مجلة مركز بابل للدراسات الإنسانية ٢٠٢٦ المجلد ١٦/ العدد ١

دور السياسة العقابية في مكافحة جرائم تقنية المعلومات

(دراسة مقارنه)

الباحث:زيد حميد صبار

مدرس القانون الجنائي المساعد

مقرر قسم علوم الادلة الجنائية (كلية السلام الجامعة)

البريد الإلكتروني Email : zaid.h.s.1995@gmail.com

الكلمات المفتاحية: السياسة العقابية، جرائم تقنية المعلومات، الأمن السيبراني، الحكومات، القانون المقارن، الردع الجنائي، الجرائم الإلكترونية.

كيفية اقتباس البحث

صبار ، زيد حميد، دور السياسة العقابية في مكافحة جرائم تقنية المعلومات (دراسة مقارنه)، مجلة مركز بابل للدراسات الانسانية، كانون الثاني ٢٠٢٦،المجلد:١٦ ،العدد:١ .

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

The Role of Penal Policy in Combating Information Technology Crimes (A Comparative Study)

Researcher:ZAID HAMEED SABBAR
Assistant Professor of Criminal Law
Department of Forensic Science\Al-Salam University College

Keywords: Penal policy, information technology crimes, cybersecurity, governments, comparative law, criminal deterrence, cybercrimes.

How To Cite This Article
SABBAR, ZAID HAMEED, The Role of Penal Policy in Combating Information Technology Crimes (A Comparative Study), Journal Of Babylon Center For Humanities Studies, January 2026,Volume:16,Issue1.

Abstract:

This study explores the role of penal policy in combating information technology crimes committed against governments, by analyzing both legislative and practical frameworks across various legal systems. It aims to assess the effectiveness of current sanctions in deterring cybercrimes that target state security, disrupt governmental operations, or breach official data. The study highlights legislative and procedural shortcomings in some countries and adopts a comparative approach, focusing on the legal frameworks in Iraq and Egypt, while drawing insights from modern international models. The findings indicate that existing penal policies require further development to keep pace with rapid technological advancements. There is a pressing need to adapt criminal penalties and modernize procedural mechanisms to ensure effective deterrence and adequate protection for government systems.

Since the dawn of humanity, people have sought to protect themselves from cybercrime, to avoid its dangers, or to mitigate the harm it may cause. They have utilized all their knowledge and ability to devise solutions, employing all their innovations in equipment, technology, and tools, and developing pre-existing plans to confront it. Information technology crimes fall within this framework, being the product of ignorant or erroneous actions, or malicious behavior intended to achieve illicit goals. These behaviors are new, brought about by modern information technology, which has evolved alongside the development of electronic equipment and digital software. They are addressed through preventative and protective measures, and sometimes through deterrent

measures by classifying them as criminal acts punishable by law. Numerous attempts have been made to define their various forms and explore how to confront them by applying existing laws established before the advent of information technology, without compromising the principle of legality in criminal law. Consequently, legislation has varied in its approach to dealing with cybercrime and in establishing a legal framework for it.

المستخلص:

تناولت هذه الدراسة دور السياسة العقابية في مكافحة جرائم تقنية المعلومات المرتكبة ضد الحكومات، وذلك من خلال تحليل الإطارين التشريعي والعملي في عدد من الأنظمة القانونية، بهدف تقييم مدى فاعلية العقوبات المقررة في ردع هذا النوع من الجرائم. وقد ركزت الدراسة على الجرائم السيبرانية التي تستهدف أمن الدولة، أو تسعى إلى تعطيل عمل مؤسساتها، أو اختراق بياناتها الرسمية، مع بيان مظاهر القصور التشريعي أو الإجرائي في بعض الدول. واعتمدت الدراسة المنهج المقارن من خلال استعراض التشريعات في القانون العراقي والمصري، إضافة إلى الاستفادة من بعض النماذج الدولية الحديثة. وتوصلت الدراسة إلى أن السياسة العقابية الحالية لا تزال بحاجة إلى تطوير في ضوء التحديات التقنية المتسارعة، مما يستلزم تكييف العقوبات وتحديث الإجراءات الجنائية بالشكل الذي يحقق الردع الفعّال ويوفر الحماية الكافية للأنظمة الحكومية.

سعى الإنسان منذ نشأته الى توقيها لتجنب مخاطرها، أو للتخفيف من مقدار الضرر التي قد تتأتى عنها، مستغلاً كل ما أتاه من علم وقدرة على استنباط الحلول، مسخراً كل ما ابتكره من معدات وتجهيزات وأدوات وما أعده من مخططات مسبقة لمواجهتها. فجرائم تقنية المعلومات لا تخرج عن هذا الإطار في كونها نتاج تصرّف جاهل أو خاطئ، أو سلوك آثم يبتغي منه مرتكبه تحقيق مآرب غير شرعية، فتلك السلوكيات هي سلوكيات مستجدة أتت بها تقنية المعلومات الحديثة والتي تطورت مع تطور التجهيزات الإلكترونية والبرمجيات الرقمية التي اعتمد عليها في تشغيلها ويتم التصدي لها من خلال اتخاذ تدابير احتياطية حمائية تارةً، وتارة أخرى بتدابير زاجرة عبر توصيفها كأفعال جرمية تستوجب العقاب على اقترافها. فتعددت المحاولات الى تحديد صورها المختلفة والبحث في كيفية مواجهتها من خلال تطبيق النصوص القائمة التي وضعت في وقت سابق على ظهور تقنية المعلومات دون الاخلال بمبدأ الشرعية الجنائية، فتباينت التشريعات في التعامل معها وفي خلق إطار قانوني لها.

المقدمة

إن التحديات التي أوجدتها التقنيات الحديثة لا تقتصر على المخاطر الماثلة في جرائمها المستجدة فقط، إنما أربكت المجتمع البشري بأفراده ودوله ومؤسساته الدولية والمحليَّة العامة

والخاصة على حد سواء، بحيث أضحوا محكومين في العيش في ظل عالمين مختلفين متباينين، أحدهما واقعي اعتادوا وتأقلموا مع مقوماته ومُكوّناته ومفاهيمه وأدبياته وعاداته وتقاليده، وآخر افتراضي مُستجد يختلفُ اختلافاً جوهرياً عن العالم الواقعي، من حيث مادياته ومقوماته ومفاهيمه وأدبياته ... الخ.

إذ لا مجال للاختيار بينهما بقبول أحدهما ورفض الآخر، لأنهما عالمان مختلفان، ولكنهما متكاملين، ينبغي التَّوفيق بين مقتضيات العيش في ظلهما مجتمعين، ومراعاة النواميس السائدة في كل منهما، بما في ذلك الالتزام إلى حد كبير، بمفاهيم وأدبيات وتقاليد كل منهما، وهذا ما يوجِبُ إعادة النظر في الكثير من المفاهيم والمرتكزات التي كان يتم التعامل معها كما لو أنها مُسلمات ممنوع المساس بها، أو حتى مخالفتها، أو توجيه النقد لها.

كل تلك المُستجدات التي حملتها التقنيات الحديثة، تسببت بارتباكات على امتداد المعمورة، بحيث أوجبت على الجميع إعارة الانتباه لما يدور في فلك الفضاء السيبراني، وما ينطوي خلفها من مخاطر من هنا كان تحرك الهيئات الدولية والإقليمية لشحذ الهمم لدى كافة الجهات المعنية من دول ومؤسسات خاصة وأفراد للتَّنبه لما يحيق بهم من مخاطر، وحثهم على المبادرة إلى اتخاذ خطوات ملموسة بحماية المُستهدفين، ومنعاً من تفشي الفوضى، ودفع أثمان باهظة نتيجة قصور وسائل وتدابير الحماية.

أيضاً كي لا يستغل الأشرار القصور التشريعي في هذا المضمار ضعف الإمكانيات الفنية والتقنية لدى الجهات المسؤولة عن توفير الحماية للمجتمع بكل مكوناته، أو إهمال المستهدفين لاستباحة المحرمات واقتراف أفظع الجرائم، وتعطيل عمل المؤسسات والأفراد، ومنع المعنيين من مزاولة أنشطتهم، وحرمان الكثيرين من تقديم الخدمات أو الاستحصال عليها.

فلم تكن استجابات الدول بالنسبة لتلك المخاطر والتحديات المستجدة على ذات المستوى، واختلفت الدول في تدخلاتها، منها من وقف موقف المتفرج متعامياً عما يحصل، ومنها من أقر بالواقع الجديد، وسعى إلى إجراء تعديلات على بعض نصوصه التشريعية، محاولاً التكيف مع التحول الذي أفرزته تقنية المعلومات بالحد الأدنى.

كما أنه منهم من عرف قدر تلك التحولات فسعى إلى إقرار قوانين خاصة للتعامل المستجدات التي ظهرت مع الفضاء السيبراني الواسع مع والسريع التحولات والعراق كدولة، وعى ما يحمله هذا الفضاء الافتراضي من مخاطر.

إلا أنه أصيب المعنيون في سلطتيه التشريعية والتنفيذية بشيء من الإرباك، نتيجة عدم إحاطتهم بأبعاد هذا الفضاء وميزاته، كما بالمفاهيم والمعايير السائدة فيه، وبالضوابط التي

تحكمه، والحيرة ما بين الخضوع لمفاهيمه ومعاييره وبين العمل على التخفيف من حالة الفلتان وانعدام المعايير فيه، من خلال اعتماد بعض الضوابط التشريعية والإجرائية، وإخضاع المتعاملين مع مكونات هذا الفضاء الاعتباري المجازي ومن يسوّق له، إلى بعض القيود التي من شأنها أن تحد من مخاطره.

أولاً: أهمية البحث

تظهر أهمية موضوع في الدور الذي تلعبه وسائل تقنيات المعلومات الحديثة في حياتنا اليومية، وتأثيره على مظاهر هذه الحياة في جميع مجالاتها، ومدى الحاجة لبحث ظاهرة جرائم هذه التقنية والعمل على خلق إطار قانوني لها، يقوم على تصنيفها وضبطها وخلق العقوبات الرادعة اللازمة لحماية البشر من تأثيرها وحماية النشاطات بكافة أنواعها، لا سيما التي تمارس من قبل البعض ضد حكومات الدول المختلفة.

ثانياً: منهج البحث

وبالنظر إلى طبيعة الموضوع محل البحث والمعلومات الواجب التوصل إليها، ومن أجل ما يرجى من أهداف، سيتم انتهاج كل من المنهج التحليلي والوصفي والمقارن، وذلك عن طريق تحليل النصوص القانونية الجزائية ذات الصلة، وتوصيفها وبيان الآراء الفقهية التي تعرضت لموضوع الدراسة، ولا سيما مقارنتها مع التشريعات الجزائية في بعض الدول العربية كالعراق ومصر والامارات ولبنان.

ثالثاً: مشكلة البحث

تكمن إشكالية البحث في طرح التساؤل الرئيسي التالي: ما مدى كفاية نصوص قوانين العقوبات القائمة في بعض الدول العربية لمواجهة جرائم تقنية المعلومات التي تمارس ضد الحكومات؟

رابعاً: هيكلية البحث

سنقوم في هذا البحث بالاعتماد على التقسيم الثنائي من خلال مطلبين حيث سنعالج في المطلب الأول مفهوم جريمة تقنية المعلومات الحديثة، اما في المطلب الثاني سوف نتطرق الى اطر الجهود المبذولة لدرء الاعتداءات المعلوماتية على الحكومات في التشريع العراقي

المطلب الأول

مفهوم جريمة تقنية المعلومات الحديثة

في بداية السبعينيات اهتم فقهاء القانون الجنائي بدراسة أولى جرائم تقنية المعلومات، كظاهرة فرضت نفسها على المجتمع، لما تنطوي عليه هذه الجرائم من مجموعة من السمات الخاصة حيث كان ارتباطها بالحاسب الآلي مميزاً لها عن غيرها من الجرائم الأخرى[١].

منذ ذلك التاريخ، وبسبب الظاهرة الحديثة نسبياً من جهة، وتطورها المتتالي من جهة أخرى، تباينت التعريفات التي استخدمت للدلالة عليها، واختلف الباحثون في تقسيم جرائم تقنية المعلومات والأفعال التي تدخل في إطار هذه الجرائم.

الفرع الأول

التعريف الضيق لجريمة تقنية المعلومات الحديثة

نظراً للصدى الكبير لثورة التكنلوجية التي عرفتها المجتمعات البشرية، فقد أدت إلى زعزعة الفهم التقليدي الذي ساد لفترة طويلة من الزمن، ولم تكن الجريمة محصنة ضد هذه التحولات، بل حاول المجرمون أن يتلاءموا مع الفهم الجديد[٢]، وابتدعوا أساليب ووسائل حديثة، تمكنت من تجاوز الاساليب التقليدية التي كانت معتادة لارتكاب الجرائم التقليدية، مما أدى إلى ظهور أنماط جديدة كجرائم تقنية المعلومات، وانتشار المجرمين المعلوماتيين وما يرتبط بهم من فيروسات وقرصنة وتزوير.

ذلك أن مفهوم جرائم تقنية المعلومات يحتاج إلى دراسة موضوعية، لحصر نطاقه وتحديد طبيعة هذه الجريمة وخصائصها التي تميزها عن غيرها من الجرائم الأخرى مع بسط نظامها القانوني في مصر وغيرها من الانظمة القانونية المقارنة[٣].

حظيت جرائم تقنية المعلومات باهتمام كبير من جانب الفقه الجنائي، الذي حدد لها تعاريف متعددة وانطلق في إطاره من زوايا مختلفة، فذهب اتجاه فقهي إلى الأخذ بتعريفات مضيقة لمفهوم جرائم تقنية المعلومات، بالنظر الى مدى ارتباطها بالحاسب الآلي، أو ارتباطها بموضوع الجريمة ذاتها أو بالنظر الى احدى الخصائص المميزة لتلك الجرائم، وهذا ما سنبينه وفقاً لما يلي:

أولاً: تعريف جرائم تقنية المعلومات من حيث ارتباطها بالحاسب:

حيث ذهب البعض في الاتجاه إلى تعريف جرائم تقنية المعلومات من منظور موحد، وهو مدى ارتباط الجرائم بالحاسب الآلي.

عرّفها الفقيه تيديمان بأنها: جميع أشكال السلوك غير القانوني أو الضار بالمجتمع التي يتم ارتكابها باستخدام الكمبيوتر.

ويعرّفها البعض على أنها: كل استخدام للكمبيوتر ونظامه من أجل الاستفادة من الخدمات التي يؤديها، دون أن يكون للمستخدم الحق في ذلك، ويلاحظ على هذا الاتجاه، عدم دقته، لأنه إذا كان من خصائص جرائم تقنية المعلومات[٤]، الا ان الحاسب الآلي ليس الجهاز الوحيد الذي يمكن من خلاله ارتكاب جرائم تقنية المعلومات، إذ يمكن ارتكاب تلك النوعية من الجرائم من

خلال أجهزة أخرى كالهاتف العادي أو الهاتف الجوال أو غيرها من الأجهزة الأُخرى التي يتفتق عنها ابتداع الآخرين .

ثانياً: تعريف جرائم تقنية المعلومات من حيث ارتباطها بموضوع الجريمة:

حيث يرى مناصري هذا الاتجاه، أنه ليست جرائم تقنية المعلومات هي أداة ارتكاب نظام المعلومات، بل تلك التي تقع على النظام أو ضمن نطاقه، ومن أنصار ذلك التعريف روزن بلاك وآخرين، يرون أن جرائم تقنية المعلومات هي: على انها نشاط غير مشروع، موجه لنسخ أو اجراء أي تحويل أو استقصاء أو الوصول للمعلومات المخزنة داخل النظام أو التي تحول عن طريقه ويندرج هذا النوع تحت جرائم المعالجة الآلية للبيانات[٥].

وفي إطار التعريفات المتقدمة، يتضح أن جرائم تقنية المعلومات، إما أن تقع على جهاز الحاسب ذاته بمكوناته المادية أو المنطقية، وإما أن تقع بواسطة الحاسب، وبالتالي يكون الحاسب مجرد وسيلة لاقترافها، وبالتالي سنميز بين حالات ثلاث فيما يأتي:

١- وقوع الجريمة على المكونات الملموسة للحاسب:

تتحقق هذه الحالة إذا كانت أجهزة الكمبيوتر ومكوناته المادية، بما في ذلك الأجهزة والمعدات والكابلات والشبكات المترابطة وآلات الطباعة والأشرطة الخام، التي يتم تسجيل البرامج والبيانات عليها، موضوعاً أو محلاً لهذه الجريمة[٦]، وبالتالي لا تثير هذه الحالات مشكلة، باعتبار هذه المكونات الملموسة محل وقوع اعتداء تتمتع بالحماية الجنائية للنصوص التقليدية المستخدمة، باعتبارها من الأموال المنقولة التي تخضع سرقتها وإتلافها للنصوص الجنائية التقليدية، وبالتالي فإن الأمر هنا لا يثير أي مشكلة تجاه تطبيق النصوص التقليدية على هذه الأموال .

٢- وقوع الجريمة على المكونات المنطقية غير المادية للحاسب:

إن تطبيق تحقق وقوع هذه الفرضية عندما تكون مكونات الجاهز الالكتروني المعلوماتي غير مادية مثل البرامج المستخدمة والبيانات والمعطيات في وسائط التخزين في الحاسب، محلاً أو موضوعاً للجريمة حيث من المتصور عملاً أن يقوم أحد الاشخاص بالاعتداء على برنامج الحاسب أو أن يدعي ملكيته أو يقوم بسرقته أو يقلده أو يتلفه أو يعطله، أو يقوم بإفشاء محتوياته، أما البيانات أو بنك معلوماته فيستطيع العبث بها، كتحريفها أو تزويرها أو نسخها.

ونظراً للطبيعة الخاصة التي تميز هذه المكونات، فإن النصوص التقليدية الحالية لقانون العقوبات، عاجزة عن مواجهة الجرائم التي قد تقع ضدها بسبب حداثتها النسبية، ولكون

النصوص الحالية تعجز عن تغطية الحالات الجديدة الطارئة، ولأن القانون الجنائي نفسه يعاني من فراغ تشريعي في المجال المعلوماتي[٧].

٣- حالة استخدام الحاسب كأداة لارتكاب الجريمة:

في هذه الحالة، لا يكون الكمبيوتر موضوع هذه الجريمة أو محلها، وبالتالي فهو ليس موضوع حماية جنائية، ولكن الجريمة في هذه الحالة تحدث من خلاله، أي يتم استخدامه كأداة لارتكابها، ومن الناحية النظرية، يمكن أن تقع بعض الجرائم بواسطة الحاسب مثل بعض أنواع الجرائم التي تقع على الذمة المالية من سرقة واحتيال وإساءة الأمانة والتزوير بأنواعه كافة وانتهاك لحرمة الحياة الشخصية، بل وتستخدم في بعض أنواع جرائم القتل وذلك بواسطة طرق عدة منها برمجة جهاز الكتروني ومن ثم تفجيره فيتم التحكم به آلياً أو جهاز لإطلاق الأشعة القاتلة[٨] .

ثالثاً: تعريف جرائم تقنية المعلومات بالنظر إلى إحدى خصائصها:

نظراً لما تتمتع به هذه الجرائم من خصائص وسمات تميزها عن الجرائم التقليدية[٩]، وتتعدد تلك الخصائص في جرائم تقنية المعلومات، وبالتبعية فإن أصحاب هذا الإتجاه يتجهون إلى تعريف جرائم تقنية المعلومات بالنظر لما تتميز به تلك الجرائم من خصائص.

هناك العديد من التعريفات التي يستخدمها الباحثون في هذا المجال، ويعتقد ديفيد تومبسون أنها: جريمة تتطلب أن يكون مرتكب الجريمة على علم بنظام المعلومات الإلكترونية لارتكابها.

١-التعريفات الفقهية:

ومن الاتجاهات الفقهية التي تبنّت التعريف الضيق، ذهب الفقيه ماروي أيضاً إلى أن جرائم تقنية المعلومات هي الفعل غير المشروع، الذي يتورط فيه الحاسوب، أو أنه الفعل الإجرامي الذي يستخدم الحاسوب كأداة رئيسية، أو هو الفعل الاجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية[١٠].

وفقاً لهذا التعريف، يجب أن تكون هناك معرفة كبيرة بتقنيات الحاسوب، ليس فقط لارتكاب الجريمة، ولكن أيضاً لملاحقتها والتحقيق فيها، وهذا التعريف يضيق بدرجة كبيرة من جرائم تقنية المعلومات [١١].

ويعرف جانب من الفقه جريمة تكنولوجيا المعلومات الحديثة على أساس سمات شخصية لدى مرتكب الفعل، وهي تحديداً سمة الدراية والمعرفة التقنية[١٢].

٢-تقييم التعريفات السابقة:

وبحسب التعريفات السابقة فإن جريمة تقنية المعلومات الحديثة، تنحصر في القضايا التي تتطلب درجة من المعرفة الفنية في ارتكابها، والتي إذا تحققت في بعض الحالات فإنها لا تتحقق في كثير منها، ففي كثير من الحالات يرتكب الفعل دون الحاجة إلى هذا القدر من المعرفة[١٣]، فالكثير من جرائم تقنية المعلومات الحديثة، ترتكب من قبل جماعة تتوزع أدوارها، بين التخطيط والتنفيذ والتحريض والمساهمة، وبعضهم قد لا يكون لديه معرفة بتقنية المعلومات، ثم ما هي حدود المعرفة التقنية، وما هو معيار وجودها للقول بقيام الجريمة، خاصة في ظل التطور الذي شهدته وسائل التقنية الحديثة من تبسيط وسائل المعالجة وتبادل المعطيات، وتحويل الأجهزة المعقدة فيما سبق إلى أجهزة تكاملية سهلة الإستخدام، حتى ممن لا يعرف شيئاً من علوم التقنية الحديثة .

بالإضافة إلى ذلك، يُنسب جانب مهم من جرائم التكنولوجيا الحديثة إلى الشخص الاعتباري، في حين أن شرط المعرفة التقنية هو شرط شخصي يتعلق بالفاعل، خاصة وأن أحد القضايا الرئيسية التي تثيرها جرائم التكنولوجيا الحديثة هي موضوع المسؤولية للشخص الاعتباري، شأنه شأن الشخص الطبيعي عن الأفعال المعتبرة جرائم تقنية حديثة[١٤].

ويلاحظ على هذا التعريف أنه يتطلب أن يكون الفعل مما يقع ضمن نطاق قانون العقوبات، وفي هذا افتراض مسبق لأنماط السلوك الجرمي في جرائم تكنولوجيا المعلومات الحديثة، وهي مسألة لا تراعي الجدل الذي لم ينته بعد حول مدى انطباق قواعد التجريم التقليدية على هذه الأفعال، والذي حسم تقريباً لجهة عدم انطباق نصوص القانون القائمة والحاجة إلى نصوص خاصة تراعي العناصر المميزة لهذه الجرائم عن غيرها من الجرائم التي عرّفها قانون العقوبات [١٥].

الفرع الثاني

صور جرائم تقنية المعلومات الحديثة ضد الحكومة

لم يقتصر أثر تقنية المعلومات الحديثة وانتشار وسائطها والتوسع في مجال استخدامها على تحول الإنسان فحسب إلى هدف لذوي النزعة الإجرامية، بل امتد أثر الاستخدام الإجرامي لها ليطال الحكومات أو بالأحرى المصلحة العامة بوجه عام.

أي تلك الحقوق التي ليست الفرد أو أفراد معينين بذواتهم وإنما هي للمجتمع في مجموع أفراده أو الحكومة باعتبارها الشخص القانوني الذي يمثل المجتمع في حقوقه ومصالحه كافة[١٦]، في ظل ما شهدته الحكومات في غالبية دول العالم من تحول إلى حكومات إلكترونية، بحيث أصبح من الممكن اختراق نظمها الإلكترونية وشبكاتها واستخدامها في التجسس والنيل من أمن

الدولة بتدمير البنية التحتية المعلوماتية التي تعتمد عليها الحكومات، وتهديد السلامة العامة وترويع المواطنين.

الفقرة الأولى

جرائم إعاقة وتحريف وتعطيل نظم المعلومات الإلكترونية الحكومية.

يقصد بنظام المعلومات الإلكتروني، مجموعة برامج وأدوات تستخدم في معالجة وإدارة البيانات والمعلومات الإلكترونية، أي كل نظام متكامل لجمع المعلومات وتصنيفها ومعالجتها وحفظها واسترجاعها ونقلها عبر الوسيط الإلكتروني[١٧]، وينبغي ألا يُفهم بأن المقصود بنظام المعلومات الإلكتروني هو جهاز الحاسب الآلي فحسب[١٨]، لأن قصر نطاق النظام الإلكتروني على الحاسبات الألية يُعد خطأ من الناحية التقنية وقصوراً في التعريف من الناحية القانونية.

لذلك الأمر سوف نتناول هنا جرائم إعاقة أو تحريف تشغيل نظم المعلومات الإلكترونية الحكومية ومن ثم سنتحدث عن جرائم تعطيل شبكات نظم المعلومات الإلكترونية الحكومية.

أولاً: جرائم إعاقة أو تحريف تشغيل نظم المعلومات الإلكترونية الحكومية.

يقصد بجرائم إعاقة أو تحريف تشعيل نظم المعالجة الآلية للبيانات والتلاعب في بياناتها، نمط السلوك الجرمي الذي يُرتكب بواسطة تقنية المعلومات الحديثة ويستهدف إعاقة أو تحريف تشغيل تلك النظم بغية تعطيلها أي منع وإفساد وظيفتها وما أعدت له، والتلاعب في بياناتها.

١-الركن المادي لجريمة إعاقة أو تحريف تشغيل نظم المعلومات الإلكترونية الحكومية.

ينصرف السلوك الإجرامي في هذه الجريمة إلى كل عمل من شأنه إرباك عمل نظام معالجة البيانات ويستوي أن يكون من شأن نشاط الجاني إعاقة أو إفساد نظام التشغيل في الإرسال، ويستوي أن يؤدي نشاط الجاني إلى توقف النظام عن العمل بصورة دائمة أو مؤقتة، ولا يشترط أن تكون الإعاقة أو الإفساد بصورة كلية، بل يمكن أن يؤدي النشاط إلى إعاقة أو إفساد جزئي للنظام [١٩].

تتفق جميع التشريعات التي حرّمت إعاقة أو تحريف تشغيل نظم المعالجة الآلية للبيانات في تحديد الأفعال التي تقوم بها هذه الجريمة مع اختلافات طفيفة فيما بينها تتعلق بالمفردات المستخدمة.

حيث نصت المادتين ١٧٧ و١٧٨ – (المقترح إضافتهم على الباب الحادي عشر من الكتاب الثاني من قانون العقوبات بموجب اقتراح القانون الذي تقدمت به لجنة تكنولوجيا المعلومات في مجلس النواب اللبناني) – على جريمة إعاقة أنظمة المعلومات، فنصت المادة ١٧٧ على معاقبة

الوصول (الدخول) أو (المكوث) في نظام معلومات بكامله أو في جزء منه، وتشديد العقوبة إذا نتج عنه المساس بعمل نظام المعلومات، وعاقبت المادة ١٧٨ كل من يقدم بنيّة الغش وبأي وسيلة على إعاقة عمل نظام معلومات أو على إفساده.

٢-الركن المعنوي.

ويتمثل الركن المعنوي الحالة الذهنية والعقلية لمرتكب الفعل الجرمي أي تواجد سوء نية و إرادة غير مقيدة و واعية للدخول في الشبكة وإحداث الضرر أو الولوج بهدف السرقة وتخريب البيانات وغيرها من الجرائم كالاعتداء على المعلومات المتعلقة بالمنظمات الحكومية أو الخاصة المملوكة للأفراد بهدف إتلافها كلياً أو جزئياً أو الانقاص من منفعتها مما يؤدي إلى إلحاق الضرر بمالكي المعلومات وتعد من الجرائم المتعمدة في حالة تواجد عنصر المعرفة بملكيتها للغير و عنصر الإرادة في تدميرها ماله الأثر السلبي في تنفيذ أنشطة المنظمة بشكل محدود أو بشكل كامل[٢٠] ، ويقسم الركن المعنوي إلى محورين هما[٢١]:

١. الإعتداء على نظام تشغيل وذلك بخلق مشكلة تؤدي إلى تباطؤ النظام في تنفيذ العمليات المطلوبة مثل معالجة المعلومات واسترجاعها وإرسالها ما يكون له الأثر السلبي على أداء المنظمة .

٢. الدخول غير المرخص إلى أنظمة المرور الإلكترونية ويتم في هذه الحالة تدمير البيانات والمعلومات كلياً والموجودة في النظام أو التعديل أو التشويه للبيانات والمعلومات مما يشكل عائقاً أمام المنظمة للاستمرار في تنفيذ عملياتها أو الحد من اتخاذ القرارات السليمة [٢٢].

فالجرائم الالكترونية هي من جرائم التقنية العالية تتطلب من المجرم الالكتروني قدراً من المعرفة والتخصص، فكان من المتصور غالباً وقوعها في صورة واحدة هي صورة العمد، على اعتبار أن الجاني خطط ودبر لارتكاب جريمته من أجل الحصول على المعلومات أو لاختراق شبكة الحاسوب، أو الاعتداء على أنظمة المعالجة الآلية للمعطيات سواءً بالإدخال أو المحو أو التعديل [٢٣].

ولهذا نجد إن المشرع العراقي في مشروع قانون الجرائم الالكترونية لسنة ٢٠١١م قد إشترط في المادة(٣/أولاً) الاستخدام العمد والقصد الجنائي حيث عاقبت المادة المذكورة : كل من استخدم عمداً أجهزة الحاسوب وشبكة المعلومات بقصد ارتكاب إحدى الأفعال الآتية... [٢٤]، وهذا يعني وجوب توافر القصد الجنائي لكل عمل تقوم به المسؤولية الجنائية فمن يدخل إلى موقع أو نظام أو يلغي أو يحذف بيانات أو معلومات أو يفشي أسرارها يجب أن يكون عالماً ومريداً لسلوكه والنتائج التي تترتب على ذلك السلوك مما يجعله خاضعاً للمسؤولية الجنائية أما إذا كان فعله

نتيجة خطأ فلا تقوم عليه المسؤولية[٢٥]، ما لم ينص القانون على خلاف ذلك، وبمقارنة سلوك الجاني في الحالات السابقة لوجدناه متطابقاً بذلك فإن جريمة الدخول غير المشروع وجريمة العبث بالنظام أو بالبيانات وجريمة التنصت على النظام وجريمة الإستيلاء على أموال الغير تعتبر جرائم عمدية يتطلب القانون علم الجاني بعناصرها و إرادة متجهة إلى هذه العناصر.

ثانياً: جرائم تعطيل شبكات نظم المعلومات الإلكترونية الحكومية.

إن شبكات نظم المعلومات الإلكترونية الحكومية ومكوناتها المنطقية ومواقعها باتت عرضة للتعطيل والتدمير باستعمال الشبكة الإلكترونية أو إحدى وسائل تقنية المعلومات الحديثة وكذلك الحال بالنسبة للمواقع الإلكترونية الحكومية، بحيث أن تعطيل هذه الشبكات الموزعة على المنشأت والمصالح الحكومية يؤدي إلى شل حركة العمل وتوقف خدمات تطبيقاتها المتعلقة بأنظمة البنية التحتية وإلحاق الضرر بالقطاعات المختلفة العسكرية والأمنية وقطاع المواصلات وقطاع الإتصالات وقطاع الطاقة والمياه وقطاع المال والبنوك.

وذهب القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها الصادر عن الجامعة العربية بالرقم ٤١٧ لسنة ٢٠٠٤ إلى تجريم أفعال إعاقة أو تشويش أو التعطيل العمد وبأية وسيلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات[٢٦]، أما في التشريع العراقي فلا يوجد في نصوص القانون ما يجرم هذه الأفعال بالنسبة للجرائم الإلكترونية الواقعة على نظم المعلومات الإلكترونية الحكومية.

ومما سبق سوف نقوم بالحديث عن جريمة إعاقة الوصول إلى الشبكات وتعطيلها ومن ثم إتلاف المكونات المنطقية لنظم المعلومات الإلكترونية وشبكاتها.

١-إعاقة الوصول إلى الشبكات وتعطيلها

من المتصور أن تتعرض البنية التحتية للشبكات، الإلكترونية الحكومية لهجمات إلكترونية بقصد تدميرها وتوقفها عن العمل، مما يؤدي إلى توقف الحكومات الإلكترونية عن عملها وبالتالي توقف القطاعات والمرافق الحيوية عن العمل، مما يهدد السلامة العامة ويُحدث أثاراً مادية وأمنية واقتصادية خطيرة[٢٧].

أما المقصود بعرقلة الخدمة أو إعاقة الوصول إلى الشبكة، حصول انقطاع في خدمة الاتصال – بالشبكات – أو بالخدمات التي تقدم إلى المستفيدين داخل الشبكة وتعدد الوسائل التي قد تتسبب في هذا الخطر من ذلك إرسال حزم وهمية تملأ مساحات الذاكرة الوسيطة

وتخريب معلومات تجزئة الرسائل بحيث إذا حاول النظام المستقل إعادة تركيبها عند الوصول فإن هذه المحاولة تتسبب في تخريب النظام[٢٨].

ويتم تعطيل الشبكة بالدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالشبكة من خلال نظام أو مجموعة نُظم مترابطة شبكياً، بحيث يتم تخريبي نقطة الاتصال[٢٩]، والحقيقة أن الشبكات وما عليها من بيانات ومعلومات مخزنة عن طريق أجهزة وتوصيلات، وغيرها وببرامج محملة على هذه الأجهزة تتعرض للهجوم عليها من أشخاص شتى أياً كان نوع هذه الشبكة، ويتم عن طريق تقنية المعلومات الحديثة[٣٠].

٢-إتلاف المكونات المنطقية لنظم المعلومات الإلكترونية وشبكاتها

لم يتعرض المشرع اللبناني بأي نص في قانون العقوبات بخصوص جريمة إتلاف المكونات المنطقية لنظم المعلومات الإلكترونية وشبكاتها، وإنما جرّم إتلاف المنقولات في المادة ٧٣٣ من الفصل الثامن (الأضرار الملحقة بأملاك الدولة والأفراد) من الباب الحادي عشر (الجرائم التي تقع على الأموال) من قانون العقوبات اللبناني[٣١].

الفقرة الثانية

جرائم التجسس الإلكتروني ضد الحكومة

التجسس ظاهرة تعود في تاريخها إلى العصور القديمة، ترافق مع تطور الحياة وتطور مع تطور العلم والتكنولوجيا، فمنذ فجر التاريخ كانت المعلومات التي تملكها الأطراف عن بعضها البعض من أهم العوامل التي تقرر مصيرها ورجحان، قواها وازدادت أهمية المعلومات أكثر فأكثر مع بلوغ العصر الرقمي حيث أصبحت قوة جديدة في حياة الشعوب وإدارة الدولة والحكم، وباتت السيطرة على مخازن المعلومات ووسائل معالجتها أكثر أهمية من الموارد الطبيعية كمصدر للقوة الاقتصادية والصناعية والعسكرية[٣٢].

أولاً: مفهوم جريمة التجسس الإلكتروني وأساسها

أتسع مفهوم التجسس المعلوماتي ليشمل أغلب الأفعال التي تمس مؤسسات الدولة والشركات والمنظمات والحياة الخاصة .... الخ، وتمثلت هذه الأفعال بالدخول غير المشروع أو اعتراض المعلومات، أو التنصت عليها أو الالتقاط لها، وأن الغرض من الدخول للنظام المعلوماتي انتهاك سرية البيانات سواء كانت سياسية أو اقتصادية ... الخ[٣٣].

١-تعريف جريمة التجسس الإلكتروني

قانوناً نجد إن التشريع العراقي قد تناول جريمة التجسس بصورتها التقليدية، إلا أنه لم يعرف التجسس، بل اكتفى بتحديد الافعال التي يعتبر مرتكبها جاسوساً، وذلك بالنص عليها في

قانون العقوبات العراقي رقم لسنة ١٩٦٩[٣٤]، والذي لم يطلق عليها لفظ التجسس من الجدير بالذكر لم يحدد المشرع العراقي الوسيلة المستخدمة للحصول على المعلومات المحظورة ونشرها أو إذاعتها[٣٥]، أما في لبنان فإن المشرع لم يضع تعريفاً عاماً له ولكنه جرّمه في قانون العقوبات رقم ٣٤٠ لعام ١٩٤٣ في المواد (٢٨١-٢٨٢-٢٨٣).

من ثم يمكن أن يكون الحصول على المعلومات السرية بطريقة الكترونية أما مشروع قانون الجرائم المعلوماتية العراقي لعام ٢٠١٢ فكذلك لم يتضمن تعريفاً للتجسس المعلوماتي والذي تناول تجريم صور التجسس المعلوماتي كالدخول أو البقاء غير المشروع جريمة الاعتراض غير المشروع جريمة تهديد أمن الدولة جريمة الاعتداء على سلامة البيانات جرائم الاعتداء على حرمة الحياة الخاصة إفشاء معلومات أو أسرار المشتركين[٣٦].

أما فقهاً يعرّف التجسس المعلوماتي بأنه: استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الالكترونية الخاصة بالدولة والحكومات والتنصت عليها، بقصد الاستحصال على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها وتشمل جميع أنواع المعلومات العسكرية والسياسية والأمنية والاقتصادية والعلمية والاجتماعية[٣٧].

٢-أساس جريمة التجسس الإلكترونية

على المستوى الدولي نجد بأن اتفاقية لاهاي الرابعة لعام ١٩٠٧ قد عرّفت الجاسوس بأنه الشخص الذي يعمل بالخفاء أو تحت ستار كاذب لجمع المعلومات أو محاولة ذلك في منطقة العمليات الحربية، بغية إيصالها للدولة المعادية الأخرى.

من الجدير بالذكر أن اتفاقية لاهاي قد حصرت معنى الجاسوس على الأجنبي دون الوطني وذلك لخضوع المواطن للقانون الوطني، كما تنطبق أحكامها على التجسس في منطقة العمليات الحربية للأطراف المتنازعة، وهو ما لا يدع مجالاً لتطبيق الإتفاقية على التجسس الذي يتم في حالة السلم[٣٨].

أما على الصعيد الوطني العراقي فنجد بأنه قد جرّم أفعال التجسس التقليدية وذلك في المادة ٣٢٨، حيث عاقبت الموظف أو المكلف بخدمة عامة الذي يعتدي على حرمة الحياة الخاصة، وكما أنه في إطار الحياة الخاصة نجد بأن المادة ٤٣٨ من قانون العقوبات العراقي قد جرّمت أفعال النشر للصور أو الأخبار أو التعليقات التي تمس الحياة الخاصة، حتى وإن كانت صحيحة إذا كان من شأن ذلك الإساءة لصاحب الشأن، أما في التشريع اللبناني فنجد بأن المشرع قد جرّم التجسس بصورته العامة في المواد ٢٨١ و ٢٨٢ و ٢٨٣.

ثانياً: طبيعة جريمة التجسس الإلكتروني

لمعرفة طبيعة جريمة التجسس الإلكتروني فسوف نقوم بالبحث في جريمة التجسس على أنها جريمة سياسية، ومن ثم سنقوم بالبحث في اعتبار جريمة التجسس الإلكتروني على أنها جريمة أمن دولة خارجي، ومن ثم سنبحث في نطاق جريمة التجسس.

١-طبيعة جريمة التجسس الإلكتروني.

أ-جريمة التجسس الإلكتروني جريمة سياسية

تناولت عدة مذاهب مفهوم الجريمة السياسية ومنها المذهب الشخصي الذي يعد من أول المذاهب التي جاءت لتحديد مفهوم الجريمة السياسية، واعتمد في ذلك على الباعث أو القصد في ارتكاب الجريمة أي الغرض الذي يريد مرتكب الجريمة الوصول اليه دون التقيد بموضوع الجريمة أو طبيعة الحق المعتدى عليه[٣٩].

وتعد جريمة التجسس من الجرائم الجنائية التي تهدد أمن الدولة الخارجي حيث يكون في الواقعة المكونة للجريمة مساس بأمن الدولة الخارجي لا بشخص من الأشخاص، ولخطورة جريمة التجسس في زمن الحرب وما بعدها دفع فقهاء القانون الجنائي إلى نزع الصفة السياسية عنها، وجعل الدول تعامل مع مرتكبيها بالقسوة وفرض عقوبة الإعدام عليهم، وترتكب هذه الجرائم في الغالب من قبل أفراد أو مجموعة أفراد، تأخذ شكل شبكات أو تنظيمات محددة[٤٠].

تخلص مما سبق أن النصوص القانونية الخاصة بجرائم الواقعة على أمن الدولة منها المادة ١٥٩ و١٦٢ و١٧٧ و١٧٨ من قانون العقوبات العراقي لم تشترط وسيلة معينة، وبالتالي يمكن أن يتم التجسس بأي طريقة للحصول على أسرار الدفاع مثلاً باستخدام تقنية المعلومات الحديثة لإجراء تنصت أو اعتراض أو التقاط أو دخول غير مشروع إلى معلومات أو بيانات تعد من أسرار الدفاع، أيا كان مكان وجودها سواءً كانت في حاسب أو موقع الكتروني.. الخ. يضاف إلى ذلك أن المشرع كان موفقاً في إيراده عبارة يعتبر من أسرار الدفاع ليشمل أي معلومات أو بيانات تتعلق بأسرار الدفاع، كما أن المشرع لم يفرق بين الوطني والاجنبي في ارتكاب جريمة النجس كما جعل فعل التجسس المرتكب من الموظف ظرفا مشدداً وهو أمر محمود.

المطلب الثاني

أطر الجهود المبذولة لدرء الاعتداءات المعلوماتية على الحكومات في التشريع العراقي

تتميز جرائم تقنية المعلومات بالطابع العالمي كونها جرائم عابرة للقارات، فكان لابد من صدور قوانين دولية وتكاتف جهود دولية لاتخاذ تدابير فعالة للحد والقضاء عليها ومعاقبة مرتكبيها، فرغم وجود بعض الإتفاقيات المقررة لمكافحة الجريمة بصورة عامة، خاصة بالجريمة

المنظمة والعابرة للحدود، والتي تنطبق تماماً وسمات جرائم تقنية المعلومات، فقد وجدت معاهدات سنّت خصيصاً لمواجهة جرائم تقنية المعلومات [٤١].

ويمكن القول، إن المشرع يجرم استعمال الوسائل المعلوماتية من أجل الحفاظ على الأمن والنظام في المجتمع، وحماية أموال الناس وممتلكاتهم وأرواحه، حيث أن الأنظمة القانونية اتت صراحةً على أفعال الجرم المعلوماتي كما في تشريعات مكافحة الجرائم المعلوماتية لبعض البلدان العربية، ولكن النقطة المحورية هنا، في نطاق هذه التشريعات المتخصصة بجرائم المعلوماتية، تبقى الحاجة الملحة إلى الرجوع إلى تلك التشريعات التقليدية التي حددت مفهوم الأفعال الجرمية لتطبيق أحكامها .

وهو ما سيتم الرجوع فيه إلى التشريعات التقليدية التي تملأ هذا الفراغ في تشريعات مكافحة جرائم المعلوماتي غير أن المشكلة ستبدو بشكل أوضح في بعض البلدان، كما في العراق، التي ليس لديها تشريعات لجرائم المعلوماتية، ولذلك سيكون السؤال عن مدى امكانية تفعيل هذه النصوص التقليدية على أفعال الإرهاب المعلوماتي كما لو حصل تهديد لإلقاء الرعب بين الناس بوساطة الإنترنت، أو تنظيم أو تروّس عصابة إرهابية مسلحة على شبكة المعلومات أيضاً، وهما صورتان للجرائم الإرهابية في القانون العراقي؟.

الحقيقة ليس هنالك ما يمنع من تطبيق أحكام القوانين التقليدية على الجرائم المعلوماتية، لأنها في حقيقتها جرائم تستحق العقاب، وأن ذلك سيبدو أنجع مما لو أفلت مرتكبوها من العقاب، إذ إن مثل هذا التجريم سيؤدي إلى تطويق هذه الجرائم والحيلولة بين فاعليها وبين الإفلات من جرائمهم، كما أن هذه الجرائم المعلوماتية لا تختلف عن نظيرتها التقليدية إلا في وسيلة ارتكابها، وهو أمر ليس مؤثراً في التجريم في التقدير، فضلاً عن أن الاجرام المعلوماتي يبدو أشد خطورة من الاجرام التقليدي بآلاف المرات نظراً إلى اتساع الهائل في استخدام شبكة الإنترنت .

وإذا كانت مجموعة من القوانين العربية، تناولت في نصوصها جريمة المعلوماتية في نصوصها التقليدية، مع ما قد يثار في ظلها من مشكلات قانونية، فإن عدداً من التشريعات العربية المتخصصة بجرائم المعلوماتية، قد قالت على تجريم أفعال الجرم المعلوماتي والعقاب عليها، ومنها القانون الإماراتي بالقول كل من أنشأ موقعاً على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات تحت مسميات تمويهية لتسهيل الإتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية، يعاقب بالسجن مدة لا تزيد على خمس سنوات [٤٢].

والحكومة العراقية في سبيلها لسنّ ما تشير إليه بـ قانون جرائم المعلوماتية لتنظيم استخدام شبكات المعلومات وأجهزة الحاسوب والأجهزة والأنظمة الإلكترونية، وكانت القراءة الأولى للقانون المقترح قد تمت أمام مجلس النواب العراقي يوم ٢٧ يوليو/تموز ٢٠١١، وكانت القراءة الثانية للقانون المقترح قد تمت يوليو/تموز ٢٠١٢، وبينما تتم كتابة مسوّدته الأولى حالياً، وقد ينتهك التشريع المقترح المعايير الدولية الحامية لإجراءات التقاضي السليمة، وحرية التعبير، وحرية تكوين الجمعيات.

يقول القانون المقترح، على وجه التحديد أنه يوفر القانون عقوبات على استخدام أجهزة الحاسوب فيما له علاقة بالعديد من الأنشطة الممنوعة، مثل الاحتيال المالي والاختلاس المادة ٧ وغسيل الأموال المادة ١٠ وتعطيل الشبكات المادة ١٤ والمراقبة غير المشروعة المادة ١٥ أولاً ب والمادة ١٦ والاعتداءات على الملكية الفكرية المادة ٢١ ومع ذلك، فإن هذا القانون لا يقتصر في استهدافه على نطاق محدود، و بالأحرى ستجرِّم أحكامه استخدام الحاسوب فيما يتصل بنطاق واسع من الأنشطة التي يتم تعريفها بشكل فضفاض – الكثير منها غير خاضع للقواعد حالياً – دون الرجوع إلى أية معايير محددة، وبالسماح للسلطات العراقية بمعاقبة الأفراد بهذه الطريقة، تبدو أحكام القانون متعارضة مع القانون الدولي والدستور العراقي، وإذا تم تطبيقها فسوف تشكل تقليصاً خطيراً لحق العراقيين في حرية التعبير وتكوين الجمعيات [٤٣].

ومن التحديات التي تواجه التشريع الوطني العراقي هي التَّحدّيات العمليّة التي تعترِضُ مُكافحة جرائم المعلوماتية على المستوى الوطني ويمكن إدراجها بين إطارين الأول التحديات التي توجبها طبيعة البيئة المعلوماتية، والثاني التحديات التي تمليها الجوانب الفنية.

فالتَّحدّيات التي توجبها طبيعة البيئة المعلوماتية ترتبط هذه التَّحدّيات بالجوانب التَّقنيّة الخاصَّةِ بالجَرائمِ السَّيبرانيَّة، بما في ذلك التَّجهيزات من حواسيب وشبكات توصيل، كما البرمجياتُ المشغِّلة لتلك الحواسيب، أو المُستَخدمة في توفير الخدمات المؤمَّنَة عَبرها، وهذا ما يَدفَع بالبعض إلى القول بأنَّ الجَريمَة الإلكترونية سهلة الارتكاب صَعبَة الاكتشاف، لوجود العديد من العقبات والتحديات التقنية[٤٤].

أما بالنسبة للتَّحديات التي تمليها الجوانب الفنّيّة في جرائم تقنية المعلومات ضد الحكومة تتصدَّرُ هذه التَّحديات التي تُمليها طَبيعَة جريمة تقنية المعلومات تلك الحكومة تلك الإشكاليات التي تُثيرُها الأدلَّةُ الجُرميَّة الرقميَّة، وخاصَّةً خلال مرحلتي التَّقصي عن الجريمة والتَّحقيق فيها، وما يتَسَبَّبُ بصعوبات عند السَّعي إلى إثباتِ وقوع الجريمة، وتحديدِ المساهمين بها، والنَّتائج الجُرمية التي أسفرت عنها.

الخاتمة

لقد اختلفت طبيعة المخاطر التي واجهتها المجتمعات البشرية وتبدلت وفق اختلاف مصادر التهديد من جهة، ومن جهة أخرى وفق التطورات الي شهدها المجتمع البشري، وإن كانت المخاطر الطبيعية لا زالت على حالها كما عرفها وعانى منها الإنسان الأول كالزلازل والبراكين والاعاصير والفيضانات والحرائق وغيرها من المظاهر الطبيعية الخطرة.

حيث سعى الإنسان منذ نشأته الى توقيها لتجنب مخاطرها، أو للتخفيف من مقدار الضرر التي قد تتأتى عنها، مستغلاً كل ما أتاه من علم وقدرة على استنباط الحلول، مسخراً كل ما ابتكره من معدات وتجهيزات وأدوات وما أعده من مخططات مسبقة لمواجهتها.

فجرائم تقنية المعلومات لا تخرج عن هذا الإطار في كونها نتاج تصرّف جاهل أو خاطئ، أو سلوك آثم يبتغي منه مرتكبه تحقيق مآرب غير شرعية، فتلك السلوكيات هي سلوكيات مستجدة أتت بها تقنية المعلومات الحديثة والتي تطورت مع تطور التجهيزات الإلكترونية والبرمجيات الرقمية التي اعتمد عليها في تشغيلها ويتم التصدي لها من خلال اتخاذ تدابير احتياطية حمائية تارةً، وتارة أخرى بتدابير زاجرة عبر توصيفها كأفعال جرمية تستوجب العقاب على اقترافها.

فتعددت المحاولات الى تحديد صورها المختلفة والبحث في كيفية مواجهتها من خلال تطبيق النصوص القائمة التي وضعت في وقت سابق على ظهور تقنية المعلومات دون الاخلال بمبدأ الشرعية الجنائية، فتباينت التشريعات في التعامل معها وفي خلق إطار قانوني لها.

بنهاية القول نجد بأن مكافحة جرائم تقنية المعلومات على كافة المستويات الدولية والمحلية تتطلب الكثير من التعاون بين مختلف الجهات المعنية بمكافحتها والاستعداد المسبق والتحضير المتقن لمواجهة عدد من الصعوبات التي تواجه الدولة والفرد على هذا الصعيد.

وفيما يلي بعض الاستنتاجات والمقترحات التي قد قمنا بالتوصل اليها خلال دراستنا:

أولاً: الاستنتاجات:

١-نخلص الى ان جرائم تقنية المعلومات هي تعبير شامل يشير الى كل نشاط اجرامي مرتبط باستخدام تقنية المعلومات الحديثة، بحيث ان غياب الارتباط بها يمنع ارتكاب مثل هذا العمل غير المشروع، ولا يختلف الامر سواء اكانت وسيلة تقنية المعلومات الحديثة أداة لإتمام النشاط الإجرامي أم كانت محلاً له أو هدف الاعتداء.

٢-جرائم تكنولوجيا المعلومات الحديثة طائفة من الجرائم التي تتميز بطبيعة خاصة عن غيرها من الجرائم فهي جريمة متعدية الحدود أو جريمة عابرة للدول ذات خصوصية لجهة قلة عدد

الحالات التي يتم اكتشافها مقارنةً في ضوء ما يتم اكتشافه من الجرائم التقليدية، وصعوبة إثباتها حتى في حال اكتشاف وقوعها والإبلاغ عنها، وتبرز ذاتيتها بصورة أكثر وضوحاً في أسلوب ارتكابها وطريقتها والأسباب أو العوامل التي تقف وراء ارتكابها.

٣-يحدد السلوك الاجرامي في كل جريمة من قبل المشرع ضيقاً واتساعاً على نحو يمكّن القاضي من تكييف السلوك الاجرامي أو فعل الجريمة ورده الى القاعدة القانونية أو النص التجريمي الذي يحكمه، معنى ذلك أنه للعقاب على الجريمة لا بد من لأن يتطابق السلوك الإجرامي للجاني مع ذات النموذج الإجرامي الوارد في قاعدة قانون العقوبات على نحو من الدقة والوضوح، بحيث لا يدع مجالاً لاختلاف الرأي في مضمونه.

٤-لا يمكن اتباع الإجراءات المحددة للكشف عن الجرائم العادية ف مجال جرائم تقنية المعلومات لما تحتاج اليه من خبرة وكفاءة ومعرفة تقنية حاسوبية من قبل الأجهزة التحقيقية سواء اكانت في مرحلة تفتيش الحاسوب أو في مرحلة التحقيق واستجواب المتهم.

ثانياً: المقترحات:

١-على المشرع العراقي إعارة الاهتمام للتوعية حول طبيعة العالم المعلوماتي والمخاطر الكامنة فيه، وضرورة اتخاذ احتياطات حمائية عند ولوج هذا العالم الافتراضي اللامتناهي الإبعاد والغريب الأطوار.

٢-على كلا التشريعين العراقي واللبناني اعتماد برامج وخطط استراتيجية متكاملة لنشر التوعية من مخاطر الجرائم المعلوماتية بما فيها تلك التي ترتكب عبر وسائط التواصل الاجتماعي، وتحديث النصوص الجزائية الموضوعية، بحيث تشمل توصيفات جرمية لكل الجرائم الإلكترونية المستجدة والتقليدية، وذلك من خلال استحداث فصل خاص بالجرائم الإلكترونية على أن توزع ضمن فئات، ووفق محل وطبية الجريمة، ووسائل ارتكابه، وإعادة النظر في توصيف الجرائم التقليدية التي يمكن ارتكابها بوسائل إلكترونية.

٣-الحرص على تحديث مختلف التشريعات المقارنة بصورة مستدامة على نحو يواكب التطورات التكنولوجية، وبخاصة مستجدات الفضاء المعلوماتي وتقنيات المعلومات والأنماط المستجدة، على نحو يحد من إمكانية إساءة استعمال نظم المعلوماتية وأدواتها ووسائلها وبرمجياتها على نحو غير مشروع.

٤-العمل على تعزيز التعاون الدولي والإقليمي والوطني بين مختلف الجهات المعنية بالتصدي لهذه النوعية من المجرمين على نحو فعال والحيلولة دون تمكين إفلاتهم من العقاب والملاحقة،

بما في ذلك عدم توفير ملاذ آمن لهم، على أن يشمل المجالات التالية، تبادل المعلومات، ونقل الإجراءات، واستعانة أجهزة تطبيق القانون في العراق ولبنان بمثيلاتها في الدول الأُخرى المعنية.

الهوامش

[١] محمد عزت فاضل ونوفل على الصفو، جرائم تقنية المعلومات المخلة بالأخلاق العامة، الطبعة الأولى، دار السنهوري، بغداد، ٢٠١٧، ص٣١.

[٢] طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠٠١، ص١١٨.

[٣] منير محمد الجنبيهي، وممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحته، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٤، ص١٩.

[٤] عادل مشموشي، جرائم المعلوماتية وتحديات مسارحها الافتراضية، أدواتها الالكترونية، أساليبها التقنية، مقتضياتها التشريعية، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٩، ص٣٩٥.

[٥] محمد عبد الله أبو بكر، موسوعة جرائم المعلوماتية جرائم الكمبيوتر والانترنت، الطبعة الأولى، المكتب العربي الحديث، الإسكندرية، مصر، ٢٠١١، ص٧٤.

[٦] محمد عزت فاضل ونوفل على الصفو، جرائم تقنية المعلومات المخلة بالأخلاق العامة، مرجع سابق، ص٣٣.

[٧] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، مصر، ٢٠٠٨، ص١٩٤.

[٨] منير محمد الجنبيهي، وممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحته، مرجع سابق، ص٢٢.

[٩] فاروق سيد حسين، الانترنت الشبكة الدولية للمعلومات، الطبعة الأولى، دار الراتب الجامعية، بيروت، لبنان، ٢٠٠١، ص١٠٤.

[١٠] فاروق سيد حسين، الانترنت الشبكة الدولية للمعلومات، مرجع سابق، ص١٠٦.

[١١] حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠١٤، ص١٨٢.

[١٢] خالدة الزعبي، الحاسوب والبرمجيات الجاهزة، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، الأردن، ٢٠٠٢، ص١٣.

[١٣] عادل مشموشي، جرائم المعلوماتية وتحديات مسارحها الافتراضية، أدواتها الالكترونية، أساليبها التقنية، مقتضياتها التشريعية، مرجع سابق، ٣٩٧.

[١٤] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٣، ص٦٤.

[١٥] خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٩، ص١١٣.

[١٦] محمود نجيب حسني، شرح قانون العقوبات –القسم الخاص، دار النهضة، القاهرة، ٢٠١٩، ص ١١.

[١٧] علي جعفر، جرائم تكنلوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، بيروت، ٢٠١٣، ص ٥٢٠.

[١٨] محمد حماد مرهج الهيتي، مدى تطبيق نصوص جرائم الإتلاف والتخريب على الإتلاف الذي يتعرض له الحاسب الآلي، دار النهضة، القاهرة، ٢٠١٠، ص ١١٩.

[١٩] مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة، القاهرة، ٢٠١٢، ص ٥٤.

[٢٠] حسن بن أحمد الشهري، الجريمة والمجرمون، الجرائم الالكترونية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، ٢٠١١، ص ١٧.

[٢١] حسن بن أحمد الشهري، المرجع نفسه، ص ١٨.
[٢٢] حسن بن أحمد الشهري، المرجع نفسه، ص ١٧.
[٢٣] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، مصر، ٢٠١٣، ص٥٠.
[٢٤] المادة(٣/أولاً) من مشروع الجرائم الالكترونية العراقي.
[٢٥] عمر محمد بن يونس، الجرائم الناشئة عن إستخدام الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٤، ص٢٩٨.
[٢٦] عمار عباس الحسيني، جرائم الحاسوب والإنترنت، منشورات الحلبي الحقوقية، بيروت، ٢٠١٩، ص ١٦٣.
[٢٧] عبد الله بن عبد العزيز بن فهد، الإرهاب الالكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، القاهرة، ٢٠٠٨، ص ١٩.
[٢٨] حسن طاهر داوود، أمن شبكة المعلومات، مركز البحوث معهد الإدارة العامة، الرياض، ٢٠٠٤، ص ١٤٠.
[٢٩] علي عدنان الفيل، الإجرام الإلكتروني، منشورات الحلبي الحقوقية، بيروت، ٢٠١١، ص ٨٦.
[٣٠] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنلوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١، ص ٥٠٠.
[٣١] المادة ٧٣٣ من قانون العقوبات اللبناني رقم ٣٤٠ لعام ١٩٤٣.
[٣٢] أنطوان بطرس، المعلومات وأهميتها في العصر الحديث، مجلة الكمبيوتر والاتصالات والإلكترونيات، المجلد الثامن، العدد ١٢، بيروت، ١٩٩٩، ص ٣٩.
[٣٣] ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي، ط١، دار السلام القانونية، بغداد، ٢٠١٧، ص ٨٣.
[٣٤] المواد (١٥٨-١٥٩-١٦٤-١٧٧) من قانون العقوبات العراقي رقم ١١١ لعام ١٩٦٩.
[٣٥] المادة ١٨٢ من قانون العقوبات العراقي رقم ١١١ لعام ١٩٦٩.
[٣٦] محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، دار المطبوعات الجامعية، القاهرة، ٢٠١٤، ص ١١٦.
[٣٧] علي جعفر، جرائم تكنلوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، مرجع سابق، ص ٥٦٩.
[٣٨] محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص ١٣.
[٣٩] سعد إبراهيم الأعظمي، جرائم التجسس، دار الشؤون الثقافية العامة، بغداد، ٢٠٠٢، ص ٥٦.
[٤٠] سعد إبراهيم الأعظمي، الجرائم الماسة بأمن الدولة الداخلي، دار الشؤون الثقافية العامة، بغداد، ٢٠٠٠، ص ٤٠.
[٤١] هدى حامد قشقوش، الجريمة المنظمة، القواعد الموضوعية والاجرائية والتعاون الدولي، ط٢، منشأة المعارف، الإسكندرية، ٢٠٠٦، ص١٨.
[٤٢] المادة ٢١ من القانون الاتحادي الخاص بمكافحة الشائعات والجرائم الالكترونية الإماراتي رقم ٣٤ لسنة ٢٠٢١.
[٤٣] عدلي محمد عبد الكرخي، جريمة الارهاب عبر الوسائل الالكترونية في القانونين اللبناني والعراقي، منشورات هاترك للطباعة والنشر، العراق، ٢٠٢٣، ص ١٠٣ وما بعدها.
[٤٤] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧، ص٤٥.

قائمة المراجع

أولاً: الكتب القانونية:

١.أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، مصر، ٢٠٠٨.
٢.حسن بن أحمد الشهري، الجريمة والمجرمون، الجرائم الالكترونية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، ٢٠١١.
٣.حسن طاهر داوود، أمن شبكة المعلومات، مركز البحوث معهد الإدارة العامة، الرياض، ٢٠٠٤.
٤.حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠١٤.
٥.خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٩.
٦.خالدة الزعبي، الحاسوب والبرمجيات الجاهزة، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، الأردن، ٢٠٠٢.
٧.سعد إبراهيم الأعظمي، الجرائم الماسة بأمن الدولة الداخلي، دار الشؤون الثقافية العامة، بغداد، ٢٠٠٠.
٨.سعد إبراهيم الأعظمي، جرائم التجسس، دار الشؤون الثقافية العامة، بغداد، ٢٠٠٢.
٩.ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي، ط١، دار السلام القانونية، بغداد، ٢٠١٧.
١٠.طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠٠١.
١١.عادل مشموشي، جرائم المعلوماتية وتحديات مسارحها الافتراضية، أدواتها الالكترونية، أساليبها التقنية، مقتضياتها التشريعية، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٩.
١٢.عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنلوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١.
١٣.عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧.
١٤.عدلي محمد عبد الكرخي، جريمة الارهاب عبر الوسائل الالكترونية في القانونين اللبناني والعراقي، منشورات هاترك للطباعة والنشر، العراق، ٢٠٢٣.
١٥.عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٣.
١٦.علي جعفر، جرائم تكنلوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، بيروت، ٢٠١٣.
١٧.علي عدنان الفيل، الإجرام الإلكتروني، منشورات الحلبي الحقوقية، بيروت، ٢٠١١.
١٨.عمار عباس الحسيني، جرائم الحاسوب والإنترنت، منشورات الحلبي الحقوقية، بيروت، ٢٠١٩.
١٩.عمر محمد بن يونس، الجرائم الناشئة عن إستخدام الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٤.
٢٠.فاروق سيد حسين، الانترنت الشبكة الدولية للمعلومات، الطبعة الأولى، دار الراتب الجامعية، بيروت، لبنان، ٢٠٠١.
٢١.محمد حماد مرهج الهيتي، مدى تطبيق نصوص جرائم الإتلاف والتخريب على الإتلاف الذي يتعرض له الحاسب الآلي، دار النهضة، القاهرة، ٢٠١٠.
٢٢.محمد عبد الله أبو بكر، موسوعة جرائم المعلوماتية جرائم الكمبيوتر والانترنت، الطبعة الأولى، المكتب العربي الحديث، الإسكندرية، مصر، ٢٠١١.
٢٣.محمد عزت فاضل ونوفل على الصفو، جرائم تقنية المعلومات المخلة بالأخلاق العامة، الطبعة الأولى، دار السنهوري، بغداد، ٢٠١٧.
٢٤.محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، دار المطبوعات الجامعية، القاهرة، ٢٠١٤.

٢٥.محمود نجيب حسني، شرح قانون العقوبات –القسم الخاص، دار النهضة، القاهرة، ٢٠١٩.
٢٦.مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة، القاهرة، ٢٠١٢.
٢٧.منير محمد الجنبيهي، وممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحته، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٤.
٢٨.نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، مصر، ٢٠١٣.
٢٩.هدى حامد قشقوش، الجريمة المنظمة، القواعد الموضوعية والاجرائية والتعاون الدولي، ط٢، منشأة المعارف، الإسكندرية، ٢٠٠٦.

ثانياً: المجلات والدوريات:

١. أنطوان بطرس، المعلومات وأهميتها في العصر الحديث، مجلة الكمبيوتر والاتصالات والإلكترونيات، المجلد الثامن، العدد ١٢، بيروت، ١٩٩٩.
٢. عبد الله بن عبد العزيز بن فهد، الإرهاب الالكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت ، القاهرة، ٢٠٠٨.

ثالثاً: القوانين:

١.قانون العقوبات العراقي رقم ١١١ لعام ١٩٦٩.
٢.القانون الاتحادي الخاص بمكافحة الشائعات والجرائم الالكترونية الإماراتي رقم ٣٤ لسنة ٢٠٢١.
٣.قانون العقوبات اللبناني رقم ٣٤٠ لعام ١٩٤٣.
٤.مشروع الجرائم الالكترونية العراقي لعام ٢٠١٢.

Reference

First: Legal Books

1.Amir Faraj Youssef, *Cybercrimes on the Internet*, 1st ed., University Publications House, Alexandria, Egypt, 2008.
2.Hassan bin Ahmed Al-Shahri, *Crime and Criminals, Cybercrimes*, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia, 2011.
3.Hassan Taher Dawood, *Information Network Security*, Research Center, Institute of Public Administration, Riyadh, 2004.
4.Hanan Rihan Mubarak Al-Mudhakhi, *Cybercrimes: A Comparative Study*, 1st ed., Al-Halabi Legal Publications, Beirut, Lebanon, 2014.
5.Khaled Mamdouh Ibrahim, *The Art of Investigating Cybercrimes*, 1st ed., Dar Al-Fikr Al-Jamei, Alexandria, Egypt, 2009.
6.Khalida Al-Zoubi, *Computer and Ready-Made Software*, 1st ed., Dar Wael for Publishing and Distribution, Amman, Jordan, 2002.
7.Saad Ibrahim Al-A'zami, *Crimes Against Internal State Security*, Public Cultural Affairs House, Baghdad, 2000.
8.Saad Ibrahim Al-A'zami, *Espionage Crimes*, Public Cultural Affairs House, Baghdad, 2002.
9.Dhirgham Jabir Attoosh Al-Mawash, *Information Espionage Crime*, 1st ed., Dar Al-Salam Legal Publishing, Baghdad, 2017.
10.Tony Michel Issa, *Legal Regulation of the Internet*, 1st ed., Al-Halabi Legal Publications, Beirut, 2001.
11.Adel Mashmoushi, *Cybercrimes and the Challenges of Virtual Arenas: Their Electronic Tools, Technical Methods, and Legislative Requirements*, 1st ed., Modern Institution for Books, Lebanon, 2019.
12.Abdel Fattah Bayoumi Hegazy, *Emerging Crimes in the Field of Modern Communications Technology*, National Center for Legal Publications, Cairo, 2011.

13.Abdullah Abdul Karim Abdullah, *Cybercrimes and the Internet*, Al-Halabi Legal Publications, Beirut, 2007.
14.Adly Mohammed Abdel-Karkhi, *Electronic Terrorism Crime in Lebanese and Iraqi Laws*, Hatrak Publishing and Printing, Iraq, 2023.
15.Afifi Kamel Afifi, *Computer Crimes, Copyrights, and the Role of Police and Law: A Comparative Study*, 1st ed., Al-Halabi Legal Publications, Beirut, Lebanon, 2003.
16.Ali Jaafar, *Modern Information Technology Crimes Against Individuals and Government*, Zein Legal Publications, Beirut, 2013.
17.Ali Adnan Al-Feel, *Electronic Crime*, Al-Halabi Legal Publications, Beirut, 2011.
18.Ammar Abbas Al-Husseini, *Computer and Internet Crimes*, Al-Halabi Legal Publications, Beirut, 2019.
19.Omar Mohammed Bin Younes, *Crimes Arising from Internet Use*, Dar Al-Nahda Al-Arabiya, Cairo, 2004.
20.Farouq Sayed Hussein, *The Internet: The International Information Network*, 1st ed., Al-Ratib University Publishing, Beirut, Lebanon, 2001.
21.Mohammed Hammad Marhej Al-Hiti, *The Extent of Applying Vandalism and Destruction Provisions to Computer Damage*, Dar Al-Nahda, Cairo, 2010.
22.Mohammed Abdullah Abu Bakr, *Encyclopedia of Cybercrimes: Computer and Internet Crimes*, 1st ed., Arab Modern Office, Alexandria, Egypt, 2011.
23.Mohammed Ezzat Fadel and Noufal Ali Al-Saffo, *Information Technology Crimes Violating Public Morality*, 1st ed., Al-Sanhouri House, Baghdad, 2017.
24.Mahmoud Suleiman Moussa, *International Espionage and Criminal Protection of National Defense and State Security*, University Publications House, Cairo, 2014.
25.Mahmoud Naguib Hosni, *Explanation of the Penal Code – Special Part*, Dar Al-Nahda, Cairo, 2019.
26.Medhat Ramadan, *Criminal Protection of Electronic Commerce*, Dar Al-Nahda, Cairo, 2012.
27.Muneer Mohammed Al-Janbei and Mamdouh Mohammed Al-Janbei, *Internet and Computer Crimes and Methods of Combating Them*, 1st ed., University Thought House, Alexandria, 2004.
28.Nabila Heba Harwal, *Procedural Aspects of Internet Crimes in the Stage of Evidence Collection: A Comparative Study*, University Thought House, Egypt, 2013.
29.Huda Hamed Qashqoush, *Organized Crime: Substantive and Procedural Rules and International Cooperation*, 2nd ed., Al-Maaref Establishment, Alexandria, 2006.

Second: Journals and Periodicals

1.Antoine Boutros, *Information and Its Importance in the Modern Age*, *Computer, Communications, and Electronics Journal*, Vol. 8, No. 12, Beirut, 1999.
2.Abdullah bin Abdulaziz bin Fahd, *Electronic Terrorism in the Information Age*, research presented to the First International Conference on Protection of Information Security and Privacy in Internet Law , Cairo, 2008.

Third: Laws

1.Iraqi Penal Code No. 111 of 1969.
2.United Arab Emirates Federal Law on Combating Information Technology Crimes of ٢٠٢١.
3.Lebanese Penal Code No. 340 of 1943.
4.Draft Iraqi Cybercrime Law of 2012.