الجريمةالالكترونية (السيبرانية) في القانون الدولي

ابراهيم احمد عبد السامرائي

قسم القانون، جامعة جيهان- اربيل، كردستان، العراق

المستخلص

تناول البحث الجريمة الالكترونية المعروفة بمصطلح (السيبرانية) لارتباطها بالفضاء وهو اوسع ميدان لارتكابها وتنفيذ اركانها، وغالبا ما تكون بين الدول او في داخل الدولة وبسبب اهميتها فقد عُرفت تعريفات متعددة وحُددت طبيعتها من انها جريمة عمدية تُرتكب لتحقيق اهداف ضارة بمصالح شخص او جهة معينة ، ولها خصائص تميزها عن الافعال الاخرى من حيث ارتكابها بواسطة الكومبيوتر ، وتناول ايضا انظمته او المعلومات التي يحتويها، او يستهدف شبكة الانترنيت والمواقع التي فيها، وعادة يساهم فيها اكثر من شخص او جهة، ولها انواع واشكال متعددة حسب الوسيلة المستخدمة او الاهداف المرجوة منها من سرقة بيانات او تعطيلها او تخريبها او تزويرها وغير ذلك. وبسب خطورتها فقد اهتمت بمواجهتها الدول والمنظمات الدولية وأُبرمت بشانها الاتفاقيات الدولية واصدرت الانظمة والتعليمات اللازمة لمنعها والحد من اضرارها ومساءلة مرتكبيها واهمها الاتفاقية الاوربية (بودابست) ونظام حماية البيانات الذي اصدرته ثم الاتفاقية العربية لحماية البيانات والاتفاقية الافريقية لحماية البيانات وارافق ذلك جهود الامم المتحدة لانشاء اتفاقية اممية شاملة لكل دول العالم.

الكلمات المفتاحية: الجريمة، السيبرانية، بودابست، اتفاقية، الجهود.

1. المقدمة

تشكل ثورة الاتصالات ابرز معالم المجتمع الدولي المعاصر، فقد اخترقت شبكة الانترنيت حدود الدول واصبح من المستحيل على دولة ان تراقب او تنظم او تضمن حقوق البيانات و بيانات مواطنيها لوحدها . وفي تصريح للامم المتحدة خلال هذا العام بان كل (36) ثانية ترتكب جريمة الكترونية، وان عدد المستخدمين للانترنيت وصل الى المليارات.

ففي عام 2005 حدث الهجوم الاستوني الالكتروني وخرب خلال ساعة واحدة الكومبيوترات في (178) دولة، وفي عام 2016 حدث هجوم (Dyn) في الولايات المتحدة الامريكية وخرب مراكز البيانات وانتقل الى اوربا، وفي عام 2017 حصل هجوم الفدية (Wannu Cry) واثر على (230000) كومبيوتر في اكثر من (150) دولة وتسبب في مشاكل مالية وتجارية وصحية كبيرة.

ولذلك فقد سعى المجتمع الدولي الى مواجهة الجريمة الالكترونية من خلال وضع قواعد وانظمة دولية تُسهل مراقبة وتنظيم ومحاسبة مرتكبي هذه الجريمة .

وقد تمكنت دول الاتحاد الاوربي من ابرام اتفاقية دولية انضمت اليها دول كثيرة من خارج الاتحاد الاوربي ، لتمثل قواعد دولية توفرالحماية والضمانة لمستخدمي الكومبيوتر وشبكة الانترنيت.

وفي الاتجاه نفسه سارت الدول العربية في ابرام اتفاقية بشأن الجريمة الالكترونية لكنها ما زالت غير نافذة حتى الآن.

واستطاعت الدول الافريقية ان تبرم اتفاقية قريبة من مستوى الاتفاقية الاوربية لمواجهة الجريمة الالكترونية.

كذلك فان الامم المتحدة قد بذلت جهودا كبيرة باتجاه ابرام اتفاقية اممية شاملة للتصدي للجريمة الالكترونية وما زالت تعمل في هذا الاتجاه.

1.1 أهداف البحث

يهدف البحث الاجابة على الاسئلة الآتية:

1. ما هي الجريمة الالكترونية ؟ وما هي طبيعتها؟ وما هي خصائصها؟ وكيفية المساهمة فيها؟ وما هي انواعها؟

مجلة جامعة جيهان- اربيل للعلوم الانسانية والاجتماعية
المجلد 6، العدد 2 (2022) .
أُستلم البحث في 28 حزيران 2022؛ قُبل في 8 اب 2022
ورقة بحث منتظمة: نُشرت في 15 اب 2022
البريد الإلكتروني للمؤلف : ibrahimahmed@gmail.com

2. ما هي الجهود الدولية لمواجهة الجريمة الالكترونية؟ وما هي اتفاقية بودابست ؟ وما هي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات؟
3. ما هي الاتفاقية الافريقية بشأن امن الفضاء الالكتروني وحماية البيانات؟
4. وما هي جهود الامم المتحدة ، من حيث تقرير الخبراء لعام 2019 ومن حيث لجنة الخبراء الحكومية الدولية لانشاء اتفاقية دولية لمكافحة الجريمة الالكترونية؟

1.2 مشكلة البحث

بذلت جهود كبيرة لمواجهة الجريمة الالكترونية وعقدت اتفاقيات دولية ورغم ذلك فان خطر هذه الجريمة ما زال قائما ، مما يتطلب بذل جهود نوعية وليست نمطية بحيث تكون الامم المتحدة هي المحور الاساسي في هذه الجهود وبحياديتها وقدرتها على التحشيد افضل مما تستطيعه اتفاقية بودابست التي تمحور عليها الدول الاوربية ، وضرورة مواكبة آخر التطورات حتى الان لانه موضوع متغير باستمرار ويحظى باهتمام كبير ، وباتجاه آخر تحاول المجموعة الاوربية ومعها الولايات المتحدة الامريكية الاستمرار بتطبيق الاتفاقية الاوربية على اكبر عدد من دول العالم وتعارض انشاء اتفاقية جديدة كالتي تسعى اليها الكثير من الدول من خلال الامم المتحدة.

1.3 طريقة البحث

مراجعة اهم الاتفاقيات الدولية المتعلقة بالجريمة الالكترونية والمقارنة بين المفاهيم الاساسية وانواع الجرائم الالكترونية وطبيعتها من اجل الوصول الى مفاهيم جامعة ومانعة وسهلة التطبيق ، اضافة الى التعليق على الموضوعات حسب اهميتها في مواجهة هذه الجريمة مما يعطي فكرة واضحة عن حجمها ومدى الحاجة الى تطويرها.

2. الجريمة الالكترونية (السيبرانية)

ينبغي الاحاطة بمفهوم واضح ومحدد للجريمة الالكترونية التي يطلق عليها عالميا بالسيبرانية لان مجال ارتكابها هو انتقال الالكترون في الفضاء سواء داخل الدولة او بين الدول الاخرى . (Eyan, 2011)

كما ان من الضروري تحديد طبيعتها الوطنية والدولية وفيما اذا كانت عمدية ام غير ذلك وعلاقتها بالضرر الذي ينجم عنها . وانها ذات خصائص تميزها عن الجرائم الاخرى من حيث استعمال الكومبيوتر والاجهزة الالكترونية وشبكاتها وطبيعة الانشطة التي تعتمد لتنفيذها .

اضافة الى معرفة انواع هذه الجريمة من انها متعددة وذات صور واشكال تتناسب مع الوسائل المستخدمة والاهداف المرجوة منها. هذا ما سيتم بحثه في الفقرات اللاحقة.

2.1 تعريف الجريمة الاليكترونية

تعددت تعريفات الجريمة الالكترونية بسبب تزايد الاهتمام الدولي بها واعتمادها على اسس مختلفة للتعريف حسب تباين الفقه القانوني لكل دولة. وسنركز على اهم التعريفات .

فتعرف بانها التخريب او التدخل الدولي ضد الانظمة الالكترونية ويمكن ان يؤدي للموت او الاذى لشخص او لاشخاص ويتسبب بضرر جسيم للملكية الطبيعية، او خلل في العلاقات المدنية، او ضرر اقتصادي (Mourlam, 2016)

وينتقد هذا التعريف بانه يحصرالافعال المكونة للجريمة في النطاق الدولي فحسب ، بينما يمكن ان تكون ايضا صادرة من جهة وطنية .

وتعرف بانها اعمال تتخذ من خلال شبكة الانترنيت تتضمن الغاء ، ازالة ، تخريب للمعلومات في الكومبيوتر او في شبكة الكومبيوترات او في كليهما (الحوامدة ,2017)

في هذين التعريفين تم التركيز على امن الكومبيوتر او شبكته ولم تهتم بالتجسس والاستغلال الالكتروني اللذين لهما مساحة واسعة من الجريمة الالكترونية .

وتعرف ايضا بانها كل فعل غير مشروع يستهدف تغيير البيانات او المعلومات بالحذف او الاضافة او المعالجة او السرقة او تحوير المعلومات او تعديلها لغايات غير مشروعة بواسطة الكومبيوتر او اية وسيلة تكنولوجية (Giles, 2018).

هذا التعريف يشمل كل الافعال الضارة بما فيها التجسس او الاستغلال الالكتروني تحت مفهوم الفعل غير المشروع الموصوف بالامثلة المتعددة الشاملة لكل انواع الضرر الذي يمكن ان تسببه الجريمة الالكترونية.

بتقديرنا ان التعريف الاخير هو تعريف شامل لكل الجرائم الالكترونية لانه استخدم عبارتي (الفعل غير المشروع) و(الغايات غير المشروعة) اي انه سيعتمد على ما سيشرع بخصوص هذه الجريمة دوليا ووطنيا من جهة ، وسيشمل اي فعل يؤدي الى غاية غير مشروعة من جهة اخرى.

2.2 طبيعة الجريمة الالكترونية

للجريمة الالكترونية طبيعة خاصة ، فهي غالبا تعتمد على انشطة جنائية داخل الدولة وانشطة اخرى في دولة او دول اخرى ، او قد تكون داخل الدولة فحسب او تاتي من دولة او دول اخرى وتستهدف دولة او دول معينة . (Daskal, 2015).

وبذلك فان القانون الوطني سوف يتعذر عليه مواجهة هذه الجريمة لوحده ، بل ينبغي ان يتضافر المجتمع الدولي من خلال القانون الدولي ،)Mourlam,2016 (وحسب نوع النشاط فيما اذا كان داخلي ام خارجي تتحدد نوع المسؤولية التي تترتب على هذه الجريمة .

كما ان هذه الجريمة ذات طبيعة عمدية سواء كان القصد مباشر او احتمالي او حصول خطأ او غلط ما دام قد تسبب بضرر على استعمال الكومبيوتر وبياناته او على شبكة الانترنيت (Giles, 2017) اي ان الصفة العمدية في هذه الجريمة قد شملت الخطأ او الغلط المجرد على خلاف الفقه الجنائي الذي يشترط ان يكون الخطأ جسيما او ان يكون الغلط كبيرا حتى يعتبر ذو صفة عمدية .

وهي بهذا الوصف انتهاك للقانون الوطني او الدولي او لكليهما ، اي انها يمكن ان تكون جريمة استنادا لاحد او كلا القانونين المذكورين بوصفها فعل غير مشروع يؤدي فيه جهاز الكومبيوتر او الجهاز الالكتروني دورا مهما لاتمام النشاط غير المشروع ، ويكون هذا النشاط مؤثر ويؤدي الى ارتكاب الجريمة (عبدالباقي، 2018).

ولذلك ينبغي توصيف الانشطة (الافعال) الجنائية لهذه الجريمة ، وهذا ما سيتم توضيحه لاحقا تحت عنوان خصائص الجريمة الالكترونية.

2.3 خصائص الجريمة الالكترونية

يمكن تحديد خصائص الجريمة الالكترونية بما ياتي:

1. الدخول غير القانوني لانظمة الكومبيوتر وللاجهزة الالكترونية الاخرى ، اي ان الدخول يشمل الموبايل او الهواتف الذكية او الآيباد او اية وسيلة الكترونية لنقل المعلومات.ويقصد بالدخول غير القانوني استنادا للتشريعات الوطنية او الدولية وفقا لنوع الدخول فيما اذا كان داخل دولة معينة او يتعداها الى دولة او دول اخرى وهو الغالب. ويتضمن الدخول غير القانوني تهديد خطير واعتداء على انظمة الكومبيوتر وبياناته وبطريقة تطفلية (غير مسموحة) وقد يكون كليا او على جزء من نظام الكومبيوتر (Carlin, 2016) ويترتب على الدخول اعتراض البيانات او التشويش عليها او التسبب بسوء استعمال الاجهزة او تغييرها او الغائها ..الخ .
2. عابرة للحدود ، وهذه الصفة غالبة للجرائم الالكترونية ، فهي تتجاوز حدود الدولة الواحدة ، وعادة تشمل كل الدول . ويؤدي ذلك الى الحاجة للتعاون الدولي من خلال الاتفاقيات الدولية من اجل تحديد المسؤولية واتخاذ الاجراءات القانونية اللازمة .(الحوامدة، 2017)
3. صعوبة اثباتها ، ان وسيلة ارتكابها ليست مادية وتسمى بالجريمة الناعمة ، فهي تعتمد على انشطة الكترونية يمكن الغائها او تغييرها ، وليس سهلا اثبات مصدرها الا من قبل متخصصين ، وتقتضي اجراءات محاكمتها لقضاة مؤهلين علميا وتقنيا في هذا النوع من الجرائم .(العدواني، 2016)

ان الخصائص اعلاه موضوع منفصل عن انواع الجرائم الالكترونية الذي سياتي لاحقا وتشمل هذه الخصائص كل انواع الجرائم الالكترونية.

2.4 المساهمة في الجريمة الالكترونية

تساهم الدول في الكثير من الانشطة الالكترونية باستهداف مصالح جهة خارجية ، وهذا ما يجعل هذه الانشطة تخضع للقانون الدولي لانها ذات آثار على سلامة المجتمع الدولي (Benvenisti, 2014) قيام الدولة بالفعل الذي تحققت به الجريمة صورة للمساهمة الاصلية (فاعل اصلي) في الجريمة الالكترونية.

وفي قضايا دولية مشهورة تعرضت الدولة للمساءلة الدولية بمجرد علمها بوجود النشاط الاجرامي ، او انها لم تتخذ الاجراءات المناسبة لمنعها .(Corfu Case,1949) فالمساهمة كانت غير مباشرة في هذه القضايا.

اما اذا ثبت علاقة الدولة بالانشطة الاجرامية فانها ستتحمل المسؤولية مباشرة بوصفها مساهمة اصلية في الجريمة . (Libya Case, 1986).

وينطبق ما تقدم على الجريمة الالكترونية فتكون الدولة مساهمة اصلية اذا تمت الجريمة بتوجيه منها ، وتكون مساهمة تبعية اذا كانت تعلم بالجريمة او لم تتخذ الاجراءات المناسبة لمنعها . (Mourlam, 2016).

ويذهب البعض الى التمييز بين السيطرة الفعالة للدولة والسيطرة العملية ، ففي قضية نيكاراغوا مع الولايات المتحدة عام 1986 اعتمدت محكمة العدل الدولية على السيطرة الفعالة للدولة حتى تكون مساهمة اصلية في الجريمة . (USA-Nicaragua Case, 1986).

اما اذا كانت الدولة ليست فاعل اصلي في الجريمة وفشلت في اتخاذ الاجراءات المناسبة فانها تكون مساهمة تبعية (شريك) لان الدولة لها السيطرة العملية على ما يحصل فيها (Tadic Case, 1996) ان مسؤولية الدولة التبعية قد تم اقرارها منذ عام 1949 في قضية (Corfu Canal).

وبلا ريب فان موضوع المساهمة في الجرائم الالكترونية عابرة للحدود معقدة جدا ، لان الانشطة تجري عبر شبكة الكومبيوترات من افراد او جهات لا يرتبط معظمهم بالدولة التي ليست لها سيطرة او علم بأكثرها ، واذا كانت للدولة علاقة بهذه الانشطة فان اثباتها ليست عملية سهلة . (Carlin, 2016)

ان الانشطة الاجرامية الالكترونية ما زالت تشكل صعوبات كبيرة للمحققين والمختصين في مجال العدالة الجنائية وبالاخص في قضايا الاحتيال او الارهاب او الانتهاك والاستغلال الجنسي للاطفال او السرقة من خلال استخدام شبكات خفية ليس من السهل الوصول اليها كما في قضايا التخريب لانظمة الكومبيوتر (الفيروسات) . (UNODC, 2019). وقد تطور الفقه الجنائي في التمييز بين مسؤولية الدولة جنائيا والمسؤولية الجنائية للافراد وللقضاء الدولي احكاما كثيرة لكل نوع من هاتين المسؤوليتان وهذا موضوع خارج اختصاص البحث .

2.5 انواع الجرائم الالكترونية

جرائم الكومبيوتر، تشمل مكونات الكومبيوتر المادية (وحدات ادخال واخراج وتخزين مرن وصلب والشاشة والطابعة). ومكونات معنوية (بيانات ، معلومات مخزنة في الكومبيوتر) تتسبب هذه الجرائم بالضرر على هذه المكونات ويمكن ان تدمرها جزئيا او كليا وقد تنتقل الى كومبيوترات اخرى . (Giles, 2018)

جرائم شبكة المعلومات، وهي افعال غير قانونية تستهدف المواقع الالكترونية بقصد تعطيلها او التشويش عليها او تعديلها او الدخول الى مواقع خاصة . وتستخدم عناوين غير حقيقية للدخول الى الشبكة ، ويتم نقل الفيروسات وارسال الرسائل المؤذية وترويج اشياء غير مشروعة . (العدواني، 2016).

جرائم على البيانات والمعلومات، وهي افعال غير قانونية (دخول او اعتراض) تستهدف وثيقة او نص موجود في شبكة الكومبيوترات بقصد سرقتها او تعديلها او اتلافها او نشرها . ومن امثلتها انتهاك الملكية الفكرية للبرامج او الانتاج الفني او الادبي او العلمي . وبامكان المتطفلين المراقبة والتنصت على الاتصالات الالكترونية . ويوجد الآن مكتبات الكترونية هائلة في الدول المتقدمة تتضمن البيانات والنصوص التي تم اعتراضها وتسجيلها في كل انحاء العالم . (Dine, 2020).

جرائم تحصل بواسطة الكومبيوتر او الاجهزة الالكترونية، وهي جرائم يكون الكومبيوتر وغيره من الاجهزة الالكترونية وسيلة لارتكابها ، مثل الاحتيال والتزوير. فيستخدم الكومبيوتر او الجهاز الالكتروني في تغيير البيانات لما يجعلها دليل اثبات لمعلومات غير صحيحة.

3. الجهود الدولية لمواجهة الجريمة الالكترونية

تنوعت الجهود الدولية في مواجهة هذه الجريمة في مطلع هذا القرن ، وكان اهمها اتفاقية بودابست لدول الاتحاد الاوربي والنظام الاوربي العام لحماية البيانات ، ثم جاءت

الاتفاقية العربية للمساهمة في مواجهة هذه الجريمة ، وايضا شاركت الدول الافريقية في اتفاقية الاتحاد الافريقي بشأن امن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي ، وفي الختام ساهمت الامم المتحدة من خلال تشكيل لجنة خبراء التي قدمت احدث تقاريرها في 2019 يتضمن استراتيجية شاملة لمواجهة الجريمة الالكترونية ، وانها تسعى لابرام اتفاقية دولية تكون اطارا عاما لتعاون جميع دول العالم في مواجهة هذه الجريمة. وهذا ما سيتم بحثه في القسم الثاني من البحث.

3.1 اتفاقية بودابست

في عام 2001 ’اقرت اتفاقية بودابست بين دول الاتحاد الاوربي ، وهي مفتوحة لانضمام اية دولة من خارج الاتحاد الاوربي. تتكون الاتفاقية من الفصول الآتية :

أ. احكام عامة، ب. التجريم، ت. احكام اجرائية، ث. التعاون القضائي والقانوني ج. احكام ختامية. واهم ما تناولته انها حددت انواع الجرائم الالكترونية ، وهي الدخول غير القانوني المتعمد ، والاعتراض غير القانوني المتعمد ، والتدخل المتعمد على البيانات والمعلومات بهدف تدميرها او حذفها او افسادها او تغييرها او تعديلها او كبتها او اخمادها ، والتدخل المتعمد في الانظمة بهدف تعطيلها او تدميرها ، واساءة استخدام الاجهزة ، واستخدام الكومبيوتر في التزوير او الاحتيال ، وجرائم دعارة الاطفال ، والجرائم المرتبطة بحق المؤلف.

كانت اتفاقية بودابست وما زالت متقدمة على الجهود الدولية الاخرى في دقة تحديد الجرائم الالكترونية وكذلك رسمت اجراءات عملية وحددت نوعية الادلة التي تثبت ارتكابها بما يراعي خصوصية هذه الجريمة وان اثباتها يعتمد على ادلة من نوعية خاصة ذات طبيعة الكترونية . (Scott, 2014).

واستطاعت الاتفاقية ان تثبت جدواها للدول من خارج الاتحاد الاوربي التي انضمت اليها، فقد صادقت المغرب عليها في عام 2018 ، وكذلك الولايات المتحدة الامريكية وكندا وجنوب افريقيا ، ليصل عدد الدول المصدقة عليها الى (55) دولة اخرى . كما تضمنت اجراءات رادعة من حيث جسامة الغرامات التي تفرضها (Dine,2020).

3.2 النظام الاوربي العام لحماية البيانات (GDPR)

في عام 2016 اقرت الدول الاوربية هذا النظام ، الذي يختص بحماية البيانات والخصوصية لجميع الافراددداخل الاتحادالاوربي . ويتعلق ايضا بتصدير البيانات الشخصية خارج الاتحاد الاوربي .

ويهدف الى تمكين المواطنين من التحكم والسيطرة على البيانات الشخصية وتبسيط بيئة التنظيمات والقوانين للمشاريع التجارية الدولية من خلال توحيدها داخل الاتحاد الاوربي . وهو نظام تنظيمي ولا يتطلب ان تصدر الدول اي تشريع لان النظام ملزم وقابل للتطبيق مباشرة. ويؤمن النظام وجود مُعرف شخصي (اسم ورقم ضمان اجتماعي وبيانات الموقع وتعريف عبر الانترنيت) وأحد العوامل الخاصة بالهوية المدنية او الفسيولوجية او الجينية او العقلية او الاقتصادية او الثقافية او الاجتماعية لكل شخص بهدف تحكمه الكامل في بياناته، ولن يسمح لاية جهة الحصول عليها بدون موافقة مالكها. وتشمل البيانات الشخصية حتى الجنسية والاصل العرقي والتوجه الجنسي والحالة الصحية (المادة 9).

ويسمح النظام للمستخدم ان يطلب مسح بياناته الموجودة لدى اية جهة الا اذا كانت تتعلق بالتزامات مالية مثل قرض (المادة 17) ، كما يجوز للاشخاص معرفة المعلومات المخزونة عنهم ولا يجوز استخدامها الا بعد موافقتهم.

وبالرغم من ان النظام مصمم لحماية مواطني الاتحاد الاوربي ، الا انه اصبح يؤثر بشكل اساسي على جميع مستخدمي مواقع الانترنيت بلا استثناء بغض النظر عن مكان تأسيس النشاط التجاري او مكان الانشطة عبر الانترنيت اذا كان يعالج بيانات او يجمعها من مواطني الاتحاد الاوربي فيجب ان يلتزم الآخرين بهذا النظام .

وتخضع المعلومات المتعلقة بالاطفال (تحت سن 16 سنة) لموافقة الوالدين (المادة 8) . واذا كان النشاط التجاري لا يتوافق مع النظام تفرض عقوبات تصل الى 4% من قيمة المبيعات السنوية في جميع انحاء العالم او فرض غرامات مالية تصل الى (20) مليون يورو (المادة 83).

ان اتفاقية بودابست والنظام الاوربي لحماية البيانات قد حققا نتائج ايجابية في التصدي للجرائم الالكترونية بدليل انضمام دول اليها من خارج الجماعة الاوربية ، ولكن رغم ذلك فان الدول العربية والافريقية اتجهت الى عقد اتفاقياتين خاصتين بهما واللتين سنتطرق اليها لاحقا ، كما ان الامم المتحدة عملت على ابرام اتفاقية دولية شاملة ولتكون مظلة لكل المجتمع الدولي.

3.3 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

عقدت هذه الاتفاقية عام 2010 وصدقت عليها (6) دول حتى الآن وهي الامارات العربية المتحدة ، الكويت ، فلسطين ، السودان ، الاردن ، العراق. ولاجل تنفيذها يجب ان تصادق عليها (7) دول ، اي انها ليست نافذة حتى الآن . واهم ما تناولته الاتفاقية فصل عن التجريم وفصل عن الاحكام الاجرائية وفصل عن التعاون القانوني والقضائي.

لم تكن الجرائم الموصوفة في الاتفاقية تتناسب مع واقع تكنولوجيا المعلومات والاتصالات (المادتين6و9) ، وكان التجريم واسعا جدا ويمكن ان يشمل تطبيقات وبرمجيات ضرورية. وتناولت الاتفاقية جريمة الاباحية المتعلقة بالاطفال وشددت المواد الاباحية والمخلة بالحياء ، الا انها فسحت المجال للدول ان تفسرها بدون تحديد او قيود (المادة 62) . وتناولت ايضا الجرائم المتعلقة بالارهاب واستعمال تقنية المعلومات ، كما جرمت نشر النعرات والفتن والاعتداء على الاديان والمعتقدات بوصفها من صور الإرهاب أيضاً على وفق الإتفاقية ، ولكنها تسمح بمحاسبة الرأي المعارض والاختلاف في المعتقدات الدينية بما يتعارض وحرية العقيدة (المادة 15).

وشددت العقوبة على جرائم تقليدية لان وسيلة ارتكابها تعتمد تقنية المعلومات ، (المادة 21) . وهذا التشديد لا مبرر له لانها يعتمد في ارتكابها على الوسيلة الالكترونية .

وفي الفصل الاجرائي نصت على عبارة غامضة (اية جرائم اخرى) يسمح للدول ان تجرم اي فعل خارج نصوص الاتفاقية وهو اسلوب يتناقض مع مبادىء القانون الجنائي الذي لا يسمح بالتجريم الا بموجب نص قطعي وصريح استنادا لمبدأ لا جريمة ولا عقوبة الا بناءا على نص (المادة 22).

ولم تنص الاتفاقية بشكل واضح على حماية خصوصية المستخدمين وبياناتهم وحقوقهم (المادة 14 تنص على حرمة الحياة الخاصة دون الاشارة للبيانات الالكترونية).

وتسمح للدول الاطراف باتخاذ الاجراءات الضرورية لتمكين السلطات المختصة من اصدار الاوامر على اي شخص او جهة مختصة بتسليم المعلومات، دون تحديد ضوابط

قانونية لهذه الاوامر (المادتين 24 و25).
اي ان الاتفاقية لم تكن تتضمن تفاصيل وافية تسهل تطبيقها على الوقائع المختلفة مثلما تضمنته اتفاقية بودابست مما ادى الى انحسار عدد الدول العربية المصدقة عليها لعدم ثقتها بجدواها.

3.4 اتفاقية الاتحاد الافريقي بشأن امن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي (إتفاقية مالابو)

عقدت هذه الاتفاقية عام 2014 وتدخل حيز النفاذ بعد تصديق(15) دولة عليها ، وتغطي نطاقا واسعا من انشطة الانترنيت بما فيها التجارة الالكترونية، وحماية البيانات والجرائم الالكترونية ، والتركيز على العنصرية وكراهية الاجانب، واستغلال الاطفال في المواد الاباحية، والامن الالكتروني الوطني (المواد 2-7) .
ويفرض على الدول المصدقة عليها سن قوانين لحماية البيانات الشخصية (المواد8-23) وانشاء سلطة عامة مستقلة (سلطة حماية البيانات الوطنية) وان تضع كل دولة استراتيجية وطنية للامن الالكتروني واصدار قوانين للجرائم الالكترونية وضمان ممارسة التجارة الالكترونية بحرية . وان تتم معالجة البيانات فقط في غرض مشروع (المواد24-31)، (Layne,2015) ولكن لم يتم تعريف الغرض المشروع.
كما اقرت الاتفاقية استثناءا في معالجة البيانات عند وجود مصلحة عامة (لاغراض تاريخية او احصائية او علمية) وهو استثناء واسع يمكن استغلاله في انتهاك خصوصية المعلومات.
بشكل عام فان الاتفاقية الافريقية متكاملة اكثر من الاتفاقية العربية وتجاوزت الانتقادات الموجهة للاخيرة ، وانها اقرب الاتفاقيات للاتفاقية الاوربية ، وكان يرتجى منها مواجهة ظاهرة تفاقم الجرائم الالكترونية في القارة الافريقية على اسس قانونية فعالة تعتمد على وسائل مبتكرة تتناسب وواقع الدول الافريقية معتمدة منهجا واسعا في تنظيم وحماية المعلومات والبيانات الالكترونية.

3.5 جهود الامم المتحدة

3.5.1 تقرير الخبراء الدوليين لعام 2019

منذ 1990 واجهت الامم المتحدة الجريمة الالكترونية المتعلقة بالكومبيوتر والانترنيت ، (قرارالجمعيةالعامة ،1990) وكان آخرها تقرير لجنة الخبراء الحكوميين لعام 2019، (UNDocs,2019 (الذي يهدف الى دراسة شاملة للجريمة الالكترونية واتخاذ التدابير الدولية للتصدي لها وتبادل المعلومات عن التشريعات الوطنية والاجراءات الفضلى والمساعدة التقنية والتعاون الدولي والتفاوض على صك قانوني عالمي جديد بشأن الجريمة الالكترونية في اطار الامم المتحدة ومراعاة الحاجة الى تدابير فعالة في اطار انفاذ القانون ومراعاة السيادة وتعديل فواعد الاثبات لكفالة جمع الادلة الالكترونية وحفظها والتاكد من صحتها واستخدامها في الاجراءات الجنائية ، اضافة الى:

1. اعتماد قواعد وطنية لتتبع الاتصالات .
2. اعتماد قواعد تنظيم عمليات التفتيش الوطنية والدولية .
3. اعتماد قواعد بشان اعتراض الاتصالات المنقولة عبر الشبكات الحاسوبية والوسائط الاخرى .
4. سن قوانين موضوعية واجرائية محايدة تكنولوجيا لتمكين الدول من التصدي للاشكال الجديدة والمستجدة للجريمة الالكترونية.
5. مواءمة التشريعات الوطنية والاتفاقيات الدولية.
6. انشاء هيئة دولية للتحقق من ادوات التحليل الجنائي الرقمية واعتمادها واعداد الادلة الارشادية وتعزيز قدرات انفاذ القانون والتدابير القضائية للتصدي للجريمة الالكترونية .

تمثل هذه التدابير تطورا كبيرا في مدى اهتمام الامم المتحدة نحو تدويل الجريمة الالكترونية وان تكون منبرا اميا لاجل ضمان قوة وقانونية الاجراءات ووضع حجر الاساس لانشاء اتفاقية دولية اممية تواجه هذه الجريمة.

3.5.2 لجنة خبراء دولية مخصصة لوضع اتفاقية دولية شاملة بشان مكافحة استخدام تكنولوجيا للمعلومات والاتصالات للاغراض الاجرامية

انشأت هذه اللجنة بموجب قرار الجمعية العامة سنة 2019، (رقم 74/247) بناءا على مقترح روسي ودعم صيني واعتراض امريكي واوربي اللذان يتمسكان باتفاقية بودابست لسنة 2001 ، وحصل القرار على موافقة (79) دولة ومعارضة (60) دولة كان اهتمامها يتركز باتجاه اخر يتمثل في مواجهة استخدام تكنولوجيا المعلومات والاتصالات لاغراض اجرامية فحسب.
واثار قرار انشاء اللجنة قلق المجموعات الحقوقية والقوى الغربية التي تخشى ان يفضي الى تقييد الحريات ويقمع حرية التعبير ، كما ذهب اليه كل من الصين وايران والعراق .
(Lupu,2017) ويرون ان توسيع اتفاقية بودابست والمشاركة فيها في مواجهة انتهاكات حق النشر والتاليف والاستغلال الجنسي للاطفال افضل من العمل على اتفاقية اخرى . بينما ترى روسيا ان هذه الاتفاقية تنتهك سيادة الدول من خلال تمكين المحققين في الوصول الى المعلومات. ركزت اللجنة في تقريرها على محورين رئيسيين هما:

1. انفاذ القانون والتحقيقات
2. الادلة الالكترونية والعدالة الجنائية

وقد تضمن كل محور تفاصيل كثيرة تمثل نقاط يمكن ان تكون موضع اتفاق من المشاركين ، ويمثل هذا التقرير سلسلة طويلة من المداولات بدأت منذ عام 2013 وما زالت مستمرة على امل ان تهيء ارضية قانونية لمشروع اتفاقية دولية تتجاوز كل المشاكل والمعوقات ويمكن ان توفر حلولا ومعالجات في مواجهة الجريمة الالكترونية في المستقبل.

الخاتمة والاستنتاجات والتوصيات

ان واقع استخدامات الكومبيوتر وشبكات الانترنيت والاجهزة الالكترونية الاخرى قد تجاوزت على خصوصية المستخدمين وانتهكت حقوقهم وبياناتهم تحت مسمى الجريمة الالكترونية . ورغم تصدي المجتمع الدولي لها فما زالت هذه الجريمة في تزايد وخطورة غير مسيطر عليها ولا تستطيع الدولة لوحدها من مواجهتها لانها ذات طبيعة عابرة للحدود وصعوبة توثيق ادلة اثباتها ، مما يستدعي ان يبذل المجتمع الدولي جهودا استثنائية ومستمرة نحو تحديث القواعد الدولية بما يضمن حماية حقوق الافراد.
ان عدم انضمام عدد من الدول الى اتفاقية بودابست او الاتفاقية العربية او الاتفاقية

الافريقية سوف يؤدي لوجود مساحة واسعة لارتكاب الجريمة الالكترونية دون وجود امكانية على التصدي لها بسبب عدم وجود الغطاء القانوني مما يشكل ثغرة يستغلها مرتكبو الجرائم الالكترونية من خلال هذه الدول.

وما زالت الرغبة الاوربية والامريكية لان يتوحد المجتمع الدولي بالانضمام الى اتفاقية بودابست رغم عدم ثقة الكثير من الدول التي تراها غير كافية في مواجهة الجرائم الالكترونية على مستوى العالم مما ادى لابرام الاتفاقيتين العربية والافريقية اللتين اعتراهما الكثير من النواقص وتعرضتا لانتقادات اثرت في عدم ثقة الدول من جدوى بالانضمام اليها ، وتسبب ذلك ان يستمر المجتمع الدولي بالب حث عن بدائل اكثر جدية وصرامة في مواجهة الجرائم الالكترونية.

وان افضل وسيلة لمواجهة هذه الجريمة هي ابرام اتفاقية دولية برعاية الامم المتحدة لتكون بديلا عالميا موحدا عن الاتفاقيات الاقليمية المحدودة النطاق من حيث عدد الدول الاطراف فيهاوتشتت الجهود الدولية . وفي الوقت نفسه تكون جميع الدول اطرافا في الاتفاقيات الاقليمية حتى يتم ابرام اتفاقية عالمية شاملة .

وبضوء ما تقدم فاننا نقدم التوصيات الآتية:

1. ان تعمل كل دولة طرف في الاتفاقيات الدولية المختصة بالجرائم الالكترونية على تقديم مقترحاتها من اجل تحديثها بضوء المتغيرات والتطورات في المجال الالكتروني .
2. تعاون الدول كافة مع اللجنة الحكومية الدولية التي انشأتها الامم المتحدة من اجل اتمام اتفاقية دولية لمواجهة الجريمة الالكترونية .
3. دعوة الدول الغير مشاركة في الاتفاقيات الاقليمية الحالية المتعلقة بالجريمة الالكترونية للانضمام اليها حتى يتم انشاء الاتفاقية الدولية الشاملة .
4. تركيز الاهتمام وبذل جهود دولية تتناسب وخطورة الجرائم الالكترونية من اجل وصفها كجريمة دولية ومحاولة اعتبارها صورة من صور العدوان الذي يمكن ان يدخل في اختصاص المحكمة الجنائية الدولية.

المصادر

الحوامدة، لورنس سعيد (2017). الجرائم المعلوماتية اركانها ووسائل مكافحتها، مجلة الميزان للدراسات الاسلامية والقانونية، جامعة طيبة، السعودية . ص8 -ص10

عبدالباقي، مصطفى عبد (2018)، التحقيق في الجريمة الإلكترونية واثباتها في فلسطين :د راسة مقارنة (2018)، مجلة دراسات، علوم الشريعة والقانون، المجلّد 45، عدد4 ، ملحق2 ، الجامعة الاردنية. ص288

العدواني، فهد دخين (2016). الانترنت والجريمة الالكترونية وطرق التغلب عليها، المجلة الدولية للتعليم بالانترنت. ص 7- 9، ص59.

إتفاقية بودابست (2001).

https://www.coe.int/en/web/cybercrime/the- budapest-convention

اتفاقية الاتحاد الافريقي بشأن امن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي (إتفاقية مالابو) (2014). .https://moeltaher.net/2-

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010

https://www.courts.gov.ps/userfiles/file/

النظام الاوربي العام لحماية البيانات GDPR (2016)

https://www.liveagent.ae/masrad-daam-alameel/gdpr-ar/

Benvenisti, Eyal. (2014). Upholding Democracy Amid the Challenges of New Technology, What Role for The Law of Global Governance? *E.J.I.L..25* (1), 240-241.

Carlin, J. (2016). Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats, *Harv.N.S.J., 7*, 539-397. Available at http://araedu.journals.ekb.eg

Daskal, J. (2015). The UN- Territoriality of Data, Yale *J.I.L., 125*, 326.

Wojeik, M. (2000). Human Rights & Corporate Responsibility, *Tulsa J.C.& I.L.,8* (1), 2.3-

Dine, A.V. (2020). When is Cyber Defense a Crime? Evaluating Active Cyber Defense Measures Under The Budapest Convention, *Chicago J.I.L., 20*, (2), 537-546.

Schmitt, M. (2017). Peacetime Cyber Responses and Wartime Cyber, Operations Under International Law: An Analytical Vade Mecum, *Harv.N.S.J., 8*, 240.241-

Eyan, B. (2011). International Law & Stability in Cyberspace, *Barkeley J.I.L., 9*, 535-536.

Shackelford, S. J. (2009), From Nuclear to Network: Analogizing Attacks in International Law. B*erkeley J.I.L., 27*(1), 195.196-

Giles, A. P. (2018), Transnational Cyber Offenses: Overcoming Jurisdictional Challenges, Yale *J.I.L., 43*, 195-19.

Kilovaty, I. (2018). Dox fare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information, Harv.N.S.J., *9*, 152-154.

Layne, S. R. (2015), Corporate Responsibility for Human Rights Violations, *Gonzaga J.I.L., 18*, (1), 40-41.

Lupu, Y. (2017). Explaining Human Rights Abuses: Comparing Contemporary Features & Historical Factors,*Vig.J.I.L., 56(2)*, 482-483.

Mourlam, A.C (2016). Unarmed Attacks: Cyber Combatants & The Right to Defend, *Calf.I.L.J., 26* (1), 19-21.

Scott, J. (2014). Extraterritoriality & Territorial Extension in EU Law , *A.J.Comp.L., 62*, 88-89.

Corfu Case (1949), https://www.icj-cij.org/en/case/1, Retrieved in 4/1/2021.

Libya Case ,1986. https://en.wikipedia.org/wiki/West_Berlin_discotheque_bombing , Retrieved in 5/1/2021.

Tadic Case 1991, https://www.icj-cij.org/en/case/91 , Retrieved in 2/2/2021.

USA & Nicaragua Case,1986, https://www.icj-cij.org/en/case/70 , Retrieved in 3/2/2021.

UNODC/CCPCJ/EG.4/2019/2 , P.21 - Report of Experts Group.

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 , Retrieved in 2/1/2021

https://en.wikipedia.org/wiki/Convention_on_Cybercrime, Retrieved in 1/12021

https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection, Retrieved in 3/2/2021

Abstract:
The research dealt with the electronic crime known by the term (cyber) because of its connection with space, which is the widest field for its perpetration and implementation of its pillars, and it is often between countries or within the state, and because of its importance, multiple definitions have been known and its nature has been defined as a deliberate crime committed to achieve goals harmful to the interests of a person or a certain party. It has characteristics that distinguish it from other acts in terms of its perpetration by a computer, its systems or the information it contains, or it targets the Internet and the sites in which it is, and usually more than one person or entity contributes to it. Or disrupting it, sabotaging it, forging it, and so on.

Keywords: Crime, Cyber, Budapest, Agreement, Effort.