سياسات الاستجابة للتهديدات السيبرانية في القارة الأفريقية

أ. أسامة منير أحمد[*]

أ.د. صبحى قنصوة [**] **د. أحمد أمل**[***]

• **مُلخص:**

يشكلَ الأمنُ السيبراني تحديا رئيسيا للجهودِ الراميةِ إلى استفادةِ دولِ القارةِ الأفريقيةِ منْ التطبيقاتِ الحديثةِ في مجالِ تكنولوجيا المعلوماتِ والاتصالاتِ ، في دفعِ عجلةِ النموِ الاقتصاديٍ وتطويرِ الهياكلِ المؤسسيةِ، حيثُ صاحبُ زيادةِ اعتمادِ الحكوماتِ الأفريقيةِ على التقنياتِ الرقميةِ الحديثةِ ، تعرضَ البيئةَ الرقميةَ الأفريقيةَ لمختلفِ صورِ التهديداتِ السيبرانية؛ مما أدى إلى تحركِ المنظماتِ الأفريقيةِ المتعددةِ الأطرافِ المتمثلةِ في الاتحادِ الأفريقيٍ والتجمعاتِ الاقتصاديةِ الإقليميةِ لوضعِ الأطرِ الفنيةِ والقانونيةِ التي تهدفُ إلى الحدِ منْ الآثارِ السلبيةِ المترتبةِ على التهديداتِ السيبرانيهْ، وتكفلَ تنسيقَ التعاونِ بينَ الجهاتِ المعنيةِ بدولِ القارةِ لتوفيرِ بيئةٍ رقميةٍ أفريقيةٍ آمنةٍ.

أظهرَ مؤشرُ الأمنِ السيبراني العالميَ الصادرِ عنْ الاتحادِ الدوليٍ للاتصالاتِ (GCI-2020؛ تباينا في تقييمِ القدراتِ الأفريقيةِ على التعاملِ معَ التهديداتِ السيبرانيهْ، حيثُ تبينَ وجودُ بعضِ الدولِ الأفريقيةِ ضمنَ الدولِ المتقدمةِ في مجالِ الأمنِ السيبراني، على عكسِ تقييمِ القارةِ الأفريقيةِ الذي جاءَ الأضعفَ بينَ مختلفِ مناطقِ العالمِ؛ مما يعدُ مؤشرٌ على اعتمادِ الدولِ الأفريقيةِ على قدراتها في التعاملِ معَ قضايا الأمنِ السيبرانيْ دونِ الوضعِ في الاعتبارِ البعدِ الإقليميٍ والقاريٍ لتلك القضايا، مما قدْ يشكلُ عائقا أمامَ الاستراتيجية الأفريقيةِ للتحولِ الرقميٍ، القائمةُ على زيادةِ أوجهِ التعاونِ بينَ دولِ القارةِ منْ خلالِ منظوماتٍ رقميةٍ تكامليةٍ تحققُ أهدافَ التنميةِ المستدامةِ لدولِ القارةِ.

الكلمات المفتاحية: الأمن السيبرانى، التهديدات السيبرانيه، سياسات الإستجابة، الإطار القارى، الإطار الإقليمى

---

[*] باحث دكتوراه بقسم السياسة والاقتصاد بكلية الدراسات الأفريقية العليا– جامعة القاهرة

[**] أستاذ العلوم السياسية بكلية الدراسات الأفريقية العليا – جامعة القاهرة

[***] أستاذ العلوم السياسية المساعد بكلية الدراسات الأفريقية العليا – جامعة القاهرة

- **Abstract**

Modern technology has led to economic growth and institutional development in African countries. However, this progress has also made the African digital environment more vulnerable to cyber threats. To address this issue, multilateral organization sincluding the African Union and regional economic groupings have established frameworks to harmonize cybersecurity legislation among member states; The ranking of African countries according to the Global Cybersecurity Index issued by the International Telecommunication Union (GCI-2020) showed that Some African countries rank highly in cybersecurity, in contrast to the evaluation of the African continent among the various regions of the world; It indicates that African countries rely more on national capabilities to face cyber threats. This indication may challenge the goal of increasing cooperation between African countries through digital systems for sustainable development.

Keywords: cyber security, Cyber thrteats for Africa, GCI regional ranking, African digital environment

- **مقدمة:**

أدتْ التطوراتُ المتلاحقةُ فى مجال تكنولوجيا المعلوماتِ والإتصالاتِ إلى ظهورِ الكثيرِ منْ التطبيقاتِ الرقميةِ الحديثةِ مثلِ الحوسبةِ الكميةِ والشبكاتُ المعرفةُ بالبرمجياتِ (SDN)، والتمثيلُ الافتراضيُ لوظائفِ الشبكةِ (FVN)، وتحليلَ البياناتِ الضخمةِ (BDA)، والذكاءُ الإصطناعيُ (AI)، وغيرها منْ التطبيقاتِ التي صاحبت إطلاق الجيلِ الخامسِ منْ تكنولوجيا الاتصالاتِ (5G)، مما ترتب عليه زيادةِ خطورةِ التهديداتِ السيبرانية واختلافِ طبيعتها ودرجة تأثيرها، الأمر الذي يجعلُ الأمنُ السيبراني ديناميا ومعقدا على نحوٍ متزايدٍ، في ظلِ حداثةِ استخدام تلكَ التطبيقاتِ وشدةِ التعقيدِ التي تتسمُ بهِ التصميماتُ الخاصةُ بها.

على غرارِ الكثيرِ منْ دولِ العالمِ عانتْ البلدانُ الأفريقيةُ منْ زيادةِ حجمِ التهديداتِ السيبرانيةْ الناجمةَ عنْ اتجاهِ الكثيرِ منْ دولِ القارةِ إلى زيادةِ الاعتمادِ على تطبيقاتِ تكنولوجيا المعلوماتِ والاتصالاتِ ، لتواكب المتغيراتِ السياسيةَ والاقتصاديةَ المرتبطةَ بالتحولِ الرقميِ على الصعيدِ الدولي، بدأً منْ مختلفِ صورِ الجريمةِ السيبرانيةْ منْ حالاتِ الاختراقِ منْ قبلُ الأفرادِ والمجموعاتِ منْ قراصنةِ شبكةِ المعلوماتِ الدوليةِ (الإنترنت)، وصولاً إلى الهجماتِ السيبرانية المحدودةَ والشاملةِ، والتي يتمُ تصنيفها طبقا للأدواتِ التقنيةِ التي تمَ استخدامها، والأهدافُ التي تكمنُ وراءَ تنفيذها؛ بالإضافةِ إلى الأنشطةِ الإجراميةِ لعصاباتِ الجريمةِ المنظمةِ العابرةِ للحدودِ، وأنشطةُ الجماعاتِ الإرهابيةِ على شبكةِ المعلوماتِ الدوليةِ (الإنترنت).

أسفرتْ التهديداتُ السيبرانيةْ للبيئةِ الرقميةِ بمختلفِ البلدانِ الأفريقيةِ عنْ العديدِ منْ الآثارِ السلبيةِ على مختلفِ النواحي الاقتصاديةِ، والتي انعكستْ بدورها على المجالاتِ السياسيةِ والاجتماعيةِ، بصورةٍ تهددُ الاستقرارَ على الصعيدِ الداخليِ بحيثُ أصبحتْ التقنياتُ التكنولوجيةُ الحديثةُ أحدَ أهمِ التهديداتِ التي تواجهُ الأمنَ القوميَ للعديدِ منْ دولِ القارةِ، الأمرُ الذي أدى إلى تحركِ المنظماتِ الأفريقيةِ المتعددةِ الأطرافِ لوضعِ الأطرِ الفنيةِ والقانونيةِ اللازمةِ للحدِ منْ تلكَ التهديداتِ؛ حيثُ طرحَ الاتحادُ الأفريقيُ

اتفاقيةَ الأمنِ السيبراني وحمايةُ خصوصيةِ البياناتِ، والتي تهدفُ إلى توفيرِ أكبرَ قدرا منْ الحمايةِ للفضاءِ السيبراني للقارةِ منْ خلالِ نظامٍ إيكولوجيٍ يتسمُ بالمرونةِ، يتيحَ التوافقُ بينَ الأطرِ التشريعيةِ والإجرائيةِ معَ التغيراتِ المطردةِ لتكنولوجيا المعلوماتِ والاتصالاتِ، كما لعبتْ التجمعاتُ الاقتصاديةُ الإقليميةُ دوراً محورياً في وضعِ أسسِ التعاونِ بينَ دولِ الإقليمِ لمجابهةِ التحدياتِ التي تفرضها الآثارُ السلبيةُ للتهديداتِ السيبرانيةْ المرتبطةَ بالتطورِ التكنولوجيِ،والتي قدْ يترتبُ عليها عدمِ الاستقرارِ السياسيِ والاجتماعيٍ على الصعيدِ الداخليٍ للدولِ الأعضاءِ.

إنطلاقا منْ نظريةِ مركبِ الأمنِ الإقليميِ (Regional SecurityComplex) أحدَ النظرياتِ القائمةِ على أساسِ نظريةِ الدراساتِ الأمنيةِ لمدرسةِ كوبنهاجن، تستعرضَ الدراسةُ سياساتِ الاستجابةِ للتهديداتِ السيبرانية في القارةِ الأفريقيةِ؛ حيثُ ينطوي الأمنُ السيبراني على التعاملِ معَ مجموعةٍ منْ التهديداتِ التى ترجعُ أهميتها السياسيةَ إلى ربطها معَ آثارها المرجعيةِ؛ أيْ أنَ "أمنَ الشبكةِ" و"الأمنُ الفرديُ" تتبعُ أهميتها السياسيةَ منْ خلالِ ربطها معَ الثوابتِ المرجعيةِ الجماعيةِ "الدولةِ" و"المجتمعُ" و"الأمةَ"، وإضافةُ الآثارِ السياسيةِ والمعياريةِ إلى البعدِ الأمنيِ؛ في ظل ارتباط التحولاتِ السياسيةِ بالبعدِ الديناميكيِ للتهديداتِ الأمنيةِ المعاصرةِ، والتي أصبحَ الكثيرُ منها يؤثرُ على وجود الفرد، والمجتمعِ، والدولةِ، بلْ وتهديدا إقليميا وعالميا.

وللوقوف على مدى ملائمة الاجراءت التي اتخذتها العديد من الدول الأفريقية للتعامل مع التهديدات الناجمة عن التطورات التكنولوجية الحديثة، سيتم تناول سياسات الاستجابة الأفريقية للتهديدات السيبرانية من خلال مبحثين:

المبحث الأول: دور المنظمات متعددة الأطراف في تحقيق الأمن السيبراني في القارة الأفريقية

المبحث الثاني: جهود تحقيق الأمن السيبراني بالقارة الأفريقية.

المبحث الأول

دور المنظمات متعددة الأطراف في تحقيق الأمن السيبراني في القارةالأفريقية

تلعب المنظمات المتعددة الأطراف دورًا محوريًّا في تنسيق المواقف السياسية نحو التعامل مع المهددات الأمنية المختلفة بين الدول الأعضاء بها؛ استنادًا على الروابط الاجتماعية والاقتصادية التي تربط بينهم، والخبرات السابقة المكتسبة من الصراعات التي عانت خلالها الدول الأعضاء من حالة عدم الاستقرار، مما يؤهلها للعب دورا محورياً لمجابهة التهديدات السيبرانيه طبقا لما سيتم عرضه على النحو التالى:

أولاً: الإطار القاري لسياسات الأمن السيبرانى

يعدّ التعاونُ بينَ الدولِ على المستوى الإقليمي والقاريٍ إحدى ركائزِ التعاونِ على الصعيدِ الدولي، حيثُ فرضتْ الطبيعةُ اللاحدودية للتهديداتِ السيبرانيةْ؛ واقعَ التعاونِ الدولي لمجابهتها والحدِ منْ الآثارِ المترتبةِ عليها، وتضمنتْ دراسةُ جويسْ حكمهُ، وكيرستينْ فينيارڈ[1]؛ عنْ الجريمةِ السيبرانيةْ والأمنُ الدوليُ على أهميةِ الدورِ الذي تلعبهُ التجمعاتُ الإقليميةُ في تعزيزِ الاستقرارِ والأمنِ، وإيجادَ شكلٍ منْ أشكالِ التعاونِ بينَ مجموعةِ الدولِ التي تشكلُ الإقليمَ لمجابهةِ التحدياتِ التي تفرضها التغيراتُ على الصعيدِ الدولي والإقليميٍ؛ حيثُ تلعبُ المنظماتُ الإقليميةُ دورا هاما ومحوريا لمزيدٍ منْ التعاونِ على المستوى متعددٍ الأطرافِ، ولا سيما في مجالِ الأمنِ السيبراني، نظرا لصعوبةِ الوصولِ إلى اتفاقيةٍ دوليةٍ ملزمةٍ متعددةٍ الأطرافِ للتعاملِ معَ التهديداتِ السيبرانية في ظلِ التناقضِ الأيديولوجيٍ واختلافِ الأولوياتِ وتباينِ الآراءِ حولَ المبادئِ الحاكمةِ لاستخدامِ الفضاءِ السيبراني وإمكانيةُ تطبيقِ القانونِ الدولي في صيغتهِ الحاليةِ على الأنشطةِ غيرِ المشروعةِ باستخدامِ التقنياتِ الرقميةَ الحديثةِ والتيتهددُ الأمنَ والسلمَ الدوليَ؛ وطبقا لما وردَ بالدراسةِ تتمثلُ دورَ الجهودِ الإقليميةِ في مجالِ الأمنِ السيبراني في الآتي:

1- J. Hakmeh, K. Vignard. ICTs, International Security and Cybercrime: **Understanding theirIntersections for Better Policymaking**, (Switzerland: Geneva, UNIDIR, 2021).

1 – بناءُ الوعي: منْ خلالِ إظهارِ الدورِ الحيويِ الذي يلعبهُ الأمنُ السيبراني في عملية التحولِ الرقمي وزيادةُ الاعتمادِ على التطبيقاتِ التكنولوجيةِ الحديثةِ المتصلةِ بشبكةِ المعلوماتِ الدوليةِ (الإنترنت) في تقديمِ الخدماتِ الحكوميةِ ومختلفَ الأنشطةِ الاقتصاديةِ مثلِ التجارةِ الإلكترونيةِ والتحويلاتِ النقديةِ، وغيرها منْ الأنشطةِ المرتبطةِ بالحياةِ اليوميةِ لأفرادِ المجتمعِ، ومدى أهمية ذلك الدور في تحقيقِ التنميةِ الاقتصاديةِ والاجتماعيةِ وتحقيقِ الأهدافِ التنموية للدولةِ.

2 – بناءُ القدراتِ: منْ خلالِ وضعِ آلياتٍ تنظمُ تبادلَ الخبراتِ وأفضلُ الممارساتِ التقنيةِ والتشريعيةِ بينَ دولِ الإقليمِ والتي تسهمُ في تطويرِ قدراتِ كلِ الأطرافِ الفاعلةِ في معادلةِ الأمنِ السيبراني، والتي تشملُ على الكوادرُ البشريةُ المؤهلةُ والمدربةُ على التعاملِ معَ كلِ الجوانبِ المتعلقةِ بالتقنياتِ الرقميةِ ولا سيما التداعياتُ الناجمةُ عنْ الهجماتِ السيبرانية، ومتخذي القرارِ منْ الساسةِ وممثلي السلطاتِ التشريعيةِ لوضعِ الأطرِ القانونيةِ والتشريعاتِ اللازمةِ لإنشاءِ الهياكلِ التنظيميةِ ووضعِ الاستراتيجياتِ الوطنيةِ للأمنِ السيبراني.

3 – التعاونُ وبناءُ الثقةِ: وتتمثلَ في وضعْ أطرَ التعاونِ بينَ دولِ الإقليمِ لمواجهةِ التحدياتِ الناجمةِ عنْ طبيعةِ التهديداتِ السيبرانية العابرةَ للحدودِ، والتي تشملُ على الاتفاقياتِ والبروتوكولاتِ المنظمة لترتيباتِ الأمنِ السيبراني على المستوى الإقليميِ والدولي، والتي تكفل مشاركةِ كافة الجهات المعنية بالتعامل مع القضايا المتعلقة بالأمن السيبرانى من العناصر الفنية، وعناصرِ إنفاذِ القانونِ في الدولِالأعضاءِ، وتنظيمِ عمليةِ تبادلِ البياناتِ والمعلوماتُ الخاصةِ بمختلف التهديدات السيبرانية وخاصة التي تتعلق بالجريمة السيبرانيه وتسهمُ في تعقبِ مرتكبيها دونَ المساسِ بالحقوقِ الدستوريةِ للمواطنينَ ويكفل احترامُ سيادةِ الدولِ على أراضيها.

وعلى صعيدِ القارةِ الأفريقيةِ تعدْ دراسةُ تنسيقِ وتنظيمِ سياساتِ الاتصالاتِ وتكنولوجيا المعلوماتِ في دولِ القارةِ منْ خلالِ وضعِ سياسةٍ إقليميةٍ منسقةٍ وإطارٍ

تنظيمي قاريْ، هيَ إحدى الخطواتِ الرئيسيةِ للاتحادِ الأفريقي لتوفيرِ بيئةٍ رقميةٍ أفريقيةٍ آمنةٍ تسهمُ في تنامي الاعتمادِ على التطبيقاتِ الرقميةِ الحديثةِ بينَ دولِ القارةِ، حيثُ تضمنَ مشروعُ تقريرِ الاتحادِ الأفريقي حولَ انتشارِ التقنياتِ التكنولوجيةِ الحديثةِ على نطاقٍ واسعٍ بدولِ القارةِ، على الكثيرِ منْ القضايا الناشئةِ التي يلزمُ معالجتها في بيئةِ تكنولوجيا المعلوماتِ والاتصالاتِ الأفريقيةِ؛ أبرزها مكافحةُ الجرائمِ السيبرانية بجميعِ أشكالها (القرصنةُ، ونشرَ الفيروساتِ والبرامجِ الخبيثةِ، واحتجازَ البياناتِ، والاحتيالُ على بطاقاتِ الائتمانِ ... إلخْ)، وأهميةُ تعزيزِ الأمنِ السيبراني بدولِ القارةِ[1].

بينما تضمنَ إعلانُ أوليفرْ تامبو (Oliver Tambo Declaration) الصادرَ عنْ الجلسةِ الاستثنائيةِ لوزراءِ الاتصالاتِ وتكنولوجيا المعلوماتِ والتي عقدتْ بجمهوريةِ جنوبَ أفريقيا في إطارِ مبادرةِ مجتمعِ المعلوماتِ الأفريقي، على أهميةِ إعدادِ اتفاقيةٍ قاريةٍ بالتعاونِ معَ لجنةِ منظمةِ الأممِ المتحدةِ الاقتصاديةِ المعنيةِ بقارةِ أفريقيا(UNECA)؛ لتنظيمِ التشريعاتِ التي تتلاءمُ معَ اتجاهِ دولِ القارةِ إلى زيادةِ الاعتمادِ على التطبيقاتِ التكنولوجيةِ الحديثةِ في مختلفِ المجالاتِ وبخاصةٍ في المجالاتِ الاقتصاديةِ، والذى يتطلبُ وضعَ مجموعةٍ منْ الأطرِ التي تنظمُ المعاملاتُ الإلكترونيةُ والأمنُ السيبراني وحمايةُ البياناتِ الشخصيةِ[2].

أسفرت الجهود الأفريقيةِ لوضعِ إطارِ قاريٍ يختصُ بالحدِ منْ التهديداتِ الناجمةِ عنْ استخدامِ تطبيقاتِ تكنولوجيا الاتصالاتِ والمعلوماتِ بدولِ القارةِ، عنْ اعتمدَ رؤساءُ دولِ وحكوماتِ الاتحادِ الأفريقي النسخةِ المنقحةِ منْ مشروعِ الاتفاقيةِ، بعدُ إدراجِ التعديلاتِ اللازمةِ للتغلبِ على الاعتراضاتِ التي واجهتهُا، خلالَ الدورةِ العاديةِ الثالثةِ والعشرينَ لمؤتمرِ الاتحادِ الأفريقي في مالابو عام (2014)، وأطلقَ عليها اسمُ اتفاقيةِ الاتحادِ

1- African Union. **Study on harmonization of telecommunication, information and communication technologies policies and regulation in Africa**,Draft Report March 2008

2- African Union. extra-ordinary conference of African union ministers in charge of communication and information technologies Johannesburg, South Africa 2009, "**Oliver Tambo Declaration** "

الأفريقي للأمنِ السيبراني وحمايةُ البياناتِ الشخصيةِ، وتهدفَ الاتفاقيةُ إلى موائمةِ قوانينِ الدولِ الأفريقيةِ بشأنِ التجارةِ الإلكترونيةِ، وحمايةُ البياناتِ، ومكافحةُ الجرائمِ السيبرانية، منْ خلالِ نهجٍ شاملٍ لإدارةِ وحوكمةِ البيئةِ الرقميةِ الأفريقيةِ والعملِ على الحدِ منْ انتشارِ الجرائمِ السيبرانية التي تشكلُ تهديدا حقيقيا لأمنِ الشبكاتِ الرقميةِ والبنيةِ التحتيةِ التكنولوجيةِ، وتؤثرُ بالسلبِ على جهود التنميةِ بدولِ القارةِ.[1]

وتضمنتْ بنودُ الاتفاقيةِ على التزاماتِ الدولِ الموقعةِ عليها منْ الدولِ الأعضاءِ بالاتحادِ طبقا للآتي:

1 – فيما يتعلقُ بحفظِ البياناتِ وضعتْ الاتفاقيةُ الأطرَ المنظمةَ لحمايةِ حفظِ وتداولِ البياناتِ على المستوى الوطنيِ أوْ بينَ الدولِ الأعضاءِ كمايلىْ:

أ– يتعينَ على كلِ دولةِ تشكيلِ هيئةٍ مسئولةٍ عنْ حمايةِ البياناتِ الوطنيةِ (DPA)، على أنْ يتوافرَ لها منْ السلطاتِ القانونيةِ والإداريةِ ما يكفلُ ضمانَ معالجةِ البياناتِ في الأغراضِ المشروعةِ، ووضعَ الإجراءاتِ التنظيميةِ الخاصةِ بعملياتِ حفظِ وتداولِ البياناتِ، والتي تتضمنُ المدةُ الزمنيةُ المحددةُ لتلكَ العملياتِ وبما يتفقُ معَ الغرضِ التي تمتْ منْ أجلهِ، معَ وجودِ استثناءاتٍ لأغراضِ المصلحةِ العامةِ ، مثلٌ البياناتِ المتعلقةِ بالوقائعِ التاريخيةِ، أوْ الدراساتِ الإحصائيةِ أوْ العلميةِ ووفقا للاتفاقيةِ.

ب– طبقا للمادةِ رقمِ (14) لا يجوزُ للمسئولِ عنْ معالجةِ البياناتِ ذاتِ الطابعِ الشخصي نقلها إلى دولةٍ ليستْ عضوا في الاتحادِ الأفريقي، ما لمْ تضمنْ هذهِ الدولةِ مستوى كافيا منْ حمايةِ الحياةِ الخاصةِ والحرياتِ والحقوقِ الأساسيةِ للأشخاصِ الذينَ تخضعُ بياناتهمْ للمعالجةِ أوْ منْ المحتملِ أنْ تتمَ معالجتها، إلا في حالةِ الحصولِ على تصريحٍ قانونيٍ منْ السلطةِ الوطنيةِ المسئولةِ عنْ حمايةِ

1- African Union. "**AU Convention on Cyber Security and Personal Data**",adopted at the 23rd Ordinary Session of the Assembly of the African Union (Malabo, 27th June 2014)

البياناتِ، ويحقَ للسلطةِ الوطنيةِ المسئولةِ حجبَ أوْ قصرِ الاطلاعِ على البياناتِ التي تخصُ الموضوعاتُ ذاتُ درجاتِ السريةِ والتي ينتجُ عنْ تسريبها تهديد للأمنِ القومي للدولةِ والتي تحددُ ضمنَ التشريعاتِ الوطنيةِ لكلِ دولةٍ.

2- وفيما يختصُ بالأمنِ السيبراني اشتملتْ الاتفاقيةُ على العديدِ منْ النصوصِ الخاصةِ بالتزاماتِ الدولِ الأعضاءِ بالاتحادِ، حيثُ تناولَ الفصلُ الثالثُ منْ الاتفاقيةِ تعزيزَ الأمنِ السيبراني ومكافحةُ الجريمةِ السيبرانية طبقا للآتي[1]

أ – تنصَ المادةُ رقمٌ (24) على تبني الدولِ الأعضاءِ لإستراتيجيات وطنيةٍ مناسبةٍ للأمنِ السيبراني تتناسبَ معَ حجمِ المخاطرِ التي تواجهها الدولةُ، على أنْ تتضمنَ على مجموعةٍ منْ الأهدافِ القوميةِ، وآلياتُ تنفيذها منْ خلالِ خطةٍ زمنيةٍ محددةٍ، كما تتضمنُ على الهياكلِ التنظيميةِ للجهاتِ المعنيةِ بتنفيذِ الاستراتيجيةِ والمهامِ التي تختصُ بها.

ب- ووفقا للمادةِ رقمٍ (25) تلتزمُ كلَ دولةٍ بوضعِ التدابيرِ التشريعيةِ والتنظيميةِ التي تراها فعالةً، لتجريمِ كافةِ الأنشطةِ التي تؤثرُ على عملِ الأنظمةِ الرقميةِ، منْ خلالِ استخدامِ البرامجِ والتطبيقاتِ التي تسهمُ في التأثيرِ على سريةِ البياناتِ التي تعالجها تلكَ المنظوماتِ أوْ تحفظِ بها، أوْ تعملُ على الأضرارِ بالبنيةِ التحتيةِ للشبكاتِ الرقميةِ، على أنْ تتولى الجهاتُ القانونيةُ الموجودةُ حاليا، أوْ التي تنشأُ بموجبُ تلكَ التشريعاتِ مسئوليةَ متابعةِ وملاحقةِ المخالفينَ؛ معَ مراعاةِ ضمانِ حقوقِ المواطنينَ التي نصَ عليها دستورُ الدولةِ، أوْ التي تحميها الاتفاقياتُ الدوليةُ لا سيما الميثاقُ الأفريقيُ لحقوقِ الإنسانِ والشعوبِ، والعهدُ الدوليُ لحقوقِ الإنسانِ.

1- Orji, Uchenna. "The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?". **Masaryk University Journal of Law and Technology,** (Czech Republic: Institute of Law and Technology, Faculty of Law, Vol.12, No.2**,** 2018). Pp 91–130.

ج – تضمنتْ المادةُ رقمٌ (26) على التزامِ الدولِ الأعضاءِ بتطويرِ القدراتِ الوطنيةِ وخلقِ ثقافةِ الأمنِ السيبراني، واتخاذَ التدابيرِ اللازمةِ لبناءِ القدراتِ وتثقيفِ وتدريبِ أصحابِ المصلحةِ ذوي الصلةِ، منْ خلالِ إعدادِ وتنفيذِ برامجَ ومباداراتْ توعيةً لمستخدمي الأنظمةِ والشبكاتِ في المؤسساتِ الحكوميةِ والقطاعِ الخاصِ ، ووضعَ المعاييرِ الخاصةِ بتدريبِ المهنيينَ العاملينَ في مجالِ تكنولوجيا المعلوماتِ والاتصالاتِ، وتطويرَ الشراكاتِ معَ القطاعِ الخاصِ ومنظماتُ المجتمعِ لوضعِ الأسسِ اللازمةِ للتعاونِ البناءِ في كلِ المجالاتِ الداعمةِ للجهودِ الحكوميةِ في المجالاتِ ذاتِ الصلةِ بنشرِ الوعيِ والأمنِ السيبراني.

د - نصتْ المادةُ رقمٌ (27) على القواعدِ التنظيميةِ الخاصةِ بإنشاءِ الهياكلِ الوطنيةِ الخاصةِ برصدِ ومتابعةِ التهديداتِ الناجمةِ عنْ استخدامِ تكنولوجيا المعلوماتِ والاتصالاتِ والتعاملِ معها في إطارٍ مؤسسيٍ ، لتوفيرِ حوكمةِ الأمنِ السيبراني، والحدُ منْ الاستخدامِ الغيرِ مشروع للتقنياتِ الرقميةِ علاوةً على وضعِ آلياتِ الاستجابةِ للنتائجِ المترتبةِ على تعرضِ الدولةِ لأيِ شكلِ منْ أشكالِ التهديداتِ السيبرانية وبخاصةَ استخدامَ العناصرِ الإجراميةِ للفضاءِ السيبراني وبما يكفلُ تأمينَ المكتسباتِ الاقتصاديةِ والاجتماعيةِ للدولِ الأعضاءِ.

هـ – وضعتْ المادةُ رقمٌ (28) المبادئُ الرئيسيةُ للتعاونِ على المستوى الإقليميِ والدوليِ، حيثُ ألزمتْ الدولُ الأعضاءُ باتخاذِ التدابيرِ التشريعيةِ التي تسمحُ بتبادلِ المعلوماتِ والبياناتِ حيالَ الجرائمِ السيبرانية وتتبعَ المشاركينَ فيها، والتوسعُ في توقيعِ الاتفاقياتِ الثنائيةِ ومتعددةِ الأطرافِ بينَ الدولِ الأعضاءِ وفقا لمبدأِ المسئوليةِ الجنائيةِ المزدوجةِ وبخاصةٍ بينَ الدولِ التي لمْ يسبقْ لها التعاونُ في مجالِ المساعدةِ الجنائيةِ، والالتزامُ بوضعِ آلياتٍ لتبادلِ المعلوماتِ حيالَ التهديداتِ السيبرانية وأنسبُ الطرقِ للتعاملِ معها منْ خلالِ التعاونِ ونقلِ الخبراتِ بينَ الجهات المعنية بالدولِ الأعضاءِ منْ جهةٍ؛ أوْ من خلال التعاونِ مع الدول ذات القدرات الفنية المتميزة فى هذا المجال فى إطار التعاون الدولى منْ جهةٍ أخرى.

وتتولى مجموعةٌ منْ الخبراءِ المتخصصينَ تحتَ مسمى فريقِ خبراءِ الأمنِ السيبراني التابعَ للاتحادِ الأفريقي (AUCSEG) التنسيقِ، وتبادلَ المعلوماتِ بينَ مختلفِ أصحابِ المصلحةِ منْ مستخدمي التطبيقاتِ الرقميةِ الحديثةِ، منْ الدولِ الأعضاءِ بالاتحادِ، والتجمعاتُ الاقتصاديةُ الإقليميةُ، والقطاعُ الخاصُ، ومنظماتُ المجتمعِ المدنيِ، بشأنَ الإستراتيجياتِ والمبادراتِ الوطنيةِ، والإقليميةَ، والقاريةَ في مجالِ الأمنِ السيبراني، وأولوياتُ تنفيذها؛ فضلاً عنْ وضعِ البرامجِ الخاصةِ ببناءِ القدراتِ فيما يتعلق بكافةَ الجوانبِ المرتبطة بقضايا الأمن السيبرانى (السياسةُ، التكنولوجيا، وتنميةُ المهاراتِ ... الخ) ومع مراعاة ملائمتها لاحتياجاتِ الدولِ، بالإضافةِ إلى معاونةِ دولِ القارةِ في إنشاءِ فرقِ التعاملِ معَ الحالاتِ الطارئةِ الناتجةِ عنْ الهجماتِ السيبرانية والتخفيفُ منْ آثارها(CERTs/CIRTs/CSIRT)، فضلاً عنْ تعزيزِ قدراتِ سلطاتِ العدالةِ الجنائيةِ المعنيةِ بالتحقيقِ في الجرائمِ السيبرانية منْ خلالِ توفيرِ الإمكاناتِ والقدراتِ الفنيةِ والعناصرِ المدربةِ على جمعِ وتحليلِ الأدلةِ الإلكترونيةِ المرتبطةِ بالأنشطةِ غيرِ المشروعةِ التي يتمُ ارتكابها بواسطةِ التطبيقاتِ التكنولوجيةِ الحديثةِ منْ خلالِ عمليةِ التشريحِ الإلكتروني (Digital forensics).[1]

كما سعى الاتحادُ الأفريقيُ للتعاونِ معَ منظماتِ المجتمعِ المدني منْ ذوي الخبرةِ لتطويرِ الأطرِ القانونيةِ والفنيةِ للبيئةِ الرقميةِ الأفريقيةِ،وتعد المبادئُ الرئيسيةُ لحمايةِ خصوصيةِ البياناتِ الشخصيةِ لمستخدمي التطبيقاتِ الرقميةِ، أحد ابرز أوجه التعاون بين الاتحاد الأفريقى ومنظمات المجتمع المدنى الممثلة فى منظمةِ مجتمعِ الإنترنت العالميةِ (Internet socity)، حيث ساهم مجموعة منْ الخبراءِ التابعين للمنظمة فى إعداد تلك المبادئ بما يتفق مع الاتفاقات الدولية المنظمةِ لذلك.[2]

1−African Union. “Cyber Security Expert Group Terms of Reference”, **the 32nd Ordinary Session of the Executive Council January 2018**

2-Personal Data Protection Guideline for Africa, avalible at: https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

ثانيا: الأطرُ المنظمةُ للأمنِ السيبرانىْ بالتجمعاتِ الاقتصاديةِ الإقليميةِ

تمتلكَ التجمعاتُ الاقتصاديةُ الإقليميةُ، الهياكلُ التنظيميةُ، والتفويضاتُ المؤسسيةُ، والاستراتيجياتُ، والسياساتُ، والمواردُ، التي تغطي كلا منْ الأبعادِ الشكليةِ والعملياتيةِ اللازمةِ لمجابهةِ التهديداتِ الأمنيةِ التي توجهَ الدولَ الأعضاءَ بها، وساهمَ تغيرُ البيئةِ الأمنيةِ وزيادةُ حجمِ التهديداتِ الناجمةِ عنْ التطوراتِ التكنولوجيةِ، في تعديلِ الاتفاقياتِ والبروتوكولاتِ المنظمةِ للتعاونِ الأمنيِ والقانونيِ بينَ الدولِ الأعضاءِ بتلكَ التجمعاتِ، لتتواءم معَ تغيرِ طبيعةِ التهديداتِ التي قدْ تتعرضُ لها تلكَ الدولِ.

1- التجمع الاقتصادي لدول غرب أفريقيا (ECOWAS)

سعتْ مفوضيةَ التجمعِ الاقتصاديِ لدولِ غربِ أفريقيا (ECOWAS) إلى الحدِ منْ الخسائرِ التي تتعرضُ لها الدولُ الأعضاءُ، نتيجةُ انتشارِ الجريمةِ السيبرانية وزيادةُ أنشطةِ عصاباتِ الجريمةِ المنظمةِ العابرةِ للحدودِ باستخدامِ التطبيقاتِ الرقميةِ، منْ خلالِ إقرارِ إطارٍ تنظيميٍ يتضمنُ الكثيرُ منْ البنودِ الحاكمةِ التي تلزمُ الدولُ الأعضاءُ بالتعاونِ فيما بينهمْ لمكافحةِ الجريمةِ السيبرانية؛ حيثُ اعتمدَ مجلسُ وزراءِ التجمعِ في دورتهِ العاديةِ السادسةِ والستينَ في أغسطسَ منْ عامٍ (2011) التوجيهِالقانوني (C/DIR1/08/11) بشأنِ مكافحةِ الجرائمِ السيبرانيةْ؛ والذي نصتْ بنودهُ على درجِ الجرائمِ السيبرانية ضمنَ القوانينِ الجنائيةِ للدولِ الأعضاءِ، بالإضافة إلى الإطارُ التنظيميُ للتعاونِ القانونيِ بينَ الدولِ الأعضاءِ، فيما يتعلقُ بالاختصاصِ القضائيِ، وتبادلَ تسليمِ المجرمينَ، والمساعدةُ في تقديمِ الأدلةِ الرقميةِ، وتتبعَ مرتكبي الجريمةِ السيبرانية بغضِ النظرِ عنْ وجودِ اتفاقياتٍ مسبقةٍ بينَ الدولِ الأعضاءِ.[1]

وفى سياق حفظ خصوصية البيانات وتأمين تداولها، نص التوجيه على تجريم كافة صور الانتهاكات للمبادئ والإجراءات التي تحكم عملية تدوال وحفظ البيانات؛ المنصوص عليها في الإطار القانوني المكمل بشأن حماية خصوصية البيانات الشخصية الصادر

1- Ecowas. Directive C/DIR.1/08/11 on fighting cyber crimes, **Ecowas official magazine Vol 59 August 2011**

فى غضون عام (٢٠١٠)، والذي ينص على المبادئ الرئيسية التي يجب أن تتضمنها القوانين الوطنية لحماية البيانات بالدول الأعضاء، وآليات متابعة تنفيذها من خلال كيانات حكومية متخصصة.

واعتمدَ برلمانُ التجمعِ الاقتصاديِ لدولِ غربِ أفريقيا (ECOWAS) الإستراتيجيةَ الإقليميةِ للأمنِ السيبراني ومكافحةُ الجرائمِ السيبرانية، والتي تهدفُ إلى تعزيزِ قدرةِ الدولِ الأعضاءِ على حمايةِ الشبكاتِ الرقميةِ، والبنى التحتيةُ الحرجةُ المرتبطةُ منْ خلالِ التطبيقاتِ الرقميةِ الحديثةِ، بالإضافةِ إلى مراكزِ حفظِ وتداولِ المعلوماتِ، وتتضمنَ بنودُ الاستراتيجيةِ على مشاركةِ مفوضيةِ التجمعِ في إعدادِ الاستراتيجياتِ الوطنيةِ للأمنِ السيبرانىْ للدولِ الأعضاءِ، بحيثُ تتضمنُ على مجموعةِ الأطرِ، والسياساتُ، والبرامجُ الواردةُ بالاستراتيجيةِ الإقليميةِ لدولِ التجمعِ، على أنْ يتمَ الانتهاءُ منْ صياغةِ تلكَ الإستراتيجياتِ قبل نهايةِ عامٍ (2022) لتوفيرِ بيئةٍ رقميةٍ آمنةٍ تتيحُ الاستفادةُ منْ استخدامِ تطبيقاتِ تكنولوجيا المعلوماتِ والاتصالاتِ ومكافحةِ الجريمةِ السيبرانية بشكلٍ فعالٍ بينَ دولِ التجمعِ[1].

٢- السوق المشتركة لدول شرق وجنوب أفريقيا (COMESA)

وضعتْ منظمةَ تجمعِ دولِ السوقِ المشتركةِ لشرقَ وجنوبِ أفريقيا(COMESA) إطارا قانونيا نموذجيا لمكافحةِ الجرائمِ السيبرانيةْ بينَ الدولِ الأعضاءِ، يرتكزَ على النصوصِ القانونيةِ الواردةِ بالأطرِ والاتفاقياتِ الدوليةِ مثلِ اتفاقيةِ مجلسِ أوروبا لمكافحة الجريمة السيبرانية (اتفاقيةُ بودابستْ)، وتوصياتِ الاتحادِ الدولي للاتصالاتِ لتشريعاتِ الجرائمِ السيبرانية كمرجعيةٍ لوضعِ البنودِ الواردةِ بهِ، ويعدَ الإطارُ القانونيُ بمثابةِ نموذجٍ لتطويرِ التشريعاتِ القانونيةِ وتوفيرِ إطارٍ موحدٍ للدولِ الأعضاءِ لتطويرِ قوانينِ الجرائمِ االسيبرانية الوطنيةَ بها، ولا يترتبُ عليهِ أيُ التزاماتٍ قانونيةٍ تفرضُ التعاونَ القضائيَ فيما بينهمْ، الأمرُ الذي يتطلبُ دخولَ الدولِ الأعضاءِ في ترتيباتٍ ثنائيةٍ منفصلةٍ لتنظيمِ التعاونِ فيما بينهم.

1- ECOWAS -Regional Strategy for Cybersecurity and the fight against Cybercrime. 2021

وتضمنتْ بنودُ الإستراتيجيةِ متوسطةً المدى (2021–2025) للمنظمةِ على أهميةِ تعزيزِ إجراءاتِ الأمنِ السيبرانىْ منْ خلالِ إضفاءِ الطابعِ المؤسسيِ على المبادراتِ التقنيةِ، والأطرُ التشريعيةُ المتعلقةُ بها على المستويينِ الوطنيِ والإقليميِ، حيثُ نصتْ الاستراتيجيةُ على أهميةِ اتخاذِ الخطواتِ التنفيذيةِ لإنشاءِ كياناتٍ مؤسسيةٍ تتولى تنظيمَ البيئةِ التشريعيةِ ومراجعةُ وتطويرُ مختلفِ السياساتِ الإقليميةِ والأطرِ التنظيميةِ بما يسهمُ في تعزيزِ المنافسةِ وتوفيرِ إمكانيةِ الوصولِ إلى مختلفِ تطبيقاتِ تكنولوجيا المعلوماتِ والاتصالاتِ، ومنْ أبرزَ تلكَ الكياناتِ المركزِ الإقليميِ للأمنِ السيبراني، وأمانةُ رابطةِ منظمي المعلوماتِ والاتصالاتِ بشرقِ وجنوبِ أفريقيا؛ كما تضمنتْ الاستراتيجيةُ على أهميةِ تأمينِ وتطويرِ البنيةِ التحتيةِ الرقميةِ، لإيجادِ بيئةٍ مواتيةٍ لمختلفِ التطبيقاتِ الرقميةِ المتطورةِ وخاصةً المتعلقةَ بربطِ الأجهزةِ الإلكترونيةِ الذكيةِ بمستخدميها والتي تعرفُ بإنترنتِ الأشياءِ (IOT)، وتعدَ منْ أبرزِ مظاهرَ التكنولوجيةِ الرقميةِ التي ارتبطتْ بظهورِ المدنِ الذكيةِ ووالصناعاتْ والمشروعاتُ المرتبطةُ بها مثلٌ الطرقِ الذكيةِ، ووسائلُ النقلِ الذكيةِ، وشبكاتُ الطاقةِ الذكيةِ.[1]

٣- الجماعة الإنمائية للجنوب الأفريقي (SADC)

يعدّ الإطارُ الإستراتيجيُ الرقميُ (e - SADC Strategic Framework) للجماعةِ الإنمائيةِ للجنوبِ الأفريقيِ؛ المرجعيةِ الرئيسيةِ للدولِ الأعضاءِ فيما يتعلقُ بتنظيمِ استخدامِ تطبيقاتِ تكنولوجيا المعلوماتِ والاتصالاتِ لتحقيقِ التكاملِ الاقتصاديِ الإقليميِ[2]، حيثُ يتضمنُ على ثلاثةِ قوانينَ نموذجيةٍ: قانونُ المعاملاتِ الإلكترونيةِ / التجارةُ الإلكترونيةُ، وقانونَ حمايةِ البياناتِ الشخصيةِ، وقانونَ الجرائمِ السيبرانية، بالإضافةِ إلى آليةٍ لتبادلِ الخبراتِ والمعلوماتِ للتغلبِ على الفجوةِ المعرفيةِ بينَ الدولِ الأعضاءِ، وإتاحةُ الوصولِ إلى الخدماتِ التي توفرها التطبيقاتُ التكنولوجيةُ الحديثةُ داخلَ الدولِ الأعضاءِ.

1- Comesa."**Midum Term Strategic plan (2021- 2025)**",(Zambia**:** Lusaka, September 17, 2020)

2- Southern African Development Community, **e-SADC Strategic Framework**, May 2010

كما اعتمدتْ المجموعةُ الوزاريةُ للجماعةِ الإنمائيةِ لإقليمِ الجنوبِ الأفريقي (SADC) مشروعِ القانونِ النموذجيِ بشأنِ جرائمِ الكمبيوترِ والجرائمِ السيبرانية في غضونِ شهرِ مارسَ منْ عامِ (2012)، وتضمنَ مشروعُ القانونِ على الكثيرَ منْ النقاطِ الحاكمةِ للعملِ بها كمرجعيةٍ قانونيةٍ في التشريعاتِ الوطنيةِ للدولِ الأعضاءِ؛ حيثُ نصَ على توصيفِ كلِ الأنشطةِ التي تندرجُ تحتَ الجرائمِ السيبرانية، وكيفيةُ التعاونِ بينَ الدولِ الأعضاءِ فيما يتعلقُ بمرتكبي هذهِ النوعيةِ منْ الجرائمِ ،على أنْ تقومَ كلُ دولةٍ بوضعِ الأطرِ القانونيةِ التي تتناسبُ معَ تشريعاتها وسياستها الداخليةِ.[1]

تضمنت الوثيقة النهائيةِ الصادرةِ عنْ اجتماعِ وزراءِ تكنولوجيا المعلوماتِ والاتصالاتِ، والإعلامُ، والنقلُ والأرصادُ الجويةُ، لدولِ الجماعةِ الإنمائيةِ للجنوبِ الأفريقي على المحتوى التقني المكملِ للبنودِ التشريعيةِ الواردةِ في مشروعِ القانونِ النموذجيِ للجريمةِ السيبرانيةْ للجماعةِ، حيثُ نصتْ على أهميةِ العملِ على إيجادِ بيئةٍ رقميةٍ تسهمُ في تعزيزِ التعاونِ والتكاملِ الإقليميِ، مما يتطلبُ تحقيقَ أقصى درجاتِ التأمينِ للشبكاتِ الرقميةِ ومراكزُ حفظِ وتشغيلِ البياناتِ، وشملتْ الوثيقةُ على أهميةِ تحقيقِ الأمنِ السيبراني منْ خلالِ إنشاءِ مراكزِ عملياتِ الأمنِ السيبراني(CSOC) ؛ وإنشاء و تطوير مراكزُ إدارةِ الحوادثِ الناتجةِ عنْ التهديداتِ السيبرانية بواسطةَ فرقِ الاستجابةِ للحوادثِ السيبرانية (CIRTs) بالدول الأعضاء وربطها، لتبادل المعلومات عن افضل الممارسات للتعامل مع مختلف صور التهديدات السيبرانيه، وتقديم المساعدة فى حالة الكوارث الطبيعية والرقمية؛ بالإضافةِ إلى آلياتِ ومحدداتِ التعاونِ بينَ الأعضاءِ والتعاونِ الدولي.[2]

٤- تجمع دول شرق أفريقيا(EAC)

وضعت مفوضية تجمع دول شرق أفريقيا الإطار القانونى المنظم لاستخدام التقنيات الرقمية، والذي يعد إطاراً مرجعياً للاسترشاد بما جاء فيه عند إعداد القوانين والتشريعات

1- Southern African Development Community, **Computer Crime and Cybercrime Model Law**

2- SADC Ministers for ICT, Information, Transport and Meteorology meeting in Namibia2018, Available at: https://www.sadc.int/sites/default/files/2021-06/Media_Statement__ICT_Information_Transport_and_Met_meeting.pdf

الوطنية للحد من الجرائم السيبرانيه بالدول الأعضاء[1]، وتولى مجموعة من الخبراء الفنيينَ التابعينَ للدولِ الأعضاءِ بالتجمعِ دولِ شرقِ أفريقيا مهمة وضع الإطارُ التنظيميُ لسياساتِ تكنولوجيا المعلوماتِ والاتصالاتِ(EAC Model ICT Policy Framework) لمواكبةِ التغيراتِ المطردةِ لتطبيقاتِ تكنولوجيا المعلوماتِ والاتصالاتِ والذي تضمنَ علما يلي:[2]

أ- السياساتِ والأطرِ القانونيةِ والفنيةِ للتعاونِ الإقليميِ والدوليِ، وآلياتِ التنسيقِ وتبادلِ المعلوماتِ عنْ أفضلِ الممارساتِ للتعاملِ الفعالِ معَ الآثارِ الناجمةِ عنْ الهجماتِ السيبرانية، والموائمةِ بينَ الجهودِ والأنشطةِ التي تقومُ بها أجهزةُ ومؤسساتُ الدولِ الأعضاءِ للتعاملِ معَ مختلفِ أشكالِ التهديداتِ السيبرانية.

ب- الأطرُ والآلياتِ المقترحةَ للربطِ بينَ المراكزِ الوطنيةِ لإدارةِ الطوارئِ، وإمكانيةِ الاستعانةِ بفرقِ العملِ المتخصصةِ في الاستجابةِ للطوارئِ الناتجةِ عنْ الهجماتِ السيبرانيةعلى المستوى الإقليميِ لتقييمِ حجم الآثار الناتجة عن التهديدات السيبرانية وتقديمِ المعاونةِ في التخلص من آثارها واستعادة كفاءة المنظومات الرقمية فى حالاتِ التعرضِ للهجماتِ السيبرانية شديدةً التعقيدِ والتأثيرِ.

ج- رفعِ مستوى الجهاتِ الفاعلةِ في منظومةِ الأمنِ السيبراني، لتوحيدِ المفهومِ حيالَ الإجراءاتِ اللازمةِ لتأمينِ الشبكاتِ والبنى التحتيةِ للدولةِ بالإضافةِ إلى نشرِ ثقافةِ الأمنِ السيبراني، منْ خلالِ برامجِ توعيةٍ تهدفُ إلى معالجةِ نقاطِ الضعفِ، وتتواءمَ معَ الاحتياجاتِ المعرفيةِ للدولِ الأعضاءِ.

ويمكنَ القولُ إنَ استجابةَ التجمعاتِ الاقتصاديةِ الإقليميةِ لتغيرِ طبيعةِ المهدداتَ الأمنيةِ للدولِ الأعضاءِ، جاءتْ في مجملها كاشفةً لضعفِ دورها الإقليميِ وعدمِ قدرتها على وضعِ إطارٍ إقليميٍ موحدٍ للتعاملِ معَ المهدداتَ الأمنيةِ الناشئةِ عنْ التطوراتِ التكنولوجيةِ، حيثُ

1- East African Community,**Legal Framework for Cyberlaws**, 2008

2- East African Community, **EAC Model ICT Policy Framework**, 20th March, 2015

لمْ يتضمنْ أيُ منْ الأطرِ التنظيميةِ المقترحةِ منْ التجمعاتِ الاقتصاديةِ الإقليميةِ التزاماتٍ على الدولِ الأعضاءِ على ضوءِ صياغتها في إطارٍ استرشاديٍ وغيرِ ملزمٍ، مما أدى إلى غيابِ الإطارِ الإقليميِ المنظمِ للتعاملِ معَ قضايا الأمنِ السيبرانيْ، وظهورَ الكثيرِ منْ الاختلافاتِ بينَ التشريعاتِ الوطنيةِ للدولِ الأعضاءِ في تلكَ التجمعاتِ وما تمَ طرحهُ منْ الأطرِ القانونيةِ والتنظيميةِ في صياغتها الإقليميةِ وهوَ ما يعكسُ غيابَ الإرادةِ السياسيةِ للالتزامِ بسياقٍ إقليميٍ موحدٍ.

كما أظهرتْ استجابةَ الدولِ الأعضاءِ للمبادراتِ التي طرحتها التجمعاتُ الاقتصاديةُ الإقليميةُ لتوفيرِ البيئةِ المناسبةِ لاستخدامِ التقنياتِ الرقميةِ الحديثةِ عنْ تفاوتِ الأولوياتِ السياسيةِ حيالَ أهميةِ توفيرِ بيئةٍ رقميةٍ آمنةٍ تكفلُ حمايةَ البياناتِ وإمكانيةِ إتاحتها وتداولها منْ وجهةِ نظرِ الساسةِ في تلكَ الدولِ، مما يعكسُ عدمَ إدراكِ حكوماتِ معظمِ الدولِ الأفريقيةِ لماهيةِ الفضاءِ السيبرانيْ، ومدى تأثيرِهِ على الصعيدِ السياسيِ الإقليميِ والدوليِ، وأهميةُ تبني استراتيجيةٍ متكاملةٍ ترتكزُ على المعطياتِ التكنولوجيةِ الحديثةِ، توفرَ بيئةً رقميةً آمنةً تسهمُ في الاستغلالِ الأمثلِ للتطبيقاتِ التكنولوجيةِ الحديثةِ في تطويرِ المجالِ الاقتصاديِ، والأداءُ الحكوميُ في تقديمِ الخدماتِ الأساسيةِ للمواطنينَ.

وعلى الرغمِ منْ عدمِ ملائمةِ استجابةِ التجمعاتِ الاقتصاديةِ الإقليميةِ للتهديداتِ الناجمةِ عنْ التطبيقاتِ الرقميةِ بصفةٍ عامةٍ، إلا أنها تتفاوتُ في درجةِ الاستجابةِ فيما بينها، حيثُ تعدْ منظمةُ تجمعِ دولِ السوقِ المشتركةِ لشرقَ وجنوبِ أفريقيا (COMESA) هيَ الأكثرُ تميزا منْ باقي التجمعاتِ الاقتصاديةِ الإقليميةِ في استجابتها للتهديداتِ الناشئةِ عنْ استخدامِ التطبيقاتِ الرقميةِ الحديثةِ، حيثُ تضمُ في عضويتها العديدَ منْ الدولِ الأكثرِ تقدما في مجالِ الأمنِ السيبرانيْ مثلِ مورشيوسْ، وجمهوريةُ مصرَ العربيةِ، ورواندا، الأمرُ الذي انعكسَ على الوعيِ الجماعيِ للدولِ الأعضاءِ نحو أهمية العمل منْ خلالِ رؤيةٍ موحدةٍ.

المبحث الثاني

جهود تحقيق الأمن السيبرانى بالقارة الأفريقية

أصبحَ الأمنُ السيبراني إحدى أهمِ الركائزِ الإستراتيجيةِ للأمنِ القوميِ للدولِ في جميعِ أنحاءِ العالمِ ، في ظلِ تزايدِ تعقيدِ الهجماتِ السيبرانية والآثارُ المترتبةُ عليها دوليا وإقليميا ، وعلى غرارِ العديدِ منْ الدولِ بمختلفِ مناطقِ العالمِ عانتْ دولُ القارةِ الأفريقيةِ منْ الخسائرِ الاقتصاديةِ الفادحةِ نتيجةَ مختلفِ صورِ التهديداتِ السيبرانيهْ ، مما تتطلبُ تبنيَ الدولِ الأفريقيةِ للأطرِ القانونيةِ والفنيةِ اللازمةِ للتعاملِ معَ تلكَ التهديداتِ والحدِ منْ آثارها ، وهوَ ما سنعرضهُ منْ خلالِ الآتي:

أولا: أوضاع الأمن السيبرانى على المستوى القارى

اعتمدَ رؤساءُ دولِ وحكوماتِ الدولِ الأفريقيةِ اتفاقيةَ الاتحادِ الأفريقي للأمنِ السيبرانىْ وحمايةُ البياناتِ الشخصيةِ؛ للعملِ بها كإطارِ قاريْ منظمٍ لكافةِ القضايا المتعلقةِ بالأمنِ السيبراني في القارةِ الأفريقيةِ، إلا أنَ إحجامَ بعضِ الدولِ الأفريقيةِ عنْ التوقيعِ على الاتفاقيةِ واعتمادِ العملِ بها، أدى إلى افتقادِ دولِ القارةِ لإطارِ العملِ المشتركِ لمجابهةِ التهديداتِ السيبرانيهْ، حيثُ تضمنتْ بنود الاتفاقيةِ على ان اعتمادها و تطبيقها فى عدد (15) دولةٍ منْ الدولِ الأعضاءِ بالاتحادِ شرطاً رئيسيا لسريانِها كإطاراً ملزماً للدولِ الموقعةِ عليها، وطبقا للاحصائيات الواردة من مفوضية الاتحاد الافريقى تبين انه تمَ التصديقُ على الاتفاقيةِ منْ قبلٌ (14) دولةٍ فقطْ منْ أصلِ(55) دولةٍ عضوا في الاتحادِ، بينما وقعتْ (18) دولةٍ علي الاتفاقية ولكنها لمْ تضعها محلَ التنفيذِ على المستوى الوطنيِ، مما أدى إلى عدمِ سريانها كإطار ملزم حتى الآنَ.[1]

وطبقا لتقريرِ الاتحادِ الدوليِ للاتصالاتِ عنْ حالةِ الأمنِ السيبراني بمختلفِ مناطقِ العالمِ ضمنها القارةُ الأفريقيةُ (The Global Cybersecurity Index)؛ قامَت العديدَ

1-African union, Convention on Cyber Security and Personal Data Protection Status List, 14 April 2023, Avalible at: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf

منْ البلدانِ الأفريقيةِ باتخاذِ خطواتٍ إيجابيةٍ نحوَ توفيرِ بيئةٍ رقميةٍ آمنةٍ لاستخدامِ التطبيقاتِ التكنولوجيةِ، منْ خلالِ تطبيقِ المعاييرِ القياسيةِ الدوليةِ في مجالِ الأمنِ السيبراني؛ حيثُ وضعتْ (38) دولةِ التشريعاتِ القانونيةِ التي تكفلُ الحدَ منْ الجرائمِ السيبرانية، بينما تمتلكُ (37) دولةٍ منْ دولِ القارةِ الأطرَ والقواعدَ المنظمةَ للأمنِ السيبراني، بالإضافةِ إلى اشتراكِ (11) دولةٍ: جنوبَ أفريقيا، بوتسوانا، أوغندا، زامبيا، بوركينا فاسو، تنزانيا، الكاميرون، نيجيريا، بنين، غانا، وكوتْ ديفوارْ في الكثيرِ منْ برامجَ ومبادراتِ الأمنِ السيبراني على المستوى الإقليميِ والدولي، واحتلتْ كلا منْ موريشيوس، تنزانيا، وغانا قمةَ التصنيفِ في القارةِ أفريقيا منْ خلالِ تحقيقِ أعلى المعدلاتِ الخاصةِ بتقييمِ الدولِ الأعضاءِ في الاتحادِ الدولي للاتصالاتِ، وتضمنَ التقريرُ تقسيمَ دولِ القارةِ الأفريقيةِ طبقا لدرجةِ تطبيقِ المعاييرِ القياسيةِ إلى الآتي: [1]

١- الدول الرائدةِ: وهيَ الدولُ التي تحصلُ على نسبةٍ (50 ٪) أوْ أعلى في تقيمُ مؤشرَ الأمنِ السيبرانيْ العالميَ، أيْ أنها تظهرُ التزاما عاليا بالمعاييرِ القياسيةِ الدوليةِ؛ ويبلغُ عددها (6) دولٌ أفريقيةٌ.

٢- الدولُ في مرحلةِ النضجِ السيبرانيْ: وهيَ الدولُ التي تحصلُ على نسبةٍ تتراوحُ ما بين (20 ٪ إلى 49 ٪) منْ نسبِ تقيمُ مؤشرَ الأمنِ السيبرانيْ، ويتضمنَ هذا التصنيفِ (11) دولةٍ أفريقيةٍ عملتْ على تطويرِ قدراتها، منْ خلالِ الاستفادةِ منْ أفضلِ الممارساتِ الخاصةِ بالأمنِ السيبرانيْ والمشاركةُ في البرامجِ والمبادراتِ الإقليميةِ والدوليةِ

٣- الدولُ في مرحلةِ البدءِ: وهيَ الدولُ التي تحصلُ على نسبةٍ أقلَ منْ (20 ٪) في تقيمُ مؤشرَ الأمنِ السيبرانيْ؛ ويندرج تحتَ هذا التصنيفِ العددِ الأكبرِ منْ الدولِ الأفريقيةِ، ويبلغَ عددها (27) دولةٍ، بدأتْ بتقديمِ التزاماتٍ في مجالِ الأمنِ السيبراني.

1- International Tele communication union, **Global cybersecurity index 2020**

تناولتْ العديدَ منْ الدراساتِ الأكاديميةِ أوضاعَ الأمنِ السيبرانىْ في مختلفِ مناطقِ القارةِ الأفريقيةِ للوقوفِ على مدى ملاءمتها للطبيعةِ المتغيرةِ للتهديداتِ السيبرانية ؛ وطبقا للدراسةِ التي أجراها مجموعةً منْ الباحثينَ القانونينِ بجامعةِ بيندورا للعلومِ والتعليمِ بدولةِ زيمبابوي، عنْ الإطارِ النموذجيِ لقانونِ مكافحةِ جرائمِ الكمبيوترِ والجريمةِ السيبرانيةْ للتجمعِ الإنمائيِ لدولِ الجنوبِ الأفريقي (SADC)، ومدى ملائمتهِ للمعاييرِ الدوليةِ وتحقيقهِ لمبدأِ الخصوصيةِ التشريعيةِ لكلِ دولةٍ منْ الدولِ الأعضاءِ؛ يواجهُ التجمعُ الإنمائيُ للجنوبِ الأفريقيِ معضلةَ مواءمةِ التشريعاتِ الوطنيةِ للدولِ، حيثُ قامتْ بعضَ الدولِ مثلَ: زيمبابوي، وليسوتو، وبتسوانا، بإدراجِ الجريمةِ السيبرانيةْ ضمنَ القوانينِ الجنائيةِ الوطنيةِ طبقا لما جاءَ بالإطارِ النموذجيِ للتجمعِ، بينما أصدرتْ الدولُ الأخرى التشريعاتِ والأطرَ القانونيةَ للتعاملِ معَ الجرائمِ السيبرانيةْ التي تستندُ على النصوصِ الواردةِ في الاتفاقيةِ الأوروبيةِ للجرائمِ الإلكترونيةِ المعروفةِ باسمِ (اتفاقيةُ بودابستْ) كمرجعيةٍ قانونيةٍ لها، مما يؤثرُ على إمكانيةِ موائمةِ تلكَ القوانينِ لتوحيدِ الجهودِ لمجابهةِ الجريمةِ السيبرانيةْ بدولِ التجمعِ.[1]

وناقشَ بيترْ روجينا الباحثِ الرواندي والسياسي المخضرم، وعضوَ اللجنةِ التشريعيةِ بتجمعِ دولِ شرقِ أفريقيا، الأدوارُ التي تلعبها التجمعاتُ الاقتصاديةُ الإقليميةُ بالقارةِ الأفريقيةِ في توفيرِ البيئةِ الرقميةِ الآمنةِ للدولِ الأعضاءِ بها؛ منْ خلالِ دراسةِ التدابيرِ الخاصةِ بالأمنِ السيباني، وحوكمةُ الإنترنت، ضمنَ الأطرِ التشريعيةِ والتنظيميةِ لدولِ تجمعِ دولِ شرقِ أفريقيا، والتي تبينَ أنها تأتي بصفةِ العمومِ دونَ وضعِ وصفٍ قانونيٍ متكاملٍ لماهيةِ الاستخداماتِ غيرِ المشروعةِ لتطبيقاتِ تكنولوجيا المعلوماتِ والاتصالاتِ مما ترتبَ عليهِ شيوعُ الصفةِ القانونيةِ لها، فضلاً عنْ وجودِ حالةٍ منْ عدمِ الوضوحِ حيالَ الإجراءاتِ القانونيةِ والتعاونِ القضائيِ بينَ الدولِ الأعضاءِ، وأشارتْ الدراسةُ إلى أنهُ على

1- MuzaririJenalda; Jeffrey Kurebwa," Multilateral Responses to Cybercrimes in the SADC Region: The Case of Zimbabwe and South Africa" **Canadian Social Science journal,** (Canada: Quebec, Canadian academy of oriental and occidental culture, Vol. 16, No. 12, 2020) Pp 1-10

الرغمِ منْ وجودِ الكثيرِ منْ الجهودِ المبذولةِ لوضعِ أنسبِ الأساليبِ للحدِ منْ استخدامِ التطبيقاتِ الرقميةِ في مختلفِ صورِ الأنشطةِ غيرِ القانونيةِ، إلا أنَ عدمَ إلمامِ متخذي القرارِ منْ الساسةِ وممثلي السلطاتِ التشريعيةِ للأبعادِ التقنيةِ للأمنِ السيبراني بالإضافةِ إلى ندرةِ الخبراءِ المختصينَ في هذا المجالِ حالتْ دونَ ذلكَ. [1]

وطبقا لنتائجِ دراسةِ الأطرِ القانونيةِ لحوكمةِ وحمايةِ البياناتِ في القارةِ الأفريقيةِ الصادرةِ عنْ مركزِ اقتصادياتِ أفريقيا بجامعةِ أكسفورد، تعاني العديدَ منْ دولِ القارةِ منْ غيابِ الرؤيةِ بينَ متخذي القرارِ نحوَ أهميةِ تهيئةِ البيئةِ الرقميةِ الداعمةِ لمتطلباتِ التحولِ الرقمي، واستخدامَ المنصاتِ الرقميةِ في مختلفِ الأنشطةِ الاقتصاديةِ، الأمرُ الذي ينعكسُ بالسلب على الأوضاعِ الاقتصاديةِ والاجتماعيةِ بمعظمِ دولِ القارةِ الأفريقيةِ؛ وأشارتْ الدراسةُ إلى تأثيرِ غيابِ الإطارِ الإقليمي المنظمِ لحمايةِ تداولِ البياناتِ داخلَ دولِ القارةِ خارجها، وما ترتبَ على ذلكَ منْ عدمِ الثقةِ في البيئةِ الرقميةِ للدولِ الأفريقيةِ؛ على الرغمِ منْ الكثيرِ منْ المبادراتِ التي طرحتها المنظماتُ الأفريقيةُ متعددةً الأطرافِ لتوفيرِ البيئةِ الرقميةِ المناسبةِ التي تكفلُ توفيرَ التأمينِ الكافي للبياناتِ خلالَ تداولها وحفظها؛ وأشارتْ الدراسةُ إلى أهميةِ توحيدِ الأطرِ القانونيةِ المنظمةِ لكافةِ أشكالِ تداولِ وحفظِ البياناتِ والتعاطي معَ القضايا المتعلقةِ بالأمنِ السيبرانيْ وخاصةَ تأمينَ البنيةِ التحتيةِ الرقميةِ، في ضوءِ مبادراتِ التكاملِ الاقتصادي الإقليمي الجاريةِ، ومنْ أبرزها إنشاءُ منطقةِ التجارةِ الحرةِ القاريةِ الأفريقيةِ (AfCFTA)، لزيادةِ الاستفادةِ منْ التقنياتِ الرقميةِ الحديثةِ في مختلفِ صورِ التبادلِ التجاري بينَ الدولِ الأفريقيةِ والانفتاحِ على الأسواقِ الإلكترونيةِ العالميةِ، منْ خلالِ المنصاتِ الرقميةِ للتجارةِ الإلكترونيةِ وتحويلِ الأموالِ وغيرها. [2]

1- Rwigema, P. C, "Digital technology and its relevance to political and social economictransformation. Case study of East African Community Region", **The Strategic Journal of Business &ChangeManagement) "** Kenya: Nairobi, Star net College, Vol. 7,no 4, 2020) Pp.1402-1436

2- Centre for the study of the economies of Africa, **Strengthening Data Governance in Africa:Project Inception Report,July 2021** (Oxford: center for the study of African Economies 2021)

ثانيا: الجهود الوطنية لتحقيق الأمن السيبراني

على الرغمِ منْ التقاريرِ الصادرةِ عنْ الجهاتِ الدوليةِ المعنيةِ بقياسِ حالةِ الأمنِ السيبرانيْ بمختلفِ مناطقَ ودولِ العالمِ، والتي تشيرُ إلى العديدِ منْ أوجهِ القصورِ في الإجراءاتِ والتدابيرِ التي اتخذتها معظمُ الدولِ الأفريقيةِ لمجابهةِ التهديداتِ السيبرانيةْ، إلا أنَ بعضَ الدولِ الأفريقيةِ احتلتْ مرتبةً متقدمةً وطبقا لمؤشرِ الأمنِ السيبراني العالميَ الصادرِ عنْ الاتحادِ الدولي للاتصالاتِ (GCI - 2020) ومنْ تلكَ الدولِ:

١- دولة موريشيوس

تمَ تصنيفُ دولةِ موريشيوس في المرتبةِ الأولى على مستوى القارةِ الأفريقيةِ والمرتبةِ السابعةِ عشرةَ على المستوى الدولي[1]، واحتلتْ موريشيوس مركزا متقدما ضمنَ المؤشرِ العالمي خلالَ السنواتِ الثلاثةِ الأخيرةِ على أنها الدولةُ الأكثرُ التزاما بالمعاييرِ الدوليةِ للأمنِ السيبراني في أفريقيا، ويرجعَ ذلكَ إلى تبني الحكومةِ لإستراتيجيةٍ متكاملةٍ للاستجابةِ الوطنيةِ لمختلفِ صورِ التهديداتِ السيبرانية طبقا للمعاييرِ القياسيةِ الدوليةِ وتشتملُ على الآتي:

أ - الاستراتيجيةُ الوطنيةُ للأمنِ السيبراني (National Cyber Security Strategy) : والتي تتضمنُ على المبادئِ التوجيهيةِ والتدابيرِ وخططِ العملِ التي منْ شأنها تعزيزَ القدراتِ والإمكاناتِ الفنيةِ والبشريةِ اللازمةِ لإدارةِ عمليةِ الدفاعِ السيبراني ، وإدارةُ الأزماتِ الرقميةِ واضطراباتُ عملياتِ تشغيلِ وإدارةِ الشبكاتِ الرئيسيةِ للبنيةِ التحتيةِ في حالةِ التعرضِ لأيِ صورةٍ منْ صورِ التهديداتِ السيبرانيةْ بغرضَ تعطيلها عنْ العملِ .

ب- إستراتيجيةُ مجابهةِ الجريمةِ السيبرانية (The Cybercrime strategy): وتتضمنَ على المبادئِ الرئيسيةِ وأولوياتُ عملِ المؤسساتِ الحكوميةِ المعنيةِ بالجرائمِ السيبرانية، والخطواتُ التي ستتخذها وكالاتُ إنفاذِ القانونِ والسلطةِ

1-International Telecommunication Union, **Global Cybersecurity Index 2020,**(Switzerland: Geneva,ITUPublications,2021)

القضائيةِ للتحري والتحقيقِ في الجرائمِ السيبرانية وملاحقةُ مرتكبيها، كما تتضمنُ على أشكالِ التعاونِ معَ مختلفِ أصحابِ المصلحةِ نحوَ العملِ معَ الجهاتِ الحكوميةِ المختصةِ لمعالجةِ كافةِ القضايا المتعلقةِ بالجرائمِ السيبرانيةْ، وتأمينَ البيئةِ الرقميةِ للدولةِ.

كما عملتْ الحكومةُ على تشكيلْ الكياناتُ المؤسسيةُ اللازمةُ لتنفيذِالإستراتيجياتِ الراميةِ إلى خلقِ بيئةٍ رقميةٍ آمنةٍ تسهمُ في تحقيقِ الأهدافِ الإستراتيجيةِ للدولةِ، مما تتطلبُ تطويرَ الهيكلِ التنظيميِ لوزارةِ تكنولوجيا المعلوماتِ والاتصالاتِ والابتكارِ لتشملَ على الكياناتِ الرئيسيةِ الآتيةِ[1]:

أ – المكتبُ المركزيُ للمعلوماتِ (CIB) :تتمثلَ مهامهُ الرئيسيةَ في تخطيطِ وتنسيقِ الحوسبةِ داخلَ المؤسساتِ الحكوميةِ المعنيةِ بتقديمِ الخدماتِ الرئيسيةِ للمواطنينَ، وتقديمَ المشورةِ الفنيةِ اللازمةِ للقطاعاتِ الحكوميةِ والخاصةِ والقطاعِ الماليِ والمصرفيِ فيما يتعلقُ باستخدامِ التطبيقاتِ التكنولوجيةِ الحديثةِ في إطارِ سياسةِ الدولةِ للتحولِ الرقميِ، والتوسعُ في تقديمِ الخدماتِ لمواطنيها في صورتها الرقميةِ ضمنَ تطبيقاتِ الحكومةِ الإلكترونيةِ.

ب– إدارةُ نظمِ المعلوماتِ المركزيةِ (CISD): المسئولةُ عنْ معالجةِ البياناتِ وتضمّ القسمَ الفنيَ، وقسمَ العملياتِ؛ وتقدمَ الإدارةَ خدماتِ الدعمِ التكنولوجيِ وتطبيقاتُ الاتصالاتِ المؤمنةِ الفعالةِ،بالإضافةِ إلى تقديمُ المساعدةِ الفنيةِ في اختيارِ أجهزةِ الكمبيوترِ، وتطويرِ البرمجياتِ، وصيانةِ المواقعِ الحكوميةِ؛ مما يسهم فى توفيرِ الأعباءِ الماليةِ والميزانياتِ المطلوبِ توفيرها للتحولِ الرقميِ في المؤسساتِ الحكوميةِ.

ج– وحدة أمنِ تكنولوجيا المعلوماتِ (ITSU): وتعدَ الوحدةُ بمثابةِ الذراعِ الحكوميةِ لتوفيرِ بيئةٍ رقميةٍ آمنةٍ لعملِ المؤسساتِ الحكوميةِ؛ منْ خلالِ تنفيذِ سياساتِ

1–Ministry of Information Technology, Communication and Innovation https://mitci.govmu.org/SitePages/Index.aspx".

الحكومةِ فيما يتعلقُ بأمنِ تكنولوجيا المعلوماتِ، ومساعدةِ الوزاراتِ/الإداراتُ في تنفيذِ المعاييرِ الأمنيةِ، وإجراءُ عملياتِ الاختبارِ والتدقيقِ الأمنيِ لكشفِ أيِ ثغراتٍ تمثلُ تهديدا أمنيا للشبكاتِ الحكوميةِ، والعمل على رفعِ الوعيِ حولَ الموضوعاتِ الخاصةِ بالأمنِ السيبرانى بين كافة مستخدمى تكنولوجياالمعلوماتِ.

د–هيئة حمايةِ البياناتِ (DPO): وتختصَ بوضعِ الآلياتِ والأطرِ التنظيميةِ التي تكفلُ حمايةَ مختلفِ أنواعِ البياناتِ الحكوميةِ وضمانِ عدمِ المساسِ بالحقوقِ الأساسيةِ للمواطنينَ في الاحتفاظِ بسريةِ البياناتِ الخاصةِ بهمْ، وتمتعَ الهيئةِ بمجموعةٍ واسعةٍ منْ السلطاتِ التي تمكنها منْ تنفيذِ مهامها طبقا لما جاءَ بقانونِ حمايةِ البياناتِ لعامٍ (2017) والذي يتوافقُ معَ المبادئِ الواردةِ باتفاقيةِ الاتحادِ الأفريقيِ للأمنِ السيبراني وحمايةُ البياناتِ الشخصيةِ ولائحةُ الاتحادِ الأوروبيِ لحمايةِ البياناتِ العامةِ.

هـ – المجلسُ الوطنيُ للحوسبةِ (NCB): هيئةٌ شبهٌ حكوميةٍ يديرها مجلسُ إدارةٍ يتكونُ منْ ممثلينَ عنْ القطاعِ الخاصِ وأصحابِ الخبرةِ بالإضافةِ إلى ممثلي الجهاتِ الحكوميةِ المعنيةِ ويعملُ طبقا لسياسةِ وزارةِ تكنولوجيا المعلوماتِ والاتصالاتِ والابتكارِ لدعمِ عمليةِ التحولِ الرقميِ وتحويلِ الدولةِ إلى مركزٍ إقليميٍ لتكنولوجيا المعلوماتِ والاتصالاتِ، والاستجابةُ بشكلِ أكثرِ فعاليةٍ للتطلعاتِ الوطنيةِ الجديدةِ في ضوءِ التحدياتِ المتعددةِ التي تفرضها التطبيقاتُ التكنولوجيةُ الحديثةُ.

و– فريقُ الاستجابةِ للحوادثِ السيبرانية (CSIRT): يعملَ على الاستجابةِ بشكلٍ فعالٍ للتهديات السيبرانية والآثار الناجمه عنها؛ والعمل على استعادة كفاءة عمل الأنظمة الرقمية المتضررة من جراء تلك الحوادث، حيثُ يشرفُ على إدارةِ الحوادثِ السيبرانية في مختلفِ القطاعاتِ الحكوميةِ والخاصةِ منْ خلالِ نظامٍ آليَ مرتبط بقاعدةَ بياناتٍ معرفيةٍ متاحةٍ لمتخصصي الأمنِ السيبراني وموظفي تكنولوجيا المعلوماتِ والاتصالاتِ؛ ويسمحَ هذا النظامِ لمركزِ عملياتِ الأمنِ

السيبراني بالتصعيدِ التلقائي فى الاستجابة للحوادثِ السيبرانيه مقارنةٍ بالطريقةِ التقليديةِ السابقةِ كما يقدمُ فريق (CSIRT) أيضا تدريبا على الحوادثِ للفرقِ التقنيةِ المنتشرةِ في الوزاراتِ/الإداراتُ؛ بالإضافةِ إلى الخدماتِ الاستباقيةِ لمكافحةِ التهديداتِ السيبرانية كجزءٍ منْ الخدماتِ التفاعليةِ التي يقدمها.

سعتْ حكومةَ موريشيوس إلى وضعِ إطارٍ تشريعيٍ محكمٍ لحمايةِ الفضاءِ السيبراني وتوفيرِ بيئةٍ رقميةٍ آمنةٍ لكلِ مستخدمي التطبيقاتِ الرقميةِ الحديثةِ، ويعد قانونُ الجريمةِ السيبرانية (Computer Misuse and Cybercrime Act) الصادرَ عامٌ (2003) النواةِ الرئيسيةِ للتشريعاتِ الخاصةِ بالحدِ منْ الأنشطةِ غيرِ المشروعةِ في الفضاءِ السيبراني حيثُ تضمنَ توصيفُ الجرائمِ التي تتمُ باستخدامِ تطبيقاتِ تكنولوجيا المعلوماتِ والاتصالاتِ التي تمَ حصرها في: الوصولُ غيرُ المصرحِ بهِ إلى بياناتِ الكمبيوترِ، والدخولُ إلى النظامِ بقصدِ ارتكابِ جرائمَ، والدخولُ غيرُ المصرحِ بهِ إلى إحدى الخدماتِ الرقميةِ واعتراضها، والتعديلُ غيرُ المصرحِ بهِ للمحتوى الرقمي، وإتلافَ أوْ منعِ الوصولِ إلى الأنظمةِ الرقميةِ، وسرقةُ اسمِ المستخدمِ وكلمةُ المرورِ، والحيازةُ غيرُ القانونيةِ للأجهزةِ والبياناتِ، والاحتيالُ الإلكترونيُ[1]؛ وتم إدخال بعض التعديلات على نصوص القانون في عام (٢٠٢١) لتتوافق مع التغيرات التي طرأت على تكنولوجيا المعلومات والاتصالات والتي انعكس تأثيرها بالتبعية على طبيعة التهديدات التي ترتبت على تلك التغيرات.[2]

فيما يختصُ بحمايةِ البياناتِ الشخصيةِ أصدرتْ حكومةَ موريشيوس قانونَ حمايةِ البياناتِ لعامٍ (2017)، ليتمّ العملُ بهِ بدلاً منْ القانونِ المعمولِ بهِ منذُ عامٍ (2004)؛ ويهدفُ القانونُ إلى حمايةِ خصوصيةِ البياناتِ الشخصيةِ وحمايةُ الحريةِ في الوصولِ إلى شبكةِ المعلوماتِ الدوليةِ (الإنترنت)، وتتوافقَ نصوصهُ معَ ما وردَ باتفاقيةِ

1- Mauritius government, **Computer Misuse and Cybercrime Act 22**, August 2003

2- Mauritius government ,**Cybersecurity and Cybercrime billNo. XV of 2021**, 22 October 2021

الاتحادِ الأوروبـي الخاصـةِ بحمايـةِ البيانـاتِ الشخصـيةِ؛ والمحـدداتِ الـواردةِ فـي القواعـدِ الأساسيةِ لحمايةِ البياناتِ الشخصيةِ (GDPR-EU 2016/679) الصادرةِ عنْ الاتحادِ الأوروبـي؛ للالتزام بالعملِ طبقاً لنصوصـه عند تبادلِ المعلومـاتِ والبيانـات الشخصـية بينَ أجهزة الدولة.[1]

٢- جمهورية تنزانيا الاتحادية

تحتل جمهوريةَ تنزانيا المرتبةِ الثانيةِ على مستوى القارةِ الأفريقيةِ طبقا لمؤشرِ الأمنِ السيبراني العـالميَ الصـادرِ عنْ الاتحـادِ الـدولي للاتصـالاتِ (GCI-2020) وهوَ مـا يعكسُ حجمَ التقدمِ الذي أحرزتـهُ الحكومـةُ التنزانيـةُ فـي مجـالِ الأمـنِ السيبراني علـى المسـتوى القـاري، حيـث وضـعت الحكومـة التنزانيـة الاسـتراتيجيةُ الوطنيـةُ لتكنولوجيـا المعلومـاتِ (2016–2021)[2]، والتـي تمثـلُ توجهـا اسـتراتيجيا أساسـيا لتعزيـزِ قطـاعِ تكنولوجيا المعلوماتِ والاتصالاتِ بالدولة لتحقيق الأهداف التنموية للخطة الاستراتيجية (تنزانيا–2025)؛ وتوفير البيئة الرقمية الآمنة لتطبيق البرامج الحكومية للتحول الرقمى، حيث وضعت العديد من البرامج في إطار سياسة الدولة للتحول الرقمي ومن أبرزها برنـامج تنزانيـا الرقمـي (DTP) التـي اطلقتـه الحكومـة فـي غضـون شـهر مـارس مـن عام(٢٠٢١).[3]

وسـعتْ الحكومـة التنزانيـة إلـى إنشـاءِ الكيانـاتِ المتخصصـةِ فـي مجـالِ تكنولوجيـا المعلومـاتِ والاتصـالاتِ وإتاحـة الإمكانـاتِ التقنيـةِ والتنظيميـةِ التـي تتوافقُ مـعَ طبيعـةِ عملها؛ وتتمثلُ أبرزَ تلكَ الكياناتِ في الآتي:

أ- مفوضيةُ تكنولوجيا المعلوماتِ والاتصالاتِ (ICT-Commission) : تمَ إنشاءَ مفوضيةِ تكنولوجيا المعلوماتِ والاتصالاتِ طبقا للمرسومِ الرئاسيِ رقمِ (532)

1- Mauritius government ,**The Data Protction act 2017,** (Act No 20 ,22 December 2017)
2- The United Republic of Tanzania,Ministry of works, transport and communication National **Information and Communications Technology Policy,** May 2016
3- The United Republic of Tanzania, Ministry of Communication and Information Technology, **Digital Tanzania Project,** March 2021

الصادرُ بتاريخِ (20) نوفمبر لسنةِ (2015) القاضي بإنشاءِ هيئةِ ضمنَ الإطارِ المؤسسي لقطاعِ تكنولوجيا المعلوماتِ والاتصالاتِ لتنسيقِ السياساتِ الوطنيةِ والعملِ على تطبيقها بمختلفِ أنحاءِ البلادِ، على أنْ تتولى المفوضيةُ مهمةَ حمايةِ البنيةِ التحتيةِ الحرجةِ وأنظمةُ تكنولوجيا المعلوماتِ والاتصالاتِ الوطنيةِ بالتنسيقِ معَ هيئةِ تنظيمِ الاتصالاتِ وفريقِ الاستجابةِ للطوارئِ وغيرها منْ الجهاتِ المعنيةِ بالدولةِ، فضلاً عنْ تقديمِ المشورةِ فيما يتعلقُ بتنسيقِ تنفيذِ السياساتِ، والرصدُ، والتقييمُ، والمراجعةُ الدوريةُ وتعزيزُ استخدامِ أنظمةِ وحلولِ تكنولوجيا المعلوماتِ والاتصالاتِ المتوافقةِ معَ المعاييرِ القياسيةِ الدوليةِ.[1]

ب- هيئة تنظيمِ الاتصالاتِ (Communications Regulatory Authority): وهيَ هيئةٌ حكوميةٌ شبهٌ مستقلةٍ مسؤولةٍ عنْ تنظيمِ قطاعيْ الاتصالاتِ والبثِ في تنزانيا تمَ إنشاؤها بموجبُ قانونَ رقمِ (2003/12) لتنظيمِ الاتصالاتِ الإلكترونيةِ والخدماتِ البريديةِ وإدارةُ الطيفِ الترددي، وتعملَ الهيئةُ بالتعاونِ معَ الشركاءِ منْ مؤسساتِ القطاعِ الخاصِ ومنظماتُ المجتمعِ المدني على إمدادِ كلِ المناطقِ بخدمةِ الاتصالِ بشبكةِ المعلوماتِ الدوليةِ (الإنترنت) ورفعُ وعيِ المستخدمينَ حيالَ الاستخدامِ الآمنِ لها، ووضعَ الضوابطِ والقواعدِ الملزمةِ للشركاتِ منْ مقدمي خدمةِ الاتصالِ عبرَ شبكةِ المعلوماتِ الدوليةِ (الإنترنت) التي تكفلُ الحدَ منْ التهديداتِ التي قدْ يتعرضُ لها مستخدمي الشبكاتِ التابعةِ لهمْ؛ حيثُ يعدْ توفيرُ بيئةِ اتصالاتٍ نظيفةٍ وآمنةٍ أحدُ الأهدافِ الرئيسيةِ التي تعملُ الهيئةُ على تحقيقها.

ج – فريقُ الاستجابةِ للأزماتِ والحوادثِ السيبرانية (TZ-CERT): أحدُ الكياناتِ التابعةِ لهيئةِ تنظيمِ الاتصالاتِ، وهوَ المسئولُ عنْ تنسيقِ الأدوارِ والمهامِ الخاصةِ بكلِ الجهاتِ المعنيةِ بالتعاملِ معَ الآثارِ الناجمةِ عنْ التهديداتِ السيبرانية على

1- Presidential Decree Government Notice (GN) No. 532, published in the **Government Gazette No. 47 Vol. 96 dated 20th November, 2015.**

مستوى الدولةِ، ويعملَ الفريقُ على ضمانِ أكبرَ قدرا منْ الفاعليةِ في التعاملِ معَ التهديداتِ السيبرانية والحدُ منْ الآثارِ السلبيةِ التي قدْ تترتبُ على حدوثها بالإضافةِ إلى العملِ على توفيرِ مستوى عالٍ وفعالٍ منْ التأمينِ للشبكاتِ الرقميةِ ومراكزُ البياناتِ والمعلوماتِ داخلَ الدولةِ وتطويرِ ثقافةِ الأمنِ السيبراني بينَ مختلفِ مستخدمي والتطبيقاتِ الرقميةِ بالإضافةِ إلى تنسيقِ التعاونِ معَ الكياناتِ الإقليميةِ والدوليةِ.

اتخذتْ الحكومةُ التنزانيةُ الكثيرَ منْ الإجراءاتِ لتوفيرِ أكبرَ قدرا منْ الحمايةِ لمستخدمى التطبيقاتِ التكنولوجيةِ الحديثةِ ووضعِ الأطرِ القانونيةِ التي تنظمُ عملَ الجهاتِ المعنيةِ بالأمنِ السيبراني والإجراءاتُ الخاصةُ بملاحقةِ مرتكبي الجرائمِ السيبرانية، تتمثل أبرزها في الآتي:

أ- قانونُ الجريمةِ السيبرانيه (Cyber Crime Ac): تمَ سنَ قانونِ الجرائمِ السيبرانية في أبريلَ منْ عامٍ (2015)؛ ويتضمن على التوصيفِ القانونيِ للأنشطةِ الإجراميةِ المتعلقةِ بتطبيقاتِ تكنولوجيا المعلوماتِ والاتصالاتِ، مثلٌ التجسسِ على البياناتِ والدخولِ غيرِ المصرحِ بهِ على الأنظمةِ والشبكاتِ وسرقةِ الهويةِ الرقميةِ وغيرها منْ الأنشطةِ غيرِ المشروعةِ؛ كما جرمَ القانونِ عددا منْ الأنشطةِ الأخرى مثلٍ نشرِ معلوماتٍ كاذبةٍ أوْ غيرِ دقيقةٍ، وإنتاجَ ونشرَ موادَ عنصريةٍ ومعاديةٍ للأجانبِ، ونقلَ أوْ إعادةِ إرسالِ رسائلِ غيرِ مرغوبٍ فيها، وغيرها منْ أنواعِ الجرائمِ التي يتمُ ارتكبها منْ خلالِ الفضاءِ السيبراني.[1]

ب – قانونُ التحويلاتِ الإلكترونيةِ: [2](Electronic Transactions Act) ينصَ على شرعيةِ مختلفِ المعاملاتِ الإلكترونيةِ مثلٍ البيعِ والشراءِ وتحويلِ الأموالِ وخدماتِ الدفعِ الإلكتروني وغيرها منْ الأنشطةِ الرقميةِ التي تحملُ الصفةُ

1- The United Republic of Tanzania, cyber crimeact,published in the **Government Gazette No 22 vol96, May 2015**

2- The United Republic of **Tanzania Electronic Transactions Act No13**, 2015

التعاقديةُ، كما يضفي الشرعيةَ القانونيةَ على كلِ الوثائقِ والمستنداتِ الصادرةِ عنْ المواقعِ الإلكترونيةِ الخدميةِ الحكوميةِ في صورتها الرقميةِ منْ خلالِ البصمةِ الإلكترونيةِ المؤمنةِ واعتمادِ استخدامِ التوقيعاتِ الإلكترونيةِ الآمنةِ، واشتملَ أيضا على تقنينِ إجراءاتِ جمعِ الأدلةِ الإلكترونيةِ لإثباتِ ارتكابٍ مختلفٍ أنواعِ الجرائمِ السيبرانية وتحديدِ التطبيقاتِ التكنولوجيةِ المستخدمةِ في ارتكابها، كما أضفى الشريعةَ القانونيةَ على الاستعانةِ بتقريرِ الأدلةِ الناتجِ عنْ التشريحِ الإلكتروني للأجهزةِ الالكترونية المستخدمةِ في الجرائمِ السيبرانية مثل (الهواتفُ المحمولةٌ – أجهزةَ حاسبِ لوحيهِ/ محمولةً – أجهزةُ حاسبٍ مكتبيةٍ ... وغيرها) في أعمالِ التقاضي.

وترتكزَ إجراءاتُ حمايةُ البياناتِ الشخصيةِ على نصوصِ دستورِ جمهوريةِ تنزانيا بموجبِ المادةِ رقمٍ (16)، والتي تنصُ على أنَ لكلِ شخصِ الحقِ في احترامِ وحمايةِ شخصهِ واحترامُ وحمايةُ مكانِ إقامتهِ واتصالاتهِ الخاصةِ، على أنَ هذا الحقِ ليسَ مطلقا طبقا لنصَ قانونُ الاتصالاتِ الإلكترونيةِ والبريديةِ لعامٍ (2010): "أنَه لغرضَ الحفاظِ على حقِ الشخصِ يتعينُ على سلطةِ الدولةِ وضعَ الإجراءاتِ القانونيةِ فيما يتعلقُ بالظروفِ والطريقةِ والمدى التي يمكنُ فيها التعدي على الحقِ في الخصوصيةِ وأمنِ الشخصِ وممتلكاتهِ وإقامتهِ دونَ الإخلالِ بأحكامِ هذا القانونِ"؛ كما تتضمنُ لوائحَ المحتوى عبرَ الإنترنت الصادرةِ عام (2018) أحكامٍ تلزمُ موفري المحتوى عبرَ الإنترنت ومقدمي خدمةِ الاتصالاتِ بتحديدِ مصادرِ معلوماتهمْ أوْ المحتوى الذي تمَ نشرهُ[1] .

٣- جمهورية غانا

تحتلَ غانا المرتبةُ الثالثةُ على مستوى القارةِ الأفريقيةِ والمرتبةِ الثالثةِ ولأربعينَ على المستوى الدولي طبقا لمؤشرِ الأمنِ السيبراني العالميَ الصادرِ عنْ الاتحادِ الدولي

1-The United Republic of Tanzania **The Electronic and Postal Communications act**, 2010

للاتصالاتِ (GCI-2020)؛ وتعدّ دولةُ غانا منْ الدولِ الأفريقيةِ الرائدةِ في مجالِ الأمنِ السيبرانىْ فهيَ واحدةٌ منْ ضمنِ عددٍ (12) دولةٍ فقطْ في القارةِ الأفريقيةِ تمتلكُ استراتيجيةً وطنيةً للأمنِ السيبراني وقدراتُ وطنيةٌ للاستجابةِ للحوادثِ، وواحدةٌ منْ أربعِ دولٍ صدقتْ على اتفاقيتيْ بودابستْ ومالابو، طبقتْ الحكومةُ الغانيةُ اقترابَ تعدديةِ أصحابِ المصالحِ لإدارةِ الموضوعاتِ ذاتِ الصلةِ باستخدامِ التطبيقاتِ التكنولوجيةِ (Multi Stakeholder approach) منْ خلالِ دمجِ ممثلينَ عنْ القطاعِ الخاصِ ومنظماتُ المجتمعِ المدنيِ ضمنَ اللجانِ الحكوميةِ المشكلةِ لوضعِ الأطرِ المنظمةِ للعملِ في الفضاءِ السيبراني واستخدامِ التطبيقاتِ التكنولوجيةِ الحديثةِ، وتعظيمَ الاستفادةِ منْ التطورِ التكنولوجيِ لدفعِ عجلةِ التنميةِ والحدِ منْ الخسائرِ الاقتصاديةِ التي ساهمتْ في التأثيرِ على حجمِ النموِ الاقتصاديِ في الدولةِ. من التطور التكنولوجي لدفع عجلة التنمية والحد من الخسائر الاقتصادية التي ساهمت في التأثير على حجم النمو الاقتصادي في الدولة.

وتضمنتْ الاستراتيجيةُ الوطنيةُ للامن السيبرانى الصادرةُ في غضونِ شهرِ يوليو عام (2015) على سياساتِ الدولة فى المجالات المتعلقة بالأمنِ السيبراني والتي تتشمل على: الخطةُ الوطنيةُ لإدارةِ الأزماتِ السيبرانية، البرنامجِ الوطنيِ للتوعيةِ بالجرائمِ السيبرانية بالاشتراكِ معَ مؤسساتِ القطاعِ الخاصِ ومنظماتُ المجتمعِ المدنيِ لرفعِ الوعيِ بينَ مستخدمي التطبيقاتِ التكنولوجيةِ الحديثةِ حيالَ وسائلِ ارتكابِ الجرائمِ السيبرانية وكيفيةُ الحدِ منها؛ كماتضمنتْ على إنشاءِ المركزِ القوميِ للأمنِ السيبراني (NCSC) كأحدِ الكياناتِ التابعةِ لمجلسِ الأمنِ القوميِ للدولةِ بهدفِ الإشرافِ على جميعِ أنشطةِ الأمنِ السيبراني ، وتنسيقُ التعاونِ بينَ أجهزةِ الدولةِ ذاتِ الصلةِ بتكنولوجيا المعلوماتِ والاتصالاتِ، ويعملَ كمركزِ معلوماتِ رئيسيٍ للتهديداتِ السيبرانية للحكومةِ لتنسيقِ الاستجابةِ لحوادثِ الأمنِ السيبراني الكبرى. [1]

1- Republic of Ghana, Ministry of Communications, **Ghana National Cyber Security Policy & Strategy ,** July 2015.

ونصت الاستراتيجيةُ الوطنيةُ للامن السيبرانى على مجموعةٌ منْ والهيئاتِ والأجهزةِ التابعةِ لوزارةِ الاتصالاتِ تتولى مسئوليةَ تنظيمِ وتأمينِ العملِ بالفضاءِ السيبراني طبقا للآتي:

1 – الهيئةُ الوطنيةُ لتكنولوجياالمعلومات (NITA): تأسستْ بموجبُ القانونَ رقم (771 / 2008) بمهمةِ وضعِ المعاييرِ والمبادئِ التوجيهيةِ لاستخدامِ التطبيقاتِ التكنولوجيةِ الحديثةِ والشراكاتِ بينَ القطاعينِ العامِ والخاصِ، فضلاً عنْ العملِ على وضعِ إستراتيجياتِ البحثِ والتطويرِ لضمانِ مواكبةِ التطورِ الدائمِ في مجالِ تكنولوجيا المعلوماتِ والاتصالاتِ لمساعدةِ الحكومةِ على تحقيقِ النموِ الاقتصاديِ وإيجادِ فرصِ عملِ قائمةٍ على التقنياتِ الرقميةِ.

2– مفوضيةُ حمايةِ البياناتِ (DPC): هيئةٌ قانونيةٌ مستقلةٌ تأسستْ بموجبُ قانونَ حمايةِ البياناتِ رقم (2012/843) وتختصّ بتنظيمِ عمليةِ الحصولِ على البياناتِ أوْ الاحتفاظِ بها أوْ استخدامها، ويخولَ للمفوضيةِ بموجبَ القانونُ الكثيرَ منْ الصلاحياتِ بما في ذلكَ سلطةَ حيازةِ وإدارةِ البياناتِ الحكوميةِ وتنظيمِ العملِ بها والاطلاعِ عليها ووضعِ الآلياتِ المناسبةِ لعمليةِ تداولِ البياناتِ بينَ الهيئاتِ والمؤسساتِ الحكوميةِ المعنيةِ، للتأكدِ منْ تنفيذِ ما جاءَ بالقانونِ، وعدمَ الإخلالِ بما جاءَ فيهِ، واتخاذَ الترتيباتِ التي تراها مناسبةٌ للتحقيقِ فى أيُ شكوى والبتِ فيها.

3– فريقُ الاستجابةِ للطوارئِ الحاسوبيةِ (CERT-GH): تمَ إنشاءَ الفريقِ الوطنيِ للاستجابةِ للأزماتِ والأحداثِ الطارئةِ التي تنتجُ عنْ التهديداتِ السيبرانية في غضونِ شهرِ أغسطسَ عام (2014)، لتنسيقِ الاستجابةِ للآثارِ الناتجةِ عنْ التهديداتِ السيبرانية، واستعادةُ كفاءةِ الأنظمةِ الرقميةِ في أسرعِ وقتٍ ممكنٍ بالتعاونِ معَ كلِ الجهاتِ المعنيةِ بهذا الشأنِ في الحكومةِ والقطاعِ الخاصِ منْ خلالِ الخدماتِ التفاعليةِ التي يتيحها لإدارةِ الحوادثِ السيبرانية والتواصلُ معَ نظرائهِ على المستوى الإقليميِ والدوليِ حيثُ يعدْ الفريقُ نقطةَ الاتصالِ الوطنيةِ (PoC) لتنسيقِ حوادثِ الأمنِ السيبراني.

4- هيئةُ الأمنِ السيبراني (CSA): تمَ إنشاءَ الهيئةِ بموجبَ قانونَ الأمنِ السيبراني رقم (1308) الصادرَ عام (2020)، وتتولى الهيئةُ مسئوليةَ وضعِ الأطرِ الفنيةِ والتنظيميةِ الخاصةِ بعملِ الكياناتِ المسئولةِ عنْ الأمنِ السيبراني داخلَ المؤسساتِ الحكوميةِ والقطاعِ الخاصِ وربطها بفريقِ الاستجابةِ للطوارئِ للحدِ منْ التهديداتِ السيبرانية وإدارةُ الحوادثِ حالَ وقوعها، كما تعملُ على التنسيقِ معَ الشركاتِ منْ مقدمي خدمةِ الاتصالِ بشبكةِ المعلوماتِ الدوليةِ (الإنترنت) حيالَ الإجراءاتِ الوقائيةِ الأزمةِ لحمايةِ مختلفِ مستخدمي الشبكةِ منْ التهديداتِ السيبرانيةِ والأطرِ القانونيةِ الملزمةِ لتكُ الشركاتِ للتعاونِ معَ جهاتِ إنفاذِ القانونِ حيالَ الاستخدامِ غيرِ المشروعِ للشبكةِ، وتدريبِ الكوادرِ الفنيةِ العاملةِ في هذا المجالِ.

وسعتْ الحكوميةُ الغانيةُ إلى توفيرِ البيئةِ التشريعيةِ المنظمةِ للعملِ بالتطبيقاتِ التكنولوجيةِ الحديثةِ، منذُ بدءِ انتشارها بالبلادِ حيثُ أصدرتْ الكثيرَ منْ القوانينِ والتشريعاتِ يتمثلُ أبرزها في الآتي:

1- قانونُ الاتصالاتِ الإلكترونيةِ رقمِ (775 / 2008): يغطي تنظيمُ الاتصالاتِ الإلكترونيةِ وخدماتُ البثِ واستخدامِ الطيفِ الكهرومغناطيسي وفقا لمعاييرَ ومتطلباتِ الاتحادِ الدولي للاتصالاتِ وتنظيمِ استخدامِ شركاتِ مقدمي الخدمةِ شبكاتِ الاتصالاتِ الإلكترونيةِ وأسلوبِ الربطِ بينها.[1]

2- قانونُ المعاملاتِ الإلكترونيةِ رقمِ (772 / 2008): يوفرَ الأساسُ القانونيُ للمعاملاتِ الإلكترونيةِ في الدولةِ وإضفاءِ الشرعيةِ على الوثائقِ والسجلاتِ الرقميةِ والتوقيعاتِ الإلكترونيةِ كما يتضمنُ التصديقُ على إنشاءِ وكالةٍ وطنيةٍ تتولى التصديقَ على إصدارِ الأكوادِ الخاصةِ بالوثائقِ والإصداراتِ الحكوميةِ والتشفيرِ والمصادقةِ على التوقيعاتِ الإلكترونيةِ، واتخاذَ كلِ الإجراءاتِ اللازمةِ لذلكَ.[2]

1-The Parliament of The Republic of Ghana, **electronic communications act,** 2008 , date of assent: 6th January, 2009.

2- The Parliament of The Republic of Ghana, **electronic transactions act**, 2008, date of assent: 18th December 2008.

3 – قانونُ حمايةِ البياناتِ رقم (843 / 2012): يوفرَ القانونُ المبادئَ القياسيةَ الواجبَ الالتزامَ بها منْ قبلُ كلِ الكياناتِ التي تختصُ بمعالجةِ البياناتِ والمعلوماتِ وينطبقُ القانونُ على جميعِ أشكالِ البياناتِ الشخصيةِ، أوْ المعلوماتِ المخزنةِ على كلٍ منْ المنصاتِ الإلكترونيةِ وغيرِ الإلكترونيةِ، كما تضمنَ القانونُ على إنشاءِ مفوضيةٍ لحمايةِ خصوصيةِ البياناتِ. [1]

٤– قانون الأمن السيبراني رقم (٢٠٢٠/١٠٣٨): وينص على إنشاء هيئة تتولى مسئولية تعزيز وتطوير سياسات الأمن السيبراني في الدولة، ووضع التدابير الوقائية التي تكفل الحد من التهديدات الناشئة عن التطورات التكنولوجية والتي تنطوى على تهديد للأمن القومى للبلاد، كما تعمل على وضع معايير القياسية للأمن السيبراني بالدولة تحت مسمي هيئة الأمن السيبراني.[2]

٤– جمهورية مصر العربية

تحتلَ جمهوريةَ مصرَ العربيةِ المركزَ الرابعَ على مستوى المنطقةِ العربيةِ والثالثُ والعشرينَ على المستوى العالمي في تطبيقِ المعاييرِ الدوليةِ للأمنِ السيبراني طبقا لمؤشرِ الاتحادِ الدولي للاتصالاتِ (GCI-2020)، حيثُ ساهمَ اتجاهُ الدولةِ إلى التحولِ الرقمي تماشيا معَ أهدافِ الاستراتجية الوطنيةَ (مصر–2030) إلى زيادةِ الاهتمامِ بمجالِ الأمنِ السيبراني للحدِ منْ الآثارِ السلبيةِ التي قدْ تترتبُ على استهدافِ البنيةِ التحتيةِ الحرجةِ أوْ اختراقِ مراكزِ البياناتِ الحكوميةِ على الأمنِ القومي للدولةِ.

تضمنت الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧–٢٠٢١) عددًا من البرامج التي تدعم أهداف الإستراتيجية لتحقيق الأمن السيبراني من خلال خطة عمل تمتد طوال الفترة الزمنية لتنفيذ الإستراتيجية من أبرزها البرامج الآتية:[3]

---

1 –The Parliament of The Republic of Ghana, data protection act 843, date of assent: 10th May, 2012

2– The Parliament of The Republic of Ghana, **cyber security act 1038**, date of assent: 29th December, 2020.

٣– رئاسة مجلس الوزراء، المجلس الأعلى للأمن السيبرانى، الأستراتيجية الوطنية للأمن السيبرانى (٢٠١٧–٢٠٢١)

١- برنامج تطوير الإطار التشريعي لتأمين الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية، بمشاركة من الأطراف المعنيين، وذوي الخبرة في القطاع الحكومي والخاص والأكاديمي ومؤسسات المجتمع المدني، مع الاسترشاد بالخبرات والتجارب والبرامج الدولية ذات الصلة.

٢- برنامج تطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبراني وتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات، وذلك بإعداد وتفعيل ما يعرف بفرق الاستجابة لطوارئ الحواسب (CERTs) أو فرق مواجهة حوادث أمن الحواسب (CSIRTs) داخل القطاعات الحيوية على المستوي الوطني، على أن تكون هذه الفرق مسئولة عن أعمال المتابعة الأمنية لشبكات الاتصالات والمعلومات الوطنية والتعامل مع أية أخطار سيبرانية تهددها.

وتماشيا معَ اتجاهِ الدولةِ إلى مواكبةِ التطورِ التكنولوجيِ والاستفادةِ منْ التطبيقاتِ التكنولوجيةِ الحديثةِ، اتخذتْ الحكومةُ الكثيرَ منْ الخطواتِ التي تهدفُ إلى تعزيزِ إجراءاتِ الأمنِ السيبراني، وإيجادَ بيئةٍ رقميةٍ آمنةٍ تسهمُ في تنفيذِ سياساتِ الدولةِ الراميةِ إلى التوسعِ في التحولِ الرقميِ، وتقديمَ خدماتِ الحكومةِ الإلكترونيةِ، اشتملتْ على تشكيلِ والأجهزةِ المعنيةِ بقضايا الاستخدامِ الآمنِ للفضاءِ السيبراني أبرزها الآتي:

1 – المجلسُ الأعلى للأمنِ السيبراني: تضمنَ قرارُ رئيسِ مجلسِ الوزراءِ رقمِ (2259/ 2014) على تشكيلِ مجلسِ أعلى لأمنِ البنى التحتيةِ للاتصالاتِ، وتكنولوجيا المعلوماتِ يتبعُ لرئاسةِ مجلسِ الوزراءِ تحتَ مسمى (المجلسُ الأعلى للأمنِ السيبراني)، ويختصَ المجلسُ بالمهامِ التاليةِ: تحديدُ البنى التحتيةِ الحرجةِ على المستوى الوطنيِ واعتمادِ أطرٍ واستراتيجياتِ وسياساتِ التأمينِ الملاءمةِ لها، وضعُ آلياتِ رصدِ المخاطرِ والتهديداتِ السيبرانية، وتحديدَ المهامِ للجهاتِ المعنيةِ بالتعاملِ معها، وإعدادَ الكوادرِ اللازمةِ لمواجهتها على المستوى الوطنيِ، وضعُ خططِ وبرامجَ للبحثِ العلميِ والتطويرِ في مجالِ الأمنِ السيبراني بالتعاونِ معَ

الجهاتِ البحثيةِ والأكاديميةِ على المستوى الوطنيِ، وبالتنسيقِ معَ الجهاتِ المناظرةِ لهُ إقليميا ودوليا.[1]

2- الجهازُ القوميُ لتنظيمِ الاتصالاتِ (NTRA): يعدْ الجهةَ المسئولةَ عنْ إدارةٍ وتنظمُ قطاعَ الاتصالاتِ في جمهوريةِ مصرَ العربيةِ بمقتضى القانونِ رقمِ (10) لسنةِ (2003) ويعملُ الجهازُ على ضمانِ تقديمِ خدماتِ الاتصالاتِ بكفاءةٍ وفعاليةٍ في جميعِ أنحاءِ البلادِ، وتوفيرَ البيئةِ الملاءمةِ لتعزيزِ مجتمعِ المعرفةِ والنهوضِ بقطاعِ تكنولوجيا المعلوماتِ والاتصالاتِ، بالإضافةِ إلى المهامِ الرقابيةِ الموكلةِ للجهازِ للتأكدِ منْ الالتزامِ بتنفيذِ المعاييرِ الصحيةِ والبيئةِ في كلِ المراكزِ التقنيةِ المسئولةِ عنْ تقديمِ الخدمةِ في البلادِ طبقا للمعاييرِ الدوليةِ المعمولِ بها.[2]

3 - المركزُ الوطنيُ لطوارئِ الحاسباتِ والشبكاتِ (EG-CERT): تمَ تشكيلُ المركزِ كأحدِ الكياناتِ التابعةِ للجهازِ القومي لتنظيمِ الاتصالاتِ في غضونِ شهرِ أبريلَ عام (2009)، ويقدمَ المركزُ الدعمُ اللازمُ لحمايةِ البنيةِ التحتيةِ الحرجةِ، والقطاعُ الماليُ ويتولى مهمةَ الاستجابةِ للحوادثِ السيبرانية والتنسيقُ بينَ الأطرافِ المعنيةِ بالتعاملِ معَ تلكَ الحوادثِ، واتخاذَ إجراءاتٍ استباقيةٍ وقائيةٍ لتعزيزِ أمنِ البنيةِ التحتيةِ الحرجةِ منْ خلالِ تحليلِ البرمجياتِ الخبيثةِ، واستخدامَ الهندسةِ العكسيةِ للوصولِ إلى مدى خطورةِ البرمجياتِ المستخدمةِ في الهجماتِ السيبرانية وأنسبُ أسلوب للتعاملِ معها، فضلا عن تبادلَ المعلوماتِ حولَ خبراتِ التعاملِ معَ مختلفِ صورِ التهديداتِ السيبرانية معَ المراكزِ المماثلةِ على المستوى القاريِ والدولي.

١- قرار مجلس الوزراء 2259 لسنة 2014 بشأن إنشاء المجلس الأعلى للأمن السيبراني، الجريدة الرسمية العدد ٥٠ مكرر (أ) بتاريخ ١٥ / ١٢ / ٢٠١٤

٢- قانون تنظيم الاتصالات، القانون رقم ١٠ لسنة ٢٠٠٣، الجريدة الرسمية العدد ٥ مكرر (أ) بتاريخ ٤ فبراير لسنة ٢٠٠٣.

وعلى صعيدِ تطويرِ الإطارِ التشريعي ليوائمَ البيئةَ الافتراضيةَ التي أوجدتها التطوراتُ التكنولوجيةُ الحديثةُ،صدرتْ عددا منْ القوانينِ التي تساعد على تنظمُ العملَ باستخدامِ التطبيقاتِ التكنولوجيةِ الحديثةِ التي تتمثلُ في الآتي:

1 – قانونُ مكافحةِ جرائمِ تقنيةِ المعلوماتِ رقم (2018/175): وتضمنَ القانونُ التوصيفُ الجنائيُ للأنشطةِ غيرِ المشروعةِ التي تتمُ بواسطةِ التقنياتِ الرقميةِ، والتي تمثلُ اعتداءً على حقوقِ مستخدمي التطبيقاتِ التكنولوجيةِ الحديثةِ خاصةً شبكةَ المعلوماتِ الدوليةِ (الإنترنت) مثل الدخولِ غيرِ المشروعِ على الصفحاتِ والمواقعِ الشخصيةِ بغرضِ الحصولِ على معلوماتِ أوْ تغيرِ المحتوى بشكلٍ يضرُ بمنْ أنشأَ أوْ أدارَ تلكَ المواقعِ أوْ الصفحاتِ، اختراقَ الأنظمةِ بغرضِ الحصولِ على المعلوماتِ أوْ التخريبِ الكلي أوْ الجزئي لمكوناتِ النظامِ، ممارسةُ كلِ الأنشطةِ غيرِ المشروعةِ مثلِ الترويجِ للبضائعِ المقلدةِ أوْ المسروقةِ أوْ الموادِ المخدرةِ وغيرها، كما تضمنَ القانونُ الإجراءاتِ المنظمةَ لعملِ عناصرِ إنفاذِ القانونِ المختصةِ برصدِ وتتبعَ العناصرَ الإجرامية وأسلوبَ جمعِ الأدلةِ الإلكترونيةِ اللازمةِ لتقديمهمْ للعدالةِ.

2 – قانونُ حمايةِ البياناتِ الشخصيةِ رقمِ (2020/151): يحددَ القانونُ العلاقةَ بينَ المعنى بالبياناتِ منْ جهةِ ومستخدمي البياناتِ كالحائزِ والمتحكمِ والمعالجِ ويوضحُ حقوقَ المعنى بالبياناتِ وشروطِ جمعها ومعالجتها، والتزاماتُ المتحكمِ والمعالجِ، كما ينظمُ إجراءاتِ استخدامِ البياناتِ الشخصيةِ باستخدامِ التطبيقاتِ المرتبطةِ بشبكةِ المعلوماتِ الدوليةِ (الإنترنت) مثل التسويقِ الإلكتروني وتحويلِ الأموالِ وغيرها منْ التطبيقاتِ، ونصَ القانونُ على الجرائمِ الخاصةِ بالتعاملِ معَ البياناتِ الشخصيةِ العقوباتِ المترتبةِ على ذلكَ، كما يؤسسُ القانونُ لإنشاءِ مركزِ حمايةِ البياناتِ الشخصيةِ الذي تتحددُ مهامهُ في الرقابةِ على إنفاذِ قانونِ حمايةِ البياناتِ الشخصيةِ، وإصدارَ التراخيصِ والتصاريحِ والاعتماداتِ اللازمةِ لمزاولةِ الشركاتِ أنشطتها واختصاصها في جمعِ ومعالجةِ بياناتِ المستخدمينَ .

- **خاتمة**

أظهرَ التفاعلُ الأفريقيُ معَ المعطياتِ التي فرضها التطورُ المطردُ في تكنولوجيا المعلوماتِ والاتصالاتِ، غيابُ النظرةِ الشموليةِ لكيفيةِ تطويعِ التطبيقاتِ التكنولوجيةِ الحديثةِ وتعظيمِ الاستفادةِ مما تتيحهُ منْ إمكانياتٍ لدفعِ عجلةِ التقدمِ ودعمِ الاستقرارِ السياسيِ والاجتماعيِ على الصعيدِ الوطنيِ والقاريِ، حيثُ تعدْ القارةُ الأفريقيةُ هيَ الأقلُ استفادةً منْ التطوراتِ التكنولوجيةِ الحديثةِ، على الرغمِ مما تملكهُ منْ مقوماتٍ تسهمُ في أنْ تكونَ القارةُ أحدَ أهمِ القوى المؤثرةِ في الفضاءِ السيبرانىْ.

وطبقًا لمؤشر الأمن السيبراني العالمي الصادر عن الاتحاد الدولي للاتصالات (GCI) تعد القارة الأفريقية الأضعف على مستوى مناطق العالم في تطبيق المعايير الدولية للأمن السيبراني، وأظهر مؤشر التقييم أن الكثير من البلدان الأفريقية لا تزال تظهر مستويات ضعيفة لمعالجة القضايا المتعلقة بالأمن السيبراني حيث تفتقر للمقومات الأساسية للأمن السيبراني، على الرغمِ منْ الجهودِ المبذولةِ على المستوى القاريِ المتمثلةِ في إطلاقِ مفوضيةِ الاتحادِ الأفريقيِ اتفاقيةَ الاتحادِ بشأنِ الأمنِ السيبراني وحمايةُ البياناتِ الشخصيةِ للعملِ بها كإطارِ قاريْ موحدٍ؛ وعلى المستوى الإقليميِ منْ خلالِ المبادراتِ المطروحةِ منْ التجمعاتِ الاقتصاديةِ الإقليميةِ لتعزيزِ الأمنِ السيبراني بالدولِ الأعضاءِ إلا أنَ غيابَ الارداة السياسيةَ للعملِ على مجابهةِ التهديداتِ السيبرانية منْ خلالِ إطارٍ جماعيٍ وتغليبِ النزعةِ الوطنيةِ إثر بالسلبِ على تلكَ الجهودِ منْ جهةٍ، وساهمَ في تميزِ بعضِ دولِ القارة الأفريقيةِ منْ جهةٍ أخرى.

ويرجع غياب الأطر المنظمة للأمن السيبرانى على المستوى القارى والاقليمى إلى غياب الآليات الداعمة للدور الذي يجب ان تلعبه المنظمات الافريقية متعددة الأطراف داخل القارة الافريقية، والتي تلزم الدول الأعضاء بتنفيذ الاتفاقيات والقرارات الصادرة عنها، وتصهر المصالح الفردية للدول فى بوتقة العمل الجماعى لصالح كافة دول القارة، على عكس الوضع الحالي لتلك المنظمات والتي لا يتعدى دورها عن اصدار التوجيهات والأطر الاسترشادية للدول الأعضاء.