محمد عسكر يكتب: البنية التحتية الرقمية في مهب الحريق

المصدر: مصر اليوم https://misryoum.com

في مشهد مأساوي إهتزت له القاهرة، إندلع أمس الإثنين 7 يوليو 2025 حريق هائل في الطابق السابع من سنترال رمسيس، أحد أهم مراكز الإتصالات في مصر. الحريق لم يكن مجرد حادث عارض، بل كشف النقاب عن هشاشة غير متوقعة في البنية الرقمية، ما يستدعي تساؤلات جادة حول إمكانية حماية مراكزنا من الكوارث المفاجئة وهل بنيتنا الرقمية الحالية تتمتع بالمرونة الكافية لتحمّل الأزمات والتعافي منها دون خسائر واسعة؟ وهل لدينا بالفعل بنية رقمية مرنة وقادرة على الصمود أمام الأزمات المتزايدة في عالم لا يعرف التوقف؟
وفقاً للبيانات الرسمية الأولية ، إندلع الحريق نتيجة ماس كهربائي داخل غرفة أجهزة الإتصالات.

ورغم سرعة تدخل الحماية المدنية، إلا أن حجم الضرر كان كبيراً. فلم تقتصر الخسائر على الجانب المادي من أرواح ومعدات، بل إنها إمتدت لتشمل إضطرابات واسعة في خدمات الإتصالات والإنترنت بعدد من أحياء القاهرة الكبرى.

كما تأثرت خدمات الدفع الإلكتروني، وتوقفت بعض التطبيقات الحكومية المرتبطة بالخوادم المركزية، ما كشف عن درجة عالية من الإعتماد المركزي غير المدعوم بتقنيات التكرار التلقائي أو البُنى الإحتياطية لتوزيع الخدمة. لقد أظهر الحادث هشاشة واضحة في قدرة البنية الرقمية الحالية على مواجهة الطوارئ، وعجزها عن إمتصاص الصدمات دون أن تنعكس مباشرة على حياة المواطنين وقطاعات الإقتصاد الحيوية فى الدولة.

ورغم جهود الجهات المعنية في إحتواء الموقف وإستعادة الخدمات تدريجياً، إلا أن غياب خطة طوارئ رقمية واضحة، وعدم جاهزية مراكز بديلة للتعامل مع الكوارث، يثير قلقاً حقيقياً بشأن قدرتنا على مواجهة سيناريوهات أكثر تعقيداً وخطورة في المستقبل.

الأمن الرقمي لا يقتصر على حماية المعلومات والبيانات فحسب، بل يبدأ أولاً من تأمين البنية الفيزيائية ذاتها: المباني، الكابلات، مراكز الطاقة، أنظمة التهوية، وأجهزة الإطفاء، بإعتبارها الأساس الذي تُبنى عليه المنظومة الرقمية برمتها. وفي حالة سنترال رمسيس، يبدو أن بعض هذه العناصر كانت غائبة أو غير كافية. ولو أن الحريق إمتد إلى الخوادم الأساسية أو الأنظمة الأخرى، لكان الأثر كارثياً على الإقتصاد الوطني. قد يُنظر إلى ما حدث في سنترال رمسيس كحادث عرضي، لكنه في الحقيقة تحذير مبكر لزلزال رقمي أكبر محتمل. فمع تسارع الرقمنة في مصر، لا بد أن ترافقها حماية هندسية وتقنية ومعمارية، تؤسس لبنية تحتية تستطيع النجاة من الحوادث، لا أن تنهار معها.

ففي عالم يتجه بسرعة فائقة نحو الرقمنة، لم تعد البنية التحتية الرقمية رفاهية تقنية، بل أصبحت العمود الفقري الذي تستند عليه الدولة الحديثة في إدارة شؤونها الاقتصادية والخدمية والأمنية. وفي دولة مثل مصر، التي قطعت شوطاً كبيراً خلال العقد الأخير في تبنّي التحول الرقمي، بات السؤال الأكثر إلحاحاً هو: كيف نؤمّن هذه البنية الحساسة التي تعتمد عليها حياة ملايين المواطنين ومؤسسات الدولة في كل لحظة؟

البنية التحتية الرقمية تشمل كل ما له علاقة بتدفق البيانات وتشغيل الخدمات الرقمية، من مراكز البيانات المركزية والموزعة، إلى شبكات الإتصالات والألياف الضوئية، وأنظمة الحوسبة السحابية، وقواعد البيانات الحكومية، والخدمات المالية الإلكترونية، ومرافق الطاقة الذكية، وغيرها من النظم المتصلة. ومع هذا الإتساع والتشابك، تتزايد المخاطر؛ فالتهديد لا يأتي فقط من الهجمات السيبرانية عبر الإنترنت، بل أيضاً من الكوارث الطبيعية، والأعطال الفنية، والإهمال البشري، بل حتى الحوادث العرضية كما شهدنا في حادث حريق سنترال رمسيس الذي أدى إلى تعطل خدمات الإتصالات والإنترنت في القاهرة.

تأمين هذه البنية لا يمكن أن يتم عبر حلول جزئية أو معالجات ظرفية، بل يحتاج إلى إستراتيجية شاملة تمزج بين البعدين التقني والتنظيمي. البداية تبدأ من الوعي بأن حماية البنية الرقمية لا تقتصر على برامج مكافحة الفيروسات أو جدران الحماية، بل تتطلب نظرة هيكلية إلى كل مكونات البنية التحتية: المباني، الأجهزة، الكابلات، البرمجيات، البشر، والسياسات. فالهجوم الإلكتروني قد يأتي من ثغرة في تطبيق بسيط، لكن الخلل الكارثي قد ينشأ من ماس كهربائي غير معالج، أو خادم غير مزوّد بنظام إطفاء تلقائي.

من أجل ذلك، يتعين علينا أولاً تحديث جميع مراكز البيانات والبنية الفيزيائية بشروط الأمان العالمي، بما يشمل أنظمة مكافحة الحريق، والتبريد، والطاقة الإحتياطية، وأنظمة المراقبة الذكية. ويجب بناء بنية مرنة تتوزع فيها الخدمات والبيانات على مواقع متعددة، لضمان إستمرار الخدمة في حالة تعطل مركز رئيسي. كما ينبغي إستخدام تقنيات التكرار التلقائي والنسخ الاحتياطي اللحظي، بحيث تتيح نسخ البيانات والعمليات بشكل لحظي أو دوري إلى مواقع بديلة، دون تدخل بشري. وتهدف هذه التقنيات إلى ضمان إستمرارية العمل وعدم فقدان البيانات في حال حدوث أي خلل، سواء كان ناتجاً عن عطل تقني، كارثة طبيعية، أو هجوم إلكتروني حتى لا يتسبب حادث بسيط في خسارة بيانات ضخمة أو إنقطاع شامل للخدمات.

على المستوى التشريعي والتنظيمي، يجب تعزيز الإطار القانوني لضمان إلتزام جميع الجهات الحكومية والخاصة بمعايير الأمن السيبراني والفيزيائي. فوجود قوانين مثل قانون مكافحة الجرائم الإلكترونية وقانون حماية البيانات الشخصية هو خطوة مهمة، لكنه غير كافٍ ما لم تقترن تلك القوانين بهيئات رقابية مستقلة لديها الصلاحيات والموارد لمتابعة التنفيذ والتفتيش وفرض العقوباتٍ عند الحاجة. وفي هذا السياق، لا بد من إنشاء كيان مستقل لحوكمة الأمن الرقمي، يجمع بين الرقابة، والتدريب، ووضع السياسات، والتنسيق بين الجهات المعنية.
جانب آخر بالغ الأهمية يتمثل في بناء القدرات البشرية. فتأمين البنية الرقمية لا يمكن أن يتحقق بدون كوادر وطنية مدربة ومؤهلة في أحدث تقنيات الأمن السيبراني وإدارة البنية التحتية. وهو ما يتطلب استثماراً جاداً في التعليم والتدريب، من خلال برامج تخصصية في الجامعات والمعاهد، وشراكات مع شركات التكنولوجيا العالمية، ومسارات مهنية حكومية تستقطب أفضل العقول وتحفزهم على البقاء داخل الدولة بدلاً من الهجرة أو الإتجاه للقطاع الخاص.
أخيراً، يجب أن تكون هناك شفافية ومصارحة مع الجمهور. فالحوادث الرقمية لا بد أن تُعلن وتُدرس ويُستفاد منها، لا أن تُخفى أو تُبرر. الثقة المجتمعية في المنظومة الرقمية لن تبنى إلا من خلال الشفافية والجاهزية، ومن خلال إظهار أن الدولة مستعدة لأي طارئ، وقادرة على المواجهة والإستجابة، وتحترم حق المواطن في معرفة ما يهدد خدماته وأمنه الرقمي.

إن تأمين البنية التحتية الرقمية في مصر لم يعد خياراً إستراتيجياً بل واجباً وطنياً. ففي دولة تسير بثبات نحو الرقمنة الشاملة، لا يجب أن تكون مراكز البيانات وقواعد الخدمات عرضة للخطر أو الإنقطاع، بل يجب أن تصبح مثلها مثل المطارات والموانئ والسدود: محصنة، محمية، وتدار وفق أعلى المعايير العالمية. فالمستقبل رقمي بلا شك، ولكن لا قيمة له إن لم يكن آمناً.