جرائم التجسس الإلكتروني في التشريع الأردني
دراسة تحليلية

*عبدالإله محمد النوايسة، ممدوح حسن العدوان**

ملخص

يتناول هذا البحث موضوع جرائم التجسس الإلكتروني في التشريع الأردني؛ نظرا لخطورة التجسس الإلكتروني المتمثل بدخول الجاني إلى الشبكة المعلوماتية، أو نظام المعلومات أو موقع الكتروني للحصول على محتوى الكتروني غير متاح للجمهور يمس الأمن الوطني أو العلاقات الخارجية للدولة أو السلامة العامة أو الاقتصاد الوطني. وجاء هذا البحث لتسليط الضوء على التشريعات الجزائية الأردنية التي وفرت الحماية للمحتوى الإلكتروني المتضمن معلومات سرية تخص الدولة، وتحديدا تلك النصوص التي جاءت في قانون حماية أسرار الدولة وقانون الجرائم الإلكترونية. لذلك تم تناول هذا البحث من خلال مبحث تمهيدي وثلاثة مباحث أخرى، حيث بيّنا في المبحث التمهيدي ماهية التجسس الإلكتروني، وعرض مفهوم التجسس بشكل عام، والمقصود بالتجسس الإلكتروني بشكل خاص، والصور السائدة للتجسس. ومن ثم وضحنا في المبحث الأول مدى قابلية ارتكاب جرائم التجسس بوسائل الكترونية وأحكامها. أما في المبحث الثاني فقد بينا التجسس في قانون الجرائم الإلكترونية الأردني، وتسليط الضوء على نص المادة 12 من هذا القانون. وأخيراً في المبحث الثالث بيّنا الجزاءات المقررة لجرائم التجسس الإلكتروني سواء في قانون حماية أسرار الدولة أو تلك المقررة في قانون الجرائم الإلكترونية.

الكلمات الدالة: التجسس، التجسس الإلكتروني، المحتوى الإلكتروني، الدخول غير المصرح به، المعلومات السرية.

المقدمة

إن تبادل البيانات والمعلومات بواسطة الإنترنت، وضعف رقابة الدول على هذه الوسيلة، جعل من ارتكاب الجرائم باستخدامها أو عبرها أمرا غاية بالسهولة؛ نظرا لاتساعها وسهولة إخفاء أدلة ارتكابها، وشعور المستخدم بعدم وجود رقابة حقيقية على ما يقوم به من أفعال، كم أن هناك قدرات لدى بعض المجرمين المعلوماتيين على إخفاء جرائمهم أو ما يترتب عليها من آثار، زاد من احتمالية ارتكاب الجرائم باستخدام تكنولوجيا المعلومات والإنترنت، حيث زادت جرائم الاختراق والاعتداء على البيانات والمعلومات، وجرائم تدمير ونقل البيانات والمعلومات المرفوعة على شبكة الإنترنت أو غيرها من الشبكات، من خلال المواقع الإلكترونية والأنظمة المعلوماتية.

فالشبكة المعلوماتية تحتوي على آلاف المواقع الإلكترونية، التي تحتوي على معلومات مهمة، كالمواقع العسكرية أو أنظمة التسليح، أو غيرها من المعلومات التي لا يجوز الاطلاع عليها إلا لمن يخوله القانون ذلك. وكما أن النظام المعلوماتي أو الموقع الإلكتروني الذي يحتوي على معلومات تمس الأمن القومي لا يجوز الدخول إليه بدون تصريح، فإنه لا يجوز التعدي على المحتوى أو سرقته أو نقله أو إتلافه.

إن من طبيعة أي دولة أن تمتلك الأسرار التي لا ينبغي لأي شخص أن يقوم بالاطلاع عليها دون إذن مسبق، وأيّ اطلاع عليها أو اعتداء، قد يؤدي لحدوث أزمات داخلية وخارجية. إذن فهذا النوع من المعلومات ينم عن خطورة كبيرة، لذلك فقد جاءت التشريعات على حماية البيانات والمعلومات، التي تؤثر على أمن الدولة الداخلي والخارجي، والمحفوظة في النظام المعلوماتي والشبكات والمواقع الإلكترونية.

إن قيام الجاني بالدخول أو الولوج إلى النظام المعلوماتي بقصد الاعتداء على بيانات أو معلومات غير متاحة للجمهور، تمس الأمن الوطني، أو العلاقات الخارجية للدولة، أو السلامة العامة، أو الاقتصاد الوطني، من خلال حذفها أو إتلافها أو تدميرها، أو

* كلية القانون، جامعة الشارقة، الامارات؛ وكلية الشيخ نوح القضاة للشريعة والقانون، جامعة العلوم الإسلامية العالمية، الأردن. تاريخ استلام البحث 2017/8/26، وتاريخ قبوله 2018/6/3.

تعديلها أو تغيرها أو نقلها أو مسحها أو إفشائها يعد جريمة تنال من أسرار الدولة، واعتداء على حقها في سرية هذه المعلومات وعدم كشفها.

لقد ارتبطت الأردن شأنها شأن باقي الدول العربية في الآونة الأخيرة بشبكة الإنترنت. وشهدت بدايات هذا القرن في الأردن الانتشار الواسع لاستخدام شبكة الإنترنت بعد ازدياد استعمال الحاسب الآلي بصفة عامة، ولقد توسع استخدام الحاسب الآلي لدى الأفراد والوحدات الحكومية على السواء وكذلك في الوحدات الإدارية والعلمية والبحثية وازدادت في ذات الوقت الأخطار التي يمكن أن تتعرض لها شبكات البيانات الحكومية في معظم الدول العربية ومن بينها الأردن، ولا يكمن الخطر في مجرد ارتباط هذه الدول أو المؤسسات الحكومية بشبكة الإنترنت أو الشبكات العالمية الأخرى فقط، ولكن في الضعف الأمني لمعظم الشبكات الحكومية في الوطن العربي، واعتماد الشبكات العربية بصورة أساسية على الشبكة العالمية، وغياب التواصل العربي في مجال الاتصال الإلكتروني ولا شك أن معظم خبراء الشبكات يعرفون أدق التفاصيل عن الشبكة العالمية وهي بذلك سهلة الاختراق نسبيا إذا لم تتوفر بعض الحلول الأمنية لهذه الشبكات.

ونظرا لخطورة التجسس الإلكتروني 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. الذي يرتكب أيضاً بصورة جريمة من الجرائم الواردة في قانون حماية أسرار ووثائق الدولة. فالفارق بين جرائم التجسس الواردة في قانون الجرائم الإلكترونية والجرائم الواردة في قانون حماية أسرار ووثائق الدولة يكمن في أن جرائم التجسس في قانون الجرائم الإلكترونية لا تقع إلا على محتوى الكتروني وبوسيلة إلكترونية، وهنالك فارق آخر يتمثل في أن جرائم التجسس في قانون حماية أسرار ووثائق الدولة يكون بصورة سر أو وثيقه مصنفه على أنها من أسرار الدولة وفقا للإجراءات المنصوص عليها في قانون حماية أسرار ووثائق الدولة.

وعليه فإننا نسعى من خلال هذا البحث وبدراسة تحليلية لنصوص قانون الجرائم الإلكترونية وقانون حماية أسرار الدولة لبيان مدى قيام جريمة التجسس الإلكتروني. وهل أن المشرِّع الأردني وفرّ الحماية اللازمة للأسرار والمعلومات التي تهم الأمن القومي؟ ومدى كفاية أحكام قانون الجرائم الإلكترونية في مكافحة جرائم الدخول غير المشروع لنظام معلوماتي والعبث بمحتوياته السرية.

ولبيان ما سبق ذكره فإننا سنقوم بتقسيم هذا البحث لمبحث تمهيدي وثلاثة مباحث كالآتي:

المبحث التمهيدي: ماهية التجسس الإلكتروني

المبحث الأول: مدى قابلية ارتكاب جرائم التجسس بوسائل إلكترونية

المبحث الثاني: التجسس في قانون الجرائم الإلكترونية

المبحث الثالث: الجزاءات المقررة لجرائم التجسس الإلكتروني.

المبحث التمهيدي

ماهية التجسس الإلكتروني

يعدّ التجسس الإلكتروني الهاجس الأخطر للدولة لا سيما بعد الانتشار السريع والواسع للشبكة العنكبوتية التي أخذت مكانها المتقدم في استخدامات الدول والأفراد على حد سواء. ولبيان ماهية التجسس الإلكتروني سنعرض مفهوم التجسس الإلكتروني في المطلب الأول، ثم نعرض للصور السائدة للتجسس في المطلب الثاني.

المطلب الأول: مفهوم التجسس الإلكتروني

يقتضي بيان مفهوم التجسس الإلكتروني، معرفة المفهوم العام للتجسس، ثم توضيح المقصود بالتجسس الإلكتروني.

الفرع الأول: المفهوم العام للتجسس

التجسس لغةً من الجس وهو اللمس باليد ويقال يجسه جساً واجتسه أي مسه ولمسه (ابن منظور، 1985)[1]، أما الجاسوس، فهو العين يتجسس الأخبار، وجمعها جواسيس ومنه الجساس، وهو وصف للمبالغة (ابن منظور، 1985)[2]

وقد حاول الفقه وضع تعريف للتجسس إلا أن هذه التعريفات متباينة وتعتمد على طبيعة السلوك المجرم في التشريع محل الدراسة؛ لأن السياسة التشريعية تختلف من دولة لأخرى كما أن جرائم التجسس تختلف من تشريع لآخر؛ لذا تأتي هذه التعريفات مختلفة (المراغي، 1998).[3]

فالتجسس نمط من أنماط السلوك الإنساني رافق نشوء المجتمعات منذ القدم وتطور بتطورها حتى غدا له في عصرنا الحاضر شأن كبير وأهمية بالغة. وهو قديم قدم البشرية فقد عرفه الفراعنة، وكذلك الصينيون فيقول حكيمهم "سان سو": "إن ما يُمَّكن الملك الحكيم والقائد الصالح من إنزال الضربة والانتصار وبلوغ ما يتجاوز حدود الرجل العادي هو المعلومات السابقة" (الدغمي، 1984).[4]

ولم تزدهر الجاسوسية وتنظم الا مع بداية الحرب العالمية الثانية، فلم يعد التجسس قاصراً على الأسرار بل تعداه إلى المعلومات الصناعية والعلمية، وأسهم بذلك التقدم العلمي وبلوغ أجهزة التجسس درجة عالية من الكفاءة (القدس العربي، 3537) .[5]

وفي نهاية القرن العشرين تغيّرت أدوات وأساليب التجسس وذلك نتيجة للثورة التكنولوجية والمعلوماتية في مجال الاتصالات فأصبح العالم قرية صغيرة، وأصبحت كل المعلومات السياسية والاقتصادية وأحياناً العسكرية معلومة للكافة، وبعد أن أصبحت الولايات المتحدة الأمريكية القوة العظمى الوحيدة في العالم فإنها تعمل جاهدة على التجسس على كل دول العالم للحفاظ على تفردها بقيادة العالم، ولأنها أكثر تقدماً فإن لها قدرات خارقة على التجسس من خلال أقمار التجسس ومحطات التنصت الضخمة وحاملات الطائرات المرتبطة بالأقمار الصناعية وهذا كله يجعل من الجالس في واشنطن يسمع ويرى كل ما يدب على وجه الأرض، وتعدّ السفارات مراكز تجسس مشروعة فكل الدول تعتمد على سفاراتها في الحصول على معلومات عن البلد الذي توجد فيه السفارة وفي كافة المجالات، وترصد ميزانيات بأرقام خيالية للقيام بذلك من الدول الكبرى وأكثر الدول التي تتجسس دبلوماسياً الاتحاد السوفياتي سابقاً والولايات المتحدة الأمريكية (الرأي، 11154).[6]

الفرع الثاني: المقصود بالتجسس الإلكتروني

التجسس الإلكتروني وفقاً لقانون الجرائم الإلكترونية يعني: 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. ويشمل أيضاً ارتكاب جريمة من الجرائم الواردة في قانون حماية أسرار ووثائق الدولة بوسيلة إلكترونية، فالفارق بين جرائم التجسس الواردة في قانون الجرائم الإلكترونية والجرائم الواردة في قانون حماية أسرار ووثائق الدولة يكمن في أن جرائم التجسس في قانون الجرائم الإلكترونية لا تقع إلا على محتوى الكتروني وبوسيلة إلكترونية، وهنالك فارق آخر يتمثل في أن جرائم التجسس في قانون حماية أسرار ووثائق الدولة يكون بصورة سر أو وثيقه مصنفه على أنها من أسرار الدولة وفقا للإجراءات المنصوص عليها في قانون حماية أسرار ووثائق الدولة.

عرَّفت المادة الثانية من قانون حماية أسرار ووثائق الدولة السر بأنه: "أية معلومات شفوية، أو وثيقة مكتوبة، أو مطبوعة، أو مختزلة، أو مطبوعة على ورق مشمع، أو ناسخ، أو أشرطة تسجيل، أو الصور الشمسية والأفلام، أو المخططات، أو الرسوم، أو الخرائط، أو ما يشابهها والمصنفة وفق أحكام هذا القانون".

على الرغم من أن هذا التعريف لا يواكب التطور التكنولوجي في الوقت الحاضر، لأنه وضع عام (1971)، وفي تلك الفترة لم يكن هناك انتشار واسع للنظم المعلوماتية والشبكات والمواقع الإلكترونية التي زاد الاعتماد عليها في وقتنا الحاضر، وقد وضع قانون الجرائم الإلكترونية في العام (2015)، وهذا يدل على حداثة هذه النظم المعلوماتية، ولكننا نعتقد أن هذا التعريف الوارد في قانون حماية أسرار الدولة، ينطبق على البيانات والمعلومات غير المتاحة للجمهور، والمخزنة داخل النظام المعلوماتي، أو المقطع الإلكتروني العائد للدولة أو المؤسسة الحكومية.

ومن خلال التعريف السابق للسر والتعداد الوارد في المادة نجد أن السر المتعلق بأمن الدولة يمكن أن يكون بأشكال مختلفة ويمكن أن يكون بشكل محتوى إلكتروني، فالمهم ليس الصورة التي يكون عليها السر وإنما التصنيف الذي يعطى لهذه المادة والإجراءات المتبعة بذلك وفق أحكام قانون حماية أسرار ووثائق الدولة.

فقد أولى المشرِّع الأردني أسرار الدولة اهتمام خاص وأفرد لها قانوناً خاصاً أطلق عليه اسم "قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971"، وعرَّف أسرار الدولة في المادة الثانية، وبيّن درجات السرية، فقسمها إلى سري للغاية (المادة 3)، وسري (المادة 6)، ومحدود (المادة 8)، ووثائق عادية (المادة 10)*.[7]

ويلاحظ من خلال تصنيف المشرِّع لأسرار الدولة أنه شمل كل الأشياء والوثائق والمعلومات المتعلقة بسلامة الدولة، وغلّب صفة الأسرار على المعلومات ذات الطابع العسكري، كما أنه لم يضع معياراً واضحاً في التمييز بين درجات السرية الثلاثة (سري للغاية، سري، محدود)وقد بالغ كذلك في الطرق التي يتم بواسطتها حفظ أسرار الدولة، ومع ذلك فإنها تظل طرق تقليدية يجب إعادة النظر فيها وتعديل القانون كي يتلأم مع التكنولوجيا الحديثة*[8]، ومن حيث التجريم لم يفرق في العقوبة اعتماداً على درجة السرية للمعلومة أو الوثيقة التي تم إفشاؤها.

أما بخصوص محل التجسس الإلكتروني وفقاً من خلال المادة 12 من قانون الجرائم فإنه يكون بصورة بيانات أو معلومات تكون على شكل محتوى الكتروني تمس الأمن الوطني، أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني.

ومصطلح الأمن الوطني يشير إلى كل شيء يتعلق بسلامة الدولة ضد الأخطار الخارجية والداخلية التي قد تؤدي بها إلى الوقوع تحت سيطرة أجنبية نتيجة ضغط خارجي أو انهيار داخلي (الكيالي، 1990)[9]. وقيل إنّ الأمن الوطني: المجموع الكلي للمصالح الحيوية للدولة كحماية الاقليم والاستقلال. ونرى أن المعلومات والبيانات عندما تتعلق بالأمن الوطني يجب تصنيفها وفقا لقانون حماية وأسرار الدولة لخطورتها من جانب ولتوفير حماية جزائية أكبر لها من جانب آخر (بدوي، 1963)[10].

والعلاقات الخارجية للملكة فتشمل كل ما يتعلق بالسياسة الخارجية للملكة وعلاقة المملكة بالدول الأخرى في شتى المجالات السياسية والاقتصادية والعسكرية وعلاقتها مع المنظمات الدولية. والسلامة العامة هي السيطرة على ما يشكل خطرا عاما أيا كان مصدره ومثالها المعلومات والبيانات التي تتعلق بالمخاطر المحتملة من مفاعل نووي إذا حدث تسريب أو انفجار، والمخاطر الناتجة عن دفن نفايات خطره، أو أثر حصول اعتصامات ومظاهرات على تعريض سلامة المواطنين للخطر.

أما الاقتصاد الوطني فيشمل السياسة الاقتصادية الداخلية والخارجية، وكل ما يتعلق بالوضع الاقتصادي والمالي للملكة غير المعلن للجمهور.

ومع أن جرائم التجسس غادرت الإقليم الخاص بالجرائم الواقعة على أمن الدولة الخارجي إلا أنها تبقى من الجرائم التي تمس أمن الدولة، مما حدا بالمشرِّع الأردني جعل الاختصاص بنظر هذه الجرائم لمحكمة أمن الدولة (المادة الثالثة) .[11]

المطلب الثاني: صور التجسس (الفاضل، 1978).[12]

أصبح التجسس في العصر الحالي شاملاً لمختلف المجالات فلم يعد يقتصر على النواحي العسكرية والحربية وإن كان هذا النوع من التجسس يمثل أهم أنواع التجسس وأخطرها، إلا أن المعلومة المطلوبة الآن تختلف عنها في الماضي، فلم تعد أعداد الجيوش وتجهيزاتها التقليدية من الأمور السرية، بل أننا نجد أنمثل هذه الأمور تتداولها صفحات الصحف والبرامج التلفزيونية عندما يحدث أزمة في منطقة معينة ويتم رسم خرائط تمثل حجم القوات في الدول المجاورة لمناطق الصراع. ولكن هناك تجسس عسكري يكون بصورة عميقة خاصة بين الدول الكبرى فتسعى هذه الدول للحصول على أسرار حربية تكنولوجية؛ كي تقف على مدى التقدم الذي وصلت إليه غيرها من الدول، فهناك سباق في التسلح المتقدم النووي والكيماوي والاشعاعي، أما الدول التي تستورد هذه التكنولوجيا فإنها تحصل على اجيال قديمة من الأسلحة، علاوة على أن مُصدر هذه التكنولوجيا القديمة يجردها من ضمان فاعليتها فتصبح عبارة عن نفايات تسعى الدول المتقدمة إلى بيعها وبأقساط ميسرة أو تقديمها كمساعدات لدول العالم الثالث الفقيرة.

وقد يكون التجسس سياسياً لمعرفة المواقف السياسية لصناع القرار في الدولة والمعلومات التي تتعلق بالسياسية الداخلية والخارجية المتبعة، أو التي تنوي الدولة السير عليها. وقد يكون التجسس معنوياً ونفسياً لشعوب الدول وقادتها ومعرفة مواطن القوة والضعف في شخصية أفراد الشعب، وعوامل الوحدة والتفرقة، والقيم السائدة في المجتمع، التيارات الحزبية والدينية ومدى تأثيرها في الأزمات، ومقدار العزيمة لدى شعب دولة ما، فالحرب المعنوية من أهم الحروب فمن خلال هذه المعلومات تستطيع الدولة المعادية استخدام السلاح المعنوي وتحطيم الروح المعنوية للشعب مما يسهل عليها كسب المعركة.

وهناك تجسس اقتصادي لمعرفة موارد الدولة وحجم انتاجها، وميزانها التجاري والاحتياطي لديها، والمدة التي تستطيع خلالها الاعتماد على ذاتها إذا تم حصارها، وكذلك معرفة المرافق الاقتصادية الحيوية لديها ومواقعها وكذلك ديونها الخارجية.

كما أن التجسس قد ينصب على المعلومات الصناعية والعلمية من خلال معرفة أسرار الصناعات، والأبحاث العلمية، خاصة إذا كانت هذه الصناعات ترفد الدفاع الوطني فهناك شركات تسهم في الإنتاج الحربي وتطوير الأسلحة، وقد يكون التجسس العلمي لمعرفة الدراسات العلمية في المجالات الزراعية، أو الهندسية، أو الصحية (المراغي، 1988).[13]

جميع المعلومات السرية السابقة سواء كانت عسكرية أو سياسية أو اقتصادية من الممكن أن تكون على شكل محتوى إلكتروني، حتى لو كان هذا المحتوى محاطب وسائل الأمن المعلوماتي، فإن المخزن الالكتروني الموجود فيه هذه الأسرار عرضة للاختراق والحصول على هذه الأسرار وإفشائها.

المبحث الأول

مدى قابلية ارتكاب جرائم التجسس بوسائل إلكترونية

وردت جرائم التجسس في المواد 114 إلى 116 من قانون حماية أسرار ووثائق الدولة وهي جريمة الدخول أو محاولة الدخول إلى أماكن محظورة بقصد الحصول على أسرار تتعلق بسلامة الدولة، وجريمة سرقة الأسرار التي تتعلق بسلامة الدولة أو الحصول عليها وجريمة إبلاغ الأسرار المتعلقة بأمن الدولة أو إفشاؤها دون سبب مشروع. وسوف نبين أحكام هذه الجرائم ومدى قابلية ارتكابها بوسائل إلكترونية.

المطلب الأول: جريمة الدخول أو محاولة الدخول إلى أماكن محظورة

تناولت هذه الجريمة المادة 114 من قانون حماية أسرار ووثائق الدولة حيث نصت على أنه: "من دخل أو حاول الدخول إلى مكان محظور قصد الحصول على أسرار، أو أشياء، أو وثائق محمية، أو معلومات يجب أن تبقى سرية حرصاً على سلامة الدولة عوقب بالأشغال الشاقة المؤبدة، وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الإعدام".

يكون النشاط الجرمي في الجريمة المنصوص عليها في المادة 14 من قانون حماية أسرار ووثائق الدولة بصورة دخول الفاعل أو محاولته الدخول إلى مكان محظور دخوله. ويفترض الدخول تخطي المكان واجتيازه، ولم يحدد المشرِّع وسائل معينة للدخول– وحسناً فعل– فيستوي أن يكون الدخول بوسائل مألوفة أو بوسائل غير مألوفة كالكسر أو الخلع أو التسلق أو بوسائل الخداع والتحايل.

ولا يشترط لقيام هذه الجريمة أن يستطيع الجاني الحصول على السر، أي أنه لا يشترط تحقيق نتيجة معينة، فهده الجريمة من جرائم الخطر المبكر التي ساوى المشرِّع فيها بين الفعل والشروع به، على أنه إذا استطاع الجاني الحصول على الأسرار فإننا ننتقل إلى نص المادة 15 من قانون حماية أسرار ووثائق الدولة.

وهذه الأماكن هي في الأغلب منشآت عسكرية ومرافق الدفاع وما يستخدم في أغراضه، كما أنها تخضع لحراسة شديدة وغالباً ما يوضع من الإشارات التي تفيد أن هذه الأماكن محظورة وممنوع اجتيازها أو الاقتراب منها، أو حتى التصوير ضمن منطقتها، وتبقى هذه الأماكن محظورة إلى أن يصدر أمر من السلطات المختصة بإلغاء الحظر عنها.

من خلال الفعل المكون للركن المادي المتمثل في الدخول أو محاولة الدخول للأماكن المحظورة، يتضح لنا أن الدخول يجب أن يكون للأماكن بمفهومها المادي، ولا يسري نص المادة 114 على فعل من يدخل لمكان افتراضي كالمواقع وأنظمة المعلومات الإلكترونية للحصول على سر من أسرار الدولة.

المطلب الثاني: جريمة سرقة الأسرار التي تتعلق بسلامة الدولة أو الحصول عليها

نصت على هذه الجريمة المادة 15 من قانون حماية أسرار ووثائق الدولة التي جاء فيها أنه: "أ–من سرق أسرار أو أشياء أو وثائق أو معلومات كالتي ذكرت في المادة السابقة أو استحصل عليها عوقب بالأشغال الشاقة المؤقتة لمدة لا تقل عن عشر سنوات.

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

حصر المشرِّع النشاط الجرمي الذي تقوم به هذه الجريمة بالسرقة والاستحصال ولكل من مصطلح السرقة وكذلك الاستحصال معنى مختلف، فالسرقة وفق تعريف المشرِّع لها في المادة 399 من قانون العقوبات تعني: اخذ مال الغير المنقول دون رضاه، وهذا يعني أن السرقة تفترض نشاط من الجاني ينطوي على تحريك الشيء محل السرقة والاعتداء على الحيازة وحرمان الحائز من الحيازة، لا يقع إلا على الأشياء المنقولة والأشياء المادية، ويلزم لوجود جريمة السرقة قصد جرمي خاص يتمثل في ظهور السارق على المال المسروق بمظهر المالك، أي لا بد أن يكون قاصداً تملك الشيء محل السرقة، فالأشياء التي تعدّ من أسرار الدولة يمكن سرقتها والوثائق كذلك وأي سر ومعلومة مجسدة بكيان مادي يمكن سرقتها وبالتالي فإنه إذا تم أخذ المعلومة أو الاطلاع عليها دون اخذ ما يجسدها من مادة فإننا لا نكون بصدد سرقة ولا يشترط أن يرافق السرقة أي ظرف من الظروف المشددة لجرائم السرقة.

وقد ساوى المشرِّع بين السرقة والاستحصال، والحقيقة أن مصطلح الاستحصال يغني عن مصطلح السرقة فهو عاما وأوسع من مفهوم السرقة، ويستوعب كافة الوسائل التي قد يلجأ لها الفاعل للحصول على السر بما فيها السرقة.

ولا بد أن يكون الفاعل قد سعى للحصول على السر فإذا وصل السر إليه دون سعي متعمد منه فإنه لا عقاب عليه، وقد أعرب المشرِّع عن ذلك بوضوح عندما استعمل كلمة "سرق"، وكذلك كلمة "استحصل" ومن المعروف في علوم اللغة أن نقل المجرد الثلاثي إلى وزن استفعل إنما هو للدلالة على الطلب (الفاضل، 1978) .[14]

وعن مدى قابلية ارتكاب هذه الجريمة بوسائل إلكترونية، نرى أن سرقة الأسرار لا ترتكب بوسائل الكترونية لأن من مقتضيات جريمة السرقة أن تقع على شيء له طبيعة مادية فلا تقع جريمة سرقة إذا قام الجاني بالحصول على محتوى إلكتروني مصنف على أنه سر من أسرار الدولة إذا تم الحصول على السر مجردا من الدعامة المادية الحاوية لهذا السر، كالذاكرة الإلكترونية أو القرص الذي يكون عليه معلومات إلكترونية مصنفه على أنها سر من أسرار الدولة، ولكن المشرِّع جرم فعل الاستحصال على سر من أسرار الدولة وطبيعة فعل الاستحصال يمكن أن يرتكب بأي وسيلة بما فيها الوسائل الإلكترونية، فإذا تم الحصول على سر من أسرار الدولة بوسيلة إلكترونية، فإن الفعل يشكل جريمة وفقا لنص المادة 115 من قانون حماية أسرار ووثائق الدولة.

ولا يشترط لإعمال الظروف المشددة لهذه الجريمة إن يوصل الفاعل السر للدولة الأجنبية أو الدولة العدوة، فيكفي أن يحصل عليه ويثبت بعد ذلك أنه إنما أراد الحصول على السر لمنفعة دولة أجنبية أو دولة عدوة*([15]).

المطلب الثالث: جريمة إبلاغ الأسرار المتعلقة بأمن الدولة أو إفشاؤها

نصت على هذه الجريمة المادة 16 من قانون حماية أسرار ووثائق الدولة بقولها: "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 وظيفة أو مسؤولية لأي سبب من الأسباب فأبلغها أو أفشاها دون سبب مشروع عوقب بالأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات.

ب- ويعاقب بالأشغال الشاقة المؤبدة إذا أبلغ ذلك لمنفعة دولة أجنبية، وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الإعدام".

وحتى تقع هذه الجريمة يجب توفر العناصر التالية:

أولاً: أن يكون فاعل الجريمة حائزاً على سر من الأسرار التي تتعلق بأمن الدولة.

ثانياً: الركن المادي للجريمة ويتمثل في فعل الإبلاغ أو الإفشاء.

ثالثاً: أن يكون الإبلاغ أو الإفشاء لسر من الأسرار التي تتعلق بأمن الدولة.

رابعاً: أن يكون فعل الإفشاء أو الإبلاغ دون سبب مشروع

إن النشاط المجرم في نص المادة 16 من قانون حماية أسرار ووثائق الدولة هو القيام بالإبلاغ أو الإفشاء، وبما أن المشرِّع استخدم كلا الاصطلاحين فهذا يعني أن لكل منهما مدلوله المختلف عن الآخر وإن أدى إلى نفس النتيجة التي يؤدي إليها الآخر. فما المقصود إذن بالإفشاء وما المقصود بالإبلاغ وما هو الفرق بينهما؟.

يقصد بالإفشاء الإفضاء بالسر إلى الغير أو تمكينه من الاطلاع عليه ولو لم يرافق ذلك بإعطاء وعائه المادي كالوثيقة أو الشيء الدال عليه (بكر، 1976)([16])، والإبلاغ في معناه لا يبتعد كثيراً عن الإفشاء فهو يعني إيصال السر إلى الغير. ورغم أنهما أي الإفشاء والإبلاغ قد يستخدما كمترادفين إلا أن هناك بعض الفروق بينهما، فإفشاء السر لا يتصور أن يقع ممن يجهل مضمون السر، أما إبلاغ السر فقد يقع ممن يعلمه وممن لا يعلمه، ويكفي أن يكون الفاعل في الإبلاغ عالماً بأن ما يقوم بإبلاغه من الأسرار المتصلة بأمن الدولة حتى ولو لم يكن يعرف محتواه، وكذلك فإن إفشاء السر لا يستهدف شخصاً أو جهة معينة أما الإبلاغ فإن الفاعل يستهدف منه إيصال السر إلى جهة معينة أو شخصاً معيناً (الفاضل، 1978).([17])

ولم يحدد المشرِّع الوسائل التي يتم من خلالها الإفشاء أو التبليغ فكل الوسائل سواء فقد يقوم الفاعل بذلك شفاهه، أو كتابةً، أو رسماً، أو تصويراً، أو بالنشر في الصحف والمجلات أو بالوسائل الإلكترونية الإنترنت أو الرسائل الإلكترونية E-Mail، أو بواسطة الرسائل عبر التلفون المحمول SMS، فلا عبره بالوسيلة أو مدى الانتشار الذي تحققه هذه الوسيلة. وبالتالي يتصور أن ترتكب هذه الجريمة بوسائل إلكترونية.

المبحث الثاني
التجسس في قانون الجرائم الإلكترونية.

تناول قانون الجرائم الإلكترونية في المادة 12 منه جرائم التجسس الإلكتروني ومع أن هذه المادة تتكون من أربع فقرات إلا أنها جميعها تتمحور حول جريمة واحدة وهي المساس ببيانات أو معلومات (محتوى إلكتروني) غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني.

تنص المادة 12/أ من قانون الجرائم الإلكترونية على أن: " يعاقب كل من دخل قصدا دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو نظام معلومات للاطلاع على بيانات أو معلومات غير متاحه للجمهور تمس الأمن الوطني أو

العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة آلاف دينار ".

وجاء في المادة 12/ج أنه:" يعاقب كل من دخل قصدا الى موقع الكتروني للاطلاع على بيانات أو معلومات غير متاحة للجمهور غير متاحه للجمهور تمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار ".

من خلال هاتين الفقرتين نجد أنهما يختلفان فقط في أن الدخول في الفقرة (أ) يكون إلى الشبكة المعلوماتية أو نظام معلومات، بينما الدخول في الفقرة (ج) يكون لموقع الكتروني، وكذلك عقوبة الغرامة في الفقرة (أ) حدها الأدنى خمسمائة دينار والأعلى خمسة آلاف دينار، بينما الغرامة في الفقرة (ج) محددة بخمسمائة دينار

تفترض جريمة التجسس الإلكتروني الواردة في المادة 12 / أ وج من قانون الجرائم الإلكترونية أن تقع جريمة دخول غير مصرح به أو بما يخالف أو يجاوز التصريح، وأن يكون الدخول الى الشبكة المعلوماتية أو نظام معلومات أو إلى موقع الكتروني، وأن يتم الدخول إلى محتوى إلكتروني يمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني غير متاح للجمهور الاطلاع عليه، وكذلك القصد الجرمي

وعليه سنبين عناصر هذه الجريمة في المطالب الآتية:

المطلب الأول: أن تقع جريمة دخول غير مصرح به أو بما يخالف أو يجاوز التصريح

أن مصطلح الدخول لازال يكتنفه الغموض من حيث ماذا يقصد به؟. ومتى يتحقق؟. رغم أن مصطلح الدخول بحد ذاته ليس جديداً على القانون الجنائي، فقد جرمت التشريعات العقابية التقليدية الدخول غير المشروع للمساكن والأماكن الخاصة والممتلكات، وجرمت هذه التشريعات الدخول للمساكن وبعض الأماكن من أجل السرقة (Burglary)، هذا النوع من الدخول لا يثير مشاكل لأنه ولوج إلى أماكن في العالم الواقعي، بعكس الولوج إلى العالم الافتراضي الذي لا يوجد فهم مشترك لمعناه؛ والسبب في ذلك أن الدخول الافتراضي مصطلح فني تقني

الفرع الأول: التعريف التشريعي للدخول

لم يرد في قانون الجرائم الإلكترونية تعريف للدخول، إلا أن بعض التشريعات عرفت الدخول، ومن هذه التشريعات قانون إساءة استخدام الكمبيوتر الإنجليزي لسنة 1990، ووفقاً لنص المادة 2/17 من هذا القانون فإن الدخول إلى أي بيانات أو برنامج موجود في جهاز كمبيوتر وذلك بجعله ينفذ أي وظيفة، ويمحو Erase))، أو يغير في البيانات أو البرامج، بنسخ أو بنقل البيانات أو البرامج من مكان حفظها إلى أي وسيلة تخزين، أو استخدام البيانات والبرامج، أو جعلها كمخرجات من الكمبيوتر المحفوظة فيه سواء بجعلها معروضة أو بأي أسلوب آخر.

وفي ولاية أركانسس الأمريكية عرفت المادة 5-41-102 من قانون الجرائم المتعلقة بالكمبيوتر رقم 908 لسنة 1987الدخول: بأنه " إعطاء تعليمات، الاتصال، تخزين البيانات، استعادتها من الكمبيوتر، أو من نظام الكمبيوتر، أو شبكة الكمبيوتر".

ومن التشريعات العربية التي عرفت الدخول غير المشروع نظام مكافحة جرائم المعلوماتية السعودي الذي عرف الدخول غير المشروع في المادة 7/2 بأنه: "دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها"، وعرفت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات الكويتي لسنة 2015 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".

يتضح لنا من العرض السابق لتعريف الدخول في بعض التشريعات اختلاف المفهوم التشريعي للدخول وهذا بدوره ينعكس على التجريم ويحدد نطاقه؛ لأن الدخول العنصر الأساسي في جريمة الدخول غير المصرح به، وفي حقيقة الأمر أن التشريعات التي لم تعرف الدخول تزيد بكثير عن تلك التي عرفته، وهو المنهج التشريعي الأسلم برأينا؛ لأن تجريم الدخول غير المصرح به للنظام المعلوماتي يرتبط بأمور تقنية متغيرة، ومتطورة فتعريف الدخول قد يحد من التجريم لعجز التعريف عن مجاراة واستيعاب المستجدات التكنولوجية.

الفرع الثاني: التعريف الفقهي للدخول

وعلى الصعيد الفقهي تم بذل محاولات عديدة لتعريف الدخول والتقريب بين فكرة الدخول الافتراضي والدخول الواقعي لإزالة الغموض الذي يكتنف هذا المصطلح، فيرى الفقيه (Orin Kerry)من جامعة جورج واشنطن أنه ينبغي لتحديد مفهوم الدخول للكمبيوتر التشبيه بين دخول الممتلكات الحقيقية ودخول الكمبيوتر، فعلى سبيل المثال لو أن أحد المستخدمين لجهاز كمبيوتر موصول بشبكة الإنترنت محمي بكلمة مرور حاول الدخول فتم الطلب منه إدخال اسم مستخدم وكلمة مرور صالحين لإتمام عملية الدخول، في هذه الحالة يمكن القول إن شاشة الكمبيوتر التي طلبت اسم مستخدم وكلمة مرور تشبه القفل الموجود على واجهة الباب، وإدخال اسم مستخدم وكلمة المرور يشبه استخدام المفتاح لفتح الباب، ويكون بالتالي المستخدم الذي يدخل اسم مستخدم وكلمة مرور صحيحين قد دخل للنظام. واقترحOrin تعريفاً موسعاً لمفهوم الدخول حيث عرفه على أنه:" أي تفاعل ناجح مع الكمبيوتر"(Any successful interaction with the computer)، ويبرر هذا التعريف الموسع كونه يساير التغيير والتطور السريع في تكنولوجيا الإنترنت(Kerr, 2003)[18].وتم تعريف الدخول بأنه:" كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي والإحاطة أو السيطرة على المعطيات التي يتكون منها، أو الخدمات التي يقدمها" (بن يونس، 2004)[19] وقيل إن الدخول هو الولوج إلى نظام معالجة آلية للبيانات باستخدام الحاسوب

وقد امتد عدم التوافق على مفهوم محدد للمقصود بالدخول للأنظمة المعلوماتية إلى الأحكام القضائية، ففي الولايات المتحدة الأمريكية رغم قلة الأحكام التي تعرضت لتعريف الدخول، إلا أنها جاءت غير متناسقة (Inconsistent)[20](Bainbridge, 2003)، وفي إنجلترا كانت المحاكم سخية في تفسيرها لما يعد حاسباً آلياً من الأجهزة في ظل غياب تشريعي له، حيث أدخلت في مفهوم الحاسب الآلي أدوات تدخل في صلب عمله لكنها لا تعد حاسباً آلياً، فالقضاء الإنجليزي وسع من مفهوم الدخول رغم القيود التشريعية الواردة على تعريف الدخول (الرواشدة، الهياجنة، 2009) .[21]

وبعد تناولنا للمفهوم التشريعي والفقهي والقضائي للدخول، نستطيع وضع فاصلاً لما يُعد من الأفعال دخولاً مجرداً وما يخرج من نطاقه بالاعتماد على فكرة انتهاك حرمة الأماكن في العالم الواقعي وتطبيقها على انتهاك الحرمة للمحل المحمي في جريمة الدخول غير المصرح به في العالم الافتراضي، فدخول النظام المعلوماتي هو دخول افتراضي غير واقعي ولكنه يمثل انتهاكاً لحرمة المحل الذي تم تخطيه افتراضياً، فالدخول يتحقق بالنشاط الإيجابي الذي يمكن الفاعل من التواجد داخل النظام أو أي من أجزائه، طالت مدته أم قصرت، تحققت له السيطرة على النظام أم لا.

فمجرد الاطلاع على البيانات أو المعلومات الظاهرة على شاشة نظام معلوماتي أو تلك التي ظهرت بصورة مخرجات أياً كان شكلها دون تدخل من الشخص لا تعد دخولاً غير مصرح به، فمن يكون جالساً في شرفة منزله وربما بداخل منزل آخر لم تسدل ستائره لا يعد مرتكباً لجريمة انتهاك حرمة منزل أو الاعتداء على الخصوصية؛ لأنه ببساطة لم يصدر منه فعل يعد تخطياً لحدود المنزل، ولم يصدر منه فعل يعد انتهكاً لحق الخصوصية ذلك أن حائز المسكن بتركه مكشوفاً خلع عن منزله الخصوصية.

ولا يشترط أن يتم الدخول بوسيلة بعينها فكل الوسائل سواء، وقد عبَر المشرِّع الأردني عن ذلك في المادة 1/3 من قانون الجرائم الإلكترونية التي نصت على أن: " كل من دخل قصداً إلى موقعٍ إلكترونيٍ أو نظام معلومات بأي وسيلة دون تصريح.... "ويستوي أن يتم الدخول بشكل مباشر أو غير مباشر كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصالات

ثانيا: أن يتم الدخول إلى محتوى إلكتروني يمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني وأن يكون هذا المحتوى غير متاح للجمهور الاطلاع عليه

ويعدّ المحتوى الإلكتروني هذا محلا للجريمة، وهو الذي يميزها عن جريمة الدخول غير المصرح به المجرد الواردة في المادة 3 من قانون الجرائم الإلكترونية، وقد سبق لنا بيان محل جريمة التجسس في المبحث الأول من هذا الفصل ونحيل بشأنه إلى هناك.

الفرع الثالث: المقصود بعدم التصريح أو تجاوز أو مخالفة التصريح

الدخول إلى النظام المعلوماتي لا يشكل جريمة إلا إذا تم دون تصريح، ويمكن القول أن الدخول المجرم هو الدخول الذي يتم دون رضاء من يملك الحق بالسماح بالدخول، ورغم اختلاف المصطلحات المستخدمة في التشريعات إلا أن لها نفس الدلالة في عدم الأحقية في الدخول إن المفهوم التقليدي لعدم التصريح يفترض أن الشخص ليس له الحق في التواجد في المكان الذي وجد فيه، هذا المفهوم يمكن تطبيقه في الدخول إلى الأماكن في العالم الواقعي، ولكن الأمر مختلف وأكثر تعقيداً في تحديد مفهوم الدخول غير المصرح به إلى النظام المعلوماتي [22] (Kerr, 2003)

وقد بين قانون إساءة استخدام الحاسب الآلي الإنجليزي لسنة 1990 مفهوم عدم التصريح، فجاء في المادة 5/17 من هذا القانون

أن الدخول غير المصرح به يكون عندما لا يكون الشخص المعني مخولاً في الدخول للبرامج والبيانات المخزنة في الحاسب الآلي، أو ولم يحصل على موافقة مسبقة من الشخص المخول بمنح هذه الموافقة، وعرفت المادة الثانية من قانون الجرائم الإلكترونية الأردني التصريح بأنه:" الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو موقع إلكتروني أو الشبكة المعلوماتية بقصد الاطلاع أو إلغاء أو حذف أو إضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول إليها أو إيقاف عمل الأجهزة أو تغيير موقع إلكتروني أو إلغائه أو تعديل محتوياته".

فالدخول يكون مصرحاً به عندما يملك الشخص الحق في الدخول للبيانات، أو عندما يمنح هذا الشخص السلطة بالدخول من شخص آخر يملك الحق بذلك، ويكون الدخول غير مصرح به إذا كان من له السيطرة على النظام قد وضع بعض القيود للدخول إليه ولم يحترم الجاني تلك القيود أو كان يتطلب ضرورة دفع مبلغ من النقود وتم الدخول دون دفع ذلك المبلغ. ولا يثير الدخول من المواقع العامة التي تقدم خدمات الإنترنت (hotspots) كالمطارات، أو الجامعات، أو المطاعم، أو المقاهي أي مشاكل بخصوص التصريح فمجرد توفير هذه الخدمة لمرتادي هذه الأماكن يعني وجود تصريح ضمني بالدخول، ومع ذلك قد تستغل هذه الخدمة في اقتراف جرائم يصعب الوصول لمرتكبيها.[23](Rizwanul, 2009)

ويدخل في مفهوم عدم التصريح بالدخول بالإضافة لعدم وجود تصريح ابتداءً حالة تجاوز التصريح أو مخالفة التصريح والدخول إلى معطيات لا يشملها التصريح، ولا يثير تجاوز التصريح والدخول إلى أجزاء من النظام غير تلك المصرح بالدخول لها أي مشكلة إذا قام بذلك أشخاص لا يعملون في المؤسسة التي تم الدخول إلى أنظمتها المعلوماتية؛ ذلك أن التصريح لا يمتد لغير الأجزاء من النظام المصرح بالدخول لها، وفي هذه الحالة فإن تجاوز التصريح يأخذ حكم عدم التصريح.

المطلب الثاني: أن يتم الدخول إلى الشبكة المعلوماتية أو نظام معلومات أو إلى موقع الكتروني.

حتى يتم النموذج القانوني لجريمة التجسس الإلكتروني الواردة في المادة 12/أ من قانون الجرائم الإلكترونية يجب أن يحصل دخول كامل إلى الشبكة المعلوماتية أو نظام معلوماتي، ولا تختلف هذه الجريمة عن الجريمة التي نصت عليها المادة 12/ج من قانون الجرائم الإلكترونية من حيث عناصر الركن المادي والمعنوي إلا في المحل الافتراضي الذي يجب الدخول إليه فيلزم في الجريمة الواردة في المادة 12/ ج أن يتم الدخول إلى موقع إلكتروني. ولكل من الشبكة المعلوماتية ونظام المعلومات، والموقع الإلكتروني مفهوم فني مختلف عن الآخر.

ويقصد بالشبكة المعلوماتية الارتباط بين أكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها (المادة 2)[24]، ويستوى أن تكون شبكة داخلية بين عدد محدود من الأنظمة المعلوماتية أو شبكة الإنترنت العالمية.

والموقع الإلكتروني عبارة عن حيز لإتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد (المادة 2) [25]. وهو بمفهومه الفني عبارة عن معلومات مخزنة بشكل صفحات وكل صفحة تحتوي على معلومات ويتم تصميمها باستعمال مجموعة من الرموز تسمى لغة تحديد النص ومن أجل الاطلاع على الصفحات يتم طلب استعراض شبكة المعلومات العالمية WWW Browser ويتم بحل رموز الصفحات الخاصة بلغة تحديد النص (الدرة، 81) Hyper Text Mark[26]. ويكتفي أن يتم إنشاء موقع الكتروني لقيام الفعل المكون للجريمة، إذا ثبت أن الغاية من ذلك تسهيل القيام بعمل إرهابي ولو لم يعقب ذلك أي نشاط، مع أنه يصعب إثبات هذه النية إذا لم تقترن بنشاط تالي لإنشاء الموقع الإلكتروني.

وقد وسع المشرِّع من نطاق الوسائل التي ترتكب من خلالها هذه الجريمة، فتقع عندما يتم استخدام أي نظام معلومات، والذي عرفته المادة 2 من قانون الجرائم الإلكترونية بأنه: مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونياً، أو إرسالها، أو تسلمها، أو معالجتها أو تخزينها أو عرضها بالوسائل الإلكترونية. وبذلك فإن جميع الوسائل الإلكترونية تصلح لأن ترتكب من خلالها هذه الجريمة.

المطلب الثالث: أن يتم الدخول للاطلاع على محتوى إلكتروني غير متاح للجمهور.

التجريم الوارد في المادة 21/أ وج من قانون الجرائم الإلكترونية، لم يقصد منه المشرِّع تجريم الدخول المجرد، وهو بذلك ليس غاية في حد ذاته، بل هو خطوة يلجأ لها الجاني من أجل الاطلاع على محتوى إلكتروني غير متاح لعامة الناس؛ لأنه كما جاء في المادة 12يمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني غير متاح للجمهور الاطلاع عليه. وقد سبق لنا بيان هذا العنصر عند بحثنا لمحل التجسس الإلكتروني في قانون الجرائم الإلكترونية فنحيل بشأنه إلى هناك،

ومن مقتضيات المحتوى غير متاح للجمهور أن يكون هذا المحتوى مؤمن بوسائل حماية إلكترونية*[27]، وطبيعي أن يكون المحتوى محفوظ في موقع أو نظام معلومات أو شبكة معلوماتية حكومية، فكل ما يمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني هو شأن عام وله أهمية بحيث قررت الجهات المختصة عدم إتاحة هذه المعلومات للعامة.

المطلب الرابع: الركن المعنوي

الركن المعنوي لجريمة التجسس الإلكتروني يكون بصورة القصد. وهذا ما عبّرت عنه المادة صراحة المادة 12 صراحة فيتعين توفر عناصر القصد الجرمي العام (General intention): العلم والإرادة علم الجاني أن فعله ينصب على نظام معلوماتي أو شبكه معلوماتية، عالما بأنه يدخل لموقع إلكتروني أو نظام معلومات، أو شبكة إلكترونية، وأنه غير مصرح له في الدخول

وبالإضافة لعنصر العلم يجب توفر عنصر الإرادة حتى يقوم القصد الجرمي، إرادة الفعل وإرادة النتيجة المتمثلة في الدخول؛ غير المصرح به، فإذا أراد الفاعل السلوك الجرمي دون إرادة تحقق النتيجة المتمثلة في الدخول فيتوفر في حقه الخطأ غير المقصود، وهو غير معاقب عليه في جريمة الدخول غير المصرح، كأن يجد شخص نفسه وقد دخل لموقع إلكتروني غير مسموح له الدخول إليه، وقد يشكل فعله هذا جريمة البقاء غير المصرح به حال اكتشافه الأمر، ورغم ذلك يبقى في النظام. فإذا توفرت عناصر القصد الجرمي العام فلا أهمية للباعث على ارتكابها فهو ليس عنصراً من عناصرها.

وتتطلب المادة12 /أ وج من قانون الجرائم الإلكترونية قصداً جرميا خاصاً في جريمة الدخول غير المصرح به يتمثل بأن تكون الغاية من الدخول الاطلاع على البيانات أو المعلومات التي تمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني*.[28]

المبحث الثالث

الجزاءات المقررة لجرائم التجسس الإلكتروني

سنبين الجزاءات المقررة لجرائم التجسس في قانون حماية أسرار ووثائق الدولة التي تصلح الوسائل الإلكترونية كوسيلة لارتكابها في المطلب الأول، وكذلك الجزاءات المقررة لجرائم التجسس الإلكتروني في قانون الجرائم الإلكترونية.

المطلب الأول: الجزاءات المقررة لجرائم التجسس في قانون حماية أسرار ووثائق الدولة.

عند بحثنا لجرائم التجسس الواردة في قانون حماية أسرار ووثائق الدولة، وجدنا أن جريمتي الاستحصال على سر من أسرار الدولة، وجريمة إفشاء وإبلاغ أسرار الدولة يمكن أن ترتكب بوسائل إلكترونية.

عاقب المشرِّع على جريمة الحصول على أسرار الدولة أو سرقتها بصورة مجردة بالأشغال الشاقة المؤقتة لمدة لا تقل عن عشر سنوات، أي من عشر إلى خمس عشرة سنة. وإذا اقترفت الجريمة لمصلحة دولة أجنبية تكون العقوبة الأشغال الشاقة المؤبدة، وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الإعدام.

ولا يشترط لإعمال الظروف المشددة لهذه الجريمة أن يوصل الفاعل السر للدولة الأجنبية أو الدولة العدوة، فيكفي أن يحصل عليه ويثبت بعد ذلك أنه إنما أراد الحصول على السر لمنفعة دولة أجنبية أو دولة عدوة*.([29])

ويعاقب مرتكب جريمة إفشاء أو إبلاغ الأسرار المتعلقة بأمن الدولة دون سبب مشروع بالأشغال الشاقة المؤقتة لمدة لا تقل عن عشر سنوات، وتشدد العقوبة إلى الأشغال الشاقة المؤبدة إذا ارتكبت الجريمة لمنفعة دولة أجنبية، وتصبح العقوبة الإعدام إذا كانت الدولة المقترفة الجريمة لمنفعتها عدوة.

المطلب الثاني: الجزاءات المقررة لجرائم التجسس في قانون الجرائم الإلكترونية

سنعرض في الأفرع الآتية الجزاءات المقررة لجرائم التجسس في قانون الجرائم الإلكترونية بصورها البسيطة، والمشددة، والجزاءات المقررة لهذه الجرائم باعتبارها من الجرائم الإلكترونية.

الفرع الأول: الجزاءات المقررة لجرائم التجسس بصورتها البسيطة

تنص المادة 12/أ من قانون الجرائم الإلكترونية على أن يعاقب كل من دخل قصدا دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو نظام معلومات للاطلاع على بيانات أو معلومات غير متاحه للجمهور تمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة الآف دينار ".

وجاء في المادة 12/ج أنه ويعاقب كل من دخل قصدا الى موقع الكتروني للاطلاع على بيانات أو معلومات غير متاحة للجمهور غير متاحه للجمهور تمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار

من خلال هاتين الفقرتين نجد أنهما يختلفان فقط في أن الدخول في الفقرة (أ) يكون الى الشبكة المعلوماتية أو نظام معلومات، بينما الدخول في الفقرة (ج) يكون لموقع الكتروني، وكذلك عقوبة الغرامة في الفقرة (أ) حدها الأدنى خمسمائة دينار والأعلى خمسة الآف دينار، بينما الغرامة في الفقرة (ج) محدده بخمسمائة دينار.

ولا يعاقب على الشروع في هذه الجنح، فمحاولة الدخول إلى نظام معلوماتي، أو شبكة معلوماتية، أو موقع إلكتروني من أجل الاطلاع على المعلومات غير المسموح للجمهور الاطلاع عليها لتعلقها بالأمن الوطني، أو العلاقات الخارجية للملكة، أو السلامة العامة، أو الاقتصاد الوطني لا يشكل جريمة في التشريع الأردني؛ لأن هذه الجرائم من الجنح ولم يرد في قانون الجرائم الإلكترونية نص يعاقب على الجنح الواردة فيه.

الفرع الثاني: الظروف المشددة لعقوبات جرائم التجسس

وردت الظروف المشددة لجريمة الدخول غير المصرح به للشبكة المعلوماتية أو نظام معلومات التي في المادة 12/ب فوفقا لنص هذه المادة إذا كان الدخول المشار اليه في المادة 12/أ بقصد الغاء أو اتلاف أو تدمير أو تغيير أو نقل أو نسخ أو إفشاء البيانات أو المعلومات غير المتاحة للجمهور التي تمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني فتكون العقوبة الاشغال الشاقة المؤقتة وبغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة الآف دينار.

فالتشديد يرتبط بالهدف الذي يسعى له الجاني من الدخول غير المصرح، فالأمر لديه تعدى حد الاطلاع إلى نية القيام بصوره من صور الاعتداء التي وردت في المادة 12/ب فإذا ثبتت هذه النية لديه كانت بمثابة قصد جرمي خاص، وهذا الأمر له أهمية حال عدم قدرته على تحقيق الغاية التي تلغياها فإذا كنت من الاهداف الواردة في النص وتحقق الدخول ولم تتحقق الغاية وقعت الجريم تامة بظرفها المشدد، وإذا حقق الجاني مبتغاه بحصول إحدى صور الاعتداء وقعت كذلك الجريمة تامه بظرفها المشدد وبما أن الجريمة عندما يتوفر الظرف المشدد جناية فإن محاولة الدخول للاعتداء على البيانات وعدم القدرة على ذلك يشكل شروع في هذه الجريمة.

وإذا كان الدخول المشار إليه في المادة 12/ج الدخول لموقع الكتروني بقصد الغاء أو اتلاف أو تدمير أو تغيير أو نقل أو نسخ أو إفشاء البيانات أو المعلومات غير المتاحة للجمهور التي تمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني فتكون العقوبة الاشغال الشاقة المؤقتة وبغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة آلاف دينار. فالظروف المشددة الواردة في المادة 12/ب ذات الظروف في المادة 12/ج باستثناء أن الدخول في هذا الظرف يكون لموقع الكتروني وكان بإمكان المشرِّع أن يحكم صياغة المادة 12 ولو فعل ذلك لأصبحت المادة 12 مكونه من فقرتين بدلا من أربع فقرات.

ويقصد بالإلغاء الإزالة سواء أكانت بشكل كلي أم جزئي، والإتلاف يكون بكل فعل يلحق ضرراً بالشيء، أما التدمير فهو خراب شامل، والتغيير له مفهوم أوسع وأشمل فهو يكون بصورة إضافة أو تعديل أو حذف، والنقل يعني تغيير الموضع، والنسخ يتحقق في حالة الحصول على البيانات والمعلومات دون أن يؤدي ذلك إلى فقدان الأصل المنسوخ عنه، والإفشاء يكون بنشر البيانات والمعلومات دون تمييز. نلاحظ أن المشرِّع ذكر ظروف متعددة ومتداخلة أحياناً في المعنى، حرصاً منه على ألا يفلت منه أي حالة من حالات الاعتداء على بيانات ومعلومات تتعلق بمصالح عليا للدولة.

الفرع الثالث: الجزاءات المقررة لجرائم التجسس باعتبارها من الجرائم الإلكترونية.

من الجزاءات التي تفرض على مرتكب جريمة التجسس الإلكتروني كونها من الجرائم المنصوص عليها في قانون الجرائم الإلكترونية، المصادرة، وإغلاق المحل الذي ارتكبت فيه الجريمة. ويقصد بالمصادرة نزع ملكية شيء ثبتت صلته بالجريمة المرتكبة وإضافته إلى أملاك الدولة دون مقابل، والمصادرة تكون عقوبة تكميلية عندما ترد على شيء يباح حيازته وتداوله، ولا يحكم بها في هذه الحالة إلا تبعاً للحكم بعقوبة أصلية، وتكون المصادرة تدبيرا احترازياً متى وقعت على شيء تعد حيازته أو تداوله جريمة وتكون في هذه الحالة وجوبية (سلامة، 2001)[30]. وجعلت المادة 13/ج من قانون الجرائم الإلكترونية أمراً جوازيًا للمحكمة وجاء فيها أن للمحكمة المختصة الحكم بمصادرة الأجهزة والأدوات والوسائل والمواد وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع إلكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون، ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة على نفقة الفاعل.

لا تسري بحق غير مرتكب الجريمة حسن النية؛ فتطبيقها على الغير حسن النية يتنافى مع مبدأ شخصية العقوبة ويعني تطبيقها على شخص أجنبي عن الجريمة لم يسهم فيها، على أنه إذا كانت الملكية مشتركه لم يصادر منها سوى حصة المتهم، ورعاية حق الغير حسن النية واجبه سواء نشأ حقه قبل ارتكاب الجريمة أو بعد ارتكابها شريطة ألا يكون عالماً بأن الشيء استعمل في الجريمة أو تحصل منها (رمضان، دون سنة نشر).[31]

وتضاعف العقوبة كذلك على مكرر أي من الجرائم الواردة في قانون الجرائم الإلكترونية ومنها بطبيعة الحال جريمة التجسس الإلكتروني (المادة 15)[32].بما أن جريمة التجسس الإلكتروني تكون بصورتها البسيطة جنحه وتكون جناية في صورتها المشددة، وهي في كلا الحاليين لا تقع بطريق الخطأ غير المقصود، فهي بذلك تصلح أن تكون محلا للاشتراك الجرمي الأصلي والتبعي وفقا للأحكام العامة في قانون العقوبات وقد خرج قانون الجرائم الإلكترونية على الأحكام العامة في الاشتراك الجرمي التبعي وساوى بين عقوبة الاشتراك الأصلي والتبعي، فوفقاً للمادة 14 من قانون الجرائم الإلكترونية يعاقب كل من قام قصداً بالاشتراك، أو التدخل، أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة فيه لمرتكبها.

الخاتمة

تناولنا في هذا البحث موضوع التجسس الإلكتروني في التشريع الأردني وخلصنا إلى أن المشرِّع الأردني قد جرّم الدخول أو محاولة الدخول إلى أماكن محظورة قصد الحصول على أسرار، أو أشياء، أو وثائق محمية، أو معلومات يجب أن تبقى سرية حرصا على سلامة الدولة، وأنه لا يشترط لقيام هذه الجريمة وفقا للمادة 114 من قانون حماي أسرار ووثائق الدولة الحصول على السر إذ أن المشرِّع اعتبر هذه الجريمة من جرائم الخطر المبكر التي ساوى فيها بين الفعل والشروع به.

إن الأسرار المتعلقة بأمن الدولة لا يمكن إفشاؤها أو الإبلاغ عنها وبخلاف ذلك يكون من وصل إلى حيازته أو علمه أي سر من الأسرار أو المعلومات أو أي وثيقة محمية بحكم وظيفته أو كمسؤول أو بعد تخليه عن وظيفته أو مسؤوليته لأي سبب من الأسباب فأبلغها أو أفشاها دون سبب مشروع استحق العقوبة الواردة في المادة 16 من قانون حماية أسرار ووثائق الدولة.

وجاء أيضاً قانون الجرائم الإلكترونية ليجرم التجسس المتمثل في المساس ببيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني. وعليه يعد كل دخول قصدا دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو نظام المعلومات للاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني جرما يقتضي العقاب في حال ثبوته وفقا للمادة 12/أ من قانون الجرائم الإلكترونية الأردني.

ووجدنا أن المشرِّع الأردني قد وسع من نطاق الوسائل التي ترتكب من خلالها هذه الجريمة، فتقع عندما يتم استخدام أي نظام معلومات، والذي عرفته المادة 2 من قانون الجرائم الإلكترونية بأنه: مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونياً، أو إرسالها، أو تسلمه، أو معالجتها أو تخزينها أو عرضها بالوسائل الإلكترونية. وبذلك فإن جميع الوسائل الإلكترونية تصلح لأن ترتكب من خلالها هذه الجريمة.

لقد أورد المشرِّع الأردني ظروف مشدده لجريمة الدخول غير المصرح به للشبكة المعلوماتية أو نظام معلومات التي في المادة 12/ب فوفقا لنص هذه المادة إذا كان الدخول المشار إليه في المادة 12/أ بقصد إلغاء أو إتلاف أو تدمير أو تغيير أو نقل أو نسخ أو إفشاء البيانات أو المعلومات غير المتاحة للجمهور التي تمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني.

فالتشديد يرتبط بالهدف الذي يسعى له الجاني من الدخول غير المصرح، فالأمر لديه تعدى حد الاطلاع إلى نية القيام بصوره من صور الاعتداء التي وردت في المادة 12/ب فإذا ثبتت هذه النية لديه كانت بمثابة قصد جرمي خاص، وهذا الأمر له أهمية حال عدم قدرته على تحقيق الغاية التي سعى إليها، فإذا كانت من الأهداف الواردة في النص وتحقق الدخول ولم تتحقق الغاية وقعت الجريمة تامة بظرفها المشدد، وإذا حقق الجاني مبتغاه بحصول إحدى صور الاعتداء وقعت كذلك الجريمة تامه بظرفها المشدد.

من خلال ما توصل إليه البحث من نتائج، فإن الباحث يوصي بما يلي:

1- أن ينص المشرِّع الأردني في قانون الجرائم الإلكترونية على تجريم البقاء غير المصرح به داخل النظام المعلوماتي، أو الشبكة الإلكترونية، أو الموقع الإلكتروني، إذا كان دخول الجاني إلى النظام بمحض الصدفة، أو السهو أو الخطأ، وكنه بقي داخل النظام الإلكتروني.

2- تعديل نص المادة (12/أ) من قانون الجرائم الإلكترونية الأردني وذلك بتشديد عقوبة الدخول غير المشروع على البيانات والمعلومات غير المتاحة للجمهور وتمس الأمن الوطني بهدف الاطلاع عليها لأن العقوبة الواردة لا تتناسب وحجم الخطر والضرر الذي قام به الجاني بحيث يتم رفع الحد الأدنى للعقوبة الجنائية.

3- تعديل نص المادة (12/د) من قانون الجرائم الإلكترونية الأردني وذلك بتشديد عقوبة نسخ المعلومات أو البيانات، أو إفشاؤها، أو إتلافها، برفع الحد الأدنى والأعلى للعقوبة الجنائية لتتناسب وحج الضرر الذي قام به الجاني لا سيما أن أفعاله قد تتخذ صور نسخ أو إفشاء أو إتلاف بيانات سرية تخص الدولة.

4- زيادة إجراءات الحماية للمعلومات والبيانات ومواقع الدولة الإلكترونية التي تحتوي على نظم تمس الأمن الوطني، أو الاقتصاد الوطني، أو المعلومات السرية للدولة.

5- تواصل التعاون الدولي لمواجهة الجريمة الإلكترونية لا سيما أن الجريمة الإلكترونية من الجرائم العابرة التي لا تقيده حدود الدول أو تشريعاتها.

الهوامش

(1) لسان العرب لابن منظور، ج4، مطبعة الشروق، بيروت، ط، 1985، ص 459.

(2) المرجع السابق، ص 337.

(3) قيل بأن التجسس يعني "سعي أي شخص أجنبي صوب الحصول على أسرار الدولة أو تسليمها لأية جهة خارجية متى كان ذلك يؤدي إلى الأضرار بمصلحة الدولة". وقيل أيضا بأن التجسس 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" د. جابر المراغي، جرائم انتهاك أسرار الدفاع عن البلاد من الناحيتين الموضوعية والإجرامية، دار النهضة العربية، القاهرة، 1998، ص91 93.

(4) محمد راكان الدغمي: التجسس وأحكامه في الشريعة الإسلامية، دار السلام، القاهرة، 1984، ص65.

(5) من أشهر عمليات التجسس العلمي تمكن الاتحاد السوفيتي سابقاً من سرقة أسرار صناعة القنبلة الذرية فيما عرف باسم قضية "جوزتكو". أكد رئيس الاستخبارات الألمانية (أو فمست هاينج) في أثناء ندوة حرب المعلوماتية) في المقر العام لأجهزة الاستخبارات الألمانية أن الحروب ستدور من الآن فصاعداً في مجال المعلوماتية، وخاصة الإنترنت، وأن أجهزة الاستخبارات تهتم بالتكنولوجيا الجديدة، والجيوش تدرب الجنود على القرصنة المعلوماتية. انظر جريدة القدس العربي، العدد 3537، تاريخ 2000/11/5.

(6) في عام 1981 قدر مكتب التحقيقات الفيدرالية (F.B.I) أن 35% من مجموع الدبلوماسيين السوفييت في الولايات المتحدة يعملون لصالح المخابرات السوفيتية، فقد كانت السفارة السوفيتية ترفع هوائياً بذبذبات عالية موجهاً قسم منه إلى البنتاغون والبيت الأبيض، والقسم الآخر إلىمركز (C.I.A) في (لانغلي).

ويلوح بيروفسكا: الجاسوسية والجاسوسية المضادة، ترجمة حكمة البيني، بيروت، ط2، 1992، ص165.

وبتاريخ 2001/3/22 أصدر الرئيس الأمريكي بوش قراراً بطرد خمسين دبلوماسياً روسياً للاشتباه بقيامهم بأنشطة تجسس، وإعمالاً لقاعدة المعاملة بالمثل أعلن وزير الخارجية الروسي (ايغور ايفانوف) إن روسيا ستطرد خمسين دبلوماسياً أمريكياً رداً على القرار الأمريكي. جريدة الرأي الأردنية العدد 11154، تاريخ 2001/3/24م.

وفي 1999/12/10 أوقف مكتب التحقيقات الفيدرالي (ستانيسلان جوسيف) الملحق بالسفارة الروسية في أثناء تواجده في محيط مبنى وزارة الخارجية الأمريكية بتهمة التجسس حيث استطاع التنصت على 50 إلى100 اجتماع لوزارة الخارجية الأمريكية وذلك من قاعة في الطابق السابع من مبنى الوزارة التي تستعملها وزيرة الخارجية (اولبريت) ومستشاروها وذلك بواسطة أجهزة تنصت تم زرعها في قاعة الاجتماعات. جريدة القدس العربي، العدد 3296، تاريخ 1999/12/11.

كما تقوم السفارات الإسرائيلية بعمليات تجسس ويوجد بهذه السفارات تقنيات عالية للتنصت، على كل الدول ومنها الولايات المتحدة الأمريكية لكن هذه الأخيرة تتغاضى عن ابنتها المدللة، ففي عام 1997 تمكن دبلوماسي إسرائيلي بالسفارة الإسرائيلية في واشنطن من نقل معلومات بالغة السرية من الملفات الأمريكية وتم كشف ذلك من خلال عملية التنصت التي تقوم بها المخابرات الأمريكية على أجهزة الاتصالات للسفارات في واشنطن، وفي أثناء المكالمة التي كان يجريها الدبلوماسي الإسرائيلي انقطع التيار الكهربائي فحدث عطلاً فنياً في جهاز تأمين المكالمات الذي تستخدمه السفارة الاسرائيلية مما أدى إلى سهولة التقاط المحادثة، وقد أعلن (نيكولاس بيرنز) المتحدث باسم الإدارة الأمريكية

عقب هذه الفضيحة أن إسرائيل بالنسبة للولايات المتحدة دولة صديقة وحليفة مهما كانت الظروف.
هلال يوسف: أسرار الجاسوسية ولعبة المخابرات، مركز الحضارة، القاهرة، 1998، ص16 وما بعدها.
وتمارس السفارة الإسرائيلية عمليات التجسس والتنصت من خلال سفاراتها الموجودة في بعض العواصم العربية، فعقب المحاولة الفاشلة لاغتيال الرئيس المصري حسني مبارك في أديس أبابا عام 1995 وفي أثناء عودته إلى القاهرة التقطت أجهزة التجسس في السفارة الإسرائيلية في القاهرة المكالمة الهاتفية التي تبين الرئيس مبارك وصفوت الشريف وزير الإعلام، وكان للإذاعة الإسرائيلية السبق في إذاعة خبر محاولة اغتيال الرئيس مبارك. جريدة الرأي الأردنية العدد 11047، تاريخ 2000/12/7م.

(7) وقد نصت المادة العاشرة من قانون حماية أسرار ووثائق الدول على الوثائق العادية حيث جاء فيها أنه "مع مراعاة أحكام أي قانون آخر تعدّ جميع الوثائق الرسمية الأخرى التي لا تشملها أحكام هذا القانون (وثائق عادية) وعلى المسؤول أن يحافظ على الوثائق العادية ويحفظها من العبث أو الضياع، ولا يجوز إفشاء مضمونها لغير أصحاب العلاقة بها ما لم يصرح بنشرها".

(8) يجري تغليف وإرسال الوثيقة المحمية المصنفة بدرجة (سري للغاية) على النحو التالي: أ- توضع الوثيقة ضمن مغلف جديد معنون إلى المرسل إليه ويختم 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
5- يرفق بالغلاف نموذج إشعار استلام.
د- يوضع المغلف ضمن مغلف آخر يكتب عليه اسم المرسل إليه ورقم الأوراق الصادرة.
هـ- على المرسل إليه إن يوقع نموذج إشعار الاستلام ويعيده بدون إبطاء إلى مصدره (المادة 4 من قانون حماية أسرار ووثائق الدولة).
وتحفظ الوثائق المحمية، من درجة (سري) بمغلف جديد مكتوب عليه اسم المرسل إليه ورقم الصادر (المادة 7 من قانون حماية أسرار ووثائق الدولة).
أما الوثيقة المحمية التي تحمل (درجة محدود) فتوضع في مغلف عادي يكتب عليه اسم المرسل إليه ويشمع بالشمع الأحمر ويختم بخاتم محدود ويكتب عليه رقم الصادر: (المادة 9 من قانون حماية أسرار ووثائق الدولة).

(9) عبدة الوهاب الكيالي: موسوعة السياسة، ج1، المؤسسة العربية للدراسات والنشر، بيروت، ط1، 1990، ص331.

(10) محمد طهبدوي: دراسات سياسية وقومية، منشأة المعارف، الإسكندرية، 1963، ص283.

(11)انظر المادة 3/أ/4 من قانون محكمة أمن الدولة الأردني.

(12) محمد الفاضل: الجرائم الواقعة على أمن الدولة، ط4، 1978، ص294 وما بعدها.

(13) يقول (يوري بالادز) المسؤول في المخابرات الروسية: "أن جواسيس الكرملين الذين نجحوا في سرقة أسرار القنبلة الذرية يسعون الآن وراء هدف آخر هو أسرار الحياة الاقتصادية الأمريكية ومنها تركيبة مشروب الكوكا كولا" ويضيف قائلاً:"إن الجواسيس لا يسعون فقط لسرقة أسرار التكنولوجيا بهدف تدعيم الصناعات الاقتصادية لبلادهم، وإنما ينقبون وراء أسرار التسويق والخطط للدول الأخرى". د. جابر المراغي، جرائم انتهاك أسرار الدفاع عن البلاد من الناحيتين الموضوعية والإجرائية، دار النهضة العربية، القاهرة، 1988، ص116.

(14) محمد الفاضل: مرجع سابق، ص380

(15) فإذا تم سرقة السر أو الحصول عليه لحساب أشخاص لا يعملون لمصلحة دولة أجنبية أو لحساب جهة ليست لها شخصية دولية باعتبارها دولة كالمنظمات الدولية فإن الظروف المشددة لا تطبق.

(16) عبد المهيمن بكر: جرائم أمن الدولة الخارجي، دراسة في القانون الكويتي والمقارن، دار النهضة العربية، القاهرة، 1976، ص183.

(17) محمد الفاضل: مرجع سابق، ص391-392.

(18) Orin S. Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization NYU LawReview, Vol. 78, No. 5, pp. 1596-1668, November 2003..p.1620

(19) عمر محمد أبو بكر بن يونس: الجوانب الموضوعية والإجرائية لجرائم الإنترنت، رسالة دكتوراة، جامعة عين شمس 2004، ص331.

(20) Bainbridge.D: Introduction tocomputerlaw,Edition4London,200...p308

(21) راجع: سامي الرواشدة؛ د. أحمد الهياجنة: مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجاً، المجلة الأردنية في القانون والعلوم السياسية، المجلد (1) العدد (3) تشرين الأول 2009، ص130.

(22)Orin s.Kerr: op.cit.p.1622.

(23)DrNiloufer.S,Rizwanul, Peter. G: Unauthorized access to wireless local area limitation of the present Australien laws, Computer law & security neReview.25,2009,536-542.p.542

(24) المادة 2 من قانون الجرائم الإلكترونية.

(25)المادة 2 من قانون الجرائم الإلكترونية.

(26) إياد علي الدرة، الإرهاب الإلكتروني، مجلة أمن المعلومات، العدد81، تشرين الثاني، ص 23.

(27) وقد تطلبت بعض التشريعات لتجريم الدخول غير المصرح به أن يكون النظام المعلوماتي الذي تم الولوج إليه محمياً بوسائل حماية أمنية،

ومن هذه التشريعات قانون العقوبات الإيطالي، المكسيكي، الفنلندي، اليوناني، الألماني، والسويسري.وفي القانون الأمريكي الفدرالي يشترط أن يتم الدخول لحاسوب محمي ويقصد بالحاسوب المحمي أي حاسوب يستخدم على وجه الحصر (Exclusively) في مؤسسة مالية أو حكومة فدرالية أو بين ولايتين أو بالتجارة الأجنبية أو بالاتصالات (انظر المادة 615 من قانون العقوبات الإيطالي، 211من قانون العقوبات المكسيكي، الفصل 38 من قانون العقوبات الفلنندي، المادة 370 من قانون العقوبات اليوناني، المادة 202 من قانون العقوبات الألماني، المادة 143)، وشدد القانون البرتغالي عقوبة جريمة الدخول غير المصرح به إذا تم الدخول بخرق قواعد الحماية، ولم يتطلب من التشريعات العربية مثل هذا الشرط سوى التشريع الكويتي فقد اشترطت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات لسنة 2015عند تعريفها للدخول غير المشروع أن يتم الدخول باختراق وسائل وإجراءات الحماية ومفهوم ذلك لزوم أن يكون النظام المخترق محمي بوسائل حماية ضد الاختراق.(انظر المادة 6 من قانون جرائم الكمبيوتر البرتغالي رقم 109 لسنة 2009 حيث إن عقوبة جريمة الدخول غير المصرح به الحبس حتى سنه وتشدد لتصبح الحبس حتى ثلاث سنوات إذا تم الدخول عن طريق خرق قواعد الأمان.

(28) وفق المادة 2/7 من النظام السعودي فإنه يعد قصد جرمي خاص الدخول غير المشروع الذي يهدف للحصول على بيانات تمس الأمن الداخلي أو الخارجي أو اقتصادها الوطني، ويعد قصد جرمي خاص في القانون العُماني الدخول بقصد الحصول على البيانات أو المعلومات الحكومية الإلكترونية السرية بطبيعتها أو بموجب تعليمات صادره بذلك لمواد 6و 7 من قانون مكافحة جرائم تقنية المعلومات العُماني رقم 12 لسنة 2011.

(29) فإذا تم سرقة السر أو الحصول عليه لحساب أشخاص لا يعملون لمصلحة دولة أجنبية أو لحساب جهة ليست لها شخصية دولية باعتبارها دولة كالمنظمات الدولية فإن الظروف المشددة لا تطبق.

(30) مأمون محمد سلامة: قانون العقوبات / القسم العام، ط2001،3، ص609.

(31) عمر السعيد رمضان: قانون العقوبات/ القسم العام دار النهضة العربية، دون سنة نشر، ص638.

(32) انظر المادة 15 من هذا القانون.

المصادر والمراجع

المراجع العربية:

ابن منظور، لسان العرب، ج4، مطبعة الشروق، بيروت، ط، 1985.

إياد علي الدرة، الإرهاب الإلكتروني، مجلة أمن المعلومات، العدد81، تشرين الثاني.

جابر المراغي، جرائم انتهاك أسرار الدفاع عن البلاد من الناحيتين الموضوعية والإجرامية، دار النهضة العربية، القاهرة، 1998.

سامي الرواشدة؛ أحمد الهياجنة: مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجاً، المجلة الأردنية في القانون والعلوم السياسية، المجلد (1) العدد (3) تشرين الأول 2009.

عبد المهيمن بكر: جرائم أمن الدولة الخارجي، دراسة في القانون الكويتي والمقارن، دار النهضة العربية، القاهرة، 1976.

مأمون محمد سلامة: قانون العقوبات / القسم العام، ط2001،3.

هلال يوسف: أسرار الجاسوسية ولعبة المخابرات، مركز الحضارة، القاهرة، 1998.

عمر السعيد رمضان: قانون العقوبات/ القسم العام دار النهضة العربية، دون سنة نشر.

عبد الوهاب الكيالي: موسوعة السياسة، ج1، المؤسسة العربية للدراسات والنشر، بيروت، ط1، 1990.

محمد الفاضل: الجرائم الواقعة على أمن الدولة، ط4، 1978.

محمد راكان الدغمي: التجسس وأحكامه في الشريعة الإسلامية، دار السلام، القاهرة، 1984.

محمد طه بدوي: دراسات سياسية وقومية، منشأة المعارف، الإسكندرية، 1963.

ويلوح بيروفسكا: الجاسوسية والجاسوسية المضادة، ترجمة حكمة البيني، بيروت، ط2، 1992.

المراجع الأجنبية:

Bainbridge. D: Introduction to computer law, Edition4London, 200....

Niloufer. S, Rizwanul, Peter. G: Unauthorized access to wireless local area limitation of the present Australien laws, Computer law & security ne Review.25,2009,536-542.

Orin S. Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization NYU Law Review, Vol. 78, No. 5, pp. 1596- 1668, November 2003.

الرسائل الجامعية:
عمر محمد أبو بكر بن يونس: الجوانب الموضوعية والإجرائية لجرائم الإنترنت، رسالة دكتوراة، جامعة عين شمس 2004.

الصحف والدوريات:
جريدة الرأي الأردنية العدد 11047، تاريخ 2000/12/7م.
جريدة الرأي الأردنية العدد 11154، تاريخ 2001/3/24م.
جريدة القدس العربي، العدد 3296، تاريخ 1999/12/11.

Cyber Espionage Crimes in Jordanian Legislation

Abedulellah Mohammed Al- Nawayseh, Mammdouh Hassan Al- adwan*

Abstract

This paper examines the subject of cyber espionage crimes in Jordanian legislation due to the risk of electronic espionage represented in the entering of the offender into the information network, information system or a website to obtain non-public electronic content which is not publicly accessible. The same electronic content compromises national security, external relations of the State, public safety or national economy. This paper aims at shedding light on the Jordanian penal legislation, which provided electronic content protection containing confidential information pertaining to the state, specifically those provisions laid down in the Law on Protection of State Secrets and the Cyber Crime Act. Therefore, this paper has been addressed through a preliminary study and three other topics. It is shown in the introductory section, the essence of cyber espionage and presenting the concept of espionage in general along with determining the meaning of cyber espionage in particular as well as common forms of the cyber espionage. Thus, we explain in the first section the extent to which cyber espionage crimes can be committed by electronic means and their provisions. In the second section, we have shown the cyber espionage in the Jordanian Cybercrime Act and highlighted the text of Article 12 of this Act. Finally, in Section III, we have stated established sanctions for cyber espionage crimes, both in Protection of State Secrets Act or those established in the Cyber Crime Act.

Keywords: Spyware; Electronic Content; Unauthorized Access and Confidential Information.

* Faculty of Law, University of Sharjah, United Arab Emirates; and Sheikh Nawah Al Qudah College of Law, International Islamic Sciences University, Jordan. Received on 26/8/2017 and Accepted for Publication on 3/6/2018.