الحماية القانونية المقررة على وثائق الدولة السرية من جرائم التجسس الإلكتروني

عمار زياد الصبح
علي جبار صالح

تاريخ الاستلام
2023/3/9
تاريخ القبول
2024/1/24

الملخص

يعتبر التجسس من أقدم الوسائل ولكنه كان بشكل تقليدي سابقًا، وبعد وجود التطور الالكتروني أخذت جرائم التجسس بالتطور مواكبة لهذا التقدم، ولم تسلم وثائق الدولة وأسرارها من هذه الجرائم، حيث وجد ضعاف النفوس غايتهم باستغلال التطور وارتكاب الجريمة من خلال الإنترنت الذي سهل عليهم ارتكاب هذه الجرائم، مما جعل هناك ضرورة لتدخل المشرع لمكافحة هذه الجرائم من خلال النصوص التشريعية والاجراءات المتبعة للحد منها، ووجدت الدراسة أن النصوص الأردنية وخاصة قانون حماية وأسرار ووثائق الدولة، وقانون العقوبات الأردني وقانون الجرائم الالكترونية لم تكن كافية بشكل كامل في مواجهة التجسس الالكتروني على وثائق وأسرار الدولة بالرغم من خطورة هذه الجرائم كونها تمس في بعض الأحيان الحياة السياسية والأمن العام الذي يلعب دورًا مهمًا في سلامة الدولة.

Prescribed Protection of Confidential State Documents from Cyberespionage Crimes

Abstract

Espionage is considered one of the oldest means, but it was in a traditional way previously, and after the existence of electronic development, espionage crimes began to develop in keeping with this progress, and state documents and secrets were not spared from these crimes, as weak souls found their purpose by exploiting development and committing crime through the Internet, which made it easier for them to commit these crimes, which made there It is necessary for the legislator to intervene to combat these crimes through the legislative texts and the procedures used to reduce them. The study found that the Jordanian texts, especially the Law of Protection, Secrets and State Documents, the Jordanian Penal Code and the Electronic Crimes Law were not fully sufficient in confronting electronic espionage on state documents and secrets despite the seriousness of these crimes Because it sometimes affects political life and public security, which plays an important role in the safety of the state.

المقدمة

تعتبر الثورة التقنية التي يشهدها العالم في مجال الاتصالات من الفوائد العظيمة التي استفادت منها البشرية في مختلف النواحي التي تمس حياة الانسان بشكل مباشر، إلا أن هذا التطور قد يتسبب في نفس الوقت في ظهور أشكال جديدة من الجرائم بالغة الخطورة، خاصة مع ربط مختلف أجهزة الحاسوب بالشبكة العالمية للإنترنت.

وتعتبر جرائم الكمبيوتر والانترنت، هي ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع وبكل المستويات الاقتصادية والاجتماعية والثقافية والأمنية.

إذا كانت مجتمعاتنا العربية لم تتأثر بشكل كبير من مثل هذه الظواهر الإجرامية، إلا أن هناك دولًا عربية كثيرة ومنها الأردن أضحت مهتمة بتلك الظواهر، ومفهومها القانوني، وسمات المجرم المعلوماتي، وهو ما سوف نحاول أن نتعرض له بشيء من التفصيل في هذه الدراسة محاولين أن نستعرض الإطار التنظيمي والتشريعي في تلك المسألة.

وفي ظل التطور الهائل الذي يشهده العالم في مجال تقنية المعلومات أصبحت الحاجة ماسة وضرورية إلى حماية المعلومات الإلكترونية خاصةً منها ما يتسم بطابع السريَّة؛ حيث برز على السطح أنواعاً من الجرائم الإلكترونية لم تكن موجودة في السابق، ومع غزو الإنترنت دول العالم أصبح من الصعوبة بمكان ضبط وكشف هذه الجرائم نظرا لكونها عابرة للحدود، وتتم بسرعة فائقة دون رقيب أو حسيب ودون رقابة من أي دولة مما أدى الي ارتكاب كافة صور النشاط الإجرامي المتعارف عليها

عبر الانترنت كالسطو على برامج الحاسوب بغرض سرقة البيانات وقاعدة المعطيات المعلوماتية حتى السرية منها واستخدامها في التجسس، أو تلك المتعلقة بالقرصنة والسطو على الأموال إلى جانب ظهور ما اصطلح عليه بالإرهاب الإلكتروني وتهديد الأمن القومي للدول، ولعل التجسس الإلكتروني يأتي في مقدمة هذه الجرائم و تعتبر حماية الأمن العام وسلامة الدولة والمحافظة على أسرارها من أهم المسؤوليات التي تقع على عاتق الدولة ويتطلب حماية الأمن القومي حماية كافة أسرار ووثائق الدولة التي لها علاقة بأمنها وسلامتها، وهذه الحماية ازدادت صعوبة في ظل التقدم التكنولوجي والعلمي والتطور في وسائل الاتصالات مما جعل وجود قانون ينظم هذه الحماية أمر في غاية الضرورة، ولقد كفل المشرع الأردني الحماية الجزائية لأسرار الدولة كونها عرضة للتجسس

بالطرق الالكترونية الحديثة عن طريق فرض عقوبات على جرائم التجسس وفقاً لقانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971 وقانون الجرائم الالكترونية، فإلى أي مدى استطاع المشرع أن يحمي هذه الأسرار من جريمة التجسس الالكتروني؟ وهل تناولت هذه التشريعات كافة الاشكاليات التي قد تواجه تعقب هذه الجريمة وهل هي رادعة؟ هذا ما سنقوم بدراسته والبحث به من خلال هذه الدراسة.

أهمية الدارسة

تتمثل أهمية هذه الدراسة في توضيح أهم النصوص القانونية التي عالجت مسألة الحماية القانونية لأسرار الدولة من التجسس الالكتروني ودراستها، وتكمن أهمية الدراسة أيضاً في بيان السياسة التي سار عليها المشرع الأردني في تجريمه للأفعال التي تؤدي إلى التجسس وإفشاء أسرار الدولة، كما ستقوم الدراسة بإجراء تحليل للنصوص الجزائية التي صاغها المشرع الأردني، وبيان مدى استيعاب هذه النصوص للواقع الحالي، وما يشهده من ظهور أنماط جديدة في جريمة التجسس مثل استخدام الوسائل الالكترونية، حيث أن الجرائم الماسة بأمن الدولة تعتبر من أخطر الجرائم التي تهدد الدولة في كيانها، وجريمة التجسس هي إحدى هذه الجرائم التي تصدى لها المشرع الأردني في قانون العقوبات بكل شدة وفي قانون الجرائم الالكترونية وغيرها من التشريعات، ولكن يبقى هذا النوع من الجرائم يتسم بالخطورة والتطور المستمر مستخدمًا أساليب حديثة يصعب كشفها خاصة مع التطور التكنولوجي الهائل في جميع المجالات، لهذا من الضروري أن يواكب ذلك تطورًا مستمرًا في النصوص والآليات للوقاية والتصدي لجريمة التجسس، خاصة أن لهذه الأخيرة صورًا متعددة فكيف تناول المشرع الأردني هذا التطور.

أهداف الدراسة:

تهدف هذه الدراسة إلى:

1-بيان المقصود بالتجسس الإلكتروني من خلال توضيح ماهيته وخطورته وأنواعه وكيفية التعامل معه.

2-التعريف بجرائم التجسس الإلكتروني وبيان مدى خطورتها.

3-معالجة النقص التشريعي إن وجد والمتعلق بحماية وثائق الدولة السرية من جرائم التجسس الإلكتروني.

مشكلة الدارسة:

تتمثل مشكلة الدراسة في الوقوف على مدى قابلية ارتكاب جرائم التجسس بوسائل الكترونية ومدى نجاعة النصوص القانونية لمواجهة جريمة التجسس الالكتروني على وثائق وأسرار الدولة، وتحليل فيما لو كان هناك قصور في التشريعات المنظمة لهذه الجرائم، أم إنها تفي بالغرض للحد من هذه الجرائم ومعاقبة الجاني عقاب رادع.

عناصر مشكلة الدارسة:

وتفرع عن المشكلة الرئيسية عدة أسئلة أهمها:

1. ما هي أسرار ووثائق الدولة التي يجب حمايتها من التجسس الالكتروني؟
2. كيف ساهم المشرع في حماية أسرار ووثائق الدولة؟

منهجية الدارسة:

في سبيل معالجة مشكلة الدارسة سيتم استخدام المنهج الوصفي والتحليلي القائم على تحليل النصوص القانونية ذات العلاقة، لاستخراج أهداف المشرع من سنها وغايتها، وتحليل النصوص التي عالجت الموضوع ومقارنتها للوصول إلى قواعد قانونية متكاملة تعالج الموضوع وعمل توصية بها إلى الجهات المختصة من أجل تلافي القصور التشريعي في هذه النصوص إن وجد.

الدراسات السابقة:

1-النوايسة، عبدالله محمد، والعدوان، ممدوح حسن، 2020 جرائم الجسس الالكتروني في التشريع الأردني دراسة تحليلية، علوم الشريعة والقانون، بحث منشور في مجلة الجامعة الأردنية وتناولت هذه الدراسة موضوع جرائم التجسس الالكتروني في التشريع الأردني، نظرًا لخطورة التجسس الالكتروني المتمثل بدخول 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، وسلطت هذه الدراسة الضوء على التشريعات الجزائية الأردنية التي وفرت الحماية للمحتوى الالكتروني المتضمن معلومات سرية تخص الدولة.

2-الشهري، سورية بنت محمد عبد الله (رسالة ماجستير) – جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الشريعة والقانون، 2015 بعنوان المسئولية الجنائية عن التجسس الإلكتروني في النظام السعودي.

وتبرز أهمية هذه الدراسة في: 1. التعرف على ماهية جريمة التجسس الإلكتروني. 2. تحديد عقوبة جريمة التجسس الإلكتروني في النظام السعودي والقانون المقارن. 3. توضيح أوجه الاتفاق والخلاف بين عقوبة جريمة التجسس في النظام السعودي والقانون المقارن والشريعة الإسلامية، وكانت أهم نتائج الدراسة نشوء أنواع جديدة من الجرائم الحديثة التي تشكل خطورة على الفرد والمجتمع نتيجة التطور في عالم المعلوماتية.

وأهم التوصيات: ضرورة تنظيم مرحلة التحضير لجريمة التجسس الإلكتروني عن طريق إجراءات ضبط مانعة من اكتمال النموذج القانوني لتلك الجريمة.2- تثقيف المختصين من رجال الأمن والتحقيق بدورات تساعدهم على فهم وضبط هذه الجريمة بشكل ميسر وسهل.

3-محمد عثمان، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط 2015 بعنوان دور القانون الدولي في مواجهة التجسس الالكتروني وهدفت هذه الدراسة إلى التعرف على دور قواعد القانون الدولي في مواجهة ظاهرة التجسس الدبلوماسي، وذلك من خلال التعرف على ماهية التجسس وأنواعه وبيان مدى شرعيته في ظل القانون الدولي، وكذلك البحث في العلاقة بين التجسس والحصانات والامتيازات الدبلوماسية، ومناقشة حق الدولة المضيفة في حماية أمنها الوطني من إساءة استعمال تلك الحصانات للوصول الى دراسة ظاهرة التجسس الدبلوماسي الالكتروني كواحدة من أهم مظاهر إساءة استعمال الامتيازات الدبلوماسية التي تهدد الامن الوطني للدولة المضيفة.

4-دراسة حياة حسين بعنوان الفضاء الالكتروني وتحديات الامن العالمي 2021 وتناولت هذه الدراسة الفضاء الالكتروني كمحور جديد من شأنه أن يسبب خسارة فادحة قد تكون اقتصادية أو عسكرية أو سياسية وتوضح اهم التهديدات التي تدار في الفضاء الالكتروني وهي الإرهاب الالكتروني والجريمة المنظمة والتجسس الالكتروني مما جعلها تحديات للأمن العالمي، كما تقترح الدراسة إطارًا نموذجيًا لتعزيز الأمان في الفضاء الالكتروني، ويشمل كافة النواحي سواء كانت استراتيجية أو تشريعية أو تنفيذية، وخلصت الدراسة لدراسة النتائج، وكان أهمها أن العصر الذي نعيش فيه هو عصر رقمي بامتياز وأن التدابير التقنية التي تتخذ لمواجهة هذا النوع من الانتهاكات في الفضاء الالكتروني غير قادرة على مكافحة هذا النوع، ومن هنا تبرز أهمية وجود إطار تشريعي

وطني في ظل تنسيق إقليمي يستكمل بتعاون دولي لمعالجة هذه المسألة. وتختلف دراستي عن هذه الدراسات بأنها تناولت القوانين والتشريعات الأردنية التي تتعلق بحماية وثائق وأسرار الدولة من التجسس الالكتروني وبيان وتوضيح القصور التشريعي فيها.

الطبيعة القانونية لجرائم التجسس الإلكتروني في القانون الأردني

ارتبطت الأردن شأنها شأن باقي الدول في الفترات الأخيرة بشبكة الانترنت وشهدت المملكة انتشاراً واسعاً لاستخدام شبكة الانترنت بعد ازدياد استعمال الحاسب الالي بصفة عامة، ولقد توسع استخدام الحاسب الآلي لدى الافراد والدوائر الحكومية على حد سواء وازدادت في نفس الوقت الأخطار التي يمكن أن تتعرض لها شبكات البيانات الحكومية، ولا يتوقف الخطر في مجرد الارتباط بشبكة الانترنت العالمية فقط بينما تكمن الخطورة أيضًا في الضعف الأمني لمعظم الشبكات الحكومية في الوطن العربي، وذلك لاعتماد الشبكات العربية على الشبكة العالمية وغياب التواصل العربي في مجالات التواصل الالكتروني ومما لا شك فيه أن معظم الخبراء المختصون في الشبكات يعرفون أدق التفاصيل عن الشبكة العالمية، وبالتالي فإنه من السهولة لهم اختراقها إذا لم تتوافر حلول أمنية لهذه الشبكات[i]، ويعرف هذا الاختراق باسم جريمة التجسس وسوف نوضح هذه الجريمة من خلال هذا الفصل بتقسيمه إلى مبحثين سنخصص الأول منهما للحديث عن ماهية جرائم التجسس الالكتروني، والثاني عن أركان جريمة التجسس الالكتروني.

ماهية جرائم التجسس الالكتروني

يعرف التجسس الإلكتروني بأنه عبارة عن عدة طرق تتمركز على التقنية التكنولوجية والبرمجية للحصول على معلومات غير معلنة على العلن، ويتم التجسس عن طريق الوصول إلى الملفات الرئيسية في الحاسوب أو الأجهزة الذكية وزرع برامج تجسس وتسجيل بيانات ثم رفعها إلى أجهزة الشخص القائم بأعمال الابتزاز وحفظها في ملفات خاصة ليتم استخدامها في الوقت المناسب، ولكن كيف عرف القانون جرائم التجسس الالكتروني؟ وماهي صور هذه الجرائم؟ هذا ما سنقوم بتوضيحه

---

[i] النوايسة عبد الإله ، والعدوان ممدوح 2019 جرائم التجسس الالكتروني في التشريع الأردني، دراسة تحليلية، مجلة دراسات علوم الشريعة والقانون، مجلد 46، عدد1 ملحق 1 ص 2 .

من خلال هذا المبحث، وذلك بتقسيمه إلى مطلبين الأول نتناول فيه تعريف جرائم التجسس في اللغة والقانون والمطلب الثاني سنخصصه للحديث عن صور جرائم التجسس الالكتروني.

المطلب الأول: تعريف جرائم التجسس الالكتروني

إن حماية أمن الدولة وسلامتها يعتبر من أهم المسؤوليات التي تقع على عاتق الدولة ويتطلب حماية امن الدولة القومي حماية أسرار الدولة ووثائقها التي لها علاقة بأمنها وسلامتها، وهذا الأمر يزداد صعوبة مع التقدم العلمي السريع والتطور التكنولوجي في مجال وسائل الاتصالات مما جعل وجود تشريعات تحمي هذه الأسرار والوثائق أمرًا ضروريًا ومؤكدًا، حيث أنه بتطور هذه الوسائل أصبح هناك تطور في أدوات التجسس أيضًا وأساليبه، وتفرع عن هذا التطور ظهور صور وأشكال وأنواع للتجسس الالكتروني، وكان لابد لنا من توضيح تعريف للتجسس مبدئياً من خلال تقسيم المطلب إلى فرعين الفرع الأول تعريف التجسس في اللغة والفقه والفرع الثاني للبحث في التعريف القانوني للتجسس.

الفرع الأول: تعريف جرائم التجسس في اللغة

اختلفت الاجتهادات في تعريف الجريمة الالكترونية اختلافًا كبيرًا، ويرجع هذا الاختلاف إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، وتباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى، فمن نظر إليها من زاوية باعتبار الأداة الالكترونية هي الوسيلة المستخدمة في ارتكاب الجريمة سواء كان جوال أو كمبيوتر أو فاكس أو كاميرا فعرفها على أنها" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي [ii]، وفيما يتعلق بالتجسس الالكتروني لغة واصطلاحاً فإنه:

أولاً: التجسس لغة

مأخوذ من الجس، وهو جس الخبر، ومعناه: بحث عنه وفحص، وتجسست فلاناً ومن فلان: بحثت عنه، والتجسس بالجيم: التفتيش عن بواطن الأمور وأكثر ما يقال في الشرِّ، والجاسُوسُ: العين

[ii] د. رستم، هشام محمد فريد، 1995 قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، ص 29.

يتجسس الأخبار ثم يأتي بها، وهو صاحب سِرِّ الشَّر، والناموسُ صاحب سرِّ الخير [iii]. التجسس من الجس، والجس هو اللمس باليد وموضعه المجسة، وجس الشخص بعينه: أحد النظر اليه ليستبينه ويستثنيه وجس الخبر: بحث عنه وتفحص وتجسس الأمر إذا تطلبه ويبحث عنه، والجاسوس صاحب سر الشر [iv].

وبالاستناد إلى المعجم الوسيط، يُعرف تجسس الخبر على أنه: "بحث عنه وفحصه"، وأن الجاسوس هو "من يتجسس الأخبار ليأتي بها". بالإضافة إلى ذلك، ورد تعريف التجسس ضمن المعجم السياسي وفقاً لما يلي: "يشمل هذا المصطلح جميع الأعمال الموجهة للحصول على المعلومات والاستخبارات عن طريق الأعمال السرية، وقد يكون ذلك عن طريق شخص يقوم بجمع المعلومات عن بلده لجهة أجنبية معينة، والبحث عن الأخبار وفحصها، وإرسالها عبر شبكة تجسس".

وقد ورد قوله تعالى " ولا تجسسوا " سورة الحجرات الآية 12، اي بمعنى لا تبحثوا عن عورات الناس وتستكشفوا عما ستره الله تعالى، كما ورد قوله تعالى " يا بني اذهبوا فتحسسوا من يوسف وأخيه " سورة يوسف الآية 87، وفيه معنى طلب الأخبار عنه.

ويُعرف ادموندسون –التجسس على أنه: "نشاط غير قانوني يمارسه شخص عينته أو كلفته دولة أجنبية بغية الحصول على معلومات سرية تتعلق بالدفاع الوطني لدولة." لذا من خلال هذا التعريف يتبين أن التجسس عملية غير قانونية تقوم بها دولة ما لحصول على المعلومات من الدولة الأخرى. وهذه المعلومات تكون سرية لما لها من تأثير على خيارات الدولة الاستراتيجية. كما يشير ديتوربت– إلى أنّ التجسس هو "(السعي سراً نحو جمع المعلومات الخاصة بالدولة بنية تسليمها إلى حكومة أجنبية الأمر الذي يؤدي إلى الإضرار بالدولة)." فيتضح من خلال هذا التعريف أن التجسس يسبب أضراراً للدولة كونها تسلم المعلومات إلى جهات أجنبية تستخدمها ضد مصالح الدولة التي تم التجسس عليها.

أما الجاسوس: فهو العين يتجسس الاخبار ثم يأتي بها وقيل الجاسوس: الذي يتجسس الاخبار [v]، والتجسس الالكتروني يعني: دخول الجاني إلى الشبكة المعلوماتية أو نظام المعلومات أو موقع

[iii] انظر: ((تهذيب اللغة)) للأزهري (242/10)، و((لسان العرب)) لابن منظور (38/6)، و((تاج العروس)) للزبيدي (15/499).

[iv] ابن منظور، ابي الفضل جمال الدين محمد بن مكرم، لسان العرب، بيروت، دار صادر، المجلد السادس، ص38.

[v] ابن منظور، ابي الفضل جمال الدين محمد بن مكرم، لسان العرب، بيروت، دار صادر، المجلد السادس، ص38.

الكتروني للحصول على محتوى الكتروني غير متاح للجمهور يمس الأمن الوطني أو العلاقات الخارجية للدول أو السلامة العامة أو الاقتصاد الوطني [vi].

ثانيًا: التجسس اصطلاحاً

لم يرد في كتب الفقه تعريفاً محدداً للتجسس، وقد يعود ذلك إلى ظهور معناه ووضوحه، حيث أنه لم يجعل الفقهاء للتجسس معنىً زائداً على المعنى اللغوي، ولم يجعل الفقهاء له موضعاً محدداً شمل فيه أحكامه، بينما كانت أحكامه موضحة في أكثر من موضع، وهذا بسبب اختلاف المواقع والميادين التي يتصل بها.

ويعتبر التجسس نمط من أنماط السلوك الانساني رافق نشوء المجتمعات منذ زمن بعيد وتطور بتطور المجتمعات حتى أصبح في عصرنا الحاضر له شأن كبير وأهمية بالغة [vii].

ولقد ورد ذكر التجسس في القرآن الكريم والسنه النبوية عن طريق النهي عنه حيث جاء في القرآن الكريم في سورة الحجرات قوله تعالى " يا أيها الذين آمنوا اجتنبوا كثيراً من الظن إن بعض الظن إثم ولا تجسسوا ولا يغتب بعضكم بعضًا ....." سورة الحجرات الآية 12، وهنا التجسس المنهي عنه هو التجسس على عورات الناس ومحاولة الوصول إلى معرفتها.

أما في السنة النبوية الشريفة جاء النهي عن التجسس في الأحاديث النبوية ومنها ما جاء عن أبي هريرة رضي الله عنه عن الرسول صلى الله عليه وسلم أه قال:" إياكم والظن فإن الظن أكذب الحديث، ولا تحسسوا ولا تجسسوا ...."[viii].

وعرف التجسس اصطلاحًا بأنه: البحث عن العورات والمعايب، وكشف ما ستره الناس [ix].

والتجسس: هو قيام الأجنبي بجمع الوثائق والمعلومات السرية المتعلقة بالوضع السياسي والاقتصادي والمواد العسكرية والتنظيم الدفاعي والهجومي للدولة، وذلك بقصد تسليم تلك الوثائق والمعلومات إلى الدول الأجنبية سواء كان ذلك مجاناً، أو بمقابل أو هو البحث عن أي نوع من

[vi] المادة 12 من قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015.

[vii] الدغمي ،محمد راكان، 1985، التجسس وأحكامه في الشريعة الإسلامية ، القاهرة، دار السلام للطباعة، ط2 ص 65.

[viii] النووي، الامام الحافظي محيي الدين ابو زكريا ، يحيى بن شرف بن مري (المنهاج في شرح صحيح مسلم بن الحجاج) شرح النووي علي مسلم بيت الأفكار الدولية – رقم 82-3583 ص 1537.

[ix] انظر: ((تهذيب اللغة)) للأزهري (242/10)، و ((لسان العرب)) لابن منظور (38/6)، و ((تاج العروس)) للزبيدي (15/499).

المعلومات خفية عن دولة معينة بهدف إيصالها إلى دولة أجنبية وذلك بنية الإضرار بالدولة المتجسس عليها [x].

وعرف التجسس أيضًا بأنه البحث والتفتيش عما يخفى من الأخبار والمعلومات السرية الخاصة بالعدو بواسطة اجهزة التجسس بقصد الاطلاع عليها والاستفادة منها في اعداد خطة المواجهة [xi].

أما فيما يتعلق بفقهاء القانون الجنائي فإنه لم يتم الاتفاق على تعريف موحد للتجسس وكان هناك رأيين في هذا الموضوع، وذهب أنصار الرأي الأول إلى تضييق مدلول التجسس بأن قصروه على وقائع جمع المعلومات العسكرية التي تفيد العدو باستعمال طرق احتيالية وصفات كاذبة [xii]، واتجه الرأي الثاني نحو التوسع في مدلول التجسس، بحيث يشمل كل فعل يخدم مصالح الدولة الأجنبية[xiii].

وهنا يرى الباحث بأن التوجه الثاني قد وسع من نطاق معنى التجسس ليشمل جميع المعلومات التي يكون من شأن تسليمها إلى دولة أجنبية للإضرار بالدولة، وهذا معناه أن التجسس هو عمل استخباراتي بحت. ويطرح تعريف التجسس بعض الصعوبات وخاصة الالكتروني منه نظرًا لجدة المصطلح التي تضاف إلى عدم وجود إجماعًا حول تعريف التجسس، حيث أن معظم التشريعات قد تفادت وضع تعريف جامع ومانع للتجسس لتترك مهمة تعريفه للفقه [xiv].

الفرع الثاني: تعريف جرائم التجسس في القانون

إنّ التجسس ظاهرة قديمة، إذ أنها ليست حديثة النشأة. فقد كانت مهنة التجسس من المهن الأساسية التي يلجأ إليها الأفراد. فاستخدمت مختلف الشعوب والحضارات التجسس لتحقيق غايات معينة، حيث كان أمرًا اهتم به الانسان بكافة المراحل التاريخية وما زال بتطور لافت. "في كل القرون الماضية مارست الأمم والشعوب الكبيرة مهنة التجسس للدفاع عن مصالحها أو لدعم تلك المصالح. لكن التجسس كان محصوراً آنذاك بفترات الحرب، باستثناء بعض الدول التي حرصت على

---

[x] الطراونة، هاني جميل 2011، الجرائم الواقعة على أمن الدولة الخارجي في التشريع الأردني، عمان، دار وائل، ص 91.

[xi] الدغمي، محمد راكان، 1985 التجسس وأحكامه في الشريعة الاسلامية ط2، القاهرة، دار السلام للطباعة، ص25–26.

[xii] حافظ مجدي محمود 1990، الحماية الجنائية لأسرار الدولة، الاسكندرية، الهيئة المصرية العامة للكتاب ص222.

[xiii] البقور، فواز 1993، التجسس في التشريع الأردني، دراسة مقارنة، ط3، عمان، ص5 .

[xiv] سلامي، ناديا. 2017. التجسس الالكتروني كأثر للاستخدام غير المشروع للفضاء الالكتروني على أمن الدولة الخارجي، مجلة دراسات، جامعة عمار ثليجي، الجزائر، العدد 56، ص 237.

المحافظة على دوائر استخبارات واسعة في جميع الظروف." فلم تكن القوى التي تنوي الغزو أو المحاربة تقوم بأي خطوة إن لم تعرف مسبقاً بكافة الأخبار والمعلومات المرتبطة بالعدو مثل جيشه وأرضه وأوضاع سلاحه وغيرها. ومن ثم أخذ يتطور مفهوم التجسس حتى بات يُنظم ضمن الأجهزة الاستخبارية للدولة. ولقد تم استخدام التجسس بمختلف أساليبه وأنواعه سواء التقليدية أو الحديثة في مختلف المراحل كفترة الغزوات وإبان الحربين العالميتين الأولى والثانية وخلال الحرب الباردة وغيرها. وعند التحدث عن تعريف جرائم التجسس بشكل عام والالكتروني بشكل خاص نجد صعوبة بالغة خاصة أن التجسس الالكتروني مصطلح جديد بالإضافة إلى عدم الاجماع على تعريف حول التجسس التقليدي، وذلك أن معظم التشريعات قد تفادت وضع تعريف جامع ومانع للتجسس لترك المهمة للفقه [xv]، وللتعرف على تعريف التجسس في القانون لابد لنا من التطرق إلى تعريف التجسس في القانون الدولي والتشريع الأردني.

أولاً: تعريف التجسس في القانون الدولي

لا شك أن ظاهرة التجسس الالكتروني وجرائم أمن الدولة كافة تحتاج إلى جهد دولي واقليمي مكثف لمواجهتها، فالطابع العالمي لجرائم الانترنت يتيح للمجرمين ارتكاب أي نشاط اجرامي في العالم، وهذا يحتم على جميع البلدان ومنذ ظهور الانترنت أن تكثف اساليب الرقابة الوطنية لكي تطال الجرائم المرتكبة في الفضاء السيبيري فاستخدام المجرمين للإنترنت يشكل تهديدًا على الامن الوطني العالمي[xvi] لذلك جاء من ضمن اهتمامات الاتفاقيات الدولية تعريف لمصطلحات تتعلق بأمن وسلامة الأوطان ومنها ما جاء في لائحة لاهاي حيث عرفت لائحة لاهاي للحرب البرية عام 1907 في المادة (29) الجاسوس بأنه ذلك الذي يعمل سراً من وراء ستار زائف للحصول على معلومات في منطقة الاعمال الحربية بنية تبليغها للفريق الخصم[xvii]، وهنا يرى الباحث بان هذه المادة وضعت تعريفا للتجسس بشكل غير مباشر بأنه يهدف إلى جمع المعلومات بطريقة سرية ويتم ذلك في منطقة الاعمال الحربية تحديدًا. وأن تعريف التجسس في المادة السابقة لا تعتبر الجاسوسية في حد ذاتها مخالفة لقواعد القانون الدولي، حيث انها في رأي القانون الدولي ضرورة

[xv] سلامي، نادية 2017، مرجع سابق، ص 237.

[xvi] عبد العزيز خالد بن سلطان، أمن منطقة الخليج.

[xvii] نصر صلاح .2002. الحرب الخفية تاريخ المخابرات، ج1، ط1، القاهرة، دار الخيال، ص 166.

من ضرورات الحرب جرى عليها القانون الدولي كما ان اقتصار تلك المادة على تناول حالة التجسس وقت الحرب سببه ان اغلب الدول التي وضعت اتفاقية لاهاي هي الدول الكبرى الاستعمارية التي أرادت أن تسبغ الصفة القانونية الشرعية على أفعال جواسيسها في وقت السلم [xviii]. والتجسس في وقت السلم فإنه لا يوجد في القانون الدولي أية نصوص تناولت التجسس على أسرار الدولة وقت السلم ذلك انه لم تبرم اية اتفاقية دولية تلتزم بمقتضاها الدول بعدم التجسس على أسرار بعضها البعض [xix]، ويعتبر التجسس في وقت السلم في نظر أغلب فقهاء القانون الدولي عملًا يتعارض مع قواعد القانون الدولي لأنه يمثل انتهاكًا وتهديدًا للسلامة الإقليمية للدول وسيادتها واستقلالها وأمنها [xx].

وبالتالي فان التجسس يكون مخالفاً لقواعد القانون الدولي اذا كانت الطرق والوسائل التي اعتمدت للحصول على المعلومات هي بحد ذاتها أعمالاً ضد القانون الدولي، كانتهاك السيادة الإقليمية بالإضافة إلى واقعة التجسس، وتلجأ الدول عادة إلى الاحتجاج على انتهاك قواعد القانون الدولي دون ان تبدي اهمية كبيرة لواقعة التجسس [xxi].

ويميز القانون الإنساني بين أنشطة المخابرات وأنشطة التجسس داخل إقليم الدولة، وقد وصفت الأنشطة الاستخبارية بقيام أفراد القوات المسلحة بجمع المعلومات لتقييم الوضع وتحديد الخيارات للتعامل مع العدو، وأنه وفقًا للقانون الدولي الإنساني، إذا قام أحد أفراد القوات المسلحة لطرف في نزاع بجمع أو محاولة جمع معلومات عن ذلك الطرف في الأراضي التي يسيطر عليها العدو، فإن ارتداء زيه العسكري أثناء أداء هذا الفعل لن يُعتبر عملاً من أعمال التجسس.

ويرى الباحث أن التجسس يعتبر أحد أهم مظاهر العلاقات الدولية في وقتنا الحاضر، ويمكن القول بأنه لا توجد دولة في العالم لا تقوم بالتجسس على الدول الأخرى، وذلك بغض النظر عن درجة العلاقة بين هذه الدول سواءً أكانت صديقة أم عدوة، وسواء أكان ذلك في زمن السلام والاستقرار أم في زمن الحروب والأزمات، وإنه تستوي بالنسبة للقانون الدولي إذا كانت جريمة التجسس قد وقعت

[xviii] البقور، فواز، التجسس في التشريع الأردني، مرجع سابق، ص26.
[xix] نصر صلاح، الحرب الخفية تاريخ المخابرات، مرجع سابق، ص179.
[xx] لحرش، عبدالرحمن2003 التجسس والحصانة الدبلوماسية، مجلة الحقوق، جامعة الكويت، العدد الرابع، ص179.
[xxi] حافظ مجدي محمود ، الحماية الجنائية لأسرار الدولة، مرجع سابق ص 238.

بالوسائل التقليدية أو كانت بالوسائل التكنولوجية الحديثة عن طريق استخدام اجهزة الحاسوب أو الاجهزة الذكية التي ظهرت مؤخراً، كون الجريمة قائمة بجميع أركانها وتحقق نفس الغاية منها.

وبدأت الدول العربية أيضًا في سن القوانين والتشريعات التي تضمن حماية أمن الدولة من جرائم التجسس الالكتروني وهذه التشريعات بحاجة إلى أذرع فنية وتطبيقية لتفعيلها على كافة المستويات[xxii].

ثانياً: التجسس في التشريع الأردني

لم يضع المشرع الأردني تعريفاً محددًا للتجسس وإنما اكتفى بالتفريق ما بين الوثائق وأسرار الدولة وتصنيفها سواء سري أو سري للغاية أو محدود، وعرفت المادة 2 من قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971[xxiii] المقصود بالأسرار والوثائق أية معلومات شفوية أو وثيقة مكتوبة أو مطبوعة أو مختزلة او مطبوعة على ورق مشمع، أو ناسخ، أو اشرطة تسجيل، أو الصور الشمسية، والافلام، أو المخططات، أو الرسوم، أو الخرائط، أو ما يشابهها والمصنفة وفق أحكام هذا القانون".

وعليه فإن قانون حماية وثائق وأسرار الدولة جاء أولا لحماية أسرار تخص مؤسسات الدولة أو أحد هيئاتها وهذه الأسرار لها علاقة بأمن الدولة، وثانيًا أن تكون هذه المعلومات على درجة من السرية ومجرد إفشائها يلحق الضرر بأمن الدولة الداخلي أو الخارجي، والتجسس الالكتروني وفقاً لقانون الجرائم الالكترونية الأردني[xxiv] رقم 27 لسنة 2015 يعني دخول الجاني إلى الشبكة المعلوماتية أو موقع الكتروني للحصول على محتوى الكتروني غير متاح للجمهور يمس الأمن الوطني أو العلاقات الخارجية للدولة أو السلامة العامة أو الاقتصاد الوطني، ويشمل أيضًا ارتكاب أحد الجرائم المنصوص عليها وفقًا لقانون حماية أسرار الدولة بوسيلة الكترونية.

ويرى الباحث هنا أن الفرق بين هذين التعريفين الواردين في قانون حماية أسرار ووثائق الدولة وقانون الجرائم الالكترونية يكمن في أن جريمة التجسس في قانون الجرائم الالكترونية تقع على محتوى الكتروني فقط ولا تشمل التجسس بالوسائل التقليدية، وأن جرائم التجسس في قانون حماية

[xxii] المؤتمر الدولي الاول لقانون الانترنت، الغردقة، جمهورية مصر العربية، وعقد في فترة 21-25-2005، كتاب عمل المؤتمر ص 98.

[xxiii] قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971 وتعديلاته.

[xxiv] قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015.

وأسرار ووثائق الدولة يكون بصورة وثائق مصنفة على درجات وهي سرية للغاية (المادة 3) تصنف بدرجة (سري للغاية) أية أسرار أو وثيقة محمية إذا تضمنت الأمور التالية:

أ–أية معلومات يؤدي إفشاء مضمونها لأشخاص تقتضي طبيعة عملهم الاطلاع عليها أو الاحتفاظ بها أو حيازتها، إلى حدوث أضرار خطيرة بأمن الدولة الداخلي أو الخارجي أو إلى فائدة عظيمة لأية دولة أخرى من شانها أن تشكل أو يحتمل أن تشكل خطراً على المملكة الأردنية الهاشمية.

ب– خطط وتفصيلات العمليات الحربية أو إجراءات الأمن العام أو المخابرات العامة أو أية خطة ذات علاقة عامة بالعمليات الحربية أو إجراءات الأمن الداخلي سواء كانت اقتصادية إنتاجية أو تموينية أو عمرانية أو نقلية.

ت–الوثائق السياسية الهامة جداً وذات الخطورة المتعلقة بالعلاقات الدولية والاتفاقيات أو المعاهدات وكل ما يتعلق بها من مباحثات ودراسات.

ج–المعلومات والوثائق المتعلقة بوسائل الاستخبارات العسكرية أو المخابرات العامة أو الاستخبارات المعاكسة أو مقاومة التجسس أو أية معلومات تؤثر على مصادر الاستخبارات العسكرية والمخابرات العامة أو المشتغلين فيها.

د– المعلومات الهامة المتعلقة بالأسلحة والذخائر أو أي مصدر من مصادر القوة الدفاعية التي يشكل إفشاؤها خطراً على أمن الدولة الداخلي أو الخارجي.

وبينت المادة 4 من ذات القانون طريقة حفظ الأسرار المصنفة بدرجة سري للغاية وهي" يجري تغليف وإرسال الوثيقة المحمية المصنفة بدرجة (سري للغاية) على النحو التالي:

أ–توضع الوثيقة ضمن مغلف جديد معنون إلى المرسل إليه وتختم بخاتم الدائرة وبخاتم (سري للغاية).

ب– يكتب على الغلاف رقم الوثيقة المحمية ثم يغلف ويشمع بالشمع الأحمر في موضعين بحيث يتعذر فتحه دون كسر الشمع الأحمر.

ج– يرفق بالغلاف نموذج إشعار استلام.

د– يوضع المغلف ضمن مغلف آخر يكتب عليه اسم المرسل إليه ورقم الأوراق الصادرة.

هـ– على المرسل إليه أن يوقع نموذج إشعار الاستلام ويعيده بلا إبطاء إلى مصدره".

والنوع الآخر للأسرار هو سري ونصت علية المادة (المادة 6) الذي جاء فيها " تصنف بدرجة (سري) أية أسرار وثيقة محمية لم تكن من درجة (سري للغاية) إذا تضمنت المعلومات التالية:

أ- أية معلومات هامة يؤدي إفشاء مضمونها لأشخاص لا تقتضي طبيعة عملهم الاطلاع عليها إلى تهديد سلامة الدولة أو تسبب أضرارًا لمصالحها، أو تكون ذات فائدة كبيرة لأية دولة أجنبية أو أية جهة أخرى.

ب- أية معلومات عن مواقع تكديس المواد الدفاعية أو الاقتصادية أو المؤسسات الحيوية المتعلقة بمصادر القوة متى كان لها مساس بسلامة الدولة.

ج- أية معلومات عن تحركات القوات المسلحة أو الأمن العام.

د- أية معلومات عن أسلحة وقوات الدول العربية الشقيقة" وجاء في المادة 7 من ذات القانون أنه "توضع الوثيقة المحمية من درجة (سري) بمغلف جديد مكتوب عليه اسم المرسل إليه ويكتب عليه رقم الصادر ثم يشمع بالشمع الأحمر ثم يوضع ضمن مغلف آخر ويكتب عليه اسم المرسل إليه ورقم الصادر".

والنوع الثالث هو محدود وعرفته المادة 8 والمادة 10 من أسرار الدولة [xxv] "تصنف بدرجة (محدود) أية معلومات أو وثائق محمية تتضمن معلومات تنطبق عليها الأوصاف التالية: أ- أية معلومات يؤدي إفشاؤها إلى أشخاص غير مصرح لهم بالاطلاع عليها إلى أضرار بمصالح الدولة أو يشكل حرجاً لها أو تنجم عنه صعوبات إدارية أو اقتصادية للبلاد أو ذات نفع لدولة أجنبية أو أية جهة أخرى قد يعكس ضرراً على الدولة. ب- أية وثائق تتعلق بتحقيق إداري أو جزائي أو محاكمات أو عطاءات أو شؤون مالية أو اقتصادية عامة ما لم يكن إفشاء مضمونها مسموحاً به. ج- تقارير الاستخبارات العسكرية ما لم تكن داخلة ضمن تصنيف آخر من درجة أعلى. د- التقارير التي من شان إفشاء مضمونها إحداث تأثير سيء على الروح المعنوية للمواطنين ما لم يؤذن بنشرها.

هـ- موجات اللاسلكي العسكرية التابعة للقوات المسلحة والأمن العام والمخابرات العامة أو أية سلطة حكومية أخرى. و- أية معلومات أو وثيقة محمية تضر بسمعة أية شخصية رسمية أو تمس هيبة الدولة ونصت المادة 9 على أنه." توضع الوثيقة المحمية التي تحمل (درجة محدود) في مغلف عادي يكتب عليه اسم المرسل إليه ويشمع بالشمع الأحمر ويختم بخاتم محدود ويكتب عليه رقم الصادر.

[xxv] نصت المادة 10 من قانون حماية أسرار ووثائق الدولة على الوثائق العادية " مع مراعاة أحكام أي قانون اخر تعد جميع الوثائق الرسمية الاخرى التي لا تشملها أحكام هذا القانون (وثائق عادية) وعلى المسؤول أن يحافظ على الوثائق العادية ويحفظها من العبث أو الضياع ولا يجوز افشاء مضمونها لغير اصحاب العلاقة مالم يصرح بنشرها".

وهنا نجد من تصنيف المشرع لأسرار الدولة أنه شمل كل الأشياء والوثائق والمعلومات المتعلقة بسلامة الدولة وغلب صفة الأسرار على المعلومات ذات الطابع العسكري، نجد هنا التعريف الوارد في قانون حماية أسرار ووثائق الدولة لا يتماشى مع التطور التكنولوجي في العصر الحالي كونه تم وضعه في وقت لم يكن هناك انتشار للنظم المعلوماتية وشبكات الانترنت.

ولقد وردت جرائم التجسس أيضًا في نصوص المواد من 14- 16 من قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971، حيث جاء فيها أنها جريمة الدخول أو محاولة الدخول إلى أماكن محضورة بقصد الحصول على أسرار تتعلق بسلامة الدولة وكذلك سرقة الأسرار التي تتعلق بسلامة الدولة أو الحصول عليها وابلاغ الأسرار المتعلقة بأمن الدولة [xxvi].

وجاء في نص المادة 14 من قانون حماية أسرار ووثائق الدولة التي تحدثت عن جريمة الدخول أو محاولة الدخول إلى أماكن محظورة ما يلي:" من دخل أو حاول الدخول إلى اماكن محظورة قصد الحصول على أسرار أو أشياء أو وثائق محمية أو معلومات يجب أن تبقى سرية حرصًا على سلامة الدولة عوقب بالأشغال المؤقتة وإذا حصلت هذه المحاولة لمنفعة دولة أجنبية عوقب بالأشغال المؤبدة أو كانت الدولة الأجنبية عدوة فتكون العقوبة الإعدام"[xxvii].

ويرى الباحث هنا أن المشرع ساوى بين الدخول ومحاولة الدخول ولم ينص على الوسائل التي يتم الحصول على السر بها ولم يحدد المشرع الأماكن المحظورة وترك تحديدها للسلطات المختصة.

كما وعالج المشرع الأردني هذه الجريمة من خلال قانون الجرائم الالكترونية رقم 27 لسنة 2015 وتناول جرائم التجسس في المادة 12 منه والتي جاء فيها :" أ- يعاقب بالحبس كل من دخل قصدًا دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية او نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الامن الوطني أو العلاقات الخارجية للمملكة، أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة اشهر وبغرامة لا تقل عن 500 دينار ولا تزيد عن 5000 دينار" ب- إذا كان الدخول المشار إليه في الفقرة "أ" من هذه المادة بقصد الغاء تلك البيانات أو المعلومات أو اتلافها أو تدميرها أو تعديلها

[xxvi] عبد الاله النوايسه، مرجع سابق، ص 365.

[xxvii] انظر قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971 المادة 14.

وتغييرها أو نقلها أو نسخها أو إفشائها فيعاقب الفاعل بالأشغال المؤقتة وبغرامة لا تقل عن 1000 دينار ولا تزيد عن 5000 دينار".

ومصطلح الامن الوطني في هذه المادة يشير إلى كل شيء يتعلق بسلامة الدولة ضد الاخطار الخارجية والداخلية التي قد تؤدي بها إلى الوقوع تحت سيطرة أجنبية نتيجة ضغط خارجي أو انهيار داخلي [xxviii]، ويرى الباحث من خلال هذه المادة أن المشرع تهاون في العقوبة في الفقرة أ رغم جسامة الفعل، حيث أنه اعتبرها جريمة جنحوية، وكان من باب الأولى أن تكون العقوبة مشددة، وأن تكون عقوبة جنائية لتتناسب مع جسامة وخطورة الفعل.

المطلب الثاني: الأحكام الخاصة بجريمة التجسس الالكتروني

تعددت الأسباب التي تدفع إلى التجسس ولعلّ أبرزها هو جمع المعلومات حول الدول المعادية مما يساهم في تكوين صورة مفصلة عن العدو في حال الحرب وكذلك معرفة سياسته الداخلية والخارجية، وهذا ما أشرنا إليه سابقاً. فيستخدمون المعلومات التي جُمعت لتحصين مكانة الدولة التي يتم التجسس لصالحها ولتأخذ خطواتها والقيام بالتكتيك تبعاً للمعلومات المتوفرة لديها. وعلى سبيل المثال، "منذ نشأة الولايات المتحدة، انخرطت في أنشطة تجسس وجمع معلومات استخبارية من أجل مهاجمة أعدائها،

وتجنب الحسابات الخاطئة، حيث التجسس يساعد الدولة على معرفة نوايا وحقائق عن الدولة التي يتم التجسس فيها. ولكن هذا مرتبط بمدى دقة وسيلة التجسس أو الجاسوس. حيث "الجاسوس عند بعض الدول قد يوفر ألف أو مليون جندي من الموت، وقد يؤدي عمله إلى مقتل ألف أو مليون أو إلى تغيير حكومة أو اسقاط عهد وقيام عهد. الجاسوس الجيد قد يغني عن فعل عشرات الطائرات النفاثة وعشرات الصواريخ وجمع المعلومات للدول الصناعية وذلك للتعرف على كافة الظروف الاقتصادية والتطورات التكنولوجية التي تنشأ في الدول الأخرى، وذلك لمعرفة كافة الأسرار الاقتصادية والتقنية. وهذا الأمر قد لا يكون مقتصر بالتجسس على الدول وإنما على الشركات. فبعض الشركات تبقي على سرية وصفة منتوجاتها وذلك لضمان تفوقها في مواجهة منافسيها. فهذا ما يدفع الأطراف الأخرى إلى القيام بالتجسس لمعرفة هذه الأسرار .

[xxviii] عبد الوهاب الكيالي، 1990 موسوعة السياسة ط2، بيروت، المؤسسة العربية للدراسات والنشر، ص 331.

ولقد تغيرت أدوات وأساليب وصور التجسس في نهاية القرن العشرين، وذلك نتيجة الثورة التكنولوجية والمعلوماتية في مجال الاتصالات، وأصبح العالم عبارة عن قرية صغيرة، وأصبحت كل المعلومات السياسية والاجتماعية والاقتصادية والعسكرية معلومات متاحة للجميع، وأصبحت أدوات التجسس أكثر تطورًا وتقدمًا وذات قدرات خارقة وعالية من خلال استخدام الاقمار الصناعية للتجسس، ومحطات التنصت الضخمة، وحاملات الطائرات المرتبطة بالأقمار الصناعية وأجهزة الحاسوب، وهذا كله جعل الجالس في مكانه يسمع ويرى كل ما يشاء أن يسمعه ويراه على وجه الارض[xxix]. وللتعرف على الأحكام الخاصة بجريمة التجسس لابد لنا من التطرق لمعرفة خصائص هذه الجريمة، وهذا ما سنقوم بتوضيحه في الفرع الاول وسنتحدث في الفرع الثاني عن صور هذه الجريمة.

الفرع الأول: خصائص جريمة التجسس الالكتروني

تعتبر عمليات التجسس عمليات قديمة قدم البشرية وقدم المنازعات البشرية، فمنذ تقدم العصور كان الإنسان يتجسس على أعدائه لمعرفة أخبارهم والخطط التي يعدونها لمواجهته، ولهذا كان للتجسس أهميته الكبيرة على كافة مستويات النزاعات الإنسانية التي مر بها البشر منذ بدء الخليقة [xxx].

وقد تطورت عمليات التجسس طبقا لما يسود المجتمع من تطورات علمية وتكنولوجية في ظل التطور التقني الهائل الذي نعيشه، فقد أصبح ما يعرف بالتجسس الإلكتروني.

تتميز جريمة التجسس الالكتروني بخصائص عديدة تختلف عن معظم الجرائم والسبب في ذلك يعود إلى ارتباطها بجهاز الحاسب الآلي أو الأجهزة الحديثة والشبكة المعلوماتية وأهم هذه الخصائص[xxxi]:

1-إن التجسس الالكتروني لا يترك أي دليل مادي بعد ارتكاب الجريمة مما يصعب عملية التعقب واكتشاف الجريمة.

[xxix] عبد الاله النوايسة، مرجع سابق، ص 8.

[xxx] منير محمد الجنبيهي، 2004 "جرائم الإنترنيت والحاسب الآلي ووسائل مكافحتها". دار الفكر الجامعية. ص 86.

[xxxi] الدربي، عبد العال واسماعيل محمد صادق، 2012 الجرائم الالكترونية، الطبعة الأولى، المركز القومي للإصدارات القومية، القاهرة. ص 55.

2-صعوبة إثبات الجريمة حيث أن هذه الجريمة تمتاز بسهولة إتلاف الادلة في حال العثور على دليل يمكن من خلاله إدانة الجاني وبالتالي فإن إثبات هذه الجريمة أمر يحيط به العديد من الصعوبات، ويرجع هذا إلى افتقاد وجود الآثار التقليدية للتجسس حيث انها تقع في خارج الواقع المادي الملموس وتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل الامور اكثر تعقيداً لدى السلطات وأجهزة الدولة [xxxii].

3-صعوبة اكتشاف الجريمة [xxxiii]، حيث أن مستخدمي هذا النوع من التجسس يمتازون بخلفيات وخبرات في استخدام الأجهزة والتقنيات الحديثة ومن جهة أخرى نجد نقص في الخبرات لدى الجهات المعنية عن كشف المخططات الإرهابية الرقمية والتجسسية.

4-إن التجسس الالكتروني يحصل في بيئة هادئة لا تحتاج إلى القوة والعنف واستعمال الأسلحة وانما تحتاج إلى شبكة انترنت وجهاز حاسوب وبعض البرامج.

5-إن جريمة التجسس الالكتروني جريمة عابرة للحدود، حيث أن شبكة الاتصالات تربط العالم من خلال اقمار صناعية والفضائيات والانترنت مما جعل العالم لا يعترف بالحدود الاقليمية للدول ولا بالمكان ولا الزمان.

وعند التمعن بهذه الخصائص نستخلص أن الجاني في جريمة التجسس الالكتروني يجب أن يتمتع بخبرة ووجود معرفة في مجال أنظمة الحاسب الالي والشبكات، وذلك على عكس مرتكب جريمة التجسس التقليدية، ويجب أن يتمتع بالدرجة كبيرة من المعرفة بأنظمة الحاسوب، وذلك كون الجريمة تستلزم اختراق للزمان والمكان دون أن تخضع لحرس الحدود ويتم ارتكابها عن بعد، وربما يكون الجاني في دولة والجهاز الذي يتم اختراقه في دولة أخرى أو أن تتم الجريمة في عدة دول.

الفرع الثاني: صور التجسس الالكتروني

إن التجسس في العصر الحالي أصبح شاملاً لمختلف مجالات الحياة ولم يعد مقتصراً فقط على المجالات العسكرية والحربية على الرغم من أن هذا النوع هو من أهم وأخطر الأنواع ومن أهم صور التجسس [xxxiv]:

[xxxii] المومني نهلا عبد القادر 2008، الجرائم المعلوماتية، ط1، دار الثقافة للنشر والتوزيع، الأردن، ص 56.

[xxxiii] المومني نهلا عبد القادر 2008، مرجع سابق، ص57.

[xxxiv] عبد الإله النوايسة، مرجع سابق ، ص 360 وما بعدها.

1-التجسس السياسي: والهدف منه معرفة المواقف السياسية لصناع القرار في الدولة والمعلومات التي تتعلق بالسياسة الداخلية والخارجية، وخطط الدولة، ووثائقها السرية وأسرارها، ومعرفة عوامل الوحدة والتفرقة والتيارات الحزبية والدينية ومدى تأثيرها في الأزمات.

2-التجسس العسكري: ويعتبر هذا النوع من اقدم أنواع التجسس وأهمها، حيث كانت الدول تعمل على جمع المعلومات العسكرية حول الدول الاخرى وذلك بغية معرفة الأسرار العسكرية والمعلومات الدقيقة حول الخطط الاستراتيجية للدولة المعادية، ويكون بصورة عميقة خصوصًا بين الدول الكبرى، فتسعى الدول للحصول على أسرار حربية تكنولوجية كي تقف على مدى التقدم الذي وصلت اليه غيرها من الدول خاصة بان تلك الدول يوجد بينها سباق في التسلح المتقدم كان التجسس العسكري من أول أنواع التجسس وأقواها، فكل دولة تسعى للحصول على المعلومات العسكرية الضرورية عن الدول المعادية والصديقة على حد سواء. والتجسس العسكري أو الحربي يهدف إلى معرفة أسرار الدول الأخرى المتعلقة بالجيوش والأجهزة العسكرية والخطط الحربية والأسلحة والصواريخ والذخائر والقنابل الذرية والتجهيزات والمواقع والعديد والعدة العسكرية، وقد أعطت العديد من الدول التجسس 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 [xxxv].

3-التجسس الدبلوماسي: وهو التجسس الذي يقوم على إساءة استعمال الحصانة الدبلوماسية، حيث تعمل البعثة الدبلوماسية على استغلال صلاحياتها وحصاناتها لجمع معلومات تقدمها لدولتها حول الدولة المضيفة، ولكن هذا النوع في بعض الأحيان ليس تجسس سري، إنما في بعض الحالات ينطلق من مهام البعثة المنوط بها إرسال تقاريرها الدورية لدولتها بالإضافة إلى الدراسات، وقد تسهم دار البعثة الدبلوماسية في تسهيل عملية التجسس باعتبارها حصناً يحتمي به أفراد البعثة الدبلوماسية ويستفيدون من حرمتها في ممارسة عملية التجسس [xxxvi].

[xxxv] أحمد بطو، مقال بعنوان: تعريف التجسس الالكتروني، منشور عبر موقع سايبر وأن بتاريخ 30-07-2021، تاريخ آخر دخول: 29-9-2022

[xxxvi] عثمان محمد، 2015، رسالة ماجستير، دور القانون الدولي لمواجهة التجسس الدبلوماسي، كلية الحقوق ، جامعة الشرق الاوسط ، الأردن، ص 52.

1-**التجسس الالكتروني:** وهو من الأنواع الحديثة التي نشطت مع بروز الثورة المعلوماتية، حيث تم اختراق مواقع الكترونية للحصول على معلومات سرية غير معلن عنها، ويتم استخدامها بين الدول الكبرى والصراعات القائمة بينها، وذلك من خلال الهجوم على مواقع الدول المعادية ومراقبة تحركاتها عبر اجهزة حديثة كما أن من الممكن أن يقوم التجسس الالكتروني بين الشركات والأفراد تكون الغاية منه ابتزاز أفراد آخرين عبر مواقع التواصل الاجتماعي [xxxvii].

2-التجسس الاقتصادي: وهو الذي يهدف لمعرفة موارد وحجم الدولة وحجم انتاجها، وميزانها التجاري والاحتياطي لديها وكذلك معرفة المرافق الاقتصادية الحيوية لديها وأماكنها، وديونها الخارجية.

3-التجسس الصناعي: ينصب هذا النوع من التجسس على المعلومات الصناعية والعلمية الخاصة بالدولة من خلال معرفة أسرار هذه الصناعات والأبحاث العلمية خاصة إذا كانت

هذه الصناعات متخصصة في آلات الدفاع الوطني، حيث أن هناك شركات تساعد في الانتاج الحربي وتطوير الأسلحة وهذه المعلومات من أهم وأخطر الأسرار في الدولة.

ويرى الباحث بأن جميع هذه المعلومات وصور التجسس قد تكون على شكل محتوى الكتروني وقد يتم اختراقه، بالرغم من وجود أمن معلوماتي وحماية معلوماتية لهذه المعلومات إلا أنها عرضة للتجسس والاختراق والحصول على المعلومات السرية وافشائها سيما أن أجهزة الحاسوب أصبحت ضرورة لا يمكن الاستغناء عنها في حفظ المعلومات والوثائق الخاصة بكل دولة.

أركان جريمة التجسس الالكتروني

اختلفت الاجتهادات في تعريف الجريمة الالكترونية اختلافاً كبيرًا، ويرجع هذا الاختلاف إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، وتباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى، فمن نظر إليها من زاوية اعتبار الأداة الالكترونية هي الوسيلة المستخدمة في ارتكاب الجريمة سواء كان جوال أو كمبيوتر أو فاكس أو كاميرا فعرفها على أنها" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي [xxxviii]، وللتعرف على أركان هذه الجريمة قسمنا هذا

[xxxvii] أحمد بطو، مقال بعنوان: تعريف التجسس الالكتروني، منشور عبر موقع سايبر وأن بتاريخ 30-07-2021، تاريخ آخر دخول: 29-9-2022.

[xxxviii] د. رستم، هشام محمد فريد، 1995، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، ص 29.

المبحث إلى مطلبين. سنتحدث في المطلب الأول منه عن الأركان العامة للجرائم الالكترونية وفي المطلب الثاني عن الأركان الخاصة بجريمة التجسس الالكتروني تحديداً.

المطلب الأول: الأركان العامة للجرائم الالكترونية

تعتبر جريمة التجسس من الجرائم الواقعة على أمن الدولة، وتمثل نمطًا من أنماط السلوك الإنساني رافق نشوء المجتمعات القديمة، وتطور بتطورها، وأصبح له في العصر الحاضر شأن كبير، وقد أولت الدول ظاهرة الجاسوسية أهمية خاصة فرصدت لتلك الظاهرة الموارد والتكنولوجيا والخطط والأفراد، وسنتحدث في هذا المطلب عن الأركان العامة للجريمة الالكترونية ونرى مدى توافقها أو اختلافها مع موضوع دراستنا وهو التجسس الالكتروني على وثائق وأسرار الدولة ولتغطية جوانب هذا الموضوع سنقسم هذا المطلب إلى فرعين كالآتي:

الفرع الأول: الركن المادي

ويتكون الركن المادي للجريمة الالكترونية من السلوك الجرمي وهو الفعل أو الامتناع عن الفعل والنتيجة الجرمية وعلاقة السببية بين الفعل والنتيجة.

أولاً: السلوك الجرمي

السلوك الجرمي في كافة الجرائم الواقعة على الأشخاص والأموال هو ما يأتي به الشخص من فعل يؤدي إلى إحداث النتيجة التي يسعى إليها، ففي جرائم القتل وفق نص المادة 326 من قانون العقوبات الأردني فإن أي سلوك من الجاني يهدف إلى إزهاق الروح هو سلوك جرمي.

وهنا هل السلوك الجرمي هذا والذي ينصرف على كافة الجرائم التقليدية ينطبق على الجريمة الالكترونية؟

بما أن الجاني في الجرائم الالكترونية يختلف عن الجاني في غيرها من الجرائم من حيث كونه ذو خبرة كافية في مجال استخدام التقنيات الحديثة [xxxix]. فإن السلوك الجرمي الذي سيصدر منه في مجال ارتكاب الجريمة الالكترونية حتما سيختلف عن الجاني التقليدي.

ففي جريمة الإرهاب الإلكتروني مثلًا، فإن السلوك الجرمي هنا، هو إطلاق صفحات أو مواقع تدعو وتحرض على الانضمام لمثل هذه الجماعات، أو مثلا تبين كيفية صنع قنابل [xl].

[xxxix] هروال، نبيلة هبة، الجوانب الاجرائية لجرائم الانترنت، دار الفكر الجامعي، ط1، 2007، ص45

ويتحدد السلوك الجرمي في النص الجزائي الذي يحدد الفعل المجرم وفقًا للشريعة الجزائية وهذه النصوص قد تكون جامدة ومحددة، أو تكون حرة مرنة وغير محددة، حيث أنه قد تطرأ أفعال جديدة لا يشملها النص فلا يكون هناك بد من إعادة التدخل التشريعي لتجريم الافعال الجديدة [xli]، وتكون النصوص مرنة عندما يصعب الإحاطة بالوصف الدقيق للسلوك الجرمي حيث يلجأ المشرع إلى عبارات عامة لوصف السلوك ويحدد النتيجة وعلاقة السببية دون تفصيل أو تحديد للسلوك محل الجريمة [xlii].

والسلوك الجرمي هو أول عناصر الركن المادي لأي جريمة فالجريمة هي السلوك المخالف لإرادة المشرع وتتحقق في العالم الخارجي بمظاهر مادية ملموسة، ويترتب على ذلك أن الأفكار النفسية داخل النفس لا يمكن العقاب عليها ولا يتفق في مجال الفقه الجزائي على مفهوم محدد للسلوك [xliii].

ثانياً: النتيجة الجرمية

والنتيجة الجرمية في الجرائم التقليدية هي ما يترتب على الفعل الذي أتاه الجاني، فلا يكفي قيام الجاني بسلوكه الإجرامي مهما بلغت جسامته، بل لا بد من أن ينتج عن هذا السلوك نتيجة، ففي جريمة القتل لا بد من أن ينتج عن سلوك الجاني وفاة المجني عليه، فإذا لم تنتج الوفاة عن فعل القتل لا نكون أمام جريمة قتل وإنما نكون أمام جريمة شروع في القتل.

أما النتيجة الجرمية في الجريمة الالكترونية، يثور النقاش بشأنها فيما إذا كانت نتيجة الفعل الجرمي في العالم الافتراضي أم في العالم الحقيقي، وفي الحقيقة فإن الفرضيتان محتملات الحدوث في الجرائم الإلكترونية، فمن الممكن حدوثها بالعالم الحقيقي، مثل إزهاق روح إنسان كانت حياته مستمرة عن طريق جهاز كمبيوتر، فباختراق هذا الكمبيوتر (جريمة الكترونية) فإن نتيجتها تكون بالعالم الحقيقي بقتل هذا الإنسان [xliv].

[xl] بحث الجرائم الإلكترونية، بحث منشور على الإنترنت بتاريخ 2012/12/7، http://droit.moontada.com/t622-topic، تم الدخول الى الموقع بتاريخ 2022/10/10 .

[xli] الصيفي، عبد الفتاح، 1997، الجرائم الواقعة على أمن الدولة، دار الهدى، مصر، ص10

[xlii] بهنام، رمسيس 1968 الجرائم المضرة بأمن الدولة، النظرية العامة للقانون الجنائي، المعارف، الاسكندرية، ص52.

[xliii] بهنام، رمسيس، مرجع سابق، ص 67.

[xliv] هروال، المرجع السابق، ص47.

ويبقى في كل الحالات الركن المادي متوافر، وكما سبق وأشرنا، فإن النتيجة الجرمية تشكل مشكلة في موضوع التوقيت والاختصاص، بحيث يمكن أن تدخل دولتين وثلاثة في ذات الجريمة، مما يشكل التنازع في تطبيق القوانين [xlv].

ثالثاً: علاقة السببية

والمقصود بها علاقة السببية بين السلوك الجرمي والنتيجة الاجرامية [xlvi]، وتعتبر علاقة السببية بين الفعل والنتيجة جوهر الركن المادي فلا يكفي لقيام الركن المادي للجريمة أن يقع سلوك اجرامي من الفاعل فقط، وأن تحدث النتيجة بل يلزم أيضًا أن تتسبب هذه النتيجة إلى صاحب هذا السلوك، أي أن يكون بينهما رابطة السببية، ولا يشترط للقول بعلاقة السببية بين السلوك والنتيجة التي حدثت مؤكدة الوقوع بالنسبة للسلوك بل يكفي أن تكون النتيجة التي حدثت محتملة الوقوع وفقا لما تجري عليه الأمور عادة [xlvii].

ويجب أن تتحقق علاقة السببية بين سلوك الجاني وبين النتيجة التي ترتبت على فعله، أي أن النتيجة الجرمية سببها سلوك الجاني، ففي جريمة القتل مثلا وفاة المجني عليه سببه سلوك الجاني الإجرامي.

وقد نستطيع تطبيق ذات القواعد العامة المطبقة على الجرائم العادية على الجرائم الالكترونية فيما يتعلق بعلاقة السببية إذا انطبقت عليها، ففي جريمة سرقة الشيء المعلوماتي، فاختلاس الشيء المعلوماتي يتحقق بالنشاط المادي الصادر عن الجاني سواء بتشغيله للجهاز للحصول على المعلومة أو البرنامج أو الاستحواذ عليها، وهو ليس في حاجة لاستعمال العنف لانتزاع الشيء، وتشغيله لجهاز لاختلاس المعلومة تتحقق النتيجة بحصوله عليها، فرابطة السببية إذن متوافرة بين نشاطه المادي والنتيجة الإجرامية والنتيجة الإجرامية [xlviii].

[xlv] هروال، المرجع السابق، ص47.

[xlvi] كامل السعيد، 2002 شرح الاحكام العامة في قانون العقوبات، دار الثقافة، عمان، ص 205

[xlvii] د.رؤوف محسن، 1966، السبب في القانون الجنائي، دراسة تحليلية مقارنة، ط2، ص 96.

[xlviii] قشقوش، هدى حامد، جرائم الحاسب الالكتروني في التشريع المقارن، 1992، دار النهضة العربية، القاهرة، ص61–62.

ويرى الباحث أنه وبالنظر إلى جرائم أمن الدولة نجد أن البعض منها يأخذ صورة الجرائم الشكلية التي يكفي فيها توافر السلوك دون وقوع النتيجة الجرمية والبعض الآخر منها يأخذ صورة الجرائم المادية التي تتطلب تحقق نتيجة إجرامية ترتبط بالسلوك برابطة السبب والمسبب.

الفرع الثاني: الركن المعنوي

ويتمثل في القصد الجرمي كما هو مفهومه في الجرائم العادية ويعني ذلك العلم بعناصر الجريمة وأن تتوجه إرادة الجاني لارتكاب هذا الفعل، وبالتالي فإن هذا الركن يتكون من علم وإرادة، وأما العلم فهو فهم الأحداث والأمور كما هي في الواقع، أي أنه يسبق الإرادة، وأما الإرادة فهي التوجه لفعل ولتحقيق الفعل الجرمي.

ويرى البعض وبحق في الجرائم الالكترونية أنه حتى لو كانت النتيجة الجرمية بسبب صدفة أو فضول، أي أن الجاني لم يقصد ابتداء أن يرتكب الجريمة، إلا أنه يبقى الركن المعنوي متوافر، حيث أن الأجدر بالفاعل أن يتراجع عن فعله لا أن يستمر، بالتالي فإن استمراره جعل الركن المعنوي متوافر [xlix].

ويرى الباحث مما سبق أن الركن المعنوي هو الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني وان الوصول إلى المجرم المعلوماتي ومعرفة مدى علمه وارادته يشكل عبء فني وتقني بالغ على القائمين بأعمال التتبع والتحليل لملابسات الوقائع الاجرامية المختلفة.

المطلب الثاني: الأركان الخاصة لجرائم التجسس الالكتروني على أسرار الدولة

لقد أصبح ارتكاب الجرائم عبر الوسائل الحديثة أمرًا منتشرًا في العالم أجمع، سيما أن هذه الوسائل قد سهلت على الجاني ارتكاب جريمته وسهولة الوصول والانتشار، نظرًا لمزاياها وحداثتها، وأن جرائم التجسس الالكتروني على أسرار ووثائق الدولة من الجرائم ذات الطابع الخاص نظرًا لخطورتها، وللتحدث عن أركان هذه الجريمة سنقسم هذا المطلب إلى فرعين الأول سنتطرق فيه إلى

[xlix] بحث الجرائم الإلكترونية، بحث منشور على الإنترنت بتاريخ 2012/12/7، http://droit.moontada.com/t622-topic دخول بتاريخ 2022/11/10

محل الجريمة وفي الفرع الثاني سنتحدث عن الركن المادي والمعنوي لجريمة التجسس الالكتروني على أسرار الدولة.

الفرع الأول: محل جريمة التجسس الالكتروني على أسرار الدولة

تتطلب الجرائم المعلوماتية على غرار الجرائم التقليدية حرفية عالية سواء عند ارتكابها، أو عند العمل على اكتشافها من الشخص الذي يرتكبها، أي يجب ان يكون ذلك الشخص خبيراً بالقدر اللازم والكافي بأمور الحوسبة والانترنت، ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي، وأن الشرطة تبحث أول ما تبحث عن خبراء الكومبيوتر عند ارتكاب هذا النوع من الجرائم، وفي جريمة التجسس على أسرار ووثائق الدولة لابد لنا من معرفة ماهي هذه الأسرار والوثائق، ولقد عرفت المادة الثانية من قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971 الأسرار والوثائق المحمية بانها (اية معلومة شفوية أو وثيقة مكتوبة أو مطبوعة أو مختزلة أو مطبوعة على ورق مشمع أو ناسخ .....) ومع توسع الاعتماد على أجهزة الحاسوب وتطور أنظمة المعلومات تطور مفهوم جريمة انتهاك أسرار ووثائق الدولة، حيث من الممكن تعريف السر الالكتروني بأنه: (كل معلومة أو وثيقة محفوظة على وسيط الكتروني لا يمكن الاطلاع عليه الا باستعمال إحدى تقنيات انظمة المعلومات، والسر الموجود على نظام معلومات يحتاج إلى سلوك معين فني ومتطور لتبيانه تمهيدا للتصرف فيه تصرفا غير مشروع)، وجاء في نص المادة 12 من قانون الجرائم توضيح لمحل جريمة التجسس الالكتروني، وهو يكون بصورة بيانات أو معلومات تكون على شكل محتوى الكتروني تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني[1].

وتعتبر ماهية أسرار ووثائق الدولة من منظور القانون رقم 50 لسنة 1971 الذي جاء لحماية أمرين وهما:

1-وجود سر ووثائق تخص مؤسسات الدولة أو احدى هيأتها وأن تكون هذه الأسرار على علاقة بأمن الدولة.

---

[1] عبد الاله النوايسة، مرجع سابق ص14.

2–ان تكون هذه المعلومات على درجة من السرية ومجرد معرفتها يلحق الضرر بأمن الدولة الداخلي أو الخارجي وعلى ذلك يجب حمايتها وأن محل الجريمة هو السر أو المعلومات والوثائق السرية [li].

ويرى الباحث بأن محل جريمة التجسس الالكتروني هي المعلومات والبيانات غير المتاحة للجمهور التي تمس الامن الوطني والعلاقات الخارجية للمملكة والسلامة العامة والاقتصاد الوطني، عدا عن أنه إن كانت تمس الأمن الوطني فإنها تعنى بالمصالح العامة لأمن الدولة الداخلي والخارجي من المخاطر، ومن هنا يتضح بأن هذه الجريمة إن كانت تمس بالأمن الوطني يجب أن تقع على معلومات سريه مخفية، من غير المعقول أن تكون هذه المخاطر الناجمة عن تقديم محتوى يضر بالمصلحة الوطنية معلنة للجمهور، فعادة ما تكون هذه البيانات والمعلومات سرية للغاية، وجاء تصنيفها في قانون حماية أسرار ووثائق الدولة لسنة 1971 بأن تكون على نمط معين (سري– سري للغاية– محدود) وتعد قواعد تصنيف وثائق الدولة والقيود المفروضة على تلك الوثائق من المسائل المهم مراعاتها لكونها قد تمنع إتاحة بعض البيانات كبيانات مفتوحة، ونظم القانون قواعد تصنيف وثائق الدولة من خلال وضع آلية لتصنيفها والتعامل معها، حيث وضع هذا القانون ثلاث درجات للتصنيف وهي: سري للغاية، وسري، ومحدود ويهدف هذا القانون بشكل عام إلى حماية مصالح الدولة الأمنية وحفظ استقرارها وسيادتها ولا يهدف إلى تصنيف جميع وثائق وبيانات الحكومة.

ولا ينظم هذا القانون البيانات التي لا تقع ضمن أي من التصنيفات الورادة في القانون ولا يمنع إتاحة هذه البيانات الغير المصنفة، وعليه فإن لموظفي الجهاز الإداري للدولة دورًا محوريًا في تحديد كمية البيانات التي يمكن اتاحتها للعامة، بتصنيف الوثائق تصنيفًا صحيحًا، وتجنب التشدد في تصنيف البيانات بدرجات تفوق المتطلبات القانونية.

وقد يتم التجسس الالكتروني على وثائق وأسرار الدولة بعدة وسائل منها التجسس من خلال البريد الالكتروني، حيث أصبح البريد الالكتروني وسيلة لا غنى عنها في الكثير من مجالات العمل الخاصة في الاتصالات الثنائية، وقد أصبح في شيوعه وانتشاره يقترب من الهاتف إلا أن مستخدمي البريد الالكتروني لا يأخذون قضية الأمن بجدية ومنهم الذين يحفظون وثائق وأسرار الدولة حيث

[li] المادة 14 من قانون حماية وثائق وأسرار الدولة رقم 50 لسنة 1971.

يكتفون باستخدام كلمة السر في الدخول إلى الحاسب الآلي كوسيلة للتامين وهي بالقطع ليست وسيلة تأمين مثالية، كما أنه في هذا الوقت أصبحت إجراءات تأمين البريد الالكتروني سهلة وممكنة وتقنياته متاحة ومتوفرة مثل تقنيات التشفير الحديثة[lii].

ويرى الباحث أنه عندما نقول أسرار الدولة لا نعني أسرار الحكومة فقط، بل الأسرار العسكرية والأمنية، وكذلك أسرار كبرى الشركات التي يعتمد عليها الاقتصاد الأردني، وأسرار الأبحاث العلمية والاختراعات، وخصوصاً التي ما زالت في طور التجريب مثل بعض الأدوية وغيرها، وجميع الدول لديها أسرارها التي يجب أن تبقى في طيّ الكتمان سواءً عن الدول الأخرى أو حتى عن شعبها، ولا يعني وجود أسرار لدى الدولة مخفية عن الشعب أنّ هذه الأسرار فضائح وانحرافات، ولكن مصالح الدولة العليا – وكمكوّن رئيس منها الشعب – تفرض ألا يكون كل شيء معروض على العامة، أو معروض في أسواق السّياسة والثقافة والاقتصاد.

واكدت ذلك محكمة العدل العليا بقرارها الذي جاء فيه (لا تملك المحكمة إلزام الادارة بإبراز وثيقة للمحاكم إذا صدرت شهادة من رئيس الوزراء بموجب المادة رقم 110 من قانون أصول المحاكمات الحقوقية تفيد أن الأسباب الواردة في الوثيقة المطلوبة إبرازها هي أسباب أمنية وأن كتاب مدير المخابرات العامة هو من وثائق الدولة السرية للغاية وأن إفشاء مضمونه يتنافى والمصلحة العامة)[liii] .

الفرع الثاني: عناصر جريمة التجسس على أسرار ووثائق الدولة

لقد أصبح الأمر سهلًا على الأشخاص المستخدمين للشبكة المعلوماتية أن يرتكبوا الجرائم بشكل عام وجريمة التجسس الالكتروني على وثائق الدولة السرية بشكل خاص، وذلك عن طريق تنفيذ الجريمة خارج إقليم الدولة أو داخلها من خلال الإعلان عن ذلك عبر شبكة الانترنت والاتصال ببعض المنظمات الدولية لاستعراض خطط تنفيذ العمل الإجرامي والاتفاق على طبيعة المعلومات المطلوبة والغاية منها.

[lii] رابحي، عزيزة 2018، الأسرار المعلوماتية وحمايتها الجزائية ، اطروحة دكتوراه ، جامعة ابي بكر بلقايد السلمان ، كلية الحقوق والعلوم السياسية، الجزائر ص 217.

[liii] قرار محكمة العدل العليا رقم 108 الصادر بجلسة 1980/1/1.

أولاً: الركن المادي لجريمة التجسس على أسرار الدولة ووثائقها

إن التقدم الذي شهده عالم التكنولوجيا مع كل ما كان يحمله من إيجابيات لحياة الإنسان إلا أنه كان في الوقت ذاتـه يحمل في طياته بذور الشر التي كانت تنتظر ممن يسقيها مياه الحياة، وسرعان ما وجدت ساقيها المتمثل بالمجرم ألمعلوماتي الذي وجد هو الآخر ضالته التي كان يبحث عنها في التكنولوجيا الحديثة التي أتاحت له فرصة ارتكاب الجريمة والحصول من ورائها على أكبر قدر ممكن من الأموال، وبأقل قدر ممكن من الخسارة والمخاطرة، معتمداً في ذلك على ما يتمتع به من مهارة فنية تقنيه في هذا الصدد، حيث يستطيع قراصنة الحاسب الالي الوصول إلى المعلومات السرية واختراق الخصوصية، وهذا ما يعرف بسلوك التجسس وهو فعل إيجابي قوامه الكشف وانتظار الحقائق المخفية، وهو عمل غير مشروع والفاعل في هذه الجريمة يسعى إلى كشف الأسرار ومعرفتها بغض النظر عن طبيعة هذه الأسرار أو معناها أو جهتها أو قيمتها، وهذه الأسرار مخفية لا يجوز الاطلاع عليها إلا من قبل فئة محددة ومحصورة وضمن قواعد وأصول مرعية تضمن حماية هذه السرية[liv].

ويتمثل الركن المادي في صورة الجريمة التامة من ثلاثة عناصر هي السلوك الجرمي والنتيجة الضارة والعلاقة السببية والركن المادي نشاط مادي يتم تجريمه عملاً بمبدأ قانونية الجرائم والعقوبات[lv].

ويتمثل الركن المادي لهذه الجريمة في السلوك الجرمي الذي يتخذ صورتين:

1-الدخول المباشر والحصول على الدعامة الالكترونية الحاوية لهذا السر أو المعلومة كالحصول على ملف مخزن فيه الأسرار أو المعلومات والوثائق، وسرقة هذه الأسرار والاستحواذ عليها وهذه الأسرار هي معلومات تخص الدولة ويجب كتمانها حرصًا على سلامة الدولة [lvi].

2-الدخول بصورة الكترونية إلى نظام تخزين المعلومات والأسرار وذلك تمهيدا لارتكاب جريمة التجسس والاطلاع على هذه الأسرار والمعلومات بوسائل الكترونية [lvii].

[liv] الزعبي جلال، والمناعسة احمد 2010 جرائم تقنية نظم المعلومات الالكترونية ط1، عمان، دار الثقافة، ص 258.

[lv] حسين علي جبار الركابي 2018، الحماية الجنائية لأمن الدولة الخارجي، منشورات زين الحقوقية، بيروت، لبنان، الطبعة الاولى، ص 58.

[lvi] الجبور، محمد عودة2012 الجرائم الواقعة على أمن الدولة وجرائم الارهاب ،ط2، دار الثقافة، عمان، ص 208.

[lvii] الزعبي جلال، المناعسة احمد ،مرجع سابق ص 266.

والوثائق بشكل عام هي الأوراق التي تحمل في طياتها كتابة بغض النظر إن كانت أوراق تقليدية أو أوراق عبر الانترنت أو الوسائل الحديثة، وبغض النظر عن نوع الكتابة الموجودة فيها سواء كانت محررة بخط اليد أو أن تكون مطبوعة، وسواء كانت رسمية أو غير رسمية، والوثائق المعنية في هذه الجرائم هي وثائق الدولة التي تحتوي على معلومات تخص الدولة وعرفها قانون حماية أسرار ووثائق الدولة الأردني رقم 50 لسنة 1971 في المادة الثانية بأنها :"اية معلومات شفوية أو وثيقة مكتوبة أو مطبوعة أو مختزلة أو مطبوعة على ورق مشمع ..... الخ". وأكدت محكمة التمييز هذه الحماية في قراراتها حيث جاء في حكم محكمة التمييز بصفتها الجزائية المتضمن:" هدف المشرع من خلال استقراء قانون حماية أسرار ووثائق الدولة من وضع هذا القانون إلى حماية أية وثيقة رسمية أو معلوماتية يشكل افشاؤها خطرا على امن الدولة الداخلي أو الخارجي كما أن مواد هذا القانون قد حددت طريقة تصنيف هذه الوثائق 1- سري للغاية 2- سري 3- درجة محدود، وأوضحت المادة التاسعة الباحثة عن درجة محدود بأن أوجبت أن توضح الوثيقة المحمية الداخلة في هذا التصنيف في مغلف عادي يكتب عليه اسم المرسل اليه ويشمع بالشمع الاحمر ويختم بختم محدود ويكتب عليه رقم صادر و....." [lviii].

ثانياً: الركن المعنوي لجريمة التجسس على أسرار الدولة ووثائقها

في حالة قيام الفاعل بالنشاط الجرمي أو ما يعرف بالسلوك الجرمي لا يكون ذلك كافيًا للمساءلة عن الفعل باعتباره جريمة من الناحية القانونية بل لابد من توافر أيضًا الركن المعنوي الذي يسند الجريمة اليه معنويًا وهو توافر القصد الجرمي وأن يكون الفعل متعمدًا وغير ناتج عن خطأ ،ويعرف القصد بأنه توجيه إرادة الجاني نحو تحقيق الواقعة المكونة للجريمة مع علمه بعناصرها كما يحدد القانون في النص الجنائي، وأن نصوص التجريم قد أوضحت ان حماية أسرار الدولة ووثائقها لها من الاهمية ما يجعل الاشتراط لتحقق التجريم وجود قصد خاص لدى الفاعل ولا يكفي فقط القصد العام لارتكاب الجرم، ويتمثل القصد الخاص بقصد الفاعل إيقاع الضرر بالدولة والإساءة لها من

[lviii] قرار رقم 37 لسنة 2005 محكمة تمييز جزاء جلسة 2005/24.

خلال التجسس على المعلومات السرية، ولذلك ينظر إلى انصراف إرادة ونية الفاعل إلى إلحاق الضرر بالدولة وأجهزتها وكذلك شخصيتها[lix].

الحماية القانونية لوثائق الدولة السرية من جرائم التجسس الالكتروني

لقد نتج عن محاولات تطبيق القوانين والتشريعات التقليدية على الأنماط المستحدثة من جرائم المعلومات الكثير من المشكلات القانونية، فصدرت في البداية احكام تطبق النصوص التقليدية على اي فعل ينطوي على اعتداء على أنظمة المعلومات والحاسوب في حين اعتبرته احكاماً اخرى فعلاً مباحاً لم يرد بشأنه نص يجرمه[lx]، وأن المشرع الأردني لم يغفل عن معالجة هذه الجرائم كما أشرنا في الفصل السابق حيث أورد صور لهذه الجرائم في قانون الاتصالات لعام 1995، وجرم قانون المعاملات الالكترونية لعام 2001 استعمال الوسائل الالكترونية في ارتكاب الجرائم، كما وأوجد التشريع الأردني عام 2010 قانون جرائم انظمة المعلومات المؤقت، والذي جرم بدوره العديد من الأفعال التي تستغل وجود التكنولوجيا في ارتكابها، وبقي هذا القانون إلى أن صدر قانون الجرائم الالكترونية رقم 27 لعام 2015 والساري المفعول لغاية الآن، وهو التشريع الاساسي لجرائم تكنولوجيا المعلومات ومن ضمنها جرائم التجسس الالكتروني على وثائق وأسرار الدولة، ونظراً لكون هذه الجريمة ذات طابع خاص لابد أن نوضح آلية الحماية القانونية لهذه الوثائق والأسرار من خلال تقسيم هذا الفصل إلى مبحثين سنتناول في الأول منهم موضوع التدابير الإضافية الخاصة بطبيعة وثائق الدولة السرية وفي الثاني الحماية الجنائية لوثائق الدولة السرية من جرائم التجسس الالكتروني.

التدابير الإضافية الخاصة بطبيعة جريمة التجسس على وثائق الدولة السرية

من الخصائص التي تتمتع بها جرائم التجسس الالكتروني على وثائق وأسرار الدولة انها تبرز ذاتيتها بصورة أكثر وضوحًا في ارتكابها، فإذا كانت الجريمة العادية تتطلب مجهودا عضلياً قد يكون في صورة عنف أو ايذاء ويحتاج إلى تدابير معينة فان الجرائم الالكترونية تتطلب القدرة

[lix] الجبور ،محمد عودة ، مرجع سابق 204.

[lx] محمد غنام، غنام 2000، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، المنصورة، دار الفكر القانوني، ص12.

العالية على التعامل مع جهاز الحاسوب بمستوى تقني عالي [lxi]، وسرية وثائق الدولة التي تكون محملة على أجهزة الكترونية تتطلب أيضًا طريقة معينة للحفاظ عليها من الاختراق أو السرقة والتجسس فما هي التدابير التي ينبغي أن تتوفر لحماية هذه الوثائق؟ هذا ما سنتعرف عليه من خلال هذا المبحث بتقسيمه إلى مطلبين المطلب الأول سنتحدث عن التدابير الاحترازية التي تسبق وقوع الجريمة والمطلب الثاني للحديث عن الاجراءات اللازمة بعد وقوع الجريمة.

المطلب الأول: التدابير الاحترازية التي تسبق وقوع الجريمة

تمثل جرائم الاعتداء على أمن الدولة الداخلي تحدى كبير يواجه المشرع الوطني في مختلف المجتمعات الإنسانية، وذلك بسبب فداحة الأضرار التي قد تنتج عن مثل هذه الجرائم التي قد يترتب عليها انهيار مجتمعات إنسانية بأكملها، وقد كانت الفترة السابقة في الوطن العربي فترة محن لكثير من دوله، حيث تعرضت العديد من هذه الدول للعديد من هذه الجرائم التي مازالت تحاول أن تتعافى منها، وتعيد لمجتمعاتها التوازن الاجتماعي والسياسي والاقتصادي، ومن هنا تظهر أهمية مواجهة هذه الجرائم بقواعد خاصة يمكن من خلالها مواجهة هذه الجرائم بقدر من الحسم والردع [lxii] وللحديث عن التدابير الاحترازية التي تسبق وقوع جرائم التجسس الالكتروني سنقسم هذا المطلب إلى فرعين، سنتناول في الفرع الأول موضوع السمات العامة للمجرم المعلوماتي وفي الفرع الثاني سنتحدث عن شروط المسؤولية الجنائية لحماية وثائق الدولة.

الفرع الأول: السمات العامة للمجرم المعلوماتي

وتعتبر معرفة السمات العامة للمجرم المعلوماتي من ضمن التدابير الاحترازية التي تساهم في الحد من الجريمة وذلك بأنه عند معرفة صفات شخص المجرم يسهل على الأجهزة متابعته والتعامل معه والتدابير الاحترازية هي وسيلة اجتماعية لدرء الخطورة، وهي إجراءات واقية تتخذ ضد من تعد حالته خطرة على سلامة المجتمع، وبالتالي فإن معرفة صفات المجرم تعتبر من ضمن الاجراءات الاحترازية المتبعة في جرائم التجسس الالكتروني على أسرار ووثائق الدولة، والمجرم المعلوماتي هو

[lxi] نهلا عبدالقادر المومني، مرجع سابق ، ص 58 .

[lxii] د. إبراهيم اللبيدي: 2006 الحماية الجنائية لأمن الدولة، دراسة مقارنة، دار الكتب القانونية، القاهرة، ص 75.

كل شخص يأتي أفعال إرادية تشكل سلوك إيجابي أو سلبي باستخدام تقنية المعلومات لإحداث نموذج اجرامي، وأن المجرم المعلوماتي يتمتع بعدة صفات يجب أخذها بعين الاعتبار عند النظر في جرائم التجسس الالكتروني على وثائق وأسرار الدولة، وذلك من أجل معرفة كيفية التعامل معه وللمساعدة على كشف الجريمة ومن هذه السمات:

1- ان المجرم المعلوماتي شديد الذكاء

وهذه الصفة من أهم وأبرز الصفات للمجرم الالكتروني وذلك لأنه يستخدم ذكائه وليس العنف أو القوة [lxiii]، حيث أن الجريمة المعلوماتية تتطلب مقدرة عقلية وذهنية عميقة، ويحاول أن يحقق أهدافه بهدوء، فالمجرم المعلوماتي يسعى إلى أن يصل إلى المواقع ويخترقها ويفكر بطرق ووسائل جديدة لا أحد يعرفها سواه لاختراق الحواجز الأمنية الالكترونية والوصول إلى مبتغاه [lxiv].

2- يخاف المجرم المعلوماتي من كشف جريمته

ويتميز المجرم المعلوماتي بخوفه الدائم من كشف جريمته وهذا الخوف عادة يميز جميع مرتكبي الجرائم إلا أن المجرم المعلوماتي وخاصة في جرائم التجسس على وثائق وأسرار الدولة يكون خائف من انكشاف أمره، وذلك لجسامة الفعل الذي يقوم به [lxv].

3- **المجرم المعلوماتي مجرم متخصص**

يتمتع المجرم المعلوماتي بقدرة عالية على استخدام المهارات والتقنيات الحاسوبية ويستغل هذه المهارات في اختراق نظام التشغيل واكتشاف كلمة المرور والشيفرات السرية خاصة فيما يتعلق بمؤسسات الدولة الخاصة ليحصل على المعلومات السرية الموجودة على هذه الأجهزة، كما أنه يقوم بإخفاء الأثر لكيلا يتم كشفه بسهولة من قبل الأجهزة الامنية حتى لا يتم ملاحقته من اي شبكة[lxvi].

[lxiii] محمد امين الرومي، 2004. جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الاسكندرية، ص22.

[lxiv] نهلا عبد القادر المومني، مرجع سابق، ص 59.

[lxv] نائلة عادل محمد قورة ،2005، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت.ص60.

[lxvi] بشرى حسين الحمداني، 2014، القرصنة الالكترونية وأسلحة الحرب الحديثة، ط1، دار اسامة للنشر، الأردن، ص 59.

4-المجرم المعلوماتي مجرم عائد وذلك يعني أنه يعود إلى ارتكاب جرائم أخرى على الشبكة المعلوماتية انطلاقًا من رغبته في سد الثغرات التي من الممكن أن تمكن الجهات المعنية من التعرف عليه [lxvii].

ويرى الباحث انه وبالرغم من السمات الخاصة بالمجرم المعلوماتي إلا أنه بالنهاية مجرم وبارتكابه للفعل الاجرامي مهما كانت الوسيلة، فإنه يتوجب إيقاع العقوبة عليه نظرًا لجسامة الفعل، وتكمن خطورة هذا المجرم بارتباطها بطبيعة الوثائق التي يتعامل معها وأهميتها، فجرائم التجسس الالكتروني تقع على وثائق غاية في الأهمية، وينتج عن التجسس عليها تهديدًا لسلامة الدولة وأمنها وهي وثائق وأسرار تستحق الحماية.

الفرع الثاني: شروط المسؤولية الجنائية لحماية وثائق الدولة

وضع المشرع الأردني مجموعة من الشروط التي بموجبها تمنح الوثيقة حماية قانونية وحصانة وهذه الشروط تتمثل في:

-ان يكون الوعاء الممثل للوثيقة مشتملا على معلومات تتسم بالسرية ويقصد بالسرية ان تكون تلك الوثائق غير متاحة للعامة، بل يكون الوصول إليها قصرًا على أشخاص معينين ومحددين دون سواهم، وهو ما يترتب عليه أن الوثائق، وهو ما يترتب عليه أن الوثائق التي يكون محتواها متاحا للكافة من حيث الوصول إليه والاطلاع عليه فإنها لا تعد وثائق محمية وقد حدد قانون حماية أسرار ووثائق الدولة نوعية المعلومات السرية ودرجة كلا منها.

-أن يمثل افشاء مضمون السر أو الوثيقة حظرًا أو ضررًا على أمن الدولة وسلامتها وسلامة أفرادها ومصالحهم سواء على الصعير الخارجي أو الداخلي أو تمثل مساسًا بحقوق الدولة أو سياستها.

-أن تكون هذه الوثائق صادرة عن الدولة أو موجهة إليها، سواء كانت صادرة من أجهزة إدارية أو ذات سلطة ومسؤولية في الدولة [lxviii].

[lxvii] غنام محمد غنام، 2010 دور قانون العقوبات في مكافحة جرائم الكومبيوتر والانترنت، دار الفكر والقانون للنشر والتوزيع، المنصورة، ص14.

[lxviii] مسفر بن حسن القحطاني 2015، جرائم نشر الوثائق والمعلومات السرية وافشائها والعقوبات المترتبة عليها في النظام السعودي، مجلة البحوث القانونية والاقتصادية – كلية الحقوق جامعة المنصورة، مصر عدد 58 ص 70.

ويعتبر المحافظة على أسرار الدولة ووثائقها وحمايتها من التجسس الالكتروني من الواجبات المهمة الملقاة على عاتق الجميع، إذ تعتبر من أهم الأسرار على صعيد الدولة لأنها ترتبط بوجودها وبقائها ويعتمد عليها أمنها من نواحي عدة، وإن بعض الوظائف العامة في الدولة تحوي على الكثير من هذه الأسرار المهمة التي يطلع عليها المكلف بخدمة عامة، أو الموظف بحكم عمله اليومي ولولا مركزه الوظيفي لما أُتيحت له إمكانية الاطلاع عليها ومعرفتها، ولما قد ينتج من إتلاف هذه الأسرار أو إفشائها من إضرار بمصالح الدولة، لذلك فان هذا الأمر يعد من أخطر الأمور التي قد تمس أمن الدولة ومصالحها, لذا حرصت الكثير من الدول في تشريعاتها على تجريم التجسس على أسرار الدولة.[lxix] لا يكفي لمسؤولية الإنسان عن جريمة التجسس الالكتروني على وثائق وأسرار الدولة مجرد اتهامه بل يتعين أن يكون لدى جهة الاتهام دليل إدانة وأن لا يتوافر لدى المتهم مانع من موانع المسؤولية أو العقاب وهي صغر السن أو الجنون أو الإكراه الملجئ، حيث أن الأصل في الإنسان البراءة، ولكي يكون مسؤولًا عن فعل معين لا بد من إثبات الادعاء، وهذا الاثبات في مجال الجريمة والعقاب يسمى دليل الادانة وهذا الدليل غالبًا ما يتوافر في مرحلة أعمال الاستدلال ويتولى إدارتها مأمور الضابطة العدلية وسلطة التحقيق والادعاء العام[lxx].

وأن سلطات الاستدلال تعمل لحساب سلطات التحقيق وتحت إشرافها وليس لعملها اتصال مباشر بالقضاء والاجراءات التي تتخذها هذه السلطات ينبغي أن لا تنطوي على قهر أو إكراه مماثل لما يتضمنه التحقيق الابتدائي، فالفرض أن الاستدلال هو مرحلة جمع المعلومات التي يعتمد فيها الموظف على مهارته وتعاون الناس معه من أجل الكشف عن الجريمة وتعاقب مرتكبها، وفي جرائم التجسس على وثائق وأسرار الدولة قد لا تتوافر في مرحلة الاستدلال لدى من يقومون بها الخبرة الكافية والضمانات التي تتوفر عادة للمحقق في الجرائم التقليدية، والتي تقتضيها حماية حقوق الأفراد وكفالة تطبيق القانون بشكل سليم، وكفاية الأدلة في هذه المرحلة هو أمر غاية في الأهمية ويعتبر من أحد المبادئ الأساسية التي يقوم عليها اكتشاف الجريمة، والهدف منها هو حماية البريء من إدانة ظالمة سيما إذا توافر أحد أسباب الإباحة أو أحد موانع المسؤولية والعقاب ومنها صغر السن أو الجنون.

[lxix] د. إبراهيم اللبيدي: 2006 الحماية الجنائية لأمن الدولة، مرجع سابق، ص 88.

[lxx] الدغيدي مصطفى محمود، 1983، التحريات والاثبات الجنائي، القاهرة، دار الشروق للطباعة والنشر، ص202.

المطلب الثاني: الاجراءات اللازمة ما بعد وقوع الجريمة

الجريمة الإلكترونية هي جريمة تقع على المؤسسات أو الأفراد مستخدمي أجهزة الحاسب الآلي أو أجهزة الهواتف الذكية، وهي بلا شك سلوك لا أخلاقي وغير مصرح به وينكره القانون ويعاقب عليه ويدينه الشرع وينبذه المجتمع، حيث يتم ارتكاب الجريمة الإلكترونية باستخدام أدوات الاتصال الحديثة بالإضافة إلى مجموعة البرامج والتقنيات المعدة لهذا الغرض، ولقد تميزت التشريعات الاجرائية لجريمة التجسس الالكتروني على وثائق وأسرار الدولة بعدة ميزات وذلك نظرًا لطبيعة هذه الجرائم الخاصة، وللتعرف على الإجراءات اللازمة ما بعد وقوع الجريمة سنقسم هذا المطلب إلى فرعين سنتحدث بالفرع الأول عن التشريعات الاجرائية الخاصة جرائم التجسس على وثائق وأسرار الدولة وفي الفرع الثاني خطورة جرائم التجسس الالكتروني على وثائق وأسرار الدولة.

الفرع الأول: التشريعات الاجرائية الخاصة جرائم التجسس

تميزت التشريعات الإجرائية لجرائم التجسس الالكتروني على أسرار ووثائق الدولة بعدة ميزات أهمها أنها ساوت ما بين الشروع والجريمة التامة، حيث أنه قد جرت القواعد العامة في التشريع على التفرقة بين الشروع في الجريمة تامًا أو ناقصًا أو تم ارتكاب الجريمة فعلًا إلا أن المشرع في هذه الجرائم تحديدًا قد خرج عن القواعد العامة، وساوى بين ارتكاب الجريمة في جرائم التجسس الالكتروني وبين الشروع سواء كان ناقصا ام تاما وذلك لخطورة جرائم التجسس كونها تمس الامن القومي والمصلحة العامة للدولة [lxxi].

وبما أن السلطات المنوط بها ملاحقة هذا النوع من الجرائم تستند في عملها ابتداءًا على القانون الموضوعي "العقابي" ومن ثم تسير وفق ما يرسمه لها القانون الإجرائي، فإن اشكالية أخرى قد تقع فيها تلك السلطات إذا ما كان القانون الإجرائي عاجزًا عن تقديم ما يلزم لتلك السلطات لملاحقة تلك الجرائم، فالقانون الإجرائي يعد وبحق المساعد الأول لتطبيق القانون العقابي ونظرًا لطبيعة جرائم التجسس الالكتروني على وثائق وأسرار الدولة فإن هذه الجرائم تخضع إلى قضاء خاص حيث نصت المادة 3 من قانون محكمة أمن الدولة رقم 17 لسنة 1959 على أنه "على الرغم من ما ورد في أي قانون آخر تختص محكمة أمن الدولة بالنظر في الجرائم المبينة ادناه التي تقع خلافا

[lxxi] عبد الاله النوايسة 2019، مجلة علوم الشريعة والقانون، المجلد 46، عدد 1، ملحق 1 ص 469.

لأحكام القوانين التالية أو ما يطرأ عليها من تعديل يتعلق بهذه الجرائم أو ما يحل محلها من قوانين:

1) جرائم الخيانة المنصوص عليها في المواد من 110 إلى 117 من قانون العقوبات رقم 16 لسنة 1960 وتعديلاته. 2) جرائم التجسس الواقعة خلافا لأحكام المواد 14 و15 و16 من قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971."

ومن خلال هذه المادة يتضح لنا أن المشرع الأردني قد خصص لنظر جرائم التجسس على أسرار ووثائق الدولة محاكم استثنائية، وهي محكمة أمن الدولة وهو استثناء من الأصل العام الذي يمنح للمحاكم الجزائية الاختصاص بنظر الجرائم المقررة بقانون العقوبات الأردني. ويستفيد من العذر المخفف للعقوبة في جرائم التجسس الالكتروني إذا أبلغ الجاني عن الجريمة قبل اتمامها أو اثناء مباشرة التحقيقات أو ساعد في القبض على باقي المتهمين وفقا لنص المادة 109 من قانون العقوبات الأردني رقم 16 لسنة 1960 والتي تنص على أنه : 1) يعفى من العقوبة من اشترك في مؤامرة على أمن الدولة أو أخبر السلطة بها قبل البدء بأي فعل مهيئ للتنفيذ، 2) إذا ارتكب فعل كهذا أو بدأ به لا يكون العذر إلا مخففًا، 3) يستفيد من العذر المخفف المتهم إذا أخبر السلطة بمؤامرة أو بجريمة على أن الدولة قبل اتمامها أو أتاح القبض ولو بعد مباشرة الملاحقات على المتهمين الآخرين أو على الذين يعرف مخبأهم".

وجرَّمت المادة 16 من قانون العقوبات، كل موظف عام قام بإفشاء أسرار الدولة والوثائق المحمية وفرض عقوبة عليه بالأشغال الشَّاقة لمدة تصل إلى عشرة سنوات.

كما فرضت المادة 355 من القانون نفسه على كل موظف عام حصل بحكم وظيفته أو مركزه الرَّسميّ على أسرار رسميّة وأباح بها لمن ليس له صلاحية الاطلاع عليها، وأقرّت بحق مرتكب الفعل عقوبة الحبس مدة لا تزيد عن ثلاث سنوات.

ووسعت المادة 16 من القانون نطاق الحماية على أسرار ووثائق الدولة، حيث امتدّ حظر إفشاء الأسرار والمعلومات إلى مرحلة بعد انتهاء العلاقة القانونيّة بين الموظف والإدارة العامّة والمتمثلة بالتقاعد، والاستقالة، والإقالة.

ومن خلال النصوص السابقة يرى الباحث أن المشرع أولى للجرائم المتعلقة بأمن الدولة ومنها جرائم التجسس الالكتروني خاصة، تضمنت تشديد الحماية الاجرائية ما بعد وقوع الجريمة ووضح من خلال هذه النصوص إمكانية الكشف عن الجريمة ولو قبل وبعد ارتكابها.

الفرع الثاني: خطورة جرائم التجسس الالكتروني على وثائق وأسرار الدولة

هناك العديد من الآراء الفقهية والقانونية التي اتجهت في تعريف مصطلح "أمن الدولة"، فقد اتجهت فئة منهم إلى أن أمن الدولة يتمثل في "قدرة الدولة على حماية مصالحها الداخلية من التهديدات الخارجية"، أو أن أمن الدولة " مجموعة من الاجراءات التي تسعى الدولة من خلالها إلى حماية حقها في البقاء، وجميع هذه الآراء تعد صحيحة ومشابهة لبعضها، حيث أن أمن الدولة تتجلى بكل ما يتعلق بمصالح الدولة المرتبطة بوحدة الدولة واستقرارها السياسي، ولا بد من الإشارة إلى أن الحماية المقررة لأمن الدولة، لا يقصد بها شخص الدولة فحسب بل تمتد هذه الحماية للحفاظ على كرامة المواطنين وأمنهم وشعورهم بالاستقرار، ونعتبر الاعتداء على أمن الدولة تاماً، سواء أكان الفعل المؤلف للجريمة تاماً أو ناقصاً أو مشروعاً فيه، حسب نص المادة 108 من قانون العقوبات الأردني. وتنص المواد (107 – 134) من قانون العقوبات الأردني، على الجرائم الواقعة على أمن الدولة الخارجي والعقوبات المقررة لِفاعليها، والمواد (135 –153) من قانون العقوبات الأردني، تنص على الجرائم الواقعة على أمن الدولة الداخلي والعقوبات المتعلقة بها.

وتختلف خطورة التجسس إذا كان موجدها ضد الأشخاص العاديين (الطبيعيين) أو الأشخاص الاعتباريين، حيث لا تكون خطورته ذات حدة إذا كان القائم به هم بعض الهواة، وكان الغرض من اختراقهم لأنظمة الحواسب والشبكات هو العبث بالمحتويات أو إلغاء بعضها أو كلها، ويتم ذلك عن طريق إدخال ملف تجسس إلى المجني عليه، ويسمى هذا الملف "حصان طروادة"، وفي حالة إصابة الجهاز بملف التجسس يقوم على الفور بفتح أحد المنافذ في جهاز الشخص المجني عليه، وهذا المنفذ هو الباب الخلفي لحدوث اتصال بين جهاز الشخص المجني عليه وجهاز المخترق[lxxii]، والملف الذي يكون لدى المجني عليه يسمى الخادم، بينما الجزء الآخر منه يسمى العميل وهو يكون لدى المخترق، والذي من خلاله يمكن للمخترق أن يسيطر على جهاز المجني عليه دون أن يشعر، فبإمكان المخترق فتح القرص الصلب لجهاز المجني عليه والعبث به كيفما يشاء سواء بحذف أو بإضافة ملفات جديدة، كذلك يمكن للمخترق معرفة كلمة السر المخزنة في الجهاز وحتى رقم بطاقة الائتمان، وكذلك يمكن للمخترق إذا كان لدى المجني عليه ميكرفون أو كاميرا ديب أن يستمع ويرى كل ما يفعله المجني عليه في المساحة التي يغطيها الميكروفون أو

[lxxii] محمد أمين الرومي، 2003، "جرائم الكمبيوتر والأنترنيت". دار المطبوعات الجامعية، ص: 136.

الكاميرا[lxxiii]. إلا أن أهميته تكمن فيما إذا كان القائم بتلك الاختراقات هي أجهزة المخابرات في بعض الدول للتجسس على الدول الأخرى.

وقد وجدت بعض حالات التجسس الدولي ومنها ما اكتشف أخيرًا عن مفتاح وكالة الأمن القومي الأمريكية، والتي قامت بزراعته في نظام التشغيل الشهير ويندوز Windows وربما يكون هذا هو أحد الأسباب الرئيسية التي دعت الحكومة الألمانية بإعلانها عن استبدالها لنظام التشغيل المذكور بأنظمة التشغيل الأخرى [lxxiv]. كما كشف أخيرًا النقاب عن شبكة دولية ضخمة للتجسس الإلكتروني تعمل تحت إشراف وكالة الأمن القومي الأمريكية (NSA) بالتعاون مع أجهزة الاستخبارات والتجسس في كل من كندا وبريطانيا ونيوزيلندا، ويطلق عليها اسم Echelon لرصد المكالمات الهاتفية والرسائل بكافة أنواعها، سواء ما كان منها برقيًا أو تلكس أو فاكس أو إلكترونياً.

ويرى الباحث أن التجسس الإلكتروني هو أحد أشكال التجسس الحديث فعلى المشرع التدخل لإنشاء قواعد قانونية لزجر التجسس على الوثائق والمعلومات السرية في الدولة، وبالنسبة للتجسس بواسطة الأقمار الصناعية والتجسس بواسطة طائرات الاستطلاع المتقدمة، فإن الدولة في معظم الأحيان لا تتمكن – رغم علمها باسم الدولة التي تتجسس عليها– من ضبط الشخص الذي يقوم بالتجسس إلا في أحوال معينة، وهي إذا ما كان التجسس يتم بالشكل القديم والذي يتم بإرسال شخص من الدولة إلى الدولة الأخرى للحصول على المعلومات من مصادره في تلك الدولة فيتم التمكن من ضبطه.

الحماية الجنائية لوثائق الدولة السرية من جرائم التجسس الالكتروني

إن الحماية الجنائية لوثائق الدولة من أهم الاجراءات المتبعة لضمان سلامة الدولة ويقصد بهذه الحماية بأنها ذلك النشاط الذي يشمل جميع الجهود التي تبذل لحماية معلومات وأسرار الدولة كالسياسة القومية والمعلومات العسكرية والقرارات الدبلوماسية وغيرها من المعلومات التي تؤثر على أمن وسلامة الدولة [lxxv]، ولمعرفة طرق هذه الحماية قسمنا هذا المبحث إلى مطلبين الأول سنتحدث فيه عن أحكام الحماية الجنائية لوثائق الدولة السرية والثاني للحديث عن عقوبة جريمة التجسس الالكتروني.

[lxxiii] محمد أمين الرومي، 2003، "جرائم الكمبيوتر والأنترنيت". مرجع سابق، ص: 137.
[lxxiv] منير محمد الجنبيهي. نفس المرجع، ص: 87.
[lxxv] هاني احمد، الجاسوسية بين الوقاية والعلاج ص30.

المطلب الأول: أحكام الحماية الجنائية لوثائق الدولة السرية

نصت المادة 114 إلى 116 من قانون حماية أسرار ووثائق الدولة على الجرائم الماسة بأمن الدولة وسرية الوثائق والمعلومات المتعلقة بها، وفي هذا المطلب سنتناول هذه الجرائم بالتفصيل ومدى كفاية النصوص التشريعية بتوفير الحماية الجنائية لهذه الوثائق وذلك بتقسيم هذا المطلب إلى فرعين الفرع الأول عن جريمة الدخول أو محاولة الدخول إلى اماكن محظورة الفرع الثاني عن جريمة ابلاغ الأسرار المتعلقة بأمن الدولة وافشائها.

الفرع الأول: جريمة الدخول أو محاولة الدخول إلى اماكن محظورة

نصت المادة 114 من قانون حماية أسرار ووثائق الدولة الأردني على أنه " من دخل أو حاول الدخول إلى مكان محضور قصد الحصول على أسرار أو أشياء أو وثائق محمية أو معلومات يجب أن تبقى سرية حرصًا على سلامة الدولة عوقب بالأشغال المؤبدة، وإذا كانت الدولة أجنبية عدوة فتكون العقوبة الإعدام " وفي هذه المادة يكون السلوك الجرمي المعاقب عليه هو دخول الفاعل أو محاولة دخوله إلى أماكن محظورة الدخول، ويفترض من مصطلح دخول أن يتخطى الفاعل المكان ويجتازه، ولم يحدد هنا المشرع وسيلة معينة للدخول، ويتساوى الدخول بوسائل مألوفة أو بوسائل غير مألوفة مثل الكسر أو الخلع أو التسلق أو بوسائل الخداع أو الغش والتحايل، ولا بد أن يتمتع الجاني في هذه الجريمة بمزايا معينة وقدرات عالية في المهارات الحاسوبية لارتكاب الجريمة، وأن يستغل هذه المهارة في اختراق أنظمة الحاسوب واكتشاف كلمة المرور والشيفرات ليحصل على المعلومة وأن لا يترك أثر[lxxvi]، وفي هذه الجريمة لا يشترط أن يستطيع الجاني الحصول على السر، أي لا يشترط تحقيق نتيجة معينة، حيث أن هذه الجريمة من جرائم الخطر المبكر التي ساوى فيها المشرع بين الفعل والشروع به، على أنه إذا استطاع الجاني الحصول على أسرار ووثائق خاصة بالدولة فإننا سننتقل إلى نص المادة 15 من قانون حماية أسرار ووثائق الدولة.

وهذه الاماكن هي غالبًا أماكن عسكرية ومرافق للدفاع وما يستخدم في أغراضه كما أنها تخضع لحراسة شديدة وعادة يوضع على هذه الأماكن ما يفيد بأنها أماكن محظور الوصول اليها أو مقيد

[lxxvi] بشرى حسين الحمداني، 2014، القرصنة الالكترونية أو أسلحة الحرب الحديثة، ط1، دار أسامة للنشر والتوزيع، الأردن ص59

وممنوع اجتيازها أو الاقتراب منها أو حتى تصويرها، وتبقى هذه الأماكن محظورة إلى أن تقوم الدولة بإلغاء الحظر عنها.

ويكون الركن المادي لهذه الجريمة هو مجرد الدخول أو محاولة الدخول إلى الاماكن المحظورة، ومن خلال هذا النص يرى الباحث أن الدخول يكون للأماكن بمفهومها المادي ولا يسري نص المادة 114 على فعل الدخول إلى الأماكن الافتراضية كالمواقع وأنظمة المعلومات الالكترونية للحصول على سر من أسرار الدولة، مما يجعل هناك ضرورة لتضمين نص خاص بهذا الجزء يتحدد فيه الوسيلة الالكترونية وكيفية تصور الجريمة بها.

أما فيما يتعلق بنص المادة 15 من قانون حماية أسرار ووثائق الدولة فلقد جاء فيه أنه "

أ–من سرق سر أو أسرار أو أشياء أو وثائق أو معلومات كالتي ذكرت في المادة السابقة أو استحصل عليها عوقب بالأشغال المؤقتة لمدة لا تقل عن عشر سنوات.

ب– إذا اقترفت الجناية لمنفعة دولة أجنبية كانت العقوبة الأشغال المؤبدة وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الإعدام".

ومن خلال هذا النص نلاحظ أن المشرع حصر النشاط الجرمي لهذه الجريمة بسرقة أو الحصول على وثائق أو معلومات سرية والسرقة تختلف عن الحصول فالسرقة في نص المادة 399 من قانون العقوبات الأردني تعني :" اخذ مال الغير المنقول دون رضاه"، وهذا يعني أن السرقة تفترض نشاط للجاني مفاده أن يتم تحريك الشيء من محله والحيازة وحرمان الحائز منه، وهذا لا يقع الا على الأشياء المنقولة ولا يمكن تصوره على غير ذلك، ويلزم لإتمام جريمة السرقة قصد جرمي خاص يتمثل بظهور السارق بمظهر المالك، أي لا بد أن يكون قاصدًا تملك الشيء محل السرقة، فالأشياء التي تعتبر أسرار ووثائق الدولة يمكن سرقتها وأي سر معلومة مجسدة بكيان مادي يمكن سرقتها، وبالتالي فإن أخذ المعلومات أو الاطلاع عليها من أجهزة الحاسب الآلي وبأي وسيلة فإنه يكون جريمة التجسس على أسرار الدولة أو سرقة أسرار الدولة ووثائقها. ومصطلح الاستحصال أو الحصول يغني عن مصطلح السرقة فهو مصطلح عام وأوسع من مفهوم السرقة ويستوعب كافة الوسائل التي قد يلجأ اليها الفاعل للحصول على السر أو المعلومات. [lxxvii]

[lxxvii] الفاضل محمد، 1978، الجرائم الواقعة على أمن الدولة، دراسة مقارنة، دار المطبوعات الجامعية، دمشق، ط4، ص 380.

الفرع الثاني: جريمة إبلاغ الأسرار المتعلقة بأمن الدولة وافشائها

جاء في نص المادة 16 من قانون حماية أسرار ووثائق الدولة على أنه " أ- من وصل إلى حيازته أو علمه أي سر من الأسرار أو المعلومات أو أية وثيقة محمية بحكم وظيفته أو كمسؤول أو بعد تخليه عن وظيفته أو مسؤوليته لأي سبب من الأسباب فابلغها أو افشاها دون سبب مشروع عوقب بالأشغال المؤقتة مدة لا تقل عن عشر سنوات، ب- ويعاقب بالأشغال المؤبدة إذا أبلغ عن ذلك لمنفعة دولة أجنبية، وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الإعدام" وعند النظر إلى هذه المادة نجد أن المشرع حدد لقيام هذه الجريمة عناصر معينة وهي أن يكون الفاعل حائزًا على سر من أسرار الدولة والعنصر الثاني هو ان الركن المادي لهذه الجريمة يتمثل في الابلاغ أو الافشاء لهذه الأسرار، والعنصر الثالث يتمثل في أن يكون الابلاغ أو النشر لسر من أسرار الدولة التي تتعلق بالأمن والسلامة، والعنصر الرابع في أن يكون فعل الافشاء أو الابلاغ بدون سبب مشروع أو بدون مبرر.

وهنا نجد أن النشاط المجرم في هذه المادة هو القيام بالإبلاغ أو الافشاء لهذه الوثائق والأسرار، ويقصد بالإفشاء الافضاء بالسر إلى الغير أو تمكينه من الاطلاع عليه [lxxviii]، أما الإبلاغ فهو يعني إيصال السر إلى الغير، وإفشاء السر لا يتصور أن يقع ممن يجهل مضمون السر أما الابلاغ فقد يقع ممن يعلمه وممن لا يعلمه، ويكفي أن يكون الفاعل في الإبلاغ عالمًا بما يقوم به من أن ما يقوم بإبلاغه هو سر من أسرار الدولة، أو وثائقها والمتصل بأمن الدولة حتى لو لم يكن يفهم محتواه، وكذلك إفشاء السر فإنه لا يستهدف شخصًا معينًا أو جهة محددة، بينما يكون الهدف منه إيصال السر أو نشره[lxxix]، وهنا يرى الباحث أن هذه الجريمة تتم بوسائل الكترونية وهي من جرائم الخطر على أمن وسلامة الدولة وتعتبر من صور التجسس الالكتروني على وثائق وأسرار الدولة التي يجب ان تتم معالجتها، وخيرًا فعل المشرع عند تشديد العقوبة عليها.

ويرى الباحث أن قيام الجاني بالدخول أو الولوج إلى النظام المعلوماتي بقصد الاعتداء على بيانات أو معلومات غير مُتاحة للجمهور، تمس الأمن الوطني أو العلاقات الخارجيّة للدّولة أو السلامة

[lxxviii] عبد المهيمن بكر، 1976، جرائم أمن الدولة الخارجي، دراسة في القانون الكويتي والمقارن، دار النهضة العربية، القاهرة ص138.

[lxxix] محمد الفاضل، مرجع سابق، ص 319.

العامّة من خلال حذفها أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو مسحها أو إفشائها يُعد جريمة تنال من أسرار الدّولة، واعتداءً على حقّها في سريّة هذه المعلومات وعدم كشفها.

المطلب الثاني: عقوبة جريمة التجسس الالكتروني

إن حماية الأمن العام والسلامة العامة للدولة من أهم مسؤوليات الدولة ويتطلب حماية الامن القومي للدولة حماية كافة أسرار ووثائق الدولة، الأمر الذي يزداد صعوبة مع التقدم العلمي والتكنولوجي مما أصبح معه وجود تشريع يحمي تلك الأسرار والوثائق أمرًا ضروريًا، وفرض عقوبات خاصة لمرتكبي هذه الجرائم لضمان الحد منها هو بذات الأهمية، فلا بد من مواكبة التشريعات لهذا التطور بما يكفل التأكد من حماية أمن الدولة وبما لا يتعارض مع حق المواطن في الحصول على المعلومات، ولقد كفل المشرع الأردني ذلك من خلال إيجاد نصوص عقابية للحد من هذه الجرائم، وللحديث أكثر عن هذه النصوص قسمنا هذا المطلب إلى فرعين سنتحدث في الفرع الأول عن عقوبة التجسس الالكتروني في قانون حماية أسرار ووثائق الدولة، وفي الفرع الثاني عن عقوبة التجسس الالكتروني في قانون حماية الجرائم الالكترونية.

الفرع الأول: عقوبة التجسس الالكتروني في قانون حماية أسرار ووثائق الدولة

إن كل عمل يضر بأمن الدولة وسلامتها ويمكن للعدو منها يعاقب مرتكبه وذلك صونًا للبلاد وتمكينًا لها ودفعًا لكل ما من شأنه أن يضر بها, ولقد حرص القانون المصري علي إنزال أقصي العقوبة لمرتكبي مثل هذه الجرائم عمدًا, حيث رصد لها عقوبة الإعدام سواءً وقعت في وقت السلم أو الحرب ولم يكن المشرع الجنائي مبالغًا في تشديد العقاب علي مرتكب هذه الطائفة من الجرائم, حيث أن أغلب التشريعات الجنائية المقارنة مثل فرنسا وإيطاليا وغيرهما قد رصدا عقوبة الإعدام لمرتكب هذه الجريمة، وعند النظر إلى قانون حماية أسرار ووثائق الدولة الأردني نجد ان المشرع عاقب على جريمة الحصول على أسرار الدولة أو سرقتها بصورة مجردة وبعقوبة الأشغال المؤقتة مدة لا تقل عن عشرة سنوات، أي من عشر إلى خمس عشرة سنة، وحدد المشرع أنه إذا اقترفت

الجريمة لمصلحة دولة أجنبية تكون العقوبة الأشغال المؤبدة وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الاعدام.[lxxx]

ولم يشترط المشرع لأعمال الظروف المشددة لهذه الجريمة أن يوصل الفاعل أو مرتكب الجريمة هذا السر إلى الدولة الأجنبية أو الدولة العدوة بل يكفي أن يحصل على السر ويثبت ذلك، وبعدها يتم تشديد العقوبة إذا علم أنه قد حصل على السر لمنفعة دولة أجنبية أو دولة عدوة كما هو موضح بالنص.

ويعاقب من ارتكب جريمة إفشاء أو إبلاغ الأسرار المتعلقة بأمن الدولة دون سبب مشروع بالأشغال المؤقتة لمدة لا تقل عن عشرة سنوات ويتم تشديد العقوبة إلى الأشغال المؤبدة إذا تم ارتكاب الجريمة لمنفعة دولة أجنبية، وتشدد العقوبة لتصبح الاعدام إذا كانت لمنفعة دولة عدوة.

ويرى الباحث أن مبدأ الشرعية الجنائية يقضي على أن تكون نصوص التجريم دقيقة وصريحة الدلالة، أما بالنسبة للنصوص الخاصة بجرائم أمن الدولة ، فإنها تتصف بالمرونة، ويرجع ذلك إلى صعوبة تحديد طبيعة هذه الجرائم فإن معالمها غير واضحة، فأمن الدولة يضيق ويتسع حسب الزمان والمكان، وتهدف هذه المرونة إلى توسيع حرية القاضي عند تطبيق النصوص، ولا يمكن تدارك هذه المرونة إلى عن طريق القضاء، ونظراً لخطورة هذه الجرائم وخطورة نتائجها، فإن العقوبة المقررة لهذه الجرائم يجب أن تتسم بالشدة، وأن تكون معظم هذه الجرائم معاقب عليها بالإعدام، والأشغال الشاقة المؤبدة أو المؤقتة في قانون العقوبات الأردني.

الفرع الثاني: عقوبة التجسس الالكتروني في قانون حماية الجرائم الالكترونية

لم يدخر المشرع الأردني جهدًا في تقرير الحماية المناسبة لوثائق الدولة وأسرارها بمختلف درجات سريتها وإيقاع العقوبة الرادعة على مرتكبي هذه الجرائم نظراً لخطورة التجسس بصفة عامّة والتجسس الإلكتروني بصفة خاصّة، وأوجد القوانين التي من شأنها توفير حماية خاصّة للمعلومات والمعطيات المتداولة عبر الشبكة العنكبوتيّة وحمايتها من الاختراق أو التلاعب بمختلف صوره، وتفطّن المشرع الأردني مُبكراً لخطورة هذا النوع من الجرائم وقام بسن العديد من الأحكام الموضوعيّة والإجرائيّة للوقاية من جريمة التجسس وجرائم المعلوماتيّة بصفة عامّة ومكافحتها.

[lxxx] المادة 15 من قانون حماية وثائق وأسرار الدولة، رقم 50 لسنة 1971.

ونصت المادة 12/أ من قانون الجرائم الالكترونية على انه "يعاقب كل من دخل قصدًا دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو نظام معلومات للاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الامن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة شهور وبغرامة لا تقل عن 500 دينار ولا تزيد عن خمسة الاف دينار أردني".

وجاء في نص المادة 12/ج من نفس القانون انه" يعاقب كل من دخل قصدا إلى موقع الكتروني للاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الامن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن 500 دينار أردني".

وعند النظر إلى هاتين المادتين نجد ان الدخول في النص الأول الفقرة أ يعني الدخول إلى الشبكة المعلوماتية، بينما الدخول في الفقرة ج من نفس القانون يكون للموقع الالكتروني بشكل عام والعقوبة والغرامة تختلف في الفقرتين بالرغم من أن جسامة الفعل واحدة فالدخول إلى الشبكة المعلوماتية يساوي تقريبًا جسامة فعل الدخول إلى الموقع الالكتروني، وكان على المشرع الأردني أن يساوي بالعقوبة المشددة بينهم وأن تكون العقوبة أكثر لتتماشى مع جسامة الفعل.

والمشرع الأردني إذا لاحظنا لم يعاقب على الشروع في هذه الجنح لمجرد محاولة الدخول إلى الشبكة المعلوماتية أو الموقع الالكتروني من أجل التجسس على المعلومات أو الاطلاع عليها لا يعتبر جريمة لتعلقها بالأمن الوطني أو لتعلقها بالعلاقات الخارجية للمملكة أو السلامة القامة أو الاقتصاد الوطني لأن هذه الجرائم من الجنح، ولم يرد في قانون الجرائم الالكترونية نص يعاقب على الجنح الواردة فيه[lxxxi]، ولقد وردت الظروف المشددة لجريمة الدخول غير المصرح به للشبكة المعلوماتية في المادة 12/ب التي نصت على أنه اذا كان الدخول المشار إليه في المادة 12/أ بقصد الغاء أو اتلاف أو تدمير أو تغيير أو نقل أو نسخ أو افشاء البيانات والمعلومات غير المتاحة للجمهور التي تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو

[lxxxi] عبد الاله النوايسة، مرجع سابق، ص 17.

الاقتصاد الوطني فتكون العقوبة الاشغال المؤقتة وبغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة الاف دينار[lxxxii].

وعند النظر لهذا النص نجد أن التشديد قد ارتبط بالهدف الذي يسعى المجرم له من دخوله إلى الموقع أو الشبكة المعلوماتية فتختلف العقوبة لمجرد الدخول والاطلاع عنها إذا كان قد ترافق معها الإفشاء أو الاتلاف للبيانات الموجودة فإذا ثبتت النية لدى الجاني للقيام بهذه الافعال تكون العقوبة مشددة.

وإذا كان الدخول في نص المادة 12/ ج يقصد به الدخول لموقع الكتروني بقصد الايذاء أو الاتلاف أو تدمير أو نقل أو افشاء المعلومات غير المتاحة للجمهور وتمس الأمن الوطني والعلاقات الخارجية فتكون العقوبة هي الأشغال المؤقتة وبغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة آلاف دينار، فالظروف المشددة في هذه المادة هي ذات الظروف المشددة في نص المادة 12/ب، وكان على المشرع أن يجمع الأفعال التي تتطلب التشديد في نص واحد.

ومن العقوبات المقررة لجرائم التجسس الالكتروني والتي ضاعفت العقوبة نص المادة 15 من قانون الجرائم الالكترونية التي نصت على مضاعفة العقوبة في حال التكرار، ومنها جرائم التجسس الالكتروني، بما أن جريمة التجسس الالكتروني تكون بصورتها البسيطة جنحة، وتكون جناية في صورتها المشددة وهي في كلا الحالتين لا تقع بطريقة الخطأ غير المقصود، ولقد ساوى قانون الجرائم الالكترونية بين الاشتراك الجرمي التبعي وساوى بينه وبين الفاعل الأصلي، وبهذا خرج عن قواعد الأحكام العامة، فنصت المادة 14 من قانون الجرائم الالكترونية على أنه " يعاقب كل من قام قصدًا بالاشتراك أو التدخل أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة فيه لمرتكبها"[lxxxiii].

[lxxxii] المادة 12 من قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015.

[lxxxiii] المادة 14 من قانون الجرائم الالكترونية رقم 27 لسنة 2015.

المراجع

-ابن منظور، أبي الفضل جمال الدين محمد بن مكرم، لسان العرب، بيروت، دار صادر، المجلد السادس.

-الفاضل محمد. 1978. الجرائم الواقعة على أمن الدولة، دراسة مقارنة، دار المطبوعات الجامعية، دمشق، ط4.

-أحمد بطو، مقال بعنوان: تعريف التجسس الالكتروني، منشور عبر موقع سايبر وان بتاريخ 30-07-2021، تاريخ آخر دخول: 29-10-2022.

-هروال، نبيلة هبة،2007 الجوانب الاجرائية لجرائم الانترنت، دار الفكر الجامعي، ط1، النوايسة، عبد الإله، والعدوان ممدوح. 2019. جرائم التجسس الالكتروني في التشريع الأردني، دراسة تحليلية، مجلة دراسات علوم الشريعة والقانون، مجلد 46، عدد1 ملحق 1.

-الطراونة، هاني جميل. 2011، الجرائم الواقعة على امن الدولة الخارجي في التشريع الأردني، عمان، دار وائل.

-محمد أمين الرومي 2003، "جرائم الكمبيوتر والأنترنيت". دار المطبوعات الجامعية.

الدغيدي مصطفى محمود، 1983، التحريات والاثبات الجنائي، القاهرة، دار الشروق للطباعة والنشر.

-د. محمد عبد الله طالب المحنا. 2007، التحريض على جرائم أمن الدولة من جهة الداخل في مصر وقطر، رسالة دكتوراه، أكاديمية شرطة، مصر.

-نائلة عادل محمد قورة. 2005، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت.

-قشقوش، هدى حامد .1992. جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة.

-الدغمي، محمد راكان، 1985. التجسس وأحكامه في الشريعة الاسلامية، ط2، القاهرة، دار السلام للطباعة.

-بشرى حسين الحمداني، 2014، القرصنة الالكترونية وأسلحة الحرب الحديثة، ط1، دار اسامة للنشر، الأردن.

-أورده، نصر صلاح، 2002، الحرب الخفية تاريخ المخابرات، ج1، ط1، القاهرة، دار الخيال.

-غنام محمد غنام، 2010. دور قانون العقوبات في مكافحة جرائم الكومبيوتر والانترنت، دار الفكر والقانون للنشر والتوزيع، المنصورة.
-حافظ مجدي محمود، 1990، الحماية الجنائية لأسرار الدولة، الاسكندرية، الهيئة المصرية العامة للكتاب.
-عبد المهيمن بكر، 1976، جرائم أمن الدولة الخارجي، دراسة في القانون الكويتي والمقارن، دار النهضة العربية، القاهرة.
-عثمان محمد، 2015، دور القانون الدولي لمواجهة التجسس الدبلوماسي، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، العراق.
-الصيفي، عبد الفتاح، 1997، الجرائم الواقعة على أمن الدولة، دار الهدى، مصر.
-عبد الوهاب الكيالي، 1990، موسوعة السياسة، ط2، بيروت، المؤسسة العربية للدراسات والنشر.
-سلامي، ناديا.2017. التجسس الالكتروني كأثر للاستخدام غير المشروع للفضاء الالكتروني على أمن الدولة الخارجي، مجلة دراسات، جامعة عمار ثليجي، الجزائر، العدد 56.
-منير محمد الجنبيهي. 2004، "جرائم الإنترنيت والحاسب الآلي ووسائل مكافحتها". دار الفكر الجامعية.
-الدربي، عبد العال واسماعيل محمد صادق، 2012، الجرائم الالكترونية، الطبعة الأولى، المركز القومي للإصدارات القومية، القاهرة.
-لحرش، عبد الرحمن. 2003. التجسس والحصانة الدبلوماسية، مجلة الحقوق، جامعة الكويت.
-البقور، فواز 1993، التجسس في التشريع الأردني، دراسة مقارنة، ط3، عمان.
-المومني نهلا عبد القادر، 2008، الجرائم المعلوماتية، ط1، دار الثقافة للنشر والتوزيع، الأردن.
بحث الجرائم الإلكترونية، بحث منشور على الإنترنت بتاريخ 2012/12/7.
.http://droit.moontada.com/t622-topic
-الزعبي جلال، والمناعسة أحمد، 2010، جرائم تقنية نظم المعلومات الالكترونية، ط1، عمان، دار الثقافة.
-الجبور، محمد عودة. 2012. الجرائم الواقعة على أمن الدولة وجرائم الارهاب، ط2، دار الثقافة.
-سلامي، نادية. 2017، التجسس الالكتروني كأثر للاستخدام غير المشروع للفضاء الالكتروني على امن الدولة الخارجي، مجلة دراسات جامعة عمار، الأغواط، العدد 56.

-رابحي، عزيزة. 2018، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، جامعة أبي بكر بلقايد السلمان، كلية الحقوق والعلوم السياسية، الجزائر.

-حسين علي جبار الركابي، 2018، الحماية الجنائية لأمن الدولة الخارجي، منشورات زين الحقوقية، بيروت، لبنان، الطبعة الأولى.

-محمد غنام، غنام، 2000، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، المنصورة، دار الفكر القانوني.

-بهنام، رمسيس، 1968، الجرائم المضرة بأمن الدولة، النظرية العامة للقانون الجنائي، المعارف، الاسكندرية.

-بشرى حسين الحمداني، 2014، القرصنة الالكترونية أو أسلحة الحرب الحديثة، ط1، دار اسامة للنشر والتوزيع، الأردن.

-د. إبراهيم اللبيدي، 2006، الحماية الجنائية لأمن الدولة، دراسة مقارنة، دار الكتب القانونية، القاهرة.

-محمد أمين الرومي، 2004، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الاسكندرية.

-عبد الاله النوايسة، 2019، مجلة علوم الشريعة والقانون، المجلد 46، عدد1، ملحق1.

-د. رستم، هشام محمد فريد، 1995، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة.

-كامل السعيد، 2002، شرح الاحكام العامة في قانون العقوبات، دار الثقافة، عمان.

-د. رؤوف محسن، 1966، السبب في القانون الجنائي، دراسة تحليلية مقارنة، ط2.

-مسفر بن حسن القحطاني، 2015، جرائم نشر الوثائق والمعلومات السرية وافشائها والعقوبات المترتبة عليها في النظام السعودي، مجلة البحوث القانونية والاقتصادية – كلية الحقوق جامعة المنصورة، مصر عدد 58.

- قانون العقوبات الأردني رقم (16) لسنة 1960 وتعديلاته.
- قانون الجرائم الالكترونية رقم (27) لسنة 2015.
- قانون حماية أسرار ووثائق الدولة رقم (50) لسنة 1971.