

تأثير الجريمة الالكترونية على الأمن في إفريقيا

The impact of cybercrime on security in Africa

فتيحة حيمر *

جامعة علي لونيسي البلدية 02 – الجزائر

f.himer@yahoo.fr

تاريخ النشر: 2024/06/30

تاريخ القبول: 2024 /04/12

تاريخ الارسال: 2024/01/15

ملخص:

أدى ظهور الجرائم الالكترونية كنمط جديد من أنماط الجريمة وما تتميز به هذه الجرائم من خاصية عابرة للحدود الإقليمية للدول، الى توجه المجتمع الدولي بما فيه الإفريقي للتعاون من أجل تصدّد دامن لتلك الجرائم التي لها بالغ الأثر السلبي على الأمن القومي للدول، ونظرا لارتباط تلك الجريمة بالتطور التكنولوجي مما يستوجب معه أن يكون القائمون على مكافحة تلك الجرائم على درجة عالية في استخدام الحاسبات الآلية، فقد اتجهت دول العالم إلى عقد دورات تدريبية متخصصة ومستمرة لأفراد من المهارة الأمن، من أجل التعرف المستمر على الفنيات الدقيقة التي تساعد على كشف الجريمة ومرتكبها، وذلك لمواكبة الركب التكنولوجي في العالم والقدرة على اكتشاف التطور في الجريمة الالكترونية. لذلك يقدم هذا المقال توصيات بوضع التشريعات والقوانين اللازمة لمعاقبة وردع مرتكبي الجرائم الالكترونية، وتقديم النصائح والحلول الفنية لمستخدمي الوسائط الالكترونية للتقليل من خطورة وأثر هذه الجريمة في إفريقيا.

الكلمات المفتاحية: الجريمة الالكترونية، الأمن، الأمن المعلوماتي، الأفريبول.

Abstract :

The emergence of cybercrime as a new type of crimes and its transnational characteristic has led the international African community to cooperate to tackle these crimes which have a very negative impact on the national security of states. As cybercrime is linked to technological development, which requires that those who fight these crimes have a high degree of skill in using computers, world countries tended to hold specialized and continuous training courses for security personnel. This was meant to continuously identify the precise techniques that help to detect crime and its perpetrator in order to keep pace with the technological process in the world and to be able to discover the development in cybercrime. So the article provides recommendations to legislation and laws to punish and deter the perpetrators of cyber crimes and providing advice and technical solutions for users of electronic media to reduce the risk and the impact of this crime.

Keywords: Cybercrime, Security, Information security, Afripol .

مقدمة:

أدت التطورات المتلاحقة في علوم الحاسب الآلي وتقنية المعلومات وشبكة الانترنت إلى نقلة علمية وتطبيقية هائلة في كافة مجالات الحياة، ومع الاستخدام المكثف لشبكة الإنترنت برزت ظاهرة الجريمة الإلكترونية بأنواعها المختلفة في عقد التسعينات من القرن الماضي، وارتفعت معدلاتها بشكل متسارع، وأدرك المجتمع الدولي مدى الحاجة الماسة لتعاون دولي وإقليمي فعال، يكبح جماح الجريمة الإلكترونية ويحد من مخاطرها الاقتصادية والاجتماعية والأمنية، بعد الارتفاع الكبير في عدد مستخدمي شبكة الإنترنت حول العالم بما في ذلك القارة السمراء، والتي شهدت هي الأخرى بدايات القرن 21 م نموا سريعا ومتزايدا في مجال التكنولوجيا الحديثة، لكن ذلك النمو رافقه تزايد في الجرائم الالكترونية، الأمر الذي جعل التكنولوجيات في جلّ الدول الأفريقية نقمة أكثر من نعمة، كونها أضرت ليس بالإفراد فقط، بل حتى بالمؤسسات الاقتصادية، المالية والسياسية، مشكلة بذلك تهديدا مباشرا للأمن في إفريقيا، لذلك الكثير من المهتمين بالوضع في إفريقيا يرون أن التهديدات الأمنية بها لم تعد مقتصرة على مخاطر من أمثال الارهاب، وتهريب المخدرات والاتجار بالبشر والهجرة غير الشرعية فقط، بل أكبر مهدد في الوقت المعاصر هو الانتشار الرهيب للجرائم الالكترونية بسبب الرقمنة التي مست شتى مجالات الحياة. تلك الجرائم تشكل حرجا عثرا أمام ارساء دعائم الأمن الذي تنتشده دول هذه القارة، بغية تحقيق أهداف التنمية بها والارتفاع ببلدانها الى مصاف الدول المتقدمة.

إشكالية البحث:

تكمن مشكلة البحث في تفاقم الجريمة الإلكترونية تزامنا وارتفاع عدد مستخدمي الانترنت إفريقيا، بل وتعدد أنواعها، وازدياد حجم خسائرها وأضرارها، بحيث أصبحت مهددا حقيقيا لأمن المعلومات في كافة المجالات العامة والحيوية بالقطاع العام والخاص، وعلى مستوى الأفراد، بل مصدر خطورة على السلم والأمن في إفريقيا، بسبب استخدام الانترنت في النشاطات الإرهابية. ومن هذا المنطلق سنبحث في هذا المقال الإشكالية التالية: ما مدى تأثير الجرائم الالكترونية على الأمن في إفريقيا؟. وتختبر الدراسة الفروض أدناه:

- كلما زادت الجرائم الالكترونية غاب الأمن المعلوماتي.
- يصبح أمن الدولة مهددا كلما غاب الأمن المعلوماتي.
- تفاقم الجرائم الالكترونية في الدول الأفريقية أخلّ بالأمن المعلوماتي ومنه بالأمن عامة في ظل الرقمنة. تسعى الدراسة الى بلوغ أهداف منها:
- من منطلق ادخال التكنولوجيا ورقمنة الأنشطة في كافة المجالات، نهدف الى إبراز التأثيرات السلبية للجرائم الالكترونية على الأمن بالدول الافريقية، والتي لا يمكن معرفتها إلا من خلال التعرض لتأثيراتها على الأمن المعلوماتي أولا.
- الوقوف على الجهود المبذولة افريقيا لمحاربة الجرائم الالكترونية.
- إبراز دور انعدام الأمن المعلوماتي في افقاد الدول الافريقية الأمن بأبعاده المختلفة.

- تقديم مقترحات من شأنها تعزيز الأمن (عامة والأمن المعلوماتي خاصة) والحد من انتشار الجرائم الالكترونية في إفريقيا.

ويتم تناول الموضوع من خلال تناول العناصر أدناه:

أولا : التأصيل المعرفي للجريمة الالكترونية والأمن

ثانيا: مظاهر الجرائم الالكترونية وعوامل التفاقم في إفريقيا

ثالثا: آليات وصعوبات مكافحة الجرائم الالكترونية في إفريقيا

رابعا: تأثيرات الجرائم الالكترونية على الأمن في إفريقيا وكيفية التعامل معها

منهجية البحث:

سنبحث هذا الموضوع بالاعتماد على المنهج الوصفي من خلال جمع البيانات والمعلومات للتعرف على حيثيات الظاهرة محل الدراسة، ثم تحليلها وربطها بمتغيرات الدراسة الأمن والأمن المعلوماتي في أفريقيا، إضافة الى منهج دراسة الحالة كون المقال سيتناول ظاهرة الجريمة الالكترونية وتأثيرها على الأمن في القارة الافريقية.

أولا: التأصيل المعرفي للجريمة الالكترونية والأمن

تتطلب مختلف الدراسات والأبحاث في خطوة هامة منها تحديد مفاهيمها الإجرائية، قصد ارشاد القارئ الى المعنى الذي سيتم توظيفه خلالها من قبل المؤلف. وعليه نحدد ضمن هذا المحور معنى كل من مفهومي الجريمة الالكترونية والأمن.

1. التأصيل المعرفي للجريمة الالكترونية :

لقد شاع تداول هذا المصطلح كثيرا في الآونة الأخيرة بين فقهاء القانون ورجال الأمن والسياسة والاقتصاد، بسبب ظهوره في كل المجالات وإضراره بها. فيا ترى ماذا يقصد به؟ وما أنواعه؟ وما الذي يميزه عن غيره من الجرائم الأخرى؟.

1.1. تعريف الجريمة الالكترونية:

يطلق عموما لفظ الجريمة على كل فعل أو سلوك غير مشروع مخالف للحق والعدل المستقيم الذي يترتب عنه عقوبة قانونية.¹ عرّفت منظمة التعاون الاقتصادي والتنمية الجريمة الالكترونية بأنها: " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".² بمعنى أنها تعني القيام بفعل أو اعتداء على الضحية سواء كان فردا أو مؤسسة أو غيرها بما يلحق بهم الضرر سواء ماديا أو ماليا أو معنويا، وباستخدام طرق تقنية وتكنولوجية متطورة يصعب معها التعرف على الجاني بسهولة. وهو المعنى الذي أكده الاستاذ توماس سميدينكوف Thomas_J. Smedinghoff في تعريفه لها بأنها: "أي ضرب من النشاط الموجّه ضدّ أو المنطوي على استخدام نظام الحاسوب".³ وأيضا الأستاذ: دافيد تومبسون David Thompson في قوله هي: "أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى

فاعلمها معرفة بتقنية الحاسب".⁴ أما الدكتور عبد الفتاح مراد فعرف جرائم الانترنت على أنها: "جميع الأفعال المخالفة للقانون والشرعية والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت وهي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات سواء لارتكابها أو للتحقيق فيها، ويقصد بها أيضا أي نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الانترنت مثل مواقع الانترنت وغرف المحادثة أو البريد الالكتروني كما تسمى كذلك في هذا الإطار بالجرائم السيبرية أو السيبرانية لتعلقها بالعالم الافتراضي".⁵ وهو تعريف حدد أن هذه الجرائم تقع في العالم الافتراضي، وأن من يحقق فيها أيضا يجب أن تكون له الخبرة والإلمام بتقنيات الحاسب الآلي، وطرق التعامل بوسائل الاتصال والتواصل الالكتروني للكشف عن خيوط الجرم.

المستخلص مما تقدم أن الجرائم الإلكترونية ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية الحديثة. وهي كل فعل أو سلوك يقع ضمن استخدام لجميع أشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصالات دورا أساسيا.⁶

2.1. خصائص الجريمة الالكترونية:

تتميز الجريمة الالكترونية عن غيرها من الجرائم بعدة خصائص أهمها:

- جريمة عالمية: لا تستثني أحد، فكل دول العالم مهددة بهذا النوع من الجرائم في ظل الانتشار الهائل للعمل بشبكة الاتصالات الدولية الانترنت، الأمر الذي سهل عمل مجرمي الفضاء الافتراضي في استهداف الضحية في أي زمان ومن أي مكان، وتخطت بذلك الجرائم الالكترونية كل الحدود الدولية.⁷
- صعوبة الإثبات: أي تعذر الحصول على ما يثبت وقوع هذا النوع من الجرائم، كونها تحدث في عالم افتراضي يتسم بالدينامكية والحركية السريعة، يصعب معه العثور على الأدلة الرقمية⁸ كون الجاني لا يترك خلفه أي أثر مادي، بل يضع رموز سرية تعيق الوصول لذلك، ولهذا ما يتم اكتشافه من هذه الجرائم يكون بالصدفة أو بعد فوات وقت معتبر على حدوثها، وعليه ما لم يكتشف منها أكثر بكثير مما كشف عنه.
- جرائم ناعمة: أي لا يحتاج مرتكبها الى أي جهد عضلي كالقتل أو السرقة، بل كل ما يحتاجه الجاني الذكاء والتفكير الذهني المصحوب بالمعرفة التقنية والحاسوبية الفائقة، إضافة الى القدرة على استخدام الانترنت.
- هي جرائم تتميز بأنها أقل عنفا من الجرائم التقليدية، فليس هناك شعور بعدم أمان تجاه المجرمين في مجال المعرفة المعلوماتية لأن مرتكبها ليسوا محترفي الإجرام.⁹
- غياب التبليغ عنها للجهات المتخصصة في مكافحتها: بسبب ما قد يترتب عن القيام بذلك من أضرار تلحق بسمعة أو مكانة، أو الوظيفة المجني عليه، خاصة اذا كان الضحية هيئة فالضرر مضاعف.
- أنها سهلة الحدوث، أي من السهل ايقاع الجرم بالمستهدف منها لصعوبة مراقبتها والحد منها.
- أنها جرائم تلحق بالضحايا أضرارا وخيمة يصعب حتى قياسها.
- أنها تتطلب أساليب وتقنيات جد متطورة لاكتشافها، فليس من السهولة بمكان تعقب مرتكبها.¹⁰

3.1. صور الجريمة الإلكترونية:

تتخذ هذه الاخيرة عدّة صور، نبين أهمها أدناه:

- جريمة الدخول غير المشروع: أي بدون ترخيص من الجهة المخولة منح هذه الصلاحية .
- تخريب الأجهزة الالكترونية أو احدى مكوناتها كالحاسوب، أو اتلاف البيانات المحفوظة بداخله.
- صناعة الفيروسات أو نشرها: قصد اتلاف المعلومات وتعطيل البرامج.
- التغيير في مواصفات وخصائص تقنية المعلومات.
- سرقة الأجهزة والمكونات أو المعلومات المخزنة بها.
- جرائم النظام العام والآداب العامة والتجارة في الجنس البشري من خلال إنشاء مواقع تعمل على الترويج للأفكار والبرامج المخالفة للنظام العام والآداب، مثل انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة للأفراد، والإساءة إلى سمعة الضحية، والدعارة وتعاطي المخدرات وانتهاج طرق تبويض الأموال و...غيرها.
- جرائم الكترونية تستهدف سلامة الدولة وأمنها الداخلي والخارجي.¹¹ فغرضها سياسي محض، ومثالها شن هجمات على المواقع الرسمية للحكومات وأنظمتها، أو سرقة معلومات تتعلق بأمن الدولة، أو تدمير مواقع عسكرية ومعلوماتية في زمن الرقمنة.
- جرائم الاعتداء على الملكية الفكرية: من خلال نقل برامج ضارة بما يحتويه جهاز الضحية. كما أن الأبحاث العلمية اليوم أصبحت متاحة الكترونيا على شبكة الانترنت، ويتم نسخها وتداولها بكل سهولة ويسر من غير أن تتسبب لمؤلفيها، وهو الأمر الذي يضر بالحقوق الفكرية للمؤلف والحقوق المجاورة.
- تزوير التوقيع الإلكتروني الذي يقوم مقام التوقيع الكتابي.¹²
- جرائم تستهدف هوية الأفراد الإلكترونية كالحصول على البريد الإلكتروني وكلمة السر الخاصة بهم، والأدهى من ذلك أنها تمتد حتى إلى انتحال الشخصية الإلكترونية، وسحب مختلف الصور والملفات الموجودة في جهاز الضحية واستخدامها كسلاح يهدده به، فيصبح تحت السيطرة..، ومنها أيضا جرائم الشتم والقذف والتشهير للإساءة الى سمعة المجني عليهم.
- جرائم الابتزاز الالكتروني تستهدف المؤسسات المالية والبنكية.¹³

2. مفهوم الأمن:

يعتبر الأمن أحد المفاهيم التي تتسم بالغموض، وغياب إجماع حول تحديد معناها بدقة، وذلك بسبب تعدد أوجه الأمن وأبعاده.

1.2. تعريف الأمن:

بداية الأمن والأمان، والأمانة، والمنة نقيض الخوف. لكن الأمن أحد المفاهيم اللغوية الثرية في المعنى، كونه يعني: عدم الخيانة، التصديق، الحفظ، الطمأنينة، الدين، الثقة، القوة، الإجارة، السلم. فحسب لسان العرب الأمن هو: "حصيلة مجموعة من الاجراءات والتدابير التربوية والوقائية والعقابية التي تدين بها الأمة ولا تتناقض مع المصالح والمقاصد المعتمدة". وحسب هنري كسنجر الأمن يعني: "أي تصرفات يسعى المجتمع عن طريقها الى حفظ حقه في البقاء". وحسب روبرت مكنمارا الأمن يعني: "التطور والتنمية، سواء منها الاقتصادية أو الاجتماعية أو السياسية في ظل حماية مضمونة". أما عند دومينيك دافيد (Dominique David) فالأمن يتمثل في: "خلو وضع ما من التهديد أو أي شكل للخطر، وتوفر الوسائل اللازمة للتصدي لذلك الخطر في حال أصبح أمرا واقعا". يتضح من كل ذلك أن الأمن يتحقق عندما تتحرر الدولة والإنسان فيها من مشاعر الخوف والقلق والتوتر لزوال ما يسبب تلك المشاعر من المخاطر الحسية. وشعور الدولة بالاطمئنان لاستيفاء مواطنها لاحتياجاتهم ومتطلباتهم المشروعة، بما في ذلك احتياجات تحقيق العدالة الاجتماعية والاقتصادية.¹⁴

2.2. أبعاد الأمن:

لقد أوضحت التعاريف المقدمة لتحديد معني مفهوم الأمن أن هناك العديد من الأبعاد لهذا الأخير تؤثر على بعضها البعض وعليه بالضرورة، كما أوضحت أيضا أنه إذا هددت كلها أو بعضها يصبح الأمن كله مهددا أو قابل للاختراق، فيا ترى ما هي تلك الأبعاد؟.

1.2.2. البعد السياسي: ويعتبر بعد جد هام يرمي الى توفير القدرة والقوة للدولة حتى تتمكن من تنظيم شؤون الرعية على أحسن وجه، كالعمل على حسن استغلال الموارد المختلفة في الداخل وجلب ما ينقصها من الخارج حتي تستطيع تلبية مختلف حاجات ومطالب المجتمع المتعددة، المتنوعة واللامتناهية. فتتغلب على مشاكلها وتصبح مصدر قوة وتأثير على المجتمع والسياسة الدوليين.

2.2.2. البعد الاقتصادي: بعد مكمل للبعد السابق لأنه يهتم بكيفية توفير المستلزمات المادية والمالية الكافية للوفاء بتلك المطالب المجتمعية التي تسعى الدولة جاهدة لتلبيتها تحقيقا للرفاه الاجتماعي، وبذلك تعطي القوة الاقتصادية للدولة ثقلا سياسيا على المستويين الاقليمي والعالمي هذا من جهة، ومن جهة أخرى تعد الركيزة الهامة والحيوية للقوة العسكرية، كيف ذلك؟ كونها (أي القوة الاقتصادية) تعمل على:

- توفير اكتفاء ذاتي من الاحتياجات المجتمعية.
- تعمل على تحويل الصناعات الحربية الهامة لتأمين مختلف المعدات والأسلحة التي تحتاج إليها القوة العسكرية.

• توفر الثروة المالية اللازمة لشراء كل ما ينقص القوة العسكرية من السوق الخارجية.

كل ذلك من شأنه تقوية ودعم القوة العسكرية بشكل كبير، وتعود طبعا القوتان الاقتصادية والعسكرية بالفائدة على القوة السياسية، حيث تتزايد قدرة وكفاءة الدولة نتيجة مساندة كل قوة للأخرى بالاستفادة من الامكانيات الكبيرة للقوة الاقتصادية والعكس صحيح أكيد.

3.2.2. البعد العسكري: وهو أكثر الأبعاد فاعلية ولا يسمح بضعفه أبداً، كونه يعرض أمن الدولة لتهديدات قد توقعها تحت الاحتلال أو تلغيها وتضمها لدول أخرى، أو تقسمها الى دويلات، أو اقتسامها مع الآخرين، أو طلب الحماية من دولة أجنبية تصبح تنتهك أمنها لقاء تأمينها من أخطار أخرى. وتوفر القوة المسلحة بالقدر الكافي مع تواجد الارادة القوية لاستخدامها، ردعا لكل من يفكر في ضرب مصالحها.

4.2.2. البعد الاجتماعي: يركز هذا البعد على اعداد المواطن صحيا، وعقليا (ثقافيا)، وأخلاقيا ضمن اطار ديني وثقافي، وموروث اجتماعي من تقاليد وعادات مجتمعية. ويهدف بذلك هذا البعد الى حماية النسيج الاجتماعي من التمزق والتناثر من خلال الحفاظ على انسجامه وتماسكه ومنه توازنه، خاصة وأن تحقيقه يقتضي بداية دراسة شاملة لمختلف قطاعات الأمن الأخرى. حتى يمكن الاستفادة من عوائده على تلك القطاعات.

5.2.2. البعد البيئي: يتمحور حول حماية النظام الايكولوجي الذي يرتكز بدوره على بقاء واستمرار الأصناف الحية، والحفاظ على البيئة وابتعادها عن مخاطر التهديد من الكوارث الطبيعية والتلوث والتصحر، فقد يتدهور النظام البيئي بفعل الحروب والنزاعات المسلحة من خلال مؤشرات تراجع الانتاج الغابي، والتلوث البيئي، وانقراض حيوانات ونباتات، ومن جهة أخرى ارتباط الأزمات الأمنية بمظاهر الندرة في الموارد الطاقوية والطبيعية، والتي غالبا ما تثير نزاعات وأزمات حول كيفية استغلالها.¹⁵

ثانيا: مظاهر الجرائم الالكترونية وعوامل تفاقمها في إفريقيا

تشتمل الجريمة المنظمة بدول القارة الافريقية على أشكال مختلفة من السلوك الإجرامي. الفئة الأولى منها تتسم باستخدام العنف (كالقتل والابتزاز والتجارة غير المشروعة، فضلا عن علاقتها بمسؤولين داخل الدولة)، وتضم عصابات المدينة والشبكات الإجرامية في كيب تاون بجنوب إفريقيا وتعمل بالتوازي مع المافيا الإيطالية. والفئة الثانية فتعد أكثر تعقيدا، تعمل كشبكات تتصل بالجماعات داخل وخارج القارة، مع التركيز على نقل المنتجات أو الموارد غير المشروعة، فهناك مثلا نخبا سياسية متورطة في التجارة غير المشروعة مع الشبكات الإجرامية في شرق وجنوب إفريقيا. أما الفئة الثالثة، فتشهد تقاطعا قويا بين المنظمات السياسية - الميليشيات أو الجماعات المسلحة - وعمليات التجارة غير المشروعة أو التهريب. وتعتبر ليبيا والساحل والقرن الإفريقي خير مثال على هذه الفئة. وآخر شكل من أشكالها بالقارة هي الجريمة السيبرانية، وهو النوع الذي تركز عليه دراستنا هذه. فعلى الرغم من إيجابيات التطور السريع للتكنولوجيا في إفريقيا، إلا أن ذلك قابله التفاقم الرهيب للجرائم الالكترونية بها، لكن السؤال المطروح هنا: ما الذي يدل على ذلك التفاقم؟ وما العوامل المتحكمة فيه؟.

1. التهديدات السيبرانية في أفريقيا:

إنّ الوضع الالكتروني والمعلوماتي في افريقيا يتعرض بين الفينة والأخرى الى العديد من التهديدات، نوجز أهمها فيما يلي:

- وصول رسائل الكترونية مزورة الى البريد الشخصي للأفراد تزعم أنّها من مصادر شرعية وتطلب منهم تقديم معلومات تتعلق بحياتهم الخاصة أو حتى أحوالهم المالية والكشف عنها ضنا منهم أنّهم في أمان .
- الابتزاز الرقمي: ويأخذ عدّة أشكال منها استدراج ضحايا وإقناعهم بضرورة تقديم صور جنسية أو غيرها من الأمور المثيرة للشبهات تستغل في ابتزازهم، وبما يحقق مبتغاهم الذميمة.
- برمجيات انتزاع الفدية: يعمل مجرمو الفضاء الافتراضي على تعطيل المنظومات الحاسوبية للعديد من المؤسسات والمنشآت العمومية الهامة أو الحساسة في المجتمعات، كالمؤسسات الصحية أو القضائية ...، ثم في مقابل إعادة تشغيلها يطالبون الجهات المسؤولة عنها دفع مالا لقاء ذلك.
- برمجيات "البوتنت" الخبيثة: التي تستخدم كوسيلة لشن هجمات الكترونية كبيرة بشكل تلقائي.
- الاحتيال بإصدار أوامر زائفة لتحويل الأموال : وهنا يقوم المجرم باختراق أنظمة البريد الإلكتروني قصد الحصول على البيانات المتعلقة بمنظومات الدفع الخاصة بشركة ما، ليخضع بعدها موظفيها لأوامره، ويجعلهم يوافقون على القيام بتحويل أموال تلك الشركة إلى حساب مصرفي هو عائد إليه في الأساس.¹⁶
- أبان استبيان قامت به وكالة "ترانسيونيون" للتقارير الائتمانية عن أنّ 68% من المبحوثين فيه بجنوب إفريقيا أقرّوا أنّهم وعائلاتهم تعرضوا فعلا للاحتيال الالكتروني منذ بداية الكوفيد 19. كما وضحت بيانات الوكالة أنّ محاولات هذا النوع من الاحتيال الذي يطال الذمة المالية للشركات قد ارتفعت بنسبة 44% سنة 2021، وذلك مقارنة بنسبها قبل جائحة كورونا.
- برامج الفدية: هي أخطر وأكثر أشكال الجرائم الالكترونية انتشارا، تقع هجماتها كل أحد عشر ثانية عالميا. حيث يقوم منفذوها باختراق أنظمة الكمبيوتر وتشفير البيانات الحيوية الموجودة بها حتى يتعذر الوصول إليها، ليطالبوا بعدها الضحية بالزامية دفع الفدية حتى يستعيد تشغيل تلك الأنظمة. فمثلا تعرضت شركة "ترانسنت" بجنوب إفريقيا لهجوم سيبراني خطير تسبب في تعطيل خدماتها بشكل هائل. وهو الأمر الذي أكده "معهد الدراسات الأمنية" بها، حيث أشار الى أنّ هذه الواقعة شكلت أكبر تعطيل تعرضت فيه سلامة البنية التحتية البحرية الحيوية لجنوب إفريقيا، حيث علقت بسببه مرافق الحاويات الآلية والإلكترونية في كيب تاون وديربان، أكثر الموانئ نشاطا وحركية في إفريقيا.

أجرت شركة (سوفوس) لأمان البرمجيات استبيانا بجنوب إفريقيا، وخرجت منه بتقرير عن "حالة برامج الفدية لعام 2021"، ، بينت فيه أنّ نسبة 24% من المبحوثين قد تعرضوا لهذا النوع من الهجوم الخطر . وذكر التقرير أنّ جنوب إفريقيا وزامبيا تعتبران الأكثر تضررا من تلك البرامج في القارة السمراء، وقد بلغ متوسط تكلفة استرداد البيانات المسروقة خلال هجمات برامج الفدية الصناعية في جنوب إفريقيا 447,097 دولارا أمريكيا. يقول المؤسس والمدير التنفيذي لشركة (آي إس ديسيجن)، المهندس فرانسوا أميجورينا: "لم يسبق أن تعرضت الشركات في إفريقيا لابتزاز بمثل هذا التوسع مثلما تتعرض له اليوم، وفي حين حدث عدد من الاعتقالات البارزة

في مجال الجرائم السيبرانية على أيدي أجهزة إنفاذ القانون خلال السنوات القليلة الماضية، فإنّ المجرمين السيبرانيين يواصلون التطور وتنويع ترسانتهم¹⁷.

2. مظاهر تفشي الجرائم الالكترونية في افريقيا:

توجد العديد من المظاهر التي تدل على انتشار الجرائم الالكترونية بالدول الافريقية مثل القرصنة، والتجسس، والاحتيال، والسروقات الالكترونية و... غيرها من الجرائم الكثيرة التي تقع في الفضاء الافتراضي، والتي أثقلت كاهل الأنظمة السياسية والاقتصادية والاجتماعية على المستوى الإفريقي، نذكر منها:

- تزايد عدد مستخدمي الانترنت في إفريقيا بالرغم من تدني نسبة ربط دول القارة بالإنترنت حيث تتذيل إفريقيا الترتيب العالمي في ذلك، فنسبة من يستخدمون شبكة الاتصالات الدولية للإنترنت بها لم تتعدى 28.2 في المائة سنة 2019، وهي نسبة منخفضة مقارنة بمعدلاتها في أوروبا التي قدرت بـ 83 في المائة، وهذا وفق أرقام أوردها "الاتحاد الدولي للاتصالات"، وعليه بالرغم من أن تلك المعدلات المنخفضة إلا أنّ الأمر لم يثني من عزيمة مجموعات الجريمة المنظمة في استغلال الإنترنت بالأمور الصارة¹⁸.
- كثرة الشكاوى المتعلقة بالجرائم الالكترونية أمام السلطات القضائية بالقارة: فقد تم مثلا رصد نحو 4000 شكاوى أمام السلطات القضائية الفرنسية ضد هجمات الكترونية مصدرها الكوديفوار خلال عام 2008 فقط، ويظل الرقم رغم هوله لا يعكس الكم الهائل من الهجمات الالكترونية، كون معظم المتضررين منها لا يبلغون أو يرفعون دعاوى ضد مقترفيها، وعليه تظل الأرقام المعلن عنها غير حقيقية لأنها في الواقع أكثر بكثير.
- تزايد الخسائر الناجمة عن هذا النوع من الجرائم: بلغت الخسائر المادية الناجمة عنها بالقارة سنة 2017 ما يقارب 3.7 مليار دولار موزعة على النحو التالي: ما قيمته 649 مليون دولار في نيجيريا، و 210 مليون دولار في كينيا، و 157 مليون دولار في جنوب إفريقيا، ووفق "التقرير التنفيذي لمخاطر الذكاء الرقمي في إفريقيا" (ACTIR) لعام 2018، الذي تم اعداده من طرف "منتدى الأمن الرقمي في إفريقيا" (ACSC) " فإنّ تلك الخسائر في سنة 2020 بلغت قيمة 2 بليون دولار، وهي نسبة في ارتفاع متزايد باستمرار، الأمر الذي ينبأ بخطورة الوضع بالقارة وتأزمه مستقبلا في حال بقاء الوضع كذلك دون حماية وردع قويين.
- الهجمات الالكترونية: فهي واسعة النطاق وتثير القلق في إفريقيا فبخلاف برامج الفدية أو الهجمات الخاصة الصغيرة، فإنّ تهديد القرصنة والفشل العام الناجم عن هجمات رفض الخدمة (DDos) يسبب أحيانا ضررا لا يمكن إصلاحه. كان هذا هو الحال، على سبيل المثال، في هجوم Mirai botnet في ليبيريا في عام 2016، والذي شل البنية التحتية للإنترنت في البلاد بأكملها. وفي عام 2019، أصيب RSAWEB، أحد مزودي خدمة الإنترنت الرائدة في جنوب إفريقيا، بالشلل ليوم كامل بعد هجوم (DDos) استهدف هجوم آخر، في أوائل عام 2021، البنك الوطني لإثيوبيا. أخيرا في كينيا حيث أدى الهجوم إلى اختراق خدمة Kaseya السحابية، مما أدى إلى إغلاق عشرات الشركات لمدة خمسة أيام تقريبا.¹⁹

الهجمات الالكترونية لم تلحق ضررا بالمؤسسات والمجتمعات في البلدان الأفريقية فحسب بل مست مختلف دول وشعوب العالم، الأمر الذي دفع بمنظمة الأمم المتحدة الى الحث على محاربة هذه الجرائم في القارة، وبالتحديد في دول الغرب الإفريقي.²⁰ ومن بين ما قامت به المنظمة تظاهرة "أكتوبر سيبراني" التي نظمها "مكتب الأمم المتحدة لمناهضة المخدرات والجرائم" (ONUDC) في العاصمة السنغالية داکار، بغرض تبادل المعارف والخبرات الفنية في مجال الأمن الرقمي، وحماية المؤسسات من الهجمات الالكترونية. فتونس مثلا وفي الثلاثي الأول من 2018 سجلت نحو 118 محاولة اختراق الكتروني، ارتفع في الثلاثي الأخير من سنة 2020 إلى حوالي 23 مليون محاولة اختراق، وهي نسب أقرتها "الوكالة الوطنية للسلامة المعلوماتية" بها. أما على المستوى الإفريقي فالهجمات صارت جد مقلقة، ففي استقصاء قامت به شركة كاسبرسكي عرفت القارة السمرء نحو 28 مليون هجوم الكتروني فقط بين شهريّ جوان وأوت من سنة 2020. وتتصدر دول الغرب الإفريقي طبعاً كالسنيغال والكوديفوار ونيجيريا والبنين الدول الإفريقية الأكثر تضرراً من الجرائم السيبرانية، وهو الأمر الذي دفع بمنظمة الاكواس في القمة 76 للمجلس الوزراء المنعقد في أبوجا يوم 19 أوت 2011 الى اتخاذ قرار مناهضة الجرائم الالكترونية في منطقة الغرب الإفريقي.

- تبادل التهم بين الدول في مجال التجسس الالكتروني والهجمات السبرانية، فقد ورد مثلاً في صحيفة لوموند الفرنسية سنة 2018 ، حيث نشرت نتائج استقصاء قامت به حول الموضوع، وتوصلت من خلاله الى أن كافة بيانات ومعلومات مقر الاتحاد الإفريقي تتحكم فيه الصين التي قامت بانجاز نظامه الرقمي وان كان الجانبين الإفريقي والصيني فندا صحة ذلك.

إنّ المستخلص من هذه المظاهر التي تدل على تفاقم الجرائم الالكترونية وامتداد آثارها داخل وخارج القارة السمرء، أنها لم تعد مقتصرة على أمن الأشخاص فقط، بل أصبحت دول القارة أيضاً تحت خطر أكبر وهو الجوسسة الخارجية، واستهداف سيادتها ومؤسساتها ونظمها من قبل القوى الكبرى، تعمل عليه كأولوية مطلقة. وهذا الخطر من المؤكد أنه ليس حكراً على إفريقيا بل كل قارات العالم مهددة به، وأخطر هجوم رقمي تعرض له العالم ذلك الذي استهدف المؤسسات الحكومية، والمخابرات، وأجهزة الأمن، والشركات النفطية في الشرق الأوسط بتاريخ 21 فيفري 2019.²⁰

3. عوامل تفاقم الجرائم الالكترونية في افريقيا:

حسب "حمدون توريه" الأمين العام السابق "للاتحاد الدولي لتكنولوجيات التواصل" إفريقيا حالياً: "أصبحت ملجأً للمجرمين الالكترونيين حيث يمكنهم ممارسة أنشطتهم غير الشرعية في مأمن من كل عقوبة"، والأمر يرجع لعدة أسباب، نذكر أهمها فيما يلي:

- تزايد عدد مستخدمي الانترنت في القارة: فقد بلغ معدل استخدام شبكة الإنترنت في القارة، خلال عام 2011 حوالي 13.5%، وارتفع إلى 28 % بحلول عام 2018. وكان سكان نيجيريا أكثرهم استخداما للإنترنت بالقارة، تلاهم المصريون، فيما رتب سكان ساو تومي، وإريتريا وغينيا الاستوائية، ضمن الدول التي يقل فيها استعمال الانترنت،²¹ والجدول التالي يوضح عدد مستخدميها في إفريقيا.

الجدول 1. عدد مستخدمي الانترنت في إفريقيا (2005/2010/2017/2019)

السنة	نسبة مستخدمو الانترنت بالمائة
2005	2 %
2010	10 %
2017	21.8 %
2019	28.2 %

المصدر: موقع المعرفة، "الانترنت في إفريقيا"، تاريخ التصفح 3 جوان 2023.

<https://m.marefa.org/w/index.php?>

يتضح من الجدول أنّ استخدام الانترنت في إفريقيا يعتبر محدود مقارنة بباقي العالم، وكل المؤشرات المتعلقة بذلك تشير الى أنّ القارة السمراء تعتبر فيما وراء الفجوة الرقمية، ومعظم الأنشطة والبنية التحتية المرتبطة بالانترنت ما بين (2007 - 2013) متركزة حسب موقع المعرفة في جنوب إفريقيا، والمغرب ومصر على التوالي، فضلا عن عدد من الاقتصاديات الصغيرة مثل موريشيوس وسيشل. وبحسب تقرير لموقع إحصائيات الإنترنت العالمي نشر في 1 مارس 2020، بلغ عدد مستخدمي الإنترنت في إفريقيا 526 مليونا من أصل مجموع السكان الذي يقدر بمليار و350 مليونا.²² وحسب تقرير الانترنت الصادر عام 2021 بلغ عدد مستخدمي الإنترنت في أفريقيا حوالي 500 مليون مستخدم، وبحسب إحصاءات نشرتها الأمم المتحدة سنة 2022، تصل نسبة الاتصال بالإنترنت في إفريقيا الى 40 % من سكانها. وفي تقييم لخدمات الانترنت بالبلدان الإفريقية سنة 2022 أقر "الاتحاد الدولي للاتصالات وخدمات المعلوماتية الرقمية"، أنّ مصر تتصدر القائمة، وهو الموضح في الجدول الموالي.

الجدول 2. ترتيب بعض الدول الإفريقية في استخدام الانترنت سنة 2022

البلد	النسبة المئوية لعدد مستخدمي خدمات الانترنت
مصر	71.9%
نيجيريا	51%
جنوب إفريقيا	68.1%
غانا	53%

الكونغو الديمقراطية	17.6%
تنزانيا	25%

المصدر: العربية نت ، "مصر تتصدر إفريقيا في الخدمات الرقمية واستخدام الإنترنت"، "تاريخ النشر: 22 يناير

2023. تاريخ التصفح: 12 جوان 2023. <https://www.alarabiya.net/aswaq/economy/2023/01/22>.

- غياب أطر قانونية كافية تحدد بدقة الفضاء السيبراني والجرائم الماسة به بدول القارة، فالتشريعات بهذا الباب في أغلبها شحيحة، وما تم سنه منها يعتبر غير كافٍ، في ظل التسارع والتغير الكبير الذي يشهده هذا المجال. الأمر الذي يتطلب من الدول الإفريقية إعادة النظر في قوانينها المتعلقة بالموضوع والعمل على تحيينها كلما استدعت الضرورة ذلك.
- ضعف البنى التحتية الرقمية: تفتقر دول القارة الإفريقية في معظمها لوجود بنية تحتية رقمية قادرة على حماية السيادة الالكترونية لدولها، وتوفير الأمن المعلوماتي بها، فالقطاع السيبراني كغيره من قطاعات الأمن الأخرى يعرف هشاشة وضعف كبيرين بها.
- الأوضاع في إفريقيا: سواء السياسية، أو الاقتصادية، أو الاجتماعية أو الأمنية تأخذ حصة الأسد في أجندات دول القارة واستراتيجياتها، وتحوز الأولوية في حياة مجتمعات، وهذا الأمر طبعاً كان سبباً في تأخير وتأجيل اهتمام إفريقيا بمجال التكنولوجيا والاتصال والرقمنة التي لا تحظى بنفس الاهتمام الذي يمنح لمواضيع تعد في نظرها أكثر خطراً من قبيل: الإرهاب، والتهريب، والهجرة غير الشرعية، والأوبئة و... غيرها.²³
- نقص الوعي لدى شعوب القارة الإفريقية بالمخاطر الجمة التي تترصد بهم وبدولهم جراء تزايد استخدام الإنترنت، في مقابل نقص الثقافة الالكترونية إضافة الى نقص الوعي بما ينجم عن عدم التبليغ عن الهجمات والجرائم الالكترونية، ومن لهم الوعي بذلك يرفضون التبليغ لأنهم يخشون من الإبلاغ عن الجرائم أكثر مما يخشونه من الجرائم أنفسهم، نتيجة الحظر، والرسوم القانونية، وزيادة أفساط التأمين، والكشف عن نقاط الضعف والفسل الأمني عن الإبلاغ... وغيرها.²⁴ في هذا الصدد نجد Kritzing and Von Solms يدعمان Kumar كومان في قوله: "إنّ ما يقرب من 80 في المائة من السكان في أفريقيا يفتقرون إلى المعرفة الأساسية بأجهزة الكمبيوتر. على الرغم من انتشار مقاهي الإنترنت، إلا أنّها غير قادرة على تحمل تكاليف برامج مكافحة الفيروسات، مما يجعلها أهدافاً سهلة للقراصنة ومشغلي الروبوتات".²⁵
- تعتبر جائحة كورونا إحدى العوامل التي ساهمت بشكل كبير في تفاقم الجرائم الالكترونية بالقارة الإفريقية والعالم أجمع، وذلك كان من خلال ما صاحبها من تطبيقات أو ملفات ضارة حملت اسم كوفيد 19 كانت وراء سرقة المعلومات الشخصية من أرقام هواتف، وبطاقات ائتمان، وأرقام لحسابات بنكية و... غيرها، وخير مثال على ذلك الهجوم الذي استهدف فروع سلسلة الفنادق العالمية Marriott International الذي تمخضت عنه سرقة المعلومات الشخصية لأزيد من 500 مليون شخص. ويضاف الى ذلك أيضاً ظهور كم هائل من

المواقع الالكترونية التي تنشر مقالات وتقوم بحملات الطيبة تزعم أنها في إطار التوعية بفيروس كورونا ومخاطره، لكنها في حقيقة الامر كانت تقوم بذلك بغرض التضليل لإلحاق الضرر بالأشخاص أو مصالح شركات، أو الدول. وفي تقرير للأمم المتحدة تم رصد حوالي 50 مقالا خلال شهر واحد كلها كانت بقصد التضليل وإلحاق الضرر بالضحية المستهدف من العملية الاجرامية.²⁶

يتبين مما تقدم أنّ تزايد الجرائم الالكترونية بالدول الأفريقية تتحكم فيه عدة عوامل، أبرزها تنامي عدد مستخدمي الانترنت، وضعف البنية التحتية الرقمية، وغياب نظم حماية قوية تجابه بها الاختراقات أو التهديدات الأمنية المعلوماتية، إضافة الى نقص الوعي لدى شعوب القارة بمخاطرها، حيث يغيب التبليغ عنها، دون أن ننسى طبعا الأوضاع الأمنية والسياسية والاقتصادية والاجتماعية المتردية فيها، والتي تشكل مناخا ملائما لاحتضان وانتشار مثل هذا النوع من الجرائم.

ثالثا: آليات وصعوبات مكافحة الجريمة الالكترونية في افريقيا

إنّ الوضع المتأزم في الدول الأفريقية جراء تفاقم الجرائم الالكترونية الماسة بمختلف القطاعات خاصة السياسية منها والاقتصادية والعسكرية، لا ينفي وجود محاولات جادة من قبل دول القارة، تمثلت أساسا في جهود وطنية، وإقليمية، وقارية للتصدي لأخطر جرم يهدد أمن الدول والمجتمعات في عصر الرقمنة.²⁷

1. آليات مكافحة الجريمة الالكترونية في افريقيا:

رغم التصاعد المستمر في أعداد المستخدمين للإنترنت والجرائم الالكترونية منذ بداية الألفية الثالثة، لم تتفاعل حكومات العالم بالقدر المطلوب لحماية الأمن السيبراني، علما بأنّ كل المجتمعات صارت تعتمد بشكل أساسي على شبكات الحاسب الآلي في القطاعين العام والخاص، وعلى مستوى الأفراد، إلاّ أنّه في السنين القليلة الماضية أصبحت حماية أمن المعلومات والاتصالات والشبكات ومواجهة الجريمة الإلكترونية تشكل أولوية في سياسات العديد من الحكومات، فبعد الهجمات الإلكترونية الشهيرة على دولة استونيا عام 2007 Cyber attacks on Estonia انتبعت الكثير من الدول لهذا الخطر الذي يدمر البنى التحتية للمعلومات وتقنية الاتصالات والشبكات، ويعطل كل المرافق الحيوية الاقتصادية والمالية والتعليمية والصحية والاجتماعية في المجالين العام الخاص.²⁸

من أبرز صور التعاون في مجال محاربة الجرائم الالكترونية والحد من انتشارها على المستوى الدولي، الاتفاقيات الدولية التي تعتبر المرجع والإطار التنظيمي والقانوني المنظم والموجه للجهود التي تبذل من أجل منع تفاقم هذا النوع من الجرائم الخطيرة، ومن المعاهدات في هذا الصدد معاهدة بودابست لمكافحة جرائم الإنترنت، وتوصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، ونيينهما فيما يلي:

- توصيات المجلس الأوروبي: لقد دفعت التطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجزائية في هذا المجال إلى إصدار المجلس الأوروبي

التوصية رقم 13 في 11 سبتمبر 1995 في شأن مشاكل الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات، وحث الدول الأعضاء بمراجعة قوانين الإجراءات الجزائية الوطنية لكي تتلاءم مع التطور في هذا المجال.

- معاهدة بودابست لمكافحة جرائم الإنترنت: تعد أولى المعاهدات المتعلقة بتلك الجرائم وتمت في العاصمة المجرية بودابست في 2001، تبرز التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية، ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الإنترنت والاستخدام السيئ لها، وقد وقعت على تلك المعاهدة 26 دولة أوروبية بالإضافة إلى كندا واليابان، وجنوب أفريقيا، والولايات المتحدة الأمريكية، وتوفر المعاهدة أسس الأمن العام، وتتضمن 48 مادة.²⁹

تعتبر هذه المعاهدة أوروبية المنشأ، غير أنها مفتوحة للدول الأخرى لطلب الانضمام إليها لتعم الفائدة منها على جميع الدول، وقد تناولت تلك المعاهدة الجرائم التي تعتبر من أكثر الجرائم شيوعا على مستوى العالم ضمنتها بالمواد من 2 الى 13 وهي تسع جرائم في ميدان جرائم التقنية: الدخول غير القانوني المتعمد إلى أي نظام كمبيوتر أو جزء منه دون حق، والاعتراض غير القانوني المتعمد، والتدخل المتعمد في المعطيات بتدميرها أو...، والتدخل المتعمد في الأنظمة، إساءة استخدام الأجهزة، التزوير المتعمد، الاحتيال المتعمد، الجرائم المرتبطة بدعارة الأطفال، وأخيرا الجرائم المرتبطة بحق المؤلف.³⁰

قصد التحقيق في جرائم الإنترنت حددت المعاهدة الطرق الواجب اتباعها في ذلك، وتوعدت الدول الموقعة عليها بالعمل من أجل الحد منها، كما حاول المعاهدة إيجاد التوازن بين الاقتراحات التي تقدمت بها أجهزة الشرطة، وما عبرت عنه المنظمات المدافعة عن حقوق الإنسان ومزودي خدمات الإنترنت من قلق، حيث تخشى منظمات حقوق الإنسان من أن تحدّ المعاهدة من حرية الأفراد، وأن تؤدي الرقابة إلى انتهاك حقوق مستخدمي الإنترنت.³¹

- المنظمة الدولية للشرطة الجنائية (الإنتربول): يعد الإنتربول أهم آليات التعاون الشرطي الدولي لمكافحة الجرائم العالمية العابرة للحدود الوطنية بصفة عامة والجريمة المعلوماتية بصفة خاصة، ومهمته الأساسية تفعيل التعاون بين أجهزة الشرطة التابعة للدول الأعضاء في المنظمة بتوحيد إجراءات التسليم، ومن خلال تنسيق العمل الشرطي وتجميع البيانات وتبادل المعلومات لتيسير خدمات التحقيق لضبط وملاحقة المجرمين الهاربين وتسلمهم إلى الدولة التي تطلب تسلمهم، وإنشاء وتطوير كل النظم القادرة على المساهمة بفاعلية في الوقاية والعقاب على جرائم القانون العام.

تقوم بتلك المهمة المكاتب المركزية والوطنية في كل دولة عضو إضافة الى جهاز دائم يتم تعيينه بواسطة السلطات الحكومية الوطنية، وبمساعدة فرق الإنتربول للتحرك إزاء الأحداث التي يمكنها تيسير مجموعة من خدمات التحقيق والتحليل في موقع الحدث بالتنسيق مع الأمانة العامة، ويقوم أيضا بتعميم التحذيرات والتنبيهات المتضمنة المعلومات الاستخباراتية والإحاطات والمشورة التحليلية والفنية عن الأخطار الإجرامية المحتملة،

ويستخدم الإنترنت أدواته الخاصة كمنظومة النشرات الدولية بمختلف أنواعها، والتقني في قواعد البيانات ، وتقديم الخبرات والدورات التدريبية في مجال مكافحة جرائم الإنترنت، وذلك بالاستعانة بمجموعة من الخبراء الدوليين والمختبرات الدولية على الصعيد العالمي، وتيسير تبادل وتحليل وتخزين البيانات الجنائية، حيث تقوم المنظمة بتزويد شرطة الدول الأطراف بكتيبات إرشادية حول جرائم الإنترنت وكيفية التدريب على مكافحتها والتحقيق فيها، وبعد الإجماع المالي المرتبط بالتكنولوجيا المتقدمة من الجرائم التي تركز عليها منظمة الإنترنت.³²

تتمحور استراتيجية الإنترنت الإقليمية لمحاربة الجرائم الالكترونية في إفريقيا حول تبادل البيانات الاستخباراتية في المجال الجنائي، وتنسيق الاجراءات تطبيق القانون ازاء هذه الجرائم، اضافة الى تبادل المعلومات فيما يخص القدرات والإمكانات الإقليمية، ويتولى تنفيذ تلك الاستراتيجية مكتب الإنترنت لعمليات مكافحة الجريمة السيبرية في إفريقيا، وذلك في إطار شراكة مع الجهات المعنية بالأمر في المنطقة، خاصة الاتحاد الأفريقي والأفريبول.³³

يشارك الإنترنت الى جانب معهد الدراسات الأمنية وبالشراكة مع المبادرة العالمية لمكافحة الجريمة المنظمة عبر الوطنية في مشروع ENACT الممول من الاتحاد الأوروبي والذي يسعى إلى الحد من تبعات وتأثيرات الجريمة المنظمة عبر الوطنية في أفريقيا على التنمية وإدارة الشؤون العامة والأمن وسيادة القانون، كما يهدف المشروع أيضا إلى إرساء قاعدة معارف شاملة بشأن دور الجريمة المنظمة في أفريقيا، تستند إلى رصد الأوضاع والتحليل المسند بالأدلة من أجل توفير معلومات تفيد في اتخاذ قرارات استراتيجية، وإلى تعزيز مهارات وقدرات الجهات الرئيسية المعنية في أفريقيا للتصدي على نحو أفضل للتهديدات التي تطرحها الجريمة عبر الوطنية، ويتمثل دور الإنترنت في المشروع في تقديم المساعدة إلى أجهزة الشرطة في أفريقيا من أجل اعتماد استراتيجيات استباقية لدرء التهديدات التي تطرحها الجريمة المنظمة، وتسهيل تبادل المعلومات وتحسين مهارات تلك الأجهزة في مجال التحقيقات،³⁴ من خلال التدريب على التحليل الجنائي، وتوسيع نطاق وصول بعض البلدان إلى منظومة الإنترنت العالمية للاتصالات الشرطية المأمونة، مع تزويد بلدان محددة بالمعدات وبرمجيات التحليل وتدريبها وتوجيهها، وكذلك تعيين محلل استخبار جنائي في كل من مكاتب الإنترنت الإقليمية الأربعة في أفريقيا، واستحداث منصة تحليل مأمونة، وأخيرا الجمع بين رؤساء وحدات التحليل في أفريقيا.³⁵

- آلية الاتحاد الإفريقي للتعاون الشرطي (الأفريبول): يعود الفضل في استحداث الجهاز إلى المبادرة الجزائرية المقدمة بمؤتمر الاقليمي الافريقي الـ 22 للإنترنت والمنعقد في الفترة الممتدة من 10 إلى 12 سبتمبر 2013 بوهان - الجزائر، والذي حضره قادة شرطة الدول الافريقية (41)، الذين تبناوا الطرح الجزائري، وقد تم العمل على تجسيد الفكرة على أرض الواقع ودخلها حيز التطبيق يوم 30 جانفي 2017، فالأفريبول إذا مؤسسة تقنية شرطية دائمة ذات طابع إقليمي تتمتع بالشخصية القانونية الدولية والأهلية القانونية اللازمة للقيام بمهامها المنوطة بها، تهدف إلى التنسيق والتعاون بين الدول الأعضاء في الاتحاد الافريقي بغرض مكافحة الجريمة

المنظمة العابرة للحدود الوطنية بمختلف صورها وأشكالها، وتتخذ من الجزائر العاصمة مقرا لانعقاد دوراتها وإن كان يجوز استثناء عقدها على إقليم أي دولة من الدول الأعضاء بناء على طلب استضافة.³⁶

تتشكل آلية "الأفريبول" من الجمعية العامة التي تضم قادة شرطة الدول الأعضاء، ومن مهامها توفير التوجيه القيادي فيما يخص التعاون الشرطي في إفريقيا، إضافة الى لجنة التوجيه المشكلة من الأعضاء الخمس لهيئة مكتب الجمعية العامة، ومفوض السلم والأمن للإتحاد الإفريقي، ورؤساء المنظمات الإقليمية للتعاون الشرطي، والمدير التنفيذي لآلية الإتحاد الإفريقي للتعاون الشرطي، ويرأس اللجنة رئيس الجمعية العامة، وضمن قواعد الإجراءات يتم النص على وظائف اللجنة وعدد اجتماعاتها وكيفية اجراءها. وأخيرا الأمانة العامة التي يعتبر مديرها المعين من طرف الجمعية العامة بناء على توصية لجنة التوجيه، المسؤول التنفيذي للأفريبول يقدم تقارير منتظمة إلى مفوضية الأمن والسلم بالإتحاد الإفريقي، وتتولى الأمانة مهام أبرزها ضمان الإدارة الفعالة "للأفريبول"، وعقد اجتماعات كل من الجمعية العامة، ولجنة التوجيه، على غرار الاجتماعات الأخرى "للأفريبول" مع الإبقاء طبعا على اتصال مع السلطات الوطنية والدولية، المعنية بتطبيق القانون.³⁷

يسعى الأفريبول حسب المادة الثالثة من النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي الى تحقيق مجموعة من الأهداف تتمثل في:

- العمل على إنشاء أطر ناظمة تضبط التعاون بين مؤسسات شرطة الدول الأعضاء على المستوى الاستراتيجي والعملياتي، قصد الكشف عن الجريمة المنظمة العابرة للحدود الوطنية والتحقيق فيها، واعداد استراتيجية افريقية محكمة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية والإرهاب والجريمة الالكترونية.
 - العمل على تعزيز التنسيق مع الهياكل والمؤسسات والمنظمات التي تعمل على مكافحة الجريمة المنظمة العابرة للحدود الوطنية.
 - تشجيع المساعدة الفنية بين مؤسسات الشرطة بالدول الأعضاء في مجالات هامة كالتدريب وتبادل الخبرات.
 - زيادة التنسيق بين قوات الشرطة لدعم السلم، والعمل مع فريق الدعم الاستراتيجي الشرطي.
 - تطوير قدرات أجهزة الشرطة في الدول الأعضاء عن طريق العمل على استحداث مراكز امتياز إفريقية تعتمد على برامج لتدريب الشرطة تتكيف مع واقع السياق الافريقي.³⁸
- يتضح من ذلك أنّ الآليات التي تعتمد عليها الدول الأفريقية في مكافحة الجرائم الالكترونية متعددة، وتتنوع بين القارية، الدولية والوطنية، وهي من الأهمية بمكان، غير أنّ التقارير والدراسات تقرر في كل مرة بأنّ الظاهرة في تنامي رهيب، وهو الأمر الذي يدلّ على عدم كفاية وقدرة الجهود المبذولة على صيانة الأمن المعلوماتي - عصر سيطرة تكنولوجيا المعلومات والاتصالات- الذي أصبح فقده أكبر مهدد لأمنها بمختلف أبعاده، السياسي العسكري والاقتصادي والاجتماعي.

2. صعوبات محاربة الجرائم الالكترونية في إفريقيا:

يواجه القائمون على عملية مكافحة الجريمة الالكترونية في الدول الافريقية مشكلات وصعوبات جمة، نذكر أبرزها فيما يلي:

- على المستوى الوطني للدول: تتعدد الصعوبات التي تواجه الدور الذي تقوم به الأجهزة الأمنية في مكافحة الجرائم الإلكترونية على المستوى الوطني، وأهم هذه الصعوبات تتمثل في:
- الافتقار إلى السياسات الضرورية لمكافحة الجريمة الالكترونية: الواقع أن تزايد هذا النوع من الجرائم في البلدان الافريقية يعزى الى عامل جد هام يتمثل في افتقارها لسياسات وتشريعات واضحة تبين كيفية التعامل مع تلك الجرائم، وحتى ما تتوفر عليه من أطر قانونية تعد غير كافية، وغير فعالة في ظل تفاقم الاجرام السيبراني بها، والتردي الرهيب للوضع.³⁹ ورغم أن الاتحاد الأفريقي قد اعتمد سنة 2014 اتفاقية بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، إلا أنه لم يوقعها بحلول جانفي 2020، إلا 14 بلدا من أصل البلدان الـ 55 الأعضاء في الاتحاد، وحسب ما أفاد به تقرير الإنتربول فإن هذا الأمر يدل على أن معظم الدول الأفريقية لا تزال تعتبر الأمن السيبراني أمرا ثانويا، وهو ما يزيد من تفاقم المشكلة وتعمدها بشكل أكبر.⁴⁰
- عدم كفاية القوانين الحالية: فالتطور المتلاحق في مجال تقنية المعلومات والاتصالات يقابله استغلال الجناة لهذه التقنية المتطورة بابتكار أساليب جديدة لارتكاب الجرائم الإلكترونية، ولذلك يتطلب الأمر مواكبة القوانين لهذه التطورات واستيعابها.
- إحصاء الكثير من الجهات عن التبليغ عن تلك الجرائم بحجة عدم الإساءة لطبيعة عمل المنشأة، وعدم بيان عجزها عن تحقيق الأمان الكافي للمعلومات، وبالتالي لأصول الأموال التي تتعامل معها، وقد يكون لذلك مردود سيء لدى العملاء الذين ربما يلجأ الكثير منهم لسحب أمواله ووقف تعاملاته مع المنشأة.
- سهولة إخفاء معالم الجريمة: وصعوبة معرفة مصدر مرتكب الفعل، بحيث إذا تم ارتكاب الفعل وظهرت نتيجته بعد فترة زمنية، مثل قيام شخص ما بزرع برنامج فيروسي يكتشف بعد تحقق آثاره التدميرية والسالبة.
- عدم وجود دليل مادي واضح: والدليل المادي الذي يتوافر قد يكون في الغالب أوراق متحصلة من الطابعة من خلال الجهاز، والدليل هنا يكون الأوراق المتحصلة وليس ما يحويه الجهاز في حد ذاته.
- وجود كم كبير من المعلومات يتعين فحصها: فالبحث عن معلومات تفيد في كشف أدلة جريمة معينة يتطلب البحث في كم كبير من الملفات والبرامج المخزنة، والتي قد يكون لها ارتباط بمعلومات خاصة بارتكاب الجريمة.

- الصعوبات على المستوى القاري: وتتمثل في:

- اختلاف مفاهيم الجريمة لاختلاف التقاليد القانونية وفلسفة النظم القانونية.
- عدم التناسق في القوانين الإجرائية فيما يتعلق بالتحري والتحقيق في الجرائم الإلكترونية.
- عدم وجود الخبرة الكافية لدى الأجهزة الأمنية والعادلة لتمحيص عناصر الجريمة.

• عدم كفاية الاتفاقيات الدولية والثنائية في مجال تسليم المجرمين.⁴¹

يتضح من كل ذلك أنّ عملية مكافحة الجرائم الالكترونية في إفريقيا تواجهها مشكلات في غاية الصعوبة، وهي لا تقتصر على المستوى القاري بل الأكثر من ذلك على المستوى الوطني لكل دولة، مما يعرقل محاربة هذه الجرائم، دون أن ننسى انكشاف هذه القارة ودولها أمام العالم المتقدم المهيم مما يزيد الأمر صعوبة.

رابعا: تأثيرات الجرائم الالكترونية على الأمن في إفريقيا وكيفية التعامل معها

أثبتت الواقع أن الجرائم الالكترونية أصبحت إحدى المهددات الخطرة لأمن المجتمعات والدول، كونها تؤثر على كل المجالات في ظل ادخال العمل بالرقمنة، الأمر الذي يحتم اليوم على الدول الافريقية العمل وطنيا واقليميا ودوليا من أجل التعاون، وتنسيق الجهود الرامية لمحاصرة الظاهرة والحد من استشرائها بها.

1. تأثير الجرائم الالكترونية على الأمن في إفريقيا:

تتضح خطورة تفاقم الجرائم الالكترونية بدول القارة الأفريقية من خلال تلك الخسائر الكبيرة التي الحقها بشتى مجالات الحياة السياسية والاقتصادية والاجتماعية والعسكرية بها، وذلك ما نسعى لإبرازه.⁴²

1.1. تأثير الجرائم الالكترونية على أمن الأفراد والأمن المجتمعي:

ما أكثر من يخترقون حياة الناس، بداعي الفضول، والغيرة، والإيذاء وقد زاد المتطفلون، والمجرمون، وزادت نسبة تعرّض الشخص للابتزاز، والملاحقة، والتهديد،⁴³ وسرقة الهوية الشخصية، وسرقة بطاقة الائتمان الخاصة به، اضافة الى الاحتيال، على الحساب المصرفي للمجني عليه، ونقل ملكية أسهمه، وزيادة الفواتير من خلال تحويل فواتير المجرم للضحية،⁴⁴ وكل ذلك طبعا له وقع كبير على أمن الفرد الشخصي والمالي والاجتماعي وحتى العلمي ... لما يسببه له من خسائر جمة كالمساس بالعلاقات الأسرية وتشكيل الخلافات بين أفراد الأسرة، ووقوع التفكك الأسري، وذلك بسبب الكثير من أنواع الجرائم المعلوماتية كالتشهير ببعض الأفراد ونشر الأخبار الكاذبة عنهم.⁴⁵

تشهد قضايا الإجرام الالكتروني في إفريقيا تزايدا متواصلا، كلف بلدانها خسائر جمة بلغت مثلا في بلدان الغرب الافريقي فقط حوالي 6.5 ملايين دولار بين عامي 2017 و 2018 فقط، وهي جرائم تستغل استخدام وسائل التواصل الاجتماعي لتسهيل مثلا جرائم تهريب المهاجرين والاتجار بالبشر، وخير مثال عن ذلك عملية Sarraounia التي حدثت بدعم من الإنترنت والتي أسفرت عن إنقاذ 232 ضحية من ضحايا الاتجار بالبشر في النيجر، منهم 46 قاصرا، كما كشفت عن أنّ 180 ضحية هم من الذكور تم تجنّدهم عن طريق رسائل نصية إلكترونية تعدّهم بتوفير مناصب شغل لهم، اضافة الى استخدامها (أي المجموعات الاجرامية) للانترنت لاستمالة الأطفال القصر والاعتداء عليهم جنسيا أو بيع مواد الاستغلال الجنسي لهم، وبما أنّ القارة الافريقية تعتبر مركز عبور عالمي، فإنّه يتزايد بها استخدام الشبكة الدولية الانترنت للاتجار بالمخدرات والمستحضرات الصيدلانية والمركبات الآلية المسروقة و... غيرها من السلع غير المشروعة التي تباع وتشتري عبر الإنترنت.⁴⁶

2.1. أثر الجريمة الالكترونية على الأمن الاقتصادي:

تعد الجريمة الالكترونية أحد أبرز التحديات الأمنية التي تواجهها الشركات والحكومات على المستوى العالمي وباتت تشكل خطراً حقيقياً يواجه الجميع وخصوصاً من الناحية الاقتصادية، حيث تخلف وراءها خسائر كبرى بمعدل وسطي يتجاوز النصف مليون دولار أمريكي للشركات الكبرى جراء كل هجمة الكترونية أو عملية اختراق تتعرض لها الشركة. ومن الجرائم ذات الأثر المادي والمالي والاقتصادي على الشركات: الاطلاع على معلومات سرية لصفقة أو أمور تسويقية والاستفادة منها، والعبث بالمخزون المعلوماتي للشركة بالحذف أو التعديل أو التعطيل، أو تحويل الحسابات المصرفية الخاصة بها، والتغيير في المبيعات، وعمليات الاحتيال، والتهديد والابتزاز.⁴⁷

إنّ الخسائر الاقتصادية الناجمة عن تلك الجرائم المعلوماتية متنوعة وقد تكون هذه الخسائر مباشرة أو غير مباشرة، أي يكون ضررها اقتصادي مباشر يرتبط بقيمة التجهيزات والبرمجيات موضوع الجريمة، وهو أقلها من حيث الأثر، وقد يرتبط بالأثر الاقتصادي الناجم عن توقف هذه المنظومات عن العمل مثلاً: اختراق وتعطيل بمنظومة شركة الطيران رغم عدم وجود أثر مالي مباشر، إلا أنّ توقف المنظومة عن العمل تؤدي إلى خسائر تقدر بالآلاف الدولارات، أو تعطيل منظومة سوق الأوراق المالية لمدة دقائق قد ينجم عنه خسائر تقدر بعشرات الدولارات أيضاً، أو سرقة الأموال الالكترونية واستخدام الشبكة للاستيلاء على أموال الغير.⁴⁸

أفصح "تقرير الأمن السيبراني في أفريقيا لعام 2017" أنّ برقيّة المربع الخسائر الناتجة عن الجرائم السيبرانية في القارة الأفريقية قد مس البنوك والخدمات المالية فينارييسلا تامجهلا نم تررضت اهنا أي نعي ام، اهبت لااصنلاو تلامعلاو تراجتلاو تاموكلما م تررضت امم رثكأ وفي تقرير رخا صدر عن "معهد بروكينغز مئس" 2018، أفاد أيضاً أنّه ومع تزايد تهديد الجرائم السيبرانية للشركات في جميع أنحاء العالم، فإنّ الخطر بالنسبة للشركات الأفريقية أكبر من ذلك. وبالرغم من أنّ إفريقيا محدودة نسبياً فيما يخص بنيتها التحتية للاتصالات، إلا أنّ انخفاض مستوى الأمن السيبراني اهبت جعلها هدفا رئيسياً لمجرمي الإنترنت.⁴⁹

3.1. تأثير الجريمة الالكترونية على الأمن السياسي-العسكري:

أمام تبني دول القارة الأفريقية على غرار دول العالم مفاهيم من قبيل الحكومة الالكترونية، والادارة الالكترونية، والمدن الذكية تكون قد رهنت سيادتها الوطنية، لأنها بسبب ذلك أصبحت منكشفة أمام الأطراف الخارجية، خاصة وأنّ شبكة الانترنت الدولية سهلت العمل على الاختراق، وضرب وحدة وأمن الدول من الداخل في وقت قصير، باستخدام الدعاية والاشاعة، وكذا تحريض الطوائف والاقليات المعارضة على خلق الفوضى والإرهاب لضرب استقرار البلد وأمنه الوطني، وهو ما أصبح يعرف بحرب العقول.

تستهدف الجريمة الالكترونية بالأساس البنية التحتية للدول، سواء كانت بنية مدنية أو عسكرية، فتشل أنظمة التشغيل وتؤثر على تدفق المعلومات، فينشأ عن ذلك تعطيل عمل العديد من المرافق الحيوية التي أصبحت في حالة فوضى، ويطل كذلك هذا النوع من الجرائم الأنظمة العسكرية بتعطيلها أو إتلافها، أو السيطرة

على نظم القيادة والطائرات من دون طيار، أو السيطرة على الغواصات النووية في أعماق البحار، وحتى الأقمار الصناعية العسكرية في الفضاء الخارجي عن طريق إخراجها عن سيطرة الدولة التابعة لها، يضاف إلى تلك الجرائم سرقة المعلومات والبيانات العسكرية أو تزيفها أو تدميرها إلكترونياً مما يفقد الدولة أمنها العسكري والسياسي.⁵⁰ وهو حال جلّ الدول الأفريقية الضعيفة عسكرياً وسياسياً، وهي نتيجة ذلك سهولة الاختراق والتجسس الإلكتروني لبياناتها ومعلوماتها العسكرية والسياسية وباقي المجالات الأخرى.

4.1. تأثير الجريمة الالكترونية على الأمن المعلوماتي:

يعتبر هذا الأخير أحد أبرز أبعاد الأمن الهامة في الوقت الحالي كونه يتعلق بأمن وسلامة وسرية وصيانة وحماية المعلومة سواء تعلق الأمر بالجانب الإداري والمعاملات التي تتبادل فيها المعلومة أو الجانب التقني والفني، أي الوسائل المستخدمة في الأمن والحفظ والصيانة والتخزين والبرمجيات، كما لا نستثني من ذلك مراكز تواجد الحاسبات، فالأمن المعلوماتي يقوم على مجموعة الوسائل الرامية إلى حماية البرامج والمعلومات الحاسوبية والتطبيقات والأجهزة الالكترونية من أي هجوم إلكتروني .

العمل على تحقيق الأمن المعلوماتي في القارة السمراء اتخذ مكانه في جدول الأعمال الإفريقي سواء للمنظمات تحت- الإقليمية أو الإقليمية منها منظمة الكواس التي اتخذت قرار في 19 أوت 2011 المتعلق بمكافحة الجرائم الالكترونية، كما اتخذ الاتحاد الإفريقي من جهته القرار رقم 473 سنة 2021 المتعلق بحقوق الإنسان والشعوب فيما يخص الذكاء الاصطناعي والروبوته وباقي التكنولوجيات الحديثة، داعياً المنظمات تحت- إقليمية الإفريقية إلى ضرورة اتخاذ كافة الأطر التشريعية اللازمة لتأطير التكنولوجيات الحديثة في إفريقيا، وذكر الاتحاد بتأثير بعض الجرائم الالكترونية كالتضليل ونشر المعلومات الخاطئة، والقيام بحملات مدعومة على الشعوب الإفريقية وحقوقها، كما دعا في نهاية القرار الدول إلى تعميق البحوث في مجال الذكاء الاصطناعي والتكنولوجيات الحديثة، وتأثيرها على إفريقيا وحقوق الشعوب وحريةتها. وبعبارة إنجيلا ماركل " تظل الهجمات الالكترونية أو المعلوماتية أخطر من الحرب الحقيقية لذلك بالرغم من الأوضاع المتردية في إفريقيا اقتصادياً وسياسياً لا بد من التركيز على دعم الأمن الرقمي فيها وتحقيق السيادة الرقمية ولو نسبياً خاصة بأنّ التكنولوجيات الحديثة والذكاء الاصطناعي أصبح يوظف لغايات سياسية كالتأثير في الرأي العام من خلال دعم المرشحين السياسيين وضرب آخرين وتأجيج الأزمات وتهدة أخرى".⁵¹

2. كفايات الحد من الجرائم الالكترونية في إفريقيا:

من أجل محاصرة هذا النوع الخطر من الجرائم الماسة بأمن المعلوماتي بالدرجة الأولى ثم بالأمن عامة في هذه القارة، نرى أنّه بالرغم من صعوبة أمر محاربة الجرائم المعلوماتية، لكن الواقع يتطلب من بلدان الإفريقية القيام بالآتي:

- وضع إطار متين للأمن السيبراني: في الدول الأفريقية من خلال توفير بنية تحتية رقمية قوية، خاصة وأنها تسعى الى رقمنة كافة مجالات الحياة خاصة الحكومية منها والمصرفية والعسكرية والتي تعد قطاعات حساسة ترتبط مباشرة بسيادة و أمن الدول.⁵²
- التأمين بالوسائل التقنية المتمثلة في تأمين الحاسبات الشخصية، وتأمين وحماية شبكة الربط بالإنترنت، وتأمين المعلومات المتداولة، والحماية من التهديدات والاختراقات.
- التأمين بوضع السياسة الأمنية التي تمس أمن الأفراد، والطبيعة، وتحديد الهياكل التنظيمية المساندة، وتصنيف المصادر العملياتية والبيانات والمعلومات، وتحديد مستويات الدخول وأحقيات التعامل، وتأمين عمليات التشغيل، وتأمين التطبيقات والشبكات والخدمات (كالبريد الإلكتروني ونقل الملفات والتجارة الإلكترونية... وغيرها)، وتأمين تجميع البيانات والتحليل والتصميم والبرمجة والتشغيل والصيانة والدعم الفني، وكذا إدارة وتحليل المخاطر وتحديد خطط استمرارية العمل، والالتزام بتشريع تأمين الحماية للبيانات على المستوى القومي والقاري.⁵³
- رفع كفاءة وفاعلية أساليب ووسائل مواجهة الجريمة الإلكترونية دوليا وفي دول القارة السمراء من حيث التقنيات المتطورة والكفاءات البشرية المؤهلة.
- التأكيد على المزيد من التعاون الإقليمي الدولي الفعال لمواجهة الجريمة الإلكترونية في افريقيا.⁵⁴
- إصدار التشريعات المواكبة لتطورات الجريمة الإلكترونية، وانسجام التشريعات الوطنية مع الاتفاقيات والقواعد الدولية، والقوانين المقارنة ذات الصلة، لتمكين أجهزة العدالة الجنائية من أداء دورها على النطاق الوطني والإقليمي والدولي بالصورة التي تسهم بالمكافحة الفعالة للجريمة الإلكترونية افريقيا.
- رفع كفاءة الأجهزة التقنية المختصة برصد التهديدات والمخاطر والتبليغ بالإنذار المبكر، وتزويدها بأحدث المعدات.
- تدريب وتأهيل الفنيين والمهندسين العاملين في مجال الأدلة الرقمية، وترشيد وتطوير أدائهم.
- تدريب وتأهيل المختصين بأجهزة العدالة الجنائية على كيفية التعامل مع الأدلة الرقمية.
- إتباع كافة وسائل التوعية الأمنية للحد من مخاطر الجريمة الإلكترونية.⁵⁵
- تحتاج إفريقيا إلى مؤسسات قوية لتكنولوجيا المعلومات والحاسوب الشخصي لتدريب خبراء الأمن السيبراني من ذوي الخبرة القوية في إدارة إعلانات النظام، والتدقيق الأمني، والتحقيق الجنائي، وأمن المعلومات، وتطوير البرمجيات للتعامل مع التحديات المستقبلية للجرائم الإلكترونية.⁵⁶

الخاتمة :

يتضح مما تقدم أنّ القارة الأفريقية ليست في معزل عن ما تشهده الساحة الدولية في الوقت المعاصر من انتشار كبير للجرائم الالكترونية الماسة بأمن المعلومات، لكنها تعرف تفاقمًا رهيبًا لها، ينبأ بتأزم الوضع أكثر في حال عدم تدارك الأمر.

النتائج: بناء على ما تضمنته هذه الدراسة نستخلص الآتي:

- وجود تعاون بين أجهزة الشرطة في مختلف الدول وأبرز هذا التعاون على المستوى الدولي إنشاء المنظمة الدولية للشرطة الجنائية (الإنترپول) لمكافحة الجرائم العابرة للحدود، ومن بينها الجرائم السيبرانية وعلى المستوى الافريقي انشاء الأفريبول.
 - سعى المجتمع الدولي إلى إبرام اتفاقيات دولية لمكافحة الهجوم السيبراني أبرزها معاهدة بودابست لمكافحة جرائم الإنترنت.
 - وجود صعوبات ومعوقات أمام التعاون الافريقي افريقي، والافريقي الدولي في مجال مكافحة الجريمة الالكترونية تحد من فاعلية إنفاذ التعاون.
 - أن آلية تنفيذ المساعدات القضائية الدولية يتم عن طريق دبلوماسي يتميز بالبطء والتعقيد، وذلك يتعارض مع طبيعة الجريمة السيبرانية والإنترنت التي تتسم بالسرعة.
 - تحقيق الأمن في افريقيا لم يعد يستدعي التركيز على تحقيق الأمن العسكري والاقتصادي فحسب، بل الى جانب ذلك يتوقف على تحقيق الأمن المعلوماتي نتيجة التهديدات السيبرانية وكثرة الجرائم الالكترونية التي أصبحت تطال كل تلك المجالات مما ساهم في إضعافها أكثر وكل ذلك أدخل بالأمن بها.
 - تبذل الدول الأفريقية مجهودات عديدة ان على المستوى الوطني أو القاري لمحاربة ظاهرة الجرائم الالكترونية للحد منها.
 - تبقى الآليات الأفريقية في مواجهة الجريمة الالكترونية غير كافية، وما هو موجود منها يحتاج للتفعيل وإعادة النظر بما يتماشى وطبيعة جرائم الانترنت التي تتميز بالسرعة.
- نقدم في الاخير مقترحات نأمل أن تسهم في الحد من الجرائم الالكترونية في افريقيا :
- ضرورة العمل على ايجاد أنظمة حماية قوية للمعلومات مع تحديثها وتجديدها باستمرار من حين لآخر بما يتماشى والمستجدات.
 - فتح المجال واسعا أمام تنظيمات المجتمع المدني حتى تتمكن من نشر الثقافة الرقمية وتوعية المجتمعات الافريقية بمخاطر الجرائم الالكترونية.
 - على الجامعات ومراكز البحث بدول القارة الاهتمام أكثر بمثل هكذا موضوعات، والعمل على ايجاد تخصصات تعنى بالمعلوماتية والجرائم الماسة بها، قصد تكوين مختصين في المجال، المجتمع في حاجة ماسة لهم.

الهوامش:

* للجريمة الإلكترونية مسميات عدة منه: جرائم الحاسوب والإنترنت، جرائم التقنية العالية، الجريمة الإلكترونية، الجريمة السيبرية، جرائم أصحاب الباقات البيضاء.

- ¹ بلفكرات رشيد، بنزعمة عبد القادر، الجريمة الإلكترونية كتهديد للأمن الوطني الجزائري، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة، (المجلد الرابع)، العدد الأول، مارس 2019، ص 512.
- ² رابحي لخضر، بن بعلاش خاليدة، "معالجة الجرائم المعلوماتية في ظل التعاون الدولي والاستجابة الوطنية"، مداخلة في المنتدى الوطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة، المنعقد بجامعة بسكرة يومي 16 و 17 نوفمبر 2015، ص 2.
- ³ محروس نصار غايب، "الجريمة المعلوماتية"، المعهد التقني الأنبار، تاريخ النشر 3 / 5 / 2011، ص 4.
- ⁴ بن صغير عبد المؤمن، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن"، ورقة: المنتدى الوطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة، المنعقد بجامعة بسكرة يومي 16 و 17 نوفمبر 2015، ص 6.
- ⁵ مرعي اسراء جبريل رشاد، "الجرائم الإلكترونية الأهداف - الأسباب - طرق الجريمة ومعالجتها"، المركز الديمقراطي العربي، (9 أغسطس 2016)، شوه في 02 / 08 / 2022، <https://democraticac.de/?p=35426>
- ⁶ بلفكرات رشيد، بنزعمة عبد القادر، مرجع سبق ذكره، ص 513.
- ⁷ regarde :UNODC , *Étude détaillée sur la Cybercriminalité*, Ébauche ,Février 2013, p 28.
- ⁸ Chawki Mohamed and others, *Cybercrime, Digital Forensics and Jurisdiction*, Studies in Computational Intelligence Volume593, Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland,2015, p20.
- ⁹ بلفكرات رشيد، بنزعمة عبد القادر، مرجع سبق ذكره ، ص 514.
- ¹⁰ مرعي اسراء جبريل رشاد ، مرجع سبق ذكره. <https://democraticac.de/?p=35426,op.Cit>
- ¹¹ بلفكرات رشيد، بنزعمة عبد القادر، مرجع سبق ذكره ، ص 514
- ¹² المرجع نفسه.
- ¹³ مرعي اسراء جبريل رشاد ، مرجع سبق ذكره..op.Cit. <https://democraticac.de/?p=35426>
- ¹⁴ حيمر فتيحة ، "السياسة العامة الأمنية في الجزائر: التحدي والاستجابة"، مجلة فكر ومجتمع، العدد 32، أوت 2016، ص152-155.
- ¹⁵ المرجع نفسه ، ص 154-155.
- ¹⁶ الانتربول، تقرير للانتربول يكشف أبرز التهديدات السيبرية في أفريقيا، (21 أكتوبر 2021)، <https://www.interpol.int/ar/1/1/2021/47>
- ¹⁷ (Africa Defense Forum ADF)، "احترسوا من اتجاهات الأمن السيبراني هذه خلال 2022"، آخر تحديث 5 يناير 2022. <https://adf-magazine.com/ar/2022/01>
- ¹⁸ الانتربول، تقرير للانتربول يحذر من أن الجريمة الإلكترونية في أفريقيا تشكل تهديدا أشد خطرا من أي وقت مضى، (14 أغسطس 2020)، <https://www.interpol.int/ar/1/1/2020/36>
- ¹⁹ العربية، "جرائم الإنترنت، تهديد متزايد في أفريقيا"، (الجمعة 14 كانون الثاني يناير 2022)، الساعة 9:16 صباحاً <https://lejournaldefafricque.com>
- ²⁰ ** في غرب إفريقيا، على سبيل المثال، ظهرت مجموعتان متميزتان من مجرمي الإنترنت، وهما «Yahoo Boys» و «Level Cybercriminals -Next» وهما يتميزان ببنيتهما ونوع الجرائم التي يرتكبانها. في حين أن Yahoo Boys تعمل في الغالب على عمليات خداع تقليدية مسبقة الرسوم، فإن Level Cybercriminals - Next ينخرطون في هجمات أكثر تعقيدا ضد الشركات وينطوى على عمليات خداع ضريبية، لها علاقات في إفريقيا وخارج القارة.
- ²⁰ حدادة رباب، الجرائم الإلكترونية والأمن الرقمي في إفريقيا، (مراجعة: الدكتوراة قعلول بدر)، تقرير قسم البحوث والدراسات الافريقية بالمركز الدولي للدراسات الاستراتيجية الامنية والعسكرية، (19 مايو 2021)، شوه في: 2022/06/28، <https://strategianews.net>

- ²¹ غوكهان قاقاق، "46 بالمئة من سكان إفريقيا يستخدمون الإنترنت بحسب موقع". "Internet World Stats"، 01.03.2021. <https://www.aa.com.tr/ar>
- ²² رامي زين الدين، "إفريقيا.. مئات الملايين ما زالوا يعيشون بلا إنترنت"، دبي، (21 مايو 2020)، 17:32. آخر تحديث 18 يناير 2021، 16:34. <https://asharq.com/ar/5q3kCEKUgPgXjCX0mV16dWarticle>.
- ²³ حدادة رباب، مرجع سبق ذكره، <https://strategianews.net,op,cit>.
- ²⁴ Chawki Mohamed and others, op, Cit, p10.
- ²⁵ E Kritzing1 and SH von Solm, A Framework for Cyber Security in Africa, IBIMA Publishing Journal of Information Assurance & Cybersecurity, Published 30 December 2012, p2. <https://strategianews.net,op,cit>.
- ²⁶ حدادة رباب، مرجع سبق ذكره، <https://strategianews.net,op,cit>.
- ²⁷ المرجع نفسه.
- ²⁸ مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى سلطنة عمان، الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون الخليجي العربية، 2016، ص 11. 12.
- ²⁹ الزهراني شيخه حسين، "التعاون الدولي في مواجهة الهجوم السيبراني"، مجلة جامعة الشارقة للعلوم القانونية، (المجلد 17)، العدد 1، يونيو 2020 م، ص 751. 755.
- ³⁰ للمزيد أنظر: مركز هردو لدعم التعبير الرقمي، التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات، القاهرة 2018، ص 23. 26.
- ³¹ الزهراني شيخه حسين، مرجع سبق ذكره، ص 751. 755.
- ³² المرجع نفسه، ص 745.
- ³³ الانتربول، "تقرير للانتربول يكشف أبرز التهديدات السيبرية في أفريقيا"، مرجع سبق ذكره. <https://www.interpol.int/ar/1/1/2021/47,op,Cit>.
- ³⁴ الانتربول، "تقرير للانتربول يحذر من أن الجريمة الإلكترونية في أفريقيا تشكل تهديداً أشد خطراً من أي وقت مضى"، 14 أغسطس، 2020. <https://www.interpol.int/ar/1/1/2020/36>.
- ³⁵ الانتربول، مشروع ENACT، "ENACT"، <https://www.interpol.int/ar/2/7/ENACT>.
- ³⁶ خالدي خديجة، "آلية الاتحاد الإفريقي للتعاون الشرطي "الأفريبول"، مجلة العلوم الاجتماعية والانسانية، المجلد 11، العدد 1، الصفحات 65 - 79، ص 67 - 69.
- ³⁷ النظام الأساسي المنظم لآلية (الأفريبول).
- ³⁸ خالدي خديجة، مرجع سبق ذكره، ص 70.
- ³⁹ E Kritzing1 and SH von Solm, op, Cit, p2.
- ⁴⁰ الانتربول، "تقرير للانتربول يحذر من أن الجريمة الإلكترونية في أفريقيا تشكل تهديداً أشد خطراً من أي وقت مضى"، مرجع سبق ذكره. <https://www.interpol.int/ar/1/1/2020/36,op,Cit>.
- ⁴¹ مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى سلطنة عمان، مرجع سبق ذكره، ص 42.
- ⁴² حسنى عز الدين زينب، "الجريمة المنظمة في القارة السمراء"، (الإثنين 16 يولييه 2018)، 9:10. <https://www.shorouknews.com>
- ⁴³ مركز هردو لدعم التعبير الرقمي، مرجع سبق ذكره، ص 5.
- ⁴⁴ regarde: UNODC, Étude détaillée sur la Cybercriminalité, Ébauche, Février 2013, p 28.

⁴⁵ الربيعة صالح بن علي بن عبد الرحمن ، الجريمة المعلوماتية مخاطرها وعقوباتها، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية، د.س.ن، ص12.

⁴⁶ الانترنتبول، "تقرير للانترنتبول يحذر من أن الجريمة الإلكترونية في أفريقيا تشكل تهديدا أشد خطرا من أي وقت مضى"، مرجع سابق. <https://www.interpol.int/ar/1/1/2020/36,op,Cit>

⁴⁷ فويقح حورية، الأبعاد الاقتصادية للجريمة الإلكترونية، مجلة الاصلاحات الاقتصادية والاندماج في الاقتصاد العالمي، (المجلد رقم14)، العدد 1، 2020/02/05، ص 240 - 250.

⁴⁸ المرجع نفسه.

⁴⁹ ADF ،"أفريقيا تتصدى للجريمة السيبرانية"، آخر تحديث 21 أغسطس 2019 . <https://adf-magazine.com/ar/2019/06>

⁵⁰ كلاع شريفة، "الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني"، مجلة الحقوق والعلوم الانسانية، (المجلد 15)، العدد 01، 2022 / 04 / 27، الصفحات 292 - 314، ص 304 .305.

⁵¹ حدادة رباب ، مرجع سبق ذكره . <https://strategianews.net,op,cit>

⁵² الانترنتبول، "تقرير للانترنتبول يكشف أبرز التهديدات السيبرية في أفريقيا"، مرجع سبق ذكره ، <https://www.interpol.int/ar/1/1/2021/47,op,Cit>

⁵³ مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى سلطنة عمان، مرجع سبق ذكره، ص 43 -44.

⁵⁴ المرجع نفسه، ص 15.

⁵⁵ المرجع نفسه، ص 41.

⁵⁶ henry Osborn Quarshie, Alexander Martin- Odoom, *Fighting Cybercrime in Africa*, Computer Science and Engineering, 2012,p 100.