جـامعة عمـــــار ثـــــليجي الأغواط
كلية الحقوق والعلوم السياسية
قسم الحقوق (القانون العام)

التحليل الجنائي المعلوماتي

مذكرة تخرج ضمن متطلبات نيل شهادة الماستر حقوق

تخصص: قانون جنائي وعلوم جنائية

من إعداد الطالبتين :

- قفصي نور الهدى
- بن الشطي مريم دعاء الصديقة

تحت إشراف :

- أ.د عبد الوهاب ملياني

اللجنة المناقشة :

الأستاذ. خضرون عطاء الله. رئيسا
الأستاذ د. ملياني عبد الوهاب مشرفا و مقررا
الأستاذ. د. رابحي لخضر مناقشا
الأستاذ. د. بوقرين عبد الحليم مناقشا

السنـــــة الجامعية 2025/2024


بسم الله الرحمن الرحيم

الشكر والعرفان

الحمد لله الذي جعل التربية مشتقة من إسمه ، وجعل اشرف الأعمال أعمال المربين والصلاة والسلام على سيد المرسلين وعلى من إهتدى بهدية إلى يوم الدين وبعد :

لابد لنا ونحن نخطو خطواتنا الأخيرة في هذه المرحلة من الحياة الجامعية بـ وقفة نعود إلى أعوام قضيناها في رحابي الجامعة مع أساتذتنا الكرام الذين قدموا لنا الكثير باذلين بذلك جهد ا كبيرا في بناء جيل الغد لتبعث الأمة من جديد

و قبل أن نمضي في تقديم أسمى آيات الشكر و الإمتنان والتقدير والمحبة إلى الذين مهدوا لنا طريق العلم والمعرفة إلى جميع أساتذتنا الأفاضل.

كن عالما فإن لم تستطع فكن متعلما ، فإن لم تستطع فأحب العلماء، فإن لم تستطع فلا تبغضهم

و أخص بالتقدير والشكر إلى من علمنا التفاؤل والمضي إلى الأمام إلى من وقف إلى جانبنا عندما ضللنا الطريق إلى المشرف الفاضل الذي كان نعم المرشد والموجه : أ.د ملياني عبد الوهاب

الذي نقول له أستاذنا الفاضلُ هذا الثناءُ لكم

فيضُ الينابيعِ والتوجيهِ تسقينا أبدي إحترامي لمن بالعلم سيرنا

لو لاهُ ما عمّتْ الأفكارُ وادينا مهما أقولُ فلن أوفيكَ حقكمُ

يا مَن بذلت الجهدَ كي للوعيِ تُرسينا

ولا يفوتنا في هذا المقام أن أسجل كلمة شكر وعرفان إلى رئيس قسم القانون العام الأستاذ خضرون عطاء الله على ما قدمه لنا من عون ومساعدة طوال مشوارنا الدراسي برحاب صدره ووسع قلبه مع أصدق الدعوات له بالتوفيق لخدمة العلم

ولا يفوتني أن أتقدم بجزيل الشكر إلى أعضاء لجنة المناقشة: أ.د لخضر رابحي

و إلى. أ د عبد الحليم بوقرين اولا لما قدماه لنا من توجيهات في مسارنا الدرسي وثانيا لقبولهم مناقشة مذكرتنا

والى كل اساتذة قسم الحقوق

كما نتقدم بأحر عبارات اشكر إلى والدينا

وفي الختام أتقدم بخالص شكرنا وتقديرنا وعرفاننا لكل من ساهم ونصح وأرشد من أجل إخراج هذه الدراسة إلى النور .

مقدمـــة

مقدمة

قد شهد القرن الماضي ثورة من نوع غير مألوف أصطلح على تسميتها بثورة المعلومات أو التقنية الجديدة، والتي أضافت كثيرا من الإيجابيات في حياتنا اليومية، إلا أنه يحمل في نفس الوقت بين طياته مخاطر ضخمة تهدد قيم وحقوق وأمن الأفراد والجماعة فقد أدى الاستعمال الغير المشروع إلى ظهور أنماطا جديدة من الجريمة وسلوك المجرمين ومن بين هذه الأنماط الحديثة التي أفرزها التزاوج بين وسائل الاتصال والتكنولوجيا الحديثة، الجريمة الكترونية أو الجريمة المعلوماتية وغيرها من المصطلحات كالجريمة السيبرانية، فرغم اختلاف التسميات إلا أنها تبقى من الجرائم التي خرجت عن المألوف، التي تعبر عن الجرائم المرتبطة بالانظمة الالكترونية المستحدثة والشبكة المعلوماتية .

ولعل تمثل الجريمة الكترونية الفعل الإجرامي الذي أخذ بعدا أكثر تعقيدا، كون أن مسرح ارتكابها ليس كبقية مسارح ارتكاب الجريمة التقليدية، فهو غير ملموس و غامض يحتاج لمعرفة كبيرة بواقعه، وهي جرائم تُرتكب باستخدام الحواسيب أو الأجهزة الذكية أو الشبكات الرقمية، تستهدف الأفراد أو المؤسسات أو حتى الدول لأن اجرام المعلوماتي لا تحده حدود ولا تأثر عليه بعد المسافات.

والجزائر مثل باقي الدوال تعاني من آثارا الجرائم الإلكترونية بسبب نقص الوسائل التكنلوجية المساعدة على اكتشافها و متابعة مرتكبيها و التحقيق فيما نسب اليهم، الأمر الذي استوجب على المشرع الجزائري اتخاذ الخطوات التشريعية الضرورية لمواجهة مثل هذه الجرائم عن طريق سن نصوص قانونية تتوافق مع هذه الانشط الإجرامية الجديدة[1].

وهذه الجرائم المعلوماتية اليوم، وان كانت حاضرة في تشريعنا الجزائي بجانبه الموضوعي في القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات من الباب الثاني لقانون العقوبات للجنايات والجنح ضد الأفراد المستلهم من قانون **قودوفران** "**Godfrain**" الفرنسي المتعلق بالغش المعلوماتي والتي لا تزال قاصرة وتحتاج الى تنقيح واضافات للإحاطة بجميع الجوانب الموضوعية لهذه الظاهرة الاجرامية[2].

و في الجانب الاجرائي للتحقيق في مثل هذا النوع من الجرائم صدرت عدة القوانين بالتشريع الوطني، تصدرها القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 (ج.ر.84.ص.8)المتعلق بالتنصت و الاعتراض الالكتروني وتعديل القانون المدني بالقانون رقم 05-10 المؤرخ في 20 يونيو

[1] جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، اطروحة دكتوراه، كلية الحقوق و العلوم السياسية بجامعة مولود معمري ،تيزي وزو، 2018، ص 2

[2] يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية: الجزائر،2018، ص ص 320-325.

2005 (ج.ر.44.ص24) بإضافته للمادة 324 مكرر المتعلقة بالتوقيع الالكتروني والقانون رقم 08-01 المؤرخ في 23 يناير 2008 يتمم القانون رقم 83-11 المتعلق بالتأمينات الاجتماعية، ونجد أهمها على الاطلاق القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة المتعلقة بالوقاية ومكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال (ج ر 47، ص05) و المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، المتعلق بتحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها(ج ر 53، ص16)

فإذا كانت الجهات المكلفة بالبحث والتحري عن الجريمة والمجرمين متعودة على التعامل مع الجريمة بصورتها التقليدية التي يمكن اكتشافها من خلال الآثار المادية، فان الاشكال والصعوبة في الجرائم الإلكترونية يبدأ من خلال الجانب الإجرائي الذي يخص البيئة الافتراضية التقنية[1]، فظهرت الحاجة إلى توظيف تكنولوجيا المعلومات في الجانب الأمني والتحقيقي، وهو ما أفرز فرعًا حديثًا من فروع العلوم الجنائية يعرف بـ **التحليل الجنائي الرقمي(Digital Forensics)** ، والذي يُعنى باستخلاص وتحليل الأدلة الرقمية من الأجهزة والأنظمة الإلكترونية بطريقة علمية وتقنية قابلة للاستعمال القضائي.

وقد أصبح التحليل الجنائي الرقمي اليوم أداة لا غنى عنها في مكافحة الجرائم المعلوماتية، حيث يمكّن من تتبع الأثر الرقمي للمجرمين، واسترجاع المعلومات المفقودة أو المخفية عمدًا، وتحديد هوية الجناة حتى في ظل محاولات التمويه والتخفي.

في الأصل، كان مجال التحليل الجنائي الرقمي يشمل فقط أجهزة الكمبيوتر ، وخاصة أجهزة الكمبيوتر الشخصية، لكن الآن توسع مجال التحليل الجنائي الرقمي ليشمل التحليل الرقمي للشبكات أيضًا ، ويتضمن مجالات الخبرة مثل التحقيق في انتهاكات أمن الشبكات ومحاولات القرصنة وسرقة البيانات.

مع إدخال معالجة الكمبيوتر في الأجهزة الأخرى، مثل وحدات نظام تحديد المواقع العالمي (GPS) ، والسيارات، والهواتف الخلوية، وآلات النسخ والفاكس، وما إلى ذلك ، توسع المجال لإضافة تخصصات فرعية إضافية

وتكمن **أهمية الدراسة** في كونه يتطرق إلى التحليل الجنائي الذي يستخدم في الجرائم الالكترونية، خاصة وأن هذه الاخيرة تتميز بنوع من الخصوصية من حيث إجراءات متابعتها من جهة و كذا صعوبة اثباتها من جهة أخرى بالإضافة الى الصعوبات التي تواجه المحققين في الكشف عنها وتتبع مرتكبيها، مما يعكس صعوبة تحليل الدليل الرقمي.

وبالتالي **يهدف** هذا البحث إلى التعرف على مفهوم التحليل الجنائي الرقمي ومجالات استخدامه في ظل تطور الجريمة وصولًا إلى الجريمة المعلوماتة. والعمل على استعراض الأدوات والأساليب

[1] نعيم سعيداني : أليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في العلوم القانونية، كلية الحقوق و العلوم السياسية ، جامعة الحاج لخضر باتنة، 2012-2013، ص 4

المستخدمة في التحليل الرقمي الجنائي مع مناقشة التحديات القانونية والتقنية التي تواجه هذا المجال، وذلك لإثبات الدليل الجنائي الرقمي

و بالنسبة لأسباب فتنقسم إلى أسباب ذاتية و أخرى موضوعية:

فالأسباب الذاتية الشغف بكل ما هو جديد في عالم تقنية وتكنولوجيات الاعلام والاتصال وكذلك رغبتنا في البحث في مجال الجريمة المعلوماتية وآليات التحري عليها. و الرغبة الشخصية في التعمق في التقاطع بين القانون والتكنولوجيا، إذ يمثل الموضوع ملتقى للعلوم القانونية والعلوم الرقمية، وهو مجال معرفي ديناميكي يواكب المستقبل، ما يجعله مجالًا محفّزًا للبحث والتطوير العلمي

اما **الاسباب الموضوعية** قد جاء اختيارنا لهذا الموضوع استجابةً لعدة اعتبارات علمية وعملية، أهمها: تزايد الجرائم الرقمية وأهمية التحليل الرقمي في التحقيقات الحديثة كما هو الحال الى قصور الإطار القانوني الجزائري.

كذلك قلة الدراسات الأكاديمية في هذا المجال حيث يُلاحظ ندرة الدراسات الجزائرية والعربية التي تتناول التحليل الجنائي الرقمي من زاوية قانونية تحليلية، ما يفتح المجال أمام البحث العلمي لسدّ هذا الفراغ المعرفي والمساهمة في إثراء النقاش.

وقد اعتمدنا في دراستنا على

دراستي **هروال هبة نبيلة: جرائم الأنترنت، دراسة مقارنة،** أطروحة دكتوراه تخصص القانون كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2014/2013.

الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، مصر (الاسكندرية): دار الفكر الجامعي، 2022، توصلنا من خلالهما إلى نتائج اهمها:

– وجود فراغ تشريعي كبير في غالبية الدول العربية فيما يتعلق بالجرائم الالكترونية و هذا ما ساعد مجرمي الأنترنت و يسر لهم ارتكاب جرائمهم بكل راحة.

– م واجهة المشرع الجزائري للتطور التكنولوجي الذي اجتاح جميع نواحي الحياة لا سيما مجال الاتصالات السلكية و اللاسلكية بإعداده للقانون09-04

وتتفق دراستنا مع هذه الدراسات في تطرقها إلى موضوع الجريمة الالكترونية خاصة من الناحية الموضوعية، بينما تختلف هذه الدراسة من حيث تناول التحليل الجنائي الرقمي في مثل هذه الجرائم و مدى مشروعيتها خاصة بالنسبة للمشرع الجزائري و هو ما سيشكل نقطة اختلاف تميز دراستنا عن باقي الدراسات السابقة و هو ما يشكل اضافة في مجال البحث العلمي، وهو يوضح اختلاف وعدم تكرار ما تم دراسته.

دراسة نعيم سعيداني : **أليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري،** رسالة ماجستير في العلوم القانونية، كلية الحقوق و العلوم السياسية ، جامعة الحاج لخضر باتنة .

اشكالية الدراسة:

مع تطور اساليب المجرمين في اختراق الانظمة، سرقة البيانات أو حتى تنفيذ هجمات الكترونية معقدة، تطورت ايضا آلات التحقيق و الكشف عن هذه الجرائم. فقد ساهم التحليل الجنائي المعلوماتي في تحويل البصمات اللرقمية الى ادلة ملموسة، مما عزز قدرة الاجهزة الامنية والقضائية على مواكبة التحديات الحديثة، فاذا استطاع هذا الفرع المتخصص ان يحدث نقلة نوعية في مواجهة الجرائم المعلوماتية فـ **كيف ساهم التحليل الجنائي الرقمي في تطوير آليات الكشف عن الجرائم الإلكترونية لضمان فعالية التحقيق؟** هذا ما سنحاول استكشافه من خلال الاشكالية الطروحة وذلك بتجزأتها الى اسئلة فرعية:على النحو التالي:

- هل للجريمة المعلوماتية تعريف محدد ؟ و ما يميزها عن الجريمة التقليدية؟
- ماهو الدليل الرقمي ؟ ماهي خصائصه؟
- ماذا نقصد بالتخليل الجنائي المعلوماتي ؟
- فيما تتجسد اجراءات تحليل وجمع الادلة الرقمية

وبالنسبة للمنهج المعتمد في هذه الدراسة فقد اخترنا المنهج **الوصفي** والذي يتطرق من جهة إلى وصف الجريمة اللمعلوماتية والدليل الرقمي من خلال التعريف وذكر خصائصها بالإضافة إلى تعريف التحليل الجنائي في مثل هذه الجرائم، ومن جهة أخرى يضم **التحليل** من خلال دراسة الأساليب التي تستخدم في التحري ومدى مشروعيتها وهذا ما يتم استخلاصه من تحليل النصوص القانونية ودراسة الجوانب الإجرائية الخاصة بها.

للإجابة على هذه الإشكالية تم اعتماد خطة ثنائية تكونت من فصلين حيث تمحور الفصل الاول حول الاطار المفاهيمي للدراسة تمثل في تحديد الاساسيات العامة للجريمة المعلوماتية والدليل الرقمي من خلال مبحثين، حيث تطرقنا في المبحث الاول الى مفهوم الجريمة المعلوماتية، خصائصها و أركانها وفي المبحث الثاني تناولنا مفهوم الدليل الرقمي وخصائصه.

و بعد القاء نظرة عامة عن الجريمة المعلوماتيى والدليل المعلوماتي من الناحية الموضوعية في الفصل الاول، قمنا بتخصيص الفصل الثاني الى التحليل الجنائي بتحديد القواعد و الجوانب الفنية والإجرائية للتعامل مع الدليل الرقمي، تطرقنا في المبحث الاول إلى فنيات الحصول على الدليل الرقمي، المبحث الثاني: الجوانب الإجرائية للحصول على الدليل الرقمي.

الفصل الأول:
الاطار المفاهيمي للجريمة المعلوماتية
و الأدلة الرقمية

تمهيد

مع التحول السريع في العصر الحديث الى العصر الرقمي وانتشار تكنولوجيا المعلومات والاتصالات بصورة مسيطرة على جميع المجالات، في مقابل هذا التطور زادت جرائم الإنترنت بشكل كبير وهذا الامر يُعزى هذا الارتفاع إلى الوفرة الكبيرة من البيانات والمعلومات على الإنترنت والتي يمكن استغلالها من قبل الجرائم الإلكترونية، حيث أن هذه الجرائم تشمل الاحتيال الإلكتروني، والاختراقات السيبرانية، والتجسس الإلكتروني، وانتهاكات حقوق الخصوصية، والكثير من الأنشطة غير القانونية الأخرى على الإنترنت، هذا الامر الذي عجل بالكثير من الخسائر للأفراد والمؤسسات والدول كل بدرجات مختلفة، لهذا كان التوجه الى مواكبة تطور هذه الجرائم من خلال العمل على تطوير أساليب المواجهة و التحقيق والاثبات الامر الذي وصل في الأخير الى التحليل الجنائي الرقمي

ولكي نصل الى فصل شامل عن الاطار المفاهيمي للتحليل الجنائي الرقمي في جرائم المعلومات و البيانات لهذا قسمنا الفصل الى:

المبحث الأول: اساسيات عن الجريمة المعلوماتية

المبحث الثاني: مفهوم الدليل الجنائي الرقمي

االمبحث الاول: اساسيات عن الجريمة المعلوماتية

ان توجد علاقة بين نظام الحاسب الالكتروني وارتكاب بعض الجرائم هو نتيجة طبيعة للتطور الحالي سواء كان الحاسب موضوعا للتحليل أو وسيلة لذلك الوسائل المعلوماتية يزيد من فرص انتشار هذا النوع الجديد من الجرائم لمعلوماتية الانحراف المعلوماتي.

ومن بين الجرائم المستحدثة الاخرى الجريمة الالكترونية ولم يتفق فقهاء القانون الجنائي في القانون المقارن على الوصف القانوني السليم أو التسمية الدقيقة لهذا المصطلح وهذا ما يثبت أن هذه أن هذه الظاهرة معقدة و لايمكن حصرها وتمس بالعدد من المجالات و من هناك من المفاهيم المتقاربة المشتقة من الإجرام المعلوماتي والغش المعلماتي، الانحراف الذي يقع بواسطة الحاسب الآلي ، الجرائم المرتبطة بالإعلام الآلي، وهذا التعدد ناتج عن الصور المختلفة لتطبيقات الكمبيوتر في أفعال غير مشروعة مرتبطة بالمعلوماتية.[1]

المطلب الاول: المصطلحات الدالة على ظاهرة الجرائم المعلوماتية

هناك تباين كبير بشأن تحديد المصطلحات المستخدمة للدلالة على الظاهرة الإجرامية الناشئة في بيئة الحاسوب وسبب هذا التباين هو التطور السريع الحاصل في بيئة الحاسوب والانترنت هنا في ما يلي أهم المصطلحات التي تدل على الجرائم السيبرانية وهي:

1- مصطلح تقنية المعلومات :

وهذا المصطلح نتيجة للتزاوج الحاصل بين الميدانيين الحوسبة والاتصال وتعرفها منظمة اليونسكو بأنها " الفروع العلمية والتقنية والهندسية و أساليب الإدارة الفنية المستخدمة في التداول ومعالجة المعلومات وفي تطبيقاتها والمتعلقة بالحواسب وتفاعلها مع الإنسان والآلات وما يرتبط بذلك من أمور اجتماعية واقتصادية وثقافية "[2]. واستخدمت تعبير جرائم تقنية المعلومات للدلالة على الجرائم الالكترونية.

2- مصطلح إساءة استخدام الحاسوب:

والشائع استعمال هذا المصطلح مع بداية نشوء ظاهرة الجرائم السيبرانية واستعمل في التشريعات[3].

3- مصطلح احتيال الحاسوب أو الغش الحاسوب

[1] P.CATALA, **Informatique et Droit Pénale ,** édition Cujas,Paris,P18 **et M**. chawky, essai sur notion de cybercriminalité ,iehel ; juillet,2006,p16, disponible sur : www.iehei.org.bibliotheque, cyber crime .pdf la date de consultation 05/03/2025

[2] يونس عرب، الجرائم السيبرانية والانترنت موسوعة القانون وتقنية المعلومات. عمان:إتحاد المصاريف العربية،2002،ص207.

[3] علي حسن الطوالبة، الجرائم الالكترونية. البحرين:مؤسسة فخراوي للدراسات والنشر،2008 ، ص.42

وهي مصطلحات استخدمت للتعبير عن أفعال الجرائم السيبرانية وصورها وليس على الظاهرة برمتها وهناك تعبيرات مشابهه مثل الغش المعلوماتي والاحتيال المعلوماتي ونصب الحاسوب[1].

4- الجرائم الاقتصادية المرتبطة بالحاسوب

وهو تعبير يتعلق بالجرائم التي تستهدف معلومات قطاعات الأعمال أو تلك التي تستهدف السرية وسلامة المحتوى وتوفر المعلومات وبالتالي يخرج من نطاقها الجرائم التي تستهدف البيانات الشخصية أو الحقوق المعنوية عن المصنفات الرقمية وكذلك الجرائم ذات المحتوى الضار أو غير المشروع وكذلك لا يعتبر هذا المصطلح كاملاً لكافة أنماط الجرائم الالكترونية[2].

5- مصطلح جرائم أصحاب الياقات البيضاء

لم يظهر هذا المصطلح من الجرائم إلا حديثاً ويرجع الفضل في ذلك إلى عالم الاجتماع لاند وترتكب هذه الجرائم من قبل الطبقة الراقية في المجتمع ذوي المناصب الإدارية الكبيرة وتشمل أنواع المختلفة من الجرائم الاختلاس والسرقة وتزوير العلامات التجارية للشركات العالمية، ووضعها على المنتجات المحلية أو عالمية غير مشهورة، واستفادة مرتكب هذه الجرائم من انتشار الانترنت في تطوير جرائمهم وطرق ارتكابها وتوسعت الرقعة الجغرافية لها بحيث أصبحت عالمية بعد ما كانت محلية[3].

6- اصطلاح جرائم الكمبيوتر والجرائم المرتبطة بالحاسوب.

عبر عن المصطلح الأول جرائم الكمبيوتر للدلالة على الأفعال التي يكون الحاسوب فيها هدفاً للجريمة كالدخول غير المسرح وإتلاف البيانات المخزنة في النظم. أما المصطلح الثاني الجرائم المرتبطة بالحاسوب فهي تلك الجرائم التي يكون الحاسوب فيها وسيلة لارتكاب الجريمة كالاحتيال والتزوير وغيرها وأطلق مصطلح جرائم الانترنت أو في مؤتمر الجرائم الانترنت المنعقد في استراليا لفترة من 16 إلى 18 فيفري1998[4].

---

[1] نفس المرجع أنف الذكر، ص43.

[2] نفس المرجع انف الذكر،ص43.

[3] عبدالله عبد العزيز اليوسف، التقنية والجرائم المستحدثة،أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها،أكاديمية نايف العربية للعلوم الأمنية،1420،ص 195.

[4] عبد الرحمان محمد بحر، معوقات التحقيق في جرائم النترنات:دراسة مسحية على ضباط الشرطة في دولة البحرين،رسالة ماجستير غير منشورة،اكاديمية نايف للعلوم الأمنية،الرياض،1420،ص03.

وأصبح هذين المصطلحين هما المستخدمين لدى فقهاء القانون في التعبير عن الجرائم المرتكبة على الكمبيوتر أي كافة الصور الجرائم السيبرانية سواء كان الحاسوب هدفا أم وسيلة وما يزال يستخدم المصطلحات حتى بعد ظهور الانترنت فأصبح المصطلح الجرائم السيبرانية أكثر استخدماً[1]

7- مصطلح نطاق أو فضاء الجرائم الالكترونية

استخدم هذا المصطلح الفقهاء في أوروبا حيث أن كلمه سيبرCyber تستخدم لدى الأكثرية بمعنى الانترنت وقد انتقلت دلالة هذه سلاح إلى تقنية المعلومات فصار يستخدم للإشارة إلى وصف مجموعة المرتبطة في ما بينها بوسائط الاتصال والمفاهيم المعرفية كون المعلومات الذي يرتكز على شبكة الانترنت والشبكة العنكبوتية العالمية والشبكات الحاسوبية الوطنية والمحلية منظمة النشرات الحاسوبية التي تؤمن الاتصال الحي بين الجميع الجهات التي استوطنت هذه البيئات الجديدة.

8- مصطلح إساءة استخدام تكنولوجيا المعلومات والاتصالات

واستخدم في القانون العربي النموذجي الموحد لمكافحة إساءة استخدام تكنولوجيا المعلومات والاتصالات في شأن مكافحة هذه الجرائم.

9- الجريمة السبيرانية:

وتتكون الجريمة السيبرانية من مقطعين هما (cyber-crimes) ، والمقصود (crimes) الجريمة و(cyber) الإلكترونية ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات أما الجريمة فهي السلوكيات والأفعال الخارجة عن القانون ويمكن أن نقول أن الجرائم السيبرانية هي المخالفات التي ترتكب ضد الأفراد أو المجموعات، بدافع الجريمة ويقصد إيذاء سمعة الضحية أو إلحاق أذى مادي أو عقلي بالضحية بشكل مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت وغرف الدردشة والبريد الالكتروني والموبايل[2].

المطلب الثاني: مفهوم الجريمة المعلوماتية

على الرغم من محورية مصطلح الجريمة المعلوماتية أوالإلكترونية " cyber crime " في العديد من الدراسات الأكاديمية التي تتناول التهديدات الإلكترونية في العصر ألحديث إلا أنه لا يوجد اتفاق على تعريف محدد لماهية الجريمة المعلوماتية وعناصرها وأشكالها.

[1] شيماء عبد الغني محمد عطاء الله،الحماية الجنائية للتعاملات الإلكترونية .الإسكندرية: دار الجامعة الجديدة،2007،ص19.

[2] مريم عبد الرحمان،مفهوم الجريمة السيبرانيةومراحلها التاريخية، مجلة الحوار السياسية والثقافية، العدد(171،)جويلية 2020 ومتاح أيضا على موقع المجلة:http://alhiwarmagazine.blogspot.com/2020/07/blog-post_10.html

الفرع الاول: مختلف التعاريف عن الجريمة المعلوماتية

و ما تجدر الاشارة اليه أن المصطلحين الأكثر شيوعا و استعمالا في الدراسات الحديثة و المتعلقة بالموضوع هما : الجريمة الالكترونية والجريمة المعلوماتية و قد إخترت إستعمال المصطلح الثاني و الذي ارتأينا ان استخدامه في هذه الدراسة هو الافضل لكونه الاكثر استعمالا في القوانين العربية المتعلقة بالموضوع، و هو الاقرب الى اللغة العربية من مصطلح الالكترونية

ويدل هذا المصطلح على الجرائم الواقعة على البيانات المعالجة آلية ويستخدم في وصف الظاهرة الإجرامية المستحدثة وتبعاً لذلك أطلقت تعبيرات الجرائم المعلوماتية أو إجرام المعلومات ومحلها لدى جانب من الفقه المالي المعلوماتي[1].

- **أولا – التعريف الفقهي:**

لقد أعطى الفقهاء والدارسون عددا ليس قليلا من التعريفات تتميز وتباين تبعا لموضع العالم المنتمية إليه وتبعا لمعيار التعريف ذاته، وقد اجتهدنا في جمع غالبية التعريفات التي وضعت في هذا الحقل

أو أنها :" الجريمة التي يكون محلها أو موضعها المعلومات بصرف النظر عما إذا كان الحاسب هو الوسيلة المستخدمة من عدمه أو أنها كل الغش معلومات ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها"[2].

وقد عرفتها الباحثة **هدى قشقوش** على أنها: " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات والجرائم السيبرانية مجموعة الجرائم التي تتصل بالمعلوماتية."[3]

ويعرفها الفقيه (**Boon Bipant**) في كتابه Fehling computer يرى بأنها:" أي فعل متعمد مرتبط بأي وجه بالحاسبات يتسبب في تكبير أو إمكانية تكبيد المجني عليه بخسارة أو حصول أو إمكانية حصول مرتكبيه على مكسب"[4].

ويعرفها خبراء منظمة التعاون الاقتصادي والتنمية للغش المعلوماتي بأنها : "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها وأيضا هي كل فعل أو امتناع

---

[1] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن. القاهرة:دار النهضة العربية،1993 ،ص17.

[2] محمد علي سويلم، الحماية الجنائية للمعاملات الإلكترونية (الجرائم المعلوماتية والإلكترونية). الإسكندرية:دار المطبوعات الجامعية،2018،ص49.نقلا عن:

M.alterman et H.bloch, la fraud informatique ,Gazette de plais, Paris,3 sept1988,p 530.

[3] هدى قشقوش، مرجع سابق، ص20.

[4] نفس المرجع الانف الذكر، ص 28.

من شأنه الاعتداء على الاموال المادية أو المعنوية يكون ناتج بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[1].

وقد عرفها الفقيه روزنبلات بأنها: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو وصول إلى معلومات المخزنة داخل الحاسوب والتي تحول عن طريقة"[2].

ويعرفها البعض الآخر من خلال مراحلها يراها الاستاذ **باكر ان** الجريمة السيبرانية تمر بست مراحل وهي:

1) البحث عن نظام الحاسب الآلي المقصود بالجريمة
2) الوصول إلى نقطة الضعف في نظام المعلومات
3) الاستفادة من نقطة الضعف والتحكم في النظام
4) تنفيذ سلوك الاجرام المقصود.
5) تحويل السلوك لربح غير مشروع للفاعل أو خسارة للمجني عليه.
6) اخفاء جميع الادلة تجنبا لكشف الجريمة و فاعلها.[3]

بعد التعرض للمحاولات الفقهية لتعريف الجريمة المعلوماتية سنتناول فيما يلي **التعريف القانوني لهذه الجريمة من طرف المشرع الجزائري.**

عرف المشرع الجزائري الجريمة المعلوماتية في المادة الثانية من القانون 09-04 والتي سماها "**الجرائم المتصلة بتكنولوجيا الاعلام والاتصال** " بأنها: " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية[4]".

الملاحظ من خلال قراة المادة السالفة الذكر هو أن المشرع الجزائري اعتمد في تعريف الجريمة المعلوماتية على معيارين هما: معيار موضوع الجريمة ومعيار وسيلة ارتكاب الجريمة والتي نستعرضها فيما يلي[5]:

---

[1] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات.اسيوط:مكتبة الآلات الحديثة،1992،ص111.

[2] محمد شتا، **فكرة الحماية الجنائية لرامج الحاسوب**. مصر (الإسكندرية): دار الجامعة الجديدة، 2001، ص 20.

[1] Parker (D.B) ; combattre la crime pénalité informatique edition1985,p18.

[4] المادة 02 من القانون رقم 09-04 المؤرخ في 5 أوت 2009. الجمهورية الجزائرية الديمقراطية الشعبية : الجريدة الرسمية، العدد47، الصادرة بـ 2009/8/16 المتضمن قانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، ص 05.

[5]عبد القادر عميمر، التحديات القانونية لاثبات الجريمة المعلوماتية، الجزائر(تلمسان): النشر الجامعي الجديد، 2021، ص ص 18-20.

1- التعريف على اساس معيار موضوع الجريمة: اعتمد المشرع الجزائري موضوع أو محل الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات كأساس لتحديد الجريمة المعلوماتية، وهي الجرائم المحددة في الفصل السابع مكرر من قانون العقوبات تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، والتي تحكمها المواد من 394 مكرر الى 394مكرر 7 من هذا القانون.

2- تعريف على اساس معيار وسيلة ارتكاب الجريمة: أضاف المشرع هذا المعيار وهي المنظومة المعلوماتية أو نظام الاتصالات الالكترونية ، بالقول: " ... و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية[1] أو نظام للاتصالات الإلكتروني، فوسيلة ارتكاب الجريمة أو تسهيل ارتكابها في هذا اتعرف هي محل اعتبار في تكيف الجريمة.

وهنا يمكن القول أن الجريمة المعلوماتية حسب المشرع الجزائري تنقسم الى طائفتين تظم **الطائفة الأولى** الجرائم التي ترتكب ضد نظام المعالجة لآلية للمعطيات وتستهدف المساس الكلي أو الجزئي بهذه المنظومة، وهي الجرائم المنصوص عليها في الفصل السابع مكرر من قانون العقوبات تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات.

فيما تتمثل الطائفة الثانية كل الجرائم الاخرى المنصوص عليها في قانون العقوبات أو في القوانين الخاصة التي يتم ارتكابها أو يتم تسهيل إرتكابها بإستخدام منظومة معلوماتية أو أي نظام للاتصالات.

و نخلص في الاخير الى القول ان الجريمة المعلوماتية هي الجريمة التي يكون محلها المعطيات المعالجة بلغة الالة أي المعلومات والبرامج، أو بمفهوم أوسع النظام المعلوماتي، إضافة إلى وسيلة ارتكابها الكمبيوتر أو أية وسيلة إلكترونية لها نفس إمكاناته، لأنه لا يمكن الدخول الى النظام بدونه.

الفرع الثاني: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بمجموعة من الخصائص منها خصائص ذاتية متعلقة بالجريمة في حد ذاتها، وخصائص تستمدها من وسائل وأساليب إرتكابها، وخصائص أخرى تستمدها من سمات مرتكبيها و دوافع إرتكابها وسنتطرق في هذا المطلب لكل نوع من هاته الخصائص على حدة.

أولا : الخصائص الذاتية للجريمة المعلوماتية

ان ما نقصد به من ذاتية الجرائم المعلوماتية هو استقلاليتها وتميزها عن غيرها من الجرائم لا سيما التقليدية منها، وذلك بمجموعة من الخصائص أثرت بشكل مباشر على التشريعات العقابية والإجرائية التقليدية القائمة، وسوف نحاول أن نبرز أهم هذه الخصائص فيما يلي:

[1] المنظومة المعلوماتية :حسب تعريف القانون الجزائريهي:"أي نظام منفصل، أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، ويقوم واحد منها أو اكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

1- الجريمة المعلوماتية جريمة عابرة للحدود:

إن انتشار شبكة الأنترنت أعطى إمكانية واسعة لربط عدد كبير من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية، دون أن تخضع لحدود الزمان والمكان، لذلك فمن السهولة أن يكون المجرم في بلد والمجني عليه مقيما في بلد أخر، وهنا تظهر الحاجة لوجود تنظيم دولي وداخلي متلائم معه لمكافحة هذا النوع من الجرائم وضبط فاعليتها.

تبعًا لذلك، لم تعد الجريمة المعلوماتية تحترم حدود الدول، بل غدت تمثل نمطًا جديدًا من الجرائم العابرة للحدود، خاصة أن الطبيعة التقنية لهذه الجرائم سمحت بخرق القوانين من بُعد، دون الحاجة إلى التواجد المادي في مسرح الجريمة. ويمكن القول إن الساحة الجغرافية للجريمة المعلوماتية قد اتسعت لتصبح عالمية، فالفاعل قد يوجد في بلد، ويقوم بالاعتداء على نظم معلومات أو بيانات تقع في بلد ثانٍ، وربما يكون الضرر اللاحق واقعًا على ضحية في بلد ثالث. وهذا ما يظهر جليًا في حالات تصميم البرامج الخبيثة (الفيروسات) في مكان معين، ثم يتم نسخها وتوزيعها على نطاق عالمي[1] .

وتتجلى خطورة هذه الخصوصية بشكل أوضح في القطاع المالي، لا سيما في المعاملات البنكية التي تتم عبر الشبكات العالمية. فقد أدى الاعتماد المتزايد على الحواسيب والاتصالات الرقمية إلى توسع نطاق الجرائم الإلكترونية ذات الطابع المالي، خصوصًا تلك المرتبطة بالتحويل الإلكتروني للأموال والتبادل الرقمي للمعلومات المصرفية

إن الميزة الأساسية التي تميز الجريمة المعلوماتية هي التباعد المكاني بين مرتكب الجريمة من جهة، وأداة ارتكابها أو محل الاعتداء من جهة أخرى. وهذا التباعد قد يكون داخل حدود الدولة نفسها، أو عابرًا للحدود إلى دول أخرى، مما يُحدث إشكاليات قانونية معقدة، أبرزها: تحديد الدولة صاحبة الاختصاص القضائي، ومدى قابلية الأدلة الرقمية للجمع والاعتراف بها قانونًا. حيث تختلف النظم القانونية من دولة إلى أخرى فيما يتعلق بحجية الأدلة المستخرجة من الحواسيب والأنظمة الرقمية[2].

وان كانت الجريمة المعلوماتية لا تنفرد لوحدها بهذه الخاصية لوجود بعض الجرائم الاخرى التي تتمتع بها كجرائم الارهاب الدولي وجرائم المخدرات، ووغسيل اللاموال الا انها لا تستلزم الانتقال عبر الحدود و الخضوع لاجراءات التفتيش و المراقبة كما هو الشان في الجرائم التقليدية[3].

---

[1] سعيد النعمان، الجريمة المعلوماتية: مفاهيمها وأشكالها القانونية، عمّان: دار الثقافة للنشر والتوزيع، 2015، ص 88.

[2] عبد الكريم شفيق، الجرائم المعلوماتية: دراسة قانونية مقارنة، الإسكندرية: دار الفكر الجامعي، 2018، ص 125.

[3] محمود احمد عبابنة، جرائم الحاسوب و أبعادها الدولية، الاردن (عمان): دار الثقافة للنشر و التوزيع،2009، ص34.

2- سهولة ارتكاب الجريمة المعلوماتية

لا تحتاج الجريمة المعلوماتية الى جهد عضلي في ارتكابها بل تعتمد على القدرات الذهنية للجاني،و تحكمه الجيد في الحاسوب و وسائل الاتصال الحديثة، و لايحتاج الجاني في ارتكابها الى التنقل او الاستعانة بمركبة لحمل المسروقات، كما أنه لا يحتاج في بعض الاحيان لمساعدة شخص اخر لارتكاب جريمته من اجل الترصد و الحماية، بل يمكن ان يقوم الجاني بجريمته في أي مكان حتى ولو كان مزدحم بالاشخاص[1] .

3- الجريمة المعلوماتية لها اثار رقمية

توصف الجريمة المعلوماتية بأنها لا تترك آثار مادية كالتي تتركها الجرائم التقليدية فلا وجود للكسر أو بقع دم، وكل ماتخلفه هي آثار رقمية ليس لها وجود مادي ملموس، كما ان الوسائل التي ترتكب بها لا تحدث جروحا ولا تسيل دماء بل هي عبارة عن اجهزة الكترونية، كما انها جريمة لا يستعمل فيها العنف الجسدي على الاطلاق، ولا يشترط فيها أي قوة او جنس الا التحكم في تقنيات الحاسوب وتكنولوجيا الاعلام والاتصال الحديثة[2].

4- صعوبة إكتشاف الجريمة الإلكترونية:

ينظر الى المعلوماتية دائما بأنها أداة محايدة ومصدر انتهاكها هو انسان ذاته، والذي غالبا ما يهيئ الفرصة لاستغلالها سواءا عن حسن نية أو سوء نية، وعليه فإن جوهر المشكلة بالانسان وشخصته ودوافعه، أما فيما يتعلق بالمجني عليهم فغالبا ما يفضلون عدم إفشاء الفعل، فلا يوجد من يرد الاعتراف بإنتهاك نظامه المعلوماتي، هذه الجرائم لا تحتاج إلى العنف ولا الى سفك الدماء أو ترك آثار اقتحام سرقة الاموال بينما هي ارقام وبيانات تمحى أو تتغيرمن السجلات المخزنة داخل ذاكرة الحاسب الالكتروني. و كون هذه الجرئم لا تترك آثار مادية خارجية فإنه يكون من الصعب إكتشافها.

و مما يزيد الامر صعوبة هو ارتكابها في الخفاء، حيث يتم نقل البيانات و المعلومات في شكل نبضات الكترونية، كما ان هذه الجرائم في الغالب الاعم تكون منظمة وترتب وتنفذ وتمس اقليم اكثر من دولة واحدة لاستخدام شبكة الاتصالات العالمية " الانترنت"[3]

---

[1] عبد القادر عميمر، مرجع سابق، ص 28.

[2] نفس المرجع آنف الذكر، ص 29.

[3] غنية باطلي، الجريمة الإلكترونية دراسة مقارنة، الجزائر: الدار الجزائرية للنشر والتوزيع، 2016، ص ص 33- 34.

5- صعوبة اثبات الجريمة المعلوماتية:

إقامة الدليل وإسناده إلى المجرم هو الأصل في الجريمة ومع التطورات العلمية الحاصلة يمكن نقل بسرعة البيانات المأخوذة من شبكات الالكترونية ومن التجهيزات الحاسوبية من مكان إلى آخر أو العبث بها وإلغاءه نظرا لطبيعة هذه البيانات التي تسمى بالدليل الرقمي[1].

فالجريمة الالكترونية لا تترك أثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية.

و يرجع السبب الرئيسي في عدم القدرة على إثباتها الى صعوبة إكتشاف أركانها، فإضافة الى الشرط المبدئي في كل جريمة ونقصد به الركن الشرعي، لا بد من إثبات ركن مادي ملموس يعبر عن إرادة الفاعل بشكل جلي، وركن معنوي يعبر عن إرادة المجرم الإلكتروني[2].

ثانيا: خصائص الجريمة المعلوماتية المستمدة من اساليب ارتكابها

ترتكب الجريمة المعلوماتية بأساليب غغير تقليدية لا تتشابه في طبيعتها، ولا في آثارها مع الوسائل التي ترتكب بها الجرائم الأخرى، وهي وسائل ذات طبيعة خاصة تنسجم مع الطبيعة الامادية للجريمة المعلوماتية، فالتعامل مع المعلومات التي عبارة عن نبضات الكترونية غير مرئية يقتضي استخدام وسائل و اساليب تتلاءم مع هذه الطبيعة.

أ - الوسائل المساعدة في ارتكاب الجرائم المعلوماتية

يقوم المجرم المعلوماتي باستغلال بعض الوسائل التكنولوجية من اجل ارتكاب جريمته سواءا ارتكب بطريقة فردية او عن طريق مجموعة من الافراد، وتستخدم هذه الوسائل بغرض الاتصال والتحضير وتنفيذ الجريمة، وسنتطرق لبعض هذه الوسائل فيما يلي:

1- البريد الالكتروني e.mail: يعد البريد الالكتروني من اهم الوسائل المستخدمة في التواصل بين مرتكبي الجرائم المعلوماتية عبر الوسائل الالكترونية، وهو عبارة عن خط مفتوح يستطيع الأشخاص من خلاله استقبال وارسال الرسائل في صورة مكتوبة أو مسموعة أو مرئية، وتعد هذه الخدمة الاكثر استخداما م طرف مستعملي الانترنت، لكونها تقصر الوقت وتختصر المسافات في عمليات التواصل

[1] صورية بورباية، التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدارسات البحثية، العدد 01 ،جامعة طاهري محمد، بشار ،2019، ص93.

[2] غنية باطلي، **مرجع سابق**، ص 44.

التجاري و الاداري وغيرها من المجالات، الاانه قد استعمل في امور سلبية و كوسيلة لإرتكاب الجرائم، فهو سهل ارتكاب انواع كثيرة من ارائم كجرائم الابتزاز واتهديد، و الاحتيال المعلوماتي[1].

2- **المواقع على الانترنت المواقع الالكترونية او صفحات الويب:** هي عبارة عن معلومات مخزنة بشكل صفحات، وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل **(HTML)** ، ولقد تم ابتكار هذا النظام في سويسرا عام 1989 من طرف المختص في المعلوماتية الانجليزي **(Tim Beners)** الذي صمم برنامج اطلق عليه اسم « World Wide Web » تتم اعتماده لاول مرة في العالم عام 1993 من خلال برنامج التصفيح Mosaic ثم من بعدها من خلال شركة Netscape الامريكية التي عملت على تعميمه ونشره من عام 1994.[2]

ويقوم المجرمون المعلوماتيون بانشاء وتصميم مواقع على شبكة الانترنت بغرض الاعداد لجرائمهم وتنفيذها، كما تقوم بعض المواقع على الاترنت بالمساهمة في تسهيل ارتكاب الجرائم المعلوماتية عن طريق تديم معلومات تتعلق بكيفية اخترا وتدمير المواقع وطرق اختراق البريد الالكتروني وكيفية الدخول الى المواقع المحجوبة، وطرق نشر الفيروسات وغيرها من النشطات المحضورة قانونيا[3].

3- منتديات المناقشة: وهي إحدى البرمجيات الإجتماعية التي تسمح للمستخدمين بإرسال موضوعات لإعضاء لقرأتها والتعليق عليها، ويتضمن المنتدى الواحد أحيانا أبوابا مختلفة يتخصص كل منها في موضوع معين، ومن ثم فˈن نطاق المواضيع المطروحة للنقاش واسع والأعضاء غير مضطرين للإتصال بالانترنت في الوقت نفسه[4].

ب- أساليب ارتكاب الجريمة المعلوماتية.

ترتكب الجريمة المعلوماتية باساليب مختلفة تتطور مع تطور التكنولوجيا و وسائل التحكم فيها، منها ماهو معروف ومنها لا يمكن التنبؤ به، ونظر لتعدد هذه الاساليب فقد قصر على ذكر بعض الاساليب الشائعة و التي نتناولها فيما يلي:

1- التحكم في المنظومة المعلوماتية عن بعد: وتسمح هذه التقنية بالتحكم الالي في المنظومة المعلوماتية للغير عن بعد مما يشكل مخاطر وتهديدات كبيرة على مرافق العامة أو الخاصة كالمطارات

---

[1] جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، مصر (القاهرة): دار النهضة العربية، 2001، ص41.

[2] عميمر عبد القادر، مرجع سابق، ص ص 30-31.

[3] نفس المرجع آنف الذكر، ص 31.

[4] محمد الامين الشوابكة، جرائم الحاسوب والانترنت (الجرائم المعلوماتية، ط 4، الاردن: عمان: دار الثقافة للنشر والتوزيع، 2001،ص45.

ومحطات القطارات والمستشفيات أو على المؤسسات والشركات الحيوية في القطاع الخاص كالبنوك والاتصالات فضلا عن الافراد العاديين، وما تلحقه بهذه القطاعات من اضرار كبيرة تتمثل في تعطيل اعمال ومسؤوليات المؤسسات الخاصة والعامة وكذا الافراد وتأجيل مشاريعهم[1].

2- التصيد Le phishing: أو الصيد الالكتروني ويقصد بهعملية استدراج الضحايا عن طريق تصميم صفحات وهمية تشبه الصفحات الاصلية تابعة لمؤسسات عمومية أو خاصة، ثم يرسل المحتالون المعلوماتيون رسائل الى الضحية تبدو وكأنها صادرة من الصفحة الاصلية يطلبون منه اتباع قواعد تقوده الى الصفحة المقلدة، ثم يطلبون ادخال المعلومات الشخصية، ويقومون باستغلال هذه المعلومات إما بالابتزاز أو سحب مبالغ مالية إذا كانت تتعلق بالحساب البنكي ن كما يمكن ان تباع هذه المعلومات للغير من اجل استغلالها وهذا ما يجعل هذه الصور من الجرائم من بين اخطر انواع الجريمة المعلوماتية[2].

3- الاختراق: وهو القدرة على الوصول لمنظومة معلوماتية معينة بطريقة غير مشروعة للاطلاع على المعطيات الموجودة فيها، والقيام بالتلاعب بها وتغيرها عن طريق التزوير كتغير عقد الملكيات مثلا باضافة او محو معلومات، كما يمكن ان يكون الهدف هو تغيير بيانات ضريبية ويتم ذلك عن طريق البحث على ثغرات في النظام المستهدف وغالبا ما تكون تلك الثغرات في نظام الحماية الخاص بالمنظومة المستهدفة[3] .

4- الحرمان من الخدمة: وتسمى ايضا هجوم حجب الخدمة أو هجمات DDOS وهي عبارة عن هجمات الهدف منها اغراق مواقع بسيل من البيانات غير اللازمة يتم ارسالها عن طريق اجهزة مصابة ببرامج خبيثة تعمل بعد اطلاقها مما يتسبب في بطئ الخدمات ويشكل ضغط على هذا الموقع مما يصعب وصول المستخدمين له نظرا لهذا الازدحام، وهو ما يؤثر سلبا على نشاط هذا الموقعن وتتم هذه الهجمات بدون كسر ملفات كلمة السر او سرقة البيانات السرية وحسب الخبراء فإنه لايوجد حل لهذا النوع من العمليات في الوقت الحالي[4].

---

[1] عميمر عبد القادر، مرجع السابق، ص 33.

[2] خالد بن سلمان الغثبر، سليمان عبد العزيز الهيشة، الاصطياد الالكتروني الاساليب و الاجراءات المضادة، المملكة العربية السعودية الرياض، مركز التميز لامن المعلومات، 2009، ص 47.

[3] مقال متاح على موقع صفحة بوابة فيتو http ://www.vetogate.com/2424631 نشر بتاريخ 2016/10/25، وتم الاطلاع عليه بتاريخ 2025/04/27،على الساعة 22:15 .

[4] عميمر عبد بالقادر، مرجع سابق، ص 37.

5- نشر الفيروسات: يعد الفيروس برنامج كباقي البرامج الموجودة على جهاز الحاسوب غير انه مصمم بغرض التأثير على البرامج الموجودة على هذا الجهاز والتسبب في العديد من المشاكل كمسح الذاكر، أو مسح بعض الملفات الهامة في نظام التشغيل، أو القيام بإصدار بعض الاوامر لبرامج دون تدخل مباشر من المستخدم، ويبدأ في التشغيل بمجرد فتح الرسالة الموجودة به[1]. ويوجد منها أنواع كثيرة مثل فيروس الدودة وحصان طروادة ، والقنبلة الموقوتة (المنطقية) وهذه تتسبب في إتلاف المكونات المنطقية للحاسب الآلي أو تعطيل شبكات الكمبيوتر عن تأدية مهامها. وتتنوع الفيروسات التي تصيب المعلومات كالآتي [2]:

5/أ- حصان طروادة (Trojan Horse): وهو عبارة عن برمجية إختراق من حيث التقنية ، فهو يختبيء داخل البرامج الموجودة بالذاكرة ثم ينشط في الوقت المحدد له وينفذ الأمر المعطى له إما بتعديل في البرنامج أو الإتلاف نهائيا أو يقوم بمحو البيانات أو تشويهها ، وقد ظهرت أولى جرائم حصان طروادة في انجلترا عام 1989 عندما قام شخص يدعى الدكتور " بوب " من أوهايو بالولايات المتحدة الأمريكية حيث كان يستخدم أسلوب إرسال حصان طروادة في ديسكات حول العالم لإرتكاب جرائم إبتزاز ، ولقد تضرر من عمله حوالي 20 ألفا في مدينة لندن بانجلترا .

5/ب- فيروس الدودة (computer worm): وهو عبارة عن برمجية تقوم بالإنتقال من حاسوب إلى آخر دون حاجة إلى تدخل إنساني لتنشيطها ، وبخاصة التنشيط الذاتي ، وبهذا تختلف الدودة عن حصان طروادة إلا أنها لا تلتصق بنظام التشغيل في الحاسوب الذي تصيبه وتتسبب حركة الدودة في تعطيل الحاسوب بتجميد لوحة المفاتيح والشاشة وتعبئه الذاكرة و تبطئة الحاسوب .

وقد ظهرت الدودة على يد " موريس " طالب الدكتوراه في علوم الحاسب بجامعة كورنل وتم برمجة دودة موريس على أن تطبع ذاتها عند تلقيها للإجابة السابقة المؤكدة . وقد انزلقت الدودة إلى نظام البريد الإلكتروني عبر ثغرة فيه تركت بقصد تسهيل عملية الدخول إليه لإصلاحه حال وجود خلل ما ولقد حطمت دودة موريس كلمات المرور وانتشرت في جميع الحواسيب .

5/ج- القنبلة المنطقية (Logic Bombs) : وهو عبارة عن فيروس يظل ساكتا حتى حدوث واقعة معينة أو كلمة محددة قد يكتبها المستخدم أو تاريخ معين يبدأ في عمله من خلال موقعه على الذاكرة ثم

[1] منير محمد الجهيني، منير ممدوح الجهيني، جرائم الانترنت والحاسب الآلي و وسائل مكافحته، مصر(الاسكندرية): دار الفكر ص59.

[2] نفس المرجع آنف الذكر، ص 39

ينشط ويقوم بتدمير البرامج أو تدمير قوائم العمال أو الزبائن . وتؤدي هذه القنبلة إلى خلل في البرمجة ونظامها.

5/د- برامج الانزال(Droppers): صممت لمراوغة برامج مكافحة الفيروسات وتعتمد على التشفير غالبا لمنع اكتشافه، و وظيفة هذه البرامج عادة هي نقل وتركيب الفيروسات فهي تنتظر لحظة حدوث أمر معين على الحاسوب لكي تطلق وتلوث بالفيروس المحمول في طياتهاا[1]

ثالثا: خصائص الجريمة المعلوماتية المستمدة من سمات مرتكبيها

لا تعد وسائل ارتكاب الجريمة المعلوماتية هي السمة الوحيدة التي تميزها عن غيرها من الجرائم فحسب، بل تستمد هذه الجرية تميزها وخصوصيتها أيضا من سمات مرتكبيها الذي يطلق عليه وصف " المجرم المعلوماتي" و الذي يتميز عن بقية المجرمين بعدة خصائص و اوصاف اختلف الباحثون في تحديديها رغم اتفاقهم على ان المجرم المعلوماتي ينتمي الى طائفة خاصة من المجريمين تقترب في سماتها الى صنف المجرمين الذين تطلق عليهم تسمية " ذوي الياقات البيضاء".

أما في الاصطلاح الالكتروني فاطلق عليه خبراء من المعلوماتية الالكترونية اسم "**الهاكر**" **Les Hakers** هو الشخص الذي يخترق الحاسب الالي ويجد متعة في فحص واستكشاف عن كثب نظام قابل للبرمجة ويسعى الى توسيع معارفه في هذا المجال الى اقصى حد، وهو يختلف عن مصطلح "**كركرز**" **Crackers** الذي يطلق على الفئة التي لديها القدرة على الاختراق وهناك من يعرفهم بمصطلح المحطمون الذي يكون هدفهم الاساسي هو انشاء ادوات برمجية تسمح بالهجوم على انظمة معلوماتية او تحطيم نظم حماية نسخ البرمجيات المدفوعة الثمن[2].

الأستاذ (parker)[3] واحد من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة و المجرم المعلوماتي بصفة خاصة ، ويرى (parker) ان المجرم المعلوماتي وان كان يتميز ببعض السمات الخاصة إلا انه في النهاية لا يخرج عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه، حتى ولو

---

[1] دلال صادق، حميد ناصر الفتال، أمن المعلومات، الأردن: دار اليازوري العلمية للنشر و التوزيع، 2008، ص 74.

[2] بشرى غريبي، خصوصية المجرم المعلوماتي ودوافعه، مجلة نومبرس الاكاديمية، المجلد الثاني، العدد02، 2021، ص103.

* يرى الأستاذ Parker أن المجرم المعلوماتي، وإن كان يتميز ببعض السمات الخاصة به إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يستوجب توقيع العقاب عليه. ويرمز الأستاذ باركر لهذه الصفات بكلمة SKRAM وهي تعني (المهارة SKILLS) (المعرفة Knowledg) (الوسيلةResources السلطة(Autority وأخيرا الباعث (Motives)،

كان غير عادي كونه يرتكب جريمة متخصصة خاصة إذا تمثلت في سرقة المعلومات المشفرة ما يلزم خبرة تقنية عالية في هذا المجال[1].

أ – أنواع المجرم المعلوماتي:

بما أن المجرم ألمعلوماتي يرتكب جرائمه وهو يمارس وظيفته في مجال الأجهزة الآلية فلابد أن يكون إنسانا اجتماعيا وسط ا تمع يقوم بواجباته ويمارس حقوقه دون وجود أي عائق من جهة، و إنسانا محترفا يتمتع بذكاء كبير من جهة أخرى. و عليه يمكننا تصنيف جناة الجريمة المعلوماتية إلى عدة أصناف يوضحها لنا الجدول الموالي:

الجدول رقم 01: أنواع المجرم المعلوماتي

الخصائص	نوع الجاني
عدم وجود نية أو قصد لإتلاف المعلومات أو تخريب أنظمة الحاسب وشبكات الاتصال. يتمثل هدفهم في الاستكشاف والبحث عن الجديد في هذا العالم الخيالي	القراصنة **(Hackers)**
أشخاص هدفهم إلحاق خسائر با ني عليهم دون أن يكون الحصول على مكاسب مالية من ضمن هذه لأهداف	القراصنة الخبيثون **(Crackers)**
الأشخاص الذين يرتكبون جرائم: المعلوماتية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر با ني عليهم	المخادعون **(Pranksters)**
يمتازون بنفس السمات التي يتميز بها المجرم التقليدي، هدفهم تحقيق الربح بطريقة غير شرعية.	االمجرمون الموظفون **Career Criminals**
والتي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية، ألا وهي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية في أغلب الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح	المقصرون جنائيا **The Criminally) Negligence**

من إعداد الباحثتان [2]

[1] أمين طعباش ، الحماية الجنائية للمعلومات الإلكترونية، مصر (الاسكندرية): مكتبة الوفاء القانونية، 2015، ص 22

[2] من إعداد الباحثتان بالإعتماد: ياسمينة بونعارة: **الجريمة الإلكترونية** على الموقع :

-http://www.univ-emir.dz/download/madjalaoussoul/39bounara-yasmina.pdf

ب- خصائص العامة للمجرم المعلوماتي.

باعتبارها قاعدة عامة فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب العام، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات ،أو على الأقل شخص لديه حد أدنى من المعرفة و القدرة على استعمال جهاز الحاسوب و التعامل مع شبكة الأنترنت.

1- **الذكاء:** يعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتية، لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل و التغيير في البرامج لذلك عادة ما يذكر أن الإجرام المعلوماتي هو إجرام الأذكياء وذلك بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف.

وتتجلى أهمية صفة الذكاء بالنسبة لمرتكب الجريمة المعلوماتية في عدم استخدامه للعنف في ارتكابه للجريمة، فالسلوك الإجرامي ينشأ من تقنيات التدمير الناعمة**Sabotage soft** فيكفي أن يقوم المجرم المعلوماتي بالتلاعب ببيانات وبرامج الحاسب الآلي لكي يمحو أو يدمر هذه البيانات أو يعطل استخدام هذه البرامج[1].

2- **المهارة:** وتشير الى القدرات التقنية والمعرفية التي يتمتع به الاشخاص الذين ينفذون جرائم المعلوماتية الكترونينا او الانشطة القانونية عبر الانترنت. تعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الآخرين، فهي التي تحدد الاسلوب الذي يرتكب به المجرم المعلوماتي الجريمة. هذه المهارات تمكنهم من الاستغلال الثغرات الامنية في الانظمة و الشبكات والبرامج لتحقيق أهدافهم، سواء كانت سرقة البيانات، أو ابتزاز، أو تعطيل خدمات، أو غير ذلك[2].

3- **التنظيم و التخطيط:** تميز الجريمة المعلوماتية عادة بوجود أكثر من فاعل للنشاط الإجرامي الواحد، إذ ترتكب أغلب الجرائم المعلوماتية من عدة أشخاص يحدد لكل شخص منهم دور معين، ويتم العمل بينهم وفقا لتخطيط وتنظيمٍ سابق على ارتكاب الجريمة.

يعد التخطيط والتنظيم عنصرين أساسيين في السلوك الإجرامي للمجرم المعلوماتي، حيث لا يتم ارتكاب الجريمة المعلوماتية بصورة ارتجالية أو عفوية، وإنما وفق مراحل محكمة تبدأ برصد الهدف، وتحليل بنيته التقنية، واستغلال الثغرات القانونية أو الأمنية المتاحة. ويقوم الفاعل المعلوماتي، سواء كان يعمل بصورة فردية أو ضمن مجموعة منظمة، باتخاذ خطوات منهجية تشمل جمع البيانات، واستخدام أدوات متقدمة للإخفاء والتشفير، واللجوء إلى هويات رقمية مزيفة أو شبكات افتراضية لحجب آثاره.

[1] نعيم سعيداني، مرجع سابق، ص 51

[2] خالد محمود ابراهيم، الجرائم المعلوماتية، ص 135.

ويتجلى التنظيم القانوني لهذه الأفعال في التشريعات الحديثة التي بدأت تعترف بأن المجرم المعلوماتي غالبًا ما يتسم بدرجة عالية من المعرفة التقنية والتخطيط المسبق، ما يستدعي التعامل معه على أنه "فاعل خطير" وفقًا لمعايير القانون الجنائي، خاصة في ظل صعوبة التتبع وتعدد الاختصاصات القضائية. وقد أشار (Casey) إلى أن طبيعة الجريمة المعلوماتية تتطلب من المشرّع نهج مقاربة خاصة تراعي الطابع العابر للحدود لهذا النوع من الإجرام، وضرورة تطوير أدوات الإثبات الرقمية لمواجهة التنظيم المعقّد لهذه الأفعال[1].

4- **التبريرية وتحيد الضمير لمرتكبي الجرائم المعلوماتية:** يُجسّد المجرم المعلوماتي المعاصر نموذجاً فريداً يجمع بين الذكاء الحادّ والانحراف الأخلاقي، حيث تُحوَّل المهارات الرقمية المتقدمة إلى أدوات للإيذاء المنظم. فما يبدو للعالم الخارجي كجريمة عشوائية، هو في الواقع عملية مُحكمة تُخطط بدقة تشبه العمليات الاستخباراتية، تبدأ بدراسة الضحية وتحليل نقاط ضعفها، مروراً بتطوير أدوات الاختراق المخصصة، وصولاً إلى التنفيذ المثالي الذي يُمحى أثره بعناية.

هذا العقل الاستراتيجي الذي يجيد تحويل الثغرات التقنية إلى فرص إجرامية، يخفي وراءه فلسفة مقلقة تبرر الانتهاك الرقمي بمنطق مزيف، إما بدعوى التحدي التقني، أو بذريعة مقاومة الأنظمة، أو بادعاء أن الضحية "المهملة" تستحق مصيرها. وهكذا يتحول الفعل الإجرامي في الوعي المشوّه إلى مجرد "لعبة ذكاء"، بينما يترك وراءه أضراراً مادية ومعنوية لا تُحصى، تفضح زيف هذه التبريرات وتؤكد أن الإبداع التقني دون ضوابط أخلاقية هو وجه آخر للهمجية العصرية.

المطلب الثالث: أركان الجريمة المعلوماتية.

تأخذ الجرائم المرتكبة عبر الإنترنت شكلاً غير الذي عليه الحال بالنسبة للجرائم التقليدية والاختلاف يكمن في طبيعة الانترنت باعتباره محلا للجريمة، كما أن الوصول إلى المجرم الإلكتروني يشكل عبئاً فنياً وتقنياً على القائمين بأعمال التتبع والتحليل الملابسات الوقائع الإجرامية فيفرض هنا على المحقق عدداً من المبادئ ينبغي تطبيقها عند التحقيق[2].

وعليه تقوم الجريمة المعلوماتية مثلها مثل باقي الجرائم التقليدية على ثلاثة أركان أساسية هي الركن الشرعي، الركن المادي، الركن المعنوي، بالإضافة الى ركن خاص و هو الركن المفترض في الجريمة المعلوماتية نتطرق لها فيما يلي:

[1] Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed., Academic Press, 2011.

[2] خالد ممدوح ابراهيم، **فن التحقيق الجنائي في الجرائم الالكترونية**، مصر (الاسكندرية): دار الفكر الجامعي، 2018، ص 52.

الفرع الاول: الركن الشرعي للجريمة المعلوماتية

يقصد بالركن الشرعي لأية جريمة وجود نص قانوني يجرم الفعل و يوضح العقاب المترتب عليه في حالة وقوع هذا الفعل، كما أنه يقصد به الصفة غير المشروعة التي تتكون نتيجة تطبيق نص التجريم المنصوص عليه في القانون على السلوك أو الفعل الذي اقترفه الفاعل، ويمكن لهذه الصفة أن تزول عن الفعل إذا توفر سبب من أسباب الاباحة الذي ينفي عنه هذه الصفة[1].

و في إطار الجريمة المعلوماتية فقد اجمع اغلب فقهاء القانون الجنائي على ضرورة سن نصوص قانونية يجرم من خلالها المشرع الافعال و الانتهاكات التي تقع على الانظمة المعلوماتية او من خلالها، و في نفس السياق المجلس الأوربي سنة 1989 توصية بهدف تشجيع الدول الاعضاء على تبني نصوص عقابية خاصة بالجريمة المعلوماتية، واختلفت الدول في الطريقة التي نظمت بها هذا الامر فمنها من ادرج هذه النصوص ضمن قانون العقوبات كما هو الحال بالنسبة للمشرع الجزائري ومنها من وضع قانونا خاصا بالجرائم المعلوماتية.[2]

في ظل تطور الجريمة المعلوماتية واتخاذها لأشكال جديدة، أدرك المشرع الجزائري حتمية التدخل التشريعي لمواكبة المستجدات، وهو ما تم من خلال القانون رقم 09-04 المؤرخ في 5 أوت 2009، الذي أدرج تعديلات هامة على قانون العقوبات، بإضافة مجموعة من المواد من 394 مكرر إلى 394 مكرر 7. وقد شكلت هذه المواد الإطار التشريعي الأساس لتجريم الأفعال المعلوماتية، بما فيها الدخول غير المشروع إلى نظم المعالجة الآلية، والتقاط البيانات أو تعديلها دون وجه حق، وتخريب أو تعطيل الأنظمة المعلوماتية، وغيرها من الأفعال ذات الطابع الإلكتروني[3].

كما أن النصوص المستحدثة تتسم بدقة المصطلحات واستيعابها للجانب التقني، إذ وردت فيها مفاهيم مثل: "نظام المعالجة الآلية للمعطيات"، و"المعطيات الإلكترونية"، و"الولوج غير المشروع"، وهي مصطلحات ذات طابع فني تبرز التخصصية التي تتطلبها مكافحة هذا النوع من الجرائم. وبهذا يكون الركن الشرعي للجريمة المعلوماتية في القانون الجزائري متحققًا بمجرد وجود نص قانوني يجرم الفعل ويقر بعقوبة مناسبة له، بما ينسجم مع المبادئ العامة للقانون الجنائي، ويعكس وعي المشرّع بخصوصيات الجريمة المعلوماتية.

يتضح إذًا أن المشرّع الجزائري قد أرسى دعائم الركن الشرعي للجريمة المعلوماتية ضمن إطار قانوني محكم ومحدد، يراعي طبيعة هذه الجريمة المتغيرة والمرتبطة بالتطور التقني، ويضع بذلك الأساس

---

[1] لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، الاردن (عمان): دار حامد للنشر والتوزيع، 2016، ص 156.

[2] عميمر عبد القادر ، مرجع سابق، ص 88.

[3] ايمان بغدادي ، أثر تعديل قانون العقوبات الج ازئري في التصدي للجريمة الإلكترونية ،مجلة افاق للبحوث و الدراسات محكمة دولية ، المركز الجامعي ايليزي، العدد04 ، 2019، ص 188

القانوني الذي يسمح للسلطات القضائية بملاحقة مرتكبي الجرائم المعلوماتية في إطار قانوني صارم ومحترم للضمانات الدستورية.

الفرع الثاني: الركن المادي

يعبر الركن المادي عن ماديات الجريمة الالكترونية والتي تبرز بها الى العالم الخارجي كأثر للسلوك الاجرامي والذي يقيد به القانون فيجعله عنصراً منت العناصر المؤلفة لجريمة معينة فلا تتوافر الجريمة الا بتوافره مع بقية العناصر الأخرى[1].

يقوم الركن المادي في الجريمة، وفقًا لما استقر عليه الفقه والقضاء، على سلوك إرادي يصدر عن إنسان مميز وعاقل، يتمثل في فعل إيجابي أو امتناع عمدي يؤدي إلى نتيجة إجرامية تمس حقًا يحميه القانون. وفي الجرائم التقليدية، لا تُعاقب الأعمال التحضيرية لعدم تحقق الشروع أو النتيجة، إلا أن الأمر يختلف في الجرائم المعلوماتية، حيث توسّع المشرّع الجزائري في نطاق التجريم، فاعتبر بعض الأفعال التحضيرية جرائم قائمة بذاتها. ويتجلى ذلك في نص المادة 16 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، التي تُجرّم حيازة أو صنع أو عرض أو بيع أو شراء أدوات معلوماتية، بما في ذلك البرامج أو المعطيات المصممة لتسهيل ارتكاب الجرائم المعلوماتية، حتى قبل تحقق النتيجة أو الشروع فيها.

كما تنص المادة 19 من نفس القانونعلى تجريم حيازة أو توزيع محتوى ذو طابع إباحي يتعلق بالأطفال، ولو لم يصاحب ذلك أي نشاط تنفيذي آخر. ويقتضي قيام الجريمة الإلكترونية توافر فعل مادي يتم في بيئة رقمية، عبر شبكة إلكترونية، مع توافر نية جنائية تكشف عن شروع جدي في ارتكاب الجريمة قد يفضي إلى نتيجة يعاقب عليها القانون.

لا يرتب القانون الجزائي أي أثر على مجرد الأفكار أو الخواطر المجردة، إذ لا يُعاقَب عليها ما لم تتحول إلى **سلوك مادي ملموس**، سواء أكان فعلاً إيجابيًا أو امتناعًا سلبيًا عمديًا يُظهر اتجاه الإرادة نحو ارتكاب الجريمة. ويُعد هذا السلوك هو العنصر المحدد لقيام الركن المادي، ومن ثمّ لقيام الجريمة. وفي الجرائم المعلوماتية، يشترط أن يتحقق هذا السلوك داخل بيئة رقمية، تشكّل مسرح الجريمة وأداتها في آنٍ واحد، ويستوجب ذلك اتصالًا فعليًا بشبكة الإنترنت[2].

غير أن مجرد وجود السلوك المادي لا يكفي، إذ لا بد أن يكون مشفوعًا **بمباشرة نشاط تقني غير مشروع**. ومن أبرز صور هذا النشاط ما نصت عليه المادة 6 من القانون 09-04، والتي تعتبر "الدخول الاحتيالي أو غير المشروع إلى منظومة معلوماتية أو نظام معالجة آلية للمعطيات" جريمة قائمة بذاتها، حتى في غياب أي ضرر فعلي أو تعديل للبيانات. فمجرد النفاذ غير المرخص إلى قاعدة بيانات، أو

---

[1] محمد عمر مصطفى، النتيجة وعناصر الجريمة، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، العدد 532، 2005، ص345 .

[2] فتيحة بن زروقي ، *الجريمة المعلوماتية في القانون الجزائري والمقارن*، الجزائر: دار هومة، 2018، ص. 65-67

إلى نظام معلوماتي عبر شبكة الإنترنت، يشكّل سلوكًا إجراميًا معاقبًا عليه قانونًا. وتشمل هذه الأفعال كذلك الاطلاع غير المشروع على المراسلات الإلكترونية، أو على البريد الإلكتروني للغير، أو الإدلاء بمعطيات كاذبة بغرض التحايل أو التمويه، وهي جميعها أفعال يُجرّمها المشرّع بالنظر إلى ما تشكّله من مساس بسرية الاتصالات والمعطيات ذات الطابع الشخصي[1].

الفرع الثالث: لركن المعنوي في الجريمة المعلوماتية

يُعد الركن المعنوي الركن الثالث من أركان الجريمة، ويقصد به الحالة الذهنية والنفسية للجاني أثناء ارتكابه الفعل الإجرامي، ويتجلى في توافر القصد الجنائي، أي إرادة الجاني الواعية والمتعمدة لارتكاب فعل غير مشروع، مع إدراكه لطبيعته غير القانونية. ويتخذ هذا الركن في الجرائم الإلكترونية طابعًا خاصًا، نظرًا لخصوصية الوسط الرقمي، وتنوع أنماط الأفعال الإجرامية، ما يجعل القصد الجنائي يختلف من جريمة إلى أخرى بحسب طبيعتها وظروف ارتكابها.

1- القصد الجنائي العام

يتطلب تحقق القصد الجنائي العام أن يكون الفاعل على علم بأن السلوك الذي يقوم به معاقب عليه قانونًا، وأنه يمسّ حقوقًا يحميها القانون، مع اتجاه إرادته إلى تحقيق هذه النتيجة. فمثلاً، في جريمة الدخول غير المشروع إلى نظام معلوماتي، يجب أن يكون الجاني على دراية بأن النظام محمي، وأن الدخول إليه تم دون إذن أو تجاوزًا للصلاحيات الممنوحة له، مع وجود غش أو تحايل تقني لتحقيق هذا الولوج[2]. وفي هذه الحالة، لا يُعتد بحسن النية أو الجهل بالقانون، طالما ثبت أن السلوك كان عمديًا ومدروسًا، ولو لم يصاحبه ضرر فعلي.

ويتحقق القصد الجنائي أيضًا في حالة تجاوز الصلاحيات، عندما يُسمح لشخص بالدخول إلى جزء معين من النظام المعلوماتي، فيتعدى حدود الترخيص ويتسلل إلى أجزاء أخرى محمية، وهو ما يُشكّل جريمة قائمة بذاتها.

2- القصد الخاص والضرر غير المتوقع

في بعض الحالات، يتطلب القانون توافر قصد خاص، كالرغبة في تحقيق ضرر أو منفعة غير مشروعة، كما هو الحال في جرائم المساس بسرية المعطيات أو تعديل محتواها. وقد يُسأل الجاني جزائيًا حتى لو تجاوز الضرر الناتج ما كان يتوقعه، أو إذا استمر في نشاطه رغم عدم قصده الأصلي لإحداث ضرر، كما هو الحال في حالة البقاء غير المشروع داخل النظام المعلوماتي، إذ يعتبر الاستمرار في التواجد داخل النظام بعد علم الفاعل بعدم قانونية وجوده، صورة من صور الركن المعنوي المفترض،

[1] نفس المرجع آنف الذكر، ص ص67 -70

[2] المادة 6 من القانون 09-04

الذي يُستدل عليه من الأفعال التي قام بها أثناء ذلك التواجد، مثل التصفح غير المرخص أو محاولة تعديل محتويات النظام[1].

ظرًا لتعقيد الجرائم الإلكترونية وصعوبة ملاحظة الحالة الذهنية للجاني، تتطلب هذه الجرائم إجراءات فنية وتقنية دقيقة لجمع الأدلة التي تثبت القصد الجنائي، وهو ما يؤكده الباحثة نبيلة هبة هروال التي تشير إلى أن "الركن المعنوي في الجرائم الإلكترونية لا يمكن إثباته إلا عبر أدلة تقنية وإجرائية متخصصة، لما تتميز به هذه الجرائم من افتراضية وأبعاد تقنية معقدة"[2]

ويُبرز الباحث عمر بن خليف هذا التعقيد بالقول إن "الركن المعنوي في الجرائم الإلكترونية يتسم بصعوبة إثباته، ويتطلب من القاضي دراسة إرادة الجاني من خلال عناصر تقنية يصعب ملاحظتها مباشرة، مما يستوجب تقديم أدلة تقنية وإثباتات دقيقة لإثبات القصد الجنائي سواء كان عامًا أو خاصًا" ،كما يؤكد أن "استمرار الجاني في النشاط الإجرامي داخل النظام المعلوماتي يعد من صور الركن المعنوي المعتبر، حيث يعكس الإصرار والوعي بغير مشروعية الفعل، وهو ما يعزز أركان الجريمة ويدعم الثبوت القضائي"[3] .

[1] سناء شيخ، محمد زكريا شيخ، مكافحة الجرائم الإلكترونية في القانون الجزائري، مجلة وميض الفكر، جوان 2020، ص 63.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، مصر (الاسكندرية): دار الفكر الجامعي، 2022، ص. 63.

[3] عمر بن خليف، الجرائم الإلكترونية في التشريع الجزائري، منشورات المجلة الجزائرية للعلوم القانونية، العدد 2، 2021، ص ص 147-145.

المبحث الثاني: االدليل الرقمي في الجرائم المعلوماتية

برزت الجرائم المعلوماتية كأحد أبرز التحديات التي تواجه العدالة الجنائية في العصر الرقمي، مما فرض تطوير أدوات إثبات جديدة تتماشى مع طبيعة هذه الجرائم .من أبرز هذه الأدوات الدليل الرقمي، الذي يُعد نتاجًا مباشراً لثورة المعلومات والاتصالان ويتميّز عن غيره من الأدلة الجنائية بخصائص تقنية وموضوعية تفرض ضوابط دقيقة في التعامل معه..

المطلب الأول: تعريف الدليل الرقميDigital Evidence

الدليل لغة هو ما يستدل به، و الدليل هو الدال أيضا، و الدليل اصطلاحا هو ما يلزم من العلم به علم شئ آخر، وغايته أن يتوصل العقل الى التصديق اليقيني فيما كان يشك في صحته، أي التوصل به الى معرفة الحقيقة.

أما الدليل قانونا فهو إقامة البينة والبرهان والحجة على شخص أمام القضاء ووفقا لأحكام القانون على واقعة قانونية متنازع عليها بين الخصوم.

وهناك العديد من التعريفات للأدلة الجنائية الرقمية اختلف الفقهاء والجهات الدولية في تحديد تعريف موحد، .وقد عرّفته المنظمة الدولية لخبراء الأدلة الرقمية **(IOCE)** سنة 2001 بأنه: " المعلومات ذات القيمة الإثباتية المحتملة، المخزنة أو المنقولة في صورة رقمية[1]"

في حين عرفه بعض الباحثين بأنه" كل بيانات يمكن استخراجها من نظام معلوماتي وتقديمها كوسيلة إثبات أمام الجهات القضائية [2]" . ويرى آخرون أنه: "الدليل الذي ينشأ في العالم الافتراضي، ويقود إلى إثبات ارتكاب جريمة أو نفيها[3].

و تلخيصا لماسبق ذكره يمكن القول بان الدليل الرقمي هو معلومات يقبلها المنطق و العقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية عن طريق ترجمة البيانات الحسابية المخزنة في اجهزة الحاسوب وملحقاته وشبكات الاتصال، ويمكن استخدامه في أي مرحلة من مراحل التحقيق او المحاكمة لاثبات فعل او شئ او شخص له علاقة بالجريمة[4].

ولم تعرف التشريعات المقارنة ومن بينها التشريع الجزائر الدليل الرقمي، ولم يورد ذكر هذا المصطلح في أي نص من النصوص القانونية المتعلقة بالموضوع.

المطلب الثاني: خصائص الدليل الرقمي:

نظرا للطبيعة الخاصة للجرائم المعلوماتية فإن دليل اثباتها يختلف يختلف ويتميز عن الدليل الجنائي التقليدي، لأن هذا النوع من الأدلة يعيش في بيئة متطورة بطبيعتها تشتمل على أنواع متعددة

[1]IOCE, Standards and Principles for Computer Evidence, October 2001.

[2]عبد الفتاح بيومي حجازي، الجرائم الإلكترونية وأدلة الإثبات الرقمية، دار الفكر الجامعي، 2018 ، ص.45

[3]عمر محمد بن يونس، الدليل الجنائي الرقمي وإجراءاته القانونية، دار كنوز المعرفة، 2020 ، ص.33

[4] عبد القاد عميمر، مرجع سابق، ص 104.

من البانات الرقمية تصلح مجتمعة أو منفردة لكي تكون دليل للإدانة أو البراءة ، فيعيد بذلك الدليل الرقمي الوسيلة الرئيسية في عملية اثبات الجرائم المعلوماتية، ويتميز الدليل الرقمي بعدة خصائص نوردها فيما لي:

- **الدليل الرقمي دليل غير ملموس** : الدليل الرقمي غير مادي فهو يتكوّن من بيانات ومعلومات، معطيات إلكترونية غير ملموسة لا تُدرك إلا عبر أنظمة معلوماتية، واخراجه في شكل مادي ملموس يتطلب الاستعانة بأجهزة الإعلام الآلي وملحقاته واستخدام أنظمة البرمجة، على ان هذه العملية ليست سوى عملية نقل لتلك المجالات من طبيعتها الرقمية الى الهيئة التي يمكن الاستدلال بها على معلومة معينة[1]، الا ان هناك من يذهب الى ابعد من ذلك ويرى ان قابلية الدليل الرقمي للتجسيد المادي هي ميزة اضافية تدعم حجية الدليل الرقمي وتزيد من موثوقيته.[2]
- **الدليل الرقمي دليل تقني:** يعكس الوسط الذي تكون فيه الدليل الرقمي طبعته التقنية وذلك راجع للآلات والاجهزة التي يستخلص منها.
- **صعوبة الوصول للدليل الرقمي:** لا يمكن الوصول الى هذا النوع من الأدلة إلا من طرف المختصين الذين لديهم معرفة وخبرة تقنية مما يستلزم خبرات متخصصة في استخراجه وتحليله.
- **ذو طبيعة ديناميكية** تمكنه من التنقل من مكان لأخر عبر شبكات الاتصال، فتعلق هذا الدليل بمسرح افتراضي يجعل الحصول عليه في مكان بعيد عبر الفضاء الرقمي ومن طرف اشخاص او هيئات ليست لهم علاقة بأطراف الجريمة ولديهم القدرة على الالمام ببعض تفاصيل الجريمة المعلوماتية كمزودي خدمات الانترنت.
- **قابل للنسخ والاسترجاع** مما يتيح حمايته من الضياع ويصعّب التخلص منه نهائيًا، وللدليل المسترجع نفس القيمة العلمية و الحجية الثبوتية الامر الذي لا يتوفر في الادلة التقليدية، و هو ما يشكل ضمانة قوية للحفاظ على الدليل الرقمي من التلاف و الفقدان والتغيير[3].
- **الدليل الرقمي علمي دقيق:** يخضع لآليات تقنية قابلة للفحص وفق مبادئ علوم الحوسبة، باستخدام برامج ونظم خاصة [4].

[1] طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، مجلة الحقوق، المجلد 12، العدد،01، جوان 2015، جامعة البحرين عمادة الدراسات العليا والبحث العلمي، ص 39.

[2] يوسف مناصرة، الدليل الالكتروني في القانون الجزائي، الجزائر: دار الخلدونية، 2018، ص 34

[3] مصطفى محمد موسى، إثبات الجرائم الإلكترونية بالدليل الرقمي، المركز القومي،2021 ، ص 64

[4] حسن مرعي، مبادئ الإثبات الرقمي، دار الجامعة الجديدة، 2019، ص 61.

المطلب الثاني: انواع الدليل الرقمي:

يعد الدليل الرقمي عنصرا حاسما في الاثبات الجنائي والمدني في العصر الحديث، حيث يستمد من الأجهزة الالكترونية و الانظمة الرقمية، وتتنوع اشكاله وفقا لمصدره وطريقة استخراجه، مما يجعله أداة قوية في الكشف عن الجرائم المعلوماتية وحتى الجرائم التقليدية التي تترك فيها آثار رقمية.

عادة يقسم الدليل الرقمي إلى ثلاث انواع وهي على النحو التالي[1]:

– **أولا:** السجلات المحفوظة في الكمبيوتر: و هي الوثائق المحفوظة أو المخزنة في الكمبيوتر مثل البريد الإلكتروني وملفات برامج معالجة الكلمات و غيرها.

– **ثانيا** :السجلات التي تم إنشاؤها بواسطة الكمبيوتر مثل سجلات الهاتف والفواتير أجهزة الحاسب الآلي (ATM) والكرت الإلكتروني الذكي .

– **ثالثاً** :السجلات التي تم حفظها عن طريق إدخالها ككل أو جزء منها تم إنشاؤها بواسطة الكمبيوتر أو عليها: مثل أوراق العمل المالية التي تحتوي على مدخلات تمت معالجتها إلى برامج أو أوراق رسمية للتعامل بإستخدام بعض برامج الحاسب الآلي مثل: I(Excel) ومن ثم تمت معالجتها من خلال البرامج بإجراء العمليات الحسابية عليه.

تُعد التقسيمات السابقة للدليل الرقمي استنتاجًا يعتمد على مصادر الدليل الرقمي، وقد توجد أنواع أخرى لم يتم التطرق إليها، من المعلوم أن الجريمة الإلكترونية هي نتاج لتطور تقنيات المعلومات والحاسوب، مما يستلزم مواكبة هذا التطور في الأدلة الرقمية لضمان فعاليتها في الإثبات، ففي حال عدم التكيف مع هذا التقدم، قد نواجه صعوبات في إثبات الجرائم المعلوماتية وفي هذا السياق، قسمت وزارة العدل الأمريكية الدليل الرقمي إلى ثلاث مجموعات رئيسية:

1. **السجلات المحفوظة في الحاسوب** :تشمل هذه الفئة الوثائق المكتوبة والمحفوظة إلكترونيًا، مثل رسائل البريد الإلكتروني، ملفات معالجة الكلمات، ورسائل غرف المحادثة على الإنترنت. تُعد هذه السجلات أدلة رقمية تم إنشاؤها بواسطة المستخدم وتخزينها في أنظمة الحاسوب.

2. **السجلات التي تم إنشاؤها تلقائيًا بواسطة الحاسوب** :تتضمن هذه الفئة البيانات التي يتم إنشاؤها تلقائيًا دون تدخل بشري مباشر، مثل ملفات السجلات(log files) ، سجلات الهاتف، وفواتير أجهزة الصراف الآلي .(ATM) تُعتبر هذه السجلات مخرجات لبرامج الحاسوب وتُستخدم كأدلة رقمية في التحقيقات.

3. **السجلات المختلطة** :تتكون هذه السجلات من بيانات تم إدخالها بواسطة المستخدم وأخرى تم إنشاؤها تلقائيًا بواسطة الحاسوب. مثال على ذلك أوراق العمل المالية التي تحتوي على مدخلات تم إدخالها في برامج مثلExcel ، حيث يتم معالجتها تلقائيًا لإجراء العمليات الحسابية[2].

---

[1] يس حسن محمد عثمان، الدليل الرقمي واثره على الدعوى الجنائية، المجلد05، العدد03، سبتمبر 2020، ص319.

[2] نفس المرجع آنف الذكر، ص 320.

وفقًا لتقسيماته، يمكن استخدام أي نوع من الدليل الرقمي في إثبات الجرائم، مما يعني أن استخدام الدليل الرقمي لا يقتصر فقط على الجرائم المعلوماتية، بل يمكن استخدام تلك الرموز والأرقام التي تُعتبر بينات كوسيلة إثبات ليس فقط في المجال الجنائي، بل حتى في المسائل المدنية .له دور كبير في تقرير حقوق الخصوم والفصل العادل في الدعاوى المدنية، خاصة في نزاعات العقود الإلكترونية .وبالتالي، فإن الدليل الرقمي بكافة أنواعه يساعد كثيرًا في تحقيق العدالة.

المطلب الثالث: حُجّية الدليل الرقمي

يشهد العصر الرقمي تزايدا كبيرا في الاعتماد على الدليل الرقمي كوسيلة إثبات في المحاكم، في الجرائم المعلوماتية و مع ذلك تختلف حجية هذا الدليل من نظام قانوني إلى آخر، حيث تفرض التشريعات شروطا معينة لقبوله أمام القضاء

الفرع الأول: حُجّية الدليل الرقمي في ظل نظام الإثبات الحر (النظام اللاتيني)

يُعتمد في الأنظمة القانونية ذات التوجه اللاتيني، مثل النظام الفرنسي، على مبدأ الإثبات الحر، الذي يمنح القاضي الجنائي سلطة تقديرية واسعة في تقييم الأدلة المعروضة أمامه، بما في ذلك الأدلة الرقمية .ففي فرنسا، لا يُشترط وجود نص قانوني خاص لقبول الدليل الرقمي، بل يُترك الأمر لتقدير القاضي، شريطة أن يتم الحصول على الدليل بوسائل مشروعة، وأن يُتاح للخصوم مناقشته خلال جلسات المحاكمة، مع احترام حقوق الدفاع.

وقد أكدت محكمة النقض الفرنسية هذا المبدأ، حيث اعتبرت أن الأدلة المستخرجة من الوسائل الإلكترونية، مثل التسجيلات الممغنطة، تُعد صالحة للإثبات أمام القضاء الجنائي، طالما تم الحصول عليها بطرق مشروعة، وتمت مناقشتها حضورياً[1] .

وفي هذا السياق، يُعتبر الدليل الرقمي تطبيقًا للأدلة العلمية، التي تتطلب في بعض الأحيان الاستعانة بالخبراء الفنيين لتفسيرها وتحليلها .فالقاضي، بحكم تكوينه القانوني، قد لا يكون مؤهلاً لتقييم الجوانب الفنية للدليل الرقمي، مما يستدعي الاستعانة بالخبرة الفنية لتحديد مدى سلامة الدليل ومصداقيته. وتجدر الإشارة إلى أن بعض التشريعات، مثل التشريع التركي، تشترط أن يكون الدليل الرقمي قابلاً للقراءة بعد استخراجه من الحاسوب أو من خلال عرضه على الشاشة، لضمان سلامته ومصداقيته [2].

وبالتالي، فإن نظام الإثبات الحر يُتيح للقاضي الجنائي الاستفادة من الأدلة الرقمية، شريطة الالتزام بالضوابط القانونية والإجرائية التي تضمن مشروعية الدليل وسلامته، مما يُسهم في تحقيق العدالة الجنائية.

---

[1] محمد المناوي، حجية الدليل الإلكتروني في إثبات الجرائم المعلوماتية، مجلة المنار، جامعة محمد الخامس بالرباط– كلية العلوم القانونية والاقتصادية والاجتماعية سلا،افريل 2020. على الموقع: revuealmanara.com

[2] جلال فضل، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني، نشر بتاريخ 2025/02/12. في صفحة القضائية على الموقع الاتي:https://alqadaeya-ye.net/?p=6068&utm_source=chatgpt.com :

وقد سارت على الأخذ بهذا الاتجاه مُعظم الدول الأوروبية (كألمانيا، واليونان، وكذلك أمريكا اللاتينية كالبرازيل)، وقد اعتمدت هذه الدول على الأخذ بنظام الإثبات الحر من حيث خضوع الأدلة الرقمية لسطات القاضي وقناعته الوجدانية، فله قبول الدليل أو رفضه، سيمًا إذا وجد أن هذه الأدلة لا تنسجم مع العقل والمنطق ووقائع الدعوى المطروحة عليه.

2- نظام الإثبات المقيد (الأنجلوسكسوني):

ويستند هذا الاتجاه على عدم منح القاضي السلطة التقديرية للدليل مهما كان نوع الدليل تقليديًا أم رقميًا، بمعنى أن القاضي لا يملك تقدير حجية الدليل بالمطلق، فالقانون هو الذي يحدد للقاضي ماهية الدليل ونوعه، وقيمته القانونية وحجيته في الإثبات الجزائي، وخلاصة ذلك أن الدليل لا يكون له القيمة القانونية إلا إذا نصّ القانون عليه وعدّه ضمن القائمة، فعدم وجود النص يعني لا قيمة للدليل، وليس له الحجية في الإثبات الجزائي. ومن الدول التي أخذت بهذا النظام بريطانيا حيث حدد المشرِّع البريطاني أدلة الإثبات في قانون الشرطة والإثبات الجنائي الصادر عام ١٩٨٤م متناولًا المشرِّع البريطاني في هذا القانون أدلة الإثبات في القضايا الجنائية بصورة دقيقة، لاسيمًا أن المشرِّع لم يمنح القاضي صلاحية تقدير الدليل من حيث قبوله أو رفضه. وقد سارت على نهج الأخذ بنظام الإثبات المقيدة العديد من الدول كالولايات المتحدة الأمريكية، وكندا، وفي أمريكا صدر قانون الحاسب الآلي عام 1984م متمخضًا عنه عدّ مخُرجات الحاسوب الإلكتروني أدلة لها قيمة وحُجتها القانونية.

3- نظام الإثبات المختلط:

أخذ هذا النظام بالجمع بين النظام اللاتيني والنظام الأنجلوسكسوني، بمعنى أن نظام الإثبات المختلط منح القاضي السلطة التقديرية لقبول الدليل في بعض أدلة الإثبات كالأدلة الرقمية. وفي أدلة أخرى القاضي لم يكن له إلا التزام بالنص القانوني، والذي يحدد القيمة والحجية للدليل هو القانون وليس القاضي، ففي بعض الدول كاليابان التي أخذت بنظام الإثبات المختلط عدّت أن الأدلة الجنائية التقليدية (كالشهادة، وأقوال المتهم والقرائن، والخبرة) هي أدلة قانونية، وليس للقاضي سلطة تقديرية فيها؛ لأن القانون هو الذي يمنح هذه الأدلة القيمة والحجة القانونية، بينما استقر الفقه الجنائي الياباني على أن الأدلة الإلكترونية تخضع للسلطة التقديرية للقاضي فمثلًا: المجالات الإلكترومغناطيسية إذا كانت غير ملموسة أو مرائية لا تُعدُّ دليلًا يستند عليه القاضي المختص، أما إذا تحولت المجالات الإلكترومغناطيسية إلى أدلة مقروءة ومرئية فيمكن عدّها دليلًا في الإثبات الجنائي، وهذه تخضع للسلطة التقديرية للقاضي بحكم طبيعة الدليل ووقائع الدعوى. مرتبط

الفرع الثاني: ضوابط حجّية الدليل الرقمي في التشريع الجزائري

رغم اعتراف المشرّع الجزائري ضمنيًا بحجّية الدليل الرقمي في المواد الجزائية، إلا أن هذا الاعتراف يظل مشروطًا بتوافر جملة من الضوابط القانونية والإجرائية التي تضمن نزاهته وسلامته. أول هذه الشروط هو: **المشروعية في الحصول على الدليل**، أي أن يتم جمع البيانات الرقمية بوسائل لا تنتهك الحقوق الدستورية، وعلى رأسها الحق في الخصوصية، وذلك وفق ما تنص عليه قواعد التحري والتحقيق في قانون الإجراءات الجزائية، ولا سيما المادتين 44 و83 مكرر من التعديلات الأخيرة .[1]كما يُشترط أن يتم **توثيق الدليل الرقمي وفق قواعد فنية دقيقة** تحفظ سلامته وتمنع التلاعب به، مثل تسجيل وقت الحصول عليه، وطريقة المعالجة، والأدوات المستخدمة، وهو ما يستدعي في كثير من الحالات الاستعانة بالخبرة الفنية المختصة[1]

ويُعدّ **مبدأ الإقناع الشخصي للقاضي** المرتكز الأساس في تقدير هذا النوع من الأدلة، إذ تعود له سلطة تقييم مدى كفاية الدليل الرقمي وقوته الثبوتية في ضوء ظروف كل قضية على حدة، وذلك استنادًا إلى مبدأ حرية الإثبات المنصوص عليه في المادة 212 من قانون الإجراءات الجزائية كما يُشترط أن يكون الدليل الرقمي قابلاً للمناقشة العلنية أمام أطراف الدعوى أثناء المرافعة، ضمانًا لحقوق الدفاع ومبدأ المواجهة. وبالتالي، فإن حجّية الدليل الرقمي لا تختلف في أصلها عن باقي الأدلة الجنائية، وإنما تستوجب مراعاة خصوصيتها التقنية والإجرائية في بيئة رقمية معقدة.[2]

[1] بيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، مصر (الإسكندرية): دار الفكر الجامعي ، 2022، ص63.

[2] عمر بن خليف، "الجرائم الإلكترونية في التشريع الجزائري"، المجلة الجزائرية للعلوم القانونية، العدد 2، 2021، ص 145.

خلاصة الفصل:

يمكن استخلاص من هذا الفصل أن "الجريمة المعلوماتية" تمثل تحديًا معاصرًا أمام الأنظمة القانونية والأمنية، نظرًا لطبيعتها المعقدة وارتباطها بالتطور التكنولوجي المتسارع. فمن خلال تحليل مفهومها وأركانها، يتضح أن هذه الجرائم تتسم بخصائص فريدة، مثل العابرة للحدود والاعتماد على تقنيات متقدمة، مما يجعل مواجهتها تتطلب آليات استباقية وتكيفًا مستمرًا .

أما فيما يخص "الدليل الرقمي"، فقد تبين أنه العامل الحاسم في كشف الجرائم الإلكترونية وإثباتها، لكنه يواجه تحديات جوهرية تتعلق بالحفاظ على سلامته وموثوقيته. فتنوع أنواعه وهشاشته يفرضان ضرورة تطوير معايير دقيقة لجمع الأدلة وتحليلها، فضلًا عن الحاجة إلى أطر قانونية تُنظم قبوله كدليل قضائي .

وعليه، فإن التكامل بين "التقني والقانوني" يظل الركيزة الأساسية لمكافحة الجرائم الإلكترونية، حيث يتطلب تعزيز التعاون بين خبراء الأمن السيبراني والمشرعين لضمان فعالية الأدلة الرقمية في تحقيق العدالة. وفي ظل التطور المستمر للجرائم المعلوماتية، تبرز أهمية مواكبة التشريعات وتطوير الأدوات التحليلية لسد الثغرات التي قد يستغلها المجرمون.

الفصل الثاني: الجوانب الفنية والإجرائية للتعامل مع الدليل الرقمي

تمهيد

أمام التطور المتسارع والهائل في مجال تكنولوجيا المعلومات والاتصال، تنوعت أشكال الجريمة وأخذت توجها رقميا أكثر تعقيدا من قبل، مما استدعى الامر على تطوير آليات خاصة في التحقيق والبحث عن الأدلة، وعلى رأسها "الدليل الرقمي". فهذا النوع من الأدلة وإن كان غير مادي بطبيعته، إلا أنه بات يحتل مكانة محورية في الإثبات الجنائي، خصوصًا في الجرائم السيبرانية والجرائم المرتكبة بواسطة الوسائط الإلكترونية.

غير أن التعامل مع الدليل الرقمي يقتضي مراعاة بعدين أساسيين: البعد الفني الذي يتعلق بطرق الحصول على البيانات وتحليلها باستخدام تقنيات خاصة، والبعد الإجرائي الذي يضمن احترام القواعد القانونية عند جمع وتقديم هذا الدليل، حتى يكون معتمدًا أمام الجهات القضائية. وقد حرص المشرّع الجزائري من خلال تعديل قانون الإجراءات الجزائية بموجب القوانين 06-22 و09-04، على إدماج ضوابط دقيقة تضمن مشروعية استخدام هذه الأدلة، دون المساس بحقوق المتقاضين وحرمة الحياة الخاصة.

وانطلاقًا من هذا نقسم الفصل الى :

المبحث الأول : الجهات الفنية المعنية بتحليل الدليل الرقمي

المبحث الثاني: الجوانب الإجرائية للحصول على الدليل الرقمي

المبحث الأول: تفنيات الحصول على الدليل الرقمي

أصبحت الجرائم الرقمية سمة العصر اليوم فهي تشكل أحد أبرز التحديات التي تواجه أجهزة العدالة الجنائية. حيث بات الدليل الرقمي يحتل مكانة محورية في التحقيقات الجنائية كونه يمثل أداة إثبات فعالة في كشف الجريمة وتحديد هوية مرتكبها. غير أن خصوصية هذا النوع من الأدلة، من حيث طبيعته التقنية، وسرعة تلفه، وإمكانية تعديله أو محوه، تفرض على الجهات المكلفة بالتحليل الجنائي اعتماد فنيات دقيقة وإجراءات متخصصة في سبيل الحصول عليه بطرق مشروعة تحافظ على سلامته وقيمته القانونية ، وفي هذا السياق نقسم المبحث الى: **(المطلب الأول)** مفهوم التحليل الجنائي المعلوماتي **(المطلب الثاني)** الجهات الفنية المعنية بتحليل الدليل الرقمي والى **(المطلب الثالث)** تحليل الدليل الرقمي من حيث مكان الحصول عليه

المطلب الأول: مفهوم التحليل الجنائي المعلوماتي

كثيرة هي الأضرار الناجمة عن جرائم المعلومات والبيانات في صورة النصب الالكتروني والاختراقات والتجسس...الخ، فالأضرار تزيد بشكل كبير، وليس فقط من خلال الخسائر المالية المباشرة، ولكن أيضًا من خلال تأثيرها على سمعة الشركات والأفراد، وتكاليف التحقيق والتصحيح، الأمر الذي يتطلب تطبيق تدابير أمنية أقوى وتكنولوجيا حماية متطورة لمكافحة التهديدات السيبرانية والحفاظ على البيانات والمعلومات الحساسة. توجد مجموعة متزايدة من المهنيين المختصين في مجال الأمن السيبراني والتحقيق الجنائي الرقمي لمساعدة في مكافحة هذه الجرائم وحماية البيانات والمعلومات.

الفرع الأول : تعريف التحليل الجنائي المعلوماتي

التحليل الجنائي الرقمي أو ما يطلق عليه ايضًا مصطلح الطب الشرعي الرقمي هو العملية المتخصصة التي تهدف إلى جمع وتحليل الأدلة الرقمية المتعلقة بالجرائم. حيث تشمل العملية استخدام أجهزة الحوسبة والتكنولوجيا الرقمية لفحص البيانات والأجهزة التي قد تحتوي على أدلة تساهم في فهم الجريمة وتحديد الجناة،[1]

[1 1] مخلوف داودي، **الطب الشرعي الرقمي إطلالة على المفهوم و أهميته في نظام العدالة الجنائية**، مجلة الاجتهاد للدراسات القانونية و الاقتصادية، المجلد21، العد01، 2022،ص396.

فهي تشمل هذه الأدلة الرقمية المعلومات والملفات والسجلات التي يمكن العثور عليها على أجهزة الكمبيوتر والهواتف المحمولة والأجهزة اللوحية والأجهزة الذكية الأخرى، ومساعدة في تقديم الأدلة أمام المحكمة[1]

كما يعرف التحليل الجنائي الرقمي على انه هو " استخدام التقنيات العلمية والتكنلوجية في عمليات التحقيق الجنائي للقضايا المخالفة للقانون في صورة جرائم المعلومات، وتتضمن فحص الجهاز أو المنظومة المعلوماتية وتحليل العمليات واسترجاع البيانات والملفات من أجل الحصول على دليل رقمي digital evidence يستخدم في التحقيقات القانونية[2]

كما جاء تعريف التحقيق الجنائي في الجرائم الإلكترونية على أنه "عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجريمة الإلكترونية من فاعل لها ودليل إلكتروني لتقديمهم إلى سلطات التحقيق القضائي المتخصصة في هذا النوع من الجرائم الإقامة العدل[3]

يتضح من التعريف أن التحقيق الجنائي في الجرائم الإلكترونية يمثل مرحلة حاسمة في مواجهة هذا النوع المعقّد من الجرائم، إذ يجمع بين الإجراءات القانونية التقليدية والمعالجة التقنية الحديثة، ويُناط به مأمور الضبط القضائي المختص الذي يتولى مهمة كشف الجريمة وتحديد مرتكبيها وجمع الأدلة الرقمية بطرق قانونية تحفظ حجيتها أمام القضاء، تمهيدًا لإحالة الملف إلى السلطات القضائية المختصة، بما يضمن احترام مبدأ الشرعية وتحقيق العدالة في بيئة رقمية تتسم بالتغير السريع والتعقيد التقني.

وهناك من عرف التحليل الجنائي الرقمي بأنه" عملية البحث في مستودع السر للمتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه أو الاطلاع على حمل منحه القانون حماية خاصة باعتباره مستودع السر بصاحبه فيمكن أن يكون المحل جهاز الكمبيوتر أو أنظمته أو الانترنت للاستدلال بها على صدق نسبة الفعل إلى شخص معين أو كذبه[4] .

[1] مخلوف داودي، الطب الشرعي الرقمي إطلالة على المفهوم و أهميته في نظام العدالة الجنائية، مجلة الاجتهاد للدراسات القانونية و الاقتصادية، المجلد21، العد01، 2022،ص

[2] جميل حسين طويل، التحليل الجنائي الرقمي، دليل عملي الطرق التحليل الجنائي الرقمي في الجرائم المعلوماتية، سوريا ، ب س، ص 10.

[3] مصطفي محمد موسي، التحقيق الجنائي في الجرائم الإلكترونية، مصر(القاهرة): مطابع الشرطة، 2009، ص 169.

[4] محمد صلاح محمد عبد المنعم، الجرائم الإلكترونية وتحدياتها –دراسة مقارنة، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، 2005، ص 234.

ويمكن تعريف التحليل الجنائي الإلكتروني على أنه الإجراءات التي يقوم بها مأموري الضبط القضائي أو المحققين عبر العالم الافتراضي لضبط الجريمة الإلكترونية والتثبت من أدلتها ومعرفة فاعلها تمهيداً لإحالتهم للمحاكمة". [1]

من خلال ما سبق من التعريف يمكن القول بأنه يتمثل في مجموعة الإجراءات التي ينفذها مأمورو الضبط القضائي أو المحققون في الفضاء الرقمي بغرض ضبط الجريمة الإلكترونية، والتأكد من صحتها من خلال جمع الأدلة الرقمية، وتحديد مرتكبي الجريمة. ويشكل هذا التحقيق خطوة أساسية في العملية القضائية، حيث يُمكّن من جمع الأدلة اللازمة التي تُستخدم لاحقًا في محاكمة المتهمين، وبالتالي تحقيق العدالة في ظل التطور التكنولوجي والتهديدات الإلكترونية المتزايدة.

الفرع الثاني :أهداف التحليل الجنائي الرقمي

التحليل الجنائي الرقمي يلعب دورًا حاسمًا في كشف الجرائم وتوجيه الإجراءات القانونية ضد المتهمين. كما يساهم في الحفاظ على الأمان السيبراني ومكافحة التهديدات الإلكترونية، حيث أن الغرض والهدف من التحقيق الجنائي في الجرائم الالكترونية تتجلى من وجوه متعددة منها ما هو متعلق بإثبات وقوع الجريمة وكيفية ارتكابها وسبب وقوعها ومعرفة الجاني واقوال الشهود واهل الخبرة وهي كالآتي:

أولا : اثبات وقوع الجريمة :

يجب على المحقق في بداية الأمر التحقق من أن هناك جريمة وقعت أي وقوعها ماديا (وفي ذلك يتم البحث عن جسم الجريمة)، فهنا يكون على المحقق جمع الأدلة التي تؤيد وقوع الجريمة مادياً فقد يبلغ المحقق بأمر وهو من نسيج الخيال للمبلغ وقصده بذلك ازعاج للسلطات أو النكاية والإيقاع بشخص ما، حيث إن انعدام جسم الجريمة ليس من شأنه القول بانعدامها أو عدم وقوعها أو كتب البلاغ فقد يثبت من التحقيق أن المجني عليه قد قتل فعلا وتتجمع في الأفق الأدلة على حدوث جريمة القتل ولكن

[1] خالد علي نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة الدكتوراة في الحقوق، كلية الحقوق – جامعة المنصورة، ب س، ص 5.

التحقيق لم يوصل إلى العثور على الجنة لأن الجاني أخفاها في مكان ما لم يهتد اليه بعد فهذا لا يقدر دليل الاتهام وليس من شأنه أن يفلت الجاني من المسئولية متى توفرت أدلة الاتهام ضده. [1]

فالتحقيق التقليدي يهدف إلى جمع الأدلة المادية من حيث إن نظام أجهزة الكمبيوتر عبارة عن كيانات معنوية لا تتوافر فيها صفة المادة سواء تتعلق ببرامج الكمبيوتر أو ما يشتمل عليه من بيانات فالتطور المتزايد في استخدام أجهزة الكمبيوتر وما صاحبها من ظهور طائفة جديدة من الجرائم يتطلب من السلطات القضائية أن تتعامل مع أشخاص مستحدثة من الأدلة في الاثبات الجنائي، حيث يتطلب اثباتها نوعا من الأدلة لا يندرج ضمن أنواع الأدلة الجنائية التي اعتادت عليها لجهات التحقيق فهذه لها خصائص ومميزات تتطلب قواعد ومواجهات جديدة تمكن من التعامل معها . مما ينبغي معه وجود أجهزة تحقيق في حاجة المهارات جديدة وتخصصات غير تقليدية للتعامل مع مثل هذا النوع من الأدلة.

ثانيا : تحديد أسلوب ارتكاب الجريمة

ينبغي على المحقق في سياق مباشرة إجراءات التحري وجمع الأدلة، أن يولي أهمية بالغة لكيفية ارتكاب الجريمة وظروف وقوعها، إذ إن لكل مجرم أسلوبا خاصا يتبعه في تنفيذ أفعاله الإجرامية، حيث أنه تعد معرفة الطريقة التي ارتكبت بها الجريمة نقطة انطلاق حاسمة في عمل المحققين لأنها تمكنهم من حصر دائرة الشبهات ضمن عدد محدود من المشتبه بهم وذلك بناءً على الخصائص النمطية أو الفريدة التي يتسم بها أسلوب الجاني في تنفيذ الجريمة[2].

فالأسلوب المستخدم في ارتكاب الجريمة، بما يشمله من كيفية التخطيط والتنفيذ، يعد من الحقائق الجوهرية التي يجب على المحقق الوصول إليها وتوثيقها بدقة، وهذا الامر يعود الى أن فهم هذا الأسلوب يُسهم في رسم خطة بحث فعّالة وموجهة نحو الجاني الحقيقي، مما يقلل من الجهد المبذول ويزيد من احتمالية الوصول إلى نتائج دقيقة.

[1] عدلي دحمان، سعد الدين ثامر البشير، التحقيق الجنائي في الجرائم الالكترونية، مذكرة ضمن متطلبات نيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، قسم الحقوق، جامعة زيان عاشور – الجلفة، 2020–2021، ص 11.

[2] عبد الله أحمد، علالي حجية المخرجات الكمبيوترية في المواد الجنائية – دراسة مقارنة، 1999، ص 12.

حيث أن إن ارتكاب جريمة باستخدام أدوات أو وسائل تقنية، كزرع برامج اختراق أو تجسس داخل أنظمة معلوماتية، يدل على أن الفاعل يملك مهارات تقنية متقدمة، وقد تكون دوافعه مرتبطة بالحصول على معلومات سرية لا يمكنه الوصول إليها بشكل مباشر. في هذه الحالة، يتعين على المحقق حصر الاشتباه في فئة محددة من الأشخاص، كموظفي قسم الصيانة أو التشغيل، أو حتى المبرمجين العاملين بالمؤسسة، خاصة أولئك الذين لديهم صلاحيات الدخول إلى الأنظمة أو التعديل في إعداداتها.

ويكتسي تحديد الأدوات المستخدمة في الجريمة أهمية خاصة، ليس فقط لتكوين تصور دقيق عن كيفية ارتكاب الفعل الإجرامي، بل كذلك لتحديد شخصية الجاني المحتملة. إذ إن طبيعة الأدوات تدل على مستوى مهارات الجاني، ودرجة التخطيط، ونوع الخبرة التي يمتلكها. كما أن معرفة هذه الأدوات يُمكّن المحقق من تحديد الأشياء التي يجب تفتيشها أو ضبطها أثناء تنفيذ الإجراءات القانونية ذات الصلة كأوامر التفتيش أو الحجز[1].

كما أن السجل الجنائي له دور جوهري في هذا السياق، حيث يوفّر قاعدة بيانات لأنماط الجرائم وأساليب تنفيذها، وهو ما يسمح بمقارنة الجريمة محل التحقيق مع جرائم سابقة قد تكون نُفذت بذات الطريقة. وبالتالي، يمكن ربطها بأشخاص اعتادوا ارتكاب جرائم مماثلة، مما يُسرّع عملية التعرف على الجاني وتوجيه الاتهام إليه.

ليتضح أن دراسة الأسلوب الإجرامي تعد أداة تحليلية دقيقة وداعمة فهي تساعد المحقق في بناء إطار عملي لتضييق دائرة الاشتباه بالمشتبه بهم في هذه الجريمة، ووضع خطة فعالة للبحث عن الجاني، وهو ما يتطلب خبرة تقنية وتحليلية عالية، خاصة في الجرائم التقنية والمعلوماتية الحديثة.

ثالثا : سبب وقوع الجريمة

على المحقق في سبيل التعرف على السبب لوقوع الجريمة (الدافع) لارتباط العلة بالمعلول، فلا جريمة بلا سبب، فالتحقق من سبب وقوع الجريمة بعد الخطوة الأولى للمحقق في ذلك فبعض الظروف يكون سابقا على وقوع الجريمة ومثالها سوء سمعة المتهم وسلوكه والشكاوي التي حدثت بالمؤسسة وبعض الظروف المعاصرة لارتكاب الجريمة مثل وجود المتهم حال وقوع الجريمة وساعة ارتكابها وبعض

[1] عمار على الصيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة،لبنان: منشورات الحلبي الحقوقية، 2015، ص 20.

من الظروف لاحق على ارتكاب الجريمة مثل تصرفات وسلوك من تحيط حوله الشبه بسبب الجريمة هو الوقائع المادية التي حدثت فاثرت في نفسية الجاني مما أدى لبروز الدافع على ارتكابه الجريمة وهو أمر نفسي داخلي يرتبط بالغرائز الإنسانية فتحديد السبب في بعض الجرائم يشكل في حد ذاته دليلاً على ارتكاب المتهم للجريمة ويكفل لتحديد السبب بحصر دائرة البحث في عدة اشخاص، إلا أن الأمر في الجرائم الإلكترونية من الصعب معرفة الحادث أو الجريمة، ذلك لأن الدافع للجاني غير واضح فيمكن أن تحدث الجريمة بالخطأ أو أن الجاني لا يحدد هدفاً وهذا راجع لأسلوب ارتكابه الجريمة كالمبرمج الذي يضع قنبلة موقوفته في النظم لدرء المسؤولية عند اكتشاف جريمة يريد إخفاؤها وعلى العموم فعن دور المحقق في معرفة سبب الجريمة هنا ليس سهلا وإنما يتطلب دقة وذكاء شديدين بالإضافة للصبر والتأني[1]

رابعا : تحديد معرفة الجاني

إن تحديد الأغراض الثلاثة المتقدمة، ما هي إلا مقدمة للوصول إلى الهدف الرابع والأخير للتحقيق الجنائي الرقمي ألا وهو معرفة مرتكب الجريمة فالتحقق من شخصية المجرم ورسم صورته[2]، فهذا الامر يعتمد على توافر معلومات عن تكوينه وذلك بالتعمق في التحقيق معه فهنالك خصائص تساعد في ذلك كالذكاء والمعرفة بالتقنيات العالية وعدم اقتران القانون وانتحال الشخصية وقوة الدافعية كالتسلية، وحب المال، والانتقام كما أن التعرف على المجرم الإلكتروني ورسم صورته يعتمد على معلومات عن تكوينه البدني والعقلي والعاطفي فلا تعتبر الصورة التي ترسم عنه دليلاً ضده إلا أنها قد تكون بداية البحث عن الأدلة

وتبنى عادة الصورة للمجرم من أقوال الشهود فهم يشكلوا عامل حاسم في تحديده إذا أحسن المحقق مناقشتهم والإحاطة بظروف كل منهم وأضف لذلك معاينة مسرح الجريمة لما تشكله من عامل مهم لكشف سبب الجريمة، وكذلك سماع الخبراء الذين يرشدون المحقق عن الأسباب المحتملة لوقوع الحادث كنقصي آثار المجرم والأدوات المستخدمة، حيث تتميز الجريمة الالكترونية بالستر والخفاء، لانها ترتكب في وسط ذا طبيعة افتراضية غير محسوسة من قبل مجرمية في كفاءة ودراية بنظم المعلومات بحيث تتوافر لديهم القدرة على اخفاء اثار الجريمة بالإضافة لاخفاء شخصياتهم على المنظمة أو المؤسسة المجني عليها

[1] عمار على الصيني، المرجع السابق، ص 25.

[2] الفاروق الحسني، أصول علم الإجرام وعلم العقاب، دار النهضة العربية، القاهرة، 2002، ص 20.

المطلب الثاني: الجهات الفنية المعنية بتحليل الدليل الرقمي

إن التعامل مع الدليل الرقمي لا يقتصر على مجرد ضبطه أو استخراجه من الأجهزة أو الشبكات، بل يتطلب أيضا تحليلا فنيا متقدما لكشف مضمونه وعلاقته بالجريمة وتقييم مدى صلاحيته للاستخدام كدليل أمام القضاء ونظرًا للطبيعة التقنية المعقدة لهذا النوع من الأدلة، فإن عمليات التحليل لا تسند إلى جهات التحقيق العادية فقط، بل تتطلب تدخل هيئات وجهات فنية مختصة تملك الكفاءة والتجهيزات اللازمة للتعامل مع الأدلة الرقمية، وضمان سلامتها خلال عمليات الفحص والاسترجاع والتوثيق.

لذلك نسعى من خلال هذا المطلب إلى تسليط الضوء على أبرز الجهات الفنية المعنية بتحليل الأدلة الرقمية حيث نترطق الى الشرطة القضائية المتخصصة (الفرع الأول) والى الخبراء المعتمدون من طرف الجهات القضائية (الفرع الثاني)

الفرع الاول: الشرطة القضائية المتخصصة

تعد الشرطة القضائية وخصوصًا الفرق المتخصصة منها في مكافحة الجرائم السيبرانية من أبرز الجهات التي تتولى تحليل الأدلة الرقمية في الجزائر، حيث إن أعضاء الشرطة القضائية موظفون منحهم القانون صفة الضبطية القضائية وخولهم بموجب هذه الصفة حقوقاً وفرض عليهم واجبات في إطار البحث عن الجرائم ومرتكبيها وجمع الاستدلالات عنها حيث يبدأ دورهم بعد وقوع الجريمة وينتهي عند فتح ملف التحقيق القضائي أو إحالة المتهم إلى جهة الحكم.، حيث يعهد إليها بالقيام بعمليات الحجز الإلكتروني، وتفتيش الأجهزة الرقمية وتحليل محتواها بموجب أوامر صادرة عن الجهات القضائية المختصة.

وتعمل هذه الفرق ضمن مديرية الأمن الوطني والدرك الوطني، وتضم تقنيين متخصصين في المعلوماتية الشرطية. ويستند تدخل الشرطة القضائية إلى قانون الإجراءات الجزائية الجزائري، لا سيما المادتين 44 و65 مكرر، اللتين تجيزان اتخاذ التدابير التقنية الحديثة لجمع الأدلة في إطار التحقيقات الابتدائية والتحقيق القضائي. كما يندرج عملهم تحت ما يسمى بـ"التحريات الإلكترونية" المقرّة ضمن القانون 09-04 المتعلق بالوقاية من الجرائم المعلوماتية[1].

[1] القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالوقاية من الجرائم المعلوماتية ومكافحتها.

حيث أنه من خلال تمديد الاختصاص المحلي للجهات القضائية قام المشرع الجزائري في أول تعديل لمواجهة الجريمة المعلوماتية بالقانون 04-15 المؤرخ في 10-11-2004 وتحديدا المواد 37 40 329 بتمديد الاختصاص المحلي للمحكمة ووكيل الجمهورية وقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم بموجب المرسوم التنفيذي 06-348 المؤرخ في 5 أكتوبر سنة 2005 ويتعلق هنا الأمر بمحكمة سيدي محمد ومحكمة قسنطينة ومحكمة ورقلة ومحكمة وهران وكل محكمة من هذه المحاكم يمتد اختصاصها الى المحاكم المجاورة لها. [1]

حيث يمكن للشرطة القضائية متى تبين الاختصاص لإحدى هذه المحاكم أو الأقطاب المتخصصة أن تتلقى التعليمات من وكيل الجمهورية لهذه المحكمة وفق المواد 40 مكرر 1 إلى 40 مكرر5 من قانون الاجراءات الجزائية المعدل والمتمم بموجب القانونين 04-14 و 06-22 [2]حيث يتعين على ضابط الشرطة القضائية متى رأى الملف المكون من طرفه في مرحلة البحث والتحري المتعلق بالجريمة المعلوماتية أن يخبر فورا وكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة.

يكون الاجراء بتقديم أصل ملف الاجراءات مرفق بنسختين ثم يقوم وكيل الجمهورية فورا بإرسال النسخة الثانية الى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة ذات الاختصاص الموسع وذلك طبعا وفقا للسلم الإداري وبعد اطلاع النائب العام على الملف واعتباره يدخل ضمن اختصاص المحكمة ذات الاختصاص الموسع يحيله الى وكيل الجمهورية لدى المحكمة ذات الاختصاص الموسع وعليه وبعد تمسك هذه الجهة باختصاصها فإن ضباط الشرطة القضائية المنجزة للملف تتلقى تعليمات مباشرة من وكيل الجمهورية للمحكمة ذات الاختصاص الموسع.

مع ضرورة الإشارة إلى أن اختصاص ضابط الشرطة القضائية في هذه الحالة يمتد إلى كافة الإقليم الوطني دون التقيد بأحكام فقرات المادة 16 من قانون الإجراءات الجزائية مع توجب إخطار النائب العام لدى المجلس القضائي ووكيل الجمهورية المختصين إقليميا[3].

---

[1] فريدة بن يونس، الإطار الناظم لإختصاص الشرطة القضائية في مواجهة الجريمة المعلوماتية في التشريع الجزائري، مجلة الاجتهاد القضائي المجلد 12 ، عدد خاص، 2020، 129.

[2] قانون رقم 06 – 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج ر العدد84 ،الصادرة بتاريخ 24 ديسمبر 2006.

[3] المادة 16 من الأمر 66 –155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

كما يمكنهم وتحت سلطتهم أعوان الشرطة القضائية ما لم يعترض على ذلك وكيل الجمهورية المختص بعد إخباره أن يمددوا عبر كامل عبر الإقليم الوطني عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الاشتباه فيهم بارتكاب الجرائم المعلوماتية، كما يخول لهم القانون مراقبة وجهة أو نقل أشياء أو أموال أو متحصلات من ارتكاب هذه الجرائم أو قد تستعمل في ارتكابها . [1]

الفرع الثاني: الخبراء المعتمدون من طرف الجهات القضائية

يعد العمل على تحليل الأدلة الرقمية ضمن اطار الجريمة المعلوماتية من المهام التي تتطلب خبرات تقنية دقيقة ومعرفة معمقة بأنظمة المعلومات، وهذا الامر يعود الى أهم ما تتميز به هذه الأدلة من تعقيد في بنيتها، وسرعة تلفها، وإمكانية التلاعب بمحتواها أو تغيير خصائصها التقنية دون ترك آثار واضحة ولو عن بعد، حيث أنه ولأجل ذلك، غالباً ما تلجأ الجهات القضائية، سواء على مستوى التحقيق الابتدائي أو التحقيق القضائي أو الحكم، إلى الاستعانة بخبراء معتمدين لديهم الكفاءة الفنية والاختصاص في مجال الإعلام الآلي والأدلة الرقمية[2].

هؤلاء الخبراء يخضعون قانونًا لأحكام المواد من 143 إلى 145 من قانون الإجراءات الجزائية الجزائري، والتي تنظم كيفية ندب الخبير، وتحديد مهمته، ووجوب تقديم تقرير فني مكتوب حول الوقائع أو المسائل الفنية المطروحة. ويملك وكيل الجمهورية أو قاضي التحقيق أو هيئة المحكمة صلاحية تكليف الخبير، متى تبين أن المسألة المطروحة تتجاوز الفهم العام وتتطلب رأيًا تقنيًا متخصصًا لفهم طبيعة الدليل الرقمي أو إثبات أصالته أو تحديد مدى صلاحيته القانونية كوسيلة إثبات.

ووفقا للتشريع الجزائري يتم تنظيم عمل هؤلاء الخبراء ضمن قوائم رسمية تصدرها المجالس القضائية عبر مختلف ولايات الوطن، وتخضع هذه القوائم لمراقبة دورية من الجهات القضائية لضمان توفر شروط الكفاءة والتخصص والنزاهة في من يُقيَّد ضمنها. ويُشترط في الخبير أن يتمتع بمؤهلات علمية وتقنية تؤهله للتعامل مع الأنظمة الرقمية وتحليل محتواها، بالإضافة إلى التحلّي بالحياد والأمانة في إعداد التقرير، بالنظر إلى الأثر الكبير الذي قد يُحدثه في توجيه سير الدعوى.

[1] فريدة بن يونس، المرجع السابق، ص 130.

[2] عبد الحكيم زردومي، الجرائم المعلوماتية في التشريع الجزائري، الجزائر: دار هومة، 2018، ص 89.

ويتم أداء مهام الخبرة تحت إشراف مباشر من الجهة القضائية المختصة، التي تُحدد نطاق المهمة بدقة في قرار الندب، وتحتفظ بحق مناقشة تقرير الخبير، بل وإمكانية رفضه أو استبداله بخبير آخر عند ثبوت الانحياز أو الإهمال. كما قد يتم استدعاء الخبير لسماع أقواله حول ما ورد في تقريره، لتمكين الخصوم من مناقشته والتأكد من مدى صحة الأسس العلمية والتقنية التي اعتمد عليها في تحليله[1].

المطلب الثالث: تحليل الدليل الرقمي من حيث مكان الحصول عليه

يعد مكان الحصول على الدليل الرقمي من الاعتبارات الأساسية التي تؤثر على حجيته ومشروعيته في اصدار الحكم، خاصة في ظل تزايد التحديات المرتبطة بخصوصية الأفراد وسرية المعلومات.

ففي البيئة الرقمية، يمكن الحصول على الأدلة من مصادر متعددة تتنوع بين الفضاءات العامة كشبكة الإنترنت المفتوحة، والخاصة مثل الأجهزة الشخصية أو الحسابات المحمية بكلمات مرور. ويترتب على هذا التنوع إشكالات قانونية متعددة تتعلق بمدى احترام الضوابط القانونية أثناء جمع الدليل، لا سيما تلك المرتبطة بحقوق الإنسان وحرمة الحياة الخاصة. لهذا نقسم المطلب الى (الفرع الأول) بالنسبة لتحليل الأجهزة الإلكترونية وفي (الفرع الثاني) بالنسبة لتحليل الملفات

الفرع الأول: بالنسبة لتحليل الأجهزة الإلكترونية

تحليل الأجهزة الإلكترونية، مثل الهواتف المحمولة والأقراص الصلبة، هو عملية استخراج الأدلة الرقمية من هذه الأجهزة .يشمل هذا التحليل استعادة البيانات المحذوفة، تحليل محتوى الأجهزة، واستخلاص معلومات مفيدة قد تكون ذات صلة بالجرائم الإلكترونية أو الحوادث الأخرى.

أولا : القرص الصلب

وفي بحثنا في التشريع الجزائري لا يوجد الى حد الان نص صريح يفصل كيفية إجراءات تحليل القرص الصلب، لكن المعتمد في القواعد العامة في قانون الإجراءات الجزائية (المواد 66 مكرر و65 مكرر 10) تؤكد على وجوب المحافظة على سلامة الدليل عند تحصيله وتحليله[2].

[1] محمد سليم قلالة، الإثبات في الجريمة الإلكترونية، دار الجامعة الجديدة، 2020، ص 56.

[2] قانون الإجراءات الجزائية الجزائري، المواد 65 مكرر، 66 مكرر.

في مجال استعادة الملفات من القرص المخرب حيث أنه في بعض الحالات يقوم المتهم بتخريب القرص الصلب قبل تمكننا من الحصول عليه ويجب علينا محاولة استعادة البيانات من القرص المخرب حيث يوجد حالتين يمكن أن نصادفها عند محاولة استعادة الملفات: [1]

1 . الملفات تعرضت لضرر فيزيائي physically damaged

2 . الملفات تعرضت لضرر منطقي logical damage

الضرر الفيزيائي: القرص الصلب يمكن أن يتعرض لضرر فيزيائي يمكن أن يقوم المتهم بكسره أو تخريبه أو يمكن أن يتعرض لتخريب بسبب مشاكل كهرومغناطيسية (صدمة كهربائية وفي هذه الحالة يوجد احتمال لنجاح عملية استعادة الملفات.

الضرر المنطقي:يمكن أن يحدث بسبب إيقاف تشغيل الجهاز بشكل خاطئ أو بسبب انقطاع الكهرباء بشكل مفاجئ أو عند إيقاف تشغيل الجهاز أثناء عملية الإقلاع.

فعظم أنظمة التشغيل تؤمن أدوات إصلاح نظام windows يحوي على أداة fsck utility يحوي على linux ونظام chkdsk utility

كما يوجد العديد من الأدوات والبرامج الأخرى التي يمكن أن تقوم بإصلاحالضرر المنطقي وتساعد على إستعادة الملفات مثل:The Sleuth Kit TestDisk

حذف الملفات لا يقوم بتدمير الملفات بشكل كامل ومن الممكن استعادتها وهذا الأمر مهم جداً لأن المتهم أو المجرم يقوم بحذف الملفات التي تثبت تورطه.

فهم عملية استعادة الملفات المحذوفة هو أمر مهم جداً في عملية التحليل الجنائي الرقمي، لهذا يعتمد المحققون في تحليله على مجموعة من الأدوات المتطورة مثل EnCase أوFTK ، التي تسمح بإجراء ما يسمى بالـ "نسخ الجنائي (Forensic Imaging) "لضمان عدم تغيير البيانات الأصلية.

[1] جميل حسين طويل، المرجع السابق، ص 67.

ثانيا: الهاتف المحمول

الهاتف الذكي هو وسيلة شخصية بامتياز كونه يحتوي على معلومات حساسة وخاصة جدا بالنسبة لصاحبه فهي تشمل الرسائل، الصور، المكالمات، وتطبيقات التواصل الاجتماعي وهو من بين الأجهزة التي تساعد كثيرا عمل المحققين في فك شفرة الجرائم المعلوماتية انطلاقا من استخدام مجموعة من البرامج المطورة الت يتملكها الجهات الخاصة والتي من خلالها يتم استخراج البيانات باستخدام أدوات متقدمة مثل Cellebrite أو .XRY

أجهزة الموبايل أصبحت موجودة في كل مكان وهي مستخدمة بشكل كبير في عمليات الاتصال وتصفح الانترنت وفي العديد من الجرائم المعلوماتية يمكن أن نجد الدليل الرقمي في جهاز الموبايل كما أن أجهزة الموبايل يمكن أن تحوي على أدلة للجرائم العادية الغير معلوماتية) لذلك من المهم فهم طريقة عمل هذه الأجهزة وأنظمة التشغيل الخاصة. [1]

فالشريحة هي أهم جزء في أي جهاز موبايل وهي التي تحدد الرقم الخاص بالمستخدم وتحوي أيضاً عن معلومات خاصة بالشبكة وتحوي أيضاً على كلمتين سر وهما: PUK PIN

1- أماكن وجود الدليل الرقمي:

أجهزة الموبايل يمكن أن تحوي على أدلة لكل من الجرائم المعلوماتية وغير المعلوماتية وهذه الأدلة يمكن أن توجد في الأماكن التالية:

سجلات الرسائل والمكالمات: معرفة الجهات التي يتواصل معها المشتبه به هو أمر مهم في أي عملية تحليل جنائي.

الصور ومقاطع الفيديو الصور ومقاطع الفيديو يمكن أن تكون دليل رقمي ضد المتهم.

سجلات GPS هذه الخدمة غير مدعومة في سوريا.

التطبيقات: معرفة التطبيقات الموجودة في الجهاز هو أمر مهم في عملية التحليل الجنائي الرقمي، يجب إحصاء وتحليل كل السجلات الخاصة بتطبيقات المحادثة والتواصل الاجتماعي وتصفح الانترنت.

[1] جميل حسين طويل، المرجع السابق، ص 67.

2- التحليل الجنائي المعلوماتي لأجهزة الموبايل:

خلال عملية التحليل الجنائي الرقمي يجب أن نقوم بتحديد الأمور التالية:

معلومات عن نوع وحالة الجهاز.

- تاريخ المكالمات والرسائل.
- جمع الصور ومقاطع الفيديو.
- معلوماتGPS
- معلومات عن اتصالات الشبكة.
- معلومات عن التطبيقات.
- سجلات المحادثة وتاريخ تصفح الانترنت.
- المعلومات عن نوع الهاتف هي أول أمر يجب أن يقوم المحقق الجنائي الرقمي بتوثيقه
- في التقرير (رقم الهاتف ونوع الجهاز والرقم التسلسلي للجهاز ونوع وإصدار نظام التشغيل).

سجل المكالمات يجب أن يتم فحصه وبشكل دقيق وتحديد الجهات التي يقوم المتهم بالاتصال معهم بشكل دوري ومعرفة تاريخ ومدة كل مكالمة.

البحث في ذاكرة الجهاز وكرت الذاكرة عن الصور ومقاطع الفيديو أو أي ملفات أخرى يمكن أن تكون متعلقة بالجريمة وهذه الملفات قد تكون أدلة هامة في الجرائم المعلوماتية والغير معلوماتية.

فحص اتصالات الشبكة ومعرفة الشبكات اللاسلكية التي تم الاتصال بها هو أمر مهم جداً ومن خلال هذه الشبكات يمكن معرفة الأماكن التي تواجد فيها المتهم وجد اسم شبكة يخص مقهى أو فندق معين)

بعض الجرائم المعلوماتية مثل إرسال البريد الواغل spam أو هجمات منع الخدمة أو حتى اختراق المواقع أو المنظومات المعلوماتية يمكن أن تتم باستخدام جهاز الموبايل.

ولخصوصية الهاتف النقال بالنشبة للأفراد نجد ان التشريع الجزائري، كما في التشريعات الوطنية والقوانين المقارنة، شرط الحصول على إذن قضائي قبل استخراج البيانات الخاصة كما يجب ضمان

احترام الحياة الخاصة طبقًا لأحكام الدستور (المادة 46) وقانون الإجراءات الجزائية الذي ينص على وجوب وجود إذن مسبق في حالات التفتيش والمراقبة التقنية للأجهزة[1].

ثالثا: تحليل شبكة الويب

معظم الجرائم المعلوماتية تتم باستخدام الشبكة وعبر الانترنت. حيث ان الفيروسات وبرمجيات التجسس Spyware وأحصنة طروادة Trojan Horse تنتشر عادة عبر الشبكة وهجمات منع الخدمة DoS (Denial of Service) تتم أيضاً باستخدام الشبكة وعبر الانترنت لذلك فإن التحليل الجنائي الرقمي للشبكة هو أمر مهم جداً.

أثناء عملية التحليل الجنائي للشبكة سوف تتعامل مع أجهزةrouters

الموجه router يمكن أن يكون عرضة للعديد من الهجمات ومنها تزوير جدول التوجيه routing tabe poisoningوالذي يسمح للمهاجم بالوصول لكامل البيانات في الشبكة الهدف. [2]

في الجرائم المعلوماتية التي تتم عبر الشبكة فإن البيانات التي يرسلها المهاجم سوف تمر من خلال أجهزة routers ومن المهم عدم إيقاف تشغيل الموجه قبل أو أثناء عملية التحليل الجنائي الرقمي للحفاظ على الدليل الرقمي داخله.

يمكننا استخدام أداة للاتصال والتفاعل مع الموجه عن بعد مثل الأداة Hyper Terminal

تحليل استخدام شبكة الإنترنت يشمل تتبع سجل التصفح، الملفات المؤقتة، عمليات التحميل، وسجلات الاتصال بالخوادم. ويمكن للمحقق الوصول لهذه البيانات من خلال أجهزة التوجيه أو المتصفح.

حيث أن في التشريع الجزائري تستغل هذه المعلومات بموجب أوامر قضائية في إطار التحري في الجرائم الإلكترونية، وهذا الاجراء استنادًا إلى قانون 09-04، الذي يتيح مراقبة الاتصال بالإنترنت في حالة الجرائم الخطيرة كالإرهاب، الاحتيال الإلكتروني، أو المساس بأنظمة المعالجة الآلية للبيانات[3].

---

[1] خالد بوعافية، الجرائم السيبرانية والتحقيق الرقمي، الجزائر: دار خليف، ، 2020، ص 120.

[2] جميل حسين طويل، المرجع السابق، ص 123.

[3] القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالوقاية من الجرائم المعلوماتية ومكافحتها.

العديد من الجرائم المعلوماتية تتم من خلال اختراق مخدمات ومواقع الويب وهذه الهجمات هي الأكثر انتشاراً في الفترة الحالية.

الهجوم على موقع الويب يمكن أن يتم من خلال إحدى الطرق التالية:

استهداف المخدم المخدم هو جهاز بمواصفات عالية يقوم باستضافة موقع أو عدد من مواقع الويب المهاجم يحاول استهداف المخدم من خلال البحث عن ثغرات محتملة في نظام التشغيل الخاص بالمخدم أو ثغرات في البرامج التي تعمل على المخدم ومحاولة استغلالها ومن ثم الوصول إلى الملفات الخاصة بالموقع والتعديل عليها أو تخريبها.

استهداف موقع الويب مواقع الويب يمكن أن تحوي على ثغرات برمجية والتي يمكن للمهاجم استغلالها وتعديل أو تخريب محتوى الموقع وأشهر هذه الثغرات هي SQL injection and XSS

استهداف المستخدم: ويتم ذلك باستخدام الهندسة الاجتماعية كمحاولة لخداع مدير الموقع أو مستخدمي الموقع من أجل الحصول على معلومات تسجيل الدخول الخاصة بهم.

الفرع الثاني: بالنسبة لتحليل الملفات

التحليل الجنائي الرقمي للملفات هو عملية فحص وتحليل الأدلة الرقمية الموجودة في الملفات، سواء كانت محذوفة أو موجودة، بهدف استخراج معلومات ذات صلة بجريمة أو حادثة معينة .يهدف التحليل الجنائي الرقمي إلى تحديد الأدلة، وفهم كيفية حدوث الجريمة، وتحديد الجناة، وتقديم نتائج التحليل كدليل في الإجراءات القانونية

أولا : تحليل الملفات المخفية والمشفرة

يوجد العديد من التقنيات الى يستخدمها المجرمين لإخفاء البيانات التي تثبت تورطهم في الجريمة المعلوماتية وهذه التقنيات تسمى Antiforensics وهي:

التشفير Cryptography

الستيغنوغرافي Steganography

إخفاء البيانات داخل الصور أو داخل ملفات أخرى)

تزوير السجلات Log tampering

تقنيات أخرى تغيير عنوان (IP)

بالتأكيد فإن المجرم سوف يحاول إخفاء البيانات التي تثبت تورطه في جريمة معلوماتية من خلال تشفير الملفات والصور أو إخفاء الملفات داخل ملفات أخرى (steganography) أو محاولة حذف أو التلاعب بالسجلات logs

بعض المجرمين ينجحون بمسح أو إخفاء الأدلة الرقمية التي تثبت تورطهم وكمحقق جنائي رقمي من الضروري أن تكون على معرفة بهذه الطرق وكيفية التعامل معها.

لذا تُستخدم برامج تحليل متخصصة لكشف الملفات المخفية أو المشفرة، كـ VeraCrypt أو Autopsy، وتلجأ الفرق الفنية إلى كسر التشفير أو محاولة استرداد كلمات المرور. وينبغي احترام مبدأ الشرعية الإجرائية في الجزائر أثناء عمليات الكسر وفك التشفير، مع ضرورة إثبات تقنية العمل في محضر رسمي.

يوجد أكثر من طريقة لتحليل واكتشاف المعلومات السرية المخبلة داخل الملفات ومنها تحليل زوج من الألوان المتقاربة في صورة معينة لاكتشاف إذا تم استبدال bits الأقل أهمية LSB ويتم ذلك باستخدام تقنية RQP (Raw Quick Pair والتي تعتمد على مبدأ زوج الألوان المتقاربة بالاعتماد على احصائيات خاصة بعدد من الألوان الفريدة.

الستيغنوغرافي مهمة جداً في عمليات التحليل الجنائي الرقمي لأن هذه الطريقة مستخدمة من قبل الجماعات الإرهابية لتبادل الرسائل السرية.

بعد مقتل أسامة بن لادن ومن خلال تحليل الأقراص الصلبة التي كانت موجودة في منزله اكتشفت القوات الاميركية أنه كان يتصل مع عناصر تنظيم القاعدة من خلال إخفاء الرسائل السرية داخل صور إباحية. [1]

تحليل الشيفرات السرية

تحليل الشيفرات السرية أمر معقد وصعب جداً وليس كما يبدو في الأفلام. حيث تتم هذه العملية من خلال محاولة فك تشفير الرسائل المشفرة باستخدام تقنية القوة الغاشمة brute force (تجربة عدد

[1] جميل حسين طويل، المرجع السابق، ص 90.

كبير جداً من القيم وبشكل أتوماتيكي على أمل أن تكون إحدى هذه القيم هي القيمة الصحيحة) وهذه الطريقة لا تنفع مع خوارزميات التشفير الحديثة.

التلاعب بالسجلات: بالإضافة لطرق تشفير وإخفاء المعلومات السابقة فإن المجرم يحاول أيضاً إخفاء العمليات التي قام بها من خلال التلاعب في السجلات logs من خلال محاولة حذف مدخلات هذه السجلات وهذا الأمر صعب ولكن من الممكن القيام به في كل من windows and linux بعد الحصول على أعلى مستوى صلاحيات في النظام.

ثانيا: تحليل البرامج الخبيثة

البرمجيات الخبيثة: هي برامج يتم تضمينها أو إدراجها في أنظمة الحاسب دون علم أو رضا المالك لأغراض تهدف إلى إلحاق الضرر بهذه الأنظمة.

وتتعدد درجات الضرر بحسب درجة خطورة هذه البرمجيات كالوصول غير المشروع والتجسس وجمع المعلومات وعرقلة العمليات وتوفير الظروف للمهاجمين للقيام بعمليات اختراق أوسع، علماً بأن بعض أنواع البرمجيات الخبيثة يستطيع تكرار نفسه والانتشار بعدد من الطرق.

عملية تحليل البرمجية الخبيثة تتضمن دراسة وفهم كيفية عمل هذه البرمجية كمحاولة لكشف من قام بخلق هذه البرمجية أو كشف الهدف من نشرها واستخدامها.

عند تحليل برمجية خبيثة معينة إذا وجدنا أن هذه البرمجية تقوم بمحاولة اتصال عكسي مع عنوان ١٤ معين من خلال هذا العنوان يمكن أن تحدد هوية الشخص الذي قام بخلق أو استخدام هذه البرمجية.

يشمل تحديد ما إذا كان الجهاز قد تم اختراقه عبر برمجيات ضارة (Malware) يمكنها التجسس أو تعديل البيانات. يعتمد التحليل على أدوات مثل IDA Pro وWireshark، ويتطلب خبرة عالية. في الجزائر، يُمكن اعتبار هذا النوع من التحليل دليلاً على وقوع جريمة معلوماتية وفقًا لقانون 09-04، لاسيما في حالة الاعتداء على سرية البيانات.

ثالثا: تحليل سجلات النظام

سجلات النظام Registry مسؤولة عن كل شيء في نظام windows وهي تحوي على كل الإعدادات والملفات التي تم فتحها ومعلومات الشبكة والبرامج وأمور أخرى.

وهي مبنية بشكل هرمي ومكونة من خمس أفرع أساسية و تحوي على معلومات مهمة جدا في عملية التحليل الجنائي الرقمي.

شركة Microsoft عرفت سجلات النظام كالتالي: قاعدة بيانات مركزية تستخدم من قبل أنظمة التشغيل الخاصة بشركة Microsoft ويتم فيها تخزين كل المعلومات الضرورية لإعدادات النظام والمستخدمين والبرامج والأجهزة وهي تحوي على معلومات خاصة بكل مستخدم والبرامج التي قام بتنصيبها على النظام والملفات والمستندات التي قام بفتحها والأجهزة المتصلة والمنافذ ports المستخدمة في اتصالات الشبكة.

سجلات النظام (Logs) توفر معلومات دقيقة عن نشاط المستخدم والجهاز، مثل تواريخ الدخول والخروج، والبرامج المشغّلة، والأخطاء. تحليلها يساعد على تتبع الخط الزمني للحدث. في الجزائر، تُستخدم هذه السجلات في التحقيقات لتدعيم باقي الأدلة الرقمية، ويجب أن تتم عملية التحليل وفقًا للقواعد الجنائية الإجرائية، مع ضمان توثيق الخطوات الفنية المتبعة.

المبحث الثاني: الجوانب الإجرائية للحصول على الدليل الرقمي

تكتسي اجراءات جمع الادلة الرقمية أهمية بالغة في ظل التطور التكنولوجي المتسارع ، حيث يشكل الدليل الرقمي عنصرا محوريا في اثبات الجرائم المعلوماتية، و العصب الرئيسي للتحقيقات القضائية المعاصرة .

المطلب الاول: من حيث الخطوات الإجرائية للحصول على الدليل الرقمي

الحصول على الدليل الرقمي من العمليات ذات الحساسية القانونية والتقنية العالية، وهذا نظرًا لما يحيط به من تعقيدات تتعلق بسرعة زواله، وسهولة التلاعب به، وتشعب مصادره ما بين أجهزة إلكترونية، وشبكات، وسُحب رقمية. لذلك، لا يمكن للسلطات الضبطية أو القضائية أن تتعامل معه تعاملاً عشوائيًا، بل يجب أن تلتزم بسلسلة من الخطوات الإجرائية المحكمة التي تضمن قانونية عملية الضبط، وصحة إجراءات الحجز، وسلامة التحليل، وتوثيق كامل مراحل التعامل مع هذا النوع من الأدلة.

من هنا، يأتي هذا المطلب لبيان أهم الخطوات الإجرائية المعتمدة قانونًا في سبيل جمع الدليل الرقمي بطريقة مشروعة في التشريع الجزائري من خلال تقسيم الى الإجراءات التقليدية في الحصول على الدليل الرقمي (الفرع الاول) ثم الى الإجراءات الحديثة في الحصول على الدليل الرقمي في (الفرع الثاني)

الفرع الأول : الإجراءات التقليدية في الحصول على الدليل الرقمي

تنقسم الإجراءات التقليدية المعتمدة في جمع الدليل الرقمي إلى ثلاث مراحل أساسية هي :**المعاينة، التفتيش، والضبط** .ورغم طابعها الكلاسيكي في مجال التحقيق الجنائي، فإنها تخضع لتكييفات دقيقة عند التعامل مع البيئة الرقمية، نظرًا لما تتسم به من خصوصية تقنية وحساسية قانونية.

أولًا :إجراء المعاينة في البيئة الرقمية

يقصد بالمعاينة: " رؤية المكان أو الشخص المشتبه فيه أو أي شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة"[1] فهي تعد من أولى الخطوات التي يُباشر بها في سياق جمع الأدلة وتهدف

[1] أشرف قنديل عبد القادر، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة الإسكندرية، 2015، ص 134.

إلى **إثبات حالة الأشياء أو الأشخاص أو الأماكن المرتبطة بالفعل الجرمي** في لحظة معينة، في البيئة الرقمية، لا تنصب المعاينة على الأشياء المادية التقليدية فقط، بل تشمل **الأنظمة المعلوماتية والأجهزة الإلكترونية والبيانات المُخزّنة.** حيث تتم المعاينة التقنية في البيئة الرقمية من خلال انتقال ضباط الشرطة القضائية إلى محل الدليل الرقمي والي يوجد مكانه في جهاز الحاسب الآلي وتحديدا تلك البيانات الرقمية في ذاكرة الجهاز[1] وذلك **لمعاينة بنية الجهاز، طبيعة برامجه، البيانات المعروضة على الشاشة، أو أي مؤشرات على ارتكاب الجريمة،** مثل تشغيل برامج مشبوهة أو تخزين محتويات غير مشروعة.

ولخصوصية الطابع الفني للمعاينة الرقمية، غالبًا ما تُجرى هذه الخطوة **بحضور خبير تقني مختص في الإعلام الآلي،** يُساعد في فحص الأنظمة وتقدير مدى الحاجة إلى التفتيش أو الضبط اللاحق، مع الالتزام بحدود ما تسمح به المعاينة دون الولوج الكامل إلى المحتوى إلا بإذن قضائي.

ثانيًا :التفتيش في البيئة الرقمية

يعد إجراء التفتيش من إجراءات التحقيق التي تهدف إلى البحث عن الحقيقة في مستودع السر، تبرز الغاية من هذا الإجراء هو الوصول إلى الأدلة التي تساهم بشكل كبير في إظهار الحقيقة وكشفها، حيث يعرف التفتيش في البيئة الرقمية بأنه:" إجراء يسمح باستخدام الوسائل الالكترونية لجمع الأدلة المخزنة أو المسجلة بشكل الكتروني [2]" وهذا ويشمل محل التفتيش في البيئة الرقمية الحاسوب الآلي والمزود الآلي للخدمة والملحقات التقنية. [3]

ويشمل محل التفتيش في هذا السياق كل من :**وحدات الحوسبة (الحاسوب، المخدم)، وسائط التخزين) أقراص، (USB، الحسابات السحابية، قواعد البيانات، والملحقات التقنية المرتبطة بها.**

حيث يتطلب هذا النوع من التفتيش: الحصول على **إذن قضائي مسبب ومحدد،** يبيّن طبيعة الجهاز أو الحساب المستهدف ومبررات الشك مع العمل على تحديد **نطاق التفتيش الزمني والمكاني والمنطقي،** لأن البيئة الرقمية قد تحتوي على بيانات شخصية لا علاقة لها بمسار القضية.

[1] عائشة بن قارة، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر 2010، ص 86.

[2] علي عدنان الفيل، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، دار الكتب والوثائق القومية العراق، 2012، ص 39

[3] أشرف قنديل عبد القادر، المرجع السابق، ص 136.

وتتم عملية تنفيذ التفتيش باستخدام **برمجيات احترافية** مثلEnCase :، FTKتضمن استخراج البيانات دون التلاعب بها أو تعديلها. وفي الأخير إعداد **محضر تقني** يوضح مراحل التفتيش، والمعطيات التي تم العثور عليها، وسلسلة الحفظ الرقمية.

ثالثًا :إجراء الضبط في البيئة الرقمية

يقع الضبط في البيئة الرقمية على أشياء ذات طبيعة معنوية كالبيانات، المراسلات والاتصالات الالكترونية، كما أثارت مسألة ضبط هذه الأخيرة جدلا فقهيا واسعا واختلافا تشريعيا حول مدى إمكانية ضبط البيانات الإلكترونية[1]

فالضبط هو الإجراء الذي يعقب إجراءات المعاينة والتفتيش، ويهدف في الغالب إلى **مصادرة الأشياء محل الجريمة أو المتعلقة بها، وحفظها كأدلة**، وفي البيئة الرقمية، لا يكون الضبط ماديا دائما، وإنما **يمس محتويات رقمية ذات طبيعة معنوية**، مثل الملفات النصية الصور، المراسلات الإلكترونية، سجلات الدخول، أو حتى الشيفرات البرمجية، وتُثير مسألة ضبط هذه المحتويات إشكاليات عدة، منها **إمكانية نسخها أو نقلها** دون ترك أثر واضح. أو **تعقيد إثبات أصالتها** ما لم تُحفظ بوسائل تقنية مثل البصمة الرقمية.(Hash value) ، وفي ذات السياق **الخصوصية الرقمية**، خاصة عند ضبط محتويات حسابات شخصية أو بيانات مشفرة.

وقد اختلفت التشريعات في ضبط البيانات الرقمية بين من **يشترط أن يُنجز على نسخ دون الأصل** حمايةً لخصوصية المتهم، وبين من يُجيز ضبط الأصل إن دعت الضرورة، على أن يُنسخ ويُؤمن فورًا بمعايير دقيقة توثق **سلسلة الحفظ(chain of custody)** ، ويجب أن يتم الضبط وفق محضر مفصل يتضمن تحديد هوية الأجهزة أو الملفات المضبوطة. وتوقيت الضبط ومكانه. وأهم الوسائل المستخدمة لحفظ البيانات وتوثيقها وامضاءات الأطراف الحاضرين من محققين وشهود وخبراء إن وُجدوا.

الفرع الثاني : الإجراءات الحديثة في الحصول على الدليل الرقمي

واكبت التشريعات الإجرائية الجزائية المقارنة تطور التقنيات التكنولوجية، فلجأت إلى إجراءات حديثة في سبيل الحصول على الدليل الرقمي، وباعتبار البيانات في البيئة الإلكترونية ذات طبيعة ديناميكية

[1] عائشة بن قارة، المرجع السابق، ص 114.

وحركية فائقة، فكان ولابد من ملائمة ذلك، يبرز هذا من خلال اللجوء إلى التحفظ المعجل على البيانات المخزنة واعتراض الاتصالات الإلكترونية فهذا هذين الإجراءين يعدان إجراءين حديثين في الحصول على الدليل الرقمي، سيتم التعرض إلى هذين الإجراءين في مايلي:

أولا: التحفظ المعجل على البيانات المخزنة

يُعد إجراء التحفظ المعجّل على البيانات المخزنة أحد أبرز الآليات المستحدثة في مجال مكافحة الجريمة المعلوماتية، وهو يطبق على البيانات التي سبق تجميعها واحتُفِظ بها من قِبل حائزي البيانات، وعلى رأسهم مقدمو خدمات الإنترنت والاتصالات. وتكمن أهمية هذا الإجراء في كونه أداة فعالة للتنقيب عن الأدلة الرقمية، خاصة في ظل الطبيعة المتقلبة للبيانات المعلوماتية، والتي تتسم بسهولة تغييرها أو حذفها، مما يجعلها عرضة للضياع أو التلاعب، وبالتالي فقدانها لقيمتها الإثباتية أمام جهات التحقيق والقضاء[1].

وبالنظر إلى خصوصية هذا النوع من الأدلة، فإن التأخر في اتخاذ إجراءات قانونية لجمعها قد يؤدي إلى إهدارها، الأمر الذي استدعى ضرورة وجود إجراء تحفظي سريع يضمن الحفاظ على هذه البيانات إلى حين اتخاذ التدابير الإجرائية المناسبة كإجراء التفتيش أو الأمر بالحصول على نسخ من البيانات أو تقديمها من طرف الجهات الحائزة لها.

وفي هذا السياق، يُعرف إجراء التحفظ المعجّل بأنه: "قيام السلطة المختصة بتوجيه أمر إلى مزوّدي الخدمات أو الأشخاص الحائزين للبيانات، يُلزمهم فيه بالتحفظ على بيانات معلوماتية مخزنة تحت سيطرتهم، وذلك بصورة مؤقتة، إلى حين استكمال الإجراءات القانونية ذات الصلة مثل التفتيش أو الحصول على البيانات بصفة رسمية". ويُشكل هذا الإجراء في حد ذاته خطوة تمهيدية مهمة نحو ضمان الحفاظ على سلامة الدليل الرقمي ومصداقيته، دون أن يُعد في ذاته إجراءً كافيًا للإثبات ما لم يُستكمل بالإجراءات القضائية اللاحقة[2].

[1] وردة شرف الدين الأحكام الإجرائية لمكافحة جريمة الاتجار بالأشخاص المرتكبة بواسطة تقنية المعلومات، مجلة الاجتهاد القضائي، مخبر أثر الاجتهاد القضائي على حركة التشريع ، كلية الحقوق و العلوم السياسية ، جامعة محمد خيضر بسكرة ، العدد السادس عشر، مارس 2018، ص 101

[2] أشرف قنديل عبد القادر، المرجع السابق، ص 180

ثانيا: اعتراض الاتصالات الالكترونية

يُعد اعتراض الاتصالات الإلكترونية من الوسائل الأساسية التي تعتمدها السلطات المختصة في سبيل جمع الأدلة الرقمية، لاسيما عندما يتعلق الأمر بالجرائم التي تتم عبر الوسائط الإلكترونية. وتكتسي هذه الوسيلة أهمية خاصة في ظل اعتماد المجرمين المعاصرين على وسائل الاتصال الرقمية لتنفيذ مخططاتهم الإجرامية وتبادل المعلومات فيما بينهم.

وتُصنَّف الاتصالات الإلكترونية المخزنة ضمن فئة البيانات الساكنة، أي تلك التي لا تكون قيد التداول الفوري، وإنما جرى حفظها في وسائط إلكترونية وتخزينها لدى مزودي الخدمات، مثل البريد الإلكتروني غير المفتوح أو الرسائل الصوتية المحتفظ بها دون الاطلاع عليها من طرف المرسل إليه. وتشكل هذه البيانات، رغم سكونها الظاهري، مصدرًا ثمينًا للمعلومات التي قد تحمل مؤشرات قوية على وقوع نشاط إجرامي أو تُسهم في تحديد هوية مرتكبيه[1].

أما من حيث طبيعتها التقنية، فإن البيانات محل الاعتراض لا تقتصر فقط على مضمون الرسائل، بل تشمل أيضًا ما يُعرف بـ بيانات المرور، وهي البيانات التي تُعالج أثناء مرور الاتصالات عبر الأنظمة المعلوماتية، وتشير إلى معلومات تقنية تتعلق بمصدر الاتصال، وجهته، وتوقيته، وحجمه، ومساره داخل البنية التحتية الإلكترونية. ويُعتبر نظام المعلومات عنصراً محورياً في هذه العملية، إذ يمثل الوسيط الذي تمر عبره هذه البيانات ويُعالجها، وهو ما يجعله هدفًا محوريًا في عمليات الاعتراض التي تتم بإذن من الجهات القضائية المختصة.

وعليه، فإن اعتراض الاتصالات الإلكترونية يمثل أداة فعالة للحصول على الدليل الرقمي، مع ضرورة التقيّد بالضوابط القانونية والإجرائية التي تحكم هذا النوع من التدخل في الخصوصيات، حفاظًا على التوازن بين مقتضيات العدالة الجنائية وحقوق الأفراد[2].

[1] محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، دار الحامد للنشر و التوزيع، الأردن، 2014، ص 236 .

[2] نور الهدى محمودي حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة 1، العدد الحادي عشر، جوان 2017، ص 911.

اللمطلب الثاني: من حيث التعامل مع الدليل الرقمي إجرائيا

يُعدّ التعامل مع الدليل الرقمي إجرائيًا مرحلة دقيقة تلي عملية الحصول عليه، وتشمل الحفظ، التوثيق، التقديم للمحكمة، والطعن فيه. في الجزائر، لا توجد نصوص تفصيلية كثيرة في هذا المجال، لكن يُعتمد على القواعد العامة في الإثبات الجنائي وعلى ما جاء في قانون الإجراءات الجزائية[1].

أولًا، يجب حفظ الدليل في بيئة آمنة تمنع تعديله أو فقدانه، مع تسجيل كل العمليات التي أجريت عليه منذ الحجز. ويجب على الخبراء والمحققين إعداد تقرير فني مفصل يتضمن وصف الجهاز، البيانات المستخرجة، البرامج المستخدمة، وأي ملاحظات تقنية. هذا التقرير يُرفق بملف الدعوى ويُعتمد عليه في التقييم القضائي للدليل.

ثانيًا، أثناء المحاكمة، يمكن للطرفين (الدفاع والنيابة) مناقشة محتوى الدليل الرقمي والطعن في مشروعيته أو في دقة التحليل الفني. في هذا السياق، يمكن للمحكمة أن تأمر بخبرة مضادة للتثبت من صحة النتائج.

ثالثًا، يجب أن يكون التعامل مع الدليل الرقمي متوافقًا مع مبادئ المحاكمة العادلة، لاسيما مبدأ المواجهة وحق الدفاع، وتُراعى المعايير الدولية مثل اتفاقية بودابست حول الجرائم السيبرانية، التي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 17-175[2].

حفظ الدليل هو أمر مهم جداً ويجب أن تتم عملية الحفظ في بيئة آمنة لا يمكن الوصول إليها من قبل أشخاص غير مصرح لهم ومن المهم أن تكون معزولة عن الحقول الكهرومغناطيسية.

ويجب أن يكون مكان الحفظ محمي من الحرائق وبعيد عن أنابيب المياه وأن يكون المكان مغلق ومقفول ويمنع أي شخص غير مصرح له من الاقتراب من هذا المكان كما يجب أن يكون مكان حفظ الدليل مراقب بشكل دائم.

[1] بوخاتم سليمان، الإثبات بالوسائل الإلكترونية في المادة الجزائية، مذكرة ماستر، جامعة الجزائر 1، 2020، ص 52.

[2] الاتفاقية الدولية لمكافحة الجريمة الإلكترونية (بودابست)، 2001.

خلاصة الفصل الثاني

يتضح من خلال هذا الفصل أن التعامل مع الدليل الرقمي في الجزائر ما يزال في طور التأسيس والتطوير، رغم إدراج بعض الآليات القانونية والتنظيمية التي تؤطره. فنيًا، تلعب الأجهزة الأمنية المتخصصة والخبراء المعتمدون دورًا جوهريًا في تحليل البيانات الرقمية، سواء كانت مخزنة في الأقراص الصلبة أو الهواتف أو ضمن شبكة الويب. كما أن تحليل الملفات المشفّرة وسجلات النظام يتطلب كفاءات تقنية دقيقة، واستعمال أدوات متطورة لضمان استخلاص الأدلة بطريقة تحفظ سلامتها وأصالتها.

أما إجرائيًا، فقد أقر المشرّع الجزائري مجموعة من الضمانات القانونية التي تضبط عمليات الحجز، التفتيش، والتحليل الرقمي، مع ضرورة الحصول على إذن قضائي مسبق ومراعاة مبادئ المحاكمة العادلة. وتُعتبر مواد قانون الإجراءات الجزائية ذات الصلة بالدليل الرقمي (65 مكرر وما يليها) الإطار القانوني الرئيسي لضمان مشروعية هذا النوع من الأدلة.

غير أن الممارسة العملية تكشف عن وجود تحديات حقيقية، منها ضعف التكوين التقني لبعض الجهات المختصة، ونقص التجهيزات الفنية الحديثة، إضافة إلى غياب إطار تشريعي مفصل يُنظم خصوصيات الأدلة الرقمية مقارنة بما هو معمول به في بعض الأنظمة المقارنة. وبالتالي، يبقى من الضروري تعزيز البنية التشريعية والفنية لمواكبة تطور الجريمة الرقمية وضمان فعالية الإثبات الجنائي .

الـــخاتـــمة

إن ما شهدته البشرية من تطورات تقنية هائلة خلال العقود الأخيرة، قد أحدث تحولًا جذريًا في مختلف نواحي الحياة، ومنها المجال الأمني والجنائي، حيث باتت الجرائم التقليدية تتراجع أمام ظهور جرائم إلكترونية متجددة ومتطورة، تستغل ثغرات التكنولوجيا الرقمية ووسائل الاتصال الحديثة لتحقيق أغراض إجرامية متنوّعة.

وقد جاءت هذه الدراسة لتسلط الضوء على "التحليل الجنائي الرقمي" كأحد الركائز الأساسية في مكافحة الجريمة الإلكترونية، التي أصبحت تشكل تهديدًا حقيقيًا للأمن الفردي والمؤسساتي، وللأمن الوطني بشكل عام. ومن خلال تناول الإطار المفاهيمي للجريمة الإلكترونية ومفهوم التحليل الجنائي الرقمي، استطعنا إبراز الفروق الجوهرية بين الجرائم التقليدية والجرائم الإلكترونية، وما يتطلبه كل منها من أدوات وتقنيات تحقيق مختلفة.

كما تطرقت الدراسة إلى الجوانب الفنية والإجرائية التي تحكم التعامل مع الأدلة الرقمية، مشددة على أن نجاح أي تحقيق جنائي رقمي يرتبط ارتباطًا وثيقًا بمدى التزام الجهات المختصة بالضوابط الفنية والإجرائية لضمان سلامة الأدلة وقانونية جمعها، ومن ثم قبولها أمام القضاء. وهذا يبرز أهمية التكوين المستمر للخبراء التقنيين والقضاة وكافة العاملين في منظومة العدالة، لتمكينهم من التعامل مع الأدلة الرقمية المتطورة والمعقدة.

من الناحية التشريعية، كشفت الدراسة عن وجود فجوة واضحة في التشريع الجزائري فيما يتعلق بالتنظيم القانوني الشامل للتحليل الجنائي الرقمي، رغم وجود بعض النصوص الجزئية التي تناولت جوانب معينة من الجرائم الإلكترونية. وهذا يشكل عقبة أساسية أمام فاعلية مكافحة هذه الجرائم، حيث إن غياب إطار قانوني متكامل يعيق قدرة السلطات القضائية والأمنية على استغلال التقنيات الحديثة بشكل فعال وموثوق، ويضعف الحماية القانونية للحقوق والحريات الأساسية في الفضاء الرقمي.

بناءً على ذلك، تبدو الحاجة ملحّة إلى تطوير المنظومة القانونية لتشمل تشريعات متخصصة تعالج الجوانب التقنية والأخلاقية للتحليل الجنائي الرقمي، وتوضح الضمانات القانونية لحقوق الأفراد، مع وضع قواعد واضحة لجمع الأدلة الرقمية، وحفظها، وتحليلها، واستخدامها في المحاكم.

علاوة على ذلك، يتطلب التقدم في هذا المجال توفير بنية تحتية تقنية حديثة، وتدريب متخصص للعاملين في الميدان القضائي والأمني، مع تشجيع البحث العلمي والدراسات التطبيقية التي تسهم في تطوير أدوات التحليل الجنائي الرقمي بما يتناسب مع التحديات المتجددة.

وفي ضوء هذه المعطيات، فإن الدراسة لا تكتفي بتقديم وصف وتحليل للواقع الحالي، بل تسعى أيضًا إلى إلقاء الضوء على أهمية التعاون بين الجهات المختلفة (القضائية، الأمنية، التقنية، التشريعية) لبناء منظومة متكاملة، قادرة على مجابهة الجرائم الإلكترونية بفعالية، وضمان حماية المجتمع من المخاطر الرقمية.

وأخيرًا، يُمكن القول إن التحليل الجنائي الرقمي يمثل مستقبل التحقيقات الجنائية، وهو ميدان يفتح آفاقًا واسعة للبحث العلمي والتقني والقانوني، ويُعد عنصرًا حيويًا في تعزيز سيادة القانون وحماية الحقوق في عصر الرقمنة. لذا تبقى الدراسة دعوة مستمرة لتطوير المعرفة والمهارات التشريعية والفنية، بهدف بناء منظومة عدالة رقمية رصينة، قادرة على مواكبة سرعة التغيرات التقنية وحماية المجتمع من تهديدات الجريمة المعلوماتية

أهم النتائج التي توصلت اليها الدراسة

- اظهرت اغلب الدراسات ان الجرائم المعلوماتية تشهد تطورا متسارعا في الاساليب والتقنيات مما جعلها تهديدا حقيقيا للأمن الفردي و المؤسسات
- اصبحث الجرائم المعلوماتية أكثر تعقيدا بسبب استخدام تقنيات متطورة مثل الذكاء الاصطناعي والتشفير
- تبين ان الادلة الرقمية لها دورا محوريا في كشف ملابسات الجرائم المعلوماتية ، شرط ان يتم جمعها وتحليلها وفق معايير قانونية وعلمية دقيقة
- صعوبة ملاحقة مجرمي الانترنات بسبب طبيعة هذا النوع من الجرائم الذي يختلف عن الجريمة التقليدية
- هناك قصور في بعض الانظمة القانونية في مواكبة التطورات التقنية، مما يعكس مدى صعوبة مكافحتها
- يظهر التحليل ان ان الجريمة المعلوماتية تفرض تحديا مضاعفا تقنيا في الكشف عنها، وقانونيا في إثباتها عبر الدليل الرقمي
- التحليل الجنائي المعلوماتي من المجالات الناشئة نسبيا

الإقترحات لتعزيز التحليل الجنائي المعلوماتي في الجزائر

- تطوير التشريعات الوطنية والدولية وتوحيدها لمواكبة مستجدات الجرائم المعلوماتيةلضمان حجية هذه الادلة أمام المحاكم
- إنشاء برامج أكاديمية وتدريبية متخصصة في الجامعات مثل كلية الهندسة المعلوماتية أو مراكز التدريب التابعة للأمن الوطني
- التعاون مع دول رائدة (مثل الولايات المتحدة) لنقل الخبرات.
- مواءمة القوانين مع المعايير الدولية (مثل اتفاقية "بودابست" للجرائم الإلكترونية
- تبسيط إجراءات جمع الأدلة الرقمية وتقديمها في المحاكم.
- توفير أدوات متطورة للتحليل الجنائي مثل "EnCase"، "FTK"، أوCellebrite " لفك تشفير الهواتف.
- إنشاء مختبرات وطنية معتمدة للفحص الرقمي.
- حملات توعوية حول الأمن السيبراني للمواطنين والشركات.
- تشجيع الإبلاغ عن الجرائم المعلوماتية عبر قنوات مخصصة.
- الانضمام إلى شبكات مكافحة الجرائم المعلوماتية العالمية.
- مشاركة البيانات حول التهديدات الإلكترونية مع دول الجوار

قائمة المصادر والمراجع

أولا – المصادر

القوانين و الأوامر و المراسيم

1- القانون رقم 06-24 مؤرخ في 28 ابريل 2024، يعدل ويتمم الأمر رقم 66-156 و المتضمن قانون العقوبات، ج ر 30 مؤرخة في 30 ابريل 2024.

2- القانون رقم **01-09** مؤرخ في 04 ربيع الثاني عام 1422 الموافق لـ 26 يونيو 2001، يعدل ويتمم الأمر رقم 156-66 المؤرخ في 18 صفر 1386 الموافق لـ 08 جوان 1966 والمتضمن قانون العقوبات. الجريدة الرسمية العدد 34 لسنة 2001.

3- القانون رقم **04-15** المؤرخ في 27 رمضان 1425الموافق لـ 10 نوفمبر 2004 .المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.الجريدة الرسمية العدد 71 لسنة 2004.

4- القانون رقم **09-04** مؤرخ في 14شعبان عام 1430الموافق 5غشت سنة ،2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها. الجريدة الرسمية العدد 47 لسنة 2009.

5-القانون **15-04** المحد للقواعد الخاصة المتعلقة بالتوقيع و التصديق الالكترونيين الصادرة بتاريخ 01 فبراير 2005 جريدة رسمية عدد06

6- الأمر رقم **21-11** المؤرخ في 25 أوت 2021، يتمم الامر رقم 66-155 المؤرخ في 08 جويلية 1966 والمتضمن قانون الاجراءات الجزائية

ثانيا – المراجع

I. المراجع باللغة العربية

أ- الكتب

1- الأسدس لينا محمد، ، **مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية،** الاردن (عمان): دار حامد للنشر والتوزيع، 2016

2- الطوالبة علي حسن، **الجرائم الالكترونية**، البحرين: مؤسسة فخراوي للدراسات والنشر،2008.

3- النعمان سعيد، **الجريمة المعلوماتية: مفاهيمها وأشكالها القانونية**، عمّان: دار الثقافة للنشر والتوزيع، 2015.

4- الصغير جميل عبد الباقي ، **الانترنت والقانون الجنائي**، مصر (القاهرة): دار النهضة العربية، 2001

5- الشوابكة محمد الامين ، **جرائم الحاسوب والانترنت (الجرائم المعلوماتية)**، ط 4، الاردن: عمان: دار الثقافة للنشر والتوزيع، 2001.

6- الفيل علي عدنان ، **إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية**، العراق: دار الكتب والوثائق القومية، 2012

7- الغثبر خالد بن سلمان، **سليمان عبد العزيز الهيشة، الاصطياد الالكتروني الاساليب و الاجراءات المضادة**، المملكة العربية السعودية الرياض، مركز التميز لامن المعلومات، 2009

8- الصيني عمار على ، **التحقيق الجنائي والوسائل الحديثة في كشف الجريمة**،لبنان: منشورات الحلبي الحقوقية، 2015.

9- الحسني الفاروق ، **أصول علم الإجرام وعلم العقاب**، مصر(القاهرة): دار النهضة العربية،2002

10- الجهيني منير محمد ، الجهيني منير ممدوح ، **جرائم الانترنت والحاسب الآلي و وسائل مكافحته**، مصر(الاسكندرية): دار الفكر.

11- باطلي غنية، **الجريمة الإلكترونية دراسة مقارنة**، الجزائر: الدار الجزائرية للنشر والتوزيع

12-بيومي حجازي عبد الفتاح ، **الجرائم الإلكترونية وأدلة الإثبات الرقمية**، دار الفكر الجامعي،.2018 .

13- بن قارة عائشة ، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر 2010.

14- بن يونس عمر محمد ، **الدليل الجنائي الرقمي وإجراءاته القانونية**، دار كنوز المعرفة، 2020.

15- بن زروقي فتيحة ، ***الجريمة المعلوماتية في القانون الجزائري والمقارن***، الجزائر: دار هومة، 2018 .

16- هروال نبيلة هبة ، **الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات**، مصر (الاسكندرية): دار الفكر الجامعي، 2022

17-رستم هشام محمد فريد، **قانون العقوبات ومخاطر تقنية المعلومات**. اسيوط: مكتبة الآلات الحديثة، 1992.

18- طويل جميل حسين ، **التحليل الجنائي الرقمي**، دليل عملي الطرق التحليل الجنائي الرقمي في الجرائم المعلوماتية، سوريا ، ب س.

19- مناصرة يوسف ، **الدليل الالكتروني في القانون الجزائي**، الجزائر: دار الخلدونية، 2018

20- موسى مصطفى محمد ، **إثبات الجرائم الإلكترونية بالدليل الرقمي**، المركز القومي،2021 .

21-ممدوح خالد ابراهيم، **فن التحقيق الجنائي في الجرائم الالكترونية**، مصر (الاسكندرية): دار الفكر الجامعي، 2018.

22- شفيق عبد الكريم، **الجرائم المعلوماتية: دراسة قانونية مقارنة**، مص (الإسكندرية): دار الفكر الجامعي، 2018.

23- شتا محمد، **فكرة الحماية الجنائية لرامج الحاسوب**. مصر (الإسكندرية): دار الجامعة الجديدة، 2001.

24- سويلم محمد علي، **الحماية الجنائية للمعاملات الإلكترونية (الجرائم المعلوماتية والإلكترونية)**. الإسكندرية: دار المطبوعات الجامعية،2018.

25-عبد الغني شيماء محمد عطاء الله، **الحماية الجنائية للتعاملات الإلكترونية** . مصر(الإسكندرية): دار الجامعة الجديدة،2007.

26- عميمر عبد القادر ، **التحديات القانونية لاثبات الجريمة المعلوماتية**، الجزائر(تلمسان): النشر الجامعي الجديد، 2021.

27-علالي عبد الله أحمد، **حجية المخرجات الكمبيوترية في المواد الجنائية** – دراسة مقارنة، 1999

28-قشقوش هدى حامد، **جرائم الحاسب الإلكتروني في التشريع المقارن**.مصر(القاهرة): دار النهضة العربية،1993.

29- قنديل أشرف عبد القادر، **الإثبات الجنائي في الجريمة الالكترونية**، مصر: الإسكندرية دار الجامعة الجديدة ، 2015.

ب- المقالات

1- الجملي طارق محمد ، **الدليل الرقمي في مجال الإثبات الجنائي**، مجلة الحقوق، المجلد 12، العدد،01، جوان 2015، جامعة البحرين عمادة الدراسات العليا والبحث العلمي.

2- بورابة صورية ، **التعاون الدولي في مكافحة الجرائم المعلوماتية**، مجلة القانون الدولي للدارسات البحثية، العدد 01 ،جامعة طاهري محمد، بشار،.2019

3- بن خليف عمر، "**الجرائم الإلكترونية في التشريع الجزائري**"، المجلة الجزائرية للعلوم القانونية، العدد 2، 2021.

4- بن يونس فريدة ، **الإطار الناظم لإختصاص الشرطة القضائية في مواجهة الجريمة المعلوماتية في التشريع الجزائري**، مجلة الاجتهاد القضائي المجلد 12 ، عدد خاص، 2020.

5- زردومي عبد الحكيم ، **الجرائم المعلوماتية في التشريع الجزائري**، الجزائر: دار هومة، 2018

6- شيخ سناء ، شيخ محمد زكريا، **مكافحة الجرائم الإلكترونية في القانون الجزائري**، مجلة وميض الفكر، جوان 2020.

7- شرف الدين وردة، **الأحكام الإجرائية لمكافحة جريمة الاتجار بالأشخاص المرتكبة بواسطة تقنية المعلومات**، مجلة الاجتهاد القضائي، مخبر أثر الاجتهاد القضائي على حركة التشريع ، كلية الحقوق و العلوم السياسية ، جامعة محمد خيضر بسكرة ، العدد السادس عشر، مارس 2018

8- محمد عمر مصطفى، **النتيجة وعناصر الجريمة**، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، العدد 532، 2005

9- محمودي نور الهدى، **حجية الدليل الرقمي في إثبات الجريمة المعلوماتية**، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة 1، العدد الحادي عشر، جوان 2017

10- زردومي عبد الحكيم ، **الجرائم المعلوماتية في التشريع الجزائري**، الجزائر: دار هومة، 2018

11- عثمان يس حسن محمد ، **الدليل الرقمي واثره على الدعوى الجنائية**، المجلد05، العدد03، سبتمبر 2020.

12- غريبي بشرى ، **خصوصية المجرم المعلوماتي ودوافعه**، مجلة نومبرس الاكاديمية، المجلد الثاني، العدد02، 2021.

ج - الدراسات غير المنشورة

ج – 1 أطروحات الدكتوراه

1- الشعار خالد علي نزال، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة الدكتوراة في الحقوق، كلية الحقوق – جامعة المنصورة، ب س.

2- براهيمي جمال ، **التحقيق الجنائي في الجرائم الإلكترونية**، اطروحة دكتوراه، كلية الحقوق و العلوم السياسية بجامعة مولود معمري ،تيزي وزو، 2018.

3- عبد المنعم محمد صلاح محمد ، **الجرائم الإلكترونية وتحدياتها** –دراسة مقارنة، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، 2005

ج-2 رسائل الماجستر

4- بحر عبد الرحمان محمد، **معوقات التحقيق في جرائم النترنات:دراسة مسحية على ضباط الشرطة في دولة البحرين**، رسالة ماجستير غير منشورة، اكاديمية نايف للعلوم الامنية، الرياض،1420

5- سعيداني نعيم، **أليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري**، رسالة ماجستير في العلوم القانونية، كلية الحقوق و العلوم السياسية ، جامعة الحاج لخضر باتنة، 2013-2012

ج -3- مذكرات الماستر

6- بوخاتم سليمان، **الإثبات بالوسائل الإلكترونية في المادة الجزائية**، مذكرة ماستر، جامعة الجزائر 1، 2020

7- عدلي دحمان، سعد الدين ثامر البشير، **التحقيق الجنائي في الجرائم الالكترونية**، مذكرة ضمن متطلبات نيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، قسم الحقوق، جامعة زيان عاشور – الجلفة، 2020-2021

د - الندوات والملتقيات

1- اليوسف عبدالله عبد العزيز ، **التقنية والجرائم المستحدثة**، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية،..1420

2- بغدادي ايمان ، **أثر تعديل قانون العقوبات الج ازئري في التصدي للجريمة الإلكترونية** ،مجلة افاق للبحوث و الدراسات محكمة دولية، العدد04، 2019.

هـ- المواقع الإلكترونية

1-المناوي محمد ، **حجية الدليل الإلكتروني في إثبات الجرائم المعلوماتية**، مجلة المنار، جامعة محمد الخامس بالرباط- كلية العلوم القانونية والاقتصادية والاجتماعية سلا،افريل 2020. على الموقع: revuealmanara.com

2-بونعارة ياسمينة: **الجريمة الإلكترونية** على الموقع :

-http://www.univ- emir.dz/download/madjalaoussoul/39bounara-yasmina.pdf

3- جلال فضل، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني، نشر بتاريخ 2025/02/12. في صفحة القضائية على الموقع الاتي::

https://alqadaeya-ye.net/?p=6068&utm_source=chatgpt.com

4 - عبد الرحمان مريم ، **مفهوم الجريمة السيبرانيةومراحلها التاريخية**، مجلة الحوار السياسية والثقافية، العدد(171،)جويلية 2020 ومتاح أيضا على موقع المجلة:

http://alhiwarmagazine.blogspot.com/2020/07/blog-post_10.html

5 – مقال متاح على موقع صفحة بوابة فيتو :**http ://www.vetogate.com/2424631**

نشر بتاريخ 2016/10/25، وتم الاطلاع عليه بتاريخ 2025/04/27،على الساعة 22:15 .

6– . التقرير التفسيري الاتفاقية بودابست الصادر خلال الدررة 109 عن لجنة اوزراء للمجلس الأروبي على الموقع التالي :http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm

II. المراجع باللغة الاجنبية:

1 Parker (D.B) ; **combattre la crime pénalité informatique** edition1985,p18.

2 P.CATALA, **Informatique et Droit Pénale ,** édition Cujas,Paris,P18 **et M**. chawky, essai sur notion de cybercriminalité ,iehel ; juillet,2006,p16, disponible sur : www.iehei.org.bibliotheque, cyber crime .pdf la date de consultation 05/03/2025

3 [1] Casey, Eoghan. **Digital Evidence and Computer Crime**: Forensic Science, Computers and the Internet. 3rd ed., Academic Press, 2011.

4 IOCE, Standards and Principles for Computer Evidence, October 2001.

فهرس المحتويات

فهرس المحتويات