلات التشريعية على الأدلة الرقمية في مجال الإثبات الجزائي، وإنما ينبغي أن تشمل المجال المدني والتجاري أيضاً، للارتباط الوثيق بينهما في مجال الادلة الرقمية ودورها في الإثبات عموماً في العصر الرقمي. إذ لم يعد بالإمكان الركون فقط "للأدلة التقليدية" لا في الإثبات الجزائي ولا الإثبات المدني.

2- في القانون الاساسي المعدل (الدستور)

أكد القانون الاساسي الفلسطيني المعدل (الدستور) على احترام الحق الدستوري في حرية التعبير عن الرأي في المادة (19) والتي جاءت على النحو التالي "لا مساس بحرية الرأي، ولكل إنسان الحق في التعبير عن رأيه ونشره بالقول أو الكتابة أو غير ذلك من وسائل التعبير أو الفن مع مراعاة أحكام القانون".

وتعني عبارة "مراعاة أحكام القانون" الواردة في النص الدستوري وجوب أن يحترم القانون العادي إرادة المشرّع الدستوري الذي كفل هذا الحق الطبيعي في حرية التعبير للناس وعدم الخروج عن إرادته، كذلك لم يكن اختيار رقم المادة (19) ارتجالياً لدى المشرّع الدستوري الفلسطيني كون هذا الرقم (رقم المادة) الذي تمَّ تخصيصه لحرية الرأي والتعبير في الدستور الفلسطيني مطابقٌ للمادة (19) من الإعلان العالمي لحقوق الإنسان وكذلك المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية المتعلقة بحرية الرأي والتعبير في المواثيق الدولية لحقوق الإنسان. والحقُ هو

التأصيلُ الطبيعي والقانوني للحرية، وأمّا الحرية فهي ممارسة هذا الحق الطبيعي والدستوري، دونما اعتبار للحدود، وعلى هذا استقرت إرادة مشرّعنا الدستوري الفلسطيني.[1]

وتجدر الإشارة إلى أن الحق في الحصول على المعلومات (الجيل الثالث من أجيال حقوق الإنسان) يندرج في إطار المادة (19) من القانون الاساسي المعدل؛ وذلك على غرار ما عليه الحال في المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية والتعليق العام رقم (34) الصادر عن اللجنة المَعنِية بحقوق الإنسان في الأمم المتحدة على المادة (19) بشأن الحق في الحصول على المعلومات[2]. وبالتالي فالقولُ إنَّ القانون الأساسي أغفل الحق في الحصول على المعلومات ينطوي على تجنٍ على الدستور وإرادة المشرّع الدستوري.

إنَّ انتهاك حرية التعبير عن الرأي بمختلف أشكالها بما يشمل الجرائم الإلكترونية التي تقتحم تخوم حرية التعبير عن الرأي وتُخالف المواثيق الدولية لحقوق الإنسان التي جرى عرضها في هذا الورقة وأحكام القانون الاساسي (الدستور) يعني أننا حتماً أمام "جريمة دستورية" موصوفة في المادة (32) من القانون الاساسي لا تسقط بالتقادم وتستوجب المساءلة والمحاسبة وإنصاف الضحايا (الانتصاف الفعّال)، وهذا ما أكدته المادة (32) التي جاءت بالآتي "كل اعتداء على أي من الحريات الشخصية أو حرمة الحياة الخاصة للإنسان وغيرها من الحقوق والحريات العامة التي يكفلها القانون الاساسي أو القانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وتضمن السلطة الوطنية تعويضاً عادلاً لمن وقع عليه الضرر".

كما وينبغي الانتباه إلى أن أي تقييد يرد على الحريات الإعلامية بموجب القانون الاساسي (المادة 27 فقرة 3) يتطلب توفر شرطين دستوريين في آن معاً؛ الأول وجود نص في القانون والثاني وجود "حكم قضائي" وإرادة مُشرّعنا الدستوري واضحة وحاسمة في هذا الشأن (وفقاً للقانون "و" بموجب حكم قضائي) والحُكم القضائي هو الحُكم الفاصل في الدعوى وليس القرار الصادر في مسار الدعوى، حِرصاً من المشرّع الدستوري الفلسطيني على "ضمانات المحاكمة العادلة" والحالة تلك، وبالتالي فإننا سنرى في تحليل واقع الجرائم الإلكترونية أمام النيابة العامة والقضاء بأن قرارات حجب المواقع الإعلامية قد خالفت أحكام الدستور.[3]

---

[1]. د. عابدين، عصام، مرجع سابق، ص 15.

[2]البنود (18) و (19) من التعليق العام رقم (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة بشأن المادة (19) من العهد.

[3]. د. عابدين، عصام ، مرجع سابق، ص 16.

3- في القرار بقانون بشأن مكافحة الجرائم الإلكترونية وتعديلاته

أبرز الانتهاكات التي وردت في نصوص هذا القرار بقانون تمثلت في؛ تعدد وحدات الجرائم الإلكترونية دون إشراف ورقابة قضائية واضحة، وإمكانية الحصول على معلومات المُشترك من مُزوّد الخدمة بطلب من النيابة فقط دون أمر قضائي، وإمكانية الحصول على الأجهزة والبيانات والمعلومات الإلكترونية وبيانات المرور وتفتيش وسائل تكنولوجيا المعلومات بطلب من النيابة دون أمر قضائي، وإمكانية حجب المواقع الإلكترونية بطلب من النائب العام بناءً على محاضر الأجهزة الأمنية خلال (24) ساعة وقرار من قاضي الصلح دون ضمانات محاكمة عادلة، بل واعتبار أيّ فعل يُشكل جريمة بموجب أيّ تشريع نافذ جريمة إلكترونية إذا ارتُكب باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات وبأيّ شكل من الاشتراك الجُرمِي!

ولا شك، أن النيابة العامة وهي الجهة التي أشرفت على إعداد مشروع الجرائم الإلكترونية قد حرصت على منح نفسها صلاحيات هائلة في نصوص هذا القرار بقانون، دون أوامر قضائية، من خلال استخدام عبارة "النيابة العامة أو القضاء" الواردة على نحو مُتكرر في نصوص قرار بقانون الجرائم الإلكترونية 2018، الأمر الذي جعل العديد من النصوص الموضوعية والإجرائية الواردة فيه مخالفة للاتفاقيات والمعايير الدولية؛ وبخاصة العهد الدولي الخاص بالحقوق المدنية والسياسية، واتفاقية بودابست المتعلقة الجرائم الإلكترونية، والمبادئ الدولية بشأن تطبيق حقوق الإنسان فيما يتعلق بالمراقبة على الاتصالات الرقمية لسنة 2013.[1]

أشارت التقارير سابقة الذكر الصادرة عن المركز الفلسطيني للتنمية والحريات الإعلامية (مدى) في توصياتها على المستوى التشريعي والسياساتي إلى أهمية وضرورة تعديل قرار بقانون الجرائم الإلكترونية رقم 2018 وإقرار قانون حق الوصول إلى المعلومات إلى جانب المساءلة والمحاسبة على انتهاكات حرية التعبير عن الرأي والحريات الإعلامية[2]. في حين لم تتطرق التقارير السنوية الصادرة عن الهيئة المستقلة لحقوق الإنسان خلال الأعوام 2018 -2021 إلى مدى الحاجة لإجراء تعديلات على قرار بقانون الجرائم الإلكترونية رقم (10) لسنة 2018 النافذ ومدى انسجامه مع المعايير الدولية لحقوق الإنسان لا سيما العهد الدولي الخاص بالحقوق المدنية والسياسية، واتفاقية بودابست (مجلس أوروبا) بشأن الجرائم الإلكترونية 2001 وتعديلاتها في مختلف جوانبها الموضوعية والإجرائية، والمبادئ الدولية لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات

[1]. د. عابدين، عصام ، مرجع سابق، ص 17.
[2]. المركز الفلسطيني للتنمية والحريات الإعلامية (مدى)، انتهاكات الحريات الإعلامية في فلسطين، التقرير السنوي 2021، ص (28).

2014 (اجتماع بروكسل واجتماع ريو دي جانيرو) والتي جرى إطلاقها رسمياً في مجلس حقوق الإنسان التابع للأمم المتحدة في جنيف.

تطبيق قرار بقانون الجرائم الإلكترونية 2018، في الواقع العملي؛ والمقصود الاعتقالات التي تجري على خلفية الجرائم الإلكترونية، يرتكز بشكل "واسع النطاق" على نص المادة (45) من القرار بقانون؛ والتي جاءت بالآتي "كل من ارتكب فعلاً يشكل جريمة بموجب أي تشريع نافذ باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات، أو اشترك فيها أو تدخل فيها أو حرض على ارتكاب ها، ولم ينص عليها في هذا القرار بقانون، يعاقب بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع".

وقد أكد التعليق العام رقم (34) الصادر عن اللجنة المَعنِية بحقوق الإنسان في الأمم المتحدة على أنه يجب أن تُصاغ قوانين التشهير بعناية لضمان الامتثال للمادة (3/19) من العهد (الاختبار ثُلاثي الأجزاء) وإلا تُستَخدم من الناحية العملية لخنق حرية التعبير. وأن تلتزم بضمانات المحاكمة العادلة .. وينبغي على الدول أن تنظر في نزع الصفة الجُرمية عن التشهير. ولا ينبغي بأيّ حال الإقرار بتطبيق القانون الجنائي إلا في أشد الحالات خطورة وإلا تكون عقوبة السجن هي العقوبة المناسبة على الإطلاق.[1]

وفيما يتعلق بالتعديلات التي جرت على قرار بقانون الجرائم الإلكترونية 2018 بموجب القرار بقانون رقم (38) لسنة 2021 المنشور في الجريدة الرسمية عدد (186) بتاريخ 2021/12/23 فإنَّ معظم نصوصه (29 مادة) لا علاقة لها بالجرائم الإلكترونية ومجالها الوارد في العهد الدولي الخاص بالحقوق المدنية والسياسية والتعليق العام (34) الصادر عن اللجنة المَعنِية بحقوق الإنسان، واتفاقية بودابست المتعلقة الجرائم الإلكترونية، والمبادئ الدولية بشأن تطبيق حقوق الإنسان فيما يتعلق بالمراقبة على الاتصالات، والمعايير ذات الصلة.

يهدف هذا التعديل 2021 إلى "دمج" قرار بقانون الاتصالات وتكنولوجيا المعلومات رقم (37) لسنة 2021 بقرار بقانون الجرائم الإلكترونية؛ وهذا واضحٌ في المادة (2) التي نصت على أن يُعدّل عنوان القانون الأصلي (الجرائم الإلكترونية) ليُصبح "قرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات"، كما أن المغزى من عملية الدمج (قرار بقانون الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات) يتمثل إلى فرض نصوص "تجريمية وعقابية" تطال قرار بقانون الاتصالات وتكنولوجيا المعلومات رقم (37) لسنة 2021 كون هذا

[1] البند (47) من التعليق العام رقم (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة بشأن المادة (19) من العهد.

القرار بقانون يخلو من نصوص تجريم وعقاب، وبذلك، تُهيمن نصوص التجريم والعقاب على القرارين بقانون في آن معاً بحصيلة عملية الدمج. وفيما يبدو أن شركة الاتصالات هي المُستفيد الأكبر من التعديلات التي جرت على قرار بقانون الجرائم الإلكترونية عام 2021.[1]

يرى الباحث هنا أن تلك النصوص القانونية التي تهدف تحصين عقد امتياز شركة الاتصالات المخالف لأحكام القانون الاساسي الفلسطيني المعدل (مادة 94) لا علاقة لها لا من قريب ولا من بعيد بالجرائم الإلكترونية. ومن الواضح، أيضا، أنَّ الاعتقاد بأن التعديل على قانون العقوبات وقانون المطبوعات والنشر يجعل واقع الجرائم الإلكترونية مُنسجماً مع المواثيق الدولية يحتاج مراجعة.[2] هناك حالة من "الفوضى التشريعية" ينبغي التعامل معها، بما يكفل بيان الجوانب الموضوعية والإجرائية للأدلة الرقمية؛ وعلى نحو منسجم مع المعايير الدولية.

4- في قانون الاجراءات الجزائية رقم 3 لسنة 2001، وتعديلاته.

أكدت المادة (206) من قانون الاجراءات الجزائية رقم 3 لسنة 2001 على ما يلي : " تقام البينة في الدعاوى الجزائية بجميع طرق الإثبات، إلا إذا نص القانون على طريقة معينة للإثبات ..".

يتضح من خلال النص المذكور أن المشرع الفلسطيني لم يفرق في الإثبات بين الأدلة التقليدية والأدلة الرقمية، حيث ورد النص على نحو عام ومطلق، والمطلق يؤخذ على إطلاقه ما لم يرد عليه تقييد. ما يعني من حيث المبدأ بأن النص المذكور يعترف بالدليل الرقمي في الإثبات في المجال الجزائي. وإن كان قانون الاجراءات الجزائية لسنة 2001 لم ينظم الاجراءات المتعلقة بالأدلة الرقمية في نصوصه وأحكامه القانونية.

وبالرجوع إلى التعديل الذي جرى على المادة (229) من قانون الاجراءات الجزائية رقم (3) لسنة (2001)، من خلال المادة (14) من القرار بقانون رقم (7) لسنة (2022)،[3] فقد نص هذا التعديل على إضافة فقرتين جديدتين تحملان الرقم (5 و6) على النحو الآتي:

" 5. يكون استخدام التقنيات والوسائل التكنولوجية الحديثة في مجال الصوت والصورة وجوبياً من قبل النيابة العامة ومن قبل المحكمة حال سماع أقوال المجني عليه في الجرائم الواقعة على العرض، وكذلك في حالة سماع الشاهد الذي لم يتم الخامسة عشرة من عمره، إلا إذا تعذر ذلك لأي سبب

---

1. د. عصام عابدين، مرجع سابق، ص 20.
2. د. عصام عابدين، مرجع سابق، ص 21.
3 . انظر المادة (14) من القرار بقانون رقم (7) لسنة (2022) بشأن تعديل المادة (229) من قانون الاجراءات الجزائية رقم 3 لسنة 2001، المنشور في الجريدة الرسمية (الوقائع الفلسطينية)، عدد ممتاز (26)، بتاريخ 2022/03/06.

كان، ويكون استخدامها جوازياً في جميع الحالات الأخرى 6. تخضع الأدوات المستخدمة في التقنية أو الوسيلة التكنولوجية الحديثة بما في ذلك الأشرطة والأقراص المدمجة لإجراءات الحفظ والحماية، للحفاظ على سريتها وخصوصية الشاهد أو المتهم".

وباستعراض التعديل المذكور على قانون الإجراءات الجزائية يتضح بأنه لم يُقدم أيّ جديد على صعيد تنظيم ومعالجة **"الجوانب الإجرائية"** في التعامل مع الأدلة الرقمية على المستوى التشريعي. والغريب في الأمر، أنه وعلى الرغم من إشارة البند (6) من التعديل المذكور إلى خضوع الأدلة الرقمية لإجراءات الحفظ والحماية والحفاظ على السرية والخصوصية إلا أن التعديل المذكور الذي جرى على قانون الإجراءات الجزائية في العام (2022)، لم يتناول تلك الجوانب الإجرائية للتعامل مع الأدلة الرقمية، **فأين هي الإجراءات التي يتحدث عنها البند المذكور في هذا التعديل؟!**

وبذلك نجد أن هذا التعديل الذي جرى على قانون الإجراءات الجزائية (2001) من خلال القرار بقانون المعدل الصادر عام (2022) ما زال يُعاني من ذات الإشكالية التي يُعاني منها قرار بقانون الجرائم الإلكترونية (2018) في المادة (37) التي نصت على أن "يُعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات". أي أن اهتمام القرارين بقانون، القرار بقانون المعدل لقانون الإجراءات الجزائية وقرار بقانون الجرائم الإلكترونية قد انصب على اعتماد الدليل الرقمي في الإثبات الجزائي لغايات **"التجريم"** فقط وليس لغايات مأسسة وتنظيم الدليل الرقمي على نحو متكامل في الإثبات. ومع الأخذ بعين الاعتبار أن قرار بقانون الجرائم الإلكترونية يطال **حرية التعبير عن الرأي، تحت ستار الجرائم الإلكترونية،** خلافاً للقانون الأساسي والمعايير الدولية، فإن **الاعتراف بالدليل الرقمي في الإثبات يخدم عملية التجريم في مجال حرية التعبير!**

كما ونُلاحظ بأن التعديل الذي جرى على قانون الإجراءات الجزائية في العام 2022 قد أحدث حالة من **"الفوضى التشريعية"** في التعامل مع الأدلة الرقمية. حيث نجد أن قانون الجرائم الإلكترونية (المادة 37) يعتبر أن **جميع الأدلة الرقمية تُعتبر من أدلة الإثبات،** بينما نجد أن التعديل الذي جرى على قانون الإجراءات الجزائية (المادة 229 بند 5) يعتبر **استخدام الأدلة الرقمية وجوبي من قبل النيابة العامة والقضاء في "الجرائم الواقعة على العِرض وعند سماع شاهد لم يتم (15) سنة من عمره فقط" وجوازي في جميع الحالات الأخرى من النيابة العامة والقضاء!**

كما أن النص المذكور لم يضع آية أسس أو ضوابط أو معايير للاستخدام "الجوازي" للأدلة الرقمية من النيابة والقضاء في غير جرائم العِرض وشهادة الأطفال تحت سن (15) سنة؟ **فما هي الأسس والمعايير والضوابط لاعتماد أو عدم اعتماد الأدلة الرقمية من النيابة والقضاء في تلك الأحوال؟!**

يؤكد الباحث على الخلل الجوهري المتمثل في "القرارات بقوانين" وخطورتها على الحقوق والحريات وفي مقدمتها الحق في حرية التعبير عن الرأي كما هو الحال في قرار بقانون الجرائم الإلكترونية. علاوة على الخلل الدستوري المتمثل في مخالفة القرارات بقوانين ذاتها للشروط الدستورية الواردة في المادة (43) من القانون الأساسي المعدل (الدستور). وعدم اهتمام تلك القرارات بقوانين بمعالجة "الجوانب الإجرائية" للأدلة الرقمية رغم أهميتها في الإثبات وتشكيل القناعة الوجدانية للقاضي بناءً على أسس وإجراءات واضحة في تلك الجوانب الفنية. كما أن تركيز تلك التشريعات قد انصب على الاعتراف بالأدلة الرقمية لغايات "التجريم" وليس لغايات مأسسة وتنظيم كافة الجوانب المتعلقة بالأدلة الرقمية في الإثبات الجزائي وما يتصل بها في الإثبات المدني. ما يعني أن الاعتراف بالأدلة الرقمية يخدم تجريم حرية التعبير بشكل واضح!

ويجدد الباحث التأكيد على أهمية وضرورة حصر الجرائم الإلكترونية بالجرائم المعترف بها في المعايير الدولية والأوروبية (اتفاقية بودابست) وإلغاء أي نص في قرار بقانون الجرائم الإلكترونية يهدف إلى تجريم حرية التعبير تحت ستار الجرائم الإلكترونية. ووجوب تنظيم جميع الجوانب الإجرائية المتعلقة بالتعامل مع الأدلة الرقمية على مستوى البحث والتحري والضبط والتحريز والحفظ والتخزين والحماية وغيرها في المجال الجزائي، وفي المجال المدني، أي تنظيم متكامل للتعامل مع الادلة الرقمية. وأهمية وضرورة وجود برامج مُستدامة للتدريب وبناء القدرات لمأموري الضبط القضائي وأعضاء النيابة العامة والقضاة على كيفية التعامل مع الأدلة الرقمية، وموازنات مالية لتلك البرامج، لأجل ضمان سلامة وفعالية التعامل معها على الأرض.

المطلب الثاني

التشريعات المقارنة والمواثيق الدولية المتعلقة بالأدلة الرقمية ودورها في الإثبات الجنائي

من أهم انجازات العلم في العصر الحديث هو اختراع الحاسب الآلي أو جهاز الكمبيوتر واتصاله بالشبكة العنكبوتية و / أو الفضاء الإلكتروني (الإنترنت) والذي يتسبب الولوج من خلالها إلى ارتكاب جرائم عابرة للقارات والتي تتسم بالدولية دون الانصرام بأية حواجز أو عوائق حدودية، يصعب كشفها أو ضبطها أو الحصول على أدلة تثبت وقوع الجريمة الرقمية وطرق التعامل مع مثل هذه الأدلة المستحدثة، ومن هنا كانت الحاجة الملحة للدول بنوعيها اللاتيني وإلانجلوسكسوني لإعادة صياغة وخلق تشريعات من شأنها الحد من ارتكاب مثل هذه الجرائم ومعرفة كيفية التعامل معها، وكذلك كان لا بد من تكاتف الدول والتعاون فيما بينها من اجل مكافحة هذا النوع من الجرائم، وسنقوم بتقسيم هذا المطلب إلى فرعين، سنتطرق إلى أهم التشريعات الدولية في النظامين اللاتيني وإلانجلوسكسوني المتعلقة بالأدلة الرقمية في الفرع الأول، وسنقوم بعرض أهم المواثيق والمؤتمرات الدولية بشأن كيفية التعامل مع الأدلة الرقمية وتبيان دورها في الإثبات الجنائي.

الفرع الأول

أهم التشريعات المقارنة ذات الصلة بالأدلة الرقمية

معظم التشريعات القانونية في النظام اللاتيني مثل فرنسا وبعض الدول التي تبنت سياستها التشريعية مثل مصر والجزائر لم تقم بصياغة نصوص قانونية خاصة فيما يتعلق بقبول الدليل الرقمي، كون أن هذه الدول المندرجة تحت مظلة النظام اللاتيني تستند لمبدأ حرية الإثبات في المسائل الجنائية، وطبقاً لهذا المبدأ يمكن للقاضي الحكم في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته، فالقاضي حر في اللجوء إلى اية طريقة يراها مناسبة للبحث عن الدليل الرقمي ووزنه وتكوين قناعته الشخصية، ومن هنا يتضح لنا انه يمكن للقاضي الجنائي الاستناد إلى الدليل الرقمي لإثبات وقوع الجريمة في مختلف الجرائم التي تم ارتكاب ها عبر الفضاء الإلكتروني.

- **التشريع الفرنسي**

صدر قانون رقم 5 لسنة 1988 بشأن جرائم الغش ألمعلوماتي المرتكبة ضد النظم المعلوماتية، وتضمن هذا القانون، لا سيما نص المادة 462 / 2 والتي جرمت الدخول أو البقاء غير المصرح به للنظام ألمعلوماتي سواء كان الدخول الغير مصرح به كلي ام جزئي، والتي نصت على انه (كل

شخص قام بالدخول أو البقاء بطريقة كلية أو جزئية في داخل نظام معالجة المعلومات، سيعاقب بالحبس الذي لا يقل عن شهرين وغرامة لا تزيد عن خمسين ألف فرنك، أو بإحدى هاتين العقوبتين، وإذا نتج عن الدخول أو البقاء الغير مشروع محو أو تعديل في المعلومات المخزنة في النظام، تكون العقوبة الحبس لمدة تتراوح ما بين شهرين إلى سنتين والغرامة تتراوح ما بين عشرة آلاف جنية إلى مائة ألف قرنك).[1]

كما وعدلت المادة سالفة الذكر في العام 1994 بالمادة 323 والتي أصبحت العقوبة الحبس سنة والغرامة بواقع مائة ألف فرنك فرنسي، وفي حال نتج عن الدخول الغير مصرح به محو أو تعديل في المعلومات الموجودة في النظام تكون العقوبة الحبس سنتان والغرامة بواقع مائتي ألف فرنك فرنسي.

وكذلك فقد أجاز المشرع الفرنسي بموجب المادة ذاتها ملاحقة ومسائلة الأشخاص الاعتباريين حال ارتكاب هم جرائم رقمية في ضوء القواعد العامة المتعلقة بملاحقة الأشخاص الاعتبارية الواردة في المادة 121 من قانون العقوبات الفرنسي.

ويرى البعض انه بالرغم من أن هذا النص يمثل خروجاً عن القواعد العامة، بحيث يعاقب على الأعمال التحضيرية للجريمة التي تسبق البدء في التنفيذ المادي لها، فانه على القواعد الخاصة بنص خاص ذلك على أساس رغبة المشرع الفرنسي في تقرير نوع من الحماية الوقائية لنظم المعلومات من مخاطر الاعتداء لمثل هذه الجرائم.[2]

ويرى البعض أن المادة (323) تعالج جريمتين مختلفتين من ناحية الركن المادي، ذلك أن المشرع يفرق ما بين الدخول من ناحية والبقاء من ناحية أخرى داخل نظام المعالجة الآلية للبيانات.[3]

ولم يحدد المشرع الفرنسي وسيلة الدخول إلى النظام، وبالتالي يجوز الدخول بأية وسيلة، مثل الدخول عن طريق كلمة السر الحقيقية عندما يكون الجاني غير مخول له باستخدامها أو استخدام برامج مشفرة خاصة، أو عن طريق استخدام الرقم الكودي لشخص أخر، أو الدخول من خلال شخص مسموح له الدخول سواء تم ذلك عن طريق شبكات الاتصال التليفونية أو محطات طرفية Terminal سواء محلية أو عالمية.[4]

---

[1]. المادة (462 / 2) من القانون رقم 5 لسنة 1988 بشأن جرائم الغش ألمعلوماتي الفرنسي.

[2]. د. القهوجي، علي عبد القادر (2000)، الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، الإمارات، ص 877.

[3]. د. تمام، احمد حسام طه (2000)، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي): دراسة مقارنة، دار النهضة العربية للنشر والتوزيع، القاهرة، ص 262.

[4]. أعزان، أمين (2009)، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، ص 101.

- **التشريع البلجيكي**

من بين التشريعات الحديثة التي أشارت إلى جرائم الاعتداء على نظم المعلومات الآلية للمعطيات، التشريع الجنائي البلجيكي بعد تعديله بالقانون الصادر بتاريخ 2000/11/28، حيث أضيف إلى قانون العقوبات البلجيكي فصل جديد هو الفصل التاسع المكرر، وقد تضمن هذا الفصل مادة جديدة هي المادة 6 مكرر، التي تضمنت في فقرتها الأولى مسألة الدخول أو البقاء غير المصرح بها في النظام الإلكتروني.[1]

ونشير إلى أن القانون البلجيكي الصادر بتاريخ 2000/11/28 بشأن الإجرام ألمعلوماتي، تضمن مجموعة من التعديلات تخص قانون العقوبات، وقانون الإجراءات الجنائية، والجدير بالذكر أن ما يهمنا في هذا القانون ارتباطاً بموضوع هذا الفصل هو المادة 6 التي تطرقت لحماية نظم المعالجة الآلية للمعطيات لكل صور الاعتداء سواء بالاختراق أو محو أو تعديل البيانات الموجودة داخل النظام الإلكتروني، بحيث نصت المادة 6 على أن يضاف إلى الكتاب الثاني من قانون العقوبات البلجيكي عنوان تاسع مكرر تحت عنوان "الخروقات ضد سرية النظم المعلوماتية والمعطيات المخزنة أو المعالجة أو المرسلة عبر هذه النظم"، وتتضمن المادة 6 من القانون الجديد مادتين هما المادة 550 مكرر و 550 مكرر 3 .[2]

- **التشريع الانجليزي**

تم استخدام قانون PACE لعام 1984 لتأسيس وتقييم الأدلة الرقمية في المحكمة، ولكن هذا القانون ينطبق على انجلترا وويلز وليس اسكتلندا، تم تطبيق CMA لعام 1990 (بصيغته المعدلة بموجب قانون الشرطة والعدل لعام 2006)، عند ظهور قضايا جرائم الكمبيوتر في محاكم المملكة المتحدة، ويتبع الفاحصون عادةً المبادئ التوجيهية التي تصدرها رابطة كبار ضباط الشرطة (ACPO) لتوثيق الأدلة وسلامتها، تم تحديثها إلى الإصدار 5 في أكتوبر 2011 عندما تم استبدال الأدلة المستندة إلى الكمبيوتر بالأدلة الرقمية التي تعكس تطور التحقيق في حوادث أمن المعلومات في سياق أوسع.

وهذه المبادئ هي :

المبدأ 1- يجب أن لا يغير أي إجراء تتخذه وكالات إنفاذ القانون، الأشخاص العاملون في تلك الوكالات أو وكلائهم، البيانات التي يمكن الاعتماد عليها لاحقاً في المحكمة.

---

1. أعزان، أمين ، مرجع سابق، ص 102.
2. أعزان، أمين ، مرجع سابق، ص 103

المبدأ 2- في الحالات التي يجد فيها الشخص انه من الضروري الوصول إلى البيانات الأصلية، يجب أن يكون ذلك الشخص مختصاً بالقيام بذلك ويكون قادراً على تقديم أدلة تشرح أهمية أفعالهم والآثار المترتبة عليها.

المبدأ 3- يجب إنشاء والحفاظ على سجل لجميع العمليات المطبقة على الأدلة الرقمية.

المبدأ 4- يتحمل الشخص والمسؤول عن التحقيق المسؤولية الكاملة عن ضمان التقيد بالقانون وهذه المبادئ.[1]

ومن الجدير بالذكر انه يتم اللجوء إلى هذه المبادئ التوجيهية واستخدامها وقبولها في انجلترا واسكتلندا، لكن القانون لم يشترط استخدامها ولم ينص عليها صراحةً، إلا انه يمكن استخدامها بشكل طوعي، والذي يشكل أساسا سليماً لسلامة الدليل الرقمي.

- **التشريع الأمريكي**

بالنسبة للولايات المتحدة الأمريكية قد تناولت مسألة قبول الأدلة الجنائية الرقمية، ومن ذلك على سبيل المثال ما نص عليه قانون الحاسب الآلي الصادر سنة 1984 في ولاية آيوا، وذلك لان الأدلة الناتجة عن الحاسب الآلي تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه، وأيضا ما احتوى عليه قانون الإثبات الصادر في سنة 1983 في ولاية كاليفورنيا، وذلك بأن النسخ المستخرجة من البيانات التي يحتويها جهاز الحاسب الآلي تكون مقبولة بوصفها أفضل وانسب الأدلة المتاحة لإثبات هذه البيانات.[2]

وتشترط المحاكم في الولايات المتحدة الأمريكية لقبول الأدلة الجنائية الرقمية بصفة عامة أن يكون جهاز الحاسب الآلي يؤدي وظائفه بصورة سليمة،[3] وأيضا أن يكون هناك ارتباط بين الواقعة والأشخاص المشتبه فيهم، بالإضافة إلى أن يكون محل ثقة ومعتمد كشرط لقبوله.[4] وعليه يقوم القضاء بتحديد درجة مصداقية وفاعلية هذا الدليل عن طريق إخضاعه لاختبار (دأوبورت) والذي هو عبارة عن اختيار قانوني لتقرير صلاحية الدليل العلمي وصلته بالواقعة الإجرامية، ونشأ هذا

---

1. د. عوض، أمل فوزي احمد (2022)، الاكتشاف الإلكتروني، حجية الأدلة الرقمية في الإثبات بين تحديات القبول وأمن المعلومات، المركز الديمقراطي العربي،، ص 90.
2. طوالبية، علي حسن محمد (2004) ، التفتيش الجنائي على نظم الحاسوب والإنترنت (دراسة مقارنة)، عالم الكتب الحديث، الأردن ، ص 59.
3. أحمد، هلالي، عبد الإله (2004)، حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة) في بحوث مؤتمر القانون والكمبيوتر والإنترنت، المجلد الثاني، الطبعة الثانية، جامعة الإمارات العربية المتحدة، ص 429.
4. المطلب، ممدوح عبد، مرجع سابق، ص 130.

الاعتبار بموجب قرار المحكمة العليا في الولايات المتحدة الأمريكية، والتي أصدرته في قضية (دأوبورت) ضد ميريل دو للصناعات الدوائية في سنة 1993.[1]

وبناء على هذا الاختيار تنحصر مسؤولية القاضي أثناء الجلسة في تحديد سلامة المنهجية المتبعة والطرق الفنية المتخذة في استخلاص الأدلة الجنائية الرقمية،[2] وذلك من خلال استخدام أربعة معايير أساسية، يتمثل المعيار الأول (التجربة والاختيار) في التحقق من انه سبق وان تجربة الطريقة المتبعة في استخلاص الدليل الجنائي الرقمي والحصول على نفس النتائج عند المقاربة، وأما المعيار الثاني (نسبة الخطأ) ويتمثل في التحقق من إمكانية وجود نسبة خطأ محتملة ترافق طريقة استخلاص الدليل، وبالنسبة للمعيار الثالث (النشر)، فهو يتعلق بنشر الطريقة المتبعة في استخلاص الدليل ومراجعتها من قبل مختصين في ها المجال، وأخيراً يتمثل المعيار الرابع (القبول) ويتمثل بقبول طريقة استخلاص الدليل الرقمي من قبل المختصين المنتسبين للمجموعات العلمية والمتخصصة في وضع أنسب الوسائل والأساليب الواجب استخدامها في استخلاص الأدلة الرقمية.[3]

وتجدر الإشارة إلى انه قبل ظهور اختيار (دأوبورت) كانت محاكم الولايات المتحدة الأمريكية تبنت اختيار (فراي) في تقرير صلاحية الدليل العلمي بصفة عامة، والذي صدر بموجب قرار المحكمة العليا للولايات المتحدة الأمريكية في سنة 1923، وكان اختيار "فراي" مقتصراً فقط على معيارين وهما التجربة والاختيار بالإضافة إلى معيار القبول،[4] إلا انه قد بينت عجزه في مواجهة أنواع جديدة من الأدلة العلمية والتي من بينها الأدلة الجنائية الرقمية، مما تحتم على الخبراء والمختصين في إيجاد معايير تتماشى مع تطور الأدلة الجنائية.[5]

ونرى مما سبق أن دور القاضي الجنائي في التشريع الأمريكي قد اقتصر على مراقبة تطبيق الشروط (المعايير) على الدليل الرقمي من الناحية الفنية وطريقة استخلاصه، ويقوم باستبعاد أية أدلة لم تتوافر فيها الشروط التي حددها القانون.

كما طبقت الولايات المتحدة في العديد من محاكمها قواعد الإثبات الفدرالية على الأدلة الرقمية بطريقة مماثلة للوثائق التقليدية، على الرغم من وجود اختلافات مهمة مثل عدم وجود معايير وإجراءات ثابتة، بالإضافة إلى ذلك تميل الأدلة الرقمية إلى أن تكون أكثر ضخامة وأكثر صعوبة في التدمير وتعديلها بسهولة، وتكرارها بسهولة، وربما تكون أكثر تعبيرية، ومتاحة بسهولة اكبر،

---

[1] . Steve Bunting and Wiliam Wei, op cit, p 500- 501.

[2]. المطلب، ممدوح عبد ، مرجع سابق، ص 130.

[3]. المطلب، ممدوح عبد ، مرجع سابق، ص 130.

[4] . Linda Volonia and Reynaldo aza anaza aldia, op cit, p 83.

[5] . Ibid, p 83.

وفي ديسمبر من العام 2006 تم سن قواعد جديدة صارمة داخل القواعد الفدرالية للإجراءات المدنية التي تتطلب الحفاظ على الأدلة المخزنة رقمياً والكشف عنها، فغالباً ما تتعرض الأدلة الرقمية للهجوم بسبب أصالتها نظراً للسهولة التي يمكن بها تعديلها.[1]

كما تقوم الولايات المتحدة الآن بتطبيق قواعد الإثبات الفدرالي على الأدلة في شكل رقمي بطريقة مشابهة تماماً للطريقة التي يتم بها تطبيقها على الأعمال الورقية التقليدية، ومع ذلك تم الاعتراف بالاختلافات من حيث الإجراءات والمعايير المعمول بها، الأدلة الرقمية هي أيضا أكثر ضخامة ويصعب تدميرها فضلاً عن تكرارها أو تعديلها بسهولة أكبر، وعلى الرغم من أن الأدلة الرقمية تتعرض للهجوم بشكل متكرر بسبب وجود مشاكل محتملة في أصالتها، إلا أن المحاكم بدأت الآن في رفض هذه الحجج ما لم يكن هناك دليل على انه تم التلاعب بالأدلة.[2]

- **على مستوى الدول العربية**

بدأ الإدراك بأهمية محاربة الجرائم الرقمية ويتزايد في بعض التشريعات العربية مثل التشريع التونسي الذي كان له فضل السبق بين الدول العربية في سن قانون خاص بالتجارة الإلكترونية، وهو القانون رقم 83 لسنة 2000 الصادر في أغسطس سنة 2000 في شأن المبادلات الإلكترونية، وفي المملكة الأردن ية الهاشمية صدر القانون رقم 85 لسنة 2001 بشأن قانون المعاملات الإلكترونية، وكان قانوناً مؤقتاً، إلا انه أصبح نهائياً بقانون جرائم أنظمة المعلومات، ذات الأمر نلاحظه في الجزائر من خلال المرسوم التنفيذي رقم 256 لسنة 1998 بشأن البريد والموصلات، والمرسوم التنفيذي رقم 307 لسنة 2000 بشأن وضع ضوابط وشروط وكيفية إقامة خدمات الإنترنت واستغلالها، وفي دبي صدر القانون رقم 2 لسنة 2002 بخصوص المعاملات والتجارة الإلكترونية، وفي البحرين صدر المرسوم بقانون رقم 28 لسنة 2002 بشأن المعاملات الإلكترونية، المعدل بالقانون رقم 13 لسنة 2006، وفي مصر اعتد القانون رقم 15 لسنة 2004 بشأن المعاملات الإلكترونية، ثم القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.[3]

وفي دول الإمارات العربية المتحدة جاء القانون رقم 2 لسنة 2002 متعلقاً بمكافحة جرائم تقنية المعلومات، وفي اليمن صدر القانون رقم 40 لسنة 2006 بخصوص أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، وفي المغرب ظهير شريف رقم 129 – 07 – 1 صادر في 19 من ذي

[1] . ISO / IEC 27037; Cybercrime Module 4 on Introduction to Digital Forensics.

[2]. د. عوض، أمل فوزي احمد، مرجع سابق، ص 92.

[3]. مرعي، احمد لطفي السيد (2022)، الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكترونية، جامعة المنصورة، المجلد الثامن، ص 10.

القعدة 1428 (30 نوفمبر 2007) بتنفيذ القانون رقم 05 /53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، وفي سلطنة عمان صدر المرسوم السلطاني رقم 69 لسنة 2008 بإصدار قانون المعاملات الإلكترونية، وفي قطر سن المرسوم بقانون رقم 16 لسنة 2010 بإصدار قانون المعاملات والتجارة الإلكترونية.[1]

الفرع الثاني

أهم المواثيق الدولية المتعلقة بالأدلة الرقمية

بسبب تطور تقنية المعلومات والاهتمام الدولي بموضوع الجرائم الإلكترونية والأدلة الرقمية وطرق استخلاصها وكيفية إثباتها، وقعت معظم الأنظمة الدولية العديد من الاتفاقيات والصكوك الدولية، ولذلك ظهرت الحاجة الملحة لمكافحة مثل هذه الجرائم والطبيعة الخطيرة لها، لا سيما طبيعتها العابرة للحدود، فقد يكون مرتب هذه الجريمة في بلد والمجني عليه في بلد أخر، وكذلك مزود الخدمة في بلد ثالث، ويتضح من ذلك صعوبة ملاحقة مرتكبي الجريمة الرقمية والحد منها، وسنتناول في هذا الفرع أهم الاتفاقيات الدولية والصكوك الخاصة في الجرائم الرقمية.

أولاً: القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء هافانا 1990 بشأن الجرائم ذات الصلة بالكمبيوتر.

يعد هذا القرار من الجهود التي بذلتها الأمم المتحدة حيث عقد هذا المؤتمر في هافانا سنة 1990، وقد حث في قراره على المتعلق بالجرائم ذات الصلة بالكمبيوتر الدول الأعضاء أن تكثف جهودها لمكافحة إساءة استعمال هذا الجهاز وبتجريم تلك الأفعال، واتخاذ الإجراءات التالية متى دعت الضرورة لذلك :

- ضمان أن الجزاءات والقوانين الراهنة بشأن سلطات التحقيق والأدلة في الإجراءات القضائية تنطبق على نحو ملائم، وإدخال تغييرات مناسبة عليها إذا دعت الضرورة لذلك.
- النص على جرائم وجزاءات وإجراءات تتعلق بالتحقيق والأدلة حيث تدعو الضرورة للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو ملائم.[2]

---

[1]. مرعي، احمد لطفي السيد ، مرجع سابق، ص 10.

[2]. . مراد، عبد الفتاح (1998) ، شرح جرائم الكمبيوتر والإنترنت، منشأة المعارف، المجلد ، الطبعة الأولى، الإسكندرية، ص 237.

كما حث الأعضاء الدول على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من اجل مكافحة الجرائم المتصلة بالكمبيوتر بما في ذلك دخولها كأطراف في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الخاصة المرتبطة بهذه الجريمة، ونصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية تنطبق بشكل تام على الأشكال الجديدة للإجرام مثل الجرائم الإلكترونية، وان تتخذ خطوات محددة نحو تحقيق هذا الهدف.

واستمرت الأمم المتحدة في رؤيتها بشان الجرائم الرقمية بصفة عامة وأوصت بضرورة وضع وتطوير :

1- معايير دولية لأمن المعالجة الآلية للبيانات.
2- اتخاذ تدابير ملائمة لحل إشكالية الاختصاص القضائي التي تثيرها الجرائم الرقمية العابرة للحدود أو ذات الطبيعة الدولية.
3- إبرام اتفاقيات دولية تنطوي على نصوص تنظيم وإجراءات التفتيش والضبط المباشر الواقع عبر الحدود، على الأنظمة المعلوماتية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت ذاته لحقوق الأفراد وحرياتهم وسيادة الدول.[1]

ثانياً: اتفاقية برن الدولية لحماية المصنفات الأدبية والفنية.

بهدف حماية حقوق المؤلفين على مصنفاتهم الأدبية بأكثر الطرق فعالية، تم إبرام اتفاقية برن الدولية في 9 سبتمبر عام 1886، والمكملة بباريس في ماي 1896، والمعدلة في برلين في 13 سبتمبر 1908، والمكملة ببرن في 20 مارس 1914، والمعدلة بروما في جون سنة 1928، وبروكسل سنة 1948، وستوكهولم في جويلية عام 1967، وباريس في جويلية عام 1971، حيث تشكل الدول الأطراف في هذه الإتفاقية اتحاداً لحماية حقوق المؤلفين على مصنفاتهم الأدبية والفنية، والتي بموجبها تتمتع برامج الحاسب الآلي " الكمبيوتر" سواء كانت بلغة المصدر أو بلغة الادلة بالحماية باعتبارها إعمالا أدبية وفقاً لما جاء فيها.[2]

[1]. حجازي، عبد الفتاح بيومي ، مرجه سابق، ص 190.
[2]. شرابشة، لندا (2009)، السياسية الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية، الاتجاهات الدولية في مكافحة الجريمة الإلكترونية ، المركز الجامعي، سوق أهراس، ص 246.

ثالثاً: مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات عام 1994 – البرازيل – بشأن جرائم الكمبيوتر.

قامت الدول المعنية بعقد هذا المؤتمر في البرازيل عام 1994 والذي تطرق بشكل كبير إلى تصنيف بعض الجرائم الرقمية كالاحتيال والغش المرتبط بالكمبيوتر عن طريق حذف وتعديل البيانات المعلوماتية، والتزوير الإلكتروني وتعطيل وظائف الكمبيوتر ونظم الاتصالات، وكذلك الدخول غير المصرح به للشبكة العنكبوتية من خلال انتهاك الإجراءات السليمة للدخول.

وكذلك فقد تمخض عن المؤتمر صدور قرار يتضمن جملة من القواعد الإجرائية ذات الصلة بالفضاء الرقمية ومنها :

- القيام بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات وتفتيش الحاسب الآلي.
- التعاون الفعال بين المجني عليهم والشهود وكلك مستخدمي المعلومات من اجل إتاحة استخدام المعلومات للأغراض القضائية.
- اعتراض الاتصالات داخل نظام الحاسب الآلي ذاته وممارسة الرقابة عليها.[1]

رابعاً: قانون الاونستيرال النموذجي

- **قانون الاونستيرال النموذجي بشأن التجارة الإلكترونية**

تنطبق نصوص هذا القانون علة أي من المعلومات التي تكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية، بحيث يتم استلامها أو تخزينها بوسائل الكترونية، ويتم تبادل هذه البيانات من خلال نقلها الكترونياً من حاسوب إلى أخر باستخدام معيار متفق عليه، مع الأخذ بعين الاعتبار تفسير هذا القانون لمصدره الدولي ولضرورة توحيد تطبيقه.[2]

- **قانون الاونستيرال النموذجي بشأن التوقيعات الإلكترونية**

اعتمد هذا النص في 5 جولية من عام 2005 وينطبق هذا القانون حيثما تستخدم توقيعات الكترونية،[3]خاصة بعدما أصبح التوقيع بمفهومه التقليدي لا يستجيب لمتطلبات السرعة والحداثة التكنولوجية، حيث انه أمام هذه التطورات تلاشت وظيفة التوقيع التقليدي ليحل محله التوقيع

---

1. مراد، عبد الفتاح ، مرجع سابق، ص 242.
2. مراد، عبد الفتاح ، مرجع سابق، ص 225.
3. الجنبيهي، منير محمد، الجنبيهي، ممدوح محمد (2006)، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، ص 111 – 115.

الإلكتروني، وهو عبارة عن كود سري أو شفرة سرية يتم الحصول عليها بعد إتباع جملة من الإجراءات.[1]

ولعل هذه الأسباب هي ما دفعت الأمم المتحدة متمثلة في لجنة القانون التجاري الدولي (الاونستيرال) إلى إصدار قانون النموذجي للتجارة الرقمية سنة 1996 والقانون النموذجي بشأن التوقيع الرقمي الصادر سنة 2001 ومعاهدة استخدام وسائل الاتصال الرقمية في العقود الدولية، وإضفاء الحجية القانونية عليها، كما اصدر الإتحاد الأوروبي التوجيه الأوروبي القانون رقم 1999 / 93 في 13 ديسمبر سنة 1999 في بشأن التوقيع الرقمي، وذلك لزم الدول الأعضاء بنقل مضمونه داخل تشريعاته الوطنية في خلال 18 شهر.[2]

خامساً: اتفاقية بودابست (جرائم المعلوماتية والاتصالات)

تم اعتماد الإتفاقية وتقريرها التفسيري من لدن لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة (٨ نوفمبر/ تشرين الثاني 2001 وفتح باب التوقيع على الإتفاقية في بودابست، في ٢٣نوفمبر/ تشرين الثاني 2001بمناسبة المؤتمر الدولي حول الجريمة الإلكترونية، والتي دخلت حيز التنفيذ عام 2004، وحتى اليوم، تم التوقيع على الإتفاقية من قبل 47 دولة من ضمنها الدول السبع وعشرين الأعضاء في الإتحاد الأوروبي ، وتم التصديق عليها من قبل 32 دولة. من الخمسة عشر التي لم يصدقوا على الإتفاقية 9 دول أعضاء في الإتحاد الأوروبي. **وتحمل اتفاقية بودابست ثلاث أهداف وهي : توحيد القانون المحلي الجنائي بشكل موضوعي ، تزويد قانون الإجراءات الجنائية المحلية بالصلاحيات اللازمة للتحقيق وملاحقة الجرائم الإلكترونية وإنشاء سلطة تعاون دولية سريعة وفعالة.**[3]

وكان الهدف من التوقيع على هذه الإتفاقية لمعالجة إشكالية دولية الجريمة الإلكترونية وكونها من الجرائم العابرة للحدود الدولية، لمساعدة الدول على ملاحقة مثل هذه الجرائم وتعقب مرتكبيها والمساعدة على العثور عليهم وإلقاء القبض عليهم، وكيفية ضبط الأدلة الرقمية المتحصلة عن هذه الجرائم، كما رسمت طرقاً واضحة وجب إتباعها بين الدول لكيفية التحقيق في الجرائم الرقمية بين الدول والتي تعهدت الدول الموقعة على التعاون الدولي فيما بينها من اجل محاربة مثل هذه الجرائم، كما بينت الإتفاقية النصوص العقابية للجريمة وأنواعها.

---

1. غنام، شريف محمد (2003)، حماية العلامات التجارية عبر الإنترنت في علاقة بالعنوان الإلكتروني، دار الجامعة الجديدة، ص 194.
2. د. عوض، أمل فوزي احمد ، مرجع سابق، ص 80.
3. تقرير توضيحي لاتفاقية الجرائم الإلكترونية. الفصل الثالث، النقطة 16.

كما أنها قضت في المادة (19) منها بإلزام الدول الأطراف بتبني التدابير والإجراءات التشريعية التي تخول السلطات المختصة الولوج إلى البيئة المعلوماتية، وذلك من اجل تيسير إثبات مثل هذه الجرائم.[1]

وتعتبر هذه الإتفاقية إحدى أكثر المحاولات تنوعاً من اجل تنسيق قوانين جديدة في دول عديدة ضد إساءة استخدام الإنترنت، كما نشير إلى أنها تأتي بعد فترة طويلة من المشاورات بين الحكومات وأجهزة الشرطة وقطاع الكمبيوتر وقد صاغ نصها عدداً من الخبراء القانونيين في مجلس أوروبا بمساعدة دول أخرى.[2]

لقد أخذ الإتحاد الأوروبي بعين الاعتبار الإتفاقية في كل مبادرة تم إطلاقها، ولكن المواقف التي اتخذها الإتحاد الأوروبي تختلف في التركيز على ضرورة الإتفاقية و تشجيع الدول بالانضمام إليها توضيح خيبة أمل الإتحاد بشأن الأعداد القليلة التي قامت بالتصديق خلال المدة الطويلة التي دخلت فيها الإتفاقية حيز التنفيذ. و الاعتراف بالحاجة إلى أدوات بديلة .خطة العمل eEurope 2002، والتي تم تبنيها في العام 2000، قامت بالإشارة سابقا إلى أن المجلس الأوروبي في خضم مناقشة اتفاقية عن الجريمة الإلكترونية و أكدت على أهمية التأكد من حصول هذه المناقشات ومن حصول التعاون حول هذه القضية، وفي المذكرات حول وضع السياسة العامة حول مكافحة الجريمة الإلكترونية ، شجعت الهيئة الدول الأعضاء التي لم تقدم على التصديق على الإتفاقية بعد- " الوثيقة الأوروبية والدولية السائدة في هذا المجال"- لفعل ذلك، كما أن قرار الإطار النظري ذكر أن قرار الإطار النظري سيكون متسق مع المنهجية المتبعة في اتفاقية الجريمة الإلكترونية.[3]

وضع برنامج ستوكهولم بعض الضغط على الدول الأعضاء ، داعيتهم إلي المصادقة على ***اتفاقية بودابست*** في اقرب وقت ممكن، هذا التشجيع تم تكراره في المقترح لـ"الإرشادات القانونية للبوت نت" حيث ان الهيئة و بشكل متواضع شاركت وأعربت عن خيبتها في أعداد دول الأعضاء القليلة التي قامت بالتصديق على الإتفاقية. وعلى الرغم من أن الهيئة كانت تسعى لإضافة تشريع جديد في مقترحها و التي حين يتم تبنيه سوف يفقد الحاجة إلى الدول الأعضاء للمصادقة علي الإتفاقية. كانت الهيئة لا تزال تدفع بالدول الأعضاء إلى فعل ذلك. وعلى الأرجح كان ذلك محاولة لمنع وضع الوثيقتين في تباين وعلى الأغلب بالأخذ في عين الاعتبار حقيقة أن التشريع الأوروبي سيستغرق

---

[1]. صفاء، نصيف (2016) ، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، المجلد الخامس، العدد الثاني، ص 268.

[2]. شرابشة، لندا، مرجع سابق، ص 241.

[3]. مقترح لقرار إطاري للمجلس بشأن الهجمات ضد أنظمة المعلومات. كوم (2002)173، ص.8.

سنوات عدة قبل أن يتم تبنيه. وأشار تقييم الأثر المرافق للمقترح بان على إجراء الإتحاد الأوروبي الأخذ بعين الاعتبار الوثائق الموجودة و لتجنب أي تكرار في الجهد. على الرغم من ذلك ، فان فحص دقيق لـمقترح "الإرشادات القانونية للبوت نت" و اتفاقية الجريمة الإلكترونية، تظهر أنه إلي حد ما يهم القانون الجنائي فإن المقترح مختلف بشكل بسيط عن الإتفاقية. واكبر نقطتي ضعف في الإتفاقية من وجهة نظر الإتحاد الأوروبي هما عدم فعالية نقاط الاتصال لـ 7/24 و حقيقة أن الإتفاقية لا تواجه بشكل خاص الهجمات ذات النطاق الكبير. و لذلك تم تقديم معايير لإزالة هذا القصور في المقترح.[1]

وبالإضافة إلى ما تم ذكره أنفا، فان من منظور الإتحاد الأوروبي أن تعليمات Botnet سيقدم ميزة أخرى وهو أن الدول التسع التي رفضت التصديق على اتفاقية الجريمة الإلكترونية سيكونون ملزمين بتعديل تشريعاتهم حينما تصبح التعليمات حيز التنفيذ. و بما أن التعليمات تحتوي على جميع عناصر القانون الثابتة في الإتفاقية وأكثر فان الهدف من توحيد تشريع الإتحاد الأوروبي سيتم تحقيقه. وعلى الرغم من الإتحاد الأوروبي قد اختار أن يستغل سلطة التشريع التي يمتلكها، فان بالنسبة لباقي العالم فان اتفاقية الجريمة الإلكترونية لم تفقد قيمتها وأهميتها. و على الرغم من كونها قد تم صياغتها قبل عقد من الزمن، فأنها استمرت بالبقاء كأداة فعالة وأكثر سلطة في محاربة الجريمة الإلكترونية، والانضمام إليها يجب أن يكون على أجندة جميع الدول التي لم تقم بذلك ، وذلك للنجاح بملاحقة الجريمة الإلكترونية الدولية.[2]

- **تجريم الأنشطة ذات العلاقة بالبرمجيات الخبيثة (Bot net) عبر اتفاقية بودابست**

شبكات الروبوت هي شبكات من أجهزة الكمبيوتر التي تعرضت للقرصنة المُستخدمة لتنفيذ العديد من عمليات الاحتيال والهجمات الإلكترونية. يتألف مصطلح "شبكة الربوتات" من كلمتي "روبوت" و"شبكة". ويمثل تجميع شبكة الروبوتات مرحلة التسلل في مخطط متعدد الطبقات. وتعمل الروبوتات كأداة لأتمتة الهجمات الجماعية، مثل سرقة البيانات وتعطل الخادم وتوزيع البرامج الضارة.[3]

تستخدم شبكات الروبوتات أجهزتك للاحتيال على أشخاص آخرين أو للتسبب في اضطرابات، وكل ذلك دون موافقتك. وقد تتساءل: "ما هجوم شبكة الروبوتات وما طريقة عمله؟" لشرح تعريف شبكة الروبوتات، سنساعدك على فهم كيفية إنشاء شبكات الروبوت وكيفية استخدامها.

---

1 . برنامج ستوكهولم – أوروبا مفتوحة وآمنة تخدم المواطنين وتحميهم، C 115/01/2010، النقطة 4.4.4.

2. لمضي، محمد أبو (2014)، التبعات القانونية في مجابهة شبكة البرامج الخبيثة، جامعة فلسطين، مدينة الزهراء، غزة، ص 9.

3. شبكة الروبوت، المقصود بشبكة البرمجيات الخبيثة، (تاريخ الدخول : 2023/11/29)، انظر الموقع الالكتروني:
https://me.kaspersky.com/resource-center/threats/botnet-attacks

لقد قامت كلا من استونيا وألمانيا بالتوقيع والمصادقة على اتفاقية الجريمة الإلكترونية. بالإضافة، فان تشريعاتهم متجانسة إلى حد كبير فيما يتعلق بالقوانين والتي تم توحيدها على مستوى الإتحاد الأوروبي مثل الاتصالات الإلكترونية و التجارة الإلكترونية و حماية البيانات الشخصية. و كيف أن الأحكام المنصوص عليها في اتفاقية الجريمة الإلكترونية و تشريع الإتحاد الأوروبي تم نقلهم إلى القوانين الخاصة بالأنظمة المحلية و كيف تم تفسيرهم في سياق مواجهة Botnet كما هو موضح بالأسفل.[1]

مبادرات الإتحاد الأوروبي ذات العلاقة بمكافحة البوت نت botnet تقع بشكل اكبر في إطار إجراءات الإتحاد بما يتعلق بمجتمع المعلومات ككل. حيث يشكلون الإطار النظري القانوني للاتحاد الأوروبي و النصوص القانونية حيث انه لا يوجد إلزام بها من قبل الدول الأعضاء في الإتحاد الأوروبي. يحتوي هذا الجزء من البحث على نظرة عامة مختصرة عن هذه المبادرات التي تتعامل بشكل مباشر و عموما بغير مباشر مع محاربة البرمجيات الخبيثة Botnet وكيف ان هذه المبادرات شكلت الخلفية القانونية للاتحاد الأوروبي بما يتعلق البوت نت Botnetحتى هذا اليوم وما هي النتائج المتوقعة من التطور الحالي في الإتحاد الأوروبي.[2]

في مناقشات اجتماع الهيئة للاتحاد الأوروبي عام 2001 بعنوان "الاتصالات وامن المعلومات :مقترح لنهج السياسة الأوروبية"، صنف الإتحاد الأوروبي ثلاث مجالات لسياسة مختلفة ولكنها مترابطة من ناحية مجابهة التحديات التي يواجها مجتمع المعلومات: سياسة الاتصالات الموجودة حاليا والأطر النظرية لحماية البيانات، السياسة المتعلقة بالجرائم الإلكترونية، والسياسة التي يتم تطويرها والمتعلقة بمعايير شبكة الحاسوب وامن المعلومات(NIS)، والتي تعالج المخاوف المتزايدة من التجسس الإلكتروني (بدافع اقتصادي أو سياسي أو علمي) و الهجمات الإلكترونية المحتملة على البنية التحتية و التي تهدد الأمن القومي.[3]

وتعريف شبكة الحاسوب وامن المعلومات (NIS) قدرة شبكة الحاسوب أو نظام المعلومات على المقاومة إلى حد موثوق به ضد الحوادث العرضية أو الإجراءات الخبيثة التي تهدد وجود و صحة

---

1. لمضي، محمد ابو ، مرجع سابق، ص 9.

2. قانون الإتحاد الأوروبي أو قانون المجتمع يعني مجموعة القواعد التي تعتمدها الجماعة الأوروبية، يتكون قانون المجتمع بشكل أساسي من المعاهدات والأدوات التي اعتمدتها المؤسسات بموجب المعاهدات، مثل اللوائح والتوجيهات، السوابق القضائية لمحكمة العدل هي أيضا أحد مصادر القانون المجتمعي.

- انظر الموقع الإلكتروني الخاص بتعريف قانون الإتحاد الأوروبي، تاريخ الزيارة 2023/12/03 - https://ar.wikipedia.org/wiki

3 . هيئة الاتحاد الأوروبي، الاتصالات وامن المعلومات، مقترح لنهج السياسة الأوروبية، (تاريخ الدخول : 2023/12/03)، الموقع الالكتروني :

http://ec.europa.eu/civiljustice/glossary/glossary_en.htm

وسلامة وسرية البيانات المخزنة أو المنقولة والخدمات ذات الصلة المقدمة من قبل أو يمكن الوصول إليها من خلال هذه الشبكات والأنظمة". ولادة سياسة أوروبية داعمة لمشروع شبكة الحاسوب وامن المعلومات NIS ،أظهر تطور الحاجة لوجود أهمية تفعيل الأمن الإلكتروني ليخدم الأمن القومي ووجب مواكبة هذا التطور على هذا الأساس في الأعوام ما بين 2004-2006 ، تم التنسيق لتطوير نهج لسياسة للاتحاد الأوروبي لحماية أنظمة البنية التحتية الحساسة(CIIP) (مثل، أنظمة التي تتحكم بالجسور والقطارات وشبكات المياه والصرف الصحي ومحطات الطاقة والأنظمة العسكرية) و قد تم تبني التشريع الأول بخصوص حماية أنظمة المعلومات للبنية التحتية الحساسة CIIP في عام 2009.[1]

يبقي البوت نت يشكل تهديداً لمستخدمين شبكة الإنترنت، لذلك يتم استخدام طرق فعالة وجديدة بين الحين والآخر لكبح استخدامه وانتشاره. وحيث تعتبر عمليات الاستيلاء أو الإزالة المباشرة للبوت نت من انجح الطرق المستخدمة لمكافحته. ومع ذلك فإن يجب ان يتم تقديم تقنيات مكافحة البوت نت بعناية لمعرفة مدى قانونيتها. في حين يبقى احتمال نشوء قيود على الإجراءات المضادة لمكافحة البوت نت قائماً من طرف أي مجال قانوني سواء القانون الإداري أو المدني أو الجنائي.

ومن جهة أخرى، إن القانون لا يكتفي بوضع قيود على سلوكيات الأشخاص فقط، وإنما يتطلب أيضا تدخل الجهات المعنية لاتخاذ إجراءات لمكافحة البوت نت في مواقف معينة، في حين أن مثل هذا الالتزام منبثق من خلفية الواجبات العامة للعمل والتصرف مهما كان، حتى ولو بدون إعطاء موضوع البوت نت اهتماما على وجه الخصوص. وبطبيعة الحال، إن مزودي خدمات الإنترنت ووكالات القضاء التنفيذية هم الذين يتحملون العبء الأكبر بهذا الخصوص، على سبيل المثال لنفترض أن شبكة الاتصالات الخاصة بمزود خدمة انترنت مهددة بخطر واضح، هنا يكون واجباً على مزود خدمة الإنترنت إبلاغ المستخدمين عن هذا الخطر، ويكون مطلوباً من قوى القانون التنفيذية أو هيئة الادعاء أن يتخذوا الإجراءات اللازمة في حال ظهرت عناصر الجريمة، إن المسؤولية المدنية عند إبلاغ مزود خدمة الإنترنت المستخدمين بالخطر الواقع تجعل الأمر صعباً على الشخص الذي يقوم باستخدام البوت نت لشن هجومه باستخدامه أجهزة المستخدمين كمنصة للهجوم. وهذا الأمر يقود إلى ضرورة وأهمية تثقيف المستخدمين عن التهديدات التي تحيط بهم

1. رسالة من المفوضية إلى المجلس والبرلمان الأوروبي واللجنة الاقتصادية والاجتماعية الأوروبية ولجنة المناطق - أمن الشبكات والمعلومات: اقتراح لنهج السياسة الأوروبية. كوم (2001)، 298، ص. 3.

على الإنترنت بما فيها البوت نت وإرشادهم إلى استخدام الإجراءات الأمنية اللازمة لحماية بياناتهم على الإنترنت.[1]

- **هيئات الأمم المتحدة (الآليات التعاقدية وغير التعاقدية) والأدلة الرقمية وانتهاك الحقوق**

أولا : فلسطين : رغم قيام السلطة الفلسطينية بإلغاء قرار بقانون الجرائم الإلكترونية رقم (16) لسنة 2017 الذي أثار موجة من الاحتجاجات من قِبل مؤسسات المجتمع المدني الفلسطيني أدت إلى إرسال مذكرتين إلى المقرر الخاص في الأمم المتحدة المعني بالحق في حرية الرأي والتعبير (السيد ديفيد كاي في ذلك الوقت)[2] في شباط وتموز 2017، وقيام الأخير بإرسال مذكرة تفصيلية إلى الحكومة الفلسطينية في آب 2017 بانتهاك القرار بقانون والممارسات التي جرت بالاستناد إليه لأحكام العهد الدولي الخاص بالحقوق المدنية والسياسية (المادة 19) والمعايير الدولية ذات الصلة، ورَدّ الحكومة الفلسطينية بمذكرة تفصيلية في أيلول 2017 وتعهدها بتعديل القرار بقانون المذكور بما يتواءم مع القانون الاساسي والمواثيق الدولية ذات الصلة (البند رقم 15 من المذكرة) وترحيب الهيئة المستقلة لحقوق الإنسان وبعض مؤسسات المجتمع المدني بالتعديلات التي جاء بها القرار بقانون الجديد 2018 بشأن الجرائم الإلكترونية، إلا أن مؤشرات الهيئة المستقلة ومؤسسات المجتمع المدني المعنية برصد ومتابعة انتهاك حرية التعبير والحقوق الرقمية على خلفية الجرائم الإلكترونية تُشير بأن تلك الانتهاكات ما زالت قائمة لا سيما أثناء التطبيق العملي لتلك النصوص المعنية بحرية التعبير والحقوق الرقمية، وسنقوم باستعراض أهم ما جاء في تقارير اللجنة المعنية بحقوق الإنسان في الأمم المتحدة وابرز ما جاء به المقررين الخاصين .

- **مبادئ جوهانسبرغ بشأن الأمن القومي وحرية التعبير والوصول للمعلومات، ومبادئ سيراكوزا بشأن القيود المتعلقة بالعهد الدولي الخاص بالحقوق المدنية والسياسية، والمبادئ العالمية للأمن القومي والحق في المعلومات (مبادئ تشواني).**

الاختبار ثُلاثي الأجزاء؛ اجتياز القيد أو الضابط الوارد على حرية التعبير ثلاث مستويات "بنجاح" للقولِ بانسجامه مع أحكام العهد الدولي للحقوق المدنية والسياسية والمعايير الدولية ذات الصلة وهذا الاختبار "الصارم والمتشدد" يسري على باقي الحقوق التي يُمكن تقييدها في العهد الدولي الخاص بالحقوق المدنية والسياسية، المستوى الأول من الفحص يتناول"القانونية" ويجب اجتيازه بنجاح؛ أي

[1]. لمضي، محمد أبو ، مرجع سابق، ص 17.
[2] . د. عابدين، عصام ، مرجع سابق، ص (38) وما بعدها.

أن يكون القيد الوارد على حرية التعبير منصوصاً عليه في القانون بنص واضح وصريح ولا يستخدم مصطلحات فضفاضة ويمكن للأفراد الحُكم على تصرفاتهم من خلاله. والمستوى الثاني من الفحص يتناول "الضرورة" ويتعلق بمشروعية الغرض من القيد (حماية الحق في الخصوصية مثلاً) وعلى قاعدة إذا كان هناك إمكانية لتوفير تلك الحماية بطرق أخرى لا تحد من حرية التعبير فلا يُصار إلى إعمال هذا القيد (أي يفشل في المستوى الثاني للفحص)، ونكون أمام انتهاك لحرية التعبير حال وضع هذا القيد. والمستوى الثالث من الفحص يتناول "التناسب" أي أن يكون القيد مناسباً لتحقيق الوظيفة الحِمائية ويجب أن يكون أقل الوسائل تدخلاً مقارنة بغيره لتحقيق الهدف المنشود؛ فإذا كان بالإمكان حذف الأخبار التي تتضمن خطاب كراهية مثلاً فلا يُصار إلى حجب الموقع الإلكتروني بأكمله لأن المصلحة المراد حمايتها قد تحققت.

- **هيئات حقوق الإنسان (الآليات التعاقدية)**

- **اللجنة المعنية بحقوق الإنسان ، التعليق العام رقم (34)، CCPR/C/GC/34، البنود رقم (2) و (3) من التعليق العام المذكور، بتاريخ 2011/09/12 .**

حيث أن التعليق العام (34) الصادر عن اللجنة المَعنِية يُمثل شرح اللجنة للمادة (19) من العهد بحصيلة نقاشاتها البنّاء مع الدول الأطراف في العهد، فقد أكد التعليق العام على أن حرية الرأي والتعبير شرطان لا غنى عنهما لتحقيق النمو الكامل للفرد، وهما عنصران أساسيان من عناصر أي مجتمع، ويشكلان حجز الزاوية لكل مجتمع تسوده الحرية والديمقراطية، وحرية التعبير شرط ضروري لإرساء مبادئ الشفافية والمساءلة التي تمثل بدورها عاملاً أساسياً لتعزيز وحماية حقوق الإنسان .[1]

- **البنود (7) و(8) من التعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة، بتاريخ 2011/09/12 .**

التقيّد باحترام حرية الرأي والتعبير مُلزم لكل دولة طرف ككل، بسلطاتها العامة الثلاث التنفيذية والتشريعية والقضائية، وعليها أن تتحمل مسؤولياتها على هذا الصعيد، ويتطلب هذا الالتزام، أيضا، من الدول الأطراف أن تضمن حماية الأشخاص من أية أعمال يقوم بها أفراد بصفتهم الشخصية أو أية كيانات خاصة وتؤدي إلى إعاقة التمتع بحرية الرأي والتعبير. تجدر الإشارة، إلى أنه ينبغي

1. - اللجنة المعنية بحقوق الإنسان ، التعليق العام رقم (34)، CCPR/C/GC/34، البنود رقم (2) و (3) من التعليق العام المذكور، بتاريخ 2011/09/12 .

على الدول الأطراف في العهد موافاة اللجنة المعنية بحقوق الإنسان بالقواعد القانونية الداخلية ذات الصلة والممارسات الإدارية والقضائية والممارسات السياساتية ذات الصلة وغيرها من الممارسات القطاعية المتعلقة بالحقوق التي تخضع للحماية بموجب المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية المتعلقة بحرية الرأي والتعبير.[1]

- **البند (15) من التعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة، بتاريخ 2011/09/12 .**

في مجال الحقوق الرقمية، أكدت اللجنة على أنه ينبغي على الدول الأطراف أن تأخذ بالحسبان مدى تأثير التطورات التي طرأت على تكنولوجيا المعلومات والاتصالات، مثل نظم نشر المعلومات الإلكترونية القائمة على خدمات الإنترنت والهاتف النقال، في إحداث تغيير كبير في ممارسة الاتصالات حول العالم. توجد اليوم شبكة عالمية لتبادل الأفكار والأفكار لا تعتمد بالضرورة على الوسطاء التقليديين لوسائط الإعلام الجماهيري. ينبغي على الدول الأطراف أن تتخذ جميع التدابير الضرورية لتعزيز استقلالية هذه الوسائط الإعلامية الجديدة وأن تضمن سُبل وصول الأفراد إليها.[2]

- **البنود (18) و (19) من التعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة، بتاريخ 2011/09/12 .**

أكدت اللجنة على أن الحق في الوصول إلى المعلومات التي تكون بحوزة السلطات والهيئات العامة مشمولة بحرية التعبير عن الرأي في المادة (19) من العهد.[3]

- **البند (21) من التعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة، بتاريخ 2011/09/12 .**

استعرضت اللجنة في البنود (21) وما بعدها من التعليق العام (34) ما نُسَميه "الاختبار ثُلاثي الأجزاء" للحُكم صحة وسلامة أيّ قيد أو ضابط يتم وضعه على الحق في حرية التعبير عن الرأي بالاستناد لأحكام المادة (19) من العهد والتعليق العام المذكور، وجوهر هذا الفحص الثلاثي، الصارم والمُتشدد، حِماية لحرية التعبير، المحمية بالعهد، يقوم على أنه لا يجوز لأي قيد أن يُعرّض الحق

1. - البنود (7) و(8) من التعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة، بتاريخ 2011/09/12 .
2. - البند (15) من التعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة، بتاريخ 2011/09/12 .
3. – البنود (18) و (19) من التعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة، بتاريخ 2011/09/12 .

نفسه (حرية التعبير) للخطر وأن لا يقلب هذا القيد العلاقة بين "الحق والقيد" وبين "القاعدة والاستثناء.[1]

- **البنود (18) و (19) من التعليق العام رقم (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة بشأن المادة (19) من العهد، بتاريخ 2011/09/12 .**

الحق في الحصول على المعلومات (الجيل الثالث من أجيال حقوق الإنسان) يندرج في إطار المادة (19) من القانون الاساسي المعدل؛ وذلك على غرار ما عليه الحال في المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية والتعليق العام رقم (34) الصادر عن اللجنة المَعنِية بحقوق الإنسان في الأمم المتحدة على المادة (19) بشأن الحق في الحصول على المعلومات.[2]

- **البند (47) من التعليق العام رقم (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة بشأن المادة (19) من العهد، بتاريخ 2011/09/12 .**

قد أكد التعليق العام رقم (34) الصادر عن اللجنة المَعنِية بحقوق الإنسان في الأمم المتحدة على أنه يجب أن تُصاغ قوانين التشهير بعناية لضمان الامتثال للمادة (3/19) من العهد (الاختبار ثُلاثي الأجزاء) وإلا تُستَخدم من الناحية العملية لخنق حرية التعبير. وأن تلتزم بضمانات المحاكمة العادلة .. وينبغي على الدول أن تنظر في نزع الصفة الجُرمية عن التشهير. ولا ينبغي بأيّ حال الإقرار بتطبيق القانون الجنائي إلا في أشد الحالات خطورة وإلا تكون عقوبة السجن هي العقوبة المناسبة على الإطلاق، كما شددت لجنة العهد الدولي؛ على أنه ينبغي إبلاء الاعتبار، على الأقل، فيما يتعلق بالتعليقات على الشخصيات العامة لتجنب المعاقبة على بيانات غير صحيحة نُشرت خطأً أو بدون سوء نية أو جعل هذه المعاقبة غير قانونية. وينبغي الاعتراف بالاهتمام العام بموضوع الانتقاد [حتى وإنْ كان صارخاً صادماً جارحاً ..] باعتباره وسيلة للدفاع. وينبغي أن تتوخى الدول الأطراف الحيطة لتفادي التدابير العقابية والجزاءات المفرطة. وأن تنظر في نزع الصفة الجُرمية عن التشهير. ولا ينبغي في أي حال من الأحوال الإقرار بتطبيق القانون الجنائي إلا في أشد الحالات خطورة وإلا تكون عقوبة السجن هي العقوبة المناسبة على الإطلاق.[3]

---

1. - البند (21) من التعليق العام (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة، بتاريخ 2011/09/12 .
2. - البنود (18) و (19) من التعليق العام رقم (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة بشأن المادة (19) من العهد، بتاريخ 2011/09/12 .
3. - البند (47) من التعليق العام رقم (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة بشأن المادة (19) من العهد، بتاريخ 2011/09/12 .

- **البنود (7) و (21) و (23) و(42) من التعليق العام رقم (34) الصادر عن اللجنة المعنية بحقوق الإنسان بشأن المادة (19) من العهد، بتاريخ 2011/09/12 .**

ومن الضروري، التذكير مُجدداً، والحالة تلك، بما ورد في التعليق العام رقم (34) الصادر عن اللجنة المَعنِية بحقوق الإنسان في الأمم المتحدة على المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية؛ حيث أكدت اللجنة على أن التقيّد بحرية الرأي والتعبير مُلزم لكل دولة طرف "ككل" بسلطاتها العامة الثلاث التنفيذية والتشريعية والقضائية. وتضمن الدولة حماية الأشخاص من أية أعمال يقوم بها أفراد بصفتهم الشخصية أو أي كيانات خاصة تقوم بعرقلة التمتع بحرية الرأي والتعبير. وعدم فرض أية قيود من شأنها أن تُعرض الحق في حرية التعبير للخطر. وعدم فرض أية قيود لتبرير كبح أي دعوة إلى إقامة نظام ديمقراطي مُتعدد الأحزاب وتحقيق مبادئ الديمقراطية وحقوق الإنسان . وأن فرض العقوبات لمجرد توجيه انتقادات للحكومة أو النظام الاجتماعي والسياسي الذي تتبناه لا يمكن أبداً أن يكون بمثابة قيد ضروري على حرية التعبير.[1]

- **البند (10) من تقرير مجلس حقوق الإنسان التابع للأمم المتحدة في قراره الصادر عام 2016 (A/HRC/32/L.20).**

أدان مجلس حقوق الإنسان التابع للأمم المتحدة في قراره الصادر عام 2016 (A/HRC/32/L.20) وتحديداً في البند (10) من القرار التدبير التي تتخذها الدول بقصد منع أو تعطيل الحق في الوصول للمعلومات أو نشرها على شبكة الإنترنت ودعا الدول إلى الامتناع عن هذه التدابير ووقفها باعتبار الوصول إلى الإنترنت حق أساسي من حقوق الإنسان .[2]

- **البنود (333 – 358 – 345) تقرير مجلس حقوق الإنسان التابع للأمم المتحدة في قراره الصادر عام 2020 (CCPR/C/PSE/1) .**

يبدو أن اللجنة المَعنِية بحقوق الإنسان (لجنة العهد) لم تَقْتَنِعْ بما ورد في تقرير دولة فلسطين المتعلق بالعهد الدولي الخاص بالحقوق المدنية والسياسية 2020 (CCPR/C/PSE/1) بشأن حرية التعبير والحريات الرقمية عموماً (البنود 333 – 358) وما ورد بشأن الجرائم الإلكترونية بشكل خاص (البند 345) وغيرها من الحقوق المكفولة في العهد الدولي. سيما وأن التقرير الرسمي لم يُشِرْ إلى أية ممارسات عملية مُرتبطة بقرار بقانون الجرائم الإلكترونية على مستوى أداء الأجهزة الأمنية والنيابة العامة والقضاء ومؤشرات وإحصائيات تُبين مدى التقدُّم الذي أحرزته دولة فلسطين في

---

[1]. - البنود (7) و (21) و (23) و(42) من التعليق العام رقم (34) الصادر عن اللجنة المعنية بحقوق الإنسان بشأن المادة (19) من العهد، بتاريخ 2011/09/12 .

[2]. - البند (10) من تقرير مجلس حقوق الإنسان التابع للأمم المتحدة في قراره الصادر عام 2016 (A/HRC/32/L.20).

مجال تعزيز وحماية حرية التعبير والحقوق الرقمية على الشبكة الإلكترونية. مع الإشارة إلى أن الممارسات العملية تأخذ حيزاً شديد الأهمية في قوائم المسائل (نواقص جوهرية في التقرير قبل النقاش أو قبول الدولة بالإجراء المُبسَّط) وفي الملاحظات الختامية للجنة بحصيلة الحوارات البنّاءة التي تُجريها، وغيرها من لجان الاتفاقيات الدولية، في مقر الأمم المتحدة بجنيف، على التقارير المُقدمة من قِبل الدول الأطراف .[1]

- **مجلس حقوق الإنسان (الآليات غير التعاقدية)**

- **البند (81) من تقرير المقرر الخاص المقدم إلى مجلس حقوق الإنسان بجنيف في العام (2013) – (A/HRC/23/40).**

يؤكد المقرر الخاص في تقريره المقدم إلى مجلس حقوق الإنسان بجنيف في العام 2013 (A/HRC/23/40) في بند الاستنتاجات والتوصيات؛ وتحديداً البند (81) على أنه "ينبغي على الدول أن تنظر إلى مراقبة الاتصالات ووسائل تكنولوجيا المعلومات كعمل تطفلي بدرجة كبيرة ربما يتعارض مع الحق في حرية التعبير والحق في الخصوصية ويهدد دعائم المجتمع الديمقراطي، ويجب أن يكون ذلك حصراً تحت إشراف سلطة قضائية مستقلة. ويجب أن يتضمن القانون ضمانات واضحة عن طبيعة التدابير الممكنة ونطاقها ومدتها الزمنية والأسس اللازمة للأمر بها ونوع الانتصاف الفعّال الذي تتضمنه التشريعات الوطنية.[2]

- **الفقرة (20) من تقرير المقرر الخاص المقدم إلى مجلس حقوق الإنسان بجنيف في العام (2017) - (A/HRC/35/22).**

القوانين التي تُلزم الجهات الخاصة بإنشاء قواعد بيانات كبيرة تشمل بيانات المستخدمين وتكون في متناول الحكومة تُثير شواغل تتعلق بالضرورة والتناسب.[3]

- **البند (56) من تقرير المقررة الخاصة المعنية بتعزيز وحماية الحق في حرية الرأي والتعبير (إيرين خان)، المقدم إلى مجلس حقوق الإنسان بجنيف في تاريخ 2021/07/30 (A/HRC/76/258).**

---

[1]. – البنود (333 – 358 – 345) تقرير مجلس حقوق الإنسان التابع للأمم المتحدة في قراره الصادر عام 2020 (CCPR/C/PSE/1) .

[2]. - البند (81) من تقرير المقرر الخاص المقدم إلى مجلس حقوق الإنسان بجنيف في العام 2013 (A/HRC/23/40).

[3]. - الفقرة (20) من تقرير المقرر الخاص المقدم إلى مجلس حقوق الإنسان بجنيف في العام 2017 (A/HRC/35/22).

في العصر الرقمي، أصبحت الإنترنت الوسيلة الرئيسية للوصول إلى المعلومات وتبادلها، وقد اعترفت هيئات حقوق الإنسان بأن الفجوة الرقمية بين الجنسين عائق رئيسي أمام تمتع النساء والفتيات بالحق في التعبير على قدم المساواة مع غيرهن، وأكد مجلس حقوق الإنسان أهمية تطبيق منهج شامل قائم على حقوق الإنسان لتوفير وتوسيع نطاق الوصول إلى الإنترنت، داعياً جميع الدول إلى سد الفجوة الرقمية بين الجنسين، وتعزيز بيئة تمكينية على الإنترنت تكون آمنة وشاملة للجميع، وجعل المنظور النسائي محورياً في القرارات المتعلقة بالسياسات والأطر التي توجه سياسات تكنولوجيا المعلومات والاتصالات.[1]

- **البنود (81) و (82) و (83) من تقرير المقررة الخاصة المعنية بتعزيز وحماية الحق في حرية الرأي والتعبير (إيرين خان)، المقدم إلى مجلس حقوق الإنسان بجنيف في تاريخ 2023/04/19 (A/HRC/53/25).**

على الرغم من الالتزام الوارد في خطة 2030 بإتاحة شبكة الإنترنت للجميع وجعلها في متناولهم، فرضت الحكومات حالات إغلاق أو إبطاء أو حجبت الاتصال ات المتنقلة لفترات متقطعة أو طويلة في 74 دولة في السنوات الخمس الماضية، وقد حدثت حالات التعطيل في اغلب الأحيان في سياق النزاعات والعمليات المسلحة والاضطرابات السياسية والاحتجاجات الواسعة والانتخابات والامتحانات.

ولا تؤدي حالات تعطيل الإنترنت إلى تقويض حرية الرأي والتعبير والتجمع السلمي فحسب، بل لها أيضا عواقب سلبية وخيمة على الحقوق ألاقتصادية والاجتماعية، فتعطل التعليم والصحة والخدمات الإلكترونية الأساسية الأخرى، فضلاً عن الأنشطة المالية والتجارية والصناعية وحياة الناس اليومية، ففي ولاية "تغراي" في أثيوبيا أدى إغلاق الإنترنت لأكثر من عامين إلى تعطيل الاتصالات والخدمات الاجتماعية الأساسية والمساعدات الإنسانية، وتسببت في محنة كبيرة للسكان المدنيين.

ويشكل قيام الدول بتعطيل متعمد للوصول إلى الإنترنت تدخلاً غير متناسب في الحق في حرية التعبير، وقد اعتبرت آليات الأمم المتحدة لحقوق الإنسان والمحاكم الإقليمية أن الإغلاق الشامل للانترنت والحجب العام للخدمات وترشيحها يشكل انتهاكاً للقانون الدولي الإنسان ي.[2]

---

1. - البند (56) من تقرير المقررة الخاصة المعنية بتعزيز وحماية الحق في حرية الرأي والتعبير (إيرين خان)، المقدم إلى مجلس حقوق الإنسان بجنيف في تاريخ 2021/07/30 (A/HRC/76/258).

2. - البند (81) و (82) و (83) من تقرير المقررة الخاصة المعنية بتعزيز وحماية الحق في حرية الرأي والتعبير، (إيرين خان)، المقدم إلى مجلس حقوق الإنسان بجنيف في تاريخ 2023/04/19 (A/HRC/53/25).

ثانياً: الأردن : أعرب مكتب الأمم المتحدة لحقوق الإنسان عن مخاوف جدية بشأن قانون الجرائم الإلكترونية الجديد الذي سيدخل حيز التنفيذ قريبا في الأردن بتاريخ 15 آب/أغسطس 2023 .

تستدعي الجريمة الإلكترونية، من دون أدنى شكّ، إلى معالجة وتنظيم. لكنّنا نعبّر عن مخاوف جدّية بشأن قانون الجرائم الإلكترونية الجديد الذي من المقرر أن يدخل حيز النفاذ قريبًا في الأردن .

يقيد ويجرم القانون الجديد الأنشطة التي يقوم بها الأفراد والمنظمات على الإنترنت. كما يفرض عقوبات على نشر محتوى قد يسيء إلى مسئولي إنفاذ القانون. من المحتمل أن يؤدي ذلك إلى إسكات الانتقادات وتقويض المساءلة العامة. كما يعاقب على التحايل على العناوين البروتوكوليّة لشبكة الإنترنت ويسمح بإزالة المحتوى أو حظره من قبل السلطات دون إشراف قضائي مناسب.

من بين الجرائم الإلكترونية الفضفاضة والمبهمة في التشريع "الحضّ على الفجور أو إغواء شخص أخر أو التعرّض للآداب العامّة،" "اغتيال الشخصيّة،" "إثارة الفتنة والنعرات أو النيل من الوحدة الوطنية" و "ازدراء الأديان". تستهدف هذه الصيغ محتوى التعبير على الإنترنت، وهي فضفاضة وقابلة للتفسير الواسع ولا تتمثّل لمتطلّبات القانون الدولي لحقوق الإنسان المتعلقة بالشرعية والهدف المشروع والضرورة والتناسب للقيود المفروضة على الحق في حرية التعبير.

ويحدد القانون أحكاما بالسجن تتراوح بين أسبوع وثلاث سنوات، وغرامات ماليّة تتراوح من 423 دولارًا أمريكيًا إلى 105 آلاف دولار أمريكي (300 دينار أردني إلى 75 ألف دينار أردني)، حسب المخالفة.

تتزايد مخاوفنا بشأن القانون نظرًا لتزايد الترهيب والمضايقة واعتقال النشطاء وسط تقلص الفضاء المدني في الأردن . تم استخدام قانون الجرائم الإلكترونية السابق لعام 2015، والذي يحل محله هذا التشريع، لاعتقال العديد من نشطاء حقوق الإنسان والصحفيين بتهم "التشهير".

من إحدى الحالات الأخيرة هي حالة الصحفي الساخر أحمد حسن الزعبي الذي حُكم عليه في 9 أغسطس بالسجن لمدة عام بموجب القانون الحالي لنشره منشورًا على Facebook في ديسمبر الماضي انتقد طريقة تعامل السلطات مع إضراب سائقي الشاحنات.

نحن ندرك حاجة الدول إلى اتخاذ خطوات لمكافحة الجريمة السيبرانية ولكن حماية الأمن وضمان الحريات عبر الإنترنت يجب أن تعامل كأهداف تكميلية.

يجب أن تستند إستراتيجية مكافحة الجرائم الإلكترونية إلى القانون الدولي لحقوق الإنسان وأن تكون واضحة ومستهدفة الجرائم الإلكترونية الأساسية، وتتجنب تحديد الجرائم بناءً على محتوى التعبير عبر الإنترنت.

إن الموافقة السريعة على التشريع - الذي قُدم إلى البرلمان في 15 يوليو، وتمريره في 2 أغسطس وموافقة الملك عليه في 12 أغسطس - يثير مخاوف بشأن الشفافية والمشاركة.

نحث السلطات الأردنية على إعادة النظر في هذا التشريع بهدف ضمان الامتثال للقانون الدولي لحقوق الإنسان ، بما في ذلك العهد الدولي الخاص بالحقوق المدنية والسياسية الذي صادقت عليه الأردن .

كما نحث السلطات على ألاستفادة من الخبرات المتاحة، بما في ذلك من المتخصصين في تكنولوجيا المعلومات والخبراء القانونيين ومنظمات المجتمع المدني ذات الصلة، وكذلك مكتب حقوق الإنسان التابع للأمم المتحدة، لتطوير تشريعات تعالج التهديدات الإلكترونية المشروعة مع حماية حقوق الإنسان الأساسية.

ثالثاً : بنغلاديش : جنيف (31 آذار/ مارس 2023) – دعا مفوّض الأمم المتّحدة السامي لحقوق الإنسان فولكر تورك بنغلاديش اليوم إلى تعليق تنفيذ قانون الأمن الرقمي فورًا.

وشدّد قائلًا: "أعرب عن قلقي البالغ حيال استخدام قانون الأمن الرقمي في جميع أنحاء بنغلاديش بهدف اعتقال الصحفيين والمدافعين عن حقوق الإنسان ومضايقتهم وترهيبهم، وإسكات الأصوات المنتقدة عبر الإنترنت."

وأضاف قائلاً: "أكّرر الدعوة التي وجّهتها إلى السلطات بفرض حظر فوري على استخدام هذا القانون وإصلاح أحكامه بشكل شامل فتتماشى مع متطلبات القانون الدولي لحقوق الإنسان . لقد سبق وقدَّمَت مفوضيّتنا تعليقات تقنية مفصلة بهدف المساعدة في مثل هذه المراجعة."

تم رفع أكثر من 2,000 دعوى بموجب هذا القانون، الذي دخل حيز التنفيذ في 1 تشرين الأول/ أكتوبر 2018. أخرها في 29 آذار/ مارس، وتتعلق بشمس الزمان، وهو صحفي يعمل في أكبر صحيفة يومية في البلاد بروثوم ألو. فتم اعتقاله ومصادرة كمبيوتره المحمول وهاتفه ومعدات أخرى يملكها وذلك أثناء تفتيش منزله. ورُفض طلب خروجه من السجن بكفالة.

ورُفِعَت أيضا دعوى ثانية ضد محرر صحيفة بروثوم ألو، ماتيور الرحمن ومصور أخر. وتستند القضية إلى تقارير أعدّاه بشأن أزمة غلاء المعيشة في بنغلاديش.

وفي شباط/ فبراير، حُكِم على الشاب بوريتوش ساركار بالسجن خمس سنوات بموجب هذا القانون أيضا، بعد اتهامه بإيذاء المشاعر الدينية في منشور له على فيسبوك.

وأشار تورك قائلاً: "أثارت مفوضيّتنا باستمرار مخاوفها حيال أحكام قانون الأمن الرقمي الفضفاضة للغاية وغير المحددة. وقد وعدت الحكومة باعتماد ضمانات تحمي من تنفيذ القانون بشكل تعسفي

أو مفرط ولكنّ هذه الخطوة تبقى غير كافية في ظلّ استمرار عمليات الاعتقال. فالقانون نفسه بحاجة إلى إعادة نظر شاملة."

ودعا المفوض السامي إلى إنشاء هيئة قضائية مستقلة تستعرض جميع الدعاوى المعلقة المرفوعة بموجب قانون الأمن الرقمي بهدف إطلاق سراح المتهمين.

كما أعرب تورك من جديد عن قلقه حيال محاكمة عادل الرحمن خان وناصر الدين آيلان من منظمة Odhikar لحقوق الإنسان التي سُحِب ترخيصها، المتهمَيْن بالإبلاغ الكاذب عن انتهاكات مزعومة لحقوق الإنسان في قضية تعود إلى العام 2013.

الخاتمة

ان الأدلة الرقمية هي أدلة عملية متطورة ناتجة عن ارتكاب جرائم رقمية عبر الفضاء الالكتروني من قبل أشخاص يملكون خبرات فنية وتقنية متخصصة لارتكاب مثل هذه الجرائم، وقد فرضت نفسها كأدلة إثبات جنائية رقمية وتتمتع بقوة ثبوتية وحجية كافية على الرغم من طبيعته التقنية المعقدة وعلى الرغم من انها أدلة غير مادية وغير مرئية يسهل إخفائها وتلفها ومحو آثرها وكذلك يسهل استرجاعها. وأن اغلب جهات الضبط القضائي وأركان ومؤسسات العدالة المختصة قد واجهت صعوبات في كيفية التعامل مع مثل هذا النوع من الأدلة ذات الطابع الرقمي، لما لها من خصائص تميزها عن أدلة الإثبات التقليدية، ونوعز ذلك إلى نقص الخبرات لدى اغلب كوادر العدالة من قضاة وأعضاء نيابة عامة ومأموري الضبط القضائي، وإلى الخلل والثغرات الواردة في التشريعات وخاصة فيما يتعلق بتنظيم المسائل الإجرائية في التعامل مع الأدلة الرقمية، وبما يكفل احترام الحقوق والضمانات الدستورية والقانونية، المكفولة في الاتفاقيات والمعايير الدولية ذات الصلة. الفجوات التشريعية لا تقتصر على الأدلة الرقمية في المجال الجنائي وإنما تطال أيضاً المجال المدني.

الأدلة الرقمية، أدلة تعتمد على الحقائق العلمية، التي لم تكن موجودة في الماضي، والتي بدأت تحتل مكانة مهمة في مجال الإثبات الجزائي، في العصر الرقمي،لما لها من أسس ومصادر علمية، ولذلك فإنه يتوجب على الدول صياغة تشريعاتها بما يضمن تحقيق الأهداف المرجوة كي يتسنى محاربة ومكافحة مثل هذه الجرائم العابرة للحدود، وإرساء أسس التعاون الدولي فيما بينها لتسهيل العمل الإجرائي كالتفتيش وضبط الأدلة الرقمية، مع الأخذ بعين الاعتبار أن تكون هذه التشريعات قائمة على تحقيق التوازن بين مصلحة المجتمع واحترام الدستور وضمان الحقوق الحريات والكرامة، وأن لا تُعرض الحق في الخصوصية للخطر.

النتائج

- لا يوجد تعريف موحد وشامل للدليل الرقمي في مختلف الدول، إلا انه يمكن اختزاله في تعريف جامع على انه عبارة عن بيانات ذات قيمة للتحقيق مخزنة على شكل نبضات مغناطيسية في الأجهزة الإلكترونية، ويتم الحصول عليها عن طريق خبراء فنيين مختصين في المجال التقني من الفضاء الإلكتروني.
- هناك تطور نسبي حاصل على الأدلة الرقمية في المجال الجزائي (قرار بقانون 2018 وتعديلاته 2022 وقانون الاجراءات الجزائية وتعديلاته) على مستوى الاعتراف بالدليل الرقمي كدليل في الإثبات، رغم الإشكاليات التي يثيرها الاعتراف على المستوى التشريعي.
- لم يقتصر التطور النسبي في التعامل مع الأدلة الرقمية في المجال الجزائي، وإنما امتد أيضا إلى المجال المدني والتجاري (قانون البينات وتعديلاته)، وبما يشمل الاعتراف بالأدلة الرقمية في المجال التجاري (الدفاتر التجارية) حيث حمل قانون البينات المعدل في العام 2022 "نصاً مستحدثاً" على قانون البينات الأصلي تمثل في المادة (5) ما يدلل على التطور الحاصل في المجال المدني والتجاري في التعامل مع الأدلة الرقمية. إذ لم يعد بالإمكان الركون على الأدلة التقليدية المدنية أيضاً في العصر الرقمي.
- اقتصرت القرارات بقوانين على الاعتراف بالدليل الرقمي، وتجاهلت اجراءات التعامل مع الدليل الرقمي في المجال الجزائي الذي انصب على تجريم حرية التعبير بعد اقتحام تخومها من خلال القرار بقانون بشان مكافحة الجرائم الالكترونية، خلافا لأحكام الدستور والمعايير الدولية.
- رغم أن الجرائم الالكترونية وما يتصل بها من أدلة رقمية جرائم عابرة للحدود إلا أن المشرع لم يعالج أيضا مشكلة الاختصاص، سواء على المستوى الوطني أو الدولي، وتعتبر إشكالية الاختصاص من أكثر الإشكاليات التي تواجه مثل هذا النوع من الجرائم، والتي يتعذر معها ضبط الأدلة الرقمية بشكل فعال، بسبب وقوع الجريمة في دولة ما وامتداد آثارها لتصل إلى دولة أو دول أخرى.
- القصور التشريعي في التعامل مع الأدلة الرقمية من شأنه أن يمس بالحقوق والحريات العامة وضمانات المحاكمة العادلة المكفولة في القانون الاساسي الفلسطيني المعدل والمعايير الدولية لحقوق الإنسان.
- لا يوجد جهد حقيقي في مجال التدريب وبناء القدرات لمأموري الضبط القضائي وأعضاء النيابة العامة والقضاء في كل ما يتصل بالأدلة الرقمية، بما ينعكس سلباً على سلامة وفعالية التعامل مع الأدلة الرقمية في الممارسات العملية.

- القرارات بقانون بحد ذاتها، التي صدرت في مجال الأدلة الرقمية في ظل غياب المجلس التشريعي، ساهمت بشكل أساسي في المساس بحرية الرأي والتعبير واقتصرت على التجريم في غياب التنظيم الإجرائي .
- هناك قصور في المعالجة المتكاملة للأدلة الرقمية في المجال الجزائي وما يتصل بها من أدلة إثبات رقمية مدنية وتجارية.
- الأدلة الرقمية، مهما علا شأنها في الإثبات الجزائي، يجب أن تخضع للسلطة التقديرية للقاضي والقناعة الوجدانية بالدليل الرقمي، لأن القاضي الجزائي من خلال سلطته التقديرية يمكن له إعمال قواعد قانونية كقاعدة تفسير الشك لصالح المتهم واستبعاد الدليل الرقمي المتحصل بطريقة غير مشروعة.وإن معالجة القصور التشريعي في التنظيم الإجرائي للأدلة الرقمية يُعزز "جودة الدليل" والقناعة الوجدانية للقاضي.

التوصيات

- إلغاء كافة النصوص الواردة في القرار بقانون بشان الجرائم الالكترونية وتعديلاته التي تنال من حرية الرأي والتعبير بمختلف أشكالها وبما ينسجم مع الحقوق والحريات الدستورية والمعايير الدولية لحقوق الإنسان (اتفاقية بودابست وتعديلاتها).
- إجراء تعديلات جوهرية على قرار بقانون الجرائم الإلكترونية بما يضمن تحري الرقابة القضائية في جميع الجوانب المتعلقة بالأدلة الرقمية والتعامل معها، بما ينسجم مع المعايير الدولية (المبادئ الدولية لتطبيق حقوق الإنسان فيما يتعلق بالاتصالات 2013).
- ضرورة معالجة النقص التشريعي المتعلق "بالجوانب الإجرائية" في التعامل مع الأدلة الرقمية في مراحلها كافة، وعدم الاكتفاء باعتبار الأدلة الرقمية مقبولة في الإثبات الجزائي في قانون الجرائم الإلكترونية، ضماناً لجودة الدليل الرقمي، وبما يشمل أيضاً الأدلة الرقمية في مجال الإثبات المدني والتجاري. للارتباط الوثيق القائم بينهما في مجال الإثبات عموماً. وبما ينسجم مع المعايير الدولية.
- ضرورة العمل على بناء قدرات مؤسسات العدالة (أجهزة إنفاذ القانون، النيابة العامة، القضاء) ضمن برامج تدريبية مستدامة في مجال التعامل مع الادلة الرقمية في المجال الجنائي، وفي المجال المدني. نظراً للطابع الفني المتخصص للأدلة الرقمي، وحرصاً على جودتها، وضماناً للحقوق والحريات.
- ضرورة العمل على إدراج موضوع الأدلة الرقمية ودورها في الإثبات الجنائي، والإثبات المدني، في مساقات مختصة في الجامعات والكليات وتدريسها بشكل إجباري، وإدراجها في المعاهد المَعنية بتطوير النيابة العامة، وكذلك المعهد القضائي المعني بتأهيل القضاة في المجال الرقمي، لأجل الاستمرار في مواكبة المستجدات والتعامل تلك الجرائم المستحدثة والمتطورة في هذا العصر الرقمي.
- وقف العمل فوراً بالقرارات بقانون بحد ذاتها، والتي لعبت دوراً كبيراً في انتهاك الحقوق والحريات وفي مقدمتها حرية الرأي والتعبير، علاوة على أنها اعترفت بالدليل الرقمي كدليل إثبات لغايات التجريم فقط وليس لمأسسة وتنظيم الدليل الرقمي على نحو متكامل في الإثبات.
- استعادة الدور الأصيل للمجلس التشريعي صاحب الاختصاص الأصيل وسلطة التشريع واحترام أحكام الدستور، والتحول نحو حياة ديمقراطية، وقيام المجلس التشريعي بمهامه الدستورية في تنظيم كافة الجوانب التشريعية المتعلقة بالأدلة الرقمية.

وفي ختام بحثتنا هذا لا نقول إلا أنَـا"إن أصبنا فمن الله، وذلك فضل الله يؤتيه من يشاء من عباده، والله ذو الفضل العظيم، وإن أخطأنا فمني وحدي، فالبحث عمل بشري والكمال لله وحده، وكل عذري أني اجتهدت وبذلت قصارى جهدي، وأجري على الله، نعم المولى ونعم النصير، ونسأل الله السداد والتوفيق من عنده، له الحمد والشكر ربنا رب العرش العظيم

قائمة المصادر والمراجع

المصادر:

(القرآن الكريم)،

الآية "45" من سورة الفرقان.

المراجع العربية:

أولاً: الكتب الفقهية

سرور، احمد فتحي (1981)، الوسيط في قانون الإجراءات الجنائية، ط4، المجلد الأول، دار النهضة العربية، القاهرة.

قنديل، أشرف عبد القادر (2018)، الوسائل الإلكترونية ودورها في الإثبات الجنائي، دراسة مقارنة ، ط1، دار الجامعة الجديدة للنشر، الإسكندرية.

عبد المطلب، ممدوح عبد الحميد، (2000)، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، دار الفتح للطباعة والنشر، الإمارات، الشارقة).

إبراهيم، خالد ممدوح، (2009)، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية.

د. عابدين، عصام ، (2018)، جهود مؤسسة الحق في مواجهة قرار بقانون الجرائم الإلكترونية. مؤسسة الحق، فلسطين.

منصور، محمد حسين، (2006)، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر.

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

د. حجازي، عبد الفتاح، (2002)، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر.

عريان، محمد علي، (2011)، الجرائم المعلوماتية، دار الجامعة الجديدة لطباعة والنشر والتوزيع، مصر، الإسكندرية.

د. ارحومه، موسى مسعود، (2009)، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، كلية القانون ـ جامعة قاريونس، طرابلس، ليبيا.

د. حجازي، عبد الفتاح بيومي (2007)، الإثبات في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة.

نجيب، هند (2016)، التعاون القضائي الدولي في مجال الجرائم الإلكترونية، المجلة الجنائية القومية، المجلد التاسع والخمسون، العدد الثاني.

الهيتي، محمد حماد (2010)، التحقيق الجنائي والأدلة الجرمية، ط 1، دار المناهج للنشر والتوزيع، عمان.

أحمد، هلالي، عبد الإله، (2000)، التزام الشاهد بالإعلام في الجريمة المعلوماتية، دراسة مقارنة، دار النهضة العربية، القاهرة.

د. عرفة، محمد عبد الحميد (2018)، مدى حجية الأدلة الإلكترونية الرقمية في الإثبات الجنائي – دراسة مقارنة – مجلة كلية الحقوق لبحوث القانونية والاقتصادية، جامعة الإسكندرية.

مراد، عبد الفتاح (1998) ، شرح جرائم الكمبيوتر والإنترنت، منشأة المعارف، المجلد ، الطبعة الأولى، الإسكندرية.

أحمد، هلالي عبد الإله (1997)، حجية المخرجات الكمبيوترية، ط1، دار النهضة العربية، القاهرة.

د. الشاذلي، فتوح، كامل، عفيف، (2003)، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة – منشورات الحلبي الحقوقية، بيروت.

د. أحمد هلالي عبد الإله، (2008)، حجية المواد الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة.

بقدار، عبد القادر كامل ، عبد السلام، محمد نور الدين (2017)، أثر مبدأ المشروعية في حجية الدليل الجزائي في القانون الجزائري، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 14 العدد1.

زغلول، طارق احمد ماهر (2016)، شرح قانون الإجراءات الجزائية العماني، الجزء الثاني، المحاكمة وطرق الطعن في الأحكام، الطبعة الأولى، دار الكتاب الجامعي.

الكيلاني فاروق (1999)، استقلال القضاء، المركز العربي للمطبوعات، بيروت، دار المؤلف للنشر والطباعة والتوزيع، الطبعة الثانية.

أحمد، هلالي، عبد الإله (2004)، حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة) في بحوث مؤتمر القانون والكمبيوتر والإنترنت، المجلد الثاني، الطبعة الثانية، جامعة الإمارات العربية المتحدة.

د. القهوجي، علي عبد القادر (2000)، الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، الإمارات.

د. تمام، احمد حسام طه (2000)، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي): دراسة مقارنة، دار النهضة العربية للنشر والتوزيع، القاهرة.

د. عوض، أمل فوزي احمد (2022)، الاكتشاف الإلكتروني، حجية الأدلة الرقمية في الإثبات بين تحديات القبول وأمن المعلومات، المركز الديمقراطي العربي، جامعة عين شمس، الطبعة الأولى، مصر.

طوالبية، علي حسن محمد (2004)، التفتيش الجنائي على نظم الحاسوب والإنترنت (دراسة مقارنة)، عالم الكتب الحديث، الأردن .

مرعي، احمد لطفي السيد (2022)، الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكترونية، جامعة المنصورة، المجلد الثامن.

الجنبيهي، منير محمد، الجنبيهي، ممدوح محمد (2006)، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية.

غنام، شريف محمد (2003)، حماية العلامات التجارية عبر الإنترنت في علاقة بالعنوان الإلكتروني، دار الجامعة الجديدة.

المعايطة، منصور عمر، (2009)، الأدلة الجنائية والتحقيق الجنائي، دار الثقافة للتوزيع والنشر، عمان، الأردن .

مصطفى، (2010)، عائشة بن قارة، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن، دار الجامعة، الإسكندرية.

ثانياً: الأطروحات والرسائل الجامعية

احمد، أبو القاسم احمد، (1994)، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، أكاديمية نايف للعلوم العربية والأمنية، الرياض.

د. البشرى، محمد الأمين، (2002)، الأدلة الجنائية الرقمية، المجلة العربية للدراسات الأمنية والتدريب، الرياض، المجلد 17، العدد 33.

الحراق، اسيا، (2017)، الإثبات بالوسائل الإلكترونية.

لميس، بوناب، (2021)، الأدلة الجنائية وحجيتها أمام القضاء الجنائي، رسالة ماجستير. جامعة العربي التبسي، الجزائر.

فراحتيه، خلود، (2021)، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير،جامعة محمد البشير الإبراهيمي.

ليدية، بسام (2017-2018)، الدليل الرقمي في الإثبات الجنائي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة- بجاية، الجزائر.

سوهيل، بن قدوم، ليدية، بسام (2017-2018)، الدليل الرقمي في الإثبات الجنائي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة- بجاية، الجزائر.

العنزي، سليمان بن مهجعة، (2003)، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية.

آمنة، هلال، (2015)، الإثبات الجنائي بالدليل الإلكتروني، مذكرة ماستر، جامعة محمد خيضر، الجزائر.

البشير، سيدي محمد، (2010) دور الدليل الرقمي في إثبات الجرائم المعلوماتية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، السعودية.

دأود، حسن طاهر، (2000)، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية.

كويمينر، مريم ، (2014)، الخصائص القانونية للإثبات الرقمي الجزائي.

هجيرة، سلامة ياسين رجال، (20156- 2017)، الإثبات الجنائي بالأدلة الرقمية، جامعة العربي التبسي، رسالة ماجستير، الجزائر.

المويشر، تركي بن عبد الرحمن، (2009)، بناء نموذج أمني لمكافحة الجرائم المعلوماتية، اطروحة دكتوراه، الفلسفة الأمنية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، السعودية.

هروال، اية نور الهدى، (2021)، الأدلة الرقمية في إثبات الجريمة الإلكترونية، رسالة ماجستير، جامعة ابن خلدون.

بن عزة، أسامة، (2018 – 2019)، سلطة القاضي الجنائي في تقدير الدليل الإلكتروني، رسالة ماجستير، جامعة العربي التبسي- تبسة، الجزائر.

بوبعاية، ابتسام (2021 – 2022)، التحقيق في الجريمة الإلكترونية، رسالة ماجستير، جامعة محمد البشير الإبراهيمي – برج بوعريريج، الجزائر.

أوساسي فؤاد (2019-2020)، دور الدليل الرقمي في الإثبات الجنائي، رسالة ماجستير، جامعة زيان عاشور- الزلفة.

شرابشة، لندا (2009)، السياسية الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية، الاتجاهات الدولية في مكافحة الجريمة الإلكترونية ، المركز الجامعي، سوق أهراس.

د. عرفة، محمد عبد الحميد (2018)، مدى حجية الأدلة الإلكترونية الرقمية في الإثبات الجنائي – دراسة مقارنة – مجلة كلية الحقوق لبحوث القانونية والاقتصادية، جامعة الإسكندرية، العدد الأول.

بلولهي، مراد (2011)، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مذكرة ماستر، جامعة محمد خيضر، الجزائر.

المطلب، طاهري عبد (2014-2015)، الإثبات الجنائي بالأدلة الرقمية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر.

أعزان، أمين (2009)، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس.

خولة عباسي (2014)، الوسائل الحديثة للإثبات الجنائي في القانون الجزائر، مذكرة استر، جامعة محمد خيضر، الجزائر.

بن طايه، عبد الرزاق، (2014)، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مذكرة ماستر، جامعة محمد خيضر، الجزائر.

ثالثاً: البحوث والمقابلات في المجلات العلمية

جيتس، بيل (1998)، المعلوماتية بعد الإنترنت – طريق المستقبل، ترجمة عبد السلام رضوان، مجلة عالم المعرفة، العدد 231، الكويت.

العربي، مصطفى إبراهيم (2016)، دور الدليل الجنائي الرقمي في الإثبات الجنائي، مجلة البحوث القانونية، العدد. المجلد 4، العدد 1، جامعة مصراتة، ليبيا

حمودة، علي محمود (2003)، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ونظمته شرطة دبي، الإمارات العربية المتحدة.

العتيبي، غازي سليمان، (2019 – 2020)، درجة توافر كفايات البحث عن الدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، السعودية.

سعيداني، نعيم، (2012 – 2013)، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، الجزائر.

فرغلي، عبد الناصر محمد والمسماري، محمد عبيد، (2007)، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، جامعة نايف العربية للعلوم الأمنية، الرياض. .

الحمداني، ميسون خلف، (2016)، مشروعية الأدلة الإلكترونية، معهد البحوث و الدراسات العربية، مجلة جامعة النهرين، العدد 2، المجلد 18، مصر.

د. دأوود، حارث عاصم، (2013)، المخاطر الأمنية في بروتوكول الإنترنت، الإصدار السادس، المجلة العربية الدولية للمعلومات، المجلد الثاني، العدد الرابع، السعودية.

د. عابدين، عصام، (2022)، واقع تطبيق الجرائم الإلكترونية في الضفة الغربية بميزان المواثيق الدولية وأحكام الدستور، معهد الحقوق، جامعة بير زيت.

د.عبد العال، أسامة حسين، (2021)، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، المجلد 11، العدد 76، مصر.

بوعناد، فاطمة زهرة (2013)، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة والدراسات القانونية الجزائرية، كلية الحقوق والعلوم السياسية بجامعة سيدي بلعباس.

الجملي، طارق محمد (2009)، الدليل الرقمي في مجال الإثبات الجنائي، ورقة مقدمة إلى ألمغاربي الأول حول المعلوماتية والقانون، ليبيا.

عبد اللطيف، براء منذر كمال، منديل، ناظر احمد (2009)، التعاون القضائي الدولي في مواجهة جرائم الإنترنت، المؤتمر العلمي الأول حول تحولات العام في مطلع الألفية الثالثة، كلية القانون، جامعة تكريت، العراق.

أحمد حمو، علاء عواد، عبد الله، ولاء (2015)، الأدلة الإلكترونية (الجوانب القانونية والتقنية)، أوراق بحثية في القانون ومكافحة الفساد، جامعة بيرزيت- معهد الحقوق.

شهاب، أحمد عبد الحكيم، د. بن مارني، نور عزم الميل (2018)، شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني، مجلة العلوم السياسية والقانون- المجلد 2، العدد 7، المركز الديمقراطي العربي ألمانيا-برلين.

موقع محاماة نت، بحث قانوني حول يقينية الدليل الرقمي كقيد للقاضي الجنائي، مقالة منشورة، تاريخ النشر: 2023/05/24، تاريخ الاطلاع: 2023/11/13، ساعة الاطلاع: 14:50.

د. العمر، احمد محمد (2020)، الدليل الرقمي وحجيته في الإثبات ، مجلة الدراسات الفقهية والقانونية، المعهد العالي للقضاء.

صفاء، نصيف (2016)، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، المجلد الخامس، العدد الثاني.

لمضي، محمد أبو (2014)، التبعات القانونية في مجابهة شبكة البرامج الخبيثة، جامعة فلسطين، مدينة الزهراء.

مريم كويمينر، (2014)، الخصائص القانونية للإثبات الرقمي الجزائي،.

الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، بحث منشور على موقع كلية القانون، جامعة كربلاء.

أشرف زهران، «النقض» توضح سلطة القاضي الجنائي في تقدير الأدلة، مقال منشور عبر الموقع الإلكتروني الخاص لنقابة المحامين المصريين، تاريخ أخر تحديث: 2023/09/18، تاريخ الاطلاع: 2023/11/08.

حجال، صادق (2018)، شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني، مجلة العلوم السياسية والقانون، تصدر عن المركز الديمقراطي العربي ألمانيا-برلين، العدد 70 فبراير 2018-المجلد 78.

د. عابدين، عصام ، ملاحظات مؤسسة الحق على مشروع القرار بقانون المعدل للجرائم الإلكترونية، 25 يناير 2018، منشورة على موقع مؤسسة الحق.

رابعاً: المؤتمرات والندوات العلمية والتقارير

يونس، عمر محمد (2006)، الدليل الرقمي، ندوة لجامعة الدول العربية للتنمية الإدارية، القاهرة.

مطردي، مفتاح بوبكر (2012)، الجريمة الإلكترونية والتغلب على تحدياتها، مؤتمر رؤساء المحاكم العليا في الدول العربية، السودان.

تقرير صادر عن مركز هردو لدعم التعبير الرقمي، (2014)، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة.

تقرير صادر عن مركز هردو لدعم التعبير الرقمي (2014)، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة.

برنامج ستوكهولم – أوروبا مفتوحة وآمنة تخدم المواطنين وتحميهم، (C 115/01/2010، النقطة 4.4.4).

مقترح لقرار إطاري للمجلس بشأن الهجمات ضد أنظمة المعلومات. كوم (2002) - (173).

خامساً: الاتفاقيات والصكوك الدولية

الإتفاقية المتعلقة بالجرائم الإلكترونية (بودابست) 2001 وتعديلاتها، مجلس أوروبا، مجموعة المعاهدات الأوروبية رقم (185)، ويُراجع أيضا التقرير التفسيري لاتفاقية بودابست الصادر عن مجلس أوروبا في 23 نوفمبر/ تشرين الثاني 2001، مجموعة المعاهدات الأوروبية رقم (185).

الإتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن مجلس الداخلية والعدل العرب بتاريخ 2010/12/21 في القاهرة.

اتفاقية برن بشأن حماية المصنفات الأدبية والفنية (لسنة 1886). (اتفاقية)

قانون الاونستيرال النموذجي بشأن التجارة الإلكترونية (1996) مع المادة الإضافية 5 مكررا بصيغتها المعتمدة في عام (1998).

قانون الاونستيرال النموذجي بشأن التوقيعات الإلكترونية (2001).

القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء هافانا 1990 بشأن الجرائم ذات الصلة بالكمبيوتر.

مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات عام 1994 – البرازيل – بشأن جرائم الكمبيوتر.

المبادئ الدولية لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات (2014).

مبادئ جوهانسبرغ بشأن الأمن القومي وحرية التعبير والوصول للمعلومات (1995).

مبادئ سيراكوزا بشأن القيود المتعلقة بالعهد الدولي الخاص بالحقوق المدنية والسياسية.

المبادئ العالمية للأمن القومي والحق في المعلومات (مبادئ تشواني) – (2013).

سادساً: الأحكام القضائية

حكم محكمة النقض الفلسطينية المنعقدة في رام الله في الدعوى الجزائية رقم (77/ 2016) الصادر بتاريخ 2016/04/04.

حكم محكمة النقض الفلسطينية المنعقدة في غزة في الدعوى الجزائية رقم (2003/205) الصادر بتاريخ 2005/10/25.

حكم محكمة النقض الفلسطينية المنعقدة في رام الله الذي يحمل الرقم (2019/140) الصادر بتاريخ 17/06/2019.

حكم محكمة النقض الفلسطينية المنعقدة في رام الله في القضية رقم (2018/599) الصادر بتاريخ 2019/03/05 .

حكم محكمة النقض الفلسطينية المنعقدة في رام الله في القضية رقم (2019/173) الصادر بتاريخ 2019/07/01 .

حكم محكمة النقض السورية الصادر بتاريخ 1968/5/23، مجموعة القواعد القانونية، رقم 15، ص 1.

حكم محكمة النقض السورية الصادر بتاريخ 1964/4/26، مجموعة القواعد القانونية، رقم 13، ص 12.

حكم محكمة النقض السورية الصادر بتاريخ 1964/11/31، مجموعة القواعد القانونية، رقم 52، ص 31

حكم محكمة النقض السورية الصادر بتاريخ 1967/11/12، مجموعة القواعد القانونية، رقم 53، ص 31.

حكم محكمة النقض السورية الصادر بتاريخ 1977/6/22، مجموعة المحامون، س 42، رقم 759، ص 583.

حكم محكمة النقض المصري الصادر بتاريخ 1973/5/23، مجموعة أحكام النقض، س 23، ق 26، ص 97.

حكم محكمة النقض المصري الصادر بتاريخ 1984/11/25، مجموعة أحكام النقض، س 35، ق 185، ص 821.

حكم محكمة النقض الفرنسية في النقض الجنائي الذي يحمل الرقم (13-81. .945)، الصادر بتاريخ 2013/10/22.

حكم محكمة النقض السورية الذي يحمل الرقم (1186) مجموعة القواعد القانونية، الصادر بتاريخ 1963/11/14.

حكم محكمة النقض السورية الصادر بتاريخ 1965/4/20، مجلة المحامون.

حكم محكمة صلح رام الله في الطلب الجزائي رقم (12/ 2019) الصادر بتاريخ 2019/10/17.

سابعاً: القوانين والتشريعات

القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018 م المعدل بالقرارين بقانون ذوات الأرقام (28) لسنة 2020، و(38) لسنة 2021.

قانون الإجراءات الجزائية رقم (3) لسنة 2001 وتعديلاته.

القرار بقانون رقم (17) لسنة 2014 بشأن تعديل قانون الإجراءات الجزائية رقم (3) لسنة 2001، والقرار بقانون رقم (13) لسنة 2018 بشأن تعديل القرار بقانون رقم (17) لسنة 2014 م بشأن تعديل قانون الإجراءات الجزائية رقم (3) لسنة 2001.

قانون البينات الفلسطيني رقم 4 لسنة 2001 الصادر بتاريخ 2001/05/12 .

قانون الجرائم الإلكترونية الأردن ي رقم (24) لسنة 2015 م.

قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018م.

القانون الاساسي الفلسطيني المعدل لسنة 2005.

قانون العقوبات المصري رقم (58) لسنة 1937 وتعديلاته.

القرار بقانون رقم 9 لسنة 2007 بشأن مكافحة غسل الأموال الصادر بتاريخ 2007/10/25.

قانون العقوبات الجزائري المعدل والمتمم، الصادر بالأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق (8) يونيو عام 1966، وتعديلاته.

القانون الفرنسي المدني من القانون رقم (2000/230).

قانون بشأن جرائم الغش ألمعلوماتي الفرنسي رقم (5) لسنة (1988).

ثامناً: هيئات الأمم المتحدة (الآليات التعاقدية وغير التعاقدية).

البند (64) من تقرير حول تعزيز وحماية الحقوق المدنية والسياسية المقدم إلى مجلس حقوق الإنسان التابع للأمم المتحدة في قراره الصادر (2022) - (A/HRC/50/55).

البند (10) من تقرير مجلس حقوق الإنسان التابع للأمم المتحدة في قراره الصادر عام (2016) - (A/HRC/32/L.20).

فقرة (19) من قائمة المسائل المقدمة من اللجنة المعنية بحقوق الإنسان في الأمم المتحدة إلى دولة فلسطين في (19/9/2022) - (CCPR/C/PSE/Q/1) .

التقرير الأولي المُقدم من دولة فلسطين إلى اللجنة المعنية بحقوق الإنسان في الأمم المتحدة بموجب المادة (40) من العهد الصادر عام (2021) - (CCPR/C/PSE/1).

البنود (2)، (3)، (7)،(8)، (15)، (18) و (19)، (21) (23)، (42)، (47)، من التعليق العام رقم (34) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة، بتاريخ 2011/09/12 – (CCPR/C/GC/34).

البنود (333 – 358 – 345) تقرير مجلس حقوق الإنسان التابع للأمم المتحدة في قراره الصادر عام (2020) - (CCPR/C/PSE/1) .

البند (81) من تقرير المقرر الخاص المقدم إلى مجلس حقوق الإنسان بجنيف في العام (2013) - (A/HRC/23/40).

الفقرة (20) من تقرير المقرر الخاص المقدم إلى مجلس حقوق الإنسان بجنيف في العام (2017) - (A/HRC/35/22).

البند (56) من تقرير المقررة الخاصة المعنية بتعزيز وحماية الحق في حرية الرأي والتعبير (إيرين خان)، المقدم إلى مجلس حقوق الإنسان بجنيف في تاريخ 2021/07/30 (A/HRC/76/258).

البنود (81) و (82) و (83) من تقرير المقررة الخاصة المعنية بتعزيز وحماية الحق في حرية الرأي والتعبير (إيرين خان)، المقدم إلى مجلس حقوق الإنسان بجنيف في تاريخ 2023/04/19 (A/HRC/53/25).

تاسعاً: المواقع الإلكترونية

قاموس كامبردج، (2003)، معنى الدليل الرقمي، (تاريخ الدخول : 2023/09/12)، انظر الموقع الالكتروني،

https://dictionary.cambridge.org/dictionary/english/digital.

نظام البروكسي، ويكيبيديا، (تاريخ الدخول: 2023/10/06)، انظر الموقع الالكتروني:

www.+Proxy/wiki/org.wikipidia.m.en//:https

برنامج المخبر لنظام التشغيل Windows، (تاريخ الدخول: 2023/10/06)، انظر الموقع الالكتروني:

www.informer.software.tracer-hack//:https

د.عابدين، عصام (2018)، ملاحظات مؤسسة الحق على مشروع القرار بقانون المعدل للجرائم الإلكترونية، (تاريخ الدخول: 2023/11/23)، منشورة على موقع مؤسسة الحق على الرابط:

https://www.alhaq.org/ar/advocacy/2291.html.

شبكة الروبوت، المقصود بشبكة البرمجيات الخبيثة، (تاريخ الدخول : 2023/11/29)، انظر الموقع الالكتروني:

https://me.kaspersky.com/resource-center/threats/botnet-attacks

تعريف قانون الإتحاد الأوروبي، ويكيبيديا، (تاريخ الدخول: 2023/12/03)، انظر الموقع الإلكتروني :

https://ar.wikipedia.org/wiki.

هيئة الاتحاد الأوروبي، الاتصالات وامن المعلومات، مقترح لنهج السياسة الأوروبية، (تاريخ الدخول : 2023/12/03)، الموقع الالكتروني:

http://ec.europa.eu/civiljustice/glossary/glossary_en.htm.

عاشراً: المقابلات

أ. ناصر جرار، تاريخ المقابلة 2023/09/20، رئيس نيابة مكافحة الجرائم الإلكترونية في دولة فلسطين، مكان إجراء المقابلة – مكتب النائب العام لدولة فلسطين، 2023.

د. فاتح حمارشة، تاريخ المقابلة 2024/03/20، أستاذ القانون في جامعة بيرزيت، محامي وقاضي سابق، مكان إجراء المقابلة - جامعة بيرزيت، 2024.

أ. عمار جاموس، تاريخ المقابلة 2024/05/28، باحث قانوني، الهيئة المستقلة لحقوق الإنسان، مكان إجراء المقابلة – مكتب الهيئة المستقلة لحقوق الإنسان، 2024.

المراجع الأجنبية:

Goodison, Sean E. and Others (2015), Digital Evidence and the U.S. Criminal Justice System, RAND Corporation, US, P.2

Gercke, Marco (2012), Understanding cybercrime: Phenomena, challenges and legal response, ITU publication, Switzerland – Geneva.

Whitcomb, Carrie Morgan (2002), An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vo1.1, no page's number.

Dutelle, Airc W (2017), An Introduction to crime scene Investigation, thired Edition, Jones & Bartleff learning, USA.

Carrier, Brian and Spafford Eugene H. (2003), Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence, Vo1.2.

Law Reform Commission (2009), Documentary and Electronic Evidence, First Published, Dublin.

Ashouri, Aida and Others (2013), An Overview of the Use of digital Evidence in International Criminal Courts, Working Paper, Salzburg Workshop on Cyber Investigation.

Mason, Stephan (2008), International Electronic Evidence, British Institute of International and Comparative law, London

Mason, Stephan (2008), International Electronic Evidence, British Institute of International and Comparative law, London, P. xxxiv.

Prosecutor v. Alfred Musema (2000), ICTR, Trial Chamber I, Case No. ICTR-96-13-T, 27, parper 53.

Eoghan Casey, Digital Evidence and Computer Crime, London: Aca- demic Press, 2000.

Eoghan Casey, Digital Evidence Op. Cit.

Brian Caeeier – Open Source Digital Forensics Tools: The Legal Argument -1- Oct. 2002.

Personal Education, File system Analysis, Brain Carrier –, United states of America, 2005.

Christine Sqarlata & David J. Byer – The Electronic Paper Trail. At 6.

Grobler, Marthie (2012), The Need for Digital Evidence Standardisation, International Journal of Digital Crime and Forensics, 4(2).

Goodison, Sean E. and Others, op.cit,

Debra Littlejohn Shinder, Scene of the cyber crime (Computer Forensic Handbook), Publishing (Inc), United stat Of America, 2002.

Steve Bunting And William Wei, Encase Computer Forensic, Wiley Publishing (inc), United stat Of America, 2006.

International Bar Association (2016), Evidence Matters in ICC Trials, The Global Voice of Legal Profession, United Kingdom.

Aljneibi, Khaled Ali (2014), The Regulation of Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform, PHD Thesis, Bangor University, Wales, UK.

Wilkinson, Sue, Association of Chief Police Officers (ACPO), Good Practice Guide for Computer-Based Electronic Evidence, published by 7safe, Official release version 4.0, United Kingdom, no date of issue.

Casey, Eoghan (2011), Digital evidence and computer crime – Forensic Science, computer and the Internet, Published by Elsevier Inc, USA.

Dutelle, Airc W. (2014), An Introduction to crime scene Investigation, second Edition, Jones & Bartleff learning, USA.

Petit, Robert and Warren, Maria and Akerson, David (2012), Prosecution Mass Atrocities Lessons from the International Tribunals, open society Foundation, Bangkok – Thailand.

Outerbridge, David and Siller, Ezra, The Admissibility of Electronic Evidence, Torys LLP, Toronto.

INTERPOL (2011), European Working Party on Information Technology Crime (EWPITC) – Project on cloud computing.

Law Reform Commission (2009), Documentary and Electronic Evidence, First Published, Dublin.

Steve Bunting and Wiliam Wei, op cit.

Linda Volonia and Reynaldo aza anaza aldia, op cit.

ISO / IEC 27037; Cybercrime Module 4 on Introduction to Digital Forensics.

الملاحق

مقابلة شخصية: أ. ناصر جرار، تاريخ المقابلة 2023/09/20، رئيس نيابة مكافحة الجرائم الإلكترونية في دولة فلسطين، مكان إجراء المقابلة – مكتب النائب العام لدولة فلسطين، 2023.

س/ هل يوجد جهد حقيقي في مجال التدريب وبناء القدرات لأعضاء نيابة الجرائم الالكترونية المتخصصة في كل ما يتصل بكيفية التعامل مع الأدلة الرقمية، بما ينعكس إيجابا على سلامة وقيمة الأدلة الرقمية في الممارسات العملية وصولاً لدوره في الإثبات؟

ج: حيث أن النيابة الالكترونية هي نيابة متخصصة بموجب أحكام القرار بقانون رقم (10) لسنة (2018) وتعديلاته، والتي نص في المادة (١/٣) منه على إنشاء وحدة متخصصة من الأجهزة المتخصصة تحت إشراف النيابة العامة، وكذلك المادة (٢/٣) حيث أوكلت للنيابة العامة وفقاً لاختصاصها النظر في دعاوى الجرائم الإلكترونية، والتي بموجبها أنشأت نيابة الجرائم الالكترونية كنيابة متخصصة بهذا النوع من الجرائم ومنذ إنشائها والعمل جاري على تطوير أداء عمل وكلاء النيابة العامة المكلفين بالتحقيق فيها حيث شمل ذلك عقد العديد من الدورات التدريبية وتنظيم عدة زيارات خارجية للاطلاع على تجارب الدول المجاورة بالإضافة للمشاركة بورشات عمل مع الشركاء بهدف الوصول إلى توحيد العمل بكافة النيابات وهذا ما نتج عنه بالفعل دليل الاجراءات الموحد لنيابة الجرائم الالكترونية مما سهل عمل أعضاء النيابة المكلفين والموظفين الإداريين المساندين.

كما قامت النيابة العامة في العام 2019 بعقد المؤتمر السنوي التاسع الفلسطيني التركي المشترك، بحضور أعمال المؤتمر بمشاركة وحضور 630 شخصا منهم 160 عضو نيابة عامة فلسطينية، و42 مشاركا من الوفد التركي، و45 وفدا دوليا، بمشاركة 22 دولة من بينهم تركيا، والذي كان بعنوان (الأدلة الرقمية: بين مقتضيات التحقيق وحقوق الإنسان)، الذي أقيم تحت رعاية الرئيس محمود عباس، أهمية الدليل الإلكتروني والذي يشكل الدليل الوحيد في إثبات هذا النوع من الجرائم، واتخاذ الإجراءات القانونية المتفق عليها بنصوص القانون ضمانا لصحة الدليل ومواءمته مع الاتفاقيات المتعلقة بحقوق الإنسان والحق في الخصوصية وضمان حرية الرأي والتعبير الذي كفلته أيضا دساتير الدول بما فيها فلسطين.

ومن أهم مخرجات المؤتمر ضرورة سن التشريعات اللازمة في مجال اعتماد الأدلة الرقمية كوسيلة من وسائل الإثبات أمام المحاكم، بما يسهل عمل النيابة العامة والقضاة في معالجة القضايا التي يباشرونها.

وتأكد النيابة العامة بهذا الخصوص على أهمية حماية البيانات والبيئة القضائية مع الأخذ بعين الاعتبار حماية الحقوق الشخصية، بوضع قائمة للدليل الإلكتروني مرتبط بالإجراءات الجنائية الرقمية ويتضمن آلية تخزين البيانات والمعلومات القضائية وحمايتها وإنشاء منتج يتيح للسلطات القضائية الحصول على المعلومات الإلكترونية في مدة قصيرة، ما ينعكس إيجابا على حماية حقوق الإنسان.

حيث أن ما يميز الجريمة الالكترونية عن باقي الجرائم أنها جريمة متطورة عابرة للحدود وسريعة الوقوع وكذلك من السهل على مرتكبيها محو آثارها بسرعة الأمر الذي يتطلب من عضو النيابة مواكبة هذا التطور ومراجعة ما يستجد من جرائم الكترونية ووسائل مستخدمة بارتكابها، حيث لا يجب على عضو النيابة الاكتفاء بالجانب النظري من نصوص قانونية جامدة بل يجب العمل على تطوير قدراته الفنية التي تمكنه بالحد الأدنى من فهم التقارير المعدة من جهات الضبط القضائي المختصين وبالتالي توضيحها بالشكل المطلوب للمحكمة المختصة.

أ. ناصر جرار، تاريخ المقابلة 2023/09/20، رئيس نيابة مكافحة الجرائم الإلكترونية في دولة فلسطين، مكان إجراء المقابلة – مكتب النائب العام لدولة فلسطين، 2023.

مقابلة شخصية، د. فاتح حمارشة، تاريخ المقابلة 2024/3/20، أستاذ القانون في جامعة بيرزيت، محامي وقاض سابق، مكان إجراء المقابلة جامعة بيرزيت، 2024.

س/ بالرجوع إلى المادة (37) من القرار بقانون رقم (10) لسنة (2018) بشأن مكافحة الجريمة الإلكترونية حيث يتبادر للذهن التساؤل التالي: هل يجوز للقاضي الجزائي أن يبني حكم الإدانة على المتهم بارتكابه جريمة الكترونية بناءً على أدلة تقليدية أي إن يقوم بربط المتهم بالتهمة المسندة إليه دون الاعتماد على الأدلة الرقمية سواء كان السبب عدم توافر أدلة رقمية أو انه قام باستبعاد الدليل الرقمي من وزن البينة المقدمة..؟

لا يمكن ربط المتهم بالتهمة المسندة إليه دون الاعتماد على الأدلة الرقمية، إذ بالنظر إلى طبيعة هذه التهمة فإن عدم وجود أدلة رقمية وفنية يُبقي الشك حول قيام المتهم بالجريمة الالكترونية قائما، ولا يمكن بدون الأدلة الرقمية والفنية التيقن من ربط المتهم بالتهمة المسندة اليه، لاحتمالية اختراق حساب المستدعي مثلا أو استعماله من شخص آخر أو غيرها من الشكوك التي لا تزول إلا بوجود دليل رقمي مقنع يمكن من خلاله التيقن من قيام المتهم بالركن المادي للجريمة الإلكترونية، لذلك اعتبرت المادة 37 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية الدليل الناتج بأي وسيلة تكنولوجية من أدلة الإثبات، لأن طبيعة هذه الجرائم لا يمكن التيقن من وقوعها من قبل الشخص المتهم وإزالة الشكوك حول قيامه بها إلا بهذه الأدلة، وإن إدانة المتهم دون وجود هذه الأدلة يعني إدانته بالتهمة المسندة إليه والشك ما زال قائما حول قيامه بها، وهو ما يعتبر خروجا عن القاعدة القاضية بأن الشك يفسر لمصلحة المتهم.

ويشترط في الدليل الرقمي أن يتمتع بالمصداقية الكافية بحيث يؤدي فعلا إلى الوصول إلى الحقيقة التي يفترض بالقاضي الجزائي أنه يسعى إليها، ويكون كذلك عندما يكون هذا الدليل مشروعا، بحيث يتم الحصول عليه بطريقة مشروعة وفقا لأحكام القانون، وأن يكون يقينيا بحيث يدلل فعلا على الوقائع المراد إثباتها، فإن تخلف أي من هذين الشرطين فإن الدليل الرقمي تنتفي عنه صفة المصداقية، ولا يصلح عندها الاعتماد عليه كدليل لإثبات الجريمة الالكترونية ويبقى الشك حول قيام المتهم بالجريمة قائما.

ويفترض عند إثبات الجريمة الإلكترونية كما هو الحال في أية جريمة أخرى أن يتم إثبات عناصر هذه الجريمة بشكل يقيني من خلال الأدلة الرقمية، لاسيما الركن المادي للجريمة بكافة عناصره، فيجب إثبات السلوك والنتيجة والعلاقة السببية بين السلوك والنتيجة.

والدليل الرقمي كغيره من وسائل الإثبات يجب أن يكون خاضعا للنقاش أمام القضاء، وذلك ليصار إلى تحقق القاضي من توافر الشروط السابق ذكرها فيه، فيكون من حق المتهم مناقشة الدليل الرقمي والتشكيك بمشروعيته أو التشكيك بكونه يقينيا.

وما يبنى على ما سبق أنه يجب على المحكمة عند الاعتماد على الدليل الرقمي أن تظهر في حكمها أسباب قناعتها بالدليل الرقمي، وأن تظهر في حكمها الأسباب التي توصلت من خلالها إلى مشروعية الدليل وأنه يقينيا، وكذلك الحال فيما لو قررت المحكمة عدم الاعتماد على الدليل الرقمي فيكون على المحكمة أن تظهر في حكمها الأسباب التي دعتها إلى عدم الأخذ بهذا الدليل.

ونظرا لخصوصية الأدلة الرقمية، ولأن هذه الأدلة قابلة للنقاش، فإن ذلك يستدعي أن يكون القاضي الذي ينظر بالجرائم الإلكترونية على دراية ومعرفة جيدة بطبيعة هذه الأدلة وكيفية الحصول عليها، لأن التحقق من مصداقية هذه الأدلة لا يتأتى واقعا إلا من خلال تخصيص قاضي يكون قادرا على التحقق من توافر شروط الأدلة الرقمية من عدمه.

د. فاتح حمارشة، تاريخ المقابلة 2024/3/20، أستاذ القانون في جامعة بيرزيت، محامي وقاضي سابق، مكان إجراء المقابلة جامعة بيرزيت، 2024.

مقابلة شخصية: أ. عمار جاموس، تاريخ المقابلة 2024/05/28، باحث قانوني، الهيئة المستقلة لحقوق الإنسان، مكان إجراء المقابلة – الهيئة المستقلة لحقوق الإنسان، 2024.

س/ مدى فاعلية وتأثير تقارير المجتمع المدني المرسلة لمجلس حقوق الإنسان (الاجراءات الخاصة) حول إلزام الدولة بإعادة صياغة التشريعات والنصوص القانونية بما يضمن عدم المساس بالحقوق والحريات الخاصة ومنع الانتهاكات تمس الحق في الخصوصية للأفراد. (القرار بقانون رقم 16 لسنة 2017) .

س/ جاء في تقرير المقرر الخاص (استخدام تكنولوجيا المعلومات والاتصالات لضمان الحق في الحياة (A/HRC/29/37) – (2015)، في البند (54) على انه ينبغي على المؤسسات الحكومية وغير الحكومية على سواء تقييم خطر انعدام "الأمن الرقمي".

- دور مؤسسات المجتمع المدني(الهيئة المستقلة لحقوق الإنسان)، في مساندة ودعم آليات الأمم المتحدة - مجلس حقوق الإنسان وإجراءاته الخاصة.

ج / التقارير فاعلة ومؤثرة إلى حد ما، وذلك عبر مساعدة المقررين الخواص والهيئات التعاقدية في تحديد المشاكل التي تعتري التشريعات وتمثل انتهاكاً لحقوق الإنسان، الأمر الذي يؤدي بالنتيجة إلى تبني المقررين الخواص والهيئات التعاقدية لتوصيات أكثر فاعلية ومفيدة من أجل تقديمها إلى السلطة الفلسطينية وحثها على اعتمادها وإجراء التعديلات اللازمة. وقد حصل تطور من هذا القبيل فيما يتصل بقانون الجرائم الالكترونية لعام 2017، وفي القرارات بقانون المعدلة لقوانين إجراءات التقاضي سنة 2022، حيث إنه وبناءً على بيانات صحفية ومذكرات قانونية صادرة عن مؤسسات المجتمع المدني والهيئة المستقلة بخصوص تلك التشريعات، وبناءً على مخاطبة من بعض المؤسسات (مؤسسة الحق) للآليات الدولية في الأمم المتحدة بشأن قرار بقانون الجرائم الإلكترونية 2017، دعا المقرر الخاص لدى الأمم المتحدة المَعني بحرية التعبير، "ديفيد كاي"، بمذكرة شاملة، الحكومة الفلسطينية إلى تعديل قانون الجرائم الالكترونية، وفعلاً تم تعديله. وفي العام 2022، دعت لجنة مناهضة التعذيب في الأمم المتحدة السلطات الفلسطينية إلى إلغاء قانون الإجراءات القضائية وفعلاً تم إلغائها.

طبعاً هناك وجه آخر لدور مؤسسات المجتمع المدني وللمؤسسة الوطنية لحقوق الإنسان (الهيئة المستقلة) في مساندة ودعم آليات الأمم المتحدة فيما يتعلق بالحق في الخصوصية وانعدام الأمن الرقمي، وذلك عبر الإشارة إلى هذه المسائل في تقارير الظل أو بحسب تسمية أخرى "التقارير

الموازية" التي تتقدم بها تلك المؤسسات إلى الهيئات التعاقدية، وتستعرض فيها مدى التزام السلطة الفلسطينية بتنفيذ التزاماتها بموجب الاتفاقية التي انضمت إليها، وتساعد هذه التقارير تلك الهيئات (مجموعة الخبراء) في إعداد قوائم المسائل، والتوصيات أو الملاحظات الختامية التي تقدمها للسلطات الفلسطينية وتحثها فيها على إجراء التعديلات اللازمة.

أ. عمار جاموس، تاريخ المقابلة 2024/05/28، باحث قانوني، الهيئة المستقلة لحقوق الإنسان، مكان إجراء المقابلة – الهيئة المستقلة لحقوق الإنسان، 2024.

Abstract

This thesis addresses the field of digital evidence and its role in criminal proof in light of international conventions and Palestinian legislation. The research problem lies in the fact that, despite the rapid transformation from traditional society to digital society and the expansion of cybercrimes, the Palestinian legislator has merely considered digital evidence as a type of proof without addressing the regulatory and procedural aspects associated with digital evidence in the criminal field, and its connection to the civil and commercial field, Moreover, it overlooks jurisdiction rules in cross-border cybercrimes, negatively impacting the judge's intuitive conviction, complete justice, and public rights and freedoms, and contradicts the Basic Law (the Constitution) and international standards.

The researcher followed the descriptive- analytical approach, while expanding on the field of international conventions as normative tools, which included the basic human rights conventions to which the State of Palestine acceded, the human rights monitoring system in relation to digital evidence (contractual and non-contractual mechanisms), and European conventions, particularly the Budapest Convention (Council of Europe). Concerning Cybercrimes, their amendments and interpretations, and international standards regarding digital communication surveillance. The researcher conducted important personal interviews on the practical side, including the cybercrime unit in the police, the cybercrime prosecution, former judges, university professors, and specialized civil society organizations, in addition to the National Institution for Human Rights.

The thesis was divided into two chapters, with two topics and two subsections for each chapter. The first chapter covers the concept of digital evidence, its characteristics and

procedures, and the second chapter dealwith the value of digital evidence in international legislation and conventions, leading to theconclusions and recommendations.

The thesis concluded several findings, the most notable of which are: There is a relative and limited legislative development regarding digital evidence in the criminal field (Decree-Law on Cybercrimes and its amendments, and the Criminal Procedures Law and its amendments) at the level of recognizing digital evidence as proof, despite the issues that recognition raises in legislative drafting, this also extended to the civil and commercial field (the Evidence Law and its amendments) indicating limited development in these areas concerning digital evidence. The decisions regarding the laws were limited to recognizing digital evidence, and ignored the procedures for dealing with it in the criminal field, in exchange for focusing on criminalizing freedom of speech through the Decree-Law on Cybercrimes. Although cybercrimes and related digital evidence are cross-border, the legislator also did not address the problem of jurisdiction, which is considered one of the most prominent problems facing this type of crime. Legislative shortcomings in dealing with digital evidence would affect the rights, freedoms, and guaranteed fair trial guarantees enshrined in the Basic Law and international standards. The decree-laws themselves, including those on digital evidence issued in the absence of the Legislative Council, contributed to infringing on freedom of expression and focused solely on criminalization without procedural regulation, reflecting a lack of comprehensive treatment of digital evidence.

The thesis provided several recommendations, most notably: the necessity to abolish all provisions in the Decree-Law on Cybercrimes that infringe on freedom of expression in alignment with constitutional rights and international standards. Substantial amendments should be made to the Decree-Law on Cybercrimes to ensure judicial oversight in all

aspects related to digital evidence, aligning with international standards (International Principles on the Application of Human Rights to Communications Surveillance 2013). Addressing the legislative gap related to procedural aspects of handling digital evidence at all stages, and not merely considering digital evidence as acceptable in criminal proof, to ensure the quality of digital evidence, including its use in civil and commercial proof due to their interconnectedness. Enhancing the capabilities of justice institutions (law enforcement agencies, public prosecution, judiciary) through training programs on handling digital evidence. Including digital evidence and its role in proof within specialized university courses and judicial institute programs, keeping up with developments. Halting the application of decree-laws that played a significant role in violating rights and freedoms, recognizing digital evidence solely for criminalization and not for institutionalization and regulation purposes. Restoring the original role of the Legislative Council in legislation, respecting the constitution, ensuring the separation of powers, promoting democratic transition, and enabling the "Legislative" to fulfill its constitutional duties in regulating all aspects of digital evidence.