وزارة التعليم العالي والبحث العلمي

جامعة الشهيد الشيخ العربي التبسي–تبسة–

كلية الحقوق وعلوم السياسية

التحقيق الجنائي في الجرائم الإلكترونية

مذكرة مقدمة لنيل شهادة نيل شهادة الماستر تخصص جريمة وأمن عمومي

من إعداد الطالبة:

–مشري نور الإيمان

تحت إشراف الأستاذة:

أ/خالدي خديجة

أعضاء لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة
عزاز هدى	أستاذة تعليم عالي	رئيسة اللجنة
خالدي خديجة	أستاذة محاضرة أ	المشرف ومقررة
مقران ريمة	أستاذة محاضرة أ	المناقشة

السنة الجامعية 2024/2023

الاهداء

إلى أعز الناس وأقربهم إلى قلبي إلى والدتي العزيزة ووالدي رحمه الله وأسكنه فسيح جناته اللذان كانا كونا وسندا لي،

وكان لدعائهما المبارك الأعظم الأثر في تسيير سفينة البحث حتى ترسو هذه الصورة.

إلى من ساندني ويسرى لي الصعاب إلى صديقتي وابنة عمتي لبنى وابن عمتي عماد ووقوفي في هذا المكان ما كان ليحدث لولا تشجيعهما المستمر.

إلى كل من أعطاني يد العون وساعدني في إنجاز هذه الذكرة.

شكر وعرفان

الشكر والحمد أولا لله الذي بيده يتم الصالحات أما بعد

الشكر الجزيل وفائق التقدير لأستاذة "خالدي خديجة" على تحملها عناء الإشراف على هذه الرسالة وعلى توجيهاتها القيمة التي أنارت الكثير من نقاط الضال فيها

كما اتوجه بخالص الشكر الى أعضاء اللجنة الموقرين الاستاذة هدى عزاز رئيسة للجنة المناقشة والأستاذة مقران ريمة مناقشة الذي حملتهم الاقدار عناء قراءة وتقويم وتقيم وإثراء هذه الرسالة

مقدمة

مقدمة

إن دخول البشرية في الألفية الثالثة كان بمثابة بداية مرحلة جديدة من النمو الفكري والمعرفي، مدفوعة بالتطور الهائل في مجالي تقنية المعلومات والاتصالات. هذا التطور كان نتيجة للاندماج التدريجي بين هذين المجالين، مما جعل استخدام الأنظمة المعلوماتية أساسياً في مختلف القطاعات بفضل ميزاتها في الدقة والسرعة في تجميع المعلومات وتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات سواء داخل الدولة الواحدة أو بين عدة دول.

ورغم الفوائد الكبيرة التي تحققت وتتحقق يومًا بعد يوم في جميع المجالات، إلا أن الاستخدام المتزايد لهذه التقنيات جاء أيضاً مع مجموعة من الآثار السلبية نتيجة للاستخدام السيئ والمفرط وغير المشروع، مما أضر بمصالح الأفراد والمجتمعات. فقد أصبحت هذه التقنيات مرتعاً لارتكاب الجرائم، مما أدى إلى بروز ظاهرة إجرامية جديدة عُرفت بجرائم تقنية المعلومات أو الجرائم الإلكترونية. وتعد هذه الجرائم من أخطر وأعقد الجرائم على الإطلاق، فهي سرية، تقنية، سهلة التنفيذ وصعبة الإثبات، تنشأ في الخفاء في بيئة إلكترونية افتراضية، وتُرتكب باستخدام الحواسيب وشبكات الإنترنت. يُنفذها أشخاص يتمتعون بذكاء ومهارات تقنية عالية، ويمتلكون أدوات المعرفة الفنية للتعامل في مجال المعالجة الآلية للمعطيات. بالإضافة إلى ذلك، تُعد هذه الجرائم عابرة للحدود عبر شبكة اتصال غير محدودة، غير مجسدة، وغير مرئية، متاحة لأي شخص حول العالم.

وبالتالي، فإن التحقيق في مثل هذه الجرائم وكيفية ضبط الأدلة الرقمية وجمعها يُعتبر من الموضوعات المستجدة التي تتطلب أسلوب تحقيق مختلف عن الجرائم التقليدية. فبعد أن كان الطابع الإجرائي التقليدي القائم على العنف والتعذيب هو الوسيلة الوحيدة للكشف عن الجريمة واستنباط الأدلة، ظهر طابع إجرائي حديث قائم على الاستعانة بالتكنولوجيا واستخدام شبكة الإنترنت. إن الطابع المميّز لأساليب التحقيق الحديثة يتجلى في تطور وسائل البحث والتحري بما يواكب حركة الجريمة وتطور أساليب ارتكابها في عصر المعلوماتية.

مقدمة

أهمية الدراسة:

تنبع أهمية دراسة الجرائم الإلكترونية من عدة جوانب، نظراً لخطورة هذه الجرائم وخصائصها الفريدة التي تميزها عن الجرائم التقليدية، وصعوبة التعامل معها وإثباتها.

تشكل الجرائم الإلكترونية تهديداً كبيراً للأفراد والمؤسسات والدول، إذ يمكن أن تسبب خسائر مالية ضخمة، وتؤدي إلى سرقة المعلومات الحساسة، وانتهاك الخصوصية، وتعطيل البنية التحتية الحيوية، كما أن الجرائم الإلكترونية تتميز بخصائص فريدة تجعلها مختلفة عن الجرائم التقليدية، يمكن أن تسبب خسائر مالية ضخمة، وتؤدي إلى سرقة المعلومات الحساسة، وانتهاك الخصوصية، وتعطيل البنية التحتية الحيوية.

أهداف الدراسة:

تهدف دراستنا إلى تحقيق عدة أهداف رئيسية تتعلق بالتحقيق الجنائي في الجرائم الإلكترونية والمتمثلة في:

1. توضيح الجهود الوطنية والدولية لمكافحة هذا النوع من الإجرام.
2. دراسة الأساليب والتقنيات المستخدمة في التحقيق الجنائي للجرائم الإلكترونية.
3. جمع الأدلة الرقمية وتحليلها، والتعامل مع الجرائم العابرة للحدود.

إشكالية الدراسة:

يمكن صياغة إشكالية حول موضوع التحقيق الجنائي في الجرائم الإلكترونية على النحو التالي:

ما مدى فعالية التحقيق الجنائي في الجرائم الإلكترونية؟

منهج الدراسة:

نظرا لخصوصية الموضوع وطبيعته القانونية التي تفرض المنهج المتبع فقد اخترنا أن نتبع منهجا يلم إلى حد ما بدراسة هذا الموضوع من مختلف جوانبه ألا وهو المنهج الوصفي الذي يقوم على وصف هذه الظاهرة الإجرامية المستحدثة.

الدراسات السابقة:

الدراسة الأولى:

نادية البلوشي" **التدريب والتأهيل للمحققين الجنائيين في الجرائم الإلكترونية**"، مذكرة لنيل شهادة ماستر، إنطلقت من إشكالية التالية" كيف يمكن تحسين برامج التدريب والتأهيل للمحققين الجنائيين في الجرائم الإلكترونية لضمان تحقيق فعالية التحقيقات مع احترام حقوق الخصوصية؟"، تهدف الدراسة إلى تقييم البرامج التدريبية المتاحة للمحققين في مجال الجرائم الإلكترونية، تقديم توصيات لتحسين جودة التدريب وتعزيز مهارات المحققين.

الدراسة الثانية:

خالد المري" **استخدام التقنيات الحديثة في التحقيقات الجنائية الرقمية**"، مذكرة لنيل شهادة ماستر، إنطلقت من إشكالية التالية" ما هي الفوائد والمخاطر المرتبطة باستخدام التقنيات الحديثة في التحقيقات الجنائية الرقمية وكيف يمكن تحقيق توازن بينها؟"، تهدف الدراسة إلى دراسة كيفية استخدام التقنيات الحديثة في التحقيقات الجنائية الرقمية، تحليل الفوائد والمخاطر المرتبطة باستخدام الذكاء الاصطناعي وتحليل البيانات.

تقسيمات الدراسة:

وقد اتبعنا في دراستنا لهذا الموضوع خطة ترتكز على فصلين فتناولنا في الفصل الأول الإطار المفاهيمي لتحقيق الجنائي الجرائم الإلكترونية بدأنا ماهية تحقيق الجنائي الجرائم الإلكترونية كمبحث أول انتقالا إلى خصائص تحقيق الجنائي في الجرائم الإلكترونية كمبحث ثاني أما الفصل الثاني يحتوي على إجراءات التحقيق الجنائي في الجرائم الإلكترونية انطلاقا من إجراءات التحقيق الجنائي المألوفة في الجرائم الإلكترونية كمبحث أول ثم إجراءات التحقيق الجنائي الخاصة في الجرائم الإلكترونية كمبحث ثاني.

الفصل الأول

تطور التكنولوجيا وانتشار استخدام الإنترنت والأجهزة الذكية أدى إلى ظهور الجريمة الإلكترونية كظاهرة إجرامية حديثة. هذه التكنولوجيا المتطورة توفر للمجرمين فرصًا جديدة لارتكاب الجرائم وتحديث أساليبهم، مما يجعلها تشكل تحديات جديدة لقوى الأمن والسلطات التشريعية.

من خلال استخدام الإنترنت، يمكن للمجرمين الوصول إلى معلومات شخصية، والقيام بعمليات احتيالية، وسرقة البيانات، وتنفيذ هجمات سيبرانية على الأنظمة والشبكات. بالإضافة إلى ذلك، استخدام الأجهزة الذكية مثل الهواتف الذكية والأجهزة اللوحية يتيح للمجرمين الوصول إلى البيانات الحساسة للأفراد والشركات والمؤسسات.

مكانة الجريمة الإلكترونية في مجال الجريمة والأمن كبيرة جدًا، وهذا بسبب قدرتها على التأثير على الفرد والمجتمع بشكل واسع النطاق، بالإضافة إلى التحديات التقنية والقانونية التي تواجه جهود مكافحتها[1].

وعليه قسمنا الفصل إلى:

المبحث الأول ماهية تحقيق الجنائي الجرائم الإلكترونية.

المبحث الثاني خصائص تحقيق الجنائي في الجرائم الإلكترونية.

[1]- أحمد مسعود مريم، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة لنيل شهادة ماجستير في القانون الجنائي، جامعة ورقلة 2013، ص22.

المبحث الأول: ماهية تحقيق الجنائي الجرائم الإلكترونية

أثيرت العديد من التساؤلات حول تحديد الطبيعة القانونية للجريمة الإلكترونية، ويرجع سبب ذلك إلى تعدد وجهات النظر بخصوص هذا النوع من الجرائم، حيث ظهرت عدة آراء فقهية في محالة فهم المقصود بالجريمة الإلكترونية.

أما التحقيق هو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل اسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه الأدلة القائمة على الجريمة. والتحقيق في الجرائم الإلكترونية يختلف عن التحقيق في الجرائم العادية من حيث الإجراءات وذلك لحادثة هذه الجريمة ومهارة مرتكبيها في الإجرام ومحو الأدلة.[1]

وعليه سنتطرق إلى مفهوم الجريمة الإلكترونية في المطلب الأول، أما في المطلب الثاني سنذكر مفهوم التحقيق الجنائي ومحقق الجنائي.

المطلب الأول: مفهوم الجريمة الإلكترونية

أن تعريف الجريمة الإلكترونية قد شهد تنوعًا كبيرًا وظهور مصطلحات متعددة للإشارة إليها. يمكن أن تكون الجرائم الإلكترونية تشمل مجموعة واسعة من الأنشطة الإجرامية التي تتعلق بالتكنولوجيا الرقمية، مثل الاحتيال عبر الإنترنت، والتطفل السيبراني، وسرقة الهوية الرقمية، والتجسس الإلكتروني، والابتزاز الإلكتروني، والاعتداء الجنسي عبر الإنترنت، وغيرها.[2]

[1]- راهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص قانون كلية الحقوق جامعة تيزي وزو، 2018، ص16.

[2]- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير جامعة تبسة، 2013، ص32.

بالنسبة لتعريف الجريمة الإلكترونية، فقد تتباين التعاريف وفقًا للمنظور والسياق القانوني للدولة أو الهيئة التي تقوم بوضع التعريف. ومن الصعب بالفعل وضع تعريف محدد وجامع للجريمة الإلكترونية بسبب تطور التكنولوجيا وتعقيدات الأنشطة الجنائية المتصلة بها.

بعض الفقهاء يرون أن الجرائم الإلكترونية مجرد امتداد للجرائم التقليدية إلى عالم الإنترنت والتكنولوجيا الرقمية، وبالتالي قد يرفضون وضع تعريف محدد لها، مؤكدين أنها تندرج ضمن القوانين الجنائية العامة.

مع تزايد الحاجة إلى التصدي للجرائم الإلكترونية، يمكن أن يكون من المفيد للتشريعات والمؤسسات القانونية تطوير تعاريف محددة للجريمة الإلكترونية تمكن من مكافحتها بشكل فعال، مع مراعاة التطورات التكنولوجية والتحديات القانونية المتزايدة[1].

الفرع الأول: تعريف الجريمة الإلكترونية لغة

كلمة "جريمة" تأتي من اللغة العربية ولها أصل في كلمة "جرم" التي تعني الذنب أو الخطأ القابل للعقاب. وفي اللغة العربية، تُستخدم كلمة "جريمة" للدلالة على الأفعال أو الأنشطة غير القانونية التي يقوم بها شخص ما والتي تتسبب في إلحاق ضرر بالآخرين أو بالمجتمع بشكل عام.

تتميز كلمة "جريمة" بمزيج من المعاني القانونية والأخلاقية، حيث تشير إلى انتهاك قانوني للقواعد واللوائح المعترف بها في المجتمع، وقد تترتب على الجريمة عواقب قانونية مثل العقوبات القضائية. [2]

[1]- سعيداني نعيم، مرجع سابق، ص34.
[2]-خالد ممدوح، أمن الجريمة الإلكترونية الدار الجامعية الإلكترونية، الإسكندرية، 2008، ص 41.

باعتبار أن الجريمة تتضمن فعلاً غير قانوني ويترتب عليه عواقب قانونية، فإنها تحمل معنى أكثر ارتباطاً بالقوانين والتشريعات في المجتمع. وتستخدم الجريمة كمصطلح للإشارة إلى تلك الأفعال التي تعتبر غير قانونية وتسبب ضررًا للآخرين أو للمجتمع ككل[1].

الفرع الثاني: تعريف الجريمة اصطلاحا

تعريف الجريمة في الفقه الإسلامي يعتمد بشكل رئيسي على النصوص الشرعية والأحكام السلطانية، وغالبًا ما يتم الرجوع فيه إلى المصادر الرئيسية للقانون الإسلامي والتفسيرات الفقهية. وفي ضوء ذلك، يمكن تلخيص تعريف الجريمة في الفقه الإسلامي بأنها مخالفات للشريعة الإسلامية تُحظر وتُعاقب عليها، سواء بحدود معينة أو تعزيرات أخرى تُقررها السلطات القضائية.

تصف التعريفات الفقهية الجرائم عادةً بأنها مخالفات للأوامر والنواهي الشرعية، وتشمل الأفعال التي تعتبر محرمة أو محظورة شرعًا. تتنوع هذه الأفعال بين المخالفات المتعلقة بالحقوق الشخصية مثل القتل والإساءة والسرقة، والمخالفات المتعلقة بالحقوق المالية مثل الاحتيال والغش في التعاملات المالية، والمخالفات الاجتماعية مثل الزنا والخمر وغيرها[2].

تعتبر هذه التعريفات أساسًا للتفكير في القوانين والأنظمة القانونية التي تُنظم الجرائم في المجتمعات الإسلامية، وتحدد العقوبات المناسبة لمرتكبيها وفقًا للقوانين الدينية والقوانين المدنية المعمول بها. ويُعتبر الاعتماد على المبادئ الشرعية في تحديد الجرائم وعقوباتها جزءًا من النظام القانوني في العديد من البلدان ذات الأغلبية الإسلامية[3].

[1]- خالد ممدوح، مرجع سابق، ص41.
[2]-ضياء مصطفى عثمان السرقة الإلكترونية، دار النفائس، عمان، الطبعة الأولى، 2011، ص32.
[3]- سعيداني نعيم، مرجع سابق، ص36.

الفرع الثالث: تعريف الجريمة الإلكترونية فقها

تفسير مفهوم الجريمة الإلكترونية يتنوع بناءً على وجهات النظر الفقهية والقانونية والتقنية المختلفة. بعض الأشخاص والمؤلفين يميلون إلى ضيق مفهوم الجريمة الإلكترونية، حيث يركزون على الحالات التي تتطلب مستوى عالٍ من المعرفة التقنية لارتكابها ومعالجتها.

وفي هذا السياق، يعتبر أنصار هذا الاتجاه الجريمة الإلكترونية كأي فعل غير مشروع يتطلب مستوى مهارة تقنية معينة لارتكابه، وأن المعرفة بتكنولوجيا الحاسوبات الآلية بشكل كبير لازمة لفهمها وملاحقتها وتحقيقها. وقد يتضمن ذلك الاعتداءات التي تهدف إلى الحصول على مكاسب مالية أو استغلال البيانات بطرق غير مشروعة[1].

من الناحية الفقهية، يمكن لهذا الاتجاه أيضًا أن يركز على المعيار الناتج عن نتيجة الاعتداء، حيث يعتبر الهدف من الجريمة الإلكترونية هو تحقيق ربح أو مكاسب مالية. وبناءً على هذا التفسير، يمكن أن تشمل الجرائم الإلكترونية أنشطة مثل الاحتيال عبر الإنترنت والتلاعب بالبيانات والاختراقات السيبرانية التي تهدف إلى الاستيلاء على المعلومات الشخصية أو الحساسة بغرض الربح أو التلاعب بالأسواق أو التأثير على السياسات.

هذا الاتجاه يسلط الضوء على الجوانب التقنية والمادية للجرائم الإلكترونية، وقد يكون له تأثير على كيفية تحديد الجرائم وتطبيق العقوبات عليها في النظام القانوني[2].

الفرع الرابع: تعريف الجريمة الإلكترونية القانوني

تعريف المشرع الجزائري للجرائم المتصلة بتكنولوجيا المعلومات والاتصالات يركز بشكل كبير على المساس بأنظمة المعالجة الآلية والبيانات المحددة في قوانين العقوبات، بالإضافة

[1]- فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري و اليمني، أطروحة لنيل شهادة الدكتوراه في القانون، فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق جامعة الجزائر 1، الجزائر،2011، ص28.

[2]- طيبي الطيب، البحث والتحقيق في جريمة تبييض الأموال في التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في الحقوق جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية قسم الحقوق الجزائر 2012، ص18.

إلى أي جريمة أخرى يمكن أن ترتكب أو تُسهل ارتكابها عن طريق الأنظمة المعلوماتية أو شبكات الاتصال.

هذا التعريف يعكس الاهتمام بتطور التكنولوجيا وتأثيرها على الجريمة، حيث يشمل الجرائم التي تتعلق بالتدخل في أنظمة المعلومات الآلية والبيانات المخزنة بها، وكذلك الجرائم التي ترتبط بالاستفادة من الشبكات الإلكترونية لارتكاب الجرائم التقليدية[1].

بالتركيز على النظم المعلوماتية وشبكات الاتصال، يتيح هذا التعريف إمكانية فحص الجرائم الإلكترونية بشكل أكثر دقة وتحديد الإجراءات القانونية والتقنية اللازمة لمكافحتها. وبالنظر إلى تطور التكنولوجيا وتوسع استخدام الإنترنت ووسائل الاتصال الإلكترونية، يعد هذا التعريف أحد الخطوات الهامة في تطوير التشريعات الجزائرية لمواكبة التحديات الحديثة في مجال مكافحة الجريمة[2].

تركز تعريفات الجرائم المتصلة بتكنولوجيا المعلومات والاتصال على عدة جوانب مهمة:

1. **المساس بأنظمة المعالجة الآلية للمعلومات:** يشمل هذا المفهوم التلاعب أو الاختراق أو الاعتداء على البنية التحتية للمعلومات، مما يعني أن الجريمة تستهدف الأنظمة الحاسوبية والبيانات المخزنة بها.
2. **الجرائم التي يسهل ارتكابها عن طريق الأنظمة المعلوماتية أو شبكات الاتصال:** يُشير هذا المفهوم إلى الجرائم التي يمكن ارتكابها أو تسهيل ارتكابها باستخدام التقنيات الحديثة للاتصال، مما يتيح فرصًا لارتكاب جرائم تقليدية بشكل أكثر فعالية[3].

تحديد نطاق الجريمة الإلكترونية بهذه الطريقة يسهل تحديد الإجراءات القانونية والتقنية اللازمة لمكافحتها، ويُظهر التحدي الذي تواجهه القوانين في مواكبة التطورات التكنولوجية

[1]- بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة ماجستير 2014 ، ص 09.
[2]- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، 2010، ص15.
[3]-فايز محمد راجح غلاب، مرجع سابق، ص30.

ومكافحة الجرائم الإلكترونية بفعالية. يوضح هذا التعريف الاهتمام المستمر بتحسين الأدوات القانونية والتشريعات لمواكبة التحديات المتعلقة بالجرائم الإلكترونية في العصر الرقمي[1].

وعلى خلاف المشرع الفرنسي الذي لم يعطي تعرفا للجريمة الإلكترونية فإن المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب المادة 02 من القانون 09-04 على أنها " جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".[2]

تُظهر هذه المقارنة بين المشرع الجزائري والمشرع الفرنسي الفروق في التعريفات القانونية للجريمة الإلكترونية. في حين أن المشرع الفرنسي لم يقدم تعريفًا صريحًا للجريمة الإلكترونية، قام المشرع الجزائري بتصنيفها تحت مصطلح "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال."

تحديد الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في القانون الجزائري يركز على الجوانب التقنية والقانونية لهذه الجرائم، ويعكس تطور التكنولوجيا وتأثيرها على الجريمة. يشمل هذا التعريف الجرائم التي تتعلق بالتدخل في أنظمة المعلومات الآلية والبيانات المخزنة بها، بالإضافة إلى الجرائم التي يمكن ارتكابها أو تسهيل ارتكابها باستخدام منظومات المعلومات أو أنظمة الاتصالات الإلكترونية[3].

هذا التعريف يعكس الاهتمام بتطوير التشريعات لمواكبة التحديات الحديثة في مجال مكافحة الجريمة الإلكترونية، ويُظهر التحدي الذي تواجهه القوانين في مواكبة التطورات التكنولوجية ومكافحة الجرائم الإلكترونية بفعالية. يتيح هذا التعريف للسلطات القضائية والأمنية

[1]-فايز محمد راجح غلاب، مرجع سابق، ص30.
[2]- المادة 02 من قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 2009.
[3]- بخي فاطمة الزهراء، مرجع سابق، ص16.

والقانونية تحديد الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال واتخاذ الإجراءات اللازمة لمكافحتها بفعالية.

اعتمد المشرع الجزائري مجموعة من المعايير لتعريف الجريمة الإلكترونية، مما يعكس تعقيد هذه الظاهرة وتطورها السريع. أحد هذه المعايير هو معيار وسيلة الجريمة، الذي يرتبط بنظام الاتصالات الإلكترونية والأجهزة والتقنيات ذات الصلة. كما يشمل المعيار الثاني موضوع الجريمة، وهو المساس بأنظمة المعالجة الآلية للبيانات، مما يعني التلاعب أو الاختراق أو الاعتداء على البنية التحتية للمعلومات. وأخيرًا، يُعتبر معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات[1].

من خلال تحديد نطاق الجريمة الإلكترونية بأنها ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، يوسع المشرع الجزائري مجال الجرائم الإلكترونية في القانون، حيث يمكن للجرائم الإلكترونية أن تشمل أي نشاط يتعلق بالمعلوماتية أو استخدام التقنيات الحديثة للقيام بأعمال غير قانونية أو مخالفة للأخلاق. هذا يُظهر التحدي الذي تواجهه القوانين في مواكبة التطورات التكنولوجية ومكافحة الجرائم الإلكترونية بفعالية.

تعكس المعايير التي اعتمدها المشرع الجزائري لتعريف الجريمة الإلكترونية تعقيد هذه الظاهرة وتطورها السريع، وتساعد في تحديد نطاق الجريمة الإلكترونية بشكل دقيق. إليك شرحاً لهذه المعايير[2]:

1. **معيار وسيلة الجريمة** :يتعلق هذا المعيار بالأدوات والتقنيات المستخدمة في ارتكاب الجريمة الإلكترونية. يشمل ذلك نظام الاتصالات الإلكترونية، مثل الإنترنت والشبكات اللاسلكية، بالإضافة إلى الأجهزة والتقنيات ذات الصلة مثل الحواسيب والهواتف الذكية.

[1]- بخي فاطمة الزهراء، مرجع سابق، ص18.
[2]-فايز محمد راجح غلاب، مرجع سابق، ص32.

2. **معيار موضوع الجريمة** :يركز هذا المعيار على طبيعة الجرائم الإلكترونية والمساس بأنظمة المعالجة الآلية للبيانات. يتضمن ذلك التلاعب بالبيانات، والاختراقات، والاعتداءات على البنية التحتية للمعلومات، وكل ما يتعلق بالاستيلاء على المعلومات أو التلاعب بها بطرق غير قانونية.

3. **معيار القانون الواجب التطبيق** :يحدد هذا المعيار الأسس القانونية والركن الشرعي للجريمة المنصوص عليها في قوانين العقوبات. يساعد ذلك في تحديد الإجراءات القانونية اللازمة لمكافحة الجرائم الإلكترونية وتطبيق العقوبات على المرتكبين[1].

بتحديد نطاق الجريمة الإلكترونية بأنها ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، يوسع المشرع الجزائري مجال الجرائم الإلكترونية في القانون، مما يتيح للسلطات القانونية والأمنية تحديد الجرائم ومكافحتها بفعالية. هذا يظهر التحدي الذي تواجهه القوانين في مواكبة التطورات التكنولوجية ومكافحة الجرائم الإلكترونية بفعالية في العصر الرقمي[2].

المطلب الثاني: مفهوم التحقيق الجنائي ومحقق الجنائي

التحقيق هو عملية أساسية بعد وقوع الجريمة لضمان العدالة وتحديد المسؤولين. يهدف التحقيق إلى جمع الأدلة والمعلومات ذات الصلة بالجريمة، وتحليلها بدقة لتحديد الحقائق وتحديد المشتبه بهم بطريقة قانونية وعادلة. تشمل عملية التحقيق استجواب الشهود، وجمع الأدلة المادية، وتحليل البيانات، واستخدام التقنيات الخاصة بالتحقيق الجنائي.

تكمن أهمية التحقيق في ضمان تحقيق العدالة ومحاسبة المسؤولين عن الجرائم، ويعد ضرورياً لتطبيق القانون بشكل فعال وإنصافي. تقوم السلطات القضائية والأمنية بإجراء التحقيقات بشكل دقيق ومنهجي للوصول إلى الحقيقة وضمان تقديم المتهمين إلى العدالة[3] .

[1]-فايز محمد راجح غلاب، مرجع سابق، ص32.
[2]- خالد ممدوح، مرجع سابق، ص45.
[3]- طيبي الطيب، مرجع سابق، ص20.

الفرع الأول: تعريف التحقيق الجنائي في الجريمة الإلكترونية

يتم التحقيق في الجرائم الإلكترونية بطريقة مشابهة للتحقيق في الجرائم الأخرى في العديد من النواحي. ومع ذلك، هناك بعض الاختلافات الفريدة فيما يتعلق بالتقنيات المستخدمة والمعرفة المطلوبة لجمع وتحليل الأدلة الرقمية.

التحقيق الجنائي في الجرائم الإلكترونية يهدف إلى جمع الأدلة وتحليلها بطريقة متخصصة.

يعكس جوهر التحقيق في الجرائم بشكل دقيق ومنهجي. حيث يركز التحقيق على جمع الأدلة والمعلومات بشكل مباشر ومنهجي، وتحليلها بعناية لكشف الحقيقة وكشف ملابسات الجريمة. يتطلب هذا العمل الجاد والمستمر للوصول إلى الحقيقة وتقديم العدالة[1].

باستخدام الأدوات والتقنيات المناسبة، يعمل المحققون على جمع الأدلة من مصادر مختلفة وتحليلها بدقة لضمان صحة النتائج. كما يتطلب التحقيق احترام الإجراءات والقوانين المعمول بها، وضمان حقوق جميع الأطراف المعنية، سواء كانوا مشتبه بهم أو شهودًا أو ضحايا.

تحديد التفاصيل وتوثيق الأدلة يسهم في بناء القضية بشكل قوي، مما يمكن المحققين من تقديم تقارير شاملة ودقيقة للسلطات القضائية لاتخاذ القرارات المناسبة. هذا التعريف يبرز الأهمية الكبيرة لدور التحقيق في تحقيق العدالة ومكافحة الجريمة بفعالية[2].

في حالة الجرائم الإلكترونية، يتطلب التحقيق استخدام تقنيات التحقيق الرقمي المتقدمة لتحليل الأدلة الرقمية وتقديمها بشكل قانوني وموثوق به أمام المحكمة. يتمثل التحدي الرئيسي

---

[1]- بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق جامعة محمد خيضر بسكرة كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر 2016، ص18.

[2]-بن كثير بن عيسى، الإجراءات الخاصة المطبقة على الإجرام الخطير، نشرة القضاة، مديرية الدراسات القانونية والوثائق، العدد 63، 2008، ص68.

في التحقيق في الجرائم الإلكترونية في جمع الأدلة الرقمية بطريقة تحافظ على سلامتها وموثوقيتها وتوثيقها بشكل صحيح لاستخدامها في إثبات الجريمة وتقديم المتهمين إلى العدالة.

وعرف التحقيق أنه مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها الإحالة المتهم إلى المحاكمة، كذلك هو مجموعة الإجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانونا، بغية تمحيص الأدلة والكشف عن الحقيقة قبل مرحلة المحاكمة[1] .

وكذلك عرف التحقيق بأنه "مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط والأوضاع المحددة قانونا بهذا التنقيب عن الأدلة وتقديرها والكشف عن الحقيقة في شأن جريمة ارتكبت كتقدير لزوم محاكمة المدعي عليه أو عدم لزومها."

هذه التعاريف تسلط الضوء على جوانب مهمة من التحقيق، حيث يُفهم التحقيق باعتباره سلسلة من الإجراءات المنظمة والمتسلسلة التي تستهدف جمع الأدلة وتحليلها فيما يتعلق بجريمة معينة. يتضمن التحقيق جمع الأدلة وتقديرها لتحديد كفايتها والتوصل إلى قرار بشأن إحالة المتهم إلى المحاكمة أو عدم لزومها[2].

وبموجب هذه التعاريف، يتضح أن التحقيق يعتبر مرحلة حاسمة في العملية القانونية، حيث يتم خلاله تحليل الأدلة والكشف عن الحقيقة بشكل دقيق ومنهجي. يعتمد نجاح التحقيق على اتباع الإجراءات القانونية المحددة والتي تكفل حقوق جميع الأطراف المعنية، بما في ذلك المتهمين والمجني عليهم[3].

---

[1]-بن كثير بن عيسى، مرجع سابق، ص68.

[2]-غسان مدحت الخبري أصول التحقيق الإبتدائي كحق من حقوق الإنسان دار الراية للنشر والتوزيع، الأردن، ط1، 2013، ص45.

[3]- بعرة سعيدة، مرجع سابق، ص19.

تُسلط هذه التعاريف الضوء على أهمية دور السلطات المختصة بالتحقيق في ضمان العدالة وتحقيق الحقيقة بشكل صحيح وفعّال. فعملية التحقيق تمثل الخطوة الأولى والحاسمة في سلسلة إنفاذ القانون، وتؤثر بشكل كبير على نتائج المحاكمات والعدالة العامة[1].

باعتبار أن التحقيق يتم بموجب القوانين والأنظمة القانونية المعتمدة، يُعزز الالتزام بالمعايير القانونية والأخلاقية الصارمة الثقة في نتائج التحقيق وفي العدالة نفسها. فهو يضمن حقوق المشتبه بهم والمتضررين على حد سواء، ويسهم في تقديم المعلومات والأدلة القوية التي تساعد في اتخاذ القرارات الصحيحة بشأن المتهمين.

بالإضافة إلى ذلك، يُعزز دور السلطات المختصة بالتحقيق ثقة الجمهور في نظام العدالة الجنائية، حيث يعكس التزامها بالشفافية والنزاهة والمساءلة المطلوبة. وبهذا الشكل، يلعب التحقيق دورًا حيويًا في حماية حقوق الأفراد وضمان تحقيق العدالة الفعّالة والموضوعية[2].

الفرع الثاني: تعريف المحقق الجنائي

ذهب جانب من الفقه إلى تعريف المحقق بأنه" كل من عهد إليه القانون بتحري الحقيقة في البلاغات والحوادث الجنائية، وتحقيقها ويسهم بدوره في كشف غموضها وصولا إلى معرفة حقيقية الحادث وكشف مرتكبيه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة".

كما عرف البعض المحقق أو الباحث الجنائي بأنه الشخص الذي يتولى ويتكلف بالتحقيق والتحري والبحث وجمع الأدلة لكشف غموض الحوادث ويتحدد دوره بالعمل على منع الجريمة قبل وقوعها أو اكتشافها بعد وقوعها، وضبط مرتكبيها والأدوات التي استعملت فيها.[3]

---

[1]- محمد طارق عبد الرؤوف، جريمة الإحتيال عبر الإنترنت الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، الطبعة الأولى 2011، ص 230.

[2]- خالد ممدوح إبراهيم فن التحقيق الجنائي الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009، ص56.

[3]- عمر بن إبراهيم بن حماد العمر، إجراءات الشهادة في مرحلة الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمينة، 2007، ص 22

وعرف المحقق بأنه "ذلك الشخص الذي عهد غليه قانونا باتخاذ كافة الإجراءات القانونية والوسائل المشروعة فيما يصل إلى عمله من جرائم بهدف الكشف عن غموضها وضبط فاعلها وتقديمه للمحاكمة".[1]

هذا التعاريف تعكس دور المحقق كمن يكلفه القانون بتحري الحقيقة في البلاغات والحوادث الجنائية، وتحقيقها بشكل مستقل وموضوعي. يهدف المحقق في هذا السياق إلى كشف الحقائق والتوصل إلى معرفة الحقيقة الكاملة حول الحادث أو الجريمة المعنية، وذلك بغية تحديد المسؤولين عنها وتقديمهم إلى المحاكمة.

باعتبار المحقق كشخص يحمل مسؤولية كبيرة للبحث عن الحقيقة، فإنه يجب أن يكون لديه المهارات الفنية والقانونية اللازمة لتحقيق هذا الهدف. يتطلب ذلك القدرة على جمع الأدلة بشكل فعال وتحليلها بشكل منهجي، بالإضافة إلى احترام الإجراءات القانونية وحقوق الأطراف المعنية[2].

هذا التعريف يبرز أهمية دور المحقق في تحقيق العدالة وتحديد المسؤوليات، حيث يسهم بشكل كبير في كشف الجرائم وتقديم المتهمين إلى المحاكمة، وبالتالي يسهم في تطبيق القانون وضمان سلامة المجتمع.

أما المشرع الجزائري فقد وضع تعرفا لقاضي التحقيق في المادة 68 من قانون الإجراءات الجزائية حيث جاء في نصها ما يلي "يقوم قاضي التحقيق وفقا لقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام وأدلة النفي"[3].

---

[1]- حسن الجوخندار، التحقيق الابتدائي في قانون الأصول المحاكمات الجزائية، دار الثقافة عمان، الطبعة الأولى، 2008، ص11.

[2]- عمر بن إبراهيم بن حماد العمر، مرجع سابق، ص24.

[3]- المادة 68 من الأمر رقم 20-04 المؤرخ في 11 محرم عام 1442 الموافق 30 غشت سنة 2020، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية. (الجريدة الرسمية عدد 51 لسنة 2020).

تعريف قاضي التحقيق الذي وضعته القوانين الجزائرية يوضح دوره الأساسي في تحقيق العدالة وكشف الحقيقة في القضايا الجنائية. وفقًا لما جاء في المادة 68 من قانون الإجراءات الجزائية، يقوم قاضي التحقيق باتخاذ جميع الإجراءات التي يراها ضرورية للكشف عن الحقيقة، ويشمل ذلك التحري عن أدلة الاتهام وأدلة النفي.

هذا يعني أن قاضي التحقيق له سلطة واسعة للقيام بالتحقيقات اللازمة، بما في ذلك إصدار أوامر التحري واستجواب الشهود والمشتبه بهم، وجمع الأدلة الفنية والمادية، وتقديم التقارير والتوصيات إلى النيابة العامة[1].

دور قاضي التحقيق أساسي في مرحلة ما قبل المحاكمة، حيث يقوم بجمع الأدلة وتحليلها وتقديمها إلى السلطات القضائية المختصة لاتخاذ القرارات المناسبة بشأن متابعة المشتبه بهم وتوجيه التهم اللازمة.

هذا التعريف يظهر أهمية دور قاضي التحقيق في إنفاذ القانون وتحقيق العدالة، وضمان تطبيق القوانين بشكل صحيح وفقًا للمبادئ القانونية وحقوق الأفراد[2].

[1]- عمر بن إبراهيم بن حماد العمر، مرجع سابق، ص25.
[2]- محمد طارق عبد الرؤوف، مرجع سابق، ص233.

المبحث الثاني: خصائص تحقيق الجنائي في الجرائم الإلكترونية

مرحلة التحقيق الابتدائي تمثل الخطوة الأولى والحيوية في عملية التحقيق في الجرائم، وخاصةً فيما يتعلق بالجرائم الإلكترونية. ففي هذه المرحلة، يتم جمع الأدلة والمعلومات الأولية التي تساعد في تحديد تفاصيل الجريمة وتحديد المشتبه بهم.

تتطلب الجرائم الإلكترونية تحقيقاً متخصصاً وفريقاً مجهزاً بالمهارات التقنية اللازمة لجمع الأدلة الرقمية والتحليل الرقمي. فالبيانات الرقمية يمكن أن تكون زلزالية في تقديم الأدلة التي تثبت الجريمة وتحديد الجاني[1].

ومع تطور التكنولوجيا، يجب أن يكون لدى المحققين الجنائيين فهم عميق للتكنولوجيا والوسائل الرقمية، بالإضافة إلى القدرة على التكيف مع التطورات الجديدة في مجال الجريمة الإلكترونية. يتطلب هذا المعرفة المستمرة والتدريب المستمر لضمان أن يكون للمحققين الجنائيين المهارات والقدرات اللازمة للتعامل مع هذه التحديات بفعالية.

باستخدام أساليب التحقيق المتقدمة والمتطورة، يمكن للمحققين جمع الأدلة الرقمية بكفاءة وفحصها بدقة للكشف عن الحقيقة وتقديم الجانيين إلى العدالة. هذا يبرز أهمية تطوير وتحديث أساليب التحقيق لمواكبة التطورات التكنولوجية ومواجهة التحديات المتزايدة في مجال مكافحة الجريمة الإلكترونية[2].

وعليه سنتطرق إلى أسلوب التحقيق الابتدائي في الجرائم الإلكترونية في المطلب الأول، أما في المطلب الثاني سنذكر عناصر التحقيق الابتدائي في الجرائم الإلكترونية.

---

[1]- فوزي عمارة، إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية كلية الحقوق والعلوم السياسية جامعة منتوري قسنطينة ، العدد 33 جوان 2010، ص59.

[2]- براهيمي جمال، مرجع سابق، ص26

المطلب الأول: أسلوب التحقيق الابتدائي في الجريمة الإلكترونية

التحقيق يشمل مجموعة من الإجراءات والتقنيات التي تُستخدم لكشف الجريمة وتحديد مرتكبيها، ويختلف من جريمة لأخرى في طرق وأساليب التحقيق المستخدمة. في الجرائم الإلكترونية، يتطلب التحقيق استخدام تقنيات خاصة تتعلق بالتحقيق الرقمي، والتي تشمل تحليل البيانات الرقمية، واسترجاع المعلومات من الأجهزة الإلكترونية، وتقديم الأدلة الرقمية أمام المحكمة.

من خلال التحقيق الابتدائي، يتم تحديد تفاصيل الجريمة بدقة، بما في ذلك نوع الجريمة، وهوية المشتبه بهم، وهوية المتضررين، والأدوات والتقنيات المستخدمة في ارتكاب الجريمة. يسعى المحققون لتحديد سبب ووضعية الجريمة، وتحليل الأدلة المتاحة لديهم بعناية لتطويق المشتبه بهم وتقديمهم للعدالة[1].

تطبيق منهج تحقيقي متخصص يعتبر أساسياً في التحقيق في الجرائم الإلكترونية، حيث يحتاج المحققون إلى الفهم العميق للتكنولوجيا والأساليب الرقمية، بالإضافة إلى القدرة على تحليل البيانات الضخمة وتحديد الأدلة الرقمية الملائمة. هذا يعزز الفرص لضمان تحقيق العدالة وتقديم المتهمين إلى المحاكمة بناءً على أدلة موثوقة وقوية[2].

الفرع الأول: وضع خطة عمل التحقيق

الخطوات التي تم ذكرها تمثل جزءًا أساسيًا من عملية التحقيق في الجرائم الإلكترونية، وهي تساهم في تنظيم وتنفيذ التحقيق بشكل فعال ومنهجي. إليك بعض النقاط الرئيسية التي يجب مراعاتها[3]:

---

[1]- حسن الجوخندار، مرجع سابق، ص23.

[2]- عمر بن إبراهيم بن حماد العمر، مرجع سابق، ص39.

[3]-آمال بن صوليح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني وفي الجزائر، مداخلة الملتقي الدولي حول " الإجرام الييبرالي المفاهيم والتحديات ، 11-12 أفريل 2017، ص14.

أولا: وضع الخطة المناسبة

تحديد خطة تحقيق دقيقة ومناسبة يعتبر أمرًا حيويًا لضمان نجاح عملية التحقيق في الجرائم الإلكترونية. إليك الخطوات التي يمكن اتخاذها لوضع الخطة المناسبة[1]:

1. **تحليل المعلومات الأولية** :يبدأ العمل بتحليل المعلومات الأولية المتاحة حول الجريمة، وذلك لفهم جوانبها المختلفة وتحديد أولويات التحقيق.
2. **تحديد الأهداف** :يتعين تحديد أهداف التحقيق بشكل واضح ودقيق، مثل تحديد هوية المتهمين، وجمع الأدلة الرقمية، وتحديد أساليب ارتكاب الجريمة.
3. **تحديد الخطوات والإجراءات** :بناءً على الأهداف، يتم تحديد الخطوات والإجراءات اللازمة لتحقيقها، بما في ذلك استخدام التقنيات الرقمية والتعاون مع الخبراء التقنيين.
4. **تحديد الموارد اللازمة** :يجب تحديد الموارد البشرية والتقنية اللازمة لتنفيذ الخطة بشكل فعال، مثل توظيف المحققين ذوي الخبرة واستخدام الأدوات والبرامج اللازمة[2].
5. **وضع جدول زمني** :يتم تحديد جدول زمني محدد لتنفيذ كل خطوة من خطة التحقيق، بما في ذلك المواعيد النهائية لتقديم التقارير والنتائج.
6. **متابعة وتقييم الأداء** :يجب متابعة تقدم التحقيق بانتظام وتقييم أداء الفريق، وإدارة أي تحديات تنشأ خلال العملية.
7. **توثيق العملية** :يجب توثيق جميع الخطوات والإجراءات المتخذة خلال عملية التحقيق، بما في ذلك الأدلة المجمعة والتحليلات المقدمة[3].

[1]- آمال بن صوليح، مرجع سابق، ص19.
[2]- فوزي عمارة، مرجع سابق، ص62.
[3]- حسن الجوخندار، مرجع سابق، ص29.

من خلال اتباع هذه الخطوات ووضع خطة تحقيق شاملة ومناسبة، يمكن تحقيق نتائج فعالة وتقديم المتهمين إلى المحاكمة بناءً على أساس قوي من الأدلة والتحليلات[1].

ثانيا: التخطيط الفني

تحقيق الجرائم الإلكترونية يتطلب فعلاً فريقًا متخصصًا يمتلك المعرفة التقنية العالية والخبرة في التحقيقات الرقمية. إليك بعض الخطوات التي يمكن اتخاذها في وضع خطة تحقيق فنية[2]:

1. **تحديد الأهداف التقنية** :يجب تحديد الأهداف التقنية للتحقيق، مثل استرجاع البيانات، وتحليل الأدلة الرقمية، وتقديم الأدلة أمام المحكمة بشكل فعال.
2. **تقييم الأدوات والتقنيات المتاحة** :يجب تقييم الأدوات والتقنيات المتاحة للتحقيق الرقمي، مثل برمجيات استرجاع البيانات وتحليلها، وأجهزة التحقيق الرقمي.
3. **توظيف الخبراء الفنيين** :ينبغي توظيف خبراء فنيين ذوي الخبرة في مجال التحقيقات الرقمية لدعم العملية التحقيقية واستخدام الأدوات والتقنيات بفعالية.
4. **تحليل البيانات الرقمية** :يتعين تطوير استراتيجية لتحليل البيانات الرقمية المجمعة، بما في ذلك استخدام تقنيات التحليل الرقمي مثل تحليل الاتجاهات والمخططات والبحث الرقمي.
5. **جمع الأدلة الرقمية بشكل صحيح** :يجب جمع الأدلة الرقمية بشكل صحيح وموثوق به، مع الحفاظ على سلامة البيانات وتوثيق سلسلة الحجة[3].

[1]- حسن الجوخندار، مرجع سابق، ص29.
[2]- السوفي نور الهدى التحقيق في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر أكاديمي في الحقوق، تخصص قانوني جنائي، جامعة قاصدي مرباح ورقلة 2017، ص21.
[3]- براهيمي جمال، مرجع سابق، ص30.

6. **التعاون والتنسيق مع الجهات المعنية** :يجب التعاون والتنسيق مع الجهات الفنية والقانونية الأخرى المعنية بالتحقيق لضمان تبادل المعلومات والدعم المتبادل.

7. **التحقق من الامتثال القانوني والأخلاقي** :يجب أن يتم التحقق من أن جميع الإجراءات التقنية والتحقيقية تتوافق مع القوانين والأنظمة القانونية والأخلاقية ذات الصلة.[1]

ثالثا: دراسة الإجراءات

دراسة الإجراءات هي خطوة حيوية في تحقيق الجرائم الإلكترونية. إليك بعض النقاط التي يجب أخذها في الاعتبار أثناء دراسة الإجراءات[2] :

1. **تحليل الجريمة وتحديد الأهداف** :يجب فهم نوع الجريمة الإلكترونية ومدى تأثيرها وتحديد الأهداف المحددة للتحقيق.

2. **تحديد الأدوات والتقنيات المطلوبة** :استنادًا إلى نوع الجريمة ونوع البيانات المعنية، ينبغي تحديد الأدوات والتقنيات المناسبة لجمع وتحليل الأدلة الرقمية.

3. **توفير الموارد البشرية والتقنية** :يجب توفير الفرق الفنية المؤهلة والأدوات اللازمة لتنفيذ الإجراءات التحقيقية بشكل فعال.

4. **وضع خطة زمنية** :ينبغي تحديد جدول زمني للإجراءات التحقيقية، بما في ذلك مواعيد جمع البيانات، وتحليلها، وتوثيق النتائج.

5. **التنسيق مع الجهات المعنية** :يجب التنسيق مع الجهات الفنية والقانونية الأخرى المعنية بالتحقيق لضمان تبادل المعلومات وتوجيه الجهود بشكل متناسق[3].

---

[1]- براهيمي جمال، مرجع سابق، ص30.

[2]- الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، الطبعة الأولى، ص84.

[3]- بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم، جامعة الجزائر، كلية الحقوق، الجزائر، 2015، ص42.

6. **ضمان الامتثال القانوني والأخلاقي** :يجب التأكد من أن جميع الإجراءات التحقيقية تتوافق مع القوانين المحلية والدولية ذات الصلة، وتحترم المبادئ الأخلاقية للتحقيق.

7. **التقييم المستمر والتحسين** :ينبغي مراجعة وتقييم الإجراءات التحقيقية بانتظام، وتحديثها وتحسينها بناءً على الخبرة والتطورات الجديدة.

باعتبارها خطوات أساسية في دراسة الإجراءات، يمكن لهذه العمليات أن تساعد في ضمان تنفيذ التحقيق بطريقة منهجية وفعالة، مما يسهم في تحقيق العدالة وتقديم المتهمين إلى المحاكمة بناءً على أدلة قوية وموثوقة[1].

رابعا: تنسيق الجهود

التنسيق الجيد بين أفراد الفريق التحقيقي أمر بالغ الأهمية لضمان نجاح العملية التحقيقية. إليك بعض النقاط التي يجب مراعاتها لتحقيق هذا التنسيق[2]:

1. **تعيين مسؤوليات واضحة** :يجب تحديد مهام كل عضو في الفريق وتوضيح مسؤولياته بشكل واضح، مما يضمن توجيه الجهود نحو أهداف التحقيق المحددة.

2. **التواصل الفعال** :ينبغي تعزيز التواصل المستمر بين أفراد الفريق، سواء كان ذلك عبر الاجتماعات الدورية أو وسائل الاتصال الأخرى، لتبادل المعلومات ومتابعة تقدم العمل.

3. **تحديد الأولويات والمهام الحرجة** :يجب تحديد الأولويات والمهام الحرجة التي يجب التركيز عليها أولاً، وتخصيص الجهود والموارد بشكل مناسب لتحقيقها[3].

---

[1]- بن فردية محمد، مرجع سابق ص42.

[2]- جواحي عبد الستار، جرائم الحاسوب - دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري مذكرة تخرج تدخل ضمن متطلبات الحصول على شهادة الماستر في العلوم الإسلامية، جامعة الشهيد حمه لخضر كلية العلوم الإجتماعية و الإنسانية، قسم العلوم الإنسانية، الجزائر 2015 ،ص31.

[3]- الفتاح بيومي حجازي، مرجع سابق ص88.

4. **حل المشكلات بشكل فوري** :يجب التعامل بفعالية مع أي مشاكل أو تحديات تواجه عملية التحقيق، والبحث عن الحلول المناسبة بشكل فوري.

5. **توجيه الدعم والتشجيع** :يجب تقديم الدعم المستمر والتشجيع بين أفراد الفريق، وتعزيز الروح الجماعية والفريقية لتحقيق أفضل النتائج[1].

6. **التنسيق مع الجهات الخارجية** :في بعض الحالات، قد تتطلب عملية التحقيق التعاون مع الجهات الخارجية مثل الشرطة، ويجب التنسيق معها بشكل جيد لضمان تدفق البيانات والمعلومات بشكل فعال.

7. **تقييم الأداء وتحسينه** :يجب إجراء تقييم دوري لأداء الفريق والعملية التحقيقية بشكل عام، وتحديد النقاط القوية والضعف، واتخاذ التدابير اللازمة لتحسين الأداء في المرات القادمة.

من خلال تنفيذ هذه الخطوات، يمكن تحقيق التنسيق الفعال بين أفراد الفريق التحقيقي، وبالتالي تحقيق أهداف التحقيق بكفاءة وفعالية[2].

خامسا: تحديد الإجراءات المسبقة

تحديد الإجراءات المسبقة هو خطوة مهمة في عملية التحقيق لضمان سلامة البيانات وفعالية العملية. إليك بعض الإجراءات التي يمكن اتخاذها:

1. **تأمين الأدلة الرقمية** :يجب توفير إجراءات لحماية الأدلة الرقمية من التلف أو التلاعب بها، مثل تخزين البيانات في مواقع آمنة واستخدام أدوات تحليل البيانات ذات السمعة الطيبة[3].

---

[1]- بن فردية محمد، مرجع سابق ص42.

[2]- الفتاح بيومي حجازي، مرجع سابق ص88.

[3]- مصطفاوي عبد القادر، أساليب البحث و التحري الخاصة و إجراءاتها، مجلة المحكمة العليا، العدد 02، 2009، ص109.

2. **تحديد السياسات والإجراءات القانونية** :ينبغي وضع سياسات وإجراءات قانونية لجمع الأدلة واستخدامها بشكل قانوني وموثوق به، مع الالتزام بالتشريعات والقوانين ذات الصلة.

3. **توفير التدريب والتوجيه** :يجب توفير التدريب المناسب لأفراد الفريق التحقيقي حول كيفية التعامل مع الأدلة الرقمية واستخدام التقنيات الرقمية المتقدمة.

4. **تقييم المخاطر الأمنية** :ينبغي إجراء تقييم للمخاطر الأمنية المحتملة التي قد تؤثر على عملية التحقيق، واتخاذ التدابير اللازمة لتقليل هذه المخاطر[1].

5. **توفير الدعم التقني** :يجب توفير الدعم التقني المناسب لأفراد الفريق التحقيقي، بما في ذلك استخدام الأدوات والبرمجيات المتخصصة في تحليل البيانات الرقمية وحمايتها.

6. **التوثيق الشامل** :ينبغي توثيق جميع الإجراءات والخطوات التي تم اتخاذها خلال عملية التحقيق، بما في ذلك جمع الأدلة وتحليلها وتوثيق النتائج.

7. **الاستعانة بخبراء** :في حالة الجرائم الإلكترونية المعقدة، ينبغي النظر في استعانة بخبراء متخصصين في التحقيقات الرقمية لمساعدة في تحليل البيانات وتقديم الخبرات الفنية.

بتنفيذ هذه الإجراءات المسبقة، يمكن تحسين جودة وفعالية عملية التحقيق في الجرائم الإلكترونية وتقليل المخاطر المحتملة المرتبطة بها[2].

[1]- مصطفاوي عبد القادر، مرجع سابق ص109.

[2]- عباسي خولة الوسائل الحديثة للإثبات في القانون الجنائي مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، 2014، ص22.

الفرع الثاني: تشكيل فريق التحقيق

تشكيل فريق التحقيق في الجرائم المعلوماتية يتطلب تنظيمًا وتخطيطًا جيديًا لضمان فعالية العملية التحقيقية. فيما يلي أعضاء يمكن أن يتكون منهم فريق التحقيق في الجرائم المعلوماتية[1]:

1. **المحققون الجنائيون** :يتولون مسؤولية جمع الأدلة وتحليلها وتقديمها بشكل ملائم لدعم القضية الجنائية.

2. **خبراء الحاسوب والشبكات** :يقومون بتحليل الأجهزة الرقمية المصادرة واستخراج البيانات والأدلة الرقمية المتعلقة بالجريمة.

3. **محللو البيانات** :يقومون بتحليل البيانات والمعلومات المصادرة لتحديد الأنماط والاتجاهات التي يمكن أن تفيد في تحديد المشتبه بهم.

4. **خبراء التحقيق الرقمي** :يتخصصون في استخدام التقنيات والأدوات الرقمية لجمع الأدلة وتحليلها وتتبع أنشطة المشتبه بهم عبر الإنترنت.

5. **الخبراء القانونيون** :يقدمون الاستشارات القانونية والتحليلات حول الجوانب القانونية المتعلقة بالتحقيق وجمع الأدلة.

6. **خبراء الأمن السيبراني** :يقدمون الخبرة في تقييم الثغرات الأمنية وتحديد الضعف في أنظمة المعلومات والشبكات.

7. **خبراء التقنيات الرقمية القضائية** :يتخصصون في استخدام التقنيات الرقمية لدعم التحقيق الجنائي وتوثيق الأدلة بشكل يمكن قبوله قانونيا في المحكمة[2].

---

[1]- جواحي عبد الستار، مرجع سابق ص33.

[2]- قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة مكملة لنيل شهادة الماستر أكاديمي في القانون، تخصص قانون عام للأعمال جامعة قاصدي مرباح ورقلة، 2014، ص25.

تعتمد فعالية عملية التحقيق في الجرائم المعلوماتية بشكل كبير على تعاون وتنسيق جهود هؤلاء الخبراء في الفريق، مما يضمن تحقيق النتائج المرجوة بشكل فعال ومنهجي[1].

المطلب الثاني: العناصر الأساسية للتحقيق الابتدائي في مجال البرمجة الإلكترونية

نقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبيها، وهناك إجراءات واحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الابتدائي وإجراءات أخرى يجب على الضبطية القضائية مراعاتها أثناء التحقيق الابتدائي[2].

الفرع الأول: الإجراءات التي يجب مراعاتها قبل البدء في التحقيق

تحديد نوع نظام المعالجة الأولية للمعطيات فهل هو كمبيوتر معزول أم متصل بشبكة معلومات.

- وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.
- إذا وقعت الجريمة على شبكة فإنه يجب حصر طرفيات الاتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الاختراق من عدمه.
- مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.
- مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.
- يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار الجريمة.[3]

---

[1]- جواحي عبد الستار، مرجع سابق ص33.

[2]- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة للطباعة والنشر، الجزائر، ط2، 2009، ص56.

[3]- صالح شنين، الحماية الجنائية للتجارة الإلكترونية، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، جامعة أبو بكر بلقايد تلمسان، كلية الحقوق، الجزائر 2013، ص36.

- فصل خطوط الهاتف حتى لا يسيئ الجاني استخدامها والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيئون استخدامها لطمس البيانات.
- التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنه من الخدع التي يستعملها الجاني عند الاختراق أن يتم ذلك بخط هاتفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتقليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك. إبعاد الموظفين عن أجهزة الحاسوب الآلي بعد الحصول منهم على كلمة السر وكذا الثغرات في حالة وجودها.
- تصوير الأجهزة المستهدفة من أمام والخلف لإثبات بأنها كانت تعمل.[1]

الفرع الثاني: الإجراءات التي يجب مراعاتها أثناء التحقيق

- عمل نسخة احتياطية من الأقراص الصلبة قبل استخدامها والتأكد فنيا من دقة النسخ.
- نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.
- العمل على فحص العلاقة بين برامج التطبيق والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.
- حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة.
- العمل على فحص وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلومات.[2]

[1]- صالح شنين، مرجع سابق ص36.
[2]- عبد العزيز ،سعد أبحاث تحليلية في قانون الإجراءات الجزائية، دار هومة للطباعة والنشر والتوزيع، الجزائر، بدون طبعة ، 2009، ص51.

- أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص وتحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة المعلومات والملفات الممسوحة وكذلك معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب.[1]

تلعب الأجهزة الفنية دروا أساسيا في صيانة أمن المجتمع وذلك إما بالقيام بدور وقائي يهدف إلى منع ارتكاب الجرائم والحيلولة دون وقوعها وتقليل فرص اقترافها، وإما القيام بدور قضائي في ضبط الجرائم ومرتكبيها بعد حدوثها.

ولقد أضاف ظهور الجرائم المعلوماتية النابعة من التطور الإلكتروني أعباء جديدة على أجهزة التحقيق لما يتطلب التصدي لهذه الجرائم من قدرات فيه لم يألفها رجال الضبطية القضائية ولم يتعودوا عليها، ما يستلزم ضرورة توفير المهارات المطلوبة في هذا المجال.[2]

والمشكلة الأساسية التي تواجب المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه فتخصصوا الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دوافع الجريمة وجمع الأدلة التقديم المتهم للمحاكة ، وفي كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول الجريمة الإلكترونية،[3] ولكن من الناحية يتضح فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى، بينما المحققون ذوي الخلفية القانونية قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم. وإذا كانت مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة و مناقشة الشهود وغير تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق. [4]

[1]- عبد العزيز، مرجع سابق ص51.
[2]- جواحي عبد الستار، مرجع سابق ص46.
[3]- صالح شنين، مرجع سابق ص39.
[4]- صالح شنين، مرجع سابق ص39.

إلا أنه يلزمه عند مباشرته التحقيق في الجريمة الإلكترونية معرفة العديد من الجوانب الفنية يقوم بعمله على أحسن وجه ونذكره منها:

معرفة الجوانب الفنية والتقنية لأجهزة الأجهزة الحاسوب الإنترنت والتي تتعلق بالجريمة المرتكبة ذلك أن افتقار ضابط الشرطة القضائية التأهيل الكافي في الميدان التقي قد يغطي إلى إتلاف وتدمير الدليل على اعتبار أن جهله بأساليب ارتكاب الجريمة المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية وتدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن بها البيانات، وبالتالية فإن الكشف عن هذه الجرائم يقتضي أن تكون الأجهزة المعنية على دراية كافية بأساسيات التعامل مع هذه الجرائم وكيفية تقصيها وضبطها وصولا إلى مرتكبيها. [1]

توفير التدريب المناسب وتعزيز التعاون بين الخبراء في مجالات متعددة يعد أمراً حيوياً في مكافحة الجرائم الإلكترونية. إذا كانت هناك نقص في المعرفة الفنية لدى بعض المحققين، يجب توفير التدريب المناسب لهم لزيادة فهمهم ومهاراتهم في مجال التحقيق الإلكتروني. كما يمكن تحسين التعاون بين فرق التحقيق والخبراء الفنيين من خلال تبادل المعرفة والخبرات وتطوير استراتيجيات مشتركة لمكافحة الجرائم الإلكترونية.

بالإضافة إلى ذلك، يجب أن يكون هناك تحسين في التوجيه والتدريب لضباط الشرطة القضائية لزيادة وعيهم بالتهديدات الأمنية الرقمية وكيفية التعامل معها.[2]

يجب أن يتلقى العاملون في مجال إنفاذ القانون تدريبًا دوريًا وتحديثًا للمعرفة بأحدث التطورات التقنية والأساليب الجديدة المستخدمة في الجرائم الإلكترونية[3].

[1]- صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، جامعة مولود معمري تيزي وزو كلية الحقوق والعلوم السياسية الجزائر، سنة 2013، ص28.

[2]- محمد حزيط، مرجع سابق ص60.

[3]- محمد حزيط، مرجع سابق ص60.

علاوة على ذلك، يمكن تحسين فعالية عمليات التحقيق الجنائي من خلال تعزيز التعاون بين الجهات القانونية والأمنية والقطاع الخاص، حيث يمكن للشركات التكنولوجية ومقدمي الخدمات الإلكترونية تقديم الدعم الفني والتعاون في جمع الأدلة الرقمية وتحليلها.

من الضروري أيضاً توفير الإمكانيات الفنية اللازمة للتحقيق في الجرائم الإلكترونية، مثل الأدوات والبرمجيات المتقدمة لتحليل البيانات الرقمية واستخراج الأدلة. ويجب على الجهات المعنية بالتحقيق الجنائي الاستثمار في بناء القدرات الفنية وتطوير التقنيات المستخدمة لمكافحة الجرائم الإلكترونية[1].

[1]- صغير يوسف، مرجع سابق ص29.

خلاصة الفصل:

تعتبر مرحلة التحقيق الابتدائي في الجرائم الإلكترونية من الخطوات الحيوية في عملية التحقيق، حيث يتم فيها جمع الأدلة والمعلومات الأولية التي تساعد في تحديد تفاصيل الجريمة وتحديد المشتبه بهم. ولتحقيق النجاح في هذه المرحلة، يجب أن يكون للمحققين الجنائيين فهم عميق للتكنولوجيا والوسائل الرقمية، بالإضافة إلى القدرة على التكيف مع التطورات الجديدة في مجال الجريمة الإلكترونية.

تتطلب الجرائم الإلكترونية تحقيقًا متخصصًا وفريقًا مجهزًا بالمهارات التقنية اللازمة لجمع الأدلة الرقمية والتحليل الرقمي. فالبيانات الرقمية يمكن أن تكون زلزالية في تقديم الأدلة التي تثبت الجريمة وتحديد الجاني. لذلك، يجب على المحققين الجنائيين أن يكونوا على دراية بالأساليب والأدوات الرقمية المتاحة لهم لجمع وتحليل هذه الأدلة بكفاءة ودقة.

باستخدام أساليب التحقيق المتقدمة والمتطورة، يمكن للمحققين جمع الأدلة الرقمية بكفاءة وفحصها بدقة للكشف عن الحقيقة وتقديم الجانيين إلى العدالة. ويعكس هذا النهج الحاجة الماسة إلى تطوير وتحديث أساليب التحقيق لمواكبة التطورات التكنولوجية ومواجهة التحديات المتزايدة في مجال مكافحة الجريمة الإلكترونية.

الفصل الثاني

واجه ظاهرة الإجرام الإلكتروني تحديات قانونية جوهرية تتعلق بالقانون الجنائي، حيث إن تطبيق النصوص التقليدية على هذا النوع من الجرائم يثير أسئلة حول احترام مبدأ الشرعية والتفسير الضيق للنصوص الجزائية. هذه الجرائم غالباً ما تكون معقدة بسبب تعاملها مع بيانات المعالجة الآلية والكيانات المنطقية غير المادية، مما يجعل الكشف عنها وإثباتها أمراً صعباً نظراً للسرعة الفائقة والدقة العالية في تنفيذها، بالإضافة إلى القدرة على محو آثارها وإخفاء الأدلة بسهولة باستخدام تقنيات متقدمة.

وقد تطور تأثير التقنية المعلوماتية على الإجراءات الجزائية بمرور الوقت، لأن النصوص التقليدية كانت موجهة نحو جرائم ترتكب في عالم مادي وملموس، حيث يلعب السلوك المادي دوراً كبيراً. في المقابل، تُرتكب الجرائم الإلكترونية في فضاء إلكتروني افتراضي وغير مادي، مما يتطلب إعادة النظر في الإجراءات التقليدية وإيجاد حلول جديدة تتناسب مع طبيعة هذه الجرائم[1].

وعليه تم تقسيم الفصل إلى:

المبحث الأول إجراءات التحقيق الجنائي المألوفة في الجرائم الإلكترونية.

المبحث الثاني إجراءات التحقيق الجنائي الخاصة في الجرائم الإلكترونية.

[1]-رشيدة بوكر الدليل الالكتروني ومدى حجيته في الاثبات الجزائي في القانون الجزائري ،مجلة جامعة دمشق للعلوم الاقتصادية المجلد 27 العدد الثاني 2011 ، ص85.

المبحث الأول: إجراءات التحقيق الجنائي المألوفة في الجرائم الإلكترونية

لا شك أن المشرع عند محاولته توسيع نطاق تطبيق إجراءات التحقيق التقليدية لتشمل الجرائم الإلكترونية كان يواجه العديد من التحديات التي تنبع من خصوصية هذه الجرائم. وتشمل هذه التحديات الإجراءات التقليدية مثل التفتيش، الضبط، المعاينة، والخبرة. هذه الإجراءات، في صورتها التقليدية، قد لا تكون كافية أو فعّالة للتعامل مع الطبيعة الفريدة للجرائم الإلكترونية والأدلة المرتبطة بها. لذا، يتطلب الأمر تطويرًا وتحديثًا لتلك الإجراءات بما يتناسب مع الخصوصية الفريدة للجرائم الإلكترونية، [1]وعليه سنتطرق إلى التفتيش في البيئة الإلكترونية في المطلب الأول، أما في المطلب الثاني فسنذكر ضبط الأدلة في الجرائم الإلكترونية.

المطلب الأول: التفتيش في البيئة الإلكترونية

يتطلب التحقيق تفتيش شخص المتهم أو منزله أو غيره أو منزله لضبط الأشياء المتعلقة بالجريمة، والتفتيش كإجراء من إجراءات التحقيق الابتدائي هو في الأصل من اختصاص سلطة التحقيق المتمثلة في قاضي التحقيق والنيابة العامة باختلاف التشريعات، إلا أنه يحول استثناء الرجال الضبطية القضائية في حالات محددة قانوناً.[2]

وقد أجمع الفقه الجنائي، على أن التفتيش كإجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقا للضمانات والضوابط المقررة قانونا. [3]

---

[1]-رشيدة بوكر، مرجع سابق، ص85.

[2]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية،2006، ص192.

[3]-نفس المرجع.

أن التفتيش ما هو إلا وسيلة للإثبات المادي، غايته هي ضبط الأدلة المادية الخاص بالجريمة، مما يجعله يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي، ومعطيات شبكة الانترنت التي ليس لها أي مظهر مادي محسوس في العالم الخارجي.[1]

الفرع الأول: محل التفتيش الإلكتروني

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره وخصوصيته، والسر الذي يحميه القانون هو ذلك الذي يودع في محل له حرمة، كالمسكن أو سيارة أو رسائل، بالتالي فمحل التفتيش قد يكون أحد المواقع المذكورة مع مراعاة الإجراءات والشروط القانونية المقررة لكل موقع على حدة. [2]

ولما كان المستودع في الجرائم الالكترونية هو الحاسب الآلي الذي يقوم في تركيبه على مكونات مادية Hard Ware كوحدات المعالجة المركزية (processeur)، وحدات الإدخال والإخراج ووحدات التخزين أو ما يسمى بوحدة التحكم (Unité De Control)، ومكونات أخرى منطقية Soft Ware برامج النظام الأساسية، البرامج التطبيقية، والبيانات المعالجة آليا كما أن له شبكات اتصالات بعدية سلكية ولاسلكية متواجدة على مستوى المحلي والدولي، فإن الأمر يتطلب منا البحث في مدى قابلية جميع هذه المكونات للتفتيش. [3]

---

[1]- براهيمي جمال التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص قانون كلية الحقوق، جامعة تيزي وزو، 2018 ص 14

[2]-بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، 2010، ص80.

[3]- على محمود على محمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، نظمته أكاديمية شرطة دبي، في الفترة من 26 الى 28 أفريل 2003، ص 135.

أولا: تفتيش المكونات المادية للحاسب

فيما يتعلق بتفتيش المكونات المادية للحاسوب الآلي بحثًا عن أدلة مادية في إطار الجرائم الإلكترونية، يتبع هذا الإجراء القواعد المعمول بها في عمليات التفتيش التقليدية. أهمية هذه القواعد تعتمد على طبيعة المكان الذي توجد فيه الأدلة. إذا كانت الأدلة موجودة في مكان خاص، مثل منزل المتهم أو ملحقاته، فإن إجراءات التفتيش تكون محكومة بقواعد محددة لا يمكن تجاوزها إلا بظروف محددة تتماشى مع التشريعات القانونية المختلفة[1].

في القانون الجزائري، على سبيل المثال، تنص المواد من (44) إلى (47) من قانون الإجراءات الجزائية على ضرورة الحصول على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق قبل القيام بتفتيش أي مسكن في حالة الجرائم المتلبس بها. يجب استظهار هذا الإذن قبل الدخول إلى المسكن والشروع في التفتيش. كما يشترط القانون أن يتم التفتيش خلال ساعات النهار، تحديداً بين الساعة الخامسة صباحاً والثامنة مساءً، وبحضور صاحب المسكن أو ممثله. وإذا تعذر حضور صاحب المسكن، يجب استدعاء شاهدين غير خاضعين لسلطة ضابط الشرطة القضائية الذي يقوم بالتفتيش[2].

هذه الإجراءات تهدف إلى حماية حقوق الأفراد وضمان عدم انتهاك خصوصيتهم إلا في حدود ما يسمح به القانون وبوجود ضمانات واضحة تحمي من التعسف في استخدام سلطة التفتيش.

[1]- عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي مجلد ،22، عدد 86، صادر عن مركز بحوث الشرطة القيادة العامة لشرطة الشارقة الإمارات العربية المتحدة 2013، ص 260

[2]- خالد ممدوح إبراهيم فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي إسكندرية 2009، ص 195.

وينبغي التمييز داخل المكان الخاص بين ما إذا كانت مكونات الحاسب منعزلة أم أنها بحواسيب أو أجهزة متواجدة في مكان آخر كمسكن الغير، ففي هذه الحالة المحقق مراعاة القيود والضمانات التي يشترطها القانون التفتيش هذه الأماكن. [1]

أما إذ كانت المكونات المادية للحاسوب متواجدة في أماكن عامة، سواء أكانت عامة بطبيعتها كالحدائق العامة والطرق العامة، أم أماكن عامة بالتخصيص كمقاهي الانترنت و محلات بيع وصيانة الحواسب، فإجراءات تفتيشها تكون وفقا للأصول الخاصة بتلك الأماكن. ويستوي الأمر بالنسبة للمكونات الموجودة بحوزة شخص ما، فبغض النظر عن صفة هذا الشخص، ميرميا كان أو عامل صيانة أو موظفا في شركة تنتج برامج الحاسب الآلي، فإن تفتيش هذه المكونات يخضع لأحكام تفتيش الأشخاص، وبالشروط والضمانات القانونية المحددة لذلك. [2]

بناء على ما سبق، يتضح أن تفتيش المكونات المادية لجهاز الحاسب وملحقاته مثل لوحة المفاتيح أو الشاشة أو الطباعة أو غيرها من الأشياء المادية المحسوسة، لا يثير أية مشاكل إجرائية أمام سلطات الاستدلال، إذ يسري عليه ما يسري على تفتيش الأشياء والأدوات المادية الأخرى من شروط وضمانات كمراعاة وقت التفتيش الإذن بالتفتيش الأشخاص القائمين بالتفتيش والأشخاص المطلوب حضورهم عند التفتيش مع مراعاة الاختصاص المكاني وعدم فض الأوراق المحرزة. كما أن أجهزة القضاء المخول لها القيام بإجراء التفتيش سواء بصفة

[1]-أحمد بن زايد جوهر الحسن المهدي، تفتيش الحاسب الآلي وضمانات المتهم، مذكرة لنيل درجة ماجستير في القانون، كلية- الحقوق جامعة القاهرة، 2009، ص 118.

[2]- بوكر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، 2012، ص 395.

أصلية أو استثنائية يمكنها تفتيش المكونات المادية في الجريمة الالكترونية دون الحاجة إلى أن تكون متخصصة في الجوانب التقنية، مثلها مثل غيرها من المكونات المادية الأخرى.[1]

ثانيا: مدى صلاحية مكونات الحاسب المنطقية للتفتيش

تعرف الكيانات المنطقية للحاسب بأنها مجموعة من البرامج والأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة معالجة البيانات.

وإذا كان الأمر قد انتهى إلى صلاحية مكونات الحاسب المادية كمحل يرد عليه التفتيش فان امتداد ذلك إلى المكونات غير المادية أو المنطقية هو محل جدل فقهي كبير حول مدى صلاحيتها لان تكون محلا للتفتيش تمهيدا لضبط الأدلة.[2]

فالخلاف حاصل في مسألة كون التفتيش وسيلة للبحث وضبط الآثار المتعلقة بالجريمة وتقديمها إلى المحكمة كدليل إدانة، لذلك يثور الشك والتساؤل حول إمكانية اعتبار البحث عن أدلة الجريمة الالكترونية في نظم وبرامج الحاسب نوعا من التفتيش، باعتبار أن البيانات الالكترونية أو البرامج في حد ذاتها تفتقر إلى مظهر مادي محسوس في المحيط الخارجي، ويستشعر الفقه صعوبة المسألة بالنظر إلى غياب الطبيعة المادية للمعلومات والبيانات، بما يجعلها تتنافى مع الهدف الذي يصبو إليه التفتيش ألا وهو البحث عن الأدلة المادية.[3]

وإزاء هذا التشكيك سعي جانب من الفقه إلى إزالته و تجنبه على نحو يسمح بتضمين التفتيش بمعناه التقليدي، البحث والتنقيب في نظم وبرامج الحواسب عن أدلة الجريمة الالكترونية، وحجتهم في ذلك هي أنه وإن كانت هذه النظم والبرامج عبارة عن نبضات أو

---

[1]- فايز محمد راجح غلاب الجرائم المعلوماتية في القانون الجزائري و اليمني، أطروحة لنيل شهادة الدكتوراه في القانون، فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق جامعة الجزائر 1، الجزائر 2011، ص 309.

[2]- عفيفي كمال عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، طبعة ثانية، منشورات الحلبي القانونية، دمشق، 2007، ص 61.

[3]- علي محمود علي حمودة، مرجع سابق، ص 81

ذبذبات الكترونية أو موجات كهرومغناطيسية إلا أنها قابلة للتسجيل والتخزين والتحميل على وسائط و دعائم مادية معينة، ولها كيان مادي محسوس من خلال استشعارها وقياسها، لذلك فمن الممكن جدا اخضاعها لقواعد التفتيش التقليدية.[1]

وعلى النقيض من ذلك، يرى جانب آخر من الفقه بأنه من غير الممكن إخضاع مكونات الحاسب المنطقية لقواعد التفتيش التقليدية، لأن هذه القواعد وضعت في وقت لم تكن نظم المعالجة الآلية والحواسيب موجودة وتطبيقاتها غير معروفة، بالتالي فطبيعة هذه المكونات تتطلب إحداث قواعد تفتيش جديدة خاصة بها، أو على الأقل تعديل قواعد التفتيش المألوفة بشكل يجعلها تتلاءم أحكامها مع متطلبات هذه التقنية الجديدة. [2]

الفرع الثاني: ضمانات التفتيش في البيئة الإلكترونية

رغم اعتبار التفتيش من الإجراءات الجوهرية في عملية التحقيق البحث عن حقيقة الجرائم إلا أن معظم القوانين الإجرائية حرصت على إحاطته بجملة من الضمانات القانونية، وذلك تفاديا لتعسف سلطات البحث والاستدلال وما يمكن أن يحدثه من اعتداء على حقوق وحريات الأفراد وحرمة مساكنهم وحياتهم الخاصة من جهة، وإحقاقا لحق الدولة ممثلة المجتمع في كشف غموض الجرائم ومتابعة مرتكبيها وتوقيع العقاب عليهم من جهة أخرى، ويمكن تقسيم هذه الضمانات إلى ضمانات موضوعية وأخرى شكلية أو إجرائية نذكرها على النحو التالي:[3]

أولا: الضمانات الموضوعية للتفتيش الإلكتروني

---

[1]- موسي مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلومات والقانون" المنعقد بأكاديمية الدراسات العليا طرابلس، في 2009/10/2829، ص 8.

[2]- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات دراسة مقارنة، دار الفكر الجامعي، الإسكندرية 2013، ص 226

[3]- براهيمي جمال، مرجع سابق، ص.14.

تتمثل الضمانات التي يجب توفرها لضمان صحة إجراءات التفتيش في الجرائم الإلكترونية في ثلاثة شروط أساسية هي[1]:

1. **سبب التفتيش** :يجب أن يكون هناك سبب وجيه ومحدد لإجراء التفتيش. عادةً ما يكون هذا السبب مستندًا إلى أدلة أو معلومات تشير إلى احتمالية وجود مواد أو أدلة متعلقة بالجريمة في المكان المحدد. في حالات الجرائم المتلبس بها، يتم تعزيز هذا السبب بحالة الجريمة الظاهرة والواضحة التي تبرر التفتيش.

2. **محل التفتيش** :يجب تحديد المكان الذي سيتم تفتيشه بشكل دقيق. لا يجوز أن يكون التفتيش عشوائيًا أو غير محدد، بل يجب أن يكون هناك توجيه واضح للأماكن التي يعتقد بوجود الأدلة فيها. على سبيل المثال، في حالة الجرائم الإلكترونية، يمكن أن يشمل محل التفتيش أجهزة الكمبيوتر أو الهواتف المحمولة أو أي أجهزة إلكترونية أخرى تتعلق بالجريمة.

3. **السلطة المختصة بالتفتيش** :يجب أن يتم التفتيش بواسطة السلطات المختصة والمخولة قانونًا للقيام بهذا الإجراء. في القانون الجزائري، على سبيل المثال، يجب أن يكون التفتيش مصحوبًا بإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق. بالإضافة إلى ذلك، يجب أن يتم التفتيش بحضور صاحب المسكن أو ممثله، وفي حالة عدم وجوده، يجب استدعاء شاهدين لضمان شفافية العملية وعدم انتهاك الحقوق[2].

هذه الشروط تهدف إلى ضمان أن يتم التفتيش بشكل قانوني ومنظم، مما يحمي حقوق الأفراد ويمنع التعسف في استخدام السلطة.

ثانيا: الضمانات الشكلية للتفتيش الإلكتروني

[1]- علي محمود علي حموده، مرجع سابق، ص 94.
[2]- نفس المرجع.

الغرض من إحاطة التفتيش بضمانات شكلية وموضوعية ليس فقط ضمان مصلحة القضاء في صحة الإجراءات المتخذة لجمع الأدلة وضمان مشروعية هذه الأدلة، بل أيضًا حماية الحقوق والحريات العامة الفردية. هذه الضمانات تعمل كسياج أمني يحمي الأفراد من التعسف وانتهاك خصوصياتهم.

عند تطبيق هذه الضمانات في مجال التفتيش الإلكتروني، قد تتحول إلى عقبات قد تعرقل تحقيق الهدف الأساسي من التفتيش. سنستعرض هذه الضمانات التي يمكن أن تشكل تحديات عند تطبيقها على التفتيش الإلكتروني، وهي[1]:

1. **إذن التفتيش المسبق** :يتطلب الحصول على إذن مكتوب من السلطات القضائية قبل الشروع في أي تفتيش. في الجرائم الإلكترونية، قد يكون من الصعب الحصول على إذن سريع نظرًا للطبيعة العاجلة التي تتطلبها بعض الحالات، حيث يمكن للمتهمين بسهولة إخفاء أو تدمير الأدلة الرقمية بسرعة.

2. **تحديد محل التفتيش بدقة** :في التفتيش التقليدي، يمكن تحديد مكان التفتيش بدقة، مثل غرفة معينة أو خزينة. أما في التفتيش الإلكتروني، يكون تحديد المكان أكثر تعقيدًا، حيث يمكن أن تكون الأدلة موزعة عبر أجهزة متعددة أو مخزنة في السحابة الإلكترونية، مما يجعل من الصعب تحديد نطاق التفتيش بشكل دقيق ومحدد[2].

3. **حضور صاحب المسكن أو ممثله** :في التفتيش التقليدي، يُشترط حضور صاحب المسكن أو ممثله لضمان شفافية العملية. في التفتيش الإلكتروني، قد يكون

[1]- فايز محمد راجح غلاب، مرجع سابق، ص 338
[2]- الفقرة 2 من المادة 68 من قانون الإجراءات الجزائية، مرجع سابق.

من الصعب تحقيق هذا الشرط بنفس الفعالية، خاصة إذا كانت الأدلة موزعة عبر شبكة واسعة أو في مواقع بعيدة عن سيطرة المتهم.

4. **التوقيت المحدد للتفتيش** :يشترط القانون الجزائري، على سبيل المثال، إجراء التفتيش خلال ساعات النهار بين الخامسة صباحًا والثامنة مساءً. في الجرائم الإلكترونية، قد تكون هذه القيود الزمنية غير عملية، حيث يمكن أن تتطلب بعض الحالات التحرك الفوري لضمان عدم ضياع الأدلة[1].

5. **وجود شاهدين** :في حالة عدم وجود صاحب المسكن، يجب استدعاء شاهدين لضمان شفافية التفتيش. في التفتيش الإلكتروني، قد يكون هذا الإجراء غير مجدٍ بنفس الطريقة التقليدية، حيث تتطلب العملية مهارات تقنية ومعرفة خاصة قد لا تتوفر لدى الشهود العاديين[2].

إجمالاً، بينما تهدف هذه الضمانات إلى حماية الحقوق الفردية، فإن تطبيقها على التفتيش الإلكتروني يتطلب توازنًا دقيقًا بين حماية الحقوق وتحقيق العدالة في ضوء التحديات الفريدة التي تفرضها الجرائم الإلكترونية[3].

المطلب الثاني: ضبط الأدلة في الجرائم الإلكترونية

يعتبر الضبط من إجراءات جمع الأدلة، وهو النتيجة الطبيعية التي ينتهي إليها التفتيش والأثر المباشر الذي يسفر عنه، ويقصد به وضع اليد على الأشياء المتعلقة بجريمة وقعت

[1]- المادة 69 من قانون الإجراءات الجزائية، مرجع سابق.
[2]- المادة 79 من قانون الإجراءات الجزائية، مرجع سابق.
[3]- فايز محمد راجح غلاب، مرجع سابق، ص 338

والتي تفيد في كشف الحقيقة عنها وعن مرتكبيها، ووضعها في أحراز مختومة ولتقدم إلى الجهة القضائية المختصة كدليل إثبات.[1]

وتحصيل الأدلة في الجرائم الالكترونية قد يرتبط بعناصر مادية كجهاز الحاسب الآلي وملحقاته، الأقراص الصلبة، الأقراص والأشرطة الممغنطة، الطباعة البرامج اللينة والمراشد، البطاقات الممغنطة وبطاقات الائتمان والمعدات المستعملة في شبكة الانترنت مثل المودم، ففي هذه الحالة فلا يطرح ضبط هذه المكونات المادية أي إشكال قانوني أو عملي لإمكانية إخضاعها الإجراءات الضبط والتحريز التقليدية.

وقد يرتبط الدليل الالكتروني بالمكونات المعنوية للحاسب، كمختلف البرامج والبيانات المعالجة آليا والمراسلات والاتصالات الالكترونية التي يجري تبادلها عبر شبكة الانترنت والبريد الالكتروني، وهنا تثير الطبيعة المجردة لهذه المكونات جدلا فقهيا واختلافا تشريعيا كبيرا حول مدى إمكانية ضبطها وفقا القواعد الضبط المألوفة، مع العلم أن الضبط بمفهوم هذه الأخيرة لا يرد إلا على الأشياء المادية.[2]

تخول سلطات البحث والتحري طريقتين لضبط البيانات المعلوماتية والأدلة الرقمية التي كانت موضوع التفتيش،[3] وفقًا للفقرتين (1 و 2) من المادة (19) للاتفاقية الأروبية. تتلخص هذه الطريقتين كما يلي[4]:

1. **الضبط التقليدي:(Saisir)**

---

[1]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت دار الثقافة للنشر و التوزيع، عمان، 2011، ص170.

[2]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006 ، ص 218 .

[3]- هلال عبد الله أحمد اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، دار النهضة العربية، القاهرة، 2011، ص 251.

[4]- انظر الفقرة الثالثة من المادة (19) من الاتفاقية الأوروبية حول الجرائم المعلوماتية لعام 2001.

- **نسخ وتحميل البيانات** :يتم نسخ وتحميل البيانات والمعطيات محل البحث على دعامة تخزين مادية مثل الأقراص الممغنطة أو بطاقات الذاكرة (فلاش ديسك).

- **التحريز** :تُضبط هذه الدعامات وتُوضع في أحراز مختومة، وفقًا لقواعد تحريز الأدلة التقليدية المنصوص عليها في قوانين الإجراءات الجزائية. هذه الطريقة تهدف إلى الحفاظ على الأدلة الرقمية بنفس الطريقة التي تُحفظ بها الأدلة المادية التقليدية[1].

2. **الحصول بطريقة مشابهة على البيانات المعلوماتية:**

- **تقنيات الحماية الفنية** :تُستخدم تقنيات وتدابير الحماية الفنية مثل التشفير، والترميز، وبرامج منع الكتابة، واستخدام خوارزميات تجزئة للملفات المشفرة. هذه التقنيات تمنع الأشخاص غير المرخص لهم من الوصول إلى البيانات الأصلية أو نسخها[2].

- **التطبيق في حالة استحالة الضبط التقليدي** :تُستخدم هذه الطريقة عندما تكون هناك أسباب تقنية تمنع ضبط البيانات والمعطيات بالطريقة التقليدية[3].

الحالات الخاصة :إذا كانت البيانات والمعلومات الرقمية تحتوي على مخاطر على النظام العام والآداب العامة، مثل تحريض الأطفال على الشذوذ الجنسي، أو التحريض على

[1]-معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم الالكترونية في التشريع الجزائري و التشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج لخضر، باتنة كلية الحقوق والعلوم السياسية قسم الحقوق، 2011-2012، ص31.
[2]- خالد عياد الحلبي، مرجع سابق، ص175.
[3]-نفس المرجع.

التمييز العنصري أو الإرهاب، أو تحتوي على برامج وفيروسات، يمكن للسلطات التحقيق القيام بتعطيل تشغيل هذه البيانات (blocage des données) أو محوها بعد أخذ نسخة منها[1].

التدابير الخاصة لضمان تحريز الأدلة الرقمية :نصت المادة 3/19 من الاتفاقية المذكورة على مجموعة من التدابير الخاصة لضمان تحريز الأدلة الإلكترونية الرقمية وحمايتها فنيًا، وصيانتها من أي تغيير أو إتلاف أو عبث قد يصيبها. هذه التدابير تضمن:

- **الحماية الفنية** :تطبيق تقنيات حماية متقدمة لضمان عدم التلاعب بالأدلة.
- **الصيانة** :الحفاظ على الأدلة بشكل يضمن سلامتها وقابليتها للاستخدام في الإجراءات القضائية[2].

هذه الطرق والتدابير تعكس التحديات الفريدة التي تفرضها الجرائم الإلكترونية، حيث تتطلب معالجة دقيقة وفعالة لحفظ الأدلة الرقمية وضمان عدم ضياعها أو التلاعب بها[3].

[1]- حسام محمد نبيل الشراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، القاهرة 2013، ص 525.

[2]- الفقرة 03 من الاتفاقية الأوروبية حول الجرائم المعلوماتية لعام 2001 ، مرجع سابق.

[3] - FIRAL-SCHUHL Christiane, cyber droit- le droit a l'épreuve de l'internet, 6ém édition Dalloz, Paris, 2011-2012, P998.

المبحث الثاني: إجراءات التحقيق الجنائي الخاصة في الجرائم الإلكترونية

أدى تطور الثورة المعلوماتية إلى ظهور أنماط جديدة من الجرائم تُعرف بالجرائم المعلوماتية، مما أثر بشكل كبير على وسائل إثبات هذه الجرائم. فقد أصبحت الطرق التقليدية التي نصت عليها قوانين الإجراءات الجزائية غير كافية لاستخلاص الأدلة المتعلقة بهذه الجرائم المستحدثة.[1] هذه الجرائم تتطلب وسائل وتقنيات جديدة تتناسب مع طبيعتها الفريدة ويمكنها فك رموزها وتحويل إشاراتها الرقمية إلى أدلة ملموسة ومقروءة،[2] وعليه سنتطرق إلى التسرب الإلكتروني في المطلب الأول، أما في المطلب الثاني فسنذكر اعتراض المراسلات والمراقبة الإلكترونية.

المطلب الأول: التسرب الإلكتروني

تعرف المادة 65 مكرر 12من القانون الإجراءات الجزائية الجزائري "التسرب على أنه قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق

[1]-معتوق عبد اللطيف، رع سابق، ص32.
[2]- المادة 100من قانون الإجراءات الجزائية، مرجع سابق.

العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك".[1]

انطلاقا من هذا التعريف، يتبين أن التسرب عملية معقدة جدا تتطلب أحيانا من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها وارتكاب أفعال محظورة قصد تحقيق الهدف النهائي من العملية، بل أحيانا يكون القيام بتلك الأفعال ضرورة لقبوله في الخلية. لذلك اعتبار لهذه الضرورة تقطن المشرع الجزائري وجرد الضابط أو العون المتسرب من المسؤولية الجنائية عن كافة الأفعال غير المشروعة التي قد يقدم على ارتكابها أثناء عملية التسرب.[2]

ليس هذا فحسب، بل أحاط المشرع المسرب كذلك بعدة ضمانات من أجل حمايته وحماية أسرته أثناء عملية التسرب وبعد انقضائها منها ما ورد في المادة 65 مكرر16من قانون الإجراءات الجزائية بأنه" لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أية مرحلة من مراحل الإجراء".[3]

وما تضمنته كذلك المادة 65 مكرر 17 من القانون نفسه بأنه " إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في الرخصة للتسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة النشاطات المذكورة في المادة 65 مكرر 14 أعلاه للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسئولا جزائيا، على أن لا يتجاوز ذلك 4 أشهر".[4]

---

[1]- المادة 65 مكرر 12 من القانون الإجراءات الجزائية، مرجع سابق.

[2]-معتوق عبد اللطيف، رع سابق، ص32.

[3]- المادة 65 مكرر 16 من القانون الإجراءات الجزائية، مرجع سابق.

[4]- المادة 65 مكرر 17 من القانون الإجراءات الجزائية، مرجع سابق.

وعلى هدى ذلك، لا يجوز اللجوء لعملية التسرب إلا في بعض الجرائم البالغة الخطورة والتي حددها المشرع الجزائري على سبيل الحصر في المادة 65 مكرر وهي: "جرائم المخدرات الجريمة المنظمة، جرائم تبييض الأموال والإرهاب الجرائم المتعلقة بالتشريع الخاص بالصرف، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات".[1]

ويمكن تصور عملية التسرب في الجرائم الالكترونية في ولوج ضابط أو عون الشرطة القضائية إلى العالم الافتراضي ومشاركته في محادثات غرف الدردشة أو حلقات النقاش المباشر حول تقنيات اختراق شبكات الاتصال أو بث الفيروسات أو انخراطه في مجموعات أو نوادي الهاكر، مستخدما في ذلك أسماء وصفات مستعارة وهمية ظاهرا فيها بمظهر طبيعي كما لو كان واحد مثلهم قصد استدراجهم والكشف عنهم وعن أعمالهم الإجرامية.[2]

نظرا للخطورة التي يشكلها إجراء التسرب على حرمة الحياة الخاصة للمشتبه فيه، فقد قيده المشرع بجملة من الشروط والضوابط الواجب مراعاتها قبل وأثناء مباشرته وهي كالتالي:

الفرع الأول :الضوابط الإجرائية

تتطلب الضوابط الإجرائية للتسرب الإلكتروني الحصول على إذن قضائي مسبق، والذي يجب أن يتضمن مجموعة من الأحكام لضمان شرعية الإجراء وحماية الحقوق. لا يمكن لضابط أو عون الشرطة القضائية الشروع في عملية التسرب من تلقاء نفسه دون الحصول على هذا الإذن من الجهات القضائية المختصة، والتي تشمل وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه، وفقًا للمادة (65 مكرر 11) من قانون الإجراءات الجزائية[3].

[1]- المادة 65 مكرر 18من القانون الإجراءات الجزائية، مرجع سابق.

[2]-معتوق عبد اللطيف، رع سابق، ص33.

[3]- المادة 65 مكرر 11 من القانون الإجراءات الجزائية، مرجع سابق.

1. **الإذن القضائي:**

- **ضرورة الإذن المسبق** :لا يجوز الشروع في عملية التسرب الإلكتروني دون إذن قضائي مسبق.

- **الجهة المختصة بإصدار الإذن** :وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه[1].

- **الرقابة المباشرة** :تتم عملية التسرب تحت الرقابة المباشرة للجهة القضائية التي أصدرت الإذن لمنع التجاوزات والتعسف في استخدام هذا الحق[2].

2. **الإذن المكتوب:**

- **ضرورة الكتابة** :يجب أن يكون الإذن مكتوبًا، وإلا كان الإجراء باطلاً. المادة (65 مكرر 15) تنص بوضوح على ضرورة أن يكون الإذن مكتوبًا تحت طائلة البطلان[3].

3. **محتوى الإذن:**

- **نوع الجريمة** :يجب أن يتضمن الإذن ذكر نوع الجريمة التي تبرر عملية التسرب.

- **اسم ضابط الشرطة القضائية** :يجب تحديد اسم ضابط الشرطة القضائية الذي ستتم العملية تحت مسؤوليته.

---

[1]-نفس المرجع.

[2]-علاوة هوام " التسرب كآلية للكشف عن جرائم في القانون الجزائري " مجلة الفقه والقانون كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر بباتنة 2012 ، ص 03.

[3]- المادة 65 مكرر 15 من القانون الإجراءات الجزائية، مرجع سابق.

- **المدة الزمنية** :يجب تحديد المدة المطلوبة لعملية التسرب، والتي لا يجب أن تتجاوز أربعة أشهر. يمكن تجديد هذه المدة وفقًا لمقتضيات التحري والتحقيق، ولكن ضمن الشروط نفسها.

4. **صلاحيات القاضي:**

- **إيقاف الإجراء** :يملك القاضي الذي أصدر الإذن صلاحية الأمر بإيقاف عملية التسرب في أي وقت قبل انقضاء الأجل المحدد[1].

الفرع الثاني: الضوابط الموضوعية

إلى جانب الضوابط الإجرائية، أحاط المشرع عملية التسرب بضوابط أخرى موضوعية يمكن إيجازها في عنصرين أساسيين[2]:

1. **عنصر التسبيب:**

- يتمثل في المبررات والحجج التي أقنعت الجهات القضائية المختصة لمنح الإذن بإجراء التسرب.

- يشمل الدوافع والأسباب التي دفعت ضابط الشرطة القضائية للجوء إلى هذه العملية، والتي عادة ما تكون ضمن موضوع طلب الإذن[3].

2. **تحديد نوع الجريمة:**

- يتعلق بتحديد نوع الجريمة التي يُصدر لها الإذن بالتسرب، والتي يجب ألا تخرج عن نطاق الجرائم السبع التي حددها المشرع.

---

[1]- براهيمي جمال، مرجع سابق، ص 87.

[2]-زورو هدي، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، العدد الحادي عشرة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة 2014، ص 121 .

[3]-نفس المرجع.

- هذه الجرائم تعتبر خطيرة لسرعة انتشارها وتأثيرها الذي يتجاوز الحدود الوطنية، كما تشمل جرائم تخطيطية تستخدم وسائل متقدمة لمحو آثار الجريمة.
- يعتبر اللجوء إلى التسرب للكشف عن مثل هذه الجرائم وإلقاء القبض على مرتكبيها أمرًا مبررًا ومفيدًا[1].

تحقيق الإجراءات الموضوعية هذه يسهم في ضمان شرعية وفعالية عمليات التسرب، بما يضمن تحقيق العدالة وحماية المجتمع من الجرائم الخطيرة في عصر التكنولوجيا الرقمية[2].

المطلب الثاني: اعتراض المراسلات والمراقبة الإلكترونية

طور الاتصال الحديث واستخدام الشبكات المعلوماتية بشكل متزايد قد دفع المشرعين في العديد من الدول إلى مراجعة قوانينهم الإجرائية لتضمين إجراءات محددة للاعتراض على المراسلات ومراقبة الاتصالات الإلكترونية. وقد كانت فرنسا من أوائل الدول التي اتخذت هذه الخطوة في عام 1991، تلاها الولايات المتحدة في عام 2000، وأوصت الاتفاقية الأوروبية حول الجرائم الإلكترونية بضرورة تبني هذه الإجراءات في تشريعات الدول الأعضاء[3].

وقد اتخذ المشرع الجزائري خطوات مماثلة، حيث أدرج قانون الإجراءات الجزائية رقم 22/06 تعديلات وتكميلات عام 2006 فصلاً كاملاً يتعلق بإجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور. وضمن هذا الفصل، تم تحديد نطاق هذه الإجراءات ووضع

[1]-علاوة هوام، مرجع سابق، ص07.
[2]-علاوة هوام، مرجع سابق، ص07.
[3]- بوكر رشيدة، مرجع سابق، ص 442.

ضوابط لضمان استخدامها بشكل مشروع[1]. وتم تعزيز هذا النظام بواسطة القانون رقم 04/09 الصادر في عام 2009[2].

تبني هذه الإجراءات يعكس الاهتمام المتزايد بمكافحة الجرائم الإلكترونية وضمان سلامة الشبكات الإلكترونية. وبفضل فعالية هذه الإجراءات في تعقب الدليل وإثبات الجرائم الإلكترونية، فإنها قد حظيت بدعم واسع من الدول المختلفة، بما في ذلك الدول الأوروبية والجزائر[3].

الفرع الأول: مفهوم الاعتراض والمراقبة الإلكترونية

عرفت لجنة خبراء البرلمان الأوروبي بمناسبة اجتماعها المنعقد بستراسبورغ في 2006/10/06 لدراسة أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية عملية اعتراض المراسلات بأنها عملية مراقبة سرية المراسلات السلكية واللاسلكية، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب جريمة.[4]

وقد اقتبس المشرع الجزائري هذا التعريف بشيء من التفصيل في المادة (65) مكرر 5 من قانون الإجراءات الجزائية، إذ اعتبر عملية مراقبة المراسلات بأنها اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للانتهاج والتوزيع، التخزين الاستقبال والعرض.[5]

---

[1]- براهيمي جمال، مرجع سابق، ص 90.

[2]- قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3]-نفس المرجع.

[4]- بوكر رشيدة، مرجع سابق، ص 446.

[5]- المادة 65 مكرر 05 من القانون الإجراءات الجزائية، مرجع سابق.

فبالرجوع إلى نص هذه المادة، نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلا للاعتراض بتلك المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية دون أن يشير إلى طبيعة هذه المراسلات، مما يفتح المجال لمختلف الرسائل المكتوبة، بغض النظر عن شكلها ،كتابة رموز ،أشكال (صور) أو الدعامة التي تنصب عليها (ورقية أو رقمية)، أو الوسيلة المستعملة لإرسالها سلكية كانت كالفاكس تلغرام أم لاسلكية (البريد الالكتروني، الهاتف النقال)، باستثناء الكتب والمجلات والرسائل والحوليات التي تعد مراسلات خاصة.[1]

وقد تأكد هذا الأمر في المادة 2 فقرة ("و ") من القانون رقم 04/09 التي عرفت الاتصالات الالكترونية بأنها "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة الكترونية".[2]

وبغض النظر عن طبيعة المراسلات السلكية واللاسلكية فعملية الاعتراض أو المراقبة تتم واسطة ترتيبات تقنية سرية يتم وضعها دون علم أو موافقة المعنيين، وذلك لغرض التصنت والتقاط وتثبيت وبث وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه فيه بصفة خاصة أو سرية في أماكن خاصة أو عمومية، ومن ثم استعمالها كدليل لمواجهة المتهم.[3]

ولعل من أهم المراسلات الالكترونية التي يهتم القائمين بالتحقيق بإخضاعها لعملية الاعتراض والمراقبة والتي تمثل مصدرا غنيا لأدلة إثبات الجرائم الالكترونية، المراسلات عبر البريد الالكتروني، كون هذه التقنية من أكثر الوسائل الحديثة استخداما للاتصال عبر الانترنت ومجالا خصبا للربط بين الأشخاص في مختلف أنحاء العالم بسرعة فائقة ودون حواجز. فهو

---

[1]- براهيمي جمال، مرجع سابق، ص 90.

[2]-المادة 02 من قانون رقم 09-04، مرجع سابق.

[3]- مصطفى محمد موسى المراقبة الالكترونية عبر شبكة الانترنت دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية، الكتاب الخامس، دار الكتب والوثائق القومية المصرية، القاهرة، 2003، ص 180

بمثابة نظام تبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة، أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة كما يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم ولا يمكن الدخول إليه بسهولة لأنه محاط بحماية فنية.[1]

الفرع الثاني: القيود الواردة على عملية اعتراض ومراقبة المراسلات

إذا كان أسلوب اعتراض المراسلات السلكية واللاسلكية دون علم أصحابها قد اثبت جدارته في كشف وإثبات الكثير من الجرائم الغامضة كتلك المتعلقة بالجرائم الالكترونية، فهو في الوقت نفسه يمثل انتهاكا خطيرا لحرمة الحياة الخاصة للإفراد واعتداء صارخا على سرية مراسلاتهم واتصالاتهم التي كفلتها معظم الدساتير والتشريعات العقابية بالحماية.[2]

ولتحقيق التوازن بين ضرورة التحقيق التي تفرضها المصلحة العامة واحترام الحياة الخاصة التي تفرضها المصلحة الفردية، تمت إحاطة عملية الاعتراض بعدد من القيود القانونية التي تضمن عدم تعسف السلطات العامة وتصون الحرية الفردية، والتي نلخصها فيما يلي:[3]

أولا: الحصول على إذن السلطة القضائية المختصة

قيد القانون اللجوء إلى عملية اعتراض او مراقبة المراسلات بشرط الحصول المسبق على إذن مكتوب ومسبب من الجهات القضائية المختصة المتمثلة عادة في وكيل الجمهورية أثناء مرحلة التحقيق الابتدائي، أو قاضي التحقيق في مرحلة التحقيق القضائي وإلا كان هذا

[1]- ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى الجزائر، 2011، ص157.

[2]- ربيحة زيدان، مرجع سابق، ص159.

[3]-زهية معمش، نسمة غائم الثبات الجنائي في الجرائم الالكترونية مذكرة الماستر تخصص قانون الخاص والعلوم الجنائية جامعة عبد الرحمان ميرة بجاية 2013، ص29.

الإجراء باطلا، فالسلطة القضائية وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لازمة لمشروعية الإجراء. [1]

وحتى يكون الإذن صحيحا ومنتجا لآثاره، يجب أن يتضمن جملة من العناصر الأساسية وهي:[2]

1. **طبيعة الجريمة :**

التي تبرر الإجراء والتي ينبغي أن تكون من ضمن الجرائم التي يجوز فيها اللجوء إلى هذه العملية، وإذا اكتشفت جرائم أخرى غير تلك الوارد ذكرها في الإذن فلا تبطل الإجراءات العارضة.[3]

2. **التعريف بالعملية:**

بمعني تحديد المراسلات والاتصالات المطلوب اعتراضها وتسجيلها تحديد الأماكن المقصودة سكنية أو غير سكانية عامة أو خاصة، إلى جانب تحديد المدة التي تستغرقها التدابير التقنية اللازمة في عملية الاعتراض، والتي يجب أن لا تتجاوز أربعة أشهر قابلة للتجديد ضمن الشروط نفسها، حسب تقدير السلطة مصدرة الإذن لمقتضيات التحري والتحقيق. وهي المدة نفسها التي حددها المشرع الفرنسي في المادة (100-1) من قانون إجراءات الجزائية الفرنسي.[4]

ولا يكفي الحصول على إذن مشمول بالعناصر المذكورة لإتمام عملية اعتراض المراسلات أو المراقبة، إنما لا بد أن تنفذ هذه العمليات تحت الرقابة المباشرة للسلطات التي أذنت بها، وذلك من خلال قيام ضابط الشرطة القضائية المأذون له بإحاطتها علما

---

[1]-نفس المرجع

[2]- براهيمي جمال، مرجع سابق، ص 93.

[3]-نفس المرجع.

[4] - voir l'article (100-1) de la loi N 2001-1062, de 15 novembre 2001 portant code de procédures pénales, JORF, 16 nov 2001, p 18215.

بكل خطوات وتطورات عملية الاعتراض والمراقبة وإخبارها بشكل دوري ومستمر عن عمليات وضع الترتيبات التقنية لهذا الغرض، ساعة بداية وانتهاء هذه العمليات على أن يدون كل ذلك في محاضر مرقمة. وبهذه الطريقة فقط نكون قد حققنا الغرض الحقيقي من هذه العمليات.[1]

ثانيا: تسبيب اللجوء إلى اعتراض أو مراقبة المراسلات

يقصد به المبرر الشرعي والضرورة الملحة التي تستدعي القيام بعملية اعتراض أو مراقبة المراسلات، وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري والتحقيق دون اللجوء إلى هذه العملية، وفي هذا الشأن يشترط على وكيل الجمهورية أو قاضي التحقيق المختص قبل منح الإذن بتنفيذ العملية المذكورة تقدير جدواها وجدية دواعيها والفائدة المنتظرة منها في إظهار الحقيقة وكشف غموض الجريمة والجناة مسبقا، ثم موازنة كل هذه العناصر للتأكد مما إذا كانت كافية لخرق مبدأ حرمة الحياة الخاصة. فإذا ارتأى بان التسبيب غير كاف رفض طلب الإذن.[2]

والجدير بالذكر هنا هو أنه إلى جانب إمكانية القيام بمراقبة الاتصالات الالكترونية في إطار التحريات والتحقيقات القضائية من أجل الوصول إلى أدلة لم يكن بالإمكان الوصول إليها دون اللجوء إلى هذا الإجراء، فقد أجاز المشرع الجزائري كذلك تطويع هذه التقنية الغرض الوقاية من احتمال وقوع جرائم خطيرة قد تهدد كيان الدولة كما قررته المادة الرابعة (4) من القانون (04/09).[3] وهنا يصبح مفهوم الضرورة الملحة التي تستدعي القيام بإجراءات المراقبة الالكترونية مبهما وغير واضح، خاصة إذا تعلق الأمر بالجرائم

[1]-زهية معمش، مرجع سابق، ص30.
[2]-زهية معمش، مرجع سابق، ص30.
[3]-المادة 4 من قانون رقم 09-04، مرجع سابق.

التي تهدد النظام العام لأن مصطلح النظام العام غير محدد المعالم وقد تنجر عنه اختلالات كبيرة من شأنها المساس بحرية الأفراد.[1]

ثالثا: تحديد الجرائم محل الاعتراض والمراقبة

إن الاستعانة بعملية اعتراض أو مراقبة المراسلات الالكترونية لغرض التحقيق غير مسموح في كافة الجرائم إنما مجال تطبيقها يتوقف عند نوع محدد فقط وهي كالتالي:

– الجرائم المذكورة على سبيل الحصر في نص المادة (65) مكرر (5) من قانون الإجراءات الجزائية، وهي جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، جرائم تبييض الأموال أو الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد والجرائم الماسة بأنظمة المعالجة الآلية.[2]

– الجرائم المنصوص عليها في الفقرات أ، ب، ج، د من المادة (04) من قانون (04/09) المتمثلة في الأفعال الموصوفة بجرائم الإرهاب أو التخريب الاعتداءات على منظومة معلوماتية الماسة بأمن الدولة بما فيها تلك التي تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني.[3]

رابعا: سرية الإجراءات وكتمان السر المهني

أي ينبغي أن تنفذ عملية الاعتراض والمراقبة في سرية تامة ودون علم أو رضا المشتبه فيه أو صاحب الأماكن، مع مراعاة عدم المساس بالسر المهني المقرر بنص المادة (45 فقرة (4) قانون إجراءات جزائية.[4]

---

[1]- نوال شعلال سلطة القاضي الجنائي في تقدير الأدلة، مذكرة مقدمة لنيل شهادة الماجستير ، فرع قانون العقوبات والعلوم الجنائية، جامعة سكيكدة، 2008، ص48.

[2]- المادة 65 مكرر 05 من القانون الإجراءات الجزائية، مرجع سابق.

[3]-المادة 04 من قانون رقم 09-04، مرجع سابق.

[4]- المادة 45 من القانون الإجراءات الجزائية، مرجع سابق.

أن المشرع الجزائري لم يشر صراحة إلى كيفية وضع الأدلة المحصل من عملية اعتراض ومراقبة المواصلات التسجيلات السمعية البصرية، البيانات الرقمية في أحراز مختومة، مما يطرح التساؤل حول مدى اعتبارها من قبيل الأشياء المضبوطة التي تخضع لأحكام المادة (84) من قانون الإجراءات الجزائية وحكم المادة(5/45) من القانون نفسه.

علما بأن هذه التسجيلات والبيانات تعتبر أدلة إثبات رقمية أصلية تقتضي الشرعية الجزائية حفظها بطريقة خاصة بوضعها في أحراز مختومة تضمن عدم التلاعب والعبث فيها بالحذف أو الإضافة، وضمها إلى ملف الإجراءات مع المحاضر التي تصف أو تنسخ محتواها للكشف عن الحقيقة.[1]

ومن ذلك كانت الحاجة إلى فتح المشرع المجال أمام سلطات التحقيق والاستدلال للاستعانة بذوي الاختصاص سواء عن طريق تسخير كل من لديهم دراية و مؤهلات في مجال سير تكنولوجيات الإعلام والاتصال من اجل تزويدهم بالمساعدة الفنية والتقنية الممكنة لتسهيل وإنجاح أية عملية من عمليات التحقيق بما فيها المراقبة الالكترونية للاتصالات كما هو منصوص في المادة (05) فقرة أخيرة من القانون رقم (04/09).[2]

أو عن طريق تكليف هؤلاء المختصين باستعمال الوسائل التقنية المناسبة والضرورية للحيلولة دون الوصول الى المعطيات التي تشكل محل الجريمة أو تحتوي أدلة لها الموجودة داخل المنظومة المعلوماتية و منع الاطلاع عليها أو نسخها أو تهريبها أو تدميرها وفقا لما تقتضيه المادتين (7و8) من القانون رقم (04/09).[3]

ويجب الاعتراف بأن تكريس المشرع الجزائري لإجراءات اعتراض المراسلات والمراقبة الالكترونية يعد خطوة جريئة تحسب له على اعتبار أنها من اخطر إجراءات التحري والتحقيق

---

[1]- نوال شعلال، مرجع سابق، ص50.
[2]-المادة 05 من قانون رقم 09-04، مرجع سابق.
[3]-المادتين 7 و8 من قانون رقم 09-04، مرجع سابق.

عبر العالم الافتراضي نظرا لما تحمله من انتهاكات مباشرة لخصوصيات الإنسان هذا من جهة، ومن جهة أخرى لان الفقه الجنائي لم يحسم الأمر بعد ويرى بان المراقبة الالكترونية لا تزال محل نظر في القانون لضرورة الالتزام بما هو مقرر في القوانين والدساتير من ضمانات احترام الحق في الخصوصية.[1]

وفصل الحديث، أنه رغم المخاوف الكثيرة التي أبداها الفقه حيال إجراءات التحقيق المستحدثة لما تحمله من عدوان على الحق في الخصوصية الذي يعد من أقوى الحقوق الدستورية الفردية، إلا أن الواقع يثبت بأن الاستعانة بهذه الإجراءات أصبح ضرورة ملحة للتصدي الفعال لظاهرة الإجرام المعلوماتي والضرورة هنا ترجع من الناحية إلى الارتفاع المتزايد لمعدل الإجرام الالكتروني نتيجة اقتحام المعلوماتية كل مجالات الحياة، ومن ناحية أخرى إلى ثبوت عجز وقصور تقنيات التحقيق التقليدية في مواجهة الجرائم الالكترونية الحديثة نتيجة عدم ملائمتها مع الطبيعة الخاصة لهذه الجرائم[2].

خلاصة الفصل:

أن المشرع عند محاولته توسيع نطاق تطبيق إجراءات التحقيق التقليدية لتشمل الجرائم الإلكترونية كان يواجه العديد من التحديات التي تنبع من خصوصية هذه الجرائم. وتشمل هذه التحديات الإجراءات التقليدية مثل التفتيش، الضبط، المعاينة، والخبرة. هذه الإجراءات، في صورتها التقليدية، قد لا تكون كافية أو فعّالة للتعامل مع الطبيعة الفريدة للجرائم الإلكترونية والأدلة المرتبطة بها. لذا، يتطلب الأمر تطويرًا وتحديثًا لتلك الإجراءات بما يتناسب مع الخصوصية الفريدة للجرائم الإلكترونية.

[1]- نوال شعلال، مرجع سابق، ص51.
[2]- نوال شعلال، مرجع سابق، ص51.

الخاتمة

الخاتمة

في الختام، يظهر أن التحقيق الجنائي للجرائم الإلكترونية يشكل تحدياً متنامياً في عصرنا الحالي الذي يتسم بالتطور التكنولوجي السريع. تتميز هذه الجرائم بخصائص فريدة تجعل منها صعبة التحقيق والمكافحة، مثل الطبيعة الافتراضية للجرائم، وسرعة انتشارها، وصعوبة تتبع الجناة. لذلك، يتطلب التحقيق الجنائي في هذه الجرائم تطوير أساليب وتقنيات جديدة، وتعزيز التعاون الدولي، وتحديث التشريعات الوطنية.

من خلال التزام الجهات المعنية بتحسين البنية التحتية الرقمية، وتطوير قدرات الأجهزة الأمنية والقضائية في مجال التحقيق الجنائي، يمكن تعزيز القدرة على مكافحة الجرائم الإلكترونية بفعالية. كما يجب توعية الجمهور بمخاطر هذه الجرائم، وتوفير التدريب المناسب للمحققين الجنائيين على التقنيات الحديثة.

باعتبار التحقيق الجنائي للجرائم الإلكترونية جزءاً حيوياً من الجهود الرامية إلى تعزيز الأمن الرقمي وحماية المجتمع، فإن تعزيز التعاون الدولي وتطوير التقنيات والأساليب المستخدمة في التحقيق يعد ضرورة ملحة. من خلال العمل المشترك والجهود المتواصلة، يمكننا تحقيق تقدم ملحوظ في مكافحة الجرائم الإلكترونية وتعزيز الأمن الرقمي على الصعيدين الوطني والدولي.

ويمكن تقديم النصائح التالية:

1. ينبغي توفير التدريب المناسب للمحققين الجنائيين لتطوير مهاراتهم في جمع الأدلة الرقمية وتحليلها، واستخدام التقنيات الحديثة في التحقيق.
2. استخدام التقنيات الجديدة مثل تحليل البيانات الضخمة والذكاء الاصطناعي يمكن أن يساعد في تحليل الأدلة الرقمية بطريقة أكثر فعالية ودقة.
3. توعية الجمهور بمخاطر الجرائم الإلكترونية وكيفية حماية أنفسهم منها يمكن أن يقلل من انتشار هذه الجرائم ويسهل عملية التحقيق.

4. يجب على المحققين الجنائيين المشاركة في دورات تدريبية منتظمة لتحديث مهاراتهم ومعرفتهم بالتقنيات الحديثة وأساليب الجرائم الإلكترونية الجديدة.

5. توثيق كل خطوة يتم اتخاذها في عملية جمع وتحليل الأدلة الرقمية لضمان الشفافية وإمكانية التحقق من الإجراءات المتبعة.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

باللغة العربية

المصادر:

أولا: قوانين

1. قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ثانيا: أوامر

1. الأمر رقم 20-04 المؤرخ في 11 محرم عام 1442 الموافق 30 غشت سنة 2020، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية. (الجريدة الرسمية عدد 51 لسنة 2020).

ثالثا: الاتفاقيات

1. الاتفاقية الأوروبية حول الجرائم المعلوماتية لعام 2001.

المراجع:

أولا: الكتب

1. مصطفى محمد موسى المراقبة الالكترونية عبر شبكة الانترنت دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية، الكتاب الخامس، دار الكتب والوثائق القومية المصرية، القاهرة، 2003.
2. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006.

3. عفيفي كمال عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، طبعة ثانية، منشورات الحلبي القانونية، دمشق، 2007.
4. خالد ممدوح، أمن الجريمة الإلكترونية الدار الجامعية الإلكترونية، الإسكندرية، 2008.
5. حسن الجوخندار، التحقيق الابتدائي في قانون الأصول المحاكمات الجزائية، دار الثقافة عمان، الطبعة الأولى، 2008.
6. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة للطباعة والنشر، الجزائر، ط2، 2009.
7. عبد العزيز ،سعد أبحاث تحليلية في قانون الإجراءات الجزائية، دار هومة للطباعة والنشر والتوزيع، الجزائر، بدون طبعة ، 2009.
8. بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، 2010.
9. ضياء مصطفى عثمان السرقة الإلكترونية، دار النفائس، عمان، الطبعة الأولى، 2011.
10. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت دار الثقافة للنشر و التوزيع، عمان، 2011.
11. بوكر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، 2012.
12. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات دراسة مقارنة، دار الفكر الجامعي، الإسكندرية 2013.
13. غسان مدحت الخبري أصول التحقيق الإبتدائي كحق من حقوق الإنسان دار الراية للنشر والتوزيع، الأردن، ط1، 2013.

14. ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى الجزائر، 2011.

15. لفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، الطبعة الأولى، د س.

ثانيا: رسائل جامعية

أ. رسائل دكتوراه

1. فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري و اليمني، أطروحة لنيل شهادة الدكتوراه في القانون، فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق جامعة الجزائر 1، الجزائر،2011.

2. صالح شنين، الحماية الجنائية للتجارة الإلكترونية، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، جامعة أبو بكر بلقايد تلمسان، كلية الحقوق، الجزائر 2013.

3. بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم، جامعة الجزائر، كلية الحقوق، الجزائر، 2015.

4. راهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص قانون كلية الحقوق جامعة تيزي وزو، 2018.

ب. مذكرات ماجستير

1. نوال شعلال سلطة القاضي الجنائي في تقدير الأدلة، مذكرة مقدمة لنيل شهادة الماجستير ، فرع قانون العقوبات والعلوم الجنائية، جامعة سكيكدة، 2008.

2. أحمد بن زايد جوهر الحسن المهدي، تفتيش الحاسب الآلي وضمانات المتهم، مذكرة لنيل درجة ماجستير في القانون، كلية– الحقوق جامعة القاهرة، 2009.

3. طيبي الطيب، البحث والتحقيق في جريمة تبييض الأموال في التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في الحقوق جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية قسم الحقوق الجزائر2012.
4. معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم الالكترونية في التشريع الجزائري و التشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج لخضر، بائنة كلية الحقوق والعلوم السياسية قسم الحقوق، 2011-2012.
5. أحمد مسعود مريم، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة لنيل شهادة ماجستير في القانون الجنائي، جامعة ورقلة 2013.
6. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، جامعة مولود معمري تيزي وزو كلية الحقوق والعلوم السياسية الجزائر، سنة 2013.
7. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير جامعة تبسة، 2013.
8. بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة ماجستير 2014.

ت. مذكرات ماستر

1. زهية معمش، نسمة غائم الثبات الجنائي في الجرائم الالكترونية مذكرة الماستر تخصص قانون الخاص والعلوم الجنائية جامعة عبد الرحمان ميرة بجاية 2013.
2. عباسي خولة الوسائل الحديثة للإثبات في القانون الجنائي مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، 2014.

3. قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة مكملة لنيل شهادة الماستر أكاديمي في القانون، تخصص قانون عام للأعمال جامعة قاصدي مرباح ورقلة، 2014.
4. جواحي عبد الستار، جرائم الحاسوب – دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري مذكرة تخرج تدخل ضمن متطلبات الحصول على شهادة الماستر في العلوم الإسلامية، جامعة الشهيد حمه لخضر كلية العلوم الإجتماعية و الإنسانية، قسم العلوم الإنسانية، الجزائر 2015.
5. بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق جامعة محمد خيضر بسكرة كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر 2016.
6. السوفي نور الهدى التحقيق في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر أكاديمي في الحقوق، تخصص قانوني جنائي، جامعة قاصدي مرباح ورقلة 2017.

رابعا: مجالات

1. على محمود على محمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، نظمته أكاديمية شرطة دبي، في الفترة من 26 الى 28 أفريل 2003.
2. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية،2006.
3. بن كثير بن عيسى، الإجراءات الخاصة المطبقة على الإجرام الخطير، نشرة القضاة، مديرية الدراسات القانونية والوثائق، العدد 63، 2008.

4. موسي مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلومات والقانون" المنعقد بأكاديمية الدراسات العليا طرابلس، في 28و 2009/10/29.
5. خالد ممدوح إبراهيم فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي إسكندرية 2009.
6. مصطفاوي عبد القادر، أساليب البحث و التحري الخاصة و إجراءاتها، مجلة المحكمة العليا، العدد 02، 2009.
7. فوزي عمارة، إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية كلية الحقوق والعلوم السياسية جامعة منتوري قسنطينة ، العدد 33 جوان 2010.
8. رشيدة بوكر الدليل الالكتروني ومدى حجيته في الاثبات الجزائي في القانون الجزائري ،مجلة جامعة دمشق للعلوم الاقتصادية المجلد 27 العدد الثاني 2011.
9. علاوة هوام " التسرب كآلية للكشف عن جرائم في القانون الجزائري " مجلة الفقه والقانون كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر بباتنة 2012.
10. عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي مجلد ،22، عدد 86، صادر عن مركز بحوث الشرطة القيادة العامة لشرطة الشارقة الإمارات العربية المتحدة 2013.
11. زورو هدي، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، العدد الحادي عشرة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة 2014.

12. آمال بن صوليح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني وفي الجزائر، مداخلة الملتقي الدولي حول " الإجرام اليبيرالي المفاهيم والتحديات ، 11-12 أفريل 2017.

باللغة الفرنسية

1. FIRAL-SCHUHL Christiane, cyber droit- le droit a l'épreuve de l'internet, 6ém édition Dalloz, Paris, 2011-2012.
2. l'article (100-1) de la loi N 2001-1062, de 15 novembre 2001 portant code de procédures pénales, JORF, 16 nov2001.

الفهرس

الفهرس

مقدمة..... 1
الفصل الأول..... 6
المبحث الأول: ماهية تحقيق الجنائي الجرائم الإلكترونية..... 8
المطلب الأول: مفهوم الجريمة الإلكترونية 8
الفرع الأول: تعريف الجريمة الإلكترونية لغة 9
الفرع الثاني: تعريف الجريمة اصطلاحا 10
الفرع الثالث: تعريف الجريمة الإلكترونية فقها 11
الفرع الرابع: تعريف الجريمة الإلكترونية القانوني 11
المطلب الثاني: مفهوم التحقيق الجنائي ومحقق الجنائي 15
الفرع الأول: تعريف التحقيق الجنائي في الجريمة الإلكترونية 16
الفرع الثاني: تعريف المحقق الجنائي 18
المبحث الثاني: خصائص تحقيق الجنائي في الجرائم الإلكترونية 21
المطلب الأول: أسلوب التحقيق الابتدائي في الجريمة الإلكترونية..... 22
الفرع الأول: وضع خطة عمل التحقيق 22
الفرع الثاني: تشكيل فريق التحقيق 29
المطلب الثاني: العناصر الأساسية للتحقيق الابتدائي في مجال البرمجة الإلكترونية . 30
الفرع الأول: الإجراءات التي يجب مراعاتها قبل البدء في التحقيق 30
الفرع الثاني: الإجراءات التي يجب مراعاتها أثناء التحقيق..... 31
الفصل الثاني..... 36

الفهرس

المبحث الأول: إجراءات التحقيق الجنائي المألوفة في الجرائم الإلكترونية..... 38

المطلب الأول: التفتيش في البيئة الإلكترونية..... 38

الفرع الأول: محل التفتيش الإلكتروني..... 39

الفرع الثاني: ضمانات التفتيش في البيئة الإلكترونية..... 43

المطلب الثاني: ضبط الأدلة في الجرائم الإلكترونية 46

المبحث الثاني: إجراءات التحقيق الجنائي الخاصة في الجرائم الإلكترونية 50

المطلب الأول: التسرب الإلكتروني 50

الفرع الأول :الضوابط الإجرائية 52

الفرع الثاني: الضوابط الموضوعية..... 54

المطلب الثاني: اعتراض المراسلات والمراقبة الإلكترونية..... 55

الفرع الأول: مفهوم الاعتراض والمراقبة الإلكترونية 56

الفرع الثاني: القيود الواردة على عملية اعتراض ومراقبة المراسلات 58

الخاتمة 59

قائمة المصادر والمراجع..... 59

ملخص

ملخص:

في العصر الرقمي، أصبحت الجرائم الإلكترونية واحدة من أخطر التحديات التي تواجه المجتمعات والحكومات. تتميز هذه الجرائم بخصائص فريدة، حيث تُرتكب في بيئة افتراضية باستخدام تقنيات المعلومات والاتصالات، مما يجعل اكتشافها ومكافحتها أمراً معقداً وصعباً. يشمل التحقيق الجنائي في الجرائم الإلكترونية مجموعة من الإجراءات والتقنيات التي تهدف إلى جمع الأدلة الرقمية وتحليلها، وتقديمها بشكل قابل للاستخدام في المحاكم.

التحقيق الجنائي في الجرائم الإلكترونية يتطلب تطوير تقنيات وأساليب جديدة تتماشى مع الطبيعة الخاصة لهذه الجرائم. كما يستلزم التعاون الفعال بين الدول وتحديث التشريعات لضمان مواجهة فعالة لهذه التحديات. من خلال تحسين الجهود الوطنية والدولية وتعزيز القدرات التقنية للمحققين، يمكن تحقيق تقدم كبير في مكافحة الجرائم الإلكترونية وحماية المجتمع من مخاطرها.

كلمات المفتاحية: الجرائم الإلكترونية، التحقيق الجنائي، التحديات.

résumé:

À l’ère du numérique, la cybercriminalité est devenue l’un des défis les plus graves auxquels sont confrontés les sociétés et les gouvernements. Ces crimes présentent des caractéristiques uniques, car ils sont commis dans un environnement virtuel utilisant les technologies de l’information et de la communication, ce qui rend leur détection et leur lutte complexes et difficiles. Les enquêtes médico-légales sur la cybercriminalité comprennent un ensemble de procédures et de techniques visant à collecter et analyser des preuves numériques et à les présenter sous une forme utilisable devant les tribunaux.

Les enquêtes médico-légales sur les cybercrimes nécessitent le développement de nouvelles technologies et méthodes compatibles avec la nature spécifique de ces délits. Cela nécessite également une coopération efficace entre les pays et une mise à jour de la législation pour garantir une réponse efficace à ces défis. En améliorant les efforts nationaux et internationaux et en renforçant les capacités techniques des enquêteurs, des progrès significatifs peuvent être réalisés dans la lutte contre la cybercriminalité et dans la protection de la société contre ses dangers.

ملخص

Mots-clés : cybercriminalité, enquête criminelle, enjeux.