التدابير الأمنية المضادة للجرائم السيبرانية

المدرس الدكتور مهدي كريم علي الشمري
وزارة الداخلية، كلية الشرطة والمعهد العالي للتطوير الأمني والإداري - بغداد \ العراق

Security Measures Against Cybercrime

Instructor Dr. Mahdi KarEEm Ali Al-Shammari
Ministry of Interior, Police College and Higher Institute for Security and Administrative Development،Baghdad - Iraq
mahdi002919@gmail.com

المستخلص

الجرائم السيبرانية هي كل سلوك غير مشروع يتم باستخدام الأجهزة الإلكترونية، ينتج عنها حصول المجرم على اغراض مادية أو معنوية مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات، وهي شكل متطور من أشكال الجريمة عبر الوطنية. وتزايد ضلوع جماعات الجريمة المنظمة يزيد من تفاقم الطابع المعقد لهذه جريمة، التي تحدث في مجال الفضاء الإلكتروني الذي لا حدود له، ويمكن لمرتكبي الجرائم السيبرانية وضحاياهم أن يتواجدوا في مناطق مختلفة، ويمكن أن تتمد آثار الجريمة عبر المجتمعات في جميع أنحاء العالم، مما يبرز الحاجة الي وضع استجابة عاجلة وديناميكية ودولية، وتشهد التقنية والتكنولوجيا تطورات كثيرة واستحداث لأمور جديدة، هذا الأمر ينذر بتطور أدوات وسبل الجريمة الإلكترونية، بشكل أكثر تعقيدا أو أشد ضررا من قبل الأمر الذي يلزم الدول لتطوير آليات مكافحة هذه الجرائم واستحداث خطوط دفاع وسن قوانين وتوعية الناس بمستحدثات هذه الجرائم وتشجيعهم للإبلاغ عنها وإن الجرائم السيبرانية تتم باستخدام شبكات المعلومات أو الأجهزة الحديثة وتطبيقاته، وعلى الرغم من أن بعض الجرائم الالكترونية يمكن المعاقبة عليها عن طريق تطويع بعض النصوص الموجودة في قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، إلا إنَّ القسم الأكبر من تلك الأفعال يمكن أن يبقى من دون عقاب لعدم وجود النصوص القانونية لتجريمه، مما يستدعي ضرورة تدخل المشترع العراقي لسن القوانين اللازمة ومنع وقوع الأفعال الجرمية ذات الصلة بالكومبيوتر والأنظمة المعلوماتية، خصوصاً وأن استعمال الكومبيوتر والاعتماد عليه في ازدياد مستمر ضمن النشاطات القانونية

ولغرض الوقاية من الجريمة السيبرانية، لابد كان من وضع تدبير ملائم يتناسب مع مقدار جسامة تلك الخطورة، وهذا ما دفع الى تقسيم التدابير على صنفين إذ أختص الصنف الأول في التدابير المانعة التي تهدف إلى منع الجريمة من الوقوع، ولو للمرة الاولى عن طريق الكشف عن خطورة الأشخاص الذين يظهرون في إحدى الحالات الاجتماعية السلبية التي افترض المشرع ضررها على المجتمع أو على الفرد ذاته، أما الصنف الثاني فهي التدابير العلاجية، التي تهدف إلى منع تكرار وقوع الجريمة للمرة التالية، بالقضاء على الخطورة الاجرامية التي تستخلصها المحكمة من مجموعة الادلة الشخصية والمادية السابقة أو المعاصرة أو اللاحقة لارتكاب الجريمة السابقة.

الكلمات المفتاحية: التدابير الأمنية-الامن السيبراني-الجرائم السيبرانية – حماية البيانات- الهجمات الالكترونية.

Abstract

Cybercrime is any illegal behavior carried out using electronic devices, resulting in the criminal gaining material or moral advantage while incurring a corresponding loss for the victim. The goal of these crimes is often hacking to steal or destroy information, and it is a sophisticated form of transnational crime. The growing involvement of organized crime groups exacerbates the complexity of this crime, which occurs in the boundless realm of cyberspace. Cybercriminals and their victims can be located in diverse regions, and the effects of the crime can extend across societies worldwide, highlighting the need for an urgent, dynamic, and international response. Technology is witnessing significant developments and the introduction of new technologies. This portends the development of cybercrime tools and methods, becoming more complex or more damaging than before. This requires countries to develop mechanisms to combat these crimes, establish lines of defense, enact laws, educate the public about these crimes, and encourage them to report them. Cybercrimes are committed using information networks or modern devices and their applications. Although some electronic crimes can be punished by adapting some of the provisions contained in the Iraqi Penal Code No. (111) of 1969, as amended, the greater part of these acts can remain necessitates the intervention of the Iraqi legislator to enact the necessary laws and prevent the occurrence of criminal acts related to computers and information systems, especially since the use of computers and reliance on them is constantly increasing within legal activities. In order to prevent cybercrime, it is necessary to put in place appropriate measures commensurate with the seriousness of the danger. category is concerned with preventive measures, the commission of the previous crime.

Keywords: Security measures, Cybersecurity, Cybercrime, Data protection, Cyberattacks

المقدمة

إنَّ أدارك الامن هو غاية القانون، وهي حقيقة توصلت اليها المجتمعات الأولى، فهو الركيزة الأولى التي تدعم الوجود المجتمعي، اذ لا مجال للاستقرار والطمأنينة دون ضمان هذه الغائية، فهل يكفل العقاب لوحده تحقيق الأمن الاجتماعي وضمان الاستقرار والطمأنينة؟ فأذا كان الجواب بالإيجاب فلماذا ما أزلت معدلات الجريمة بازدياد، واذ كانت الإجابة بالسلب فما هي الوسيلة التي يمكن أن تقف الى جانب العقاب لإكمال الجزاء الجنائي. في تحقيق اغراضه، لذا كان لابد من البحث عن تكامل الجزاء الجنائي لتعزيز الدفاع الاجتماعي ضد الجريمة، والذي يبدأ من مرحلة المنع والوقاية، مرورا بالتجريم والعقاب، وينتهي بمرحلة التنفيذ العقابي المعزز بالتأهيل النفسي والاجتماعي، وهذه المراحل في حقيقة الأمر ماهي الا انعكاس للتراث الإنساني، الذي جسدته جهود الفقهاء والفلاسفة في ميدان استتباب الامن الاجتماعي، والذي أفرز لنا تجارب غنية في محاربة الظواهر الاجرامية، والتي كان من أبرزها ما طرح من نظريات دارت حول تطوير الجزاء الجنائي تبني رؤية جديدة قائمة على ازدواجية الجزاء – العقاب التدبير – إذ يمثلان كليهما أقصى درجات الضبط الاجتماعي، وينبع اساسهما من حق للمجتمع في الدفاع عن نفسه إزاء أي تهديد محتمل يمكن أن يمس الاستقرار والطمأنينة بوسائل تلائم درجة تلك الخطورة عليه عد العقاب الصورة الأولى، واحتل مركز الصدارة في ميدان الجزاء الجنائي، الا أن دوره ظل قاصرا على مرحلة ما بعد ارتكابه الجريمة، وقصر مفهوم الكفاح ضد الاجارم في أضيق نطاق عليه كان لابد من إيجاد صورة جزائية ثانية تتولى مهمة منع الجريمة من الوقوع للمرة الأولى او الوقاية من ارتكابها مرة اخرى، وهذا بالفعل ما دفع الفلاسفة وأصحاب الفكر الى محاولة سد تلك الثغرة في الميدان الجزائي عن طريق التدبير الأمني.

اولا – أهمية الدراسة

بعد موضوع التدابير الأمنية المضادة للجرائم السيبرانية كفيل بحماية الحدود العراقية من الأخطار التي تتعرض لها عن طريق الجرائم السيبرانية.

ان التحقيق في علم الجريمة الجرائم السيبرانية وكيفية ضبط الأدلة الإلكترونية من الموضوعات المبتكره في بلدان العالم كما أن طبيعة الأدلة الإلكترونية وكيفية التعامل معها من قبل جهات التحقيق تعتبر من الموضوعات المهمة القانونية والعملية، فيبحث التحقيق الجنائي

في مختلف الجرائم ومنها الجرائم السيبرانية المرتكبة من أفراد المجتمع وفقاً لإجراءات معينة سعياً وراء الكشف عن الجريمة ومعرفة الحقيقة، فالتحقيق الجنائي بهذا النوع من الجرائم فن بحاجة إلى موهبة ووجود الفن والموهبة بحاجة للإتقان، ولن يتأتى ذلك إلا بممارسة العمل من خلال عنصر بشري يسمى «المحقق» فهو مدار التحقيق الجنائي ومحوره، من يتولى البحث عن الحقيقة لكشف مرتكبي الجرائم ومباشرة إجراءات التحقيق وجمع أدلة الإدانة أو البراءة ضد مرتكبيها تمهيداً لإحالتهم إلى المحكمة.

ثانيا - إشكالية الدراسة

ازدحم العالم بشبكات اتصالية دقيقة ومتطورة تنقل وتشغل المعلومات والبيانات من مناطق متباعدة باستخدام تقنيات لا تكفل لها أمنا كاملا، ويتاح في ظلها التلاعب عبر الحدود بتلك المعطيات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أو الأفراد أو الشركات أضرارا فادحة، يغدو عندها التعاون الدولي واسع المدى في مكافحة الجرائم المعلوماتية ومن بينها جرائم الإنترنت أمرا محتوما، بنظرة متأنية للأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية ومنها الجرائم المتعلقة بشبكة الإنترنت، يتضح عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحا في أحد الأنظمة قد يكون مجرما وغير مباح في نظام آخر، ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر، ومن ثم اختلاف السياسة التشريعية المنتهجة، يطرح انتشار الإنترنت خارج حدود الدولة تحديات قانونية تتعلق بسيادة الدول وصلاحية محاكمها التي تمتد فقط على مساحتها الجغرافية. ولكن بما أن جرائم الإنترنت ظاهرة عالمية جديدة تمتد خارج نطاق الحدود الوطنية فإن ذلك يستلزم لنجاح مكافحة تلك الجرائم تنسيقًا كبيرًا بين القوانين الداخلية والمعاهدات الدولية والتعاون بين مختلف البلدان، وعليه تتمحور اشكالية الدراسة في هل هناك تدابير كافية لمواجهة الجرائم السيبرانية؟

ثالثا - أهداف الدراسة

اعتمدت الدراسة على التدابير اللازمة لمواجهة ومكافحة الجرائم المستحدثة والجديدة من نوعها، والتي تتم عبر شبكة الإنترنت ووسائل التكنولوجيا الحديثة بشكل عام، خلال السنوات الماضية؛ إذ شكلت الجرائم الإلكترونية خطرًا كبيرًا، لما تتمتع به من خصائص من بينها الاعتماد

على استخدام الحاسب الألي والتقنيات التكنولوجية الحديثة، وعدم وجود مواجهة مباشرة بين الجاني والمجني عليه، وتعدد مسارح الجريمة الإلكترونية، ذلك أن المواجهة الأمنية والمعني بها وزارة الداخلية، إذ تم إنشاء إدارة مباحث الانترنت المتخصصة في مواجهة كافة الجرائم والأنشطة غير المشروعة والتي تتم عبر شبكة الانترنت ومنصات التواصل الاجتماعي، كما تتعاون الإدارة مع كافة أجهزة ومؤسسات الدولة في تحديث معلوماتها لمساعدة الضباط العاملين بالإدارة، وإمدادهم بكافة الأجهزة التكنولوجية الحديثة لمواجهة هذه الجرائم.

رابعا – أسئلة الدراسة

1 – ما هو مفهوم الجرائم السيبرانية وما هي اهم صورها؟
2 – ماهي اهم طرق الوقاية من الجرائم السيبرانية؟
3 – ما هو مفهوم التدابير الأمنية وما هي صورها واهم التشريعات التي واجة تلك الجرائم؟

منهجية البحث – خامسا

تم استخدام في هذه الدراسة المنهج الوصفية التحليلي، التي يقوم على أساس تعين خصاص المشكلة واهم التشريعات التي عالجتها وتحليلها للوقوف على السلبيات ومحاولة رفعها والتوصية باتخاذ او تعديل مواد قانونية تزيد من الحماية من تلك الجرائم.

سادسا – هيكلية الدراسة

ستتناول هذه الدراسة الموضوع في مبحثين، يخصص المبحث الأول لمفهوم الجرائم السيبرانية واهم صورها بينما يخصص المبحث الثاني لاهم التدابير الأمنية المضادة المتخذة في التشريعات الوطنية لمكافحة تلك الجرائم.

المبحث الأول
ماهية الجرائم السيبرانية وصورها وآثارها

تعد الجريمة السيبرانية نتاج الاستخدام الخاطئ لثورة التكنولوجيا التي لحقت بالعالم في القرن العشرين، وهي اثر من الآثار غير المرغوبة لهذا التقدم العلمي المذهل الذي جعل المجرم يختبئ خلف شاشة ما ويمارس عملا اجراميا بالاعتداء على مصلحة يحميها النظام للضحية، وتتم الجريمة عن طريق قيام الجاني بالضغط على المجني عليه المحتمل بالتهديد تارة والوعيد تارة اخرى وذلك بنشر معلومات او صور او تسجيلات لا يرغب المجني عليه في اظهارها على الملأ، ولغرض الإحاطة علماً بماهية الجريمة السيبرانية سوف نقسمه الى مطلبين نبحث في الأول منه مفهوم تلك الجرائم ونخصص المطلب الثاني لصور تلك الجرائم.

المطلب الاول: مفهوم الجرائم السيبرانية

للجريمة السيبرانية مدلولات عدة، وأن كانت تلتقي من إذ الوسيلة إذ تتم باستخدام التكنولوجيا والواقع الافتراضي كمسرح جريمة، وكذلك مرتكبها ذو مهارات وصفات تميزه عن المجرم التقليدي، ومن الاهمية بمكان الوقوف على اسباب ودوافع هذه الجريمة الخطيرة التي تلقي بإثارها السلبية على المجتمع.

عليه سنقسم دراسة هذا المطلب على فرعين، نتناول في التعريف اللغوي والفقهي للجرائم السيبرانية، ونخصص الفرع الثاني التعريف القانوني للجرائم السيبرانية، وعلى النحو الآتي:

الفرع الاول: التعريف اللغوي والفقهي للجرائم السيبرانية

وهي تتكون من Cyber Crimes- اولا - مدلول الجريمة السيبرانية في اللغة: هي احدى الجرائم الالكترونية وهي الجريمة السيبرانية ويستخدم مصطلح (Cyber) والمقطع الاخر (Crimes) من مقطعين هما الجريمة السيبرانية لوصف فكرة ان الجريمة تتم من خلال التقنية الحديثة[1].

1 -الصحاح تاج اللغة وصحاح العربية، لإسماعيل بن حماد الجوهري، دار العلم للملايين ط، بدون سنة نشر، ص 1723-1

ثانيا– الجريمة السيبرانية في الفقه: الجريمة فهي تلك الافعال المخالفة للقانون[1]، وقد اصطلح على تعريف الجرائم السيبرانية بانها الافعال التي ترتكب ضد الافراد او المجموعات من الافراد بدافع ايذاء سمعة الضحية او اذى مادي او غير مادي او عقلي مباشر او غير مباشر باستخدام الاتصال مثل الانترنت غرف الدردشة، البريد الالكتروني، الهاتف النقال، والحاسب الآلي[2]، وفي معظم الاحيان يكون الحصول عليها غير مشروع لانتفاء صفة الرضا والقبول كأن يكون الضحية اقل من سن الرشد او عن طريق الدخول غير المشروع للحسابات الالكترونية التهكير، أو عن طريق استغلال الجاني لصفته الوظيفية كأن يكون موظفا عاما يمكن له الاطلاع على الرسائل او البرقيات او الاتصالات الهاتفية او شبكة الانترنت او عاملا في الاستعلامات تودع لديه هواتف المراجعين او يستغل صفته المهنية أو الفنية كأن يكون مصلحا او متاجرا بالهواتف الذكية او مجهزا للأنترنت فضلا عن حالات سرقة الهواتف او نسيانها في الأماكن العامة[3].

اذ ان الجريمة السيبرانية هي استخدام وسائل الاتصال وتكنولوجيا المعلومات في تهديد وترهيب ووعيد بحمل شخص على القيام بدفع اموال او طلب امور اخرى من المجني عليه والذي يخشى نشر اسرار الحياة الخاصة به وذلك خلافا لإحكام القانون والنظام العام والآداب العامة[4].

الفرع الثاني: تعريف الجرائم السيبرانية قانوناً

لم يواكب قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل هذه الجرائم مع انه نص في المادة 182 علي معاقبة من ينشر أو يذيع اخبار بأية صورة وعلي أي وجه وبأية وسيلة معلومات أو صور أو وثائق أو مكاتبات أو غير ذلك، خاصة بدوائر الدولة والمصالح الحكومية وكانت محظور نشرها أو اذاعتها، كما ورد في بعض مواده تعريف الاصطناع في المادة 291 عقوبات انشاء محرر لم يكن له وجود من قبل ونسبته إلى غير محرره دون ما ضرورة لتعمد تقليد محرر بالذات وخط انسان معين، وعاقب في المادة 361 من عطل عمدا وسيلة من وسائل الاتصال السلكية أو اللاسلكية المخصصة للمنفعة العامة، وفي المادة 403 عاقب صانع أو مستورد أو

1- الصحاح تاج اللغة وصحاح العربية، لاسماعيل بن حماد الجوهري، دار العلم للملايين ط، بدون سنة نشر، ص 1723-

2- د. داليا عبد العزيز: المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في النظام السعودي، دراسة مقارنة السعودية، 2017، ص 27

3- ماجد عمار: المسؤولية القانونية الناشئة عن استخدام فيروس برنامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، 1989، ص 156

4- د.داليا عبد العزيز: مرجع سابق، ص 27.-

حائز المطبوعات والكتب والرسوم المخلة بالحياء والآداب العامة، وفي المادة 404 عاقب كل من جهر باغان أو اقوال فاحشة أو مخلة بالحياء بنفسه أو بواسطة جهاز آلي وفي محل عام، وفي المادة 432 عاقب كل من هدد بالقول أو الفعل أو الإشارة كتابة أو شفاها، واعتبر في المادة 434 أفعال رمي الغير بما يخدش الشرف أو الاعتبار أو جرح المشاعر وان لم يتضمن اسناد واقعة معينة من الظروف المشددة اذا وقع بطريق النشر بالصحف أو المطبوعات أو طرق الاعلام الأخرى.

ولما كان مشروع قانون مكافحة الجرائم الالكترونية يهدف إلى مكافحة هذه الجرائم التي تشكل تهديدا لأمن المجتمع وامن الدولة والاستقرار، بالإضافة إلى أن التطور السريع في مجال تقنية المعلومات تستوجب توفير الحماية القانونية ومعاقبة كل من يرتكب فعلا يخالف القانون واقتران تلك العقوبات بالظروف المشددة عند فرض العقوبة، خصوصا بعد ظهور حالات الابتزاز والانتحال والاحتيال والتعدي على الشرف والأخلاق وقيم المجتمع وظهور صور جديدة تتمادى في أفعالها تتحدى القانون والمجتمع وتتطوع العقل العلمي والفني إلى عقل إجرامي مقترن بخلل نفسي، ليكون ضرره كبيرا، وتمس بالحياة الخاصة للأفراد وتهدد الأمن الوطني والسيادة الوطنية وتضعف الثقة بالتقنيات الحديثة وتهدد ابداع العقل البشري، ومن أجل توفير الحماية القانونية لنظم الحاسوب التي تعمل الدولة على تشجيع الاعتماد عليها في الأنشطة كافة، خصوصا أن العراق يضع أقدامه حديثا، سالكا طريق التطور التقني والمعلوماتي، الذي يسهم بشكل مؤكد في ترصين خطوات بناء دولة القانون التي ينشدها الجميع[1].

وبصدده يمكن القول أن الجريمة السيبرانية: هي إحدى الجرائم المستحدثة التي يقوم فيها الجاني باستخدام مهاراته الفنية ومعرفته بخبايا التكنولوجيا، وعن طريق امتلاكه لبرمجيات متطورة تستطيع اختراق المواقع الشخصية أو البيانات المخزنة على اي اداة متصلة بالإنترنيت أو بأي شبكة محلية أو دولية اخرى يستطيع الحصول بواسطتها على بيانات بمختلف اشكالها سواءً من اشخاص طبيعية أو معنوية أو منظمات، بهدف استخدام هذه البيانات للحصول عن طريق الاجرام السيبراني على ما يريد من نفع مادي او معنوي سواء لغاية شخصية في نفسه، أو لتحقيق غاية يطلبها طرف آخر منه وتنفيذ طلبات لمصلحة جهة أخرى.

المطلب الثاني: صور الجريمة السيبرانية

تعد من الجرائم ذات الصور المختلفة والانواع المتعددة والمتشعبة، إذ ان هذه الصور تتنوع مرة بالنظر الى المجني عليه المستهدف، ومرة اخرى الى الهدف من ارتكاب هذه الجريمة

1- د. داليا عبد العزيز: مرجع سابق: ص 27.-

او المنفعة التي يحصل عليها الجاني السيبراني من ارتكاب هذه الجريمة ونتناول ذلك وفق التقسيم من ثم:

الفرع الاول: الاعتداء السيبراني على الجرائم المستحدثة

سنتناول هذا الفرع على ثلاث فقرات، نتطرق في الفقرة الأولى منه الى الاعتداء السيبراني على الاخلاق، وبيان العلاقة بين التطور السيبراني في زيادة ارتكاب جرائم الاتجار بالبشر، وكذلك بيان العلاقة بين التطور السيبراني مع المخدرات، وكذلك الاستيلاء والنصب والاحتيال وعلى النحو الآتي

أولا – الاعتداء السيبراني على الاخلاق: يهدف كلا من القانون والأخلاق إلي ضبط السلوك الاجتماعي للأفراد، وذلك بغية الحفاظ علي حقوق ومصالح ومشاعر المواطنين، وعدم تعرضهم للإيذاء أو الضرر، وإذا كانت الأخلاق ذات طبيعة «مثالية» تسعي إلي تحقيق ما ينبغي أن يكون، فإن القانون ذو نزعة واقعية» يسعي إلي تحقيق الممكن والمتاح، وكانت الأخلاق في المجتمعات البدائية مدمجة مع القانون والدين في كتلة واحدة تمثلها الأعراف والعادات والتقاليد[1]، ولم يكن للفرد حقوق في تلك المجتمعات فهو يتحرك في مجموعة من الأعراف والعادات والتقاليد، تبلغ قدرا كبيراً من الصرامة[2]،فالتقاليد والأعراف تتحكم في كل مظاهر حياة الإنسان في تلك العصور، ويوشك الفرد ألا يكون كائنا مستقلا بذاته في البيئة البدائية، وإذ قامت الدولة المدنية الحديثة [3]، وحلت الدولة محل الأسرة والقبيلة والعشيرة، ساد القانون، ومع ظهور الدولة المدنية الحديثة، وبخاصة مع تطور المجتمعات الصناعية، لم يعد من الممكن الإقتصار علي الأعراف، والعادات والتقاليد لمواجهة احتياجات الحياة في ظل سرعة التطورات، وتغير الظروف الإجتماعية والإقتصادية، وبذلك ظهرت الحاجة إلي ضرورة تنظيم أوضاع المجتمع عن طريق الأوامر والتشريعات[4].

مما لا شك فيه أن العالم أصبح يعاني من مشكلات اجتماعية أفرزتها البيئة الرقمية، بيد أن هذه الاشكالية أصبحت مسارا للبحث والدراسة، لا سيما في مجال علم الإجتماع، مثل الغزو الثقافي الرقمي، والبرمجة السيبرانية، والإبتزاز، والتنمر الإلكتروني.... إلخ، وفي ضوء هذه البيئة المتغيرة، ثمة حاجة ملحة لإتخاذ إجراءات – علي الصعيدين المحلي والدولي – لحماية الإستهلاك

1- د. داليا عبد العزيز: مصدر سابق، ص23.-

2- د. ماجد عمار: مرجع سابق،ص44.-

3- عبد الرحمن جلهم حمزة، جرائم الانترنيت من منظور شرعي وقانوني، ظافر للتصميم والطباعة، بغداد، بلا سنة نشر، ص22.

4- عبد الفتاح بيومي حجازي، الاثبات الجنائي في جرائم الكمبيوتر والانترنين، دار الكتب القانونية، القاهرة، 2007، ص28.-

والخصوصية، ومجابهة تقنية المعلومات ضد جميع أشكال الجريمة السيبرانية، ففي ظل ما يشهده العالم من تطور سريع ومتزايد في النظم الذكية والأجهزة الإلكترونية، وما صاحبهما من هجمات وجرائم سيبرانية غدت الضرورة ملحة لنشر دعائم الأمن السيبراني وتأمين سلامة الممارسة الإلكترونية [1]، وأن من أهم ركائز وممارسات الأمن السيبراني اجتماعيا، ومجتمعيا من خلال تحليل بعديه الإجتماعي، والقانونى لكونهما أهم بعدين، فأولهما: يبرز المخاطر والتهديدات الإجتماعية، وثانيهما: يعكس آليات المواجهة، وسبل الحماية التشريعية والتنظيمية[2]

ثانيا – دور التطور السيبراني والاتجار بالبشر: إن التقدم في التكنولوجيا، لا سيما تكنولوجيات المعلومات والاتصالات التي يتيسر الوصول إليها عن طريق الهواتف الذكية والإنترنت، يشكل وييسر جرائم الاتجار والتهريب ويخلق حواجز إضافية أمام اكتشافها والتحقيق فيها، وسوف ينظر هذا الجزء في كيفية الاستفادة من التكنولوجيات لمنع هذه الجرائم وكشفها والتدخل فيها وإحباطها في نهاية المطاف، كما سيشير أيضًا إلى جانب حاسم آخر من جوانب استخدام التكنولوجيا هذه؛ أي كيف تقوم الدول ووكالات إنفاذ القانون والهيئات الخاصة بجمع المعلومات التي يتم الحصول عليها أثناء عمليات التحقيق هذه والاحتفاظ بها واستخدامها، وتثير جميع هذه الإجراءات مخاوفا محتملة بشأن خصوصية البيانات الشخصية، ولتعطيل شبكات الاتجار بالبشر وتهريب المهاجرين، فعلى سبيل المثال، تستخدم سلطات انفاذ القوانين التكنولوجيا لتحديد المتاجرين والمهربين والتنقيب في البيانات لتحديد المعاملات المشبوهة، فقد أصبحت التكنولوجيا على الحدود منتشرة على نحو متزايد، وهذا يؤثر على سهولة الحركة ولكنه يتيح أيضًا الفرصة لمكافحة التهريب، شريطة أن تكون قوات الحدود مدربة تدريبًا كافيًا على القضايا وأن تكون قادرة على تحديد مؤشرات التهريب، ويمكن للتكنولوجيا أيضًا أن تيسر تسجيل المعلومات المتعلقة بضحايا الاتجار الذين تم التعرف عليهم وتخزينها وتحليلها وتبادلها، وعلاوة على ذلك، يمكن استخدام الدليل على أن المشتبه بهم قد استخدموا هويات متصل مزيفة أو برامج تجسس لدحض ادعاءات الجمعيات البريئة وإثبات النية الإجرامية، وتساعد عمليات حجز الرحلات الجوية والسجلات المصرفية لعمليات السحب النقدي في الخارج في إثبات الاتجار عبر الوطني[3].

ثالثا – التطور السيبراني والمخدرات: ترتبط فكرة دراسة أشكال الانحراف عبر الإنترنت؛ بالتمييز بين استخدام الإنترنت من أجل القيام بأشكال جديدة من السلوك المنحرف، أو استخدامه

1- رامي متولي القاضي، مكافحة الجرائم المعلوماتية،ط1، دار النهضة العربية، القاهرة، 2011،ص22.-

2- رشدي، محمد السعيد، الانترنين والجوانب القانونة لنظم المعلوات، دار النهضة العربية، القاهرة،2000، ص 33.-

3- هادي حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضه العربيه، 1992، ص32.-

كطريقة جديدة من أجل تنفيذ الأشكال القديمة من السلوك المنحرف، ولقد أشارت الدراسات إلى أن الإنترنت يتميز بقدرته الفريدة علي تمكين بعض الأفراد من تنفيذ ممارسات منحرفة جديدة، وإعادة إنتاج ممارسات قديمة تعبر عن أشكال من الانحراف

وتعد ممارسة تعاطي المخدرات الرقمية من الممارسات المنحرفة الجديدة المرتبطة بالإنترنت، والتي انتشرت بين مجموعات كبيرة من شباب بعض المجتمعات الغربية، إلى الحد الذي أصبحت معه مشكلة تهدد أمن الشباب وحياتهم، ومع بداية دخولها إلى عدد من المجتمعات العربية – وإن كان على نحو أقل حتى الآن يصبح من الأهمية ومن واجب العلم أن يقوم بمحاولة الاقتراب من طبيعة هذه الممارسة، ونشأتها وتطورها والأبعاد الثقافية المرتبطة بها، وما قد يترتب عليها من مخاطر وأضرار على أمن مجتمعنا العربي، وخاصة أمن شبابه، إذ أنهم الشريحة الأكثر تعرضا لمثل هذه الأخطار[1].

رابعا – الاستيلاء والنصب والاحتيال: كان لإختراع الكمبيوتر وتطوره واستخدامه في إجراء الإتصال عبر الانترنت، اثر عظيم، إذ يعد ثورة جديدة متطورة في مجال الاعلام والاتصالات، فالانترنت غير الكثير من المفاهيم الخاصة بالمكان والزمان، ولم تعد العلاقة بين الفرد ووسيلة الاعلام علاقة المتلقي الذي لا يوجد له دور سوى ان يطلع على ما تقدمه الوسيلة الاعلامية، إذ صار طرفاً فعالاً يستطيع أن ينشأ موقعاً على الانترنت يطلع عليه عدد كبير من الناس في انحاء العالم قد يتجاوز عددهم عدد من يطلع على اوسع الصحف العالمية انتشاراً، ويمكن لأي شخص ان يطلع على الكم الهائل من المعلومات التي توجد على مواقع الانترنت ويستطيع ان يرسل رسائل لمن يرغب في العالم ومن مسكنه عن طريق البريد الالكتروني ويمكنه ان يصحبها بأفلام أو بقطع من الموسيقى او بعض الصور والرسوم او برنامج من برامج الكمبيوتر، ويمكن لهذا الشخص ان يتلقى الرد على رسالته في الحال كما يمكنه ان يخاطب مراسله ويراه في ذات الوقت عن طريق استخدام ملحقات الصوت والصورة الخاصة بجهاز الكمبيوتر، ومع شيوع إستخدام وسائل تقنية المعلومات وتزايد الاعتماد على نظم المعلومات وشبكات الحاسوب وفي مقدمتها الإنترنت، شاعت في السنوات الاخيرة طائفة جديدة من الجرائم التي تستهدف المعلومات وبرامج الحاسوب كالدخول غير المرخص به الى انظمة الحاسوب والشبكات والاستيلاء على المعلومات أو إتلافها عبر تقنيات الفايروسات وغيرها من وسائل التدمير المعلوماتي وجرائم قرصنة البرمجيات، وشاعت ايضا الجرائم التي تستخدم الحاسوب وشبكات الاتصال كوسيلة لارتكاب انشطة جرمية

1- رامي متولي القاضي، مرجع سابق، ص33.-

تقليدية كالإحتيال عبر الحاسوب والتزوير باستخدام التقنيات الحديثة والنصب الالكتروني فضلا عن الاستيلاء غير المشروع [1]، هذا عوضا عن طائفة جديدة من الجرائم استخدمت تكنلوجيا المعلومات كبيئة لها، كما في جرائم توزيع المحتوى غير القانوني والضار عبر الانترنت كمخازن البيانات الجرمية ومواضيع لتنسيق أنشطة الجريمة المنظمة وجرائم غسيل الأموال الالكترونية، وجريمة الاحتيال والنصب والاستيلاء الالكتروني تعد واحدة من هذه الجرائم الهامة، دراستها مسألة هامة وضرورية بسبب تطور الحياة الاقتصادية واتجاه نشاط الافراد نحو زيادة ثرواتهم ونشوء أساليب ذلك النشاط، ومن هنا عمد الكثير من المحتالين على اختصاص هذه القرصنة واستغلال تلك الرغبة عليهم لإعمال ذكائهم ومهاراتهم للاستيلاء على بعض اموالهم ولاسيما ممن تتوفر فيه الطيبة والسذاجة والثقة الزائدة. وجرائم الانترنت من الجرائم الحديثة إذ ان حروب المستقبل ستخسر او تربح عبر شبكة الانترنت وليس في ارض المعركة لان تدمير نظم الحاسوب الحديثة لأي دولة ممكن ان يرجعها الى القرون الوسطى، كذلك يستلزم منعها ومكافحتها مكافحة فعالة بإتباع نهج دولي منسق اضافة الى التنسيق الداخلي [2]، ان هذا النوع من الجريمة السيبرانية تكون الفئة المستهدفة كمجني عليه الحكومة والشركات والجهات ذات الشخصية المعنوية كالوزارات والمصارف والبنوك وذلك إذ تتم الجريمة عن طريق الحصول على معلومات سرية خاصة بالضحية كمؤسسة والتهديد بالإعلان عن هذه المعلومات ونشرها للآخرين[3] وهناك نوع من الجريمة السيبرانية تكون فيها الفئة المستهدفة كضحية هي الحكومات والشركات والمؤسسات ذات الشخصية المعنوية. وذلك إذ تتم جريمة الابتزاز عن طريق الحصول على معلومات سرية خاصة بالضحية كمؤسسة او شركة أو وزارة حكومية، والتهديد بالإعلان عن هذه المعلومات ونشرها للأخرين[4]. وقد تبدأ جريمة الابتزاز بمتطفل أو دخيل على مواقع مهمة، ثم تتمحور شكل الجريمة ليكون التهديد بنشر هذه المعلومات حتى عن طريق السطو على موقع الشخص المعنوي ضحية الجريمة وابتزازه [5]" لا سيما وان المجرم لديه يقين بملاءمة الضحية المالية وبأنه لن يعاني من كونه معسر.

1- احمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الالي، الحماية الجنائية للحاسب الالي، دراسة مقارنة،القاهرة،2000، ص33.-

2- قايد اسامة، الحماية الجنائية وبنوك المعلومات، دار النهضة العربية،القاهره،1998،ص10.-

3- سردار علي عزيز، النطاق القانوني لإجراءات التحقيق الابتدائي، كلية القانون، جامعة السليمانية، 2008، ص111.-

4- سامي مرزوق نجاء المطيري، مرجع سابق، ص48. -

5- صالح بن محمد، المهيني المسند، عبد الرحمن بن راشد، جرائم الحاسب الالي، الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، العدد29، الرياض،2015،ص.181

الفرع الثاني: الابتزاز والتهديد السيبراني على امن الداخلي والخارجي

سنتناول هذا الفرع في فقرتين نتناول في الأولى الابتزاز السيبراني ونتطرق في الثانية الى التهديد السيبراني على امن الدولة الداخلي والخارجي.

اولا – الابتزاز السيبراني: سنتناول هذه الفقرة على وفق الآتي:

1 – **الابتزاز السيبراني ضد المرأة:** يعد اكثر انواع الجريمة السيبرانية شهرة وانتشارا إذ تعد المرأة النموذج المثالي في ارتكاب الجريمة سيما اذا كان الرجل هو الجاني السيبراني والضحية امرأة [1]، وبين السب والقذف والتهديد والترهيب تقع فتيات كثيرات ضحية المبتزين على الانترنت، اما بسبب علاقة سابقة سواء كانت زواجا او صداقة، أو بسبب التهاون في مشاركة البينات والمعلومات الخاصة مع اشخاص ليسوا محل نفسه، والجاني السيبراني قد يكون خطط لجريمة منذ البداية، وقد تزرع الفكرة في رأسه بعد ان تتوطد اواصر العلاقة بينه وبين الضحية، وقد تجتمع في ضحية الجريمة السيبرانية امرأة وايضا من الاحداث، إذ غالبا ما تتجاوب بسبب العار الذي تترقبه امامها اذا ما ذكرت في رفض طلبات الجاني[2].

2 – **الابتزاز السيبراني ضد الاحداث:** الاحداث من أكثر الفئات اتصالا بالتكنولوجيا ووسائل التواصل الاجتماعي واكثر ولعا بها، إذ باتت تشكل حيزا كبيرا من يومهم مما يسهل انزلاقهم في الجريمة إذ ان الطفل في الطالب يستهدف من اجل مطامع جنسية او تسرب معلومات عن الاهل او الام او الاخت او الاقارب ويستهل الجاني السيبراني جهل الطفل في التصرف ويمارس جريمة التسلل الى عقل الطفل واخضاعه ومن خلال الالعاب الالكترونية والحوارات عبر منصات التحاور في الالعاب والبلي ستيشن ومواقع الالعاب اون لاين في الغالب استغلال حب الطفل للعبة والتقرب منه والحصول منه على معلومات او صور ومقاطع ومن ثمة ابتزازه بنشر تلك المحتويات للعائلة[3]

وتكثر جرائم الابتزاز من خلال قيام الجاني السيبراني بالضغط على الحدث بتهديده بنشر صور او تسجيل مرئي او محادثات على مواقع الدردشة او اية مادة، عن واقعة أو وقائع يكون من شأنها تحقير للمجني عليه عند اهله ووطنه[4]،فالطفل يخضع للابتزاز ويستجيب للمبتز بسبب

1- محمد علي عريان،الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004،ص62.-

2- سردار علي عزيز،مرجع سابق، ص122.-

3- عادل عبد العال إبراهيم، جرائم الاستغلال الجنسي للأطفال عبر شبكة الانترنيت وطرق مكافحتها في التشريعات الجنائية والمتهم الجنائي الإسلامي، جامعة الازهر، مصر،2013، ص55.

4- خليفه بن علي بن محمد الزريق، ابتزاز الاحداث وعقوبته في النظام السعودي، دراسة تاصيلية مقارنة تطبيقية، رسالة ماجستير جامعة نايف العربية للعلوم الأمنية، الرياض،2015،ص72-73

الثقة المفرطة التي كونها الجاني خلال التواصل لفترات طويلة مع الطفل، فضلاً عن الخوف من تهديد الجاني في حالة عدم الاستجابة لرغباته والتعرض للعنف او الاهمال في المنزل والبحث عن اهتمام من طرف ما والحاجة المادية التي يحتاجها الطفل، وضعف التواصل الاسري مما يجعل الطفل لا يتحدث لوالديه ورغبة الضحية الناتجة عن الزيارات المتكررة لمواقع الاباحية، فقدان احد الابوين مما يجعل الطفل يلجأ للبديل عبر مواقع الشبكة العنكبوتية[1].

3 - **الابتزاز السيبراني ضد الرجال:** يقع الرجال ضحية للجريمة السيبرانية من اجل الحصول على الاموال وبالعادة يدرس الجاني السيبراني وضع الشخص الاجتماعي وحياته واصدقائه وبياناته لغاية التمهيد لارتكاب جريمة الجريمة السيبرانية فق ديكون الرجل ميسور الحال لديه اموال كثيرة كونه تاجر او مقاول او رجل اعمال من الاثرياء ماديا وتعرضه للابتزاز من بعض النساء المحترفات ببيع الهوى على المواقع الالكترونية وتهديده بنشر الصور او مقاطع مصورة لتهديد مركزه الاجتماعي، كما يكون الرجل عرضه لجرائم الابتزاز بشكل عام بسبب ابتزازه في مجال عمله او اي معلومات بشكل عام يرى الرجل الضحية ان الافصاح عنها ونشرها يؤذي شرفه وسمعته في البداية يبدأ من خلال ارسال طلبات صداقة وطلبات التعارف عبر الانترنت ومن ثم الحصول على بيانات ومعلومات اضافية او استعمال كاميرات المحادثة وممارسة الجنس عن طريق الكاميرات ومن ثم الاحتفاظ بتلك المقاطع إذ يتم الانتقال الى اي وسيلة للتواصل المرئي مثل برامج الفيديو المشهورة، واتس آب فايبر، مسنجر فيس بوك، ايمو، سكايب[2]، وذلك يرجع الى انه غالبا ما يكون تهديد الجاني السيبراني للمرأة هنا ادواته فيها صورا فاضحة او محادثات خادشة للحياء، او عرضا مرئيا لعلاقة غير شرعية جمعت ما بين الجاني السيبراني وضحيته، والجاني السيبراني قد يكون خطط لجريمته منذ البداية، وقد تزرع الفكرة في رأسه بحجة ان تتوطد اواصر العلاقة بينه وبين ضحية جريمة ابتزازه المرتقبة، وقد تجتمع في ضحية الجريمة السيبرانية كونها امرأة وايضا من الاحداث، إذ تتضاعف فرصة الجاني السيبراني في هذه الحالة في ارتكاب جريمته والوصول الى مآربه بالضغط على الضحية. والتي غالبا ما تتجاوب بسبب العار الذي تترقبه امامها اذا ما فكرت في رفض طلبات الجاني، اذ تظهر امامها صورتها بعد ان ينشر على الملأ ما حرصت على اخفاؤه[3]

1- عادل عبد العال إبراهيم، مرجع سابق،ص121.-

2- عبد العزيز بن حمين بن احمد الحمين، الابتزاز ودور الرئاسة العامة لهيئة الامر بالمعروف، ندوة الابتزاز، مركز باحثات لدراسات المراة بالتعاون مع قسم الثقافة الإسلامية جامعة الملك سعود، الرياض،1432هـ ص61.

3- سردار علي عزيز، مرجع سابق، ص55.-

لاعتبارها ان في نشره معرة لها ولأهلها، سيما اذا كان سبب الابتزاز علاقة جنسية غير مشروعة ينظر لها الدين والمجتمع بالتحريم والرفض والاستهجان[1].

ثانيا – التهديد السيبراني على امن الداخلي والخارجي

يحتل موضوع الاعتداءات السيبرانية بصورة عامة حيزاً كبيراً من اهتمام فقهاء القانون لما تشكله هذه الظاهرة من خطر جسيم على المجتمع بما يخلفه من ضياع للأمن، وتدمير للممتلكات، وانتهاك للحرمات، وتدنيس للمقدسات، وقتل، وخطف للمدنيين الآمنين، وتهديد لحياة الكثير منهم، ففي ظل انتشار ظهور التكنولوجيا الحديثة، وأزدياد إعتماد العالم عليهما، لم يعد الإرهابي بحاجة الا لجهاز حاسوب آلي وتأمين إتصاله بشركة الإنترنت للقيام بالأعمال الإرهابية، ذلك أن الإرهاب الإلكتروني هو خطر يهدد المجتمع الدولي بإجمعه وخطورته تتركز في سهولة استخدام شبكة الإنترنت، وانتشار استخدام وسائل التواصل الإلكتروني بين الجماعات الإرهابية في الترويج والتنظيم للمخططات الإرهابية[2]

إذ أن لكل جريمة أركانها الخاصة بها والتي تميزها عن غيرها وتقوم بتحديد نطاقها وترسم لها حدودها الفاصلها التي تفصلها عن غيرها من الجرائم والتي اذا إنتفى أحدها تنتفي معه الجريمة، وهذه الأركان مستنبطة من المبادئ العامة للتجريم، وجريمة الإرهاب بالالكتروني لها أركان ثلاث، أولهما الركن المادي الذي هو عبارة عن المظهر الخارجي لنشاط الجاني، وآلية تنفيذ تلك الجريمة بإستخدام الوسائل الإلكترونية، وثانيهما الركن المعنوي الذي يتمثل في القصد الجنائي أي علم الجاني بموضوع جريمة الإرهاب وإرادة الدخول فيه، وثالثهما الركن القانوني متمثلاً بالنص التشريعي الذي يحدد شروط العقاب، تطبيقاً لمبدأ الشرعية الجزائية المتمثل في لا جريمة ولا عقوبة الا بنص[3]. ويُعد الاعتداء السيبراني أخطر الظواهر الإجرامية التي تهدد أمن وسلامة المجتمع، فهو صورة مستحدثة للإرهاب التقليدي الذي استغل التطور التكنولوجي ووسائل الاتصال الحديثة في بث الرعب والخوف في نفوس الأفراد والاعتداء على أمن الدول واستقرارها، وذلك عن طريق استخدام شبكة الإنترنت للقيام بأعمالهم الإرهابية والترويج للأفكار الضالة المتطرفة وبث البيانات والتصريحات والأفلام المصورة التي تعلم كيفية استعمال الأسلحة

1- عادل عبد العال إبراهيم، مرجع سابق، ص121.-

2- د. داليا عبد العزيز، مرجع سابق، ص 27.-

3- عادل عبد العال إبراهيم، مرجع يابق، ص121.-

وصنع المتفجرات والقيام بالعمليات الانتحارية، أو من خلال تدمير البنى التحتية للدول والمؤسسات الدولية، وهذا عن طريق اختراق الشبكات السلكية واللاسلكية بواسطة الفيروسات والبرامج الخبيثة تحقيقاً لأغراض وغايات ارهابية بحته وما له من اثر كبير على امن الدولة، كما يعد الارهاب الالكتروني واحد من اهم المسائل الجديرة بالاهتمام ذلك ان اغلبية دول العالم تستخدم تقنيات ووسائل التواصل الاجتماعي على نطاق واسع وبشكل شبه يومي ومستمر، لذا يجب ان يكون هناك توازن بين ذلك الاستخدام وبين امن الدولة، وبين طبيعة الاجراءات المتخذة من الدول لمواجهة تلك الاخطار المتجددة، وصولا الى تضيق الخناق على العناصر الارهابية التي تستغل وسائل التكنولوجيا الحديثة في ارتكاب جرائمها الارهابية[1].

1- عادل عبد العال ابراهيم، مرجع سابق، ص 121.-

المبحث الثاني
مفهوم التدابير الامنية ودور التشريعات في مكافحة الجرائم السيبرانية

يعد موضوع التدابير الامنية من أشد الموضوعات جدلاً بين فقهاء القانون الجنائي، والتي انتجت تيارات فكرية مختلفة حاولت ان تؤسس لنظرية عامة للتدابير القانونية، ومن اجل الوقوف على المعنى الادق والذي يتفق مع غائية الجزاء في تحقيق الأمن والاستقرار عن طريق حماية المصلحة المعتبرة، كان من الواجب تقسيم هذا المبحث الى مطلبين نبحث في الأول تحديد مفهومها ونخصص المطلب الثاني لدور التشريعات في مكافحة تلك الجرائم.

المطلب الاول: مفهوم التدابير الامنية

سنتولى في هذا المطلب دراسة اليه مدلول التدابير الأمنية في الاطار اللغوي والفقهي وكذلك مدلولها القانوني في ضوء الفرعيين الآتيين.

الفرع الاول: المدلول اللغوي الفقهي للتدبير

سنتولى تقسيم هذا الفرع على فقرتين، نتطرق في الفقرة الأولى المعنى اللغوي للتدبير، ونبين في الفقرة الثانية المعنى الفقهي للتدبير على النحو الآتي:

اولا – المعنى اللغوي للتدبير يشير مصطلح التدبير في معاجم اللغة العربية الى معنى الاحتياط والاستعداد[1] ويقصد به الإجراءات الاحتياطية [2]، والتدبير هو جمع لغير المصدر، مفرده دَبَرَ، ويقال دَبَرَ الأمر أذا ساسه ونظر في عاقبته [3]، أو أن تنظر إلى ما تؤول إليه عاقبته، والتدبير هو تقويم الامر على ما يكون فيه صلاح عاقبته أي تقويم الأمر على مقدار يقع معه الصلاح[4]، ويقصد به أن يُحكم الأمر وينزل فيه القضاء مثلما في قوله تعالى: (يُدَبِّرُ الْأَمْرَ مِنَ السَّمَاءِ إِلَى الْأَرْضِ ثُمَّ يَعْرُجُ إِلَيْهِ فِي يَوْمٍ كَانَ مِقْدَارُهُ أَلْفَ سَنَةٍ مِّمَّا تَعُدُّونَ) [5]. وتستخدم كلمة في

1- د. احمد مختار عمر، معجم اللغة العربية المعاصرة، المجلد الأول، ط2، عالم الكتاب، 2008، ص2476.-
2- محمد بن مكرم ابن منظور، لسان العرب، المجلد الأول، دار بيروت الطباعة، بيروت،1995، ص 273.-
3- محمد رواس قلعجي، معجم لغة الفقهاء، الطبعة الثانية، دار النفائس للطباعة والنشر،1988، ص127.-
4- ابي الهلال العسكري، معجم الفروق اللغوية، الطبعة السادسة، مؤسس النشر الإسلامي،مدينة قم، 213، ص121.-
5- سورة السجدة، الاية 5.-

اللغة الإنكليزية للدلالة على معنى التدابير في الاصطلاح القانوني، فيما يعبر عنها كأداة قياس بالاصطلاح العام، أما في اللغة الفرنسية تستخدم للدلالة على التدبير[1].

ثانيا – التعريف الفقهي للتدابير الأمنية: يشار بالسبق إلى النظريات الوضعية في استعمال مصطلح التدبير للدلالة على الجزاء الذي يوجه الى معالجة الخطورة [2]، وعلى الرغم من اتجاه اغلب الفقه إلى الإقرار بضرورة معالجة الخطورة بواسطة التدابير، إلا إن الفقهاء اختلفوا في تحديد مدلولها، فهل هي تدابير علاجية تعالج الخطورة الاجرامية أم هي تدابير وقائية تتسع لتعالج الخطورتين الاجتماعية والإجرامية، ومن هذا الاساس انقسم الفقه الى اتجاهين، إذ ذهب الاتجاه التقليدي الى ان التدابير هي وسائل علاجية تستهدف الخطورة التي تكشف عنها الجريمة فقط، وتهدف إلى منع ارتكاب الجريمة مرة أخرى، أي حصر نطاق التدابير في الاحتراز، حين عرفت بأنها (مجموعة من الإجراءات تواجه خطورة جرمية كامنة في شخص مرتكب الجريمة لتدرأها عن المجتمع) [3]، وعرفها آخر بانها مجموعة إجراءات يقررها المشرع لمواجهة خطورة إجرامية كامنة في شخص مرتكب الجريمة بهدف درء هذه الخطورة عن المجتمع[4].

ويتجه آخر الى عدها أسلوباً يقصد به العلاج والتأهيل اذ عرفت بأنها مجموعة من الأساليب العلاجية التي توجه الى الخطورة الاجرامية بقصد تأهيل المجرم واصلاحه والعمل على حماية المجتمع ويشترط لفرضها صدور حكم قضائي، فيما غلب آخر الصفة القضائية حين عرفها بانها إجراءات تصدر وفق حكم قضائي لتجنيب المجتمع الخطورة الاجرامية الكامنة في مرتكب الجريمة[5]، وفي الاتجاه ذاته عبر عنها أخر بأنها مجموعة من الإجراءات نص عليها المشرع بغية مواجهة ما يكمن في شخص مقترف الجريمة من خطورة انيط بالقضاء مهمة الحكم بها، ولذا لا سبيل للقضاء ان يحكم بها الا بوجود نص قانوني[6]، وعرفه اخر بانه جزاء او تدبير امن يحدده المشرع لمواجهة الخطورة الاجرامية التي تطويها شخصية مرتكب الجريمة لتدرأها عن المجتمع[7] ونخلص مما تقدم ان الاتجاه التقليدي حصر التدابير في اضيق نطاق حين جعلها مقتصرة على علاج الخطورة الاجرامية فقط.

1- د. يوسف عبد المنعم الأحول، قانون الإجراءات الجنائية الفرنسي،ط1، دار النهضة العربية، القاهرة، 2016، ص2.-

2 -د. يوسف عبد المنعم الاحول، المصدر أعلاه، ص73.-

3- د. محمود نجيب حسني، دروس في علم الاجرام وعلم العقاب، دار النهضه العربية، القاهرة، 1988، ص 245.-

4- د. يوسف عبد المنعم الاحول، المصدر أعلاه، ص 261.-

5- د. يسر نور علي، ود. امال عثمان، الوجيز في علم الاجرام والعقاب، دار النهضة العربية، القاهرة، 1977،ص 270.-

6- د. حاتم بكار، حماية حق المتهم في محاكمة عادلة، مؤسسة المعارف للطباعة، الإسكندرية، 1998، ص489.-

7- د. عبد الرزاق فخري الحديثي، شرح قانون العقوبات القسم العام، مطبعة الزمان، بغداد، 1992، ص 512.-

أما الاتجاه الحديث من الفقه حاول أن يوسع من نطاق التدابير لعلاج الخطورة السابقة لارتكاب الجريمة، فضلاً عن الخطورة اللاحقة للجريمة، لذا يقصد بها على وفق هذا الاتجاه الإجراءات الموجهة لمنع ارتكاب الجرائم ولو للمرة الأولى، فهي التدابير الموجهة لمعالجة الخطورة الاجرامية الكامنة، والتي تكشف عنها الجريمة الأولى التي ارتكبها، وتستخلصها المحكمة من الامارات الشخصية والمادية، وهي تهدف في الوقت عينه الى معالجة الخطورة الاجتماعية التي افترضها المشرع في بعض الاشخاص الخطرين، ولذا عُرفت بأنها (مجموعة من الإجراءات التي تطبق على من تثبت خطورته الاجرامية او الاجتماعية على النظام الاجتماعي)

الفرع الثاني: المدلول القانوني للتدابير

على الرغم من ان المشرع العراقي لم يتظم التدابير في قوانين عقابية وقوانين خاصة عدة، الا انه لم يتجه الى إيجاد تنظيم قانوني موحد يجمع هذه التدابير وفق نظرية قانونية متسقة، بل أتت متناثرة في مواد قانونية عدة، منها ما جاء في متن قانون العقوبات وأخرى ذكرت في قانون أصول المحاكمات الجزائية فضلاً عن تنظيمه للتدابير في عدد من القوانين الخاصة كقانون الأحداث وقانون مكافحة المخدرات والمؤثرات العقلية، وأورد عدداً من التدابير في تشريعات أخرى نظمت الامن الاجتماعي كقانون الإقامة وقانون لمرور وقانون الأسلحة وقانون الدفاع المدني، اما من إذ التسمية اطلق قانون العقوبات العراقي التدابير الاحترازية على الفصل الرابع من الباب الخامس[1]، فيما نظم قانون أصول المحاكمات الجزائية تدابير حفظ السلام وحسن السلوك في الباب الثالث من الكتاب السادس، ووصفها بالعسكرية في أسبابه الموجبة [2]، فيما ذكر قانون رعاية الاحداث مصطلح التدابير فقط في المادة (76) دون تحديد صفتها، فيما استخدم قانون الدفاع المدني في المادة (1) عاشراً) تعبير التدابير القانونية للدلالة على تدابير السلامة العامة والتي عرفها بأنها الإجراءات الاحترازية التي تنفذها الجهات المعنية بالدفاع المدني بهدف تأمين الحماية اللازمة للسكان، وأطلق عليها قانون مكافحة المخدرات والمؤثرات العقلية رقم (50) لسنة 2017 في مواد (39 – 40) تدابير معالجة المدمنين.

1- عالج قانون العقوبات العراقي التدابير الاحترازية في المواد(103-127) وقسمت الى تدابير سالبة للحرية او مقيدة لها او تدابير سالبة للحقوق او تدابير مادية.

2- حددت المذكره الايضاحية لقانون أصول المحاكمات الجزائية العراقي الغاية المتوخاة في معرض حيثها عن أهمية إقرار التدابير حفظ السلام وحسن السلوك في وقاية المجتمع من الجريمة.

وعلى صعيد التشريعات العربية [1]، إذ استعمل قانون العقوبات الجزائري مصطلح (تدابير الأمن) [2]، فيما اطلق مشروع قانون العقوبات المصري تسمية (التدابير الجنائية)، اما قانون العقوبات الإماراتي رقم (3) لسنة 1987 النافذ وصفها أيضاً بالتدابير الجنائية والتي جمع فيها تدابير الدفاع الاجتماعي والتدابير الاحترازية)[3]، فيما استعمل مصطلح التدابير فقط في تعديل قانون العقوبات المصري النافذ في المادة (88/د) من تعديل قانون العقوبات رقم (97) عام 1992 دون تحديد صفتها، فيما استعمل مصطلح التدابير الاحترازية في بعض القوانين العقابية ومنها اللبناني والسوري والعراقي، فيما نظمت العديد من القوانين الاجرائية تدابير الخطورة الاجتماعية السابقة للجريمة تحت تسميات مختلفة)[4].

يلخص الباحث مما تقدم انه وعلى الرغم من عدم وحدة التنظيم التشريعي للتدابير في التشريعات العراقية، إلا ان من الثابت السياسة الجنائية المعاصرة بوصف التدابير الصورة الثانية من صور الجزاء الجنائي، والتي اما تقتصر على معنى الاحتراز فقط، أي تعالج نوع واحد من الخطورة فقط والتي تكشف عنه الجريمة السابقة فقط، أو توسع من نطاق التدابير حين توجه الى معالجة نوعي الخطورة الاجتماعية اذا كانت سابقة على الجريمة، أو الاجرامية اللاحقة على ارتكاب الجريمة، وكلاهما يخضعان الى اصل واحد وهو الجزاء الجنائي الهادف الى تنظيم الرد الاجتماعي إزاء الخطورة.

المطلب الثاني: التشريعات الوطنية المختصة بمكافحة الجرائم السيبرانية

ان ثورة الاتصالات عن بعد قد غيرت الكثير من المفاهيم التقليدية التي كانت تسير دفة الحياة قبل بزوغ فجر هذه الثورة، فبدأنا نسمع عن العمليات المصرفية الالكترونية وعن الحكومة الالكترونية وعن المستندات والنقود الالكترونية وعن التوقيع الالكتروني في اطار المعاملات التي تتم عن طريق الشبكة العالمية (الانترنت) الا ان ظهور هذه العمليات الجديدة اوجب توفير الحماية الجنائية لها ضد صور الاعتداء المتطورة، والتي قد تقع عليها بالوسائل الالكترونية المتطورة، الا ان ذلك قد اظهر قصورا كبيرا في النصوص الجنائية الموضوعية والاجرائية، إذ اصبحت هذه

1- د. غالب عبيد، شرح قانون العقوبات العام،ط1،مطبعة جعفر العصامي، بغداد، 2010، ص168.-

2- المادة(4) قانون العقوبات الجزائري.-

3- د. محمود سامي القرني، النظرية العامة للتدابير الاحترازية، أطروحة دكتوراه، جامعة عين شمس، كلية الحقوق، 1989، ص 4-5.

4- نظم قانون أصول المحاكمات الجزائية العراق احكامها في المواد(317-321) تحت تسمية حفظ السلام وحسن السلوك.-

النصوص عاجزة عن كفالة توفير الحماية الفاعلة للمصالح والقيم التي افرزتها ثورة الاتصالات عن بعد، لان الجريمة ظاهرة اجتماعية، تتأثر طبيعتها وحجمها بالتحولات الاقتصادية والاجتماعية والثقافية دوليا ووطنيا، ولم التشريع العراقي يفرد نص خاص يعالج الجرائم السيبرانية بشكل مستقل على الرغم من خصوصيته بالنظر للمغايرة في طريقة الارتكاب والمصلحة المحمية، لذا سوف نستعرض تلك النصوص وفقاً لما يأتي:

الفرع الاول: قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل

لم ينظم قانون العقوبات العراقي الجرائم السيبرانية، فقد جاءت نصوصه خالية من الإشارة إلى الجرائم الواقعة عليها[1]، لذا كان من الواجب الرجوع إلى النصوص الواردة في قانون العقوبات لبيان مدى أمكانية انطباقها على هذه الجريمة أو لا، ومن خلال تحليل النصوص التي عالجت الجرائم السيبرانية أن نلاحظ أن المشرع العراقي وبالمقام الأول لم يعالج الجرائم السيبرانية بشكل منفصل ولم يتطرق في كل نصوصه إلى عبارة تدل على ذلك، وإنما ترك أمر معالجتها للنصوص العامة التي عالجت الموضوع، ولعلنا من هذا المنطلق يمكننا أن نسجل عدد من المأخذ على المعالجة القانونية لهذه الجريمة، فالجرائم السيبرانية لها عدد من الصور التي تميزها عن غيرها، ومن ثم فمعالجتها في نفس سياق المعالجة التقليدية للجرائم السيبرانية فيه قصور واضح، ومن ثم فلا يجوز القياس في مورد النص، أما من ناحية أخرى فأن التزوير الالكتروني في البطاقة الوطنية غير مجرم كون المشرع العراقي لم يتطرق إلى هذا النوع المستحدث[2].

ويلاحظ هنا أن التجريم في مجال قانون العقوبات محكوم بمبدأ مهم قد نص عليه المشرع العراقي في قانون العقوبات وأكد عليه لاحقاً في الدستور العراقي ألا وهو (لا جريمة ولا عقوبة ألا بنص) ذاك أن إغفال تنظيم جريمة لها آثار اقتصادية سيئة على النظام القانوني والاقتصادي للدولة من شانه أن يؤدي إلى ترك ثغرات يمكن من خلالها المجرمون أن ينفذوا من العقاب، وقد أكدت محكمة استئناف بابل الاتحادية بصفتها التمييزية[3] هذا المبدأ عند إصدارها لحكم تضمن

1- د. عبود السراج، المبادئ العامة في قانون العقوبات لنظرية العقوبة، منشورات جامعة دمشق، مركز التعليم المفتوح،2005،ص133.-

2- ايمن عبد الله فكري، مرجع سابق، ص 34.-

3- قرار محكمة تميز بابل الاتحادية بصفتها التمييزية رقم(2011/120/ هيئة جزائية) بتاريخ 2011/8/4 قرار غير منشور.-

صحة القرار الصادر من محكمة جنح المسيب برفض الشكوى لعدم احتواء القوانين العقابية النافذة على أي نص يجرم استعمال البريد الالكتروني ومعرفة الرقم السري وما يرتب بعدم جواز القياس في التجريم لمثل هذه الأفعال على جرائم أخرى لان مثل هذا الأمر يؤدي إلى المساس بمبدأ دستوري وجنائي عتيد منصوص عليه في أغلب الدساتير والقوانين العقابية ألا وهو مبدأ لا جريمة ولا عقوبة ألا بنص، وعليه أتمنى على المشرع العراقي إدخال تعديلات على قانون العقوبات لتجريم الاعتداءات التي تمس المعلومات بصورة عامة والجرائم السيبرانية بصورة خاصة.

الفرع الثاني: قانون التوقيع الالكتروني والمعاملات الالكترونية

يعد قانون التوقيع الالكتروني رقم (78) لسنة 2012 من القوانين الحديثة التي وفرت الحماية للتوقيع الالكتروني والذي يهدف إلى تعزيز الإطار القانوني للمعاملات الالكترونية وإسباغ حجية قانونية على الوسائل الالكترونية[1] والذي يمكن من احد أهم مكونات البطاقة الوطنية ومن العناصر الأساسية للتكوين المادي ويمكن تعريف بأنه (علامة شخصية تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو أصوات وغيرها وله طابع منفرد يدل على نسبته للموقع ويكون معتمدا من جهة التصديق)[2].

وتضمن القانون تنظيم للتوقيع الالكتروني والمستندات الالكترونية، منها ما جاء في المادة (1 / ثالثا) التي عرفت التوقيع الالكتروني بأنه مجموعة من المعلومات والبيانات والنصوص والصور والإشكال والأصوات والرموز وما شابه ذلك التي تنشا أو تدمج أو تعالج أو ترسل أو تستلم بوسائل الكترونية (وكذلك ما جاء في نفس المادة الفقرة (تاسعاً) التي عرفت المستندات الالكترونية بأنها المحررات أو الوثائق التي تنشا أو تدمج أو تخزن أو ترسل أو تستقبل كلياً أو جزيئا بوسائل الكترونية بما في ذلك تبادل البيانات الكترونياً أو البريد الالكتروني أو البرق أو التلكس أو النسخ البرقي ويحمل توقيعاً الكترونياً) إما المادة (3 / أولا /ج) فقد صرحت بسريان القانون على الأوراق المالية والتجارية الالكترونية)، والجدير بالذكر أن القانون قد ساوى بين المحررات العادية والالكترونية وأعطاها نفس الحجية المقررة للمحررات الورقية وذلك في المادة (13 / أولا) التي نصت على تكون للمستندات الالكترونية والكتابة الالكترونية والعقود الالكترونية ذوات الحجية القانونية لمثيلتها الورقية أذا توافرت فيها الشروط آلاتية:

1 -المادة(2) قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم(78) لسنة 2012.-

2- المادة(الأولى/ رابعا) قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم(78) لسنة 2012.-

أ- أن تكـون المعلومـات الـواردة فيها قابلـة للحفـظ والتخزين إذ يمكن اسـترجاعها في أي وقت.

ب- أمكانية الاحتفاظ بها بشكل الذي تم إنشاؤها أو إرسالها أو تسلمها به أو بأي شكل يسهل به أثبات دقة المعلومات التي وردت فيها عند إنشائها أو إرسالها أو تسلمها بما لا يقبل التعديل بالإضافة أو الحذف

ج- أن تكون المعلومات الواردة فيها دالة على من ينشؤها أو يتسلمها وتاريخ ووقت إرسالها وتسلمها.

المطلب الثالث: دور أجهزة قوى الامن الداخلي في مواجهة الجرائم السيبرانية

الجرائم السيبرانية في العراق شأنها شأن باقي الدول الأخرى تتميز بالحداثة، والتوسع بالاطراد مع توسع استخدام وسائل التواصل الاجتماعي، والتكنلوجيا الحديثة، وهذا يستتبع بالضرورة توسع عمل جهات الضبط القضائي، ووسائل مقاومة الجريمة والاستدلال عليها، والعديد من الصعوبات التي تواجههم في سبيل ذلك، ومقدار التطور الذي ادخل على عمل سلك الشرطة لمواجهة مختلف أنواع الجرائم، وهذا ما سنتناوله في فرعين تاليين:

الفرع الأول: الصعوبات التي تعترض عمل رجل الشرطة في تلك الجرائم

للجريمة أنواع متعددة ومختلفة وقلما يعنى القانون ببيانها، وهذا أسلوب انتهجه المشرع القانوني في أغلب قوانين العقوبات، فقد اكتفى المشرع ببيان أنواع الجرائم بالنظر إلى جسامة الجريمة وطبيعتها فقط[1]، فقد جاء في قانون العقوبات رقم (111) المعدل لسنة 1969 المعدل، ببيان إلى جناية وجنحة ومخالفة، واستدل عليها بمدة العقوبة المقررة لكل واحدة منها[2]، أما من إذ طبيعتها فقد قسم المشرع الجرائم إلى جرائم سياسية واعتيادية، وبين شروط وأركان تحقق تلك الجرائم واستدل عليها من طبيعة أفعالها[3]، لكنه لم يتطرق الى الجرائم السيبرانية لا من بعيد ولا من قريب، ليس هو فقط وانما كذلك قانون اصول المحاكمات الجزائية العراقي، الذي يمثل القانون

1- د. علي حسين خلف ود. سلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، دار العاتك، مصر، القاهرة، 2006، ص 285.-

2- المواد(23-27) قانون عقوبات عراقي رقم(111) لسنة 1969 المعدل.-

3- المادة(20) قانون عقوبات العراقي رقم (111) لسنة 1969 المعدل.-

الاجرائي الام لبقية القوانين، وهذه تمثل اول عقبة وصعوبة تقف في وجه أعضاء الضبط القضائي ومنهم رجال الشرطة في ممارسة مهامهم المناط بهم اتخاذها ف يتعقب الجرائم والمجرمين.

وهناك العديد من السمات التي تتسم بها الجرائم السيبرانية تجعل من الصعب على سلطات الضبط التعامل معها والقبض على مرتكبيها، وضبط أدلتها، ومن أهم تلك الصعوبات[1].

أولا - عدم وجود قانون مختص بالجرائم السيبرانية

ان تزايد استخدام وسائل التكنلوجيا الحديثة، وتسارع تطورها، وكذلك انتشار وسائل التواصل الاجتماعي، أدى كل ذلك الى تزايد وتيرة الجرائم السيبرانية بشكل ملحوظ في الآونة الأخيرة، وهذه الزيادة في عدد الجرائم من المفترض أن يقابلها زيادة في عدد القوانين التي تواجه الاجرام المعلوماتي في شتى المجالات، كما يجب أن يقابلها زيادة في الوسائل المستخدمة في تتبع الجريمة ومرتكبيها كماً ونوعاً [2].

الا أن الملاحظ في العراق انه لم يصدر حتى الآن أي قانون مختص بالجرائم السيبرانية، كما سبق ان اوضحنا ذلك، مما يضطر القضاة الى اللجوء الى النصوص العامة في قانون العقوبات، وتكييف الجرائم السيبرانية التي ترتكب وفقها، وهذا الأمر قد يستقيم مع بعض الجرائم الا أن هلا يستقيم مع البعض الآخر، نظراً لطبيعة بعض الجرائم السيبرانية الخاصة[3].

اما عن الجانب الاجرائي والذي يخص موضوعنا، فالطبيعة الالكترونية للجرائم الالكترونية تفرض على الجهات المختصة بالاستدلال نهج سبل خاصة من أجل الوصول الى مرتكب الفعل والى الدليل، فوجود الجريمة في عالم افتراضي يحتم على رجل الشرطة اتباع تقنية برمجية خاصة، توصله الى الجريمة والى الفاعل، وتوثق الدليل، وكول ذلك يستلزم بالضرورة قواعد قانونية تقنن وتبيح لرجل الشرطة ولباقي أعضاء الضبط القضائي اتخاذ الإجراءات اللازمة لذلك، وتحرم الأفعال التي تعد من قبيل التعدي على حرية وخصوصية الافراد، ومن دون وجود قانون ينظم ذلك تبقى المسألة محط اجتهاد فيما يخص كيفية الاستدلال عن الجرائم وضبطها، واجراء التفتيش للوصول الى الدليل، وحتى كيفية المحافظة على الدليل من الضياع بعد أن يتوصل اليه رجل الشرطة[4].

1- د. محمد الأمين البشري، مرجع سابق، ص 45.-

2- د. ايمن عبد الله فكري، مرجع سابق، ص 89.-

3- حسن علي حسين علي، الجزائي في قانون الإجراءات الجنائية، منشاة المعارف، الإسكندرية،2008، ص 133.-

4- طه احمد متولي، الدليل العلمي واثره في الاثبات الجنائي، مطابع الشرطة، القاهره، 2008، ص67.-

ثانيا – عدم كفاية القوانين الموجودة

وقد سبق وان بينا ان نقص القوانين الخاصة بالجرائم المعلوماتية والالكترونية، سيدفع الجهات المختصة بالاستدلال الى التوجه صوب ما هو موجود من قوانين تحكم كيفية اتخاذ هذا الاجراء أو ذاك[1].

الا أن القوانين المتواجدة بحكم انها تعالج جرائم تقليدية، وأدلة مادية واقعية يمكن الحصول عليها بشكل ملموس من مسرح الجريمة أو من أي مكان آخر، وهو أمر يسهل تتبعه والقيام به من قبل أعضاء الضبط القضائي، بخلاف الجرائم السيبرانية، والتي تتواجد في عالم افتراضي لا واقعي ومادي ملموس، يتطلب أن يكون القانون قد نظم طريقة القيام بذلك في مثل هكذا واقع افتراضي، لا أن يوكل كل ذلك الى قوانين تحكم نوع مختلف من الجرائم، وهي لا تكفي في وجه من الوجوه الى شمول كول تلك الأنواع المستحدثة من الجرائم بأحكامها، الأمر الذي يجعل القوانين الحالية عاجزة عن سد النقص الذي يعتريها لمواجهة كافة الفروض التي تطرأ، والتي تزداد وتتنوع كلما ازدادت أو تنوعت وسائل التكنلوجيا الحديثة ووسائل التواصل الاجتماعي[2].

ثالثاً – احجام الكثير من الجهات والمجنى عليهم عن الإبلاغ عن تلك الجرائم

وتكمن وراء احجام بعض الجهات التي تقع عليها الجرائم السيبرانية عن الإبلاغ عنها العديد من الأسباب المختلفة، وبغض النظر عن الأسباب التي دعت الى الاحجام عن الإبلاغ عن وقوع الجرائم السيبرانية، الأ ذلك يبقى صعوبة تعترض طريق الوصول الى تلك الجرائم، وتشكل عوائق امام السلطات المختصة في أداء مهامهم في الاستدلال عن وقوع الجرائم، والتوصل الى مرتكبيها، لان الاخبار عن وقوع الجرائم طريق مهم من الطرق التي تساعد أعضاء الضبط القضائي في الوصول الى مرتكبي الجرائم، والى الأدلة التي توصل الى الجريمة المرتكبة والى الحقيقة[3].

1- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنيت، دار النهظة العربية، القاهرة، 2009، ص34.-

2- سعيد محمد عبد الكريم الابراهيمي، سلطات أعضاء الضبط القضائي في التحري وجمع الأدلة، كلية القانون،200، ص87

3- مصطفى محمود موسى، الجهاز الالكتروني لمكافحة الجريمة سلسلة اللواء الأمنية في مكافحة الجريمة الالكترونية، الجزء الأول، سنة 2001، ص88.

رابعاً - سهولة إخفاء معالم الجريمة

تتميز الجرائم السيبرانية بالعديد من الميزات الخاصة، من بينها ميزة سهولة إخفاء معالم الجريمة، بسبب الطبيعة الافتراضية للجريمة الالكترونية، فما دام السلوك الجرمي الي يمثل الركن المادي للجريمة الالكترونية هو عبارة عن معلومات يتم تخزينها في أي جهاز حاسوب أو موبايل أو قرص... الخ من وسائل حفظ المعلومات الالكترونية، فان ذلك يسهل بشكل كبير إخفاء تلك المعلومات، وكذلك إمكانية التخلص منها، ومحو آثار الجريمة وطمسها، مما يصعب عملية البحث عن الجريمة وعن الأدلة، ويصعب من ثم الوصول الى مرتكب الفعل[1].

خامساً - عدم وجود دليل مادي واضح

وكما قلنا مسبقاً فان الجرائم السيبرانية تكون ذات طابع افتراضي لا مادي، وهذا يجعل من الأدلة التي يمكن الحصول عليها ادلة غير مادية، وغير ملموسة، والدليل المادي يتميز بسهولة الحصول عليه، وصعوبة ازالته أو إزالة آثاره، كما يتميز بالاستقرار والثبات نوعا ما، وكل ذلك لا يوجد في الدليل المتحصل من الجرائم السيبرانية، وهذا ما يصعب الوصول الى الدليل في الوقت ذاته[2].

يلخص الباحث مما سبق أن مؤسسات الدولة تقوم كل في مجال اختصاصها بفرض النظام وسيادة القانون بواسطة أجهزتها الإدارية والقضائية من جهة، والتوعية الاجتماعية ومسؤولية المجتمع المدني في الحفاظ على الامن العام من جهة أخرى، ومن مؤسسات الدولة الهامة التي يقع على عاتقها عبء توفير الأمن: إدارة الشرطة التي تضطلع بمهمة حق الدولة في فرض قيود تحدّ بها من حريات الأفراد بقصد حماية النظام العام في مختلف مظاهره (الأمن العام والسكينة العامة والصحة العامة)، وفي سبيل ذلك تؤدي الشرطة عدة وظائف تضبطها القوانين أهمها الوظيفة الإدارية والقضائية والاجتماعية، متبعة في ذلك وسائل ردعية ووقائية، مثل أعمال الضبط القضائي الهادفة لتتبع المجرمين والكشف عنهم وإلقاء القبض عليهم لتقديمهم للعدالة التي تقتص منهم لغاية توفير الأمن للمواطنين، أو الضبط الإداري الذي يُنظّم شؤون الناس اليومية ويرسم حدود كل فرد وواجباته وذلك بواسطة (مثلا) شرطة المرور، والبناء، وحفظ الأمن العام،

1- لواء دكتور محمد فاروق كامل، القواعد الفنية للعمل الشرطي لمكافحة الجريمة، ط1،دار الكتاب الجامعي،2004، ص10.

2- د. صالح محمد امين، حدود اختصاصات الشرطة القضائية في مرحلة التحريات وجمع الاستلالات في القانون العراقي والمقارن، مجلة قوى الامن الداخلي، العدد5، 1984، ص 77.

إلى جانب الوظيفة الاجتماعية التي قوامها توعية المواطن بأهمية وضرورة الحفاظ على أمنه الخاص وأمن الجماعة بالتعاون الوثيق مع الشرطة، وتقديم يد المساعدة للمواطنين والتقرب من بعض مشاكلهم الاجتماعية بالخصوص، ذلك أن غياب وتراجع معدلات الجريمة بمختلف أشكالها يعبر عن حالة الامن العام، والعكس فإن تفشي الإجرام يعني حالة غياب الامن العام، فمعيار الأمن منوط بقدرة المؤسسات الحكومية والاجتماعية في من الحد من الجريمة والتصدي لها، وأن حماية الأفراد والجماعة من مسؤولية الدولة خلال فرض النظام وبسط سيادة القانون بواسطة الأجهزة الأمنية والقضائية، واستخدام القوة إذا تطلب المر ذلك ليتحقق الأمن والشعور بالعدالة التي تعزز الانتماء للدولة بصفتها الحامي الأمين لحياة الناس وممتلكاتهم وتوفير العيش الكريم لهم، لا شك أن لجهاز الشرطة عملا كبيرا وأساسيا في تحقيق الامن العام، أولا بأدائه الدور الكامل في خدمة الأمن العام بالتعاون مع مؤسسات الدولة الأخرى، وثانيا تقربه من المواطن وتعاونه معه لتجسيد هذا الأمن[1].

الفرع الثاني: التطور الذي ادخل على عمل وزارة الداخلية في مواجهة الجرائم

ان التطورات التي حصلت وانعكست على عمل جهاز الشرطة، والصعوبات التي طرحناها، دعت الى الحاجة لإيجاد سبل جديدة ومتطورة لمواجهة الجرائم السيبرانية، من خلال اتباع وسائل متطورة في عمل رجل الشرطة، تسهل له عملية تعقب الجرائم ومرتكبيها، في مثل هكذا نوع من الجرائم[2].

وان القوانين المتعلقة بقوى الأمن الداخلي كقانون عقوبات قوى الأمن الداخلي رقم (14) لسنة 2008 المعدل، وقانون أصول المحاكمات الجزائية لقوى الأمن الداخلي رقم (17) لسنة 2008، كان القصد منها تنظيم عمل مؤسسات قوى الأمن الداخلي بصورة تحقق السرعة في أداء الخدمة، والحفاظ على الضبط والربط بين صفوف الشرطة فهو متعلق بهذه الفئة دون غيرها، وذلك من خلال تنظيم أهم القواعد العامة المتعلقة بإجراءات المتنوعة التي يمارسها رجل الشرطة، ولكن بوصفه رجل شرطة، لا بوصفه عضو من اعضاء الضبط القضائي، اللذين يعدون بوصفهم هذا مساعدين لجهاز القضاء.

من هذا المنطلق كان لوزارة الداخلية عن طريق تشكيلاتها المختلفة دور بارز في التصدي للجرائم الالكترونية، ونهضت بالواجبات والمهام المناطة بها، ومن أهم التشكيلات المستحدثة في وزارة الداخلية والنشاطات التي تمارسها بما يلي:

1- د. نعيم مغبغب، مرجع سابق، ص 23.-

2- اللواء الدكتور اياد عبد الحمزة بعيوي، النقيب الحقوقي بلال عبد الرحمن المشهداني، السؤولية الجزائية المترتبة على جريمة الابتزاز الالكتروني، دراسة مقارنة، ط1، مكتبة القانون المقارن، بغداد، 2020، ص45.

اولا – دائرة العلاقات الاعلام[1]

تماشياً مع خطط وزارة الداخلية وتوجيهاتها في تطويق الجرائم السيبرانية، وتقديم مرتكبيها للقضاء، برز دور دائرة العلاقات والاعلام في هذه الوزارة، لتعزيز دور الوعي الأمني والتصدي للجريمة الالكترونية، عن طريق برامجها وانشطتها المتنوعة، فقد حرص الاعلام الأمني في وزارة الداخلية، شأنه شأن بقية تشكيلات الوزارة، على النهوض بالمهام والواجبات المناطة به، وتأدية دوره الفاعل في المجتمع كجزء من المنظومة الأمنية العراقية مع كل خطر يبرز في البلاد، وينتشر ليشمل مساحات واسعة.

ومع توسع الجرائم السيبرانية التي شخصت عن طريق القسام الرصد والاعلام الأمني، وسعب الاستبيان في الدائرة، التي اجرت مسحاً شاملاً للتعرف على الجرائم السيبرانية واضرارها على المجتمع، إذ تم الاطلاع على النتائج العملية والعلمية المشار اليها، فكان واجباً على عاتق هذه الدائرة بكونها معنية بالاعلام الأمني في الوزارة أن تضع الخطط والبرامج، وتنفيذ استراتيجية وقائية تعتمد التوعية والتثقيف هدفاً لها، من أجل المساهمة قدر المستطاع في درء خطر الجريمة، وقد نفذت دائرة العلاقات والاعلام جملة من الواجبات:

1 – قيام دائرة العلاقات والاعلام بالتنسيق مع قسم الشرطة المجتمعية في وكالة الوزارة لشؤون الشرطة، وبعد الاتفاق مع وزارة التربية التي أعطت تصريحاً الزيارة المؤسسات التربوية، وخاصة مدارس الفتيات في المراحل الإعدادية والمتوسطة والمعاهد والجامعات.

2 – تقوم هذه الدائرة من خلال فرقها الاعلامية بالتغطية المباشرة لانشطة دوائر الوزارة المختصة في موضوع الجرائم السيبرانية، عن طريق التنسيق مع وسائل الاعلام المختلفة، وهذا بحد ذاته يعد رادعاً مهما جداً لمرتكبي الجريمة، وكذلك عنصر تنبيه وتوعية للمواطنين من مخاطر هذه الجريمة.

3 – اطلاق دائرة العلاقات والاعلام في وزارة الداخلية حملة (ابنتنا تهمنا) وهي حملة الكترونية وميدانية، استهدفت تثقيف وتوعية الفتيات في اعمار المراهقة، من عمليات الابتزاز الالكتروني – على وجه الخصوص – وتوجيههن بالحذر من الانجرار وراء المبتزين عبر مواقع التواصل الاجتماعي.

4 – طبع الملصقات التوعوية والتثقيفية ونشرها في عدد من الطرق العامة، بالتعاون مع بعض منظمات المجتمع المدني، للتحذير من الوقوع ضحية للجرائم الالكترونية.

1- المادة(9/أولا-و) قانون وزارة الداخلية رقم(20) لسنة 2016.-

5 – القيام بلقاءات ميدانية واجراء سلسلة من اللقاءات مع السادة الوزراء المعنيين بملف الاتصال والانترنت والجرائم السيبرانية لخلق رؤى العمل المشترك للتقليل من نسبة الجرائم السيبرانية[1].

ثانيا – مديرية مكافحة الاجرام:

مديرية مكافحة الإجرام هي إحدى التشكيلات الحيوية المهمة والفعالة لوزارة الداخلية، تأسست عام 1972 إذ أطلق عليها في بداية تشكيلها تسمية (الشرطة السرية) وقد أنيط بها التحقيق في الجرائم الغامضة والمهمة آنذاك، بعد ذلك تم تغيير اسم التشكيل إلى مكافحة الإجرام) وفي عام 2013 ونتيجة للتطورات التي حدثت في البلاد على الصعيد السياسي والاقتصادي والاجتماعي والتي أدت بدورها إلى ازدياد معدل الجريمة وتطورها في المجتمع تطلبت الحاجة إلى وجود تشكيل متكامل وعلى درجة عالية من الجاهزية والكفاءة في قمع الجريمة وردعها[2]، تتمحور الأهداف الإستراتيجية التي تسعى المديرية الى مكافحة الجرائم السيبرانية، فجرائم التخريب والاتلاف وسرقة المعلومات، وجرائم الاعتداء على الحقوق الفكرية، والجرائم السيبرانية.... الخ جميعها ترتكب ويستحق فاعلها العقاب، سواء ارتكبها بطريقة تقليدية، أم بطريق الكتروني، لذا فان القاضي لا يستطيع رفض شكوى يتقدم بها شخص كان تعرض لجريمة الكترونية بحجة عدم وجود نص يحكمها، بل انه سينظرها وفق قواعد قانون العقوبات العام[3].

1- حسين بن سعيد الغافري، مرجع سابق، ص33.-

2- أصدرت وزارة الداخلية أمراً باستحداث مديرية مكافحة إجرام محافظة بغداد وتم المصادقة على الهيكل التنظيمي والقياس بموجب الأمر الاداري المرقم 13330 في 16/7/2013 والصادر من وكالة الوزارة للشؤون الادارية والمالية وتتكون من مقر المديرية وقسم الكرخ لمكافحة الاجرام وقسم الرصافة لمكافحة الاجرام ترتبط بها (10) مكاتب لكل قسم ومن ضمنها ايضا مكتبين لمكافحة سرقة السيارات في جانبي الكرخ والرصافة اضافة الى قسم مكافحة جرائم الاتجار بالبشر ومن ضمنها لجنتين في جانبي الكرخ والرصافة, أما مكاتب المكافحة في المحافظات فإن ارتباطها يكون فنياً فقط في الوقت الحاضر, وقد تم دعمها بضباط ومنتسبين لهم خبرة في عمل المكافحة والتحقيق والقبض على المجرمين, وفعلا تم القبض على العديد من العصابات الإجرامية الخطرة التي كانت تعيث فساداً في المجتمع. واستمر العمل باتجاه توسيع العمل بطاقات اضافية من خلال فتح مكاتب اكثر لتغطية عموم مفاصل محافظة بغداد والسيطرة على اكبر رقعة جغرافية ممكنة لتضييق الخناق على الجريمة ومرتكبيها فتم افتتاح (4) مكاتب اضافية لتكون في المحصلة الحالية (14) مكتب في جانب الكرخ و(12) مكتب في جانب الرصافة اضافة الى استحداث الوحدة التحقيقية الخاصة في مقر المديرية والتطلع الى فتح عدة مكاتب اضافية وحسب الاحتياج.

3- لواء د. اياد عبد الحمزة بعيوي، نقيب بلال عبد الرحمن محمود، مرجع سابق، ص 98.-

وقد أدت مديرية مكافحة الاجرام دوراً فعالاً في تقديم العون والمساعدة لجهاز القضاء للحد من تزايد الجرائم السيبرانية، والمساهمة في القبض على مرتكبيها، والاستدلال عن تلك الجرائم، والأدلة التي تقود الى مرتكب احدى تلك الجرائم.

ثالثا - قسم مكافحة الجرائم السيبرانية في وكالة الاستخبارات

في عام 2007 م تم استحداث قسم متخصص لمكافحة الجرائم السيبرانية (قسم مكافحة الجرائم السيبرانية) الذي يعد التشكيل الاختصاصي الأساسي في وزارة الداخلية، والذي يعمل بتماس مع القضاء العراقي في مكافحة الجرائم السيبرانية، وينفذ الأدوار المهمة والمعقدة بشقيها الفني والاستخباري، كونه يتعامل مع جرائم مستحدثة وفق إمكانيات تقنية، وبنى تحتية وتشريعية فقيرة في الدولة، تفتقر الى ادنى الخدمات بالإضافة الى تعامل كوادر الوكالة مع اخطر أنواع الجرائم السيبرانية، وهي الإرهاب 3 الالكتروني، ومحاربة التطرف، وبث الاشاعات الهادفة الى زعزعة الأمن والاستقرار».

فقد أدت دوراً فاعلاً في مكافحة الجرائم السيبرانية بمختلف اشكالها، ووفق القوانين والمعايير الدولية، وباستخدام الأساليب الفنية الحديثة قدر المستطاع، واستخلاص البيانات والمعلومات من شرائح الموبايل، وأجهزة الحاسوب، وذاكرة الهواتف العائدة للمتهمين بالجرائم، كما قامت بإجراء التدقيق الأمني لمنح الموافقات الأمنية لأصحاب الأبراج ومجهزي خدمة الانترنت، كذلك حجب الحسابات والصفحات على مواقع اتواصل الاجتماعي (فيسبوك - تويتر - انستكرام) والتي تعود للمجموعات الإرهابية والمروجة للجرائم المنظمة، وكذلك متابعة قضايا غسيل الأموال التي تتم من خلال الأجهزة الالكترونية، وغيرها الكثير من الاعمال المهمة التي مارستها هذه الشعبة المهمة من شعب وزارة الداخلية العراقية.

رابعا - مديرية الأمن السيبراني:

استحدثت وزارة الداخلية العراقية هذا المركز من اجل بناء فضاء سيبراني آمن وموثوق يعزز الثقة في التقنيات الرقمية لوزارة الداخلية ويحمي البيانات والمعلومات عالية الاهمية من التهديدات السيبرانية والامن السيبراني هو مجموعة الإجراءات والتقنيات والسياسات المستخدمة لحماية الفضاء السيبراني من التهديدات والاختراقات والحد من الهجمات الإلكترونية.

أ- منع الاطلاع او التعديل او الحذف او الاضافة الغير مصرح بها على البيانات.
ب- الحد من اساءة استخدام تكنلوجيا المعلومات والاتصالات.
ت- منع الاختراق وتسريب قواعد البيانات والكتب الرسمية وتعطيل الخدمات الالكترونية
ث- التأكد من عدم إساءة استخدام الصلاحيات في الانظمة الالكترونية.

وحسب الاستراتيجية الوطنية للامن السيبراني وبدعم من السيد وزير الداخلية المحترم تم تأسيس مركز الأمن السيبراني في وزارة الداخلية في 4/12/2022، يعد مركز الأمن السيبراني مركز أمني معلوماتي يعنى بمجالات الأمن السيبراني ويرتبط بمكتب معالي السيد الوزير يعمل المركز على تعزيز جهود وزارة الداخلية في بناء منظومة فعالة للأمن السيبراني ويهدف الى تطويرها وتنظيمها لحماية الوزارة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفعالية بما يضمن استدامة العمل والحفاظ على الأمن الوطني وسلامة بيانات ومعلومات المؤسسات والأفراد ومن مهام مركز الأمن السيبراني:

أ- وضع السياسات والاستراتيجيات الخاصة بالأمن السيبراني ومتابعة تنفيدها.
ب- ادارة حوادث وتهديدات الأمن السيبراني.
ت- الكشف عن الثغرات الامنية في التطبيقات والمواقع والأنظمة.
ث- الكشف عن نقاط الضعف في البنى التحتية للشبكات السلكية واللاسلكية
ج- تحليل مواقع الانترنت ومواقع التواصل الاجتماعي.
ح- تثقيف ونشر الوعي الأمني بين منسوبي قوى الامن الداخلي وباقي شرائح المجتمع.
خ- مراقبة وتحليل مراكز البيانات والمحطات الطرفية الخاصة

خامسا – قسم الاستجابة الأولية في مديرية الاتصالات والنظم المعلوماتية:

يقوم القسم بتامين الاتصالات اللاسلكية المشفرة بجميع مفاصل الوزارة والوزرات والدوائر الحكومية الأخرى عن طريق إدارة وتشغيل وصيانة منظومة الاستجابة الأولية التي تعمل بنظام التترا في بغداد والمحافظات وفقا للمواصفات القياسية ومراقبة عمل كافة مواقع المنظومة معيدات البث من خلال غرفة المراقبة الـ (CC) للتأكد من صلاحيتها للعمل وصيانة وتصليح المعدات الخاصة بالمنظومة وبالتنسيق مع الشركات المتعاقد معها لهذا الغرض وفتح الدورات لرفع الكفاءة الفنية للكادر العامل وإعداد الطلبات الخاصة بتامين المواد الاحتياطية وإدخال وإخراج الأجهزة العاملة على المنظومة بناءً على طلب يقدم من الجهة المستفيدة أو عند حصول

سوء استخدام للأجهزة ويرتبط بالقسم الشعب من ثمة: يقوم بتامين الاتصالات اللاسلكية المشفرة لجميع مفاصل الوزارة والوزرات والدوائر الحكومية الأخرى عن طريق إدارة وتشغيل وصيانة منظومة الاستجابة الأولية التي تعمل بنظام التترا في بغداد والمحافظات ومراقبة عمل كافة مواقع المنظومة.

واخيرا بهدف دعم العمل الأمني في مكافحة الجريمة بمختلف أشكالها، حصلت موافقة السيد القائد العام للقوات المسلحة على ما عرضه السيد وزير الداخلية لاستحداث مديرية مكافحة الجرائم الإلكترونية، وستعمل هذه المديرية المستحدثة على التحقيق في الجرائم التي تتم عن طريق مواقع التواصل الاجتماعي، وتأتي هذه الخطوة بدعم مباشر من قبل السيد القائد العام للقوات المسلحة وبإشراف السيد وزير الداخلية لمنع او الحد من هكذا جرائم إلكترونية.

لما تقدم يتضح ان لوزارة الداخلية دورا كبيراً في تحقيق الامن والاستقرار الداخلي والخارجي بما تتخذه من خطوات في التعامل مع احداث وتطورات مراحل الجريمة، سواء من محاولات منع وقوع الجرائم من خلال التدابير التأمينية اللازمة ان من خلال التدابير اللازم اتخاذها بعد وقوع الجريمة للإقلال حجم الخسائر الناتجة عنها، وكذلك يتمثل هذا الدور من خلال اتخاذ إجراءات امن المعلومات ومن خلال المديريات والاقسام ذات العلاقة لمواجهة تلك الجرائم المنظمة، وكذلك يتبلور دور جهاز الشرطة في عمليتي التفتيش والضبط لما يسفر هذا التفتيش من ادلة تفيد في اثبات وقوع الجريمة والتحقق من وقوعها، وصولاً الى الوقاية من الجرائم السيبرانية.

الخاتمة

بعد ان اتممنا دراسة بحثنا الموسوم التدابير الأمنية المضادة للجرائم السيبرانية» تبين لنا ان المجتمع المعلوماتي اصبح ومنذ اواخر القرن الماضي ومطلع القرن حقيقة واقعة لا تجريد وبعد ان تم استعراض موقف التشريعات في معظم الانظمة القانونية لمواجهة او التصدي لهذه الظاهرة الاجرامية الخطيرة المتمثلة بالجرائم السيبرانية، ذلك أن التغيرات التي طرأت على المجتمع الدولي في استعمال التقنيات التكنلوجية الحديثة في مجال الاتصالات وتقنية المعلومات كاستخدام الحاسوب والهواتف النقالة الذكية ومواقع التواصل الاجتماعي وغيرها من الوسائل الاتصال الحديثة عبر شبكات الاتصال وشبه المعلومات الدولية « الانترنت حتى أصبح العالم بفضلها قرية صغيرة لا تفصلها عن بعضه الحدود المعروفة بين الدول، ظهر نتيجة ذلك الإجرام المنظم الذي يصعب على أعضاء الضبط القضائي مكافحته وضبط مرتكبيه أو الحصول على أدلة كافية لإدانتهم لتقديمها إلى القضاء وتحقيق العدالة الجنائية إلا باتباع أساليب تحري خاصة، ومن بين أهم تلك الأساليب هو المراقبة بأجهزة إلكترونية خاصة بعد إذن قضائي أو رسمي وفق ضوابط محددة تغليبا للمصلحة الأجدر والأولى في الرعاية وهي حماية أمن المجتمع في مكافحة الإجرام المنظم وجرائم المعلوماتية وضبط مرتكبيها وإنزال العقاب المقرر لهم على مصلحة الأفراد في الحفاظ على مكنون أسرارهم وحقهم في سرية اتصالاتهم ومراسلاتهم الخاصة، وعليهم سنقسم الخاتمة الى مجموعة من الاستنتاجات والمقترحات على وفق الآتي:

أولا – الاستنتاجات

1) يهدف القانون الجنائي الى تحقيق ثلاث اهداف وهي حماية المصالح المعتبرة وتوفير الطمأنينة، وتحقيق العدالة، وفي حقيقة الامر فان الحكمة الماردة منها هي تحقيق الأمن، وهذا لا يتم الا من خلال منع أي ضرر أو خطر او تهديد مستقبلي للوجود الاجتماعي، ولتحقيق هذه الغائية كان لا بد من اشتمال القانون الجنائي على الوسائل التي تكفل تحقيق هذه الغائية، واهم وسيلة هي التدابير الوقائية التي تكفل منع الجريمة او الوقاية من ارتكابها مستقبلاً.

2) ان الجزاء الجنائي يرد في صورتين اما عقابا اوتدبير، ولكل منهما مجاله الخاص لتحقيق الفاعلية والموائمة في مواجهة الجريمة، ومن هنا انفرد التدبير في تحقيق مهمة المنع والوقاية، والتي يمكن ان ترد على معنى الاحتراز فقط، أي قصر التدبير على الحالة التي تظهر بها الخطورة على شكل جريمة، أو يرد بمعنى المنع والذي اقر بوجود حالات تثبت وجود الخطورة، حتى ولو يرتكب صاحبها الجريمة وهذه الخطورة عدت منبعاً للجريمة، والتي افترض المشرع خطورة الأشخاص المتصفين بأحد الحالات المحددة قانوناً، كما هو الحال في بعض ظواهر التشرد والاشتباه والانحراف عند فئة الاحداث.

3) الاهمية البالغة للتدابير الأمنية التي اولاها المشرع بنصوص جزائية تحمل بين ثناياها اشد العقوبات التي يمكن ان يتضمنها قانون جزائي، لما لهذه التحوطات والتدابير الأمنية من اثر بالغ في امن هذه المؤسسة ورصانتها وعدم تعرضها للخطر حتى ولو كان هذا الاعتداء بشكل معنوي من خلال تنشيط همة المقاتل في هذه المؤسسة، وان امن وسلامة وسيادة البلد لا تصان ولا تؤمن الا من خلال حماية مؤسساتها الأمنية الامنية ذات الطابع الأمني وجعلها قوية رصنة ضد اي اختراق وكما يقال الجيش سور للوطن.

4) بات واضحاً لنا مدى قصور التشريعات الجزائية ومنها قانون العقوبات بوضعه الحالي لا يكفي لمواجهة هذا النوع الجديد والخطير من الجرائم فهل يعني ذلك ان نقف مكتوفي الأيدي ازاء هذا الفراغ او النقص التشريعي ونترك بدون عقاب افعال اجرامية رغم خطورتها ام نخالف مبدأ الشرعية الجزائية والذي يقي بأن لا جريمة ولا عقوبة الا بنص ومن ثم نسمح للقضاء ان يتدخل لملئ هذا الفراغ التشريعي او سد ذلك النقص القائم، ام يسارع المشرع لسن التشريعات الجديدة او تعديل التشريعات القائمة حتى تلائم في تطبيقها ثورة الاتصالات المعلوماتية التي تحييها البشرية بالشكل الذي يجعلها كفيلة بوضع التدابير اللازمة لمواجهة الجرائم السيبرانية.

5) الجرائم السيبرانية الفعل الإجرامي الجديد الذي ظهر مع التطور التكنولوجي والطفرة النوعية الرقمية التي بات يعرفها الفضاء التواصلي المفتوح عبر الإنترنت، ومن ثم صار الحديث عن وجود فعل جُرمي مرتبط أساسا بهذه الثورة إذ تدفق المعلومات وإذ المعطيات الخاصة والعامة أضحت مُشرعة وفي متناول الجميع، ومن هنا يتحتم على أجهزة الشرطة مواجهة التحديث في ارتكاب هذه الجرائم المستجدة، والمنوعة.

6) بزوغ وسائل حديثة في ارتكاب الجرائم تختلف عن الوسائل التقليدية المعروفة، كبرنامج الفيروس والبرامج الشبيهة بالفيروس، فضلاً عن ظهور انماط حديثة في اساليب ارتكاب الجرائم مثل كسر كلمات السر وانتحال الشخصية وغيرها من الاساليب الاجرامية الحديثة، مع محدودية دور اجهزة الشرطة في مواجهة الجرائم الالكترونية وذلك لعدة اسباب أهمها القصور التشريعي في مواجهة تلك الجرائم، وعدم وجود كوادر أمنية مؤهلة لمواجهة هذه الانماط الاجرامية المستحدثة، وكذلك ضعف آليات الأجهزة الشرطية لمواجهة هذه الجرائم.

7) الجرائم السيبرانية هي ظاهرة خطيرة تخترق المجتمع وتهدد كيانه وتضرب في مقتل أهم أهداف المجتمع المتحضر في تحقيق الأمن والاستقرار وشعور المواطنين بالأمان في حياتهم، وهي من الجرائم المستحدثة التي تتم في عالم افتراضي ملئ بالشفرات والرموز.

ثانيا – المقترحات

1) اصدار تشريعات جديدة تتضمن تقرير الجرائم وتحديد العقوبات المناسبة لها بغية حماية النظام المعلوماتي، وايجاد ادلة اثبات جديدة مع طبيعة هذه الجرائم وذلك لعدم ملائمة ادلة الاثبات التقليدية في القانون الجنائي لا ثباتها، واعتماد الدقة والوضوح والحبكة القانونية عند تحديد انماط السلوك الاجرامي والابتعاد عن التعبيرات الغامضة او المطاطية التي تحمل أكثر من معنى او دلالة.

2) عدم الاقتصار عند التجريم والعقاب على انماط السلوك المحظور المرتكبة حالياً بل يجب مراعاة الابعاد المستقبلية لان تكنلوجيا المعلومات والحواسيب في تطور سريع بل يكاد يكون مذهل، وإعداد مشروع المراقبة مواقع التواصل الاجتماعي والانترنت بما يهدف لحماية أمن الدولة وسيادتها شريطة عدم الاعتداء على الحق في الخصوصية.

3) الأختيار الامثل والدقيق لعناصر أمن واستخبارات الوحدات والدوائر الأمنية لأنهم سيكونون المؤتمنين بالمقاوم الاول عليها وهم اول المسؤولين عن أي خرق الكتروني يمكن ان يطال هذه المؤسس.

4) سد الفراغ التشريعي في مجال الجرائم السيبرانية، على أن يكون شاملا للقواعد الموضوعية والإجرائية، وعلى وجه الخصوص النص صراحة على تجريم الدخول

غير المصرح به إلى الحاسب الآلي وشبكات الاتصال (الإنترنت) والبريد الإلكتروني، وكذلك اعتبار البرامج والمعلومات من الأموال المنقولة ذات القيمة، أي تحديد الطبيعة القانونية للانشطة الإجرامية التي تمارس على الحاسب الآلي والإنترنت، وأيضا الاعتراف بحجية للأدلة الرقمية وإعطاؤها حكم المحررات التي يقبل بها القانون كدليل إثبات.

5) ضرورة نشر الوعي المجتمعي بمخاطر الجرائم السيبرانية بتظافر جهود منظمات المجتمع المدني ووسائل الاعلام من خلال إقامة الحلقات النقاشية وورش العمل والندوات والمؤتمرات وخاصة للفئات المستهدفة للطلبة في المدارس والجامعات وكذلك لرجال الدين من خلال التعريف بالآثار السلبية لأنتهاك هذه الوسائل.

6) دعوة المشرع العراقي الى ضرورة التدخل بإصدار قانون مكافحة الجرائم المعلوماتية، بما لا يتعارض مع الحقوق والحريات المكفولة دستوريا في العراق، مع تضمينه نص يجيز للجهات المعنية القبض ومحاكمة مجرمي أنتهاك الحق في الخصوصية، وتوفير ضمانات لضحايا الجريمة محل البحث.

7) التنسيق وتوحيد الجهود بين الجهات المختلفة: التشريعية والقضائية والضبطية والفنية، وذلك من اجل سد منافذ جريمة الاعتداء على وسائل الاتصال السلكية واللاسلكية قدر المستطاع، والعمل على ضبطها واثباتها بالطرق القانونية والفنية.

8) التعاون الدولي من خلال مراقبة كل دولة للأعمال الاجرامية التخريبية الالكترونية الواقعة في أراضيها ضد دول أو جهات أخرى خارج هذه الأراضي.

9) تفعيل دور اجهزة الشرطة لمواجهة الجرائم السيبرانية من خلال التمييز بين مرحلتين مهمتين في التعامل مع تلك الجرائم هما:

أ- مرحلة ما قبل وقوع الجريمة (أمن المعلومات وذلك من خلال الخطوات الاتية:

1) اتباع القواعد التي تحكم أمن المعلومات من خلال تحديد المعلومات المهمة وتحليل المخاطر والتهديدات وتحليل القابلية للعدوان وتطبيق الإجراءات المضادة ومرحلة التقييم.

2) الاهتمام بوجود الآتي: انظمة الاستكشافات والاقتحام داخل المنشآت أو المؤسسات من خلال دوائر الحماية، وحدة الضبط جهاز الاشارة، وسيلة ارسال جهاز انذار إضاءة كافية.

3) الاهتمام بتطبيق انظمة للسيطرة على قواعد الدخول والخروج من خلال اتباع قواعد ضبط الدخول والخروج للأشخاص وتحديد الهوية بالرؤية والمعرفة الخاصة أو باستخدام الخصائص البيولوجية.
4) تطبيق نظم الدوائر التلفزيونية المغلقة من خلال الكاميرات وشاشات الرصد وأجهزة نقل الصور من خلال شبكات الألياف الضوئية والبلاستيكية.
5) استخدام الخصائص البيولوجية سواء عن طريق بصمة الإبهام أو حدقة العين أو بصمة الصوت، أو بصمة خط اليد في عملية التأمين.
6) اعداد برامج امن المعلومات من خلال تحديد أشخاص تتولى المسؤولية في إتمام ذلك.

ب- مرحلة ما بعد وقوع الجريمة، وهي المرحلة التي تعرف بأنها أزمة مما يتطلب التعامل مع الأمر بأسلوب إدارة الازمات من خلال ما يلي:

1) تكوين فريق لمواجهة الجرائم السيبرانية بداية من المدير ومشغل النظام والمراقب والمراجع والمحقق الجنائي والمستشار الفني وأفراد الحماية.
2) تحديد اختصاص كل عضو بالفريق، واتباع عناصر التدريب على مواجهة الجرائم السيبرانية.
3) تحديد اسلوب عمل فريق مواجهة الجرائم السيبرانية إذ يتواكب مع أسلوب عمل المنشأة مع عدم أهمال الأسس التي يجب على اي فريق اتباعها عند مواجهته للأزمة المعلوماتية، وهذه الاسس هي القدرة على تحقيق التنسيق والتكامل والترابط بين مختلف الانشطة التي يقوم عليها اعضاء الفريق الواحد، فضلاً عن القدرة على التنبؤ بالاحداث المستقبلية والمرونة في التنفيذ السريع لمواجهة الاحداث المتتابعة والسريعة والفجائية، وتوفير الامكانيات اللازمة لذلك.
4) تحديد واجبات فريق مواجهة الجرائم السيبرانية من خلال جمع الحقائق المتعلقة بالمؤسسة قبل البدء في وضع الخطة وإعداد السيناريوهات، وتقديم خطة عمل تفصيلية لمواجهة الجرائم الالكترونية.
5) تطوير عمل اجهزة الشرطة من خلال تكوين تشكيل مستقل لمواجهة الجرائم السيبرانية، والعمل على تدريبه وإكسابه الخبرة في التعامل مع هذه النوعية من الجرائم، فضلاً عن أهمية التنسيق ما بين الشركات التي تعتمد على أجهزة الحاسبات الآلية وبين أجهزة الشرطة مثل وجود وسيلة إنذار عند الأجهزة الأمنية للإخطار بوقوع اي جريمة من الجرائم الالكترونية.

6) نقترح على المشرع العراقي العراقي استحداث هذا النوع من أساليب التحري الخاصة في مواجهة الجرائم السيبرانية وتنظيم أحكامه بنصوص صريحة في قانون أصول المحاكمات الجزائية رقم 23 لسنة 1971 المعدل وعلى غرار العديد من القوانين الإجرائية الجزائية في الدول العربية كقانون الإجراءات الجنائية المصري ولتحقيق الموائمة بين حقوق الافراد وحرياتهم ومصلحة الدولة والمجتمع في مواجهة الجرائم الخطيرة.

المصادر

القران الكريم

أولا: المعاجم

1. الصحاح تاج اللغة وصحاح العربية، لإسماعيل بن حماد الجوهري، دار العلم للملايين ط، بدون سنة نشر.
2. محمد بن مكرم ابن منظور، (1995)، لسان العرب، المجلد الأول، دار بيروت االطباعة، بيروت.
3. محمد رواس قلعجي، (1988)، معجم لغة الفقهاء، الطبعة الثانية، دار النفائس للطباعة والنشر.
4. ابي الهلال العسكري،(2013)، معجم الفروق اللغوية، الطبعة السادسة، مؤسس النشر الإسلامي،مدينة قم.

ثانيا: الكتب

1. د. داليا عبد العزيز،(2017)،المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في النظام السعودي، دراسة مقارنة السعودية.
2. ماجد عمار،(1989)، المسؤولية القانونية الناشئة عن استخدام فيروس برنامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة.
3. عبد الرحمن جلهم حمزة، جرائم الانترنيت من منظور شرعي وقانوني، ظافر للتصميم والطباعة، بغداد، بلا سنة نشر.
4. عبد الفتاح بيومي حجازي،(2007)،الاثبات الجنائي في جرائم الكمبيوتر والانترنيت، دار الكتب القانونية، القاهره.
5. رامي متولي القاضي،(2011)، مكافحة الجرائم المعلوماتية،ط1، دار النهضة العربية، القاهرة.
6. رشدي، محمد السعيد، (2004)،الانترنيت والجوانب القانونية لنظم المعلومات، دار النهضة العربية، القاهرة.
7. هادي حامد قشقوش،(1992) جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضه العربيه
8. احمد حسام طه،(2000)، الجرائم الناشئة عن استخدام الحاسب الالي، الحماية الجنائية للحاسب الالي، دراسة مقارنة،القاهرة.
9. قايد اسامة،(1998)، الحماية الجنائية وينوك المعلومات، دار النهضة العربية،القاهره.
10. سردار علي عزيز،(2008) النطاق القانوني لإجراءات التحقيق الابتدائي، كلية القانون، جامعة السليمانية.

11. صالح بن محمد، المهيني المسند، عبد الرحمن بن راشد،(2015)، جرائم الحاسب الالي، الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، العدد29، الرياض.

12. محمد علي عريان،(2004)،الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية.

13. عادل عبد العال إبراهيم،(2013)، جرائم الاستغلال الجنسي للأطفال عبر شبكة الانترنيت وطرق مكافحتها في التشريعات الجنائية والمتهم الجنائي الإسلامي، جامعة الازهر، مصر.

14. خليفه بن علي بن محمد الزريق،(2015)، ابتزاز الاحداث وعقوبته في النظام السعودي، دراسة تاصيلية مقارنة تطبيقية، رسالة ماجستير جامعة نايف العربية للعلوم الأمنية، الرياض.

15. عبد العزيز بن حمين بن احمد الحمين،(1432هـ) الابتزاز ودور الرئاسة العامة لهيئة الامر بالمعروف، ندوة الابتزاز، مركز باحثات لدراسات المراة بالتعاون مع قسم الثقافة الإسلامية جامعة الملك سعود، الرياض.

16. د. احمد مختار عمر،(2008)، معجم اللغة العربية المعاصرة، المجلد الأول، ط2، عالم الكتاب.

17. د. يوسف عبد المنعم الأحول،(2016)، قانون الإجراءات الجنائية الفرنسي،ط1، دار النهضة العربية، القاهرة.

18. د. محمود نجيب حسني،(1988)، دروس في علم الاجرام وعلم العقاب، دار النهضه العربية، القاهرة.

19. د. يسر نور علي، ود. امال عثمان،(1977)، الوجيز في علم الاجرام والعقاب، دار النهضة العربية، القاهرة.

20. د. حاتم بكار،(1998)، حماية حق المتهم في محاكمة عادلة، مؤسسة المعارف للطباعة، الإسكندرية.

21. د. عبد الرزاق فخري الحديثي،(1992)، شرح قانون العقوبات القسم العام، مطبعة الزمان، بغداد.

22. د. غالب عبيد،(2010)، شرح قانون العقوبات العام،ط1،مطبعة جعفر العصامي، بغداد.

23. د. محمود سامي القرني،(1989)، النظرية العامة للتدابير الاحترازية، أطروحة دكتوراه، جامعة عين شمس، كلية الحقوق.

24. د. عبود السراج،(2005)، المبادئ العامة في قانون العقوبات لنظرية العقوبة، منشورات جامعة دمشق، مركز التعليم المفتوح.

25. د. علي حسين خلف ود. سلطان عبد القادر الشاوي، (2006)، المبادئ العامة في قانون العقوبات، دار العاتك، مصر، القاهرة.

26. حسن علي حسين علي،(2008)، الجزائي في قانون الإجراءات الجنائية، منشاة المعارف، الإسكندرية.

27. طه احمد متولي،(2008)، الدليل العلمي واثره في الاثبات الجنائي، مطابع الشرطة، القاهر.

28. حسين بن سعيد الغافري،(2009)، السياسة الجنائية في مواجهة جرائم الانترنيت، دار النهظة العربية، القاهرة.

29. سعيد محمد عبد الكريم الابراهيمي،(2000)، سلطات أعضاء الضبط القضائي في التحري وجمع الأدلة، كلية القانون.

30. مصطفى محمود موسى،(2001)، الجهاز الالكتروني لمكافحة الجريمة سلسلة اللواء الأمنية في مكافحة الجريمة الالكترونية، الجزء الأول.

31. لواء دكتور محمد فاروق كامل،(2004)، القواعد الفنية للعمل الشرطي لمكافحة الجريمة، ط1،دار الكتاب الجامعي.

32. د. صالح محمد امين،(1984)، حدود اختصاصات الشرطة القضائية في مرحلة التحريات وجمع الاستلالات في القانون العراقي والمقارن، مجلة قوى الامن الداخلي، العدد5،.

33. اللواء الدكتور اياد عبد الحمزة بعيوي، النقيب الحقوقي بلال عبد الرحمن المشهداني،(2020)، السؤولية الجزائية المترتبة على جريمة الابتزاز الالكتروني، دراسة مقارنة، ط1، مكتبة القانون المقارن، بغداد.

ثالثا: القوانين

1. قانون العقوبات العراقي رقم(111) لسنة 1969 المعدل.

2. قانون أصول المحاكمات الجزائية العراقي رقم(23) لسنة 1963.