Security Policy Papers
أوراق السياسات الأمنية
https://spp.nauss.edu.sa/index.php/spp
ورقة تحليل سياسات أمنية

مختبرات الأدلة الجنائية الرقمية: تحديات الواقع التشغيلي وبدائل التنظيم

Digital Forensic Laboratories: Operational Challenges and Organizational Alternatives

المخرجات الرئيسة

- يشهد حجم الأدلَّة الرقميَّة وتعقيدها تزايُدًا ملحوظًا، بما يفوق في بعض الحالات القدرة الاستيعابيَّة الحاليَّة للمختبرات الحكوميَّة، الأمر الذي قد يؤدِّي إلى تراكُم القضايا وتأخُّر إصدار التقارير الفنيَّة، وينعكس على سرعة الفصل القضائي.
- تتوافر ثلاثة نماذج رئيسة للتعامل مع مختبرات الأدلَّة الرقميَّة، تتمثل في: الاستمرار بالنموذج الحكومي الكامل، أو التعاون مع القطاع الخاص، أو اعتماد نموذج هجين يقوم على الإشراف الحكومي مع تشغيل أو استثمار خاص، بما يحقق كفاءة تشغيليَّة أعلى، مع الحفاظ على سريَّة الأدلَّة الرقميَّة وضمان العدالة الإجرائيَّة.
- تُظهِر التجارِب الدوليَّة أن إشراك القطاع الخاص في أعمال مختبرات الأدلَّة الرقميَّة يمكن أن يكون خيارًا عمليًّا وفعَّالًا، شريطة خضوعه لاعتماد فني إلزامي، ورقابة قضائيَّة، وإطار واضح للمساءلة وضبط الجودة.

- قد يسهم التعاون غير المنضبط مع القطاع الخاص في تحسين الكفاءة التشغيليَّة، إلا أنه قد يترتَّب عليه تحديات تنظيميَّة واحتمالات تضارُب مصالح، بما قد يؤثِّر في موثوقيَّة التقارير الفنيَّة وقبولها قضائيًّا، ما لم يُنظَّم بضوابط تشغيليَّة واضحة

المستخلص

أصبحت الأدلَّة الجنائيَّة الرقميَّة ركيزة أساسيَّة في منظومة العدالة الحديثة، ولم يَعُد حضورها مقصورًا

Abstract

Digital forensics has become a fundamental pillar of modern justice systems. Its role is no longer confined to cybercrime investigations;

على الجرائم السيبرانيَّة، بل امتد ليشمل معظم القضايا الجنائيَّة، مع تحوُّل الهواتف الذكيَّة والحسابات السحابيَّة ومنصات التواصُل الاجتماعي والمعاملات الإلكترونيَّة إلى مصادر رئيسة للإثبات أمام القضاء. وقد تَعزَّز هذا التوجُّه مع اتساع الاقتصاد الرقمي وارتفاع معدلات استخدام الإنترنت ووسائل التواصُل الاجتماعي في العالم العربي، مِمَّا أفرز تضخُّمًا متزايدًا في حجم البيانات الرقميَّة وتعقيدًا في مصادرها.

وفي مقابل هذا التوسُّع الكمي والنوعي، برزت تحديات تتعلق بمواكبة التطوير المتوازن في الموارد البشريَّة والبنية التقنيَّة والزمن الإجرائي داخل المختبرات الرقمية، الأمر الذي قد يسهم في تراكم القضايا وتأخُّر التقارير الفنيَّة، بما ينعكس على سرعة الفصل القضائي واستقرار الأحكام. كما تبرز هذه التحديات بصورة أوضح في ظل تنامي استخدام أدوات الذكاء الاصطناعي في إنتاج البيانات وتعديلها، وما يرتبط بذلك من قضايا تتعلق بأصالة المحتوى والأدلة الرقمية.

وانطلاقًا من ذلك، تبحث هذه الورقة خيار التعاون مع القطاع الخاص في إدارة مختبرات الأدلَّة الرقميَّة بوصفه توجُّهًا عمليًّا لتحسين الكفاءة وتسريع العدالة.

وقد استندت هذه الورقة إلى تحليل مقارن لأربع تجارِب تنظيميَّة في إشراك القطاع الخاص في إدارة مختبرات الأدلَّة الرقميَّة وتشغيلها، هي: المملكة المتحدة، والولايات المتحدة الأمريكيَّة، وأستراليا، وسنغافورة، بوصفها نماذج تنظيميَّة متنوعة عبر أربع قارات مختلفة، وأنظمة قانونيَّة متباينة ذات تأثير دولي واضح.

وتخلص هذه الورقة إلى ثلاثة بدائل، يتمثَّل أبرزها في النموذج الهجين القائم على الإشراف الحكومي مع الاستفادة التشغيليَّة، باعتباره الخيار الأكثر توازنًا من حيث الكفاءة والحجيَّة القضائيَّة.

rather, it now extends to most criminal cases, as smartphones, cloud accounts, social media platforms, and electronic transactions have evolved into primary sources of judicial evidence. This trend has been reinforced by the expansion of the digital economy and the increasing rates of internet and social media usage across the Arab world, resulting in a growing volume of digital data and increasing complexity in its sources.

In parallel with this quantitative and qualitative expansion, several challenges have emerged concerning the ability of digital forensic laboratories to achieve balanced development in human resources, technical infrastructure, and procedural timelines. These challenges may contribute to case backlogs and delays in issuing technical reports, thereby affecting the speed of judicial proceedings and the consistency of judicial rulings. Such challenges have become even more pronounced with the growing use of artificial intelligence tools in generating and modifying data, and the associated concerns regarding the authenticity of digital content and digital evidence.

Against this backdrop, the paper explores the option of engaging the private sector in the management of digital forensic laboratories as a practical approach to enhancing efficiency and accelerating the administration of justice.

The paper is based on a comparative analysis of four organizational experiences involving private-sector participation in the management and operation of digital forensic laboratories: the United Kingdom, the United States of America, Australia, and Singapore. These cases represent diverse organizational models across four different continents and varying legal systems with clear international influence.

The paper concludes by proposing three alternatives, the most prominent of which is the hybrid model based on governmental oversight combined with private-sector operational utilization, as it represents the most balanced option in terms of efficiency and judicial admissibility.

المقدمة

تتجسَّد المعضلة الأمنيَّة الأساسيَّة في الفجوة التشغيليَّة المتنامية بين الطلب القضائي المتزايد على خدمات الأدلَّة الجنائيَّة الرقميَّة، والقدرة الفعليَّة للمختبرات التابعة لأجهزة الشرطة على الاستجابة لهذا الطلب بالكفاءة والسرعة والدقة المطلوبة. هذه الفجوة لم تَعُد مرتبطة بزيادة عدد القضايا فحسب، بل بتغيُّر نوعي في طبيعة البيئة الرقميَّة ذاتها. ففي عام 2024، بلغ عدد الأجهزة المتصلة بالإنترنت عالميًّا نحو 18.5 مليار جهاز، وَفْقَ تقديرات IoT Analytics، مع توقُّعات بارتفاع هذا العدد إلى قرابة 39 مليار جهاز بحلول عام 2030، والانتشار الواسع لتطبيقات الذكاء الاصطناعي، والطلب المتزايد على البيانات المتولِّدة من هذه الأجهزة.

التعقيد في استخراج الأدلَّة

إن أي واقعة جنائيَّة محتملة قد ترتبط بسلسلة أجهزة مترابطة، لا بجهاز واحد يمكن عزله وتحليله تحليلًا مستقلًّا. فالفرد اليوم لا يُنتج أثرًا رقميًّا من هاتفه فقط، بل من شبكة متكاملة تشمل: أجهزة إنترنت الأشياء، والساعات الذكيَّة، وأنظمة المركبات المتصلة، وأجهزة المنزل الذكي، والبنية التحتيَّة للمدن الذكيَّة. وبهذا تحوَّل مسرح الجريمة الرقمي من وحدة تخزين محدودة إلى منظومة بيانات مُتعدِّدة الطبقات، تتطلَّب تحليلًا تكامليًّا عابرًا للأجهزة والمنصات.

ويظهر ضغط هذه الفجوة بوضوح عند النظر إلى التحوُّل من الحاسوب الشخصي إلى الهاتف الذكي، ثم إلى المركبات المتصلة ذات الأنظمة شبه الذاتيَّة، فالمركبة الحديثة تحتوي على أكثر من 100 وحدة تحكُّم إلكترونيَّة (ECUs) تولِّد بيانات تشغيليَّة وسلوكيَّة باستمرار. يعني ذلك أنَّ حادثًا مروريًّا أو واقعة جنائيَّة قد تستدعي استخراج بيانات من أنظمة مُتعدِّدة داخل المركبة نفسها، تشمل بيانات السرعة، وأنماط الكبح، والموقع الجغرافي، وسجلات الاتصال الشبكي.

كما أن أنظمة المدن الذكيَّة، من كاميرات المرور إلى حساسات البنية التحتيَّة، تُنتج تدفُّقات بيانات مستمرة قد تكون جزءًا من السياق لأي قضية. هذا الاتساع في مصادر الأدلَّة يفرض قدرات تحليليَّة تتجاوز منهج الفحص التقليدي القائم على جهاز واحد.

التعقيد مع انتشار أدوات الذكاء الاصطناعي

لم يعُد المحتوى الرقمي دليلًا مباشرًا على فعل بشري، بل قد يكون ناتجًا عن أنظمة توليديَّة متقدمة. وتشير البيانات الرسميَّة في دولة الإمارات العربيَّة المتحدة إلى أن نسبة استخدام أدوات الذكاء الاصطناعي قد بلغت نحو 97% في عام 2025، وهي من أعلى النسب عالميًّا، ما يعكس الانتشار المتسارع للتقنيات التوليديَّة في مختلف الأنشطة الرقميَّة. وبذلك لم يعُد دور المختبر يقتصر على استخراج البيانات، بل أصبح يشمل التحقُّق من أصالتها وتحليل خصائصها التقنيَّة ومصدر إنشائها، في ظل احتماليَّة معالجة البيانات أو إعادة بنائها آليًّا قبل حفظها. كما يزداد هذا التحدي تعقيدًا بسبب طبيعة العديد من نماذج الذكاء الاصطناعي التي تعمل وَفْقَ ما يُعرف بنموذج «الصندوق الأسود»، حيث يصعب تفسير آليَّة اتخاذ القرار أو تتبُّع كيفيَّة توليد المحتوى الرقمي بدقَّة.

ارتفاع تكلفة التأهيل المستمر للخبراء والأجهزة

إنَّ الأدوات الجنائيَّة الرقميَّة تتطلَّب تحديثات

دوريَّة، وترخيصًا مرتفع الكلفة لمواكبة الإصدارات الجديدة من أنظمة التشغيل والأجهزة. كما أن الخبير الرقمي لم يعُد يكتفي بفهم تقنيَّات النسخ، بل أصبح مُطالَبًا بفهم بيئات سحابيَّة، وتحليل سجلات شبكيَّة، والتعامل مع بيانات إنترنت الأشياء، وتقييم المحتوى الناتج عن أنظمة ذكاء اصطناعي. وهذا التوسُّع في متطلَّبات المهارة يطيل فترة التأهيل، ويرفع كلفة الاستثمار في الكادر البشري، ويجعل الاعتماد على زيادة عدد الموظفين فقط غير كافٍ لسد الفجوة.

إن مجموع هذه التحوُّلات -المتمثِّلة في: تضاعُف الأجهزة المتصلة، وتعدُّد مصادر الأدلَّة، وتضخُّم حجم البيانات، واتساع نطاق الإثبات الرقمي في القضايا التجاريَّة والمدنيَّة، وتأثير الذكاء الاصطناعي في طبيعة المحتوى- يُوجِد ضغطًا هيكليًّا على منظومة الأدلَّة الجنائيَّة الرقميَّة يتجاوز حدود الحلول الإداريَّة التقليديَّة. فالمشكلة لم تَعُد في عدد القضايا فقط، بل في تعقيد البيئة التقنيَّة التي تُنتج الأدلَّة ذاتها.

المقارنة المعياريَّة الدوليَّة

استندت هذه الورقة إلى تحليل أربع تجارِب تنظيميَّة مختلفة في مجال التعاون مع القطاع الخاص، وإشراكه في إدارة المختبرات الرقميَّة وتشغيلها، وهي: المملكة المتحدة، والولايات المتحدة الأمريكيَّة، وأستراليا، وسنغافورة. بناءً على منهجيَّة تهدف إلى تمثيل نماذج تنظيميَّة متنوِّعة في تنظيم مختبرات الأدلَّة الجنائيَّة الرقميَّة الخاصَّة، إذ تُغطِّي هذه العيِّنة أربع قارات مختلفة، وتمثِّل أنظمة قانونيَّة متباينة ذات تأثير دولي واضح. كما تُعد هذه الدول من البيئات المتقدِّمة تقنيًّا، وتواجه كثافة عالية في القضايا السيبرانيَّة والجرائم المعقَّدة، الأمر الذي أسهم في تطوير أطر تنظيميَّة ناضجة ومختبرة عمليًّا. ويتيح ذلك إجراء مقارنة معياريَّة متوازنة، واستخلاص دروس تنظيميَّة قابلة للتكييف مع السياق العربي.

بتحليل التجارِب الأربع الواردة، يتضح أن تنظيم المختبرات الجنائيَّة في القطاع الخاص لا يُدار وَفْقَ فلسفة مُوحَّدة، بل وَفْقَ توازن مختلف بين التشريع والرقابة المؤسَّسيَّة وسلطة المحكمة في قبول الدليل. فالمملكة المتحدة والولايات المتحدة وأستراليا وسنغافورة، جميعها تسمح من حيث المبدأ بإنتاج تقارير فنيَّة من مختبرات خاصَّة، غير أن قوة هذه التقارير ومدى اندماجها في منظومة العدالة يختلفان تبعًا للإطار القانوني وآليَّة الضبط المعتمَدة.

في المملكة المتحدة، يُشكِّل Forensic Science Regulator Act 2021 نقطة ارتكاز تنظيميَّة واضحة، إذ لم يقتصر على الاعتراف بدور المختبرات الجنائيَّة في القطاع الخاص، بل أخضعها لمدوَّنة ممارسة قانونيَّة مُلزِمة تُطبَّق على جميع أنشطة العلوم الجنائيَّة المستخدَمة في التحقيقات. وبهذا، فإن التقرير الصادر عن مختبر خاص لا يُقاس فقط بكفاءة الخبير أو قوة النتيجة الفنيَّة، بل بمدى التزام المختبر بإجراءات جودة موثقة تشمل ضبط سلسلة الحيازة، وآليات مراجعة العمل، وإدارة النسخ الجنائيَّة، وتتبُّع كل خطوة تحليليَّة منذ تسلُّم الدليل حتى إصدار التقرير. كما تتضمَّن هذه المدوَّنة متطلَّبات واضحة تتعلَّق بإدارة البيانات داخل المختبر، من حيث حفظ النسخ الأصليَّة، ومنع الوصول غير المصرَّح به، وتوثيق أي عمليَّة استخراج أو تحليل أو نقل بيانات. ويُعزِّز هذا الإطار بما ورد في دليلACPO/NPCC للممارسات المثلى في الأدلَّة الرقميَّة، الذي يؤكد مبدأ عدم تغيير الدليل الرقمي

جدول 1

المقارنة المعياريَّة الدوليَّة لتنظيم مختبرات الأدلَّة الجنائيَّة الرقميَّة الخاصَّة

محور المقارنة	المملكة المتحدة (UK)	الولايات المتحدة (US)	أستراليا (Australia)	سنغافورة (Singapore)
الإطار القانوني	Forensic Science Regulator Act 2021 يفرض إصدار مدوَّنة ممارسة قانونيَّة لتنظيم أنشطة العلوم الجنائيَّة المستخدَمة في التحقيقات، بغضِّ النظر عن كون المنفِّذ حكوميًّا أو خاصًّا.	لا يوجد منظِّم وطني اتحادي واحد يمنح ترخيصًا لمزودي الأدلَّة الجنائيَّة الرقميَّة من القطاع الخاص، ويُعد الضابط الأساسي على المستوى الاتحادي هو Federal Rules of Evidence، ولا سيَّما Rule 702 التي تنظِّم قبول شهادة الخبير أمام المحكمة. وعلى مستوى الولايات، توجد أطر تنظيميَّة أوضح، فمثلًا: يُنظِّم قانون تكساس (Texas CCP Art. 38.35) التحليل الجنائي للأدلَّة المستخدَمة في الإجراءات الجنائيَّة، ويُقر صراحةً بأن «مختبر الجريمة» قد يكون جهة حكوميَّة أو خاصَّة.	• لا يوجد قانون DF اتحادي. • الإطار العملي هو: قانون الأدلَّة (قبول الرأي الخبير) + ضوابط المحكمة لسلوك الخبير + منظومة اعتماد قويَّة (NATA/ISO17025) عند العمل كمختبرات/اختبارات قانونيَّة.	• الإطار الإجرائي أصبح أكثر صرامة مع Rules of Court 2021. • ساري من 1 أبريل 2022. • لا يجوز استخدام خبرة خبير إلا بموافقة المحكمة (O12 r2)، كأساس موضوعي لقبول «رأي الخبراء».
متطلبات الاعتماد والترخيص	تفرض المدوَّنة القانونيَّة التزام الجهات المنفِّذة لأنشطة العلوم الجنائيَّة بتطبيق نظام جودة مُعتمَد، وتُعد المرجع الإلزامي الذي تُقيَّم على أساسه جودة الممارسة، وقد يترتَّب على الالتزام بها متطلبات اعتماد أو تقييم جودة بحسب طبيعة النشاط.	لا يوجد ترخيص اتحادي موحَّد لجميع أنشطة الأدلَّة الجنائيَّة الرقميَّة، إلا أن اعتماد ISO/IEC 17025 عبر جهات مثل: ANAB (هيئة الاعتماد الوطنيَّة الأمريكيَّة للمختبرات) يُعد ممارسة شائعة للمختبرات الجنائيَّة العامَّة والخاصَّة، مع وجود أطر تنظيميَّة على مستوى بعض الولايات -مثل: تكساس- تربط التحليل الجنائي المستخدَم في الإجراءات الجنائيَّة بنظام اعتماد وتنظيم ولائي.	أصدرت NATA (الهيئة الوطنيَّة الأستراليَّة لاعتماد المختبرات) ملحقًا تفسيريًّا يوضِّح كيفيَّة تطبيق معيار ISO/IEC 17025 في مجال التحليل القانوني والعلوم الجنائيَّة، بما يراعي متطلبات العمل القضائي وإدارة الأدلَّة، ويشمل المختبرات والمرافق المعتمَدة والمتقدِّمة.	يوفِّر SAC/SINGLAS (مجلس الاعتماد السنغافوري ونظام اعتماد المختبرات في سنغافورة) منظومة اعتماد رسميَّة للمختبرات وَفْقَ معيار ISO/IEC 17025، تشمل إجراءات اعتماد واضحة وإرشادات تنظيميَّة معتمَدة للاستخدام في السياق القضائي والمهني.

محور المقارنة	المملكة المتحدة (UK)	الولايات المتحدة (US)	أستراليا (Australia)	سنغافورة (Singapore)
أنواع القضايا المسموح بإسنادها إلى القطاع الخاص، وهل حُددت بقانون؟	لا توجد قائمة قانونيَّة محدَّدة بأنواع القضايا التي يمكن إسنادها إلى القطاع الخاص، إذ ينصبُّ التنظيم على أنشطة العلوم الجنائيَّة المستخدَمة في التحقيقات والإجراءات القضائيَّة، خصوصًا في القضايا الجنائيَّة، مع إمكانيَّة الاحتجاج بالمدوَّنة القانونيَّة في القضايا الجنائيَّة والمدنيَّة على حدٍّ سواء، بما يشمل النزاعات المدنيَّة والتجاريَّة متى قُدِّمت الخبرة للمحكمة.	على المستوى الاتحادي، لا توجد قائمة مُحدَّدة لأنواع القضايا التي يمكن إسنادها إلى القطاع الخاص.	لا توجد قائمة قانونيَّة تُحدِّد أنواع القضايا. وعمليًّا، يمكن إشراك القطاع الخاص في القضايا الجنائيَّة والمدنيَّة والتجاريَّة، على أن يُحسَم القبول استنادًا إلى قواعد قبول الخبرة القائمة على المعرفة المتُخصِّصة والتزام الخبير بسلوك مهني مستقل.	لا توجد قائمة قانونيَّة لأنواع القضايا، إلا أن استخدام خبرة القطاع الخاص في التقاضي المدني والتجاري مقيَّد عمليًّا بشرط موافقة المحكمة وتحقيق معيار «الإسهام المادي»، أي أن تُضيف الخبرة فائدة حقيقيَّة ومؤثِّرة لفهم المحكمة لمسألة فنيَّة لا يمكن حسمها دون خبير.
أبرز التحديات	تتمثل أبرز التحديات في صعوبة التزام جميع مزوِّدي خدمات العلوم الجنائيَّة، سواء أكانوا جهات حكوميَّة أم شركات خاصَّة، بمتطلَّبات المدوَّنة القانونيَّة، إضافةً إلى أن أي إخفاق في الالتزام بمعايير الجودة من أحد المزوّدين قد يمتد أثره ليؤثِّر في عدة قضايا، لأن المدوَّنة تُعد مرجعًا قانونيًّا أمام المحكمة، ويجوز للقاضي الاستناد إلى عدم الامتثال لها لتقليل قوة الدليل أو التشكيك في قبوله.	تتمثل أبرز التحديات في تفاوت المعايير بين الولايات والمحاكم، إضافةً إلى نزاع متكرر حول ما إذا كانت مُخرَجات أدوات الأدلَّة الجنائيَّة الرقميَّة تُعد إجراءً تقنيًّا آليًّا يمكن قبوله مباشرة، أم عملًا فنيًّا مُتخصِّصًا يتطلَّب اختيار إعدادات التحليل وتفسير النتائج، وبالتالي يستوجب إخضاع الشخص الذي نفَّذ التحليل لشروط قبول شهادة الخبير، وهو ما توضِّحه قضيَّة Williams الصادرة عام 2023، المتعلِّقة بأداة Cellebrite، التي أبرزت الإشكال الإجرائي والمعياري في التعامل مع هذا النوع من الأدلَّة الرقميَّة.	على الرغم من أن اعتماد المختبرات، مثل: ISO/IEC 17025، يساعد على رفع مستوى الجودة الفنيَّة والتنظيميَّة، فإنه لا يمنع وحده وقوع أخطاء أو اختلافات في تفسير النتائج أو تطبيق المنهجيَّات، ما لم يُدعَم هذا الاعتماد بنظام جودة فعلي وممارسة مهنيَّة سليمة وسلوك خبير واضح يضمن الاستقلاليَّة والدقَّة.	قد تؤدِّي قواعد الإجراءات المدنيَّة لعام 2021 (ROC 2021) إلى الحد من تقديم الخبرات غير الضروريَّة أمام المحكمة، لكنها في المقابل ترفع عبء التحضير على الأطراف لإقناع المحكمة بأهميَّة الخبرة وحاجتها الفعليَّة.

المصدر: إعداد الباحثَين (2026).

وضرورة توثيق جميع الإجراءات بما يضمن إمكانيَّة التحقُّق والمراجعة المستقلَّة. وهذا النموذج يجعل الامتثال المؤسسي شرطًا سابقًا ومؤثرًا في وزن الدليل، ويمنح المحكمة معيارًا موضوعيًّا يمكن الاحتجاج به عند تقييم التقرير. إلا أن صرامة هذا الإطار تفرض عبئًا عاليًا على المختبرات الخاصَّة، إذ إن أي إخلال بمعايير المدوَّنة قد يمتدُّ أثره إلى قضايا مُتعدِّدة، نظرًا لكونها مرجعًا قانونيًّا عامًّا يُحتج به قضائيًّا.

أما في الولايات المتحدة، فالصورة مختلفة، إذ لا يوجد مُنظِّم اتحادي واحد يمنح ترخيصًا للمختبرات الجنائيَّة في القطاع الخاص على مستوى الدولة. ويرتكز الإطار الاتحادي أساسًا على Federal Rules of Evidence – Rule 702، التي تنظم قبول شهادة الخبير، حيث إن المحكمة لا تكتفي بقبول التقرير لأنه صادر عن مختبر معتمد، بل تفحص منهجيَّة التحليل نفسها. وَفْقَ هذا الإطار، يتعيَّن على الجهة التي قدَّمت التقرير أنْ تُثبت أنَّ الشخص الذي أجرى التحليل مؤهَّل علميًّا أو مهنيًّا، وأنَّ المنهجيَّة المستخدَمة قابلة للاختبار والتحقُّق، وأنها تستند إلى مبادئ موثوقة ومعترَف بها، وأنها طُبِّقت تطبيقًا صحيحًا على وقائع القضيَّة. وقد تطلب المحكمة من الخبير شرح خطوات الاستخراج، وأدوات التحليل، والإعدادات التقنيَّة المستخدَمة، وكيف جرى الحفاظ على النسخة الأصليَّة للبيانات من دون تعديل. وعلى مستوى بعض الولايات، مثل: تكساس، يضيف Texas Code of Criminal Pro-cedure Article 38.35 بُعدًا تنظيميًّا يقر بإمكانيَّة أن يكون مختبر الجريمة جهة حكوميَّة أو خاصَّة. وتُفحَص إدارة النسخ الجنائيَّة وسلامة الدليل عمليًّا من خلال استجواب الخبير وملفات التوثيق، أكثر مما تُفرَض عبر تشريع تفصيلي مركزي. وهذا يمنح مرونة كبيرة، لكنه يجعل قوة التقرير مرتبطة بقدرة المختبر الخاص على الدفاع عن منهجيَّته أمام المحكمة في كل قضيَّة على حدة.

وفي أستراليا، لا يوجد قانون اتحادي خاص بالأدلَّة الجنائيَّة الرقميَّة، لكن النظام يعتمد عمليًّا على مزيج من قانون الأدلَّة، وضوابط سلوك الخبير، ومنظومة اعتماد فني تقودها National Association of Testing Authorities, Australia (NATA) وَفْقَ معيارISO/IEC 17025 . هذا المعيار لا يقتصر على دقَّة الأجهزة، بل يشمل نظامًا متكاملًا لإدارة الجودة داخل المختبر الخاص، يتضمَّن توثيق الإجراءات، وضبط العينات، وتسجيل كل خطوة تحليليَّة، وإجراء تدقيق داخلي دوري، واختبارات كفاءة للعاملين. وفيما يتعلَّق بإدارة البيانات، يفرض نظام الاعتماد وجود سياسات مكتوبة للتحكُّم في الوصول إلى البيانات، وتحديد صلاحيات المستخدمين، وحماية النسخ الجنائيَّة من التعديل، وتوثيق أي عمليَّة استخراج أو تحليل. وهنا يكون الضبط مؤسسيًّا تقنيًّا، أي: إن المختبر الخاص يخضع لمراجعة دوريَّة للتأكُّد من أن نظام الجودة يعمل فعليًّا، وليس مجرد إطار شكلي. غير أن هذا الاعتماد، مع أهميَّته، لا يعفي التقرير من الخضوع لتقييم المحكمة من حيث ملاءمته وارتباطه بوقائع القضيَّة.

أما سنغافورة، فتتبنَّى نموذجًا يجمع بين الاعتماد الفني والرقابة الإجرائيَّة المسبقة. فبموجب Rules of Court 2021، وتحديدًا Order 12 Rule 2 (O12 r2)، لا يجوز استخدام خبرة خبير إلا بموافقة المحكمة، وعلى أساس أن تضيف هذه الخبرة «إسهامًا ماديًّا» في فهم مسألة فنيَّة لا يمكن حسمها من دونها. والمقصود بالإسهام الماديّ: أنْ يكون التقرير ضروريًّا لحسم نقطة مؤثرة في النزاع، وليس مجرد رأي إضافي يمكن

الاستغناء عنه. ويتكامل هذا الإطار مع منظومة اعتماد رسميَّة للمختبرات عبر Singapore Accreditation Council - Singapore Laboratory Accreditation Scheme (SAC/SINGLAS) وَفْقَ معيار ISO/IEC 17025 ، وهذا الاعتماد يفرض على المختبرات سياسات واضحة لإدارة الأدلَّة الرقميَّة، تشمل تخزين البيانات في بيئات آمنة، وتوثيق سلسلة الحيازة، وضبط صلاحيات الوصول، وضمان إمكانيَّة تتبُّع أي تعديل أو عمليَّة تحليل جرت على البيانات. وبذلك، فإن التقرير الصادر عن مختبر جنائي في القطاع الخاص يمر بمرحلتين من الضبط، الأولى: فنيَّة مؤسَّسيَّة عبر نظام الاعتماد، والثانية: قضائيَّة عبر شرط الموافقة المسبقة.

وبالتحليل، يتبيَّن أن الفارق بين هذه النماذج لا يتعلَّق بالسماح أو المنع، بل بطريقة تنظيم وضبط عمل القطاع الخاص. ففي المملكة المتحدة، الرقابة تشريعيَّة مؤسَّسيَّة مركزيَّة ذات أثر مباشر في وزن التقرير الفني المقدَّم. وفي الولايات المتحدة ضبط العمل قضائيٌّ بالدرجة الأولى، حيث تُختبر منهجيَّة المختبر الخاص أمام المحكمة في إطار Rule 702. وفي أستراليا، يقوم ضبط العمل أساسًا على الاعتماد الفني المؤسسي عبر National Association of Testing Authorities, Australia (NATA)، مع تكامل ذلك مع قانون الأدلَّة. أما في سنغافورة، فيجتمع الاعتماد الفني عبر Singapore Accreditation Council - Singapore Laboratory Accreditation Scheme (SAC/SINGLAS) مع رقابة إجرائيَّة مسبقة تشترط موافقة المحكمة قبل إدخال التقرير أصلًا.

وتكشف المقارنة بين النماذج الأربعة عن أنَّ إشراك المختبرات الرقميَّة الخاصَّة لا يكون عشوائيًّا، بل من خلال إطار واضح يضمن إمكانيَّة التحقُّق الموضوعي من جودة العمل. فالتجرِبة البريطانيَّة تُبرز أهميَّة تحويل معايير الجودة إلى التزام قانوني يجعل الامتثال المؤسسي جزءًا من وزن الدليل نفسه، بينما تؤكِّد التجرِبتان الأستراليَّة والسنغافوريَّة أن الاعتماد الفني الرسمي والمراجعات الدوريِّة يوفِّران بيئة مستقرة تُقيَّم فيها المختبرات على أساس نظام جودة فعلي يشمل توثيق الإجراءات وضبط سلسلة الحيازة وإدارة البيانات.

في المقابل، تُبرز التجرِبة الأمريكيَّة دور المحكمة باعتبارها الجهة الحاسمة في منح التقرير قوته الإجرائيَّة، حيث يُختبَر التقرير من خلال منهجيَّته وقابليَّته للتحقُّق، لا من خلال صفة الجهة التي أصدرته. وهذا يعكس مبدأ أساسيًّا مفاده أن قوة الدليل لا ترتبط بكون المختبر حكوميًّا أو خاصًّا، بل بقدرته على الدفاع عن إجراءاته بشفافية أمام القضاء.

كما تؤكِّد التجارِب الأربع أن إدارة البيانات داخل المختبر ليست مسألة تقنيَّة جانبيَّة، بل عنصر جوهري في حماية سلامة الدليل، وأن قابليَّة تتبُّع الإجراءات منذ تسلُّم البيانات حتى إصدار التقرير شرط أساسي لتفادي الطعن أو الاستبعاد. وفي ضوء ذلك، يتبيَّن أن النموذج الأكثر استقرارًا هو الذي يجمع بين الاعتماد الفني والرقابة القضائيَّة وإطار مساءلة واضح، بحيث تُبنى الثقة على شفافية الإجراءات وقابليَّتها للتدقيق، لا على ملكيَّة المختبر.

البدائل السياساتيَّة

البديل الأول: الإبقاء على النموذج الحكومي الكامل

يقوم هذا البديل على استمرار إدارة وتشغيل مختبرات الأدلَّة الرقميَّة بالكامل من قِبَل الجهات الحكوميَّة، بما يشمل البنية التحتيَّة التقنيَّة والكوادر البشريَّة والإجراءات الفنيَّة والقانونيَّة المرتبطة بتحليل الأدلَّة الرقميَّة. ويتميَّز هذا النموذج بقدرته على ضمان مستوى مرتفع من السيطرة المؤسَّسيَّة وحماية السيادة

الرقميَّة، حيث تبقى البيانات والأدلَّة الحساسة ضمن المؤسسات الحكوميَّة، وتخضع بالكامل للإجراءات القضائيَّة وسلسلة الحيازة.

ومع أنَّ هذا المسار يمنح أعلى درجات السيطرة المؤسَّسيَّة، فإن كلفته الإجماليَّة تكون عادةً أعلى من النماذج البديلة، نظرًا لاعتماد مختبرات الأدلَّة الرقميَّة الحكوميَّة على استثمارات تقنيَّة وبنية تحتيَّة متقدِّمة قادرة على التعامل مع مختلف أنواع الأدلَّة الرقميَّة والقضايا الجنائيَّة المعقَّدة. فالمختبرات الحكوميَّة تتطلَّب منظومة متكاملة من المختبرات التخصُّصيَّة، تشمل: مختبرات تحليل الحواسيب والهواتف المحمولة، ومختبرات استخراج البيانات المتقدِّمة باستخدام تقنياتChip-Off وJTAG، إضافة إلى مختبرات تحليل الوسائط المُتعدِّدة والصوتيَّات الرقميَّة، ومختبرات تحليل الطائرات المسيَّرة والأجهزة الذكيَّة، فضلًا عن وحدات مُتخصِّصة لتحليل التشفير وكسر كلمات المرور.

كما تتطلَّب هذه المختبرات أنظمة تخزين بيانات واسعة النطاق لحفظ النسخ الجنائيَّة للأدلَّة الرقميَّة، وتطبيق أنظمة متقدِّمة لإدارة الأدلَّة الرقميَّة وسلسلة الحيازة، إضافةً إلى بيئة أمن معلومات متقدِّمة تشمل الشبكات المعزولة وأنظمة التحكُّم في الوصول والمراقبة المستمرة. وتضاف إلى ذلك تكاليف تجهيز محطات عالية الأداء، وشراء الأدوات البرمجيَّة الجنائيَّة المُتخصِّصة، وتجديد التراخيص السنويَّة لهذه الأدوات، إضافة إلى متطلَّبات التشغيل والصيانة.

وبسبب هذه المتطلَّبات التقنيَّة والتشغيليَّة المُتعدِّدة، فإن التكلفة الإجماليَّة لإنشاء مختبر حكومي متكامل للأدلَّة الرقميَّة تكون مرتفعة نسبيًّا، حيث تشير التقديرات العمليَّة لتجهيز هذه المختبرات إلى أن إجمالي تكلفة الإنشاء والتجهيز قد يتراوح عادةً بين 3 و7 ملايين دولار بحسب حجم المختبر ونطاق عمله وعدد القضايا التي يتعامل معها سنويًّا.

ولا تقتصر التكاليف المطلوبة على تجهيز المختبرات فحسب، بل تشمل أيضًا توظيف وتأهيل الكوادر المُتخصِّصة في التحقيق الجنائي الرقمي. وحسب موقع SANS، فإنَّ معدَّل رواتب حديثي التخرُّج من فاحصي الأدلَّة الرقميَّة الحاصلين على درجة البكالوريوس في تخصُّص الأدلَّة الرقميَّة يتراوح بين 50,000 $ و70,000$ سنويًّا، بينما يحصل حديثو التخرُّج من برامج الماجستير على راتب سنوي يقارب 80,000$.

والتعامُل مع الأدلَّة الرقميَّة يتطلَّب خبرات فنيَّة مُتخصِّصة تُكتَسَب من خلال برامج تدريبيَّة متقدِّمة ومستمرَّة، فعلى سبيل المثال: تبلغ تكلفة الدورة التدريبيَّة المُتخصِّصة في مجال التحقيق الجنائي الرقمي ضمن برامج SANS Digital Forensics نحو 8,780 دولارًا للدورة الواحدة التي تمتدُّ لستة أيام-(SANS In stitute) . ويعرض الجدول 2 تقديرًا لتكلفة تدريب خبير الأدلَّة الرقميَّة، حيث يتطلب تأهيل الخبير عادةً برنامجًا تدريبيًّا يمتد، على الأقل، أربعة أو خمسة أسابيع تدريبيَّة.

وعلى الرغم من أن هذا النموذج يوفر مستوى مرتفعًا من العدالة الإجرائيَّة؛ نظرًا لاستقلاليَّة المختبرات الحكوميَّة، فإن الحفاظ على هذا المستوى يتطلَّب استثمارات ماليَّة كبيرة في البنية التحتيَّة التقنيَّة، وتأهيل الكوادر البشريَّة المُتخصِّصة. فمختبرات الأدلَّة الرقميَّة تعتمد على أجهزة تحليل متقدِّمة، وبرمجيَّات احترافيَّة، وأنظمة تخزين وأمن معلومات، إضافة إلى التدريب المستمر للخبراء. ومع توسُّع حجم الأدلَّة الرقميَّة وتطور أدوات التحليل، ترتفع كلفة التحديث والصيانة التي لا تقل عن 10% سنويًّا، والتأهيل

جدول 2
تكلفة تدريب خبير الأدلَّة الرقميَّة

محور المقارنة للخبير الواحد	التكلفة
تكلفة الدورة التدريبيَّة (أسبوع تدريبي)	$ 8,780
تكلفة اليوم التدريبي الواحد	نحو $ 1,460
برنامج تدريبي لمدة خمسة أسابيع	نحو $ 43,900

المصدر: إعداد الباحثَين (2026).

باستمرار، ما قد يفرض عبئًا ماليًّا كبيرًا على الجهات الحكوميَّة ويجعل التوسُّع في إنشاء مختبرات جديدة أو استحداث وظائف تقنيَّة مُتخصِّصة أكثر تكلفةً وتعقيدًا.

البديل الثاني: استثمار القطاع الخاص في مختبرات الأدلَّة الرقميَّة

يقوم هذا البديل على تمكين القطاع الخاص من تشغيل مختبرات الأدلَّة الرقميَّة، أو تقديم خدمات التحليل الجنائي الرقمي، ويُنظَر إلى هذا النموذج باعتباره خيارًا يتيح قدرًا أكبر من المرونة التشغيليَّة، إذ يمكن للقطاع الخاص الاستثمار بسرعة أكبر في التقنيات الحديثة واستقطاب الخبرات المتُخصِّصة، ما قد يُسهِم في رفع كفاءة التحليل الجنائي الرقمي وتسريع معالجة القضايا المرتبطة بالأدلَّة الإلكترونيَّة.

غير أن هذا النموذج يطرح في المقابل عددًا من التحديات المرتبطة بالمخاطر النظاميَّة واحتمالات تضارُب المصالح في البيئة الربحيَّة، وبخاصَّةٍ عندما تعمل المختبرات الخاصَّة وَفْقَ عقود ماليَّة مرتبطة بعدد القضايا أو سرعة إنجاز التحليل الرقمي. ففي مثل هذه الحالات، قد ينشأ تضارب محتمل بين الاعتبارات التجاريَّة للمختبر، مثل: تعظيم الإيرادات أو تقليل زمن إنجاز القضايا، وبين متطلبات الحياد العلمي والدقة الجنائيَّة التي يجب أن تحكم عمليَّة تحليل الأدلَّة الرقميَّة. وقد يؤدِّي ذلك إلى إثارة تساؤلات قانونيَّة حول استقلاليَّة التقارير الفنيَّة وموضوعيَّتها، وهو ما قد ينعكس مباشرةً على ثقة القضاء بنتائج التحليل الجنائي الرقمي، ويزيد احتمالات الطعن في الأدلَّة الرقميَّة أمام المحاكم أو المطالبة بإعادة الفحص الفني في بعض القضايا.

ولهذا السبب، يتطلب تطبيق هذا النموذج وجود إطار تنظيمي يُحدِّد بوضوح نطاق عمل المختبرات الخاصَّة، ويضمن اعتمادها وَفْقَ معايير مهنيَّة وتقنيَّة، إضافةً إلى إخضاعها لآليَّات رقابة وتقييم دوري لضمان جودة التحليل الفني والحفاظ على موثوقيَّة الأدلَّة الرقميَّة. بالإضافة إلى تقليل مخاطر تضارب المصالح، والحد من التفاوت في مستوى الأداء بين المختبرات المختلفة، بما يحافظ على مصداقيَّة التقارير الفنيَّة أمام الجهات القضائيَّة.

البديل الثالث: النموذج الهجين

يقوم النموذج الهجين على الجمع بين الإشراف الحكومي على الإجراءات الجنائيَّة وسلسلة الحيازة من جهة، والاستفادة من قدرات القطاع الخاص التقنيَّة والاستثماريَّة من جهةٍ أخرى. ويهدف هذا النموذج إلى تحقيق توازن بين الكفاءة التشغيليَّة والضمانات القانونيَّة

جدول 3
مقارنة بين البدائل السياساتيَّة

محور المقارنة	النموذج الحكومي الكامل	استثمار القطاع الخاص في مختبرات الأدلَّة الرقميَّة	النموذج الهجين
الكفاءة التشغيليَّة	قدرة إنجاز مستقرَّة لكنها قد تتأثَّر بتراكُم القضايا ونقص الخبراء المُتخصِّصين	قدرة إنجاز أعلى نسبيًّا نتيجة مرونة الاستثمار واستقطاب الخبرات التقنيَّة	قدرة تشغيليَّة متوازنة عبر توزيع القضايا بين مختبرات حكوميَّة ومختبرات معتمَدة
الكلفة التقديريَّة	استثمارات حكوميَّة مرتفعة تشمل إنشاء المختبرات والبنية التقنيَّة والتشغيل المستمر	يتحمَّل القطاع الخاص الاستثمار في البنية التحتيَّة والتقنيات والتشغيل	تقاسُم تكاليف الاستثمار والتشغيل
المخاطر النظاميَّة	منخفضة بسبب السيطرة الحكوميَّة الكاملة على المختبرات والإجراءات	مرتفعة نتيجة احتمالات تضارُب المصالح في البيئة الربحيَّة	منخفضة من خلال تطوير إطار تنظيمي ورقابي يشرف على المختبرات المعتمَدة
العدالة الإجرائيَّة	مرتفعة بسبب استقلاليَّة المختبرات الحكوميَّة وارتباطها المباشر بالجهات العدليَّة	تكون عرضة للطعن في بعض الحالات القضائيَّة	مرتفعة وجود آليَّات اعتماد ورقابة حكوميَّة على المختبرات
السيادة على الأدلَّة الرقميَّة	مرتفعة لأن البيانات والأدلَّة تبقى ضمن السيطرة الحكوميَّة	أقل نسبيًّا لمشاركة شركات خاصَّة أو مزوِّدي خدمات خارجيين	مرتفعة لوجود ضوابط تنظيميَّة وإشراف حكومي على معالجة الأدلَّة

المصدر: إعداد الباحثَين (2026).

من خلال إنشاء إطار تنظيمي يسمح باعتماد مختبرات خاصَّة تعمل تحت إشراف الجهات الحكوميَّة المختصَّة.

وفي هذا النموذج، تحتفظ الجهات الحكوميَّة بدورها في تنظيم الإجراءات القضائيَّة والرقابة على جودة التحليل الجنائي، بينما يسهم القطاع الخاص في توفير البنية التحتيَّة التقنيَّة والكوادر المُتخصِّصة.

كما يسهم هذا النموذج في تقليل العبء المالي على الحكومة من خلال تقاسُم تكاليف الاستثمار في البنية التحتيَّة التقنيَّة، مع الحفاظ على معايير العدالة الإجرائيَّة والسيادة الرقميَّة. ولهذا يُنظَر إلى النموذج الهجين باعتباره خيارًا توازنيًّا يجمع بين الكفاءة التشغيليَّة والرقابة المؤسَّسيَّة. وقد يُسهِّل هذا النموذج استثمار الأصول الحكوميَّة عن طريق تأجير المختبرات الرقميَّة للقطاع الخاص.

الخاتمة

تؤكِّد هذه الورقة أهمية تمكين متخذ القرار من الموازنة بين البدائل الثلاثة المطروحة لتنظيم إنشاء وتشغيل مختبرات الأدلة الجنائية الرقمية، بما يحقق التكامل بين الكفاءة الفنية والموثوقية القضائية

والاستدامة. بهدف تقديم خدمات متكاملة تشمل جمع الأدلَّة وتحريزها، وفحص الأجهزة الرقميَّة المُتعدِّدة، وتحليل الأدلَّة وإعداد تقارير فنيَّة قابلة للاستخدام القضائي، مع إتاحة الاستعانة بخبراء معتمَدين لدى الجهات العدليَّة. إلا أن نجاح هذا التوجُّه يتطلَّب ضرورة وجود إطار تنظيمي حكومي واضح يُنظِّم عمل المختبرات الخاصَّة، ويشمل:

- تصنيفًا محدَّدًا لأنواع القضايا المسموح بإسنادها إلى المختبرات الخاصَّة لمنع الإسناد العشوائي.
- تحديدًا دقيقًا لنطاق المسؤوليَّة الفنيَّة والقضائيَّة وحدود الصلاحيَّات لضمان المساءلة.
- الالتزام الكلي بالتشريعات المتعلِّقة بحماية البيانات الشخصيَّة والجنائيَّة.

ومن أجل ضمان جودة الخدمات وموثوقيَّتها، يُعد إلزام المختبرات بالحصول على اعتماد فني وَفْقَ ISO/IEC 17025 ممارسة دوليَّة مُثلَى، كما يستلزم اعتماد أطر مهنيَّة وإجرائيَّة معترَف بها لإدارة وفحص الأدلَّة وسلسلة الحيازة، مثل دليل ACPO/NPCC وإرشادات NIST، مِمَّا يسهم في سلامة الأدلَّة الرقميَّة ومصداقيَّتها.

وفيما يخص الكوادر البشريَّة، يوصَى بوضع شروط تأهيل مُلزِمة للخبراء في الأدلَّة الرقميَّة، تتضمَّن برامج تدريب معتمَدة، واختبارات كفاءة دوريَّة، ومتطلَّبات تطوير مهني مستمر، مع إشراك الجامعات والمؤسسات الأكاديميَّة المُتخصِّصة في تصميم هذه البرامج وتنفيذها (مِمَّا يضمن مسارًا تأهيليًّا مؤسسيًّا ومنهجيًّا للمحققين الرقميين). كذلك وضع وصف وظيفي موحَّد للمحققين الرقميين استنادًا إلى أطر كفاءات معتمدة تقارَن بالأطر الدوليَّة، مثل:NIST NICE Framework ، والإطار السعودي لكوادر الأمن السيبراني(SCyWF)، لضمان وضوح المهام، وتحديد المسؤوليَّات الفنيَّة، وترسيخ آليَّات المساءلة المهنيَّة، حيث إن تطبيق هذه التوصيات يوازن بين تعزيز مشاركة القطاع الخاص وتطوير القدرات الوطنيَّة من جهة، والحفاظ على نزاهة الأدلَّة والإجراءات القضائيَّة وصلاحيتها من جهة أخرى.

المراجع

Ace Computers. (2023). Building a digital forensics lab: Equipment checklist and setup guide.

https://acecomputers.com/building-a-digital-forensics-lab/

Bayt Magazine. (2024). Arab world hits record 348 million internet users in 2024.

https://baytmagazine.com/report-arab-world-hits-record-348m-internet-users-in-2024/

Communications, Space and Technology Commission. (2025, May 12). CST issued the Saudi Internet Report 2024.

https://www.cst.gov.sa/ar/media-center/news/N2025051200

Emarat Al Youm. (2025, December 23). Local business report.

https://www.emaratalyoum.com/business/local/2025-12-23-1.1999542

Europol. (2022). Internet organised crime threat assessment (IOCTA). European Union Agency for Law Enforcement Cooperation.

https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta

https://jordantimes.com/news/local/1249b-gb-broadband-data-consumed-q1-2024-trc

Morocco World News. (2025). Morocco's digital market booms with 3.7 million new online shoppers.

https://www.moroccoworldnews.com/2025/11/266971/moroccos-digital-market-booms-with-3-7-million-new-online-shoppers/

National Association of Testing Authorities. (2021). Forensic science – ISO/IEC 17025 and forensic interpretations (Appendix).

https://nata.com.au/files/2021/05/Forensic-Science-ISO-IEC-17025-Appendix-effective-feb-2020.pdf

National Cybersecurity Authority. (2020). The Saudi Cybersecurity Workforce Framework (SCyWF).

https://nca.gov.sa/scywf_en.pdf

National Institute of Justice. (2020). Addressing the digital evidence backlog. U.S. Department of Justice.

https://nij.ojp.gov/topics/articles/addressing-digital-evidence-backlog

National Institute of Standards and Technology. (2020). Computer forensics tool testing program.

https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program

Onyx Consulting. (2025). Morocco adds 3.7M new online shoppers in 2025.

Gartner, Inc. (2024, November 19). Gartner forecasts worldwide public cloud end-user spending to total $723 billion in 2025.

https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025

Government of the United Kingdom. (2021). Forensic Science Regulator Act 2021 (c. 14).

https://www.legislation.gov.uk/ukpga/2021/14/pdfs/ukpga_20210014_en.pdf

Government of the United Kingdom. (2023). Statutory code of practice for forensic science activities.

https://www.gov.uk/government/publications/statutory-code-of-practice-for-forensic-science-activities

GSMA. (2024). The mobile economy Middle East & North Africa 2024.

https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/11/181124-Mobile-Economy-MENA-2024.pdf

IoT Analytics. (2025, October 28). State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally.

https://iot-analytics.com/number-connected-iot-devices/

Jordan Pulse. (n.d.). Digital economy report.

https://www.jordanpulse.com/article/13557

Jordan Times. (2024). 1249B GB broadband data consumed in Q1 2024.

evidence in criminal proceedings. Computer Law & Security Review, 55, 106040. https://doi.org/10.1016/j.clsr.2024.106040

Texas Legislature. (2019). Texas Code of Criminal Procedure, Article 38.35. https://statutes.capitol.texas.gov/?tab=1&code=CR&chapter=CR.38&artSec=38.35

United Nations Office on Drugs and Crime. (2022). Public–private partnerships in cybercrime investigations. https://www.unodc.org/documents/cybercrime/PublicPrivatePartnerships_Cybercrime.pdf

Vermeer, M. J. D., Woods, D., & Jackson, B. A. (2018). Identifying law enforcement needs for access to digital evidence in remote data centers. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2240/RAND_RR2240.pdf

https://onyx.ma/morocco-adds-3-7m-new-online-shoppers-in-2025/

Parliament of New South Wales. (1995). Evidence Act 1995 (NSW), section 79. https://classic.austlii.edu.au/au/legis/nsw/consol_act/ea199580/s79.html

SANS Institute. (2024). Digital acquisition & rapid triage (FOR498). https://www.sans.org/cyber-security-courses/digital-acquisition-rapid-triage

Singapore Accreditation Council. (2023). Laboratory accreditation documentation. https://www.sac-accreditation.gov.sg/resources/sac-documents/laboratory-accreditation/

Singapore Attorney-General's Chambers. (2021). Evidence (Amendment) Act 2021. https://sso.agc.gov.sg/SL-Supp/S914-2021/

Stoykova, R. (2024). A new right to procedural accuracy: A governance model for digital

May 2026 مايو 2026

Centre for Cybercrime and Economic Crime
Naif Arab University for Security Sciences, Saudi Arabia, Riyadh

مركز الجرائم السيبرانية والاقتصادية
جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، الرياض

Keywords: digital forensics, digital forensic laboratories, privatization, chain of custody, operational challenges

الكلمات المفتاحية: الأدلة الجنائية الرقمية، مختبرات الأدلة الجنائية الرقمية، الخصخصة، سلسلة الحيازة، التحديات التشغيلية

Production and hosting by NAUSS

Email: coecdf@nauss.edu.sa
doi: 10.26735/JXRI1843