المادة العلمية للقاء التدريبي
التحول الرقمي والحكومة الذكية
2025م

ديـــوان المحاسبـــة
State Audit Bureau
State of Qatar • دولـــة قطـــر

فهرس المحتويات

رقم التسلسل	البيان	رقم الصفحة
	المقدمة	4
اولاً	حكومة قطر الرقمية	5
1	دور حكومة قطر	5-6
2	النهج المتبع في التحول الرقمي	6
3	الرؤية والأهداف الاستراتيجية	6-7
4	المحاور الاستراتيجية لبرنامج حكومة قطر الرقمية	7-9
5	أبرز المشاريع والمبادرات	9-10
ثانياً	استراتيجيات التحول الرقمي للأجهزة العليا للرقابة المالية والمحاسبة	11
1	التحول الرقمي في ديوان المحاسبة القطري	11-12
2	تجارب عربية في التحول الرقمي للأجهزة الرقابية	13-14
3	التوجهات العالمية في التحول الرقمي للأجهزة العليا للرقابة	14-16
4	المعايير والممارسات الدولية ذات الصلة	16-18
ثالثاً	تطبيق الحكومة الذكية في الأجهزة العليا للرقابة	19
1	برامج ديوان المحاسبة	19-20
2	استراتيجية الذكاء الاصطناعي في أعمال الرقابة	21-22
رابعاً	التحديات التي تواجه التحول الرقمي والحكومة الذكية	22
1	التحول الرقمي والمواطنة الرقمية	22-23
2	الاستثمار في التعليم والتدريب	23-24
3	الأمن السيبراني وحماية البيانات	24-25
خامساً	دور الرقابة في التحول الرقمي والحوكمة الذكية	26
1	ضمان الامتثال للقوانين والمعايير القياسية	26-27
2	التقييم المستمر للأداء والمخاطر	27-28
3	الشفافية والمساءلة	28-29
4	إدارة الموارد التقنية والمالية	30
5	دعم الابتكار التكنولوجي	30-32
سادساً	التحديات الي تواجه الرقابة على التكنولوجيا المعلومات في الحكومة الذكية	32
1	تطور التكنولوجي السريع	32-33
2	مواجهة الهجمات الإلكترونية	33-34
3	تحديات تدريب وتطوير الموظفين	35-36
	الخاتمة	36-37

المقدمة:

أصبح التحول الرقمي ومبادرات الحكومة الذكية محورًا أساسيًا في تطوير العمل الحكومي وتعزيز كفاءة الخدمات العامة. فالحكومات الذكية تسعى للاستفادة من تقنيات المعلومات والاتصالات لتقديم خدمات متكاملة وسريعة عبر منصات رقمية متطورة، مع التركيز على تبسيط الإجراءات وتلبية احتياجات المواطنين بشكل أفضل. وترى دول عدة أن هذه التحولات الرقمية تعزز النمو الاقتصادي وتحسّن مستوى معيشة المواطنين من خلال الارتقاء بكفاءة العمليات الحكومية. كما تُولي الأجهزة الرقابية اهتمامًا خاصًا للحكومة الذكية بوصفها رافعة مهمة لتعزيز نظم الرقابة المالية، إذ تؤكد مبادرات عديدة أهمية الرقابة الإلكترونية في إطار هذا التحول الشامل.

وفي إطار استراتيجيات التحول الرقمي، تبنت الأجهزة العليا للرقابة المالية والمحاسبة أدوات وتقنيات تدقيق متقدمة. فتسعى هذه الأجهزة إلى استخدام الذكاء الاصطناعي وتحليلات البيانات والبلوك تشين وإنترنت الأشياء لتحسين جودة وكفاءة أعمالها. كما يركز جهاز الرقابة على بناء قدرات المدققين من خلال التدريب المستمر، حيث تبرز تقارير دولية ضرورة استبدال المنهجيات التقليدية بأخرى مبنية على الذكاء الاصطناعي لرفع فعالية عمليات التدقيق.

تتجلّى تطبيقات الحكومة الذكية في الرقابة المالية باستخدام نظم تدقيق إلكترونية متطورة وأدوات تحليل وتبادل بيانات متكاملة. فمثلاً، يساهم استخدام نظم ذكاء الأعمال في تحليل البيانات المالية وكشف أنماط الإنفاق غير الطبيعية والكشف المبكر عن المؤشرات الاحتيالية مما يعزز الشفافية وكفاءة توزيع الموارد. كما تساعد تقنيات الذكاء الاصطناعي في تسريع عمليات التدقيق وزيادة دقتها من خلال توفير المعلومات والأدلة في الوقت المناسب. ومن ناحية تبادل المعلومات، قام ديوان المحاسبة القطري بإنشاء قاعدة بيانات إلكترونية موحدة لكافة الجهات الخاضعة لرقابته، بهدف تسهيل جمع المعلومات والارتقاء بالتنسيق مع الجهات الرقابية الأخرى. ومع ذلك، يواجه التحول الرقمي في قطاع الرقابة المالية تحديات تتعلق بضمان أمن البيانات وتطوير البنية التحتية وبناء الكفاءات البشرية والتأقلم مع التنظيمات الجديدة.

اولاً: حكومة قطر الرقمية

تعد حكومة قطر الرقمية مبادرة استراتيجية تهدف إلى توظيف التكنولوجيا الحديثة للارتقاء بالخدمات الحكومية وتعزيز الكفاءة والشفافية. تأتي هذه الجهود ضمن إطار رؤية قطر الوطنية 2030 التي تسعى إلى تحويل قطر إلى دولة متقدمة تحقق التنمية المستدامة. امتلكت قطر مقومات قوية للتحول الرقمي بفضل الاستثمار الكبير في البنية التحتية للاتصالات وتكنولوجيا المعلومات ودعم القيادة للتحديث الحكومي. وقد بدأت الرحلة مبكرًا، حيث شهد عام 2003 إطلاق أول بوابة حكومة إلكترونية في قطر، مما أتاح تقديم خدمات رقمية شاملة وسهّل وصول المواطنين والمقيمين إلى المعلومات والخدمات. ومنذ ذلك الحين، تبنّت الدولة سياسات داعمة للابتكار الرقمي، مستفيدةً من مواردها لتعزيز مجتمع واقتصاد قائمين على المعرفة.

على الصعيد الوطني، أدركت قطر مبكرًا أهمية التحول الرقمي كعامل ممكن لتحقيق التنويع الاقتصادي وتحسين جودة الحياة. وقد صرّحت الدولة في محافل دولية بأن التحول الرقمي عنصر أساسي لتحقيق رؤية 2030 وبناء دولة متقدمة قادرة على المنافسة عالميًا. في هذا السياق، تم دمج خطط الحكومة الرقمية ضمن الاستراتيجيات الوطنية للتنمية، وتأسست هيئات مختصة لقيادة البرنامج مثل وزارة الاتصالات وتكنولوجيا المعلومات. وبفضل صغر حجم السكان نسبياً وارتفاع معدلات انتشار الإنترنت (تتجاوز 95% من السكان)، وفّرت قطر بيئة مناسبة لاعتماد الخدمات الإلكترونية بسرعة وفاعلية.

1. دور حكومة قطر الرقمية

يلعب برنامج حكومة قطر الرقمية دورًا محوريًا في تحديث القطاع العام وتحقيق الإدارة الحكومية الرشيدة. فالهدف الأساس هو رفع كفاءة الأداء الحكومي عبر تبسيط الإجراءات وأتمتة العمليات وتقليل الاعتماد على الورق، مما ينعكس في خدمات أسرع وأكثر دقة للمستفيدين. كما يسعى البرنامج إلى تعزيز الشفافية والمساءلة من خلال إتاحة المعلومات والبيانات الحكومية ورفع مستوى التواصل بين الحكومة والجمهور. وبذلك تساهم الحكومة الرقمية في تعزيز مبادئ الحوكمة كالنزاهة والشفافية، وترسيخ ثقة المواطنين في المؤسسات العامة.

ومن الأدوار المهمة أيضًا تحفيز الاقتصاد الرقمي عبر خلق فرص أعمال في قطاع تكنولوجيا المعلومات وتشجيع الابتكار وريادة الأعمال الرقمية. فقد استثمرت قطر موارد مالية كبيرة لتحقيق هذا التحول، حيث خصصت الحكومة مبلغ 9 مليارات ريال قطري (نحو 2.5 مليار دولار) لتنفيذ برنامج التحول الرقمي الشامل. ويركز هذا الاستثمار على تطوير التقنيات والبنية التحتية، ودعم الابتكار ووضع التقنيات الحديثة –

لاسيما الذكاء الاصطناعي – في قلب النمو الاقتصادي والحضري. وبالتالي، لا يقتصر التحول الرقمي على الجانب التقني فقط، بل يمتد ليكون ركيزة لتنويع الاقتصاد وبناء مجتمع معرفي متقدم.

2. النهج المتبع في التحول الرقمي

اتبعت حكومة قطر نهجًا متدرجًا ومنظمًا في تنفيذ برنامجها للتحول الرقمي. في المراحل الأولى، ركزت الجهود على تطوير البنية التحتية الرقمية وتعزيز جاهزية الأجهزة الحكومية. تم إنشاء شبكة حكومية موحدة واتخذت خطوات لضمان أمن المعلومات وحماية البيانات. كما جرى إطلاق بوابات إلكترونية مركزية مثل بوابة الخدمات الحكومية الإلكترونية (حكومي – Hukoomi) لتكون منصة شاملة تتجمع فيها الخدمات في مكان واحد. تميز هذا النهج بالتركيز على تبسيط الإجراءات وإعادة هندسة العمليات الحكومية قبل رقمنتها، لضمان فعالية التحول وعدم مجرد نقل التعقيدات الورقية إلى الأنظمة الإلكترونية.
وفي إطار النهج نفسه، وضعت الدولة استراتيجيات رقمية وطنية تقود المسيرة وتنسّق الجهود بين مختلف الجهات. فعلى سبيل المثال، أطلقت استراتيجية حكومة قطر الرقمية 2020 في عام 2014 لترسم خارطة طريق واضحة للنهوض بالمستقبل الرقمي. تضمنت هذه الاستراتيجية خططًا زمنية محددة ومؤشرات قياس للأداء، مما ساعد الجهات الحكومية على متابعة التقدم المحرز. كما تم تبني سياسات حوكمة تقنية المعلومات لضمان التنسيق وتجنب الازدواجية بين المشاريع المختلفة، حيث وُضِع نموذج حوكمة يسد الفجوة بين التخطيط الاستراتيجي والتنفيذ الميداني لتحقيق الرؤية. هذا النهج الممنهج ساهم في تحقيق مواءمة بين الرؤية الوطنية والتنفيذ التشغيلي على أرض الواقع.

3. الرؤية والأهداف الاستراتيجية

ترتكز رؤية حكومة قطر الرقمية على بناء حكومة متميزة رقميًا تضع الناس في المقدمة. وهذا يعني توفير خدمات حكومية تتسم بالكفاءة والتكامل، وتتمحور حول احتياجات المستفيدين – سواء كانوا مواطنين أم مقيمين أم مؤسسات أعمال. ومن خلال هذه الرؤية، تسعى قطر إلى أن تكون الحكومة استباقية ومبادرة، بحيث تقدم خدمات ذكية تراعي الظروف الحياتية المختلفة وتسهم في تحسين جودة الحياة. وتطمح الرؤية إلى تحقيق تحوّل شامل يجعل الخدمات متاحة عبر قنوات رقمية متعددة بشكل سلس وآمن، على مدار الساعة، بحيث يشعر المستخدم بأن الحكومة قريبة منه وفي خدمته دائمًا.

ولتحقيق هذه الرؤية، وُضعت أهداف استراتيجية طموحة. من أبرزها رفع ترتيب قطر في مؤشرات الحكومة الإلكترونية العالمية. وقد أثمرت الجهود تقدماً ملحوظاً في مؤشر الأمم المتحدة لتطوير الحكومة الإلكترونية (EGDI)، حيث قفزت قطر من المركز 78 عالميًا إلى المركز 53 في إصدار عام 2024. بل وكانت ضمن أكثر 5 دول عالميًا تحسينًا في هذا المؤشر خلال تلك الفترة، مما يدل على تسارع وتيرة التحول الرقمي. وتشمل الأهداف أيضًا توفير خدمات حكومية متكاملة وذكية تلبي توقعات المستخدمين، وتعزيز كفاءة التشغيل الداخلي بالمؤسسات الحكومية عبر التحول إلى بيئة رقمية قليلة الاعتماد على المعاملات الورقية. كما تولي الرؤية أهمية خاصة لضمان أمن المعلومات وحماية خصوصية المستخدمين ضمن منظومة الخدمات الرقمية.

4. المحاور الاستراتيجية لبرنامج حكومة قطر الرقمية

يعتمد برنامج حكومة قطر الرقمية على عدد من المحاور أو الركائز الاستراتيجية التي توجه المبادرات والمشاريع. هذه المحاور تشكل معًا إطارًا شاملاً لتحقيق التحول الرقمي المتكامل، ويمكن تلخيص أبرزها كالتالي:

- محور البنية التحتية الرقمية المتطورة: ويهدف إلى توفير بنية تحتية عالمية المستوى للاتصالات وتقنية المعلومات تتسم بالأمان والاستدامة. يشمل ذلك شبكات اتصال عالية السرعة والاعتمادية، ومراكز بيانات سحابية حكومية تدعم مشاركة الموارد بين الجهات، بالإضافة إلى بنية تحتية تشريعية وتنظيمية تمكّن التحول الرقمي.

- محور الخدمات الحكومية الإلكترونية: الذي يركز على تحسين الخدمات ورفع كفاءة وفعالية تقديمها رقمياً. في هذا المحور يتم إعادة تصميم الخدمات حول المستفيد (حياة المستخدم)، بحيث تصبح خدمات رقمية بسيطة وذات معنى تغطي مختلف مجالات الحياة (مثل خدمات الزواج، وتأسيس الأعمال، والرعاية الصحية، وغيرها) بطريقة متكاملة. والهدف هو ضمان وصول الخدمات إلكترونيًا بشكل سهل وشفاف للمواطنين والمقيمين والشركات.
- محور البيانات والتقنيات الحديثة: وهو معني ببناء أسس قوية لإدارة البيانات واعتماد التقنيات الناشئة. تسعى قطر من خلاله إلى الاستفادة من تحليل البيانات الضخمة والذكاء الاصطناعي وتقنية البلوك تشين في اتخاذ القرار وصياغة السياسات العامة. كما يتضمن المحور تطوير سياسات لإدارة البيانات الحكومية وفتحها (Open Data) للاستخدام العام وتعزيز الابتكار القائم على البيانات.

- محور الابتكار الرقمي وريادة الأعمال: الذي يستهدف تنمية قطاع رقمي ابتكاري ومزدهر من خلال دعم الاستثمارات والبحوث التطبيقية. من أمثلة ذلك إنشاء مركز حاضنة الأعمال الرقمية الذي يقدم الدعم للشركات الناشئة والمواهب المحلية في مجال التكنولوجيا. وكذلك برنامج مسرّعة تسمو (TASMU) للمدن الذكية والابتكار، والذي يوفر منصات تجريبية وحلول ذكية في مجالات مثل الزراعة الذكية والأمن الغذائي وغيرها.

- محور المجتمع الرقمي وبناء القدرات: وهو يهدف إلى بناء مجتمع واعٍ ومتمكن رقمياً عبر نشر الثقافة الرقمية وتعزيز المهارات. يتضمن هذا المحور برامج لرفع كفاءة الموظفين الحكوميين رقمياً، وإطلاق مبادرات تدريبية لجميع فئات المجتمع لاكتساب المهارات اللازمة للتعامل مع الخدمات الرقمية بثقة وأمان. ويُعد برنامج مثل استوديو 6/5 مثالاً حيث يوفر مساحة إبداعية للشباب لتطوير مهارات البرمجة والابتكار التكنولوجي.

- محور الاستدامة وكفاءة الاستثمار: حيث تسعى قطر إلى ضمان استثمارات مستدامة وحلول تقنية ذات جدوى. يتضمن ذلك إشراك القطاع الخاص في تنفيذ المشاريع، وتبني حلول تشاركية على مستوى الحكومة مثل منصات وخدمات مشتركة بين الجهات لتجنب الازدواجية. كما يشمل تحسين ممارسات المشتريات الحكومية في مجال تقنية المعلومات للحصول على أفضل العروض التقنية والمالية.

هذه المحاور الستة تشكل الإطار العام الذي توزعت ضمنه 29 مشروعًا رئيسيًا وضعتها قطر كخطة عمل تهدف إلى إيصالها إلى المراتب العليا عالميًا في الحكومة الإلكترونية بحلول 2030. ومن خلال هذه المشاريع، تعمل الدولة على بناء حكومة رقمية متكاملة توفر خدمات فعالة وسهلة الوصول، وتقيم بنية تحتية رقمية آمنة ومتقدمة، وكذلك تمكّن المجتمع رقمياً ليكون شريكاً فاعلاً في الاقتصاد الرقمي.

5. أبرز المشاريع والمبادرات

شهدت مسيرة حكومة قطر الرقمية إطلاق العديد من المشاريع والمبادرات التي تركت أثرًا ملموسًا في المجتمع والاقتصاد. نذكر فيما يلي بعض الأمثلة البارزة على هذه المشاريع:

- بوابة "حكومي" للخدمات الإلكترونية: وهي البوابة الرسمية للحكومة الإلكترونية في قطر ، وتعد مركزًا شاملاً يمكن من خلاله الوصول إلى مئات الخدمات الحكومية إلكترونيًا. تتيح المنصة للمستخدمين إجراء معاملات متنوعة (كالبحث عن وظيفة، تجديد الوثائق الرسمية، دفع الفواتير، وغيرها) بسهولة ومن أي مكان وعلى مدار الساعة. وقد أسهمت "حكومي" في تبسيط تجربة المستخدم عبر الحكومة وجعلها أكثر تكاملاً.

- تطبيقات الخدمات الحكومية الذكية: تبنّت الدوائر الحكومية المختلفة تطبيقات للهواتف الذكية لتقديم خدماتها. مثال على ذلك تطبيق "مطراش 2" التابع لوزارة الداخلية، والذي يمكّن المستخدمين من إنجاز العشرات من الخدمات المرورية وخدمات الإقامات والجوازات عبر الهاتف بسهولة. هناك أيضًا تطبيقات مثل "صحتك" للخدمات الصحية و"عون" لخدمات البلدية وغيرها، مما يعكس توجّه قطر نحو خدمات حكومية متنقلة وذكية.

- مشروع "استوديو 6/5": وهو حاضنة شبابية تقنية أطلقها وزارة الاتصالات وتكنولوجيا المعلومات، يستهدف تنمية مهارات البرمجة والابتكار الرقمي بين فئة الشباب. يقدم الاستوديو بيئة تعليمية إبداعية تحفّز التفكير التصميمي وتصميم الحلول التقنية. وقد تمكّن العديد من الشباب من خلال هذا المشروع من تطوير تطبيقات ومشاريع تقنية ناشئة، مما يدعم اقتصاد الابتكار في الدولة.

- مركز قطر للحاضنة الرقمية: وهو مركز يوفّر بيئة حاضنة للمشروعات الرقمية الناشئة، عبر توفير مساحات عمل ودعم فني وإرشادي وروابط مع المستثمرين. خرج من هذه الحاضنة عدد من الشركات التقنية الناشئة التي بدأت تسهم في الاقتصاد المحلي وتقديم حلول رقمية مبتكرة في السوق.
- برنامج قطر الذكية (تسمو TASMU): مبادرة وطنية تشمل تطوير حلول ذكية لمواجهة تحديات وطنية في قطاعات مثل النقل، والصحة، والبيئة، واللوجستيات. على سبيل المثال، تم تطوير منصة تحليل الأمن الغذائي الوطني ضمن برنامج تسمو لمراقبة المخزون الغذائي والتنبؤ بالاحتياجات باستخدام البيانات الضخمة. كذلك هناك منصة المجتمع الزراعي الرقمي لدعم المزارعين بالتقنية والمعلومات لتحقيق استدامة في القطاع الزراعي. تعد هذه الحلول جزءًا من توجه الحكومة لبناء مدن ذكية تستخدم البيانات والتقنيات لتعزيز جودة الحياة.

- مشروع الحكومة المفتوحة والبيانات المفتوحة: حيث أطلقت قطر بوابة البيانات المفتوحة (data.gov.qa) التي توفر مئات مجموعات البيانات الحكومية للعامة بهدف تعزيز الشفافية ودعم الابتكار القائم على البيانات. كما اعتمدت سياسة الانفتاح على المعلومات الحكومية وفق ضوابط تحمي الخصوصية، بما يمكّن الباحثين ورواد الأعمال من تطوير تطبيقات وخدمات جديدة تعتمد على البيانات الحكومية.

تعكس هذه المشاريع جانباً من جهود حكومة قطر الرقمية المتواصلة، منها ازدياد كبير في استخدام الخدمات الإلكترونية. على سبيل المثال، رصد جهاز التخطيط والإحصاء ارتفاعًا بنسبة 202.4% في معاملات الحكومة الإلكترونية خلال سنة واحدة فقط، مما يدل على إقبال الجمهور على المنصات الرقمية بدل الطرق التقليدية. كذلك تحتل قطر اليوم مراكز متقدمة عربيًا في مؤشر الخدمات الإلكترونية ومؤشر البنية التحتية للاتصالات، حيث جاءت الخامسة عالميًا في مؤشر البنية التحتية 2024 نتيجة الاستثمارات الضخمة في شبكات النطاق العريض والاتصالات. ومع استمرار تنفيذ الأجندة الرقمية 2030 بخطوات ثابتة، يُتوقع أن تحقق قطر مزيدًا من التحسين في مؤشراتها الدولية، خاصة مع التركيز على بناء حكومة رقمية متكاملة وآمنة وسهلة الوصول لجميع فئات المجتمع.

ثانياً: استراتيجيات التحول الرقمي للأجهزة العليا للرقابة المالية والمحاسبة

1. التحول الرقمي في ديوان المحاسبة القطري

كجهاز أعلى للرقابة المالية والمحاسبة في دولة قطر، يتولى ديوان المحاسبة دوراً حيوياً في ضمان الشفافية وحسن إدارة المال العام. وقد أدرك الديوان أنه لكي يواصل أداء مهامه بكفاءة عالية في عصر الثورة الرقمية، فلا بد من تبني استراتيجيات للتحول الرقمي داخل المؤسسة. لهذا، بدأ ديوان المحاسبة القطري خلال السنوات الأخيرة تنفيذ خطة شاملة للتحول الرقمي في أساليب العمل الرقابي والتدقيقي.

إحدى ركائز هذه الاستراتيجية هي أتمتة عمليات التدقيق وتحديث أدوات وأساليب العمل. يعمل الديوان على تطوير منصة إلكترونية متكاملة لإدارة عمليات التدقيق، بحيث تسمح هذه المنصة للمدققين بتنفيذ مراحل التخطيط وجمع الأدلة وتوثيق الملاحظات وإعداد التقارير بشكل إلكتروني سلس. ويشمل ذلك إنشاء قاعدة بيانات مركزية لجميع الجهات الخاضعة للرقابة، مما يسهل تتبع الملاحظات السابقة وتاريخ كل جهة

وتعزيز عملية المتابعة وتنفيذ التوصيات. وقد أثمر هذا التوجه عن تحقيق العديد من الإنجازات المهمة، كان أبرزها استخدام نظام "Archer" الإلكتروني في كافة إدارات التدقيق بالديوان. نظام Archer يُستخدم لإدارة وتوثيق مراحل مهام التدقيق والرقابة بشكل مركزي، ويمكّن المدققين من تخطيط المهام، تنفيذها، ومتابعة الملاحظات إلكترونيًا. كما يسمح بتجميع البيانات، إصدار التقارير، وضمان توحيد الإجراءات داخل الإدارات المختلفة. هذا النظام يُعتبر جزءًا من بنية التحول الرقمي الرقابي للديوان، ويُسهم في رفع الكفاءة وتحسين جودة العمل. وقد كشف ديوان المحاسبة في قطر عن توجه لإنشاء قاعدة بيانات إلكترونية للجهات الحكومية بهدف رقمنة المعلومات المتعلقة بالرقابة على تلك الجهات، بما يساعد على رفع كفاءة التحليل والمتابعة.

كما وضع الديوان خارطة طريق لتطبيق الذكاء الاصطناعي في التدقيق على مدى ثلاث سنوات. فبحسب تصريحات حديثة في مارس 2024، بدأ الديوان المرحلة الأولى بالتوعية والتدريب لموظفيه حول تقنيات الذكاء الاصطناعي وإمكاناتها في العمل الرقابي. تم تنظيم مؤتمر متخصص وورش عمل لشرح مفاهيم الذكاء الاصطناعي ومدى ارتباطها بمهنة التدقيق المالي. وستلي ذلك مراحل تجريبية لتطبيق حلول الذكاء الاصطناعي عمليًا في بعض مهام التدقيق، ثم تحليل الاحتياجات التقنية ووضع خطة تنفيذ شاملة. ويؤكد مسؤولو الديوان أن تبني الذكاء الاصطناعي سيكون تدريجيًا وعلى مراحل لضمان جاهزية الكوادر واستيعاب العمليات الجديدة. هذا النهج المرحلي يضمن تقليل المخاطر المرتبطة بالتغيير التكنولوجي والاستفادة القصوى من الفرص.

وقد أشار مسؤولو ديوان المحاسبة القطري إلى أن قطاع التدقيق خاضع لعملية التحول الرقمي عالميًا، وأن الذكاء الاصطناعي يعد تقنية مفصلية ستغير نمط العمل التقليدي للتدقيق. فمن خلال حلول الذكاء الاصطناعي، يمكن أتمتة جميع العمليات الروتينية للتدقيق بدرجة كبيرة، وتحليل كم هائل من البيانات بسرعة تفوق القدرات البشرية، مما يؤدي إلى تحسين دقة عمليات المراجعة وضمان كفاءة العمل. على سبيل المثال، بوسع خوارزميات التعلم الآلي فحص سجلات مالية ضخمة لاكتشاف أنماط غير عادية أو مؤشرات على هدر أو فساد مالي ربما يغفل عنها التدقيق اليدوي. كما يمكن للتقنيات الذكية أن تساعد في التنبؤ بالمخاطر المالية مستقبلاً والتعرف الاستباقي على مواطن الضعف في نظم الرقابة الداخلية لدى الجهات المشمولة بالمراجعة.

ولتأهيل الموارد البشرية لهذه النقلة، يعمل الديوان على تطوير مهارات المدققين الرقمية. إذ يؤكد مسؤولوه ضرورة أن يفهم المدققون أساسيات الذكاء الاصطناعي ويحددوا الأدوار الجديدة التي سيضطلعون بها في ظل

الأتمتة. فمن المتوقع أن يتحول دور المدقق إلى محلل ومقيم للنماذج والنتائج التي تنتجها الأنظمة الذكية، مما يتطلب وعيًا بتقنيات تحليل البيانات ومعرفة بمخاطر وفرص استخدام الذكاء الاصطناعي. ولهذا، تشمل استراتيجية الديوان برامج تدريب متخصصة لرفع الكفاءات في مجالات تحليلات البيانات وأدوات CAATs (تقنيات التدقيق بمساعدة الحاسوب) وغيرها.

علاوة على ذلك، ينسق ديوان المحاسبة القطري مع الاستراتيجية الوطنية للدولة في مجالي التحول الرقمي والذكاء الاصطناعي. فقد ناقش مؤتمر الديوان كيفية تطبيق استراتيجية قطر الوطنية للذكاء الاصطناعي في أعمال الرقابة والتدقيق. وهذا يعني أن جهود الديوان ليست بمعزل عن السياق الأوسع؛ بل هي جزء من رؤية شاملة لجعل قطر من الدول الرائدة في استخدام التكنولوجيا المتقدمة في القطاع الحكومي بما فيه قطاع الرقابة المالية والمحاسبية. ومن الجدير بالذكر أن قطر أطلقت استراتيجيتها الوطنية للذكاء الاصطناعي عام 2019 بهدف توظيف AI في القطاعات ذات الأولوية، ويبدو أن قطاع التدقيق الحكومي بات أحد تلك القطاعات التي تُستهدف لتعزيزها بالتقنية الحديثة.

2. تجارب عربية في التحول الرقمي للأجهزة الرقابية

لم يقتصر التحول الرقمي في مجال الرقابة المالية على قطر وحدها؛ فهناك العديد من الأجهزة العليا للرقابة في الدول العربية التي بدأت رحلتها نحو تبني التكنولوجيا في التدقيق. وتختلف درجة التقدم من دولة لأخرى حسب الإمكانات والموارد والتوجه الاستراتيجي لكل جهاز رقابي.

وفي سياق التعاون العربي، شهدت المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة (ARABOSAI) اهتمامًا متزايدًا بتبادل الخبرات في مجال التحول الرقمي. نظمت ARABOSAI عدة اجتماعات وورش عمل لمناقشة استراتيجيات الرقمنة في أعمال التدقيق وكيفية استفادة الأجهزة الرقابية من التقنيات الحديثة كتحليل البيانات الضخمة والذكاء الاصطناعي. كما دعت المنظمة إلى تعزيز البنية التحتية الرقمية للأجهزة الأعضاء وإنشاء وحدات داخلية متخصصة في تقنية المعلومات والتدقيق الإلكتروني. ومن المبادرات المشجعة تشكيل فرق عمل إقليمية لوضع أدلة إرشادية في مجالات مثل التدقيق الإلكتروني، وأمن المعلومات في بيئة الرقابة، وغيرها، بهدف توحيد المفاهيم ورفع قدرات الأجهزة الرقابية العربية.

الجدير بالذكر أن التوجه نحو الحكومة المفتوحة والبيانات المفتوحة في بعض الدول العربية أتاح للأجهزة الرقابية فرصة أكبر للحصول على البيانات الحكومية بسرعة وشفافية. فمثلاً، إذا نشرت حكومة ما بيانات موازناتها ومصروفاتها بشكل مفتوح على الإنترنت، يمكن لديوان المحاسبة هناك استخدام أدوات برمجية لتحليل تلك البيانات واستخراج المؤشرات التي تعينه في التدقيق. وهكذا فإن تحول الحكومات العربية رقميًا يخلق بيئة مواتية لتحديث أساليب عمل الأجهزة الرقابية نفسها.

رغم تفاوت التجارب، يمكن القول إن معظم الأجهزة العليا للرقابة في المنطقة باتت تدرك حتمية التحول الرقمي. فهي أمام تحدي مزدوج: التأقلم مع البيئة الرقمية للجهات الخاضعة لرقابتها (حيث أصبحت هذه الجهات تستخدم أنظمة مالية وإدارية إلكترونية يجب على المدقق فهمها وتقييمها)، وتحديث بيئة العمل الداخلية للجهاز الرقابي لضمان كفاءة وفعالية أنشطته. ويشمل ذلك الاستثمار في نظم إدارة الوثائق الإلكترونية، وقواعد البيانات الرقابية، وأدوات التحليل الإلكتروني، فضلًا عن التدريب المستمر للمدققين على استخدام التكنولوجيا. بعض الأجهزة العربية بدأت بالفعل في تطوير منصات شكاوى إلكترونية تمكن المواطنين من رفع بلاغات أو شكاوى حول المخالفات المالية والإدارية عبر الإنترنت للأجهزة الرقابية مباشرة، ما يعزز دور المشاركة المجتمعية في الرقابة.

3. التوجهات العالمية في التحول الرقمي للأجهزة العليا للرقابة

عالميًا، تشهد الأجهزة العليا للرقابة المالية (SAIs – Supreme Audit Institutions) موجة تحول رقمي سريعة مدفوعة بالتطور التكنولوجي المتسارع وارتفاع توقعات أصحاب المصلحة. فمع تنامي حجم البيانات الحكومية وتعقيد العمليات المالية، لم يعد النهج التقليدي في التدقيق كافيًا لتغطية المخاطر وضمان الشفافية. لذلك، تتجه SAIs حول العالم إلى الابتكار في أساليب التدقيق من خلال اعتماد التقنيات الحديثة.

أحد التوجهات الرئيسية هو استخدام تحليل البيانات الضخمة (Analytics Big Data). فالعديد من الأجهزة الرقابية الوطنية باتت تستخدم فرقًا من محللي البيانات وخبراء التقنية للعمل جنبًا إلى جنب مع المدققين التقليديين. يقوم هؤلاء بتحليل قواعد بيانات ضخمة (كبيانات الضرائب، أو الجمارك، أو سجلات الإنفاق الحكومي) لاستخراج رؤى وأنماط مهمة. هذا التحليل يمكن أن يكشف عن مخالفات أو احتيال أو هدر للمال العام بشكل أكثر فعالية مما كان ممكنًا بالطرق اليدوية. على سبيل المثال، استطاعت بعض SAIs عبر أدوات

البيانات اكتشاف معاملات شاذة في مشتريات حكومية أو تكرار غير منطقي في صرف نفقات معينة، مما أدى إلى تحقيقات أعمق وتوفير مبالغ كبيرة.

كذلك، تتبنى الأجهزة الرقابية العالمية أدوات الذكاء الاصطناعي والتعلم الآلي. فكما سبقت الإشارة، يمكن للذكاء الاصطناعي دعم التدقيق عبر الكشف التلقائي عن الشذوذ Anomaly Detection في السجلات المالية، أو تصنيف المستندات وفهرستها (مثلاً عقود، فواتير) لتسهيل مراجعتها، أو حتى مساعدة المدقق في تقييم الأداء من خلال نماذج التنبؤ. على سبيل المثال، بعض أجهزة الرقابة طوّرت روبوتات برمجية (RPA) تقوم بمراجعة مستندات كثيرة روتينية والتحقق من امتثالها للأنظمة، مما وفر آلاف ساعات العمل اليدوي وسمح للمدققين بالتركيز على الجوانب التحليلية الأعلى قيمة.

توجه آخر عالمي هو إنشاء منصات إلكترونية تفاعلية للتقارير والمتابعة. الكثير من SAIs أنشأ بوابات إلكترونية لنشر تقاريرها للجمهور بطريقة بيانات مفتوحة وتفاعلية، حيث يمكن لأي مهتم استعراض النتائج المالية والتوصيات عبر رسوم بيانية ولوحات معلومات. هذه الشفافية الرقمية تعزز من قيمة التقارير الرقابية وتجعل أثرها ممتدًا لأوسع شريحة من المجتمع. بعض الأجهزة المتقدمة قدمت كذلك تطبيقات للهواتف تتيح للمواطن تتبع تنفيذ التوصيات الإصلاحية من قبل الحكومات، مما يربط الجمهور مباشرة بعملية الرقابة والمساءلة.

على صعيد المعايير والإرشادات الدولية، أصدر الانتوساي (INTOSAI) – المنظمة الدولية للأجهزة العليا للرقابة – أدلة ومبادرات لدعم التحول الرقمي. فمثلاً، أطلقت مبادرة رقمنة عمليات التدقيق (ADOPTE) لتشجيع الأجهزة على تبني أساليب تدقيق مدعومة تقنيًا. كما طوّرت لجنة معايير الانتوساي أدلة حول التدقيق في بيئات تكنولوجيا المعلومات وأصدرت المعيار ISSAI 5300 الخاص بتقنية المعلومات. كذلك، أنشأت الانتوساي ومنظمات إقليمية مثل الأولاسيفس OLACEFS برامج لمساعدة الأجهزة الأعضاء في بناء خطط استراتيجية للتحول الرقمي وتبادل أفضل الممارسات. هذه الجهود على المستوى الدولي توفر خارطة طريق مرجعية لأي جهاز رقابي يسعى للانتقال إلى العصر الرقمي.

من التحديات التي رصدتها الدراسات العالمية أن العديد من SAIs لا تزال تتخذ نهجًا تفاعليًا بدلًا من استباقي في التحول الرقمي. بمعنى أنها تنتظر ظهور الحاجة خلال عمليات التدقيق لتبني تقنية معينة، بدلاً من التخطيط المسبق لتغيير نموذج العمل التقليدي. إلا أن هناك بعض الأجهزة "الطلائعية" التي

وضعت استراتيجيات رقمية متكاملة وجعلت التحول الرقمي جزءًا من خطتها المؤسسية الشاملة. هذه الأجهزة غالبًا ما تحظى بدعم موارد وتمويل كافٍ، ولديها قيادة عليا تؤمن بتوظيف التكنولوجيا. في المقابل، تواجه أخرى قيودًا مثل نقص التمويل أو مقاومة التغيير التنظيمي أو عدم توفر الكفاءات التقنية، مما يبطئ من عملية التحول.

بشكل عام، الملامح المشتركة للاستراتيجيات العالمية الناجحة في الرقابة الرقمية تتضمن:

- تبني إطار حوكمة تقنية داخل SAI يحدد رؤية وأهداف التحول الرقمي ومسؤوليات التنفيذ.
- الاستثمار في البنية التحتية التقنية (أجهزة، شبكات، أمن سيبراني) اللازمة لدعم التطبيقات الحديثة وتحليل البيانات.
- بناء القدرات البشرية عبر التدريب والتوظيف لمختصي تحليل بيانات وتقنية معلومات للعمل جنبًا إلى جنب مع المدققين الماليين.
- تحديث السياسات والإجراءات الداخلية لاستيعاب العمليات الرقمية، مثلاً إجراءات جمع الأدلة إلكترونياً، وحماية البيانات، والتوقيع الإلكتروني على التقارير.
- تعزيز التعاون مع الأطراف ذات الصلة: مثل التعاون مع إدارات تقنية المعلومات في الجهات الخاضعة للرقابة لفهم أنظمتها، والتنسيق مع هيئات مكافحة الفساد، وكذلك الانفتاح على الجمهور عبر التكنولوجيا لتعزيز المشاركة والمساءلة.

يمكننا القول إن التحول الرقمي لم يعد خيارًا كماليًا للأجهزة العليا للرقابة، بل هو ضرورة تمليها البيئة الحديثة. فمن أجل الاستمرار في أداء دورها كمراقب أمين على المال العام وتحقيق قيمة مضافة حقيقية، يجب أن تكون الأجهزة الرقابية قادرة على العمل بكفاءة وسرعة في بيئة رقمية تتدفق فيها المعلومات بشكل لحظي. والأجهزة التي نجحت في ذلك بدأت ترى فوائد ملموسة مثل تحسين جودة عمليات التدقيق ومخرجاته، وتقليص الوقت اللازم لإصدار التقارير، ورفع قيمة التوصيات المقدمة بفضل رؤى أعمق قائمة على البيانات.

4. المعايير والممارسات الدولية ذات الصلة

في سياق تبني استراتيجيات التحول الرقمي، تسترشد الأجهزة العليا للرقابة بالعديد من الأطر والمعايير الدولية في مجال تقنية المعلومات وأمنها، لضمان اتباع أفضل الممارسات وضبط الجودة في بيئة العمل الرقمي. من أبرز تلك الأطر والممارسات:

- إطار COBIT لحوكمة تقنية المعلومات: يعد إطار «كوبيت» COBIT (اختصارًا لـ Control Objectives for Information and Related Technologies) إطار حوكمة تقنية معلومات معترف به دوليًا. يوفر COBIT مجموعة من المبادئ والأدوات لإدارة وضبط استخدام تقنية المعلومات في المؤسسات بهدف مواءمة التقنية مع أهداف العمل وتحقيق قيمة مضافة. يُعرّف COBIT بأنه إطار يساعد المؤسسات على تحسين أداء الأعمال عبر استخدام متوازن لتكنولوجيا المعلومات مع تقليل المخاطر المحتملة المرتبطة بها. بالنسبة للأجهزة الرقابية، يشكل COBIT مرجعية هامة عند تدقيق نظم تقنية المعلومات في الجهات الحكومية، حيث يغطي مجالات متعددة من حوكمة وأمن وإدارة الموارد التقنية. كما يمكن للجهاز الرقابي نفسه تطبيق مبادئ COBIT لضبط عمليات التقنية الداخلية لديه – كتطوير سياسات تقنية المعلومات، وإدارة التغييرات، ومراقبة خدمات تقنية المعلومات – لضمان أن التحول الرقمي يسير وفق ضوابط مؤسسية رصينة.

- معيار ISO/IEC 27001 لنظم إدارة أمن المعلومات: هو المعيار الدولي الأشهر في أمن المعلومات (صدر عن المنظمة الدولية للتقييس ISO واللجنة الكهروتقنية الدولية IEC). يحدد هذا المعيار متطلبات إنشاء نظام إدارة أمن المعلومات (ISMS) داخل المنظمة. والالتزام به يعني أن المؤسسة تتبع نهجًا منهجيًا في تقييم المخاطر الأمنية ووضع ضوابط لحماية سرية المعلومات وسلامتها وتوفرها. بالنسبة للأجهزة العليا للرقابة، تكمن أهمية ISO 27001 في نقطتين: الأولى كمرجعية عند تدقيق أمن المعلومات في المؤسسات الحكومية والشركات التي تقوم بتدقيقها، حيث يُعد امتثال تلك الجهات للمعيار مؤشرًا إيجابيًا على نضج ممارساتها الأمنية. والثانية كدليل لتأمين البيئة الرقمية الداخلية للجهاز الرقابي ذاته، خاصة مع الانتقال لاستخدام البيانات الإلكترونية والحوسبة السحابية. فتطبيق الديوان للمعيار ISO 27001 أو حصوله على شهادة الامتثال له يعني أنه يتبع أفضل الممارسات العالمية في حماية بيانات عمليات التدقيق وحفظ السرية والخصوصية.

- إطار NIST للامن السيبراني: هو إطار أصدره المعهد الوطني للمعايير والتقنية في الولايات المتحدة (NIST)، وهو نهج شامل قائم على إدارة المخاطر لتعزيز الأمن السيبراني. يتميز إطار NIST بتقسيمه عملية إدارة الأمن إلى 5 وظائف أساسية: التعريف (Identify)، الحماية (Protect)، الكشف (Detect)، الاستجابة (Respond)، والتعافي (Recover). وقد لاقى هذا الإطار اعتمادًا واسعًا عالميًا كمرجع لبناء استراتيجيات الأمن السيبراني في المؤسسات. يمكن للأجهزة العليا للرقابة الاستفادة من إطار NIST بوصفه دليلًا عند مراجعة الوضع الأمني السيبراني للجهات الحكومية:

فمثلاً يمكن تقييم مدى قيام جهة ما بتحديد أصولها الحيوية وتقييم المخاطر (Identify)، أو مدى فعالية ضوابط الحماية لديها كإدارة الوصول والتشفير (Protect)، وكذلك قدراتها على رصد الحوادث (Detect) والتعامل معها (Respond) والتعافي منها (Recover). كما يفيد إطار NIST الجهاز الرقابي نفسه لضمان حماية البنية التحتية الرقمية التي يعتمد عليها في أداء مهامه، خاصة وأن البيانات الرقابية شديدة الحساسية وتحتاج لإجراءات صارمة ضد أي اختراق أو هجوم سيبراني.

- معيار PCI DSS لأمان بيانات بطاقات الدفع: هو معيار أمني متخصص يُعنى بحماية بيانات بطاقات الائتمان والخصم (Debit/Credit Cards). نشأ هذا المعيار عن مجلس أمن صناعة بطاقات الدفع (Security Standards Council PCI) ويضع مجموعة من متطلبات الأمن الواجب اتباعها من قبل أي منظمة تتعامل مع بيانات البطاقات، كالمتاجر الإلكترونية أو الجهات التي تستلم مدفوعات إلكترونية. تتضمن هذه المتطلبات مثلاً تشفير بيانات البطاقة، وضبط الوصول إلى أنظمة معالجة المدفوعات، ومراقبة الشبكات التي تنقل بيانات البطاقات وغيرها. أهمية PCI DSS للأجهزة العليا للرقابة تظهر عند تدقيق الجهات الحكومية التي تقبل مدفوعات إلكترونية – مثل بوابات الدفع للخدمات الحكومية أو هيئات الجمارك والضرائب التي تستلم الرسوم عبر البطاقات. إذ يُتوقع من تلك الجهات الامتثال لمعيار PCI DSS لضمان بيئة مدفوعات آمنة، ويمكن للديوان أن يُضمّن في برنامجه التدقيقي التحقق من مستوى الامتثال وتطبيق الضوابط المنصوص عليها في المعيار. كذلك بعض الأجهزة الرقابية التي ربما تعالج بيانات مالية للمواطنين (في حال كان لديها بوابات شكاوى مالية أو نحو ذلك) قد تهتم بتطبيق أجزاء من PCI DSS لضمان عدم تسرب أي بيانات دفع حساسة عبر منصاتها.

إضافة إلى ما سبق، هناك معايير وأطر أخرى قد تكون ذات صلة مثل إطار ITIL لإدارة خدمات تقنية المعلومات، ومعايير التدقيق على نظم المعلومات الصادرة عن ISACA (مثل معايير CISA)، وكذلك إطار COSO لإدارة المخاطر والرقابة الداخلية الذي يستخدم أيضًا في تقييم بيئة الرقابة الإلكترونية. الهدف من الاهتمام بهذه المعايير هو التأكد من أن التحول الرقمي يسير وفق ضوابط ومعايير عالمية تضمن الجودة وتقلل المخاطر. فعندما يواكب الجهاز الرقابي أفضل الممارسات الدولية، يكتسب ثقة أكبر في نتائج عمليات المراجعة، ويكون قادرًا على مساعدة الجهات الخاضعة للرقابة في تحسين أنظمتها بإعطائها توصيات تستند إلى معايير معترف بها.

ثالثاً: تطبيق الحكومة الذكية في الأجهزة العليا للرقابة

1. برامج ديوان المحاسبة

ضمن جهود ديوان المحاسبة القطري لتطبيق مبادرات الحكومة الذكية في مجال الرقابة المالية، تبنّى الديوان نظام Archer الإلكتروني لإدارة عمليات التدقيق. يوفر هذا النظام منصة موحّدة وشاملة تُغطي جميع مراحل عملية المراجعة والتدقيق داخل الديوان. وقد مكّن Archer فرق التدقيق في الديوان من تنظيم مهامهم بكفاءة أكبر عبر تخطيط مهام التدقيق وجدولتها، وتوثيق الملاحظات والنتائج أثناء العمل الميداني، ومتابعة توصيات التدقيق لضمان تنفيذها من قبل الجهات الخاضعة للرقابة، إضافة إلى توحيد إجراءات العمل واتباع منهجية موحدة عبر كافة الإدارات الرقابية. هذا التوحيد ساهم في رفع مستوى الاتساق والجودة في عمليات التدقيق، حيث أصبحت فرق المراجعة تعمل وفق أفضل الممارسات القياسية ضمن نظام واحد شامل. كما يساعد النظام على الحفاظ على سجل تدقيق إلكتروني مركزي لكل مهمة، مما يُسهّل تتبّع الملاحظات من مرحلة التخطيط وحتى إنجاز التقارير النهائية والتوصيات. وبذلك، عزز ديوان المحاسبة حوكمة إجراءات التدقيق من خلال منصة Archer التي تربط جميع جوانب عملية المراجعة في بيئة رقمية موثوقة.

يعتمد ديوان المحاسبة كذلك على برمجيات متقدمة لتحليل البيانات بهدف دعم عملية التدقيق واكتشاف الأنماط غير المعتادة في البيانات المالية والإدارية. تتيح أدوات تحليل البيانات فحص كميات ضخمة من السجلات والمعاملات لاستخراج المؤشرات الشاذة أو الحالات الشاذة التي قد تدل على أخطاء أو تجاوزات. فعلى سبيل المثال، يمكن للنظام تحديد حالات عدم الاتساق أو الانحراف عن المعدلات الطبيعية في الإنفاق أو الإيرادات بشكل سريع ودقيق. يساعد هذا التحليل المُعمّق المدققين على تركيز جهودهم على المناطق عالية الخطورة، والتعرّف المبكر على أي اختلالات أو مخالفات مالية محتملة. وقد أكد مسؤولون في الديوان أن استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة سيُحدث نقلة نوعية في كفاءة وفعالية العمل الرقابي، حيث يُساهم في تحديد الأخطاء بسرعة ودقة أعلى، ويُمكّن من تقييم المخاطر بقدر أكبر من الشمولية. علاوة على ذلك، تدعم هذه الأدوات عملية صياغة الملاحظات والتوصيات بشكل علمي ومدروس استنادًا إلى الأدلة الرقمية المكتشفة، مما يعزّز مصداقية ودقة التقارير الرقابية النهائية.

أدت هذه البرامج الرقمية إلى أتمتة العديد من عمليات التدقيق التي كانت تُنجز يدويًا في الماضي. بفضل منصة Archer والتطبيقات المساندة لها، تم أتمتة إجراءات مثل جمع البيانات وإعداد أوراق العمل ومتابعة مهام المراجعة، بحيث تتم هذه الخطوات بصورة تلقائية أو شبه تلقائية داخل النظام. هذا النهج قلّل من العمل

الروتيني المكرر ومن الحاجة إلى إدخال البيانات عدة مرات في أنظمة مختلفة، مما ساهم في تقليل نسبة الأخطاء البشرية الناتجة عن التكرار. على سبيل المثال، المعلومات المالية التي تدخل النظام مرة واحدة يمكن لجميع الفرق استخدامها دون حاجة لإعادة نسخها، مما يقضي على الازدواجية في الجهود. كما أن التكامل بين وظائف التخطيط والتوثيق والتقرير داخل منصة واحدة يعني عدم تكرار نفس العمل في مراحل متعددة. ونتيجةً لذلك، تمكن الديوان من تسريع إنجاز عمليات التدقيق وتوفير الوقت والموارد، حيث أصبحت التقارير تصدر في وقت أقصر وبدقة أعلى. إلى جانب السرعة، انعكست الأتمتة إيجابًا على جودة نتائج التدقيق؛ فالإجراءات الموحدة والرقابة الآلية أدت إلى رفع كفاءة وفعالية عملية التدقيق بشكل عام. وتعزّز هذه التحسينات الثقة في مخرجات التدقيق، سواء لدى الجهات الخاضعة للرقابة أو أصحاب القرار، نظرًا لشفافية العمليات ودقة النتائج في ظل منظومة تدقيق ذكية وشاملة.

يتميز نهج ديوان المحاسبة الرقمي أيضًا بتحقيق تكامل عالٍ بين مختلف أدوات وأنظمة التدقيق، مما أسهم في تسهيل العمل الجماعي ضمن بيئة رقمية متكاملة. إن منصة Archer نفسها جزء من منظومة أوسع لدى الديوان، حيث ترتبط بأنظمة أخرى مثل نظام مشاركة الملفات والمراسلات الإلكترونية المستخدم لتبادل المستندات والتقارير بين المدققين والجهات الخاضعة للرقابة. هذا التكامل يضمن تدفق المعلومات بسلاسة بين فرق العمل، فمثلاً يتم إرسال الملاحظات والتقارير ومتابعة الردود عبر نظام إلكتروني موحّد بدلًا من الطرق التقليدية الورقية أو المنفصلة. كما تسمح المنصة لعدة مدققين بالعمل بشكل تعاوني ومتزامن على نفس المهمة، مع إمكانية الوصول الفوري إلى آخر التحديثات والمستندات المتعلقة بالتدقيق. وقد أدى ذلك إلى تعزيز التنسيق والتواصل داخل فرق التدقيق، حيث يمكن لكل عضو الاطلاع على مخرجات زملائه وإضافة تعقيباته في ذات البيئة الرقمية. إضافةً إلى ذلك، يتيح التكامل مع أدوات تحليل البيانات أن تُدرج نتائج التحليلات مباشرةً في عملية التدقيق دون عوائق، مما يربط بين الرؤى التحليلية وإجراءات المراجعة الفعلية. كما يستخدم الديوان نظام Kiteworks لتبادل الملفات والمستندات مع الجهات الخاضعة للرقابة، ويوفر بيئة رقمية مشفّرة تضمن حماية البيانات الرقابية الحساسة عند إرسالها أو استلامها. يُسهم النظام في تقليل المعاملات الورقية، تسريع التواصل، وتعزيز الشفافية من خلال تتبع عمليات التبادل بدقة. ويأتي هذا ضمن توجه الديوان لتعزيز التحول الرقمي الكامل وتوفير بنية تواصل آمنة وفعالة، تواكب متطلبات الحكومة الذكية.

2. استراتيجية الذكاء الاصطناعي في أعمال الرقابة

كما أسلفنا، الذكاء الاصطناعي (AI) يمثل أحد أبرز مجالات الحكومة الذكية وأكثرها تأثيراً في مستقبل التدقيق والرقابة. إن استراتيجية تبني الذكاء الاصطناعي داخل الأجهزة العليا للرقابة باتت ملامحها تتشكل في العديد من الدول، وتهدف هذه الاستراتيجيات إلى إعادة ابتكار وظيفة التدقيق بالاستفادة القصوى من قدرات AI.

في قطر، أطلق ديوان المحاسبة بالفعل مبادرة لإدخال الذكاء الاصطناعي في العمل الرقابي على مراحل. وقد وُضعت رؤية واضحة لهذه الاستراتيجية تتضمن رفع وعي المدققين بالذكاء الاصطناعي كخطوة أولى، ثم تحديد مجالات التطبيق المناسبة، يليها التطوير والتنفيذ وأخيرًا التقييم المستمر. من الأمثلة على تطبيقات محتملة ضمن هذه الاستراتيجية:

- المراجعة الذكية للبيانات المالية: عبر خوارزميات تعلم الآلة التي يمكن أن تتعلم من بيانات سنوات سابقة لتحديد ما يعتبر نمطًا "طبيعيًا" لمصروفات جهة معينة، ثم إبراز الحالات الشاذة عن هذا النمط في السنة الحالية لتحليلها. هذا يساعد المدقق في توجيه الانتباه بسرعة إلى بؤر الخطر دون الغوص يدوياً في آلاف السطور من جداول البيانات.

- التدقيق التنبئي: استخدام تقنيات التعلم الآلي التنبئي للتعرّف على المؤشرات المبكرة لمشكلات محتملة. على سبيل المثال، قد تُطوَّر نماذج تنبؤية تتوقع احتمال تعثر مشروع حكومي معين أو تجاوز تكلفته للميزانية المخصصة بناءً على خصائص ذلك المشروع ومقارنته ببيانات مشاريع سابقة. هذه التنبؤات تساعد المدقق على تركيز التدقيق على المشاريع ذات الاحتمال الأعلى للمشاكل وبالتالي تقديم توصيات استباقية.

- مساعد مدقق افتراضي: حيث يمكن لتقنيات معالجة اللغة الطبيعية (NLP) أن تنشئ نظامًا يقرأ التقارير المالية والتدقيقية الضخمة ويرخّص أهم المعلومات للمدقق. بل ويمكن أن يجيب هذا المساعد الافتراضي على أسئلة يطرحها المدقق بلغة طبيعية، مثل: "ما كانت أبرز ثلاث مخالفات مالية في وزارة الصحة آخر 5 سنوات؟" مستنداً إلى قاعدة بيانات التقارير السابقة. مثل هذا النظام يختصر الوقت في البحث اليدوي ويضمن عدم إغفال معلومات مهمة.

- اكتشاف الاحتيال الإلكتروني: مع زيادة المعاملات عبر الإنترنت وأنظمة الدفع الرقمية، أصبح الاحتيال الإلكتروني تحديًا. الذكاء الاصطناعي يوفر أدوات قوية لاكتشاف أنماط الاحتيال (كعمليات

الدفع المشبوهة، أو التحايل في أنظمة المناقصات الإلكترونية). يمكن برمجة خوارزميات للتعلم من حالات احتيال معروفة ثم تطبيقها على البيانات الجارية في الأنظمة الحكومية لتنبيه المدقق عند حدوث نشاط مشابه. بعض أجهزة الرقابة الغربية تستخدم بالفعل أنظمة ذكاء اصطناعي تراقب الإنفاق باستخدام البطاقات الحكومية أو نظم المشتريات العامة وتنبه على الفور عند وقوع عملية خارج السياق المعتاد (كشراء كميات غير اعتيادية، أو تجزئة طلبات الشراء بطريقة مريبة).

- تحسين جودة التدقيق وأداء المدققين: عبر استخدام الذكاء الاصطناعي في تحليل أداء فرق التدقيق أنفسهم. مثلاً تحليل كم الوقت المستغرق في كل مرحلة من مراحل التدقيق، واستخدام التقنيات الذكية لتحديد نقاط الاختناق (bottlenecks) في العملية وإيجاد حلول لها. أو تحليل تقارير التدقيق الصادرة تلقائيًا بحثًا عن جودة صياغة التوصيات واتساقها مع الأدلة، بحيث يُنبه المدقق أو المشرف عند وجود فجوات. هذا جانب إداري/تشغيلي لكنه مهم لضمان أن الذكاء الاصطناعي لا يخدم فقط التدقيق على الجهات الخارجية بل أيضًا يطور العمل الداخلي للجهاز الرقابي.

رابعاً: التحديات التي تواجه التحول الرقمي والحكومة الذكية

1. التحول الرقمي والمواطنة الرقمية

يمثل التحول الرقمي في الحكومات نقلة نوعية في طريقة تقديم الخدمات العامة وإدارة العلاقة بين الدولة والمواطن. فبدلاً من الإجراءات التقليدية البيروقراطية، تتيح التكنولوجيا الحديثة خدمات أسرع، أكثر دقة، وشمولًا. غير أن نجاح هذه النقلة مرهون بتحقيق ما يُعرف بـ"المواطنة الرقمية"، والتي تتجلى في قدرة الأفراد على التفاعل مع الدولة من خلال الوسائل الرقمية، واستخدام الخدمات الإلكترونية بوعي وأمان.
في قطر، أدى التركيز الحكومي على تطوير الخدمات الإلكترونية إلى توسيع نطاق المواطنة الرقمية – أي قدرة المواطنين على الوصول للخدمات والمشاركة الرقمية بأمان وفعالية. أطلقت قطر بوابة الحكومة الإلكترونية "حكومي" التي توفر أكثر من 1,400 خدمة رقمية، يُمكن إنجاز 650+ منها بالكامل عبر الإنترنت للمواطنين والمقيمين والزوار. وقد أثمر ذلك عن ارتفاع معدل استخدام الخدمات الإلكترونية ورضا المستخدمين؛ إذ تم رقمنة نحو 71% من الخدمات الحكومية في قطر وتحقيق معدل رضا للمستخدمين بلغ 74% بحسب بيانات بوابة حكومي 2024. هذه الأرقام تعكس تقدمًا مهمًا، لكنها تكشف أيضًا تحديات في إشراك كافة فئات المجتمع رقمياً. فعلى الرغم من أن قطر تتمتع بانتشار واسع للإنترنت والهواتف

الذكية، يبقى تحدي رفع وعي كبار السن وبعض الفئات الأقل دراية رقمياً قائمًا لضمان عدم ترك أي شريحة خارج التحول الرقمي. وقد بدأت قطر بمعالجة ذلك عبر برامج توعية ومناهج تعليمية تشمل الثقافة الرقمية والأمان الإلكتروني في المدارس والمجتمع. تؤكد وزارة الاتصالات وتكنولوجيا المعلومات في قطر على أن تعزيز الثقافة الرقمية لدى جميع الشرائح إلى جانب الاهتمام بالأمن السيبراني يضمن مشاركة آمنة وشاملة في المنصات الرقمية، مما يرسخ بيئة رقمية أكثر شمولًا للجميع.

إقليميًا، يشهد العالم العربي تفاوتًا في مستوى النضج الرقمي للمواطنين، حيث قطعت بعض الدول شوطًا كبيرًا في تحسين الشمول الرقمي، بينما لا تزال أخرى تعاني من ضعف البنية التحتية وتدني الوصول إلى الإنترنت في المناطق الريفية. عالميًا، تُظهر تقارير الاتحاد الدولي للاتصالات أن حوالي 33% من سكان العالم لا يزالون خارج البيئة الرقمية، ما يجعل المواطنة الرقمية تحديًا دوليًا يتطلب تعاونًا وسياسات شاملة تدمج التعليم، التوعية، وإتاحة التكنولوجيا.

2. الاستثمار في التعليم والتدريب

تظهر التجربة القطرية أن تنمية رأس المال البشري هي حجر الزاوية للتحول الرقمي الناجح. لذلك استثمرت قطر بقوة في التعليم والتدريب التقني لبناء كوادر وطنية قادرة على قيادة برامج التحول الرقمي. أطلقت برنامج التدريب الحكومي الرقمي وأكاديمية قطر الرقمية (QDGTP) الذي يهدف إلى بناء قدرات استثنائية في مجال تكنولوجيا المعلومات والاتصالات لدى موظفي القطاع الحكومي. وضع البرنامج هدفًا طموحًا بتدريب 1,000 موظف حكومي سنويًا وحصول 250 منهم على شهادات احترافية دولية كل عام. وقد حقق البرنامج في مراحله الأولى نتائج لافتة، حيث قدّم 1,053 دورة تدريبية متخصصة وفّر خلالها 15,000 مقعدًا تدريبيًا، ونال 1,506 متدرب شهادات دولية معتمدة. توسع نطاق التدريب ليشمل 86 جهة حكومية في مرحلته الثانية، وتم حتى الآن تأهيل 633 موهبة قطرية عبر أكاديمية قطر الرقمية التي انطلقت عام 2024. هذه الاستثمارات تعكس إدراك قطر بأن مواكبة التطور التكنولوجي المتسارع يتطلب تطويرًا مستمرًا لمهارات الموظفين وإعادة صقلها. كما أنشأت قطر مراكز ابتكار وحاضنات تقنية (مثل مركز حاضنة الأعمال الرقمية وبرامج بالتعاون مع شركات تقنية كبرى) لتزويد الشباب ورواد الأعمال بالخبرات العملية في مجالات كالذكاء الاصطناعي وتحليل البيانات، بما يعزز كوادر المستقبل الرقمية.

غير أن التحدي الأبرز في هذا المجال لا يقتصر على التدريب فقط، بل يشمل أيضًا الفجوة بين مخرجات التعليم التقليدي ومتطلبات العصر الرقمي. ففي دول عديدة، لا تزال المناهج الجامعية بعيدة عن التطورات التقنية الحديثة مثل الذكاء الاصطناعي وتحليل البيانات الضخمة، مما يتطلب إصلاحات تعليمية هيكلية.

عالميًا، تؤكد تقارير منظمة التعاون الاقتصادي والتنمية (OECD) أن ملايين الوظائف مهددة بالزوال إذا لم يتم تأهيل العاملين لمهارات المستقبل. بات الاستثمار المستمر في التعليم والتدريب والتأهيل ضرورة استراتيجية لكل دولة تطمح للانتقال إلى حكومة ذكية، بحيث تضمن وجود العقول والخبرات القادرة على تصميم وتنفيذ وإدارة التحول الرقمي بكفاءة.

3. الأمن السيبراني وحماية البيانات

مع تزايد اعتماد الحكومات على الأنظمة الرقمية والبيانات الضخمة، برز الأمن السيبراني وحماية البيانات كتحدٍ مصيري يجب معالجته ضمن جهود التحول الرقمي. في قطر، اتُخذت خطوات حثيثة لتعزيز أمن المعلومات والبنى التحتية الحيوية وحماية خصوصية الأفراد. فقد أنشأت الدولة الوكالة الوطنية للأمن السيبراني (NCSA) عام 2021 لتكون الجهة المختصة بوضع السياسات والمعايير الأمنية على المستوى الوطني. وتتكامل هذه الخطوة مع إطار تشريعي قوي؛ حيث كانت قطر سبّاقة إقليميًا في سنّ قانون لحماية البيانات الشخصية (القانون رقم 13 لسنة 2016) الذي يعد أول قانون من نوعه في الشرق الأوسط، متوافق في مبادئه مع اللائحة الأوروبية العامة لحماية البيانات (GDPR). كما أصدر المشرّع القطري قانونًا لمكافحة الجرائم الإلكترونية سنة 2014 يجرّم الاختراق وسرقة الهوية والاحتيال الإلكتروني. وتماشياً مع أفضل الممارسات الدولية، تبنت قطر معايير الأيزو 27001 لنظم إدارة أمن المعلومات ضمن العديد من الهيئات الحكومية والبنوك لضمان تطبيق ضوابط صارمة لحماية البيانات. إضافة لذلك، أطلقت قطر الإستراتيجية الوطنية للأمن السيبراني (أولها في 2014 وتحديث جديد في 2024) لتعزيز قدرات الكشف والاستجابة للهجمات، وإنشاء مراكز عمليات أمنية على مستوى الدولة.

هذه الخطوات جاءت نتيجة لتصاعد حجم التهديدات السيبرانية، خاصة مع استضافة الدولة فعاليات عالمية مثل كأس العالم، والتي شكّلت بيئة مستهدفة للهجمات الإلكترونية. لذلك، كثفت قطر من جهود التدريب، وأطلقت مراكز عمليات أمنية رقمية ترصد التهديدات على مدار الساعة.

وعلى الصعيد العالمي، لا يختلف المشهد كثيرًا من حيث ارتفاع وتيرة الهجمات وتعاظم تحديات حماية البيانات. فقد شهد العالم سلسلة من الهجمات السيبرانية البارزة التي طالت مؤسسات حكومية في دول متقدمة ونامية على حد سواء – من اختراق نظم مدن ذكية وشبكات كهرباء، إلى هجمات برامج الفدية التي عطلت مرافق صحية وتعليمية. ووفق تقرير مخاطر الأمن المعلوماتي 2023 الصادر عن إحدى شركات التأمين العالمية، فإن قطاع الحكومة يأتي ضمن القطاعات الأكثر تضررًا من خروقات البيانات، بمتوسط تكلفة عالمي للخرق يبلغ نحو 5$ ملايين. من جهة أخرى، استجابت الحكومات عبر سن تشريعات لتعزيز الخصوصية وحماية البيانات الشخصية. فبحلول 2025، كان لدى أكثر من 150 دولة حول العالم قوانين لحماية البيانات على غرار الـGDPR في الاتحاد الأوروبي. كما تتبنى معظم الحكومات معايير أمن معلومات دولية (ISO 27001، إطار NIST الأميركي، إلخ) لتكون جزءًا من نظمها الداخلية. ومع ذلك، تظل القدرات الدفاعية متفاوتة، مما يستلزم تعاونًا دوليًا أوثق لتبادل المعلومات عن التهديدات وبناء قدرات الدول الأقل تطورًا تقنيًا. في المجمل، يمثل الأمن السيبراني وحماية البيانات تحديًا عالميًا مشتركا لا غنى عن معالجته لضمان نجاح واستدامة التحول الرقمي والحكومة الذكية.

خامساً: دور الرقابة في التحول الرقمي والحوكمة الذكية

1. ضمان الامتثال للقوانين والمعايير القياسية

تلعب أجهزة الرقابة والتنظيم دور الضامن لالتزام الجهات الحكومية بالمعايير القانونية والفنية الضرورية للتحول الرقمي السليم. في قطر، هناك حرص على الامتثال للمعايير العالمية والمحلية على حد سواء. فعلى صعيد حماية البيانات الشخصية، تُلزم هيئات الرقابة (مثل مكتب حماية البيانات في مركز قطر المالي والجهات التنظيمية الحكومية) المؤسساتِ بتطبيق مبادئ القانون رقم 13 لعام 2016 والتشريعات ذات الصلة، والتي تتماشى إلى حد كبير مع اشتراطات اللائحة الأوروبية GDPR. وقد شهدنا كما أسلفنا قيام الجهات الرقابية بفرض عقوبات في حالات خرق تلك القوانين. أيضًا، تفرض قطر على الهيئات الحكومية الكبرى التقيد بإجراءات ضمان جودة الخدمات الإلكترونية وفق معايير مثل ISO/IEC 27001 لنظم أمن المعلومات وISO 20000 لإدارة خدمات تقنية المعلومات. وكثيرًا ما يستعين ديوان المحاسبة وغيره من أجهزة التدقيق في قطر بأطر عمل دولية مثل إطار حوكمة تقنية المعلومات COBIT للتأكد من أن نظم المعلومات الحكومية تدار بكفاءة وأمان وتتوافق مع الأهداف الاستراتيجية. ويُذكر أن ديوان

المحاسبة القطري عضو في المجموعة الدولية للأجهزة العليا للرقابة المالية (الإنتوساي) وتحديدًا في الفريق العامل المعني بتدقيق تكنولوجيا المعلومات (WGITA)، مما يتيح له تبادل أفضل الممارسات مع نظرائه عالمياً في مجال معايير رقابة تقنية المعلومات. مثل هذا التعاون الدولي يساعد على تحديث منهجيات الرقابة باستمرار وفق أحدث المعايير. على سبيل المثال، يوفر إطار COBIT إرشادات واضحة لتقييم حوكمة تقنية المعلومات تشمل مواءمة عمليات تقنية المعلومات مع أهداف المؤسسة، والتحقق من الامتثال التنظيمي، وضمان كفاءة وأمن العمليات التقنية. توظيف هذه المعايير يجعل عمليات التدقيق أكثر شمولاً، فلا تقتصر على فحص الضوابط فحسب، بل تقيّم أيضًا الأداء وإدارة المخاطر والتحسين المستمر. وبذلك، تساهم الرقابة في قطر في التأكد من أن مشاريع التحول الرقمي تنفذ ضمن ضوابط الحوكمة الرشيدة وبما يتفق مع التشريعات والقواعد الفنية المعتمدة محليًا ودوليًا.

فدور الرقابة في ضمان الامتثال ليس مجرد تدقيق شكلي، بل هو عنصر جوهري لضبط مسار التحول الرقمي ضمن حدود القانون والمعايير المعتمدة، بما يكفل الثقة والاستدامة للمبادرات الرقمية. كما تساهم الرقابة في فرض التزام تعاقدي وتقني في المشتريات الرقمية، مما يحمي المال العام.

2. التقييم المستمر للأداء والمخاطر

يتطلب عالم التكنولوجيا سريع التطور أن تتبنى الحكومات نهجًا مستمرًا في تقييم أداء مشاريعها الرقمية وإدارة المخاطر المرافقة. تقوم أجهزة الرقابة في قطر بدور فاعل في هذا الشأن عبر عمليات مراجعة دورية مرحلية لمؤشرات أداء الخدمات الإلكترونية والمشاريع التقنية الكبرى. فعلى سبيل المثال، عند تنفيذ مشروع منصة رقمية جديدة، قد يشترط ديوان المحاسبة القطري إجراء تقييمات فصلية لمدى تحقيق المنصة لأهدافها الخدمية وكفاءتها التشغيلية، مع تحديد المخاطر التقنية أو الأمنية التي تظهر ومعالجتها فورًا. كما تم تأسيس فرق مشتركة بين الجهات الرقابية والتنفيذية لرصد تقدم تنفيذ الأجندة الرقمية الوطنية 2030 التي تتضمن 6 ركائز استراتيجية، لضمان اكتشاف أي تعثر أو مخاطر مبكرًا وتصحيح المسار لتحقيق مستهدفات التحول الرقمي في موعدها. وضمن إطار إدارة المخاطر، اعتمدت قطر المعيار الوطني لضمان المعلومات (NIAS) في 2023 الذي يفرض على كل مؤسسة تقييم مخاطر منتظم يغطي الجوانب التقنية والتشغيلية وحوكمة الأمن. وتقوم الوكالة الوطنية للأمن السيبراني وهيئة تنظيم الاتصالات بمتابعة امتثال الجهات الحساسة لإجراء اختبارات اختراق دورية وتمارين محاكاة للهجمات (تمارين صمود) للوقوف على جاهزيتها والتعامل مع نقاط الضعف. رغم ذلك، أحد التحديات هو ضمان جعل هذه التقييمات مستمرة

وليست موسمية فقط؛ إذ تُظهر الدراسات العالمية أن نسبة قليلة نسبيًا من المؤسسات هي التي تطبق تقييم مخاطر بشكل متواصل. ففي استطلاع ISACA/Protiviti لعام 2015 مثلًا، تبيّن أن 16% فقط من كبرى الشركات تقوم بتحديث تقييمات مخاطر تقنية المعلومات باستمرار، بينما البقية تكتفي بدورية سنوية أو نصف سنوية. هذا الواقع حثّ الجهات الرقابية في قطر على الدفع نحو تعزيز آليات المراقبة اللحظية قدر الإمكان، فتم مثلاً إنشاء منظومات لوحات مؤشرات لحظية لدى مركز عمليات الحكومة الرقمية لقياس أداء الخدمات الإلكترونية (مدى توفرها، زمن الاستجابة، ...إلخ) وتنبيه المسؤولين فور أي تراجع ملموس.

في السياق العربي، تتزايد القناعة بأهمية المتابعة المستمرة للأداء والمخاطر في مشاريع الرقمنة الحكومية. بعض دول الخليج تبنت منهجيات المراجعة المرنة (Agile Audit) لمشاريع تقنية المعلومات، بحيث يشارك المدققون في دورات المشروع منذ بداياته بدلاً من الانتظار لنهايته، مما يمكنهم من تقييم المخاطر أولًا بأول وتقديم توصيات فورية. دول عربية أخرى بدأت بالاستفادة من حلول التكنولوجيا نفسها لتعزيز الرقابة – كاستخدام منصات ذكاء اصطناعي لمراقبة الشبكات الحكومية على مدار الساعة، أو اعتماد أنظمة إنذار مبكر للمخاطر السيبرانية. أما عالميًا، فقد أصبح التقييم المستمر ركناً رئيسيًا في حوكمة تقنية المعلومات؛ فالمعايير الدولية مثل معيار إدارة الخدمات التقنية ISO 20000 وإطار ITIL تشدد على أهمية دورة التحسين المستمر، والتي تتضمن التقييم المنتظم للأداء وسد الثغرات بشكل تكراري. كذلك، ظهر توجه نحو المراجعة المستمرة (Continuous Auditing) باستخدام أدوات برمجية تقوم آليًا بجمع بيانات الأداء والضبط الداخلي وتنبيه المدققين إلى أي شذوذ أو خطر في الوقت الفعلي. على سبيل المثال، في الولايات المتحدة، يوصي مكتب المساءلة الحكومي (GAO) الوكالات بتنفيذ مراقبة مستمرة للمشاريع التقنية عالية التكلفة أو الأهمية لتلافي فشل المشاريع قبل وقوعه. هذا التحول إلى التقييم المستمر يستهدف معالجة حقيقة أن المخاطر التقنية يمكن أن تتطور بسرعة وتتسبب بأضرار كبيرة إن لم يتم رصدها مبكرًا. بالتالي، دور الرقابة الحديث يتجاوز المراجعات التقليدية المتباعدة إلى نظام إنذار مبكر ورفيع المستوى يستشعر التحديات فور بروزها ويضمن بقاء التحول الرقمي على المسار الصحيح ويحقق أهدافه بكفاءة وأمان.

3. الشفافية والمساءلة

تسهم الرقابة كذلك في ترسيخ مبادئ الشفافية والمساءلة ضمن منظومة الحوكمة الذكية. في قطر، قطعت الحكومة أشواطًا في إشراك الجمهور وتحقيق شفافية أكبر عبر إطلاق مبادرات البيانات المفتوحة والمنصات التفاعلية، مع وجود رقابة تضمن مصداقية هذه الجهود واستمراريتها. فقد دشنت قطر بوابة البيانات المفتوحة الوطنية عام 2019 (data.gov.qa) لإتاحة طيف واسع من البيانات الحكومية للجمهور، بغرض تعزيز الثقة وتمكين روّاد الأعمال والباحثين من الاستفادة منها. ويشرف على هذه المبادرة وزارة الاتصالات وتكنولوجيا المعلومات بالتعاون مع أمانة التخطيط التنموي، وتتم مراقبة تنفيذ سياسة البيانات المفتوحة عبر لجان مشتركة تضمن تحديث البيانات دورياً وجودتها. ومن جهة أخرى، تؤكد الأجهزة الرقابية – كديوان المحاسبة – على مبدأ الإفصاح عن نتائج أداء المشاريع الرقمية الكبرى. على سبيل المثال، قد يُلزِم الديوان جهةً ما بنشر تقارير أداء منصة إلكترونية معينة سنوياً، أو إعلان مؤشرات خدمة العملاء ورضاهم، بهدف تعزيز المساءلة أمام الجمهور. بالإضافة إلى ذلك، هناك توجه لأن تتضمن الاستراتيجيات الرقمية مؤشرات شفافية، مثل معدلات نشر البيانات الحكومية وعدد الخدمات التي يتم الإفصاح عن مستويات جودتها بشكل علني. وقد أدى هذا إلى وضع قطر في مصاف الدول السباقة بالمنطقة في مجال الحكومة المفتوحة، حيث تُظهر تقييمات مؤشر البيانات المفتوحة تحسنًا مطردًا في تصنيف قطر. بالتوازي، يُمارَس نوع من الرقابة الشعبية بفضل الخدمات الرقمية؛ إذ يُمكن للمواطنين والمقيمين تقييم الخدمات الحكومية إلكترونيًا وإرسال الشكاوى عبر بوابة حكومي أو التطبيقات الحكومية، وهنا يأتي دور الرقابة الرسمية في التأكد من معالجة تلك الشكاوى بشفافية وفي التقارير السنوية.

أصبحت الشفافية إحدى سمات الحكومة الرقمية الناجحة، وترتبط مباشرة بمستويات الثقة العامة. يذكر تقرير أممي أن 55% من دول العالم لديها مبادرات بيانات مفتوحة وطنية مصحوبة بكاتالوج بيانات مركزي، إلا أن التفاوت ما زال كبيرًا في مدى جودة ونطاق البيانات المنشورة. وهنا يأتي دور الرقابة لضمان ألا تكون مبادرات الشفافية شكلية فقط. كما نبه تقرير البارومتر المفتوح للبيانات إلى مشكلة ما يسمى "غسل البيانات المفتوحة"، حيث تعلن الحكومات عن بوابات مفتوحة لتحسين صورتها لكن من دون تغيير حقيقي في ثقافة الشفافية والمساءلة. لذا تشدد منظمات دولية مثل OECD والبنك الدولي على ضرورة وجود إطار حوكمة للبيانات المفتوحة يرعاه جهاز حكومي رقابي لضمان تنفيذ سياسات الإفصاح بشكل فعّال. أيضًا، يساعد التدقيق التقني في بناء المساءلة؛ إذ يقوم المدققون بفحص سجلات الأنظمة الإلكترونية (Audit Logs) للتحقق من عدم إساءة استخدام السلطة الرقمية، ويضمنون وجود مسارات مراجعة واضحة لكل تعامل رقمي مما يمكّن من تتبع أي خلل إلى مصدره ومحاسبة المسؤول عنه. بعض الدول سنت قوانين "حق الحصول على المعلومات" التي تسمح للمواطنين بطلب بيانات من أي جهاز حكومي والشكوى

إن رُفض طلبهم بلا مسوغ، وهو ما يدفع الجهات لاعتماد الشفافية كافتراضية. في النهاية، تعتبر المساءلة الجانب التكميلي للشفافية؛ فالرقابة لا تكتفي بجعل المعلومات متاحة، بل تتأكد من استخدام تلك المعلومات لمحاسبة المقصرين وتصحيح الأخطاء. ومتى ما شعر المواطنون أن حكوماتهم أكثر شفافية ومسؤولية، تزداد ثقتهم في الخدمات الرقمية المقدمة وينخرطون فيها بفعالية أكبر، الأمر الذي يحقق أحد أهم أهداف التحول الرقمي.

4. إدارة الموارد التقنية والمالية

من الأدوار المحورية للرقابة في سياق التحول الرقمي التأكد من الإدارة الرشيدة للموارد التقنية والمالية المخصصة لهذا التحول. في قطر، استثمرت الحكومة مبالغ كبيرة في تطوير البنية التحتية الرقمية (مثل شبكات الألياف الضوئية وبناء مراكز بيانات حكومية سحابية) وفي مشاريع التحول الرقمي للجهات المختلفة. ومن هنا برزت أهمية متابعة رقابية حثيثة لضمان أن هذه الموارد تُدار بكفاءة وتحقق العائد المرجو منها للمجتمع. يقوم ديوان المحاسبة والأجهزة الرقابية المعنية بمراجعة خطط الإنفاق على المشاريع الرقمية الكبرى قبل اعتمادها، للتأكد من واقعية الميزانيات وتجنب التضخيم. ثم أثناء التنفيذ، تُرفع تقارير مرحلية حول نسب الإنجاز مقابل الصرف المالي. فإذا تبين وجود تجاوز في التكاليف أو تأخر غير مبرر، يتم التحقيق في الأسباب واتخاذ الإجراءات التصحيحية وربما إيقاف المشروع إن كان مُهدِرًا للمال العام. وقد اكتسبت قطر خبرة جيدة في إدارة المشاريع التقنية الضخمة بكفاءة – كبرنامج الحكومة الإلكترونية وبرنامج تسمو – حيث تتابع لجان توجيهية متعددة القطاعات تلك المشاريع وتقيّم مردودها بشكل مستمر. فعلى سبيل المثال، بعد تطبيق نظام موارد حكومي موحد، أظهر تقرير رقابي أنه حقق وفرًا سنويًا بنسبة معينة عبر تقليل الازدواجية، فتمت مشاركة هذه النتيجة لدعم قرارات توسيع التطبيق في جهات أخرى. بالمقابل، إن وُجد مشروع لا يحقق أهدافه التقنية أو يواجه عقبات متكررة، قد توصي الرقابة بإعادة التخطيط أو إعادة توجيه موارده إلى أولويات رقمية أخرى أكثر جدوى. كذلك، تتولى الرقابة فحص إجراءات المشتريات التقنية – مثل عقود أنظمة المعلومات والاستشارات التقنية – لضمان التنافسية، وخلوها من التضارب، والامتثال للمعايير التعاقدية، وهو ما يعكس التوازن بين دعم الابتكار وضبط الإنفاق.

5. دعم الابتكار التكنولوجي

قد يُنظر إلى الرقابة أحيانًا على أنها وظيفة تقليدية لضبط الإجراءات فحسب، لكن في عصر الحكومة الذكية أضحى من أدوار الرقابة المهمة أيضًا دعم الابتكار التكنولوجي وتوجيهه بشكل سليم. في قطر، شجعت القيادة على الابتكار في الخدمات الحكومية من خلال مبادرات مثل مختبر تسمو للابتكار وحاضنات للمشاريع الرقمية الناشئة. ولم تكن أجهزة الرقابة بمنأى عن هذا التوجه؛ فقد تبنت نهجًا يوازن بين التحفيز والتقنين. فعلى سبيل المثال، عند قيام جهة حكومية بتجربة تقنية جديدة (كالذكاء الاصطناعي في خدمة العملاء أو سلسلة الكتل في السجلات الحكومية)، يتعاون المدققون منذ البداية لتحديد الضوابط اللازمة دون تثبيط التجربة ذاتها. تم إنشاء ما يشبه "بيئات تجريبية" رقابية تسمح للجهات بالابتكار ضمن حدود متفق عليها، على أن يتم تقييم النتائج قبل التوسع. أيضًا، يشجع ديوان المحاسبة القطري الجهات على تبني أدوات التحليل المتقدم والبيانات لتحسين الأداء، بل واعتمد هو نفسه تقنيات التدقيق بمساعدة الحاسوب والذكاء الاصطناعي، في رسالة مفادها أن الرقابة ليست عدوًا للتقنية بل مستخدم إيجابي لها. علاوة على ذلك، تساهم الرقابة في قطر في إزالة العقبات البيروقراطية أمام الابتكار؛ فإذا كشفت المراجعات وجود لوائح أو إجراءات قديمة تعيق تنفيذ حلول رقمية جديدة (مثلاً اشتراطات ورقية غير مبررة أو تداخل صلاحيات)، يمكن أن توصي بتعديل تلك اللوائح لتواكب التحول الرقمي. وقد حصل ذلك فعليًا حين ساعدت توصيات رقابية في تحديث بعض التشريعات للسماح بتبادل البيانات بين الجهات عبر منصات رقمية بشكل قانوني سلس. من جهة أخرى، تحرص الرقابة على ألا يأتي الابتكار على حساب مبادئ الحوكمة؛ فهي تدعم التجريب السريع (fail–fast) شريطة وجود خطة واضحة لإدارة المخاطر المحيطة بالتقنية الجديدة وحماية بيانات المستخدمين أثناء التجارب.

الابتكار الحكومي بات مؤشرًا رئيسيًا على فعالية الحكومة. وتوصي منظمات مثل OECD بأن تتبنى الحكومات ما يسمى "حوكمة تجريبية" (Experimental Governance) حيث يتم تجربة الحلول الرقمية الجديدة على نطاق صغير وتشارك نتائجها بشفافية، مع وجود إطار رقابي مرن يوازن بين الإبداع والمخاطر. العديد من الدول المتقدمة أنشأت وحدات ابتكار حكومي (GovTech Labs) بفرق مشتركة من المبتكرين والمشرّعين للبحث في التقنيات الناشئة كتحليل البيانات الضخمة في صنع القرار أو استخدام الروبوتات في الخدمات، ووضع ضوابط استباقية لها قبل انتشارها. ومن الأمثلة، مختبر الابتكار التنظيمي في كندا الذي يجمع منظمي القطاعات المختلفة لبحث كيفية تحديث الأطر التشريعية لدعم التقنيات الحديثة. أيضًا، الأجهزة الرقابية العليا دوليًا تواكب هذا التطور؛ فإنتوساي (المنظمة الدولية للأجهزة العليا للرقابة) لديها

مبادرات لدراسة أثر التقنيات الناشئة على أساليب التدقيق، ونشرت مؤخراً دليلاً حول تدقيق خوارزميات الذكاء الاصطناعي لضمان استخدامها بشكل أخلاقي وفعّال في الجهات الحكومية. يتضح إذن أن دور الرقابة لم يعد جامدًا، بل أصبح شريكًا استراتيجيًا في الابتكار من خلال توفير بيئة موثوقة لتجريب الحلول الجديدة وتقييمها بعدالة وشفافية. وعندما يشعر المبتكرون أن هناك تفهمًا رقابيًا وتشريعيًا لمشاريعهم، فإن ذلك يشجعهم على المضي قدمًا بخطى أسرع. وبالمحصلة، يؤدي هذا التكامل بين الرقابة والابتكار إلى حكومة أكثر مرونة وذكاءً، قادرة على التطور واستيعاب التقنيات المستقبلية بأقل قدر من المخاطر.

سادساً: التحديات التي تواجه الرقابة على تكنولوجيا المعلومات في الحكومة الذكية

1. التطور التكنولوجي السريع

يُشكّل التطور التقني المتسارع ربما التحدي الأكبر الذي يواجه الرقابة على تكنولوجيا المعلومات في عصر الحكومة الذكية. في قطر، تعمل أجهزة التدقيق والرقابة جاهدةً لمجاراة نسق الابتكار التقني. لكن مع ظهور تقنيات جديدة مثل الذكاء الاصطناعي التوليدي، وسلاسل الكتل (Blockchain)، وإنترنت الأشياء (IoT)، تجد الجهات الرقابية نفسها أمام منحنى تعلم حاد. فهذه التقنيات قد تدخل الخدمة قبل أن تتبلور معايير واضحة لإدارتها أو تدقيقها. على سبيل المثال، إذا بدأت وزارة ما في قطر استخدام خوارزميات ذكاء اصطناعي لاتخاذ قرارات معينة (كإعطاء أولوية لمعاملات ما)، سيحتاج المدققون إلى فهم كيفية عمل هذه الخوارزميات وتقييم العدالة والشفافية فيها، وهو أمر جديد نسبيًا ويتطلب خبرات تقنية عميقة. وقد بادرت قطر عبر ديوان المحاسبة إلى ابتعاث وتدريب بعض كوادرها في مجالات تدقيق الأنظمة المتقدمة، كما تستعين بخبراء أو شركات استشارية أحيانًا للمساعدة في عمليات المراجعة التقنية شديدة التخصص. ومع ذلك يبقى التحدي قائمًا: فبمجرد ما يكتسب المدققون مهارة تقنية معينة، تكون التكنولوجيا نفسها قد تطورت إلى جيل أحدث. ويؤكد خبراء التدقيق أن مجاراة التكنولوجيا تبقى سباقًا مستمرًا لن ينتهي. وفي الاستطلاعات العالمية، صنّف رؤساء التدقيق في المؤسسات مواكبة التغيرات التقنية والبنية التحتية المتجددة على أنها التحدي التقني الأول عالميًا أمام مهامهم. وأقرّ 88% منهم بأن سرعة الابتكار تجعل من الصعب وضع خطط تدقيق ثابتة. وقد شهدنا في قطر والمنطقة حالات تأخر فيها التدقيق عن ملاحقة تقنية ما، مثل تأخر وضع إطار رقابي لخدمات الحوسبة السحابية العامة لسنوات قليلة بعد اعتماد الجهات لها، مما أوجد فترة فراغ معياري. للتغلب على ذلك، تحاول الرقابة في قطر اتباع نهج استباقي: مثلاً، عند استشراف توجه وطني لتبنّي تقنية المدن الذكية وإنترنت الأشياء ضمن برنامج تسمو، بدأت فرق التدقيق بدراسة

مخاطر إنترنت الأشياء (مثل الثغرات الأمنية في أجهزة الاستشعار والخصوصية) حتى قبل انتشارها الواسع، لتتمكن من طرح توصيات استباقية. هذا التحدي يتفاقم عند التفكير في تقنيات المستقبل كالعملات الرقمية للبنوك المركزية أو الميتافيرس الحكومي؛ فالرقابة مطالبة بتعلمها سريعًا ووضع أطر رقابتها، وإلا فقد تستغل الثغرات لارتكاب تجاوزات قبل أن تدركها أعين الرقابة.

على المستوى الإقليمي، تعاني أجهزة رقابة تقنية المعلومات في كثير من الدول العربية من نقص الكفاءات المتخصصة القادرة على فهم التقنيات الوليدة. إذ ما زال التركيز الأكبر ينصب على تدقيق نظم المعلومات التقليدية (كالتطبيقات المالية ونظم الموارد البشرية)، بينما التقنيات الأحدث كتحليلات البيانات الضخمة أو منصات الخدمات الذاتية بالذكاء الاصطناعي لم تحظ بعد بنفس مستوى الفهم الرقابي. يظل الواقع أن التطور التقني أسرع من استجابة كثير من الأطر البيروقراطية. ويؤدي هذا أحيانًا إلى تأخر في إصدار تشريعات أو أدلة رقابية مطلوبة، ما يضعف الرقابة مؤقتًا. عالميًا، تدرك أجهزة الرقابة العليا هذا التحدي بشكل جليّ. وأفاد المسح العالمي المشترك بين ISACA وشركة Protiviti أن التغير التقني المتسارع تصدّر للسنة الخامسة على التوالي قائمة تحديات مدققي تكنولوجيا المعلومات. ويدعو قادة التدقيق إلى اتباع استراتيجيات مرنة للتعامل مع ذلك، منها: التعلم المستمر للمدققين عبر دورات وشهادات محدثة باستمرار، وتحديث معايير الرقابة دورياً (فمثلًا تم إصدار COBIT 2019 ليحل محل COBIT 5 لمواكبة مستجدات التحول الرقمي)، والاستعانة بخبرات خارجية عند اللزوم للتدقيق في مجالات دقيقة. كما بدأت بعض أجهزة الرقابة استخدام تقنيات رقابية مبتكرة نفسها – كالاعتماد على برمجيات ذكاء اصطناعي تمشيطية لتدقيق البيانات الضخمة لأن العنصر البشري وحده لا يكفي – وهذا يخفف الفجوة قليلاً.

2. مواجهة الهجمات الإلكترونية

مع تصاعد وتيرة وخطورة الهجمات السيبرانية، بات على أجهزة الرقابة والتدقيق في الحكومة الذكية أن تواجه تحديًا مزدوجًا: حماية نفسها ومنظوماتها من الاختراق، وفي الوقت ذاته التأكد من متانة دفاعات الجهات الحكومية ضد تلك الهجمات. في قطر، على سبيل المثال، لا تقتصر جهود الأمن السيبراني على الفرق التقنية فحسب، بل أصبحت جزءًا من عملية التدقيق الدوري. يقوم مدققو تقنية المعلومات بفحص سجلات الحوادث الأمنية في كل جهة، والتحقق من اتباعها لسياسات الأمن المعتمدة (مثل سياسات كلمات المرور، وتشفير البيانات الحساسة، وخطط استمرارية الأعمال). كما قد يشارك المدققون أحيانًا في اختبارات جاهزية كتمارين الاستجابة لحوادث اختراق للتأكد من أن فرق تقنية المعلومات قادرة على التعامل الفعّال.

وعندما ترصد الرقابة ثغرات متكررة – كعدم تطبيق ترقيعات برمجية هامة أو ضعف إجراءات إدارة الحسابات – فإنها توجه توصيات صارمة وقد ترفع الأمر إلى مستويات عليا للمساءلة إذا استمر الإهمال. إضافة لذلك، فإن أجهزة الرقابة نفسها (كديوان المحاسبة) أصبحت هدفًا محتملًا للهجمات كونها تحتفظ ببيانات حساسة عن مؤسسات الدولة. لذا استثمر ديوان المحاسبة القطري في تعزيز أمن بنيته الخاصة، عبر تحديث أنظمة الحماية وتطبيق معايير الأمن المعلوماتي داخليًا، بل وخضع طوعًا لتقييم أمن سيبراني مستقل للتأكد من سلامة إجراءاته. فرغم أن دور الديوان رقابي، أدرك مسؤولوه أنهم ليسوا محصنين من الاستهداف الرقمي ويجب أن يكونوا قدوة في الامتثال لضوابط الأمن.

إقليميًا، نجد وضعًا مشابهًا. فقد تعرضت مواقع حكومية في دول عربية لهجمات إلكترونية ذات دوافع مختلفة (سياسية، إجرامية، إرهابية)، ما أدى أحيانًا إلى تسريب بيانات مواطنين أو تعطيل خدمات مهمة. هذا الواقع فرض على الرقابة تبني نهج "التدقيق الأمني" المتخصص. فصارت فرق التدقيق تشمل مهارات في الأمن السيبراني أو تتعاون مع فرق الأمن الداخلي لإجراء مراجعات أمنية تقنية (Technical Security Audits) على الشبكات والأنظمة المهمة.
عالميًا، لا تختلف الصورة كثيرًا. إذ كشف تقرير الاتحاد الدولي للمراجعين الداخليين لعام 2022 أن أقل من نصف أجهزة التدقيق حول العالم تشعر بالثقة في قدرتها على تقييم ضوابط الأمن السيبراني بشكل فعال، مما يشير إلى حاجة كبيرة لسد فجوة المهارات في هذا المجال. كما أن تنامي استخدام التقنيات السحابية والعمل عن بعد عقّد مهمة الرقابة الأمنية، حيث أصبحت الحدود التقليدية للشبكات الحكومية غير واضحة. ونتيجة لذلك، تتعاون العديد من الأجهزة الرقابية مع وكالات الأمن السيبراني الوطنية.

إن تحدي الهجمات الإلكترونية يفرض على الرقابة أن تكون دومًا في حالة تأهب وتحديث. فأي ثغرة غير ملتفت لها قد تتسبب في اختراق يكلف الكثير. ومن هنا أصبح معيار "المرونة السيبرانية" مؤشرًا جديدًا يهتم به المدققون – وهو قدرة المؤسسة على التعافي السريع من الهجوم واستمرار العمليات. الرقابة الحكيمة لا تكتفي بمنع الخروقات، بل تركز أيضًا على وجود خطط تعافي لدى الجهات واختبارها دوريًا. هكذا، تسهم الرقابة في بناء جدار صد متين في وجه الهجمات الإلكترونية التي لا تنفك تتطور كماً ونوعاً، وذلك عبر التحفيز المستمر للتحسين الأمني والمساءلة الصارمة عند التقصير في حماية أصول الدولة الرقمية.

3. تحديات تدريب وتطوير الموظفين

من التحديات الجوهرية التي تواجه الرقابة على تقنية المعلومات هي تطوير قدرات الكادر البشري الرقابي ذاته ليواكب متطلبات الحكومة الذكية. في قطر، أدرك ديوان المحاسبة وغيره من أجهزة الرقابة أن الاستثمار في تأهيل المدققين هو استثمار في جودة الرقابة المستقبلية. لذا اعتمد برامج تدريب سنوية تشمل أحدث ما توصلت إليه معايير تدقيق تقنية المعلومات. يتم إيفاد موظفين لدورات وشهادات احترافية مثل شهادة مدقق نظم المعلومات المعتمد (CISA) وشهادات في حوكمة تقنية المعلومات (مثل COBIT). كما يجري التعاون مع جامعات ومراكز متخصصة محليًا (كجامعة حمد بن خليفة ومعهد قطر لبحوث الحوسبة) لتقديم ورش عمل لموظفي الرقابة حول مواضيع حديثة كالتحليل الجنائي الرقمي وتدقيق أمن التطبيقات. وعلى الرغم من هذه الجهود، تظل هناك صعوبة في الحفاظ على الكفاءات العالية داخل الجهاز الرقابي. فالسوق القطرية والخليجية تنافس على الخبرات التقنية، وغالبًا ما تستقطب شركات التكنولوجيا أو حتى الجهات التنفيذية الحكومية أنفسها المدققين المهرة بعروض وظيفية مغرية. هذا يضع تحديًا أمام أجهزة الرقابة في استبقاء الخبرات عبر توفير حوافز مادية ومعنوية ومسارات وظيفية جذابة. وقد أشار تقرير لـ ISACA أن ثلث المتخصصين التقنيين عالميًا غيّروا وظائفهم خلال عامين، مما يجعل مسألة تدوير الكفاءات تحديًا عالميًا أيضًا. في قطر، حاول الديوان معالجة ذلك جزئيًا عبر خلق مسارات مهنية تقنية داخل هيكله، تتيح للمدقق التخصص والتدرج في مجال تدقيق تقنية المعلومات حتى مناصب قيادية، بدلًا من اعتباره مجالًا فرعيًا مؤقتًا.

قد تبنت المنظمة العربية للأجهزة العليا للرقابة (ارابوساي) مبادرة في السنوات الأخيرة لإقامة دورات إقليمية متخصصة لتدريب مدققي تقنية المعلومات العرب، بهدف رفع المستوى العام وتبادل الخبرات. رغم ذلك، يبقى التعلم المستمر تحديًا ثقافيًا ومؤسسيًا؛ فالرقابة الحكومية تقليديًا قد لا تخصص ما يكفي من الميزانية والوقت لتدريب موظفيها مقارنة بالقطاع الخاص. ولهذا نرى فجوة في بعض الأجهزة بين المهارات المطلوبة (مثلاً فهم أمن الشبكات أو قواعد البيانات) والمهارات المتوفرة لدى المدققين الميدانيين، مما قد يؤدي إلى عدم كشف بعض المشكلات أو الاعتماد الزائد على استشاريين خارجيين.

أما دوليًا، فقد تم التعرف على هذه المشكلة بوضوح. تصنِّف استطلاعات معهد المدققين الداخليين نقص مهارات تقنية المعلومات في فرق التدقيق كأحد أبرز المخاطر التي تهدد قدرة وظيفة التدقيق على أداء دورها في المستقبل. وفي دراسة عالمية حديثة، أشار 60% من مسؤولي التدقيق إلى صعوبة في إيجاد

الأشخاص ذوي المعرفة والمهارات المناسبة في مجال التدقيق التقني. لمواجهة ذلك، تنتهج الكثير من الأجهزة الرقابية حول العالم استراتيجيات متنوعة، منها: التوظيف المرن (مثلاً جلب خبراء تقنية بعقود قصيرة للمشروعات)، وبرامج التوجيه والتعلم أثناء العمل pairing حيث يعمل مدقق تقليدي بجانب خبير تقني لتبادل المعارف. كما برز توجه نحو "إعادة تشكيل فرق التدقيق" بحيث تضم خلفيات متنوعة (ماليين، قانونيين، تقنيين) لضمان تغطية شاملة لمختلف جوانب التحول الرقمي. إحدى الممارسات الجيدة عالميًا أيضًا هي إقامة مراكز تميز داخل جهاز الرقابة تركز على مجال تقني معين (مثلاً مركز تميز للتدقيق السيبراني) تقوم بوضع منهجيات متطورة وتدريب بقية الفريق عليها. ومما لا شك فيه أن التعاون الدولي مفيد هنا؛ فبرامج الإنتوساي تتيح إعارة خبراء بين الأجهزة وتقديم ورش عمل متقدمة.

باختصار، التحدي البشري في الرقابة التقنية يتلخص في سؤال: من يراقب الرقباء تقنيًا؟ والحل يكمن في بناء الرقيب التقني نفسه عبر التعليم والتدريب والتحفيز. في الحكومة الذكية، لا تكفي مهارات التدقيق التقليدية، بل يحتاج المدقق إلى أن يكون ملمًا بالتكنولوجيا بعمق وفضوليًا لتعلم الجديد دومًا. حينها فقط تستطيع أجهزة الرقابة الوقوف نداً بند مع المؤسسات الخاضعة لها في فهم الأنظمة والخدمات الرقمية، وبالتالي تقييمها بموضوعية وفعالية. إن تأهيل جيل جديد من المدققين التقنيين العرب والعالميين بات ضرورة ملحة توازي في أهميتها تأهيل المبرمجين ومحللي البيانات وغيرهم، لأن وجود رقابة قوية هو ما سيضمن في نهاية المطاف نجاح التحول الرقمي ضمن ضوابط الحوكمة الرشيدة.

الخاتمة

إن التحول الرقمي الحكومي والانتقال نحو نموذج الحكومة الذكية يحملان وعودًا كبيرة بتحسين حياة المواطنين وتعزيز كفاءة وشفافية القطاع العام. وقد استعرضنا كيف تمكنت قطر من تحقيق قفزات نوعية في هذا المجال مدفوعة برؤية وطنية واضحة واستثمارات استراتيجية في البنية الرقمية ورأس المال البشري، مما أثمر تحسين ترتيبها العالمي في مؤشرات الحكومة الإلكترونية وتوسعة نطاق الخدمات المقدمة عبر الإنترنت. غير أن الطريق نحو التحول الرقمي هو محفوف بتحديات ترتبط بالثقافة الرقمية لدى المجتمع، وبناء المهارات اللازمة، وتأمين الفضاء السيبراني ضد الأخطار المتزايدة. وفي هذا السياق، يتجلى دور الحوكمة والرقابة كعامل تمكين وضبط في آن واحد. فالرقابة الرشيدة تضمن أن هذا التحول يتم بطريقة تحفظ حقوق المواطنين الرقمية (كالخصوصية)، وتلتزم بالمعايير والموجهات العالمية، وتحقق النتائج المأمولة بأفضل استخدام للموارد، وفي الوقت نفسه لا تكبح جماح الإبداع التقني بل توجهه وتدعمه. لقد رأينا كيف أن امتثال المؤسسات للقوانين والسياسات ليس أمرًا يُترك للمصادفة، بل هو نتيجة منظومة رقابية متكاملة تتابع وتقيّم وتصحح بشكل مستمر. كما لمسنا أن الشفافية والمساءلة لم تعدا مفاهيم نظرية، بل تم تفعيلهما عبر البيانات المفتوحة ومؤشرات الأداء العلنية، مما عزز ثقة الجمهور ومشاركته.

على الجانب الآخر، تدرك أجهزة الرقابة ذاتها أنها بحاجة للتطور المستمر لمواجهة تحديات المرحلة. فالتكنولوجيا تركض للأمام، والهجمات السيبرانية تزداد تعقيدًا وجرأة، وفجوات المهارات تضغط على الجميع. لذا بدأت الرقابة تتخذ خطوات استباقية بالتدريب والتعاون الدولي وتبني أدوات تقنية للرقابة، لكي لا تصبح الحلقة الأضعف في مسيرة الحكومة الذكية. التجارب العالمية أظهرت أن الدول التي وفقت في التحول الرقمي هي تلك التي وازنت بين الابتكار والضبط؛ أي شجعت الإدارات على التفكير خارج الصندوق وفي نفس الوقت وفرت خطوطًا حمراء واضحة ومساءلة دقيقة لضمان عدم الانحراف أو التقصير. وفي الدول العربية، بالرغم من تفاوت مستويات التقدم الرقمي، هناك اتجاه عام نحو تعزيز الحوكمة الرقمية والاستفادة من الدروس المستقاة عالميًا وإقليميًا لتجنب الأخطاء وتسريع الخطى. إن بناء حكومة ذكية فعلاً لا يتوقف عند شراء أحدث التقنيات، بل يتطلب ترسيخ ثقافة رقمية جديدة يكون فيها المواطن شريكًا فاعلاً، وتكون فيها المؤسسات العامة مرنة ومسؤولة، وتكون فيها الرقابة حصن الأمان وضمان الاستدامة.

وفي الختام، يمكن القول إن التحول الرقمي والحوكمة الذكية وجهان لعملة واحدة؛ فلا قيمة للتحول التقني دون حوكمة تحمي مساره وتعظّم منافعه، ولا تُجدي الحوكمة التقليدية في عصر التقنية ما لم تتكامل مع أدوات التحول الرقمي. التجربة القطرية تقدم نموذجًا ملهمًا إقليميًا، حيث التكامل واضح بين الاستثمار التقني والرشد

الرقابي. والتحدي المقبل يكمن في استمرار هذا التوازن مع ظهور تحديات جديدة مستقبلًا كالذكاء الاصطناعي العام أو تقنيات الميتافيرس وغيرها. سوف يبقى النجاح حليف من يتبنى التعلم المستمر والتكيف السريع – سواء أكان جهة منفذة أم جهازًا رقابيًا – لأن التغيير أصبح هو القاعدة. وبقدر ما نُحسن إدارة هذا التغيير ونوجهه لما فيه الخير العام، بقدر ما سننجح في بناء حكومات أكثر ذكاءً وإنسانيةً معًا، تواكب العصر وتستشرف المستقبل بثقة ومسؤولية.