Al-rafidain of Law (ARL)
ISSN: 1819-1746
E-ISSN: 2664-2778
https://alaw.uomosul.edu.iq

Digital forensics and legal guarantees for the accused in an electronic environment

Anas Mahmood Khalaf[1]
College of Law/ University of Mosul
Anas mhmood@uomosul.edu.iq

Article information
Article history
Received 8 July, 2025
Revised 3 August, 2025
Accepted 3 August, 2025
Available Online 1 September, 2025

Keywords:
- Digital Investigation
- Respect for the Law
- Guarantees
- Digital Evidence

Correspondence:
Anas Mahmood Khalaf
Anas mhmood@uomosul.edu.iq

Abstract

This research examines the concept of digital criminal investigation and the legal guarantees afforded to the accused within the context of the electronic environment. As technological advancements continue to reshape the landscape of criminal activity, cybercrime presents a growing challenge to legal systems worldwide. The increasing reliance on digital evidence in criminal proceedings underscores the urgent need to uphold the rights of the accused during all stages of digital investigation. The study analyzes the procedures involved in digital criminal investigations—such as the collection, preservation, and analysis of electronic evidence—and evaluates their alignment with international legal standards for fair trial rights. Particular attention is given to legal safeguards aimed at preventing violations, including unlawful surveillance, data breaches, and coercive methods of evidence gathering. By exploring the tension between effective law enforcement and the protection of individual rights, the research offers recommendations for strengthening legal frameworks to ensure justice and due process in the digital age.

Doi: 10.33899/alaw.2025.162568.1353
© Authors, 2025, College of Law, University of Mosul This is an open access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0).

التحقيق الجنائي الرقمي والضمانات القانونية للمتهم في بيئة الكترونية

أنس محمود خلف
كلية القانون/ جامعة الموصل

معلومات البحث
تاريخ البحث
الاستلام ٨ تموز, ٢٠٢٥
التعديلات ٣ آب, ٢٠٢٥
القبول ٣ آب, ٢٠٢٥
النشر الإلكتروني ١ أيلول, ٢٠٢٥
الكلمات المفتاحية
- التحقيق الرقمي
- احترام القانون
- الضمانات
- الدليل الرقمي

المستخلص

ان مع التطور التكنولوجيا وتوسيع استخدام الانترنت، برزت جرائم جديدة ذات طابع رقمي تستوجب آليات تحقيق متخصصة، تعرف بالآليات التحقيق الجنائي الرقمي، والذي يهدف الى جمع الأدلة الرقمية وتحليلها لاستخدامها امام الجهات القضائية، الا ان تلك النوع من اجراءات التحقيق تثير تحديات قانونية مهمة امام القائمين على تلك الاجراءات، خاصة فيما يتعلق بضمان حقوق المتهم وحمايتها من الانتهاكات، والتي تطرأ للخصوصية البيئية الإلكترونية وطبيعتها التقنية المعقدة، لذا فان للطبيعة التحقيق الجنائي الرقمي، وكذلك اجراءاتها وادواتها التقنية، والتي يستعرض الاشكاليات القانونية المرتبطة به، لا سيما ما يتعلق بمدى التزام الجهات المختصة بالضمانات الدستورية، وكذلك القانونية، والمكفولة للمتهم، والمتمثلة بالحق في الخصوصية، وآليات المراسلات السرية المعهودة، من ضمانات التفتيش والمصادرة، والحق في الدفاع وغيرها من الاجراءات، لذا من المؤمل العمل الى تحقيق التوازن الدقيق بين متطلبات مكافحة الجرائم الإلكترونية ومدى فاعليتها في التحقيق الرقمي، وبين مدى الضرورة الرقمية في الاحترام الذات للحقوق الاساسية للمتهم، في بيئة رقمية قد تكون عرضة للانتهاك او الاستغلال او التعدي، وبهذا فان للضمانات دور مهم وفعال لتحقيق اجراءات ذات هدف فعال وبارز في توفير بيئة امنه للخصوصية الرقمية سواء على الصعيد الداخلي او على الصعيد الدولي، في تحقيق نوع من التوازن لها وفق معايير ذات صبغة فعال، في التحقيق الجنائي وفق خلق نوع من الضمانات للمتهم في بيئة الكترونية، واتخاذ الحيطة اللازمة من اي اختراق سيبراني فيها.

المقدمة

ان في ضل التطور الهائل للتكنلوجيا المعلومات وكذلك الاتصالات، والذي اصبحت فيها الجريمة لا تقتصر على الواقع المادي، بل امتدت الى الفضاء الإلكتروني، مما افرزت نوعاً جديداً من الجرائم والتي تعرف بالجرائم الإلكترونية، او يمكن ان يطلق عليها بالجرائم السيبرانية، لذا فقد تترتب على ذلك ضرورة تحديث الآليات القانونية في التحقيق الجنائي، لتشمل ادوات واساليب رقمية متطورة، وكذلك قادرة على التتبع الرقمي وتحليلها للجرائم الرقمية، عليه فان لمفهوم العام للجرائم الرقمية في التحقيق الجنائي بانها العملية القانونية والفنية التي تهدف الى جمع الأدلة الرقمية وكذلك كيفية حفظها، وتحليلها من حيث عرضها امام الجهات القضائية، ضمن معايير قانونية بحقوق الافراد، اذ تكمن اهمية هذا النوع من اجراءات المزعمة في التحقيق، في كونه يتعامل مع ادلة جديدة ومتطورة، اي غير ملموسة، لذا قد تتعرض للتلف او التغير بسهولة، مما يستلزم اعتماد اجراءات دقيقة وعملية في جمعها، وكذلك حفظها، عليه فان في المقابل نلاحظ انه هناك تطور في وسائل التحقيق الجنائي، من خلال الضرورة الملحة الى الحفاظ على الضمانات القانونية للمتهم، خاصة في بيئة قد من الممكن ان تستغل فيها الوسائل التقنية للإضرار، لذا فان التحقيق الجنائي الرقمي، رغم دورة الفعال، والتي يجب ان يمارس ضمن اطار قانوني البراءة، وعدم اجباره كدليل يقدم، ضد نفسه، لذا في الحصيلة النهائية ضمان سلامة الدليل في الاثبات، وعدم افلات الجاني من العقاب، وعدم تفشي تلك الجرائم، في ردع الغير، لذا فمن هنا تأتي اهمية البحث في هذا المضمار، والتي نسعى دائماً لتسليط الضوء على التوازن الرقمي في الادلة، واحترام الضمانات القانونية للمتهم، في بيئة الإلكترونية سليمة، وهو ما يمثل تحدياً كبيراً امام الانظمة القضائية في العصر الرقمي.

اولاً: اهمية البحث:

ان لتزايد انتشار الجرائم الكترونية، وتطور اساليبها مع انتشار الكبير للتكنلوجيا والاعتماد على الانترنت، في ظهور انماط جديدة، ومتطورة، ومختلفة في الاحتيال الإلكتروني، من ابتزاز، وقرصنة، لذا فان تلك الجرائم تتطلب ادوات وتقنيات خاصة لإجراءات التحقيق الجنائي فيها في مختلف عن الاساليب التقليدية، لذا اضحت الضرورة الفعلية في تنظيم

التحقيق الجنائي الرقمي والذي يتطلب تحليل البيانات وتتبع الانشطة الإلكترونية فيها، في استخدام وسائل غير مشروعة للحصول على الادلة.

ثانياً: اشكالية البحث:

ان هذا الموضوع، يعد من القضايا المهمة في التحقيق الجنائي الرقمي ومن ضمانات القانونية المتهم في بيئة الإلكترونية في العصر الحاضر، لذا فإنها من الامور المعقدة، التي تثير الكثير من التساؤلات القانونية والتحقيق الجنائي فيها، اي مدى نجاح اجراءات التحقيق الجنائي الرقمي في كشف تلك الجرائم، وضبط مرتكبيها، مع مراعات الضمانات الكترونية خاص ان تلك البيانات اذ تتسم بالتغير السريع والمعقد التقني، من اتلاف الدليل، وعدم مواكبة التطورات القانونية لها، في تحديد المركز القانوني للفاعل، في تحديد مكان وجود المتهم او البيانات خارج الولاية القضائية، لمكان ارتكاب الجريمة.

ثالثاً: اهداف البحث:

ان من الاهداف الرئيسية للتحقيق الجنائي الرقمي هو الكشف عن الجرائم الإلكترونية وعن فاعليها، والمتمثل بالاحتيال الإلكتروني في الابتزاز الرقمي، والاختراق الانظمة، والجرائم المالية الإلكترونية، وكذلك الارهاب عبر شبكة الانترنت، وكذلك اهميتها في جمع الادلة بطرق قانونية موثوق بها تصلح للاستخدام والإدانة امام المحاكم المختصة، من تحليل للأدلة وتفسيرها، وكذلك في الحفاظ على سلامة تلك البيانات، في تحديد الهوية الرقمية للمشتبه بهم، وكذلك منع تكرار تلك الجرائم مستقبلاً.

رابعاً: منهجية البحث:

بصفة عامة نتبع في بحثنا هذا الى استخدام المنهج التحليلي وكذلك المنهج الوصفي لبعض النصوص القانونية في بيان المفهوم التحقيق للجرائم وضمانات المتهم في الادلة الرقمية الإلكترونية، وفق معاير التحقيق الجنائي للإثبات القضائي فيها.

المبحث الاول

مفهوم التحقيق الرقمي واجراءاته

ان للتطور الهائل في للتكنلوجيا المعلومات، وكذلك الاعتماد المتزايد على الانظمة الرقمية، اذ ظهرت الحاجة الى مجال متخصص يعرف بالتحقيق الجنائي الرقمي، اذ يعد هذا المجال فرعاً من فروع الأدلة الجنائية، وبالتالي يهدف الى جمع وحفظ وتحليل البيانات الرقمية بطريقة تمكن من استخدامها كدليل في القضايا القانونية والجنائية، اذ يتم ذلك في اجهزة الحاسوب ويتم التعامل معها كأنظمة للتشغيل، للبرامج، والملفات، وسجلات النظام، كما يشمل مراقبة وتحليل حركة مرور البيانات على الشبكة لاكتشاف التهديدات او التسريبات، كما يركز على الهواتف الذكية، وكذلك الاجهزة اللوحية، واستخراج البيانات منها، كما انه يتم التحقق في وسائط متعددة، وبتنوع الصور، والفيديوهات، والتسجيلات الصوتية، للتأكد من صحتها وعدم التلاعب بها، ولضمان مصداقية الأدلة الرقمية، يجب اتباع خطوات دقيقة وحاسمة، وبالتالي الى تحديد الأجهزة او المصادر التي قد تحتوي على ادلة رقمية متعلقة بالقضية، مثل اجهزة الحاسوب او البريد الإلكتروني او كاميرات المراقبة، اذ يتم من خلال حماية الاجهزة والبيانات الرقمية من التلاعب او التلف في استخدام التجميد الرقمي، لضمان بقاء البيانات على حالها، وتم في حالت كانت العملية جمع الادلة الرقمية باستخدام ادوات متخصصة دون التأثير على البيانات الأصلية، غالباً ما يتم انشاء نسخة رقمية من الوسائط للتخزين، من فحص البيانات الرقمية بهدف استخدام المعلومات المفيدة، والمتمثلة بمعرفة مدى تعديل اي ملف ما، او قد يطرأ لها من برامج التي تتيح الدخول الى النظام، او ما اذا كانت هناك برمجيات خبيثة، وللتوضيح أكثر سوف نقوم بتقسيم هذا المبحث الى عدة مطالب، نتناول في المطلب الاول مفهوم التحقيق الرقمي، وفي المطلب الثاني آليات جمع الادلة الإلكترونية، وبالشكل التالي:

المطلب الاول

مفهوم التحقيق الرقمي

ان للمفهوم الخصوصية الرقمية، طابع العام والقدرة الفرد على التحكم بمعلوماته الشخصية وكيفية استخدامها، وكذلك عدم مشاركتها، مع اي جهة او شخص، اذ تشمل تلك الحق الحفاظ على سرية المراسلات، والمعلومات الصحية، من البيانات البيو مترية، وكذلك

سجلات التصفح، والموقع الجغرافي، وغيرها من البيانات الحساسة، وللتوضيح أكثر يمكن ان نقسم هذا المطلب الى عدة فروع وبالشكل الاتي:

الفرع الاول: تعريف التحقيق الرقمي:

اذ عرف التحقيق الرقمي "بأنه هو عملية تحديد، واسترداد، وتحليل، وحفظ الادلة الرقمية من الاجهزة الإلكترونية مثل الحواسيب، والهواتف الذكية وغيرها، من الخوادم، واجهزة التخزين، وايضاً حتى الشبكات"[١].

كما عرف التحقيق الرقمي بانه: "عملية جمع وحفظ وتحليل الأدلة الرقمية المتعلقة بجريمة ما، وذلك باستخدام ادوات وتقنيات تكنلوجية حديثة، تشمل هذه الأدلة البيانات المستخرجة من الحواسيب، الهواتف الذكية، الانترنت منصات التواصل الاجتماعي، الخوادم، والبريد الإلكتروني، وغيرها من المصادر الرقمية"[٢].

يتضح لنا اذ يتم ذلك باستخدام ادوات متخصصة، وتقنيات محددة لضمان عدم تغيير او تلف البيانات الرقمية، مما يسمح باستخدامها في المحاكم او في التحقيقات الأمنية، لذا فهو جريمة مستحدثة مرتبطة بالشبكة العنكبوتية والتي يصعب فيها تحديد الطبيعة القانونية للشخص الفاعل.

(١) سراج الدين محمد الروبي، الاستجوابات الجنائية في مفهومها الجديد، (الدار المصرية اللبنانية |١٩٩٧)، ص٤٣.

(٢) د. عبد الستار الجميلي ومحمد عزيز، التحقيق الجنائي الحديث- بين النظريات والتطبيق، (مطبعة دار السلام، بغداد |١٩٧٦)، ص٥١.

الفرع الثاني: الفرق بين التحقيق التقليدي والرقمي:

هناك فرق بين التحقيق الرقمي، والتحقيق التقليدي، اذ يعتبران اسلوبان يستخدمان في جمع الأدلة وتحليلها، ضمن السياقات الجنائية او الامنية، لكن لكل منهما لدواته وبيئته الخاصة به، لذا فأننا نعول الى الفرق بينهما بالشكل الاتي:

اولاً: التحقيق التقليدي:

غالباً ما يكون التحقيق الجنائي التقليدي، الذي يتم على ارض الواقع، اذ يعتمد على جمع الادلة المادية وتحليلها، من معاينة مسرح الجريمة، او جمع البصمات، وكذلك الحمض النووي، او استجواب الشهود، والبحث في الوثائق الورقية، من مراقبة الأماكن جسدياً، والذي يتم استخدامها في مجالات عدة منها جرائم القتل والسرقة، وكذلك الاعتداء، وغيرها من الجرائم المادية، التي يمكن ان يستفاد منها في اجراءات التحقيق والاثبات [١].

ثانياً: التحقيق الرقمي:

بصفة عامة ان التحقيق الرقمي، والذي يتم في الفضاء الإلكتروني، ويهتم بجمع الأدلة من الأجهزة الرقمية والشبكات، من حيث ادوات تحليل الهواتف الذكية واجهزة الكمبيوتر، واجراءات استرجاع البيانات والانشطة على الإنترنت، وكذلك اجراءات الفحص للسجلات الشبكات وانظمة المراقبة الرقمية، في المجلات التي تستخدم فيها الجرائم الإلكترونية، والمتمثلة بالاختراق والاحتيال الإلكتروني، والابتزاز، وغيرها، من اجل التوصل الى تحليل انشطة وسائل التواصل، والتتبع للأنشطة المشتبه بهم عبر التواصل، والتتبع المشتبه بهم عبر الانترنت، من اجل التوصل الى الحقيقة او الادلة الدامغة للأثبات[٢].

فمن خلال ما تم ذكرة من توضيح للدليل الرقمي عن الدليل التقليدي في الاثبات، اذ ان كثير من القضايا الحديثة والتي يتم استخدام التحقيق الجنائي الرقمي والتقليدي معاً، خاصة عندما يكون للجريمة جانب مادي واخر رقمي، والتي تتمثل بجريمة قتل بعد

(١) د. عبد العزيز حمدي، البحث الفني في مجال الجريمة سلسلة كشف الجريمة بالوسائل العلمية الحديثة، الجزء الاول، (الطبعة الاولى |١٩٧٣)، ص٤٢.

(٢) عبود صالح التميمي، التحقيق الجنائي العملي، (الطبعة الاولى |٢٠٠٦)، ص٦٤.

اجراءات عملية الابتزاز وغيرها، لذا فان القانون العراقي في قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل، اذ يتناول بعض الجرائم التقليدية التي ترتكب عبر وسائل إلكترونية (التهديد والتشهير) لكنة لا يتضمن معالجة صريحة للأدلة الرقمية، كما ان قانون مكافحة الجرائم الإلكترونية، اذ تمت مناقشة عدة قوانين في مجلس النواب العراقي كجرائم المرتكبة عبر الإنترنت وحماية البيانات الشخصية، وصلاحية الضبط القضائي في التحري الرقمي، وبهذا فان قانون الاثبات رقم ١٠٧ لسنة ١٩٧٩ لم يتضمن على الادلة الرقمية صراحة، لكن بشرط عدم مخالفة النصوص القانونية او المساس بالحقوق الدستورية.

الفرع الثالث: الجهات المخولة بإجراء التحقيق الرقمي:

ان في الاغلب هناك اختلاق في الجهات التي تتولى التحقيق الجنائي او التكليف بالتحقيق الرقمي من بلد لآخر، وبحسب نظام كل دولة، لكن الصفة الغالبة تكون صفة رسمية تتولى تلك المهام، ومتخصصة لها صلاحيتها القانونية، في التحقيق الرقمي، والتقنية، فيما يلي نظرة علية الجهات الامنية والشرطية، من وحدات الجرائم الإلكتروني في الوزارة ذات العلاقة، والمتمثلة بوزارة الداخلية، والتي هي ادارة التحقيقات الجنائية او ما يسمى بالأمن السيبراني، لذا فان تلك الجهات تتعامل مع الجرائم الإلكترونية بدقة متناهية، من اختراق او ابتزاز الإلكتروني، للجرائم المالية عبر الانترنت، فمن تلك الجهات الادعاء العام، والشرطة، وهيئات الاتصالات، والهيئات الاستخباراتية، في وزارة الدفاع، او قد يكون منقبل جهات خاصة معتمدة بموجب تفويض قضائي، والتي تكون تحت اشراف قضائي، لكن بالرغم من التطور الحاصل في المجتمع الدولي، في اجراءات التحقيق الجنائي الرقمي، الان انه العراقي يفتقر الى جودة عالية في هذا المجال، من لوائح خاصة بتنظيم التحقيق الرقمي، وتحديد من له الصلاحية بالتحقيق وتحليل الادلة الرقمية، والتي غالياً ما تنتهي مهمتها، بعد معاينة التفاصيل وتحليها قانونياً، وعرضها على الجهات المختصة[١].

(١) د. عمار عباس الحسيني، |"مدى مشروعية التسجيل الصوتي بالهواتف النقالة كدليل في الاثبات الجنائي"|، منشور في |مجلة جامعة اهل البيت|، بالعدد الثامن، (٢٠٠٩)، ص٧٢.

المطلب الثاني

آليات جمع الأدلة الإلكترونية

ان مع التطور التكنلوجي، وكذلك لظهور الانترنت، اصبحت البيانات الشخصية تجمع بكميات هائلة من قبل الحكومات، والمتمثلة بالشركات وتطبيقاتها الإلكترونية، وان تلك البيانات غالباً ما تستخدم في مجالات مختلفة منها، الاعلانات، وكذلك تحسين الخدمات او حتى الرقابة عليها، لذا فانه من هنا برزت

الحاجة الى قوانين تنظيم طريقة جمع تلك البيانات وكذلك استخدامها، وللتوضيح أكثر يمكن تقسيم هذا المطلب الى عدة فروع وبالشكل التالي:

الفرع الاول: الادوات في جمع الأدلة الرقمية:

اذ يعتبر جمع الادلة الرقمية، هو الجزء الاساسي من علم الادلة الجنائية، والذي يتطلق التأني والتدقيق ودراسة كل حال على حدة، طالما يشمل تقنيات مخصصة للحصول على البيانات، التي يمكن استخدامها كدليل من التحقيقات، وان من بين تلك الادوات هي، ادوات التصوير والقرص الصلب، والذي يستخدم لعمل نسخة طبق الاصل من القرص بدون تعديل البيانات الأصلية، وكذلك تحليل النظام والملفات وسجلات النظام والبرامج الخبيثة وغيرها، من ادوات التحليل الهواتف المحمولة الذكية، وادوات الشبكات وتحليل الحزم، وادوات استعادة البيانات المحذوفة، والتي تستخدم في ارجاع الملفات، كل هذا الادوات تستخدم في الفحص السريع والدقيق للأدلة الحية، في تحليل الادلة[1].

اما المشرع الفرنسي فقد اشار الى التحقيق الرقمي في جمع الادلة الرقمية من الاجهزة الإلكترونية، او الشبكات، وهو مجال تطور قانون الاجراءات الجنائية اذ ينظم طرق تفتيش الاجهزة الرقمية، لذا فان في السياق الجرائم المنظمة او الخطيرة تعزز صلاحيات الضبط القضائي في الوصول الى البيانات المشفرة او عبر الانترنت، فان قانون مكافحة الجريمة الإلكترونية، والمعروف بقانون الثقة في الاقتصاد الرقمي، اذ يعد حجر الزاوية في

(١) د. احمد عوض بلال، قاعدة استبعاد الادلة المتحصلة بطرق غير مشروعة في الاجراءات الجنائية، (الطبعة الثانية، دار النهضة العربية، القاهرة |٢٠٠٨)، ص٦٣.

تنظيم الانترنت والجرائم المرتبطة به، كما ان الاتفاقية الدولية بودابست بشأن الجريمة الإلكترونية ٢٠٠١ والتي تهدف الى تعاون مشترك في التحقيقات العابرة للحدود[١].

الفرع الثاني: حجية الادلة الرقمية امام القضاء:

ان لحجية الادلة الرقمية، او الإلكترونية، امام القضاء قرينة قانونية قاطعة، والتي تعتبر وسيلة اثبات في الدعاوي القضائية، وان الادلة الالكترونية، هي اي معلومات ذات طابع رقمي يمكن استخراجها او حفظها من الجهاز إلكتروني، وتتكون ذات صلة بواقعية القضية، اذ تعتمد الحجية الادلة الرقمية على عدة عوامل منها، القوانين الداخلية المنظمة، مثل السعودية، ومصر، والامارات، والمغرب، والعراق، تم سن قوانين خاصة بالمعاملات الإلكترونية او مكافحة الجرائم الإلكترونية، اذ تعترف بحجية الأدلة الرقمية، ومن اجل سلامة التحقيق القضائي فان القضاء لا يكتفي بوجود الدليل الرقمي، بل يشترط الى اثبات ان الدليل لم يعدل او يزور، في استخدام وسائل التحقيق الجنائي الرقمي، لذا فان بعض الانظمة تشترط ان يكون الدليل صادراً عن جهة موثوقة، او مرفقاً بتقرير خبراء معتمدين، في الادلة الرقمية، وان يكون تحليل الخبراء في نوع الختم والتحليل الزمني، اذ يعزز حجية المستندات الرقمية فيها الى صعوبة انكارها، والتي طالما كانت فعال في مجال العمال التجارية، لكن بالمقابل لا تكون مطلق فهي عرض للتزوير، وان تكون موضع طعن وشك امام وجهة الخبراء وفق معاير الاصول القانونية، لكن بصفة عامة فهي اصبحت في المحاكم أكثر قبولاً للأدلة من تشهير وابتزاز الإلكتروني، وان بعض المحاكم تعاملت مع الادلة الإلكترونية الرقمية مساوية مع الادلة المادية، اذا استوفت الشروط والإثبات[٢].

نستنج مما تم ذكره ان للأدلة الرقمية تتمتع بحجية امام القضاء ما دامت مستوفية للشروط، والاجراءات القانونية، من تقنيات معينة، اذ تتزايد اهميتها مع التطور

(١) د. وصفي محمد علي، الوجيز في الطب العدلي، (المكتبة القانونية، بغداد |٢٠٠٧)، ص٨٣.

(٢) د. كريم خميس البديري، الخبرة في الاثبات الجزائي، (بدون مطبعة، بغداد |٢٠٠٨)، ص٦٢.

التكنلوجيا، وكذلك الزيادة في الجرائم والمنازعات ذات الطابع الإلكتروني، وبهذا فان الدليل الرقمي يعد من ادلة الاثبات القاطعة اما المحاكم المختصة.

الفرع الثالث: المشكلات التقنية والقانونية المرتبطة بالدليل الرقمي:

اذ يستخدم الدليل الرقمي او الإلكتروني بشكل فعال في التحقيقات الجنائية، والقضائية القانونية، اذ يعول الى تلك المهمة الى الاعتماد المتزايد على التكنلوجيا، اذ ان هناك العديد من المشكلات التقنية، والقانونية المرتبطة به، والتي غالباً ما تكون مشكلات تقنية، اذ ان سهولة التلاعب والتعديل فيها، سواء في البيانات الرقمية، من تعديل او حذف، والذي ربما يدعوا الوضع فيها الى الشك في اصالة تلك الادلة، او قد تكون عرضة للتلف او الفقد، قد تتعرض الى الاعطال، في البرمجيات والذي بدورة يؤدي الى فقدان البيانات، وبالتالي الى صعوبة استرجاع البيانات المحذوفة، او المشفرة، اذ يتطلب ادوات وتقنيات متقدمة ومكلفة للمحافظة عليها واسترجاعها، اذ ان الادلة بصفة عامة تعتبر سجلات محادثات او ملفات صوت او فيديو او تقنيات، اذ هنا صعوبة التأكد من مصادر تلك البيانات، اما من جانب المشكلات القانونية التي تواجه تلك الادلة الرقمية، منها الشرعية والاذن القانوني في اختراق الخصوصية الرقمية للشخص، والتي تعتبر من خصوصية الافراد، او قد تكون هناك تحديات في جمع الادلة المخزونة العابرة للحدود، والتي تكون في دولة اخرى، واحياننا الصعوبة تكمن في معرفة شخصية الشخص الفاعل، والتي طالما الاشخاص الذين يرتكبون تلك الجرائم يستخدمون اسماء وحسابات مزيفة، لذا فان هنا يتطلب الدقة في اجراءات الادلة الرقمية فيها[1].

وبهذا فانا نتضح لنا انه للدليل الرقمي قوى لكنة في نفس الوقت يعتبر دليلاً هش، اذ يحتاج الى التعامل به بدقة وحذر، وفق معايير قانونية لضمان قبوله امام المحاكم المختصة، عليه فان للسلطات ان تراعي الدقة وان تتوخى الحذر في التعامل مع تلك الادلة الرقمية، وان تعتمد على كوادر مدربة قانونية تقنياً للتعامل معه.

(١) د. قدوري عبد الفتاح الشهواني، مسرح الجريمة، (دار النهضة العربية، القاهرة| ٢٠٠٦)، ص٦٤.

المبحث الثاني

الضمانات القانونية للمتهم في التحقيق الرقمي

يشهد العالم تحول رقمي شاسع، في التعاملات، اذ لم تعد الجرائم محصورة في العالم الافتراضي فقط، بل اصبحت الجرائم الإلكترونية تمثل تحدياً حقيقاً للعدالة الجنائية، مع التوسع في استخدام وسائل التحقيق الرقمي، اذ تبرز الحاجة الى ضمان حماية حقوق المتهم، في تحقيق التوازن بين مكافحة الجريمة او احترام الحريات الفردية، لذا فان الاصل انه يعد المتهم بريئا حتى تثبت ادانته، بموجب محاكمة عادلة، اذ تعتبر الضمانات القانونية احد الركائز الأساسية التي تحمي هذا المبدأ، لذا فان في سياق التحقيق الرقمي، تكتسب تلك الضمانات اهمية خاصة نظراً للدور التي تقوم به، من الاحتمالات للتلاعب بتلك الادلة، او انتهاكها، لذا فمن بين تلك الضمانات، مبدأ الشرعية الاجرائية، والذي يكون عدم اتخاذ اي اجراء ضد اي شخص الا وفق او بموجب نص قانوني، وكذلك احترام الحق في الخصوصية، الاصل عدم انتهاك اي خصوصية شخص، الا وفق قرار صادر من محكمة مختصة، اي ان تكون سابق عليها اذن قضائي، وان الهدف منها ان يكون هناك سلامة في الادلة الرقمية، في توخي الحذر في جمع تلك الادلة، وان تراعي السرية في جمع الادلة في الاتصالات، والرسائل فيها، كون انها تعتبر انتهاك صريحاً للحق في الخصوصية، والتأكد من مصدر البيانات، وكذلك عدم تزويرها، ويجب على القائمين على تلك المهام، من موظفي الضبط القضائي، ان يكونوا ملمين بأمور التقنيات في جمع الادلة اي يجب ان يتمتع بخبرة عالية فيها، وللتوضيح أكثر سوف نقوم بتقسيم هذا المبحث الى عدة مطالب، اذ نتناول في المطلب الاول الحق في الخصوصية وحماية البيانات، وفي المطلب الثاني، حق الدفاع وضمانات المحاكمة العادلة، وبالشكل التالي:

المطلب الاول

الحق في الخصوصية وحماية البيانات

ان في الاساس للحق في الخصوصية الرقمية، يكمن من الحقوق الأساسية التي تكفل كرامة الإنسان الأخرى مثل حرية التعبير والأمن الشخصي، ومع التوسع الرقمي المتسارع، اذ اصبحت حماية البيانات الشخصية امراً حتمياً لا مفر منه، وذلك من اجل

ضمان تلك الخصوصية، اذ باتت تلك الخصوصية، الفردية عرضة للاختراق والتجسس، وكذلك الاستغلال من قبل جهات متعددة.

الفرع الاول: مبدأ سرية الاتصالات والمراسلات:

اذ تعد سرية المراسلات من المبادئ الأساسية التي تكرس حماية الحياة الخاصة وكذلك حرية الأفراد، اذ تتصف من ضمن الحقوق والحريات الخاصة وكذلك من الحريات الفردية، كما انها تصنف ايضاً من الحقوق والحريات العامة التي كفلها الدساتير والقوانين في معظم دول العالم، اذ انه يمكن القول ان هذا المبدأ ان جميع اشكال التواصل، سواء كانت مكتوبة، او صوتية او إلكترونية، يجب ان تظل محمية من اي تدخل او اطلاع من قبل الآخرين، والمقصود هنا السلطات وغيرها، الا في حالات استثنائية، يمكن ان يحددها القانون، اذ نصت الدساتير على عدم انتهاك تلك الخصوصية، اذ اشار الدستور المصري في المادة (٥٧) منه على انه": للحياة الخاصة حرمة، وهي مصونة لا تمس، وتضمن الدولة حماية سرية المراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية وغيرها من وسائل الاتصال، ولا يجوز مصادرتها او الاطلاع عليها او رقابتها الا بإمر قضائي مسبب ولمدة محددة وفقاً لأحكام القانون". اما ما اشارت الية المواثيق والاتفاقيات الدولية، هي العهد الدولي الخاص بالحقوق المدنية والسياسية، في المادة (١٧) والذي تنص على انه": لا يجوز تعرض أحد لتدخل تعسفي او غير قانوني في خصوصياته او اسرته او بيته او المراسلات"[١].

عليه يمكن القول انه من خلال ما ذكر يبقى مبدأ سرية الاتصالات والمراسلات من اهم ركائز الدولة القانونية، التي تحترم الحقوق والحريات الفردية، اذ يجب ان توازن التشريعات بين حماية تلك المبدأ مع ضرورة التوازن بينها وبين حماية الامن العام، والذي يقضي الالتزام الصارم بالضمانات القضائية، حتى لا يتحول الاستثناء الى قاعدة يمكن ان تنتهك بها الحريات.

(١) فاضل عباس الملا، التحقيق الجنائي في قضاء الامام علي (ع)، (المكتبة الحيدرية| ٢٠٠٩)، ص٥٢.

الفرع الثاني: مدى مشروعية اختراق الأنظمة الرقمية:

يمكن القول ان الاختراق هو عملية قرصنة بحد ذاتها، اذ يكون اختلافها فقط في الحصول الاذن من جهات ذات العلاقة والمتمثلة بالقضاء على انتهاك تلك الخصوصية، وان يكون ذلك وفق القانون، والا الاصل ان يكون ذلك التدخل انتهاك ومحظور اصلاً يحاسب علية القانون، والذي يوصف بانه دخول غير مصرح به الى انظمة، وشبكات او بيانات بهدف السرقة، او التخريب او التجسس، والذي يعد اختراق غير قانوني تماماً، في اغلب التشريعات الدولية، وتكون العقوبات متشددة فيها، او بالغرامة، كما لحظر تلك الاجراءات لها اثر مادي تقني على بعض الدول(١).

الفرع الثالث: التوازن بين مصلحة المجتمع وحقوق الافراد:

ان للتحول الرقمي في عصرنا الحالي دور بارز وفعال، اذ اصبحت التحقيقات الجنائية والرقابية دور تعتمد بشكل متزايد على الأدلة الرقمية، والمتمثل بالبيانات الهاتف والبريد الإلكتروني، وغيرها، من سجلات مواقع التواصل الاجتماعي، بالرغم من اهمية هذه الادلة في حماية الامن القومي، لمكافحة الجريمة، من اجل ضمان العدالة، الا ان استخدامها يثير تساؤلات جوهرية تتعلق بحقوق الأفراد، خاصة فيما يخص الخصوصية، والحرية في التعبير، وغيرها من الضمانات للمحاكمة العادلة(٢).

اذ تعد اهمية التحقيق الرقمي من التحقيقات او الادوات الفعالة في الكشف عن الجرائم المعقدة مثل الإرهاب الإلكتروني، والاحتيال المالي، والتجار بالبشر، وجرائم الإنترنت، لذا فمن مصلحة المجتمع ان تمتلك السلطات ادوات متقدمة لملاحقة الجناة، خاصة في ظل تطور الجريمة الرقمية، وتعقيد ادواتها(٣).

لاسيما في مقابل كل ما تم ذكره اذ يتطلب احترام حقوق الافراد من خلال وضع ضوابط صارمة على اساليب جمع وتحليل البيانات الرقمية، فالدساتير وكذلك المواثيق

(١) د. قدوري عبد الفتاح الشهواني، مصدر سابق، ص٨٣.
(٢) عبود صالح التميمي، مصدر سابق، ص٩٨.
(٣) د. احمد عوض بلال، مصدر سابق، ص٩٢.

الدولية، والمتمثل بالإعلان العالمي لحقوق الانسان والعهد الدولي للحقوق المدنية وكذلك السياسية، والتي تؤكد على انه كافة تلك الحقوق لها خصوصية، العمل على عدم المساس بها، او التعرض للتفتيش او المراقبة التعسفية فيها.

المطلب الثاني

حق الدفاع وضمانات المحاكمة العادلة

ان للتقدم التكنلوجي يفرض تحديات قانونية واخلاقية جديدة، لذا فان على المجتمع الدولي العمل على وضع حلول يمكن ان تواكب تلك التحديات من خلال تطوير تشريعات متوازنة تتضمن الامن العام دون التفريط في الحقوق الاساسية، عليه ان للتوازن بين حق الدفاع وضمانات المحاكمة العادلة، في التحقيق الرقمي ليس خياراً، بل ضرورة لضمان مجتمع عادل وآمن فيها، وللتوضيح أكثر يمكن تقسيم هذا المطلب الى عدة فروع وبالشكل التالي:

الفرع الاول: اخطار المتهم والتحقيق بحضوره:

ان من اساسيات العمل في التحقيق هي اخطار المتهم، والتحقيق بحضوره، وهو اجراء قانوني مهم يتبع في سياق التحقيقات الجنائية، بقصد اعلام المتهم بالتهم الموجه اليه، والتي تمكنه من الحضور للدفاع عن نفسه اثناء التحقيق الجنائي، من اجراء التبليغ بالحضور، وكذلك موعد المرافعة او الجلسة، نوع الجريمة او التهمة المسندة الية، واعلام في حق الدفاع عن نفسة، وتدوين اقوال وعدم ارغام على قول اي شيء ليس صحيحاً، اذ يوجب الدستور احترام الشخص، واحترام حقوق طبقاً للدستور والقوانين المعمول بها، والمتمثل بالإجراءات الجنائية[1].

الفرع الثاني: الاستعانة بمحام وخبير تقني:

ان الغاية من الاستعانة بمحامي للمتهم، هو لضمان المحاكمة العادلة من خلال الدفاع عن حقوق المتهم، والتي تعد من الضمانات الاساسية في اي نظام قضائي عادل، اذ

(١) د. رمزي رياض عوض، سلطة القاضي الجنائي في تقدير الأدلة– دراسة مقارنة، (دار النهضة العربية، القاهرة [٢٠٠٤)، ص٦٥.

تدخل ضمن حقوق الدفاع المكونة للمتهم في مراحل التحقيق والمحاكمة، وان يقدم النصح القانوني في تسريع الاجراءات القانونية، وكذلك الحضور اثناء التحقيق، كما ان دور الخبير التقني يكمن في تمحيص الادلة والتأكيد من سلامة المراسلات والمكالمات الصوتية، والتأكيد على انها لا تبت بصلة من الذكاء الصناعي، وكذلك يكون دور الخبير التقني في فحص الاجهزة والبيانات الرقمية، من تحليل المصادر والرسائل والصور، من اجل تقديم تقرير فني نهائي فيها، او عن القضية المطروحة امام[١].

يتضح لنا ان الدور الفعال الذي يلعبه المحامي، او الخبير التقني، دوراً بارزاً في القضية، من اجل الدفاع عن المتهم من التهم الموجه ضده، وذلك لحماية الحقوق القانونية، خاص في القضايا ذات الطابع الرقمي او التقني، والتي يمكن ان تغير مسار القضية اذ ظهر وجود خلل فيها، وفق معايير العدل والانصاف، من اجل التوصل الى نتائج سليمة.

الفرع الثالث: الطعن في الادلة الرقمية:

تعد اجراءات الطعن بالأدلة الرقمية من اهم النقاط في الدعاوي الجنائية والمدنية الحديثة، نظراً لانتشار التكنلوجيا، وكذلك اعتماد الجهات القضائية على البيانات الرقمية كأدلة، ولكن مثلها مثل اي دليل اخر، يمكن الطعن فيها قانوناً، اذ يتم التشكيك في مشروعيتها وموثوقيتها، او حتى سلامة اجراءات الحصول عليها، اذ يجب جمع الادلة وفق الاذن من القاضي المختص، وفقاً لإجراءات التقاضي الفعال، وان يتم التوثيق على الدليل كان عرضة للاختراق او الفيروسات، او يكون الطعن من خلال فبركات او معدلات استخدام ادوات رقمية، لذا فان الطعن يأخذ مجال في الادلة الرقمية بعد ثاني، قد يكون اثبات بطلان الاجراءات القانونية في جمعها، او شكوك في التلاعب او التزوير، او قصور في التوثيق او الحماية التقنية، او قد يكون في الاستعانة بخبير تقني لدعم الطعن فيها[٢].

(١) د. جميل عبد الباقي الصغير، ادلة الاثبات الجنائي والتكنلوجيا الحديثة، (دار النهضة العربية، القاهرة |٢٠٠٣)، ص٦٠.

(٢) د. كريم خميس البديري، مصدر سابق، ص٧٩.

المبحث الثالث

التحديات والحلول التشريعية

ان من التحديات التي تواجها الحلول التشريعية كثيرة، نظراً لتعقيد البيئة الرقمية فيها، هذا من جهة، ومن جهة اخرى للتطوير التكنلوجيا المستمر، اثر كبير على التحديات القانونية للتحقيق الرقمي، وان هذه التحديات قد لا تؤثر فقط على فعالية التحقيق، بل تذهب الى ابعد من ذلك، اذ تثير ايضاً قضايا تتعلق بالخصوصية الشخصية، وللعدالة، لذا فان لحقوق الافراد، توجب الالتزام بها، وصيانتها وعدم المساس بها، فان غياب القصور التشريعي والقانوني الداخلي، والتي لا تواكب القوانين الوطنية في ظل التطورات الجريمة المنظمة الرقمية واساليب التحقيق الحديثة فيها، يعتبر عائق امام تلك الجهات، في صيانة التحقيق الرقمي، فان انتهاك تلك الخصوصية يشكل ناقوس خطر يدق في عرش العدالة، وذلك من خلال استخدام ادوات المراقبة والتنصت، والتي قد تصطدم بالحقوق الدستورية، والمتمثل بالحماية البيانات الشخصية او حرية التعبير، اذ يكمن من تلك التحديات العابرة للحدود، مما يخلق صعوبة التعاون بيد تلك الدول بكل مهنية وحياد، لا سيما ان اي تأخير في اصدار او تنفيذ اوامر التفتيش للقوانين التقليدية قد لا تسمح بسرعة الوصول الى الادلة الرقمية، بشكل سليم، مما يؤدي الى فقدان قيمتها المعنوي، والمادية، عليه فان الكثير من القضايا التشفير واخفاء المعلومات، والبيانات، خاص في ظل وجود آليات التشفير محصنة، تعيق عمل الاشخاص القائمين على التحقيق الرقمي، في جمع الادلة او حتى في معرفة وجودها، وذلك من اجل التوازن بين الخصوصية الشخصية، والامن الرقمي، من خلال تفعيل دور التعاون الدولي المشترك، عليه وللتوضيح أكثر سوف نقسم هذا المبحث الى عدة مطالب، اذ نتناول في المطلب الاول، الثغرات التشريعية في الضمانات الرقمية، وفي المطلب الثاني، المقاربات المقارنة والتوصيات الاصلاحية، وبالشكل التالي:

المطلب الاول

الثغرات التشريعية في الضمانات الرقمية

نلاحظ انه للتحول السريع نحو العالم الرقمي، اصبحت البيانات الشخصية، والهوية الإلكترونية، في التعاملات الرقمية جزء لا يتجزأ من حياة الافراد والمؤسسات، لذا فان في هذا السياق برزت الحاجة الى الضمانات القانونية والتي تحمي الأفراد من التعدي على خصوصيتهم وحقوقهم الرقمية، غير ان الواقع التشريعي لا يواكب تلك التطورات بشكل كبير في بعض الاحيان، من قبل أطراف مختلفة، اذ يؤدي الى انتهاك قانونية وحقوق تلك الفئة، وللتوضيح أكثر، وللتوضيح أكثر يمكن ان نقسم هذا المطلب الى عدة فروع وبالشكل التالي:

الفرع الاول: غياب النصوص التشريعية:

بالرغم من التقدم الحاصل في التشريعات الداخلية، الا انه لا تزال بعض تلك الدول تفتقر الى قوانين واضحة تعمل الى حماية تلك الخصوصية، والمتمثل بالإنترنت وغيرها، مما يجعل جمع تلك البيانات او مراقبة الأفراد قانونية في بعض الحالات دون موافقة صريح له، حتى وان كانت هناك بعض وجود من القوانين، والتي قد تكون فيها ثغرات في آليات الانفاذ، والمتمثل بضعف العقوبات، او غياب جهة الرقابة المستقلة، او تعقيداتها في تقديم الشكاوى [1].

لذا فان من خلال البحث انه هناك الكثير من القوانين الغير محدثة، او ضعف في صياغتها التشريعية، مما يجعلها غير ملائمة للتحديات الحالية، مثل البيانات البيو مترية، او استخدام تقنيات التتبع عبر التطبيقات، يمكن القول ان العالم الرقمي متسارع، لا ينتظر بطء التشريعات التي لا تواكب التطورات التقنية، التي تترك فراغاً خطيراً يمكن ان يستغل على حساب الافراد او المؤسسات، لذا فان من الضروري ان تتحرك الجهود الدولية، في تكثيف العمل المشترك، لسد تلك الثغرات التشريعية، من اجل ضمان تلك الحقوق الرقمية، وبناء بيئة امنه وعادلة للفضاء السيبراني، في التحقيق الرقمي.

(١) فاضل عباس الملا، مصدر سابق، ص٩٠.

الفـرع الثاني: التداخل بين الامن القومي والحقـوق الفرديـة:

ان في العالم الافتراضي الرقمي يزداد فيه التهديد الامني، وكذلك التطور في الادوات المراقبة والسيطرة، اذ تبرز فيه الجدل بشكل جدي حول تباين العلاقات والآراء جول العلاقة بين الأمن القومي والحقوق الفردية، هذا من جانب، ومن جانب اخر فان الدول تسعى الى حماية اراضيها ومواطنيها من التهديدات، التي طالما برزة في محور التقيد لتلك الحقوق بل والعمل على صيانتها والمناهضة لأي حركة تهدف الى انتهاك لتلك الخصوصية الرقمية، سواء على المستوى الفرد، او على الصعيد الامن القومي، من اجل تحقيق التوازن بين متطلبات الامن القومي، من اجل العمل الى حفاظ على الحريات الاساسية التي تعد جوهر النظم الديمقراطية، عليه فان مفهوم الامن القومي، يشير الى بيان القدرة للدولة على حماية مصالحها الاساسية، بما يشمل السيادة الوطنية، والعمل الى الاستقرار الداخلي، وسلامة المواطنين من التهديدات الخارجية، والمتمثلة بالإرهاب، او ما يعرف بالجريمة المنظمة، اما الحقوق الفردية بصفة عامة هي تلك الحريات الاساسية التي يتمتع بها كل فرد، والمتمثل بحرية التعبير وحرمة الحياة الخاصة، وحرية التنقل وغيرها من الحقوق، اذ تنتهي تلك الحقوق بانتهاك حرية حقوق الغير، والتي نصت عليها الدساتير والمواثيق الدولية، والاعلان العالمي لحقوق الإنسان[1].

نستنتج ان للتدخل بين الامن القومي والحقوق الفردية، واحداً من أكثر التحديات تعقيداً في العصر الحديث، فالأمن لا يجب ان يكون مبرراً لتفويض الحريات، كما لا ينبغي ان تكون الحريات مدخلاً لتقويض الاستقرار، لذا تدعي الضرورة الى تحقيق التوازن بين الشراكة المجتمعية حقيقة لضمان ان تظل الدولة امنة ومواطنيها احراراً.

(١) د. احمد عوض بلال، مصدر سابق، ص٧٤.

المطلب الثاني

المقاربات المقارنة والتوصيات الاصلاحية

ان في اطار مكافحة الارهاب والجريمة المنظمة الكترونياً، والتي توسعت الحكومات في استخدام تقنيات المراقبة، مما آثار مخاوف بشأن الخصوصية وحرية التعبير، فالكثير من المجتمع الدولي عمل الى اعتماد قوانين تسمح لها بجمع البيانات الشخصية، دون موافقة الافراد، اذ دعت الضرورة الى ذلك، وهو ما يعد انتهاكاً واضحاً للحقوق الفردية في نظر العديد من المنظمات الحقوقية، في حالة الازمات، التي تضطر فيها الحكومات الى تقيد حرية الصحافة، ومنها قد تحظر المظاهرات، تحت ذريعة الحفاظ على النظام العام، الا انه هذا قد يستغل سياسة لقمع المعارضين من قبل الاشخاص المتنفذين، التي تقيد التعبير عن الرأي العام، وللتوضيح أكثر يمكن ان نقسم هذا المطلب الى عدة فروع وبالشكل التالي:

الفرع الاول: التشريعات الاوربية والامريكية:

لقد توسعت الولايات المتحدة، في الاثار من حد تلك الحريات في قانون (باتريوت آكت) الذي اقر بعد هجمات ١١ سبتمبر ٢٠٠١ جدلاً واسعاً بشأن التوسع في الصلاحيات والمراقبة الحكومية، والتي اعتبرتها حالة طارئ توجد التوسع في اتخاذ التدابير اللازمة، اما في بريطانيا فقد تكررت الانتقادات للممارسات المراقبة الواسعة التي تم الكشف عنها في اعقاب تسريبات ادوارد سنودن، وايضاً في دولة الصين، فقد اتخذت الامن القومي كغطاء للرقابة الشاملة على المواطنين، وقمع الحريات السياسية، وهو ما يثير انتقادات واسعة من المنظمات الحقوقية الدولية[1].

الفرع الثاني: نماذج من الضمانات المتقدمة:

ان للحقوق الرقمية ضمانات عدة، وهي تدابير او السياسات التي تهدف الى حماية حقوق الافراد في الفضاء الرقمي، والمتمثلة بالخصوصية، في حق التعبير والوصول الى معلومات، والامن السيبراني، والتي توجب على التشريعات حماية تلك البيانات، والمتمثل

(١) د. محمد معروف عبد الله، |"الطبعة الوراثية ودورها في الاثبات الجنائي"|، |مجلة زانكو|، العدد الثامن، جامعة صلاح الدين، أربيل، (٢٠٠٣)، ص٦٦.

باللائحة العامة لحماية البيانات (GDPR) في الاتحاد الاوربي، التي تمنح للأفراد حق التحكم في البيانات، وايضاً قوانين حرية التعبير التي تضمن الحق في التعبير عن الرأي دون رقابة غير قانونية، وكذلك قوانين مكافحة الجريمة الإلكترونية، لحماية الأفراد من الاحتيال، او الابتزاز، والهجمات الإلكترونية، لذا يمكن ان تكون هناك ضمانات اخرى متعددة مثل التشفير في استخدام تقنيات التطبيقات لحماية المحادثات والمعلومات، او اعداد الخصوصية، التي تمكن من رؤية المعلومات او تتبعه عبر الانترنت، وكذلك حمايتها من اختراق الفايروسات، والعمل الى وضع آليات تمكن الافراد من تقديم شكاوى بشأن الانتهاكات الرقمية ومتابعة قضائياً او ادارياً[1].

الخاتمة

ان من خلال البحث في مضمار التحقيق الجنائي الرقمي، وفق معاير الضمانات التي يتمتع بها المتهم، في بيئة الإلكترونية امنة، اذ توصلنا الى عدة نتائج فيه، وعليه يمكن ان نورد عدة مقترحات في هذا المجال:

النتائج:

١. ان التحقيق الجنائي الرقمي أصبح ضرورة ملحة في ظل تزايد الجرائم الإلكترونية بشكل فضيع، لذا باتت من الضروري ان تمتلك الجهات القضائية، وكذلك اجهزة الدول، من نفاذ القانون، وكذلك ادوات وتقنيات رقمية متقدمة للكشف عن الأدلة الإلكترونية، في عملية تتبع الجناة، بمهنية.

٢. البيئة الرقمية تفرض تحديات جديدة على التحقيق الجنائي، في طبيعة الأدلة الرقمية، والمتمثل بسهولة اتلافها، او تغيرها، او صعوبة ربطها مباشرة بشخص معين، اذ تفرض تحديات كبيرة تقع على عاتق القائمين بالتحقيق، اذ يتطلب مهارة عالية فنية، وقانونية متخصصة، للعمل وفق معاير الدق والامان.

---

(١) وليد السيد سليم، ضمانات الخصوصية في الانترنت، (دار الجامعة الجديدة، الاسكندرية |٢٠١٢)، ص٥٩.

٣. الحاجة الى توازن دقيق بين التحقيق وحقوق المتهم، على الرغم من اهمية التحقيقات الرقمية في كشف الحقيقة، إلا ان من ضمانات المتهم مثل الحق في الخصوصية، وسرية الاتصالات، وحق الدفاع يجب ان يبقى مصانة لضمان محاكمة عادلة.

٤. غياب التشريعات الرقمية متخصصة في بعض الدول يفتح الباب للتعسف، في غياب قوانين واضحة لتنظيم التحقيقات الرقمية، قد تستخدم الأدلة الإلكترونية بطرق تنتهك مبدأ الشرعية الإجرائية، او تقبل ادلة تم الحصول عليها بوسائل غير مشروعة.

٥. يلعب الخبراء الفنين الدور الحاسم للخبراء للفنيين، اذ يكمن للخبراء التحقيق الإلكترونية دوراً بارزاً، في شرح للقضايا وتحليل النتائج المعقدة التي تتطلب فهماً تقنياً عميقاً.

التوصيات:

١. مواءمة التشريعات مع المعايير الدولية، والمتمثل باللائحة العامة لحماية البيانات في الاتحاد الاوربي (GDPR)، تكون ملمة ومواكبة للتحقيق الجنائي والرقمي فيها.

٢. حث العمل الجماعي الى تحديث القوانين بشكل دوري لمواكبة التطور التكنلوجيا، والمتقدم المتسارع فيه.

٣. تكثيف الجهود للعمل الى تعزيز الشفافية والمساءلة في جميع البيانات واستخدامها، لتحقيق التوازن بين مصلحة الفرد عن الامن الدولي.

٤. انشاء هيئات مستقلة للرقابة على الانتهاكات الرقمية، لتحديد نقاط الخلل، وتحقيق الرقابة الفعال على المنظومة العنكبوتية.

٥. تكثيف الجهود لتعزيز التوعية الرقمية للمواطنين حول حقوقهم، في بيئة الإلكترونية امنه.

Funding

The author declare that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Conflicts of interest

The authors declare that there Is no conflict of Interest

Acknowledgments

The author would like to express his appreciation to college of law for supplying the materials for this study.

References

First: Books

1- Al-Rubi. Siraj al-Din, Criminal Investigations in Their New Concept, (Dar Al-Masryah Al-Lubnaniyyah, |1997).
2- Al-Jumaili. Abdul Sattar & Aziz. Muhammad, Modern Criminal Investigation - Between Theories and Practice, (Dar Al-Salam Press, Baghdad |1976).
3- Hamdi. Abdul Aziz, Technical Research in the Field of Crime, Crime Detection Series Using Modern Scientific Means, Part One, (First Edition |1973).

4- Al-Tamimi. Abbud, Practical Criminal Investigation, (First Edition |2006).
5- Al-Husayni. Ammar, The Extent of the Legality of Mobile Phone Audio Recordings as Evidence in Criminal Proof, (Consultation in Ahl al-Bayt University Journal, Issue No. 8 |2009).
6- Bilal. Ahmad, The Rule of Excluding Evidence Obtained by Illegal Means in Criminal Procedures, (Second Edition, Dar al-Nahda al-Arabiya, Cairo |2008).
7- Ali. Wasfi, A Brief Introduction to Forensic Medicine, (Legal Library, Baghdad| 2007).
8- Al-Badri. Karim, Expertise in Criminal Evidence, (no publisher, Baghdad |2008).
9- Al-Shahwani. Qaddouri, Crime Scene, (Dar Al-Nahda Al-Arabiya, Cairo |2006).
10- Al-Mulla. Fadhel, Criminal Investigation in the Judiciary of Imam Ali (peace be upon him), (Al-Haidariya Library, |2009).
11- Awad. Ramzi, The Authority of the Criminal Judge in Assessing Evidence: A Comparative Study, (Dar Al-Nahda Al-Arabiya, Cairo |2004).
12- Al-Saghir. Jamil, Criminal Evidence and Modern Technology, (Dar Al-Nahda Al-Arabiya, Cairo |2003).

13- Abdullah. Muhammad, Genetic Imprinting and Its Role in Criminal Evidence, (Zanko Journal, Salahuddin University, Erbil, Issue 8, |2003).
14- Salim. Walid, Privacy Guarantees on the Internet, (Dar Al-Jamiah Al-Jadida, Alexandria |2012).

Second: Lows

1. Iraqi Penal Code No. 111 of 1969.
2. French Criminal Procedure Code No. 141 of 1961.
3. French Constitutional Law No. 38 of 2019.

Third: International agreements

1. The Budapest Convention on Cybercrime of 2001.
2. The International Covenant on Civil and Political Rights of 1966.