الخبرة في التحقيقات الرقمية كآلية للبحث والتحري عن الجرائم الخاصة

Expertise in Digital Investigations as a Mechanism for the Detection and Inquiry into Specific Crimes

دوارة فاطمة الزهرة (*) طالبة دكتوراه
كلية الحقوق والعلوم السياسية
مخبر الدراسات والبحوث في القانون والأسرة والتنمية الإدارية
جامعة محمد بوضياف-المسيلة- الجزائر
fatma-zohra.douara@univ-msila.dz

عبدلي حمزة أستاذ محاضر أ
كلية الحقوق والعلوم السياسية
مخبر الدراسات والبحوث في القانون والأسرة والتنمية الإدارية
جامعة محمد بوضياف-المسيلة-الجزائر
Hamza.abdelli@univ-msila.dz

تاريخ الارسال: 2025/10/06	تاريخ القبول: 2025//12/14	تاريخ النشر: 2025/12/29

ملخص:

يشهد الواقع المعاصر توسعًا كبيرًا في الجرائم الرقمية، ما يفرض تحديات على الجهات المختصة بالتحقيق، إذ لم تعد الخبرات التقليدية كافية للكشف عنها أو جمع الأدلة، وتبرز الخبرة في التحقيقات الرقمية كأداة أساسية لتعزيز فاعلية البحث والتحري في الجرائم الخاصة، لما توفره من إمكانات تقنية للكشف عن الأدلة وحمايتها.

يعد تطوير قدرات المحققين الرقمية شرطًا ضروريًا لاستجابة قانونية أكثر كفاءة، إذ يعيق نقص التأهيل التقني وضعف البنية التكنولوجية جهود كشف الجرائم وملاحقة مرتكبيها. كما يمثل التدريب وتوفير الموارد التقنية والمادية مدخلًا للارتقاء بقدرات فرق التحقيق وضمان العدالة الرقمية، كما تعزز الخبرة الرقمية قدرة المحققين على مواجهة التطور المستمر في أساليب الجرائم الإلكترونية وحماية الحقوق القانونية، مما يجعلها عنصرًا جوهريًا في فعالية التحقيقات الحديثة.

الكلمات المفتاحية: التحقيقات الرقمية؛ المحقق الإلكتروني؛ البحث والتحري؛ الجرائم الخاصة؛ الخبرة الرقمية.

***المؤلف المرسل:** ط د/دوارة فاطمة الزهرة

Abstract:

The contemporary context witnesses a marked expansion of cybercrimes, posing significant challenges to investigative authorities, as traditional expertise is insufficient to detect such offenses or collect relevant evidence, Digital investigative expertise is a core tool to enhance the efficiency of investigating private crimes, providing technical capabilities to uncover and safeguard electronic evidence.

Developing investigators' digital competencies is essential for an effective legal response, as insufficient training and weak technological infrastructure hinder crime detection and prosecution, Training programs and adequate technical resources strengthen investigative teams' capabilities and ensure digital justice, Digital expertise also enables investigators to address evolving cybercrime methods and protect legal rights, making it pivotal to the effectiveness of modern digital investigations.

Keywords: Digital Investigations; Digital Investigator; Inquiry and Investigation; Private Crimes; Digital Expertise.

مقدمة:

أدى التطور المتسارع في تكنولوجيا المعلومات والاتصالات إلى ظهور أنماط جديدة من السلوك الإجرامي، تُعرف بالجرائم الإلكترونية أو الجرائم الناشئة عن إساءة استخدام الحاسوب والشبكات المعلوماتية.

تمتاز هذه الجرائم بطبيعتها التقنية المعقدة، والأساليب المبتكرة التي يلجأ إليها مرتكبوها لإخفاء آثارهم، مما يضع تحديات كبيرة أمام الأساليب التقليدية للتحقيق، وفي ظل هذا الواقع برزت الحاجة الملحة إلى تطوير منهجيات البحث والتحري عن الجرائم الخاصة، بحيث تجمع بين القواعد الفنية للتحقيق الجنائي، والتقنيات الحديثة القادرة على التعامل مع مسرح الجريمة الإلكتروني بكفاءة عالية.

إن القائمين على البحث والتحري عن الجرائم الخاصة يجب أن يتصفوا بدرجة رفيعة من الكفاءة والخبرة، وهذه الصفات لا تقتصر على المعرفة النظرية بالقوانين والإجراءات، بل

تشمل أيضاً الإلمام العميق بالجوانب التقنية المرتبطة بالجريمة، فالكفاءة هنا تعني القدرة على توظيف أدوات التحليل الرقمي، واسترجاع البيانات المحذوفة، وتحديد مصادر الهجمات الإلكترونية، وربط الأدلة الرقمية بالوقائع المادية بشكل منهجي.

أما الخبرة، فهي تراكم المعرفة العملية الناتجة عن مواجهة مواقف تحقيق فعلية، بما يمكن المحقق من التعامل مع الأدلة الإلكترونية الحساسة دون الإضرار بها، وفهم طبيعة الجريمة الإلكترونية وسلوك مرتكبيها، واستباق أساليبهم في الإخفاء والتمويه، وبذلك يصبح المحقق قادراً على كشف غموض الجريمة، والوصول إلى الحقيقة بأعلى درجات الدقة والسرعة.

تكمن أهمية هذه الدراسة في مواجهة التحديات الناجمة عن التطور المتسارع في الجرائم الإلكترونية، التي تتسم بالتعقيد التقني والابتكار في إخفاء الأدلة، كما توفر الدراسة إطارًا لتطوير منهجيات البحث والتحري عن الجرائم الخاصة بما يضمن دمج الخبرة القانونية مع التقنيات الحديثة، مما يعزز قدرة المحققين على التعامل مع الأدلة الرقمية بكفاءة ودقة، وحماية الحقوق القانونية في الفضاء الرقمي.

أما بالنسبة لأهداف هذه الدراسة فتتمثل في:

-تسليط الضوء على أهمية الكفاءة والخبرة الرقمية للمحققين في البحث والتحري عن الجرائم الخاصة.

- توضيح المهارات التقنية اللازمة للتعامل مع الأدلة الرقمية واسترجاع البيانات وربطها بالوقائع.

-إبراز دور الخبرة العملية في تمكين المحقق من مواجهة أساليب الإخفاء والتمويه لدى مرتكبي الجرائم الإلكترونية.

من خلال ما تقدم يمكن طرح الاشكالية التالية: الى أي مدى تبرز أهمية تكوين المحققين حول الجرائم الإلكترونية؟ وما هي أهم أساسيات عمل المحققين في الأفعال المجرمة في البيئة الإلكترونية؟

للاجابة عن هذه الاشكاية اعتمدنا على المنهج الوصفي لوصف كل من التأهيل الذي يخضع له المحققون والمهارات الرقمية الواجب اكتسابها من طرف المحققين والتحديات المعيقة لتطوير هذه المهارات.

وبناءً على ذلك، نقسم هذا الموضوع الى كل من: المبحث الأول الذي يتناول التأهيل الرقمي للمحققين للبحث والتحري عن الجرائم الخاصة والمبحث الثاني يتعلق بتطوير المهارات الرقمية للمحققين والتحديات المعيقة لذلك.

المبحث الأول: التأهيل الرقمي للمحققين للبحث والتحري عن الجرائم الخاصة.

يُعدّ تأهيل المحققين في مجال البحث والتحري عن الجرائم الخاصة خطوة جوهرية لضمان فعالية العمل التحقيقي ودقته، إذ إن طبيعة هذه الجرائم وما تتسم به من خصوصية وحساسية تستلزم توفر كفاءات مهنية عالية، ويتطلب ذلك معالجة أوجه القصور المتمثلة في نقص الخبرة العملية والمعرفية لدى بعض المحققين، وهو ما قد ينعكس سلبًا على جودة الإجراءات ونتائجها، وفي المقابل، فإن رفع مستوى الكفاءة لا يتحقق إلا من خلال تزويد المحققين بمجموعة من المهارات المتخصصة التي تمكّنهم من التعامل مع هذه القضايا بمرونة ودقة، الأمر الذي يفرض دراسة شاملة لكل من أوجه النقص القائمة والمهارات الواجب اكتسابها لتحقيق الأداء الأمثل.

لذالك قمنا في هذا المبحث للتطرق لكل من: نقص خبرة وكفاءة المحققين في المجال الرقمي (المطلب الأول)، والى المهارات الواجب اكتسابها لرفع كفاءة المحققين(المطلب الثاني).

المطلب الأول: نقص خبرة وكفاءة المحققين في المجال الرقمي.

أصبحت الجرائم الإلكترونية تمثل تحدياً بارزاً لأجهزة التحقيق، نظراً لارتباطها بوسائل تقنية متطورة تختلف جذرياً عن الجرائم التقليدية، غير أن واقع الممارسة يكشف عن قصور في خبرة وكفاءة المحققين بمجال التعامل مع الأدلة الرقمية وأساليب ارتكاب هذه الجرائم، وهو ما انعكس سلباً على فعالية إجراءات البحث والتحري، ويعود هذا القصور، من جهة إلى عوامل ذاتية مرتبطة بالمحققين أنفسهم أو مايسمى بالعوائق الذاتية المرتبطة بالمحققين (الفرع الأول)، ومن جهة أخرى إلى التحديات التقنية والقصور المؤسساتي (الفرع الثاني).

الفرع الأول: العوائق الذاتية المرتبطة بالمحققين.

رغم أن الجهات المختصة بالتحقيق، من رجال الضبطية القضائية والقضاة، تضطلع بدور محوري في عمليات البحث والكشف عن مرتكبي الجرائم التقليدية، إلا أن مساهمتها في ميدان مكافحة الجرائم الإلكترونية لا تزال محدودة ولا ترقى إلى المستوى المطلوب، ويعود هذا

القصور إلى جملة من العوامل، منها ما يرتبط بالشخصية المهنية للمحقق ذاته، مثل التردد أو التخوف من التعامل مع تقنيات الإعلام والاتصال الحديثة، بما في ذلك شبكة الإنترنت، فضلاً عن ضعف الاهتمام بمواكبة التطورات المتسارعة في أنماط الإجرام الإلكتروني وأساليبه المستحدثة.[1]

كما أن هناك أسبابًا أخرى تتصل بنقص الكفاءة الفنية لدى المحققين في التعامل مع التقنيات الإلكترونية الحديثة، وافتقارهم للخبرة العملية في أساليب البحث والتحري المتعلقة بالجرائم المرتبطة بهذه الوسائل، ويعود ذلك في الغالب إلى عدم إحاطتهم بطرق ارتكاب الجرائم الإلكترونية، وعدم إلمامهم بـ"اللغة العلمية الرقمية" التي يتداولها المتخصصون في مجال الإعلام الآلي.[2]

إذ تتميز هذه الفئة باستخدام مصطلحات علمية خاصة أصبحت السمة المميزة لتواصلهم المهني، بل إنهم لجأوا إلى اختصار هذه المصطلحات باستخدام الحروف اللاتينية الأولى، مكونين بذلك ما يُعرف بـ"لغة المختصرات" التي تبقى غامضة وغير مفهومة إلا للمنخرطين في هذا المجال أو المتخصصين فيه.[3]

بالإضافة الى ذالك فإن قصور الخبرة العملية لدى بعض القائمين على التحقيق قد يقود، في كثير من الحالات، إلى إتلاف الأدلة أو فقدانها بشكل نهائي، إذ إن عدم إدراكهم لطرق ارتكاب الجرائم المعلوماتية وأساليبها التقنية يجعلهم عرضة لارتكاب أخطاء تؤثر مباشرة في سلامة الدليل الرقمي، فقد ينجم عن هذه الأخطاء، على سبيل المثال، إفساد محتوى الحاسوب والقرص المرن والممغنط، مما يؤدي إلى محو أو تدمير المعلومات التي تمثل ركيزة أساسية في إثبات الجريمة.[4]

وفي أحيان أخرى، قد تُرتكب الجريمة الإلكترونية أمام أعين سلطات الضبط دون أن يتم التعامل معها بما يقتضيه الموقف، بل قد يصل الأمر إلى أن يقدم بعضهم المساعدة للجناة عن غير قصد، ودون وعي بحقيقة ما يقومون به، ومن هذا المنطلق يؤكد الخبراء المتخصصون في مكافحة هذا النمط من الإجرام أن الأنظمة المعلوماتية وما تتعرض له من اعتداءات تمثل تحديًا جوهريًا للعدالة الجنائية، إذ إن رجل الأمن الذي لم يتلق تدريبًا متخصصًا، واقتصرت خبراته على الجرائم التقليدية كالقتل أو الاعتداء أو السرقة، لن يكون

مهيأً للتعامل مع الجريمة الإلكترونية المعاصرة التي تُرتكب باستخدام تقنيات متقدمة ومعقدة.[5]

الفرع الثاني: التحديات التقنية والقصور المؤسساتي.

إن الطبيعة الفريدة للبيئة الإلكترونية، وما يميز الدليل الإلكتروني الرقمي من طابع غير مادي، يشكلان تحديًا جوهريًا أمام الأجهزة الموكلة بمهام البحث والتحري، إذ يتطلب إثبات الجرائم الإلكترونية الاعتماد على أدلة ذات خصوصية تقنية عالية، الأمر الذي يستدعي أن يمتلك القائمون على التحقيق قدرات خاصة ومهارات متقدمة، تمكّنهم من مجابهة الأساليب التقنية المعقدة والتعامل بكفاءة مع التطور المستمر في ميدان تكنولوجيا المعلومات.[6]

إن حالة القصور والضعف التي اعترت أجهزة إنفاذ القانون في مواجهة التحديات المستجدة التي يفرضها الإجرام الإلكتروني، قد دفعت بعدد من الدول إلى انتهاج سياسات جديدة قائمة على الاستعانة بخبراء ومتخصصين ذوي تأهيل عالٍ في ميدان تكنولوجيا الإعلام والاتصال، وضمهم إلى صفوف الأجهزة الأمنية والهيئات القضائية، كما عملت هذه الدول على إعداد وتنظيم برامج تدريبية متخصصة وورش عمل وندوات تهدف إلى تبادل المعارف والخبرات بين العاملين في هذا المجال، بغية الارتقاء بقدرات هذه المؤسسات وتعزيز جاهزيتها لمكافحة الجرائم الإلكترونية بكفاءة وفعالية أكبر.[7]

وفي الجزائر تم استحداث تخصص حقوق واعلام آلي، ففي هذا الاطار شهدت جامعة المسيلة خطوة رائدة في مجال التكوين الأكاديمي من خلال فتح تخصص يجمع بين الحقوق والإعلام الآلي، وهو تخصص يستجيب لمتطلبات العصر الرقمي وما يفرضه من تحديات متسارعة، فالتطور التكنولوجي والتحول الرقمي العالمي أوجبا ضرورة إعداد كفاءات قانونية ملمة بالمعارف التقنية، مما يسمح بتكوين طلبة القانون تكويناً مزدوجاً يجمع بين دراسة القواعد القانونية، خاصة تلك المتعلقة بالقضايا الرقمية، واكتساب مهارات في الإعلام الآلي تؤهلهم للتعامل بكفاءة مع المستجدات التكنولوجية. وتكمن أهمية هذا التخصص في تمكين الخريجين من مواكبة التغيرات التي تعرفها مجالات القانون الخاص والعام على السواء، وتعزيز قدرات القضاء والضبطية القضائية في التصدي للجرائم الإلكترونية والإشكالات القانونية المرتبطة بها.

أما بالنسبة لشروط الالتحاق بهذا التخصص في جامعة مسيلة والمواد المدرسة فيه كما يلي:[8]

ان للتسجيل في هذا التخصص يتم حسب الترتيب على أساس المعدل الموزون المحسوب أو المعدل العام المحصل عليه في امتحان البكالوريا اللذان ينبغي أن يساويان أو يفوقان 13/20، معدلات القبول للسنوات الماضية:

الأولوية1: 14.96 (2024)

الأولوية2: 13.06 (2024)

أما أهم المواد المدرسة في هذا التخصص فهي:

-رياضيات (تحليل وجبر، إحصاء واحتمالات)

-الخوارزميات وبنية المعطيات - مدخل للعلوم القانونية قانون إداري - قانون دستوري - فلسفة القانون - تاريخ النظم - قانون دولي عام -قانون الأسرة - قانون جنائي -قانون تجاري - قانون مدني مصطلحات قانونية تكنولوجيا المعلومات والاتصال -أدوات البرمجة للرياضيات - اقتصاد سياسي – مدخل إلى الشريعة الإسلامية بنية الحاسوب - أنظمة التشغيل - قواعد المعطيات شبكات - نظرية البيانات برمجة تطبيقات الويب - نظم المعلومات - هندسة البرامج - البحث عن المعلومات أمن المعلومات - منطق رياضي - نظرية اللغات- حقوق الإنسان - قانون العمل - الإجراءات الجزائية

-قانون الإجراءات المدنية والإدارية - منهجية البحث العلمي - لغة أجنبية - ذكاء اصطناعي.

المطلب الثاني: المهارات الواجب اكتسابها لرفع كفاءة المحققين.

إن مباشرة التحقيق في الجرائم الإلكترونية تفرض على المحقق امتلاك مؤهلات تقنية ذات طابع خاص، تختلف جوهرياً عن المهارات التقليدية التي تقتضيها الجريمة العادية، ففي هذا النوع من القضايا لا يقف دور المحقق عند حدود إجراءات جمع الأدلة في مسرح الجريمة أو استجواب الشهود فحسب، بل يتعدى ذلك إلى توظيف أدوات رقمية وتقنيات متطورة ترتبط ارتباطاً وثيقاً بعالم تكنولوجيا المعلومات، ومن ثم فإن نجاح التحقيق يظل رهيناً بمدى إلمام المحقق بالتطورات الحديثة في المجال التقني، وبقدرته على استغلال البرمجيات

والوسائل الإلكترونية المتخصصة لاستخراج الأدلة الرقمية وتحليلها بدقة، وفي هذا السياق وجب معرفة حالات استعمال المحقق لمهاراته الالكترونية (الفرع الأول)، ثم معرفة أنواع المهارات الالكترونية الخاصة بالمحقق الالكتروني (الفرع الثاني).

الفرع الأول: حالات استعمال المحقق لمهارته الالكترونية.

تتمثل الحالات التي يجب أن يستعمل المحقق مهاراته الإلكترونية في عدة نقاط أساسية وهي:[9]

أولا: عند تلقي بلاغ حول جريمة إلكترونية.

يتعين على المحقق، عند استلامه بلاغًا يتصل بجريمة إلكترونية، أن يولي اهتمامًا دقيقًا للجوانب التقنية التي قد يتضمنها البلاغ، وأن يبادر إلى طرح الأسئلة اللازمة حول التفاصيل الفنية المتعلقة بالواقعة، خاصة تلك التي قد يغفل المبلّغ عن ذكرها أو يجهل أهميتها بالنسبة لسير التحقيق.

ثانيا: العمل على إدارة عمليات التفتيش على مسرح الجريمة.

يجب على المحقق أن يشرف إشرافًا مباشرًا على عملية التفتيش الميداني، من خلال توجيه الفريق القائم بالعمل وتوزيع المهام عليهم بما يحقق الانسجام والكفاءة، مع ضمان الالتزام التام بالضوابط القانونية والإجرائية، حتى تتسم عملية التحقيق بالسلامة من أي بطلان.

ثالثا: معرفة أسلوب ارتكاب الجريمة والأدوات المستخدمة فيها.

على المحقق أن يقوم بمقابلة الشهود واستجواب المتهمين، مع ضرورة امتلاكه خلفية تقنية تمكّنه من فهم المصطلحات الفنية المرتبطة بأجهزة الحاسوب والشبكات الإلكترونية، وهو ما يضمن قدرته على استيعاب آلية ارتكاب الجريمة والأدوات المستعملة فيها.

رابعا: التحاور مع الخبراء التقنيين في الفريق.

خلال سير التحقيق، يتعين على المحقق أن يتبادل المعلومات مع الخبراء الفنيين باستمرار، وأن يطّلع على التقارير الصادرة عن المختبرات الجنائية الرقمية التي تناولت فحص الأدلة، وذلك لتعزيز رؤيته الفنية والقانونية للقضية.

خامسا: في حالة استدعاء المحقق للمحكمة.

قد تستلزم ظروف المحاكمة استدعاء المحقق للإدلاء بشهادته أمام المحكمة في إطار الدعوى، وفي هذه الحالة يجب أن يكون مستعدًا لعرض المسائل الفنية المتعلقة بالجريمة الإلكترونية بأسلوب قانوني واضح ودقيق، يتيح لهيئة المحكمة فهم الوقائع وتقدير قيمة الدليل الرقمي.[10]

الفرع الثاني: أنواع المهارات الالكترونية الخاصة بالمحقق الالكتروني.

تتمثل أنواع المهارات التي يجب أن يكتسبها المحقق الإلكتروني في مايلي:

أولا: التعرف على المكونات المادية لأجهزة الإعلام الآلي والهواتف النقالة واللوحات الإلكترونية.

يُعد الإلمام بالمكونات المادية للحاسوب وملحقاته ركيزة أساسية لنجاح أعمال التحقيق في الجرائم المعلوماتية، فالمحقق بحكم مسؤوليته، مطالب بفهم تفصيلي لبنية الأجهزة المادية وما يرتبط بها من معدات مساندة، إلى جانب الإحاطة الكاملة بالأدوات والتقنيات التي يمكن أن يوظفها مرتكبو الجرائم عبر الفضاء الرقمي.[11]

هذا الوعي التقني يمنح المحقق القدرة على التعامل بكفاءة مع الشهود، وصياغة استجوابات دقيقة للمتهمين، وفهم التحاليل الفنية التي يقدمها الخبراء المتخصصون، أما غياب هذه المعرفة، فيمكن أن يؤدي إلى تجاهل أدلة مهمة أو التسبب في تعديل البيانات أو إتلافها عن غير قصد، مما يُفضي إلى الإضرار بسير التحقيق ويؤثر على سلامة ومصداقية نتائجه.[12]

ثانيا: معرفة أساسيات عمل شبكات الإنترنت وأهم مصطلحاتها.

إن الإحاطة بمبادئ تشغيل شبكات الإنترنت والمصطلحات الفنية المرتبطة بها تُعد مطلبًا جوهريًا للمحقق عند مباشرة التحقيقات في الجرائم الإلكترونية، فالمعرفة بآلية عمل هذه الشبكات، وطرق اختراقها، وسبل اعتراض حزم البيانات، وكذلك تقنيات تتبع مصدر الهجمات، تمكّن المحقق من تحليل مسار الجريمة بدقة. كما ينبغي أن يكون على دراية بكيفية انتقال البيانات بين الأجهزة في صورة حزم بيانات، لما لهذه المعلومات من دور محوري

في تفسير الأدلة التقنية وتحديد الكيفية التي تم بها تنفيذ الجريمة، الأمر الذي يعزز من قوة الدليل وفاعلية إجراءات التقصي.[13]

ثالثا: معرفة الجوانب الفنية المتعلقة بالجرائم الإلكترونية.

إن الإلمام بالأبعاد الفنية المرتبطة بالجرائم الإلكترونية يمثل عنصراً محورياً لتمكين المحقق من أداء مهامه بكفاءة عالية، إذ تشتمل هذه المعارف على مجموعة من المفاهيم النظرية المتخصصة التي يمكن تحصيلها من خلال البحث والدراسة المستمرة، والاطلاع على مصادر متنوعة، سواء كانت مطبوعات متخصصة أو مواقع إلكترونية موثوقة.[14]

وتتفرع هذه الجوانب الفنية إلى محاور أساسية يتعين على المحقق استيعابها وإتقانها على النحو الآتي:[15]

- ضرورة إحاطة المحقق بالمنظومات التشريعية الجنائية المطبقة في أكثر من دولة، مع فهم دقيق لآليات إنفاذها عند التصدي للجرائم المرتكبة عبر الفضاء الإلكتروني، بما يتيح التعامل الفعال مع القضايا ذات البعد العابر للحدود.

- تمثل دراسة السوابق القضائية البارزة في ميدان الجرائم الإلكترونية وسيلة عملية لتعزيز خبرة المحقق، إذ تُمكّنه من استخلاص الدروس المستفادة من تجارب أجهزة العدالة في مواجهة هذا النمط من الإجرام.

-الإلمام بالطابع الدولي لهذه الجرائم وفهم آثارها على علاقات التعاون القضائي والأمني بين الدول، يعد من المعارف الجوهرية التي تسهّل على المحقق المشاركة في جهود التنسيق الدولي ومتابعة القضايا العابرة للأقاليم.

- الانتظام في متابعة ما يصدر عن المصادر الموثوقة على شبكة الإنترنت، مثل الدوريات العلمية والنشرات المتخصصة، يسهم في إبقاء المحقق على اطلاع دائم بالمستجدات التقنية والقانونية في هذا المجال سريع التطور.

- امتلاك القدرة على تحديد السمات الجوهرية للفئات الإجرامية التي تمارس هذا النوع من الجرائم، وفهم أنماط سلوكها المميزة، يُعد أداة مهمة تساعد المحقق على التنبؤ بتحركات الجناة وبناء استراتيجيات فعالة لمواجهتهم.

رابعا: معرفة الأشكال المختلفة للملفات والتطبيقات الإلكتونية.

إن الإلمام بالأنماط المتعددة للملفات الإلكترونية والتطبيقات الأساسية للحواسيب والهواتف النقالة، يُعد من المقومات الجوهرية التي يجب أن يتحلى بها المحقق عند مباشرة التحقيقات في الجرائم المعلوماتية، فالملفات التي تتضمن أدلة رقمية غالبًا ما تشكل الدعامة الرئيسية التي يستند إليها العمل التحقيقي في الحاسوب.[16]

مما يفرض على المحقق امتلاك القدرة على التعامل مع كميات ضخمة من هذه الملفات، والتي قد تبلغ آلافًا أو حتى ملايين العناصر، ويتطلب ذلك مهارة في تحديد الملفات ذات الصلة بالقضية دون غيرها، وهو ما يمثل تحديًا بالغ التعقيد في هذا المجال. كما أن فحص هذه البيانات يجب أن يتم في إطار احترام "الحق في الخصوصية المعلوماتية" للأفراد، بحيث تتوازن متطلبات التحقيق مع الضمانات المقررة لحماية الحياة الخاصة.[17]

خامسا: معرفة الجرائم الإلكترونية والخصائص التي تتميز بها.

تعد أنواع الجرائم الإلكترونية وخصائصها المميزة قاعدة أساسية لنجاح أي تحقيق في هذا الميدان، إذ أن مواجهة جريمة يجهل المحقق طبيعتها أو طرق ارتكابها يجعل الوسائل الأخرى عديمة الجدوى، ومن ثم فإن المعرفة التفصيلية بالأساليب المستخدمة في ارتكاب هذه الجرائم، وأنماطها، وآثارها، تعد بمثابة حجر الزاوية لتحقيق العدالة في البيئة الرقمية، فإن هذه الدراية تمنح المحقق القدرة على اختيار الأساليب التحقيقية الأكثر ملاءمة، وتساعده في تتبع الجناة وفهم البنية الإجرامية التي يعملون من خلالها، وهو ما يضمن فاعلية الإجراءات المتخذة في كشف الحقيقة.[18]

سادسا: معرفة الإلمام الفني والمعرفي للتعامل مع الجرائم الإلكترونية.

تُعد قلة الإلمام الفني والمعرفي بآليات التعامل مع الجرائم الإلكترونية من أبرز العقبات التي تعترض المحققين في هذا النوع من القضايا، فكثير من العاملين في هذا المجال يفتقرون إلى التدريب المتخصص الذي يمكّنهم من استيعاب طبيعة هذه الجرائم ودوافع مرتكبيها، أو إتقان أساليب جمع الأدلة الرقمية وتحليلها.[19]

وفي حالات عديدة، قد يتصور المحقق أن البيانات الرقمية المضبوطة تمثل دليلًا قاطعًا على الجريمة، إلا أنها قد تكون مستمدة بطرق غير مشروعة أو تفتقر إلى شروط

القبول القانوني، ولهذا فإن تزويد المحقق بالمعرفة التقنية الحديثة، وربطها بالمهارات التحقيقية التقليدية، يشكل ضرورة ملحة، ويتطلب برامج تدريبية متقدمة تدمج بين فهم الحوسبة وتقنيات التحقيق الكلاسيكية، لضمان سلامة الإجراءات وصحة الأدلة.[20]

سابعا: ضرورة إلمام المحقق بالموضع المحتمل للأدلة.

يجب على المحقق أن يمتلك معرفة دقيقة بكيفية تحديد مواقع الأدلة الإلكترونية المحتملة،[21] وأن يفهم طبيعة الشكل الذي قد تتخذه هذه الأدلة سواء أكانت في صورة رقمية أو مادية، ويكتسب تحويل الأدلة الرقمية إلى أشكال مادية، مثل الوثائق الورقية، أهمية كبرى، إذ يتيح ذلك للقاضي الاطلاع عليها بسهولة واستيعاب تفاصيلها بشكل كامل، ويشترط في هذه العملية أن تكون البيانات المنقولة إلى الورق مماثلة تمامًا لما هو موجود على الوسائط الإلكترونية، بما يضمن سلامة الأدلة وموثوقيتها القانونية، ويتعين على المحقق أن يضمن أن كل الأدلة المجمعة تعكس الحقيقة دون أي تحريف، وأن تكون مؤهلة لتقديمها أمام المحكمة كأدلة موثوقة وراسخة.[22]

فينبغي للمحقق أن يبدأ بتحديد جميع الاحتمالات التي يمكن أن تكون مرتبطة بالجريمة، اعتمادًا على الأدلة التي تم استخلاصها والحقائق المستخلصة منها، ويتطلب هذا نهجًا دقيقًا في فحص الأدلة المتاحة، مع إعداد تحليل أولي للمسارات المحتملة التي قد تؤدي إلى تحديد مرتكبي الجريمة وكشف ملابساتها، ومن الضروري أن يستند المحقق إلى القواعد الفنية والمنهجية العلمية في وضع خطة عمل مدروسة، تبدأ من أقوى الاحتمالات وتراعي جميع السيناريوهات الممكنة. ويجب أن يتجنب المحقق التركيز على احتمال واحد فقط دون دراسة البدائل الأخرى، مع الحرص على عدم التسرع في استخلاص استنتاجات مسبقة، بل معالجة كل احتمال بعناية لضمان تغطية شاملة لجميع جوانب القضية.

المبحث الثاني: تطوير المهارات الرقمية للمحققين والتحديات المعيقة لذلك.

يمثل تطوير مهارات المحققين في مجال الجرائم الخاصة ضرورة مستمرة تفرضها التطورات المتسارعة في أساليب ارتكاب هذه الجرائم والوسائل التقنية المستخدمة فيها، ولتحقيق ذلك تتعدد السبل التي يمكن من خلالها صقل مهارات المحققين وتعزيز قدراتهم على مواجهة التحديات العملية، سواء عبر التدريب المتخصص أو الاستفادة من الخبرات الميدانية والتقنية، غير أنّ عملية التطوير تصطدم في كثير من الأحيان بجملة من المعوقات

التي تحدّ من فعاليتها، مثل القيود التنظيمية أو ضعف الإمكانيات المتاحة أو غياب التنسيق بين الجهات المختصة، مما يستوجب تحليلًا متعمقًا لهذه السبل والمعوقات على حد سواء للوصول إلى حلول واقعية قابلة للتطبيق، من خلال هذا المبحث نتناول كل من تطوير المهارات الرقمية المحققين للبحث والتحري عن الجرائم الخاصة (المطلب الأول)، معيقات تطوير المهارات الرقمية للمحققين للبحث والتحري عن الجرائم الخاصة (المطلب الثاني).

المطلب الأول: تطوير المهارات الرقمية للمحققين للبحث والتحري عن الجرائم الخاصة.

يخضع المحققون في المجال الرقمي لسلسلة من البرامج التدريبية المتخصصة، والتي تهدف إلى تزويدهم بالمهارات الإلكترونية المتقدمة لمواجهة مختلف أشكال الجرائم المعلوماتية، ولا سيما تلك المتعلقة بالشرف والأخلاق في الفضاء الرقمي. ولمعرفة طبيعة هذا التدريب وخصائصه، للإحاطة والتعرف على نوع هذه التدريبات وخصائصها نتطرق الى تعريف التدريب الخاص بالمحققين الإلكترونيين (الفرع الأول)، مجالات تدريب المحققين الالكترونيين (الفرع الثاني)، ثم الى تحديد خطوات التفتيش الالكتروني (الفرع الثالث)، والى الفرق المسؤولة عن التحقيق في الجرائم الإلكترونية (الفرع الرابع)، وأخيرا الى تحديد إجراءات التحقيق الالكتروني(الفرع الخامس).

الفرع الأول: تعريف التدريب الخاص بالمحققين الإلكترونيين.

يشير مفهوم تدريب رجال العدالة إلى العملية المنهجية المنظمة التي يتم فيها وضع برامج تدريبية متكاملة، مدعومة بالموارد المالية والبشرية، بهدف تعزيز كفاءة العاملين في الأجهزة القضائية، ويشمل هذا التدريب القضاة، المحققين في النيابة العامة، رجال الضبط القضائي، بالإضافة إلى الموظفين المساعدين مثل الخبراء والمتعاونين في هذا المجال، ويكمن الهدف الأساسي من هذه البرامج في صقل مهاراتهم العملية ورفع مستوى أدائهم المهني، بما يضمن تحقيق العدالة بفعالية وكفاءة أكبر، كما يسهم في تعزيز ثقة المجتمع في النظام القضائي وضمان التوازن بين حماية حقوق الأفراد وتحقيق المصلحة العامة.[23]

يُعَدّ التعامل مع الجرائم الإلكترونية مهمة تتطلب من المحقق امتلاك رصيد معرفي ومهاري متخصص لا يمكن اكتسابه إلا عبر برامج تدريبية موجهة ومستمرة، ويُنظر إلى التدريب هنا باعتباره عملية منهجية متطورة تهدف إلى تضييق الفجوة بين الأداء الفعلي

للمحققين والمتطلبات العملية للوظيفة، من خلال هذه البرامج التدريبية يتم تحديد واكتساب المهارات الأساسية لكل فرد، الأمر الذي يساهم بشكل مباشر في تعزيز كفاءتهم، وتمكينهم من أداء مهامهم بكفاءة وفعالية أكبر في مواجهة التحديات الرقمية المعقدة.[24]

ولا يقتصر هذا التدريب على الأساليب التقليدية، بل يتجاوزها ليشمل تطوير مهارات فنية دقيقة مرتبطة بالجرائم الإلكترونية، بما يمكن المحقق من التعامل مع المستجدات التقنية واستخدام الأدوات والأساليب المتقدمة في التحقيقات الجنائية، ومن خلال هذا التدريب المتخصص، يصبح المحقق أكثر استعدادًا لمواجهة التعقيدات المرتبطة بالتحقيقات الرقمية، حيث يتحول إلى عنصر محوري في سعي العدالة لتحقيق نتائج دقيقة وموثوقة في بيئة إلكترونية تتسم بالتطور السريع والمتلاحق.[25]

الفرع الثاني: مجالات تدريب المحققين الإلكترونيين.

تعد من الركائز الأساسية في إعداد المحققين في الجرائم الإلكترونية ضمان شمولية التدريب لمجالات متعددة متعلقة بالتقنيات الرقمية الحديثة، ويتضمن ذلك تقديم محاضرات متخصصة ودراسات حالة عملية تغطي مجالات الحوسبة والشبكات المعلوماتية، إلى جانب تحليل الموضوعات المدرجة ضمن منهج الدورات التدريبية، ومن بين القضايا المركزية التي يستوجب التركيز عليها ما يلي:

أولا: أنواع المخاطروالتهديدات.

تمثل هذه الفئة كافة المخاطر المحتملة التي قد تهدد نظم الكمبيوتر والبنى التحتية للشبكات المعلوماتية وأجهزة الهاتف واللوحات الإلكترونية، ومن هذا المنطلق من الضروري أن يمتلك المحقق فهمًا شاملاً لكل الاحتمالات والتهديدات المحتملة التي قد تواجهه أثناء إجراء التحقيقات في الجرائم الإلكترونية، بما يمكنه من اتخاذ التدابير الوقائية المناسبة والتخطيط الاستراتيجي.[26]

ثانيا: التعامل مع الأدلة المستحدثة في مجال الإثبات الجنائي.

تشمل هذه الفئة الأدلة الرقمية التي قد تبرز أثناء التحقيق في الجرائم المعلوماتية، ويتطلب ذلك من المحققين التسلح بمعرفة دقيقة حول الأدوات والتقنيات المثلى لجمع هذه

الأدلة وتحليلها، بما يضمن سلامة البيانات ودقتها القانونية، ويكفل قبولها في سياق الإجراءات القضائية، مع مراعاة المعايير المهنية المعتمدة.[27]

ثالثا: أنواع الجرائم الرقمية المترتبة عن استخدام الكمبيوتروشبكات الإنترنت.

يشمل هذا الجانب دراسة الجرائم الناتجة عن استغلال التقنيات الرقمية، والتي قد تتراوح بين الاحتيال الإلكتروني، والاختراقات غير القانونية، والتشهير عبر الشبكات، وغيرها من أشكال الجرائم التي تتسم بطابعها المعلوماتي، مما يستدعي من المحقق الإلمام بكافة الأشكال الممكنة لهذه الجرائم وطرق مواجهتها.[28]

رابعا: المنهج التحقيقي في الجرائم الإلكترونية.

يمثل هذا المنهج نهجًا متمايزًا عن الطرق التقليدية المعتمدة في التحقيق الجنائي، حيث يبدأ المحقق بتجميع الاستدلالات المتعلقة بالجريمة الرقمية وفق خطة عمل دقيقة مبنية على المعلومات المتاحة، وتشكل هذه الخطة الإطار الأساسي لتحديد المراحل التالية للتحقيق، بما يشمل اختيار فريق العمل الفني المناسب الذي سيعمل بالتنسيق مع المحققين لجمع وتحليل الأدلة الرقمية بطريقة منهجية ومنظمة، مما يضمن فعالية التحقيق وتحقيق النتائج المرجو.[29]

يتضمن هذا المنهج التحقيقي عدة مراحل من أهمها:[30]

1:التخطيط للتحقيق.

تبدأ المرحلة الأولى بوضع خطة عمل منظمة ودقيقة، تعتمد على نتائج المعاينة المبدئية لمسرح الجريمة، وتشمل هذه المرحلة فحص أنظمة الحماية الرقمية، وتحديد مصادر الخطر المحتملة، ثم صياغة تصور شامل يضمن مواجهة الجريمة الإلكترونية بفعالية وكفاءة، مع الأخذ بعين الاعتبار جميع الاحتمالات التقنية والقانونية.

2: إجراءات التحقيق.

تشمل هذه الإجراءات تحديد المسار العملي لجمع الأدلة الرقمية، ويشتمل ذلك على عمليات التفتيش الممنهجة، والمراقبة المستمرة، واستخدام أحدث التقنيات الرقمية. ويهدف هذا الترتيب المنهجي إلى ضمان جمع الأدلة بطريقة قانونية سليمة تحافظ على سلامتها وقيمتها الإثباتية أمام القضاء.

3: أساليب التحقيق الخاصة بالجرائم الإلكترونية.

تتمثل في توظيف تقنيات الاستجواب والمواجهة بطريقة منهجية ومدروسة، حيث يتم عرض كل حالة على حدة وتحليلها بدقة متناهية، ويسهم هذا النهج في استنباط المعلومات الدقيقة، وفهم أبعاد الجريمة الرقمية، مع مراعاة الالتزام بالمعايير القانونية وأصول التحقيق الجنائي.

4: عملية جمع المعلومات.

تشكل هذه العملية حجر الزاوية في التحقيق، إذ يتم تجميع البيانات من مصادر متنوعة، سواء كانت رقمية أو مادية، ثم تحليلها بعمق لاستخلاص الأدلة الموثوقة. ويضمن هذا التحليل الدقيق تكامل الأدلة وموثوقيتها القانونية، بما يسهم في تحقيق نتائج التحقيق بكفاءة وفعالية.

5: الاستعانة بالذكاء الاصطناعي.

لقد أضحى الاعتماد على تقنيات الحاسوب والذكاء الاصطناعي ركيزة أساسية في مجال التحقيقات الجنائية الرقمية، إذ أثبتت هذه الوسائل فعاليتها في عمليات جمع الأدلة وتحليلها بدقة، وصولاً إلى استخلاص الحقائق ذات الصلة بالقضية محل البحث. كما يتيح الذكاء الاصطناعي إمكانية حصر الوقائع وتحديد الفرضيات والأسباب المحتملة، إلى جانب تقديم مختلف الاحتمالات الممكنة، ليُصار بعد ذلك إلى استنتاج النتائج استناداً إلى معادلات حسابية تتم معالجتها عبر الحاسوب، وذلك من خلال برامج متخصصة وُضعت لهذا الغرض على نحو دقيق ومنهجي.[31]

الفرع الثالث: تحديد خطوات التفتيش الالكتروني.

يستلزم التحقيق في الجرائم الإلكترونية اهتمامًا دقيقًا بمجموعة من العناصر الجوهرية، ومن أبرزها عمليات التفتيش والضبط داخل فضاء الإنترنت، وفي هذا الإطار يجب تكوين فريق مختص بإجراءات التحقيق، يضم إلى جانب فرق التفتيش التقليدية رجال الأمن والحراسات، قوات الحماية، إضافة إلى خبير مختص في تكنولوجيا المعلومات، ويُعد هذا التشكيل متعدد التخصصات ضروريًا لضمان تنفيذ عمليات التفتيش على الأنظمة المعلوماتية بدقة وفعالية، وفق إجراءات قانونية محكمة، وتشمل هذه العمليات ما يلي:[32]

أولا: البحث والتدقيق في مسرح الجريمة.

يتم تنفيذ هذه المرحلة وفق الإجراءات المعتمدة لتفتيش الأماكن التقليدية، مع مراعاة الخصوصية الرقمية والالتزام بالقواعد القانونية التي تضمن سلامة الأدلة الرقمية وقيمتها الإثباتية.

ثانيا: التأكد من نسخ البيانات المخزنة بدقة.

يشتمل ذلك على نسخ كافة البيانات الموجودة على الأجهزة المستهدفة، قبل البدء باستخدامها في التحليل والتحقيق، لضمان عدم فقدان أي معلومة أو تلوثها.

ثالثا: التحقق من خلو الجهاز المستهدف من أقراص إضافية.

يعد هذا الإجراء ضروريًا للتأكد من عدم وجود وسائط خارجية تحتوي على معلومات هامة قد تؤثر على سير التحقيق، مع فحص كل الملحقات الرقمية المصاحبة للجهاز بعناية متناهية.

رابعا: نسخ وتحليل المحتويات المخزن.

تشمل هذه المرحلة استرجاع الملفات المحذوفة من سلة المهملات أو الملفات المخفية، مع إجراء بحث نصي دقيق باستخدام الكلمات المفتاحية ذات الصلة بالقضية، ويهدف هذا الإجراء إلى استخراج الأدلة الرقمية بطريقة منهجية تضمن تكاملها وموثوقيتها القانونية، بما يعزز قوة التحقيق أمام القضاء.

تلعب المعلومات المتعلقة بالأدوات والبرمجيات المتخصصة في التحقيقات الإلكترونية دورًا محوريًا في إدارة عمليات المراقبة والتحقيق الرقمي، فبينما يتولى فريق الضبط القضائي مهمة ضبط البيانات والمعلومات المخزنة على أجهزة الكمبيوتر، يصبح من الضروري أيضًا تأمين الأدلة الرقمية بدقة متناهية، بما يشمل حفظها في صناديق مخصصة مع تمييزها بعلامات واضحة لضمان سلامتها وسلامة محتواها، ويعد الهدف الأساسي من هذه الإجراءات حماية الأدلة الإلكترونية من أي تلاعب أو فقدان محتمل، الأمر الذي يستلزم اتباع منهجية علمية منظمة لضمان الحفاظ على البيانات والمعلومات بشكل متكامل، أما على صعيد التدريب فإن أسلوب العمل الجماعي "الفريق" يبرز كالأكثر ملاءمة لمواجهة الجرائم الإلكترونية، نظرًا لطبيعتها التي تتطلب تنسيق جهود عدة أفراد لضمان نجاح التحقيقات،

وحتى في الحالات التي تتعلق بجهاز كمبيوتر واحد، يُستحسن أن يقوم الفريق بالعمل الجماعي، مع تجهيز كل عضو بجهاز كمبيوتر محمول مزود ببطاقة شبكة، يمكن من خلاله أخذ نسخة احتياطية من المعلومات المخزنة على الأجهزة الموجودة في مسرح الجريمة، بما يضمن سلامة الأدلة وموثوقيتها القانونية.[33]

الفرع الرابع: الفرق المسؤولة عن التحقيق في الجرائم الاكترونية.

تستند فلسفة العمل في هذا السياق إلى منهجية تعتمد على التنسيق بين مجموعة متنوعة من الخبراء المتخصصين ضمن مهمة مشتركة، وهو الأمر الذي يحاكي أساليب إدارة المشاريع الكبرى. تكمن الفكرة الأساسية في توظيف الموارد البشرية بأقصى كفاءة ممكنة، حيث يشارك كل خبير في مجال محدد، بما يضمن تحقيق هدف موحد يتمثل في ضبط التحقيق في الجرائم الإلكترونية بدقة عالية، مع المحافظة على صحة وسلامة الأدلة الرقمية أثناء جمعها وتحليلها.[34]

يتكون الفريق المسؤول عن التحقيق في الجرائم الإلكترونية من ثلاث مجموعات أساسية، كل منها يتبنى دورًا محددًا يكمّل باقي الأدوار:[35]

أولا: المجموعة الأولى هي المسؤولة عن تنفيذ القانون.

1: قائد الفريق.

يجب أن يمتلك قائد الفريق خبرة واسعة في مجال التحقيقات الجنائية، مع معرفة دقيقة بأنواع الجرائم المرتبطة بالحواسيب والإنترنت، يتولى القائد السيطرة الكاملة على موقع الجريمة، ويقوم بتوزيع المهام على أعضاء الفريق مع متابعة دقيقة لتنفيذها وفق المعايير القانونية المعتمدة.

2: المحقق الجنائي.

يضم الفريق عادة أكثر من محقق جنائي، وذلك حسب طبيعة الجريمة الإلكترونية، يشترط أن يكون المحقق ملمًا بأساليب وطرق التحقيق الجنائي التقليدية، إلى جانب خبرة متخصصة في مجالات الجرائم الإلكترونية، بما يتيح له فهم طبيعة الأدلة الرقمية واستنتاج المعلومات القانونية الدقيقة.

3: خبراء ضبط الأدلة الإلكترونية.

هؤلاء المتخصصون يتحملون مسؤولية جمع الأدلة الرقمية بطريقة ممنهجة وموثقة، مع ضمان سلامتها وعدم المساس بها، لضمان قبولها قانونيًا في الإجراءات القضائية.

4: خبراء التصوير والبصمات والرسم التخطيطي والخوارزميات.

تقع على عاتق هؤلاء توثيق مسرح الجريمة بدقة، عبر استخدام تقنيات التصوير الاحترافية، ورصد البصمات، وإعداد الرسوم التخطيطية للمكان، بما يساهم في تقديم صورة واضحة وموثوقة للأحداث أمام الجهات القضائية.

ثانيا: المجموعة الثانية تضم المتخصصين في التدقيق ومراجعات الحسابية.

تتولى هذه المجموعة تحليل الحسابات والبيانات المالية والإلكترونية المرتبطة بالجريمة، بما يتيح كشف أي تلاعب أو عمليات احتيالية، ويعزز من مصداقية الأدلة المستخرجة من الأنظمة الرقمية المختلفة.

ثالثا: المجموعة الثالثة تشمل المتخصصين في معالجة البيانات إلكترونيًا.

تتمثل مهمتهم في معالجة وتحليل المعلومات الرقمية والبيانات الإلكترونية باستخدام أدوات وتقنيات متقدمة، لضمان استخراج المعلومات الحيوية التي تدعم التحقيقات القانونية، بما يسهم في تقديم أدلة دقيقة يمكن الاعتماد عليها في الإجراءات القضائية.

الفرع الخامس: تحديد إجراءات التحقيق الالكتروني.

عند الشروع في التحقيق مع الأطراف المتورطة في الجرائم الإلكترونية، يقوم فريق المحققين والخبراء باتباع مجموعة من الإجراءات المنهجية الدقيقة التالية:[36]

أولا: تبادل المعلومات.

يقوم ضباط الشرطة القضائية وخبراء الحاسوب بتبادل المعلومات المتعلقة بالجريمة، حيث يطلع الضباط الخبير على ترتيب المتهمين والشهود، والأسلوب الأمثل لتوجيه الأسئلة لهم، مما يعزز من فعالية جمع المعلومات وموثوقية النتائج.

ثانيا: توثيق مسرح الجريمة.

يتم تسجيل كافة التفاصيل المرتبطة بالحاسوب أو الجهاز الرقمي المضبوط، مثل حالة تشغيله عند الضبط أو وضع الإيقاف، وحالة الاتصال بالإنترنت خلال وقت المعاينة، هذه العملية تعد خطوة أساسية لضمان سلامة الأدلة الرقمية وموثوقيتها أمام الجهات القضائية.

ثالثا: تحديد الأمور الواجب توضيحها.

يقوم الخبير الرقمي ومأمور الضبط القضائي بحصر النقاط الأساسية التي تتطلب توضيحًا، ويتم ترتيب هذه الأمور وفق أولويتها القانونية والتحقيقية، لضمان معالجة كل جانب من جوانب الجريمة بدقة وموضوعية.

رابعا: وضع خطة التحقيق.

استنادًا إلى النتائج الأولية، يقوم فريق التحقيق بإعداد خطة شاملة تتضمن جميع الخطوات اللازمة لجمع وتحليل الأدلة، بما يضمن سير التحقيق وفق منهجية قانونية دقيقة وفعالة.

خامسا: التنسيق بين المحققين والخبراء.

يعد التنسيق الوثيق بين المحققين والخبراء في استخراج البيانات المخزنة أمرًا جوهريًا، إذ يتطلب الأمر تحديد مكان البيانات الرقمية المخزنة على جهاز الكمبيوتر أو ملحقاته، خاصة وأن المجرمين الإلكترونيين غالبًا ما يحفظون معلوماتهم على أجهزة الحاسوب أو وسائط تخزين مثل الأقراص المدمجة والفلاشات، مما يفرض دقة عالية في جمع الأدلة.

سادسا: البحث عن البرامج المناسبة.

يقوم الفريق بالبحث عن البرمجيات المتخصصة في كشف البيانات المخزنة وتحليلها، مع تحديد التدابير الضرورية لضمان حماية الأدلة الرقمية وحفظها من أي تلاعب أو تلف.

سابعا: حفظ الأدلة الرقمية.

يشمل ذلك إجراءات الحفاظ على الأدلة كما تم ضبطها، مع ضمان نقلها وتخزينها في حالة سليمة تحافظ على سلامتها القانونية والتقنية.

ثامنا: الالتزام بالقوانين.

من الضروري التقيد بالتشريعات الخاصة بحماية حقوق الأفراد وسرية المعلومات الشخصية و البريد الإلكتروني، لتجنب أي طعن قانوني في الأدلة المستخلصة أو في الإجراءات التي اتخذها مأمور الضبط القضائي.

المطلب الثاني: معيقات تطوير المهارات الرقمية للمحققين للبحث والتحري عن الجرائم الخاصة.

إنّ نجاح أجهزة العدالة الجنائية في التصدي للجرائم ذات الطبيعة الخاصة، لاسيما تلك المرتبطة بالبيئة الرقمية، يظل رهيناً بمدى كفاءة المحققين الإلكترونيين وقدرتهم على امتلاك مهارات متقدمة تتيح لهم فهم خصوصية هذه الجرائم والتعامل مع أساليب ارتكابها بكفاءة، غير أنّ الواقع العملي يكشف عن وجود جملة من المعوقات التي تحول دون الارتقاء بمستوى هذه المهارات، وتعرقل مساعي تطويرها بما يتناسب مع خطورة الجرائم الإلكترونية وتنوع صورها.

يتم تقسيم هذه المعيقات الى كل من المعيقات التدريبية والتحديات التكنولوجية (الفرعالأول)، والى المعيقات المادية والمالية (الفرع الثاني).

الفرع الأول: المعيقات التدريبة والتحديات التكنولوجية.

تتمثل هذه المعوقات في أبعاد متعددة، بعضها تقني مرتبط بسرعة تطور التكنولوجيا وصعوبة ملاحقتها بالتدريب المستمر، وبعضها مؤسساتي يتعلق بمحدودية الإمكانيات المادية والبشرية المرصودة للتأهيل والتكوين، فضلاً عن عوامل قانونية وتنظيمية تعيق أحياناً مواكبة المستجدات.

فبالرغم من المساعي المكثفة التي بُذلت من أجل تعزيز كفاءة الأجهزة الأمنية والسلطات القضائية في مواجهة الجرائم الإلكترونية، إلا أن هذه الجهود لم تكن كافية لتمكينها من مواكبة التطور المتسارع الذي يشهده هذا النوع من الإجرام، ويُعزى ذلك إلى جملة من العوامل، يأتي في مقدمتها تشعب المهام المنوطة بهذه الأجهزة وتعدد مجالات تدخلها، وهو ما يحول دون تخصيصها وقتاً وإمكانات كاملة للتعامل مع الجرائم الإلكترونية، وفي هذا الإطار ارتفعت الأصوات المطالبة بإنشاء وحدات متخصصة للتحقيق في الجرائم ذات الطبيعة المعلوماتية، تكون مهمتها الأساسية التصدي لهذه الظاهرة دون تشتيت، كما أن الطابع

المستحدث للجرائم الإلكترونية، وما يرافقه من تنوع في أساليب ارتكابها، يشكل عائقاً أمام تكوين خبرة عملية متراكمة لدى المحققين، لاسيما مع التضخم الهائل للمعلومات المتاحة عبر شبكة الإنترنت، والتي تستلزم وقتاً وجهداً بالغين من أجل تحليلها. ويضاف إلى ذلك التباين المستمر في الأجهزة والبرامج والتطبيقات التكنولوجية، الأمر الذي يزيد من صعوبة إعداد برامج تدريبية قادرة على تمكين المحققين من تتبع أنماط هذه الجرائم بفعالية.

الفرع الثاني: المعيقات المادية والمالية.

وإلى جانب ما تقدم، تتجلى عقبة أخرى لا تقل خطورة، تتمثل في محدودية الاعتمادات المالية المرصودة لتأهيل رجال الضبطية القضائية في مجال مكافحة الجرائم الإلكترونية، فغالباً ما تكون هذه الموارد غير كافية لتوفير برامج تدريب متخصصة على مستوى عالٍ، أو لاستقطاب خبراء ذوي كفاءة في ميدان تكنولوجيا المعلومات إلى صفوف الأجهزة الرسمية، وتتضاعف حدة هذا التحدي في ظل المنافسة القوية التي تفرضها المؤسسات الخاصة، حيث تلجأ هذه الأخيرة إلى استقطاب الكفاءات المتميزة من خلال عروض وظيفية ومزايا مالية يصعب على القطاع الحكومي مجاراتها، وهو ما يؤدي في نهاية المطاف إلى نزيف في القدرات البشرية المؤهلة التي تحتاجها الدولة لتعزيز أجهزتها الأمنية والقضائية في هذا الميدان الحساس.[37]

الخاتمة:

من خلال ما تم عرضه يتضح أن واقع البحث والتحري عن الجرائم الخاصة، ولا سيما تلك ذات الطابع الحساس، يعاني من جملة من الإشكاليات التي تؤثر سلبًا على فعالية التحقيقات ودقة النتائج المتوصل إليها، ويمكن تلخيص أهم النتائج السلبية فيما يلي:

أولا: النتائج :

-تثمين فتح تخصص حقوق واعلام آالي في جامعة مسيلة، لما له من أثر في دعم تكوين القضاة وأعوان الضبطية القضائية في مجال الجرائم الإلكترونية، وتعزيز قدراتهم في التعامل مع الأدلة الرقمية.

-ضعف الخبرة العملية لدى بعض المحققين في التعامل مع الجرائم الخاصة، مما يؤدي إلى قصور في جمع الأدلة وفهم السياق الجنائي للقضية.

- محدودية المهارات التقنية والرقمية لدى المحققين، خاصة في الجرائم التي تتطلب تعقب آثار إلكترونية أو تحليل بيانات رقمية.

- غياب برامج تدريب متخصصة ومستمرة في مجال البحث والتحري عن الجرائم الخاصة، مما يضعف قدرة المحققين على مواكبة المستجدات.

- الاعتماد المفرط على الطرق التقليدية في البحث والتحري، وعدم استغلال الإمكانيات العلمية والتقنية الحديثة.

- عدم وجود آليات واضحة لتبادل الخبرات والمعلومات بين المحققين وأجهزة إنفاذ القانون، مما يحد من الاستفادة من التجارب الناجحة.

- نقص الموارد المادية والتقنية المخصصة لدعم عمليات البحث والتحري في الجرائم الخاصة.-غياب الإطار القانوني الواضح الذي يحدد ضوابط وإجراءات البحث في بعض الجرائم الحساسة، مما قد يخلق فجوات قانونية أثناء التحقيق.

ثانيا: التوصيات:

تثمين فتح تخصص حقوق واعلام آالي في جامعة المسيلة

- وضع برامج تدريب وتأهيل مستمرة للمحققين، تركز على الجوانب النظرية والعملية، مع تضمين مهارات التعامل مع الجرائم الحساسة سواء للسلك القضائي أو الضبطية القضائية.

- دمج التقنيات الحديثة في عمليات البحث والتحري، مثل أدوات التحليل الرقمي، وأنظمة تتبع الأدلة الإلكترونية.

- إنشاء وحدات أو فرق متخصصة في التحقيق بالجرائم الخاصة، تضم خبراء في الجوانب القانونية، النفسية، والتقنية في الضبطية القضائية.

- تطوير آليات للتنسيق وتبادل المعلومات بين مختلف الأجهزة الأمنية والقضائية، بما يضمن سرعة الوصول إلى الأدلة.

- توفير موارد مادية وتقنية كافية لدعم عمليات البحث والتحري، مع تخصيص ميزانية مستقلة للوحدات المختصة.

- مراجعة وتحديث الأطر القانونية المنظمة للتحقيق في الجرائم الخاصة، بما يتوافق مع التطورات التقنية والمجتمعية.

-تكوين قضاة مختصين في الجرائم الإلكتونية.

- تشجيع المحققين على المشاركة في ورش عمل ومؤتمرات دولية لاكتساب الخبرات والاطلاع على أفضل الممارسات.

الهوامش:

[1] عبد الرحمان محمد بحر، معوقات التحقيق في جرائم الانترنت، مذكرة لنيل شهادة الماجستير في العلوم الشرطية، قسم العلوم الشرطية ومعهد الدراسات العليا بجامعة نايف العربية للعلوم الأمنية بدبي، 1999، ص -ص .95-96.

[2] ENISA, Annual Incident Reports 2011, octobre 2012.p123

[3] خالد ممدوح ابراهيم، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، مصر، 2019، ص 69.

[4] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجية الحديثة، دار النهضة العربية، مصر، 2002، ص 115.

[5] حسين بن سعيد بن سيف الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، دار النهضة العربية، مصر، 2009، ص 410.

[6] محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، الإمارات العربية المتحدة، 3 -5-2004، ص 1070.

[7] محمد الأمين البشري، مرجع سابق، ص 1077.

[8] جامعة محمد بوضياف المسيلة، عرض التكوين في ليسانس مزدوج (إعلام آلي- حقوق)، 2024/2023، أنظر الموقع: https://www.univ-msila.dz/site/offre-droitinf/ .2025-10-2

[9] محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت-دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية-، رسالة مقدمة لنيل شهادة ماجستير في العلوم الشرطية، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية بالسعودية، 2001، ص-ص.93-94.

[10] D. Bigo, « La mondialisation de l'(in)sécurité? Réflexions sur le champ des professionnels de la gestion des inquiétudes et analytique de la transnationalisation des processus d'(in)sécurisation », Cultures & Conflits, nº 58, été 2005, p205.

[11] C. Gilbert, Conférence Mines ParisTech De la gestion des risques à l'organisation de la résilience. Implications d'un changement de perspectives, 7 juin 2011. F. Guarnieri& E. Przyswa, «Cybercriminalité contrefaçon les interactions entre réel et virtuel' », Cahiers de la sécurité n° 15, 2011, p 50

[12] حسين بن سعيد بن سيف الغافري، مرجع سابق، ص 394.

[13] حسيب السيد المحلاوي أنيس، الخبرة القضائية في الجرائم المعلوماتية والرقمية، دار الفكر الجامعي، مصر، 2016، ص 102.

[14] U. Beck, Pouvoir et contre-pouvoir à l'heure de la mondialisation, Flammarion Champs Essais, 2009, p200

[15] عدنان الفيل علي، اجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، مصر، 2012، ص26.

[16] The regional computer forensies.laboratoryTE.USA. cyber criminalite.p234

[17] محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي- دراسة مقارنة-، دار الجامعة الجديدة، مصر، 2018، ص163.

[18] حسين بن سعيد بن سيف الغافري، مرجع سابق، ص 398.

[19] Bace, Rebecca (2000) Interusion Indianapolis, Indiaina Detection, MecmillabTechniccat Publishing.p.116

[20] محمد كمال شاهين، مرجع سابق، ص164.

[21] MarkMonitor, Brandjacking Index, été 2009.p153.

[22] حسيب السيد المحلاوي أنيس، مرجع سابق، ص104.

[23] محمد الكومي ياسر، محمود أبو حطب، الحماية الجنائية والأمنية للتوقيع الاكتروني -دراسة مقارنة-، منشأة المعارف، مصر، 2014، ص 291.

[24] محمد النويجم صلاح، تقويم كفاءة العملية التدريبية في معاهد التدريب الأمنية بمدينة الرياض من وجهة نظر العاملين فيها، رسالة مقدمة لنيل شهادة الماجستير، جامعة نايف العربية للعلوم الأمنية بالسعودية، 2005، ص9.

[25] حامد طنطاوي إبراهيم، التحقيق الجنائي من الناحيتين النظرية والعلمية، ط1، دار النهضة العربية، القاهرة، 2000، ص3.

[26] فريد رستم هشام محمد، الجرائم المعلوماتية -اصول التحقيق الجنائي الفني-، مجلة الأمن والقانون، أكاديمية شرطة دبي، العدد02، 1999، ص130.

[27] جبار الحسناوي علي، جرائم الحاسوب والأنترنت، دار اليازوري للنشر والتوزيع، عمان، 2009، ص124.

[28] المرجع نفسه.

[29] حسين بن سعيد الغافري، مرجع سابق، ص170.

[30] بيومى عبد الفتاح حجازي، المبادئ العامة في جرائم الصحافة والنشر، منشأة المعارف، مصر 2009، ص88.

[31] S. Leman-Langlois, « Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial, Criminologie, vol. XXXIX, n° 1, printemps 2006, p99.

[32] عبد الباقي الصغير جميل، أدلة الاثبات الجنائي والتكنولوجيا الحديثة -أجهزة الرادار، الحاسبات الآلية، البصمة الوراثية (دراسة مقارنة)، دار النهضة العربية، مصر، 2001، ص-ص.121-122.

[33] جبار الحسناوي علي، مرجع سابق، ص 128.

[34] فريد رستم هشام محمد، مرجع سابق، ص 45.

[35] بيومي عبد الفتاح حجازي، مرجع سابق، ص90.

[36] عبد الباقي مصطفى، التحقيق في الجريمة الإلكترونية وأثباتها في فلسطين (دراسة مقارنة)، مجلة علوم الشريعة والقانون، كلية القانون بالجامعة الأردنية، العدد 04، 2018، ص286.

[37] حسين بن سعيد بن سيف الغافري، مرجع سابق، ص 411.