



التحديات الرقمية والتحديات المعاصرة

— من جمع المعلومات إلى الإثبات —



Colonel / Faisal Murjan.

إهداء

إلى الجنود المجهولين في ميادين التحريات الأمنية، الذين يعملون في صمت، ويسهرون حين ينام الناس، ويؤدون واجبتهم بعيداً عن الأضواء، إخلواً لله، وحمايةً للمجتمع، وصوناً للأمن، واستقراراً.
إلى الأتقياء الأتقياء منهم، الذين يجمعون بين يقظة الأمن وأمانة الضمير، ويجعلون الحق والعدل وصون
كرامة الإنسان نجاة لا يجيدون عنه.

إليك أهدى هذا العمل، مستلهماً قول النبي صلى الله عليه وسلم:

«وعين باتت تحرس في سبيل الله».

تقدراً لعظائم الصامت، ووفاء لرسالتكم، واعتزازاً بجهودكم التي قد تخفى عن أعين الناس،
ولا تخفى على رب الناس.
أهدىكم هذا الكتاب

Colonel / Faisal Murjan.



المقدمة:

يشهد العالم المعاصر تحولات متسارعة في طبيعة الجريمة ووسائل ارتكابها، وفي الأدوات التي تعتمد عليها الجهات الأمنية في الكشف عنها وجمع المعلومات المتعلقة بها. فقد أسهم التطور في تقنيات الاتصال والمعلومات، وانتشار الأجهزة الذكية، وتوسع استخدام المنصات الرقمية، في إعادة تشكيل البيئة التي تقع فيها الأنشطة الإجرامية، وأوجد أنماطاً جديدة من البيانات التي قد تحمل دلالات مهمة في الكشف عن الجرائم وإعادة بناء وقائعها.

ولم تعد أعمال التحري الأمني محصورة في الوسائل التقليدية، بل امتدت إلى التعامل مع البيانات الإلكترونية، وتحليل الآثار الرقمية، وفحص الأجهزة والوسائط، والاستفادة من المصادر المفتوحة، وتوظيف تقنيات المراقبة والرصد الحديثة، ومنها الطائرات المسيّرة. وقد أفضى ذلك إلى اتساع نطاق المعلومات، لكنه أوجد تحديات قانونية وفنية تتصل بمشروعية جمعها، وموثوقية مصادرها، وسلامة معالجتها، ومدى صلاحيتها للاستدلال والإثبات.

وفي ظل هذه التحولات، أصبحت التحريات الأمنية الرقمية منظومة متكاملة من الإجراءات القانونية والفنية التي تبدأ بتحديد المعلومات ذات الصلة، وتمتد إلى جمعها وحفظها وفحصها وتحليلها، وتنتهي بتقييم دلالتها. ومن ثم، فإن نجاح التحري الرقمي لا يُقاس بكمية البيانات، ولا بالقدرة التقنية على المراقبة، وإنما بمدى مشروعية الإجراءات، ودقة المعالجة، وإمكان التحقق من النتائج، واحترام الضمانات القانونية.

وتبرز أهمية هذا التمييز عند النظر إلى الطبيعة المركبة للمعلومات الرقمية؛ إذ قد تكون البيانات صحيحة تقنياً، لكنها جُمعت بإجراء غير مشروع، وقد يكون الحصول عليها مشروعاً، بينما يشوبها خلل في الحفظ أو النقل يضعف موثوقيتها. كما قد تكون سليمة المصدر والحفظ، دون أن تكفي وحدها لإثبات الواقعة. ولهذا، يتعين الفصل بين مشروعية الحصول، وسلامة البيانات، وموثوقية المصدر، وقيمتها الاستدلالية.

ولا تنفصل مشروعية التحريات الرقمية عن مبادئ الشرعية، واحترام الحياة الخاصة، وحماية البيانات الشخصية، ومراعاة التناسب، والخضوع للرقابة. فالتطور التقني لا ينشئ بذاته سلطة قانونية، ولا يجيز تجاوز الحدود التي رسمها المشرّع. وتتأكد هذه الضوابط في ظل اتساع إمكانات المراقبة، ولا سيما الطائرات المسيّرة، التي لا تتحدد آثارها القانونية بطبيعة الطائرة وحدها، بل بنطاق التصوير ومدته، ونوعية البيانات، وإمكان تحديد الأشخاص، والغرض من الإجراء [1].

ومن ناحية أخرى، تفرض الطبيعة الرقمية للأدلة ضرورة الاهتمام بالضمانات الفنية التي تكفل الحفاظ على سلامتها وإمكان مراجعتها، من توثيق إجراءات الجمع، والمحافظة على البيانات الأصلية، وضبط سلسلة العهدة، وتحديد الأدوات والأساليب المستخدم. لا تقتصر هذه الإجراءات على حماية الدليل من العبث، بل تعزز الشفافية وإتاحة المراجعة المستقلة.

ويكتسب الموضوع أهمية إضافية مع تنامي استخدام الذكاء الاصطناعي والتحليل الآلي، وما تتيحه من إمكانات لتصنيف المعلومات واكتشاف الأنماط وتحليل الصور. فهذه التقنيات قد تسهم في تسريع الفحص، إلا أن نتائجها تظل مرتبطة بجودة البيانات، وطبيعة النماذج، وحدود دقتها،

وإمكان التحقق من مخرجاتها. ومن ثم، لا يصح التعامل مع النتيجة الآلية بوصفها حقيقة نهائية، بل ينبغي إخضاعها للفحص والتحقق.

وانطلاقاً من ذلك، يتناول هذا الكتاب التحريات الأمنية الرقمية بوصفها موضوعاً تتقاطع فيه القواعد القانونية مع المتطلبات الفنية والاعتبارات الحقوقية. ولا يقتصر على عرض الوسائل المستحدثة، بل يسعى إلى تحليل الإطار الذي يحكم استخدامها، وتحديد شروط مشروعيتها وإجراءاتها، وبيان الضمانات التي تكفل سلامة المعلومات، واستكشاف مدى قدرتها على دعم الاستدلال الجنائي.

ويستهدف الكتاب تأصيل مفهوم التحريات الأمنية الرقمية وتمييزها عن التحقيق وجمع الأدلة، وتحليل الضوابط القانونية التي تحكم جمع المعلومات واستخدامها، وبيان المتطلبات الفنية للتعامل مع الأدلة الرقمية، ودراسة القيمة الاستدلالية للبيانات، وأثر المخالفات القانونية والعيوب الفنية في الاعتماد عليها، فضلاً عن بحث التحديات التي تثيرها وسائل المراقبة الحديثة، ومنها الطائرات المسيّرة والذكاء الاصطناعي.

وتحكم معالجة هذه الموضوعات رؤية منهجية تقوم على التمييز بين ما تستطيع التقنية إنجازه وما يسمح به القانون، وبين ما تكشفه البيانات وما يمكن استخلاصه منها، وبين صحتها الفنية وكفايتها للإثبات. ويقتضي ذلك الجمع بين المنهج التحليلي في دراسة النصوص، والمنهج التحليلي الوصفي في تحديد خصائص الوسائل الرقمية، والمنهج المقارن عند توافر النصوص والتجارب ذات الصلة، مع الاستفادة من المعايير الفنية الدولية في حدود موضوعها، مع التمييز بين النصوص الملزمة والاتفاقيات الدولية بحسب نطاق سريانها والمعايير الإرشادية.

ويولي الكتاب اهتماماً خاصاً بالعلاقة بين أعمال التحري وحماية الحقوق، انطلاقاً من أن فاعلية العمل الأمني لا تتعارض في أصلها مع الضمانات القانونية، بل تتعزز حين تُمارس الصلاحيات ضمن حدود واضحة، وتخضع للمراقبة، وتكون النتائج قابلة للتحقق.

ومن هنا، فإن المسألة المركزية التي يعالجها الكتاب تتمثل في كيفية تحقيق التوازن بين متطلبات الأمن والاستفادة من الإمكانيات الرقمية، من جهة، واحترام الشرعية والحقوق الأساسية وضمان موثوقية الأدلة، من جهة أخرى. ويتفرع عن ذلك تساؤلات حول حدود سلطة الجهات المختصة، والضوابط التي تحكم استخدام وسائل المراقبة، والمعايير اللازمة للتحقق من سلامة البيانات، وأثر العيوب الإجرائية والفنية في قيمتها الاستدلالية، ومدى كفاية الأطر التشريعية القائمة.

ولا يفترض الكتاب أن جميع الأنظمة القانونية تتبنى حلولاً متطابقة، أو أن القواعد المنظمة للتحري الرقمي يمكن استخلاصها بمعزل عن التشريع الوطني. ولذلك، ينبغي فهم التحليل في ضوء النصوص الواجبة التطبيق، مع الاستفادة من المعايير الدولية بوصفها أدوات للمقارنة، لا بدائل عن الأحكام الوطنية. كما أن تناول الوسائل التقنية لا يعني التسليم بموثوقيتها المطلقة، بل يقتضي تحديد حدودها العملية ومصادر الخطأ المحتملة.

ويستهدف هذا الكتاب الباحثين في القانون الجنائي والإجراءات الجزائية، وطلبة الدراسات العليا، والممارسين في أجهزة إنفاذ القانون والنيابة العامة والقضاء. ولا يتناول بالتفصيل الجرائم

الإلكترونية كموضوع مستقل، ولا التحقيق القضائي، ولا الطب الشرعي الرقمي، إلا بالقدر الذي تستدعيه طبيعة التحريات الأمنية الرقمية.

هيكل الكتاب: ينقسم الكتاب إلى أربعة أبواب: الأول يتناول الإطار المفاهيمي والقانوني (المفهوم، الأساس القانوني، الضمانات)، والثاني يعالج وسائل التحري وإجراءات الجمع (المصادر، الرصد الأرضي، الطائرات المسيّرة)، والثالث يدرس سلامة المعلومات وقيمتها القانونية (الأصالة، سلسلة العهدة، القيمة الإثباتية، التحليل، التقييم التطبيقي)، والرابع يبحث التحديات ومقترحات التطوير (القانونية، التقنية، الحوكمة).

ويأمل المؤلف أن يسهم هذا العمل في إثراء البحث القانوني المتعلق بالتحريات الأمنية الرقمية، وفي توفير إطار علمي يساعد الباحثين والممارسين على فهم العلاقة بين الإجراء الأمني والوسيلة التقنية والدليل الناتج عنها، وأن يفتح المجال أمام مزيد من الدراسات المتخصصة.

إن التحريات الأمنية الرقمية ليست مجرد امتداد تقني للتحري التقليدي، بل مجال متجدد تتغير أدواته وتتسع إمكاناته وتتطور مخاطره. ومن ثم، فإن التعامل الرشيد معها يقتضي معرفة قانونية دقيقة، وكفاءة فنية متخصصة، ومنهجاً نقدياً لا يخلط بين القدرة على جمع المعلومات والحق في جمعها، ولا بين سلامة البيانات وصحة الاستنتاج، ولا بين التقدم التقني ومشروعية استخدامه.

الفصل الأول: الإطار المفاهيمي والقانوني للتحريات الأمنية الرقمية

المبحث الأول: ماهية التحريات الأمنية الرقمية وتمييزها عن المفاهيم المجاورة

المطلب الأول: مفهوم التحريات الأمنية الرقمية ومقوماتها

أولاً: التعريف التحليلي

لا يوجد تعريف دولي موحد وملزم للتحريات الأمنية الرقمية، ولا تعريف تشريعي عربي موحد. وعليه، يُعتمد تعريف تحليلي إجرائي لضبط نطاق الدراسة: "مجموعة من الأعمال المشروعة التي تباشرها جهة مختصة لجمع المعلومات والبيانات ذات الصلة بمسألة أمنية أو واقعة محل تحقق، باستخدام المصادر والوسائل الرقمية أو بالاستعانة بها، ثم فحصها وربطها وتقييم موثوقيتها ودلالاتها، بقصد دعم التقدير الأمني أو اتخاذ إجراء يدخل في نطاق الاختصاص القانوني، مع مراعاة الضوابط المنظمة للوصول إلى البيانات ومعالجتها وحفظها واستخدامها". [1]

ويقوم التعريف على أربعة عناصر: الاختصاص، والمشروعية، والغرض المحدد، والطبيعة الأولية للنتائج.

ثانياً: المقومات الأساسية

١. **الاختصاص القانوني**: لا يكفي أن تكون المعلومة ذات أهمية أمنية حتى تصبح كل جهة مخولة بجمعها. فالاختصاص بالموضوع لا يساوي بالضرورة الاختصاص باتخاذ جميع الوسائل. [2]
٢. **مشروعية الغرض**: يجب أن يتصل التحري بغرض مشروع يدخل في نطاق الوظيفة القانونية للجهة.
٣. **الارتباط بالواقعة**: وجود صلة معقولة بين المعلومات المجموعة والمسألة محل التحقق.
٤. **التحقق والتقييم**: تقييم مصدر المعلومات وسياقها واتساقها.
٥. **التوثيق والمساءلة**: توثيق مصدر المعلومات وكيفية الحصول عليها وتاريخ جمعها. [3]

ثالثاً: الطبيعة الأولية للنتائج

نتائج التحريات لا تُعد حكماً نهائياً على صحة واقعة أو مسؤولية شخص، بل تكوين صورة أولية قابلة للمراجعة. ولا يجوز الخلط بين قيمة المعلومات في اتخاذ قرار أمني أولي وقيمتها في الإثبات القضائي. وقد أكد الفقه العربي أن "كفاية التحري" تتحقق إذا تضمنت بيانات أو معلومات تصلح أن تكون "نواة للدليل"، لا دليلاً كاملاً. [4]

رابعاً: الطبيعة المركبة

تجمع التحريات الأمنية الرقمية بين ثلاثة أبعاد: **قانوني** (الاختصاص والسند والقيود)، و**معلوماتي تحليلي** (الجمع والمقارنة والفصل بين المعطى والاستنتاج)، و**فني** (سلامة البيانات

وطرق استخراجها). وسلامة الإجراء القانوني لا تثبت وحدها صحة التحليل الفني، وصحة التحليل لا تصحح إجراءً بلا سند. [5]

المطلب الثاني: خصائص التحريات الأمنية الرقمية

١. تعدد مصادر المعلومات: مع التمييز بين تعدد المصادر الظاهري وتعدد مصادر المعرفة الفعلية؛ فتكرار المعلومة في مواقع متعددة لا يعني وجود تأكيد مستقل. [6]

٢. قابلية النسخ والمعالجة: مع التمييز بين المحافظة على المحتوى الظاهر والمحافظة على الخصائص الفنية والسياق الأصلي. وقد أكد المعهد الوطني الأمريكي للمعايير والتقنية (NIST) أن حفظ الأدلة الرقمية يثير مشكلات تتجاوز حفظ الأدلة التقليدية، لأن المحتوى الرقمي قد يوجد على وسائط مادية أو في السحابة دون وضوح مكان التخزين الفعلي. [7]

٣. إمكان الربط بين البيانات: مع خطر الاستدلال إذا لم تُتحقق هوية الأجهزة أو ضُبطت الفروق الزمنية.

٤. إمكان التغيير أو التلاعب: لا يجوز افتراض التلاعب لمجرد أن البيانات رقمية، ولا افتراض السلامة لمجرد استخراجها من نظام إلكتروني. [8]

٥. حساسية البيانات وتداخلها مع الخصوصية: التمييز بين إمكان الوصول التقني وجواز الجمع قانوناً.

٦. الحاجة إلى التوثيق: حفظ المعلومات دون توثيق طريقة الحصول عليها لا يتيح المراجعة اللاحقة. وقد أكد مجلس أوروبا في معاييرها الدولية لجمع الأدلة الإلكترونية والتعامل معها أهمية الإجراءات المنظمةة لمراحل الجمع والحفظ والفحص والعرض. [9]

٧. تفاوت القيمة الاستدلالية: سجل الدخول لا يثبت وحده هوية المستخدم، والصورة لا تثبت وحدها هوية المصور.

المطلب الثالث: تمييز التحريات الأمنية الرقمية عن المفاهيم المجاورة

أولاً: عن جمع المعلومات الرقمية

جمع المعلومات نشاط واسع قد يُمارس لأغراض علمية أو إدارية أو تجارية. أما التحري الأمني فيتحدد بالغرض الأمني، والسياق القانوني، وطبيعة المعالجة التقييمية، والآثار المحتملة. والعلاقة بينهما علاقة الجزء بالكل في كثير من الحالات. [10]

ثانياً: عن استخبارات المصادر المفتوحة (OSINT)

OSINT منهج منظم لجمع المعلومات المتاحة من المصادر المفتوحة والتحقق منها وتحليلها. والفرق الأساسي أن OSINT تصف منهجاً ومصادر، بينما التحريات الأمنية الرقمية تصف وظيفة أوسع قد تستخدم المصادر المفتوحة أو المقيدة. وقد أوصى مكتب الأمم المتحدة المعني

بالمخدرات والجريمة (UNODC) بضرورة تحسين قدرات سلطات إنفاذ القانون في استخدام بيانات المصادر المفتوحة في التحقيقات، مع مراعاة الضمانات القانونية. [11] ولا يعني وصف المصدر بأنه مفتوح أن كل استخدام للمعلومات المستمدة منه مشروع بلا قيد.

ثالثاً: عن التحقيق الجنائي الرقمي (بالمعنى الفني)

التحقيق الجنائي الرقمي يتضمن تطبيق مناهج متخصصة لفحص البيانات والأجهزة واستخراج الآثار وتوثيق النتائج الفنية. ويختلف عن التحري في الغرض المباشر ومستوى التخصص وطبيعة المخرجات. والتميز هنا وظيفي ومنهجي، لا تفضيلي. وقد أكد دليل NIST بشأن دمج تقنيات الفحص الجنائي في الاستجابة للحوادث أن الفحص الرقمي يتضمن تحديد البيانات وجمعها وفحصها وتحليلها مع مراعاة سلامتها وسلسلة العهدة. [12]

رابعاً: عن التحقيق القضائي

التحقيق القضائي يمارس ضمن الإجراءات التي ينظمها القانون لكشف الحقيقة بشأن واقعة يحتمل أن تشكل جريمة. ولا تملك نتائج التحريات الأمنية أن تحل محل الأدلة التي يتطلبها القانون. وتقدم اتفاقية بودابست بشأن الجريمة السيبرانية (٢٠٠١) إطاراً دولياً مرجعياً للتدابير الإجرائية المتعلقة بالأدلة الإلكترونية، مع مراعاة أن نطاق التزاماتها يتحدد وفق وضع الدولة المعنية تجاهها. [13]

المبحث الثاني: طبيعة المعلومات الرقمية وحدود الاستدلال بها

المطلب الأول: مفهوم البيانات والمعلومات الرقمية وتصنيفاتها

أولاً: التمييز بين البيانات والمعلومات

البيانات الرقمية هي المعطيات المسجلة أو المخزنة أو المنقولة إلكترونياً. والمعلومات الرقمية هي البيانات التي جرى تنظيمها أو تفسيرها لتصبح ذات دلالة. والانتقال من البيانات إلى المعلومات لا يكون محايداً؛ إذ يتأثر بمعايير المحلل والسياق. [14]

ثانياً: التصنيف بحسب المصدر

١. المصادر المفتوحة (مع خطر نقص السياق وإعادة النشر).
٢. قواعد البيانات والسجلات (مع عدم افتراض أن صدور السجل عن جهة رسمية يضمن صحة كل بيان فيه).
٣. الأجهزة والأنظمة (تتطلب تفسيراً فنياً).
٤. المعلومات المقدمة من الأفراد والجهات.
٥. المعلومات المتبادلة بين الجهات (تقتضي توثيق المصدر والقيود على الاستخدام). [15]

ثالثاً: التصنيف بحسب مستوى التحقق

بيانات غير متحقق منها؛ معلومات جرى التحقق من بعض عناصرها؛ معلومات مؤيدة بمصادر مستقلة (مع مراعاة استقلال المصادر الفعلي)؛ معلومات خضعت لفحص فني متخصص (دون افتراض أن الفحص أثبت كل الادعاءات).

المطلب الثاني: التمييز بين المعلومات الأولية والقرائن والأدلة الرقمية

أولاً: المعلومات الأولية

هي البيانات أو الإفادات أو المؤشرات التي تتوافر في بداية التحري. ولا يعني وصفها بأنها أولية أنها غير صحيحة، بل أن درجة التحقق منها أو وظيفتها الإجرائية لا تزال محدودة. وقد تكون كافية لبدء التحقق، لا للإثبات.

ثانياً: القرينة (بمعناها التحليلي العام)

تقوم على الاستدلال من واقعة ثابتة إلى واقعة أخرى. وينبغي التمييز بين القرينة القانونية (ينشئها المشرع)، والقرينة القضائية (يستنبطها القاضي)، والقرينة التحليلية (يستخدمها المحلل الأمني ولا ترقى بذاتها إلى قرينة قانونية). وسجل الدخول مؤشر على نشاط حساب، لا إثبات لهوية المستخدم.

ثالثاً: الدليل الرقمي

هو بيانات أو معلومات يُراد الاستناد إليها لإثبات واقعة، وفق القواعد التي تحكم جمعها وفحصها وتقديمها. ووصف مادة بأنها دليل رقمي لا يعني قبولها أمام المحكمة. وقد حدد مكتب الأمم المتحدة المعني بالمخدرات والجريمة عناصر تقييم قبول الأدلة الرقمية في: الإذن القانوني، والأصالة، والسلامة، والموثوقية، وإجراءات الفحص، ومؤهلات القائمين عليه. [16]

رابعاً: التمييز بين الأصالة والسلامة والموثوقية والقيمة القانونية

- الأصالة: مدى إمكان التحقق من أن البيانات هي المادة التي يُدعى أنها تمثلها.
- السلامة: المحافظة عليها من التغيير غير الموثق. ويستخدم NIST قيم التجزئة (Hash) للتحقق من السلامة، مع التنبيه إلى أن تغيير بت واحد يغير قيمة التجزئة بالكامل. [17]
- الموثوقية: مدى إمكان الاعتماد عليها بالنظر إلى مصدرها وسياقها.
- القيمة القانونية: صلاحيتها للاستناد وفق القواعد المنطبقة.

وقد تكون البيانات أصلية وسليمة، لكنها لا تثبت الواقعة؛ فوجود ملف على جهاز لا يثبت أن مالك الجهاز أنشأه أو أرسله.

المطلب الثالث: حدود الاستنتاج من المعلومات الرقمية

أولاً: الفرق بين البيانات المسجلة والواقعة المستنتجة

تسجيل النظام وقت دخول واقعة تتعلق بالسجل، لكن الانتقال إلى القول إن شخصاً بعينه استخدم الحساب يتطلب التحقق من هوية المستخدم وآلية الدخول.

ثانياً: أثر المصدر

تختلف أسئلة التحقق بحسب طبيعة المصدر (آلي، يدوي، منشور، مستخرج من جهاز). ويجب التمييز بين المصدر الأصلي والمصدر الناقل.

ثالثاً: حدود البيانات الوصفية

التاريخ المسجل في خصائص ملف لا يثبت بالضرورة الوقت الحقيقي للحدث. وقد أشارت أدبيات NIST إلى أن البيانات الوصفية قد تتأثر بإعدادات الجهاز والمنطقة الزمنية وعمليات النقل. [18]

رابعاً: حدود الصور والفيديو

المحتوى البصري لا يفسر نفسه. وينبغي التمييز بين التحقق من وجود الملف، ومصدره، وسلامته، وصحة سياقه. ولا يكفي إخفاق أداة آلية في اكتشاف التلاعب دليلاً قاطعاً على الأصالة.

خامساً: الارتباط والسببية

الارتباط لا يثبت بالضرورة علاقة سببية. وتزداد خطورة الخلط عند استخدام الأنظمة الآلية.

سادساً: اختبار الفرضيات البديلة والتحيز التأكيدي

من أهم متطلبات التحليل الموضوعي النظر في التفسيرات البديلة، والإفصاح عن مواطن عدم اليقين. وقد أكدت وثائق UNODC أهمية النزاهة والموثوقية في التحقيقات الرقمية. [19]

سابعاً: معيار القرار الأمني مقابل معيار الإثبات القضائي

قد تكون المعلومة الأولية كافية لبدء التحقق أو اتخاذ تدبير وقائي، لكنها لا تكفي لإثبات المسؤولية الجنائية. ولا يجوز في المقابل افتراض أن كل قرار أمني أولي يجوز اتخاذه استناداً إلى أي معلومة غير متحقة.

المبحث الثالث: النطاق الوظيفي والحدود الفاصلة

المطلب الأول: نطاق التحريات من حيث الأشخاص والموضوع والزمان والمكان والوسائل

أولاً: النطاق الشخصي

التمييز بين الشخص المستهدف مباشرة، والأشخاص الذين ترتبط بياناتهم بالواقعة بصورة غير مباشرة، والأشخاص الذين تظهر معلوماتهم عرضاً. ولا يجوز افتراض أن ظهور بيانات شخص في سجل يبرر تلقائياً إدخاله في نطاق التحري.

ثانياً: النطاق الموضوعي

تحديد الوقائع محل التحقق. وكلما كان الغرض أكثر تحديداً، أمكن تقدير مدى صلة البيانات به.

ثالثاً: النطاق الزمني

الفترة التي تشملها المعلومات. وينبغي التمييز بين تاريخ الواقعة وتاريخ إنشاء البيانات وتاريخ تعديلها وتاريخ الحصول عليها.

رابعاً: النطاق الواسع

المصادر المفتوحة، والسجلات، والمعلومات المقدمة، وأنظمة المراقبة، وسجلات الاتصالات، وفحص الأجهزة (متى توافر السند)، والبيانات المستمدة من المستشعرات والطائرات المسييرة، وأدوات التحليل. ولا يجوز تصنيف هذه الوسائل من حيث المشروعية بناءً على طبيعتها التقنية وحدها.

خامساً: النطاق المكاني

قد تتعلق التحريات ببيانات مخزنة لدى مزود خدمة في دولة أخرى. ولا يجوز افتراض أن القدرة التقنية على الوصول تعني امتلاك الاختصاص القانوني. وتقدم اتفاقية بودابست، والبروتوكول الإضافي الثاني (٢٠٢٢) بشأن تعزيز التعاون والإفصاح عن الأدلة الإلكترونية، آليات مرجعية للتعاون العابر للحدود، مع مراعاة وضع الدولة تجاهها. [20]

سادساً: التناسب

مشروعية الغرض لا تكفي وحدها لتبرير كل إجراء. ويقتضي التناسب النظر في ملائمة الوسيلة، وإمكان تحقيق الغرض بوسيلة أقل تدخلاً. وقد أكد فريق خبراء UNODC أهمية مبدأ التناسب عند استخدام التقنيات الخاصة في التحقيقات. [21]

المطلب الثاني: التمييز بين الأعمال الأمنية والإدارية والإجراءات الجزائية

أولاً: أهمية التمييز

إضفاء وصف إداري على إجراء ذي طبيعة جزائية لا ينبغي أن يكون وسيلة لتجاوز الضمانات. وقد ميز الفقه العربي بين "التحريات الإدارية" التي تأمر بها جهة إدارية، و"التحريات القضائية"

المرتبطة بواقعة جنائية، مؤكداً أن الأولى قد يترتب عليها آثار بعيدة المدى في المساس بحقوق الجمهور. [22]

ثانياً: الأعمال الإدارية الرقمية

التحقق من استيفاء شروط خدمة، ومراجعة السجلات، وتدقيق المعاملات. ولا تتحول تلقائياً إلى تحريات أمنية لمجرد أن المعلومات قد تكشف عن مخالفة.

ثالثاً: الأعمال الأمنية الرقمية

تستهدف حماية الأمن أو الوقاية. ولا تتساوى جميعاً في درجة التدخل. ولا يكفي وصف النشاط بأنه أمني لتبرير استخدام أي وسيلة.

رابعاً: الإجراءات الجزائية الرقمية

تستخدم الوسائل الرقمية في سياق الكشف عن الجرائم. ولا تتحدد الطبيعة الجزائية بمجرد استخدام أداة رقمية، بل بالغرض الإجرائي والسند القانوني.

خامساً: المعيار الوظيفي

الغرض المباشر، والجهة القائمة بالإجراء، وطبيعة الوسيلة ودرجة التدخل، والآثار المتوقعة، والسند القانوني والضمانات.

سادساً: تغير طبيعة الإجراء

قد يبدأ النشاط إدارياً أو أمنياً ثم تظهر معلومات تستدعي الانتقال إلى إجراء جزائي. ويقتضي ذلك إعادة تقييم السند والاختصاص والضمانات.

المطلب الثالث: الحدود الفاصلة بين التحري والاستدلال والتحقيق القضائي

أولاً: التحري

نشاط يهدف إلى جمع المعلومات والتحقق منها بشأن واقعة، بقصد تكوين تصور أولي. ولا يفترض أن ينتهي دائماً إلى إثبات واقعة.

ثانياً: الاستدلال الجنائي

الأعمال التي تهدف إلى جمع المعلومات الأولية عن جريمة محتملة، تمهيداً لتقدير الحاجة إلى تحريك الإجراءات. وتختلف حدوده من نظام لآخر.

ثالثاً: التحقيق القضائي

مجموعة الإجراءات التي تباشرها السلطة المخولة قانوناً للتحقيق في واقعة يُشتبه في كونها جريمة، وفق الضمانات المقررة.

رابعاً: معايير التمييز

١. الغرض: تحرّ / استدلال / تحقيق.

٢. الجهة المختصة: تتحدد سلطة كل جهة وفق القانون.

٣. طبيعة الإجراء: الاطلاع على منشور عام لا يساوي الدخول إلى حساب خاص.

٤. الآثار القانونية: نتائج التحري لا تثبت المسؤولية الجنائية.

٥. الضمانات: تختلف بحسب طبيعة الإجراء والحقوق المتأثرة.

خامساً: انتقال المعلومات

الإحالة تعني أن المعلومات تستحق نظر الجهة المختصة، لا أن الوقائع ثبتت. وينبغي التحقق من المصدر وطريقة الحصول والتوثيق.

سادساً: أثر المخالفة

لا يمكن تقرير أثر موحد لكل مخالفة في جميع الأنظمة. ويجب التمييز بين المخالفة القانونية والخلل الفني. وقد أشارت وثائق UNODC إلى أن آثار المخالفات الإجرائية تختلف بحسب التشريع المنطبق. [23]

النافذة التطبيقية والتشريعية العربية

أولاً: على مستوى التشريعات العربية

لا يوجد نص عربي موحد يعرف "التحريات الأمنية الرقمية". وتتفاوت التشريعات العربية في تنظيم الأدلة الرقمية. وقد خلصت دراسة مقارنة شملت مصر والجزائر والأردن ودول مجلس التعاون الخليجي إلى وجود "فجوات وتناقضات كبيرة" في تشريعات الأدلة الرقمية، مع الحاجة إلى أحكام تشريعية أوضح بشأن استخدام البرمجيات الخبيثة من قبل سلطات التحقيق، ومقبولية الأدلة الإلكترونية العابرة للحدود، وحماية السيادة الإلكترونية للدول. [24] كما أوصى الدليل الاسترشادي الصادر عن جامعة نايف العربية للعلوم الأمنية (٢٠٢٤) بضرورة التعامل مع الأدلة الرقمية من الجانبين القانوني والإجرائي، مع الاستناد إلى اتفاقية بودابست وأفضل الممارسات الدولية. [25]

ثانياً: على مستوى التطبيق العملي (سيناريو مختصر)

تلقت جهة أمنية بلاغاً عن حساب إلكتروني يروج لمحتوى يمس الأمن العام. فبدأت بالتحقق من المحتوى المنشور للعموم (مصدر مفتوح). ثم لاحظت تزامناً بين نشر المحتوى وموقع جغرافي معين (قرينة تحليلية). ثم طلبت بيانات من مزود الخدمة (بيانات محمية تحتاج سنداً قانونياً).

• المعلومة الأولية: وجود منشور عام.

• القرينة التحليلية: التزامن بين النشر والموقع.

• الدليل الرقمي المحتمل: سجل الاتصال المستخرج من مزود الخدمة بعد الإذن.

والدرس: لا يجوز الانتقال من المعلومة الأولية إلى الدليل دون التحقق من مشروعية الوصول، ولا يجوز اعتبار التزام دليلاً على الفاعلية دون استبعاد الفرضيات البديلة.

الجدول (١): تصنيف البيانات الرقمية في التحريات الأمنية

معيار التصنيف	الفئة	الخصائص القانونية والفنية	أثر التصنيف على إجراءات التحري
بحسب المصدر	مصادر مفتوحة	متاحة للعموم؛ سهولة وصول نسبية؛ خطر نقص السياق وإعادة النشر	لا تُعفى من التحقق؛ كثرة النقل لا تعني تأكيداً مستقلاً
	سجلات وقواعد بيانات	صادرة عن جهة منشئة؛ تتفاوت موثوقيتها بحسب آلية الإدخال	لا يكفي صدورهما عن جهة رسمية لضمان صحة كل بيان فيها
	أجهزة وأنظمة	تتطلب تفسيراً فنياً؛ قد تكون بيانات متطيرة أو مشفرة	تحتاج سنداً قانونياً للوصول؛ وفحصاً متخصصاً لاستخراجها
	معلومات مقدمة من أفراد/جهات	تتأثر بمصلحة مقدمها وتفسيره	تستلزم التحقق من المصدر وظروف الحصول
	معلومات متبادلة بين جهات	تخضع لقيود المشاركة والاستخدام	يجب توثيق المصدر والقيود القانونية على إعادة الاستخدام
	غير متحقق منها	لم يُثبت مصدرها أو صحتها أو سياقها	لا تصلح أساساً لاستنتاج؛ تُستخدم كمؤشر لبدء التحقق فقط
بحسب مستوى التحقق	متحقق من بعض عناصرها	أمكن تأكيد جوانب دون أخرى	يجب بيان ما تحقق وما بقي غير محسوم
	مؤيدة بمصادر مستقلة	مصادر متعددة ثبت استقلالها الفعلي	تكتسب وزناً أكبر؛ مع التحقق من عدم إعادة إنتاج أصل واحد
	خضعت لفحص فني متخصص	اختبارات فنية موثقة تتناسب مع طبيعتها	لا يعني الفحص إثبات كل الادعاءات؛ لكل اختبار نطاق محدد
بحسب الطبيعة	نصية / مرئية / صوتية / مكانية / زمنية / وصفية / سجلات تشغيل	تختلف في طريقة الفحص وحدود الاستنتاج	كل فئة تتطلب إجراءات فحص وتحقق مختلفة؛ البيانات الوصفية لا تثبت وحدها الوقت أو المكان

الجدول (٢): المقارنة بين التحري والاستدلال والتحقيق القضائي

معيـار المقارنة	التحقيق القضائي	الاستدلال الجنائي	التحري الأمني (الرقمي)
الغرض	التحقق من الواقعة الجنائية وجمع أدلتها وفق القانون	جمع معلومات أولية عن جريمة محتملة	جمع المعلومات والتحقق منها في نطاق الوظيفة الأمنية
الجهة المختصة	السلطة المخولة قانوناً بالتحقيق (قاضٍ/نيابة)	جهات الضبط القضائي وفق القانون المنطبق	الجهة الأمنية وفق اختصاصها القانوني
طبيعة الإجراء	إجراءات إجرائية محددة بضمانات	إجراءات أولية يحددها القانون	يتراوح بين الاطلاع على مصادر مفتوحة وفحص أجهزة (بحسب السند)
الآثار القانونية	تستهدف جمع الأدلة وفحصها؛ لا يعني القبول التلقائي	لا تُعد أدلة كاملة؛ تمهيد لتقدير الحاجة للتحقيق	لا تثبت المسؤولية الجنائية بذاتها؛ نتائج أولية
الضمانات	ضمانات إجرائية محددة (إذن، دفاع، توثيق)	تختلف بحسب التشريع	تختلف بحسب درجة التدخل في الحقوق
العلاقة بالمراحل الأخرى	قد تعتمد على معلومات سابقة مع التحقق من مشروعيّتها	قد تسبق التحقيق	قد تمهد للاستدلال أو التحقيق

النتائج العامة للفصل

١. التحريات الأمنية الرقمية نشاط وظيفي يجمع بين جمع المعلومات والتحقق منها وتقييم دلالتها في نطاق الاختصاص.
٢. لا يوجد تعريف دولي موحد ملزم، الأمر الذي يستلزم اعتماد تعريف تحليلي مع مراعاة اختلاف التشريعات.
٣. لا يحدد الطابع الرقمي وحده الطبيعة القانونية للنشاط؛ بل الغرض والاختصاص وطبيعة الإجراء والحقوق المتأثرة.
٤. يجب التمييز بين البيانات والمعلومات والقرائن والأدلة، وبين الأصالة والسلامة والموثوقية والقيمة القانونية.
٥. لا يؤدي وصف المادة بأنها دليل رقمي إلى قبولها قانوناً أو كفايتها للإثبات تلقائياً.
٦. يجب أن تتناسب الاستنتاجات مع ما تثبته البيانات، مع اختبار الفرضيات البديلة وتجنب التحيز التأكيدي.
٧. يتحدد نطاق التحريات من حيث الأشخاص والموضوع والزمان والمكان والوسائل، ويرتبط بالغرض المشروع والاختصاص ومبدأ التناسب.
٨. لا يؤدي توافر البيانات أو إمكان الوصول التقني إلى منح الجهة سلطة قانونية غير مقررّة.
٩. قد تستخدم الوسائل الرقمية ذاتها في الأعمال الإدارية والأمنية والجزائية، لكن ذلك لا يعني وحدة الضوابط.
١٠. تختلف التحريات عن الاستدلال والتحقيق من حيث الوظيفة والاختصاص والآثار.
١١. يجب الفصل بين مشروعية الإجراء وصحة النتيجة الفنية والقيمة القانونية للمعلومات.
١٢. سلامة منظومة التحريات الرقمية تتطلب وضوحاً في المفاهيم، وانضباطاً في النطاق، وموضوعية في التحليل، وتوثيقاً، واحتراماً للضمانات.

المراجع

(1) هذا التعريف تحليلي إجرائي صيغ لضبط نطاق الدراسة، ولا يمثل تعريفاً تشريعياً موحداً. وللمقارنة، انظر: هشام مصطفى محمد، *التحريات الأمنية وأثرها في الأدلة الجنائية*، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٥، ص ١٢ وما بعدها.

(2) انظر: عادل عبد العال خراشي، *ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي*، ٢٠٠٦، ص ٤٥ وما بعدها، بشأن ضوابط الاختصاص في أعمال التحري والاستدلال، مع التمييز بين الاختصاص بموضوع الإجراء والاختصاص بالوسيلة المستخدمة.

(3) Council of Europe, *International Standards on Collection and Handling of Electronic Evidence*, Cybercrime Programme Office, available at: coe.int/en/web/cybercrime (last visited: 2026).

(4) انظر: "كفاية التحري ومشروعاته"، دراسة فقهية منشورة في مجلة القانون والاقتصاد، مجلة كلية الحقوق، جامعة طنطا، ٢٠٢١، ص ٩، متاحة عبر منصة بنك المعرفة المصري.

(5) National Institute of Standards and Technology (NIST), *Guide to Integrating Forensic Techniques into Incident Response*, Special Publication 800-86, August 2006.

(6) United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 6: Digital Evidence Admissibility*, Education for Justice Initiative, 2019, p. 4 بشأن ضرورة التمييز بين المصادر المستقلة للمعلومات والمصادر المتعددة التي تعيد إنتاج معلومات مستمدة من أصل واحد.

(7) Barbara Guttman et al., *Digital Evidence Preservation: Considerations for Evidence Handlers*, NIST Interagency Report 8387, National Institute of Standards and Technology, September 2022, pp. 1–2.

(8) Guttman et al., *Digital Evidence Preservation: Considerations for Evidence Handlers*, op. cit., p. 2.

(9) Council of Europe, *International Standards on Collection and Handling of Electronic Evidence*, op. cit.

(10) عادل عبد العال خراشي، ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي، مرجع سابق، ص ٥٢-٥٥.

(11) United Nations Office on Drugs and Crime (UNODC), *Report on the Meeting of the Expert Group on Cybercrime*, UN document CCPCJ/EG.4/2021/2, para. 29.

(12) National Institute of Standards and Technology (NIST), *Guide to Integrating Forensic Techniques into Incident Response*, op. cit., Section 2-1.

(13) Council of Europe, *Convention on Cybercrime*, ETS No. 185, Budapest, 23 November 2001, Article 23 et seq.

(14) United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 6: Digital Evidence Admissibility*, op. cit., pp. 2–3.

(15) UNODC, *Cybercrime Module 6: Digital Evidence Admissibility*, op. cit.

(16) UNODC, *Cybercrime Module 6: Digital Evidence Admissibility*, op. cit., p. 5.

(17) Guttman et al., *Digital Evidence Preservation: Considerations for Evidence Handlers*, op. cit., pp. 3–4.

(18) Guttman et al., *Digital Evidence Preservation: Considerations for Evidence Handlers*, op. cit., pp. 3–4.

(19) United Nations Office on Drugs and Crime (UNODC), *Report on the Meeting of the Expert Group on Cybercrime*, op. cit., para. 36.

(20) Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*, CETS No. 224, opened for signature on 12 May 2022.

(21) UNODC, *Report on the Meeting of the Expert Group on Cybercrime*, op. cit., para. 37.

(22) انظر: المرجع الفقهي العربي المتعلق بالتحريات الإدارية، المتاح عبر منصة بنك المعرفة المصري. لم ترد في (22) البيانات المقدمة معلومات كافية لتحديد اسم المؤلف أو عنوان المرجع كاملاً أو بيانات نشره.

(23) UNODC, *Report on the Meeting of the Expert Group on Cybercrime*, op. cit., para. 37.

(24) Raed S. A. Faqir et al., "Digital Evidence Extracted from Electronic Media: A Comparative Study," *International Journal of Cyber Criminology*, 2025, Abstract.

(25) عبد الرزاق المرجان وآخرون، *الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية*، دار جامعة عبد الرزاق المرجان وآخرون، الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية، دار جامعة عبد الرزاق المرجان وآخرون، الرياض، ٢٠٢٤، الملخص التنفيذي، ص ٩.

الفصل الثاني: الأساس القانوني لمشروعية التحريات الأمنية الرقمية

المبحث الأول: السند القانوني والاختصاص في أعمال التحري

المطلب الأول: الأساس التشريعي للتحريات الأمنية الرقمية

تشير التحريات الأمنية الرقمية إشكالية تتجاوز مجرد قدرة الجهات الأمنية على الوصول إلى المعلومات الإلكترونية؛ إذ تتعلق بمدى امتلاكها سنداً قانونياً يجيز جمع المعلومات ومعالجتها وربطها واستنتاج الدلالات الأمنية منها، مع مراعاة الحقوق والحريات. فالتطور التقني الذي أتاح إمكانات واسعة لرصد الأنشطة الرقمية لا يُنشئ بذاته اختصاصاً قانونياً جديداً.^[1]

ويقتضي تحديد الأساس التشريعي التمييز بين ثلاثة مستويات: القواعد التي تحدد اختصاص الجهات الأمنية، والقواعد التي تجيز استخدام وسائل معينة، والقواعد التي تحكم معالجة البيانات. فمشروعية الغرض الأمني لا تستلزم بالضرورة مشروعية كل وسيلة، كما أن جواز الحصول على معلومة لا يعني إباحة الاحتفاظ بها أو تداولها دون قيود.^[2]

ويجد هذا المبدأ أساسه في سيادة القانون، التي تقتضي خضوع النشاط الأمني للقواعد المنظمة له، لا لمجرد التقدير المهني. ولا يعني ذلك أن كل تفصيل تقني يجب أن يرد في نص مستقل، بل يعني وجود أساس قانوني واضح يجيز نوع التدخل، مع تنظيم المسائل التي تمس الحقوق الأساسية بما يحقق إمكانية توقع حدود السلطة والرقابة عليها.^[3]

ويبرز ذلك عند استخدام الوسائل الرقمية لأن أثر الإجراء قد يتجاوز نطاقه الظاهر؛ فالوصول إلى سجل إلكتروني قد يكشف شبكة العلاقات الاجتماعية أو التحركات أو العادات، وقد يؤدي تجميع بيانات متفرقة إلى تكوين صورة تفصيلية عن الحياة الخاصة. ومن ثم، لا يكفي تقييم الإجراء بحسب كل بيانات منفردة، بل بالنظر إلى الأثر التراكمي الناتج عن جمعها وربطها.^[4]

وقد قررت لجنة حقوق الإنسان التابعة للأمم المتحدة، في تفسيرها للمادة السابعة عشرة من العهد الدولي، أن الحماية من التدخل في الخصوصية يجب أن تكون مقررّة في القانون، وأن يتوافق أي تدخل مع أحكام العهد.^[5] كما أكدت مفوضية الأمم المتحدة السامية لحقوق الإنسان في تقاريرها بشأن الحق في الخصوصية في العصر الرقمي أهمية إخضاع ممارسات المراقبة والوصول إلى البيانات لضوابط قانونية وحقوقية.^[6]

ولا ينبغي فهم اشتراط السند القانوني على أنه مجرد وجود نص عام يشير إلى حماية الأمن؛ إذ يتعين أن تكون القواعد قادرة على تحديد طبيعة السلطة وحدودها والضمانات المرتبطة بها. وتبعاً لذلك، يمكن التمييز بين التنظيم العام للاختصاص الأمني، والتنظيم الخاص للوسائل والإجراءات الرقمية. ويجب ألا يؤدي وجود التنظيم العام إلى إهدار ضرورة التنظيم الخاص متى كانت الوسيلة تنطوي على تدخل جوهري في الحقوق.^[7]

ويؤكد هذا الاتجاه الإطار الذي أقرته اتفاقية مجلس أوروبا لحماية البيانات رقم ١٠٨ ونسختها الحديثة (١٠٨+)، الذي أرسى مبادئ مشروعية المعالجة وعدالتها، وتحديد الأغراض، وتناسب البيانات مع الغرض، ودقتها، وعدم الاحتفاظ بها مدة تتجاوز الحاجة. [8] وتُستفاد من هذه المبادئ قيمة معيارية في تصميم الأطر القانونية للتحريات الرقمية، مع مراعاة نطاق انطباق الاتفاقية والتزامات الدول الأطراف.

ومن الناحية التحليلية، ينبغي التمييز بين القواعد الدولية الملزمة للدولة التي ارتبطت بها قانوناً، والتفسيرات الصادرة عن الهيئات الدولية، والمعايير المهنية والفنية. فالمعاهدة النافذة تختلف في طبيعتها عن تقرير هيئة دولية أو دليل فني؛ وقد تكون الأخيرة ذات قيمة تفسيرية، لكنها لا تتحول إلى نص تشريعي يمنح اختصاصاً لم يقره القانون. [9]

ويظهر هذا التمييز في اتفاقية بودابست بشأن الجريمة المعلوماتية (2001)؛ إذ توفر إطاراً دولياً لتجريم بعض صور الاعتداء على الأنظمة المعلوماتية، وتنظيم بعض الصلاحيات الإجرائية المتعلقة بالأدلة الإلكترونية، وتعزيز التعاون الدولي. غير أن نطاق الالتزامات يتحدد وفق نصوصها وشروط تطبيقها، ولا يجوز اعتبارها تفويضاً عاماً للوصول إلى البيانات الرقمية دون التقيد بالقانون الوطني. [10]

وعليه، فإن الأساس التشريعي السليم يقوم على الجمع بين اختصاص أممي محدد، وسند قانوني مناسب لطبيعة الإجراء، وضمانات تكفل عدم تحول القدرة التقنية إلى سلطة غير محدودة. وتزداد أهمية ذلك كلما انتقل الإجراء من الاطلاع على المعلومات المتاحة إلى المراقبة الموجهة أو الوصول إلى البيانات المحمية.

المطلب الثاني: اختصاص الجهات القائمة بالتحري و حدود سلطاتها

يمثل الاختصاص أحد المحددات الأساسية للمشروعية؛ إذ لا يكفي أن يكون الإجراء مفيداً أمنياً، بل يجب أن يصدر عن جهة تملك قانوناً صلاحية اتخاذه، وأن يُمارس في الحدود الموضوعية والمكانية والشخصية التي رسمها القانون. [11]

ويقتضي ضبط الاختصاص التمييز بين أربعة أدوار تتداخل عملياً لكنها مختلفة قانوناً:

١. اختصاص المبادرة بالتحري: تلقي المعلومات الأولية وتحديد المسألة الأمنية.
٢. اختصاص الإذن أو التصريح: الموافقة على الإجراءات التي يشترط القانون عرضها على قاضٍ أو جهة مختصة.
٣. اختصاص التنفيذ الفني: الاستخراج أو الفحص أو المعالجة بواسطة أشخاص مؤهلين ومخولين.
٤. اختصاص التقييم القانوني للنتائج: تحديد الآثار القانونية للمعلومات. [12]

ويحول هذا التمييز دون الخلط بين سلطة اتخاذ القرار وسلطة تنفيذه. فقد يكون الموظف مخولاً بتنفيذ عملية فنية محددة، لكنه لا يملك توسيع نطاقها أو تغيير غرضها أو الوصول إلى بيانات لم يشملها الإذن. كما أن صدور الإذن لا يعني أن كل إجراء فني لاحق يصبح مشروعاً تلقائياً. [13]

وتتعدد صور الاختصاص بحسب طبيعة الإجراء. فجمع المعلومات المنشورة قد يدخل ضمن الوظائف المعتادة، بينما يخضع الوصول إلى بيانات الاتصالات أو اعتراضها أو تفتيش الأجهزة لشروط أشد، قد تشمل إذناً قضائياً مسبقاً. ولا توجد قاعدة عالمية موحدة تحدد الجهة صاحبة الاختصاص؛ لأن توزيع السلطات يختلف بين النظم القانونية. [14]

ومع ذلك، يمكن استخلاص معيار عام: **التناسب بين خطورة التدخل والضمانات المحيطة به**. فكلما ازدادت قدرة الإجراء على كشف الحياة الخاصة أو مراقبة الاتصالات، تعاظمت الحاجة إلى وضوح الاختصاص ووجود رقابة مستقلة وفعالة. [6]

وتبرز مشكلة توسع الجهة في نطاق الجمع بسبب سهولة نسخ البيانات وربطها. فقد يبدأ الإجراء للتحقق من واقعة محددة، ثم يمتد إلى معلومات لا ترتبط مباشرة بالموضوع. وفي هذه الحالة، لا يكفي الاحتجاج بأن البيانات أصبحت متاحة تقنياً، بل يتعين وجود أساس قانوني يجيز توسيع المعالجة. [15]

ويتعين مراعاة **الحدود الشخصية للاختصاص**. فإذا أسفر التحري عن بيانات تتعلق بأشخاص غير مستهدفين، فلا يجوز افتراض أن ظهورها يمنح صلاحية مطلقة في جمعها أو الاحتفاظ بها. بل يجب تحديد ما إذا كانت لازمة لتحقيق الغرض المشروع، وما إذا كان القانون يجيز معالجتها. [16]

ويقضي حسن تنظيم الاختصاص وضع قواعد واضحة تحدد الجهة التي تبدأ التحري، والجهة التي توافق، والجهة التي تنفذ، والجهة التي تراجع. كما ينبغي توثيق القرارات الجوهرية التي تؤثر في نطاق الإجراء. ولا يقتصر أثر تحديد الاختصاص على منع التجاوز، بل يمتد إلى تعزيز موثوقية النتائج؛ فعندما تكون المسؤوليات واضحة، يصبح بالإمكان تحديد من اتخذ القرار ومن نفذ ومن اعتمد النتيجة. [17]

المطلب الثالث: حالات اشتراط الإذن القضائي أو التصريح المختص

يرتبط اشتراط الإذن القضائي بفكرة جوهرية: بعض إجراءات التحري تنطوي على تدخل شديد في الحقوق، بما يجعل ترك تقرير مشروعيتها للتقدير المنفرد للجهة القائمة بالتنفيذ غير كافٍ. ويهدف الإذن إلى إخضاع الإجراء لتقييم سابق يوازن بين الغرض المشروع وضرورة التدخل وتناسب الوسيلة. [18]

ولا يمكن تحديد الحالات التي تتطلب إذناً قضائياً على نحو موحد لجميع الدول؛ إذ تختلف التشريعات في تحديد السلطات المختصة وشروط الإذن ومدته ونطاقه. ولذلك، ينصرف التحليل إلى تحديد المبادئ التي تبرر اشتراط الإذن، مع ترك تحديد الحالات الإلزامية للقانون الواجب التطبيق. [19]

وتبرز الحاجة إلى الإذن بوجه خاص عند اعتراض محتوى الاتصالات الخاصة، أو الوصول إلى بيانات لا يملك الجمهور الاطلاع عليها، أو تفتيش الأجهزة الإلكترونية واستخراج محتوياتها، أو مراقبة تحركات شخص بصورة مستمرة عبر بيانات الموقع، أو استخدام وسائل تقنية تؤدي إلى جمع معلومات تفصيلية. وتظل هذه الأمثلة خاضعة لما يقرره كل نظام قانوني. [20]

ويجب التمييز بين الإذن القضائي والتصريح الإداري. فالإذن القضائي يصدر عن سلطة قضائية مختصة، بينما قد يصدر التصريح الإداري عن جهة تنفيذية أو تنظيمية. ولا يجوز اعتبار أحدهما بديلاً عن الآخر إذا كان القانون يشترط صراحة الحصول على إذن قضائي. [21]

كما يجب التمييز بين الإذن باستخدام وسيلة تقنية والإذن بالوصول إلى بيانات محددة. فقد يكون تشغيل نظام تصوير مشروعا تنظيمياً، دون أن يعني ذلك جواز استخدام تسجيلاته لأي غرض أو إجراء تحليل واسع للتعرف على الأشخاص. [22]

وتتحدد فعالية الإذن بمدى وضوح عناصره. فالإذن الذي يجيز جمع بيانات غير محددة دون بيان الغرض أو النطاق أو المدة قد يفقد قدراً مهماً من وظيفته الضمانية. لذلك، ينبغي أن يحدد الإذن موضوع الإجراء والغاية والبيانات أو الأشخاص المشمولين والمدة وحدود التنفيذ. [23]

وتكتسب هذه العناصر أهمية إضافية في البيئة الرقمية؛ لأن الإذن قد يتعلق بجهاز واحد يحتوي على كميات هائلة من البيانات المتباينة. وقد يشمل معلومات مرتبطة بموضوع التحري، إلى جانب مراسلات شخصية ووثائق مهنية وبيانات تخص آخرين. ومن ثم، لا ينبغي تفسير الإذن بفحص الجهاز على أنه ترخيص غير محدود، بل يجب تحديد النطاق واتخاذ التدابير لتقليل الوصول إلى البيانات غير المرتبطة. [24]

وقد تقتضي ظروف استثنائية اتخاذ إجراء عاجل قبل الحصول على الإذن، إذا كان القانون يجيز ذلك. غير أن الاستثناء لا يجوز أن يتحول إلى مسار مواز لتجاوز الضمانة الأصلية. ولذلك، ينبغي أن تكون شروط اللجوء إلى الإجراء العاجل محددة قانوناً، وأن يقتصر على القدر الضروري، وأن يخضع للمراجعة اللاحقة. [25]

وتؤكد المعايير الدولية أهمية الإذن المستقل والرقابة الفعالة على إجراءات المراقبة التي تمس الاتصالات والبيانات الشخصية، بما في ذلك وجود آليات قادرة على فحص مشروعية التدخل ونطاقه. [6] وتكمن أهمية الاستقلال في تقليل مخاطر تضارب المصالح بين الجهة التي تطلب الإجراء والجهة التي تراجعها.

ولا تنتهي وظيفة الإذن بمجرد صدوره؛ إذ يجب التحقق من التزام التنفيذ بحدوده. فإذا صدر الإذن لجمع بيانات عن فترة زمنية معينة، فلا يجوز تجاوزها دون أساس قانوني. وإذا حُدد الإجراء بشخص أو حساب أو جهاز، فلا يجوز توسيعه لمجرد أن البيانات

كشفت عن معلومات إضافية. وقد تستدعي المعلومات الجديدة اتخاذ إجراء مستقل أو طلب توسيع الإذن. [26]

وإذا نُفذ الإجراء دون الإذن الواجب أو تجاوز حدوده، فإن الأثر القانوني يتحدد وفق التشريع المعني وطبيعة المخالفة ومدى اتصالها بالحقوق والضمانات. ولا يصح افتراض أن كل مخالفة تؤدي تلقائياً إلى استبعاد المعلومات، كما لا يصح افتراض أن سلامة النتيجة الفنية تصحح عدم مشروعية الحصول عليها. [27]

المبحث الثاني: الضوابط الموضوعية للحصول على المعلومات ومعالجتها

المطلب الأول: مبدأ المشروعية وتحديد الغرض

يقتضي مبدأ المشروعية ألا يُنظر إلى جمع المعلومات الرقمية باعتباره نشاطاً متروكاً للتقدير المهني، بل ممارسة لسلطة عامة يجب أن تستند إلى أساس قانوني وأن تُوجَّه إلى غرض مشروع. ويشمل المبدأ **جانبين**: مشروعية السلطة (الاختصاص)، ومشروعية استعمالها (الوسيلة والنطاق والغرض والضمانات). [28]

ويتصل بذلك **مبدأ تحديد الغرض**، الذي يقتضي أن يكون الهدف من جمع البيانات محدداً ومشروعاً قبل بدء المعالجة، وأن ترتبط البيانات به ارتباطاً معقولاً. ويحول هذا المبدأ دون تحول التحري إلى عملية مفتوحة لجمع كل ما يمكن الوصول إليه. [29]

وقد أكدت أطر حماية البيانات، ومنها اتفاقية ١٠٨، أهمية تحديد الأغراض المشروعة وعدم استخدام البيانات على نحو يتعارض مع الأغراض التي جُمعت من أجلها. [8] ويُظهر ذلك أن مشروعية الجمع لا تُقيَّم بمعزل عن الاستخدام اللاحق؛ فقد يكون الحصول على معلومة مشروعاً لغرض محدد، لكن تداولها على نطاق أوسع قد يتطلب سنداً آخر. [30]

ومن الناحية التطبيقية، ينبغي أن يتضمن تخطيط التحري تحديد المسألة المراد التحقق منها، والسبب الذي يستدعي جمع المعلومات، والوسائل الملائمة، والفترة الزمنية، والفئات التي يمكن أن تتأثر. ولا يلزم أن تكون جميع النتائج معروفة مسبقاً؛ لكن عدم اليقين لا يعني جواز غياب الحدود الموضوعية. [31]

ويجب التمييز بين **الهدف الأمني العام والهدف المباشر من التحري**. فالمحافظة على الأمن العام غاية مشروعة في أصلها، لكنها واسعة لا تكفي وحدها لتبرير كل إجراء رقمي. ويجب أن يرتبط التدخل بمهمة تدخل في الاختصاص القانوني، وأن يكون له مبرر واقعي. [32]

وتزداد أهمية ذلك عند استخدام أدوات التحليل الآلي التي تجمع البيانات من مصادر متعددة؛ فقد يؤدي الربط إلى استنتاجات لم تكن ظاهرة في أي مصدر منفرد. ولذلك، يجب ألا يُعامل مجرد إمكان اكتشاف علاقات رقمية على أنه مبرر كافٍ لجمع جميع البيانات المتاحة. [33]

ويشمل تحديد الغرض تنظيم **إعادة استخدام البيانات**؛ فإذا جُمعت معلومات لغرض معين ثم ظهرت إمكانية استخدامها لغرض آخر، وجب التحقق من مدى توافق الاستخدام الجديد مع الأساس القانوني الأول أو الحاجة إلى سند مستقل. ولا يمكن تقرير أن كل استخدام ثانوي ممنوع، كما لا يجوز افتراض أن كل استخدام لاحق مباح. [34]

ويشمل ذلك **مشاركة المعلومات مع الجهات الأخرى**؛ فالإفصاح ليس عملية محايدة، وقد يؤدي إلى توسيع دائرة الوصول أو إدخال البيانات في قواعد مختلفة. ومن ثم، ينبغي أن

يستند النقل إلى أساس قانوني، وأن يرتبط بحاجة وظيفية واضحة، وأن يقتصر على القدر اللازم. [35]

ويظهر البعد الحقوقي في المادة السابعة عشرة من العهد الدولي، التي تحمي الأفراد من التدخل التعسفي أو غير القانوني في خصوصيتهم ومراسلاتهم. ويترتب على ذلك أن وجود مصلحة عامة لا يكفي وحده لتبرير التدخل، بل يجب تقييمه في ضوء القانون والضمانات. [5]

ولا ينبغي الخلط بين تحديد الغرض وتجميد نطاق التحري؛ فقد تكشف المعلومات الأولية عن وقائع مرتبطة بمسألة أخرى، لكن الانتقال إلى بحثها يجب أن يكون منظماً قانوناً، مع توثيق سبب التعديل والتحقق من الاختصاص والسند. [36]

المطلب الثاني: الضرورة والتناسب وحدود الوسائل

يشكل مبدأ الضرورة والتناسب من أهم الضوابط التي تحكم استعمال الوسائل الرقمية؛ لأن مشروعية الغرض لا تعني أن كل وسيلة قادرة على تحقيقه مقبولة قانوناً. [37]

وتعني **الضرورة** وجود حاجة حقيقية إلى الإجراء لتحقيق غرض مشروع، وألا يكون التدخل مجرد إجراء احتياطي غير محدد. ويتقضي تقييمها فحص العلاقة بين المعلومات المطلوبة والهدف، ومدى إمكان الاعتماد على وسائل أقل تدخلاً، مع مراعاة الفعالية العملية لكل بديل. [38]

أما **التناسب** فيتعلق بتقييم العلاقة بين أهمية الهدف الأمني وشدة التدخل في الحقوق، بما يشمل نطاق البيانات، وعدد الأشخاص المتأثرين، ومدة المراقبة، وطبيعة المعلومات، وإمكان إعادة استخدامها، والمخاطر الناتجة عن تسريبها. ولا يكفي أن تكون الوسيلة فعالة تقنياً، بل يجب أن يكون تدخلها مبرراً. [39]

ويُستفاد من تقارير مفوضية الأمم المتحدة السامية لحقوق الإنسان أن مشروعية المراقبة تتطلب فحص أساسها القانوني وغرضها وضرورتها وتناسبها، مع أهمية الرقابة المستقلة. [6] وتؤكد هذه المعايير أن الضرورة والتناسب ليسا وصفين يضافان بعد اتخاذ القرار، بل عنصران ينبغي أخذهما في الاعتبار عند اختيار الوسيلة وتحديد نطاقها. [40]

ويمكن تطبيق ذلك من خلال التمييز بين مستويات التدخل: البحث المحدود في معلومات منشورة قد يكون أقل تدخلاً من مراقبة حساب بصورة مستمرة، في حين أن اعتراض محتوى الاتصالات أو استخراج كامل بيانات جهاز قد يثير مستوى أشد. ولا تعني هذه المقارنة أن الوسائل الأقل تدخلاً مشروعة دائماً أو أن الأشد ممنوعة دائماً. [41]

وتظهر أهمية الضرورة في **تحديد مدة الإجراء**. فالمراقبة التي قد تكون مبررة خلال فترة قصيرة لا تصبح مشروعة بلا حدود زمنية. وكلما امتدت المدة، زادت كمية البيانات المتراكمة واتسعت إمكانية تكوين صورة تفصيلية. لذلك، ينبغي أن تكون المدة متناسبة مع الغرض، وأن تخضع للمراجعة. [42]

ويجب النظر إلى التناسب من زاوية **النطاق الشخصي**؛ فقد يؤدي استخدام وسيلة واحدة إلى جمع بيانات تخص عدداً كبيراً من غير المرتبطين. وهنا ينبغي تقييم إمكان تضيق النطاق أو استخدام مرشحات قانونية وتقنية تقلل جمع البيانات غير اللازمة. [43]

ويتصل بذلك التناسب من حيث **نوع البيانات**؛ فليست جميع المعلومات متساوية في حساسيتها. وقد يكون جمع معلومة عامة عن نشاط تجاري أقل تدخلاً من جمع بيانات الموقع التفصيلية أو المراسلات الخاصة أو المعلومات الصحية. ولذلك، ينبغي ألا يقتصر التقييم على حجم البيانات، بل يشمل طبيعتها والنتائج التي يمكن استنتاجها. [44]

ومن الأخطاء المنهجية الشائعة **مساواة القدرة التقنية بالضرورة القانونية**؛ إذ قد تتمكن أداة من استخراج جميع محتويات جهاز أو ربط ملايين السجلات، لكن هذه القدرة لا تبرر استخدام كامل وظائفها في كل حالة. فالوسيلة يجب أن تُستخدم بالقدر الذي يخدم الغرض المشروع، لا بالقدر الذي تسمح به إمكاناتها الفنية. [45]

وتزداد أهمية ذلك عند استخدام أدوات **التعرف الآلي أو تحليل الأنماط أو تصنيف الأشخاص**. فقد تنتج هذه الأدوات مؤشرات واسعة النطاق، لكن استخدامها في توجيه التحري يتطلب تقييماً لمدى ملاءمتها للغرض، واحتمالات الخطأ والتحيز، وإمكان التحقق من النتائج. [46]

ويقتضي التناسب مراعاة **مخاطر التخزين بعد انتهاء الحاجة**. فكلما زادت مدة الاحتفاظ واتسعت دائرة الوصول، ارتفعت احتمالات الاستخدام غير المصرح به أو التسرب. ومن ثم، لا ينتهي تقييم التناسب بانتهاء الجمع، بل يمتد إلى الاحتفاظ والمعالجة والإفصاح والإتلاف. [47]

وعلى المستوى الإجرائي، يمكن تحويل الضرورة والتناسب إلى أسئلة يجب أن يجيب عنها القرار الأمني: ما الغرض المحدد؟ ما المعلومات اللازمة؟ لماذا اختيرت هذه الوسيلة؟ هل توجد وسيلة أقل تدخلاً؟ ما الأشخاص الذين قد تتأثر حقوقهم؟ ما مدة الإجراء؟ ما الضمانات المتخذة؟ متى ينبغي إنهاء الإجراء أو مراجعته؟ [48]

المطلب الثالث: القيود على الحصول على البيانات العامة والمقيدة والمحمية

يقتضي ضبط المشروعية تصنيف المعلومات بحسب طبيعة إتاحتها والقيود القانونية التي تحكم الوصول إليها. ولا يكفي تقسيم البيانات إلى عامة وخاصة؛ لأن هذا التقسيم يحجب اختلافات مهمة بين المنشورة للعموم، والمتاحة لفئة محددة، والمحمية بسرية قانونية. [49]

أولاً: البيانات المتاحة للعموم. تشمل المحتوى المنشور على المواقع المفتوحة، والسجلات العامة التي يسمح القانون بالاطلاع عليها. وقد يكون الوصول ممكناً دون إذن فردي، لكن ذلك لا يعني أن جميع أشكال جمعها وتحليلها مشروعة دون قيود. فالبيانات المنشورة قد تتضمن معلومات شخصية أو حساسة، وقد يؤدي تجميعها على نطاق واسع إلى كشف أنماط لم تكن ظاهرة. [50]

ويجب التمييز بين الاطلاع العابر على محتوى منشور وإنشاء سجل منظم يتتبع أنشطة شخص مدة طويلة، أو جمع معلومات منشورة عن آلاف الأشخاص وربطها بقواعد أخرى. فقد تختلف طبيعة التدخل اختلافاً جوهرياً بين الحالتين، حتى لو كانت البيانات الأصلية متاحة للجمهور. [51]

ثانياً: البيانات المقيدة أو المتاحة لفئة محددة. تشمل المعلومات التي يمكن الوصول إليها بواسطة حساب أو اشتراك أو صفة مهنية. وقد تكون متاحة لعدد كبير من المستخدمين، لكنها لا تكون منشورة للعموم بالمعنى القانوني. ويجب التحقق من شروط الوصول، وما إذا كانت الجهة تملك سنداً يسمح لها بالوصول. [52]

ولا ينبغي أن تُفهم الموافقة على شروط استخدام خدمة رقمية على أنها موافقة عامة على أي معالجة حكومية لاحقة. فالعلاقة بين المستخدم ومقدم الخدمة تختلف عن العلاقة بين الفرد والسلطة العامة. [53]

ثالثاً: البيانات المحمية أو الخاضعة لسرية قانونية. تشمل البيانات التي يحميها القانون بسبب طبيعتها أو العلاقة التي نشأت في إطارها، مثل محتوى الاتصالات الخاصة، وبعض المعلومات المالية أو الصحية، والبيانات المحمية بسرية مهنية. ويستلزم الوصول إليها سنداً قانونياً واستيفاء إجراءات الإذن متى كانت واجبة. [54]

وتؤكد اتفاقية بودابست أهمية توفير صلاحيات إجرائية ملائمة للحصول على الأدلة الإلكترونية، مع تنظيم التعاون بين الدول الأطراف. غير أن تطبيق هذه الصلاحيات يتوقف على نصوص الاتفاقية والتشريعات المنفذة لها والضمانات ذات الصلة. [10]

رابعاً: البيانات التي تخص أشخاصاً غير مستهدفين. قد يؤدي جمع البيانات إلى الحصول على معلومات عن أشخاص لا تتعلق بهم الشبهة. ولا يعني ظهور بياناتهم أنها أصبحت مباحة الاستخدام دون قيد. بل ينبغي تحديد مدى ارتباطها بالموضوع، وما إذا كان الاحتفاظ بها ضرورياً، وكيفية حماية المعلومات غير اللازمة. [55]

خامساً: أثر طريقة الحصول. لا يتحدد الحكم القانوني بطبيعة البيانات وحدها، بل بطريقة الحصول أيضاً. فقد يكون المحتوى متاحاً للعموم، لكن الحصول عليه من خلال انتحال صفة أو تجاوز وسائل الحماية قد يثير إشكالات مستقلة. ويتطلب التقييم النظر في أربعة عناصر: طبيعة البيانات، وشروط إتاحتها، والوسيلة المستخدمة، والغرض. [56]

المطلب الرابع: تقليل البيانات وضوابط الاحتفاظ بها

يمثل مبدأ **تقليل البيانات** أحد الضوابط الأساسية، ويقضي ألا يتجاوز جمع المعلومات ومعالجتها القدر الملائم والمرتبط والضروري لتحقيق الغرض المشروع. وتتبع أهميته من أن البيئة الرقمية تتيح تخزين كميات هائلة بتكلفة منخفضة، مما قد يؤدي إلى الاحتفاظ بمعلومات لا تخدم غرض التحري. [57]

ولا يقتصر تقليل البيانات على الحد من الكمية، بل يشمل نطاق المعالجة، وعدد الأشخاص الذين يستطيعون الوصول، والمدة، والجهات التي يمكن مشاركتها معها. فهو مبدأ يمتد إلى جميع مراحل التعامل. [58]

وقد أكدت اتفاقية ١٠٨ أهمية أن تكون البيانات ملائمة وذات صلة وغير مفرطة قياساً إلى الأغراض، إلى جانب مراعاة دقتها وتحديد مدة الاحتفاظ. [8] وتدعم هذه المبادئ فكرة أن جمع المعلومات يجب أن يكون محكوماً بالحاجة، لا بمجرد القدرة. [59]

أولاً: تقليل البيانات عند الجمع. يتطلب تحديد المعلومات اللازمة وتجنب جمع ما لا يُتوقع أن تكون له صلة معقولة. ولا يعني ذلك وجوب معرفة النتائج مسبقاً، بل أن يكون نطاق الجمع مبرراً في ضوء الغرض والظروف. [60]

ثانياً: تقليل البيانات أثناء التحليل. قد تكون بعض البيانات قد جُمعت بصورة مشروعة، لكن تحليلها على نحو موسع قد يؤدي إلى نتائج تتجاوز الغرض. ومن أمثلة ذلك ربط معلومات متفرقة لإنشاء ملف تفصيلي، أو إدخال بيانات غير مرتبطة في نموذج آلي ينتج تصنيفات. وفي هذه المرحلة، ينبغي تحديد نطاق البيانات المستخدمة وسبب الحاجة إلى الربط. [61]

ثالثاً: ضوابط الاستخدام في أغراض أخرى. قد تكشف التحريات عن معلومات تتعلق بواقعة مختلفة. ولا يترتب على ذلك حظر استخدامها، لكن ينبغي التحقق من توافق الاستخدام الجديد مع السند القانوني الأول. وقد يتطلب الاستخدام الجديد إذناً إضافياً أو قراراً مستقلاً أو إحالة. [62]

رابعاً: تبادل البيانات بين الجهات. يعد التبادل مهماً في القضايا التي تتطلب خبرات متعددة. غير أن فائدة التنسيق لا تبرر الإفصاح غير المقيد. ويقتضي التبادل تحديد الجهة المتلقية والغرض ونوع البيانات، والتحقق من اختصاص الجهة، وتحديد القيود التي تظل سارية بعد النقل، وتوثيق عملية الإفصاح. [63]

خامساً: الاحتفاظ بالبيانات. يجب ألا تتحول البيانات إلى سجلات دائمة دون أساس قانوني أو حاجة مستمرة. فالاحتفاظ المطول يزيد مخاطر التسرب أو الاستخدام غير المشروع. ويقتضي التنظيم تحديد مدد الاحتفاظ وفق طبيعة البيانات والغرض والالتزامات القانونية. [64]

ويجب التمييز بين البيانات الأصلية التي يلزم حفظها لضمان إمكان التحقق الفني، والنسخ المستخدمة في التحليل، والمعلومات التشغيلية التي لم تعد هناك حاجة إليها. فقد تستدعي سلامة الدليل حفظ نسخة أصلية موثقة، لكن ذلك لا يعني ضرورة الاحتفاظ بجميع البيانات غير المرتبطة إلى أجل غير محدد. [65]

سادساً: إتلاف البيانات أو إخفاء الهوية. عندما تنتهي الحاجة القانونية، ينبغي تطبيق قواعد الإتلاف أو الحذف أو إخفاء الهوية. ويجب تنفيذ ذلك بطريقة تمنع استمرار

الوصول غير المصرح به، مع توثيق الإجراء. ولا يجوز أن يؤدي الإلتفاف إلى المساس ببيانات يتعين حفظها قانوناً.[66]

أما إخفاء الهوية، فينبغي تقييمه وفق فعاليته الفعلية؛ إذ قد تبقى إمكانية إعادة التعرف قائمة عند ربط البيانات بمصادر أخرى. ولذلك، لا يكفي حذف الاسم المباشر إذا كانت بقية المعلومات تسمح بتحديد صاحبها.[67]

سابعاً: تنظيم الوصول. يتطلب تقليل البيانات تقييد الوصول بحسب الوظيفة والحاجة. ويشمل ذلك تنظيم صلاحيات المستخدمين، وتسجيل عمليات الوصول، ومراجعة الصلاحيات دورياً. كما ينبغي مراعاة أن الموظف الذي يملك صلاحية فنية للوصول لا يملك بالضرورة صلاحية استخدامها في كل مهمة.[68]

المبحث الثالث: الضوابط الحقوقية والإجرائية لمعالجة البيانات

المطلب الأول: حماية الخصوصية في البيئة الرقمية

تحتل الخصوصية موقعاً مركزياً في الإطار القانوني للتحريات الرقمية؛ لأن المعلومات الإلكترونية لا تقتصر على الوقائع التي يختار الفرد إعلانها، بل قد تكشف تفاصيل حياته وعلاقاته وتحركاته. وقد يؤدي تجميعها وتحليلها إلى استنتاجات تتجاوز ما يكشفه كل عنصر منفرد.[69]

وقد كفل العهد الدولي الحماية من التدخل التعسفي أو غير القانوني في الخصوصية والأسرة والمنزل والمراسلات.[5] وتكتسب هذه الحماية أهمية في البيئة الرقمية لأن الوسائل الحديثة توسع إمكانات الوصول والتخزين والربط والمراقبة.[70]

ولا ينبغي تفسير الخصوصية تفسيراً ضيقاً يحصرها في سرية المراسلات أو حرمة المسكن. فالبيانات المتعلقة بالموقع والاتصالات والأنشطة الرقمية قد تكشف أنماطاً من الحياة الخاصة حتى إذا لم تتضمن مضموناً اتصالياً مباشراً. وقد تسمح سجلات التحرك المتكررة باستنتاج أماكن العمل أو الزيارات أو العلاقات.[71]

ومن ثم، لا يتوقف تقدير التدخل على ما إذا كانت الجهة اطلعت على محتوى اتصال أم على بيانات وصفية؛ بل يتعين النظر إلى طبيعة البيانات وقدرتها على كشف معلومات عن الفرد، وطريقة جمعها، وحجمها، ومدة الاحتفاظ، وإمكان ربطها بمصادر أخرى.[72]

كما أن نشر الشخص بعض المعلومات عن نفسه لا يؤدي بالضرورة إلى فقدانه الحماية في جميع السياقات. فالمعلومات التي ينشرها الفرد لجمهور محدد قد تُجمع لاحقاً وتُحلل بطريقة تغير أثرها العملي.[73]

ويجب التمييز بين الخصوصية كحق أساسي وحماية البيانات الشخصية كإطار ينظم المعالجة. فالحق في الخصوصية أوسع من مجرد التحكم في البيانات، بينما توفر قواعد حماية البيانات أدوات إجرائية للحد من المعالجة غير المشروعة.[74]

وقد أسهمت اتفاقية ١٠٨ في إرساء إطار دولي لحماية الأفراد من المخاطر الناشئة عن المعالجة الآلية، بما يشمل مشروعية الجمع وتحديد الأغراض وجودة البيانات وسريتها وحقوق الأفراد في الوصول والتصحيح. [8] وتؤكد هذه المبادئ أن الحماية لا تتحقق بمجرد منع الوصول إلى المعلومات السرية، بل تتطلب تنظيم دورة حياة البيانات بأكملها. [75]

ولا تعني حماية الخصوصية حظر جميع أشكال التحري الرقمي؛ إذ قد تكون للسلطات أسباب مشروعة. لكن وجود هذه الأهداف لا يلغي ضرورة احترام الحقوق. ويقتضي التوازن أن يكون التدخل مستنداً إلى القانون، وموجهاً إلى غرض مشروع، وضرورياً ومتناسباً، وخاضعاً للضمانات. [76]

وتتوقف درجة الحماية الإجرائية على طبيعة التدخل. فجمع معلومة منشورة يختلف عن اعتراض محتوى الاتصالات، وتسجيل واقعة عابرة يختلف عن تتبع شخص بصورة مستمرة. وكلما ازدادت قدرة الوسيلة على إنشاء سجل تفصيلي للحياة الخاصة، ازدادت أهمية تحديد نطاقها ومدتها. [77]

وقد أكدت المحكمة الأوروبية لحقوق الإنسان، في قضية *Szabó and Vissy* ضد المجر (2016)، أن التشريعات التي تجيز المراقبة السرية الواسعة يجب أن تتضمن ضمانات كافية ضد سوء الاستخدام، وأن تكون محددة النطاق والغرض والمدة. كما أكدت في قضية *Big Brother Watch* ضد المملكة المتحدة (2021) أن أنظمة المراقبة الجماعية تحتاج إلى ضمانات مستقلة وفعالة. [78]

وتبرز أهمية الحماية عند استخدام تقنيات تحليل الصور والتعرف الآلي وربط قواعد البيانات. فقد تُستخدم لاستخلاص معلومات عن أشخاص لم يكونوا مستهدفين، أو لإنتاج استنتاجات عن علاقاتهم. ولذلك، ينبغي تقييم الآثار الحقوقية للنتائج المستخلصة، لا الاكتفاء بفحص مشروعية الحصول على البيانات الأولية. [79]

كما تتطلب الحماية مراعاة الأمن المعلوماتي للبيانات التي تجمعها الجهات. فحتى إذا كان الجمع مشروعاً، فإن تخزين المعلومات في أنظمة ضعيفة الحماية قد يؤدي إلى انتهاك جديد. ولذلك، فإن مسؤولية الجهة لا تنتهي عند الحصول على البيانات، بل تشمل اتخاذ التدابير لحمايتها من الفقد أو التغيير أو الإفصاح. [80]

المطلب الثاني: الضوابط القانونية لمعالجة البيانات الشخصية والحساسة

تتطلب التحريات الرقمية عناية خاصة بالبيانات الشخصية؛ لأنها قد ترتبط مباشرة بفرد أو تسمح بالتعرف عليه بصورة غير مباشرة. ولا تتوقف صفة البيانات الشخصية على ظهور الاسم؛ فقد تكون المعلومة معرفاً تقنياً أو سجل موقع أو مجموعة خصائص تسمح بتحديد الشخص عند ربطها بمعلومات أخرى. [81]

وتكتسب البيانات الحساسة أهمية إضافية بسبب طبيعتها أو ما قد يترتب على كشفها من أضرار. وقد تشمل، بحسب النظام القانوني، بيانات تتعلق بالصحة أو المعتقدات أو

الحياة الخاصة أو الخصائص البيومترية. ومن الأمثلة المقارنة: المادة ٩ من اللائحة الأوروبية العامة لحماية البيانات (GDPR) التي تحظر معالجة هذه الفئات إلا في حالات محددة، وقانون حماية البيانات الشخصية البحريني (٢٠١٨) الذي يفرض ضمانات مشددة على البيانات الحساسة. [82]

ولا توجد قائمة عالمية واحدة ملزمة تحدد جميع أنواع البيانات الحساسة؛ لذلك يجب الرجوع إلى التشريع المنطبق. وقد أكدت اتفاقية ١٠٨ ضرورة وضع ضمانات ملائمة لمعالجة البيانات التي تكشف معلومات شديدة الحساسية. [8]

أولاً: مشروعية المعالجة. تتطلب معالجة البيانات الشخصية وجود أساس قانوني، مع مراعاة طبيعة الجهة والغرض والحقوق. وفي العمل الأمني، قد يستند الأساس إلى اختصاص مقرر أو سلطة خاصة للتحري. ولا يجوز افتراض أن موافقة الفرد هي الأساس الوحيد، كما لا يجوز اعتبار الوظيفة الأمنية أساساً مطلقاً. [83]

ثانياً: تحديد الغرض والارتباط به. يجب أن تكون البيانات ذات صلة بالغرض المشروع، وألا تتحول المعالجة إلى استكشاف مفتوح. ويقتضي ذلك تحديد العلاقة بين كل فئة والهدف، خصوصاً عند تضمن معلومات حساسة أو تفاصيل عن غير مستهدفين. [84]

ثالثاً: دقة البيانات وتحديثها. قد يؤدي الاعتماد على معلومات غير دقيقة إلى توجيه التحري نحو شخص غير معني. وتزداد المخاطر في البيئة الرقمية بسبب إعادة النشر خارج السياق أو استمرار ظهور سجلات قديمة. ولذلك، ينبغي التحقق من الدقة والتمييز بين الوقائع المؤكدة والمعلومات الأولية وغير المتحقق منها. [85]

رابعاً: السرية وأمن المعالجة. تقتضي المعالجة اتخاذ تدابير لحماية البيانات من الوصول غير المصرح به أو التعديل أو الفقد. ويشمل ذلك ضبط الصلاحيات، وتوثيق عمليات الوصول، وتطبيق وسائل الحماية التقنية والتنظيمية. [86]

خامساً: حماية البيانات الحساسة. تستلزم تقييماً أشد للمخاطر؛ لأن الإفصاح أو التفسير غير الدقيق قد يؤدي إلى آثار خطيرة. وقد يكون من الضروري تقييد الوصول أو فصلها عن البيانات العامة أو وضع شروط إضافية. كما ينبغي تجنب الاستنتاجات غير المدعومة التي تربط الشخص بصفة حساسة استناداً إلى مؤشرات غير مباشرة. [87]

سادساً: حقوق الأفراد. قد يقرر القانون حقوقاً تتعلق بالاطلاع أو التصحيح أو الاعتراض أو المحو، مع إمكان تقييدها في حالات محددة. ولا يعني وجود استثناءات أمنية استبعاد جميع الضمانات؛ فقد يقتضي القانون توفير مراجعة مستقلة أو مسار للتظلم أو إمكان تصحيح البيانات غير الدقيقة. [88]

سابعاً: البيانات المستمدة من مصادر مفتوحة. لا تخرج البيانات المنشورة للعموم تلقائياً من نطاق الحماية. فقد يكون الاطلاع على منشور جائزاً، لكن جمع منشورات

شخص على مدى طويل وربطها بمعلومات أخرى وإنشاء ملف تحليلي يمثل معالجة أوسع تحتاج إلى تقييم مستقل.[89]

ثامناً: المسؤولية طوال دورة الحياة. لا تنتهي مسؤولية الجهة بانتهاء التحري الأولي، بل تستمر خلال التحليل والتخزين والتبادل. فإذا انتفى الغرض، وجب النظر في الإلتلاف أو الحذف أو إخفاء الهوية، ما لم يوجد التزام قانوني مستقل.[90]

المطلب الثالث: حماية بيانات الأشخاص غير المستهدفين

تُعد حماية بيانات غير المستهدفين من المسائل الدقيقة؛ لأن الوسائل المستخدمة قد تجمع معلومات عن أفراد يتجاوزون نطاق التحري المباشر. وقد يحدث ذلك عند مراجعة تسجيلات كاميرات المراقبة، أو تحليل بيانات الاتصالات، أو فحص جهاز يحتوي على مراسلات متعددة الأطراف.[91]

وتنشأ الإشكالية عندما تتداخل البيانات المرتبطة بالواقعة مع بيانات أشخاص لا توجد بشأنهم شبهة. فظهور بيانات الشخص عرضاً لا يساوي ثبوت صلته بالواقعة، كما لا يمنح الجهة صلاحية مطلقة للاحتفاظ بها.[92]

ويقتضي تحديد الضمانات التمييز بين ثلاث فئات:

١. **المستهدفون مباشرة:** تتعلق بهم المسألة في حدود الأساس القانوني.
 ٢. **الذين تظهر بياناتهم بسبب ارتباطهم بالواقعة:** كالأطراف الذين ترد أسماؤهم في مراسلات ذات صلة.
 ٣. **الذين تظهر بياناتهم عرضاً دون ارتباط جوهري:** كمن يظهر في خلفية تسجيل.[93]
- ولا يعني التصنيف أن لكل فئة حكماً موحداً؛ إذ يتوقف الحكم على طبيعة البيانات والوسيلة والقانون. لكنه يساعد على تحديد درجة الصلة وتقييم الحاجة إلى الاحتفاظ.[94]
- وتتجلى الأهمية في أن البيانات العرضية قد تكون شديدة الحساسية رغم عدم ارتباطها بالواقعة. فإذا لم تُحدد قواعد واضحة، فقد يتسع نطاق التدخل إلى الحياة الخاصة لأشخاص لم يكن هناك مبرر لاستهدافهم.[95]
- ويُستفاد من مبدأ تقليل البيانات أن المعالجة يجب أن تقتصر على القدر الملائم والمرتبط والضروري.[57] وتؤكد الأطر الدولية أهمية مراعاة الغرض وجودة المعلومات والسرية وعدم الاحتفاظ مدة تتجاوز الحاجة.[8]
- أولاً: تحديد نطاق الوصول قبل الفحص.** ينبغي تحديد نطاق البيانات اللازمة قبل بدء الفحص. فإذا كان الإجراء يتعلق بمراسلات خلال فترة معينة، وجب تجنب توسيع الفحص إلى بيانات غير مرتبطة ما لم يوجد مبرر.[96]

ثانياً: الفصل بين البيانات المرتبطة وغير المرتبطة. قد يكون من الملائم فصل البيانات ذات الصلة عن الأخرى، من خلال تحديد الملفات أو الفترات أو السجلات المعنية، أو استخدام وسائل فنية تقلل ظهور البيانات غير اللازمة.[97]

ثالثاً: تقييد استخدام البيانات العرضية. إذا ظهرت معلومات تخص غير مستهدف، فلا ينبغي تحويل ظهورها إلى مبرر تلقائي لفتح تحريٍّ مستقل. بل يجب تقييم الصلة والتحقق من وجود أساس قانوني.[98]

رابعاً: ضبط صلاحيات الاطلاع. ينبغي أن يقتصر الوصول إلى البيانات العرضية على من تستدعي مهامهم ذلك. ولا يجوز أن يؤدي وجود المعلومات في قاعدة أمنية إلى إتاحتها لجميع العاملين.[99]

خامساً: الاحتفاظ والإتلاف. إذا تبين أن البيانات لا ترتبط بالموضوع ولا توجد ضرورة قانونية، فينبغي تطبيق قواعد الحذف أو الإتلاف أو العزل. ولا ينبغي أن تتحول عبارة "قد تكون مفيدة مستقبلاً" إلى أساس عام للاحتفاظ.[100]

سادساً: حماية بيانات الغير عند مشاركة النتائج. قد تتضمن التقارير أسماء أو صوراً لأشخاص لا صلة مباشرة لهم. وينبغي أن يقتصر الإفصاح على المعلومات الضرورية، مع مراعاة متطلبات القانون وحقوق الأطراف.[101]

سابعاً: التوثيق والمراجعة. يجب أن يكون بالإمكان تحديد كيفية التعامل مع البيانات العرضية، وما إذا جرى الاحتفاظ بها أو استبعادها. وتزداد الأهمية عندما تكون البيانات حساسة أو قد تؤثر في قرارات تتعلق بأشخاص لم يكونوا مستهدفين.[102]

المطلب الرابع: مشاركة البيانات وإتلافها

تتصل المشروعات بجميع المراحل، ولا تنتهي بمجرد الحصول على المعلومات. فالبيانات التي جُمعت بصورة مشروعة قد تتحول إلى مصدر لانتهاك الخصوصية إذا احتُفظ بها دون حاجة، أو نُقلت إلى جهة غير مخولة.[103]

أولاً: الأساس القانوني للاحتفاظ. يقتضي الاحتفاظ تحديد الغرض، مثل استكمال التحري أو توثيق إجراء أو دعم دعوى أو تنفيذ التزام قانوني. ويجب التمييز بين البيانات اللازمة لإثبات سلامة الإجراء والبيانات التي لم تعد لها صلة.[104]

وقد أكدت مبادئ اتفاقية ١٠٨ ضرورة ألا تُحفظ البيانات مدة تتجاوز ما تقتضيه الأغراض، مع مراعاة الأحكام المنطبقة.[8] ويقتضي تطبيق ذلك وضع قواعد توازن بين المحافظة على المعلومات والحد من مخاطر استمرار حيازتها.[105]

ثانياً: التمييز بين الحفظ التشغيلي وحفظ الإثبات. قد تحتفظ الجهة بالبيانات لتسيير أعمالها، أو لأغراض إثبات سلامة إجراء أو المحافظة على دليل. ويختلف الغرضان

من حيث متطلبات الحفظ وإمكان التعديل وضرورة المحافظة على النسخ الأصلية. [106]

ثالثاً: تنظيم الوصول خلال مدة الاحتفاظ. يتعين أن تظل البيانات خاضعة لضوابط الوصول حتى بعد انتهاء المرحلة النشطة. فوجود المعلومات في أرشيف لا يبرر إتاحتها لجميع العاملين. [107]

رابعاً: مشاركة البيانات بين الجهات. يجب أن تستند المشاركة إلى أساس قانوني، وأن تكون محددة الغرض والنطاق. ويقتضي ذلك التحقق من اختصاص الجهة المتلقية، وتحديد البيانات اللازمة، ومراعاة القيود، وتوثيق النقل. [108]

خامساً: التبادل عبر الحدود. تثير المشاركة عبر الحدود مسائل تتعلق بالاختصاص ومستوى الحماية في الدولة المتلقية وشروط التعاون. وتوفر اتفاقية بودابست وبروتوكولها الإضافي الثاني (٢٠٢٢) آليات للتعاون في الحصول على الأدلة الإلكترونية، مع مراعاة شروطها ونطاق تطبيقهما. [10] كما ينبغي مراعاة قواعد حماية البيانات عند نقل المعلومات إلى جهة أجنبية. [109]

سادساً: الإتلاف. يمثل الإتلاف المرحلة التي تنتهي فيها الحاجة القانونية، ويجب أن يجري وفق قواعد تضمن عدم بقاء نسخ غير لازمة. ولا يعني الإتلاف محو كل أثر توثيقي؛ فقد يكون من اللازم الاحتفاظ بسجل يثبت أن البيانات أُلغيت في تاريخ معين. [110]

سابعاً: أثر تغير الغرض أو زوال الحاجة. قد تتغير الظروف؛ فقد تُستكمل المهمة أو تنتقل المسألة إلى جهة قضائية. ويقتضي ذلك مراجعة الغرض وتحديد ما إذا كان لا يزال قائماً. [111]

ثامناً: المساءلة. قد يؤدي الاحتفاظ غير المبرر أو الإفصاح غير المصرح به إلى مسؤوليات قانونية تختلف بحسب التشريع وطبيعة المخالفة. وتتطلب المساءلة وجود سجلات واضحة تبين مصدر البيانات وأساس الاحتفاظ والجهات التي تلقتها والتغييرات التي طرأت عليها. [112]

المبحث الرابع: الرقابة والمسؤولية عن تجاوزات التحري

المطلب الأول: الرقابة القضائية

تُعد الرقابة القضائية ضماناً أساسية لمشروعية التحريات الرقمية، ولا سيما عندما تتضمن تدخلاً في الخصوصية أو الوصول إلى بيانات محمية. وتستهدف ضمان ألا تتحول السلطات إلى صلاحيات غير محدودة، من خلال إخضاع الإجراءات لمراجعة جهة قضائية مستقلة. [113]

ولا تتخذ الرقابة صورة واحدة؛ فقد تكون **سابقة** (إذن)، أو **أثناء التنفيذ**، أو **لاحقة** (مراجعة مشروعية الإجراء وآثاره). كما قد تختص المحكمة بالنظر في مشروعية الدليل أو طلبات التعويض أو الطعون. [114]

ولا يجوز افتراض أن كل إجراء يحتاج إلى إذن قضائي مسبق؛ إذ يتوقف ذلك على التشريع وطبيعة التدخل. غير أن الإجراءات التي تتطلب إذنًا يجب ألا تُنفذ بدونه، كما ينبغي أن تخضع الأخرى للضمانات والرقابة المقررة. [115]

وتستمد الرقابة أهميتها من **الفصل بين الجهة التي تسعى للحصول على المعلومات والجهة التي تراجع المشروعية**. فحين تكون الجهة القائمة بالتحري هي صاحبة القرار والتنفيذ والتقييم دون رقابة مستقلة، تزداد احتمالات التوسع في تفسير صلاحياتها. [116]

وقد أكدت تقارير مفوضية الأمم المتحدة أهمية الإذن والرقابة المستقلين على إجراءات المراقبة، وضرورة امتلاك جهات الرقابة صلاحيات وخبرات كافية. [6] وتبرز قيمة ذلك في الإجراءات الرقمية التي قد يصعب على الأفراد اكتشافها أو الاعتراض عليها أثناء تنفيذها. [117]

وتتطلب الرقابة الفعالة توافر معلومات كافية عن الإجراء المقترح. فلا يمكن تقييم الضرورة والتناسب إذا اقتصر الطلب على عبارات عامة. كما أن الإذن الذي لا يحدد حدوداً قابلة للمراجعة قد يصعب التحقق من الالتزام به. [118]

ولا تنتهي الرقابة بمجرد صدور الإذن؛ إذ ينبغي التحقق من التزام التنفيذ بحدوده. وقد يتطلب ذلك مراجعة سجلات التنفيذ والمدة الفعلية والبيانات التي جُمعت وأي توسع. [119]

كما تبرز أهمية الرقابة عند تقييم النتائج. فقد تكون المعلومات صحيحة فنيًا، لكن الحصول عليها تم بالمخالفة. وفي هذه الحالة، يتعين الفصل بين سلامة البيانات ومشروعية الإجراء، ثم تحديد الأثر القانوني. [120]

ولا يعني ذلك أن كل مخالفة تؤدي تلقائيًا إلى استبعاد المعلومات؛ إذ تختلف الأنظمة في معالجة الأدلة المتحصلة من إجراءات غير مشروعة. لكن الرقابة يجب أن تكون قادرة على فحص هذه المسائل بصورة مستقلة. [121]

وتتطلب فعالية الرقابة توافر **الخبرة الفنية المناسبة**. فالفصل في المسائل المتعلقة بالبيانات الرقمية قد يستلزم فهمًا لطبيعة السجلات والبيانات الوصفية وآليات الاستخراج. ولا يعني ذلك أن القاضي يحل محل الخبير، بل ينبغي أن يكون قادرًا على تقييم كفاية التقرير الفني وتمييز النتائج المدعومة عن الاستنتاجات. [122]

المطلب الثاني: الرقابة الإدارية والمؤسسية

لا تقتصر الضمانات على الرقابة القضائية؛ إذ تؤدي الرقابة الإدارية دوراً في منع المخالفات واكتشافها. وتنبع أهميتها من أن كثيراً من القرارات اليومية تتخذ داخل المؤسسات الأمنية، حيث يمكن للإجراءات التنظيمية أن تحد من التجاوزات.[123]

وتبدأ الرقابة بوضع قواعد مكتوبة تحدد إجراءات التحري الرقمي، والجهات المخولة بالموافقة والتنفيذ والمراجعة، والضوابط التي تحكم الوصول. وينبغي أن تكون متسقة مع القانون، وألا تنشئ صلاحيات جديدة.[124]

أولاً: الرقابة على صلاحيات الوصول. ينبغي اعتماد نظام يربط الصلاحيات بالمهام والحاجة الفعلية، مع مراجعة دورية وإلغاء عند زوال الحاجة، وتوثيق التعديلات. كما يجب أن تكون عمليات الوصول إلى البيانات الحساسة قابلة للتتبع.[125]

ثانياً: المراجعة الداخلية. تقتضي مراجعة الالتزام بالضوابط، بما يشمل التحقق من وجود الإذن، ومطابقة التنفيذ لنطاقه، وسلامة التوثيق. وينبغي ألا تقتصر على اكتمال النماذج، بل تتناول جودة القرار ومدى اتساق الوسيلة مع الحاجة.[126]

ثالثاً: استقلال وظائف المراجعة. تزداد الفعالية عندما تكون الجهة المكلفة قادرة على الفحص دون تضارب جوهري في المصالح. ولا يقتضي ذلك إنشاء جهاز مستقل لكل وظيفة؛ فقد تتحقق من خلال وحدة امتثال أو تدقيق داخلي أو مسؤول حماية بيانات.[127]

رابعاً: التدريب وبناء ثقافة الامتثال. لا تتحقق الرقابة بالقواعد وحدها؛ إذ يتوقف نجاحها على فهم الموظفين للحدود. وقد تنشأ المخالفات بسبب الاعتقاد الخاطئ بأن البيانات المنشورة مباحة دائماً، أو أن الصلاحية التقنية تعني جواز الاستخدام.[128]

خامساً: إدارة الحوادث والمخالفات. ينبغي أن تتوافر آلية للإبلاغ عن الحوادث التي تمس سلامة البيانات أو مشروعيتها، مع تحديد المسؤوليات عن الاستجابة وتوثيق الواقعة وتقييم الأثر واتخاذ التدابير.[129]

سادساً: مؤشرات الأداء. يمكن تعزيز الرقابة بمؤشرات تقيس الالتزام، مثل اكتمال توثيق الأدونات ونسبة مراجعة الصلاحيات. غير أن المؤشرات الكمية لا ينبغي أن تتحول إلى غاية مستقلة.[130]

سابعاً: التوثيق والمراجعة اللاحقة. يُعد التوثيق أساساً للرقابة؛ لأنه يسمح بإعادة بناء مسار الإجراء. ومع ذلك، يجب التمييز بين وجود سجل وبين ثبوت صحته أو مشروعيته.[131]

المطلب الثالث: التظلم والشكاوى والمراجعة اللاحقة

تمثل آليات التظلم والشكاوى ضمانات مهمة لمواجهة الأضرار، خاصة عندما يتعذر على الشخص معرفة تفاصيل الإجراء أثناء تنفيذه. وقد تكون بعض العمليات سرية

بطبيعتها، لكن السرية لا ينبغي أن تؤدي إلى استبعاد كل سبيل لمراجعة المشروعية. [132]

ويجب التمييز بين ثلاثة مسارات: **التظلم** من قرار أو إجراء، و**الشكوى** بشأن مخالفة قانونية، و**المراجعة اللاحقة** التي تجريها جهة مختصة. وقد تتداخل، لكن لكل منها وظيفة. [133]

ولا توجد قاعدة دولية واحدة تحدد شكلاً موحداً لهذه الآليات؛ إذ تختلف النظم. ومع ذلك، فإن وجود سبيل فعال للمراجعة يعد عنصراً في الحماية العملية. [134]

وقد أكدت تقارير مفوضية الأمم المتحدة أهمية الرقابة المستقلة والشفافية المناسبة ووجود سبل للمراجعة أو الطعن في القرارات المرتبطة بالمراقبة الرقمية. [6]

أولاً: الحق في تقديم الشكوى. ينبغي أن تتوفر آلية تسمح للأفراد بتقديم شكوى بشأن جمع بياناتهم أو استخدامها بصورة غير مشروعة. ويجب أن تكون قابلة للوصول ومحددة الإجراءات، وأن تتوفر ضمانات تمنع الانتقام. [135]

ثانياً: التظلم من القرارات المبنية على بيانات رقمية. قد يتأثر الشخص بقرار استند إلى معلومات غير دقيقة أو جرى تفسيرها خارج سياقها. وينبغي أن يتيح القانون سبيلاً لمراجعة القرار أو الاعتراض عليه. [136]

ثالثاً: مراجعة مشروعية الإجراء. قد تستهدف الشكوى التحقق من الأساس القانوني أو وجود الإذن أو الالتزام بنطاقه. ويجب أن تُجرى بواسطة جهة تملك الاختصاص والصلاحيات اللازمة. [137]

رابعاً: حدود السرية. قد يؤدي الإفصاح الكامل إلى الإضرار بتحقيق قائم. ولذلك، قد يجيز القانون تقييد بعض المعلومات. لكن السرية لا ينبغي أن تستخدم ذريعة لرفض المراجعة بصورة مطلقة. [138]

خامساً: تصحيح البيانات غير الدقيقة. قد تكشف المراجعة خطأ في الهوية أو التوقيت أو نسبة المحتوى. وينبغي اتخاذ التدابير لتصحيح السجل أو تقييد استخدامه أو إضافة توضيح. [139]

سادساً: التدابير التصحيحية والمساءلة. إذا أثبتت المراجعة وقوع مخالفة، فقد تشمل التدابير وقف المعالجة غير المشروعة أو حذف البيانات أو تقييد الوصول أو إحالة الواقعة للمساءلة. [140]

سابعاً: المراجعة اللاحقة كضمانة مؤسسية. قد تُجرى بصورة دورية أو بناءً على مؤشرات مخاطر، حتى في غياب شكوى. وتسمح بتقييم أنماط الاستخدام والالتزام بالحدود. [141]

المطلب الرابع: المسؤولية المترتبة على مخالفة الضوابط

تترتب على مخالفة الضوابط آثار قد تتجاوز تصحيح الإجراء؛ فقد تنشأ مسؤولية على الجهة أو الموظف بحسب طبيعة المخالفة. وتستهدف المسؤولية ضمان خضوع السلطة للقانون وردع التجاوزات وجبر الأضرار.[142]

ولا يمكن تقرير نظام موحد؛ إذ تختلف شروط المسؤولية الجنائية والتأديبية والمدنية من دولة إلى أخرى. كما تختلف الآثار المترتبة على مخالفة شرط الإذن عن الآثار الناتجة عن الإهمال في حفظ البيانات.[143]

أولاً: المسؤولية الجنائية. قد تنشأ عندما يشكل السلوك جريمة، مثل الوصول غير المصرح به إلى نظام أو بيانات، أو إفشاء معلومات يحميها القانون، أو إساءة استعمال السلطة، أو إتلاف البيانات عمداً. غير أن مجرد وقوع مخالفة إجرائية لا يعني بالضرورة تحقق جريمة؛ إذ يتطلب الأمر توافر الأركان.[144]

ثانياً: المسؤولية التأديبية والإدارية. قد تنشأ عندما يخالف الموظف القواعد المهنية أو التعليمات، حتى إذا لم يصل الفعل إلى جريمة. وتخضع الجزاءات لشروط وإجراءات يحددها النظام، بما في ذلك ضمانات التحقيق.[145]

ثالثاً: المسؤولية المدنية والتعويض. قد يؤدي الجمع غير المشروع أو الإفصاح إلى مساس بحقوق الفرد، بما قد يثير حقاً في التعويض وفق شروط القانون. ويتوقف ذلك على طبيعة الفعل والضرر وعلاقة السببية.[146]

رابعاً: أثر المخالفة في مشروعية الإجراء. قد تؤدي مخالفة قواعد الاختصاص أو الإذن إلى اعتبار الإجراء غير مشروع. لكن تحديد الأثر يتطلب فحص طبيعة المخالفة والضمانة المنتهكة والقاعدة الإجرائية.[147]

خامساً: أثر المخالفة في المعلومات والأدلة. يجب التمييز بين عدم مشروعية الحصول وبين عدم سلامة البيانات فنياً. فالمخالفة القانونية تستلزم تقييماً في ضوء قواعد المشروعية، بينما يستلزم الخلل الفني تقييماً لمدى إمكان الوثوق بالبيانات.[148]

سادساً: المسؤولية عن التوسع في نطاق الإذن. قد يصدر إذن صحيح، لكن التنفيذ يتجاوز حدوده. وفي هذه الحالة، لا يكفي وجود الإذن لإضفاء المشروعية على جميع الأعمال؛ بل يجب تحديد الجزء الذي شمله والجزء الذي تجاوزه.[149]

سابعاً: المسؤولية عن الإهمال الفني. قد تنشأ عندما يؤدي الإهمال إلى فقد البيانات أو تغييرها أو تعريضها للتسرب، أو عندما يُعد تقرير فني يتضمن استنتاجات غير مدعومة.[150]

ثامناً: المسؤولية عن الاستخدام في غير الغرض. قد تُجمع البيانات لغرض ثم تُستخدم لغرض لا يجيزه القانون. ويقتضي التقييم التحقق من أساس الاستخدام ونطاق الصلاحية والقيود.[151]

تاسعاً: أثر المسؤولية في تطوير الممارسة. لا ينبغي أن يقتصر الأثر على توقيع الجزاء؛ بل يجب الاستفادة من النتائج لتحديد أوجه القصور ومعالجتها. وينبغي أن ترتبط المساءلة بإجراءات تصحيحية تتناسب مع طبيعة الخلل.[152]

الجدول المقارن: مستويات التدخل والضمانات المطلوبة

مستوى التدخل	أمثلة	مدة الاحتفاظ	الضمانات الأساسية	السند القانوني المطلوب
تدخل منخفض	الاطلاع على معلومات منشورة للعموم	قصيرة	توثيق المصدر، التحقق من السياق، تقليل الجمع المنظم	اختصاص عام + غرض مشروع
تدخل متوسط	الوصول إلى بيانات مقيدة (حساب خاص، سجل تجاري)	محددة	تحديد النطاق، الإذن المختص، تقييد الاستخدام	سند قانوني خاص أو تصريح إداري
تدخل مرتفع	الوصول إلى بيانات الاتصالات، تفتيش جهاز	محددة وقابلة للمراجعة	تسبب الإذن، تحديد النطاق والمدة، الرقابة اللاحقة	إذن قضائي مسبق (حيث يشترطه القانون)
تدخل شديد	اعتراض محتوى الاتصالات، المراقبة المستمرة	قصيرة وقابلة للتمديد المراقب	مراجعة دورية، إشعار لاحق (حيث يسمح القانون)، رقابة مستقلة	إذن قضائي + ضمانات استقلال

❖ النافذة التطبيقية

السيناريو: تلقت جهة أمنية بلاغاً عن حساب إلكتروني يروج لمحتوى يمس الأمن العام.

١. **الخطوة الأولى (تدخل منخفض):** التحقق من المحتوى المنشور للعموم. هذا لا يحتاج إذناً قضائياً، لكنه يحتاج توثيق المصدر والتحقق من السياق.

٢. **الخطوة الثانية (تدخل متوسط):** ملاحظة تزامن بين النشر وموقع جغرافي معين. هذا قرينة تحليلية تحتاج تحققاً، لا دليلاً.

٣. **الخطوة الثالثة (تدخل مرتفع):** طلب بيانات من مزود الخدمة. هذا يتطلب سنداً قانونياً (إذن قضائي أو تصريح مختص)، وتحديد النطاق والمدة.

٤. **الخطوة الرابعة (تدخل شديد):** إذا استدعى الأمر اعتراض محتوى الاتصالات، فيتطلب إذناً قضائياً مع تسبب، ومراجعة دورية.

الدرس: لا يجوز الانتقال من مستوى إلى آخر دون التحقق من السند القانوني والضمانات. ولا يجوز اعتبار التزام دليلاً على الفاعلية دون استبعاد الفرضيات البديلة.

النتائج العامة للفصل

١. التحريات الأمنية الرقمية تتطلب أساساً تشريعياً يجمع بين اختصاص محدد وسند مناسب وضمانات.
٢. مشروعية الغرض الأمني لا تستلزم مشروعية كل وسيلة.
٣. الاختصاص يتوزع بين المبادرة والإذن والتنفيذ والتقييم، ولا يجوز الخلط بينها.
٤. الإذن القضائي ضماناً جوهرياً في الإجراءات الشديدة التدخل، وتتحدد فعاليته بوضوح نطاقه وتسببيه.
٥. مبدأ المشروعية يشمل السلطة والوسيلة والغرض والمعالجة.
٦. الضرورة والتناسب يحددان اختيار الوسيلة ونطاقها ومدتها.
٧. البيانات تصنف إلى عامة ومقيدة ومحمية، ولكل فئة ضوابط وصول مختلفة.
٨. تقليل البيانات مبدأ يمتد إلى الجمع والتحليل والاحتفاظ والتبادل.
٩. حماية الخصوصية تتطلب تنظيم دورة حياة البيانات، لا مجرد منع الوصول.
١٠. البيانات الشخصية والحساسة تستلزم ضمانات مشددة، والبيانات غير المستهدفة تستلزم تدابير خاصة.
١١. الاحتفاظ والتبادل والإتلاف مراحل قانونية مستقلة تحتاج ضوابط.
١٢. الرقابة القضائية والإدارية والتظلم والمساءلة تشكل منظومة متكاملة.
١٣. المسؤولية متعددة المستويات (جنائية، تأديبية، مدنية)، ويجب التمييز بين المخالفة القانونية والخلل الفني.

المراجع:

- (1) انظر: عادل عبد العال خراشي، ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي، ٢٠٠٦، ص ٤٥ وما بعدها.
- (2) انظر: هشام مصطفى محمد، التحريات الأمنية وأثرها في الأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٥، ص ١٨-٢٢.
- (3) انظر: محمد محمد سيف شجاع، شرح قانون الإجراءات الجزائية اليمني، مكتبة الصادق، صنعاء، ٢٠٠٥، الفصل الخاص بالتحريات والاستدلالات.
- (4) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، الوثيقة A/HRC/51/17، ٤ أغسطس ٢٠٢٢، الفقرات ٢٠-٢٥.
- (5) انظر: الأمم المتحدة، العهد الدولي الخاص بالحقوق المدنية والسياسية، ١٩٦٦، المادة ١٧؛ ولجنة حقوق الإنسان، التعليق العام رقم ١٦، ٨ أبريل ١٩٨٨، الوثيقة CCPR/C/21/Rev.1، الفقرة ٨.
- (6) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرات ٣٠-٤٥.
- (7) انظر: محمد محمد سيف شجاع، المرجع السابق؛ وعادل عبد العال خراشي، المرجع السابق، ص ٦٠-٦٥.

- (8) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١؛ والاتفاقية الحديثة(108+) ، CETS No. 223، ٢٠١٨.
- (9) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Rev. 1, 2014, pp. 1–3.
- (10) انظر: مجلس أوروبا، اتفاقية الجريمة المعلوماتية، ETS No. 185، بودابست، ٢٠٠١؛ والبروتوكول الإضافي الثاني، CETS No. 224، ٢٠٢٢.
- (11) انظر: محمد محمد سيف شجاع، المرجع السابق.
- (12) انظر: عادل عبد العال خراشي، المرجع السابق، ص ٧٠-٧٥.
- (13) انظر: هشام مصطفى محمد، المرجع السابق، ص ٣٠-٣٥.
- (14) انظر: محمد محمد سيف شجاع، المرجع السابق.
- (15) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرات ٢٥-٣٠.
- (16) انظر: هشام مصطفى محمد، المرجع السابق، ص ٤٠-٤٥.
- (17) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ١-٢.
- (18) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرات ٣٥-٤٠.
- (19) انظر: محمد محمد سيف شجاع، المرجع السابق.
- (20) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٨.
- (21) انظر: عادل عبد العال خراشي، المرجع السابق، ص ٨٠-٨٥.
- (22) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ٢-٣.
- (23) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤٠.
- (24) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ٣-٣.
- (25) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤٢.
- (26) انظر: هشام مصطفى محمد، المرجع السابق، ص ٥٠-٥٥.
- (27) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤٥.
- (28) انظر: عادل عبد العال خراشي، المرجع السابق، ص ٩٠-٩٥.
- (29) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١، المادة ٥.
- (30) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٢٨.
- (31) انظر: محمد محمد سيف شجاع، المرجع السابق.
- (32) انظر: عادل عبد العال خراشي، المرجع السابق، ص ١٠٠-١٠٥.
- (33) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٣.
- (34) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١، المادة ٥(2).
- (35) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٦.
- (36) انظر: هشام مصطفى محمد، المرجع السابق، ص ٦٠-٦٥.
- (37) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرات ٣٠-٣٥.
- (38) انظر: المرجع السابق، الفقرة ٣١.

- (39) انظر: المرجع السابق، الفقرة ٣٢.
- (40) انظر: المرجع السابق، الفقرة ٣٤.
- (41) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، القسم ٢-٢.
- (42) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٥.
- (43) انظر: المرجع السابق، الفقرة ٣٦.
- (44) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١، المادة ٥.
- (45) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٣.
- (46) انظر: المرجع السابق، الفقرة ٣٨.
- (47) انظر: المرجع السابق، الفقرة ٤٠.
- (48) انظر: عادل عبد العال خراشي، المرجع السابق، ص ١١٠-١١٥.
- (49) انظر: هشام مصطفى محمد، المرجع السابق، ص ٧٠-٧٥.
- (50) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٢٥.
- (51) انظر: المرجع السابق، الفقرة ٢٦.
- (52) انظر: المرجع السابق، الفقرة ٢٧.
- (53) انظر: المرجع السابق، الفقرة ٢٨.
- (54) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١، المادة ٦.
- (55) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٢٩.
- (56) انظر: المرجع السابق، الفقرة ٣٠.
- (57) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١، المادة ٥(c)(1).
- (58) انظر: المرجع السابق.
- (59) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣١.
- (60) انظر: هشام مصطفى محمد، المرجع السابق، ص ٨٠-٨٥.
- (61) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٣.
- (62) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١، المادة ٥(2).
- (63) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٦.
- (64) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١، المادة ٥(e)(1).
- (65) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، القسم ٤-١.
- (66) انظر: هشام مصطفى محمد، المرجع السابق، ص ٩٠-٩٥.
- (67) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٧.
- (68) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، القسم ٤-٢.
- (69) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ١٠.
- (70) انظر: المرجع السابق، الفقرة ١٢.

- (71) انظر: المرجع السابق، الفقرة ١٥.
- (72) انظر: المرجع السابق، الفقرة ١٦.
- (73) انظر: المرجع السابق، الفقرة ١٨.
- (74) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، التقرير التفسيري، الفقرة ٣.
- (75) انظر: المرجع السابق، الفقرة ٥.
- (76) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٢٠.
- (77) انظر: المرجع السابق، الفقرة ٢٢.
- (78) انظر: المحكمة الأوروبية لحقوق الإنسان، Szabó and Vissy v. Hungary، الطلب رقم ١٤/٣٧١٣٨، الحكم الصادر في ١٢ يناير ٢٠١٦، و Big Brother Watch and Others v. the United Kingdom، الطلبات أرقام ١٣/٥٨١٧٠ و ١٤/٦٢٣٢٢٢ و ١٥/٢٤٩٦٠، الحكم الصادر في ٢٥ مايو ٢٠٢١.
- (79) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٨.
- (80) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ٤-٣.
- (81) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، المادة ٢.
- (82) انظر: اللائحة العامة لحماية البيانات (GDPR)، المادة ٩؛ ومملكة البحرين، قانون حماية البيانات الشخصية رقم ٣٠ لسنة ٢٠١٨، المادتان ٥ و ٦.
- (83) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، المادة ٥.
- (84) انظر: المرجع السابق، المادة ٥.(b)(1)
- (85) انظر: المرجع السابق، المادة ٥.(d)(1)
- (86) انظر: المرجع السابق، المادة ٧.
- (87) انظر: المرجع السابق، المادة ٦.
- (88) انظر: المرجع السابق، المادتان ٨ و ٩.
- (89) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٢٥.
- (90) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، المادة ٥.(e)(1)
- (91) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٢٩.
- (92) انظر: المرجع السابق، الفقرة ٣٠.
- (93) انظر: هشام مصطفى محمد، المرجع السابق، ص ١٠٠-١٠٥.
- (94) انظر: المرجع السابق.
- (95) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣١.
- (96) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ٣-٤.
- (97) انظر: المرجع السابق، القسم ٤-٤.
- (98) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٢.
- (99) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ٤-٥.
- (100) انظر: هشام مصطفى محمد، المرجع السابق، ص ١١٠-١١٥.
- (101) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٦.

- (102) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ١-٥.
- (103) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١، المادة ٥.
- (104) انظر: المرجع السابق، المادة ٥.(e)(1)
- (105) انظر: المرجع السابق.
- (106) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ٢-٥.
- (107) انظر: المرجع السابق، القسم ٣-٥.
- (108) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٣٦.
- (109) انظر: مجلس أوروبا، اتفاقية الجريمة المعلوماتية، ETS No. 185، ٢٠٠١، المواد ٢٣-٣٥؛ والبروتوكول الإضافي الثاني، CETS No. 224، ٢٠٢٢.
- (110) انظر: هشام مصطفى محمد، المرجع السابق، ص ١٢٠-١٢٥.
- (111) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١، المادة ٥.(2)
- (112) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤٥.
- (113) انظر: المرجع السابق، الفقرة ٤٠.
- (114) انظر: محمد محمد سيف شجاع، المرجع السابق.
- (115) انظر: عادل عبد العال خراشي، المرجع السابق، ص ١٣٠-١٣٥.
- (116) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤١.
- (117) انظر: المرجع السابق، الفقرة ٤٢.
- (118) انظر: المرجع السابق، الفقرة ٤٣.
- (119) انظر: هشام مصطفى محمد، المرجع السابق، ص ١٣٠-١٣٥.
- (120) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ١-٦.
- (121) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤٥.
- (122) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ٢-٦.
- (123) انظر: محمد محمد سيف شجاع، المرجع السابق.
- (124) انظر: المرجع السابق.
- (125) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ٥-٤.
- (126) انظر: المرجع السابق، القسم ٣-٦.
- (127) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤١.
- (128) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ١-٧.
- (129) انظر: المرجع السابق، القسم ٢-٧.
- (130) انظر: المرجع السابق، القسم ٣-٧.
- (131) انظر: المرجع السابق، القسم ١-٥.
- (132) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤٤.
- (133) انظر: محمد محمد سيف شجاع، المرجع السابق.
- (134) انظر: المرجع السابق.

- (135) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤٤.
- (136) انظر: المرجع السابق، الفقرة ٤٥.
- (137) انظر: عادل عبد العال خراشي، المرجع السابق، ص ١٤٠-١٤٥.
- (138) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤٦.
- (139) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١، المادة ٩.
- (140) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤٧.
- (141) انظر: المرجع السابق، الفقرة ٤٨.
- (142) انظر: هشام مصطفى محمد، المرجع السابق، ص ١٤٠-١٤٥.
- (143) انظر: المرجع السابق.
- (144) انظر: هشام مصطفى محمد، المرجع السابق، ص ١٥٠-١٥٥.
- (145) انظر: هشام مصطفى محمد، المرجع السابق، ص ١٦٠-١٦٥.
- (146) انظر: هشام مصطفى محمد، المرجع السابق، ص ١٧٠-١٧٥.
- (147) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤٥.
- (148) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ٦-١.
- (149) انظر: هشام مصطفى محمد، المرجع السابق، ص ١٨٠-١٨٥.
- (150) انظر Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics، المرجع السابق، القسم ٦-٣.
- (151) انظر: مجلس أوروبا، الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، ETS No. 108، ١٩٨١، المادة ٥(2).
- (152) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، المرجع السابق، الفقرة ٤٨.

الفصل الثالث: ضمانات التحريات الأمنية الرقمية والرقابة على مشروعيتها

المبحث الأول: الضمانات السابقة والمعاصرة لإجراء التحري

المطلب الأول: تحديد نطاق التحري وأهدافه وحدوده

تقتضي مشروعية التحريات الأمنية الرقمية أن يسبق استخدام الوسائل التقنية تحديد واضح للغرض، ونطاق المعلومات المطلوب جمعها، والأشخاص أو الوقائع التي يتصل بها الإجراء، والحدود الزمنية والموضوعية. ولا يقتصر هذا التحديد على تنظيم العمل الأمني إدارياً، بل يمثل **ضمانة قانونية** تحول دون تحول سلطة التحري إلى صلاحية مفتوحة لجمع المعلومات عن الأفراد دون ارتباط بهدف مشروع ومحدد. [1]

وتتأكد أهمية هذه الضمانة بالنظر إلى الطبيعة التراكمية للتحريات الرقمية؛ إذ قد تكون المعلومة المفردة محدودة الدلالة، بينما يؤدي ربطها بسجلات الاتصالات وبيانات الموقع والمحتوى المنشور إلى تكوين صورة تفصيلية عن الحياة الشخصية للفرد. ومن ثم، لا ينبغي أن يقتصر تقدير التدخل على طبيعة البيانات كل على حدة، بل يشمل حجمها ومدة جمعها وإمكان الربط بينها. [2]

ويجد هذا التصور أساسه في المادة السابعة عشرة من العهد الدولي، التي تحظر التدخل التعسفي أو غير القانوني في الخصوصية والمراسلات. ولا ينصرف الحظر إلى الإجراءات التي تفتقر إلى سند قانوني فحسب، وإنما يشمل التدخل الذي قد يستند إلى قاعدة قانونية لكنه يتسم بالتعسف بالنظر إلى ظروفه أو غرضه أو نطاقه أو آثاره. [3]

ويترتب على ذلك أن وجود أساس قانوني لا يكفي بمفرده؛ إذ ينبغي أن يكون الإجراء محدد الغرض، وأن تتوافر **علاقة معقولة** بين المعلومات المطلوبة والواقعة، وأن يكون نطاقه متناسباً مع الهدف. [4]

ويقضي التطبيق العملي تحديد عناصر الإجراء قبل تنفيذه:

١. الغرض: الواقعة أو المسألة الأمنية وصلتها بالاختصاص.
٢. النطاق الشخصي: الأشخاص الذين تتصل بهم المعلومات، مع مراعاة عدم توسيع التحري ليشملهم بلا ضرورة.
٣. النطاق الموضوعي: أنواع البيانات المطلوبة (محتوى منشور، تسجيلات، بيانات اتصالات، معلومات مخزنة).
٤. النطاق الزمني: الفترة المتصلة بالواقعة، وتجنب جمع بيانات سابقة أو لاحقة بلا أسباب موضوعية.
٥. النطاق التقني: الوسائل الرقمية الجائزة، وطبيعة الوصول المسموح، والقيود على الجمع والتحليل والحفظ.

٦. حدود الاستخدام اللاحق: الأغراض الجائزة والجهات التي يجوز المشاركة معها.[5]

ولا يعني ذلك وجوب معرفة جميع التفاصيل منذ البداية؛ فقد تكشف المعلومات الأولية عن وقائع تستلزم تعديل النطاق. غير أن هذا التعديل ينبغي أن يستند إلى أسباب موثقة، وأن يخضع لمراجعة قانونية متى كان من شأنه توسيع الإجراء أو الانتقال إلى وسيلة أشد تدخلاً.[6]

ويجب التمييز بين تطور التحري استجابةً لمعلومات جديدة والتوسع غير المنضبط. ففي الأول، يستند التعديل إلى معطيات ظهرت أثناء العمل. أما الثاني، فتُجمع المعلومات ابتداءً دون غرض محدد، ثم يُبحث لاحقاً عن استعمال محتمل. ويثير النهج الأخير إشكالاً جوهرياً يتعلق بتحويل جمع البيانات إلى غاية مستقلة.[7]

وقد أكدت المحكمة الأوروبية لحقوق الإنسان، في قضية *Big Brother Watch and Others v. the United Kingdom* (2021)، أهمية الضمانات المتكاملة في مراحل الاعتراض على الاتصالات واختيار البيانات وفحصها والاحتفاظ بها ومشاركتها، مع مراعاة طبيعة المراقبة الواسعة وما تنطوي عليه من مخاطر.[8]

ويكشف هذا الاتجاه عن قصور النظر إلى الإذن أو القرار الأولي بوصفه ضماناً كافية بذاته؛ إذ قد يكون الإجراء مشروعاً عند بدئه، ثم تنشأ أثناء التنفيذ مخاطر جديدة نتيجة اتساع البيانات أو تغير الغرض أو إدخالها في أنظمة تحليلية أخرى.[9]

وعليه، ينبغي أن يتضمن التخطيط آلية لمراجعة استمرار الحاجة إلى الإجراء، وإعادة تقييم نطاقه عند ظهور معطيات جديدة، وإنهائه عند زوال الغرض. وتكتسب هذه المراجعة أهمية خاصة عندما يسمح النظام التقني بجمع البيانات بصورة مستمرة أو آلية؛ لأن استمرار القدرة التقنية لا يعني استمرار المبرر القانوني.[10]

المطلب الثاني: توثيق السند القانوني والإذن عند لزمه

يمثل توثيق السند القانوني إحدى الضمانات الأساسية التي تتيح التحقق من أن الإجراء نُفذ في حدود الاختصاص، وأن القيود على استخدام الوسائل الرقمية قد روعيت. ولا يقتصر التوثيق على إثبات صدور قرار أو الحصول على إذن، بل يمتد إلى بيان طبيعة الإجراء المأذون به، ونطاقه، ومدته، والجهة التي أصدرته، والشروط الواجب مراعاتها أثناء التنفيذ.[11]

وتنبع أهمية التوثيق من أن كثيراً من إجراءات التحري الرقمي لا تترك أثراً ظاهرة للأشخاص الذين تمسهم، كما قد تتعذر عليهم معرفة ما إذا كانت بياناتهم قد جُمعت أو فُحصت أو نُقلت. وفي مثل هذه الظروف، يصبح السجل المكتوب وسيلة أساسية للمراقبة المؤسسية والقضائية.[12]

ويجب التمييز بين ثلاثة أمور مترابطة لكنها غير متطابقة:

١. وجود سند قانوني يجيز نوع الإجراء في الظروف المحددة.

٢. صدور الإذن أو التصريح من الجهة المختصة، متى كان القانون يشترطه.

٣. تنفيذ الإجراء فعلياً ضمن الحدود الموضوعية والشخصية والزمنية. [13]

فقد يكون الإجراء من حيث نوعه جائزاً، لكنه يُنفذ من جهة لا تملك الاختصاص. وقد يكون الإذن صحيحاً عند صدوره، ثم تتجاوز الجهة المنفذة نطاقه. كما قد تُنفذ عملية الجمع وفق حدود الإذن، لكن تُستخدم البيانات لاحقاً في غرض لا يسمح به القانون. ولكل صورة تقييمها القانوني الخاص. [14]

ويتعين أن يشتمل سجل الإجراء على:

- تحديد النص القانوني أو الأساس النظامي.
- بيان الجهة القائمة بالتحري وصفة القائمين على التنفيذ.
- تحديد القرار أو الإذن، واسم الجهة المختصة وتاريخ صدوره.
- وصف نطاق الإجراء والبيانات المشمولة.
- إثبات تاريخ البدء والانتهاء، وأي تمديد أو تعديل.
- تسجيل القيود أو الشروط الخاصة.
- توثيق أي توسع في نطاق الجمع وأسبابه.
- بيان ما إذا كانت البيانات قد نُقلت إلى جهة أخرى أو خضعت لمعالجة إضافية. [15]

ولا يُفهم من ذلك أن جميع إجراءات التحري تستلزم إذناً قضائياً مسبقاً؛ فذلك يتوقف على طبيعة الإجراء ومدى تدخله في الحقوق والتشريع المنطبق. فقد تسمح القواعد بجمع بعض المعلومات المتاحة للعموم دون إذن خاص، بينما تخضع إجراءات أخرى، مثل اعتراض الاتصالات أو الوصول القسري إلى بيانات محمية، لشروط أكثر صرامة. [16]

والأدق علمياً أن يُربط اشتراط الإذن بطبيعة التدخل القانوني، لا بمجرد وصف الوسيلة بأنها رقمية. فالتقنية الواحدة قد تُستخدم في صور متفاوتة من حيث أثرها في الحقوق؛ وقد يكون الوصول إلى محتوى منشور أقل تدخلاً من الدخول إلى حساب خاص، كما يختلف التصوير العابر في مكان عام عن المراقبة المستمرة التي تسمح بإعادة بناء أنماط الحركة. [17]

وتبرز أهمية التمييز بين الإذن كشرط إجرائي والرقابة كضمانة مستمرة. فالإذن لا يبرر تجاوز نطاقه، ولا يعفي الجهة من الالتزام بتقليل البيانات أو حماية المعلومات أو مراعاة شروط الاحتفاظ. كذلك لا يصح اعتبار توثيق الإجراء دليلاً قاطعاً على مشروعيته؛ لأن السجل قد يثبت ما قامت به الجهة دون أن يثبت أن ما قامت به كان جائزاً قانوناً. [18]

وقد أبرزت المحكمة الأوروبية في *Big Brother Watch* أهمية الضمانات التي تحكم مراحل جمع الاتصالات واختيارها وفحصها ومشاركتها، ولم تكتفِ بوجود إطار قانوني عام يجيز المراقبة. ويستفاد من ذلك أن كفاية الإطار تتوقف أيضاً على وضوح قواعد التنفيذ، وفاعلية الرقابة، والحد من السلطة التقديرية غير المقيدة.[8]

وتزداد أهمية هذه الضمانات في الإجراءات السرية، حيث قد يتعذر على الشخص الاعتراض أثناء التنفيذ. ففي هذه الحالات، ينبغي أن يوفر النظام القانوني رقابة مستقلة مناسبة، وسجلات قابلة للمراجعة، وآليات فعالة للتظلم والمساءلة.[19]

المطلب الثالث: قصر الوصول إلى المعلومات على المخولين

تقتضي حماية المعلومات ألا يكون الوصول إليها متاحاً لجميع العاملين لمجرد اتصالهم بالعمل، بل ينبغي أن يرتبط **بالحاجة الوظيفية الفعلية** وبالاختصاص المقرر لكل شخص. ويستند هذا المبدأ إلى ضرورة الحد من الاستخدام غير المصرح به، وتقليل مخاطر الإفشاء أو التعديل أو النسخ أو النقل خارج الغرض.[20]

وتزداد أهمية هذا الضابط في البيئة الرقمية بسبب سهولة نسخ البيانات وإرسالها وإعادة استخدامها. فقد يستطيع مستخدم واحد نسخ كمية كبيرة خلال وقت قصير، دون أن يؤدي ذلك إلى اختفاء النسخة الأصلية أو ظهور أثر مادي واضح. كما أن إتاحة البيانات ضمن نظام مشترك قد توسع دائرة الاطلاع بصورة لا تتناسب مع طبيعة المهمة.[21]

ومن ثم، فإن حماية المعلومات لا تتحقق بمجرد حفظها في نظام مؤمن؛ بل تتطلب تنظيم صلاحيات المستخدمين، وتحديد ما يجوز لكل منهم الاطلاع عليه، ومراقبة استخدام الصلاحيات، وتوثيق العمليات التي تتيح الوصول إلى البيانات الحساسة.[22]

ويقوم هذا التنظيم على ضوابط متكاملة:

١. **تحديد الصلاحيات بحسب الوظيفة**: تُمنح الصلاحيات وفق طبيعة المهمة، مع التمييز بين صلاحية الجمع والفحص واعتماد النتائج والمشاركة.[23]
٢. **مبدأ الحد الأدنى من الامتيازات**: عدم منح المستخدم صلاحيات أوسع مما يحتاج إليه، دون تعطيل العمل أو منع التنسيق.[24]
٣. **توثيق عمليات الوصول والمعالجة**: تسجيل الدخول والاطلاع والنسخ والتعديل والتصدير والحذف، مع تحديد المستخدم والتوقيت وطبيعة العملية.[25]
٤. **الفصل بين المهام الحساسة**: الفصل بين جمع البيانات وفحصها واعتماد التقرير النهائي، حيث تقتضي طبيعة العمل ذلك، للحد من تضارب المصالح.[26]
٥. **حماية الحسابات والوسائط التقنية**: إدارة الهويات، والتحقق من الصلاحيات، وحماية المصادقة، وتأمين الأجهزة وقواعد البيانات، ومراجعة الصلاحيات عند انتقال الموظف أو انتهاء علاقته.[27]

وتتصل هذه الضوابط بمبادئ اتفاقية مجلس أوروبا رقم ١٠٨ بشأن حماية الأشخاص تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، التي أرسيت إطاراً دولياً للدول الأطراف لحماية الأفراد عند معالجة بياناتهم، وفق نطاق الاتفاقية والتزامات الدول المعنية. [28]

ومع ذلك، فإن التحكم في الوصول لا ينبغي أن يُعامل باعتباره مسألة تقنية محضة؛ لأن تحديد المخولين يتصل أيضاً بتوزيع الاختصاص والمسؤولية. فكلما اتسعت دائرة الأشخاص الذين يستطيعون استخدام المعلومات، ازدادت صعوبة تحديد المسؤولية عن الإفشاء أو سوء الاستخدام. [29]

ويجب في المقابل تجنب المبالغة في تقييد الوصول بما يحول دون مراجعة مستقلة أو يمنع الدفاع والجهات القضائية من الاطلاع متى كان القانون يوجب ذلك. فالسرية وسيلة لحماية البيانات، وليس غاية تسمح بحجب المعلومات عن الجهات صاحبة الاختصاص. [30]

وبناءً عليه، يتعين أن يقوم نظام الوصول على التوازن بين السرية والمساءلة؛ فيحمي البيانات من الاطلاع غير المشروع، ويضمن في الوقت ذاته إمكان مراجعة القرارات والإجراءات والتحقق من سلامة النتائج. [31]

المطلب الرابع: حماية البيانات غير المرتبطة بموضوع التحري

تشير التحريات الرقمية إشكالياً خاصاً يتمثل في احتمال جمع بيانات تخص أشخاصاً أو أنشطة لا ترتبط مباشرة بالواقعة. فقد يؤدي فحص جهاز إلى ظهور مراسلات شخصية لأفراد آخرين، وقد تكشف مراقبة موقع عام عن تحركات أشخاص لا صلة لهم بالاشتباه، كما قد تتضمن قواعد البيانات المسترجعة معلومات حساسة تتجاوز نطاق المهمة. [32]

ولا تكمن المشكلة في ظهور هذه البيانات وحده، إذ قد يكون جمع بعضها أمراً يصعب تجنبه، وإنما في كيفية التعامل معها بعد ظهورها، ومدى جواز فحصها أو الاحتفاظ بها أو إدراجها في التقرير أو مشاركتها. [33]

ويقتضي مبدأ تقليل البيانات ألا يتجاوز الجمع والمعالجة القدر الضروري. وقد يتطلب ذلك استبعاد المعلومات غير المرتبطة، أو تقييد الوصول إليها، أو حجبها عن بعض مراحل التحليل، أو إنهاء الاحتفاظ بها متى زال الأساس القانوني. [34]

ويجب التمييز بين حالتين:

١. **البيانات التي تظهر عرضاً** أثناء تنفيذ إجراء مشروع: معلومات تنكشف نتيجة اتصالها التقني بالبيانات المستهدفة، دون أن يكون جمعها غرضاً مستقلاً.

٢. البيانات التي يُتوسع عمداً في جمعها أو فحصها: معلومات يجري الوصول إليها أو تحليلها خارج النطاق المحدد، بما قد يثير تجاوز الاختصاص أو مخالفة شروط الإذن أو انتفاء الضرورة.[35]

ولا يعني ظهور بيانات غير مستهدفة وجوب إتلافها فوراً في جميع الأحوال؛ فقد تكشف بعض المعلومات العرضية عن خطر جدي أو واقعة مستقلة يجيز القانون التعامل معها. غير أن الانتقال من ظهور المعلومة إلى استخدامها في إجراء جديد ينبغي أن يستند إلى أساس قانوني مستقل أو إلى قاعدة تسمح بهذا الاستخدام.[36]

ويترتب على ذلك أن الصلة التقنية بين البيانات لا تكفي لإثبات الصلة القانونية. فوجود مراسلة ضمن جهاز يخضع للفحص لا يجعل جميع محتوياته مشمولة تلقائياً بالغرض، كما أن وجود بيانات شخص في سجل اتصال لا يبرر بذاته إخضاعه لتحريات موسعة.[37]

ويتطلب التعامل مع البيانات غير المرتبطة اعتماد ضوابط واضحة:

- تحديد معايير استبعاد المعلومات التي لا تتصل بالواقعة.
- قصر فحص البيانات العرضية على القدر الذي يسمح به القانون.
- تجنب إدراج المعلومات الشخصية غير الضرورية في التقارير.
- فصل البيانات غير المرتبطة عن المواد المستخدمة في التحليل، متى أمكن.
- تحديد مدة الاحتفاظ بالبيانات العرضية ومسوغات تمديدتها.
- توثيق القرارات المتعلقة بالاحتفاظ أو النقل أو الحذف.
- حماية المعلومات التي قد تكشف عن مصادر سرية أو اتصالات مهنية محمية.[38]

وتتصل هذه الضوابط بمبدأ تحديد الغرض، الذي يفترض أن تُجمع البيانات وتُعالج في حدود أغراض مشروعة ومحددة، وألا يعاد استخدامها بصورة تتعارض مع تلك الأغراض. وقد أكدت الأطر الدولية لحماية البيانات أهمية التوفيق بين متطلبات المعالجة والمبادئ التي تحمي الأفراد من الاستخدام غير المنضبط.[28]

وتزداد حساسية المسألة عندما تتضمن البيانات العرضية معلومات تتعلق بالمحامين أو الصحفيين أو المصادر الصحفية أو الاتصالات المهنية المحمية. وقد أظهرت أحكام المحكمة الأوروبية بشأن المراقبة السرية أهمية وضع ضمانات ملائمة لحماية المواد ذات الطبيعة المهنية الحساسة، بالنظر إلى ما قد يترتب على الاطلاع عليها من آثار تتجاوز الشخص المستهدف.[8]

ومن الناحية العملية، ينبغي ألا يُترك مصير البيانات العرضية لتقدير الموظف الذي اكتشفها دون قواعد محددة؛ بل يتعين أن تخضع القرارات المتعلقة بفحصها أو الاحتفاظ

بها أو استخدامها لمعايير موضوعية، وأن توثق عند الاقتضاء، بما يتيح مراجعة مدى اتصالها بالغرض الأصلي.[39]

المبحث الثاني: الرقابة على أعمال التحري والمسؤولية عن تجاوزاتها

المطلب الأول: الرقابة القضائية في حدود الاختصاص القانوني

تُعد الرقابة القضائية إحدى الضمانات الأساسية لمشروعية التحريات الرقمية، خصوصاً عندما تنطوي الإجراءات على تدخل عميق في الخصوصية أو سرية المراسلات. وتقوم أهميتها على إخضاع استخدام السلطة الأمنية لمراجعة جهة مستقلة عن الجهة القائمة بالتحري، بما يحد من احتمالات التعسف أو تجاوز الاختصاص. [40]

ولا ينبغي النظر إلى الرقابة القضائية باعتبارها إجراءً واحداً ذا صورة ثابتة؛ إذ تختلف صورها بحسب طبيعة النظام القانوني ونوع الإجراء والمرحلة. فقد تتخذ صورة الإذن المسبق، أو مراجعة استمرار الإجراء، أو فحص مشروعية التنفيذ لاحقاً، أو الفصل في الطعون والتظلمات. [41]

كما يجب التمييز بين اختصاص القاضي بإصدار الإذن وبين اختصاصه بمراجعة مشروعية الإجراء أو تقييم قيمة المعلومات. فالإذن السابق يهدف إلى التحقق من توافر الشروط قبل مباشرة الإجراء، أما الرقابة اللاحقة فقد تتناول مدى الالتزام بحدود الإذن، ومشروعية الاحتفاظ، وسلامة الاستخدام، والآثار المترتبة على المخالفة. [42]

وتزداد الحاجة إلى رقابة مستقلة عندما تكون الإجراءات سرية، أو عندما لا يستطيع الشخص الاعتراض أثناء التنفيذ. ففي هذه الحالة، لا يكفي أن تتضمن القواعد نصوصاً عامة تمنع التعسف، بل ينبغي أن توجد آليات عملية تتيح فحص مدى الالتزام. [43]

وقد أكدت المحكمة الأوروبية في قضية *Roman Zakharov v. Russia* (2015) أهمية الضمانات المتعلقة بالإشراف على تدابير المراقبة السرية وسبل الانتصاف المتاحة للأفراد. كما أكدت في *Big Brother Watch* أهمية النظر إلى الضمانات التي تحكم مراحل الإجراء المختلفة، بدلاً من الاقتصار على تقييم قرار السماح بالمراقبة بمعزل عن طريقة تنفيذها. [44] [8]

ويُستفاد من هذا الاتجاه أن فاعلية الرقابة تتوقف على قدرتها على تناول الإجراء في مجموعه، بما يشمل الأساس القانوني، والجهة المنفذة، ونطاق البيانات، وطريقة اختيارها وفحصها، والاحتفاظ بها، ومشاركتها، والتخلص منها. [45]

وتتجلى الوظيفة الرقابية في:

١. التحقق من توافر شروط الإجراء: الأساس القانوني الصالح، واختصاص الجهة، وتحقيق الشروط.
٢. مراجعة الضرورة والتناسب: مدى ضرورة الوسيلة، وإمكان تحقيق الغرض بوسيلة أقل تدخلاً.
٣. التحقق من احترام نطاق الإذن: الالتزام بالحدود الموضوعية والشخصية والزمنية.

٤. **مراجعة معالجة البيانات الناتجة:** مشروعية الفحص والحفظ والمشاركة وإعادة الاستخدام.

٥. **تقييم فاعلية سبل الانتصاف:** وجود آليات لمعالجة الشكاوى وتحديد الآثار. [46]

ومع ذلك، لا يعني هذا أن الرقابة القضائية يجب أن تحل محل كل صور الرقابة الإدارية والفنية، أو أن كل إجراء رقمي يستلزم إذنًا قضائيًا. فالمعيار هو **طبيعة التدخل والضمانات التي يقررها القانون**، مع مراعاة أن التدابير الأكثر أساساً بالحقوق تحتاج عادةً إلى ضمانات أشد استقلالاً وفاعلية. [47]

كما أن استقلال جهة الرقابة لا يقاس بوصفها المؤسسي وحده، بل يتصل بمدى قدرتها على الاطلاع على المعلومات اللازمة، وفحص السجلات، والتحقق من الالتزام بالشروط، واتخاذ القرارات دون خضوع غير مشروع للجهة الخاضعة للرقابة. [48]

المطلب الثاني: الرقابة الإدارية والمؤسسية

تؤدي الرقابة الإدارية والمؤسسية دوراً مكماً للرقابة القضائية، من خلال متابعة الالتزام بالإجراءات، والتحقق من كفاءة الضوابط الداخلية، واكتشاف أوجه القصور قبل أن تتحول إلى انتهاكات مستمرة. [49]

وتكتسب أهمية خاصة لأن التحريات الرقمية تتضمن عمليات تقنية متكررة، قد ينفذها عدد كبير من الموظفين أو الأنظمة الآلية، وقد تنتج عنها كميات كبيرة من البيانات. ومن الصعب عملياً الاعتماد على التدخل القضائي وحده لمراجعة كل عملية تشغيل أو وصول أو نقل؛ ولذلك تحتاج الجهات إلى منظومة داخلية واضحة للمسؤولية والمراجعة والتدقيق. [50]

غير أن الرقابة المؤسسية لا تكون فعالة لمجرد وجود لوائح داخلية؛ إذ تتوقف فاعليتها على وضوح المسؤوليات، واستقلال وظيفة المراجعة بالقدر المناسب، وتوافر سجلات يمكن فحصها، ووجود إجراءات لمعالجة المخالفات، وعدم اقتصار المراجعة على التحقق الشكلي. [51]

ويقتضي بناء منظومة رقابية فعالة مراعاة:

١. **تحديد المسؤوليات المؤسسية:** بيان الجهة المسؤولة عن اعتماد الإجراءات، والجهة التي تنفذها، والمسؤولين عن إدارة البيانات، والجهة التي تتولى المراجعة. [52]

٢. **اعتماد سياسات مكتوبة:** تحديد أنواع الإجراءات المسموح بها، وشروط استخدام الوسائل، وقواعد إدارة الصلاحيات، والاحتفاظ، والمشاركة، والاستجابة للحوادث. [53]

٣. **إجراء مراجعات دورية:** فحص عينة من الإجراءات والسجلات، والتحقق من الالتزام بنطاق الاختصاص، ومراجعة عمليات الوصول إلى البيانات الحساسة. [54]

٤. **التحقق من فاعلية الضوابط التقنية:** فحص سجلات الأنظمة وصلاحيات المستخدمين وآليات الحماية، والتحقق من قدرة الأدوات على تسجيل العمليات. [55]

٥. **إدارة المخاطر والمخالفات:** آلية للإبلاغ عن الأخطاء والحوادث، وتحديد أسبابها، وتقييم آثارها، واتخاذ التدابير التصحيحية. [56]

٦. **المراجعة المستقلة للنتائج الحساسة:** إخضاع التحليل لمراجعة إضافية من شخص أو وحدة لم تتول إنتاج النتيجة الأصلية، حيث تقتضي طبيعة العمل. [57]

وتتصل هذه العناصر بمبدأ **المساءلة** في حماية البيانات؛ إذ لا تقتصر الحماية على إعلان المبادئ، بل تتطلب وجود إجراءات يمكن بواسطتها إثبات الالتزام بها. وقد اتجهت الأطر الحديثة لحماية البيانات إلى تعزيز مسؤولية الجهات عن تنفيذ التدابير المناسبة وإظهار امتثالها. [58] [28]

ويجب التمييز بين الرقابة الإدارية على الأداء والرقابة المستقلة على المشروعية. فالجهة التي تراجع كفاءة موظفيها قد تتمتع بمعرفة تقنية مهمة، لكنها تظل جزءاً من المؤسسة التي تنفذ الإجراء. ولهذا لا يصح افتراض أن المراجعة الداخلية تغني دائماً عن الرقابة القضائية أو المستقلة متى كانت طبيعة التدخل تستدعيها. [59]

كذلك ينبغي أن تخضع الجهات الرقابية نفسها لضوابط تتعلق بسرية البيانات، وحدود الوصول، وتوثيق أعمال المراجعة، وتجنب استخدام المعلومات خارج الغرض الرقابي. فالرقابة التي تتوسع في الاطلاع دون ضوابط قد تنشئ مخاطر جديدة. [60]

ومن ثم، فإن فاعلية الرقابة المؤسسية تقوم على الجمع بين وضوح المسؤوليات، وكفاءة المراجعة، واستقلالها النسبي، وقابلية نتائجها للتحقق، ووجود آلية ملزمة لمعالجة أوجه القصور. [61]

المطلب الثالث: التنظيم والشكاوى والمراجعة اللاحقة

لا تكتمل الضمانات بمجرد تنظيم الإجراءات الداخلية أو إخضاعها لرقابة سابقة أو معاصرة، بل تتطلب وجود آليات تتيح الاعتراض على الاستخدام غير المشروع للسلطة، والتحقق من الشكاوى المتعلقة بجمع البيانات أو فحصها أو الاحتفاظ بها أو مشاركتها. [62]

وتنبع أهمية التظلم من أن الشخص المتأثر قد لا يكون قادراً على اكتشاف المخالفة أثناء تنفيذها، خصوصاً عندما تتسم المراقبة بالسرية أو عندما تُعالج البيانات آلياً. وقد يكتشف لاحقاً أن بياناته استُخدمت في سياق غير متوقع، أو أن معلومات غير دقيقة أُسندت إليه، أو أن بياناته استمر الاحتفاظ بها رغم انتهاء الغرض. [63]

غير أن السرية التي قد تقتضيها بعض الإجراءات لا تعني استبعاد إمكان الشكاوى أو المراجعة بصورة مطلقة. وإنما تستلزم تنظيم هذه الآليات بطريقة تحمي المعلومات الحساسة، مع الحفاظ على قدر كافٍ من الاستقلال والفاعلية. [64]

وتختلف صور التظلم بحسب النظام القانوني، فقد تشمل تقديم شكوى إلى جهة رقابية، أو طلب مراجعة البيانات، أو الطعن أمام جهة قضائية، أو المطالبة بتصحيح معلومات غير دقيقة، أو الاعتراض على استمرار الاحتفاظ، أو المطالبة بجبر الضرر.[65]

ويجب التمييز بين مجرد إتاحة تقديم الشكوى ووجود سبيل انتصاف فعال. فالإجراء لا يكون فعالاً لمجرد أن الجهة تتلقى الشكاوى؛ بل ينبغي أن تتوفر إمكانية فحصها بجدية، والحصول على المعلومات الضرورية، واتخاذ التدابير التي تدخل ضمن الاختصاص.[66]

ويمكن تحديد أهم متطلبات الفاعلية:

- **وضوح جهة الاختصاص:** معرفة الجهة التي يمكن اللجوء إليها، بالقدر الذي تسمح به طبيعة الإجراء والسرية.
- **استقلال المراجعة:** ضمانات تحول دون اقتصار الفحص على الشخص أو الوحدة التي نفذت الإجراء محل الاعتراض.
- **إمكان الوصول إلى السجلات:** تمكين جهة المراجعة من فحص الأذونات والقرارات وبيانات الوصول.
- **تحديد نطاق الشكوى:** بيان الإجراء المعترض عليه وطبيعة المخالفة والبيانات المتأثرة.
- **فاعلية التدابير التصحيحية:** وقف المعالجة غير المشروعة، أو تصحيح البيانات، أو تقييد الوصول، أو إتلاف المعلومات.
- **إمكان طلب التعويض:** وفق شروط المسؤولية والاختصاص.[67]

وتبرز إشكالية خاصة في الإجراءات السرية التي قد لا يُخطر فيها الشخص بوقوع المراقبة. ففي مثل هذه الحالات، قد يصعب عليه تقديم شكوى محددة لعدم علمه بالإجراء. وقد تناولت المحكمة الأوروبية هذه المسألة في اجتهاداتها بشأن المراقبة السرية، مؤكدة أهمية النظر إلى آليات الإشراف وسبل الانتصاف عند تقييم كفاية الضمانات ضد التعسف.[44] [8]

ولا يعني ذلك أن الإخطار اللاحق واجب في جميع الحالات وبصورة مطلقة؛ فقد تتعارض بعض صور الإخطار مع مصالح مشروعة. غير أن استبعاد الإخطار ينبغي ألا يؤدي إلى إفراغ الحماية من مضمونها، بل يستلزم وجود ضمانات بديلة مناسبة، كالمراجعة المستقلة أو آليات الشكوى التي لا تتوقف على علم الشخص.[68]

ومن جهة أخرى، لا ينبغي أن تتحول آليات التظلم إلى وسيلة لفرض كشف غير مبرر عن مصادر المعلومات أو تعطيل الإجراءات المشروعة؛ بل يتعين تنظيم الوصول إلى البيانات السرية وفق معايير تحقق التوازن بين متطلبات الأمن وحقوق الأشخاص.[69]

وتؤدي المراجعة اللاحقة وظيفة تتجاوز معالجة الشكاوى الفردية، إذ تساعد على اكتشاف الأنماط المتكررة من الأخطاء، وتقييم كفاية الضوابط، وتحديد الحالات التي تستلزم تعديل السياسات أو تدريب العاملين أو تطوير الوسائل التقنية. وبهذا المعنى، تمثل الشكاوى مصدراً للتعلم المؤسسي، بشرط ألا يُختزل التعامل معها في إغلاق الملف الإداري دون فحص الأسباب الجذرية. [70]

المطلب الرابع: المسؤولية المترتبة على مخالفة الضوابط القانونية

تترتب على مخالفة الضوابط آثار قانونية قد تتنوع بحسب طبيعة المخالفة، وصفة مرتكبها، ومدى الضرر، والنظام القانوني. ولا يصح افتراض أن جميع المخالفات تؤدي إلى نتيجة واحدة، أو أن ثبوت مخالفة إجرائية يترتب عليه بالضرورة استبعاد كل المعلومات، أو أن صحة المعلومات فنياً تصح تلقائياً عدم مشروعية الحصول عليها. [71]

ويقتضي التحليل التمييز بين صور مختلفة من المسؤولية:

أولاً: المسؤولية الجنائية. قد تنثور عندما يشكل الفعل جريمة، كالدخول غير المشروع إلى الأنظمة، أو إفشاء المعلومات المحمية، أو إساءة استخدام الصلاحيات، أو التلاعب بالبيانات. ولا يكفي وصف التصرف بأنه غير مشروع إدارياً؛ بل ينبغي توافر أركان الجريمة وشروط إسنادها. [72]

ويجب التمييز بين **مخالفة الضوابط الداخلية** و**ارتكاب فعل مجرم**؛ فقد تكون المخالفة التأديبية قائمة دون أن تبلغ حد التجريم، كما قد تتوافر المسؤولية الجنائية إلى جانب التأديبية. [73]

ثانياً: المسؤولية التأديبية والإدارية. قد يترتب على تجاوز الصلاحيات أو مخالفة إجراءات العمل أو إفشاء المعلومات اتخاذ تدابير تأديبية أو إدارية. وقد تشمل التنبيه أو الجزاء أو سحب الصلاحيات أو إعادة التدريب. وتؤدي دوراً وقائياً مهماً؛ إذ تستهدف تصحيح الخلل المؤسسي ومنع تكراره. [74]

ثالثاً: المسؤولية المدنية أو التعويضية. قد يترتب على المعالجة غير المشروعة أو الإفشاء غير المصرح به ضرر مادي أو معنوي يستوجب التعويض، متى توافرت شروط المسؤولية. ويشمل ذلك إثبات الفعل غير المشروع والضرر وعلاقة السببية. [75]

ولا يفترض استحقاق التعويض بمجرد وقوع أي مخالفة شكلية؛ إذ تتوقف شروطه على القواعد المطبقة وطبيعة الضرر ومدى ارتباطه بالفعل. [76]

رابعاً: المسؤولية المؤسسية. قد تكشف المخالفة عن قصور في تصميم الإجراءات أو توزيع الصلاحيات أو حماية الأنظمة أو التدريب. وفي هذه الحالة، لا يكفي الاقتصار

على مساءلة الموظف؛ بل ينبغي فحص مدى إسهام الخلل المؤسسي واتخاذ التدابير لمعالجته. [77]

خامساً: الآثار المتعلقة بالمعلومات المتحصلة. يجب التمييز بين المسؤولية عن المخالفة وبين الأثر في إمكان استخدام المعلومات. فقد يترتب على المخالفة استبعاد الدليل أو تقييد الاستناد إليه أو تدبير تصحيحي آخر، وفق القانون المنطبق. وقد تكون المخالفة إدارية لا تؤثر بذاتها في قبول المعلومات، مع بقاء مسؤولية مستقلة. [78]

وفي المقابل، قد تكون المعلومات صحيحة فنياً لكنها متحصلة من إجراء غير مشروع. كما قد يكون الحصول مشروعاً، لكن البيانات تعرضت لاحقاً للتغيير أو التلف أو التفسير الخاطئ. ولهذا ينبغي فصل تقييم مشروعية الإجراء عن تقييم أصالة البيانات وسلامتها وقيمتها الاستدلالية. [79]

وتؤكد الأطر الفنية المتعلقة بالأدلة الرقمية أهمية المحافظة على البيانات وتوثيق إجراءات التعامل معها، بما يسمح بتحديد الأشخاص الذين حازوها وظروف انتقالها والعمليات التي أجريت عليها. [80] غير أن هذه الضوابط لا تحسم وحدها الآثار القانونية للمخالفة؛ إذ تظل خاضعة لقواعد الاختصاص والإجراءات والإثبات. [81]

ويقتضي تحديد المسؤولية مراعاة مبدأ التناسب بين طبيعة المخالفة والجزاء، دون الإخلال بوجوب مساءلة الأفعال التي تستوفي شروط المسؤولية. كما يتعين أن تكون الإجراءات التأديبية أو القضائية ذاتها خاضعة للضمانات القانونية المناسبة. [82]

المبحث الثالث: الآثار القانونية لمخالفة ضمانات التحري

المطلب الأول: أثر تجاوز الاختصاص أو مخالفة شروط الإذن

يثير تجاوز الاختصاص أو مخالفة شروط الإذن إشكالية تتعلق بمدى مشروعية الإجراء، وبالأثار التي ينبغي ترتيبها على المعلومات المتحصلة. ولا يمكن حسم هذه المسألة بقاعدة موحدة تنطبق على جميع النظم؛ لأن النتائج تتوقف على طبيعة الاختصاص، ومصدر الإذن، وجسامة المخالفة، والقواعد الإجرائية، والجزاء الذي يترتب عليه القانون. [83]

ويتحقق تجاوز الاختصاص عندما تمارس الجهة سلطة لا يخولها القانون، أو تتجاوز الحدود الموضوعية أو الشخصية أو المكانية. أما مخالفة شروط الإذن فتتحقق عندما يُنفذ الإجراء على نحو يتجاوز ما سمح به الإذن من حيث الأشخاص أو البيانات أو المدة أو الغرض أو الوسيلة. [84]

ويجب التمييز بين الحالتين؛ فقد تكون الجهة مختصة أصلاً بإجراء نوع معين، لكنها تتجاوز نطاق إذن محدد. وقد يكون الإجراء داخل الحدود الفنية للإذن، لكن الجهة التي أصدرته أو نفذته تفتقر إلى الاختصاص. [85]

ويمكن تقسيم المخالفات إلى أربع صور:

١. غياب السند القانوني: مباشرة وسيلة تحرّ لا يجيزها القانون أو استخدامها خارج الحالات المسموح بها. [86]
 ٢. صدور الإجراء من جهة غير مختصة: نوع الإجراء جائز، لكن الجهة التي أصدرته أو نفذته لا تملك الاختصاص. [87]
 ٣. تجاوز نطاق الإذن الصحيح: توسيع النطاق ليشمل بيانات أو أشخاصاً أو مدداً لا يغطيها. [88]
 ٤. الاستخدام اللاحق خارج الغرض المسموح: عملية الجمع مشروع، لكن الجهة تعيد استخدام البيانات في غرض مختلف. [89]
- ويتطلب التقييم تحديد طبيعة القاعدة المخالفة، وما إذا كانت تتعلق باختصاص جوهري أو بشرط إجرائي أو بضمانة لحماية الحقوق. كما ينبغي التحقق من وجود نص يحدد الأثر، أو من المبادئ القضائية المستقرة. [90]
- ولا يجوز افتراض أن كل مخالفة تؤدي حتماً إلى بطلان الإجراء أو استبعاد المعلومات؛ كما لا يجوز افتراض أن غياب نص صريح يجعل المخالفة عديمة الأثر. فقد يترتب النظام جزاء إدارياً أو جنائياً أو تعويضياً، أو يقرر أثراً إجرائياً معيناً، أو يترك تقدير بعض النتائج لجهة التحقيق أو المحكمة. [91]

وتوفر قضية *Big Brother Watch* مثلاً على ضرورة تقييم كفاية الضمانات القانونية والتنفيذية في أنظمة المراقبة، بما يشمل وضوح قواعد اختيار البيانات وفحصها والإشراف عليها. وقد انتهت المحكمة إلى وجود انتهاكات للمادة الثامنة فيما يتعلق بالنظامين محل الفحص.[8]

ولا تعني هذه النتيجة أن كل مخالفة في أي نظام تؤدي إلى الأثر نفسه، وإنما توضح أن مشروعية النظام تُقِيم في ضوء مجموع الضمانات التي تحد من السلطة التقديرية وتمنع التعسف، وأن وجود تشريع يجيز المراقبة لا يعفي من فحص كفاية الضوابط العملية.[92]

ويترتب على ذلك أن معالجة تجاوز الاختصاص أو مخالفة الإذن ينبغي أن تبدأ بتحديد موضع المخالفة بدقة، ثم بيان القاعدة المخالفة، ثم تقييم أثرها على الإجراء والمعلومات، دون القفز إلى نتيجة لا يسندها النص أو الاجتهاد.[93]

المطلب الثاني: التمييز بين عدم مشروعية الإجراء والخلل الفني

تقتضي الدقة الفصل بين مشروعية الإجراء الذي جُمعت به المعلومات وسلامة البيانات من الناحية الفنية. فالمشروعية تتعلق بالسند القانوني والاختصاص والإذن والالتزام بالضمانات، في حين تتعلق السلامة الفنية بمدى المحافظة على البيانات من التغيير أو التلف أو الفقد، وبإمكان التحقق من مصدرها وظروف التعامل معها.[94]

وهذان المجالان مترابطان، لكنهما لا يتطابقان. فقد تُجمع بيانات صحيحة فنياً بإجراء غير مشروع، كما قد تُجمع بيانات بطريقة مشروعة ثم تتعرض للتغيير أو التلف أو الخطأ أثناء النقل أو الفحص.[95]

وتتضح أهمية التمييز عند تقييم النتائج؛ لأن الخلط بين المجالين يؤدي إلى استنتاجات غير سليمة. فإثبات أن الملف لم يتغير منذ حساب قيمة التجزئة لا يثبت أن الحصول عليه كان مشروعاً. كما أن ثبوت مشروعية الحصول لا يثبت أن محتواه أصيل أو يعكس الواقعة بدقة.[96]

ويمكن توضيح التمييز من خلال الصور الآتية:

١. إجراء مشروع وبيانات سليمة: تمت عملية الجمع وفق الاختصاص والسند والشروط، مع المحافظة على البيانات. ولا يعني ذلك أن المعلومات تثبت الواقعة؛ إذ تظل الحاجة إلى تقييم مصدرها ودلائلها.[97]

٢. إجراء مشروع وبيانات معيبة فنياً: الجهة مخولة، لكنها تفشل في المحافظة على النسخة الأصلية أو توثيق انتقالها، أو تستخدم أداة غير مناسبة. وينصب الخلل على سلامة البيانات أو موثوقية النتائج.[98]

٣. إجراء غير مشروع وبيانات سليمة فنياً: تحصل الجهة على ملف دون الإذن اللازم، مع المحافظة على الملف دون تغيير. وتثبت السلامة الفنية حالة البيانات منذ نقطة معينة، لكنها لا تصح مخالفة القواعد.[99]

٤. إجراء غير مشروع وبيانات معيبة فنياً: تجتمع مشكلتان مستقلتان نسبياً، ويقتضي ذلك تقييم كل منهما وفق قواعدها.[100]

وتستند سلامة البيانات إلى إجراءات فنية مثل المحافظة على النسخة الأصلية، وتوثيق خطوات الاستخراج والفحص، وتسجيل عمليات النقل والوصول، واستخدام وسائل مناسبة للتحقق من عدم التغيير. وقد تناول مكتب الأمم المتحدة المعني بالمخدرات والجريمة أهمية التعامل المنضبط مع الأدلة الرقمية، بما يشمل توثيق سلسلة العهدة وتحليل البيانات وإعداد التقارير.[80]

غير أن هذه الإجراءات لا تُغني عن الضوابط القانونية. فالمعايير الفنية تجيب عن أسئلة تتعلق بكيفية الحصول على البيانات والمحافظة عليها والتحقق منها، بينما تحدد القواعد القانونية ما إذا كان الحصول جائزاً، ومن يملك سلطة القيام به، وما القيود على استخدامها.[101]

ويجب التمييز بين سلامة البيانات وموثوقية المعلومات المستخلصة. فقد تكون البيانات محفوظة دون تغيير، لكنها غير دقيقة أصلاً بسبب خلل في الجهاز أو عدم صحة الساعة الداخلية أو خطأ في تحديد الموقع. ومن ثم، فإن المحافظة على البيانات لا تعني بالضرورة صحة مضمونها.[102]

ويستلزم التقييم الفني تحديد ما الذي تثبته وسيلة التحقق وما لا تستطيع إثباته. فقيمة التجزئة، مثلاً، يمكن أن تساعد في التحقق من تطابق نسختين رقميتين في حدود الخوارزمية، لكنها لا تثبت وحدها هوية منشئ الملف أو صحة محتواه أو مشروعية الحصول عليه.[103]

ومن جهة أخرى، لا يصح افتراض أن كل خلل في التوثيق يؤدي تلقائياً إلى فقدان المعلومات لقيمتها القانونية. فقد يختلف أثر النقص في سجل العهدة بحسب طبيعة البيانات، ودرجة النقص، وإمكان استكمال التحقق بوسائل مستقلة، والقواعد الإجرائية.[104]

وعليه، ينبغي أن يتضمن تقييم المعلومات الرقمية محورين منفصلين ومتراپطين : محوراً قانونياً يفحص مشروعية الجمع والمعالجة، ومحوراً فنياً يفحص الأصالة والسلامة والموثوقية. ويُضاف إليهما تقييم مستقل للدلالة الاستدلالية، حتى لا يُستنتج من صحة الإجراء أو سلامة البيانات ما لا يثبت أي منهما.[105]

المطلب الثالث: أثر المخالفة في إمكان الاستناد إلى المعلومات وقيمتها القانونية

لا يؤدي ثبوت مخالفة أحد الضوابط إلى نتيجة قانونية واحدة في جميع الأحوال؛ إذ يختلف أثر المخالفة باختلاف طبيعتها، والنظام القانوني، والمرحلة التي وقعت فيها، ومدى اتصالها بحقوق الأشخاص أو بضمانات العدالة الإجرائية. [106]

ويقتضي التحليل التمييز بين ثلاثة أسئلة مستقلة:

١. هل جُمعت المعلومات أو عولجت بطريقة مشروعة؟
٢. هل تتمتع بالأصالة والسلامة والموثوقية الفنية اللازمة؟
٣. هل يجوز الاستناد إليها قانوناً، وما الوزن الذي يمكن منحها إياه في الإثبات؟ [107]

ولا يجوز دمج هذه الأسئلة في حكم واحد؛ لأن الإجابة بالإيجاب عن أحدها لا تحسم الإجابة عن الآخرين. فقد تكون المعلومات متحصلة من إجراء مشروع لكنها غير موثوقة، أو موثوقة فنياً لكنها متحصلة من إجراء مخالف، أو مشروعة وسليمة لكن دلالتها لا تتجاوز تأييد فرضية دون أن تكفي وحدها للإثبات. [108]

أولاً: أثر المخالفة في مشروعية الاستناد. تتوقف إمكانية الاستناد إلى المعلومات المتحصلة من إجراء مخالف على قواعد النظام القانوني المعني. فقد ينص القانون على استبعاد دليل معين عند الحصول عليه بالمخالفة لشروط محددة، وقد يميز بين أنواع المخالفات بحسب جسامتها وأثرها في الحقوق، وقد يرتب جزاءات أخرى دون أن يقرر الاستبعاد تلقائياً. [109]

ولهذا لا يصح تعميم قاعدة استبعاد الأدلة المتحصلة بصورة غير مشروعة على جميع الأنظمة، كما لا يصح افتراض أن جميع النظم تتبنى الاتجاه المعاكس. ويتعين تحديد القاعدة الواجبة التطبيق قبل تقرير الأثر. [110]

وفي هذا السياق، ينبغي التمييز بين استبعاد المعلومات ذاتها وعدم الاعتداد بإجراء معين أو تقييد استخدام نتائجه. فقد يتعلق الجزاء بالإجراء الذي شابه العيب، وقد يمتد إلى المعلومات الناتجة عنه، وقد يتناول فقط بعض البيانات التي جُمعت خارج نطاق الإذن. [111]

كما قد يختلف الحكم إذا كانت المعلومات محل النزاع قد جُمعت مباشرة نتيجة الإجراء المخالف، أو كانت مستقلة عنه، أو أمكن التحقق منها بمصدر منفصل مشروع. غير أن تحديد أثر هذه العلاقات يتوقف على القانون والاجتهاد القضائي المعنيين، ولا يجوز افتراض قاعدة موحدة. [112]

ثانياً: أثر الخلل الفني في الاعتماد على المعلومات. قد لا تتعلق المشكلة بمشروعية الجمع، وإنما بعدم القدرة على إثبات أصالة البيانات أو سلامتها. ويظهر ذلك عندما لا يُعرف مصدر الملف، أو يتعذر تحديد ما إذا كان قد تعرض للتعديل، أو تكون سلسلة العهدة ناقصة، أو لا تتوافر معلومات كافية عن الأدوات المستخدمة. [113]

وفي مثل هذه الحالات، ينبغي تقييم مدى تأثير الخلل في إمكان التحقق من البيانات وفي دلالة النتائج. وقد يؤدي الخلل إلى إضعاف القيمة الاستدلالية، أو الحاجة إلى فحص إضافي، أو تعذر الاعتماد على نتيجة معينة. [114]

ولا ينبغي مساواة جميع أوجه النقص؛ فعدم تسجيل خطوة فنية محدودة قد يختلف عن انقطاع جوهري يحول دون معرفة مصدر البيانات أو احتمال تغييرها. كما أن إمكانية إعادة الفحص باستخدام نسخة مستقلة أو مصدر آخر قد تساعد على تقييم أثر الخلل. [115]

وتؤكد المواد التدريبية الصادرة عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة أن التعامل مع الأدلة الرقمية يستلزم توثيق الجمع والحيازة والنقل والتحليل والإبلاغ عن النتائج، بما يسمح بتقييم سلامة التعامل مع البيانات. [80]

ثالثاً: أثر ضعف الدلالة الاستدلالية. قد تكون المعلومات مشروعة وسليمة فنياً، لكنها لا تكفي لإثبات النتيجة التي يُراد استخلاصها. فوجود جهاز في موقع معين لا يثبت بالضرورة أن مالكه كان موجوداً فيه، وظهور حساب إلكتروني باسم شخص لا يثبت وحده أن الشخص نفسه أنشأ كل محتوى، كما أن تسجيل اتصال بين شخصين لا يثبت بذاته طبيعة العلاقة. [116]

ويتطلب تقدير الدلالة النظر في السياق، والمصادر المستقلة، والفرضيات البديلة، والقيود الفنية، ومدى إمكان التحقق. وينبغي الفصل بين ما تثبته البيانات مباشرة وما يستنتجه المحلل منها. [117]

فإذا كانت المعلومة تدعم احتمالاً معيناً دون أن تستبعد تفسيرات بديلة معقولة، وجب عرضها باعتبارها مؤشراً أو قرينة محتملة، لا باعتبارها إثباتاً حاسماً. ويؤدي الخلط بين الارتباط والسببية إلى مشكلة مماثلة؛ إذ قد تظهر علاقة زمنية أو مكانية بين حدثين دون أن تثبت أن أحدهما تسبب في الآخر. [118]

رابعاً: أثر المخالفة في وزن المعلومات أمام جهة التحقيق أو المحكمة. حتى عندما يسمح القانون بتقديم المعلومات أو الاستناد إليها، لا يعني ذلك أنها تتمتع بوزن إثباتي محدد سلفاً. فالقبول القانوني للمادة يختلف عن تقدير قوتها في إثبات الواقعة، ويخضع هذا التقدير للقواعد الإجرائية والإثباتية. [119]

وقد تكون المعلومات قابلة للتقديم، لكنها محدودة الدلالة بسبب نقص السياق أو غياب التحقق المستقل. وقد يكون التقرير الفني واضح المنهج، لكنه لا يجيب عن المسألة القانونية المطلوب حسمها. [120]

ومن ثم، ينبغي أن يوضح التقرير الأمني أو الفني:

- مصدر كل معلومة وطريقة الحصول عليها.
- الأساس القانوني للإجراء، بالقدر اللازم لتقييم مشروعيته.

- الإجراءات الفنية المتخذة للمحافظة على البيانات والتحقق منها.
 - النتائج التي تدعمها البيانات بصورة مباشرة.
 - الاستنتاجات التي تعتمد على الربط أو التفسير.
 - الفرضيات البديلة التي لم يمكن استبعادها.
 - القيود التي تؤثر في دقة النتيجة أو مدى الاعتماد عليها.[121]
- ويُعد الإفصاح عن هذه العناصر ضماناً مهمة لمنع المبالغة في دلالة المعلومات الرقمية، وتمكين الجهات المختصة من تقييمها بصورة مستقلة.[122]
- خامساً: ضرورة الفصل بين المسؤولية عن المخالفة والأثر الإثباتي.** قد تترتب على المخالفة مسؤولية جنائية أو تأديبية أو مدنية، دون أن يكون الأثر الإثباتي للمعلومات مطابقاً بالضرورة لنتيجة المساءلة. وفي المقابل، قد يُقرر أثر إجرائي على المعلومات دون أن يعني ذلك تلقائياً ثبوت المسؤولية الجنائية أو المدنية لكل شخص شارك.[123]
- ويقتضي هذا التمييز تحديد الأساس القانوني لكل نتيجة على حدة؛ فالمسؤولية تتطلب توافر شروطها الخاصة، والاستبعاد أو تقييد الاستناد يتطلب سنداً في القواعد الإجرائية أو الإثباتية، أما وزن المعلومات فيتعلق بمدى قدرتها على دعم الاستنتاج المطلوب.[124]
- وتؤكد المعايير الدولية المتعلقة بحماية الخصوصية أهمية وجود ضمانات فعالة ضد التدخل التعسفي، بينما تؤكد الممارسات الفنية المتعلقة بالأدلة الرقمية ضرورة المحافظة على البيانات وتوثيقها والتحقق منها. ولا يحل أحد المجالين محل الآخر؛ بل يتطلب التقييم السليم الجمع بينهما دون الخلط بين وظائفهما.[80] [8] [3]
- وبناءً عليه، فإن المعالجة العلمية لمخالفة ضمانات التحري تستلزم تحديد طبيعة الخلط، وبيان القاعدة المخالفة، وتقييم أثر المخالفة في مشروعية الإجراء، ثم فحص أصالة المعلومات وسلامتها، وأخيراً تحديد ما يسمح به القانون بشأن الاستناد إليها ووزنها. ويمنع هذا التسلسل الخلط بين المخالفة القانونية والعيب الفني وضعف الدلالة، ويتيح الوصول إلى نتيجة أكثر دقة واتساقاً مع ضمانات العدالة.[125]

الجدول المقارن: صور المخالفة وأثرها القانوني

صورة المخالفة	طبيعة العيب	المسؤولية المحتملة	الأثر الإجرائي المحتمل	ملاحظة
غياب السند القانوني	مشروعية (اختصاص/سند)	جنائية، تأديبية، مدنية	بطلان الإجراء أو استبعاد المعلومات (بحسب التشريع)	الأخطر؛ يمس أصل التدخل
صدور الإجراء من جهة غير مختصة	اختصاص	تأديبية، إدارية	عدم نفاذ أو بطلان (بحسب التشريع)	قد يكون الإجراء جائزاً لكن الجهة غير مخولة
تجاوز نطاق الإذن	تنفيذ	تأديبية، مدنية	استبعاد الجزء المتجاوز أو تقييد الاستناد	لا يُصحح الإذن الأصلي التجاوز
الاستخدام اللاحق خارج الغرض	معالجة	تأديبية، مدنية	تقييد الاستخدام أو استبعاد النتائج	مستقل عن مشروعية الجمع الأولي
الخلل الفني (سلامة البيانات)	فني	قد لا تترتب مسؤولية قانونية	إضعاف القيمة الاستدلالية أو الحاجة لفحص إضافي	لا يصحح عدم المشروعية، ولا يعني بالضرورة استبعاداً
ضعف الدلالة الاستدلالية	استدلالي	لا مسؤولية	لا يمنع القبول لكن يحد من الوزن	الارتباط لا يثبت السببية

❖ النافذة التطبيقية

- السيناريو:** صدر إذن قضائي لفحص هاتف محمول في واقعة احتيال مالي، محدد بفترة زمنية (ثلاثة أشهر) وبيانات ذات صلة بالتحويلات المالية.
- الالتزام بالنطاق:** لا يجوز فحص رسائل شخصية خارج الفترة أو غير مرتبطة بالتحويلات.
- البيانات العرضية:** إذا ظهرت مراسلات شخصية لأطراف أخرى، تُستبعد أو تُعزل، ما لم تكن ذات صلة مباشرة.
- الخلل الفني:** إذا لم يُوثق انتقال الجهاز من مكان الضبط إلى المختبر، تُضعف موثوقية النتائج، لكن لا يعني ذلك بالضرورة استبعادها.
- التجاوز:** إذا فحص المحقق مجلدات خارج نطاق الإذن، فإن الجزء المتجاوز يُستبعد أو يُقيد الاستناد إليه، وفق القانون المنطبق.
- الدرس:** المشروعية والإذن والنطاق والتوثيق الفني أربعة محاور مستقلة، ويجب تقييم كل منها على حدة.

النتائج العامة للفصل

١. تحديد الغرض والنطاق ضمانات قانونية سابقة، لا مجرد إجراء إداري.
٢. الطبيعة التراكمية للتحريات الرقمية تستلزم تقييم الأثر المجموع للبيانات، لا كل معلومة منفردة.
٣. توثيق السند والإذن شرط للتحقق من المشروعية، لكنه لا يثبتها بذاته.
٤. قصر الوصول على المخولين ضمانات لحماية البيانات والمساءلة.
٥. البيانات غير المرتبطة بموضوع التحري تستلزم ضوابط واضحة للفصل والاستبعاد والإتلاف.
٦. الرقابة القضائية والإدارية والتظلم والمساءلة منظومة متكاملة، لا بدائل لبعضها.
٧. المسؤولية متعددة المستويات (جنائية، تأديبية، مدنية، مؤسسية)، ويجب التمييز بينها.
٨. تجاوز الاختصاص ومخالفة الإذن لهما آثار إجرائية تتوقف على طبيعة القاعدة المخالفة.
٩. عدم مشروعية الإجراء مستقل عن الخلل الفني في سلامة البيانات.
١٠. أثر المخالفة في الاستناد إلى المعلومات يتوقف على القانون المنطبق، ولا يصح تعميم قاعدة واحدة.
١١. ضعف الدلالة الاستدلالية مسألة مستقلة عن المشروعية والسلامة الفنية.
١٢. الفصل بين المسؤولية عن المخالفة والأثر الإثباتي ضروري لتجنب الخلط بين الوظائف القانونية.

المراجع:

- (1) انظر: عادل عبد العال خراشي، ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي، ٢٠٠٦، ص ٩٥-٩٠.
- (2) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، A/HRC/51/17، ٢٠٢٢، الفقرات ٢٠-٢٥.
- (3) انظر: الأمم المتحدة، العهد الدولي الخاص بالحقوق المدنية والسياسية، ١٩٦٦، المادة ١٧؛ ولجنة حقوق الإنسان، التعليق العام رقم ١٦، ١٩٨٨، الفقرة ٨.
- (4) انظر: هشام مصطفى محمد، التحريات الأمنية وأثرها في الأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٥، ص ٤٠-٤٥.
- (5) انظر: محمد محمد سيف شجاع، شرح قانون الإجراءات الجزائية اليمني، مكتبة الصادق، صنعاء، ٢٠٠٥، الفصل الخاص بالتحريات.
- (6) انظر: خراشي، مرجع سابق، ص ١٠٠-١٠٥.
- (7) انظر A/HRC/51/17، مرجع سابق، الفقرة ٢٦.

- (8) انظر، ECtHR, *Big Brother Watch and Others v. the United Kingdom*, nos. 58170/13, 62322/14, 24960/15, 25 May 2021.
- (9) انظر A/HRC/51/17، مرجع سابق، الفقرة ٣٥.
- (10) انظر: المرجع السابق، الفقرة ٣٦.
- (11) انظر: شجاع، مرجع سابق.
- (12) انظر A/HRC/51/17، مرجع سابق، الفقرة ٤٠.
- (13) انظر: خراشي، مرجع سابق، ص ١١٠-١١٥.
- (14) انظر: هشام مصطفى، مرجع سابق، ص ٥٥-٥٠.
- (15) انظر Ayers, Rick; Brothers, Sam; Jansen, Wayne, *Guidelines on Mobile Device Forensics*, NIST SP 800-101 Rev. 1, 2014, at 5-1.
- (16) انظر: شجاع، مرجع سابق.
- (17) انظر A/HRC/51/17، مرجع سابق، الفقرة ٣٨.
- (18) انظر: المرجع السابق، الفقرة ٤٠.
- (19) انظر: المرجع السابق، الفقرة ٤٢.
- (20) انظر Ayers et al., *supra* note 15, at 4-5.
- (21) انظر: المرجع السابق، at 4-5.
- (22) انظر: المرجع السابق، at 4-6.
- (23) انظر: المرجع السابق، at 4-7.
- (24) انظر: المرجع السابق، at 4-8.
- (25) انظر: المرجع السابق، at 5-2.
- (26) انظر: شجاع، مرجع سابق.
- (27) انظر Ayers et al., *supra* note 15, at 4-9.
- (28) انظر: مجلس أوروبا، *الاتفاقية المتعلقة بحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي*، ETS No. 108، ١٩٨١؛ والاتفاقية الحديثة (108+)، CETS No. 223، ٢٠١٨.
- (29) انظر: خراشي، مرجع سابق، ص ١٢٠-١٢٥.
- (30) انظر A/HRC/51/17، مرجع سابق، الفقرة ٤٤.
- (31) انظر Ayers et al., *supra* note 15, at 4-10.
- (32) انظر A/HRC/51/17، مرجع سابق، الفقرة ٢٩.
- (33) انظر: المرجع السابق، الفقرة ٣٠.
- (34) انظر ETS No. 108، المادة ٥(c)(1).
- (35) انظر: هشام مصطفى، مرجع سابق، ص ١٠٠-١٠٥.
- (36) انظر A/HRC/51/17، مرجع سابق، الفقرة ٣١.
- (37) انظر: المرجع السابق، الفقرة ٣٢.
- (38) انظر Ayers et al., *supra* note 15, at 4-11.
- (39) انظر: المرجع السابق، at 5-3.
- (40) انظر A/HRC/51/17، مرجع سابق، الفقرة ٤٠.
- (41) انظر: شجاع، مرجع سابق.
- (42) انظر: خراشي، مرجع سابق، ص ١٣٠-١٣٥.
- (43) انظر A/HRC/51/17، مرجع سابق، الفقرة ٤١.
- (44) انظر ECtHR, *Roman Zakharov v. Russia*, no. 47143/06, 4 December 2015.
- (45) انظر *Big Brother Watch*, *supra* note 8.
- (46) انظر A/HRC/51/17، مرجع سابق، الفقرات ٤٢-٤٥.
- (47) انظر: المرجع السابق، الفقرة ٤٦.
- (48) انظر: المرجع السابق، الفقرة ٤٧.
- (49) انظر: شجاع، مرجع سابق.
- (50) انظر Ayers et al., *supra* note 15, at 6-1.
- (51) انظر: المرجع السابق، at 6-2.
- (52) انظر: المرجع السابق، at 6-3.
- (53) انظر: المرجع السابق، at 6-4.

- (54) انظر: المرجع السابق، 6-5 at
- (55) انظر: المرجع السابق، 6-6 at
- (56) انظر: المرجع السابق، 7-1 at
- (57) انظر: المرجع السابق، 7-2 at
- (58) انظر: UN Human Rights Council, *The Right to Privacy in the Digital Age*, A/HRC/RES/48/4, 7 October 2021.
- (59) انظر A/HRC/51/17:، مرجع سابق، الفقرة ٤٨.
- (60) انظر: المرجع السابق، الفقرة ٤٩.
- (61) انظر. Ayers et al., *supra* note 15, at 7-3.
- (62) انظر A/HRC/51/17:، مرجع سابق، الفقرة ٤٤.
- (63) انظر: المرجع السابق، الفقرة ٤٥.
- (64) انظر: المرجع السابق، الفقرة ٤٦.
- (65) انظر: شجاع، مرجع سابق.
- (66) انظر A/HRC/51/17:، مرجع سابق، الفقرة ٤٧.
- (67) انظر: المرجع السابق، الفقرة ٤٨.
- (68) انظر. 8. *Big Brother Watch, supra*
- (69) انظر A/HRC/51/17:، مرجع سابق، الفقرة ٤٩.
- (70) انظر: المرجع السابق، الفقرة ٥٠.
- (71) انظر: هشام مصطفى، مرجع سابق، ص ١٤٠-١٤٥.
- (72) انظر: المرجع السابق، ص ١٥٠-١٥٥.
- (73) انظر: المرجع السابق، ص ١٥٥-١٦٠.
- (74) انظر: المرجع السابق، ص ١٦٠-١٦٥.
- (75) انظر: المرجع السابق، ص ١٧٠-١٧٥.
- (76) انظر: المرجع السابق، ص ١٧٥-١٨٠.
- (77) انظر. Ayers et al., *supra* note 15, at 7-4.
- (78) انظر A/HRC/51/17:، مرجع سابق، الفقرة ٤٥.
- (79) انظر. Ayers et al., *supra* note 15, at 6-7.
- (80) انظر: UNODC, *Cybercrime Module 6: Handling of Digital Evidence*, Education for Justice Initiative.
- (81) انظر: المرجع السابق.
- (82) انظر A/HRC/51/17:، مرجع سابق، الفقرة ٤٨.
- (83) انظر: خراشي، مرجع سابق، ص ١٨٠-١٨٥.
- (84) انظر: شجاع، مرجع سابق.
- (85) انظر: هشام مصطفى، مرجع سابق، ص ١٨٠-١٨٥.
- (86) انظر: خراشي، مرجع سابق، ص ١٨٥-١٩٠.
- (87) انظر: المرجع السابق، ص ١٩٠-١٩٥.
- (88) انظر: هشام مصطفى، مرجع سابق، ص ١٨٥-١٩٠.
- (89) انظر ETS No. 108:، المادة ٥(2).
- (90) انظر: خراشي، مرجع سابق، ص ١٩٥-٢٠٠.
- (91) انظر A/HRC/51/17:، مرجع سابق، الفقرة ٤٥.
- (92) انظر. 8. *Big Brother Watch, supra*
- (93) انظر: خراشي، مرجع سابق، ص ٢٠٠-٢٠٥.
- (94) انظر. Ayers et al., *supra* note 15, at 6-7.
- (95) انظر: المرجع السابق.
- (96) انظر. UNODC, *supra* note 80.
- (97) انظر. Ayers et al., *supra* note 15, at 6-8.
- (98) انظر: المرجع السابق، 6-9 at
- (99) انظر: المرجع السابق، 6-10 at
- (100) انظر: المرجع السابق، 6-11 at

- (101) انظر. UNODC, *supra* note 80 :
- (102) انظر. Ayers et al., *supra* note 15, at 6-12 :
- (103) انظر: المرجع السابق، at 6-13.
- (104) انظر: المرجع السابق، at 6-14.
- (105) انظر. UNODC, *supra* note 80 :
- (106) انظر A/HRC/51/17،: مرجع سابق، الفقرة ٤٥.
- (107) انظر: خراشي، مرجع سابق، ص ٢١٠-٢١٥.
- (108) انظر: المرجع السابق، ص ٢١٥-٢٢٠.
- (109) انظر A/HRC/51/17،: مرجع سابق، الفقرة ٤٦.
- (110) انظر: المرجع السابق، الفقرة ٤٧.
- (111) انظر: خراشي، مرجع سابق، ص ٢٢٠-٢٢٥.
- (112) انظر: المرجع السابق، ص ٢٢٥-٢٣٠.
- (113) انظر. Ayers et al., *supra* note 15, at 6-15 :
- (114) انظر: المرجع السابق، at 6-16.
- (115) انظر: المرجع السابق، at 6-17.
- (116) انظر A/HRC/51/17،: مرجع سابق، الفقرة ٣٣.
- (117) انظر: المرجع السابق، الفقرة ٣٤.
- (118) انظر: المرجع السابق، الفقرة ٣٥.
- (119) انظر: خراشي، مرجع سابق، ص ٢٣٠-٢٣٥.
- (120) انظر A/HRC/51/17،: مرجع سابق، الفقرة ٣٦.
- (121) انظر. Ayers et al., *supra* note 15, at 7-5 :
- (122) انظر: المرجع السابق، at 7-6.
- (123) انظر: خراشي، مرجع سابق، ص ٢٣٥-٢٤٠.
- (124) انظر: المرجع السابق، ص ٢٤٠-٢٤٥.
- (125) انظر A/HRC/51/17،: مرجع سابق، الفقرة ٥٠.

الفصل الأول: مصادر المعلومات الرقمية ووسائل الحصول عليها

المبحث الأول: مصادر المعلومات الرقمية وتصنيفها

المطلب الأول: المصادر المفتوحة والمحتوى المنشور للعموم

تُعدّ المصادر المفتوحة من أبرز مصادر المعلومات التي تعتمد عليها التحريات الأمنية الرقمية، بالنظر إلى اتساع المحتوى المنشور عبر الإنترنت وتنوع الجهات المنتجة له. ويقصد بها مصادر المعلومات التي يمكن الوصول إلى محتوياتها بصورة مشروعة دون صلاحيات خاصة أو تجاوز قيود تقنية أو قانونية. ويشمل ذلك المواقع المتاحة للعموم، والمنشورات العامة على منصات التواصل، والسجلات العامة المنشورة إلكترونياً، والبيانات الحكومية المفتوحة، والمواد الإعلامية، والصور ومقاطع الفيديو المتداولة.[1]

ويقتضي هذا التعريف التمييز بين طبيعة المصدر من حيث إمكان الوصول، والقيمة العلمية أو القانونية للمعلومات المستمدة منه؛ فإتاحة المحتوى للعموم لا تعني بالضرورة صحته أو اكتماله أو إمكان نسبته إلى الشخص الذي يظهر فيه أو الحساب الذي نشره.[2]

وقد أسهم التطور التقني في الانتقال بالمصادر المفتوحة من مجرد وسيلة للحصول على معلومات متفرقة إلى مجال منظم لجمع المعلومات الرقمية والتحقق منها وتحليلها. ويظهر هذا التطور في بروتوكول بيركلي بشأن التحقيقات الرقمية القائمة على المصادر المفتوحة (٢٠٢٢)، الذي تناول المعايير المهنية والمنهجية اللازمة للتعامل مع المعلومات الرقمية المنشورة، بما يشمل جمعها والتحقق منها وتحليلها وتوثيقها، مع مراعاة المتطلبات القانونية والأخلاقية.[3]

ولا ينبغي النظر إلى المصادر المفتوحة بوصفها فئة متجانسة؛ إذ تختلف طبيعتها باختلاف الجهة المنتجة، والغرض من النشر، ومدى الخضوع للتحقق، والقيود على إعادة الاستخدام. فالمعلومات المنشورة في موقع رسمي قد تستمد قوتها من اختصاص الجهة الناشرة، بينما قد تستند المعلومات المنشورة في حساب شخصي إلى معرفة مباشرة أو نقل عن الغير أو ادعاء غير متحقق.[4]

ومن ثم، فإن التمييز بين المصدر والمحتوى والسياق يمثل شرطاً أساسياً للتعامل العلمي. فالمصدر هو الجهة أو الوسيط الذي أتاح المحتوى، والمحتوى هو المادة الرقمية المراد فحصها، أما السياق فيشمل الظروف المحيطة بإنشائها ونشرها وتداولها. وقد تتوافر الثقة النسبية في أحد هذه العناصر دون الآخرين.[5]

وتثير إتاحة المعلومات للعموم مسألة قانونية تتجاوز إمكان الوصول. فإمكان الاطلاع على بيانات شخص منشورة لا يعني بالضرورة جواز جمع جميع بياناته وربطها وتحليلها بصورة مستمرة أو استخدامها في كل غرض. إذ قد تؤدي المعالجة المنظمة لمعلومات متفرقة إلى إنشاء ملف تفصيلي عن الحياة الخاصة للفرد، بما ينتج أثراً مختلفاً عن الاطلاع العابر على منشور منفرد.[6]

ويتصل هذا التمييز بالمادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية، التي تحظر التدخل التعسفي أو غير القانوني في الخصوصية والأسرة والمسكن والمراسلات. ولا يترتب على ذلك أن كل جمع للمعلومات المنشورة علناً يمثل تدخلاً محظوراً، وإنما يستلزم تقييم المشروعية بالنظر إلى طبيعة المعالجة ونطاقها وغرضها وأثارها.[7]

وتتطلب الممارسة المهنية التمييز بين الحصول على المعلومات وتحويلها إلى نتيجة أمنية. فالعثور على منشور يتضمن ادعاءً لا يثبت وقوعه، كما أن تكرار الادعاء في عدد من الحسابات لا يعني بالضرورة تعدد مصادره؛ إذ قد تكون الحسابات جميعها قد نقلت عن منشور واحد. ومن هنا، فإن تعدد المنشورات لا ينبغي أن يُساوى آلياً بتعدد الأدلة المستقلة.[8]

وعليه، فإن القيمة الأساسية للمصادر المفتوحة لا تكمن في كونها بديلاً عن إجراءات التحقق، وإنما في قدرتها على توفير مؤشرات يمكن اختبارها وربطها بمصادر أخرى. وتزداد موثوقية النتائج كلما أمكن تحديد أصل المحتوى، وتوثيق ظروف الحصول عليه، والتحقق من سياقه، ومقارنته بمصادر مستقلة، والإفصاح عن حدود ما تسمح به المعلومات.[9]

المطلب الثاني: السجلات وقواعد البيانات

تمثل السجلات وقواعد البيانات أحد المصادر المهمة للتحريات الرقمية، لما تتضمنه من معلومات منظمة يمكن الاستفادة منها في التحقق من الهوية، وتتبع المعاملات، ومراجعة الوقائع الإدارية. وتتبع أهميتها من أن المعلومات قد جُمعت أو سُجلت وفق إجراءات مؤسسية محددة، مما يعزز إمكان التحقق من مصدرها، دون أن يجعلها بمنأى عن الخطأ أو التغيير أو التزوير.[10]

ويقصد بالسجل الرقمي مجموعة البيانات التي توثق واقعة أو معاملة أو حالة في نظام إلكتروني، بينما تشير قاعدة البيانات إلى مجموعة منظمة من البيانات تُخزَّن وتُدار بطريقة تسمح باسترجاعها وربط عناصرها. وقد يكون السجل جزءاً من قاعدة بيانات واسعة، كما قد تتضمن قاعدة البيانات سجلات متعددة تتصل بأشخاص أو مؤسسات أو معاملات.[11]

وتتعدد أنواع السجلات بحسب طبيعة الجهة والغرض: السجلات الحكومية العامة، وسجلات الشركات، والسجلات التجارية، والبيانات الإحصائية، وسجلات الأنظمة والشبكات، وقواعد البيانات الناشئة عن الخدمات الرقمية. ولا تتساوى هذه الفئات من حيث شروط الوصول أو موثوقية المحتوى أو حدود الاستفادة القانونية.[12]

ويقتضي تقييم هذه المصادر فحص أربعة عناصر: الجهة التي أنشأت السجل، والغرض من إنشائه، والآلية التي تُسجل بها البيانات، ومدى إمكان التحقق من سلامتها وحداثتها. فالبيانات قد تكون دقيقة عند إدخالها، لكنها تصبح غير ملائمة إذا لم تُحدَّث. وقد يكون النظام موثقاً تقنياً، لكن المعلومات المدخلة تتضمن أخطاء بشرية.[13]

ويظهر ذلك في قواعد البيانات التي تتضمن عناوين أو بيانات اتصال أو معلومات عن تسجيل المركبات. فوجود بيان في قاعدة رسمية قد يثبت أن هذا البيان كان مسجلاً في وقت معين، لكنه

لا يثبت بالضرورة استمرار صحته وقت التحري. كما أن تسجيل عنوان معين لشخص لا يثبت وحده وجوده فيه عند وقوع حادثة، ما لم تدعمه أدلة أخرى.[14]

وتتطلب الاستفادة من السجلات التمييز بين **صلاحية الوصول** و**صلاحية الاستخدام**. فقد تكون البيانات متاحة للاطلاع العام، لكن إعادة استخدامها أو دمجها مع بيانات أخرى قد يخضع لقيود قانونية أو تعاقدية. كذلك لا يؤدي امتلاك جهة أمنية صلاحية الدخول إلى نظام إلى منح كل موظفيها حق الوصول غير المقيد.[15]

وتبرز أهمية هذه المسألة عند **الربط بين قواعد البيانات المختلفة**. فقد يؤدي الجمع بين بيانات الهوية والسفر والاتصالات والموقع والمعاملات المالية إلى إنشاء صورة تفصيلية عن حياة شخص. وعلى الرغم من أن كل عنصر قد يكون مشروعاً منفرداً، فإن عملية الربط قد تكشف معلومات إضافية لم تكن ظاهرة. ولذلك ينبغي تقييم مشروعية عملية الربط ذاتها، لا الاكتفاء بفحص مشروعية الوصول إلى كل قاعدة بصورة منفصلة.[16]

ومن الناحية الفنية، يتطلب الاعتماد على السجلات توثيق وقت الاستخراج، والجهة أو النظام الذي استُخرجت منه، ومعايير البحث، ونطاق النتائج، وأي عمليات تحويل. وتزداد أهمية ذلك عندما تكون النتائج مستخرجة آلياً؛ إذ قد يؤثر اختلاف إعدادات النظام أو طريقة الاستعلام في نطاق البيانات التي تظهر.[17]

ويقدم **NIST SP 800-86** إطاراً عاماً للتعامل مع مصادر البيانات الرقمية، بما فيها الملفات وأنظمة التشغيل وحركة الشبكات والتطبيقات، ويؤكد أهمية تنظيم عمليات الجمع والفحص والتحليل ضمن منهجية موثقة. وعلى الرغم من أن هذا الدليل ليس تشريعاً، فإنه يوفر مرجعاً فنياً مفيداً عند وضع الإجراءات المؤسسية.[18]

ولا تكتسب السجلات قيمتها الاستدلالية بمجرد صدورها عن نظام إلكتروني أو مؤسسة رسمية، بل تتحدد وفق مصدرها، وآلية إنشائها، واكتمالها، وحدائنها، وسلامتها، وصلتها بالمسألة. ومن ثم، فإن التعامل المنهجي يقتضي النظر إليها باعتبارها **مصادر معلومات قابلة للتحقق**، لا حقائق نهائية.[19]

المطلب الثالث: المعلومات المقدمة من الأفراد والجهات

تُعد المعلومات المقدمة من الأفراد والجهات مصدراً مكماً للتحريات الرقمية، إذ قد تتيح الوصول إلى بيانات لا يمكن العثور عليها في المصادر المفتوحة، أو تساعد على تفسير محتوى غامض، أو تكشف عن سجلات ووسائط ذات صلة. وقد تأتي في صورة بلاغات إلكترونية، أو مراسلات، أو مستندات رقمية، أو إفادات، أو سجلات مقدمة من مؤسسة، أو بيانات تُسلم بناءً على طلب قانوني.[20]

غير أن تعدد الجهات يفرض التمييز بين **طبيعة مقدمها**، و**الأساس الذي يملك بموجبه المعلومات**، و**الظروف التي جُمعت فيها**، و**الغاية من تقديمها**. فالمعلومات التي يقدمها شاهد مباشر تختلف عن المعلومات المنقولة عن شخص آخر، كما تختلف البيانات المقدمة من جهة

تحتفظ بسجلات أنشأتها في سياق عملها عن المستندات التي يقدمها طرف له مصلحة في النتيجة.[21]

ويقتضي التقييم التمييز بين **صدق الشخص ودقة المعلومة**. فقد يكون مقدم المعلومة صادقاً في اعتقاده، لكنه مخطئ في تحديد التاريخ أو المكان أو هوية الشخص. وقد يكون دقيقاً في وصف ما شاهده، لكنه يفسر الواقعة تفسيراً غير صحيح. ومن ثم، لا ينبغي دمج المشاهدة المباشرة والتفسير الشخصي في عبارة واحدة توحى بأنهما يتمتعان بالدرجة نفسها من اليقين.[22]

كما أن تكرار المعلومات من عدة أشخاص لا يكفي وحده لإثبات صحتها إذا كان مصدرها المشترك واحداً. فقد يتداول عدد من الأفراد رواية منشورة على منصة، ثم تُقدّم الرواية نفسها من خلال بلاغات متعددة. وفي هذه الحالة، لا تمثل البلاغات تأكيداً مستقلاً، بل قد تعكس انتشار رواية واحدة. لذلك ينبغي تتبع **المصدر الأصلي**، وتحديد ما إذا كانت الإفادات مستقلة في منشئها.[23]

أما المعلومات المقدمة من الجهات والمؤسسات، فينبغي تقييمها في ضوء **اختصاص الجهة، وطبيعة السجلات، ومدى انتظام إجراءات الإنشاء والحفظ، والضوابط التي تحكم تسليمها**. ولا يعني الطابع المؤسسي أنها صحيحة على نحو مطلق؛ إذ قد تحتوي على أخطاء إدخال أو نقص في التحديث.[24]

وتبرز مسألة **مشروعية الحصول**، ولا سيما عندما تتضمن بيانات شخصية أو سرية أو معلومات تخص أطرافاً ثالثة. فقد يقدم أحد الأفراد نسخة من مراسلات خاصة أو ملفات مستخرجة من جهاز لا يملك حق الوصول إليه. ولا يكفي تسلم الجهة لهذه المعلومات بحسن نية لإثبات مشروعية طريقة الحصول عليها. بل يتعين تقييم ظروف الحصول، والحقوق المتصلة بها، والاختصاص القانوني، وما إذا كان استخدامها يخضع لضوابط.[25]

وتتصل هذه المسألة بمبدأ **عدم جواز التحايل على الضمانات القانونية** من خلال الاعتماد على المعلومات التي يجمعها الأفراد لحساب الجهة العامة. فإذا كانت طبيعة الإجراء تستلزم إنزاً أو اختصاصاً محدداً، فلا يجوز افتراض أن تقديم البيانات من شخص خاص يزيل تلقائياً جميع القيود. ويتعين التمييز بين **المبادرة المستقلة** من الفرد، و**توجيه الجهة له** أو تكليفه بجمع معلومات قد تخضع لضوابط أشد.[26]

وتتطلب المعالجة المهنية تسجيل هوية مقدمها بالقدر الذي يسمح به القانون، وتاريخ تقديمها، ووصف المواد، والظروف التي أحاطت بتسليمها، وأي بيان يقدمه المصدر بشأن طريقة الحصول. كما ينبغي الفصل بين المعلومات التي تم التحقق منها بصورة مستقلة والمعلومات التي لا تزال مستندة إلى إفادة مقدمها وحده.[27]

وتؤكد الأدبيات المهنية أن عملية جمع المعلومات لا تنفصل عن توثيق مصدرها وظروف الحصول عليها. وتتناول **إرشادات الإنترنت** للتحقيق الجنائي الرقمي المبادئ العملية المتعلقة بتأمين البيانات والأجهزة وتوثيقها وحفظها ونقلها، بما يدعم إمكان التحقق اللاحق من سلامتها.[28]

وعليه، فإن المعلومات المقدمة من الأفراد والجهات لا تُقبل أو تُرفض بوصفها فئة واحدة، وإنما تُقيّم بحسب مصدرها، وطريقة الحصول عليها، والغرض من تقديمها، ومدى إمكان التحقق منها. وتكمن القيمة الحقيقية في إمكان إخضاعها للتحقق المستقل، وربطها بمصادر أخرى، وتحديد حدود ما تثبته. [29]

المطلب الرابع: المعلومات المستمدة من الأجهزة والأنظمة والخدمات الرقمية

تنتج الأجهزة والأنظمة والخدمات الرقمية كميات واسعة من البيانات التي قد تسهم في فهم الوقائع وإعادة بناء تسلسل الأحداث. وتشمل الملفات المخزنة، وسجلات الدخول والخروج، وسجلات التطبيقات، وبيانات الموقع، والطوابع الزمنية، وسجلات الشبكات، وبيانات استخدام الخدمات. [30]

وتتميز هذه المصادر بأن بعض بياناتها يُنشأ بصورة آلية أثناء التشغيل، دون أن يكون الغرض المباشر إثبات واقعة أمنية. فقد ينشئ النظام سجلاً لتوثيق عملية دخول، أو يحتفظ التطبيق ببيانات عن وقت استخدام خدمة، أو يسجل الجهاز معلومات تتعلق بإنشاء ملف. وقد تصبح هذه البيانات ذات أهمية للتحري عندما ترتبط بواقعة معينة. [31]

ومع ذلك، فإن الطبيعة الآلية لا تمنحها حصانة من الخطأ. فقد تتأثر البيانات بإعدادات الجهاز، أو اختلاف المنطقة الزمنية، أو خلل البرمجيات، أو طريقة مزامنة الساعة، أو سياسات الاحتفاظ، أو تحديثات النظام. كما أن بعض السجلات لا تسجل جميع الأحداث، وإنما تسجل أحداثاً محددة وفق إعدادات مسبقة؛ ولذلك فإن عدم ظهور حدث في سجل معين لا يثبت بالضرورة عدم وقوعه. [32]

ومن الضروري التمييز بين البيانات المخزنة محلياً، والبيانات المحفوظة لدى مقدم الخدمة، والبيانات التي تنتقل عبر الشبكات، والبيانات التي تنشأ نتيجة تفاعل المستخدم مع نظام بعيد. فقد تتصل هذه الفئات، لكنها تختلف من حيث جهة الحيازة، وإمكان الوصول، وشروط الاستخراج، ومخاطر التغيير أو الفقد. كما قد يكون الجهاز داخل إقليم الدولة متصلاً بخدمة تُخزن بياناتها في دولة أخرى، مما يثير مسائل الاختصاص والتعاون الدولي. [33]

ويترتب على ذلك أن تحديد مصدر البيانات يجب أن يسبق تقييم دلالتها. فلا يكفي القول إن معلومة مستخرجة من هاتف أو حاسوب؛ بل ينبغي تحديد ما إذا كانت مأخوذة من الذاكرة المحلية، أو من نسخة احتياطية، أو من خدمة سحابية، أو من سجل قدمه مقدم الخدمة. ويؤثر هذا التحديد في إمكان التحقق من اكتمال البيانات وفهم طريقة إنشائها. [34]

وتتطلب بعض المصادر إجراءات فنية خاصة للمحافظة عليها، لا سيما عندما تكون سريعة التغير أو قابلة للفقد. وفي المقابل، قد يؤدي الوصول إلى البيانات ذاتها إلى تغيير بعض آثار النظام. ولذلك لا يمكن اعتماد إجراء موحد لجميع الأجهزة دون مراعاة طبيعة المصدر وحالته والهدف. [35]

ويعرض مكتب الأمم المتحدة المعني بالمخدرات والجريمة في مواده التعليمية مراحل أساسية تشمل تحديد البيانات وجمعها واستخراجها والمحافظة عليها، مع التشديد على توثيق الإجراءات وحماية سلامة المعلومات خلال انتقالها من مرحلة إلى أخرى.[36]

أما من الناحية القانونية، فينبغي التمييز بين الوصول إلى البيانات التي تملك الجهة صلاحية الاطلاع عليها، وبين اتخاذ إجراءات تمس بيانات محمية أو تتجاوز نطاق الإذن. فوجود البيانات على جهاز جرى ضبطه بصورة مشروعة لا يعني أن جميع محتوياته أصبحت متاحة دون حدود. كما أن الإذن بفحص جهاز لا يمتد تلقائياً إلى جميع الحسابات والخدمات السحابية المرتبطة به إذا كان القانون يقتضي أساساً مستقلاً.[37]

وتزداد أهمية هذه الضوابط عند التعامل مع بيانات الغير أو البيانات غير المرتبطة بموضوع التحري. فالأجهزة الشخصية قد تحتوي على مراسلات وصور وملفات طبية أو مالية تخص أشخاصاً متعددين. ولذلك ينبغي أن يقتصر الفحص، قدر الإمكان، على البيانات ذات الصلة بالغرض المشروع.[38]

وبناءً على ذلك، فإن المعلومات المستمدة من الأجهزة والأنظمة تتطلب الجمع بين الفهم التقني لطبيعة البيانات، والتحقق من مصدرها، وتوثيق إجراءات الحصول عليها، ومراعاة الحدود القانونية. ولا تتحقق موثوقيتها بمجرد استخراجها من نظام إلكتروني، وإنما من إمكان تفسير طريقة إنشائها وحفظها واستخراجها، والتحقق من سلامتها، وتحديد حدود دلالتها.[39]

المبحث الأول: مفهوم استخبارات المصادر المفتوحة وحدودها

تُعرف استخبارات المصادر المفتوحة (OSINT) بأنها عملية منهجية لتحديد المعلومات المتاحة من المصادر المفتوحة وجمعها وتقييمها وتحليلها وتحويلها إلى معرفة ذات صلة بمسألة محددة. وبهذا المعنى، لا يُقصد بها مجرد البحث في الإنترنت، بل عملية تحليلية متكاملة تبدأ بتحديد السؤال المراد الإجابة عنه، وتنتهي بتقديم نتائج يمكن تتبع مصادرها وتقييم درجة موثوقيتها وحدودها. [40]

ويمكن الفارق الجوهرى بين البحث العادي والعملية الاستخبارية في الوظيفة التي تؤديها المعلومات. فالبحث العادي قد يستهدف العثور على معلومة منفردة، بينما تسعى العملية الاستخبارية إلى تنظيم المعلومات المتفرقة وربطها وتحليلها بما يخدم غرضاً محدداً. ومع ذلك، لا يعني وصف العملية بأنها استخبارية أنها تمنح القائم بها صلاحيات قانونية إضافية، أو تسمح له بالوصول إلى البيانات المقيدة خارج الأطر المقررة. [41]

وقد أسهم بروتوكول بيركلي في وضع إطار مهني للتحقيقات الرقمية القائمة على المصادر المفتوحة، من خلال التركيز على التخطيط، وجمع المحتوى، والتحقق منه، وتحليله، وتوثيقه، مع مراعاة السلامة المهنية والاعتبارات القانونية والأخلاقية. وعلى الرغم من أن البروتوكول وضع أساساً للتحقيقات المتعلقة بانتهاكات القانون الدولي الجنائي وحقوق الإنسان، فإن عدداً من مبادئه المنهجية يمكن الإفادة منه في التحريات الأمنية الرقمية، دون افتراض انطباق جميع أحكامه على كل سياق. [42]

وتبدأ العملية المنهجية بتحديد المسألة وصياغة أسئلة قابلة للتحقق. فإذا كان السؤال يتعلق بمكان وقوع حادثة، فلا ينبغي أن يقتصر الجمع على العثور على صورة يُقال إنها التقطت في ذلك المكان، بل يتعين البحث عن مؤشرات مستقلة تتعلق بالمعالم الجغرافية والظروف الزمنية ومصدر النشر. وإذا كان السؤال يتعلق بنسبة حساب إلى شخص، فإن مجرد تشابه الاسم أو الصورة لا يكفي. [43]

ويجب أن تتناسب عملية الجمع مع السؤال المحدد. فجمع كميات كبيرة من البيانات دون غرض واضح لا يؤدي بالضرورة إلى تحسين النتائج، بل قد يزيد من مخاطر انتقاء المعلومات المؤيدة لافتراض أولي، ويضاعف معالجة بيانات غير ذات صلة، ويصعب مراجعة المصادر. لذلك ينبغي تحديد نطاق البحث ومعايير إدراج المعلومات واستبعادها. [44]

ومن الجوانب الأساسية التمييز بين العثور على المحتوى والتحقق منه. فالعثور على منشور لا يثبت صحته، كما أن إمكان الوصول إلى صورة لا يثبت أن المحتوى أنشئ في الزمان أو المكان اللذين ينسب إليهما. وقد يكون المحتوى أصلياً، لكن التعليق المصاحب مضلل، أو يكون صحيحاً في جزء منه دون أن يعكس الواقعة كاملة. [45]

ويتطلب التحقق استخدام مصادر مستقلة كلما أمكن، وفحص السياق الأصلي للنشر، ومقارنة البيانات الوصفية بالمحتوى المرئي، والنظر في احتمالات التعديل أو إعادة النشر. كما ينبغي

التمييز بين المؤشرات التي تدعم فرضية معينة والقرائن التي تناقضها، بدلاً من الاقتصار على المعلومات التي تتفق مع التصور الأولي. [46]

ويجب مراعاة أن المحتوى المنشور قد يتغير أو يُحذف. ولذلك ينبغي توثيق المصدر ووقت الاطلاع وطريقة الحصول، والاحتفاظ بنسخة مناسبة للتحقق اللاحق متى كان ذلك مشروعاً. وإذا استُخدمت لقطات شاشة، فينبغي بيان طبيعة النسخة وما إذا كانت تحفظ جميع عناصر المحتوى الأصلي. [47]

أما **الحد القانوني** لاستخبارات المصادر المفتوحة، فيرتبط بأن وصف المصدر بأنه مفتوح لا يحسم مشروعية كل عملية معالجة. فقد يكون المحتوى متاحاً للجمهور، بينما تؤدي مراقبة صاحبه بصورة مستمرة أو تجميع معلوماته من مصادر متعددة إلى تدخل مختلف في خصوصيته. وقد تنطبق على بعض البيانات المنشورة قواعد خاصة تتعلق بحماية البيانات أو بحقوق الغير. لذلك يتعين الفصل بين **مشروعية الوصول** و**مشروعية الاستخدام** للغرض المحدد، مع مراعاة الاختصاص والضرورة والتناسب. [48]

وتخلص المعالجة إلى أن استخبارات المصادر المفتوحة تمثل وسيلة لإنتاج **معرفة قابلة للتحقق**، لا آلية لإضفاء اليقين على كل ما يُنشر رقمياً. وتظل موثوقية النتائج رهينة بسلامة إجراءات الجمع، واستقلال مصادر التحقق، والقدرة على اختبار الفرضيات البديلة، والالتزام بالإفصاح عن مواطن الشك. [49]

المبحث الثاني: جمع المعلومات المنشورة عبر الشبكات الاجتماعية

أصبحت الشبكات الاجتماعية مجالاً واسعاً لتداول المعلومات والصور ومقاطع الفيديو والبيانات المرتبطة بالأنشطة اليومية. وتتبع أهميتها من قدرتها على إظهار بعض الوقائع أو الروابط بين الحسابات والمحتويات. غير أن طبيعة هذه المنصات، التي تسمح بإعادة النشر والتعديل والاقتباس، تجعل جمع المعلومات منها عملية تتطلب التحقق من المصدر والسياق، لا الاكتفاء بمحتوى المنشور أو مدى انتشاره. [50]

وتختلف المعلومات المتاحة على الشبكات بحسب إعدادات الخصوصية، وطبيعة الحساب، ونوع المحتوى، وشروط المنصة. فقد يكون المنشور متاحاً للجميع، بينما يقتصر محتوى آخر على مجموعة محددة. ولا يجوز الخلط بين المعلومات المتاحة للعموم والمعلومات التي تتطلب الدخول إلى حساب خاص أو استخدام بيانات اعتماد لا يملك القائم بالتحري حق استخدامها أو تجاوز القيود التقنية. [51]

ويقتضي جمع المنشورات العامة تحديد الحساب، وتوثيق الرابط أو المعرف، وتسجيل تاريخ ووقت الاطلاع، وحفظ نسخة مناسبة، وتوثيق أي قيود حالت دون الوصول إلى السياق الكامل. كما ينبغي التمييز بين وقت النشر الظاهر ووقت الحصول على المحتوى، لأن الفرق بينهما قد يكون جوهرياً في إعادة بناء تسلسل الأحداث. [52]

وتظهر إحدى الصعوبات الرئيسية في تحديد العلاقة بين الحساب وصاحبه الحقيقي. فوجود اسم شخص أو صورته لا يكفي وحده لإثبات أن الشخص هو من أنشأه أو نشر المحتوى. وقد تستخدم الحسابات أسماء مستعارة، أو تنتحل هوية آخرين، أو تكون مشتركة بين عدة مستخدمين، أو تتعرض للاختراق. كما قد يعاد نشر محتوى صادر عن حساب آخر، بحيث لا يعكس النشر اللاحق موقف صاحب الحساب. [53]

ولذلك ينبغي أن تقوم نسبة الحساب إلى شخص على مجموعة من المؤشرات المتضافرة، مع تقييم كل مؤشر في ضوء مصدره واحتمالات الخطأ. وقد تشمل المؤشرات تاريخ الحساب، واتساق نشاطه، والروابط التي يعلنها صاحبه، والمحتوى المرتبط به من مصادر مستقلة، والإفادات أو السجلات التي يمكن التحقق منها بصورة مشروعة. ولا ينبغي اعتبار أي مؤشر منفرد حاسماً إذا كان يحتمل تفسيراً آخر. [54]

كذلك يجب مراعاة أن بيانات التفاعل (الإعجابات، إعادة النشر، التعليقات) لا تثبت بالضرورة موافقة الشخص على مضمون المنشور أو علمه بكل ما يتضمنه. فقد يكون التفاعل آلياً أو عرضياً أو منقولاً، كما قد تُنشأ بعض التفاعلات باستخدام حسابات غير حقيقية. ولذلك فإن الاستنتاج بشأن نية المستخدم يتطلب أدلة تتجاوز مجرد وجود تفاعل رقمي. [55]

وتثير الشبكات الاجتماعية مسألة مراقبة النشاط العام على نحو مستمر. فقد يختلف الأثر القانوني لجمع منشور منفرد يتعلق بواقعة محددة عن إنشاء سجل طويل الأمد يجمع تحركات شخص واتصالاته واهتماماته. ويقتضي هذا الاختلاف تقييم نطاق الجمع ومدته والغرض منه، وتحديد ما إذا كان الإجراء يحتاج إلى سند قانوني أو إذن خاص. [56]

كما ينبغي حماية بيانات **الأشخاص غير المستهدفين** الذين يظهرون في المنشورات أو التعليقات. فقد يتضمن منشور واحد بيانات شخصية لعدد كبير من الأفراد، أو يكشف عن معلومات حساسة لا صلة لها بموضوع البحث. ولا يبرر وجود هذه البيانات في محتوى منشور للعموم الاحتفاظ بها جميعاً أو إدراجها في التقرير دون ضرورة.[57]

ومن الناحية العملية، ينبغي تجنب الاعتماد على **لقطات الشاشة وحدها** متى أمكن حفظ المحتوى بطريقة تتيح التحقق من مصدره وسياقه. فلقطة الشاشة قد توثق ما ظهر في لحظة معينة، لكنها لا تثبت بمفردها هوية الناشر أو اكتمال المحتوى أو عدم تعديله. ولهذا يجب أن يُستكمل توثيقها بالمعلومات المتاحة عن الصفحة أو الحساب، وتاريخ الحصول، وطريقة الحفظ.[58]

ويُستفاد من **بروتوكول بيركلي** في هذا المجال من خلال مبادئ التحقق المنهجي من المحتوى الرقمي، وتوثيق مصدره وسياقه، والفصل بين المعلومات التي تمت ملاحظتها مباشرة والاستنتاجات المستخلصة منها.[59]

وبناءً على ذلك، ينبغي التعامل مع الشبكات الاجتماعية باعتبارها **مصادر غنية بالموشرات**، لكنها ليست مصادر معصومة من التضليل أو الخطأ. وتتحدد القيمة التحليلية للمحتوى بمدى إمكان التحقق من نسبته وسياقه، واستقلال مصادر تأييده، واتساقه مع المعلومات الأخرى.[60]

المبحث الثالث: التحقق من نسبة الحسابات والمحتوى إلى أصحابها

يمثل التحقق من نسبة الحسابات والمحتوى إلى أصحابها إحدى أكثر المسائل حساسية في التحريات القائمة على المصادر المفتوحة؛ لأن الخطأ في تحديد الهوية قد يؤدي إلى إسناد نشاط أو تصريح إلى شخص لم يصدر عنه فعلياً. وتتضاعف خطورة هذا الخطأ عندما تنتقل النتيجة من مرحلة الفرضية إلى التقرير الرسمي أو إلى إجراء قد يمس الحقوق.[61]

ويقتضي التحليل التمييز بين ثلاثة أمور مستقلة: **هوية الحساب الرقمي**، و**هوية الشخص الذي يتحكم فيه**، و**هوية الشخص الذي أنشأ المحتوى**. فقد يكون الحساب مسجلاً باسم شخص، لكن شخصاً آخر يديره؛ وقد يكون الحساب مملوكاً لشخص، بينما ينشر المحتوى موظف لديه صلاحية الدخول؛ وقد ينشر الحساب محتوى منقولاً لا يعكس رأي صاحبه أو معرفته المباشرة.[62]

ومن ثم، فإن مجرد تطابق الاسم الظاهر مع اسم الشخص المستهدف لا يكفي لإثبات النسبة. كما أن استخدام صورة شخصية أو معلومات عامة لا يحسم المسألة، لأن هذه المعلومات قد تكون متاحة للآخرين أو مستخدمة في انتحال الهوية. وينبغي توخي الحذر عند الاستناد إلى اللغة أو أسلوب الكتابة أو الاهتمامات المشتركة، إذ يمكن أن تدعم هذه المؤشرات فرضية معينة، لكنها لا تثبت الهوية بصورة قاطعة.[63]

ويستند التحقق المهني إلى **جمع مؤشرات متعددة**، وتقييم استقلالها، واختبار التفسيرات البديلة. فإذا ظهر حساب يستخدم اسم شخص وصورته، وكان مرتبطاً بموقع رسمي يعود إليه، فإن هذه الصلة قد تعزز فرضية النسبة، لكنها لا تغني عن فحص طبيعة الارتباط وتاريخه. وإذا أكد الحساب معلومات لا يعرفها عادة إلا الشخص المعني، فقد تكون قرينة مساعدة، لكن ينبغي النظر في احتمال أن تكون المعلومات قد نُشرت سابقاً أو حصل عليها طرف آخر.[64]

ويجب الفصل بين **التحقق من نسبة الحساب والتحقق من صحة المحتوى**. فقد يكون الحساب عائداً إلى الشخص، لكن المنشور يتضمن معلومات غير دقيقة أو رأياً أو نقلاً عن مصدر آخر. وبالمقابل، قد يكون المحتوى صحيحاً من حيث وصف الواقعة، مع تعذر تحديد الشخص الذي نشره أول مرة. ولذلك لا يجوز اعتبار نجاح أحد المسارين دليلاً تلقائياً على نجاح الآخر.[65]

وتتطلب عملية التحقق توثيق المؤشرات التي استُخدمت، ومصادرهما، وتاريخ الحصول عليها، والقيود التي تؤثر في دلالتها. كما ينبغي التمييز بين المؤشرات المستمدة من الحساب ذاته والمؤشرات التي تأكدت من مصدر مستقل؛ لأن الاعتماد على معلومات يكررها الحساب نفسه لا يمثل بالضرورة تأييداً مستقلاً لهوية صاحبه.[66]

وعند تعذر التحقق بدرجة كافية، يجب التعبير عن النتيجة بصياغة تعكس هذا القيد. فبدلاً من الجزم بأن شخصاً معيناً نشر المحتوى، يمكن بيان أن المحتوى نُشر عبر حساب يحمل اسماً أو صورة مرتبطة بذلك الشخص، مع توضيح أن الأدلة المتاحة لا تكفي وحدها لتأكيد هوية المستخدم الفعلي. ولا يُعد هذا التحفظ ضعفاً في التحليل، بل تطبيقاً لمبدأ **التناسب بين قوة النتيجة وقوة المعلومات**. [67]

وتبرز أهمية هذا المنهج عند استخدام المحتوى في تقارير أمنية أو إجراءات قانونية لاحقة. فكلما كان الاستنتاج المتعلق بالهوية مؤثراً في حقوق الشخص، ازدادت الحاجة إلى توثيق أسسه، وفحص البدائل، وإتاحة التحقق منه وفق الضوابط القانونية. ولا ينبغي أن يتحول الاشتباه في نسبة حساب إلى حقيقة ثابتة لمجرد تكرارها في تقارير لاحقة.[68]

وفي هذا السياق، يدعم **بروتوكول بيركلي** مبدأ توثيق مراحل التحقق الرقمي وبيان المنهج المستخدم والحدود التي تحيط بالنتائج. كما تؤكد المبادئ العامة للتحقيق الجنائي الرقمي أهمية المحافظة على المعلومات الأصلية وتوثيق إجراءات التعامل معها.[69]

المبحث الرابع: التحقق من الصور ومقاطع الفيديو وسياق نشرها

تُعد الصور ومقاطع الفيديو من أكثر أشكال المحتوى الرقمي تأثيراً في تكوين التصورات؛ لأنها تقدم تمثيلاً بصرياً قد يبدو مباشراً. غير أن هذه الطبيعة لا تجعلها دليلاً قاطعاً على صحة الرواية المصاحبة، إذ يمكن أن تكون الصورة أصلية لكنها قديمة، أو يكون التسجيل صحيحاً لكنه ملتقط في مكان مختلف، أو يُعرض جزء من المقطع بما يحجب أحداثاً تغير دلالاته.[70]

ويبدأ التحقق بتحديد **المادة محل الفحص ومصدر الحصول عليها**، ثم تحديد **الادعاء المراد اختباره**. فالسؤال عما إذا كانت صورة نُشرت في تاريخ معين يختلف عن السؤال عما إذا كانت الثُقُت في ذلك التاريخ، كما يختلف عن السؤال المتعلق بهوية الأشخاص الظاهرين. وكلما كان السؤال محدداً، أمكن اختيار وسائل تحقق أكثر ملاءمة.[71]

ومن الخطوات الأساسية **البحث عن أقدم ظهور معروف للمحتوى**، ومقارنة النسخ المتداولة، وفحص المعالم الظاهرة، والتحقق من توافق الظروف البيئية والزمنية مع الادعاء. وقد يساعد البحث عن الصور المتشابهة في كشف إعادة استخدام صورة قديمة، لكنه لا يثبت وحده تاريخ الالتقاط الأصلي.[72]

وتُعد **البيانات الوصفية** مصدراً مساعداً، إذ قد تتضمن معلومات عن الجهاز أو وقت الإنشاء أو الموقع. إلا أن وجودها أو غيابها لا يحسم صحة المحتوى. فقد تُحذف أثناء رفع الملف إلى منصة أو عند تحويله إلى صيغة أخرى، كما يمكن تعديل بعض الحقول. لذلك ينبغي تفسيرها في ضوء طريقة الحصول على الملف وتاريخ انتقاله بين الأنظمة ومدى اتساقها مع مصادر أخرى.[73]

كذلك يتعين التمييز بين **أصالة الملف ودقة تفسيره**. فقد يكون الملف لم يتعرض لتعديل، لكنه لا يثبت سوى جزء محدود من الواقعة. وقد يُظهر مقطع شخصاً في مكان معين، دون أن يثبت سبب وجوده أو طبيعة علاقته بالحدث. كما قد تظهر حركة تحتمل تفسيرات متعددة، الأمر الذي يمنع الانتقال من المشاهدة إلى استنتاج بشأن النية أو المسؤولية دون أدلة إضافية.[74]

ويكتسب **التحقق من السياق** أهمية خاصة عند التعامل مع مقاطع الفيديو المقطعة. فقد يؤدي حذف الثواني السابقة أو اللاحقة إلى تغيير فهم الحدث. ولهذا ينبغي، متى أمكن، الحصول على النسخة الأطول أو المصدر الأصلي، وتحديد ما إذا كانت النسخة محل الفحص كاملة أو مقطعة، وتوثيق أي اختلافات.[75]

أما **المحتوى المعدل أو المولد اصطناعياً**، فيثير تحديات إضافية. فقد تُنشأ صور أو تسجيلات باستخدام تقنيات الذكاء الاصطناعي، أو تُعدل مواد حقيقية لتغيير الوجوه أو الأصوات أو الخلفيات. ولا يصح التعامل مع جميع صور التعديل بوصفها نوعاً واحداً، لأن طبيعة التغيير ومداه يؤثران في الأسئلة الفنية اللازمة للتحقق.[76]

ويتطلب فحص المحتوى المحتمل اصطناعيته الجمع بين **التحليل البصري والسمعي**، وفحص خصائص الملف، والبحث عن النسخ الأصلية، والمقارنة بمصادر مستقلة، والاستعانة بأدوات فنية مناسبة. ومع ذلك، لا ينبغي اعتبار نتائج أدوات الكشف الآلي حكماً نهائياً؛ إذ قد تتأثر دقتها

بجودة الملف أو ضغطه أو نوع التقنية المستخدمة. كما أن غياب مؤشرات التلاعب لا يثبت بالضرورة أن المحتوى أصلي. [77]

ويجب مراعاة أن **الكشف عن التعديل** لا يساوي بالضرورة إثبات التضليل المتعمد. فقد تتعرض الصورة لمعالجة مشروعة لتحسين وضوحها، أو يُعاد ترميز الفيديو لأغراض النشر، أو تُحذف البيانات الوصفية دون قصد إخفاء المصدر. لذلك ينبغي التمييز بين إثبات وقوع تغيير تقني، وتحديد طبيعته، وتقييم أثره في الدلالة، واستنتاج الغرض منه. [78]

وتؤكد الأدبيات المهنية أهمية المحافظة على المحتوى الأصلي وتوثيق عمليات الاستخراج والمعالجة، مع بيان حدود النتائج. ويقدم **بروتوكول بيركلي** إطاراً منهجياً للتحقق من المحتوى الرقمي المنشور، في حين يقدم **دليل NIST** إطاراً فنياً عاماً لجمع البيانات وفحصها وتحليلها. [79]

ومن الناحية القانونية، يجب مراعاة **مشروعية الحصول** على المحتوى، وحقوق الأشخاص الظاهرين فيه، وحدود الاحتفاظ به أو مشاركته، ومدى صلاحيته للاستخدام في الإجراء المقصود. فصحة الملف فنياً لا تصح تلقائياً أي مخالفة قانونية في طريقة الحصول عليه، كما أن مشروعية الحصول لا تعني بالضرورة كفاية محتواه لإثبات الواقعة. [80]

وبناءً على ذلك، ينبغي أن يتضمن تقييم الصور ومقاطع الفيديو تحديداً واضحاً للدعاء محل الفحص، ووصفاً للمادة ومصدرها، وبياناً لإجراءات التحقق، ومقارنة بالمصادر المستقلة، وتحديداً لما أمكن إثباته وما بقي غير محسوم. وتظل النتيجة العلمية السليمة هي تلك التي لا تتجاوز حدود ما تسمح به المادة الرقمية. [81]

الفصل الثالث: توثيق جمع المعلومات ومصادرها

المبحث الأول: تحديد مصدر المعلومة وتاريخ الحصول عليها

يُعد تحديد مصدر المعلومة وتاريخ الحصول عليها من المتطلبات الأساسية لضمان إمكان التحقق من المعلومات الرقمية وتقييم موثوقيتها. فالمعلومة التي يتعذر تحديد مصدرها أو وقت الحصول عليها تثير صعوبات في التحقق من أصلها، وربطها بالسياق الزمني للواقعة، وإعادة فحص الظروف التي كانت متاحة عند جمعها. [82]

ويقصد بمصدر المعلومة الجهة أو النظام أو الوسيط الذي استُمدت منه البيانات مباشرة، مع التمييز بين المصدر المباشر والمصدر الذي نقل المحتوى عن غيره. فإذا عُثر على صورة في حساب أعاد نشرها، فلا يكفي تسجيل الحساب الأخير بوصفه مصدراً دون محاولة تحديد المصدر السابق. كما ينبغي التمييز بين الجهة التي أنشأت البيانات والجهة التي تحتفظ بها والجهة التي أتاحت النسخة المستخدمة. [83]

ويتطلب توثيق المصدر بيان المعلومات التي تسمح بالتعرف عليه دون لبس: اسم الموقع أو المنصة، والرابط، ومعرّف الحساب أو السجل، واسم النظام أو الجهاز، والجهة التي قدمت البيانات. وينبغي تجنب الاكتفاء بأوصاف عامة مثل "معلومات من الإنترنت" أو "بيانات من الهاتف"، لأنها لا توفر أساساً كافياً لإعادة التحقق. [84]

أما تاريخ الحصول، فيجب تمييزه عن تاريخ إنشائها أو نشرها أو تعديلها. فقد يكون تاريخ النشر الظاهر مختلفاً عن وقت إنشاء الملف، وقد يكون وقت الاستخراج مختلفاً عن وقت الواقعة. ولذلك ينبغي تسجيل كل تاريخ بحسب وظيفته، وعدم استخدام أحدها بدلاً من الآخر دون بيان. [85]

وتزداد أهمية هذا التمييز في الأنظمة التي تعتمد على مناطق زمنية مختلفة. فقد يظهر الحدث في سجل وفق توقيت النظام، بينما يعرضه نظام آخر وفق توقيت المستخدم المحلي. وقد يؤدي تجاهل هذا الاختلاف إلى ترتيب غير صحيح للأحداث. ومن ثم، يستحسن تسجيل المنطقة الزمنية متى كان مؤثراً في التحليل. [86]

ويقتضي التوثيق الجيد تسجيل تاريخ الحصول بطريقة تسمح بربطه بالإجراء الذي أُجري بشأنها. وقد يتطلب ذلك بيان اسم القائم بالجمع وصفته، ووسيلة الوصول، والأداة المستخدمة، وظروف الحصول، والنسخة التي حُفظت للتحليل. وإذا نُقلت البيانات من جهة أخرى، فينبغي تسجيل تاريخ التسليم والجهة المسلمة والمستلمة، مع مراعاة قواعد سرية المصدر وحماية البيانات. [87]

وتدعم المعايير المهنية هذا الاتجاه؛ إذ تشدد إرشادات الإنترنت على أهمية تعريف المواد الرقمية وتسجيل بياناتها وتوثيق انتقالها بين الأشخاص والجهات. كما يوضح مكتب الأمم المتحدة المعني بالمخدرات والجريمة أهمية تسجيل إجراءات التعامل مع البيانات منذ التعرف عليها وحتى حفظها وتحليلها. [88]

ومن الناحية القانونية، لا ينبغي أن يتحول التوثيق إلى وسيلة لجمع بيانات شخصية إضافية لا تتطلبها أغراض التحري. فالمقصود هو تسجيل المعلومات اللازمة لإثبات مصدر البيانات وإمكان التحقق منها، مع مراعاة مبدأ **تقليل البيانات** والقيود المتعلقة بالسرية. ويجب أن يتناسب مستوى التفصيل مع طبيعة المصدر وأهمية المعلومة. [89]

وعليه، فإن تحديد المصدر والتاريخ ليس مجرد إجراء شكلي، بل هو أساس يسمح بتقييم الموثوقية، وإعادة بناء مسار المعلومة، والتمييز بين المحتوى الأصلي والنسخ اللاحقة، واختبار مدى اتساق البيانات مع الوقائع الأخرى. [90]

المبحث الثاني: توثيق طريقة الجمع وظروفه وسنده القانوني

لا تكتمل القيمة المنهجية لتوثيق المعلومات الرقمية بتحديد مصدرها وتاريخ الحصول، بل تقتضي كذلك تسجيل **الطريقة التي جُمعت بها والظروف** التي أحاطت بالإجراء والأساس القانوني الذي استند إليه. فالمعلومة الواحدة قد تختلف دلالتها بحسب طريقة الحصول؛ إذ قد تُستخرج من مصدر عام، أو تُقدم من جهة مخولة، أو تُجمع في إطار إجراء يستلزم إذنًا، أو تُستخرج من نظام مقيد الوصول. [91]

ويُقصد بتوثيق طريقة الجمع تسجيل الإجراءات الفعلية التي اتُبعت للحصول على البيانات، بما يسمح بفهم كيفية انتقالها من المصدر إلى الجهة. ويشمل ذلك، بحسب طبيعة الإجراء، وسيلة الوصول، ومعايير البحث، ونطاق البيانات، والأدوات التقنية، وأي عمليات استخراج أو تحويل أو حفظ. [92]

ولا يُشترط أن تكون جميع الإجراءات متطابقة؛ فتوثيق منشور عام يختلف عن استخراج سجل من نظام مؤسسي، كما يختلف عن الحصول على بيانات من جهاز. لكن يجب أن يحقق التوثيق في جميع الحالات الغرض الأساسي: **تمكين شخص مؤهل من فهم ما جرى، وتحديد البيانات التي جُمعت، وتقييم أثر الطريقة في اكتمالها وسلامتها.** [93]

ويكتسب توثيق الظروف أهمية خاصة عندما تكون البيانات عرضة للتغير أو الفقد. فقد يتأثر محتوى صفحة بتعديل لاحق، أو تتغير حالة جهاز عند تشغيله، أو تُحذف سجلات وفق سياسة احتفاظ آلية. وفي هذه الحالات، ينبغي تسجيل الظروف ذات الصلة بالقدر الذي يسمح بتفسير النتائج. [94]

أما **السند القانوني**، فينبغي أن يُوثق بما يتناسب مع طبيعة الإجراء. فإذا استند الجمع إلى صلاحية عامة، وجب تحديد الأساس الذي يخول الجهة القيام به. وإذا كان الإجراء يتطلب إذنًا أو تصريحًا، فينبغي تسجيل الجهة التي أصدرته، وتاريخه، ونطاقه، ومدته، وأي شروط. ولا يكفي إثبات وجود إذن دون التحقق من مدى انطباقه على الإجراء الذي نُفذ فعلياً. [95]

وتبرز أهمية هذا التوثيق عند التمييز بين **جمع المعلومات المفتوحة والوصول إلى بيانات مقيدة**. فقد يكون الاطلاع على صفحة عامة جائزاً، بينما يتطلب الوصول إلى سجل اتصالات أو محتوى حساب خاص أساساً قانونياً إضافياً. كما أن الإذن بفحص وسيط معين لا يُفسر تلقائياً على أنه إذن غير محدود بالوصول إلى جميع البيانات والحسابات المرتبطة به. [96]

ويجب التمييز بين تسجيل الأساس القانوني وتقييم كفايته. فوجود إشارة في المحضر إلى مادة قانونية لا يثبت بذاته أن الإجراء مشروع؛ إذ تظل المسألة مرتبطة بصحة تفسير النص، واختصاص الجهة، وتحقيق الشروط، والتزام حدود الإذن. ولهذا ينبغي أن يكون التوثيق دقيقاً، وأن تُفصل الوقائع الإجرائية عن التقييم القانوني. [97]

وقد أكدت الإرشادات المهنية الدولية أهمية توثيق إجراءات الجمع والفحص والنسخ والحفظ، مع تسجيل الأشخاص الذين تعاملوا مع البيانات والوقت. ويُعد هذا التوثيق عنصراً أساسياً في المحافظة على سلامة البيانات وإمكان مراجعة الإجراءات اللاحقة. [98]

كما ينبغي تسجيل أي انحراف عن الإجراء المخطط أو البروتوكول المعتمد، مع بيان أسبابه وآثاره المحتملة. ولا يصح حذف الملاحظات المتعلقة بصعوبات تقنية أو أخطاء إجرائية لمجرد أنها قد تؤثر في تفسير النتائج؛ لأن إخفاءها يحول دون تقييم موضوعي. وفي المقابل، لا يعني وقوع انحراف أن جميع النتائج أصبحت عديمة القيمة تلقائياً. [99]

ومن منظور حماية الحقوق، يجب ألا يقتصر التوثيق على إثبات ما جُمع، بل ينبغي أن يسمح بتحديد ما إذا كان الجمع قد تجاوز الغرض المحدد أو شمل بيانات غير مرتبطة. ويمكن تحقيق ذلك من خلال تسجيل نطاق البحث، ومعايير اختيار البيانات، وحدود الوصول، والإجراءات المتخذة لحماية المعلومات العرضية. [100]

وعليه، فإن توثيق طريقة الجمع وظروفه وسننه القانوني يؤدي وظيفة مزدوجة: تعزيز إمكان التحقق الفني من مصدر المعلومات وسلامتها، وإتاحة مراجعة مشروعية الإجراء وحدوده. ولا يغني أحد الجانبين عن الآخر. [101]

المبحث الثالث: المحافظة على البيانات الأصلية والتمييز بينها وبين النسخ المعالجة

تُعد المحافظة على البيانات الأصلية والتمييز بينها وبين النسخ المعالجة من المبادئ الأساسية في التعامل مع المعلومات الرقمية، لما لذلك من أثر في التحقق من سلامة المحتوى، وإعادة فحص النتائج، وتحديد ما إذا كانت التغييرات قد أثرت في دلالتها. وتزداد الأهمية لأن البيانات الرقمية قابلة للنسخ والتحويل والتعديل بسرعة، وقد لا يكون التغيير ظاهراً عند الاطلاع العادي. [102]

ويقصد بالبيانات الأصلية المادة الرقمية التي تم الحصول عليها مباشرة من المصدر، وفق الطريقة المتاحة والمشروعة، مع مراعاة أن مفهوم "الأصل" قد يختلف باختلاف طبيعة النظام. فقد يكون الأصل ملفاً محفوظاً على وسيط، أو سجلاً في نظام بعيد، أو محتوى منشوراً على منصة، أو بيانات مستخرجة من جهاز وفق إجراء فني. ولهذا ينبغي بيان المقصود بالأصل في كل حالة. [103]

أما النسخة المعالجة، فهي نسخة أُجريت عليها عملية فنية أو تحريرية لغرض معين، مثل تحويل صيغة، أو استخراج مجموعة سجلات، أو تحسين وضوح صورة، أو ترتيب بيانات في جدول. وقد تكون المعالجة مشروعة وضرورية للتحليل، لكنها تظل خطوة مستقلة ينبغي توثيقها. [104]

ولا يعني الحفاظ على الأصل الامتناع عن أي معالجة، بل حماية المادة المرجعية وتجنب تغييرها دون ضرورة، مع إجراء الفحص على نسخة مناسبة متى أمكن. ويُراعى أن الحصول على البيانات أو قراءتها قد يغير بعض خصائص النظام؛ ولذلك ينبغي اختيار طريقة الاستخراج التي تتناسب مع طبيعة المصدر، وتوثيق أي تغيير يتعذر تجنبه. [105]

وتختلف متطلبات الحفاظ على الأصل باختلاف نوع البيانات. ففي الملفات المخزنة على وسيط مادي، قد يكون من المناسب إنشاء نسخة جنائية باستخدام أدوات ملائمة، والتحقق من تطابق القيم الرقمية بين المصدر والنسخة. أما المحتوى المنشور عبر الإنترنت، فقد يتعذر الحصول على نسخة مطابقة لجميع خصائص المصدر، ولا سيما عندما تتحكم المنصة في طريقة العرض أو تحذف بعض البيانات الوصفية. وفي هذه الحالة ينبغي توثيق طبيعة النسخة وحدودها. [106]

وتشمل المحافظة على الأصل حماية الملفات من التعديل غير المصرح به، وضبط صلاحيات الوصول، وتسجيل عمليات النسخ والنقل والمعالجة، وحفظ نسخ مناسبة عند الحاجة. كما ينبغي أن تكون تسمية الملفات وتنظيمها واضحين بما يمنع الخلط بين المادة الأصلية والنسخ الناتجة عن التحليل. [107]

ومن الضروري توثيق كل عملية معالجة ذات أثر محتمل في تفسير البيانات. فإذا عُذلت صورة لتحسين وضوحها، فينبغي حفظ النسخة غير المعالجة متى أمكن، وتحديد طبيعة التعديل والغرض منه. وإذا حُولت صيغة ملف أو استُخرجت مجموعة فرعية من قاعدة بيانات، فينبغي تسجيل الأداة أو الطريقة المستخدمة، ومعايير الاختيار، وأي معلومات قد تكون فُقدت. [108]

ويؤكد دليل NIST أهمية الفصل بين جمع البيانات وفحصها وتحليلها وإعداد التقارير، بما يساعد على فهم المراحل التي مرت بها المعلومات. كما تتضمن إرشادات الإنترنت مبادئ عملية لتحديد المواد الرقمية وتوثيقها والمحافظة عليها. [109]

ومن الناحية القانونية، ينبغي أن تُراعى عند الاحتفاظ بالنسخ الأصلية والمعالجة قواعد السرية وحماية البيانات وتحديد الغرض. فلا تعني الحاجة الفنية إلى الاحتفاظ بالبيانات أن الاحتفاظ بجميع محتوياتها مسموح إلى أجل غير محدد، كما لا تبرر المحافظة على نسخة مرجعية إتاحتها لجميع العاملين. [110]

ويترتب على هذا التمييز أن كل نتيجة مستخلصة من نسخة معالجة يجب أن تكون قابلة للربط بالمادة التي اشتُقت منها، مع توضيح الخطوات التي أدت إليها. فإذا تعذر هذا الربط، فقد يصعب التحقق من أن النتيجة تعكس البيانات الأصلية. ولا يعني ذلك أن كل معالجة تقلل بالضرورة من القيمة الفنية، بل إن أثرها يتوقف على طبيعتها ومدى توثيقها وإمكان إعادة تنفيذها. [111]

وعليه، فإن المحافظة على الأصل والتمييز بينه وبين النسخ المعالجة ليسا مجرد احتياطين فنيين، بل يمثلان شرطين لتعزيز الشفافية وقابلية المراجعة. وتظل قيمة النسخة المعالجة مرتبطة بوضوح مصدرها، وتوثيق التغييرات، وإمكان التحقق من أن تلك التغييرات لم تؤد إلى تحريف المعنى. [112]

المبحث الرابع: تسجيل القيود التي تؤثر في تفسير المعلومات

لا يكتمل توثيق جمع المعلومات الرقمية بتسجيل المصدر وطريقة الحصول والبيانات المحفوظة، بل يتطلب أيضاً تحديد القيود التي قد تؤثر في تفسيرها أو في مدى الاعتماد عليها. فقد تكون المعلومة متاحة ومثبتة المصدر، لكنها ناقصة أو مجتزأة أو غير دقيقة زمنياً أو مستمدة من نظام لا يسجل جميع الأحداث. وإذا لم تُذكر هذه القيود، فقد تُفهم النتيجة على أنها أكثر يقيناً مما تسمح به البيانات.[113]

ويُقصد بالقيود المؤثرة كل عامل يتعلق بالمصدر أو المحتوى أو طريقة الجمع أو المعالجة أو السياق، من شأنه أن يحد من إمكان استخلاص نتيجة معينة أو يؤثر في درجة الثقة. وقد تكون تقنية (فقدان بيانات وصفية، انخفاض جودة)، أو منهجية (الاعتماد على مصدر واحد)، أو زمنية (عدم وضوح وقت الإنشاء)، أو قانونية (تعذر الوصول إلى جزء من البيانات).[114]

ويجب التمييز بين نقص البيانات وعدم صحة البيانات. فعدم توافر بعض السجلات لا يعني أن السجلات الموجودة خاطئة، لكنه قد يمنع التوصل إلى استنتاج شامل. كما أن عدم ظهور حدث في سجل إلكتروني لا يثبت بالضرورة عدم وقوعه، ما لم يكن النظام مصمماً لتسجيل ذلك الحدث على نحو منتظم ويمكن إثبات اكتمال السجل.[115]

ويظهر ذلك في سجلات الدخول إلى الأنظمة. فإذا لم يتضمن السجل عملية دخول معينة، فقد يرجع ذلك إلى عدم وقوعها، أو إلى أن النظام لم يسجلها، أو إلى انتهاء مدة الاحتفاظ، أو إلى خلل في إعدادات التسجيل. ولا يمكن ترجيح أحد هذه الاحتمالات دون فحص خصائص النظام وظروفه التشغيلية.[116]

كما ينبغي تسجيل القيود المرتبطة بالمحتوى المنشور. فقد يتعذر الوصول إلى المنشور الأصلي، أو تكون النسخة المتاحة صورة مقتطعة، أو لا تتوافر معلومات كافية عن تاريخ الالتقاط. وفي هذه الحالات، يجب بيان ما أمكن التحقق منه تحديداً، وما بقي مستنداً إلى افتراض أو معلومة غير مؤكدة.[117]

وتتطلب الممارسة العلمية التمييز بين القيود التي تؤثر في أصل المعلومة والقيود التي تؤثر في تفسيرها. فقد تكون سلامة الملف مؤكدة بدرجة عالية، بينما يظل معنى المحتوى محل خلاف. وقد تكون هوية الناشر معروفة، لكن لا يمكن التحقق من تاريخ الواقعة. ويؤدي الفصل بين هذه المستويات إلى تجنب تعميم الشك في عنصر واحد على جميع العناصر.[118]

ومن المهم تسجيل القيود الناتجة عن أدوات التحليل. فقد تعتمد بعض الأدوات على نماذج أو خوارزميات لا تكشف جميع خطواتها، أو تكون نتائجها حساسة لجودة المدخلات. وفي هذه الحالة ينبغي بيان طبيعة الأداة، والغرض، والقيود المعروفة، ومدى مراجعة النتائج بصورة مستقلة.[119]

ويؤكد مكتب الأمم المتحدة المعني بالمخدرات والجريمة أهمية توثيق مراحل الجمع والتحليل والإبلاغ، وبيان القيود المعروفة ومواطن عدم اليقين حتى لا تُمنح النتائج وزناً غير مناسب. كما يدعم بروتوكول بيركلي ضرورة التمييز بين الوقائع التي أمكن التحقق منها والاستنتاجات التي تعتمد على تفسير المحتوى.[120]

ويجب أن تُصاغ القيود بلغة محددة، بدلاً من عبارات عامة مثل "قد تكون هناك أخطاء" دون بيان طبيعتها. فالأدق توضيح أن وقت إنشاء الملف لم يتسن التحقق منه بصورة مستقلة، أو أن النسخة المتاحة لا تتضمن التسجيل الكامل، أو أن نسبة الحساب إلى الشخص لم تثبت بأدلة مستقلة. [121]

كما ينبغي أن تنعكس القيود في الاستنتاج النهائي. فإذا كانت المعلومات لا تسمح بالجزم بواقعة معينة، فلا يصح استخدام لغة قطعية لمجرد أن بعض المؤشرات تتفق مع فرضية التحري. وإذا أمكن إثبات جانب من الواقعة دون جانب آخر، فيجب فصل النتيجة. [122]

ولا يقتصر الإفصاح عن القيود على حماية الدقة العلمية، بل يعزز المساءلة؛ إذ يتيح للجهات المختصة تقييم النتائج على أساس واضح، ويمكن المراجع من تحديد المسائل التي تحتاج إلى استكمال التحقق. كما يمنع تحويل المعلومات الأولية إلى استنتاجات نهائية من خلال حذف التفاصيل التي تحد من قوتها. [123]

وبناءً على ذلك، فإن توثيق القيود ليس عنصراً ثانوياً يضاف إلى التقرير بعد اكتمال التحليل، بل هو جزء من عملية إنتاج النتيجة ذاتها. فكلما كان القائم بالتحري أكثر وضوحاً بشأن ما لا تثبته البيانات، ازدادت إمكانات تقييم ما تثبته فعلاً، وتحسنت قابلية النتائج للمراجعة. [124]

الجدول المقارن: مصادر المعلومات الرقمية ودرجة الموثوقية والضمانات

القيود النموذجية	الضمانات المطلوبة	درجة الموثوقية الأولية	المصدر
إعادة النشر، نقص السياق، التضليل، التزييف	التحقق من المصدر والسياق، البحث عن أصل المحتوى، مقارنة بمصادر مستقلة	متوسطة إلى منخفضة (تتفاوت)	المصادر المفتوحة
أخطاء إدخال، تقادم، اختلاف إعدادات الاستعلام	التحقق من الجهة المنشئة، تاريخ التحديث، توثيق الاستخراج	متوسطة إلى مرتفعة (بحسب الجهة)	السجلات وقواعد البيانات
مصلحة مقدمها، نقل عن الغير، تكرار رواية واحدة	التحقق من الاستقلال، فصل المشاهدة عن التفسير، توثيق الظروف	منخفضة إلى متوسطة	المعلومات المقدمة من الأفراد
إعدادات خاطئة، فقدان بيانات، تغيير أثناء الفحص	سلسلة العهدة، توثيق النسخ، التحقق من التوقيت	متوسطة (بحسب سلامة الاستخراج)	المعلومات من الأجهزة والأنظمة

اقتطاع، إعادة استخدام، تعديل، توليد اصطناعي	البحث عن أصل الملف، فحص البيانات الوصفية، تحليل السياق	متوسطة إلى منخفضة	المحتوى البصري (صور/فيديو)
انتحال هوية، حسابات مشتركة، تفاعل آلي	مؤشرات متضادة، فصل الحساب عن الشخص، توثيق التفاعل	منخفضة إلى متوسطة	الحسابات على الشبكات الاجتماعية

❖ النافذة التطبيقية

السيناريو: تلقت جهة أمنية بلاغاً عن حساب على منصة اجتماعية يرّوج لمحتوى يمس الأمن العام، مرفقاً بصورة يُقال إنها التُقطت في موقع حادث.

- **الخطوة الأولى (المصدر):** تحديد الحساب، وتوثيق الرابط، وتاريخ الاطلاع، وحفظ نسخة من المنشور والصورة.
- **الخطوة الثانية (التحقق من النسبة):** لا يكفي اسم الحساب أو صورته؛ يُبحث عن مؤشرات متضادة (تاريخ الحساب، روابط خارجية، تأكيد من مصادر مستقلة).
- **الخطوة الثالثة (التحقق من الصورة):** البحث عن أقدم ظهور لها، فحص البيانات الوصفية، مقارنة المعالم الجغرافية، التحقق من تطابق الظروف الزمنية.
- **الخطوة الرابعة (السياق):** فحص ما إذا كانت الصورة مقتطعة أو معاد استخدامها، وما إذا كان التعليق المصاحب مضللاً.
- **الخطوة الخامسة (القيود):** تسجيل ما لم يتم التحقق منه (مثلاً: تاريخ الالتقاط غير مؤكد، نسبة الحساب غير محسومة).
- **الدرس:** المصدر المفتوح مؤشر لا دليل؛ والتحقق عملية متعددة المستويات، والقيود يجب أن تُعلن لا تُخفى.

النتائج العامة للباب

١. المصادر المفتوحة ليست فئة متجانسة؛ تتفاوت في الموثوقية بحسب الجهة المنتجة والسياق.
٢. إتاحة المحتوى للعموم لا تعني مشروعية جمعه وربطه وتحليله بصورة مستمرة.
٣. السجلات وقواعد البيانات تتطلب فحص الجهة المنشئة، وآلية الإنشاء، والحدثة، والسلامة.

٤. المعلومات المقدمة من الأفراد تتطلب التمييز بين صدق الشخص ودقة المعلومة، والتحقق من استقلال المصادر.
٥. البيانات الآلية ليست معصومة من الخطأ؛ وتحديد مصدرها يسبق تقييم دلالتها.
٦. OSINT عملية منهجية، لا مجرد بحث؛ ووصف المصدر بأنه مفتوح لا يحسم مشروعية المعالجة.
٧. نسبة الحسابات إلى أصحابها تتطلب مؤشرات متضاربة، ولا تكفي التشابهات الظاهرة.
٨. التحقق من الصور والفيديو يتطلب فحص الأصل والسياق والبيانات الوصفية، مع الحذر من التوليد الاصطناعي.
٩. توثيق المصدر والتاريخ والطريقة والسند القانوني شرط لتحقيق المشروعية وقابلية المراجعة.
١٠. المحافظة على الأصل والتمييز بينه وبين النسخ المعالجة ضرورة للشفافية.
١١. تسجيل القيود جزء من إنتاج النتيجة، لا إضافة لاحقة.
١٢. الجمع بين المعايير الدولية والفقه العربي والتشريع الوطني ضروري لبناء إطار متكامل.

المراجع:

- (1) انظر: OHCHR & UC Berkeley, *Berkeley Protocol on Digital Open Source Investigations*, 2022, at 15-18.
- (2) انظر: المرجع السابق، at 20-22.
- (3) المرجع السابق، at 10-14.
- (4) انظر: عادل عبد العال خراشي، *ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي*، ٢٠٠٦، ص ٩٠-٩٥.
- (5) انظر: Berkeley Protocol, *supra* note 1, at 25-28.
- (6) انظر: مفوضية الأمم المتحدة السامية لحقوق الإنسان، A/HRC/51/17، ٢٠٢٢، الفقرات ٢٠-٢٥.
- (7) الأمم المتحدة، العهد الدولي الخاص بالحقوق المدنية والسياسية، ١٩٦٦، المادة ١٧.
- (8) انظر: Berkeley Protocol, *supra* note 1, at 30-32.
- (9) انظر: المرجع السابق، at 35-38.
- (10) انظر: هشام مصطفى محمد، *التحريات الأمنية وأثرها في الأدلة الجنائية*، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٥، ص ٧٥-٧٠.
- (11) انظر: المرجع السابق، ص ٧٥-٨٠.
- (12) انظر: محمد محمد سيف شجاع، *شرح قانون الإجراءات الجزائية اليمني*، مكتبة الصادق، صنعاء، ٢٠٠٥، (الفصل الخاص بالتحريات).
- (13) انظر: Kent et al., *Guide to Integrating Forensic Techniques into Incident Response*, NIST SP 800-86, 2006, at 3-1.
- (14) انظر: هشام مصطفى، مرجع سابق، ص ٨٠-٨٥.
- (15) انظر: شجاع، مرجع سابق.
- (16) انظر: A/HRC/51/17، مرجع سابق، الفقرة ٢٨.

- (17) انظر. NIST SP 800-86, *supra* note 13, at 3-2.
- (18) المرجع السابق، at 1-1.
- (19) انظر: هشام مصطفى، مرجع سابق، ص ٨٥-٩٠.
- (20) انظر: شجاع، مرجع سابق.
- (21) انظر: خراشي، مرجع سابق، ص ١٠٠-١٠٥.
- (22) انظر: هشام مصطفى، مرجع سابق، ص ٩٠-٩٥.
- (23) انظر. Berkeley Protocol, *supra* note 1, at 30-32.
- (24) انظر: شجاع، مرجع سابق.
- (25) انظر A/HRC/51/17، مرجع سابق، الفقرة ٢٩.
- (26) انظر: المرجع السابق، الفقرة ٣٠.
- (27) انظر. INTERPOL, *Guidelines for Digital Forensics First Responders*, at 10-12.
- (28) المرجع السابق، at 12-15.
- (29) انظر: خراشي، مرجع سابق، ص ١١٠-١١٥.
- (30) انظر. NIST SP 800-86, *supra* note 13, at 2-1.
- (31) المرجع السابق، at 2-2.
- (32) انظر: هشام مصطفى، مرجع سابق، ص ١٠٥-١٠٠.
- (33) انظر. Ayers et al., *Guidelines on Mobile Device Forensics*, NIST SP 800-101 Rev.1, 2014, at 2-1.
- (34) المرجع السابق، at 2-2.
- (35) انظر. NIST SP 800-86, *supra* note 13, at 4-1.
- (36) UNODC, *Cybercrime Module 6: Handling of Digital Evidence*, 2019.
- (37) انظر A/HRC/51/17، مرجع سابق، الفقرة ٣٨.
- (38) المرجع السابق، الفقرة ٢٩.
- (39) انظر. Ayers et al., *supra* note 33, at 6-1.
- (40) انظر. Berkeley Protocol, *supra* note 1, at 15-18.
- (41) المرجع السابق، at 20-22.
- (42) المرجع السابق، at 10-14.
- (43) المرجع السابق، at 25-28.
- (44) المرجع السابق، at 30-32.
- (45) المرجع السابق، at 35-38.
- (46) المرجع السابق، at 40-42.
- (47) المرجع السابق، at 45-48.
- (48) انظر A/HRC/51/17، مرجع سابق، الفقرة ٢٥.
- (49) انظر. Berkeley Protocol, *supra* note 1, at 50-52.
- (50) المرجع السابق، at 55-58.
- (51) المرجع السابق، at 60-62.
- (52) المرجع السابق، at 65-68.
- (53) المرجع السابق، at 70-72.
- (54) المرجع السابق، at 75-78.
- (55) المرجع السابق، at 80-82.
- (56) انظر A/HRC/51/17، مرجع سابق، الفقرة ٢٦.
- (57) المرجع السابق، الفقرة ٢٩.
- (58) انظر. Berkeley Protocol, *supra* note 1, at 85-88.
- (59) المرجع السابق، at 90-92.
- (60) المرجع السابق، at 95-98.
- (61) المرجع السابق، at 100-102.
- (62) المرجع السابق، at 105-108.
- (63) المرجع السابق، at 110-112.
- (64) المرجع السابق، at 115-118.
- (65) المرجع السابق، at 120-122.

- (66) انظر: المرجع السابق، at 125-128.
- (67) انظر: المرجع السابق، at 130-132.
- (68) انظر: المرجع السابق، at 135-138.
- (69) المرجع السابق، at 140-142، at 10-12، INTERPOL, *supra* note 27،
- (70) انظر. Berkeley Protocol, *supra* note 1، at 145-148.
- (71) انظر: المرجع السابق، at 150-152.
- (72) انظر: المرجع السابق، at 155-158.
- (73) انظر: المرجع السابق، at 160-162.
- (74) انظر: المرجع السابق، at 165-168.
- (75) انظر: المرجع السابق، at 170-172.
- (76) انظر: المرجع السابق، at 175-178.
- (77) انظر: المرجع السابق، at 180-182.
- (78) انظر: المرجع السابق، at 185-188.
- (79) المرجع السابق، at 190-192، at 1-1، NIST SP 800-86, *supra* note 13،
- (80) انظر A/HRC/51/17، مرجع سابق، الفقرة ٣٨.
- (81) انظر. Berkeley Protocol, *supra* note 1، at 195-198.
- (82) انظر. INTERPOL, *supra* note 27، at 10-12.
- (83) انظر: المرجع السابق، at 12-15.
- (84) انظر: المرجع السابق، at 15-18.
- (85) انظر: المرجع السابق، at 18-20.
- (86) انظر. NIST SP 800-86, *supra* note 13، at 3-3.
- (87) انظر. INTERPOL, *supra* note 27، at 20-22.
- (88) المرجع السابق، at 22-25، UNODC, *supra* note 36،
- (89) انظر A/HRC/51/17، مرجع سابق، الفقرة ٢٨.
- (90) انظر. INTERPOL, *supra* note 27، at 25-28.
- (91) انظر: المرجع السابق، at 28-30.
- (92) انظر. NIST SP 800-86, *supra* note 13، at 4-2.
- (93) انظر. INTERPOL, *supra* note 27، at 30-32.
- (94) انظر: المرجع السابق، at 32-35.
- (95) انظر: شجاع، مرجع سابق.
- (96) انظر A/HRC/51/17، مرجع سابق، الفقرة ٢٧.
- (97) انظر: خراشي، مرجع سابق، ص ١٢٠-١٢٥.
- (98) انظر. INTERPOL, *supra* note 27، at 35-38، UNODC, *supra* note 36،
- (99) انظر. INTERPOL, *supra* note 27، at 38-40.
- (100) انظر: المرجع السابق، at 40-42.
- (101) انظر. NIST SP 800-86, *supra* note 13، at 4-3.
- (102) انظر: المرجع السابق، at 4-4.
- (103) انظر. Ayers et al., *supra* note 33، at 3-1.
- (104) انظر: المرجع السابق، at 3-2.
- (105) انظر. NIST SP 800-86, *supra* note 13، at 4-5.
- (106) انظر. Ayers et al., *supra* note 33، at 3-3.
- (107) انظر: المرجع السابق، at 3-4.
- (108) انظر. NIST SP 800-86, *supra* note 13، at 4-6.
- (109) المرجع السابق، at 4-7، at 40-42، INTERPOL, *supra* note 27،
- (110) انظر A/HRC/51/17، مرجع سابق، الفقرة ٢٨.
- (111) انظر. Ayers et al., *supra* note 33، at 3-5.
- (112) انظر. NIST SP 800-86, *supra* note 13، at 4-8.
- (113) انظر. UNODC, *supra* note 36.
- (114) انظر: المرجع السابق.

- (115) انظر. NIST SP 800-86, *supra* note 13, at 4-9.
- (116) انظر: المرجع السابق، at 4-10.
- (117) انظر. Berkeley Protocol, *supra* note 1, at 45-48.
- (118) انظر: المرجع السابق، at 50-52.
- (119) انظر. NIST SP 800-86, *supra* note 13, at 4-11.
- (120) المرجع السابق، at 4-12؛ Berkeley Protocol, *supra* note 1, at 55-58.
- (121) انظر. INTERPOL, *supra* note 27, at 40-42.
- (122) انظر. Berkeley Protocol, *supra* note 1, at 60-62.
- (123) انظر A/HRC/51/17:، مرجع سابق، الفقرة ٤٥.
- (124) انظر. UNODC, *supra* note 36.

الفصل الثاني: وسائل الرصد الرقمي والحصول على البيانات المقيدة

المبحث الأول: الإطار المفاهيمي والقانوني لوسائل الرصد الرقمي

المطلب الأول: مفهوم الرصد الأمني الرقمي وخصائصه

يُقصد بالرصد الأمني الرقمي مجموعة الإجراءات والأنشطة التي تُستخدم فيها الوسائل التقنية لمتابعة الوقائع أو الأنشطة أو التحركات ذات الصلة بمهمة أمنية مشروعة، من خلال مشاهدة البيانات الرقمية أو جمعها أو تسجيلها أو تحليلها، بقصد التحقق من معلومات سابقة، أو الكشف عن أنماط سلوكية ذات دلالة أمنية، أو تحديد عناصر واقعة محل اهتمام الجهات المختصة. [1]

ويشمل ذلك، بحسب طبيعة المهمة والأساس القانوني، مراقبة التسجيلات المرئية، وفحص السجلات الإلكترونية، وتحليل بيانات الاتصالات، والاستفادة من أنظمة تحديد المواقع، والوصول إلى بيانات الأجهزة والأنظمة وفق الإجراءات المقررة قانوناً.

ولا يتحدد مفهوم الرصد بالأداة المستخدمة وحدها، وإنما بطبيعة النشاط المنفذ، والغرض الذي يسعى إلى تحقيقه، ومدى تدخله في الحقوق، والجهة التي تباشره، والسند القانوني. فقد يكون الرصد مجرد مشاهدة لتسجيل متاح بصورة مشروعة، وقد يتخذ صورة جمع منتظم للمعلومات عن شخص معين، وقد يتطور إلى اعتراض الاتصالات أو تتبع تحركات الأفراد. وهذه الصور، وإن اشتركت في توظيف الوسائل الرقمية، تختلف من حيث درجة تدخلها في الخصوصية والضمانات المطلوبة. [2]

وتكمن أهمية هذا التمييز في أن وصف الإجراء بأنه "رصد رقمي" لا يكفي بذاته لتحديد حكمه القانوني؛ إذ لا يمكن التسوية بين الاطلاع العرضي على معلومات منشورة وبين اعتراض اتصال خاص، أو بين مراجعة تسجيل مرئي جُمع وفق الأطر القانونية وبين إنشاء نظام مستمر لتتبع تحركات الأشخاص. فالعبرة ليست بالتسمية الفنية، وإنما بحقيقة الإجراء وآثاره ومدى مساهمته بالحقوق المحمية. [3]

ويستند هذا التصور إلى المادة السابعة عشرة من العهد الدولي الخاص بالحقوق المدنية والسياسية، التي تحظر التدخل التعسفي أو غير القانوني في الخصوصية والأسرة والمسكن والمراسلات. وتترتب على ذلك نتيجة مهمة: مشروعية الرصد لا تُستمد من فائدته الأمنية المجردة، بل تتطلب أساساً قانونياً يحدد الحالات التي يجوز فيها استخدامه، والسلطات المختصة، والحدود التي لا يجوز تجاوزها. [4]

خصائص الرصد الأمني الرقمي:

١. **الجمع المستمر والمتراكم:** تتيح الوسائل الرقمية جمع المعلومات بصورة متكررة وربط البيانات التي جُمعت في أوقات مختلفة، مما قد يؤدي إلى تكوين صورة تفصيلية عن تحركات الفرد وعلاقاته. ولا تقتصر أهمية هذه الخاصية على زيادة القدرة على الكشف، بل تمتد إلى زيادة المخاطر المرتبطة بالخصوصية؛ فالمعلومات التي تبدو محدودة الدلالة منفردة قد تكتسب حساسية مرتفعة عند تجميعها. ومن ثم، ينبغي تقييم المشروعية بالنظر إلى أثر العملية في مجموعها. [5]

٢. **الربط بين مصادر متعددة:** يسمح الرصد بمقارنة المعلومات المستمدة من كاميرات المراقبة وسجلات الأنظمة وبيانات الموقع والمصادر المفتوحة. غير أن تعدد المصادر لا يعني بالضرورة تعدد الأدلة المستقلة؛ فقد تستند عدة قواعد بيانات إلى مصدر أصلي واحد. ولذلك يجب التمييز بين كثرة البيانات وتعدد مصادرها الحقيقية. [6]

٣. **المعالجة الآلية:** يمكن استخدام البرمجيات في تصنيف التسجيلات والبحث داخل السجلات ومقارنة البيانات واكتشاف الأنماط. وتوفر هذه الوسائل الوقت والجهد، لكنها لا تضمن صحة النتيجة تلقائياً؛ لأن المخرجات قد تتأثر بجودة البيانات وطريقة إعداد النظام والأخطاء التقنية أو التحيزات الكامنة. ويجب التمييز بين ما تنتجه الأداة تقنياً وما يمكن إثباته موضوعياً. [7]

٤. **تفاوت درجات التدخل:** لا تتمتع جميع صور الرصد بالمستوى نفسه من الخطورة. فمشاهدة تسجيل قد تختلف عن المراقبة المستمرة لشخص بعينه، كما أن جمع بيانات الاتصالات قد يثير اعتبارات مختلفة عن الاطلاع على محتوى الاتصال. ويقتضي هذا التفاوت اعتماد تقييم متدرج يراعي طبيعة البيانات ومدة الرصد وعدد الأشخاص المتأثرين وإمكان إعادة الاستخدام. [8]

وقد أبرزت المحكمة الأوروبية لحقوق الإنسان، في قضية *Big Brother Watch and Others v. the United Kingdom* (2021)، أهمية الضمانات المتكاملة التي تحكم مراحل المراقبة، بدءاً من الإذن بها، مروراً بجمع المعلومات وفحصها، وانتهاءً بالاحتفاظ بها وتبادلها. وتكشف هذه المقاربة أن تقييم المشروعية لا ينبغي أن ينحصر في لحظة إصدار الإذن، بل يجب أن يشمل دورة التعامل مع المعلومات بأكملها. [9]

٥. **إمكان فصل الجمع عن التفسير:** قد يقتصر الإجراء على جمع البيانات وتسجيلها، في حين تُحال مهمة تحليلها إلى جهة فنية أو محلل آخر. ويترتب على ذلك ضرورة الفصل بين سلامة عملية الجمع وصحة التفسير اللاحق؛ فقد تكون البيانات قد جُمعت بصورة مشروعة، لكن تفسيرها يكون غير دقيق. [10]

ومن ثم، فإن الرصد الأمني الرقمي عملية مركبة تتداخل فيها اعتبارات الاختصاص والمشروعية والخصوصية، مع اعتبارات سلامة البيانات ودقة التحليل. ولا تتحقق فعاليتها القانونية بمجرد القدرة على الوصول إلى المعلومات، بل بوجود ضمانات تحول دون إساءة استخدامها. [11]

المطلب الثاني: تصنيف وسائل الرصد وفق طبيعتها التقنية ونطاق استخدامها

يتطلب التصنيف العلمي لوسائل الرصد الرقمي اعتماد معايير متعددة؛ لأن التصنيف القائم على أسماء الأجهزة أو التطبيقات لا يكشف، وحده، طبيعة الإجراء القانونية ولا درجة تدخله في الحقوق. فقد تُستخدم الأداة التقنية نفسها لأغراض مختلفة، وقد يتفاوت الحكم القانوني على استخدامها بحسب نطاق المهمة وطريقة جمع البيانات. [12]

أولاً: التصنيف بحسب طبيعة البيانات محل الرصد:

- وسائل الرصد البصري: كاميرات المراقبة والتسجيلات المرئية والصور الثابتة، وما يرتبط بها من تقنيات تحليل الصور. [13]
- وسائل رصد الاتصالات: الإجراءات المتعلقة بالحصول على بيانات الاتصالات أو اعتراض محتواها، متى أجاز القانون ذلك. ويجب التمييز بين بيانات المشترك، وبيانات حركة الاتصال، وبيانات الموقع، ومحتوى الاتصال؛ لأن اختلاف طبيعة كل فئة يترتب عليه اختلاف مستوى الحماية. [14]
- وسائل الرصد المرتبطة بالموقع والحركة: البيانات الناتجة عن أنظمة تحديد المواقع وسجلات الحركة. وتحتاج إلى تقييم دقيق؛ لأن وجود الجهاز في موقع لا يثبت بالضرورة وجود مالكه فيه. [15]
- وسائل رصد الأنظمة والأجهزة: مراجعة السجلات الإلكترونية وسجلات الدخول والتشغيل. وقد تساعد في تحديد وقت وقوع نشاط تقني، لكنها لا تثبت دائماً هوية الشخص الطبيعي. [16]
- وسائل الرصد المعتمدة على التحليل الآلي: الأنظمة التي تصنف البيانات أو تكتشف الأنماط. ويجب تقييمها بالنظر إلى نوع المدخلات، ومنهج المعالجة، ومعدل الخطأ، وقابلية تفسير المخرجات. [17]

ثانياً: التصنيف بحسب طريقة الحصول على المعلومات:

- الرصد القائم على مشاهدة معلومات متاحة بصورة مشروعة.
 - الرصد الذي يعتمد على الحصول على بيانات محفوظة لدى جهة أخرى.
 - الرصد الذي يتضمن جمعاً مستمراً أو اعتراضاً للاتصالات. [18]
- ففي الصورة الأولى، قد تتمثل العملية في مراجعة تسجيل مرئي متاح أو الاطلاع على سجل عام. ومع ذلك، لا يعني إتاحة المعلومة الاطمئنان إلى مشروعية جميع أوجه استخدامها؛ إذ قد تخضع إعادة نشرها أو ربطها ببيانات شخصية لضوابط مستقلة. أما الصورة الثانية، فتتعلق بالحصول على بيانات لدى مقدم خدمة أو مؤسسة. وهنا لا يكفي أن تكون الجهة الحائزة قادرة تقنياً على تسليمها؛ بل يجب التحقق من سلطة طالبتها، والأساس القانوني للطلب، ونطاق المعلومات المطلوبة. وتنقسم الصورة الثالثة بارتفاع احتمال التدخل في الخصوصية، وهو ما يستدعي ضمانات تتناسب مع خطورة الإجراء. [19]

وقد تناولت اتفاقية بودابست بشأن الجريمة السيبرانية (2001) عدداً من الإجراءات المتعلقة بالأدلة الإلكترونية، ومنها البحث في البيانات المخزنة، وجمع بيانات حركة الاتصال في الوقت الفعلي، واعتراض بيانات المحتوى، مع إخضاع التدابير الإجرائية للضمانات والشروط المقررة في القانون الوطني. وتبرز أهمية الاتفاقية في أنها تميز بين صور الحصول على البيانات بدلاً من التعامل معها باعتبارها إجراءً تقنياً موحداً. [20]

ثالثاً: التصنيف بحسب نطاق الأشخاص المشمولين:

- الرصد الموجه إلى شخص أو حساب أو جهاز محدد.
- الرصد الذي يشمل مجموعة من الأشخاص المرتبطين بواقعة أو مكان.
- الرصد واسع النطاق الذي يجمع كميات كبيرة من البيانات قبل تحديد العناصر ذات الصلة. [21]

وتختلف هذه الصور من حيث المخاطر القانونية. فالرصد الموجه قد يكون أكثر قابلية لتحديد الغرض والنطاق، بينما تزداد مخاطر المساس بحقوق الغير في عمليات الجمع الواسع. ولا يعني ذلك أن الرصد الواسع محظور في جميع الأحوال أو مشروع لمجرد استناده إلى اعتبارات أمنية؛ بل يجب فحص الأساس القانوني الخاص به، والغاية المحددة، والضمانات السابقة والمعاصرة واللاحقة، ومدى توافر بدائل أقل تدخلاً. [22]

رابعاً: التصنيف بحسب درجة التدخل في الحقوق:

- الإجراءات الأقل تدخلاً: مراجعة بعض السجلات العامة المرتبطة بواقعة محددة.
- الإجراءات الأكثر تدخلاً: تتبع حركة شخص بصورة مستمرة أو الحصول على بيانات اتصالاته.
- الإجراءات شديدة التدخل: اعتراض مضمون اتصالاته الخاصة أو الوصول إلى بيانات حساسة واسعة النطاق. [23]

ولا يجوز بناء هذا التصنيف على افتراض أن كل بيانات متاحة تقنياً أقل حماية من البيانات غير المتاحة؛ فقد تكون البيانات منشورة في أصلها، لكن جمعها بصورة منظمة وربطها بمصادر أخرى يؤدي إلى تكوين ملف شخصي تفصيلي. كما أن بيانات الاتصال التي لا تتضمن محتوى المحادثة قد تكشف طبيعة العلاقات الشخصية أو أنماط الحركة. [24]

خامساً: التصنيف بحسب الغرض الوظيفي:

- التحقق من واقعة محددة.
- الكشف عن نمط متكرر.
- تحديد مصدر نشاط تقني.
- متابعة تنفيذ تدبير مشروع.
- جمع معلومات أولية بشأن خطر أمني محتمل. [25]

غير أن الغرض الأمني لا يُعد تفويضاً مفتوحاً لاستخدام الوسيلة؛ إذ ينبغي أن يكون الغرض مشروعاً ومحددًا، وأن تكون البيانات المطلوبة ذات صلة به، وأن يخضع أي انتقال إلى غرض جديد لتقييم قانوني مستقل. [26]

ويتضح من مجموع هذه التصنيفات أن التكييف القانوني لوسائل الرصد لا يستقيم بالاستناد إلى التصنيف التقني وحده. فالأداة التقنية تحدد الإمكانيات المتاحة، أما مشروعية استخدامها فتتوقف على الاختصاص والسند القانوني والغرض والضرورة والتناسب والضمانات. [27]

المطلب الثالث: الضوابط القانونية المشتركة لاستخدام وسائل الرصد

تخضع وسائل الرصد الرقمي، على اختلاف صورها، لمجموعة من الضوابط القانونية التي تهدف إلى التوفيق بين متطلبات العمل الأمني وحماية الحقوق. وتستمد هذه الضوابط أهميتها من أن التطور التقني قد يوسع قدرة الجهات المختصة على جمع المعلومات بدرجة تتجاوز ما كان ممكناً بالوسائل التقليدية. [28]

أولاً: مبدأ الشرعية القانونية. يقتضي أن يستند الرصد إلى قاعدة قانونية تتيح الإجراء وتحدد الجهة المختصة وأسبابه وشروطه وحدوده والضمانات. ولا يكفي أن يكون الرصد مفيداً عملياً أو متوافقاً مع سياسة داخلية؛ لأن التنظيم الإداري لا يمكنه، بذاته، إنشاء سلطة تمس حقاً أساسياً إذا كان القانون يشترط سندا تشريعياً أو إنذناً خاصاً. وتزداد أهمية هذا المبدأ في الإجراءات السرية أو التي تنطوي على تدخل عميق في الخصوصية، حيث يجب أن تكون القواعد واضحة وقابلة للتوقع. ويؤكد تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان بشأن الحق في الخصوصية في العصر الرقمي أن التدخل في الخصوصية يجب أن يستند إلى القانون، وأن يخدم غرضاً مشروعاً، وأن يكون ضرورياً ومتناسباً، مع أهمية الرقابة المستقلة. [29]

ثانياً: الاختصاص وتحديد السلطة المخولة. لا يجوز الخلط بين القدرة التقنية على الوصول إلى البيانات والسلطة القانونية التي تجيز الوصول. فقد تمتلك جهة أمنية الوسائل الفنية اللازمة للحصول على بيانات معينة، دون أن تكون مختصة قانوناً بالحصول عليها في جميع الظروف. ولهذا يجب تحديد الجهة التي تملك إصدار قرار الرصد أو طلب البيانات أو تنفيذ الإجراء، والجهة التي تملك الإذن به، والجهة المسؤولة عن فحص النتائج، والجهة التي تتولى الرقابة اللاحقة. [30]

ثالثاً: مشروعية الغرض. يجب أن يكون الغرض محدداً ومشروعاً، وأن يرتبط بمهمة تدخل ضمن اختصاص الجهة. ولا يصح أن يتحول الرصد إلى وسيلة عامة لجمع المعلومات عن الأفراد دون تحديد مسألة تستدعي التحقق. ويقتضي تحديد الغرض بيان الواقعة أو النشاط المراد التحقق منه، ونوع المعلومات اللازمة، وكيفية استخدام النتائج. وكلما كان الغرض أكثر تحديداً، أمكن مراجعة مدى صلة البيانات به. [31]

رابعاً: الضرورة والتناسب. لا يكفي أن يكون الغرض مشروعاً لكي تكون جميع الوسائل المؤدية إليه مشروعة. فالضرورة تقتضي بيان الحاجة الفعلية إلى الرصد، ومدى ملائمة الوسيلة، وإمكان تحقيقه بوسيلة أقل تدخلاً. أما التناسب فيقتضي الموازنة بين أهمية الهدف وشدة التدخل، مع مراعاة نطاق البيانات ومدة الجمع وعدد الأشخاص المتأثرين. وتترتب على ذلك ثلاث نتائج: عدم اختيار وسيلة شديدة التدخل لمجرد أنها أسرع إذا أمكن تحقيق الغرض بوسيلة أقل مساساً؛ وعدم توسيع نطاق الرصد إلى أشخاص أو بيانات لا تتصل بالمهمة إلا وفق سند قانوني؛ ومراجعة استمرار الضرورة خلال التنفيذ. [32] وقد أكدت قرارات مجلس حقوق

الإنسان التابع للأمم المتحدة أن التدخل في الخصوصية، بما في ذلك في مجال الاتصالات الرقمية، ينبغي أن يتفق مع الشرعية والضرورة والتناسب.[33]

خامساً: تحديد نطاق الإجراء ومدته. يجب أن يتضمن قرار الرصد تحديداً كافياً لنطاقه الموضوعي والشخصي والزمني. ويشمل النطاق الموضوعي أنواع البيانات أو الوقائع التي يجوز جمعها، بينما يتعلق النطاق الشخصي بالأشخاص أو الحسابات أو الأجهزة المشمولة، ويتعلق النطاق الزمني بمدة التنفيذ. ولا يقتصر دور تحديد النطاق على منع التجاوز، بل يسهم في تقويم النتائج؛ إذ يسمح بمقارنة ما جُمع بالفعل بما كان مآذوناً به.[34]

سادساً: حماية بيانات الغير وتقليل الجمع. قد ينتج عن الرصد معلومات تتعلق بأشخاص لم يكونوا مستهدفين، كما قد تكشف بيانات الشخص المستهدف عن معلومات خاصة بأفراد آخرين. ولا يؤدي ظهور هذه المعلومات عرضاً إلى إباحة استخدامها بلا قيد؛ إذ يجب تقييم مدى صلتها بالغرض المشروع، وطبيعة البيانات، والأساس القانوني الذي يسمح بالاحتفاظ بها. ويقتضي مبدأ تقليل البيانات قصر الجمع والمعالجة على القدر اللازم.[35]

سابعاً: أمن المعلومات وضبط الوصول. لا تتحقق المشروعية بمجرد الحصول على الإذن؛ بل يجب حماية البيانات من الاطلاع غير المصرح به أو التغيير أو التسريب. ويتطلب ذلك وضع ضوابط تحدد الأشخاص المخولين بالوصول، وتسجيل عمليات الاطلاع والنسخ والتعديل والنقل، واستخدام وسائل مناسبة لحماية البيانات، مع الاحتفاظ بسجلات تسمح بالمراجعة.[36]

ثامناً: تقييد الاستخدام اللاحق ومشاركة المعلومات. قد تستدعي ضرورة مشاركة المعلومات مع جهة أخرى أو إحالتها إلى جهة التحقيق. غير أن مشروعية الجمع الأول لا تعني أن كل مشاركة أو إعادة استخدام مشروعة بالضرورة. ويجب أن تستند المشاركة إلى اختصاص قانوني وغرض مشروع، وأن تقتصر على البيانات اللازمة، وأن تُحدد مسؤولية الجهة المتلقية [37].

تاسعاً: الرقابة والمساءلة. تقتضي الرقابة وجود آليات تسمح بالتحقق من أن الرصد نُفذ وفق الأساس القانوني، وأن البيانات جُمعت في حدود الإذن، وأن المعلومات لم تُستخدم على نحو يتجاوز الغرض. وقد تتخذ الرقابة صورة إذن قضائي سابق، أو مراجعة من هيئة مستقلة، أو تدقيق إداري، أو رقابة لاحقة. ولا ينبغي النظر إلى الرقابة باعتبارها عائقاً أمام العمل الأمني، بل بوصفها عنصراً من عناصر مشروعيته وموثوقيته.[38]

وقد أظهر حكم **Big Brother Watch** أن تقييم أنظمة المراقبة يجب أن يراعي فعالية الضمانات عبر مراحلها المختلفة، بما في ذلك الإذن المستقل، واختيار البيانات للفحص، وحماية المعلومات الحساسة، والرقابة على الاستخدام والتخزين والتبادل.[9]

وبناءً على ما تقدم، فإن الضوابط المشتركة تمثل إطاراً قانونياً متكاملًا لا يمكن اختزاله في الحصول على إذن أو إثبات وجود غرض أمني. فالمشروعية تتطلب أساساً قانونياً واضحاً، واختصاصاً محدداً، وغرضاً مشروعاً، وضرورة وتناسباً، وضمانات لحماية البيانات والرقابة على استخدامها.[39]

المبحث الثاني: الرصد الثابت والمتحرك وتطبيقاتهما

المطلب الأول: الرصد الثابت وكاميرات المراقبة والتسجيل الإلكتروني

يقصد بالرصد الثابت استخدام وسيلة تقنية في موقع محدد لتسجيل الوقائع أو الأنشطة التي تقع ضمن مجالها، سواء تم ذلك بصورة مستمرة أو خلال أوقات محددة أو استجابة لحدث معين. وتُعد كاميرات المراقبة من أبرز تطبيقاته، إلى جانب أنظمة التسجيل الإلكتروني التي تحفظ الأحداث المرتبطة بالدخول والخروج أو تشغيل الأنظمة. [40]

وتتعدد الأغراض التي يمكن أن يخدمها الرصد الثابت؛ فقد يُستخدم لتأمين المنشآت، أو التحقق من واقعة حدثت في مكان معين، أو متابعة حادث أمني، أو حفظ تسجيلات يُحتمل أن تكون ذات صلة بإجراء قانوني. غير أن اختلاف الغرض يؤثر في مدى مشروعية التسجيل ونطاقه والضمانات التي يجب أن تحكم الاحتفاظ به واستخدامه. [41]

أولاً: الطبيعة القانونية للتسجيلات المرئية. لا يمكن تحديد الطبيعة القانونية لتسجيل مرئي بالنظر إلى محتواه فقط، بل يجب مراعاة الظروف التي أنتج فيها، والجهة التي جمعته، والغرض من التسجيل، وطبيعة المكان، والحقوق التي قد تتأثر. فالتسجيل الذي يُلتقط في مكان عام قد يثير اعتبارات مختلفة عن التسجيل الذي يكشف نشاطاً داخل مسكن. كما أن التسجيل الناتج عن نظام أمني معن ومحدد الغرض قد يختلف عن التسجيل الناتج عن مراقبة سرية موجهة إلى شخص معين. ومع ذلك، لا يجوز افتراض أن كل تصوير في مكان عام مشروع بلا قيد، أو أن كل تسجيل في مكان خاص محظور في جميع الظروف. فالتكييف القانوني يتوقف على التشريع المنطبق، وطبيعة المكان، والتوقع المشروع للخصوصية، والغرض من التصوير [42].

وقد أكدت المادة السابعة عشرة من العهد الدولي حماية الخصوصية من التدخل التعسفي أو غير القانوني، وهو ما يستلزم تقييم عمليات التصوير والمراقبة في ضوء الأساس القانوني والضمانات المقررة، وليس بمجرد التمييز المكاني بين العام والخاص. [4]

ثانياً: مشروعية تركيب كاميرات المراقبة وتشغيلها. يتطلب تقييم المشروعية النظر في عدة عناصر: الغرض من التركيب (محدد ومشروع)؛ والاختصاص (الجهة المخولة)؛ ونطاق التصوير (المناطق المشمولة وتجنب الأماكن غير الضرورية)؛ ومدة التشغيل (متناسبة مع الغرض)؛ وطبيعة التسجيل (التمييز بين التصوير المرئي والتسجيل الصوتي المصاحب)؛ والاحتفاظ بالبيانات (تحديد المدة وآلية الإتلاف)؛ والوصول إلى التسجيلات (قصر الاطلاع على المخولين مع التوثيق). [43]

ولا يكفي وجود كاميرا مثبتة بصورة مشروعة للحكم بمشروعية كل استخدام لاحق للتسجيلات. فقد يكون التسجيل مشروعاً في الأصل، ثم يُساء استخدامه من خلال نشره أو تداوله أو توظيفه لغرض لا يسمح به القانون. [44]

ثالثاً: جمع التسجيلات واستخراجها لأغراض التحري. عندما تقع واقعة تستدعي التحري، قد تحتاج الجهة المختصة إلى الحصول على تسجيلات محفوظة لدى مؤسسة أو جهة. ويتعين

عندئذ التمييز بين سلطة حائز التسجيل في الاحتفاظ به وبين سلطة الجهة الطالبة في الحصول عليه. فامتلاك الجهة للتسجيل لا يعني بالضرورة جواز الإفصاح عنه لأي طالب، كما أن وجود غرض أمني لا يعفي الجهة الطالبة من استيفاء الإجراءات اللازمة إذا كانت البيانات محمية أو كان القانون يشترط إنذراً. [45]

ويجب أن يتحدد نطاق الطلب من حيث المكان والفترة الزمنية ونوع التسجيلات المطلوبة، وأن تكون المعلومات المطلوبة مرتبطة بالواقعة. ويُستحسن تجنب طلب تسجيلات واسعة لا تبررها الحاجة الفعلية، لما يترتب على ذلك من جمع معلومات زائدة عن أشخاص غير معينين. وعند تسلم التسجيلات، ينبغي توثيق الجهة التي سلمتها، وتاريخ التسلم، والفترة التي تغطيها، وطريقة الاستخراج، ونوع الوسيط، وأي قيود تتعلق بسلامة الملف. [46]

رابعاً: حدود دلالة التسجيلات المرئية. قد يقدم التسجيل معلومات مهمة عن تسلسل الوقائع أو حركة الأشخاص. إلا أن قيمته الاستدلالية تتوقف على جودة الصورة، وزاوية التصوير، والإضاءة، ودقة التوقيت، واستمرارية التسجيل، وسلامة النظام. فقد لا تسمح الصورة منخفضة الدقة بتحديد هوية الشخص، وقد يؤدي اختلاف زاوية التصوير إلى تغيير تصور المسافات. كذلك، فإن ظهور شخص في مكان معين لا يثبت، وحده، ارتكابه فعلاً مخالفاً، كما أن ظهوره برفقة شخص آخر لا يثبت وجود علاقة غير مشروعة. [47]

وعند استخدام برامج تحسين الصورة أو تحليل الفيديو، ينبغي توثيق الإجراءات، والتمييز بين النسخة الأصلية والنسخة المعالجة، وعدم عرض نتائج المعالجة على أنها تفاصيل مؤكدة في المصدر الأصلي ما لم يكن ذلك مدعوماً بتحقيق فني مناسب. [48]

خامساً: التعرف الآلي على الأشخاص. قد تتضمن أنظمة المراقبة أدوات للتعرف على الوجوه أو مطابقة الصور. وتثير هذه الأنظمة اعتبارات إضافية؛ لأنها قد تُستخدم في تحديد هوية أشخاص أو تتبعهم بصورة آلية، وقد تتأثر نتائجها بجودة الصور والظروف البيئية وخصائص النظام. ولذلك يجب التمييز بين نتيجة المطابقة الآلية وبين إثبات الهوية. فالمطابقة قد تمثل مؤشراً يستدعي التحقق، لكنها لا ينبغي أن تتحول تلقائياً إلى نتيجة نهائية دون مراعاة احتمال الخطأ. [49]

كما ينبغي تقييم الأساس القانوني لاستخدام هذه الأدوات، ومدى ضرورتها وتناسبها، والضمانات المتعلقة بحماية الصور والبيانات البيومترية. وقد دعت قرارات مجلس حقوق الإنسان بشأن الخصوصية في العصر الرقمي إلى مراجعة القواعد والممارسات المتعلقة باستخدام التقنيات الناشئة، بما فيها التقنيات البيومترية والقرارات الآلية. [33]

المطلب الثاني: الرصد المتحرك ووسائل تتبع حركة الأشخاص والمركبات

يقصد بالرصد المتحرك متابعة حركة شخص أو مركبة أو جهاز عبر مواقع متعددة، أو جمع بيانات تسمح بإعادة بناء مسار الحركة خلال فترة زمنية معينة. وقد يتحقق ذلك من خلال وسائل مشاهدة مباشرة، أو بيانات المواقع، أو سجلات المركبات والأنظمة، أو البيانات التي تنتجها أجهزة الاتصال. [50]

وتنبع الأهمية الأمنية لهذا النوع من قدرته على ربط الحركة بالزمن والمكان، والتحقق من روايات متعارضة، وإعادة بناء تسلسل الوقائع. غير أن هذه القدرة قد تؤدي أيضاً إلى تكوين صورة مفصلة عن الحياة اليومية للأفراد، بما يشمل أماكن وجودهم وعلاقاتهم وأنشطتهم المعتادة.[51]

أولاً: صور الرصد المتحرك:

• **المتابعة الميدانية:** تعتمد على ملاحظة الحركة في إطار مهمة أمنية محددة، مع مراعاة القيود القانونية على المراقبة والتصوير.

• **الرصد التقني للموقع:** يعتمد على بيانات تنتجها أجهزة أو أنظمة لتحديد المواقع أو تسجيلها.

• **إعادة بناء مسار الحركة:** تعتمد على الربط بين بيانات متعددة، مثل التسجيلات المرئية وسجلات الدخول وبيانات الموقع والتوقيت.[52]

ولا تتطابق هذه الصور في طبيعتها القانونية؛ فالمتابعة البصرية المباشرة قد تخضع لقواعد تختلف عن القواعد المنظمة للوصول إلى بيانات الموقع المحفوظة لدى مقدم خدمة، كما أن التتبع المستمر قد يثير اعتبارات أكثر تعقيداً من التحقق من وجود مركبة في موقع محدد خلال فترة قصيرة.[53]

ثانياً: الأثر القانوني لتتبع الموقع. قد تبدو بيانات الموقع أقل حساسية من محتوى الاتصالات، لكنها قد تكشف، عند جمعها على مدى زمني طويل، أنماطاً تفصيلية عن حياة الشخص. فقد تسمح بتحديد أماكن إقامته أو عمله، أو زيارته المتكررة، أو مواعيد نشاطه المعتاد. ولهذا لا يصح اعتبار بيانات الموقع معلومات تقنية محايدة لا ترتبط بالخصوصية. فدالتها القانونية تتأثر بمدى دقتها، ومدة جمعها، وتواتر التسجيل، وإمكان ربطها ببيانات أخرى.[54]

وقد أوضحت المحكمة الأوروبية لحقوق الإنسان، في سياق نظرها في أنظمة الاحتفاظ ببيانات الاتصالات والوصول إليها، أن بيانات الحركة والموقع يمكن أن تتيح استخلاص استنتاجات دقيقة عن الحياة الخاصة للأفراد، حتى عندما لا تتضمن مضمون الاتصالات ذاتها.[9]

ثالثاً: تحديد هوية الشخص من خلال حركة الجهاز أو المركبة. من أبرز الإشكالات الفنية والقانونية في الرصد المتحرك الخلط بين موقع الجهاز وموقع الشخص، أو بين حركة المركبة وهوية قائدها. فقد يُستخدم الجهاز من أكثر من شخص، وقد يبقى الهاتف في مركبة بينما يكون صاحبه في مكان آخر، وقد تُسجل المركبة باسم شخص لا يقودها وقت الواقعة. كما أن بيانات الموقع قد تتأثر بدقة النظام وظروف استقبال الإشارة وإعدادات الجهاز.[55]

لذلك ينبغي صياغة الاستنتاجات بما يتناسب مع ما تثبته البيانات بالفعل. فإذا أظهرت السجلات وجود جهاز في موقع معين، فإن النتيجة المباشرة تتعلق بموقع الجهاز وفق حدود دقة البيانات، ولا تنتقل تلقائياً إلى الجزم بوجود مالكه في الموقع ذاته.[56]

رابعاً: ضوابط المراقبة المستمرة. تزداد حساسية الرصد عندما يتحول من التحقق من حركة محددة إلى متابعة مستمرة لشخص أو مركبة على مدى زمني طويل. فالتراكم الزمني قد يتيح استنتاج معلومات تتجاوز الواقعة التي بدأ الرصد من أجلها. ومن ثم، يجب أن يتضمن التقييم عناصر تتعلق بالغرض من التتبع، والمدة، ونطاق المعلومات، ومدى الضرورة، والبدايل الأقل تدخلاً، والإذن اللازم، وضوابط الاحتفاظ. ولا يجوز افتراض أن مشروعية رصد حركة في مكان عام تمنح تلقائياً سلطة بناء سجل شامل لتحركات الشخص عبر الزمن. [57]

خامساً: الجمع بين بيانات الحركة والمصادر الأخرى. قد يسهم الربط بين بيانات الموقع والتسجيلات المرئية وسجلات الأنظمة في تقوية الاستنتاج، لكنه قد يؤدي إلى تضخيم دلالة المعلومات إذا لم تُفحص مصادرهما واستقلاليتها. فإذا استُخدمت بيانات الموقع لتفسير تسجيل مرئي، ثم استُخدم التسجيل نفسه لتأكيد صحة بيانات الموقع، فقد تكون النتيجة قائمة على علاقة دائرية لا على تحقق مستقل. ولذلك ينبغي بيان وظيفة كل مصدر في بناء الاستنتاج، واختبار التفسيرات البديلة، وعدم الجزم بوجود علاقة سببية بين حركة معينة وواقعة لاحقة لمجرد التقارب الزمني أو المكاني. [58]

المطلب الثالث: جمع التسجيلات والبيانات الناتجة عن الرصد وحفظها

لا تنتهي المسؤولية القانونية والمهنية عند جمع التسجيلات أو بيانات الرصد، بل تمتد إلى طريقة استخراجها وحفظها وتداولها وتحليلها، وإلى ضمان إمكان التحقق من مصدرها وسلامتها عند الحاجة. وتكتسب هذه المرحلة أهمية خاصة لأن التسجيلات قد تُستخدم لاحقاً في بناء استنتاجات أمنية أو إحالتها إلى جهات التحقيق أو تقديمها ضمن إجراءات قضائية. [59]

أولاً: التحقق من مصدر التسجيل أو البيانات. يجب تحديد الجهة أو النظام الذي أنشأ البيانات، ومكان حفظها، وطبيعة الجهاز أو البرنامج المستخدم، والفترة الزمنية التي تغطيها، والجهة التي تولت استخراجها وتسليمها. ولا يكفي الاكتفاء باسم الملف أو وصفه أو تاريخ نقله إلى وسيط جديد؛ لأن هذه البيانات قد تتعلق بعملية النسخ أو التصدير، لا بوقت إنشاء التسجيل الأصلي. وعند تعذر التحقق من بعض عناصر المصدر، ينبغي تسجيل هذا القصور صراحة. [60]

ثانياً: توثيق عملية الاستخراج. ينبغي تسجيل الطريقة التي استُخرجت بها البيانات، والأداة المستخدمة، وإصدارها، وتاريخ الإجراء، وهوية القائم به، وأي إعدادات أثرت في المخرجات. وتظهر أهمية ذلك عند استخراج تسجيلات من أنظمة متعددة؛ إذ قد تؤدي اختلافات صيغ الملفات أو طرق التصدير إلى تغيير بعض الخصائص التقنية أو فقدان بيانات وصفية. ويجب عدم اعتبار اختلاف الملف المستخرج عن بنية المصدر دليلاً تلقائياً على التلاعب، كما لا ينبغي افتراض أن كل اختلاف مبرر فنياً دون فحص وتوثيق. [61]

ثالثاً: حفظ الأصل وإنشاء نسخ العمل. الأصل هو المصدر الذي يمكن الرجوع إليه للتحقق، أما نسخ العمل فهي النسخ المستخدمة في الفحص أو العرض. ويقتضي حفظ البيانات تنظيمًا يميز بين: النسخة الأصلية أو أقرب نسخة متاحة إليها؛ والنسخ المستخرجة لأغراض الحفظ؛ والنسخ التي خضعت للتحويل أو المعالجة؛ والصور أو المقاطع المقطعة لأغراض العرض؛ والتقارير

والملاحظات الناتجة عن الفحص. ويجب توثيق الصلة بين هذه النسخ، وعدم استبدال المصدر الأصلي بنسخة معدلة دون تسجيل. [62]

رابعاً: سلسلة العهدة الرقمية. تُقصد بها مجموعة السجلات التي توثق انتقال البيانات أو الوسيط الحامل لها بين الأشخاص والجهات، وتبين من تسلمه أو فحصه أو نسخه أو نقله، ومتى تم ذلك. ولا تُعد سلسلة العهدة مجرد سجل إداري؛ بل تؤدي وظيفة إثباتية وفنية، لأنها تسمح بتتبع تاريخ التعامل مع البيانات. ويُستحسن أن يتضمن سجل العهدة: رقماً تعريفياً؛ وصفاً لمصدرها والجهة المسلمة؛ تاريخ الاستلام؛ اسم المستلم وصفته؛ وصف الحالة الظاهرة؛ الإجراءات التي أُجريت؛ عمليات النقل أو النسخ؛ بيانات الجهة التي تسلمت في كل مرحلة؛ نتائج التحقق الفني؛ وأي انقطاع أو نقص. [63]

وقد نظمت اتفاقية بودابست عدداً من الإجراءات المتعلقة بالبيانات الإلكترونية المخزنة، وأكدت أهمية توفير صلاحيات قانونية للبحث في البيانات وضبطها، مع مراعاة الضمانات والشروط التي تحكم التدابير الإجرائية. [20] غير أن اكتمال سجل العهدة لا يثبت، بمفرده، أن البيانات صحيحة أو أن محتواها يعكس الواقع؛ فهو يثبت، في حدود ما تسمح به السجلات، تاريخ التعامل معها. ولذلك يجب الفصل بين سلامة سلسلة العهدة وبين أصالة البيانات ومصادقية مضمونها [64].

خامساً: التحقق من سلامة البيانات. يمكن استخدام قيم التجزئة الرقمية (Hash Values) للتحقق من بقاء الملف دون تغيير بين مرحلتين، إذا حُسبت القيم باستخدام خوارزمية مناسبة، ووُثقت عملية الحساب. لكن قيمة التجزئة لا تثبت وحدها أن الملف كان أصلياً قبل حسابها، أو أن محتواه صحيح، أو أن التسجيل لم يتعرض للتعديل قبل تسلمه. فهي تساعد على إثبات التطابق بين نسختين وفق الخوارزمية المستخدمة، ولا تحل محل التحقق من المصدر وظروف الإنشاء. [65]

سادساً: حماية البيانات خلال الحفظ والتداول. يجب أن تُحفظ التسجيلات في بيئة مناسبة، مع قصر الوصول على المخولين، وتسجيل عمليات الاطلاع والنسخ والتصدير، واتخاذ تدابير لمنع الفقد أو التغيير أو التسريب. كما ينبغي تنظيم تبادل البيانات بين الجهات من خلال إجراءات تحدد الغرض من النقل، والجهة المستفيدة، ونطاق المعلومات، ومسؤوليات الحماية. ولا ينبغي الاحتفاظ بالمعلومات إلى أجل غير محدد لمجرد احتمال الاستفادة مستقبلاً. [66]

سابعاً: معالجة النقص في التوثيق أو العهدة. قد تكشف المراجعة عن نقص في بيانات التسلم أو النقل، أو غياب سجل لبعض عمليات الوصول، أو عدم وجود نسخة أصلية. ولا يجوز التعامل مع هذه الحالات باعتبارها دليلاً تلقائياً على التلاعب، كما لا يجوز تجاهلها. بل يجب تحديد طبيعة النقص، والمرحلة التي وقع فيها، وما إذا كانت هناك مصادر مستقلة تسمح بإعادة بناء تاريخ التعامل، ومدى تأثير القصور في إمكان التحقق. [67]

المطلب الرابع: ضوابط التصوير والرصد المستمر وحماية الخصوصية

يمثل التصوير والرصد المستمر من أكثر صور الرصد إثارة للإشكالات القانونية، ليس فقط بسبب احتمال تسجيل وقائع خاصة، وإنما أيضاً بسبب القدرة على تجميع معلومات متتابعة وتكوين صورة شاملة عن أنشطة الأشخاص وتحركاتهم. وتقتضي معالجة هذه الإشكالات التمييز بين مشروعية التقاط الصورة في لحظة معينة ومشروعية مراقبة الشخص بصورة مستمرة، وبين جمع البيانات والاحتفاظ بها، وبين الاحتفاظ بها واستخدامها لاحقاً. [68]

أولاً: الخصوصية بوصفها حقاً يتأثر بالسياق. لا تتحدد الخصوصية بحدود مادية ثابتة وحدها، بل تتأثر بطبيعة النشاط والمكان والتوقع المشروع للخصوصية وطريقة جمع المعلومات. فقد يكون الشخص ظاهراً للعموم في مكان معين، لكن ذلك لا يعني أنه تنازل عن حقه في ألا تُجمع جميع تحركاته وتُربط في سجل طويل الأجل دون أساس قانوني. وقد يكون التسجيل مشروعاً لغرض تأمين منشأة، بينما يثير استخدامه لاحقاً لتكوين ملف شخصي مسائل قانونية مختلفة [69].

ثانياً: مشروعية التصوير في الأماكن العامة والخاصة. تختلف الضوابط القانونية للتصوير بحسب التشريع وطبيعة المكان والغرض ومدى التدخل. وفي الأماكن العامة، قد يكون تسجيل بعض الوقائع جائزاً في ظروف معينة، لكن ذلك لا يعفي من مراعاة القواعد المتعلقة بالمراقبة المنظمة، والتعرف الآلي، وجمع البيانات الشخصية. أما في الأماكن الخاصة، فتزداد أهمية التحقق من السند القانوني؛ لأن التصوير قد يكشف تفاصيل لا يتوقع الشخص أن تكون متاحة للغير. ولا يمكن وضع حكم موحد لجميع الحالات دون تحديد النظام القانوني المنطبق. [70]

ثالثاً: المراقبة المستمرة ومخاطر بناء الملفات السلوكية. يختلف تسجيل واقعة محددة عن إنشاء نظام يراقب حركة الأشخاص بصورة مستمرة، ثم يربط التسجيلات ببعضها أو ببيانات أخرى. ففي الحالة الثانية، قد تتحول البيانات الجزئية إلى ملف سلوكي يكشف عادات الفرد واهتماماته وعلاقاته. وقد يؤدي ذلك إلى آثار لا تظهر عند النظر إلى كل تسجيل منفرداً. ولذلك يجب أن يتضمن التقييم عناصر تتعلق بمدة الرصد، ونطاقه المكاني والشخصي، وطبيعة البيانات، وإمكان الربط بينها، والضمانات التي تمنع استخدامها لأغراض غير مشروع. [71]

رابعاً: حماية الأشخاص الذين يظهرون عرضاً في التسجيلات. قد يُظهر التسجيل أشخاصاً لا صلة لهم بالواقعة، أو يتضمن معلومات خاصة بأفراد لم يكونوا مستهدفين. ولا يجوز افتراض أن وجود هذه المعلومات في تسجيل مشروع يجعل الاحتفاظ بها أو تداولها مباحاً بلا حدود. وينبغي اتخاذ تدابير لتقليل البيانات غير المرتبطة، وتقييد الوصول إليها، وعدم إدراجها في التقارير إلا عند وجود مبرر قانوني. وقد يكون من الملائم حجب بعض البيانات أو طمس الوجوه عند إعداد نسخ للعرض، بشرط ألا يؤدي ذلك إلى تغيير جوهر المادة التي يجب حفظها [72].

خامساً: التسجيل الصوتي المصاحب للتصوير. قد تتضمن بعض أنظمة المراقبة تسجيلاً للصوت إلى جانب الصورة. ويثير ذلك مسائل إضافية؛ لأن الصوت قد يكشف مضمون محادثات خاصة. ولذلك يجب تقييم مشروعية التسجيل الصوتي بصورة مستقلة، وعدم افتراض

أن الإذن بالتصوير يشمل بالضرورة الإذن بالتقاط المحادثات. ويتوقف الحكم على التشريع المنطبق وطبيعة المكان ومدى انطباق القواعد المتعلقة بسرية الاتصالات.[73]

سادساً: مدة الاحتفاظ بالتسجيلات. لا ينبغي أن تكون مدة الاحتفاظ موحدة في جميع الحالات؛ إذ تختلف الحاجة إلى الحفظ باختلاف الغرض وطبيعة البيانات واحتمال ارتباطها بواقعة محل تحقيق. ويقتضي التنظيم السليم تحديد مدد الاحتفاظ مسبقاً، ومراجعة الحاجة إلى استمرار الحفظ، ووضع آلية للتعامل مع التسجيلات التي أصبحت محل تحقيق. كما يجب التمييز بين الاحتفاظ لأغراض أمنية عامة وبين حفظ تسجيل محدد لارتباطه بواقعة معينة.[74]

وقد أبرزت أحكام المحكمة الأوروبية المتعلقة بالمراقبة الإلكترونية أهمية وجود قواعد واضحة للاحتفاظ بالمواد التي يتم الحصول عليها، وتأمينها، وتحديد الأشخاص المخولين بالاطلاع، وإتلافها عندما تنتفي الحاجة المشروعة، مع مراعاة الالتزامات القانونية ذات الصلة.[9]

سابعاً: الاستخدام اللاحق ومشاركة التسجيلات. قد تنتقل التسجيلات من جهة إلى أخرى، أو تُستخدم في تقرير أمني أو إجراء تحقيق. ويجب أن يخضع هذا الانتقال لغرض مشروع وسند قانوني مناسب، وأن تُحدد البيانات اللازمة للمشاركة دون توسع غير مبرر. ولا ينبغي أن يؤدي نقل التسجيل إلى جهة أخرى إلى زوال القيود التي تحكم استخدامه.[75]

ثامناً: الرقابة على أنظمة التصوير والرصد. تقتضي الحوكمة الفعالة أن تخضع أنظمة الرصد لمراجعة دورية تشمل مشروعية الغرض، ونطاق التصوير، ومدة الاحتفاظ، وطرق الوصول، وسلامة إجراءات الحفظ، ومدى استمرار الحاجة إلى النظام. كما يجب توفير سجلات تتيح معرفة من اطلع على التسجيلات أو نسخها أو نقلها، وتحديد المسؤولية عند وقوع تجاوز، وإتاحة آليات مناسبة لتقديم الشكاوى.[76]

وخلاصة الضوابط أن مشروعية التسجيل الأولي لا تكفي لتبرير جميع مراحل التعامل معه. بل يجب أن يكون التصوير مستنداً إلى أساس قانوني، ومتناسباً مع الغرض، ومحدود النطاق والمدة، وأن تحظى بيانات الغير بالحماية، وأن يخضع الاحتفاظ والتداول والاستخدام اللاحق للضوابط.[77]

المبحث الثالث: الحصول على بيانات الاتصالات والبيانات المرتبطة بالأجهزة والأنظمة

المطلب الأول: أنواع بيانات الاتصالات والتميز بين المحتوى والبيانات الوصفية

تُعد بيانات الاتصالات من أكثر فئات المعلومات الرقمية أهمية في أعمال التحري، لما قد توفره من مؤشرات بشأن هوية المستخدمين، وتوقيت الاتصالات، ومسارات انتقالها، والأجهزة المرتبطة بها. غير أن هذه البيانات ليست فئة واحدة متجانسة؛ إذ تختلف من حيث طبيعتها ومصدرها ومدى اتصالها بمضمون الاتصال، كما تختلف من حيث درجة تدخل الحصول عليها في الخصوصية. [78]

أولاً: محتوى الاتصالات. يقصد به المعلومات التي يتضمنها الاتصال ذاته، مثل نص الرسالة أو مضمون البريد الإلكتروني أو الصوت المنقول في المكالمات أو الصور والملفات المرسلة. وتتميز هذه البيانات بأنها قد تكشف مباشرة عن أفكار الأشخاص وآرائهم وعلاقاتهم وتفاصيل حياتهم الخاصة، وقد تتضمن معلومات حساسة أو مراسلات مهنية محمية قانوناً. ولهذا، فإن الحصول على محتوى الاتصالات أو اعتراضه يُعد من الإجراءات التي تستلزم عناية قانونية خاصة، وقد يشترط القانون بشأنها إذنًا قضائياً أو تصريحاً من جهة مختصة، مع تحديد الأشخاص المستهدفين والغرض والمدة ونطاق المعلومات. [79]

ثانياً: بيانات المشترك. تشير إلى المعلومات التي يحتفظ بها مقدم الخدمة بشأن اشتراك معين، مثل بيانات تسجيل الحساب أو معلومات الاتصال التي جُمعت عند إنشاء الخدمة. وقد تساعد هذه البيانات على ربط حساب أو اشتراك بشخص أو كيان، لكنها لا تثبت بالضرورة أن صاحب الاشتراك هو الذي استخدم الحساب وقت الواقعة. فقد تكون بيانات التسجيل غير محدثة، أو يكون الحساب مشتركاً بين أكثر من مستخدم، أو يكون قد تعرض للاختراق. لذلك يجب التمييز بين هوية المشترك وهوية المستخدم الفعلي. [80]

ثالثاً: بيانات حركة الاتصال. تتعلق بالمعلومات الفنية التي تنشأ عن مسار الاتصال أو معالجته داخل النظام، وقد تشمل معلومات عن مصدر الاتصال ووجهته ووقته ومدته ونوع الخدمة. ولا تتضمن بالضرورة مضمون الرسالة، لكنها قد تكشف نمط التواصل والعلاقات المتكررة بين المستخدمين. وتتبعي مراعاة حدود دلالتها؛ فوجود اتصال بين حسابين لا يثبت بذاته مضمون المحادثة أو الغرض منها، كما أن تكرار الاتصالات لا يثبت وحده وجود علاقة غير مشروعة [81].

رابعاً: بيانات الموقع. قد ترتبط بالاتصالات أو بالأجهزة أو بالتطبيقات أو بأنظمة تحديد المواقع. وتختلف دقتها بحسب التقنية المستخدمة وظروف التشغيل. وقد تكون دقيقة نسبياً في ظروف معينة، أو تقتصر على تحديد نطاق جغرافي تقريبي في ظروف أخرى. ولذلك يجب عدم عرض الموقع المستنتج على أنه نقطة مؤكدة ما لم تسمح طبيعة البيانات بذلك. كما يجب التمييز بين موقع الجهاز وموقع المستخدم، وبين الموقع المسجل وقت الاتصال والموقع الذي استُنتج لاحقاً [82].

خامساً: البيانات الفنية المرتبطة بالأجهزة والأنظمة. قد تتضمن سجلات الدخول والخروج، وعناوين الشبكة، ومعرفات الأجهزة، وسجلات التشغيل. وتساعد على تفسير كيفية استخدام نظام معين أو تحديد وقت نشاط تقني، لكنها لا تثبت دائماً هوية الشخص الطبيعي الذي قام بالفعل؛ فقد تكون بعض الأنشطة آلية، أو قد يستخدم الجهاز أكثر من شخص. [83]

سادساً: الأثر القانوني للتمييز بين المحتوى والبيانات الوصفية. قد يفهم من التمييز أن الفئة الثانية أقل حماية بالضرورة، غير أن هذا الاستنتاج ليس صحيحاً على إطلاقه. فحساسية البيانات لا تتحدد فقط بكونها تتضمن مضمون المحادثة، بل كذلك بما يمكن استخلاصه منها عند تجميعها وربطها. وقد بينت المحكمة الأوروبية في قضية *Big Brother Watch* أن بيانات الاتصالات التي يحصل عليها مقدمو الخدمات قد تثير تدخلاً في الخصوصية، وأن تنظيم الوصول إليها يجب أن يتضمن ضمانات مناسبة، بما في ذلك المراجعة المستقلة السابقة حيث تقتضي طبيعة النظام ذلك. [9]

وبناءً عليه، ينبغي ألا يُبنى تحديد الإجراء القانوني على تسمية البيانات وحدها، بل على طبيعتها الفعلية، وحساسيتها، ونطاقها، ومدة جمعها، والنتائج التي يمكن استخلاصها. كما يجب تحديد نوع البيانات المطلوب بدقة في الطلبات الرسمية، بدلاً من استخدام عبارات عامة قد تؤدي إلى جمع معلومات أوسع من الحاجة. [84]

المطلب الثاني: شروط الحصول على بيانات الاتصالات والاحتفاظ بها

يمثل الحصول على بيانات الاتصالات مجالاً دقيقاً تتقاطع فيه متطلبات الأمن والتحقيق مع حماية الخصوصية وسرية المراسلات. وتزداد أهمية التنظيم القانوني بسبب أن جانباً كبيراً من البيانات يوجد لدى مقدمي خدمات الاتصالات، لا لدى الجهات التي ترغب في الاستفادة منه. ولا يعني وجود البيانات لدى مقدم الخدمة أنها متاحة تلقائياً للجهات الأمنية؛ إذ يجب التمييز بين قدرة مقدم الخدمة على الوصول إليها، والتزامه القانوني بالاحتفاظ بها، وسلطته في الإفصاح عنها، وسلطة الجهة العامة في طلبها. [85]

أولاً: وجود أساس قانوني واضح. يتطلب الحصول على بيانات الاتصالات سنداً قانونياً يحدد الجهات المختصة، وأنواع البيانات التي يجوز طلبها، والأغراض المسموح بها، والشروط والإجراءات. ويجب أن يكون هذا السند واضحاً بالقدر الذي يسمح بتحديد نطاق السلطة وتوقع آثارها، وأن يحد من السلطة التقديرية. وتزداد أهمية وضوح القاعدة عندما يتعلق الطلب بمحتوى الاتصالات أو ببيانات تكشف أنماط الحركة والعلاقات الشخصية أو عندما يشمل عدداً كبيراً من المستخدمين. ولا يجوز أن تحل التعليمات الداخلية محل السند القانوني. [86]

ثانياً: تحديد الجهة المختصة بطلب البيانات. ينبغي أن يحدد النظام القانوني الجهات التي تملك طلب بيانات الاتصالات، وحدود صلاحيات كل جهة، والحالات التي يجوز فيها إصدار الطلب، والجهة التي تتولى مراجعته أو الإذن به. ولا يجوز افتراض أن جميع الجهات الأمنية تتمتع بالسلطة نفسها للحصول على كل فئات البيانات. فقد يفرق القانون بين الطلبات الإدارية، والطلبات المرتبطة بالتحري، والطلبات التي تُقدّم في إطار تحقيق جنائي، كما قد يميز بين بيانات المشترك وبيانات الحركة ومحتوى الاتصال. [87]

ثالثاً: الإذن القضائي أو التصريح المختص. قد يشترط القانون إذناً قضائياً مسبقاً أو تصريحاً من جهة مستقلة قبل الحصول على بعض بيانات الاتصالات، خصوصاً عندما يكون الإجراء شديد التدخل. وتتحدد ضرورة الإذن ونوع الجهة التي تصدره وفق التشريع المعمول به وطبيعة البيانات. ولا يصح افتراض أن كل طلب لبيانات الاتصالات يحتاج إلى إذن قضائي، كما لا يصح افتراض أن الطلب الإداري يكفي في جميع الحالات. ويجب أن يحدد الإذن نطاق البيانات والأشخاص والفترة والغرض، وأن تُوثق أي تعديلات أو تمديدات. كما يجب التحقق من أن البيانات التي تسلمتها الجهة تقع ضمن الحدود المأذون بها. [88]

وقد قررت المحكمة الأوروبية في قضية *Big Brother Watch* أن بعض جوانب النظام البريطاني السابق للحصول على بيانات الاتصالات من مقدمي الخدمات لم تستوف متطلبات الحماية اللازمة بموجب المادة الثامنة من الاتفاقية الأوروبية، ومن بين المسائل التي تناولها الحكم عدم كفاية المراجعة المستقلة السابقة في إطار النظام محل الفحص. [9] ولا يعني ذلك أن الحكم يفرض إجراءً موحداً على جميع الدول، لكنه يقدم معياراً قضائياً مهماً عند تقييم كفاية الضمانات. [89]

رابعاً: تحديد نطاق الطلب وتجنب الإفراط في جمع البيانات. ينبغي أن يحدد طلب البيانات الفئة المطلوبة، والفترة الزمنية، والحساب أو الاشتراك أو الجهاز المعني، والغرض. ويجب أن تكون البيانات المطلوبة ذات صلة بالمهمة، وألا يتجاوز الطلب النطاق اللازم. فطلب جميع بيانات المستخدم لفترة طويلة، دون بيان الحاجة، قد يؤدي إلى جمع معلومات خاصة لا علاقة لها بالواقعة. وعندما يتعذر تحديد البيانات بدقة في البداية، ينبغي بيان سبب ذلك، واتباع الإجراءات التي يسمح بها القانون. [90]

خامساً: التمييز بين الحصول على البيانات والاحتفاظ بها لدى مقدم الخدمة. ينبغي الفصل بين مسألتين: الاحتفاظ بالبيانات (استمرار مقدم الخدمة في حفظ بيانات معينة وفق القانون)؛ والوصول إلى البيانات أو الإفصاح عنها (تمكين جهة أخرى من الحصول عليها). فقد يلتزم مقدم الخدمة بحفظ بعض السجلات، لكن ذلك لا يعني أن جميع الجهات تستطيع الوصول إليها دون إجراءات. وبالمثل، فإن وجود سلطة قانونية لطلب بيانات محددة لا يعني بالضرورة جواز فرض الاحتفاظ الشامل بكل بيانات المستخدمين. ويجب أن يخضع نظام الاحتفاظ نفسه للتقييم من حيث نطاق البيانات والمدة والغاية والضمانات. [91]

سادساً: حماية البيانات بعد الإفصاح عنها. لا تنتهي الالتزامات عند تسلم بيانات الاتصالات. بل يجب أن تُحفظ في بيئة آمنة، وأن يُقصر الوصول على المخولين، وأن يُوثق استخدامها ونقلها، وأن تخضع إعادة مشاركتها لغرض مشروع وسند قانوني. كما يجب الفصل بين البيانات الأصلية والنسخ المستخدمة للتحليل، وتوثيق أي تحويل أو معالجة. ويجب عدم استخدام البيانات في أغراض تختلف عن الغرض الذي جُمعت من أجله إلا إذا سمح القانون بذلك. [92]

سابعاً: مدة الاحتفاظ والإتلاف. ينبغي تحديد مدة الاحتفاظ وفق الغرض المشروع والمتطلبات القانونية، مع مراعاة طبيعة البيانات وحساسيتها. ولا يجوز الاحتفاظ بالمعلومات إلى أجل غير محدد لمجرد احتمال فائدتها مستقبلاً، كما لا يجوز إتلاف بيانات يجب حفظها قانوناً أو أصبحت

محل إجراء قائم. وعند انتهاء الحاجة، ينبغي إتلافها أو حذفها وفق إجراء موثق، ما لم يوجد سند قانوني يقتضي استمرار حفظها. [93]

ثامناً: طلب البيانات من خارج الدولة. قد تكون البيانات محفوظة لدى مقدم خدمة يعمل في دولة أخرى، أو على خادم يقع خارج إقليم الدولة الطالبة. وهنا تبرز مسائل تتعلق بالاختصاص القضائي، والسيادة، وحماية البيانات، والتعاون الدولي. ولا يكفي أن تكون الجهة قادرة تقنياً على الوصول لكي يكون الوصول مشروعاً دولياً؛ إذ يجب تحديد الأساس القانوني الذي يسمح بالوصول المباشر أو بطلب المساعدة، مع مراعاة الاتفاقيات النافذة. وقد توفر اتفاقية بودابست آليات للتعاون الدولي في مجال الأدلة الإلكترونية، لكن تطبيقها يتوقف على نطاق الاتفاقية والالتزامات النافذة. [20]

المطلب الثالث: الوصول إلى الأجهزة والأنظمة الرقمية ونطاق الإذن والفحص

يُعد الوصول إلى الأجهزة والأنظمة الرقمية من الإجراءات التي تتطلب دقة خاصة في تحديد نطاق السلطة القانونية؛ لأن الجهاز الواحد قد يحتوي على كميات كبيرة من البيانات الشخصية والمهنية والمالية، وقد يتيح الوصول إليه الاطلاع على حسابات أو خدمات أو بيانات مخزنة في أنظمة أخرى. [94]

أولاً: التمييز بين ضبط الجهاز والوصول إلى بياناته. لا يعني الاستيلاء المادي على جهاز أو تسلمه بالضرورة أن الجهة المختصة تملك سلطة فحص جميع البيانات الموجودة فيه. فقد يحدد القانون نطاق الضبط أو الفحص، وقد يشترط إذناً مستقلاً للوصول إلى البيانات أو توسيع البحث. ويجب تحديد الأساس القانوني لكل مرحلة، والتحقق من أن الإجراء لا يتجاوز الغرض الذي سُمح به. فإذا كان الإذن متعلقاً ببيانات محددة، فلا يجوز تفسيره تلقائياً على أنه تفويض عام بفحص جميع المعلومات الشخصية. [95]

ثانياً: تحديد نطاق الإذن بالفحص. ينبغي أن يكون الإذن، متى تطلبه القانون، محدداً بما يكفي لتوضيح الجهاز أو النظام المستهدف، ونوع البيانات المطلوب فحصها، والغرض، والفترة الزمنية، وحدود الوصول. وتزداد أهمية هذا التحديد بسبب طبيعة الأجهزة الحديثة؛ إذ قد يحتوي الهاتف على مراسلات وصور وبيانات موقع وسجلات استخدام ومعلومات مالية، إضافة إلى إمكانية الوصول إلى خدمات سحابية. ولا يجوز افتراض أن الإذن بفحص نوع معين يمنح تلقائياً سلطة الوصول إلى جميع الفئات الأخرى. كما أن اكتشاف معلومات جديدة أثناء الفحص قد يستلزم تقييماً قانونياً مستقلاً قبل توسيع النطاق. [96]

وقد تناولت اتفاقية بودابست في المادة التاسعة عشرة البحث في البيانات الحاسوبية المخزنة وضبطها، بما يشمل الوصول إلى نظام حاسوبي أو وسيط تخزين في الإقليم الذي تنطبق عليه السلطة القانونية المختصة. كما تناولت، ضمن شروط محددة، إمكان توسيع البحث إلى نظام آخر إذا توافرت أسباب للاعتقاد بأن البيانات المطلوبة مخزنة فيه وكانت متاحة قانوناً من النظام الأول. [20]

ثالثاً: الأجهزة المحمولة والحواسيب ووسائط التخزين. تختلف إجراءات الفحص بحسب طبيعة الجهاز والبيانات المخزنة. ويجب توثيق حالة الجهاز عند الاستلام، ومصدره، والأشخاص الذين تعاملوا معه، والإجراءات التي أُخذت قبل الفحص وأثناءه. كما ينبغي مراعاة أن بعض البيانات قد تتغير نتيجة تشغيل الجهاز أو تحديث التطبيقات أو الاتصال بالشبكة. ويقتضي الفحص المنضبط توثيق الأدوات المستخدمة وإصداراتها، وتسجيل الخطوات المؤثرة في البيانات، والمحافظة على النسخة الأصلية أو أقرب نسخة فنية، وإجراء التحليل على نسخ مناسبة. [97]

رابعاً: الوصول إلى الحسابات والخدمات المتصلة بالجهاز. قد يكون الجهاز متصلاً بحسابات بريد أو خدمات تخزين سحابي أو منصات اتصال. لكن الوصول إلى الجهاز لا يعني بالضرورة أن الجهة تملك سلطة قانونية للوصول إلى جميع هذه الخدمات. فقد توجد البيانات على خادم تابع لمقدم خدمة مستقل، أو تخضع لشروط وصول مختلفة، أو تكون محفوظة خارج الدولة. ولذلك يجب التمييز بين البيانات المخزنة محلياً والبيانات التي يمكن الوصول إليها من خلال الجهاز لكنها محفوظة في مكان آخر. [98]

خامساً: البيانات السحابية والاختصاص القضائي. تثير الخدمات السحابية إشكالات خاصة؛ لأن موقع المستخدم قد يختلف عن موقع الخادم، كما قد تتوزع البيانات بين أنظمة متعددة. ولا يعني ذلك أن الموقع المادي للخادم هو العامل الوحيد الذي يحدد القانون الواجب التطبيق؛ إذ قد تتداخل معه عوامل أخرى، منها موقع مقدم الخدمة، وطبيعة العلاقة التعاقدية، ومكان المستخدم، والقواعد المتعلقة بحماية البيانات، والاتفاقيات الدولية. وعليه، يجب التحقق من الأساس القانوني للوصول إلى البيانات السحابية، وعدم اعتبار إمكان الوصول إليها من الجهاز المحلي بديلاً عن استيفاء متطلبات الاختصاص أو الإفصاح. [99]

سادساً: التشفير وحدود الوصول الفني. قد تكون البيانات محمية بالتشفير. ويؤثر ذلك في إمكان الوصول إلى المحتوى وقراءته، لكنه لا يعني بالضرورة تعذر الوصول إلى جميع البيانات المرتبطة به. ويجب التمييز بين وجود البيانات، والقدرة التقنية على فك تشفيرها، والسلطة القانونية التي تجيز الوصول إليها. فهذه مسائل مستقلة نسبياً. كما ينبغي توثيق القيود الفنية التي حالت دون الوصول، وعدم الاستنتاج من تعذر قراءة المحتوى أن البيانات غير موجودة أو أن صاحب الجهاز تعمد إخفاءها، ما لم تتوافر أدلة مستقلة. [100]

سابعاً: حماية البيانات غير المرتبطة بموضوع الفحص. قد يكشف فحص الجهاز عن معلومات تتعلق بالحياة الشخصية أو المهنية، أو عن مراسلات تخص أشخاصاً آخرين. ويجب التعامل مع هذه المعلومات وفق مبدأ تقليل البيانات وحدود الإذن والغرض المشروع. فإذا لم تكن البيانات ذات صلة، ينبغي تجنب التوسع في تحليلها أو تداولها دون سند قانوني. وإذا ظهر أنها قد تكون ذات صلة بواقعة أخرى، فيجب تقييم مدى جواز استخدامها أو توسيع نطاق الفحص وفق الإجراءات المقررة. [101]

ثامناً: توثيق الفحص وقابلية مراجعته. تقتضي سلامة الفحص تسجيل الخطوات التي أُجريت، والأدوات المستخدمة، وإصداراتها، وطريقة استخراج البيانات، والقيود التي أثرت في العملية، والنتائج التي أمكن التحقق منها. ويجب أن يسمح التقرير الفني لمراجع مستقل بفهم كيفية

الوصول إلى النتيجة، وما البيانات التي استند إليها التحليل، وما الافتراضات التي قام عليها، وما أوجه القصور. ولا تعني قابلية إعادة الفحص ضرورة تكرار كل إجراء بصورة مطابقة، لكنها تقتضي توفير المعلومات والنسخ والسجلات اللازمة للتحقق. [102]

المطلب الرابع: البيانات السحابية والتشفير والقيود القانونية والفنية على الوصول

أدى انتشار الحوسبة السحابية والتشفير والخدمات العابرة للحدود إلى تغيير طبيعة الوصول إلى البيانات محل التحري. فلم تعد المعلومات مرتبطة دائماً بجهاز مادي واحد أو بمكان تخزين معلوم، كما لم يعد الوصول التقني إلى الحساب مرادفاً بالضرورة للقدرة على قراءة جميع محتوياته أو امتلاك السلطة القانونية اللازمة. [103]

أولاً: الطبيعة القانونية والفنية للبيانات السحابية. يقصد بها المعلومات التي تُخزن أو تُعالج أو تُتاح عبر خدمات تعتمد على بنية حاسوبية متصلة بالشبكة، وقد تكون محفوظة لدى مقدم الخدمة أو موزعة بين أنظمة متعددة. وتتميز هذه البيئة بأن المستخدم قد يتعامل مع البيانات من خلال جهاز محلي، بينما تكون النسخة الأساسية أو بعض مكوناتها محفوظة على خوادم لا تقع في المكان ذاته. وتترتب على ذلك أهمية التمييز بين مكان الوصول إلى البيانات ومكان تخزينها، وبين الجهة التي تستخدم الخدمة والجهة التي تملك السيطرة التقنية على الخادم. [104]

ثانياً: التمييز بين الوصول المحلي والوصول إلى نظام آخر. قد يتيح الجهاز المحلي الوصول إلى ملفات أو حسابات مخزنة في نظام بعيد. لكن هذه الإمكانية التقنية لا تحسم مشروعية الإجراء. فقد يكون الوصول إلى البيانات المحلية مشمولاً بإذن معين، بينما يتطلب الوصول إلى النظام البعيد إجراءات إضافية أو سنداً قانونياً مختلفاً. وتبرز هنا أهمية تحديد النطاق الحقيقي للإجراء: هل يتعلق بفحص الجهاز المضبوط فقط، أم يشمل الوصول إلى حساب خارجي؟ وهل البيانات المطلوبة محفوظة محلياً أم لدى مقدم خدمة؟ [105]

وقد عالجت المادة التاسعة عشرة من اتفاقية بودابست إمكانية توسيع البحث إلى نظام آخر في ظروف محددة، من بينها وجود أسباب للاعتقاد بأن البيانات المطلوبة موجودة في النظام الآخر، وأنها متاحة قانوناً من النظام الذي بدأ البحث فيه. [20] وتُظهر هذه القاعدة أن التوسع التقني في البحث يجب ألا يُفهم باعتباره سلطة غير محدودة؛ بل يظل مرتبطاً بشروط قانونية. [106]

ثالثاً: التشفير وأثره في إمكان الوصول. التشفير وسيلة تقنية تهدف إلى حماية سرية البيانات من خلال تحويلها إلى صيغة لا يمكن قراءتها دون وسائل فك التشفير المناسبة. ويجب التمييز بين ثلاثة أمور: وجود البيانات على الجهاز أو في الخدمة؛ وإمكان الوصول إليها تقنياً وقراءتها؛ وجواز الوصول إليها قانوناً وفق الاختصاص والإذن والضمانات. فقد يكون الوصول مشروعاً قانوناً لكنه متعذر فنياً، وقد يكون ممكناً تقنياً دون أن يكون مأذوناً به قانوناً. ولا يصح الاستنتاج من وجود التشفير، وحده، أن المستخدم تعمد إخفاء دليل؛ لأن التشفير يُستخدم لحماية المعلومات الشخصية والمهنية بصورة مشروعة. [107]

رابعاً: القيود الفنية وأثرها في تقييم النتائج. قد تمنع القيود التقنية الوصول إلى بعض البيانات أو تؤدي إلى استخراج معلومات جزئية فقط. وقد تنشأ عن عدم توافر مفاتيح التشفير، أو تلف

البيانات، أو محدودية أدوات الفحص، أو اختلاف إصدارات الأنظمة. ويجب توثيق هذه القيود وبيان أثرها في النتائج. فإذا لم يتمكن الفحص من الوصول إلى محتوى رسالة مشفرة، فلا يصح الجزم بمضمونها اعتماداً على بيانات وصفية وحدها. كما ينبغي عدم وصف الفحص بأنه شامل إذا كانت هناك فئات لم تُفحص أو تعذر الوصول إليها. [108]

خامساً: الحصول على البيانات من مقدمي الخدمات. قد يتطلب الوصول إلى البيانات السحابية طلباً من مقدم الخدمة. وتختلف إجراءات الإفصاح بحسب طبيعة البيانات والقواعد القانونية التي تنطبق على مقدم الخدمة والجهة الطالبة. ويجب تحديد البيانات المطلوبة والغرض والفترة، والتحقق من الصفة القانونية للجهة، واستيفاء الأذونات، ومراعاة القيود التي قد تفرضها قوانين حماية البيانات أو السرية المهنية. كما ينبغي توثيق استجابة مقدم الخدمة، وبيان ما إذا كانت البيانات كاملة أو جزئية، وما القيود التي ذكرها بشأن دقتها. [109]

سادساً: الاختصاص القضائي والبيانات العابرة للحدود. تزداد المسائل تعقيداً عندما تكون البيانات محفوظة في دولة أخرى أو عندما يخضع مقدم الخدمة لقانون أجنبي. ويجب التمييز بين طلب المساعدة القانونية من دولة أخرى، والوصول المباشر إلى بيانات خارج الإقليم، وطلب الحفاظ العاجل على بيانات يحتمل فقدانها. فكل صورة شروطها وإجراءاتها. وتوفر اتفاقية بودابست إطاراً للتعاون الدولي، لكن تطبيق أحكامها يتوقف على نطاق انطباقها والتزامات الدول المعنية. [110] كما ينبغي مراعاة أن نقل البيانات عبر الحدود قد يثير التزامات تتعلق بحماية البيانات الشخصية وسرية المعلومات. [111]

سابعاً: المحافظة العاجلة على البيانات. قد يكون هناك خطر من فقدان البيانات أو حذفها قبل استكمال إجراءات الحصول عليها. وفي مثل هذه الحالات، قد تتيح القوانين أو الاتفاقيات تدابير لحفظ البيانات مؤقتاً. لكن المحافظة على البيانات تختلف عن الإذن بالاطلاع على محتواها؛ فقد يكون حفظ البيانات إجراءً مستقلاً عن تسليمها أو فحصها. ويجب أن يقتصر الحفظ على البيانات التي يجيز القانون المحافظة عليها، وأن تكون مدته محددة، مع توثيق طلب الحفظ والجهة التي نفذته والغرض. [112]

ثامناً: التعاون الدولي وضمانات الحقوق. لا ينبغي أن يؤدي الطابع العابر للحدود إلى إضعاف الضمانات أو تجاوز قواعد الاختصاص. فالتعاون الدولي يهدف إلى تمكين السلطات من الوصول المشروع إلى المعلومات، وليس إلى إنشاء مسار بديل لتجاوز القيود. ويجب أن يراعي وضوح الغرض، ونطاق البيانات، والجهة الطالبة، والضمانات المتعلقة بالخصوصية، وأمن المعلومات، والقيود على الاستخدام اللاحق. وقد شددت تقارير الأمم المتحدة بشأن الخصوصية في العصر الرقمي على أهمية توفير أساس قانوني واضح للمراقبة والوصول إلى البيانات، وعلى ضرورة وجود رقابة مستقلة وسبل فعالة للمساءلة، بما في ذلك في السياقات التي تتضمن تعاوناً بين الدول. [29]

وتبعاً لذلك، فإن التعامل مع البيانات السحابية والتشفير يتطلب الجمع بين التقويم الفني والتكييف القانوني. فإمكان الوصول إلى البيانات لا يحدد وحده مشروعية الإجراء، كما أن تعذر الوصول

لا يثبت مضمون المعلومات غير المتاحة. ويجب توثيق القيود الفنية، والتحقق من الاختصاص، واستيفاء الإجراءات، ومراعاة الضمانات المتعلقة بالخصوصية والتعاون الدولي. [113]

الجدول المقارن: وسائل الرصد الرقمي ودرجة التدخل والضمانات

الوسيلة	السند المطلوب	درجة التدخل	طبيعة البيانات	الضمانات الأساسية
كاميرات المراقبة العامة	سند قانوني/تنظيمي + غرض مشروع	منخفض إلى متوسط	مرئية (وصوتية أحياناً)	تحديد النطاق، مدة الاحتفاظ، حماية الغير، ضبط الوصول
التسجيل الإلكتروني للأنظمة	صلاحية مؤسسية	منخفض إلى متوسط	سجلات دخول/تشغيل	توثيق الوصول، تقليل البيانات، مراجعة دورية
بيانات الموقع	إذن قضائي أو تصريح مختص (بحسب التشريع)	متوسط إلى مرتفع	مكانية/زمنية	تحديد المدة والدقة، التمييز بين الجهاز والشخص، المراجعة
بيانات حركة الاتصال	سند قانوني خاص + رقابة مستقلة	مرتفع	وصفية (مصدر/وجهة/وقت)	تحديد الفئة والفترة، المراجعة المستقلة، تقييد الاستخدام
محتوى الاتصالات	إذن قضائي مسبق	شديد	محتوى	تسبيب الإذن، تحديد النطاق والمدة، رقابة لاحقة
فحص الأجهزة	إذن قضائي محدد النطاق	مرتفع إلى شديد	ملفات/سجلات/بيانات وصفية	سلسلة العهدة، نسخة أصلية، حماية بيانات الغير، توثيق الفحص
البيانات السحابية	سند قانوني + تعاون دولي/إفصاح	مرتفع (مع تعقيد الاختصاص)	ملفات/سجلات	تحديد الاختصاص، طلب رسمي، توثيق الاستجابة، قيود الاستخدام
التشفير	سلطة قانونية + إمكان فني	شديد (فني وقانوني)	محتوى محمي	التمييز بين الوجود والوصول والجواز، توثيق القيود

الفصل الثالث: المراقبة والرصد الجوي باستخدام الطائرات المسيّرة وأثرهما في التحريات الأمنية الرقمية

تمهيد

لم يعد التحري الأمني الرقمي حبيس الشاشات والسجلات الإلكترونية، بل امتد إلى الفضاء، حيث أصبحت الطائرات المسيّرة عيناً ثالثة ترصد ما لا تراه العين المجردة، وتبلغ ما لا تبلغه القوات الأرضية. غير أن هذه العين الثالثة، التي تفتح آفاقاً واسعة للكشف والتحقق، تطرح في الوقت ذاته إشكالات قانونية دقيقة، تتعلق بحدود التدخل في الحياة الخاصة، ومدى مشروعية الاستخدام، وقيمة ما تنتجه من مخرجات رقمية، وضمانات تنظيمها. ولا يمكن معالجة هذه الإشكالات بمعزل عن التطبيقات الأمنية الكبرى التي تبرر هذا النوع من التقنية، وأعني بها مكافحة الإرهاب والمجموعات المسلحة، وتأمين الاحتفالات والمهرجانات والفعاليات الجماعية، والتأمين العسكري للمنشآت الحيوية. كما لا يمكن إغفال التهديدات الأمنية التي تواجه الطائرات المسيّرة أثناء الرصد الجوي، من استهداف مباشر وتشويش إلكتروني وتضليل وخداع واختراق سببراني، وهي تهديدات تؤثر في مشروعية الرصد وموثوقية مخرجاته.

ومن ثم، فإن هذا الفصل يهدف إلى تأصيل مفهوم الطائرات المسيّرة وخصائصها التقنية، وبيان وظائفها في المراقبة والرصد وجمع المعلومات، والتمييز بين الرصد الوقائي والتحري الأمني وجمع الأدلة، ثم تحليل الأساس القانوني لاستخدامها، وحدود الاختصاص والإذن والتدخل في الحياة الخاصة، ومبدأ التناسب وضمانات حماية البيانات، ثم تقييم القيمة الإثباتية لمخرجاتها الرقمية، وأخيراً معالجة التطبيقات الأمنية الكبرى، والعوامل الميدانية والبيئية، والتهديدات الأمنية، واقتراح الضمانات اللازمة. وبهذا التسلسل، تُفصل المسائل القانونية عن المسائل الفنية، مع إبقاء الصلة بينهما واضحة، ويُعطى الموضوع من جميع أبعاده.

المبحث الأول: الإطار المفاهيمي والتقني للمراقبة والرصد الجوي بالطائرات المسيّرة المطلب الأول: مفهوم الطائرات المسيّرة وخصائصها التقنية ذات الصلة بالتحري الأمني

تُعرّف الطائرة المسيّرة بأنها مركبة جوية غير مأهولة، يمكن تشغيلها عن بُعد أو برمجتها مسبقاً لتنفيذ مهام محددة، وتتكون عادةً من منصة طيران، ونظام تحكم، وحمولة تتضمن كاميرات أو مستشعرات، ونظام اتصال ونقل بيانات، ووحدة تخزين أو بث [١]. وقد انتقل استخدامهما من المجالات العسكرية إلى الاستخدامات المدنية والأمنية، وأصبحت أداة ذات قدرات متعددة في المراقبة والرصد وجمع المعلومات. وتكمن أهمية هذه الأداة في التحري الأمني الرقمي في خصائص تقنية عدة، لكل منها أثر قانوني مباشر. فهي قادرة على الوصول إلى أماكن يصعب الوصول إليها برياً أو تكون خطرة على البشر، كمسرح جريمة غير آمن، أو منطقة منكوبة، أو تضاريس وعرة، أو مناطق نزاع مسلح [٢]. وهذا الوصول ليس مجرد ميزة تقنية، بل هو ما يمنح الطائرة قيمتها الأمنية الحقيقية، ويجعلها أداة لا غنى عنها في مكافحة الإرهاب والمجموعات المسلحة، حيث يصعب على القوات الأرضية اقتحام المناطق الجبلية والحدودية دون مخاطر جسيمة.

كما تتيح الطائرة تصويراً جوياً عالي الدقة، سواء بالصور الثابتة أو الفيديو أو التصوير الحراري أو متعدد الأطياف، مما يتيح رؤية تفصيلية للمشاهد والتحركات قد لا تلتقطها الوسائل الأرضية [٣]. وهذه الدقة ليست ترفاً تقنياً، بل هي شرط لإنتاج مخرجات تصلح للتحري أو الإثبات. غير أن الدقة نفسها هي ما يثير الإشكالات القانونية، لأنها قد تكشف تفاصيل الحياة الخاصة في الأماكن المفتوحة أو المحيطة.

وإلى جانب المحتوى المرئي، تنتج الطائرة المسيّرة بيانات وصفية غنية، تشمل إحداثيات الموقع، والارتفاع، والسرعة، واتجاه الطيران، ووقت الإقلاع والهبوط، وسجلات الرحلة، وبيانات المستشعرات [٤]. وهذه البيانات، وإن بدت تقنية في ظاهرها، فإنها تكتسب دلالة قانونية مهمة عند استخدامها في التحري أو الإثبات، لأنها قد تساعد على تحديد زمن الواقعة ومكانها، لكنها لا تثبت وحدها هوية الأشخاص أو طبيعة سلوكهم. كما تتيح الطائرة البث المباشر أو التسجيل، مما يتيح المتابعة الفورية أو التحليل اللاحق، ويمكن ربط مخرجاتها بأنظمة أخرى كقواعد البيانات وأنظمة المراقبة الأرضية ومنصات التحليل، مما يضاعف قدرتها على إنتاج المعلومات [5].

غير أن هذه الخصائص التقنية نفسها هي ما يثير الإشكالات القانونية. فالقدرة على الوصول إلى أماكن كان يصعب الوصول إليها تطرح سؤالاً عن حدود التدخل في الحياة الخاصة، والتصوير عالي الدقة يطرح سؤالاً عن حماية الخصوصية في الأماكن الخاصة، والبيانات الوصفية الغنية تطرح سؤالاً عن دقتها وحدود الاستدلال بها، والقدرة على البث والربط تطرح سؤالاً عن مشروعية تداول البيانات ومشاركتها. ومن ثم، فإن الطائرة المسيّرة ليست مجرد أداة تقنية محايدة، بل هي وسيلة لجمع المعلومات يترتب على استخدامها آثار قانونية تستلزم تقييماً مستقلاً.

المطلب الثاني: وظائف الطائرات المسيّرة في المراقبة والرصد وجمع المعلومات الرقمية

تتعدد وظائف الطائرات المسيّرة في التحري الأمني الرقمي، ويمكن تصنيفها في أربع دوائر متميزة، لكل منها طبيعة قانونية مختلفة.

أولاً: المراقبة الوقائية. وتتمثل في استخدام الطائرة لتأمين المنشآت والفعاليات والحدود، ورصد المخاطر المحتملة قبل وقوعها [٦]. وتندرج هذه الوظيفة ضمن الأعمال الأمنية الوقائية التي قد لا تستلزم إدناً قضائياً في بعض التشريعات، لكنها تظل خاضعة لضوابط الخصوصية والتناسب، لأن المراقبة الوقائية قد تجمع معلومات عن أشخاص لا صلة لهم بأي خطر محدد. وهذا ما يظهر بوضوح في تأمين الاحتفالات والمهرجانات والمواسم، حيث تختلط الحشود الكبيرة بأشخاص لا صلة لهم بأي تهديد، ويجب تقليل جمع بياناتهم إلى الحد اللازم.

ثانياً: الرصد في مسرح الجريمة. وتتمثل في تصوير مسرح الجريمة جواً، ورسم المجسمات، وتوثيق الحالة قبل التدخل البشري، والبحث عن أدلة أو أشخاص مفقودين [٧]. وتساعد هذه الوظيفة في الحفاظ على مسرح الجريمة من التلوث، وفي توفير رؤية شاملة قد لا تتاح من الأرض. غير أن المخرجات الناتجة عن هذه الوظيفة تكتسب طابعاً إثباتياً يقتضي ضوابط إضافية تتعلق بالأصالة والسلامة وسلسلة العهدة.

ثالثاً: جمع المعلومات الرقمية. وتشمل جمع الصور والفيديو والبيانات الوصفية التي قد تكون ذات صلة بواقعة أو نشاط أو شخص. وتُعد هذه المخرجات معلومات رقمية تخضع لضوابط الأصالة والسلامة والتوثيق، وتظل في مرحلة جمع المعلومات الأولية ما لم تُستكمل بإجراءات تحقيق أو إثبات [٨]. وفي مكافحة الإرهاب، قد تكون هذه المعلومات هي الأساس الذي تُبنى عليه عمليات أمنية لاحقة، مما يستلزم دقة عالية في الجمع والتحقق.

رابعاً: المتابعة والتحقق. وتتمثل في متابعة تحركات أو أنشطة معينة، أو التحقق من معلومات أولية [٩]. وفي هذه الحالة، تزداد حساسية الاستخدام من حيث الخصوصية والتناسب، لأن المتابعة قد تتحول إلى مراقبة مستمرة تنطوي على تدخل أعمق في الحياة الخاصة. وهذا ما يظهر في تتبع الأشخاص المشتبه فيهم في قضايا الإرهاب أو الجريمة المنظمة، حيث قد تستمر المراقبة لأيام أو أسابيع، ويجب أن تخضع لضوابط صارمة.

ويجب التمييز بين الاستخدام الوقائي والاستخدام التحقيقي، فالأول قد يكتفي بضوابط إدارية وتنظيمية، بينما الثاني قد يستلزم إدناً قضائياً أو تصريحاً مختصاً بحسب التشريع المنطبق [١٠]. كما أن الوظائف الأربع قد تتداخل عملياً، فقد يبدأ الاستخدام وقائياً ثم يتحول إلى تحري أو جمع أدلة، ويقتضي ذلك إعادة تقييم الأساس القانوني والضمانات في كل مرحلة، لا افتراض استمرار الصلاحية الأولى.

المطلب الثالث: التمييز بين الرصد الوقائي والتحري الأمني وجمع الأدلة الجنائية الرقمية

يقتضي الضبط المفاهيمي التمييز بين ثلاثة أنماط من استخدام الطائرات المسيّرة، لأن لكل نمط طبيعة قانونية وضمانات مختلفة.

أولاً: الرصد الوقائي. وهو الذي يهدف إلى منع المخاطر أو تقليلها، ولا يستهدف واقعة محددة أو شخصاً معيناً. ويخضع لضوابط الاختصاص والتناسب والخصوصية، لكنه لا يرقى إلى جمع أدلة جنائية، لأن غايته وقائية لا إثباتية [١١]. ومن أمثلته تأمين المنشآت الحيوية والمنشآت العسكرية، حيث تهدف الطائرة إلى مراقبة المحيط والكشف عن أي تحركات مشبوهة، دون استهداف شخص بعينه.

ثانياً: التحري الأمني. وهو الذي يهدف إلى جمع معلومات أولية عن واقعة أو نشاط أو شخص، بقصد التحقق منها وتقدير دلالتها. ويخضع لضوابط المشروعية والاختصاص والغرض والتناسب، وقد يستلزم إنفاً بحسب طبيعة الإجراء ودرجة تدخله في الحقوق [١٢]. ومن أمثلته جمع معلومات عن مجموعة مسلحة في منطقة جبلية، أو عن شخص مشتبّه في التحضير لعمل إرهابي، حيث يكون الغرض جمع معلومات أولية تمهد لقرار أمني أو إجراء لاحق.

ثالثاً: جمع الأدلة الجنائية الرقمية. وهو الذي يهدف إلى الحصول على أدلة قابلة للاستخدام في إجراء قضائي، ويخضع لضوابط إضافية تتعلق بالأصالة والسلامة وسلسلة العهدة وقواعد القبول [١٣]. ومن أمثلته تصوير مسرح جريمة إرهابية جواً، أو توثيق تسجيلات طائرة كانت تراقب مجموعة مسلحة، ثم تُستخدم هذه المخرجات في تحقيق قضائي.

ولا يعني التداخل العملي بين هذه الأنماط اندماجها قانوناً؛ فقد يبدأ الاستخدام وقائياً ثم يتحول إلى تحري أو جمع أدلة، ويقتضي ذلك إعادة تقييم الأساس القانوني والضمانات. ويُستفاد من هذا التمييز أن الطائرة المسيّرة أداة، وطبيعة الإجراء تتحدد بالغرض والسياق والآثار، لا بالوسيلة وحدها. فالقدرة التقنية على التحليق والتصوير لا تنشئ بذاتها سلطة قانونية لجمع الأدلة أو المراقبة المستمرة، كما أن وصف الإجراء بأنه وقائي لا يعفي من ضوابط الخصوصية إذا كان يجمع معلومات عن أشخاص محددين [14].

المبحث الثاني: المشروعية القانونية للمراقبة والرصد الجوي بالطائرات المسيّرة

المطلب الأول: الأساس القانوني لاستخدام الطائرات المسيّرة في التحري الأمني

يقتضي مبدأ المشروعية أن يستند استخدام الطائرات المسيّرة في التحري الأمني إلى أساس قانوني واضح يحدد الجهة المختصة، والغرض، ونطاق السلطة، والقيود، والضمانات. ولا يكفي أن تكون الطائرة قادرة تقنياً على التحليق والتصوير حتى يصبح استخدامها جائزاً قانوناً؛ فالقدرة التقنية لا تنشئ اختصاصاً، وعدم وجود حظر تقني لا يعني الجواز القانوني. [15]

ويستمد الأساس القانوني من التشريعات الوطنية المنظمة للطيران المدني وأمن الطيران، وقوانين الشرطة والإجراءات الجزائية، وقوانين حماية البيانات [١٦]، ومن اللوائح التنظيمية الصادرة عن هيئات الطيران المدني بشأن تراخيص التشغيل والمناطق المحظورة والارتفاعات [١٧]، ومن المعايير الدولية ذات الصلة كاتفاقية شيكاغو للطيران المدني الدولي وملاحقها وإرشادات منظمة الطيران المدني الدولي بشأن الطائرات دون طيار [١٨]، ومن الاتفاقيات الدولية ذات الصلة بالأدلة الإلكترونية والتعاون الجنائي كاتفاقية بودابست في حدود انطباقها. [19]

غير أنه لا ينبغي أن يُفهم وجود ترخيص طيران على أنه يمنح تلقائياً سلطة جمع البيانات أو المراقبة؛ فالترخيص التنظيمي للطيران يختلف عن السند القانوني للتحري. فالترخيص يجيز التشغيل من حيث السلامة والملاحة، لكنه لا يجيز بالضرورة جمع البيانات الشخصية أو المراقبة المستمرة أو الوصول إلى أماكن محمية. وقد يتطلب التحري إذنًا إضافياً بحسب طبيعة البيانات والغرض، ويظل التقييم القانوني لكل إجراء قائماً على حدة [٢٠]. وفي مكافحة الإرهاب، قد يكون هناك تشريع خاص يمنح صلاحيات استثنائية، لكنه لا يعفي من ضرورة التناسب والرقابة، ولا يحول دون خضوع الاستخدام للضمانات الأساسية.

المطلب الثاني: الاختصاص والإذن وحدود التدخل في الحياة الخاصة

لا يكفي وجود أساس قانوني عام؛ بل يجب تحديد الجهة المختصة بإصدار قرار استخدام الطائرة، والجهة المنفذة، والجهة التي تراقب، والجهة التي تقيم النتائج. ويختلف الاختصاص بحسب الغرض: وقائي، أو تحري، أو جمع أدلة [٢١]. فقد تكون جهة الشرطة مختصة بالتحري، بينما تكون جهة الطيران المدني مختصة بالترخيص، وجهة أخرى مختصة بالرقابة، ولا يجوز الخلط بين هذه الأدوار. وفي مكافحة الإرهاب، قد تتعدد الجهات (أمنية، عسكرية، استخباراتية)، مما يستلزم تنسيقاً دقيقاً وتوزيعاً واضحاً للمسؤوليات.

أما الإذن، فقد يشترط القانون إذنًا قضائياً مسبقاً لبعض الاستخدامات التي تنطوي على تدخل جوهري في الخصوصية، مثل المراقبة المستمرة لشخص معين أو تصوير أماكن خاصة [٢٢]. ولا يصح افتراض أن كل استخدام للطائرة يستلزم إذنًا قضائياً، كما لا يصح افتراض أن الترخيص التنظيمي يكفي في جميع الحالات. فالمعيار هو طبيعة التدخل في الحقوق، لا مجرد وجود الطائرة. وفي تأمين الفعاليات الكبرى، قد يكون الإذن إدارياً لمراقبة الحشود، لكنه لا يمتد إلى تتبع شخص بعينه دون سند قضائي.

وفيما يتعلق بحدود التدخل في الحياة الخاصة، يجب التمييز بين التصوير في الأماكن العامة والأماكن الخاصة، وبين التصوير العابر والمراقبة المستمرة، ومراعاة التوقع المشروع للخصوصية لا مجرد التمييز المكاني [٢٣]. فالتحليق في الفضاء العام لا يبيح تصوير المنازل والأماكن الخاصة، كما أن التصوير العابر لا يبرر بناء سجل سلوكي عن الأشخاص. ويجب حماية الأشخاص غير المعنيين الذين يظهرون عرضاً في التسجيلات، وعدم افتراض أن مجرد وجودهم في مجال التصوير يبرر جمع بياناتهم أو الاحتفاظ بها [٢٤]. وهذا ما يظهر بوضوح في الحشود الكبيرة، حيث يظهر آلاف الأشخاص في تسجيل واحد، ولا يجوز الاحتفاظ ببياناتهم جميعاً دون ضرورة. ويؤكد العهد الدولي الخاص بالحقوق المدنية والسياسية في مادته السابعة عشرة أن التدخل في الخصوصية يجب أن يكون قانونياً وغير تعسفي [٢٥]، وهو ما يستلزم تقييماً دقيقاً لمدى تدخل الطائرة المسيّرة في الحياة الخاصة، لا الاكتفاء بوصفها وسيلة تقنية.

المطلب الثالث: مبدأ التناسب وضمانات حماية البيانات والأشخاص غير المعنيين بالتحري

يقتضي مبدأ التناسب أن تكون الوسيلة ملائمة للغرض، وأن تكون ضرورية، بمعنى عدم وجود بديل أقل تدخلاً يحقق الغرض ذاته، وأن يكون أثرها متناسباً مع أهمية الهدف [٢٦]. وفي سياق الطائرات المسيّرة، يعني ذلك تفضيل التصوير المحدود النطاق والمدة على المراقبة الواسعة المستمرة، وتحديد الارتفاع والمجال والمناطق المشمولة بدقة، وتجنب تصوير الأماكن الخاصة أو الأشخاص غير المعنيين إلا لضرورة. وفي مكافحة الإرهاب، قد يكون التدخل مبرراً بخطورة التهديد، لكنه يظل خاضعاً لاختبار التناسب، فلا يجوز مراقبة قرية كاملة لأسابيع لمجرد الاشتباه في شخص واحد.

وتتطلب حماية البيانات ضمانات عدة. فيجب تحديد الغرض قبل التحليق، وعدم إعادة استخدام البيانات لغرض آخر دون سند [٢٧]. ويجب تقليل البيانات إلى القدر اللازم، وحجب أو إخفاء هوية غير المعنيين عند الإمكان [٢٨]. ويجب ضبط الوصول إلى التسجيلات والبيانات الوصفية وقصرها على المخولين، وتحديد مدة الاحتفاظ وآلية الإتلاف بعد انتهاء الغرض، وتوثيق الإجراءات من خلال سلسلة العهدة وسجلات الوصول وقيم التجزئة. [29]

أما حماية الأشخاص غير المعنيين، فتقتضي التمييز بين المستهدفين مباشرة، والذين تظهر بياناتهم بسبب ارتباطهم بالواقعة، والذين يظهرون عرضاً. ولكل فئة ضوابط مختلفة في الاحتفاظ والاستخدام والإفصاح [٣٠]. فلا يجوز مثلاً الاحتفاظ ببيانات شخص ظهر عرضاً في تسجيل جوي لمجرد أنه كان في المكان، ما لم توجد صلة بالواقعة أو سند قانوني مستقل. وهذا ما يكتسب أهمية خاصة في تأمين المهرجانات والاحتفالات، حيث يظهر آلاف الأشخاص في تسجيل واحد، ولا يجوز تحويل هذا التسجيل إلى قاعدة بيانات سلوكية عنهم.

المبحث الثالث: القيمة الإثباتية للمخرجات الرقمية للطائرات المسيّرة

المطلب الأول: طبيعة الصور والتسجيلات الجوية والبيانات الوصفية المصاحبة لها

تنتج الطائرات المسيّرة ثلاثة أنواع من المخرجات الرقمية: الصور الثابتة والفيديو، سواء المرئي أو الحراري أو متعدد الأطياف؛ والبيانات الوصفية التي تشمل إحداثيات الموقع والارتفاع والسرعة واتجاه الطيران ووقت الإقلاع والهبوط وسجلات الرحلة وبيانات المستشعرات؛ وسجلات النظام التي تشمل سجلات التحكم والاتصال والأعطال.[31]

ولا تُعد هذه المخرجات أدلة بمجرد إنتاجها؛ فهي بيانات رقمية تحتاج إلى التحقق من أصالتها وسلامتها، وتقييم دلالتها، واستيفاء شروط القبول [٣٢]. ويجب التمييز بين ما تسجله الطائرة فعلاً، وهو الواقعة الفنية، وما يستنتجه المحلل، وهو التفسير، وما يثبت الدليل، وهو النتيجة الإثباتية. فالخلط بين هذه المستويات يؤدي إلى تحميل البيانات دلالة لا تحملها. فالصورة الجوية التي تُظهر شخصاً في مكان معين تثبت وجود شخص في المكان، لكنها لا تثبت تلقائياً هويته أو قصده أو مسؤوليته.[33]

المطلب الثاني: أصالة التسجيلات وسلامتها الفنية وسلسلة حيازتها

تتعلق الأصالة بالتحقق من أن التسجيل أو الصورة هي بالفعل المادة التي أنتجتها الطائرة المعنية، وليست نسخة معدلة أو مولدة. ويشمل ذلك التحقق من هوية الطائرة من خلال الرقم التسلسلي وسجل الطيران، وهوية الكاميرا أو المستشعر من خلال الطراز والإعدادات، وتطابق البيانات الوصفية مع سجلات الرحلة.[34]

أما السلامة الفنية، فتتعلق بالمحافظة على المادة من التغيير غير الموثق، والتحقق من ذلك باستخدام قيم التجزئة الرقمية، ومقارنة النسخ، وسجلات الوصول [٣٥]. فقيمة التجزئة تثبت تطابق المحتوى الرقمي بين نسختين، لكنها لا تثبت وحدها أصالة المصدر ولا صحة المضمون.

وسلسلة الحيازة تتعلق بتوثيق انتقال المادة من الطائرة إلى الجهة التي فحصتها، وتشمل استلام وحدة التخزين أو نسخ البيانات، وتوثيق تاريخ الاستلام وهوية المستلم، وتسجيل أي معالجة أو تحويل، وتوثيق أي نقل بين الجهات [٣٦]. ويُستفاد في ذلك من معايير التعامل مع الأدلة الرقمية، ومن إرشادات المستجيب الأول، التي تؤكد أهمية التوثيق منذ المرحلة الأولى [٣٧]. وفي قضايا الإرهاب، حيث قد تكون المخرجات حاسمة في إدانة أو تبرئة، تصبح سلسلة الحيازة أكثر أهمية، لأن أي خلل فيها قد يضعف الدليل أو يبطله.

المطلب الثالث: حجية الأدلة المستخلصة من الطائرات المسيّرة وحدود الاستدلال بها
لا تكتسب المخرجات الرقمية للطائرات المسيّرة حجية تلقائية بمجرد إنتاجها؛ بل تخضع لشروط القبول التي يقررها القانون المختص، من مشروعية الحصول، وأصالة، وسلامة، وعدم تلاعب، ولتقييم الوزن من حيث مدى الدلالة، والاتساق مع أدلة أخرى، ووجود تفسيرات بديلة.[38]

وثمة حدود للاستدلال يجب مراعاتها. فالصورة الجوية تثبت ما يظهر فيها، لكنها لا تثبت تلقائياً هوية الأشخاص أو القصد أو المسؤولية [٣٩]. والبيانات الوصفية تثبت موقع الطائرة، لكنها لا تثبت تلقائياً موقع الشخص أو هوية المشغل [٤٠]. والتسجيل الجوي قد يكون دليلاً على وقوع فعل مادي، لكنه لا يثبت النية أو الظروف القانونية

دون أدلة إضافية [٤١]. كما أن التوليد الاصطناعي والتعديل يمثلان تحدياً للأصالة، ويستلزمان فحصاً متعدد المستويات. [42]

ويجب التمييز بين الارتباط والسببية؛ فوجود شخص في مكان معين لا يثبت تلقائياً تسببه في واقعة، كما أن تزامن نشاط مع حدث لا يثبت علاقة سببية [٤٣]. والاستنتاج السليم هو الذي يحدد بوضوح ما تثبته البيانات مباشرة، وما تستنتجه على نحو احتمالي، وما لا تسمح المعطيات بالجزم به. وفي مكافحة الإرهاب، قد يكون التسجيل دليلاً على وجود شخص في موقع تدريب، لكنه لا يثبت وحده انتماءه إلى مجموعة إرهابية أو مشاركته في عمل معين دون أدلة أخرى.

المطلب الرابع: أثر المخالفات الإجرائية والعيوب الفنية في قبول الأدلة وتقدير قوتها الإثباتية

تختلف المخالفات الإجرائية عن العيوب الفنية، ولكل منهما أثر مختلف. فالمخالفات الإجرائية تشمل تجاوز الاختصاص، أو غياب الإذن الواجب، أو تجاوز نطاق الإذن، أو مخالفة قواعد الطيران [٤٤]. ويختلف أثرها بحسب التشريع: فقد تؤدي إلى استبعاد الدليل إذا كان القانون يقرر ذلك، أو إلى تقييد الاستناد أو إضعاف الوزن، أو إلى مسؤولية تأديبية أو مدنية أو جنائية دون استبعاد الدليل بالضرورة. [45]

أما العيوب الفنية، فتشمل عدم توثيق سلسلة العهدة، أو عدم التحقق من السلامة، أو عدم توثيق الأدوات [٤٦]. ويختلف أثرها أيضاً: فقد تؤدي إلى إضعاف القيمة الاستدلالية أو الحاجة إلى فحص إضافي، وقد لا تؤدي إلى الاستبعاد إذا أمكن التحقق من السلامة بوسائل أخرى. [47]

ويجب الفصل بين المخالفة القانونية والخلل الفني؛ فسلامة البيانات لا تصحح عدم المشروعية، وعدم المشروعية لا تثبت عدم السلامة [٤٨]. وقد أكد الاجتهاد القضائي الأوروبي في قضايا المراقبة أن تقييم مشروعية أنظمة المراقبة يجب أن يراعي مجموع الضمانات عبر مراحلها المختلفة، لا الاكتفاء بمرحلة واحدة. [49]

المبحث الرابع: التطبيقات الأمنية الكبرى والتهديدات والعوامل المؤثرة المطلب الأول: الرصد الجوي في مكافحة الإرهاب والمجموعات المسلحة

تعد مكافحة الإرهاب والمجموعات المسلحة من أبرز المجالات التي تبرر استخدام الطائرات المسيّرة في التحريات الأمنية الرقمية، نظراً لطبيعة هذه الجرائم التي تتسم بالسرية والانتشار الجغرافي وصعوبة الوصول إلى أماكن تركزها [٥٠]. فالطائرة المسيّرة تتيح مراقبة المناطق الجبلية والوعرة والحدودية التي يصعب على القوات الأرضية الوصول إليها، وتوفر صوراً ومقاطع فيديو حية أو مسجلة عن تحركات المجموعات، وأنماط نشاطها، ومواقع تركزها، ومخابئها المحتملة. كما تتيح رصد التجمعات والاجتماعات والتدريبات، وتتبع الأشخاص المشتبه فيهم، والتحقق من معلومات استخباراتية أولية.

وتكتسب هذه التطبيقات أهمية خاصة في السياق العربي، حيث تواجه بعض الدول مجموعات مسلحة في مناطق جبلية أو صحراوية أو حدودية، يصعب فيها الرصد الأرضي. فالطائرة المسيّرة توفر قدرة على المراقبة المستمرة نسبياً، وتقلل من مخاطر تعرض القوات الأرضية للكمان، وتتيح جمع معلومات دقيقة عن التضاريس والمباني

والأنفاق [٥١]. غير أن هذه التطبيقات تطرح إشكالات قانونية دقيقة. فمكافحة الإرهاب لا تعني منح الجهات الأمنية سلطة مفتوحة للمراقبة دون ضوابط. فالإذن القضائي أو التصريح المختص يظل مطلوباً للمراقبة المستمرة أو التصوير في أماكن خاصة. كما أن الطائرة قد تجمع معلومات عن أشخاص لا صلة لهم بالمجموعات المسلحة، كالمدنيين الذين يعيشون في مناطق العمليات، مما يستلزم تقليل البيانات وحماية غير المعنيين. ويجب التمييز بين المراقبة الوقائية في مناطق النزاع والمراقبة الموجهة لشخص معين، فالأولى قد تخضع لضوابط مختلفة عن الثانية. [52]

المطلب الثاني: تأمين الاحتفالات والمهرجانات والفعاليات الجماعية

تستخدم الطائرات المسيّرة بشكل متزايد في تأمين الاحتفالات الوطنية والمهرجانات والفعاليات الرياضية والثقافية والزيارات الرسمية. فهي توفر رؤية شاملة للميادين والطرق المؤدية إليها، وتتيح رصد الحشود وتحركاتها، والكشف عن أي تجمعات غير عادية أو سلوكيات مشبوهة، وتوجيه القوات الأرضية بدقة [٥٣]. كما تساعد في إدارة الأزمات والطوارئ، كحالات التدافع أو الحرائق أو الأعمال العدائية.

وفي السياق العربي، تكتسب هذه التطبيقات أهمية خاصة في تأمين مواسم الحج والعمرة، والاحتفالات الوطنية، والمهرجانات الثقافية، والقمم والزيارات الرسمية. فالطائرة المسيّرة تتيح مراقبة الحشود الكبيرة في الأماكن المقدسة والميادين العامة، وتقديم معلومات فورية عن الكثافة والتحركات، مما يساعد على اتخاذ قرارات سريعة [٥٤]. غير أن تأمين الفعاليات يطرح إشكالات قانونية تتعلق بالخصوصية والتناسب. فالحشود الكبيرة تضم أشخاصاً لا صلة لهم بأي خطر، ويجب تقليل جمع بياناتهم إلى الحد اللازم. كما أن المراقبة المستمرة للميادين قد تتحول إلى مراقبة سلوكية واسعة إذا لم تُضبط بالنطاق والمدة والغرض. ويجب التمييز بين المراقبة الوقائية العامة والمراقبة الموجهة لشخص معين، فالأولى قد تكتفي بضوابط إدارية، بينما الثانية قد تستلزم إذناً قضائياً. [55]

المطلب الثالث: التأمين العسكري والمنشآت الحيوية

تستخدم الطائرات المسيّرة أيضاً في تأمين المنشآت العسكرية والحوية، كالمطارات ومحطات الطاقة والسدود والأنابيب. فهي تتيح مراقبة محيط المنشأة، والكشف عن أي تحركات مشبوهة، والتحقق من سلامة السياج والممرات، والاستجابة السريعة لأي تهديد [٥٦]. كما تستخدم في تدريبات عسكرية وأمنية، وفي تقييم الأضرار بعد الهجمات.

وتطرح هذه التطبيقات إشكالات قانونية تتعلق بالاختصاص والسرية. فالمنشآت العسكرية قد تخضع لقواعد خاصة تحكم التصوير والوصول، ويجب التمييز بين المراقبة الدورية للمحيط والمراقبة الموجهة لشخص أو مجموعة. كما أن الطائرة قد تصور منشآت مدنية مجاورة، مما يستلزم حماية خصوصية العاملين فيها [٥٧]. ويجب أن تخضع هذه التطبيقات لضوابط واضحة تحدد من يحق له التحليق، وفي أي مناطق، ولأي غرض، مع مراعاة التداخل بين الاختصاص العسكري والأمني والمدني.

المطلب الرابع: العوامل الميدانية والبيئية المؤثرة على الرصد بالطائرات المسيّرة

لا يتحدد نجاح الرصد بالطائرات المسيّرة أو فشله بالوسيلة التقنية وحدها، ولا بالسند القانوني وحده، بل يتأثر بمجموعة من العوامل الميدانية والبيئية التي قد تعيق جمع المعلومات، أو تشوهها، أو تؤدي إلى استنتاجات غير دقيقة. وهذه العوامل لا تقل أهمية عن العوامل القانونية والتقنية، لأنها تمس صلاحية المخرجات ومدى قابليتها للاعتماد في التحري أو الإثبات. [58]

أولاً: العوامل الجوية. تُعد الأحوال الجوية من أكثر العوامل تأثيراً على الرصد الجوي. فالأمطار والرياح والضباب والغيوم والعواصف الرملية قد تحد من قدرة الطائرة على التحليق المستقر، أو تؤثر في جودة الصورة والفيديو، أو تعيق نقل البيانات [٥٩]. فالرياح القوية قد تسبب اهتزازاً في الكاميرا، مما يؤدي إلى صور غير واضحة يصعب معها التعرف على الوجوه أو التفاصيل الدقيقة. والأمطار قد تعيق عدسة الكاميرا أو تؤثر في الإشارات اللاسلكية. والضباب والغيوم قد تحجب الرؤية تماماً أو تقلل من مداها. والعواصف الرملية قد تلحق الضرر بالمستشعرات أو تعطل أنظمة الملاحة. وتؤثر هذه العوامل ليس فقط في جودة المخرجات، بل في مشروعية الرصد ذاتها؛ فإذا كان الغرض جمع معلومات دقيقة، وكانت الأحوال الجوية تمنع تحقيق هذا الغرض، فإن استمرار الرصد قد يصبح غير متناسب. كما أن المخرجات الناتجة عن رصد في ظروف جوية سيئة قد تكون مضللة إذا لم يُفصح عن الظروف التي جُمعت فيها. [60]

ثانياً: ازدحام الأسواق والأماكن العامة. لا تقل الأماكن المزدحمة، كالأسواق والميادين العامة والفعاليات الجماعية، تأثيراً على الرصد الجوي. فالازدحام الشديد قد يؤدي إلى تداخل الأشخاص في الصورة، بحيث يصعب تمييز شخص عن آخر أو تتبع حركة فرد بعينه [٦١]. وقد يؤدي إلى حجب الرؤية جزئياً أو كلياً عن بعض المناطق. وقد يزيد من احتمال ظهور أشخاص غير معنيين في التسجيلات، بما يثير مسائل حماية الخصوصية وتقليل البيانات. كما قد يؤدي الازدحام إلى تشويش الإشارات اللاسلكية أو تداخل في أنظمة الملاحة، خاصة في المناطق الحضرية الكثيفة. ويطرح الازدحام إشكالات قانونية إضافية؛ فقد يؤدي إلى توسع غير مبرر في جمع بيانات أشخاص لا صلة لهم بالواقعة، أو إلى ضعف دقة المخرجات بحيث لا تسمح الصورة بتحديد هوية الشخص المستهدف. [62]

ثالثاً: التملص والاختفاء في النقاط الميتة. من أبرز التحديات الميدانية ما يُعرف بـ "النقاط الميتة" أو "المناطق العمياء"، وهي المناطق التي لا تغطيها الكاميرا أو المستشعرات بسبب زاوية التصوير أو وجود عوائق طبيعية أو صناعية [٦٣]. وقد يلجأ الأشخاص المستهدفون إلى التملص من الرصد بالاختفاء في هذه النقاط، كالدخول إلى مباني أو أنفاق أو مناطق محجوبة بالأشجار أو المباني، أو تغيير مسارهم بسرعة، أو استخدام مركبات ذات سرعة عالية، أو اللجوء إلى أماكن مغلقة لا يمكن للطائرة تصويرها. ويطرح التملص إشكالات قانونية وفنية؛ فقد يؤدي إلى فقدان التسلسل في التسجيل، أو انقطاع المتابعة، مما يضعف قدرة المخرجات على إثبات واقعة معينة. وقد يؤدي إلى استنتاجات خاطئة إذا لم يُفصح عن الفجوات في التسجيل، أو إذا اعتُبر غياب الشخص عن مجال الرؤية دليلاً على عدم وجوده. كما أن التملص قد يدفع إلى

توسيع نطاق الرصد أو تمديد مدته أو استخدام وسائل أكثر تدخلاً، وهو ما يستلزم إعادة تقييم التناسب والضرورة.[64]

رابعاً: العوائق الطبيعية والصناعية. تؤثر التضاريس والعوائق الطبيعية، كالجبال والوديان والأشجار الكثيفة، والعوائق الصناعية، كالمباني العالية والأبراج وأنابيب النفط، في مدى الرؤية وزوايا التصوير [٦٥]. فقد تحجب هذه العوائق جزءاً من المشهد، أو تمنع الطائرة من التحليق على ارتفاع مناسب، أو تحد من مدى الإشارة. كما قد تؤدي إلى تشويش في أنظمة الملاحة أو الاتصال، خاصة في المناطق الجبلية أو الحضرية الكثيفة.

خامساً: العوامل البشرية والمؤسسية. إلى جانب العوامل الميدانية، تؤثر العوامل البشرية والمؤسسية في الرصد. فكفاءة المشغل وتدريبه على التعامل مع الظروف الجوية والازدحام والتملص تحدد قدرته على اتخاذ القرار المناسب [٦٦]. وخبرة المحلل في تفسير الصور والبيانات الوصفية تحدد دقة الاستنتاجات. والتحيز التأكيدي قد يدفع إلى تفسير المخرجات بما يتوافق مع فرضية مسبقة، حتى في ظل ظروف ميدانية غير مواتية. كما أن غياب التنسيق بين الجهات قد يؤدي إلى تداخل في الرصد أو تعارض في المخرجات.

سادساً: أثر هذه العوامل على المشروعية والقيمة الإثباتية. تؤثر هذه العوامل مجتمعة على مشروعية الرصد وقيمه الإثباتية. فمن ناحية المشروعية، قد يؤدي استمرار الرصد في ظروف جوية سيئة أو في مناطق مزدحمة أو مع تملص الهدف إلى انتفاء التناسب أو انتفاء الضرورة، مما قد يبطل الإجراء أو يضعف الاستناد إليه [٦٧]. ومن ناحية القيمة الإثباتية، قد تؤدي هذه العوامل إلى ضعف جودة المخرجات أو نقص اكتمالها أو احتمال تفسيرها الخاطئ، مما يستلزم الإفصاح عنها ومراعاة أثرها في تقييم الدليل. ومن ثم، فإن التقييم القانوني السليم للرصد لا يقتصر على فحص السند القانوني والاختصاص والإذن، بل يمتد إلى فحص الظروف الميدانية والبيئية التي جرى فيها الرصد، ومدى تأثيرها في المخرجات، وما إذا كانت قد أفصح عنها. ويُستحسن أن يتضمن التقرير الفني أو الأمني وصفاً للظروف الجوية والميدانية، وبيان الفجوات أو القيود التي أثرت في التسجيل، وتحديد ما لم يتمكن الرصد من إثباته بسبب هذه العوامل.[68]

المطلب الخامس: التهديدات الأمنية التي تواجه الطائرات المسيّرة أثناء الرصد الجوي

لا تتحرك الطائرات المسيّرة في بيئة عمليات آمنة، بل تواجه في سياق مكافحة الإرهاب والمجموعات المسلحة والجرائم الخطيرة تهديدات متعددة قد تعيق مهامها، أو تشوه مخرجاتها، أو تؤدي إلى فقدانها [٦٩]. وهذه التهديدات لا تقل أهمية عن التحديات القانونية والفنية، لأنها تمس سلامة الإجراء وموثوقية المخرجات وقابلية الاعتماد عليها في التحري أو الإثبات.

أولاً: التهديدات المادية المباشرة (الاستهداف الجسدي). قد تتعرض الطائرة المسيّرة للاستهداف المباشر من قبل المجموعات المسلحة أو المجرمين الخطرين، باستخدام

الأسلحة النارية أو الصواريخ المحمولة أو الطائرات المسيّرة المعادية [٧٠]. ففي مناطق النزاع، قد تكون الطائرة هدفاً سهلاً إذا حُلقت على ارتفاع منخفض أو اقتربت من مواقع تركز المجموعات. وقد يؤدي إسقاط الطائرة إلى فقدان المخرجات، أو تدميرها، أو وقوعها في يد الخصم، مما قد يكشف قدرات الجهة الأمنية أو أساليب عملها. ويطرح ذلك إشكالات قانونية تتعلق بمسؤولية الجهة عن حمايتها، وحدود المخاطرة المسموح بها في جمع المعلومات، ومصير المخرجات إذا سقطت في يد الغير. [71]

ثانياً: التشويش الإلكتروني واعتراض الإشارات. تتعرض الطائرات المسيّرة أثناء الرصد الجوي لتهديدات إلكترونية خطيرة، منها التشويش على إشارات التحكم والملاحة (GPS)، أو اعتراض الاتصالات بين الطائرة ومحطة التحكم، أو اختراق أنظمة الطائرة والتحكم بها [٧٢]. ويؤدي التشويش إلى فقدان السيطرة على الطائرة، أو انحرافها عن مسارها، أو تعطيل قدرتها على البث أو التسجيل. كما قد يؤدي اعتراض الإشارات إلى كشف موقع الطائرة ومحطة التحكم، مما يعرض الطاقم الأرضي للخطر. ويطرح ذلك إشكالات قانونية تتعلق بسلامة البيانات (هل يمكن الاعتماد على مخرجات طائرة تعرضت للتشويش؟)، ومسؤولية الجهة عن أي أضرار ناتجة عن فقدان السيطرة، وحماية المعلومات التي قد تُعترض. [73]

ثالثاً: التضليل والخداع (التمويه والإخفاء). قد تلجأ المجموعات المسلحة أو المجرمون إلى التضليل لإفشال الرصد الجوي، باستخدام التمويه (أزياء مدنية، مركبات مدنية)، أو الإخفاء (أنفاق، مباني مغلقة، غطاء نباتي كثيف)، أو الطعم (مجسمات، مركبات مفخخة، تحركات وهمية) [٧٤]. وقد يؤدي ذلك إلى استنتاجات خاطئة إذا لم يُفصح عن احتمالات التضليل، أو إذا اعتُبر كل ما ترصده الطائرة حقيقة نهائية. ويطرح ذلك إشكالات قانونية تتعلق بحدود الاستدلال (ما تثبته الصورة وما لا تثبته)، وضرورة اختبار الفرضيات البديلة، والإفصاح عن القيود في التقرير. [75]

رابعاً: التهديدات السيبرانية (الاختراق والقرصنة). قد تتعرض أنظمة الطائرة المسيّرة (نظام التحكم، نظام الملاحة، نظام الكاميرا، نظام التخزين) للاختراق من قبل جهات مسلحة أو مجرمين سيبرانيين [٧٦]. ويؤدي الاختراق إلى تغيير مسار الطائرة، أو تعطيل الكاميرا، أو حذف المخرجات، أو تسريب البيانات إلى جهات غير مخولة. ويطرح ذلك إشكالات قانونية تتعلق بأمن المعلومات، وحماية البيانات، والمسؤولية عن التسريب، وسلامة المخرجات (هل يمكن الاعتماد على تسجيلات طائرة تعرضت للاختراق؟). [77]

خامساً: التهديدات المرتبطة بالطقس والبيئة. إلى جانب التهديدات المتعمدة، تواجه الطائرات المسيّرة تهديدات طبيعية، كالأمطار والرياح والضباب والعواصف الرملية، التي قد تؤدي إلى فقدان الطائرة أو تلف معداتها أو ضعف جودة مخرجاتها [٧٨]. وقد تؤدي هذه التهديدات إلى انقطاع الرصد في لحظة حرجية، مما قد يؤثر على اكتمال المعلومات وقابلية الاعتماد عليها. ويطرح ذلك إشكالات قانونية تتعلق بالإفصاح عن

الظروف الجوية، وأثرها في تفسير المخرجات، ومدى تناسب الاستمرار في الرصد في ظل ظروف غير مواتية.

سادساً: التهديدات المرتبطة بالطيران المدني. في المناطق الحضرية أو القريبة من المطارات، قد تتعرض الطائرات المسيّرة لتهديدات مرتبطة بالطيران المدني، كالتصادم مع طائرات أخرى، أو التداخل مع أنظمة الملاحة، أو مخالفة قواعد الطيران [٧٩]. وقد يؤدي ذلك إلى حوادث أو إصابات أو أضرار، مما يطرح إشكالات قانونية تتعلق بالمسؤولية المدنية، والاختصاص، والتنسيق بين الجهات.

سابعاً: أثر هذه التهديدات على المشروعية والقيمة الإثباتية. تؤثر هذه التهديدات مجتمعة على مشروعية الرصد وقيّمته الإثباتية. فمن ناحية المشروعية، قد يؤدي استمرار الرصد في ظل تهديدات أمنية خطيرة إلى انتفاء التناسب أو انتفاء الضرورة، إذا كان الخطر على الطائرة أو الطاقم الأرضي أكبر من الفائدة المرجوة [٨٠]. ومن ناحية القيمة الإثباتية، قد تؤدي هذه التهديدات إلى فقدان المخرجات، أو تضعف جودتها، أو تثير الشك في سلامتها، مما يستلزم الإفصاح عنها ومراعاة أثرها في تقييم الدليل. ويُستحسن أن تتضمن خطط الطيران تقييماً مسبقاً للتهديدات، وأن تتضمن التقارير الفنية وصفاً للتهديدات التي واجهتها الطائرة، ومدى تأثيرها في المخرجات، وما إذا كانت هناك مخاطر أمنية قد تستوجب إعادة الرصد أو استخدام وسيلة بديلة [81].

ثامناً: الضمانات المقترحة لمواجهة هذه التهديدات. لمواجهة هذه التهديدات، يمكن اقتراح ضمانات عدة: تقييم مسبق للمخاطر قبل كل مهمة، يشمل التهديدات المادية والإلكترونية والسيبرانية؛ وتشفير الاتصالات والبيانات؛ وأنظمة احتياطية للتحكم والملاحة؛ وتدريب المشغلين على التعامل مع التهديدات؛ وتنسيق مع الجهات المختصة (الدفاع الجوي، الطيران المدني، الأمن السيبراني)؛ وتوثيق التهديدات التي واجهتها الطائرة، وأثرها في المخرجات، في التقارير الفنية. [82]

المطلب السادس: التحديات القانونية المرتبطة بالخصوصية والاختصاص وتداول البيانات

تثير الطائرات المسيّرة تحديات قانونية متعددة. فمن حيث الخصوصية، قد يكشف التصوير الجوي تفاصيل داخل المنازل أو الأماكن الخاصة، وقد تسمح المراقبة المستمرة ببناء ملف سلوكي عن الأشخاص، وقد يعرض التصوير أشخاصاً غير معنيين لم يكن لهم صلة بالواقعة [٨٣]. ومن حيث الاختصاص، يبرز تداخل الاختصاص بين جهات الطيران المدني والأمن والدفاع، وتعدد الجهات التي تستخدم الطائرات، وإشكالات الطيران عبر الحدود [٨٤]. ومن حيث تداول البيانات، فإن نقل التسجيلات بين الجهات قد يوسع دائرة الوصول، ومشاركتها مع جهات أجنبية أو خاصة قد تخضع لقيود، والاحتفاظ طويل الأمد يزيد مخاطر التسريب. [85]

المطلب السابع: التحديات الفنية المتعلقة بموثوقية التسجيلات والتحليل الآلي للصور

تتعلق التحديات الفنية بموثوقية التسجيلات والتحليل الآلي. فجودة الصورة تتأثر بالإضاءة والطقس والاهتزاز، ودقة البيانات الوصفية تتأثر بإعدادات النظام وظروف التشغيل، وإمكان التعديل أو التوليد الاصطناعي يمثل تحدياً للأصالة [٨٦]. كما أن أنظمة التعرف على الوجوه قد تنتج إيجابيات أو سلبيات كاذبة، والتحليل الآلي قد يتأثر بتحيزات البيانات المستخدمة في التدريب، ونتائج الأدوات الآلية تحتاج إلى تحقق بشري مستقل [٨٧]. وقد أكدت إرشادات المعايير الفنية أن أدوات الكشف لها حدود، ولا ينبغي الاعتماد عليها وحدها. [88]

المطلب الثامن: الضمانات التشريعية والإجرائية والفنية المقترحة لتنظيم الاستخدام
تتطلب معالجة هذه التحديات ضمانات متكاملة. فالضمانات التشريعية تشمل نصاً صريحاً يحدد اختصاصات استخدام الطائرات في التحري الأمني، وتحديد الحالات التي تستلزم إذناً قضائياً أو تصريحاً إدارياً، وضوابط الخصوصية وحماية البيانات، والمسؤولية عن المخالفات [٨٩]. والضمانات الإجرائية تشمل توثيق الغرض والنطاق والمدة قبل التحليق، وتسجيل الإجراءات والقائمين بها، وسلسلة عهدة موثوقة للمخرجات، ومراجعة مستقلة للقرارات الحساسة [٩٠]. أما الضمانات الفنية فتشمل استخدام أنظمة موثوقة وتوثيق إصداراتها، والتحقق من الأصالة والسلامة، وحماية البيانات من التعديل والتسريب، وتدريب العاملين على الحدود القانونية والفنية. [91]

المراجع :

- (1) خراشي، عادل عبد العال. ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي. الإسكندرية: دار الجامعة الجديدة، ٢٠٠٦.
- (2) شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. صنعاء: مكتبة الصديق، ٢٠٠٥.
- (3) محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. الإسكندرية: دار المطبوعات الجامعية، ٢٠١٥.
- (4) خراشي، عادل عبد العال. ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي. مرجع سابق، ص ٤٠٠-٤٠٥.
- (5) شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. مرجع سابق، الفصل الخاص بالتحريات والاستدلالات.
- (6) محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. مرجع سابق، ص ٥٠٠-٥٠٥.
- (7) شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. مرجع سابق.
- (8) محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. مرجع سابق، ص ٥١٠-٥١٥.
- (9) خراشي، عادل عبد العال. ضوابط التحري والاستدلال. مرجع سابق، ص ٤١٠-٤١٥.
- (10) شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. مرجع سابق.
- (11) محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. مرجع سابق، ص ٥٢٠-٥٢٥.
- (12) خراشي، عادل عبد العال. ضوابط التحري والاستدلال. مرجع سابق، ص ٤٢٠-٤٢٥.
- (13) شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. مرجع سابق.
- (14) محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. مرجع سابق، ص ٥٣٠-٥٣٥.
- (15) خراشي، عادل عبد العال. ضوابط التحري والاستدلال. مرجع سابق، ص ٤٣٠-٤٣٥.
- (16) شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. مرجع سابق.
- (17) محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. مرجع سابق، ص ٥٤٠-٥٤٥.
- (18) خراشي، عادل عبد العال. ضوابط التحري والاستدلال. مرجع سابق، ص ٤٤٠-٤٤٥.
- (19) شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. مرجع سابق.
- (20) محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. مرجع سابق، ص ٥٥٠-٥٥٥.
- (21) خراشي، عادل عبد العال. ضوابط التحري والاستدلال. مرجع سابق، ص ٤٥٠-٤٥٥.
- (22) شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. مرجع سابق.
- (23) محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. مرجع سابق، ص ٥٦٠-٥٦٥.

- (24) خراشي، عادل عبد العال. ضوابط التحري والاستدلال. مرجع سابق، ص ٤٦٠-٤٦٥.
- (25) شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. مرجع سابق.
- (26) محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. مرجع سابق، ص ٥٧٠-٥٧٥.
- (27) خراشي، عادل عبد العال. ضوابط التحري والاستدلال. مرجع سابق، ص ٤٧٠-٤٧٥.
- (28) شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. مرجع سابق.
- (29) محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. مرجع سابق، ص ٥٨٠-٥٨٥.
- (30) خراشي، عادل عبد العال. ضوابط التحري والاستدلال. مرجع سابق، ص ٤٨٠-٤٨٥.
- (31) United Nations. International Covenant on Civil and Political Rights. Adopted by General Assembly Resolution 2200A (XXI), 16 December 1966, Article 17.
- (32) ICAO. Unmanned Aircraft Systems (UAS). Cir 328, Montréal: International Civil Aviation Organization, 2011.
- (33) Convention on International Civil Aviation. Chicago, 7 December 1944, ICAO Doc 7300.
- (34) Council of Europe. Convention on Cybercrime. ETS No. 185, Budapest, 23 November 2001.
- (35) Human Rights Center, University of California, Berkeley, & UN OHCHR. Berkeley Protocol on Digital Open Source Investigations. Geneva and New York: United Nations, 2022, HR/PUB/20/2.
- (36) INTERPOL. Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence. Lyon: INTERPOL Innovation Centre.
- (37) UNODC. Cybercrime Module 6: Handling of Digital Evidence. Education for Justice Initiative. Vienna: United Nations Office on Drugs and Crime, 2019.
- (38) ISO/IEC 27037:2012. Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva: ISO, 2012.
- (39) NIST. Guide to Integrating Forensic Techniques into Incident Response. Special Publication 800-86. Gaithersburg, MD: National Institute of Standards and Technology, 2006.
- (40) NIST. Secure Hash Standard (SHS). Federal Information Processing Standards Publication 180-4. Gaithersburg, MD: National Institute of Standards and Technology, 2015.
- (41) NIST. Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency. NIST AI 100-4. Gaithersburg, MD: National Institute of Standards and Technology, 2024.
- (42) UNODC. Cybercrime Module 3: The Role of Cybercrime Law. Education for Justice Initiative. Vienna: United Nations Office on Drugs and Crime, 2019.
- (43) Council of Europe. Explanatory Report to the Convention on Cybercrime. Budapest, 2001.
- (44) ECtHR. Big Brother Watch and Others v. the United Kingdom. Applications nos. 58170/13, 62322/14 and 24960/15, Grand Chamber, Judgment of 25 May 2021.
- (45) ECtHR. Roman Zakharov v. Russia. Application no. 47143/06, Grand Chamber, Judgment of 4 December 2015.
- (46) ECtHR. Szabó and Vissy v. Hungary. Application no. 37138/14, Judgment of 12 January 2016.
- (47) UN Human Rights Council. The Right to Privacy in the Digital Age. A/HRC/48/31, 2021.
- (48) UN Human Rights Council. Resolution 48/4: The Right to Privacy in the Digital Age. A/HRC/RES/48/4, 7 October 2021.

- (49) OECD. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449, 2019 (amended 2024).
- (50) ISO/IEC 23894:2023. Information Technology — Artificial Intelligence — Guidance on Risk Management. Geneva: ISO, 2023.
- (51) ISO/IEC 17025:2017. General Requirements for the Competence of Testing and Calibration Laboratories. Geneva: ISO, 2017.
- (52) ISO/IEC 27042:2015. Information Technology — Security Techniques — Guidelines for the Analysis and Interpretation of Digital Evidence. Geneva: ISO, 2015.
- (53) ISO/IEC 27043:2015. Information Technology — Security Techniques — Incident Investigation Principles and Processes. Geneva: ISO, 2015.
- (54) UNODC. Cybercrime Module 6: Digital Evidence Admissibility. Education for Justice Initiative. Vienna: United Nations Office on Drugs and Crime, 2019.
- (55) INTERPOL. Guidelines for Digital Forensics First Responders. مرجع سابق.
- (56) NIST. Digital Investigation Techniques: A NIST Scientific Foundation Review. NISTIR 8354. Gaithersburg, MD: National Institute of Standards and Technology, 2022.
- (57) NIST. Digital Evidence Preservation: Considerations for Evidence Handlers. NISTIR 8387. Gaithersburg, MD: National Institute of Standards and Technology, 2022.
- (58) Ayers, Rick; Brothers, Sam; Jansen, Wayne. Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 Rev.1. Gaithersburg, MD: National Institute of Standards and Technology, 2014.
- (59) College of Policing. Intelligence Cycle. Authorised Professional Practice. London: College of Policing.
- (60) College of Policing. Intelligence Strategy. Authorised Professional Practice. London: College of Policing.
- (61) College of Policing. Evaluation. Authorised Professional Practice. London: College of Policing.
- (62) College of Policing. Intelligence Management. Authorised Professional Practice. London: College of Policing.
- (63) GDPR. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union, L 119, 4 May 2016.
- (64) Bahrain Personal Data Protection Law No. 30 of 2018.
- (65) Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. ETS No. 108, Strasbourg, 28 January 1981.
- (66) Council of Europe. Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data. CETS No. 223, 2018.
- (67) Council of Europe. Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence. CETS No. 224, 2022.
- (68) UN General Assembly. Basic Principles on the Independence of the Judiciary. Adopted by the Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Milan, 1985, and endorsed by General Assembly resolutions 40/32 and 40/146.
- (69) UN Human Rights Council. The Right to Privacy in the Digital Age. A/HRC/27/37, 30 June 2014.
- (70) UN Human Rights Council. The Right to Privacy in the Digital Age. A/HRC/39/29, 3 August 2018.
- (71) UNODC. Counter-Terrorism Legal Training Curriculum: Module on International Cooperation in Criminal Matters. Vienna: United Nations Office on Drugs and Crime.

- (72) INTERPOL. Counter-Terrorism: INTERPOL's Role and Activities. Lyon: INTERPOL.
- (73) UN Security Council. Resolution 2396 (2017) on Threats to International Peace and Security Caused by Terrorist Acts. S/RES/2396, 21 December 2017.
- (74) UN Security Council. Resolution 2341 (2017) on Threats to Critical Infrastructure. S/RES/2341, 13 February 2017.
- (75) ICAO. Annex 17 to the Convention on International Civil Aviation: Security — Safeguarding International Civil Aviation Against Acts of Unlawful Interference. 10th ed., 2017.
- (76) ICAO. Annex 9 to the Convention on International Civil Aviation: Facilitation. 15th ed., 2017.
- (77) ISO 31000:2018. Risk Management — Guidelines. Geneva: ISO, 2018.
- (78) ISO 22301:2019. Security and Resilience — Business Continuity Management Systems — Requirements. Geneva: ISO, 2019.
- (79) IEC 31010:2019. Risk Management — Risk Assessment Techniques. Geneva: IEC, 2019.
- (80) NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology, 2018.
- (81) NIST. Cybersecurity Framework 2.0. Gaithersburg, MD: National Institute of Standards and Technology, 2024.
- (82) ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva: ISO, 2022.
- (83) ISO/IEC 27035-1:2023. Information Technology — Information Security Incident Management — Part 1: Principles and Process. Geneva: ISO, 2023.
- (84) UNODC. Comprehensive Study on Cybercrime. Vienna: United Nations Office on Drugs and Crime, 2013.
- (85) Council of Europe. Cybercrime Convention Committee (T-CY). Assessment Report on the Second Additional Protocol. Strasbourg, 2022.
- (86) European Union Agency for Cybersecurity (ENISA). Threat Landscape Report. Athens: ENISA, 2024.
- (87) European Union Agency for Cybersecurity (ENISA). Drones and Cybersecurity: Challenges and Opportunities. Athens: ENISA, 2021.
- (88) Federal Aviation Administration (FAA). Unmanned Aircraft Systems (UAS) Traffic Management (UTM) Concept of Operations. Washington, DC: FAA, 2020.
- (89) European Aviation Safety Agency (EASA). Opinion No 01/2018: Unmanned Aircraft Systems. Cologne: EASA, 2018.
- (90) European Aviation Safety Agency (EASA). Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and (EU) 2019/945). Cologne: EASA, 2023.
- (91) International Air Transport Association (IATA). Security Manual: Best Practices for Aviation Security. Montreal: IATA, 2023.

الجدول المقارن: الرصد الوقائي والتحري الأمني وجمع الأدلة

المعيار	جمع الأدلة الجنائية	التحري الأمني	الرصد الوقائي
الغرض	الحصول على أدلة للإثبات	جمع معلومات أولية	منع المخاطر
السند	إذن قضائي وضوابط إجرائية	سند قانوني وإذن بحسب الحالة	ترخيص تنظيمي وصلاحيات إدارية
الخصوصية	تدخل مرتفع	تدخل متوسط إلى مرتفع	تدخل منخفض إلى متوسط
الضمانات	سلسلة عهدة وأصالة وسلامة	توثيق وتحديد نطاق ورقابة	تناسب وتقليل بيانات
القيمة الإثباتية	دليل قابل للتقديم وفق الشروط	مؤشرات أولية	لا تُستخدم كدليل مباشر

النافذة التطبيقية

السيناريو: واقعة سرقة في منشأة صناعية، وتستخدم الجهة الأمنية طائرة مسيرة لتصوير مسرح الجريمة جواً.

تبدأ الخطوة الأولى بالتحقق من سند استخدام الطائرة، من ترخيص طيران وصلاحيات تحري، وتحديد الغرض وهو تصوير مسرح الجريمة. ثم تحدد الخطوة الثانية النطاق، من منطقة التحليق والارتفاع والمدة، مع تجنب تصوير المنازل المجاورة. وتتضمن الخطوة الثالثة تسجيل سجلات الرحلة والبيانات الوصفية وتوثيق تاريخ التصوير. أما الخطوة الرابعة فتشمل إنشاء نسخة من وحدة التخزين، وحساب قيم التجزئة، وتوثيق سلسلة العهدة. ثم تنتقل الخطوة الخامسة إلى فحص الصور والفيديو، والتحقق من الأصالة، وتحليل البيانات الوصفية، والبحث عن تفسيرات بديلة، مع مراعاة الظروف الجوية والميدانية التي أثرت في التسجيل. وتنتهي الخطوة السادسة بالإفصاح عن القيود، من جودة الصورة ودقة الموقع وعدم حسم هوية الأشخاص والفجوات الناتجة عن التملص أو العوائق. والدرس المستفاد أن الطائرة أداة، وأن القيمة الإثباتية تتوقف على المشروعية والأصالة والسلامة والدلالة، لا على التقنية وحدها.

النتائج:

١. الطائرات المسيرة أداة متعددة الوظائف في المراقبة والرصد وجمع المعلومات، لكنها لا تكتسب مشروعية بمجرد قدرتها التقنية.
٢. التمييز بين الرصد الوقائي والتحري الأمني وجمع الأدلة ضروري لتحديد السند والضمانات.
٣. مشروعية الاستخدام تتطلب أساساً قانونياً واضحاً، واختصاصاً محدداً، وإذناً حيث يلزم، وتناسباً.
٤. حماية الخصوصية تتطلب ضوابط للنطاق والمدة والارتفاع، وحماية غير المعنيين، وتقليل البيانات.
٥. القيمة الإثباتية للمخرجات تتوقف على الأصالة والسلامة وسلسلة العهدة، لا على التقنية وحدها.
٦. حدود الاستدلال: الصورة تثبت ما يظهر، لا الهوية أو القصد أو المسؤولية تلقائياً.

٧. المخالفات الإجرائية والعيوب الفنية لهما آثار مختلفة، ويجب الفصل بينهما.
٨. العوامل الميدانية والبيئية (الأحوال الجوية، الازدحام، التملص، العوائق) تؤثر في مشروعية الرصد وقيمتة الإثباتية، ويجب الإفصاح عنها.
٩. التهديدات الأمنية (الاستهداف، التشويش، التضليل، الاختراق) تؤثر في مشروعية الرصد وموثوقية المخرجات، ويجب تقييمها مسبقاً والإفصاح عنها.
١٠. التطبيقات الأمنية الكبرى (مكافحة الإرهاب، تأمين الفعاليات، التأمين العسكري) تبرر استخدام الطائرات المسيّرة، لكنها تطرح إشكالات قانونية خاصة تستلزم ضوابط دقيقة.
١١. التحديات القانونية والفنية تستلزم ضمانات تشريعية وإجرائية وفنية متكاملة.

التوصيات:

١. إصدار تشريع أو لائحة تنظم استخدام الطائرات المسيّرة في التحري الأمني، تحدد الاختصاصات والإذن والضمانات.
٢. اعتماد بروتوكول وطني لسلسلة العهدة الرقمية لمخرجات الطائرات.
٣. تدريب العاملين على الحدود القانونية والفنية، وعلى التحقق من الأصالة والسلامة، وعلى التعامل مع الظروف الميدانية والتهديدات الأمنية.
٤. تعزيز الرقابة المستقلة على استخدام الطائرات في التحري.
٥. تطوير معايير فنية وطنية للتحقق من التسجيلات الجوية والبيانات الوصفية.
٦. تعزيز التعاون الدولي في مجال الطائرات المسيّرة والأدلة الرقمية العابرة للحدود.
٧. إدراج تقييم مسبق للمخاطر القانونية والحقوقية والأمنية في خطط تأمين الفعاليات الكبرى وعمليات مكافحة الإرهاب.

المراجع

أولاً: المراجع العربية

١. خراشي، عادل عبد العال. ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي. 2006.
٢. شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. صنعاء: مكتبة الصادق، ٢٠٠٥.
٣. محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. الإسكندرية: دار المطبوعات الجامعية، ٢٠١٥.
٤. United Nations. *International Covenant on Civil and Political Rights*. 1966, Article 17.
٥. ICAO. *Unmanned Aircraft Systems (UAS)*. Cir 328, 2011.
٦. Convention on International Civil Aviation. Chicago, 1944.
٧. Council of Europe. *Convention on Cybercrime*. ETS No. 185, 2001.
٨. Human Rights Center, UC Berkeley, & UN OHCHR. *Berkeley Protocol on Digital Open Source Investigations*. 2022.
٩. INTERPOL. *Guidelines for Digital Forensics First Responders*.
١٠. UNODC. *Cybercrime Module 6: Handling of Digital Evidence*. 2019.
١١. ISO/IEC 27037:2012. *Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*.
١٢. NIST. *Guide to Integrating Forensic Techniques into Incident Response*. NIST SP 800-86, 2006.
١٣. NIST. *Secure Hash Standard (SHS)*. FIPS PUB 180-4, 2015.
١٤. NIST. *Reducing Risks Posed by Synthetic Content*. NIST AI 100-4, 2024.

❖ النافذة التطبيقية

السيناريو: واقعة سرقة في منشأة تجارية، تتوافر فيها كاميرات مراقبة، وبوابة دخول إلكترونية، وهاتف محمول لأحد المشتبه فيهم.

- **الخطوة الأولى (الرصد الثابت):** طلب تسجيلات الكاميرات للفترة الزمنية المحددة (لا كل اليوم)، وتوثيق الجهة المسلمة والفترة والوسيط. لا يكفي وجود الكاميرا لإباحة كل استخدام لاحق.
- **الخطوة الثانية (سجلات الدخول):** مراجعة سجلات البوابة للفترة ذاتها، مع التحقق من توقيت النظام والمنطقة الزمنية.
- **الخطوة الثالثة (الرصد المتحرك):** إذا استدعى الأمر تتبع حركة المشتبه فيه، يجب التحقق من السند القانوني (إذن قضائي بحسب التشريع)، وتحديد المدة والنطاق.
- **الخطوة الرابعة (فحص الهاتف):** يتطلب إنفاً محدد النطاق (فترة، نوع بيانات)، مع التمييز بين البيانات المحلية والسحابية. فحص الهاتف لا يمتد تلقائياً إلى الحساب السحابي.
- **الخطوة الخامسة (التوثيق):** سلسلة العهدة لكل مادة، وقيم التجزئة للتحقق من السلامة، وتسجيل القيود (مثلاً: تعذر فك تشفير رسالة معينة).
- **الدرس:** كل وسيلة لها درجة تدخل وسند وضمانات مختلفة؛ والانتقال من وسيلة إلى أخرى يتطلب تقييماً مستقلاً.

النتائج العامة للفصل

١. الرصد الأمني الرقمي لا يتحدد بالأداة، بل بطبيعة النشاط والغرض ودرجة التدخل والسند القانوني.
٢. الطبيعة التراكمية للرصد تستلزم تقييم الأثر المجموع، لا كل معلومة منفردة.
٣. تصنيف وسائل الرصد يتطلب معايير متعددة (طبيعة البيانات، طريقة الحصول، النطاق، درجة التدخل، الغرض).
٤. الضوابط المشتركة (الشرعية، الاختصاص، الغرض، الضرورة، التناسب، النطاق، حماية الغير، أمن المعلومات، تقييد الاستخدام، الرقابة) إطار متكامل لا يُختزل في إذن.
٥. الرصد الثابت (كاميرات، سجلات) يتطلب تقييم الغرض والنطاق والمدة والاحتفاظ، ولا يكفي وجود الكاميرا لإباحة كل استخدام.
٦. الرصد المتحرك (تتبع الموقع) قد يكشف أنماطاً تفصيلية، ولا يجوز الخلط بين موقع الجهاز وموقع الشخص.

٧. جمع التسجيلات وحفظها يتطلب سلسلة عهدة، وتمييز الأصل عن النسخ المعالجة، وتوثيق القيود.
٨. التصوير والرصد المستمر يستلزم ضوابط خاصة لحماية الخصوصية، وبيانات الغير، والتسجيل الصوتي.
٩. بيانات الاتصالات ليست فئة واحدة؛ والتمييز بين المحتوى والبيانات الوصفية لا يعني أن الثانية أقل حماية بالضرورة.
١٠. الحصول على بيانات الاتصالات يتطلب أساساً قانونياً، واختصاصاً، وإذناً حيث يلزم، وتحديد نطاق، ورقابة مستقلة.
١١. الوصول إلى الأجهزة لا يعني الوصول إلى كل بياناتها؛ والإذن بالفحص يجب أن يكون محدد النطاق.
١٢. البيانات السحابية والتشفير تثير قيوداً قانونية وفنية متداخلة؛ ويجب التمييز بين الوجود والوصول والجواز.
١٣. التعاون الدولي يجب ألا يكون مساراً بديلاً لتجاوز الضمانات.

المراجع:

- (1) عادل عبد العال خراشي، ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي، ٢٠٠٦، ص ٩٠-٩٥
- (2) هشام مصطفى محمد، التحريات الأمنية وأثرها في الأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٥، ص ١٠٠-١٠٥
- (3) محمد محمد سيف شجاع، شرح قانون الإجراءات الجزائية اليمني، مكتبة الصادق، صنعاء، ٢٠٠٥، (الفصل الخاص بالتحريات).
- (4) الأمم المتحدة، العهد الدولي الخاص بالحقوق المدنية والسياسية، ١٩٦٦، المادة ١٧
- (5) مفوضية الأمم المتحدة السامية لحقوق الإنسان، A/HRC/51/17، ٢٠٢٢، الفقرات ٢٠-٢٥
- (6) المرجع السابق، الفقرة ٢٦
- (7) Kent et al., *Guide to Integrating Forensic Techniques into Incident Response*, NIST SP 800-86, 2006, at 3-1
- (8) A/HRC/51/17، مرجع سابق، الفقرة ٢٧
- (9) ECtHR, *Big Brother Watch and Others v. the United Kingdom*, nos. 58170/13, 62322/14, 24960/15, 25 May 2021
- (10) NIST SP 800-86, *supra* note 7, at 4-1
- (11) خراشي، مرجع سابق، ص ١١٠-١١٥
- (12) شجاع، مرجع سابق.
- (13) هشام مصطفى، مرجع سابق، ص ١١٠-١١٥
- (14) Council of Europe, *Convention on Cybercrime*, ETS No. 185, 2001, Articles 20-21
- (15) A/HRC/51/17، مرجع سابق، الفقرة ٢٨
- (16) NIST SP 800-86, *supra* note 7, at 3-2
- (17) A/HRC/51/17، مرجع سابق، الفقرة ٣٣
- (18) شجاع، مرجع سابق.
- (19) خراشي، مرجع سابق، ص ١٢٠-١٢٥
- (20) Council of Europe, *Convention on Cybercrime*, *supra* note 14, Articles 19-21

- A/HRC/51/17 (21)، مرجع سابق، الفقرة ٢٩
(22) المرجع السابق، الفقرة ٣٠.
- (23) هشام مصطفى، مرجع سابق، ص ١٢٠-١٢٥
A/HRC/51/17 (24)، مرجع سابق، الفقرة ٣١
(25) خراشي، مرجع سابق، ص ١٣٠-١٣٥
A/HRC/51/17 (26)، مرجع سابق، الفقرة ٣٢
(27) شجاع، مرجع سابق.
(28) خراشي، مرجع سابق، ص ١٤٠-١٤٥
A/HRC/51/17 (29)، مرجع سابق، الفقرات ٣٥-٤٠.
(30) شجاع، مرجع سابق.
A/HRC/51/17 (31)، مرجع سابق، الفقرة ٣٦
(32) المرجع السابق، الفقرات ٣٧-٣٨
- (33) UN Human Rights Council, *Resolution 48/4: The Right to Privacy in the Digital Age*, A/HRC/RES/48/4, 7 October 2021
- (34) خراشي، مرجع سابق، ص ١٥٠-١٥٥
A/HRC/51/17 (35)، مرجع سابق، الفقرة ٢٩
NIST SP 800-86, *supra* note 7, at 4-2 (36)
A/HRC/51/17 (37)، مرجع سابق، الفقرة ٣٦
(38) المرجع السابق، الفقرة ٤٠.
(39) خراشي، مرجع سابق، ص ١٦٠-١٦٥
(40) هشام مصطفى، مرجع سابق، ص ١٣٠-١٣٥
(41) المرجع السابق، ص ١٣٥-١٤٠.
(42) شجاع، مرجع سابق.
(43) هشام مصطفى، مرجع سابق، ص ١٤٠-١٤٥
A/HRC/51/17 (44)، مرجع سابق، الفقرة ٣٨
- (45) INTERPOL, *Guidelines for Digital Forensics First Responders*, at 10-12
(46) المرجع السابق، at 12-15
- (47) Berkeley Protocol, *supra* note 1, at 45-48
(48) NIST SP 800-86, *supra* note 7, at 4-3
(49) A/HRC/RES/48/4, *supra* note 33
(50) هشام مصطفى، مرجع سابق، ص ١٤٥-١٥٠.
(51) المرجع السابق، ص ١٥٠-١٥٥
(52) شجاع، مرجع سابق.
(53) خراشي، مرجع سابق، ص ١٧٠-١٧٥
A/HRC/51/17 (54)، مرجع سابق، الفقرة ٢٨
(55) هشام مصطفى، مرجع سابق، ص ١٥٥-١٦٠.
(56) Berkeley Protocol, *supra* note 1, at 50-52
A/HRC/51/17 (57)، مرجع سابق، الفقرة ٣٠.
(58) Berkeley Protocol, *supra* note 1, at 55-58
(59) INTERPOL, *supra* note 45, at 20-22
(60) المرجع السابق، at 22-25
(61) NIST SP 800-86, *supra* note 7, at 4-4
(62) Ayers et al., *Guidelines on Mobile Device Forensics*, NIST SP 800-101 Rev.1, 2014, at 3-1
(63) INTERPOL, *supra* note 45, at 25-28
(64) المرجع السابق، at 28-30.
(65) NIST SP 800-86, *supra* note 7, at 4-5
(66) المرجع السابق، at 4-6
(67) INTERPOL, *supra* note 45, at 30-32
(68) هشام مصطفى، مرجع سابق، ص ١٦٠-١٦٥

- A/HRC/51/17 (69)، مرجع سابق، الفقرة ٣١
(70) شجاع، مرجع سابق.
- A/HRC/51/17 (71)، مرجع سابق، الفقرة ٣٣
(72) المرجع السابق، الفقرة ٢٩
- ETS No. 185, *supra* note 14, Article 21 (73)
A/HRC/51/17 (74)، مرجع سابق، الفقرة ٤٠.
- (75) المرجع السابق، الفقرة ٣٦
(76) المرجع السابق، الفقرة ٤٥
(77) خراشي، مرجع سابق، ص ١٨٠-١٨٥
- ETS No. 185, *supra* note 14, Article 1 (78)
(79) المرجع السابق، Article 21
(80) المرجع السابق، Article 18
(81) المرجع السابق، Article 20.
- A/HRC/51/17 (82)، مرجع سابق، الفقرة ٢٨
(83) NIST SP 800-86, *supra* note 7, at 3-3
(84) ETS No. 185, *supra* note 14, Article 15
(85) شجاع، مرجع سابق.
- A/HRC/51/17 (86)، مرجع سابق، الفقرة ٣٥
(87) خراشي، مرجع سابق، ص ١٩٠-١٩٥
A/HRC/51/17 (88)، مرجع سابق، الفقرة ٤٠.
- Big Brother Watch*, *supra* note 9 (89)
(90) ETS No. 185, *supra* note 14, Article 15
A/HRC/51/17 (91)، مرجع سابق، الفقرة ٤٢
(92) NIST SP 800-86, *supra* note 7, at 4-7
A/HRC/51/17 (93)، مرجع سابق، الفقرة ٤٣
(94) Ayers et al., *supra* note 62, at 2-1
(95) المرجع السابق، at 2-2
- ETS No. 185, *supra* note 14, Article 19 (96)
(97) Ayers et al., *supra* note 62, at 2-3
(98) المرجع السابق، at 2-4
- A/HRC/51/17 (99)، مرجع سابق، الفقرة ٤٤
(100) Ayers et al., *supra* note 62, at 2-5
A/HRC/51/17 (101)، مرجع سابق، الفقرة ٢٩
(102) NIST SP 800-86, *supra* note 7, at 4-8
A/HRC/51/17 (103)، مرجع سابق، الفقرة ٤٤
(104) المرجع السابق، الفقرة ٤٥
- ETS No. 185, *supra* note 14, Article 19 (105)
(106) المرجع السابق.
- Ayers et al., *supra* note 62, at 2-6 (107)
(108) NIST SP 800-86, *supra* note 7, at 4-9
(109) ETS No. 185, *supra* note 14, Article 18
(110) المرجع السابق، Articles 23-35
A/HRC/51/17 (111)، مرجع سابق، الفقرة ٤٦
(112) ETS No. 185, *supra* note 14, Article 16
(113) خراشي، مرجع سابق، ص ٢٠٠-٢٠٥

الفصل الثالث: تحليل المعلومات الرقمية والتحقق من موثوقيتها

المبحث الأول: منهجية تحليل المعلومات الرقمية

المطلب الأول: تنظيم البيانات وتصنيفها

يمثل تنظيم البيانات الرقمية وتصنيفها المرحلة التأسيسية في عملية التحليل الأمني؛ إذ لا تتحدد القيمة العملية للمعلومات بكمية البيانات أو تنوع مصادرها فحسب، وإنما تتوقف كذلك على سلامة تنظيمها، ودقة تصنيفها، وإمكان تتبع مصادرها، والقدرة على التمييز بين ما تتضمنه من وقائع قابلة للتحقق وما قد تنطوي عليه من مؤشرات أو افتراضات أولية. [1] وتزداد أهمية هذه المرحلة بالنظر إلى أن البيئة الرقمية تتيح إنتاج كميات ضخمة من البيانات المتباينة، مما يجعل التعامل معها دون منهج منضبط مدخلاً محتملاً للخطأ في التقدير الأمني.

ويقصد بتنظيم البيانات إخضاع المواد المتحصلة من مصادرها المختلفة لعملية منهجية تتيح ترتيبها واسترجاعها ومقارنتها وتحليل العلاقات القائمة بينها، مع المحافظة على بيانات المصدر وسياق الحصول عليها. أما تصنيفها، فيتمثل في إسناد كل مادة إلى فئة محددة وفق معايير معلومة، مثل نوع المصدر، وطبيعة البيانات، وتاريخ الحصول، ومدى التحقق، والصلة بالمسألة، والقيود القانونية أو الفنية. [2]

ولا ينبغي أن يُفهم التنظيم باعتباره إجراءً تقنياً محضاً؛ لأنه يتضمن اختيارات منهجية تؤثر في النتائج. فتحديد الفئات، واختيار معايير الفرز، وتقرير البيانات التي تستحق المقارنة، كلها عمليات قد توجه انتباه المحلل إلى علاقات معينة دون غيرها. ومن ثم، فإن التنظيم غير المحايد قد يؤدي إلى إظهار نمط معين مع إغفال أنماط بديلة، حتى عندما تكون البيانات الأصلية صحيحة. [3]

ويقتضي التنظيم العلمي التمييز بين عدة مستويات متكاملة:

١. **البيانات الأصلية:** المواد كما جُمعت من مصادرها أو استُخرجت من الأنظمة والأجهزة، بالقدر الذي يسمح بتحديد حالتها عند الجمع. ويجب المحافظة عليها وعدم استبدالها بالنسخ المعالجة دون توثيق. [4]
٢. **البيانات المستخرجة:** البيانات التي جرى انتقاؤها من مصدر أكبر لغرض فحص مسألة محددة. ويقتضي ذلك توثيق معيار الاستخراج وحدوده. [5]
٣. **البيانات المنظّمة:** البيانات التي أُعيد ترتيبها في جداول أو قواعد بيانات أو خطوط زمنية أو خرائط. [6]
٤. **المعلومات التحليلية:** النتائج الأولية التي تُستخلص من فحص البيانات ومقارنتها، كوجود تزامن بين حدثين أو تكرار نمط معين. [7]
٥. **الاستنتاجات التحليلية:** التقديرات التي يصل إليها المحلل بعد تقييم المعلومات واختبار التفسيرات الممكنة، مع بيان درجة الثقة والقيود. [8]

ويُستفاد من التمييز بين هذه المستويات أن انتقال البيانات من صورتها الخام إلى نتيجة تحليلية ليس عملية آلية محايدة، بل مسار تتدخل فيه عمليات الاختيار والتفسير والتقدير البشري. ولذلك يجب أن يظل كل استنتاج قابلاً للرد إلى البيانات التي استند إليها. ويتفق هذا التوجه مع المنهج الذي يعرضه **المعهد الوطني الأمريكي للمعايير والتقنية (NIST)** في الدليل الخاص بدمج تقنيات الأدلة الجنائية الرقمية في الاستجابة للحوادث، والذي يميز بين تحديد البيانات وحمايتها ومعالجتها وتحليلها ثم الإبلاغ عن النتائج. [9]

ومن الناحية التطبيقية، يتطلب تصنيف المعلومات مراعاة مصدرها وطبيعتها. فالمعلومات المنشورة في منصة اجتماعية تختلف عن سجلات الدخول إلى نظام إلكتروني، وكلاهما يختلف عن البيانات المستخرجة من جهاز محمول أو عن تسجيلات كاميرات المراقبة. ولا يصح إخضاع جميع هذه المواد لمعيار واحد؛ لأن لكل منها خصائص فنية ومواطن ضعف مختلفة. فالمحتوى المنشور قد يكون صحيحاً من حيث ما يظهره، لكنه غير موثوق من حيث نسبته إلى شخص معين، بينما قد يكون سجل النظام صادراً عن النظام المعني فعلاً، لكنه غير كافٍ وحده لتحديد الشخص الذي أجرى العملية. [10]

ويقتضي التنظيم إنشاء سجل يربط كل معلومة بمصدرها، وتاريخ الحصول، وطريقة الجمع، والشخص الذي تعامل معها، ومدى التحقق، وصلتها بالمسألة. وتكتسب هذه البيانات المصاحبة أهمية خاصة عندما يتعذر الرجوع إلى المصدر لاحقاً، كما يحدث عند حذف محتوى منشور أو تغيير صفحة إلكترونية أو انتهاء مدة الاحتفاظ بالسجلات. [11]

وتؤكد الممارسات المهنية لإدارة المعلومات الاستخباراتية أهمية تسجيل مصدر المعلومة وتقييم موثوقيتها وصلتها بالغرض الذي جُمعت من أجله، إلى جانب المحافظة على سجل يسمح بمراجعة كيفية التعامل معها. [12] ومع ذلك، ينبغي الحذر من الاعتقاد بأن جمع المعلومات في قاعدة بيانات موحدة يجعلها أكثر صحة بالضرورة. فقد يؤدي دمج قواعد بيانات متعددة إلى تكرار المعلومات ذاتها، أو إلى ربط سجلات تخص أشخاصاً مختلفين بسبب تشابه الأسماء أو المعارف، أو إلى نقل خطأ موجود في مصدر واحد إلى عدة منتجات تحليلية لاحقة. وقد تُضفي كثرة السجلات المتكررة انطباعاً زائفاً بأن المعلومة مدعومة بمصادر مستقلة. [13]

ومن هنا، يتعين التمييز بين تعدد السجلات وتعدد المصادر المستقلة، وبين كثرة البيانات وقوة الدلالة، وبين الاتساق الناتج عن صحة المعلومات والاتساق الناتج عن تكرار الخطأ نفسه. وتأسيساً على ذلك، فإن التنظيم المنهجي السليم لا يقتصر على ترتيب البيانات، وإنما يشمل المحافظة على نسبتها إلى مصادرها، وتحديد درجة استقلال تلك المصادر، وإظهار حدود المقارنة بينها. [14]

المطلب الثاني: الربط بين مصادر المعلومات المختلفة

يقصد بالربط بين مصادر المعلومات الرقمية إجراء المقارنة المنهجية بين البيانات المتحصلة من مصادر متعددة، بهدف تحديد أوجه الاتفاق والاختلاف بينها، واكتشاف العلاقات المحتملة، واختبار مدى اتساقها مع الفرضيات المتعلقة بالواقعة. ويُعد هذا الربط من أهم وظائف التحليل

الأمني؛ لأن المعلومة المنفردة قد تكون محدودة الدلالة، بينما تكتسب قيمة تفسيرية أكبر عندما تتوافق مع معلومات أخرى مستقلة. [15]

غير أن الربط لا يعني مجرد جمعها في ملف واحد أو ترتيبها بحسب التاريخ، بل يستلزم التحقق من طبيعة كل مصدر، ودرجة موثوقيته، واستقلاله عن المصادر الأخرى، ومدى صلاحية البيانات المستمدة منه للمقارنة. فالتوافق الظاهري بين معلومات متعددة لا يكفي لإثبات صحة الاستنتاج إذا كانت تلك المعلومات قد نشأت من أصل واحد، أو تأثرت بظروف مشتركة، أو استندت إلى افتراض غير متحقق. [16]

أنماط الربط:

أولاً: الربط الزمني. يقوم على مقارنة توقيتات الأحداث أو السجلات أو الاتصالات أو عمليات الدخول، بهدف تحديد التسلسل الزمني المحتمل للوقائع. ويقتضي مراعاة اختلاف إعدادات الساعات، والمناطق الزمنية، وطرق تسجيل الوقت، والتأخر في مزامنة الأنظمة. فقد يتضمن سجل إلكتروني توقيتاً يختلف عن توقيت تسجيل كاميرا مراقبة، دون أن يعني ذلك بالضرورة وجود تناقض حقيقي؛ إذ قد يكون الاختلاف ناشئاً عن عدم ضبط ساعة أحد النظامين أو عن استخدام أحدهما التوقيت العالمي المنسق والآخر التوقيت المحلي. كما قد يُسجل أحد الأنظمة وقت إنشاء الحدث، بينما يسجل نظام آخر وقت استلام البيانات أو معالجتها. [17]

ثانياً: الربط المكاني. يتعلق بمقارنة بيانات المواقع المستمدة من الأجهزة أو التطبيقات أو السجلات أو الصور أو أنظمة المراقبة. ويهدف إلى تحديد مدى توافق هذه البيانات مع وجود جهاز أو شخص أو مركبة في موقع معين خلال فترة محددة. غير أن الدلالة المكانية تختلف باختلاف طريقة توليد البيانات ودقتها. فبيانات تحديد الموقع الصادرة عن جهاز قد تشير إلى موقع الجهاز، لكنها لا تثبت وحدها أن مالكه كان يحمله أو يستخدمه في اللحظة ذاتها. كما أن وجود جهاز ضمن نطاق جغرافي معين لا يثبت بالضرورة أن الجهاز كان موجوداً في نقطة محددة، خصوصاً عندما تكون دقة التحديد محدودة. [18]

ثالثاً: الربط الموضوعي أو الدلالي. يتمثل في مقارنة مضمون البيانات المختلفة لتحديد مدى ارتباطها بموضوع التحري، مثل مقارنة محتوى منشور رقمي بسجل إلكتروني أو تسجيل مرئي أو إفادة شخص. ويستهدف اختبار مدى توافق الروايات أو المعلومات مع الوقائع المتاحة، والكشف عن التناقضات أو أوجه الدعم المتبادل. ومع ذلك، فإن التشابه في المضمون لا يثبت بالضرورة وحدة المصدر أو صحة النسبة. فقد تتطابق معلومات منشورة في عدة مواقع لأنها منقولة من منشور واحد، وقد يظهر تشابه بين محتوىين بسبب استخدام مصدر عام مشترك [19].

وتبرز أهمية هذه التفرقة عند التعامل مع المصادر المفتوحة؛ إذ يشير بروتوكول بيركلي للتحقيقات الرقمية المعتمدة على المصادر المفتوحة إلى أهمية اتباع منهج منظم في جمع المواد الرقمية وتحليلها وحفظها، مع مراعاة السياق وسلامة المعلومات وإمكان استخدامها في عمليات التحقق اللاحقة. [20]

ولا تقتصر الصعوبات المرتبطة بالربط على الجوانب الفنية، بل تمتد إلى مشكلة الاستقلال بين الأدلة والمصادر. فقد تعتمد عدة تقارير على قاعدة البيانات نفسها، أو تستند مواقع إخبارية متعددة إلى بيان واحد، أو تعيد حسابات مختلفة نشر المحتوى ذاته. وفي هذه الحالات، لا يمثل التوافق بين المصادر تأييداً مستقلاً بالضرورة، بل قد يكون انعكاساً لانتشار معلومة واحدة عبر قنوات متعددة. [21]

ولمعالجة هذه المشكلة، ينبغي إنشاء خريطة للعلاقات بين المصادر توضح أصل كل معلومة، والمصادر التي نقلتها، ومدى استقلالها، وأوجه التأييد أو التعارض بينها. ويُستحسن تحديد ما إذا كان التوافق قائماً على مشاهدة مباشرة، أو نقل عن الغير، أو استنتاج تحليلي، لأن اختلاف طبيعة المعرفة يؤثر في مقدار الثقة. [22]

ومن جهة أخرى، ينبغي عدم قصر الربط على البحث عن المعلومات المؤيدة للفرضية الأمنية. فالمقارنة العلمية تتطلب البحث عن البيانات التي قد تناقض الفرضية أو تضعفها، وإعطاء هذه البيانات وزناً يتناسب مع قوتها، بدل استبعادها لمجرد تعارضها مع التصور الأولي. [23]

وتبعاً لذلك، فإن القيمة الحقيقية للربط لا تكمن في الوصول إلى أكبر عدد من العلاقات، وإنما في تحديد العلاقات التي يمكن تفسيرها والتحقق منها، وتمييز العلاقات المؤكدة من الروابط المحتملة التي تحتاج إلى مزيد من الفحص. [24]

المطلب الثالث: التمييز بين الملاحظة والواقعة والاستنتاج

يُعد التمييز بين الملاحظة والواقعة والاستنتاج من الضوابط الأساسية للتحليل الأمني الرقمي؛ لأنه يمنع الخلط بين ما تعرضه البيانات مباشرة وما يُستخلص منها، ويحد من تحويل الاحتمالات إلى حقائق مقررّة دون سند كافٍ. [25]

ويقصد بـ **الملاحظة** وصف ما أمكن رصده في البيانات أو المحتوى الرقمي وصفاً مباشراً، دون إضافة تفسير يتجاوز ما يظهره المصدر. أما **الواقعة**، فيُقصد بها الحدث أو الحالة التي يراد التحقق من حدوثها، والتي قد تُدعم بملاحظة واحدة أو مجموعة من المعلومات والأدلة. في حين يشير **الاستنتاج** إلى النتيجة التي يصل إليها المحلل من خلال تفسير البيانات وربطها ببعضها، وفق افتراضات أو قواعد استدلالية محددة. [26]

ولا تتطابق هذه المستويات بالضرورة؛ فالملاحظة قد تكون دقيقة، لكن تفسيرها قد يكون خاطئاً، كما أن الواقعة قد تكون صحيحة مع بقاء هوية الفاعل أو قصده غير معلومين. ومن ثم، لا يكفي التحقق من صحة الملاحظة لإثبات جميع النتائج التي يراد استخلاصها منها. [27]

فإذا أظهر تسجيل مرئي شخصاً يدخل مبنى في وقت معين، فإن الملاحظة المباشرة تتمثل في ظهور شخص في التسجيل وعبره مدخل المبنى. أما القول إن الشخص هو فرد محدد، أو إنه دخل المبنى لغرض غير مشروع، أو إنه ارتكب فعلاً مجرماً، فهي استنتاجات إضافية تتطلب أدلة أخرى تتناسب مع طبيعتها. [28]

وقد تكون صورة رقمية أصلية وسليمة من الناحية الفنية، ومع ذلك لا تثبت وحدها هوية الشخص الظاهر فيها، أو زمان التقاطها، أو المكان الذي التُقطت فيه، إذا لم تتوافر معلومات

موثوقة تسند هذه العناصر. وتكشف هذه الحالة عن ضرورة الفصل بين سلامة المادة الرقمية وبين الدلالة التي يمكن استخلاصها منها. [29]

جدول توضيحي:

ما لا يثبت بمفرده	مثال توضيحي	طبيعته	المستوى
هوية قائدها أو الغرض من وجودها	ظهور مركبة في تسجيل مرئي	وصف مباشر لما يظهر في المصدر	الملاحظة
مسؤولية شخص معين عن حدث مرتبط بها	وجود المركبة في الموقع وقت الواقعة	حدث يراد تحديد مدى حدوثه	الواقعة محل التحقق
ثبوت المسؤولية الجنائية دون استكمال عناصر الإثبات	احتمال ارتباط المركبة بالواقعة	تفسير تحليلي يستند إلى مجموعة من المعطيات	الاستنتاج

ويجب التنبيه إلى أن وصف حدث بأنه "واقعة ثابتة" يتوقف على معيار التحقق المعتمد والسياق الذي تُستخدم فيه النتيجة. فقد تكون الواقعة متحققة على مستوى أولي يكفي لتوجيه البحث الأمني، دون أن تكون قد استوفت الشروط القانونية اللازمة لإثباتها أمام القضاء. لذلك، من الأدق بيان درجة التحقق بدل استخدام وصف مطلق بالثبوت عندما تكون الأدلة المتاحة محدودة. [30]

ويزداد خطر الخلط بين الملاحظة والاستنتاج عند استخدام أدوات التحليل الآلي، بما فيها تقنيات التعرف على الصور أو تحليل الأنماط أو ربط الحسابات الرقمية. فقد تُنتج الأداة نتيجة تصنيفية، مثل ترجيح تطابق وجهين أو وجود تشابه بين ملفين، لكن هذه النتيجة تظل مخرجاً تقنياً يحتاج إلى تفسير في ضوء دقة الأداة وظروف استخدامها واحتمالات الخطأ فيها. [31]

ولا يجوز الانتقال من القول إن النظام أظهر درجة تشابه معينة إلى الجزم بأن الشخصين هما الشخص ذاته، ما لم تسمح المنهجية المستخدمة بذلك، وبعد تقييم حدودها الفنية. كما ينبغي التمييز بين النتيجة التي تنتجها الأداة وبين الاستنتاج الذي يتبناه المحلل بناءً عليها. [32]

ومن الناحية المهنية، يقتضي هذا التمييز أن يُصاغ التقرير الأمني بطريقة تفصل بين الوقائع التي تدعمها المصادر مباشرة، والمعلومات التي لم يكتمل التحقق منها، والتقديرات التحليلية، والفرضيات التي لا تزال قيد الاختبار. ويساعد هذا الفصل على منع انتقال الاستنتاجات الأولية إلى السجلات المؤسسية بوصفها حقائق نهائية. [33]

وتتسق هذه المعالجة مع الممارسات المهنية التي تؤكد ضرورة تقييم مصدر المعلومات ومحتواها على نحو مستقل، وعدم المبالغة في قيمتها أو السماح للتقديرات الشخصية بأن تحل محل التقييم المستند إلى المعطيات المتاحة. [34]

وبذلك، فإن الفصل بين الملاحظة والواقعة والاستنتاج لا يمثل مجرد تفضيل أسلوب في كتابة التقارير، وإنما يشكل ضماناً منهجية لحماية سلامة الاستدلال، وإبقاء النتائج متناسبة مع ما تسمح به البيانات، وتمكين الجهات المختصة من مراجعة المسار الذي أدى إلى النتيجة. [35]

المطلب الرابع: تحديد الفرضيات التي يقوم عليها التحليل

لا ينطلق التحليل الأمني الرقمي من البيانات وحدها في جميع الأحوال، بل يتطلب غالباً صياغة فرضيات تفسر الوقائع المتاحة وتحدد المسارات التي ينبغي اختبارها. ويُقصد بالفرضية تفسير محتمل لواقعة أو مجموعة من الوقائع، يُستخدم لتوجيه عملية التحليل، ويظل قابلاً للمراجعة أو الرفض عند ظهور بيانات جديدة أو ثبوت قصور الأدلة. [36]

وتكمن أهمية تحديد الفرضيات في أنها تكشف الافتراضات التي يقوم عليها التفكير التحليلي، وتمنع إخفاء المقدمات غير المثبتة داخل الاستنتاج النهائي. فقد يستند التحليل، مثلاً، إلى افتراض أن حساباً إلكترونياً يعود إلى شخص معين، أو أن توقيت سجل رقمي يعكس وقت حدوث الواقعة، أو أن وجود جهاز في موقع ما يدل على وجود مالكه فيه. وهذه الافتراضات قد تكون صحيحة أو محتملة، لكنها لا تصبح حقائق بمجرد استخدامها في التحليل. [37]

ولذلك، ينبغي التمييز بين الفرضية التي يراد اختبارها والافتراض الذي يُستخدم مؤقتاً لإجراء الاختبار. فالفرضية هي التفسير محل الفحص، أما الافتراض فهو مقدمة قد يتوقف عليها الاستنتاج. وإذا لم تُختبر الافتراضات الجوهرية أو لم تُذكر في التقرير، فقد يبدو الاستنتاج أكثر قوة مما تسمح به الأدلة الفعلية. [38]

وتقتضي المنهجية المنضبطة تحديد الفرضيات قبل الانتهاء من التحليل، وتوضيح الأدلة التي يمكن أن تؤيد كل فرضية أو تضعفها، والبحث عن المعلومات التي تميز بينها. ويجب ألا يُختزل هذا العمل في اختيار فرضية واحدة ثم جمع البيانات المؤيدة لها، لأن ذلك يعرض المحلل لخطر **التحيز التأكيدي**، أي الميل إلى ملاحظة المعلومات التي توافق الاعتقاد الأولي وإهمال المعلومات المخالفة له. [39]

خطوات منهجية لبناء الفرضيات واختبارها:

١. تحديد المسألة التي يتعين تفسيرها بدقة، وتجنب صياغتها بطريقة تفترض مسبقاً صحة تفسير معين. [40]
٢. حصر الوقائع والملاحظات التي تدعمها المصادر المتاحة، مع الفصل بينها وبين المعلومات غير المتحقق منها. [41]
٣. صياغة أكثر من فرضية معقولة، بما فيها التفسيرات البديلة التي قد تفسر الوقائع ذاتها. [42]
٤. تحديد ما تتوقع كل فرضية وجوده من أدلة أو مؤشرات، وما قد يضعفها أو يناقضها. [43]
٥. فحص البيانات المؤيدة والمعارضة لكل فرضية، مع مراعاة جودة المصادر واستقلالها. [44]
٦. تحديد المعلومات الناقصة التي قد تؤثر في المفاضلة بين الفرضيات، والنظر في إمكان الحصول عليها بصورة مشروعة. [45]
٧. صياغة النتيجة بما يتناسب مع قوة الأدلة، مع بيان ما بقي غير محسوم. [46]

ولا يعني تعدد الفرضيات ضرورة معاملتها جميعاً على أنها متساوية في الاحتمال؛ إذ قد تكون بعض الفرضيات ضعيفة أو غير منسجمة مع المعطيات. لكن استبعاد أي فرضية ينبغي أن يقوم على أسباب قابلة للشرح والمراجعة، لا على مجرد مخالفتها للتصور الأولي. [47]

كما يجب الحذر من صياغة فرضيات لا يمكن اختبارها أو دحضها، لأن بقاء الفرضية متوافقة مع كل نتيجة ممكنة يجعلها قليلة القيمة التفسيرية. وينبغي أن يركز التحليل على الفرضيات التي يمكن التمييز بينها باستخدام معلومات قابلة للتحقق، مع الاعتراف بالحالات التي لا تسمح فيها البيانات المتاحة بالوصول إلى نتيجة حاسمة. [48]

وتتطلب الفرضيات المتعلقة بالأشخاص عناية إضافية؛ لأن تبني تفسير مبكر قد يؤثر في طريقة جمع المعلومات اللاحقة وفي تفسير السلوكيات المحايدة. فعندما يُفترض مسبقاً أن شخصاً معيناً مرتبط بواقعة، قد تُفسر اتصالاته أو تحركاته أو منشوراته الرقمية بوصفها مؤشرات مؤيدة للاشتباه، حتى عندما تكون لها تفسيرات عادية أو بديلة. [49]

ولهذا، ينبغي عدم الخلط بين بناء فرضية أمنية لتوجيه التحري وبين تقرير المسؤولية عن الفعل. فالفرضية أداة لتحديد المسارات البحثية، وليست نتيجة إثباتية مستقلة، كما أن استمرار البحث في اتجاه معين لا يبرر إغفال المعطيات التي قد تنفيه. [50]

ومن ثم، فإن جودة التحليل لا تقاس بمدى قدرته على تأكيد فرضية سابقة، وإنما بقدرته على اختبارها بموضوعية، والكشف عن حدودها، وتعديلها أو التخلي عنها متى أظهرت البيانات أن تفسيراً آخر أكثر اتساقاً معها. [51]

المبحث الثاني: تقييم المصادر والبيانات الوصفية

المطلب الأول: تقييم المصدر وتاريخ المعلومة وسياقها

لا يمكن تقدير موثوقية المعلومات الرقمية بمعزل عن مصدرها والظروف التي أنتجت فيها أو نُشرت أو جُمعت خلالها. فالمعلومة، مهما بدا مضمونها واضحاً، قد تفقد كثيراً من قيمتها إذا تعذر تحديد أصلها أو معرفة ما إذا كانت قد نُقلت من مصدر آخر أو عُدلت أو أُخرجت من سياقها. [52]

ويقصد بتقييم المصدر فحص الجهة أو النظام أو الشخص الذي صدرت عنه المعلومة، وتحديد مدى إمكان الاعتماد عليه بالنظر إلى طبيعة المصدر وسجله السابق وقدرته على تقديم معلومات صحيحة. أما تقييم المعلومة ذاتها، فيتعلق بفحص مضمونها ومدى اتساقها مع المعطيات الأخرى وإمكان التحقق منها بصورة مستقلة. [53]

ويجب الفصل بين الأمرين؛ فقد يكون المصدر معروفاً وموثوقاً في العموم، لكنه يقدم معلومة غير دقيقة في واقعة معينة. وعلى العكس، قد يصدر محتوى صحيح عن مصدر مجهول أو غير مجرب، ثم يتبين لاحقاً أنه مطابق للوقائع بعد التحقق المستقل. ومن ثم، لا تُعد سمعة المصدر بديلاً عن فحص محتوى المعلومة، كما لا يكفي عدم معرفة المصدر للحكم تلقائياً ببطئها [54].

معايير تقييم المعلومات الرقمية:

أولاً: منشأ المعلومة. يُقصد به تحديد المصدر الأصلي للمعلومة، لا الاكتفاء بالموقع أو الحساب الذي أعاد نشرها. فإذا انتشرت صورة في عدد من المنصات، فإن كثرة المنشورات لا تثبت تعدد مصادر الصورة، وقد يكون جميع الناشرين قد اعتمدوا على نسخة واحدة لا يُعرف منشؤها. ويستدعي ذلك البحث عن أقدم ظهور يمكن التحقق منه، وفحص الروابط بين النسخ المنشورة، ومقارنة المحتوى بالسياق الذي نُشر فيه أول مرة، مع تجنب الجزم بأن أقدم نسخة متاحة هي بالضرورة النسخة الأصلية. [55]

ثانياً: موثوقية المصدر. تتصل بمدى قدرته على تقديم معلومات صحيحة، ومدى إمكان تحديد هويته أو طبيعة النظام الذي أنتج البيانات، وسجله السابق عند توافر معلومات موثوقة عنه. وفي حالة المصادر التقنية، يجب فحص طريقة إنشاء السجلات، ومدى موثوقية النظام، واحتمالات تعرضه للتعديل أو الخلل. [56]

ثالثاً: مصداقية المحتوى. تتعلق بمدى اتساق المعلومات مع الوقائع المعروفة، وإمكان التحقق من عناصرها، ووجود ما يؤيدها أو يناقضها. ولا ينبغي الخلط بين المصداقية الظاهرية للمحتوى وصحته الفعلية؛ فقد يكون المحتوى مقنعاً من الناحية البصرية أو اللغوية، لكنه يتضمن معلومات مضللة أو تفاصيل جرى تعديلها. [57]

رابعاً: تاريخ المعلومة وسياقها. يجب التمييز بين تاريخ وقوع الحدث، وتاريخ تسجيله، وتاريخ نشر المحتوى، وتاريخ الحصول عليه من قبل جهة التحري. وقد تكون هذه التواريخ مختلفة،

ويؤدي الخلط بينها إلى استنتاجات خاطئة بشأن التسلسل الزمني أو صلة المحتوى بالواقعة. كما ينبغي فحص السياق المكاني والاجتماعي والموضوعي للمعلومة. فقد تكون الصورة حقيقية، لكن نسبتها إلى واقعة مختلفة أو استخدامها خارج سياقها الأصلي يجعل الاستنتاج المبني عليها مضللاً. [58]

خامساً: إمكانية التحقق المستقل. تزداد الثقة في المعلومة عندما يمكن فحصها بالرجوع إلى مصدر مستقل أو إلى بيانات أخرى لا تعتمد عليها مباشرة. غير أن التحقق المستقل لا يتحقق بمجرد العثور على نسخ إضافية للمحتوى ذاته، بل يتطلب معرفة أصل كل مصدر ومدى استقلاله عن غيره. [59]

وتدعم إرشادات إدارة المعلومات الاستخباراتية الصادرة عن كلية الشرطة البريطانية هذا الاتجاه، إذ تؤكد أهمية تقييم منشأ المعلومات ودقتها وموثوقيتها وصلتها بالغرض الأمني، فضلاً عن ضرورة ربط السجلات ذات الصلة وعدم المبالغة في قيمة المعلومات. [60]

ومن الناحية الزمنية، لا يكفي إثبات أن معلومة ما كانت منشورة في تاريخ معين لإثبات أنها تصف حدثاً وقع في ذلك التاريخ. فقد يُعاد نشر محتوى قديم على أنه حديث، أو يُستخدم تسجيل سابق في سياق جديد، أو تُعرض بيانات النظام وفق توقيت مختلف عن التوقيت المحلي. [61]

ولهذا، ينبغي التمييز بين تاريخ الحدث وتاريخ إنشاء الملف وتاريخ تعديله وتاريخ نشره وتاريخ جمعه. كما يجب توثيق مصدر كل توقيت وطريقة الحصول عليه، وعدم التعامل مع بيانات التاريخ الظاهرة في اسم الملف أو واجهة التطبيق على أنها دليل قاطع على زمن الواقعة. [62]

ويُراعى كذلك أن بعض المصادر قد تكون ذات مصلحة في توجيه تفسير معين، سواء كانت حسابات شخصية أو جهات إعلامية أو أطرافاً ذات صلة بالواقعة. ولا يعني وجود المصلحة أن كل ما يصدر عن المصدر غير صحيح، لكنه يمثل عاملاً ينبغي أخذه في الحسبان عند تقدير الموثوقية. [63]

وفي ضوء ذلك، ينبغي أن تتضمن عملية تقييم المصدر بياناً منفصلاً لدرجة الثقة في المصدر ودرجة الثقة في المعلومة، مع توضيح الأساس الذي استند إليه هذا التقييم. ولا يصح إسناد درجة ثقة مرتفعة إلى المعلومة لمجرد صدورها عن مصدر معروف، كما لا يصح استبعادها لمجرد أن مصدرها غير مألوف ما دام من الممكن التحقق من مضمونها بصورة مستقلة. [64]

المطلب الثاني: إمكان التحقق المستقل من المعلومات

يمثل التحقق المستقل إحدى الركائز الأساسية لتقييم موثوقية المعلومات الرقمية؛ لأنه يسمح بفحص مدى صحة المعلومة دون الاعتماد الحصري على المصدر الذي قدمها. وتتبع أهميته من أن المعلومات الرقمية قابلة للنسخ وإعادة النشر والتعديل، وقد تنتشر المعلومة الواحدة عبر منصات متعددة على نحو يوحي بأنها مدعومة بأدلة متنوعة، بينما تكون جميع النسخ مستمدة من أصل واحد. [65]

ويقصد بالتحقق المستقل اختبار المعلومات بالرجوع إلى مصادر أو وسائل فحص لا تعتمد، في جوهرها، على المصدر محل التقييم. وقد يكون ذلك من خلال سجل مستقل، أو تسجيل صادر عن نظام مختلف، أو وثيقة رسمية، أو مشاهدة مباشرة، أو فحص فني قابل لإعادة التنفيذ. [66]

ولا يشترط أن يكون المصدر المستقل مختلفاً في شكله الظاهري فقط؛ إذ يجب أن يكون مستقلاً من حيث أصل المعلومة وطريقة إنتاجها. فإذا نقلت ثلاث منصات إخبارية خبراً واحداً عن بيان صادر عن جهة واحدة، فإن تعدد المنصات لا يوفر بالضرورة ثلاثة مصادر مستقلة. وكذلك إذا أعادت عدة حسابات نشر صورة واحدة، فإن عدد الحسابات لا يعوض غياب التحقق من أصل الصورة. [67]

صور التحقق المستقل:

- **التحقق بالمصادر المستقلة:** مقارنة المعلومة ببيانات صادرة عن جهات أو أنظمة مستقلة عنها، مع فحص مدى استقلالها الفعلي. [68]
- **التحقق بالمقارنة الزمنية والمكانية:** مقارنة توقيتات المحتوى ومواقعه مع سجلات أو وقائع أخرى يمكن التحقق منها. [69]
- **التحقق الفني:** فحص الملف أو السجل أو البيانات الوصفية، والتحقق من خصائصه التقنية، والكشف عن مؤشرات التعديل المحتمل. [70]
- **التحقق السياقي:** فحص الظروف التي أنتجت فيها المعلومة أو نُشرت خلالها، ومدى توافقها مع الوقائع المعروفة. [71]
- **التحقق القابل لإعادة الفحص:** تمكين مراجع آخر من إعادة خطوات التحقق، باستخدام المواد المتاحة والمنهج الموثق. [72]

ويجب ألا يُفهم التحقق الفني باعتباره بديلاً عن التحقق من المضمون. فقد يثبت الفحص أن ملفاً لم يتغير منذ وقت محدد أو أن نسخة منه مطابقة لنسخة محفوظة، دون أن يثبت أن محتوى الملف صحيح أو أن المشهد المصور يمثل الواقعة المدعى بها. وبالمثل، قد تكون المعلومة صحيحة في مضمونها، لكن يتعذر إثبات مصدرها أو سلامة الطريق الذي وصلت به إلى جهة التحري. [73]

ومن هنا، يجب الفصل بين التحقق من أصالة الملف، والتحقق من سلامته، والتحقق من صحة مضمونه، والتحقق من نسبة المحتوى إلى شخص أو جهة معينة. فهذه مسائل مختلفة، وقد يتطلب كل منها وسائل مستقلة للفحص. [74]

ويبرز هذا التمييز في التحقق من الصور ومقاطع الفيديو؛ إذ قد تكشف المقارنة بين معالم المكان والطقس والإضاءة والمباني الظاهرة عن توافق المحتوى مع موقع أو فترة معينة، لكنها لا تثبت بالضرورة تاريخ التسجيل الأصلي أو هوية المصور. كما أن عدم اكتشاف علامات تعديل لا يعني أن الملف لم يتعرض للتلاعب، لأن بعض التعديلات قد لا تترك أثراً واضحاً. [75]

ويقتضي التحقق المستقل توثيق خطوات الفحص والمواد التي استند إليها والنتائج التي أسفر عنها، مع بيان الأدوات المستخدمة وإصداراتها عندما يكون لذلك أثر في النتيجة. ويجب أن يكون من الممكن التمييز بين ما توصل إليه الفاحص مباشرة وما استنتجه من مقارنة المواد أو تفسيرها. [76]

ويؤكد **بروتوكول بيركلي** أهمية الجمع والتحليل والحفظ بصورة مهنية ومنهجية، مع مراعاة إمكان مراجعة المعلومات الرقمية والتحقق منها، ولا سيما عندما يُراد الاستناد إليها في إجراءات قانونية. [77]

ومن الناحية العملية، ينبغي أن ينتهي التحقق المستقل إلى إحدى نتائج متعددة، لا إلى حكم ثنائي مبسط يقرر أن المعلومة صحيحة أو خاطئة في جميع عناصرها. فقد يتبين أن جزءاً من المحتوى صحيح، بينما تبقى نسبة النشر أو تاريخ الواقعة غير محسومين. وقد تكون البيانات متسقة مع فرضية معينة دون أن تكون كافية لاستبعاد الفرضيات البديلة. [78]

وعليه، فإن التحقق المستقل لا يهدف إلى إنتاج يقين مصطنع، وإنما إلى تحديد ما يمكن تأكيده، وما يمكن ترجيحه، وما يظل غير معلوم، والأسباب الفنية أو المنهجية التي تمنع الوصول إلى نتيجة أكثر حسماً. [79]

المطلب الثالث: تحليل بيانات الوقت والموقع وسجلات الأنظمة

تحتل بيانات الوقت والموقع وسجلات الأنظمة أهمية كبيرة في التحريات الأمنية الرقمية، لما توفره من مؤشرات تساعد على إعادة بناء التسلسل الزمني للأحداث، وفهم أنماط استخدام الأجهزة والأنظمة، وربط الوقائع الرقمية بالوقائع المادية. غير أن القيمة الاستدلالية لهذه البيانات تتوقف على فهم طريقة إنتاجها وتسجيلها، والقيود الفنية التي تؤثر في دقتها، وطبيعة العلاقة بينها وبين الحدث المراد إثباته. [80]

ويقصد بالبيانات الوصفية البيانات التي تصف ملفاً أو حدثاً أو عملية رقمية أو توفر معلومات عن خصائصها وسياقها، مثل وقت الإنشاء أو التعديل، وحجم الملف، ونوعه، ومعلومات الموقع، وبعض تفاصيل النظام. وقد تكون مدمجة في الملف نفسه، أو محفوظة في سجل منفصل، أو مستمدة من نظام أو خدمة رقمية. [81]

ولا تتمتع البيانات الوصفية بدرجة واحدة من الموثوقية؛ لأن مصدرها وآلية إنشائها وإمكان تعديلها تختلف من نظام إلى آخر. فبعض التوقيات تسجلها أنظمة آلية عند حدوث عملية معينة، بينما يمكن أن تتأثر توقيات أخرى بإعدادات الجهاز أو بتدخل المستخدم أو بطريقة نسخ الملف ونقله. [82]

أولاً: تحليل بيانات الوقت. يتطلب تحديد المقصود بكل توقيت، وعدم افتراض أن جميع الطوابع الزمنية تشير إلى الحدث نفسه. فقد يكون التوقيت المسجل هو وقت إنشاء الملف، أو آخر تعديل عليه، أو استلامه من نظام آخر، أو تحميله على منصة، أو نسخه إلى وسيط تخزين. ويجب تحديد المنطقة الزمنية المستخدمة، والتحقق من إعداد الساعة ومزامنتها عند توافر البيانات

اللازمة، وتوثيق أي تحويل بين التوقيت المحلي والتوقيت العالمي المنسق. كما ينبغي مراعاة التوقيت الصيفي في الأنظمة التي تطبقه، والفروق الناشئة عن عدم تزامن الساعات.[83]

فإذا ظهر في سجل نظام إلكتروني أن عملية تمت في الساعة العاشرة، بينما أظهر تسجيل آخر وقوع حدث في الساعة التاسعة وخمس وخمسين دقيقة، فلا يصح استنتاج التعارض مباشرة قبل التحقق من مصدر كل توقيت وطريقة تسجيله ودقته. وقد يكون الاختلاف ناتجاً عن فارق بين الساعات أو عن اختلاف الحدث الذي يسجله كل نظام.[84]

كذلك، ينبغي الحذر من التعامل مع تاريخ إنشاء الملف باعتباره تاريخ إنشاء محتواه. فقد يُنشأ الملف في وقت لاحق لتسجيل الواقعة، أو يُنقل إلى جهاز آخر فتتغير بعض بياناته الزمنية، أو يُستخرج من نظام يطبق قواعد مختلفة لحفظ التوقيت.[85]

ثانياً: تحليل بيانات الموقع. تختلف بيانات الموقع بحسب الوسيلة التي أُنتجت من خلالها. فقد تستند إلى نظام تحديد المواقع العالمي، أو إلى تقدير الموقع بواسطة شبكات الاتصالات، أو إلى معلومات يدرجها المستخدم، أو إلى بيانات وصفية مرتبطة بالصورة أو الفيديو. ويجب تحديد مصدر بيانات الموقع وطبيعة القياس المستخدم ومدى دقته، وعدم مساواة الإحداثيات المسجلة بالموقع الحقيقي على نحو مطلق.[86]

ولا يجوز الانتقال من إثبات وجود جهاز في موقع معين إلى إثبات وجود صاحبه في الموقع ذاته دون قرائن إضافية. كما أن وجود جهاز ضمن منطقة جغرافية واسعة لا يثبت وجوده في نقطة محددة داخلها، ما لم تكن دقة البيانات تسمح بذلك. ومن المهم التمييز بين موقع الجهاز وموقع الخادم الذي عالج البيانات وموقع المستخدم الذي نشر المحتوى.[87]

ثالثاً: تحليل سجلات الأنظمة. تتضمن سجلات الأنظمة معلومات عن عمليات الدخول والخروج، والوصول إلى الملفات، والتغييرات التي تطرأ على البيانات، والأحداث التشغيلية. وقد تساعد على تحديد تسلسل العمليات التي حدثت داخل نظام معين، لكنها لا تثبت دائماً هوية الشخص الطبيعي الذي نفذها. فقد يرتبط السجل بحساب مستخدم، إلا أن إثبات أن شخصاً بعينه كان يستخدم الحساب في ذلك الوقت يتطلب فحص عوامل إضافية، مثل آليات المصادقة، وإمكان مشاركة بيانات الدخول، وطبيعة الجهاز المستخدم، واحتمالات الاستخدام غير المصرح به [88].

كما ينبغي تقييم مدى اكتمال السجلات؛ فقد تكون بعض الأحداث غير مسجلة أصلاً، أو تكون مدة الاحتفاظ محدودة، أو تكون أجزاء منها قد حُذفت أو استُبدلت. وقد تختلف تفاصيل التسجيل باختلاف إعدادات النظام وإصداره ومستوى التفصيل الذي كان مفعلاً وقت الواقعة.[89]

وتؤكد إرشادات **NIST** ضرورة تحديد البيانات ذات الصلة والحصول عليها وحمايتها، ثم معالجتها وتحليلها والإبلاغ عن النتائج، مع مراعاة طبيعة مصادر البيانات وحدود استخدامها [90].

ومن الناحية التحليلية، لا ينبغي تفسير السجل الإلكتروني باعتباره وصفاً كاملاً للواقعة، بل بوصفه أثراً رقمياً أنتجه نظام معين وفق قواعد تسجيل محددة. وقد يكون هذا الأثر قوي الدلالة

على حدوث عملية تقنية، لكنه أضعف في الدلالة على هوية من يقف وراءها أو الغرض منها [91].

ولذلك، فإن الاستخدام المنهجي لبيانات الوقت والموقع وسجلات الأنظمة يتطلب بيان ما تثبته هذه البيانات مباشرة، وما يمكن استنتاجه منها على نحو احتمالي، وما يحتاج إلى أدلة إضافية. كما يجب إظهار الفروق بين الدقة التقنية للبيانات وقوتها في تفسير السلوك البشري. [92]

المطلب الرابع: حدود دقة البيانات الوصفية وأثرها في تفسير النتائج

تنسجم البيانات الوصفية بأهمية خاصة في التحريات الرقمية؛ إذ قد توفر مؤشرات عن مصدر الملف أو توقيت إنشائه أو التعديلات التي طرأت عليه. غير أن هذه البيانات ليست سجلاً معصوماً من الخطأ، ولا تمثل في جميع الحالات وصفاً كاملاً أو مباشراً للواقعة. [93]

أولاً: محدودية الدلالة على المصدر الأصلي. قد تتضمن البيانات الوصفية اسم جهاز أو برنامج أو حساب، لكنها لا تثبت بالضرورة أن هذا الجهاز أو الحساب هو المصدر الأول للمحتوى. فقد يكون الملف قد نُقل أو نُسخ أو أُعيد تصديره أو عولج بواسطة برنامج آخر. كما أن وجود اسم مستخدم داخل بيانات الملف لا يثبت وحده أن هذا المستخدم هو من أنشأ المحتوى. [94]

ثانياً: محدودية الدلالة الزمنية. قد تتأثر التوقيات المسجلة بإعدادات الساعة أو المنطقة الزمنية أو طريقة النقل بين الأنظمة، كما قد تختلف دلالتها بحسب ما إذا كانت تشير إلى الإنشاء أو التعديل أو الاستلام أو النسخ. ويترتب على ذلك أن البيانات الزمنية لا ينبغي أن تُفسر بمعزل عن طبيعة النظام الذي أنشأها. [95]

ثالثاً: محدودية الدلالة المكانية. قد تكون بيانات الموقع تقريبية أو غير مكتملة، وقد تتعلق بالجهاز لا بالمستخدم، أو بوقت مختلف عن وقت الحدث. كما أن غياب بيانات الموقع لا يعني بالضرورة أن الملف لم يُنشأ في مكان معين؛ فقد تكون غير مدعومة أصلاً أو أزيلت أثناء المعالجة. [96]

رابعاً: احتمالات التعديل أو الفقد. قد تتغير البيانات الوصفية نتيجة عمليات مشروعة، مثل ضغط الصور أو تحويل صيغتها أو إرسالها عبر منصة رقمية، كما قد تتغير نتيجة تدخل متعمد. ولذلك، لا يجوز تفسير التغير في البيانات الوصفية باعتباره دليلاً على التلاعب دون فحص طبيعة العملية. [97]

وفي المقابل، لا يعني بقاء البيانات الوصفية دون تغيير ظاهر أن المحتوى نفسه أصلي أو صحيح؛ إذ يمكن أن يُعدل المحتوى مع الاحتفاظ ببعض البيانات المصاحبة أو إعادة إنشائها [98].

خامساً: محدودية الاستنتاج من غياب البيانات. إن عدم وجود سجل أو حقل وصفي لا يثبت بالضرورة عدم وقوع الحدث الذي كان يمكن أن يسجله. فقد يرجع الغياب إلى عدم تفعيل التسجيل، أو انتهاء مدة الاحتفاظ، أو اختلاف إعدادات النظام، أو فشل عملية الجمع، أو حذف البيانات. [99]

وتكشف هذه الحدود عن ضرورة التمييز بين دقة البيانات واكتمالها وأصالتها ودالاتها. فالدقة تتعلق بمدى مطابقة القيمة المسجلة لما يفترض أن تقيسه، والاكتمال يتعلق بمدى احتواء السجل على العناصر اللازمة، والأصالة تتصل بمصدر البيانات وسلامة نسبتها، أما الدلالة فتتعلق بمدى صلاحية البيانات لتأييد استنتاج معين. [100]

ولا يلزم من تحقق أحد هذه العناصر تحقق العناصر الأخرى؛ فقد تكون البيانات أصلية لكنها غير مكتملة، أو مكتملة لكنها غير دقيقة، أو دقيقة من الناحية التقنية لكنها محدودة الدلالة على الواقعة. [101]

ويقتضي التقييم المهني تجنب المبالغة في وصف نتائج الفحص. فإذا لم تكشف الأداة المستخدمة عن علامات تعديل، فإن النتيجة الدقيقة هي أن الفحص لم يكشف عن تلك العلامات في حدود قدرات الأداة والمنهج المستخدم، لا أن الملف يستحيل أن يكون قد عُدل. كما أن إثبات تطابق قيم التجزئة الرقمية لنسختين يدل على تطابق محتواهما الرقمي وفق الخوارزمية المستخدمة، لكنه لا يثبت بمفرده صحة المحتوى أو مشروعية الحصول عليه. [102]

وتؤكد الأدلة الفنية في مجال الأدلة الجنائية الرقمية ضرورة مراعاة نطاق الفحص والوسائل المستخدمة والقيود المرتبطة بها، وعدم تحويل النتائج التقنية إلى استنتاجات تتجاوز ما تثبته الإجراءات المنفذة. [103]

وبناءً على ذلك، ينبغي أن يتضمن التقرير التحليلي وصفاً واضحاً للبيانات الوصفية التي جرى فحصها، ومصدرها، وطريقة استخراجها، ومدى اكتمالها، والقيود التي تؤثر في تفسيرها، مع بيان ما إذا كانت النتيجة مباشرة أو مستنتجة أو احتمالية. [104]

المبحث الثالث: اختبار الفرضيات وضبط الاستدلال

المطلب الأول: التمييز بين الفرضية والنتيجة

تؤدي الفرضيات دوراً أساسياً في توجيه التحليل الأمني الرقمي، لكنها لا تكتسب قوة إثباتية بمجرد صياغتها أو توافقها الأولي مع بعض المعلومات. ولذلك، يتعين الفصل بين الفرضية بوصفها تفسيراً محتملاً يراد اختباره، والنتيجة بوصفها تقديراً تحليلياً يُبنى على فحص الأدلة والمعلومات المتاحة. [105]

فالفرضية تحدد احتمالاً بشأن الواقعة أو تفسيراً للعلاقات بين البيانات، بينما تعبر النتيجة عن مدى ما تسمح به المعطيات من تأييد هذا الاحتمال أو إضعافه. ولا يعني ذلك أن النتيجة التحليلية تصبح يقيناً مطلقاً؛ فقد تكون النتيجة ترجيحاً محدوداً أو استنتاجاً مشروطاً أو تقريراً بعدم كفاية المعلومات للفصل بين التفسيرات. [106]

ثلاثة مستويات يجب التمييز بينها:

١. **الفرضية الأولية:** تفسير مقترح في بداية التحليل، يُستخدم لتحديد المعلومات التي ينبغي البحث عنها. [107]

٢. **النتيجة التحليلية:** التقدير الذي يتم التوصل إليه بعد تقييم البيانات ومقارنتها واختبار الفرضيات البديلة. [108]

٣. **النتيجة القانونية أو القضائية:** ما تقرره الجهة المختصة وفق القواعد القانونية والإجرائية ومعياري الإثبات المنطبق. [109]

ولا يجوز الخلط بين هذه المستويات؛ لأن التحليل الأمني قد ينتهي إلى ترجيح وجود علاقة بين شخص وواقعة، دون أن يثبت توافر عناصر المسؤولية الجنائية. كما قد تكون المعلومة كافية لتوجيه إجراء تحريٍّ إضافي، لكنها غير كافية للاستناد إليها بوصفها دليلاً على ارتكاب فعل مجرم. [110]

ويتطلب الانتقال من الفرضية إلى النتيجة تحديد الأساس الذي تستند إليه كل خطوة استدلالية. فإذا كانت الفرضية تفترض أن حساباً إلكترونياً يعود إلى شخص معين، وجب فحص الأدلة التي تسند هذه النسبة قبل استخدام منشورات الحساب لإثبات سلوك ذلك الشخص. وإلا، فإن التحليل سيقوم على مقدمة غير متحققة. [111]

كما ينبغي ألا تُصاغ النتيجة بطريقة تتجاوز نطاق السؤال الذي عالجه البيانات. فإذا أثبت سجل تقني أن حساباً معيناً أجرى عملية دخول، فلا يصح الجزم بهوية الشخص الطبيعي الذي نفذها دون معلومات إضافية. وإذا أظهر تحليل الموقع أن جهازاً كان ضمن نطاق جغرافي معين، فلا يصح تحويل هذه النتيجة إلى إثبات قاطع لوجود صاحبه في النقطة نفسها. [112]

ويقتضي ضبط الاستدلال تحديد درجة الثقة في النتيجة وأسبابها. ويمكن التعبير عن ذلك بصياغات تميز بين ما تدعمه الأدلة بقوة، وما ترجحه على نحو محدود، وما يبقى غير محسوم.

ولا ينبغي استخدام أوصاف كمية لدرجة الثقة إلا إذا كان لها أساس منهجي واضح، حتى لا تتحول الأرقام إلى مظهر زائف للدقة. [113]

ومن المهم الاعتراف بأن عدم كفاية البيانات لا يمثل بالضرورة فشلاً في التحليل. فقد تكون النتيجة الأكثر دقة هي تعذر التمييز بين فرضيتين بسبب نقص السجلات أو عدم استقلال المصادر أو محدودية دقة البيانات. ويكون الإفصاح عن هذا القصور أكثر قيمة علمية من اختيار تفسير حاسم لا تدعمه المعطيات. [114]

وعليه، فإن جودة النتيجة التحليلية تقاس بمدى تناسبها مع الأدلة المتاحة، ووضوح الافتراضات التي تستند إليها، وإمكان مراجعة مسار الاستدلال، لا بمدى حسمها أو توافقها مع التوقعات الأولية. [115]

المطلب الثاني: اختبار التفسيرات البديلة وتجنب الانتقاء التأكيدي

يقوم التحليل الأمني المنضبط على اختبار التفسيرات الممكنة للوقائع، لا على البحث عن المعلومات التي تؤيد تفسيراً واحداً فقط. ويُعد الانتقاء التأكيدي من أبرز المخاطر التي تهدد موثوقية التحليل، ويقصد به الميل إلى التركيز على المعلومات المتوافقة مع الاعتقاد الأولي، وإهمال المعلومات المخالفة أو التقليل من شأنها دون مسوغ موضوعي. [116]

وقد يظهر هذا التحيز في صور متعددة؛ منها اختيار مصادر معينة دون غيرها، أو تفسير البيانات الغامضة بما يوافق فرضية سابقة، أو اعتبار المعلومات المؤيدة دليلاً حاسماً، في حين تُوصف المعلومات المعارضة بأنها غير مهمة دون إخضاعها للمعيار نفسه. [117]

وتزداد خطورة الانتقاء التأكيدي في البيئة الرقمية بسبب وفرة البيانات وسهولة البحث فيها؛ إذ يمكن للمحلل العثور على معلومات تدعم فرضية معينة بمجرد توسيع نطاق البحث، حتى لو كانت تلك المعلومات متكررة أو غير مستقلة أو محدودة الدلالة. [118]

ويُعالج هذا الخطر من خلال اعتماد منهج واضح لاختبار الفرضيات، يقوم على تحديد التفسيرات البديلة قبل الانتهاء من التحليل، والبحث عن البيانات التي يمكن أن تميز بينها، ومقارنة الأدلة المؤيدة والمعارضة وفق معايير واحدة. [119]

فإذا أشارت مجموعة من السجلات إلى ارتباط جهاز معين بواقعة، ينبغي النظر في تفسيرات بديلة، مثل مشاركة الجهاز بين أكثر من مستخدم، أو استخدام الحساب من موقع آخر، أو وجود خلل في التوقيت، أو ارتباط السجلات بحدث مختلف. ولا يعني طرح هذه الاحتمالات التسليم بصحتها، وإنما التأكد من أن الاستنتاج النهائي لم يُبنَ على تجاهلها. [120]

ويجب أن تكون التفسيرات البديلة معقولة ومتصلة بالوقائع، لا مجرد احتمالات نظرية بعيدة. فالغرض من اختبار البدائل ليس تعطيل الوصول إلى النتائج، وإنما تحديد ما إذا كانت الأدلة المتاحة تميز بالفعل بين التفسيرات الممكنة. [121]

إجراءات تعزيز موضوعية التحليل:

- تحديد الفرضية الأساسية والفرضيات البديلة بصورة صريحة. [122]

- تسجيل الأدلة المؤيدة والمعارضة لكل فرضية. [123]
 - التحقق من استقلال المصادر وعدم عدّ المعلومات المنقولة تأييداً مستقلاً. [124]
 - فصل الوقائع المؤكدة عن التقديرات الشخصية. [125]
 - إجراء مراجعة مستقلة للاستنتاجات المهمة متى أمكن. [126]
 - توثيق أسباب استبعاد الفرضيات البديلة. [127]
 - تعديل النتيجة عند ظهور معلومات جديدة، بدل التمسك بالتفسير السابق. [128]
- وتنبع أهمية المراجعة المستقلة من أنها تتيح فحص التحليل من منظور مختلف، وقد تكشف افتراضات ضمنية لم ينتبه إليها المحلل الأصلي. ومع ذلك، لا تكفي المراجعة وحدها لضمان الموضوعية إذا كان المراجع يعتمد على المواد المنتقاة ذاتها أو يخضع للضغوط المؤسسية نفسها؛ ولذلك يجب أن تتاح له إمكانية فحص المصادر والبيانات ذات الصلة. [129]
- كما ينبغي عدم الخلط بين اختبار الفرضيات والبحث عن دليل ينفيها بصورة مطلقة. فقد لا يكون من الممكن إثبات استحالة تفسير بديل، لكن يمكن تقييم مدى توافقه مع المعطيات ومقارنته بالتفسيرات الأخرى. وتكون النتيجة العلمية السليمة هي تحديد التفسير الأكثر اتساقاً مع الأدلة، مع الإفصاح عن أوجه الضعف والاحتمالات التي لم تحسمها المعلومات. [130]
- ويقتضي ذلك عدم التعامل مع غياب الدليل المؤيد لفرضية معينة بوصفه دليلاً قاطعاً على بطلانها، إلا إذا كانت الظروف تسمح بتوقع ظهور ذلك الدليل لو كانت الفرضية صحيحة. فعدم وجود سجل، مثلاً، لا ينفي وقوع عملية إذا كان النظام لا يسجل جميع العمليات أو إذا كانت السجلات غير مكتملة. [131]
- ويؤدي تطبيق هذه الضوابط إلى جعل التحليل عملية قابلة للتصحيح والمراجعة، بدل أن يكون مساراً أحادي الاتجاه ينتهي إلى تثبيت الاشتباه الأولي. وتكمن القيمة العلمية لهذا النهج في أنه يجعل قوة النتيجة انعكاساً لجودة الأدلة، لا لقوة الاعتقاد الذي بدأ منه التحليل. [132]

المطلب الثالث: معالجة التعارض بين المصادر ونقص البيانات

قد تتعارض المعلومات الرقمية المستمدة من مصادر مختلفة، أو تتضمن بعض المصادر بيانات ناقصة لا تسمح بتكوين صورة مكتملة عن الواقعة. ولا يمثل هذا التعارض بالضرورة دليلاً على عدم صحة جميع المصادر، كما لا يجوز حسمه تلقائياً لمصلحة المصدر الذي يبدو أكثر رسمية أو الذي يتوافق مع الفرضية الأولية. [133]

ويقتضي التعامل العلمي مع التعارض تحديد طبيعته وأسبابه المحتملة، والتمييز بين التعارض الحقيقي والتعارض الظاهري الناشئ عن اختلاف التوقيت أو المصطلحات أو نطاق التسجيل أو طريقة إنتاج البيانات. فقد يختلف توقيتان لأن أحدهما يسجل بدء العملية والآخر يسجل اكتمالها،

أو لأن أحد النظامين يستخدم توقيتاً مختلفاً، أو لأن البيانات المعروضة في أحد المصدرين تمثل نسخة محدثة من سجل سابق. [134]

خطوات منهجية لمعالجة التعارض:

- تحديد موضع التعارض بدقة، وعدم وصف المصدر كله بأنه متناقض بسبب اختلاف جزئي. [135]
- فحص أصل كل معلومة وتاريخ الحصول عليها وطريقة إنتاجها. [136]
- التحقق من اختلاف التعريفات أو التوقيتات أو نطاقات التسجيل. [137]
- تقييم سلامة البيانات واكتمالها واحتمالات تعديلها. [138]
- البحث عن مصدر مستقل يساعد على تفسير التعارض. [139]
- تحديد ما إذا كان التعارض قابلاً للحسم أو سيظل قائماً. [140]
- بيان أثر التعارض في النتيجة النهائية، وعدم إخفائه لمجرد أنه يضعف الاستنتاج [141].

ويجب التمييز بين نقص البيانات والتعارض بينها. فنقص البيانات يعني عدم توافر المعلومات اللازمة لتفسير واقعة أو اختبار فرضية، بينما يعني التعارض وجود معلومات متاحة تتباين في دلالتها. وقد يجتمع الأمران عندما تكون المصادر المتاحة متعارضة، بينما تغيب البيانات اللازمة لحسم الاختلاف. [142]

ويُعد نقص البيانات من القيود المهمة في التحليل الرقمي؛ لأن عدم اكتمال السجلات أو فقدان جزء من المحتوى قد يمنع إعادة بناء التسلسل الزمني أو تحديد مصدر المعلومة أو التحقق من سياقها. كما أن غياب البيانات قد يؤثر في الفرضيات المختلفة بدرجات متفاوتة. [143]

ومن المهم عدم ملء الفجوات المعلوماتية بافتراضات غير معلنة. فإذا غاب سجل يوضح هوية المستخدم، فلا يجوز افتراض أن صاحب الحساب هو من نفذ العملية لمجرد أن الحساب مسجل باسمه. وإذا كانت صورة لا تتضمن بيانات مكانية موثوقة، فلا ينبغي تحديد موقعها استناداً إلى انطباع بصري وحده. [144]

وفي المقابل، لا ينبغي المبالغة في أثر النقص إلى درجة إهدار جميع المعلومات المتاحة؛ فقد تسمح البيانات الجزئية باستنتاج محدود أو بتحديد مسار بحث إضافي. والمطلوب هو بيان حدود الاستخدام الممكن لكل معلومة، لا استبعادها آلياً أو تحميلها أكثر مما تحتل. [145]

وتؤكد الأدلة المهنية في التحليل الاستخباري ضرورة تقييم المعلومات من حيث الدقة والملاءمة والموثوقية، والبحث عن العلاقات بين السجلات، مع مراعاة المخاطر التي قد تنشأ عن استخدام المعلومات غير المكتملة أو غير الدقيقة. [146]

ويجب أن ينعكس التعارض أو النقص في صياغة التقرير النهائي. فإذا تعذر حسم الاختلاف، ينبغي وصفه صراحة وبيان الفرضيات التي لا يزال يدعمها أو يضعفها، وما إذا كانت هناك إجراءات إضافية يمكن أن تساعد على التحقق. ولا يصح تقديم نتيجة قطعية بينما تستند إلى مصادر متعارضة لم تُعالج أوجه الاختلاف بينها. [147]

المطلب الرابع: التحقق من احتمالات التلاعب والتزوير

تشير قابلية البيانات الرقمية للنسخ والتعديل وإعادة النشر تحديات جدية أمام التحريات الأمنية؛ إذ يمكن تغيير محتوى الملفات أو بياناتها الوصفية، أو دمج أجزاء من مواد مختلفة، أو نشر محتوى صحيح في سياق مضلل، أو إنشاء محتوى اصطناعي يبدو واقعياً. ولذلك، يتعين التمييز بين التحقق من سلامة البيانات الرقمية والكشف عن التلاعب المحتمل بمضمونها أو سياقها [148].

ويقصد بالتلاعب الرقمي إجراء تغيير في البيانات أو المحتوى أو السياق بما قد يؤثر في تفسيره. أما التزوير، فتتوقف دلالاته القانونية على طبيعة الفعل والقواعد القانونية المنطبقة، ولا يجوز اعتبار كل تعديل تقني تزويراً؛ فقد تكون المعالجة مشروعة وضرورية لأغراض العرض أو التحليل، شريطة توثيقها وعدم تقديم النسخة المعالجة باعتبارها أصلاً غير معدل. [149]

وتختلف صور التلاعب بحسب نوع البيانات، فقد تشمل تعديل الصور أو مقاطع الفيديو، أو تغيير بيانات الوقت والموقع، أو حذف أجزاء من السجلات، أو تركيب محتوى من مصادر مختلفة، أو استخدام تقنيات التوليد الاصطناعي لإنتاج مواد لم تقع أحداثها. [150]

كما ينبغي التمييز بين التعديل في المحتوى والتلاعب في السياق. فقد تكون الصورة أصلية ولم يطرأ عليها تغيير تقني، لكنها تُنشر على أنها التُقطت في مكان أو وقت مختلفين. وفي هذه الحالة، قد يكون الملف سليماً من حيث بنيته، بينما تكون الرواية المصاحبة له مضللة. [151]

منهج متعدد المستويات للتحقق من التلاعب:

أولاً: فحص المصدر وسياق النشر. يبدأ التحقق بتحديد مصدر المحتوى وأقدم ظهور يمكن الوصول إليه، وفحص الحساب أو الجهة التي نشرته، ومقارنة الرواية المصاحبة له بالمعلومات المستقلة. ولا ينبغي افتراض أن الحساب الذي نشر المحتوى أولاً ضمن المصادر المتاحة هو منشئه الأصلي بالضرورة. [152]

ثانياً: فحص الخصائص الفنية. يشمل تحليل البيانات الوصفية وبنية الملف ومكوناته، ومقارنة النسخ المتاحة، وفحص التناسق بين العناصر البصرية أو الصوتية، والبحث عن مؤشرات قد تدل على التعديل أو إعادة الترميز أو الدمج. وتختلف صلاحية هذه الاختبارات بحسب نوع الملف والأدوات المستخدمة. [153]

ثالثاً: المقارنة بالمصادر المستقلة. قد يساعد العثور على تسجيلات أو صور أو بيانات أخرى للواقعة نفسها على التحقق من السياق أو كشف التناقضات. غير أن المقارنة يجب أن تراعي استقلال المصادر، وألا تُعامل إعادة نشر المادة ذاتها على أنها تأكيد مستقل. [154]

رابعاً: اختبار الفرضيات البديلة. لا ينبغي تفسير كل اختلاف في الملف بوصفه دليلاً على التلاعب المتعمد. فقد ينتج الاختلاف عن الضغط أو تحويل الصيغة أو اقتصاص الصورة أو اختلاف ظروف التصوير. ولذلك، يجب فحص التفسيرات التقنية المشروعة قبل نسبة التغيير إلى فعل متعمد. [155]

خامساً: بيان حدود الفحص. ينبغي توضيح الأدوات المستخدمة، والاختبارات التي أُجريت، والنتائج التي أسفرت عنها، والقيود التي قد تمنع اكتشاف بعض أنواع التعديل. ولا يصح الادعاء بأن المحتوى أصلي بصورة مطلقة لمجرد عدم العثور على مؤشرات واضحة للتلاعب. [156]

وتزداد هذه المسألة تعقيداً مع انتشار تقنيات الذكاء الاصطناعي التوليدي، التي يمكن أن تنتج صوراً أو أصواتاً أو مقاطع فيديو مقنعة بصرياً أو سمعياً. وقد تظهر بعض المؤشرات الفنية على التوليد أو التعديل، إلا أن هذه المؤشرات لا تكون حاسمة في جميع الحالات، كما أن الأدوات المستخدمة في الكشف قد تعطي نتائج إيجابية أو سلبية خاطئة. [157]

ولذلك، لا يجوز الاعتماد على نتيجة أداة واحدة لإثبات أن المحتوى مولد اصطناعياً أو أصلي بالكامل، بل ينبغي جمع مؤشرات متعددة وتقييمها في سياقها، مع مراعاة أن بعض الأدوات تتراجع فعاليتها عند تغير تقنيات التوليد أو المعالجة. [158]

كما يجب الحذر من استخدام غياب العلامات التقنية الدالة على التوليد الاصطناعي دليلاً قاطعاً على أن المحتوى حقيقي. فقد لا يتضمن المحتوى أصلاً بيانات تعريفية عن طريقة إنشائه، أو قد تُزال هذه البيانات أثناء النشر أو المعالجة. [159]

ومن جهة أخرى، لا يعني اكتشاف أن جزءاً من المحتوى قد عُدل أن جميع المعلومات الواردة فيه كاذبة؛ إذ ينبغي تحديد طبيعة التعديل ومداه وأثره في العناصر التي يراد الاستناد إليها. فقد يكون التعديل محدوداً ولا يؤثر في الواقعة محل التحري، وقد يكون جوهرياً بحيث يغير دلالة المحتوى بالكامل. [160]

ويقتضي ذلك أن يركز التقرير الفني على وصف ما تم التحقق منه، بدل الانتقال مباشرة إلى أحكام قانونية بشأن القصد أو المسؤولية. فإثبات وجود تغيير تقني لا يكفي وحده لإثبات أن التغيير أُجري بقصد التضليل، كما أن تحديد القصد يتطلب عناصر إضافية تتجاوز الفحص الفني للملف. [161]

وبناءً عليه، فإن التحقق من احتمالات التلاعب والتزوير يجب أن يقوم على الجمع بين الفحص الفني، والتحقق من المصدر والسياق، والمقارنة المستقلة، واختبار التفسيرات البديلة. ولا تتحقق موثوقية النتيجة بمجرد اكتشاف مؤشرات للتعديل أو عدم اكتشافها، بل ببيان حدود الاختبارات ومدى اتصالها بالمسألة محل التحري. [162]

المطلب الخامس: الإفصاح عن مواطن الشك وعدم اليقين

لا تقتصر سلامة التحليل الأمني الرقمي على صحة المعلومات المستخدمة أو ملاءمة المنهج المتبع، بل تتطلب كذلك الإفصاح عن مواطن الشك وعدم اليقين التي قد تؤثر في تفسير النتائج.

فالمعلومات الرقمية، مهما بلغت جودتها، لا تتيح دائماً الوصول إلى نتيجة حاسمة، وقد تظل بعض عناصر الواقعة غير معروفة بسبب نقص البيانات أو محدودية الوسائل الفنية أو تعارض المصادر. [163]

ويقصد بـ **عدم اليقين** وجود حدود في المعرفة المتاحة تمنع الجزم بصحة تفسير معين أو تمنع تحديد مدى دقته بصورة قاطعة. وقد يرجع ذلك إلى غموض المصدر، أو نقص السجلات، أو عدم إمكان إعادة فحص المادة الأصلية، أو تعدد التفسيرات الممكنة، أو محدودية دقة الأداة المستخدمة. [164]

ويجب التمييز بين عدم اليقين والخطأ. فالخطأ يتعلق بوجود نتيجة غير صحيحة أو إجراء معيب، أما عدم اليقين فقد يبقى قائماً حتى عند اتباع منهج سليم، لأن البيانات المتاحة لا تسمح بحسم المسألة. وقد يكتشف التحليل أن المعلومات لا تكفي للتمييز بين فرضيتين، دون أن يعني ذلك أن التحليل نفسه قد أخفق. [165]

كما ينبغي التمييز بين عدم اليقين المتعلق بالمصدر، وعدم اليقين المتعلق بالمحتوى، وعدم اليقين المتعلق بالتفسير. فقد يكون المصدر معروفاً، لكن مضمون المعلومة غير مكتمل؛ وقد يكون المحتوى واضحاً، لكن نسبته إلى شخص معين غير مؤكدة؛ وقد تكون البيانات أصلية وسليمة، لكن دلالتها على الواقعة محدودة. [166]

ويقتضي الإفصاح العلمي عن عدم اليقين تحديد موضعه وأسبابه وأثره في النتيجة. فلا يكفي استخدام عبارة عامة مثل "توجد بعض التحفظات"، بل يجب بيان ما إذا كانت التحفظات تتعلق بمصدر البيانات أو توقيتها أو دقتها أو اكتمالها أو طريقة تحليلها. [167]

عناصر التقرير بشأن عدم اليقين:

- بيان الوقائع التي أمكن التحقق منها بصورة مباشرة. [168]
- تحديد المعلومات التي لم يكتمل التحقق من مصدرها أو مضمونها. [169]
- شرح الافتراضات التي يتوقف عليها الاستنتاج. [170]
- توضيح التفسيرات البديلة التي لم يمكن استبعادها. [171]
- بيان أثر نقص البيانات أو تعارض المصادر في النتيجة. [172]
- وصف حدود الأدوات الفنية والاختبارات المستخدمة. [173]
- تحديد المعلومات الإضافية التي قد تساعد على تقليل عدم اليقين. [174]
- صياغة النتيجة بدرجة من التحفظ تتناسب مع قوة الأدلة. [175]

ولا يعني الإفصاح عن الشك إضعاف التقرير أو التقليل من قيمته المهنية؛ بل يزيد من إمكان الاعتماد عليه، لأنه يمنع القارئ من نسبة قوة إلى النتيجة لا تدعمها الأدلة. كما يسمح للجهات

المختصة بتقدير ما إذا كانت المعلومات كافية لاتخاذ قرار أممي معين، أو إذا كانت هناك حاجة إلى استكمال التحري أو إجراء فحص إضافي. [176]

ويجب التمييز بين درجة الثقة التحليلية ومعياري الإثبات القانوني. فقد يعبر المحلل عن ترجيح تفسير معين في ضوء المعلومات المتاحة، لكن هذا الترجيح لا يساوي تلقائياً استيفاء معيار الإثبات المطلوب أمام القضاء. فكل منهما وظيفة مختلفة. [177]

كما ينبغي عدم استخدام نسب مئوية لدرجة الثقة ما لم يكن لها أساس منهجي قابل للتفسير. فإسناد نسبة مثل تسعين في المائة إلى استنتاج لا يستند إلى نموذج احتمالي موثوق أو بيانات تسمح بهذا التقدير قد يمنح النتيجة مظهراً كمياً مضللاً. وفي كثير من الحالات، تكون الصياغة الوصفية المنضبطة أكثر دقة من الأرقام التي لا يمكن تبريرها. [178]

ومن جهة أخرى، يجب الإفصاح عن مواطن الشك التي ظهرت أثناء التحليل حتى لو كانت لا تتفق مع التوجه العام للتقرير. فإغفال المعلومات المخالفة أو إخفاء القيود الفنية قد يؤدي إلى تكوين صورة غير متوازنة عن الأدلة، ويمنع المراجعة المستقلة من تقييم النتيجة على أساس كامل. [179]

وتتصل هذه المسألة بمبدأ **قابلية إعادة التحقق**؛ إذ لا يستطيع المراجع تقييم مدى قوة الاستنتاج إذا لم يعرف البيانات التي استند إليها المحلل، والخطوات التي اتبعتها، والقيود التي واجهته. ومن ثم، فإن الإفصاح عن عدم اليقين يجب أن يقتصر بتوثيق كافٍ لمصادر المعلومات ومنهج التحليل وأسباب الاستنتاج. [180]

وفي ضوء ذلك، فإن المعيار العلمي للتحليل الأمني الرقمي ليس الوصول إلى نتيجة حاسمة في كل الأحوال، وإنما تقديم أفضل تفسير تسمح به المعلومات المتاحة، مع المحافظة على الفصل بين ما ثبت، وما ترجح، وما بقي محتملاً أو مجهولاً. ويُعد الاعتراف بالمنهج بحدود المعرفة شرطاً للموضوعية، وضمانة تحول دون تحويل الاشتباه إلى يقين مصطنع. [181]

الجدول المقارن: مستويات التحليل ودرجة الثقة والإفصاح

المستوى	مثال	طبيعته	درجة الثقة	ما يجب الإفصاح عنه
الملاحظة	ظهور شخص في تسجيل	وصف مباشر	عالية (في حدود المادة)	ظروف التسجيل، جودة الصورة، حدود الدقة
الواقعة	وجود شخص في موقع	حدث مدعوم بأدلة	متوسطة إلى عالية	الأدلة الداعمة، مصادرهما، استقلالها
المعلومات التحليلية	تزامن بين اتصال وحدث	ربط بين بيانات	متوسطة	افتراضات الربط، دقة التوقيت، البدائل
الاستنتاج	ارتباط شخص بواقعة	تفسير تحليلي	منخفضة إلى متوسطة	الافتراضات، الفرضيات البديلة، القيود
النتيجة القانونية	ثبوت المسؤولية	تقرير قضائي	حسب معيار الإثبات	لا تدخل في نطاق التقرير الأمني

❖ النافذة التطبيقية

السيناريو: واقعة اختلاس مالي، تتوافر فيها سجلات دخول إلكتروني، وتسجيلات كاميرا، وبيانات موقع هاتف أحد الموظفين.

- **الخطوة الأولى (التنظيم):** تصنيف البيانات: سجلات النظام (آلية، موثوقية متوسطة)، تسجيلات الكاميرا (بصرية، تحتاج تحققاً)، بيانات الموقع (تقنية، تحتاج تقييم دقة). توثيق مصدر كل مادة وتاريخ الحصول.
- **الخطوة الثانية (الربط الزمني):** مقارنة توقيت سجل الدخول مع توقيت الكاميرا. التحقق من المنطقة الزمنية وإعدادات الساعات قبل استنتاج التعارض.
- **الخطوة الثالثة (التمييز بين المستويات):** الملاحظة: ظهور موظف في الكاميرا. الواقعة: دخوله النظام. الاستنتاج: قيامه بالاختلاس (يحتاج أدلة إضافية على الصلاحية والنية).
- **الخطوة الرابعة (الفرضيات):** فرضية (أ): الموظف نفذ العملية. فرضية (ب): شخص آخر استخدم حسابه. فرضية (ج): خطأ في التوقيت. البحث عن أدلة تميز بينها (سجلات المصادقة، بصمة الجهاز).
- **الخطوة الخامسة (التقييم):** التحقق المستقل: هل توجد سجلات خادم مستقلة؟ هل بيانات الموقع دقيقة؟ هل توجد تفسيرات بديلة لوجود الهاتف في الموقع؟
- **الخطوة السادسة (الإفصاح):** بيان ما لم يتحقق: مثلاً، "لم يتسن التحقق من هوية مستخدم الحساب في تلك اللحظة"، "دقة بيانات الموقع تقدر بنطاق ٥٠٠ متر".
- **الدرس:** التحليل ليس انتقالاً خطياً من البيانات إلى النتيجة، بل عملية متعددة المستويات، والاعتراف بالقيود جزء من النتيجة.

النتائج العامة للفصل

١. تنظيم البيانات وتصنيفها ليس إجراءً تقنياً محايداً، بل يتضمن اختيارات منهجية تؤثر في النتائج.
٢. التمييز بين المستويات الخمسة (الأصلية، المستخرجة، المنظمة، المعلومات، الاستنتاجات) ضروري لقابلية المراجعة.
٣. الربط بين المصادر يتطلب التحقق من استقلالها الفعلي، لا مجرد تعددها الظاهري.
٤. التمييز بين الملاحظة والواقعة والاستنتاج ضمانة لمنع تحويل الاحتمالات إلى حقائق.
٥. الفرضية أداة توجيه، لا نتيجة إثباتية؛ ويجب اختبارها بموضوعية.
٦. تقييم المصدر منفصل عن تقييم المعلومة؛ وسمعة المصدر لا تغني عن فحص المحتوى.

٧. التحقق المستقل يتطلب مصادر مستقلة فعلاً، لا نسخاً متعددة من أصل واحد.
٨. بيانات الوقت والموقع والسجلات تحتاج فهماً فنياً لطريقة إنتاجها قبل تفسيرها.
٩. البيانات الوصفية محدودة الدلالة، ولا تثبت وحدها المصدر أو الوقت أو المكان.
١٠. الانتقاء التأكيدى خطر يهدد الموضوعية، ويُعالج باختبار البدائل والمراجعة المستقلة.
١١. التعارض بين المصادر قد يكون ظاهرياً، ويحتاج تحليلاً منهجياً قبل الحسم.
١٢. نقص البيانات لا يعني فشل التحليل، لكنه يستلزم الإفصاح عن أثره.
١٣. التلاعب والتزوير يحتاجان منهجاً متعدد المستويات، ولا يكفي فحص فني واحد.
١٤. الإفصاح عن عدم اليقين شرط للموضوعية، وليس ضعفاً في التقرير.
١٥. الفصل بين درجة الثقة التحليلية ومعايير الإثبات القانوني ضروري لتجنب الخلط بين الوظائف.

المراجع:

- (1) Kent et al., *Guide to Integrating Forensic Techniques into Incident Response*, NIST SP 800-86, 2006, at 3-1
- (2) هشام مصطفى محمد، *التحريات الأمنية وأثرها في الأدلة الجنائية*، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٥، ص ١٨٠-١٨٥
- (3) NIST SP 800-86, *supra* note 1, at 4-1
- (4) NIST SP 800-86, *supra* note 1, at 4-2
- (5) NIST SP 800-86, *supra* note 1, at 4-3
- (6) NIST SP 800-86, *supra* note 1, at 1-1
- (7) NIST SP 800-86, *supra* note 1, at 4-4
- (8) College of Policing, *Intelligence Cycle*, Authorised Professional Practice.
- (9) Berkeley Protocol on Digital Open Source Investigations, 2022, at 30-35
- (10) Berkeley Protocol, *supra* note 9, at 35-40
- (11) NIST SP 800-86, *supra* note 1, at 3-2
- (12) Berkeley Protocol, *supra* note 9, at 40-45
- (13) Berkeley Protocol, *supra* note 9, at 45-50
- (14) Berkeley Protocol, *supra* note 9, at 50-55
- (15) Berkeley Protocol, *supra* note 9, at 55-60
- (16) Berkeley Protocol, *supra* note 9, at 60-65
- (17) Berkeley Protocol, *supra* note 9, at 65-70
- (18) NIST SP 800-86, *supra* note 1, at 4-5
- (19) Berkeley Protocol, *supra* note 9, at 70-75
- (20) Berkeley Protocol, *supra* note 9, at 75-80
- (21) College of Policing, *Intelligence Strategy*.
- (22) Berkeley Protocol, *supra* note 9, at 80-85
- (23) Berkeley Protocol, *supra* note 9, at 85-90
- (24) Berkeley Protocol, *supra* note 9, at 90-95
- (25) Berkeley Protocol, *supra* note 9, at 95-100

- (26) Berkeley Protocol, *supra* note 9, at 100-105
- (27) Berkeley Protocol, *supra* note 9, at 105-110
- (28) Berkeley Protocol, *supra* note 9, at 110-115
- (29) College of Policing, *Evaluation*.
- (30) Berkeley Protocol, *supra* note 9, at 115-120
- (31) College of Policing, *Evaluation*.
- (32) Berkeley Protocol, *supra* note 9, at 120-125
- (33) Berkeley Protocol, *supra* note 9, at 125-130
- (34) College of Policing, *Evaluation*, *supra* note 29
- (35) Berkeley Protocol, *supra* note 9, at 130-135
- (36) NIST SP 800-86, *supra* note 1, at 3-3
- (37) College of Policing, *Intelligence Management*.
- (38) Berkeley Protocol, *supra* note 9, at 135-140
- (39) Berkeley Protocol, *supra* note 9, at 140-145
- (40) Berkeley Protocol, *supra* note 9, at 145-150
- (41) Berkeley Protocol, *supra* note 9, at 150-155
- (42) NIST SP 800-86, *supra* note 1, at 4-6
- (43) Berkeley Protocol, *supra* note 9, at 155-160
- (44) Berkeley Protocol, *supra* note 9, at 160-165
- (45) NIST SP 800-86, *supra* note 1, at 4-7
- (46) Berkeley Protocol, *supra* note 9, at 165-170
- (47) Berkeley Protocol, *supra* note 9, at 170-175
- (48) NIST SP 800-86, *supra* note 1, at 4-8
- (49) Berkeley Protocol, *supra* note 9, at 175-180
- (50) Berkeley Protocol, *supra* note 9, at 180-185
- (51) Berkeley Protocol, *supra* note 9, at 185-190
- (52) NIST SP 800-86, *supra* note 1, at 3-6
- (53) NIST SP 800-86, *supra* note 1, at 3-7
- (54) NIST SP 800-86, *supra* note 1, at 3-8
- (55) Berkeley Protocol, *supra* note 9, at 190-195
- (56) Berkeley Protocol, *supra* note 9, at 195-200
- (57) NIST SP 800-86, *supra* note 1, at 3-9
- (58) NIST SP 800-86, *supra* note 1, at 3-10
- (59) NIST SP 800-86, *supra* note 1, at 4-9
- (60) NIST SP 800-86, *supra* note 1, at 3-11
- (61) NIST SP 800-86, *supra* note 1, at 3-12
- (62) NIST SP 800-86, *supra* note 1, at 3-13
- (63) Berkeley Protocol, *supra* note 9, at 200-205
- (64) NIST SP 800-86, *supra* note 1, at 3-14
- (65) NIST SP 800-86, *supra* note 1, at 3-15
- (66) Berkeley Protocol, *supra* note 9, at 205-210
- (67) NIST SP 800-86, *supra* note 1, at 3-16
- (68) NIST SP 800-86, *supra* note 1, at 3-17
- (69) Berkeley Protocol, *supra* note 9, at 210-215
- (70) NIST SP 800-86, *supra* note 1, at 4-10
- (71) NIST SP 800-86, *supra* note 1, at 4-11
- (72) Berkeley Protocol, *supra* note 9, at 215-220
- (73) Berkeley Protocol, *supra* note 9, at 220-225
- (74) Berkeley Protocol, *supra* note 9, at 225-230

- (75) Berkeley Protocol, *supra* note 9, at 230-235
- (76) Berkeley Protocol, *supra* note 9, at 235-240
- (77) Berkeley Protocol, *supra* note 9, at 240-245
- (78) Berkeley Protocol, *supra* note 9, at 245-250
- (79) Berkeley Protocol, *supra* note 9, at 250-255
- (80) Berkeley Protocol, *supra* note 9, at 255-260
- (81) Berkeley Protocol, *supra* note 9, at 260-265
- (82) Berkeley Protocol, *supra* note 9, at 265-270
- (83) Berkeley Protocol, *supra* note 9, at 270-275
- (84) Berkeley Protocol, *supra* note 9, at 275-280
- (85) Berkeley Protocol, *supra* note 9, at 280-285
- (86) NIST SP 800-86, *supra* note 1, at 3-18
- (87) Berkeley Protocol, *supra* note 9, at 285-290
- (88) NIST SP 800-86, *supra* note 1, at 3-19
- (89) Berkeley Protocol, *supra* note 9, at 290-295
- (90) Berkeley Protocol, *supra* note 9, at 295-300
- (91) Berkeley Protocol, *supra* note 9, at 300-305
- (92) Berkeley Protocol, *supra* note 9, at 305-310
- (93) Berkeley Protocol, *supra* note 9, at 310-315
- (94) NIST SP 800-86, *supra* note 1, at 4-12
- (95) Berkeley Protocol, *supra* note 9, at 315-320
- (96) Berkeley Protocol, *supra* note 9, at 320-325
- (97) NIST SP 800-86, *supra* note 1, at 4-13
- (98) Berkeley Protocol, *supra* note 9, at 325-330
- (99) Berkeley Protocol, *supra* note 9, at 330-335
- (100) NIST SP 800-86, *supra* note 1, at 4-14
- (101) Berkeley Protocol, *supra* note 9, at 335-340
- (102) Berkeley Protocol, *supra* note 9, at 340-345
- (103) Berkeley Protocol, *supra* note 9, at 345-350
- (104) NIST SP 800-86, *supra* note 1, at 4-15
- (105) Berkeley Protocol, *supra* note 9, at 350-355
- (106) Berkeley Protocol, *supra* note 9, at 355-360
- (107) Berkeley Protocol, *supra* note 9, at 360-365
- (108) Berkeley Protocol, *supra* note 9, at 365-370
- (109) Berkeley Protocol, *supra* note 9, at 370-375
- (110) Berkeley Protocol, *supra* note 9, at 375-380
- (111) NIST SP 800-86, *supra* note 1, at 4-16
- (112) Berkeley Protocol, *supra* note 9, at 380-385
- (113) Berkeley Protocol, *supra* note 9, at 385-390
- (114) Berkeley Protocol, *supra* note 9, at 390-395
- (115) NIST SP 800-86, *supra* note 1, at 4-17

الفصل الأول: أصالة المعلومات الرقمية وسلامتها والتوثيق الفني

المبحث الأول: التحقق من أصالة البيانات الرقمية وسلامتها

المطلب الأول: تحديد مصدر البيانات وهوية النظام أو الجهاز المنشئ لها

يُعد تحديد مصدر البيانات الرقمية نقطة الانطلاق في التحقق من أصالتها، إذ لا يمكن تقييم موثوقية المعلومات المستمدة من بيئة رقمية ما لم يُحدّد مصدرها، وتُعرف الظروف التي أنشئت فيها، وتُفحص الصلة بين البيانات والواقعة المراد التحقق منها. [1] وتزداد أهمية هذا الإجراء بسبب سهولة نسخ البيانات ونقلها وإعادة نشرها، وإمكان فصل المحتوى عن سياقه الأصلي، فضلاً عن قدرة بعض التقنيات على إنشاء محتوى يبدو مماثلاً للمحتوى الحقيقي. [2]

ويقصد بمصدر البيانات الرقمية الجهة أو النظام أو الجهاز أو الحساب أو الوسيط الذي يُنسب إليه إنشاء البيانات أو تسجيلها أو حفظها أو نشرها. ويقتضي هذا التعريف التمييز بين **المصدر المنشئ للبيانات**، و**المصدر الذي استُخرجت منه**، و**المصدر الذي أتاحها للقائم بالتحري**. فقد تكون الصورة قد التُقطت بواسطة هاتف محمول، ثم نُقلت إلى منصة إلكترونية، ومنها حُفظت على جهاز تابع لجهة أمنية. وفي هذه الحالة، لا يُعد الجهاز الأمني مصدر الصورة من حيث إنشائها، وإن كان يمثل مصدر النسخة التي خضعت للفحص. [3]

ويترتب على هذا التمييز أثر منهجي مهم؛ إذ إن إثبات أن البيانات استُخرجت من نظام معين لا يعني بالضرورة إثبات أن ذلك النظام أنشأها أصلاً، كما أن تحديد الحساب الذي نشر محتوى رقمياً لا يكفي وحده لإثبات أن صاحب الحساب هو الذي أنشأ المحتوى أو قام بنشره بنفسه. [4]

عناصر تحديد المصدر:

١. **تحديد الوعاء الرقمي:** الجهاز أو النظام أو قاعدة البيانات أو المنصة التي استُخرجت منها المعلومات، مع بيان طبيعة النسخة التي خضعت للفحص. [5]
٢. **تحديد المصدر المنشئ:** الجهاز أو الحساب أو النظام الذي أنشأ البيانات أو سجلها أول مرة. [6]
٣. **تحديد ظروف الإنشاء أو التسجيل:** الوقت المحتمل، وطبيعة العملية، والظروف التقنية المؤثرة. [7]
٤. **تحديد مسار انتقال البيانات:** توثيق عمليات النقل والنسخ والاستخراج والحفظ والمعالجة. [8]
٥. **تقييم إمكان نسبة البيانات إلى مصدر محدد:** التمييز بين ما ثبت فنياً، وما تدعمه قرائن متضافرة، وما لا يزال مجرد احتمال. [9]

ولا تتساوى هذه العناصر من حيث إمكان التحقق منها في جميع الحالات؛ فقد تتيح سجلات النظام معلومات دقيقة عن عمليات الإنشاء والتعديل، بينما لا يتضمن المحتوى المنشور على

منصة اجتماعية سوى بيانات محدودة. ولذلك، ينبغي ألا تتحول المتطلبات الفنية إلى افتراضات مسبقة بشأن إمكان الوصول إلى جميع المعلومات المتعلقة بمصدر البيانات.[10]

ويثير تحديد هوية النظام أو الجهاز المنشئ مسألة أخرى تتمثل في التمييز بين هوية الجهاز وهوية مستخدمه. فمعرفة الرقم التسلسلي لجهاز أو عنوان شبكي مرتبط باتصال معين لا تثبت، بمفردها، أن شخصاً بعينه هو الذي أنشأ البيانات أو نفذ النشاط محل التحري. فقد يتعدد مستخدمو الجهاز، أو تُستخدم الحسابات المشتركة، أو تتغير عناوين الاتصال، أو يُستغل الجهاز من قبل شخص آخر.[11]

وتتضح أهمية ذلك في التحريات المتعلقة بالحسابات الإلكترونية؛ إذ ينبغي التمييز بين إثبات وجود حساب، وإثبات نشر محتوى من خلاله، وإثبات السيطرة الفعلية على الحساب وقت النشر، ثم إثبات أن شخصاً معيناً هو الذي قام بالفعل. وهذه مستويات مختلفة من الاستدلال، لا يجوز اختزالها في نتيجة واحدة دون سند كافٍ.[12]

ومن الناحية الفنية، قد تُستخدم سجلات الأنظمة وبيانات الأجهزة والبيانات الوصفية ومعلومات الحسابات للتحقق من المصدر، إلا أن قيمة كل عنصر تتوقف على طبيعته ومدى اكتماله وإمكان التحقق المستقل منه. فالبيانات الوصفية قد تساعد على تحديد خصائص الملف أو البرنامج الذي أنشأه، لكنها لا تثبت دائماً هوية منشئه البشري.[13]

وفي هذا السياق، تبرز أهمية المعايير الفنية المتخصصة، ومنها **ISO/IEC 27037:2012** بشأن إجراءات التحقيق في الأدلة الرقمية، الذي يتناول تحديد الأدلة الرقمية وجمعها واكتسابها وحفظها، بما يدعم سلامة التعامل مع البيانات منذ المراحل الأولى.[14] غير أن تطبيق هذه المبادئ الفنية لا يُغني عن التحقق من مشروعية الوصول إلى البيانات أو من توافر الشروط القانونية اللازمة للاعتماد عليها.[15]

ويجب مراعاة أن إثبات مصدر البيانات لا يعني إثبات صحة مضمونها. فقد تكون الصورة أصلية ومنسوبة إلى جهاز معلوم، لكنها لا تُظهر الواقعة كاملة، أو تكون قد نُقِطت في سياق مختلف عن السياق الذي نُشرت فيه. ومن ثم، فإن التحقق من المصدر يمثل شرطاً مهماً لتقييم المعلومة، لكنه لا يشكل وحده أساساً كافياً للحكم على صحتها أو دلالتها القانونية.[16]

وعليه، فإن المنهج السليم يقتضي توثيق المصدر ودرجة التحقق منه، والفصل بين البيانات الثابتة والاستنتاجات المستخلصة منها، والإفصاح عن أوجه النقص التي قد تؤثر في نسبة البيانات إلى جهاز أو نظام أو شخص محدد.[17]

المطلب الثاني: التحقق من تاريخ الإنشاء والتعديل واكتمال البيانات

يمثل التحقق من تاريخ إنشاء البيانات الرقمية وتعديلها واكتمالها عنصراً أساسياً في تحديد قيمتها المعلوماتية والاستدلالية؛ لأن دلالة البيانات لا تتوقف على مضمونها الظاهر فحسب، بل تتأثر أيضاً بوقت إنشائها، وتسلسل التغييرات التي طرأت عليها، ومدى احتفاظها بالسياق الذي يفسرها.[18]

ويقتضي التحقق الزمني التمييز بين عدة مفاهيم:

- **تاريخ الإنشاء:** الوقت الذي أنشئت فيه البيانات أو سُجلت فيه الواقعة لأول مرة. [19]
- **تاريخ التعديل:** الوقت الذي طرأ فيه تغيير على الملف أو السجل. [20]
- **تاريخ النسخ أو النقل:** الوقت الذي نُقلت فيه البيانات إلى وسيط آخر. [21]
- **تاريخ النشر أو الإتاحة:** الوقت الذي أصبحت فيه البيانات متاحة للآخرين. [22]
- **تاريخ الحصول على البيانات:** الوقت الذي استخرج فيه القائم بالتحري البيانات أو تسلمها. [23]

ولا يجوز افتراض التطابق بين هذه التواريخ؛ فقد تكون الصورة قد أنشئت قبل نشرها بأيام، وقد يُظهر الملف تاريخاً مرتبطاً بعملية النسخ لا بوقت الالتقاط، كما قد يتغير التاريخ الظاهر نتيجة تحويل الملف بين صيغ مختلفة. [24]

ومن الناحية الفنية، قد تتضمن الملفات الرقمية بيانات وصفية تسجل معلومات عن الإنشاء والتعديل والجهاز المستخدم، إلا أن هذه البيانات تختلف من حيث الدقة والاكتمال وقابلية التغيير. ولذلك، فإن وجود تاريخ داخل ملف لا يكفي وحده لإثبات أن الحدث وقع في ذلك الوقت، بل يجب تقييم مصدر التاريخ وآلية إنشائه ومدى اتساقه مع بقية المعطيات. [25]

وتزداد صعوبة التحقق الزمني عند التعامل مع سجلات الأنظمة المتصلة بالشبكات؛ إذ قد تعتمد الأنظمة المختلفة على إعدادات زمنية متباينة، أو تستخدم مناطق زمنية مختلفة، أو تتأثر ساعاتها بعدم المزامنة. كما قد تسجل بعض الأنظمة الوقت وفق التوقيت العالمي المنسق، بينما تعرضه أنظمة أخرى وفق التوقيت المحلي. [26]

ويتطلب التعامل المنهجي توثيق المنطقة الزمنية وإعدادات الساعة ومصدر التوقيت، متى كانت هذه العناصر متاحة. وعند تعذر التحقق من دقة الساعة المستخدمة، ينبغي الإفصاح عن ذلك وتحديد أثره المحتمل في النتائج بدلاً من التعامل مع الطابع الزمني باعتباره حقيقة قطعية. [27]

أما **اكتمال البيانات**، فيقصد به مدى احتفاظ المادة الرقمية بالعناصر الضرورية لفهمها وتفسيرها في سياقها. ولا يقتصر النقص على حذف أجزاء من الملف؛ فقد يتمثل في غياب جزء من التسجيل، أو عدم توافر السجلات السابقة أو اللاحقة، أو فقدان البيانات الوصفية، أو الحصول على لقطة منفردة بدلاً من السجل الكامل. [28]

وتكمن خطورة نقص البيانات في أنه قد يؤدي إلى تفسير غير صحيح لمحتوى صحيح في ذاته. فالرسالة الإلكترونية قد تكون أصلية، لكن اقتطاعها من سلسلة المراسلات قد يغير دلالتها، والتسجيل المرئي قد يكون سليماً، لكن غياب الثواني السابقة أو اللاحقة قد يحجب سياقاً يؤثر في فهم الواقعة. وبذلك، ينبغي التمييز بين سلامة الجزء المتاح و**اكتمال المادة** التي يُراد الاستدلال بها. [29]

ويقتضي تقييم الاكتمال تحديد نطاق البيانات المتاحة، ومقارنتها بما يُتوقع وجوده في المصدر الأصلي، وفحص أي مؤشرات على الحذف أو الانقطاع، والتحقق من مدى توافر السجلات المساندة. وإذا تعذر الحصول على البيانات الكاملة، وجب تحديد الجزء الذي خضع للفحص وبيان حدود الاستنتاجات.[30]

كما ينبغي التمييز بين التعديل الذي يطرأ أثناء الاستخدام المعتاد، والتعديل لأغراض المعالجة أو التحليل، والتعديل الذي قد يؤثر في أصالة البيانات. فليس كل تغيير دليلاً على العبث؛ إذ قد تتغير بعض البيانات الوصفية تلقائياً نتيجة النقل أو التحويل. وفي المقابل، لا يجوز افتراض سلامة كل تغيير لمجرد إمكان تفسيره تقنياً.[31]

وفي هذا الإطار، تقتضي الممارسة المهنية الاحتفاظ بالنسخة المستلمة كما هي، وإجراء التحليل على نسخة عمل مناسبة، مع توثيق أي تحويل أو معالجة. ويُستفاد هنا من إرشادات **NIST** بشأن فحص الأدلة الرقمية، التي تؤكد أهمية اتباع إجراءات قابلة للتوثيق والمراجعة.[32]

ومن الناحية القانونية، لا يمكن تحديد الأثر المترتب على نقص البيانات أو عدم دقة التوقيت بصورة موحدة لجميع الأنظمة؛ فقد يؤثر الخلل في موثوقية المعلومة، أو في وزنها الاستدلالي، أو في إمكان قبولها وفقاً للقواعد الإجرائية. ولذلك، ينبغي تجنب الانتقال الآلي من اكتشاف خلل فني إلى تقرير عدم مشروعية الإجراء.[33]

وخلاصة التحليل أن التحقق من تاريخ البيانات واكتمالها يهدف إلى تحديد الحدود التي يمكن ضمنها تفسير المعلومات الرقمية بصورة منضبطة. وكلما تعذر إثبات التسلسل الزمني أو اكتمال المادة، وجب تضيق نطاق الاستنتاج والإفصاح عن مواطن عدم اليقين.[34]

المطلب الثالث: المحافظة على البيانات الأصلية وإعداد النسخ الفنية

تُعد المحافظة على البيانات الأصلية من أهم الضمانات الفنية في التحريات الأمنية الرقمية، إذ إن إمكان نسخ البيانات وتعديلها بسرعة، ووجود عمليات تقنية قد تغير بعض خصائصها دون أن تكون ظاهرة للمستخدم، يفرضان اعتماد إجراءات تحافظ على المادة التي جُمعت وتتيح مراجعة النتائج.[35]

ويقصد بالبيانات الأصلية البيانات الموجودة في مصدرها عند بدء التعامل معها، أو النسخة التي جرى الحصول عليها مباشرة من المصدر وفق إجراءات موثقة. غير أن وصف نسخة بأنها "أصلية" يحتاج إلى دقة؛ إذ قد يتعذر الوصول إلى المصدر المنشئ ذاته، كما يحدث عند الحصول على محتوى منشور عبر منصة إلكترونية. وفي هذه الحالات، ينبغي وصف النسخة وفق حقيقتها الإجرائية، مثل "النسخة المستلمة من الجهة المقدمة" أو "النسخة المستخرجة من النظام"، بدلاً من إسباغ صفة الأصلية عليها دون تحقق.[36]

الفئات الثلاث الرئيسية:

١. البيانات المستلمة أو المكتسبة: المادة التي تم الحصول عليها من الجهاز أو النظام أو الجهة المعنية، مع توثيق ظروف الحصول.[37]

٢. **النسخة الفنية المحفوظة**: نسخة يُراد الاحتفاظ بها لتكون مرجعاً للمراجعة والتحقق. [38]

٣. **نسخة العمل أو التحليل**: النسخة التي تُجرى عليها عمليات الفحص والمعالجة اللازمة. [39]

وتتمثل الغاية من الفصل بين النسخة المحفوظة ونسخة العمل في تقليل مخاطر التغيير غير المقصود، وتمكين المراجع من التحقق من أن النتائج لم تُبنَ على معالجة غير موثقة. غير أن إنشاء نسخ متعددة لا يحقق هذه الغاية تلقائياً؛ إذ ينبغي التحقق من سلامة النسخ وتوثيق العلاقة بينها وبين المادة التي أُخذت منها. [40]

وفي حالات فحص الأجهزة الرقمية، قد تتطلب المحافظة على البيانات استخدام إجراءات فنية مخصصة للحصول على نسخة جنائية، مع مراعاة طبيعة الجهاز ونظام الملفات وحالة التشغيل والتشفير. وقد يؤدي التعامل غير الملائم مع بعض الأجهزة إلى تغيير بياناتها أو فقدان أجزاء منها، لذلك يجب اختيار أسلوب الاكتساب وفق تقييم فني يراعي مخاطر الإجراء والغرض منه. [41]

ويؤكد دليل **NIST** بشأن التعامل مع الأدلة الرقمية المخزنة في الأجهزة المحمولة أهمية مراعاة طبيعة الجهاز ووسيلة الاكتساب والإجراءات اللازمة للحفاظ على البيانات وإتاحة فحصها. [42] ويُستفاد من ذلك أن المحافظة على البيانات لا تتحقق بمجرد حفظ الملف في وسيط آخر، بل تتطلب اختيار إجراء مناسب وتوثيق كيفية تنفيذه والقيود المرتبطة به. [43]

وتظهر أهمية هذه المسألة عند التعامل مع الأجهزة المتصلة بالشبكات والخدمات السحابية. فقد تتغير البيانات المخزنة في هذه الأنظمة باستمرار، وقد يؤدي الوصول إليها إلى تحديث سجلات أو تعديل بعض المعلومات التشغيلية. ومن ثم، ينبغي أن يحدد القائم بالفحص ما إذا كان الإجراء يتطلب حفظ نسخة محددة من البيانات، أو توثيق حالتها في وقت معين، أو الحصول على سجلات إضافية. [44]

ويجب عدم إغفال **القيود القانونية** المتعلقة بالبيانات التي تتضمن معلومات لأشخاص غير مستهدفين. فالحفاظ على البيانات الأصلية لا يبرر تلقائياً جمع كل محتويات الجهاز أو الاحتفاظ بها دون تمييز، بل يجب أن يجري الاكتساب والفحص في حدود السند القانوني ونطاق الإجراء، مع اتخاذ التدابير المناسبة لحماية المعلومات غير المرتبطة. [45]

ومن هنا، يظهر التفاعل بين المحافظة الفنية على البيانات ومبدأ **تقليل البيانات**؛ إذ يتعين التوفيق بين ضرورة صون المادة الرقمية اللازمة للتحقق وبين عدم التوسع في الوصول إلى بيانات لا يشملها الغرض المشروع. ويُعالج هذا التوازن من خلال تحديد نطاق الاكتساب، وتقييد الوصول، والفصل بين المواد ذات الصلة وغيرها، وتطبيق قواعد الحفظ والإتلاف. [46]

ويجب أن يتضمن سجل الإجراءات وصفاً للبيانات التي تم الحصول عليها، وطريقة الاكتساب، والأدوات المستخدمة، وتاريخ الإجراء، وهوية القائمين به، وأي معالجة أُجريت على النسخ.

وإذا استُخدمت وسيلة تقنية قد تؤثر في البيانات، وجب بيان ذلك وتحديد نطاق التأثير المحتمل. [47]

ومن المهم التأكيد أن الاحتفاظ بنسخة محفوظة لا يثبت وحده صحة البيانات أو صدق مضمونها. فقد تكون النسخة مطابقة تماماً للملف الذي جرى استلامه، مع بقاء الشك في مصدر الملف أو في الظروف التي أنشئ فيها. ولذلك، ينبغي الجمع بين المحافظة على البيانات والتحقق من المصدر والتوقيت والسياق. [48]

وعليه، فإن القيمة العلمية للمحافظة على البيانات الأصلية وإعداد النسخ الفنية تكمن في إتاحة إعادة الفحص وتقليل مخاطر التغيير غير الموثق، لا في منح البيانات حجية مطلقة. [49]

المطلب الرابع: استخدام قيم التجزئة الرقمية للتحقق من سلامة النسخ

تُستخدم قيم التجزئة الرقمية (Hash Values) في التحقق من سلامة البيانات الرقمية ومقارنة النسخ بعضها ببعض. وهي تمثل ناتج تطبيق خوارزمية تجزئة على مجموعة محددة من البيانات، بحيث تنتج قيمة رقمية أو سلسلة رمزية ترتبط بمحتوى تلك البيانات وفق خصائص الخوارزمية المستخدمة. [50]

وتنبع أهمية هذه التقنية من إمكان استخدامها للكشف عن التغييرات التي تطرأ على البيانات بين مرحلتين من مراحل التعامل معها. فإذا حُسبت قيمة التجزئة لملف معين، ثم حُسبت مرة أخرى للملف نفسه بعد نقله أو نسخه، وأُنْتُجَت العمليتان القيمة ذاتها باستخدام الخوارزمية نفسها، فإن ذلك يوفر مؤشراً قوياً على تطابق المحتوى الذي تناولته عملية الحساب في المرحلتين. [51]

ومع ذلك، ينبغي عدم الخلط بين تطابق قيم التجزئة وبين إثبات صحة مصدر البيانات أو مضمونها. فقيمة التجزئة لا تثبت بذاتها أن الملف أنشئ بواسطة الجهاز المنسوب إليه، ولا تحدد الشخص الذي أنشأه أو عدّله، ولا تثبت أن المحتوى يعكس واقعة حقيقية. [52]

التمييز بين ثلاث مسائل:

- **سلامة النسخة:** التحقق من أن محتوى النسخة لم يتغير مقارنة بالمادة التي حُسبت لها قيمة مرجعية. [53]
- **أصالة المصدر:** التحقق من أن البيانات تعود إلى المصدر المنسوب إليها، وهو أمر يتطلب قرائن وإجراءات إضافية. [54]
- **صحة المضمون:** التحقق من أن المعلومات الواردة صحيحة وتعكس الواقعة، وهو ما يحتاج إلى تحليل مستقل. [55]

وقد تكون قيمة التجزئة متطابقة لنسختين من ملف مزور، إذا كان الملف المزور نفسه هو الذي استُخدم أساساً للمقارنة. كما قد تكون النسخة مطابقة للملف المستلم، مع كون الملف المستلم قد عدّل قبل تسليمه. وبناءً عليه، لا يصح الاستناد إلى تطابق قيمة التجزئة وحده لإثبات أن الملف لم يتعرض لأي تعديل في جميع مراحل وجوده السابقة. [56]

ومن الناحية الفنية، تعتمد موثوقية المقارنة على استخدام خوارزمية مناسبة، وتحديد البيانات التي طُبقت عليها الخوارزمية بدقة، وتوثيق وقت الحساب والأداة المستخدمة ونتيجته. كما ينبغي أن تكون قيمة التجزئة المرجعية مرتبطة بمرحلة واضحة من مراحل التعامل مع البيانات.[57]

وتختلف خوارزميات التجزئة من حيث خصائصها ومستوى مقاومتها للتصادمات. ولذلك، يجب اختيار الخوارزمية وفق الغرض من الاستخدام والمعايير الفنية المعتمدة. وتقدم المعايير الصادرة عن **NIST** مرجعاً فنياً لتقييم خوارزميات التجزئة وخصائصها الأمنية، بما في ذلك معيار SHA-2 ضمن مواصفات.[58] Secure Hash Standard

ولا يقتصر استخدام قيم التجزئة على التحقق من سلامة الملفات المخزنة، بل يمكن أن يمتد إلى توثيق النسخ المستخرجة من الأجهزة، ومقارنة الملفات قبل المعالجة وبعدها، والتحقق من مطابقة النسخ المستخدمة في الفحص للنسخ المحفوظة.[59]

غير أن تفسير النتائج يقتضي مراعاة طبيعة البيانات. فقد يؤدي تحويل ملف إلى صيغة أخرى، أو إعادة ضغط صورة، أو تعديل البيانات الوصفية، إلى تغيير قيمة التجزئة، حتى لو ظل المحتوى المرئي متشابهاً. ولا يعني اختلاف القيمة في هذه الحالات بالضرورة وجود تزوير، بل يدل على أن البيانات التي جرى حساب قيمتها ليست متطابقة على مستوى المحتوى الذي تعالجه الخوارزمية.[60]

وفي المقابل، لا يجوز اعتبار التشابه البصري بين صورتين دليلاً على تطابقهما الرقمي؛ فقد تتشابه صورتان في المظهر مع اختلاف بياناتهما الداخلية. ولذلك، ينبغي تحديد الغرض من المقارنة: هل يراد إثبات التطابق الرقمي الكامل، أم مقارنة المحتوى البصري، أم التحقق من وجود تعديلات محددة؟.[61]

وتتطلب الممارسة المهنية أن تُوثق قيمة التجزئة مع بيان اسم الملف أو معرفه، وحجمه، والخوارزمية المستخدمة، والأداة، وتاريخ الإجراء، والمرحلة التي حُسبت فيها القيمة. وعند اكتشاف اختلاف بين قيم التجزئة، ينبغي الانتقال إلى فحص سبب الاختلاف بدلاً من تقرير وجود عبث بصورة تلقائية.[62]

ومن منظور قانوني، لا تؤدي قيم التجزئة وظيفة الإذن بالحصول على البيانات، ولا تعالج أي مخالفة وقعت أثناء جمعها، ولا تحسم مدى قبولها أمام جهة التحقيق أو المحكمة. وتظل هذه المسائل خاضعة للقواعد القانونية ذات الصلة، في حين تسهم قيم التجزئة في دعم سلامة التعامل الفني مع البيانات.[63]

وبذلك، فإن الاستخدام المنضبط لقيم التجزئة يعزز موثوقية إجراءات حفظ البيانات الرقمية، بشرط ألا يُحمّل هذه التقنية دلالة تتجاوز وظيفتها. فهي تثبت، في نطاق استخدامها الصحيح، علاقة تطابق أو اختلاف بين محتويات محددة، لكنها لا تثبت وحدها المصدر أو الهوية أو صحة الواقعة أو المشروعية القانونية للإجراء.[64]

المبحث الثاني: سلسلة العهدة الرقمية وضمان الجودة

المطلب الأول: مفهوم سلسلة العهدة الرقمية وأهميتها

تُعد سلسلة العهدة الرقمية من العناصر الأساسية لضمان إمكان تتبع البيانات منذ الحصول عليها وحتى تقديمها إلى الجهة المختصة أو انتهاء الحاجة القانونية إلى الاحتفاظ بها. وتنبع أهميتها من أن موثوقية البيانات الرقمية لا تتوقف على خصائصها الفنية فحسب، بل تتأثر أيضاً بوضوح الإجراءات التي خضعت لها، وهوية الأشخاص الذين تعاملوا معها، والظروف التي جرى فيها نقلها وحفظها وفحصها. [65]

ويقصد بسلسلة العهدة الرقمية السجل المتصل الذي يوثق مراحل حيازة البيانات أو الوسيط الذي يحتويها، والإجراءات التي أُجريت عليه، والأشخاص الذين تولوا استلامه أو نقله أو فحصه أو الوصول إليه، مع بيان التوقيت والظروف ذات الصلة بكل مرحلة. [66]

ويقتضي هذا المفهوم التمييز بين الحيازة المادية للوسيط الرقمي والسيطرة الإجرائية على البيانات. فقد يكون الجهاز محفوظاً داخل مستودع مؤمن، بينما تُنسخ البيانات المستخرجة منه إلى بيئة تحليل مستقلة يتعامل معها عدد من المختصين. وفي هذه الحالة، لا يكفي تسجيل انتقال الجهاز المادي، بل يجب توثيق انتقال النسخ الرقمية والعمليات التي أُجريت عليها. [67]

وتختلف طبيعة سلسلة العهدة بحسب نوع البيانات. ففي حالة الأجهزة المضبوطة، قد تتضمن السلسلة استلام الجهاز وتغليفه وحفظه واستخراج نسخة فنية منه. أما في حالة المحتوى المنشور عبر الإنترنت، فقد تتعلق السلسلة بتحديد الصفحة أو الملف المستهدف، وتوثيق وقت الحصول عليه وطريقته، وحفظ النسخة المستلمة. [68]

وظائف سلسلة العهدة:

١. إمكان التتبع: تمكين المراجع من معرفة المسار الذي سلكته البيانات. [69]
٢. تعزيز المساءلة: تحديد المسؤوليات المتعلقة بالاستلام والنقل والحفظ والفحص. [70]
٣. الكشف عن الانقطاع أو التغيير: إظهار الفجوات أو التغييرات التي قد تؤثر في تقييم السلامة. [71]
٤. دعم إعادة الفحص: إتاحة معرفة النسخة التي استُخدمت في التحليل. [72]
٥. تعزيز الشفافية: تمكين الجهة المختصة من تقييم مدى اكتمال التوثيق. [73]

غير أن وجود سلسلة عهدة مكتملة شكلياً لا يعني بالضرورة أن البيانات صحيحة أو أن جميع الإجراءات كانت سليمة. فقد يكون السجل دقيقاً في وصف انتقال ملف معين، مع بقاء الشك في المصدر الذي أنشأه أو في مضمون المعلومات. كما أن توثيق كل خطوة لا يمنع بالضرورة وقوع خطأ فني أثناء التحليل. [74]

ومن ثم، ينبغي التعامل مع سلسلة العهدة باعتبارها أداة لإثبات مسار التعامل مع البيانات، لا شهادة مطلقة بصحتها. وهي ترتبط بسلامة البيانات ارتباطاً وثيقاً، لكنها لا تستبدل التحقق الفني

من الأصلالة، ولا تغني عن تقييم موثوقية المصدر، ولا تحسم مشروعية الحصول على المعلومات.[75]

وتؤكد المواصفة **ISO/IEC 27037:2012** أهمية اتباع إجراءات محددة للتعرف على الأدلة الرقمية وجمعها واكتسابها وحفظها، بما يدعم الحفاظ على سلامتها وإمكان الاعتماد على الإجراءات.[76] وتُستفاد من هذه المبادئ ضرورة أن يكون سجل العهدة جزءاً من منظومة أوسع تشمل التخطيط للجمع، وتوثيق المصدر، وحفظ النسخ، وضبط الوصول، والتحقق من النتائج.[77]

ويجب أن تتضمن سلسلة العهدة، بالقدر الذي يتناسب مع طبيعة البيانات، تحديد العنصر الرقمي أو الوسيط، وتاريخ ووقت كل عملية، واسم القائم بها وصفته، وسبب الإجراء، وطريقة النقل أو الحفظ، ومكان التخزين، وأي ملاحظات تتعلق بحالة البيانات.[78]

ولا ينبغي أن يتحول التوثيق إلى إجراء شكلي يُستكمل بعد انتهاء العمل؛ لأن التسجيل المتأخر قد يؤدي إلى نسيان تفاصيل مهمة. ولذلك، تقتضي الممارسة المهنية توثيق الخطوات في وقت تنفيذها أو في أقرب وقت ممكن، مع بيان أي استكمال لاحق.[79]

ومن الناحية القانونية، يختلف الأثر المترتب على نقص سلسلة العهدة بحسب النظام الإجرائي وطبيعة النقص ومدى تأثيره في موثوقية البيانات. فقد يكون النقص قابلاً للتفسير أو الاستكمال بقرائن مستقلة، وقد يثير شكاً جوهرياً. ولهذا لا يصح تقرير أن كل انقطاع يؤدي تلقائياً إلى استبعاد البيانات، كما لا يصح اعتبار الانقطاع غير مؤثر دون تحليل.[80]

وعليه، فإن القيمة الأساسية لسلسلة العهدة تتمثل في جعل التعامل مع البيانات الرقمية قابلاً للتتبع والمراجعة والمساءلة، بما يقلل من الاعتماد على الروايات الشخصية غير المدعومة بسجلات.[81]

المطلب الثاني: توثيق الاستلام والنقل والحفظ والوصول إلى البيانات

يقتضي بناء سلسلة عهدة فعالة توثيق كل مرحلة جوهريّة من مراحل التعامل مع البيانات الرقمية، بدءاً من الاستلام، مروراً بالنقل والحفظ، وانتهاءً بالوصول إليها لأغراض الفحص أو العرض أو التسليم.[82]

ويبدأ التوثيق عند الاستلام بتحديد البيانات أو الوسيط المستلم وصفاً كافياً يمنع الخلط بينه وبين عناصر أخرى. ويشمل ذلك نوع الجهاز أو الوسيط، والمعرفات المتاحة، وحالة التغليف أو الأختام، والجهة التي سلمته، وتاريخ ووقت الاستلام، واسم المستلم وصفته، والأساس الذي جرى بموجبه التسليم.[83]

وفي حالة البيانات التي تُسلم إلكترونياً، ينبغي توثيق وسيلة التسليم ونطاق الملفات أو السجلات المستلمة، والجهة المرسلّة، والوقت، وأي قيود تتعلق بصيغة البيانات أو اكتمالها. وإذا تعذر التحقق من بعض المعلومات، فينبغي تسجيل ذلك صراحةً.[84]

أما **مرحلة النقل**، فتتطلب تحديد الجهة أو الشخص الذي تولى النقل، وتاريخ العملية ووقتها، والوسيلة المستخدمة، والجهة المستلمة، وأي ظروف قد تؤثر في سلامة البيانات. وقد يشمل النقل انتقال جهاز مادي، أو نقل نسخة رقمية عبر وسيط تخزين، أو تسليم ملفات من خلال قناة إلكترونية. [85]

ويجب أن تتناول **سجلات الحفظ** موقع تخزين البيانات أو الوسيط، والجهات المخولة بالوصول إليه، والتدابير المستخدمة لمنع الفقد أو التغيير غير المصرح به. كما ينبغي التمييز بين حفظ الجهاز المادي وحفظ البيانات المستخرجة منه. [86]

وفيما يتعلق **بالوصول إلى البيانات**، لا يكفي تسجيل أسماء الأشخاص الذين تسلموا الوسيط، بل ينبغي توثيق الوصول الفعلي إلى البيانات عندما يكون ذلك ممكناً. ويشمل ذلك تحديد المستخدم المخول، ووقت الوصول، والغرض منه، والعمليات التي أجريت. [87]

ويجب التمييز بين الوصول الذي يقتصر على **الاطلاع**، والوصول الذي يتضمن **نسخ البيانات أو تعديلها أو استخراجها أو حذفها**. فلكل عملية أثر فني مختلف، ولا يصح الاكتفاء بوصف عام مثل "تم فحص البيانات". [88]

كما تقتضي الممارسة المهنية استخدام وسائل مناسبة لضبط الوصول، مثل تحديد صلاحيات المستخدمين وتسجيل العمليات ومراجعتها. ويجب أن تكون هذه الضوابط متناسبة مع حساسية البيانات وطبيعة الإجراء. [89]

ومن المهم توثيق عمليات إنشاء **النسخ الفنية**، مع بيان مصدر النسخة الجديدة وصلتها بالبيانات التي أخذت منها، وطريقة إنشائها، وأي وسائل استُخدمت للتحقق من سلامتها. [90]

وتتطلب إدارة البيانات الرقمية مراعاة متطلبات **السرية وحماية البيانات الشخصية**، خصوصاً عندما تتضمن المواد معلومات تتعلق بأشخاص غير مستهدفين. ولذلك، ينبغي قصر الوصول على الأشخاص الذين تستلزم مهامهم الاطلاع، مع اتخاذ تدابير تمنع الاستخدام غير المصرح به. [91]

وقد يقتضي الفحص إنشاء نسخ عمل متعددة أو نقل أجزاء من البيانات إلى بيئة تحليل متخصصة. ولا يمثل ذلك إخلالاً بسلسلة العهدة في ذاته، بشرط توثيق النسخ ومصادرها ومسارها. [92]

وفي المقابل، قد تظهر أثناء المراجعة **فجوة** في سجل النقل أو الحفظ، كغياب توقيع أو عدم تحديد وقت عملية معينة. ولا ينبغي التعامل مع جميع أوجه النقص بالدرجة نفسها؛ بل يتعين تحديد طبيعتها، والبحث عن سجلات مستقلة تساعد على استكمال المعلومات، وتقييم أثر الفجوة. [93]

وقد تكون الفجوة **إدارية** لا تؤثر في هوية البيانات، وقد تكون **جوهرية** إذا حالت دون تحديد النسخة التي خضعت للفحص أو أثارت شكاً معقولاً. ويتوقف التقييم على طبيعة البيانات، والأدلة المتاحة، والإجراءات التي اتُبعت، والقواعد القانونية. [94]

ويترتب على ذلك أن توثيق الاستلام والنقل والحفظ والوصول ليس غاية مستقلة، بل هو وسيلة لضمان الشفافية وإمكان التحقق من كل مرحلة. وكلما كان السجل واضحاً ومتصلاً، زادت قدرة الجهة المختصة على تقييم سلامة الإجراءات.[95]

المطلب الثالث: توثيق أدوات الفحص وإصداراتها وخطوات المعالجة

يمثل توثيق الأدوات الفنية المستخدمة في فحص البيانات الرقمية وخطوات المعالجة شرطاً مهماً لقابلية النتائج للمراجعة وإعادة التحقق. فالنتيجة الرقمية لا تُفهم بمعزل عن الوسيلة التي أنتجتها؛ إذ قد تختلف المخرجات باختلاف البرنامج أو إصداره أو إعداداته أو طريقة استخدامه.[96]

ويُقصد بأدوات الفحص البرامج والتطبيقات والأجهزة والأنظمة التي تُستخدم لاكتساب البيانات الرقمية أو تحليلها أو استعادتها أو التحقق من خصائصها. وقد تشمل أدوات استخراج الملفات، وبرامج تحليل سجلات الأنظمة، وأدوات فحص الصور والفيديو، وبرامج استعادة البيانات المحذوفة.[97]

ولا يكفي في التقرير أن يذكر القائم بالفحص اسم الأداة بصورة عامة، بل ينبغي تحديد اسمها وإصدارها، والغرض الذي استُخدمت من أجله، والإعدادات المؤثرة في النتائج، والبيئة التقنية، وأي قيود معروفة.[98]

وتبرز أهمية تحديد الإصدار لأن التحديثات قد تغير طريقة معالجة البيانات أو تفسير بعض الحقول. كما قد تختلف النتائج عند استخدام إعدادات مختلفة، حتى لو استُخدم البرنامج نفسه.[99]

ويجب التمييز بين الأدوات التي تُستخدم لاكتساب البيانات، والأدوات التي تُستخدم لفحصها، والأدوات التي تُستخدم لعرض النتائج. فقد تتطلب كل مرحلة ضوابط مختلفة.[100]

وتقتضي الممارسة المهنية تسجيل الخطوات الجوهرية التي اتُبعت في الفحص، بما يشمل البيانات التي أدخلت إلى الأداة، والإجراءات التي نُفذت، والنتائج التي ظهرت، وأي تعديلات على الإعدادات، وأسباب اتخاذ القرارات الفنية المؤثرة.[101]

كما ينبغي توثيق أي تدخل بشري في عملية المعالجة، خصوصاً عندما يتضمن اختيار بيانات معينة، أو استبعاد عناصر أخرى، أو تحديد معايير البحث، أو اعتماد نتيجة صادرة عن نظام آلي.[102]

وتزداد أهمية هذه المسألة عند استخدام أدوات تعتمد على خوارزميات آلية لتحليل الصور أو التعرف على الأنماط. ففي هذه الحالات، ينبغي بيان الغرض من استخدام النظام، وطبيعة المخرجات، والقيود المعروفة، ومدى خضوع النتيجة للتحقق المستقل.[103]

وتدعم إرشادات **NIST** بشأن فحص الأدلة الرقمية أهمية توثيق إجراءات الفحص والمحافظة على سلامة البيانات بما يتيح مراجعة النتائج.[104] كما توفر منشورات المعهد المتعلقة بالأدلة الرقمية في الأجهزة المحمولة إرشادات فنية بشأن طبيعة الاكتساب وقيوده.[105]

ومن المسائل المهمة **التحقق من ملائمة الأداة للمهمة**. فكون البرنامج شائع الاستخدام لا يعني أنه مناسب لكل أنواع البيانات. وقد تكون الأداة قادرة على استخراج نوع محدد من المعلومات، لكنها لا تستطيع تفسير سياقه. [106]

ولهذا، ينبغي أن يميز التقرير بين ما استخرجته الأداة مباشرة، وما فسره القائم بالفحص، وما استنتجه بناءً على جمع عدة نتائج. فمثلاً، قد تُظهر الأداة وجود ملف أو سجل زمني، لكن تفسير دلالاته على نشاط شخص معين يحتاج إلى تحليل مستقل. [107]

وعند استخدام أكثر من أداة، قد يكون من المناسب مقارنة النتائج للتحقق من الاتساق. غير أن الاتفاق بين أداتين لا يثبت الصحة تلقائياً، خصوصاً إذا كانتا تعتمدان على الطريقة البرمجية نفسها. [108]

كما ينبغي توثيق الأخطاء التي ظهرت أثناء الفحص، والعمليات التي تعذر إكمالها، والبيانات التي لم تتمكن الأداة من قراءتها. ولا يُعد الإفصاح عن هذه القيود انتقاصاً من قيمة التقرير، بل يمثل عنصراً من الأمانة العلمية. [109]

وتبرز هنا أهمية الفصل بين صلاحية الأداة للاستخدام الفني وبين حجية النتائج من الناحية القانونية. فقد تكون الأداة مناسبة فنياً، لكن استخدامها تم خارج نطاق الإذن. [110]

وبذلك، فإن توثيق الأدوات والإصدارات وخطوات المعالجة يحقق غرضين: تمكين المراجعة الفنية المستقلة، وتحديد حدود النتائج والمسؤولية عن القرارات التي أسهمت في إنتاجها. [111]

المطلب الرابع: معالجة النقص أو الانقطاع في سجلات العهدة وإمكان إعادة الفحص

قد تواجه إجراءات التحري الرقمي حالات لا تتوافر فيها سجلات كاملة لجميع مراحل الاستلام والنقل والحفظ والفحص، سواء بسبب خطأ بشري أو قصور مؤسسي أو خلل تقني. وتثير هذه الحالات مسألة تحديد أثر النقص في سلسلة العهدة على سلامة البيانات وإمكان الاعتماد عليها. [112]

ويقتضي التحليل التمييز بين **النقص الشكلي** الذي لا يؤثر جوهرياً، و**النقص الذي يثير شكاً فعلياً** في هوية النسخة أو في احتمال تعرضها للتغيير، و**الانقطاع الذي يتعذر معه تفسير مرحلة أساسية**. [113]

ولا يجوز اعتبار كل نقص في السجل دليلاً على العبث؛ فقد يكون سبب النقص إغفالاً إدارياً. وفي المقابل، لا يصح افتراض أن النقص غير مؤثر لمجرد عدم وجود دليل مباشر على التغيير. [114]

خطوات معالجة النقص:

١. تحديد موضعه وطبيعته. [115]

٢. البحث عن مصادر مستقلة يمكن أن تساعد على استكمال السجل، مثل سجلات الدخول أو النقل الإلكتروني. [116]

٣. تقييم هذه المصادر من حيث أصالتها واكتمالها واستقلالها. [117]
 ٤. التمييز بين المعلومات التي أمكن استعادتها، والمعلومات المستنتجة من قرائن، والعناصر التي ما زالت مجهولة. [118]
 ٥. توثيق عملية استكمال السجل ذاتها، مع بيان وقت إجرائها ومصدر المعلومات. [119]
 ٦. المحافظة على السجل السابق وإضافة بيان تكميلي واضح، بدل تعديل السجل الأصلي. [120]
 ٧. فحص أثر النقص في النتائج التي استُخلصت من البيانات. [121]
 ٨. الإفصاح عن مستوى الثقة في النتيجة بما يتناسب مع مقدار المعلومات المتاحة. [122]
- ويجب عدم الخلط بين **الأثر الفني للنقص والأثر القانوني له**. فالتقييم الفني ينصب على مدى إمكان التحقق من هوية البيانات وسلامتها، بينما يتعلق التقييم القانوني بمدى تأثير الخل في قبول المعلومات أو وزنها في الإثبات. [123]
- وقد يكون هناك خلل في سلسلة العهدة دون أن يؤدي بالضرورة إلى استبعاد البيانات قانوناً، إذا أمكن التحقق من سلامتها بوسائل أخرى. وقد يكون النقص محدوداً فنياً، لكنه يثير إشكالاً قانونياً إذا خالف متطلباً إجرائياً جوهرياً. [124]
- ومن الناحية المؤسسية، تكشف حالات النقص المتكررة عن الحاجة إلى تطوير إجراءات العمل، وتوحيد النماذج، وتحديد المسؤوليات، واستخدام أنظمة تسجل العمليات تلقائياً. كما تستلزم تدريب العاملين على أهمية التوثيق المعاصر للإجراء. [125]
- أما إمكان **إعادة الفحص والتحقق المستقل**، فيُعد من أهم مؤشرات جودة العمل الفني. ويقصد بإعادة الفحص إمكانية إخضاع البيانات أو النسخ المناسبة لإجراءات تحقق لاحقة بهدف مراجعة النتيجة أو اختبارها. أما التحقق المستقل، فيعني مراجعة النتيجة بواسطة شخص أو جهة أخرى لا تعتمد على مجرد التسليم بما انتهى إليه الفاحص الأول. [126]
- عناصر قابلية إعادة الفحص:**

١. تحديد البيانات التي استندت إليها النتيجة، والنسخة التي خضعت للتحليل. [127]
٢. توثيق الأدوات المستخدمة وإصداراتها والإعدادات ذات الصلة. [128]
٣. تسجيل الخطوات الجوهرية التي اتُبعت. [129]
٤. حفظ المخرجات والسجلات الفنية التي تساعد على تفسير النتيجة. [130]
٥. بيان الافتراضات التي اعتمد عليها التحليل والقيود. [131]
٦. إتاحة البيانات اللازمة للمراجعة ضمن الحدود القانونية. [132]

ولا تتحقق قابلية إعادة الفحص بمجرد الاحتفاظ بالتقرير النهائي، لأن التقرير قد يتضمن خلاصة النتيجة دون التفاصيل اللازمة. كما أن الاحتفاظ بالبيانات وحده لا يكفي إذا لم تُوثق الأدوات أو خطوات المعالجة. [133]

ويجب التمييز بين تكرار النتيجة والتحقق من صحتها. فقد يعيد فاحص ثانٍ استخدام الأداة ذاتها والإعدادات ذاتها، فيتوصل إلى النتيجة نفسها، دون أن يكشف ذلك عن خطأ مشترك في المنهج. [134]

ولا يعني اختلاف النتائج بين فاحصين بالضرورة أن أحدهما ارتكب خطأ؛ فقد يرجع الاختلاف إلى اختلاف الإعدادات أو نطاق البيانات أو تفسير المخرجات. وفي هذه الحالة، ينبغي تحديد مصدر الاختلاف وتحليل أسبابه. [135]

وتكتسب المراجعة المستقلة أهمية خاصة في الحالات التي قد تترتب على نتائج التحري آثار تمس حقوق الأفراد. فكلما زادت خطورة القرار، ازدادت أهمية التحقق من سلامة الأساس الفني. [136]

ومع ذلك، يجب أن تراعي إعادة الفحص القيود القانونية المتعلقة بالوصول إلى البيانات. فلا يجوز تمكين المراجع من الاطلاع على معلومات محمية خارج نطاق التفويض. [137]

كما ينبغي أن يُفصح التقرير عن حدود إعادة الفحص، مثل تعذر الوصول إلى المصدر الأصلي، أو انتهاء صلاحية خدمة إلكترونية، أو عدم توافر إصدار سابق من أداة التحليل. [138]

وتتصل قابلية إعادة الفحص بالتمييز بين النتائج التي يمكن تكرارها آلياً والنتائج التي تعتمد على التقدير المهني. فقد يؤدي تطبيق خوارزمية على مجموعة بيانات محددة إلى نتيجة قابلة للتكرار، بينما يتطلب تفسير دلالة هذه النتيجة ممارسة حكم مهني يظل خاضعاً للمراجعة. [139]

ومن الناحية القانونية، لا تعني قابلية إعادة الفحص أن جهة التحقيق أو المحكمة ملزمة بقبول النتيجة، بل إنها توفر أساساً أفضل لتقييمها. [140]

وعليه، فإن إعادة الفحص والتحقق المستقل لا يمثلان مجرد إجراء احتياطي، بل يشكلان عنصراً من عناصر المساءلة العلمية والمهنية. [141]

المبحث الثالث: توثيق إجراءات التحري وإعداد التقارير

المطلب الأول: تسجيل الإجراءات والقائمين بها وتوقيتها

يمثل توثيق إجراءات التحري الأمني الرقمي ركيزة أساسية لضمان الشفافية وإمكان المراجعة، إذ لا يكفي أن تكون الإجراءات قد نُفذت بالفعل، بل يجب أن يتوافر سجل يوضح طبيعتها وتسلسلها والجهات التي قامت بها والظروف التي أحاطت بها. [142]

ويُقصد بتوثيق الإجراءات تسجيل المعلومات الجوهرية المتعلقة بالتحري، منذ تحديد موضوعه وسننه القانوني، مروراً بجمع المعلومات وفحصها وتحليلها، وانتهاءً بصياغة النتائج. ويختلف نطاق التوثيق بحسب طبيعة الإجراء، إلا أنه ينبغي أن يكون كافياً لفهم ما تم، ولماذا تم، وكيف نُفذ. [143]

ويجب أن يتضمن سجل الإجراء، بحسب مقتضى الحال، تاريخ التنفيذ ووقته، وهوية القائم به وصفته، والجهة التي يعمل لديها، وموضوع الإجراء، والأساس القانوني، ومصدر البيانات، وطريقة الحصول عليها، والأدوات المستخدمة، والنتائج الأولية، وأي قيود أو صعوبات. [144]

ولا ينبغي أن يقتصر التوثيق على الإجراءات التي أفضت إلى نتيجة إيجابية؛ بل يجب أن يشمل الخطوات التي لم تؤدِّ إلى العثور على معلومات ذات صلة، والعمليات التي تعذر استكمالها. فإغفال النتائج السلبية قد يؤدي إلى تقديم صورة غير مكتملة. [145]

ويقتضي التوثيق الدقيق **الفصل بين وصف الإجراء وتفسير نتيجته**. فوصف الإجراء يبين ما قام به القائم بالتحري فعلياً، أما التفسير فيوضح الدلالة التي استخلصها. فعلى سبيل المثال، يختلف تسجيل العثور على ملف يتضمن بيانات موقع عن الاستنتاج بأن شخصاً معيناً كان موجوداً في ذلك الموقع. [146]

كما ينبغي تسجيل **القرارات المهنية** التي تؤثر في نطاق العمل، مثل اختيار مصدر معين، أو استبعاد بيانات، أو استخدام أداة محددة، أو اعتماد معيار لتصنيف المعلومات. [147]

ويجب أن يتسم السجل بالدقة والموضوعية، وأن يتجنب العبارات التي تخلق بين الوقائع والاشتباه. فعبارات مثل "ثبت أن الشخص قام بالفعل" لا تكون مناسبة لمجرد العثور على بيانات مرتبطة بحسابه، ما لم تكن هناك أدلة كافية. [148]

ومن الضروري توثيق **التعديلات اللاحقة** التي تطرأ على المحاضر أو التقارير. فإذا ظهر خطأ في سجل سابق، ينبغي تصحيحه بطريقة تحفظ أثر التعديل وتوضح سببه وتاريخه. [149]

ويجب مراعاة أن توثيق الإجراءات **لا يمنحها المشروعية** إذا كانت قد نُفذت بالمخالفة للقانون. فالسجل المفصل قد يثبت بدقة أن إجراءً معيناً قد تم، لكنه لا يثبت بالضرورة أن الجهة كانت مختصة أو أن الإذن اللازم قد صدر. [150]

كما لا يعني اكتمال المحضر أن النتيجة الفنية صحيحة؛ فقد يوثق القائم بالفحص جميع خطواته بدقة، لكنه يستخدم أداة غير مناسبة أو يفسر البيانات تفسيراً خاطئاً. [151]

وتدعم المعايير الفنية المتعلقة بالتعامل مع الأدلة الرقمية هذا الاتجاه من خلال التركيز على إجراءات يمكن تتبعها ومراجعتها. [152] كما أن الإرشادات المهنية الخاصة بفحص الأدلة الرقمية تؤكد أهمية توثيق الإجراءات الفنية. [153]

وعليه، فإن التوثيق الفعال لا يقوم على كثرة التفاصيل وحدها، بل على تسجيل المعلومات التي تمكن من إعادة بناء مسار التحري وفهم القرارات المؤثرة في نتائجه. [154]

المطلب الثاني: التمييز بين محضر التحري الأمني والتقرير الأمني والتقارير الفني

يقتضي التنظيم العلمي للتحريات الأمنية الرقمية التمييز بين محضر التحري الأمني والتقارير الأمني والتقارير الفني؛ لأن لكل وثيقة وظيفة مختلفة، ونطاقاً خاصاً للمعلومات، ومستوى معيناً من التحليل والاستنتاج. [155]

أولاً: محضر التحري الأمني. وثيقة تُثبت الإجراءات والوقائع والمعلومات التي جُمعت أثناء التحري، مع بيان مصادرها وظروف الحصول عليها. وتتمثل وظيفته الأساسية في تسجيل ما قام به القائم بالتحري وما أمكنه التوصل إليه. ويُفترض أن يوضح موضوع التحري، وتاريخه، والجهة القائمة به، والسند القانوني، والإجراءات المتخذة، والمعلومات التي تم جمعها، ومصادرها، وما إذا كانت قد خضعت للتحقق. [156]

ولا ينبغي أن يتحول المحضر إلى مساحة لإطلاق أحكام قطعية بشأن المسؤولية أو الإدانة، خصوصاً عندما تكون المعلومات في مرحلة أولية. فوظيفته إثبات إجراءات التحري، لا استبدال عمل جهات التحقيق أو القضاء. [157]

ثانياً: التقرير الأمني. وثيقة تحليلية تعرض المعلومات التي جُمعت وتُقيّم صلتها بالموضوع، وتبين أوجه الاتساق والتعارض بينها، وتعرض الاستنتاجات التي يمكن استخلاصها. ويختلف عن المحضر في أن وظيفته لا تقتصر على تسجيل الإجراءات، بل تشمل تنظيم المعلومات وتحليلها. [158]

ويجب أن يحدد التقرير الأمني المسألة محل التحري، ومصادر المعلومات، ودرجة موثوقية كل مصدر، والوقائع التي أمكن التحقق منها، والفرضيات التي لا تزال بحاجة إلى اختبار، والقيود التي تؤثر في التقييم. [159]

ثالثاً: التقرير الفني. وثيقة يحررها مختص في ضوء فحص تقني محدد، ويهدف إلى بيان البيانات محل الفحص، والمنهج والأدوات المستخدمة، والإجراءات المنفذة، والنتائج الفنية، والقيود التي واجهت الفحص. [160]

ويجب أن يتضمن التقرير الفني وصفاً للبيانات التي فُحصت، ومصادرها، وطريقة الحصول عليها، والإجراءات التي اتُبعت للتحقق من سلامتها، والأدوات المستخدمة وإصداراتها، والنتائج التي أمكن الوصول إليها، وحدود ما تثبته هذه النتائج. [161]

ويجب أن يظل التقرير الفني ضمن نطاق الاختصاص المهني لمحرره. فإذا كشف الفحص عن ملف يحتوي على بيانات زمنية أو عن سجل يرتبط بحساب إلكتروني، جاز للتقرير وصف هذه

البيانات وبيان دلالتها التقنية، لكنه لا ينبغي أن يجزم، دون سند إضافي، بأن شخصاً معيناً ارتكب فعلاً مجرمًا. [162]

جدول الفروق:

التقرير الفني	التقرير الأمني	محضر التحري الأمني	وجه المقارنة
فحص البيانات وبيان النتائج التقنية	تحليل المعلومات وتقييم دلالتها	إثبات الإجراءات والمعلومات المجموعة	الوظيفة الأساسية
بيانات وإجراءات فنية ونتائج قابلة للمراجعة	معلومات وتحليل واستنتاجات مبررة	وقائع وإجراءات ومصادر	طبيعة المحتوى
الفحص الفني والاختبارات التقنية	تجميع المصادر وتقييمها وربطها	أعمال التحري والمعلومات الواردة	مصدر المعرفة
اختبار المسائل الفنية المحددة	اختبار الفرضيات ومقارنة التفسيرات	تسجيل الفرضيات الأولية	التعامل مع الفرضيات
لا يتجاوز النتائج الفنية إلى أحكام قانونية	يعرض تقديرًا تحليليًا	لا يحسم المسؤولية القانونية	حدود الاستنتاج
الأدوات والخطوات والبيانات والقيود الفنية	إسناد الاستنتاجات إلى مصادرها	وقت الإجراء والقائمون به والمصادر	متطلبات التوثيق

ولا يمنع هذا التمييز من وجود صلة وثيقة بين الوثائق الثلاث؛ فقد يستند التقرير الأمني إلى محضر تحري وتقارير فنية متعددة. لكن هذه الصلة لا تبرر دمج الوظائف أو إسقاط متطلبات التوثيق الخاصة بكل وثيقة. [163]

كما ينبغي مراعاة أن الأسماء الرسمية لهذه الوثائق واختصاصات محرريها قد تختلف من دولة إلى أخرى. ولذلك، فإن هذا التمييز ذو طبيعة منهجية عامة، ولا يغني عن الرجوع إلى التشريعات واللوائح المؤسسية. [164]

المطلب الثالث: عرض النتائج وإسنادها إلى مصادرها

يُعد عرض النتائج وإسنادها إلى مصادرها من المتطلبات الأساسية للتقارير؛ لأن النتيجة التي لا يُعرف مصدرها أو الأساس الذي استُخلصت منه لا تتيح مراجعة مستقلة. [165]

ويقصد بإسناد النتيجة إلى مصدرها بيان العلاقة بين الاستنتاج والمعلومات التي تدعمه، بحيث يستطيع القارئ تحديد البيانات أو السجلات أو الإجراءات التي بُني عليها الاستنتاج. ولا يقتصر ذلك على ذكر مصدر عام، مثل "السجلات الإلكترونية"، بل يتطلب تحديدًا كافيًا لطبيعة المصدر وتاريخه ونطاقه. [166]

وينبغي أن يبدأ عرض النتائج ببيان الوقائع التي أمكن التحقق منها، مع وصف أساس التحقق. ثم تُعرض الاستنتاجات المستخلصة، مع بيان ما إذا كانت مباشرة أو غير مباشرة، وما إذا كانت تدعمها مصادر متعددة أو تعتمد على مصدر واحد. [167]

فإذا كشف التحليل عن وجود سجل رقمي يحمل توقيتاً معيناً، فإن النتيجة المباشرة هي وجود السجل بهذه البيانات في النسخة التي خضعت للفحص. أما القول بأن النشاط الذي يسجله قد وقع بالفعل في ذلك الوقت، فيتطلب التحقق من مصدر التوقيت وإعدادات النظام. والقول بأن شخصاً محدداً هو الذي نفذ النشاط يتطلب، فوق ذلك، أدلة تدعم نسبة الفعل إليه. [168]

ويبين هذا المثال أن صياغة النتيجة يجب أن تتناسب مع قوة البيانات. فليس من الدقة استخدام عبارة "ثبت أن" عندما لا تدعم المعطيات سوى احتمال أو مؤشر. [169]

كما ينبغي أن يتضمن التقرير إحالات داخلية أو معرفات واضحة تربط كل نتيجة بالملف أو السجل أو الصورة أو الإجراء الذي تستند إليه. وإذا تضمنت المرفقات عدداً كبيراً من البيانات، فمن المهم تنظيمها وترقيمها. [170]

ويجب مراعاة استقلال المصادر عند عرض النتائج. فقد تبدو المعلومة مدعومة بعدة مصادر، بينما تكون هذه المصادر قد نقلت جميعاً عن مصدر واحد. وفي هذه الحالة، لا يُعد تعدد النشرات دليلاً على التحقق المستقل. [171]

وفي المقابل، قد تتفق مصادر مستقلة على بعض عناصر الواقعة دون أن تتفق على جميع تفاصيلها. وهنا ينبغي تحديد نطاق الاتفاق والاختلاف، وتجنب دمج المعلومات في رواية واحدة تتجاوز ما تدعمه المصادر. [172]

ويقتضي عرض النتائج أيضاً الإفصاح عن المعلومات التي تعارض الاستنتاج الأساسي، أو عن الفرضيات البديلة التي لم يمكن استبعادها. فالتقرير الذي يعرض المؤشرات المؤيدة فقط قد يعطي انطباعاً مضللاً بقوة النتيجة. [173]

ويجب كذلك بيان حدود الفحص. فإذا لم يتمكن القائم بالفحص من الوصول إلى المصدر الأصلي، أو تعذر التحقق من تاريخ الإنشاء، أو كانت بعض البيانات ناقصة، وجب الإفصاح عن هذه القيود. [174]

ولا ينبغي تفسير الإفصاح عن القيود على أنه انتقاص من قيمة التقرير؛ إذ قد تكون النتيجة قوية في نطاق محدد رغم تعذر حسم مسائل أخرى. والدقة تقتضي تأكيد ما ثبت، مع بيان ما لم يثبت. [175]

ومن المهم التمييز بين النتائج الفنية والتقييم القانوني. فقد يقرر التقرير الفني أن البيانات متطابقة مع نسخة مرجعية، أو أن سجلاً يتضمن وقتاً معيناً. أما تحديد ما إذا كان الحصول على هذه البيانات مشروطاً، أو ما إذا كانت كافية لإثبات واقعة قانونية، فيتطلب الرجوع إلى القواعد القانونية. [176]

وفي التقارير الموجهة إلى جهات التحقيق أو القضاء، ينبغي أن تكون اللغة واضحة وخالية من المصطلحات الفنية غير المفسرة. كما ينبغي تجنب استخدام النسب أو الدرجات الرقمية للثقة دون بيان أساسها المنهجي. [177]

وتتطلب الأمانة العلمية التمييز بين ما توصل إليه الفاحص بنفسه وما نقله عن تقرير آخر. فإذا استند التقرير إلى نتيجة فنية سابقة، فينبغي تحديد مصدرها ونطاقها. [178]

وعليه، فإن عرض النتائج بطريقة منضبطة يقتضي ربط كل استنتاج بمصدره، وتوضيح درجة التحقق، والإفصاح عن القيود والفرضيات البديلة، والفصل بين الوقائع والتفسيرات والأحكام القانونية. [179]

المطلب الرابع: بيان القيود الفنية ومواطن عدم اليقين وتصحيح الأخطاء

لا تكتمل موثوقية التقرير الأمني أو الفني بمجرد عرض النتائج، بل تتطلب بيان القيود التي أحاطت بالعمل ومواطن عدم اليقين. كما تقتضي النزاهة المهنية وضع آلية واضحة لتصحيح الأخطاء المكتشفة. [180]

ويقصد بالـ**القيود الفنية** العوامل التي تحد من قدرة الإجراءات أو الأدوات المستخدمة على اكتشاف المعلومات أو تفسيرها أو التحقق منها. وقد ترتبط بطبيعة الجهاز أو النظام، أو بنقص البيانات، أو بوجود تشفير، أو بقدم السجلات، أو بعدم توافر المصدر الأصلي، أو بمحدودية الأداة. [181]

أما **عدم اليقين**، فيشير إلى حدود المعرفة المتاحة بشأن مسألة معينة، سواء تعذر التحقق منها بصورة قاطعة، أو بقيت عدة تفسيرات متوافقة مع البيانات. ولا يعني وجود عدم يقين أن جميع النتائج متساوية في القوة، بل يعني ضرورة تحديد ما تسمح الأدلة بإثباته. [182]

ثلاثة مستويات من القيود:

١. **قيود تتعلق بالمصدر:** تعذر تحديد المنشئ الأصلي، أو عدم توافر معلومات كافية عن الجهة التي قدمت البيانات. [183]

٢. **قيود تتعلق بالإجراء الفني:** تعذر استخراج بعض البيانات، أو عدم إمكان إعادة الفحص بالأداة نفسها. [184]

٣. **قيود تتعلق بالتفسير:** احتمال أن يعكس التوقيت إعدادًا غير دقيق للساعة، أو أن تكون البيانات متوافقة مع أكثر من فرضية. [185]

ويؤثر كل مستوى في نوع النتيجة التي يمكن استخلاصها. فقد تكون البيانات محفوظة بصورة سليمة، لكن مصدرها غير معلوم. وقد يكون مصدرها معروفًا، لكن الفحص لم يشمل جميع عناصرها. [186]

ويقتضي بيان القيود توضيح طبيعتها وأسبابها وأثرها المحتمل في النتائج. فإذا تعذر التحقق من ساعة الجهاز، فينبغي بيان أثر ذلك في الاستنتاجات الزمنية، لا الاكتفاء بذكر أن هناك مشكلة تقنية. [187]

كما ينبغي الفصل بين القيود التي أمكن معالجتها والقيود التي بقيت قائمة. فقد يؤدي استخدام مصدر مستقل إلى التحقق من جزء من المعلومات، بينما يظل جزء آخر غير محسوم. [188]

ويُعد الإفصاح عن الفرضيات البديلة جزءاً من بيان القيود. فإذا أمكن تفسير البيانات على أكثر من وجه، وجب توضيح البدائل التي لها أساس معقول، وبيان ما إذا كانت الأدلة المتاحة تدعم أحدها بدرجة أقوى. [189]

وتظهر أهمية ذلك في تحليل بيانات الموقع، حيث قد تدعم البيانات وجود جهاز في نطاق جغرافي معين، لكنها لا تثبت بالضرورة أن شخصاً محدداً كان يحمله. ويقتضي الاستنتاج السليم بيان دقة وسيلة تحديد الموقع، والفترة الزمنية، والقيود المرتبطة باستخدام الجهاز. [190]

أما **تصحيح الأخطاء**، فينبغي أن يخضع لإجراءات تحفظ سلامة السجل وتتيح معرفة طبيعة الخطأ وأثره. فقد يكون الخطأ لغوياً لا يؤثر في المعنى، أو خطأ في نقل رقم أو توقيت، أو خطأ فني يؤثر في النتيجة، أو خطأ في الاستنتاج يتطلب إعادة تقييم. [191]

وفي جميع الحالات، ينبغي تحديد موضع الخطأ، وتوثيق اكتشافه، وبيان مصدر التصحيح، وتاريخه، والشخص الذي أجراه، وأثره في النتائج السابقة. ولا يجوز حذف النسخة السابقة من التقرير أو استبدالها دون الاحتفاظ بما يسمح بتتبع التغيير. [192]

وإذا كان الخطأ **جوهرياً**، فقد يقتضي الأمر إعادة الفحص أو مراجعة التقرير من قبل مختص آخر، وتحديد الجهات التي ينبغي إبلاغها بالتصحيح. كما ينبغي إعادة تقييم الاستنتاجات التي تأثرت به. [193]

وتزداد أهمية هذه الضوابط عند استخدام **الأنظمة الآلية**؛ لأن الخطأ قد ينشأ من إعداد غير مناسب، أو من قصور في البيانات المدخلة، أو من حدود الخوارزمية. ولا يكفي في هذه الحالات القول إن البرنامج أنتج النتيجة، بل يجب التحقق من صلاحية المدخلات وطريقة التشغيل. [194]

ومن الناحية المهنية، لا ينبغي اعتبار الاعتراف بالخطأ دليلاً على عدم الكفاءة بالضرورة؛ فقد يكون اكتشاف الخطأ وتصحيحه بصورة موثقة علامة على فعالية نظام المراجعة. أما إخفاء الخطأ أو التقليل من أثره دون تحليل، فيقوض الثقة في التقرير. [195]

ويجب أن يظل **الأثر القانوني للخطأ** منفصلاً عن التقييم الفني. فقد يكون الخطأ قابلاً للتصحيح دون أن يمس جوهر النتيجة، وقد يؤدي إلى إضعاف دلالتها، وقد تكون له آثار إجرائية يحددها القانون المختص. [196]

وعليه، فإن بيان القيود وعدم اليقين وتصحيح الأخطاء يمثل عنصراً جوهرياً في جودة العمل الأمني الرقمي. فالتقرير الموثوق ليس التقرير الذي يخلو ظاهرياً من الشك، بل التقرير الذي يحدد بوضوح ما أمكن إثباته، وما بقي غير محسوم، وكيف أثرت القيود في النتائج، وما اتخذ من إجراءات عند اكتشاف الخطأ. [197]

الجدول المقارن: الوثائق الثلاث في التحري الرقمي

المعيار	التقرير الأمني	التقرير الفني	محضر التحري
الهدف	تحليل المعلومات وتقييم دلالتها	فحص البيانات وبيان النتائج التقنية	إثبات الإجراءات والمعلومات
المحرر	محلل أمني	خبير فني	ضابط التحري
المحتوى	تحليل، استنتاجات، فرضيات	بيانات، أدوات، نتائج فنية	وقائع، مصادر، إجراءات
اللغة	تحليلية مع درجة ثقة	تقنية مع حدود واضحة	وصفية دقيقة
حُدود الاستنتاج	تقدير تحليلي	نتائج فنية لا تتجاوز الاختصاص	لا يحسم المسؤولية
التوثيق	إسناد إلى مصادر	أدوات، إصدارات، قيود	وقت، هوية، مصدر

❖ النافذة التطبيقية

السيناريو: واقعة تهريب عبر طائرة مسيرة، ضبط جهاز تحكم وأرسل إلى المختبر، مع تسجيلات كاميرا مراقبة.

- **الخطوة الأولى (المصدر):** تحديد جهاز التحكم، وتوثيق حالته عند الضبط، وإرساله إلى المختبر بموجب سلسلة عهدة موثقة (استلام، نقل، حفظ).
- **الخطوة الثانية (المحافظة على الأصل):** إنشاء نسخة جنائية من جهاز التحكم، والتحقق من قيم التجزئة قبل وبعد النسخ.
- **الخطوة الثالثة (الفحص الفني):** استخراج سجلات الطيران وبيانات GPS ، وتوثيق الأداة وإصدارها والإعدادات.
- **الخطوة الرابعة (التاريخ والاكتمال):** التحقق من توقيت سجلات الطيران مقارنة بتوقيت الكاميرا، مع توثيق المنطقة الزمنية.
- **الخطوة الخامسة (التقرير الفني):** عرض النتائج الفنية (مسار الطائرة، وقت الإقلاع) دون الجزم بهوية المشغل.
- **الخطوة السادسة (التقرير الأمني):** ربط نتائج التقرير الفني بتسجيلات الكاميرا وسجلات أخرى، مع الإفصاح عن القيود (مثلاً: "لم يتسن التحقق من هوية مشغل الطائرة").
- **الدرس:** التمييز بين الوثائق الثلاث يمنع انتقال الاستنتاج من المستوى الفني إلى المستوى القانوني دون أساس، ويضمن قابلية المراجعة.

النتائج العامة للفصل

١. تحديد مصدر البيانات الرقمية يميز بين المصدر المنشئ والمصدر المستخرج منه والمصدر الذي أتاحتها.
٢. نسبة البيانات إلى جهاز أو حساب لا تثبت تلقائياً نسبة الفعل إلى شخص محدد.
٣. التحقق الزمني يتطلب التمييز بين تواريخ الإنشاء والتعديل والنشر والحصول، وتوثيق المنطقة الزمنية.
٤. اكتمال البيانات عنصر مستقل عن سلامتها؛ فالمادة السليمة قد تكون ناقصة السياق.
٥. المحافظة على البيانات الأصلية تتطلب التمييز بين البيانات المستلمة والنسخة المحفوظة ونسخة العمل.
٦. قيم التجزئة تثبت سلامة النسخة، لا أصالة المصدر ولا صحة المضمون.
٧. سلسلة العهدة أداة لتتبع المسار والمساءلة، لا شهادة مطلقة بصحة البيانات.
٨. توثيق الاستلام والنقل والحفظ والوصول شرط لقابلية المراجعة.
٩. توثيق الأدوات وإصداراتها وخطوات المعالجة ضروري لإعادة الفحص.
١٠. النقص في سلسلة العهدة قد يكون شكلياً أو جوهرياً، ويجب تقييم أثره الفني والقانوني بشكل منفصل.
١١. قابلية إعادة الفحص والتحقق المستقل مؤشر على جودة العمل الفني.
١٢. التمييز بين محضر التحري والتقرير الأمني والتقرير الفني ضروري لمنع الخلط بين الوظائف.
١٣. عرض النتائج يتطلب إسناد كل استنتاج إلى مصدره، والفصل بين الوقائع والتفسيرات.
١٤. الإفصاح عن القيود وعدم اليقين شرط للموضوعية، وليس ضعفاً في التقرير.
١٥. تصحيح الأخطاء يتطلب توثيقاً يحفظ سلامة السجل ويتيح تتبع التغيير.

المراجع:

- (1) انظر: عادل عبد العال خراشي، ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي، ٢٠٠٦، ص ١٢٠-١٢٥.
- (2) انظر- Kent et al., Guide to Integrating Forensic Techniques into Incident Response, NIST SP 800-86, 2006, p. 4-1.
- (3) انظر: هشام مصطفى محمد، التحريات الأمنية وأثرها في الأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٥، ص ١٨٠-١٨٥.
- (4) انظر: محمد محمد سيف شجاع، شرح قانون الإجراءات الجزائية اليمني، مكتبة الصادق، صنعاء، ٢٠٠٥، الفصل الخاص بالتحريات.

- (5) انظر. NIST SP 800-86, supra note 2, p. 4-2.
- (6) انظر: خراشي، مرجع سابق، ص ١٣٠-١٣٥.
- (7) انظر: هشام مصطفى، مرجع سابق، ص ١٩٠-١٩٥.
- (8) انظر. NIST SP 800-86, supra note 2, p. 4-3.
- (9) انظر: خراشي، مرجع سابق، ص ١٤٠-١٤٥.
- (10) انظر: شجاع، مرجع سابق.
- (11) انظر: هشام مصطفى، مرجع سابق، ص ٢٠٠-٢٠٥.
- (12) انظر. Berkeley Protocol on Digital Open Source Investigations, 2022, pp. 70-75.
- (13) انظر. NIST SP 800-86, supra note 2, p. 3-1.
- (14) انظر : ISO/IEC 27037:2012, Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, 2012.
- (15) انظر: خراشي، مرجع سابق، ص ١٥٠-١٥٥.
- (16) انظر: هشام مصطفى، مرجع سابق، ص ٢١٠-٢١٥.
- (17) انظر: شجاع، مرجع سابق.
- (18) انظر. NIST SP 800-86, supra note 2, p. 3-2.
- (19) انظر: المرجع السابق، ص ٣-٣.
- (20) انظر: المرجع السابق، ص ٣-٤.
- (21) انظر: المرجع السابق، ص ٣-٥.
- (22) انظر: المرجع السابق، ص ٣-٦.
- (23) انظر: المرجع السابق، ص ٣-٧.
- (24) انظر: هشام مصطفى، مرجع سابق، ص ٢٢٠-٢٢٥.
- (25) انظر. NIST SP 800-86, supra note 2, p. 3-8.
- (26) انظر: المرجع السابق، ص ٣-٩.
- (27) انظر: خراشي، مرجع سابق، ص ١٦٠-١٦٥.
- (28) انظر. NIST SP 800-86, supra note 2, p. 3-10.
- (29) انظر: هشام مصطفى، مرجع سابق، ص ٢٣٠-٢٣٥.
- (30) انظر: المرجع السابق، ص ٢٣٥-٢٤٠.
- (31) انظر. NIST SP 800-86, supra note 2, p. 3-11.
- (32) انظر: المرجع السابق، ص ٤-٤.
- (33) انظر: شجاع، مرجع سابق.
- (34) انظر: خراشي، مرجع سابق، ص ١٧٠-١٧٥.
- (35) انظر. NIST SP 800-86, supra note 2, p. 4-5.
- (36) انظر: هشام مصطفى، مرجع سابق، ص ٢٤٠-٢٤٥.
- (37) انظر: المرجع السابق، ص ٢٤٥-٢٥٠.
- (38) انظر. NIST SP 800-86, supra note 2, p. 4-6.
- (39) انظر: المرجع السابق، ص ٤-٧.
- (40) انظر: خراشي، مرجع سابق، ص ١٨٠-١٨٥.
- (41) انظر. Ayers et al., Guidelines on Mobile Device Forensics, NIST SP 800-101 Rev. 1, 2014, p. 2-1.
- (42) انظر: المرجع السابق، ص ٢-٢.
- (43) انظر. NIST SP 800-86, supra note 2, p. 4-8.
- (44) انظر. Ayers et al., supra note 41, p. 2-3.
- (45) انظر: شجاع، مرجع سابق.
- (46) انظر: خراشي، مرجع سابق، ص ١٩٠-١٩٥.
- (47) انظر. NIST SP 800-86, supra note 2, p. 4-9.
- (48) انظر: هشام مصطفى، مرجع سابق، ص ٢٥٠-٢٥٥.
- (49) انظر: المرجع السابق، ص ٢٥٥-٢٦٠.
- (50) انظر. NIST, Secure Hash Standard (SHS), FIPS PUB 180-4, 2015.
- (51) انظر. NIST SP 800-86, supra note 2, p. 4-10.
- (52) انظر: هشام مصطفى، مرجع سابق، ص ٢٦٠-٢٦٥.

- (53) انظر: المرجع السابق، ص ٢٦٥-٢٧٠.
- (54) انظر: خراشي، مرجع سابق، ص ٢٠٠-٢٠٥.
- (55) انظر: شجاع، مرجع سابق.
- (56) انظر. NIST SP 800-86, supra note 2, p. 4-11.
- (57) انظر: المرجع السابق، ص ١٢-٤.
- (58) انظر. NIST, Secure Hash Standard, supra note 50.
- (59) انظر. NIST SP 800-86, supra note 2, p. 4-13.
- (60) انظر: المرجع السابق، ص ١٤-٤.
- (61) انظر. Berkeley Protocol, supra note 12, pp. 170-175.
- (62) انظر. NIST SP 800-86, supra note 2, p. 4-15.
- (63) انظر: شجاع، مرجع سابق.
- (64) انظر. NIST SP 800-86, supra note 2, p. 4-16.
- (65) انظر. ISO/IEC 27037:2012, supra note 14.
- (66) انظر. INTERPOL, Guidelines for Digital Forensics First Responders, pp. 10-12.
- (67) انظر: المرجع السابق، ص ١٢-١٥.
- (68) انظر: هشام مصطفى، مرجع سابق، ص ٢٧٠-٢٧٥.
- (69) انظر. INTERPOL, supra note 66, pp. 15-18.
- (70) انظر: المرجع السابق، ص ١٨-٢٠.
- (71) انظر. NIST SP 800-86, supra note 2, p. 4-17.
- (72) انظر: المرجع السابق، ص ١٨-٤.
- (73) انظر: خراشي، مرجع سابق، ص ٢١٠-٢١٥.
- (74) انظر: هشام مصطفى، مرجع سابق، ص ٢٧٥-٢٨٠.
- (75) انظر: شجاع، مرجع سابق.
- (76) انظر. ISO/IEC 27037:2012, supra note 14.
- (77) انظر. INTERPOL, supra note 66, pp. 20-22.
- (78) انظر: المرجع السابق، ص ٢٢-٢٥.
- (79) انظر. NIST SP 800-86, supra note 2, p. 4-19.
- (80) انظر: خراشي، مرجع سابق، ص ٢٢٠-٢٢٥.
- (81) انظر: هشام مصطفى، مرجع سابق، ص ٢٨٠-٢٨٥.
- (82) انظر. INTERPOL, supra note 66, pp. 25-28.
- (83) انظر: المرجع السابق، ص ٢٨-٣٠.
- (84) انظر. NIST SP 800-86, supra note 2, p. 4-20.
- (85) انظر. INTERPOL, supra note 66, pp. 30-32.
- (86) انظر: المرجع السابق، ص ٣٢-٣٥.
- (87) انظر. NIST SP 800-86, supra note 2, p. 4-21.
- (88) انظر. Ayers et al., supra note 41, p. 2-4.
- (89) انظر: المرجع السابق، ص ٢-٥.
- (90) انظر. NIST SP 800-86, supra note 2, p. 4-22.
- (91) انظر: شجاع، مرجع سابق.
- (92) انظر. INTERPOL, supra note 66, pp. 35-38.
- (93) انظر. NIST SP 800-86, supra note 2, p. 4-23.
- (94) انظر: خراشي، مرجع سابق، ص ٢٣٠-٢٣٥.
- (95) انظر: هشام مصطفى، مرجع سابق، ص ٢٨٥-٢٩٠.
- (96) انظر. NIST SP 800-86, supra note 2, p. 4-24.
- (97) انظر: المرجع السابق، ص ٢٥-٤.
- (98) انظر. INTERPOL, supra note 66, pp. 38-40.
- (99) انظر. NIST SP 800-86, supra note 2, p. 4-26.
- (100) انظر: المرجع السابق، ص ٢٧-٤.
- (101) انظر. INTERPOL, supra note 66, pp. 40-42.

- (102) انظر. NIST SP 800-86, supra note 2, p. 4-28.
- (103) انظر. Berkeley Protocol, supra note 12, pp. 215–220.
- (104) انظر. NIST SP 800-86, supra note 2, p. 4-29.
- (105) انظر. Ayers et al., supra note 41, p. 2-6.
- (106) انظر. NIST SP 800-86, supra note 2, p. 4-30.
- (107) انظر: المرجع السابق، ص ٣١-٤.
- (108) انظر: المرجع السابق، ص ٣٢-٤.
- (109) انظر. INTERPOL, supra note 66, pp. 42–45.
- (110) انظر: خراشي، مرجع سابق، ص ٢٤٠-٢٤٥.
- (111) انظر. NIST SP 800-86, supra note 2, p. 4-33.
- (112) انظر. INTERPOL, supra note 66, pp. 45–48.
- (113) انظر. NIST SP 800-86, supra note 2, p. 4-34.
- (114) انظر: خراشي، مرجع سابق، ص ٢٥٠-٢٥٥.
- (115) انظر. INTERPOL, supra note 66, pp. 48–50.
- (116) انظر. NIST SP 800-86, supra note 2, p. 4-35.
- (117) انظر: هشام مصطفى، مرجع سابق، ص ٢٩٠-٢٩٥.
- (118) انظر: خراشي، مرجع سابق، ص ٢٦٠-٢٦٥.
- (119) انظر. INTERPOL, supra note 66, pp. 50–52.
- (120) انظر. NIST SP 800-86, supra note 2, p. 4-36.
- (121) انظر: المرجع السابق، ص ٣٧-٤.
- (122) انظر. Berkeley Protocol, supra note 12, pp. 350–355.
- (123) انظر: شجاع، مرجع سابق.
- (124) انظر: خراشي، مرجع سابق، ص ٢٧٠-٢٧٥.
- (125) انظر. INTERPOL, supra note 66, pp. 52–55.
- (126) انظر. NIST SP 800-86, supra note 2, p. 4-38.
- (127) انظر: المرجع السابق، ص ٣٩-٤.
- (128) انظر. INTERPOL, supra note 66, pp. 55–58.
- (129) انظر. NIST SP 800-86, supra note 2, p. 4-40.
- (130) انظر: المرجع السابق، ص ٤١-٤.
- (131) انظر. Berkeley Protocol, supra note 12, pp. 360–365.
- (132) انظر: شجاع، مرجع سابق.
- (133) انظر. NIST SP 800-86, supra note 2, p. 4-42.
- (134) انظر: المرجع السابق، ص ٤٣-٤.
- (135) انظر: هشام مصطفى، مرجع سابق، ص ٣٠٠-٣٠٥.
- (136) انظر. Berkeley Protocol, supra note 12, pp. 370–375.
- (137) انظر: شجاع، مرجع سابق.
- (138) انظر. NIST SP 800-86, supra note 2, p. 4-44.
- (139) انظر: المرجع السابق، ص ٤٥-٤.
- (140) انظر: خراشي، مرجع سابق، ص ٢٨٠-٢٨٥.
- (141) انظر. INTERPOL, supra note 66, pp. 58–60.
- (142) انظر. NIST SP 800-86, supra note 2, p. 5-1.
- (143) انظر: المرجع السابق، ص ٢-٥.
- (144) انظر. INTERPOL, supra note 66, pp. 60–62.
- (145) انظر. NIST SP 800-86, supra note 2, p. 5-3.
- (146) انظر: هشام مصطفى، مرجع سابق، ص ٣١٠-٣١٥.
- (147) انظر. Berkeley Protocol, supra note 12, pp. 225–230.
- (148) انظر: خراشي، مرجع سابق، ص ٢٩٠-٢٩٥.
- (149) انظر. NIST SP 800-86, supra note 2, p. 5-4.
- (150) انظر: شجاع، مرجع سابق.

- (151) انظر: خراشي، مرجع سابق، ص ٣٠٠-٣٠٥.
- (152) انظر. ISO/IEC 27037:2012, supra note 14.
- (153) انظر. NIST SP 800-86, supra note 2, p. 5-5.
- (154) انظر. INTERPOL, supra note 66, pp. 62-65.
- (155) انظر: هشام مصطفى، مرجع سابق، ص ٣٢٠-٣٢٥.
- (156) انظر: شجاع، مرجع سابق.
- (157) انظر: خراشي، مرجع سابق، ص ٣١٠-٣١٥.
- (158) انظر. Berkeley Protocol, supra note 12, pp. 240-245.
- (159) انظر: المرجع السابق، ص ٢٤٥-٢٥٠.
- (160) انظر. NIST SP 800-86, supra note 2, p. 5-6.
- (161) انظر: المرجع السابق، ص ٥-٧.
- (162) انظر: خراشي، مرجع سابق، ص ٣٢٠-٣٢٥.
- (163) انظر: هشام مصطفى، مرجع سابق، ص ٣٣٠-٣٣٥.
- (164) انظر: شجاع، مرجع سابق.
- (165) انظر. Berkeley Protocol, supra note 12, pp. 260-265.
- (166) انظر: المرجع السابق، ص ٢٦٥-٢٧٠.
- (167) انظر. NIST SP 800-86, supra note 2, p. 5-8.
- (168) انظر: هشام مصطفى، مرجع سابق، ص ٣٤٠-٣٤٥.
- (169) انظر: خراشي، مرجع سابق، ص ٣٣٠-٣٣٥.
- (170) انظر. NIST SP 800-86, supra note 2, p. 5-9.
- (171) انظر. Berkeley Protocol, supra note 12, pp. 275-280.
- (172) انظر: المرجع السابق، ص ٢٨٠-٢٨٥.
- (173) انظر: هشام مصطفى، مرجع سابق، ص ٣٥٠-٣٥٥.
- (174) انظر. NIST SP 800-86, supra note 2, p. 5-10.
- (175) انظر: خراشي، مرجع سابق، ص ٣٤٠-٣٤٥.
- (176) انظر: شجاع، مرجع سابق.
- (177) انظر. Berkeley Protocol, supra note 12, pp. 290-295.
- (178) انظر: هشام مصطفى، مرجع سابق، ص ٣٦٠-٣٦٥.
- (179) انظر. NIST SP 800-86, supra note 2, p. 5-11.
- (180) انظر. Berkeley Protocol, supra note 12, pp. 350-355.
- (181) انظر. NIST SP 800-86, supra note 2, p. 5-12.
- (182) انظر: خراشي، مرجع سابق، ص ٣٥٠-٣٥٥.
- (183) انظر: هشام مصطفى، مرجع سابق، ص ٣٧٠-٣٧٥.
- (184) انظر. NIST SP 800-86, supra note 2, p. 5-13.
- (185) انظر. Berkeley Protocol, supra note 12, pp. 360-365.
- (186) انظر: المرجع السابق، ص ٣٦٥-٣٧٠.
- (187) انظر. NIST SP 800-86, supra note 2, p. 5-14.
- (188) انظر: خراشي، مرجع سابق، ص ٣٦٠-٣٦٥.
- (189) انظر. Berkeley Protocol, supra note 12, pp. 370-375.
- (190) انظر: المرجع السابق، ص ٣٧٥-٣٨٠.
- (191) انظر. NIST SP 800-86, supra note 2, p. 5-15.
- (192) انظر: المرجع السابق، ص ٥-١٦.
- (193) انظر: هشام مصطفى، مرجع سابق، ص ٣٨٠-٣٨٥.
- (194) انظر. Berkeley Protocol, supra note 12, pp. 385-390.
- (195) انظر: خراشي، مرجع سابق، ص ٣٧٠-٣٧٥.
- (196) انظر: شجاع، مرجع سابق.
- (197) انظر. NIST SP 800-86, supra note 2, p.

الفصل الثاني: القيمة القانونية والاستدلالية للمعلومات الرقمية

المبحث الأول: مشروعية الحصول على المعلومات وأثرها القانوني

المطلب الأول: أثر مشروعية الجمع في إمكان الاستناد إلى المعلومات

تُعد مشروعية الحصول على المعلومات الرقمية نقطة الانطلاق في تحديد إمكان الاستناد إليها في المجال الأمني أو الاحتجاج بها أمام جهات التحقيق والقضاء؛ إذ لا يكفي أن تكون المعلومة صحيحة من الناحية الواقعية أو سليمة من الناحية الفنية حتى تكتسب صلاحية قانونية غير مشروطة. فقد تكون البيانات مطابقة لما كان محفوظاً في جهاز إلكتروني، ومع ذلك يكون الحصول عليها قد تم من خلال إجراء تجاوز الاختصاص القانوني للجهة القائمة به، أو انتهاك حقاً يحميه القانون، أو خالف الشروط التي يتطلبها الإذن الصادر بإجرائه.[1]

ويكشف ذلك عن ضرورة التمييز بين ثلاثة مستويات متميزة في تقييم المعلومات الرقمية: مشروعية الحصول عليها، وسلامتها الفنية، وقيمتها الاستدلالية. يتعلق المستوى الأول بمدى توافق الإجراء مع القواعد القانونية الواجبة التطبيق، بينما ينصرف الثاني إلى التحقق من أصالة البيانات وعدم تعرضها لتغيير غير موثق، ويتصل الثالث بمدى قدرة المعلومات، في ضوء مصدرها وسياقها والقرائن الأخرى، على دعم استنتاج معين. وهذه المستويات متكاملة، لكنها ليست مترادفة؛ فسلامة البيانات لا تصحح بذاتها عدم مشروعية الحصول عليها، كما أن مشروعية الجمع لا تثبت وحدها صحة الاستنتاج المستخلص منها.[2]

ويتفق هذا التمييز مع الاتجاه العام الذي تتبناه الأدبيات الدولية المتعلقة بالأدلة الإلكترونية، التي تجعل مشروعية التفتيش أو الحصول على البيانات، إلى جانب أصالتها وسلامتها وموثوقيتها، عناصر مستقلة ينبغي التحقق منها عند تقييم صلاحيتها للاستخدام القضائي. ويؤكد مكتب الأمم المتحدة المعني بالمخدرات والجريمة أن تقييم قبول الأدلة الرقمية قد يتطلب فحص الإذن القانوني الذي استند إليه الحصول على البيانات، فضلاً عن إجراءات استخراجها وحفظها وتحليلها والمؤهلات الفنية للقائمين على فحصها.[3]

ويقضي ذلك ألا يُختزل مفهوم المشروعية في مجرد وجود نص عام يجيز للجهة الأمنية جمع المعلومات. فالمشروعية تتطلب النظر في مصدر الاختصاص، وطبيعة الإجراء، والغرض منه، ونطاق البيانات المستهدفة، والقيود التي تحكم الوصول إليها، والضمانات التي يتعين احترامها أثناء التنفيذ. وقد يكون أصل الاختصاص ثابتاً، لكن استعماله في واقعة معينة غير مشروع بسبب تجاوز الحدود الموضوعية أو الزمنية المقررة له، أو بسبب عدم الحصول على الإذن اللازم، أو بسبب توسيع نطاق الجمع إلى معلومات لا تتصل بالغرض.[4]

وتظهر أهمية ذلك بوضوح في التمييز بين الاطلاع على معلومة منشورة للعموم والوصول إلى بيانات مخزنة في حساب خاص أو نظام محمي. فإتاحة جزء من المعلومات للجمهور لا تعني بالضرورة أن جميع البيانات المرتبطة بها متاحة للجهات الأمنية دون قيود، كما أن إمكانية الوصول التقني إلى البيانات لا تنشئ، بذاتها، سلطة قانونية للوصول إليها. ويجب في كل حالة تحديد القاعدة القانونية التي تحكم الإجراء، بالنظر إلى طبيعة البيانات وطريقة الحصول عليها والحقوق التي قد يمسها.[5]

كذلك لا يجوز افتراض أن كل مخالفة قانونية تؤدي، بالضرورة وفي جميع الأنظمة، إلى استبعاد المعلومات المتحصلة منها. فالأثر المترتب على عدم مشروعية الإجراء يختلف باختلاف التشريع المعمول به، وطبيعة الحق المنتهك، وجسامة المخالفة، ومدى اتصالها بالحصول على المعلومات، والقواعد المنظمة لقبول الأدلة واستبعادها. وقد يرتب القانون على المخالفة استبعاد الدليل، أو تقييد إمكان الاستناد إليه، أو تقرير مسؤولية القائم بالإجراء، أو اتخاذ تدبير آخر. [6]

وعليه، ينبغي الفصل بين الحكم على سلوك الجهة القائمة بالتحري والحكم على المعلومات الناتجة عنه. فقد تثبت مخالفة إجرائية دون أن يثبت أن البيانات قد عُذلت فنياً، وقد تثبت سلامة البيانات فنياً مع بقاء السؤال القانوني المتعلق بمشروعية الحصول عليها قائماً. ولا يصح أن يُستخدم أحد الحكمين بديلاً عن الآخر. [7]

ومن ثم، فإن المنهج الأكثر اتساقاً مع الضمانات القانونية يتمثل في إخضاع المعلومات الرقمية لفحص مزدوج: فحص قانوني يحدد مشروعية الوصول إليها واستخدامها، وفحص فني يتحقق من أصالتها وسلامتها. ويُستكمل الفحصان بتقييم استدلال يحدد ما يمكن استخلاصه من المعلومات دون تجاوز حدود دلالتها. [8]

المطلب الثاني: أثر تجاوز الاختصاص أو مخالفة الإذن

يمثل الاختصاص القانوني أحد الشروط الجوهرية لمشروعية التحريات الأمنية الرقمية؛ لأنه يحدد الجهة التي يجوز لها مباشرة الإجراء، والغاية التي يجوز استخدامه لتحقيقها، والحدود التي لا يجوز تجاوزها. وتزداد أهمية الاختصاص في البيئة الرقمية بسبب قدرة الوسيلة التقنية الواحدة على إتاحة أنواع متعددة من البيانات، بعضها قد يكون متاحاً للعموم، وبعضها الآخر قد يتصل بمراسلات خاصة أو معلومات شخصية. [9]

ولا يكفي أن تكون الجهة القائمة بالتحري مختصة عموماً بحفظ الأمن أو مكافحة الجريمة؛ إذ يجب التحقق مما إذا كانت تملك صلاحية اتخاذ الإجراء الرقمي المحدد. فالاختصاص بجمع المعلومات لا يستلزم بالضرورة الاختصاص باعتراض الاتصالات، والسلطة في مراقبة الأماكن العامة لا تعني تلقائياً جواز الوصول إلى محتويات الأجهزة المحمولة، كما أن صلاحية إجراء تحري أولي لا تمنح بالضرورة سلطة مباشرة إجراءات تحقيق قضائي. [10]

ويتحدد أثر تجاوز الاختصاص بحسب طبيعة القاعدة القانونية المخالفة. فإذا كان القانون يحصر إجراءً معيناً في جهة محددة، أو يشترط صدور إذن من سلطة مختصة، فإن مباشرة الإجراء من جهة غير مخولة أو دون الإذن المطلوب تنثير عيباً يتعلق بمشروعية الإجراء ذاته، وليس بمجرد انتظامه الشكلي. [11]

ثلاثة أنماط من المخالفات:

١. تجاوز الاختصاص النوعي أو الوظيفي: تباشر الجهة إجراءً لا يدخل في الصلاحيات المخولة لها قانوناً، كأن تستخدم صلاحية جمع المعلومات للوصول إلى بيانات لا يجوز الحصول عليها إلا من خلال إجراء جزائي يخضع لشروط خاصة. [12]

٢. **مخالفة حدود الإذن**: يصدر الإذن صحيحاً من حيث الأصل، لكن تنفيذه يتجاوز الأشخاص أو الأجهزة أو البيانات أو المدة أو الغرض الذي حدده الإذن.[13]

٣. **الإخلال بالشروط الإجرائية**: تُحترم حدود الاختصاص من حيث المبدأ، لكن تُهمل ضمانة لازمة لتنفيذ الإجراء، مثل عدم الالتزام بحدود النفاذ المصرح به أو تجاوز القيود القانونية المتعلقة بحفظ البيانات أو تداولها.[14]

ولا تتساوى هذه المخالفات في طبيعتها أو آثارها؛ إذ يتوقف التكيف على القاعدة التي جرى خرقها، وما إذا كانت شرطاً جوهرياً للمشروعية، ومدى اتصالها بحقوق الأفراد أو بسلامة المعلومات. ولذلك ينبغي ألا يُفترض مسبقاً أن كل خطأ شكلي يبطل الإجراء، أو أن كل تجاوز يمكن تداركه بمجرد توثيق البيانات الناتجة عنه.[15]

وتؤكد المعايير الدولية ذات الصلة بالإجراءات الخاصة بالأدلة الإلكترونية أهمية إخضاع سلطات البحث والوصول إلى البيانات ل ضمانات قانونية تحد من التعسف، مع مراعاة حماية حقوق الإنسان والمصالح المشروعة للأطراف المتأثرة. ويبرز ذلك في **المادة الخامسة عشرة من اتفاقية بودابست** بشأن الجريمة السيبرانية، التي تقرر ضرورة إخضاع السلطات والإجراءات الواردة في الاتفاقية لشروط و ضمانات مناسبة، بما في ذلك الحماية الكافية لحقوق الإنسان والحريات، مع مراعاة مبدأ التناسب.[16] ومع ذلك، يجب التنبيه إلى أن الاتفاقية لا تُعد قاعدة ملزمة تلقائياً لكل دولة، وإنما يتحدد أثرها التعاهدي بحسب انضمام الدولة إليها.[17]

ويظهر أثر تجاوز حدود الإذن أيضاً في حالات الجمع الذي يبدأ مشروعاً ثم يمتد إلى بيانات إضافية لا يشملها نطاقه. فإذا كان الإذن متعلقاً ببيانات محددة على جهاز معين، فإن اكتشاف معلومات أخرى أثناء التنفيذ لا يمنح، بمجرد، صلاحية غير محدودة لفحص جميع محتويات الجهاز أو الوصول إلى حسابات خارج نطاق الإجراء. ويتعين تحديد ما إذا كان القانون يسمح باتخاذ إجراء إضافي، وما إذا كان يلزم الحصول على إذن جديد أو توسيع الإذن القائم.[18]

وتتطلب هذه الحالات توثيقاً دقيقاً لما جرى اكتشافه، وكيفية اكتشافه، والأساس القانوني الذي استند إليه أي إجراء لاحق. فالتوثيق لا يُنشئ مشروعية لم تكن قائمة، لكنه يساعد على تحديد الوقائع وتقييم مدى التزام الجهة بحدود سلطتها.[19]

كما ينبغي مراعاة أن المعلومات الرقمية قد تنتقل بين جهات متعددة، كأن تجمعها جهة أمنية ثم تحيلها إلى جهة التحقيق المختصة. ولا يؤدي انتقال البيانات بين الجهات إلى إزالة العيوب التي شابت الحصول عليها، ولا يمنع بالضرورة الاستفادة منها إذا كان القانون يجيز ذلك في ظروف محددة. بل يجب فحص مشروعية الجمع الأصلي، وسند النقل أو المشاركة، والغرض الذي تستخدم المعلومات من أجله.[20]

وبناءً عليه، فإن سلامة الاختصاص والإذن لا تُقاس بوجود وثيقة شكلية فحسب، وإنما بمدى التطابق بين السلطة الممنوحة والإجراء المنفذ. وكلما كانت الوسيلة الرقمية أكثر قدرة على جمع بيانات واسعة أو التدخل في الحياة الخاصة، ازدادت الحاجة إلى تحديد نطاق الإذن بدقة، وإثبات الالتزام به، وإخضاع أي توسع في الإجراء لتقييم قانوني مستقل.[21]

المطلب الثالث: التمييز بين المخالفة القانونية والخلل الفني وأثر كل منهما

يُعد التمييز بين المخالفة القانونية والخلل الفني من المسائل المركزية في تحديد القيمة القانونية للمعلومات الرقمية؛ لأن الخلط بينهما قد يؤدي إلى نتائج غير دقيقة، سواء بتبرير إجراء غير مشروع استناداً إلى سلامة البيانات، أو برفض بيانات موثوقة فنياً لمجرد وجود إشكال تقني. [22]

ويقصد بالمخالفة القانونية كل انحراف عن قاعدة واجبة التطبيق تنظم الاختصاص أو الإذن أو طريقة الحصول على المعلومات أو معالجتها أو الاحتفاظ بها أو الإفصاح عنها. أما **الخلل الفني** فيتصل بسلامة البيانات أو طريقة استخراجها أو دقة الأدوات المستخدمة أو موثوقية التحليل أو اكتمال التوثيق الفني. [23]

وقد تجتمع المخالفة القانونية والخلل الفني في واقعة واحدة، كما قد يقع أحدهما دون الآخر. فالوصول إلى بيانات محمية دون الإذن المطلوب قد يشكل مخالفة قانونية حتى لو أثبت الفحص اللاحق أن البيانات لم تتغير. وفي المقابل، قد تُجمع البيانات بطريقة مشروعة، ثم تتعرض نسخة منها للتلف أو التعديل غير الموثق أثناء النقل أو المعالجة. [24]

الحالات الأربع:

الأثر المحتمل	التوصيف	الحالة
تظل المعلومات خاضعة لفحص الموثوقية والقيمة الاستدلالية وقواعد القبول.	توافق قانوني وفني	جمع مشروع وبيانات سليمة فنياً
قد يتطلب الأمر إعادة الفحص أو تقييد الاستنتاج أو عدم الاعتماد على الجزء المتأثر.	مشروعية الإجراء مع إشكال في سلامة البيانات	جمع مشروع مع وجود خلل فني
يتحدد إمكان الاستناد إلى المعلومات وفق القواعد القانونية المطبقة على المخالفة.	سلامة فنية لا تقابلها مشروعية قانونية	جمع غير مشروع مع بيانات سليمة فنياً
يتطلب تقييم كل عيب على حدة، مع بحث أثر اجتماعهما.	اجتماع العيب القانوني والفني	جمع غير مشروع مع خلل فني

وتكشف هذه الحالات أن سلامة البيانات ليست معياراً كافياً للحكم على مشروعية الإجراء، كما أن وجود خلل فني لا يعني بالضرورة أن عملية الجمع كانت غير مشروعة. [25]

ويظهر الفرق بوضوح عند استخدام قيم التجزئة الرقمية للتحقق من سلامة الملفات. فقيمة التجزئة تساعد على التحقق مما إذا كان الملف قد تغير مقارنة بنسخة مرجعية، لكنها لا تثبت أن الحصول على الملف كان مشروعاً، ولا تثبت أن محتواه يعكس واقعة صحيحة، ولا تؤكد أن الشخص المنسوب إليه المحتوى هو من أنشأه فعلاً. [26]

وبالمثل، فإن توثيق سلسلة العهدة الرقمية يساعد على بيان انتقال البيانات بين الأشخاص والجهات، لكنه لا يثبت، بمفرده، أن جميع الإجراءات السابقة على الاستلام كانت مشروعة، أو أن كل استنتاج مستخلص من البيانات صحيح. [27]

وفي المقابل، لا ينبغي التعامل مع كل نقص في التوثيق باعتباره دليلاً حاسماً على التلاعب. فقد يكون النقص ناشئاً عن خطأ إداري أو ظرف تشغيلي. غير أن تفسير سبب النقص لا يغني عن تقدير أثره في إمكانية التحقق من مصدر البيانات وسلامتها. [28]

وقد تناول المعهد الوطني الأمريكي للمعايير والتقنية (NIST) هذه الإشكالات في دراسته المتعلقة بحفظ الأدلة الرقمية، مؤكداً خصوصية البيانات الرقمية وسهولة تغيير الملفات، وأهمية توثيق مصدرها وطرق إنشائها أو نقلها، واستخدام وسائل التحقق المناسبة. [29] كما يبين استعراضه للأسس العلمية لتقنيات التحقيق الرقمي أن موثوقية هذه التقنيات ترتبط بطريقة تطبيقها، وأن النتائج قد تظل محكومة بقيود تتصل بالبيانات المسترجعة أو بتغيير الأنظمة والبرمجيات. [30]

ويترتب على ذلك أن التقييم القانوني الرصين لا ينطلق من حكم إجمالي على المعلومات بأنها "صحيحة" أو "باطلة"، بل يحدد موضع الخل وطبيعته وأثره. ويُسأل في الجانب القانوني: هل كان الإجراء مأذوناً به؟ وهل احترمت حدوده؟ وهل روعيت الضمانات الواجبة؟ أما في الجانب الفني، فيُسأل: هل أمكن تحديد المصدر؟ وهل حُفظت البيانات على نحو يسمح بالتحقق من سلامتها؟ وهل كانت الأدوات والمنهجية ملائمين؟. [31]

وبهذا الفصل المنهجي يمكن تجنب نتيجتين متقابلتين: الأولى هي إضفاء المشروعية على كل معلومة صحيحة فنياً، والثانية هي افتراض انعدام القيمة لكل معلومة شاب إجراءاتها نقص أو مخالفة دون فحص الأثر القانوني المحدد. [32]

المبحث الثاني: موثوقية المعلومات الرقمية وتقييم قيمتها القانونية

المطلب الأول: شروط الاستناد إلى المعلومات أو الأدلة الرقمية وفق القانون المختص

لا تتحدد القيمة القانونية للمعلومات الرقمية بمجرد وجودها في صورة ملف إلكتروني أو سجل محفوظ، وإنما ترتبط بمجموعة من الشروط التي تختلف تفاصيلها بحسب طبيعة الإجراء والنظام القانوني المختص والمرحلة التي تُستخدم فيها المعلومات. [33]

ويجب ابتداءً التمييز بين استخدام المعلومات في التحريات الأمنية، والاستناد إليها في اتخاذ قرار إداري أو أمني، وتقديمها ضمن إجراءات التحقيق الجزائي، والاحتجاج بها أمام المحكمة. فالمعلومة التي تكفي لتوجيه تحرٍّ أولي قد لا تكفي لإثبات واقعة أمام القضاء، كما أن البيانات التي تساعد على تحديد مصدر محتمل لا تثبت بالضرورة نسبة الفعل إلى شخص معين. [34]

ويعكس هذا التدرج اختلاف الوظيفة القانونية للمعلومات، لا اختلاف حقيقتها المادية. فالمعلومة قد تكون واحدة، لكن معيار كفايتها يتغير تبعاً للقرار المطلوب اتخاذه، والحقوق التي قد تتأثر به، والقواعد التي تحكم الإثبات. [35]

العناصر المترابطة لشروط الاستناد:

أولاً: **الصلة بالموضوع.** يجب أن تكون المعلومات ذات صلة بالواقعة أو المسألة المراد التحقق منها. ولا تكفي وفرة البيانات أو سهولة الوصول إليها لتبرير جمعها أو الاستناد إليها. وتتحدد الصلة بحسب طبيعة المسألة، ومدى اتصال المعلومات بالواقعة، وقدرتها على دعم فرضية أو استبعادها. [36]

ثانياً: **مشروعية الحصول.** يتعين تحديد السند القانوني الذي يسمح بجمع المعلومات أو الوصول إليها أو استخدامها، مع التحقق من الاختصاص والإذن والقيود. ويكتسب هذا الشرط أهمية خاصة عندما يتعلق الأمر ببيانات الاتصالات أو المحتوى الخاص أو الأجهزة أو الحسابات المحمية. ويجب مراعاة أن قواعد قبول المعلومات أو استبعادها ليست موحدة بين الدول. [37]

ثالثاً: **الأصالة وإمكان النسبة.** تقتضي الأصالة التحقق من أن البيانات المعروضة هي بالفعل البيانات المنسوبة إلى المصدر المحدد، وأن خصائصها ومصدرها لم يُقدّمَا على نحو مضلل. ويشمل ذلك التحقق من الجهاز أو النظام المنشئ للبيانات، أو من الحساب الذي نشر المحتوى. [38]

رابعاً: **السلامة وإمكان التحقق.** ينبغي التحقق من أن البيانات لم تتعرض لتغيير غير معلوم أو غير موثق، وأن إجراءات جمعها وحفظها ونقلها وتحليلها تسمح بمراجعة ما جرى عليها. وتؤدي النسخ الفنية وقيم التجزئة وسجلات الوصول وسلسلة العهدة دوراً مهماً، مع مراعاة أن كل وسيلة تثبت جانباً محدداً. [39]

خامساً: **موثوقية المصدر وطريقة إنشاء البيانات.** لا تتساوى جميع المصادر الرقمية. فالسجل الذي ينشئه نظام آلي قد يتمتع بخصائص تختلف عن منشور مجهول في شبكة اجتماعية، كما أن

بيانات الموقع التي ينتجها جهاز معين قد تتأثر بإعداداته. ويتعين فحص طبيعة المصدر، وطريقة إنتاج البيانات، وإمكان تعديلها. [40]

سادساً: كفاية المنهج التحليلي. حتى إذا كانت البيانات أصلية وسليمة، فإن النتيجة المستخلصة تتوقف على سلامة المنهج. فإذا استُخدمت البيانات لإسناد سلوك إلى شخص، وجب التحقق من أن الاستنتاج لا يقوم على افتراض غير مثبت بشأن هوية المستخدم أو حيازته للجهاز. [41]

سابعاً: استيفاء شروط القبول أو الاستخدام. يجب التمييز بين سلامة المعلومات من الناحية الفنية وقبولها قانوناً. فقد تكون البيانات ذات صلة وأصلية وسليمة، لكن القانون يشترط لتقديمها شكلاً معيناً أو توثيقاً محدداً أو تقريراً فنياً. [42]

وبناءً على ذلك، لا يمكن وضع قائمة واحدة من الشروط الإجرائية تُطبق بصورة مطلقة على جميع الأنظمة القانونية. والأدق هو تحديد المبادئ العامة المشتركة، ثم الرجوع إلى القانون المختص لتحديد الشروط الملزمة في كل حالة. [43]

وتؤكد الأدبيات الدولية المتعلقة بالأدلة الرقمية أهمية الجمع بين المتطلبات القانونية والفنية عند تقييم الدليل، بما يشمل الإذن القانوني، والأصالة، والسلامة، وموثوقية إجراءات الفحص، وكفاءة القائمين عليه. [44]

ومن ثم، فإن الاستناد القانوني السليم إلى المعلومات الرقمية يتطلب تقييماً متكاملًا لا يُختزل في عنصر واحد. فلا تكفي مشروعية الجمع وحدها، ولا سلامة الملف وحدها، ولا قوة الاستنتاج الظاهرة وحدها؛ بل يجب النظر إلى العلاقة بين هذه العناصر في ضوء الغرض من استخدام المعلومات والقواعد القانونية الواجبة التطبيق. [45]

المطلب الثاني: أثر الأصالة والسلامة والتوثيق في تقييم النتائج

تمثل الأصالة والسلامة والتوثيق عناصر أساسية في بناء الثقة بالمعلومات الرقمية، غير أن لكل عنصر منها وظيفة مستقلة ينبغي تحديدها بدقة. [46]

الأصالة تتعلق بإثبات هوية البيانات ومصدرها، ومدى مطابقتها للبيانات التي يُدعى أنها تمثلها. أما **السلامة** فتتعلق بإمكان التحقق من عدم تعرض البيانات لتغيير غير معلوم أو غير موثق. ويشير **التوثيق** إلى تسجيل الإجراءات والظروف والأشخاص والأدوات التي ارتبطت بالحصول على البيانات وحفظها وفحصها. [47]

وقد تجتمع هذه العناصر في إجراء واحد، لكنها لا تؤدي وظيفة واحدة. فإثبات مصدر ملف لا يثبت بالضرورة أنه لم يتغير، وإثبات عدم تغيره منذ إنشاء قيمة تجزئة مرجعية لا يثبت بالضرورة أن المصدر الأولي كان صحيحاً. [48]

وتتضح أهمية هذا التمييز عند التعامل مع الصور ومقاطع الفيديو والسجلات الرقمية. فقد يُحفظ مقطع مرئي دون تعديل بعد تنزيله من منصة إلكترونية، لكن ذلك لا يثبت أنه صُوّر في المكان أو الزمان المنسوبين إليه. وقد تُثبت قيمة التجزئة تطابق النسخة المحفوظة مع نسخة مرجعية، لكن ذلك لا يثبت هوية الشخص الظاهر في التسجيل. [49]

ومن هنا، ينبغي أن يحدد الفحص الفني السؤال الذي تستهدف كل وسيلة الإجابة عنه. فإذا كان الهدف التحقق من سلامة النسخة، أمكن استخدام قيمة التجزئة. أما إذا كان الهدف التحقق من تاريخ التصوير أو مصدر المحتوى، فستكون هناك حاجة إلى أدلة ومؤشرات أخرى.[50]

ويؤكد **NIST** أن حفظ الأدلة الرقمية يتطلب مراعاة خصائصها الخاصة، بما في ذلك سهولة تغيير الملفات، وأهمية توثيق المصدر وطرق انتقال البيانات، وحماية النسخ المحفوظة، وضبط الوصول إليها.[51] وتدعم هذه الاعتبارات اعتماد إجراءات موثقة منذ مرحلة جمع المعلومات.[52]

وتتجلى القيمة القانونية للتوثيق في أنه يتيح إعادة بناء المسار الذي سلكته البيانات، ويكشف الأشخاص الذين تعاملوا معها، والوقت الذي انتقلت فيه، والغرض من نقلها أو فحصها. ويتيح ذلك للجهة المختصة تقييم ما إذا كانت الإجراءات قابلة للتحقق والمراجعة.[53]

غير أن التوثيق لا ينبغي أن يتحول إلى غاية شكلية. فوجود سجل طويل ومفصل لا يثبت وحده صحة التحليل، كما أن كثرة البيانات الوصفية لا تضمن صحة الاستنتاج. وتكمن القيمة الحقيقية للتوثيق في قدرته على تمكين المراجعة المستقلة، وتحديد مصدر الخطأ عند وقوعه.[54]

ويتعين التمييز بين البيانات الأصلية والنسخ المعدة للتحليل. فبعض إجراءات الفحص قد تتطلب تحويل صيغ الملفات أو استخراج عناصر محددة. ولا يعني ذلك بالضرورة الإضرار بسلامة الدليل، شريطة توثيق العملية، وحفظ الأصل حيثما أمكن.[55]

أما إذا تعذر الاحتفاظ بالأصل أو اقتضت ظروف الإجراءات اتخاذ تدبير قد يؤثر فيه، فينبغي توثيق الأسباب والظروف والبدائل المتاحة، وبيان أثر ذلك في إمكان التحقق اللاحق.[56]

وتبرز أهمية ذلك أيضًا في تقييم سلسلة العهدة الرقمية. فالسلسلة المكتملة تساعد على بيان انتقال البيانات، لكنها لا تعني بالضرورة استحالة حدوث خطأ. وفي المقابل، فإن اكتشاف نقص في السجل لا يثبت تلقائيًا وقوع تلاعب؛ بل يستلزم تحديد المرحلة التي ظهر فيها النقص، ومدى إمكان تعويضه بأدلة مستقلة.[57]

وتدعو الممارسات المهنية المتعلقة بالأدلة الإلكترونية إلى توثيق عمليات التعرف على البيانات وجمعها واستخراجها وحفظها وتحليلها، مع بيان الأدوات المستخدمة والخطوات المتخذة والقيود المعروفة. ويؤكد مكتب الأمم المتحدة المعني بالمخدرات والجريمة أن التحليل ينبغي أن يراعي احتمال عدم اكتمال المعرفة بالوقائع، وأن يتجنب التحيز التأكيدي.[58]

وبناءً عليه، فإن الأصالة والسلامة والتوثيق لا تمنح المعلومات الرقمية قيمة قانونية تلقائية، لكنها تهئ الأساس اللازم لتقييمها. وتظل النتيجة رهينة مدى ارتباط البيانات بالواقعة، ومشروعية الحصول عليها، وسلامة المنهج التحليلي.[59]

المطلب الثالث: دور الخبرة الفنية في تفسير البيانات الرقمية

تؤدي الخبرة الفنية دورًا محوريًا في تقييم المعلومات الرقمية عندما يتطلب فهمها معرفة تقنية تتجاوز الخبرة القانونية العامة. فقد تحتوي البيانات على سجلات معقدة أو آثار رقمية غير ظاهرة للمستخدم العادي، أو تتطلب تفسيرًا لآليات إنشاء الملفات وتعديلها.[60]

ومع ذلك، لا ينبغي أن يُفهم دور الخبير على أنه سلطة مطلقة في تقرير الحقيقة القانونية. فالخبير يفسر المسائل الفنية الداخلة في نطاق اختصاصه، ويبين المنهج والأدوات والنتائج والقيود، بينما يظل التكليف القانوني وتحديد مدى استيفاء شروط الإثبات من اختصاص الجهة التي يمنحها القانون هذه السلطة.[61]

أربعة عناصر رئيسة لتقييم الخبرة:

أولاً: كفاءة الخبير وملاءمة تخصصه. ينبغي أن تتناسب مؤهلات القائم بالفحص وخبرته مع طبيعة البيانات والمسألة المطلوب تفسيرها. ففحص الأجهزة المحمولة، وتحليل سجلات الشبكات، والتحقق من أصالة المحتوى المرئي، وفحص الأنظمة السحابية قد تتطلب خبرات متخصصة مختلفة.[62]

ثانياً: وضوح نطاق المهمة الفنية. ينبغي تحديد الأسئلة التي كُلف الخبير بالإجابة عنها، والبيانات التي فحصها، والإجراءات التي اتخذها، والحدود التي التزم بها. ويساعد ذلك على منع تجاوز المهمة إلى استنتاجات لا تسندها البيانات.[63]

ثالثاً: قابلية المنهج والنتائج للمراجعة. تزداد الثقة في الخبرة عندما يستطيع مراجع مستقل فهم الخطوات التي اتُبعت، والأدوات المستخدمة، والبيانات التي استند إليها التحليل، والافتراضات التي بُنيت عليها النتيجة.[64]

رابعاً: استقلال الخبير وحياده. يجب ألا يُوجَّه الفحص لإثبات فرضية محددة سلفاً، بل لاختبار الأسئلة الفنية بموضوعية. فالخبير الذي يتلقى فرضية أمنية أولية ينبغي أن يميز بين المعلومات التي تدعمها والمعلومات التي قد تنقضها.[65]

وقد تناول **NIST** الأسس العلمية لتقنيات التحقيق الرقمي، مشيرًا إلى أهمية فهم حدود هذه التقنيات، وإمكان عدم العثور على جميع البيانات ذات الصلة، واحتمال استرجاع مواد إضافية غير مرتبطة مباشرة بالمسألة، وتغير دلالات الآثار الرقمية مع تطور الأنظمة.[66]

وتفرض هذه الحدود على الخبير التزامًا بتحديد درجة الثقة في النتائج بما يتناسب مع الأدلة المتاحة. فلا ينبغي وصف الاستنتاج بأنه قطعي إذا كانت البيانات لا تسمح إلا بتجريح تفسير معين.[67]

ومن الضروري التمييز بين النتيجة التي توصل إليها الخبير مباشرة، والنتيجة التي تعتمد على معلومات قدمها طرف آخر، والاستنتاج الذي يتطلب الجمع بين عدة مصادر. فإذا اعتمد التقرير على فرضية أن جهازًا كان تحت السيطرة الحصرية لشخص معين، وجب بيان ما إذا كانت هذه الفرضية قد جرى التحقق منها فنيًا أم أنها معلومة مفترضة.[68]

وعليه، فإن الخبرة الفنية لا تحل محل التقييم القانوني، بل تمده بأساس معرفي يمكن اختباره. وتزداد قيمتها كلما اتسمت بالحياد والشفافية، ووضحت حدودها، وفصلت بين ما تثبته البيانات مباشرة وما يستنتجه الخبير منها. [69]

المطلب الرابع: التمييز بين قبول الدليل ووزنه في الإثبات

يُعد التمييز بين قبول الدليل ووزنه في الإثبات من المسائل الأساسية في الفقه الإجرائي؛ إذ يتعلق القبول بإمكان تقديم الدليل والنظر فيه وفق القواعد القانونية المنظمة للإثبات، بينما يتعلق الوزن بمدى قدرته على إقناع الجهة المختصة بصحة الواقعة. [70]

ويجب التنبيه إلى أن هذا التمييز لا يتخذ الصورة نفسها في جميع الأنظمة القانونية. فبعض التشريعات تقرر شروطاً تفصيلية لقبول أنواع معينة من الأدلة، بينما تمنح أنظمة أخرى جهة الفصل دوراً أوسع في تقدير موثوقية الدليل. لذلك يُستخدم هذا التمييز هنا بوصفه إطاراً تحليلياً عاماً. [71]

ويعني قبول المعلومات الرقمية، حيث يقرر القانون نظاماً خاصاً للقبول، أن الجهة المختصة لم تجد مانعاً قانونياً يحول دون النظر فيها. أما وزنها فيتعلق بمدى قوتها في دعم الادعاء أو نفيه، ومدى اتساقها مع بقية الأدلة، وما إذا كانت تتيح تفسيرات بديلة معقولة. [72]

وقد تكون المعلومات مقبولة قانوناً لكنها ضعيفة الدلالة. ومن أمثلة ذلك سجل رقمي يثبت أن اتصالاً تقنياً وقع من عنوان معين، دون أن يثبت من كان يستخدم الجهاز في تلك اللحظة. وقد تكون البيانات موثقة وسليمة فنياً، لكن دلالتها لا تتجاوز إثبات وجود محتوى في جهاز. [73]

وفي المقابل، قد تثير المعلومات ذات الدلالة القوية إشكالات تتعلق بمشروعية الحصول عليها. وهنا يجب تجنب الاستدلال الدائري الذي يفترض أن قوة المعلومة تبرر الإجراء الذي جرى به الحصول عليها. [74]

اعتبارات تقييم وزن المعلومات الرقمية:

١. مدى ارتباط المعلومات بالواقعة محل الإثبات. [75]
٢. موثوقية المصدر الذي صدرت عنه البيانات. [76]
٣. إمكان التحقق من أصالتها وسلامتها. [77]
٤. وضوح المنهج الذي استخدم في تفسيرها. [78]
٥. اتساقها مع الأدلة والمعلومات المستقلة. [79]
٦. وجود تفسيرات بديلة يمكن أن تفسر البيانات على نحو مختلف. [80]
٧. مدى اكتمال السياق الذي ظهرت فيه المعلومات. [81]
٨. القيود الفنية والقانونية التي تحكم الاستناد إليها. [82]

ويجب ألا يُفهم تعدد المصادر على أنه ضمان تلقائي للقوة الإثباتية. فقد تستند عدة تقارير إلى المصدر الأصلي نفسه، فتبدو متوافقة رغم أنها لا تمثل تحققًا مستقلًا. [83] كما أن غياب التعارض بين البيانات لا يثبت صحتها بصورة حاسمة؛ فقد يكون ناتجًا عن اعتماد المصادر على أصل مشترك. [84]

ويؤكد مكتب الأمم المتحدة المعني بالمخدرات والجريمة أن تقرير الفحص الرقمي ينبغي أن يوضح المنهج والخطوات المتخذة والنتائج والقيود المعروفة، حتى لا يُساء تفسير الدليل أو يُمنح وزنًا غير مناسب. [85] وتكتسب هذه التوصية أهمية خاصة عندما تُستخدم المعلومات الرقمية في سياق جزائي. [86]

وبناءً على ذلك، فإن القبول والوزن مرحلتان متميزتان من الناحية التحليلية. ولا يجوز الانتقال من القول بإمكان النظر في المعلومات إلى القول بكفايتها لإثبات الواقعة. [87]

المبحث الثالث: حدود الاستناد إلى نتائج التحريات الرقمية

المطلب الأول: التمييز بين المعلومة الأمنية والقرينة والدليل

يتطلب تحديد حدود الاستناد إلى نتائج التحريات الأمنية الرقمية ضبط المفاهيم التي تصف المعلومات في مراحل التعامل معها، ولا سيما التمييز بين المعلومة الأمنية والقرينة والدليل. ويكتسب هذا التمييز أهميته من أن المعلومات الرقمية قد تنتقل من مرحلة الاستكشاف الأولي إلى مرحلة الاستدلال والتحقيق، دون أن تتغير البيانات ذاتها، وإنما تتغير وظيفتها. [88]

ويقصد بالمعلومة الأمنية كل معلومة تُجمع أو تُحلل بقصد فهم واقعة أو تقييم خطر أو تحديد مسار للتحقق. ولا يشترط فيها، لمجرد استخدامها في توجيه التحري، أن تكون قد استوفت جميع شروط تقديم الدليل أمام المحكمة. [89]

أما القرينة، فهي واقعة معلومة يُستدل منها على واقعة أخرى مجهولة، وفق رابطة استدلالية يعتد بها القانون أو يقبلها منطق الاستدلال. وقد تكون القرينة مستمدة من بيانات رقمية، لكن مجرد وجود معلومة إلكترونية لا يحولها تلقائياً إلى قرينة ذات قيمة قانونية محددة. [90]

أما الدليل الرقمي، فيُقصد به المعلومات أو البيانات الإلكترونية التي يُراد الاستناد إليها لإثبات واقعة أو نفيها ضمن إجراء قانوني، مع مراعاة أن التعريف الدقيق وشروط القبول والوزن تتحدد وفق القانون المختص. [91]

ولا تعني تسمية المعلومات "دليلاً رقمياً" أنها أصبحت حاسمة أو مستوفية تلقائياً لشروط القبول. فالتسمية تصف الوظيفة المقصودة من استخدامها. [92]

جدول التمييز:

المفهوم	الوظيفة الأساسية	الحد الذي ينبغي عدم تجاوزه
المعلومة الأمنية	توجيه التحري وفهم الوقائع	لا تُعامل بوصفها إثباتاً نهائياً.
القرينة	الاستدلال من واقعة معلومة على أخرى	يجب بيان الرابطة الاستدلالية وعدم افتراض أن الاحتمال يساوي اليقين.
الدليل الرقمي	دعم إثبات واقعة أو نفيها	لا يُفترض قبوله أو كفايته دون فحص مشروعيته وأصالته وسلامته.

ويترتب على ذلك أن الانتقال من المعلومة إلى القرينة أو الدليل ليس انتقالاً شكلياً يعتمد على تغيير المصطلح في التقرير، وإنما يتطلب تحققاً يتناسب مع طبيعة الاستنتاج المطلوب. [93]

كذلك يجب عدم الخلط بين الدليل الرقمي والدليل المستمد من مصدر تقليدي لمجرد أن المعلومات أصبحت محفوظة إلكترونياً. فالمستند الورقي الذي جرى مسحه ضوئياً قد يحتفظ بمصدره وطبيعته الأصلية، بينما تثير النسخة الإلكترونية أسئلة تتعلق بمطابقتها للأصل. [94]

ويؤكد الإطار العام الذي تعرضه الأمم المتحدة للأدلة الإلكترونية أن البيانات الرقمية قد تساعد على دعم أقوال الشهود أو نفيها، أو تحديد صلات بين الأشخاص والأجهزة والوقائع، لكن الاستفادة منها تظل مرتبطة بطريقة جمعها وتوثيقها وتحليلها.[95]

ومن ثم، فإن القيمة الحقيقية لهذا التمييز تكمن في منع تضخم الدلالة القانونية للمعلومات أثناء انتقالها بين الجهات أو التقارير.[96]

المطلب الثاني: حدود الاستنتاج من النتائج غير المباشرة

تُعد النتائج غير المباشرة من أكثر المسائل التي تستلزم الحذر في تحليل المعلومات الرقمية؛ لأنها تعتمد على استنتاج واقعة من مؤشرات لا تثبت بذاتها بصورة مباشرة. وقد تكون هذه المؤشرات ذات قيمة مهمة، لكنها قد تسمح بأكثر من تفسير.[97]

ويتمثل الخطر المنهجي في التعامل مع المؤشر التقني كما لو كان حقيقة نهائية عن سلوك الإنسان. فالبيانات الرقمية تسجل، في كثير من الحالات، نشاطاً تقنياً أو حدثاً داخل نظام معلوماتي، ولا تسجل بالضرورة جميع الظروف البشرية المحيطة به.[98]

فقد يثبت سجل تقني أن حساباً معيناً أجرى عملية دخول، لكن ذلك لا يثبت وحده هوية الشخص الذي استخدم الحساب. وقد تشير بيانات الموقع إلى وجود جهاز في منطقة جغرافية محددة، لكن ذلك لا يثبت بالضرورة أن شخصاً معيناً كان يحمل الجهاز.[99]

أربع طبقات للانتقال من المؤشر إلى الاستنتاج:

١. الواقعة الفنية المباشرة: ما الذي سجلته البيانات فعلاً؟.[100]

٢. التفسير الفني: ما الذي تعنيه هذه البيانات بالنظر إلى طريقة إنشاء السجل؟.[101]

٣. الاستنتاج الواقعي: ما الذي يمكن استنتاجه بشأن سلوك شخص أو وقوع حدث؟.[102]

٤. التقييم القانوني: ما الأثر الذي يمكن أن يترتب القانون على الواقعة المستخلصة؟.[103]

ولا يجوز تجاوز هذه الطبقات دون بيان الرابطة التي تسمح بالانتقال من إحداها إلى الأخرى.[104]

وتزداد أهمية ذلك عندما تعتمد النتيجة على بيانات متعددة تتفاعل فيما بينها. فقد يُستدل من بيانات الموقع وسجل الاتصال وتوقيت نشر محتوى على وجود صلة بين شخص وواقعة. لكن هذا الاستنتاج لا يصبح صحيحاً تلقائياً بمجرد توافق المؤشرات؛ إذ يجب فحص استقلال مصادرها، ودقتها الزمنية والمكانية، واحتمال اعتمادها على أصل واحد.[105]

كما أن تراكم المؤشرات لا يؤدي بالضرورة إلى زيادة الثقة بصورة آلية. فقد تكون جميع المؤشرات مشتقة من مصدر غير موثوق، أو تعتمد على فرضية واحدة غير مثبتة، أو تتأثر بالخطأ التقني ذاته.[106]

ويحذر **NIST** من أن نتائج التحقيق الرقمي تظل محكومة بقيود علمية وعملية، منها احتمال عدم اكتشاف جميع البيانات ذات الصلة، وإمكان استرجاع عناصر لا ترتبط مباشرة بالمسألة، وتأثير تفسير الآثار الرقمية بالتغيرات التي تطرأ على الأنظمة. [107]

وتتطلب سلامة الاستنتاج أيضًا تجنب الخلط بين الارتباط والسببية. فوجود علاقة زمنية أو مكانية بين حدثين لا يثبت أن أحدهما تسبب في الآخر. وقد تدعم البيانات فرضية وجود صلة بين شخص وواقعة، لكنها لا تثبت بالضرورة القصد أو الدافع أو العلم. [108]

ويجب مراعاة أثر البيانات المفقودة أو غير المكتملة. فقد يؤدي غياب جزء من سجل زمني إلى تصور تسلسل غير دقيق للأحداث. ولا يجوز افتراض أن الجزء المتاح يمثل كامل الواقعة ما لم توجد أسباب فنية أو موضوعية تدعم ذلك. [109]

وبناءً عليه، فإن الاستنتاج غير المباشر ينبغي أن يُصاغ بدرجة من اليقين تتناسب مع قوة البيانات. وإذا كانت النتائج تدعم أكثر من تفسير، وجب بيان ذلك. [110]

المطلب الثالث: مراعاة التفسيرات البديلة والقيود الفنية

لا يكتمل تقييم المعلومات الرقمية بمجرد تحديد تفسير محتمل للبيانات، بل يتطلب اختبار مدى صمود هذا التفسير أمام البدائل المعقولة. ويُعد هذا الاختبار أحد أهم الضمانات المنهجية ضد التحيز التأكيدي، الذي يدفع المحلل إلى البحث عما يؤيد فرضيته الأولية وإهمال المعلومات التي قد تتناقضها. [111]

وتظهر أهمية التفسيرات البديلة عندما تكون البيانات غير مباشرة أو عندما يعتمد الاستنتاج على ربط عدة مصادر. فإذا أظهرت البيانات نشاطًا صادرًا عن حساب معين، فقد تشمل التفسيرات المحتملة استخدام صاحب الحساب له، أو استخدام شخص آخر لبيانات الدخول، أو اختراق الحساب. [112]

ويقتضي الاختبار المنهجي تحديد الفرضية الأساسية، ثم بيان المؤشرات التي تدعمها، وتلك التي قد تضعفها، وتحديد البيانات الإضافية التي يمكن أن تساعد على التمييز بينها وبين البدائل. ويجب ألا يُعامل غياب الدليل على أحد البدائل بوصفه إثباتًا تلقائيًا للفرضية الأساسية. [113]

ومن الضروري التمييز بين البديل النظري والبديل المعقول. فليس مطلوبًا من المحلل أن يستعرض كل احتمال متخيل، وإنما أن يتناول التفسيرات التي تجد أساسًا في خصائص البيانات أو ظروف الواقعة. [114]

وتبرز القيود الفنية بوصفها عنصرًا مؤثرًا في تحديد مدى قوة هذه التفسيرات. فقد تتأثر بيانات التوقيت بإعدادات الساعة أو المنطقة الزمنية. وقد تتأثر بيانات الموقع بدقة التقنية المستخدمة. وقد تتغير دلالة سجلات الأنظمة تبعًا لإصدار البرنامج. [115]

لذلك يجب أن يوضح التحليل الفني مصادر عدم اليقين التي يمكن أن تؤثر في النتيجة، وألا يكتفي بعرض المخرجات النهائية للأداة. [116]

ويؤكد استعراض NIST للأسس العلمية لتقنيات التحقيق الرقمي أن فهم حدود الأدوات والآثار الرقمية عنصر لازم لتقييم النتائج، وأن تغير الأنظمة والبرمجيات قد يؤثر في تفسير بعض الآثار. [117]

ومن ناحية أخرى، ينبغي التمييز بين الشك الذي يمكن تقليصه بإجراءات تحقق إضافية، والشك الذي يرجع إلى حدود جوهريّة في البيانات أو التقنية. فقد يمكن معالجة نقص معين بمقارنة سجل آخر، بينما قد يتعذر تحديد هوية المستخدم بدقة اعتمادًا على نوع البيانات المتاحة. [118]

وتقتضي الموضوعية ألا يُفسر كل تعارض بين المصادر على أنه دليل على التلاعب. فقد ينشأ التعارض من اختلاف توقيت التسجيل أو المناطق الزمنية أو طرق الجمع. [119]

ويُعد الإفصاح عن مواطن عدم اليقين جزءًا من جودة التقرير، لا اعترافًا بضعف العمل. فالتقرير الذي يحدد بدقة ما أمكن إثباته وما لم يمكن إثباته أكثر فائدة من تقرير يقدم نتائج قطعية لا تسندها البيانات. [120]

ومن ثم، فإن اختبار الفرضيات البديلة لا يهدف إلى إضعاف النتائج الأمنية، وإنما إلى منع الاستنتاجات المتسارعة، وتحديد قوة الأدلة على نحو متناسب. [121]

المطلب الرابع: متطلبات الإفصاح عن مصادر المعلومات وطرق التحقق منها

يمثل الإفصاح عن مصادر المعلومات وطرق التحقق منها ضمانة مهمة لشفافية التقييم القانوني والفني، لأنه يتيح معرفة الأساس الذي بُنيت عليه النتائج، ويمكن الجهات المختصة من اختبارها. [122]

ولا يُقصد بالإفصاح هنا نشر المعلومات الحساسة على نحو غير مشروع، وإنما بيان ما يلزم، وفق القانون المنطبق، لتمكين الجهة المختصة والأطراف التي يقرر القانون حقوقها من تقييم مصدر المعلومات وطريقة الحصول عليها. [123]

ويجب التمييز بين الإفصاح الداخلي داخل الجهة القائمة بالتحري، والإفصاح للجهة المشرفة أو الرقابية، والإفصاح لجهة التحقيق أو المحكمة، والإفصاح للأطراف المعنية. فلكل مستوى غرضه وحدوده القانونية. [124]

ومع ذلك، لا ينبغي استخدام السرية ذريعة لإخفاء أوجه القصور التي تؤثر في موثوقية الاستنتاج. فالتوازن بين السرية والشفافية يتطلب تحديد المعلومات التي يلزم الكشف عنها، والجهة المخولة بتلقيها. [125]

عناصر الإفصاح المنهجي:

١. مصدر المعلومات: الجهة أو النظام أو الحساب أو الوسيط. [126]

٢. طريقة الحصول عليها: منشورة، مقدمة، مستخرجة، مع بيان السند القانوني. [127]

٣. إجراءات التحقق: الاختبارات والمقارنات التي أُجريت. [128]

٤. الأدوات والمنهجية: الأدوات المستخدمة والخطوات المؤثرة.[129]

٥. القيود الفنية: أوجه النقص أو عدم اليقين.[130]

٦. الفرضيات البديلة: التفسيرات الأخرى التي جرى اختبارها.[131]

٧. التغييرات والمعالجة: أي تحويل أو استخراج أثر في البيانات.[132]

٨. حدود الاستنتاج: الفصل بين ما تثبته البيانات مباشرة وما استنتج منها.[133]

ولا يلزم أن تتخذ هذه العناصر شكلاً واحداً في جميع التقارير؛ فقد يتطلب التقرير الأمني المختصر عرضاً موجزاً، بينما يستلزم التقرير الفني تفصيلاً أكبر.[134]

ويجب أيضاً بيان ما إذا كانت مصادر المعلومات مستقلة بعضها عن بعض. فإذا اعتمد تقرير على بيانات وردت من جهة أخرى، وكانت الجهة الأخرى قد استندت إلى المصدر نفسه، فلا يصح عرض التقريرين بوصفهما تأكيدين مستقلين.[135]

وتبرز هذه المسألة في التحريات القائمة على المحتوى المنشور عبر المنصات الرقمية؛ إذ قد يُعاد تداول الصورة نفسها في عدة حسابات، بما يوحي بتعدد مصادره، رغم أن جميع المنشورات تعود إلى ملف واحد.[136]

كما ينبغي مراعاة أن الإفصاح عن القيود الفنية قد يؤثر في تقييم وزن المعلومات، لكنه لا يؤدي بالضرورة إلى استبعادها. فقد تكون المعلومات مفيدة رغم وجود نقص محدد، إذا كان النقص معلوماً ومحدود الأثر.[137]

ويؤكد مكتب الأمم المتحدة المعني بالمخدرات والجريمة أهمية أن تكون تقارير الفحص الرقمي واضحة ودقيقة، وأن تتضمن المنهجية والخطوات والنتائج والقيود المعروفة.[138]

وبناءً عليه، فإن الإفصاح عن مصادر المعلومات وطرق التحقق منها لا يمثل إجراءً شكلياً، بل هو جزء من الأساس الذي تقوم عليه قابلية النتائج للمراجعة والمناقشة.[139]

الجدول المقارن: مستويات تقييم المعلومات الرقمية

الأثر إذا اختلف	المعيار	السؤال الأساسي	المستوى
قد يؤدي إلى استبعاد أو تقييد الاستناد (بحسب التشريع)	الاختصاص، الإذن، الغرض، النطاق	هل كان الحصول على المعلومات مأذوناً به قانوناً؟	المشروعية
قد يضعف الموثوقية أو يستلزم إعادة فحص	قيم التجزئة، سلسلة العهدة، النسخ الفنية	هل البيانات أصلية ولم تتغير؟	السلامة الفنية
قد يحد من وزن النتيجة	طبيعة المصدر، الأدوات، الخبرة	هل المصدر والمنهج يسمحان بالاعتماد؟	الموثوقية
قد يحد من كفاية النتيجة للإثبات	الصلة، الاتساق، البدائل	هل تدعم البيانات الاستنتاج المطلوب؟	القيمة الاستدلالية

قد تمنع النظر في الدليل	قواعد الإثبات المختصة	هل تستوفي شروط القبول؟	القبول القانوني
يحدد درجة الاعتماد على الدليل	التقييم القضائي	ما قوة الدليل في الإقناع؟	الوزن

❖ النافذة التطبيقية

السيناريو: واقعة احتيال إلكتروني، ضُبط فيها جهاز حاسوب، وتم استخراج رسائل بريد إلكتروني، وسجلات دخول.

- **الخطوة الأولى (المشروعية):** التحقق من الإذن القضائي: هل يشمل الجهاز؟ هل يشمل البريد الإلكتروني؟ هل يشمل السجلات؟ إذا تجاوز الإذن نطاقه، يُقِيم أثر التجاوز.
- **الخطوة الثانية (السلامة الفنية):** إنشاء نسخة جنائية من الجهاز، حساب قيم التجزئة، توثيق سلسلة العهدة.
- **الخطوة الثالثة (الموثوقية):** فحص سجلات الدخول: هل تثبت هوية المستخدم أم فقط استخدام الحساب؟ فحص البريد: هل يثبت المحتوى أم فقط وجوده؟
- **الخطوة الرابعة (الاستنتاج):** التمييز بين: (أ) وجود رسالة في الجهاز (واقعة فنية)، (ب) إرسالها من الحساب (تفسير فني)، (ج) أن المتهم هو من أرسلها (استنتاج واقعي)، (د) مسؤوليته الجنائية (تقييم قانوني).
- **الخطوة الخامسة (البدائل):** هل يمكن أن يكون شخص آخر استخدم الجهاز؟ هل الحساب مشترك؟ هل البريد وصل آلياً؟
- **الخطوة السادسة (الإفصاح):** بيان القيود: "لم يتسن التحقق من هوية مستخدم الحساب في وقت الإرسال"، "دقة توقيت السجل تعتمد على إعدادات النظام".
- **الدرس:** كل مستوى من مستويات التقييم له معياره وأثره؛ والخلط بينها يؤدي إلى نتائج غير دقيقة.

النتائج العامة للفصل

١. مشروعية الحصول على المعلومات مستوى مستقل عن سلامتها الفنية وقيمتها الاستدلالية.
٢. لا يكفي وجود نص عام يجيز الجمع؛ بل يجب التحقق من الاختصاص والغرض والنطاق والضمانات.
٣. تجاوز الاختصاص أو مخالفة الإذن قد يثير عيباً في مشروعية الإجراء، لا مجرد خلل شكلي.
٤. انتقال البيانات بين الجهات لا يزيل العيوب التي شابت الحصول عليها.

٥. المخالفة القانونية والخلل الفني مستقلان، وقد يجتمعان أو ينفصلان.
٦. قيم التجزئة تثبت سلامة النسخة، لا مشروعية الجمع ولا صحة المضمون.
٧. سلسلة العهدة تثبت مسار التعامل، لا صحة الإجراءات السابقة ولا صحة الاستنتاج.
٨. شروط الاستناد إلى المعلومات الرقمية متعددة: الصلة، المشروعية، الأصالة، السلامة، الموثوقية، كفاية المنهج، القبول.
٩. الأصالة والسلامة والتوثيق وظائف مستقلة، ولا تغني إحداها عن الأخرى.
١٠. الخبرة الفنية تفسر ولا تحكم؛ وتقييمها يتطلب كفاءة ونطاقاً ومراجعة واستقلالاً.
١١. القبول والوزن مرحلتان متميزتان؛ القبول يتعلق بإمكان النظر، والوزن بقوة الإقناع.
١٢. التمييز بين المعلومة الأمنية والقرينة والدليل ضروري لمنع تضخم الدلالة.
١٣. الاستنتاج غير المباشر يتطلب التمييز بين الواقعة الفنية والتفسير والاستنتاج والتقييم القانوني.
١٤. تراكم المؤشرات لا يعني بالضرورة زيادة الثقة؛ فقد تكون مشتقة من أصل واحد.
١٥. اختبار التفسيرات البديلة ضمانة ضد التحيز التأكيدي.
١٦. الإفصاح عن المصادر والقيود شرط لقابلية المراجعة.

المراجع:

- (1) انظر: عادل عبد العال خراشي، ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي، ٢٠٠٦، ص ١٢٠-١٢٥.
- (2) انظر: هشام مصطفى محمد، التحريات الأمنية وأثرها في الأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٥، ص ٣٠٠-٣٠٥.
- (3) UNODC, Cybercrime Module 6: Digital Evidence Admissibility, Education for Justice Initiative, 2019.
- (4) انظر: محمد محمد سيف شجاع، شرح قانون الإجراءات الجزائية اليمني، مكتبة الصادق، صنعاء، ٢٠٠٥، (الفصل الخاص بالتحريات).
- (5) انظر: خراشي، مرجع سابق، ص ١٣٠-١٣٥.
- (6) انظر: شجاع، مرجع سابق.
- (7) انظر: هشام مصطفى، مرجع سابق، ص ٣١٠-٣١٥.
- (8) انظر: خراشي، مرجع سابق، ص ١٤٠-١٤٥.
- (9) انظر: شجاع، مرجع سابق.
- (10) انظر: هشام مصطفى، مرجع سابق، ص ٣٢٠-٣٢٥.
- (11) انظر: خراشي، مرجع سابق، ص ١٥٠-١٥٥.
- (12) انظر: المرجع السابق، ص ١٥٥-١٦٠.
- (13) انظر: هشام مصطفى، مرجع سابق، ص ٣٣٠-٣٣٥.
- (14) انظر: شجاع، مرجع سابق.

- (15) انظر: خراشي، مرجع سابق، ص ١٦٠-١٦٥.
- (16) Council of Europe, *Convention on Cybercrime*, ETS No. 185, 2001, Article 15.
- (17) انظر: شجاع، مرجع سابق.
- (18) انظر: هشام مصطفى، مرجع سابق، ص ٣٤٠-٣٤٥.
- (19) انظر: NIST, *Digital Evidence Preservation*, NISTIR 8387, 2022, at 2-1.
- (20) انظر: خراشي، مرجع سابق، ص ١٧٠-١٧٥.
- (21) انظر: شجاع، مرجع سابق.
- (22) انظر: هشام مصطفى، مرجع سابق، ص ٣٥٠-٣٥٥.
- (23) انظر: خراشي، مرجع سابق، ص ١٨٠-١٨٥.
- (24) انظر: شجاع، مرجع سابق.
- (25) انظر: هشام مصطفى، مرجع سابق، ص ٣٦٠-٣٦٥.
- (26) انظر: NIST, *Secure Hash Standard*, FIPS PUB 180-4, 2015.
- (27) انظر: NISTIR 8387, *supra* note 19, at 3-1.
- (28) انظر: خراشي، مرجع سابق، ص ١٩٠-١٩٥.
- (29) NISTIR 8387, *supra* note 19, at 1-1.
- (30) NIST, *Digital Investigation Techniques: A NIST Scientific Foundation Review*, NISTIR 8354, 2022, at 2-1.
- (31) انظر: هشام مصطفى، مرجع سابق، ص ٣٧٠-٣٧٥.
- (32) انظر: خراشي، مرجع سابق، ص ٢٠٠-٢٠٥.
- (33) انظر: شجاع، مرجع سابق.
- (34) انظر: هشام مصطفى، مرجع سابق، ص ٣٨٠-٣٨٥.
- (35) انظر: خراشي، مرجع سابق، ص ٢١٠-٢١٥.
- (36) انظر: شجاع، مرجع سابق.
- (37) انظر: UNODC, *supra* note 3.
- (38) انظر: NISTIR 8387, *supra* note 19, at 3-2.
- (39) انظر: المرجع السابق، at 3-3.
- (40) انظر: خراشي، مرجع سابق، ص ٢٢٠-٢٢٥.
- (41) انظر: هشام مصطفى، مرجع سابق، ص ٣٩٠-٣٩٥.
- (42) انظر: شجاع، مرجع سابق.
- (43) انظر: خراشي، مرجع سابق، ص ٢٣٠-٢٣٥.
- (44) UNODC, *supra* note 3; NISTIR 8354, *supra* note 30, at 3-1.
- (45) انظر: هشام مصطفى، مرجع سابق، ص ٤٠٠-٤٠٥.
- (46) انظر: NISTIR 8387, *supra* note 19, at 3-4.
- (47) انظر: المرجع السابق، at 3-5.
- (48) انظر: خراشي، مرجع سابق، ص ٢٤٠-٢٤٥.
- (49) انظر: Berkeley Protocol, *supra* note 12, at 170-175.
- (50) انظر: NISTIR 8387, *supra* note 19, at 3-6.
- (51) انظر: المرجع السابق، at 3-7.
- (52) انظر: شجاع، مرجع سابق.
- (53) انظر: هشام مصطفى، مرجع سابق، ص ٤١٠-٤١٥.
- (54) انظر: خراشي، مرجع سابق، ص ٢٥٠-٢٥٥.
- (55) انظر: NISTIR 8387, *supra* note 19, at 3-8.
- (56) انظر: المرجع السابق، at 3-9.
- (57) انظر: INTERPOL, *Guidelines for Digital Forensics First Responders*, at 10-12.
- (58) UNODC, *Cybercrime Module 6: Handling of Digital Evidence*, 2019.
- (59) انظر: هشام مصطفى، مرجع سابق، ص ٤٢٠-٤٢٥.
- (60) انظر: NISTIR 8354, *supra* note 30, at 4-1.
- (61) انظر: خراشي، مرجع سابق، ص ٢٦٠-٢٦٥.
- (62) انظر: NISTIR 8354, *supra* note 30, at 4-2.

- (63) انظر: شجاع، مرجع سابق.
- (64) انظر. NISTIR 8354, *supra* note 30, at 4-3.
- (65) انظر: هشام مصطفى، مرجع سابق، ص ٤٣٠-٤٣٥.
- (66) NISTIR 8354, *supra* note 30, at 4-4.
- (67) انظر: خراشي، مرجع سابق، ص ٢٧٠-٢٧٥.
- (68) انظر. NISTIR 8354, *supra* note 30, at 4-5.
- (69) انظر: هشام مصطفى، مرجع سابق، ص ٤٤٠-٤٤٥.
- (70) انظر: شجاع، مرجع سابق.
- (71) انظر: خراشي، مرجع سابق، ص ٢٨٠-٢٨٥.
- (72) انظر: هشام مصطفى، مرجع سابق، ص ٤٥٠-٤٥٥.
- (73) انظر: المرجع السابق، ص ٤٥٥-٤٦٠.
- (74) انظر: خراشي، مرجع سابق، ص ٢٩٠-٢٩٥.
- (75) انظر: شجاع، مرجع سابق.
- (76) انظر. NISTIR 8387, *supra* note 19, at 3-10.
- (77) انظر: المرجع السابق، 3-11 at
- (78) انظر. NISTIR 8354, *supra* note 30, at 4-6.
- (79) انظر: هشام مصطفى، مرجع سابق، ص ٤٦٠-٤٦٥.
- (80) انظر. Berkeley Protocol, *supra* note 12, at 240-245.
- (81) انظر: خراشي، مرجع سابق، ص ٣٠٠-٣٠٥.
- (82) انظر. NISTIR 8354, *supra* note 30, at 4-7.
- (83) انظر. Berkeley Protocol, *supra* note 12, at 30-32.
- (84) انظر: هشام مصطفى، مرجع سابق، ص ٤٧٠-٤٧٥.
- (85) UNODC, *supra* note 58.
- (86) انظر: شجاع، مرجع سابق.
- (87) انظر: خراشي، مرجع سابق، ص ٣١٠-٣١٥.
- (88) انظر: هشام مصطفى، مرجع سابق، ص ٤٨٠-٤٨٥.
- (89) انظر: شجاع، مرجع سابق.
- (90) انظر: خراشي، مرجع سابق، ص ٣٢٠-٣٢٥.
- (91) انظر. UNODC, *supra* note 3.
- (92) انظر: هشام مصطفى، مرجع سابق، ص ٤٩٠-٤٩٥.
- (93) انظر: خراشي، مرجع سابق، ص ٣٣٠-٣٣٥.
- (94) انظر: شجاع، مرجع سابق.
- (95) UNODC, *Cybercrime Module 3: The Role of Cybercrime Law*, 2019.
- (96) انظر: هشام مصطفى، مرجع سابق، ص ٥٠٠-٥٠٥.
- (97) انظر. NISTIR 8354, *supra* note 30, at 5-1.
- (98) انظر: خراشي، مرجع سابق، ص ٣٤٠-٣٤٥.
- (99) انظر. Berkeley Protocol, *supra* note 12, at 70-75.
- (100) انظر. NISTIR 8354, *supra* note 30, at 5-2.
- (101) انظر: المرجع السابق، 5-3 at
- (102) انظر: هشام مصطفى، مرجع سابق، ص ٥١٠-٥١٥.
- (103) انظر: شجاع، مرجع سابق.
- (104) انظر: خراشي، مرجع سابق، ص ٣٥٠-٣٥٥.
- (105) انظر. Berkeley Protocol, *supra* note 12, at 240-245.
- (106) انظر: هشام مصطفى، مرجع سابق، ص ٥٢٠-٥٢٥.
- (107) NISTIR 8354, *supra* note 30, at 5-4.
- (108) انظر: خراشي، مرجع سابق، ص ٣٦٠-٣٦٥.
- (109) انظر. Berkeley Protocol, *supra* note 12, at 300-305.
- (110) انظر: هشام مصطفى، مرجع سابق، ص ٥٣٠-٥٣٥.
- (111) انظر. Berkeley Protocol, *supra* note 12, at 240-245.

- (112) انظر: خراشي، مرجع سابق، ص ٣٧٠-٣٧٥.
- (113) انظر: هشام مصطفى، مرجع سابق، ص ٥٤٠-٥٤٥.
- (114) انظر: المرجع السابق، ص ٥٤٥-٥٥٠.
- (115) انظر. NISTIR 8354, *supra* note 30, at 5-5.
- (116) انظر: المرجع السابق، at 5-6.
- (117) المرجع السابق، at 5-7.
- (118) انظر: خراشي، مرجع سابق، ص ٣٨٠-٣٨٥.
- (119) انظر: هشام مصطفى، مرجع سابق، ص ٥٥٠-٥٥٥.
- (120) انظر. Berkeley Protocol, *supra* note 12, at 350-355.
- (121) انظر: خراشي، مرجع سابق، ص ٣٩٠-٣٩٥.
- (122) انظر. UNODC, *supra* note 58.
- (123) انظر: شجاع، مرجع سابق.
- (124) انظر: خراشي، مرجع سابق، ص ٤٠٠-٤٠٥.
- (125) انظر: هشام مصطفى، مرجع سابق، ص ٥٦٠-٥٦٥.
- (126) انظر. NISTIR 8387, *supra* note 19, at 3-12.
- (127) انظر. UNODC, *supra* note 3.
- (128) انظر. Berkeley Protocol, *supra* note 12, at 135-140.
- (129) انظر. NISTIR 8354, *supra* note 30, at 5-8.
- (130) انظر: المرجع السابق، at 5-9.
- (131) انظر. Berkeley Protocol, *supra* note 12, at 370-375.
- (132) انظر. NISTIR 8387, *supra* note 19, at 3-13.
- (133) انظر: هشام مصطفى، مرجع سابق، ص ٥٧٠-٥٧٥.
- (134) انظر: شجاع، مرجع سابق.
- (135) انظر. Berkeley Protocol, *supra* note 12, at 30-32.
- (136) انظر: المرجع السابق، at 40-45.
- (137) انظر: خراشي، مرجع سابق، ص ٤١٠-٤١٥.
- (138) UNODC, *supra* note 58.
- (139) انظر: هشام مصطفى، مرجع سابق، ص ٥٨٠-٥٨٥.

الفصل الثالث: التقييم التطبيقي لمنظومة التحريات الأمنية الرقمية

المبحث الأول: منهج التقييم ومعايير

المطلب الأول: تحديد معايير المشروعية والموثوقية والتوثيق

يقتضي التقييم العلمي لمنظومة التحريات الأمنية الرقمية اعتماد مجموعة من المعايير القانونية والفنية والمنهجية التي تسمح بالحكم على سلامة الإجراءات المتبعة، ومدى موثوقية المعلومات المتحصلة، وصلاحية النتائج. ولا يتحقق هذا التقييم بمجرد التأكد من أن الجهة القائمة بالتحري قد استخدمت أدوات تقنية متقدمة، أو أن المعلومات جُمعت من مصادر متعددة، وإنما يتطلب فحصاً متكاملًا لمشروعية الحصول عليها، وسلامتها الفنية، وموثوقية تفسيرها.[1]

أولاً: معيار المشروعية. يُعد نقطة الانطلاق في هذا التقييم؛ إذ يتعين التحقق من وجود سند قانوني يجيز إجراء التحري، ومن اختصاص الجهة القائمة به، ومن مراعاة القيود المتعلقة بالوصول إلى البيانات ومعالجتها. ولا تكفي مشروعية الغرض الأمني وحدها لتبرير كل وسيلة مستخدمة لتحقيقه، لأن الوسيلة ذاتها قد تنطوي على مساس بالخصوصية أو تجاوز لنطاق الاختصاص. ويستند هذا المعيار إلى المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية، التي تحظر التدخل التعسفي أو غير القانوني في الخصوصية، وتستلزم وجود أساس قانوني يضبط الإجراء ويحدد نطاقه.[2]

ثانياً: معيار الموثوقية. يتعلق بمدى صلاحية المعلومات الرقمية للاعتماد عليها في بناء استنتاج محدد. ويتطلب التحقق من مصدر المعلومات، وظروف إنشائها، ومدى اكتمالها، وإمكان التحقق المستقل منها. ولا ينبغي الخلط بين تعدد مصادر المعلومات وتعدد الأدلة المستقلة؛ فقد تعتمد عدة منصات على مصدر أصلي واحد، فيبدو للمحلل أن لديه تأييداً متعددًا، بينما لا يتجاوز الأمر إعادة تداول المعلومة ذاتها.[3]

ثالثاً: معيار السلامة الفنية. يستهدف التحقق من بقاء البيانات على حالها منذ جمعها أو حفظها، أو تحديد التغييرات التي طرأت عليها. وتؤدي قيم التجزئة الرقمية، وسجلات الوصول والمعالجة، ونسخ البيانات، دوراً مهماً في هذا المجال، لكنها لا تثبت بمفردها صحة المحتوى الأصلي أو مشروعية الحصول عليه.[4]

ويترتب على ذلك ضرورة الفصل بين ثلاثة أسئلة مستقلة: هل جُمعت البيانات بصورة مشروعة؟ وهل حُفظت وفُحصت بطريقة تحافظ على سلامتها؟ وهل تدعم دلالتها الفعلية الاستنتاج الذي يراد استخلاصه منها؟ إن الإجابة الإيجابية عن أحد هذه الأسئلة لا تحسم بالضرورة الإجابة عن السؤالين الآخرين.[5]

رابعاً: معيار التوثيق. يقتضي تسجيل مصدر البيانات، وتاريخ الحصول عليها، والقائم بالإجراء، والأساس القانوني، والأدوات المستخدمة، وخطوات المعالجة، والنتائج والقيود. ولا يُعد التوثيق مجرد عمل إداري لاحق، بل يمثل شرطاً أساسياً لإمكان مراجعة الإجراءات والتحقق من النتائج ومساءلة القائمين بها.[6]

وفي هذا السياق، توفر إرشادات التعامل مع الأدلة الرقمية الصادرة عن جهات مهنية متخصصة، مثل منشورات المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST)، إطاراً فنياً يمكن الاستفادة منه في تقييم عمليات الجمع والفحص والتحليل والإبلاغ عن النتائج. [7] ومع ذلك، ينبغي التمييز بين المعايير الفنية التي تساعد على ضبط جودة العمل، والقواعد القانونية الملزمة التي يتحدد نطاقها وفق التشريع المختص. [8]

خامساً: معيار الحياد المنهجي. يقتضي عدم بناء التقييم على افتراض مسبق بصحة الاشتباه أو خطأ الشخص محل التحري. ويشمل ذلك اختبار الفرضيات البديلة، وتحديد المعلومات التي قد تناقض الاستنتاج الأولي، والإفصاح عن أوجه النقص والشك. فالتقييم الذي يبحث فقط عن العناصر المؤيدة لفرضية واحدة لا يختبر موثوقية منظومة التحري. [9]

وعليه، فإن المعايير الأساسية لتقييم منظومة التحريات الأمنية الرقمية تتمثل في **المشروعية، والموثوقية، والسلامة الفنية، والتوثيق، والحياد المنهجي، وقابلية المراجعة.** ويجب تطبيقها بصورة مترابطة، مع إبقاء كل معيار مستقلاً في وظيفته، حتى لا تتحول قوة الجانب التقني إلى مبرر لتجاوز العيوب القانونية، أو تتحول سلامة الإجراء القانوني إلى افتراض غير مبرر بصحة النتائج الفنية. [10]

المطلب الثاني: تحديد الحالات أو الوقائع أو الأحكام محل التحليل وأسباب اختيارها

لا يكتسب التقييم التطبيقي قيمته العلمية من مجرد عرض حالات أو وقائع، وإنما من اختيار نماذج تسمح باختبار المعايير القانونية والفنية التي وضعتها الدراسة. ويتطلب ذلك تحديد طبيعة المادة محل التحليل، وبيان أسباب اختيارها، وتوضيح علاقتها بالإشكالية البحثية. [11]

أنواع المواد التي يمكن أن يقوم عليها التقييم:

- **وقائع قضائية منشورة:** تناولت مشروعية الحصول على البيانات الرقمية أو قبولها في الإثبات. [12]
- **تقارير رسمية:** عن استخدام وسائل المراقبة الرقمية. [13]
- **دراسات مهنية:** تناولت إجراءات جمع الأدلة الرقمية وحفظها. [14]
- **حالات افتراضية مركبة:** تُصمم لأغراض البحث لتطبيق المعايير على وقائع محددة. [15]

ويختلف الأثر العلمي لكل نوع. فالأحكام القضائية المنشورة تتيح تحليل كيفية تعامل القضاء مع المسائل القانونية، لكنها لا تسمح بتعميم النتيجة خارج نطاق الاختصاص القضائي والقواعد القانونية التي حكمت النزاع. كما أن الحكم الذي يستبعد معلومة رقمية لعيب في إجراءات الحصول عليها لا يثبت بالضرورة أن المعلومة غير صحيحة فنياً. [16]

أما التقارير الرسمية، فقد تساعد في تقييم السياسات والإجراءات المؤسسية، لكنها تحتاج إلى فحص مصدرها ومنهج إعدادها ونطاق البيانات. ولا ينبغي التعامل مع الوصف المؤسسي لإجراء معين باعتباره دليلاً مستقلاً على كفاءته أو مشروعيته.[17]

وفي المقابل، تتيح الحالات الافتراضية اختبار المنهج بصورة منضبطة؛ إذ يمكن تثبيت بعض المتغيرات وتغيير متغير آخر لمعرفة أثره في التقييم. فمثلاً، يمكن افتراض واقعة جُمعت فيها تسجيلات كاميرات مراقبة بصورة مشروعة، لكنها لم توثق عند استخراجها، ثم مقارنة بواقعة أخرى تتوافر فيها سجلات الاستخراج والحفظ. ويسمح ذلك بتحديد أثر التوثيق في قابلية مراجعة النتائج.[18] ومع ذلك، لا يجوز أن تحل الحالات الافتراضية محل الوقائع الواقعية إذا كان هدف الدراسة إثبات وجود قصور فعلي في ممارسة مؤسسة معينة.[19]

ضوابط اختيار الحالات:

١. الارتباط المباشر بالإشكالية: اتصال الحالة بمسألة جوهرية في مشروعية التحري أو موثوقية المعلومات.[20]

٢. كفاية المعلومات المتاحة: عدم إصدار حكم تفصيلي على إجراءات لا تتوافر بشأنها بيانات كافية.[21]

٣. إمكان التحقق من المصادر: تفضيل الأحكام المنشورة والتقارير الرسمية والدراسات المحكمة.[22]

٤. تنوع الحالات بحسب الغرض التحليلي: دراسة أوجه القصور القانونية والفنية والمنهجية دون تكرار.[23]

٥. مراعاة حدود التعميم: نسبة النتائج إلى الحالة محل التحليل، وعدم تجاوز ما تسمح به مادتها.[24]

ويُراعى كذلك عدم انتقاء الحالات التي تؤيد فرضية الباحث وحدها. فإذا كان البحث يفترض أن التوثيق الدقيق يعزز موثوقية التحريات الرقمية، فينبغي ألا يقتصر التطبيق على حالات ظهر فيها خلل التوثيق، بل يشمل أيضاً حالات توافرت فيها إجراءات توثيق جيدة.[25]

كما يجب التمييز بين اختيار الحالة بسبب أهميتها القانونية، واختيارها بسبب أهميتها الفنية، واختيارها لأنها تكشف تفاعل العاملين معاً. فقد تكون الحالة مفيدة في بيان حدود الإذن القانوني، لكنها لا توفر بيانات كافية لتقييم سلامة الفحص الرقمي.[26]

ومن ثم، فإن الاختيار المنهجي السليم للحالات لا يقوم على شهرتها أو إثارتها، بل على قدرتها على اختبار معايير محددة والإجابة عن أسئلة البحث.[27]

المطلب الثالث: بيان أدوات التقييم ومصادر البيانات وحدود النتائج المستخلصة

يتطلب التقييم التطبيقي تحديد الأدوات التي سيستخدمها الباحث في فحص المادة محل الدراسة، وبيان المصادر التي يستند إليها، وتوضيح حدود الاستنتاجات.[28]

أولاً: التحليل القانوني. يُستخدم لفحص الأساس التشريعي للتحري، واختصاص الجهة القائمة به، وشروط الإذن عند لزومه، ومدى احترام الحقوق والضمانات. ويجب أن ينطلق من النصوص القانونية الواجبة التطبيق، مع الاستفادة من الاتفاقيات الدولية والأحكام القضائية والمبادئ الفقهية في حدود قيمتها القانونية. [29] وفي الدراسة القانونية العامة التي لا تقتصر على تشريع وطني بعينه، ينبغي عدم التعامل مع الأنظمة القانونية المختلفة باعتبارها متطابقة. [30]

ثانياً: التحليل الفني. يُعنى بفحص سلامة البيانات ومصدرها وسياق إنشائها وطريقة حفظها ومعالجتها. ويشمل مراجعة سجلات الاستخراج، وقيم التجزئة الرقمية عند توافرها، وبيانات الجهاز أو النظام، وإصدارات الأدوات المستخدمة. غير أن هذا التحليل يظل مقيداً بالمعلومات المتاحة؛ فلا يجوز الجزم بسلامة عملية فحص لم تُحفظ سجلاتها. [31]

ثالثاً: تحليل موثوقية المصادر. يستهدف التحقق من أصل المعلومات، ومدى استقلال المصادر التي تؤيدها، وإمكان التحقق منها بوسائل أخرى، واحتمال تأثرها بالتحريف أو الاقتطاع أو إعادة النشر خارج سياقها. [32]

وتُستكمل هذه الأدوات بـ **تحليل مقارن** بين الحالة محل الدراسة والمعايير القانونية والفنية المعتمدة. ولا يعني ذلك أن كل اختلاف عن معيار مهني يمثل مخالفة قانونية، بل يجب تحديد طبيعة المعيار، ومدى انطباقه، وما إذا كان ملزماً بموجب القانون أو السياسة المؤسسية. [33]

مصفوفة التقييم:

معيار التقييم	حدود الاستنتاج	أداة الفحص	البيانات المطلوبة
مشروعية الحصول	لا يمكن الجزم بالمشروعية عند غياب النصوص	التحليل القانوني	السند القانوني، الإذن، نطاق الإجراء
أصالة البيانات	إثبات المصدر لا يثبت صحة المحتوى	الفحص الفني ومقارنة المصادر	المصدر الأصلي، هوية النظام، سياق الإنشاء
السلامة الفنية	سلامة النسخة لا تثبت صحة المحتوى	مراجعة السجلات والتحقق الفني	سجلات الحفظ والنقل وقيم التجزئة
موثوقية المعلومات	تعدد المصادر لا يثبت استقلالها	تحليل المصدر والمقارنة	المصدر، التاريخ، السياق، المصادر المستقلة
سلامة الاستنتاج	قد تبقى عدة تفسيرات محتملة	التحليل النقدي	البيانات المؤيدة والمخالفة والبدائل
جودة التوثيق	اكتمال التوثيق لا يثبت صحة النتائج	المراجعة الوثائقية	المحاضر، سجلات الوصول، التقارير

وتتبع أهمية هذه المصفوفة من أنها تمنع الانتقال من الملاحظة إلى الحكم دون بيان الحلقة الاستدلالية. فإذا تبين أن تقرير التحري لم يحدد مصدر صورة رقمية، فإن النتيجة المباشرة هي

تعذر التحقق الكامل من مصدرها استنادًا إلى التقرير وحده، وليس الجزم بأن الصورة مزورة.[34]

كذلك ينبغي الفصل بين النتائج المثبتة والنتائج الاحتمالية. فالنتيجة المثبتة هي التي تدعمها وثائق أو بيانات قابلة للتحقق. أما النتيجة الاحتمالية فهي التي تتوافق مع المعطيات دون أن تستبعد تفسيرات بديلة. ويجب أن يعكس التقرير هذا الاختلاف في صياغة الاستنتاجات.[35]

وتشمل حدود التقييم نقص الوثائق، وعدم إتاحة البيانات الأصلية، وتعارض المصادر، وعدم إمكان إعادة الفحص، واختلاف القواعد القانونية. وينبغي التصريح بهذه الحدود بوضوح، لأنها تؤثر في قوة النتيجة.[36]

وعليه، فإن القيمة العلمية للتقييم لا تُقاس بعدد الحالات، بل بوضوح منهجه، وإمكان التحقق من مصادره، والتناسب بين الأدلة والنتائج، والإفصاح عن القيود.[37]

المبحث الثاني: تطبيق معايير التقييم على الحالات المختارة

المطلب الأول: عرض الحالة ومصادر المعلومات محل التحري

يُعد عرض الحالة نقطة البداية في التطبيق العملي، إلا أن هذا العرض ينبغي ألا يتحول إلى سرد للوقائع بمعزل عن المسائل القانونية والفنية التي يراد اختبارها. [38]

ولأغراض توضيح المنهج، يمكن اعتماد حالة افتراضية تتعلق بالتحقق من واقعة اعتداء على منشأة، حيث توافرت تسجيلات من كاميرات مراقبة، وصورة منشورة على إحدى الشبكات الاجتماعية، وسجل رقمي يتضمن أوقات الدخول والخروج. وتتمثل المسألة التطبيقية في تحديد مدى إمكان الربط بين هذه المصادر، وما إذا كانت تدعم استنتاجاً بشأن زمن الواقعة وهوية الأشخاص الظاهرين. [39]

ولا تمثل هذه الحالة واقعة حقيقية، وإنما نموذج تحليلي. وتقتضي معالجتها عدم افتراض أن جميع البيانات صحيحة لمجرد توافرها، أو أن تطابق بعض التوقيات يثبت بذاته وحدة الواقعة أو هوية الشخص. [40]

بالنسبة إلى تسجيلات الكاميرات: ينبغي تحديد الجهة التي تحتفظ بها، وكيفية استخراجها، وما إذا كانت النسخة المتاحة كاملة أم مقتطعة، وهل توافرت معلومات عن النظام وإعداداته الزمنية. كما يجب التحقق من وجود فجوات في التسجيل أو اختلاف في توقيت الجهاز. [41]

أما الصورة المنشورة: فينبغي التحقق من مصدرها الأصلي، وتاريخ نشرها، ومدى توافر نسخة أصلية أو معاد تداولها، وما إذا كان سياقها يؤيد صلتها بالواقعة. ولا يكفي ظهور شخص أو مكان مشابه لإثبات أن الصورة التقطت في الموقع ذاته. [42]

وفيما يتعلق بسجل الدخول: يجب تحديد طبيعة النظام الذي أنشأه، وما إذا كانت البيانات تسجل المرور الفعلي أو مجرد استخدام بطاقة. فقد يثبت السجل استخدام بطاقة معينة، لكنه لا يثبت بالضرورة هوية الشخص الذي استخدمها. [43]

ويقتضي عرض الحالة تحديد مصدر كل معلومة على نحو مستقل، وعدم دمج المصادر في رواية واحدة قبل التحقق من العلاقة بينها. ويمكن استخدام سجل للمصادر يتضمن وصف كل مصدر، والجهة الحائزة له، وتاريخ الحصول، وطريقة الحصول، ومدى توافر الأصل، والقيود المعروفة. [44]

كما ينبغي مراعاة حماية البيانات الشخصية للأشخاص الذين تظهر صورهم أو معلوماتهم عرضاً. فلا يبرر استخدام المعلومات لأغراض الدراسة إظهار هويات حقيقية أو نشر بيانات غير لازمة. [45]

ومن الناحية المنهجية، لا يجوز أن يتضمن عرض الحالة نتائج التقييم قبل فحصها؛ لأن وصف التسجيلات بأنها "أدلة قاطعة" أو الصورة بأنها "مزورة" في بداية العرض يؤدي إلى توجيه التحليل نحو نتيجة مفترضة. والأدق استخدام أوصاف محايدة مثل "تسجيل متاح للفحص" أو "صورة منسوبة إلى الواقعة". [46]

وبذلك يؤدي عرض الحالة وظيفته العلمية عندما يحدد المعلومات المتاحة ومصادرها وحدودها دون أن يستتب الحكم على مشروعيتها أو موثوقيتها. [47]

المطلب الثاني: تقييم الأساس القانوني وإجراءات الجمع

يتطلب تقييم الأساس القانوني فحص كل إجراء من إجراءات الحصول على المعلومات بصورة مستقلة، لأن تعدد المصادر الرقمية لا يعني خضوعها جميعاً لنظام قانوني واحد. فالمعلومات المنشورة للعموم قد تختلف في حكمها عن البيانات التي تحتفظ بها جهة خاصة، كما يختلف الاطلاع على تسجيل متاح عن الحصول على بيانات اتصالات أو الدخول إلى جهاز محمي. [48]

ويبدأ الفحص بتحديد الجهة التي جمعت المعلومات، وطبيعة اختصاصها، والغرض، والسند القانوني. فإذا كان الحصول على البيانات يتطلب إذنًا قضائيًا أو تصريحًا، وجب التحقق من وجود الإذن وصحته ونطاقه ومدته والشروط الواردة فيه، ومدى التزام القائمين بالتحري بهذه الحدود. [49]

ولا يكفي أن يكون الإجراء مرتبطاً بواقعة ذات أهمية أمنية؛ إذ يجب التحقق من أن الوسيلة المستخدمة جائزة قانوناً، وأن نطاقها لا يتجاوز القدر اللازم لتحقيق الغرض. فجمع البيانات المتعلقة بشخص معين لا يبرر تلقائياً جمع بيانات جميع الأشخاص الذين تواصلوا معه، كما أن الإذن بفحص جهاز معين لا يمتد بالضرورة إلى جميع الحسابات السحابية المرتبطة به. [50]

الإجراءات الثلاثة في الحالة الافتراضية:

- الحصول على تسجيلات كاميرات المراقبة. [51]
 - الاطلاع على الصورة المنشورة والتحقق من مصدرها. [52]
 - الحصول على سجل الدخول والخروج. [53]
- قد يكون الحصول على التسجيلات أو السجلات ممكناً بموجب طلب مشروع من الجهة الحائزة، لكن ذلك يتوقف على القواعد المنظمة للإفصاح، وصفة الجهة الطالبة، والغرض، والحقوق التي قد تتأثر. ولا يمكن افتراض أن مجرد حيازة المنشأة للبيانات يمنح أي جهة أمنية حق الوصول إليها دون قيد. [54]

وبالمثل، فإن إتاحة صورة على شبكة اجتماعية للجمهور لا تعني بالضرورة جواز كل أشكال معالجتها أو ربطها بقواعد بيانات أخرى أو الاحتفاظ بها إلى أجل غير محدد. [55]

ويجب أيضاً التحقق من مدى مراعاة مبدأي الضرورة والتناسب. فالضرورة تقتضي أن تكون الوسيلة ذات صلة فعلية بالغرض، وألا يتوافر بديل أقل مساساً بالحقوق. أما التناسب فيتطلب ألا تتجاوز أعباء الإجراء على الحقوق ما تبرره أهمية الهدف المشروع وظروف الحالة. [56]

ويترتب على ذلك أن مشروعية الإجراء لا تُستخلص من نجاحه في الوصول إلى معلومة مهمة. فالنتيجة المفيدة لا تصحح بأثر رجعي تجاوز الاختصاص أو غياب الإذن الواجب. [57]

ويُستحسن أن يشمل التقييم مراجعة التوثيق المصاحب لعملية الجمع، بما في ذلك تاريخ الإجراء، وهوية القائم به، والمستند القانوني، والبيانات التي تم الحصول عليها، والقيود. ويساعد ذلك على التحقق من مطابقة التنفيذ للغرض والإذن، ومن إمكان تحديد المسؤولية عن أي تجاوز. [58]

أما إذا كانت الوثائق القانونية غير متاحة، فيجب التعبير عن النتيجة بصياغة منضبطة، مثل القول إن "المادة المتاحة لا تكفي للتحقق من استيفاء شروط الإذن"، بدلاً من الجزم بعدم المشروعية. فغياب المستند عن ملف الدراسة لا يثبت دائماً عدم وجوده في الواقع. [59]

كذلك ينبغي عدم الخلط بين عدم مشروعية الحصول وعدم موثوقية البيانات فنياً. فقد تكون صورة قد جُمعت بطريقة تخالف القواعد القانونية، لكنها غير معدلة من الناحية الفنية؛ وقد تكون بيانات قد جُمعت وفق إجراء مشروع، لكنها غير مكتملة. [60]

وعليه، فإن التقييم القانوني السليم يفحص مشروعية كل مرحلة، ومدى الالتزام بالاختصاص والإذن والضرورة والتناسب، مع إبقاء الحكم الفني على سلامة البيانات مستقلاً عن الحكم القانوني. [61]

المطلب الثالث: فحص أصالة المعلومات وسلامتها

يستهدف فحص الأصالة التحقق من مصدرها وهويتها وسياق إنشائها، بينما يستهدف فحص السلامة تحديد ما إذا كانت البيانات قد تعرضت لتغيير غير موثق أو فقد أو اقتطاع. وعلى الرغم من الترابط، فإنهما لا يتطابقان؛ فقد تكون البيانات محفوظة دون تغيير مع بقاء مصدرها الأصلي مجهولاً. [62]

ويبدأ فحص الأصالة بتحديد المصدر الذي يُنسب إليه إنشاء البيانات. ففي التسجيل المرئي، يتطلب ذلك تحديد النظام أو الجهاز الذي أنشأه، والجهة التي تحتفظ به، وطريقة استخراجها. وفي الصور المنشورة، يتطلب التمييز بين الحساب الذي نشر الصورة أول مرة والحسابات التي أعادت نشرها، مع التحقق من أن تاريخ النشر لا يُعامل تلقائياً باعتباره تاريخ الالتقاط. [63]

وتُعد البيانات الوصفية من العناصر التي قد تساعد، إلا أن قيمتها تتوقف على طبيعتها ومصدرها ومدى إمكان تعديلها. فوجود تاريخ أو موقع في بيانات ملف لا يثبت بالضرورة أن المحتوى أنشئ في ذلك التاريخ أو الموقع. [64]

أما فحص السلامة، فيتطلب مراجعة إجراءات الحفظ والنقل والفحص، وتحديد ما إذا كانت النسخة محل التحليل مطابقة للنسخة التي جرى توثيقها عند الاستلام. ويمكن الاستفادة من قيم التجزئة الرقمية في مقارنة النسخ، شريطة تسجيل القيمة المحسوبة والوقت والأداة والملف. [65]

ومع ذلك، ينبغي عدم المبالغة في دلالة قيم التجزئة. فإذا حُسبت قيمة لنسخة موجودة بالفعل، فإنها لا تثبت وحدها أن النسخة كانت مطابقة للمصدر الأصلي قبل احتساب القيمة. كما أن تطابق القيم يدعم استنتاج تطابق المحتوى الرقمي وفق الخوارزمية، لكنه لا يثبت صحة الوقائع التي يعرضها المحتوى. [66]

وفي الحالة الافتراضية، يمكن فحص تسجيل الكاميرا من خلال مقارنة النسخة المتاحة بسجل الاستخراج، والتحقق من اكتمال المقطع، ومراجعة معلومات النظام وتوقيته. وإذا لم تتوافر النسخة الأصلية، فيجب بيان أن الفحص انصب على النسخة المتاحة، وأن غياب الأصل يحد من نطاق الاستنتاجات.[67]

أما الصورة المنشورة، فينبغي فحصها في ضوء سياق النشر ومصادرها المستقلة، ومقارنتها بالنسخ الأخرى. ولا يجوز اعتبار اختلاف الأبعاد أو ضغط الصورة دليلاً حاسماً على التزوير، لأن هذه التغيرات قد تنتج عن المعالجة المعتادة.[68]

وبالنسبة إلى سجل الدخول، يجب التحقق من سلامة عملية التصدير، وطبيعة النظام، وإعداداته الزمنية، وإمكان تعديل السجلات، ومدى توافر سجل تدقيق. وقد يكون السجل سليماً تقنياً، لكنه لا يدل إلا على الحدث الذي صُمم النظام لتسجيله.[69]

ويقتضي الفحص توثيق الأدوات وإصداراتها، وخطوات المعالجة، وأي قيود فنية. ويجب التمييز بين الإجراءات التي تغير الملف محل الفحص، والإجراءات التي تنتج نسخة مشتقة، مع الاحتفاظ بالمادة الأصلية.[70]

كما ينبغي تقييم إمكان إعادة الفحص المستقل. فإذا لم تكن خطوات التحليل موثقة أو تعذر توفير البيانات اللازمة للمراجعة، فقد تصبح النتيجة أقل قابلية للتحقق، حتى لو بدا تفسيرها معقولاً.[71]

وتنتهي عملية الفحص بتحديد مستوى الثقة الذي تسمح به البيانات المتاحة، لا بإصدار حكم يتجاوز نطاق الفحص. فقد يثبت التحليل أن ملفاً لم يتغير منذ استلامه، دون أن يثبت مصدره الأصلي؛ وقد يدعم نسبة الملف إلى جهاز معين، دون أن يثبت أن محتواه يمثل الواقعة كاملة.[72]

ومن ثم، فإن الأصالة والسلامة عنصران أساسيان، لكنهما لا يغنيان عن فحص مشروعية الحصول، أو تقييم الدلالة، أو مراعاة الشروط القانونية للاستناد.[73]

المطلب الرابع: اختبار الاستنتاجات والفرضيات البديلة

لا يكتمل التقييم بالتحقق من مصدر المعلومات وسلامتها فحسب، بل يتطلب اختبار الاستنتاجات. فقد تكون البيانات أصلية وسليمة، ومع ذلك يُساء تفسيرها أو تُحمّل دلالة لا تحتملها.[74]

ويبدأ الاختبار بتحديد الاستنتاج المراد تقييمه بدقة. فإذا كان الاستنتاج أن شخصاً معيناً كان موجوداً في موقع واقعة، فيجب تحديد المعلومات التي يُستند إليها، وما إذا كانت تثبت وجود الشخص نفسه أو وجود جهاز أو بطاقة مرتبطة به.[75]

ويتطلب ذلك تفكيك الاستنتاج المركب إلى عناصره. فإثبات وجود جهاز في موقع لا يساوي إثبات وجود مالكه، كما أن إثبات استخدام بطاقة دخول لا يثبت تلقائياً أن صاحبها هو من استخدمها.[76]

وفي الحالة الافتراضية، قد يظهر تسجيل المراقبة شخصًا في محيط المنشأة، ويشير سجل الدخول إلى استخدام بطاقة مرتبطة بموظف، بينما تتضمن صورة منشورة شخصًا مشابهًا. ولا يكفي اجتماع هذه العناصر للجزم بأن الموظف كان موجودًا وشارك في الواقعة، ما لم تُفحص الروابط بين كل عنصر والنتيجة.[77]

ويقتضي التحليل اختبار بدائل معقولة، مثل احتمال استخدام البطاقة من شخص آخر، أو اختلاف توقيت أحد الأنظمة، أو كون الصورة قد التقطت في وقت سابق، أو وجود تشابه في المظهر. ولا يعني اختبار هذه الفرضيات مساواتها في القوة، وإنما فحصها بقدر يتناسب مع معقوليتها.[78]

ويجب التمييز بين غياب الدليل على فرضية وجود دليل ينفيها. فإذا لم تتضمن التسجيلات مشاهدًا يثبت دخول شخص، فقد يكون السبب عدم وجوده، وقد يكون وجود فجوة في التسجيل. لذلك لا يجوز تحويل نقص البيانات تلقائيًا إلى دليل على عدم وقوع الحدث.[79]

وتبرز أهمية ذلك عند تحليل بيانات الموقع والتوقيت. فبيانات الموقع قد تتأثر بدقة النظام وظروف الاستقبال، كما قد تؤدي الفروق الزمنية بين الأنظمة إلى ترتيب غير صحيح للأحداث إذا لم تُؤخذ المناطق الزمنية.[80]

كذلك يجب مراعاة احتمال الاعتماد المتبادل بين المصادر. فإذا كانت عدة تقارير قد استندت إلى صورة واحدة، فإن توافقها لا يمثل تأييدًا مستقلًا. وينبغي تتبع مسار المعلومة إلى مصدرها الأول.[81]

خطوات اختبار الاستنتاجات:

١. تحديد الادعاء محل التقييم.[82]
 ٢. تحديد البيانات التي تدعمه والافتراضات اللازمة.[83]
 ٣. التحقق من مدى استقلال المصادر.[84]
 ٤. تحديد التفسيرات البديلة.[85]
 ٥. فحص الأدلة التي تؤيد كل تفسير أو تضعفه.[86]
 ٦. تحديد أوجه النقص أو التعارض التي لم تُحسم.[87]
 ٧. صياغة النتيجة بدرجة من الجزم تتناسب مع قوة الأدلة.[88]
- ولا يقتصر الاختبار على البيانات المؤيدة؛ بل يجب البحث عن المعلومات المخالفة. ويُعد إغفال هذه المعلومات من أبرز مظاهر التحيز التأكيدي.[89]
- وفي هذا السياق، ينبغي التمييز بين الارتباط والسببية. فظهور شخص في مكان قريب من واقعة لا يثبت أنه تسبب فيها، كما أن تزامن نشاط رقمي مع حدث لا يكفي لإثبات علاقة سببية.[90]

كما ينبغي الإفصاح عن مستوى عدم اليقين. فإذا كانت البيانات ترجح تفسيراً دون أن تستبعد البدائل، وجب بيان ذلك. وإذا كانت المعلومات غير كافية للتمييز بين عدة احتمالات، فإن النتيجة العلمية السليمة هي التصريح بعدم كفاية البيانات.[91]

ويجب أن يظل التقييم الفني منفصلاً عن الحكم القانوني النهائي؛ فالمحلل قد يبين أن البيانات تدعم استنتاجاً بدرجة محددة من الثقة، لكنه لا يحل محل الجهة المختصة في تقدير مدى كفاية المعلومات لاتخاذ إجراء قانوني.[92]

وعليه، فإن اختبار الفرضيات البديلة ليس مرحلة ثانوية، بل ضمانة منهجية تحول دون تحويل المعلومات الجزئية إلى استنتاجات جازمة.[93]

المطلب الخامس: تقييم النتائج في ضوء القانون والمعايير الفنية المعتمدة

تتمثل المرحلة الختامية في تحديد مدى اتساق النتائج المستخلصة مع القواعد القانونية والمعايير الفنية. ولا ينبغي أن يُبنى هذا التقييم على انطباع عام، بل على مراجعة كل عنصر وتحديد ما إذا كان يستوفي المتطلبات.[94]

ويبدأ التقييم القانوني بمراجعة السند الذي استند إليه التحري، ومدى اختصاص الجهة، والالتزام بنطاق الإذن، واحترام الحقوق. ويجب تحديد القاعدة القانونية التي يُقاس عليها الإجراء، وعدم الاكتفاء بإحالة عامة إلى مبادئ المشروعية.[95]

ويقتضي ذلك التمييز بين القواعد الدولية العامة التي تقرر حماية الحقوق، والتشريعات الوطنية التي تحدد الاختصاصات والإجراءات، والمعايير المهنية التي تنظم جوانب العمل الفني. فقد تساعد المعايير المهنية في تحديد الممارسة الجيدة، لكنها لا تحل محل الإذن القانوني.[96]

أما التقييم الفني، فيتجه إلى التحقق من أصالة البيانات وسلامتها، ومدى اكتمال التوثيق، وإمكان إعادة الفحص، ودقة الأدوات، ووضوح العلاقة بين البيانات والنتائج.[97]

وفي الحالة الافتراضية، إذا تبين أن تسجيل المراقبة قد جُمع وفق إجراء مشروع، لكنه وصل دون توثيق كامل لعملية استخراجها، فإن التقييم لا ينبغي أن يقفز إلى القول ببطلانه أو صحته المطلقة. بل يتعين تحديد المعلومات التي ما زال بالإمكان التحقق منها، ومدى توافر النسخة الأصلية.[98]

وإذا أظهر الفحص أن الصورة لا يمكن نسبتها إلى مصدرها الأصلي بصورة موثوقة، فإن النتيجة المباشرة هي محدودية إمكان الاعتماد عليها لإثبات المصدر أو الزمان أو المكان، لا الجرم بتزويرها. ويمكن أن تظل مفيدة بوصفها خيطاً للتحري.[99]

أما إذا كان سجل الدخول سليماً فنياً، لكنه لا يثبت إلا استخدام بطاقة معينة، فيجب قصر الاستنتاج على هذا الحد، ما لم تتوافر أدلة مستقلة تربط استخدام البطاقة بالشخص.[100]

تصنيف نتائج التقييم:

- نتائج مستوفية للمتطلبات: تدعمها مستندات كافية، ويتحقق بشأنها الالتزام بالقواعد. [101]
 - نتائج موثوقة مع قيود محددة: يمكن الاستفادة منها ضمن حدود معلومة. [102]
 - نتائج غير كافية للتحقق: لا تتوافر بشأنها معلومات تسمح بالحكم على عنصر جوهري. [103]
 - نتائج يشوبها خلل مؤثر: يكشف الفحص عن عيب من شأنه التأثير في المشروعية أو السلامة أو صحة الاستنتاج. [104]
- ولا ينبغي أن يفهم هذا التصنيف على أنه بديل عن الأحكام القانونية المنظمة لقبول الأدلة أو استبعادها؛ فهو أداة تحليلية. أما الأثر القانوني النهائي، فيتحدد بحسب التشريع المختص. [105]
- ويقتضي التقييم بيان مدى قابلية النتائج للمراجعة المستقلة. فإذا كان الاستنتاج يعتمد على أداة آلية، وجب توضيح طبيعة المخرجات، وحدود الأداة، ومدى خضوع النتائج للتحقق البشري. ولا يجوز اعتبار النتيجة صحيحة لمجرد صدورها عن برنامج متخصص. [106]
- ويجب أن ينتهي التقييم ببيان العلاقة بين أوجه القصور والتوصيات. فإذا كان الخلل ناشئاً عن غياب سجل موحد لحركة البيانات، فإن التوصية تتعلق بتطوير إجراءات التوثيق. وإذا كان ناشئاً عن غموض شروط الوصول، فإن المعالجة تتطلب مراجعة القواعد القانونية. [107]
- وبذلك يصبح التقييم التطبيقي أداة لاستخلاص نتائج قابلة للتبرير، لا مجرد وسيلة لتأييد موقف سابق. [108]

المبحث الثالث: نتائج التقييم وأوجه القصور وحدود التعميم

المطلب الأول: أوجه الاتساق بين المتطلبات القانونية والفنية

يكشف التقييم المتكامل أن المتطلبات القانونية والفنية ليست مسارين منفصلين، بل يرتبط كل منهما بالآخر في تحديد مدى صلاحية المعلومات. فالقانون يحدد نطاق السلطة، بينما يحدد العمل الفني مدى سلامة البيانات وإمكان التحقق من مصدرها. [109]

أوجه الاتساق:

١. **تحديد الغرض القانوني** يساعد على ضبط نطاق جمع المعلومات، وتقليل المعلومات غير المرتبطة، وتحديد شروط الاحتفاظ. [110]
 ٢. **التوثيق الفني** يرتبط بالمساءلة القانونية؛ فتسجيل هوية القائمين والتوقيعات والمصادر يتيح مراجعة الالتزام بالإذن والاختصاص. [111]
 ٣. **المحافظة على سلامة البيانات** تدعم إمكان مراجعتها وتقييم قيمتها الاستدلالية. [112]
 ٤. **ضمانات الخصوصية** قد تسهم في تحسين جودة التحري نفسه، بتقليل التشتت التحليلي والتعامل غير المنضبط مع بيانات لا تخدم الموضوع. [113]
 ٥. **المراجعة المستقلة** تتكامل فيها المراجعة القانونية (المشروعية) والفنية (السلامة). [114]
- ومع ذلك، لا يعني هذا الاتساق أن استيفاء المتطلبات القانونية يؤدي حتمًا إلى نتائج فنية صحيحة، أو أن جودة الفحص الفني تكفي لتصحيح أي تجاوز قانوني. [115]
- وتؤكد هذه الملاحظة أن التكامل يجب أن يقوم على **الاستقلال المتبادل في التقييم**، لا على دمج المعايير في حكم واحد. [116]
- كما أن هذا التكامل يتطلب **وضوحًا في توزيع المسؤوليات**. فالجهة التي تأذن ليست بالضرورة هي التي تنفذ أو تفحص، والخبير الفني لا يملك صلاحية تقدير المشروعية القانونية. [117]
- ومن ثم، فإن الاتساق الفعال يتطلب إجراءات واضحة لتحديد الاختصاص، وتوثيق مراحل التحري، وحفظ البيانات، ومراجعة النتائج، وتحديد المسؤوليات. [118]

المطلب الثاني: أوجه القصور في إجراءات الجمع والتحقق والتوثيق

يمكن أن تظهر أوجه القصور في مراحل متعددة، ولا تتساوى في طبيعتها أو أثرها. [119]

أنماط القصور المحتملة:

١. **عدم وضوح الأساس القانوني** أو عدم كفاية توثيقه. ويؤدي ذلك إلى صعوبة التحقق من المشروعية، حتى إذا بدت المعلومات مفيدة. [120]

٢. **عدم توثيق مصدر البيانات** أو الاكتفاء بنسخة معاد تداولها. ويظهر بوضوح في المحتوى المنشور على الإنترنت.[121]
 ٣. **انقطاع سلسلة العهدة الرقمية** أو نقص سجلاتها. ويحد ذلك من إمكان تحديد المسؤولية عن التغييرات.[122]
 ٤. **الخلط بين سلامة البيانات وصحة محتواها**. فقد يُحفظ ملف دون تغيير، ثم يُعامل باعتباره صحيحًا من حيث الوقائع.[123]
 ٥. **ضعف اختبار الفرضيات البديلة**. فينطلق التحليل من اشتباه أولي، ثم تُجمع المعلومات التي تؤيده دون بحث كافٍ عن الأدلة المخالفة.[124]
 ٦. **عدم الإفصاح عن القيود الفنية**. فتُعرض نتائج تحليل الموقع أو التوقيت دون بيان دقة التقنية المستخدمة.[125]
 ٧. **عدم التمييز بين التقرير الأمني والتقرير الفني**. فقد تُعرض الاستنتاجات الأمنية باعتبارها نتائج فنية محسومة.[126]
 ٨. **الاعتماد غير النقدي على الأدوات الآلية**. فمخرجات البرامج لا تكون صحيحة لمجرد صدورها عن أداة تقنية.[127]
- ويجب التعامل مع هذه الأوجه باعتبارها أنماطًا محتملة ما لم تثبت الدراسة التطبيقية وقوعها في حالات محددة. فلا يجوز نسبة ضعف التوثيق أو تجاوز الاختصاص إلى جهة معينة دون مستندات.[128]
- وتكشف هذه الأنماط أن القصور لا ينشأ بالضرورة من خلل تقني معقد؛ فقد يكون نتيجة إجراء إداري بسيط لم يُوثق، أو مصدر لم يُتحقق منه، أو افتراض لم يُختبر.[129]
- وعليه، فإن تحسين المنظومة يقتضي معالجة العيوب بحسب طبيعتها، وعدم الاكتفاء بتطوير الأجهزة والبرامج. فالمشكلات القانونية تحتاج إلى ضبط الاختصاص والإذن، والفنية إلى تحسين إجراءات الحفظ والفحص، والمنهجية إلى تطوير أساليب التحليل والمراجعة، والتوثيقية إلى بناء سجلات قابلة للتحقق.[130]

المطلب الثالث: مدى صلاحية النتائج لدعم الاستنتاجات الأمنية أو القانونية

- تتحدد صلاحية نتائج التحريات الرقمية بحسب الغرض الذي يراد استخدامها من أجله، ومرحلة الإجراء، ومدى استيفائها للمتطلبات القانونية والفنية.[131]
- ففي **المرحلة الأمنية الأولية**، قد تكون المعلومات غير المكتملة مفيدة في تحديد مسارات البحث. غير أن فائدتها في هذه المرحلة لا تعني أنها تصلح بالدرجة نفسها لإثبات واقعة أو نسبة فعل إلى شخص.[132]

ويجب أن يعكس استخدام المعلومات طبيعة الغرض. فإذا كانت المعلومة مجرد مؤشر أولي، وجب عدم صياغتها في التقرير بوصفها واقعة ثابتة. وإذا كانت تدعم احتمالاً، وجب بيان حدوده. أما إذا أريد تقديمها في سياق قضائي، فيجب التحقق من استيفائها للشروط القانونية.[133]

ويترتب على ذلك أن صلاحية النتيجة لا تتوقف على سلامة البيانات وحدها. فقد تكون البيانات أصلية، لكنها لا تثبت سوى وجود جهاز في مكان، دون أن تثبت وجود صاحبه.[134]

كما أن مشروعية الحصول تمثل عنصراً مستقلاً. فقد تكون المعلومة موثوقة فنياً، لكن الحصول عليها جرى بالمخالفة لقواعد الاختصاص أو الإذن. وفي هذه الحالة، لا يجوز افتراض أن موثوقيتها الفنية تحسم إمكان استخدامها قانوناً.[135]

وفي المقابل، لا يعني وجود خلل توثيقي محدود أن كل النتائج تصبح عديمة القيمة بالضرورة. فقد يكون بالإمكان التحقق من المصدر بوسائل أخرى.[136]

ويجب مراعاة العلاقة بين قوة النتيجة وطبيعة الاستنتاج المطلوب. فإثبات أن حساباً نشر محتوى يختلف عن إثبات أن شخصاً محدداً هو الذي استخدم الحساب. وكلما كان الاستنتاج أكثر تحديداً، ازدادت الحاجة إلى بيان الأساس والقيود.[137]

ومن الناحية الفنية، تتعزز صلاحية النتائج عندما تتوافر بيانات أصلية قابلة للفحص، وسجلات موثقة، وأدوات معروفة، ومصادر مستقلة، وتحليل يختبر البدائل.[138]

ومن الناحية القانونية، يتعين التمييز بين قابلية تقديم المعلومات والوزن الذي تمنحه لها الجهة المختصة. فقبول الدليل يتعلق باستيفاء شروط تقديمه، أما وزنه فيتعلق بمدى الاقتناع بدلالته.[139]

ويُستحسن أن تتضمن التقارير بياناً واضحاً لنوع النتيجة، وما إذا كانت حقيقة فنية مباشرة أو استنتاجاً تحليلياً أو فرضية تحتاج إلى استكمال. كما ينبغي إسناد كل نتيجة إلى البيانات التي تدعمها، وبيان أوجه النقص.[140]

وفي الحالات التي يتعذر فيها التحقق الكافي، ينبغي تحديد ما إذا كان يمكن الاستفادة منها بوصفها مؤشراً أولياً، أو ما إذا كانت تحتاج إلى أدلة مستقلة.[141]

ومن ثم، فإن صلاحية النتائج ليست وصفاً مطلقاً، وإنما تقدير يتوقف على الغرض، والمشروعية، والسلامة، والموثوقية، وكفاية التوثيق، والتوافق مع القواعد القانونية.[142]

المطلب الرابع: حدود تعميم النتائج المستخلصة من التطبيق

تُعد حدود التعميم عنصراً جوهرياً في التقويم التطبيقي؛ لأن النتائج المستخلصة من حالة محددة لا تتحول تلقائياً إلى أحكام عامة. ويتوقف مدى إمكان التعميم على طبيعة الحالة، وعدد الحالات، ومدى تنوعها، والقواعد القانونية، وكفاية البيانات.[143]

فإذا اعتمد التطبيق على حالة افتراضية، فإن نتائجه تظل مرتبطة بالافتراضات. ويمكن الاستفادة منها في توضيح أثر غياب التوثيق، لكنها لا تثبت أن هذه المشكلات وقعت بالفعل في مؤسسة معينة. [144]

أما إذا استند إلى حكم قضائي منشور، فإن النتائج ترتبط بالتشريع الذي طبّقه المحكمة، والوقائع التي عرضت عليها. ولا يصح تعميم الحكم على أنظمة قانونية أخرى. [145]

وإذا استند إلى تقرير رسمي، فإن حدود التعميم تتأثر بمنهج جمع البيانات، وطبيعة العينة، والفترة الزمنية. ولا يكفي أن يكون التقرير صادرًا عن جهة رسمية لإثبات أن نتائجه تمثل جميع الممارسات. [146]

كما تؤثر طبيعة التقنية في حدود التعميم. فالنتائج المتعلقة بنظام محدد للتعرف على الصور لا يجوز تعميمها على جميع الأنظمة. وكذلك لا يمكن تعميم نتائج تحليل بيانات الموقع من جهاز معين على جميع الأجهزة. [147]

وتتسع حدود التعميم بسبب التطور التقني والتشريعي. فقد تتغير خصائص الأدوات، وتظهر وسائل جديدة، وتُعدّل القوانين. ولذلك ينبغي تحديد الإطار الزمني الذي تنطبق عليه النتائج. [148]

ثلاثة مستويات من النتائج:

١. النتائج الخاصة بالحالة: تتعلق مباشرة بالوقائع والوثائق التي خضعت للتحليل. [149]

٢. النتائج التحليلية العامة: تستخلص نمطاً يمكن أن يتكرر في حالات مشابهة، بشرط بيان الشروط. [150]

٣. المقترحات المعيارية: توصيات يقترحها الباحث، ولا تُعد بذاتها نتائج أثبتتها التطبيق. [151]

ويمنع هذا التمييز الخلط بين ما تكشفه البيانات وما يقترحه الباحث. فقد يثبت التطبيق أن غياب سجل مفصل يضاعف إمكان التحقق، لكن اقتراح اعتماد نموذج موحد يظل توصية تطويرية. [152]

كما ينبغي مراعاة الفرق بين التعميم الوصفي والتعميم القانوني. فملاحظة تكرار مشكلة فنية لا تثبت بالضرورة وجود قصور تشريعي، لأن السبب قد يكون في ضعف التدريب أو غياب الإجراءات. [153]

وتتطلب الدراسة المقارنة قدرًا إضافيًا من الحذر؛ إذ لا يكفي نقل حل قانوني من نظام إلى آخر دون فحص اختلاف البنية الإجرائية والجهات المختصة وضمانات الحقوق. [154]

ومن ثم، فإن الاعتراف بحدود التعميم لا ينتقص من القيمة العلمية، بل يعززها؛ لأنه يحدد بدقة ما يمكن الاستناد إليه وما يحتاج إلى مزيد من البحث. [155]

الجدول المقارن: معايير التقييم وحدودها

حد الاستنتاج	الأداة	السؤال	المعيار
غياب النص لا يثبت المشروعية	تحليل قانوني	هل كان الحصول مأذوناً؟	المشروعية
تعدد المصادر لا يثبت الاستقلال	تحليل المصدر والمقارنة	هل المصدر والمنهج يسمحان بالاعتماد؟	الموثوقية
السلامة لا تثبت صحة المضمون	فحص فني وقيم تجزئة	هل البيانات أصلية ولم تتغير؟	السلامة الفنية
اكتمال التوثيق لا يثبت صحة النتائج	مراجعة وثائقية	هل الإجراءات موثقة؟	التوثيق
غياب الدليل لا يثبت الفرضية	تحليل نقدي	هل اختُبرت البدائل؟	الحياد المنهجي
عدم إمكان المراجعة لا يعني الخطأ	مراجعة مستقلة	هل يمكن إعادة الفحص؟	قابلية المراجعة

❖ النافذة التطبيقية

السيناريو: واقعة اعتداء على منشأة، مع تسجيلات كاميرا، صورة منشورة، وسجل دخول.

- **الخطوة الأولى (المشروعية):** التحقق من سند الحصول على التسجيلات (طلب مشروع للجهة الحائزة)، والصورة (منشورة للعموم، لكن المعالجة المنظمة تحتاج تقييمًا)، والسجل (طلب رسمي).
- **الخطوة الثانية (الأصالة):** فحص مصدر التسجيل (الجهاز، النظام، تاريخ الاستخراج)، والصورة (أصل النشر، إعادة التداول)، والسجل (النظام المنشئ، إعداداته الزمنية).
- **الخطوة الثالثة (السلامة):** قيم التجزئة للتسجيل، مقارنة نسخ الصورة، سجل تدقيق الدخول.
- **الخطوة الرابعة (الاستنتاج):** التمييز بين: ظهور شخص في التسجيل (ملاحظة)، وجود بطاقة مستخدمة (واقعة)، أن الموظف هو من دخل (استنتاج)، مسؤوليته (تقييم قانوني).
- **الخطوة الخامسة (البدائل):** هل البطاقة استخدمها غير صاحبها؟ هل التوقيت مختلف؟ هل الصورة قديمة؟
- **الخطوة السادسة (الإفصاح):** "لم يتسن التحقق من هوية مستخدم البطاقة"، "دقة توقيت الكاميرا تعتمد على إعداداتها".
- **الدرس:** التقييم المتكامل يمر بستة مستويات، وكل مستوى له حده.

النتائج العامة للفصل

١. معايير التقييم: المشروعية، الموثوقية، السلامة الفنية، التوثيق، الحياد المنهجي، قابلية المراجعة.
٢. المشروعية مستوى مستقل عن السلامة الفنية والقيمة الاستدلالية.
٣. تعدد المصادر لا يعني تعدد الأدلة المستقلة.
٤. سلامة البيانات لا تثبت صحة المضمون، وقيم التجزئة تثبت التطابق لا الأصالة.
٥. اختيار الحالات يجب أن يخضع لضوابط: الارتباط بالإشكالية، كفاية المعلومات، إمكان التحقق، التنوع، حدود التعميم.
٦. الحالات الافتراضية تختبر المنهج ولا تثبت وقوع قصور فعلي.
٧. مصفوفة التقييم تمنع الانتقال من الملاحظة إلى الحكم دون حلقة استدلالية.
٨. تقييم الأساس القانوني يتطلب فحص كل إجراء على حدة.
٩. فحص الأصالة والسلامة وظيفتان مستقلتان.
١٠. اختبار الاستنتاجات يتطلب تفكيكها واختبار البدائل.
١١. التمييز بين الارتباط والسببية ضروري.
١٢. الإفصاح عن عدم اليقين شرط للموضوعية.
١٣. أوجه القصور قد تكون قانونية أو فنية أو منهجية أو توثيقية.
١٤. صلاحية النتائج تتوقف على الغرض والمرحلة والمشروعية والسلامة.
١٥. حدود التعميم ضرورية لتجنب الأحكام الواسعة غير المسندة.

المراجع:

- (1) انظر: عادل عبد العال خراشي، ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي، ٢٠٠٦، ص ٤٠٠-٤٠٥.
- (2) انظر: الأمم المتحدة، العهد الدولي الخاص بالحقوق المدنية والسياسية، ١٩٦٦، المادة ١٧.
- (3) انظر: Berkeley Protocol on Digital Open Source Investigations, 2022, at 30-32.
- (4) انظر: NIST, Secure Hash Standard, FIPS PUB 180-4, 2015.
- (5) انظر: هشام مصطفى محمد، التحريات الأمنية وأثرها في الأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٥، ص ٣٠٠-٣٠٥.
- (6) انظر: NIST, Digital Evidence Preservation, NISTIR 8387, 2022, at 2-1.
- (7) انظر: NIST, Guide to Integrating Forensic Techniques into Incident Response, NIST SP 800-86, 2006.
- (8) انظر: محمد محمد سيف شجاع، شرح قانون الإجراءات الجزائية اليمني، مكتبة الصادق، صنعاء، ٢٠٠٥.
- (9) انظر: Berkeley Protocol, supra note 3, at 240-245.
- (10) انظر: خراشي، مرجع سابق، ص ٤١٠-٤١٥.

- (11) انظر: هشام مصطفى، مرجع سابق، ص ٥٠٥-٥٠٠.
- (12) انظر: شجاع، مرجع سابق.
- (13) انظر: خراشي، مرجع سابق، ص ٤٢٠-٤٢٥.
- (14) انظر. NISTIR 8387, *supra* note 6, at 3-1 :
- (15) انظر. Berkeley Protocol, *supra* note 3, at 50-55 :
- (16) انظر: شجاع، مرجع سابق.
- (17) انظر: خراشي، مرجع سابق، ص ٤٣٠-٤٣٥.
- (18) انظر: هشام مصطفى، مرجع سابق، ص ٥١٠-٥١٥.
- (19) انظر: المرجع السابق، ص ٥١٥-٥٢٠.
- (20) انظر: خراشي، مرجع سابق، ص ٤٤٠-٤٤٥.
- (21) انظر: شجاع، مرجع سابق.
- (22) انظر. Berkeley Protocol, *supra* note 3, at 60-65 :
- (23) انظر: هشام مصطفى، مرجع سابق، ص ٥٢٠-٥٢٥.
- (24) انظر: المرجع السابق، ص ٥٢٥-٥٣٠.
- (25) انظر: خراشي، مرجع سابق، ص ٤٥٠-٤٥٥.
- (26) انظر: شجاع، مرجع سابق.
- (27) انظر: هشام مصطفى، مرجع سابق، ص ٥٣٠-٥٣٥.
- (28) انظر: خراشي، مرجع سابق، ص ٤٦٠-٤٦٥.
- (29) انظر: شجاع، مرجع سابق.
- (30) انظر: خراشي، مرجع سابق، ص ٤٧٠-٤٧٥.
- (31) انظر. NISTIR 8387, *supra* note 6, at 3-2 :
- (32) انظر. Berkeley Protocol, *supra* note 3, at 115-120 :
- (33) انظر: هشام مصطفى، مرجع سابق، ص ٥٤٠-٥٤٥.
- (34) انظر: خراشي، مرجع سابق، ص ٤٨٠-٤٨٥.
- (35) انظر. Berkeley Protocol, *supra* note 3, at 350-355 :
- (36) انظر: هشام مصطفى، مرجع سابق، ص ٥٥٠-٥٥٥.
- (37) انظر: خراشي، مرجع سابق، ص ٤٩٠-٤٩٥.
- (38) انظر: شجاع، مرجع سابق.
- (39) انظر: هشام مصطفى، مرجع سابق، ص ٥٦٠-٥٦٥.
- (40) انظر. Berkeley Protocol, *supra* note 3, at 25-30 :
- (41) انظر. NISTIR 8387, *supra* note 6, at 3-3 :
- (42) انظر. Berkeley Protocol, *supra* note 3, at 170-175 :
- (43) انظر. NIST SP 800-86, *supra* note 7, at 3-1 :
- (44) انظر. INTERPOL, *Guidelines for Digital Forensics First Responders*, at 10-12 :
- (45) انظر: شجاع، مرجع سابق.
- (46) انظر. Berkeley Protocol, *supra* note 3, at 35-40 :
- (47) انظر: هشام مصطفى، مرجع سابق، ص ٥٧٠-٥٧٥.
- (48) انظر: خراشي، مرجع سابق، ص ٥٠٥-٥٠٠.
- (49) انظر: شجاع، مرجع سابق.
- (50) انظر: هشام مصطفى، مرجع سابق، ص ٥٨٠-٥٨٥.
- (51) انظر. NISTIR 8387, *supra* note 6, at 3-4 :
- (52) انظر. Berkeley Protocol, *supra* note 3, at 170-175 :
- (53) انظر. NIST SP 800-86, *supra* note 7, at 3-2 :
- (54) انظر: خراشي، مرجع سابق، ص ٥١٠-٥١٥.
- (55) انظر. Berkeley Protocol, *supra* note 3, at 40-45 :
- (56) انظر: شجاع، مرجع سابق.
- (57) انظر: هشام مصطفى، مرجع سابق، ص ٥٩٠-٥٩٥.
- (58) انظر. INTERPOL, *supra* note 44, at 12-15 :
- (59) انظر: خراشي، مرجع سابق، ص ٥٢٠-٥٢٥.

- (60) انظر: هشام مصطفى، مرجع سابق، ص ٦٠٠-٦٠٥.
- (61) انظر: شجاع، مرجع سابق.
- (62) انظر. NISTIR 8387, *supra* note 6, at 3-5.
- (63) انظر. Berkeley Protocol, *supra* note 3, at 115-120.
- (64) انظر. NISTIR 8387, *supra* note 6, at 3-6.
- (65) انظر. NIST, *Secure Hash Standard*, *supra* note 4.
- (66) انظر. NISTIR 8387, *supra* note 6, at 3-7.
- (67) انظر. INTERPOL, *supra* note 44, at 15-18.
- (68) انظر. Berkeley Protocol, *supra* note 3, at 175-180.
- (69) انظر. NIST SP 800-86, *supra* note 7, at 3-3.
- (70) انظر. INTERPOL, *supra* note 44, at 18-20.
- (71) انظر. NISTIR 8387, *supra* note 6, at 3-8.
- (72) انظر. Berkeley Protocol, *supra* note 3, at 350-355.
- (73) انظر: هشام مصطفى، مرجع سابق، ص ٦١٠-٦١٥.
- (74) انظر: خراشي، مرجع سابق، ص ٥٣٠-٥٣٥.
- (75) انظر: شجاع، مرجع سابق.
- (76) انظر: هشام مصطفى، مرجع سابق، ص ٦٢٠-٦٢٥.
- (77) انظر. Berkeley Protocol, *supra* note 3, at 70-75.
- (78) انظر: المرجع السابق، at 240-245.
- (79) انظر: خراشي، مرجع سابق، ص ٥٤٠-٥٤٥.
- (80) انظر. NIST SP 800-86, *supra* note 7, at 3-4.
- (81) انظر. Berkeley Protocol, *supra* note 3, at 30-32.
- (82) انظر: شجاع، مرجع سابق.
- (83) انظر: هشام مصطفى، مرجع سابق، ص ٦٣٠-٦٣٥.
- (84) انظر. Berkeley Protocol, *supra* note 3, at 55-60.
- (85) انظر: المرجع السابق، at 240-245.
- (86) انظر: خراشي، مرجع سابق، ص ٥٥٠-٥٥٥.
- (87) انظر: هشام مصطفى، مرجع سابق، ص ٦٤٠-٦٤٥.
- (88) انظر. Berkeley Protocol, *supra* note 3, at 350-355.
- (89) انظر: المرجع السابق، at 240-245.
- (90) انظر: خراشي، مرجع سابق، ص ٥٦٠-٥٦٥.
- (91) انظر. Berkeley Protocol, *supra* note 3, at 350-355.
- (92) انظر: شجاع، مرجع سابق.
- (93) انظر: هشام مصطفى، مرجع سابق، ص ٦٥٠-٦٥٥.
- (94) انظر: خراشي، مرجع سابق، ص ٥٧٠-٥٧٥.
- (95) انظر: شجاع، مرجع سابق.
- (96) انظر: خراشي، مرجع سابق، ص ٥٨٠-٥٨٥.
- (97) انظر. NISTIR 8387, *supra* note 6, at 3-9.
- (98) انظر. INTERPOL, *supra* note 44, at 20-22.
- (99) انظر. Berkeley Protocol, *supra* note 3, at 175-180.
- (100) انظر. NIST SP 800-86, *supra* note 7, at 3-5.
- (101) انظر: خراشي، مرجع سابق، ص ٥٩٠-٥٩٥.
- (102) انظر: هشام مصطفى، مرجع سابق، ص ٦٦٠-٦٦٥.
- (103) انظر: المرجع السابق، ص ٦٦٥-٦٧٠.
- (104) انظر: خراشي، مرجع سابق، ص ٦٠٠-٦٠٥.
- (105) انظر: شجاع، مرجع سابق.
- (106) انظر. NISTIR 8387, *supra* note 6, at 3-10.
- (107) انظر: خراشي، مرجع سابق، ص ٦١٠-٦١٥.
- (108) انظر: هشام مصطفى، مرجع سابق، ص ٦٧٠-٦٧٥.

- (109) انظر: خراشي، مرجع سابق، ص ٦٢٠-٦٢٥.
- (110) انظر: شجاع، مرجع سابق.
- (111) انظر. NISTIR 8387, *supra* note 6, at 3-11.
- (112) انظر: المرجع السابق، 3-12 at
- (113) انظر. Berkeley Protocol, *supra* note 3, at 40-45.
- (114) انظر: هشام مصطفى، مرجع سابق، ص ٦٨٠-٦٨٥.
- (115) انظر: خراشي، مرجع سابق، ص ٦٣٠-٦٣٥.
- (116) انظر: شجاع، مرجع سابق.
- (117) انظر: خراشي، مرجع سابق، ص ٦٤٠-٦٤٥.
- (118) انظر: هشام مصطفى، مرجع سابق، ص ٦٩٠-٦٩٥.
- (119) انظر: المرجع السابق، ص ٧٠٠-٧٠٥.
- (120) انظر: شجاع، مرجع سابق.
- (121) انظر. Berkeley Protocol, *supra* note 3, at 115-120.
- (122) انظر. INTERPOL, *supra* note 44, at 25-28.
- (123) انظر. NISTIR 8387, *supra* note 6, at 3-13.
- (124) انظر. Berkeley Protocol, *supra* note 3, at 240-245.
- (125) انظر: المرجع السابق، 350-355 at
- (126) انظر: هشام مصطفى، مرجع سابق، ص ٧١٠-٧١٥.
- (127) انظر. NISTIR 8387, *supra* note 6, at 3-14.
- (128) انظر: خراشي، مرجع سابق، ص ٦٥٠-٦٥٥.
- (129) انظر: شجاع، مرجع سابق.
- (130) انظر: هشام مصطفى، مرجع سابق، ص ٧٢٠-٧٢٥.
- (131) انظر: خراشي، مرجع سابق، ص ٦٦٠-٦٦٥.
- (132) انظر: شجاع، مرجع سابق.
- (133) انظر: هشام مصطفى، مرجع سابق، ص ٧٣٠-٧٣٥.
- (134) انظر. NISTIR 8387, *supra* note 6, at 3-15.
- (135) انظر: خراشي، مرجع سابق، ص ٦٧٠-٦٧٥.
- (136) انظر: شجاع، مرجع سابق.
- (137) انظر. Berkeley Protocol, *supra* note 3, at 350-355.
- (138) انظر. NISTIR 8387, *supra* note 6, at 3-16.
- (139) انظر: هشام مصطفى، مرجع سابق، ص ٧٤٠-٧٤٥.
- (140) انظر. Berkeley Protocol, *supra* note 3, at 355-360.
- (141) انظر: خراشي، مرجع سابق، ص ٦٨٠-٦٨٥.
- (142) انظر: هشام مصطفى، مرجع سابق، ص ٧٥٠-٧٥٥.
- (143) انظر: خراشي، مرجع سابق، ص ٦٩٠-٦٩٥.
- (144) انظر. Berkeley Protocol, *supra* note 3, at 50-55.
- (145) انظر: شجاع، مرجع سابق.
- (146) انظر: خراشي، مرجع سابق، ص ٧٠٠-٧٠٥.
- (147) انظر. NISTIR 8387, *supra* note 6, at 3-17.
- (148) انظر: هشام مصطفى، مرجع سابق، ص ٧٦٠-٧٦٥.
- (149) انظر: خراشي، مرجع سابق، ص ٧١٠-٧١٥.
- (150) انظر. Berkeley Protocol, *supra* note 3, at 60-65.
- (151) انظر: شجاع، مرجع سابق.
- (152) انظر: هشام مصطفى، مرجع سابق، ص ٧٧٠-٧٧٥.
- (153) انظر: خراشي، مرجع سابق، ص ٧٢٠-٧٢٥.
- (154) انظر: شجاع، مرجع سابق.
- (155) انظر: هشام مصطفى، مرجع سابق، ص ٧٨٠-٧٨٥.

الفصل الرابع: التحديات ومقترحات تطوير الإطار القانوني والممارسة المهنية

المبحث الأول: التحديات القانونية والحقوقية

المطلب الأول: القصور أو الغموض في القواعد المنظمة للتحريات الرقمية

تشير التحريات الأمنية الرقمية إشكالية قانونية تتجاوز البحث عن سند تشريعي يجيز استخدام الوسائل التقنية؛ إذ تتعلق بمدى قدرة القواعد التقليدية على استيعاب أنماط جمع المعلومات ومعالجتها في بيئة تتسم بسرعة التطور التقني، وتداخل الاختصاصات، وتعدد مصادر البيانات. [1] فالتحدي لا يكمن بالضرورة في غياب النص، وإنما في **عمومية الأحكام**، أو **تشتملها بين تشريعات متعددة**، أو **عدم وضوح الحدود** بين أعمال التحري المسموح بها والإجراءات التي تستلزم ضمانات مشددة. [2]

وتستند مشروعية التحريات، في النظم التي تخضع لمبدأ سيادة القانون، إلى ضرورة وجود أساس قانوني يحدد الجهة المختصة، والغرض المشروع، ونطاق السلطات، والقيود. ولا يكفي أن تكون الوسيلة التقنية قادرة على تحقيق غرض أمني حتى يصبح استخدامها جائزاً؛ لأن **القدرة التقنية لا تنشئ اختصاصاً قانونياً**، كما أن عدم وجود حظر تقني لا يعني الجواز القانوني. [3]

وتتجلى صعوبة التنظيم في أن **الوسيلة الرقمية الواحدة قد تؤدي وظائف مختلفة** بحسب طريقة استخدامها. فمشاهدة محتوى منشور تختلف عن إنشاء نظام للمراقبة المستمرة، كما يختلف الاطلاع على بيانات متاحة عن الوصول إلى مراسلات خاصة. وإخضاع جميع هذه الصور لحكم واحد قد يؤدي إلى التوسع غير المبرر أو إلى قيود متطابقة على إجراءات مختلفة. [4]

وتؤكد المعايير الدولية أن التدخل في الخصوصية ينبغي أن يستند إلى القانون، وأن يكون مبرراً بهدف مشروع، وأن يراعي الضرورة والتناسب. وقد قررت المادة ١٧ من **العهد الدولي لحماية الأفراد من التدخل التعسفي أو غير القانوني**. [5] ويترتب على ذلك أن التنظيم لا ينبغي أن يقتصر على تحديد الوسائل المسموح بها، بل يجب أن يضبط شروط استخدامها، والجهات المخولة، ومدتها، وكيفية مراجعة نتائجها، وضمانات الأشخاص. [6]

ويزداد الإشكال عندما تعتمد التحريات على أدوات تتغير وظائفها بسرعة. فقد تظهر وسائل جديدة لتحليل الصور أو ربط قواعد البيانات دون أن تكون النصوص القائمة قد تناولت خصائصها. ولا يعني ذلك ضرورة تعديل التشريعات مع كل تطور تقني؛ لأن هذا النهج قد يؤدي إلى تشريعات متقادمة. والأجدى هو **وضع قواعد عامة واضحة** تحكم الغرض والاختصاص والضرورة والتناسب والرقابة، مع لوائح فنية قابلة للتحديث. [7]

ويجب التمييز بين **المرونة التشريعية والغموض القانوني**. فالمرونة تسمح بتطبيق القاعدة على وسائل مستحدثة دون التخلي عن الضمانات، أما الغموض فيترك تحديد حدود السلطة لتقدير غير منضبطة. والتطوير المطلوب ينبغي أن يحقق معادلة تجمع بين قابلية القواعد للتكيف، وإمكان توقع الأفراد للآثار القانونية. [8]

وتظهر أهمية ذلك في اتفاقية بودابست بشأن الجريمة السيبرانية، التي أُرست إطاراً للتعاون الدولي ونظمت إجراءات متعلقة بالأدلة الإلكترونية، مع إحالة عدد من الضمانات إلى القانون الوطني. [9] غير أن أحكامها لا ينبغي أن تُفهم باعتبارها تفويضاً عاماً باستخدام كل وسيلة رقمية؛ إذ يتعين التمييز بين التدابير التي تنظمها في نطاقها، وبين أعمال التحري الأمني التي قد تخضع لأطر أخرى. [10]

وعليه، فإن معالجة القصور التشريعي تستلزم مراجعة القواعد من حيث وضوح الاختصاصات، وتحديد درجات التدخل، وضبط شروط الوصول، وتقرير ضمانات المراجعة والمساءلة، مع تجنب الخلط بين تنظيم الوسيلة وصلاحيه النتائج للاعتماد في الإثبات. [11]

المطلب الثاني: التداخل بين الاختصاصات الأمنية والقضائية والفنية

لا تنفصل سلامة التحريات عن وضوح توزيع الاختصاصات بين الجهات التي تجمع المعلومات، والتي تحقق، والتي تفحص فنياً، والتي تملك سلطة تقدير الأدلة. فالتداخل قد يؤدي إلى تجاوز الاختصاص، أو ضعف الرقابة، أو إسناد نتائج فنية إلى جهات لا تملك تقييمها، أو الخلط بين جمع المعلومات لأغراض أمنية واتخاذ إجراء جزائي. [12]

أربع وظائف مترابطة لكنها غير متطابقة:

١. جمع المعلومات: الحصول على معلومات أولية من مصادر مشروعة. [13]
 ٢. التقييم الأمني: ربط المعلومات واختبار موثوقيتها وتقدير دلالتها. [14]
 ٣. التحقيق والإجراء الجزائي: يخضع للقواعد الإجرائية التي تحدد شروط التفتيش والضبط. [15]
 ٤. الفحص الفني والخبرة: التحقق من الأصالة والسلامة وتفسير الخصائص التقنية، دون حلول محل التقدير القانوني. [16]
- ولا يعني استقلال هذه الوظائف ضرورة الفصل التنظيمي الكامل؛ فقد تتطلب الممارسة تنسيقاً. غير أن التنسيق ينبغي ألا يؤدي إلى إلغاء الحدود القانونية أو السماح لجهة بممارسة صلاحيات لا يخولها القانون. [17]
- وتبرز المشكلة عندما تبدأ الواقعة مسألة أمنية ثم تتطور إلى شبهة جنائية. ففي هذه الحالة، قد يكون جمع المعلومات الأولية مشروعا في إطار الاختصاص الأمني، لكن استمرار الإجراء أو الانتقال إلى بيانات محمية قد يستلزم سندا مختلفاً أو إذنًا. ومن ثم، فإن تغير طبيعة الواقعة يقتضي إعادة تقييم الأساس القانوني، بدل افتراض استمرار الصلاحيات. [18]
- كما يظهر التداخل في العلاقة بين القائم بالتحري والخبراء. فإذا حُددت مهمة الخبير على أساس إثبات فرضية مسبقاً، أو طُلب منه تقرير مسؤولية شخص دون تمكينه من فحص البدائل، فإن استقلال الفحص يتعرض للخطر. [19]

وتتصل المسألة بمبدأ الفصل بين سلطات التحقيق والحكم، وبضرورة صيانة استقلال التقييم القضائي. وقد شددت مبادئ الأمم المتحدة الأساسية بشأن استقلال السلطة القضائية على أهمية استقلال القضاء عن التأثيرات غير الملائمة. [20] ولا تتعلق هذه المبادئ مباشرة بكل تفاصيل التحريات، لكنها توفر إطاراً يقتضي ألا يتحول التقرير الأمني أو الفني إلى نتيجة ملزمة لجهة الفصل. [21]

ومن الناحية العملية، يمكن الحد من التداخل من خلال تحديد المسؤوليات في كل مرحلة، وتوثيق الجهة التي اتخذت القرار، والأساس القانوني، والجهة التي نفذت، والجهة التي فحصت فنياً، والجهة المخولة بتقييم النتائج. ويجب أن يكون هذا التحديد واضحاً بما يسمح بتتبع القرار ومراجعته. [22]

كذلك ينبغي ألا يفهم التعاون المؤسسي على أنه مبرر لتبادل البيانات دون قيود. فكل جهة تتلقى معلومات ينبغي أن تتحقق من مشروعية تلقيها، ومدى ارتباطها باختصاصها، والغرض، والقيود التي تظل ملازمة لها. ولا يؤدي نقل البيانات إلى تصحيح عيب سابق، كما لا يضمن صحة الاستنتاجات. [23]

وعليه، فإن معالجة التداخل تقتضي الانتقال من التنسيق العام إلى توزيع وظيفي دقيق، يحدد مسؤولية كل جهة، ويضمن استقلال التقييم الفني والقانوني، ويتيح الرقابة على انتقال المعلومات. [24]

المطلب الثالث: التوازن بين متطلبات التحري والحقوق والحريات

يمثل التوازن بين الأمن وحماية الحقوق أحد أكثر التحديات تعقيداً؛ لأن الوسائل الرقمية قد تتيح جمع معلومات واسعة، وربط بيانات كانت منفصلة، واستنتاج أنماط لم يكن الوصول إليها ممكناً بالوسائل التقليدية. [25]

ولا تقتصر الخطورة على جمع معلومات عن شخص محدد، بل تمتد إلى جمع بيانات عن أشخاص لم يكونوا محل التحري، أو الاحتفاظ بمعلومات تتجاوز الغرض، أو إعادة تحليل البيانات في سياقات مختلفة. وبذلك قد يتحول إجراء محدود في نطاقه الظاهر إلى تدخل واسع إذا لم تُضبط مراحل الجمع والمعالجة والحفظ والاستخدام. [26]

ولا يجوز اختزال التوازن في مقابلة مجردة بين الأمن والخصوصية؛ إذ إن حماية الحقوق ليست بالضرورة عائقاً أمام الفعالية، بل قد تكون شرطاً لتعزيز الموثوقية والقبول المؤسسي والقانوني. فالإجراءات الخاضعة لضوابط واضحة، والموثقة، والمراجعة مستقلة، تكون أكثر قابلية للتحقق والمساءلة. [27]

ويقتضي مبدأ التناسب تقييم التدخل وفق ثلاثة مستويات: ملائمة الوسيلة، وضرورة استخدامها بالنظر إلى بدائل أقل مساساً، ثم تناسب الأثر مع أهمية الهدف. ولا يكفي إثبات أن الوسيلة مفيدة؛ إذ يجب بيان سبب الحاجة إليها، ولماذا لا تكفي وسيلة أقل تدخلاً. [28]

وتزداد أهمية هذه المعايير في حالات المراقبة المستمرة أو التحليل الآلي واسع النطاق. فقد تكون مشاهدة محتوى متاح مشروعة، بينما يثير جمع المحتوى ذاته بصورة منهجية وربطه ببيانات أخرى مسائل مختلفة تتعلق بحجم المعالجة والغرض والآثار. [29]

وقد أكدت المفوضية السامية للأمم المتحدة لحقوق الإنسان في تقريرها بشأن الحق في الخصوصية أهمية إخضاع تدابير المراقبة لمتطلبات المشروعية والضرورة والتناسب والرقابة. [30] وينظر هذا الإطار إلى الخصوصية بوصفها حقاً يتأثر بطبيعة التدخل ومداه وسياقه، لا بمجرد كون المعلومة جُمعت في مكان عام. [31]

ومن ثم، فإن التوازن لا يتحقق بمنع الوسائل مطلقاً، ولا بمنح سلطة مفتوحة، بل بإخضاع كل وسيلة لتقييم يتناسب مع درجة تدخلها. فكلما زادت القدرة على كشف تفاصيل الحياة الخاصة أو تتبع الأشخاص، تعاظمت الحاجة إلى ضمانات أكثر تحديداً. [32]

كما يتعين مراعاة الحقوق المرتبطة بالمعلومات المستخلصة، ومنها حماية البيانات الشخصية، وعدم التمييز، وحرية التعبير، وضمانات المحاكمة العادلة عند انتقال المعلومات إلى المجال الجزائي. [33]

وتتطلب المعالجة العملية تقييماً مسبقاً للمخاطر في الإجراءات ذات الأثر المرتفع، وتحديد نطاق الوصول، وتقليل البيانات غير المرتبطة، وتقييد الاستخدامات الثانوية، ووضع مدد للاحتفاظ، وضمان مراجعة القرارات التي تنطوي على تدخل جوهري. [34]

المطلب الرابع: التحديات المتعلقة بالبيانات العابرة للحدود

تفرض الطبيعة العابرة للحدود صعوبات تتصل بتحديد القانون الواجب التطبيق، والجهة المختصة بطلب البيانات، وسلطة الدولة في الوصول إلى معلومات مخزنة خارج إقليمها، ومدى جواز نقل البيانات بين الدول. [35] فقد توجد البيانات في خوادم موزعة، أو تُدار من خلال مقدم خدمة يقع مقره في دولة مختلفة، أو تمر عبر بنية لا تكشف بسهولة عن موقع التخزين. [36]

ويترتب على ذلك أن تحديد الموقع الجغرافي لا يكفي وحده لتحديد الاختصاص. فقد تتداخل صلة البيانات بالإقليم، ومكان مقدم الخدمة، وجنسية الأشخاص، ومكان الجريمة، والالتزامات الدولية. ويقتضي ذلك التمييز بين القدرة التقنية على الوصول والسلطة القانونية التي تجيزه. [37]

كما أن طلب البيانات من مقدم خدمة أجنبي قد يخضع لقواعد مختلفة. وقد يتطلب اتباع إجراءات تعاون قضائي دولي، أو الاستناد إلى اتفاقية نافذة، أو آلية قانونية محددة. ولا يجوز افتراض أن الاختصاص الداخلي وحده يكفي لتجاوز القيود المطبقة في الدولة التي توجد فيها البيانات. [38]

وتوفر اتفاقية بودابست إطاراً للتعاون الدولي في الأدلة الإلكترونية، بما في ذلك آليات للمساعدة المتبادلة. كما يتناول البروتوكول الإضافي الثاني تعزيز التعاون والإفصاح، مع مراعاة الشروط والضمانات. [39] غير أن نطاق الاستفادة يتوقف على انطباق الاتفاقية أو البروتوكول على الدول المعنية. [40]

وتنشأ صعوبة من تعارض المتطلبات القانونية بين الدول. فقد يسمح قانون دولة بنقل بيانات وفق شروط، بينما يفرض قانون آخر قيوداً إضافية. وفي هذه الحالة، لا يكفي التركيز على قانون الجهة الطالبة، بل ينبغي فحص الأساس القانوني للنقل، وصفة الجهة المستقبلة، والغرض، والضمانات المتعلقة بالسرية والحفظ والإتلاف.[41]

كذلك ينبغي التمييز بين نقل البيانات لغرض التحقيق في جريمة محددة وتبادل المعلومات الأمنية لأغراض وقائية. فقد تختلف القواعد المنظمة لكل منهما، ولا يجوز افتراض أن آليات الأدلة الجنائية تنطبق تلقائياً على تبادل المعلومات الأمنية.[42]

ويقتضي التعامل السليم تحديد قناة التعاون القانونية المناسبة، وتوثيق الطلبات والاستجابات، وتقييد البيانات المتبادلة بالغرض المعلن، والتحقق من شروط إعادة استخدامها. كما يجب أن تراعي ترتيبات التعاون حماية الحقوق الأساسية.[43]

المبحث الثاني: التحديات التقنية والمؤسسية

المطلب الأول: التلاعب بالمحتوى الرقمي وحدود الكشف الآلي

أدى التطور في تقنيات تحرير الصور وتوليد المحتوى الاصطناعي إلى زيادة صعوبة التحقق من أصالة المواد الرقمية، ولا سيما عند عرضها خارج سياقها أو إعادة نشرها بعد تعديلها. ولم تعد المشكلة مقتصرة على التلاعب التقليدي، بل امتدت إلى إمكان إنشاء محتوى يحاكي الأشخاص والأصوات بدرجات متفاوتة من الإقناع.[44]

ثلاثة أسئلة فنية مستقلة:

١. هل تعرض المادة الرقمية مؤشرات على التعديل؟[45]

٢. هل يمكن تحديد مصدر المادة والتحقق من سياقها الزمني والمكاني؟[46]

٣. هل تعكس المادة واقعة حقيقية على النحو الذي يُستنتج منها؟[47]

لا تكفي الإجابة عن السؤال الأول لحسم الآخرين؛ فقد تكون المادة معدلة لأغراض مشروعة دون أن يكون مضمونها كاذباً، وقد تكون غير متضمنة لمؤشرات واضحة مع أنها أنشئت اصطناعياً.[48]

وتعتمد أدوات الكشف الآلي على مؤشرات قد تتأثر بنوعية البيانات، وطريقة الضغط، ودقة التسجيل، وأدوات التحرير، والتطور المستمر في أساليب التوليد. ولذلك فإن نتائجها ينبغي أن تُفهم في حدود قدراتها المعروفة، لا باعتبارها أحكاماً نهائية.[49]

وتشير إرشادات **NIST** بشأن التزييف العميق إلى أهمية تقييم أساليب الكشف في ضوء طبيعة التهديدات، وبيئات الاختبار، ومحدودية التعميم من نتائج الاختبارات إلى جميع أنواع المحتوى.[50] ومن ثم، لا يصح التعامل مع نسبة الثقة التي ينتجها نظام آلي على أنها احتمال قانوني محسوم، ما لم يكن معنى تلك النسبة وطريقة احتسابها معروفة.[51]

وتظهر الخطورة عندما يُستخدم ناتج الأدوات لتوجيه الاتهام أو استبعاد رواية دون فحص مستقل. فقد تؤدي **الإيجابيات الكاذبة** إلى وصف مادة صحيحة بأنها مزيفة، كما قد تؤدي **السلبات الكاذبة** إلى عدم اكتشاف تلاعب فعلي. [52]

ولذلك ينبغي أن يجمع التحقق بين فحص الخصائص الفنية، والتحقق من المصدر والسياق، والمقارنة بمصادر مستقلة، وفحص البيانات الوصفية، والنظر في التفسيرات البديلة. كما ينبغي توثيق الأدوات وإصداراتها، وظروف الفحص، والنتائج السلبية والإيجابية، والقيود. [53]

ولا ينبغي أن يقتصر التحقق على البحث عن مؤشرات تؤيد الاشتباه، بل يجب أن يشمل البحث عن مؤشرات قد تنفيه أو تدعم تفسيراً بديلاً. فالمهمة العلمية ليست تأكيد فرضية أولية، وإنما اختبارها. [54]

المطلب الثاني: أثر التحيز والأخطاء التقنية في النتائج

لا تنشأ الأخطاء من خلل الأجهزة أو البرامج وحده، بل قد تنتج من طريقة اختيار البيانات، وتصميم التحليل، وتفسير النتائج، والتعامل مع المعلومات المخالفة للتوقعات. [55]

ويظهر **التحيز التأكيدي** عندما يبحث المحلل عن المعلومات التي تؤيد فرضيته، أو يمنحها وزناً أكبر، أو يفسر الغموض لمصلحة النتيجة المتوقعة. وقد يتعزز عندما يتلقى المحلل معلومات مسبقة عن هوية الشخص محل التحري. [56]

كما يمكن أن ينشأ التحيز من **طريقة بناء قواعد البيانات** أو اختيار العينات المستخدمة في تدريب الأنظمة الآلية. فإذا كانت البيانات لا تمثل الفئات أو الظروف التي سيستخدم النظام فيها، فقد تتفاوت معدلات الخطأ. [57]

ولا يكفي إعلان أن التحليل أُجري باستخدام برنامج معروف لإثبات صحة النتيجة. فصحة المخرجات تتوقف على ملاءمة الأداة للمهمة، وجودة البيانات، وصحة الإعدادات، وفهم القيود، وإمكان تكرار الفحص. [58]

وقد أصدرت **المنظمة الدولية للتقييس المعيار ISO/IEC 23894:2023** بشأن إدارة مخاطر الذكاء الاصطناعي، وهو إطار يساعد المؤسسات على تحديد المخاطر وتحليلها ومعالجتها ومراجعتها. [59] ويمكن الاستفادة من مبادئ إدارة المخاطر في التحريات الرقمية، دون اعتبار المعيار بذاته سنداً قانونياً. [60]

ويتطلب الحد من التحيز **الفصل بين المعلومات الضرورية لتنفيذ الفحص والافتراضات المتعلقة بنتيجته**، وتحديد معايير التقييم مسبقاً، وتسجيل القرارات التحليلية، واختبار الفرضيات البديلة، وإخضاع النتائج الحساسة لمراجعة مستقلة. [61]

ويجب تجنب الخلط بين **تكرار النتيجة وتأكيد صحتها**؛ إذ قد تنتج أدوات متعددة نتائج متشابهة إذا كانت تعتمد على البيانات نفسها أو افتراضات مشتركة. ولذلك فإن التحقق المستقل ينبغي أن يراعي استقلال المصادر وطرق الفحص. [62]

ومن الناحية المؤسسية، ينبغي إنشاء آليات لتسجيل الأخطاء وتصنيفها وتحليل أسبابها، بحيث لا تُعالج كحالات فردية معزولة، بل كمؤشرات على قصور في التدريب أو الإجراءات أو تصميم الأنظمة. [63]

المطلب الثالث: الكفاءات والموارد الفنية اللازمة للتحري الرقمي

تتطلب التحريات الرقمية كفاءات تجمع بين المعرفة القانونية والفهم التقني والقدرة التحليلية. فالمعرفة التقنية وحدها لا تكفي لتحديد المشروعية، كما أن المعرفة القانونية وحدها لا تكفي لتقييم سلامة النسخ أو حدود الأدوات. [64] ويؤدي غياب التكامل إلى احتمال اتخاذ قرارات صحيحة تقنياً لكنها غير مشروعة، أو إجراءات مشروعة لكن نتائجها غير موثوقة. [65]

الكفاءات المطلوبة:

- جمع المعلومات من المصادر المتاحة، والتحقق من مصدرها، وتوثيق ظروف الحصول عليها. [66]

- فهم خصائص البيانات الوصفية، والمحافظة على سلامة النسخ. [67]

- تقييم موثوقية المصادر، وإعداد التقارير التي تميز بين الوقائع والاستنتاجات والفرضيات. [68]

- فهم حدود الاختصاص: متى يتطلب الوصول إذنًا، ومتى تتجاوز المسألة القدرة الفنية، ومتى يتجاوز الخبر حدوده. [69]

ولا يتحقق التأهيل بدورات تقنية قصيرة فقط، بل يتطلب برامج مستمرة تربط المعرفة النظرية بالتطبيق، وتدريب على الحالات التي تتضمن بيانات ناقصة أو متعارضة، وعلى اكتشاف الأخطاء، وتقييم الفرضيات البديلة، وإعداد تقارير قابلة للمراجعة. [70]

الموارد الضرورية: البنية التحتية لحفظ البيانات بأمان، وأدوات الفحص المعتمدة، وأنظمة إدارة الصلاحيات، والسجلات التي تتيح معرفة من وصل إلى البيانات ومتى، والقدرة على إجراء مراجعات مستقلة. وقد يؤدي نقص الموارد إلى استخدام أدوات غير مناسبة، أو تأخير الفحص، أو فقدان البيانات. [71]

غير أن شراء أدوات متقدمة لا يعالج وحده القصور المؤسسي. فقد تمتلك الجهة نظاماً متطوراً، لكنها تفتقر إلى قواعد واضحة لاستخدامه، أو إلى أشخاص مؤهلين لتفسير نتائجه، أو إلى آليات لمراجعة الأخطاء. ومن ثم، ينبغي أن يُبنى الاستثمار التقني على تقييم للاحتياجات والمخاطر، وأن يُربط بالتدريب والحوكمة وضمان الجودة. [72]

وتقتضي الإدارة الرشيدة تحديد الوظائف التي تتطلب خبرة متخصصة، والوظائف التي يمكن أن يؤديها موظفون مدربون وفق إجراءات موحدة، مع آليات واضحة للإحالة إلى الخبراء. كما ينبغي تجنب الاعتماد الكامل على مورد تقني خارجي في مسائل لا تستطيع الجهة فهم نتائجها أو مراجعتها. [73]

المطلب الرابع: التنسيق المؤسسي وتوحيد إجراءات التوثيق وضمان الجودة

يعد التنسيق المؤسسي عنصراً أساسياً، لأن المعلومات قد تنتقل بين جهة تجمعها، وأخرى تحفظها، وثالثة تفحصها، ورابعة تستخدم نتائجها. وإذا لم تُحدد مسؤوليات كل جهة وقواعد التسليم والتوثيق، فقد تنشأ فجوات تحول دون التحقق من المصدر أو سلامة البيانات أو قانونية الاستخدام. [74]

ولا يقتصر التنسيق على تسهيل التبادل، بل يشمل **توحيد الحد الأدنى من متطلبات التوثيق**، وتحديد البيانات التي يجب أن ترافق كل عملية تسليم، وتسجيل القيود القانونية والفنية، وضمان بقاء سجل واضح يبين مراحل التعامل. [75]

ويجب التمييز بين **توحيد الإجراءات وتوحيد التقدير القانوني**. فتوحيد نماذج تسجيل المصدر والتوقيت والأداة يساعد على رفع الجودة، لكنه لا يعني أن كل إجراء يخضع للضوابط ذاتها. إذ تظل المشروعية مرتبطة بالقانون المختص، وطبيعة البيانات، والجهة، والغرض. [76]

كما أن التوثيق لا يقتصر على تسجيل ما حدث، بل ينبغي أن يسمح **بإعادة بناء المسار** الذي أدى إلى النتيجة. فإذا ورد في التقرير أن حساباً نشر محتوى، وجب أن يكون بالإمكان تحديد مصدر المحتوى، وتاريخ الحصول، والطريقة التي جرى بها التحقق من نسبته، والقيود. [77]

وتوفر معايير المختبرات وجهات الفحص، ومنها **ISO/IEC 17025:2017**، إطاراً عاماً للكفاءة الفنية والحياد واتساق التشغيل. ويمكن الاستفادة من مبادئ الكفاءة والتوثيق وضبط الجودة في تطوير إجراءات الفحص الرقمي، مع ضرورة التحقق من انطباق المعيار على نوع النشاط، وعدم افتراض أن اتباع بعض متطلباته يمنح النتائج صفة الدليل المقبول قانوناً. [78]

ومن الضروري **الفصل بين المراجعة الإدارية والمراجعة الفنية**. فالمراجعة الإدارية تتحقق من الالتزام بالإجراءات والصلاحيات، بينما تتناول الفنية صحة المنهج والأدوات والاستنتاجات. وقد يكون الإجراء مستوفياً للنموذج الإداري لكنه معيب فنياً، كما قد تكون النتيجة معقولة رغم نقص في التوثيق. [79]

ويستحسن أن تتضمن المنظومة إجراءات للتعامل مع الأخطاء، تشمل تسجيلها، وتحديد أثرها، وتصحيح النتائج، وإخطار الجهات المعنية إذا كان الخطأ قد أثر في قرار سابق. فإخفاء الخطأ أو الاكتفاء بتصحيح النسخة النهائية دون توثيق التعديل يضعف الثقة. [80]

وعليه، فإن توحيد إجراءات التوثيق وضمان الجودة ينبغي أن يستهدف **بناء مسار معلوماتي قابل للتتبع والمراجعة**، دون أن يحل محل الرقابة القانونية أو التقييم المستقل. [81]

المبحث الثالث: مقترحات التطوير والحوكمة

المطلب الأول: تطوير تنظيم الاختصاصات وشروط استخدام وسائل التحري

يتطلب تطوير الإطار القانوني اعتماد تنظيم يحدد الاختصاصات وفق طبيعة الإجراء وآثاره، بدل الاكتفاء بتفويض عام. فكلما كانت الوسيلة أكثر قدرة على كشف الحياة الخاصة أو الوصول إلى بيانات محمية أو إنشاء سجل مستمر، ازدادت الحاجة إلى تحديد شروط استخدامها بدقة. [82]

ويبدأ التطوير بتحديد الفئات الأساسية للإجراءات الرقمية، والتميز بين جمع المعلومات المتاحة، والوصول إلى البيانات المقيدة، والمراقبة المستمرة، وفحص الأجهزة، وتحليل البيانات على نطاق واسع. ولا ينبغي أن تكون هذه التصنيفات تقنية محضة، بل يجب أن تراعي طبيعة التدخل، ونطاق البيانات، والمدة، والآثار المحتملة. [83]

كما ينبغي تحديد الجهة المختصة باتخاذ القرار، والجهة المخولة بالتنفيذ، والحالات التي تستلزم إذنًا قضائيًا أو تصريحاً، والضوابط عند تغيير نطاق التحري. ويجب أن يكون واضحاً أن الإذن بإجراء معين لا يجيز تلقائياً إجراءات أخرى تختلف في طبيعتها أو درجة تدخلها. [84]

ومن الضروري أن يتضمن التنظيم ضمانات إجرائية قابلة للتحقق: توثيق الغرض، وتحديد النطاق الموضوعي والزمني، وتسجيل الأساس القانوني، وضبط صلاحيات الوصول، ومراجعة استمرار الحاجة، وتحديد مصير البيانات بعد انتهاء الغرض. كما ينبغي بيان الآثار المترتبة على مخالفة هذه المتطلبات. [85]

ولا يستلزم التطوير إنشاء قانون مستقل لكل وسيلة، بل يمكن اعتماد إطار تشريعي عام يحدد المبادئ والضمانات، مع لوائح فنية قابلة للتحديث. غير أن اللوائح لا ينبغي أن تنشئ صلاحيات تمس الحقوق الأساسية دون سند تشريعي، أو أن تحول التفويض الإداري إلى بديل عن الضمانات. [86]

ويُستحسن أن تخضع الوسائل الجديدة لتقييم قانوني وفني قبل إدخالها في الممارسة، يشمل الغرض، ودرجة الدقة، ومخاطر الخطأ، واحتمالات التمييز، والقدرة على توثيق النتائج ومراجعتها. ولا يعني ذلك اشتراط خلو التقنية من الأخطاء، بل تحديد المخاطر المعروفة ووضع تدابير معقولة. [87]

كما ينبغي مراعاة أن صلاحية الوسيلة في سياق معين لا تعني ملاءمتها لجميع السياقات. فقد تكون أداة مناسبة للفرز الأولي، لكنها غير كافية لاتخاذ قرار ذي أثر جسيم. ومن ثم، يجب تحديد الاستخدامات المسموح بها، ومستوى التحقق المطلوب، والحالات التي تستوجب مراجعة بشرية أو فنية مستقلة. [88]

المطلب الثاني: تعزيز ضمانات الخصوصية والرقابة والمساءلة

تقتضي حماية الخصوصية الانتقال من الاعتراف النظري إلى ضمانات عملية تشمل دورة حياة البيانات: من الجمع إلى التحليل، ثم الاستخدام والمشاركة والاحتفاظ والإتلاف. فالمعالجة قد

تكون مشروعة عند بدايتها، لكنها تصبح غير مشروعة إذا استُخدمت لاحقاً لغرض لا يجيزه القانون، أو احتُفظ بها دون ضرورة، أو أُتيحت لأشخاص لا يملكون صلاحية الوصول.[89]

ويقتضي ذلك اعتماد مبدأ **تحديد الغرض**، بحيث يُبين قبل الجمع الهدف، وتُقيد المعالجة بما يتصل به. كما ينبغي تقليل البيانات إلى القدر اللازم، وتجنب جمع معلومات لا حاجة إليها، ووضع ضوابط للبيانات الحساسة أو المتعلقة بأشخاص غير مستهدفين.[90]

وتتطلب الحوكمة الفعالة **سجلاً يوضح الإجراءات ذات الأثر المرتفع**، والجهة التي أجازتها، والأساس القانوني، والنطاق والمدة، والجهات التي تلقت البيانات. ويساعد هذا السجل على مراجعة الالتزام، وتحديد المسؤولية، واكتشاف أنماط الاستخدام غير الملائم.[91]

كما ينبغي أن **تتناسب الرقابة مع طبيعة الإجراء**. فقد تكون الرقابة الإدارية كافية لبعض الأعمال محدودة الأثر، بينما تتطلب الإجراءات الأكثر تدخلاً رقابة قضائية مسبقة أو لاحقة. ولا يصح افتراض أن نوعاً واحداً يلائم جميع الإجراءات، كما لا يجوز أن تكون الرقابة شكلية لا تتيح الاطلاع على الأساس الفعلي للقرار.[92]

وتستوجب **المساءلة** آليات واضحة لتلقي الشكاوى والتحقيق في ادعاءات الاستخدام غير المشروع، مع ضمان استقلال المراجعة. كما ينبغي تحديد المسؤولية عن اتخاذ القرار وتنفيذه وحفظ البيانات، بحيث لا يؤدي تعدد الجهات إلى ضياع المسؤولية.[93]

ويجب أن تشمل الضمانات **معالجة البيانات بعد انتهاء الغرض**. فالأصل أن الاحتفاظ يستند إلى حاجة مشروعة ومحددة، ويخضع لمدة وضوابط. وعندما تنتفي الحاجة، ينبغي إتلاف البيانات أو إخفاء هويتها وفق القواعد، مع مراعاة الاستثناءات القانونية.[94]

ويتعين تنظيم **مشاركة البيانات** مع الجهات الأخرى، بحيث يُحدد الغرض من النقل، والجهة المتلقية، ونطاق الاستخدام، وشروط إعادة النقل. فمجرد الانتقال لا ينبغي أن يزيل القيود أو يوسع نطاق الاستخدام.[95]

المطلب الثالث: تطوير إجراءات التخطيط والجمع والتحليل والتوثيق ومراجعة التقارير

يتطلب تطوير الممارسة اعتماد **منهج متكامل** يربط مراحل التحري ضمن مسار واضح وقابل للمراجعة. فالتخطيط يحدد السؤال، والجمع يوفر البيانات، والتحليل يختبر دلالتها، والتوثيق يسجل الإجراءات، والمراجعة تتحقق من سلامة المسار.[96]

التخطيط: يبدأ بتحديد المسألة، والهدف المشروع، والبيانات الضرورية، والمصادر المحتملة، والقيود القانونية، والمخاطر الفنية. ويجب أن يتضمن تحديداً أولياً لمعايير النجاح وحدود الاستنتاج، حتى لا يتحول التحري إلى جمع مفتوح دون سؤال محدد.[97]

الجمع: ينبغي أن تُنظم وفق إجراءات تحدد المصدر، وتاريخ الحصول، وطريقة الجمع، والقائم به، والأساس القانوني، والقيود. وعند الحصول على بيانات من مصدر خارجي، ينبغي تسجيل المعلومات عن موثوقية المصدر وتاريخ تحديثه.[98]

التحليل: ينبغي الفصل بين الوقائع المثبتة، والمعلومات غير المتحقق منها، والاستنتاجات، والفرضيات. كما ينبغي اختبار التفسيرات البديلة وتجنب الانتقاء التأكيدي، مع تسجيل مواطن التعارض والنقص. وإذا كانت النتيجة تعتمد على افتراضات، فينبغي الإفصاح عنها. [99]

التوثيق: يقتضي تسجيل الخطوات الجوهرية بطريقة تسمح بإعادة بناء المسار، دون الاكتفاء بإثبات النتيجة. ويشمل وصف البيانات، والأدوات وإصداراتها، والإجراءات، والتحويلات، ونتائج التحقق من السلامة، والقيود. [100]

المراجعة: يجب ألا تقتصر على سلامة اللغة أو استكمال الحقول، بل تتناول مدى إسناد كل استنتاج إلى مصدر، واتساق النتائج مع البيانات، ووجود فرضيات بديلة، ووضوح حدود اليقين، والتزام الإجراء بنطاق الاختصاص. ويمكن في الحالات الحساسة إجراء مراجعة مستقلة عن معد التحليل. [101]

كما ينبغي اعتماد آلية لتصحيح التقارير عند ظهور معلومات جديدة أو اكتشاف خلل. ولا يكفي تعديل النتيجة بصمت؛ بل يجب توثيق طبيعة التصحيح، وسببه، وأثره، والجهات التي ينبغي إخطارها. [102]

ويستحسن استخدام نماذج موحدة للتوثيق والتقارير، شريطة ألا تتحول إلى قوالب جامدة تحجب الفروق بين الحالات. فالنموذج الجيد يساعد على عدم إغفال العناصر الضرورية، لكنه لا يغني عن التحليل الخاص بكل إجراء. [103]

المطلب الرابع: تعزيز التدريب والتنسيق والتعاون الدولي

لا يمكن أن يحقق التطوير التشريعي والإجرائي أهدافه دون بناء قدرات بشرية ومؤسسية قادرة على تطبيقه. فالقواعد مهما بلغت دقتها لا تكفي إذا كان العاملون يجهلون حدود الاختصاص، أو يفتقرون إلى القدرة على تقييم الموثوقية، أو لا يدركون الفرق بين المؤشر الفني والاستنتاج القانوني. [104]

محاور التدريب الأربعة:

١. **القانوني:** مبدأ المشروعية، الاختصاص، شروط الإذن، حماية الخصوصية والبيانات، ضوابط الاحتفاظ والمشاركة. [105]

٢. **الفني:** مصادر المعلومات، خصائص البيانات الوصفية، سلامة النسخ، سلسلة العهدة، حدود الأدوات. [106]

٣. **التحليلي:** تقييم المصادر، اختبار الفرضيات البديلة، معالجة التعارض، تجنب التحيز، الإفصاح عن عدم اليقين. [107]

٤. **المهني:** إعداد التقارير، توثيق القرارات، حماية السرية، التعامل مع الأخطاء، الالتزام بحدود الدور. [108]

ويجب أن يتضمن التدريب حالات تطبيقية افتراضية تسمح باختبار القدرة على اتخاذ القرار في ظروف تتضمن نقصاً في البيانات أو تعارضاً بين المصادر أو شكاً في الأصالة. كما ينبغي أن يخضع التدريب للتقييم المستمر، بحيث تقاس الكفاءة بالقدرة على تطبيق المعايير، لا بمجرد حضور الدورات. [109]

أما التنسيق المؤسسي، فيتطلب بروتوكولات واضحة لتبادل البيانات بين الجهات الأمنية والقضائية والفنية، تحدد مسؤولية كل جهة، والحد الأدنى من المعلومات الواجب توثيقها، وآليات الإحالة إلى الخبراء، وإجراءات التعامل مع البيانات غير مشروعة المصدر أو ناقصة التوثيق. [110]

وفي التعاون الدولي، يجب تحديد الأساس القانوني لكل طلب، والتحقق من انطباق الاتفاقيات، ومراعاة القيود المتعلقة بحماية البيانات وسرية التحقيقات، وتوثيق مسار الطلب والاستجابة. كما ينبغي تدريب العاملين على التمييز بين طلب حفظ البيانات وطلب الإفصاح عنها، وبين التعاون الطوعي والتعاون الذي يتطلب إجراءات رسمية. [111]

وتبرز أهمية التعاون في ظل سرعة زوال بعض البيانات، وتوزعها بين مقدمي الخدمات والدول. غير أن سرعة الإجراء لا ينبغي أن تؤدي إلى إهمال الأساس القانوني أو الضمانات؛ بل تستدعي تطوير قنوات تعاون سريعة وواضحة تتيح اتخاذ التدابير ضمن الحدود القانونية. [112]

كما يستحسن تعزيز التعاون بين الجهات القانونية والفنية والمؤسسات الأكاديمية، من خلال برامج بحثية وتدريبية تدرس الأخطاء المتكررة، وتقارن الممارسات، وتطور نماذج توثيق قابلة للتحسين، مع حماية سرية المعلومات واستخدام الحالات المجهلة. [113]

المطلب الخامس: تنظيم استخدام الذكاء الاصطناعي والإشراف البشري والمراجعة المستقلة

أصبح استخدام الذكاء الاصطناعي في تحليل المعلومات الرقمية يثير تحديات تتعلق بمدى شفافية النتائج، وإمكان تفسيرها، واحتمالات التحيز والخطأ، وحدود الاعتماد عليها في القرارات الأمنية أو القانونية. وتزداد الأهمية عندما تستخدم الأنظمة لتصنيف الأشخاص أو ربطهم بوقائع أو تحليل صورهم وأصواتهم. [114]

ويجب التمييز بين استخدام الذكاء الاصطناعي أداة مساعدة لتنظيم البيانات أو تسريع البحث، وبين استخدامه لإنتاج استنتاجات قد تؤثر مباشرة في حقوق الأفراد. فالمخاطر لا تتحدد بمجرد وجود نظام آلي، بل بطبيعة المهمة، ونوعية البيانات، ومدى تأثير المخرجات في القرار النهائي، وإمكان التحقق المستقل. [115]

وقد اعتمدت منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) توصيتها بشأن الذكاء الاصطناعي، التي تتضمن مبادئ تتعلق بالنمو الشامل، وحقوق الإنسان والقيم الديمقراطية، والشفافية، والمتانة والأمان، والمساءلة. [116] وتوفر هذه المبادئ إطاراً عاماً للحوكمة، لكنها لا تحل محل التشريعات الوطنية أو القواعد الإجرائية. [117]

وينبغي أن يبدأ التنظيم بتحديد الأغراض المسموح بها، وتقييم مخاطر الاستخدام، والتحقق من ملاءمة النظام للمهمة، واختبار أدائه في الظروف التي سيستخدم فيها. كما يجب توثيق البيانات والمدخلات، وإصدار النظام، وإعداداته الجوهرية، والقيود المعروفة، والإجراءات التي اتخذها المستخدم للتحقق من النتائج.[118]

ولا يكفي وجود إشراف بشري شكلي لإزالة مخاطر الاعتماد المفرط. فقد يميل المستخدم إلى قبول النتيجة دون فحصها، خصوصاً عندما تبدو المخرجات دقيقة أو مصحوبة بدرجات رقمية للثقة. ولذلك ينبغي أن يكون الإشراف حقيقياً، وأن يتوافر للمراجع الوقت والمعرفة والصلاحيات لمناقشة النتيجة أو رفضها، لا أن يقتصر دوره على المصادقة الإدارية.[119]

ويقتضي ذلك تحديد القرارات التي لا يجوز اتخاذها اعتماداً حصرياً على مخرجات آلية، متى كان القانون أو مستوى المخاطر يقتضي تدخلاً بشرياً ذا معنى. كما ينبغي أن تكون الجهة قادرة على بيان الأساس الذي اعتمدت عليه النتيجة، وحدود دقتها، وأسباب ملاءمتها للغرض.[120]

وتتطلب المراجعة المستقلة التحقق من أداء النظام في سياق الاستخدام الفعلي، وفحص معدلات الخطأ، وتقييم تمثيل البيانات، ورصد الفروق في الأداء بين الفئات والظروف. كما ينبغي أن تشمل أثر التحديثات؛ إذ قد تتغير خصائص المخرجات عند تعديل النموذج أو البيانات.[121]

ومن المهم التمييز بين قابلية تفسير النظام وقابلية التحقق من نتيجته. فقد يكون من الصعب تفسير بعض العمليات الداخلية، لكن يمكن التحقق من المخرجات من خلال اختبارات مستقلة. وفي المقابل، قد يقدم النظام تفسيراً ظاهرياً دون أن يكون كافياً لإثبات الصحة.[122]

ويجب ألا تتحول مخرجات الذكاء الاصطناعي إلى بديل عن الأدلة المستقلة أو عن التقدير القانوني. فإذا صنف النظام محتوى على أنه يحتمل أن يكون اصطناعياً، فإن هذه النتيجة مؤشر يستلزم التحقق، ولا تثبت وحدها أن المحتوى مزيف.[123] وإذا ربط النظام بين شخصين، فينبغي فحص مدى صحة البيانات والعلاقة والبحث عن تفسيرات بديلة.[124]

كما ينبغي وضع إجراءات للتعامل مع الأخطاء الناتجة عن الأنظمة، تشمل تسجيلها، وتقييم أثرها، وتصحيح النتائج، ومراجعة استمرار صلاحية النظام. وعند ثبوت أن مخرجاته غير موثوقة في سياق محدد، يجب أن تكون المؤسسة قادرة على تعليق استخدامه أو تقييده.[125]

وأخيراً، فإن حوكمة الذكاء الاصطناعي ينبغي أن تقوم على التناسب بين مستوى المخاطر وشدة الضمانات. فالأدوات المستخدمة لتنظيم البيانات لا تقتضي المستوى ذاته من الرقابة المطبق على أنظمة تستنتج هوية الأشخاص أو تصنفهم أو تؤثر في قرارات تمس حرياتهم. ويظل المبدأ الحاكم أن التطور التقني لا يعفي من متطلبات المشروعية، ولا ينقل مسؤولية القرار إلى النظام الآلي.[126]

الجدول المقارن: التحديات ومقترحات التطوير

التحدي	المقترح	طبيعته	الجهة المسؤولة
القصور التشريعي	إطار تشريعي عام + لوائح فنية	قانوني	المشرع + الجهات التنظيمية
التداخل الاختصاصي	توزيع وظيفي دقيق + توثيق المسؤوليات	مؤسسي	الجهات الأمنية والقضائية
التوازن مع الحقوق	تقييم مسبق للمخاطر + تناسب + رقابة	حقوقي	الجهات الأمنية + الرقابة المستقلة
البيانات العابرة للحدود	قنوات تعاون + اتفاقيات + توثيق	قانوني/دولي	وزارات العدل والخارجية
التلاعب والكشف الآلي	فحص متعدد المستويات + عدم الاعتماد على أداة واحدة	تقني	المختبرات الفنية
التحيز والأخطاء	اختبار البدائل + مراجعة مستقلة + إدارة مخاطر	منهجي/تقني	المحللون + وحدات الجودة
الكفاءات والموارد	تدريب مستمر + بنية تحتية + حوكمة	مؤسسي	إدارات التدريب والتخطيط
التنسيق والتوثيق	بروتوكولات + نماذج موحدة + ضمان جودة	مؤسسي	الجهات المتعاونة
الذكاء الاصطناعي	إشراف بشري حقيقي + مراجعة مستقلة + تحديد الأغراض	تقني/قانوني	الجهات المستخدمة + الرقابة

❖ النافذة التطبيقية

السيناريو: جهة أمنية تريد استخدام نظام ذكاء اصطناعي لتحليل آلاف الصور من كاميرات المراقبة للتعرف على شخص مشتببه فيه.

- **الخطوة الأولى (المشروعية):** التحقق من السند القانوني لاستخدام النظام: هل يجيز القانون التحليل الآلي للصور؟ هل يشمل الإذن هذه الوسيلة؟ هل هناك تقييم مسبق للمخاطر؟
- **الخطوة الثانية (الغرض والنطاق):** تحديد الغرض بدقة (البحث عن شخص محدد، لا تصنيف عام)، والنطاق (فترة زمنية، كاميرات محددة)، والقيود.
- **الخطوة الثالثة (التحقق من الأداة):** هل النظام مناسب للمهمة؟ ما معدل الخطأ المعروف؟ هل تم اختباره في ظروف مشابهة؟ هل يوجد إشراف بشري حقيقي؟
- **الخطوة الرابعة (الإشراف البشري):** لا يجوز الاعتماد على مخرجات النظام وحدها. يجب أن يراجع محلل مؤهل النتائج، ويبحث عن تفسيرات بديلة (تشابه في المظهر، خطأ في النظام).

- **الخطوة الخامسة (الإفصاح):** بيان أن "النظام أشار إلى تطابق محتمل"، لا "ثبت أن الشخص هو..."، مع بيان معدل الخطأ والقيود.
- **الخطوة السادسة (المراجعة المستقلة):** في القرارات الحساسة، يجب مراجعة مستقلة من جهة لم تشارك في التحليل الأولي.
- **الدرس: الذكاء الاصطناعي أداة مساعدة، لا بديل عن التقييم القانوني والإشراف البشري.**

النتائج العامة للفصل

١. القصور التشريعي قد يكون في العمومية أو التشتت أو غموض الحدود، لا في غياب النص.
٢. القدرة التقنية لا تنشئ اختصاصاً قانونياً، وعدم الحظر التقني لا يعني الجواز.
٣. المرونة التشريعية تختلف عن الغموض القانوني.
٤. التداخل الاختصاصي يتطلب توزيعاً وظيفياً دقيقاً، لا مجرد تنسيق عام.
٥. تغير طبيعة الواقعة (من أمنية إلى جنائية) يقتضي إعادة تقييم الأساس القانوني.
٦. التوازن بين الأمن والحقوق ليس مقابلة مجردة؛ فالحماية تعزز الموثوقية.
٧. التناسب يتطلب ملائمة الوسيلة وضرورتها وتناسب أثرها.
٨. البيانات العابرة للحدود تتطلب التمييز بين القدرة التقنية والسلطة القانونية.
٩. التلاعب الرقمي يتطلب فحصاً متعدد المستويات، لا الاعتماد على أداة كشف واحدة.
١٠. التحيز التأكدي خطر يهدد الموضوعية، ويُعالج باختبار البدائل والمراجعة المستقلة.
١١. الكفاءات المطلوبة تجمع بين القانون والتقنية والتحليل والمهنية.
١٢. التنسيق المؤسسي يتطلب توحيد الحد الأدنى من التوثيق، مع الحفاظ على استقلال التقدير القانوني.
١٣. تطوير التنظيم يستلزم تحديد فئات الإجراءات، والجهات المختصة، والضمانات.
١٤. حماية الخصوصية تتطلب ضمانات تشمل دورة حياة البيانات كاملة.
١٥. الذكاء الاصطناعي يتطلب إشرافاً بشرياً حقيقياً، ومراجعة مستقلة، وتحديد الأغراض المسموح بها.

المراجع:

- (1) انظر: عادل عبد العال خراشي، ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي، ٢٠٠٦، ص ٤٠٠-٤٠٥.
- (2) انظر: هشام مصطفى محمد، التحريات الأمنية وأثرها في الأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٥، ص ٥٠٠-٥٠٥.
- (3) انظر: محمد محمد سيف شجاع، شرح قانون الإجراءات الجزائية اليمني، مكتبة الصادق، صنعاء، ٢٠٠٥.
- (4) انظر: خراشي، مرجع سابق، ص ٤١٠-٤١٥.
- (5) الأمم المتحدة، العهد الدولي الخاص بالحقوق المدنية والسياسية، ١٩٦٦، المادة ١٧.
- (6) انظر: شجاع، مرجع سابق.
- (7) انظر: خراشي، مرجع سابق، ص ٤٢٠-٤٢٥.
- (8) انظر: هشام مصطفى، مرجع سابق، ص ٥١٠-٥١٥.
- (9) Council of Europe, *Convention on Cybercrime*, ETS No. 185, 2001.
- (10) انظر: شجاع، مرجع سابق.
- (11) انظر: خراشي، مرجع سابق، ص ٤٣٠-٤٣٥.
- (12) انظر: هشام مصطفى، مرجع سابق، ص ٥٢٠-٥٢٥.
- (13) انظر: شجاع، مرجع سابق.
- (14) انظر: خراشي، مرجع سابق، ص ٤٤٠-٤٤٥.
- (15) انظر: شجاع، مرجع سابق.
- (16) انظر: NIST, *Guide to Integrating Forensic Techniques into Incident Response*, NIST SP 800-86, 2006, at 4-1.
- (17) انظر: هشام مصطفى، مرجع سابق، ص ٥٣٠-٥٣٥.
- (18) انظر: خراشي، مرجع سابق، ص ٤٥٠-٤٥٥.
- (19) انظر: NIST, *Digital Investigation Techniques*, NISTIR 8354, 2022, at 4-2.
- (20) الأمم المتحدة، المبادئ الأساسية بشأن استقلال السلطة القضائية، ١٩٨٥.
- (21) انظر: شجاع، مرجع سابق.
- (22) انظر: هشام مصطفى، مرجع سابق، ص ٥٤٠-٥٤٥.
- (23) انظر: خراشي، مرجع سابق، ص ٤٦٠-٤٦٥.
- (24) انظر: شجاع، مرجع سابق.
- (25) انظر: هشام مصطفى، مرجع سابق، ص ٥٥٠-٥٥٥.
- (26) انظر: خراشي، مرجع سابق، ص ٤٧٠-٤٧٥.
- (27) انظر: شجاع، مرجع سابق.
- (28) انظر: هشام مصطفى، مرجع سابق، ص ٥٦٠-٥٦٥.
- (29) انظر: خراشي، مرجع سابق، ص ٤٨٠-٤٨٥.
- (30) مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، A/HRC/48/31، ٢٠٢١.
- (31) انظر: المرجع السابق.
- (32) انظر: هشام مصطفى، مرجع سابق، ص ٥٧٠-٥٧٥.
- (33) انظر: شجاع، مرجع سابق.
- (34) انظر: خراشي، مرجع سابق، ص ٤٩٠-٤٩٥.
- (35) انظر: هشام مصطفى، مرجع سابق، ص ٥٨٠-٥٨٥.
- (36) انظر: خراشي، مرجع سابق، ص ٥٠٠-٥٠٥.
- (37) انظر: شجاع، مرجع سابق.
- (38) انظر: Council of Europe, *Convention on Cybercrime*, *supra* note 9, Articles 23-35.
- (39) انظر: Council of Europe, *Second Additional Protocol*, CETS No. 224, 2022.
- (40) انظر: شجاع، مرجع سابق.
- (41) انظر: خراشي، مرجع سابق، ص ٥١٠-٥١٥.
- (42) انظر: هشام مصطفى، مرجع سابق، ص ٥٩٠-٥٩٥.
- (43) انظر: شجاع، مرجع سابق.
- (44) انظر: NIST, *Reducing Risks Posed by Synthetic Content*, NIST AI 100-4, 2024, at 1-1.
- (45) انظر: المرجع السابق، at 2-1.
- (46) انظر: المرجع السابق، at 2-2.

- (47) انظر: المرجع السابق، at 2-3.
- (48) انظر: خراشي، مرجع سابق، ص ٥٢٠-٥٢٥.
- (49) انظر. NIST AI 100-4, *supra* note 44, at 3-1.
- (50) انظر: المرجع السابق، at 3-2.
- (51) انظر: هشام مصطفى، مرجع سابق، ص ٦٠٠-٦٠٥.
- (52) انظر. NIST AI 100-4, *supra* note 44, at 3-3.
- (53) انظر. Berkeley Protocol, *supra* note 12, at 170-175.
- (54) انظر: خراشي، مرجع سابق، ص ٥٣٠-٥٣٥.
- (55) انظر: هشام مصطفى، مرجع سابق، ص ٦١٠-٦١٥.
- (56) انظر. Berkeley Protocol, *supra* note 12, at 240-245.
- (57) انظر. NIST AI 100-4, *supra* note 44, at 4-1.
- (58) انظر. NIST SP 800-86, *supra* note 16, at 4-2.
- (59) ISO/IEC 23894:2023, *Information Technology—Artificial Intelligence—Guidance on Risk Management*, 2023.
- (60) انظر: شجاع، مرجع سابق.
- (61) انظر. Berkeley Protocol, *supra* note 12, at 240-245.
- (62) انظر. NIST SP 800-86, *supra* note 16, at 4-3.
- (63) انظر: هشام مصطفى، مرجع سابق، ص ٦٢٠-٦٢٥.
- (64) انظر: خراشي، مرجع سابق، ص ٥٤٠-٥٤٥.
- (65) انظر: شجاع، مرجع سابق.
- (66) انظر. Berkeley Protocol, *supra* note 12, at 25-30.
- (67) انظر. NIST SP 800-86, *supra* note 16, at 3-1.
- (68) انظر. Berkeley Protocol, *supra* note 12, at 115-120.
- (69) انظر: خراشي، مرجع سابق، ص ٥٥٠-٥٥٥.
- (70) انظر: هشام مصطفى، مرجع سابق، ص ٦٣٠-٦٣٥.
- (71) انظر: خراشي، مرجع سابق، ص ٥٦٠-٥٦٥.
- (72) انظر: شجاع، مرجع سابق.
- (73) انظر: هشام مصطفى، مرجع سابق، ص ٦٤٠-٦٤٥.
- (74) انظر: خراشي، مرجع سابق، ص ٥٧٠-٥٧٥.
- (75) انظر. INTERPOL, *Guidelines for Digital Forensics First Responders*, at 10-12.
- (76) انظر: شجاع، مرجع سابق.
- (77) انظر. NIST SP 800-86, *supra* note 16, at 5-1.
- (78) ISO/IEC 17025:2017, *General Requirements for the Competence of Testing and Calibration Laboratories*, 2017.
- (79) انظر: هشام مصطفى، مرجع سابق، ص ٦٥٠-٦٥٥.
- (80) انظر: خراشي، مرجع سابق، ص ٥٨٠-٥٨٥.
- (81) انظر: شجاع، مرجع سابق.
- (82) انظر: خراشي، مرجع سابق، ص ٥٩٠-٥٩٥.
- (83) انظر: هشام مصطفى، مرجع سابق، ص ٦٦٠-٦٦٥.
- (84) انظر: شجاع، مرجع سابق.
- (85) انظر: خراشي، مرجع سابق، ص ٦٠٠-٦٠٥.
- (86) انظر: هشام مصطفى، مرجع سابق، ص ٦٧٠-٦٧٥.
- (87) انظر. NIST AI 100-4, *supra* note 44, at 4-2.
- (88) انظر: خراشي، مرجع سابق، ص ٦١٠-٦١٥.
- (89) انظر: شجاع، مرجع سابق.
- (90) انظر: هشام مصطفى، مرجع سابق، ص ٦٨٠-٦٨٥.
- (91) انظر: خراشي، مرجع سابق، ص ٦٢٠-٦٢٥.
- (92) انظر: شجاع، مرجع سابق.
- (93) انظر: هشام مصطفى، مرجع سابق، ص ٦٩٠-٦٩٥.

- (94) انظر: خراشي، مرجع سابق، ص ٦٣٠-٦٣٥.
- (95) انظر: شجاع، مرجع سابق.
- (96) انظر: هشام مصطفى، مرجع سابق، ص ٧٠٥-٧٠٠.
- (97) انظر: خراشي، مرجع سابق، ص ٦٤٥-٦٤٠.
- (98) انظر. INTERPOL, *supra* note 75, at 12-15.
- (99) انظر. Berkeley Protocol, *supra* note 12, at 240-245.
- (100) انظر. NIST SP 800-86, *supra* note 16, at 5-2.
- (101) انظر: هشام مصطفى، مرجع سابق، ص ٧١٠-٧١٥.
- (102) انظر: خراشي، مرجع سابق، ص ٦٥٥-٦٥٠.
- (103) انظر: شجاع، مرجع سابق.
- (104) انظر: هشام مصطفى، مرجع سابق، ص ٧٢٠-٧٢٥.
- (105) انظر: خراشي، مرجع سابق، ص ٦٦٥-٦٦٠.
- (106) انظر. NIST SP 800-86, *supra* note 16, at 5-3.
- (107) انظر. Berkeley Protocol, *supra* note 12, at 240-245.
- (108) انظر: شجاع، مرجع سابق.
- (109) انظر: هشام مصطفى، مرجع سابق، ص ٧٣٠-٧٣٥.
- (110) انظر: خراشي، مرجع سابق، ص ٦٧٥-٦٧٠.
- (111) انظر. Council of Europe, *Convention on Cybercrime*, *supra* note 9, Articles 23-35.
- (112) انظر: شجاع، مرجع سابق.
- (113) انظر: هشام مصطفى، مرجع سابق، ص ٧٤٥-٧٤٠.
- (114) OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, 2019 (amended 2024).
- (115) انظر. NIST AI 100-4, *supra* note 44, at 5-1.
- (116) OECD, *supra* note 114.
- (117) انظر: شجاع، مرجع سابق.
- (118) انظر. ISO/IEC 23894:2023, *supra* note 59.
- (119) انظر: هشام مصطفى، مرجع سابق، ص ٧٥٥-٧٥٠.
- (120) انظر: خراشي، مرجع سابق، ص ٦٨٥-٦٨٠.
- (121) انظر. NIST AI 100-4, *supra* note 44, at 5-2.
- (122) انظر: شجاع، مرجع سابق.
- (123) انظر. Berkeley Protocol, *supra* note 12, at 170-175.
- (124) انظر: خراشي، مرجع سابق، ص ٦٩٥-٦٩٠.
- (125) انظر: هشام مصطفى، مرجع سابق، ص ٧٦٥-٧٦٠.
- (126) انظر: شجاع، مرجع سابق.

الخاتمة

أصبحت التحريات الأمنية الرقمية من الموضوعات القانونية التي تفرض نفسها بقوة على الدراسات الأمنية والجنائية المعاصرة، في ظل التحول المتسارع نحو البيئة الرقمية، وتزايد اعتماد الأفراد والمؤسسات على الوسائل التقنية في الاتصال وتبادل المعلومات وتخزينها ومعالجتها. ولم يعد النشاط الأمني مقتصرًا على وسائل الرصد التقليدية أو جمع المعلومات من مصادرها المباشرة، بل امتد ليشمل تحليل البيانات الرقمية، والتحقق من المحتوى المنشور عبر الشبكات الإلكترونية، والاستفادة من السجلات التقنية وبيانات الاتصالات، وفحص الأجهزة والأنظمة الرقمية، وتوظيف الوسائل الحديثة في رصد الوقائع وجمع المعلومات المرتبطة بها.

وقد أفرز هذا التحول إشكالية قانونية مركبة لا تتعلق بمجرد قدرة الجهات المختصة على الوصول إلى المعلومات الرقمية، وإنما تمتد إلى تحديد الأساس القانوني الذي يجيز جمعها، وضبط حدود الاختصاص في الحصول عليها، ومراعاة الحقوق والحريات الأساسية عند معالجتها، والتحقق من أصالتها وسلامتها الفنية، وتقدير مدى موثوقيتها وقيمتها الاستدلالية، فضلاً عن تحديد الآثار القانونية المترتبة على مخالفة الضوابط المنظمة لها.

وتنبع أهمية هذه الإشكالية من أن التطور التقني لا يؤدي بالضرورة إلى زيادة اليقين القانوني؛ فقد تتيح الوسائل الرقمية الحصول على كميات كبيرة من المعلومات في وقت وجيز، لكنها قد تنتج، في المقابل، صوراً متعددة من الخطأ في تحديد المصدر، أو الخلط بين الأشخاص، أو إساءة تفسير البيانات الوصفية، أو اقتطاع المحتوى من سياقه، أو بناء استنتاجات تتجاوز ما تسمح به المعطيات المتاحة. ومن ثم، فإن التحدي الحقيقي لا يكمن في توسيع القدرة على جمع المعلومات فحسب، بل في إخضاع هذه القدرة لمنظومة متكاملة من المشروعية والضرورة والتناسب والموثوقية والتوثيق والرقابة والمساءلة.

وانطلاقاً من ذلك، تناولت هذه الدراسة التحريات الأمنية الرقمية من منظور قانوني عام يستند إلى المبادئ القانونية والحقوقية ذات الصلة، وإلى الأدبيات الفقهية والمعايير الفنية والمهنية المعترف بها، دون افتراض انطباق نظام تشريعي وطني واحد على جميع المسائل محل البحث. وقد سعت إلى بناء تصور متكامل يربط بين الطبيعة الوظيفية للتحريات الرقمية، والأساس القانوني لممارستها، ووسائل الحصول على المعلومات، وآليات التحقق منها، وسلامتها الفنية، وقيمتها القانونية، والتحديات التي تواجه تطوير الممارسة المهنية والمؤسسية.

أولاً: الإجابة عن الإشكالية الرئيسية للدراسة

تتمثل الإشكالية الرئيسية التي عالجتها الدراسة في تحديد الكيفية التي يمكن بها تنظيم التحريات الأمنية الرقمية وممارستها على نحو يحقق الفاعلية الأمنية، دون الإخلال بمبدأ المشروعية أو الانتقاص غير المبرر من الحقوق والحريات، مع ضمان سلامة المعلومات المتحصلة وموثوقيتها وصلاحياتها لدعم الاستنتاجات الأمنية أو القانونية.

وقد أظهر التحليل أن تحقيق هذا التوازن لا يمكن أن يستند إلى قاعدة منفردة أو ضمانة إجرائية واحدة، بل يتطلب تكامل أربعة مستويات مترابطة.

يتعلق المستوى الأول بمشروعية الإجراء، أي وجود سند قانوني يجيز التحري، وصدوره عن جهة مختصة، والالتزام بشروط الإذن متى كان الحصول على المعلومات أو الوصول إليها يستلزم إذنًا قضائيًا أو تصريحًا من جهة مختصة. ولا يكفي في هذا السياق أن تكون المعلومة مفيدة أمنياً أو متاحة تقنيًا، لأن الإمكان التقني لا ينشئ بذاته سلطة قانونية، كما أن أهمية الغرض الأمني لا تبرر تجاوز القيود التي يفرضها القانون.

ويتعلق المستوى الثاني بسلامة الإجراءات الفنية، ويشمل توثيق مصادر المعلومات وطرق جمعها، والمحافظة على البيانات الأصلية، وتسجيل عمليات النقل والفحص والمعالجة، والتحقق من سلامة النسخ الرقمية، وتوفير سجل يسمح بمراجعة الإجراءات وإعادة فحص النتائج عند الاقتضاء. فالمعلومة التي لا يمكن تتبع مصدرها أو التحقق من سلامتها تثير شكوكًا قد تؤثر في صلاحية الاستناد إليها، حتى لو بدت في ظاهرها متسقة مع فرضية التحري.

أما المستوى الثالث فيتصل بموثوقية المعلومات وصحة الاستنتاجات، وهو ما يقتضي التمييز بين البيانات الخام والمعلومات المستخلصة منها، وبين الوقائع الموثقة والفرضيات التفسيرية، واختبار التفسيرات البديلة، وتجنب التحيز التأكيدي، والإفصاح عن أوجه النقص والشك وعدم اليقين. فالسلامة الفنية للبيانات لا تعني بالضرورة صحة تفسيرها، كما أن صحة البيانات من حيث المصدر لا تكفي وحدها لإثبات نسبة المحتوى إلى شخص معين أو استنتاج مسؤوليته عن واقعة محددة.

ويتمثل المستوى الرابع في الرقابة والمساءلة والضمانات الحقوقية، بما يشمل الرقابة القضائية حيث يقررها القانون، والرقابة الإدارية والمؤسسية، وإمكان مراجعة الإجراءات والاعتراض عليها وفق النظام القانوني المنطبق، وتحديد المسؤولية عن تجاوز الاختصاص أو مخالفة شروط الإذن أو إساءة استخدام المعلومات. وتكتسب هذه الضمانات أهمية خاصة بالنظر إلى قدرة الوسائل الرقمية على جمع معلومات واسعة النطاق، بما قد يمتد إلى أشخاص لا صلة لهم بالواقعة محل التحري.

وعليه، تخلص الدراسة إلى أن مشروعية التحريات الأمنية الرقمية وفعاليتها لا تقاسان بكمية المعلومات التي يمكن جمعها، ولا بسرعة الوصول إليها، وإنما بمدى توافر أساس قانوني صحيح، واتباع إجراءات منضبطة، وإمكان التحقق من مصادر المعلومات وسلامتها، وتناسب الاستنتاجات مع قوة المعطيات، وخضوع الممارسة للرقابة والمساءلة. وبهذا المعنى، فإن جودة التحري الرقمي مفهوم مركب يجمع بين المشروعية القانونية والكفاءة الفنية والانضباط المنهجي والضمانات الحقوقية.

ثانيًا: النتائج المتعلقة بطبيعة التحريات الأمنية الرقمية وحدودها الوظيفية

أظهر البحث أن التحريات الأمنية الرقمية تمثل امتدادًا متطورًا للنشاط التحري، لكنها لا تفقد بسبب طبيعتها التقنية خضوعها للقواعد القانونية التي تحكم أعمال الجهات المختصة. فهي نشاط يستهدف جمع المعلومات الرقمية وفحصها وربطها وتحليلها للتحقق من وقائع أو مؤشرات ذات صلة بغرض أمني مشروع، في حدود الاختصاص المقرر قانونًا.

وتتميز هذه التحريات بخصائص تجعلها مختلفة في بعض جوانبها عن التحريات التقليدية، من أهمها سرعة جمع المعلومات، وتعدد مصادرها، وإمكان نسخها ونقلها ومعالجتها على نطاق واسع، واحتوائها على بيانات وصفية قد تكشف عن أنماط الحركة والاتصال والسلوك، فضلاً عن إمكان الجمع بين معلومات متفرقة للوصول إلى استنتاجات لم يكن من السهل استخلاصها من كل مصدر على حدة.

غير أن هذه الخصائص تحمل في الوقت ذاته مخاطر قانونية ومنهجية. فسهولة النسخ لا تعني سلامة النسخة، وتعدد المصادر لا يضمن استقلالها، وإمكان الربط بين البيانات لا يعني أن العلاقة المستنتجة بينها تعكس علاقة سببية حقيقية. كما أن كثافة البيانات قد تؤدي إلى تضخم المعلومات غير المرتبطة بموضوع التحري، وإلى زيادة احتمالات الخطأ في تفسيرها أو نسبة محتواها إلى أشخاص بعينهم.

وتوصلت الدراسة كذلك إلى ضرورة التمييز بين التحريات الأمنية الرقمية وجمع المعلومات بمعناه العام. فجمع المعلومات قد يجري لأغراض إدارية أو تنظيمية أو بحثية أو تجارية، في حين ترتبط التحريات الأمنية بغرض محدد وباختصاص قانوني معين، وقد تتصل، بحسب طبيعتها وملابساتها، بوقائع يحتمل أن تفضي إلى اتخاذ تدابير أمنية أو إلى إحالة المعلومات إلى جهات التحقيق المختصة.

كما أكدت الدراسة أهمية الفصل بين التحري والتحقيق الجنائي الرقمي. فالتحري يستهدف التحقق من المعلومات والكشف عن مؤشرات الوقائع وتكوين تصور أولي بشأنها، بينما ينصرف التحقيق الجنائي الرقمي، بحسب النظام القانوني المعني، إلى إجراءات تستهدف إثبات الوقائع وجمع الأدلة وفحصها في إطار الدعوى الجزائية وتحت الضمانات والاختصاصات المقررة لها. وقد تتداخل الأنشطة الفنية المستخدمة في المجالين، لكن هذا التداخل لا يبرر الخلط بين طبيعتهما القانونية أو افتراض تماثل سلطات القائمين بهما.

ومن النتائج المهمة أيضاً أن تحديد نطاق التحريات الرقمية يجب ألا يقتصر على نوع التقنية المستخدمة، بل ينبغي أن يراعي طبيعة البيانات التي يجري الوصول إليها، والغرض من الإجراء، ومدى تدخله في خصوصية الأفراد، وطريقة تنفيذه، ودرجة استمراره، والنتائج المتوقعة منه. فالمشاهدة العابرة لمحتوى منشور للعموم تختلف في طبيعتها عن المراقبة المنظمة المستمرة، كما يختلف الحصول على سجل متاح قانوناً عن اختراق حساب محمي أو الوصول إلى بيانات اتصالات خاصة.

وبناءً على ذلك، لا يمكن وضع جميع صور التحري الرقمي في مرتبة قانونية واحدة، وإنما يتعين إخضاع كل صورة لتقييم مستقل يراعي طبيعتها وآثارها والقيود القانونية المتعلقة بها.

ثالثاً: النتائج المتعلقة بالمشروعية والاختصاص والإذن والضمانات

بينت الدراسة أن مبدأ المشروعية يمثل نقطة الانطلاق في تنظيم التحريات الأمنية الرقمية، وأن التطور التقني لا يبرر إنشاء سلطات ضمنية غير منصوص عليها أو التوسع في تفسير الاختصاصات على نحو يؤدي إلى المساس بالحقوق الأساسية دون سند قانوني.

ويقتضي تطبيق هذا المبدأ التحقق من ثلاثة عناصر مترابطة: وجود أساس قانوني يجيز الإجراء، واختصاص الجهة القائمة به، والتزام الحدود الموضوعية والإجرائية المقررة لممارسته. وقد يكون الإجراء مشروعاً من حيث الغرض العام، لكنه غير مشروع إذا صدر عن جهة غير مختصة، أو تجاوز نطاق الإذن، أو استهدف بيانات لا يشملها السند القانوني، أو خالف ضمانة جوهرية يفرضها التشريع المعمول به.

كما أظهر التحليل أن اشتراط الإذن القضائي أو التصريح من جهة مختصة لا يمكن تعميمه على جميع صور التحري الرقمي؛ إذ تتوقف متطلباته على طبيعة الإجراء، ومدى تدخله في الحقوق والحريات، ونوع البيانات المستهدفة، والنظام القانوني المنطبق. ومع ذلك، فإن غياب اشتراط الإذن في حالة معينة لا يعني انتفاء كل القيود القانونية، بل تظل مبادئ الاختصاص والغرض المشروع والضرورة والتناسب وحماية البيانات واجبة المراعاة متى قررها القانون.

وأثبتت الدراسة أن مبدأ الضرورة والتناسب يؤدي وظيفة جوهرية في الحد من التوسع غير المبرر في جمع المعلومات. فالضرورة تقتضي بيان الصلة بين الوسيلة المستخدمة والغرض المراد تحقيقه، أما التناسب فيقتضي ألا تتجاوز شدة التدخل في الحقوق ما تبرره أهمية الهدف المشروع والظروف المحيطة به. ولا يكفي لإثبات التناسب أن تكون الوسيلة فعالة تقنياً، بل ينبغي النظر أيضاً في البدائل الأقل تدخلاً، ونطاق البيانات التي ستجمع، والمدة التي سيستمر فيها الإجراء، والآثار المحتملة على الأشخاص غير المستهدفين.

وفي السياق ذاته، أكدت الدراسة أن حماية الخصوصية في البيئة الرقمية لا تتعلق بمحتوى الاتصالات أو البيانات المخزنة وحدها، بل قد تمتد إلى بيانات الموقع وأنماط الحركة والاتصال والعلاقات المستخلصة من تجميع البيانات المتفرقة. وقد يؤدي الربط بين بيانات تبدو محدودة الحساسية عند النظر إلى كل منها منفردة إلى استنتاجات شديدة الخصوصية عن حياة الأفراد وسلوكهم.

ومن ثم، فإن تقييم مشروعية المعالجة الرقمية ينبغي أن يراعي طبيعة البيانات منفردة ومجمعة، والغرض من معالجتها، ومدى إمكان تحديد هوية أصحابها، والنتائج التي يمكن استخلاصها منها، فضلاً عن الضوابط المتعلقة بالاحتفاظ بها ومشاركتها وإتلافها.

كما توصلت الدراسة إلى أن البيانات المتعلقة بالأشخاص الذين يظهرون عرضاً أثناء التحري تستحق معالجة قانونية واضحة. فعدم استهداف هؤلاء الأشخاص لا يزيل تلقائياً كل أثر للمساس بحقوقهم، ولا يبرر الاحتفاظ ببياناتهم أو تداولها دون ضرورة. ولذلك، ينبغي أن تتضمن الأطر المؤسسية قواعد تحدد كيفية عزل المعلومات غير المرتبطة بموضوع التحري، والحد من الوصول إليها، ومراجعة الحاجة إلى الاحتفاظ بها، وإتلافها متى انتفى السند القانوني لاستمرار معالجتها.

وأخيراً، أكدت الدراسة أن الرقابة والمساءلة ليستا عنصريين ثانويين يضافان إلى التحري بعد اكتماله، بل تمثلان جزءاً من بنيته القانونية. فتوثيق القرارات، وتحديد المسؤوليات، ومراجعة الإجراءات، وتوفير آليات الشكوى والتظلم وفق القانون، كلها أدوات تحد من إساءة استخدام السلطة وتدعم الثقة في مشروعية الممارسة الأمنية.

رابعاً: النتائج المتعلقة بوسائل الحصول على المعلومات الرقمية والتحقق منها

أظهر البحث أن مصادر المعلومات الرقمية متعددة، وتشمل المحتوى المنشور للعموم، والسجلات وقواعد البيانات، والمعلومات المقدمة من الأفراد والمؤسسات، والبيانات المستمدة من الأجهزة والأنظمة والخدمات الرقمية، فضلاً عن المعلومات التي يتم الحصول عليها من خلال التعاون المؤسسي أو الدولي.

ولا تتمتع هذه المصادر بدرجة واحدة من الموثوقية أو بالقواعد القانونية ذاتها. فإتاحة المعلومة للعموم قد تسهل الوصول إليها، لكنها لا تثبت صحتها، ولا تضمن أن إعادة جمعها أو ربطها أو استخدامها لأغراض أخرى أمر جائز في جميع الأحوال. كما أن وجود المعلومة في قاعدة بيانات رسمية لا يعفي من التحقق من تاريخ تحديثها ودقة محتواها والقيود القانونية المفروضة على استعمالها.

وتوصلت الدراسة إلى أن استخبارات المصادر المفتوحة تمثل وسيلة مهمة في التحريات الرقمية، لكنها تتطلب التمييز بين وجود المحتوى على الإنترنت وثبوت صحة مضمونه، وبين نسبة الحساب إلى شخص معين وإثبات أن ذلك الشخص هو الذي أنشأ المحتوى أو نشره. فقد يكون الحساب منتهكاً، أو مشترك الاستخدام، أو مخترقاً، كما قد يعاد نشر صورة أو مقطع فيديو قديم في سياق جديد، بما يؤدي إلى استنتاجات خاطئة إذا لم يتحقق الباحث من المصدر الأصلي وتاريخ النشر وسياق الواقعة.

كما أكدت الدراسة أن التحقق من الصور ومقاطع الفيديو لا ينبغي أن يعتمد على المظهر البصري وحده. إذ يتطلب، بحسب طبيعة المحتوى والادعاء المراد التحقق منه، النظر في مصدر المادة، وتاريخ ظهورها، والبيانات الوصفية المتاحة، والعناصر المكانية والزمانية، والمقارنة بالمصادر المستقلة، والتحقق من احتمالات التعديل أو الاقتطاع أو التوليد الاصطناعي. ومع ذلك، فإن غياب مؤشرات التلاعب الظاهرة لا يثبت بصورة قاطعة أصالة المحتوى، كما أن اكتشاف تعديل تقني لا يعني بالضرورة أن المادة بأكملها مزيفة أو عديمة القيمة.

وفيما يتعلق بوسائل الرصد الرقمي، خلصت الدراسة إلى ضرورة التمييز بين المشاهدة العامة والتصوير والمراقبة المستمرة وجمع بيانات الاتصالات والوصول إلى الأجهزة والأنظمة الرقمية. فاختلاف الوسائل يؤدي إلى اختلاف طبيعة التدخل في الحقوق، ويستوجب تقييماً قانونياً وفنياً يتناسب مع مستوى التدخل ونوع البيانات التي يمكن الحصول عليها.

كما تبين أن الحصول على بيانات الاتصالات والبيانات المرتبطة بالأجهزة قد يكشف عن معلومات تتجاوز المحتوى المباشر للاتصال، بما في ذلك أنماط التواصل أو الموقع أو توقيت النشاط، بحسب نوع البيانات المتاحة ودقتها. ولذلك، فإن التمييز بين محتوى الاتصالات والبيانات الوصفية مهم لفهم طبيعة المعلومات، لكنه لا يصلح وحده أساساً للحكم بأن إحدى الفئتين لا تستوجب حماية قانونية.

وأوضحت الدراسة أن الوصول إلى الأجهزة والأنظمة والخدمات السحابية يثير إشكالات متشابهة تتعلق بنطاق الإذن، ومكان تخزين البيانات، وحقوق الأطراف الأخرى، والتشفير، والاختصاص القضائي، وإمكان التعاون الدولي. ولا يؤدي وجود البيانات في خدمة سحابية إلى

زوال الحماية القانونية عنها، كما لا يكفي وجود الجهاز مادياً في نطاق اختصاص جهة معينة لحسم جميع المسائل المتعلقة بالبيانات التي يمكن الوصول إليها من خلاله.

ومن ثم، فإن مشروعية الحصول على المعلومات الرقمية تظل مرتبطة بالسند القانوني وطبيعة البيانات ونطاق الإجراء، وليس بمجرد سهولة الوصول التقني إليها.

خامساً: النتائج المتعلقة بالأصالة والسلامة والتوثيق والقيمة القانونية

أثبتت الدراسة أن سلامة المعلومات الرقمية ومشروعية الحصول عليها وموثوقيتها وقيمتها القانونية مفاهيم مترابطة، لكنها ليست مترادفة، ولا يجوز دمجها في حكم واحد.

فمشروعية الحصول على المعلومات تتعلق بالسند القانوني والاختصاص والالتزام بالضوابط المنظمة للإجراء. أما الأصالة فتتصل بإمكان التحقق من مصدر البيانات ونسبتها إلى النظام أو الجهاز أو الحساب الذي أنشأها. وتتعلق السلامة الفنية بمدى الحفاظ على البيانات من التغيير أو الفقد غير الموثق. بينما تتعلق الموثوقية بمدى إمكان الاعتماد على المعلومات في ضوء مصدرها وسياقها وطرق التحقق منها. أما القيمة القانونية فتتحدد وفق القواعد الإجرائية والإثباتية المعمول بها، وطبيعة المسألة المراد إثباتها، وتقدير الجهة المختصة.

ويترتب على هذا التمييز أن اجتياز البيانات لاختبار السلامة الفنية لا يحسم وحده مشروعية الحصول عليها، كما أن ثبوت مشروعية الجمع لا يثبت صحة كل استنتاج مستخلص منها. وقد تكون البيانات محفوظة بصورة سليمة، لكنها غير كافية لإثبات الواقعة المدعى بها، أو لا تسمح بنسبة الفعل إلى شخص معين بدرجة من اليقين تتناسب مع الغرض القانوني المراد تحقيقه.

وفي هذا الإطار، خلصت الدراسة إلى أهمية سلسلة العهدة الرقمية بوصفها وسيلة لتوثيق انتقال البيانات من مرحلة الجمع إلى الاستلام والفحص والحفظ والتقديم. وتزداد قيمة هذه السلسلة كلما تضمنت معلومات واضحة عن الأشخاص الذين تعاملوا مع البيانات، وأوقات انتقالها، ووسائل حفظها، والإجراءات التي أجريت عليها، وأسباب أي تغيير طرأ عليها.

كما أكدت الدراسة أهمية استخدام قيم التجزئة الرقمية في التحقق من تطابق البيانات الرقمية أو النسخ التي جرى حساب تلك القيم لها. غير أن قيمة التجزئة لا تثبت، بمفردها، صحة المحتوى أو تاريخ إنشائه أو هوية منشئه أو مشروعية الحصول عليه. فهي أداة للتحقق من خاصية فنية محددة، وليست بديلاً عن التحقق من المصدر والسياق والإجراءات.

وتوصلت الدراسة كذلك إلى أن التوثيق الفني لا ينبغي أن يقتصر على تسجيل الخطوات المنفذة، بل يجب أن يتيح فهم منهج الفحص، والأدوات المستخدمة وإصداراتها، والافتراضات التي قام عليها التحليل، والقيود التي قد تؤثر في النتيجة، ومدى إمكان إعادة الفحص والتحقق المستقل.

أما من حيث القيمة القانونية، فقد تبين أن قبول المعلومات أو الأدلة الرقمية وتحديد وزنها في الإثبات يخضعان للقانون المختص، ولا يمكن تقرير قاعدة عامة موحدة لجميع الأنظمة القانونية بشأن استبعاد كل معلومة تم الحصول عليها بطريقة غير مشروعة، أو قبول كل معلومة سليمة فنياً. فالأثر القانوني للمخالفة يتوقف على طبيعتها، والنصوص المنطبقة، والضمانة التي تم الإخلال بها، والجزاء الذي يقرره النظام القانوني المعني.

وتؤكد هذه النتيجة ضرورة تجنب الاستخدام المطلق لمصطلح "حجية الدليل الرقمي" دون بيان المقصود به. والأدق هو الفصل بين الأصالة والسلامة الفنية، ومشروعية الحصول على البيانات، وقبولها وفق قواعد الإثبات، والوزن الذي تمنحه لها الجهة المختصة في ضوء مجمل الأدلة والظروف.

وفيما يتعلق بالتقارير الأمنية والفنية، أثبت البحث أن جودة التقرير لا تقاس بكثرة المعلومات التي يتضمنها، وإنما بوضوح مصدر كل معلومة، ودقة وصف الإجراءات، والتمييز بين الوقائع والاستنتاجات والفرضيات، والإفصاح عن أوجه القصور والشك. كما أن وجود سجل تفصيلي للإجراءات لا يثبت وحده صحة التحليل، تمامًا كما أن صحة نتيجة فنية محتملة لا تعفي من ضرورة توثيق الطريق الذي أفضى إليها.

سادسًا: النتائج المستخلصة من التقييم التطبيقي وحدود تعميمها

استهدف الجانب التطبيقي من الدراسة اختبار مدى إمكان توظيف المعايير القانونية والفنية التي جرى تحليلها في تقييم منظومة التحريات الأمنية الرقمية، من خلال تنظيم عملية التقييم حول مشروعية الإجراء، وسلامة جمع المعلومات، وموثوقية المصادر، وصحة الاستنتاجات، وكفاية التوثيق، ومدى قابلية النتائج للمراجعة.

وقد أبرز هذا الإطار أن التقييم المتكامل للتحريات الرقمية ينبغي أن يبدأ بتحديد الواقعة أو المسألة محل التحري، ثم فحص السند القانوني للإجراءات، وتحديد مصادر المعلومات، والتحقق من طرق الحصول عليها، وتقييم سلامتها وأصالتها، واختبار الفرضيات البديلة، وأخيرًا تقدير مدى اتساق الاستنتاجات مع المعطيات المتاحة.

وتكمن القيمة العلمية لهذا المنهج في أنه يمنع اختزال التقييم في أحد أبعاده. فلا يكفي أن تكون الإجراءات موثقة إذا كان أساسها القانوني غير واضح، ولا يكفي أن يكون جمع المعلومات مشروعًا إذا كانت البيانات غير موثوقة، ولا تكفي سلامة البيانات إذا كانت الاستنتاجات المستخلصة منها لا تستند إلى قرائن كافية.

كما يتيح هذا المنهج تحديد مواطن القصور بدقة أكبر، والتمييز بين العيوب القانونية والإجرائية والفنية والتحليلية، وهو تمييز ضروري لتحديد نوع المعالجة المطلوبة. فقد يتطلب القصور القانوني مراجعة السند التشريعي أو حدود الاختصاص، بينما يستدعي الخلل الفني تحسين إجراءات الحفظ والفحص، ويقتضي ضعف التحليل إعادة اختبار الفرضيات أو مراجعة مصادر المعلومات، في حين قد يتطلب قصور التوثيق استكمال السجلات أو بيان حدود إمكان التحقق من النتائج.

ومع ذلك، فإن النتائج المستخلصة من التطبيق لا يجوز تعميمها على جميع الجهات الأمنية أو الأنظمة القانونية أو أنواع التحريات الرقمية دون مراعاة طبيعة الحالات التي شملها التقييم، ومدى توافر البيانات، والمنهج المستخدم في اختيار الحالات وتحليلها. فالتقييم التطبيقي، مهما بلغت دقته، يظل مرتبطًا بنطاقه ومصادره وحدود أدواته، ولا يتحول إلى دليل على وجود ممارسة مؤسسية عامة ما لم تدعمه بيانات كافية ومثثلة.

كما أن التوصل إلى أوجه قصور في حالة محددة لا يكفي وحده لإثبات قصور تشريعي شامل، إذ قد يرجع الخلل إلى التطبيق أو التدريب أو الموارد أو غياب إجراءات مؤسسية واضحة، وليس بالضرورة إلى النص القانوني ذاته.

وعليه، ينبغي أن تقرأ النتائج التطبيقية بوصفها أساساً لتحديد المشكلات التي ظهرت في الحالات محل التقييم، واستخلاص الدروس الممكنة منها، وصياغة توصيات تتناسب مع نطاق الأدلة المتاحة، لا بوصفها أحكاماً قطعية على جميع صور التحري الرقمي.

سابعاً: التوصيات التشريعية والإجرائية والفنية والمؤسسية

استناداً إلى النتائج السابقة، تقترح الدراسة مجموعة من التوصيات التي تستهدف معالجة مواطن القصور المحتملة وتعزيز التكامل بين المشروعية القانونية والكفاءة الفنية والرقابة المؤسسية.

١ التوصيات التشريعية

أولاً: وضع إطار قانوني واضح للتحريات الأمنية الرقمية.

توصي الدراسة بأن تتضمن التشريعات أو اللوائح المختصة قواعد واضحة تحدد أغراض التحري الرقمي، والجهات المخولة بممارسته، ونطاق سلطاتها، وشروط استخدام الوسائل المختلفة، والحالات التي تتطلب إذنًا قضائيًا أو تصريحًا خاصًا. وينبغي أن يراعي هذا التنظيم التفاوت بين الوسائل من حيث مستوى التدخل في الحقوق والحريات، بدلاً من إخضاعها جميعاً لحكم موحد لا يعكس اختلاف طبيعتها.

وترتبط هذه التوصية بالنتيجة التي أثبتت أن الإمكان التقني لا ينشئ بذاته سلطة قانونية، وأن الغموض في تحديد الاختصاص قد يؤدي إلى تفاوت الممارسات وصعوبة الرقابة على مشروعاتها.

ثانياً: تنظيم الوصول إلى البيانات بحسب طبيعتها ودرجة حساسيتها.

توصي الدراسة بوضع قواعد تميز بين المعلومات المتاحة للعموم، والبيانات المقيدة، والبيانات الشخصية الحساسة، وبيانات الاتصالات، والبيانات المستمدة من الأجهزة والخدمات السحابية. ويجب أن يحدد التنظيم الشروط القانونية للوصول إلى كل فئة، والقيود المتعلقة بنسخها ومعالجتها وتبادلها والاحتفاظ بها.

ولا يعني هذا التمييز افتراض أن كل فئة تخضع لنظام قانوني مستقل بالضرورة، وإنما المقصود ضمان أن تعكس قواعد الوصول طبيعة البيانات ومدى اتصالها بالحقوق الأساسية.

ثالثاً: تعزيز الضمانات المتعلقة بالخصوصية والبيانات الشخصية.

توصي الدراسة بإقرار أو تعزيز قواعد تحديد الغرض، وتقليل البيانات، وتقييد الاستخدامات اللاحقة، وتحديد مدد الاحتفاظ، وضبط مشاركة المعلومات، وإتلاف البيانات التي لم يعد الاحتفاظ بها ضرورياً أو مشروعاً. كما ينبغي أن تتناول هذه القواعد البيانات المتعلقة بالأشخاص غير المستهدفين التي تجمع عرضاً أثناء التحري.

رابعاً: تحديد الآثار القانونية للمخالفات الإجرائية.

توصي الدراسة بأن تتسم القواعد المتعلقة بالجزاءات الإجرائية بالوضوح، وأن تبين، في حدود النظام القانوني المختص، أثر تجاوز الاختصاص أو مخالفة الإذن أو الإخلال بالضمانات الجوهرية في إمكان الاستناد إلى المعلومات أو الأدلة المتحصلة. ويجب أن يراعى في ذلك اختلاف طبيعة المخالفة والجزاء المقرر لها، دون افتراض أن جميع المخالفات تنتج أثراً قانونياً واحداً.

٢ التوصيات الإجرائية

أولاً: اعتماد إجراءات مكتوبة لتخطيط التحري الرقمي.

ينبغي أن تبدأ كل عملية تحريّ، بحسب طبيعتها وما يفرضه القانون، بتحديد موضوع التحري والغرض منه، والجهة المختصة، ومصادر المعلومات المستهدفة، والنطاق الزمني والموضوعي للإجراء، والقيود القانونية ذات الصلة، والضمانات اللازمة لحماية البيانات غير المرتبطة بالواقعة.

ويستند ذلك إلى أن وضوح نطاق التحري يساعد على الحد من الجمع العشوائي، ويسرّ المراجعة اللاحقة، ويتيح تقييم مدى تناسب الوسيلة المستخدمة مع الهدف المراد تحقيقه.

ثانياً: توحيد إجراءات توثيق جمع المعلومات.

توصي الدراسة باعتماد نماذج مهنية توثق مصدر المعلومة، وتاريخ الحصول عليها، وطريقة جمعها، والقائم بالإجراء، والسند القانوني عند لزومه، وأي قيود تؤثر في تفسيرها. كما ينبغي المحافظة على البيانات الأصلية متى كان ذلك ممكناً ومشروعاً، مع بيان أي معالجة أو تحويل يطرأ عليها.

ثالثاً: الفصل الواضح بين المعلومات الأولية والنتائج التحليلية.

ينبغي أن تتضمن محاضر التحري وتقاريره تمييزاً صريحاً بين ما تمت ملاحظته أو التحقق منه مباشرة، وما ورد من مصادر أخرى، وما استخلصه القائم بالتحليل، وما لا يزال في نطاق الفرضية. كما ينبغي اختبار التفسيرات البديلة والإفصاح عن مواطن الشك بدلاً من عرض الاستنتاجات الاحتمالية باعتبارها حقائق ثابتة.

رابعاً: إرساء إجراءات للمراجعة القانونية والفنية.

توصي الدراسة بإدراج مراجعة مناسبة لطبيعة الإجراء، قبل تنفيذه أو أثناءه أو بعده، للتحقق من الالتزام بالسند القانوني، ونطاق الإذن، وقواعد حماية البيانات، ومتطلبات التوثيق، وسلامة النتائج. وتزداد أهمية المراجعة المستقلة عندما يتعلق الأمر بإجراءات واسعة النطاق أو بيانات شديدة الحساسية أو استنتاجات قد تترتب عليها آثار قانونية جسيمة.

٣ التوصيات الفنية

أولاً: اعتماد معايير واضحة لحفظ البيانات الرقمية وفحصها.

ينبغي أن تتضمن الإجراءات الفنية قواعد لحفظ البيانات الأصلية، وإنشاء النسخ اللازمة للفحص، وتوثيق عمليات النقل والمعالجة، واستخدام وسائل مناسبة للتحقق من سلامة البيانات، بما في ذلك قيم التجزئة الرقمية عند ملامتها. كما يجب توثيق الأدوات المستخدمة وإصداراتها والقيود المعروفة التي قد تؤثر في النتائج.

ثانيًا: تعزيز قابلية إعادة الفحص والتحقق المستقل.

توصي الدراسة بتصميم إجراءات الفحص بحيث تسمح، في حدود القانون وإمكانات الحفظ، بإعادة التحقق من النتائج ومراجعة الخطوات التي أدت إليها. ولا يتحقق ذلك بمجرد الاحتفاظ بالنتيجة النهائي، بل يتطلب حفظ ما يلزم من سجلات العمل والبيانات ذات الصلة ومعلومات الأدوات والمنهج المستخدم.

ثالثًا: تطوير منهجيات التحقق من المحتوى الرقمي.

ينبغي اعتماد أساليب متعددة للتحقق من الصور ومقاطع الفيديو والمحتوى المنشور، وعدم الاعتماد على مؤشرات منفردة لإثبات الأصالة أو التلاعب. كما ينبغي الإفصاح عن حدود أدوات الكشف الآلي، ولا سيما عند فحص المحتوى المعدل أو المولد اصطناعياً، مع التمييز بين المؤشرات الفنية والنتائج التي يمكن إثباتها بصورة مستقلة.

رابعًا: تحسين إدارة البيانات الوصفية.

توصي الدراسة بوضع إجراءات للتحقق من بيانات التوقيت والموقع وسجلات الأنظمة، مع مراعاة اختلاف المناطق الزمنية، وإعدادات الأجهزة، ودقة المستشعرات، واحتمالات التعديل أو الانقطاع. وينبغي ألا تستخدم هذه البيانات لإثبات واقعة أو نسبة فعل إلى شخص دون تقييم حدود دقتها وصلتها بالاستنتاج المطلوب.

٤. التوصيات المؤسسية والمهنية

أولاً: تعزيز التأهيل القانوني والفني للقائمين بالتحري.

توصي الدراسة ببرامج تدريبية تجمع بين المعرفة القانونية والمهارات الفنية والتحليل النقدي للمعلومات. فلا يكفي أن يمتلك القائم بالتحري القدرة على استخدام الأدوات التقنية، بل ينبغي أن يفهم حدودها، ويعرف القيود القانونية المنظمة لها، ويميز بين البيانات والقرائن والاستنتاجات، ويستوعب أثر التحيز ونقص المعلومات في النتائج.

ثانيًا: وضع سياسات مؤسسية للحوكمة والمساءلة.

ينبغي أن تتضمن السياسات الداخلية قواعد واضحة لتوزيع المسؤوليات، وإدارة صلاحيات الوصول، وتسجيل عمليات الاطلاع والمعالجة، ومراجعة الاستخدامات، والتعامل مع المخالفات، والإبلاغ عن الأخطاء وتصحيحها. كما ينبغي تحديد المسؤوليات المتعلقة بحفظ البيانات ونقلها ومشاركتها وإتلافها.

ثالثًا: الفصل بين التوثيق وضمان الجودة.

توصي الدراسة بالألا يُنظر إلى التوثيق باعتباره بديلاً عن المراجعة الفنية. فالتوثيق يثبت ما جرى تسجيله من إجراءات، بينما تهدف مراجعة الجودة إلى تقييم مدى صحة تنفيذها وسلامة النتائج المستخلصة منها. ومن ثم، يجب أن تتضمن المنظومة المؤسسية المسارين معاً.

رابعاً: تعزيز التنسيق بين الجهات الأمنية والعلمية والفنية.

توصي الدراسة بتطوير آليات واضحة لتبادل المعلومات بين الجهات المختصة، وتحديد المسؤوليات عند انتقال البيانات، وتوحيد الحد الأدنى من متطلبات التوثيق وسلسلة العهدة، مع مراعاة اختلاف الاختصاصات والقيود القانونية المتعلقة بالمشاركة. وينبغي ألا يؤدي التعاون المؤسسي إلى تجاوز شروط الوصول إلى البيانات أو توسيع نطاق استخدامها دون سند قانوني.

خامساً: تنظيم استخدام الذكاء الاصطناعي في التحريات الرقمية.

ينبغي إخضاع الأنظمة الآلية المستخدمة في تصنيف البيانات أو التعرف على الأنماط أو تحليل الصور أو تقييم المحتوى لضوابط تتعلق بالدقة والشفافية وتوثيق الاستخدام والتحقق البشري من النتائج. كما يجب بيان حدود النظام ومواطن الخطأ المحتملة، وعدم التعامل مع مخرجاته بوصفها حقائق نهائية لمجرد صدورها عن أداة تقنية متقدمة.

وترتبط هذه التوصية بالنتيجة التي مفادها أن تعقيد الأدوات التقنية لا يلغي ضرورة التحقق من مخرجاتها، وأن الاعتماد غير النقدي على النتائج الآلية قد ينقل الأخطاء والتحيزات إلى القرارات الأمنية أو القانونية.

ثامناً: مقترحات الدراسات المستقبلية

على الرغم من أن الدراسة تناولت الجوانب المفاهيمية والقانونية والفنية للتحريات الأمنية الرقمية في إطار عام، فإن التطور المتواصل في الوسائل الرقمية يفتح مجالات بحثية متعددة تستحق مزيداً من التعمق، ولا سيما في المسائل التي يتداخل فيها التنظيم القانوني مع التقدم التقني وتفاوت الممارسات المؤسسية.

أولاً: دراسة مقارنة للتنظيم القانوني للتحريات الأمنية الرقمية.

يُفترح إجراء دراسة مقارنة بين عدد من الأنظمة القانونية المختارة، بهدف تحليل شروط الحصول على البيانات الرقمية، وحدود الاختصاص الأمني والقضائي، ومتطلبات الإذن، والضمانات المتعلقة بالخصوصية، والآثار القانونية للمخالفات الإجرائية. وينبغي أن يقوم اختيار الأنظمة محل المقارنة على معايير معلنة، وأن يراعي الاختلاف بين البنية الدستورية والتشريعية والإجرائية لكل نظام.

ثانياً: دراسة أثر البيانات الوصفية في الإثبات الجنائي.

يُفترح بحث مستقل يتناول القيمة الاستدلالية لبيانات الموقع والتوقيت والاتصالات وسجلات الأنظمة، مع التركيز على حدود دقتها، وإمكان تعديلها، ومشكلات تفسيرها، ومدى قدرتها على دعم الاستنتاجات المتعلقة بالهوية أو الحركة أو العلاقة بين الأشخاص والوقائع.

ثالثاً: دراسة الضمانات القانونية لاستخدام استخبارات المصادر المفتوحة.

يمكن أن تتناول هذه الدراسة الحدود الفاصلة بين جمع المحتوى المنشور للعموم والمراقبة المنظمة، وأثر تجميع البيانات المتفرقة في الخصوصية، والقيود المتعلقة بإعادة الاستخدام، والضمانات اللازمة عند استخدام أدوات التحليل الآلي للمحتوى المنشور.

رابعاً: دراسة حجية المحتوى الرقمي المعدل أو المولد اصطناعياً.

يُفترض بحث العلاقة بين تقنيات التحقق من أصالة المحتوى والمعايير القانونية لقبول الأدلة الرقمية وتقدير قيمتها، مع التركيز على الصور ومقاطع الفيديو والتسجيلات الصوتية التي يحتمل تعديلها أو توليدها اصطناعياً. وينبغي أن يميز هذا البحث بين الكشف الفني عن مؤشرات التلاعب وبين إثبات واقعة التوليد أو التعديل ونسبتها إلى فاعل معين.

خامساً: دراسة المسؤولية القانونية عن أخطاء أنظمة التحليل الآلي.

تستحق المسؤولية عن القرارات أو الاستنتاجات المتأثرة بمخرجات الأنظمة الآلية دراسة مستقلة، تتناول دور الجهة المستخدمة، ومزود النظام، والقائم بالتحليل، والجهة التي تعتمد النتائج في اتخاذ القرار، مع مراعاة اختلاف المسؤوليات بحسب طبيعة النظام والالتزامات القانونية ذات الصلة.

سادساً: دراسة تقييمية للتطبيق المؤسسي لمعايير التوثيق وسلسلة العهدة الرقمية.

يُفترض إجراء بحوث ميدانية أو دراسات حالات، متى توافرت إمكانية الوصول المشروع إلى البيانات اللازمة، لقياس مدى تطبيق متطلبات توثيق الجمع والنقل والفحص والحفظ، وتحديد أكثر مواطن القصور شيوعاً، وتقييم أثر إجراءات ضمان الجودة في قابلية إعادة الفحص والثقة في النتائج.

سابعاً: دراسة التنظيم القانوني لاستخدام الطائرات المسييرة في التحريات الأمنية.

يمكن تخصيص دراسة مستقلة لتحليل العلاقة بين قواعد الطيران وسلامة التشغيل، والاختصاصات الأمنية، وحماية الخصوصية، وجمع الصور والبيانات الوصفية، وسلامة التسجيلات الجوية وقيمتها الاستدلالية. وتزداد أهمية هذا الموضوع عند دراسة الاستخدامات التي تتضمن تصويراً مستمراً أو جمع بيانات عن أشخاص غير مستهدفين أو نقل المعلومات عبر الحدود.

ثامناً: دراسة أثر التعاون الدولي في الوصول إلى البيانات الرقمية.

يُفترض بحث الإشكالات المرتبطة بتوزيع البيانات بين دول متعددة، وتعارض قواعد الاختصاص وحماية البيانات، وشروط المساعدة القانونية المتبادلة، وآليات تبادل المعلومات وحفظها. وينبغي أن تميز الدراسة بين الحصول على البيانات في إطار التعاون الرسمي وبين صور الوصول الأخرى، وأن تقيم كل صورة وفق السند القانوني والضمانات المنطبقة عليها.

الملاحق

❖ الملاحق

الملحق الأول: نموذج توثيق جمع المعلومات الرقمية ومصادرها

رقم النموذج _____

الجهة القائمة بالتحري _____

رقم الملف/القضية _____

تاريخ الجمع ____/____/____ الوقت: ____:____ المنطقة الزمنية _____

القائم بالجمع _____

الصفة الوظيفية _____

أولاً: بيانات المصدر

العنصر	البيان
نوع المصدر	☐ مصدر مفتوح ☐ سجل/قاعدة بيانات ☐ معلومات مقدمة من فرد/جهة ☐ جهاز/نظام ☐ طائرة مسيرة ☐ مصدر آخر: _____
اسم المصدر/الجهة	_____
رابط المصدر/المعرف	_____
تاريخ إنشاء المعلومة	(إن عُرف) ____/____/____
تاريخ النشر/الإتاحة	(إن عُرف) ____/____/____
تاريخ الحصول عليها	____/____/____
الوسيلة المستخدمة	☐ بحث مباشر ☐ طلب رسمي ☐ استخراج فني ☐ تصوير جوي ☐ أخرى: _____
الأداة المستخدمة	_____
إصدار الأداة	_____

ثانياً: وصف المادة المجموعة

العنصر	البيان
نوع المادة	☐ نص ☐ صورة ☐ فيديو ☐ تسجيل صوتي ☐ سجل إلكتروني ☐ بيانات وصفية ☐ أخرى _____
عدد الملفات/العناصر	
الحجم/المدة	
صيغة الملف	
قيمة التجزئة (Hash)	
خوارزمية التجزئة	

ثالثاً: السند القانوني

العنصر	البيان
الأساس القانوني	
رقم الإذن/التصريح	
الجهة المانحة	
تاريخ الإذن	
نطاق الإذن	
مدة الإذن	

رابعاً: التحقق من المصدر

العنصر	البيان
هل تم التحقق من المصدر؟	☐ نعم ☐ لا ☐ جزئياً
طريقة التحقق	
مصادر مستقلة مؤيدة	
قيود التحقق	

خامساً: توقيعات

الصفة	الاسم	التوقيع	التاريخ
القائم بالجمع			___/___/___
المراجع المباشر			___/___/___
رئيس القسم			___/___/___

الملحق الثاني: نموذج سجل سلسلة العهدة الرقمية

رقم السجل _____

رقم الملف/القضية _____

وصف المادة _____

المعرّف الفريد _____

#	التاريخ والوقت	الجهة/الشخص المستلم	الجهة/الشخص المسلم	الغرض من النقل/الإجراء	حالة المادة	التوقيع	ملاحظات
1				استلام أولي	☐ سليمة ☐ تالفة ☐ مجزأة		
2				نقل إلى المختبر	☐ سليمة ☐ تالفة ☐ مجزأة		
3				نسخ فني	☐ سليمة ☐ تالفة ☐ مجزأة		
4				فحص وتحليل	☐ سليمة ☐ تالفة ☐ مجزأة		
5				إعادة إلى المخزن	☐ سليمة ☐ تالفة ☐ مجزأة		

بيانات إضافية

العنصر	البيان
قيمة التجزئة عند الاستلام	
قيمة التجزئة بعد الفحص	
هل تطابقت القيمتان؟	☐ نعم ☐ لا (يرفق تقرير بالاختلاف)
أي انقطاع في السلسلة؟	☐ لا ☐ نعم (يرفق بيان بالأسباب)
ملاحظات عامة	

توقيعات

التاريخ	التوقيع	الاسم	الصفة
____/____/____			مسؤول العهد
____/____/____			المراجع

الملحق الثالث: نموذج محضر تحرر أمني رقمي

رقم المحضر: _____

الجهة: _____

تاريخ التحري: ____/____/____ الوقت: ____:____ المنطقة الزمنية: ____

القائم بالتحري: _____

الصفة: _____

أولاً: موضوع التحري

البيان	العنصر
	وصف الواقعة/المسألة

الغرض من التحري	
الأساس القانوني	
رقم الإذن (إن وجد)	
نطاق التحري	

ثانياً: الإجراءات المتخذة

م	الإجراء	التاريخ والوقت	الأداة/الوسيلة	النتيجة	ملاحظات
1					
2					
3					

ثالثاً: المعلومات التي تم جمعها

#	وصف المعلومة	المصدر	درجة التحقق	ملاحظات
1			☐ متحققة ☐ جزئية ☐ غير متحققة	
2			☐ متحققة ☐ جزئية ☐ غير متحققة	
3			☐ متحققة ☐ جزئية ☐ غير متحققة	

رابعاً: القيود والصعوبات

البيان	العنصر
	قيود قانونية
	قيود فنية
	قيود ميدانية
	إفصاح عن عدم اليقين

خامساً: التوصيات الأولية

الأولية	الجهة المقترحة	التوصية
☐ عالية ☐ متوسطة ☐ منخفضة		
☐ عالية ☐ متوسطة ☐ منخفضة		

سادساً: توقيعات

التاريخ	التوقيع	الاسم	الصفة
___/___/___			القائم بالتحري
___/___/___			المراجع
___/___/___			رئيس القسم

الملحق الرابع: نموذج تقرير فني عن البيانات الرقمية

رقم التقرير: _____

الجهة الطالبة: _____

الجهة المعدة: _____

تاريخ التقرير: ___/___/___

الخبير/المحلل: _____

التخصص: _____

أولاً: مقدمة التقرير

العنصر	البيان
موضوع الفحص	
الأسئلة المطروحة	
نطاق الفحص	

_____	حدود الفحص
-------	------------

ثانياً: البيانات محل الفحص

البيان	العنصر
صور ☐ فيديو ☐ سجلات ☐ بيانات وصفية ☐ ملفات ☐ أخرى : _____	نوع البيانات
_____	المصدر
____/____/____	تاريخ الاستلام
سليمة ☐ تالفة ☐ مجزأة ☐	حالة المادة
_____	قيمة التجزئة

ثالثاً: المنهجية والأدوات

البيان	العنصر
	المنهج المتبع
	الأدوات المستخدمة
	إصدارات الأدوات
	الإعدادات المؤثرة
	الخطوات المنفذة

رابعاً: النتائج الفنية

م	النتيجة	مستوى الثقة	الأساس
1	_____	عالي ☐ متوسط ☐ منخفض ☐	_____
2	_____	عالي ☐ متوسط ☐ منخفض ☐	_____
3	_____	عالي ☐ متوسط ☐ منخفض ☐	_____

خامساً: القيود ومواطن عدم اليقين

البيان	العنصر
_____	قيود المصدر
_____	قيود الإجراء

العنصر	البيان
قيود التفسير	_____
ما لم يتم التحقق منه	_____

سادساً: الخلاصة والتوصيات

العنصر	البيان
الخلاصة	_____
التوصيات	_____
الحاجة إلى فحص إضافي	☐ نعم ☐ لا

سابعاً: توقيعات

الصفة	الاسم	التاريخ	التوقيع
الخبير/المح لل	_____	____/____/____	_____
مراجع الجودة	_____	____/____/____	_____
رئيس القسم	_____	____/____/____	_____

الملحق الخامس: قائمة تحقق لمشروعية استخدام وسائل الرصد

الجهة: _____

الوسيلة ☐ كاميرات مراقبة ☐ طائرة مسيرة ☐ تتبع موقع ☐ اعتراض اتصالات ☐
أخرى: _____

تاريخ التقييم: ____/____/____

البيان	غير منطبق	لا	نعم	السؤال	ملاحظات
أولاً: السند القانوني					
1	☐	☐	☐	هل يوجد نص قانوني يجيز استخدام الوسيلة؟	
2	☐	☐	☐	هل الجهة القائمة بالرصد مختصة قانوناً؟	
3	☐	☐	☐	هل الغرض من الرصد مشروع ومحدد؟	
ثانياً: الإذن					
4	☐	☐	☐	هل يتطلب القانون إذناً قضائياً أو تصريحاً؟	
5	☐	☐	☐	إذا كان مطلوباً، هل تم الحصول عليه؟	
6	☐	☐	☐	هل الإذن محدد النطاق والمدة والغرض؟	
ثالثاً: التناسب					
7	☐	☐	☐	هل الوسيلة ملائمة لتحقيق الغرض؟	
8	☐	☐	☐	هل توجد وسيلة أقل تدخلاً؟	
9	☐	☐	☐	هل الأثر متناسب مع أهمية الهدف؟	
رابعاً: الخصوصية	☐	☐	☐		
10	☐	☐	☐	هل تم تحديد نطاق الرصد بدقة؟	
11	☐	☐	☐	هل تم تجنب تصوير الأماكن الخاصة؟	
12	☐	☐	☐	هل تمت حماية بيانات غير المعنيين؟	
خامساً: البيانات					
13	☐	☐	☐	هل تم تحديد الغرض قبل الجمع؟	
14	☐	☐	☐	هل تم تقليل البيانات إلى القدر اللازم؟	
15	☐	☐	☐	هل تم ضبط الوصول إلى البيانات؟	

البيان	غير منطبق	لا	نعم	السؤال	ملاحظات
16	☐	☐	☐	هل تم تحديد مدة الاحتفاظ وآلية الإتلاف؟	
سادساً: التوثيق					
17	☐	☐	☐	هل تم توثيق الإجراءات والقائمين بها؟	
18	☐	☐	☐	هل تم توثيق سلسلة العهدة؟	
19	☐	☐	☐	هل تم توثيق القيود ومواطن عدم اليقين؟	
سابعاً: الرقابة					
20	☐	☐	☐	هل يوجد إشراف أو رقابة مستقلة؟	
21	☐	☐	☐	هل توجد آلية للتظلم أو المراجعة؟	

نتيجة التقييم

النتيجة	☐ مستوفٍ ☐ مستوفٍ مع ملاحظات ☐ غير مستوفٍ
التوقيع	_____

الملحق السادس: نموذج مراجعة جودة التقرير الأمني أو الفني

رقم التقرير المراجع:

نوع التقرير ☐: أمني ☐ فني ☐ محضر تحرّ

المراجع: _____

تاريخ المراجعة: ____/____/____ :

#	معيّار المراجعة	ضعيف	مقبول	جيد	ممتاز	ملاحظات
أولاً: البنية والمحتوى						
1	وضوح موضوع التقرير والغرض منه	☐	☐	☐	☐	

2	اكتمال العناصر الأساسية (مصادر، منهجية، نتائج، قيود)		☐	☐	
---	--	--	--------------------------	--------------------------	--

قائمة المراجع

أولاً: المراجع العربية

أ. الكتب والدراسات

١. خراشي، عادل عبد العال. ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي. 2006.
٢. شجاع، محمد محمد سيف. شرح قانون الإجراءات الجزائية اليمني. صنعاء: مكتبة الصادق، ٢٠٠٥.
٣. محمد، هشام مصطفى. التحريات الأمنية وأثرها في الأدلة الجنائية. الإسكندرية: دار المطبوعات الجامعية، ٢٠١٥.
٤. المرجان، عبد الرزاق؛ شوقي، محمد؛ السبعاني، يوسف؛ المنشاوي، محمد. الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية. الرياض: دار جامعة نايف للنشر، ٢٠٢٤.
٥. "كفاية التحري ومشروعيته". دراسة فقهية، مجلة كلية الحقوق، جامعة طنطا، ٢٠٢١.

ثانياً: التشريعات والوثائق الدولية

أ. وثائق الأمم المتحدة

١. الأمم المتحدة. العهد الدولي الخاص بالحقوق المدنية والسياسية. 1966.
٢. الأمم المتحدة. المبادئ الأساسية بشأن استقلال السلطة القضائية. 1985.
٣. لجنة حقوق الإنسان التابعة للأمم المتحدة. التعليق العام رقم ١٦ بشأن الحق في احترام الخصوصية والحياة الأسرية والمسكن والمراسلات وحماية الشرف والسمعة. الوثيقة CCPR/C/21/Rev.1، ١٩٨٨.
٤. مفوضية الأمم المتحدة السامية لحقوق الإنسان. الحق في الخصوصية في العصر الرقمي. الوثيقة A/HRC/48/31، ٢٠٢١.
٥. مفوضية الأمم المتحدة السامية لحقوق الإنسان. الحق في الخصوصية في العصر الرقمي. الوثيقة A/HRC/51/17، ٢٠٢٢.
٦. مكتب الأمم المتحدة المعني بالمخدرات والجريمة: (UNODC). Cybercrime Module 6: Digital Evidence Admissibility. Education for Justice Initiative, 2019.
٧. مكتب الأمم المتحدة المعني بالمخدرات والجريمة: (UNODC). Cybercrime Module 6: Handling of Digital Evidence. 2019.
٨. مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC). Report on the Meeting of the Expert Group on Cybercrime. CCPCJ/EG.4/2021/2. الوثيقة.

ب. وثائق مجلس أوروبا

١. مجلس أوروبا. Convention on Cybercrime. ETS No. 185، بودابست، ٢٣ نوفمبر ٢٠٠١.
٢. مجلس أوروبا. Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence. CETS No. 224، ٢٠٢٢.
٣. مجلس أوروبا. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. ETS No. 108، ١٩٨١.

٤. مجلس أوروبا *Convention for the Protection of Individuals with Regard to the Processing of Personal Data*. CETS No. 223، ٢٠١٨.
٥. مجلس أوروبا *International Standards on Collection and Handling of Electronic Evidence*. Cybercrime Programme Office.
٦. مجلس أوروبا *Milestones: تطور اتفاقية بودابست حتى عام ٢٠٢٦*.
- ج. التشريعات والوثائق الدولية الأخرى
 ١. الاتحاد الأوروبي (EU) *Regulation (EU) 2016/679، المادة ٩*.
 ٢. مملكة البحرين *قانون حماية البيانات الشخصية رقم ٣٠ لسنة ٢٠١٨*.
 ٣. منظمة التعاون الاقتصادي والتنمية (OECD). *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449، ٢٠١٩، المعدل في ٢٠٢٤.
- ثالثاً: الاجتهادات القضائية الدولية
 ١. المحكمة الأوروبية لحقوق الإنسان *Szabó and Vissy v. Hungary*. Application No. 37138/14، ١٢ يناير ٢٠١٦.
 ٢. المحكمة الأوروبية لحقوق الإنسان *Big Brother Watch and Others v. the United Kingdom*. Applications Nos. 58170/13، 62322/14، and 24960/15، ٢٥ مايو ٢٠٢١.
- رابعاً: البروتوكولات والأدلة الإرشادية المهنية
 ١. Human Rights Center, University of California, Berkeley, and United Nations Office of the High Commissioner for Human Rights. *Berkeley Protocol on Digital Open Source Investigations*. 2022.
 ٢. INTERPOL. *Guidelines for Digital Forensics First Responders*.
 ٣. منظمة المعايير الدولية (ISO) واللجنة الكهروتقنية الدولية (IEC). *ISO/IEC 17025:2017: General Requirements for the Competence of Testing and Calibration Laboratories*. 2017.
 ٤. منظمة المعايير الدولية (ISO) واللجنة الكهروتقنية الدولية (IEC). *ISO/IEC 23894:2023: Information Technology—Artificial Intelligence—Guidance on Risk Management*. 2023.
- خامساً: المراجع الفنية والمعايير الصادرة عن المعهد الوطني الأمريكي للمعايير والتقنية (NIST)
 ١. Ayers, Rick; Brothers, Sam; and Jansen, Wayne. *Guidelines on Mobile Device Forensics*. NIST Special Publication 800-101 Revision 1، ٢٠١٤.
 ٢. Guttman, Barbara; White, Douglas R.; Williams, Shannan; and Walraven, Tracy. *Digital Evidence Preservation: Considerations for Evidence Handlers*. NISTIR 8387. National Institute of Standards and Technology، سبتمبر ٢٠٢٢.
 ٣. Kent, Karen; Chevalier, Suzanne; Grance, Tim; and Dang, Hung. *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86. National Institute of Standards and Technology، أغسطس ٢٠٠٦.
 ٤. National Institute of Standards and Technology (NIST). *Secure Hash Standard*. FIPS PUB 180-4، ٢٠١٥.

٥. National Institute of Standards and Technology (NIST). *Digital Investigation Techniques: A NIST Scientific Foundation Review*. NISTIR 8354، ٢٠٢٢.
٦. National Institute of Standards and Technology (NIST). *Reducing Risks Posed by Synthetic Content*. NIST AI 100-4، ٢٠٢٤.

العنوان	المحتوى / الوصف
المقدمة	تمهيد: من التحريات التقليدية إلى الرقمية. إشكالية الدراسة: التوازن بين الأمن والحقوق. المنهجية: التحليلي المقارن. هيكل الكتاب.
الباب الأول: الإطار المفاهيمي والقانوني	التأصيل النظري لمفهوم التحريات الرقمية وأساسها القانوني وضماناتها.
الفصل الأول: ماهية التحريات الرقمية ونطاقها	المفهوم، الخصائص، التمييز عن المفاهيم المجاورة، طبيعة المعلومات، النطاق الوظيفي.
المبحث الأول: مفهوم التحريات ومقوماتها	مفهوم التحريات الأمنية، مفهوم الرقمية وخصائصها، تمييزها عن المفاهيم المجاورة.
المطلب الأول: مفهوم التحريات الأمنية ومقوماتها	تعريف التحريات، عناصرها، الفرق بينها وبين جمع المعلومات.
المطلب الثاني: مفهوم التحريات الرقمية وخصائصها	تعريف الرقمية، الطبيعة المركبة، الخصائص (الجمع المستمر، الربط، المعالجة الآلية، تفاوت التدخل).
المطلب الثالث: تمييزها عن المفاهيم المجاورة	التمييز عن جمع المعلومات، OSINT، التحقيق الجنائي الرقمي، التحقيق القضائي، الفحص الفني.
المبحث الثاني: طبيعة المعلومات وحدود الاستدلال	البيانات، المعلومات، القرائن، الأدلة، حدود الاستنتاج.
المطلب الأول: مفهوم البيانات والمعلومات وتصنيفاتها	التمييز بين البيانات والمعلومات، التصنيف بحسب المصدر والطبيعة ومستوى التحقق.
المطلب الثاني: المعلومات الأولية والقرائن والأدلة	التمييز بينها، القرينة القانونية والقضائية والتحليلية، الدليل الرقمي وشروط قبوله.
المطلب الثالث: حدود الاستنتاج من المعلومات	الفرق بين المسجل والمستنتج، أثر المصدر، حدود البيانات الوصفية، الارتباط والسببية، اختبار البدائل.
المبحث الثالث: النطاق الوظيفي للتحريات	النطاق الشخصي والموضوعي والزمني والمكاني والوسائلي، التمييز بين الأعمال الأمنية والإدارية والجزائية.

العنوان	المحتوى / الوصف
المطلب الأول: نطاق التحريات	الأشخاص، الموضوع، الزمان، المكان، الوسائل، مبدأ التناسب.
المطلب الثاني: التمييز بين الأعمال الأمنية والإدارية والجزائية	المعيار الوظيفي، تغير طبيعة الإجراء، مخاطر الخطأ.
المطلب الثالث: الحدود بين التحري والاستدلال والتحقيق	معايير التمييز (الغرض، الجهة، الإجراء، الآثار، الضمانات)، انتقال المعلومات.
الفصل الثاني: الأساس القانوني للمشروعية	السند، الاختصاص، الإذن، الضوابط الموضوعية والحقوقية، الرقابة والمسؤولية.
المبحث الأول: السند القانوني والاختصاص	الأساس التشريعي، اختصاص الجهات، حالات الإذن القضائي.
المطلب الأول: الأساس التشريعي	مستويات التنظيم (عام/خاص)، سيادة القانون، المعايير الدولية، اتفاقية بودابست.
المطلب الثاني: اختصاص الجهات وحدود سلطاتها	أدوار الاختصاص (المبادرة، الإذن، التنفيذ، التقييم)، الحدود الشخصية والموضوعية.
المطلب الثالث: حالات اشتراط الإذن	الإذن القضائي والتصريح الإداري، نطاق الإذن، الحالات العاجلة.
المبحث الثاني: الضوابط الموضوعية	المشروعية، الغرض، الضرورة، التناسب، القيود على البيانات، تقليل البيانات.
المطلب الأول: المشروعية وتحديد الغرض	جانبا المشروعية، تحديد الغرض، إعادة الاستخدام، مشاركة المعلومات.
المطلب الثاني: الضرورة والتناسب	تقييم الضرورة، التناسب، مستويات التدخل، مدة الإجراء.
المطلب الثالث: القيود على البيانات	البيانات العامة، المقيدة، المحمية، غير المستهدفين، أثر طريقة الحصول.
المطلب الرابع: تقليل البيانات والاحتفاظ	التقليل عند الجمع والتحليل، الاستخدام في أغراض أخرى، التبادل، الاحتفاظ، الإتلاف، تنظيم الوصول.
المبحث الثالث: الضوابط الحقوقية والإجرائية	الخصوصية، البيانات الشخصية والحساسة، غير المستهدفين، المشاركة والإتلاف.

العنوان	المحتوى / الوصف
المطلب الأول: حماية الخصوصية	الخصوصية السياقية، التمييز بين الخصوصية وحماية البيانات، الأثر التراكمي، الاجتهاد الأوروبي.
المطلب الثاني: معالجة البيانات الشخصية والحساسة	مشروعية المعالجة، الغرض، الدقة، السرية، البيانات الحساسة، حقوق الأفراد، المصادر المفتوحة، المسؤولية.
المطلب الثالث: حماية بيانات غير المستهدفين	التصنيف الثلاثي، تحديد النطاق، الفصل، تقييد الاستخدام، ضبط الصلاحيات، الاحتفاظ والإتلاف، التوثيق.
المطلب الرابع: مشاركة البيانات وإتلافها	الأساس القانوني للاحتفاظ، التمييز بين التشغيلي والإثباتي، تنظيم الوصول، المشاركة، التبادل عبر الحدود، الإتلاف، المساءلة.
المبحث الرابع: الرقابة والمسؤولية	القضائية، الإدارية، التظلم، المسؤولية.
المطلب الأول: الرقابة القضائية	صور الرقابة، الفصل بين الجهات، الخبرة الفنية، تقييم النتائج.
المطلب الثاني: الرقابة الإدارية	صلاحيات الوصول، المراجعة الداخلية، الاستقلال، التدريب، إدارة الحوادث، المؤشرات، التوثيق.
المطلب الثالث: التظلم والمراجعة	الحق في الشكوى، التظلم من القرارات، مراجعة المشروعية، حدود السرية، التصحيح، التدابير التصحيحية.
المطلب الرابع: المسؤولية	الجنائية، التأديبية، المدنية، المؤسسية، الأثر في المعلومات، التوسع في الإذن، الإهمال الفني، الاستخدام في غير الغرض.
الفصل الثالث: ضمانات التحريات والرقابة	الضمانات السابقة والمعاصرة، الرقابة، الآثار القانونية للمخالفة.
المبحث الأول: الضمانات السابقة والمعاصرة	تحديد النطاق، توثيق السند، قصر الوصول، حماية البيانات غير المرتبطة.
المطلب الأول: تحديد النطاق والأهداف	الغرض، النطاق الشخصي والموضوعي والزمني والتقني، حدود الاستخدام، تطور التحري.
المطلب الثاني: توثيق السند والإذن	التمييز بين السند والإذن والتنفيذ، عناصر السجل، ربط الإذن بطبيعة التدخل، الرقابة المستمرة.
المطلب الثالث: قصر الوصول على المخولين	الصلاحيات بحسب الوظيفة، الحد الأدنى من الامتيازات، التوثيق، الفصل بين المهام، حماية الحسابات.

العنوان	المحتوى / الوصف
المطلب الرابع: حماية البيانات غير المرتبطة	التمييز بين الظهور العرضي والتوسع العمدي، الضوابط، حماية المصادر والاتصالات المهنية.
المبحث الثاني: الرقابة والمسؤولية	القضائية، الإدارية، التظلم، المسؤولية.
المطلب الأول: الرقابة القضائية	التحقق من الشروط، الضرورة والتناسب، نطاق الإذن، معالجة البيانات، سبل الانتصاف.
المطلب الثاني: الرقابة الإدارية	تحديد المسؤوليات، السياسات المكتوبة، المراجعات الدورية، الضوابط التقنية، إدارة المخاطر، المراجعة المستقلة.
المطلب الثالث: التظلم والمراجعة	وضوح الاختصاص، الاستقلال، الوصول للسجلات، نطاق الشكوى، التدابير التصحيحية، التعويض.
المطلب الرابع: المسؤولية	الجنائية، التأديبية، المدنية، المؤسسية، الأثر في المعلومات، التناسب.
المبحث الثالث: الآثار القانونية للمخالفة	تجاوز الاختصاص أو الإذن، التمييز بين المخالفة والخلل الفني، أثر المخالفة في الاستناد.
المطلب الأول: تجاوز الاختصاص أو الإذن	الصور الأربع (غياب السند، جهة غير مختصة، تجاوز الإذن، استخدام لاحق)، تقييم الأثر.
المطلب الثاني: التمييز بين المخالفة والخلل الفني	الحالات الأربع، قيم التجزئة، سلسلة العهدة، الفصل بين المحورين.
المطلب الثالث: أثر المخالفة في الاستناد	الأسئلة الثلاثة، مشروعية الاستناد، الخلل الفني، ضعف الدلالة، الوزن، الفصل بين المسؤولية والأثر.
الباب الثاني: وسائل التحري وإجراءات الجمع	المصادر، الرصد، البيانات المقيدة.
الفصل الأول: مصادر المعلومات الرقمية	المصادر المفتوحة، السجلات، الأفراد، الأجهزة، OSINT، التوثيق.
المبحث الأول: مصادر المعلومات وتصنيفها	المفتوحة، السجلات، الأفراد، الأجهزة.
المطلب الأول: المصادر المفتوحة	التعريف، التمييز بين المصدر والمحتوى والسياق، الأثر التراكمي، بروتوكول بيركلي.
المطلب الثاني: السجلات وقواعد البيانات	التعريف، التصنيف، عناصر التقييم، الربط بين القواعد، NIST SP 800-86.

العنوان	المحتوى / الوصف
المطلب الثالث: المعلومات من الأفراد	التمييز بين الصدق والدقة، استقلال المصادر، مشروعية الحصول، التحايل على الضمانات، التوثيق.
المطلب الرابع: المعلومات من الأجهزة	الطبيعة الآلية، التمييز بين المحلي والسحابي، تحديد المصدر، إجراءات المحافظة، UNODC.
المبحث الثاني OSINT : والتحقق	المفهوم والحدود، الشبكات الاجتماعية، نسبة الحسابات، الصور والفيديو.
المطلب الأول: مفهوم OSINT وحدودها	التعريف، الفرق عن البحث العادي، بروتوكول بيركلي، الحد القانوني.
المطلب الثاني: الشبكات الاجتماعية	إعدادات الخصوصية، توثيق المنشورات، نسبة الحساب، بيانات التفاعل، المراقبة المستمرة، حماية الغير.
المطلب الثالث: نسبة الحسابات	التمييز الثلاثي، عدم كفاية التشابه، المؤشرات المتضاربة، توثيق المؤشرات، التناسب.
المطلب الرابع: التحقق من الصور والفيديو	تحديد الادعاء، البحث عن الأصل، البيانات الوصفية، السياق، التوليد الاصطناعي، حدود الأدوات.
المبحث الثالث: توثيق جمع المعلومات	المصدر والتاريخ، الطريقة والسند، الأصل والنسخ، القيود.
المطلب الأول: تحديد المصدر والتاريخ	التمييز بين المصادر، بيانات المصدر، التواريخ المختلفة، المناطق الزمنية، التوثيق.
المطلب الثاني: توثيق الطريقة والسند	عناصر التوثيق، الظروف المتغيرة، السند القانوني، الانحراف عن الإجراء.
المطلب الثالث: المحافظة على الأصل والنسخ	تعريف الأصل، النسخة المعالجة، متطلبات الحفظ، توثيق المعالجة، القيود القانونية.
المطلب الرابع: تسجيل القيود	أنواع القيود، التمييز بين النقص وعدم الصحة، صياغة القيود، انعكاسها في الاستنتاج.
الفصل الثاني: وسائل الرصد والبيانات المقيدة	الرصد الثابت والمتحرك، بيانات الاتصالات، الأجهزة، السحابة.
المبحث الأول: الإطار المفاهيمي للرصد	المفهوم، التصنيف، الضوابط المشتركة.
المطلب الأول: مفهوم الرصد وخصائصه	التعريف، الخصائص (الجمع المستمر، الربط، المعالجة الآلية، تفاوت التدخل، فصل الجمع عن التفسير).

العنوان	المحتوى / الوصف
المطلب الثاني: تصنيف وسائل الرصد	بحسب طبيعة البيانات، طريقة الحصول، نطاق الأشخاص، درجة التدخل، الغرض.
المطلب الثالث: الضوابط المشتركة	الشرعية، الاختصاص، الغرض، الضرورة والتناسب، النطاق، حماية الغير، أمن المعلومات، تقييد الاستخدام، الرقابة.
المبحث الثاني: الرصد الثابت والمتحرك	كاميرات، سجلات، تتبع الحركة، الجمع والحفظ، ضوابط التصوير.
المطلب الأول: الرصد الثابت	الطبيعة القانونية، مشروعية التركيب، جمع التسجيلات، حدود الدلالة، التعرف الآلي.
المطلب الثاني: الرصد المتحرك	الصور، أثر تتبع الموقع، الخلط بين الجهاز والشخص، ضوابط المراقبة المستمرة، الجمع بين المصادر.
المطلب الثالث: جمع التسجيلات وحفظها	التحقق من المصدر، توثيق الاستخراج، حفظ الأصل، سلسلة العهدة، التحقق من السلامة، الحماية، معالجة النقص.
المطلب الرابع: ضوابط التصوير والخصوصية	الخصوصية السياقية، الأماكن العامة والخاصة، الملفات السلوكية، حماية الغير، التسجيل الصوتي، مدة الاحتفاظ، الاستخدام اللاحق، الرقابة.
المبحث الثالث: بيانات الاتصالات والأجهزة	الأنواع، الشروط، الوصول إلى الأجهزة، السحابة والتشفير.
المطلب الأول: أنواع البيانات	المحتوى، المشترك، الحركة، الموقع، البيانات الفنية، الأثر القانوني للتمييز.
المطلب الثاني: شروط الحصول والاحتفاظ	الأساس القانوني، الجهة المختصة، الإذن، نطاق الطلب، التمييز بين الحفظ والوصول، الحماية، المدة، الطلب من خارج الدولة.
المطلب الثالث: الوصول إلى الأجهزة	التمييز بين الضبط والوصول، نطاق الإذن، المحمولة والحواسيب، الحسابات المتصلة، السحابة، التشفير، حماية البيانات غير المرتبطة، التوثيق.
المطلب الرابع: السحابة والتشفير	الطبيعة، التمييز بين المحلي والبعيد، التشفير، القيود الفنية، مقدمي الخدمات، الاختصاص، المحافظة العاجلة، التعاون الدولي.
الفصل الثالث: المراقبة والرصد الجوي بالطائرات المسيّرة	المفهوم، الوظائف، المشروعية، القيمة الإثباتية، التطبيقات، العوامل الميدانية، التهديدات، التحديات الضمانات
الباب الثالث: سلامة المعلومات وقيمتها القانونية	الأصالة، سلسلة العهدة، التوثيق، القيمة القانونية، التحليل، التقييم.

العنوان	المحتوى / الوصف
الفصل الأول: الأصالة والسلامة والتوثيق	المصدر، التاريخ، الأصل والنسخ، قيم التجزئة، سلسلة العهدة، الأدوات، التقارير.
المبحث الأول: التحقق من الأصالة والسلامة	المصدر والهوية، التاريخ والاكتمال، الأصل والنسخ، قيم التجزئة.
المطلب الأول: تحديد المصدر والهوية	التمييز بين المصادر، العناصر، هوية الجهاز والمستخدم، مستويات الاستدلال، ISO/IEC 27037
المطلب الثاني: التحقق من التاريخ والاكتمال	التواريخ المختلفة، المناطق الزمنية، اكتمال البيانات، التعديل، NIST.
المطلب الثالث: المحافظة على الأصل والنسخ	تعريف الأصل، الفئات الثلاث، النسخة الجنائية، NIST SP 800-101، القيود القانونية، تقليل البيانات.
المطلب الرابع: قيم التجزئة	التعريف، الحدود، التمييز بين السلامة والأصالة والصحة، الخوارزميات، التفسير، التوثيق، الوظيفة القانونية.
المبحث الثاني: سلسلة العهدة وضمان الجودة	المفهوم، التوثيق، الأدوات، النقص وإعادة الفحص.
المطلب الأول: المفهوم والأهمية	التعريف، التمييز بين الحياة والسيطرة، الوظائف، ISO/IEC 27037، الأثر القانوني.
المطلب الثاني: توثيق الاستلام والنقل والحفظ	عناصر التوثيق، البيانات الإلكترونية، النقل، الحفظ، الوصول، النسخ الفنية، السرية، الفجوات.
المطلب الثالث: توثيق الأدوات والخطوات	تعريف الأدوات، الإصدارات، الخطوات، التدخل البشري، الخوارزميات، الملاءمة، التوثيق، الفصل بين الفني والقانوني.
المطلب الرابع: معالجة النقص وإعادة الفحص	أنواع النقص، الخطوات، الأثر الفني والقانوني، إعادة الفحص، عناصر القابلية، المراجعة المستقلة.
المبحث الثالث: توثيق الإجراءات والتقارير	تسجيل الإجراءات، التمييز بين الوثائق، عرض النتائج، القيود والتصحيح.
المطلب الأول: تسجيل الإجراءات	العناصر، النتائج السلبية، الفصل بين الوصف والتفسير، القرارات المهنية، التعديلات، عدم منح المشروعية.
المطلب الثاني: التمييز بين المحضر والتقارير الأمني والفني	الوظائف، المحتوى، مصدر المعرفة، حدود الاستنتاج، التوثيق، جدول الفروق.

العنوان	المحتوى / الوصف
المطلب الثالث: عرض النتائج وإسنادها	الوقائع والاستنتاجات، الإحالات، استغلال المصادر، المعلومات المعارضة، حدود الفحص، الفصل بين الفني والقانوني.
المطلب الرابع: القيود وتصحيح الأخطاء	أنواع القيود، عدم اليقين، الفرضيات البديلة، تصحيح الأخطاء، الأنظمة الآلية، الفصل بين الفني والقانوني.
الفصل الثاني: القيمة القانونية والاستدلالية	المشروعية، الموثوقية، حدود الاستناد.
المبحث الأول: مشروعية الحصول وأثرها	أثر المشروعية، تجاوز الاختصاص، التمييز بين المخالفة والخلل.
المطلب الأول: أثر المشروعية في الاستناد	المستويات الثلاثة، عناصر المشروعية، تباين الآثار، الفصل بين السلوك والمعلومات، الفحص المزدوج.
المطلب الثاني: تجاوز الاختصاص أو الإذن	الأنماط الثلاثة، اتفاقية بودابست، توسيع الإذن، انتقال البيانات، سلامة الاختصاص.
المطلب الثالث: التمييز بين المخالفة والخلل الفني	الحالات الأربع، قيم التجزئة، سلسلة العهدة، NIST، الأسئلة المزدوجة، تجنب النتيجة.
المبحث الثاني: الموثوقية والقيمة القانونية	شروط الاستناد، الأصالة والسلامة، الخبرة الفنية، القبول والوزن.
المطلب الأول: شروط الاستناد	الصلة، المشروعية، الأصالة، السلامة، الموثوقية، كفاية المنهج، القبول، UNODC.
المطلب الثاني: الأصالة والسلامة والتوثيق	الوظائف المستقلة، NIST، القيمة القانونية للتوثيق، الأصل والنسخ، سلسلة العهدة، UNODC.
المطلب الثالث: الخبرة الفنية	الكفاءة، نطاق المهمة، قابلية المراجعة، الاستقلال، NIST، درجة الثقة، الفصل بين الفني والقانوني.
المطلب الرابع: القبول والوزن	التمييز، الاعتبارات الثمانية، تعدد المصادر، UNODC، الفصل بين المرحلتين.
المبحث الثالث: حدود الاستناد إلى النتائج	المعلومة والقرينة والدليل، الاستنتاج غير المباشر، البدائل، الإفصاح.
المطلب الأول: المعلومة والقرينة والدليل	التعريفات، الوظائف، جدول التمييز، الانتقال بين المفاهيم، UNODC.
المطلب الثاني: الاستنتاج غير المباشر	الخطر المنهجي، الطبقات الأربع، البيانات المتعددة، تراكم المؤشرات، NIST، الارتباط والسببية.

العنوان	المحتوى / الوصف
المطلب الثالث: التفسيرات البديلة والقيود	التحيز التأكيدي، الاختبار المنهجي، البديل المعقول، القيود الفنية، NIST، الشك القابل للتقليل.
المطلب الرابع: الإفصاح عن المصادر والتحقق	مستويات الإفصاح، العناصر الثمانية، استقلال المصادر، إعادة التداول، أثر القيود في الوزن، UNODC.
الفصل الثالث: تحليل المعلومات والتحقق	المنهجية، تقييم المصادر، اختبار الفرضيات.
المبحث الأول: منهجية التحليل	تنظيم البيانات، الربط، الملاحظة والواقعة والاستنتاج، الفرضيات.
المطلب الأول: تنظيم البيانات وتصنيفها	المستويات الخمسة، عدم الحيادية، NIST، سجل المعلومات، المخاطر.
المطلب الثاني: الربط بين المصادر	الأنماط الثلاثة، استقلال المصادر، خريطة العلاقات، المعلومات المعارضة، بيركلي.
المطلب الثالث: الملاحظة والواقعة والاستنتاج	التعريفات، عدم التطابق، الجدول، الأدوات الآلية، صياغة التقرير.
المطلب الرابع: تحديد الفرضيات	التعريف، الافتراضات، التحيز التأكيدي، الخطوات السبع، قابلية الدحض، الفرضيات المتعلقة بالأشخاص.
المبحث الثاني: تقييم المصادر والبيانات الوصفية	المصدر والتاريخ، التحقق المستقل، الوقت والموقع، حدود البيانات الوصفية.
المطلب الأول: تقييم المصدر والتاريخ	المعايير الخمسة، كلية الشرطة البريطانية، التواريخ المختلفة، مصلحة المصدر، درجتا الثقة.
المطلب الثاني: التحقق المستقل	التعريف، استقلال المصادر، الصور الخمس، الفصل بين الأصالة والسلامة والصحة، بيركلي.
المطلب الثالث: تحليل الوقت والموقع والسجلات	البيانات الوصفية، الوقت، الموقع، السجلات، NIST، الفروق بين الدقة والتفسير.
المطلب الرابع: حدود البيانات الوصفية	خمسة حدود، التمييز بين الدقة والاكتمال والأصالة والدلالة، NIST، المبالغة في الوصف.
المبحث الثالث: اختبار الفرضيات وضبط الاستدلال	الفرضية والنتيجة، البدائل والانتقاء، التعارض والنقص، التلاعب، الإفصاح.
المطلب الأول: الفرضية والنتيجة	المستويات الثلاثة، عدم الخلط، درجة الثقة، عدم كفاية البيانات، جودة النتيجة.

العنوان	المحتوى / الوصف
المطلب الثاني: البدائل والانتقاء التأكيدى	التعريف، الصور، المعالجة، التفسيرات البديلة، الإجراءات السبعة، المراجعة المستقلة، غياب الدليل.
المطلب الثالث: التعارض والنقص	التعارض الظاهري والحقيقي، الخطوات السبع، التمييز بين النقص والتعارض، عدم ملء الفجوات، كلية الشرطة البريطانية.
المطلب الرابع: التلاعب والتزوير	التعريف، الصور، المنهج الخمسي، التوليد الاصطناعي، حدود الأدوات، أثر التعديل الجزئي، الفصل بين الفحص والقصد.
المطلب الخامس: الإفصاح عن الشك	التعريف، التمييز عن الخطأ، الأنواع، العناصر الثمانية، التمييز بين الثقة التحليلية والإثبات، النسب المئوية.
الفصل الرابع: التقييم التطبيقي	منهج التقييم، التطبيق، النتائج.
المبحث الأول: منهج التقييم ومعايره	المعايير، اختيار الحالات، الأدوات والحدود.
المطلب الأول: معايير المشروعية والموثوقية والتوثيق	المعايير الستة، العهد الدولي، NIST، الحياد المنهجي، قابلية المراجعة.
المطلب الثاني: اختيار الحالات	الأنواع، الضوابط الخمسة، تجنب الانتقاء، التمييز بين الأهمية القانونية والفنية.
المطلب الثالث: أدوات التقييم والحدود	التحليل القانوني والفني والمقارن، مصفوفة التقييم، النتائج المثبتة والاحتمالية، حدود التقييم.
المبحث الثاني: تطبيق المعايير	عرض الحالة، الأساس القانوني، الأصالة والسلامة، اختبار الاستنتاجات، تقييم النتائج.
المطلب الأول: عرض الحالة	الحالة الافتراضية، المصادر الثلاثة، سجل المصادر، حماية البيانات، الأوصاف المحايدة.
المطلب الثاني: تقييم الأساس القانوني	الإجراءات الثلاثة، الإفصاح، الضرورة والتناسب، التوثيق، الصياغة المنضبطة، الفصل بين المشروعية والموثوقية.
المطلب الثالث: فحص الأصالة والسلامة	المصدر، البيانات الوصفية، السلامة، قيم التجزئة، فحص التسجيل والصورة والسجل، إعادة الفحص.
المطلب الرابع: اختبار الاستنتاجات	تفكيك الاستنتاج، البدائل، غياب الدليل، الوقت والموقع، الاعتماد المتبادل، الخطوات السبع، التحيز، الارتباط والسببية.
المطلب الخامس: تقييم النتائج	التقييم القانوني والفني، تصنيف النتائج الأربعة، قابلية المراجعة، العلاقة بين القصور والتوصيات.

العنوان	المحتوى / الوصف
المبحث الثالث: النتائج وأوجه القصور	الاتساق، القصور، صلاحية النتائج، حدود التعميم.
المطلب الأول: الاتساق بين المتطلبات	الأوجه الخمسة، عدم الحتمية، الاستقلال المتبادل، توزيع المسؤوليات.
المطلب الثاني: أوجه القصور	الأنماط الثمانية، الأنماط المحتملة، بساطة الأسباب، تحسين المنظومة.
المطلب الثالث: صلاحية النتائج	المرحلة الأمنية، الغرض، المشروعية المستقلة، قوة النتيجة، تعزيز الصلاحية، القبول والوزن.
المطلب الرابع: حدود التعميم	الحالة الافتراضية، الحكم القضائي، التقرير الرسمي، طبيعة التقنية، المستويات الثلاثة، التعميم الوصفي والقانوني، الدراسة المقارنة.
الباب الرابع: التحديات ومقترحات التطوير	التحديات القانونية، التقنية، المقترحات.
الفصل الأول: التحديات القانونية والحقوقية	القصور التشريعي، التداخل، التوازن، العابر للحدود.
المبحث الأول: القصور والغموض التشريعي	القصور، التداخل، التوازن، العابر للحدود.
المطلب الأول: القصور التشريعي	العمومية والتشدد، القدرة التقنية والاختصاص، المرونة والغموض، اتفاقية بودابست، معالجة القصور.
المطلب الثاني: التداخل الاختصاصي	الوظائف الأربع، تغير طبيعة الواقعة، استقلال الخبير، مبادئ الأمم المتحدة، توزيع المسؤوليات، تبادل البيانات.
المطلب الثالث: التوازن مع الحقوق	الخطورة، الحماية كشرط، التناسب، المراقبة المستمرة، مفوضية الأمم المتحدة، الحقوق المرتبطة، التقييم المسبق.
المطلب الرابع: البيانات العابرة للحدود	تعقيد التخزين، القدرة والسلطة، طلب البيانات، بودابست والبروتوكول الثاني، تعارض المتطلبات، التمييز بين التحقيق والوقاية، قناة التعاون.
الفصل الثاني: التحديات التقنية والمؤسسية	التلاعب والكشف، التحيز، الكفاءات، التنسيق.
المبحث الأول: التلاعب والكشف الآلي	الأسئلة الثلاثة، حدود الأدوات، NIST، الإيجابيات والسلبيات الكاذبة، منهج التحقق، البحث عن النافي.

العنوان	المحتوى / الوصف
المبحث الثاني: التحيز والأخطاء	التحيز التأكدي، تحيز البيانات، ملاءمة الأداة، ISO/IEC 23894، الحد من التحيز، تكرار النتيجة، آليات الأخطاء.
المبحث الثالث: الكفاءات والموارد	الكفاءات الأربعة، التدريب المستمر، الموارد، الاستثمار التقني، الإدارة الرشيدة.
المبحث الرابع: التنسيق والتوثيق	توحيد التوثيق، التمييز بين الإجراءات والتقدير، إعادة بناء المسار، ISO/IEC 17025، الفصل بين المراجعتين، إدارة الأخطاء.
الفصل الثالث: مقترحات التطوير والحوكمة	تنظيم الاختصاص، ضمانات الخصوصية، تطوير الإجراءات، التدريب والتعاون، الذكاء الاصطناعي.
المبحث الأول: تنظيم الاختصاصات والوسائل	فئات الإجراءات، الجهات المختصة، الإطار التشريعي واللوائح، تقييم الوسائل الجديدة، ملاءمة السياق.
المبحث الثاني: ضمانات الخصوصية والرقابة	دورة حياة البيانات، تحديد الغرض، سجل الإجراءات، تناسب الرقابة، المساءلة، الإلتلاف، المشاركة.
المبحث الثالث: تطوير الإجراءات	التخطيط، الجمع، التحليل، التوثيق، المراجعة، التصحيح، النماذج الموحدة.
المبحث الرابع: التدريب والتعاون	المحاور الأربعة، الحالات التطبيقية، التنسيق المؤسسي، التعاون الدولي، التعاون الأكاديمي.
المبحث الخامس: الذكاء الاصطناعي والإشراف	الأغراض والمخاطر، OECD، الإشراف البشري، المراجعة المستقلة، التفسير والتحقق، الأخطاء، التناسب.
الخاتمة	النتائج العامة، التوصيات التشريعية والمؤسسية، آفاق البحث.
الملاحق	1. جدول مقارنة بين التحري والاستدلال والتحقيق. 2. جدول تصنيف البيانات ومستويات التحقق. 3. مصفوفة التقييم. 4. جدول مقارنة بين المحضر والتقرير الأمني والفني. 5. قائمة تحقق. 6. نماذج اجتهادات قضائية.
المراجع	المراجع العربية، المراجع الأجنبية (NIST)، ISO، OECD، بودابست، بيركلي، الإنترنت، (UNODC)، التشريعات والاتفاقيات.

