الجهود العربية والإفريقية لمواجهة الجرائم الإلكترونية في الفترة 2010 – 2023

Arab and African efforts to confront cybercrime in the period 2010-2023

د. عماد حسين محمد الفريحات: محامي وباحث قانوني، المملكة الأردنية الهاشمية.

Dr. Emad Hussein Muhammad Alfreihat: Lowyer and Legal Researcher, Hashemite Kingdom of Jordan.

Email: emadalfreihat@gmail.com

DOI: https://doi.org/10.56989/benkj.v3i5.323

الملخص:

هدفت الدراسة إلى التعرف على الجهود العربية والإفريقية المتعلقة بمواجهة الجرائم الإلكترونية، خاصة في ظل الصعوبة التي تُواجهها إجراءات التحقيق في هذا النوع من الجرائم والمتمثلة في إخفاء الجريمة وسهولة وسرعة محو أو تدمير أدلة ومعالم الجريمة والضخامة البالغة لكمية البيانات المراد فحصها على الشبكة، ولتحقيق أهداف الدراسة فقد اعتمد الباحث على البحث المنهج الوصفي، وذلك من خلال تحليل نصوص الاتفاقيات الخاصة بالجريمة الإلكترونية والأحكام القضائية إن وجدت، وتوصلت الدراسة إلى مجموعة من النتائج أبرزها: أنّ الدول العربية دأبت إلى تكثيف جهودها من أجل الحد من الجرائم الإلكترونية لما ينطوي على هذه الجرائم من مخاطر جمّة تلحق بالمؤسسات والأفراد خسائر باهظة، باعتبارها تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة (البيانات والمعلومات والبرامج في كل أنواعها)، وأوصلت الدراسة بمجموعة من التوصيات أبرزها: ضرورة توحيد الجهود الدولية والإقليمية وعلى مستوى دول العالم لأن الجريمة الإلكترونية ليس لها حدود بل هي تطول كل دول العالم، بغض النظر عن بعدها وقربها حين ارتكابها، وضرورة تأهيل وتنمية رجال الضبطية القضائية على الأساليب التقنية والحديثة المستخدمة في هذه الجرائم، وتدريبهم على التدابير الواجب اتخاذها في هذا المجال، للإسراع في الكشف عن الجريمة وتعقبها، من أجل عدم ضياع الدليل إعطاء الضبطية القضائية المزيد من الوسائل التقنية المتطورة.

الكلمات المفتاحية: الجرائم الإلكترونية، جرائم تقنية المعلومات، تقنية المعلومات، تكنولوجيا المعلومات، الأمن السيبراني، الضبطية القضائية.

Abstract:

The study aimed to identify the Arab and African efforts related to confronting cybercrime, especially in light of the difficulty faced by investigation procedures in this type of crime represented in concealing the crime and the ease and speed of erasing or destroying evidence and features of the crime and the extremely large amount of data to be examined on the network, and to achieve the objectives of the study The researcher relied on the descriptive research method, by analyzing the texts of the conventions on cybercrime and judicial rulings, if any, and the study reached a set of results, most notably: that the Arab countries have intensified their efforts to reduce cybercrime due to the dangers that these crimes entail.

Exorbitant losses are inflicted on institutions and individuals, as it aims to attack data with its broad technical implications (data, information, and programs of all kinds). The countries of the world, regardless of their distance and proximity when they were committed, and the necessity of qualifying and developing the judicial police officers on the technical and modern methods used in these crimes, and training them on the measures that must be taken in this field, in order to expedite the detection and tracking of the crime, in order not to lose the evidence. More advanced technology.

Keywords: cybercrime, information technology crimes, information technology, information technology, cyber security, judicial police.

المقدّمة:

إن أهم ما يُميز العصر الحالي عن غيره من العصور هو ما نشهده اليوم من تطور مثير في المجالات التكنولوجية، الأمر الذي انعكس على مجمل مجالات الحياة، بحيث نستطيع القول بثقة بأنه لم يُعد هناك شأن يتصل بالحياة الانسانية إلّا ناله نصيب من هذا التطور التكنولوجي المثير الذي أحدث ثورة أدخلت البشرية في عصر جديد، وعلى الرغم من الايجابيات العديدة التي أحدثتها تقنية الانترنت في تسهيل نقل وتبادل المعلومات، إلّا أنْ هناك خشية متزايدة من تنامي الخروق والسلبيات والأعراض الجانبية لهذه الشبكة واستغلالها من قبل بعض الشركات والهيئات والعصابات والأفراد لارتكاب وتعميم أعمال وأفعال تتقاطع مع القوانين ومع الاعراف والأخلاق والآداب.

هذا ولم يعد الأمن مفهوماً ضيقاً على ضبط الجرائم التقليدية وتعقب مرتكبيها بالنسبة للدول العربية ودول الإتحاد الإفريقي، بل أمتد مفهومه إلى أوسع من ذلك بحيث يرقى إلى مستوى استيعاب المتطلبات الاقتصادية والسياسية والاجتماعية في كل المجالات، ووضع الاستراتيجيات الأمنية التي تهدف إلى حمايتها واستقرائها قبل أن تعبث بها يد العابثين، وتعد جهود الدول العربية وجهود دول الإتحاد الإفريقي هي الأساس الذي يرتكز عليه التعاون في مجال مكافحة الجرائم الإلكترونية، وقد تم عقد العديد من الاتفاقيات تحت مظلة منظمة جامعة الدول العربية، ومظلة الإتحاد الإفريقي تعمل على التعاون في مجال مكافحة الجرائم الإلكترونية.

مشكلة البحث:

تتمثل مشكلة البحث في مدى الصعوبة التي تُواجهها إجراءات التحقيق في هذا النوع من الجرائم والمتمثلة في اخفاء الجريمة وسهولة وسرعة محو أو تدمير أدلة ومعالم الجريمة والضخامة البالغة لكمية البيانات المراد فحصها على الشبكة، وتبرز كذلك صعوبات في مسائل جمع الأدلة من المعاينة والتفتيش والضبط وغيرها من الاجراءات، فضلاً عن الطابع العالمي الذي تمتاز به هذه الجرائم لكونها من الجرائم التي تتجاوز عنصري الزمان والمكان، وبذلك عقد الاتفاقيات الدولية ومنها الاتفاقيات الإقليمية للحد من هذه الجريمة.

والسؤال الرئيسي في مشكلة البحث هو هل استطاعت الجهود الدولية من القدرة على التأثير ومكافحة الجرائم الإلكترونية من خلال التشريعات والأحكام التي وضعتها من خلال الاتفاقيات الدولية والإقليمية؟

إضافة إلى ذلك هناك عدة تساؤلات فرعية في مشكلة البحث أهمها:

أ–هل الجهود الدولية والعربية استطاعت أن تحد من مشكلة الجرائم الإلكترونية؟

ت– هل استطاعت الدول فيما بينها أن تقوم بتسليم المجرمين أو على الأقل تنفيذ ما جاء في بنود الاتفاقيات حول من ارتكب الجرائم الإلكترونية؟

منهج البحث:

نعتمد في هذا البحث المنهج الوصفي، وذلك من خلال تحليل نصوص الاتفاقيات الخاصة بالجريمة الإلكترونية والأحكام القضائية إن وجدت، وذلك للوصول إلى النتائج والتوصيات المرجوة، في نطاق التحقيق الجنائي محاولين قدر الامكان وضع اليد على بعض الحلول الناجعة لمكافحة هذه الظاهرة الإجرامية، مستندين في ذلك إلى عرض وتحليل النصوص القانونية المتعلقة بهذا المجال.

أهمية البحث:

تكمن أهمية البحث في مدى الخطورة التي تُشكلها الجرائم الإلكترونية؛ إذ إنها تطال الحق في الحصول على المعلومات وتمس حرمة الحياة الخاصة للأفراد وتُهدد الأمن الوطني وتُؤدي إلى فقدان الثقة بالتقنية وغيرها من مفاصل الحياة العامة المختلفة، ولذلك تنبهت الدول العربية؛ إذ تظافرت الجهود من أجل عقد الاتفاقيات تحت مظلّة الجامعة العربية وكان ذلك، وكذلك الدول الأفريقية قد عقدت الاتفاقيات حول الجرائم الإلكترونية تحت مظلّة الإتحاد الأفريقي.

هيكلية البحث:

- المقدّمة:
- المبحث الأول: الجهود العربية في مواجهة الجرائم الإلكترونية.
- المبحث الثاني: اتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي.
- الخاتمة: النتائج التوصيات

المبحث الأول: الجهود العربية في مواجهة الجرائم الإلكترونية

تمهيد:

دأبت الدول العربية إلى تكثيف جهودها من أجل الحد من الجرائم الإلكترونية لما ينطوي على هذه الجرائم من مخاطر جمّة تلحق بالمؤسسات والأفراد خسائر باهظة، باعتبارها تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة –البيانات والمعلومات والبرامج في كل أنواعها–، وتطاول المعطيات المخزّنة، والمعلومات المنقولة عبر نظم المعلومات وشبكاتها، وهذا يُظهر مدى خطورة الجريمة الالكترونية، فهي تطاول الحق في المعلومات والحقوق المالية وحقوق الملكية الفكرية والحق المعنوي؛ إذ حرصت الأمانة العامة لمجلس وزراء الداخلية العرب على مكافحة هذه الجرائم بوضع استراتيجية عربية من خلال إعطاء دور للجامعة العربية باتخاذ إجراءات محددة انبثقت من خلالها اتفاقيات عربية وإصدار قانون عربي من أجل مكافحة هذه الجريمة.

وسوف نتناول هذا المبحث في مطلبين، خصصنا المطلب الأول لدور جامعة الدول العربية في مواجهة الجرائم الإلكترونية من خلال الاتفاقيات العربية، وبيّنا في المطلب الثاني الجهود العربية من خلال القانون الجزائي العربي الموحد والقانون النموذجي العربي.

المطلب الأول: دور جامعة الدول العربية في مواجهة الجرائم الإلكترونية من خلال الاتفاقيات العربية

نجحت منظمة جامعة الدول العربية في إبرام عدد من الاتفاقيات التي تعد جهداً متواضعاً في مجال مكافحة الجرائم الإلكترونية، ومن أهمها الاتفاقية العربية لحماية حقوق المؤلف لسنة 1981، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي اعتمدها مجلس وزراء الداخلية العرب في القاهرة في دورته الواحدة والثلاثين بتاريخ 21/ ديسمبر/ 2010، وسوف نتناول هاتين الاتفاقيتين في فرعين خصصنا الفرع الأول للاتفاقية العربية لحماية حقوق المؤلف لسنة 1981، وبيّنا في الفرع الثاني الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لعام 2010م.

الفرع الأول: الاتفاقية العربية لحماية حقوق المؤلف لسنة 1981[1]

أقرّت هذه الاتفاقية بتاريخ 5 تشرين الثاني 1981 بهدف حماية حقوق المؤلفين على المصنفات الأدبية والفنية والعلمية بطريقة فعالة وموحدة، وتجاوباً مع المادة (21) من ميثاق الوحدة الثقافية العربية الصادر في سنة 1964 التي أهابت بالدول العربية أن تضع كل منها تشريعاً لحماية الملكية الأدبية والفنية[2].

وهذه الاتفاقية التي أوصى بها مؤتمر وزراء الثقافة العرب المنعقد في بغداد لسنة 1981، والتي دعت إلى وضع التشريعات اللازمة لحماية الملكية الأدبية والفنية والعلمية، والتي قد تكون هدفاً للجريمة الإلكترونية؛ إذا ما وجدت طريقها للنشر على الشبكة الدولية للمعلومات، لذا ألزمت المادة (23) من هذه الاتفاقية الدول الأعضاء العمل على إنشاء مؤسسات وطنية لحماية حقوق الملكية الأدبية والفنية والعلمية بقولها:" تعمل الدول الأعضاء على إنشاء مؤسسات وطنية لحماية حقوق المؤلف ويحدد التشريع الوطني بنية هذه المؤسسات واختصاصاتها".

ولضمان تحقيق بنود هذه الاتفاقية والتزام الدول الأعضاء بها، فقد انشئت بمقتضى نص المادة (24)، لجنة دائمة لحماية حقوق المؤلف من ممثلي الدول الأعضاء لمتابعة تنفيذ هذه الاتفاقية وتبادل المعلومات بما يكفل حماية المصالح المعنوية والمادية للمؤلفين بقولها:" 1-تنشأ لجنة دائمة لحماية حقوق المؤلف من ممثلي الدول الأعضاء لمتابعة تنفيذ هذه الاتفاقية وتبادل المعلومات بما يكفل حماية المصالح المعنوية والمادية للمؤلفين. 2-ينشأ مكتب لحماية الملكية الأدبية والفنية والعلمية في الإدارة العامة للمنظمة العربية ويتولى أمانة اللجنة الدائمة لحماية حقوق المؤلف.3-تضع اللجنة نظامها الداخلي ويصبح نافذاً بعد إقراره من المجلس التنفيذي والمؤتمر العام للمنظمة"[3].

وتُعدُّ الاتفاقية العربية لحماية حق المؤلف أول اتفاقية تبرمها الدول العربية في هذا الميدان، وبرغم الاتصال المباشر الذي وقع بين الجهات المعدة لهذه الاتفاقية والمنظمة العالمية للملكية الفكرية بقصد أن تكون الحماية متناغمة والتزامات البلدان العربية تجاه الاتفاقيات الدولية ذات الصلة، إلّا أن هذه الاتفاقية وعلى رأي بعض الفقه العربي عرفت نواقص عديدة بحيث لم ترق إلى المستوى الذي كانت تروم له البلدان العربية حينها، وبقراءة نصوص هذه الاتفاقية نجدها لم تتبنَّ أية إشارة للنص

([1]) مقر توقيع هذه الاتفاقية بغداد، ونشرت في الجريدة الرسمية العراقية، العدد الحادي عشر، تاريخ النشر 1986/01/01 الموافق 1406/04/20هـ، ص420 وما بعدها.

([2]) بلال محمود عبد الله، حق المؤلف في القوانين العربية، ط1، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، بيروت، 2018م، ص21.

([1]) خالد حسن أحمد لطفي، الإرهاب الإلكتروني، آفة العصر الحديث والآليات القانونية للمواجهة، دار الفكر الجامعي، الإسكندرية، 2018م، ص178.

على نظام الإدارة الجماعية لحق المؤلف وللحقوق المجاورة، ولربما يرجع السبب في ذلك إلى كون أنه لا توجد اتفاقية دولية تلزم على الدول العمل بنظام الإدارة الجماعية لحق المؤلف والحقوق المجاورة[1].

الفرع الثاني: الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لعام 2010م

إنّ جهود الجامعة العربية في مكافحة الجرائم الإلكترونية توّجت بتوقيع اتفاقية عربية لمكافحة جرائم تقنية المعلومات في نهاية سنة 2010، حيث صدرت بعد موافقة مجلسا وزراء الداخلية والعدل العرب عليها في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 1432/1/15هـ الموافق 2010/12/21[2]، ودخلت حيز النفاذ اعتبارا من تاريخ 2014/2/7، بعد مضي ثلاثين يومياً من تاريخ إيداع وثائق التصديق عليها أو إقرارها من سبع دول عربية إعمالاً للفقرة (3) من الأحكام الختامية للاتفاقية التي تنص على أنه: "3- تسري هذه الاتفاقية بعد مضي ثلاثون يوما من تأريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية"[3].

تهدف الاتفاقية إلى تعزيز التعاون بين الدول فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها وأفرادها، وتتكون هذه الاتفاقية من (43) مادة، منها (21) مادة في باب التجريم، و(8) مواد إجرائية تتعلق بحقوق السلطات وجمع المعلومات وتتبع المستخدمين، وضبط المواد المخزنة على الحواسيب الشخصية والأجهزة التقنية، ويتكون الفصل الرابع من (14) مادة تنظم التعاون بين الدول الأعضاء في تبادل معلومات المستخدمين؛ حيث يكون نطاق سريان هذه الاتفاقية على المستوى الإقليمي[4].

وتضمنت الاتفاقية المذكورة الأحكام الموضوعية والمتمثلة في تجريم الأفعال المكونة لجرائم تقنية المعلومات وهي: الاختراق، والاعتراض، والاعتداء على سلامة البيانات والملكية الفكرية، وإساءة استخدام وسائل تقنية المعلومات، والتزوير، والاحتيال، والإباحية، وجرائم تقنية المعلومات المتعلقة

([2]) سامر محمود دلالعة، بحث بعنوان (التدابير الدولية في مجال الإدارة الجماعية لحقوق المؤلف والحقوق المجاورة بين النظرية والتطبيق، دراسة مقارنة)، منشور في مجلة المنارة للبحوث والدراسات، المجلد الثالث عشر، العدد الثامن، جامعة آل البيت، عمّان، 2007م، ص221-222.

([2]) سليم بشير، حل مشكلة تنازع الاختصاص الجنائي الدولي في مجال مكافحة جرائم التجارة الإلكترونية-وفقاً للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010م، بحث منشور بمجلة الحقوق والحريات، جامعة محمد خيضر-بسكرة، الجزائر، المجلد (5)، العدد (1)، السنة 2019م، ص123.

([3]) الفقرة (3) من الأحكام الختامية للاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

([4]) صفاء كاظم غازي الجياشي، رسالة ماجستير بعنوان (جريمة قرصنة البريد)، كلية القانون، جامعة بابل، 2016م، ص42.

بالإرهاب الإلكتروني، وغسل الأموال والمخدرات، والإتجار بالجنس البشري والأسلحة، والاستخدام غير المشروع لأدوات الائتمان والوثائق الإلكترونية"، فضلاً عن تشديد العقوبات على الجرائم التقنية التي ترتكب بواسطة تقنية المعلومات [1].

وتضمنت هذه الاتفاقية جريمة التسبب بالحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع [2]، فضلا عن ذلك تجريم أفعال إنتاج أو عرض أو توزيع أو تشفير أو نشر أو شراء أو بيع، أو اسيتراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات، وكذلك تم تجريم المقامرة والتحريض على الدعارة والفجور وجرائم الآداب العامة[3]، بالإضافة إلى الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد أو التشهير والسب والقذف والإساءة إلى السمعة بواسطة تقنية المعلومات[4]، إضافة إلى ذلك تناولت الاتفاقية العربية الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات[5]، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة

([1]) رامي متولّي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، ط1، دار النهضة العربية، القاهرة، 2011م، ص75.

([2]) نصت المادة (11) من الاتفاقية على أنه:" جريمة الاحتيال: التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق: 1-إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات. 2-التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها. 3-تعطيل الأجهزة والبرامج والمواقع الإلكترونية". ونصت المادة (12) من هذه الاتفاقية على أن:" جريمة الإباحية: 1-انتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات. 2-تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر. 3-يشمل التشديد الوارد في الفقرة (2) من هذه المادة، حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات".

([3]) نصت المادة (13) من هذه الاتفاقية على أن:" الجرائم الأخرى المرتبطة بالإباحية: هي المقامرة والاستغلال الجنسي".

([4]) نصت المادة (14) من هذه الاتفاقية على أن:" جريمة الاعتداء على حرمة الحياة الخاصة: الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات".

([5]) نصت المادة (15) من هذه الاتفاقية على أن:" الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات: 1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها. 2-تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية. 3-نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية. 4-نشر النعرات والفتن والاعتداء على الأديان والمعتقدات".

بواسطة تقنية المعلومات[1] والجرائم المتعلقة لانتهاك حق المؤلف والحقوق المجاورة [2]، وجرائم الاستخدام غير المشروع لأدوات الدفع الإلكترونية[3]، وهي (بطاقات الدفع المسبق، الحوالات المصرفية، المواقع الإلكترونية أو الحسابات، شركات التحويل)[4]، وخيراً جريمة الشروع والاشتراك في ارتكاب الجرائم، هذا وتعد هاتان الاتفاقيتان مثالاً واضحاً على جهود الجامعة العربية والمنظمات المتخصصة التابعة لها في مجال تنظيم حقوق المؤلف، وإن كان يعد هذا جهداً متواضعاً بوصفها تصب في اتجاه الوقاية من جرائم الحاسوب[5].

هذا وبالرجوع إلى ميثاق جامعة الدول العربية لسنة 1945 بوصفه دستور هذه المنظمة، لا يمكن العثور فيه على ما يشير إلى الجرائم الإلكترونية، وما يرتبط به من تفرعات، ومع ذلك فإن تأويل الدلالة العامة لبعض النصوص الواردة في هذا الميثاق، قد يخدم جهود مكافحة الإرهاب، ومن ذلك ما جاء في المادة الثانية من هذا الميثاق والتي أوضحت مقاصد هذه المنظمة في تحقيق التعاون بين الدول الأعضاء لصيانة استقلالها وسيادتها[6].

([1]) نصت المادة (16) على أن:" الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات: 1-القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال. 2-الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها. 3-الاتجار بالأشخاص. الاتجار بالأعضاء البشرية. 4-الاتجار غير المشروع بالأسلحة".

([2]) نصت المادة (17) على أن:" الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة: انتهاك حق المؤلف؛ كما هو معرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي".

([3]) نصت المادة (18) على أن:" الاستخدام غير المشروع لأدوات الدفع الإلكترونية:-1 كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكترونية بأي وسيلة كانت. 2-كل من استولى على بيانات أي أداة من أدوات واستعملها أو قدمها للغير أو سهل للغير الحصول عليها. 3- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع. 4-كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك".

([4]) ناظم محمد نوري الشمري، عبد الفتاح زهير العبد اللات، الصيرفة الإلكترونية، ط1، دار وائل للنشر، عمّان، 2008م، ص80.

([5]) نصت المادة (19) على أن:" الشروع والاشتراك في ارتكاب الجرائم: 1-الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف. 2-الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية. 3-يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئياً".

([6]) نصت المادة (2) من ميثاق الجامعة العربية لسنة 1945 على أنه:" الغرض من الجامعة توثيق الصلات بين الدول المشتركة فيها، وتنسيق خططها السياسية، تحقيقا للتعاون بينها وصيانة لاستقلالها وسيادتها، والنظر بصفة عامة في شؤون البلاد العربية ومصالحها. كذلك من أغراضها تعاون الدول المشتركة فيها تعاوناً وثيقاً بحسب نظم

ويمكن القول أن مقاصد منظمة جامعة الدول العربية ستتعارض بالضرورة مع ما تنطوي عليه وسائل الجرائم الإلكترونية من تجاوزات وإخلال لسلطة وسيادة الدول عبر التعرض لنظم المعلومات المرتبطة بالمؤسسات السيادية أو حتى إمكانية التحريض ضد النظام باستغلال وسائل التواصل الإلكتروني فضلا عن إمكانية استغلال المعلومات الحساسة، وتوظيفها ضد مصالح الدولة العربية المستهدفة، الأمر الذي يستدعي تعاون الدول العربية طبقا لهذه للمادة الثانية من الميثاق سابقة الذكر لمواجهة مثل هذه الانشطة الإرهابية عبر الفضاء الإلكتروني، وهو الاتجاه الذي أكدته المادة الثالثة من الميثاق حينما خولت مجلس الجامعة ، تقرير وسائل التعاون مع الهيئات الدولية التي قد تنشأ في المستقبل لكفالة الأمن والسلام[1].

المطلب الثاني: الجهود العربية من خلال القانون الجزائي العربي الموحد والقانون النموذجي العربي

هناك جهود عربية حول تشريع وسن قوانين موحدة عن طريق الجامعة العربية للحد من الجرائم الإلكترونية، وتكللت هذه الجهود بإصدار القانون الجزائي العربي الموحد لسنة 1996، والقانون النموذجي العربي لسنة 2003، وسوف نتناول هذه القانونين بفرعين على التوالي:

الفرع الأول: القانون الجزائي العربي الموحد بموجب القرار رقم (229) لسنة 1996

إن أبرز الجهود العربية المبذولة من أجل الحماية من جرائم الحاسب الآلي، اعتماد وزراء العدل العرب للقانون الجزائي العربي الموحد قانوناً نموذجياً بموجب القرار (229) لسنة 1996، وبالرجوع إلى المذكرة الإيضاحية لهذا القانون[2].

وباستعراض الباب السابع الخاص بالجرائم ضد الأشخاص يلاحظ الباحث أن هذا القانون احتوى على فصل خاص بالاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية، وذلك

كل دولة منها وأحوالها في الشؤون الآتية: 1-الشؤون الاقتصادية والمالية، ويدخل في ذلك التبادل التجاري والجمارك، والعملة، وأمور الزراعة والصناعة.2-شؤون المواصلات ويدخل في ذلك السكك الحديدية، والطرق، والطيران، والملاحة، والبرق، والبري 3-شؤون الثقافة .4-شؤون الجنسية، والجوازات، والتأشيرات، وتنفيذ الأحكام وتسليم المجرمين.5-الشؤون الاجتماعية.6-الشؤون الصحية".

(1) نصت المادة (3) من الميثاق على أنه:" يكون للجامعة مجلس يتألف من ممثلي الدول المشتركة في الجامعة، ويكون لكل منها صوت واحد مهما يكن عدد ممثليها. وتكون مهمته القيام على تحقيق أغراض الجامعة، ومراعاة تنفيذ ما تبرمه الدول المشتركة فيها من اتفاقات في الشؤون المشار إليها في المادة السابقة، وفي غيرها، ويدخل في مهمة المجلس كذلك تقرير وسائل التعاون مع الهيئات الدولية التي قد تنشأ في المستقبل، لكفالة الأمن والسلام، لتنظيم العلاقات الاقتصادية والاجتماعية".

(2) علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية للنشر والتوزيع، عمّان، 2018م، ص132.

في المواد (461 إلى 464)؛ إذ أشارت المواد (461، 462، 463) على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية، وكيفية جمع المعلومات الإسمية وكيفية الاطلاع عليها، والعقاب المطبق في حال ارتكاب هذه الجرائم[1].

أما المادة (464) فقد أشارت بعقاب من يقوم بفعل الدخول بطريق الغش إلى كامل أو جزء من المعالجة الآلية للمعلومات، وعرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتادة، وتغيير المعلومات داخل النظام وتزوير وثائق المعالجة الآلية، وسرقة المعلومات [2]، وتعد هذه المحاولة على الرغم من تواضعها أبرز ما تم على صعيد تعزيز التعاون على المستوى وطننا العربي من الناحية التشريعية [3].

([1]) نصت المادة (461) من القانون الجزائي العربي الموحد رقم (229) لسنة 1996 على أنه:" يعاقب بالحبس والغرامة كل من قام بأحد الأفعال الآتية: 1. دفع الغير إلى القيام بمعالجات آلية لمعلومات اسمية ولو نتيجة إهمال دون مراعاة الإجراءات القانونية الأولية لاستعمالها؛ 2. دفع الغير إلى القيام بمعالجات آلية لمعلومات اسمية ودون مراعاة الاحتياطات الضرورية للمحافظة على سلامة تلك المعلومات وعلى الخصوص بالحيلولة دون تحريفها أو إتلافها أو إبلاغها إلى أشخاص ليس لديهم إذن للحصول عليها؛ 3. جمع معلومات بأية وسيلة غير مشروعة أو إجراء معالجة لمعلومات اسمة تتعلق بشخص رغم معارضته المبنية على أسباب مشروعة؛ 4. جمع معلومات اسمية تتعلق بجرائم أو أحكام صادرة بالإدانة أو الاحتفاظ بها في ذاكرة المعلومات في غير الحالات المسموح بها قانوناً".

– ونصت المادة (462) من نفس القانون على أنه:" يعاقب بالحبس مدة تزيد على سنة وبالغرامة كل من حصل على معلومات أسمية خاصة بالغير أثناء تسجيلها أو ترتيبها أو إرسالها بأية وسيلة من وسائل المعالجة التي من شأن إفشائها المس بسمعة المعنى بالأمر أو بحياته الشخصية، مما يمكن إطلاع الغير ممن تسمح له صفته الاطلاع على تلك المعلومات دون إذن المعنى بالأمر".

– ونصت المادة (463) من ذلك القانون على أنه:" تطبق مقتضيات الفقرات 2،3،4، من المادة (461) إذا وقعت نفس الأفعال الواردة بها على الجذاذات غير الآلية أو الميكاتوغرافية التي ينحصر استعمالها على وجه الخصوص على ممارسة الحق في الحياة الشخصية ".

([2]) نصت المادة (464) من القانون الجزائي العربي الموحد رقم (229) لسنة 1996 على أنه:" يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من: 1. دخل بطريق الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات، أو بقي فيه وتضاعفت العقوبات إذا نتج عن ذلك إما محو المعلومات التي يحتوي عليها النظام أو تعديلها وإما تعطيل تشغيل ذلك النظام؛ 2. عرقل أو أفسد عمداً تشغيل نظام المعالجة الآلية للمعلومات؛ 3. أدخل أو عدل بطريق الغش معلومات في نظام المعالجة الآلية على المعلومات التي يحتوي عليها؛ 4. زور للإضرار بالغير وثائق المعالجة الآلية أو استعمل الوثائق المزورة المذكورة أعلاه مع علمه ذلك؛ 5. سرق معلومات من نظام المعالجة الآلية".

([3]) محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار العلم والثقافة للنشر والتوزيع، عمّان، 2005م، ص171.

الفرع الثاني: القرار رقم (495) المتضمن القانون العربي النموذجي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لسنة 2003[1]

اعتمد القانون العربي الاسترشادي الإماراتي لمكافحة جرائم تقنية المعلومات، في الجامعة العربية من قبل وزراء العدل العرب في الدورة التاسعة عشر بتاريخ 2003/10/8 [2]، استناداً إلى قرارها المرقم (495_د 19_2003/10/8)، وذلك عبر الأمانة الفنية لمجلس وزراء العرب [3].

وأبرز ما يمكن ذكره بخصوص الجهود العربية المبذولة في سبيل تحقيق التقارب والتوافق بين النصوص التشريعية العقابية والإجرائية الوطنية التي تعني بالإجرام الإلكتروني، القرار رقم (495) المتضمن القانون العربي النموذجي لمكافحة الجريمة الإلكترونية، لاسيما بعد أن أدى رواج المعلومات في كل الدول العربية إلى ظهور عدة ممارسات إجرامية في هذا النطاق مما حدا بهذه الدول إلى المحاولة لإيجاد سبل تشريعية ناجعة لمواجهة هذا النوع من الجرائم المتجددة [4].

ويمثل هذا القانون القواعد الأساسية الإرشادية التي يمكن أن يستعين بها المشرع في الدول العربية عندما يريد سن نصوص وطنية بخصوص الجرائم الإلكترونية، سواء باستحداث قوانين خاصة بذلك أو تحديث قوانينه القائمة، وقد تضمن هذا القانون (27) مادة، موزعة على أربعة أبواب [5]، عالج الباب الأول الجرائم الإلكترونية والعقوبات المقررة إزائها، حيث تم النص عليها في المواد من (3 إلى 22) ويمكن تلخيصها فيما يلي[6]:

([1]) تم إعداد هذا القانون من قبل لجنة مشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب والمكتب التنفيذي لمؤتمر وزراء الداخلية العرب؛ إذ جرى إقراره بوصفه منهجاً استرشادياً للمشرع الوطني عند إعداد تشريع يتعلق بالجرائم المعلوماتية.

([2]) اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم (495) –19، 2003/10/8، واعتمده مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (417) – د21–، 2004.

([3]) عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم المعلوماتية)، منشورات الحلبي الحقوقية، بيروت، 2007م، ص180

([4]) عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، أكاديمية نايف العربية للعلوم الأمنية–الرياض، 2009م، ص50.

([5]) ملياني عبد الوهاب، رسالة دكتوراه بعنوان (أمن المعلومات في بيئة الأعمال الإلكترونية)، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبي بكر بلقايد، الجزائر، 2017م، ص160.

([6]) عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الاسكندرية، 2006م، ص10.

1- جريمة الولوج غير المشروع وبغير حق إلى موقع أو نظام معلوماتي، والتلاعب في بياناته، مع تشديد العقوبة إذا كان بغرض إلغاء أو حذف أو تدمير أو إنشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات شخصية [1].

2- جريمة تزوير المستندات المعالجة في نظام معلوماتي واستعمالها[2].

3- جريمة الإدخال المؤدي إلى إيقاف أو تعطيل نشاط الشبكة المعلوماتية، أو إتلاف البرامج أو البيانات فيها [3].

4- جريمة التصنت [4]، واعتراض المراسلات دون وجه حق عبر الشبكة المعلوماتية [5].

5- الجرائم المخلة بالآداب العامة والنظام العام وأمن الدولة عبر الشبكة المعلوماتية [6].

([1]) نصت المادة الثالثة من القانون العربي النموذجي لمكافحة الجريمة الإلكترونية لسنة 2003 على أنه:" 1-كل من دخل عمداً وبغير وجه حق موقعاً أو نظاماً معلوماتيا يعاقب بالحبس ... والغرامة ..... أو بإحدى هاتين العقوبتين. 2-فإذا كان الدخول بقصد إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات شخصية يكون الحد الأدنى لعقوبة الحبس ..... ولعقوبة الغرامة.....".

- وقد عرف القانون العربي النموذجي الاختراق بأنه: "الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات، وذلك عن طريق انتهاك الإجراءات الأمنية.

([2]) نصت المادة (4) من نفس القانون على أنه:" كل من ارتكب تزويراً في أحد المستندات المعالجة في نظام معلوماتي يعاقب بالحبس مدة لا تقل عن .... ويعاقب بذات العقوبة كل من أستعمل المستند المزور مع علمه بالتزوير".

([3]) نصت المادة (6) من نفس القانون على أنه:" كل من أدخل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات بغرض ذلك ولم يتحقق غرضه يعاقب بالحبس .... والغرامة ..... أو بإحدى هاتين العقوبتين. فإذا تحقق الغرض كان الحد الأدنى لعقوبة الحبس ..... ولعقوبة الغرامة ....".

([4]) يقوم التنصت على التمركز في موقع معين داخل شبكة الاتصالات وتسجيل أو حفظ البيانات المتبادلة فيما بين الأنظمة المعلوماتية. انظر: نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، 2008م، ص159.

([5]) نصت المادة (8) من نفس القانون على أنه:" كل من تنصت أو التقط أو أعترض بدون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، يعاقب بالحبس.... والغرامة .... أو بإحدى هاتين العقوبتين".

([6]) نصت المادة (9) من هذا القانون على أنه:" كل من استعمل الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها في تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس ..... والغرامة ..... أو بإحدى هاتين العقوبتين".

وتناول الباب الثاني، التجارة والمعاملات الإلكترونية، أما الباب الثالث فقد تناول تدابير حماية حقوق الملكية الفكرية عبر الوسائل الإلكترونية، في حين عالج الباب الرابع الجوانب الإجرائية المتعلقة بالجرائم الإلكترونية [1].

وأورد هذا القانون وصفاً لجريمة الاحتيال المعلوماتي والتي أطلق عليها تسمية جريمة الاحتيال عن طريق الشبكة المعلوماتية والحاسوب وعالجها في نص المادة العاشرة منه بقولها:" كل من توصل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس... والغرامة... أو بإحدى هاتين العقوبتين"[2].

ويلاحظ أن المشرع في القانون العربي النموذجي لمكافحة الجريمة الإلكترونية قد شدد في عقوبة جريمة الاحتيال عبر شبكة الإنترنت العالمية بحيث إذا وجدت عقوبة في قوانين العقوبات العربية بالإضافة إلى العقوبة الموجودة في القانون العربي النموذجي لمكافحة الجريمة الإلكترونية، فإن العقوبة الأشد هي الواجبة التطبيق، وكذلك يلاحظ أن المشرع في هذا القانون قد ترك أمر تحديد العقوبة–الحبس والغرامة–إلى القانون الوطني لكل دولة بما يتلاءم مع التشريعات وسياسة التجريم والعقاب [3].

هذا من جهة ومن جهة أخرى عالج نفس القانون الاحتيال بواسطة بطاقات الدفع الإلكترونية للأموال في نص المادة (11) منه بقولها:" كل من استخدم الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي (وما في حكمها) في الوصول، بدون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية وما في حكمها بقصد استخدامها في الحصول على بيانات الغير أو أمواله أو ما تتيحه من خدمات، يعاقب بالحبس.... والغرامة.... أو بإحدى هاتين العقوبتين"[4].

([1]) ضرغام جابر عطوش، جريمة التجسس المعلوماتي (دراسة مقارنة)، ط1، المركز العربي للنشر والتوزيع، القاهرة، مكتبة دار السلام القانونية، النجف الأشرف، 2017م، ص66. كذلك: سليمان أحمد فضل، المواجهة التشريعية الناشئة عن استخدام معلومات الإنترنت، دار النهضة العربية، القاهرة، 2007م، ص437.

([2]) موفق علي عبيد وساهر ماضي ناصر، بحث بعنوان (ماهية جريمة الاحتيال المعلوماتي)، منشور في مجلة جامعة تكريت للعلوم القانونية، السنة السابعة، العدد الخامس والعشرون، جمادي الآخرة/ 1435هـ–أذار/ 2015م، ص195 وما بعدها.

([3]) إبراهيم بشار عواد، رسالة دكتوراه بعنوان (جريمة الاحتيال عبر شبكة المعلومات الدولية، دراسة مقارنة بين القانون الأردني والقانون المصري)، كلية الدراسات القانونية العليا، جامعة عمّان العربية، عمّان، 2009م، ص180.

([4]) عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ط1، دار النهضة العربية، القاهرة، 2004م، ص42.

وتعتبر بطاقات الائتمان بطاقات وفاء فوري، أو على شكل دفعات أو بعد مضي فترة، والتي يتم عن طريقها سداد أثمان المشتريات أو الحصول على الخدمات لحامليها؛ كما تقوم بطاقات الائتمان بوظائف أخرى وهي كونها أداة في بعض أنواعها، وأداة ضمان الشيكات في أنواعها الأخرى[1].

وبطاقة الائتمان، هي عبارة عن بطاقة مصنوعة من البلاستيك تصدر من مؤسسة ما إلى حاملها أي العميل تخوله الحق في الحصول على تسهيل ائتماني من الجهة المصدرة لهذه البطاقات لحاملها؛ حيث يقدمها للتاجر ويحصل على سلع وخدمات تسدد قيمتها للتاجر من قبل الجهة التي اصدرت البطاقة، وقد ظهرت البطاقات الائتمانية لأول مرة في الولايات المتحدة الامريكية قبل الحرب العالمية الاولى ثم انتقلت إلى فرنسا في أواخر العشرينات من القرن المنصرم [2].

وبالرجوع إلى أحكام هذا القانون يلاحظ أنه قد جعل عقوبة الانتفاع بدون وجه حق عن طريق الشبكة المعلوماتية على ارتكاب الجريمة مساوية من حيث المقدار للعقوبة المقررة لها، وذلك لخصوصية وطبيعة هذا النوع من الجرائم، وهذا ما نصت عليه المادة (12) من القانون الإسترشادي بقولها:" كل من انتفع، بدون وجه حق عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بخدمات الاتصالات يعاقب بالحبس ... والغرامة ..." [3].

ونصت المادة (13) من نفس القانون على أنه:" 1-كل من أنتج أو أعد أو هيأ أو أرسل أو خزن عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها ما من شأنه المساس بالنظام العام أو الآداب العامة يعاقب بالحبس ... والغرامة ... 2-فإذا كان الفعل موجهاً إلى حدث يكون الحد الأدنى لعقوبة الحبس ... ولعقوبة الغرامة".

يتضح من هذا النص أن كل نشاط يعمله الشخص المحتال (الجاني) عن طريق شبكة المعلومات أو أجهزة الحاسب الآلي من شأنه المساس بالنظام العام أو الآداب العامة يعاقب بالحبس

([1]) نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، ط1، منشورات الحلبي الحقوقية، بيروت، 2005م، ص508.

([2]) عمر سالم، الحماية الجنائية لبطاقات الوفاء، دار النهضة العربية، القاهرة، 1995م، ص14 وما بعدها. كذلك عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، ط1، دار الفكر الجامعي، الإسكندرية، 2008م، ص16.

([3]) فريد جبور، حماية المستهلك عبر الإنترنت ومكافحة الجريمة الإلكترونية، منشورات الحلبي الحقوقية، بيروت، 2008م، ص240.

والغرامة إضافةً إلى ذلك إذا كان هذا النشاط موجهاً إلى حدث يكون الحد الأدنى لعقوبة الحبس ولعقوبة الغرامة[1].

ونص هذا القانون على العديد من المواد التي من شأنها توفير الحماية القانونية لخصوصية ما يتم نشره وتداوله على الشبكة المعلوماتية من معلومات وبيانات وأرقام تتعلق بالبطاقات الائتمانية، وأرقام وبيانات الحسابات المصرفية أو أية وسيلة من وسائل الدفع الإلكتروني، وكذلك كل استخدام لأي من وسائل تقنية المعلومات في تزوير أو تقليد أو نسخ للبطاقات الائتمانية أو البطاقات المدنية؛ كما عاقب كل من ابتز أو هدد شخصاً آخر لحمله على القيام بفعل أو الامتناع عنه، وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات[2].

ونرى أنَّ القانون الاسترشادي من القوانين المتقدمة والفعالة في الوطن العربي لمكافحة جرائم شبكة المعلومات الدولية ومن بينها جريمة الاحتيال؛ حيث وضع هذا القانون القواعد الأساسية التي يتعين على المشرع العربي اللجوء إليها عند سن قانون وطني لمكافحة هذه الجريمة، سواءً أكان القانون الوطني مستقلاً لمكافحة هذه الجريمة المستحدثة أم كان تعديلاً لقانون العقوبات المطبق في أي دولة من الدول العربية.

وتجدر الإشارة إلى أنه هناك مبادرات لتحديث وتطوير عمل النيابات العامة في الدول العربية التي يقوم بتنفيذها برنامج الأمم المتحدة الإنمائي – برنامج إدارة الحكم في الدول العربية (UNDP) منذ العام 2002، وتم تنظيم مجموعة من الأنشطة تتضمن ندوات تثقيفية ودورات تدريبية بغية توطيد المعرفة لدى أعضاء النيابات العامة حول الجرائم الحديثة من أجل تفعيل دورهم في تعزيز حكم القانون وبناء قدراتهم لجهة استخدام أساليب ومنهجيات التحقيق المتطورة، وقد ركز المشروع ضمن إطار نشاطاته على موضوع مكافحة الجرائم الإلكترونية، وتحقيقاً لهذه الغاية قام بتنظيم ندوة إقليمية تحت عنوان (الجرائم المتصلة بالكمبيوتر)[3].

ونظراً لأهمية القانون العربي لمكافحة جرائم الإنترنت، فقد حث المؤتمر الإقليمي للدول العربية حول جرائم الإنترنت من خلال العديد من التوصيات، الدول العربية على استخدام هذا القانون كنموذج

([1]) المستشار أيمن بن ناصر بم حمد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، دراسة مقارنة، ط1، مكتبة القانون والاقتصاد، الرياض، 1436هـ-2015م، ص183.

([2]) انظر: المواد (14، 15، 16، 17، 18، 19، 20، 21، 22، 23، 24، 25، 26، 27)، من القانون العربي النموذجي لمكافحة الجريمة الإلكترونية وما في حكمها لسنة 2003م.

([1]) وسيم حرب، كتاب برنامج تعزيز حكم القانون في بعض الدول العربية، مشروع تحديث النيابات العامة، كتاب أعمال الندوة حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 2007م، ص8.

يمكن أن يساعدهم في وضع قانون وطني فيما يتعلق بجرائم الإنترنت، ويساعدهم في الوقت نفسه على تجسيد تقارب وتلائم بين هذه القوانين الوطنية بعضها البعض[1].

المبحث الثاني: اتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي لسنة 2014

تمهيد:

هناك جهود اقليمية في مواجهة الجرائم الإلكترونية تقودها منظمات اقليمية بين دول يجمعها قاسم مشترك مثلما تطرقنا عن جهود الجامعة العربية كالاتحاد الإفريقي، وذلك يعبر عن توجهات الدول نحو ضرورة وضع أطر وأنظمة قانونية إقليمية لمكافحة الجريمة الإلكترونية في ظل غياب إطار عالمي موحد واختلاف الأقاليم من حيث البنية التحتية التكنلوجية، وطريقة مقاربتها لموضوع الجريمة الإلكترونية وتشعباتها الدولية.

وسوف نقسم هذا المبحث إلى مطلبين تناولنا في المطلب الأول أوليات الجهود المبذولة من قبل الإتحاد الأفريقي للح من الجرائم الإلكترونية والأمن السيبراني، وبيّن في المطلب الثاني أحكام اتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014.

المطلب الأول: أوليات الجهود المبذولة من قبل الإتحاد الأفريقي للحد من الجرائم الإلكترونية والأمن السيبراني

نتناول في هذا المطلب بداية الجهود المبذولة من قبل الإتحاد الإفريقي للحد من الجرائم الإلكترونية والأمن السيبراني والقواعد العامة التي تناولتها اتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014 في فرعين على التوالي:

([2]) انظر: لتوصية رقم (1) الصادرة عن المؤتمر الإقليمي للدول العربية حول جرائم الانترنت المنعقد في الدار البيضاء بتاريخ 19- جوان 2007، متاحة باللغة العربية على الموقع:

http://www.arab-niaba.org/publications/crime/casablanca/recommendations-a.pdf.

- التوصية رقم (2) الصادرة عن المؤتمر الإقليمي للدول العربية حول جرائم الانترنت المنعقد في القاهرة بتاريخ 26، 27 نوفمبر 2007، متاحة باللغة العربية على الموقع:

https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_Arabic.pdf

الفرع الأول: بداية الجهود المبذولة من قبل الإتحاد الإفريقي للحد من الجرائم الإلكترونية والأمن السيبراني

بداية الجهود كانت من خلال المؤتمر الاستثنائي الذي عقد في جوهانسبرغ جنوب أفريقيا سنة 2009، لوزراء الإتحاد الإفريقي للقطاعات المتعلقة بالاتصالات وتكنولوجيا المعلومات للبلدان الإفريقية، نوقشت العديد من القضايا المتعلقة بتنامي الاستخدام المتزايد لتكنولوجيا المعلومات والاتصالات وأثر استخدامها السيئ على الأمن السيبراني للبلدان الإفريقية، وتقرر على أثر هذه المناقشات أن تضع مفوضية الإتحاد الإفريقي وبمشاركة لجنة الأمم المتحدة الاقتصادية لأفريقيا، إطاراً قانونياً للبلدان الإفريقية يعالج كافة المسائل المتعلقة بحماية البيانات، والأمن السيبراني، والتجارة الإلكترونية.

بناء على ذلك قدم الإتحاد الإفريقي لسنة 2011، مشروعاً لاتفاقية تتعلق بإرساء إطاراً قانونياً موثوقاً للأمن في الفضاء السيبراني، تسعى من خلاله الدول الأعضاء والمجموعات الاقتصادية والإقليمية في أفريقيا إلى محاولة تحديد الأهداف والتوجهات الرئيسية لمجتمع المعلومات، وتعزيز الأنظمة الحالية الخاصة بالأمن السيبراني وحماية البيانات والتجارة الإلكترونية، مسترشداً بالقانون التأسيسي للاتحاد والمعتمد في سنة 2000، أخذاً بنظر الاعتبار أن الاتفاقية تتكفل بالالتزامات الحالية للدول الأعضاء في الإتحاد على المستويات الإقليمية الفرعية والإقليمية والدولية لبناء مجتمع المعلومات[1].

وتجدر الإشارة إلى أنّ ولاية الاتفاقية لا تقتصر على الأمن السيبراني والجرائم الإلكترونية فحسب، بل شملت أيضا قضايا مجتمع المعلومات (حماية المعلومات ذات الطابع الشخصي، والتجارة الإلكترونية)، أخذه بنظر الاعتبار الالتزام باحترام مبادئ حقوق الإنسان الأساسية المكفولة بموجب أحكام القوانين المحلية ولاسيما الميثاق الإفريقي لحقوق الإنسان والشعوب، وكذلك بموجب الاتفاقيات والمعاهدات الدولية المتعلقة بحقوق الإنسان، وتعد هذه الاتفاقية أكثر شمولاً من أغلب الاتفاقيات والصكوك الإقليمية الأخرى بالرغم من أن الإتحاد الإفريقي أرجأ اعتمادها مرات عدة ولكنها اعتمدت مؤخراً في عام 2014، ووقعت من قبل (14) دولة ولم يصادق عليها إلا من قبل (5) دول من أصل (55) دولة.

(1) For more information, see: CCDCOE – The Nato Cooperative Cyber Defence Center Of Excellence, African United, Published Online At: https://ccdcoe.org/organisations/au/, Last visit In: 05/03/2020.

هذا وتسعى الاتفاقية لوضع أحكام القانون الجنائي الإجرائية والموضوعية لمعالجة حوكمة الأمن السيبراني ومكافحة الجرائم الإلكترونية في دول الإتحاد الإفريقي، ولفرض التزامات وتدابير واسعة النطاق على الدول الأعضاء لوضع سياسات وطنية لتعزيز استقرار الأمن السيبراني، وكذلك الأُطر القانونية والتنظيمية والمؤسسية للأمن السيبراني المحوكمة ومراقبة ومكافحة الجرائم الإلكترونية.

الفرع الثاني: القواعد العامة التي تناولتها اتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014

تتألف اتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي من أربعة فصول، تناولت في الفصل الأول كل ما يتعلق بالتجارة الإلكترونية من حيث جوانبها المختلفة، كالمسؤولية التعاقدية للموردين الإلكترونيين للسلع والخدمات، والتزامات المعاهدة في الشكل الإلكتروني وأمن المعاملات (التجارة) الإلكترونية، وفي الفصل الثاني تناولت أحكام قضايا حماية البيانات ذات الطابع الشخصي، وأكد الفصل الثالث على التزامات الدول بتعزيز الأمن الإلكتروني ومكافحة الجريمة الإلكترونية، أما الأحكام الختامية فقد تناولتها الاتفاقية في الفصل الرابع[1].

وفي هذا الصدد فقد أشارت الاتفاقية إلى العديد من الالتزامات التي يقع على الدول الأطراف تنفيذها والتي تتمثل في إنشاء إطار وطني موحد للأمن السيبراني، وتعزيز ثقافة الأمن السيبراني، وإنشاء مؤسسات وطنية لإدارة الأمن السيبراني، وحماية البنية التحتية للمعلومات الحرجة، واتخاذ الإجراءات والتدابير المناسبة لمكافحة الجرائم الإلكترونية، وتعزيز وتنسيق التعاون الدولي والقانوني لمكافحة الجرائم الإلكترونية.

تناولت الاتفاقية تعاريف بعض المصطلحات الواردة في أحكامها والتي من أهمها (الاتصالات الإلكترونية، البيانات المحوسبة، البنية التحتية الحيوية للإنترنت، تكنولوجيا المعلومات والاتصالات، القاصر، المواد الإباحية التي يستغل فيها الأطفال، نظام الحاسوب، مدونة قواعد السلوك، التجارة الإلكترونية، الاتفاقات السرية[2]؛ كما تناولت أحكام ومجال تطبيق التجارة الإلكترونية، والمسؤولية التعاقدية لمزودي السلع والخدمات عن طريق الوسائل الإلكترونية، والدعاية، والالتزامات التعاقدية

([1]) For more information, see: African Union, African Union Convention on Cyber Security and Personal Data Protection, Published Online At: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection, Last visit In: 05/03/2020

([1]) المادة (1) من اتفاقية الإتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي لسنة 2009.

في الشكل الإلكتروني لأحكام وأنواع العقود الإلكترونية، والكتابة في شكل إلكتروني، وأحكام تأمين المعاملات الإلكترونية في المادة (7) من الاتفاقية؛ كما تضمنت الاتفاقية ايضاً أحكام حماية البيانات ذات الطابع الشخصي في المواد (8، 9، 10)، فقد أشارت المادة (8) على أهداف الاتفاقية فيما يتعلق بالبيانات ذات الطابع الشخصي، والتي تقوم على أساس التزام الدول الأطراف بوضع إطار قانوني يهدف إلى تعزيز الحقوق الأساسية والحريات العامة، ومكافحة الجرائم التي من شأنها انتهاك الخصوصية دون المساس بالحريات والحقوق الأساسية للأفراد؛ كما تناولت في المادة (9) مجال تطبيق الاتفاقية والإجراءات التي تقع ضمن نطاق أحكامها، كجمع أو معالجة أو أرسال أو تخزين أو استخدام البيانات ذات الطابع الشخصي من قبل الأشخاص الطبيعيين أو الدولة أو المجتمعات المحلية والهيئات الاعتبارية العامة أو الخاصة سواء كانت بصورة آلية أو غير آلية وضمن أراضي دول الإتحاد الإفريقي على ان تتصل هذه الإجراءات بالأمن العام والدفاع والبحث العلمي والملاحقة الجنائية أو أمن الدولة، وتضمنت المادة (10) الإجراءات الأولية لمعالجة البيانات ذات الطابع الشخصي والهدف من معالجتها، شريطة أن تكون منسجمة مع الهدف الذي جمعت من أجله، وأن تلتزم الجهة المعالجة بعدم كشفها لطرف ثالث، وعدم انتهاكها للحياة الخاصة أو للحريات الفردية، وأن تتم الإجراءات وفق الآليات التشريعية أو التنظيمية.

أما عن أحكام الإطار المؤسسي لحماية البيانات ذات الطابع الشخصي في المادتين (11،12)، فقد أشارت المادة (11) إلى أحكام وضع، تشكيل وتنظيم سلطات الحماية الوطنية للبيانات ذات الطابع الشخصي، والزمت الاتفاقية الدول الأطراف بإنشاء سلطة مسؤولة عن حماية البيانات ذات الطابع الشخصي تتمتع بسلطة إدارية مستقلة ومحايدة؛ كما ألزمتهم على تزويد سلطة الحماية الوطنية بالموارد البشرية والفنية والمالية اللازمة لإنجاز مهامها التي نصت عليها، ويقع على عاتق سلطة الحماية ضمان معالجة البيانات وفقاً لأحكام الاتفاقية، على أن يخضع أعضائها للسرية المهنية وفقاً للنصوص السارية في كل دولة طرف وأن يتمتعوا بالحصانة الكاملة فيما يخص الآراء التي يعبرون عنها عند ممارستهم لمهامهم، وحددت أحكام وواجبات وصلاحيات سلطات الحماية الوطنية في إداء مهامها بضمان معالجة البيانات ذات الطابع الشخصي، وفقاً لأحكام الاتفاقية في الدول الأطراف في الإتحاد الإفريقي في المادة (12)؛ كما وضعت الاتفاقية أحكام الالتزامات المتعلقة بالشروط التي تحكم معالجة البيانات ذات الطابع الشخصي فقد تناولت المادة (13) المبادئ الأساسية التي تحكم معالجة البيانات ذات الطابع الشخصي، والمتمثلة بمبدأ الموافقة والشرعية في معالجة البيانات ذات الطابع الشخصي، ومبدأ القانونية والنزاهة في معالجة البيانات ذات الطابع الشخصي، وبمقتضاه يجب أن يتم جمع وتسجيل ومعالجة وتخزين ونقل البيانات ذات الطابع الشخصي بطريقة قانونية ونزيهة وخالية من الاحتيال، ومبدأ القصد، الصلة والتخزين للبيانات ذات الطابع الشخصي للمعالجة، وبمقتضاه يجب أن يكون جمع البيانات من أجل أهداف محددة، واضحة وشرعية، ويجب أن تكون

كافية وذات صلة وغير مفرطة فيما يتعلق بالأهداف التي من أجلها تم جمعها ومن ثم معالجتها؛ كما يجب حفظ البيانات لمدة لا تتجاوز المدة المطلوبة لتحقيق الأهداف التي جمعت من أجلها ومن ثم القيام بمعالجتها، ولايجوز بعد الفترة المذكورة الاحتفاظ بالبيانات إلا لتلبية االحتياجات محددة لمعالجة البيانات لأغراض تأريخية أو إحصائية أو بحثية وفقاً للأحكام القانونية.

هذا وقد نصت المادة (14) على المبادئ المتعلقة بمعالجة البيانات الحساسة، والتي تتعهد الدول بتطبيقها بموجب هذه المادة وهي: حظر أي جمع أو معالجة للبيانات التي تكشف الأصل،(العرق الإثني أو الإقليمي)، البنوة الأبوية، الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو الانتماء النقابي، الحياة الجنسية والمعلومات الوراثية أو، بشكل عام، بيانات عن الحالة الصحية للشخص المعني، مع مراعاة بعض الاستثناءات المنصوص عليها في الاتفاقية، والتي لا يحول تطبيق أحكامها من تطبيق التشريعات الوطنية فيما يتعلق بوسائل الإعلام المطبوعة أو المسموعة أو المرئية فضلا عن أحكام القانون الجنائي التي تنص على شروط حق الرد والتي تمنع وتحد وتعوض على وعند الضرورة قمع االنتهاكات الخصوصية الإضرار التي لحقت بسمعة الفرد؛ كما لا يجوز للمسؤول عن معالجة البيانات، نقل البيانات ذات الطابع الشخصي إلى دولة ليست عضواً في الإتحاد الإفريقي مالم تضمن هذه الدولة مستوى كافياً من حماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص الذين تخضع بياناتهم للجمع أو المعالجة، اما فيما يتعلق بترابط ملفات البيانات ذات الطابع الشخصي فقد نصت الاتفاقية في المادة (15)، على وجوب أن يُمكن ترابط ملفات البيانات من تحقيق أهداف قانونية وتشريعية تمثل مصلحة مشروعة لموظفي معالجة البيانات، ويجب أن تخضع لتدابير أمنية مناسبة وأن تأخذ بنظر الاعتبار مبدأ الصلة للبيانات التي سيتم ترابطها.

أمّا عن الأحكام المتعلقة بحقوق الشخص موضوع البيانات ذات الطابع الشخصي في المواد (16، 17، 18، 19) فقد تناولت المادة (16) حق الشخص موضوع البيانات في الاطلاع على سبب، وآلية، وهوية الجهة المسؤولة عن جمع معالجة البيانات، وفئات البيانات المطلوبة، ومدة الاحتفاظ بها، وغيرها من المعلومات التي تكون من الأهمية ان يطلع عليها الشخص موضوع البيانات المطلوب جمعها ومعالجتها.

أمّا فيما يتعلق بأحكام الحق في الوصول إلى المعلومات؛ حيث أشارت المادة (17) إلى حق الشخص الطبيعي موضوع جمع ومعالجة البيانات الشخصية إلى الطلب من الموظف القائم بالإجراءات تزويده بمعلومات تمكنه من تقييم أو الاعتراض على إجراءات المعالجة، تأكيد أو عدم تأكيد معالجة البيانات الخاصة به، معلومات عن الغرض من المعالجة، فئات البيانات الشخصية المعنية، المستفيدين، المتلقين الذين تم الإفصاح لهم عن البيانات.

هذا وفي حق الاعتراض تناولت المادة (18) هذا الموضوع؛ حيث أشارت إلى حق أي شخص طبيعي في الاعتراض، لأسباب مشروعة، على معالجة البيانات ذات الطابع الشخصي الخاصة به، وله الحق في إبلاغه قبل كشف بياناته إلى طرف ثالث أو استخدامها، وان يعرض عليه صراحةً حق الاعتراض، مجاناً، على هذه الإفصاحات والاستخدامات، أما ما يتعلق بحق التصحيح أو الحذف، فقد أجازت الاتفاقية للشخص الطبيعي الطلب من مسؤول معالجة البيانات تصحيح أو إكمال أو تحديث أو حجب أو حذف، حسب الاقتضاء، للبيانات ذات الطابع الشخصي الخاصة به.

وتناولت الاتفاقية كذلك أحكام التزامات المسؤول عن معالجة البيانات ذات الطابع الشخصي في المواد (20، 21، 22، 23) وهي:

1. التزامات السرية، والتي توجب وتلزم أن تكون معالجة البيانات حصرياً بواسطة أشخاص يعملون تحت سلطة المسؤول عن معالجة البيانات وبموجب تعليمات صادرة منه.
2. التزامات التأمين، والتي تلزم مسؤول المعالجة اتخاذ جميع الاحتياطات اللازمة، بناء على طبيعة البيانات، لاسيما، منع تغيير هذه البيانات أو إتلافها أو الاطلاع عليها من قبل أطراف ثالثة غير مرخص لها بذلك.
3. التزامات التخزين؛ حيث يجب حفظ البيانات ذات الطابع الشخصي لمدة لا تتجاوز المدة الضرورية لتحقيق الهدف من جمعها ومعالجتها.
4. ضمان التزامات الاستدامة فقد ألزمت الاتفاقية المسؤول عن الجمع والمعالجة اتخاذ كافة التدابير اللازمة لضمان ان البيانات ذات الطابع الشخصي يمكن استخدامها بغض النظر عن الجهاز التقني المستخدم في العملية؛ كما عليه أن يضمن ألّا تشكل التطورات التقنية عائقاً أمام هذا الاستعمال.

أما فيما يتعلق بتعزيز الأمن الإلكتروني ومكافحة الجريمة الإلكترونية من خلال تدابير الأمن الإلكتروني الواجب اتخاذها على المستوى الوطني، في المواد (24، 25، 26، 27، 28)، ففي إطار تأمين الفضاء الإلكتروني الوطني بمقتضى السياسة الوطنية والاستراتيجية الوطنية، فقد ألزمت المادة (24) كل دولة طرف بوضع سياسة وطنية لأمن الفضاء الإلكتروني والتي تعترف بأهمية البنية التحتية الأساسية للمعلومات بالنسبة للدولة، وتحديد المخاطر التي تواجهها باستخدام نهج لمكافحة كافة المخاطر، وأن توضح طريقة تنفيذ أهداف هذه السياسة؛ كما والزمتهم على اعتماد إستراتيجيات مناسبة وكافية لتنفيذ سياسة وطنية للأمن الفضائي السيبراني لاسيما في مجال الإصلاح التشريعي والتنمية ورفع مستوى التوعية وبناء القدرات، والشراكة بين القطاعين العام والخاص، والتعاون الدولي على سبيل المثال لا الحصر.

المطلب الثاني: أحكام اتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014

هناك مجموعة تدابير وإجراءات تناولتها اتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014 تتعلق بإجراءات النظام الوطني لتأمين الفضاء الإلكتروني والهياكل الوطنية لرصد تأمين الفضاء الإلكتروني، والتعاون الدولي والجرائم الخاصة بتكنولوجيا المعلومات والاتصالات، وسوف نتناولها في فرعين خصصنا الفرع الأول للتدابير والإجراءات القانونية للنظام الوطني لتأمين الفضاء الإلكتروني والهياكل الوطنية لرصد تأمين الفضاء الإلكتروني، وبيّنا في الفرع الثاني أحكام تتعلق بالتعاون الدولي والحد من الجرائم الخاصة بتكنولوجيا المعلومات والاتصالات.

الفرع الأول: التدابير والإجراءات القانونية للنظام الوطني لتأمين الفضاء الإلكتروني والهياكل الوطنية لرصد تأمين الفضاء الإلكتروني

اولاً: التدابير القانونية التي تناولتها اتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي:

هذه التدابير تناولتها المادة (25) من الاتفاقية ويمكن لنا أن نجملها بالآتي:

أ-**تشريعات مكافحة جريمة الفضاء الإلكتروني:** حيث تلتزم كل دولة طرف باعتماد تدابير تشريعية و/أو تنظيمية تراها فعالة لتجريم كافة الأعمال الجنائية التي تؤثر على سرية ونزاهة وتوافر وبقاء أنظمة تكنولوجيا المعلومات والاتصالات والبيانات التي تعالجها والبنية التحتية للشبكات الأساسية، فضلاً عن اتخاذ تدابير إجرائية فعالة لمتابعة وملاحقة المجرمين.

ب-**السلطات التنظيمية الوطنية:** حيث تلتزم كل دولة طرف باعتماد تدابير تشريعية و/أو تنظيمية تراها ضرورية لإسناد مسؤولية محددة إلى المؤسسات سواء المنشأة حديثاً أو القائمة سابقاً، وكذلك الموظفين لها بغية منحهم سلطة وأهلية قانونية للتصرف في جميع جوانب تطبيق الأمن الفضائي الإلكتروني، على سبيل المثال لا الحصر، الاستجابة لحوادث أمن الفضاء الإلكتروني والتنسيق والتعاون في مجال العدالة التصالحية، تحقيقات الطب الشرعي والنيابة العامة، ...الخ.

ت-**حقوق المواطنين:** من خلال اعتماد تدابير قانونية في مجال الأمن الفضائي الإلكتروني، ووضع أطر لتنفيذها؛ حيث تلتزم كل دولة طرف بضمان ان لا تعيق هذه الإجراءات حقوق المواطنين التي يضمنها الدستور الوطني والقوانين الداخلية، والحقوق التي تحميها الاتفاقيات الدولية، لاسيما الميثاق

الإفريقي لحقوق الإنسان والشعوب، وكذلك الحقوق الأساسية مثل الحق في حرية التعبير واحترام الخصوصية والحق في محاكمة عادلة.

ث–حماية البنية التحتية الحيوية: عبر إلزام كل دولة طرف باعتماد إجراءات تشريعية و/أو تنظيمية تراها ضرورية لتحديد القطاعات الحساسة لأمنها الوطني وازدهار اقتصادها، بالإضافة إلى أنظمة تكنولوجيا المعلومات والاتصالات المصممة للعمل في هذه القطاعات الحساسة باعتبارها بنية تحتية حيوية للمعلومات، مع القيام بفرض عقوبات أكثر صرامة إزاء الأعمال الإجرامية التي تستهدف هذه القطاعات واتخاذ إجراءات وتدابير لحمايتها.

ثانياً: إجراءات النظام الوطني لتأمين الفضاء الإلكتروني:

أما فيما يتعلق بإجراءات النظام الوطني لتأمين الفضاء الإلكتروني، فقد أشارت أحكام المادة (26) إلى العديد من الإجراءات منها:

أ– ثقافة تأمين الفضاء الإلكتروني: تلتزم كل دولة طرف بتشجيع ثقافة أمن الفضاء الإلكتروني بين أصحاب المصلحة، الحكومات والشركات والمجتمع المدني، والتي تطور وتملك وتدير وتشغل وتستخدم نظم المعلومات والشبكات، على ان تركز هذه الثقافة على الأمن عند القيام بتطوير أنظمة وشبكات المعلومات؛ كما وتلتزم الدول الأطراف في إطار الترويج لثقافة أمن الفضاء الإلكتروني ببعض الإجراءات المتمثلة بإنشاء خطة تأمين فضاء إلكتروني للأنظمة التي تديرها حكومات هذه الدول، إعداد وتنفيذ برامج ومبادرات للتوعية بالأمن لمستخدمي الأنظمة والشبكات، التشجيع على تطوير ثقافة أمن الفضاء الإلكتروني، وتعزيز مشاركة المجتمع المدني.

ب– دور الحكومات: تلتزم كل دولة طرف بلعب دور قيادي في تطوير ثقافة الأمن السيبراني داخل حدودها، من خلال التوعية والتعليم والتدريب ونشر المعلومات للجمهور.

ت– الشراكة بين القطاعين العام والخاص: تلتزم كل دولة عضو بتطوير هذه الشراكة كنموذج لإشراك الصناعة والمجتمع المدني والمجتمع الأكاديمي في تعزيز الأمن السيبراني.

ث– التعليم والتدريب: تلتزم كل دولة عضو باتخاذ التدابير اللازمة لبناء القدرات بهدف توفير التدريب الذي يغطي كل مجالات أمن الفضاء السيبراني، وتشجيع التعليم الفني للمهنيين العاملين في مجال تكنولوجيا المعلومات.

ثالثاً: إجراءات والهياكل الوطنية لرصد تأمين الفضاء الإلكتروني:

وفيما يتعلق بإجراءات الهياكل الوطنية لرصد تأمين الفضاء الإلكتروني، فقد تناولت أحكام المادة (27) العديد من الإجراءات منها:

أ- **حوكمة أمن الفضاء الإلكتروني:** تقوم كل دولة طرف باتخاذ الإجراءات الكفيلة لإنشاء آلية مؤسسية ملاءمة مسؤولة عن حوكمة الفضاء الإلكتروني، على أن تكون الحوكمة وفق إطار وطني قادر على مواجهة التحديات ومعالجة جميع القضايا التي تتعلق بأمن المعلومات على المستوى الوطني وفي أكبر نطاق ممكن من مجالات أمن الفضاء السيبراني.

ب-**الإطار المؤسسي:** بمقتضاه تلتزم كل دولة طرف باعتماد التدابير التي تراها ضرورية لإنشاء المؤسسات المناسبة لمكافحة الجريمة الإلكترونية وضمان الرصد والاستجابة للحوادث والتنبيهات والتنسيق الوطني العابر للحدود، من مشاكل أمن الفضاء السيبراني وكذلك التعاون الدولي.

الفرع الثاني: أحكام تتعلق بالتعاون الدولي والحد من الجرائم الخاصة بتكنولوجيا المعلومات والاتصالات

أولاً: أحكام تتعلق بالتعاون الدولي:

وفي ضوء ما يتعلق بالتعاون الدولي فقد نصت الاتفاقية في المادة (28) على العديد من التدابير التي تتعلق بالتعاون الدولي، والتي تلزم الدول الأطراف على ضمان أن التدابير التشريعية و/أو التنظيمية المعتمدة لمكافحة الجرائم الإلكترونية من شأنها أن تعزز إمكانية الموائمة الإقليمية لهذه التدابير وأن تحترم مبدأ المسؤولية الجنائية المزدوجة؛ كما تلزم الدول الأطراف التي ليس لديها اتفاقيات للمساعدة المتبادلة في مجال الجرائم الإلكترونية بالتشجيع على توقيع اتفاقيات للمساعدة القانونية فيما بينها وفقاً لمبدأ المسؤولية الجنائية المزدوجة مع القيام في ذات الوقت بتعزيز تبادل المعلومات، وتشجيع إنشاء مؤسسات لتبادل المعلومات بشأن تهديدات الفضاء الإلكتروني مثل فرق الاستجابة لطوارئ الكومبيوتر، والاستفادة من وسائل التعاون الدولي القائمة بهدف الاستجابة للتهديدات الإلكترونية وتحسين أمن الفضاء الإلكتروني.

ومما تجدر الإشارة إليه إن الاختلاف الرئيسي بين اتفاقية الإتحاد الإفريقي وغيرها من الاتفاقيات الإقليمية المماثلة مثل اتفاقية مجلس أوربا بشأن الجرائم الإلكترونية، في إن مشروع اتفاقية الإتحاد الإفريقي في حال عدم وجود أي صك يتعلق بالتعاون الدولي، لا يمكن استخدامه لهذا الغرض، فقد عبرت المادة (28) أنفة الذكر على هذا المفهوم المختلف حيث يتعين بموجب المادة أعلاه ان تلتزم الدول الأطراف باتخاذ التدابير التي تراها ضرورية لتعزيز تبادل المعلومات وتقاسم البيانات على نحو سريع وعاجل ومتبادل من قبل مؤسسات الدول الأعضاء المسؤولة عن تطبيق

القانون والمؤسسات المماثلة في الدول الأعضاء الأخرى المسؤولة عن تطبيق القانون في الإقليم على أساس ثنائي أو متعدد الأطراف[1].

ثانياً: الحد من الجرائم الخاصة بتكنولوجيا المعلومات والاتصالات:

أ- الجرائم الخاصة بتكنولوجيا المعلومات والاتصالات:

أشارت المادة (29) إلى الجرائم الخاصة بتكنولوجيا المعلومات والاتصالات، والتي تتضمن" جرائم النفاذ أو محاولة النفاذ غير المشروع إلى الأنظمة الحاسوبية، والبقاء أو محاولة البقاء عن طريق الاحتيال في كل أو جزء من النظام المعلوماتي، والتداخل غير القانوني على النظام، إدخال أو محاولة إدخال بيانات عن طريق الاحتيال في نظام الحاسوب، والاعتراض غير القانوني للبيانات، والتداخل غير القانوني على البيانات"؛ كما تجدر الإشارة إلى إن المادة (29) تناولت مفهوماً جديداً وليس حكماً قانونياً جنائياً ولم يسبق للاتفاقيات أو الصكوك الإقليمية الأخرى أن تطرقت له، وهو إلزام الأطراف على تبني لوائح ونظم من شأنها أن تلزم دوائر الأعمال التجارية على إخضاع منتجاتها لاختبار مواطن الضعف المكتشفة في المنتجات؛ كما تناولت ذات المادة تجريم إنتاج وبيع وحيازة أو نشر أو عرض أو التنازل أو تقديم المعدات المتاحة للكومبيوتر أو برنامج أو أي جهاز أو بيانات أو توليد أو إنتاج كلمة السر أو رمز وصول مماثل للبيانات الإلكترونية، وتكون مصممة خصيصاً أو مكيفة لارتكاب الجرائم بصورة غير قانونية، كذلك تجريم الخروقات على البيانات المحوسبة، والنشاطات الإجرامية ذات الصلة بالمحتوى غير القانوني لاسيما إنتاج المواد الإباحية التي يستغل فيها الأطفال ونشرها والحصول على هذه المواد وتداولها وتملكها وتيسير نفاذ القصر إلى هذه المواد الإباحية، وجرائم نشر مواد تنطوي على العنصرية وكره الأجانب والهجمات العنصرية المرتكبة من خلال أنظمة حاسوبية، وجرائم الإنكار المتعمد أو الموافقة على تبرير الأفعال التي تعتبر إبادة جماعية أو جرائم ضد الإنسانية، وتناولت كذلك الجرائم المتعلقة بإجراء تأمين الرسائل الإلكترونية والتزام الدول باتخاذ ما يلزم من تدابير تشريعية و/ أو تنظيمية لضمان مقبولية الأدلة الرقمية في القضايا الجنائية.

ب- عملت الاتفاقية على موائمة جرائم تقليدية معينة إلى تكنولوجيا المعلومات والاتصالات:

لقد عملت الاتفاقية على موائمة جرائم تقليدية معينة إلى تكنولوجيا المعلومات والاتصالات، فقد أشارت في المادة (30) إلى جرائم الممتلكات وألزمت الدول الأطراف على اتخاذ التدابير التشريعية والتنظيمية لتجريم انتهاك الممتلكات كالسرقة والاحتيال وحيازة البضائع المسروقة وإساءة استخدام الثقة وابتزاز الأموال والإرهاب وغسل الأموال التي ترتكب بواسطة وسائل الاتصال الرقمية، وكذلك

(1) For more information, see: Alisdair A. Gillespie, Cybercrime: Key Issues and Debates, Routledge, New York, USA, 2016, P.262.

الأفعال التي تؤثر في سرية أنظمة تكنولوجيا المعلومات والاتصالات وما يتصل بها من شبكات البنية التحتية للدفاع الوطني وسلامتها وتوفرها واستخدامها فضلاً عن التدابير الإجرائية التي تتعلق بمعاقبة الجناة وملاحقتهم قضائياً؛ كما وتناولت في ذات المادة المسؤولية الجنائية للأشخاص الاعتباريين من خلال إلزام الدول الأطراف على اتخاذ التدابير التشريعية اللازمة لضمان أن تتحمل الشخصيات الاعتبارية غير الدولة، المسؤولية الجنائية عن الجرائم المنصوص عليها في الاتفاقية على أن لا تستبعد مسؤولية الأشخاص الطبيعيين كونهم مرتكبي لهذه الجرائم أو شركاء فيها.

الخاتمة:

بعد الانتهاء من هذا الجهد المتواضع توصلنا إلى مجموعة من النتائج والتوصيات أهمها:

اولاً: النتائج:

1- أنّ الدول العربية دأبت إلى تكثيف جهودها من أجل الحد من الجرائم الإلكترونية لما ينطوي على هذه الجرائم من مخاطر جمّة تلحق بالمؤسسات والأفراد خسائر باهظة، باعتبارها تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة (البيانات والمعلومات والبرامج في كل أنواعها).

2- تهدف الاتفاقية إلى تعزيز التعاون بين الدول فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها وأفرادها، وتتكون هذه الاتفاقية من (43) مادة، منها (21) مادة في باب التجريم، و(8) مواد إجرائية تتعلق بحقوق السلطات وجمع المعلومات وتتبع المستخدمين، وضبط المواد المخزنة على الحواسيب الشخصية والأجهزة التقنية، ويتكون الفصل الرابع من (14) مادة تنظم التعاون بين الدول الأعضاء في تبادل معلومات المستخدمين؛ حيث يكون نطاق سريان هذه الاتفاقية على المستوى الإقليمي.

3- تكللت جهود الإتحاد الإفريقي منذ بدايتها من خلال المؤتمر الاستثنائي الذي عقد في جوهانسبرغ جنوب أفريقيا سنة 2009، لوزراء الإتحاد الإفريقي للقطاعات المتعلقة بالاتصالات وتكنولوجيا المعلومات للبلدان الإفريقية، نوقشت العديد من القضايا المتعلقة بتنامي الاستخدام المتزايد لتكنولوجيا المعلومات والاتصالات وأثر استخدامها السيئ على الأمن السيبراني للبلدان الإفريقية، وتقرر على أثر هذه المناقشات أن تضع مفوضية الإتحاد الإفريقي وبمشاركة لجنة الأمم المتحدة الاقتصادية لأفريقيا، إطاراً قانونياً للبلدان الإفريقية يعالج كافة المسائل المتعلقة بحماية البيانات، والأمن السيبراني، والتجارة الإلكترونية.

ثانياً: التوصيات:

1- ضرورة توحيد الجهود الدولية والإقليمية وعلى مستوى دول العالم لأن الجريمة الإلكترونية ليس لها حدود بل هي تطول كل دول العالم، بغض النظر عن بعدها وقربها حين ارتكابها.

2- ضرورة نشر الوعي بين أفراد المجتمع من خلال إقامة الدورات والندوات والمؤتمرات ووسائل الإعلام بخطورة الجرائم الإلكترونية، وإعطاء دور في هذا المجال للعلماء ورجال الدين والمختصين.

3- ضرورة تأهيل وتنمية رجال الضبطية القضائية على الأساليب التقنية والحديثة المستخدمة في هذه الجرائم، وتدريبهم على التدابير الواجب اتخاذها في هذا المجال، للإسراع في الكشف عن الجريمة وتعقبها، من أجل عدم ضياع الدليل إعطاء الضبطية القضائية المزيد من الوسائل التقنية المتطورة.

قائمة المصادر والمراجع:

أولاً: الكتب القانونية:

1- المستشار أيمن بن ناصر بم حمد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، دراسة مقارنة، ط1، مكتبة القانون والاقتصاد، الرياض، 1436هـ-2015م.

2- بلال محمود عبد الله، حق المؤلف في القوانين العربية، ط1، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، بيروت، 2018م.

3- خالد حسن أحمد لطفي، الإرهاب الإلكتروني، آفة العصر الحديث والآليات القانونية للمواجهة، دار الفكر الجامعي، الإسكندرية، 2018م.

4- رامي متولّي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، ط1، دار النهضة العربية، القاهرة، 2011م.

5- سليمان أحمد فضل، المواجهة التشريعية الناشئة عن استخدام معلومات الإنترنت، دار النهضة العربية، القاهرة، 2007م.

6- عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، أكاديمية نايف العربية للعلوم الأمنية-الرياض، 2009م.

7- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الاسكندرية، 2006م.

8- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم المعلوماتية)، منشورات الحلبي الحقوقية، بيروت، 2007م.

9- علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية للنشر والتوزيع، عمّان، 2018م.

10- عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ط1، دار النهضة العربية، القاهرة، 2004م.

11- عمر سالم، الحماية الجنائية لبطاقات الوفاء، دار النهضة العربية، القاهرة، 1995م.
عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، ط1، دار الفكر الجامعي، الإسكندرية، 2008م.

12- فريد جبور، حماية المستهلك عبر الإنترنت ومكافحة الجريمة الإلكترونية، منشورات الحلبي الحقوقية، بيروت، 2008م.

13- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار العلم والثقافة للنشر والتوزيع، عمّان، 2005م.

14- ناظم محمد نوري الشمري، عبد الفتاح زهير العبد اللات، الصيرفة الإلكترونية، ط1، دار وائل للنشر، عمّان، 2008م.

15- نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، ط1، منشورات الحلبي الحقوقية، بيروت، 2005م.

16- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، 2008م.

17- وسيم حرب، كتاب برنامج تعزيز حكم القانون في بعض الدول العربية، مشروع تحديث النيابات العامة، كتاب أعمال الندوة حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 2007م.

18- ضرغام جابر عطوش، جريمة التجسس المعلوماتي (دراسة مقارنة)، ط1، المركز العربي للنشر والتوزيع، القاهرة، مكتبة دار السلام القانونية، النجف الأشرف، 2017م.

ثانياً: الرسائل العلمية:

1- إبراهيم بشار عواد، رسالة دكتوراه بعنوان (جريمة الاحتيال عبر شبكة المعلومات الدولية، دراسة مقارنة بين القانون الأردني والقانون المصري)، كلية الدراسات القانونية العليا، جامعة عمّان العربية، عمّان، 2009م.

2- صفاء كاظم غازي الجياشي، رسالة ماجستير بعنوان (جريمة قرصنة البريد)، كلية القانون، جامعة بابل، 2016م.

3- ملياني عبد الوهاب، رسالة دكتوراه بعنوان (أمن المعلومات في بيئة الأعمال الإلكترونية)، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبي بكر بلقايد – تلمسان، الجزائر، 2017م.

ثالثاً: المجلّات والدوريات العلمية:

1- سامر محمود دلالعة، بحث بعنوان (التدابير الدولية في مجال الإدارة الجماعية لحقوق المؤلف والحقوق المجاورة بين النظرية والتطبيق، دراسة مقارنة)، منشور في مجلة المنارة للبحوث والدراسات، المجلد الثالث عشر، العدد الثامن، جامعة آل البيت، عمّان، 2007م.

2- سليم بشير، بحث بعنوان (حل مشكلة تنازع الاختصاص الجنائي الدولي في مجال مكافحة جرائم التجارة الإلكترونية–وفقاً للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010م)، منشور بمجلة الحقوق والحريات، جامعة محمد خيضر –بسكرة، الجزائر، المجلد (5)، العدد (1)، السنة 2019م.

3- موفق علي عبيد وساهر ماضـي ناصر، بحث بعنوان (ماهية جريمة الاحتيال المعلوماتي)، منشور في مجلة جامعة تكريت للعلوم القانونية، السنة السابعة، العدد الخامس والعشرون، جمادي الآخرة/ 1435هـ–أذار/ 2015م.

رابعاً: المراجع الأجنبية:

1- Alisdair A. Gillespie, Cybercrime: Key Issues and Debates, Routledge, New York, USA, 2016.