مجلة رسالة الحقوق ISSN-2032-2075

القصـــور التشـــريعي في مواجهـــة الجرائـــــم السيبرانيـــة
(بين غياب النصوص وضبابية التكييف القانوني)

Legislative shortcomings in addressing cybercrimes between the absence of texts and the ambiguity of legal classification.

بحث مقدم من قبل
الاستاذ المساعد الدكتور هناء اسماعيل ابراهيم الاسدي
جمهورية العراق / وزارة التخطيط

الخلاصة:
حظى موضوع الجريمة السيبرانية بأهمية كبيرة في المجتمع الدولي اذ ان طبيعتها الدولية فرضت على المجتمع الدولي تبني سياسات فاعلة لمواجهتها لا سيما وان اهميتها تنبع من طبيعتها القانونية الخاصة فهي من الظواهر البارزة في العالم الحديث فلا يقتصر تأثيرها على الافراد بل يطال المؤسسات والشركات والانظمة الحكومية والامن القومي للدول وعليه فأن القصور التشريعي تجاه هذه الجرائم قد احدث خللاً في عملية مواجهة الجريمة السيبرانية واثر بشكل واضح على تحقيق العدالة الجنائية في مكافحته بالتالي فأن ضعف التشريعات القانونية والاجراءات ادى الى ضعف قدرة السلطات في التصدي لها، فهذه الجرائم تفرض ضغوطاً كبيرة على الانظمة الامنية والقانونية مما يستلزم التطور المستمر في السياسات والتشريعات لمكافحتها ومما زاد من حدتها وتأثيرها انها جرائم يصعب اكتشافها واثباتها امام القضاء وعليه شرعت العديد من الدول لتقنين هذه الظاهرة لغرض ردعها والحد منها وذلك على الصعيدين الدولي والمحلي ومن ثم محاولة التصدي لها بوسائل واستراتيجيات مستحدثة.

الكلمات المفتاحية : القصور التشريعي ، المواجهة ، الجرائم السيبرانية، غياب النصوص ،ضبابية التكييف القانوني.

Abstract
Cybercrime is of great importance to the international community, as its international nature has compelled the international community to adopt effective policies to confront it, especially since its importance stems from its special legal nature. It is one of the prominent phenomena in the modern world, as its impact is not limited to individuals, but also extends to institutions, companies, government systems, and the national security of countries. Therefore, the legislative shortcomings regarding these crimes have created a flaw in the process of confronting cybercrime and have clearly affected the achievement of criminal justice in combating it. Consequently, the weakness of legal legislation and procedures has led to a weakness in the ability of authorities to confront it. These crimes impose great pressure on security and legal systems, which necessitates the continuous development of policies and legislation to combat them. What has increased their severity and impact is that they are crimes that are difficult to detect and prove in court. Therefore, many countries have begun to legislate this phenomenon in order to deter and reduce it at the international and local levels, and then try to confront it with new means and strategies.

Key words: Legislative shortcomings , addressing cybercrimes , the absence , the ambiguity , legal classification

المقدمة

تعد الجريمة السيبرانية حديثة عهد فقد ظهرت وتطورت بظهور وتطور التكنولوجيا، فهي جريمة مبتكرة ومتطورة عابرة للحدود ذات خصائص مختلفة كليا عما هي عليه في الجريمة التقليدية مما جعلها صعبة الخضوع لمجريات التحقيق في الجريمة التقليدية، كما انها جرائم متنوعة متعددة متطورة غير محدودة الزمان والمكان، فأصبحت الجريمة السيبرانية الشغل الشاغل للمجتمعات والدول بسبب سرعة تطورها وازدياد حدة اثارها ووقعها على المجتمعات وانعكاساتها السلبية على كيانات الدول فأصبح بذلك لزاماً على الدول اتخاذ تدابير امنية ووضع استراتيجيات وسن تشريعات لمكافحة هذه الجرائم او على الاقل التقليل من أثارها.

اهمية الدراسة

ان دراسة كل جريمة هي ذات اهمية امنية قبل كل شيء وتبرز اهمية دراسة هذا الموضوع في كونه يسلط الضوء على ثغرات قانونية حقيقة تؤثر على فاعلية المواجهة القانونية للجرائم السيبرانية ومدى خطورة عدم وجود قوانين لردعها وان وجدت فأنها لم تخلو من الثغرات لذلك فأن من غير المجدي ان تخضع الجرائم السيبرانية للقوانين ذاتها التي تخضع لها الجريمة التقليدية.

اشكالية الدراسة

تنطلق الدراسة من اشكالية رئيسة مفادها كيف ساهم القصور التشريعي في تفاقم الجريمة السيبرانية، وما هي انعكاسات ذلك على تكييفها مع مكافحة الجريمة السيبرانية.

فرضية البحث

تنطلق الدراسة من فرضيات مفادها:

1- ان غياب نصوص قانونية صريحة يشكل عقبة امام تجريم الافعال السيبرانية

2- ان غموض بعض التشريعات القانونية في مكافحة الجريمة السيبرانية تؤدي الى تضارب الإراء والاحكام القضائية حولها.

منهجية الدراسة

من اجل اتمام الدراسة وفق منهجية علمية واثبات الفرضية التي تستند اليها فقد اتبع المنهج التحليلي من خلال تحليل النصوص القانونية والمنهج المقارن لاستعراض التجارب الدولية.

المبحث الاول/ الاطار المفاهيمي للقصور التشريعي والجريمة السيبرانية

ان الشروع بتوضيح ما يقصد بالجريمة السيبرانية والقصور التشريعي فيها يعد خطوة هامة لإيضاح ما قد يواجه القارئ من مصطلحات ومفاهيم تطرأ عليه ولكي تكون هناك صورة ذهنية حول ما سيتم تناوله في هذه الدراسة وكما يأتي

المطلب الاول / مفهوم القصور التشريعي للجريمة السيبرانية وخصائصها

تتعدد التعريفات الخاصة بالقصور التشريعي وتتعدد بحسب وجهات النظر لدى الباحثين الا ان اهم تلك التعريفات هو وجهة نظر الفقه القانوني فما هو القصور التشريعي في الفقه القانوني؟

الفرع الاول :تعريف القصور التشريعي

يقصد **بالقصور التشريعي** في الفقه القانوني هو الحالة التي لا ينظم فيها القانون المسألة كما ينبغي ان يكون وفقاً للقواعد العامة والمعايير القانونية والذي يتمثل في ثغرات تخل في تكامل النظام القانوني وآلياته، اذ انه يحدث عندما لا تقدم مصادر القانون اي قاعدة قانونية لحل مسألة متطورة مثل الجريمة السيبرانية[1] في حين تعددت واختلفت تعريفات القصور التشريعي باختلاف وجهات نظر الباحثين ومنها ما يعرف **القصور التشريعي** هو عدم موائمة النصوص التشريعية للحياة الاجتماعية والسياسية السائدة في المجتمع وقت تطبيق تلك النصوص وعدم تضمن النص التشريعي لما تقوم اليه الحاجة من احكام تفصيلية او جزئية في ظل تغيرات جوهرية فهو يعبر عن تطور قضايا المجتمع تطوراً جوهرياً وعدم قدرة النصوص القانونية التي وضعت في وقت سابق على مواكبة هذا التطور[2].

الفرع الثاني: مفهوم الجريمة السيبرانية

تعرف الجريمة عموماً «فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبراً احترازياً»[3] اما الجريمة السيبرانية فتعرف بأنها كل نشاط اجرامي يتم باستخدام تقنية المعلومات والشبكات السيبرانية، يهدف الى الحصول على المعلومات او التلاعب بها او تدميرها او ايذاء الافراد او المؤسسات او الاضرار بالأنظمة السيبرانية، وتتميز بأنها (الجريمة السيبرانية) تتم بشكل سريع دون ان تترك اي اثر مادي ملموس مما يجعل من الصعب التحقيق فيها ومحاسبة مرتكبيها [4] وتعرف الجريمة السيبرانية في الفقه الدستوري بأنها كل فعل غير مشروع يقوم به كل من يمتلك القدرة على استخدام التكنولوجيا والحاسبات الآلية بكفاءة عالية لإرتكابه من ناحية وملاحقته من ناحية اخرى اذ ان القائمون على ارتكابها يكونوا على درجة عالية من الدراية بهذه التكنولوجيا. [5]

الفرع الثالث: خصائص الجريمة السيبرانية

للجريمة السيبرانية خصائص مختلفة تميزها عن الجريمة التقليدية متمثلة بالاتي:

1- **الجريمة السيبرانية عابرة للحدود:** فهي جرائم تقع بين اكثر من دولة وهي بذلك غير معترفة بالحدود الجغرافية مثلها مثل جرائم غسيل الاموال، فان اهم ما اضفته الشبكات السيبرانية هو الطبيعة الدولية العابرة للحدود فيمكن للمجرم المعلوماتي ارتكاب الجريمة في بلد ما والمجني عليه في بلد آخر وقد يكون الضرر الواقع على البيانات في بلد آخر، فهي لا تعرف الحدود الجغرافية للدول لارتباط العالم بشبكة

واحدة وهو احد اسباب الارتباك القضائي من حيث التحقيق القضائي والمحاكمة[6] كما وتتصف بسرعة تنفيذها سرعة التنفيذ: فلا يتطلب تنفيذ الجريمة السيبرانية الوقت الكبير وبضغطة واحدة على لوحة المفاتيح يمكن ان تنقل اموال طائلة تصل الى ملايين الدولارات من مكان الى اخر وهذا لا يعني انها لا تتطلب التحضير والتخطيط والاعداد قبل التنفيذ او استخدام برامج ومعدات معينة لتنفيذها[7]

2- الجرائم السيبرانية صعبة الاثبات: يستخدم مرتكبي الجرائم السيبرانية وسائل فنية معقدة وسريعة في احيان كثيرة قد لا تستغرق بضع ثواني فضلا عن سهولة محو الدليل والتلاعب فيه فضلا عن عدم تقبل القضاء في الكثير من الدول للأدلة الرقمية التقنية التي تتكون من دوائر وحقول مغناطيسية ونبضات غير ملموسة وتكمن صعوبة اثباتها في ان متابعتها واكتشافها يحدث عن طريق الصدفة ومن الصعوبة حصرها في مكان معين، فهي لا تترك اثر واضح، فما هي الا ارقام تدور في السجلات والمواقع كما ان غالبية الجرائم السيبرانية لم تكتشف بعد وتعود صعوبة ذلك لعدة اسباب :[8]

أ- لا تترك اثراً بعد ارتكابها .

ب- فضلا عن صعوبة الاحتفاظ بأثارها، ثم أنها قد لا تترك اثاراً.

ت- تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها اذ انها تعتمد على الكفاءة والخبرة ومستوى ذكاء عالٍ في ارتكابها.

ث- تعتمد على الخداع والضبابية في ارتكابها.

ح- جرائم ناعمة لا تمارس بالعنف ولا تحتاج الى اي مجهود عضلي عند ارتكابها.

3- الجريمة السيبرانية تعد جرائم ناعمة وشديدة الخطورة: بسبب خفتها وصعوبة اكتشافها تصنف بأنها جرائم هادئة، اذ يمكن ان لا يُلاحظ الشخص المتضرر ارتكابها أثناء تواجده على الشبكة، فالجاني يمتلك مهارات تقنية متقدمة تسمح له بالقيام بتلك الجرائم دون أن يتم الكشف عنها، مثل سرقة الأموال أو إرسال فيروسات ضارة إلى البرامج وأجهزة الكمبيوتر وهي كلها افعال غير ملموسة.[9] فهي جرائم لا تحتاج الى العنف والجثث وسفك الدماء او اي اثار اقتحام وسرقة اموال فكل ما تعتمد عليه هو رقمي تقني يعدل ويغير او يمحى كلياً او جزئياً من سجلات مخزونة على الحاسب الآلي وهو ما يرتبط ايضاً بصعوبة اكتشافها فأن خاصية كونها جرائم ناعمة مرتبطة بصعوبة اكتشافها واثباتها.[10] ورغم كونها جرائم ناعمة الا انها تتصف بشدة خطورة الآثار المترتبة عليها فما يترتب عليها من خسائر مالية وأثار نفسية جسيمة على فئات المجتمع المختلفة يجعلها اشد خطرا على المجتمعات لا سيما جرائم النصب والاحتيال التي تقع على البنوك والمؤسسات المالية والجرائم المتعلقة بالاطفال ثم ان ما يضاعف من خطورتها انه من الصعوبة بمكان التنبؤ بها او توقع حدوثها ومن يقوم بارتكابها فضلا عن عزوف ضحاياها عن التبليغ عما لحقهم من اضرار خوفا من المجتمع او خوف المؤسسات المالية من الحاق الضرر بسمعتها واسمها في السوق [11]

المطلب الثاني/ انواع الجرائم السيبرانية واسباب صعوبة اكتشافها

الفرع الاول: انواع الجرائم السيبرانية

تتنوع الجرائم السيبرانية وتتعدد ما بين جرائم شخصية واخرى قد تضر المصالح العامة بالتالي فأن تعددها وتباينها كبير وذلك بحسب المستهدفين منها وبحسب غاية مرتكبيها من ارتكابها وعليه سنقسم انواع الجرائم السيبرانية الى ما يأتي: [12]

1- جرائم الاعتداء على الحياة الخاصة: وتعني هذه الجرائم انتهاك حرمة الحياة الخاصة للأفراد متمثلة صور تلك الانتهاكات النشر العلني للوقائع الخاصة التي تمس الشخص كإفشاء واقعة اصابته بمرض مخزي او عجز عن سداد ديونه او نشر صور خاصة قد لا يرغب المجني عليه بكشفها، كذلك تشويه سمعته في نظر الجمهور او الاستيلاء على المعلومات الشخصية كالاسم والصورة والبيانات المتصلة بالحياة الخاصة

2- جرائم الاعتداء على حقوق الملكية الفكرية: وذلك يعني الاعتداء على الملكية الفكرية للأشخاص مثل سرقة العلامات التجارية وبراءات الاختراع، كذلك نسخ وتقليد البرامج ومن ثم اعادة انتاجها وصنعها دون تراخيص من اصحاب الاختراع والفكرة فهو اعتداء على الحقوق المالية والادبية

3- جرائم الاموال والسطو على اموال البنوك: متمثلة بالوصول غير المشروع لأموال البنوك والمصارف وارقام البطاقات الائتمانية ومن ثم تحويل الاموال من حسابات العملاء الى حسابات خاصة وتتم عمليات السرقة بطرق عديدة منها ان يقوم المجرم بإدخال بيانات غير صحيحة او تعديل بعض البيانات او مسحها بغرض اختلاس الأموال او نقلها، فضلا عن عمليات اخرى تتعلق بغسيل الاموال والتي تنتشر في صور متعددة منها المخدرات ولعب الأقمار والتزوير ولعل هذه الجرائم تكون واضحة للعيان من ناحية امكانية اكتشافها وهي لا تختلف عن الجرائم التقليدية في اثارها فهي تحمل المسمى نفسه والجميع على دراية بأنها غير شرعية ومخالفة للنظام [13]

4- جرائم استغلا الاطفال: تعد صناعة ونشر الاباحة جريمة في كثير من دول العالم خاصة تلك التي تستخدم الاطفال ويتخذ ذلك الاستغلال اشكالا متعددة انطلاقاً من الصور وصولاً الى التسجيلات المرئية (مقاطع الفيديو) وتستمر اثار هذه الجرائم حتى بعد انتهاء الاعتداء الفعلي وذلك بسبب استمرار تناقل الصور ونشرها وينتمي معظم منتجي هذه المواد الى فئتين واسعتين وهم المتربصون جنسياً بالأطفال ومجاميع الأجراء المنظم التي تجتذب ارباح طائلة نتيجة ترويجها [14]

الفرع الثاني: اسباب صعوبة اكتشاف الجريمة السيبرانية

لاشك ان فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الافعال الاجرامية التقليدية لذا من الطبيعي ان نعيد نفس الاختلاف في الاسباب والعوامل التي تدفع في ارتكاب الفعل الغير مشروع فضلاً عن ذلك تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الاسباب التي

تختلف عن الجرائم التقليدية كما ان الجاني الالكتروني يختلف عن المجرم العادي ويأتي في مقدمة اسباب الجريمة المعلوماتية غاية التعلم والتي تتمثل في استخدام الكمبيوتر والامكانيات المستحدثة لنظم المعلومات وهناك أمل الربح وروح الكسب التي كثيراً ما تدفع الى التعدي على نظم المعلومات بالأضافة الى الدوافع الشخصية والمؤثرات الخارجية[15] ويمكن رد الاسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية الى عدم ترك هذه الجريمة لأي اثر خارجي بصورة مرئية كما ان الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات اخرى لان الجريمة المعلوماتية جريمة عابرة الى الدول (دولية)فأن قدرت الجاني على تدمير دليل الادانة في اقل من الثانية الواحدة يشكل عامل اضافي في صعوبة اكتشاف هذا النوع من الجرائم فأن الجرائم المعلوماتية في اكثر صورها الفنية لا يلاحظها المجني عليه ولا يعلم بوقوعها وحجب السلوك المكون له واخفائه عن طريق التلاعب غير المرئي في الذبذبات الالكترونية كما ان المجني عليه يلعب دور اساسيا في صعوبة اكتشاف الجريمة المعلوماتية حيث يحرص البعض الى عدم الكشف عن ما تعرض له وابلاغ السلطات المختصة تجنباً للأضرار[16]

المبحث الثاني / الاشكاليات الموضوعية والاجرائية للجرائم السيبرانية

واجهت بعض الدول اشكالية القصور التشريعي في عملية مكافحتها للجريمة السيبرانية ما بين تشريعات ضبابية لا تتواءم وحجم الجريمة السيبرانية واخرى لم تشرع قانوناً لمكافحتها لا سيما في دول عالم الجنوب اذ ان بعض نصوص التشريعات لم يحالفها التوفيق واصابها القصور التشريعي لإغفالها مثل هذا الاتجاه التشريعي وعدم تضمينها بما يخدم التعاون الدولي في التصدي لهذه الظاهرة الاجرامية او عدم ترشيد وتوجيه المجتمع المحلي لمثل هذا التعاون رغم اهميته بالنظر لطبيعة مثل هذه الجرائم التقنية التي تتطلب مزيد من التنظيم والتعاون فيما بين الدول كونها جرائم دولية عابرة للحدود ويمكننا تناول بعض اوجه القصور التشريعي وكما يأتي:

المطلب الاول/ ضبابية التكييف القانوني واسبابه

سنقسم هذا المطلب الى فرعين وكما يأتي

الفرع الاول: غموض التكييف القانوني

ان صعوبة التكييف القانوني لهذه الجرائم تكمن في طبيعتها الخاصة اذ ان القواعد التقليدية لم تكن مخصصة لهذه الظواهر الاجرامية الحديثة وبالتالي فأن تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها اشكالية اثباتها، كما ويثور الشك في احيان كثيرة حول اي النصوص التجريمية هو الاصلح وايها اكثر تناسباً للتطبيق فخضعت مشكلة التنازع الظاهري بين النصوص لعدة قواعد وكما يأتي:

أ- النص الخاص يقيد النص العام

ب- النص طويل المدى يستغرق النص قصير المدى

ت- النص الاصلي يغني عن النص الاحتياطي

كما ووضعت قواعد اخرى لتوضيح التفسير والقياس للنصوص ومنها

أ- لا اجتهاد في مورد النص

ب- عدم جواز الاجتهاد والقياس في النصوص الجزائية

ت- النصوص الجزائية لا تحتمل التأويل ولا يتوسع في تفسيرها وتؤخذ بأضيق حدودها وغيرها من القواعد التي كفلت تفسير النصوص، الا ان كل هذه النصوص تقف عند خط احمر مفاده عدم جواز الخروج على مبدأ الشرعية وعدم جواز مخالفته فلا جريمة او عقوبة الا بنص ومن هنا تثار مشكلة كيفية التعامل مع الجرائم السيبرانية امام القضاء وسعياً لتجاوز هذه التحديات ووضع التشخيص الامثل لظاهرة الجرائم السيبرانية ومكافحتها على كافة الاصعدة اي من ناحية التجريم والعقاب والملاحقة الاجرائية فهذا يستلزم امرين اولهما [17]

أ- الاقتناع بخطورة هذه الظاهرة الاجرامية والتوفيق بين احترام مبدأ السيادة الوطنية لكل دولة في صورته التقليدية والنزول قدر المستطاع اما مقتضيات التعاون الدولي وبما يكفل نجاعة وفعالية تحقق الجهود التي تنصب في التصدي لظاهرة الجرائم السيبرانية

ب- تطوير البنية التشريعية الجنائية بذكاء تشريعي متواصل ومواكب ودؤوب يسد ثغرات الانظمة الجنائية وبما يجعلها قادرة على اخضاع هذه الجرائم لنصوصها ومواكبة التطورات التي يعتمدها مرتكبوا هذه الجرائم في تنفيذ جرائمهم على ان يتم هذا التطور في اطار ما يسمح به القانون وكفالة احترام مبدأ شرعية الجرائم والعقوبات من ناحية ومبدأ الشرعية الاجرائية من ناحية وان يتكامل هذا التطور في الدور والهدف مع المعاهدات الدولية

وتواجه القاعدة تحديان رئيسان على درجة كبيرة من الخطورة يتمثل التحدي الاول في اتجاه التشريعات العقابية في الوقت الحاضر الى التعابير الواسعة الفضفاضة والتحدي الاخر يتمثل في التوسع في التفسير والتي نتطرق لها بشيء من التفصيل فيما يأتي:

1- عدم قدرة النصوص التقليدية على التعامل مع الجرائم السيبرانية: وهو امر طبيعي في ضل تطور الاداة المستخدمة في ارتكاب الجريمة السيبرانية على الرغم من التشابه في بعض الجرائم السيبرانية مع الجرائم التقليدية مثل الابتزاز والسرقة والاحتيال على الاموال الا ان الاختلاف يكمن في الاداة المستخدمة فيها التي ادت الى تغيير طبيعة الجريمة ذاتها، لذلك استوجب وجود طرق ووسائل اخرى لمكافحتها ومواجهة المخاطر التي تشكلها كما وتتطلب تشريعات قادرة على التعامل معها لمواكبة تطورها، وكما ذكرنا سابقا كيف ان التشريعات لا يمكن ان تخضع لهوى التفسير فلا جريمة ولا عقوبة الا بقانون[18] ولا يمكن التوسع في تفسير نصوص القوانين بما يخرج هذه النصوص عن مضامينها فهي نصوص لا يتوسع ولا يجتهد فيها.

2- التعابير الواسعة الفضفاضة: المتفق عليه ان التشريعات الجزائية تتسم بدقة العبارات ووضوحها وتلقى مسؤولية ذلك على المشرع الذي يجتهد على وضع الصياغات والمفردات الدقيقة والمحددة فيترتب على ذلك ان اي تفسير يتوسع به يجب ان يكون لصالح المتهم ويجب ان يغلب كفة براءة المتهم على كفة ادانته، وفي حديثنا عن التعابير والمصطلحات فأنها انتشرت بشكل كبير حتى يصار الى استخدام القوانين التقليدية في مكافحتها وردعها فضلا عن اعتبار البعض منها ضمن الجرائم المستحدثة والامثلة على ذلك كثيرة منها الغش والتزوير المعلوماتي وعرقلة عمل واداء الحاسوب ادخال معلومات وهمية او مزورة والدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات والتلاعب بالبرامج والاعتداءات العمدية على نظام المعالجة الالية للمعطيات

ومن مظاهر القصور التشريعي التي ادت الى صعوبة التكييف وضبابيته هو التوسع في تعريفات الجرائم في القوانين الموضوعة لمكافحة الجريمة السيبرانية فقد اجتهدت في اختيار مجموعة من المفاهيم من عالم الحاسوب والانترنت ونظم المعلومات بأنها الاكثر شيوعاً في عالم الانترنت فضلا عن اختلاف تلك التعريفات من بلد الى اخر ومن قانون الى اخر فترتب على ذلك التباين في التعريفات نتائج عديدة يمكن اجمالها بالآتي:[19]

أ- عدم انضباط التعريفات في كثير من القوانين والتدليل على ذلك بالاختلاف في التعريف بين القوانين وكذلك بينها وبين الوثيقة

ب-توسعت بعض القوانين في التعريفات حتى ان بعضها قام بتعريف جرائم محددة بذاتها مثل تعريف جريمة الاحتيال المعلوماتي وتعريف الدخول غير المشروع والحقيقة هذا الامر غير مستساغ في السياسة التشريعية بأن يلجأ القانون لتعريف الجرائم وان كان هناك حكمة تشريعية فأن تعريفها يرد في مكانها من القانون وليس في المادة المخصصة للتعريفات في بدايته.

ج- معظم التعريفات واسعة فضفاضة غير دالة بدقة على التجريم المقصود من الفعل فمثل هذه التعريفات تكون صالحة للدراسات الاكاديمية لا للقوانين الاجرائية والتجريم.

د- ذهبت بعض التشريعات بعيداً حتى وصل الامر الى قيامها بتعريف ذات الجريمة بتسميات مختلفة ففي النظام السعودي اطلق عليها تسمية الجريمة السيبرانية بينما القانون القطري بتسميتها الجريمة السيبرانية والقانون العماني عرفها بجرائم تقنية المعلومات بالرغم من ان هذه التعريفات لا تزيد ولا تؤخر في التشريع وانها من شأن الفقه والقضاء.

بالتالي فأن ما آلت اليه تلك التعبيرات الواسعة والتعريفات واتخاذ المشرعين منحى آخر لغرض توضيح المقصود من الجريمة السيبرانية ادى الى تشتت واضح في عملية تجريم الاختراقات والانتهاكات السيبرانية اذ ان عدم الاتفاق على مصطلح واحد ما بين مشرعي القوانين في الدول على توحيد المعنى المقصود للجرائم ادى الى صعوبة تكييف الجريمة مع الجزاء الواقع عليها وكما وتمكن المجرم من الهروب والانفلات من العقاب بمجرد الرجوع على تفسير كل مشرع لتلك الجريمة كونها تعد تفسيرات متباينة اختلفت بحسب وجهة نظر كل مشرع فقد يتم تكييف جرائم الاختراق على انها دخول غير مشروع او تكييف الابتزاز الالكتروني كتهديد مما لا يعكس بدقة طبيعة الفعل الاجرامي.

الفرع الثاني: اسباب القصور التشريعي

ان اعمال القانون في مواجهة الاجرام السيبراني يستلزم اتخاذ اجراءات تتجاوز ما هو سائد في المدونة العقابية التقليدية لما تتسم به من الحداثة والسرعة وسهولة التنفيذ واخفاء الاثار بالتالي فأن ظهور هذه الانماط الجديدة من الجرائم يشكل عبئاً على الاجهزة القضائية الامر الذي يجب ان يرافقه اجهزة بمختلف انواعها على درجة عالية من الكفاءة والقدرة على التعامل مع الجريمة السيبرانية ولا يمكن تحقيق ذلك الا بتدريب الكوادر القضائية من خلال الاستفادة من خبرات ومهارات الاخرين عن طريق اشخاص اكفاء مؤهلين على نقل التجارب والمهارات وبما ان كفاءة الدول تختلف فيما بينها وذلك بحسب تقدم الدولة فأن اجهزة العدالة في الدول النامية ليست لديها الجاهزية لمواجهة الجرائم المتعلقة بشبكة الانترنت لافتقارها مقومات ذلك من الكفاءات البشرية والمادية الامر الذي يدعو الي ضرورة التعاون الدولي لتبادل تلك الخبرات والمهارات [20] كما ويمكننا ايجاز ابرز الاسباب التي ادت الى ظهور اشكالية القصور التشريعي فيما يأتي:[21]

1- نظرا لتنوع النظم القانونية الاجرائية من دولة الى اخرى فأن طرق الاستدلال والتحقيق والمحاكمة قد تثبت فائدتها في دولة ما لكنها قد تكون عديمة الفائدة في دولة اخرى او قد لا يسمح بأجرائها فيها، فاذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات او التحقيق على انها مشروعة في دولة ما فأنها قد تكون غير مشروعة في دولة اخرى وهو ما يدخل في اطار الاختلاف التشريعي بين الدول او مشكلات الاختصاص الدولي

2- هناك بعض التشريعات غير كافية للتعامل مع هذا التحدي الناشئ مما ينعكس في صعوبة تقديم العقوبات للمرتكبين وتطبيق القانون بشكل فعال ومن ثم تظهر الجريمة كتحدي دولي يتطلب تعاوناً فعالاً بين الدول لتطوير اطار قانوني شامل يمكّن من مواجهة التحديات المتزايدة وضمان حماية الامن الرقمي والمعلوماتي في الساحة الدولية

3- ضعف التعاون الدولي والتنفيذ الالزامي على الرغم من وجود اتفاقيات دولية الا ان عدد الدول المصدقة على بعض الاتفاقيات لا يتجاوز نصف العالم مما يضعف الزاميتها والتناغم القانوني الدولي لها، فضلا عن ما ينتج عنها من زيادة العبء الاداري في اجراءات التبادل القانوني الدولي والتي تعيق سرعة وفعالية الملاحقة القضائية [22]

4- سرعة التلف والتغيير في الادلة لذا تتطلب تحركاً سريعاً واجراءات صارمة لحفظها مما يثقل كاهل التشريعات القانونية لا سيما وان كل جزئية في الجريمة السيبرانية قابلة للتغيير لذلك فأن مسألة التشريع تتطلب وقت وجهد واحاطة بجزئياتها.

فضلا عما تقدم من القصور التشريعي الذي تعاني منه اغلب دول العالم نتيجة الاختلالات في التعاون الدولي الا ان هناك بلدان لا تزال بعض التشريعات فيها تفتقر الى نصوص قانونية صريحة تجرم بعض الافعال السيبرانية لا سيما الدول العربية ولكن لا يمكن القول بانعدام وجود تلك النصوص لأن غالبية دول العالم قد شرعت قوانين لمكافحة الجريمة السيبرانية ولكن تلك القوانين لم تخلو من الهفوات المتمثلة بصعوبة تكييفها او ضعف صراحتها بتجريم افعال معينة وعليه يمكننا الشروع بإيضاح نماذج لبعض البلدان التي عانت من القصور التشريعي وكما يأتي:

القصور التشريعي في القوانين العربية

ان وضع القانون وتطبيقه واستيعابه يتطلب مرور مدة من الزمن، ولكن ما نشاهده من سرعة التطور وجهل نتائجه تتموقع في منظور زمني آخر، ويكمن الخطر في سرعة تعرض كل قانون جديد للتجاوز والنقد والتعديل والالغاء وذلك بحسب دقة التفاصيل والجزئيات التي يعنيها وعليه فالأمر يجبر على التساؤل عن الوقت المناسب لتدخل التشريع وعن كيفية الاقتصار على المبادئ العامة مع امكانية تطويرها مستقبلاً فعلى الرغم من اهمية جودة واستقرار الاحكام القانونية وانها تعد من ضرورات الامن القومي الا انها سرعان ما تضعف نتيجة لهث القانون وعجزه عن مسايرة وتيرة التطور والتهافت التكنولوجي والعملي [23]، واذا كان المجال التكنولوجي يزعزع استقرار القانون ويزعج العقول القانونية المحافظة الا انه عامل فعال في تقدم القانون وتطوره لمواكبته التطورات التي طرأت على المجتمع وشكلت جملة الظواهر السلبية وابرزها الجريمة السيبرانية المستحدثة والتي تحتاج الى تشريع ليتصدى لها من خلاله. وفي الحديث عن الدول العربية ففي **العراق** لا يوجد حتى الان قانون خاص وشامل لمعالجة جميع اشكال الابتزاز سواء كان الكترونياً او مباشراً اذ يكون التعامل مع هذه القضايا استنادا الى مواد قانون العقوبات العراقي رقم 111 لسنة 1969 الا ان هذه النصوص التي وضعت قبل عقود لم تصمم لمواكبة اشكال الابتزاز الحديثة واساليبها المتطورة وبحسب القانون العراقي تدرج جرائم التهديد والابتزاز ضمن المواد (430-432) من قانون العقوبات وتصل العقوبة فيها تبعاً لخطورة الفعل الى السجن سبع سنوات، اما في **مصر** فلا يوجد نظام قانوني خاص بجرائم المعلومات حتى عام 2017، الا ان القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم السيبرانية والتي تفرض نوعاً من الحماية الجنائية ضد الافعال الشبيهة بالأفعال المكونة لأركان الجريمة السيبرانية [24] الا انه تم تلافي تلك الإشكالية عام 2018 وذلك بوضع قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 المصري، ولم تكن **فلسطين** بمنأى عن اوجه القصور التشريعي فمنذ وقت كان لا وجود لقانون خاص بجرائم السيبرانية في دولة فلسطين سوى تعديلات ادخلت على قانون العقوبات الصادر عام 1939 وكان ذلك عام 2003 كون ان النصوص القديمة لم تعد قادرة وكافية لمواجهة ظاهرة الجرائم السيبرانية مما دفع دولة فلسطين لوضع سياسة جنائية متطورة وما لبث كثيراً حتى صدر القرار بقانون رقم 10 لعام 2018 بشأن الجرائم السيبرانية [25]كما وعانت **المغرب والجزائر** من ذات الاشكالية اما في **مملكة البحرين** فلا توجد فيها قوانين خاصة بجرائم الانترنت وان وجد نص قريب عن الفعل المدان فأن العقوبة المنصوص عليها لا تتلاءم وحجم الاضرار المترتبة على جريمة الانترنت[26] وعليه فأن الشروع بإصدار القوانين الباتة والملزمة للحد من قضايا الجرائم السيبرانية اصبح ضرورة ملحة في عالمنا المعاصر لا سيما وان هذه الجرائم اصبحت تهدد امن المجتمع الدولي وعليه سنتناول في الفصل القادم اهم التشريعات التي تناولت مكافحة الجريمة السيبرانية وآليات الردع الخاصة بها.

المطلب الثالث/ الجهود الدولية والاقليمية لمكافحة الجريمة السيبرانية

اصبح لزاماً على المجتمع الدولي ان يتصدى لهذه الظاهرة ذات الطابع الاجرامي التقني بسن القوانين العقابية والاجرائية التي تتناسب وخطورة الجرائم السيبرانية ووضع المزيد من الضوابط لمكافحتها وللحماية من اخطارها على ان تنصب هذه الجهود في عدة محاور، منها تنظيم وحماية استخدام تقنية المعلومات من الجرائم والانتهاكات وحماية البيانات المتصلة بالحياة الشخصية وضمان حماية البيئة التقنية وعليه تكاتفت الجهود في مجال مكافحة الجريمة التقنية لوضع نصوص عقابية واجرائية لردع مثل هذه الجرائم وهو ما سنبينه في التقسيم الآتي:

الفرع الاول: الاتفاقيات الدولية

1- اتفاقية بودابست 2001

جاءت اتفاقية بودابست بضرورة اتباع سياسات جنائية قادرة على حماية المجتمع من الجريمة السيبرانية واشارت الى ضرورة توحيد السياسات الواجب اتباعها في مكافحة الجريمة السيبرانية وذلك من خلال العمل المشترك بين الدول والتعاون فيما بينها لتسهيل مكافحة الجرائم السيبرانية وتطبيق اجراءات التحقيق وملاحقة المجرمين ووضع نظام تعاون دولي يتمتع بسرعة وفاعلية التنفيذ ، وجاء نص المادة ٢٢ من الاتفاقية متضمن الاجراءات المتعلقة بالاختصاص القضائي للجريمة السيبرانية مؤكدا على ضرورة اعتماد الدول الأطراف على ما يلزم من تدابير تشريعية حتى تتمكن المحاكم في الدول الأطراف من ممارسة حقها في الاختصاص القضائي ضمن صلاحياتها المتعلقة بالجرائم الواردة في الاتفاقي[27]ة وكذلك نصت الاتفاقية على عدم استبعاد الاختصاص الجنائي لأحد الأطراف الذي ينص عليه احد الاطراف وفقاً لقانونه الوطني ومطالبة الاطراف في الاتفاقية بالتشاور حول الاختصاص الأكثر ملائمة لتطبيقه على مرتكبي الجرائم السيبرانية كما وتناولت الاتفاقية موضوعة التفتيش حيث نصت على ضرورة تبسيط الإجراءات فيما يتعلق بالتحقيق لكل من الدول الاعضاء الموقعة في الاتفاقية، من حيث تفتيش الأنظمة السيبرانية وتحويل السلطات المختصة بالتحقيق بإمكانية الدخول المراد تفتيشها والتي لها علاقة بالجريمة السيبرانية، وفضلا عما اشارت اليه الاتفاقية من مبادئ اجرائية متمثلة بتوفير تنسيق بين عناصر الجرائم السيبرانية والقانون الجنائي الوطني وانشاء نظام فعال للتعاون الدولي والزام الدول الموقعة على الاتفاقية بتضمين معلومات رقمية او

الكترونية في قوانينها الداخلية لاستخدامها كأدلة قانونية امام القضاء، والتأكيد على وجوب قبول الادلة السيبرانية كجزء من التحقيقات الجنائية[28]، فأنها نصت على اجراءات جنائية جديدة لمكافحة الجريمة السيبرانية متمثلة بالآتي:[29]

1- الحفظ السريع للمعطيات المخزنة
2- تجميع المعلومات الخاصة بالمشتركين وذلك لغرض تحديد هوية الجاني مثل فترة الاشتراك والاستخدام
3- التفتيش المعلوماتي فمن الضروري تأكيد الحصول على اذن رسمي لتفتيش البيانات السيبرانية وحجز الادلة
4- تخويل السلطات بالدخول على المعطيات السيبرانية
5- فرض اجراء التنصت كخطوة جديدة لمكافحة الجريمة السيبرانية
6-ضرورة التعاون الدولي لتبادل المعلومات بالسرعة الممكنة لغرض تفادي انفلات المجرم من العقاب لاسيما مرتكبي الجريمة السيبرانية العابرة للحدود
7- الالتزام والتنفيذ من خلال اصدار التشريعات واتخاذ الاجراءات الضرورية لتنظيم الجريمة السيبرانية، كما ويجب استخدام مصطلحات جديدة اقرب الى مجال التكنولوجيا مع مناقشة مسألة تطور المفاهيم في المجال السيبراني

2- الاتفاقية الافريقية لمكافحة الجريمة السيبرانية لسنة 2014 (اتفاقية مالابو)

تم تبنيها في يونيو 2014 خلال الدورة العادية الثالثة والعشرين لجمعية الاتحاد الافريقي في مالابو غينيا الاستوائية وقعت العديد من دول الاتحاد الافريقي عليها وقد تضمنت الاتفاقية احكاماً تتعلق بالتحقيق في الجرائم السيبرانية وملاحقة مرتكبيها واحكاما اخرى تتعلق بالمعاملات السيبرانية وحماية البيانات الشخصية[30] دخلت الاتفاقية حيز التنفيذ في 8 يونيو 2023 بعد تصديق 15 دولة عليها الزمت الأتفاقية الدول الاطراف فيها على ما يأتي[31]:

أ- مواءمة التشريعات الوطنية مع احكام الاتفاقية في محاورها والمتمثلة ب(المعاملات السيبرانية، حماية البيانات ذات الطابع الشخصي، تعزيز الامن الالكتروني ومكافحة الجريمة السيبرانية).
ب- تجريم الجرائم السيبرانية وتحديد الاختصاص وتوفير ادوات تحقيق وحفظ الادلة رقمية.
ت- انشاء آليات تعاون دولي مثل تقديم وتبادل المساعدة القضائية وتبادل المعلومات وتوفير نقاط اتصال لغرض تبادل الخبرات وتوفير الدعم المتبادل فيما بين الدول.
ث- تأسيس هيئة مستقلة لحماية البيانات واصدار اطر ترخيص.

كما وتناولت الاتفاقية تجريم الافعال غير المشروعة ومنها الدخول غير المشروع للمواقع واعتراض البيانات واتلافها او اتلاف الانظمة والاحتيال المعلوماتي والمحتوى الضار فضلا عن تشديدها على ألا تؤدي تدابير الامن السيبراني الى انتهاك الحقوق الدستورية المتمثلة بحرية التعبير والخصوصية [32]

3- اتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية 2010

بهدف تعزيز التعاون بين الدول العربية لمحاربة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها، فصدر عن جامعة الدول العربية دليل استرشادي لمكافحة هذه الجرائم فسعت لتجريم الاعمال غير المشروعة التي ترتكب بواسطة الفضاء السيبراني ودعا الدول المصدقة على الاتفاقية الى ضرورة موائمة تشريعاتها مع احكام الاتفاقية وتجريم جميع اشكال الجرائم المستحدثة كما وشجع المجلس الدول لمنع الارهابيين من استغلال تكنولوجيا المعلومات والاتصالات بهدف التحريض على دعم انشطتهم الارهابية وتخطيطها والاعداد لها وقد عنيت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بمواجهة عدة جرائم ومن اهمها:[33]

1- جريمة الدخول غير المشروع والاعتداء على سلامة البيانات.
2- جرائم التزوير والاحتيال.
3- الجرائم الاباحية وجرائم انتهاك حقوق الملكية الفكرية.
4- جرائم اساءة استخدام وسائل تقنية المعلومات و الاعتراض غير المشروع لخط سير البيانات.

الفرع الثاني: التشريعات الدولية والعربية

بدأت البلدان في تنظيم تشريعاتها لمواجهة النمط الجديد من الجرائم المستحدثة لمواكبة التطور السريع فيها لذلك قننت **فرنسا** عام 1988 ثم في عام 1994 بمقتضى تعديلات اساسية وجوهرية في قوانينها العقابية ظاهرة السيبرانية وفي **الولايات المتحدة الامريكية** اصدرت عام 1988 قانونين مختصين بالجرائم السيبرانية وهما كل من قانوني الغش والتعسف بالحاسوب وقانون سرية المخابرات السيبرانية وتطبق **كندا** قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الالي عام 1985 بوضع تعديلات على قانونها الجنائي وبما يشتمل على قوانين خاصة بجرائم الحاسب الآلي والانترنت كما شمل القانون الجديد تحديد عقوبات لجرائم المخالفات الحاسوبية وجرائم التدمير والدخول غير المشروع لأنظمة الحاسب الآلي[34]

اما الدول العربية يتفاوت مستوى الدول العربية في اتجاهها لمعالجة الجريمة السيبرانية ففي **العراق** ما زال المشرع العراقي يواصل التأجيل في اصدار قانون مخصص لتنظيم الجرائم السيبرانية بسبب الظروف الراهنة ومع ذلك تم تقديم مشروع قانون يحتوي على 33 مادة الى مجلس النواب الا ان تم الغاءه من قبل جهات معينة كونه قد يعارض مصالحها الخاصة ويمكن ان يكون سب التأجيل لمثل هكذا مشاريع قوانين هو عدم مراعاة المعايير والمبادئ اللازمة للتشريع ولكن هذا لا يعني عدم خضوع الجريمة السيبرانية للقانون بل يطبق عليها القوانين الآتية:

1- قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل.
2- قانون اصول المحاكمات الجزائية رقم (23) لسنة 1971.
فضلا عن قوانين اخرى متمثلة بقانون المطبوعات العراقي رقم (206) لسنة 1968 والذي يخص الصحف والمجلات ويستند عليه فيما ينشر على مواقع التواصل الاجتماعي وكذلك قانون الاثبات العراقي (107) لسنة 1979 وقانون مكافحة الارهاب رقم (13) لسنة 2005 فيما يخص جرائم الارهاب الالكتروني في المادة الاولى منه التي نصت على تجريم كل فعل اوقع بالممتلكات العامة او الخاصة او اثارة الرعب والخوف بأي وسيلة كانت
ويمكننا ان نتناول وبإيجاز موقف المشرع العراقي والحماية الجزائية بجريمة انتهاك المراسلات الالكترونية من خلال عناصر عدة وكما يأتي[35]
1- عرف المشرع العراقي القصد الجرمي في المادة 33فقرة1 من قانون العقوبات النافذ بأنه توجيه الفاعل أرادته الى ارتكاب الفعل المكون للجريمة هادفاً الى تحقيق نتيجة جرمية التي وقعت او اي نتيجة جرمية اخرى وبما ان انتهاك حرمة مراسلات البريد الالكتروني من الجرائم العمدية التي تتطلب توفر القصد الجرمي بعنصري العلم والارادة، لذا يجب على الفاعل ان يكون عالماً بأن فعله مخالفاً للقانون الالكتروني للغير أو التقاطها او حجبها عن المرسل أليهم أفعال تشكل قرينة على علم الفاعل بعدم مشروعيتها.
2- القصد الجرمي هو الارادة وتتحقق اذا ما اتجهت نحو ارتكاب الفعل المكون للجريمة من الحصول على النتيجة التي يستهدف حدوثها الفاعل او اي نتيجة جرمية اخرى حتى لو كان الفاعل لا يريد وقوعها غير المشروع في نظام المعالجة الالكترونية للبيانات او في جزء من يعاقب بالحبس لمدة سنة وغرامة قدرها (100000)مئة الف افرانك فرنسي فان نتاج الارادة بانه نشاط نفسي واع يتجه لاتجاهاً جدياً نحو غرض معين بحيث يسيطر هذا النشاط على الحركات العفوية ثم يدفعها نحو تحقيق هذا الغرض
ويجب ملاحظة ان الارادة المعتد بها قانوناً هي الارادة الصحيحة الصادرة عن إنسان مسؤول جزائياً ذي ارادة حرة غير مكره. أذ يعد الاكراه مانعاً من موانع المسؤولية الجزائية فتنص المادة (62) من قانون العقوبات العراقي النافذ على ان لا يسئل جزائياً من أكرهته على ارتكاب جريمة قوة مادية أو معنوية لم يستطع دفعها والعقوبة على ذلك تعد جريمة التنصت او الالتقاط او اعتراض المراسلات الالكترونية عن طريق شبكات المعلوماتية او وسائل تقنية المعلومات من جرائم الجنح ومن خلال ما تقدم يمكن لنا معرفة الاهمية البالغة التي تتمتع بها المراسلات الالكترونية بشكل عام ومراسلات البريد الالكتروني بشكل خاص وكونها من الحريات الحديثة واللصيقة بشخص الانسان والتي تعد من اهم الامور الحياتية الخاصة بالفرد لأنه غالباً ما يعمد من خلالها والتي تداول اسرار حياته الخاصة بينه وبين الاخرين ولكل ذلك لابد للمشرع الجزائي العراقي ان يأخذ بنظر الحسبان هذه المصلحة المستحدثة والجديدة بحماية القانون ولاسيما وان هنالك بعض القوانين التي تعاقب على حرمة الحياة الخاصة للإنسان عبر الشبكات المعلوماتية فحسب انما مجرد الدخول للنظام المعلوماتي بصورة غير مصرح بها يستدعي المشرع العراقي لسند الفراغ الشرعي لحماية مراسلات البريد الالكتروني لكونها تتضمن أسرار الحياة الخاصة للإفراد، وهناك نصوص تقترح أضافتها لقانون العقوبات العراقي:-
1-يعاقب بالحبس وبالغرامة او أحدى هاتين العقوبتين كل شخص فتح او التقط او حجب او اخفى او عدل رسالة الكترونية مرسلة بواسطة شبكة المعلومات او احدى وسائل تقنية المعلومات او افشى سراً تضمنته رسالة الكترونية.
2-اذا كان مرتكب احدى الافعال المذكورة اعلاه موظفاً او مكلفاً بخدمة في أحدى دوائر الاتصالات يعد ذلك ظرفاً مشدداً[36]
اما **الأمارات العربية المتحدة** فقد اصدرت مرسوما بقانون اتحادي رقم (34) لعام 2021 فيما يتعلق بمكافحة الشائعات والجرائم السيبرانية وبدأ تنفيذه في الثاني من يناير 2022 وجاء هدف القانون لتوفير اطار قانوني شامل لتعزيز حماية المجتمع من الجرائم السيبرانية التي تتم من خلال شبكات الانترنت والتقنيات ذات الصلة وحماية المواقع السيبرانية والبيانات الحكومية لدولة الامارات ومكافحة انتشار الشائعات والبيانات والاخبار المزيفة والاحتيال الالكتروني وحماية حفظ الخصوصية والحقوق الشخصية، فالقانون يوضح الافعال الممنوعة والعقوبات المترتبة على اي فرد يقوم بأنشاء او استخدام موقع الكتروني لغرض الاختراق والهجوم على نظم المعلومات والبيانات الحكومية وكذلك نشر المعلومات التي تضر امن الدولة كما ويتناول مجموعة من الجرائم السيبرانية المتنوعة الاخرى.
اما في **فلسطين** فقد وضعت سياسة جنائية متطورة تلبي احتياجات المجتمع الفلسطيني وتغطي العجز في التشريع النافذ فجاء نص المادة 393 لتعالج موضوع الاقتحام بطرق الغش لنظم المعلومات الخاص بالغير وكذلك تعطيل النظام او محو البيانات التي يحتويها النظام وفضلا عن تناوله جريمة الفساد وعرقلة الحاسب الآلي، فصدر قانون رقم 10 لسنة 2018 بشأن الجرائم السيبرانية ويمكن الاشارة لبعض الجرائم التي فرض لها عقوبة جنائية وكما يأتي: [37]
1- كل من اعاق او عطل الوصول الى الخدمة او الدخول الى الاجهزة او البرامج او مصادر البيانات او المعلومات بأي وسيلة كانت عن طريق الشبكة السيبرانية او احدى وسائل تكنولوجيا المعلومات.
2- كل من قام عمداً بفك بيانات مشفرة في غير الاحوال المصرح بها قانوناً.
3- كل من زور مستنداً الكترونيا من مستندات الدولة او الهيئات او المؤسسات العامة معترفا بيه قانوناً في نظام معلوماتي.
وغيرها الكثير من الجرائم السيبرانية التي نص عليها القانون منها حقوق الملكية الفكرية والادبية وكل أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على إحدى وسائل تكنولوجيا المعلومات، بقصد إدارة مشروع مقامرة أو تسهيله أو تشجيعه أو الترويج له أو عرض ألعاب مقامرة، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني ولا تزيد على ألف دينار

أردني[38]، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين، فضلا عن عقوبات اخرى لجرائم غسيل الاموال والمتاجرة بالأعضاء البشرية باستخدام تكنولوجيا المعلومات.

اما في **المملكة العربية السعودية** والتي كانت من اكثر الدول عرضة للجرائم السيبرانية غير المشروعة فقد صدر قرار رئيس مجلس الوزراء رقم 79 والمتعلق بنظام مكافحة الجرائم السيبرانية وصدق عليه بالمرسوم الملكي رقم (م/ 17) عام 2007 والذي تضمن آليات متكاملة لمكافحة الجرائم السيبرانية فقد تضمن المرسوم نصوصاً تجرم التنصت على ما هو مرسل الى اجهزة الحاسب الآلي دون مسوّغ نظامي صحيح والدخول غير المشروع للمواقع السيبرانية او اعاقة الوصول الى الخدمات او مسح البرامج او البيانات المستخدمة وتجريم كل فعل من شأنه المساس بأمن الدولة ومعلوماته فقد تصل العقوبات بالسجن لمدة لا تزيد عن عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال في الجرائم التي تمس أمن الدولة متمثلة بكل فعل من شأنه أن يؤدي إلى الدخول غير المشروع إلى موقع الكتروني او نظام معلوماتي مباشرة أو عن طريق الشبكة السيبرانية أو احد اجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي والخارجي للدولة[39] وفي **مصر** نالت الجريمة السيبرانية اهتمام المشرع المصري كما واصدر رئيس جمهورية مصر العربية قراراً برقم 276 لسنة 2014 بشأن الموافقة على انضمام جمهورية مصر العربية الى الاتفاقية لمكافحة جرائم تقنية المعلومات، وقد اصدر المشرع المصري القانون رقم 175 لسنة 2018 المتعلق بمكافحة جرائم تقنية المعلومات وقد حدد القانون مجموعة من الالتزامات على مقدمي الخدمة منها المحافظة على سرية المعلومات وخزنها وعدم افشائها او الافصاح عنها وحماية المعلومات المتعلقة بالمواقع والحسابات الخاصة التي يدخل عليها الاشخاص ومراعاة حرمة الحياة الخاصة، ولعل ابرز ما تم تجريمه في القانون المصري ما يأتي [40]

1- جريمة الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنينها.
2- جريمة تجاوز حدود الحق في الدخول الى الحسابات الخاصة ونظم السيبرانية.
3- جريمة الدحول غير المشروع الى على نظام معلوماتي محظور الدخول عليه.
4- جريمة الاعتراض غير المشروع بدون وجه حق على المعلومات والبيانات او كل ما هو متبادل عن طريق الشبكة السيبرانية او احد اجهزة الحاسب الآلي.
5- جريمة الاعتداء على سلامة المعلومات والبيانات والنظم السيبرانية سواء بتعطيل او اتلاف او تعديل او الغاء كلي او جزئي للبرامج والبيانات والمعلومات المخزنة او المعالجة او المولدة على اي نظام معلوماتي.
6 جريمة الاعتداء على البريد الالكتروني والحسابات الخاصة وجريمة الاعتداء على الانظمة السيبرانية الخاصة بالدولة.
7- جريمة الاعتداء على سلامة الشبكة السيبرانية والاحتيال على بطاقات البنوك والخدمات وادوات الدفع الالكتروني.

ومما تجدر الاشارة اليه ان مصر قد اصدرت قوانين كثيرة لمعالجة القضايا التي تعترضها قبل تشريع قانون رقم 175 المصري 2018 حيث اصدر المشرع المصري قانون مكافحة غسيل الاموال رقم 80 لسنة 2002 وقانون حماية الملكية الفكرية رقم 82 لسنة 2002 وقانون تنظيم الاتصالات رقم 10 لسنة 2003 وقانون التوقيع وعليه تعد مصر من الدول التي واكبت تطور الجريمة السيبرانية في تشريعاتها.

وعليه حاولت العديد من الدول وضع قوانين وتشريعات بغية الحد من ظاهرة مكافحة الجريمة السيبرانية او الحد منها لكن ذلك لا يعني انها قد المت بكل جوانب الجريمة السيبرانية كما ان هناك بعض الدول لم تشرع قوانين لمكافحة الجريمة السيبرانية ومنها العراق انما فقط بقي مسودة قانون فضلا عن صعوبة مواكبة تطور الجريمة السيبرانية لذلك نرى ان احد ابرز اسباب القصور التشريعي هو طبيعة الجريمة السيبرانية المتطورة غير المسيطر عليها فضلا عن التماهي في اصدار قوانين تشريعية قادرة على مكافحتها في العديد من الدول العربية وهو امر لابد من معالجته كونها جرائم دولية تزعزع نظام وامن المجتمع الدولي وعليه سنتطرق الى مجموعة من الاستراتيجيات التي يمكن ان تكون فاعلة للحد من الجريمة السيبرانية.

الفرع الثالث: آليات مكافحة الجريمة السيبرانية

لمكافحة تهديدات الامن السيبراني يجب على البلدان تطوير استراتيجيات قوية للأمن السيبراني الوطني والاستثمار في البنية التحتية والادوات والموظفين بغية اكتشاف الهجمات السيبرانية والوقاية منها والاستجابة لها ويشتمل ذلك على انشاء فرق لحالات الطوارئ في الكمبيوتر وتعزيز الشراكات بين القطاعين العام والخاص في الامن السيبراني وتعزيز التعاون الدولي لتبادل افضل الممارسات وتنسيق الاستجابات على التهديدات السيبرانية فضلا عن الحاجة الملحة لبناء القدرات في خصوصية البيانات وحمايتها وذلك من خلال رفع الوعي العام بحقوق خصوصية البيانات يجب على الحكومات ومنظمات المجتمع المدني والقطاع الخاص التعاون لتطوير ونشر المواد التعليمية والاستثمار في المبادرات التي تبني مهارات ومعرفة اصحاب المصلحة فضلا عن اهمية الحملات التي تبلغ المواطنين بحقوقهم بموجب قوانين حماية البيانات والمخاطر المرتبطة بمشاركة المعلومات الشخصية وذلك من خلال استضافة ورش عمل كما وتشتمل بناء القدرات على تدريب المهنيين القانونيين وموظفي انفاذ القانون وأخصائي تكنولوجيا المعلومات وغيرهم من اصحاب المصلحة والمعنيين لمواجهة هذه الجرائم [41] تعزيز الاطر القانونية والتنظيمية من خلال مراجعة وتحديث قوانين خصوصية البيانات واغلاق الفجوات التشريعية واعتماد لوائح جديدة تماشياً مع التطورات في الاساليب الاجرامية فضلا عن اهمية التنسيق والتعاون عبر الحدود لتسهيل التدفق الحر للبيانات وضمان معايير حماية الخصوصية، اضافة الى ذلك تعد المشاركة والانخراط في الحوار والتعاون لمحاذاة اطر حماية البينات الخاصة بها وانشاء آليات لنقل البيانات عبر الحدود امر بالغ الاهمية في سبيل انجاح عملية حماية البيانات وسلامتها [42] كما ويمكننا

التطرق الى عدة وسائل يمكن استخدامها لغرض لمكافحة الجريمة السيبرانية من خلال الاستفادة من برامج وتقنيات الكترونية متنوعة وكما يأتي:

1- اعتراض المراسلات السيبرانية

ان عملية اعتراض المراسلات السيبرانية تنصب عادة على رسائل البريد الالكتروني حيث يعتبر البريد الالكتروني من الوسائل الحديثة للاتصال في مجال الانترنت اذ يحتوي على العديد من المعلومات كتاريخ انشاء الرسالة وتاريخ ارسالها وتلقيها وكذلك عنوان المرسل وعنوان المرسل اليه ولكن تبقى المعلومات التي تحتويها حاشية رسالة البريد الالكتروني هي الاهم، بحيث تتضمن على عنوان التعريف لمرسلها والذي يتكون من اربعة اجزاء يشير الجزء الاول منه الى المنطقة الجغرافية والجزء الثاني لعنوان مزود الخدمة لمجموعة الحاسبات الآلية المترابطة والجزء الاخير يحدد الحاسب الآلي الذي تم الاتصال بواسطته [43]

2- الحماية من التسريب الالكتروني

يجب على مستخدمي الحسابات والمواقع السيبرانية والمؤسسات اتخاذ اجراءات امان رقمي فعالة، مثل تحديث البرامج والانظمة بشكل مستمر ومنتظم واستخدام كلمات مرور قوية وتفعيل التحقق الثنائي للدخول الى الحسابات الرقمية وتوعية المستخدمين حول مخاطر الهجمات السيبرانية فالتسرب الالكتروني يشير الى الكشف غير المصرح به عن معلومات او بيانات الكترونية من خلال هجوم الكتروني او خرق امان او اهمال في التعامل مع المعلومات الرقمية ويشمل التسرب الالكتروني سرقة البيانات والتجسس والتسريب العرضي للمعلومات وفقدان السيطرة على البيانات والهجمات السيبرانية الاخرى وقد تكون المعلومات المسربة شخصية وحساسة وقد تكون بيانات حكومية فيكون تأثيره كبير على الافراد والشركات بما في ذلك فقدان الخصوصية وسرقة الهوية والتأثير الاقتصادي الضار وعليه فأن عملية حماية الافراد لأنفسهم باتخاذ اجراءات وقاية او حماية يعد من الضرورات لتجنب التسرب الالكتروني.

3- المراقبة السيبرانية

تعتبر المراقبة السيبرانية من اهم مصادر التحري التي غالبا ما يستعان بها في البحث والتقصي عن الجرائم، سواء كانت تلك التقليدية او المستحدثة كجرائم الانترنت فالمقصور بها هي عملية استخدام التقنيات الرقمية لرصد ومراقبة الانشطة السيبرانية سواء على مستوى الافراد او الكيانات الحكومية او الشركات ويشمل ذلك تحليل وتتبع البيانات الرقمية مثل استخدام الانترنت والاتصالات السيبرانية وسجلات النشاط على الاجهزة الرقمية ويمكن تنفيذ الرقابة السيبرانية لأغراض متنوعة منها الامان الوطني ومراقبة انشطة موظفي الدوائر الحكومية وبيئة العمل[44]

4- المساعدة القضائية

هي كل اجراء قضائي تقوم به دول ما من شأنه تسهيل مهمة المحاكمة من دولة الى اخرى بصدد جريمة من الجرائم قد تكون هذه المساعدة رسمية او غير رسمية، اذ انها تعد احد صور التعاون الدولي في المسائل الجنائية وهي من الآليات الفعالة لمواجهة الجرائم السيبرانية لا سيما فيما يتعلق بالتوفيق بين حق الدولة في ممارسة اختصاصها الجنائي داخل حدودها الاقليمية وحقها في توقيع العقاب [45]

الخاتمة

يحظى موضوع الجريمة السيبرانية بأهمية كبيرة في المجتمع الدولي اذ ان طبيعتها الدولية فرضت على المجتمع الدولي تبني سياسات فاعلة لمواجهتها لا سيما وان اهميتها تنبع من طبيعتها القانونية الخاصة فهي من الظواهر البارزة في العالم الحديث فلا يقتصر تأثيرها على الافراد بل يطال المؤسسات والشركات والانظمة الحكومية والامن القومي للدول وعليه فأن القصور التشريعي تجاه هذه الجرائم قد احدث خللاً في عملية مواجهة الجريمة السيبرانية واثر بشكل واضح على تحقيق العدالة الجنائية في مكافحته بالتالي فأن ضعف التشريعات القانونية والاجراءات ادى الى ضعف قدرة السلطات في التصدي لها، فهذه الجرائم تفرض ضغوطاً كبيرة على الانظمة الامنية والقانونية مما يستلزم التطور المستمر في السياسات والتشريعات لمكافحتها ومما زاد من حدتها وتأثيرها انها جرائم يصعب اكتشافها واثباتها امام القضاء وعليه شرعت العديد من الدول لتقنين هذه الظاهرة لغرض ردعها والحد منها وذلك على الصعيدين الدولي والمحلي ومن ثم محاولة التصدي لها بوسائل واستراتيجيات مستحدثة.

الاستنتاجات

1- ان التطور المتسارع لتكنولوجيا المعلومات يفوق ويتعدى في احيان كثيرة قدرة التشريعات الجزائية على مواكبته مما يؤدى الى وجود فجوات قانونية تُستغل من قبل مرتكبي تلك الجرائم

2-تعاني التشريعات التقليدية من صعوبة تطبيقها على الجرائم المعلوماتية بسبب الطبيعة المختلفة للجريمة المعلوماتية عن الجريمة التقليدية

3-يساهم غياب التخصص التقني لدى الجهات التحقيقية والقضائية في تعميق اثر القصور التشريعي مما يؤدى الى افلات الجناة من المسائلة القانونية

4-ان عدم توحيد المفاهيم القانونية بين التشريعات الوطنية والدولية يحد من فاعلية التعاون القضائي بين الدول في مكافحة الجرائم المعلوماتية العابرة للحدود

5- يثبت البحث ان تحديث التشريعات المعلوماتية بصورة دورية اصبح ضرورة قانونية لمواكبة تطور الجريمة الالكترونية ولضمان تحقيق الحماية الجنائية الفعالة للمجتمع الرقمي اذ ان القصور التشريعي لا يكمن فقط في غياب النصوص بل يمتد الى ضعف الصياغة القانونية وعدم مرونتها في استيعاب المستجدات التقنية

المقترحات

1- انشاء مراكز دراسات وبحوث تضم متخصصين في مكافحة الجرائم السيبرانية وذلك لغرض مواكبة التطور الحاصل في الجريمة السيبرانية ووسائل تنفيذها ومن ثم محاولة اقامة الندوات والبحوث العلمية وبما يعزز تجارب الدول في الحالات المماثلة لغرض اسقاط تجاربها على الجرائم التي يمكن ان تقع داخل بلد معين.
2- دعم البنى التحتية الرقمية للجهات المعنية بمكافحة الجرائم السيبرانية بغية تحقيق العدالة الجنائية.
3- تدريب القضاة والمحققين على الجوانب الفنية وذلك من خلال اقامة الدروات والورش التدريبية.
4- تعزيز التعاون الدولي بغية تبادل الخبرات والتقنيات المتطورة فيما بينها.
5- العمل على صياغة قوانين مرنة قادرة على ان تضم بين طياتها مختلف الجرائم السيبرانية.

الهوامش

1. JURISPRUDENCE CONSTITUTIONNELLE/ Questionnaire/pour le XIVe Congrès de la Conférence des Cours constitutionnelles européennes/p1،
2. محمد نجم محسن، دور القاضي الدستوري في اصلاح القصور التشريعي، المجلة القانونية، جامعة القاهرة، مصر، مجلد 9، العدد3، 2021، ص918
3. محمود نجيب حسني، شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 1989 ، ص 1 وما بعدها.
4. عماد مفلح الحسبان وآخرون،الجرائم المستحدثة(المعلوماتية،الألكترونية، السيبرانية) دار الخليج للنشر والتوزيع،الاردن2024ص130
5. خالد ظاهر عبدالله جابر السهيل المطيري، مواجهة الجرائم السيبرانية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، مصر، المجلد 31، العدد2، 2019،ص17
6. خالد ظاهر عبدالله جابر السهيل المطيري، مصدر سبق ذكره، ص25
7. عبدالعال الديربي ومحمد صادق اسماعيل، الجرائم السيبرانية (دراسة قانونية قضائية مقارنة)، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص54-55
8. عماد مفلح الحسبان وآخرون، مصدر سبق ذكره، ص139
9. عبد المؤمن الصغير، الطبيعة الخاصة للجريمة السيبرانية المرتكبة عبر الأنترنيت في التشريع الجزائري والتشريع المقارن، مجلة الحقوق و الحريات، جامعة محمد خيضر، بسكرة، المجلد2 ،2014، ص72
10. عادل يوسف عبدالنبي الشكري، الجريمة السيبرانية وازمة الشرعية الجزائية، مركز دراسات الكوفة، جامعة الكوفة، كلية القانون، 2008، ص116
11. خالد ظاهر عبدالله جابر السهيل المطيري، مصدر سبق ذكره، ص26
12. عماد مفلح الحسبان وآخرون، مصدر سبق ذكره، ص 146-147
13. علي حمزة عباس وانمار علي ابراهيم، القصور التشريعي لجرائم تقنية المعلومات، عدد خاص بالمؤتمر العلمي الدولي الثالث لجامعة جيهان- اربيل في القانون والعلاقات الدولية والاعلام، 2017العدد 3، ص170
14. صغير يوسف، الجريمة المرتكبة عبر الانترنت(رسالة ماجستير)جامعة مولود معمري، كلية الحقوق والعلوم السياسية2013ص52
15. عبد العال الديربي، مفاهيم استتراجية لجريمة المعلوماتية، بحث منشور في الموقع الالكتروني العربي لابحاث الفضاء الالكترونية www.accronline.com ، ص75.
16. نهلاء عبد القادر الموسني، الجرائم المعلوماتية، بحث منشور في الموقع الالكتروني www.kenanonline.comK، ص26.
17. مفتاح بوبكر المطردي، الجريمة السيبرانية والتغلب على تحدياتها، ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23-2012/9/25، ص20
18. مداوي سعيد مداوي القحطاني، الجريمة السيبرانية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج العربية، الامانة العامة، قطر، 2016، ص36
19. مداوي سعيد مداوي القحطاني، مصدر سابق، ص36-37
20. رعد فجر الراوي، القصور التشريعي في مواجهة الهجمات السيبرانية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 10، العدد 39، 2021، ص205
21. Alison Peters and Amy Jordan ,ARTICLES, Countering the Cyber Enforcement GaP: Strengthening Glopal Capacity on Cybercrime, JOURNAL OF NATIONAL SECURITY LAW & POLICY,
22. Alison Peters and Amy Jordan ,ARTICLES, Countering the Cyber Enforcement GaP: Strengthening GLOPAL Capacity on Cybercrime, JOURNAL OF NATIONAL SECURITY LAW & POLICY,

23. منذر الشاوي، الانسان والعدالة، بغداد، 2016، ص317
24. علي حمزة عباس وانمار علي ابراهيم، القصور التشريعي لجرائم تقنية المعلومات، مجلة جامعة جيهان- اربيل العلمية، عدد خاص بالمؤتمر العلمي الدولي الثالث لجامعة جيهان العدد 3، 2018، ص176
25. خالد ظاهر عبدالله جابر السهيل المطيري، مصدر سبق ذكره، ص38
26. علي حمزة عباس وانمار علي ابراهيم، مصدر سبق ذكره، 176
27. بنظر المادة 22 من اتفاقية بودابست
28. اتفاقية بودابست لمكافحة الجرائم السيبرانية/ المواد (16-20) 2023/11/23
29. اتفاقية بودابست لمكافحة الجرائم السيبرانية/ المواد (16-20) 2023/11/23
30. Mohamed Aly Bouke & others, African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions, 2013, p1
31. اتفاقية الاتحاد الافريقي بشأن امن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي، 27 يونيو 2014
32. اتفاقية الاتحاد الافريقي بشأن امن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي، 27 يونيو 2014
33. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، 2010
34. علي حمزة عباس وانمار علي ابراهيم، مصدر سبق ذكره، ص175
35. علي عواد الكردي. الحماية الجزائية في جريمة انتهاك المراسلات الالكترونية. بحث منشور على الموقع الالكتروني www.dorar-aliraq.net .
36. علي عواد الكردي. الحماية الجزائية في جريمة انتهاك المراسلات الالكترونية. بحث منشور على الموقع الالكتروني www.dorar-aliraq.net .
37. قرار قانون رقم 10 لسنة 2018 في 13 شعبان والمتعلق بالجرائم السيبرانية، المقتفي فلسطين، اعداد معهد الحقوق في جامعة بيرزيت
38. ينظر المادة (23) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم السيبرانية.
39. ينظر المادة 7/2 من قانون جرائم السيبرانية لسنة 2007 السعودي
40. ينظر قانون رقم 175 لسنة 2018 المصري
41. Mohamed Aly Bouke & others, African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions, 2013, p5
42. Mohamed Aly Bouke & others, African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions, 2013, p10-13
43. زيدان زيبحة، الجريمة السيبرانية في التشريع الجزائري والدولي، درا الهدى للطباعة والنشر، الامارات (الشارقة)، 2011، ص159
44. نبلة هبة هروال، الجوانب الاجرائية لجرائم الانترنت، دار الفكر الجامعي، الاسكندرية، 2019، ص 197
45. احمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، دار النهضة العربية، 1994، ص91

المصادر

الكتب العربية

1. احمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، دار النهضة العربية، 1994
2. زيدان زيبحة، الجريمة السيبرانية في التشريع الجزائري والدولي، درا الهدى للطباعة والنشر، الامارات (الشارقة)، 2011
3. عادل يوسف عبدالنبي الشكري، الجريمة السيبرانية وازمة الشرعية الجزائية، مركز دراسات الكوفة، جامعة الكوفة، كلية القانون، 2008
4. عبدالفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي (دراسة متعمقة في التعريف بجرائم التقنية الحديثة والمجرم المعلوماتي: انحراف الاحداث بسبب الانترنت- مكافحة ادمان الانترنت لدى بعض الفئات، دار النهضة العربية، 2009
5. عماد مفلح الحسبان وآخرون، الجرائم المستحدثة (المعلوماتية، الألكترونية، السيبرانية) دار الخليج للنشر والتوزيع، الاردن، 2024
6. محمود نجيب حسني، شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 1989
7. مداوي سعيد مداوي القحطاني، الجريمة السيبرانية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج العربية، الامانة العامة، قطر، 2016
8. منذر الشاوي، الانسان والعدالة، بغداد، 2016
9. نبلة هبة هروال، الجوانب الاجرائية لجرائم الانترنت، دار الفكر الجامعي، الاسكندرية، 2019

الرسائل

1. صغير يوسف، الجريمة المرتكبة عبر الانترنت (رسالة ماجستير)، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، 2013.

المجلات

1. خالد ظاهر عبدالله جابر السهيل المطيري، مواجهة الجرائم السيبرانية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، مصر، المجلد 31، العدد2، 2019
2. رعد فجر الراوي، القصور التشريعي في مواجهة الهجمات السيبرانية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 10، العدد 39، 2021
3. عبد المؤمن الصغير، الطبيعة الخاصة للجريمة السيبرانية المرتكبة عبر الأنترنيت في التشريع الجزائري والتشريع المقارن، مجلة الحقوق و الحريات، جامعة محمد خيضر، بسكرة، المجلد2 ،2014
4. علي حمزة عباس وانمار علي ابراهيم، القصور التشريعي لجرائم تقنية المعلومات، عدد خاص بالمؤتمر العلمي الدولي الثالث لجامعة جيهان- اربيل في القانون والعلاقات الدولية والاعلام، 2017العدد 3
5. علي حمزة عباس وانمار علي ابراهيم، القصور التشريعي لجرائم تقنية المعلومات، مجلة جامعة جيهان- اربيل العلمية، عدد خاص بالمؤتمر العلمي الدولي الثالث لجامعة جيهان العدد 3، 2018،
6. محمد نجم محسن، دور القاضي الدستوري في اصلاح القصور التشريعي، المجلة القانونية، جامعة القاهرة، مصر، مجلد 9، العدد3، 2021
7. مفتاح بوبكر المطردي، الجريمة السيبرانية والتغلب على تحدياتها، ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23-2012/9/25

القوانين والتشريعات

1. اتفاقية الاتحاد الافريقي بشأن امن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي، 27 يونيو 2014
2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، 2010
3. اتفاقية بودابست لمكافحة الجرائم السيبرانية/ المواد (16-20) 2023/11/23
4. اتفاقية بودابست لمكافحة الجرائم السيبرانية/ المواد (16-20) 2023/11/23
5. قرار قانون رقم 10 لسنة 2018 في 13 شعبان والمتعلق بالجرائم السيبرانية، المقتفي فلسطين، اعداد معهد الحقوق في جامعة بيرزيت
6. ينظر المادة (23) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم السيبرانية.
7. ينظر المادة 7/2 من قانون جرائم السيبرانية لسنة 2007 السعودي
8. ينظر قانون رقم 175 لسنة 2018 المصري

الأنترنت والمواقع الالكترونية

1. عبد العال الديربي، مفاهيم استراجية لجريمة المعلوماتية، بحث منشور في الموقع الالكتروني العربي لابحاث الفضاء الالكترونية www.accronline.com
2. علي عواد الكردي. الحماية الجزائية في جريمة انتهاك المراسلات الالكترونية. بحث منشور على الموقع الالكتروني www.dorar-aliraq.net
3. نهلاء عبد القادر الموسني، الجرائم المعلوماتية، بحث منشور في الموقع الالكتروني www.kenanonline.com

المصادر الاجنبية

1. Alison Peters and Amy Jordan ,ARTICLES, Countering the Cyber Enforcement GaP: Strengthening Glopal Capacity on Cybercrime, JOURNAL OF NATIONAL SECURITY LAW & POLICY.
2. Alison Peters and Amy Jordan ,ARTICLES, Countering the Cyber Enforcement GaP: Strengthening GLOPAL Capacity on Cybercrime, JOURNAL OF NATIONAL SECURITY LAW & POLICY.
3. Congrès de la Conférence des Cours constitutionnelles ،CONSTITUTIONNELLE/ Questionnaire/pour le XIVe européennes/.
4. Mohamed Aly Bouke & others, African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions, 2013.
5. Mohamed Aly Bouke & others, African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions, 2013.
6. Mohamed Aly Bouke & others, African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions, 2013.