المقدمة

تقرير الرقابة السنوي لمراقب الدولة المخصص لموضوع السيبرانية وأنظمة المعلومات مطروح على طاولة الكنيست وفقًا لقانون مراقب الدولة، سنة 1958-5718 م. [نص مدمج]. يتناول هذا التقرير جوانب مركزية من الحماية السيبرانية، وأمن المعلومات، والخدمات الرقمية في القطاع العام.

أصبح الفضاء الرقمي في السنوات الأخيرة بنية تحتية أساسية في نشاط دولة إسرائيل. تُستخدم أنظمة المعلومات، والخدمات المحوسبة، ومسارات العمل الرقمية اليوم كأساس لعمل الوزارات الحكومية، وهيئات الطوارئ، والسلطات العامة، ومنظومات الخدمة للمواطن. إلى جانب المزايا العديدة التي تجلبها معها التحولات الرقمية - ومنها نجاعة الخدمة العامة، تحسين إمكانية الوصول، توفير الموارد، وتعزيز الاستمرارية الوظيفية - تتعاظم أيضًا المخاطر الناجمة عن التهديدات السيبرانية، تسرب المعلومات والفجوات في حماية أنظمة المعلومات. يفرض هذا الواقع على جميع الهيئات العامة أن تضمن أن تكون أنظمتها مؤمنة، موثوقة، متاحة، وقادرة على الصمود سواء في الأوقات الاعتيادية الروتينة أو في أوقات الطوارئ.

تُعتبر الحماية السيبرانية وأمن أنظمة المعلومات اليوم من ركائز الأداء السليم للدولة الحديثة. تركز الأنظمة الرقمية معلومات شخصية واقتصادية وأمنية بأحجام هائلة، وتُستخدم كبنية تحتية لعمل الوزارات الحكومية وهيئات الطوارئ والخدمات العامة الحيوية. في عصر تتعاظم فيه التهديدات السيبرانية باستمرار، وخاصة في فترات الطوارئ والأزمات، يُطلب من الدولة توفير جاهزية متقدمة تضمن حصانة الأنظمة وحماية خصوصية المواطنين واستمرار تقديم الخدمات للجمهور بصورة متواصلة وآمنة وموثوقة. إن تعزيز هذا المجال ليس مجرد حاجة تكنولوجية، بل هو ركيزة مركزية للأمن القومي، لثقة الجمهور بمؤسسات الدولة ولقدرة الحكومة على تقديم خدمة عامة ناجعة، متقدمة، ومتاحة لجميع المواطنين.

تبرز أهمية تعزيز حماية أنظمة المعلومات والبنى التحتية الرقمية بشكل خاص على خلفية الواقع الأمني المعقد الذي تعيشه دولة إسرائيل في السنوات الأخيرة. في هذه الفترات تتزايد محاولات الهجوم في الفضاء السيبراني التي تنفذها جهات معادية، إلى جانب حاجة هيئات الدولة إلى ضمان الاستمرارية الوظيفية وتقديم الخدمات الحيوية للجمهور حتى خلال ظروف الطوارئ. لقد أوضحت أحداث من هذا النوع أن أنظمة المعلومات والخدمات الرقمية وبنى العمل عن بُعد ليست مجرد أدوات إدارية وتكنولوجية، بل أنها تعتبر مكونًا مركزيًا في حصانة الدولة الوطنية وفي قدرتها على الاستمرار في العمل بصورة متواصلة وناجعة وآمنة.

تتناول الفصول الأربعة في هذا التقرير جوانب مختلفة ومتكاملة من المجال السيبراني وأنظمة المعلومات في القطاع العام:

- **أنظمة المعلومات وأمن المعلومات و السيبرانية في وزارة الخارجية**
- **الحماية السيبرانية في العمل عن بُعد في الأوقات الروتينيّة وفي حالات الطوارئ**
- **أمن وحماية منظومات المعلومات في وزارة البناء والإسكان**
- **الخدمات الرقمية للجمهور: منظومة التعريف الوطنية والمنطقة الشخصية الحكوميّة**

خضعت الفصول الثلاثة الأولى لإجراء السرية في اللجنة الفرعية التابعة للجنة شؤون مراقبة الدولة في الكنيست، وقد قررت اللجنة عدم عرضها كاملة على طاولة الكنيست، وإنما نشر أجزاء منها فقط، حفاظًا على أمن الدولة.

تشير نتائج الرقابة إلى وجود فجوات في الجاهزية، في إدارة المخاطر، في الإشراف وفي تطبيق السياسة الحكومية في هذا المجال، إلى جانب

حصول تقدم جزئي فقط في إتاحة وتوفير الخدمات الرقمية وفي دمج آليات حماية ورقابة متقدمة. على الرغم من أن كل واحد من التقارير يتناول مجالًا فريدًا من نوعه، فإن مجملها يوضح أن تعزيز حماية أنظمة المعلومات وضمان الاستمرارية الوظيفية وتعميق التحول الرقمي للخدمة العامة هي تحديات وطنية تستوجب معالجة جهازية ومنسقة ومستمرة.

أُجريت الرقابة بشأن **أنظمة المعلومات وأمن المعلومات و السيبرانية في وزارة الخارجية** خلال حرب السيوف الحديدية، وقد كشفت عن وجود فجوات في مجال إدارة وتطوير أنظمة المعلومات في الوزارة، وكذلك في مجال أمن المعلومات والحماية السيبرانية. ونظرًا إلى دورها، تُعد وزارة الخارجية هدفًا رئيسيًا لهجمات السايبر من قبل جهات معادية متنوعة، بدءًا من القراصنة (الهاكرز) ووصولًا إلى جهات دولية. تؤكد نتائج الرقابة الحاجة إلى تعزيز آليات الإشراف والرقابة لدى إدارة وزارة الخارجية في كل ما يتعلق بأنظمة المعلومات وأمن المعلومات في الوزارة، بهدف ضمان التشغيل السليم لمنظومة الحوسبة والاتصالات التابعة لها، وتحسين مستوى حماية الوزارة وممتلكاتها.

يتناول أحد فصول التقرير **تطبيق السياسة الحكومية لتعزيز الخدمات العامة الرقمية بواسطة منظومة التعريف الوطنية والمنطقة الشخصية الحكومية**. أظهرت الرقابة أنه رغم اتخاذ العديد من القرارات الحكومية منذ سنة ٢٠١٤ بشأن تعزيز الخدمات المحوسبة، وعلى الرغم من أن نحو ٤,٦ مليون مواطن مسجلون بالفعل في منظومة التعريف الوطنية، فإن تطبيق هذه السياسة لا يزال جزئيًا وبطيئًا. ١٦٪ فقط من الخدمات التي تم حصرها موصولة بمنظومة التعريف، نحو ٢٣٪ فقط من النماذج المحوسبة المعرّفة تُدار بواسطتها، من بين آلاف الخدمات الحكومية أتيح الوصول الى وفقط ٢٣٣ نموذج فقط في المنطقة الشخصية. كما تبيّن أن ١٥ سلطة فقط من أصل ٢٥٨ سلطة محلية اتصلت بمنظومة التعريف الوطنية، وأن نطاق اتصال الوزارات الحكومية والهيئات العامة الإضافية بهذه المنظومات محدود، بصورة تمس بقدرة الجمهور على تلقي خدمة حكومية رقمية كاملة، بسيطة، ومتاحة.

يتناول فصل إضافي **أمن وحماية أنظمة المعلومات في وزارة البناء والإسكان**، التي تحتفظ بملايين السجلات التي تتضمن معلومات شخصية وحساسة عن المواطنين والمستحقين للسكن والمقاولين. تستخدم الوزارة لغرض نشاطها عشرات الأنظمة من المعلومات، وفي سنة ٢٠٢٥ بلغت ميزانية أمن وحماية المعلومات السيبرانية الخاصة بها نحو ٦,٥ مليون شيكل - أي حوالي ٩٪ من ميزانية الحوسبة الإجمالية للوزارة. أظهرت الرقابة وجود إخفاقات جوهرية في إدارة أمن المعلومات والسيبرانية في الوزارة، ومنها فجوات في مراقبة صلاحيات إمكانيات الوصول، عدم استنفاد عمليات إدارة المخاطر، غياب آليات إنذار كافية وعدم استكمال تسجيل قواعد المعلومات كما يقتضيه القانون. تبرز هذه النتائج بشكل خاص في ظل الارتفاع الملحوظ (نحو ١٣٠٪) في نطاق الإنذارات السيبرانية التي وردت بشأن الوزارة في سنة ٢٠٢٤، وتوضح أهمية ضمان توفير حماية فعالة لأصول المعلومات التابعة للدولة.

يتناول التقرير أيضًا **الحماية السيبرانية في العمل عن بُعد**، الذي أصبح في السنوات الأخيرة جزءًا لا يتجزأ من نشاط الهيئات العامة والأمنية، وبشكل أكبر خلال فترة جائحة الكورونا وخلال حرب السيوف الحديدية. في إطار الرقابة تم فحص جاهزية الهيئات الحيوية، ومنها شرطة إسرائيل والسلطة القطرية للإطفاء والإنقاذ، للتعامل مع التهديدات السيبرانية المرافقة للعمل عن بُعد. أظهرت الرقابة وجود فجوات معينة في مدى ملاءمة آليات الحماية والرقابة للمخاطر القائمة، كما تم أيضًا الكشف عن وجود نواقص وإخفاقات من خلال فحص اختراق أجراه مكتب مراقب الدولة لمنظومة العمل عن بُعد التابعة لسلطة الإطفاء والإنقاذ. تؤكد هذه النتائج الحاجة إلى استكمال إعداد خطط العمل وتعزيز الجاهزية للأمن السيبراني في الهيئات الحيوية في الدولة.

يشير مجمل نتائج التقرير إلى أن تقدم دولة إسرائيل

نحو الحوكمة الرقمية المتقدمة يستوجب استثمارًا متواصلًا في البنى السيبرانية التحتية، في إدارة المخاطر، في الرقابة وفي الإنفاذ، إلى جانب وجوب تعاون وثيق بين جميع الهيئات العامة. إن الحماية الملائمة لأنظمة المعلومات والخدمات الرقمية ليست مجرد حاجة تكنولوجية - بل إنها شرط ضروري للحفاظ على ثقة الجمهور وحماية خصوصية المواطنين وضمان الأداء السليم والمتواصل للخدمة العامة.

يقع على كاهل الهيئات الخاضعة للرقابة واجب العمل بصورة سريعة وناجعة لتصحيح الإخفاقات والنواقص التي ذُكرت في هذا التقرير.

أتوجه بالشكر الجزيل إلى المستخدمين في مكتب مراقب الدولة، الذين عملوا على إعداد هذا التقرير بمهنية وبدقة وإخلاص، ومن منطلق الشعور بالرسالة. آمل أن تساعد نتائج التقرير وتوصياته في تعزيز المنظومات السيبرانية وأمن المعلومات في القطاع العام، وأن تسهم في تحسين الخدمة المقدمة لمواطني دولة إسرائيل.

نبتهل وندعو بالشفاء العاجل للجرحى، واعادة تأهيل المختطفين الذين عادوا إلينا وأبناء عائلاتهم، وبعودة جميع المُخْلين إلى بيوتهم، وسلامة جنودنا، ونجاح قوات الأمن في الدفاع عن بلادنا.

متنياهو أنـجلمان
مراقب الدولة
ومفوَّض شكاوى الجمهور

القدس،
أيّار **2026**