مجلة العلوم التربوية والتنمية
مجلة علمية دورية محكمة
ربع سنوية
تعالج القضايا التربوية والتنموية
تصدرها
مؤسسة مصر المستقبل للتنمية

العدد(٢) أبريل ٢٠٢٥

مفهوم الأمن الرقمي وآليات حمايته

إعداد

أ.د./ عائشة عبد الفتاح الدجدج

أستاذ أصول التربية المساعد

كلية الدراسات العليا للتربية

جامعة القاهرة

مفهوم الأمن الرقمي وآليات حمايته

د./ عائشة عبد الفتاح الدجدج [١]

المقدمة

في ظل التقدم التكنولوجي المتسارع، أصبحت الوسائط الرقمية جزءًا لا يتجزأ من حياة الأفراد والمجتمعات، حيث تسهم في تيسير الأعمال اليومية وتعزيز التواصل العالمي. ومع ذلك، فإن هذا الاعتماد المتزايد على التكنولوجيا جلب معه تحديات كبيرة تتمثل في الجرائم الرقمية التي تهدد أمن المعلومات وخصوصية المستخدمين. تتنوع هذه الجرائم بين السرقة الإلكترونية، الابتزاز، التشهير، وغيرها من الأفعال التي تستهدف الأفراد والمؤسسات على حد سواء. ونتيجة لضعف البنية التحتية الرقمية في بعض الأحيان، وسوء استخدام التكنولوجيا، أو الجهل بمخاطرها، يقع العديد من المستخدمين ضحايا لهذه التهديدات.

من هنا، برزت أهمية الأمن الرقمي كضرورة ملحة لمواجهة هذه التحديات، حيث يُعد الأمن الرقمي أداة فعالة للحفاظ على سلامة البيانات وضمان استمرارية الأنظمة المعلوماتية. يهدف هذا البحث إلى استعراض مفهوم الأمن الرقمي، تسليط الضوء على مخاطر الجرائم الرقمية، وبحث آليات حماية الأمن الرقمي، مع تقديم توصيات لتعزيز هذا المجال على المستويين الوطني والدولي.

مفهوم الأمن الرقمي

يُعرف الأمن الرقمي بأنه مجموعة الإجراءات والتقنيات التي تهدف إلى حماية الأنظمة المعلوماتية والبيانات من التهديدات الرقمية. وبشكل أكثر تفصيلًا، يُمكن تعريف الأمن الرقمي على أنه "القدرة على استخدام شبكة الإنترنت وغيرها من الوسائط الرقمية بفعالية دون التعرض لمخاطر أو تهديدات قد تُعرض خصوصية المعلومات وسريتها للخطر" (مركز هود، ٢٠١٧). كما يُشير الأمن الرقمي إلى قدرة الأنظمة المعلوماتية على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة التي تستهدف البيانات المتداولة أو المخزنة، وذلك ضمن إطار توافقي يضمن الاستدامة والأمان.

يُعتبر الأمن الرقمي جزءًا لا يتجزأ من الأمن السيبراني، وهو مفهوم أوسع يشمل حماية البنية التحتية الرقمية بجميع مكوناتها، بما في ذلك الأجهزة، البرمجيات، الشبكات، والبيانات. ووفقًا لتصنيف المؤشر العالمي للأمن السيبراني (GCI) الصادر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة، تحتل بريطانيا المرتبة الأولى عالميًا في هذا المجال، بفضل استثماراتها الكبيرة في

١ - أستاذ أصول التربية المساعد- كلية الدراسات العليا للتربية- جامعة القاهرة

تطوير البنية التحتية الرقمية وتشريعاتها المتقدمة. أما على المستوى العربي، فتتصدر المملكة العربية السعودية الترتيب، تليها مصر وقطر، مما يعكس الجهود المبذولة في المنطقة لتعزيز الأمن الرقمي.

إن الأهمية المتزايدة للأمن الرقمي تأتي من دوره في الحد من الجرائم الرقمية التي تتطور باستمرار، سواء من حيث الأساليب أو التأثير. فمع انتشار التقنيات الحديثة مثل الذكاء الاصطناعي والحوسبة السحابية، أصبحت الحاجة إلى حماية البيانات أكثر إلحاحًا، خاصة في ظل تزايد الاعتماد على الخدمات الرقمية في مختلف المجالات.

مخاطر الجرائم الرقمية

تشكل الجرائم الرقمية تهديدًا متزايدًا في العصر الحديث، حيث تتنوع أشكالها وتتطور أساليبها باستمرار. من أبرز هذه الجرائم السرقة الإلكترونية، التي تستهدف البيانات الشخصية أو المالية للأفراد والمؤسسات، والابتزاز الإلكتروني الذي يعتمد على تهديد الضحايا بنشر معلومات حساسة أو تشفير بياناتهم. كما تشمل الجرائم الرقمية التشهير عبر الإنترنت، والتزوير الرقمي، واختراق الأنظمة بهدف التخريب أو التجسس.

تتفاقم هذه المخاطر نتيجة عدة عوامل، أبرزها ضعف البنية التحتية الرقمية في بعض الدول، وسوء استخدام التكنولوجيا من قِبل المستخدمين، والجهل بمخاطر الإنترنت. فعلى سبيل المثال، قد يقوم مستخدم غير مدرك بمشاركة بياناته الشخصية على منصات غير آمنة، أو قد يفتح روابط مشبوهة تؤدي إلى اختراق جهازه. كما أن غياب الوعي الكافي بأهمية تحديث البرمجيات واستخدام كلمات مرور قوية يزيد من مخاطر التعرض للهجمات الرقمية.

علاوة على ذلك، فإن الجرائم الرقمية لا تقتصر على الأفراد فقط، بل تمتد لتشمل المؤسسات والحكومات، حيث تُستهدف الأنظمة الحيوية مثل البنوك، المستشفيات، والبنية التحتية الوطنية. هذا الواقع يفرض ضرورة تطوير استراتيجيات فعالة للتصدي لهذه التهديدات، وهو ما يبرز أهمية الأمن الرقمي كأداة أساسية للحماية.

آليات حماية الأمن الرقمي

لحماية الأمن الرقمي والحد من الجرائم الإلكترونية، هناك مجموعة من الآليات التي يمكن اعتمادها على المستويات القانونية، التكنولوجية، والدولية. ومن أبرز هذه الآليات :

١. تشريع قوانين صارمة :يُعد استحداث قوانين متخصصة لمكافحة الجرائم الرقمية خطوة أساسية. يجب أن تتضمن هذه القوانين قواعد واضحة للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، مع تجريم أفعال مثل محو البيانات أو تعديلها بشكل غير قانوني .

٢. فرض عقوبات رادعة :تشمل العقوبات الحبس والغرامات المالية على الأفعال التي تمس بالمصنفات الرقمية أو حقوق الملكية الفكرية، مثل التقليد، التزوير، أو الاستغلال غير المشروع للمصنفات المحمية قانونًا .

٣. تعزيز أنظمة الرقابة :يتطلب الأمن الرقمي مضاعفة أنظمة الرقابة التكنولوجية، مع مرافقتها بإطار قانوني ملائم يضمن فعالية التطبيق. على سبيل المثال، يمكن استخدام أنظمة كشف التسلل والبرمجيات المتقدمة لمراقبة الأنشطة المشبوهة .

٤. إقرار قواعد دولية :أُقرت العديد من الاتفاقيات الدولية لمكافحة الجرائم الرقمية، مثل اتفاقية بودابست التي وضعت إطارًا قانونيًا لتجريم الأفعال التي تمس بأمن المعلومات. هذه الاتفاقية تُعد نموذجًا للتعاون الدولي في هذا المجال .

٥. تطوير التكنولوجيا :يجب الاستثمار في تحديث البرمجيات وتطوير أنظمة الحماية مثل الجدران النارية وبرامج مكافحة الفيروسات، إلى جانب اعتماد تقنيات التشفير لحماية البيانات أثناء النقل والتخزين.

تتطلب هذه الآليات تعاونًا وثيقًا بين الحكومات، المؤسسات، والأفراد لضمان تحقيق أعلى مستويات الأمان الرقمي. كما أن الجمع بين الإجراءات القانونية والتكنولوجية يُعد ضروريًا لمواجهة التحديات المتزايدة في هذا المجال.

التوصيات

لتعزيز الأمن الرقمي والحد من مخاطر الجرائم الإلكترونية، يُقترح عدد من التوصيات التالية :

- رفع الوعي الرقمي :يجب تثقيف المستخدمين بمخاطر التكنولوجيا وسوء استخدامها، من خلال حملات توعية تُبرز أهمية حماية البيانات الشخصية واستخدام كلمات مرور قوية .

- تعزيز التعاون الدولي :يُعد التعاون بين الدول أمرًا حيويًا لمكافحة الجرائم الرقمية عابرة الحدود، وذلك من خلال تبادل المعلومات والخبرات وتطوير معايير مشتركة .

- تطوير البنية التحتية الرقمية :ينبغي الاستثمار في تحسين البنية التحتية الرقمية من خلال اعتماد برامج حديثة للتصدي للهجمات الرقمية، والاستعانة بخبراء متخصصين في مجال الأمن السيبراني .

• إعداد كوادر متخصصة :هناك حاجة ماسة لتدريب خبراء في مجالات الشرطة والقضاء والتكنولوجيا للتعامل مع الجرائم الرقمية بكفاءة، مع التركيز على تطوير مهاراتهم في الكشف عن الجرائم وتحليل البيانات.

الخاتمة

يُعد الأمن الرقمي ركيزة أساسية لضمان استدامة التحول الرقمي في المجتمعات الحديثة. وفي ظل تزايد الجرائم الإلكترونية، أصبح من الضروري اعتماد استراتيجيات شاملة تجمع بين التشريعات القانونية، الحلول التكنولوجية، والتوعية المجتمعية للحد من هذه التهديدات. من خلال تطبيق الآليات المقترحة وتعزيز التعاون الدولي، يُمكن تحقيق بيئة رقمية آمنة تُتيح للأفراد والمؤسسات الاستفادة من التكنولوجيا دون التعرض للمخاطر