جامعة اكلي محند اولحاج البويرة

كلية الحقوق والعلوم السياسة

قسم القانون العام

العقبات الإجرائية لإثبات الجريمة الإلكترونية

مذكرة لنيل شهادة الماستر في القانون

تخصص: القانون الجنائي والعلوم الجنائية

إعداد الطالبين:

زروقي ياسر

زبيشة سيدعلي

إشراف الأستاذة:

دراح سعاد

لجنة المناقشة:

الاستاذ(ة) :قتال حمزة.....رئيسا

الأستاذ(ة): دراح سعاد.....مشرفا و مقررا

الأستاذ(ة): مزهود حكيم.....ممتحنا

السنة الجامعية:2025-2026

شكر و عرفان

امتثالاً لقول رسول الله صلى الله عليه وسلم: «من لا يشكر الناس لا يشكر الله.»

كان لزاماً علينا تسجيل الشكر والاعتراف ونسبة الفضل لأصحابه، استجابةً:

عامةً نشكر كل من أعاننا، وساندنا، فمن كتم المعروف فقد شكر.

فالشكر أولاً وآخراً يعود على أن هذا السلوك طريق البحث والتشبه بأهل العلم، وإن كان بيننا وبينهم مفاوز.

كما نخص بالشكر أستاذنا الكريم ومعلمنا الفاضل المشرف على هذا البحث الأستاذ الدكتورة وراح سعاد ، جزاها الله خيراً، فما منحها إلا وافر العطاء وخالص الدعاء.

كما نشكر السادة الأساتذة المناقشين، وكل الزملاء، وكل من قدم لنا فائدة وأعاننا بمرجع.

نسأل الله أن يجزيكم عنا خيراً، وأن يجعل عملهم في ميزان حسناتكم.

اهداء

بسم الله مسبب الأسباب، وواهب الألباب، وخالق آدم وحواء من تراب

..، أما بعد

أهدي ثمرة عملي هذا إلى التي أفضّلها عن نفسي

فهي التي صنعت من أجلي والتي لم أرها يوماً ما تبخل جهداً

في سبيل إسعادي دائماً وأبداً، إلى أمي الحبيبة.

دائماً ما ننسى دروب الحياة،

ويضيع منا من يسيطر على أذهاننا في كل طريق نسلك

، فلم أرك تبخل عليّ بأي شيء طيلة حياتي، والدي أعتز به أطال الله في عمره.

الى جدتي الحنون :الجاحة الزهرة

إلى أخواتي الذين اشد بهم عضدي,واستمد منهم العون و القوة.

(مروة , نهال , احمد رامي)

وإلى جميع عائلتي , أصدقائي وزملائي في هذا العمل، إلى كل من علمني حرفاً.

لكم جميعاً من ساعدوني وكانوا دوماً بجانبي.

زروقي ياسر

إهداء

أهدي ثمرة نجاحي وجهدي في مسيرة دراستي ككل إلى روح أختي وحبيبتي وفقيدتي رحمة الله عليها

التي لولا الله عز وجل ثم هي وأمي الغالية لم أكن لأصل إلى هذه المواصيل.

إلى أمي العزيزة منبع كل شيئ التي رافقتني منذ بداية المسيرة وكانت مثل النور الذي ينير دربي أسال الله العظيم ذو العرش العظيم

أن يديمكي تاجا فوق رأسي ويحفظك لي وأن تكوني الشمعة التي تنير حياتي.

إلى أبي العزيز وإخواني الأعزاء أحبائي أدامكم الله سندا لي في هذه الحياة.

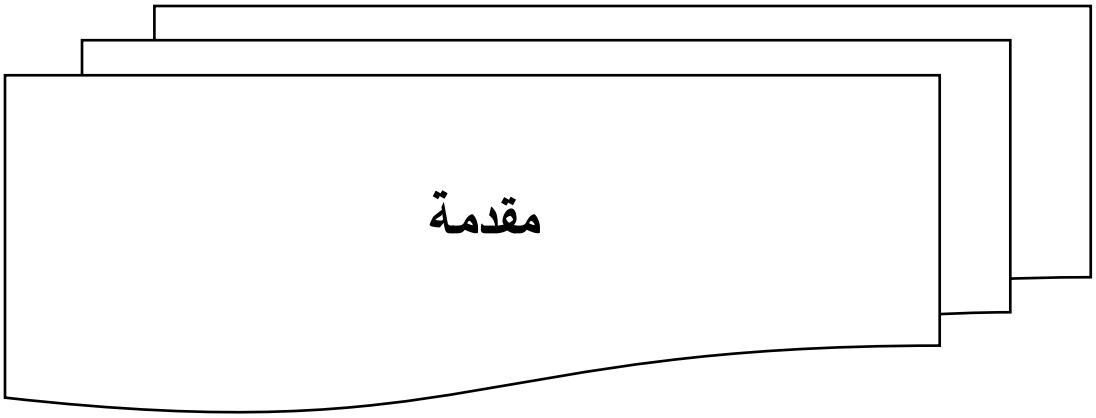
إلى أفراد عائلتي الكريمة أنتم النعمة التي رزقني بها الله عز وجل.

إلى كل من أحبهم قلبي ونسيهم قلمي.

إلى كل من كان لهم أثر على حياتي.

إلى كل من ساهم في مساعدتي.

زبيشة سيدعلي


مقدمة

تعد الجريمة المعلوماتية من الجرائم المعقدة و ذلك لارتباطها الوثيق بالتطور التكنولوجي الحاصل , في هذا العصر, فقد صاحب هذا التطور الذي مس مختلف جوانب الحياة جانب سلبي تمثل في استغلال هذا التطور في ظهور نوع جديد من الجرائم كرست مختلف التشريعات كافة الوسائل لمكافحتها و الوقاية منها , و قد كان تحديد الاطار القانوني المتكامل لمكافحة الجريمة المعلوماتية و الوقاية منها يثير الكثير من الاشكالات للقضاء و العديد من التحديات للمشرعين , و ذلك في ظل المفهوم التقليدي للجريمة التي كانت محصورة في عالم تقليدي مادي ملموس كان يسهل كثيرا التعامل القانوني معها . غير انه مع التطورات التكنولوجية التي جادت بها الثورة المعلوماتية التي شكلت عالما افتراضيا لا مادي و غير ملموس , تضاعف حجم الرهان الذي اضحى يطرح امام المشرعين في ايجاد حلول قانونية مستحدثة بامكانها مواجهة اساليب اجرامية تقنية و معلوماتية اضحت تطال النظم المعلوماتية و البيانات المخزنة فيها , الذي انتقل مع هذه الثروة من نطاق العالم المادي و التقليدي المحسوس الى عالم افتراضي معلوماتي و تقني ساعد كثيرا , خاصة في بدايته في تسهيل الاساليب و الاعتداءات الاجرامية التي اصبحت الانظمة المعلوماتية عرضة لها.

ذلك؛ لأن الجريمة في العام الافتراضي اتخذت مفاهيم و ابعاد جديدة ، او ضحت لها جوانب مستجدة لم تألف النصوص القانونية التي كانت تكرس الحماية القانونية لهذه الجريمة غير قادرة على تأطير حماية قانونية فعالة لها ، و بل اعجزها في الكثير من الاحيان ، خاصة و ان كل جوانب الحياة الخاصة للافراد اضحت عبارة عن نبضات الكترونية معالجة رقميا و بيانات تعالج و تنقل و تخزن عبر قنوات و نظم معلوماتية متطورة و متجددة بسرعة فائقة مقارنة مع النصوص القانونية التي في سنها و نشرها نوع من البطء المشهود، الامر الذي وضع المشرع في كل دول العالم امام فكرة بطأ المواجهة القانونية مقابل السرعة غير المألوفة التي تعرفها الاساليب و الطرق المعلوماتية التي اضحت طائفة المجرمين المعلوماتيين يسلكونها

ذلك كله؛ ما كان دافعا لنا لاختيار هذا الموضوع لاجل دراسة ابعاد تطور موضوع الجريمة في المجال المعلوماتي الذي كان تحول و تطور مفهوم الجريمة ذاتها، الذي اصبح يعرف بالجريمة المعلوماتية القائمة في عالم افتراضي مستحدث يقتضي الحماية القانونية مثلما كانت الحماية من الجريمة في مفهومها التقليدي

قام المشرع الجزائري و على غرار اغلب مشرعي دول العالم؛ و في ضوء بعض التجارب القانونية الدولية و الاقليمية و الوطنية، سيما التي اثبتت نجاحها؛ بمكافحة هذه الجريمة و الوقاية منها. حيث يعتبر الحق في الحماية من الجرائم المعلوماتية من الحقوق الاساسية التي يضمنها القانون. وتأكيدا لهذا المبدأ قام المشرع الجزائري باستحداث قانون خاص اضافة الى ما تضمنه قانون العقوبات، يتعلق اساسا بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها، و سعى من خلاله الى الموازنة بين حقوق و حريات الافراد في حرمة حياتهم الخاصة و حق الدولة في الاطلاع عليها حفاظا على المصلحة العامة

تتجلى اهمية هذه الدراسة في تبيان ما أن كانت التعديلات الدستوري و القانونية التي تبناها المشرع كافية لتعزيز آليات الوقاية من الجريمة المعلوماتية ، و التصدي للمخاطر التي باتت تهدد النظم المعلوماتية و البيانات المخزنة فيها ، و ذلك بعد أن حاولنا تحديد مفهوم عام للجريمة الجديدة التي جادت بها الثورة المعلوماتية، كما حاولنا قدر الإمكان بأن نجعل من دراستنا هذه اسهاما في نشر الوعي لدى الأفراد و تهريفهم بالخاطر المستجدة في مجال عالم معلوماتي متسارع في تطوراته في ظل ظهور نوع من الاجرام عرف بالإجرام المعلوماتية مع محاولة توجيه العاملين و المتعاملين و المستخدمين لحدود و ظوابط المعالجات الالية للمعطيات .

كانت اهمية الموضوع السابقة السبب الرئيسي في اختيارنا لدراسته، بالإضافة لكونه محل اهتمام كبير من قيل الاتفاقيات و الدساتير و التشريعات لدرجة انه أصبح من الصعب حصر و تحليل و مقارنة نصوص هذه الأخيرة . كما كان موضوعا لعديد من الدراسات القانونية التي من الصعب عدها و حصرها و التي كل منها تتناول جانب من الموضوع و في نطاق تشريع من التشريعات الحديثة، غير انه يبقى موضوعا حديثا في التشريع الجزائري الذي بدأ بالتصدي للموضوع منذ وقت قصير مقارنة بالتشريعات الأخرى يضاف لكل ما سبق، سبب اخر شخصي يكمل في اهتمامنا الكبير بالمجال المعلوماتي و بكل القوانين التي تأطره ، خاصة القوانين التي سنت لمواجهة الظاهرة الخطيرة المتمثلة في الاجرام الإلكتروني الخطير.

اما عن أهداف الدراسة فانصبت حول محاولة إيضاح مفهوم الجريمة في المجال المعلوماتي الذي دائما ما يثير اشكالات قانونية غير مألوفة كلما اقترن بموضوع من مواضيع القانونية التقليدية، و انه مع صدور قانون جزائري خاص يتعلق بهذا المفهوم الحديث و تأطير جوانبه و تكريس أساليب وقاية مختلفة له، كما حاولنا تحقيق العديد من الأهداف الأخرى المرتبطة بالهدف السابق، لعل اهمها –في نظرنا –إيضاح الإطار المفاهيمي للموضوع مع تبيان العقبات التي تواجه سلطات التحقيق في اثبات الجريمة المعلوماتية .

و من هذا المنطلق تكمن اشكالية **الدراسة في مدى تفاقم الاعتداء على الانظمة المعلوماتية و البيانات المخزنة فيه او مواصلة التحدي لمجارات التطور المستمر للوسائل التقنية التي يرتكب من خلالها السلوك الاجرامي؟**

لذا ؛ فإنه في محاولتنا لتبيان اهمية الموضوع و تحقيق الأهداف التي نصبو إليها من خلالها ، حاولنا الإجابة عن الإشكالية المحورية تتمثل في تحديد الإطار المفاهيمي للجريمة (الفصل الاول) و بيان عقبات اثبات الجريمة المعلوماتية التي واجهها المشرع (الفصل الثاني).

كل ذلك باتباع المنهج التحليلي كمنهج اساسي في هذه الدراسة، و ذلك من خلال تحليل النصوص و الآليات القانونية في مجال مكافحة الجريمة المعلوماتية . كما قمنا بالاستراحة بالمنهج التاريخي الذي مكننا من تبيان مراحل تطور مفهوم الجريمة لتصل لمرحلتها الحالية و اتخاذها الطابع المعلوماتي ، و هو المنهج الذي فرض علينا أن نستعين أيضا بالمنهج الوصفي الذي بدونه لا يمكننا وصف الظواهر التقنية و القانونية مع اعتمادنا على المنهج المقارن الذي مكننا من مقارنة بعض الآليات القانونية التي اعتمدها المشرع الجزائري في مكافحة الجريمة المعلوماتية و تعريفها مع ذلك المتبع في التشريع الفرنسي و بعض التشريعات العربية الأخرى.

الفصل الاول

الإطار المفاهيمي للجريمة المعلوماتية

الفصل الاول

الاطار المفاهيمي للجريمة المعلوماتية

ظهرت الجريمة المعلوماتية التي تعد من من الجرائم المستحدثة كردة فعل ناتج عن التطور السريع الحاصل في مجال المعلوماتية , و كذا تزايد انعدام او نقص الجانب الالي و شبكة الانترنت , فبالرغم من الانعكاسات الايجابية للثروة المعلوماتية على تحسين ظروف الحياة و تغييرها الى الافضل , الا ان هذا التطور صاحبه الاستعمال السيء لشبكة الانترنت و نظم الحاسب الالي . هذا الاستعمال السيء حمل في حياته سلبيات متمثلة في القيام بافعال غير مشروعة , و من خلال ذلك استطاع الجناة تطوير طرق الاجرام انتقالا من العالم الخارجي المادي الملموس الى بيئة رقمية تستعمل فيها فيها التقنية كوسيلة للقيام بالافعال المجرمة , و هذا ما ادى الى ظهور نوع جديد من الجرائم تتسم بخطورة كبيرة تعرف بالجرائم الالكترونية او الجرائم المعلوماتية , و اختلفت تسميتها فنجد ان المشرع الجزائري سماها في القانون المتضمن قانون العقوبات بالجرائم الماسة بالانظمة المعالجة الالية للمعطيات و اطلق عليها في القانون 09ٍ_04[1] الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال . و يعتبر ظهور هذا النوع من الجرائم كنتيجة حتمية للتطور العلمي التقني المستحدث الذي بدا بالانتشار على نطاق واسع حتى تجاوز حدود الدول , اذ اصبحت الجريمة المعلوماتية ظاهرة عالمية تهدد كيان المجتمعات نظرا لخطورتها و صعوبة اثباتها و استخلاص الدليل فيها من البيئة الرقمية .

[1] القانون 09_04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، مؤرخ في 14 شعبان 1430 الموافق ل 5 غشت سنة 2009.

سنتطرق في دراستنا لهذا الفصل الى ما هية الجريمة المعلوماتية (المبحث الاول) من حيث تعريفها و تبيان خصائصها و ذكر انواعها و الاركان الواجب توافرها لقيامها , كما سنقوم مفهوم الدليل الاكتروني و انواعه (المبحث الثاني).

المبحث الاول

ماهية الجريمة المعلوماتية

ادى تطور الانظمة المعلوماتية و اتباع حدود استعمالها الى حتمية بذل جهود من طرف الباحثين لمجاراة هذا التطور, و بما ان الانظمة المعلوماتية اصبحت وسيلة تساعد على ارتكاب الاجرام بل و اصبحت وسيلة عصرية لارتكابه ,مما دفع بمختلف التشريعات بذل جهود من اجل تحديد هذا النوع من الجرائم و الحد منها .وادى زيادة اهتمام الباحثين المختصين من ميادين مختلفة الى تنوع تعريفها و تسمياتها .

يعتبر تعدد مجالات استعمال الانظمة المعلوماتية عائقا امام اعطاء تعريف موحد للجريمة المعلوماتية وتحديد انواعها (المطلب الاول) و تبيان اركانها و خصائصها (المطلب الثاني) .

المطلب الأول

تعريف الجريمة المعلوماتية و انواعها

تباينت تعريفات الجريمة المعلوماتية بتباين مختلف المصطلحات التي اطلقت عليها , مما اكسب الموضوع اهمية دراسية كبيرة خاصة من الناحية القانونية , و التي يجد المشرع نفسة ملزما بتحديد مصطلح للجريمة يقتضي الوضوح .وهو مقتضى دستوري وجب مراعاته اثناء وضع القواعد القانونية التي تجرم الفعل حماية للافراد التي تخاطبهم هذه القواعد .

و سيتم التطرق في دراستنا لهذا المطلب الى تعريف الجريمة المعلوماتية (الفرع الاول) و الى انواعها (الفرع الثاني).

الفرع الاول : تعريف الجريمة المعلوماتية

يصعب تحديد تعريف شامل و موحد للجريمة المعلوماتية , و بالرغم من الاجتهادات الفقهية و القانونية الا انهم لم يتمكنوا من حصرها في تعريف واحد شامل , رغم توفر نصوص قانونية تتعلق بارتكاب هذا النوع من الجرائم ,واجتهادات فقهية سابقة اعطت اهمية للدراسة في هذا المجال وهذا ما يبين صعوبة تحديد تعريف دقيق لهذه الجريمة .

اولا : تعريف الفقه للجريمة الإلكترونية

ساهم الفقه بشكل كبير في محاولة تحديد تعريف دقيق للجريمة المعلوماتية , حيث سعى الفقهاء لايجاد تعريف دقيق لها و من ابرز التعريفات نجد ;

تعريف الفقيه ROSANBLATT " الذي عرف الجريمة على انها ,"نشاط غير مشروع موجه لاحدى عمليات النسخ او حذف او تغيير او الوصول الى المعلومات المخزنة داخل الحاسب ,او التي يتم تحويله عن طريقه " [1] .

و يعرفها الفقيه PARKER بانها " كل فعل مجرم يرتكب عمدا له صلة بالمعلومات تنشا عن خسارة تلحق بالمجني عليه او كسب يحققه الجاني "[2]

[1] سميرة معاشي، الجريمة المعلوماتية (دراسة تحليلة لمفهوم الجريمة المعلوماتية) مجلة الفكر، العدد 17، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، 2018 ص 402.

[2] علوي علي احمد الشارفي، الوجيز في جرائم تقنية المعلومات، الطبعة الاولى المركز الديمقراطي العربي للدراسات السياسية و الاستراتيجية و الاقتصادية، المانيا ،2024 ، ص 33.

نجد ايضا تعريف الاستاذ SOLARZ الذي اعتبرها انها " اي نمط من انماط الجريمة التي تقوم على مبدا الشرعية و نجدها مرتبطة بتقنية المعلوماتية[1] , او يقصد بها كل الجرائم المنصوص عليها في قانون العقوبات من الجرائم التقليدية ولكن يكون ارتكابها بواسطة تقنية المعلوماتية .

عرفت ايضا بانها الجريمة التي تلعب فيها برامج المعلوماتية وبيانات الكمبيوتر دورا رئيسيا , و رغم هذا الاختلاف الظاهر بين التعاريف الفقهية السابقة الا انهم يتفقون في عناصر جوهرية كالقصد الجنائي و استعمال التقنية و المساس بحق عمدي قانونا[2] .

ثانيا : التعريف القانوني للجريمة المعلوماتية

سار اغلب المشرعين في الانظمة المقارنة على عدم وضع تعريف قانوني للجريمة المعلوماتية , غير ان البعض فيهم قام بوضع تعاريف لنظام المعلومات .

ا_ تعريف الجريمة المعلوماتية في التشريع الجزائري :

اكتفى المشرع في قانون العقوبات الجزائري بذكر بعض الافعال المعاقب عليها في قسم خاص استحدثه المشرع سنة 2004 وسماه (بجرائم المساس بأنظمة المعالجة الالية للمعطيات) حيث اشارت المواد من 394 مكرر الى 394 مكرر 8 من هذا القسم الى صور الجريمة كالدخول او االبقاء عن طريق الغش حذف او تغيير معطيات المنظومة ,تخريب نظام التشغيل للمنظومة و غيرها من الصور التي وضعها المشرع دون اعطاء تعريف محدد للجريمة[3].

[1] سميرة معاشي، نفس المرجع، ص402.
[2] خالد شريف، الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال في التشريع الجزائري، مجلة البيان للدراسات القانونية، المجلد 10، العدد 01، جامعة محمد خيضر بسكرة ، 2025 ص 119 _ 140.
[3] الطاهر زحمي , الجرائم المعلوماتية في التشريع الجزائري و تدابير الوقاية منها , مجلة التشريع الاعلامي , المجلد 02 , العدد 01 , كلية العلوم و الاتصال , جامعة الجزائر 3 , 2023 , ص ص 05 _23 ً 07.

عرف المشرع الجزائري الجريمة المعلوماتية في القانون رقم 09-04 و المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال في المادة الثانية منه . بان الجريمة بمعناها الجديد جرائم المرتبطة بتكنولوجيا الاعلام و الاتصال هي جرائم المساس بانظمة المعالجة الالية للمعطيات او اي جريمة اخرى تركب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام الاتصالات الالكترونية[1].

وسع هذا التعريف من نطاق الجريمة لتنتقل من الاعتداءات على الانظمة الى الجرائم التقليدية التي ترتكب او يسهل ارتكابها بواسطة هذه التقنيات[2] .

ب_ تعريف الجريمة المعلوماتية في التشريعات الاخرى :

1_**التشريع الفرنسي** : عالج المشرع الفرنسي الجريمة المعلوماتية سابقا بذلك معظم تشريعات دول العالم . وذلك بقانون 78_17 المتعلق بتكنولوجيا المعلومات و الحريات سنة 1978 , الى غاية تعديل بقانون سنة 2023 هذا الاخير لم يضع تعريف للجريمة المعلوماتية بل اطلق عليها جرائم المساس بانظمة المعالجة الالية للمعطيات[3] و ذكر صورها كحذف البيانات و تعديلها و الهجمات على انظمة المعلومات .

2-**التشريع الاردني** : اكتفى المشرع الاردني في قانون المعاملات الالكترونية الاردني رقم 85 لسنة 2001 بتعريف االنظام المعلوماتي و الذي يعتبر عنصرا اساسيا لصور الجريمة

[1] انظر المادة 02 من القانون 09_04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال .
[2] خالد شريف , الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال في التشريع الجزائري , مرجع سابق ص125.
[3] كريمة رزاق بارة , الجريمة الالكترونية المتعلقة بالاشخاص وفقا للتشريع الفرنسي و التشريع الجزائري ,المجلة الجزائرية للحقوق و العلوم السياسية , المجلد 08, العدد 02 , المركز الجامعي عبد الحفيظ بوصوف , ميلة , 2024 , ص ص 452_470 ص 455.

الالكترونية . حيث عرفه بانه " النظام الالكتروني المستخدم لانشاء رسائل المعلومات او ارسالها او تخزينها او تسليمها او تجهيزها على اية وجه اخر[1] ".

الفرع الثاني : انواع الجريمة المعلوماتية :

تعتبر حداثة الجريمة المعلوماتية و تطورها باستمرار مع تطور التكنولوجيا عائقا امام تحديدها و الحد منها , فنجد ان اساليب ارتكابها تتطور بشكل مستمر مما يؤدي الى تنوع في ارتكاب هذه الجريمة , مما يؤدي الى صعوبة تحديد انواع هذه الاخيرة بدقة .

من خلال التعريف السابق للجريمة يتضح ان محل الجريمة يكون اما افراد سواء كانوا طبيعيين او معنويين و اما ان تكون معطيات او بيانات رقمية او حتى اجهزة الكترونية[2] .

اولا: حسب الافراد : يكون هذا القسم من الجرائم مستهدفا للافراد او هويتهم المعلوماتية بطرق غير مشروعة[3]. ونجد منها :

1_الارهاب الالكتروني : تفاقم هذا النوع من الجرائم اذ اصبح يشكل تهديدا حقيقيا على الدول , و ذلك من خلال سعي الجناة اى تخويف الناس و زعزعة استقرار الدول و احداث الفوضى و اضطرابات امنية , و يكون ذلك في صورة تعطيل المصالح الاساسية للافراد كالخدمات المالية و الصحية . بل وحتى الشبكات الحكومية و العسكرية[4]. و بالرغم من ان المشرع الجزائري لم

[1] ريمة بن عميروش , عن خصوصية الجريمة المعلوماتية , مدلة الفقه القانوني و السياسي ,المجلد 02,العدد02,جامعة محمد الصديق بن يحيى ,جيجل ,2020 ص ص 73_88 ص77 .

[2] نور الدين بن سولة , الجرائم الالكترونية في ضوء التشريع الجزائري , مجلة الحوار المتوسطي ,المجلد التاسع , العدد10, جامعة معسكر , 2018 , ص ص270_278 ص 271 .

[3] نور الدين بن سولة , المرجع نفسه , ص272 .

[4] حمد محمد الدوسري , انواع الجرائم الالكترونية و تحديات مكافحتها , مجلة المنار للدراسات و البحوث القانونية , كلية الحقوق و العلوم السياسية , جامعة يحيى فارس , المدية ,المجلد 09 , العدد01, كلية القانون , جامعة لوسيل , قطر , 2025 , ص ص 90 _111 , ص 97.

يقسم الجريمة المعلوماتية الى ان هذا النوع سعى للوقاية منه في القانون 09\04 في نص المادة 04 [1]منه التي نصت على

" يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 اعلاه في الحالات الاتية :

_ للوقاية من الافعال الموصوفة بجرائم الارهاب او التخريب او الجرائم الماسة بامن الدولة .

_ في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام او الدفاع الوطني او مؤسسات الدولة او الاقتصاد الوطني . ... "

2_ جرائم المحتوى : يستخدم مرتكبوا هذا النوع من الجرائم الانترنت لتهديد و ممارسة المضايقات على الافراد و المؤسسات , وذلك من خلال التنمر على الافراد او ابتزازهم و نشر معلومات خاطئة عليهم , او تشويه سمعتهم و كما يتضمن هذا النوع من الجرائم سرقة هوية الافراد و انتحال شخصيتهم على الانترنت . و قد يسبب ذلك اضرار نفسية او اجتماعية لضحايا هؤلاء[2] .

3_ الاحتيال الالكتروني : يقوم هذا النوع على خداع الافراد و المؤسسات من اجل الحصول على تفاصيل حسابات بنكية او ارقام ائتمان على سبيل المثال , و يعتمد هؤلاء على البريد الالكتروني و مواقع الانترنت المزيفة على انها مواقع بنوك رسمية او شركات كبرى كوسيلة للحصول على معلومات شخصية او مالية من اجل القيام باعمال غير قانونية [3] .

[1] المادة 04 من القانون 09_04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال , مؤرخ في 14 شعبان 1430 الموافق ل 5 غشت 2009 .

[2] حمد محمد الدوسري , انواع الجرائم الالكترونية و تحديات مكافحتها , مرجع سابق , ص 98.

[3] حمد محمد الدوسري , مرجع نفسه ص 98.

ثانيا : من حيث موضوع البيانات و المعطيات : يستهدف هذا النوع المكونات المادية للاجهزة و المكونات غير المادية المتمثلة في البيانات و المعططيات التي يتم حفضها داخل الاجهزة و الشبكات[1] و نجد منها :

1_ القرصنة الالكترونية : يهدف الجاني في هذا النوع من الجرائم للوصول الى البيانات المخزنة و التلاعب بها , و ذلك من خلال اختراق انظمة الكمبيوتر , وهذا يدخل ضمن صور الجرائم المنصوص عليها في القسم السابع مكرر عن قانون العقوبات الجزائري كجريمتي الدخول او البقاء عن طريق الغش , الحذف او تغيير معطيات المنظومة , ويهدف الجاني من خلال ارتكابه لهذه الافعال الى تحقيق فائدة عالية او تدمير سمعة او المساس بالامن المؤسساتي[2] .

2_ الفيروسات : تعد من اكثر الانشطة انتشارا في البيئة الرقمية لما تسببه من اضرار للاجهزة و الانظمة, حيث تهدف الى تعطيل البيانات و البرامج المخزنة و تدميرها مما يؤدي الى وقوع اضرار اقتصادية و مادية كبيرة , حيث تشكل هذه الفيروسات تهديدا يمس بالانظمة الامنية للدول وجب الحد منها, اذ ينتج عنها زيادة تكاليف الصيانة و اهدار الموارد و تدهور الانظمة التشغيلية [3].

[1] نور الدين بن سولة , مرجع سابق , ص 272.
[2] حمد محمد الدوسري , مرجع سابق , ص 97.
[3] حمد محمد الدوسري , المرجع والموضع نفسه , ص 97.

المطلب الثاني

اركان وخصائص الجريمة المعلوماتية

ساهم التطور التكنولوجي في انفجار معلوماتي كبير اثر بشكل كبير على مختلف جوانب حياة الانسان, كما واجهت اغلب التشريعات صعوبة كبيرة في التعامل مع الجرائم المرتبطة بالمجال المعلوماتي التي تكون الوسائل التقنية وسيلة رئيسية لارتكاب الجريمة .

و ما يميز الجريمة المعلوماتية عن باقي الجرائم انها جرائم مستحدثة و تختلف عن الجرائم التقليدية من حيث محلها و نتائجها و اسلوب ارتكابها . مما وضع اغلب مشرعي دول العالم امام حتمية تحديد هذه الجريمة و التعامل معها مع ما يميزها عن باقي الجرائم .

سنتطرق في دراستنا لهذا المطلب الى اركان الجريمة المعلوماتية (الفرع الاول) و ذكر ما يميزها من خصائص (الفؤع الثاني).

الفرع الاول : اركان الجريمة المعلوماتية :

تتمثل اركان الجريمة المعلوماتية في العناصر الواجب توافرها لقيام الجريمة , حيث تقترن بها فوجودها يعني قيام الجريمة و عدمها ينفيها و يبيحها . و تنقسم اركان الجريمة الى ثلاثة اركان بداية بالركن الشرعي و هو الاساس القانوني الذي يحوي الفعل او الامتناع الذي يجرمه هذا الاخير , ثم الركن المعنوي القائم على العلم و الارادة و ما يميز الجريمة المعلوماتية هو وجود نظام المعاجة الالية للمعطيات او وسيلة تقنية كركن خاص وجب تحققه للبحث في توافر اركان اية جريمة معلوماتية[1] .

[1] نبيل ونوغي , عبد الرؤوف زيوش , الجريمة المعلوماتية في التشريع الجزائري ,مجلة العلوم القانونية و الاجتماعية , المجلد الرابع , العدد الثالث , جامعة مولود معمري تيزي وزو , 2019 , ص ص 127_139 ص132 .

سنقوم في هذا الفرع بدراسة اركان جريمة جمع معطيات شخصية بطرق تدليسية او غير نزيهة او غير مشروعة .

_ اولا : الركن الشرعي : يعني اعتراف المشرع بوضع نص يجرم الفعل طبقا لمبدا الشرعية "لا جريمة و لا عقوبة الا بنص " و ذلك حماية لحقوق الافراد و حرياتهم من اي اعتداء قد يطالهم . فالركن الشرعي هو السند القانوني الذي يستند عليه لتوجيه الاتهامات و ادانة الفاعل .

يتمثل الاساس القانوني للجريمة سالفة الذكر في نص المادة 59 من القانون 18_07 [1] و التي نصت على انه يعاقب بالحبس من سنة واحدة الى ثلاث سنوات و بغرامة من 100 الف الى 300 الف دينار .كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية او غير نزيهة او غير مشروعة .

_ثانيا الركن المادي : يقوم الركن المادي للجريمة بتوافر عنصرين اساسيين:

أ_ السلوك الاجرامي : المتمثل في عملية جمع المعطيات شخصية باستعمال طرق تدليسية او غير نزيهة او غير مشروعة .

ب_ محل الجريمة : و هو ان يكون السلوك واقع على معطيات شخصية

يتمثل العنصر الاول في الالمام المسبق بالمعطيات الشخصية التي لا يسمح بجمعها او معالجتها , حيث تكون عملية جمعها خارج الحالات المسموح بها قانونا و ذلك دون ترخيص صريح من صاحب المعطيات , او ان يتم جمعها من طرف اشخاص غير المحددين قانونا[2] .

[1] انضر المادة 59 من القانون 18_07 يتعلق بحماية الاشخاص الذاتيين في مجال معالجة المعطيات ذات الطابع الشخصي , ج ر العدد 34 الصادر في 25 رمضان 1439 الموافق ل 10 يونيو .2018 .

[2] فريد روابح , جرائم الجمع غير المشروع للمعطيات الشخصية الرقمية في التشريع الجزائري , مجلة الحقوق و العلوم السياسية, جامعة خنشلة, المجلد 09 , العدد 01 ,جامعة محمد لمين دباغين سطيف , 2022 , ص ص 80 _100 , ص83 .

اما العنصر الثاني فالمعطيات الشخصية تمثل محل الجريمة و لكي يقوم ركنها المادي وجب ان تقوم المعالجة الالية على معطيات ذات الطابع الشخصي كعنوانه , اسمه , او رقم هاتفه . و معطيات اخرى من شانها انها تحدد هوية الشخص و قد اكدت ذلك لجنة المعلومات و الحريات الفرنسية CNIL بانها بيانات تجعل من الشخص قابلا للتحديد و قد تكون صفة او رقم او جملة.

يخضع اسقاط الواقعة و تكييف المعلومات ما اذا كانت تعبير عن المعطيات الشخصية الى السلطة التقديرية للقاضي[1] .

_ثالثا الركن المعنوي : يعرف بانه العلم بعدم مشروعية الفعل المجرم و اتجاه الارادة لارتكابه و هذا ما يقوم عليه الركن المعنوي عنصري العلم و الارادة.

فالاول هو ادراك السلوك غير المشروع الذي يسبق ارادته في ارتكابه , اما الارادة فتتمثل في رغبة الشخص في تحقيق السلوك الاجرامي , و قد تتخذ ارادته صور القصد الجنائي العام او الخاص.

فالقصد الجنائي العام :هو الغاية الفورية و المباشرة للسلوك الاجرامي و ينحصر في حدود تحقق الجريمة المعلوماتية .

و يعني بالقصد الجنائي الخاص : هو ما وجب توافره في بعض الجرائم التي اشترطها المشرع اضافة الى تحقق الاركان السابقة , فلا يكفي تحقق نتيجة الجريمة بل هو ابعد عن ذلك اي ان يكون للمجرم نوايا اخرى من وراء ارتكاب الجريمة [2].

[1] نعيم سعيداني , الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة), الطبعة الاولى , المؤسسة الحديثة للكتاب , لبنان , 2022 , ص 601 .

[2] نبيل ونوغي , زيوش عبد الرؤوف , الجريمة المعلوماتية في التشريع الجزائري , مرجع سابق , ص 136_137 .

يقوم الركن المعنوي للجريمة محل الدراسة بمجرد توفر القصد الجنائي العام , فهي تعد من الجرائم العمدية التي لا يشترط فيها قصدا خاص بل يكفي علم الجاني و ارادته لقيام الركن المعنوي , فبمجرد علم الجاني بان المعطيات التي يجمعها هي معطيات شخصية و ان جمعها يشكل فعل غير مشروع تتجه ارادته الي القيام بالفعل المجرم .

الفرع الثاني : خصائص الجريمة المعلوماتية :

تتميز الجريمة المعلوماتية بجملة من الخصائص ة التي يصعب على الدول من خلالها القيام بوضع اليات وقائية للحد منها و مكافحتها . حيث ان ارتباط هذه الخصائص بمميزات الاجهزة الالكترونية و البرامج التي يستخدمها و شبكة الانترنت و مختلف التطبيقات التي توظفها يزيد من صعوبة محاربة هذه الجريمة,[1] و ذلك ما جعل خصائصها تختلف عن الجريمة التقليدية نذكر منها :

أولا_ الجريمة المعلوماتية جريمة عابرة للحدود : تتصف الجريمة المعلوماتية بالطابع الدولي ذلك لعالمية استخدام شبكة الانترنت و التي اصبحت الوسيلة الاساسية لارتكاب هذه الجريمة يوسع من رقعة ارتكابها

كما انها لا تعترف بالمكان و الحدود فقد ترتكب الجريمة في دولة و تظهر نتائجها في دولة اخرى او عدة دول , و هذا ما يخلق مشاكل اخرى تتمثل في تحديد القانون الواجب تطبيقه و صعوبة اتخاذ اجراءات الملاحقة اللازمة خاصة عندما يخضع لمبدا المعاملة بالمثل بين الدول غير المتعاونة فيما بينها في هذا المجال[2].

[1] لامية طالة , الجريمة الالكترونية :بعد جديد لمفهوم الاجرام عبر منصات مواقع التواصل الاجتماعي , مجلة الرواق للدراسات الاجتماعية و الانسانية ,المجلد 06 , العدد 02 , جامعة الجزائر 03 , 2020 , ص ص62_91 , ص 74 .

[2] سعيد مسعود الكثيري , الجريمة الالكترونية في ضل اتفاقية بودابست :الاطار المفاهيمي و التصنيفي , مجلة البحوث القانونية و الاقتصادية , المجلد 09 , العدد 01 , جامعة ظفار عمان , 2026 . ص ص944 _965 , ص950 ,

ثانيا_ صعوبة اكتشاف الجريمة المعلوماتية : تعد هذه الجريمة من الجرائم الخفية و المتسترة , لانها تعتمد على القدرات الفنية في ارتكابها مما يجعل اكتشافها امرا صعبا , فالوسائل التي ترتكب بها كالفيروسات و سرقة البيانات الخاصة و اتلافها و التجسس و غيرها يصعب ترك اثار و الاحتفاظ بها ان وجدت , هذا ما يدفع الى وجوب استعمال وسائل تقنية و بذل مهارات فنية لاكتشافها و اثباتها , خاصة ان الجاني يستخدم وسائل و مهارات فنية تعتمد على التمويه في ارتكابها و التظليل لعدم معرفة مرتكبيها[1].

ثالثا_ قلة الابلاغ عن الجريمة المعلوماتية : نجد ان معظم الجرائم المعلوماتية تم اكتشافها بالصدفة , و ذلك راجع الى صعوبة اكتشاف المجني عليه, او حتى عدم اكتشافه لها و قد يرجع عدم التبليغ ايضا لخوفه عن نتائج التبليغ في بعض الجرائم كالتشهير خاصة و ان البيئة الرقمية تعتبر حيزا شخصيا بالدرجة الاولى , كما نجد احصائيات هذه الجريمة توحي بان عدد الحالات التي تم اكتشافها اقل بكثير من عدد وقوع هذه الجريمة[2], كما ان نسبة كبيرة من الجرائم التي تم اكتشافها لم يتم ذلك الا بعد مرور وقت زمني طويل مما ادى الى صعوبة استرجاع البيانات او تعويض الضحية بل حتى محاسبة الجاني[3].

رابعا_ وقوع الجريمة في بيئة المعالجة الالية للمعطيات : تمثل هذه الخاصية شرطا اساسيا واجب توفره لقيام اركان الجريمة المعلوماتية , كما نجد ان من خصائصها انها تقع في بيئة المعالجة الالية للمعطيات فاذا تخلف ذلك الشرط تتحول الجريمة من كونها جريمة معلوماتية الى جريمة تقليدية[4] . فلابد من الاستعانة بالحاسب الالي كوسيلة لارتكاب الجريمة , و ذلك

[1] محمد رحموني ,خصائص الجريمة الالكترونية و مجالات استحدامها ,مجلة الحقيقة , العدد 41 , جامعة احمد دراية , ادرار , 2018 , ص ص 432_451 , ص 441 .

[2] سعيد مسعود الكثيري , الجريمة الالكترونية في ضوء اتفاقية بودابست , مرجع سابق , ص 951 .

[3] حمد محمد الدوسري , انواع الجرائم الالكترونية و تحديات مكافحتها , مرجع سابق , ص 95 .

[4] ريمة بن عميروش , عن خصوصية الجريمة الالكترونية , مرجع سابق , ص 79 .

خلاف ما اذا كان هذا الاخير هو محل الاعتداء فيعتبر هذا الفعل جريمة تقليدية يتكفل بها قانون العقوبات كسابق الجرائم العادية قبل صدور قانون 04_15 سالف الذكر . فالمقصود من ذلك المساس بالكيان المعنوي للحاسب من حذف و تعديل بالمعلومات المخزنة فيه , و لا يدخل في هذا الاطار مكوناته المادية كسرقة الحاسوب او العبث به ففي هذه الحالة تعتبر جريمة تقليدية خارجة عن اطار المجال المعلوماتي .

المبحث الثاني

الدليل الرقمي

نظرا للتطور الذي يشهده مجتمعنا في العصر الحالي فإن الجرائم لم تعد تقتصر على الواقع المادي فقط صارت ترتكب في الفضاء الإكتروني الإفتراضي وتسمى بالجرائم الإلكترونية والتي تعد أخطر حتى من الجرائم العادية نظرا لصعوبة التحقيق والإثبات فيها ولذلك أصبح الدليل الرقمي أحد أبرز الاعمدة التي يعتمد عليها في إثبات الجرائم الإكترونية لإرتباطه إرتباطا وثيقا بها, وإنطلاقا من ذلك في هذا المبحث محل دراستنا سوف نتناول الدليل الرقمي ونقوم بتحديد المقصود به (المطلب الاول) ومن ثم تبيان أنواعه وخصائصه (المطلب الثاني).

المطلب الأول

مفهوم الدليل الرقمي

يعد الدليل الرقمي ركيزة من الركائز الأساسية التي تساهم في الإثبات ونظرا لأنه مصطلح مستحدث أو يمكننا القول أنه أداة إثبات مستحدثة سوف نتطرق إليه في مطلبنا هذا وذلك من خلال تعريفه في الفرع الأول وبعدها تبيان مميزاته في الفرع الثاني.

الفرع الأول: تعريف الدليل الرقمي

بما أن المشرع الجزائري لم يعرف الدليل الرقمي تعريفا صريحا في هذا الفرع سوف نتطرق إلى تعريف الدليل الرقمي لغويا وإصطلاحيا وقانونيا.

1. التعريف اللغوي:

الدليل لغة هو الْمُرْشِد، وَالْمُرْشِدُ: النَّاصِب، وَالذَّاكِرُ؛ وَمَا بِهِ الإِرْشَادُ[1].

والدليل هو المرشد إِلَى الْمَطْلُوب، يذكر وَيُرَاد بِهِ الدَّال، وَمِنْه: (يَا دَلِيل المتحيرين) أَي: هاديهم إِلَى مَا تَزُول بِهِ حيرتهم[2].

يقول إبن منظور: والدَّلِيل ما يُسْتَدَلُّ به، والدَّلِيل الدَّالُّ، وقد دَلَّه على الطريق، يَدُلُّه دَلالة ودِلالة ودُلولة، والدَّلِيل والدِّلِّيلى الذي يَدُلُّك، والجمع أَدِلَّة وأَدِلاَّء، والاسم الدِّلالة والدَّلالة بالكسر والفتح[3].

---

[1] أبو زكريا يحيى بن موسى الرهوني، تحفة المسؤول في شرح مختصر منتهى السول، الطبعة الأولى، دار البحوث للدراسات الإسلامية وإحياء التراث، دبي، الإمارات، 2002، ص 161.

[2] أيوب بن موسى الحسيني القريمي الكفوي، الكليات معجم في المصطلحات والفروق اللغوية، الطبعة الثانية، مؤسسة الرسالة للطباعة والنشر والتوزيع، بيروت، لبنان، 1998، ص 439.

[3] إبن منظور، لسان العرب، دار المعارف، القاهرة، 2016، ص 1414.

وقد جاء في القرأن الكريم قوله تعالى: ﴿ أَلَمْ تَرَ إِلَىٰ رَبِّكَ كَيْفَ مَدَّ الظِّلَّ وَلَوْ شَاءَ لَجَعَلَهُ سَاكِنًا ثُمَّ جَعَلْنَا الشَّمْسَ عَلَيْهِ دَلِيلًا﴾[1].

أما بالنسبة لكلمة الرقمي هي إسم منسوب للدليل (الدليل الرقمي) فالرقم من أصل "[رقم– رقما– ورقم] اي ان أصل الكلمة هو "رقم" وهي علامات الأعداد المعروفة١و٢و٣الخ[2]، فالرقمي صفة لكل ما تستخدم فيه الأرقام لتمثيل الأعداد أو البيانات أو الرموز[3].

2. التعريف الإصطلاحي:

تعددت وإختلفت تعريفات الدليل الرقمي التي جاء بها الفقهاء، فقد عرفه البعض على انه: «الدليل الذي يجد له أساساً في العالم الإفتراضي ويقود إلى الجريمة»، وكما عرفه البعض الاخر على انه: المعلومات المنطقية التي يتم الحصول عليها من خلال اجهزة الحاسب الألي وملحقاته وشبكات الإتصال، ويمكن إستخدامها لإثبات فعل معين او شيء ما او شخص له علاقة بجريمة[4].

وكذلك عرف بأنه الدليل المأخوذ من أجهزة الكمبيوتر، ويكون على شكل مجالات او نبضات مغناطيسية وكهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجيا المعلومات،

[1] أنظر الآية 45 من سورة الفرقان.

[2] زكية مهنى، الأدب الرقمي من النص إلى الوسيط، مجلة الاثر، العدد 26، جامعة عبد الرحمان ميرة بجاية (الجزائر)، سبتمبر، 2016، ص 21.

[3] زكية مهنى، المرجع نفسه، ص 22.

[4] مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، العدد 03، الجزء الثاني، اكتوبر، 2018، ص 193.

وهو مكون رقمي لتقديم معلومات في اشكال متنوعة مثل النصوص المكتوبة او الصور او الأصوات او الاشكال والرسوم، من اجل اعتماده أمام الأجهزة القانونية[1].

ومن جانب اخر عرفه الفريق العلمي العامل المعني بالأدلة الرقمية (SWGDE) على انه اي معلومة ذات قيمة إثباتية سواء تم تخزينها أو نقلها بصيغة رقمية[2].

اي من خلال التعريفات السابقة وتعريفات اخرى نستنتج بان اغلبها يعرف الدليل الرقمي على انه عبارة عن معلومات لها اشكال مختلفة تكون بصيغة رقمية تستخرج من الحاسب الالي أوأي جهاز رقمي او حتى شبكات الإتصال ولها اهمية من ناحية التحقيق او فيما يخص الإثبات في الجرائم المعلوماتية.

3. التعريف القانوني:

لم يحدد المشرع الجزائري تعريفا تشريعيا صريحا فيما يخص الدليل الرقمي شأنه شأن العديد من التشريعات، ولكنه اتاح إستخدامه كوسيلة اثبات في القانون 09-04 الذي يتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، في المقابل اتجهت بعض التشريعات الى النص صراحة على الدليل الرقمي وتعريفه، إما في قوانين خاصة بمكافحة الجرائم المعلوماتية او حتى قوانين اخرى.

ومن الأمثلة نذكر المشرع المصري الذي عرف الدليل الرقمي صراحة في المادة 1 من القانون رقم 175 لسنة 2018 (في شأن مكافحة جرائم تقنية المعلومات) بما يأتي: "أي معلومات

[1] احمد حمو، علاء عواد واخرون، الأدلة الالكترونية (الجوانب القانونية والتقنية)، دون طبعة، دون دار نشر، فلسطين، 2015، ص 11.

[2] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Third Edition, Published by Elsevier Inc, 2011, P07.

إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها ، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة"[1].

وكما عرفه قانون مكافحة جرائم تقنية المعلومات العماني بأنه كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات أيا كان شكله كالكتابة والصور والأصوات والرموز والإشارات[2].

الفرع الثاني: خصائص الدليل الرقمي

نظرا للطبيعة التقنية التي يتميز بها الدليل الرقمي عن باقي الادلة بما فيهم الادلة المادية مما يجعله يتصف بعدة خصائص لذلك في هذا الفرع سوف نتناول ابرز الخصائص وأهمها التي يمتاز بها الدليل الرقمي.

أولا_ الدليل الرقمي دليل علمي وتقني:

كما أشرنا سابقا أن الدليل الرقمي دليل ذو طبيعة تقنية، نظرا للبيئة الإفتراضية التي ينشأ فيها والتي تجعله ثمرة هذا التطور التكنولوجي للمعلومات، فبينما الأدلة المادية هي ادلة تقليدية بكونها ملموسة وترى بالعين المجردة الدليل الإلكتروني يكون ذو طبيعة الكترونية غير ملموسة، فا من أجل الوصول إلى المحتوى المتكون من بيانات ومعلومات التعامل معه يحتاج بطبيعة الحال إلى وسائل وانظمة غير تقليدية تتناسب مع طبيعته كما يحتاج ايضا مختصين وخبراء

[1] أنظر المادة 01 من القانون رقم 175 المؤرخ في 14 أوت 2018، يتعلق بمكافحة جرائم تقنية المعلومات، الجريدة الرسمية المصرية، العدد 32 مكرر(ج)، الصادر في 14 أوت 2018، دون ذكر الصفحة.

[2] أحمد محمد عمر، الدليل الرقمي وحجيته في الإثبات الجزائي، مجلة الدراسات الفقهية والقانونية، العدد الثالث، المعهد العالي للقضاء، سلطنة عمان، يناير، 2020، ص 133.

فنيين كل هذا من أجل إدراك و إستخراج هذه المعلومات ومن ثم تحويلها لمادة تكون قابلة للإطلاع من قبل المختصين[1].

ثانيا_ الدليل الرقمي دليل متنوع ومتطور:

الأدلة الرقمية متنوعة ومتطورة في نفس الوقت، فمن ناحية التنوع فهو يتخذ عدة أشكال وعدة هيئات وتستمد هذه الأدلة وجودها سواءا من اجهزة الحاسوب او حتى من شبكات الإتصال أو كذلك من فضاء الانترنت، ومن ابرزها يمكن ان نجد المرسالات عبر البريد الإلكتروني أو محتويات المواقع الإلكترونية كذلك النصوص والصور والمقاطع سواء كانت مقاطع فيديو مرئية او تسجيلات صوتية، يمكن ان تكون ايضا بيانات مستخدمي الشبكة او حتى ملفات الحاسب الألي[2]، وكل هذه الأدلة لها قيمة قانونية في الإثبات، وكل هذا التنوع في الأدلة إن دل فهو يدل على التطور المستمر سواء من ناحية الادلة نفسها أو من ناحية الأدوات المستعملة لإيجادها، فإن وجدت وسائل لتشويه هذا الدليل سوف توجد وسائل لمنع هذا التشوه والتعقيد مما يخلق تنافس تقني[3].

ثالثا_ الدليل الرقمي دليل يصعب التخلص منه:

على عكس الدلائل المادية التي يمكن محوها وإتلافها بكل سهولة الدليل الرقمي من اصعب الادلة فيما يتعلق سواء بالإتلاف او المحو أو حتى التخلص منها وهذه ميزة جوهرية يتميز بها

[1] درابلة العمري سليم، حجية الدليل الرقمي في الإثبات الجنائي، أطروحة مقدمة لنيل شهادة دكتوراه علوم، تخصص القانون الجنائي والعلوم الجنائية،كلية الحقوق، جامعة الجزائر 01، 2025/2024، ص 44-45.

[2] درابلة العمري سليم، المرجع نفسه، ص 50.

[3] درابلة العمري سليم، المرجع نفسه، ص 50.

عن الدلائل التقليدية، فالأدلة المادية على سبيل المثال كالأوراق او المستندات يمكن تمزيقها وحرقها، كذلك ايضا البصمات يمكن مسحها وإزالتها ولا يمكن ارجاعها الى حالتها السابقة[1]، أما الدليل الرقمي تقنيا يمكن إرجاع وإصلاح البيانات التي تم محوها(سواء حذفت بأوامر بسيطة مثل DELETE او FORMAT او حتى اوامر متقدمة) واتلافها،وذلك عن طريق برامج وادوات وأوامر مخصصة مهمتها استرجاع الأشياء المحذوفة مهما كانت هيئتها صور ملفات او حتى بيانات ومعلومات متلفة[2].

رابعا_ الدليل الرقمي دليل ثابت وقابل للنسخ:

يتميز الدليل الرقمي بالثبوت وانه يبقى مستمر مع مرور الزمن بمجرد إنشائه أو حفظه ويعود ذلك إلى القدرة على انتاج نسخ متعددة منه وحمايتها مما يسهل للمحققين القدرة على الوصول الى بيانات او معلومات التي تم التعامل معها سابقا واستعادتها[3]، في الأصل ان النسخة لا تعادل قوة الاصل في مجال الإثبات لكن ذلك لا ينطبق على الدليل الرقمي بالعكس النسخ تعتبر ميزة تحمي الدليل من الضياع او التعديل او الحذف او حتى التلف وانشاء عدة نسخ لا يغير من قيمتها بل تبقى لها نفس القيمة العلمية مثلها مثل الدليل الاصلي[4].

[1] امال بهنوس، الدليل الرقمي في الإجراءات الجنائية، المجلة الأكاديمية للبحث القانوني، العدد 02، جامعة وهران 2 محمد بن أحمد، وهران، الجزائر، 2017، ص 177.

[2] صهيب سهيل غازي زامل، البحث والتحري عن الدليل الإلكتروني في المسائل الجزائية، أطروحة للحصول على شهادة الدكتوراه، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة وهران 2، 2022/2021، ص 24.

[3] عبد الرزاق، محمد شوقي واخرون، الدليل الإسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية، دون طبعة، دار جامعة نايف للنشر، المملكة العربية السعودية، 2024، ص 16.

[4] مسعود بن حميد المعمري، مرجع سابق، ص 200-201.

خامسا _ الدليل الرقمي دليل عابر للحدود:

الدليل الرقمي دليل يمكن ان يعبر حدود جغرافية مهولة ودول في ظرف ثواني على عكس الدليل المادي الذي يمكن ان يقتصر على اقليم معين، مما يجعل ضبط أو تتبع هذه الأدلة

فيما يخص الجرائم الإلكترونية إلى الحاجة الماسة للخبرة الفنية والعلمية العالية والذكاء العالي[1]، فشساعة العالم لإفتراضي وسرعته عقدت عملية تعقب هذه الأدلة نظرا لسرعتها وإمكانية تخزين هذه البيانات والمعلومات في عدة دول[2]، بحيث تتعدد مصادر هذه الدلائل لتشمل عدة انواع منها نذكر نصوص ورموز وصور وفيديوهات كلها متداولة عبر منصات التواصل الإجتماعي و شبكات الإتصال المختلفة، والتي يمكن من خلالها استخلاص دلائل لإثبات إدانة أو براءة متهم أو متهمين وفق شروط معينة[3].

المطلب الثاني

أنواع الدليل الرقمي وأشكاله

بما أن الدليل الرقمي يعتبر من الادلة الحديثة المتشعبة نظرا لتعدد مصادره ففي هذا المطلب سوف نتناول انواع الدليل الرقمي في الفرع الأول أما في الفرع الثاني سوف نتطرق الى اشكاله

الفرع الأول: أنواع الدليل الرقمي:

يرى بعض الفقهاء بان الجريمة الإلكترونية هي الجرائم التي لها علاقة بالكمبيوتر والشبكة المعلوماتية أو ما يعرف باسم الويب والأنترنت، أما الأنترنت فهي الية نقل المعلومات عن

[1] احمد ابو زيد شحاته، دور الدليل الرقمي في تعزيز قناعة القاضي في الإثبات الجنائي، مجلة العلوم القانونية والإقتصادية، العدد الاول، يناير، 2024، ص 601-602.

[2] درابلة العمري سليم، مرجع سابق، ص 55.

[3] أحمد ابو زيد شحاته، المرجع نفسه، ص 601.

طريق البروتوكولات الخاصة بالاتصال السلكي واللاسلكي[1]، وانطلاقا من التعريف السابق فلقد قسم الفقهاء الدليل الرقمي الى اربعة انواع:

اولا: الدليل الرقمي المرتبط بالحاسوب وشبكاته:

ويقصد بها الأدلة الناتجة عن السلوك او الفعل الغير قانوني(الجرائم المعلوماتية) الذي يستهدف الحاسب الالي والشبكات التابعة له، سواء وقع ذلك السلوك على المكونات المادية او المعنوية او على قواعد البيانات الداخلية[2].

ثانيا: الادلة الرقمية المتعلقة بشبكة الانترنت:

ويقصد بها تلك الدلائل المستخلصة من الجرائم المعلوماتية التي ترتكب عبر شبكة الأنترنت العالمية والتي تقع على المحتوى الرقمي، ومن امثلة ذلك يمكن ان نذكر جرائم الإختراق الإلكتروني والجرائم المتعلقة ببطاقات الإئتمان من احتيال وسرقة معلومات[3].

ثالثا: الدليل الرقمي المتعلق ببروتوكولات تبادل المعلومات:

وهي تلك الدلائل الناتجة عن السلوكيات الإجرامية التي تقع على آليات انتقال البيانات بين مستخدمي الشبكة، ومن امثلة هذه السلوكيات الغير قانونية نذكر استخدام عناوين بروتوكول

[1] زياد بن محمد عادي العتيبي، دراسة استطالعية حول حجية ألأدلة الرقمية في إثبات الجرائم المعلوماتية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد التاسع والعشرون، جدة، المملكة العربية السعودية، اكتوبر، 2020، ص 18.

[2] زياد بن محمد عادي العتيبي، المرجع نفسه، ص 18.

[3] مسعود بن حميد المعمري، مرجع سابق، ص 202.

انترنت وهمية غير حقيقية (Ip Spoofing،Fake Ip Address)، أو الدخول إلى مواقع غير مسموح بالولوج لها[1].

رابعا: الدليل الرقمي المتعلق بالشبكة العالمية للمعلومات:

وهي الأدلة التي تنتج عن الجرائم التي يستخدم فيها الحاسب الالي او الانترنت كوسيلة من أجل إرتكاب هذه الجرائم ومن الأمثلة نذكر جرائم غسيل الأموال وجرائم تهريب المخدرات[2].

وهناك اتجاه فقهي اخر يقسم الدليل الرقمي الى نوعين رئيسيين:

أدلة اعدت لتكون وسيلة إثبات.

وأدلة لم تعد لتكون وسيلة إثبات.

1.أدلة اعدت لتكون وسيلة إثبات:

بحيث أن هذا النوع من الأدلة ينقسم الى قسمين رئيسيين:

القسم الأول الذي يكون اليا أي تلقائي، بحيث هي السجلات والبيانات التي يتم إنشائها وتخزينها عن طريق الأجهزة الألية سواء كانت الحاسب الالي أو أي جهاز رقمي اخر دون تدخل العنصر البشري في انشائها، ومن الأمثلة يمكن أن نذكر سجلات الهاتف وفواتير العمليات المصرفية الصدارة عن اجهزة الصراف الالي (ATM)[3]، اما بالنسبة للقسم الثاني هو السجلات المختلطة بحيث يكون ذو طبيعة مختلطة يشمل كل من العنصر البشري و العنصر الالي أي يشترك في تكوينها كل منهما ومن الامثلة ان يقوم الانسان بعملية الإدخال بحيث يدخل بيانات

[1] زياد بن محمد عادي العتيبي، المرجع نفسه, ص 19.

[2] زياد بن محمد عادي العتيبي، المرجع و الموضع نفسه، ص 19.

[3] أحمد محمد العمر، مرجع سابق، ص 139.

معينة وتقوم الالة بمعالجة هذه البيانات او حفضها او حتى اجراء عمليات حسابية عليها (مثل برنامج Excel)[1].

2.أدلة لم تعد لتكون وسيلة إثبات (تلقائية):

أما بالنسبة لهذا النوع من الأدلة فهي تنشأ تلقائيا بدون إرادة من الشخص بحيث يتركها ورائه بدون رغبة منه في وجودها وهذا ما يسمى بالأثر أو البصمة الرقمية، وتتجسد هذه الأدلة في الأثار الناجمة عن إستخدام الحاسب الالي أو تصفح شبكة الأنترنت سواء كانت اتصالات او رسائل وايميلات مرسلة كانت او تم استقبالها، وبالرغم من أن هذه الأدلة لم تعد في الأصل ليقوم المستخدم بحفظها إلا انه يمكن ضبطها ورصدها عن طريق وسائل مخصصة لتصبح وسيلة اثبات يعتد بها[2].

الفرع الثاني: اشكال الدليل الرقمي

للدليل الرقمي عدة أشكال من بينها نذكر:

أولا: الصور الرقمية

تختلف الصور الرقمية عن الصور العادية الفوتوغرافية في كونها نتاجا للكاميرات الرقمية والمعالجات الحاسوبية اذ تتميز بسهولة الوصول اليها ومعالجتها وتحمليها وتخزينها عبر شبكة الأنترنت أو حتى الأجهزة الإلكترونية المتنوعة، وتستخدم هذه الصور لتجسيد الحقائق المرئية

[1] أحمد محمد العمر، مرجع سابق، ص 139.

[2] رقية محمودي، نور الهدى قدوح، الجرائم الإلكترونية في المجتمع الجزائري:تشخيص الواقع وتحديات الأمن السيبراني، اعمال الملتقى الإفتراضي، كلية العلوم الإنسانية و الإجتماعية، الطبعة الأولى، جامعة يحيى فارس المدية، الجزائر، 2022، ص 163.

المتعلقة بالجرائم و إسترجاع احداث الجريمة، تقدم كدليل مادي سواء في شكل مطبوعات ورقية أو عبر العرض على الشاشات[1].

ثانيا: التسجيلات الصوتية

يقصد بها التسجيلات التي يتم تسجيلها وتخزينها عن طريق الأجهزة الإلكترونية من مكالمات و محادثات ورسائل صوتية وغيرها سواء كانت على الهاتف او على شبكة الأنترنت[2].

ثالثا: النصوص المكتوبة

وهي كافة المعلومات والبيانات التي يتم كتابتها أو إنشائها بواسطة الأجهزة الإلكترونية المختلفة سواء كانت نصوصا مكتوبة أو أرقام أو تواريخ زمنية، ومن ابرز الأمثلة التي يمكن ذكرها الرسائل عبر البريد الإلكتروني والرسائل النصية كما تمتد لتشمل الملفات والوثائق النصية[3].

[1] صهيب سهيل غازي زامل، مرجع سابق، ص 31.

[2] أحمد محمد العمر، مرجع سابق، ص 144.

[3] صهيب سهيل غازي زامل، مرجع سابق، ص 28-29.

الفصل الثاني

إجراءات إثبات الجرائم المعلوماتية ومعوقاتها

الفصل الثاني

إجراءات إثبات الجرائم المعلوماتية ومعوقاتها

إن التطور والنهضة الإلكترونية والتقنيات الحديثة التي نشهدها في العصر الحالي إمتدت حتى وصلت للعالم الإجرامي وجعلت الجرائم التي تتعلق بالعالم الإفتراضي أصعب حتى من الجرائم العادية نظرا للبيئة التي ترتكب فيها، بحيث أصبحت لها اساليب وإجراءات خاصة للحماية منها وإثباتها، أما فيما يخص هذا الأخير فهو أصعب جزء نظرا لسرعة هذه الجرائم لأن الإثبات يعتمد بشكل رئيسي ويمكن القول انه لا يتحقق إلا بتوفر بالدليل، ووجود الدليل من عدمه يعتمد على ما إن ترك الجاني اثار ورائه، وطبيعة الدليل الرقمي الإلكترونية هي ما تجعل الوصول إليه واستخلاصه صعبا نظرا لما يمكن ان يحدث من سهولة في التلاعب فيها أو حتى تشفيرها والسرعة فيما يتعلق بحذفها وذلك ما يجعل عملية إثباتها أكثرا تعقيدا.

وعليه يهدف هذا الفصل إلى دراسة إجراءات الإثبات وما يمكن أن يواجهها من صعوبات ومعيقات، وهذا من خلال مبحثين رئيسيين، فيما يخص المبحث الأول سوف نتطرق إلى القواعد الإجرائية كل من الإجراءات المألوفة والمستحدثة في إستخلاص الدليل الإلكتروني، أما بالنسبة إلى المبحث الثاني سوف نتناول مايمكن أن يعترضها من معيقات.

المبحث الأول

القواعد الإجرائية

مما لا شك فيه أن الحصول على الدليل الرقمي أو تتبعه من الأمور الصعبة لكنه ليس مستحيلا لأنه لا يوجد بما يسمى بالجريمة المتكاملة، وفي حين أن المشرع نظم عدة أساليب وإجراءات من أجل الوقاية ومنع الجرائم والجريمة الإلكترونية من بينها، إلا أن الجرائم الإلكترونية لا يمكن أن يعتمد فيها الإجراءات المألوفة بشكل مطلق لأن اغلب الأثار والأدلة التي يمكن أن تترك تكون ذات طابع إلكتروني غير مادية، لذلك يجب أن تعتمد أيضا إجراءات حديثة تخص هذا النوع، ومن خلال ما سبق في مبحثنا هذا سوف نتناول كل من الاجراءات المألوفة لإستخلاص الدليل الإلكتروني في المطلب الأول، أما بالنسبة للإجراءات المستحدثة سوف نتطرق إليها في المطلب الثاني.

المطلب الأول

القواعد الإجرائية المألوفة لإستخلاص الدليل الإلكتروني

في مطلبنا هذا سوف نتناول الإجراءات المألوفة والتي تتمثل في المعاينة (الفرع الأول) والتفتيش والضبط (الفرع الثاني).

الفرع الأول: المعاينة في الجريمة الإلكترونية

فيما يخص مكافحة الجرائم ككل بأنواعها تعتبر المعاينة من اهم الإجراءات القانونية فيما يخص التحقيق والبحث، ففي هذا الفرع سوف نتناول المعاينة فيما يخص الجرائم الإلكترونية ومكان إجرائها و الإجراءات الخاصة بها.

أولا. تعريف المعاينة :

بالرغم من أهمية المعاينة كإجراء فيما يخص التحقيق والإثبات إلا أن اغلب التشريعات ومن بينها المشرع الجزائري لم يحددو تعريفا صريحا للمعاينة، إذ أن المعاينة تعد إجراءا تحقيقيا يهدف إلى الإنتقال لمسرح الجريمة من أجل إستخلاص وجمع الأدلة وكل ما يمكن أن يساعد في إثبات وقوع الجريمة والكشف عن الحقيقة[1].

والمعاينة لغة هي العين والمعاينة، وعاينه، ورآه عينا : لم يشك في رؤيته إياه، ورأيت فلانا عينا أي مواجهة، وعاينت الشيء أي أبصرته[2].

أما من الناحية الإصطلاحية المعاينة هي الكشف الحسي المباشر لإثبات الشيء أو الشخص من خلال الرؤية أو الفحص المباشر[3].

وكما ذكرنا سابقا أن المشرع لم يعرف المعاينة أما من جانب الفقه عرفت المعاينة بعدة تعريفات منها نذكر: المعاينة هي إجراء قانوني مادي وفني يكون الغرض والهدف منه التوثيق الدقيق لوضعية الأشخاص وتصوير واقعي يشمل كل ما يحتويه مسرح الجريمة والأماكن وكل الأشياء التي ترتبط بالجريمة نفسها لكشف كل تفاصيلها[4]، وكذلك تعريف اخر يرى بأن المعاينة اجراء

[1] محمد باسل صالح جرار، معاينه مسرح الجريمة الالكتروني ودوره في الاثبات الجنائي وفق التشريع الفلسطيني، قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2022، ص 47.

[2] Rajab Mohammed Nada, Inspection as a Means of Evidence in Administrative Judiciary, journal port science research, volume 7, Egypt, 2024, p 444.

[3] Rajab Mohammed Nada, Ibid., p 444.

[4] محمد باسل صالح جرار، المرجع نفسه، ص 48.

مقتضاه إنتقال المحقق إلى مسرح الجريمة ليشاهد بنفسه ويجمع كل الاثار التي تتعلق بهذه الجريمة وكل ما يمكن جمعه من أجل كشف الحقيقة[1].

ومن خلال التعريفات التي تطرقنا إليها يمكننا القول بأن المعاينة هي إجراء قانوني يتمثل في الإنتقال الى مسرح الجريمة من أجل الكشف عن كل الأثار وجمع كل الأدلة التي من شأنها أن تقودنا إلى كشف كل ماهو مخفي.

ثانيا: مكان إجراء المعاينة في الجريمة الإلكترونية :

ومن خلال ماسبق ككل فإن الجريمة محل إجراء المعاينة هي الجريمة التقليدية والجريمة المستحدثة كذلك ألا وهي الجريمة الإلكترونية[2]، لكن المعاينة العادية المادية لا يمكن أن تكون ذات أهمية كبيرة في الجرائم الالكترونية لأنه ليس من النادر وإنما قليلا ما يترك الجاني دلائل واثار مادية في الجرائم الالكترونية(ما يتخلف عنها يكون رقمي غير ملموس) ورائه عكس الجرائم التقليدية التي دلائلها واثارها مادية[3]، لكنها تبقى واردة لأن مسرح الجريمة الإلكترونية ينقسم الى قسمين:

1. مسرح تقليدي: مسرح الجريمة التقليدي يقصد به المكان المادي الذي يكون خارج النطاق الرقمي للحاسوب والأنترنت بحيث يشمل بصفة أساسية العناصر الملموسة لمكان وقوع الجريمة،

[1] عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي دراسة مقارنة، رسالة مقدمة من الطالبة عائشة بن قارة للحصول على درجة الماجستير في الحقوق، كلية الحقوق، جامعة الإسكندرية، 2009، ص 47.

[2] سومية قلات، حاحة عبد العالي، مقتضيات المعاينة المعلوماتية في التشريع الجزائري، مجلة الحقوق والحريات، المجلد 11، العدد 1، كلية الحقوق والعلوم السياسية جامعة بسكرة، الجزائر، 2023، ص 523.

[3] عائشة بن قارة مصطفى، المرجع نفسه، ص49.

إذ يترك فيه المجرم غالبا أدلة مادية منها نذكر البصمات أو وسائط تخزين رقمية أو حتى أشيائه الشخصية[1].

2. مسرح إفتراضي: أما المسرح الإفتراضي يكون داخل نطاق العالم الإلكتروني الإفتراضي، ويتكون من البيانات المخزنة والمنقولة عبر أجهزة الحاسوب وشبكة الأنترنت وأيضا في وحدات التخزين المتواجدة داخل الحاسب الالي[2].

الجرائم الإلكترونية نظرا لتميزها عن الجرائم التقليدية في كون أدلتها ذات طبيعة رقمية غير مرئية يجعل مسرح الجريمة يختلف ولذلك قبل الإنتقال لموقع الجريمة يجب اتباع مجموعة من الضوابط الفنية منها نذكر[3]:

الحصول على معلومات عن المكان المستهدف قبل قصده والإنتقال إليه وكذا معلومات عن الأجهزة المتوقع التعامل معها وعددها ومواصفاتها بالإضافة الى معرف شبكة الإتصال المستخدمة والمرتبطة بها، وكذلك تشكيل وتجهيز فريق مختص من الخبراء الفنيين، ونظرا للطبيعة الخاصة للأماكن التي قد ترتكب فيها الجريمة الإلكترونية يجب التأكيد على ضرورة حيازتهم للأوامر القضائية اللازمة من أجل التفتيش[4]، وأيضا من الأشياء التي يجب ذكرها هي توفير الأدوات و المعدات والبرامج الضرورية للعملية سواء برامج فحص أو برامج نسخ من أجل نسخ محتوى وحدات التخزين الموجودة داخل الجهاز[5] (من الأمثلة نذكر برنامج Open text encase forensic).

[1] عائشة بن قارة مصطفى، المرجع نفسه، ص 50-51.

[2] عائشة بن قارة مصطفى، المرجع والموضع نفسه، ص 51.

[3] عائشة بن قارة مصطفى، المرجع والموضع نفسه، ص 51.

[4] عائشة بن قارة مصطفى، المرجع والموضع نفسه، ص 51.

[5] عائشة بن قارة مصطفى، المرجع والموضع نفسه، ص 51.

ثالثا:. اجراءات المعاينة في الجريمة الإلكترونية:

من الاجراءات القانونية للمعاينة يمكن ان نذكر:

توقيت إجراء المعاينة المعلوماتية: نظرا لطبيعة الجرائم الإلكترونية الفريدة أجاز المشرع القيام بإجراءات المعاينة في أي وقت من أوقات الليل والنهار وذلك لا يكون إلا بإذن مسبق من وكيل الجمهورية المختص على عكس الجرائم التقليدية التي يكون وقت معاينتها محصور بين الخامسة صباحا والثامنة مساءا[1]، وهذا ما نصت عليه المادة 78 الفقرة 3 من قانون الإجراءات الجزائية[2].

ومن الاجراءات التي يوصي ايضا الخبراء باتباعها نذكر:

1. تصوير كل ما له صلة بالوسائل المستخدمة في إرتكاب هذه الجريمة سواء من أجهزة الحاسب الالي نفسها أو من أجهزة ثانوية ذات صلة بالوسيلة الرئيسية والتي هي الحاسب الالي من أدوات إدخال وأدوات إخراج وحتى التي تكون مزدوجة ذات إدخال وإخراج في نفس الوقت وكل ما يتعلق بالمكان نفسه بصفة عامة مع تدوين زمان ومكان وتاريخ المعاينة والتوثيق[3].

2. ضرورة معاينة الحالة الأصلية أو الوضعية التي وجدت بها توصيلات الكابلات والأسلاك الكهربائية التي ترتبط بالحاسب الالي والمتصلة بالنظام الخاص به[4].

---

[1] سومية قلات، حاحة عبد العالي، المرجع نفسه، ص 528.

[2] المادة رقم 78 من القانون رقم 25-14 المؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 54،

[3] مسعود بن حميد المعمري، مرجع سابق، ص 212.

[4] نورة طرشي، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2012/2011، ص 113.

3. قد يخلف المجرم ورائه أشياء بسيطة لا يعطيها إنتباه تكون ذات إفادة للمحققين من أقراص وأشياء متلفة مرمية وأوراق مطبوعة ممزقة في سلة المهملات أو مكان مخصص يرمي فيه هذه الأشياء بحيث يمكن الإستعانة بها وأخذ البصمات منها التي تكون لها صلة بالجريمة نفسها[1].

4. أيضا الحفاظ على وثائق الإدخال والمخرجات الورقية(المخرجات الورقية هي البيانات والمعلومات التي تحول الى مستندات ملموسة من خلال طابعة ورقية وما شابهها)، من أجل فحصها ورفع البصمات والاثار المادية المتواجدة عليها[2].

5. الحذر التام عند التعامل مع النظام المستخدم والمستندات الموجودة بداخله وكذا المعلومات التي فيه، لأن أي فعل قام به المجرم داخل النظام يعتبر اثر قد خلفه[3].

6. الحفاظ على وحدات التخزين الخارجية من فلاش ديسكات و أقراص صلبة وحتى الأقراص العادية(DVD-CD)، وخاصة الأقراص بوضعها في أجهزة تتيح للمحققين قراءة محتواها دون التغيير فيه[4].

7. الإستعانة وإستشارة الخبراء وأهل الإختصاص عند الحاجة[5].

[1] نورة طرشي، المرجع نفسه، ص 114.

[2] عائشة بن قارة مصطفى، مرجع سابق، ص 52.

[3] عائشة بن قارة مصطفى، مرجع سابق، ص 52.

[4] مسعود بن حميد العميري، مرجع سابق، ص 213.

[5] عائشة بن قارة مصطفى، مرجع سابق، ص 52.

الفرع الثاني: التفتيش والضبط في الجريمة الإلكترونية

يعتبر التفتيش والضبط بدورهما من أهم إجراءات التحقيق، بحيث هدفهما يتمثل في إيجاد أي شيء من شأنه أن يكشف الحقيقة، ففي فرعنا هذا سوف نتناول التفتيش والضبط فيما يخص الجرائم الإلكترونية.

أولا: التفتيش في الجريمة الإلكترونية

التفتيش من أهم الإجراءات التحقيقية لكونه خطوة ركيزة تهدف إلى جمع كل ماهو ذو أهمية ويعتبر كدليل يساعد في الكشف عن الحقيقة، وحتى لا يكون هذا التفتيش وسيلة تخرق الحياة الخاصة أو الحرمة الخاصة بطبيعة الحال هو إجراء قانوني يكون مبني على أمر او إذن من السلطة المختصة ويكون منظم من عدة قوانين خاصة قانون الإجراءات الجزائية والقانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

ولقد تم تعريف التفتيش من عدة فقهاء من بينها نذكر تعريف الفقه الفرنسي الذي عرفه على انه بحث بوليسي او قضائي يكون وفق قواعد قانونية ينفذ في مسكن أي شخص أو في أي مكان اخر حيث يمكن أن توجد أشياء يكون إكتشافها مفيدا في إظهار الحقيقة[1]، كما عرفه المجلس الأوروبي على أنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني[2].

[1] عبد الله علي محمد منصور المرزوقي، حليمه خالد المدفع، خصوصية الدليل الرقمي في الإثبات الجنائي وفقا للتشريع الإماراتي، مشروع أطروحة الماجستير في القانون العام، جامعة الشارقة، 2025، ص 16.

[2] حسن بن علي قاسم الشبعاني، إجراءات استخراج الدليل الإلكتروني، مجلة الأندلس للعلوم الإنسانية والإجتماعية، المجلد 10، العدد 80، كلية الأنظمة والدراسات القضائية، الجامعة الإسلامية بالمدينة المنورة، المملكة العربية السعودية، سبتمبر، 2023، ص 137.

ومن خلال ما سبق بإختصار التفتيش هو إجراء تحقيقي قانوني الهدف منه جمع الأدلة وجمع ما يمكن جمعه من أجل كشف الحقيقة.

إلا أن التفتيش فيما يخص الجرائم الإلكترونية يتمحور بكثرة حول المعلومات والبيانات الإلكترونية التي يمكن ايجادها سواء في الفضاء الإلكتروني أو في الحاسب الالي أو حتى في نظام الحاسب الالي بصفة عامة كالملفات و البرامج وكل اثر رقمي الكتروني وذلك لطبيعة هذه الجريمة، ولكن ذلك لا يعني أن التفتيش المادي غير مهم لأنه بالإمكان أن يقودنا إلى الجاني أو شيء يخص الجريمة.

1. تفتيش المكونات المادية للحاسب الالي

يهدف تفتيش المكونات المادية للحاسب الالي إلى البحث عن الأدلة المادية والمؤشرات والاثار التي يمكن أن تساهم أو تساعد في الكشف عن الحقيقة من أجل تحديد مرتكبي هذه الجريمة، ونظرا لأن التفتيش هنا يركز بالتحديد ويصب على الأجزاء والمكونات المحسوسة للحاسب الالي فإنه يخضع للقوانين والقواعد نفسها المعمول بها في التفتيش العادي للجرائم ومن الأمثلة يمكن أن نذكر جريمة السرقة أو جريمة القتل وما شابه ذلك[1]، بحيث أن الإجراءات القانونية لتفتيش المكونات المادية تحدد بناءا على طبيعة المكان الذي تم العثور فيه على الجهاز (مكان عام أو مكان خاص)، بحيث إذا وجدت مع شخص في مكان عام مثل الطرق أو مقهى عام أو مقهى أنترنت فإن التفتيش هنا يتم وفق القواعد القانونية المعمول بها والمخصصة لهذه الأماكن[2]، أما في حالة وجدت في مكان خاص كمسكن المتهم ففي هذه الحالة التفتيش يخضع

[1] مسعود بن حميد المعمري، مرجع سابق، ص 217.

[2] جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018، ص 16.

لنفس القواعد والضوابط القانونية المقررة و المنصوص عليها لتفتيش المساكن وبنفس الضمانات[1](المكونات المادية نقصد بها الاشياء مثل لوحة المفاتيح الفأرة شاشة الكمبيوتر الطباعة وما شابهها من ملحقات الجهاز).

2. تفتيش المكونات المعنوية للحاسب الالي

المكونات المعنوية يمكن تقسيمها الى قسمين: القسم الأول هو المكونات الموجودة في الجهاز أي في نظام التشغيل نفسه وكل ما يحتويه النظام سواءا من برامج أساسية موجودة في النظام مثبتة فيه أو برامج أخرى تطبيقية يستخدمها الشخص أو حتى بيانات ومعلومات تكون موجودة في النظام خلفت من طرف صاحب الجهاز لإستخدامه للجهاز من ملفات صور وما شابهها[2]، أما القسم الاخر من المكونات المعنوية مرتبط بشبكات المعلوماتية والأنترنت والفضاء الإفتراضي عامة بحيث يتسم هذا النوع بصعوبة تفتيشه نظرا لطبيعة المعلومات أو البيانات التي تكون مستهدفة لأن الشبكة المتعامل معها قد تكون محلية أو عالمية، وهذا النوع من البيانات والمعلومات يتطلب خبرة فنية ودهاء عاليين من أجل تعقب وتفتيش وإستخراج هذه الأدلة لأنها لا تكون ثابتة عكس القسم الأول التي تكون مخزنة في الجهاز[3].

3. تفتيش الشبكة المعلوماتية للحاسب الالي

مع ظهور الأنترنت ادى التطور الذي نشهده في تكنولوجيا المعلومات إلى خروج الإتصالات من الإيطار العادي البسيط الى فضاء عالمي شاسع بحيث أن هذا التطور جعل من التفتيش تحديا عويصا ومعقدا نوعا ما، فالشبكة المعلوماتية نقصد بها كل ترابط سلكي أو لاسلكي بين

[1] نورة طرشي، مرجع سابق، ص 118.

[2] مسعود بن حميد المعمري، مرجع سابق، ص 218.

[3] مسعود بن حميد المعمري، مرجع سابق، ص 218.

جهازين أو أكثر بحيث ينقسم نطاق هذه الشبكات إلى قسمين ألا وهما محلي وعالمي، بحيث أن الموضوع يصبح أكثر تعقيدا عندما تكون البيانات المستهدفة مخزنة في نطاق إختصاص قضائي لدولة أخرى أو موزعة على عدة دول[1]، لذلك هناك حالتين يجب التحدث عنهما:

- **إتصال جهاز المتهم بجهاز اخر داخل إقليم الدولة نفسها**

ويقصد بذلك مثلا المعلومات أو البيانات المراد إستهدافها وتفتيشها يتم إرسالها من حاسب الي إلى حاسب اخر خاص بشخص اخر متواجد على نفس الإقليم[2]، فيما يخص هذه الحالة فقد نصت المادة رقم 05 الفقرة الثانية من نص القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها أنه طبقا للحالة المذكورة في الفقرة(أ) اذا تبين أن المعطيات المراد البحث عنها مخزنة في نظام معلوماتي اخر ويمكن الولوج أو الوصول إليها عن طريق النظام الأول، يجوز وبعد إخطار السلطة القضائية المختصة مسبقا تمديد عملية التفتيش إلى النظام الأول[3].

- **إتصال جهاز المتهم بجهاز اخر موجود خارج إقليم الدولة**

ونقصد بذلك أن المعلومات أو البيانات المراد تفتيشها والمتعلقة بالجريمة تم إرسالها وتخزينها في جهاز اخر عن طريق الأنترنت وهذا الجهاز موجود خارج الإقليم أي خارج الدولة ،إلا أنه وعلى عكس الحالة الأولى هنا تمديد التفتيش مقيد بحيث أن المادة رقم 05 الفقرة الثالثة من القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و

[1] جمال براهيمي، المرجع نفسه، ص 20-21.

[2] جمال براهيمي، المرجع نفسه، ص 22.

[3] المادة رقم 05 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد 47.

الإتصال ومكافحتها نصت على أن الحصول على هذه المعطيات يكون بناءا على مساعدة السلطات المختصة بموجب الإتفاقيات الدولية ووفقا لمبدأ المعاملة بالمثل[1]، أما في الحالات الإستعجالية أجاز المشرع للسلطات المختصة تبادل المساعدات القضائية الدولية عن طريق وسائل الإتصال السريعة مثل الفاكس أو البريد الإلكتروني شرط التأكد من صحتها للأمن الكافي[2].

ثانيا: الشروط القانونية للتفتيش في الجريمة الإلكترونية:

تنقسم إلى قسمين أساسيين(شروط شكلية وشروط موضوعية):

1. الشروط الشكلية:

أ. الحضور أثناء إجراء التفتيش في الجريمة الإلكترونية:

في نص المادة 76 الفقرة الأولى من قانون الإجراءات الجزائية نص المشرع الجزائري على ضرورة حضور المتهم في حالة إذا كان التفتيش في المسكن الخاص به، لكن في بعض الأحيان قد يتعذر عليه الحضور لذلك اتاح المشرع له أن ينيب غيره ليحضر أثناء إجراء التفتيش، واذا إمتنع عن الحضور من تلقاء نفسه أو كان هاربا وجب إستدعاء شاهدين، إلا أن المشرع وفي الفقرة الأخيرة من نفس المادة إستثنى تطبيق هذه الأحكام فيما يخص التفتيش في الجرائم الإلكترونية[3].

ب. وقت إجراء التفتيش في الجريمة الإلكترونية:

[1] المادة رقم 05 من القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها، المصدر نفسه.

[2] المادة رقم 16 من القانون رقم 09-04، المصدر نفسه.

[3] المادة رقم 76 من قانون الإجراءات الجزائية، مصدر سابق.

نص المشرع الجزائري في نص المادة 78 من قانون الإجراءت الجزائية على ما إذا كان التفتيش يتعلق بالجرائم الإلكترونية فإن وقت التفتيش يكون في كل ساعات الليل والنهار وهذا ما تم النص عليه في الفقرة الرابعة[1].

2. الشروط الموضوعية:

أ. سبب التفتيش:

يعتبر السبب هو الركيزة الأساسية والحافز لإتخاذ قرارات إجراءات التفتيش، ولا ينشأ ذلك إلا في حالة وقوع جريمة سواء كانت جناية أو جنحة مع ضرورة توفر أدلة وقرائن قوية تشير إلى وجود ما يفيد في الكشف عن حقيقة المشبه فيه أو غيره[2].

ب. محل التفتيش:

بحيث يجب أن يكون المحل مما يجيز القانون تفتيشه، والمحل يرتبط غالبا بمكان معين مثل منزل المتهم أو شخص محدد بصفته مالكا أو حائزا للجهاز، لذلك يوجب القانون مراعاة طبيعة المكان الذي توجد فيه الوسائل الإلكترونية التي تكون موضوع التفتيش والإلتزام بكافة الضمانات القانونية المحيطة بها، كما يجب التأكيد أيضا على بعض الإستثنائات التي تتعلق بالحصانة

[1] المادة رقم 78 من قانون الإجراءات الجزائية.

[2] ليندة بومحراث، إجراءات التحقيق الخاصة بالجرائم السيبيرانية، يوم دراسي حول الجريمة السيبيرانية، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، 2022، ص 16-17.

القانونية بحيث يمنع تفتيش أشخاص أو أماكن معينة لمثل الدبلوماسيين وأعضاء البرلمان ومكاتب المحاميين وماشبه ذلك[1].

ج. السلطة المختصة بالتفتيش:

فيما يخص السلطة المختصة فقد حددها المشرع الجزائري في نص المادة 5 من القانون رقم 09-04 من ضباط الشرطة القضائية وكذا السلطات القضائية المختصة في إيطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 التفتيش ولو عن بعد[2].

ثالثا: الضبط في الجريمة الإلكترونية

الضبط الإلكتروني في الجرائم الإلكترونية يختلف عن الضبط في الجرائم العادية بحيث يركز بصفة عامة على ضبط الأدلة المعنوية من بيانات أو معلومات يمكن ضبطها وأن تكون كدليل يستخدم في الكشف عن الحقيقة، وضبط الأدلة المادية موجود أيضا بطبيعة الحال من وحدات إدخال وإخراج للجهاز مثل الطابعة ولوحة المفاتيح وما شابه ذلك كلها يمكن ضبطها، ولقد نصت المادة 06 من القانون رقم 09-04 على أنه ليس من الضروري حجز كل المنظومة برمتها ولكن يمكن نسخ المعطيات اللازمة وتخزينها بحيث تكون قابل للحجز والوضع في احراز[3]، واذا كان الحجز غير ممكن لأسباب معينة يمكن للسلطة المختصة القيام بإستعمال تقنيات اللازمة من أجل منع الوصول لها من أجل منع أي تدخل يمكن أن يعبث بها بحيث تكون في أمان وهذا ما أشارت إليه المادة 07 من القانون رقم 09-04[4].

---

[1] ليندة بومحراث، المرجع نفسه، ص 17.

[2] المادة رقم 05 من القانون رقم 09-04، المصدر السابق.

[3] المادة رقم 06 من القانون رقم 09-04، المصدر السابق.

[4] المادة رقم 07 من القانون رقم 09-04، المصدر السابق.

المطلب الثاني

القواعد الإجرائية الحديثة لاستخلاص الدليل الإلكتروني

بعدما تناولنا في المطلب السابق الإجراءات التقليدية في هذا المطلب سوف نتطرق إلى الإجراءات الحديثة والي تتمثل في اسلوب التسرب والمراقبة الإلكترونية في الفرع الأول واسلوب إعتراض المراسلات في الفرع الثاني.

الفرع الأول: أسلوب التسرب والمراقبة الإلكترونية

يعتبر أسلوب التسرب والمراقبة الإلكترونية من أهم الأساليب أو الإجراءات الحديثة فيما يخص الجرائم الإلكترونية، وفي هذا الفرع سوف نتطرق إلى كل منهما على حدة.

-أولا: التسرب

يعتبر أسلوب التسرب من أحدث الإجراءات وأكثرها فعالية خاصة فيما يخص الجرائم الإلكترونية، وقد نص المشرع الجزائري على تعريف التسرب في نص المدة 120 من قانون الإجراءات الجزائية بأن التسرب هو قيام ضابط أو عون الشرطة القضائية بمراقبة الأشخاص المشتبه فيهم عن طريق إيهامهم أنه فاعل معهم أو شريك لهم[1]، إنطلاقا من تعريف المشرع الجزائري السابق نرى إلى أي مدى عملية التسرب معقدة بحيث تتطلب أحيانا القيام بأفعال ممنوعة قانونيا والإنخراط المباشر فيها من أجل إثبات الولاء لهذه الجماعة الإجرامية ويبين لهم

[1] المادة رقم 120 من قانون الإجراءات الجزائية، المرجع السابق.

أنه واحد منهم من أجل عدم شكهم فيه، وتقديرا لهذه الضرورات قام المشرع الجزائري بحماية الضابط أو العون المتسرب من خلال تجريده من المسؤولية الجنائية للأفعال التي يقوم بها[1].

كما أن المشرع نص في المادة 125 من قانون الإجراءات الجزائية على أنه لايجوز في أي مرحلة من المراحل الإجرائية للتسرب الكشف عن هوية الذين يقومون بعملية التسرب[2]، وذلك من أجل حمايتهم.

ويتمثل التسرب الإلكتروني في الجرائم الإلكترونية في أن الضابط أو عون الشرطة القضائية يدخل إلى العالم الإفتراضي ويشمل ذلك الإنضمام والإنخراط في مجموعات قرصنة مثلا عبر تقمصه لهويات معينة وأسماء مستعارة تضمن إندماجه فيها بشكل عادي، منتديات هاكرز وغرف دردشة معينة(مثل غرف الدردشة والمنتديات التي تكون في الأنترنت المظلم على سبيل المثال التي يجتمع فيها معظم الهاكرز) وذلك من أجل جمع الأدلة والمعلومات الكافية حول كل الأعمال الغير القانونية التي يقومون بها[3].

-ضوابط التسرب:

1.الضوابط الإجرائية:

تتمثل الركيزة الأساسية للضوابط في ضرورة الحصول على الإذن القضائي المسبق، اذ يمنع على ضباط أو أعوان الشرطة القضائية ممارسة أي عملية تسرب من دون إذن قضائي مسبق

[1] جمال براهيمي، المرجع السابق، ص 84.

[2] المادة رقم 125 من قانون الإجراءات الجزائية.

[3] جمال براهيمي، المرجع السابق، ص 85.

من السلطات المختصة[1] وهذا ما نصت عليه المادة 120 من قانون الإجراءات الجزائية، ويجب أن يكون هذا الإذن مكتوبا وإلا كان باطلا طبقا لنص المادة 124 من نفس القانون[2].

2.الضوابط الموضوعية:

والتي تتمثل في المبررات التي تكون مرفقة في الإذن المكتوب، وكذا هوية ضابط الشرطة القضائية والدوافع والأسباب التي جعلته يلجأ لعملية التسرب[3]، وهذا ما نصت عليه المادة 124 الفقرة الثانية من قانون الإجراءات الجزائية[4].

-ثانيا:المراقبة الإلكترونية

لم يحدد المشرع الجزائري المقصود بالمراقبة الإلكترونية صراحة في أي نص ولكنه إكتفى بتحديد مفهوم الإتصالات الإلكترونية بحيث يرى بأن المراقبة الإلكترونية هي عملية تتم على

الإتصالات الإلكترونية وفي حالات حددها القانون[5]، بحيث يمكننا تعريف المراقبة الإلكترونية على أنها تدابير إجرائية يتولاها خبير وتهدف إلى تتبع وترصد الأنشطة التي يقوم بها المشتبه به وكل ما يصدر عنه سواء نصوص مكالمات تسجيلات صوتية وماشابه ذلك[6]، كما نص المشرع الجزائري في نص المادة 03 على أنه وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وهذا القانون(رقم09-04) أجاز وضع ترتيبات تقنية لمراقبة الإتصالات

[1] جمال براهيمي، المرجع السابق، ص 85.
[2] المادة رقم 124 من قانون الإجراءات الجزائية.
[3] جمال براهيمي، مرجع سابق، ص 86.
[4] المادة رقم 124 من قانون الإجراءات الجزائية.
[5] ليندة بومحراث، مرجع سابق، ص 19.
[6] ليندة بومحراث، مرجع سابق، ص 19.

الإلكترونية وتجميع وتسجيل محتواها وذلك لمستلزمات التحريات أو التحقيقات القضائية الجارية[1].

1. الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

تم النص عليها في المادة 04 من نفس القانون وهي:

– بغرض الوقاية من الجرائم الإرهابية أو أعمال التخريب، وكذا الجرائم التي تمس بأمن الدولة.

– في إيطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

–لضرورات التحري والتحقيق القضائي، متى تعذر أو تعسر الوصول إلى نتائج الأبحاث الجارية بالوسائل العادية دون اللجوء إلى المراقبة الإلكترونية.

_ عند توفر معلومات جدية تفيد بإحتمال وقوع إعتداء يستهدف منظومة معلوماتية من شأنه المساس بالنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.[2]

2.شروط المراقبة الإلكترونية:

من الشروط التي تم الإشارة اليها في نص المادة 04 من القانون رقم 09-04 نجد:

–إجراء عملية المراقبة الإلكترونية يكون بإذن مكتوب من السلطة المختصة.

–وجود ضرورة تتطلب اللجوء لهذا الإجراء.

–أن يكون هذا الإجراء لمقتضيات التحريات والتحقيقات القضائية.[3]

[1] المادة رقم 03 من القانون 09-04.

[2] المادة رقم 04 من القانون 09-04.

[3] ليندة بومحراث، مرجع سابق، ص 20.

الفرع الثاني: أسلوب إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور

بالرغم من أهمية هذا الأسلوب إلا أن المشرع الجزائري لم ينص على تعريفه صراحة وانما إكتفى بتنظيمه في نصوص قانون الإجراءات الجزائية.

-أولا تعريف إعتراض المراسلات:

يمكننا تعريف إعتراض المراسلات على أنها إجراء يتم بشكل سري وخفي، ويتضمن مساسا بخصوصية وسرية المحادثات الخاصة، وهذا الإجراء تأمر به السلطات القضائية المختصة وفقا للأشكال والأطر التي حددها القانون وذلك يكون بغرض إستخلاص كل مايمكن أن يكون دليل يثبت إرتكاب الجريمة، كما يشمل أيضا التنصت والإعتراض عبر التقنيات المختلفة والوسائل السلكية واللاسلكية المختلفة[1].

بحيث نص المشرع الجزائري في نص المادة 114 من قانون الإجراءات الجزائية أن إعتراض المراسلات هي التي تكون بواسطة وسائل الإتصال السلكية واللاسلكية[2].

-ثانيا تعريف تسجيل الأصوات وإلتقاط الصور:

المشرع لم يضع تعريفا صريحا أيضا لكل من تسجيل الأصوات وإلتقاط الصور، لكن يمكننا تعريف كل منهما على حدة، فتسجيل الأصوات هو تدوين وحفظ المحادثات الشفوية واللقاءات الكلامية التي تدور بين الأشخاص سواء اتسمت بالسرية أو العلنية في أماكن خاصة أو عامة وتكون عبر أجهزة تقنية مخصصة لهذا الغرض، مما يتيح إعادة الإستماع إليها لاحقا[3]، أما

[1] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، بدون طبعة، دار الجامعة الجديدة، الإسكندرية، مصر، 2019، ص 254.

[2] المادة رقم 114 من قانون الإجراءات الجزائية.

[3] يزيد بوحليط، المرجع نفسه، ص 260.

بالنسبة لإلتقاط الصور هي إجراء يتم بإستخدام الكاميرات أو الأجهزة المتخصصة لتوثيق هيئة المشتبه فيه لإثبات واقعة أو استخدامها كدليل[1].

ضوابط أسلوب إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور

تم النص على كل الضوابط في قانون الإجراءات الجزائية والتي سوف نتطرق إليها فيما يلي:

الضوابط الإجرائية:

-من الضوابط الإجرائية الهامة هي إذن وكيل الجمهورية المختص أو قاضي التحقيق بمباشرة هذا الإجراء أو هذه العملية (نص المادة 114 من قانون الإجراءات الجزائية)[2].

_ كما أن هذه الإجراء المرخص به يكون تحت إشراف المباشر لوكيل الجمهورية المختص، وفي حالة فتح تحقيق قضائي أيضا ينفذ هذا الإجراء تحت رقابة قاضي التحقيق المباشرة كذلك[3].

- كما أن هذا الإجراء يتم دون المساس بالسر المهني وضمان احترامه[4].

- منح المشرع الحق لكل من وكيل الجمهورية وضابط الشرطة القضائية المأذون له، وقاضي التحقيق أو ضابط الشرطة القضائية الذي ينوبه الإستعانة بأي عون مؤهل ذو خبرة كافية في مجال الإتصالات السلكية واللاسلكية من أجل تولي المهام التقنية المتعلقة بالعمليت المنصوص عليها في المادة 114[5].

---

[1] يزيد بوحليط، المرجع نفسه، ص 264.

[2] المادة رقم 114 من قانون الإجراءات الجزائية.

[3] المادة رقم 114 من قانون الإجراءات الجزائية.

[4] المادة رقم 115 من قانون الإجراءات الجزائية.

[5] المادة رقم 117 من قانون الإجراءات الجزائية.

– تدوين وتحرير محضر لكل عملية يقوم بها ضابط الشرطة القضائية بكل تفاصيلها حتى ساعة وتاريخ بداية العمليات حتى انتهائها[1].

– ومن الإجراءات نجد أيضا أن كل ما تم التوصل إليه من صور مراسلات محادثات تساهم في كشف الحقيقة أن تدون في محضر رسمي يودع بملف وتحفظ[2].

_ تثبيت وسائل التقنية دون موافقة المعنيين، وذلك بهدف إلتقاط تسجيل أو بث الأحاديث الخاصة والسرية للأفراد سواء في الأماكن العامة أو الخاصة[3].

الضوابط الموضوعية:

– أن يشمل الإذن كافة البيانات والمعطيات الكفيلة بتحديد الإتصالات المستهدفة بالإلتقاط، وكذا تحديد الأماكن المعنية مع المدة الزمنية لسريانها[4].

– أن يكون الإذن مكتوبا لحد يكون أقصاه أربعة أشهر مع إمكانية تجديده بذات الشروط الإجرائية[5].

[1] المادة رقم 118 من قانون الإجراءات الجزائية.
[2] المادة رقم 119 من قانون الإجراءات الجزائية.
[3] المادة رقم 114 من قانون الإجراءات الجزائية.
[4] المادة رقم 116 من قانون الإجراءات الجزائية.
[5] المادة رقم 116 من قانون الإجراءات الجزائية.

المبحث الثاني

عوائق الإثبات :

يعتبر مفهوم الاثبات في الجرائم المعلوماتية شانه شأن المفهوم العام للاثبات , و هو اقامة الدليل على وقوع الجريمة مكتملة الاركان و نسبها للمتهم وفق ما حدده القانون , غير ان طبيعة الجريمة المعلوماتية تفرض وجود ظروف و اساليب خاصة لاثباتها . كما وجب استحداث اساليب اجرائية من اجل جمع الادلة في الجرائم المعلوماتية , التي اصبحت مم الصعب اثباتها و ذلك لخاصيتها من حيث سهولة محو الدليل و عدم ترك اثاره و غيرها من الخصائص التي سيتم دراستها في هذا المبحث .

سنتطرق في دراستنا لهذا المبحث الى اهم المعوقات التي تواجه سلطات التحري و التحقيق في اثبات الجرائم المعلوماتية , لا سيما منها المرتبطة بالدليل الرقمي (المطلب الاول) و خصوصية التحقيق (المطلب الثاني) .

المطلب الاول

المعوقات المتعلقة بخصوصية الدليل الالكتروني .

يعد الاثبات الجنائي عملية متكاملة مرتبطة ببعضها البعض , تهدف للبحث عن الادلة الجنائية عبر مراحل , و التي تبين من خلالها ثبوت حدوث الواقعة و ظروف ارتكابها و معالجة اسبابها . بحيث تواجه الجريمة صعوبات عديدة عند اثباتها , و هذا ما دفع سلطة التحقيق للجوء الي البيئة الرقمية للبحث عن ادلة من شانها الحد من هذه الجرائم .

و يعتبر الدليل الرقمي وسيلة اثبات اساسية في هذا النوع من الجرائم , الا ان استخلاصه يحيط به الكثير من الصعوبات و تتمثل اغلبها في عدم وجود الدليل الرقمي (الفرع الاول) و سهولة محوه و فقدان اثارالجريمة[1] (الفرع الثاني) .

الفرع الاول : عدم وجود الدليل الرقمي :

يتميز الدليل الرقمي عن الدليل التقليدي من حيث الطبيعة التقنية , فالدليل الرقمي يقوم بانتاج نبضات الكترونية تتكون من سلسلة من ارقام [2]. و اذا كان الدليل الرقمي في الجريمة التقليدية ذو طبيعة مادية و مرئية يمن استخلاصه بر اساليب التحري و التحقيق التى اعتاد المحققون القام بها كالمعاينة و التفتيش و غيرها , فان الامر يختلف تماما في عملية البحث عن الدليل الرقمي , فما يميز هذا الاخير انه غير مرئي و شكله المتمثل في سلسلة الارقام غير المتشابهة بالرغم من انها لا تتجاوز وحدة الرقم الثنائي (0_1) يعقد عملية الاطلاع عليه . كما ان حجم و شكل هذه النبضات يجعل من عملية استيعابها امرا مستحيلا للبشر بدون استعمال وسائل تقنية تعالج هذه الذبذبات, لذا وجب الاستعانة باجهزة تقنية و استخدام برامج ملائمة للاطلاع على الدليل الرقمي و استخراجه في هيئة عادية ملموسة , يمكن تقديمها للقضاء.[3]

[1] الطيبي البركه , اشكالية الاثبات في الجرائم الالكترونية , مجلة الافاق العلمية , المجلد 11 , العدد , 01 , جامعة ادرار ' 2018 , ص ص 266_284 , ص 268 .

[2] عماد بلغيث , جغلولي يوسف , صعوبات التحقيق في الجرائم الالكترونية , مجلة الرسالة للدراسات و البحوث الانسانية , المجلد 06 , العدد 03, جامعة محمد بوضياف , المسيلة , 2021 , ص 70_83 , ص 79 .

[3] هانية بوشارب , بن شهرة بتول , صعوبة عملية استخلاص الدليل اللكتروني , المجلد 09 , العدد 1 جامعة الاخوة منتوري , قسنطينة , 2023, ص69.

يعد الدليل الرقمي عبارة عن تركيبة من المعطيات الرقمية في شكل ذبذبات رقمية سريعة و متطورة يصعب تفسيرها و فهمها , و هذا ما يوجب استخدام وسائل تقنية في استنباط هذا النوع من الادلة [1].

يعتبر تمكن المختصين في التحقيق من الاطلاع على الدليل الرقمي مرحلة من مراحل اثبات الجريمة , فمبجرد الاطلاع لا يعني فهمه و اعتماده كدليل مبني على الجزم و اليقين الذي لا يقوم الدليل الا بهما .ففهمه و ادراكه و التاكد من صحته يعتبر تحديا قائما امام جهات التحقيق التي انحصرت مهامها في جرائم تقليدية يمكن التعامل معها . كما يرى جانب من الفقه ان مسؤولية اكتشاف الجريمة و ضبط مرتكبيها و محاكمتهم يقع على عاتق الاجهزة الحكومية المطالبة بتوفير كافة الامكانيات التقنية اللازمة ة تسخير كامل الجهود للتحقيق في الجرائم المعلوماتية , حتى و ان تطلب عليها الامر استقطاب كفاءات مهنية تقنية في هذا المجال [2].

استحدث المشرع الجزائري وسائل تقنية لاستخلاص الدليل الرقمي في القانون 09_04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الاعلام و الاتصال و مكافحتها, في المواد 4,5,6, 11 منه . و المتمثلة في اجراءات مراقبة الاتصالات الالكترونية و حجز المعطيات و تفتيش منظومة معلوماتية , و ايضا حفظ المعطيات المتعلقة بحركة السير من طرف مقدمو الخدمات , محاولة منه لاستغلال الدليل الالكتروني و الحد من اغلب الجرائم المنتشرة [3],

الفرع الثاني : سهولة محو الدليل و فقدان اثار الجريمة :

[1] رانية حداد , دور الدليل الرقمي في منظومة العدالة الجنائية المعاصرة , المجلد 11 ,العدد 01 , جامعة خنشلة ,2025, ص ص 801_811 , ص 805 .

[2] الطيبي البركه , اشكالية الاثبات في الجزائم الالكترونية , مرجع سابق , ص 270 .

[3] الطيبي البركه , مرجع نفسه , ص 271 .

تعيق خاصية سهولة محو الدليل الرقمي جهات التحقيق المختصة في الجرائم المعلوماتية , فارتباطه بها يزيد من صعوبة اثباتها خاصة ان عملية محو الدليل او تدميره يعد امرا في غاية السهولة بالنسبة للجاني و لا يستغرق وقتا طويلا , اذ يمكن التحكم في المعلومات التي تعتبر محلا للتنقيب الجنائي من قبل الجاني , مما يسهل عملية محو الدليل و تدميره[1] . و بالنظر الى الخاصية التي تتميز بها الجرائم المعلوماتية , فان عملية التحقيق فيها و اثباتها يحيط به الكثير من التحديات و الصعوبات , و التي من بينها عدم ترك اثار عادية خارجية تساعد على اكتشاف الجريمة . فنجد ان سلوك ارتكاب الجريمة يتسم بالهدوء و يتم فيه الاعتماد على الارقام و البيانات مما يجعل عملية تغييرها و محوها من ذاكرة الحاسوب امرا سهلا , لايترك خلفه اي اثار خارجية , عكس الجرائم التقليدية التي يقوم السلوك الاجرامي فيها على اعمال عنف تتمثل في التكسير او السرقة او الاقتحام او الجرح ... و غيرها من سلوكيات المجرمة التي تخلف اثار تسهل عملية التحقيق فيها[2].

يشكل سهولة اخفاء الجناة للدليل الرقمي او محوه او تدميره تحديا حقيقيا امام سلطات التحقيق لاثبات الجرائم المعلوماتية , بما ان خاصية الدليل الرقمي في انه عبارة عن نبضات الكترونية يتم من خلالها تسجيل البيانات يزيد من امكانية اخفـاء الدليل و سهولة محوه في مدة زمنية قصيرة . و قد لا يستغرق ذلك من الجاني ساعات طويلة بل يحتاج الى بضع دقائق او حتى اجزاء من الدقيقة حسب مؤهلات الجاني التقنية و امكانياته في القيام بالفعل [3].

[1] حيمي سيدي محمد , معوقات التحقيق الجنائي في الجرائم الالكترونية , المجلة الاكاديمية للبحوث القانونية و السياسة , المجلد 06 , العدد 01 , جامعة ابو بكر بالقايد تلمسان , 2022 , ص ص 1734_1752 , ص 1746 .

[2] عبد الغاني حسونة , التجديات القانونية لاثبات الجريمة المعلوماتية ,مجلة الاجتهاد القضائي , المجلد 15 , العدد 01 ,جامعة محمد خيضربسكرة, 2023 ,ص16 .

[3] عبد الغني حسونة , مرجع نفسه , ص16.

نجد ان الجاني دائما ما يحرص على محو الاثار التي من شانها اثبات ارتكابه للفعل المجرم , و ذلك من خلال اعتماده على بعض التقنيات التي تساعد على محو البيانات و تعديلها في وقت قصير . و لكن رغم حرصه نجد ان الدليل الرقمي غالبا ما يترك بعد محوه او تعديله اثارا يصعب اكتشافها الا من طرف خبراء متخصصون في هذا المجال . و بذلك يمكن كشف التلاعبات التي قام بها الجاني لمحو اثار جريمته , الا ان جهات التحقيق غالبا ما تفتقر الى تلك المعرفة و الخبرة التي تمكنها من كشف الجرائم المعقدة التي يتطلب التحقيق فيها احاطة كاملة بالتكنولوجيا الحديثة و بمختلف العقبات التي تصعب الوصول الى الدليل الرقمي[1].

قام المشرع الجزائري في هذا الاطار بمحاولة فيه للتخفيف من صعوبة اثبات الجرائم المعلوماتية عن طريق الدليل الرقمي التي يتم محوه. بالزام عقد الخدمات بحفظ كل المعطيات التي تمكن عن التعرف غلى مستعملي الخدمة و المعطيات التي تتعلق بالتجهيزات الطرفية المستعملة للاتصال . بالاضافة الى الخصائص التقنية و تاريخ و وقت و جهة الاتصال و كل المعطيات التي تسمح بالتعرف على اطراف الاتصال و عناوين المواقع المطلع عليها , و هذا من خلال القانون 09_04 المتضمن القواعد الخاصة المتعلقة بالوقاية من جرائم تكنولوجيا الاعلام و الاتصال . و ذلك للحفاظ على الاثار التقنية التي تسمح بتتبع مسار الجريمة المعلوماتية اثباتها[2].

المطلب الثاني

المعوقات المتعلقة بخصوصية التحقيق

[1] الطيبي البركه , اشكالية الاثبات في الجرائم الالكترونية , مرجع سابق , ص 272_273 .
[2] عبد الغني حسونة , التحديات القانونية لاثبات الجريمة المعلوماتية , مرجع سابق , ص16.

يعتبر التحقيق الرقمي في الجرائم المعلوماتية مجموعة اساليب و طرق متبعة من طرف الجهات المتخصصة في التحقيق من اجل كشف الحقائق و تقديم ادلة الاثبات الرقمية في شكل ادلة ملموسة تساهم في اثبات الجريمة امام الجهة القضائية , و قد يحيط بعملية التحقيق صعوبات عديدة تعيق المحققين في الوصول الى الادلة و اثبات ارتكاب الفعل المجرم , كما قد يمس بمستوى اجهزة التحقيق اذا فشلوا في استخلاص الادلة و الوصول الى نتيجة من شانها اثبات وقوع الجريمة , و قد يكسب المحرم ثقة كبيرة في افلاته من العقاب مما يزيد من محاولات القيام بهذه الجرائم التي اصبحت الاجهزة الامنية غير قادرة على الحد منها , و ذلك راجع الى الصعوبات المتعلقة بكشف غموض الجريمة (الفرع الاول) و كذا الصعوبات المتعلقة بالتعاون الدولي للتحقيق في الجرائم المعلوماتية (الفرع الثاني).

الفرع الاول : المعوقات المتعلقة بصعوبة كشف غموض الجريمة :

يتميز التحقيق عبر مراحله في الجريمة المعلوماتية بداية من مرحلة البحث و التحري بصعوبته التي ترجع الى عدة معوقات تعترض كشف غموض الجريمة و نجد اهمها :

أولا : الكم الهائل من البيانات : تعرف الانظمة المعلوماتية على اختلاف انواعها بقدراتها الهائلة على تخزين البيانات بما يعادل عدد كبير من الصفحات الورقية و قد يتجاوز ذلك مئات الالاف , و لو قام المحققون بطباعة ما تخزنه الانظمة المعلوماتية لاحتاج الى وقت كبير و كميات كبيرة جدا من الاوراق ,كما نستنزف من هذه العملية جهدا كبيرا قد لا يتوج بنتائج ايجابية توصله الى تحصيل الدليل و كشفه .لذا وجب على الانظمة الحكومية توفير الية للفرز الذاتي للبيانات المخزنة حتى يتسنى لجهات التحقيق الوقوف على الملفات غير المشروعة [1].

[1] عبد الغني حسونة , التحديات القانونية لاثبات الجريمة المعلوماتية , مرجع سابق , ص 18 .

تشكل البيانات المتداولة في الانظمة الالكترونية و المتميزة بكثرتها احدى العوائق البارزة التي تعقد عملية التحقيق في الجرائم التي تقع عليها او بواسطتها , فالبحث عن الادلة في حاسب واحد يتطلب فحصا دقيقا للمعطيات المخزنة في الاف الملفات هذا ما يكلف المحقق وقتا طويلا و جهدا كبيرا , مما يجعل الوصول الى الدليل الرقمي امر شبه مستحيل[1].

غاب المشرع الجزائري عن محاولة تسوية مشكل حجم البيانات كعائق امام سلطة التحقيق , و تركه لسلطتهم الاستدلالية التي تختلف جسب ظروف كل قضية , و هذا ما يعد امرا منطقيا لان العائق ذو طبيعة تقنية وجب مواجهته مواجهت تقنيا[2].

ثانيا : مميزات الجرائم الالكترونية : تتميز الجريمة الالكترونية بسرعة تنفيذها و حداثة اساليب ارتكابها و سهولة اخفاء اثارها , و تقوم اساسا على الخداع في ارتكابها و محاولة التضليل في التعرف على مرتكبيها ,مما يصعب على المحقق العادي التعامل معها . فهي تحتاج الي خبرة فنية للكشف عنها .و هذا ما يقتضي ضرورة المام جهات التحقيق و المحاكمة بمعرفة انظمة الحاسب الالكترونيو طريقة تشغيل اساليب ارتكاب الجرائم عليها او بواسطتها , مع قدرتهم على التعامل معها و سرعة التصرف فيها , حتي يتسنى لهم ظبط الادوات المستحدمة في الجريمة , وهذا ما اوجب اعداد برامج تدريب و تاهيل كفاءات فنية لمواحهة صعوبات التحقيق و الوصول الى النتائج المطلوبة بكفاءة عالية[3].

ثالثا : عدم تناسب اجراءات التحقيق العادية مع الجريمة المعلوماتية :

ساهم التطور التكنولوجي السريع في المجال المعلوماتي في خلق تحديات حالة دون مكافحة الجريمة و ضبطها , فكلما تبنت الانظمة الحكومية اساليب جديدة للتحقيق بعد معالجة

[1] حيمي سيدي محمد , معوقات التحقيق الجنائي في الجرائم الالكترونية , مرجع سابق , ص 1747 .
[2] عبد الغني حسونة ,التحديات القانونية لاثبات الجريمة المعلوماتية , مرجع سابق ,ص18 .
[3] الطيبي البركه , اشكالية الاثبات في الجرائم الالكترونية , مرجع سابق , ص 276 .

صعوبات سبقتها تطور اساليب الاجرام و القرصنة بشكل يصعب مسايرته من طرف السلطات من مختلف دول العالم . حيث لم تتمكن الدول من السيطرة على هذه الجريمة , و في اغلب الجرائم نجد ان وسائل الاجرام اكثر تطورا من وسائل مكافحته المسخرة من طرف الدولة , كما نجد ان الامر تعدى تصور النصوص العقابية المتعلقة بالجريمة المعلوماتية بل وصل الى تصور النصوص القوانين الاجرائية التي لا تتلائم مع طبيعة هذا النوع من الجرائم ,فنجد ان معظم اجراءات التحقيق و المتابعة تتعارض مع طبيعة الوسائل المستحدمة في تنفيذ الجريمة التي يكون محلها البيانات و هذا ما يشكل عائقا كبيرا امام سلطات التحقيق[1].

سار المشرع الجزائري و على نهج اغلب مشرعي دول العالم في مواجهة صعوبات مكافحة الجريمة المعلوماتية , بوضع اساليب خاصة تتوافق مع الطبيعة التقنية لهذه الجرائم من خلال قانون 09_04 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها. و نجد اهم هذه الاساليب اجراء المراقبة الالكترونية الذي يضمن اسلوبي الوقاية و المكافحة , و احراءات تفتيش النظم المعلوماتية و حفظ معطيات السير من طرف مقدمي الخدمات.

و في سابقة نجد ان المشرع تعامل مع هذه الجريمة بصرامة كبيرة و سمح بوضع ترتيبات تقنية حتى قبل وقوع الفعل المجرم , بل بمجرد الشك غير المبني على الجزم و اليقين بوقوع الجريمة و لم يراع حرمة الحياة الخاصة للافراد . و قد بكون ذلك بسبب خطورة الجرائم خاصة الماسة بامن الدولة[2] منها. هذا ما دفع المشرع الجزائري لانشاء هيئة خاصة تابعة لمصالح وزارة الدفاع

[1] عبد الغني حسونة , التحديات القانونية لاثبات الجريمة المعلوماتية , ملرجع سابق , ص 18_19 .
[2] طيبي البركه , اشكالية الاثبات في الجرائم الالكترونية , مرجع سابق , ص277 .

الوطني لمكافحة الجريمة نظرا للمعدات التقنية التي تحوزها , مما يساعد على كشف الجناة حتى و ان استعملوا وسائل التمويه و التضليل[1].

يمكن القول ان كشف غموض الجريمة المعلوماتية مسؤولية تقع على عاتق سلطات التحقيق , للمطالبة بتدريب و تاهيل كفاءات ملمة بالتقنيات الاساسية للتكنولوجيا و مواكبة التطور التقني في هذا المجال ,حتى و ان تطلب ذلك الاستعانة بخبراء تقنيين لاستخلاص الادلة الالكترونية في الامور المعقدة للتاكد من صحة الادلة و تقديمها امام الجهات القضائية.

الفرع الثاني : ضعف التعاون الدولي في مكافحة الجرائم المعلوماتية :

ساهم البعد الدولي للجريمة المعلوماتية في افلات الجناة من العقاب و تطوير نشاطهم , باستغلال بعض الثغرات منها عدم التعاون الدولي في مجال مكافحة الجريمة بين بعض الدول . مما فرض على المجتمع الدولي ضرورة البحث على اساليب اكثر ملاءمة مع طبيعة الجريمة المعلوماتية و خاصيتها العابرة للحدود الوطنية , فالسياسة الجنائية القائمة على المبادئ القانونية التقليدية لا تتماشى مع ما شهد العالم من تطور في مجال المعلوماتية خاصة في اساءة استعمالها كوسيلة لارتكاب الجرائم بطريقة احترافية .كما انها لا تحقق الغرض المرجو منها في ظل ظهور هذا النوع من الجرائم [2].

اثر وقوع الجريمة المعلوماتية في دولة ما و بلوغ اضرارها و تحقق نتائجها في دولة اخرى على العلاقات الدولية ,و تعريض مصالحها المشتركة للخطر , فقيام الجاني بالرتكاب جريمة تضر بمصلحة دولة اجنبية غير الحامل لجنسيتها او المساس بسيادتها , قد يؤثر على علاقة دولته بها بالرغم من عدم علمها بوقوع الجريمة و ذلك لتحقق النتيجة خارج حدودها , فمثلا

[1] الطاهر رحمي , الجريمة المعلوماتية في التشريع الجزائري , مرجع سابق , ص 10_11.
[2] احمد ميلودية , الجريمة المعلوماتية : المفهوم _حتمية تطوير اليات اتعاون الدولي في مجال مكافحتها , مجلة الدراسات القانونية و السياسية , المجلد 04 , ألعدد 02 , حامعة عمار ثليجي الاغواط , 2018 , ص ص 266_283 , ص 274 .

وقوع الجريمة على اعضاء السلك الدبلوماسي او الاطلاع على اسرار دولهم او جمع المعلومات بغية التجسس عليهم يؤدي الى اضطراب العلاقات الدولية و بلتالي ضعف التعاون فيما بينهما.[1] فوجب عاى الدول التحلي بكامل المسؤولية و عدم تساهلها في ترك المجال للمجرمين في الافلات من العقاب من هذا الباب , خاصة انهم اصبحو يستغلون العلاقات التاريخية الحساسة و المضطربة بين الدول لارتكاب جرائمهم .

تتمتع كل دولة بالسيادة في مباشرة سلطاتها التشريعية و القضائية و التنفيذية في حدود اقليمها , لكن نجد ان الاختصاص القضائي اصبح عائقا امام الامساك بالمجرمين و محاسبتهم نتيجة رفض التسليم بحجة الاختصاص القضائي و مبدا عدم تسليم الدولة لرعاياها , ادى ذلك الي بروز تنازع حول الاختصاص بين الدول فيما بينها و بين الدول و القضاء الدولي يظهر هذا التنازع من خلال تسليم المجرمين و احصائيات ادانتهم و محاسبتهم . و يعد حق منع تسليم المواطنين مبا قانونيا تلتزم به اغلب دول العالم و يصعب حرقه و المساس به لاعتباره محل اهتمام دولي [2].

يشكل عدم وجود نموذج واحد للنشاط الاجرامي المعلوماتي عائق من معوقات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية , فالانظمة القانونية القائمة في اغلب الدول لمواجهة الجريمة و عدم وجود اتفاق عام مشترك حول صور و نموذج استخدام الانظمة المعلوماتية على وجه غير مشروع , يزيد من صعوبة التنسيق و تحقيق صور التعاون الدولي . فما يكون فعلا مباحا في دولة يشكل جريمة في دولة اخرى و ذلك راجع لعدة عوامل منها

[1] علوي علي احمد الشارفي , الوجيز في جرائم تقنية المعلومات , مرجع سابق , ص 100 .
[2] ملاك وردة , اشكالات تفويض جهود التعاون الدولي في مكافحة الجرائم الدولية , مجلة النبراس للدراسات القانونية , المجلد 08 ,العدد 02 , جامعة العربي التبسي , تبسة , الجزائر , 2025 , ص 28.

اختلاف الثقافات و الديانات و العادات و التقاليد ... و غيرها من العوامل التي تخلق اختلاف في شرعية السلوك المرتكب [1].

ساهم اختلاف النظم القانونية الاجرائية في تعقيد عملية التعاون الدولي في مكافحة الجريمة المعلوماتية ,فاختلاف طرق البحث و التحري احدى اسباب عدم تحقيق النتائج المطلوبة , و ذلك يرجع الى اختلاف فاعليتها فنجاعة طرق البحث و التحري قد تثبت فائدتها في دولة كما قد تكون عديمة الفائدة في دولة اخرى . و هذا من اسباب فشل التعاون الدولي في تحقيق نتائج من شانها الحد من ارتكاب الجريمة المعلوماتية . و هذا ما يزيد ايضا من صعوبة ابرام معاهدات ثنائية او جماعية بين الدول لتحقيق الحماية المطلوبة في ظل تطور برامج و نظم الحاسب الالي و شبكة الانترنت .

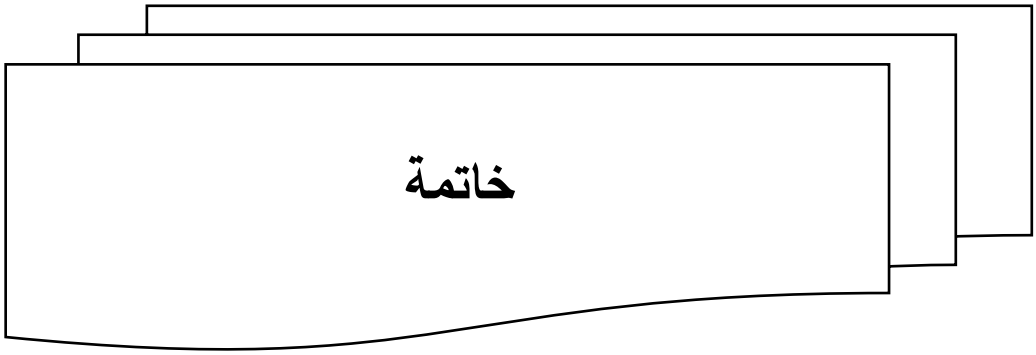
اصبحت مكافحة الجريمة المعلوماتية امرا حتميا يستلزم تعاونا دوليا لايجاد الوسائل المناسبة لتحقيق نتيجة فعالة في مواجهة هذه الجرائم , فوجب على المجتمع الدولي السعي للتوفيق بين التشريعات الخاصة التى تضمن مكافحة هذه الجرائم , حتى يتماشى مع سرعة ارتكاب الجريمة و ضرورة كشفها قبل محو اثارها من خلال تبادل المعلومات و اتخاذ الاجراءات المتوافقة من اجل القاء القبض على الجاني و تسليمه . كما وجب ضمان حجية الادلة التي تم جمعها امام الجهات القضائية للدول المتعاونة فيما بينها . و تعد هذه الاسباب وسيلة تساعد على تحقيق التعاون الدولي في مكافحة الجريمة المعلوماتية[2].

يظهر ان المشرع الجزائري وضع قيود على طلبات المساعدة الدولية القضائية حفاظا على سيادتها و على نظامه العام , و قد نص في الفصل السادس من القانون 09_04 سالف

[1] طيبي البركه , اشكالية الاثبات في الجرائم الالكترونية , مرجع سابق , ص 279.
[2] طيبي البركه ,اشكالية الاثبات في الجريمة الاكترونية , مرجع سابق , ص 279 .

الذكر[1] على وضع قواعد تتعلق بالاختصاص القضائي و تبادل المعلومات في اطار المساعدة القضائية .

[1] انظر الفصل السادس من القانون 09_04 .


خاتمة

الخاتمة:

في ختام هذه الدراسة التطور التكنولوجي المتسارع الذي نعيشه في عصرنا الحالي أفرز أنماطا وأنواعا إجرامية جديدة كليا والتي تختلف جوهريا عن الجرائم التقليدية مما أصعب فكرة مواكبتها بحيث تمتاز بخصائص تميزها عن هذه الأخيرة نظرا لطبيعتها الرقمية الإلكترونية وبيئتها وسرعة حدوثها، ونظرا لخطورة الظاهرة وتهديدها المباشر لأمن المجتمع باتت الحماية الجنائية أمرا ملحا، ونتيجة لهذه التحديات برز الدليل الرقمي بوصفه وسيلة إثبات تتمتع بقوة ثبوتية وحجية قانونية كافية في المسائل الجنائية، مما يفرض على القضاء والأنظمة القانونية ضرورة اعتماده والأخذ به نظرا لقيمته القانونية في مجال الإثبات الجنائي، وبالرغم من المحاولات والتحديات التي يقوم بها المشرع فيما يخص مواكبة هذه الجرائم من الناحية الإجرائية والقانونية إلا أنه ما يزال هناك معيقات من شأنها أن تعرقل هذه الإجراءات والمواكبات الحاصلة فيما يخص مواجهة وإثبات هذه الجرائم وكلما تطورت الإجراءات والوسائل التي من شأنها مواجهة هذه الجرائم من الناحية الأخرى نجد بأن هذه الجرائم تتطور بدورها.

وعليه يمكن ايجاز اهم النتائج المتوصل اليها في هذا البحث فيما يلي :

1. تتميز الجرائم الإلكترونية عن غيرها من الجرائم التقليدية بجملة من الخصائص والسمات التي تمنحه طابعا مميزا وتجعله مختلفا، وكذلك الأمر بالنسبة للدليل الإلكتروني.
2. للدليل الإلكتروني دور محوري في الكشف عن الجرائم الإلكترونية وإثباتها ونسبتها إلى مرتكبيها كما يمكن أن يمتد أثرها إلى المساهمة في إثبات بعض الجرائم التقليدية.
3. كما يعد الدليل الرقمي المستمد من إجراءات باطلة دليلا غير مشروع، مما يفقده قوته الثبوتية وحجيته القانونية.
4. أدى التطور المتسارع في مجال تكنولوجيا المعلومات إلى استحداث أساليب ووسائل حديثة ومتطورة لارتكاب الجرائم، مما أفرز أنواعا إجرامية جديدة.
5. إستخلاص الأدلة المرتبطة بهذه الجرائم يتطلب كفاءة ومعرفة تقنية عاليتين في مجال التكنولوجيا.

6. جاء القانون رقم 09-04 باليات وإجراءات مستحدثة لجمع الدليل الرقمي وإستخراجه كما نظم أيضا المراقبة الإلكترونية والتفتيش والضبط.

و بهذا نخرج بجملة من الاقتراحات ضرورة اخذ الحطة و الحذر عند استعمال النظم الالية و البرامج و البيانات المعلوماتية :

1. توفير برامج تدريبية للمحققين الجنائيين عن طريق وضع محاكاة لهذه الجرائم بهدف تنمية مهاراتهم في جمع الأدلة وتعزيز قدرتهم على توظيف التقنيات الحديثة.
2. تعديل قانون الإجراءات الجزائية بما يتلائم مع طبيعة الأدلة الرقمية وخصائصها وآليات التعامل معه وحفظه.
3. يستحسن إستحداث وحدات أمنية متخصصة في التصدي للجرائم الإلكترونية تتمتع بالكفاءة التقنية والفنية اللازمة لمتابعة هذه الجرائم.
4. تدعيم التشريعات السارية بنصوص قانونية حديثة تتضمن إجراءات تواكب التطورات المتسارعة في الوسائل التقنية وأساليب إرتكابها.
5. تدعيم الإجراءات المعتمدة في إستخلاص الدليل الرقمي بآليات حديثة.
6. الحث على توعية أفراد المجتمع بمخاطر الجرائم الإلكترونية يمكن أن يساهم في تسهيل جهود الجهات المختصة في إجراءات التحقيق.

قائمة المراجع

قائمة المصادر والمراجع

أولا: المصادر:

1. القرآن الكريم.

ثانيا: المراجع:

أولا:الكتب:

1. أبو زكريا يحيى بن موسى الرهوني، تحفة المسؤول في شرح مختصر منتهى السول، الطبعة الأولى، دار البحوث للدراسات الإسلامية وإحياء التراث، دبي، الإمارات، 2002.

2. أيوب بن موسى الحسيني القريمي الكفوي، الكليات معجم في المصطلحات والفروق اللغوية، الطبعة الثانية، مؤسسة الرسالة للطباعة والنشر والتوزيع، بيروت، لبنان، 1998.

3. إبن منظور، لسان العرب، د ط، دار المعارف، القاهرة، 2016.

4. احمد حمو، علاء عواد واخرون، الأدلة الالكترونية (الجوانب القانونية والتقنية)، دون طبعة، دون دار نشر، فلسطين، 2015.

5. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، بدون طبعة، دار الجامعة الجديدة، الإسكندرية، مصر، 2019.

6. نعيم سعيداني , الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة), الطبعة الاولى , المؤسسة الحديثة للكتاب , لبنان , 2022.

7. علوي علي احمد الشارفي , الوجيز في جرائم تقنية المعلومات , الطبعة الاولى، المركز الديمقراطي العربي للدراسات السياسية و الاستراتيجية و الاقتصادية , المانيا 2024.

8. عبد الرزاق، محمد شوقي واخرون، الدليل الإسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية، دون طبعة، دار جامعة نايف للنشر، المملكة العربية السعودية، 2024.

9. رقية محمودي، نور الهدى قدوح، الجرائم الإلكترونية في المجتمع الجزائري:. تشخيص الواقع وتحديات الأمن السيبراني، اعمال الملتقى الإفتراضي، كلية العلوم الإنسانية و الإجتماعية، الطبعة الأولى، جامعة يحيى فارس المدية، الجزائر، 2022.

ثانيا: الأطروحات:

أ-الدكتورة

1. جمال براهيمي ، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018.

2. درابلة العمري سليم، حجية الدليل الرقمي في الإثبات الجنائي، أطروحة مقدمة لنيل شهادة دكتوراه علوم، تخصص القانون الجنائي والعلوم الجنائية،كلية الحقوق، جامعة الجزائر 01، 2025/2024.

3. صهيب سهيل غازي زامل، البحث والتحري عن الدليل الإلكتروني في المسائل الجزائية، أطروحة للحصول على شهادة الدكتوراه، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة وهران 2، 2022/2021.

ب-الماجستير

4. محمد باسل صالح جرار، معاينه مسرح الجريمة الالكتروني ودوره في الاثبات الجنائي وفق التشريع الفلسطيني، قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2022.

5. نورة طرشي ، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2012/2011.

6. عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي دراسة مقارنة، رسالة مقدمة من الطالبة عائشة بن قارة للحصول على درجة الماجستير في الحقوق، كلية الحقوق، جامعة الإسكندرية، 2009.

7. عبد الله علي محمد منصور المرزوقي، حليمه خالد المدفع، خصوصية الدليل الرقمي في الإثبات الجنائي وفقا للتشريع الإماراتي، مشروع أطروحة الماجستير في القانون العام، جامعة الشارقة، 2025.

ثالثا: المقالات العلمية

1. أحمد محمد عمر، الدليل الرقمي وحجيته في الإثبات الجزائي، مجلة الدراسات الفقهية والقانونية، العدد الثالث، المعهد العالي للقضاء، سلطنة عمان، يناير، 2020.
2. أحمد ابو زيد شحاته، دور الدليل الرقمي في تعزيز قناعة القاضي في الإثبات الجنائي، مجلة العلوم القانونية والإقتصادية، العدد الاول، يناير، 2024.
3. أمال بهنوس ، الدليل الرقمي في الإجراءات الجنائية، المجلة الأكاديمية للبحث القانوني، العدد 02، جامعة وهران 2 محمد بن أحمد، وهران، الجزائر، 2017.
4. أحمد ميلودية , الجريمة المعلوماتية : المفهوم _حتمية تطوير اليات التعاون الدولي في مجال مكافحتها , مجلة الدراسات القانونية و السياسية , المجلد 04 , ألعدد 02 , حامعة عمار ثليجي الاغواط , 2018.
5. هانية بوشارب , بن شهرة بتول , صعوبة عملية استخلاص الدليل اللكتروني , المجلد 09 , العدد 1 جامعة الاخوة منتوري , قسنطينة , 2023.
6. زكية مهنى، الأدب الرقمي من النص إلى الوسيط، مجلة الاثر، العدد 26، جامعة عبد الرحمان ميرة بجاية (الجزائر)، سبتمبر، 2016.
7. زياد بن محمد عادي العتيبي، دراسة استطالعية حول حجية أألدلة الرقمية في إثبات الجرائم المعلوماتية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد التاسع والعشرون، جدة، المملكة العربية السعودية، اكتوبر، 2020.
8. حمد محمد الدوسري , انواع الجرائم الالكترونية و تحديات مكافحتها , مجلة المنار للدراسات و البحوث القانونية , كلية الحقوق و العلوم السياسية , جامعة يحيى فارس , المدية ,المجلد 09 , العدد01, كلية القانون , جامعة لوسيل , قطر , 2025.
9. حسن بن علي قاسم الشبعاني، إجراءات استخراج الدليل الإلكتروني، مجلة الأندلس للعلوم الإنسانية والإجتماعية، المجلد 10، العدد 80، كلية الأنظمة والدراسات القضائية، الجامعة الإسلامية بالمدينة المنورة، المملكة العربية السعودية، سبتمبر، 2023.
10. حيمي سيدي محمد , معوقات التحقيق الجنائي في الجرائم الالكترونية , المجلة الاكاديمية للبحوث القانونية و السياسة , المجلد 06 , العدد 01 , جامعة ابو بكر بالقايد تلمسان , 2022.
11. الطيبي البركه , اشكالية الاثبات في الجرائم الالكترونية , مجلة الافاق العلمية , المجلد 11 , العدد , 01 , جامعة ادرار , 2018.

12. الطاهر زحمي , الجرائم المعلوماتية في التشريع الجزائري و تدابير الوقاية منها , مجلة التشريع الاعلامي , المجلد 02 , العدد 01 , كلية العلوم و الاتصال , جامعة الجزائر 3 , 2023.
13. كريمة رزاق بارة , الجريمة الالكترونية المتعلقة بالاشخاص وفقا للتشريع الفرنسي و التشريع الجزائري ,المجلة الجزائرية للحقوق و العلوم السياسية , المجلد 08, العدد 02 , المركز الجامعي عبد الحفيظ بوصوف , ميلة , 2024.
14. لامية طالة , الجريمة الالكترونية :بعد جديد لمفهوم الاجرام عبر منصات مواقع التواصل الاجتماعي , مجلة الرواق للدراسات الاجتماعية و الانسانية ,المجلد 06 , العدد 02 , جامعة الجزائر 03 , 2020.
15. ليندة بومحراث ، إجراءات التحقيق الخاصة بالجرائم السيبيرانية، يوم دراسي حول الجريمة السيبيرانية، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، 2022.
16. مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، العدد 03، الجزء الثاني، اكتوبر، 2018.
17. ملاك وردة , اشكالات تفويض جهود التعاون الدولي في مكافحة الجرائم الدولية , مجلة النبراس للدراسات القانونية , المجلد 08 ,العدد 02 , جامعة العربي التبسي , تبسة , الجزائر , 2025.
18. محمد رحموني ,خصائص الجريمة الالكترونية و مجالات استحدامها ,مجلة الحقيقة , العدد 41 , جامعة احمد دراية , ادرار , 2018.
19. نبيل ونوغي , عبد الرؤوف زيوش , الجريمة المعلوماتية في التشريع الجزائري ,مجلة العلوم القانونية و الاجتماعة , المجلد الرابع , العدد الثالث , جامعة مولود معمري تيزي وزو , 2019.
20. نورالدين بن سولة , الجرائم الالكترونية في ضوء التشريع الجزائري , مجلة الحوار المتوسطي ,المجلد التاسع , العدد10 جامعة معسكر , 2018.
21. سميرة معاشي ,الجريمة المعلوماتية (دراسة تحليلة لمفهوم الجريمة المعلوماتية) مجلة الفكر, العدد السابع عشر ,كلية الحقوق و العلوم السياسية ,جامعة محمد خيضر , بسكرة , 2018.
22. سعيد مسعود الكثيري , الجريمة الالكترونية في ضل اتفاقية بودابست :الاطار المفاهيمي و التصنيفي , مجلة البحوث القانونية و الاقتصادية , المجلد 09 , العدد 01 , جامعة ظفار عمان , 2026.

23. سومية قلات ، حاحة عبد العالي، مقتضيات المعاينة المعلوماتية في التشريع الجزائري، مجلة الحقوق والحريات، المجلد 11، العدد 1، كلية الحقوق والعلوم السياسية جامعة بسكرة، الجزائر، 2023.
24. عماد بلغيث , جغلولي يوسف , صعوبات التحقيق في الجرائم الالكترونية , مجلة الرسالة للدراسات و البحوث الانسانية , المجلد 06 , العدد 03, جامعة محمد بوضياف , المسيلة , 2021.
25. عبد الغاني حسونة , التجديات القانونية لاثبات الجريمة المعلوماتية ,مجلة الاجتهاد القضائي , المجلد 15 , العدد 01 ,جامعة محمد خيضر، بسكرة, 2023.
26. فريد روابح , جرائم الجمع غير المشروع للمعطيات الشخصية الرقمية في التشريع الجزائري , مجلة الحقوق و العلوم السياسية, جامعة خنشلة, المجلد 09 , العدد 01 ,جامعة محمد لمين دباغين سطيف , 2022.
27. ريمة بن عميروش , عن خصوصية الجريمة المعلوماتية , مدلة الفقه القانوني و السياسي ,المجلد 02,العدد02,جامعة محمد الصديق بن يحيى ,جيجل ,2020.
28. رانية حداد , دور الدليل الرقمي في منظومة العدالة الجنائية المعاصرة , المجلد 11 ,العدد 01 , جامعة خنشلة.2025
29. خالد شريف , الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال في التشريع الجزائري , مجلة البيان للدراسات القانونية , المجلد 10 , العدد 01 , جامعة محمد خيضر بسكرة, 2025.

رابعا: النصوص القانونية:

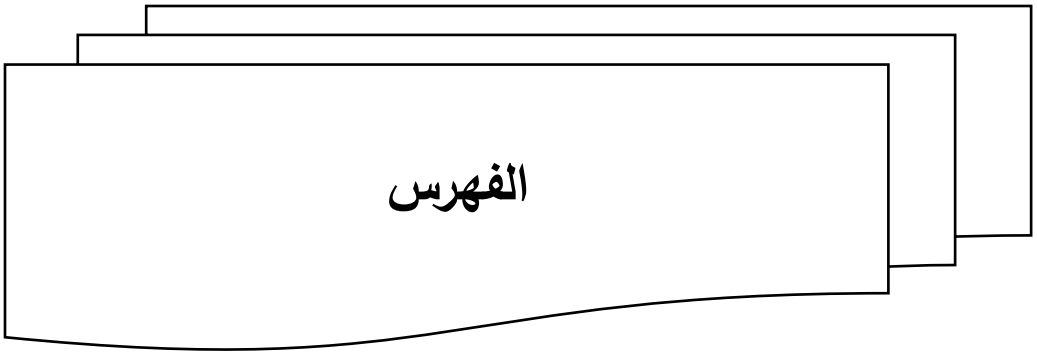
1. القانون رقم 25-14 المؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 54، الصادر بتاريخ 13 أوت 2025.
2. القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 غشت 2009.
3. القانون رقم 18_07 يتعلق بحماية الاشخاص الذاتيين في مجال معالجة المعطيات ذات الطابع الشخصي , الجريدة الرسمية العدد 34 الصادر في 25 رمضان 1439 الموافق ل 10 يونيو 2018.

4. القانون رقم 175 المؤرخ في 14 أوت 2018، يتعلق بمكافحة جرائم تقنية المعلومات، الجريدة الرسمية المصرية، العدد 32 مكرر(ج)، الصادر في 14 أوت 2018.

خامسا: المراجع باللغة الإنجليزية:

1. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Third Edition, Published by Elsevier Inc, 2011.

2. Rajab Mohammed Nada, Inspection as a Means of Evidence in Administrative Judiciary, journal port science research, volume 7, Egypt, 2024.


الفهرس

الفهرس

مقدمة 5
الفصل الاول: الاطار المفاهيمي للجريمة المعلوماتية 6
المبحث الاول: ماهية الجريمة المعلوماتية 7
المطلب الأول: تعريف الجريمة المعلوماتية و انواعها 7
الفرع الاول: تعريف الجريمة المعلوماتية 8
أولا: تعريف الفقه للجريمة الإكترونية 8
ثانيا: التعريف القانوني للجريمة المعلوماتية 9
أ_ تعريف الجريمة المعلوماتية في التشريع الجزائري : 9
ب_ تعريف الجريمة المعلوماتية في التشريعات الاخرى :.....10
الفرع الثاني: انواع الجريمة المعلوماتية : 11
أولا: حسب الافراد : 11
ثانيا: من حيث موضوع البيانات و المعطيات : 13
المطلب الثاني: اركان وخصائص الجريمة المعلوماتية 14
الفرع الاول: اركان الجريمة المعلوماتية :.....14
_ أولا: الركن الشرعي : 15
_ثانيا: الركن المادي :.....15
المبحث الثاني 19

الدليل الرقمي 19
المطلب الأول: مفهوم الدليل الرقمي 20
الفرع الأول: تعريف الدليل الرقمي 20
الفرع الثاني: خصائص الدليل الرقمي 23
المطلب الثاني: أنواع الدليل الرقمي وأشكاله 26
الفرع الأول: أنواع الدليل الرقمي: 26
أولا: الدليل الرقمي المرتبط بالحاسوب وشبكاته: 27
ثانيا: الادلة الرقمية المتعلقة بشبكة الانترنت: 27
ثالثا: الدليل الرقمي المتعلق ببروتوكولات تبادل المعلومات: 27
رابعا: الدليل الرقمي المتعلق بالشبكة العالمية للمعلومات: 28
الفرع الثاني: اشكال الدليل الرقمي 29
أولا: الصور الرقمية 29
ثانيا: التسجيلات الصوتية 30
ثالثا: النصوص المكتوبة 30
الفصل الثاني 32
إجراءات إثبات الجرائم المعلوماتية ومعوقاتها 32
المبحث الأول 33
القواعد الإجرائية 33

المطلب الأول: القواعد الإجرائية المألوفة لإستخلاص الدليل الإلكتروني 33

الفرع الأول: المعاينة في الجريمة الإلكترونية 33

أولا: تعريف المعاينة : 34

ثانيا: مكان إجراء المعاينة في الجريمة الإلكترونية : 35

ثالثا:. اجراءات المعاينة في الجريمة الإلكترونية: 37

الفرع الثاني: التفتيش والضبط في الجريمة الإلكترونية 39

I–أولا: التفتيش في الجريمة الإلكترونية 39

أولا: تفتيش المكونات المادية للحاسب الالي 40

ثانيا: تفتيش المكونات المعنوية للحاسب الالي 41

ثالثا: تفتيش الشبكة المعلوماتية للحاسب الالي 41

رابعا: الشروط القانونية للتفتيش في الجريمة الإلكترونية:.....43

II–ثانيا: الضبط في الجريمة الإلكترونية 45

المطلب الثاني القواعد الإجرائية الحديثة لاستخلاص الدليل الإلكتروني 46

الفرع الأول: أسلوب التسرب والمراقبة الإلكترونية 46

–أولا: التسرب.....46

–ثانيا:المراقبة الإلكترونية 48

الفرع الثاني: أسلوب إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور 50

–أولا: تعريف إعتراض المراسلات: 50

-ثانيا: تعريف تسجيل الأصوات وإلتقاط الصور: 50

المبحث الثاني: عوائق الإثبات : 53

المطلب الاول: المعوقات المتعلقة بخصوصية الدليل الالكتروني 53

الفرع الاول: عدم وجود الدليل الرقمي : 54

الفرع الثاني: سهولة محو الدليل و فقدان اثار الجريمة : 55

المطلب الثاني: المعوقات المتعلقة بخصوصية التحقيق 57

الفرع الاول: المعوقات المتعلقة بصعوبة كشف غموض الجريمة : 58

أولا: الكم الهائل من البيانات : 58

ثانيا: مميزات الجرائم الالكترونية : 59

ثالثا: عدم تناسب اجراءات التحقيق العادية مع الجريمة المعلوماتية : 59

الفرع الثاني: ضعف التعاون الدولي في مكافحة الجرائم المعلوماتية : 61

خاتمة 65

قائمة المراجع 68

الفهرس 75