مجلة جامعة الانبار للعلوم القانونية والسياسية

اسم المقال: المكافحة القانونية للجرائم السيبرانية دراسة تحليلية
اسم الكاتب: د. هيرش فاضل شاكر
رابط ثابت: https://political-encyclopedia.org/index.php/library/6282
تاريخ الاسترداد: 2026/11/03 11:05 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة جامعة الانبار للعلوم القانونية والسياسية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

Journal of Anbar University for Law and Political Sciences
مجلة جامعة الانبار للعلوم القانونية والسياسية
P. ISSN: 2706-5804 E.ISSN: 2075-2024
Volume 13- Issue 2- September 2023 المجلد ١٣- العدد ٢ –ايلول ٢٠٢٣

Legal combating cybercrime, an analytical study

[1] Dr. Hersh Fadel Shaker
[1] Faculty of Law and Politics / Newroz University
Public international law

Abstract:

Under the light of the great development that the world is witnessing especially at the technological level, various governmental and non-governmental agencies worked to take an advantage of this development and some of them took an advantage of that in a positive way. On the contrary; there are other parties that have sought to exploit this development and the vast cyberspace that is somewhat out of control for other (Criminal) purposes. This led to the emergence of the so-called cybercrime. In view of the seriousness of these crimes at all levels, States have worked to enact legislation to combat this type of crime and this is also done by the international community (both Global and Regional) and this is through the issuance of declarations and the conclusion of agreements that work to reduce these crimes .

Here we would like to sign out an important point, which is that confronting these cybercrimes is an urgent necessity at the present time due to the danger these crimes pose to the lives of individuals as well as their effects on international peace and security.

Through studying on this subject, it has become clear to us that the efforts exerted in this regard need to be more serious than they are now to face the seriousness of these crimes, especially those related to terrorism, as the current efforts are characterized by shortcomings and the evidence is the noticeable increase in the rates of these crimes at the present time.

1: Email:
hershsamade@yahoo.com
2: Email

DOI

Submitted: 15/7/2023
Accepted: 09/08/2023
Published: 01/10/2023

Keywords:
Terrorism
Saudi Law
Electronic Crimes.

©Authors, 2022, College of Law University of Anbar. This is an open-access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

المكافحة القانونية للجرائم السيبرانية
دراسة تحليلية

[١] د. هيرش فاضل شاكر
[١] كلية القانون والسياسة / جامعة نوروز

الملخص:

في ظل التطور الكبير الذي يشهده العالم خصوصاً على المستوى التكنلوجي، عملت الجهات المختلفة الحكومية وغير الحكومية على استغلال هذا التطور ومنهم من استغل هذا التطور بشكل ايجابي، وعلى النقيض من ذلك هناك جهات اخرى سعت الى استغلال هذا التطور والفضاء الالكتروني الرحب البعيد عن السيطرة نوعاً ما لأغراض اخرى (اجرامية)، وهو ما ادى الى ظهور ما يسمى بالجرائم السيبرانية، وازاء خطورة هذه الجرائم على كافة المستويات عملت الدول على سن تشريعات لمواجهة هذا النوع من الاجرام وهذا ما قام به ايضاً المجتمع الدولي (العالمي والاقليمي) على حد سواء ، وذلك من خلال اصدار الاعلانات وابرام الاتفاقيات التي تعمل على الحد من تلك الجرائم .

وهنا نود الاشارة الى نقطة مهمة وهي ان مواجهة هذه الجرائم الالكتروني تعتبر ضرورة ملحة في الوقت الحاضر نظرا لما تشكله هذه الجرائم من خطورة على حياة الافراد فضلاً عن تأثيراتها على السلم والامن الدوليين .

ومن خلال دراسة هذا الموضوع تبين لنا ان الجهود المبذولة في هذا الصدد تحتاج الى جدية اكبر مما هي عليه الان لمواجهة خطورة هذه الجرائم وخصوصاً تلك المتعلقة بالإرهاب منها ، فالجهود الحالية تتصف بالقصور والدليل هي الزيادة الملحوظة في نسب هذه الجرائم في الوقت الراهن .

الكلمات المفتاحية:

الارهاب ، القانون السعودي ، الجرائم الالكترونية .

المقدمة

أولاً: التعريف بموضوع البحث :

لم تعد الجرائم كما كانت سابقاً محافظة على طابعها التقليدي المعروف والتي تحكمها القواعد القانونية النافذة في الدولة، بل أدى التطور التكنولوجي الذي اجتاح العالم الى إبراز وظهور انماط جديدة للجرائم يتم ارتكابها من خلال الفضاء الالكتروني، معتمدة على الانترنت والحاسوب، هذا الامر دفع الدول العربية والغربية منها الى مسايرة التطور وإصدار تشريعات خاصة بهذا النوع من الإجرام ، وقد سار على ذات النهج المجتمع الدولي (العالمي والاقليمي) ، ايضاً من اجل اعطاء تصور واضح عن الموضوع ارتأينا الى تقسيم المقدمة على النحو التالي :

ثانياً: أهمية موضوع البحث :

يحظى موضوع الإجرام السيبرانية بأهمية كبيرة جداً، وهذه الأهمية نابعة عن الزيادة الملحوظة في نسب واحصائيات هذا النوع من الإجرام الالكتروني، لذلك فأن أهمية موضوع البحث تنبع من أهمية الموضوع ذاته فهو (البحث) يتناول الدور المبذول من قبل التشريعات

الداخلية والدولية في مواجهة هذا النوع من الإجرام وهذا بحد ذاته يشكل أهمية تستوجب الدراسة بسبب ندرة المعالجات لهذا الموضوع .

ثالثاً: اشكالية موضوع البحث:

تتجسد الاشكلية الرئيسية للموضوع في نقص المعالجات القانونية التي عالجت هذا النوع من الجرائم، الامر الذي يتطلب اقتراح سبل للمعالجة توازي الخطورة التي تتصف بها هذه الجريمة .

رابعاً: اسئلة موضوع البحث :

يتمحور البحث حول مجموعة من الأسئلة لعل أهما ما يأتي :

١- ما المقصود بالجرائم السيبرانية وما هي أنواع هذه الجرائم ؟

٢- ما مدى فعالية وجدية التشريعات الداخلية في مواجهة الجرائم السيبرانية ؟

٣- هل بذل المجتمع الدولي جهوداً كافية للحد من الجرائم السيبرانية ؟

٤- ماهي الوسائل أو الآليات التي يمكن من خلالها الحد من هذا النوع من الإجرام؟

خامساً: منهجية موضوع البحث :

اعتمدنا في كتابة هذا البحث على المنهج التحليلي الذي يعول على تحليل النصوص التشريعية الداخلية والدولية بقصد بيان مدى فعاليتها وجدواها في مواجهة الجرائم السيبرانية، اي تحديد مواطن الخلل في تلك النصوص وبيان سبل تفعيلها .

سادساً: فرضية موضوع البحث :

تنطلق فرضية البحث من نقطة أساسية مفادها ان المعالجات أو الجهود المبذولة من قبل المجتمع الدولي والداخلي على حد سواء غير كافية لمواجهة الجرائم السيبرانية والدليل على ذلك ان هذه الجرائم في حالة زيادة مستمرة الامر الذي يستوجب ايجاد آليات اكثر نجاعة لمواجهتها بقصد مكافحتها أو الحد منها .

سابعاً: نطاق موضوع البحث :

المعروف ان الجرائم السيبرانية يتم مواجهتها على الصعيدين الدولي والداخلي ونحن وفي اطار هذه الدراسة سوف لن نميل الى التحديد في الاشارة الى المواجهة القانونية وانما سنتطرق الى كلا المعالجات اي على الصعيدين الداخلي والدولي .

ثامناً: هيكلية موضوع البحث :

بقصد الاحاطة بمفردات البحث من جوانبه كافة ارتأينا الى تقسيمه على مبحثين، حيث تم تخصيص المبحث الاول للبحث في ماهية الجرائم السيبرانية ، أما البحث الثاني فقد خصصناه للبحث في مواجهة هذه الجرائم على الصعيدين الدولي والداخلي .

I. المبحث الاول

ماهية الجرائم السيبرانية

يتضح لنا وبشكل جلي أن الجريمة السيبرانية آخذة في الازدياد والنماذج التقنية الحالية لمعالجة الجريمة السيبرانية غير فعالة في وقف الزيادة في الجرائم الإلكترونية، هذا يشير إلى أن هناك حاجة ماسة إلى مزيد من الاستراتيجيات الوقائية من أجل الحد من الجرائم الإلكترونية، مثلما هو مهم لفهم خصائص المجرمين من أجل فهم الدوافع وراء الجريمة ومن ثم تطوير ونشر استراتيجيات منع الجريمة، من المهم أيضا فهم الضحايا، أي خصائص مستخدمي أنظمة الكمبيوتر من أجل فهم الطريقة التي يقع بها هؤلاء المستخدمون ضحية للجرائم الإلكترونية، فمن المعروف العصر الحالي سريع جدا لاستخدام عامل الوقت لتحسين عامل الأداء، هذا ممكن فقط بسبب استخدام الإنترنت(١).

علماً ان الجريمة الالكترونية ليست جريمة قديمة، وانا هي جريمة حديثة النشأة قياساً على بقية أنواع الجرائم، وقد جرى تعريفها على انها أي نشاط إجرامي يحدث من خلال أجهزة الكمبيوتر أو الإنترنت أو أي تقنية أخرى معترف بها بموجب قانون تكنولوجيا المعلومات، هناك عدد من الأنشطة غير القانونية التي يتم إرتكابها عبر الإنترنت من قبل مجرمين مهرة تقنيا، وبوجه اوسع، يمكن القول أن الجريمة الإلكترونية تشمل أي نشاط غير قانوني حيث يكون الكمبيوتر أو الإنترنت إما أداة أو هدفا أو كليهما، الجريمة السيبرانية هي شر لا يمكن السيطرة عليه وله أساسه في إساءة استخدام والاعتماد المتزايد على أجهزة الكمبيوتر في الحياة الحديثة، حيث تتطور استخدام اجهزة الكمبيوتر والتقنيات الأخرى المرتبطة به في الحياة اليومية بسرعة وأصبح دافعا يسهل راحة المستخدم، كما إنه وسيط لا حصر له ولا قياس، ومن الامثلة على بعض الجرائم الإلكترونية التي ظهرت حديثا هي "المطاردة الإلكترونية والإرهاب السيبراني وانتحال البريد الإلكتروني وتفجير البريد الإلكتروني والمواد الإباحية الإلكترونية والتشهير الإلكتروني" وما إلى ذلك، وقد تندرج بعض الجرائم التقليدية أيضاً ضمن فئة الجرائم الإلكترونية إذا ما تم ارتكابها من خلال الكمبيوتر أو الإنترنت(٢) .

ومن الجدير بالذكر أن الجريمة الإلكترونية مصطلح يستخدم لوصف النشاط الإجرامي على نطاق واسع حيث تكون أجهزة الكمبيوتر أو شبكات الكمبيوتر أداة أو هدفاً أو

(١) يعرف مصطلح الإنترنت على أنه مجموعة من ملايين أجهزة الكمبيوتر التي توفر شبكة من الاتصالات الإلكترونية بين أجهزة الكمبيوتر، هناك الملايين من أجهزة الكمبيوتر متصلة بالإنترنت، يقدر الجميع استخدام الإنترنت ولكن هناك وجهًا آخر للعملة وهو الجريمة الإلكترونية عن طريق استخدام الإنترنت. للمزيد ينظر: Yerra Shankar Rao،Hemraj Saini ، T.C.Panda / International Journal of Engineering Research and Applications (IJERA) ISSN: www.ijera.com Vol. 2 ،Issue 2 ،Mar-Apr 2012 ،p.202.

(2) P. R.K.Chaubey، An Introduction to Cyber Crime and Cyber law، Kamal Law House،2012،p3.

مكاناً للنشاط الإجرام ي وتشمل كل شيء من الاختراق الإلكتروني إلى هجمات رفض الخدمة، كما أنها تستخدم لتشمل الجرائم التقليدية التي تستخدم فيها أجهزة الكمبيوتر أو الشبكات لتمكين النشاط غير المشروع، ويمكن للجريمة الإلكترونية أن توقف أي خط سكة حديد أينما كانت، وقد تضلل الطائرات في رحلتها عن طريق التضليل بإشارات خاطئة، وقد تتسبب في وقوع أي بيانات عسكرية مهمة في أيدي الدول الأجنبية، وقد توقف وسائل الإعلام الإلكترونية وبالتالي يمكن ان يؤدي ذلك الى انهيار نظام اية دولة من الدول مهما بلغت قوتها في غضون ثوان قليلة[١]. عليه ومن أجل الاحاطة بمفردات هذا المبحث ارتأينا الى تقسيمه على مطلبين حيث خصصنا المطلب الاول للبحث في مفهوم الجرائم السيبرانية، اما المطلب الثاني فسنتطرق من خلاله الى ذاتية هذه الجرائم وكما يأتي:

I.أ. المطلب الاول

مفهوم الجرائم السيبرانية

بداية لا بد ان نشير الى انه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الأخر يطلق عليها جريمة الاختلاس أو الاحتيال المعلوماتي، وآخرون يفضلون تسميتها بالجريمة المعلوماتية[٢]. الامر الذي يستوجب منا ايراد تعريف للجرائم السيبرانية مع بيان التطور التاريخي لها وذلك في الفرعين الآتيين:

I.أ.١. الفرع الأول

التأصيل التاريخي للجرائم السيبرانية

تعود جذور الجرائم الإلكترونية الى الوقت الذي تم فيه إنشاء شبكات الكمبيوتر الأولية وفي نفس الوقت بسبب نمو الحوسبة الشخصية ، كانت هذه الأحداث بمثابة توسع في الجريمة الإلكترونية، حيث نشأ الهاكرز الرواد في (معهد ماساتشوستس للتكنولوجيا) في عام (١٩٦٠) وفي عام (١٩٦٣) وعلى الرغم من أن المصطلح كان يهدف إلى وصف الاستخدام الخيالي للتلاعب بأجهزة الكمبيوتر، الا انه ومع مرور السنين، اكتسب المصطلح دلالة مختلفة ارتبطت بإحداث الأضرار بأنظمة المعلومات وأجهزة الكمبيوتر، وقد ذكر أينار ستيفرود في هذا السياق أنه وفي عام (١٩٧٨) ، أرسل أول بريد إلكتروني كرسائل غير مرغوب فيها، كانت شركة المعدات الرقمية هي التي ارتكبت هذه الإساءة باستخدام قائمة توزيع شبكة وكالة مشروعات الأبحاث المتقدمة للإعلان عن كمبيوتر جديد، وكانت السويد من الدل المتقدمة

(1) Nayak، S. D.Impact Of Cyber Crime:Issuues and CHallenges ،October 2013،pp.2-3.

(٢) سامي الشوا، *ثورة المعلومات وانعكاساتها على قانون العقوبات*،ط١، (القاهرة: دار النهضة العربية، ١٩٩٤)، ص٤.

والسباقة التي سنت قانوناً يحمي البيانات يسمى "قانون البيانات السويدية لعام (١٩٧٣)، وينص على أنه يجب حماية البيانات ضد أي وصول غير مصرح به.

وكانت الولايات المتحدة الأمريكية ثاني دولة تسن قانونا لمعاقبة الجرائم الإلكترونية، تم تقديم هذا القانون من قبل السناتور (أبي ريبيكوف) وتم التصديق عليه كـ "قانون حماية أنظمة الكمبيوتر الفيدرالي لعام (١٩٧٧)، كل هذه الأحداث المعزولة كانت حاسمة لإدخال الطب الشرعي الحاسوبي والطب الشرعي الرقمي، ويعتبر كلاهما علم وفن، كان (روبرت موريس جونيور) أول مجرم إلكتروني يخضع للمحاكمة وحكم عليه في عام (١٩٨٩) بموجب "قانون الاحتيال وإساءة استخدام الكمبيوتر لعام (١٩٨٦)[١].

اما بالنسبة للهند فقد تطورت الجريمة الإلكترونية فيها من دودة موريس إلى أدوات الفدية، وتعمل العديد من الدول بما في ذلك الهند على وقف مثل هذه الجرائم أو الهجمات، لكن هذه الهجمات تتغير باستمرار وتؤثر على الدول كافة [٢].

ومن الجدير بالذكر أن أول جريمة إلكترونية مسجلة كانت في عام (١٨٢٠)، وهذا ليس مفاجئاً بالنظر إلى حقيقة وهي أن العداد الذي يُعتقد أنه أقدم شكل من أشكال الكمبيوتر ، كان موجودًا منذ (٣٥٠٠) قبل الميلاد في الهند واليابان والصين، ومع ذلك، فقد بدأ عصر أجهزة الكمبيوتر الحديثة بالمحرك التحليلي لتشارلز باباج في عام (١٨٢٠)، حيث أنتج جوزيف ماري جاكار صانع المنسوجات في فرنسا، هذا الجهاز الذي يسمح بتكرار سلسلة من الخطوات في نسج الأقمشة الخاصة، وهو ما أدى ذلك إلى اشاعة الخوف بين موظفي جاكار من أن عملهم التقليدي وسبل عيشهم يتعرضون للتهديد، [٣].

I.أ.٢. الفرع الثاني

تعريف الجرائم السيبرانية

بداية نود التنويه الى انه وبالرغم من مرور وقت طويل نسبياً على ظهور الجرائم الإلكترونية الا أنه لا يزال هناك اختلافاً كبيراً بين الأكاديميين وخبراء أمن الكمبيوتر ووكالة إنفاذ القانون والمستخدمين فيما يتعلق بالتعريف الحقيقي للجريمة الإلكترونية، حيث هناك

(1) REGNER SABILLON، JEIMY CANO، VICTOR CAVALLER، JORDI SERRA،Cybercrime and Cybercriminals: A Comprehensive Study،VOL. 4، NO. 6، JUNE 2016،p.166.

(2) Krishnan، Dolly & Mohit Verma، Cyber security And Cyber Laws around the World and India: Major Thrust Highlighting Jharkhand for Concerns، Indian Politics & Law Review Journal، The Law Bridge Publishers، 20th July،(2020)،p.23.

(3) Baiden، John E. "Cyber Crimes، A PAPER PRESENTED ON: CYBER LAWS IN PAKISTAN; A SITUATIONAL ANALYSIS AND WAY FORWARD June 24، 2006،p.9.

تباين في وجهات النظر حول ماهية الجريمة الإلكترونية ومما لا شك فيه أن عدم الوضوح في التعريف له تأثير على كل جانب من جوانب الوقاية من الجريمة الإلكترونية ومعالجتها[١]، هذا وأن عدم الوضوح في التعريف لا ينكر بعض المحاولات التي بذلت في هذا السياق الا ان هذه المحاولات لم تنجح في وضع تعريف مانع وجامع للجريمة الالكترونية ، ومن الجدير بالذكر أن الجرائم الإلكترونية يمكن إدراجها تحت ثلاث فئات، الأولى هو عندما تصبح أنظمة تكنولوجيا المعلومات والاتصالات والملكية الفكرية أهدافاً للاستغلال والتطفل وسرقة الهوية وسرقة المعلومات، والثانية هو استخدام أجهزة تكنولوجيا المعلومات والاتصالات كوسيلة لارتكاب الجرائم، وعلى سبيل المثال، تُستخدم أجهزة الكمبيوتر في المنزل لتشغيل برامج ضارة للتطفل على أجهزة الكمبيوتر الأخرى لسرقة الأموال والهوية وكلمات المرور، والفئة الثالثة هي استخدام أجهزة الاتصالات وتكنولوجيا المعلومات كوسيلة لارتكاب الجرائم، على سبيل المثال، تندرج الفتنة والتنافر والاضطراب والافتراء والتحريض على نطاق أوسع ضمن هذه الفئة، ويقول بعض الناس أنه يجب محاكمة هذه القضايا بموجب قوانين الإنترنت، ولكن هل هناك بالفعل قوانين يمكن استخدامها للتعامل مع هذه القضايا، على سبيل المثال، التحريض على الفتنة والقذف، يمكن اتهام المرء بموجب قانون العقوبات[٢]، على العموم سنشير في هذا الفرع الى تعريف الجرائم السيبرانية لغة واصطلاحاً في فقرتين مستقلتين وكما يأتي:

هذا وعلى الرغم من محاولات الخبراء والدول والمنظمات الدولية والتحالفات الإقليمية لوضع تعريف موحد للعمليات السيبرانية ، لم يتم تحديد الاستقرار بشكل عام، بالنسبة للولايات المتحدة وحلف شمال الأطلسي، فإن الجوانب الاقتصادية والمادية للجرائم الإلكترونية مركزة ، على عكس السيادة الوطنية لمنظمة شنغهاي للتعاون والحفاظ على الحدود والهوية الثقافية للشعوب، من القانون الدولي في مجالات الصراع والحرب تنص (Cyberanism) على أن "كل جرائم الإنترنت، سواء كانت دفاعية أو هجومية ، يُعتقد أنها تسبب إصابة أو موت للإنسان أو ضرر للأشياء المادية[٣].

وقبل التطرق الى تعريف الجرائم السيبرانية على الصعيد الفقهي نود الاشارة الى أن مصطلح السيبرانية هي كلمة انجليزية مشتقة من كلمة (Cyber) وتعني: مرتبط بالحاسوب أو

(1) Sarah Gordon، Richard Ford، On the Definition and Classification of Cybercrime. Springer-Verlag France،Vol 2،(2006)،p.3.
(2) Hong Lu، Bin Liang، Melanie Taylor، A Comparative Analysis of Cybercrimes and Government Law Enforcement in China and United States. Published in Springer Science،2010،p.4.
(3) Michael N.Schmitt، Tallinn Manual on the International Law Applicale to Cyber Warfare، Prepared by the International Group of Experts at the Invitationof the NATO cooperative cyber defence Center of excellence، Cambridge University press، 2013،p.91.

شبكات الحاسوب، وقيل: كلمة يونانية مشتقة من كلمة (kybernetes) وتعني: الشخص الذي يدير دفة السفينة، مجازاً للمتحكم[١].

وقد اورد الفقهاء لهذا المصطلح جملة من التعاريف، حيث يعد وليام جيبسون (William Gibson) أول من أستخدم كلمة (cyber) مقترنة بكلمة(Space) لتظهر في مصطلح الفضاء السيبراني (cyber space) في كتابة الكلاسيكي في عام (١٩٨٢)[٢].

يشكل مصطلح الجرائم الإلكترونية[٣] أفعالًا غير قانونية حيث يكون الجهاز الرقمي أو نظام المعلومات إما أداة أو هدفًا أو مجرد مزيج من الاثنين. يمكن استخدام تعبير الجرائم الإلكترونية بالتبادل إما كجريمة كمبيوتر ، أو جريمة إلكترونية ، أو جرائم تقنية عالية ، أو جريمة عصر المعلومات ، أو جرائم إلكترونية ، أو جرائم متعلقة بالحاسوب ، أو جرائم رقمية[٤].

ويمكن أيضاً تعريف مصطلح الجريمة الإلكترونية على أنها فعل تم ارتكابه أو حذفه في انتهاك لقانون يحظره أو يأمر به ويتم فرض العقوبة عليه عند الإدانة، تمثل الكلمات الأخرى الجريمة الإلكترونية على أنها "نشاط إجرامي مرتبط بشكل مباشر باستخدام أجهزة الكمبيوتر، وتحديداً التعدي غير القانوني على نظام الكمبيوتر أو قاعدة بيانات أخرى ، أو التلاعب أو سرقة البيانات المخزنة أو عبر الإنترنت، أو تخريب المعدات والبيانات، فضاء

(١) عبدالعزيز بن فهد محمد بن داود، "الجرائم السيبرانية : دراسة تأصيلية مقارنة"، *بحث منشور في مجلة الاجتهاد للدراسات القانونية والاقتصادية*، المجلد ٩، العدد ٣، (٢٠٢٠): ص١٤٨.

(٢) ليون برخو، "الهاكطولوجيا ودورها في تفسير الهجمات الالكترونية وتأثيرها على الممارسة الصحفية دراسات اعلامية"، مركز الجزيرة للدراسات،٢٠١٧، متاح على الموقع الالكتروني التالي : https://studies.aljazeera.net/ar/mediastudies/2017/11/171102072849895.html تاريخ الزيارة ٢٠٢٣/٧/٧.

(٣) في حين أن معنى مصطلح "الهاكر" قد تغير على مدى العقود الماضية ، فإن تصور أنشطة هذه المجموعة يُنظر إليه في الغالب على أنه مظلمة وشريرة وتعمل في بيئات تحت الأرض وخاصة بهدف إحداث ضرر لأنظمة معلومات المجتمع. المتسللون هم الوكلاء الرئيسيون في أنشطة الجرائم الإلكترونية. يمكن أن تكون دوافعهم من مجرد الاستمتاع الشخصي - مثل أطفال البرامج النصية الذين يقومون بتشويه مواقع الويب وكسر كلمات مرور الوصول ، إلى ما يرضي الاعتراف بهم كقراصنة من النخبة من خلال كسر الأمن السيبراني والسرقة. للمزيد ينظر:

B. Arief، M.A. Bin Adzmi، and T. Gross،Understanding Cybercrime from Its Stakeholders‘ Perspectives: Part 1—Attackers،‖ IEEE Security & Privacy، vol. 13، no. 1،2015، p.71

(4) United Nations Office on Drugs and Crime - UNODC (2013). Comprehensive study onCybercrime‖.Vienna،Austria<https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

الإنترنت أو الفضاء السيبراني ينمو بسرعة كبيرة وكجرائم الإنترنت، بعض أنواع مجرمي الإنترنت مذكورة أدناه[١].

ويعرف بعض الفقه المختصين في القانون الدولي بأنه: استخدام الطيف الإلكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجهاً لوجه مع الانظمة التي تحكم البنى التحتية[٢].

و عرف الفقيهان (Sussman) و(Haston) مصطلح الجرائم الإلكترونية في عام (١٩٩٥) بأنها "مجموعة من الأفعال أو السلوكيات حيث تستند هذه الأفعال إلى العنصر المادي للجريمة وطريقة العمل التي تؤثر على بيانات الكمبيوتر أو الأنظمة، ويشكل مصطلح الجرائم الإلكترونية أفعالًا غير قانونية حيث يكون الجهاز الرقمي أو نظام المعلومات إما أداة أو هدفا أو مجرد مزيج من الاثنين..." [٣].

كما عرفها الفقيه (Fuertes) بالقول بأنها، هجوم عبر الإنترنت يقوم على التسلل الى مواقع إلكترونية غير مرخص بالدخول اليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى[٤].

أما الفقيه ماركو روسيني (Marco Roscini) فقد عرفها بأنها: تطويع الإمكانيات الإلكترونية العسكرية لأجل التأثير في مواقع أخرى وتعطيلها وتدميرها سواء أكانت تقدم خدمات مدنية أو عسكرية[٥]. وعرفها

ووصف بابو وباريشات (Babu & Parishat، M.) الجريمة الإلكترونية بأنها: نشاط إجرامي يُرتكب على الإنترنت[٦]، بينما وصف مويترا (Moitra) حالات الجرائم الإلكترونية التي يكون فيها الإنترنت متورطا[٧]، هذا ويتفق العديد من الباحثين على أن

(1) Bowen، Mace (2009)، Computer Crime، Available at: http://www.guru.net/، Visited: 5/07/2023.
(2) Shin، Beomchul، "The Cyber Warfare and the Right of self- Defense: Legal perspectives and the Case of the United States، IFANS، VOI.19، N1، June 2011،p.6.
(3) McQuade، III، S.Understanding and managing cybercrime‖، Boston: Pearson/Allyn and Bacon،(2006)،p.128.
(4) Micheal S.Fuertes، "Cyber warfare، Unjust Actins in a just war"، Florida International University، Full 2013، p.1.
(5) Marco Roscini، "World Wide Warfare- Jus ad bellum and the use of Cyber Force"، Max Planck Yearbook of United Nations Law، Volume 14، 2010، p.91.
(6) Babu، M.، & Parishat، M. (2004). What is cybercrime? Retrieved August 8، 2023، Available from http://www.crime research.org/analytics/702./
(7) Moitra، S. Developing Policies for Cyber crime. European Journal of Crime، Criminal Law and Criminal Justice،(2005)،p.435.

الجريمة الالكترونية هي الأنشطة غير القانونية التي يتم إجراؤها باستخدام الكمبيوتر كوسيلة وشبكة الإنترنت كموقع لوقوع الجريمة [١].

ونحن من جانبنا يمكن ان نعرف الجريمة السيبرانية على أنها " هي الجريمة التي ترتكب عن طريق الانترنيت وباستخدام الاجهزة الالكترونية كالحاسوب او الهاتف المحمول".

I.ب. المطلب الثاني

ذاتية الجرائم السيبرانية

تمتاز الجرائم السيبرانية بجملة من الخصائص التي تعبر عن ذاتية هذه الجريمة ، كما انها (الجريمة السيبرانية تقسم الى عدة أنواع ، عليه وبقصد الاحاطة بخصائص الجريمة السيبرانية وأنواعها ارتأينا الى تقسيم هذا المطلب على فرعين وكما يأتي :

I.ب.١. الفرع الاول

خصائص الجرائم السيبرانية

إن طبيعة الجرائم السيبرانية[٢] وتمييزها عن الجرائم التقليدية يرجع إلى الوسط الذي ترتكب فيه الجريمة وهي الآداة أو الوسيلة التي استخدمها الجاني في ارتكاب فعله غير المشروع، وتتطلب توفر معرفة أو حد ادني من الثقافة التقنية لدى الجاني، وهي لا تخرج عن كونها سلوك إجرامي ينشأ بارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون، وتتجه إرادة الجاني إليه رغم وجود نص قانوني يجرم السلوك[٣].

إن الجريمة السيبرانية تتميز بعدة خصائص منها :

أولا : جرائم ترتكب بواسطة الأجهزة الاكترونية كالحاسب الالي والهواتف الخلوية :

وهما الأداتان التي تمكن المجرم من دخول الإنترنت لتنفيذ جريمته.

(1) S. Philippsohn. Trends in Cybercrime—An Overview of Currentfinancial Crimes on the Internet. Computers & Security، (2001)، p.53.

(٢) صور الجرائم السيبرانية:١- الاختراق.٢- التعطيل.٣- التعديل.٤- الدخول غير المشروع.٥- الاستخدام غير المشروع. ٦- الاستغلال. للمزيد ينظر: أبو بكر محمد بن الحسن بن دريد الأزدي، رمزي منير بعلبكي، الناشر: دار العلم للملايين ، ط١،١٩٨٧ بيروت، ص١٢١.

(٣) احمد طارق عفيفي صادق، *الجرائم الالكترونية جرائم الهاتف المحمول*، (القاهرة: المركز القومي للإصدارات القانونية، ٢٠١٥)،ص٢٤.

ثانيا : جرائم خفية :

فليس من السهولة اكتشافها لضعف القدرة الفنية للضحية وذلك مقارنة بالمجرم ، ولربما أيضا لمهارات المجرم الفنية والعلمية المتقدمة لقدرته على إخفائها ، أو لخوف الضحية من الإبلاغ عن الجريمة تجنبا للإساءة الى السمعة[١].

ثالثا : جرائم سريعة التنفيذ :

فسرعة ارتكاب الجريمة قد تكون خلال جزء من الثانية ، وقد لا تتطلب الإعداد قبل التنفيذ .

رابعا : جرائم عن بعد :

فيمكن للجاني تنفيذ جريمته وهو في دولة بعيدة كل البعد عن المجني عليه[٢].

خامسا : جرائم عابرة للحدود :

فهي لا تعرف الحدود الجغرافية للدول ، لارتباط العالم بشبكة واحدة ، وهذا قد يسبب إشكاليات لدى الاختصاص القضائي من حيث التحقيق والمحاكمة، وذلك تبعا لتعقيد الإجراءات التي تحكمها الاتفاقيات والمعاهدات والعلاقات الدولية، والتنازع فيما بينهما على أي القانون الواجب التطبيق .

سادسا : جرائم صعبة الإثبات :

وتكمن " صعوبة إثباتها إلى أن متابعتها واكتشافها عن طريق الصدفة ، ومن الصعوبة حصرها في مكان معين ، حيث أنها لا تترك أثرا واضحا للعيان ، أو المشاهدة بالعين المجردة ، فما هي إلا أرقام تدور في السجلات والمواقع الاكترونية ، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها ، وتعود صعوبتها لأسباب عديدة اهمها :

١ -إنها كجريمة لا تترك أثرا بعد ارتكابها .
٢ -صعوبة الاحتفاظ الفني بآثارها إن وجدت .
٣ -تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها .
٤ -تعتمد على الخداع في ارتكابها ، والتضبيب في التعريف على مرتكبيها .

---

(١) محمود أحمد القرعان ، *الجرائم الإلكترونية* ، ط١ ، (عمان: الاردن، دار وائل للنشر والتوزيع ، ٢٠١٧)،ص١٩.

(٢) تميم عبدالله سيف التميمي ، *الجرائم المعلوماتية في الاعتداء على الأشخاص* ، ط١، ، (الرياض: مكتبة القانون والاقتصاد ، ٢٠١٦)،ص١٦.

٥ -تعتمد على مستوى من الذكاء المرتفع في ارتكابها.

سابعا : جرائم ناعمة :

فهي جرائم لا تمارس بالعنف ، ولا تحتاج إلى أدني مجهود عضلي ، بعكس بعض الجرائم التقليدية[١]. ويختلف مفهوم الجريمة الإلكترونية اختلافاً كبيراً عن الجريمة التقليدية، بسبب نمو تقنية الإنترنت لذا اكتسبت هذه الجريمة اهتماماً خطيراً وغير مقيد مقارنة بالجريمة التقليدية، لذلك من الضروري فحص الخصائص المميزة للجرائم الإلكترونية.

I.ب.٢. الفرع الثاني
أنواع الجرائم السيبرانية

سنتناول في هذا الفرع التمييز بين الجرائم السيبرانية والجرائم العادية ومن ثم سنتطرق الى أنواع الجرائم السيبرانية في فقرتين مستقلتين وكما يأتي :

تتنوع الجرائم السيبرانية[٢] بحسب النظر إليها، فبالنظر إلى قصد الجاني تقسم هذه الجرائم الى: عمدية وغير عمدية، وبالنظر إلى وقت الجريمة تقسم الى : متلبس بها وغير متلبس بها، وبالنظر إلى جسامتها تقسم هذه الجرائم الى: جسيمة وغير جسيمة، وبالنظر إلى مصدرها جرى تقسيمها الى : وطنية في حال أن منصات الهجوم أو القائمين عليها داخل البلد المستهدف وعالمية في حال أن منصات الهجوم أو القائمين عليها خارج البلد المستهدف[٣]. عليه وبشكل عام يمكن اجمال أنواع الجرائم السيبرانية بما يأتي :

اولاً : الإرهاب السيبراني[٤]: يتضمن الإرهاب السيبراني استخدام الإنترنت في الإرهاب أو الهجمات الإرهابية.

ثانياً : الاختطاف بمساعدة الإنترنت: هذه ليست أخبارًا عن تزايد عمليات الاختطاف ، فالكثير منهم لا يدركون أن الخاطفين يتلقون المساعدة من خلال أنشطة ضحاياهم على وسائل

---

(١) روان بنت عطية هلا الصحفي، "الجرائم السيبرانية"، *بحث منشور في مجلة الإلكترونية الشاملة متعددة التخصصات*، المجلد ١،العدد ٢٤ ، بدون بلد النشر،(٢٠٢٠): ص١٢.

(٢) أسباب الجرائم السيبرانية:١- تهديد للأمن القومي والعسكري.٢- الاستيلاء على المعلومات.٣- قهر النظام واثبات التفوق على تطور وسائل التقنية.٤- تحقيق الأرباح والمكاسب المادية. للمزيدد ينظر:
Moses A. A. and Hight C. I، 'Cyber Crime Detection and Control Using the Cyber Under Identification Model'، International Journal of Computer Science and Information Technology and Security، Vol5،2015، Issue-5، p.354.

(٣) د .عبد العزيز بن فهد بن محمد بن داود، "الجرائم السيبرانية : دراسة تأصيلية مقارنة"، *بحث منشور في مجلة الاجتهاد للدراسات القانونية والاقتصادية*، المجلد ٩، العدد ٣، (٢٠١٩): ص١٥٠.

(٤) المقصود بالإرهاب السيبراني: العدوان أو التخويف أو التهديد مادياً أو معنوياً بإستخدام الوسائل الالكترونية الصادرة من دول أو جماعات على الانسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق بشتى صنوفه وصور الأفساد في الأرض. للمزيد ينظر: أيسر محمد عطية، "دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الالكتروني وطرق مواجهته"، *ورقة بحثية مقدمة في الملتقي العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية*، *عمان، الاردن*، (٢٠١٤): ص٩.

التواصل الاجتماعي وبيانات تحديد الموقع الجغرافي على هواتفهم الذكية، بيانات تحديد الموقع الجغرافي هي معلومات يمكن استخدامها لتحديد الموقع المادي لجهاز إلكتروني باستخدام الهواتف الذكية المدمجة في وظيفة نظام تحديد المواقع العالمي (GPS)، مما يسمح للخدمات القائمة على الموقع باكتشاف ونشر معلومات عن المالكين، بدأ الخاطفون في استخدام المواقع الجغرافية والعلامات الجغرافية للتعرف على ضحاياهم.

ثالثاً : سرقة الهوية الاحتيالية: هو عمل إجرامي يقوم فيه شخص ما باسترداد معلومات مهمة من خلال التظاهر بأنه شخص آخر، وعلى سبيل المثال، إنشاء صفحة ويب بنك خاطئة لاسترداد معلومات حساب الفرد، المفهوم بسيط، يكتسب الشخص إمكانية الوصول إلى معلوماتك الشخصية ويستخدمها لمصلحته الخاصة، مثل أشياء فريدة مثل الأرقام التعريفية واستخدامها لارتكاب جريمة[١].

رابعاً : المواد الإباحية على الإنترنت: يعد استخدام الويب في الاعتداء الجنسي من الاهتمامات البحثية النشطة للغاية، لقد وجد أن المواد الإباحية على الإنترنت هي اتجاه مزعج خاصة بين الشباب حيث تم استخدام برامج تصفية الويب للكشف عن المواد الإباحية على الإنترنت في البلاد، يحتوي على صور فاحشة وصور وكتابات وما إلى ذلك، وهناك أيضا استخدام الإنترنت للتنزيل والبث بحيث يتم استخدام الإنترنت لجذب الأطفال غير المشتبه بهم في إساءة معاملة الأطفال وتوزيع المواد الإباحية الخاصة بالأطفال. اتجاه آخر هو استخدام الهواتف المحمولة والإنترنت للبغايا. لذلك ، فإن البغايا الآن يعلنون عن أعمالهم عبر الإنترنت ، ويعرضون أجزائهم الحساسة والجنسية والخاصة لمستخدمي الإنترنت.

خامساً : القرصنة: يستخدم المتسللون نقاط الضعف والثغرات الموجودة في نظام التشغيل لتدمير البيانات وسرقة المعلومات المهمة من كمبيوتر الضحية. يتم ذلك عادةً باستخدام برنامج مستتر مثبت على جهازك. يحاول العديد من المتسللين الوصول إلى الموارد من خلال برامج اختراق كلمات المرور، يمكن للقراصنة أيضا مراقبة ما تفعله على جهاز الكمبيوتر الخاص بك واستيراد الملفات إلى جهاز الكمبيوتر الخاص بك، يمكن للمتسلل تثبيت العديد من البرامج على نظامك دون علمك، يمكن استخدام هذه البرامج لسرقة المعلومات الشخصية مثل كلمات المرور ومعلومات بطاقة الائتمان، يمكن أيضا اختراق البيانات المهمة للشركة للحصول على معلومات سرية حول خطط الشركة المستقبلية[٢].

(1) Sunil. C. Pawar، Dr. R. S. Mente & Bapu. D.Chendage،Cyber Crime، Cyber Space and Effects of Cyber Crime،nternational Journal of Scientific Research in Computer Science، Engineering and Information Technology،Volume 7، Issue 1،February-2021، pp.212-213

(2) Krishnan، Dolly & Mohit Verma، Cyber security And Cyber Laws around the World and India: Major Thrust Highlighting Jharkhand for Concerns، Indian Politics & Law Review Journal، The Law Bridge Publishers، 20th. July،(2020)،p.23

II. المبحث الثاني

المواجهة القانونية للجرائم السيبرانية

كان للاتفاقيات الدولية والإقليمية، الأثر البالغ على تشريعات العديد من دول العالم، حيث قامت هذه الأخيرة بتبني فكرة الحماية الجزائية لمستخدمي الأنترنت وكذا البيانات المخزنة في النظم المعلوماتية، وعليه سنتطرق من خلال هذا المطلب لأبرز النماذج التشريعية العربية والغربية، حيث خصصنا المطلب الاول المواجهة في اطار التشريعات الوطنية، اما المطلب الثاني فقد تطرقنا من خلاله الى المواجهة الدولية للجرائم السيبرانية وكما يلي :

II.أ. المطلب الاول

المواجهة في اطار التشريعات الوطنية

لقد حاولت عدة أعمال أكاديمية بيان مفهوم السيبرانية"، وفي هذا الصدد، لم يبد التشريع الوطني اهتماما إزاء وجود تعريف دقيق للكلمة، وفي مستعرض رد الدول على الاستبيان الملحق بهذه الدراسة، وجد أن عددا من الدول أشارت إلى ما يقرب من (٢٠٠) مادة من مواد التشريع الوطني، فأقل من (٢) في المائة استعملت كلمة "جريمة سيبرانية" في عنوان التشريع أو في نطاق الأحكام التشريعية، ومن المسميات الأكثر شيوعا، إلى حد ما، في التشريعات، " جرائم الحاسوب [١] ، الاتصالات الإلكترونية" [٢] ، "تكنولوجيا المعلومات" [٣] ، أو " جرائم التكنولوجيا المتقدمة" [٤] ، فمن الناحية العملية، قننت العديد من هذه التشريعات جرائم جنائية والتي تم تضمنيها في مفهوم الجريمة السيبرانية، مثل النفاذ غير المشروع إلى نظام حاسوبي، أو التدخل في النظم الحاسوبية أو البيانات الحاسوبية، فإذا استخدم التشريع مصطلح "جريمة سيبرانية" بشكل محدد في عنوان أحد القوانين أو الفصول (مثل: "قانون الجريمة السيبرانية") فنادراً ما يشتمل الفصل التعريفي في التشريع على تعريف لكلمة "جريمة سيبرانية" [٥] ، وعندما تم إدراج مصطلح "جريمة سيبرانية" كتعريف قانوني،

(١) ينظر على سبيل المثال: قانون جرائم الحاسوب الماليزي(١٩٩٧) ، قانون جرائم الحاسوب السيرلنكي (٢٠٠٧)، قانون جرائم الحاسوب السوداني(٢٠٠٧).

(٢) ينظر على سبيل المثال: ألبانيا ، الاتصالات الإلكترونية في جمهورية ألبانيا ، القانون رقم (٩٩١٨) ، ٢٠٠٨، فرنسا، قانون النشر والاتصالات الإلكترونية (إصدار موحد) ٢٠١٢ ؛ تونغا ، قانون الاتصالات لعام (٢٠٠٠).

(٣) ينظر على سبيل المثال ، الهند ، قانون تكنولوجيا المعلومات لعام (٢٠٠٠) ؛ المملكة العربية السعودية ، القانون الجنائي لتكنولوجيا المعلومات لعام (٢٠٠٧).

(٤) ينظر على سبيل المثال، صربيا، قانون تنظيم واختصاص السلطات الحكومية لمكافحة جرائم التكنولوجيا العالية (٢٠١٠).

(٥) ينظر على سبيل المثال: بوتسوانا، قانون جرائم الإنترنت والحاسوب (٢٠٠٧) ، بلغاريا؛ الفصل التاسع، القانون الجنائي رقم (٩٢) لعام (٢٠٠٢) ، كمبوديا مشروع قانون؛ جرائم الإنترنت (٢٠١٢) ، جامايكا، قانون الجرائم المتعلقة بالشبكات الإلكترونية (٢٠١٠) ، ناميبيا، قانون إساءة استعمال الحاسوب والجرائم الحاسوبية (٢٠٠٣).

فالنهج الشائع قد دأب على تعريفها ب " الجرائم المشار إليها في هذا القانون" [١] ،عليه سنتناول المواجهة في اطار التشريعات الوطنية على حدة في فرعين مستقلين وكما يلي :

II.أ.١. الفرع الاول

المواجهة القانونية في العراق

أعدت الحكومة العراقية مشروع قانون جرائم المعلوماتية وتم احالته الى مجلس النواب عام (٢٠١١) وتمت القراءة الاولى في مجلس النواب ولا زال قيد التشريع، ويتضمن مشروع هذا القانون (٣١) مادة موزعه على أربع فصول حيث يتضمن الفصل الاول التعاريف والأهداف والفصل الثاني الاحكام العقابية والفصل الثالث إجراءات جمع الأدلة والتحقيق والمحاكمة والفصل الرابع احكام عامة وختامية بالإضافة الى الاسباب الموجبة، وقد عرف المشرع العراقي الجريمة المعلوماتية على أنها: هي نشاط اجرامي ايجابي أو سلبي تستخدم فيه تقنية متطورة تكنلوجيا بطريقة مباشرة أو غير مباشرة كوسيلة أو كهدف لتنفيذ الفعل الإجرامي العمدي في البيئة المعلوماتية [٢] .

وقد أشار مشروع القانون في فصل الاحكام العقابية في (مادتين فقط) الى مواد سوء استخدام شبكة الانترنت لأغراض السب والقذف والتشهير وهما:

المادة (٢١/ثالثا) : والتي تنص على " يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (٢٠٠٠٠٠٠) مليوني دينار ولا تزيد على (٥٠٠٠٠٠٠) خمسة ملايين دينار من اعتدى على أي من المبادئ أو القيم الدينية أو الأخلاقية أو الاسرية أو الاجتماعية أو حرمة الحياة الخاصة عن طريق شبكة المعلومات أو أجهزة الحاسوب باي شكل من الاشكال".

والمادة (٢٢/ثالثا) : التي نصت على " يعاقب بالحبس مدة لا تزيد على (٢) سنتين وبغرامة لا تقل عن (٣٠٠٠٠٠٠) ثلاثة ملايين دينار ولا تزيد على (٥٠٠٠٠٠٠) خمسة مليون دينار أو بإحدى هاتين العقوبتين كل من استخدم اجهزة الحاسوب وشبكة المعلومات في نسبة للغير عبارات أو صور أو أصوات او أية وسيلة أخرى تنطوي على القذف والسب" [٣] .

والملاحظ على هذا المشروع ما يأتي :

---

(١) ينظر على سبيل المثال: عمان، مرسوم ملكي رقم (١٢)، لسنة (٢٠١١) بإصدار قانون مكافحة جرائم الإنترنت، الفلبين، قانون مكافحة الجرائم الإلكترونية ٢٠١٢.

(٢) د. احمد عبد الكريم عبد الوهاب و د. محمود عبدالرحمن خلف، "اشكالية الأمن السيبراني العراقي بين التهديدات السيبرانية والتقنين المقيد للحريات"، *بحث منشور في مجلة باسية*، المجلد ١٢، العدد ٦٠، (٢٠٢٠): ص١٣.

(٣) "نحو تشريع قانون جرائم المعلومات"، تاريخ الزيارة ٢٠٢٣/٧/١٥، متاح على الرابط التالي : **ar.parliament.iq\2018\10\13\2.**

١- ان مشروع القانون لم يولي لجرائم المتعلقة بتخريب المواقع العسكرية والاجهزة داخل تلك المؤسسات.
٢- لم يتطرق مشروع القانون الى العقوبات الخاصة بجرائم الارهاب السيبراني وكذلك لم يذكر اي عقوبات بخصوص المواقع والصفحات التي تحث على الطائفية.

كانت منظمة حقوق الانسان (Human Right Watch) أول من ندد واستنكر مشروع هذا القانون اذ وصمه بكونه: قانون سيء الصياغة وعقوباته غاشمة تخرق الحق في إجراءات التقاضي وتنتهك حرية التعبير، وقد فصلت منظمة حقوق الانسان الفقرات التي تنتهك حرية الافراد، وقد نصت المادة (٢١) وكذلك المادة (٢٢) ان نطاق تلك المادتين واسع وفضفاض ولا تخضع الى معايير محددة، وبالسماح للسلطات العراقية بمعاقبة الأفراد بهذه الطريقة، تبدو أحكام القانون متعارضة مع القانون الدولي والدستور العراقي، واذا تم تطبيقها فسوف تشكل تقليصاً خطيراً لحق العراقيين في حرية التعبير وتكوين الجمعيات [١].

كما يرفض تقرير منظمة حقوق الانسان المادة (٣) في قانون الجرائم المعلوماتية المقترح، اذ تنص : على السجن المؤبد وعلى غرامة تتراوح بين (٢٥٠٠٠٠٠٠) الى (٥٠٠٠٠٠٠) لكل من استخدم عمدًا أجهزة الحاسوب وشبكة المعلومات بقصد: "المساس باستقلال البلاد ووحدتها وسلامتها أو مصالحها الاقتصادية أو السياسية أو العسكرية أو الأمنية العليا... بقصد زعزعة الأمن والنظام العام أو تعريض البلاد للخطر، إذ يمكن ان يكون هذا النص القانوني بمثابة الاساس لمحاكمة كل من لديه أي ارتباط مع منظمة أو حركة تعد "معادية" لأنها تنتقد الحكومة أو السياسات الحكومية، ويمكن للمسؤولين في السلطات أو الحكومة ان يعتبروا أية منظمة أو الاحزاب السياسية المعارضة "معادية" [٢].

إلا أنه وفي جزء من العراق وهو إقليم كوردستان العراق، والذي يتمتع بسلطات دستورية، ومنها سلطة إصدار القوانين بالشكل الذي لا يتناقض مع الدستور العراقي، فقد بادر المشرع الكوردستاني الي اصدار قانون فيما يخص الإجرام المعلوماتي [٣]، حيث تنص المادة الثانية من هذا القانون على أنه" يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على خمس سنوات وبغرامة لا تقل عن مليون دينار و لا تزيد على خمسة ملايين دينار أو بإحدى هاتين العقوبتين كل من أساء استعمال الهاتف الخلوي أو أية أجهزة اتصال سلكية أو لاسلكية أو الانترنيت أو البريد الالكتروني و ذلك عن طريق التهديد أو القذف أو السب أو نشر أخبار... " [٤]، وكذلك تنص المادة الثالثة من نفس القانون على أنه " يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن سبعمائة وخمسون ألف دينار ولا

(١) ينظر تقرير منظمة هيومنرايتسووتش، تاريخ الزيارة ٢٠٢٣/٧/١٥، وعلى الرابط الالكتروني التالي: **https://www.hrw.org/sites/default/files/reports/iraq0712arForUpload.pdf**.
(٢) د. احمد عبد الكريم عبد الوهاب وآخرون، مصدر سابق،ص١٤.
(٣) قانون منع اساءة استعمال أجهزة الاتصالات رقم (٦)، لعام (٢٠٠٨).
(٤) ينظر: المادة (٢)، من قانون منع اساءة استعمال أجهزة الاتصالات، لعام (٢٠٠٨).

تزيد على ثلاثة ملايين دينار أو بإحدى هاتين العقوبتين كل من تسبب عمداً باستخدام واستغلال الهاتف الخلوي أو أية أجهزة اتصال سلكية أو لاسلكية أو الانترنيت أو البريد الالكتروني في إزعاج غيره في غير الحالات الواردة في المادة الثانية من هذا القانون" [١].

على الرغم من ذلك فأن إصدار هذا القانون يعد خطوة إيجابية نحو مواكبة التطور والتخلص من مشكلة الفراغ التشريعي والأمني، الا أن المشرع الكردستاني كان بإمكانه أن يستغل الفرصة ويرصد كافة الجرائم المعلوماتية في هذا القانون، ومنها على سبيل المثال ارتكاب الأعمال الإرهابية عبر الوسائل التقنية الحديثة أو ما يسمى بالإرهاب الإلكتروني حالياً.

II.أ.٢. الفرع الثاني

المواجهة في اطار تشريعات بعض الدول

من الجدير بالذكر ان التشريعات العربية والغربية قد اوجدت نظاماً قانونياً للتعامل مع الجرائم السيبرانية ، عليه سنشير في هذا الفرع الى تلك المعالجة في فقرتين مستقلتين وكما يأتي :

أولا: موقف تشريعات بعض الدول العربية من الجرائم السيبرانية (المعلوماتية):

عندما نبحث عن النصوص والتشريعيات العربية عموماً تجاه الجرائم المعلوماتية، نجد أنه هنالك فراغ تشريعي كبير، حيث أن غالبية من الدول العربية تفتقر الى قانون لتجريم الجرائم المعلوماتية، ولكن في ذات الوقت هناك دول عربية قد تصدت لهذه الظاهرة بقوانين مستقلة، وما يلفت النظر هو أن نشير هنا الى قانون العربي النموذجي [٢] حيث تختص المحاكم الجزائية السعودية بالجرائم السيبرانية إذا كانت الجريمة السيبرانية جريمة وطنية وقد تقدم بيان المراد بها ، للمادة الرابعة والعشرين والخامسة والعشرين من نظام المرافعات الشرعية الصادر بالمرسوم الملكي ذي الرقم (م/١) لعام (٢٠١٣)، والمادة الثامنة والعشرين بعد المائة من نظام الإجراءات الجزائية، وتكون المحاكمة وفقاً لنظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي ذي الرقم (م/١٧) لعام (٢٠٠٨) [٣].

هذا وقد تضمنت المادة الخامسة من النظام المذكور عقوبة الجرائم السيبرانية الوطنية بكافة صورها، وأن عقوبتها: السجن مدة لا تزيد عن أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين [٤].

(١) ينظر: المادة (٣) من قانون منع اساءة استعمال أجهزة الاتصالات، لعام (٢٠٠٨).
(٢) القانون العربي النموذجي في شأن مكافحة جرائم الكومبيوتر والأنترنت، الذي تم اقراره في عام ٢٠٠٣، بوصفه منهجاً استرشادياً يلزم به المشرع الوطني عند اعداد تشريع في الجرائم المعلوماتية.
(٣) ينظر، المادة (٢٤) و(٢٥)، من نظام المرافعات الشرعية السعودية ، لعام (٢٠١٣).
(٤) ينظر، المادة (٥)، من نظام مكافحة جرائم معلوماتية السعودية، لعام (٢٠٠٧).

أما إذا كانت الجريمة السيبرانية جريمة عالمية وقد تقدم بيان المراد بها فإما أن يكون المجرم سعودياً أو غير سعودي، فإن كان سعودياً، فيكون اختصاصها للمحاكم الجزائية السعودية، للمادة الرابعة والعشرين من نظام المرافعات الشرعية الصادر بالمرسوم الملكي ذي الرقم (م/١) لعام (٢٠١٣)، والمادة الثامنة والعشرين بعد المائة من نظام الإجراءات الجزائية، وان كان غير سعودي، فيخضع لقوانين العقوبات العالمية، ويطبق في حقه الاتفاقيات المختصة بالتعاون الأمني والعدلي، على أنه يحق لكل دولة من حيث المبدأ محاكمة من ألحق بها الضرر على أراضيها ولو غيابياً [١]. ان الجهود الحكومية في مكافحة جرائم المعلوماتية :لا شك أن القوانين لا يكفي في حد ذاتها ولا يتحقق الهدف منها إلا بإحداث أجهزة ومؤسسات حكومية لتنفيذها. وفي هذا الإطار تقوم الوزارات والهيئات الحكومية السعودية المختلفة بجهود جبارة في مكافحة الإجرام الإلكتروني بمختلف أشكاله [٢]، ونذكر منها على سبيل المثال:(وزارة الإتصالات وتقنية المعلومات السعودية[٣]، وزارة الداخلية السعودية [٤] ، وزارة العدل السعودية [٥] ، الهيئة الوطنية للأمن السيبراني، وهيئة الإتصالات وتقنية المعلومات السعودية) [٦].

أما دولة الامارات العربية المتحدة فهي الأخرى أيضاً تصدت للجرائم المعلوماتية بسنها تشريع خاص في شأن مكافحة جرائم تقنية المعلومات، تحظر دولة الإمارات العربية المتحدة الجرائم المعلوماتية باعتبارها جرائم مستحدثة، وقد أصدرت القانون الاتحادي رقم (٢) لعام (٢٠٠٦) في شأن مكافحة جرائم تقنية المعلومات وهو من القوانين الريادية الأولى في العالم العربي الذي تضمن تفاصيل كثيرة، حيث وضح معاني المصطلحات المستعملة وذات الدلالة القانونية وهي المعلومات الإلكترونية، البرنامج المعلوماتي، نظام المعلومات الإلكتروني، الشبكة المعلوماتية، المستند الإلكتروني، الموقع وغيرها من المصطلحات، كما بيّن النظام الجرائم المعلوماتيّة والعقوبات المقررة لها والتدابير لمكافحة هذه الجرائم، وقد صدر مؤخراً قانون الجرائم الإلكترونية الجديد، الذي تم تبنيه بموجب المرسوم بقانون اتحادي

---

(١) عبدالعزيز بن فهد محمد بن داود، مصدر سابق، ص١٥١.

(٢) للمزيد ينظر، لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركانها وآلية مكافحتها دراسة تحليلية مقارنة"، *بحث منشور في مجلة الميزان للدراسات الإسلامية والقانونية*، المجلد ٤، العدد ١، (٢٠١٧): ص٢١١.

(٣) للمزيد ينظر: نرمين سليمان، "أثر الجرائم الإلكترونية على الأبعاد الداخلية للأمن القومي: دراسة حالة المملكة العربية السعودية خلال الفترة من (٢٠٠٦) الى (٢٠١٦)"، (رسالة دكتوراه في العلوم السياسية، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية، مصر، ٢٠١٨)،ص٢٠٧.

(٤) للمزيد ينظر:

Melissa Hathaway، Francesca Spidalieri، and Fahad Alsowailm، Kingdom of Saudi Arabia Cyber Readiness at a Glance، Potomac Institute for Policy Studies. p.10.

(٥) للمزيد ينظر: أحمد عبد الله الخشاشنة، "تحريز الأدلّة الرقميّة وأثرها في كشف الجريمة"، *مجلّة الدراسات الأمنيّة، الأردن*، المجلد١، العدد١٦، (٢٠١٩): ص ٧ وما بعدها.

(٦) للمزيد ينظر: فؤاد الصلاحي، "الأمن السيبراني، إستراتيجية الهيئة الوطنيّة للأمن السيبراني"، *بحث منشور في مجلة الدوحة، وزارة الإعلام*، (٢٠١٥): ص١٢٩، متاح على الرابط التالي:
ar.pdf-https://nca.gov.sa/national_cybersecurity_strategy تاريخ الزيارة ٢٠١٣/٧/١٨.

رقم (٣٤) لعام (٢٠٢١) في شأن مكافحة الشائعات الجرائم الإلكترونية ليحل محل القانون الاتحادي السابق لعام (٢٠١٢) [١].

وفي قطر فقد نص قانون العقوبات القطري الصادر بالقانون رقم (١١) لعام (٢٠٠٤) على جرائم الحاسب الآلي، وأدرجها ضمن الجرائم الواقعة على المال، ونظمها في (١٨) مادة تبدأ بالمادة (٣٧٠) وتنتهي بالمادة (٣٨٧) ، حيث احتوت على أحكام تتعلق بنظام المعالجة الآلية للبيانات، وفيروس الحاسب الآلي، وبطاقات الدفع الممغنطة، وتعتبر دولة قطر من أوائل الدول العربية التي وضعت أحكاماً في قانون العقوبات تتعلق بالجرائم ذات الصلة بالحاسب الآلي، كما أهتم المشرع القطري أيضا بالتعاون القضائي الدولي في مجال الجريمة وهذا يتجلى من خلال ما تضمنه قانون الإجراءات الجنائية القطري رقم (٢٣) لعام (٢٠٠٤) من أحكام، كما أولى المشرع القطري اهتماما كبيراً للتعاون الدولي في مجال مكافحة الجريمة، كما أصدر القانون رقم (١٤) لعام (٢٠١٤) المتعلق بمكافحة الجرائم الإلكترونية لمواجهة الاعتداءات التي يتعرض لها النظام المعلوماتي، ومواكبة الوسائل الحديثة التي يرتكب بها هذا النوع من الجرائم والذي تضمن كل الأحكام والآليات وسبل التعاون الدولي لمكافحتها، وفي نفس الصدد أصدر المشرع القطري القانون رقم (٢٠) لعام (٢٠١٩) المتعلق بمكافحة غسل الأموال وتمويل الإرهاب، هذا بالإضافة إلى الأجهزة المتعددة المختصة في مكافحة الجرائم المعلوماتيّة ومنها نيابة الجرائم الإلكترونية، نيابة التعاون الدولي، إدارة مكافحة الجرائم الاقتصادية والإلكترونية، إدارة الاتصال للشرطة العربية والدولية (الإنتربول) بوزارة الداخلية التي تقوم بجهود كبيرة في هذا المجال وغيرها [٢].

وفي مصر تأسست الجمعية المصرية لمكافحة جرائم المعلوماتية في عام (٢٠٠٥) ، وهي منظمة غير حكومية تعمل على نشر الوعي واعداد الدراسات والمؤتمرات حول هذه الجرائم، وتعتبر حركة التشريع في مجال مكافحة الجريمة السيبرانية في مصر، ضعيفة مقارنة بدولة الإمارات العربية المتحدة، إلا أن تطبيق بعض النصوص التقليدية المتعلقة بالتزوير والاحتيال والسرقة والمساس باعتبار الأشخاص، لا يزال مستمراً في القانون المصري.

ويعتبر قانون التوقيع الإلكتروني الصادر لعام (٢٠٠٤)، أول قانون يصدر بشأن الأفعال المتعلقة بالنظم المعلوماتية في مصر، حيث جرم أفعال بموجب المادة (٢٣) منه [٣] ، تتعلق بالحصول على توقيع أو وسيط أو محرر إلكتروني بدون وجه حق، أو اعتراضه أو تعطيله عن أداء وظائفه وقد عرف الوسيط الإلكتروني في الفقرة الرابعة من المادة الأولى من قانون التوقيع الإلكتروني المصري بأنه " أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني"، فهو عبارة عن نظام معلوماتي يساعد على إنشاء التوقيع الإلكتروني واصدار المحررات الإلكترونية [٤].

---

(١) معهد دبي القضائي، قانون مكافحة الشائعات والجرائم الإلكترونية لدولة الإمارات العربية المتحدة مرسوم بقانون اتحادي رقم (٣٤)، لعام (٢٠٢١)، التشريعات والقوانين لدولة الإمارات العربية المتحدة ١٦ ، معهد دبي القضائي، دبي، ٢٠٢٢.

(٢) مريم عبد اللطيف المسلماني، "مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الإلكترونية"، *مجلة القانون والمجتمع*، المجلد ١٠ ، العدد ٢ ، (٢٠٢٢): ص ٣٠ وما بعدها.

(٣) ينظر: المادة (٢٣)، من قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥)، لعام (٢٠١٨).

(٤) عبد الله عبد الكريم عبد الله، *جرائم المعلوماتية والإنترنت*، (بيروت: منشورات الحلبي الحقوقية، ٢٠٠٧)، ص٩٣. أسامة مهمل، "الإجرام السيبيراني"، (رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف-المسلية،الجزائر،٢٠١٨)،ص٣٧.

وعلى صعيد اخر كخطوة جديدة قام المشرع الجزائري بسن القانون ٠٤/٠٩ المتعلق بالوقاية من تكنولوجيات الإعلام والاتصال ومكافحتها، وان كان تجسيد بنوده على ارض الواقع مازال ضعيفا الى حد الساعة نتيجة إهمال الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وفي تحديد العقوبة المناسبة في حق مرتكبيها، حيث تقتصر العقوبات في غالبية الأحيان على الغرامة المالية فقط [١] .

ثانيا/ تشريعات بعض الدول الغربية من الجرائم السيبرانية(المعلوماتية):

تأتي بريطانيا كثالث دولة التي سنت قوانين خاصة بجرائم الحاسب الآلي، حيث أقرت قانون مكافحة التزوير والتزييف لعام (١٩٨١)، والذي شمل في تعاريفه الخاصة، تعريف تزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها، سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى [٢] . ثم أصدرت بعد ذلك قانونا خاص بإساءة استخدام الحاسوب الآلي لعام (١٩٩٠) ، الذي نظم جرائم الحاسب الآلي ضمن ثلاث فئات، تتعلق الأولى بالدخول غير المصرح به إلى معطيات الحاسب الآلي وبرامجه المخزنة، والثانية فقد تناولت تجريم الدخول غير المصرح به مع وجود نية ارتكاب أو تسهيل ارتكاب جرائم أخرى، أما الثالثة فتتعلق بتجريم الإتلاف المعلوماتي وذلك من خلال نص المادة الثالثة من هذا القانون [٣] .

وفي فرنسا نص المشرع الفرنسي من خلال قانون العقوبات الفرنسي، على تجريم الاعتداء على أنظمة معالجة البيانات، وذلك بموجب الفصل الثالث من الباب الثاني منه، ومن ضمن الجرائم التي نصَ عليها هذا الفصل، إدخال أو مسح أو تغيير معلومات بطرق الغش، المادة (٣/٣٢٣) كما نص أيضا على تجريم عدة أفعال تقع ضد المصالح العليا للدولة، وذلك إذا انصبت على المعلومات أو البيانات التي تمت معالجتها إلكترونيا، المواد (٦/٤١١) الي (١٠/٤١١) والي جانب هذه النصوص، فإن المشرع الفرنسي قد نص على بعض الجوانب المتصلة بالمستند الإلكتروني في قوانين أهمها، قانون الإثبات والتوقيع الإلكتروني الصادر عام (٢٠٠٠) واللائحة الصادرة عام (٢٠٠١) التي أقر من خلالها الأخذ بالدليل الإلكتروني في الإثبات والتوقيع الإلكتروني [٤] .

و تعد الولايات المتحدة الأمريكية الدولة التالية بعد السويد من حيث إصدار قوانين خاصة بها ومستقلة، والتي تجرم الجرائم الإلكترونية، إذ أنها شرعت قانوناً مستقلاً لحماية

---

(١) احمد بن خليفة، حفوظة الأمير عبد القادر، "الجريمة الالكترونية وآليات التصدي لها"، *بحث منشور في مجلة الامتياز لبحوث الاقتصاد والادارة*، المجلد ١، العدد١ ، (٢٠١٧): ص١٦٥

(٢) علي جبار الحسيناوي، جرائم الحاسوب والأنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان،٢٠٠٩،ص١٦٥.

(٣) عبد اللطيف معتوق، "الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري ,التشريع المقارن"، (رسالة ماجستير، جامعة العقيد الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، ٢٠١٢)، ص٩٠.

(٤) فتيحة رصاع، "الحماية الجنائية للمعلومات على شبكة الأنترنت"،(رسالة ماجستير، جامعة أبي بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية،٢٠١٢)،ص٩٤.

أنظمة الحساب الآلي (١٩٦٥-١٩٨٥) وفي عام (١٩٨٥) حدد معهد العدالة القومي الأمريكي، خمسة أنواع رئيسية للجرائم المعلوماتية [١].

وهي:

١- جرائم الحاسب الآلي الداخلية.
٢- جرائم الاستخدام غير المشروع عن بعد.
٣- جرائم التلاعب الحاسب الآلي.
٤- دعم التعاملات الإجرامية.
٥- سرقة البرامج الجاهزة والمكونات المادية للحاسب.

وفي عام (١٩٨٨) ثمة قانونين متخصصين بالجرائم المعلوماتية، تم أصدارهما، وهما : قانون الغش والتعسف في الكمبيوتر، أما القانون الثاني فهو قانون سرية الإتصالات الألكترونية الخاصة، أو التصنت عليها بشكل غير مرخص به [٢]، وفي عام (١٩٩٦) صدر قانون الإتصالات الذي تضمن نصوصاً خاصة بقانون آداب الإتصالات، وتناول تقييد حرية الاطلاع على الصور والمواد المخلة بالآداب العامة المنتشرة على شبكة الانترنت، وفي عام (١٩٩٧) أصدرت المحكمة العليا الأمريكية حكما بعدم دستورية البعض من نصوص آداب الأتصالات [٣].

II.ب. المطلب الثاني

المواجهة الدولية للجرائم السيبرانية

بخصوص مفهوم الجرائم السيبرانية في ظل الاتفاقيات الدولية، فإن عددا قليلا من الصكوك الدولية أو الإقليمية تضمنت تعريفا للجريمة السيبرانية، فعلى سبيل المثال: خلت كل من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وكذلك مشروع اتفاقية الاتحاد الأفريقي، من تعريف الجريمة السيبرانية لأغراض الاتفاقية، بالإضافة إلى ذلك، لم تستخدم اتفاقية دول الكومنولث المستقلة حول التعاون في مكافحة الجرائم في مجال المعلومات الحاسوبية مصطلح "جريمة سيبرانية"، ولكنها عرفتها باعتبارها "جريمة تتعلق بالمعلومات الحاسوبية [٤]":" فعل إجرامي يستهدف المعلومات الحاسوبية"، وعلى النهج نفسه، تضمنت اتفاقية منظمة شنغهاي للتعاون تعريف "المعلومات الحاسوبية" بأنها "استخدام موارد المعلومات و (أو) التأثير عليها في المجال المعلوماتي

---

(1) Scott Charney And Kent Alexsander، Computer Crime،1996،Vol 45، Emory L.J.P.949.

(٢) د. طوني ميشال عيسى، *التنظيم القانوني لشبكة الأنترنت*، (لبنان: دار صادر، ٢٠٠١)،ص١٩١.

(٣) د. حمد عبيد الكعبي، *الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت*، ط٢، (القاهرة: دار النهضة العربية، ٢٠٠٩): ص٧١.

(٤) الاتفاقية المتعلقة بالتعاون بين بلدان كومنولث الدول المستقلة، الفقرة (أ)، المادة الأولى.

لأغراض غير مشروعة" [١] مما يستلزم اضطلاع المواجهة الدولية للجرائم السيبرانية للقيام بهذا الدور، وهو ما سنبحثه في الفروع الآتية:

II.ب.١. الفرع الاول
المواجهة الدولية العالمية للجرائم السيبرانية

تعد الجريمة السبرانية من الجرائم العابرة للحدود والتي لا تقف عند حدود الدولة بل تتعدى إلى دول أخرى، وقد يساهم أكثر من شخص في دول مختلفة في ارتكاب جريمة سبرانية واحدة يقع ضحيتها عدد من الأفراد يقيمون في بلدان متعددة الأمر الذي يتطلب معه وجوب التعاون بين الدول لمكافحة هذه الجريمة والتعاون المقصود هنا لا يقتصر على التعاون القضائي بين الدول بل يشمل التعاون الفني، إلا أن هذا التعاون ليس بالأمر اليسير بل تواجهه صعوبات وهذا ما سنحاول بيانه في هذه الفرع [٢].

اولاً : مواجهة المنظمات الدولية للجريمة السيبرانية :

المؤتمرات التي دعت لمواجهة النتائج السيئة والاضرار التي قد تلحق بالنظام الاجتماعي والاخلاقي للمجتمع الدولي من جراء الاستخدام السيء لأجهزة الاتصال الحديثة، ذلك ان خطر هذه الوسائل اخذ منحى في منتهى الخطورة حيث اصبحت هذه الجرائم (المعلوماتية) ذات طابع عال من التقنية كأرسال الفايروسات في أيام معينة من السنة وتدمير عدد هائل من اجهزة الحاسوب التابعة للدولة او للأفراد، وتسبب ضرراً فادحاً في عملية التنمية للدول ويمكن ابراز دور المنظمات الدولية في هذا الصدد من خلال ما يأتي :

١- القرار الصادر عن الأمم المتحدة بشأن جرائم الكمبيوتر – هافانا ١٩٩٠:

بعد انعقاد مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين في مدينة ميلانو الإيطالية عام (١٩٨٥) ، والذي تمت من خلاله الإشارة إلى مشكلة الجريمة السيبرانية، حيث انبثقت عنه مجموعة من التوجيهات من بينها تكليف لجنة الخبراء العشرين لدى منظمة الأمم المتحدة، بدراسة موضوع حماية نظم المعلومات والاعتداء على الحاسب الآلي، والتي بدورها أقرت جملة من التوصيات والمقترحات والمبادئ، التي تبناها المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين المنعقد في عام (١٩٩٠) بالعاصمة الكوبية هافانا [٣].

تتلخص توصيات مؤتمر هافانا أساسا في التأكيد على ضرورة وضع إطار قانوني دولي بتظافر جهود جميع الدول الأعضاء، من أجل التعاون على الحد من انتشار وتعاظم آثار هذه الظاهرة الإجرامية المستحدثة، وذلك بأن تقوم كل دولة عضو بتكثيف جهودها لمكافحة إساءة استخدام الكمبيوتر [٤] ، وأشار القرار أنه على الدول الأعضاء وفي سبيل مواجهة الإجرام السيبراني اتخاذ مجموعة من الإجراءات تتلخص في:

---

(١) اتفاق منظمة شنغهاي، الملحق (١).

(٢) حسين بن سعيد بن سيف الغافري، "الجهود الدولية في مواجهة جرائم الانترنيت"، بحث منشور على الشبكة الدولية، تاريخ الزيارة ١٩ / ٧ / ٢٠٢٣، متاح على الرابط التالي www.minshawi.com ، ص٥.

(٣) علي جبار الحسيناوي، *جرائم الحاسوب والأنترنت*، (الاردن : دار اليازوري العلمية للنشر والتوزيع،عمان،٢٠٠٩)، ص١٤٧.

(٤) محمود أحمد عبابنة، *جرائم الحاسوب وأبعادها الدولية*، ط١، (عمان: دار الثقافة للنشر والتوزيع، ٢٠٠٩ الاردن)، ص١٥٥.

- تحديث القوانين وأغراضها الجنائية كحاجة فعلية من أجل ضمان تطبيق الجزاءات والقوانين الراهنة بشأن جهات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم.
- وضع أحكام واجراءات تتعلق بالتحقيق والأدلة للتصدي لمثل هذا الشكل الجديد والمعقد من أشكال النشاط الإجرام ي، ومصادرة أو رد الأصول الناجمة عن ارتكاب جرائم ذات صلة بالحاسوب.
- اعتماد تدابير لزيادة وعي الجماهير والعاملين في الأجهزة القضائية وأجهزة التنابذ، بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحاسب الآلي.

اعتماد تدابير مناسبة لتدريب القضاة والمسؤولين لأجل منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والادعاء فيها [١] .

٢ـ القرارات الصادرة عن المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر ـ ريودي جانيرو ١٩٩٤:

أوصى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي انعقد في ريودي جانيرو بالبرازيل في عام (١٩٩٤)، والذي تم من خلاله مناقشة جرائم الحاسب الآلي بأن تتضمن قائمة الحد الأدنى من الأفعال المشكلة لجرائم الحاسب الآلي والمتعين تجريمها والتي يمكن ذكرها على النحو التالي:

- الاحتيال أو الغش المرتبط بالكمبيوتر.
- تزوير الكمبيوتر أو التزوير المعلوماتي.
- الاضرار بالبيانات والبرامج وتشمل المحو والإتلاف والتعطيل للمعطيات.
- تخريب واتلاف الكمبيوتر.
- الدخول غير المصرح به: وهو الولوج إلى نظام ما عن طريق انتهاك إجراءات الأمن.
- الاعتراض غير المصرح به : وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام الكمبيوتر أو عدة نظم أو شبكة اتصالات [٢].

II.ب.٢. الفرع الثاني

المواجهة الدولية الاقليمية للجرائم السيبرانية

أبرمت مجموعة من الاتفاقيات العربية الجماعية بين دول اعضاء الجامعة العربية كانت أولها في العام (١٩٥٤)، وعرفت ب(اتفاقية تسليم المجرمين) ، وهي أول عمل جماعي

(١) عبد الله عبد الكريم عبد الله، *جرائم المعلوماتية والإنترنت*، (بيروت: منشورات الحلبي الحقوقية، ٢٠٠٧)، ص١٠٨.

(٢) عبد اللطيف معتوق، "الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري او التشريع المقارن"، (رسالة ماجستير، جامعة العقيد الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، ٢٠١٢)، ص١٠٠.

على مستوى الدول العربية ، وبعدها في العام (١٩٦٠)، اصدر مجلس جامعة الدول العربية قرار رقم (١٦٨٥) بالاتفاق على انشاء المنظمة العربية للدفاع الاجتماعي ضد الجريمة وبعدها إحدى المنظمات المتخصصة في نطاق جامعة الدول العربية ووافقت جميع الدول الاعضاء على ذلك ومن ضمنها العراق، حددت القاهرة مقرر لها وصارت تمارس اعمالها عن طريق الأمانة العامة من خلال مكاتبها الأول في بغداد اطلق عليه (مكتب مكافحة الجريمة) والثاني في دمشق، والثالث في القاهرة (مكتب مكافحة المخدرات)، واستمر العمل حتى العام (١٩٨٢) ، وفي العام (١٩٨٨)، تم انشاء (مجلس وزراء الداخلية العرب) يهدف الى تنمية وتوثيق التعاون بين الحدود العربية لمكافحة الجريمة اختص بالقيام برسم السياسات العامة والعمل المشترك لتنفيذ هذه السياسات انشاء الهيئات والأجهزة اللازمة لتحقيق أهدافه مع تعزيز وسائل التعاون مع الهيئات الدولية المعنية باختصاصاته ، وتضمن ايضا دعم الاجهزة الأمنية ذات الامكانيات المحدودة [١] .

أولا: الاتفاقية الامريكية المتعلقة بجرائم الحاسب الالي والانترنيت لعام (١٩٩٩):

عقد في جامعة ستانفورد في ولاية كاليفورنيا في الولايات المتحدة مؤتمر في عام (١٩٩٩) بمشاركة العديد من الهيئات والمنظمات الدولية والممثلين القانونيين وتم اقتراح هذه الاتفاقية لتعزيز الحماية من الارهاب وجرائم الحاسب الالي وتضمنت المادة الاولى من الاتفاقية تعريفا للمصطلحات المستعملة في هذه الاتفاقية، واوجبت الاتفاقية كذلك على الولايات أو الاعضاء فيها تبني معايير موحدة لمواجهة هذه الجرائم وفرض عقوبات تتناسب مع درجة خطورتها [٢] ، فقد بينت الجرائم المعلوماتية وهي التوصيل غير المصرح به وتعديل وحذف البيانات بهدف الاضرار بالمؤسسات التي تملك هذه الخدمات او حذف البيانات بتغييرها لإعطاء معلومات كاذبة بهدف ايقاع اضرار مادية ، اما المادة (٤) فقد أوضحت احكام المحاولة او المساعدة والتحريض والاغراء والتآمر على ارتكاب الجريمة المعلوماتية وكذلك بينت هذه الاتفاقية أحكام اختصاص الولايات الاعضاء في اتخاذ الاجراءات القانونية الملائمة [٣] وكذلك التعاون بين الولايات في اقامة الدعوى (م/ ٦ ١٢) ووجوب انضمام

(١)عبد الكريم الردايدة ،*الجرائم المستحدثة واستراتيجية مواجهتها* ،(عمان: دار الحامد للنشر والتوزيع، ط١، ٢٠١٣)، ص٢٥٢.

(٢) يتعين على كل طرف تبني مثل هذه الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لتجريم الأفعال الجنائية بموجب قانونه المحلي ، عند ارتكابها عمداً، للوصول إلى نظام الكمبيوتر بالكامل أو أي جزء منه دون حق، قد يطلب أحد الأطراف ارتكاب الجريمة من خلال انتهاك الإجراءات الأمنية بقصد الحصول على بيانات الكمبيوتر أو أي نية أخرى غير نزيهة، أو فيما يتعلق بنظام كمبيوتر متصل بنظام كمبيوتر آخر. للمزيد ينظر: المادة (٢)، من اتفاقية الامريكية المتعلقة بجرائم الحاسب الالي والانترنيت، لعام ١٩٩٩.

(٣) ينظر، المادة (٥)، من اتفاقية الامريكية المتعلقة بجرائم الحاسب الالي والانترنت، لعام ١٩٩٩.

الاعضاء لإتمام حماية البنية التحتية للمعلومات [١] ، كما اوجبت الاتفاقية ضرورة تقديم تقارير سنوية للاتحاد [٢] .

ثانياً: اتفاقية بودابست لمكافحة جرائم المعلوماتية والأنترنت – بودابست (٢٠٠١):

حرصاً على حماية مصالح المواطنين وحقوقهم، تقدمت اللجنة الأوروبية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية في عام (٢٠٠١) بمشروع اتفاقية جرائم الكومبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتي إعداد مسودتها النهائية التي أقرت لاحقاً في العاصمة المجرية بودابست في عام (٢٠٠١) وتعرف اتفاقية بودابست (باتفاقية الجرائم الإلكترونية سايبر كرايم)، وتعتبر من الاتفاقيات الدولية المهمة التي تم إبرامها لمكافحة الجرائم المعلوماتية، وتعد الاتفاقية الوحيدة والمعروفة بالاتفاقية الدولية لمكافحة الجرائم التي ترتكب عبر الأنترنت [٣] .

وقد وقعت على هذه الاتفاقية (٢٦) دولة أوروبية بالإضافة الي كندا وأمريكا وجنوب أفريقيا واليابان، ورغم أن هذه الاتفاقية هي في الأصل اتفاقية الأوروبية المنشأ، إلا أنها اتفاقية ذات طابع عالمي، لكونها مفتوحة للدول الاخرى لطلب الانضمام من خارج أوروبا، مما يجعلها إطار دولياً مفيداً للعمل على مكافحة الجرائم السيبرانية الدولية [٤] ، وتتكون هذه الاتفاقية من مقدمة وأربعة فصول، وبالنتيجة فإن مقدمة هذه الاتفاقية استعرضت أهدافها ومنطلقاتها و مرجعياتها السابقة وما تقوم علية من جهود إرشادية وتوجيهية وتدابير إقليمية ودولية، وتضمن الفصل الثاني الذي جاء تحت عنوان الجوانب الموضوعية والإجرائية للجرائم المعلوماتية (المواد ٢-٢٢)، وجاء الفصل الثالث بعنوان الأحكام المتعلقة بالجرائم المعلوماتية عابر للحدود (المواد ٢٣-٣٥) والمتعلقة بالاختصاص والتعاون الدولي، أما الفصل الرابع جاء بالأحكام الختامية (المواد ٣٦-٤٨) [٥] .

(١) ينظر: المادة (١٢)، من اتفاقية الامريكية المتعلقة بجرائم الحاسب الالي والانترنيت، لعام ١٩٩٩.

(٢) محروس نصار غريب، "الجريمة المعلوماتية"، *بحث منشور في مجلة التقني*،المجلد٢٤،العدد١٠، (٢٠١١):ص٢١.

(٣) د. سليمان احمد فضل، *المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية*، (القاهرة: دار النهضة العربية، ٢٠١٣)،ص٤٢٩.

(٤) اتفاقية بودابست لمكافحة جرائم المعلوماتية، لعام ٢٠٠١، صادرة عم مجلس أوروبا رقم (١٨٥)، في ٢٠٠١/١١/٢٣.

(٥) د. نبراس ابراهيم مسلم، "الجرائم السيبرانية وأثرها على الأمن السيبراني"، *بحث منشور في مجلة القادسية للقانون والعلوم السياسية*،المجلد١٢،العدد١، (٢٠٢١): ص٣٨٦.

وقد نصت هذه الاتفاقية على تسمية مجموعة من الأعمال الإرهابية عبر الوسائل الإلكترونية غير المشروعة، وحث الدول الأعضاء فيها على تجريمها في تشريعيات داخلية، كما تضمنت الاتفاقية عدة طوائف من الجرائم الالكترونية [١] ، وهي على النحو الآتي:

الطائفة الاولى: الجرائم التي تستهدف أمن المعلومات الإلكترونية.

الطائفة الثانية: الجرائم المرتبطة بالحاسوب الإلكتروني.

الطائفة الثالثة: الجرائم المرتبطة بالمحتوي الإلكتروني.

الطائفة الرابعة: الجرائم السيبرانة.

وقد تناولت هذه المعاهدة الجرائم التي تعد أكثر انتشاراً على مستوي العالم مثل الإرهاب الإلكتروني وعمليات تزوير بطاقات الأتمان ودعرة الأطفال ...الخ، وعلى أثر اتساع النغمة الدولية لمكافحة الجريمة المعلوماتية، من حيث ضرورة السعي الي تكوين أرضية قانونية تعمل على دعم الكفاح الدولي المشترك ضد الجريمة عبر الأنترنت، وبناءً على توصية مجلس وزراء أوروبا وقراراته المختلفة حول المشاكل والحلول التي يمكن طرحها وأعداد مشروعات قوانين تسير على هديها المجموعة الأوروبية، فقد قام مجلس أوروبا [٢] ، منذ ثمانينات القرن العشرين بمحاولات عدة، من أجل أعداد مشروعات عمل لمواجهة الأنشطة الإجرامية والتهديدات المحتملة كالاختراق والأنشطة الإجرامية الأخرى ذات العلاقة بالحاسوب، ومن تلك المحاولات أعداد اتفاقية تتضمن في محتواها ضرورة تسهيل التعاون الدولي في الإجراءات الجنائية في الجرائم الناشئة غن استخدام الحاسوب والأنترنت [٣].

ثالثاً: بروتوكول ستراسبورغ (٢٠٠٣):

تم وضع هذا البروتوكول الاضافي في عام (٢٠٠٣)، بهدف تتميم مضامين اتفاقية الجريمة المعلوماتية، حيث تضمن هذا البروتوكول (١٧) مادة ضمن أحكام الفصل الثالث من البروتوكول المعنون ب"العلاقة بين الاتفاقية وهذا البروتوكول" في المادة (٨) منه الي أن القواعد الإجرائية المضمنة باتفاقية بودابست تطبق على الجرائم المشار اليها في البروتوكول

(1) Michael Gervais، "Cyber Attacks and the Laws of War"، Berkeley Journal of International Law، vol. 30، lss. 2، 2012.p.167.

(٢) مجلس أوروبا (The Council Of Europe) (COE): يتكون من (٤١) دولة، تأسس في عام (١٩٤٩)، كاتحاد مضاد للأفكار الدكتاتورية التي سادت أوروبا في النصف الأول من القرن العشرين ولتقوية حركة الدفاع عن حقوق الانسان وتطوير الحركة الديموقراطية ودور القانون في هذه الأطار، وعلى مدة سنوات عد المجلس الأوروبي الملاذ الآمن للدول الأوروبية لكل حوار يمكن أن يكون مفيداً وتنثبق عنه اتفاقيات في هذه الاطار بين الدول الاعضاء. للمزيد حول هذه المجلس، ينظر: الرابط التالي، تاريخ الزيارة ٢٠٢٣/٧/٢١، http:Lwww.Coe.int.

(٣) د. خليل يوسف جندي ميراني، *سياسة التجريم في ظل العولمة(دراسة مقارنة)*، ط١، ايران، (رانم، ٢٠١٨)،ص٢٦٨.

[١] ، وذلك فيما يخص أحكام الاختصاص المشار اليها في المادة (٢٢) من اتفاقية بودابست مع ما قد يلزم من تعديل، وكذا أحكام المواد من (١٤ الي ٢١) المتعلقة بنطاق القواعد الاجرائية والشروط والضمانات المرتبطة بها والقواعد الإجرائية المتعلقة بسرعة التحفظ على بيانات الكومبيوتر المخزنة وإصدار الأوامر وتفتيش وحجز بيانات الكومبيوتر والتجمع الفوري لها[٢].

رابعاً: القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية الذي صادق عليه مجلس وزراء العدل العرب بتاريخ (١٠ / ٠٨ / ٢٠٠٣):

نص هذا القانون على جملة من الأحكام الموضوعية والإجرائية تعمل على الحد من الجريمة المعلوماتية وقد جاء في المادة (٢٦) منه ما يلي:" تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه ولو أُرتكبت كلياً أو جزئياً خارج إقليم الدولة متى أضرت بإحدى مصالحها ويختص القضاء الوطني بنظر الدعاوى المترتبة عليه." ومن خلال هذا النص نلاحظ أن القانون أخذ بمبدأ العينية باعتماده على المصلحة الوطنية كمعيار أساسي لثبوت الاختصاص وبالتالي تطبيق القانون الجنائي الوطني، كما أن هذا القانون لم يعين أي جهة تتولى عملية الضبط القضائي في جرائم المعلوماتية مما يعني أنه ترك المجال مفتوحا للدول العربية من خلال إعطاء تلك السلطة لأي هيئة أو جهة تراها قادرة على اكتشاف ومتابعة تلك الجرائم [٣] .

خامساً: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات(٢٠١٠):

في عام (٢٠١٠) وافق مجلس وزراء الداخلية والعدل العرب في اجتماعهم المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة، على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، تحتوي هذه الاتفاقية على (٤٣) مادة، وجاء في المادة الأولى منها " تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم، حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها "، ونجد في الفصل الثاني تأصيلا للأفعال التي تعد مجرمة، أما الفصل الثالث منها فقد تم التعرض من خلاله إلى نطاق تطبيق الأحكام الإجرائية، وفي الفصل الرابع نصَ على التعاون القانوني والقضائي، أما الفصل الخامس فتضمن أحكاما ختامية [٤] .

---

(١) ينظر: المادة (٨)، من بروتوكول ستراسبورغ، عام ٢٠٠٣.

(٢) والذي يطلق عليه البروتوكول الإضافي لاتفاقية الجريمة المعلوماتية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهة الأجانب التي ترتكب عبر أنظمة الكومبيوتر، تاريخ الزيارة ٢٠٢٣/٧/٢٢، متاح على الرابط الالكتروني التالي: http:Lconventions ، coe.intLtreatyLfrLtreatiesLHtmlL189.htm .

(٣) د. حمزه بن فهم السلمي، "الجرائم المعلوماتية والضوابط القانونية لمكافحتها على الصعيدين الوطني والدولي"، *بحث منشور في مجلة الجامعة العراقية*، العدد ٥٩، (٢٠٢٣): ص٥٨٩.

(٤) فاروق خلف، " الآليات القانونية لمكافحة الجريمة المعلوماتية "، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة محمد خيضر بسكرة، الموسوم بعنوان: الجريمة المعلوماتية بين الوقاية والمكافحة،٢٠١٥،ص٨.

الخاتمة

في ختام هذا البحث توصلنا الى جملة من النتائج والتوصيات سندرجها على النحو التالي :

أولا : النتائج :

١. أن الجرائم السيبرانية ظاهرة إجرامية حديثة وليدة التطورات الهائلة في نظم تقنية المعلومات والاتصالات وتُعد من أكبر السلبيات التي خلفتها الثورة المعلوماتية، لكونها تتمثّل في اعتداءات خطيرة على الأفراد والمؤسسات وأمن الدول، وهو ما يترك في النفوس شعوراً بعدم الثقة وانعدام الأمن في التعامل والاستفادة من الثورة الرقمية.

٢. أن الجرائم السيبرانية تختلف عن الجرائم العادية من حيث أسلوب ارتكابها فهي جرائم ناعمة لا تحتاج مجهود بدني بل إلى الموهبة والمهارة الفنية والتقنية وكما تختلف من حيث شخص مرتكبها والوسيلة المستعملة في ارتكابها وهي من الجرائم الصعبة الاكتشاف والتي تحتاج إلى خبراء مختصين في التحقيق فيها لأن المجرم لا يترك أثراً عند ارتكابها .

٣. أن الجرائم السيبرانية كثيرة ومتشعبة وتتعدد صور ارتكابها بين الإرهاب والمخدرات والإتجار بالبشر إلى السب والقذف والقرصنة والجرائم المالية واختراق المواقع ومنها ما يشكل جناية خطرة وتتدرج لتصل الى الجنح وهي جرائم يصعب حصرها.

٤. أن تنامي ظاهرة الجرائم السيبرانية عبر الوطنية، وتخطي آثارها حدود الدول، أفرز جملة من التحديات القانونية على الصعيد الإجرائي تجسدت أساساً في بعض الصعوبات التي تكتنف إثبات هذه الجرائم وقبول الدليل بشأنها باعتبارها لا تترك أثراً مادياً ملموساً.

٥. ورغم الجهود التي بُذلت ولا تزال تُبذل، فإن هذه التحديات تبقى مستعصية على الحل في كثير من الأحيان في غياب استراتيجية واضحة للتعامل مع هذه الطائفة من الجرائم ومرتكبيها لاسيما في الدول التي لم تبادر بعد إلى تعديل تشريعاتها بما يكفل تجاوز القوالب القانونية التقليدية التي لم تعد تناسب هذا العصر.

ثانيا : التوصيات:

١. وجوب تعديل نظام مكافحة جرائم السيبرانية ونظام الإجراءات الجزائية بما يتلاءم مع أنواع الجرائم السيبرانية وخطورتها وطرق مكافحتها ، وذلك من خلال إنشاء مركز دولي مقره الأمم المتحدة يسمى "المركز الدولي لمكافحة جرائم السيبرانية، لتنسيق الجهود في مجال مكافحة الجرائم السيبرانية، وعقد المؤتمرات الدولية ذات العلاقة بالجرائم السيبرانية وإعداد الاتفاقيات الدولية أيضاً ذات الصلة بالموضوع.

٢. إبرام اتفاقية دوليّة لتعزيز التعاون الدولي بجميع صوره لمواجهة التحديات الإجرائية الناجمة عن الجرائم السيبرانية عبر الوطنية ، على ان تكون هذه الاتفاقية من الاتفاقيات الشارعة التي تلتزم بها الدول كافة وذلك لخطورة هذا النوع من الجرائم وتداعياته على السلم والامن الدولي .

٣. إنشاء محاكم أو دوائر متخصصة في الجرائم السيبرانية في كل المجالس القضائية لمجابهة هذه الظاهرة ، وهذا الامر ينطبق على الدول والمجتمع الدولي على حد سواء .
٤. تعزيز التعاون والمساعدة الوطنية والدولية في مجال مكافحة جرائم الإنترنت وذلك من خلال إعداد وتبني استراتيجية موحدة من الأمانة العامّة لمجلس التعاون لدول الخليج العربية تنطلق من رؤيتها وأهدافها ومبادئها والخطط والبرامج التنفيذية لمواجهة الجرائم السيبرانية.
٥. بناء القدرات في مجال تقنية المعلومات لرصد وتحليل التهديدات الأمنيّة المحتملة للجرائم السيبرانية وآثارها والإنذار المبكر باحتمالات وقوعها .
٦. بناء القدرات في مجال العدالة الجنائية (الشرطة والادعاء العام – القضاء) لتطوير التحقيقات الجنائية في مجال الجرائم السيبرانية والأدلة الرقمية وذلك بتوفير التدريب والتأهيل المناسب لرفع الكفاءة المهنية في هذا المجال الذي يواجه قصوراً نسبياً ملحوظاً.
٧. عقد اللقاءات في المدارس والجامعات، وحثَّ دور العبادة والمؤسسات الدينية من أجل توعية المجتمع بمخاطر هذه الجرائم وأثرها على المجتمع، وعقد الورشات والمؤتمرات الوطنية في مجال مكافحة الجرائم السيبرانية بهدف تبادل الخبرات والخروج بالتوصيات التي تساهم في حل المشكلات الناتجة عن هذه الجرائم وتشجيع البحث والتطوير في مجال الحماية من الجرائم السيبرانية.
٨. اتخاذ التدابير اللازمة لحماية البنيات التحتيّة الحساسة وتعزيز صمودها في وجه الاختراقات والهجمات الإلكترونية.

قائمة المصادر

أولاً: الكتب

١. احمد طارق عفيفي صادق، *الجرائم الالكترونية جرائم الهاتف المحمول*، القاهرة: المركز القومي للإصدارات القانونية، ٢٠١٥.
٢. تميم عبدالله سيف التميمي، *الجرائم المعلوماتية في الاعتداء على الأشخاص* ، ط١، الرياض: مكتبة القانون والاقتصاد ، ٢٠١٦.
٣. د. طوني ميشال عيسى، *التنظيم القانوني لشبكة الأنترنت*، لبنان: دار صادر، ٢٠٠١.
٤. د.احمد عبيد الكعبي، *الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت*،ط٢، القاهرة: دار النهضة العربية، ٢٠٠٩.
٥. سامي الشوا، *ثورة المعلومات وانعكاساتها على قانون العقوبات*،ط١، القاهرة: دار النهضة العربية، ١٩٩٤.
٦. عبد الله عبد الكريم عبد الله، *جرائم المعلوماتية والإنترنت*، بيروت: منشورات الحلبي الحقوقية، ٢٠٠٧.
٧. علي جبار الحسيناوي، *جرائم الحاسوب والأنترنت*، عمان: دار اليازوري العلمية للنشر

والتوزيع، ٢٠٠٩.
٨. محمود أحمد القرعان، *الجرائم الإلكترونية*، ط١، عمان: دار وائل للنشر والتوزيع، الاردن، ٢٠١٧.
٩. محمود أحمد عبابنة، *جرائم الحاسوب وأبعادها الدولية*، ط١، الاردن: دار الثقافة للنشر والتوزيع، عمان،٢٠٠٩.
١٠. د. سليمان احمد فضل، *المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية*، القاهرة: دار النهضة العربية، ٢٠١٣.
١١.
١٢. د. خليل يوسف جندي ميراني، *سياسة التجريم في ظل العولمة(دراسة مقارنة)*، ط١، ايران: رانم، ،٢٠١٨.
١٣. عبد الكريم الردايدة ،*الجرائم المستحدثة واستراتيجية مواجهتها* ،عمان: دار الحامد للنشر والتوزيع، ط ١ ، ٢٠١٣،ص٢٥٢.

ثانياً: البحوث والدراسات

١. احمد بن خليفة، حفوظة الأمير عبد القادر، "الجريمة الالكترونية وآليات التصدي لها"، *بحث منشور في مجلة الامتياز لبحوث الاقتصاد والادارة*، المجلد ١، العدد١ ،(٢٠١٧).
٢. أحمد عبد الله الخشاشنة، "تحريز الأدلّة الرقميّة وأثرها في كشف الجريمة"، *مجلّة الدراسات الأمنيّة*، المجلد١، العدد١٦، الأردن،(٢٠١٩).
٣. أسامة مهمل، "الإجرام السيبيراني"، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف-المسلية، الجزائر، ٢٠١٨.
٤. أيسر محمد عطية، "دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الالكتروني وطرق مواجهته"، *ورقة بحثية مقدمة في الملتقي العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية*، عمان، الاردن،(٢٠١٤).
٥. عبد اللطيف معتوق، "الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري او التشريع المقارن"، رسالة ماجستير، جامعة العقيد الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، ٢٠١٢.
٦. د. حمزه بن فهم السلمي، "الجرائم المعلوماتية والضوابط القانونية لمكافحتها على الصعيدين الوطني والدولي"، *بحث منشور في مجلة الجامعة العراقية*.
٧. د.احمد عبد الكريم عبد الوهاب و د. محمود عبدالرحمن خلف، "اشكالية الأمن السيبراني العراقي بين التهديدات السيبرانية والتقنين المقيد للحريات"، *بحث منشور في مجلة باسية*، المجلد ١٢، العدد ٦٠، (٢٠٢٠).
٨. د.عبد العزيز بن فهد بن محمد بن داود، "الجرائم السيبرانية : دراسة تأصيلية مقارنة"، *بحث منشور في مجلة الاجتهاد للدراسات القانونية والاقتصادية*، المجلد ٩، العدد ٣، (٢٠١٩).

٩. روان بنت عطية هلا الصحفي، "الجـرائـم السيبـــرانيـة"، بحث *منشور في مجلة الإلكترونية الشاملة متعددة التخصصات*، المجلد ١،العدد ٢٤ ، بدون بلد النشر،(٢٠٢٠).
١٠. عبد اللطيف معتوق، "الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري ,التشريع المقارن"، رسالة ماجستير، جامعة العقيد الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، ٢٠١٢.
١١. عبدالعزيز بن فهد محمد بن داود، "الجرائم السيبرانية : دراسة تأصيلية مقارنة"، بحث *منشور في مجلة الاجتهاد للدراسات القانونية والاقتصادية*، المجلد ٩، العدد ٣، (٢٠٢٠).
١٢. ليون برخو، "الهاكطولوجيا ودورها في تفسير الهجمات الالكترونية وتأثيرها على الممارسة الصحفية دراسات اعلامية"، *مركز الجزيرة للدراسات*، (٢٠١٧).
١٣. فتيحة رصاع، "الحماية الجنائية للمعلومات على شبكة الأنترنت"، رسالة ماجستير، جامعة أبي بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية،٢٠١٢.
١٤. لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركانها وآلية مكافحتها دراسة تحليلية مقارنة"، *بحث منشور في مجلة الميزان للدراسات الإسلامية والقانونية*، المجلد ٤، العدد ١، (٢٠١٧).
١٥. مريم عبد اللطيف المسلماني، "مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الإلكترونية"، *مجلة القانون والمجتمع*، المجلد ١٠ ، العدد ٢ ، (٢٠٢٢).
١٦. معهد دبي القضائي، "قانون مكافحة الشائعات والجرائم الإلكترونية لدولة الإمارات العربية المتحدة مرسوم بقانون اتحادي رقم (٣٤) لعام (٢٠٢١) التشريعات والقوانين لدولة الإمارات العربية المتحدة ١٦"، *معهد دبي القضائي، دبي*، (٢٠٢٢).
١٧. فاروق خلف، " الآليات القانونية لمكافحة الجريمة المعلوماتية "، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة محمد خيضر بسكرة، الموسوم بعنوان: الجريمة المعلوماتية بين الوقاية والمكافحة، ٢٠١٥.
١٨. نرمين سليمان، "أثر الجرائم الإلكترونية على الأبعاد الداخلية للأمن القومي: دراسة حالة المملكة العربية السعودية خلال الفترة من (٢٠٠٦) الى (٢٠١٦)"، رسالة دكتوراه في العلوم السياسية، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية، مصر، ٢٠١٨.
١٩. د. نبراس ابراهيم مسلم، "الجرائم السيبرانية وأثرها على الأمن السيبراني"، *بحث منشور في مجلة القادسية للقانون والعلوم السياسية*،المجلد١٢، العدد١، (٢٠٢١).
٢٠. محروس نصار غريب، "الجريمة المعلوماتية"، *بحث منشور في مجلة التقني*، المجلد٢٤، العدد١٠، (٢٠١١)، ص٢١.

ثالثاً: القوانين والتشريعات

١. بلغاريا، الفصل التاسع، القانون الجنائي رقم (٩٢)، لسنة (٢٠٠٢).
٢. بوتسوانا، قانون جرائم الإنترنت والحاسوب (٢٠٠٧).
٣. تونغا ، قانون الاتصالات لعام (٢٠٠٠).

٤. جامايكا قانون الجرائم المتعلقة بالشبكات الإلكترونية (٢٠١٠).
٥. عمان، مرسوم ملكي رقم (١٢)، لسنة (٢٠١١)، بإصدار قانون مكافحة جرائم الإنترنت، الفلبين، قانون مكافحة الجرائم الإلكترونية ٢٠١٢.
٦. قانون تنظيم واختصاص السلطات الحكومية لمكافحة جرائم التكنولوجيا العالية (٢٠١٠).
٧. قانون جرائم الحاسوب السوداني(٢٠٠٧).
٨. قانون جرائم الحاسوب السيرلنكي (٢٠٠٧)
٩. قانون جرائم الحاسوب الماليزي(١٩٩٧)
١٠. القانون رقم (٩٩١٨)، ٢٠٠٨، فرنسا
١١. قانون مكافحة جرائم تقنية المعلومات المصري رقم(١٧٥)، لعام (٢٠١٨).
١٢. قانون منع اساءة استعمال أجهزة الاتصالات رقم (٦)، لعام (٢٠٠٨)، اقليم كوردستان العراق.
١٣. كمبوديا مشروع قانون جرائم الإنترنت (٢٠١٢).
١٤. المملكة العربية السعودية ، القانون الجنائي لتكنولوجيا المعلومات لعام (٢٠٠٧).
١٥. ناميبيا، قانون إساءة استعمال الحاسوب والجرائم الحاسوبية (٢٠٠٣).
١٦. نظام المرافعات الشرعية السعودية ، لعام (٢٠١٣).
١٧. نظام مكافحة جرائم معلوماتية السعودية، لعام (٢٠٠٧).
١٨. القانون العربي النموذجي في شأن مكافحة جرائم الكومبيوتر والأنترنت

رابعاً: الاتفاقيات الدولية

١. إتفاقية الامريكية المتعلقة بجرائم الحاسب الالي والانترنيت، لعام ١٩٩٩.
٢. اتفاقية بودابست لمكافحة جرائم المعلوماتية، لعام ٢٠٠١،صادرة عم مجلس أوروبا
٣. الاتفاقية المتعلقة بالتعاون بين بلدان كومنولث الدول المستقلة، الفقرة (أ) المادة الأولى.

خامساً: المواقع الالكترونية

١. نحو تشريع قانون جرائم المعلومات: ar.parliament.iq\2018\10\13\2
٢. الشبكة الدولية، متاح على الرابط التالي www.minshawi.com .
٣. ينظر تقرير منظمة هيومنرايتسووتش وعلى الرابط الالكتروني التالي:
٤. https://www.hrw.org/sites/default/files/reports/iraq
٥. المادة (٨)، من بروتوكول ستراسبورغ، عام ٢٠٠٣، والذي يطلق عليه البروتوكول الإضافي لاتفاقية الجريمة المعلوماتية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهة الأجانب التي ترتكب عبر أنظمة الكومبيوتر، متاح على الرابط الالكتروني التالي : coe.intLtreatyLfrLtreatiesLHtmlL189.htm ،http:Lconventions.

سادساً: المصادر الأجنبية

1. B. Arief، M.A. Bin Adzmi، and T. Gross،Understanding Cybercrime from Its Stakeholders‘ Perspectives: Part 1—Attackers،‖ IEEE Security & Privacy، vol. 13، no. 1،2015.
2. Babu، M.، & Parishat، M. (2004). What is cybercrime? Retrieved August 8، 2023، Available from http://www.crime research.org/analytics/702./
3. Baiden، John E. "Cyber Crimes، A PAPER PRESENTED ON: CYBER LAWS IN PAKISTAN; A SITUATIONAL ANALYSIS AND WAY FORWARD June 24، 2006.
4. Hemraj Saini، Yerra Shankar Rao، T.C.Panda / International Journal of Engineering Research and Applications (IJERA) ISSN: www.ijera.com Vol. 2، Issue 2،Mar-Apr 2012.
5. Krishnan، Dolly & Mohit Verma، Cyber security And Cyber Laws around the World and India: Major Thrust Highlighting Jharkhand for Concerns، Indian Politics & Law Review Journal، The Law Bridge Publishers، 20th. July،(2020).
6. Marco Roscini، "World Wide Warfare- Jus ad bellum and the use of Cyber Force"، Max Planck Yearbook of United Nations Law، Volume 14، 2010، p.91.
7. McQuade، III، S.Understanding and managing cybercrime‖، Boston: Pearson/Allyn and Bacon،(2006).
8. Melissa Hathaway، Francesca Spidalieri، and Fahad Alsowailm، Kingdom of Saudi Arabia Cyber Readiness at a Glance، Potomac Institute for Policy Studies.
9. Michael Gervais، "Cyber Attacks and the Laws of War"، Berkeley Journal of International Law، vol. 30، lss. 2، 2012.
10. Michael N.Schmitt، Tallinn Manual on the International Law Applicale to Cyber Warfare، Prepared by the International Group of Experts at the Invitationof the NATO cooperative cyber defence Center of excellence، Cambridge University press، 2013.

11. Hong Lu، Bin Liang، Melanie Taylor، A Comparative Analysis of Cybercrimes and Government Law Enforcement in China and United States. Published in Springer Science،2010.

12. Micheal S.Fuertes، "Cyber warfare، Unjust Actins in a just war"، Florida International University، Full 2013.
13. Moitra، S. Developing Policies for Cyber crime. European Journal of Crime، Criminal Law and Criminal Justice،(2005)..
14. Moses A. A. and Hight C. I، 'Cyber Crime Detection and Control Using the Cyber Under Identification Model'، International Journal of Computer Science and Information Technology and Security، Vol5،2015، Issue-5.
15. Nayak، S. D.Impact Of Cyber Crime:Issuues and CHallenges ،October 2013.
16. P. R.K.Chaubey، An Introduction to Cyber Crime and Cyber law، Kamal Law House،2012.

17. REGNER SABILLON، JEIMY CANO، VICTOR CAVALLER، JORDI SERRA،Cybercrime and Cybercriminals: A Comprehensive Study،VOL. 4، NO. 6، JUNE 2016.
18. S. Philippsohn. Trends in Cybercrime—An Overview of Currentfinancial Crimes on the Internet. Computers & Security، (2001).
19. Sarah Gordon، Richard Ford، On the Definition and Classification of Cybercrime. Springer-Verlag France،Vol 2،(2006).
20. Scott Charney And Kent Alexsander، Computer Crime،1996،Vol 45، Emory L.J.
21. Shin، Beomchul، "The Cyber Warfare and the Right of self-Defense: Legal perspectives and the Case of the United States، IFANS، VOI.19، N1، June 2011.
22. Sunil. C. Pawar، Dr. R. S. Mente & Bapu. D.Chendage،Cyber Crime، Cyber Space and Effects of Cyber Crime،nternational Journal of Scientific Research in Computer Science، Engineering and Information Technology،Volume 7، Issue 1،February-2021.

23. United Nations Office on Drugs and Crime - UNODC (2013). Comprehensive studyonCybercrime‖.Vienna،Austria<https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.