جريمة التجسس الإلكتروني في إطار مشروع قانون جرائم المعلوماتية العراقي لسنة ٢٠١١

م.د. إسراء يونس هادي
esraaalmola2019@gmail.com

م.د. أسامة احمد النعيمي
usama200670@yahoo.com

كلية الحقوق / جامعة الموصل

THE CRIME OF CYBER ESPIONAGE WITHIN THE FRAME OF PROJECT OF IRAQI INFORMATIVE CRIME ACT OF 2011

Lecturer .Dr. Isra'a Yunis Hadi al- Moulah
University of Mosul/ College of Rights
Lecturer .Dr. Usama Ahmed al-Neemy
University of Mosul/ College of Rights

الملخص

تعد جريمة التجسس الإلكتروني من الجرائم ذات الخطورة والتطور المستمر، وذلك لدخول الجاني إلى موقع إلكتروني أو نظام المعلومات أو الشبكة المعلوماتية للحصول على محتوى إلكتروني غير متاح للجمهور يمس الأمن الوطني أو العلاقات الخارجية للدولة أو الاقتصاد الوطني مستخدما أساليب حديثة يصعب كشفها خاصة مع التطور التكنولوجي الهائل في جميع المجالات.

وجاء هذا البحث لتسليط الضوء على مدى الحماية الجنائية التي وفرها المشرع العراقي للمحتوى الإلكتروني المتضمن معلومات سرية تخص الدولة، والتي تضمنها مشروع قانون جرائم المعلوماتية لسنة ٢٠١١ للتصدي لهذه الجريمة كونها تعد من الجرائم الماسة بأمن الدولة وتهدد كيانها. لذلك تم تناول هذا البحث من خلال مبحثين، خصص المبحث الأول لبيان ماهية التجسس الإلكتروني، وبينا فيه تعريف التجسس بشكل عام، وتعريف التجسس الإلكتروني بشكل خاص، والصور السائدة للتجسس، فضلا عن تميز التجسس الإلكتروني عما يشتبه به، أما في المبحث الثاني فقد وضحنا فيه أركان جريمة التجسس الإلكتروني والعقوبة المقررة لها.

الكلمات المفتاحية: التجسس، قانون، معلومات، الإلكتروني

Abstract

The crime of cyber espionage is one of the serious and continually developing crimes due to the access of an offender to a website, information system or information network to obtain electronic content that is not available to the public affecting national security, the external relations of the state or the national economy using modern methods that are difficult to detect, especially with the huge technological development. in all fields. This research highlights the extent of criminal protection provided by the Iraqi legislator for electronic content containing confidential information belonging to the State, and included in the draft law of information crimes of 2011 to address this crime as it is a crime against the security of the State that threatens its existence. Therefore, this research deals with two sections, the first section was devoted to the definition of electronic spyware, and the definition of espionage in general, and the definition of electronic espionage in particular, and the prevalent images of spy, in addition to distinguishing electronic espionage from what is suspected, In the second section we have explained the elements of the crime of cyber espionage and the penalty prescribed for it.

Keywords: espionage, law, information, electronic

المقدمة

أولاً: التعريف بموضوع البحث وأهميته: لاشك أن أهمية المعلومات قد ازدادت في الوقت الحاضر الذي يعرف بكونه عصر المعلومات الرقمية حيث أضحت المعلومات قوة جديدة في حياة الشعوب وإدارة الدولة والحكم، بل إن أهميتها باتت تفوق أهمية الموارد الطبيعية من حيث كونها مصدرا للقوة العسكرية والصناعية والاقتصادية، وحيث إن التجسس ظاهرة بشرية صاحبت المجتمع الإنساني منذ نشأته الأولى، وظلت تلازمه عبر التاريخ، وقد تطورت في عصرنا الحاضر وأصبحت من الممارسات الاعتيادية التي تعتمد عليها الدول في حماية أمنها ووجودها، وأصبحت أيضا أكثر خطراً بتأثير التقدم العلمي والتقني الذي أفرزته الثورة المعلوماتية، إذ من خلال التجسس تحصل

الدول بواسطة أجهزتها الاستخبارية على أسرار أو معلومات الدولة واستغلالها بما يضر بالمصلحة الوطنية للدولة أو إفشائها إلى دول أخرى تكون عادة معادية لها، عليه فقد اتجه المشرع في العديد من الدول إلى توفير الحماية اللازمة لهذه المعلومات والبيانات، سواء أكان ذلك عن طريق تعديل قوانينها أم عن طريق استحداث قوانين خاصة تجرم كل ما من شانه الإضرار بتلك البيانات أو المعلومات، ومن ضمنها تجريم التجسس على البيانات والمعلومات الإلكترونية، وهو الأمر الذي اتجه إليه المشرع العراقي في مشروع قانون الجرائم المعلوماتية الذي ضمنه النصوص المتعلقة بجريمة التجسس الإلكتروني[١]، وما تقدم يجعل للبحث في جريمة التجسس الإلكتروني أهمية كبيرة، فضلا عن إن هذه الجريمة لم تعد تمثل فقط اعتداءً على المصالح الوطنية للدولة فحسب، بل بدأت تأخذ بعدا أوسع من خلال تأثيرها الضار على المصالح الشخصية للإفراد بفعل وجود التقنيات العالية والاستخدام الواسع للشبكة المعلوماتية الذي جعل من حدود الدول مستباحة لمن يسعى للحصول وبشكل غير مشروع على المعلومات السرية المتعلقة بأنشطتها المختلفة ومنها الأنشطة المالية والاقتصادية والتجارية والصناعية [٢].

ثانيا: مشكلة البحث: تتمثل مشكلة البحث في إيجاد أجوبة لمجموعة من التساؤلات أهمها: ما مفهوم التجسس الإلكتروني، وماهي صوره وأساليبه، وما هي أركان جريمة

(١) تجدر الإشارة إلى إن المادة (٣) من اتفاقية بودابست المتعلقة بالإجرام المعلوماتي والموقعة بتاريخ ١١/٢٣ / ٢٠٠١ قد جرمت التجسس والتنصت على البيانات والمعلومات الرقمية، إذ أوجبت هذه المادة على الدول الأطراف في الاتفاقية اتخاذ الإجراءات التشريعية اللازمة لإصدار نص قانوني أو تشريعي بأنها تشكل جرائم بموجب القانون الوطني عند ارتكابها عن قصد، وذلك من حيث اعتراض سير البيانات دون وجه حق بالوسائل الفنية لقطع عمليات البث والإرسال الغير عمومية لبيانات الحاسب الآلي إلى، أو من، أو داخل منظومة الحاسب الآلي بما في ذلك ما ينبعث من منظومة الحاسب الآلي من موجات كهرومغناطيسية تحمل معها المعلومات والبيانات.

(٢) تم الكشف عن العديد من حالات التجسس الدولي ومنها ما اكتشف مؤخرا عن مفتاح وكالة الأمن القومي الأمريكيNSA الذي قامت بزراعته في نظام التشغيل الشهير ويندوز، كما توجد شبكة دولية ضخمة للتجسس الإلكتروني تابعة للوكالة ذاتها تعمل بالتعاون مع أجهزة الاستخبارات والتجسس في كندا وبريطانيا واستراليا ونيوزيلندا لرصد المكالمات الهاتفية والرسائل بأنواعها كافة يطلق عليها اسم ECHELON، فضلا عن ذلك فقد أشار تقرير صادر عن وزارة التجارة والصناعة البريطانية إلى زيادة نسبة التجسس على الشركات التجارية والصناعية من ٣٦ % عام ١٩٩٤ إلى ٤٥% عام ١٩٩٩. ينظر: محمد محمد الألفي، جرائم التجسس والإرهاب الإلكتروني عبر الإنترنت، مقال منشور على الموقع الإلكتروني http://www.cyberlawnet.ne، تاريخ الزيارة ٢٠١٩/٨/٢٣.

التجسس الإلكتروني والعقوبة المقررة لها، وهل إن المشرع العراقي في مشروع قانون الجرائم المعلوماتية لسنة ٢٠١١ والذي لم يقر لحد الآن قد تضمن النصوص الكافية لمكافحة هذه الجريمة والحد من أثارها الخطيرة.

ثالثا: نطاق البحث: اقتضت طبيعة البحث تحديد نطاقه في دراسة جريمة التجسس الإلكتروني في إطار مشروع قانون جرائم المعلوماتية العراقي لسنة ٢٠١١، ومن ثم يخرج من نطاق البحث جريمة التجسس المنصوص عليها في قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل أو القوانين الخاصة الأخرى.

رابعا: منهجية البحث: اقتضت دراسة موضوع البحث الاعتماد على المنهج الاستقرائي والتحليلي لنصوص مشروع قانون جرائم المعلوماتية، فضلا عن المنهج المقارن، إذ قارنا موقف المشرع العراقي مع موقف المشرع في القوانين العربية الإماراتي والسعودي والقطري والكويتي الخاصة بالجرائم الإلكترونية من اجل الاستفادة من المسلك الذي سار عليه المشرع في كل منها عند تنظيمه لأحكام هذه الجريمة للوصول إلى المقترحات التي يمكن الاستفادة منها من قبل المشرع العراقي عند إصداره للقانون.

خامسا: هيكلية البحث: اقتضى تناول موضوع البحث تقسيمه إلى مبحثين وكالآتي: المبحث الأول:ماهية التجسس الإلكتروني.المبحث الثاني:أركان جريمة التجسس الإلكتروني والعقوبة المقررة لها.

المبحث الأول

ماهية التجسس الإلكتروني

للبحث في أي موضوع ينبغي أولاً أن نُبيَّن ماهيته، وللتعرف على ماهية التجسس الإلكتروني لابد أولاً من التعريف بالتجسس الإلكتروني وتحديد صوره ووسائله، ومن ثم لابد أيضا تمييزه عما يشتبه به، وعليه سنقسم هذا المبحث إلى مطالب ثلاثة، وذلك على النحو الآتي:

المطلب الأول: التعريف بالتجسس الإلكتروني

للتعريف بالتجسس الإلكتروني،لابد أولاً من تعريف التجسس لغةً واصطلاحاً، ومن ثم تعريف التجسس الإلكتروني، وبيان ذلك وفقا للاتي: **أولاً: تعريف التجسس لغةً**

واصطلاحاً:إن تحديد مفهوم التجسس بصورة دقيقة ومحددة ينبغي أولا تعريف التجسس لغةً،ومن ثم تعريفه اصطلاحاً،وذلك على النحو الآتي:

١- **تعريف التجسس لغةً:** مأخوذ من الجَسِّ: وهو جَسُّ الخبر، ومعناه: بحث عنه وفحص، وتَجَسَّسْتُ فلانًا ومن فلان: بحثت عنه، والتَّجَسُّسُ بالجيم التفتيش عن بواطن الأمور، وأكثر ما يقال في الشرِّ، والجاسُوسُ: العين يَتَجَسَّسُ الأخبار ثم يأتي بها، وهو صاحب سِرِّ الشَّر، والناموسُ صاحب سرِّ الخير[١]. وقيل إن التجسس بالجيم: تتبع الظاهر، وبالحاء المهملة تتبع البواطن[٢]، وقد ورد في قوله تعالى: "ولا تجسسوا"[٣]، أي لا تبحثوا عن عورات المسلمين وتستكشفوا عما ستره الله تعالى.

٢- **تعريف التجسس اصطلاحاً:** نظراً لتعدد أفعال التجسس واختلافها فقد خلت غالبية القوانين من تعريف التجسس ومنها القانون العراقي، واكتفت بدلا عن ذلك بتحديد صور السلوك المجرم المحقق للجريمة الذي لكل منها ذاتيته الخاصة والمميزة عن سواه.

أما الفقه الجنائي فقد تعددت تعريفاته لجريمة التجسس، إلا إن هذه التعريفات جاءت متباينة لاختلاف السلوك المجرم المحقق للجريمة من دولة إلى أخرى، إلا انه يمكن لنا أن نميز بين اتجاهين في تعريف التجسس، الأول: يذهب إلى التضييق من مدلوله بحيث يقصره على وقائع جمع المعلومات العسكرية التي تفيد العدو باستعمال طرق احتيالية وصفات كاذبة، ومن ثم تعريف التجسس بأنه: "قيام الأجنبي بجمع الوثائق والمعلومات السرية المتعلقة بالوضع السياسي والاقتصادي والموارد العسكرية والتنظيم الدفاعي والهجومي للدولة، وذلك بقصد تسليم الوثائق والمعلومات إلى الدولة الأجنبية سواء كان ذلك مجاناً أو بمقابل"[٤]، كما عرف بأنه: "البحث والتنقيب عما

(١) ينظر: محمد بن أبي بكر بن عبد القادر الرازي، مختار الصحاح، باب الجيم، مكتبة لبنان، بيروت، ١٩٨٦، ص٣٢٤.

(٢) ينظر:جمال الدين بن منظور، لسان العرب، ج٥، دار المعارف، بيروت، لبنان، ١٩٨٢، ص٢٣٧.

(٣) سورة الحجرات/ الآية ١٢.

(٤) ينظر: مجدي محمود حافظ، الحماية الجنائية لأسرار الدولة، الهيئة المصرية العامة للكتاب، الإسكندرية، ١٩٩٠، ص٢٢٢.

يتعلق بالعدو من معلومات سرية باستخدام الوسائل السرية والفنية ونقل ذات المعلومات بذات الوسائل أو بواسطة العملاء والجواسيس والاستفادة منها في إعداد الخطط"[١].

أما الثاني: فقد وسع من مدلول التجسس بحيث شمل كل فعل يخدم مصالح الدولة الأجنبية' لذا عرف التجسس وفقا له بأنه: "السعي سراً صوب جمع المعلومات المتعلقة بالدولة وذلك بنية تسليمها إلى حكومة أجنبية، ويكون من شأن ذلك الإضرار بالدولة"[٢]. أو هو "البحث عن أي نوع من المعلومات خفية، عن دولة معينة بهدف إيصالها إلى دولة أجنبية وذلك بنية الإضرار بالدولة التي يتجسس عليها"[٣]. وعرف أيضا بأنه "نقل أو إفشاء خبر أو أي أمر من الأمور التي تعتبر سراً من أسرار الجمهورية العراقية، وكان من ذلك الإضرار بالمصلحة الوطنية والقومية للقطر العراقي والأمة العربية، إلى أي جهة خارجية أو داخلية مسلحة سواء كان ذلك لقاء منفعة أو بدونها"[٤]، وعلى الرغم من عدم الاتفاق على تعريف موحد للتجسس، فالمتفق عليه أن التجسس هو عملية الحصول على معلومات ليست متوفّرة عادةً للعامّة، وهو أحد الأنواع والسبل الملتوية في الحروب الحديثة والقديمة ويمثل تربصاً وخطراً داهماً على الدولة التي يتجسس عليها، ويقوم به شخص يطلق عليه مصطلح الجاسوس[٥]، فضلا عن اعتبار التجسس من الجرائم المخلة بأمن الدولة الخارجي.

---

(١) ينظر:فواز البقور، التجسس في التشريع الأردني، دراسة مقارنة، ط٣، عمان، ١٩٩٣، ص٢٥.

(٢) ينظر: عصام احمد علي السنيدار، البعثة الدبلوماسية بين الحصانة ومقتضيات الأمن الوطني، رسالة ماجستير، الجامعة الأردنية، عمان، ٢٠٠١، ص٩١.

(٣) ينظر: هاني جميل الطراونة، الجرائم الواقعة على امن الدولة الخارجي في التشريع الأردني/ دراسة مقارنة، دار وائل، عمان، ٢٠١١، ص٩١.

(٤) ينظر: سعد إبراهيم الاعظمي، جرائم التجسس في التشريع العراقي، دراسة مقارنة، رسالة ماجستير، جامعة بغداد، ١٩٨١، ص١٧.

(٥) يعرف الجاسوس بأنه: الشخص الذي يعمل في الخفاء أو تحت شعار كاذب ليحصل على معلومات عن العمليات العسكرية لدولة محاربة بهدف إيصالها للعدو، أو هو ذلك الشخص الذي يجمع أو يحاول جمع معلومات ذات قيمة عسكرية، في الخفاء أو باستعمال الغش والخداع. للتفصيل ينظر: د. علي صادق أبو هيف، القانون الدولي العام، ج١، منشأة المعارف، الإسكندرية، ١٩٧٥، ص٨٤٦ ؛ عبد الإله محمد النوايسة، ممدوح حسن العدوان، جرائم التجسس الإلكتروني في التشريع الأردني / دراسة مقارنة، بحث منشور في مجلة دراسات في علوم الشريعة والقانون، مجلد ٤٦، العدد ١، ٢٠١٩، ص٤٦٩ ؛ ويراجع: المادة (٤٦) من بروتوكول ١٩٧٧ الملحق باتفاقية جنيف لعام ١٩٤٩.

ثانياً: تعريف التجسس الإلكتروني: لا يختلف التجسس الإلكتروني عن التجسس العام إلا في الأداة المستخدمة وهي تكنولوجيا المعلومات التي وفرت للجاسوس الإلكتروني الحرية والسهولة في التجسس بعيداً عن أعين الرقيب، فقد عرف بأنه:"دخول الجاني إلى الشبكة المعلوماتية أو نظام المعلومات أو موقع إلكتروني للحصول على محتوى إلكتروني غير متاح للجمهور يمس الأمن الوطني أو العلاقات الخارجية للدولة أو السلامة العامة أو الاقتصاد الوطني"(١)، وعرف أيضا بأنه:"استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الإلكترونية الخاصة بالدول والحكومات والتنصت عليها بقصد الحصول على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها، تشمل جميع المعلومات العسكرية والأمنية والسياسية والاقتصادية والعلمية والاجتماعية"(٢)، كما عرف التجسس الإلكتروني أو ما يعرف بحرب التجسس المعلوماتي بأنه:"عبارة عن عدة طرق لاختراق المواقع الإلكترونية ومن ثم سرقة بعض المعلومات التي قد تكون في قائمة الأهمية والخطورة للطرف المتلقي والمسروق منه"(٣).

والملاحظ من التعاريف السابقة اتفاقها من حيث المضمون وان اختلفت في ألفاظها، الا انه يمكن لنا بالاستناد اليها والى النصوص الجزائية التي تناولت الجريمة، سواء في مشروع قانون جرائم المعلوماتية العراقي لسنة ٢٠١١ والقوانين المقارنة تحديد العناصر الأساسية التي يقوم عليها التجسس الإلكتروني، وهذه العناصر هي:

(١) ينظر: عطوة مضعان مسلم أبو غليون، الجرائم الإلكترونية بين الشريعة الإسلامية والقوانين الوضعية، رسالة ماجستير، كلية الدراسات العليا، الجامعة الأردنية، ٢٠٠٩، ص٦٥.

(٢) ينظر: د. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة/ دراسة مقارنة، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٣، ص٥٦٩.

(٣) تجسس إلكتروني، منشور على موقع الانترنيت https://ar.wikipedia.org/wiki تاريخ الزيارة ١٧/ ٥/ ٢٠١٩.

١- إن التجسس الإلكتروني لا يتم إلا باستخدام وسيلة من وسائل تقنية المعلومات الحديثة، سواء أكانت حاسب ألي أم نظام معلوماتي أم موقع أم شبكة إلكترونية أو معلوماتية.. الخ.

٢- إن محل التجسس الإلكتروني هو محتوى إلكتروني لا يتاح للجمهور استخدامه أو الاطلاع عليه، فمعظم الدول إن لم يكن جميعها تحتفظ في الوقت الحاضر بوثائقها السرية مخزنة بهيئة رقمية في مزودات سرية.

٣- إن الغاية من التجسس الإلكتروني هي الوصول أو الحصول بطريقة غير مشروعة على بيانات أو معلومات سرية بطبيعتها أو بحكم القانون، ويستوي في هذا الصدد ان يكون الحصول على البيانات أو المعلومات قد تم عن طريق الاستخدام غير المشروع لأجهزة الحاسب الالي وبرامجه وانظمته والمواقع وشبكات الإلكترونية أو المعلوماتية، كما ويستوي أن تكون البيانات أو المعلومات تتعلق بالجانب العسكري أو السياسي أو التجاري أو الصناعي أو الاجتماعي، إذ إن التجسس الإلكتروني لم يعد يقتصر على الجانب العسكري، وان كانت هذه الصورة تمثل أهم صور التجسس واخطره، وإنما تعداه إلى الحياة الخاصة وإلى النشاط التجاري والصناعي، بل إن التجسس في صورته الأخيرة أصبح يشكل أهمية قصوى للجهة التي تتجسس نتيجة للأسرار البالغة الحساسية والأهمية التي يحتفظون بها، فضلاً عن أن الكثير من الجماعات الإرهابية أصبحت تعول على المعلومات الشخصية للأفراد في سبيل استقطابهم وتجنيدهم ضمن تنظيماتهم وجماعاتهم الإرهابية [١].

ومن الجدير بالذكر أن ظاهرة التجسس الإلكتروني قد انتشرت مع نهاية القرن العشرين وبداية الألفية الجديدة نتيجة للثورة التكنولوجية والمعلوماتية في مجال المعلومات والاتصالات، إذ تغيرت وسائل وأساليب التجسس من الطرق التقليدية إلى الطرق الإلكترونية، لاسيما مع الانتشار الواسع لاستخدام الشبكة المعلوماتية (الإنترنت)

(١) ينظر: علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في القانون العماني مقارنة بالشريعة الإسلامية والقانون الجنائي الدولي، المؤتمر الدولي الأول، العلوم الشرعية، تحديات الواقع وأفاق المستقبل، ٢٠١٨، ص١٢٧٥.

على المستوى العالمي، ولا يقتصر خطر التجسس على اختراق الشبكات والأنظمة والمواقع الإلكترونية للوصول إلى البيانات أو المعلومات الموجودة بها على فئة العابثين من مخترقي الأنظمة أو ما يعرفون اصطلاحا"HACKERS"أو منظمات عالم الإنترنت السفلي التي تحاول بشكل مستمر اختراق الأنظمة الشبكات والمواقع الموجودة في العالم اجمع، إذ إن المخاطر الناشئة عن عمل هذه الفئة محدودة وتقتصر في الغالب على العبث أو إتلاف البيانات أو المعلومات، والتي يمكن التغلب عليها عن طريق عمل نسخ احتياطية للبيانات والمعلومات [١].

وإنما يكمن الخطر في عمليات الاختراق التي تنفذها الأجهزة الاستخبارية للحصول على أسرار أو معلومات الدولة، ومن ثم إفشائها لدول أخرى تكون عادة معادية لها، أو استغلالها بالشكل الذي يضر بالمصالح الوطنية للدولة الذي يتجسس عليها كالاختراق الذي حدث لموقع وزارة الدفاع الأمريكية البنتاغون في العامين الماضيين، واختراق موقع وزارة الدفاع الفرنسية لغرض سرقة معلومات عن الاستطلاعات والمناورات والنظام الصاروخي الفرنسي [٢]، وكذلك ما تتعرض له مصادر المعلومات السرية المتعلقة بأنشطة الشركات والمؤسسات التجارية والصناعية التي يترتب على التجسس عليها تكبدها لخسائر مالية جسيمة، فضلا عن الأضرار المعنوية والأدبية.

المطلب الثاني: صور التجسس الإلكتروني ووسائله

للتجسس الإلكتروني صور متعددة تهدف جميعها إلى الحصول على المعلومات التي لا يتاح للجمهور الاطلاع عليها كما أن له وسائله المستحدثة التي تتفق مع طبيعة الجريمة، ويمكن بيان ذلك على النحو الآتي:

أولاً: صور التجسس الإلكتروني: نوضح فيما يلي أهم صور التجسس الإلكتروني وكالآتي:

(١) ينظر: د.حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت / دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٩، ص٣٧٣-٣٧٤.
(٢) تجسس إلكتروني، مصدر سابق.

١- التجسس العسكري: يعد التجسس العسكري أول أنواع التجسس واقواه، فكل دولة تسعى للحصول على المعلومات المتعلقة بالجيوش والأجهزة العسكرية والخطط الحربية والأسلحة والصواريخ والذخائر والتجهيزات والمواقع والعدة العسكرية، هذه المعلومات تتعلق بالجانب الأمني والاستراتيجي للبلاد وتعد أكثر المعلومات حساسية وسرية في أي دولة(١). وقد أعطت العديد من الدول للتجسس العسكري رعاية مميزة من خلال رصد الأموال، وإنشاء دوائر ومكاتب مختصة بشؤون التجسس، وتدريب الجواسيس، وتنظيم شبكات التجسس بصورة علمية دقيقة، ولا يقتصر التجسس العسكري على زمن الحرب بل ينشط أيضاً في زمن السلم تحسباً للحرب وتوخياً لتحقيق المخططات العسكرية.

٢- التجسس الاقتصادي: يهدف التجسس الاقتصادي إلى الوقوف على حقيقة المقدرات الاقتصادية للدول الأخرى سواء أكانت دولة معادية أم دولة صديقة، لمعرفة مواردها وثرواتها ووضعها المالي والنقدي ومستوى تجارتها وصناعتها وزراعتها وطرق استثمارها وتجارتها الخارجية، وهذه مما تفيد العدو في تهيئة أسباب الحصار الاقتصادي والتجارة وتنظيمه، كما تفيد في الاستيلاء على مرافق البلاد العامة عند الاحتلال، والإفادة من ثرواتها المدخرة وتنظيم عمليات المصادرة(٢).

٣- التجسس العلمي: يهتم التجسس العلمي بالاطلاع على الأسرار كافة من بحوث ودراسات واختراعات علمية قد تكون عسكرية وصناعية وغيرها، بهدف سرقتها أو بهدف اتخاذ الاحتياطات اللازمة لمواجهتها(٣).

٤- التجسس السياسي: يهدف التجسس السياسي إلى معرفة المواقف السياسية والقوة المؤثرة في البلاد واتجاه قادتها ومبادئ ورأي كل منهم ومعرفة مواطن القوة والضعف بين أبناء البلاد والخلافات التي تجري بين الأحزاب والمنظمات ومدى

(١) ينظر: د. علي جعفر، مصدر سابق، ص٥٧٠.
(٢) ينظر: د. محمد الفاضل، الجرائم الواقعة على امن الدولة، ج١، ط٣، بلا مكان طبع، دمشق، ١٩٥٨، ص٢٩٥.
(٣) ينظر: د. علي جعفر، المصدر السابق، ص٥٧١.

ثقة الشعب بقادتها وغيرها من الأمور التي تتعلق بالدولة[١]، فالتجسس السياسي قد يكون معنوياً ونفسياً، فالحرب المعنوية من أهم الحروب فمن خلال هذه المعلومات تستطيع الدولة المعادية استخدام السلاح المعنوي وتحطيم الروح المعنوية للشعب مما يسهل عليها كسب المعركة[٢]. بمعنى أن التجسس السياسي لا يقل خطورة عن أنواع التجسس الأخرى، فهو يرمي إلى مراقبة أوضاع وأسرار سياسات الدول الأخرى، إن على الصعيد الداخلي أو على الصعيد الخارجي.

٥- التجسس الدبلوماسي: هو أحد صور التجسس يقوم بممارسته أفراد البعثات الدبلوماسية دون إخفاء صفاتهم الدبلوماسية وذلك عن طريق جمع المعلومات السرية بوسائل غير قانونية مستغلين الوضع الإيجابي الذي تكونون فيه نتيجة تمتعهم بالحصانات والامتيازات الدبلوماسية، ومستعينين على الأغلب بالوسائل الدبلوماسية كمقر البعثة الدبلوماسية والحقيبة الدبلوماسية وغيرها[٣]. ويمكن تصنيف التجسس الدبلوماسي ضمن التجسس وقت السلم على أساس إن العلاقات الدبلوماسية بين الدولتين الموفدة والمضيفة تقطع بمجرد نشوب الحرب بينهما[٤].

ثانيا: وسائل التجسس الإلكتروني: في ظل التقدم العلمي والتكنولوجي والمعلوماتي حدث تغير كبير في وسائل وأساليب التجسس على الدول والأشخاص بحيث تعددت وسائله لتواكب زمن المعلوماتية، منها ذات تقنية عالية الجودة، ومنها صغيرة الحجم جداً، ومنه ما يبدو على هيئة أشياء نستخدمها في حياتنا تصلح للتجسس الإلكتروني، ومن ابرز هذه الوسائل والأساليب ما يلي:

١- نظام إيكيلون "Echelon" وهو نظام تجسسي عالمي لرصد البيانات واعتراضها ونقلها، أنشأته وكالة الأمن القومي الأمريكية، وتقوم بتشغيله بالتعاون مع

(١) ينظر: سعد إبراهيم الاعظمي، مصدر سابق، ص٢٤.
(٢) ينظر: د. محمد الفاضل، المصدر السابق، ص٢٩٤.
(٣) ينظر: محمد عدنان عثمان، دور القانون الدولي في مواجهة التجسس الدبلوماسي، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٥، ص٨.
(٤) ينظر: عبد الرحمن لحرش، التجسس والحصانة الدبلوماسية، بحث منشور في مجلة الحقوق، جامعة الكويت، العدد ٤، السنة ٢٧، ٢٠٠٣، ص١٨٠.

المؤسسات الاستخبارية في المملكة المتحدة وكندا وأستراليا ونيوزلندا، ونظام إيكيلون المستخدم حالياً ابتدأ العمل به منذ عام ١٩٤١، وهو يقوم بالتجسس على الاتصالات الهاتفية السلكية واللاسلكية والإلكترونية المدنية والعسكرية في العالم، وتستخدم شبكة الإنترنيت ومجموعة من الأقمار الصناعية الخاصة به وكابلات بحرية مغلقة لهذا النظام تمتد عبر المحيطات لنقل الاتصالات إلى المركز الرئيسي، وقد ضجت عشرات الدول الأوروبية والأمريكية بالشكوى من هذا النظام لأنه يمثل تجسساً إلكترونياً أمريكياً مستمراً عليها، تستبيح معلوماتها وأسرارها وأنظمتها واتصالاتها المدنية والعسكرية بما يؤثر على حياة شعوب تلك الدول تأثيرا شديداً[١].

٢- برنامج بريزم "Prism"وهو برنامج تجسس رقمي مصنف بأنه سري للغاية يشغل من قبل وكالة الأمن القومي الأمريكية، وأعتبر هذا البرنامج أحد البرامج التجسسية الضخمة الذي يتيح لوكالة الأمن القومي الأمريكي عبر جمع وتحليل المعلومات، الوصول المباشر إلى خوادم الإنترنيت الكبرى للتنصت واعتراض اتصالات الهواتف الذكية والحصول على رسائل البريد الإلكترونية والمحادثات دون حاجة للطلب من مقدمي تلك الخدمات ودون الحصول على أوامر قضائية، ويعمل هذا البرنامج منذ عام ٢٠٠٧ طبقاً لاتفاق مع عمالقة شركات الاتصالات، إذ إن ياهو وغوغل ومايكروسوفت وسكاب وآبل وفيس بوك وبالتورك تؤمن مدخلاً خلفياً للوكالة إلى كل اتصال يتم عبرها[٢].

٣- لمبات تجسس: أحبطت جمارك طرود البريد السريع بقرية البضائع بمطار القاهرة الدولي، محاولة تهريب لمبات تجسس، مزودة بكاميرات تصوير دقيقة لأغراض

(١) ينظر: محمد عدنان عثمان، المصدر السابق، ص٣٩.
(٢) ينظر: راجح الخوري، كوكب الجواسيس، مقالة منشورة في جريدة الشرق الأوسط، العدد ١٢٨٤٨، ٢٠١٤، ص٣١.

التجسس قادمة من هونج كونج داخل طرد شخصي لتضليل رجال الجمارك ولاستخدامها في أغراض تجسس من نوع لِيَد[١].

٤- ميدالية بكاميرا تشبه ريموت السيارة: كما تمكن رجال الجمارك بمطار القاهرة الدولي، من إحباط محاولة راكبة ليبية من تهريب ٤ أجهزة لاسلكي و٣ أجهزة تنصت دقيقة توضع فيها شريحة هاتف محمول تستخدم للتسجيل الصوتي، وميدالية بكاميرا تشبه ريموت السيارة، وزي شبيه بزي الجيش المصري[٢].

٥- فلاش كمبيوتر: الجهاز يقوم بالتنصت وتسجيل الصوت لفترات طويلة جدا، وهو مخفي بشكل فلاش كمبيوتر غير ملفت للنظر تماما، ولا يصدر عنه أي صوت أو إضاءة أثناء عمله، والفلاش مزود بميكروفونات دقيقة وحساسة جدا تلتقط الصوت بكل وضوح داخل المكان الموضوع به الفلاش سواء السيارة أو الغرفة أو المكتب أو أي مكان آخر، ومساحة ذاكرة الفلاش ٨ جيجا[٣].

٦- لاقط للصوت من المسافات البعيدة: الجهاز عبارة عن سماعة تنصت لاقط حساس جدا للصوت، تقوم بالتقاط الأصوات بوضوح على مسافة ٥٠ مترا، ويُعد أحدث جهاز تنصت عن بعد واختراق الحواجز، ويمكن السماع بوضوح لكل ما يقال حتى وإن كان المكان بعيد[٤].

وتجدر الاشارة إلى أن هناك عدة طرق للحماية من التجسس الإلكتروني أو التقليل من المخاطر المترتبة عليه، كاستخدام تقنية (MAC ADDRES) عوضاً عن (IP ADDRESS) لحماية الشبكات اللاسلكية الداخلية، لأنه يصعب اختراقها ويستطيع مدير الشبكة من خلالها تحديد عدد الأجهزة المصرح لها بالاتصال واستخدام الشبكة، وتشفير البيانات باستخدام تقنية (WIRED EGUIVALENT)، وكذلك

(١) سباق التجسس الإلكتروني وزعزعة النظام العالمي، ٢٠١٧، منشور على موقع الانترنيت https://annabaa.org/arabic/informatics/13571تاريخ الزيارة ٢٠١٩/٧/٩.

(٢) غزلان جلال، احدث اجهزة التجسس الإلكتروني، ٢٠١٥، منشور على موقع الانترنيت https://machahid24.com/panorama/73838.html تاريخ الزيارة ٩/٧/ ٢٠١٩.

(٣) سباق التجسس الإلكتروني وزعزعة النظام العالمي، المصدر السابق.

(٤) ينظر: غزلان جلال، المصدر السابق.

استخدام بعض برامج مكافحة التجسس الإلكتروني الشهيرة من ذلك: (SPYWARE BLASTER) الذي لا يقتصر دوره فقط على القضاء على برامج التجسس الإلكتروني، بل يقوم بدور المراقب لمنع أية ملفات تجسس من اقتحام الجهاز أو الشبكة، ومثل برنامج (AD AWARE) الذي يعد من اشهر برامج مكافحة التجسس، حيث يقوم بإزالة ملفات التجسس غير المرغوب فيها مباشرة، وأيضا برنامج (WEBROOT SPY SWEEPER) وهو من أقوى البرامج لمكافحة التجسس الإلكتروني حيث يقوم بمراقبة وإزالة ملفات التجسس، كما يقوم بإعطاء شرح موجز عن خطورة الملف المضبوط قبل مسحه نهائيا، فضلا عن إتباع كافة الاحتياطات الأمنية المعهودة لحماية سرية البيانات أو المعلومات من ذلك: تثبيت برامج الحواط النارية، وعدم الاتصال بالنقاط المجانية والابتعاد عن مشاركة الملفات قدر الإمكان، وضبط الملفات السرية وإحاطتها بكلمة مرور قوية، وقطع الاتصال بالشبكة اللاسلكية قبل غلق أجهزة الحاسب الآلي، والحرص على عمل تحديات الأمان باستمرار [١].

المطلب الثالث: تمييز التجسس الإلكتروني عما يشتبه به

للتجسس الإلكتروني ذاتيته الخاصة التي تميزه عما قد يشتبه به من مفاهيم أخرى، ونبين فيما يلي أهم أوجه الشبه والاختلاف بين التجسس الإلكتروني وما يختلط به من مفاهيم كالإرهاب الإلكتروني والقرصنة الإلكترونية، وعلى النحو الآتي:

أولاً: تمييزه عن الإرهاب الإلكتروني: الإرهاب بشكل عام هو استخدام العنف أو التهديد به ضد مجموعة من الأفراد بهدف إرعابهم وتخويفهم، ويتعدى ذلك الخوف والإرعاب إلى أشخاص آخرين، وكل ذلك من اجل تحقيق هدف محدد [٢]، أما

(١) للتفصيل ينظر: علي بن محمد بن سالم العدوي، مصدر سابق، ص١٢٨٦ ؛ أسامة الكسواني، التجسس الإلكتروني وطرق مكافحته، منشور على موقع الانترنيت، http://alqabas. Com. تاريخ الزيارة ٢٠١٩/٦/٢١.

(٢) للتفصيل في تعريف الإرهاب ينظر: عامر مرعي حسن، جرائم الإرهاب في القانون الجنائي / دراسة مقارنة، رسالة ماجستير، معهد البحوث والدراسات العربية، جامعة الدول العربية، القاهرة، ٢٠٠٨، ص٥٢-٧٢.

الإرهاب الإلكتروني فيراد به "كل نشاط إجرامي مخطط ومنظم مخالف للقانون باستخدام وسائل التقنية الإلكترونية الرقمية لتحقيق غرض معين"[١].

وقد اتخذ الإرهاب الإلكتروني أبعادا جديدة وأفاقا أرحب مع تطور وسائل تقنية المعلومات الحديثة ووسائل الاتصالات، إذ يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على الشبكة المعلوماتية لبث أفكارهم والدعوة إلى مبادئهم والتعبئة الفكرية وتجنيد الارهابين الجدد، وإعطاء التعليمات والتلقين والتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن الهجمات الإرهابية، حيث بات التقاء الارهابين لتعلم الإجرام وكيفية تنفيذ الأعمال الإرهابية وتبادل الآراء والأفكار والمعلومات بخصوصها أكثر سهولة بوجود الشبكات الإلكترونية [٢].

ومما تقدم يتضح إن كلاً من التجسس الإلكتروني والإرهاب الإلكتروني يعتمد على استخدام وسائل تقنية المعلومات الحديثة كأجهزة الحاسب الآلي وبرامجه وأنظمته والشبكة المعلوماتية في ارتكاب أفعالهم الجنائية، كما إن كلا منهما قد يقوم به فرد أو تنظيم أو دولة ما للوصول إلى غرض إجرامي محدد، فضلا عن إن كلا منهما يعد جريمة عابرة للحدود والدول والقارات وغير خاضعة لنطاق إقليمي محدد [٣]، إلا انه يمكن التمييز بينهما من حيث:

١- **الهدف أو الغرض منهما:** الإرهاب الإلكتروني هدفه النيل من الوحدة الوطنية وتعريض امن وسلامة المجتمع وحياة المواطنين وحرياتهم ومقدساتهم للخطر بغية تحقيق مارب سياسية أو فكرية أو دينية أو طائفية أو عنصرية [٤]. بينما الهدف من التجسس الإلكتروني الحصول على أسرار ومعلومات تتعلق بالدولة أو

(١) ينظر: د. مصطفى محمد موسى، الإرهاب الإلكتروني، ط١، دار الكتب والوثائق القومية المصرية، القاهرة، ٢٠٠٩، ص١٧٣.
(٢) ينظر: د. علي جعفر، مصدر سابق، ص٥٨٨.
(٣) ينظر: د. فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، ط ٢، بلا مكان طبع، ٢٠١٠، ص٣٧٧.
(٤) يراجع: المادة (١) من قانون مكافحة الإرهاب العراقي رقم (١٣) لسنة ٢٠٠٥.

مؤسساتها أو الشركات التابعة لها، ومن ثم إفشائها أو استغلالها بما يضر المصلحة العامة والوحدة الوطنية للدولة(١).

٢- **الأساليب المتبعة في كل منهما:** الإرهاب الإلكتروني يعتمد على أسلوب إنشاء وإدارة المواقع الإلكترونية تحت مسميات وهمية على الشبكة المعلوماتية والتي يتم من خلالها تجنيد وتدريب الارهابين والتواصل مع بعضهم البعض بأساليب متقدمة، فضلا عن إثارة الرأي العام والترويج لأفكارهم ونشر العمليات الإرهابية، سواء المنفذة منها أم تلك التي تتضمن عمليات تصنيع وإعداد الأجهزة المتفجرة أو الحارقة أو أي مواد أو أدوات أخرى تستخدم في التخطيط لهذه الأعمال أو تنفيذها(٢)، في حين إن التجسس الإلكتروني يعتمد على الاستخدام غير المشروع لأجهزة الحاسب الآلي وبرامجه وأنظمته ونظم المعلومات والشبكات الإلكترونية للوصول إلى البيانات أو المعلومات، فضلا عن التنصت على البيانات أو المعلومات أو التقاطها أو اعتراضها دون وجه حق، إذ انه يتم في الخفاء وعن طريق الخداع أو التنكر (٣).

ثانياً: تمييزه عن القرصنة الإلكترونية: يقصد بالقرصنة الإلكترونية، النسخ الغير مشروع لنظم التشغيل للحاسب والدخول غير المشروع بقصد تدمير المواقع الإلكترونية وكل من فك أو نزع أو اتلف تشفيرا لتوقيع إلكتروني أو أجهزة الحاسوب أو شبكة المعلومات(٤)، فالتجسس الإلكتروني والقرصنة الإلكترونية كلاهما عبارة عن ممارسات غير مشروعة تتم عبر الشبكة المعلوماتية-الانترنيت-وتستهدف

(١) ينظر: مصطفى محمد موسى، مصدر سابق، ص١٧٨.

(٢) ينظر: عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي الأول، بعنوان "حماية امن المعلومات والخصوصية في قانون الانترنيت، المنعقد بالقاهرة في المدة ٢-٤ يونيو-٢٠٠٨، ص١٣؛ د. فتحي محمد أنور عزت، المصدر السابق، ص٣٨٤.

(٣) ينظر: علي عدنان الفيل، الإجرام الإلكتروني / دراسة مقارنة، ط١، منشورات زين الحقوقية، بيروت، لبنان، ٢٠١١، ص٦٠.

(٤) ينظر: كاظم عبد جاسم الزيدي، مكافحة الجرائم المعلوماتية في التشريع العراقي، ٢٠١٢، منشور على موقع الانترنيت https://www.hjc.iq/view.1645/ تاريخ الزيارة ٨/٦/ ٢٠١٩.

المعلومات الموجودة في أجهزة الحاسب الآلي[١]، إلا انه يمكن التفريق بينهما من حيث:

١- **الجهة المنفذة:** القرصنة عادة يتم تنفيذها من قبل الهواة العابثون من محترفي الأنظمة المعلوماتية الذين يبحثون عن التسلية أو إثبات قدراتهم أو العبث وإتلاف المحتويات التي يمكن التغلب عليها من خلال استعادة نسخة أخرى من البرنامج مخزونة في مكان آمن، في حين التجسس الإلكتروني يقتصر في الغالب على التنظيمات الإرهابية وأجهزة الاستخبارات التي تسعى للحصول على المعلومات والأسرار المتعلقة بدولة ما بشتى الطرق من اجل استغلالها بما يضر مصلحة تلك الدولة أو بيعها لدولة معادية لها[٢].

٢- **مقدار الخطر**:إن مقدار الخطر يكون اشد وحجم الضرر في التجسس الإلكتروني اكبر وبالتالي لا توصف القرصنة الإلكترونية إرهابا كما يوصف بها التجسس الإلكتروني، حيث إن القرصنة عندما بدأت لم يأخذ الطابع الشرير في بدية الأمر بل العكس كانت تطلق على من لديه عبقرية في ابتكار برامج سريعة ومدهشة في أنظمة الحواسيب، إلا إن الأمر اتجه إلى الجانب السلبي في وقتنا الحاضر[٣].

المبحث الثاني

أركان جريمة التجسس الإلكتروني والعقوبة المقررة لها

في عصر المعلومات وبفعل وجود تقنيات عالية التقدم فقد تبدل نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها ومنها نمط الجريمة التي قد يحتفظ بعضها باسمها التقليدي مع تغيير بسيط أو جوهري في طرق أو وسائل ارتكابها، ومن هذه الجرائم الحديثة في طرقها ووسائلها والقديمة في اسمها جريمة التجسس الإلكتروني التي أخذت أشكال حديثة تتماشى مع التطور التقني وتغير وتطور الأساليب التي يحاول من

(١) ينظر: علي بن محمد بن سالم العدوي، مصدر سابق، ص١٢٧٥.
(٢) ينظر: محمد الحسن، القرصنة الإلكترونية تاريخ من الأخطار، مجلة التقدم العلمي، العدد٩٩، ٢٠١٧، ص٣٤.
(٣) ينظر: مأمون حرب، امن المعلومات في فضاءات انترنيت الأشياء، مجلة التقدم العلمي، العدد ٩٩، ٢٠١٧، ص١٢.

خلالها الجواسيس الوصول إلى أهدافهم، ومن هذا المنطلق فقد اتجه المشرع في العديد من الدول إلى تجريم التجسس على البيانات والمعلومات الإلكترونية ومن ضمنها المشرع العراقي في مشروع قانون جرائم المعلوماتية، عليه سنقسم هذا المبحث إلى مطالب ثلاثة وكالآتي:

المطلب الأول: الركن المادي لجريمة التجسس الإلكتروني

تبدو أهمية الركن المادي في الجريمة من حيث انه لا يمكن أن توجد جريمة بغير الركن المادي لها، فهو مادياتها أي ما يدخل في كيانها وتكون له طبيعة مادية ملموسة، وبغير هذه الماديات لا يمكن أن يصيب المجتمع أضرار أو يوجد اعتداء على الحقوق أو المصالح التي يحميها القانون، ويتكون الركن المادي من عناصر ثلاثة هي: الفعل "السلوك الإجرامي" والنتيجة الإجرامية والعلاقة السببية، والعنصر الأخير لا يثير صعوبات في هذا الصدد، لذا سنتناول العنصريين الأول والثاني وعلى النحو الآتي:

أولا: السلوك الإجرامي: تفترض الجريمة ارتكاب فعل محظور جنائيا يقوم به الركن المادي للجريمة، ويطلق على هذا الفعل تعبير السلوك الإجرامي، وهذا السلوك هو النشاط المادي الذي يرتكبه الجاني وبدونه لا توجد الجريمة، وقد عالج المشرع العراقي جرائم التجسس الإلكتروني في المواد (٣ / ثانيا) و(١٥) و(١٦) من مشروع قانون الجرائم المعلوماتية [١]، ومن خلال استقراء النصوص المتقدمة يتبين إن السلوك الإجرامي الذي تتحقق به الجريمة يتخذ أحد الصور الآتية:

(١) تجدر الإشارة إلى أن المشرع العراقي جرم التجسس بصورته العامة في الباب الأول من الكتب الثاني من قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل، إذ عاقب كل من سعى لدى دولة أجنبية أو تخابر معها أو مع أحد ممن يعملون لمصلحتها للقيام بأعمال عدائية ضد العراق قد تؤدي إلى الحرب أو إلى قطع العلاقات الدبلوماسية أو دبر لها الوسائل المؤدية إلى ذلك (المادة ١٥٨)، وكذلك كل من سعى لدى دولة أجنبية معادية أو تخابر معها أو مع أحد ممن يعملون لمصلحتها لمعاونتها في عملياتها الحربية ضد العراق أو للإضرار بالعمليات الحربية لجمهورية العراق= =وكل من دبر لها الوسائل المؤدية إلى ذلك أو عاونها بأي وجه على إنجاح عملياتها الحربية (المادة ١٥٩)، كما عاقب من سعى لدى دولة أجنبية أو لدى أحد ممن يعملون لمصلحتها أو تخابر مع أي منهما وكان من شان ذلك الإضرار بمركز العراق الحربي أو السياسي أو الاقتصادي (المادة ١٦٤)، أو سعى للحصول بأي وسيلة على شيء يعتبر من أسرار الدفاع عن البلاد بقصد

أولا: الاستخدام غير المشروع لأجهزة الحاسوب وبرامجه أو أنظمته أو شبكة المعلومات التابعة للجهات الأمنية أو العسكرية أو الاستخبارية: نصت على هذه الصورة من صور السلوك الإجرامي المحققة لجريمة التجسس الإلكتروني المادة (٣ / ثانيا) من مشروع قانون الجرائم المعلوماتية العراقي لسنة ٢٠١١، التي جاء فيها: "يعاقب.... كل من استخدم عمدا أجهزة الحاسوب وبرامجه أو أنظمته أو شبكة المعلومات التابعة للجهات الأمنية أو العسكرية أو الاستخبارية بقصد الإضرار بها أو النسخ منها أو بقصد إرسال محتواها لجهة معادية أو الاستفادة منها لتنفيذ جرائم ضد امن الدولة الداخلي أو الخارجي، أو تسهيل إخفاء معالم تلك الجرائم أو تغطيتها"[١].

ويشترط لتحقق الجريمة قيام الجاني باستخدام أحد أجهزة الحاسب الآلي وبرامجه أو أنظمته أو شبكة المعلومات التابعة للجهات الأمنية أو العسكرية أو الاستخبارية، وقد استعمل المشرع للتعبير عن هذه الصورة مصطلح (الاستخدام) على خلاف القوانين المقارنة التي استعملت مصطلح (الدخول غير المشروع أو غير المصرح به).

ونرى إن مصطلح الاستخدام الذي استعمله المشرع العراقي أدق واعم من مصطلح الدخول غير المشروع، إذ انه لا يثير اللبس والغموض حول تحديد المقصود به على خلاف الدخول غير المشروع الذي لا زال محل خلاف حول تحديد المقصود به على مستوى القوانين التي عرفته ومنها القانون السعودي الذي عرفه في المادة (١ / ٧) بأنه: "دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام

إتلافه لمصلحة دولة أجنبية، أو إفشائه لها أو لأحد ممن يعملون لمصلحتها (المادة ١/١٧٧)، وكل من سلم أو أفشى سرا من أسرار الدفاع إلى دولة أجنبية أو لأحد ممن يعملون لمصلحتها (المادة ٢/١٧٧)، أو أتلف لمصلحة دولة أجنبية وثائق أو أشياء أخرى تعتبر من أسرار الدفاع عن البلاد أو جعله غير صالح لأن ينتفع به (المادة ١٧٧/ ٣). كذلك عاقب كل من أذاع إشاعات كاذبة ومغرضة أو عمد إلى دعاية مغرضة أو مثيرة وكان من شان ذلك إلحاق ضرر بالاستعدادات الحربية للدفاع عن البلاد أو بالعمليات الحربية للقوات المسلحة أو إثارة الفزع بين الناس أو إضعاف الروح المعنوية في الأمة نتيجة الاتصال مع دولة أجنبية (المادة ١٧٨).

(١) يقابلها نص المادة (٤) من قانون مكافحة جرائم تقنية المعلومات الإماراتي الاتحادي رقم ٥ لسنة ٢٠١٢، والمادة (٧ /٢) من نظام الجرائم المعلوماتية السعودي، والمادة (٣) من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥، والمادة (٢) من قانون مكافحة الجرائم الإلكترونية القطري رقم ١٤ لسنة ٢٠١٤.

معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها"، وكذلك القانون الكويتي، إذ عرفت المادة (١) منه الدخول غير المشروع بأنه: "النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو النظام المعلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح".

أو على مستوى الفقه الذي قدم تعريفات عديدة للدخول غير المشروع، إذ عرف بأنه: "كافة الأفعال التي تسمح بالولوج إلى نظام معلومات إلكتروني"[١]، كما عرف بأنه: "توجيه هجمات إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية (Confidentiality)، أو المساس بالسلامة والمحتوى والتكاملية (Integrity)، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها (Availability)"[٢]، كما عرف بالقياس على فكرة انتهاك حرمة الأماكن في العالم الواقعي وتطبيقها على انتهاك حرمة المحل المحمي في حال الدخول غير المشروع للعالم الافتراضي بأنه: "النشاط الإيجابي الذي يمكن الفاعل من التواجد داخل النظام أو أي من أجزائه، طالت المدة أم قصرت، تحققت له السيطرة على النظام أم لا"[٣].

كما إن مصطلح الاستخدام يتسع ليشمل الحالات التي يتمكن فيها الجاني أو الفاعل من استعمال أجهزة الحاسب الآلي أو برامجه أو أنظمته أو شبكة المعلومات، سواء أكان الجاني من الأشخاص المصرح لهم باستخدام تلك الأجهزة أم كان من الأشخاص غير المصرح لهم بذلك على خلاف الدخول غير المشروع، إذ إن مجرد الدخول إلى نظام المعلومات الإلكتروني لا يعد فعلا غير مشروع، وإنما يستمد الفعل عدم مشروعيته من كونه غير مصرح به، أي أن يكون الدخول قد تم دون وجه حق، فمناط عدم المشروعية في حال الدخول تتأتى من انعدام سلطة الجاني في الدخول إلى هذا النظام مع علمه بذلك، والتي تتحقق في حالتين الأولى: أن يكون الدخول إلى

(١) ينظر: د. علي جعفر، مصدر سابق، ص٤١٤.
(٢) ينظر: د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩، ص٢٤٢.
(٣) ينظر: عبد الإله محمد النوايسة، ممدوح حسن العدوان، مصدر سابق، ص٤٧٤.

النظام قد تم دون الحصول على تصريح من المسؤول عن النظام، والثانية: أن يكون الدخول إلى النظام قد تم من شخص لديه تصريح بالدخول إلا انه تجاوز حدود التصريح الممنوح له[١].

وصفوة القول إن فكرة الاستخدام – الاستعمال – تختلف عن فكرة الدخول، لان دائرة الاستخدام أوسع من دائرة الدخول، فكل استخدام لنظام معلوماتي دون رضاء صاحبه يمثل دخولا بلا شك فيه، بينما الدخول لا يعني بالضرورة استخدام النظام، فقد يتصل الشخص بالنظام ومن ثم يكون قائما بالدخول فيه ولكنه لا يستعمل إمكانيات النظام، كأن يكتفي بالاطلاع على النظام بوسائل سلكية أو بوسائل غير سلكية أو باستعمال برامج خاصة بالاقتحام والجاني يكتفي عندئذ بالاطلاع دون استخدام النظام[٢].

ويشترط لتحقق الاستخدام أن يكون لأحد أجهزة الحاسب الآلي وبرامجه أو أنظمته أو شبكة المعلومات ولكل منها مفهوم فني يختلف عن الأخر، فالحاسب الآلي أو بحسب تعبير المشرع (الحاسوب) يراد به "كل جهاز أو مجموعة أجهزة مترابطة بعضها مع بعض تقوم بعمليات المعالجة الآلية للبيانات"[٣]، أما البرامج فهي "مجموعة الأوامر التي تجعل النظام قادرا على أداء عمليات المعالجة الآلية للبيانات"[٤]، بينما يراد بنظام معالجة المعلومات "النظام الإلكتروني المستخدم لإنشاء رسائل المعلومات أو إرسالها أو تسلمها أو معالجتها أو تخزينها على أي وجه"[٥]، في حين يقصد بشبكة المعلومات "مجموعة من أجهزة الحاسوب أو أنظمة معالجة المعلومات مترابطة مع بعضها البعض للحصول على البيانات والمعلومات وتبادلها كالشبكات الخاصة والعامة والشبكة العالمية لخدمات المعلومات (الإنترنت) وما في حكمها"[٦].

(١)ينظر:د.علي جعفر، المصدر سابق، ص٤١٤ ؛ د.حسين بن سعيد الغافري، مصدرسابق، ص٣٤٩
(٢) ينظر: د. خالد ممدوح إبراهيم، مصدر سابق، ص٢٥٠-٢٥١.
(٣) يراجع: المادة (١/ أولا) من مشروع قانون الجرائم المعلوماتية الخاصة بالتعاريف والأهداف.
(٤) يراجع: المادة (١/ رابعا) من مشروع قانون الجرائم المعلوماتية الخاصة بالتعاريف والأهداف.
(٥) يراجع:المادة(١/رابع عشر) من مشروع قانون الجرائم المعلوماتية الخاصة بالتعاريف والأهداف.
(٦) يراجع: المادة (١/ تاسعا) من مشروع قانون الجرائم المعلوماتية الخاصة بالتعاريف والأهداف.

ويتفق موقف المشرع العراقي في هذا الصدد مع موقف القوانين المقارنة التي وسعت من نطاق الوسائل التي ترتكب من خلالها الجريمة، ومن ثم فان جميع الوسائل الإلكترونية تصلح لان ترتكب من خلالها الجريمة، ومع ذلك فقد اشترط المشرع العراقي لقيام الجريمة أن يكون الجاني قد استخدام أحد أجهزة الحاسب الآلي وبرامجه أو أنظمته أو شبكة المعلومات التابعة لإحدى الجهات الأمنية أو العسكرية أو الاستخبارية، على خلاف موقف المشرع في القوانين المقارنة، فالمشرع في القانون الإماراتي والسعودي والكويتي استلزم أن يكون الدخول بدون تصريح إلى موقع إلكتروني أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية المعلومات من دون أن يحدد الجهات التي يلزم أن تكون هذه الوسائل تابعة لها [١]، بينما اشترط المشرع القطري أن يكون الجاني قد تمكن من الدخول غير المشروع عن طريق الشبكة المعلوماتية أو عن طريق أحد وسائل تقنية المعلومات إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها من دون أن يحددها بالجهات الأمنية أو العسكرية أو الاستخبارية [٢].

وفي هذا الصدد نرى أن المشرع العراقي قد ضيق من نطاق تحقق هذه الصورة من صور السلوك الإجرامي التي تقوم بها جريمة التجسس الإلكتروني، إذ انه لم يشمل بها حالة قيام الجاني أو الفاعل باستخدام أجهزة الحاسب الآلي وبرامجه أو أنظمته أو شبكة المعلومات التابعة لأجهزة الدولة الأخرى أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها، فضلا عن عدم شموله لحالة استخدام الوسائل الإلكترونية الخاصة بالمنشآت التجارية والصناعية والمالية، لاسيما إذا أخذنا بنظر الاعتبار إن جريمة التجسس الإلكتروني لا تقتصر في الوقت الحاضر على الحصول على البيانات والمعلومات المتعلقة بالأسرار الأمنية أو العسكرية أو الاستخبارية، وإنما تتسع لتشمل البيانات والمعلومات الحكومية ذات الطابع السري سواء بطبيعتها أم بمقتضى تعليمات

(١) يراجع: المادة (٤) من قانون مكافحة جرائم تقنية المعلومات الإماراتي الاتحادي، والمادة (٧ /٢) من نظام مكافحة الجرائم المعلوماتية السعودي، والمادة (٣) من لقانون مكافحة جرائم تقنية المعلومات الكويتي

(٢) يراجع: المادة (٢) من قانون مكافحة الجرائم الإلكترونية القطري.

صادرة بذلك، فضلا عن تلك المتعلقة بالأسرار الخاصة بالمنشآت التجارية والصناعية والمالية.

ثانيا: تجاوز نطاق التصريح المخول به أو اعتراض أي معلومات خلال عمليات تبادلها: نصت الفقرة (أولا / أ) من المادة (١٥) على هذه الصورة بقولها: "يعاقب..

أولا:- كل من: أ – تجاوز عمدا نطاق التصريح المخول به أو اعترض أي معلومات خلال عمليات تبادلها".

ولم تتضمن أيا من القوانين المقارنة نصا مشابها لهذا النص، ويرجع ذلك برائينا إلى أن هذه القوانين قد نصت على صورة السلوك الإجرامي المحقق لجريمة التجسس الإلكتروني المتمثل بالدخول غير المشروع أو غير المصرح به وهي تشمل – كما بينا أنفا – حالة الدخول إلى النظام من قبل شخص لديه تصريح بالدخول إلا انه تجاوز حدود التصريح الممنوح له.

وعلى أية حال، فأن تجاوز نطاق التصريح المخول به تتحقق في حال كون الجاني أو الفاعل يملك الحق في الدخول إلى جزء من النظام المعلوماتي – سواء أكان الدخول إلى هذا الجزء أصلا من ضمن صلاحياته بحكم وظيفته أم تم منحه هذا الحق من شخص أخر يملك الحق في ذلك – إلا انه تجاوز حدود صلاحياته أو حدود الأذن الممنوح له وذلك بالدخول إلى جزء أخر غير مسموح له بالدخول فيه باعتباره لا يدخل ضمن صلاحياته أو لأنه لم يشمله التصريح [١].

ويلاحظ بان المشرع في هذه الصورة يعاقب الجاني أو الفاعل بمجرد تجاوزه حدود التصريح المخول له، فمجرد التجاوز تقوم به الجريمة حتى وان لم يترتب على تجاوزه ضرر أو يتحقق له فائدة من وراء التجاوز، طالما إن التجاوز قد تم على خلاف صلاحياته أو الأذن الممنوح له.

(١) ينظر: د.عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠١، ص٣٠.

ويرى جانب من الفقه [١] – نؤيده – إن تجاوز التصريح لا يثير أية مشكلة إذا قام بذلك أشخاص لا يعملون في المؤسسة التي تم الدخول إلى أنظمتها المعلوماتية، إذ إن التصريح أو الأذن بالدخول إلى جزء من النظام لا يمتد لغير تلك الأجزاء من النظام المصرح بالدخول لها، فإذا ما تم الدخول إلى أجزاء من النظام غير تلك المصرح بالدخول لها، فان تجاوز التصريح في هذه الحالة يأخذ حكم عدم التصريح، وإنما المشكلة تثور في حالة حصول التجاوز من قبل العاملين في المؤسسة التي يوجد فيها النظام، إذ يصعب في كثير من الأحيان معرفة عما إذا كان التجاوز قد تم عمدا أم عن طريق الخطأ.

كما يتحقق السلوك الإجرامي في هذه الصورة أيضا بقيام الجاني أو الفاعل باعتراض أي معلومات خلال عمليات تبادلها، ويراد به إعاقة المعلومات لمنع وصولها إلى الجهة المرسلة إليها، إذ إن الاعتراض في حقيقته يتمثل بالحيلولة بين الشيء وبين بلوغ هدفه [٢]، والواضح هنا إن المصلحة التي يهدف المشرع إلى حمايتها من خلال النص على تجريم فعل الاعتراض تتمثل في حماية الحق في احترام المعلومات والبيانات المرسلة، إذ إن هذا الفعل يشكل انتهاكا للحق في احترام الاتصالات، وهو ينطبق على جميع أشكال النقل الإلكتروني للمعلومات والبيانات التي تتم عبر استخدام أي وسيلة من وسائل تقنية المعلومات الحديثة، كأجهزة النقال أو البريد الإلكتروني [٣].

ويختلف الاعتراض عن الدخول إلى نظام معلوماتي، إذ انه لا يتضمن تداخلا في نظام معلوماتي ينتمي إلى جهاز حاسب آلي معين، وإنما يتمثل في إعاقة أو منع وصول المعلومات إلى الجهة المرسلة إليها عن طريق استخدام وسائل سلكية تتصل بالنظام المعلوماتي أو عن طريق التقاط المعلومات بوسائل التقاط حديثة عن بعد

(١) ينظر: عبد الإله محمد النوايسة، ممدوح حسن العدوان، مصدر سابق، ص٤٧٥ ؛ د. حسين بن سعيد الغافري، مصدر سابق، ص٣٤٩-٣٥٠.
(٢) ينظر: د. فايق عوضين محمد تحفه، الحماية القانونية والأمنية للاتصالات السلكية واللاسلكية، ط١، دار الكتب العلمية للنشر والتوزيع، القاهرة، ٢٠١٤، ص٢١٧.
(٣) ينظر: د. حسين بن سعيد الغافري، المصدر السابق، ص٣٩٦.

ومنعها من الوصول إلى الجهة المرسلة إليها [١]، ومن ثم فان الاعتراض لا يدخل ضمن السلوك الذي تعاقب عليه بعض القوانين بوصفه دخولا أو استخداما غير مشروع، كما انه لا يعد معاقبا عليه بوصف التنصت كما سنبين ذلك أنفا.

ومع تأييدنا لموقف المشرع العراقي في النص على هذه الصورة من صور السلوك الإجرامي المحققة لجريمة التجسس الإلكتروني والذي يتفق مع موقف المشرع في اغلب القوانين المقارنة -حسب ما سنبينه عند تناولنا للسلوك الإجرامي المتمثل بالتقاط أو اعتراض المعلومات دون وجه حق -، إلا أننا نسجل عليه انه عاد ونص على هذه الصورة في المادة (١٦) التي نصت على انه: "يعاقب... كل من التقط أو اعترض بدون وجه حق ما هو مرسل عن طريق أحد أجهزة الحاسوب أو شبكة المعلومات..."، مما يعني وجود نصين يعاقبان على الفعل ذاته، وهو الأمر الذي لا يتفق مع مبدأ تخصيص عقوبة واحدة لكل فعل مجرم، فضلا عن انه قد يؤدي إلى تناقض الأحكام القضائية وعدم وحدتها، وتجدر الإشارة إلى أن الاعتراض المعاقب عليه هو الاعتراض الذي يتم دون وجه حق، ومن ثم إذا اقتضت متطلبات حماية امن الدولة الداخلي أو الخارجي اعتراض البيانات أو المعلومات وتم ذلك بعد الحصول على أذن الجهات المختصة، فان السلوك في هذه الحالة يعد مباحا [٢].

ثالثا: التنصت على البيانات والمعلومات المخزنة أو المتبادلة في نظم المعلومات أو مراقبتها: نصت الفقرة (أولا / ب) من المادة (١٥) من المشروع على هذه الصورة بقولها:"ب- تنصت أو راقب البيانات والمعلومات المخزنة أو المتبادلة في نظم المعلومات"[٣]، والملاحظ من خلال النص إن السلوك الإجرامي يتمثل في واحد من فعلين هما: التنصت والمراقبة.

(١) ينظر: د. خالد ممدوح إبراهيم، مصدر سابق، ص٢٤٩.
(٢) ينظر: د. فايق عوضين محمد تحفه، مصدر سابق، ص٢١٧.
(٣) تجدر الإشارة إلى أن المشرع الإماراتي لم ينص على تجريم فعل التنصت، بينما جرم المشرع الكويتي والسعودي والقطري فعل التنصت وذلك بعده أحد الأفعال التي تقع بها جريمة التجسس الإلكتروني مع أفعال أخرى هي الاعتراض والالتقاط للمعلومات في المواد (٤/ ٣)، (٣/ ١)، (٤) حسب التسلسل.

والتصنت هو أحد وسائل التجسس الإلكتروني الذي يتم عن طريق التسمع للمواد المتداولة عبر نظم المعلومات الإلكترونية بين طرفين أو أكثر، ذلك إن فعل التصنت قوامه فعل الإصغاء والاستماع [١].

ويلزم لقيام الجريمة أن يكون الجاني قادرا على السمع، وان تكون المواد المتداولة مسموعة، سواء أكانت أصوات أشخاص أو أصوات موسيقية أو أي أصوات أخرى مفهومة أم غير مفهومة، ومن ثم يشترط لقيام الجريمة أن يكون الجاني قادرا على التسمع حتى وان لم يفهم اللغة المسموعة، فان كان غير قادر على التسمع لأنه أصم أو لان المادة المتداولة غير مسموعة فان الجريمة تنتفي في هذه الحالة، إذ لا يكون ثمة انتهاك لحرمة وسرية المادة المتداولة[٢]. كما يلزم أيضا أن يكون التصنت قد تم دون مسوغ قانوني صحيح، فان كان للتصنت مسوغ قانوني، فلا تتحقق الجريمة [٣].

أما المراقبة فيراد بها مراقبة سير المعلومات المتداولة عبر نظم المعلومات الإلكترونية ومعرفة الجهات المرسلة لها والمرسلة إليها.

ويختلف التنصت عن المراقبة في إن الأول يشترط فيه أن تكون المواد المتداولة مواد صوتية مسموعة أما الثاني فلا يشترط فيه ذلك، فالمراقبة تتحقق حتى وان كانت المواد المتداولة غير مسموعة، وفي كلا الحالتين فان التقاط الموجات الكهربائية الصادرة عن نظام المعلومات الإلكتروني يعد الوسيلة الأساسية للتنصت ومراقبة المعلومات المتداولة عبر النظام، والتي من خلالها يتمكن الجاني من معرفة محتوى اتصال وكذلك معرفة المعلومات والجهات المرسلة لها والمرسلة إليها التي تتم داخل نظام معلوماتي واحد أو بين نظامين مختلفين أو بين عدة أنظمة ترتبط فيما بينها من خلال شبكة معلومات، ومن ثم جمع المعلومات المطلوبة عن بعد [٤].

(١) ينظر: محمد مصطفى صدور، د. منال ماجد، جريمة التنصت على الاتصالات الهاتفية في إطار قانون الاتصالات السوري رقم ١٨ لسنة ٢٠١٠، بحث منشور في مجلة جامعة البعث، مج ٣٦، ع ١١، ٢٠١٤، ص٦٦.

(٢) ينظر: د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠١٠، ص٣٤٠ -٣٤١.

(٣) المصدر اعلاه، ص٣٤١.

(٤) ينظر: د. علي جعفر، مصدر سابق، ص٥٨١.

رابعا: التقاط أو اعتراض البيانات والمعلومات بدون وجه حق: نصت على هذه الصورة المادة (١٦) من المشروع بقولها: "يعاقب... كل من التقط أو اعترض بدون وجه حق ما هو مرسل عن طريق أحد أجهزة الحاسوب أو شبكة المعلومات لاستخدامها في تحقيق منفعة مالية له أو لغيره"[١].

ولم يتضمن مشروع قانون الجرائم المعلوماتية العراقي نصا يحدد المقصود بالتقاط المعلومات، بينما عرف المشرع السعودي الالتقاط بأنه: "مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح"[٢]، في الاتجاه ذاته سار المشرع الكويتي، إذ عرف الالتقاط المعلوماتي بأنه: "مشاهدة البيانات أو المعلومات الواردة في أي رسالة إلكترونية أو سماعها أو الحصول عليها، ويشمل ذلك المنقولة إلكترونيا"[٣]، وكذلك فعل المشرع الإماراتي إذ عرفه بأنه: "مشاهدة البيانات أو المعلومات أو الحصول عليها"[٤]، والمشرع القطري الذي عرفه بأنه: "مشاهدة البيانات أو المعلومات الإلكترونية أو الحصول عليها"[٥].

والواضح من خلال العرض السابق لتعريف الالتقاط في القوانين المقارنة انه يلزم لتحقق السلوك الإجرامي الذي تقوم به الجريمة في هذه الصورة مجرد إطلاع الجاني – أو كما ورد التعبير عنها ب (المشاهدة) – على البيانات أو المعلومات التي تظهر على شاشة نظام معلوماتي أو تلك التي تظهر بصورة مخرجات أيا كان شكلها دون تدخل من الشخص، وهو بذلك يختلف عن الاستخدام أو الدخول غير المشروع الذي يتطلب الولوج إلى النظام المعلوماتي واستخدامه [٦]، فالالتقاط يتحقق بمجرد الاطلاع أو المشاهدة للبيانات أو المعلومات الغير متاحة للجمهور، سواء أكانت معلومات عسكرية

(١) يقابلها المادة (١٥) من قانون مكافحة جرائم تقنية المعلومات الإماراتي الاتحادي، والمادة (٤/ ٣) من قانون مكافحة جرائم تقنية المعلومات الكويتي، والمادة (٣/ ١) من نظام مكافحة الجرائم المعلوماتية السعودي، والمادة (٤) من قانون مكافحة الجرائم الإلكترونية القطري.
(٢) يراجع: المادة (١ / ١٠) من نظام مكافحة الجرائم المعلوماتية السعودي.
(٣) يراجع: المادة (١) من قانون مكافحة جرائم تقنية المعلومات الكويتي.
(٤) يراجع: المادة (١) من قانون مكافحة جرائم تقنية المعلومات الإماراتي الاتحادي.
(٥) يراجع: المادة (١) من قانون مكافحة الجرائم الإلكترونية القطري.
(٦) يراجع: المادة (١) من قانون مكافحة جرائم تقنية المعلومات الكويتي.

أم سياسية أم اقتصادية، وسواء تم ذلك باستخدام أي وسيلة من وسائل تقنية المعلومات الحديثة للتحكم أو مراقبة المحتوى الإلكتروني.

ثانيا: النتيجة الإجرامية: هي العنصر الثاني من عناصر الركن المادي، ويقصد بها الأثر المترتب على السلوك الإجرامي والذي يعتد به المشرع في التكوين القانوني للجريمة [١]، وللنتيجة الإجرامية مدلولان: الأول مادي، ويراد به التغيير الملموس الذي يظهر في العالم الخارجي كأثر للنشاط الإجرامي، وإذا كانت اغلب الجرائم تتحقق فيها النتيجة بمدلولها المادي، فأن بعضها لا يترتب عليها اثر مادي ملموس في العالم الخارجي، ويطلق على النوع الأول الجرائم المادية ذات النتيجة، بينما يطلق على النوع الثاني الجرائم الشكلية أو جرائم السلوك المجرد، حيث يقتصر المشرع على تجريم السلوك دون اشتراط تحقيق نتيجة مادية معينة.

أما النتيجة بمدلولها القانوني فيقصد بها الاعتداء على الحق أو المصلحة التي يحميها القانون، سواء تمثل هذا الاعتداء في ضرر فعلي يقع على الحق أو المصلحة أو ضرر محتمل أي مجرد تعريض الحق أو المصلحة المحمية للخطر، وتقسم الجرائم تبعا لذلك إلى نوعين: الأول جرائم الضرر وهي التي يترتب على ارتكاب السلوك الإجرامي فيها ضرر فعلي على الحق أو المصلحة التي يحميها القانون، والثاني جرائم الخطر وهي التي يترتب على ارتكاب السلوك الإجرامي فيها تعريض الحق أو المصلحة محل الحماية القانونية للخطر [٢].

وبالتتبع للنصوص القانونية الخاصة بجريمة التجسس الإلكتروني، سواء في مشروع قانون الجرائم المعلوماتية العراقي أم في القوانين المقارنة، نجد إن أيا منها لم يتطلب لقيام الجريمة تحقق نتيجة إجرامية معينة، وهذا الأمر يترتب عليه نتائج عديدة هي:

(١) ينظر: د. محمود محمود مصطفى، شرح قانون العقوبات، القسم العام، ط ١٠، مطبعة جامعة القاهرة، القاهرة، ١٩٨٣، ص٢٧٦.

(٢) ينظر: د. ماهر عبد شويش، قانون العقوبات، القسم العام، مطبعة دار الحكمة، جامعة الموصل، ١٩٩٠، ص١٩٢-١٩٣.

١- إن جريمة التجسس الإلكتروني التي ترتكب في أي صورة من صور السلوك الإجرامي المحققة للجريمة هي جريمة من الجرائم الشكلية أو جرائم السلوك المجرد.

٢- لا مجال للبحث في موضوع الشروع في جريمة التجسس الإلكتروني، ذلك إن الشروع بعده "البدء بتنفيذ فعل بقصد ارتكاب جناية أو جنحة إذا أوقف أو خاب أثره لأسباب لا دخل لإرادة الفاعل فيها"[١]، يتطلب أن يترتب على السلوك الإجرامي نتيجة إجرامية بالمدلول المادي لها لإمكانية القول بوقف أو خيبة الأثر لأسباب خارجة عن إرادة الجاني، ومن ثم فان جريمة التجسس الإلكتروني إما أن تقع في صورتها التامة وإما أن لا تقع.

٣- لا مجال أيضا للبحث في موضوع العلاقة السببية في جريمة التجسس الإلكتروني، اذ ان البحث في العلاقة السببية ينبني على وجود نتيجة مادية تترتب على ارتكاب السلوك الإجرامي، وعدم وجود نتيجة للسلوك بطبيعته لا يترك مجالا للبحث في العلاقة السببية للجريمة المتحققة من هذا السلوك.

المطلب الثاني: الركن المعنوي لجريمة التجسس الإلكتروني

جريمة التجسس الإلكتروني من الجرائم العمدية، ويتعين لتحقق الركن المعنوي فيها توافر القصد الجنائي العام بعنصريه: العلم والإرادة، في جميع صور السلوك الإجرامي المحققة للجريمة، إذ يجب أن ينصرف علم الجاني إلى أن السلوك الذي يرتكبه يشكل استخداما لأجهزة الحاسوب وبرامجه أو أنظمته أو شبكة المعلومات التابعة للجهات الأمنية أو العسكرية أو الاستخبارية دون الحصول على تصريح بذلك أو انه قد تجاوز نطاق التصريح المخول به عند استخدامها أو قام باعتراض أي معلومات خلال عمليات تبادلها أو التنصت أو مراقبة البيانات والمعلومات المخزنة أو المتبادلة في نظم المعلومات أو التقطها أو اعترضها دون وجه حق، فضلا عن اتجاه إرادته إلى ارتكاب أي فعل من الأفعال السابقة والآثار المترتبة عليه.

(١) يراجع: المادة (٣٠) من قانون العقوبات العراقي النافذ.

فضلا عن تطلب القصد العام، فان المشرع العراقي تطلب لقيام الجريمة توافر القصد الخاص في صورتين من صور السلوك الإجرامي المحققة للجريمة، الأولى تتعلق بالاستخدام غير المشروع لأجهزة الحاسوب وبرامجه أو أنظمته أو شبكة المعلومات التابعة للجهات الأمنية أو العسكرية أو الاستخبارية، إذ تطلب أن يتم بقصد الإضرار بها أو النسخ منها أو إرسال محتواها لجهة معادية أو الاستفادة منها لتنفيذ جرائم ضد امن الدولة الداخلي أو الخارجي، أو تسهيل إخفاء معالم تلك الجرائم أو تغطيتها [١].

وموقف المشرع العراقي من هذه الناحية يتفق مع موقف المشرع في القوانين المقارنة – باستثناء المشرع القطري – التي تتطلب لتحقق الركن المعنوي في جريمة الدخول غير المشروع إلى موقع إلكتروني أو نظام معلومات أو شبكة إلكترونية توافر القصد الخاص فضلا عن توافر القصد العام، وهو يتمثل بحسب موقف المشرع الإماراتي ب"قصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية"[٢]، أو "للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني" بحسب موقف المشرع السعودي[٣]، أو بـ "قصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون" بحسب موقف المشرع الكويتي[٤].

وحيث أن القصد من جريمة التجسس الإلكتروني في صورة الاستخدام غير المشروع لأجهزة الحاسوب ونظم المعلومات والمواقع والشبكات الإلكترونية الحكومية هو الحصول على المعلومات التي تتعلق بأمن الدولة سواء من حيث الداخل أو الخارج أيا كان نوعها (عسكرية أو أمنية أو سياسية أو اقتصادية أو مالية أو غيرها)، لذا فإننا نرى أن (قصد الحصول) الذي تطلبه المشرع في القوانين المقارنة أكثر دقة في التعبير عن القصد الخاص المتطلب لتتحقق الركن المعنوي للجريمة هذا من جهة، ومن جهة

(١) يراجع: المادة (٣ / ثانيا) من مشروع قانون جرائم المعلوماتية العراقي.
(٢) يراجع: المادة (٤) من قانون مكافحة جرائم تقنية المعلومات الإماراتي الاتحادي.
(٣) يراجع: المادة (٢/٧) من نظام مكافحة الجرائم المعلوماتية السعودي.
(٤) يراجع: المادة (٣ / ١) من قانون مكافحة جرائم تقنية المعلومات الكويتي.

أخرى فان تطلب هذا القصد (قصد الحصول) من شانه ان يضفي حماية اشمل وأوسع للمعلومات والبيانات الحكومية السرية، اذ انه يستوعب الوسائل كافة التي يلجا إليها الجاني للحصول على هذه البيانات أو المعلومات.

فضلا عن ذلك، فان الاقتصار على تطلب هذا القصد يغني عن البحث فيما دفع الجاني إلى ارتكاب الجريمة سواء أكان ذلك للإضرار بها أم النسخ منها أم إرسال محتواها لجهة معادية أم الاستفادة منها لتنفيذ جرائم ضد امن الدولة الداخلي أو الخارجي، أم تسهيل إخفاء معالم تلك الجرائم أو تغطيته أم للانتفاع بها في أي مجال من المجالات، لان كل ما تقدم يدخل ضمن الباعث على الجريمة، والقاعدة العامة أن الباعث لا يدخل ضمن تكوين الجريمة ولا يعتد به [١].

عليه نقترح على المشرع العراقي تعديل نص الفقرة (ثانيا) من المادة (٣) من مشروع قانون الجرائم المعلوماتية قبل إصداره وجعلها بالشكل الآتي: "يعاقب..... كل من استخدام أجهزة الحاسوب وبرامجه أو أنظمته أو شبكة المعلومات بقصد الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة، أو أي بيانات أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية"

ويمكن إضافة فقرة أخرى لها تقرر تشديد العقوبة إذا ترتب على الاستخدام غير المشروع إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نسخها أو نشرها أو إعادة نشرها أو تسليمها إلى جهة معادية وحسب ما سنبينه عند تناولنا لعقوبة جريمة التجسس الإلكتروني.

أما الحالة الثانية التي تطلب فيه المشرع العراقي للقصد الخاص فتتعلق بالتقاط البيانات أو المعلومات المرسلة عن طريق أحد أجهزة الحاسوب أو شبكة المعلومات أو اعتراضها دون وجه حق، إذ يتطلب لتوافر الركن المعنوي توافر القصد الخاص المتمثل باستخدام الجاني للبيانات أو المعلومات التي تم التقاطها أو اعتراضها لتحقيق منفعة

(١) نصت المادة (٣٨) من قانون العقوبات العراقي النافذ على انه: "لا يعتد بالباعث على ارتكاب الجريمة ما لم ينص القانون على خلاف ذلك".

مالية له أو لغيره [١]، وحيث أن تطلب هذا القصد قد يؤدي إلى إفلات العديد من مرتكبي الجريمة من العقوبة وذلك على الرغم من تحقق أركان الجريمة إذا ثبت أن التقاط البيانات أو المعلومات من قبل الجاني لم يكن لاستخدامها في تحقيق منفعة مالية له أو لغيره' كما إن هذا القصد لم يطلبه المشرع في أي من القوانين المقارنة، عليه نقترح على المشرع حذف عبارة (لتحقيق منفعة مادية له أو لغيره) من نص المادة (١٦) من مشروع قانون الجرائم المعلوماتية قبل إصداره.

المطلب الثالث: عقوبة جريمة التجسس الإلكتروني

لم يجعل المشرع العراقي لجريمة التجسس الإلكتروني عقوبة واحدة وإنما تدرج بالعقوبة بحسب خطورة السلوك الإجرامي المحقق للجريمة والآثار المترتبة عليه، إذ فرض عقوبة السجن المؤبد والغرامة التي لا تقل عن خمسة وعشرين مليون دينار ولا تزيد على خمسين مليون دينار إذا ارتكبت جريمة التجسس عن طريق الاستخدام غير المشروع لأجهزة الحاسوب وبرامجه أو أنظمته أو شبكة المعلومات التابعة للجهات الأمنية أو العسكرية أو الاستخبارية [٢].

فيما نزل بالعقوبة وجعلها السجن مدة لا تزيد على سبع سنوات والغرامة التي لا تقل عن خمسة وعشرين مليون دينار ولا تزيد على خمسون مليون دينار إذا ارتكبت الجريمة عن طريق التقاط أو اعتراض البيانات والمعلومات بدون وجه حق [٣].

كما هبط بالعقوبة وجعلها الحبس والغرامة التي لا تقل عن عشرة ملايين دينار ولا تزيد على خمسة عشر مليون دينار إذا ارتكبت الجريمة عن طريق تجاوز نطاق التصريح المخول به أو اعتراض أي معلومات خلال عمليات تبادلها أو عن طريق التنصت على البيانات والمعلومات المخزنة أو المتبادلة في نظم المعلومات أو مراقبتها [٤]' فإذا ترتب على أي فعل من هذه الأفعال حذف أو تدمير أو تغيير أو تعييب أو تعطيل أو إعادة نشر البيانات أو المعلومات فان العقوبة تصبح الحبس مدة لا تقل عن

(١) يراجع: المادة (١٦) من مشروع قانون جرائم المعلوماتية العراقي.
(٢) يراجع: المادة (٣ / ثانيا) من مشروع قانون جرائم المعلوماتية العراقي.
(٣) يراجع: المادة (١٦) من مشروع قانون جرائم المعلوماتية العراقي.
(٤) يراجع: المادة (١٥ / أولا) من مشروع قانون جرائم المعلوماتية العراقي.

أربع سنوات والغرامة التي لا تقل عن خمسة عشر مليون دينار ولا تزيد على خمسة وعشرون مليون دينار [١].

أما بالنسبة للقوانين المقارنة، فنجد إن عقوبة الدخول غير المشروع إلى موقع إلكتروني أو نظام معلومات أو شبكة إلكترونية في القانون السعودي هي: "السجن مدة لا تزيد على عشر سنوات والغرامة التي لا تزيد على خمسة ملايين ريال أو بإحدى هاتين العقوبتين"[٢]، في حين جعل القانون الإماراتي العقوبة: "السجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تزيد على مليون وخمسمائة ألف درهم، وإذا ترتب على الدخول تعرض البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر فتكون العقوبة السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تزيد على مليوني درهم"[٣].

أما القانون القطري فعاقب على الجريمة ب:"الحبس مدة لا تتجاوز ثلاث سنوات والغرامة التي لا تزيد على خمسمائة ألف ريال، وعلى أن تضاعف العقوبة إذا ترتب على الدخول الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أي بيانات أو معلومات حكومية سرية أو إلغاء البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو إلحاق الضرر بالمستفيدين أو المستخدمين أو الحصول على أموال أو خدمات أو مزايا غير مستحقة"[٤]. وكذلك عاقب القانون الكويتي عليها ب:"الحبس مدة لا تتجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة ألاف دينار لا تتجاوز عشرة ألاف دينار أو بإحدى هاتين العقوبتين، وإذا ترتب على الدخول إلغاء البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو

(١) يراجع: المادة (١٥ / ثانيا) من مشروع قانون جرائم المعلوماتية العراقي.
(٢) يراجع: المادة (٧ / ٢) من نظام مكافحة الجرائم الإلكترونية السعودي.
(٣) يراجع: المادة (٤) من قانون مكافحة جرائم تقنية المعلومات الإماراتي الاتحادي.
(٤) يراجع: المادة (٢) من قانون مكافحة الجرائم الإلكترونية القطري.

تعديلها فتكون العقوبة الحبس مدة لا تتجاوز عشر سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تتجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين"[١].

كما نجد أن العقوبة وفقا لقوانين المقارنة في حال ارتكاب الجريمة عن طريق التقاط البيانات أو المعلومات أو اعتراضها دون وجه حق هي وفقا للقانون السعودي: "السجن مدة لا تزيد على سنة والغرامة التي لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين"[٢]، ووفقا للقانون الإماراتي هي: "الحبس والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تزيد على خمسمائة ألف درهم أو بإحدى هاتين العقوبتين، فإذا أفشى الجاني المعلومات التي حصل عليها بغير وجه حق فتكون العقوبة الحبس مدة لا تقل عن سنة واحدة"[٣]، أما القانون القطري فحدد العقوبة ب:"الحبس مدة لا تتجاوز سنتين والغرامة التي لا تزيد على مائة ألف ريال أو بإحدى هاتين العقوبتين"[٤]. في حين حدده القانون الكويتي ب:"الحبس مدة لا تتجاوز سنتين والغرامة التي لا تقل عن ألفي دينار ولا تتجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين"[٥].

ومما تقدم يتضح اتجاه المشرع العراقي وكذلك المشرع في القوانين المقارنة إلى التشديد في العقوبة المقررة للجريمة إذا ارتكبت عن طريق الاستخدام أو الدخول غير المشروع لأجهزة الحاسب الآلي أو نظم المعلومات أو الشبكة الإلكترونية وذلك يتبين من وجوب الحكم على مرتكب الجريمة بالعقوبتين السالبة للحرية – على اختلاف المدة المحددة لها – والمالية، إذ إن المشرع استخدم الأداة (واو) التي تفيد الجمع ولم يستخدم الأداة (أو) التي تفيد التخيير أو يضمن النص عبارة (أو بإحدى هاتين العقوبتين)، وهذا اتجاه يحسب للمشرع العراقي والمشرع في القوانين المقارنة لان الجريمة في هذه الصورة

(١) يراجع: المادة (٣) من قانون مكافحة جرائم تقنية المعلومات الكويتي.
(٢) يراجع: المادة (٣ / ١) من نظام مكافحة الجرائم الإلكترونية السعودي، علما أن العقوبة وفقا لهذه الفقرة تفرض على من ارتكب جريمة التجسس الإلكتروني عن طريق التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي.
(٣) يراجع: المادة (١٥) من قانون مكافحة جرائم تقنية المعلومات الإماراتي الاتحادي.
(٤) يراجع: المادة (٤) من قانون مكافحة الجرائم الإلكترونية القطري.
(٥) يراجع: المادة (٤) من قانون مكافحة جرائم تقنية المعلومات الكويتي، علما أن العقوبة وفقا لهذه المادة تفرض على من ارتكب الجريمة عن طريق التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي وسيلة من وسائل تقنية المعلومات دون وجه حق.

تتعلق بالحصول على البيانات أو المعلومات المتعلقة بأسرار الدولة سواء العسكرية أو الأمنية أو الاقتصادية أو التجارية.... الخ، ومن ثم تتطلب التشديد في العقوبة التي تفرض على مرتكبها، فضلا عن إن من شان ذلك إضفاء المزيد من الحماية القانونية لهذه البيانات والمعلومات.

ومع ذلك نجد إن مقدار العقوبة التي قررها المشرع العراقي للجريمة، سواء السالبة للحرية (السجن المؤبد) أم المالية قد جاءت شديدة جدا بالمقارنة مع العقوبة المقررة في القوانين المقارنة، لذا واستكمالا لما اقترحناه عند تناولنا للركن المعنوي للجريمة، نقترح أن يحدد المشرع العقوبة بالسجن المؤقت والغرامة التي لا تقل عن عشرة ملايين دينار ولا تزيد على خمسة عشر مليون دينار، وفي حال ترتب على الاستخدام غير المشروع تعرض البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر أو تسليمها إلى جهة معادية فتكون العقوبة السجن المؤبد والغرامة التي لا تقل عن خمسة وعشرين مليون دينار ولا تزيد على خمسين مليون دينار، مع إمكانية رفع العقوبة وجعلها الإعدام إذا كان الجاني موظفا أو مكلفا بخدمة عامة في إحدى المؤسسات العسكرية أو الأمنية أو الاستخبارية.

كما يتضح أيضا أن موقف المشرع العراقي في التشديد في العقاب على الجريمة بقي مستمرا حتى في حال ارتكاب الجريمة عن طريق تجاوز نطاق التخويل أو التقاط البيانات أو المعلومات أو اعتراضها أو التصنت عليها، إذ يجب الحكم بالعقوبتين السالبة للحرية والمالية – بالرغم من إن المشرع هبط في مقدار العقوبتين – على مرتكب الجريمة، وهذا الموقف من المشرع العراقي جاء على خلاف موقف المشرع في غالبية القوانين المقارنة التي هبط المشرع فيها بالعقوبة المقررة لهذه الأفعال مع الإبقاء على السلطة التقديرية للقاضي في فرض واحدة من العقوبتين بحسب ظروف الجريمة وظروف مرتكبها، وهذا الاتجاه الأخير بتقديرنا ينسجم مع مبدأ التفريد العقابي الذي يعد أحد المبادئ الأساسية في السياسة الجنائية المعاصرة، فضلا عن إن خطورة الجريمة والآثار المترتبة عليها في هذه الصور لا ترقى إلى مرتبة الخطورة المترتبة على

الاستخدام غير المشروع لأجهزة الحاسب الآلي أو نظم المعلومات أو الشبكة الإلكترونية التابعة للجهات الحكومية على مختلف تصنيفاتها، عليه نقترح على المشرع العراقي تعديل المادتين (١٥، ١٦) بإضافة عبارة (أو بإحدى هاتين العقوبتين) إليها.

وتجدر الإشارة إلى إن القوانين المقارنة قد نصت على الظروف المشددة للعقوبة، اذ عد المشرع الإماراتي ارتكاب أي جريمة منصوص عليها في القانون ومنها جريمة التجسس الإلكتروني لحساب أو لمصلحة دولة أجنبية أو أي جماعة إرهابية أو جمعية أو منظمة أو هيئة غير مشروعة ظرف مشددا للعقوبة، أما المشرع القطري فعد ظرفا مشددا للعقوبة ارتكاب الجريمة من قبل موظف عام، في حين إن المشرع الكويتي عد ظرفا مشددا للعقوبة ارتكاب الجريمة من قبل عصابة منظمة أو موظف عام أو من شخص كانت قد صدرت بحقه أحكام عن جرائم مماثلة، سواء من المحاكم الوطنية أم الأجنبية [١]، بينما لم ينص المشرع العراقي على الظروف المشددة للعقوبة، وبالتالي يتم تطبيق القواعد العامة الخاصة بالظروف المشددة الواردة في قانون العقوبات [٢].

وأخيرا تجدر الإشارة إلى إن القانون العراقي والقوانين المقارنة قد نصت على ان فرض العقوبات المنصوص عليها في القانون لا يمنع من فرض أي عقوبة اشد تقضي بها القوانين النافذة [٣]، كما إنها أجازت للمحكمة أن تقضي بمصادرة أو إتلاف الأدوات أو الأجهزة أو البرامج المستخدمة في ارتكاب الجريمة بشرط عدم الإخلال بحقوق الغير حسن النية [٤].

(١) يراجع: المادة (٤٦) من قانون مكافحة جرائم تقنية المعلومات الإماراتي الاتحادي، والمادة (٥١) من قانون مكافحة الجرائم الإلكترونية القطري، والمادة (١١) من قانون مكافحة جرائم تقنية المعلومات الكويتي

(٢) يراجع: المادة (٣٠) من مشروع قانون جرائم المعلوماتية العراقي التي نصت على انه: "تطبق القوانين التالية في كل ما لم يرد به نص في القانون: أولا: قانون العقوبات رقم ١١١ لسنة ١٩٦٩. ثانيا: قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١ ".

(٣) يراجع: المادة (٢٧) من مشروع قانون جرائم المعلوماتية العراقي، ويقابلها المادة (٤٨) من قانون مكافحة جرائم تقنية المعلومات الإماراتي الاتحادي، والمادة (٤٤) من قانون مكافحة الجرائم الإلكترونية القطري، والمادة (١٢) من نظام مكافحة الجرائم الإلكترونية السعودي، والمادة (١٦) من قانون مكافحة جرائم تقنية المعلومات الكويتي.

(٤) يراجع: المادة (٢٩) من مشروع قانون جرائم المعلوماتية العراقي، ويقابلها المادة (٤١) من قانون مكافحة جرائم تقنية المعلومات الإماراتي الاتحادي، والمادة (٥٣) من قانون مكافحة

الخاتمة

بعد الانتهاء من هذا البحث توصلنا إلى جملة من النتائج والتوصيات ندرجها كالآتي:

أولا: النتائج

١- ان العناصر الأساسية التي يقوم عليها تحديد مفهوم التجسس الإلكتروني تتمثل، إن التجسس الإلكتروني لا يتم إلا باستخدام وسيلة من وسائل تقنية المعلومات الحديثة، وإن محله هو محتوى إلكتروني لا يتاح للجمهور استخدامه أو الاطلاع عليه، فضلا عن إن الغاية منه هي الوصول أو الحصول بطريقة غير مشروعة على بيانات أو معلومات سرية بطبيعتها أو بحكم القانون، تتعلق بالجانب العسكري أو السياسي أو التجاري أو الصناعي أو الاجتماعي للدولة.

٢- للتجسس الإلكتروني صور متعددة تهدف جميعها إلى الحصول على المعلومات التي لا يتاح للجمهور الاطلاع عليها منها العسكرية والسياسية والاقتصادية والعلمية والدبلوماسية، كما أن له وسائله المستحدثة التي تتفق مع طبيعة الجريمة.

٣- يتفق موقف المشرع العراقي في مشروع قانون جرائم المعلوماتية لسنة ٢٠١١ مع موقف غالبية القوانين المقارنة في تحديد صور السلوك الإجرامي الذي تتحقق فيه الجريمة والمتمثلة بالاستخدام غير المشروع لأجهزة الحاسب الآلي وبرامجه أو أنظمته أو شبكة المعلومات التابعة لإحدى الجهات الأمنية أو العسكرية أو الاستخبارية وتجاوز نطاق التصريح المخول به أو اعتراض أي معلومات خلال عمليات تبادلها، فضلا عن التنصت على البيانات أو المعلومات أو التقاطها أو اعتراضها دون وجه حق.

٤- أن المشرع العراقي قد ضيق من نطاق السلوك الإجرامي الذي تقوم به جريمة التجسس الإلكتروني في صورة الاستخدام غير المشروع لأجهزة الحاسب الآلي وبرامجه أو أنظمته أو شبكة المعلومات باشتراطه أن تكون تلك الأجهزة أو برامجها

الجرائم الإلكترونية القطري، والمادة (١٣) من نظام مكافحة الجرائم الإلكترونية السعودي، والمادة (١٣) من قانون مكافحة جرائم تقنية المعلومات الكويتي.

أو أنظمتها تابعة لإحدى الجهات الأمنية أو العسكرية أو الاستخبارية، ومن ثم فأنه لم يشمل بها حالة قيام الجاني أو الفاعل بالاستخدام غير المشروع لأجهزة الدولة الأخرى أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها، فضلا عن عدم شموله لحالة استخدام الوسائل الإلكترونية الخاصة بالمنشآت التجارية والصناعية والمالية.

٥- إن جريمة التجسس الإلكتروني التي ترتكب في أي صورة من صور السلوك الإجرامي المحققة للجريمة هي جريمة من الجرائم الشكلية أو جرائم السلوك المجرد، إذ لم يتطلب المشرع لقيام الجريمة تحقق نتيجة إجرامية معينة.

٦- إن جريمة التجسس الإلكتروني من الجرائم العمدية التي يتطلب لتحقق الركن المعنوي فيها توافر القصد الجنائي بعنصريه العلم والإرادة، ولم يتطلب المشرع القصد الخاص إلا في حالتين هما: الاستخدام غير المشروع لأجهزة الحاسب الآلي وبرامجه أو أنظمته أو شبكة المعلومات التابعة لإحدى الجهات الأمنية أو العسكرية أو الاستخبارية والتقاط البيانات أو المعلومات المرسلة عن طريق أحد أجهزة الحاسوب أو شبكة المعلومات أو اعتراضها دون وجه حق.

ثانيا: التوصيات

نقترح على المشرع العراقي في حال إصدار قانون جرائم المعلوماتية ما يأتي:

١- تعديل نص المادة (٣ / ثانيا) من المشروع من ناحيتين الأولى: أن يشمل النص حالة قيام الجاني أو الفاعل بالاستخدام غير المشروع لأجهزة الدولة الأخرى أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها، فضلا عن عدم شموله لحالة الاستخدام غير المشروع للوسائل الإلكترونية الخاصة بالمنشآت التجارية والصناعية والمالية، والثانية تعديل مقدار العقوبة المقررة للجريمة، سواء السالبة للحرية أم المالية، إذ إنها قد جاءت شديدة جدا بالمقارنة مع العقوبة المقررة في القوانين المقارنة، ونقترح أن يحدد المشرع العقوبة بالسجن المؤقت والغرامة التي لا تقل عن عشرة ملايين دينار ولا تزيد على خمسة عشر مليون دينار، وفي حال ترتب على الاستخدام غير المشروع تعرض البيانات أو المعلومات للإلغاء أو

الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر أو تسليمها إلى جهة معادية فتكون العقوبة السجن المؤبد والغرامة التي لا تقل عن خمسة وعشرين مليون دينار ولا تزيد على خمسين مليون دينار، مع إمكانية رفع العقوبة وجعلها الإعدام إذا كان الجاني موظفا أو مكلفا بخدمة عامة في إحدى المؤسسات العسكرية أو الأمنية أو الاستخبارية.

٢- تعديل نص الفقرة (أولا / أ) من المادة (١٥) من المشروع وبحذف عبارة (أو اعترض أي معلومات خلال عمليات تبادلها)، لأنه عاد ونص على هذه الصورة من صور السلوك الإجرامي في المادة (١٦) من مشروع القانون ذاته، مما يعني وجود نصين يعاقبان على الفعل ذاته، وهو الأمر الذي لا يتفق مع مبدأ تخصيص عقوبة واحدة لكل فعل مجرم، فضلا عن انه قد يؤدي إلى تناقض الأحكام القضائية وعدم وحدتها.

٣- تعديل نص المادتين (١٥ و١٦) من مشروع قانون جرائم المعلوماتية وذلك بإضافة عبارة (أو بإحدى هاتين العقوبتين) إلى نص المادتين، إذ إن من شأن ذلك الإبقاء على السلطة التقديرية للقاضي في فرض واحدة من العقوبتين بحسب ظروف الجريمة وظروف مرتكبها، وهو ما ينسجم مع مبدأ التفريد العقابي الذي يعد أحد المبادئ الأساسية في السياسة الجنائية المعاصرة، فضلا عن إن خطورة الجريمة والآثار المترتبة عليها في هذه الصور لا ترقى إلى مرتبة الخطورة المترتبة على الاستخدام غير المشروع لأجهزة الحاسب الآلي أو نظم المعلومات أو الشبكة الإلكترونية التابعة للجهات الحكومية على مختلف تصنيفاتها.

٤- حذف عبارة (لتحقيق منفعة مادية له أو لغيره) من نص المادة (١٦) من المشروع، حيث إن تطلب هذا القصد قد يؤدي إلى إفلات العديد من مرتكبي الجريمة من العقوبة وذلك على الرغم من تحقق التجسس، كما إن هذا القصد لم يتطلبه المشرع في أي من القوانين المقارنة.

المصادر

أولاً: الكتب اللغة

١- جمال الدين بن منظور، لسان العرب، ج٥، دار المعارف، بيروت، لبنان، ١٩٨٢.

٢- محمد بن أبي بكر بن عبد القادر الرازي، مختار الصحاح، باب الجيم، مكتبة لبنان، بيروت، ١٩٨٦.

ثانيا: الكتب القانونية

١- د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩.

٢- د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠١٠ .

٣- د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠١ .

٤- د. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة/ دراسة مقارنة، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٣ .

٥- د.علي صادق أبو هيف،القانون الدولي العام، ج١، منشأة المعارف، الإسكندرية، ١٩٧٥.

٦- علي عدنان الفيل، الإجرام الإلكتروني / دراسة مقارنة، ط١، منشورات زين الحقوقية، بيروت، لبنان، ٢٠١١ .

٧- د. فايق عوضين محمد تحفه، الحماية القانونية والأمنية للاتصالات السلكية واللاسلكية، ط١، دار الكتب العلمية للنشر والتوزيع، القاهرة، ٢٠١٤ .

٨- د. فتحي محمد انور عزت، الادلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، ط ٢، بلا مكان طبع، ٢٠١٠ .

٩- فواز البقور، التجسس في التشريع الأردني، دراسة مقارنة، ط٣، عمان، ١٩٩٣.

١٠-د.ماهر عبدشويش، قانون العقوبات، القسم العام،مطبعة دار الحكمة، جامعة الموصل، ١٩٩٠

١١-مجدي محمود حافظ، الحماية الجنائية لأسرار الدولة، الهيئة المصرية العامة للكتاب، الإسكندرية، ١٩٩٠ .

١٢-محمد راكان الدغمي، التجسس وأحكامه في الشريعة الإسلامية، ط٢، دار السلام للطباعة والنشر، القاهرة، ١٩٨٥ .

١٣-د. محمد الفاضل،الجرائم الواقعة على امن الدولة،ج١،ط٣، بلا مكان طبع، دمشق، ١٩٥٨.

١٤- د.محمود محمود مصطفى،شرح قانون العقوبات،القسم العام، ط١٠،مطبعة جامعةالقاهرة، القاهرة،١٩٨٣ .

١٥- د. مصطفى محمد موسى، الإرهاب الإلكتروني، ط١، دار الكتب والوثائق القومية المصرية، القاهرة، ٢٠٠٩ .

١٦- هاني جميل الطراونة، الجرائم الواقعة على امن الدولة الخارجي في التشريع الأردني/دراسة مقارنة، دار وائل، عمان، ٢٠١١

ثانيا: البحوث والدوريات

١- عبد الإله محمد النوايسة، ممدوح حسن العدوان، جرائم التجسس الإلكتروني في التشريع الأردني / دراسة مقارنة، بحث منشور في مجلة دراسات في علوم الشريعة والقانون، مجلد ٤٦، العدد ١، ٢٠١٩ .

٢- عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي الأول، بعنوان حماية امن المعلومات والخصوصية في قانون الانترنيت، المنعقد بالقاهرة في المدة ٢-٤ يونيو، ٢٠٠٨ .

٣- عبد الرحمن لحرش، التجسس والحصانة الدبلوماسية، بحث منشور في مجلة الحقوق، جامعة الكويت، العدد ٤، السنة ٢٧، ٢٠٠٣ .

٤- علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في القانون العماني مقارنة بالشريعة الإسلامية والقانون الجنائي الدولي، المؤتمر الدولي الأول، العلوم الشرعية، تحديات الواقع وأفاق المستقبل، ٢٠١٨ .

٥- محمد مصطفى صدور،د.منال ماجد،جريمة التنصت على الاتصالات الهاتفية في إطارقانون الاتصالات السوري رقم١٨لسنة٢٠١٠،منشورفي مجلة جامعة البعث،مجلد٣٦،العدد١١،٢٠١٤

ثالثا: الرسائل الجامعية

١- سعد إبراهيم الاعظمي، جرائم التجسس في التشريع العراقي،دراسة مقارنة، رسالة ماجستير، جامعة بغداد، ١٩٨١ .

٢- عصام احمد علي السنيدار، البعثة الدبلوماسية بين الحصانة ومقتضيات الأمن الوطني، رسالة ماجستير، الجامعة الأردنية، عمان، ٢٠٠١ .

٣- عطوة مضعان مسلم أبو غليون، الجرائم الإلكترونية بين الشريعة الإسلامية والقوانين الوضعية، رسالة ماجستير، كلية الدراسات العليا، الجامعة الأردنية، ٢٠٠٩ .

٤- محمد عدنان عثمان، دور القانون الدولي في مواجهة التجسس الدبلوماسي، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٥.

رابعا: الانترنيت

١- أسامة الكسواني، التجسس الإلكتروني وطرق مكافحته، منشور على موقع الانترنيت، http://alqabas. Com. تاريخ الزيارة ٢٠١٩/٦/٢١.

٢- تجسس إلكتروني، منشور على موقع الانترنيت https://ar.wikipedia.org/wiki تاريخ الزيارة ١٧/ ٥/ ٢٠١٩.

٣- سباق التجسس الإلكتروني وزعزعة النظام العالمي، ٢٠١٧، منشور على موقع الانترنيت https://annabaa.org/arabic/informatics/13571تاريخ الزيارة ٢٠١٩/٧/٩.

٤- غزلان جلال، احدث اجهزة التجسس الإلكتروني، ٢٠١٥، منشور على موقع الانترنيت https://machahid24.com/panorama/73838.html تاريخ الزيارة ٧/٩/ ٢٠١٩.

٥- كاظم عبد جاسم الزيدي، مكافحة الجرائم المعلوماتية في التشريع العراقي، ٢٠١٢، منشور على موقع الانترنيت .https://www.hjc.iq/view١٦٤٥/ تاريخ الزيارة ٦/٨/ ٢٠١٩.

٦- محمد محمد الألفي، جرائم التجسس والإرهاب الإلكتروني عبر الإنترنت، مقال منشور على الموقع الإلكتروني http://www.cyberlawnet.ne، تاريخ الزيارة ٢٠١٩/٨/٢٣ .

خامساً: القوانين

١- بروتوكول ١٩٧٧ الملحق باتفاقية جنيف لعام ١٩٤٩.

٢- قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ وتعديلاته .

٣- قانون مكافحة الارهاب العراقي رقم (١٣) لسنة ٢٠٠٥.

٤- نظام الجرائم المعلوماتية السعودي رقم ٧٩ لسنة ١٤٢٨هـ.

٥- مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١ .

٦- قانون مكافحة جرائم تقنية المعلومات الإماراتي الاتحادي رقم ٥ لسنة ٢٠١٢

٧- قانون مكافحة الجرائم الإلكترونية القطري رقم ١٤ لسنة ٢٠١٤ .

٨- قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ .

٩- نظام الجرائم المعلوماتية السعودي رقم ٧٩ لسنة ١٤٢٨هـ.