الأمن السيبرانى.. ومكافحة الفساد وطنياً

بقلم: القاضى / حاتم جعفر
الرئيس بمحاكم الاستئناف
وخبير الأمن السيبراني والادلة الرقمية بالاتحاد الدولي للاتصالات

زاد الوعى العالمى بأهمية الأمن السيبرانى فى السنوات الأخيرة نتيجة للتطور الهائل فى طريقة استخدام التكنولوجيا ونوعية ذلك الاستخدام، الأمر الذى أدى إلى حتمية اللجوء لتلك الوسائل الجديدة مما ساعد وأسس فى ظهور مصطلح التحول الرقمى وزيادة نسبة الاعتمادية على تلك الوسائل. كما ظهرت بشكل واضح الضرورة الملحة للتوسع فى هذا التحول الرقمى مع ظهور وانتشار جائحة كورونا فى العالم والذى حول الأمر من اختيار ورفاهية إلى أسلوب حياة وحتمية لا غنى عنها ولا بديل لها، وهو ما دفع عجلة التحول الرقمى فى مصر نحو الانتشار لمزاياه العديدة ومنها توفير الوقت والجهد والمال وسهولة تقديم الخدمات للمواطنين وتمكينهم من الاستفادة بذلك التطور وهو ما يتماشى مع رؤية مصر ٢٠٣٠، وقد استتبع ذلك ضرورة تأمين تلك المعاملات الناتجة عن التحول الرقمى فى إطار متناسق ومتناغم مع باقى جهود الدولة بما يسمح بمنع ومكافحة الفساد فى تلك البيئة التكنولوجية وما نتج عنها من آليات جديدة وأساليب متطورة فى الفساد واحتياج ذلك لأساليب أكثر تطوراً فى منعه ومكافحته.

وقد اهتمت مصر بمجال الأمن السيبرانى منذ وقت مبكر كما سعت للريادة وتصدر المشهد العربى والإفريقى فى المؤشرات الدولية وكانت فى مقدمة الدول التى تسعى لاستمرارية التحسين وخلق تجربة ناجحة ورائدة فى الشرق الأوسط حيث حققت المركز التاسع عالمياً فى المؤشرالعالمى للأمن السيبرانى «GCI» لعام ٢٠١٤، وفى ضوء حوكمة الأمن السيبرانى على الصعيد الوطنى قامت مصر بإصدار الاستراتيجية الوطنية للأمن السيبرانى ٢٠١٧ -٢٠٢١ التزاماً بالاتجاهات العالمية الحديثة والتزاماً بالاستحقاقات الواردة بالدستور المصرى الصادر فى ٢٠١٤ فى المادة ٣١ من الدستور« أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذى ينظمه القانون» .

وقد سعت مصر نحو بناء وتأسيس منظومة حديثة قادرة على حماية الفضاء السيبرانى المصرى حيث تم إنشاء المجلس الأعلى للأمن السيبرانى برئاسة وزير الاتصالات وتكنولوجيا المعلومات، ويضم المجلس ممثلين من الحكومة والقطاع الخاص والمجتمع المدنى ويضم بين أعضائه ممثلا لهيئة الرقابة الإدارية. ويهدف المجلس إلى تعزيز الأمن السيبرانى فى مصر وحماية البنى التحتية الحيوية الحكومية والخاصة من الهجمات السيبرانية المحتملة .

وقد اتخذ المجلس العديد من القرارات المنظمة لتحقيق هذا الهدف، بما فى ذلك تطوير القدرات الوطنية للأمن السيبراني، وتعزيز التعاون الدولى فى هذا المجال بالإضافة للإشراف على تنفيذ الاستراتيجية الوطنية للأمن السيبرانى .

إن التعرض لدور الأمن السيبرانى فى مكافحة الفساد يتطلب التأكيد على أن الفساد ظاهرة اجتماعية وسياسية واقتصادية تهدد النظام العام والأمن القومى والتنمية المستدامة للدول، ويمكن تعريفه بأنه «انحراف أو تدمير للنزاهة فى أداء الوظائف العامة من خلال الرشوة والمحاباة» كما يمكن تعريفه بأنه «الأعمال غير النزيهة التى يقوم بها الأشخاص الذين يشغلون منصب فى السلطة وذلك لتحقيق مكاسب خاصة أو إساءة استغلال الموارد المتاحة».

والأمن السيبرانى كما عرفه الاتحاد الدولى للاتصالات هو، مجموعة الأدوات والسياسات والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتقنيات التى يمكن استخدامها فى حماية توفر وسلامة وسرية الأصول فى البنية التحتية الموصولة التابعة للحكومة والمنظمات الخاصة والمواطنين، وتشمل هذه الأصول أجهزة الحوسبة الموصولة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات والبيانات فى البيئة السيبرانية»

ومن أخطر أشكال الجرائم السيبرانية تلك التى تستهدف القطاعات الحكومية، خاصة المسؤولة منها عن مكافحة الفساد. فهذه القطاعات تحتاج إلى حماية عالية لبياناتها وأنظمتها من أى تدخل خارجى قد يهدف إلى التأثير على سير عملها ، أو يهدف إلى إفشاء معلومات سرية أو إلى تغيير نتائج التحقيقات أو إلى تشويه سمعتها أو إلى تعطيل خدماتها، وهذه الإجراءات هى عصب ما يهدف إليه الأمن السيبرانى من تحقيق ثلاثة أهداف رئيسية وهى

السرية CONFIDENTIALITY وهى منع الوصول للمعلومات إلا من خلال الأشخاص المصرح لهم وتحديد من له صلاحية التعديل أو الحذف أو الإضافة.

السلامة أو النزاهة INTEGRITY وهى ضمان صحة وسلامة المعلومات عند إدخالها أوحفظها أو انتقالها داخل النظام

التوافر AVAILABILITY وهو ضمان الوصول للمعلومة فى أى وقت وعدم تعطل ذلك ويعد المساس بأى مكون من المكونات الثلاثة السابقة خرقاً لإجراءات الأمن السيبرانى .

وبالنظر للتعريف السابق للأمن السيبرانى ومكوناته وتعريف الفساد نجد أن الأمن السيبرانى هو جهاز مكافحة الفساد فى النظم المؤتمتة وقواعد بياناتها بعد التحول الرقمى وكلما تم تطبيق سياسات الأمن السيبرانى بدقة زادت قدرة المؤسسة على منع ومكافحة الفساد مع الأخذ فى الاعتبار الاختراقات الخارجية وتطور التقنيات المستخدمة لكشف الثغرات وكذا التهديدات الداخلية INSIDER THREATS نتيجة لتواطؤ بعض الفاسدين داخل المؤسسة فخطر داخلى واحد يعادل جهود مؤسسات تحاول الاختراق من الخارج، لذا يجب العمل بصفة مستمرة على

توعية المستخدمين بأهمية الأمن السيبرانى ورفع قدراتهم.

تحديث الأنظمة والبرامج المستخدمة بشكل دورى ومتابعة ذلك

استخدام البرامج الأمنية للكشف عن الهجمات الالكترونية وتحليلها.

مواكبة التطور العالمى فى هذا المجال خاصة باستخدام تقنيات الذكاء الاصطناعى

يتكون الأمن السيبرانى دائماً من ثلاثة مكونات أساسية وهى « الأشخاص والإجراءات أو العمليات والتقنية « PEOPLE PROCESS TECHNOLOGY FRAMEWORK وهذه المكونات لابد أن تتكامل لتحقيق الأمن السيبرانى فشراء أحدث الأنظمة واتخاذ افضل الإجراءات لا يفيد مع عدم وجود كوادر واعية قادرة على فهم المنظومة والعمل بها كذلك وجود كوادر واعية وتقنيات حديثة متقدمة بلا إجراءات وسياسات واضحة اهدار للأموال، إذن فهو مثلث متكامل لا غنى فيه لشئ عن الاخر .

ولتحقيق الحوكمة السيبرانية CYBERSECURITY GOVERNANCE داخل مؤسسات الدولة وغيرها يجب تبنى استراتيجية للأمن السيبرانى تتضمن وضع أطر تشريعية وتنظيمية محكمة وسياسات معلنة تنظم الإجراءات والممارسات والمساءلة داخل الأنظمة الرقمية، كما يجب تحديد المسئوليات والصلاحيات بين الجهات القائمة التنفيذ والتدقيق بكل وضوح منعاً للتداخل، ووجود آليات محددة وواضحة للرقابة والمساءلة على القطاعين العام والخاص.

إن العلاقة بين الأمن السيبرانى ومكافحة الفساد علاقة طردية طول الوقت فكلما زاد الوعى والاهتمام بتطبيق معايير وضوابط الأمن السيبرانى زاد مقدار منع ومكافحة الفساد بالعمل على تمكين الحوكمة السيبرانية وهى عصب الأمن السيبرانى وكلما اتجهت الدول والمؤسسات لها تكون النتائج مبهرة لأن وجود سياسة سيبرانية واضحة ومحكمة ومعلنة تزيد الشفافية وتمكن من المراقبة تارة بتصنيف البيانات والمعلومات وتحديد صلاحيات المستخدمين فى الوصول إليها والقدرة

من أخطر أشكال الجرائم السيبرانية تلك التى تستهدف القطاعات الحكومية، خاصة المسؤولة منها عن مكافحة الفساد. فهذه القطاعات تحتاج إلى حماية عالية لبياناتها وأنظمتها من أى تدخل خارجى قد يهدف إلى التأثير على سير عملها ، أو إفشاء معلومات سرية أو تغيير نتائج التحقيقات أو تشويه سمعتها أو تعطيل خدماتها

اهتمت مصر بمجال الأمن السيبرانى منذ وقت مبكر وكانت فى مقدمة الدول التى تسعى لاستمرارية التحسين وخلق تجربة ناجحة ورائدة فى الشرق الأوسط حيث حققت المركز التاسع عالمياً فى المؤشرالعالمى للأمن السيبرانى «GCI» لعام ٢٠١٤، وفى ضوء حوكمة الأمن السيبرانى وعلى الصعيد الوطنى قامت مصر بإصدار الاستراتيجية الوطنية للأمن السيبرانى ٢٠١٧ -٢٠٢١ التزاماً بالاتجاهات العالمية الحديثة والتزاماً بالاستحقاقات الدستورية

على تعديلها وتارة بتحليل نتائج الأنظمة المؤتمتة، بعد أن كان مصطلح إعادة هندسة الإجراءات والرقابة عليها هو الطاغى قبل التحول الرقمى ووجود إجراءات وتعليمات محددة يتم محاسبة المخطئ والمقصر عليها أصبح فى ظل التحول الرقمى المعيار الأمثل للتدقيق والمراجعة هو وجود سياسات وضوابط للأمن السيبرانى وهو الأمر الذى تتضح معه أهمية الأمن السيبرانى ودوره الفعال فى منع ومكافحة الفساد، ولما كان مكافحة الفساد من أهم التحديات التى تواجه المجتمعات فى جميع أنحاء العالم، وتشكل التهديدات السيبرانية جزءاً أساسياً من هذه التحديات، لذلك تتطلب مكافحة الفساد بواسطة الأمن السيبرانى استخدام مجموعة واسعة من الأدوات والتطبيقات التى تساعد فى الكشف عن الجرائم السيبرانية والوقاية منها منعاً للفساد :-

- أدوات مراقبة الشبكات: تساعد فى رصد الأنشطة غير المشروعة على الشبكات وتحد المخاطر السيبرانية والهجمات الإلكترونية ويفضل أن يتم ذلك من خلال "NETWORK OPERATIONS CENTER"
- أدوات تحليل البيانات وهى تستخدم لتحديد أنماط غير عادية أو مشبوهة ووفقاً لتصورات تتناسب وطبيعة قواعد البيانات والوظائف.
- أدوات تشفير البيانات وفك التشفير والتى تستخدم لحماية البيانات الحساسة .
- أدوات الحماية من الفيروسات والبرامج الخبيثة والعمل على حجبها وإزالتها.
- أدوات ادارة الهوية والوصول والتحقق من المستخدمين المخولين.
- أدوات إدارة الصلاحيات والتى تعمل على إدارة وتعيين صلاحيات الحسابات.
- أدوات إدارة الحوادث السيبرانية والتى تساعد فى استعادة الأنظمة والبيانات .

إن التحدى الحقيقى فى المرحلة الحالية هو الانتقال للتحول الرقمى دون القدرة على مواكبة ذلك بغطاء قوى وأساس متين للأمن السيبرانى وهو ما يعد بحد ذاته فساد فى المسار الإداري، لأن حجم النفقات على الأمن السيبرانى فى المؤسسات لا يمثل واحد بالمائة من حجم الخسائر خاصة فى بعض هجمات فيروس الفدية وتشفير البيانات وكذا تسريب البيانات الحساسة خاصة أنه يدخل ضمن الأصول الرقمية المطلوب حمايتها والبُنى التحتية للدولة خاصة الحرجة منها ويكفى أن نقول إنه من المتوقع أن تتجاوز تكلفة الهجمات الإلكترونية على الاقتصاد العالمي حاجز الـ ١١,٥ تريليون دولار أميركى فى ٢٠٢٣، و بأن ترتفع التكلفة العالمية للجرائم السيبرانية إلى ٢٣ تريليون دولار أميركى بحلول عام ٢٠٢٧.

لدينا تحديات جمة ومخاطر كُثر إلا أن التحديات الخاصة بمكافحة الفساد وخاصة السيبرانية تمثل نمطا جديدا يتطلب القدرة على مواجهته وصده منذ إعداد الدراسة التحليلية للأنظمة والاستفاضة فى شرح سبب منح ومنع الصلاحيات مرورا بإختبار الكود المصدرى للنظام وفحص مواضع الضعف وعلاجها وصولا لتقارير تقييم ومؤشرات الأداء لكامل النظام، فتحديد الصلاحيات وفقاً للصفات والمسميات الوظيفية على النظام يعمل على ضبط الأداء وحوكمة الاختصاصات وعماد ذلك ومرده أن« المعرفة قدر الحاجة» والحاجة معيارها فى هذا الصدد الصفة الوظيفية وهى التى تمنع أى فساد ناتج عن تداخل الاختصاصات أو عدم وضوحها أو استغلال المستخدمين لأن كل صاحب صلاحية مطالب بالحفاظ عليها والزود عنها بقدر تحمل مسئولية الإخلال بها أو المساس بما ينسب إليه داخل النظام الالكترونى لانه لا مجال لانكار المسئولية فى ظل تحديد الهويات الرقمية وضمانية الوصول بالاشتراطات الخاصة بكل مستخدم من خلال نظم التحقق من الهويات وغيرها، كما أن العمل داخل أنظمة الدولة خاصة فى حال اختلافها وتباين تقنياتها وهيكلية بنائها يتطلب قدرا عاليا من الخبرة والمرونة فى مجال تأمينها وتحليل بياناتها ومعالجتها بمراعاة القوانين واللوائح المنظمة فالبيانات الضخمة «BIG DATA» هى بترول المستقبل وكشف أنماط التلاعب فيها هى قدرة تحليل هذا البترول ومنع ومكافحة الفساد فيه .