الجريمة السيبرانية وحدود المسؤولية الجنائية في الفضاء الرقمي

أ.م.د.انس محمود خلف

جامعة الموصل/ كلية الحقوق

Cybercrime and the Limits of Criminal Liability in the Digital Space

Dr. ANAS MAHMOOD KHALAF

University of Mosul / College of Law

المستخلص: تعد الجريمة السيبرانية من التحديات القانونية الحديثة التي تواجها المسؤولية الجنائية في الفضاء الرقمي حول العالم, ومنها القضاء العراقي, اذ يكون لنتيجة التطور السريع في التقنيات المعلومات والاتصالات, اذ اصبح الفضاء الإلكتروني مسرحاً لارتكاب افعال مجرمة مثل الاختراق, او الاحتيال الإلكتروني, او الابتزاز, او السرقة البيانات,, مما يستدعي تطور ادوات قانونية فعالة لمواجهتها, اذ يركز هذا البحث على تحليل الاطار القانوني للجريمة السيبرانية في العراق, مع بيان حدود المسؤولية الجنائية في هذا المجال, من حيث تحديد الفاعل في الفضاء الرقمي, وصعوبة اثبات القصد الجنائي في بعض الجرائم الإلكترونية, كما يناقش العقوبات القانونية وآليات مكافحة جرائم المعلوماتية, ومدى توصل البحث في مضمار تلك تحديد المسؤولية عن كافة المساهمين فيها, من حيث شراء مستلزمات الانترنت او التزود بالأنترنت وغيرها من الممارسات,, اذ ان القضاء العراقي لا يزال يواجه تحديات كبيرة في تطبيق القواعد الجنائية التقليدية, على الجرائم السيبرانية, بسبب غياب التشريعات المتخصصة, كما لقصور معلومات الخبراء الفنين في مجال جرائم السيبرانية من تهكير, اوغيرها في التتبع للأدلة الرقمية, مما يؤثر على فعالية الملاحقة القضائية في تحقيق وجمع الادلة في الفضاء الرقمي, وبهذا اذ يختم البحث بجملة من التوصيات, واهمها ضرورة اصدار قانون خاص بجرائم المعلوماتية, والتي يتضمن تعريفات دقيقة للجريمة السيبرانية, في حدود المسؤوليات الجنائية

بوضوح, الى جانب جملة من تأهيل الكوادر القضائية, والفنية المختصة من الخبرة للهجمات الجرائم السيبرانية.. **الكلمات المفتاحية:** الدليل الرقمي – السيبرانية – الفضاء – الإلكتروني

Abstract : Cybercrime has emerged as a serious threat in the digital age, affecting individuals, institutions, and nature of cybercrime and examines the extent of criminal liability under Iraqi law. It analyzes, how Iraqi jurisprudence addresses various forms of cybercrime, including hacking, identity theft, online fraud, and unauthorized access to data. The research also investigates the challenges facing the Iraqi legal system in prosecuting cybercriminals, such as the lack of comprehensive cyber legislation, technical expertise, and the transnational, nature of cyber offenses. Furthermore, the paper assesses the boundaries of criminal responsibility, particularly in cases involving indirect participation corporate liability, and juvenile offenders. Through a comparative lens, the study proposes legal reforms and judicial, strategies to enhance the effectiveness of Iraq`s legal response to cybercrime while ensuring due process, and the protection of fundamental rights. **Keywords** Digital Directory – Cyber – Space – Electronic.

المقدمة: ان في مستهل الحديث عن الحرب السيبرانية فان تلك الجرائم حديث النشأة بل هي شبة ظاهرة جديدة في ظل التطور المتسارع للتكنلوجيا وانتشار استخدام الانترنت, ووسائل الاتصال في الفضاء الرقمي, اذ برزت الجرائم السيبرانية كأحد ابرز التحديات التي تواجه المجتمعات الحديثة زمنها العراق, اذ تعد الجريمة السيبرانية من الظواهر القانونية المستحدثة التي تتسم بالتعقيد والتنوع, اذ تشمل انشطة غير مشروعة تتم عبر الفضاء الإلكتروني مثل

الاختراق, او الاحتيال الإلكتروني,, وسرقة البيانات, والتشهير الرقمي, كنوع من الجرائم التي ترتكب في الفضاء الالكتروني في العصر الرقمي, لذا فان النقاش يدور حول طبيعة حكم تلك السلوك الانساني في الفضاء الإلكتروني, والذي يتمحور حول طبيعة القواعد التي تحكم الفضاء الإلكتروني للحرب السيبرانية, لذا فان آلية انشاء تلك القواعد وتطبيقها في نطاق القانون الدولي, قد يثار الجدل والاشكال الفقهي في مدى امكانية خضوع الحرب الإلكترونية الى احكام القانون الدولي, وفق المعاير الاتفاقيات الدولية للقانون الدولي,, لذا فعلى هذا المحور قد يعد الفضاء الإلكتروني في منطقة بلا قانون يحكم تلك التصرفات والخروقات, والذي يقر بوجود فراغ قانوني دولي من اجل السيطرة والحد من تلك الجرائم السيبرانية, وبالحصيلة النهائية فان تلك الجرائم لا تحكمها اي قوانين او اتفاقيات دولية, بالرغم من انتهاكها للخصوصية الدولية, وبهذا فان الطبيعة المترابطة للشبكات العنكبوتية الإلكترونية, اذ من غير المتصور استهداف كجزء من الشبكة دون التأثير على باقي الاجزاء سواء أكانت الهجمة الإلكترونية, او اي هجمة بالمفهوم التقليدي,, عليه فانه تقع على عاتق المجتمع الدولي, هو تحقيق الحماية اللازمة لمواطنيها, وتبنى على اساس تدعيم وتكريس السيادة الدولية, التي تتمتع بها, على الصعيد الدولي من اجل عدم انتهاك تلك السيادة والحظر, قدر الامكان من تلك الجرائم السيبرانية.

اولاً: اهمية البحث: تكمن اهمية هذا البحث الى تسليط الضوء على اهم المبادئ الراعية لتلك الجرائم في القانون الدولي للفضاء الرقمي, في ظل تنامي الاعتماد على التكنلوجيا, وتحديد مدى امكانية تطبيقها على الحرب السيبرانية, خاصة في استخدام الفضاء الالكتروني في الحرب,, بغية تبعثر عمل تلك القوانين خصوصاً اذ غالباً ما تكون تلك الاهداف من جراء تلك الهجمات او الحروب قد تكون مدنية وليس عسكرية على الاغلب, لما لها من مردود سلبي على السكان المدنيين.

ثانياً: اهداف البحث: قد تثار في هذا السياق تساؤلات عدة وجوهرية, حول حدود المسؤولية الجنائية في الجرائم السيبرانية, خاصة في ظل الطبيعة الافتراضية لهذا الافعال, وتعدد الاطراف المعنيين بها, من منفذين مباشرين الى اطراف مسهلة او متغاضية,, ومن هنا تبدوا اهمية البحث

في مضمار هذا الموضوع لما له اثر على القضاء العراقي, في تفسير النصوص القانونية القائمة وكذلك التكييف الافعال ضمن اطار المسؤولية الجنائية للفضاء الرقمي, وفقاً لأحكام القانون العراقي.

ثالثاً: مشكلة البحث: تتمتع خصوصية الفضاء الرقمي الالكتروني في عدم وجود قانون اي دولة بإمكانها فرض سيطرتها او سيادتها عليه, لذا فان الاشكالية يؤدي الى استخدامه بشكل قد يضر البشر,, الاتجاه الدولي في مجال تطبيق القواعد القانونية على الشبكة الإلكترونية او العالم الافتراضي او المعلوماتي يتجه من اجل العمل لتطبيق القواعد, والمبادئ العامة المعروفة الراعية للقوانين الدولية, لصعوبة الوصول الى اتفاق دولي جديد خاص, وملزم للفضاء الرقمي الإلكتروني.

رابعاً: منهجية البحث: سنعتمد في بحثنا هذا الى ثلاثة مناهج, منها المنهج التحليلي, والذي سيطرح الاسس القانونية, التي يستند عليها مبدأ مسؤولية الجرائم السيبرانية المرتكبة, ثم نناقشها ونحلل ظواهرها,, وكذلك العمل على المنهج الوصفي من حيث, من خلال الوصف الوقائع وبصورة خاصة في الجوانب النظرية للبحث في ارتكاب جريمة السيبرانية,, وكذلك المنهج التاريخي لتحديد التأصيل التاريخي, لتلك الجرائم وتحديد المسؤولية للفضاء الرقمي.

خامساً: خطة البحث:

المبحث الاول: الاطار المفاهيمي للجريمة السيبرانية.

المطلب الاول: تعريف الجريمة السيبرانية وطبيعتها.

المطلب الثاني: اركان الجريمة السيبرانية.

المبحث الثاني: المسؤولية الجنائية في الفضاء الرقمي.

المطلب الاول: المسؤولية الجنائية الفردية:

المطلب الثاني: المسؤولية الجنائية المعنوية (الشركات ومزودو الخدمة):

المبحث الثالث: التحديات القانونية والقضائية.

المطلب الاول: المسؤولية الجنائية الفردية.

المطلب الثاني: الاطار التشريعي لمكافحة الجريمة السيبرانية.

المبحث الاول: الاطار المفاهيمي للجريمة السيبرانية

اذ بالرغم من الفوائد الكثيرة للتحول الرقمي, الا انه له عدة استخدامات وبحسب الغاية التي يبتغي من جراء استخدام لتلك المنظومة, ومنا استخدام التكنلوجيا لأغراض اجرامية افرزت مشاكل قانونية جديدة تتعلق بإثبات في الفضاء الرقمي, اذ يعتبر لتحدي جديد هو تحديد شخصية الفاعل,, زما هو المحاكم التي يخضع لها تلك الجريمة السيبرانية, مما خلق للقضاء العراقي تحدي جديد في مواجهة تلك الجرائم بمفردات قانونية حديثة, لذا فقد سعت التشريعات العراقية, وان كانت محدودة في هذا الجانب الى تنظيم بعض الجوانب المرتبطة بالجرائم الإلكترونية, سواء من خلال قوانين العقوبات او مشاريع القوانين الخاصة, والراعية لتلك الجرائم السيبرانية,, في ظل الثورة الرقمية المتسارعة, اصبحت الجريمة السيبرانية احد التهديدات الكبرى التي تواجه الأفراد, والمجتمعات والدول, مع تطور التكنولوجيا مما زاد من فاعلية وتطور الاشخاص الفاعلية والممارسين لتك الجرائم, لذا فقد تعددت تلك الجرائم وغالياً ما تكون منها ضد الافراد كالتنمر الإلكتروني والابتزاز الجنسي وسرقة البيانات الشخصية, وكذلك الجرائم ضد الممتلكات مثل اختراق الانظمة البنكية او التلاعب في البيانات المالية, وايضاً جرائم تقع ضد الحكومات وهي محور بحثنا والتي تحدث الهجمات الإلكترونية على البنية التحتية او جرائم نشر الدعاية الارهابية, وللتوضيح اكثر سوف نقوم بتقسيم هذا المبحث الى عدة مطالب,, نتناول في المطلب الاول, تعريف الجريمة السيبرانية وطبيعتها, وفي المطلب الثاني اركان الجريمة السيبرانية وبالشكل الاتي:

المطلب الاول: تعريف الجريمة السيبرانية وطبيعتها

الجريمة السيبرانية:" هي اي نشاط غير قانوني يتم غبر الانترنت او من خلال انظمة الحاسوب, وتستهدف الافراد, او المؤسسات, او الحكومات, ويشمل استخدام التكنلوجيا الرقمية, لارتكاب افعال بالأمن, او الخصوصية, او الممتلكات الرقمية"[1].

كما عرفة:" بانها الجريمة الإلكترونية هي اي نشاط غير قانوني يرتكب باستخدام الحاسوب, او شبكة الانترنت, كأداة او كهدف او كليهما, وتشمل هذه الجرائم مجموعة, واسعة من الافعال, ومثل اختراق الانظمة وسرقة البيانات, وكذلك الاحتيال الإلكتروني, ونشر البرمجيات الخبيثة, والابتزاز الرقمي, وانتهاك الخصوصية"[2]. كما عرف دليل تالين في القاعدة رقم (30) الهجمات السيبرانية:" هي عمليات سيبرانية, سواء كانت هجومية او دفاعية, والتي يهدف من خلالها بصورة معقولة التسبب بالاصابة, او الوفاء, او الأشخاص, او الاضرار او تدمير الاعيان (الاهداف)"[3].

طبيعة الجريمة السيبرانية:

1. غير مادية: لا يتطلب وجوداً مادياً للجاني في مكان وقوع الجريمة, مما يجعل تتبعها,, اوالتحقيق فيها اكثر تعقيداً, اذ تتم في الفضاء الإلكتروني.

(1) انطونيو كاسيزي, القانون الدولي الجنائي, ط3 باللغة الانكليزية, 2013, ط1 باللغة العربية2015, ترجمة صادر ناشرون, بيروت, ص45.
(2) جون ماري هنكرتس, القانون الدولي الانساني العرفي, المجلد الاول, لقواعد اللجنة الدولية للصليب الاحمر, مطبعة برنت للإعلان والدعاية, القاهرة, 2007, ص65.
(3) هو دليل اكاديمي يطبق القانون الدولي على الفضاء السيبراني في سياق النزاعات المسلحة, سنة 2013.

2. عابرة للحدود: يمكن ان تتم من اي مكان في العالم, وتستهدف ضحايا في دول مختلفة,, ما يصعب الملاحقة القانونية لها, اذ يمكن ارتكابها من اي مكان في العالم ما يعقد عملية تتبع الجناة فيها.

3. متنوعة: تشمل انواعاً متعددة مثل, الاختراق وسرقة البيانات والاحتيال المالي عبر الانترنت في الفضاء الرقمي, نشر البرمجيات الخبيثة (الفيروسات, الفدية) الابتزاز الإلكتروني,, انتهاك حقوق الملكية الفكرية.

4. سريعة التطور: تتطور تقنياتها باستمرار, مما يتطلب تحديثاً دائماً للتشريعات والامن السيبراني, تتغير وتتكيف بسرعة مع تطور التكنولوجيا.

5. صعوبة الاثبات: من الصعب, جمع الادلة وتحديد هوية الجاني, اذ تؤثر على الامن الشخصي, والمالي,, والوطني.

الفرع الاول: التمييز بين الجريمة التقليدية والسيبرانية: هناك عدة اوجه تختلف فيها الجريمة التقليدية عن الجريمة السيبرانية من حيث المكان, وطبيعة الأدلة,, ففي من حيث المكان تحدث الجريمة السيبرانية في الفضاء الرقمي الإلكتروني (الافتراضي), في تقع الجريمة العادي في العالم العادي والواقعي, اما من حيث الوسيلة فالجريمة السيبرانية ترتكب باستخدام اجهزة الكترونية وشبكات الانتزنت,, في حين ادوات الجريمة العادية ترتكب بأدوات مادية مثل السلاح او اليد, اما من حيث الهدف فالجريمة السيبرانية تهدف للوصول الى معلومات, واموال الكترونية, او تعطيل انظمة المعلومات السرية,, في حين تكون الجريمة العادية في الاستيلاء على اشياء مادية, او الحاق الاذى الجسدي, اما جانب الادلة فتكون للجريمة السيبرانية سجلات رقمية,, وعناوين, ورسائل إلكترونية, اما الجرائم العادية غالباً ما تكون بصمات, وكامرات, وشهود عيان, والجرائم العادية غالباً ما تكون ضمن الحدود اي محلية, اما الجرائم السيبرانية لها

طابع دولي لا تتقيد بالحدود, اي عابرة للحدود الدولية, وهذا يعقد موضوع التحقق منها وكشفها وصعوبة القبض على الشخص الفاعل[1].

الفرع الثاني: خصائص الجريمة السيبرانية: تتمتع الجريمة السيبرانية بعدة خصائص (الجرائم الإلكترونية) تميزها عن الجرائم التقليدية, اذ تشمل على ما يلي:

1. الطابع غير المادي: اذ لا تتطلب الجريمة السيبرانية وجوداً مادياً, فهي ترتكب في الفضاء الرقمي, باستخدام الاجهزة,, والبرمجيات.

2. الانتشار والواسع وسرعة التنفيذ: اذ يمكن تنفيذها بسرعة فائقة ومن اماكن متباعدة حول الكون, وغالباً ما يصعب تتبع الفاعل بسبب اخفاء الهوية,, واستخدام الشبكات المشفرة.

3. متعدد الاشكال والانواع: غالباً ما يشتمل الاحتيال الإلكتروني الاختراق, وسرقة المعلومات من خلال الابتزاز الرقمي,, من اجل نشر برامج الفايروسيه وغيرها في الفضاء الرقمي.

4. تهديد للأمن المعلوماتي والاقتصادي: تؤثر على الافراد, والمؤسسات الحكومية, ويمكن ان تؤدي الى خسائر مادية,, اومعنوية جسيمة.

5. سهولة وسرعة ارتكابها مقارنة بالجرائم التقليدية: اذ يمكن لأي شخص لديه مهارات تقنية بسيطة, وان يرتكب جريمة إلكترونية دون الحاجة الى قوة جسدية,, او ادوات تقليدية.

6. ذات طابع دولي: غالباً ما يكون الشخص الذي يتقن تلك الصفة في استعمال الحاسوب لديه مهارات بسيطة ان يرتكب جريمة إلكترونية في الفضاء الرقمي,, دون الحاجة الى قوة جسدية, او ادوات تقليدية.

([1]) محمد طاهر قاسم, الاساس القانوني للمسؤولية عن الأشياء الخطرة امام القضاء العراقي, مجلة الرافدين للحقوق, المجلد13, العدد49, السنة16, ص179.

7. صعوبة الاثبات والتحقيق: ان من الصعب كشف هوية الشخص الفاعل, من خلال كشف وتعقب الادلة الرقمية وتتبع العناوين[1].

الفرع الثالث: تصنيف الجرائم السيبرانية: يمكن ان تصنف الجرائم السيبرانية والتي يمكن ان يتم بناء على طبيعة الجريمة والهدف منها,, فيما يكون نوع الهدف منها وفق معاير معينه:

اولاً: حسب الهدف من الجريمة:

1- جرائم ضد الافراد: تتكون الجرائم ضد الافراد عدة جرائم منها الابتزاز الإلكتروني, وكذلك جرائم التشهير,, والاساءة عبر الانترنت, ومنها اختراق الحاسبات الشخصية, وكذلك الحرش الإلكتروني,, وسرقة الهوية, والتهكير وفق اختراق البرامج, الشخصية للغير, وتحديد المسؤولية في الفضاء الرقمي.

2- جرائم ضد البنية التحتية: يكون الهدف من تلك الجرائم هو السيطرة على منظومات البنى التحتية, واختراق الاجهزة, او الشبكات وكذلك البرمجيات الخبيثة, والمتمثلة بالفيروسات, والديدان وبرمجيات الفدية,, والمتمثلة بسرقة البيانات, وتدمير او تعطيل انظمة التشغيل, او البيانات, او السيطرة عليها, وتقيدها او غيرها, لغرض سرقة تلك البيانات.

3- جرائم ضد الحكومات او المؤسسات: ان الاساس التي تقوم عليه الجرائم السيبرانية, هو التحسس واختراق المنظومات لتلك الدولة في الهجمات على البنى التحتية,, والحيوية من كهرباء وماء وغيرها, من اجل نشر المعلومات في سرية, واختراق مؤسسات حكومية للإرهاب الإلكتروني, او ما يسمى بالقرصنة ضد برامج المؤسسات الحكومية[2].

([1]) انطونيو كاسيزي, مصدر سابق, ص74.

([2]) محمد طه البشير, الوجيز في نظرية الالتزام في القانون المدني العراقي, الجزء الاول, (مصادر الالتزام), ط4, المكتبة القانونية, بغداد, 2010, ص259.

ثانياً: بحسب نوع الاداة المستخدمة: هناك جرائم عدة تستخدم في الاختراق السيبراني,, والمتمثل بالبرامج الخبيثة, والجرائم التي تعتمد على الهندسة الاجتماعية, كالتصيد الإلكتروني, وتحديد المسؤولية, والجرائم باستخدام ادوات القرصنة,, عن طريق كسر كلمات المرور او الاستغلال[1].

ثالثاً: حسب الجهة الفاعلة: هناك عدة جهات فعال تكون مهمتها اختراق اي منظومة من قراصنة افراد هاكرز, وعصابات منظمة إلكترونية,, وجهات دولية, او حكومية في سياق الحروب السيبرانية[2].

المطلب الثاني: اركان الجريمة السيبرانية:

هناك اركان عدة للجريمة السيبرانية اي الجريمة المعلوماتية, والتي هي العناصر الأساسية التي يجب ان تتوافر حتى تعد الجريمة, واقعة قانونية ويحاسب عليها الفاعل,, وتتشابه في تركيبها مع اركان الجرائم التقليدية ولكنها تتميز بخصوصيتها, لأرتباطها بالتكنلوجيا, والفضاء السيبراني هي كالاتي:

الفرع الاول: الركن المادي: ان للركن المادي له عدة عناصر رئيسية: والمتمثل بالسلوك الاجرامي في فعل ايجابي كالاختراق ونشر فيروسات, وكذلك سرقة بيانات او سلبي كالتقاعس عن حماية نظام معلومات مسؤول عنه, في الفضاء الرقمي, والتي تتكون من النتيجة الاجرامية هي الاثر الضار للفعل, والمتمثل بتدمير النظام او تسريب معلومات حساسة, من خلال العلاقة السببية,, والتي يجب ان تكون الفعل هو السبب المباشر, في النتيجة[3].

الفرع الثاني: الركن المعنوي: ان المقصود بالركن المعنوي هنا القصد الجنائي, والذ يتمثل في نية الجاني وارادته الواعية, لارتكاب الجريمة من قصد جنائي عاماً كنية لارتكاب الفعل المحظور, خاصة بغية الاضرار بشخص او تحقيق منفعة غير مشروعة,, والتي تتمثل في

(1) محمد طاهر قاسم, مصدر سابق, ص72.
(2) محمد طاهر قاسم, مصدر سابق, ص73.
(3) عبدالله سليمان, شرح قانون العقوبات, القسم العام, ديوان المطبوعات الجامعية, الجزائر, 2003, ص59.

تحقيق عمل غير مشروع مثل الابتزاز مقابل المال, اذ تبنى المسؤولية الجنائية في القانون على توافر اركان معينة, لا بد نت تحققها لإثبات قيام الجريمة, والمتمثل بالركن الشرعي, والركن المادي والركن المعنوي,, اذ يعد الركن المعنوي احد ابرز تلك الاركان هو توافر الركن المعنوي, فالأراد تلعب دوراً بارزاً لارتكاب الفعل الجرمي, لذا فلا يكفي مجرد وقوع الفعل المادي, بل لابد من ان بصاحبه توجه نفسي ذاتي معين يدل الى القصد, او الاهمال[1].

الفرع الثالث: الركن المفترض: يتمثل هنا بالركن المفترض بجهاز الكمبيوتر وشبكة الانترنت, وكذلك بريد الالكتروني في تطبيقات من قواعد بيانات, فان للجرائم لها اركان متعددة فالجريمة في القانون تبنى على اركان ما هو مادي منها, وما هو معنوي, ومنها ما يعرف بالركن المفترض,, والمفترض قانوناً, وهو ذلك العنصر المشترط مسبوق لقيام الجريمة, رغم انه لا يعد من اركان الجريمة التقليدية (الركن المادي والركن المعنوي) او الركن المشترط, او ما يسمى بالشرط المفترض, والذي يعد بانه يكون شرطاً سابقاً على توافر الشرط المفترض, ولا تتحقق الجريمة, الا بوجوده, وتحديد المسؤولية في الفضاء الرقمي[2].

المبحث الثاني: المسؤولية الجنائية في الفضاء الرقمي

ان مع التطور السريع في التكنولوجيا الرقمية المعلوماتية والاتصالات, اذ اصبحت الضرورة الفعلية تلعب دوراً بارزاً للتدخل للحد من تلك الجريمة او تقيدها قدر الامكان, والتي اصبحت جزاً لا يتجزأ من الحياة اليومية, حيث تمارس تلك النشاط الاجتماعي,, والاقتصادي, والقانوني, وقد ادى هذا التوسع الى ظهور جرائم رقمية جديدة, والتي تلزم الضرورة الى المواجهة القانونية, من اجل تجديد الكيان للمسؤولية التقصيرية الجنائية في الفضاء الرقمي, عليه فان للفضاء الرقمي هو البيئة الافتراضية الناتجة عن استخدام الشبكة العنكبوتية الرقمية, والمتمثلة بالأنترنت, وتحديد المسؤولية في الفضاء الرقمي, اذ تشمل مواقع الانترنت الالكترونية ضمن وسائل التواصل الاجتماعي, بخلاف حالة الجريمة العادية, والتي تكون الجريمة الرقمية عي كل

(1) عبدالله سلمان, مصدر سابق, ص60.
(2) عبدالرحمن خلفي, محاضرات في القانون الجنائي العام, دار الهدى للطباعة والنشر والتوزيع, الجزائر, 2013, ص64.

فعل غير مشروع,, اذ يتم باستخدام الوسائل التكنلوجيا, مثل اختراق الانظمة الالكترونية, وفق الاحتيال التكنلوجي في نشر المواد القرصنة, خاص وان تلك الجريمة تحدث, وتنتهي ولا يمكن القبض على الشخص الفاعل, او التعرف على هويت الجاني كون انها تحدث بدون سابق انذار وتنتهي, لكن تظهر بعد الانتهاء من القرصنة, او ارتكابها, اذ طالما يكون يم الشخص الفاعل آلية التشفير, وادوات الاختفاء, هذا من جانب ومن جانب اخر فان نقص الكوادر الفنية,, والتي تكون ملمة من اجل تحليل الرقمي للشخص الجاني, تكون شبه معدومة كون ان الاشخاص القائمين على تلك الجريمة, لديهم الخبرة الكافية التي تجعلهم يحددون لحظة انطلاق الجريمة السيبرانية, والمتمثلة بالجرائم الرقمية, ونقطة الانسحاب ومن ثم الاختفاء, علية يمكن القول ان المسؤولية الجنائية في الفضاء الرقمي تمثل تحدياً حديثاً, اذ يتطلب استجابة قانونية مرنه, وكذلك شاملة, ويمكن الحل في تطور التشريعات, ورفع مستوى الوعي الرقمي, في تعزيز التعاون الدولي قبل المحلي كون انه شأن دولي, وذلك من اجل تحقيق العدالة الفعال في هذا العالم الرقمي, وللتوضيح اكثر قمنا بتقسيم هذا المبحث الى عدة مطالب وبالشكل التالي:

المطلب الاول: المسؤولية الجنائية الفردية:

ان الصفة الغالبة للمسؤولية الجنائية الفردية, من المبادئ الاساسية في القانون الجنائي, اذ تقوم على عاتق الشخص الفاعل التبعات الجزائية التي تلزمه بتحمل المسؤولية وحدة,, دون ان تمتد تلك التبعات الى غيره, وبهذا نكون امام عدالة انتقالية في تحمل الفعل المرتكب, والمتمثل فيها العنصر الجزائي في القصد الجنائي, لتحديد المسؤولية في الفضاء الرقمي, وللتوضيح اكثر قمنا بتقسيم هذا المطلب الى عدة فروع, لذا سوف نتناول في الفرع الاول الفعال المباشر, وفي الفرع الثاني الشريك والمساهم الإلكتروني,, وفي الفرع الثالث مسؤولية المستخدم العادي او الغير المتخصص, وبالشكل الاتي:

الفرع الاول: الفاعل المباشر: ان المسؤولية الفردية صدعة اهميتها في حفظ النظام القانوني في تحقيق العدالة الدولية, اذ ظهرة بشكل واضح في القانون الجنائي الدولي, خاصة بعد الحرب العالمية الثانية,, حيث طبق على القادة العسكريين والمدنيين في محاكمات نورمبرغ, واقرتها مبدأ

ان الافراد يمكن ان يحاسبوا جنائياً على الجرائم الدولية مثل جرائم الحرب والجرائم ضد الانسانية والابادة الجماعية, عليه فان المسؤولية الجنائية الفردية هي ضمانة قانونية واخلاقية لتحقيق العدالة,, اذ تعد من الاسس التي تبنى عليها سيادة القانون, وهي التي تؤكد ان العقوبات لا توقع الا على من ارتكب الفعل الاجرامي, عن وعي واختيار, وهو ما يكرس مبادى العدالة الجنائية في المجتمعات الحديثة[1].

الفرع الثاني: الشريك والمساهم الالكتروني: يلعب الشريك او المساهم دوراً بارزاً في الجرائم الإلكترونية, بقصد به المساهمة في الفضاء الرقمي, او المشاركة في ارتكاب الجريمة من دون ان يكون هو الفاعل الرئيسي, ويشمل ذلك اشكالاً متعددة بحسب القانون الجنائي, والمتمثل سواء بالتحريض وهو من يدفع او يشجع الشخص الفاعل الرئيسي على ارتكاب الجريمة, قد يتم بإقناع شخص باختراق حساب جهة معينة, او يزوده بدوافع من المساعدات المالية,, والمعنوية, من خلال اختراق البيانات المسروقة, اذ يتم وفق تخطيط او توجيه من اجل التنفيذ لاختراق النظام, لذا فان اغلب التشريعات يعاقب الشريك, او المساهم بالعقوبة ذاتها, او بعقوبة مخففة, وبحسب درجة تورطه,, ببعض القوانين اذ تفرق بين الشريك الاصلي, او المساعد, او المتستر, بعد وقوع الجريمة[2].

يتضح لنا من خلال ما تم ذكره عن المسؤولية الفردية, اذ انها لها اهمية في الحفاظ على النظام القانوني,, من اجل تحقيق العدالة, واستتباب الامن, لذ فهي تكون منصفة, وضامنه في عدم تعدي حدود التقصير الى غير الشخص الفاعل, وعدم معاقبة الابرياء,, هذا من جانب ومن جانب اخر تحديد المسؤولية في الفضاء الرقمي, اذ يكون في تحمل كل شخص تبعات سلوكة الاجرامي, وانحرافه على حدة, ويمكن القول انها تمثل الركيزة الاساسية في المحاكمات العادلة وفق ضمانات قانونية متاح للجميع.

([1]) سلمان شمران العيساوي, الدور الجنائي لمجلس الامن الدولي في ظل نظام روما الاساسي, مكتبة صباح, بغداد, 2012, ص116.

([2]) اسامة صبري محمد, فقدان المدنيين للحق في الحماية من الهجمات المباشرة, مجلة جامعة الانبار للعلوم القانونية والسياسية, العدد السادس, 2012, ص123.

المطلب الثاني: المسؤولية الجنائية المعنوية (الشركات ومزودو الخدمة):

وللتوضيح اكثر قمنا بتقسيم هذا المطلب الى عدة فروع والذي سوف نتناول في الفرع الاول موقف التشريعات من مسؤولية الشركات عن الجرائم السيبرانية, وفي الفرع الثاني مدى مسؤولية مزودي الخدمة, وفي الفرع الثالث حالات الاعفاء, اوالتخفيف, وبالشكل التالي:

الفرع الاول: موقف التشريعات من مسؤولية الشركات عن الجرائم السيبرانية: ان المسؤولية الجنائية المعنوية المترتبة على الشركات مزودي خدمات الانترنت في جرائم الإلكترونية, لذا ففي القانون العراقي لا يوجد حتى الآن قانون محدد يعالج الجرائم الإلكترونية بشكل شامل, لذا فان مع ذلك تتعامل الجهات الامنية مع تلك الجرائم استناداً الى بعض المواد من جانب القياس في قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل, والذي يتناول بعض الجرائم المتعلقة بإساءة استخدام اجهزة الاتصالات, وتحديد المسؤولية في الفضاء الرقمي, لكن هذا القانون لا يغطي تلك الجريمة تكيفاً دقيقاً,, علية ومن الجدير بالذكر ان هناك نقاشاً حول مشروع مقترح لقانون الجرائم الإلكترونية, والذي يواجه انتقادات لبعض مواده لقصورها على بعض الجرائم كون انها تنتهك لبعض الحريات من خلال اجراءات التحري للتدابير الاحترازية التي تتبع في عملية التعقب, وللمساهمين او من تقع حوله الشبهات في ارتكاب لتلك الجرائم[1].

الفرع الثاني: مدى مسؤولية مزودي الخدمة: ان الصفا الغالبة والمعمول بها على انه المسؤولية التقصيرية تقع على جميع المساهمين في ارتكاب اي جريمة,, اذ تتزايد اهمية تحديد مسؤولية مزودي خدمة الانترنت, في الجرائم السيبرانية, نظراً لتنامي استخدام شبكات الانترنت في انشطة الجرائم, وقد تخلف تلك المسؤولية باختلاف الدور الذي يؤديه المزود, سواء كانت متعهده, وصول, او مزود خدمة الانترنت, لذا فان المسؤولية لها اثار مدنية وجزائية في الفضاء الرقمي,, ومن اجل بيان تلك الاثار فان سوف اقوم بتقسيم تلك الى فرعين وبالشكل التالي:

(1) ادم عبدالجبار عبدالله بيدار, حماية حقوق الأنسان اثناء النزاعات المسلحة الدولية بين التشريعات والقانون, منشورات الحلبي الحقوقية, 2009, ص146.

اولاً: المسؤولية المدنية: لاسيما ان مزودي خدمة الانترنت تقع عليهم مسؤولية مدنية, اذا ثبت تقصيرهم المتعمد في اداء واجباتهم, والمتمثلة عدم اتخاذ التدابير الحيطة والحذر الفنية, او التنظيمية كافية لحماية البيانات,, او منع الاستخدام غير المشروع للخدمة, وقد تشمل تلك المسؤولية التعويض عن الاضرار المادية دون الاضرار المعنوية عليه, فأنها تلحق بالمتضررين, لذا فان بعض التشريعات تعتبر المزود مسؤولاً او تحمل جزء من المسؤولية عن المحتوى الغير مشروع, في حال كان على علم به ولم يتخذ الاجراءات اللازمة لإزالة او البلاغ عنه قد الامكان, عليه فان المسؤولية الجنائية تختلف لمزودي الخدمة بحسب التشريعات الوطنية, لذا ففي بعض الدول,, لا يحمل المزود اي مسؤولية بل تعفية في حال ثبت هناك حسن النية لدية, مالم يكون على علم بتلك الجريمة المرتكبة, لكن الحقيقة والواقع, يجب ان يتعرضوا الى المسؤولية في حال كان هناك علم او دراية بالموضوع,, اذ اقر الفقه الدولي في دليل تالين بالسلطة التي تملكها الدولة على البنية التحتية السيبرانية, والتي جاء فيه لا يجوز للدولة ان تسمح بمعرفتها, وعلمها باستخدام البنية التحتية السيبرانية, الواقعة في اقليمها, او التي تحت سيطرتها,, فان معيار المسؤولية وفق دليل تالين التفسيري ان شراء الادوات والمواد في مشاركة غير مباشرة في العمل العدائي, ولكن يكون في اطار اتجاه خبراء دليل تالين تلك الحركة تعتبر مشاركة مباشرة وتحديد المسؤولية في الفضاء الرقمي[1].

الفرع الثالث: حالات الاعفاء والتخفيف: ان لجميع الدول لها غاية تسعى لها الى تحقيق العدالة, من اجل سن قوانين لمواجهة تلك الجريمة, والمتمثل بجرائم التقنية المعلوماتية, ومكافحة جرائم الانترنت, كما توجد اتفاقيات دولية كاتفاقية بودابست حول الجريمة السيبرانية لسنة 2001,, وهي اول اتفاقية دولية تهدف الى تعزيز التعاون لمكافحة الجرائم الإلكترونية, لكنها لا تعالج الحرب السيبرانية بشكل مباشر, اذ كان مضمونها هي تنسيق الجهود الدولية لمكافحة الجريمة السيبرانية, لكن تكون اجراءات الاعفاء,, او التخفيف لدى الدول في لم يثبت تعاون مزود خدمة الانترنت, او لم يكن على علم او دراية في تلك الجريمة المرتكبة علية فان الصفة

(1) ايناس ابو حميرة, الاضرار الجانبية في النزاعات المسلحة في القانون الدولي الإنساني, مجلة العلوم القانونية والشرعية, جامعة الزاوية, ليبيا, العدد السادس, 2015, ص112.

الغالبة, وتحديد المسؤولية في الفضاء الرقمي, والاصل عدم مقصريه مزودي الانترنت من اي مسؤولية يجب اعفاءه من تلك الجرائم مالم يثبت العكس, والمتمثل بتواطؤه في المساهمة في ارتكاب افعال تجرمها القوانين[1].

يتضح لنا مما تم ذكره من المسؤولية الفردية, او الجماعية, وما دور الاعفاء عن تلك المسؤولية, اذ تتراوح تلك المسؤولية الفاعل الاصيل عن مزودي خدمة الانترنت,, بين المدنية والجنائية, اذ تعتمد على دورهم في تقديم الخدمة, ومدى تقصيرهم في اتخاذ التدابير اللازمة لمنع حدوث مثل تلك الجرائم السيبرانية,, لذا فمن المهم ان يكون هناك توازن بين حماية حقوق المستخدمين, الاصل هو ضمان عدم تحميل مزودي الخدمة مسؤولية غير مبررة عن افعال المستخدمين, في تحديد المسؤولية في الفضاء الرقمي.

المبحث الثالث: التحديات القانونية والقضائية

ان في ظل التقدم التكنلوجي, والتحول الرقمي العالمي, والمتسارع, اذ برزت الحروب السيبرانية, كأحد اخطر التهديدات التي تواجه الامن القومي, وسيادة الفضاء الرقمي للدول, عليه فان الحروب التقليدية تعتمد على الأسلحة والجنود, بل انتقلت الى ابعد من ذلك في تطور الميادين, والمتمثل بالفضاء الالكتروني,, حيث تشن الهجمات عبر الشبكات, وتستهدف البنية التحتية الحيوية, لذا فان المؤسسات الحكومية, الشركات الكبرى بل وحتى المواطنين, اذ ترافق تلك التحولات مجموعة من التحديات القانونية والقضائية, التي لم تكن منظومة القانون الدولي, مهيأة للتعامل معها بالشكل الكافي, علية ان للحروب السيبرانية هي استخدام التكنلوجيا الرقمية, لشن هجمات على انظمة المعلومات والاتصالات لدولة ما,, اذ يهدف الى احداث ضرر شلل في البنية التحتية, او جمع معلومات استخبارتية, فقد تأخذ تلك الهجمات عدة اشكال, لذا فان اغلب التشريعات الوطنية لم تصمم في الاصل لمواجهة الجرائم في الفضاء الرقمي, مما يخلق فجوات قانونية كما ان وتيرة تحديث القوانين ابطأ من تطور اساليب الجريمة السيبرانية, على

(1) اسماء ابراهيم علي الياسري, الوضع القانوني للشركات الأمنية الخاصة في القانون الدولي الإنساني (دراسة تطبيقية في العراق), رسالة ماجستير, جامعة كربلاء, 2014, ص75.

الرغم من وجود اتفاقيات دولية مثل اتفاقية بودابست لمكافحة الجريمة السيبرانية,, الا ان تفاوت التشريعات, ومحدودية تبادل المعلومات في تحديد الاختصاص المكاني والقانون الواجب التطبيق, وللتوضيح سوف نقوم بتقسيم هذا المبحث الى عدة مطالب, ففي المطلب الاول مشكلات الاثبات والتتبع الرقمي,, وفي المطلب الثاني الاطار التشريعي لمكافحة الجريمة السيبرانية, وبالشكل التالي:

المطلب الاول: مشكلات الاثبات والتتبع الرقمي:

لا يمكن حصر مشاكل الاثبات للتبع الرقمي بشكل دقيق, كون انها معاير غير ثابت, ومتجددة, ومتغيرة في نفس الوقت,, مما تشكل عائق امام الامن السيبراني, اذ من الصعب الوثوق بالأدلة الرقمية كون انها من السهل التلاعب بالملفات الرقمية, وكذلك التزييف, وظهور تقنيات الذكاء الاصطناعي مما جعل من الصعب التميز بين الحقيق والواقع, كما انه صعوبة الكشف والتعرف على هوية الفاعل,, لذا ففي الغالب ان الاشخاص الذين يستخدمون تلك الجرائم لطالما يستخدمون اسماء حركية, وفق عناوين مظللة, وحسابات مزيفة, وبالأخير عدم وجود معاير ثابت, وموحدة يمكن الاستناد عليها في الاثبات للكشف عن هوية الفاعلين للجرائم السيبرانية, وتحديد المسؤولية في الفضاء الرقمي[1], وللتوضيح اكثر سوف نقوم بتقسيمة الى عدة فروع بالشكل التالي:

الفرع الاول: صعوبات التحقيق في الجرائم السيبرانية: يواجه التحقيق في الجرائم السيبرانية,, صعوبات في الادلة الرقمية في تقديمها امام المحاكم اذ يتطلب تقنيات عالية, مما يعد عائقاً في بطء الاجراءات التقاضي, مقارنة بسرعة الهجمات السيبرانية, تحدث في ثوان ثم تنهي ولا يتم الكشف عنها الا بعد حدوثها اذ لا يمكن تفاديها, وبهذا فان اجراءات جمع الادلة امام المحاكم المختصة اشهر لعدة او لسنوات, ما يحد من فاعلية الرد القضائي, لذا فان الحرب السيبرانية تفرض, واقعاً جديداً يتجاوز قدرات النظم القانونية التقليدية,, وتكون هناك حاجة ماسة الى

(1) عبد محمد علي اسوادي, المركز القانوني للشركات الامنية في القانون الدولي الإنساني, مجلة رسالة الحقوق, جامعة كربلاء, السنة السادسة, العدد الثالث, 2014, ص85.

التطوير الاطار القانوني بصفة دولية, والعمل الى ادوات الاثبات في الفضاء الرقمي, اما اذا كان هناك اطار قانوني غير منتظم, وقاعدة قانونية رصينة, سيظل تلك الحروب السيبرانية, تخلخل انتهاك سيادة الدول بين الحين والاخر, لما لها اثر سلبي على كيان تلك الدول[1].

نستنتج انه الادلة الرقمية صعبت الاثبات, والتي تحتاج الى سلسة من اجراءات التحقيق لفهم تلك الحركات, وقبولها قانوناً, وبالأخير عدم قهم القضاة وكذلك المحامين لتلك التقنيات,, مما يضعف الاعتماد على الادلة في الفضاء الرقمي, كون ان الصعوبة التي يواجها القضاة, والمحامين لفهم وتتبع تلك الادلة, والتي غالباً ما تكون عرضة للتغير والاختفاء, فان هنا شبكة الانترنت تكون امتداد لسلسة من الامدادات العالمية,, من جماعات التهكر.

الفرع الثاني: دور الخبرة الرقمية: تلعب الخبرة الرقمية دوراً بارزاً وجوهرياً في الادلة الخاصة بالحرب السيبرانية, كونها تشكل الاساس في تحليل الهجمات, وتحديد مصادرها وفهم اهدافها, اذ تتكون ادوات الخبراء الرقمية من سجلات للدخول, وكذلك ذاكرة النظام وملفات الحفظ,, وبعض الاتصالات المشبوهة, فان كل تلك المواد تعمل على تفكيك البرمجيات الخبيثة لفهم طريقة عملها, في تحديد المسؤولية في الفضاء الرقمي, وما اذا كانت هناك خصائص تدل على جهة معينة, والمتمثل بلغات برمجية او ادوات معروفة لدول معينة, من خلال العمل الى تحديد الجهات الفاعلة من خلال دراسة نمط تلك الهجمات السيبرانية,, من توقيت وكذلك استخدام البنى التحتية, لتحليل تأثير الهجوم على حجم البيانات التي تم سرقتها او تدميرها, والمخلفات التي تتركها الجريمة السبيرانية في المنظومة الالكترونية[2].

يتضح لنا انه الخبرة الرقمية لا تقتصر على التعامل مع التقنية فحسب, بل تذهب الى ابعد من ذلك اذ تشمل ايضاً في فهم السياقات الجيوسياسي في الفضاء الرقمي, والاعمال اللوجستية للنظام السلوكية للمهاجمين,, والعمل الى الحد من القدرة على تقديم تقارير دقيقة,

---

([1]) جون- ماري هنكرتس ولويز دوزوالد-بك, القانون الدولي الانساني العرفي, المجلد الاول: القواعد اللجنة الدولية للصليب الاحمر, القاهرة 2007, ص62.

([2]) خديجة عرسان, الشركات الامنية الخاصة في ضوء القانون الدولي الإنساني, مجلة جامعة دمشق للعلوم الاقتصادية والقانونية, المجلد28, العدد الاول, 2012, ص209.

تساعد في اتخاذ قرارات استراتيجية, وبخلاف تلك الخبرة, تصبح محاولات التتبع والتحقيق في الحروب السيبرانية ضعيفة, ولا يمكن التعويل عليها في الاثبات.

المطلب الثاني: الاطار التشريعي لمكافحة الجريمة السيبرانية:

ان للتطور الهائل, والمتسارع للتقنيات المعلومات, والاتصالات, لعبت الجريمة السيبرانية دوراً بارزاً واحداً من اكبر التحديات التي تواجه الدول والمجتمعات في تحديد المسؤولية في الفضاء الرقمي, فقد تجاوزت الجرائم حدود المكان,, والزمان, واصبحت تتم عبر شبكة الانترنت بسهولة وسرعة, وبتكاليف رمزية, لذا اصبحت الحاجة ملحة الى تفعيل دور التشريعي, وفعال يهدف الى مكافحة تلك الجرائم والعمل الى ضمان الامن السيبراني, وحماية الافراد والمؤسسات, من اجل العمل الى وجود اطار قانوني, واضح يعد امراً بالغ الاهمية لمكافحة الجريمة السيبرانية,, وكذلك تحديد الافعال المجرمة حيث يوضح القانون ما يعتبر لجريمة الكترونية, في حماية الحقوق, والحريات من خلال الموازين بين مكافحة الجريمة, وضمان الخصوصية, من اجل التعزيز التعاون الدولي العابر للحدود[1], وللتوضيح اكثر سوف نقوم بتقسيمة الى عدة فروع وبالشكل التالي:

الفرع الاول: تحليل القوانين الوطنية: اما على مستوى التشريع الداخلي الدولي, فانه ينبغي القول بانه لا يوجد في ممارسات الدول ما يشير الى الاختصاص القضائي للجرائم السيبرانية, لكن تتحتم الضرورة الى توحيد الصف ضد الممارسات التي تشير لهذا الاختصاص بشان جرائم الانترنت,, لذا فان قضية (Toben) عام 2000 وهو اصحاب المدونات عبر الانترنت, والذي قام بنشر مقالات وافكار هن النازية, اذ تم رفض الانتهاكات المنسوبة للنازية, والتحريض على الكراهية, وعلى هذا الاساس تم اعتقال لانتهاك المادة (130) من القانون الجنائي الألماني, وبهذا فان الاثار الضارة باعتبار عنصراً من عناصر الجريمة التي حدثة في المانيا[2].

([1]) العقون ساعد, ظوابط سير الاعمال العدائية في القانون الدولي الإنساني, اطروحة دكتوراه, جامعة الحاج لخضر- باتية, الجزائر, 2014, 123.

([2]) حوبه عبدالقادر, الوضع القانوني للمقاتلين في القانون الإنساني, اطروحة دكتوراه, جامعة الحاج لخضر-باتية, 2013, ص26.

ان من خلال البحث يتضح لنا انه لا يحتوي قانون العقوبات العراقي على اي نص خاص بالجرائم السيبرانية,, في تحديد المسؤولية في الفضاء الرقمي, الا انه يطبق المبادئ العامة لتلك الجريمة, كما ان قانون الاتصالات رقم 94 لسنة 2004 يضع بعض الضوابط حول استخدام الاتصالات والانترنت, وان استخدامه كأساس لمعاقبة الشخص الفاعل في الجرائم السيبرانية, شبة غير محسوم, اما بما يخص التشريع الاردني فقد عرف:" بانها الافعال غير القانونية التي ترتكب باستخدام انظمة الحاسوب او الشبكة الإلكترونية, وتشمل مجموعة واسعة من الافعال والمتمثل بالاختراق, والاحتلال الإلكتروني, وسرقة البيانات, والتشهير عبر الانترنت, وغيرها", فقد كان قانون الجرائم الإلكترونية الاردني رقم 27 لسنة 2015, فقد عالج اهم الجرائم الإلكترونية من الدخول الغير المشروع الى الأنظمة, والاختراق الحاسوب,, وتكون العقوبة حبس ثلاثة اشهر في حال تم التعطيل او حذف تكون العقوب ستة اشهر, اما الاحتيال من سنة الى ثلاثة سنوات[1].

الفرع الثاني: الاتفاقيات الدولية: ان لدليل تالين للحروب السيبرانية الى ان الدولة تمارس ولايتها القضائية على اساس الوجود المادي او القانوني,, ان الطبيعة الخاصة للفضاء السيبراني, في تحديد المسؤولية في الفضاء الرقمي, والعمليات التي تجري من خلال هذا الفضاء, كما اتفاقية بودابست لعام 2001 الخاص بالجرائم الإلكترونية, وكذلك اتفاقية بودابست الثانية البروتوكول الثاني لعام 2021, وايضاً هناك مبادرات للأمم المتحدة الخاص لمكافحة استخدام تكنلوجيا المعلومات والاتصالات لأغراض اجرامية, ايضاً هناك بعض المبادرات الاقليمية, مثل اتفاقية مالابو لعام 2014 حول الامن السيبراني وحماية البيانات,, والذي من المؤمل لا يمنع اي دولة من حقها الشرعي في ممارسة سلطتها على الاشخاص والبنية التحتية السيبرانية, التي تقع على اقليمها, لذا فقد اشار الخبراء في دليل تالين الى صور اخرى من الولاية الاقليمية للدولة, في حالة العمليات السيبرانية, والمتمثل هي جنسية الفاعل, او جنسية الضحية, او تهديد الامن

(1) خديجة عرسان, مصدر سابق, ص87.

القومي للدولة, للانتهاك في القاعدة عالمية للقانون الدولي, في الولاية القضائية العالمية او الشاملة[1].

وبخصوص الجرائم السيبرانية الدولية فان للمحكمة الجنائية الدولية الخاصة بيوغسلافيا السابقة, اذ اتخذت نهجاً معيناً بشأن اختبار القضايا والانتهاكات القانون الدولي, اذ يتم تحديد معايير للمسؤولية في الفضاء الرقمي, من خلال خطورة الجرائم واعداد الضحايا, ومدة الجرائم ونطاق التدمير,, ودور الشخص الفاعل من خلال موقعه وسلطته, ومشاركته المزعومة في الجرائم الموجهة ضده في مرحلة التحقيق, اما في حالة عدم تمتع مرتكب هذه الجرائم باي منصب في الهرم الوظيفي للدولة, عليه فان المسؤولية الفردية عن المشاركة المباشرة في الهجمات السيبرانية, من خلال ارتكاب, الهجوم او مسؤولية القادة والرؤساء, او التحريض او قد تكون من خلال المساعدة على تنفيذ الهجمات السيبرانية[2].

فقد اشارة المادة (24) من دليل تالين في المسؤولية الجنائية التي تقع على عاتق الرؤساء في اعطاء الاوامر في الهجمات السيبرانية,, وان مفهوم دليل تالين بأن مفهوم القائدة لا يشمل العسكرين فقط, بل من الممكن ان يكون القائد مدنياً لا يحمل اي صفة عسكرية, او قد يكون في اعمال التحريض, او انه من المؤمل بان من شأن تحريضه على الاغلب بان يسبب جرائم دولية وفق السير العادي للأمور التي ينبغي الاشارة اليها في الجرائم, السيبرانية باي صفة كانت, والمتمثل بالقصد في تحقيق الضرر او معيار الكثافة في الهجوم على المعلومات للفضاء الرقمي, والمتمثل بفورية تحقق الضرر على اساس الفعل, سواء كانت من تقديم مساعدة من خلال تصميم, او تنفيذ,, او تشويش للهجوم, فقد ذهب دليل تالين في الحالة المشاركة المباشرة في الهجمات السيبرانية, من قبل جماعات منظمة ففي هذا الحالة يطبق بشأن نسبة تصرفاتهم

(1) فليح غزلان, المركز القانوني للأفراد اثناء اللاسلم في القانون الدولي, اطروحة دكتوراه, جامعة ابوبكر بلقايد, تلمسان, الجزائر, 2013, ص201.
(2) كريم محمد رضيمة, حماية المدنيين في زمن الحرب, رسالة ماجستير, كلية الحقوق, جامعة النهرين, 2008, ص35.

غير المشروعة دولياً, الى الدولة معيار السيطرة الكاملة,, في حالة المشاركة في الهجمات السيبرانية, من قبل جماعات متشتته في التنظيم او افراد[1].

ففي الولايات المتحدة الامريكية هي من الدول التي قامت بتشريع قوانين وتشكيل محاكم متخصصة لمعاقبة المشاركين مباشرة في العمليات سواء كان هؤلاء من مواطنيها ام من مواطني دول اخرى,, ففي عام 2001 انشئت صورة جديدة من الجرائم, وعقوباتها تحت تسمية القتل من قبل المقاتلين غير المتمتعين بالمزايا, ففي اطار الهجمات السيبرانية للفضاء الرقمي,, تتحمل الدولة المسؤولية القانونية الدولية للعمليات السيبرانية, التي تنسب اليها, والتي تشكل خرقاً لالتزام دولي[2].

نستنتج من خلال القانون الدولي في اطار الهجمات السيبرانية, يكون هناك التزام دولي بضمان احتراق الحقوق الشخصية للدول ضد الهجمات السيبرانية, بضمان احترام القانون الدولي وفق قواعد القانونية, الآمرة في القانون الدولي, في اهم الالتزامات التي تكفل عدم انتهاك المشاركة المباشرة وعدم الفرار من المسؤولية التقصيرية, للهجمات السيبرانية, وان معيار العلاقة الكافية في المسؤولية التقصيرية من جراء الجرائم السيبرانية, سواء من خلال التزويد بالأنترنت, او شراء المواد التي تدخل في عمليات الجريمة السيبرانية, والتي تلزم توفر شرط العلاقة العامة فيها,, الى عنصر الارتباط المباشر بعمل الجريمة السيبرانية, وان يكون متصلاً اتصالاً مباشراً بالعمليات العدائية, اي يكون الفعل مصمماً خصيصاً لدعم تلك الجريمة, وان مزودي تلك البرامج في التقنيات المشاركة في الهجمات لتلك الجرائم, اذ يتمثل المسؤولية عن تلك الجرائم السيبرانية.

الخاتمة

اولاً: النتائج:

(1) نادر اسكندر العسكري, تطور مفهوم المشاركة المباشرة في العمليات العدائية في القانون الدولي الإنساني, مؤسسة عامل وجامعة الحكمة, 2011, ص110.

(2) محمد حمد العسبلي, المركز القانوني لأسرى الحرب في القانون الدولي الإنساني, ط1, منشأة المعارف بالاسكندرية, 2005, ص35.

1. غياب تعريف قانوني موحد للحرب السيبرانية, اذ لا يوجد حتى اليوم اتفاق دولي ملزم يعرف بدقة ماهية الحرب السيبرانية, او يميز بين العمل العدواني السيبراني والاختراق غير العدائي, مما يخلق فجوة قانونية في المسالة والمحاسبة الفعالة.

2. نلاحظ هناك اشكالية تطبيق مبادى القانون الدولي الانساني (قانون النزاعات المسلحة, والمتمثل بمبدأ التمييز, والتناسب,, والضرورة العسكرية فيها, اذ يصعب تطبيقها على الفضاء الرقمي, بسبب صعوبة تحديد الجهة الفاعلة, وتقدير آثار الهجوم.

3. ان الهجمات السيبرانية تنتهك سيادة الدولة التي تقوم بالهجوم عليها, لذا فهي انتهاك معقداً, تقنياً, وقانونياً, خاص في ظل امكانيات, استخدام تقنيات اخفاء المصدر, في الاثبات في الفضاء الرقمي.

4. كما انها يتضح لنا فيها صعوبة تحديد المسؤولية الدولية, اذ يكون للدولة التي يشن عليها الهجوم قد تنكر مسؤوليتها, او تنفيذ عبر جهات غير حكومية من داخل تلك البلد دون علم ودراية بتلك الهجمات, وبشكل غير رسمي مما يصعب تحميلها لتلك المسؤولية في الفضاء الرقمي, امام المحاكم الدولية.

5. ضعف الدليل الرقمي في الاثبات للجريمة السيبرانية, امام المحاكم المختصة اذ يتطلب تقنيات عالية, عبر سلسلة من المواثيق الصارمة لضمان عدم التلاعب بها, هو امر لا يمكن التعويل عليه, في الهجمات السيبرانية كدليل مادي, للفضاء الرقمي.

ثانياً: المقترحات:

1. العمل على تعديل الاتفاقيات الدولية ومنها اتفاقية لاهاي لسنة 1907 وكذلك اتفاقية جنيف لعام 1949 والبروتوكول الاضافي لعام 1977 وميثاق الامم المتحدة من اجل استيعاب آليات او جرائم الإلكترونية, والمتمثلة بالهجمات السيبرانية في الفضاء

الرقمي, بغرض تجريم تلك الهجمات, وحالات الدفاع عن النفس, من قبل الدول التي تتعرض للهجوم.

2. اعداد برامج علم من قبل القائمين لتحديد آليات الادلة الرقمية وفق معايير الاثبات والدليل القطعي, لغرض ادانة اي جه من المحتمل مساهمتها بالاشتراك في تلك الجريمة.

3. العمل على اعداد مؤتمرات دولية راعية للتثقيف المجتمع الدولي, من خطورة الجرائم السيبرانية, والتحذير منها وعدم انتهاك الخصوصية الدولية والتي تعتبر انتهاك لتلك السيادة.

4. ان بط اجراءات التقاضي في تلك الجرائم, والذي يتطلب خبراء لكوادر متخصصة لمعرفة تقنية داخل المؤسسات في الفضاء الرقمي, ويتم من خلال التعاون الدولي, من اجل انضمام العراق الى الاتفاقيات الدولية, مثل اتفاقية بودابست للجريمة الإلكترونية.

5. نامل من المشرع العراقي اعداد قانون خاص بالجرائم السيبرانية, لتحديد المسؤولية في الفضاء الرقمي.

المصادر والمراجع

اولاً: الكتب:

1. انطونيو كاسيزي, القانون الدولي الجنائي, ط3 باللغة الانكليزية, 2013, ط1 باللغة العربية2015, ترجمة صادر ناشرون, بيروت.
2. جون ماري هنكرتس, القانون الدولي الانساني العرفي, المجلد الاول, لقواعد اللجنة الدولية للصليب الاحمر, مطبعة برنت للإعلان والدعاية, القاهرة, 2007.
3. هو دليل اكاديمي يطبق القانون الدولي على الفضاء السيبراني في سياق النزاعات المسلحة, سنة 2013.
4. محمد طه البشير, الوجيز في نظرية الالتزام في القانون المدني العراقي, الجزء الاول, (مصادر الالتزام), ط4, المكتبة القانونية, بغداد, 2010.
5. عبدالله سليمان, شرح قانون العقوبات, القسم العام, ديوان المطبوعات الجامعية, الجزائر, 2003.

6. عبدالرحمن خلفي, محاضرات في القانون الجنائي العام, دار الهدى للطباعة والنشر والتوزيع, الجزائر, 2013.

7. سلمان شمران العيساوي, الدور الجنائي لمجلس الامن الدولي في ظل نظام روما الاساسي, مكتبة صباح, بغداد, 2012.

8. ادم عبدالجبار عبدالله بيدار, حماية حقوق الأنسان اثناء النزاعات المسلحة الدولية بين التشريعات والقانون, منشورات الحلبي الحقوقية, 2009.

9. ايناس ابو حميرة, الاضرار الجانبية في النزاعات المسلحة في القانون الدولي الإنساني, مجلة العلوم القانونية والشرعية, جامعة الزاوية, ليبيا, العدد السادس, 2015.

10. نادر اسكندر العسكري, تطور مفهوم المشاركة المباشرة في العمليات العدائية في القانون الدولي الإنساني, مؤسسة عامل وجامعة الحكمة, 2011.

11. محمد حمد العسبلي, المركز القانوني لأسرى الحرب في القانون الدولي الإنساني, ط1, منشأة المعارف بالاسكندرية, 2005.

ثانياً: الرسائل والاطاريح:

12. اسماء ابراهيم علي الياسري, الوضع القانوني للشركات الأمنية الخاصة في القانون الدولي الإنساني (دراسة تطبيقية في العراق), رسالة ماجستير, جامعة كربلاء, 2014.

13. العقون ساعد, ظوابط سير الاعمال العدائية في القانون الدولي الإنساني, اطروحة دكتوراه, جامعة الحاج لخضر- باتية, الجزائر, 2014.

14. حوبه عبدالقادر, الوضع القانوني للمقاتلين في القانون الإنساني, اطروحة دكتوراه, جامعة الحاج لخضر- باتية, 2013.

15. فليح غزلان, المركز القانوني للأفراد اثناء اللاسلم في القانون الدولي, اطروحة دكتوراه, جامعة ابوبكر بلقايد, تلمسان, الجزائر, 2013.

16. كريم محمد رضيمة, حماية المدنيين في زمن الحرب, رسالة ماجستير, كلية الحقوق, جامعة النهرين, 2008.

17. جون- ماري هنكرتس ولويز دوزوالد-بك, القانون الدولي الانساني العرفي, المجلد الاول: القواعد اللجنة الدولية للصليب الاحمر, القاهرة 2007.

ثالثاً: البحوث المجلات:

1. عبد محمد علي اسوادي, المركز القانوني للشركات الامنية في القانون الدولي الإنساني, مجلة رسالة الحقوق, جامعة كربلاء, السنة السادسة, العدد الثالث, 2014.

2. محمد طاهر قاسم, الاساس القانوني للمسؤولية عن الأشياء الخطرة امام القضاء العراقي, مجلة الرافدين للحقوق, المجلد13, العدد49, السنة2016.

3. اسامة صبري محمد, فقدان المدنيين للحق في الحماية من الهجمات المباشرة, مجلة جامعة الانبار للعلوم القانونية والسياسية, العدد السادس, 2012.

4. خديجة عرسان, الشركات الامنية الخاصة في ضوء القانون الدولي الإنساني, مجلة جامعة دمشق للعلوم الاقتصادية والقانونية, المجلد28, العدد الاول, 2012.

رابعاً: القوانين:

1. قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.
2. قانون الاتصالات العراقي رقم 94 لسنة 2004.
3. قانون الجرائم الإلكترونية الاردني رقم 27 لسنة 2015.

خامساً: الاتفاقيات:

1. اتفاقية بودابست الثانية البروتوكول الثاني 2021.
2. اتفاقية مالابو 2014.
3. قانون دالتين لسنة 2013.
4. اتفاقية بودابست 2001.
5. التروتوكول الاضافي لعام 1977.
6. اتفاقية جنيف لعام 1949.
7. اتفاقيات لاهاي لعام 1907.