وزارة التعليـــم العـالي والبحـــث العلمـــــي

جامعـة العـربي التبســي – تبســة –

كليـة الحقـوق والعلـوم السياسية

قســـم الحقـوق

آليـات مكافحـة التـجسس الإلكتـرونـي

أطروحة مقدمـة لنيـل شهـادة دكتـوراه العلـوم فـي القانون الجنائي

إعـداد الطالبـــة:
نـاديـة سلامـي

إشـراف الأستـــاذ:
الطـاهـر دلـول

لجنـــة المنـــاقشـــة

إسم ولقب الأستاذ	الرتبة العلمية	الجامعة الأصلية	الصفة
بشيـر هادفـي	أستاذ	جامعة العربي التبسـي– تبسة –	رئيســـــــاً
الطاهر دلـــول	أستاذ	جامعة العربي التبسـي– تبسة –	مشرفاً ومقرراً
الأخضر بوكحيل	أستاذ	جامعة باجـي مختـار– عنابة –	عضواً مناقشاً
سعـاد نويـــري	أستاذ محاضر(أ)	جامعة العربي التبسـي– تبسة –	عضواً مناقشاً
كوسـر عثامنية	أستاذ محاضر(أ)	جامعة عباس لغرور– خنشلة –	عضواً مناقشاً
هشـام بخـوش	أستاذ محاضر(أ)	جامعة محمد الشريف مساعدية–سوق أهراس–	عضواً مناقشاً

السنـــــــة الجامعيـــــــة:

2019 -2018

بسم الله الرحمن الرحيم

شـــُـكر

أتقدم بجزيل الشكر وخالص العرفان إلى أستاذي البروفيسور: الطاهر دلول، الذي ساعدني كثيراً في إنجاز هذه الأطروحة.

كما أتوجه بشكري لأساتذتي الكرام أعضاء لجنة المناقشة لقبولهم مناقشة هذه الأطروحة.

ولا يفوتني كذلك شُكر جميع من ساعدني وتمنى لي التوفيــق والنجــاح.

إهـــــــداء

إلى عائلتـــي.

مـــــــقـــــــدمـــــــــــة

مقدمـــــــــة:

أولاً- التعريــف بالموضـــــوع:

لطالما إرتبط وجود الدولة واستمرارها بمدى قدرتها على التفاعل مع الظروف المحيطة بها، وكذا على حكامة القرارات التي تتخذها مسايرة للتغيرات التي تحصل في أحيان كثيرة نتيجة تداخل معطيات عديدة على درجات متفاوتة من الأهمية. وتعتمد عملية إتخاذ مثل هكذا قرارات على إمكانية الدولة على تجميع المعلومات بمختلف أنواعها.

وقد عرفت المعلومات تطوراً ملفتاً إن على صعيد الأهمية أو وسائل الجمع؛ فمن زاوية الأهمية تبدو جلية المكانة المحورية التي تحتلها المعلومة في بناء السياسة الأمنية للدولة بمختلف مستوياتها: المستوى الاجتماعي، والمستوى الثقافي، والمستوى الاقتصادي، والمستوى السياسي، والمستوى العسكري، وإن طغى في يومنا هذا المستوى الاقتصادي على المستويات الأخرى؛ لتصبح المعلومة الاقتصادية قيمة مالية تراهن عليها كل الدول على رأسها الدول المتقدمة؛ أما من زاوية وسائل جمع المعلومة، يشهد العالم نمواً ملفتاً وسريعاً لها لا يقع ضمن دائرة حصر أو تعداد؛ فما يكشف للعلن منها ويصيب المطلع عليها بالذهول يُعد في نظر من يطورها ويبتكر غيرها وسيلة تقليدية تجاوزها الزمن. هذا التطور على مستوى تحصيل المعلومة كان نتاجاً لعوامل كثيرة أهمها على الإطلاق التطور الذي شهدته وتشهده تكنولوجيات الإعلام والاتصال.

وقد أحدثت تكنولوجيات الإعلام والاتصال ثورة في الماديات والمفاهيم غيرت كثيراً من أساليب الحياة والتفاعل مع الآخرين؛ فظهر بموازاة العالم الحقيقي، عالم آخر افتراضي يمارس عبره الأشخاص (طبيعيون ومعنويون) ذات التصرفات الكلاسيكية ولكن بوسائل حديثة، اصطلح على تسميته بالعالم أو الفضاء الالكتروني. وكما أسهم هذا الأخير في تحسين نمط ونوعية العيش، فقد سهل كذلك أساليب القيام بممارسات ضارة شكلت انتهاكاً لسيادة الدول الأخرى ولو بحجة ممارسة الدولة لحقها في البقاء الذي يرتبط – كما تمت الإشارة إليه أنفاً- بكم المعلومات التي تجمعها عن نظيراتها من الدول الأخرى؛ فانتقلنا من مفهوم التجسس التقليدي المُمارس في الفضاء الاعتيادي، إلى مفهوم جديد هو التجسس الإلكتروني الممارس في الفضاء الإلكتروني.

هذا المفهوم الجديد أضاف كماً آخر من التساؤلات إلى رصيد إبهام ومطاطية المصطلح القديم (التجسس)، كما غير زاوية دراسته بإضافة عناصر مستجدة تشكل ماهية هذا المفهوم الحديث؛ إذ لم تظل الدولة فاعله ومُحتكِر ممارسته الوحيد؛ بحيث زاحمها في هذا كل من الأفراد لحسابهم الخاص، سواء بدافع إثبات الذات وتحدي الحماية الفنية للمنظومات المعلوماتية المحتوية لأسرار الدفاع الوطني، أم بدافع الفضول فقط، أم بدافع الانتقام، أم بدافع الحصول على المال، وإلى جانب الأفراد إتخذت المؤسسات ذات الصبغة الإقتصادية –أساساً– من التجسس الإلكتروني التقنية المحورية للحصول على الأسرار الاقتصادية للمؤسسات الأجنبية الأخرى، وفي أحيان كثيرة بدعم قانوني وفني من دولها ممثلة في أجهزتها الإستخباراتية (تمثل المؤسسات الأمريكية النموذج الأمثل)، وعلاوة على الأفراد والمؤسسات، برزت الجماعات الإجرامية المنظمة كأحد الفواعل الدولية الممارسة للتجسس الإلكتروني؛ إذ تشكل المتاجرة بالمعلومات السرية خاصة الاقتصادية منها مصدراً مغر آخر لجمع الثروة، كما نلاحظ أن التجسس الإلكتروني أصبح أحد أهم الأساليب والتقنيات المستخدمة من طرف الجماعات الإرهابية لأجل توفير المعلومات الإستراتيجية لبناء خطط الإعتداءات وتهديد البُنى التحتية الحيوية للدول ونشر الرعب في شعوبها. كل هذه الفواعل التقليدية منها (الدول)، أو الجديدة (أفراد، مؤسسات، جماعات الجريمة المنظمة، جماعات الإرهاب الإلكتروني)، وجدت في التجسس الإلكتروني ضالتها لتحقيق أهدافها بمختلف أبعادها، مدفوعة بمجموعة من الامتيازات التي يوفرها، كتقليص الجهد وخفض التكلفة وربح الوقت، وتجاوز عقبة الإقليمية، مستغلة إتجاه الدول والمؤسسات لتخزين أسرارها على هيئة رقمية، وتبني الدول لأسلوب الحكومة الإلكترونية كبديل للكلاسيكية.

كل المعطيات السالف ذكرها تشير وتبين التهديد الذي يشكله التجسس الإلكتروني على أمن الدولة الخارجي، وعلى الأفراد كوحدة أساسية ومركزية في مفهوم أمن الدولة الحديث؛ مما دفع الدول إلى تكثيف جهودها للتصدي لهذه الظاهرة المستحدثة من خلال رصد جملة من آليات المكافحة وإن تباينت في فعاليتها بتدرج مستويات ونطاق تطبيقها (المستوى الوطني، المستوى الإقليمي، المستوى الدولي)؛ وبناءً على ما تقدم جاءت فكرة البحث في هذا الموضوع والموسوم بـــ "آليات مكافحة التجسس الإلكتروني".

ثانيـــاً- أهميـــــة الموضـــــوع: تظهر أهمية موضوع "آليات مكافحة التجسس الإلكتروني" في عدة أوجه يمكن إيجازها فيما يلي:

1- المكانة المحورية التي تحتلها التقنيات الحديثة حالياً؛ إذ تعتمد الدول كما الأفراد عليها في ممارسة كافة الأنشطة بمختلف مستويات تعقيدها، حتى أن الدول أضحت تخزن بياناتها وأسرارها القومية في شكل رقمي على وسائط تخزين إلكترونية تَسهُل استعادتها ونقلها ومعالجتها آلياً.

2 – تظهر أهمية الموضوع من خلال التشابك الموجود فيه؛ بحيث أن التجسس الإلكتروني يُعد جريمة ماسة بأمن الدولة من جهة، وجريمة إلكترونية من جهة أخرى؛ وعليه فهو يجمع بين الأهمية التي يطرحها كلا الموضوعين السابقين مع الأخذ بعين الإعتبار جدتهما وحداثتهما.

3- يعالج موضوع التجسس الإلكتروني جملة من المسائل التي تعبر عن تأثر القوانين العقابية بإفرازات الثورة التكنولوجية والانتقال إلى العصر الرقمي، خاصة ما يتعلق منها ببروز أنماط إجرامية مستحدثة ومعقدة ومرتبطة ببعضها البعض، وما يستتبع ذلك من ضرورة مسايرة هذه التطورات عن طريق ضبط قواعد التجريم والعقاب من جهة، وتقرير قواعد إجرائية خاصة من جهة ثانية.

4- الآثار السلبية العميقة التي يرتبها التجسس الإلكتروني، سواء على الدول من خلال المساس بأمنها الخارجي، وتهديد سلامة فضائها الإلكتروني، وسلامة بُناها التحتية الحيوية، وكذلك تهديم وتجاوز المفهوم التقليدي للسيادة؛ أو على الأفراد من خلال المساس أساساً بحقهم في الحياة الخاصة، وهو الحق المكفول دستورياً والمحمي وطنياً ودولياً، وهذا بشكل مُمنهج وتحت غطاء قانوني وتبريرات متعددة.

5- تميز التجسس الإلكتروني عن التجسس التقليدي، سواء من حيث وسائل ممارسته التي تتسم بالتنوع والاتساع لدرجة أنها تستعصي على التعداد والحصر، الأمر الذي يرجع إلى التطور السريع للتكنولوجيات الحديثة، بحيث لا يكاد الفرد يستوعب تقنية معينة حتى يفاجأ بظهور أخرى؛ أو من حيث مرتكبيه؛ إذ يلاحظ بروز مفهوم الجاسوس الإلكتروني الذي تجاوز من حيث المواصفات والأدوار تلك المقررة للجاسوس التقليدي باعتباره عميلاً وفياً في أغلب الحالات لدولته التي يربطه بها واجب الولاء والشعور بالانتماء، إذ أضحى هذا المجرم الإلكتروني فاعلاً ضمن مجموعة فواعل جديدة تضاف إلى الدولة باعتبارها الممارس التقليدي والوحيد للتجسس، فأصبح الفرد الذي يمتلك بعض التفوق الذهني والمعارف التقنية يخترق ويتجسس على أسرار الدفاع الوطني الإلكترونية للدول الأخرى وهذا لحسابه

الخاص وبغض النظر عن الدوافع، بالإضافة إلى استخدام كل من المؤسسات، وجماعات الجريمة المنظمة، وكذا منظمات الإرهاب الإلكتروني، لتقنيات التجسس الإلكتروني إما للحصول على ذات الأسرار بغية إستغلالها في تطوير نشاطات معينة، أو تحقيق الهيمنة كما هو الحال بالنسبة للمؤسسات الاقتصادية، أو التربح من خلال المتاجرة بها كما هو الحال بالنسبة لجماعات الجريمة المنظمة، أو استخدامها في الاعتداء على الدول ونشر الخوف كما هو الحال بالنسبة لمنظمات الإرهاب الإلكتروني.

6- الطبيعة الخاصة وإن أمكن القول المتناقضة للتجسس الإلكتروني؛ إذ يُعد سلوكاً مشروعاً وغير مشروع في ذات الوقت؛ فكل الدول تمارسه وإن لطفت من حدة المصطلح مستخدمة لفظ الإستخبار، وكل الدول تنشئ وبواسطة قوانين أجهزة خاصة للقيام به، وتسوق في هذا الإطار عديد الحجج والمبررات، على رأسها حفظ أمنها، وممارسة حقها في البقاء واستباق الأخطار التي تهددها ومنها تلك التي يشكلها الإرهاب، أو جماعات الجريمة المنظمة، أو السباق نحو التسلح، لكنها في ذات الوقت تعتبر التجسس ماساً بسيادتها وتعده جريمة خطيرة إن استهدفها وترتب عليه أقصى العقوبات في قوانينها الداخلية.

7- تظهر أهمية موضوع التجسس الإلكتروني في غزارة محتواه وثراء المصطلحات التي يقوم عليها، وكذا في ارتباطه بالعديد من القوانين والعلوم الأخرى؛ إذ يجد امتداده بالإضافة إلى قانون العقوبات، وقانون الإجراءات الجزائية، في قوانين متمايزة عن بعضها إن في المحتوى أو في مجال التطبيق، كالقانون الدولي الإنساني، وقانون الفضاء الخارجي، والقانون الدولي الدبلوماسي، وغيرها، كما يُعد أحد الموضوعات ذات الصلة الوثيقة بالعلوم السياسية والعلاقات الدولية.

ثالثـــاً- أسبـــاب إختيـــار الموضـــوع: يرجع إختيار دراسة موضوع "آليات مكافحة التجسس الإلكتروني" إلى عدة أسباب منها ما هو شخصي، ومنها ما هو موضوعي:

1- الأسبـاب الشخصيـة لإختيـار الموضـوع: تتمثل في:

أ- الرغبة في دراسة الموضوع، خاصة بعد الإطلاع على بعض المؤلفات التي تناولت الجرائم الماسة بأمن الدولة بصفة عامة، ومنها على وجه التحديد جريمة التجسس، بالإضافة إلى تلك التي تناولت الجرائم الإلكترونية.

ب- الإسهام ولو بشكل متواضع في إضافة دراسة للمكتبة القانونية،؛ خاصة في ظل ندرة إن لم أقل انعدام المراجع التي تناولت موضوع التجسس الإلكتروني.

2- الأسبـــاب الموضوعيـــة لإختيـــار الموضـــوع: تتمثل في:

أ- الأهمية البالغة التي يحضى بها مفهوم الأمن الخارجي للدولة؛ إذ يعد أحد أهم الأولويات الأساسية التي تسعى كل دولة لتأمينها وحفظها من شتى أشكال التهديدات التي يمكن أن تعترضها، وذلك برصد كافة الجهود لتحقيق هذه الغاية.

ب- مساس التجسس الإلكتروني ليس فقط بأمن الدولة الخارجي، إنما تجاوز أثره غاية تعريض الحياة الخاصة للأفراد للانكشاف، فميزة إستئثار الشخص بحياته الخاصة وحفظها بعيداً عن الآخرين لم تعد تحض بذلك الاحترام في ظل الانتهاك المتزايد لها بواسطة التجهيزات الحديثة ومختلف التطبيقات التي توفرها: من هواتف وأنترنت وأقمار صناعية.

رابعـــاً- الدراســـات السابقـــــة: نظراً لجدة الموضوع فإن الدراسات الأكاديمية بشأنه قليلة جداً، والمتوفر منها إما أنه يتناول التجسس في شكله التقليدي فقط، أو أنه يحصر مجال الدراسة في جانب محدد لا غير، وأهم هذه الدراسات ما يلي:

1- رسالة دكتوراه موسومة بـ "الحماية الجنائية لأسرار الدفاع في مواجهة التقدم التكنولوجي الحديث" للباحث عماد الدين محمد كامل الجمل، حيث تناول موضوع دراسته من خلال بابين، قام بالتقديم لهما بباب تمهيدي بعنوان "الأحكام العامة لجرائم إنتهاك أسرار الدفاع النووية"، وتطرق الباب الأول من الدراسة إلى "الحماية الوقائية لأسرار الدفاع النووية"، أما الباب الثاني فتناول "جرائم إنتهاك أسرار الدفاع النووية"، ورغم إقتصار الدراسة على الأسرار النووية دون غيرها -وهو ما لا يعكسه العنوان المفتوح للمذكرة- إلا أن الباحث برر هذا التخصيص بأهمية طائفة أسرار الدفاع النووية والتي تأتي حسبه على رأس قائمة أسرار الدفاع المتجسس عليها بإستخدام أجهزة التجسس الحديثة؛ ليتخذ بذلك من هذا الصنف من الأسرار مثالاً تطبيقياً يسقط عليه الأحكام العامة التي تحكم جرائم التجسس في قانون العقوبات.

2- رسالة دكتوراه موسومة بـ "الجرائم المضرة بأمن الدولة عبر الأنترنت" للباحث محمد محمد صالح الألفي، حيث تناول موضوع دراسته من خلال بابين، قام بالتقديم لهما بفصل تمهيدي بعنوان "أثر التقدم العلمي وثورة الاتصالات على حركة جرائم أمن الدولة"، وتطرق الباب الأول من الدراسة إلى "النظام

القانوني لجرائم أمن الدولة عبر الانترنت"، أما الباب الثاني فتناول "الأحكام العامة لجرائم أمن الدولة عبر الانترنت"، وما يمكن ملاحظته على هذه الدراسة إقتصارها فقط على جريمة الإرهاب الإلكتروني والإرهاب التقليدي، وهو ما لا يعكسه لا عنوان الرسالة، ولا عناوين الأبواب، كما أنه ربط في كثير من المواضع الإرهاب الالكتروني بالتجسس الإلكتروني رغم ذاتية كل منهما المستقلة.

3- رسالة دكتوراه موسومة بـ "النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن" للباحث محمود سليمان موسى، حيث تناول موضوع دراسته من خلال قسمين، قدم لهما بباب تمهيدي بعنوان "جرائم التجسس عبر العصور"، وتطرق القسم الأول من الدراسة إلى "تحليل الفكرة العامة للتجسس الدولي" من خلال بابين، تناول الباب الأول "ماهية التجسس الدولي"، والباب الثاني "المحل القانوني للتجسس الدولي"، وتطرق القسم الثاني من الدراسة إلى "نطاق التجسس وأحكامه" من خلال بابين كذلك، تناول الباب الأول "صور التجسس في قانون العقوبات الليبي المقارن"، والباب الثاني "أحكام التجسس"، وتعد هذه الدراسة أكثر الدراسات شمولاً لموضوع التجسس؛ بحيث تناولت بالطرح والشرح كل الجزئيات المتصلة به، إلا أنها لم تتناول النمط المستحدث من التجسس ألا وهو التجسس الإلكتروني.

4- رسالة دكتوراه موسومة بـــ "جرائم الانترنت" للباحثة هبة نبيلة هروال، حيث تناولت موضوع دراستها من خلال ثلاثة أبواب، قدمت لها بفصل تمهيدي بعنوان "ماهية جرائم الانترنت"، وتطرق الباب الأول من الدراسة إلى "جرائم الاعتداء على الأشخاص عبر الأنترنت"، وتطرق الباب الثاني إلى "جرائم الإعتداء على الأموال عبر الانترنت"، وتطرق الباب الثالث إلى "جرائم العدوان على أمن الدولة عبر الانترنت"، حيث خصصت الباحثة الفصل الأول منه لدراسة "الإرهاب عبر الانترنت"، بينما أفردت الفصل الثاني لـ "التجسس عبر الانترنت"، وقد تميزت هذه الدراسة بإحاطتها بكافة صور جرائم الانترنت حتى الماسة منها بأمن الدولة وتحديداً جريمة التجسس الإلكتروني.

خامســاً- أهـــداف الدراســـة: ترمي هذه الدراسة إلى تحقيق عدة أهداف، يمكن إيجازها في العناصر التالية:

1- الإجابة عن إشكالية البحث، وتساؤلاته الفرعية.

2- إستخلاص أهم الفروق الموجودة بين الشكل التقليدي للتجسس، والشكل المستحدث منه أي التجسس الإلكتروني، من خلال مقابلة جميع العناصر المكونة لكليهما ببعضها.

3- عرض جهود مكافحة التجسس الإلكتروني سواء الوطنية أو الإقليمية أو الدولية.

4- محاولة تقييم فعالية الجهود الوطنية والإقليمية والدولية لمكافحة التجسس الإلكتروني في الحد منه، وتوفير الحماية لأسرار الدفاع الوطني من شتى الاعتداءات الإلكترونية.

سادساً- صعوبـــات الدراســـــة: يمكن إيجاز الصعوبات المواجهة في سبيل إعداد هذا البحث في العناصر التالية:

1- تظهر صعوبة دراسة التجسس الإلكتروني في تجاوزه للأطر القديمة التي تحكم التجسس التقليدي خاصة من حيث صياغة نصوص التجريم؛ بحيث وإن اِعتُبِر التجسس الإلكتروني شكلاً من أشكال التجسس عامة، إلا أنه يُفلت من دائرة النصوص التجريمية القديمة في عديد الحالات، فلا يمكن مثلا تطبيق نص الإتلاف الذي يقع على الأشياء ذات الطبيعة المادية على الإتلاف الإلكتروني الذي يقع على المحتوى المعلوماتي الذي يُعد ذا طبيعة معنوية، ولا النص الذي يجرم الدخول المادي للأماكن المحظورة على فعل الاختراق الإلكتروني مثلاً.

2- تظهر صعوبة دراسة التجسس الإلكتروني بالإضافة إلى ما تم عرضه في العنصر السابق، في التداخل الكبير بين مفهوم التجسس التقليدي والتجسس الإلكتروني؛ بحيث يطرح هذا التداخل إشكالية أي النصين يطبق: النص التقليدي أم النص المستحدث؟ وذلك بالنظر لعدة اعتبارات أهمها أن النص التقليدي يُعد المرجعية التي تحكم التجسس بصفة عامة بغض النظر عن صوره والدليل عدم استغناء المشرع عنه أو تعديله، وكذلك بالنظر إلى خصائص صياغة النصوص التجريمية المتعلقة بأمن الدولة التي تعتمد على مصطلحات مرنة ومطاطة يمكن أن تستوعب الصور الجديدة منها؛ أما النص المستحدث المتعلق بتجريم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات فينص صراحةً على حالة الاعتداء على الدفاع الوطني، مما يتطلب تناول النصين بالدراسة والتحليل والمقابلة لتحديد الحالات التي يشملها كل منهما.

3- إزدواجية نظرة وتعامل الدولة الواحدة مع موضوع التجسس الإلكتروني؛ فبينما تبرر الدولة سلوكها بممارسته بحقها في حفظ أمنها والتحوط لإعتداءات محتملة سواء كانت إرهابية أو من طرف جماعات الجريمة المنظمة، أو غير ذلك، تقوم ذات الدولة بتجريم أفعال التجسس التي تطالها وتخصص لها أقصى العقوبات، وقد تفردها بقضاء خاص؛ مما يجعل من محاولة وضع إطار تعاون دولي صريح

ومباشر للتصدي للتجسس الإلكتروني أمرا مستبعداً، بل العكس هو الملاحظ في الممارسة الدولية بحيث يتم الوقوف على عديد مشاريع وأنظمة تعاون دولي غرضها التجسس الإلكتروني.

4- إبهام وغموض المصطلح التقني الذي يحكم الجريمة الإلكترونية عامة ومنها التجسس الإلكتروني؛ فالثورة التكنولوجية أفرزت ثروة على مستوى المصطلح لم تحض بالاهتمام المطلوب من حيث الشرح أو تعميم دراستها خاصة في الجامعات؛ ما يؤدي في مجال القانون الجزائي للمساس بأهم مبادئه: مبدأ المشروعية، هذا من جهة، ومن جهة أخرى نلحظ الخلط الموجود على مستوى المصطلحات، فالبعض يستخدم لفظ "التجسس الإلكتروني" للتعبير عن المساس بخصوصية الأفراد رغم أنه في الأصل دال على طائفة من الجرائم الماسة بأمن الدولة، مع ضرورة ملاحظة أن المساس بخصوصية الأفراد قد يُشكل في ظروف معينة صورة من صور التجسس الإلكتروني الرامي إلى المساس بأمن الدولة.

5- جدة موضوع التجسس الإلكتروني وحداثته، وفي المقابل ندرة المراجع التي تتناوله خاصة على المستوى الوطني، بحيث لا يوجد حتى مجرد تأصيل مفاهيمي له، والمتوفر من المراجع يتناول التجسس إما في صورته التقليدية (على قلتها أيضاً في هذا الجانب)، أو يتناول التجسس الإلكتروني كجزئية بسيطة جداً ضمن الجرائم الإلكترونية لا تعدو كونها إعادة سرد لوقائع وقصص تناولتها صفحات الجرائد أو وكالات الإخبار، مما حتم محاولة توظيف واستغلال ما تم جمعه، وكذا الاجتهاد في الربط بين المعلومات المتوفرة .

سابعـــاً- إشكاليـــــة الموضـــــوع:

أدت التسهيلات التي أفرزتها منتجات الثورة التكنولوجية، وكذا تحسينها لنمط تسيير الدولة وعلاقتها مع الأفراد، وترقيتها لنوعية حياتهم؛ إلى تعميم استخدام التقنيات والوسائط الإلكترونية وزيادة الاعتماد عليها والتبعية لها وربط شتى قطاعات الدولة بها حتى الحساسة منها، وبرغم الامتيازات التي يوفرها هذا الربط للدولة فقد منح بالموازاة مع ذلك فرصاً لعديد الأطراف لاستخدامه للمساس بأمنها الخارجي وبأسرار دفاعها الوطني، وهذا عن طريق نمط مستحدث من التجسس هو التجسس الإلكتروني، وفي ظل إدراك الدول لخطورة هذا السلوك وآثاره الملموسة على عديد المستويات؛ فقد سعت إلى رصد جملة من الآليات لمكافحته، وهو ما يدفع لطرح الإشكالية التالية:

ما مدى فعالية الآليات الوطنية والإقليمية والدولية في مكافحة التجسس الإلكتروني، في ظل إزدواجية نظرة وتعامل الدولة الواحدة مع التجسس الإلكتروني من جهة، وتأثير التباين في أهمية مستويات الأمن (أمن وطني – أمن إقليمي– أمن دولي) من جهة أخرى؟.

تندرج تحت هذه الإشكالية الرئيسية التساؤلات الفرعية التالية:

1– ما المقصود بالتجسس الإلكتروني كجريمة ماسة بأمن الدولة الخارجي في ظل المعطيات الجديدة للفضاء الالكتروني؟.

2– ما هي الجهود المرصودة لمكافحة التجسس الإلكتروني سواء على المستوى الوطني، أو المستوى الإقليمي، أو المستوى الدولي؟.

ثامنـــاً– منهـــج البحـــث فـي الموضـــوع:

بهدف الإجابة على إشكالية الدراسة، وعلى تساؤلاتها الفرعية، تم الاعتماد أساساً على المنهج الاستقرائي، وذلك من خلال محاولة تجميع الأحكام الجزئية التي توفرها المادة القانونية سواء الوطنية أو الدولية؛ بغية الخروج بمبادئ عامة تحكم التجسس الإلكتروني، كما تمت الاستعانة بكل من المنهج الوصفي التحليلي، وهذا لتوضيح عناصر مفهوم التجسس الإلكتروني، وتحليل آليات مكافحته سواء الوطنية (في شقيها الموضوعي والإجرائي)، أو الإقليمية أو الدولية؛ وبالمنهج التاريخي لأجل عرض المراحل التي مر بها التجسس ليظهر بشكله الحالي؛ وبالمنهج المقارن في تحديد المفاهيم الأساسية للموضوع، وعرض موقف باقي التشريعات من التجسس الإلكتروني، والمقابلة بين الجهود الوطنية وتلك الدولية المرصودة لمكافحته، وكذلك لإجراء مقابلة بين عناصر التجسس التقليدي والتجسس الإلكتروني سواء من حيث التعريف أو الخصائص أو المحل أو التجريم والعقاب.

تاسعـــاً– خطـــة البحـــث فـي الموضـــوع:

من أجل الإجابة على الإشكالية الرئيسية ومجموع التساؤلات الفرعية السابق إثارتها، سيتم تناول موضوع "آليات مكافحة التجسس الإلكتروني" وفقاً لخطة ثنائية تتضمن بابين كالآتي:

- **البـــــاب الأول:** بعنوان "ماهية التجسس الإلكتروني"، وفيه سيتم تناول العناصر التي تكون الإطار التأصيلي والمفاهيمي لفكرة التجسس الإلكتروني، وهذا من خلال تقسيمه إلى فصلين، يُخصص الفصل الأول لمفهوم التجسس الإلكتروني، بينما يُخصص الفصل الثاني لمحل التجسس الإلكتروني.

- **البـــــاب الثاني:** بعنوان "الجهود الوطنية والجهود الدولية لمكافحة التجسس الإلكتروني"، وفيه ستتم محاولة تحليل ومناقشة جهود مكافحة التجسس الإلكتروني، وهذا من خلال تقسيمه إلى فصلين، يُخصص الفصل الأول للجهود الوطنية لمكافحة التجسس الإلكتروني، بينما يُخصص الفصل الثاني للجهود الدولية لمكافحة التجسس الإلكتروني.

وقد انتهى البحث إلى خاتمة، سيتم من خلالها عرض نتائج الدراسة، وتوصياتها.

البـــاب الأول: ماهيـــة التـــجسس الإلكترونـــــي.

الفصـــل الأول: مفهوم التـــجسس الإلكترونـــــي.

الفصـــل الثاني: محـل التـــجسس الإلكترونـــــي.

البـــــاب الأول:

ماهيـــــة التجـــسس الإلكترونـــي

شهدت البشرية في سياق تطورها ثورات ثلاث: الثورة الزراعية، والثورة الصناعية، والثورة المعلوماتية، لتشكل هذه الأخيرة القائمة أساسا على الحواسيب الآلية وشبكات الاتصالات، والموصوفة بالموجة التطورية الثالثة؛ أهم محطات هذا التطور على الإطلاق، ليس فقط لكونها حسنت نوعية حياة الإفراد بشكل ملفت، وفتحت أفاقاً جديدة أمام الدول من خلال استخدام عناصرها في تحقيق التنمية بكل أبعادها وبأقل التكاليف وباختزال للوقت والجهد مما انعكس نهايةً بالإيجاب على العلاقة بين هذه الدول وشعوبها –وهو مبتغى كل سياسة مرسومة من طرفها– بل لكونها رسمت حدود عالم آخر افتراضي مواز للعالم الحقيقي الذي يمارس فيه الأفراد والدول تعاملاتهم المادية، إصطلح على تسميته بالفضاء الإلكتروني، تم نقل مختلف جوانب حياة هذه الأطراف إليه، وكما جعله الأفراد مكانا يحتفظون فيه بكل ما يتعلق بحياتهم الخاصة فعلت الدول ذات الأمر؛ إذ أصبحت تخزن أسرار دفاعها الوطني بهيئة رقمية وتتخذ من الوسائط الإلكترونية التي وفرتها التكنولوجيات الحديثة وسائل لمعالجة هذه الأسرار، ونظراً لكون هذه الأخيرة ثروة إستراتيجية لطالما سعت الدول الأخرى للحصول عليها لاعتبارات مختلفة، وذلك عن طريق التجسس عليها؛ فقد استتبع تحول هذه الأسرار إلى هيئة إلكترونية وظهور ما يمكن تسميته بسر الدفاع الوطني الإلكتروني، تحول مواز في طبيعة هذا التجسس؛ إذ أصبحنا أمام مفهوم مستحدث هو التجسس الإلكتروني، هذا الأخير يطرح عديد الإشكاليات المتعلقة أساساً بمدلوله؛ إذ يعد أكثر المصطلحات المعاصرة غموضاً بالنظر للخلط الواقع بينه وبين غيره من المصطلحات، أو لاستعماله للدلالة على مفاهيم أخرى، وكذا بالنظر لصعوبة تحديد ماهية التجسس التقليدي أساساً، ولغموض واتساع نطاق فكرة أمن الدولة عموماً، يضاف لهذا، الثورة المشهودة على مستوى المصطلح إذ للعصر الإلكتروني مصطلحاته الخاصة التي تشكل ماهيته وأهم سماته؛ فأصبحت بذلك مسألة الإحاطة بمدلول التجسس الإلكتروني ضرورة محورية لتحديد سبل مواجهته؛ وعليه سيتم الإلمام بماهية التجسس الإلكتروني من خلال تقسيم هذا الباب إلى فصلين، يتناول الفصل الأول مفهوم التجسس الإلكتروني، ويتناول الفصل الثاني محل التجسس الإلكتروني.

الفصـــل الأول:

مفهـــوم التجـــسس الإلكترونـــي.

إن ارتباط كافة مناحي الحياة بالتكنولوجيا الحديثة من أبسط مظاهرها إلى أعقدها؛ جعل من كل الأنشطة التي كانت تمارس سابقاً بطريقة ملموسة وبنمط تفاعلي تصبح باستخدام الوسائط الإلكترونية معاملات رقمية لا مادية. هذه التبعية الشبه مطلقة أدت إلى بروز تهديدات جديدة ومتعددة الأبعاد تواجه الأفراد والدول على الخصوص؛ بحيث برغم ما قدمته هذه التكنولوجيات من خدمات للمجتمع فقد منحت بالموازاة مع ذلك تقنيات تتطور باستمرار، وفرصاً متعددة لأطراف مختلفة لاستخدامها في المساس بحقوق الدول الأخرى على رأسها الحق في الأمن الخارجي والحق في السيادة، وذلك عن طريق توظيف الوسائط الإلكترونية للوصول إلى أسرار دفاعها الوطني بواسطة التجسس الالكتروني، هذا الأخير الذي يعد أحد المفاهيم المستحدثة التي تفرض وجوب التصدي لتحليلها وتبيان كافة العناصر التي تشكل مدلولها؛ ولهذا الغرض سيتم تقسيم هذا الفصل إلى ثلاثة مباحث: يتناول المبحث الأول تعريف التجسس الإلكتروني وخصائصه، ويتناول المبحث الثاني التطور التاريخي للتجسس الإلكتروني، بينما يتناول المبحث الثالث صور التجسس الإلكتروني وأبعاده.

المبحـــث الأول: تعريف التجـــسس الإلكتروني وخصائصـــه.

تتطلب الإحاطة بمصطلح التجسس الإلكتروني منعاً لاختلاطه ووضعاً لحدود التمايز بينه وغيره من المصطلحات؛ ضرورة تعريفه، وتبيان مجموع الخصائص التي تميزه وتأسس لذاتيته الخاصة واستقلاله عن مصطلح التجسس التقليدي؛ وعليه سيتم تقسيم هذا المبحث إلى مطلبين: يتناول المطلب الأول تعريف التجسس الإلكتروني، ويتناول المطلب الثاني خصائص التجسس الإلكتروني.

المطـــلب الأول: تعريـــف التجـــسس الإلكترونـــي.

صاحب التطور العلمي وانتشار استخدام تكنولوجيات المعلومات والاتصالات، ظهور مجموعة مصطلحات مستحدثة، ورغم كون الأمر جد طبيعي إذ لكل مرحلة تاريخية مصطلحاتها المميزة خاصة إذا كانت سمة هذه المرحلة التطور على مستوى التقنية، فبالمقابل يصبح التصدي لضبط مفهوم هذه المصطلحات أمراً حتمياً خاصة بالنسبة لميدان القانون الجزائي، وفي هذا الإطار وبغية التوصل إلى تعريف التجسس الإلكتروني يستوجب الرجوع بدايةً إلى الأصل اللغوي لمصطلح التجسس الإلكتروني،

ومن ثم التطرق إلى تعريفه القانوني والفقهي؛ وعليه سيتم تقسيم هذا المطلب إلى فرعين: يتناول الفرع الأول التعريف اللغوي للتجسس الإلكتروني، ويتناول الفرع الثاني التعريف القانوني والفقهي للتجسس الإلكتروني.

الفـــرع الأول: التعريـــف اللغـــوي للتجـــسس الإلكترونـــي.

يتكون مصطلح التجسس الإلكتروني من كلمتين: كلمة "التجسس"، وكلمة "إلكتروني"، وسيُعرض معنى كل منهما في الآتي:

أولاً- المعنـى اللغـــوي لكلمـــة "تجـــسس":

يقصد بالتجسس في اللغة: البحث عن الخبر واستطلاعه[1]. وقيل التجَسُّسُ التفتيش عن بواطن الأمور، وهو بالجيم طلب الشخص الخبر للغير، وبالحاء طلبه لنفسه[2]. كما قيل تجسّس الخبر تفحصه بطريقة غير مشروعة، ومنه إشتُقت كلمة جاسوس، وهو من يقوم بجمع معلومات سرية لجهة معينة، أما الجاسوسية فهي مصدر صناعي من جاسوس، وتعني مهارة جمع المعلومات عن شخص أو جهة أو نحوهما، لصالح فرد أو جهة أخرى معادية[3].

ثانياً- المعنـى اللغـوي والعلمـي لكلمـة "إلكترونـــي":

بالرجوع إلى مجموعة من المراجع اللغوية الأجنبية بحثاً عن المقصود بلفظ "إلكتروني"؛ نجد أنها تعرفه دوماً بالاستناد إلى أصله من حيث كونه كلمة علمية وتقنية بحتة؛ حيث اشتُقت من كلمة "إلكترون"، والذي يرمز إلى جزيئة متناهية الصغر تدور حول نواة الذرة وتحمل شحنة كهربائية سالبة، وتعد الإلكترونات أحد مكونات المادة[4]، ونسبة إليها نجد ميدان الإلكترونيك وهو فرع من التقنية التي تدرس وتستخدم تنوع المجال الإلكتروني(المجال الإلكترومغناطيسي، المجال الكهربائي...) من أجل

---

[1]- يوسف محمد رضا، معجم العربية الكلاسيكية والمعاصرة، مكتبة لبنان ناشرون، لبنان، 2006، ص. 469.

[2]- أبي الفضل جمال الدين محمد بن مكرم ابن منظور الإفريقي المصري، لسان العرب، المجلد الثالث، ط 4، دار صادر للطباعة والنشر، لبنان، 2005، ص. 147.

[3]- أحمد مختار عمر، معجم اللغة العربية المعاصرة، عالم الكتب للنشر والتوزيع والطباعة، مصر، 2008، ص. 374.

[4]- Alain Rey, Le ROBERT MICRO, Dictionnaire De la langue française,3eme edition, Paris, 1998, p.441.

إلتقاط، ونقل، وإستغلال وإستخدام المعلومة، وقد اتسع ليشمل حالياً تقنيات متعددة أبرزها الحواسيب والاتصالات ومعالجة الإشارة وكذا الأتمتة...[1].

وفي سبيل البحث عن صلة بين المفهوم العلمي للفظ "إلكتروني" السابق طرحه وبين ما يرمي إليه المشرع حين إستخدامه لذات اللفظ؛ تم الإطلاع على مجموعة من القوانين بحثا عن تعريفه، وقد سبقت الإشارة إلى أن الثورة التكنولوجية أدت إلى حدوث ثورة موازية على مستوى المصطلحات، وكـــان لزاماً على المشرع في الحقل القانوني أن يقوم بتوضيح معناها بشكل يرفع اللبس عنها، ويحفظ مبدأ المشروعية الذي يستلزم وضوح المصطلحات فيما يخص النص الجنائي، وهذا ما حاول فعله؛ إذ نلحظ عند الإطلاع على القوانين التي تنظم الجوانب ذات الصلة بكل ما هو إلكتروني، تخصيص المشرع المواد الأولى منها دائما لاستعراض مجموعة من المصطلحات وشرحها، لكن الغالب منها لم يتناول بالتعريف لفظ "إلكتروني"، باستثناء ما ورد في قانون التجارة الإلكترونية بإمارة دبي والذي يحمل رقم 02 لسنة 2002؛ بحيث عرف لفظ "إلكتروني" في المادة الثانية منه بأنه: كل ما يتصل بالتكنولوجيا الحديثة وذو قدرات كهربائية أو رقمية أو مغناطيسية أو لاسلكية أو بصرية أو كهرومغناطيسية أو مؤتمتة[2] أو ضوئية أو ما شابه ذلك[3]، وبإجراء مقابلة بسيطة بين التعريفين نلحظ التطابق الموجود بينهما؛ ولعل هذا ما يفرضه العصر الحالي فهو عصر الآلة والتقنيات المتقدمة المحكومة بقوانين علمية دقيقة، وعلى المشرع أن يتبع الأصل بهذا الخصوص. وما يمكن ملاحظته أيضا على التعريف العلمي السابق صلته الواضحة كذلك بالمعنى المستخدم في المجال القانوني للدلالة على أنظمة المعالجة الآلية للمعطيات، والتي يتم من خلالها التعامل مع أسرار الدفاع الوطني للدول، إن إدخالاً، أو تخزينا، أو نقلا، أو تعديلاً، وغير ذلك من التصرفات التقنية، هذه الأنظمة التي تشكل الحواسيب أهم عنصر فيها وإن لم تكن أوحدها، وهو ما سيتم إرجاء دراسته إلى الفصل الثاني من هذا الباب.

---

[1]- Yves Garnier, LA ROUSSE Dictionnaire encyclopédique, France, 2001, p. 525.

[2]– كلمة أتمتة مستمدة من كلمة Automatisme، ويقصد بها تحويل العمليات الإدارية من عمليات ورقية إلى إجراءات إلكترونية تتم معالجتها إلكترونياً داخل الحاسب الآلي وملحقاته (ببساطة يقصد التحويل التلقائي)، أنظر: عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، مصر، 2009، ص. 43.

[3]– نفس المرجع، ص. 42.

الفـــرع الثانـــي: التعريف القانونـــي والفقهـــي للتجـــسس الإلكترونـــي.

يطرح تعريف التجسس الإلكتروني من الناحية القانونية والفقهية بعض الصعوبات؛ بالنظر إلى جدة المصطلح التي تضاف إلى عدم وجود إجماع أصلاً حول تعريف التجسس في صورته التقليدية؛ وعليه وجب التطرق ابتداءً إلى تعريف التجسس التقليدي ثم الانتقال إلى تعريف التجسس الحديث أو الإلكتروني، وهو ما سيتم عرضه في الآتي:

أولاً- تعريـف التجـسس التقليـدي:

سيتم بدايةً عرض موقف التشريعات من عملية تعريف التجسس، بمعنى بحث التعريف القانوني للتجسس، ومن ثم التطرق إلى التعريف الفقهي له، وذلك كالآتي:

أ- **التعريـف القانونـي للتجـسس التقليـدي:** القاعدة العامة في معظم التشريعات الداخلية للدول تتمثل في تفادي وضع تعريف جامع ومانع للتجسس لتترك ذات المهمة للفقه، لكن بالرجوع للاتفاقيات الدولية نجد أن إتفاقية لاهاي المتعلقة بقوانين وأعراف الحرب في البر قد تصدت لتبيان الشروط الواجب توافرها في الشخص الذي يقوم بجمع معلومات معينة ليوصف بوصف الجاسوس، ومنها يستنبط تعريف التجسس؛ حيث نصت على أنه: "لا يمكن أن يعتبر كجاسوس إلا الفرد الذي يعمل في الخفاء أو تحت ستار كاذب لجمع المعلومات أو محاولة جمع المعلومات في منطقة العمليات الحربية لإحدى الدول المتحاربة بنية إيصالها للطرف المعادي"[1]؛ وعليه لنكون أمام جريمة تجسس لابد من توافر الشروط الآتية:

- العمل في الخفاء أو تحت ستار كاذب بمعنى العمل بشكل سري أو باستخدام وسائل تتكرية.
- جمع المعلومات أو محاولة جمع المعلومات.
- أن يتم جمع المعلومات أو محاولة جمعها في منطقة العمليات الحربية لإحدى الدول المتحاربة.
- أن يتم جمع أو محاولة جمع المعلومات لمصلحة دولة معادية.

أما فيما يتعلق بموقف المشرع الجزائري فنجد أنه قد سلك مسلك بقية التشريعات الداخلية للدول الأخرى بحيث تفادى وضع تعريف للتجسس في نصوصه القانونية، واكتفى فقط بذكر الأفعال التي تشكل

[1]- المادة 29 من إتفاقية لاهاي المتعلقة بقوانين وأعراف الحرب في البر المؤرخة في 18 أكتوبر 1907، والتي دخلت حيز التطبيق في 26 جوان 1910.

في حال قيامها الركن المادي لجريمة التجسس[1]، كما اتجه إلى إقرار معيار الجنسية كفاصل بين ما يعتبر جريمة خيانة وبين ما يعتبر جريمة تجسس[2]؛ فذات الأفعال تُكيف على أساس أنها جريمة خيانة في حال ارتكابها من قبل جزائري، بينما تُكيف –باستثناء فعل حمل السلاح ضد الجزائر[3]– على أساس أنها جريمة تجسس في حال ارتكابها من قبل أجنبي، لكنه بالمقابل استثنى بصريح العبارة طائفة العسكريين والبحارة الذين يكونون في خدمة الجزائر من مجال إعمال هذا المعيار في بعض المواضع؛ إذ تكيف طائفة من الأفعال التي يقومون بها على أساس أنها خيانة شأنهم في ذلك شأن الجزائريين[4].

ويمكن تحديد الأفعال المعتبرة جريمة تجسس بحسب ترتيب ورودها في قانون العقوبات كالآتي:

1– أفعال التجـسس التي يقترفها الأجانب ماعدا العساكر أو البحارة الذين يكونون في خدمة الجزائر دون تحديد لوقت ارتكابها أكان وقت سلم أو حرب، وهي:

– القيام بالتخابر مع دولة أجنبية بقصد حملها على القيام بأعمال عدوانية ضد الجزائر أو تقديم الوسائل اللازمة لذلك سواء بتسهيل دخول القوات الأجنبية إلى الأرض الجزائرية أو بزعزعة ولاء القوات البرية أو البحرية أو الجوية أو بأية طريقة أخرى.

– تسليم قوات جزائرية أو أرض أو مدن أو حصون أو منشآت أو مراكز أو مخازن أو مستودعات حربية أو عتاد أو ذخائر أو مبان أو سفن أو مركبات للملاحة الجوية مملوكة للجزائر أو مخصصة للدفاع عنها إلى دولة أجنبية أو إلى عملائها.

---

[1] – تنص المادة 64 من قانون العقوبات على أنه: "يرتكب جريمة التجسس ويعاقب بالإعدام كل أجنبي يقوم بأحد الأفعال المنصوص عليها في الفقرات 2 و3 و4 من المادة 61 وفي المادتين 62 و63".

[2]– تم تبني معيار الجنسية كمعيار أساسي للتمييز بين جريمتي التجسس والخيانة في المادة 64 أعلاه وذلك من خلال ربطه بين جريمة التجسس وارتكابها من قبل أجنبي.

[3] – تم النص على فعل حمل السلاح ضد الجزائر في الفقرة الأولى من المادة 61 من نفس القانون.

[4] – ورد هذا الاستثناء في كل من المادتين 61 و62 من قانون العقوبات؛ بحيث تنص المادة 61 على أنه: "يرتكب جريمة الخيانة ويعاقب بالإعدام كل جزائري وكل عسكري أو بحار في خدمة الجزائر يقوم بأحد الأعمال الآتية..." بينما تنص المادة 62 على أنه: " يرتكب جريمة الخيانة ويعاقب بالإعدام كل جزائري وكل عسكري أو بحار في خدمة الجزائر يقوم في وقت الحرب بأحد الأعمال الآتية...".

– إتلاف أو إفساد سفينة أو سفن أو مركبات للملاحة الجوية أو عتاد أو مؤن أو مبان أو إنشاءات من أي نوع كانت وذلك بقصد الإضرار بالدفاع الوطني أو إدخال عيوب عليها أو التسبب في وقوع حادث وذلك تحقيقاً لنفس القصد[1].

2– أفعـال التجـسس التي يقترفها الأجانب ماعدا العساكر أو البحارة الذين يكونون في خدمة الجزائر مع حصر إرتكابها في وقت الحرب، وهي:

– تحريض العسكريين أو البحارة على الانضمام إلى دولة أجنبية أو تسهيل السبيل لهم إلى ذلك، والقيام بعمليات تجنيد لحساب دولة في حرب مع الجزائر.

– القيام بالتخابر مع دولة أجنبية أو مع أحد عملائها بقصد معاونة هذه الدولة في خططها ضد الجزائر.

– عرقلة مرور العتاد الحربي.

– المساهمة في مشروع لإضعاف الروح المعنوية للجيش أو للأمة يكون الغرض منه الإضرار بالدفاع الوطني مع علمه بذلك[2].

3– أفعـال التجـسس التي يقترفها كافة الأجانب دون استثناء، وهي:

– تسليم معلومات أو أشياء أو مستندات أو تصميمات يجب أن تحفظ تحت ستار من السرية لمصلحة الدفاع الوطني أو الإقتصاد الوطني إلى دولة أجنبية أو أحد عملائها على أية صورة ما وبأية وسيلة كانت.

– الإستحواذ بأية وسيلة كانت على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو إلى أحد عملائها.

– إتلاف مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد معاونة دولة أجنبية أو ترك الغير يتلفها[3].

---

[1] – المادة 61 من قانون العقوبات.

[2] – المادة 62 من نفس القانون.

[3] – المادة 63 من نفس القانون.

ب- التعـــريف الفقهـــي للتجـــسس التقليـــدي: بالنظر إلى عدم وجود تعريف قانوني للتجسس في معظم التشريعات فقد حاول الفقه التصدي لهذه العملية. وبالرجوع إلى المحاولات الفقهية في هذا الصدد نلحظ عدم وجود اتفاق على تعريف واحد للتجسس؛ ويعود هذا للطبيعة المتجددة لهذا السلوك، ويمكن الوقوف على ذلك من خلال جملة التعاريف التي ستعرض في الآتي مع تحليل، ومناقشة، وتقييم كل تعريف على حدة:

1- تعـريف الفقـــه الغربـــي للتجـــسس: من بين أهم التعاريف الممنوحة للتجسس في الفقه الغربي، التعاريف الآتية:

- يُعرِف الفقيه "روبير ديتوربيه" التجسس بأنه: "البحث عن أي نوع من المعلومات خفية عن دولة معينة بهدف إيصالها لدولة أجنبية وذلك بنية الإضرار بالدولة المتجسس عليها"[1].

ما يلاحظ على هذا التعريف أنه يوافق الفكرة التقليدية التي تعتبر التجسس أسلوباً خفياً لجمع المعلومات، وهي الفكرة التي تتماشى مع الطرح الوارد في المادة 29 من اتفاقية لاهاي المتعلقة بقوانين وأعراف الحرب على البر السابق الإشارة إليها أعلاه ، لكن السائد حالياً أن القانون يعاقب على الحصول على أسرار الدولة مهما كانت الوسيلة سراً أو علناً، كما أن الفقيه روبير ديتوربيه إشترط ضرورة أن يهدف الجاني إلى الإضرار بالدولة المتجسس عليها، وهو ليس بالشرط المطلق؛ إذ هناك حالات يكفي فيها الحصول أو تسليم المعلومات دون أن تكون هناك نية الإضرار ليقوم فعل التجسس، فالفاعل قد يهدف للحصول على المال لقاء تلك المعلومات فالقانون هنا لا يعتد بالنية.

- يُعرِف الفقيه "غارو" التجسس بأنه: "السعي الذي يقوم به الأجنبي لجمع الوثائق والمعلومات السرية حول الموارد العسكرية وتنظيمات الدولة الهجومية أو الدفاعية ووضعها السياسي أو الاقتصادي بقصد تسليم هذه الوثائق والمعلومات إلى حكومة أجنبية مجاناً أو لقاء منفعة مالية"[2].

ما يلاحظ على هذا التعريف أنه تجاوز فكرة الخفاء كصفة لازمة للتجسس، كما أنه قام بتعداد أصناف المعلومات السرية الخاضعة للحماية وقسمها إلى معلومات عسكرية ومعلومات سياسية ومعلومات

[1]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، دار المطبوعات الجامعية، مصر، 2014، ص. 92.

[2]- سعد إبراهيم الأعظمي، جرائم التجسس في التشريع العراقي، 1981، ص. 15.

إقتصادية، كما أضاف عنصراً آخر يعد ضرورياً لتعريف التجسس ولتمييزه عن الخيانة؛ إذ قصر ممارسة التجسس على الأجانب بمعنى أخذه بعيار الجنسية، وهو المعيار الغالب حاليا في التفرقة بين الفعلين.

– يُعرِف الفقيه "بيير هوغني" التجسس بأنه: "كل نشاط يقوم به أجنبي ويخدم به مشاريع أو مصالح أمة أجنبية"[1].

ما يلاحظ على هذا التعريف أنه لم يعد يحصر التجسس في أفعال البحث والتقصي عن الأسرار، بل تجاوزه ليشمل كل الأنشطة التي من شأنها أن تخدم دولة أجنبية، وهذا ما يتوافق مع التعداد الذي يضعه المشرعون لأفعال التجسس والتي تتجاوز مجرد البحث والتقصي، وهو ما يمكن ملاحظته في مواد قانون العقوبات الجزائري السابق ذكرها أعلاه. بالإضافة إلى أن هذا التعريف قد وسع بصورة ضمنية صور التجسس ومجالاته ليشمل كل ما من شأنه أن يخدم مشاريع أو مصالح أمة أجنبية سواء كان مجالاً عسكرياً أو إقتصادياً أو سياسياً بل يمكن أن يستوعب حتى الجانب الاجتماعي والثقافي للدولة –التي تمثل أحد أوجه محل التجسس في الوقت الحاضر– كما يلاحظ أيضا على ذات التعريف أنه حصر فئة مرتكبي التجسس على الأجانب متبنياً كالتعريف السابق معيار الجنسية للتفريق بين التجسس والخيانة. إلا أن ما يؤخذ على هذا التعريف؛ أنه جعل التجسس نشاط يتم بواسطته خدمة مشاريع أمة أجنبية رغم أنه قد يتم خدمة مشاريع دولة أجنبية بنشاطات لا تتضمن فعل تجسس.

2 – تـعريف الفقــه العربــي للتجـــسس: من بين أهم التعاريف الممنوحة للتجسس في الفقه العربي ما يلي:

– يُعرِف الدكتور "محمد الرافعي" التجسس بأنه: "النشاط المتضمن إفشاء الأسرار المتعلقة بتكوين الدولة وهيبتها واعتبارها و قوتها التي تحرص الدولة على إحاطتها بالكتمان وعدم العلم بها من قبل الدول المعادية"[2].

ما يؤخذ على هذا التعريف أنه حصر التجسس في فعل إفشاء الأسرار؛ إذ أن كل التشريعات ومنها الجزائري تعتبر الإتلاف وزعزعة الروح المعنوية للجيش وكذا الدخول إلى أماكن محظورة على الجمهور مثلا جرائم تجسس. كما أنه حصر فعل التسليم لمصلحة دولة معادية، وهو ما يجانب الصواب؛

[1]– محمد الفاضل، الجرائم الواقعة على أمن الدولة، ط 4، المطبعة الجديدة، سوريا، 1978، ص. 311.

[2]– أحمد محمد الرفاعي، الجرائم الواقعة على أمن الدولة، دار البشير للنشر والتوزيع، الأردن، 1990، ص.115.

إذ يُفهم من هذا التعريف جواز تسليم أسرار الدولة لدولة أخرى حليفة أو ليست في حالة عداء معها وهو ما لا يستقيم.

– يُعرِف الدكتور "مجدي محمود محب حافظ" التجسس بأنه: "سعي أي شخص أجنبي صـــوب الحصول على أسرار الدولة أو تسليمها لأية جهة خارجية متى كان ذلك يؤدي إلى الإضرار بمصلحة الدولة"[1].

ما يؤخذ على هذا التعريف أنه كسابقه حصر التجسس في فعلي السعي للحصول على أسرار الدولة، أو تسليمها رغم أن التجسس أشمل من هذين الفعلين ويصدق ما قيل سابقا في هذا المقام. كما أن هذا التعريف ورغم أنه تجاوز فكرة التسليم لدولة معادية بتوسيعه للجهة التي يمكن أن تستفيد من أسرار الدولة؛ إذ مدها لتشمل أية جهة أجنبية بدون تخصيص، إلا أنه اشترط أن يؤدي هذا التسليم إلى الإضرار بمصلحة الدولة وهذا مالا يمكن الجزم به؛ إذ لا يمكن تحديد الحالات التي قد يؤدي فيها تسليم سر الدولة لإضرار بها، والحالات التي لا يؤدي التسليم لذلك؛ فسر الدولة يجب حفظه بغض النظر عن أي ظرف خارجي.

– يُعرِف الدكتور "محمد سليمان موسى" التجسس بأنه: "كل نشاط يقوم به أجنبي يكون من شأنه انتهاك أو خرق قواعد المحافظة التي تحيط بالأسرار المتعلقة بالدفاع الوطني"[2].

يعد هذا التعريف أكثر التعاريف السابقة دقة لأنه تجاوز مآخذها من حيث:

– حصره فئة مرتكبي التجسس على الأجانب؛ وعنصر الجنسية هو مناط التفريق بين التجسس الخيانة، وهو المعيار الذي تبناه المشرع الجزائري كذلك في المادة 64 من قانون العقوبات.

– تجاوزه الفكرة القديمة التي تجعل الخفاء صفة لازمة للتجسس.

[1]– مجدي محمود محب حافظ، موسوعة جرائم الخيانة والتجسس في التشريع المصري والتشريعات العربية والتشريعات الأجنبية والشريعة الإسلامية، دار محمود للنشر والتوزيع، مصر، 2010، ص. 298.

[2]– محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، أطروحة دكتوراه، مقدمة لكلية الحقوق، جامعة الإسكندرية، مصر، 1997 ، ص. 112.

– عدم حصره أنواع الأسرار بالإضافة إلى عدم قيامه بتعدادها، بل وسع مجال النشاط ليشمل كل الأنشطة التي تمس بأسرار الدفاع الوطني سواء كانت أسرار عسكرية أم سياسية أم اقتصادية أم علمية أم اجتماعية.

– عدم حصره لنوع النشاط الماس بالدفاع الوطني في الحصول على الأسرار أو تسليمها فقط، الأمر الذي يتماشى مع ما هو منصوص عليه في القوانين العقابية وتلك التي تنظم أسرار الدفاع الوطني بالنسبة للدول التي تملك مثل هذه التشريعات، وكذا مع التطورات التي يمكن أن تحدث أو التعديلات التي يمكن أن تطرأ على القوانين المختلفة نتيجة تغير الظروف.

ثانيـاً– تعـريف التجـسس الإلكترونـي:

سيتم بداية عرض موقف التشريعات من عملية تعريف التجسس الإلكتروني، ومن ثم التطرق إلى التعريف الفقهي له بإتباع نفس منهج دراسة تعريف التجسس التقليدي.

أ– **التعـريف القانونـي للتجـسس الإلكترونـي:** بالرجوع إلى قانون العقوبات الجزائري نجد أن المشرع الجزائري لم يعرف التجسس الإلكتروني كما فعل بخصوص التجسس التقليدي–هو مذهب التشريعات الأخرى– ولكنه حاول مسايرة التطورات التقنية الحاصلة وذلك بنصه على تجريم التجسس الإلكتروني وتعداده لمجموعة الأفعال المكونة له من خلال تعديل قانون العقوبات في سنة 2004[1]، الذي استحداث القسم السابع مكرر المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات من الفصل الثالث المعنون بالجنايات والجنح ضد الأموال [2]، وهذا التجريم يستشف من قراءة المادة 394 مكرر3 التي تنص على: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد".

[1]– جاء هذا التعديل بموجب القانون رقم (04–15) المؤرخ في العاشر من نوفمبر سنة 2004.

[2]– حوى القسم السابع مكرر عند استحداثه ثمانية مواد وذلك من المادة 394 مكرر إلى غاية المادة 394 مكرر7، هذا القسم الذي عرف إضافة مادة جديدة هي المادة رقم 394 مكرر8 وذلك بموجب القانون رقم 16–02 المؤرخ في 19 يونيو سنة 2016 المتمم للقانون العقوبات؛ بحيث تنص المادة المستحدثة على العقوبات المقررة لمقدم خدمات الانترنت الذي رغم إعذاره من قبل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أو رغم صدور أمر أو حكم قضائي يلزمه بذلك لا يقوم بالتدخل الفوري لسحب أو تخزين المحتويات التي تشكل جريمة منصوص عليها قانونا أو لا يقوم بوضع الترتيبات التقنية لذلك، بحيث قررت له الحبس من سنة إلى ثلاث سنوات والغرامة من 2.000.000 دج إلى 10.000.000 دج أو إحدى هاتين العقوبتين فقط.

وباستقراء مواد القسم السابع مكرر أعلاه نستخلص مجموعة الأفعال التي تكون جريمة التجسس الإلكتروني إذا استهدفت الدفاع الوطني وهي:

– الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك[1].

– الدخول أو البقاء المؤدي إلى تخريب نظام اشتغال المنظومة[2].

– إدخال أو إزالة أو تعديل – بطريق الغش– المعطيات في نظام المعالجة الآلية[3].

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم[4].

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصلة من إحدى الجرائم المنصوص عليها في هذا القسم[5].

ب– التعريـــف الفقهـــي للتجـــسس الإلكترونـــي: يعد مصطلح التجسس الإلكتروني واحداً من أهم مصطلحات العصر الحالي، وأهم الآثار السلبية للثورة التكنولوجية على أمن الدولة الخارجي، ورغـــــم تداول هذا المصطلح وعلى نطاق واسع إلا أن مفهومه لا يزال مبهما؛ بداية نظراً لاستخدامه بشكل عام للتعبير عن انتهاك خصوصية الأفراد والدول على حد السواء، بالإضافة إلى ندرة الدراسات التي تصدت للتأصيل لهذه الظاهرة على الأقل من الناحية المفاهيمية، لكن رغم ذلك يمكن رصد بعض التعاريف التي منحت لمصطلح التجسس الإلكتروني مع مناقشة وتحليل كل تعريف على حدة، وهذا كالأتي:

[1]– الفقرة الأولى من المادة 394 مكرر من قانون العقوبات.

[2]– الفقرة الثالثة من المادة 394 مكرر من نفس القانون.

[3]– المادة 394 مكرر2 من نفس القانون.

[4]– البند الأول من المادة 394 مكرر2 من نفس القانون.

[5]– البند الثاني من المادة 394 مكرر من نفس القانون.

1- "التجسس الإلكتروني أو ما يطلق عليه أيضا التجسس المعلوماتي يتجسد فيما يلي:

- الاستحواذ بدون وجه مشروع وقانوني على معلومات ذات أهمية لاسيما فيما يتعلق بأمن الدولة.

- الاستحواذ بدون وجه مشروع وقانوني على أسرار التعامل التجاري والتقنية الصناعية بجميع صورها"[1].

ما يمكن ملاحظته على هذا التعريف أنه لم يقصر وسائل التجسس الإلكتروني فقط على الحواسيب بل وسع من دائرة التقنيات والوسائل الإلكترونية التي يكن استغلالها لهذا الغرض. كما أنه لم يحصر نوع المعلومات محل التجسس في تلك الأسرار العسكرية أي المفهوم التقليدي لأمن الدولة، ولكن مد هذا التعريف مداه ليشمل الأسرار التجارية والصناعية بتخصيصها الجزئية الثانية وبشكل مستقل عن باقي طوائف أسرار الدولة الأخرى وهو الإتجاه السائد حالياً؛ إذ تتجه غالبية الدول إلى تعظيم مكانة هذه الأسرار وجعل السر الاقتصادي أهم صور التجسس الإلكتروني. ولكنه بالمقابل لم يشر إلى ضرورة أن يكون مرتكب فعل التجسس أجنبيا، ولا إلى باقي الأفعال التي تشكل جريمة التجسس الإلكتروني بمفهومه الحالي السابق توضيحها أعلاه، بل اكتفى بذكر فعل الاستحواذ فقط. ويبقى أهم مآخذ هذا التعريف أنه لم يشر إطلاقاً إلى ضرورة إستخدام وسيط إلكتروني؛ إذ أن ما يميز صورة التجسس التقليدي عن صورته المستحدثة هو ممارسته عبر هذه الوسائط؛ وعليه يمكن القول أن هذا التعريف لا يضع حدود إستقلالية التجسس الإلكتروني عن التقليدي، وأنه يصدق أكثر على هذا الأخير.

2- التجسس الإلكتروني هو: "قيام أحد الأشخاص الغير مصرح لهم بالدخول إلى نظام التشغيل في مختلف أجهزة الاتصالات بطريقة غير شرعية ولأغراض غير سوية حيث يتاح للشخص المتجسس أن ينقل أو يمسح أو يضيف ملفات أو برامج كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أو التصوير أو التخزين على أن ينبني هذا الأمر على أساس منظم أو

[1]- سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، منشورات الحلبي الحقوقية، لبنان، 2011، ص. 325.

فردي بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية وهذا باستخدام الموارد المعلوماتية والأنظمة الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات"[1].

ما يمكن ملاحظته على هذا التعريف أنه أشار إلى أطراف التجسس الحديث لتشمل الأفراد، والدول، والمؤسسات، وحتى الجماعات المهيكلة سواء في إطار الجريمة المنظمة أو الإرهاب الإلكتروني كما جعل من الوسائط الإلكترونية المتعددة عنصراً أساسياً لقيام التجسس الإلكتروني وبذلك تمييزه عن التجسس التقليدي، إلا أن ما يؤخذ عليه أنه لم يشر إلى محل التجسس والذي يجب أن يكون سراً متعلقاً بأمن الدولة. كما أنه لم يشر إلى ضرورة أن يكون الفاعل أجنبيا. بالإضافة إلى أنه حصر صور الأفعال التي يقوم بها الشخص المتجسس في طائفة معينة لا تشكل بمفردها جريمة التجسس الإلكتروني السابق توضيحها أعلاه وإن قام بذكر أهمها.

3- التجسس الإلكتروني هو: "الحصول وتجميع المعلومات السرية المخزنة والمحفوظة داخل الحواسيب المرتبطة بالأنترنت والخاصة بسياسة الدولة وبدفاعها ونظامها الاقتصادي والصناعي وكذا أبحاثها العلمية خاصة تلك المتعلقة بأبحاث الطاقة النووية وتسليمها إلى حكومة أجنبية أخرى أو تجميع معلومات شخصية عن مستخدمي الأنترنت بغية إستغلالها لأغراض معينة"[2].

ما يلاحظ على هذا التعريف أنه لم يحصر فقط التجسس الإلكتروني في الأفعال التي قد تتعرض لها الدولة فقط كطرف وحيد، بل أضاف لها طرفاً آخر له أهميته الخاصة وهو: الفرد؛ بحيث يشكل فعل جمع معلومات سرية عنه شكلاً من أشكال المساس بأمن الدولة -وهو ما سيتم التطرق له لاحقا بنوع من التفصيل- كما حاول استعراض أصناف المعلومات محل التجسس الإلكتروني ليجعل من أبحاث الطاقة النووية مثالاً أساسياً. لكن ما يؤخذ على هذا التعريف أنه حصر سلوكات التجسس في الحصول والتجميع والتسليم وهي بعضٌ من كُل. كما حصر مكان تواجد هذه المعلومات في الحواسيب المرتبطة بالأنترنت وهو أمر غير صحيح؛ فالحاسوب بمفرده يعد أداة للمعالجة الآلية للمعطيات ويمكن من خلاله ودون أن

[1]- ياسين قوتال، جريمة التجسس الإلكتروني ومخاطرها على أمن الدولة، مداخلة في إطار الملتقى الوطني حول الجرائم الماسة بأمن الدولة، معهد العلوم القانونية والإدارية، المركز الجامعي عباس لغرور، خنشلة، 12- 13 ديسمبر 2011.

[2]- هبة نبيلة هروال، جرائم الأنترنت (دراسة مقارنة)، أطروحة دكتوراه، مقدمة لكلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2013- 2014، ص. 372.

يكون مرتبطاً بالأنترنت المساس بأسرار الدولة. كما يؤخذ على هذا التعريف أنه أهمل تحديد الغرض من تجميع المعلومات الشخصية؛ إذ يجب أن يكون الغرض هو إستغلالها للمساس بالدفاع الوطني.

4- التجسس الإلكتروني هو: "إستخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الإلكترونية الخاصة بالدول والحكومات، والتنصت عليها بقصد الإستحصال على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها تشمل جميع أنواع المعلومات العسكرية والأمنية والسياسية والاقتصادية والعلمية والاجتماعية"[1].

ما يلاحظ على هذا التعريف أنه ورغم ذكره لضرورة وجود وسيط إلكتروني للقول بقيام التجسس الإلكتروني، ورغم أنه حاول تعداد المجالات الماسة بالدفاع الوطني؛ إلا أنه حصر أفعال التجسس الإلكتروني في فعل الدخول غير القانوني إلى نظام معالجة آلية للمعطيات دون غيرها من الأفعال. كما أنه لم يذكر الأطراف الفاعلة في جريمة التجسس الإلكتروني واكتفى فقط بالإشارة إلى الدول والحكومات كطرف مستهدف وحيد.

5- "التجسس الإلكتروني أو الجوسسة الرقمية أي الحاسوبية ترصد ومراقبة عن طريق التسلل إلى الأجهزة الحاسوبية أو محاولة إعتراض الإشارات وحزم المعلومات التي ترسل من قبل الأجهزة عبر الأنترنت، تعتبر الحواسيب أحد أهم وسائل التجسس على الخصوصيات الفردية لقدرة المختصين على تلقي معلومات منها دون علم أصحاب الأجهزة أنفسهم"[2].

ما يلاحظ على هذا التعريف -كسابقه- حصره لأفعال التجسس الإلكتروني في أصناف محددة. كما أنه حصر وسيلة التجسس في الأنترنت كما هو الشأن في التعريف السابق. بالإضافة إلى أنه لم يحدد مجالات التجسس الإلكتروني واكتفى بالإشارة إلى المساس بخصوصية الأفراد فقط.

6- استخدم بعض الباحثين تعبير القرصنة الإلكترونية للدلالة على مفهوم التجسس الإلكتروني بالقول بأن: "القرصنة الإلكترونية تشير إلى استخدام وسائل الاتصال وتكنولوجيا المعلومات الحديثة في

---

[1]- علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، (دون بلد نشر)، 2013، ص. 569.

[2]- حنان أوشن ووادي عماد، التجسس الإلكتروني وآليات مكافحته في التشريع الجنائي الجزائري، مداخلة مقدمة في إطار الملتقى الوطني حول الجرائم الماسة بأمن الدولة، معهد العلوم القانونية والإدارية، المركز الجامعي عباس لغرور، خنشلة، 12-13 ديسمبر 2011.

ممارسة غير مشروعة تستهدف التحايل على أنظمة المعالجة الآلية للبيانات لكشف البيانات الحساسة(المصنفة) أو تغييرها أو التأثير على سلامتها أو حتى إتلافها"[1].

هذا التعريف يعبر عن الإتجاه الذي يخلط بين مفهوم التجسس الإلكتروني والقرصنة الإلكترونية؛ بحيث استخدم الثاني للدلالة على الأول، رغم أن تعبير التجسس الإلكتروني أشمل من تعبير القرصنـــة الإلكترونية ويحتويها. بالإضافة إلى أن القرصنة تستخدم أكثر للتعبير على سلوك الأفراد لا الدول وتحديداً في مجال المساس بحقوق المؤلف والملكية الصناعية وهو مجرد صورة من صور التجسس الإلكتروني.

7– ذهبت بعض الدراسات في مسلكها الرامي لتعريف التجسس الإلكتروني إلى محاولة تبريره وجعله سلوكاً مسموحاً خاصةً في القطاع الاقتصادي، وهذا باستخدام مصطلح الاستخبار الإلكتروني بدلاً من مصطلح التجسس الإلكتروني، فعُرف بأنه: "الحصول على المعلومة وتحليلها بغرض الكشف والتتبع والتنبؤ بقدرات ونوايا وكذا النشاطات التي توفر سبل التصرف لأجل ترقية وتطوير صنع القرار[2]، وفي نفس الإطار عرف بأنه المعرفة حول الخصوم الإلكترونيين وكذا طرائقهم ومناهجهم المجتمعة مع المعرفة حول وضعية أمن منظمة ما في مواجهة خصومها ومناهجهم"[3].

بالرجوع إلى مفهوم الاستخبار لتحديد علاقته بمفهوم التجسس، نجد أنه يستخدم للدلالة على عملية جمع المعلومات عن الخصم أو حتى عن الحليف أحياناً أو عن دولة محايدة، أو هو المعرفة والعلم التي يجب أن تتوفر لدى كبار المسؤولين من المدنيين والعسكريين حتى يمكنهم العمل لتأمين سلامة الأمن القومي ، وبصفة عامة يمكن القول بأن الاستخبارات تمارس نوعين من النشاط:

– **أولهمـــا:** الحصول على المعلومات المتعلقة بالدول الأخرى لإمداد المسؤولين بها.

[1]– ليتيم فتيحة وليتيم نادية، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، العدد الثاني عشر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، ص. 242.

[2]-Troy Townsend and others, SEI Emerging Technology center: Cyber intelligence Tradecraft project, SoftwareEngineering Institute, Carnegie Mellon University,USA,2013,p.2, etude publier sur le site:www.sei.cmu.edu, le sit a été visiter le:23/11/2015.

[3]- Strategic Cyber Intelligence, publication of the intelligence and national security alliance (INSA), Arlington, USA, March 2014, p . 3, Etude publier sur le site:www.insaonline.org, le sit a été visité le:23/11/2015.

– **ثانيهمـــا:** منع التجسس وإلقاء القبض على العملاء والجواسيس وذلك لشل نشاط الإستخبارات المعادية ، وبمعنى آخر الوقاية من نشاط الاستخبارات الأجنبية[1].

بتحليل المفهوم السابق نجد بأن الدولة تستخدم للدلالة على التجسس الذي تقوم به لفظ الاستخبار كنوع من تلطيف المصطلح وإضفاء المشروعية عليه، بينما تستخدم مصطلح التجسس للتعبير عن ذات الأفعال في حالة ارتكابها من قبل دولة أخرى. كما يتبين الفرق بين الاستخبار والتجسس في كون الثاني جزء من الأول؛ بحيث يعد التجسس وسيلة من بين عدة وسائل لجمع المعلومات الإستخبارية، إضافة للمعلومات التي يمكن الحصول عليها من مصادر أخرى كأسرى الحرب والسكان والسياح والإذاعة والتلفزيون وغيرها.

من خلال استعراض جملة التعاريف السابقة وتقييمها كل على حدة، وعلى هدي التعريف المخُتار سابقاً للتجسس التقليدي، وكذا المصطلحات التي استخدمها المشرع الجزائري للتعبير عن الجريمة الإلكترونية يمكن إقتراح التعريف الآتي:

التجسس الإلكتروني هو كل سلوك يرتكبه أجنبي، ويستهدف أنظمة المعالجة الآلية للمعطيات أو يستخدمها كوسيلة، ومن شأنه المساس بسر من أسرار الدفاع الوطني التي تتجسد في شكل معلومات إلكترونية، بغض النظر عن طبيعة مرتكبه والجهة المستفيدة منه، سواء كانت دولة أو مؤسسة أو جماعة إجرامية أو فرداً عادياً.

المـــطلب الثانـــي: خصائـــص التجـــسس الإلكترونـــي.

يأخذ التجسس الإلكتروني مكانته كأحد أبرز الإفرازات السلبية للثورة التكنولوجية من مجموع الخصائص التي ترسم ذاتيته؛ فتقوم من جهة بتمييزه عن الصورة التقليدية للتجسس، كما تبين أوجه التقارب بينه وبين هذه الصورة من جهة أخرى، وتتعدد هذه الخصائص لتعكس موقع التجسس الإلكتروني من بقية مصطلحات العصر المعلوماتي؛ وبناء عليه سيتم التطرق بدايةً لعرض الخصائص المشتركة بين التجسس الإلكتروني والتجسس التقليدي وذلك في الفرع الأول، ومن ثم سيتم عرض الخصائص التي ينفرد بها التجسس الإلكتروني عن التجسس التقليدي وذلك في الفرع الثاني.

[1]– زكي زكي حسين زيدان، الإستخبارات العسكرية ودورها في تحقيق الأمن القومي للدولة في الفقه الإسلامي والقانون الوضعي، دار الكتاب القانوني، مصر، 2009، ص. ص. 9– 10.

الفـــرع الأول: الخصائـص المشتـركة بين التجـسس الإلكتروني والتجسس التقليـدي.

يشترك كل من التجسس الإلكتروني والتجسس التقليدي في مجموعة من الخصائص يمكن توضيحها في العناصر الآتية:

أولاً- التجـسس الإلكتروني جريمـة من جرائـم أمـن الدولـة الخارجـي:

ستتم دراسة هذا العنصر بالتطرق بدايةً إلى مفهوم أمن الدولة في العصر المعلوماتي، ثم موقع التجسس الالكتروني من جرائم أمن الدولة.

أ- مفهـوم أمـن الدولـة في العصـر المعلوماتـي: يعتبر مفهوم أمن الدولة من أكثر المفاهيم غموضاً وتعقيداً فهو مفهوم واسع ومرن؛ إذ يمكن استعماله في العديد من المواقف والمجالات والظروف بدءاً من الإجراءات البسيطة التي تقوم بها سلطة الدولة بقصد تأمين المواطنين ضد الأخطار المحتملة التي تمس أنفسهم أو أموالهم، إلى الإجراءات الخاصة بتأمين الدولة نفسها في مواجهة الأخطار المحدقة بها داخلياً وخارجياً. وقد اختلف الفقه في تحديد مصطلح "أمن الدولة"؛ فذهب البعض إلى تعريفه بأنه: "قدرة الدولة على حماية مصالحها الداخلية من التهديدات الخارجية كما عُرف بأنه مجموعة الإجراءات التي تسعى الدولة من خلالها إلى حماية حقها في البقاء أو هو مجموعة المصالح الحيوية للدولة"[1]، بينما يفضل البعض الآخر إستخدام مصطلح الأمن القومي للدلالة على أمن الدولة ويعرفه بأنه: "تأمين كيان الدولة والمجتمع ضد الأخطار التي تتهددها داخلياً وخارجياً وتأمين مصالحهما وتهيئة الظروف المناسبة اقتصادياً واجتماعياً لتحقيق الأهداف والغايات التي تعبر عن الرضاء العام في المجتمع"[2]. وحالياً وبالانتقال إلى المجتمع المعلوماتي الذي تشكل المعلومات البنية التحتية الأساسية فيه، ومع زيادة الاعتماد على تقنيات المعلومات زادت احتمالية التعرض للفشل أو التخريب مما يهدد الأمن الوطني للمجتمع والدولة؛ أصبح للأمن مفهوم من المنظور المعلوماتي؛ بحيث يعرف الأمن الوطني من هذا المنظور على أنه: الإحساس الجمعي الفعلي والتخيلي بعدم وجود و/ أو تأثير التهديدات الفيزيقية والتخيلية لبنى المجتمع

[1]- محمود سليمان موسى، الجرائم الواقعة على أمن الدولة (دراسة مقارنة في التشريعات العربية والقانونين الفرنسي والإيطالي في ضوء المفاهيم الديمقراطية والدستورية المعاصرة ومبادئ حقوق الإنسان)، دار المطبوعات الجامعية، مصر، 2009، ص. 7.

[2]- جمال على زهران، الأمن الإقليمي: التهديدات والتحديات في ظل الأمن القومي العربي، مجلة الغدير، العدد الرابع والستون، دار الفلاح للنشر والتوزيع، لبنان، خريف 2013، ص. 25.

المعلوماتية (وخاصة الحساسة منها في جوانبها العسكرية والاجتماعية والثقافية والاقتصادية ...) المختلفة أياً كان مصدرها داخلي (مشكلات إجتماعية) أو خارجي (صراعات وحروب) و تستدعي التأهب و/ أو الفعل الاجتماعي و/ أو التأهب والفعل الرسمي لمواجهتها[1].

ب- موقـع التجـسس الإلكترونـي مـن جرائـم أمـن الدولـة: للدولة كما للأفراد مصالح وقيم وحقوق أساسية تعمد إلى صونها بالقانون الجزائي، وإلى الذود عنها بالعقاب، وتنقسم الحقوق الأساسية للدولة إلى زمرتين:

الأولـى- زمرة الحقوق التي تشتقها الدولة من طبيعة كونها تجسيداً للأمة في علاقاتها مع الأمم الأخرى في الميدان الدولي، وتعبيراً عن إرادتها في الحرية والاستقلال والدولة إنما تستمد هذه الحقوق بصفتها شخصاً من أشخاص القانون الدولي، أو الحقوق الدولية.

الثانيـة- زمرة الحقوق التي لا غنى للدولة عن ممارستها وحمايتها لكي تتمكن أجهزتها ومؤسساتها من النهوض بأعباء الحكم والقيام بوظائفها الأساسية حيال الرعية من أفـراد وجـماعـات، وتشتق الدولة هذه المهام من طبيعتها كحكومة وتمارس هذه الحقوق بصفتها شخصاً من أشخاص القانون الداخلي، أو الحقوق الداخلية[2].

تبعاً لتقسيم حقوق الدولة إلى طائفتين فقد تم تصنيف جرائم أمن الدولة أيضاً تبعاً لذلك إلى جرائم أمن دولة داخلي، وجرائم أمن دولة خارجي. ويقصد بالأولى تلك الجرائم التي تنطوي على الإعتداء على النظام الداخلي للدولة والمساس بالأمن والاستقرار الذي يتمتع به الناس بقصد الإطاحة بالسلطة القائمة وإستبدالها، وإستبدال النظام السياسي والاجتماعي بنظام آخر. أما الجرائم المضرة بأمن الدولة الخارجي فهي الأفعال المجرمة التي تقع على الدولة في علاقاتها بالدول الأخرى[3]، ويراد منها الإعتداء على إستقلالها أو زعزعة كيانها في المحيط الدولي أو الإساءة إلى علاقاتها بالدول الأخرى أو إعانة عدوها

---

[1]- ذياب البداينة، الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، الأردن، 2006، ص. 23.

[2]- جاك يوسف الحكيم ورياض الخاني، شرح قانون العقوبات القسم الخاص (الجرائم الواقعة على أمن الدولة الخارجي)، منشورات جامعة دمشق، سوريا، 2009، ص. 49.

[3]-محمد بن محمد سالم عدود، الجرائم المضرة بأمن الدولة الداخلي وعقوباتها في القانون الموريتاني، أطروحة دكتوراه الفلسفة في العلوم الأمنية، مقدمة لقسم العدالة الجنائية بكلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010، ص. 51.

عليها. وبمعنى أبسط فإن الجرائم الماسة بأمن الدولة الداخلي تقع على الدولة في علاقاتها بالمحكومين، بينما الجرائم الماسة بأمن الدولة الخارجي تقع على الدولة في علاقاتها بالدول الأخرى[1]، ويندرج التجسس الإلكتروني ضمن طائفة الجرائم الماسة بأمن الدولة الخارجي شأنه في هذا شأن التجسس التقليدي.

ثانيـاً- التجـسس الإلكتروني جريمـة يرتكبهـا فـرد أجنبـي:

يشترك التجسس الإلكتروني مع التجسس التقليدي في ضرورة أن يتم ارتكابه من قبل فرد أجنبي، بمعنى أن يكون حاملاً لجنسية دولة أخرى. وقد ذهبت معظم التشريعات في هذا الصدد إلى الأخذ بجنسية الفرد كمعيار للتفرقة بين جريمتي التجسس والخيانة، ومنها المشرع الجزائري[2]؛ والحكمة من استلزام المشرع لصفة المواطن في جرائم الخيانة من الوضوح بمكان؛ فرباط الجنسية يفـرض على المواطن واجب الولاء لدولته ومن أولويات هذا الولاء ألا يرتكب جريمة تؤثر على أمنها[3]، فالمواطن الذي يخون هذا الواجب هو أشد إجراماً وأكثر خطراً من ذلك الأجنبي الذي يقدم على إيذاء سلامة الدولة الأخرى خدمة لوطنه فالأول خائن بلا جدال أما الثاني فيعتبر جاسوساً وهو و إن لم يكن قد راعى آداب الضيافة وقواعد السلم الدولي في البلاد التي أساء إلى أمنها وسلامتها فإنه لا يعد خائناً[4]، ورغم كون الخيانة بحسب هذا الرأي أشد جرماً وأكثر خطورة من التجسس بالنظر لاعتبار الولاء فإن المشرع الجزائري قام بالمساواة بينهما إن في الركن المادي، أو في العقوبات.

تجدر الإشارة في هذا المقام وبصدد التفرقة بين جريمة التجسس وجريمة الخيانة إلى أن الفقه قد اتجه إلى وضع معايير أخرى هي:

- **المعيـار الموضوعـي أو المـادي:** ويستند إلى طبيعة الفعل المكون للجريمة؛ فالخيانة تتمثل في تسليم الشخص ما أودع بين يديه من سر أو قوة مادية، بينما ينصرف التجسس إلى الحالة التي لا يكون الشخص فيها ممتلكاً للسر أو موجوداً بين يديه ولكنه يبحث ويتقصى للوصول إليه؛ فعملية

---

[1]- عبد المهيمن بكر، جرائم أمن الدولة الخارجي (دراسة مقارنة في القانون الكويتي والمقارن)، دار النهضة العربية، مصر، 1976، ص. 2.

[2]- أقر المشرع الجزائري معيار الجنسية للتفرقة بين جريمتي التجسس والخيانة من خلال المادة 64 من قانون العقوبات التي تم التطرق اليها سابقاً.

[3]-عبد الفتاح مصطفى الصيفي، قانون العقوبات اللبناني (جرائم الاعتداء على أمن الدولة وعلى الأموال)، دار النهضة العربية للطباعة والنشر، لبنان، 1972، ص. 22.

[4]- سعد إبراهيم الأعظمي، مرجع سابق، ص. ص. 38-39.

التجسس هي البحث عن الأسرار المتصلة بالدفاع القومي، أما الخيانة فهي تسليم شيء سراً كان أو حصناً أو أسلحة[1]. لكن هذا المعيار انتُقد لصعوبة تطبيقه؛ نظراً للتداخل الموجود بين الفعلين المكونين لجريمتي التجسس والخيانة؛ لأن البحث عن السر حتى التوصل إليه يعتبر عمل تجسس فإذا صار بين يدي الجاني وسلمه كان الفعل خيانة فيكون قد قام بنفسه بالفعلين فعل الاستقصاء وفعل التسليم في آن واحد[2].

- **المعيـار الشخصـي أو النفسـي:** بحيث يعتد في هذا المعيار بالباعث؛ فإذا كان الجاني مدفوعاً بالرغبة في إيذاء الدولة أو بالحنق عليها فالفعل خيانة، أما إذا كان دافعه التهور أو الطمع في منفعة أو مال فالفعل من قبيل التجسس[3]. لكن يؤخذ على هذا المعيار أن من الصعوبة بمكان تطبيقه لأن البحث عن الباعث وهو مسألة محض نفسية من أشق الأمور، يضاف إلى هذا أن من شأنه أن يؤدي إلى تعدد الوصف القانوني الذي تخضع له الجريمة الواحدة إذا أسهم فيها أكثر من جان تختلف بواعثهم[4].

الفـرع الثانـي: الخصائص التي ينفـرد بها التجـسس الإلكترونـي عن التجـسس التقليـدي.

يأخذ التجسس الإلكتروني الخصائص التي تميزه عن التجسس التقليدي من التطورات الحاصلة على هذا الأخير، والتي جاءت كنتيجة حتمية للثورة التكنولوجية التي غيرت الكثير من مفاهيم الجرائم التقليدية ومنحتها أبعاداً أخرى تتعلق خاصة بوسيلة ارتكابها وبالبيئة التي تستهدفها، ويمكن إجمال هذه الخصائص في العناصر الآتية:

أولاً- التـجسس الإلكترونـي جريمـة إلكترونيـــة:

يُعد التجسس الإلكتروني أحد الجرائم الإلكترونية. وقد أثارت مسألة تحديد مدلول هذه الأخيرة الكثير من النقاش؛ فهناك من يحصر نطاق ممارستها على الحاسوب فقط سواء كان هذا الأخير وسيلة أو هدفا للجريمة ويهمل كون لفظ "إلكتروني" يشمل علاوة على الحاسوب كل الوسائط الإلكترونية الأخرى؛ إذ يقصد بمصطلح "الكتروني" -كما تمت الإشارة إليه في معرض الحديث عن التعريف اللغوي للتجسس الإلكتروني- كل ما يتصل بالتكنولوجيا الحديثة وذو قدرات كهربائية أو رقمية أو مغناطيسية أو لاسلكية

[1]- عبد المهيمن بكر، مرجع سابق، ص. 5.

[2]- سعد إبراهيم الأعظمي، مرجع سابق، ص. 36.

[3]- عبد المهيمن بكر، مرجع سابق، ص. 6.

[4]- عبد الفتاح مصطفى الصيفي، مرجع سابق، ص. 36.

أو بصرية أو كهرومغناطيسية أو مؤتمتة أو ضوئية أو ما شابه ذلك، ومن هذا المعنى أخذت الوسائط الإلكترونية أيضاً معناها بحيث تعرف على أساس أنها: شبكة الحاسب الآلي أو الانترنت أو أي شبكة إلكترونية[1]؛ لذا فإن أكثر التعاريف التي حاولت تجاوز هذه الخلافات تعريف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا عام 2000، الذي أقر بأن الجريمة الإلكترونية هي: كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية[2]، فهذا التعريف وبالإضافة إلى تجاوزه الانتقادات السابقة جاء شاملاً لمفهوم الجرائم التي ترتكب باستخدام الكمبيوتر أو باستخدام الأنترنت أو أي وسيط إلكتروني آخر.

بالرجوع إلى قانون العقوبات الجزائري نجد أن المشرع الجزائري قد استخدم مصطلح الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات للدلالة على الجرائم الإلكترونية. لكن تجب الإشارة هنا إلى أن المصطلح المستخدم من قبل المشرع الجزائري يعبر فقط عن تلك السلوكات التي يكون هذا النظام هدفاً لها؛ وعليه لا تطبق هذه النصوص على الجرائم التي يكون نظام المعالجة الآلية للمعطيات وسيلـة لارتكابها كأصل عام[3]، رغم أن المشرع الجزائري استدرك الأمر في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ بحيث نص على أن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تشمل جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية[4]، بمعنى أن المشرع الجزائري يعترف بالمفهوم الكامل للجريمة الإلكترونية ويتخذ عن طريق هذا القانون كل التدابير الإجرائية لمكافحتها لكنه في ذات الوقت وفي إطار قانون العقوبات يجرم فقط جزءاً منها وهي السلوكات التي تستهدف نظام المعالجة الآلية أما السلوكات التي ترتكب بواسطته فإن المشرع هنا تركها عموماً

---

[1]– علي جعفر، مرجع سابق، ص. 32.

[2]– جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات (رؤية جديدة للجريمة الحديثة)، دار البداية، الأردن، 2010، ص. 110.

[3]– يستثنى من هذا الأصل العام حالة حيازة أو إفشاء أو نشر المعطيات المتحصل عليها من إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وهي الجريمة المنصوص عليها في المادة 394مكرر2 من قانون العقوبات.

[4]– الفقرة (أ) من المادة الثانية من القانون رقم 09-04 المؤرخ في 5 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

لتندرج ضمن النصوص التقليدية فيه، وهو أمر يستوجب إعادة النظر؛ إذ لا يمكن الاستناد إلى قانون إجرائي بالأساس لتجريم أفعال تندرج ضمن قانون العقوبات. وكما اتجه المشرع الجزائري إلى استخدام مصطلح الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات ومصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، نلحظ اتجاهات أخرى تستخدم تعابير مختلفة للدلالة على نفس الجريمة كمصطلحات: الجريمة المعلوماتية، جرائم الكمبيوتر، جرائم الأنترنت، جرائم تكنولوجيا المعلومات أو حتى جريمة الغش المعلوماتي.

وباعتبار التجسس الإلكتروني جريمة إلكترونية فقد أخذ ذات خصائصها؛ إذ يتصف تبعاً لذلك بما يلي:

أ- التجـسس الإلكتروني جريمـة إلكترونيـة متعديـة الحـدود: إذ أن المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان، فبعد ظهور شبكات المعلومات لم تعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة[1]، فهناك تباعد جغرافي بين الفاعل والمجني عليه، ومن الوجهة التقنية بين الوسيط الإلكتروني أداة الجريمة وبين المعطيات محل الجريمة، هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة لكنه بفعل سيادة تقنيات شبكات النظم والمعلومات إمتد خارج هذه الحدود دون تغيير في الاحتياجات التقنية ليطال دول أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعطيات محل الاعتداء[2]، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان إرتكاب التجسس عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى[3].

ب- التجـسس الإلكتروني جريمة إلكترونية سهلة الارتكاب لكن صعبة الإكتشاف والإثبـات: فالجرائم التقنية ومنها التجسس الإلكتروني تعد جرائم ناعمة لأنها لا تحتاج إلى أدنى مجهود عضلي ولا تحتاج إلى سلوكيات مادية وفيزيائية متعددة لتحقيق النتيجة فيها، لذا تعتبر أيضا جرائم مغرية ويزداد

[1]- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص. 51.

[2]- خالد إبراهيم ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2009، ص. 78.

[3]- حنان أوشن ووادي عماد، التجسس الإلكتروني وآليات مكافحته في التشريع الجنائي الجزائري، مجلة الحقوق والعلوم السياسية، العدد الثاني، جامعة عباس لغرور، خنشلة، الجزائر، أكتوبر 2014، ص. 132.

الإغراء كلما انتشرت وسائل تقنية المعلومات ومعرفة الأفراد بها[1]. وتقابل السهولة في الارتكاب صعوبة في الاكتشاف والإثبات؛ وهذا لكونها جريمة هادئة لا عنف فيها، كما أنها جريمة فنية لا تترك أثرا كالآثار التي يتركها اقتحام مكان ما، كما أنها تعتمد على تغيير الأرقام والبيانات أو محوها من ذاكرة الحاسوب أو النظام المستهدف[2]، فتميز هذه الجرائم ومنها التجسس الإلكتروني بانعدام وجود دليل مرئي ملموس لكون الأدلة الإلكترونية عبارة عن نبضات إلكترونية تنساب عبر أجزاء الحاسوب والشبكة ما يُهيئ الجو المناسب للجاني ويتيح له سهولة محو أدلة الإدانة أو تدميرها في زمن متناه القصر قد لا يستغرق أكثر من ثوان، بالإضافة إلى اعتماد هذه الجرائم على الخداع في ارتكابها والتضليل في التعرف على مرتكبها؛ فقد يستخدم الجاني إسماً مستعاراً أو يرتكب فعله من خلال إحدى مقاهي الانترنت[3].

ج- التجسس الإلكتروني جريمة إلكترونية تستخدم وتستهدف نظام المعالجة الآلية للمعطيات:

سبقت الإشارة إلى أن المشرع الجزائري قد تدارك النقص المسجل على مستوى قانون العقوبات الذي يعتبر أن التجسس الإلكتروني يستهدف أنظمة المعالجة الآلية للمعطيات -باستثناء حالة حيازة أو إفشاء أو نشر المعطيات المتحصل عليها من إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بحيث يمكن أن يستخدم فيها نظام المعالجة الآلية للمعطيات كوسيلة لارتكاب التجسس الإلكتروني- وذلك عن طريق توسيع مفهوم الجريمة الإلكترونية بموجب قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لتشمل الأفعال التي تستهدف نظام المعالجة الآلية وكذلك الأفعال التي ترتكب بواسطته دون تحديد لهذه الأفعال؛ وعلـيه فالتجسس الإلكتروني قد يستهدف نظام المعالجة الآلية للمعطيات لكن يشترط هنا أن يكون هذا النظام في حالة تشغيل بمعنى أن تتم عملية التجسس الإلكتروني أثناء المعالجة الآلية للمعطيات بمختلف المراحل التي تمر بها هذه المعالجة، سواء كان ذلك عند مرحلة إدخال هذه المعطيات أو أثناء مرحلة المعالجة أو مرحلة إخراج المعلومات، ففي مرحلة الإدخال حيث تترجم المعلومات إلى لغة مفهومة من قبل الآلة يكون من السهل إدخال بيانات جديدة لا علاقة لها بالمعطيات القائمة ومحو البيانات الأساسية المطلوب إدخالها، وفي مرحلة المعالجة حيث يمكن إدخال أي

---

[1]- جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص. 93.

[2]- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، الجامعة الجديدة للنشر، مصر، 2001، ص. 97.

[3] - هبة نبيلة هروال، مرجع سابق، ص. 43-45.

تعديلات على البرنامج يمكن التلاعب في برنامج النظام المعلوماتي وتشغيل برامج جديدة تلغي جزئياً أو كلياً عمل البرامج الأصلية، أما المرحلة الأخيرة المتعلقة بالمخرجات ففيها يتم التلاعب في النتائج التي يخرجها النظام المعلوماتي[1]. ومن ناحية أخرى قد يستخدم نظام المعالجة الآلية للمعطيات كوسيلة لارتكاب التجسس الإلكتروني، وتجدر الإشارة هنا إلى أن نظام المعالجة الآلية للمعطيات مصطلح واسع ومرن يتسع ليشمل العديد من الوسائل ولا يقتصر فقط مفهومه على الحواسيب، وسيتم التفصيل في مفهومه لاحقا.

د- التجـسس الإلكتروني جريمة إلكترونية ترتكبـها فئة خاصـة: أدى التطور على مستوى وسائل ارتكاب التجسس إلى بروز طائفة جديدة من المجرمين بإمكانها التحكم في هذه الوسائل والتقنيات، فبالموازاة مع الجاسوس التقليدي ظهر الجاسوس الإلكتروني كفئة لها ذات خصائص المجرم الإلكتروني اتخذت من التجسس الإلكتروني مجالاً للنشاط؛ فإذا كان الجاسوس التقليدي لا يعتمد في نشاطه على تجهيزات معينة، بل كان يوظف لهذا الغرض قواه البدنية خاصةً، بعكس الجاسوس الإلكتروني الذي أصبح يعتمد على الآلات وعلى مقدرته الذهنية أساساً؛ فعملاء التجسس حالياً قد تخلوا عن أقنعتهم وأسلحتهم لاجئين إلى الحواسيب التي تعطيهم مداخل غير محدودة إلى عالم الشبكات، وأصبح الجاسوس الجيد لا يُقاس بموهبته في التنقل متخفياً وبشكل غير مكشوف عبر الحدود، ولكن بمقدرته على قرصنة الشفرات والرموز التي تمنحه إمكانية الدخول إلى قواعد البيانات التي تحوي المعلومات الحساسة[2]، وبغض النظر عن التقسيمات المختلفة لأصناف المجرمين الإلكترونيين بحيث نجد الكثير منها، فإن هؤلاء ومن ضمنهم طائفة الجواسيس الإلكترونيين يتميزون بما يلي:

1- المهـــارة: إذ أن الجريمة الإلكترونية ومنها التجسس الإلكتروني كنموذج تتطلب قدراً من المهارة يتمتع بها الفاعل والتي يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة أو بمجرد التفاعل مع الآخرين، وهذا لا يعني ضرورة أن يكون مرتكب الجريمة على قدر كبير من العلم في هذا المجال بل إن الواقع العملي قد اثبت أن بعض الجرائم ارتكبها مراهقون وأشخاص لهم مستو دراسي محدود.

[1] – خالد إبراهيم ممدوح، الجرائم المعلوماتية، مرجع سابق، ص. ص.84-85.

[2]- Louise I. Gerdes, Espionage and intelligence Gathering, Greenhaven press, United States of America, 2004, p. p. 173 – 174.

2- المعرفـــة: ويقصد بها هنا التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها؛ فالجناة يمهدون لجرائمهم بالتعرف على المحيط الذي تدور فيه حتى لا يصطدموا بأشياء غير متوقعة من شأنها إفشال أفعالهم أو الكشف عنهم.

3- الوسيلـــة: يراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته (سواء كانت وسائل مادية كالتجهيزات التقنية المتطورة، أو كانت وسائل ذاتية كالخبرة والقدرة على التعامل مع تلك التجهيزات التقنية من خلال درجة إتقان اللغات البرمجية).

4- الباعـــث: هناك دوافع متعددة تحرك الجاسوس الإلكتروني، وبعكس الجاسوس التقليدي الذي يسعى غالباً لخدمة بلده بغض النظر عن الإمتيازات الممنوحة له، فإن الجاسوس الحديث لم يعد ينحصر مفهومه في ذلك الشخص الذي يرتبط بدولة معينة ويعمل لحسابها، فبالإضافة إلى هذا قد لا تربطه بالدولة أية رابطة ومع هذا يتجسس إلكترونياً لحسابها بدافع تحقيق الكسب المادي، أو قد يتجسس بدافع الانتقام من الطرف المستهدف، أو بدافع الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية. وأياً كان الباعث فإنه يوجد شعور دائم لدى مرتكب الفعل بأن ما يقوم به لا يدخل في عداد الجرائم[1].

ثانيـاً- التجـسس الإلكترونـي تقنيـة من تقنيات الإرهـاب الإلكترونـي:

مع إنتشار تقنية نظم الاتصالات المعلوماتية وانتشار وسائلها وشيوع شبكة الأنترنت، ومع تطور نظم الحاسب الآلي والتي تشكل في مجموعها الفضاء الإلكتروني؛ فقد تطور الإجرام الإرهابي سواء من حيث طبيعة السلوك آخذاً في هذا الإطار منحنى معنوياً اعتمد على التقنية أكثر منه على الفعل المادي، أو من حيث الأهداف التي وإن كانت سابقاً مادية بحتة فقد أضيف إليها حديثاً أهداف معنوية ازدادت وتنوعت مع إزدياد وتنوع الاستخدامات التقنية لنظم المعلومات واعتماد المرافق الحيوية في الدولة عليها[2]؛ إذ جلبت هذه التقنيات الحديثة في جانبها المظلم المزيد من الخيارات والفرص لإجراء حروب معلومات وإرهاب فضائي، فهناك المزيد من الوسائل التي يمكن استغلالها في عمليات التخريب وإلحاق الأضرار والأذى المتعمد والحرب النفسية، وهناك المزيد من مختلف أنواع مصادر المعلومات التي يمكن مهاجمتها، وهناك المزيد من الأدوات التي يمكن استخدامها لتنفيذ هجمات على مصادر المعلومات،

[1]- علي جعفر، مرجع سابق، ص. ص. 108- 111.

[2]- جلال محمد الزعبي وأسامة أحمد المناعسة، مرجع سابق، ص. 272.

وهناك الأدوات الجديدة المؤتمتة الآلية التي يمكن استخدامها في الدفاع أيضاً ولكن نادراً ما يكون الدفاع عملية ناجحة تماماً، وغالباً ما تتأخر تقنية الدفاع عن تقنية الهجوم[1] فتضاعف بذلك خطر الإرهاب على الدولة والأفراد في ظل استغلال ميزات الوسائط الإلكترونية، وأضحى الإرهاب الإلكتروني بذلك أحد أهم التهديدات التي تواجه الدول حالياً. هذا المصطلح لجدته وعدم تعريف صورته التقليدية لا زال يكتنفه الغموض ويثير بشأنه الكثير من النقاش، وفي هذا الإطار نقف على عديد المحاولات لتعريفه وفك غموضه، ومنها القائل بأن الإرهاب الإلكتروني: "عمل إجرامي يتم تحضيره عن طريق إستخدام أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية، ينتج عنه تدمير أو تعطيل الخدمات لبث الخوف بهدف إرباك وزرع الشك لدى السكان، وذلك بهدف التأثير على الحكومة أو السكان لخدمة أجندة سياسية أو اجتماعية أو إيديولوجية"[2]. بالإضافة إلى هذا هناك من يعتبر الإرهاب الإلكتروني امتداداً للإرهاب التقليدي؛ لذا يعتد في تعريف الأول بالثاني فيذهب إلى أن الإرهاب الإلكتروني هو: "العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله باستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتى صنوف العدوان وصور الإفساد، فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية من أجل تخويف وترويع الآخرين وإلحاق الضرر بهم أو تهديدهم"[3].

ويأخذ الإرهاب الإلكتروني مستخدماً نظم المعلومات شكلين:

الأول- شن هجمات على شبكات الكمبيوتر أو القيام بعمليات الدفاع عن طريق شبكات الكمبيوتر.

---

[1]- ذياب موسى البداينة، الإرهاب المعلوماتي، مداخلة مقدمة في إطار الحلقة العلمية الموسومة ب" الأنترنت والإرهاب"، قسم البرامج التدريبية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، بالتعاون مع جامعة عين شمس، القاهرة، 15-19 نوفمبر 2008.

[2]- عادل عبد الصادق محمد الجخة، أثر الإرهاب الإلكتروني على مبدأ إستخدام القوة في العلاقات الدولية، مذكرة ماجستير، مقدمة لقسم العلوم السياسية بكلية الاقتصاد والعلوم السياسية، جامعة القاهرة، 2009، ص. 81.

[3]- محمد محمد صالح الألفي، الجرائم المضرة بأمن الدولة عبر الأنترنت، أطروحة دكتوراه، مقدمة لكلية الحقوق، جامعة القاهرة، 2011، ص. 34.

الثاني– عن طريق جمع المعلومات والاستخبارات وإستغلال أنظمة العدو من أجل دعم المتطلبات الإستخباراتية أو جمع المعلومات التي تسهل هجوم شبكات الكمبيوتر، ويمكن أن يستخدمها الإرهابيون والمجرمون سواء دعمتهم دولة أم لا [1].

ورغم إعتبار الإرهاب أساساً عملاً يقوم به الأفراد لأغراض مختلفة، إلا أنه من جانب آخر قد تلجأ الدولة إلى الإرهاب الإلكتروني –وهو ما يسمى بإرهاب الدولة– فقد تستخدمه دولة ما كأداة للحرب ضد دولة أخرى معادية لها، أو في مجال الاستخبارات المعادية ضد الدول الأخرى، أو قد تقوم به بالتعاون مع جماعة إرهابية أو أفراد للإضرار بغيرها[2].

من العرض السابق تتبين حدود العلاقة الموجودة بين كل من التجسس الإلكتروني والإرهاب الإلكتروني، التي يمكن إيجازها في عنصرين كالآتي:

أ– أوجـه التشابـه بيـن التجـسس الإلكترونـي والإرهـاب الإلكترونـي: وتتمثل في:

1– كلتا الجريمتين تعتبران جريمة إلكترونية.

2– كلتا الجريمتين تستخدمان الوسائط الإلكترونية لتنفيذها.

3– كلتا الجريمتين تنفذان عن بعد.

4– كلتا الجريمتين قد يرتكبهما الأفراد كما الدول.

5– كلتا الجريمتين تشتركان في غرض الوصول إلى المعلومات الحساسة الموجودة في الأنظمة المعلوماتية أو تعديلها أو إتلافها.

ب– أوجـه الإختـلاف بيـن التجـسس الإلكترونـي والإرهـاب الإلكترونـي: وتتمثل في:

1– يعد التجسس الالكتروني جريمة ماسة بأمن الدولة الخارجي بينما يعد الإرهاب الإلكتروني جريمة ماسة بأمن الدولة الداخلي.

[1] – محمد محمد صالح الألفي، مرجع سابق، ص. 85.

[2]– بشرى حسين الحمداني، القرصنة الإلكترونية وأسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، الأردن، 2014، ص. 51.

2- كلتا الجريمتين مستقل عن الآخر من حيث النصوص التي تحكمها وركنها المادي[1].

3- تختلف الجريمتان في موضوعهما وجوهرهما فجوهر الإرهاب الإلكتروني هو نشر الرعب والخوف أما التجسس الإلكتروني فلا يهتم بهذه الغاية وإن تولدت كنتيجة في سياق ممارسته، بل جوهره هو التوصل إلى أسرار الدفاع الوطني كما المساس به.

4- تحتج بعض الدول وتحديداً المتقدمة بممارستها التجسس الإلكتروني برغبتها في مكافحة الإرهاب، بينما يستخدم الإرهاب التجسس الإلكتروني وتقنياته للتهديد والاعتداء على الدول كما الأفراد.

5- عمليات الإرهاب الإلكتروني تظهر للعلن وتظهر آثارها سريعاً وهو أصلا هدف المنظمات الإرهابية بغية تحقيق الصيت والانتشار وزرع الرعب بين الدول والأفراد، بعكس عمليات التجسس الإلكتروني الذي يعتمد أساساً على الخفاء لإنجاحه واستمراره فهو وسيلة دائمة وليست مرحلية إذ هناك احتمال بعدم انكشافها على الإطلاق، وما يبرز للعلن يكون إما نتيجة الاكتشاف من الأطراف المستهدفة، أو نتيجة إعتراف الفرد الذي كلف بالقيام بها أو الذي على دراية بممارستها، أو من طرف الدولة الفاعلة ذاتها في حالة مرور المدد القانونية التي بعدها تصبح وثائقها المصنفة مسموحة للنشر والاطلاع.

وكحوصلة يمكن القول بأن التجسس الإلكتروني يعد أحد أساليب الإرهاب الإلكتروني؛ حيث يوفر المعلومة ويمنح فرصة تعديلها وتحريفها أو إتلافها أو إستغلالها في هجمات إلكترونية أو واقعية أخرى، سواء تم هذا برعاية أو بدعم دولة أخرى، أو من طرف أفراد ومنظمات إرهابية قد تستخدمه للحصول على أسرار الدولة لتوظيفها في وضع مخططات هجومية، أو لبيعها لمنظمات أو دول أخرى وجني مبالغ مالية من خلالها يمكن أن تستخدم أيضا في عمليات أخرى.

ثالثـاً- التجـسس الإلكترونـي تقنيـة من تقنيـات الحـرب الإلكترونيـة:

إن الميدان الرقمي أو الفضاء الإلكتروني كمفهوم يغطي جميع الكيانات التي يمكن الربـط بينهـا

[1]- تجدر الإشارة إلى أن المشرع الجزائري لم يكن يُفرد جريمة الإرهاب الإلكتروني بمواد خاصة وصريحة، إلا أنه تدارك الأمر من خلال المادتين87 مكرر 11 و87 مكرر12 المُضافتان بموجب القانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016 المعدل لقانون العقوبات، حيث جرم استخدام تكنولوجيات الإعلام والاتصال كوسائل لتنفيذ أفعال مُعتبرة كجريمة إرهابية.

رقميا[1]؛ يعد الميدان الخامس للعمليات العسكرية إلى جانب الجو والبحر والأرض والفضاء، واستخدام الموجودات الرقمية فيه كأسلحة أو كأدوات استخبار بدون شك أصبحت تتطور بسرعة؛ فمن جهة أضحت هذه الكيانات الرقمية جزءاً كاملاً في العمليات العسكرية، ومن جهة أخرى فإن تزايد التبعية لهذه الكيانات غالبا ما يخلق القابلية للاعتداء، بل أصبح أحد أهم الميادين وأصبحت عديد الدول تمتلك جيشها الإلكتروني الخاص وهذا إما للدفاع على البُنى المعلوماتية أو حتى المادية خاصتها أو مهاجمة البنى المعلوماتية والمادية للدول الأخرى؛ نظراً لارتباط كل مناحي الحياة في الدولة بالوسائط الإلكترونية فلم تعد هناك فقط حرب تقليدية بوسائل تقليدية بل انتقلنا إلى مفهوم جديد هو الحرب الإلكترونية أو كما تسمى أيضا حرب المعلومات، هذه الأخيرة التي تعتبر من المفاهيم الغامضة ولكن المستخدمة بكثرة لوصف حرب المستقبل أو الحرب المرتبطة بعصر المعلومات، كما تستخدم للدلالة على تخريب المعلومات أو تدميرها أو سرقتها أو تحريفها أو إساءة استخدامها أو المنع من الوصول إليها أو تقليل موثوقيتها أو استخدامها ضد أصحابها، فهي باختصار سرقة الأسرار، إنها قلب المعلومات ضد أصحابها وحرمان الطرف الآخر (العدو) من استخدام تقنياته[2]، إن هذا المفهوم يعبر عن النمط الأول للحرب المعلوماتية وهو النمط الهجومي فقط، بينما هناك تعاريف أخرى أكثر شمولا وتتضمن فضلاً عن هذا النمط، النمط الدفاعي؛ بحيث تعرف وكالة نظم الدفاع المعلوماتية الأمريكية (DISA) هذه الحرب بأنها: الأفعال المنفذة لتحقيق تفوق معلوماتي لدعم الإستراتيجية العسكرية الوطنية من خلال التأثير في معلومات الدعاية ونظم المعلومات في الوقت الذي تحمى وتصان المعلومات ونظمها لدينا[3]، فالحرب الإلكترونية من هذا المنظور تهدف إلى إمتلاك الهيمنة المعلوماتية من خلال الحصول على عرض دقيق وشامل للوضعية تسمح بإتخاذ قرار إستراتيجي مناسب وآني فهو شرط بنيوي للأولوية والامتياز والتفوق العسكري،

[1]-The Defence cyber strategy, publication of the Netherlands ministry of defence, Netherlands, September 2012, p. 4, publier sur le site : www.ccdcoe.org ,le site a été visité le : 23-11-2015.

[2]– ذياب البداينة، الأمن وحرب المعلومات، مرجع سابق، ص. 154.

[3]– نفس المرجع، ص. 156.

كما أنها تغطي كل الطرائق الهادفة إلى إلحاق الضرر بخصم، أو لضمان تفوق وهيمنة بواسطة امتلاك المعلومات، كما يشمل التجسس الصناعي وكل أشكال التخريب الإلكتروني[1].

بتحليل المفاهيم السابقة ومقارنتها بمجموعة الأفعال التي تشكل جريمة التجسس الإلكتروني السابق عرضها، نلحظ تشابهاً من حيث محل وموضوع كليهما الأمر الذي يؤدي إلى التسليم بكون التجسس الإلكتروني هو أحد أهم أوجه الحرب الإلكترونية وأدواتها سواء في نمطها الهجومي الذي يستهدف الحصول على السر أو تعديله أو إتلافه ومنع مالكه (الدولة) من إستخدامه، أو في نمطها الدفاعي المتمثل في حماية المعلومات الذاتية وهذا لا يتأتى – كذلك – إلا بوضع إستراتيجية فعالة لهذه الحماية تقوم وترتكز لنجاحها على معرفة ما يملكه الطرف الآخر من معلومات وأسرار، وعليه فالتجسس الإلكتروني وسيلة للهجوم كما هو وسيلة للدفاع.

المبـحث الثانـي: التطـور التاريخـي للتجـسس الإلكترونـي.

مر التجسس الإلكتروني بعدة مراحل أسهمت في بلورة شكله الحالي؛ بحيث تأثر بكل واحدة منها وانطبع بما تحمله من سمات عامة سواء من الناحية القانونية أو من الناحية العلمية، ولكن في هذا الصدد يتم الوقوف على صعوبة الفصل بين مراحل تطور التجسس التقليدي وذلك الحديث لاعتبارات عدة؛ أهمها أن التجسس الإلكتروني يبقى صورة من صور التجسس عامة، بمعنى أنه إمتداد له، بالإضافة إلى وجود تداخل كبير بين المرحلتين؛ ففي الوقت الذي كان يمارس فيه التجسس بصورته التقليدية ويخضع للنصوص القانونية السائدة في ذلك الوقت كانت الاكتشافات والتقنيات الإلكترونية تشهد ولادتها ونموها بشكل سريع؛ بحيث لا يمكن الجزم بتاريخ أول استخدام للتقنيات الإلكترونية في عمليات التجسس أي تاريخ أول عملية تجسس إلكتروني. وفي ظل عدم وجود دراسات في هذا الجانب فستتم محاولة الفصل بين المرحلتين بالربط بين المعطيات الجزئية العامة المستقاة من مراجع مختلفة. وعليه سيتم تقسيم هذا المبحث إلى مطلبين: يتناول المطلب الأول التطور التاريخي للتجسس التقليدي، ويتناول المطلب الثاني أثر التطور التقني في ظهور مفهوم التجسس الإلكتروني.

[1]-François-Bernard Huyghe, qu'est-ce que la guerre de l'information?, étude publier sur le site: http://www.huyghe.fr, le site a été visité le: 04/02/2015.

المطلــب الأول: التطــور التاريخــي للتجــسس التقليــدي.

إن التطور التاريخي للتجسس يرجع في بداياته إلى ظهور وتطور مفهوم الجرائم الماسة بأمن الدولة بإعتباره أحد أوجهها، والذي تأثر بدوره بمجموعة الظروف السياسية والاجتماعية السائدة في كل مرحلة. وعلى كل سيتم الرجوع إلى بدايات التجسس إنطلاقاً من العصور القديمة والوسطى وصولا إلى تطوره في العصر الحديث وهذا من خلال تقسيم هذا المطلب إلى ثلاثة فروع: يتناول الفرع الأول منها التجسس في العصور القديمة، ويتناول الفرع الثاني التجسس في العصور الوسطى، بينما يتناول الفرع الثالث التجسس في العصر الحديث.

الفـــرع الأول: التجــسس فـي العصــور القديمـــة.

إن ظاهرة التجسس ليست ظاهرة حديثة، بل هي قديمة وموغلة في القدم؛ إذ نشأت مع نشأة أُولى المجتمعات البشرية وأياً كانت صورة هذا المجتمع أسرة ، عشيرة قبيلة، قرية، مدينة ... فمتى ظهر أي تجمع بشري وفي أي زمن فقد نشأ التجسس؛ لأن كل تجمع يسعى جاهداً لمعرفة ما لدى غيره من التجمعات الأخرى من أسرار أو معلومات. وقد ارتبطت هذه الظاهرة في الماضي البعيد بالقدرات الخارقة للآلهة والأساطير وكانت الوسيلة الأولى للحصول على المعلومات في ذلك الزمن تتمثل في اللجوء إلى العرافين والكهان والسحرة بإعتبارهم وسطاء بين البشر وبين الآلهة؛ حيث يكون لهؤلاء حق معرفة نوايا ورغبات الآلهة وما سيحدث فيما يتعلق بمصائر البشر، وغالباً ما يتم ذلك عن طريق الوحي أو الإلهام أو التنجيم أو الأحلام، ثم أخذ التجسس بعد ذلك طابعا أكثر واقعية فلم يعد مرتبطًا بالإرادة الآلهة أو الأرواح، ولكنه إرتبط بقوة ومشيئة الحكام والغزاة وإرادة المحافظة على الجماعة السياسية تحت سلطان الملك[1]، لتختلف أحكامه باختلاف الحضارات والقوانين، كما سيتبين من خلال العناصر الآتية:

أولاً- التجــسس عنـد الفراعنـــة:

عرف الفراعنة التجسس منذ القدم؛ حيث كان لهم جهاز للاستخبارات مهمته التجسس على الدول الأجنبية، كما يختص بحماية الدولة من أخطار التجسس الأجنبي. وقد كان ملوك الفراعنة يعلقون أهمية كبيرة على هذه الأجهزة لصيانة الأمن الداخلي من جهة وللحصول على المعلومات السرية عن القوات المعادية ودرجة تنظيمها من جهة أخرى. وقد كان التشريع الفرعوني يفرق بين جرائم الإعتداء على

[1]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 19.

المصالح العامة وجرائم الإعتداء على المصالح الخاصة، وكانت جرائم الإعتداء على المصالح العامة تشمل على وجه أخص التجسس أو إفشاء أسرار الوطن لأعداء البلاد، وكانت العقوبة التي يقررها القانون لجرائم التجسس تتحدد تبعاً للطريقة التي ارتكب بها الفعل المادي؛ فإذا تم التجسس عن طريق تبليغ أسرار الدولة إلى دولة معادية مشافهة فالعقوبة قطع لسان الجاسوس، أما إذا ارتكب الفعل عن طريق مكاتبة العدو فإن العقوبة تكون قطع إصبع الجاسوس؛ فسياسة المشرع الفرعوني تتجه إلى أن يكون الجزاء من جنس العمل و ذلك بهدف الردع العام[1]. أما بالنسبة للنظام القضائي ففي حالة الجرائم الماسة بأمن الملك أو الملكة ومنها التجسس، فقد كانت تشكل محاكم استثنائية، ونظراً لأهمية المحاكمة؛ فإن نائب الملك "النائب العام" الذي يمثل النيابة العامة هو من يتولى تعيين القضاة بإسم الملك ثم يعين نفسه بعدهم فهو مفوض من قبل الملك في ممارسة تلك السلطة. وقد كانت إجراءات المحاكمة في القضايا الماسة بأمن الدولة أي بأمن الملك أو الملكة تُعقد بصورة سرية حيث تكون محاضر الجلسات موجزة ولا تنشر أسباب الحكم وذلك خلافا للقضايا الجنائية العادية التي كانت ترد أسبابها مطولة وكاملة[2].

ثانيـاً- التجـــسس عنـد البابلييـــن:

يعتبر قانون حمورابي القانون السائد في بابل، وكان ينظر إلى كل فعل ضار بالأسرة أو الدولة جريمة يعاقب عليها بشدة؛ إذ كانت عقوبة الإعدام مقررة للجرائم التي تمس أمن الدولة أو التآمر على مصالحها أو عرقلة تنفيذ أوامرها أو التكتم على مؤامرات قطاع الطرق. على أن قانون حمورابي لم يتضمن نصاً صريحاً يتعلق بجرائم التجسس ومع ذلك فإن هذه الجرائم كان يعاقب عليها بموجب أحكام التشريع التي تهدف إلى وضع حماية فعالة للجيش من كل مساس بأمنه بإعتباره جزءاً لا يتجزأ من أمن الدولة؛ ومن ثم فكل فعل يشكل إعتداء على أمن الجيش كان يعاقب عليه ومن هذه الأفعال التجسس. وكان حمورابي يهدف من وراء هذه التجريمات إلى إشاعة الأمن والاستقرار في البلاد عن طريق الجزاءات الجنائية الصارمة؛ ولهذا فإن عقوبة الإعدام كانت هي العقوبة التي ينص عليها القانون لكل من يرتكب أفعالاً تؤدي إلى الإضرار بأمن الدولة أو لمن يعبث بهذا الأمن أو يشيع الاضطراب في الدولة، وكان التجسس يدخل في مفهوم هذه الجرائم لأن من شأنه إلحاق الضرر بأمن وكيان الدولة. كما فرض

[1]- زكي زكي حسين زيدان، مرجع سابق، ص. ص. 19- 20.

[2]- مجدي محب حافظ، الحماية الجنائية لأسرار الدولة، الهيئة المصرية العامة للكتاب، مصر، 1997، ص. ص 24-25.

حمورابي على كل من يعلم بوقوع أية جريمة من هذه الجرائم أن يبلغ عنها بمجرد العلم بها باعتباره شاهداً عليها وإلا وقع تحت طائلة العقاب. وبذلك فقد إشتهر قانون حمورابي بمزايا عديدة جعلته يظهر على أنه متقدم على العصر الذي وجد فيه فأحكام قانون العقوبات التي يتضمنها تدل على أن الجريمة والعقوبة تخضع لإشراف الدولة بصفة عامة[1].

ثالثـاً- التجـسس عنـد الرومـان:

قسم القانون الروماني الجرائم إلى طائفتين: جرائم عامة تتعلق بالمصلحة العامة، وجرائم خاصة تتعلق بمصلحة فردية، وقد كان التجسس يدخل ضمن الطائفة الأولى رغم أن جرائم التجسس في ظل هذا القانون كانت تسمى جرائم الخيانة العظمى أو جرائم بيع الوطن، وقد كانت هذه الأخيرة تعرف بجرائم المساس بصاحب الجلالة أو التاج[2]، والتي تم النص عليها في قانون الألواح الإثني عشر للدلالة على الجرائم الماسة بأمن الدولة؛ حيث قام الإمبراطور فيها بتجسيد مجموعة الحقوق السيادية للدولة الرومانية والجرائم التي تحمي شخص وسلطة الإمبراطور ليصبح هذا المفهوم أكثر مرونة واتساعاً ليشمل بعض الجرائم الخطيرة كحمل السلاح ضد الدولة والمؤامرة ضد حياة الإمبراطور أو الضباط السامون، وكذا بعض الجرائم الأقل خطورة كتدمير تماثيل الإمبراطور أو سب ذكراه[3]، ومن هنا يلحظ التطابق في ظل هذا القانون بين مفهوم أمن الدولة والإمبراطور؛ فالمساس بأي شكل بالإمبراطور هو مساس بالدولة ذاتها. كما يندرج ضمن مفهوم الخيانة في هذا القانون أيضا تسليم أسرار الدولة أو إفشاء المعلومات العسكرية إلى الدولة الأجنبية، ولم يكن نطاق التجريم يشمل الوقائع المادية فقط ولكنه كان يمتد ليشمل الأفكار والمعتقدات التي يؤمن بها الإنسان[4].

وقد كانت تختص بنظر الجرائم الماسة بالعظمة أو الجلالة ومن بينها جرائم التجسس محاكم خاصة، وكانت هذه المحاكم تتمتع بسلطات واسعة تخرج على القواعد العامة والأحكام المنطقية المعقولة

---

[1]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 23-24.

[2]- إبراهيم شاكر محمود الجبوري، جرائم الاعتداء على أمن الدولة من الداخل والخارج، المركز القومي للإصدارات القانونية، مصر، 2011، ص. 23.

[3]-Allen M. Lenden et autres, les crimes contre l'Etat, commission de réforme du droit du Canada, Canada 1986, p .p .3 – 4.

[4]- مجدي محمود محب حافظ، موسوعة جرائم الخيانة والتجسس، مرجع سابق، ص. 45.

التي يقرها القانون الجنائي وتخضع لها المحاكم الأخرى؛ فللقاضي حرية مطلقة في تقدير الوقائع التي تشكل جريمة من جرائم المساس بالجلالة دون أن يكون ملتزماً بمعيار موضوعي أو منطقي، ولهذا لم يكن التجريم منحصراً في نطاق الأفعال المادية فحسب وإنما كان يشمل أيضا الكتابات والأقوال والأفكار التي تراود أي شخص، كما لم يكن للمتهمين بهذه الجرائم أية ضمانات أو حقوق للدفاع عن أنفسهم في مواجهة الإتهامات التي توجه إليهم وذلك باعتبارهم أعداء للدولة؛ ومن ثم فإن المحاكمة في مثل هذه الجرائم كانت بمثابة مرحلة أولى من مراحل الحرب ضد العدو، وعلى ذلك لم يكن الحكم الصادر في الدعوى سوى وسيلة للدعاية والإعلان أكثر منه فصلاً في قضية جزائية بالإدانة[1].

أما بخصوص العقوبات فقد نُص على عقوبة الإعدام حرقاً بالنسبة لمرتكبي جرائم التجسس باعتبارها من الجرائم الماسة بالجلالة أو العظمة، وكان تنفيذ هذه العقوبة يقترن دوما بالشدة والوحشية؛ إذ كان يلقى بالمحكوم عليه في نار ملتهبة أو للحيوانات المفترسة، وكان التنفيذ يتم في إحدى المناسبات الوطنية[2]، وإذا توفي المتهم قبل الحكم فلا تسقط الدعوى وإنما تحاكم ذكراه من بعده، أما أموال المحكوم عليه فكانت تصادر جميعها. ولم يكن القانون الروماني يمنح فاعلي هذه الجرائم أية ضمانة ولم يكن يعترف لهم بأي حق من حقوق الدفاع المقررة لسواهم[3].

الفـــرع الثاني: التجـسس فـي العصـور الوسـطى.

شهدت العصور الوسطى ظهور الدولة الإسلامية التي ارتكزت في إدارة كل جوانبها على مبادئ التشريع الإسلامي، هذا من جهة، ومن جهة أخرى وبعد مرور عقود على نشأة الدولة الإسلامية وفيما يخص دول العالم الأخرى والتي تصنف ضمن ذات العصر، فقد شكل القانون الفرنسي أبرز النظم السائدة في ذلك الوقت؛ وعليه ستتم دراسة التجسس في العصور الوسطى وفقا لعنصرين: يتضمن العنصر الأول التجسس في بداية عهد الدولة الإسلامية، ويتناول العنصر الثاني التجسس في القانون الفرنسي.

[1]– محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. 29.

[2]– محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 28.

[3]– محمد الفاضل، مرجع سابق، ص. 37.

أولاً- التجـسس فـي بدايـة عهـد الدولـة الإسلاميـــة:

قُبيل البعثة النبوية كانت هناك دولتان كبيرتان في العالم لكل منها أسلوبها الخاص في الحرب، وهما: دولة الفرس ودولة الروم. وكانت دولة الروم تستعمل الجواسيس ضد العرب قبل ظهور الإسلام حتى أن مكة المكرمة قبل الإسلام كانت لا تخلو من الجواسيس الذين يعملون لحساب الرومان، وكان فيها بيوت تجارية رومانية يستخدمها الرومان للشؤون التجارية في الظاهر وللتجسس على أحوال العرب سراً[1]. ومن جهة أخرى فقد عرف العرب قبل الإسلام إستخدام العيون والعملاء لجمع المعلومات في حروبهم مع بعضهم البعض ومع أعدائهم؛ إذ كان القادة يستعينون قبل الدخول في القتال بمخبرين يرسلونهم إلى العدو للحصول على معلومات عن قواتهم وعن مواقعهم وعن مدى استعدادهم للحرب. كما استعمل العرب الرموز والشفرة والإشارة إذ كانوا يستخدمون التراب أو الرمل للدلالة على كثرة العدو، والشوك للدلالة على قوة العدو، وعبروا بالشوك الذي تكسر رؤوسه بشوكة العدو الذي لا يُخشى جانبه[2].

بعد بزوغ فجر الإسلام وإرساءه لقواعد جديدة في كل المجالات، كان التشريع الإسلامي موافقاً لما كان سائدا آنذاك بخصوص التجسس؛ فهو يجيز ممارسته ضد الدول الأجنبية والمعادية وفي المقابل يعاقب على هذا النشاط إذا وقع لحساب دولة أجنبية أو معادية ضد مصالح الدولة الإسلامية؛ ولهذا كان التجسس على العدو من المسائل التي اهتم بها الرسول صلى الله عليه وسلم في غزواته، كما كان يعتني بإختيار الأشخاص الذين تناط بهم مهام معينة في هذا المجال. كذلك سار على هذا النهج النبوي الخلفاء الذين جاءوا بعده وأولوه رعايتهم وكانوا يعتبرونه من الأعمال الجليلة والخطيرة[3]؛ وهذا إنطلاقاً من الأهمية التي تلعبها الاستخبارات إذ أن مستقبل أية أمة أو دولة يتوقف على دقة وكمال المعلومات التي تصل إليها والتي تنير الطريق أمام القرارات العليا للدولة، فمعرفة العدو وتحدياته ومعرفة مؤامراته ومخططاته شيء أساسي، فالتخطيط السليم لأية معركة يتوقف على معرفة أسرار العدو ورصد تحركاته ولا سبيل لذلك إلا بواسطة بث العيون واستخدام التجسس على الأعداء بكل الوسائل الممكنة[4].

---

[1]- محمد راكان الدغمي، التجسس وأحكامه في الشريعة الإسلامية، ط2، دار السلام للطباعة والنشر والتوزيع والترجمة، مصر، 1985، ص. ص. 50-51.

[2]- زكي زكي حسين زيدان، مرجع سابق، ص. 26.

[3]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. 581.

[4]- زكي زكي حسين زيدان، مرجع سابق، ص. 11.

وقد كان الرسول صلى الله عليه وسلم لا يدخل معركة إلا بعد معرفة حالة العدو ومعسكراته ومواقعه العسكرية وطبيعة الأرض. وكان له صلى الله عليه وسلم عيون محلية في المدينة المنورة وعيون في مكة يطلعونه على كل صغيرة وكبيرة قد تضر بالمصلحة العامة للمسلمين في السلم والحرب، ففي مكة المكرمة كان العباس بن عبد المطلب عم النبي صلى الله عليه وسلم يأتيه بالأخبار، وكان العباس يرغب في الهجرة إلا أن الرسول صلى الله عليه وسلم كتب إليه أن مقامه في مكة خير، كما كانت له العيون من القبائل العربية الأخرى فقد كان عبد الله بن حدرد الأسلمي من قبيلة هوزان عيناً له في حنين؛ فبعد فتح مكة في السنة الثامنة للهجرة قررت القبائل العربية في هوزان وثقيف أن تغزوا الرسول صلى الله عليه وسلم قبل أن يبدأ المسلمون بغزوهم، وعندما سمع الرسول صلى الله عليه وسلم نبأ هوزان وثقيف أرسل عبد الله بن أبي حدرد الأسلمي ليأتيه بالمعلومات اللازمة، فدخل فيهم وعرف ما أجمعوا عليه، وسمع من مالك بن عوف قائد هوزان ثم جاء إلى الرسول صلى الله عليه وسلم يخبره الخبر. وقد حرص الرسول صلى الله عليه وسلم من جهة أخرى ألا تتسرب الأخبار إلى العدو وعمل على مقاومة جواسيس قريش في مكة والمدينة، فقد قام عليه الصلاة والسلام ببث عيونه ودورياته لتجوس الدروب حول المدينة لتحول دون تسرب المعلومات إلى قريش، كما بث عيونه عليه الصلاة والسلام في الداخل ليقضي على كل خبر يمكن أن يصل أو يتسرب إلى قريش عن طريق عيونها داخل صفوف المسلمين وهذا في فتح مكة في السنة الثامنة للهجرة؛ وذلك ليتمكن صلى الله عليه وسلم من السيطرة على الموقف وليستفيد من عنصر المبادرة أيضا، إذ كان صلى الله عليه وسلم يعرف أهمية حفظ السر في حروبه فكان يعمي على العدو تحركاته ولا يُظهر للناس الجهة التي يريدها أو القبيلة التي يريد قتالها إلا في تبوك؛ نظراً للمشقة التي تحتاج إلى الاستعداد الكامل وأخذ المؤونة[1].

بالرجوع إلى أحكام التشريع فيما يخص التجسس، وبعد تبيان أن هذا التشريع يجيز ممارسة الجاسوسية على الدول الأجنبية والمعادية ومن جهة أخرى يجرم ذات السلوك إذا وقع مساساً بمصلحة الدولة الإسلامية –وهو في هذا لا يخرج عن السائد والمعروف من الأحكام في كل الأزمنة والعصور– فإنه وفقاً لهذه النظرة قد وضع القواعد التي تحكم التجسس المجرم وفقها، فالتشريع الإسلامي لا ينظر إلى التجسس على اعتباره من الجرائم السياسية؛ وذلك لأن جوهر هذه الأخيرة يتمثل في خروج جمع من الأفراد على السلطة الحاكمة بقصد الإطاحة بها أو تغييرها، أي أن الجريمة السياسية هي كل نشاط

[1]– محمد راكان الدغمي، مرجع سابق، ص. ص. 55– 61.

يستهدف المساس بالنظام القائم، وهذا مالا يتوافر في أفعال التجسس التي لا تستهدف المساس بنظام الحكم، ولكن بوجود وكيان الدولة والمجتمع معا؛ ولهذا فإن هذه الجرائم في حقيقتها تشكل إعتداء على شخصية الأمة الإسلامية بأسرها؛ وعليه لا تعد جرائم سياسية ولكنها تعتبر جرائم عادية تتصف بالخطورة لذا فقد قررت لها عقوبات شديدة وصارمة[1] تتمثل في القتل أو الصلب أو قطع الأيدي والأرجل من خلاف أو النفي.

من خلال العرض السابق يتضح مدى التقدم والنضج الذي تتصف به أحكام الشريعة الإسلامية؛ فهي من جهة قد أرست سياسية رشيدة فيما يتعلق بمواجهة الإجرام السياسي ترتكز على وجوب التمييز بين المجرمين السياسيين وبين المجرمين العاديين، ومن جهة أخرى أرست مبدأ التفرقة بين الدولة ككيان مستقل قائم بذاته وبين الأشخاص المكونين له سواء كانوا حكاماً أم محكومين، وقد ترتب عن هذه التفرقة تمييز بين الجرائم التي تقع على الدولة وبين الجرائم التي تقع على الحكام أو على نظام الحكم؛ إذ كانت هذه الجرائم في الأنظمة القديمة تشكل وحدة واحدة تعرف بجرائم المساس بالجلالة أو العظمة وذلك على أساس أن الإعتداء على الملوك أو الحكام أو أياً كانت تسمياتهم هو إعتداء على الدولة، ولم تعرف التشريعات الوضعية مبدأ إستقلال الدولة كشخص معنوي إلا بعد الثورة الفرنسية سنة 1789[2].

ثانيـاً- التجـــسس فـي القانـون الفرنســي:

يُعد القانون الفرنسي الأنموذج الأكثر أهمية الذي كان سائداً في النظم القانونية في العصور الوسطى؛ إذ أخذ القانون الفرنسي في هذا العصر بالمفهوم الروماني للتجسس؛ بحيث تم تبني مبادئه بعد أن دخل هذا القانون إلى أوروبا الغربية في القرن الحادي عشر وهذا كنتيجة لتبني الملوك إرادياً للمفهوم الروماني للجرائم ضد الجلالة كنموذج للجرائم ضد الدولة[3]، وظهر ذلك جلياً من خلال تقسيم جرائم المساس بالجلالة إلى نوعين: النوع الأول وهو جرائم المساس بالجلالة من الدرجة الأولى، ويقصد بها جرائم القتل أو محاولة قتل الملك أو أحد أفراد عائلته أو التآمر ضد الدولة أو زعزعة استقرار الحكم، أما النوع الثاني فيتمثل في الجرائم الماسة بالجلالة من الدرجة الثانية، ويقصد بها جرائم التآمر ضد الجيش أو ضد حكام الأقاليم أو إهانة الملك أو أحد أفراد عائلته أو إهانة أحد أفراد حاشيته الملكية بالقول أو

[1]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. 588.

[2]- نفس المرجع، ص. ص. 589- 590.

[3]- Allen M. Lenden et autres, op. cit, p. 4.

بالكتابة، وكذا تهريب السلاح وخصوصاً إلى دول المشرق أو هروب العسكريين إلى صفوف العدو، أو إنشاء تحصينات عسكرية خاصة دون موافقة مسبقة أو التجسس لصالح قوى أجنبية[1]. وكان التجسس يشمل العديد من الجرائم كالتفاوض مع العدو وعقد صلات أو مراسلات مع أمراء أجانب، والإشتراك في تجمع معادي والتآمر على الملك أو على أحد أبناءه أو على إحدى مصالح الدولة.

نظراً للطبيعة الخاصة للجريمة والعقوبة بالنسبة لأفعال المساس بالجلالة الملكية فقد روعي أن تكون الجهة المختصة بالتحقيق والمحاكمة فيها على درجة عالية من المسؤولية والإلمام بمختلف التجريمات التي تمس الذات الملكية؛ ولهذا أُعطي هذا الإختصاص للغرفة الكبرى فـي البرلمان فهي الجهة التي تملك حق محاكمة المتهمين والتحقيق معهم في هذه الجرائم[2].

أما العقوبات المقررة للجرائم الماسة بالجلالة ومنها التجسس فقد كانت مطبوعة بالوحشية والقسوة؛ حيث كان يتعرض كل من يتهم في هذه الجرائم للتعذيب والتنكيل لكي يعترف بجريمته أو بشركائه، وإذا كانت العقوبة في مثل هذه الأحوال هي الإعدام فإن المحكوم عليه لا يصل إلى هذه النهاية إلا بعد أن يمر بمعاناة قاسية؛ فتقطع يده اليمنى ثم ساقيه ثم بقية أجزاء جسمه قطعاً ثم تجمع وترمى في رصاص مذوب أو زيت ملتهب وأخيراً تحرق هذه القطع وينشر رمادها في الهواء، وهذا العقاب لم يكن كافياً في نظر مشرعي ذلك العصر؛ فأضافوا إليه جزاءات أخرى كهدم بيت المحكوم عليه، والحكم بنفي وإبعاد أفراد أسرته إلى الأبد، وحظر العودة عليهم تحت التهديد بالإعدام شنقاً، ومنع أهالي المحكوم عليه الآخرون من حمل إسمه مستقبلا، فضلاً عن مصادرة كافة أمواله. ومن جهة أخرى فقد كانت المسؤولية الجنائية عن جرائم المساس بالجلالة ومنها التجسس تخضع لقواعد خاصة ومختلفة تماماً عن القواعد والمبادئ العامة التي تحكم المسؤولية الجنائية في القانون؛ فهذه المبادئ تقتضي عدم تقرير المسؤولية الجنائية إلا إذا توافرت ملكتي الشعور والإرادة و من ثم لا يجوز مساءلة من لا يتمتع بهما مثل صغار السن أو الأحداث أو المكرهين على ارتكاب الفعل أو العبيد، إلا أن هذه القواعد لا تطبق في حالة الجرائم الماسة بالجلالة، ومن ثم تصح مساءلة ومعاقبة من لا يتمتع بملكتي الشعور والإرادة كالأطفال والأحداث والمكرهين على ارتكاب الفعل متى ثبت ارتكابهم له، بل إن أعضاء الأسرة الملكية والأمراء الذين لا يخضعون لأحكام القانون الجنائي نظراً للحصانة التي يتمتعون بها، يمكن أن توجه إليهم تهم تتعلق بالجرائم الماسة

[1]– مجدي محب حافظ، الحماية الجنائية لأسرار الدولة، مرجع سابق، ص. 48.

[2]– محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 35.

بالجلالة، مثل الخيانة والتجسس تأسيساً على أن مثل هذه الجرائم لا تخضع لأحكام الحصانة التي تحول دون المساءلة الجنائية، بل إن الأمر تجاوز هذه الحدود بكثير؛ إذ أن الدعوى الجزائية كانت ترفع على جثث الأموات لكي تعاقب ذكراهم وتمحي أسمائهم ولمصادرة أموالهم[1].

الفـــرع الثالـــث: التجـــسس في العصر الحديـــث.

جرت العادة على ربط بداية العصر الحديث عند الكثيرين بقيام الثورة الفرنسية؛ وهذا بالنظر إلى نتائجها خاصة على مستوى النصوص القانونية، فبعد قيام الثورة الفرنسية في سنة 1789 حدث تغيير جوهري في طبيعة ومضمون الجرائم الماسة بالذات الملكية، وظهر لأول مرة مفهوم أو تعبير الجرائم المخلة بأمن الدولة، ويمكن إجمال هذا التغيير في عنصرين:

أولاً– جعلت مبادئ الثورة الفرنسية من الدولة شخصية معنوية مستقلة عن أشخاص الحاكمين، ولم يعد هؤلاء سوى أداة من أدوات الحكم، ولم يعد المقصود بالحماية الحاكمون، وهكذا حل مفهوم الجرائم المخلة بأمن الدولة محل الجرائم الماسة بالعظمة أو الماسة بولي الأمر.

ثانياً– التمييز بين الجرائم المخلة بأمن الدولة الخارجي وبين الجرائم المخلة بأمن الدولة الداخلي، فالأولى تهدد الدولة نفسها مباشرة في وجودها وفي كيانها وفي بقائها، أما الثانية فلا تمس سوى أجهزة الدولة أي شكل حكومتها والمؤسسات التي خلقتها للقيام بأعباء السلطة فهي تهدف إلى تغيير الحكومة لا إلى تقويض الأمة[2]؛ وظهر كنتيجة لذلك وكأحد انعكاسات الثورة في العالم التفرقة بين الولاء للوطن وبين الولاء للنظام أو على حد تعبير الفقيه الفرنسي جارسون "مع الثورة ظهر فصل بين الارتباط بالنظام وبين الواجب تجاه الوطن"[3].

أدى التمييز بين جرائم أمن الدولة الخارجي وبين جرائم أمن الدولة الداخلي إلى تغيير النظرة إلى طبيعة كل واحدة منها، ففي ظل القانون الروماني الذي كان يدرج كل من الطائفتين السابقتين ضمن الجرائم الماسة بالعظمة والجلالة الملكية على اعتبار أن شخصية الملك أو الإمبراطور تمثل التجسيد

[1]– محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 34–35.

[2]– إبراهيم شاكر الجبوري، مرجع سابق، ص. ص. 27– 28.

[3]– محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 30.

الواقعي للدولة، فقد كانت هذه الجرائم جميعاً تأخذ طابع الإجرام السياسي، إلا أنه وفي ظل النظام الجديد حيث أصبح للدولة شخصيتها المستقلة والمنفصلة عن شخصية حكامها وظهور الطائفتين السابقتين من الجرائم؛ فقد ثار التساؤل حول طبيعة كل منهما وهو ما يستتبع بحث طبيعة التجسس إن كان جريمة سياسية أم جريمة عادية، ونظراً للآثار المهمة التي تترتب عن التفريق بينهما سواء من حيث عدم إمكانية التسليم وإقرار معاملة خاصة للمجرمين السياسيين خاصة من حيث العقوبة وطرق تنفيذها؛ فقد حاول الفقه وضع معايير للتفرقة بين الصنفين من الجرائم، ويمكن إجمال هذه المعايير فيما يلي:

أ- **المعيـار الشخصـي:** وبحسبه تعتبر الجريمة سياسية إذا كان الدافع لارتكابها سياسياً أو كان الغرض من تنفيذها سياسياً؛ بحيث لا يرمي فيها الفاعل إلى تحقيق مأرب شخصي، بل غايته مجردة من المصلحة الشخصية ومرتبطة حسب رأيه بمصلحة المجتمع والوطن. ولم يسلم هذا المعيار من النقد؛ حيث يرى معارضوه أن الدافع السياسي لا يكفي لإضفاء الطابع السياسي على الجريمة إعتباراً إلى كون الدافع ليس ركنا من أركان الجريمة.

ب- **المعيـار المـادي أو الموضوعـي:** ويعتمد على موضوع الجريمة كضابط للجريمة السياسية؛ ومن ثم تعد جريمة سياسية الجرائم التي تخل بتنظيم وسير السلطات العمومية أو بمصلحة سياسية للدولة أو بحق سياسي للمواطنين. ويعاب على هذا المعيار اتساعه[1]، ونظره إلى الجريمة من خلال ركنها المادي فقط مع إغفال تام لركنها المعنوي وعدم الإهتمام بنبل الباعث وشرف القصد.

ج- **المعيـار التوفيقـي:** إزاء الثغرات التي تكتنف كل من المذهب الشخصي والمذهب الموضوعي ذهب فريق من الفقه إلى وجوب التوفيق بينهما للوصول إلى معيار يكون أكثر قبولا لتحديد الجريمة السياسية؛ وعليه يشترط لاعتبار جريمة ما جريمة سياسية أن يكون محل العدوان فيها سياسياً حسب ما يتطلب المذهب الموضوعي، وأن يكون الدافع أو الباعث عليها سياسياً طبقا لما ينادي به المذهب الشخصي، ويجب أن يتوافر هذان الشرطان معا[2].

بتطبيق هذه المعايير بإختلافها نجد أنها إعتبرت جرائم الإعتداء على أمن الدولة بقسميه الداخلي والخارجي جرائم سياسية سواء في التشريعات الجنائية المختلفة أو في نظر كتاب القانون وشراحه؛ وذلك

[1]- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط 5، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، ص. 32.

[2]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 158.

لما فيها من إعتداء على إستقلال الدولة السياسي أو التهجم على نظمها المقررة ولأن هذه الجرائم مسلطة ضد الصالح العام، ورتبوا على ذلك نتائج منها عدم إمكانية تسليم الجاني، ولم يكن في وسع المشرع في كثير من الدول أن يقرر لها عقوبة الإعدام المفروضة لكثير من الجرائم العادية. لكن ومع تعدد أشكال الإعتداء على أمن الدولة الخارجي ووضوح خطورتها وفداحة آثارها خاصة بعد الحرب العالمية الأولى؛ ذهب فقهاء القانون الجنائي إلى إعادة النظر في صفة الجريمة السياسية وفي الإمتيازات القانونية التي يتمتع بها مرتكبوها فأبعدوا هذه الصفة عنها[1]. كما أسهم التوتر الدولي والتسابق على التسلح والتقدم الصناعي وتجربة الحرب العالمية الأولى وظهور شبح الحرب العالمية الثانية في إزدياد مخاوف الدول من الإعتداء على أمنها الخارجي؛ فذهبت دولة بعد الأخرى إلى إخراج الجرائم الماسة بأمن الدولة الخارجي ومنها التجسس من نطاق الجرائم السياسية وإعادتها إلى طائفة الجرائم العادية، بل وشددت العقوبات المقررة لها [2]. والجدير بالذكر هنا أن دائرة الجرائم السياسية قد أخذت في الانكماش إبتداءاً من النصف الثاني من القرن العشرين إلى درجة أن البعض يتوقع أن ينقرض قريبا التمييز بين الجرائم السياسية والجرائم العادية، بل إن البعض الأخر يشكك حتى في حقيقة هذا الصنف من الجرائم؛ لاسيما بعد الاتفاقات التي حصلت في المنظمات الدولية والإقليمية على إخراج معظم الجرائم التي اصطلح على تسميتها جرائم سياسية من دائرة الجرائم السياسية وإدخالها في نطاق الجرائم العادية، كالجرائم الإرهابية وجرائم الاعتداء على رؤساء الدول وأعضاء أسرهم[3].

رغم التوجه إلى الإقرار بأن التجسس جريمة عادية إلا أن أهم نتائج التفريق بين الجرائم السياسية والجرائم العادية وهو إمكانية التسليم في هذه الأخيرة، لا يطبق هنا؛ إذ بالرجوع إلى العرف الدولي نجد أنه يجري على عدم التسليم لا في جريمتي التجسس أو الخيانة العظمى فحسب بل حتى في جرائم القانون العام المتصلة بها لتعذر فصلها، بينما يذهب بعض الفقهاء إلى رفض الرأي القائل بعدم جواز تسليم الجاسوس إذا ما إلتجأ لدولة لا مصلحة لها في خدماته لأن الأسباب التي دعت الفقهاء إلى مراعاة حماية المجرم السياسي لا يمكن أن تنطبق في حالة الجاسوس[4].

---

[1]– سعد إبراهيم الأعظمي، مرجع سابق، ص. ص. 57– 58.

[2]– عبد الفتاح مصطفى الصيفي، مرجع سابق، ص. 28.

[3]– أحسن بوسقيعة، الوجيز في القانون الجزائي العام، مرجع سابق، ص. 34.

[4]– سعد إبراهيم الأعظمي، مرجع سابق، ص. 64.

كخلاصة لتطور التجسس التقليدي يمكن القول بأنه عرف تغيرات على مستوى المفهوم والمعالجة القانونية؛ فبعد أن كان في ظل القانون الروماني وتحديداً في ظل ما عرف بالجرائم الماسة بالعظمة أو الجلالة يعاقب تحت وصف الخيانة العظمى، وجد ذاتيته المستقلة عنها في ظل القوانين التي أسهمت الثورة الفرنسية في نشوئها وأصبح يعد أحد الجرائم الماسة بأمن الدولة الخارجي.

المطلـــب الثانـــي: أثـــر التطور التقنـــي فـــي ظهور التجـــسس الإلكترونـــي.

ليس هناك أشق على الباحث من تأريخ الأفكار؛ لأن الفكرة لا تولد فجأة ولكنها تتكون عبر الزمان، فتحديد مبدئها ومنتهاها إذن أمر غير مستطاع وإذا تم فإنما يتم إعتماداً على عرض إستنتاج مبناه المظاهر الخارجية للفكرة وليس الفكرة ذاتها[1]، وفي حالة التجسس الإلكتروني شأنه شأن كل المصطلحات التي تجد مصدرها في العلوم التكنولوجية بعيداً عن العلوم الإنسانية فإن الفكرة مبهمة ومظاهرها الخارجية تتطلب العودة لمنشأ وكذا لتطور التقنيات التي منحت للتجسس وصفه الإلكتروني، وفي هذا السياق يمكن تحديد مرحلتين أساسيتين مرت بهما هذه التقنيات لتصل إلى الشكل المعروفة به حاليا؛ حيث شهدت المرحلة الأولى طفرة على مستوى وسائل الإتصال وهذه المرحلة اصطلح على تسميتها بثورة الاتصالات الأولى، ثم شهدت المرحلة الثانية ظهور الحاسوب وظهور شبكة الأنترنت كوسيلة للاتصال الحديث والربط بين مختلف الحواسيب، سميت بالثورة المعلوماتية، هاتين الثورتين اللتين شملتا كل دول العالم ومنها الجزائر أثرتا بشكل كبير على طرائق إرتكاب التجسس؛ وتبعاً لذلك ستتم دراسة هذا المطلب من خلال ثلاثة فروع: يتناول الفرع الأول مرحلة ثورة الإتصالات، ويتناول الفرع الثاني مرحلة الثورة المعلوماتية، بينما سيخصص الفرع الثالث لانعكاسات التطور التقني على المنظومة القانونية في الجزائر.

الفـــرع الأول: مرحـــلة ثـــورة الإتصـــالات.

بدايةً يعرف الإتصال بأنه: إنتقال المعلومات من جهة إلى جهة أخرى بواسطة الكلمة أو الكتابة أو الإشارة، ويندرج تحته نقلها بالصور، وسُمي هذا النوع بالإتصال المرئي، وكذلك يدخل فيه نقل المعلومات باستخدام الأجهزة الكهربائية – السلكية واللاسلكية – نحو الإتصال الهاتفي والبريد الإلكتروني والاتصال عبر الأقمار الصناعية، بينما عرف الإتحاد الدولي للإتصالات السلكية واللاسلكية الإتصالات

[1]– محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 20.

بأنها: عمليات تساعد المرسل على إرسال المعلومات بأية وسيلة من وسائل النظم الكهرومغناطيسية من تلفون أو فاكس أو تلكس أو بث إذاعي أو تلفزيوني أو غير ذلك[1].

لاشك أن الإنسان قد أثبت حاجته في كل الأزمنة للتواصل؛ فالرومانيون مثلاً استخدموا الإشارات الليلية بواسطة النار من على المرتفعات، ودول أخرى تواصلت بواسطة الحمام الزاجل، لتظهر فيما بعد طرق التشفير من أجل جعل الرسائل غير مفهومة في حالة التقاطها من طرف الأعداء، وخلال النهضة ازدهرت كل أشكال طرق التشفير، لكن بالموازاة مع ذلك تم إتهام المشفرين بالشعوذة[2]. وقد حصلت ثورة الإتصالات الأولى بإختراع صموئيل مورس جهاز التلغراف السلكي عام 1837، وهذا الجهاز هو أولى الوسائل التي استخدمها الإنسان لنقل الرسائل بالإشارات الكهربائية (ولما كانت الإشارات الكهربائية تنتقل بسرعة تقارب سرعة الضوء سُمي التلغراف بالبرق باللغة العربية)[3]؛ بحيث شهد عام 1844 إرسال أول رسالة تحملها وسيلة إتصال وذلك عبر خط لاسلكي للتلغراف كان طوله سبعون كيلومترا، وكان الإرسال من تيار مباشر وكان المرسل هو المخترع صموئيل مورس، وقد بدأ هذا الإختراع في الإنتشار وتعددت الجهات التي وظفته كي تسهل أعمالها، وقد تجاوز إمتداد هذا الإختراع حدود الولايات المتحدة الأمريكية إلى بلدان أوروبا ولكن في إطار شبكات محلية بسبب عدم توافق الأنظمة القومية المختلفة حيث كانت الخطوط التلغرافية تنتهي في حدود الدولة المرسلة الأمر الذي ألجأ المستخدمين للوسائل التلغرافية المرسلة للدولة المجاورة إلى تسليم الرسالة في حدود الدولة ثم حملها باليد إلى الطرف الأخر حتى تبدأ رحلة جديدة[4]. ومنذ إندلاع الحرب الأهلية في الولايات المتحدة الأمريكية كانت خطوط التلغراف هدفا مهما للقوات المتحاربة إذ كان عمال الإشارة يتداخلون على خطوط المواصلات السلكية عن طريق توصيل

---

[1]– تنوير أحمد بن محمد نذير، حق الخصوصية (دراسة مقارنة بين الفقه الإسلامي والقانون الانجليزي)، أطروحة دكتوراه في الفقه الإسلامي، مقدمة لكلية الشريعة والقانون، الجامعة الإسلامية العالمية بإسلام أباد، 2007، ص. ص.240–241.

[2]-Daniel TANT, guerre électronique et chiffrement, association des réservistes de chiffre et de la sécurité de l'information(ARCSI), France, publié sur le site www.arcsi.fr, le site a été visité le: 23/11/2015.

[3]– تنوير أحمد بن محمد نذير، مرجع سابق، ص. 247.

[4]– عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، مصر، 2011، ص. 7.

هاتف على التوازي مع كل خط من هذه الخطوط للتنصت على المحادثات[1]، وقد سهل هذه العملية إختراع الهاتف سنه 1876 من طرف الكسندر غراهام بل "Alexander Graham Bell"، وسرعان ما صار الهاتف من أهم أدوات الإتصال لا على صعيد الأقاليم فحسب بل على صعيد العالم كله[2]، وفي سنة 1888 تمكن العالم "هرتز H. Hertz " من التوصل إلى الموجات الكهرومغناطيسية و دراستها؛ وبفضلها أصبح التقاط الموجات سهلا سنة 1890 وذلك بفضل جهاز التقاط الترددات الكهربائية للعالم" برانلي Branly"، ليقوم العالم "بوبوف A.S Popov" بإختراع الهوائي سنة 1895؛ والذي سمح للمخترع "ماركوني Marconi" في نفس العام من التمكن من نقل الإشارات الراديو كهربائية أو ما يعرف بإشارة المورس "les signaux de T.S.F" وذلك على بعد عشرات الكيلومترات[3]؛ فظهرت بذلك أجهزة الإتصال اللاسلكية؛ ونتيجة لتزايد استخدام اللاسلكي كان طبيعياً أن تظهر الشوشرة على الإتصالات اللاسلكية والتي كانت في البداية طبيعية نتيجة لما يعرف بالتداخل البيني للموجات الكهرومغناطيسية، ليتم فيما بعد الاستخدام المتعمد للشوشرة لإعاقة الإتصالات اللاسلكية بين الوحدات العسكرية المعادية لإرباكها وشل سيطرتها على قواتها وأسلحتها، ولتستخدم التقنيات اللاسلكية في أعمال الاستطلاع اللاسلكي على شبكات العدو اللاسلكية بهدف الحصول على المعلومات، كما استخدمت في تطوير تجهيزات لتحديد مواقع السفن والطائرات وذلك خلال الحربين العالميتين الأولى والثانية[4]، لتسمح فيما بعد الخلايا الكهروضوئية المخترعة من طرف العالم"ك.ف برون K.f Braun" ببروز العديد من التجهيزات كالسينما الناطقة والتلفزيون، والأهم ببروز الرادار. وحالياً تمثل النواقل النصفية والترونزيستورات المكتشفة من طرف كل من "ج. باردين J. Bardeen" و" و.هـ براتان W.H Bratain "، و" و. شوكلي W. Shockley " التطور التكنولوجي الذي يتحكم في تطور مجال الإلكترونيات؛ بحيث أدت التحديثات المدخلة عليه إلى ظهور الرقاقات المعالجة "les microprocesseus" التي تمثل الآن قاعدة الصناعات الإلكترونية والوسائط الحديثة؛ بحيث يتوسع حالياً مجال تطبيق الإلكترونيات إلى عديد التقنيات كالحواسيب والاتصالات ومعالجة الإشارة والأتمتة...[5].

---

[1]– بشرى حسين الحمداني، مرجع سابق، ص. 101.

[2]– تنوير أحمد بن محمد نذير، مرجع سابق، ص. 248.

[3]-Yves Garnier, op. cit, p. 525.

[4]– بشرى حسين الحمداني، مرجع سابق، ص. 101–104.

[5]-Yves Garnier, op. Cit, p. 525.

الفـــرع الثانـــي: مرحـــلة الثـــورة المعلوماتيـــة.

في نهاية القرن العشرين إجتاحت العالم ما أطلق عليه الثورة المعلوماتية، وقد وصفت هذه الثورة بالموجة التطورية الثالثة؛ إنطلاقاً من كونها يمكن أن تقود إلى إدخال المجتمعات الإنسانية في حيز متطور قائم على محورية المعرفة والمعلومات، ولا تقتصر ثورة المعلومات الحالية على شق التطور الهائل الذي طرأ على تقانة المعلومات التي يلعب الحاسوب الآلي الدور الرئيس فيها بل يقترن بها التطور المصاحب في تقانة الإتصالات؛ ولذا فإن هناك من يطلق إصطلاح "المعلواتصالية" لوصف هذا التطور المعلوماتي[1]؛ وعليه فالثورة المعلوماتية قوامها الحاسب الآلي ووسائل الإتصالات الحديثة على رأسها الأنترنت، هذه الوسائل التي أصبحت حاليا جوهر التجسس الإلكتروني.

يعرف الحاسوب بأنه: "جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات بطريقة ما وذلك بتنفيذ عمليات ثلاث أساسية هي إستقبال البيانات المدخلة (الحصول على الحقائق المجردة)، ومعالجة البيانات إلى معلومات (إجراء الحسابات والمقارنات ومعالجة المدخلات)، وإظهار المعلومات المخرجة (الحصول على النتائج)"[2]، وقد عرف الحاسوب بإعتباره آلة عدة تغيرات، بحيث أن أول كمبيوتر كان سنة 1946 وكان يتكون من أكثر من 18000 صمام إلكتروني وكان حينها يحتل بناية كاملة ويزيد وزنه عن ثلاثين طنا وكانت تلك البناية في حاجة لأجهزة تبريد عملاقة لإزالة الحرارة الناجمة عن تلك الصمامات الإلكترونية، ومع ذلك فإن فعاليته لم تكن أكثر من فعالية آلة حاسبة صغيرة مما يستعملها تلاميذ المدارس الآن[3]، ليخضع للعديد من التعديلات والتطويرات إبتداءاً من سنة 1951، وذلك بظهور الجيل الأول من الحواسيب إلى غاية الأجيال المعاصرة منه التي تقوم على خصائص، أهمها محاكاة الدماغ البشري والتشبه به، وتتركز تقنياتها على مفاهيم الشبكات العصبية والمعالجة المتوازية؛ حيث تستطيع هذه الحاسبات التعامل مع المعلومات بسرعة تتعدى سرعات حاسبات الأجيال السابقة بآلاف المرات ويمكنها تفسير الكلام البشري وتشخيص الأجسام والصور بالأبعاد الثلاثية، بمعنى أن الشبكة العصبية مبنية على عدد من المعالجات المتداخلة والمترابطة مشابهة

[1]– ثامر كامل محمد، تداعيات عاصفة الأبراج (الإستراتيجيات الدولية في عصر العولمة)، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2002، ص. 115.

[2]– نهلا عبد القادر المومني، مرجع سابق، ص. 20.

[3]– عبد الصبور عبد القوي علي المصري، الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، مصر، 2008، ص. 13.

للخلايا العصبية في الدماغ، أما تقنيات المعالجة المتوازية فهي عنصر من العناصر المهمة الأخرى؛ حيث أصبح بالإمكان معالجة من خمسة إلى خمسة عشر بليون عملية حسابية في الثانية وذلك بوضع أكثر من ست مئة معالج دقيق تعمل بشكل متواز لمعالجة البيانات والإيعازات المطلوبة[1].

أما الأنترنت فتعرف على أنها: "شبكة عالمية دولية ووسيلة من وسائل الإتصال والتواصل بين الشبكات تجمع مجموعة من أجهزة الحاسب الآلي المرتبطة ببعضها إما عن طريق خطوط الهاتف أو الأقمار الصناعية"[2]، وتستخدم الأنترنت كإختصار لمصطلح الشبكة العالمية للمعلومات، وتعني بذلك مجموعة لامتناهية من الحاسبات الآلية المرتبطة معاً بوسيلة إلكترونية عبر العالم لتبادل البيانات والمعلومات بأشكالها المختلفة[3]. ومن أهم خصائص الأنترنت التي تمتاز بها عن غيرها من وسائل الإتصالات، كونها غير مملوكة لأحد ومن ثم ليس لها إدارة أو مركز رئيس على الإطلاق؛ وذلك لأن الأنترنت يدار من تشكيلة من آلاف شبكات الكمبيوتر التابعة للشركات والأفراد كل منهم يقوم بتشغيل جزء منها كما يدفع تكاليف ذلك، وكل شبكة تتعاون مع الأخرى لتوجيه حركة مرور المعلومات حتى تصل لكل منهم وبمجموع هؤلاء تتكون الأنترنت، وقد كان هذا المبدأ أي اللامركزية الباعث الحقيقي لإنشاء الأنترنت؛ فلما كانت الحرب الباردة قائمة بين الولايات المتحدة الأمريكية والإتحاد السوفياتي سابقاً فكرت وزارة الدفاع الأمريكية في إنشاء نظام إتصالات يبقى محفوظا عن التوقف عند وقوع الكوارث ولاسيما عند الهجوم النووي، فقررت الوزارة أن تنشأ نظاماً جديداً للإتصال لا تكون له البداية ولا النهاية علاوة على هذا لا يكون له مركز رئيسي[4]، وعليه قامت وزارة الدفاع الأمريكية في عام 1969 بإنشاء وكالة الأبحاث المتقدمة "ARPA" فكانت النتيجة شبكة الأربانت " ARPANET" التي ربطت بين مراكز الحواسيب المختلفة وأنظمة الراديو والأقمار الصناعية الخاصة بالولايات المتحدة في كل أنحاء العالم، ثم تطور المشروع إلى الإستعمال السلمي خاصة من قبل الجامعات؛ ونظراً للازدحام الكبير الذي كان يميز الشبكة فقد تم تقسيمها إلى قسمين؛ فظهرت شبكة الميلنت" MILNET" للأغراض العسكرية فقط [5]، ثم ظهرت الحاجة الماسة إلى إستخدام نفس الشبكات لأغراض تجارية يستفيد منها الأفراد

[1]– نهلا عبد القادر المومني، مرجع سابق، ص. 33.

[2]–عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، مرجع سابق، ص. 22.

[3]– جلال محمد الزعبي وأسامة أحمد المناعسة، مرجع سابق، ص. 32.

[4]– تنوير أحمد بن محمد نذير، مرجع سابق، ص. 249.

[5]– نهلا عبد القادر المومني، مرجع سابق، ص. 37.

والمؤسسات والشركات رغم عدم إرتياح مؤسسة العلوم القومية الأمريكية وبعض العاملين بالشبكات الرسمية لهذا التطور، إلا أن الشركات استطاعت من خلال نفوذها في الحكومة الفيدرالية ودوائر الحكومة الأمريكية أن تفتح المجال للإستخدام التجاري للشبكة محلياً وعالمياً إبتداءاً من سنة 1993[1].

أدت التطورات التقنية السابقة إلى إدخال تغييرات عميقة في مفهوم الجرائم فبرزت للوجود طائفة الجرائم الإلكترونية التي لم تكن تحظى بذات الإهتمام المشهود حاليا؛ بحيث ظهرت أولى المعالجات لما يسمى جرائم كمبيوتر في الستينات، والتي اقتصرت على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي والاستخدام غير المشروع للبيانات المخزنة في نظم الكمبيوتر، وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شيء عابر أم ظاهرة جرمية مستجدة، بل وثار الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة الحوسبة وبقي التعامل معها أقرب إلى النطاق الأخلاقي. ومع تزايد إستخدام الحواسيب الشخصية ظهرت الدراسات المسحية والقانونية التي إهتمت بجرائم الكمبيوتر، وفي الثمانينات طفا إلى السطح مفهوم جديد لجرائم الكمبيوتر ارتبط بعمليات إقتحام نظم الكمبيوتر عن بعد وأنشطة نشر الفيروسات الإلكترونية، وشاع إصطلاح الهاكرز المعبر عن مقتحمي النظم لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل في غالب الأحيان محصوراً بالحديث عن رغبة المخترقين في تجاوز إجراءات أمن المعلومات وفي إظهار تفوقهم التقني، وأنحصر الحديث عن مرتكبي هذه الأفعال بالحديث عن صغار السن من المتفوقين الراغبين في التحدي والمغامرة[2].

ويرجع إمتداد تاريخ ظهور الهاكرز كأحد الفواعل الدولية الحالية في مجال التجسس الإلكتروني إلى ما قبل سنة 1969 حيث لم يكن للكمبيوتر وجود ولكن كانت هناك شركات الهاتف والتي اعتبرت المكان الأول لظهور الهاكرز، فبالعودة لسنة 1878 في الولايات المتحدة الأمريكية وتحديداً في إحدى شركات الهاتف المحلية أين كان أغلب العاملين في تلك الفترة من الشباب المتحمس لمعرفة المزيد عن هذه التقنية الجديدة والتي حولت مجرى التاريخ، فكان هؤلاء الشباب يستمعون ويتنصتون على المكالمات التي تجرى في هذه المؤسسة وكانوا يغيرون الخطوط الهاتفية؛ فتجد مثلا المكالمة الموجهة إلى السيد مارك تصل إلى السيد جون وكل هذا كان بغرض التسلية لتعلم المزيد؛ لهذا قامت الشركة بتغيير الكوادر

[1]– عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، مرجع سابق، ص. 24.

[2]– يوسف حسن يوسف، الجرائم الدولية للأنترنت، المركز القومي للإصدارات القانونية، مصر، 2011، ص. 20.

العاملة بكوادر نسائية[1]، وهو الاتجاه الذي عم في تلك الفترة، لكن الهاكرز كمصطلح كان يحمل معن مختلف تماماً عما يحمله هذه الأيام؛ فقد بدأت كصفة تشير إلى عبقرية مبرمجي الكمبيوتر وقدرتهم على إبتكار أنظمة وبرامج حاسوب أكثر سرعة، ومن أشهر من إكتسب هذه الصفة "دينيس ريتش" و"كين تومسون" اللذان صمما برامج اليونكس عام 1969، أما الهاكرز بالمفهوم السيئ فلم يكن لهم وجود قبل عام 1981 وهو تاريخ ظهور أول حاسوب شخصي من إنتاج شركة"IBM"؛ ذلك أن عملية القرصنة الإلكترونية كانت غاية في الصعوبة لعدة أسباب منها أن النُسخ الأولى للحواسيب كانت ضخمة وتحتاج إلى غرف كبيرة ذات درجات حرارة ثابتة. وفي بادئ الأمر عُرف قراصنة الكمبيوتر بالكراكرز كوصف لمجموعة الأشرار الذين يلجأون إلى حواسيب الآخرين منتهكين خصوصيتهم، وكذلك تمييزاً لهم عن الهاكرز وهم الأخيار، لكن مع مرور الزمن أصبح اللفظ يطلق على الفريقين دون تمييز وأصبحت العبرة بشيوع اللفظ لا بما كان يشير إليه[2]، وتبلورت فكرة المجرم الإلكتروني المتفوق المدفوع بأغراض جرمية خطيرة القادر على إرتكاب أفعال تستهدف الاستيلاء على المال أو تستهدف التجسس والاستيلاء على البيانات السرية الاقتصادية والاجتماعية والسياسية والعسكرية، وشهدت التسعينات من القرن الماضي تنامياً هائلاً في حقل الجرائم التقنية وتغيراً في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته الأنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات[3]، وفي المقابل بدأت تبرز أهمية بعض المجالات في التصدي للجريمة الإلكترونية وتحتل المكانة الأساسية الواجبة لها بعد أن كانت من آخر الاهتمامات، أبرز هذه المجالات مجال الأمن المعلوماتي؛ إذ في البداية لم يكن ثمة إهتمام بمسائل الأمن بقدر ما كان الإهتمام ببناء الشبكة وتوسيع نشاطها؛ ولهذا لم يتم بناء الشبكة في المراحل الأولى على نحو يراعي تحديات أمن المعلومات فالإهتمام الأساسي تركز على الربط والدخول ولم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة، بيد أن النظرة تغيرت تماما في 1988/11/02 ويرجع ذلك إلى حادثة موريس الشهيرة؛ فقد إستطاع الشاب "موريس" أن ينشر فيروساً إلكترونياً عُرف بدودة موريس مكن من مهاجمة آلاف الكمبيوترات مستفيداً من ثغرات الأمن الموجودة فيها وقد تسبب في أضرار بالغة أبرزها وقف آلاف الأنظمة عن العمل وتعطيل وإنكار الخدمة؛ وهو ما أدى إلى لفت النظر إلى حاجة شبكة

[1]– عبد الصبور عبد القوي علي المصري، مرجع سابق، ص. 55.

[2]– بشرى حسين الحمداني، مرجع سابق، ص. 12.

[3]– يوسف حسن يوسف، مرجع سابق، ص. 21.

الأنترنت إلى توفير معايير الأمن، وبدأ المستخدمون يفكرون ملياً في الثغرات ونقاط الضعف، وتضاعفت بعد تلك الحادثة الهجمات المستهدفة للشبكة واحتلت واجهات الصحف عناوين رئيسية حول أخبار هذه الهجمات والخسائر الناجمة عنها، وهي الهجمات التي تستهدف تعطيل النظام عن العمل من خلال ضخ سيل من المعلومات والرسائل تؤدي إلى عدم قدرة النظام المستهدف على التعامل معها أو تجعله مشغولاً وغير قادر على التعامل مع الطلبات الصحيحة، وشاعت أيضا الهجمات المعتمدة على الأنترنت نفسها لتعطيل مواقع الأنترنت، وقد تعرضت كل من وكالة المخابرات الأمريكية ووزارة العدل الأمريكية والدفاع الجوي الأمريكي والناسا وغيرها من الهيئات الحساسة لهجمات من هذا النوع؛ هذه التغيرات في وسائل الهجوم وحجم الأضرار الناجمة عنها أظهر الحاجة إلى التفكير بخطط الأمن مع مطلع التسعينات للدفاع عن النظم ومواقع المعلومات وبدأت تظهر مع بداية التسعينات وسيلة الجدران النارية كإحدى وسائل الأمن المعلوماتي والتي تطورت بالإضافة إلى غيرها من وسائل الحماية بشكل ملفت[1].

بالموازاة مع الآثار المترتبة عن الثورة التكنولوجية الحديثة على مستوى المفاهيم بظهور الجريمة الإلكترونية وما استتبعها من مصطلحات وتعدد للوسائط الإلكترونية التي يمارس عبرها التجسس الإلكتروني؛ فقد أدت ذات التطورات المرتبطة أساساً بالقدرة على التصنيع والأبحاث العلمية المتعلقة بهذه التكنولوجيات وبما تمثله من رأس مال ضخم أصبحت معه محل أطماع من قبل الدول والكيانات الأخرى أكثر من أي وقت مضى، إلى تغير في سلم ترتيب أولويات الأمن في الدولة في العصر الإلكتروني، وبذلك تغير موقع مجالات التجسس وفقاً لذلك، فإذا كان الأمن يقوم على عدة أبعاد جرى الاتفاق على تقسيمها إلى العناصر الآتية:

- **البعـد العسكـري:** وهو البعد الذي لطالما اقترن بمفهوم أمن الدولة أو الأمن القومي، ويعني التحرر من التهديد العسكري[2].

- **البعـد السياسـي:** ويتمثل في الحفاظ على الكيان السياسي للدولة.

- **البعـد الاقتصـادي:** ويعني توفير المناخ المناسب للوفاء باحتياجات الشعب وتوفير سبل التقدم والرفاهية.

---

[1]- جعفر حسن جاسم الطائي، مرجع سابق، ص. 122.

[2]- معمر بوزنادة، المنظمات الإقليمية ونظام الأمن الجماعي، ديوان المطبوعات الجامعية، الجزائر، 1992، ص. 16.

– **البعـد الاجتماعـي:** ويعني توفير الأمن للمواطنين بالقدر الذي يزيد من تنمية شعور الشعوب بالإنتماء والولاء.

– **البعـد الإيديولوجـي أو المعنـوي:** ويعني تأمين الفكر والمعتقدات والحافظة على العادات والتقاليد والقيم[1].

وكما سبق القول، إذا كان الأمن يقوم على الأبعاد السالفة ورغم الترابط الكبير بينها إذ لا يمكن تحقيق بعد بدون أو على حساب بعد آخر، إلا أن الراجح حالياً إحتلال الأمن الاقتصادي الصدارة بين الأبعاد الأخرى على حساب البعد التقليدي المهيمن سابقاً ألا وهو البعد العسكري.

إن العلم والتطور التكنولوجي الذي له إنعكاس على طرائق ممارسة التجسس لا يتوقف عند حدود؛ فقد شهد العالم في الآونة الأخيرة ثورة صناعية لا تماثلها ثورة أخرى سميت بتكنولوجيا التصغير اللامتناهي (أو ما يعرف بتكنولوجيا النانو)، والتي يوحي إسمها بصناعة أجهزة كانت في السابق تحمل حيزا كبيراً فأصبحت بفضل هذه التكنولوجيا لا ترى بالعين المجردة؛ والسر يكمن في أن هذه الصناعة لا تقوم على الذرة كمقياس تقليدي وإنما تقوم على مقياس النانو، وأصبحت حالياً الدول الصناعية تضخ الملايين من الدولارات من أجل تطوير التكنولوجيا النانوية، ويذهب الدارسون في إطار تعريف هذه الأخيرة إلى القول بأنها عبارة مؤلفة من شطرين: الشطر الأهم فيها هو النانو، هذا الأخير يعد أدق وحدة قياس مترية معروفة حتى الآن (النانو متر) وهو يساوي واحد على مليار من المتر، أما العبارة ككل "التكنولوجيا النانوية" فإنها تعني حرفيا تقنيات تصنيع على مقياس النانو متر، وهي علم تعديل الجزيئات أو الذرات لصنع منتجات جديدة، أو أنها التطبيق العلمي الذي يتولى إنتاج الأشياء عبر تجميعها على المستوى الصغير من مكوناتها الأساسية مثل الذرة والجزيئات، ومادامت كل المواد مكونة من ذرات مرتصفة وفق تركيب معين؛ فإننا نستطيع أن نستبدل ذرة عنصر ونرصف بدلها ذرة لعنصر آخر، وهكذا نستطيع صنع شيء جديد ومن أي شيء تقريباً وبأي مواصفات يريدها الشخص، أو إيجاد أشياء بمواصفات ليست موجودة في الطبيعة مع إختصار الوقت والتكلفة وزيادة في الأداء، ويعتبر مجال التجسس المجال الخصب لتقنية النانو بحيث أن هذه التكنولوجيا لديها القدرة على تعزيز أجهزة المراقبة بشكل كبير بفضل حجمها الصغير مثل الكاميرات والميكروفونات، كما لهذه التكنولوجيا أن تحضر جيشاً

[1]– جمال علي زهران، مرجع سابق، ص. ص. 13–14.

من الجراثيم على شكل آلات متناهية في الصغر توجه من ممرات الهواء إلى أجهزة الكمبيوتر وتسيطر بذلك على جميع المعطيات الآلية دون أن يشعر بها أحد وتعد هذه من أدوات التجسس المعلوماتي عن طريق الإختراق الآلي[1].

الفـــرع الثالـــث: إنعكاســات التطـور التقني على المنظومـة القانونية فـي الجزائـــر.

لم تكن الجزائر شأنها شأن سائر دول العالم بمنأى عن التطورات الحاصلة على مستوى التقنية، حيث عملت الجزائر على الاستفادة من خدمات شبكة الأنترنت ومختلف التقنيات المرتبطة بها من خلال إرتباطها بشبكة الأنترنت في مارس 1994 عن طريق مركز البحث العلمي والتقني "CRIST" الذي تم إنشاءه من طرف وزارة التعليم العالي والبحث العلمي في مارس 1986، وكان من مهامه الأساسية إقامة شبكة وطنية وربطها بشبكات إقليمية ودولية، ويرجع الدور الأساسي في إنتشار شبكة الأنترنت في البداية لهذا المركز بإعتباره تنظيم حكومي تولى مسؤولية ترقية واستعمال المعلومات العلمية والتقنية وإهتم بدعم تكنولوجيا الإتصال والمعلومات في الجزائر، كما تكفل بتطبيق مشاريع مغاربية في إطار شراكة مع بعض الدول في شمال إفريقيا بالإضافة إلى ذلك استفاد المركز من تجهيزات للربط بالأنترنت ومن برامج لتكوين المستخدمين الذين يقومون بتنظيم الاشتراك من خلال المركز ليغطي مؤسسات مختلفة في القطر، وكحلقة في مراحل تطور الأنترنت جاء المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت سنة 1998 المتعلق بضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها والمعدل بموجب المرسوم التنفيذي رقم 2000-307 المؤرخ بتاريخ 14 أكتوبر سنة 2000 من أجل تحديد المعايير والشروط المتعلقة بكيفيات وضع الأنترنت والاستفادة من خدماتها، وقد تميزت هذه المرحلة ببروز مزودين آخرين في قطاعات عامة وخاصة تتقاسم مهمة التزويد بالأنترنت مع مركز البحث العلمي والتقني؛ وهو ما أدى إلى تطور في عدد مستخدمي الشبكة[2]. كما سعت الجزائر إلى بناء مجتمع المعلومات ودعمه وتطويره، وفي هذا الإطار ركزت مطالب الجزائر في المنتدى العالمي لسياسات الإتصالات بالجزائر في أفريل سنة 2009 على

[1]- صبرينة بن سعيد، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا "الإعلام والاتصال"، أطروحة دكتوراه في القانون الدستوري، مقدمة لقسم الحقوق بكلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2014-2015، ص. ص. 99- 103.

[2]- عبد الكريم عاشور، دور الإدارة الإلكترونية في ترشيد الخدمة العمومية في الولايات المتحدة الأمريكية والجزائر، مذكرة ماجستير في العلوم السياسية والعلاقات الدولية، مقدمة لقسم العلوم السياسية والعلاقات الدولية بكلية الحقوق والعلوم السياسية، جامعة منتوري، قسنطينة، 2009-2010، ص. ص.117- 120.

ضرورة نقل المعرفة والخبرة لصالح البلدان النامية التي هي بأمس الحاجة لتحسين مستواها بهدف إقامة مجتمع معلومات عالمي شامل وبالتالي سعت الجزائر إلى وضع لجنة قيادة مجتمع المعلومات هدفها البحث عن آفاق تنمية التكنولوجيا في الجزائر والتي تتكون من مختلف القوى المؤثرة في هذا المجال للتأكيد على العمل المشترك بما يخدم أهداف السياسة الوطنية[1]، ومن جهة ثانية فقد تم فتح المجال أمام متعاملي الهاتف النقال لوضع البنى الأساسية لاستغلال تقنيات الأجيال الجديدة من الهواتف المحمولة بما يسمح بتطوير الربط بالأنترنت للأفراد؛ حيث تم في هذا الإطار وبتاريخ 02 ديسمبر من سنة 2013 توقيع مراسيم تنفيذية حول رخص استغلال الجيل الثالث لمتعاملي الهاتف النقال.

لقد سعت الجزائر إلى تطوير بنيتها المعلوماتية خاصة من خلال نشر استخدام تكنولوجيا المعلومات والاتصالات فاحتلت بذلك جزء من الفضاء الإلكتروني؛ ومن تداعيات هذا أن أصبحت الجزائر وكباقي الدول عرضة لتهديدات الجريمة الإلكترونية؛ مما دفع المشرع إلى تعديل النصوص القانونية القائمة، وكذا وضع مجموعة من النصوص القانونية الجديدة التي تهدف إلى محاولة التصدي لهذا الصنف المستحدث من الجرائم، ويمكن استعراض ذلك فيما يلي:

أولاً- تعديـل قانـون العقوبـات:

قام المشرع الجزائري بتجريم ما سماه بـ" المساس بأنظمة المعالجة الآلية للمعطيات " وذلك بتعديل قانون العقوبات في سنة 2004، وهذا باستحداث القسم السابع مكرر المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات[2] من الفصل الثالث المعنون بالجنايات والجنح ضد الأموال، بحيث نص على مضاعفة العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام وذلك دون الإخلال بتطبيق عقوبات أشد[3]. ولقد جاء في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام؛ مما دفع بالكثير من الدول إلى النص على معاقبتها، وأن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية، وأن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات، وسوف تُمكن لا محالة من مواجهة بعض أشكال الإجرام

[1]- عبد الكريم عاشور، مرجع سابق، ص. 129.

[2]- راجع الوارد في هامش الصفحة 23 من هذه الرسالة.

[3]- المادة 394 مكرر3 من قانون العقوبات.

الجديد[1]. وتجدر الإشارة أن مواجهة جرائم الإعتداء على نظم المعالجة الآلية كانت إحدى بنود إتفاق يؤسس للشراكة بين الجزائر والإتحاد الأوروبي الذي عقد بتاريخ 22 أفريل سنة 2002 والذي صادقت عليه الجزائر بموجب القانون رقم 2003- 1144 المؤرخ في 02 ديسمبر سنة 2003[2].

وتماشياً مع ما تم النص عليه في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المشار إليه أدناه من إلتزامات مفروضة على مقدمي الخدمات؛ ونظراً لإدراك المشرع الجزائري لأهمية تعاون هؤلاء في مكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بصفة عامة؛ فقد قام باستحداث المادة 394 مكرر 8 للقسم السابع مكرر الذي ينظم هذه الجرائم، وذلك بموجب القانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016 المتمم لقانون العقوبات؛ بحيث تتضمن هذه المادة تقرير الجزاء الذي يوقع على مقدمي الخدمات في حالة عدم قيامهم بالتدخل الفوري لسحب أو تخزين المحتويات التي تشكل جرائم منصوص عليها قانوناً أو جعل الدخول إليها غير ممكن، أو عدم القيام بوضع الترتيبات التقنية التي تسمح بسحب أو تخزين المحتويات التي تشكل جرائم منصوص عليها قانوناً أو جعل الدخول إليها غير ممكن[3]، وتظهر أهمية هذا النص خاصة في حالة جرائم التعامل غير المشروع في المعطيات سواء كانت هذه المعطيات صالحة لارتكاب جرائم التجسس الإلكتروني أو كانت متحصلة منها فهذه

---

[1]- نسيم سعيداني، آليات البحث والتحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة ماجستير في العلوم الجنائية، مقدمة لقسم الحقوق بكلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2013، ص. 41.

[2]- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، 2012، ص. ص. 16-17.

[3]- تنص المادة 394 مكرر8 من قانون العقوبات على: "دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساريي المفعول يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من (2.000.000 دج) إلى (10.000.000 دج) أو بإحدى هاتين العقوبتين فقط مقدم خدمات الانترنت بمفهوم المادة 2 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي لا يقوم رغم اعذراه من الهيئة الوطنية المنصوص عليها في القانون المذكور أو صدور أمر أو حكم قضائي يلزمه بذلك:

أ- بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا.

ب- بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة (أ) من هذه المادة أو لجعل الدخول إليها غير ممكن".

المعطيات تشكل تهديداً لأسرار الدفاع الوطني لذلك يلتزم مقدم الخدمات بالتدخل لسحبها أو تخزينها أو جعل الدخول إليها غير ممكن أو بوضع الترتيبات اللازمة لتحقيق هذه الغايات.

ثانيـاً- تعديـل قانـون الإجـراءات الجزائيـة:

تزامناً مع التعديل الذي عرفه قانون العقوبات بالنص على طائفة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؛ قام المشرع الجزائري في ذات التاريخ (أي في سنة 2004) بإدخال تعديلات على قانون الإجراءات الجزائية وذلك بالنص على بعض الأحكام الاستثنائية لمتابعة هذه الجرائم[1]، وتتعلق هذه الأحكام أساساً بتحديد قواعد الاختصاص المحلي بمتابعة طائفة محددة على سبيل الحصر ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، لكن اهتمام المشرع الجزائري بالمواجهة الإجرائية لهذه الجرائم توضح أكثر من خلال تعديل قانون الإجراءات الجزائية لسنة 2006[2]؛ بحيث قام من جهة بإدخال تعديلات جوهرية في إجراءات التحري والتحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات كتلك المتعلقة بشروط التفتيش خاصة الزمنية؛ وقام من جهة ثانية باستحداث إجراءات جديدة كما هو الشأن بالنسبة لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور وإجراء التسرب، ليشهد بعد ذلك تعديل قانون الإجراءات الجزائية في سنة 2015[3] إدخال أحكام جديدة مست كذلك الجرائم الماسة بأمن الدولة بصفة عامة، ويتعلق الأمر خاصة بالتعديلات الجوهرية التي عرفتها المادة 588 المنظمة لمفهوم وشروط إعمال مبدأ العينية؛ إذ وسع المشرع الجزائري من مجال هذا الإعمال ليشمل إضافة إلى جرائم أخرى كل جناية ضد أمن الدولة الجزائرية أو مصالحها الأساسية، كما تخلى فيها عن شرط تسليم المتهم الأجنبي للقضاء الجزائري لممارسة اختصاصه بنظر الجرائم المنسوبة إليه، وسيتم الرجوع إلى كل هذه الأحكام بالدراسة والتحليل في العناصر القادمة.

ثالثـاً- قانـون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهـا:

نظراً للتطور الكبير وغير المسبوق الذي عرفه العالم في مجال تكنولوجيات الإعلام والاتصال خلال السنوات الأخيرة، ونظراً لاتساع دائرة توفرها وانتشارها واستخدامها، مما قد يشكل خطراً على أمن

[1]- القانون رقم 04-14 المؤرخ في العاشر نوفمبر من سنة 2004 المتضمن تعيل الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية.

[2]- كان هذا التعديل لقانون الإجراءات الجزائية بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر سنة 2006.

[3]- كان هذا التعديل لقانون الإجراءات الجزائية بموجب الأمر رقم 15-02 المؤرخ في 23 يوليو من سنة 2015.

الدولة وعلى البنيات التحتية والمجالات الحيوية بمختلف أنواعها؛ فقد تطلب الوضع تحيين وتعزيز الحماية الجزائية لنظم المعالجة الآلية للمعطيات؛ فوجد المشرع نفسه مضطراً للتدخل مرة أخرى لمسايرة هذه التطورات لكن هذه المرة بإصدار قانون مستقل هو القانون رقم 09-04 المؤرخ في الخامس أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]. وأهم ما يميز هذا القانون أنه وسع من مفهوم الجرائم الإلكترونية والتي فضل تسميتها بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكما سبقت الإشارة إليه فالمشرع الجزائري قد حصر طوائفها من خلال النص في قانون العقوبات في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي تتألف في معظمها من الجرائم التي تستهدف هذه الأنظمة، ليعدل المشرع مفهومه لها بتتمتها بواسطة قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بطوائف الجرائم التي تستخدم تلك الأنظمة كوسيلة لارتكابها، هذا من جهة، ومن جهة ثانية يُعد هذا القانون قانوناً إجرائياً بالأساس؛ بحيث تضمن على وجه التخصيص النص على الإجراءات الحديثة في مجال التحري والتحقيق في الجريمة الإلكترونية ليضع بذلك حداً للمشكلات التي تمت إثارتها في شأن صلاحية الآليات الإجرائية التقليدية للتطبيق بشأنها، كمراقبة الاتصالات الإلكترونية، وتفتيش المنظومات المعلوماتية، وحجز المعطيات المعلوماتية، وحفظ المعطيات المتعلقة بحركة السير، واعتراض المعطيات المتعلقة بالمحتوى، ونص على تطبيق هذا القانون في حالة الجرائم الماسة بأمن الدولة وتلك التي تشكل تهديداً للنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، كما تضمن النص في الفصل الخامس منه على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته وأحال بشأن تحديد تشكيلتها وتنظيمها وكيفيات سيرها إلى التنظيم[2].

رابعـاً- المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهـا:

حيث جاء هذا المرسوم تطبيقاً للمادة 13 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وبحسب ذات المرسوم فإن هذه الهيئة هي سلطة إدارية مستقلة تتمتع

[1]- رشيدة بوكر، مرجع سابق، ص. 18.

[2]- أنظر المادة 13 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

بالشخصية المعنوية والاستقلال المالي تابعة لوزارة العدل[1]، وتلعب هذه الهيئة دوراً أساسياً في الوقاية من الجرائم الإلكترونية ومكافحتها، ويتمحور دورها أساساً على تعزيز ودعم الجهود الإجرائية الوطنية للوقاية من هذه الجرائم ومكافحتها بصورة عامة، وهذا يظهر من خلال المهام التي تضطلع بها، وأبرزها القيام باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بالإضافة إلى ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة وتطوير التعاون مع المؤسسات والهيئات الوطنية المعنيـة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والمساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال، وكذا المساهمة في تحديث المعايير القانونية في مجال اختصاصها[2].

إضافة إلى عينة القوانين السابقة هناك العديد من الأحكام الهامة التي يمكن استنباطها من قوانين أخرى وضعها المشرع الجزائري بغرض حماية أمن الدولة ومكافحة الجرائم الإلكترونية ومنها التجسس الإلكتروني، ومن أمثلة هذه القوانين نجد القانون المتعلق بالبريد وبالمواصلات السلكية واللاسلكية[3]، والمرسوم التنفيذي المحدد لقواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة[4]، والتي سيتم التطرق إليها لاحقا.

المبـــحث الثالـــث: صـــور التجـــسس الإلكترونـــي وأبعـــاده.

لعبت التطورات التي مست بشكل أساسي أساليب ممارسة التجسس من حيث توسيع نطاق انتشار واستخدام التكنولوجيات الحديثة للمعلومات والاتصالات لتشمل حتى الأفراد؛ دوراً مهما في بروز أنواع جديدة ومستحدثة من التجسس تضاف إلى الأنواع التقليدية التي كانت معروفة سابقاً، كما كان لمختلف

[1]– المادة 2 من المرسوم الرئاسي رقم 15–261 المؤرخ في 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]– المادة 4 من نفس المرسوم الرئاسي.

[3]– القانون رقم 2000–03 المؤرخ في 5 أوت سنة 2000 الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية

[4]– المرسوم التنفيذي رقم 09–410 المؤرخ في 10 ديسمبر 2009 يحدد قواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة

تلك التطورات إنعكاس ملحوظ على المفهوم العام للتجسس والمتعلق أساساً بشقي أو بُعديْ الأسباب الدافعة إليه والآثار المترتبة عليه؛ بحيث يتعلق الشق أو البعد الأول بإيجاد مبررات جديدة للقيام بالتجسس الإلكتروني، بمعنى ظهور أسباب إضافية للقيام به ترتبط تحديداً بالعصر الحالي وما ينطوي عليه من ظروف دولية مستجدة، بينما يتعلق الشق أو البعد الثاني بآثاره والتي كان أيضا للبيئة الدولية وللتكنولوجيات الحديثة دور هام في توسيعها؛ وعليه سيتم تقسيم هذا المبحث إلى مطلبين: يتناول المطلب الأول دراسة صور التجسس الإلكتروني، بينما يتناول المطلب الثاني دراسة أبعاد التجسس الإلكتروني.

المطلـــب الأول: صـــور التجـــسس الإلكترونـــي.

إن هدف عمليات التجسس هو الحصول على المعلومات، وكل الدول بدون استثناء بحاجة إلى الوصول إليها لأجل تكوين آرائها واتخاذ قراراتها وممارسة حقها في البقاء وإن كان يتعارض مع حق الدول الأخرى في السيادة، وتتنوع صور التجسس الإلكتروني تبعاً لموضوع هذه المعلومات من جهة، وتبعاً للوسيلة المتبعة للحصول عليها من جهة أخرى؛ وعليه سيتم التطرق في الفرع الأول لصور التجسس من حيث الموضوع، وفي الفرع الثاني لصور التجسس من حيث الوسيلة.

الفـــرع الأول: صـور التجـسس الإلكتروني من حيث الموضـوع.

تتعدد أنواع المعلومات التي تحتاجها الدولة مع الأخذ بالاعتبار كون هذه المعلومات قد شهدت تطوراً من حيث الأهمية وتوسعاً من حيث الأبعاد، حيث لم تعد فقط المعلومات العسكرية أو السياسية أو الدبلوماسية هي موضوع التجسس الأوحد والأهم، بل أضحت حاليا المعلومات الاقتصادية أكثر المعلومات طلباً، وهذا ما سيتم إبرازه في العناصر الآتية.

أولاً- التجـسس الإلكترونـي العسكـري:

ينصب التجسس الإلكتروني العسكري على المعلومات والأسرار ذات الصبغة العسكرية، ويعد هذا النوع من التجسس أقدم الأنواع على الإطلاق؛ بحيث ظلت الأسرار العسكرية ولفترة طويلة تمثل المحور الأساسي الذي ترتكز عليه فكرة الحماية الجنائية للدفاع الوطني أو الاستقلال السياسي للدولة؛ ومن ثم كانت المعلومات العسكرية تمثل الهدف الرئيس للتجسس في الماضي فعُد بذلك التجسس العسكري أقدم

الجرائم التي عرفتها التشريعات الجنائية في نطاق حماية كيان وأمن الدولة[1]، حتى إن البعض يجعل غاية التجسس الحصول على أكبر قدر من المعلومات السرية عن الجيش وسلاحه ومعداته وتدريبه وضباطه واستعداده وخطط أركان حربه في حالة وقوع حرب أو وشوك اندلاعها، وهو بذلك ينظر للتجسس ويعرفه من زاويته العسكرية[2]، وفي هذا الإطار يمكن تعريف السر العسكري محل هذه الصورة من التجسس بأنه: كل المعلومات أو الأشياء أو الفهارس أو الأساليب التي تتعلق بالشؤون العسكرية التي يجب أن تبقى متكتما عليها لاعتبارات الدفاع الوطني[3].

لطالما عُدت المؤسسات العسكرية من أهم مؤسسات الدولة وأبرزها استخداماً للمعلوماتية؛ وبالتالي كانت ومازالت مجالاً خصباً لمحاولات التجسس والاختراق نظراً لما يتوافر لدى العاملين فيها من معلومات تهم البلد[4]، وبالتالي يهدف التجسس العسكري إلى الحصول على المعلومات المتعلقة بالقدرة العسكرية لدولة ما، ويلاحظ هنا أن الحصول على المعلومات العسكرية يكون أكثر صعوبة في زمن السلم منه في زمن الحرب، وكذا الحصول على الخطط الحربية ومعرفة أصناف الأسلحة ونظم التعبئة ومستوى تدريب الأفراد ومعنوياتهم وروحهم القتالية وحتى المعلومات التي قد تبدو ثانوية مثل تاريخ حياة الضباط واهتماماتهم ودائرة أصدقائهم مطلوبة ضمن المعلومات العسكرية[5].

ومن الأمثلة على هذا النوع من التجسس ما حدث خلال حرب الخليج حيث استطاع خمسة متسللين من هولندا وذلك في الفقرة ما بين 1990 و1991 أن يخترقوا 34 نظاماً من أنظمة الكمبيوتر في مواقع الجيش الأمريكي على الأنترنت بما في ذلك المواقع التي كانت موجهة مباشرةً لعملية عاصفة الصحراء واستطاعوا تصفح الملفات فيها والبريد الإلكتروني والبحث عن الكلمات الأساسية والحساسة فيها واستطاعوا الحصول على معلومات عن مواقع دقيقة للقوات الأمريكية وأنواع الأسلحة التي تمتلكها تلك القوات وحركة السفن الحربية الأمريكية في منطقة الخليج، كما تمكنوا من نسخ معلومات عسكرية هامة وملء عدد من الاسطوانات المرنة بها، لدرجة أنهم عندما لم يجدوا متسعا للبيانات التي حصلوا عليها قاموا باختراق أجهزة الكمبيوتر في عدة جامعات وحملوا تلك المعلومات عليها، وقد حاول هؤلاء المتسللون

[1]– محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 246.

[2]– عدنان الخالدي، موسوعة أشهر جواسيس العالم، دار أسامة للنشر والتوزيع، الأردن، 2010، ص. 9.

[3]– محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. 246.

[4]– حسين بن سعد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، دار النهضة العربية، مصر، 2009، ص.378.

[5]– سعد إبراهيم الأعظمي، مرجع سابق، ص. 25.

بيع المعلومات التي تحصلوا عليها للعراق لكنها رفضت خشية أن يكون هذا فخاً لهم، ورغم قيام هؤلاء المخترقين بمسح كل آثار أنشطتهم من سجلات الأنظمة التي اخترقوها وذلك محاولة لإخفاء تسللهم إلا أنه تم تحديد هوياتهم، لكن الولايات المتحدة الأمريكية كانت عاجزة عن أن تقوم بأي عمل حيالهم؛ إذ لم تكن أعمال التسلل إلى شبكات الكمبيوتر غير قانونية في هولندا في ذلك الوقت، كما لم تنجح محاولات استدراج بعضهم إلى الولايات المتحدة الأمريكية للقبض عليهم[1].

ثانيـاً- التجـسس الإلكترونـي السياسـي:

يُقصد بالتجسس السياسي: "مراقبة أوضاع وسياسات الدول على الصعيد الداخلي والخارجي وذلك من خلال رصد تحركات ونشاطات القادة والزعماء والحكام والأحزاب والمنظمات السياسية والأمنية، واستطلاع مواقف زعماء الدول وقادتها السياسيين واتجاهاتهم ومبادئهم وآرائهم، كذلك يهدف التجسس السياسي إلى تقدير القوى المعنوية ومواطن الضعف في الأمة وعوامل الفرقة والإتحاد بين الأحزاب والمنظمات وطاقاتها"[2]، كما ينصب التجسس السياسي إضافة لطائفة المعلومات السابقة، على المعلومات المتعلقة بتقدير قوة الطوائف الدينية والقوميات والتركيبة الاجتماعية لكافة قوة الشعب، وأهم القضايا التي يمكن أن تثير الخلافات المذهبية أو العرقية أو الطائفية في الدولة والتي تكون لها أهمية كبيرة لدى الدول الأخرى[3].

ثالثـاً- التجـسس الإلكترونـي الدبلوماسـي:

يُقصد بالتجسس الدبلوماسي: "تلك الأنشطة التجسسية التي يمارسها الأفراد المتمتعون بالحصانات والامتيازات الدبلوماسية، والمتمثلة في جمع المعلومات بطرق غير قانونية مع العلم أن هؤلاء الأفراد يمارسون هذا النوع من التجسس دون إخفاء صفتهم الدبلوماسية، وهذا ما يميزه عن صور التجسس

[1]- ذياب البداينة، مرجع سابق، ص. ص. 191-192.

[2]- محمد عدنان عثمان، دور القانون الدولي في مواجهة التجسس الدبلوماسي، مذكرة ماجستير في القانون العام، مقدمة لكلية الحقوق، جامعة الشرق الأوسط، دون بلد، 2015، ص. 30.

[3]- عاطف فهد المغاريز، الحصانة الدبلوماسية بين النظرية والتطبيق، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص. 156.

الأخرى، ويمكن تصنيف التجسس الدبلوماسي ضمن التجسس وقت السلم، على أساس أن العلاقات الدبلوماسية بين الدولتين الموفدة والمضيفة تُقطع بمجرد نشوب الحرب بينهما"[1].

ويمكن القول أن التجسس الدبلوماسي قد ينصب على كل طوائف الأسرار مهما كان نوعها؛ بحيث يسعى المبعوثون الدبلوماسيون للوصول إلى أي معلومة قد تهم دولهم سواء كانت عسكرية أو سياسية أو إقتصادية أو غيرها، وهذا رغم توجه بعض الدارسين إلى إلحاق هذا الصنف من التجسس بالتجسس السياسي[2].

رغم الارتباط التاريخي الوثيق والمعروف بين الجوسسة والدبلوماسية لحد اعتبار السفراء الأجانب أحيانا أفضل من الجواسيس[3]، إلا أن الأسرار الدبلوماسية كما السياسية لم تكن تعتبر في العديد من التشريعات صراحة كأسرار، ومثاله القانون الفرنسي؛ حيث أن المشرع الفرنسي لم يحسم مسألة اعتبار السر الدبلوماسي أو السياسي ضمن سر الدفاع إلا في سنة 1934؛ إذ ظلت مثل هذه المعلومات قبل هذا التاريخ خارج نطاق التجريم والعقاب باعتبارها لا تمثل أهمية محسوسة بالنسبة للدفاع الوطني وهذا يعني أن البحث عنها أو الحصول عليها أو إفشاءها أو تسليمها لم يكن محل عقاب، على أن ذلك لم يمنع القضاء الفرنسي وبناء على اعتبارات الحماية الفعالة الواجب تقريريها لأمن الدولة من إدخال المعلومات السياسية والدبلوماسية ضمن مفهوم سر الدفاع[4].

رابعـــاً- التجـــسس الإلكتروني الاقتصـــادي والصناعـــي:

كان الإتجاه السائد سابقاً يضيق من نوع المعلومات الاقتصادية التي يمكن أن تدخل ضمن مفهوم الأسرار وعليه المستحقة للحماية القانونية؛ باعتبار أن كشفها قد يؤدي إلى المساس بأمن الدولة؛ إذ لم يكن يعتبر المعلومات الاقتصادية في كل الحالات سراً من أسرار الدفاع عن البلاد إلا إذا كانت تخص نشاط الدولة الاقتصادي في عملية الإنتاج الحربي لخدمة الجيش والمنشآت الاقتصادية التي تدخل في

---

[1]- محمد عدنان عثمان، مرجع سابق، ص. 69.

[2]- أنظر: سعد إبراهيم الأعظمي، مرجع سابق، ص. 145.

[3]- في القرن الخامس عشر أسهم الإيطاليون إسهاماً هاماً في عملية جمع المعلومات عندما أنشئوا السفارات الدائمة لهم في الخارج ولم يكد يبدأ القرن السادس عشر حتى نهجت الدول الأوروبية نهج إيطاليا فانشئوا أيضاً سفارات لهم، أنظر: زكي زكي حسين زيدان، مرجع سابق، ص. 30.

[4]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 252.

خطط الدفاع عن البلاد[1]، فجعل بذلك القطاع الاقتصادي يستمد أهميته من ارتباطه وخدمته للأغراض العسكرية فقط، لكن هذا المفهوم الضيق للمعلومات الاقتصادية عرف تطورات ملحوظة في وقتنا الحالي انعكست على مكانة التجسس الاقتصادي ومفهومه ومشتملاته.

مع انتهاء الحرب الباردة وتغير أساليب الصراع الدولي والعالمي وغلبة الصراع التقني والتجاري والاقتصادي على الصراع العسكري؛ تغيرت أولويات التجسس بين الدول فحل التجسس الاقتصادي محل التجسس العسكري والسياسي، ولما كان الصراع الدولي يتجه أساساً نحو المغالبة والتنافس في ساحة الانجازات الاقتصادية والنجاحات التجارية من فوز بتعاقدات وزيادة صادرات وانتزاع أسواق جديدة؛ فإن هذا يعني بالضرورة أن تسعى الدول بكل السبل للسطو على الأسرار الاقتصادية والتقنية وليس أسهل لاختصار الطريق من سرقة الأسرار العلمية والتقنية والتجارية للدول الأخرى[2]، وقد شهدت تسعينات القرن العشرين سيلاً من التحذيرات والتصريحات والدراسات من كل عواصم الدول الصناعية تقريباً تتحدث عن الجاسوسية الاقتصادية والتقنية محذرة من خطرها ومعلنة بداية عصرها الذهبي[3]، ونظراً لأهمية المعلومة الاقتصادية والصناعية في تحقيق الأمن الاقتصادي للدولة والذي له تأثير جلي على باقي مستويات الأمن الأخرى للدولة؛ أصبحت الدول تسعى جاهدة وبكل الوسائل لحماية معلوماتها من جهة والاطلاع على جديد الدول الأخرى في المجال الاقتصادي من جهة أخرى، مستفيدة من التسهيلات التي توفرها التقنيات الحديثة خاصةً في ظل اعتماد القطاعات الاقتصادية على الحوسبة والربط بالأنترنت، ويكفي في هذا الإطار التذكير بأن أحد أكبر أنظمة التجسس الإلكتروني عبر الأقمار الصناعية في العالم وهو نظام "إيشلون" كان سبب إنشاءه الرئيسي القيام بعمليات التجسس على المعلومات الاقتصادية لكل دول العالم، بل ويلاحظ الدعم السياسي والاستخباراتي الصريح للقطاعات الاقتصادية الحيوية في بعض الدول المتقدمة من خلال التصريحات العلنية وكذلك من خلال إنشاء هيئات ترسم العلاقة بين المؤسسات الاقتصادية وأجهزة الاستخبارات لغرض توفير المعلومات الاقتصادية المتعلقة بالدول أو المؤسسات الأجنبية وجعلها في خدمة تطوير الاقتصاد الوطني وحسم معركة المنافسة الاقتصادية الدولية واحتكار

[1]– سعد إبراهيم الأعظمي، مرجع سابق، ص. 146.

[2]– ممدوح الشيخ، التجسس التكنولوجي (سرقة الأسرار الاقتصادية والتقنية)، مكتبة بيروت، مصر، 2007، ص. 125.

[3]– نفس المرجع، ص. 93.

الأسواق العالمية[1]، فهذه المعلومات الآن أصبحت مورداً استراتيجياً يستخدم كسلاح للهيمنة الاقتصادية على المستوى الدولي؛ إذ أن هذه القيمة الإستراتيجية للمعلومة تمثل الشكل الجديد لرأس المال مما يجعلها جد قيّمة، كما أن فكرة المعلومة الصناعية الإستراتيجية لا يتحدد فقط بالمعلومات التقنية البحتة لكن يتضمن كل أشكال المعلومة المرتبطة بعالم المؤسسة، كالمعطيات الاقتصادية والمالية والشخصية وخطوط الإنتاج والمعلومات حول المنتجات والتسويق والأسعار، وكذلك المعطيات المتعلقة بالبحث والتنمية والتطوير، كما أن الضرورة العملية لحماية المعلومات الإستراتيجية والمعارف ذات القيمة أصبحت محسوسة أكثر فأكثر في القطاع الخاص كما العام[2]؛ لذا نجد أن معظم الحكومات في العالم اليوم تحاول أن تضع في مؤسساتها أنظمة كاملة تحكم جمع ومعالجة وحركة المعلومة، وتُطور في ذات الوقت القدرة على استغلال وتسيير المعلومة لتفادي وقوعها في أيدي المنافسين؛ بحيث أصبحت كبريات المؤسسات

[1]– إن أفضل مثال لتوجه الدول الجديد بعد الحرب الباردة إلى نمط جديد من التجسس وهو التجسس الاقتصادي خاصة ولدعم المؤسسات الاقتصادية وجعل أجهزة المخابرات في خدمتها، يظهر في سياسة الولايات المتحدة الأمريكية؛ حيث يلاحظ دعم هذا التوجه إن على مستوى تصريحات المسؤولين أو على مستوى خلق آليات مؤسساتية لهذا الدعم، فمن جهة لا يتوانى بعض المسؤولين رغم حساسية مناصبهم من الإعلان عن دعم المؤسسات الاقتصادية بكل الوسائل والطرق ففي كلمة ألقاها الرئيس السابق للولايات المتحدة الأمريكية بيل كلنتون سنة 1994 بدا واضحاً الإتجاه نحو إقرار دور جديد للمخابرات في مجال مراقبة الاتصالات والمعاملات الإلكترونية؛ إذ أكد على دورها في المساهمة في رخاء ورفاهية الولايات المتحدة الأمريكية مع ما يعنيه ذلك من دور على المستوى الاقتصادي (راجع أكثر: منى الأشقر جبور وعزيز ملحم بربر، أمن الشبكات والأنترنت، مداخلة مقدمة في إطار الحلقة العلمية الموسومة بـ "الأنترنت والإرهاب"، قسم البرامج التدريبية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، القاهرة، 15– 19/ 11/ 2008.)، وكذلك قيام العديد من مدراء وكالة المخابرات المركزية الأمريكية وعبر صفحات الجرائد بالتصريح بأن وظيفة هذه الوكالة هو التجسس على منافسي المؤسسات الأمريكية وتوفير الدعم لها، كما رافعت هذه الوكالة من أجل تقوية ودعم الرقابة التي تمارسها أصلاً المصالح الأمريكية على المصالح والوكالات الأجنبية دون استثناء والتي تحاول الاستيلاء على الأسرار التجارية الأمريكية، ومن جهة ثانية يلاحظ قيام الرئيس السابق جورج بوش بتاريخ 07 جانفي بإنشاء ما سُمي بـ "برنامج أمن الصناعة الوطنية" الذي أسس لمستقبل تعاون وطيد بين المصالح الكبرى للاستعلامات والمؤسسات والشركات الأمريكية وذلك لإدراكه بوادر ظهور المنافسة، وبدوره قام بيل كلنتون بإثراء النص مستلهماً من مجلس الأمن الوطني المؤسس في بداية الحرب الباردة والذي يقدم الاستشارة للرئاسة حول السياسة الخارجية للولايات المتحدة، وقام بتأسيس المجلس الاقتصادي الوطني الملحق بالبيت الأبيض والذي تتمثل وظيفته في مساعدة الرئيس في تحديد التوجهات الاقتصادية، أنظر:

-Frédéric Chapier, l'économie c'est la guerre : les agents sucrets au service du big business, édition du seuil, paris, p. p. 19 – 21.

[2]- Koenraad Dassen, sûreté du l'Etat, Bruscelles, Belgique, 2005,p.56, ouvrage publie sur le site: http//www.suretedeletat.be, lesite aété visité le:07/02/2015.

بغض النظر عن جنسيتها تتبع سبلاً كانت تعد مناهج مستخدمة من قبل المصالح السرية لأجل حماية المعلومة الأصلية، ومن أبرز هذه الطرق ما يلي:

أ- تصفية وانتقاء المعلومات التي تخرج من المؤسسة أو البلد؛ وعليه فالمعلومات المتوفرة في السوق هي فقط تلك التي ترغب المؤسسة في تركها تفلت.

ب- إغراق المنافسين بكتلة معلوماتية معقدة تجعل معالجتها مستحيلة.

ج- إعطاء وإيصال معلومات مغلوطة من أجل تغطية الصحيحة؛ وبذلك جعل المنافسين في حالة تيه[1].

لقد امتد أثر التحول في سلم ترتيب أهمية المعلومات محل التجسس ليشمل بروز مصطلحات جديدة لها ذات معنى التجسس لكن استخدمت كنوع من تخفيف حدة دلالاته؛ بحيث نقف كثيراً على استخدام تعبير الاستخبار الصناعي أو الاقتصادي، والذي يُعرف بأنه: مجموعة التصرفات والأنشطة المنظمة للبحث والمعالجة والتوزيع وكذا لحماية المعلومة المفيدة للفاعلين الاقتصاديين والمتحصل عليها بطريقة مشروعة، فالاستخبار الاقتصادي يغطي ما يعبر عنه عادة بفكرة اليقظة التكنولوجية أو المراقبة التنافسية، ومن جهة أخرى نجد بأن التجسس الاقتصادي يعبر عن تصرف تقوم به حكومة أجنبية باستخدام وبتسهيل وسائل غير مشروعة، مستترة واحتيالية لأجل جمع معلومات أو استخبارات اقتصادية، وكل من هذين التعريفين يسمحان بالوقوف على عدم التوافق بينهما فكل منهما مختلف في طريقة الحصول على المعلومة وفي طريقة خلق المعرفة المرتبطة باتخاذ القرار[2]، وفي الواقع فإن الحدود الفاصلة بين مفاهيم اليقظة التكنولوجية والاستخبار الاقتصادي والتجسس الاقتصادي غير واضحة وغالباً ما يعبر عن التجسس الاقتصادي بأنه انحراف غير صحي لليقظة التكنولوجية، وبأنه سرطان الاستخبار الاقتصادي، لكن من الصعب تحديد أين تنتهي اليقظة أو الاستخبار وأين يبدأ التجسس؛ فعادة يبدأ البحث

[1]- Joëlle Noailly, l'espionnage industriel au cœur de la guerre mondiale du renseignement Economique, mémoire de metrise, université Lyon 2 , 1999-1997 , p .p. 14-15, Publier sur le site : www.strategique.free.fr , le site a été visité le : 04-02-2015.

[2]- Dany Deschenes , le système échelon: une nouvelle donne dans l'espionnage électronique , bulletin le maintien de la paix , n°50 , janvier 2001 , université laval , Québec, canada , p . 2 , Publier sur le site :www.ulaval.ca/iqhei , le site a été visité le :04-02-2015.

عن المعلومة بوضع نظام لليقظة ثم يتجه نحو التجسس الاقتصادي، فهذا الأخير يعد مكملاً للأول؛ لذا فلا يُتردد في اللجوء إليه[1].

ويستهدف التجسس الاقتصادي كل ما يتعلق بالجهود الاقتصادية للبلاد، فهي تشمل المعلومات المالية كالأعمال التحضيرية لمعاهدة جمركية وحركة الصادرات والواردات واتفاقيات التعاون الاقتصادي مع الدول الأخرى وكذا أسرار صناعة سلع معينة، ولا يقتصر الأمر على الإنتاج الصناعي للدولة بل يمتد إلى الشركات الخاصة التي تفيد الدولة من إنتاجها[2]؛ بحيث تشمل الحماية القانونية حالياً رأس مال المؤسسات التي أصبح يتخذ شكل معلومات غير مادية سهلة السرقة خاصة في ظل اقتصاد معولم طغت فيه سمة الصراع وحدة المنافسة المتولدة بفعل الأزمة؛ بحيث لم يعد هذا الموضوع رهاناً جزئياً ولكنه أصبح مسألة مصلحة وطنية؛ لأن حماية أسرار الأعمال هو حماية لمناصب عمل ولتكنولوجيا واستثمارات حساسة[3]؛ وهذا ما أدى ببعض الدول إلى وضع قوانين خاصة تحكم التجسس الاقتصادي، وفي هذا الإطار نجد وكأفضل مثال القانون الأمريكي للتجسس الاقتصادي الذي صادق عليه الكونغرس في أكتوبر سنة 1996 ويسمى بقانون كوهن "loi Cohen" نسبة للنائب الذي قدمه، وكان منتهاه بوضوح تعزيز الترسانة القانونية الأمريكية في مواجهة الاستخبارات الاقتصادية؛ حيث يعاقب هذا القانون على أفعال التجسس الاقتصادي الممارسة من طرف أو لحساب حكومة أجنبية، ولا يقتصر محل الحماية فيه على الإمكانيات الاقتصادية والعلمية الوطنية، بل يمتد ليشمل أسرار الأعمال سواء كان محتواها استراتيجي أم لا في مواجهة كل أشكال الالتقاط بواسطة الغير غير المرخص له بذلك، ويوسع في تعريفها حيث تشمل كل معلومة –تحت أي شكل كان– غير عمومية ومحفوظة سرية من طرف مالكها مادامت تمثل قيمة اقتصادية سواء كانت هذه المعلومة عبارة عن معلومة مالية أو اقتصادية أو تجارية أو حتى مجرد أسرار تقنية أو صناعية خاصة[4]، وقد تم الاستناد على هذا القانون لتوجيه اتهامات بتجسس

[1]- Joëlle Noailly, op. cit. p. p. 22 – 25.

[2]– زكي زكي زيدان، مرجع سابق، ص. 124.

[3]- Bernard CARAYON, secret des affaires (protéger le secret des affaires: un enjeu national): bulletin du droit des secret d'affaires-BSA-n°=1,publication de l'institut de l'IE, paris, triméstre 3, novembre 2012, publié sur le site: www.institut-ie.fr, le site a été visité le: 04/02/2015.

[4]- Bertrand WARUSFEL, la loi américaine sur l'espionnage économique, revue droit te défense, paris, 1997, p. 64, publié sur le site www.driot.univ-paris5.fr,le site a été visité le : 23/11/2015.

إلكتروني صناعي لأطراف أجنبية رغم يقين الولايات المتحدة الأمريكية بصعوبة إعماله على هذه الحالات[1].

أما على الصعيد الأوروبي فنجد أن بلجيكا من بين الدول التي لها قوانين خاصة ومتفردة في هذا المجال ويتعلق الأمر خاصة بقانونها العضوي المؤرخ بتاريخ 30 نوفمبر سنة 1998 المنظم للاستعلام والأمن، والذي ينظم عملية جمع المعلومات حول نشاطات الأفراد والجماعات التي تهدد أو يمكن أن تهدد القيم والمصالح الأساسية للبلاد، ويقسم ذات القانون القيم المحمية بموجبه إلى ثلاثة طوائف رئيسية: الطائفة الأولى هي أمن الدولة الداخلي وحفظ النظام الديمقراطي والدستوري، والطائفة الثانية تتعلق بأمن الدولة الخارجي والعلاقات الدولية، والطائفة الثالثة تتعلق بالقدرات الاقتصادية والعلمية[2]؛ حيث قام المشرع هنا بالإشارة إلى هذه الطائفة بشكل مستقل رغم صلتها الوثيقة بالطائفتين الأولتين، وهذا ما لا يدع مجالا للشك عن المكانة المحورية التي أصبحت المعلومة الاقتصادية تحتلها وانتباه المشرعين لهذا الأمر.

[1]– إن أبرز مثال هنا والذي اعتُبِر كسابقة، اتخاذ الولايات المتحدة الأمريكية لقرار تاريخي في علاقاتها مع الصين؛ بحيث قامت بتاريخ 19 ماي من سنة 2014 بإضافة أسماء وصور خمسة ضباط صينيين إلى قائمة الأشخاص المبحوث عنهم وذلك بتهمة قيامهم بعمليات تجسس إلكتروني صناعي ضد مؤسسات أمريكية منذ سنة 2006، ورغم أنه كان من الواضح أن هذا الإجراء وعلى الصعيد القانوني ليس له أي حظ في التوصل إلى تسليم العسكريين المبحوث عنهم أو محاكمتهم كما أنه من الواضح بأنه لن يُعطل أو يُعرقل الممارسات الصينية، إلا أنه شكل ردة فعل الأمريكان على تصرفات الحكومة الصينية التي بحسب تصريحات مدير (FBI) تمارس منذ وقت طويل التجسس الإلكتروني من أجل مساعدة مؤسساتها في أن تأخذ الريادة الاقتصادية، لكن قيام الولايات المتحدة بوضع صور هؤلاء العسكريين على صفحات (FBI) بنفس طريقة عرض مجرمي الياقات البيضاء أو القتلة أو الإرهابيين، مما جعل أسماءهم و صورهم تجوب العالم من طرف عديد وسائل الإعلام؛ يدل على وجود إرادة المساس بصورة هؤلاء الأفراد ومن وراءهم بطبيعة الحال صورة الصين، وقد خلقت هذه القضية موضوع خلاف بين الدولتين؛ إذ اعتبر المتحدث بإسم وزارة الشؤون الخارجية الصيني أن الإجراء الأمريكي انتهاك للعلاقات الدولية وتأسف للضربة الموجهة للثقة المتبادلة بين الدولتين، علاوة على هذا ذكر الطرف الصيني بأنه ومنذ قضية سنودن، الولايات المتحدة الأمريكية هي من يتجسس على القوى الأجنبية وعليها من خلال الدخول إلى شبكات إداراتها وجيشها ومؤسساتها وأن الصين قد طلبت توضيحات من واشنطن والتوقف عن ممارساتها معتبرة ذلك نقصاً في الإخلاص في الخطاب مع الولايات المتحدة الأمريكية حول الأمن الإلكتروني، وقررت توقيف نشاطات مجموعة العمل التي تم تنصيبها في ذات الميدان، ويشهد الواقع أن المواجهة والصدام بين الدولتين في الفضاء الإلكتروني لم ينته، أنظر:
- Daniel Ventre, cyberespionnage et diplomatie : l'exemple des tensions chine / Etats-Unis, les grands dossiers diplomatie, n°23, p. p. 17 – 18, article publié sur le site www.chaire-cyber.fr, le site a été visité le : 23/11/2015.

[2]- Koenraad Dassen, op. cit., p. p.7-8.

كحوصلة لما سبق ذكره يمكن القول أن التجسس الاقتصادي الآن أصبح يحتل ريادة الصور الأخرى من التجسس؛ باعتبار الاقتصاد عصب حياة الدولة ومحرك كل مجالاتها الأخرى، وأهم ما يمكن ملاحظته في هذا الإطار أن الحماية القانونية للسر الاقتصادي أصبحت في عديد الدول تساوي بين القطاع العام والقطاع الخاص؛ مما يوسع من مفهوم أمن الدولة ويضيق الحدود بين علاقة الدولة بالأفراد.

الفـــرع الثانـــي: صـــور التجـــسس الإلكترونـــي من حيث الوسيلـــة.

إن ما يمنح التجسس وصفه الإلكتروني هو ارتكابه بواسطة التقنيات الحديثة، ونميز في هذا الشأن بين ثلاثة أنماط من التجسس من حيث الوسيلة: التجسس الذي يتم عن طريق الحواسيب والأنترنت، والتجسس عن طريق الهواتف النقالة، والتجسس عن طريق الأقمار الصناعية، مع الإشارة إلى العلاقة الوثيقة والارتباط الوظيفي بين هذه الوسائل الثلاثة، وستتم دراسة هذه الوسائل الثلاثة من خلال العناصر الآتية:

أولاً- التجـــسس الإلكترونـــي بواسطـــة الحواســـيب والأنترنت:

تعد الأنترنت أهم وسيلة للإتصال حالياً؛ إذ تقوم بربط مجموعة من أجهزة الحاسب الآلي ببعضها إما عن طريق خطوط الهاتف أو الأقمار الاصطناعية، وأول ما نشأت هذه الشبكة كانت لأغراض عسكرية لتتوسع فيما بعد لتشمل كافة مناحي الحياة؛ حيث أصبح الكمبيوتر أحد أهم وسائل التجسس الإلكتروني استخداماً، وأضحت الأنترنت الرابط الذي يمكن جهاز حاسوب ما وبواسطة تقنيات خاصة تتطور باستمرار من الاختراق والحصول على المعلومات الموجودة في جهاز آخر أو تعديلها أو حذفها أو إتلافها أو الاطلاع عليها أو إفشاءها، وهذه السلوكات تشكل جميعها جوهر التجسس الإلكتروني، ويحتل استخدام الكمبيوتر والأنترنت الصدارة من بين وسائل التجسس الأخرى ، بل إن كل من الهاتف والأقمار الصناعية تعد تقنيات تابعة الآن للحاسوب.

قد يستخدم الكمبيوتر والأنترنت كما سبقت الإشارة إليه كوسيلة للحصول على الأسرار المرتبطة بأمن الدولة، أو لنشرها وافشاءها، أو لتعديلها، أو إتلافها، وتشكل الأمثلة الآتية أهم التطبيقات في هذا الميدان:

أ-الكمبيوتـــر والأنتـــرنت كوسيلة للحصول على المعلومـــات السريـــة: لم يعد التجسس في ظل ما يشهده العالم في مجال تكنولوجيا المعلومات والاتصالات مقتصراً على تجنيد عملاء في الدول الأخرى

للحصول على المعلومات العسكرية أو الدفاعية خاصتها، أو تجنيدهم في المؤسسات التجارية والصناعية بهدف التوصل إلى أسرار هذه المنشآت، أو اللجوء إلى رشوة العاملين فيها أو ابتزازهم، فالتقنية الرقمية فتحت آفاقا واسعة للقيام بالتجسس دون حاجة لاختراق الدول أو المؤسسات من قبل العناصر البشرية هذه التقنيات كثيرة ويصعب حصرها إذ أنها تتطور باستمرار، وهناك سعي وبحث دائم من قبل الدول والجهات المختلفة للوصول إلى مراحل متقدمة في مجال صناعتها[1]، ويمكن الإشارة في هذا الصدد إلى أهم التقنيات المستخدمة في هذا المجال:

1- تقنيـــة الأبـــواب الخلفيـــة: والتي تعرف أيضا بتقنية أبواب المصيدة؛ بحيث تستغل هذه التقنية في الوصول غير المشروع وغير المحدود إلى برامج وملفات وبيانات النظام؛ إذ من المعتاد عند إعداد البرامج ترك ثغرات أو نقاط دخول غير معلن عنها تتجنب إجراءات الأمن العادية، وذلك بهدف السماح بإضافة تعليمات إلى البرنامج لتلافي ما قد يظهر فيه من أخطاء، ووجود هذه الثغرات قد لا يكون متعمداً دائما حيث يمكن أن توجد عرضاً في بعض الأحيان نتيجة أخطاء في التصميم الكلي للنظام أو نتيجة مواطن ضعف في مجموعة الدارات الإلكترونية للحاسب، وعندما يكون تركها مقصوداً فإنها تلغى في الطبعة النهائية للبرنامج، غير أن هذا الإلغاء قد يتم في بعض الأحيان تعمد إغفاله؛ وبذلك يكون متاحاً إذا ما وجدت عمداً أو عرضاً الوصول إلى أجزاء من النظام غير مصرح بولوجها والاطلاع على ملفات البيانات المخزنة بداخله، وإذا كانت البيانات في حالة انتقال فيما بين النهايات الطرفية فإن أساليب التقاطها تختلف باختلاف الوسيلة الناقلة، فمثلا البيانات التي يجري نقلها عبر الأسلاك المعدنية أو خطوط الهاتف المخصصة لنظم الاتصالات الإلكترونية لا يحتاج معترضها لأكثر من جهاز التقاط بسيط يمكن تركيبه من وحدات إلكترونية تتوافر في الأسواق وتثبيته بطريقة خفية داخل صناديق التوزيع التي تنتهي إليها معظم وسائل الاتصال السلكية واللاسلكية، وقد يضاف جهاز حث إلى جهاز الالتقاط كي يعمل فحسب في حال وجود بيانات أو إشارات في السلك أو الخط الذي تجري مراقبته[2].

2- تقنيـــة ملفـــات التجـــسس والاختـــراق: وقوامها السيطرة عن بعد، وهي لا تتم إلا بوجود عاملين مهمين، الأول البرنامج المسيطر، ويعرف بالعميل، والثاني الخادم الذي يقوم بتسهيل عملية

---

[1]- نهلا عبد القادر المومني، مرجع سابق، ص. 216.

[2]- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، مصر، 1994، ص. ص.141-144.

الاختراق ذاتها، وبعبارة أخرى لابد من توفر برنامج على كل من جهازي المخترق والضحية، ففي جهاز الضحية يوجد برنامج الخادم، وفي جهاز المخترق يوجد برنامج العميل، وتختلف طرق اختراق الأجهزة والنظم باختلاف وسائل الاختراق[1]، لكن أهمها نجد برنامج حصان طروادة، وبرنامج الكعكة "cookies"، وعلى كل فإن إدخال ملفات التجسس إلى جهاز المجني عليه يتم عن طريق ثلاث طرق غالباً: إما من خلال برامج المحادثة عبر الأنترنت، أو من خلال البريد الإلكتروني للشخص أو الجهة المجني عليها عن طريق إرسال رسائل إلكترونية إلى المجني عليه، أو عند زيارة الشخص أو الجهة المعنية لمواقع مجهولة على الأنترنت[2].

3- تقنيـــة برامـــج المراقبـــة الشاملـــة: تتكون برامج المراقبة الشاملة من مجموعة من البرامج في برنامج واحد؛ حيث تجمع هذه البرامج كل من برنامج تسجيل المفاتيح (يقوم بتسجيل كل كبسة يضغطها مستخدم الكمبيوتر من لوحة المفاتيح؛ إذ يمكن بواسطتها تسجيل أسماء المواقع التي يزورها المستخدم، وجميع عناوين البريد الإلكتروني، وكلمات السر، والملفات المطبوعة، وكل ما يمكن إدخاله إلى الكمبيوتر عبر لوحة المفاتيح)، وأيضا برنامج مراقبة الأنترنت (يركز على كل ما يتعلق بنشاطات المستخدم عبر الانترنت كالمواقع التي زارها، والبرامج التي تم تنزيلها وأين تم حفظها، وجميع رسائل البريد الإلكتروني الواردة و الصادرة ...)، بالإضافة إلى المزيد من مزايا المراقبة؛ إذ يمكن لبرامج المراقبة الشاملة تسجيل ما يجري في الغرفة إذا كان جهاز الحاسب مزوداً بكاميرا أو تسجيل الأحاديث الدائرة في الغرفة إذا كان مزوداً بميكروفون[3].

وفي إطار تقنيات مراقبة الأنترنت يمكن إدراج برنامج "بريسم" كأكثر الأمثلة المتداولة على الصعيد العالمي حالياً لنشاطات التجسس، والذي شكل مصدر أزمة دبلوماسية وإحراج سياسي للولايات المتحدة الأمريكية أكثر حتى مما شكله كشف برنامج التجسس الإلكتروني المعروف بـ "إيشلون"، ويمثل بريسم برنامج سري للتجسس الإلكتروني على شبكة الأنترنت عن طريق الدخول لقواعد البيانات الخاصة بعديد الشركات الكبرى في مجال الاتصالات عبر الأنترنت، وقد وضع حيز الخدمة منذ سنة 2007 من

---

[1]- عبد الصبور عبد القوي علي المصري، مرجع سابق، ص. ص. 64-65.

[2]- نهلا عبد القادر المومني، مرجع سابق، ص. 219.

[3]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، مصر، 2009، ص. ص. 344-345.

طرف وكالة الأمن القومي الأمريكي؛ بحيث يقوم باختبار المعطيات المتنقلة في العالم ككل في الوقت الحقيقي، ويتم حفظ المعطيات خلال بضعة أيام وبعدها يتم إما تخزينها أو محوها بحسب المعلومات التي يتم البحث عنها من طرف محللي الوكالة[1].

[1]- l'affaire snowden et la nouvelle géopolitique du cyberespionnage, p. 3, article publier sur le site : http : //www.la-rem.eu, le site a été visité le : 05/02/2014.

– هذا وقد شكلت قضية إدوارد سنودن (عميل متعاقد متخصص في علم الحاسوب عمل كمحلل للمعلومات لدى وكالة المخابرات المركزية الأمريكية ثم مسؤول النظام في وكالة الأمن القومي) مسرب المعلومات السرية حول برنامج بريسم في جوان من سنة 2013 أهم القضايا التي حضت بالاهتمام الدولي حاليا؛ إذ أثارت ردود فعل كثيرة إن على مستوى الولايات المتحدة الأمريكية أو على مستوى دول العالم، فعلى المستوى المحلي اعتبرت تسريبات سنودن الأخطر في تاريخ الاستخبارات الأمريكية وهو ما جاء في تصريح لنائب مدير وكالة الاستخبارات الأمريكية والذي وصفه بالخائن الذي وضع الأمريكيين في خطر أكبر؛ لأن الإرهابيين سيتعلمون الكثير من هذه التسريبات وسيكونون أكثر يقظة، وفي نفس الإطار وصف الرئيس الأمريكي أوباما هذه التسريبات بأنها خيانة عظمى، وهو ذات الوصف الذي استخدمه أعضاء الكونغرس الذين طالبوا بمعاقبته، لأن هذه التسريبات شكلت مصدر أزمة دبلوماسية كونية وإحراج سياسي للولايات المتحدة الأمريكية خاصة اتجاه حلفائها؛ الأمر الذي دفع الرئيس أوباما إلى الإعلان في أوت 2013 عن إجراء تعديل لقانون الباتريوت، كما أعلن مدير وكالة الأمن القومي عن إلغاء 90% من مناصب محللي النظم وتعويضهم ببرامج معلوماتية لضمان عدم تسريبات جديدة؛ إذ أن ما مكن سنودن من الوصول لكم هائل من المعلومات السرية كان عمله كمحلل معلوماتي وكمسؤول للنظام في ذات الوكالة وكذا في وكالة الاستخبارات المركزية الأمريكية، أما على المستوى الدولي وبالإضافة إلى موجة الاستنكار والتنديد بالتجسس من طرف عديد الدول والكيانات المدافعة عن حقوق الإنسان وعن الحياة الخاصة للأفراد فقد اتخذت بعض الدول بعض القرارات، ومثالها قيام كل من البرازيل وألمانيا بالعمل على إصدار لائحة أممية لحماية الحريات الشخصية توسع لائحة سنة 1966 التي دخلت حيز التنفيذ في 1976 إلى نشاط الأنترنت، وقيام ألمانيا عبر مستشارتها بعرض مبادرة على زعماء دول الاتحاد الأوروبي على هامش قمة بروكسيل لإصدار اتفاق ضد التجسس وطالبت أمريكا بالقيام بأفعال ملموسة وليس الاكتفاء بالاعتذار، ويشار هنا إلى أن تسريبات سنودن قد هيمنت على قمة الاتحاد الأوروبي إلى درجة وضع الولايات المتحدة في قفص الاتهام، من جهة أخرى قامت العديد من الدول في أمريكا الجنوبية بمنح حق اللجوء السياسي لادوارد سنودن لكنه بقي في روسيا التي منحته اللجوء السياسي المؤقت لمدة سنة في الأول أغسطس (أوت) سنة 2013 بعد أن قضى عدة أسابيع في المنطقة الدولية لمطار موسكو وقد تسبب ذلك في توتر العلاقات بين روسيا والولايات المتحدة الأمريكية التي كانت قد تقدمت إليها بطلب تسليم سنودن في 24 جوان سنة 2013 أي بعد يوم واحد من وصوله إلى مطار موسكو وذلك بتهمة التجسس وسرقة ممتلكات حكومية ونقل معلومات تتعلق بالدفاع الوطني دون إذن والنقل المتعمد لمعلومات مخابرات سرية لشخص غير مسموح له بالاطلاع عليها، لكن روسيا رفضت التسليم بحجة عدم وجود اتفاقيات تعاون قضائي تنظم هذا الموضوع، أنظر لمزيد من التفاصيل:

– يونس الزرهوني، القصة الكاملة لمفجر أكبر فضيحة خيانة في التاريخ الأمريكي إدوارد سنودن، مقالة منشورة على الموقع الالكتروني www.th3professional.com/2013/08/blog-post-19.html، تمت زيارة الموقع بتاريخ: 21/ 08/ 2016.

4- تقنيـــة قرصنـــة الطابعـــة: إن التكنولوجيا قد تطورت بشكل كبير خلال السنوات الأخيرة فمعظم الطابعات أصبحت متعددة الوظائف ومدمجة في شبكة المعلوماتية وتحتوي على قرص صلب لأجل تخزين المعطيات، وغالبا ما يتم إدارتها والتحكم فيها انطلاقا من الخارج عبر الأنترنت، وبواسطة بعض العمليات البسيطة يمكن لأي شخص أن يدخل إلى إعدادات الطابعة المستهدفة، وتغيير الإعدادات أو جعل الشبكة غير قابلة للاستخدام أو التقاط الملفات ، وأيضاً إمكانية الاستحواذ على الملفات المطبوعة وحتى المنسوخة والمصورة خاصة[1].

ب- الكمبيوتـر والأنترنت كوسيلة لنشر وإفشـاء المعلومـات السريـــة: تعتبر الأنترنت أفضل وسيلة لتحقيق مفهوم إفشاء الأسرار على أوسع نطاق مكاني وبأكثر امتداد زمني مقارنة بالوسائل التقليدية، فقد حصل وأن نشرت إحدى المجلات في الولايات المتحدة الأمريكية مقالاً حول كيفية صنع قنبلة نووية لكن الحكومة لم تثر ضجة كالتي تثيرها عادة الآن عند نشر مثل هذه المواضيع الحساسة على شبكة الأنترنت؛ إذ إعتبرت بأن ذلك المقال سيختفي ببساطة في "ضباب المعلومات"، أما الأنترنت فتقوم برفع هذا الضباب بواسطة أدوات مثل محركات البحث التي تقوم بإيجاد أي شيء تم نشره[2].

ومن أهم القضايا التي يمكن الإشارة إليها في هذا الصدد والتي تم استخدام الأنترنت فيها كمجال لنشر أسرار العديد من الدول قضية موقع ويكيليكس، وهو موقع متخصص في نشر الوثائق السرية للدول والمسربة من مصادر مختلفة، أسسه المدعو جوليان اسانج وهو صحفي ومبرمج استرالي كان هاكراً عندما كان مراهقاً، ويصنف البعض هذا الموقع على أنه منظمة إعلامية بينما أُدرج كمكتبة في استراليا، وبينما فضل مؤسسه اعتباره صنفا من الصحافة العلمية[3]، كما يذهب البعض لوصف هذا الموقع بأنه أحد عوارض مشكلة جديدة كانت نتاج التقدم التكنولوجي الذي سمح بحيازة كمية ضخمة من البيانات وبتكلفة متدنية أو بدون تكلفة من طرف فرد أو أكثر لتنشر حصرياً على الخط[4].

- l'affaire snowden et la nouvelle géopolitique du cyberespionnage, op. cit, p. 7.

[1]- Alexandre lienard, lutter contre l'espionnage industriel, réseau vincibilis, étude publié sur le site www.utbm.fr, le site a été visité le : 23/11/2015.

[2]- Tim Maurer, Wikileaks2010: A Glimpse of future, discution paper, explorated in cyber intenational relations discussion paper series, Belfer center for science and international Affaires, Harvard Kennedy school, USA, August 2011, p. 37, Publier sur le site: www.maurer-dp-2011-10-wikileaks-final, le site a été visité le: 23-11-2015.

[3]- Ibid, p. 22.

[4]- Ibid, p. 4.

ج- الكمبيوتـر والأنتـرنت كوسيلـة لتعديـل وإتلاف المعلومـات السريـــة: بحيث يستخدم الكمبيوتر والأنترنت كوسيلة لارتكاب جريمة الإتلاف المعلوماتي، والتي تتمثل في الاعتداء على الوظائف الطبيعية لحواسيب أخرى، وذلك بالتعدي على البرامج والبيانات المخزنة أو المتبادلة بينها عبر الشبكة العالمية، بمحوها أو تعديلها أو تغيير نتائجها أو بطريق التشويش على النظام المعلوماتي بما يؤدي إلى إعاقة سير النظام الآلي[1]. وتتنوع الطرق الفنية والتقنية المستخدمة لإتلاف البيانات والبرامج بدءاً بفيروسات الحاسب الآلي ومروراً ببرامج الدودة وانتهاء بالقنابل المنطقية أو الزمنية [2]، ومن الأمثلة الواقعية على الإتلاف الإلكتروني نجد مثلا قيام إيران بإرسال الدودة المعلوماتية المسماة "شامون shamoon" إلى القواعد البترولية للعربية السعودية، إذ تمكنت هذه الدودة في أكتوبر من سنة 2012 أن تدمر المعلومات الموجودة على ثلاثين ألف (30.000) حاسوب خاص بمجمع "أرامكو"[3].

قد يقول قائل بأن أفضل الأساليب لتلافي كل هذه الأضرار هو ببساطة عدم ربط الحواسيب التي تحوي معلومات حساسة وسرية بالأنترنت وهذا بالفعل مسلك الدول[4]، لكن لا يمكن الجزم بفعاليته المطلقة، ويؤيد الحاصل في الواقع هذا الطرح؛ ففي سنة 2010 تم تسجيل أول هجوم تدميري من نوعه على المفاعل النووي "بوشهار و ناتانز" في إيران بواسطة فيروس يدعـى "ستكسنت stuxnet" حيث استطاع التغلغل في أنظمة المنشآت النووية الإيرانية مستفيداً من فجوات لم تكن معروفة حتى ذلك الوقت في نظام ويندوز، ويُعتقد إصابته لنحو مئة جهاز من أجهزة الطرد المركزي المستخدمة في تخصيب اليورانيوم، وإدخال هذا الفيروس لم يكن عن طريق الأنترنت بل باستخدام وصلة "USB" تم وصلها بالنظام في خطة مدروسة بحيث انتشر الفيروس باحثاً عن هدف ونوع محدد من أجهزة التحكم في عمل أجهزة تخصيب

---

[1]- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص. 216.

[2]- نفس المرجع، ص. 237.

[3]- Gerard Peliks, la cybercriminalité, livres blanc de forum ATENA, France, Mai 2013, p. 7.

[4]- بل إن بعض الدول ذهبت إلى حد إختيار عدم الربط المطلق بشبكة الأنترنت وفي كل مناحي نشاطها وليس الاكتفاء بعدم الربط على القطاعات الحساسة والسرية فقط، وأبرز مثال في هذا الصدد نجد كوريا الشمالية، بحيث أعلنت بتاريخ 12 فيفري من سنة 2014 -فقط- عن ربطها لعشرين (20) حاسوباً بالشبكة الدولية للأنترنت، أنظر:

- Ryan Burton, 2014 une Année d'actualité cyber, publication de cellule cyberdéfense, 22 janvier 2015, France, p. 5, publier sur le site : www.cil.cnrs.fr, le site a été visite le: 23/11/2015.

اليورانيوم، فإذا وجد الهدف بدأ بالعمل التخريبي، وفي الحالة العكسية يكمل انتشاره باحثاً عن أجهزة جديدة في الشبكة، وقد قام نشاطه على تسريع عملية التخصيب عن طريق التحكم في بعض الأجهزة الخاصة بذلك بطريقة غير ملحوظة للعاملين هناك؛ بحيث تقوم بتقديم قراءات مغلوطة على شاشات المراقبة توضح أن كل شيء على ما يرام؛ وقد أدى هذا الفيروس إلى تعطيل عملية التخصيب وتعطيل تقدم البرنامج النووي الإيراني لمدة سنتين منذ زرع الفيروس في عام 2009، وقد تطلب عمل هذا الفيروس خبراء بكفاءة عالية في مجال عمل أنظمة التشغيل وبدراية داخلية في كيفية عمل المصنع بأدق التفاصيل، وفي غالب الأمر تم استخدام عملاء بالداخل[1].

ثانيـاً- التجـسس الإلكترونـي بواسطـة الهواتـف النقالـة:

بالرغم من أن عمليات التجسس على المكالمات الهاتفية تعتبر من أقدم عمليات التجسس المعروفة إذ كانت تستهدف الهواتف التقليدية التي لا تزيد عن كونها أجهزة لنقل مكالمات من خلال الأسلاك التي تربط بين نقطتين (المرسل والمستقبل) يمر فيها تيار كهربائي وفق ذبذبات صوت المتكلم[2]، فالتطور الذي شهدته هذه الأجهزة أدى إلى تغيير جوهري في وظائفها المعروفة سابقاً التي لا تتعدي نقل الصوت؛ وهذا بظهور الهاتف النقال الذي يتميز بالأساس عن الهاتف العادي أو الثابت بكونه جهازاً لاسلكياً، وتعتبر تكنولوجيا الهواتف النقالة التكنولوجيا الرائدة في عصرنا الحالي، وكان من أولى الخدمات التي وفرتها لنا الهواتف النقالة خدمة نقل وتبادل البيانات التي بدأت بتبادل الرسائل النصية القصيرة "SMS" إلى أن تطور الآن ليشمل تحميل ملفات كبيرة من المواد المسموعة والمرئية على الهواتف مباشرة ثم أضيفت إليها إمكانية الدخول على الأنترنت التي فتحت بدورها آفاقاً عدة لاستخدامات الهواتف النقالة

---

[1]- بشرى حسين الحمداني، مرجع سابق، ص. ص. 126- 127.

- ومن الأمثلة كذلك على نقل الأسرار النووية بدون أن يكون هناك ربط بالشبكة ما عُرف بقضية "وان هو لي Wen Ho Lee" وهي قضية تجسس الصين على برنامج الولايات المتحدة الأمريكية للسلاح النووي، وهو ما تم الانتهاء إليه في أفريل من سنة 1999؛ حيث قام الدكتور "لي" بنقل كم هائل من المعلومات حول السلاح النووي من مخبر لوس ألموس وهو ما يعادل 400.000 صفحة من الأسرار النووية، وما يمثل ثمرة خمسين سنة ومئات بلايين الدولارات من الأبحاث، وأرجع البعض سبب هذا إلى القصور والتأخر في آليات التجسس المضاد، راجع أكثر:

- Louise I. Gerdes, op. cit, p. p. 164 – 167.

[2]- أروى محمد تقوى، مدى مسؤولية مشغلي الهاتف النقال عن إساءة استخدامه في الاتصال بالأنترنت، مجلة الحقوق، المجلد الحادي عشر، العدد الثاني، سوريا، ص. 355.

وأصبحت هذه الأجهزة توفر خدمات كانت في وقت مضى مخصصة للحواسيب الموصولة بالأنترنت[1] من حيث إمكانية تخزين واستقبال ومعالجة المعلومات وإرسالها[2].

إن أنشطة الاختراق امتدت بشكل كبير إلى نظم الهاتف والاتصالات وأصبح ذات النشاط لا يستهدف أنظمة الكمبيوتر فقط بل تزايدت أنشطة الاختراق لخطوط الهاتف هذا من جهة، ومن جهة أخرى قد يستخدم الهاتف كوسيلة فعالة للتجسس بالنظر إلى تعدد التقنيات والبرمجيات الحديثة والخصائص التي تمتاز بها الهواتف الحالية، فمثلا بإمكان البرمجيات التي يمكن تحميلها على أنواع معينة من الهواتف المحمولة أن تسكت قارع الأجراس (الرنة) وتقطع العروض الضوئية التي عادة ما تحفز عند استقبال المكالمات فيمكن للمتصل أن يستمع آنذاك للمحادثات التي تتم بداخل الغرفة التي يوجد بها ذات الهاتف[3]، كما يمكن باستخدام تقنية الرسائل الصامتة وهي تقنية مخصصة للهواتف المحمولة الذكية من فئة الجيل الثالث بحيث يتم برمجة هذه الرسائل بشكل لا يشعر حامل الهاتف بوصولها بحيث تساعد مرسلها على التحديد الدقيق لمكان تواجد الشخص وذلك عبر استخدام معادلة تقوم باحتساب قوة إشارة الموجات المنبعثة من الجهاز المحمول تبعاً لأقرب ثلاث مراكز مستقبلة لهذه الموجات[4].

ثالثـاً- التجـسس الإلكترونـي بواسطـة الأقمـار الصناعيـة:

تمثل الأقمار الصناعية أحد أهم طرق التجسس في الوقت الحالي، لكن عملها يبقى مرتبطاً بالحواسيب التي تقوم بتحليل ما يتم التقاطه. وقد جاءت الأقمار الصناعية كنتيجة للسباق نحو الفضاء الذي كان بين الإتحاد السوفيتي سابقا والولايات المتحدة الأمريكية، فكان الاتحاد السوفياتي أول من أطلق قمراً صناعياً والمعروف بـ "سبوتنيك1" وهذا في 4 أكتوبر 1957 وتلاه إطلاقه لقمر ثان يدعى "سبوتنيك 2"، وتلاحق إطلاق الأقمار الصناعية من جانب الدولتين في سرعة وتقدم مطردين وقد بلغ عدد الأقمار حتى سبتمبر 1961 وفقا للبيانات الرسمية واحداً وخمسين قمراً أمريكيا، وستة عشر قمراً روسيا؛ ليصبح الفضاء الخارجي اليوم مزدحماً بعدد كبير منها ولأغراض مختلفة، كالمتابعة العلمية، وإجراء الاتصالات

[1]- صبرينة بن سعيد، مرجع سابق، ص. ص .111-112.

[2]- أروى محمد تقوى، مرجع سابق، ص. 354.

[3]- بشرى حسين الحمداني، مرجع سابق، ص. 39.

[4]- وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، مذكرة ماجستير في التخطيط والتنمية السياسية، مقدمة لكلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2013، ص. 100.

لأجل التنبؤ بالطقس، ولخدمة الملاحة والملاحظة العسكرية[1]. وتظهر الاستعمالات العسكرية لهذه الأقمار في الاستطلاع والتصوير ومراقبة الأهداف على الأرض، وفي التحذير المبكر بالهجوم على الدولة، وكذا للتشويش على ما يصدر من الأقمار الصناعية الأخرى أو عن مراكز سطح الأرض من إشارات أو موجات بالراديو والتلفزيون أو الرادار، ومن الصعوبة التمييز بين الأقمار الصناعية التي تستخدم لأغراض الرصد الجوي وبين تلك التي تطلق للتجسس وجمع المعلومات وتلك التي تطلق للقيام بالمهمتين معا[2]. وقد شهدت هذه التقنية تطوراً هاماً في تكنولوجيا تحليل الصور الملتقطة؛ بحيث أصبح من الممكن تكوين صورة ثلاثية الأبعاد تبعاً للمعلومات القادمة من الفضاء الخارجي ويمكن استخدامها في اكتشاف نقاط ضمن المناطق الواقعة تحت حراسة مشددة، كما باستطاعة هذه الأقمار أيضا الرؤية عبر السحب وليلا، وباستطاعة بعضها اكتشاف التحركات تحت سطح الأرض[3]؛ وعليه تكون هذه الوسيلة للتجسس الإلكتروني أخطر الوسائل على الإطلاق؛ فإن كان من الممكن وضع آليات وقائية للتجسس عبر الأنترنت أو الهاتف فإنه من الصعب على الأقل حاليا تفادي التجسس بواسطة الأقمار الصناعية؛ بالنظر لعديد الاعتبارات أهمها أن هذه التقنية محتكرة من طرف بعض الدول المتطورة فقط، بالإضافة إلى صعوبة تفادي الانكشاف لهذه الأقمار التي تستفيد من حرية الملاحة الفضائية؛ إذ أن الفضاء الخارجي لا يخضع لسيادة دولة معينة لذا لا يمكن التحجج بفكرة السيادة لإبطال عمل هذه الأقمار.

يُعد نظام "ايشلون" أبرز الأمثلة وأكثرها شهرة في مجال التجسس الإلكتروني عبر الأقمار الصناعية، ويعرف هذا النظام عموماً بأنه نظام تنصت إلكتروني عالمي يعبر عن أحد أوجه الاتفاقية المعروفة بـ "UKUSA" الموقعة بين الولايات المتحدة الأمريكية والمملكة البريطانية سنة 1947 والتي توسعت فيما بعد لتشمل دولاً أخرى تتوزع عليها قواعد التنصت، إذ تكلف كل قاعدة بتغطية أقاليم محددة؛ وعليه فهذه الاتفاقية تهدف إلى تقاسم وتشارك المعلومة بين مختلف المصالح السرية ووكالات الاستخبارات[4]، وهذا النظام المكون من 12 قمراً صناعياً مزوداً بكاميرات رقمية متطورة وكمبيوترات

---

[1]– ليلى بن حمودة، الاستخدام السلمي للفضاء الخارجي، المؤسسة الجامعية للدراسات والنشر والتوزيع، لبنان، 2008، ص. 11.

[2]– نفس المرجع، ص. 232.

[3]– ياسين قوتال، مرجع سابق.

[4]– يعبر نظام "إيشلون" عن أحد أوجه التعاون الذي جمع بين بعض الدول في مجال جمع الاستخبارات، هذا التعاون يرجع إلى فترة الحرب العالمية الثانية؛ إذ أظهرت هذه الأخيرة للعلن أهمية التجسس على المراسلات المتعلقة أساسا بإلتقاط =

متقدمة ولواقط إلكترونية ضخمة، وتصل قدرات هذه الأقمار إلى حد تصوير أي جسم على الأرض يصل حجمه لحجم كرة البيسبول في أي وقت ليلاً ونهاراً وأياً كانت حالة الطقس، وتستطيع فحص حركة الاتصالات وتبادل البيانات في كل أنحاء العالم انطلاقاً من الاتصالات الهاتفية ورسائل الفاكس ورسائل البريد الإلكتروني وشبكة الأنترنت إلى المعلومات التي تنقل عن طريق محطات الأقمار الاصطناعية والاتصالات السلكية والكوابل في أعماق البحار والتي تعالج فيما بعد بمساعدة حواسيب متطورة جداً، ورغم علم عديد الدول بوجود هذا النظام إلا أن خروجه للعلن لأول مرة كان نتيجة لتقرير أوروبي حمل عنوان "تقييم تقنيات التحكم السياسي" صدر في ديسمبر من سنة 1997[1]، وقد كان هذا النظام يترجم الحاجة إلى الاستخبار العسكري لكنه طور لأغراض الاستخبار الاقتصادي وأصبح إستراتيجياً مع عولمة المبادلات والمنافسة الاقتصادية [2].

المطلـــب الثانـــي: أبعـــاد التجـــسس الإلكترونـــي.

تشمل أبعاد التجسس الإلكتروني جميع مظاهره وكل العناصر ذات الصلة سواء بنشوئه أو بتداعياته، فلا تقتصر في هذا المجال على النتائج المترتبة عنه بل أيضاً على مجموعة الظروف التي أدت إلى هذه النتائج، ولصعوبة الفصل هنا بين السبب والنتيجة لارتباطهما الوثيق؛ فكثيراً ما يكون السبب هو الأثر، ويبرز هذا تحديداً من الأساس الذي تنبني عليه مبررات مشروعية التجسس ألا وهو سعي الدولة لحماية وصون أمنها؛ فالدولة تتحجج كسبب للقيام بالتجسس على دولة أخرى بحقها في حفظ أمنها من كل اعتداء وتقوم تأسيساً على ذلك بالمساس بأمن الدول الأخرى؛ وانطلاقاً من هذا المفهوم ستتم

=وتحليل الشفرات والموجات الإلكترومغناطيسية المعادية، وفي الواقع فالبريطانيون نجحوا في كسر شفرة الاتصالات الألمانية وقرروا بعد تردد كبير أن يتقاسموا أسرارهم مع الأمريكيين بموجب اتفاق شراكة بينهما يدعى "BRUSA" هذا الاتفاق الذي أصبح مقدمة لاتفاق سري للأمن بين الدولتين والمعروف بـ "UKUSA" سنة 1947 يتمحور حول تقاسم الملتقطات الإلكترومغناطيسية، والذي أسس لمواصلة عمليات التقاط الاستخبارات في زمن السلم، ليعرف انضمام دول أخرى ككندا واستراليا وزلندا الجديدة؛ وعليه تم تقسيم مناطق النفوذ والمسؤوليات التي تتضمن قواعد التنصت بين هذا الدول، وتسعى وكالة الأمن القومي إلى إلغاء التبعية والارتباط للقواعد الأرضية في الدول الأجنبية من خلال تدعيم الصناعة المعلوماتية التي تهدف إلى تطوير آلات لها القدرة على معالجة عدة تريليونات من العمليات في الثانية (التريليون يساوي 1000 مليار) وكذلك من خلال السيطرة على تقنيات التشفير، أنظر:

- Dany Deschenes, op. cit, p. p. 2– 5.

[1]– ممدوح الشيخ، مرجع سابق، ص. ص. 34–35.

[2]- L'affaire snowden et la nouvelle géopolitique du cyberespionnage, op. cit, p. 9.

دراسة أبعاد التجسس الإلكتروني من خلال فرعين: يتناول الفرع الأول أسباب التجسس الإلكتروني، ويتناول الفرع الثاني آثار التجسس الإلكتروني.

الفـــرع الأول: أسبــاب التجــسس الإلكترونــي.

أسهمت عديد الظروف والمعطيات في تسبيب وتبرير سلوك التجسس، وكذا في نقله من صورته التقليدية إلى الصورة الإلكترونية المعروف بها حالياً، ويمكن إجمال أهم الأسباب الدافعة إلى التجسس الإلكتروني في العناصر الثلاثة الآتية:

أولاً- حفــظ أمــن الدولــة والتصـدي لكل التهديدات المحتملــة:

ترتكز ممارسة التجسس بصفة عامة ودون تخصيص للإلكتروني منه، على حق الدولة في حماية أمنها، فبدون هذا الأمن يصبح بقاءها مهدداً فهو كما يذهب إليه سبينوزا جوهر الدولة[1]، ويعتبر أمن الدولة أو الأمن القومي كما يفضل البعض تسميته الهدف النهائي للدولة يعيش ويتعايش معها ويسعى القائمون على حكم الدولة في لحظة تاريخية ما إلى تحقيق الحدود المعقولة منه في ضوء الظروف والمعطيات التي تفرض نفسها على صناع القرار آنذاك؛ لذلك ليس غريباً القول أن أحد مداخل تقييم الحكم في فترة تاريخية ما يتمثل في كيفية تحقيق الأمن القومي للدولة والحفاظ عليه في مواجهة الآخرين وخاصة الأعداء الخارجيين[2]، وإذا كان أمن الدولة هو مجموع مصالحها الحيوية ومن ثم فتحقيقه إنما يتم بحمايتها، وهذه الحماية لا تقاس فقط بالقدرة العسكرية بل بأي تصرفات يسعى المجتمع من خلالها إلى تأكيد حقه في البقاء[3]، ويشكل جمع المعلومات من خلال ممارسة الجاسوسية أولى هذه التصرفات، فإذا كانت الجاسوسية في الماضي تعتبر وسيلة من وسائل الحرب ومن ثم ارتبطت بها على هذا النحو وجودا وعدما، فان الجاسوسية المعاصرة تجاوزت هذا المدى وأصبحت تشكل ضرورة في زمن السلم أكثر منها ضرورة في زمن الحرب وجب القيام بها وبكل عناية لأن الدور الذي تؤديه في نطاق حماية الأمن الوطني للدولة هو دور متعاظم الأهمية ومتعاظم الأثر والتأثير، دور يعود إليه الفضل في بناء الأمم والدول وحماية مصالحها والحفاظ على كيانها واستقلالها، كما يمكن أن يكون له نفس الدور في تدمير هذه الدول

---

[1]- فاوي الملاح، سلطات الأمن والحصانات والامتيازات الدبلوماسية، دار المطبوعات الجامعية، مصر، 1993، ص. 48.

[2]- جمال علي زهران، مرجع سابق، ص. 16.

[3]- فاوي الملاح، مرجع سابق، ص. 52.

وإضاعة استقلالها، ومن أجل ذلك أضحى التجسس في هذا العصر ضرورة لا يمكن تجاهلها أو التغاضي عنها، فالجاسوسية في عالم اليوم تعتبر أداة ووسيلة وفوق ذلك وظيفة أساسية لازمة لحياة الدول، وظيفة تتجاوز إطار الضرورة وتصل إلى أبعاد الحتمية، وظيفة ذات طابع خاص تمارس منذ القدم ومعترف بها ضمناً ولكنها غير مجازة ومن ثم تتم في السر والخفاء، إنها وسيلة الدول للهيمنة وإخضاع الغير وفرض الأمر الواقع، ومن هنا ستبقى الجاسوسية ما بقيت الدول حريصة على حماية مصالحها وحقوقها الوطنية ولكن خارج القانون[1]، وفي هذا الإطار يطرح تساؤل هام حول الطبيعة القانونية لكل من فكرة الأمن القومي وفكرة المصلحة العليا للدولة، ومما لاشك فيه أن فكرة الأمن القومي إنما هي فكرة قانونية تستند إلى حق الدولة في حماية أمنها القومي وهي مظهر من مظاهر سيادة الدولة ونتيجة من نتائج هذه السيادة، ويترتب على حق الدولة في حماية أمنها القومي حقها في أن تضع الخطوط والإجراءات التي تراها كفيلة بتحقيق أمنها القومي في جميع المجالات اقتصادياً وسياسياً وعسكرياً واجتماعياً، على النحو الذي يؤدي بالدولة إلى تحقيق وظائفها الثلاث، بينما نجد الطبيعة القانونية لفكرة المصلحة العليا للدولة لا تستند إلى القانون بل هي خروج عنه تستهدف أساساً صالح الدولة، وهي في هذا الإطار تتفق مع فكرة الأمن القومي في ضرورة تفضيل صالح الدولة على أي اعتبارات أخرى[2]، فيما يذهب رأي مؤيد إلى اعتبار المصلحة القومية جزء من كل بل والقلب في دائرة الأمن القومي التي تتسع لتشمل كل ما يمكن تسميته بالمصلحة القومية[3]؛ وعليه لا يمكن الفصل بين حدود ما يعتبر قانونياً أو ما يعتبر غير قانوني في إطار أمن الدولة؛ خاصة في عصرنا الحالي والذي تغيرت فيه بعض المفاهيم مما انعكس خصوصاً على تبرير التجسس وإعطاءه غطاء مشروعية له، ويمكن تحديد أهم هذه المتغيرات في العناصر الآتية:

أ- بروز الإرهاب واستخدامه كغطاء لممارسات أخرى من ضمنها التجسس؛ ففي سنة 1978 أصدر الكونغرس الأمريكي قانون الاستخبارات الأجنبية، ووفقا لهذا القانون يجوز التنصت على الدول الأجنبية وموظفيها، وفي أعقاب أحداث 11 سبتمبر 2001 التي زعزعت أمن الولايات المتحدة الأمريكية بدأ الكونغرس إجراء العديد من التعديلات على القوانين القائمة فأصدر قانون الباتريوت الذي حمل رقم

[1]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 6-7.

[2]- فاوي الملاح، مرجع سابق، ص. 55.

[3]- جمال علي زهران، مرجع سابق، ص. 20.

3162-107 متضمناً العديد من الإجراءات الصارمة بغية تمكيـن السلطات من تعقـب المسؤولين عن هجمات سبتمبر والوقاية من أية هجمات مستقبلية مماثلة، ومن هذه الإجراءات التوسع في مراقبة اتصالات الإرهابيين سواء في التحقيقات الجنائية أو لجمع الاستخبارات الأجنبية[1]، وفي المقابل تلجأ الدول التي تمتلك أو تشارك في أنظمة للتجسس الإلكتروني إلى تبرير شرعية سلوكاتها بالقول بأن الدافع هو مكافحة الإرهاب، وأن هذه الأنظمة لها دور رئيس في هذا وبدونها لا يمكن رسم استراتيجيات مكافحة ملائمة وناجحة.

ب- تغير مفهوم الحرب كنتاج للثورة المعلوماتية؛ بحيث ظهرت الحرب المعلوماتية كقطيعة إستراتيجية مع الصراعات الكلاسيكية بسبب خصائصها (عالمية ميدان التحرك وتعدد فـــرص النجـــاح للمهاجم)، فبالنسبة لعدد من المحللين فإن ميدان المعركة المستقبلي سيكون الفضاء الإلكتروني[2]؛ لأن هذا الأخير يختصر التكلفة سواء البشرية أو المالية، فمن جهة حرب الغد أو الحرب المعلوماتية تهدف أساساً لإبعاد الإنسان عن ساحة المعركة فالجندي يخوض قبل كل شيء حرب معلومات[3]، ومن جهة ثانية نجد أن تمويل العمليات العسكرية العادية أمر مكلف لذا فتمويل فريق حرب معلومات تقني مؤلف من متخصصين بعمليات التسلل عبر أجهزة الكمبيوتر وشبكاته باستخدام آخر ما توصلت إليه تقنية الحاسبات الآلية أقل كلفة بكثير[4]؛ فأكثر ما تتطلبه هذه الحرب هو التحكم في تقنيات اختراق البنى التحتية المعلوماتية والاحترافية العالية والقدرة على تجاوز إجراءات المراقبة والتشفير دون نسيان الكشف المسبق عن القطاعات المفتاحية المدنية والعسكرية للخصم[5].

---

[1]- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية (دراسة تأصيلية تحليلية ومقارنة للتنصت على المحادثات التليفونية والتي تجري عبر الأنترنت والأحاديث الشخصية نظرياً وعملياً)، دار المطبوعات الجامعية، مصر، 2009، ص. ص. 42-44.

[2]- Irnerio Seminatore, la géopolitique a l'âge numérique, sixième conférence de la onzième année de l'academia diplomatica europaea, institut européen des relations internationales, Bruxelles, 13/02/2014, publie sur le site www.ieri.be, le site a été visité le 04/02/2015.

[3]- René Trégouet, présentation de colloques: introduction générale, actes de la rencontre internationale de prospective du sénat intitulé "la guerre du futur : analyse prospective de l'avenir des conflits, palais du Luxembourg, jeudi 27 novembre 2003, publié sur le site www.penseemiliterre.fr, le site a été visité le 23/11/2015.

[4]- ذياب موسى البداينة، الإرهاب المعلوماتي، مرجع سابق.

[5]- Irnerio Seminatore, op. cit.

ج- السباق التكنولوجي والعلمي في مجال التسلح؛ فمنذ أن اكتشف الإنسان الحرب ارتبط بتطوير تكنولوجيات جديدة لأسلحته بغرض حيازة التفوق على الخصم، هذا التسابق نحو التسلح كان دوماً مرتبطاً بالأبحاث التكنولوجية هذه الأخيرة التي تبقى جوهرية لأجل تطوير الأنظمة المستقبلية للتسلح فالريادة في مجال التسابق هنا تعود لمخابر الأبحاث العلمية[1]؛ فعصرنا الحالي يتميز بتقوية الشراكة بين البحث العام المدني والبحث في قطاع الدفاع خاصة في ظل العولمة التي غيرت الرهانات وأشكال التهديدات مما يتطلب استثمارات جديدة في ميدان البحث، هذا التداخل بين القطاع المدني والعسكري يدلل عليه أن عديد المنتجات المدنية تم تبنيها لأغراض واستخدامات عسكرية، والأسواق المدنية أصبحت مهمة جداً في بعض القطاعات خاصة المعلوماتية والإلكترونية[2]، هذا الدور الذي لعبته الشراكة في ميدان البحث لتطوير التكنولوجيا خاصة المتعلقة بالتسليح والتي انفردت بها بعض الدول المتقدمة وجعلتها حكراً عليها، وفي ذات الوقت سعت لأن تمنع غيرها بأساليب عديدة (أهمها الأدوات القانونية من خلال وضع اتفاقيات دولية للحد من التسلح) من أن تصل إلى ذات المستوى، وفي هذا الصدد نذكر ما جاء في الوثيقة الرسمية المنشورة من طرف البيت الأبيض الأمريكي في 20 سبتمبر 2002 عقب تفجيرات الحادي عشر سبتمبر بعنوان "إستراتيجية الأمن الوطني للولايات المتحدة الأمريكية" من أنها ستعمل من أجل منع وصرف كل الخصوم المحتملين من الدخول في سباق التسلح على أمل التفوق و التساوي في القوة معها[3]، وعليه فالدول المتقدمة تعمل على تطوير الأبحاث في ميدان التطوير التكنولوجي خاصة للأغراض العسكرية وفي ذات الوقت تعمل على مراقبة باقي الدول لمنعها من ذات النشاط متحججة بضرورة وقف التسابق نحو التسلح.

د- تصدر الأمن الاقتصادي لقائمة أولويات الأمن القومي للدولة؛ فالأمن القومي اليوم لم يعد يرتكز على القوة العسكرية بل أصبحت الهيمنة والريادة الاقتصادية الدولية أهم مرتكزاته، فالعولمة من

[1]- Jean –Baptiste De Fontenilles et autres, la course technologique en matière d'armement: une nécessité qui peut être métriser ou, au contraire, un risque technologique déconnecté de la réalité opérationnelle et géostratégique, rapport sur les travaux de la comité n°=7 à la 45eme session national, 2009,p . 134-135. rapport publié sur le site www.chear,france/wiheden.fr, le site a été visité le 23/11/2015.

[2]- Jean-Jaque Gagnpain, les révolution technologiques qui préparent le futur, actes de la rencontre internationale de prospective du sénat intitulé "la guerre du futur: analyse prospective de l'avenir des conflits, palais du Luxembourg, jeudi 27 novembre 2003, publié sur le site www.penseemiliterre.fr, le site a été visité le 23/11/2015.

[3]- René Trégouet, op. cit.

منظورها الاقتصادي تدل على تنامي واستقلالية الاقتصاد مقارنة بالسياسة خاصة؛ وقد أسهم في هذا المفهوم تحول التقنيات وثورة المعلومات التي سمحت بالنقل السريع لرؤوس الأموال، وكذا توسع وتمدد شبكات الاستثمار التجاري المقامة من طرف الشركات متعددة الجنسيات، وتقدم المفاوضات متعددة الأطراف بغرض تحرير المبادلات وتحرير اقتصاديات الدول التي هي في طريق النمو، فالعلاقات بين السلطة السياسية والسلطة الاقتصادية قد عدلت بشكل معتبر، فالدولة لم تعد تحوي داخل حدودها الاقتصاد الوطني بل هي ذاتها أصبحت قطعة من الأسواق الدولية[1]؛ فالمجتمع الدولي اليوم أصبح إن صح التعبير السوق الدولي والهيمنة فيه لمن يهيمن اقتصادياً لذلك نلحظ بروز التجسس الاقتصادي كأهم صور التجسس حالياً، حتى أن الدول المتقدمة الآن تتجه لدعم التجسس الذي تقوم به مؤسساتها الاقتصادية العامة كما الخاصة وتسخر جهود أجهزتها الاستخبارية لهذا الغرض، بل وتجعل الاستخبار الاقتصادي في قلب سياسات المؤسسة فيما يتعلق بأمنها المعلوماتي؛ إذ أنه يمكنها من كشف التهديدات المحتملة ويؤدي إلى الحد أو التقليل من منافذ التهديد الهجومي، والحد من تكلفة الوقت وأرباح العدو بدخوله إلى الشبكة المعلوماتية؛ إذ ليس من المجدي الاعتماد والاتكال على الدفاع؛ وعليه يستوجب على المؤسسات والمنظمات أن تعرف كل ما يدور حولها بشكل يمكنها من تحديد متى سيتم القيام بأي هجوم أو متى يكون هناك اعتداء وشيك[2]، فحماية المعلومات والأسرار الاقتصادية للدولة يتطلب التجسس على المعلومات والأسرار الاقتصادية للدول الأخرى، ويأخذ لفظ العدو المستخدم أعلاه معان خاصة في مجال التجسس الاقتصادي، فإلى جانب العدو الحقيقي هناك العدو المحتمل ويقصد به الأصدقاء، بل إن الخبراء يذهبون إلى أن جمع المعلومات عن الأصدقاء يفوق جمع المعلومات عن الأعداء[3].

ثانيـاً– الثـورة التكنولوجيـة والتحـول إلـى الفضـاء الإلكترونـــي:

مرت البشرية حتى الآن بثلاث مراحل تطورية تم التعبير عنها باستخدام مصطلح الثورة للدلالة على التغييرات الجذرية التي رافقتها على مختلف الأصعدة، من الثورة الزراعية إلى الثورة الصناعية إلى

[1]- Saida Bedar, perspectives et prospectives du contexte stratégique, actes de la rencontre internationale de prospective du sénat intitulé "la guerre du futur : analyse prospective de l'avenir des conflits, palais du Luxembourg, jeudi 27 novembre 2003, publié sur le site www.penseemiliterre.fr, le site a été visité le 23/11/2015.

[2]- cyberthreat intelligence and the lessons from law enforcement, publication of KPMG, Suiss, May 2013, p. 3, publié sur le site: wwwkpmg.com, le site a été visité le: 23/11/2015.

[3]– ممدوح الشيخ، مرجع سابق، ص. ص. 159– 160.

الثورة المعلوماتية والتي سميت كذلك بالموجة التطورية الثالثة؛ بحيث يبقى النصف الثاني من القرن العشرين قرن المعلومات، ولاشك أن استخدام أجهزة تسمح بمعالجة هذه المعلومات هو ركيزة هذه الثورة الهائلة؛ فقد كانت المعلومات المتولدة عن التفاعلات البشرية محدودة إلى حد كبير ولم يمثل حجمها أية مشكلة أمام عمليات تجميعها وتخزينها ومعالجتها واسترجاعها، لكن مع تقدم الإنسان وزيادة معارفه وعلومه بدأ كم المعلومات بالتزايد وإزاء هذه الطفرة بدت الطرق التقليدية لجمع وتنظيم المعلومات عاجزة عن تلبية احتياجات المستفيدين منها بكفاءة وفاعلية ؛وأصبح من الضروري استخدام أساليب علمية وتقنية متطورة لمواجهة هذا الكم من المعلومات؛ فكانت أن ظهرت الحواسيب الآلية للتحول إلى مخازن كبيرة قادرة على تجميع واستيعاب كم ضخم من المعلومات، وقادرة أيضا على استرجاعها بسرعة فائقة ودقة متناهية؛ ومن ثم أصبحت المعلومات مورداً لا يقل ولا ينضب بل يتزايد دوما وهي في الوقت الراهن مفتاح للموارد الأخرى ومصدر قوة سياسية واقتصادية لمن يحسن جمعها وتنسيقها واستخدامها[1]. وبظهور تقنيات الاتصال الحديثة وفي مقدمتها الأنترنت ظهر ما يعرف حالياً بتكنولوجيا المعلومات والاتصالات "TIC" كنتيجة للمزاوجة بين تكنولوجيا المعلومات وتكنولوجيا الاتصالات؛ إذ مكن هذا التزاوج من نقل ذلك الكم الهائل من المعلومات عبر العالم ككل بمعنى أن هذا الانتقال لا يخضع لقانون أو حدود مما منح الفرص الثمينة للدول والأفراد للحصول على المعلومات المصنفة حساسة وسرية من بينها، وما زاد من خطورة الوضع كون هذه التكنولوجيات قد أدخلت في جميع نواحي حياتنا، فهناك إدارة إلكترونية وتجارة إلكترونية و تعليم إلكتروني وتقاضي إلكتروني وصحة إلكترونية، وكذلك حرب وجيش إلكتروني، وبالموازاة مع هذا أصبح لدينا أيضا مواطن إلكتروني، وبتحول كل المفاهيم الكلاسيكية إلى مفاهيم إلكترونية تحول أيضا العالم الواقعي الحقيقي إلى عالم افتراضي سمي بالفضاء الإلكتروني، وهو كمصطلح استخدم للتعبير عن الأنترنت عام 1991 وأصبح فيما بعد مفهوماً أشمل منها ليضم كل الاتصالات والشبكات وقواعد البيانات ومصادر المعلومات؛ وأصبحت بنية النظام الإلكتروني تعني المكان الذي لا يعد جزءاً من العالم المادي أو الطبيعي؛ حيث أنها ذو طبيعة افتراضية رقمية إلكترونية تتحرك في بيئة إلكترونية حيوية تعمل من خلال خطوط الهاتف وكابلات الاتصالات والألياف البصرية والموجات الكهرومغناطيسية[2]، ويمتاز هذا الفضاء أو العالم الجديد بما يلي:

[1]– محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، مصر، 2004، ص. ص. 12-14.

[2]– عادل عبد الصادق محمد الجخة، مرجع سابق، ص. ص. 28-29.

أ- الفضاء الإلكتروني وبعكس باقي الأبعاد (الأرض، الجو، البحر، الفضاء) غير مادي (باستثناء بناه التحتية)، فهو مشكل من حزم من الإلكترونات المسافرة وليس من مواد صلبة.

ب- الفضاء الإلكتروني غير إقليمي لأن المواقع الجغرافية للمشتركين فيه مختلفة (وتتغير باستمرار).

ج- الفضاء الإلكتروني متغير وغير ممركز لأنه غير مرتبط أو تابع لأي مركز أو قاعدة.

د- الفضاء الإلكتروني لا يخضع لسلطة أو تبعية سلمية لأن بناه مسطحة وأفقية[1].

هـ- الفضاء الإلكتروني يمتاز بغياب الحدود الجغرافية وغياب الحكم القاهر لعنصر الزمن[2]؛ إذ يشكل تحولا جديداً في التاريخ الإنساني؛ ففي الوقت الحقيقي أو شبه الحقيقي يحدث كل شيء[3].

لقد أدى النمو السريع للفضاء الإلكتروني وتزايد تشابك وربط الأنظمة إلى توسيع إمكانيات جمع المعلومات لذا فالحصول على وضعية نوعية للاستخبار في هذا الفضاء هو شرط مسبق لحماية البنى التحتية وكذا لقيادة وإدارة العمليات؛ فكيانات الدفاع تحتاج لامتلاك بصيرة واضحة فيما يخص التهديدات الإلكترونية التي يمكن أن تتعرض لها لأجل أن تكون قادرة على حماية ذاتها بشكل فعال في مواجهة هذه التهديدات وهذا يتطلب معرفة هذه التهديدات نفسها كما التفطن لإمكانات ونوايا المعتدين المحتملين[4]؛ فيتم استخدام التجسس للوقاية من التجسس .

ثالثـاً- القيمـة الماليـة الكبيرة للمعلومـات الحساسـة وظهـور فواعـل دوليـة جديـدة:

تشكل المعلومات الحساسة والتي تسعى الدول جاهدة لإبقائها سرية وحمايتها من كل أشكال التهديدات الإلكترونية الحالية مصدراً للثروة؛ بما تمثله من قيمة تجارية عالية، ونظراً لكون الفضاء الإلكتروني ملكاً إنسانياً مشتركاً وليس حكراً على دولة أو جهة معينة؛ فقد أصبحت لكل مكوناته ذات المكانة وذات الدور وذات القدرة على إحداث الأضرار؛ وعليه لم تعد الدولة الممارس الوحيد للتجسس، بل ظهرت إلى جانبها فواعل كثيرة: كالأفراد وجماعات الجريمة المنظمة والمنظمات الإرهابية، وهناك من

[1]- Laurent Murawiec, la cyber guerre, publie sure le site www.societestrategie.fr, le site a été visité le: 23/11/2015.

[2]- عادل عبد الصادق محمد الجخة، مرجع سابق، ص. 29.

[3]- Laurent Murawiec , op. cit.

[4] - The Defence cyber strategy, op. cit. p. 12.

الباحثين من وضع سلم ترتيب لهذه الفواعل تبرز موقعها ومستويات التهديد الذي تشكله بحيث ترتب هذه التهديدات في خمس مستويات انطلاقاً من متغيري الإمكانيات والتأثير، فيأتي في المستوى الأول الأفراد (الهاكرز – الكراكرز)، ثم يأتي المرتزقة والمستأجرون الإلكترونيون في المستوى الثاني، ثم تليها منظمات الجريمة المنظمة العابرة للحدود ثم منظمات الإرهاب العابر للحدود، وفي المستوى الخامس يأتي الاستخبار الأجنبي الممارس من قبل الدول[1]، فالكل يسعى للوصول إلى مخزون المعلومات السري للدول مدفوعاً ببواعث متباينة؛ فالأفراد باختلاف المسميات التي تطلق عليهم قد يمارسونه لحسابهم الخاص إما ابتغاء تحقيق مكاسب مادية من خلال المتاجرة فيها، أو لإثبات الذات وتحقيق الشهرة، أو لتحدي أنظمة الحماية والأمن المعلوماتي، أو لمجرد التسلية وتمضية الوقت، أو بغرض الانتقام من جهة معينة، خاصة من قبل المستخدمين؛ فالمستخدمون يمكن أن يكونوا جبهة الدفاع في مؤسسة معينة، أو أن يكونوا أكبر تهديداتها؛ إذ لهم حالياً القدرة أكثر من أي وقت مضى على الدخول إلى كم هائل من المعلومات والبيانات، فتقريباً أي مستخدم بإمكانه أن يسرق معلومات حساسة[2]، وهناك صنف آخر من الأفراد يسمون بالمرتزقة أو المستأجَرون الإلكترونيون وكما تدل عليه تسميتهم يعملون لمن يدفع؛ بحيث أن العمليات الإلكترونية ذات المدى المتسع تستدعي التواجد المتزامن للقدرات والتخصصات المعلوماتية الجد دقيقة ووسائل متطورة، ويوجد في الفضاء الإلكتروني شبكة حقيقية من المرتزقة تسمح بتغطية الاحتياجات المرتبطة بتسيير وقيادة العمليات الإلكترونية، كذا نجد مطوري برامج الإتلاف كالفيروسات، وبرامج الاختراق كأحصنة طروادة، يتم التكفل بها من قبل مطورين يعرضون خدماتهم بمقابل[3]، أما جماعات الجريمة المنظمة فهدفها الأوحد تحقيق المكاسب المالية لحد أن البعض سماها بالكوارتل الإلكترونية التي ستجاوز كوارتل المخدرات في طرح التهديدات الواسعة للأمن الكوني[4]، وهناك منظمات الإرهاب التي يتجاوز خطرها الأصناف السابقة رغم أنها قد توظفهم للحصول على المعلومات، وقد تم شرح هذا

[1]- Kevin A.O'Brien, cyberintelligence: for threat profiling of sub-state actors in the information aga, rand Europe, Cambridge, united kingdom, p. 30, study published on: www.isodarco.it, 23/11/2015.

[2]- cyberespionage: the harsh reality of advanced security threats, publication of DELOITTE (centre for security and privacy solution), 2011, p.12, study published on: www.isaca.org, 23/11/2015.

[3]- Pierre Caron, la guerre électronique n'aura pas lieu, association des anciens de l'école de guerre économique, p. 7, article publié sure le site www.bdc.aege.fr, le site a été visité le: 23/11/2015.

[4]- cyberespionage: the harsh reality of advanced security threats, op. cit, p.5.

العنصر في معرض الحديث عن خصائص التجسس الإلكتروني، وتبقى الإشارة إلى صنف جديد في هذا الإطار وهو مجموعة المواقع الإلكترونية التي تقوم بنشر ملفات وتقارير سرية تخص دول مختلفة، وهذه المواقع كثيرة وتتزايد بإستمرار، لكن أهمها وأكثرها شهرة نجد موقع ويكيليكس، وكل هذه المواقع لها مبرر مشترك لما تقوم به: "إخضاع القوة التي تمارس خلف الأبواب المغلقة للتدقيق والفحص الشعبي والجماهيري" وهذا باستخدام الأنترنت كأرضية لخلق الشفافية كما يزعم مؤسسوها[1].

الفـــرع الثانـــي: آثـــار التجـــسس الإلكترونـــي.

سبقت الإشارة إلى أن أهم أثر للتجسس الإلكتروني هو ذاته أهم سبب دافع لممارسته، فالتجسس يأتي كسبب لحماية أمن الدولة وفي ذات الوقت يؤدي للمساس بأمن الدولة، ونظرا للحديث في أكثر من موقع على مفهومه ومشتملاته فسوف تقتصر دراسة الآثار على عنصرين مهمين هما: أثر التجسس الإلكتروني على سيادة الدولة، وأثر التجسس الإلكتروني على الحياة الخاصة للأفراد.

أولاً- أثـر التجـسس الإلكترونـي على سيـادة الدولـة:

يقصد بالسيادة كعنصر من عناصر الدولة أنه توجد إلى جانب الإقليم والسكان سلطة لا تعلوها سلطة تستأثر بمباشرة جميع الاختصاصات داخل حدود الإقليم في مواجهة الرعايا وتتصرف في الخارج على قدم المساواة مع غيرها من السيادات المماثلة[2]، ومن المعروف وجود ارتباط وثيق بين أمن الدولة وسيادتها، فالأول يعد مظهرا للثاني وانعكاسا له؛ إذ يمكن للدولة استناداً لميزة السيادة أن تتخذ كل ما تراه كفيلاً بحماية أمنها، ويعد السعي للوصول إلى أسرار الدول الأخرى من بين ما يمكن للدولة اللجوء إليه لتحقيق هذا الغرض؛ وعليه يكون لكافة الدول استناداً للغطاء الشرعي "السيادة" أن تمارس التجسس على بعضها وهي بذلك تستند على السيادة لتمس بالسيادة، هذا المظهر يُعد الأثر التقليدي للتجسس بصفة عامة دون تخصيص لصنف منه، لكن ذات الأثر عرف تغييرات عميقة ارتبطت بالعناصر الحديثة التي أُدخلت على مفهوم السيادة ذاتها المرتبط بقدرة السلطة على التحكم في عنصري الإقليم والشعب؛ بحيث وكما سبقت الإشارة إليه أدى تعميم تقنيات المعلومات والاتصالات إلى ظهور عالم مواز للعالم الحقيقي اصطلح على تسميته بالفضاء الإلكتروني يمارس عبره الأفراد كما الدول ذات التصرفات التقليدية لكن

[1]- Daniel Domscheit-Berg, Inside wikileaks, crown publishers, New York, United states, 2011, p. 8.

[2]- فاوي الملاح، مرجع سابق، ص. 77.

بطريقة إلكترونية؛ فطغى هذا المشهد التطوري على السيادة بمفهومها القديم ليشكل ما يعرف بسيادة الفضاء السيبيريني، والذي ما فتئ وأن أصبح الوطن الجديد للإنسان وحتى الدولة[1]، فتغير بذلك مفهوم الإقليم والشعب الذين تمارس السلطة عليهما سيادتها الداخلية؛ فالإقليم لم تعد حدوده محصنة؛ إذ استطاعت ثورة المعلومات والاتصالات أن تفرز مجالات جديدة سواء أمام الدول المتطورة تمكنها من إفراغ السيادة الإقليمية للدولة من مضمونها؛ فلم تعد السيادة في إطارها الإقليمي بالسياج المغلق على الدولة التي تمارسها، بل إن المجالات الأساسية للسيادة الإقليمية أصبحت متاحة ومفتوحة ومباح التعرف عليها لحائزي الوسائل والأجهزة الإلكترونية المختلفة كالتنصت عن طريق الأقمار الصناعية؛ بحيث أصبحت الدول المالكة لهذه الأجهزة المتطورة تَنْفُذ للمجالات الأساسية للسيادة الإقليمية وتتعرف عليها بدون موافقة الدولة المعنية[2]، كما يمكن للأفراد وجماعات الجريمة المنظمة وكذا لمنظمات الإرهاب أن تستغل التقنيات التي تمنحها الحواسيب والأنترنت لاختراق الفضاء الإلكتروني للدول والحصول على أسرار دفاعها الوطني من أي نقطة في العالم دون منح أية أهمية للحدود الجغرافية التقليدية. وبالإضافة إلى الإقليم نجد الشعب المكون الثاني للدولة قد تأثر مفهومه بالثورة المعلوماتية؛ إذ أن المهم في الشعب ليس كونه مجموعة من البشر كما قد يوحي التعريف القانوني للمصطلح، وإنما تكمن أهمية الشعب وماله من تأثير مباشر على قوة الدولة في مدى تماسك هذا الشعب وولائه للدولة التي ينتمي إليها، ونتيجة لتأثيرات هذه الثورة والشبكات الحاسوبية على إدراك المرء للزمان والمكان والتحكم في المسافات والقفز على الفواصل الجغرافية يمكن أن يتكون نوع من الإحساس بالولاء والمشاركة وهو ما يطلق عليه المجتمعات الإلكترونية ومن شأن ذلك أن يضعف من ولاء الشعوب لدولهم[3].

وعليه فالتجسس الإلكتروني وعلاوة على مساسه بالسيادة بالمفهوم التقليدي، يجد مجال تأثيره في المفهوم الحديث للسيادة أي سيادة الفضاء الإلكتروني بتجاوزه للحدود الإقليمية التقليدية واستفادته من مفهوم الشعب الإلكتروني المتحرر من روابط الولاء لدولة معينة؛ وعليه فأثر التجسس الإلكتروني على السيادة مستمد من خصائص العصر المعلوماتي.

---

[1]– وليد غسان سعيد جلعود، مرجع سابق، ص. 49.

[2]– ليلى بن حمودة، مرجع سابق، ص. 34.

[3]– ثامر كامل محمد، مرجع سابق، ص. ص. 124–125.

ثانيـاً- أثــر التجـسس الإلكتروني على الحياة الخاصـة للأفــراد:

في مقابل مساس التجسس الإلكتروني بالدول، فهو وبذات الغرض يعرض الحياة الخاصة للأفراد للانكشاف؛ وهذا من خلال جمع المعطيات عن الأفراد؛ الأمر الذي يُمكن من رسم صورة كاملة عن الدولة والتعرف على بنيتها الاجتماعية ومواطن الخلل فيها أو حتى لابتزاز الأفراد واستغلالهم في الوصول لأسرار الدفاع الوطني[1].

ويعد الحق في الخصوص من الحقوق السابقة على وجود الدولة ذاتها لذا فقد حظيت الحياة الخاصة للأفراد بحماية دستورية وقانونية كبيرة في دول العالم قاطبة وشهدت السنوات الأخيرة استجابة تشريعية على مستويات مختلفة لدواعي هذه الحماية وسايرها القضاء بتجاوب ملحوظ مؤيداً من الفقه لما للحياة الخاصة للأفراد من أهمية قصوى على كيان الفرد و المجتمع معا[2]. وتعرف الحياة الخاصة بأنها: "تلك الرقعة من حياة الإنسان التي يجب أن يترك فيها يعيش في حياة حميمية سرية وهادئة بعيداً عن أنظار وأسماع وتدخل الغير ورقابتهم وذلك في حدود المشروعية"[3]، وتشمل الحياة الخاصة في العصر المعلوماتي ثلاثة طوائف من المعطيات الشخصية تختلف من حيث قابلية جمعها، وهي:

أ- **المعطيـات الشخصيـــة:** وهي المعلومات المتعلقة بشخص طبيعي معرف أو يمكن تعريفه مباشرة أو بطريقة غير مباشرة بالرجوع إلى العناصر المرتبطة به و الخاصة به، كالاسم واللقب، والعنوان الطبيعي أو الإلكتروني، ورقم الهاتف، وتاريخ ومكان الميلاد، ورقم الضمان الاجتماعي، والبصمة الرقمية، وهذه المعطيات يمكن جمعها وتخزينها مع إمكانية حق الدخول والتصحيح والتعديل من طرف حاملها.

---

[1]- ومن الأمثلة تعرض صفحة (mon compte) بموقع أورانج للاختراق بتاريخ 2014/01/16؛ مما أدى إلى سرقة معطيات شخصية لـ 800.000 زبون، لتتعرض للاختراق مجدداً في 2014/05/07؛ مما أدى إلى سرقة معطيات 1300 زبون، ومن أمثلته أيضاً تصريح مؤسس (vkontakte) النظير الروسي للفايسبوك، بأن المصالح السرية الروسية طلبت منه معلومات شخصية عن معارضين روسيين وأوكرانيين، وأنه قام برفض إفشاءها مما جعله يضطر لمغادرة البلاد، أنظر:
- Ryan Burton, op. cit, p. p. 4-8.

[2]- سوزان عدنان الأستاذ، انتهاك حرمة الحياة الخاصة عبر الانترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد الثالث، المجلد التاسع والعشرون، سوريا، 2013، ص. 423.

[3]- صفية بشاتن، الحماية القانونية للحياة الخاصة، أطروحة دكتوراه، مقدمة لكلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012، ص. 103.

ب- المعطيـات الحساســة: وهي تلك المعطيات ذات الأصل العرقي أو الإثني، وكذا الآراء السياسية والفلسفية والدينية، والمعطيات المتعلقة بالصحة أو بالحياة الجنسية، ولا يمكن جمعها إلا بالموافقة الصريحة للشخص المعني.

ج- معطيـات الربـط أو التواصـل: وهي المعلومات التي تسمح بتحديد هوية مالك اشتراك انطلاقاً من رقم الهاتف أو عنوان (IP)، ويمكن جمعها في الشروط المحددة حصراً بالقانون وهي مشابهة للمعطيات ذات الطبيعة الشخصية[1].

وفي ظل الوسائط الإلكترونية الحديثة أمكن لعديد الأطراف التوصل إلى المعلومات المرتبطة بالحياة الخاصة للأفراد واستغلالها في خدمة مصالحها وللإضرار بأمن الدولة، وهذا يرجع إلى العوامل الآتية:

أ - إتاحة الحاسبات الآلية إمكانات فائقة لتخزين ومعالجة واسترجاع ومقارنة ونقل كم هائل من البيانات.

ب - ظهور ما يسمى ببنوك المعلومات؛ حيث تقوم الكثير من المؤسسات الكبرى والشركات الحكومية والخاصة بجمع بيانات عديدة ومفصلة عن الأفراد تتعلق بالوضع المادي والصحي والعائلي أو العادات الاجتماعية أو العمل ... وتستخدم الحاسبات وشبكات الاتصال في تخزينها ومعالجتها وتحليلها والربط بينها واسترجاعها ونقلها؛ وهو ما يمنح فرص الوصول إليها على نحو غير مأذون ويفتح مجالاً أوسع لإساءة استخدامها[2].

ج- عرض الذات على الأنترنت؛ بحيث أن تطور الأنترنت وتحديداً الشبكات الاجتماعية ومبدأ عملها القائم على تشجيع مستخدميها على إذاعة كم كبير من المعلومات؛ دفعت الأفراد إلى العرض وبصورة مستمرة ومتزايدة لحياتهم الخاصة فيها[3]، كما أن جهات أخرى قد تستخدم هذه الشبكات أو مواقع

---

[1]- Cecile DOUTRIAUSC, donnés personnelles et cybersurveillance, la RDN, chaire cyber-défense et cyber-sécurité, n°=775, paris, décembre 2014,p. 2, publié sur le site www.chaire-cyber.fr, le site a été visité le: 23/11/2015.

[2]- هشام محمد فريد رستم، مرجع سابق، ص. ص. 197-180.

[3]- Emmanuèle DAOUD et autres, libertés fondamentales et protection des données personnelles, revue LAMY droit des affaires (RRDA), numéro 87, Walters Kluwer, France, novembre 2013.p. 85.

أخرى كمواقع التوظيف الوهمية وبعض المواقع الإحصائية وذلك في التواصل مع الأفراد والحصول منهم على المعلومات وخاصةً باستخدام أساليب الهندسة الاجتماعية، والتي تقوم على استخدام حيل نفسية وتكنولوجية لسحب المعلومات الحساسة من مستخدمي الحواسيب والأنترنت والوصول إلى عمق مخزونهم المعلوماتي وكذا تلك المعلومات المتعلقة بواقعهم القومي والاجتماعي؛ ومن ثم إعادة صياغتها بشكل سياسي واقتصادي واجتماعي وأمني يضر بالأمن القومي للدولة المستهدفة[1]، ومن جهة أخرى هناك الكثير من البرامج المعتبرة كوسائل اتصال مهمة ومستخدمة بكثرة عبر الأنترنت والتي تحتفظ بكم هائل من المعلومات المختلفة حول الأفراد لكنها بالمقابل وكما يرى الكثيرون تطرح إشكاليات تتعلق بمدى إتباعها لإجراءات الأمن التي تضمن الحفاظ على سرية تلك المعلومات الشخصية، وكذا على سرية محتويات الاتصالات التي تتم بين الأفراد؛ مما دفع بعض الدول إلى تقييد استخدامات مثل هذه البرامج[2].

[1]– وليد غسان سعيد جلعود، مرجع سابق، ص. 58.

[2]– وهو الموقف الذي اتخذته فرنسا حيال برنامج الاتصال عبر الأنترنت المسمى بـ "السكايب" فنظراً لعدم إتباعه لعدد من معايير الأمن من جهة، وقدرته على جمع واستخدام قائمة كبيرة من المعلومات الشخصية؛ فقد تم منعه في الجامعات وفي مراكز الأبحاث وفي المدارس العليا منذ سنة 2005، أنظر:

- Abderrahmane Nitaj, la cryptographie et la confiance numérique, étude, université de Caen Basse, Normandie, 23 mars 2013, p. p. 6– 7.

الفصـــــل الثانـــي:

محـــــل التجـــــسس الإلكترونـــــي.

تهدف الدولة من خلال الأحكام الصارمة التي تقررها للتجسس إلى حماية أسرار دفاعها الوطني من كل أشكال الاعتداء التي يمكن أن تتعرض لها؛ وهذا بالنظر إلى تشعب هذه الأسرار وتعدد صورها وتعلقها بكافة نواحي حياة الدولة وركائزها العسكرية والسياسية والاجتماعية والاقتصادية؛ وعليه يؤدي التوصل إليها إلى المساس بأمن الدولة وتهديد مقومات بقائها؛ لذا حرصت جميع الدول على اتخاذ كافة الإجراءات لإبقاء أسرارها بعيدة عن الكشف والاطلاع. لكن بتطور التقنية وانتشار استخدام الحواسيب الآلية وشبكات الإتصالات بشكل واسع اتجهت الدولة لاستخدام هذه التقنيات والاستفادة مما توفره من مزايا، ليشمل الأمر حتى استخدامها لتخزين أسرارها بصورة رقمية يسهل معالجتها آليا؛ مما استتبع أن تتطور تقنيات الوصول إلى تلك الأسرار فأصبحنا أمام تجسس إلكتروني يستهدف أسراراً إلكترونية. وتجدر الإشارة إلى أن السر الإلكتروني يأخذ ميزته هذه من استخدام أنظمة المعالجة الآلية في تخزينه واسترجاعه ونقله وإدخال مختلف التعديلات عليه، ولا يمس هذا بمفهوم السر بحيث يبقى ذاته، بمعنى أن ما يجعل سراً من الأسرار إلكترونياً هو وسيلة المعالجة (حواسيب وشبكات اتصال) لكن جوهر السر يبقى واحداً لا يتغير بتغير وعاء السر (نظام المعالجة الآلية) ولا بتغير شكله (معلومات إلكترونية)؛ وعليه ستتم دراسة محل التجسس الإلكتروني (أسرار الدفاع الوطني) من خلال مبحثين: يتناول المبحث الأول مفهوم سر الدفاع الوطني، بينما يتناول المبحث الثاني وعاء سر الدفاع الوطني الإلكتروني وشكله.

المبحـــث الأول: مفهـــوم ســـر الدفـــاع الوطنـــي.

تطرح الإحاطة بمفهوم سر الدفاع الوطني عديد الصعوبات تتعلق من جهة بمرونة مصطلح سر الدفاع الوطني وعدم وجود تعريف موحد أو شامل له، وبتعدد صور وأنواع هذا السر والتي تختلف أهميتها من دولة لأخرى وبتغير الأزمنة من جهة ثانية؛ وعليه ستتم دراسة مفهوم سر الدفاع الوطني من خلال تقسيم هذا المبحث إلى مطلبين: يتطرق المطلب الأول لتعريف سر الدفاع الوطني، ويتطرق المطلب الثاني لأنواع سر الدفاع الوطني.

المطلـــب الأول: تعريـف ســـر الدفـاع الوطنـــي.

السر لغة هو: "ما تكتمه السريرة وجمعه أسرار و سرائر وهو لب كل شيء"[1]. أما في القانون ورغم وجود العديد من النصوص التي تنظم وتحمي أسراراً متعددة ومختلفة الطبيعة إلا أنه لم يرد تعريف لمعظم هذه الأسرار، ومن حسن الصياغة التشريعية للمشرع أنه يبعد نفسه دائماً عن التعريفات خاصة في الأشياء ذات الطبيعة المتغيرة غير الثابتة؛ لأن في تعريفها تقييد لها وإفلات المتغير غير الثابت منها من دائرة التجريم والعقاب؛ لذا لم يُعرف المشرع السر نظراً لطبيعته غير الثابتة والمتغيرة لأن ما يعتبر سراً في زمن أو مكان معين قد لا يعتبر كذلك في غيره[2]؛ ولهذا يتعين دائماً الرجوع إلى العرف وإلى ظروف كل حالة على حدة، يضاف إلى هذه الصعوبة عدم الاتفاق حتى على تسمية موحدة لهذه الأسرار فتظهر في هذا الصدد مصطلحات عديدة أهمها مصطلح الدفاع الوطني، وعليه ومحاولة للإحاطة بتعريف سر الدفاع الوطني سيتم بدايةً التطرق إلى المقصود بالسر وكذا بالدفاع الوطني وذلك من خلال الفرع الأول، ثم التطرق إلى اتجاهات تعريف سر الدفاع الوطني في الفرع الثاني.

الفـــرع الأول: تعريـف مصطلـح الســر ومصطلح الدفـاع الوطنـي.

سيتم تناول تعريف كل من مصطلحي السر والدفاع الوطني في العنصرين الآتيين كل على حدة:

أولاً- تعريـف الســـر:

لم يتفق الفقهاء في معرض تعريفهم للسر على تعريف موحد وشامل له، وفي هذا الإطار يمكن التمييز بين ثلاثة اتجاهات حاول كل منها تعريف مصطلح السر بصفة عامة ومن وجهة نظر مختلفة، ويمكن في هذا الصدد إدخال سر الدفاع ضمن هذه الاتجاهات؛ وعليه سيتم عرض المحاولات الفقهية لتعريف السر في العناصر الثلاثة التالية:

---

[1]- محمد محمد صالح الألفي، مرجع سابق، ص. 162.

[2]- عماد الدين محمد كامل الجمل، الحماية الجنائية لأسرار الدفاع في مواجهة التقدم التكنولوجي الحديث، أطروحة دكتوراه في الحقوق، مقدمة لكلية الحقوق، جامعة القاهرة، دون تاريخ مناقشة، ص. 77.

أ- الإتجـــاه الأول أو النظريـــة الشخصيـــة:

وهو الإتجاه الذي يذهب إلى تعريف السر انطلاقاً من العلاقة الموجودة بين السر وبين الشخص المؤتمن عليه؛ بحيث تقتضي السرية ألا يعلم بالمركز أو الخبر إلا الأشخاص الذين تحتم ظروف المركز أو الخبر وقوفهم على هذه السرية ، ومن بين أهم التعاريف التي تندرج ضمن هذا الإتجاه نرصد الآتية:

1- السر هو صفة تخلع على موقف أو مركز أو خبر أو عمل؛ وتؤدي إلى إيجاد رابطة تتصل بهذا الموقف أو المركز أو الخبر أو العمل بالنسبة لمن له حق العلم به ولمن يلتزم بكتمانه وعدم إفشائه للغير.

2- السر هو العلاقة التي تربط بين شخص معين ومعرفة شيء أو واقعة ما، وأن هذه العلاقة تفرض على هذا الشخص التزامين أحدهما سلبي بعدم إفشاء السر، والآخر إيجابي بمنع الغير من معرفة هذا السر.

3- السر هو واقعة أو صفة ينحصر نطاق العلم بها في عدد محدد من الأشخاص إذا كانت ثمة مصلحة يعترف بها القانون لشخص أو لأكثر في أن يظل العلم بها محصورا في ذلك النطاق.

4- السر هو أمر متصل بشخص أو بشيء من خاصيته أن يظل مجهولا لكل شخص غير مكلف قانونا بحفظه أو باستخدامه؛ بحيث يكون العلم به غير متجاوز عددا محدوداً من الأفراد وهم الذين كلفوا بحفظه أو باستخدامه[1].

5- أما بالتخصيص فيقصد بالسر في إطار أمن الدولة إسباغ الدولة على واقعة أو شيء ما صفة السرية؛ بحيث يتعين بقاؤه محجوباً عن غير من كلف بحفظه واستعماله ما لم تتقرر إباحة إذاعته على الناس كافة دون تمييز، وتتحقق إرادة الدولة في إضفاء السرية إما صراحة بالتنبيه إلى عدم إذاعته وإما بالنظر إلى طبيعة الواقعة أو الشيء موضوع السر في ظروف معينة؛ فليس بشرط إذن توافر السرية أن ينبه على حافظ السر بعدم إذاعته متى كانت طبيعته تنطق بالسرية[2].

---

[1]- عماد الدين محمد كامل الجمل، مرجع سابق، ص. ص. 78-79.

[2]- مصطفى مجدي هرجة، التعليق على قانون العقوبات، المجلد الثاني، دار محمود للنشر والتوزيع، مصر، دون تاريخ نشر، ص. ص. 38-39.

6- كما يقصد به في ذات الإطار مبدأ العلاقة المادية أو الشخصية الذي يشير إلى الحد الموضوع بواسطة إرادة مختصة بمعرفة شيء ما أو واقعة معينة يجب أن تكون سرية بالنسبة لغير الذين لهم صفة شرعية في الإلمام بها أو الاطلاع عليها، والإرادة التي تفرض السرية بالنسبة لتلك الواقعة هي إرادة الدولة سواء كان ذلك صراحة أم ضمنا[1].

يلاحظ بأن هذه التعاريف تشترك جميعها في ضرورة وجود علاقة بين السر وبين الشخص الحائز له؛ بحيث يقع عليه التزام عدم كشفه وإذاعته للآخرين، كما يقع عليه التزام القيام بما يجب بغية منع الآخرين من التوصل إليه، والدولة في إطار التخصيص الذي تتطلبه هذه الدراسة هي الجهة التي تحدد هؤلاء الأشخاص، لكن قد يصل إلى علم شخص من الأشخاص معلومات غير مباحة للإذاعة وبأية طريقة أو وسيلة كانت رغم أنهم ليسوا مؤتمنين على هذه الأسرار وليست لهم أية علاقة بها ورغم ذلك يمنع عليهم إفشاء هذه الأسرار أو تناقلها؛ وعليه فتعريف السر من هذه الوجهة منتقد.

ب- الإتجـاه الثانـي أو نظريـة الضـــرر:

وهو إتجاه يعرف السر انطلاقاً من الضرر الذي يسببه إفشاءه ومعرفته من قبل الآخرين، بحيث من أهم التعاريف التي قيلت بهذا الصدد ما يلي:

1- السر هو صفة تلحق بالشيء أو بالواقعة التي بذيوعها ينال صاحب الحق ضرر يلحق بالحق أو بالمصلحة التي يراد المحافظة عليها وحمايتها[2].

2- أما بالتخصيص؛ فيقصد بالسر في إطار أمن الدولة الصفة التي تلحق بالشيء أو بالواقعة التي بإعلانها يلحق الضرر بالمصلحة القومية المراد حمايتها، وهناك درجات لهذه السرية فهناك السري والسري جداً والسري للغاية بحسب موضوعه وما يتعلق به من معلومات، والدولة هي التي تسبغ هذا الوصف على ما تراه من معلومات إما صراحة بإعلان ذلك وإما ضمنا بحسب موضوع السر[3].

---

[1]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 202.

[2]- مجدي محب حافظ، الحماية الجنائية لأسرار الدولة، مرجع سابق، ص. 158.

[3]- محمد محمد صالح الألفي، مرجع سابق، ص. 162.

بالرغم من أن هذا الإتجاه قد تجاوز الانتقاد الموجه لسابقه من حيث اعتماده على الضرر كمعيار لتعريف السر دون التقيد بضرورة وجود علاقة بين السر وحائزه، إلا أن السر يستوجب الكتمان بذاته بغض النظر عن كون الإفشاء قد يسبب ضررا أم لا.

ج- الإتجـاه الثالـث أو نظريـة المصلحـة الاجتماعيـة:

وهو اتجاه يعرف السر بالنظر إلى مصلحة الشخص في إبقاءه كذلك؛ ومضمون هذا الإتجاه يتمثل في أن الواقعة تعتبر سرية طالما كانت هناك مصلحة لشخص ما في عدم البوح بها، وهذا الإتجاه شأنه شأن الإتجاهات السابقة التي تطبق على الأسرار بصفة عامة دون تخصيص للأسرار المتعلقة بالدولة يجد أساسه الوحيد في المصلحة الاجتماعية التي قصد المشرع المحافظة عليها لأن الصالح العام صالح المجتمع بأكمله يتطلب تلك الحماية من أجل ضمان الممارسة المنتظمة والسليمة لبعض المهن الضرورية للحياة الاجتماعية؛ ومن هنا فإن القانون يهدف إلى حماية الصالح العام الذي يتطلب الحفاظ عليه التزام مطلق على صاحب المهنة بعدم الإفشاء من أجل صيانة الثقة الضرورية التي لا غنى عنها لممارسة بعض المهن التي تشكل بدورها جزءاً من النظام العام؛ فيعد في حكم السر الواجب كتمانه طبقاً لهذا الإتجاه كل أمر يكون سراً ولو لم يشترط كتمانه صراحة، كما يعد سراً كل أمر وصل إلى علم الأمين عن طريق الحدس أو الخبرة الفنية دون أن يُفضى إليه به[1].

وبتخصيص هذا المفهوم واتخاذ أمن الدولة أنموذجاً للتطبيق؛ نجد بأن السمة الرئيسية لأسرارها تتمثل في أن الالتزام بالمحافظة على هذه الأسرار هو التزام مطلق ويعلو على جميع الالتزامات الأخرى حتى لو كانت مقررة في القانون، كما أن هذا الالتزام ليس محصوراً فقط في الأشخاص الذين يعلمون بسر الدفاع الوطني بموجب وظائفهم أو أعمالهم، بل هو التزام عام ملقى على عاتق جميع الأشخاص بدون استثناء وسواء كان علمهم بهذا السر قد تم بسبب العمل أو بحكم المصادفة، وفي هذا الإطار يُعرف السر بأنه: المعلومات التي يعتبرها القانون ماسة بالمصالح العليا للدولة أو تلك التي تعد موضوعاً لهذه المصالح[2].

[1]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 203-204.

[2]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 205.

من عرض الإتجاهات السابقة نخلص إلى أن تعريف السر بصفة عامة وفي ميدان الدفاع الوطني كمثال غير مرتبط بالعلاقة الشخصية التي يمكن أن تربط شخصاً معيناً بسر معين، بمعنى ليس من الضروري أن يتم تسليم السر لشخص ما وفرض التزام المحافظة عليه لاعتباره كذلك؛ فيمكن أن يصل السر إلى الشخص بأية طريقة كانت ودون أن يكون من المؤتمنين عليه، كما لا يشترط أن يؤدي إفشاء السر إلى الإضرار بصاحبه؛ فكما تم توضيحه سالفاً السر يأخذ أهميته من تمتعه بخاصية الكتمان وعدم الذيوع بغض النظر عن تولد ضرر من ذلك؛ وعليه فالاتجاه الأخير هو الأكثر سداداً لأنه لا يتطلب وجود صلة شخصية ولا ضرراً للقول بتحققه، فقط ضرورة ارتباطه بمصلحة عامة وفي إطار هذه الدراسة هي مصلحة الأمن القومي.

بالرجوع إلى قانون العقوبات الجزائري لمعرفة الإتجاه الذي أخذ به المشرع؛ نجد أنه قد تطلب ضرورة حدوث ضرر يلحق الدفاع الوطني لكي يمكن القول بتحقق جريمة التجسس والمساس بالأسرار، لكنه في المقابل لم يشترط وجوبه في كل صور هذه الجريمة بحيث قصره على بعض الصور فقط ومنها صورة إتلاف أو إفساد سفينة أو سفن أو مركبات للملاحة الجوية أو عتاد أو مؤن أو مبان أو إنشاءات من أي نوع كانت أو إدخال عيوب عليها أو التسبب في وقوع حادث، ولكن يشترط هنا أن يكون ذلك بقصد الإضرار بالدفاع الوطني[1]، وكذلك ما جاء بخصوص جريمة المساهمة في مشروع لإضعاف الروح المعنوية للجيش أو الأمة لكن مع اشتراط أن يكون الغرض من ذلك الإضرار بالدفاع الوطني[2]. أما فيما يتعلق بالإتجاهات والنظريات الأخرى (النظرية الشخصية ونظرية المصلحة الاجتماعية) وباستقراء المواد المتعلقة بالتجسس وفيما يخص النظرية الشخصية نجد أن المشرع لم ينص فيها على ضرورة وجود علاقة شخصية أي عدم ضرورة أن يكون الشخص مؤتمن على السر، لكنه في القسم الثاني المعنون بجرائم التعدي الأخرى على الدفاع الوطني أو الاقتصاد الوطني استخدم لفظ الحارس والأمين تحديداً منه للأشخاص الذين تقوم بشأنهم جريمة إتلاف أو إبلاغ الأسرار دون قصد الخيانة أو التجسس[3]. أما فيما يخص نظرية المصلحة الاجتماعية فيستنتج من طبيعة جرائم التجسس أنها تمس حتماً بمصلحة الدولة لكن المشرع هنا آثر استخدام مصطلح الدفاع الوطني للدلالة على أمن الدولة وهو المصطلح الذي يتكرر

[1]– البند الرابع من الفقرة الأولى من المادة 61 من قانون العقوبات.

[2]– البند الرابع من المادة62 من نفس القانون.

[3]– المادة 66 من نفس القانون.

كثيراً ليس فقط في القسم الأول المخصص لجرائم الخيانة والتجسس وكذا في القسم الثاني المخصص لجرائم التعدي الأخرى على الدفاع الوطني أو الاقتصاد الوطني، هذا فيما يخص مواد قانون العقوبات التي تحكم التجسس في صورته التقليدية، وباستقراء المواد التي تحكم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات نجد النص على العقوبات المقررة لهذه الجرائم في حالة ما إذا استهدفت الجريمة الدفاع الوطني دون اشتراط لضرورة أن يؤدي الاعتداء إلى إلحاق ضرر به[1]؛ وعليه نستنتج أن المشرع الجزائري لم يأخذ بنظرية على حساب الأخرى ولكنه حاول توظيف كل نظرية في موقع معين وهذا خدمة لأغراض معينة ارتآها المشرع.

ثانيـاً- تعريـف الدفـــاع الوطنـــي:

تختلف القوانين العقابية في استخدام المصطلحات وذلك للدلالة على الأسرار المرتبطة بأمن الدولة؛ بحيث نجد تعابير عديدة منها: أسرار الدولة والأسرار العسكرية، الأسرار المتصلة بالدفاع عن حدود أمن الدولة، الأسرار العسكرية والاقتصادية، الأسرار المتصلة بالقدرات الحربية أو بالدفاع العسكري، الأسرار المتصلة بمصالح أمن الدولة، الأسرار الرسمية، معلومات الدفاع، الأسرار المتصلة بسلامة الإقليم، أسرار شؤون البلاد الحربية[2]، بينما هناك طائفة من الدول استخدمت في صلب قوانينها العقابية مصطلح أسرار الدفاع الوطني وهو ذات الاتجاه الذي أخذ به المشرع الجزائري؛ بحيث فضل استخدام لفظ الدفاع الوطني كلما أراد الإشارة إلى أمن الدولة فيما يخص الأفعال المكونة للركن المادي لجريمة التجسس كما ربط تعداده للأسرار محل التجسس بذات اللفظ، ومن أمثلته نص قانون العقوبات على فعل إتلاف أو إفساد سفينة أو سفن أو مركبات للملاحة الجوية أو عتاد أو مؤن أو مبان أو إنشاءات من أي نوع كانت وذلك بقصد **الإضرار بالدفاع الوطني** أو إدخال عيوب عليها أو التسبب في وقوع حادث وذلك تحقيقا لنفس القصد[3]، وكذلك نصه على فعل المساهمة في مشروع لإضعاف الروح المعنوية للجيش أو للأمة يكون الغرض منه الإضرار **بالدفاع الوطني**[4]، وكذالك نصه على فعل تسليم معلومات أو أشياء أو مستندات أو تصميمات يجب أن تحفظ تحت ستار من السرية لمصلحة **الدفاع الوطني** أو الاقتصاد

---

[1]- المادة 394 مكرر 3 من قانون العقوبات.

[2]- عماد الدين محمد كامل الجمل، مرجع سابق، ص. 81.

[3]- البند الرابع من الفقرة الأولى من المادة 61 من قانون العقوبات.

[4]- البند الرابع من المادة 62 من نفس القانون.

الوطني إلى دولة أجنبية أو أحد عملائها[1]، كما استخدمها المشرع الجزائري بصدد تجريم السلوكات الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك في المادة 394 مكرر3 السابق تناولها؛ وعليه فهو التعبير الذي سيستخدم في هذه الدراسة للدلالة على أسرار الدولة، لذا وجب التطرق للمقصود به إستجلاءاً لأي غموض ودفعاً لأي تساؤل بخصوصه.

إن فكرة الدفاع الوطني فكرة حديثة نسبياً؛ إذ أنها ترتبط قبل كل شيء بمفهوم الدولة المستقلة ذات الشخصية القانونية المنفصلة عن شخصية حكامها، وقد أصبحت هذه الفكرة أساساً ومرتكزاً لتحقيق أمن الدولة الخارجي ووسيلة للحد من النشاطات المعادية للدول الأجنبية وذلك عن طريق تجنيد مختلف قوى الأمة لمواجهة تلك الأنشطة، فالدفاع الوطني بذلك يعني مجموع القوى التي تملكها الأمة والتي يمكن تسخيرها في الوقت المناسب لتحقيق الأمن القومي وحمايته ضد العدوان الخارجي أو مجرد التهديد به، فالدفاع الوطني بهذا الوصف يمثل جهاز المناعة الأول في جسد الدولة؛ فهو يرتبط بالوسائل التي تدخرها الدولة بقصد حماية كيانها السياسي في مواجهة الأخطار أو التهديدات الخارجية وسواء كانت هذه الوسائل مادية أو معنوية وسواء تعلقت بالموارد الاقتصادية أو الصناعية أو العسكرية أو العلمية أو السياسية؛ وعليه فالدفاع الوطني بذلك يعتبر وسيلة الدولة في صيانة وجودها بين الأمم الأخرى[2].

يتسم الدفاع الوطني بخصائص تبرز أهميته أهمها اتصافه بالشمول؛ بحيث أنه يضم كل قطاعات الدولة إذ ليس ثمة نشاط يمكن أن يكون خارج نطاق مخطط الدفاع الوطني أو أن يكون بعيداً عن الاهتمامات الأساسية للدفاع عن البلاد؛ فالدفاع الوطني في الدولة المعاصرة يتكون من مختلف قوى الأمة وتأتي في مقدمتها القوات المسلحة بمختلف فروعها وأجهزتها ومرافقها، ولا ينحصر الدفاع الوطني فقط في الجانب العسكري بل يشمل كذلك الجوانب الاقتصادية والصناعية ويمتد ليشمل النشاط التجاري والنقدي ويتجاوز ذلك إلى الجانب النفسي عندما يتعلق الأمر بالحالة المعنوية للشعب أو الجيش في مواجهة المخاطر الأجنبية[3]. كما أنه يتصف بالدوام؛ فهو لا يتوقف على وجود حالة الحرب أو التهديد بالعدوان؛ لأن المفهوم الحديث للدفاع قد أسقط نهائياً التمييز التقليدي بين حالة الحرب وحالة السلم خاصة

---

[1]– البند الأول من المادة 63 من قانون العقوبات.

[2]– محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 118–119.

[3]– نفس المرجع، ص. 123.

في ظل المتغيرات الدولية المتلاحقة التي يتولد عنها قيام حالة دائمة من الشعور بالخطر والإحساس بالتهديد. كما يتسم الدفاع الوطني بكونه يمثل مصلحة قومية عليا وهذا بالنظر إلى أهدافه وغاياته[1].

هناك علاقة وطيدة بين كل من مفهوم الدفاع الوطني وأمن الدولة من جهة، وبين مفهوم الدفاع الوطني والتجسس من جهة ثانية؛ فمن جهة يمكن القول أن علاقة الدفاع الوطني بأمن الدولة هي علاقة عضوية؛ فالدفاع الوطني يتحدد بالوسائل والإجراءات التي تقوم بها الدولة في سبيل حماية أمنها القومي فلا يتصور وجود أي منهما بدون الآخر، على أن مفهوم أمن الدولة في الواقع أكثر اتساعاً وشمولاً من فكرة الدفاع الوطني؛ وذلك لأن المفهوم الأول يشتمل على مظهرين أمن الدولة الداخلي وأمن الدولة الخارجي، أما الدفاع الوطني فهو ليس إلا مجرد وسيلة لتحقيق حماية ذلك الأمن في جانبه الخارجي والعلاقة بينهما أي بين أمن الدولة والدفاع الوطني هي كالعلاقة بين الغاية والوسيلة، ومن هنا كان الدفاع الوطني بمثابة كائن مادي ملموس لأنه يتعلق بالموجودات التي تدخرها الدولة أو تلك التي يمكن تجنيدها أو تسخيرها لتحقيق الحماية الضرورية لأمن الدولة أو لكيانها على الصعيد الدولي؛ فهو بذلك وسيلة تهدف إلى تحقيق غاية معينة تتمثل في أمن الدولة الذي يعبر في واقع الأمر عن مجرد الإحساس الذاتي أو الشعور المعنوي للدولة في أنها في مأمن من الأخطار أو التهديدات الخارجية[2]؛ ومن جهة أخرى فالتجسس الدولي في العصر الحديث يرتبط بفكرة الدفاع الوطني على نحو وثيق؛ حتى أنه يمكن لنا القول أن التجسس هو في حقيقته كل نشاط يستهدف الإضرار بالدفاع الوطني لدولة معينة وهذا يعني أنه لا وجود للتجسس الدولي ما لم يكن هناك سلوك يستهدف العدوان على المقومات والركائز التي يعتمد عليها الدفاع الوطني في دولة معينة وفي فترة زمنية معينة أيضا، فالمصلحة المحمية في جرائم التجسس تتمثل في حقيقة الأمر في حق الدولة في الدفاع الوطني عن وجودها وكيانها[3]، وكل هذا الكلام يخص التجسس بصفة عامة بغض النظر عن صورته.

---

[1]– محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. ص. 119-120.

[2]– محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص.126-127.

[3]– محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. ص. 117-118.

الفـــرع الثانـــي: إتجاهـات تعريـف ســر الدفــاع الوطنـــي.

ككل المصطلحات المرتبطة بأمن الدولة من حيث مرونتها واتساعها بحيث تستعصي على الجمع والتحديد في تعريف موحد وواضح ويمتاز بالثبات؛ فقد أخذ مصطلح سر الدفاع الوطني ذات السمات من المفهوم العام الذي يتبعه، وقد سبقت الإشارة إلى عدم الاتفاق حول تعريف السر وكذا اتصاف فكرة الدفاع الوطني بالشمول والتجدد؛ إذ هي فكرة متغيرة تخضع لظروف العصر وما يمليه من ضرورة مسايرته، وبالنظر إلى أن تحديد سر الدفاع الوطني يؤدي إلى تحديد ما إذا كنا بصدد جريمة تجسس أم لا، بمعنى اكتمال النموذج القانوني الذي على أساسه سيعاقب شخص ما؛ فالأمر هنا يتعلق بوضع قوانين أي باختصاص أصيل للسلطة التشريعية، ولكن قد تحتم ظروف معينة مرتبطة أساساً بطبيعة سر الدفاع الوطني إشراك كل من السلطتين التنفيذية والقضائية في هذه المهمة؛ وعليه ستتم دراسة تعريف سر الدفاع الوطني من خلال عنصرين: يتناول العنصر الأول التعريف التشريعي لسر الدفاع الوطني، بينما يتناول العنصر الثاني دور السلطة الإدارية والسلطة القضائية في تعريف وتحديد سر الدفاع الوطني.

أولاً- التعــريف التشريعــي لســـر الدفــاع الوطنـــي:

تنحصر مهمة المشرع في معظم الحالات في وضع الإطار العام الذي يحكم ظاهرة من الظواهر مع تحديد عناصرها والشروط المتطلبة فيها لتخضع للنموذج القانوني الذي يقوم بوضعه، إلا أنه عندما يتعلق الأمر بأسرار الدفاع الوطني التي تتصل بوجود الدولة وبقائها بين الأمم خاصة مع تعدد وتنوع تلك الأسرار التي لم تعد قاصرة على المجال العسكري، بل شملت جميع المراكز الحيوية في الدولة وجميع خططها وبرامجها في مختلف النواحي الاقتصادية والصناعية والدبلوماسية والاجتماعية والسياسية، حتى أصبحت تلك الأسرار هدفاً إستراتيجياً للحرب الشاملة في عصر التقدم العلمي والتكنولوجي؛ الأمر الذي دفع المشرع إلى مراجعة سياسته التشريعية[1] من خلال محاولة وضع تعريف لأسرار الدفاع الوطني، فَمِثل هذا التعريف على جانب كبير من الأهمية؛ لأن القول بوجود سر الدفاع يعني تماماً القول بوجود جريمة فالأمر مرتبط بمبدأ شرعية الجرائم والعقوبات، وهذا ما يدفع للقول بأنه ليس هناك سر للدفاع الوطني بدون نص تأسيساً على قاعدة لا جريمة ولا عقوبة بدون نص؛ لأن القانون وهو يعاقب على جرائم

[1]- عماد الدين محمد كامل الجمل، مرجع سابق، ص. 82.

التجسس بأشد العقوبات جسامةً يجب عليه أن يحدد سر الدفاع على نحو واضح[1]، والتشريعات العقابية في محاولة منها للتصدي لتعريف سر الدفاع الوطني لم تجر على الوتيرة ذاتها وإنما نهج كل منها في ذلك نهجا مستقلاً متبعاً أسلوباً مختلفاً، ولكن يمكن رد هذه الأساليب إلى ثلاثة كالآتي:

أ- الأسلـوب القائــم على الصيغــة العامــة والمجــردة:

بحيث تتجه بعض التشريعات صوب عدم وضع تعريف محدد لأسرار الدفاع الوطني؛ وذلك باعتبارها أفكاراً واسعة وتتنوع إلى صور كثيرة مما لا يجوز معه تقييدها بتعريف محدد؛ لذلك فإن المشرع يكتفي بنص تشريعي عام يشمل ما يجب كتمانه حرصاً على سلامة الدولة دون الدخول في تفاصيل تعداد الأسرار المشمولة بالحماية الجنائية. ومن التشريعات التي أخذت بهذا الأسلوب التشريع الهولندي الذي عرف أسرار الدفاع الوطني بأنها المسائل التي تمس أمن الدولة، وكذلك التشريع السويسري الذي يعرف أسرار الدفاع الوطني بأنها الوقائع والترتيبات والوسائل التي تشملها السرية من أجل مصلحة الدفاع الوطني[2].

لكن هذه التعريفات من الاتساع والمرونة والغموض بمكان؛ بحيث لغرض تعريف سر الدفاع الوطني استعملت مصطلحات أكثر شمولاً واتساعاً منه، مثل المسائل التي تمس أمن الدولة أو الوقائع والترتيبات والوسائل التي تشملها السرية لمصلحة الدفاع الوطني؛ بحيث يطرح التساؤل عن المقصود بكل هذه المصطلحات، ومما لاشك فيه أن المشرع الجنائي في هذه الدول يسعى من خلال استعمال صيغة عامة وجامعة لسر الدفاع أن يصل إلى تعريف شامل لهذا السر بحيث يتضمن مختلف الأشكال التي يمكن أن يتجسد فيها مثل هذا السر إلا أنه قد أوقع قوانين هذه الدول في حالة من الغموض والتضارب؛ إذ من شأن تلك الصيغة أن تؤدي إلى الحط من مبدأ شرعية الجرائم والعقوبات؛ بحيث أنها تخول المحاكم سلطات واسعة في تفسير النصوص المتعلقة بسر الدفاع الوطني وهي عادة نصوص مرنة وغير محددة؛ مما قد يصل إلى حد تجريم أفعال أو وقائع لم يعينها النص الجنائي بصورة مؤكدة وقت صدوره[3].

---

[1]- محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 414.

[2]- مجدي محب حافظ، موسوعة جرائم الخيانة والتجسس، مرجع سابق، ص. ص. 215-216.

[3]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 210.

ب- الأسلـوب القائـــم علـى التعريـف التعـــدادي:

تذهب طائفة من التشريعات إلى محاولة وضع تعريف شامل لأسرار الدولة وذلك عن طريق سرد كل ما يمكن أن يعتبر من أسرار الدولة، وفي هذا الإطار يعتبر قانون العقوبات المصري المثال الذي يعبر عن هذا الأسلوب؛ بحيث قام المشرع في المادة 85 (وهي المادة المأخوذة حرفيا من قانون العقوبات الفرنسي القديم) بتعداد ما يمكن أن يعتبر سراً من أسرار الدفاع الوطني، وهي ما يمكن الاستئناس به لبيان فكرة السر؛ وعليه يعتبر سراً الأمور التالية:

1- المعلومات الحربية والسياسية والدبلوماسية والصناعية التي بحكم طبيعتها لا يعلمها إلا الأشخاص الذين لهم صفة في ذلك ويجب مراعاة لمصلحة الدفاع عن البلاد أن تبقى سراً على من عدا هؤلاء من الأشخاص.

والواقع أن هذه المعلومات بطبيعتها سرية لأنها تتعلق بشؤون تتكون منها قوة الدولة في مواجهتها لأعدائها.

2- الأشياء والمكاتبات والمحررات والوثائق والرسوم والخرائط والتصميمات والصور وغيرها من الأشياء التي يجب لمصلحة الدفاع عن البلاد ألا يعلم بها أحد إلا من يناط بهم حفظها أو استعمالها والتي يجب أن تبقى سراً على من عداهم خشية أن تؤدي إلى إفشاء معلومات حربية أو سياسية أو دبلوماسية أو صناعية.

3- الأخبار والمعلومات المتعلقة بالقوات المسلحة وتشكيلاتها وتحركاتها وعتادها وتموينها وأفرادها ، وبصفة عامة كل ما له مساس بالشؤون العسكرية والإستراتيجية ولم يكن قد صدر إذن كتابي من القيادة العامة للقوات المسلحة بنشره أو إذاعته.

والتشكيلات معناها الأوضاع المختلفة التي تشكل فيها القوات المسلحة في هجومها أو دفاعها عندما تواجه العدو، أما التحركات ويطلق عليها فنيا "التكتيك" فهي فن تقدم الجيش وتحركه للأمام أو للخلف في الميدان لمباشرة القتال الفعلي عندما يواجه العدو وعلى العكس منها مصطلح " الإستراتيجية"؛ إذ أن الشؤون الإستراتيجية هي الخطط المستقبلية واسعة المدى وبعيدة الأثر بالنسبة لسير القتال في سائر الميادين مثل إمدادات الجيش بقوات جديدة.

4- الأخبار والمعلومات المتعلقة بالتدابير والإجراءات التي تتخذ لكشف الجرائم المنصوص عليها في هذا الباب آو تحقيقها آو محاكمة مرتكبيها، ومع ذلك فيجوز للمحكمة التي تتولى المحاكمة أن تأذن بإذاعة ما تراه من مجرياتها.

ويتناول هذا النص بالحماية الإجراءات التي تباشرها سلطة التحقيق بصدد التحقيق أو التصرف فيه والإجراءات التي تباشرها المحكمة وما يتم أمامها من إجراءات، ولقد ورد بالمذكرة الإيضاحية أن الغرض من هذه الفقرة هو ضمان حصر نطاق جرائم الاعتداء على أمن الدولة وعدم إفلات الجناة من العقاب، ولقد أراد المشرع بذلك أن يحول دون نشر ما يدور في السر أثناء ملاحقة الجناة الذين ارتكبوا إحدى الجرائم الماسة بأمن الدولة[1].

إن هذا الأسلوب القائم على التعداد في محاولة الوصول إلى تعريف سر الدفاع الوطني قد انتهى في الواقع إلى صيغ واسعة وأكثر غموضاً؛ فمن يستطيع تحديد طبيعة معلومات معينة على أنها تدخل في نطاق أسرار الدفاع؟، ليس من شك في أن هناك وقائع عديدة لا يثور حولها الشك لتعلقها مباشرة بالدفاع الوطني للدولة عندما تمس المقومات العسكرية أو الاقتصادية أو الصناعية أو العلمية للدولة، ولكن هناك وقائع أخرى عديدة يكتنفها الغموض ولا يستطيع المرء الحكم على طبيعتها السرية بصورة قاطعة اعتماداً على التعريف الذي يرتكز على التعداد، ومثاله الشك أو التردد في القول بأن عدد العمال أو المستخدمين في منشأة لصناعة الملابس العسكرية يشكل سراً من أسرار الدفاع[2].

ج- الأسلـوب التكميلـي فـي تعريـف سـر الدفـاع الوطنـي:

نظراً لما يثيره الأسلوب السابق من غموض وتضارب لجأت بعض التشريعات إلى الاستعانة بوسيلة تكميلية للمساعدة في تحديد سر الدفاع الوطني بصورة أكثر وضوحا؛ بحيث تميل هذه التشريعات إلى تجنب تعريف أسرار الدولة تعريفاً دقيقاً وتتجه نحو تقسيم الأسرار إلى أسرار حقيقية[3]، وأسرار اعتبارية؛ فإذا كانت الواقعة بطبيعتها لا تشكل سراً من أسرار الدفاع فعلى محكمة الموضوع أن تبحث عن مدى اعتبارها كذلك عن طريق الاستعانة برأي السلطات المختصة ذات العلاقة وأن تطبق معياراً

[1]- عبد الفتاح مصطفى الصيفي، مرجع سابق، ص. ص. 104-106.

[2]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 211-212.

[3]- مجدي محب حافظ، الحماية الجنائية لأسرار الدولة، مرجع سابق، ص. 164.

موضوعياً مؤداه أن الواقعة تدخل في حكم سر الدفاع الوطني إذا كان من الممكن أن يترتب على ذيوعها أو معرفة إحدى الدول الأجنبية بها وقوع ضرر بالدفاع الوطني[1].

رغم أن هذا الاتجاه الذي أحال على سلطات الدولة التنفيذية مهمة إصدار مراسيم لتبين فيها الأسرار الاعتبارية وهو بهذا الشكل يكون قابلا للتعديل والتكملة ويجاري التطورات الحاصلة دون الحاجة إلى تعديل قانون العقوبات في كل مرة، بالإضافة إلى أنه يمنح القضاة حرية تحديد ما قد يدخل ضمن أسرار الدفاع وتفادي العجز في متابعة المجرمين في ظل عدم وجود نص صريح، إلا أن هذا الإتجاه يمكن كل من السلطتين القضائية والتنفيذية من التدخل في عمل السلطة التشريعية؛ بمعنى التعدي على الاختصاص الأصيل لهتين السلطتين.

د- موقـف المشـرع الجزائـري من تعريـف سـر الدفـاع الوطنـي:

بالرجوع إلى مواد قانون العقوبات الجزائري التي تحكم جريمة التجسس التي تضمنها القسم الأول المعنون بجرائم الخيانة والتجسس من الفصل الأول المعنون بالجنايات والجنح ضد أمن الدولة نجد أن المشرع الجزائري قد تفادى تضمين تلك المواد تعريفاً لأسرار الدفاع الوطني واكتفى بتعابير عامة تشمل ما ينبغي كتمانه لمصلحة الدفاع الوطني دون أن يتدخل في تفاصيل التعداد؛ بحيث نص على أنه يعاقب بالإعدام من يقوم "بتسليم معلومات أو أشياء أو مستندات أو تصميمات يجب أن تحفظ تحت ستار السرية لمصلحة الدفاع الوطني أو الاقتصاد الوطني ..."[2]، فجعل السر إما أن يكون معلومات أو أشياء أو مستندات أو تصميمات مع ما لهذه التعابير من سعة ومرونة وإبهام، وقد اجتهد الفقه في محاولة لتحديد معناها كالآتي:

1- المعلومـــات:

يرى الفقه أنها الحقائق التي يتوصل إليها أهل المعرفة من العلماء وذوي الاختصاص، وتشمل أيضا الأخبار التي تروى صحيحة كانت أم خاطئة والأنباء التي تصل لذوي الشأن بخصوص الدفاع عن

[1]- محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص.417.

[2]- البند الأول من المادة 63 من قانون العقوبات.

البلاد ومن أمثلتها المعلومات المتعلقة باختراع جديد[1]، أو المعلومات التي يتلقاها المختصون في الميدان عن عجز في الذخائر والمؤن أو وقوع فريق من القوات المحاربة في الأسر أو البيانات الخاصة بالخطط الحربية أو بشؤون التسليح والتدريب والتنظيم والتعبئة وعدد القوات الفعلية والاحتياطية ومراكز الدفاع أو بالخدمات المتصلة بميدان القتال أو بالأوامر الصادرة إلى الضباط أثناء سير القتال أو الأنباء المتضمنة تراجع الجيش، وكذلك المعلومات الدبلوماسية المتعلقة بسير المفاوضات السياسية أو بالمذكرات التي تنطوي على السياسية الخارجية حيال بعض الدول الأجنبية[2]، ومن المسلم به أن هذه المعلومات إنما تستقي عناصرها من الأشياء والمستندات والتصميمات التي سيتم شرحها في الآتي:

2- الأشيـــاء:

يقصد بها الأسرار ذات الكيان المادي المحسوس، وتشمل على الأخص الأسلحة والذخائر والآلات والمعدات والعدد الميكانيكية والأدوات وقطعها وإن كانت منفصلة والمواد الكيميائية أو عناصرها التي تتكون منها[3].

3- المستنـــدات:

وتفضل بعض التشريعات تسميتها بالوثائق، وهي جميع أنواع المحررات المكتوبة كالمذكرات والتقارير والأبحاث المختصة ...

4- التصميمـات :

وهي الرسوم والخرائط التي تبين مشاريع اقتصادية أو عسكرية[4]، ومن التشريعات من يدخل هذه التصميمات ضمن طائفة المستندات كما هو حال قانون العقوبات السوري.

لكن بالتوسع في قراءة مواد قانون العقوبات التي تحكم جرائم أمن الدولة في قسمها الثاني المعنون

---

[1]- عبد الله سليمان، دروس في شرح قانون العقوبات الجزائري (القسم الخاص)، ط2، ديوان المطبوعات الجامعية، الجزائر، 1989، ص. 38.

[2]- محمد الفاضل، مرجع سابق، ص. 342.

[3]- جاك يوسف الحكيم ورياض الخاني، مرجع سابق، ص. 229.

[4]- عبد الله سليمان، مرجع سابق، ص. 38.

بجرائم التعدي الأخرى على الدفاع الوطني أو الاقتصاد الوطني وهي في معظمها سلوكات تهدف إلى إطلاع الغير على سر من أسرار الدفاع الوطني ولكن دون قصد التجسس؛ نجد أنها استخدمت ذات المصطلحات السابقة للدلالة على هذا السر أي استخدمت ألفاظ المعلومات والأشياء والمستندات والتصميمات، إلا أنها فصلت أكثر فيما يمكن أن يعتبر سراً من أسرار الدفاع الوطني؛ بحيث شملت بعض الأسرار التي تطرق إليها مشرعون آخرون كالمشرع المصري مثلا في المادة 85 السابق عرضها، وهذا ما يتضح من خلال نصها على المعاقبة بالسجن المؤقت من عشر سنوات إلى عشرين سنة كل من يسلم بغير إذن سابق من السلطة المختصة إلى شخص يعمل لحساب دولة أو مؤسسة أجنبية إختراعا يهم الدفاع الوطني أو معلومات أو دراسات أو طريقة صنع تتصل بإختراع من هذا النوع أو بتطبيقات صناعية تهم الدفاع الوطني، أو يفشي إليه شيئا من ذلك[1]، وكذلك من خلال نصها على المعاقبة بالحبس من سنة إلى خمس سنوات كل من يقدم معلومات عسكرية لم تجعلها السلطة المختصة علنية وكان من شأن ذيوعها أن يؤدي بجلاء إلى الإضرار بالدفاع الوطني إلى علم شخص لا صفة له في الاطلاع عليها أو إلى علم الجمهور[2]، وكذلك من خلال نصها على المعاقبة بالسجن المؤقت من عشر سنوات إلى عشرين سنة كل من قام بعمل رسومات أو بأخذ صور أو برسم خرائط أو بعمليات طوبوغرافية في منطقة محرمة حددتها السلطة العسكرية أو البحرية وكذا بنفس العقوبة لمن أفشى إلى شخص لا صفة له معلومات متعلقة بالتدابير التي تتخذ لكشف مرتكبي الجنايات والجنح المنصوص عليها في القسمين الأول (المتضمن جرائم الخيانة و التجسس)، والثاني (المتضمن جرائم التعدي الأخرى على الدفاع الوطني والاقتصاد الوطني) وشركائهم وللقبض عليهم وإما بسير إجراءات المتابعة والتحقيق وإما بسير المحاكمة أمام جهات القضاء أو قام بإذاعة شيء من ذلك علناً[3].

وعليه لا يمكن الحكم على توجه المشرع الجزائري بخصوص تعريفه لسر الدفاع الوطني من خلال المواد التي تحكم فقط التجسس وإلا دفعنا هذا للتسليم بأنه قد اعتمد الأسلوب القائم على الصيغة العامة والمجردة؛ لأنه اكتفي في صلبها بالتدليل على أن سر الدفاع الوطني هو المعلومات والأشياء والمستندات والتصميمات المرتبطة بمصلحة الدفاع الوطني، ولكن يجب النظر إلى هذا المفهوم من خلال

[1]– المادة 68 من قانون العقوبات.

[2]– المادة 69 من نفس القانون.

[3]– المادة 70 من نفس القانون.

كافة المواد التي تحكم الجرائم الماسة بأمن الدولة باعتبار أن جوهرها كما سبق شرحه هو الدفاع الوطني؛ وعليه فالمشرع الجزائري وضع الإطار العام لتعريف سر الدفاع الوطني من خلال المواد التي تحكم جريمة التجسس ليفصل فيما بعد فيها بإعطاء أمثلة تندرج ضمن التعريف العام؛ ومنه يمكن القول أن المشرع الجزائري قد اتبع الأسلوب القائم على التعريف التعدادي.

وتجدر الإشارة في هذا الإطار إلى أن المشرع الجزائري قد أخذ جُل هذه الأحكام من قانون العقوبات الفرنسي القديم؛ بحيث نص هذا الأخير في مادته 72 التي تم استحداثها بموجب مرسوم 4 يونيو سنة 1960 على أن سر الدفاع الوطني يتمثل في المعلومات والأشياء والوثائق أو الأساليب التي يجب أن تظل سرية لمصلحة الدفاع الوطني، كما نص ذات القانون على أمثلة وقائع أخرى تدخل ضمن مفهوم سر الدفاع الوطني مثل المعلومات العسكرية غير المنشورة من جانب السلطات المختصة التي يؤدي نشرها أو إفشاؤها إلى وقوع ضرر بالدفاع الوطني وكذلك المعلومات المتعلقة بالتدابير القضائية، بمعنى وجود تطابق بين تعريف سر الدفاع الوطني المتضمن في قانون العقوبات الفرنسي القديم و بين تعريف سر الدفاع الوطني في قانون العقوبات الجزائري الحالي، إلا أن المشرع الفرنسي قد تجاوز هذا التعريف بوضعه لأخر جديد بحيث لم يعد لمفهوم سر الدفاع الوطني ذلك المعنى المعروف في القانون القديم ولكنه أصبح يعني بموجب المادة 413-9 في فقرتها الأولى البيانات والأساليب والأشياء والمعلومات المعالجة آليا والفهارس التي تهم الدفاع الوطني وتكون موضوعا لتدابير الحماية المحددة لقيود نشرها أو إذاعتها[1]، وأهم ما يمكن ملاحظته على هذا التعريف أنه أشار صراحة للمعلومات الإلكترونية أي تلك المعالجة آلياً واعتبرها داخلة في سر الدفاع الوطني، وهي خطوة سديدة ليس لأنها تعترف بوجود معلومات مختلفة من حيث الطبيعة والجوهر عن المعلومات التقليدية؛ لأنه وكما سبقت الإشارة إليه فالمعلومة تأخذ وصفها الإلكتروني من استخدام أنظمة المعالجة الآلية للتعامل معها وليس لأن المعلومات قد تغير جوهرها فالمعلومة العسكرية والاقتصادية والصناعية والسياسية والدبلوماسية تبقى ذاتها ولا يتغير جوهرها فقط بدل أن تستخدم الوسائل البشرية في التعامل معها كالقيام بتصنيفها أو أرشفتها أو نقلها يدوياً يعوض نظام المعالجة كل هذه التصرفات؛ بحيث يمكن بعد إدخال هذه المعلومات إلى نظام المعالجة الآلية للمعطيات أن يتم تخزينها واسترجاعها وتعديلها ونقلها بواسطة هذا النظام؛ ولكن الخطوة سديدة لأن المشرع بهذا قد اعترف بوجود تأثير للثورة المعلوماتية وللعصر الحديث على تطور تقنيات التجسس ومنه

[1]– محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. 230.

يجب على قانون العقوبات والمنظومة التشريعية ككل أن تواكب هذا التطور وتستجيب للحاصل، وحبذا لو يتجاوز المشرع الجزائري الصياغة العامة التي تبناها ويخص المعلومات الإلكترونية بالذكر في صلب المواد التقليدية التي تتناول سر الدفاع الوطني.

ثانيـاً- دور السلطة الإداريـة والسلطة القضائيـة في تعريف وتحديد سر الدفـاع الوطنـي:

سيتم التعرض لدور كل من السلطة الإدارية والسلطة القضائية في تعريف وتحديد ما يمكن أن يندرج في تعريف سر الدفاع الوطني من خلال العنصرين الآتيين:

أ- دور السلطـة الإداريـة في تعريـف وتحديـد سـر الدفـاع الوطنـي:

تجب الإشارة بداية إلى أن أسرار الدفاع الوطني التي تمثل محل جرائم التجسس يجب أن يكون تحديدها وتعريفها منوطاً بالمشرع وحده وهذا ما يفرضه مبدأ شرعية الجرائم والعقوبات، أما تخويل جهة أخرى سلطة تعيين سر الدفاع فإنه يؤدي إلى خلق جرائم لم ينص عليها القانون وهذا بدوره ينطوي على انتهاك خطير ليس فقط لمبدأ المشروعية ولكن أيضا لمبدأ الفصل بين السلطات، ومع ذلك نلاحظ أن هناك العديد من التشريعات تخول السلطات الحكومية صلاحية اعتبار بعض الوقائع أو الوثائق أو الأشياء ضمن سر الدفاع الوطني[1]، وهذا عن طريق إصدار مرسوم لتحديد بعض أنواع أسرار الدولة المحظور نشرها أو إذاعتها؛ وعليه وفي هذا الإطار يمكن تقسيم موقف التشريعات المقارنة من تخويل السلطات الإدارية التدخل لإصدار مراسيم لاستكمال النقص التشريعي في مجال تحديد مفهوم أسرار الدفاع الوطني إلى ثلاثة اتجاهات رئيسية كالآتي:

1- الاعتـراف للسلطة الإداريـة بتحـديد سـر الدفـاع الوطنـي:

تتجه بعض التشريعات إلى الاعتراف للسلطة الإدارية بأن تلعب دوراً كاملاً في استكمال النقص التشريعي في مجال تحديد أسرار الدفاع الوطني، وتتبنى هذا التوجه خاصة التشريعات التي قسمت الأسرار إلى نوعين: أسرار بطبيعتها وأسرار حكمية أي اعتبارية، أما الأسرار بطبيعتها فإنه لا يعلمها إلا الأشخاص المنوط بهم حفظها وصيانتها؛ لأن المصلحة العامة تقتضي أن تبقى سراً على من عداهم، والأسرار الحكمية وهي المعلومات أو الوثائق أو غير ذلك من الأشياء التي ليست في ذاتها سراً ولكنها

[1]- محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 417.

تعتبر في حكم الأسرار لأن إذاعتها تؤدي إلى الوقوف على مضمون سر حقيقي، أو لأنها تعتبر في حكم الأسرار بمقتضى أمر من الحكومة، ومن هذه التشريعات التشريع الإيطالي[1].

2- عـدم الاعتـراف للسلطـة الإداريـة بتحـديد سـر الدفـاع الوطنـي:

هذا الإتجاه يسود في كثير من التشريعات خاصة في ألمانيا ولوكسمبورغ؛ ففي هذه الدول لا تملك السلطات الإدارية أية سلطة أو صلاحية تجعلها تضفي على واقعة ما صفة سر الدفاع بصورة اعتبارية، وهي لا تملك ذلك لأنه المفروض على السلطات الحكومية احترام القواعد الدستورية وقيامها بأي دور في هذا الإطار يشكل مساساً بمبدأ الفصل بين السلطات ويهدم مبدأ الشرعية الجنائية ويعرض الحريات والحقوق الفردية للخطر[2].

3- جـواز تدخـل السلطـة الإداريـة فـي تعييـن سـر الدفـاع:

هذا الاتجاه يسود بعض التشريعات ومنها القانون البلجيكي والقانون السويسري والقانون الهولندي؛ فالمبدأ العام في هذه التشريعات يرتكز على الشرعية الجنائية فيما يتعلق بتحديد سر الدفاع، إلا أن المشرع في هذه الدول يقبل على سبيل الاستثناء الخروج على تلك القاعدة وذلك بصدور تفويض من السلطة التشريعية للحكومة أي للسلطة الإدارية[3]، ففي بلجيكا يسمح استثناء للحكومة بناء على تفويض تشريعي بإصدار مرسوم بشأن تحديد مفهوم أسرار الدولة، أما في هولندا فإنه يجوز للسلطة الإدارية أن تفرض حظراً على بعض الوثائق السرية وإن كان ذلك الحظر مقصوراً على الموظفين الملتزمين بحكم وظائفهم باحترام كتمان الأسرار المطلعين عليها، وفي سويسرا خول المجلس الفيدرالي سلطة تحديد المؤلفات العسكرية التي تنطبق عليها القواعد الخاصة بالحماية الجنائية وكذلك منح سلطة لاتخاذ كافة الإجراءات الضرورية في إطار القانون إلى الجهات العسكرية وكل هيئة مختصة وإلى كل قيادة عسكرية[4]، على أنه تجب الإشارة هنا إلى أن السلطات الإدارية في هذه الدول وإن كانت تملك دوراً في تعيين سر

---

[1]- مجدي محب حافظ، موسوعة جرائم الخيانة والتجسس، مرجع سابق، ص. 250.

[2]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. ص. 213- 214.

[3]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. 214.

[4]- مجدي محب حافظ، الحماية الجنائية لأسرار الدولة، ص. 187.

الدفاع بصورة اعتبارية إلا أن ذلك لا يكون إلا في نطاق محدود وبصفة استثنائية وبشرط وجود تفويض تشريعي بذلك[1].

مهما كان من موقف التشريعات المختلفة إزاء منح السلطة الإدارية حق تعريف سر الدفاع الوطني من خلال التدخل في تحديد ما يعتبر كذلك، فإن ذات التشريعات تتفق في حالة منح السلطة الإدارية حق تقرير أو إدخال أسرار الدول الحليفة التي تتعلق بالدفاع الوطني ضمن سر الدفاع المحمي جنائيا في التشريع الداخلي، والأصل في أسرار الدفاع الخاصة بالدول الحليفة أنها لا تدخل في نطاق حماية القانون الوطني وبناء على ذلك فإن أفعال انتهاك هذه الأسرار لا تشكل جرائم ومن ثم لا يعاقب عليها سواء وقعت داخل أو خارج إقليم الدولة، إلا أن المشرع ولاعتبارات المصلحة المشتركة للدول الأعضاء في معاهدة تحالف يبسط حمايته الجنائية على أسرار هذه الدول؛ وعليه فإن الانتهاكات التي تقع على هذه الأسرار تعتبر كما لو كانت قد وقعت على أسرار الدفاع بالنسبة لجميع الدول المتحالفة، وليس من شك في أن الانضمام إلى معاهدة أو حلف عسكري أو المشاركة في إقامته يتم بناء على قرار السلطات الإدارية الوطنية؛ ويترتب على مثل هذا القرار اعتبار الجرائم التي تمس أسرار دولة حليفة كما لو وقعت على أسرار الدول الأخرى المشتركة معها في هذا الحلف آو تلك المعاهدة؛ ومن ثم يمكن ملاحقة الفاعل ومعاقبته بمقتضى قانون الدولة التي تجري محاكمته أمام محاكمها ولا يستطيع المتهم أن يدفع مسؤوليته بأن ما ارتكبه من أفعال لا يمس سيادة أو أمن الدولة التي يحاكم أمام قضائها، على أن هناك تشريعات تقرر هذه القاعدة بصفة عامة وبصرف النظر عن زمن ارتكاب الفعل، وهناك تشريعات تأخذ بهذه القاعدة في زمن الحرب فقط[2]، أما المشرع الجزائري فقد قرر هذه القاعدة بصفة عامة؛ إذ نص في المادة 94 من قانون العقوبات على أنه: "يجوز للحكومة بمرسوم تصدره أن تخضع الأفعال التي ترتكب ضد أمن الدول الحليفة أو الصديقة للجزائر لكل أو بعض الأحكام الخاصة بالجنايات أو الجنح ضد أمن الدولة سواء في وقت الحرب أو السلم".

[1]– محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 419.

[2]– محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 215.

ب- دور السلطــة القضائيــة فـي تعريـف وتحـديد سر الدفـاع الوطنـي:

إن كل النصوص القانونية التي حاولت تعريف أسرار الدفاع الوطني عجزت عن الوصول إلى تعريف محدد وواضح له؛ الأمر الذي يؤدي إلى الغموض والإبهام عند تطبيقها، ولما كان عبئ تفسير هذه النصوص يقع على القاضي فهو مطالب في هذه الحالة بتجلية هذا الغموض عن طريق قواعد التفسير الكاشف التي تقتضي تطبيق النص على كل ما تتسع له فكرة الشارع ولو لم تشر إليه حرفية النص، وفي هذا الإطار لا يَكون للقاضي أن يُكوِن اقتناعه بمعزل عن رأي الجهة الإدارية، فهي التي تكتشف الواقعة في أغلب الأحيان وهي التي تقدر حسب القواعد الإدارية المنظمة مدى سرية بعض الوثائق أو المعلومات؛ لذا فإن المحكمة عادة ما تستطلع رأي الجهة الإدارية لتقدير مدى سرية الوثائق أو المعلومات في الواقعة المعروضة عليها[1]. وإحالة تحديد سر الدفاع الوطني على القاضي قد يبره المشرع نفسه، وفي هذا الصدد ورغم أن قانون العقوبات المصري قد حاول وضع تعريف شامل لأسرار الدفاع الوطني وقام لأجل ذلك بتعداد كل ما يمكن أن يندرج ضمن ذلك التعريف، إلا أن المشرع قام بالإفصاح من خلال المذكرة الإيضاحية للقانون المصري أنه في أحوال كثيرة تكون طبيعة الوثيقة أو المعلومات بحيث لا تدع مجالاً للشك في أنها تتضمن سراً من أسرار الدفاع عن البلاد بينما قد تقع حالات لا يتبين فيها معنى السرية بطريقة جلية وإذ ذاك يرجع الأمر إلى تقدير المحكمة وفي مثل هذه الأحوال يحسن بالمحكمة أن تأخذ رأي السلطات ذات الشأن وهي أقدر من غيرها على الحكم على أهمية الوثيقة أو المعلومات التي تجري بشأنها المحاكمة وعلى سريتها، ومن المسلم به أن رأي السلطات ذات الشأن رأي استشاري غير ملزم للمحكمة فلها أن تأخذ به ولها أن تطرحه جانباً على أنها إذا أخذت برأي هذه السلطات فإن هذا لا يؤثر في سلامة الإجراءات؛ لأن الأمر يتعلق باقتناع المحكمة برأي استشاري قُدم لها[2]، وهنا تظهر استقلالية السلطة القضائية عن السلطة الإدارية؛ بحيث وبالإضافة إلى أن القاضي يأخذ برأي السلطات الإدارية على سبيل الاستشارة غير الملزمة إذ يحتفظ لنفسه بكامل الحرية في تقدير الطبيعة السرية التي قررتها السلطات الإدارية، فإن هذه الأخيرة لا تتدخل بصورة إلزامية في عمل أو اختصاص محكمة الموضوع التي تنظر الدعوى من أجل تحديد ما إذا كانت المعلومات أو الوثائق

[1]- مجدي محب حافظ، موسوعة جرائم الخيانة والتجسس، مرجع سابق، ص. 238.

[2]- عبد الفتاح مصطفى الصيفي، مرجع سابق، ص. 108.

المنتهكة تمثل سراً من أسرار الدفاع[1]، وإذا استعرضنا موقف التشريعات العقابية المقارنة فإننا نجد أن غالبيتها لا تلزم القاضي باستشارة خبير معين أو سلطة ما لاستطلاع رأيها بشأن مدى سرية وثيقة معينة أو معلومة ما، ولكن من الناحية الواقعية فإنه يشق على المحكمة في أغلب الحالات أن تفصل في الموضوع دون الاستعانة بخبير، وعلى سبيل المثال فالتشريع الفرنسي لا يلزم المحكمة باستشارة الجهة الإدارية أو العسكرية كمصدر للخبرة، بيد أن جهات التحقيق تقوم عادة باستطلاع رأي الجهات المعنية سواء كانت إدارية أم عسكرية حول طابع السرية في الوقائع أو المعلومات التي تتضمنها التحقيقات[2].

وهناك بعض التشريعات تعطي للمحاكم سلطة واسعة في تحديد سر الدفاع الوطني كالقانون البلجيكي والقانون الهولندي (وهي القوانين التي تم الإبراز في موضع سابق أنها لا تحيل على السلطات الإدارية لتعريف سر الدفاع الوطني إلا كاستثناء) وقانون لوكسمبورغ؛ وهذا يرجع إلى أن هذه التشريعات تأخذ بالصيغة العامة والمجردة عند تعريفها لسر الدفاع الوطني وتترك لمحكمة الموضوع حرية تقدير ما إذا كانت الواقعة موضوع الدعوى تدخل أو لا تدخل في إطار تلك الصيغة العامة لسر الدفاع، ويضاف إلى ذلك أن هذه التشريعات تغل يد السلطة الإدارية فيما يتعلق بتحديد سر الدفاع الوطني وهذا يعني أن حرية التقدير الواسعة التي تتمتع بها المحاكم الجنائية في هذا الشأن يمكن أن يؤدي بها إلى تفسير النصوص الجنائية وهي عادة نصوص مرنة وفضفاضة بصورة واسعة مما يتعارض مع مبدأ الشرعية الجنائية، ويلاحظ هنا أن القانون الفرنسي الجديد وفي محاولة منه لمواجهة هذه المسألة الدقيقة قد تدخل بوضع قاعدة جديدة لأول مرة في التشريع الفرنسي تهدف إلى رفع التضارب بين السلطات المعنية بسر الدفاع، وهذه القاعدة مؤداها أن لمجلس الدولة سلطة تحديد سرية المعلومات والوثائق والمعطيات المبرمجة آليا والفهارس والأساليب وغير ذلك من الأشياء التي تحمل طابع سر الدفاع الوطني، وهذا ما تضمنته الفقرة الأخيرة من المادة 413 من قانون العقوبات وذلك عن طريق مرسوم يصدره المجلس[3].

---

[1]– محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 422.

[2]– مجدي محب حافظ، الحماية الجنائية لأسرار الدولة، مرجع سابق، ص. 178.

[3]– محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 217–218.

نخلص بعد استعراض مجمل المحاولات التشريعية لتعريف سر الدفاع الوطني وبعد تناول دور كل من السلطتين الإدارية والقضائية في تحديد ما يعتبر سراً للدفاع إلى القول بأن هـذه المهمـة مـن الصعوبة بمكان؛ إذ لم توفق أي من تلك المحاولات في وضع معيار محدد يمكن على أساسه التمييز بين ما يعتبر سراً وما لا يعتبر كذلك؛ وهذا يرجع أساساً لكون سر الدفاع متعدد الجوانب؛ إذ أن المعلومات أو الأشياء أو المستندات التي يمكن أن تأخذ وصف سر الدفاع تتعلق بجوانب متعددة ويتباين بعضها عن بعض بشكل تام؛ وهذا يجعل الوصول إلى تعريف أو صيغة عامة تجمع مختلف هذه الجوانب أمراً صعباً إن لم يكن مستحيلاً، ويعتبر ما فسر به الأستاذ "اندريه فيتي" هذه الصعوبة أفضل ما يمكن قوله في هذا المقام إذ صرح: "إن الصراع بين الدول في هذا العصر هو صراع شامل لأنه يستغرق كل المصادر الحية للأمة في جميع الميادين العسكرية والاقتصادية والمالية وعلى صعيد الأشخاص كافة سواء كانوا عسكريين أم مدنيين شباباً وشيوخاً، وهو ثانية صراع شامل لأن هدفه النهائي يكمن في قهر العدو لتحقيق الهيمنة، وهو أخيراً صراع شامل لأنه مستمر دائما خارج نطاق الصراع المسلح والذي قد يبدو ظاهرياً أنه صراع أقل مأساوية ولكنه ليس أقل ضراوةً"[1].

وفي إطار هذه الدراسة وبعد عرض المحاولات الفقهية المختلفة الرامية لتعريف السر بصفة عامة وبدون تخصيص، وكذا تناول جوانب الخلل فيها وتقييمها، وبعد عرض المحاولات التشريعية لتعريف سر الدفاع الوطني، والإشارة إلى أن جوهر سر الدفاع الوطني هو ذاته في كل الأزمنة المتغير هو طريقة التعامل معه ومعالجته، فبعد أن كانت معالجة مادية بواسطة الإنسان تحولت إلى معالجة آلية بواسطة الآلة؛ وعليه يمكن اقتراح التعريف العام التالي لسر الدفاع الوطني:

سر الدفاع الوطني هو كل ما يتصل بمظاهر الدفاع الوطني المختلفة (عسكرية أو اقتصادية أو سياسية أو دبلوماسية أو اجتماعية)، سواء تمت معالجته بطريقة تقليدية أم عن طريق نظام معالجة آلية للمعطيات، ويستوجب إبقاءه مكتوما لمصلحة أمن الدولة.

ومنه يشتق تعريف سر الدفاع الوطني الإلكتروني فيكون:

[1]– محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 442.

كل ما يتصل بمظاهر الدفاع الوطني المختلفة (عسكرية أو اقتصادية أو سياسية أو دبلوماسية أو اجتماعية)، والذي يعتمد في معالجته (تخزيناً واسترجاعاً وتعديلاً ونقلاً) على أنظمة المعالجة الآلية للمعطيات، ويستوجب إبقاءه مكتوما لمصلحة أمن الدولة .

المطـــلب الثـــاني: أنـــواع ســـر الدفـــاع الوطنـــي.

الأسرار المتصلة بالدفاع الوطني أو الأمن الخارجي للدولة هي أسرار متعددة ومتجددة ويختلف بعضها عن بعض في الطبيعة وفي المحتوى، ويمكن تقسيمها إلى ثلاثة فئات: فئة الأسرار الحقيقية أو المطلقة، وهي تشمل كل سر يُنبئ عن طبيعته السرية من خلال ذاتيته، وفئة الأسرار المفترضة التي تتفرع بدورها إلى أسرار حكمية وأسرار اعتبارية، كما توجد طائفة من الأسرار ذات طبيعة خاصة تختلف عن الأسرار الحقيقية والأسرار المفترضة من حيث المضمون أو الطبيعة؛ وعليه سيتم التطرق إلى كل فئة من هذه الفئات الثلاث في فرع مستقل.

الفـــرع الأول: الأســـرار الحقيقيـــة.

الأسرار الحقيقية أو المطلقة أو الفعلية هي الأسرار بطبيعتها، أي الأسرار التي تُنبئ عن سريتها بذاتها، وتعرف على أنها: المعلومات المتعلقة بالشؤون الحربية والسياسية والاقتصادية والصناعية ... والتي هي بحكم طبيعتها تعد من الأسرار ولا يعلمها إلا الأشخاص الذين يناط بهم حفظ وثائقها الرسمية وصيانتها، والتي تقتضي مصلحة الدفاع عن البلاد أن تبقى سراً على من عداهم[1].

وبالرجوع إلى قانون العقوبات الجزائري يمكننا استخلاص تعريف الأسرار الحقيقية، والتي تشير حسبه إلى المعلومات أو الأشياء أو المستندات أو التصميمات التي يجب أن تحفظ تحت ستار من السرية لمصلحة الدفاع الوطني أو الإقتصاد الوطني[2]، وهو تقريباً ذات التعريف الفقهي المشار إليه أعلاه.

وتشمل الأسرار الحقيقية قطاعات عديدة ومختلفة ولها شروط لكي تعد كذلك، وعليه سيتم عرض أصناف الأسرار الحقيقية، ومن ثم شروط الأسرار الحقيقية في العنصريين الآتيين:

[1]– سعد إبراهيم الأعظمي، مرجع سابق، ص. 141.

[2]– المادة 63 من قانون العقوبات.

أولاً- أصنـــاف الأســـرار الحقيقيـــة:

تتنوع أصناف الأسرار الحقيقية بحسب تنوع القطاعات التي تخدم الدفاع الوطني وتتغير بحسب إملاءات ظروف العصر؛ فبعد أن كان السر العسكري أكثر أسرار الدفاع الوطني إحاطة بالحماية والأهمية، أصبح في الوقت الحالي سر الدفاع الوطني الاقتصادي يوازيه أهمية وأصبح المحل الذي تستهدفه عمليات التجسس الإلكتروني لارتباطه الوثيق بمجالات الدفاع الأخرى. كما ظهر حديثاً سر الدفاع النووي كصنف له ذاتيته الخاصة وأهميته الملفتة؛ بحيث له ارتباطات بالأسرار الأخرى كالسر العسكري والسر الاقتصادي وحتى السر الدبلوماسي؛ الأمر الذي لا يمكن معه تصنيفه والحديث عنه كتابع لهذه الأصناف، ومن جهة ثانية -وكما سبق القول- فإن هذه الأسرار بمختلف أصنافها قد أصبحت تأخذ شكلاً إلكترونياً باعتماد الدولة على تكنولوجيات المعلومات والاتصالات في معالجتها، لكن جوهر هذه الأسرار يبقى واحداً؛ وعليه فالأسرار الفعلية تشتمل على ما يلي:

أ- الأســـرار العسكريـــة:

ويقصد بها تلك الأسرار المتعلقة بالشؤون العسكرية التي يجب أن تبقى متكتماً عليها لاعتبارات الدفاع الوطني، وسواء كانت هذه الأسرار تخص القوات المسلحة العاملة أو الاحتياطية، كما يشمل كذلك الكوادر التي تنظم عمل ونشاط تلك القوات[1]، وتشتمل على البيانات والمعلومات حول المعدات ومقارنة وتوزيع القوات سواء في ميدان القتال أو الحدود السياسية للدولة، كما يشمل الخطط الدفاعية وأساليب الاتصال والتشفير بين أجزاء المنظومة العسكرية، بالإضافة إلى غرف العمليات الخاصة بالأزمات والكوارث على المستويات المختلفة وما تتضمنه من عملية تبادل المعلومات والبيانات وتحليلها وصياغة السيناريوهات والبدائل وأساليب العمل بها[2].

ب- الأســـرار السياسيـــة والدبلوماسيـــة:

ويقصد بها تلك الأسرار المتعلقة بسياسة الدولة الداخلية أو الخارجية سواء الحالية أو الخطوط العريضة للسياسة المستقبلية للدولة متى اتصلت بالدفاع عن البلاد مباشرة أو بطريق غير مباش[3]، ومنها

[1]- محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 451.

[2]- محمد محمد صالح الألفي، مرجع سابق، ص. 118.

[3]- عبد الحكم فودة ، الموسوعة الجنائية الحديثة، دار الفكر والقانون، مصر، 2002، المجلد الأول، ص. 589.

أيضا ما يتعلق بقرارات الحكومة وموقفها إزاء بعض الأحداث التي تجري في الدول الأجنبية أو موقفها من موقف دولة أجنبية حيال دولة أجنبية أخرى، كما يشتمل على المعلومات الدبلوماسية، ومن قبيلها تقارير السفراء والقناصل إلى وزير الخارجية، والتعليمات المرسلة من هذا الوزير إليهم، والتقارير المرفوعة إلى الوزير ذاته من إدارات الخارجية لما تحتوي عليه تلك الخطابات والتعليمات من بيان لخطة الدولة في السياسة الخارجية وما ترمي إليه الدولة من أهداف وما ترسمه من تدابير[1].

ج- الأســـرار الاقتصاديـــة:

ويقصد بها تلك الأسرار التي تضم كافة المعلومات والبيانات الخاصة باقتصاديات المؤسسات والدول، وتشمل المعلومات المتعلقة بالقطاعات الاقتصادية[2]، والسياسات المالية للدولة، ومواردها الاقتصادية، واتجاهاتها، وبرامج تنظيم الاستفادة منها، وحالة المواد التموينية، والمخزون الإستراتيجي من كل مادة تموينية، وطرق الصناعة، والاختراعات العلمية[3]، كما تشمل تلك المعلومات المتعلقة بالقدرات الصناعية والمصادر الطبيعية، بل إن المعلومات عن الخواص الطبيعية للدول مثل صلاحية مياه الأنهار أو تكوين التربة هامة للغاية[4].

تعتبر المعلومات الاقتصادية إحدى أهم الدعائم التي تستند عليها الدول في العصر الحديث؛ وذلك لأن الاقتصاد في عالم اليوم يلعب دوراً هاماً في تقرير مصير الدول، وعندما يكون الاقتصاد في دولة ما عارياً فإن كل شيء يصبح عارياً؛ فالاقتصاد هو القوة وأساس حركة الدول والحكومات؛ ومن هنا تبرز أهمية الحفاظ على السر الاقتصادي لاسيما وأنه من الصعب على أية دولة أن تحقق درجة مطلقة من الاكتفاء الذاتي لكي تستطيع الاستغناء عن العالم الخارجي المحيط بها ومن ثم فإنها مضطرة لأن تنظر إلى خارج حدودها؛ ومن هنا يأتي دور التجسس الاقتصادي كأداة ووسيلة وفوق ذلك وظيفة أساسية ولازمة للحياة، وظيفة تتجاوز إطار الضرورة وتصل إلى أبعاد الحتمية وذلك بعد أن تغيرت مفاهيم القوة بصورة جذرية؛ فبعد أن كان مفهوم القوة يرتبط بحيازة أكبر عدد ممكن من القوات والجيوش وحيازة الأسلحة ووسائل الردع والفتك، أصبحت القوة اليوم مرتبطة بقوة الاقتصاد لأنه عصب حياة الدول إذ يرجع

---

[1]- سعد إبراهيم الأعظمي، مرجع سابق، ص. 145.

[2]- محمد محمد صالح الألفي، مرجع سابق، ص. 117.

[3]- عماد الدين محمد كامل الجمل، مرجع سابق، ص. ص. 90-91.

[4]- مجدي محب حافظ، الحماية الجنائية لأسرار الدولة، مرجع سابق، ص. 117.

تقدم كثير من الدول إلى نجاحها في الوصول إلى أسرار الصناعة والتجارة والزراعة والسياحة وخاصة أسرار المصارف التي تملك قوة المال وقوة استخدامه؛ وذلك لأن الدور الرئيسي للتجسس الاقتصادي يقوم على تأمين استمرارية تدفق البيانات من مصادرها مما يمكن صانع القرار من المعرفة المسبقة بالأحداث وإجراء تقديرات سليمة للمواقف المختلفة ومعالجة كافة الأشياء التي تجب معرفتها مقدماً وذلك قبل الإقدام على أي تصرف أو سلوك، فعملية تأمين الذات ترتبط ارتباطاً عضوياً بتأمين الحصول على المعلومات مسبقاً؛ وعلى هذا الأساس يمكن القول أن أهداف كل دولة أو كيان يتوقف على ما يتم الحصول عليه من معلومات ضرورية[1].

د- الأســـرار النوويـــة:

تشكل الأسرار النووية طائفة متفردة من طوائف أسرار الدفاع الوطني لارتباطها بجوانبه المتعددة (العسكرية والاقتصادية والاجتماعية ...)، بالإضافة إلى التطورات العديدة التي لحقت بها؛ بحيث يمكن أن نفرق في هذا الإطار بين قسمين من هذا السر هما: السر النووي العسكري، والسر النووي المدني كالآتي:

1- الســـر النـــووي العسكـــري:

إرتبط ظهور هذا السر باستخدام الطاقة النووية للأغراض عسكرية؛ بحيث أدى اكتشاف هذه الطاقة في 1939 وبعده بناء أول مفاعل نووي في العالم في الولايات المتحدة الأمريكية في سنة 1942، إلى تطوير القدرات العسكرية في مجال التسلح؛ بحيث برزت هذه الطاقة في وقت كانت قوة الدول تقاس بقوتها العسكرية، وفي ظروف كان الشاغل الرئيسي للدول فيها هو الهيمنة وبناء منظومة دفاعية تواجه مختلف التهديدات الخارجية بالعدوان المسلح تحديداً، وقد مثلت حينها ولازالت الأسلحة النووية أفضل وسيلة لتحقيق هذا الهدف؛ وعليه فقد كانت الأسرار النووية المرتبطة بتصنيعها أكثر الأسرار إستهدافاً ولا أدل على ذلك من أن الجواسيس السوفيات قد لعبوا دوراً حاسماً في تصنيع القنبلة الذرية السوفياتية الأولى والتي فجرت في 26 أوت من سنة 1949؛ بحيث أن البرنامج النووي السوفياتي بدأ منذ 1943 وقد سمح عمل الجواسيس بتسريع وتيرته، فالسوفيات كانوا يملكون الفيزياء الأساسية لكنهم كانوا يفتقرون إلى

[1]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. ص. 254- 255.

الخبرات العملية فيما يتعلق بتخصيب اليورانيوم وقد قام علماء شاركوا في مشروع مانهاتن بسرقة هذه الخبرات[1]، وبرغم أن العالم وقف على القوة التدميرية لهذا النوع من الأسلحة بمناسبة إلقاء القنبلة الذرية الأولى على مدينة هيروشيما في 6 أغسطس من سنة 1945 وبعدها بثلاثة أيام إلقاء القنبلة الثانية على مدينة ناكازاكي، ورغم ردود الفعل على كافة المستويات إلا أن ذلك لم يوقف التسابق نحو الحصول على مثل هذه الأسرار والتوصل إلى تصنيع مثل هذه الأسلحة؛ ففور اكتشاف إمكانية استخدام الطاقة النووية لأغراض التسليح أصبح حصول بعض الدول القوية آنذاك عليها أمراً محتماً. ومهما بلغت شدة الاحتجاجات المناهضة لمثل هذه الأسلحة ومناداتها بنزعها كان من الواضح أن حكومات الدول الحائزة عليها لا يثق بعضها ببعض بالقدر الكافي لاتخاذ مثل تلك الخطوة؛ فهي تعتقد أن امتلاك رادع نووي قادر على الصمود هو أمر حيوي لآمنها القومي؛ لذا تركزت الجهود هنا على الحد منها دون نزعها الكامل وهو ما أسفر صياغة معاهدة عدم إنتشار الأسلحة النووية، التي فتح باب التوقيع عليها في يوليو سنة 1968 ودخلت حيز التنفيذ في مارس من سنة 1970، والذي كان من بين أهم أهدافها هو إنشاء نظام دولي يتيح النقل الآمن لتكنولوجيا الطاقة النووية المدنية وفيه تشرف الوكالة الدولية للطاقة الذرية على نظام ضمانات يكون لها بموجبه الوصول الكامل والمفتوح للبرامج النووية المدنية لدى جميع الدول غير الحائزة لأسلحة نووية بما في ذلك حق التفتيش الدوري على مفاعلاتها ومنشآتها النووية المدنية؛ وعليه كان أهم أوجه النقد الرئيسية التي وجهت إلى هذه المعاهدة أنها تمنح القوى الحائزة بالفعل لأسلحة نووية وضعاً مميزاً، وعلى الرغم من أن مؤتمر استعراض المعاهدة الذي عقد سنة 1995 قد أقر تمديد معاهدة عدم الإنتشار النووي إلى أجل غير مسمى إلا أن الدول الحائزة على مثل هذه الأسلحة لم تكتف بذلك المركز المميز لكنها ذهبت في عكس إتجاه العمل على إنهاء سباق التسلح النووي وذلك بتطوير برامجها النووية[2].

ما يستخلص من السرد السابق أنه طالما هناك تسابق نحو تطوير القدرات النووية العسكرية؛ فسيبقى واجب الحذر المفروض على هذه الدول يحتم عليها ممارسة التجسس للإطلاع على أسرار

[1]– فرانك دانينو، وكالة الاستخبارات المركزية الأمريكية CIA حكاية سياسية 1947–2007، ترجمة عبير المنذر، مؤسسة الإنتشار العربي، لبنان، 2009، ص. ص. 71– 72.

[2]– بول ويلكينسن، العلاقات الدولية، ترجمة لبنى عماد تركي، مؤسسة هنداوي للتعليم والثقافة، مصر، 2013، ص. ص. 112–114.

بعضها البعض وتحديداً بين الدول المتقدمة التي تملك هذه التكنولوجيا المتطورة خاصة في ظل اعتماد هذه التكنولوجيات وبصورة شبه كاملة على أنظمة المعالجة الآلية، ولا أدل على ذلك من حادثة المفاعل النووي الإيراني وفيروس "ستكسنت" التي تم التعرض لها سابقاً، ومن جهة أخرى نجد أن الإطار القانوني الذي يحكم التسليح النووي وفي مقدمته معاهدة حظر الإنتشار النووي المُشار إليها أعلاه يعطي غطاء من الشرعية لبعض الدول المتقدمة والحائزة أصلاً على برامج للتطوير النووي للأسلحة أن تراقب وحتى تتجسس على برامج الدول الأخرى بحجة منعها من استخدام الطاقة النووية لأغراض غير سلمية مما يمكنها من الاطلاع على الأسرار النووية لهذه الدول.

2- الســـر النـــووي المدنـــي:

لوقت قريب كان هناك فقط صنف واحد من الأسرار النووية وهو السر النووي العسكري، وببروز متغيرات جديدة أصبح معها السر النووي المدني يوازي من حيث القيمة ذلك العسكري؛ فقد أدت النتائج المدمرة لاستخدام الطاقة النووية لأغراض غير سلمية يتصدرها التسليح إلى الإتجاه نحو محاولة الحد من إنتشار هذا النوع من الاستخدام فجاءت المعاهدة الدولية لحظر إنتشار الأسلحة كتتويج للجهود في هذا الإطار، وبغض النظر عن الانتقادات الموجهة إليها فقد أسهمت في التشجيع على استغلال تلك الطاقة لخدمة الإنسان وتطوير مختلف جوانب حياته، وحالياً أصبح هذا الاستخدام المدني السلمي ركيزة لا غنى عنها بالنظر لما تقدمه هذه الطاقة من بدائل وحلول للمشاكل القائمة؛ بحيث تستخدم لمواجهة الخطر الشديد الذي يهدد البشرية والمتمثل في أزمة الطاقة التقليدية؛ إذ أصبحت الطاقة النووية مصدراً أساسياً للتزود بالكهرباء لا غنى عنه لدى الدول الصناعية والتقليل من اللجوء إلى استخدام البترول والغاز الطبيعي، كما أصبحت ركيزة أساسية تقوم عليها الصناعة الحديثة وعصبها في الدول المتقدمة، بالإضافة إلى استخدامها في وسائل النقل البحرية والبرية وفي أبحاث الفضاء؛ بحيث تستغل في إطلاق صواريخ الفضاء وتسيير المركبات الفضائية، علاوة على أنها تستخدم في الأقمار الصناعية التي تقوم بوظائف عديدة، كما تستخدم هذه الطاقة في المجال الطبي والزراعي والإنتاج الحيواني[1].

إن اعتماد مختلف جوانب نشاط الدولة على الطاقة النووية جعلت من هذه الأخيرة ركيزة إستراتيجية في الدفاع الوطني ودفعت الدول بذلك كما الشركات الصناعية الكبرى إلى التنافس بضراوة

[1]- عماد الدين محمد كامل الجمل، مرجع سابق، ص. ص. 49-51.

على سر استخدام هذه الطاقة وكل بحث علمي مستجد بخصوصها وأية تطويرات أو استعمالات جديدة لها، ليضفي تطور تقنيات التجسس بُعداً آخر لهذا التنافس، وقد جاء هذا أيضا كنتيجة لإدخال تلك الأسرار النووية شبكات المعلومات الخاصة بمختلف الدول الأمر الذي أدى بتلك الدول إلى استخدام تقنياتها الحديثة للتجسس على تلك الأسرار وفك شفرات تلك الشبكات وفتح أسواق لعملاء مدربين على أعلى مستوى وخاصة في مجال المعالجة الآلية للمعلومات؛ فأصبحت المعلومات النووية الإلكترونية هي المفتاح السحري لموارد الدول الأخرى وسلعة أو خدمة تباع وتشترى ومصدر قوة اقتصادية وسياسية لمن يحسن جمعها واستخدامها[1].

يبدو تفرد وتميز السر النووي عامة من ارتباطه بجميع أنواع الأسرار الحقيقة السابق ذكرها؛ بحيث في هذا الإطار يوجد معلومات نووية عسكرية، ومعلومات نووية اقتصادية، ومعلومات نووية دبلوماسية، على النحو التالي:

1- المعلومـات النوويـــة العسكريـــة:

المعلومات النووية العسكرية هي تلك المعلومات التي تمثل إحدى دعائم المركز العسكري النووي للدولة في زمن السلم كما في زمن الحرب، والتي تتعلق بالقوة المعدة للقتال النووي سواء عاملة أم احتياطية، ونظام التجنيد الخاص بها، وكذا البرامج والخطط التدريبية الموضوعة لتأهيل وإعداد تلك القوة بدنياً و نفسياً وفنياً للعمل في هذا المجال، وكذلك حجمها، ومهامها، وأسرار استحكاماتها النووية، وأساليبها في القتال، وإستراتيجيتها في الهجوم والدفاع، ونوع ومدى تطور أسلحتها النووية واختراعاتها، وكافة الخطط والأوامر التي تصدرها القيادات في هذا المجال.

يدخل في عداد المعلومات النووية العسكرية أيضا تلك التي تتعلق بالتوصل إلى سلاح نووي جديد أو تطوير سلاح قائم، والسفن النووية التي تستطيع السير لمسافات طويلة دون التزود بالوقود، وكذلك أي معلومات عن المفاعلات النووية الموجودة التي تخدم الأغراض العسكرية من حيث عددها ونوعها وأسرار استحكاماتها حتى تلك التي تمد المعسكرات الحربية بالكهرباء، وكذلك تلك المفاعلات النووية تحت الإنشاء، بالإضافة أيضا إلى المعلومات المتعلقة برصيد الدولة من المواد النووية وخاصة اليورانيوم الطبيعي باعتبارها مواد نووية إستراتيجية تستخدم في التصنيع النووي الحربي.

[1]- عماد الدين محمد كامل الجمل، مرجع سابق، ص. 54.

2- المعلومـات النوويـة الاقتصاديـة:

المعلومات النووية الاقتصادية هي تلك المعلومات التي تتعلق بكافة الأنشطة والمنشات الاقتصادية النووية التي تخدم الدفاع الوطني؛ بحيث أدى إدخال الاستخدامات السلمية للطاقة النووية ضمن الخطة الاقتصادية للدول إلى إقامة منشآت اقتصادية نووية سواء حكومية أو خاصة تعمل في كافة المجالات من طب وصناعة وزراعة ومحطات طاقة نووية لتوليد الكهرباء، كل هـذه الأنشـطة وما حققته أصبحت عنصراً مهماً ضمن خطط التعبئة الاقتصادية للدول، كما تعد المعلومـات الخاصـة بالصناعات النووية من المعلومات الاقتصادية الهامة والإستراتيجية خاصة في ظل التقدم الملحوظ في هذه الصناعات؛ بحيث أصبحت تمثل عصب اقتصاديات الدول المتقدمة وما نتج عنها من أسرار تقنياتها المختلفة التي تحرص الدول دائما على كتمانها والحفاظ عليها، ومن بين هذه الأسرار الصناعية نذكر صناعة الوقود النووي، وتصنيع بعض أجزاء المفاعلات النووية، فضلاً عما لمخزون اليورانيوم الطبيعي وكميته ودرجة نقاوته والبلوتونيوم من أهمية للدفاع عن البلاد كمواد نووية إستراتيجية خاصة تستخدم في التصنيع النووي الحربي.

3- المعلومـات النوويـة الدبلوماسيـة:

المعلومات النووية الدبلوماسية هي تلك المعلومات التي تتعلق بعلاقة الدولة بغيرها من أشخاص القانون الدولي العام من دول ومنظمات دولية في المجال النووي والتي تخدم شؤون الدفاع، وكذلك الموضوعات النووية التي تنظم أو تحل أو يتفاوض بشأنها بالطريق الدبلوماسي، فبالنظر لطبيعة النشاط النووي وآثاره التي تتعدى حدود الدول؛ فقد تواترت الدول على عقد منظومة من المعاهدات الدولية التي تنظم سبل التعاون في هذا المجال خاصة في الاستخدام السلمي له الأمر الذي نتج عنه تداول بعض الأسرار النووية على موائد المفاوضات مما استلزم وضع بنود في هذه الاتفاقيات تفرض الالتزام بالمحافظة على هذه الأسرار[1].

[1]- عماد الدين محمد كامل الجمل، مرجع سابق، ص. ص. 110-112.

ثانيـاً- شـــروط الأســـرار الحقيقيـــة:

يلاحظ من خلال عرض أنواع الأسرار الحقيقية أن ما ورد ضمنها كان على سبيل المثال لا الحصر؛ بحيث أنه من المستحيل تعداد كل ما يندرج ضمن كل طائفة منها نظراً لمتغيرات العصر التي قد تظهر وقائع جديدة أو تضفي السرية على وقائع كانت تعتبر قبلاً وقائع عادية أو تخلع صفة السرية على بعض الوقائع الأخرى وتجعلها مباحة للاطلاع أو التداول بين الناس؛ فنكون بذلك أمام كم كبير من المعلومات يُثار التساؤل حول انتماءها لطائفة الأسرار الحقيقية؛ ولهذا فقد تم تحديد شروط اعتبار معلومة معينة كسر حقيقي بالرجوع للقانون وآراء الفقهاء، وتتمثل شروط الأسرار الحقيقية في أمرين: الأول هو ضرورة أن تكون هذه المعلومات متعلقة بمصلحة الدفاع الوطني، أما الأمر الثاني فيجب أن تكون هذه المعلومات بطبيعتها من الأسرار التي لا يعلمها إلا الأشخاص الذين لهم صفة الاطلاع عليها، وتفصيل ذلك كالآتي:

أ- الشرط الأول: ضـرورة أن تكـون المعلومـات المعينـة متعلقـة بمصلحـة الدفـاع الوطنـي:

نص المشرع الجزائري صراحةً على هذا الشرط في قانون العقوبات وقد تضمنته المادة 63 التي تم استنباط تعريف سر الدفاع الوطني منها والذي يعني حسبها المعلومات أو الأشياء أو المستندات أو التصميمات التي يجب أن تحفظ تحت ستار من السرية لمصلحة الدفاع الوطني أو الاقتصاد الوطني؛ وعليه يستوجب لإعتبار أمر معين سراً حقيقياً يجب أن يكون متعلقاً بمصلحة الدفاع الوطني أي أن يتعلق بصيانة سلامة الدولة وسيادتها ووسائل الدفاع عن كيانها في شتى الميادين في زمن السلم كما في زمن الحرب؛ ذلك أن الدفاع في الوقت الحاضر لم يعد مقصوراً على ميادين القتال بين القوات الحربية بخططها ومعداتها، وإنما أصبح يقتضي فضلاً على ذلك تعبئة كل الجهود السياسية والدبلوماسية وحشد كافة الإمكانيات الاقتصادية الحيوية لتدعيم القوات المسلحة وزيادة قدراتها وصمودها ولسد احتياجات المدنيين ووقايتهم؛ ولهذا وجب أن تأخذ فكرة الدفاع معناها الشمولي في شتى الميادين ودون تفرقة بين أن تكون المعلومات متعلقة بالدفاع عن البلاد في الحاضر أو المستقبل[1].

[1]- سعد إبراهيم الأعظمي، مرجع سابق، ص. 147.

ب- الشرط الثانـي: ضـرورة أن تكـون المعلومـات المعنية بطبيعتها من الأسرار التي لا يعلمها إلا الأشخاص الذين لهـم صفة الاطلاع عليهـا:

ويمكن استخلاص هذا الشرط من صياغة المادة 63 من قانون العقوبات الجزائري وتحديداً من تعبير "التي يجب أن تحفظ تحت ستار من السرية"؛ وعليه يجب أن تكون هذه المعلومات ذات طبيعة سرية ولا يعلمها إلا الأشخاص الذين لهم صفة الاطلاع عليها ويجب مراعاة لمصلحة الدفاع عن البلاد أن تبقى سراً على من عدا هؤلاء الأشخاص، وغني عن البيان أن هذه الطبيعة السرية تكون في أحوال كثيرة من الوضوح بحيث لا تدع مجالاً للشك في أنها تتضمن سراً من الأسرار المتعلقة بسلامة الدولة، لكن تنوع المعلومات تبعاً لتنوع المجالات ذات الصلة بالدفاع الوطني قد يجعل أن تقع حالات أخرى لا تتبين حتى المحكمة فيها وجه السرية أو مدى علاقتها بالدفاع الوطني بصورة أكيدة وفي مثل هذه الحالات -وكما سبقت الإشارة إليه- يَحسُن بالمحكمة أن ترجع إلى الاستئناس برأي السلطات ذات الشأن من عسكرية وإدارية؛ لأن الأمر متعلق بمسألة فنية لا تستطيع المحكمة كشفها ذلك لأن الدوائر الحكومية المختصة أعرف بمقومات السر وحقيقته وبضرورات سلامة الدولة ومصلحة الدفاع عنها، وهذا الرأي لا يلزم المحكمة إلزاماً إنما يخضع لتقديرها ولها أن تقبله كما لها أن ترفضه[1].

ويتعين أن يظل السر مستوراً أو متكتماً عنه في مواجهة غير من كلف بحفظه أو استعماله؛ وعليه يفقد السر طبيعته السرية إذا تقرر إباحته ورفع السرية عنه من طرف الجهات المختصة بمرور مدة زمنية معينة بحيث يكون لكل ذي شأن دون تمييز أن يحصل على مضمونه، أو في حالة ما إذا ذاعت هذه المعلومات وانتشرت بين الناس عن طريق نشرها في صحيفة مثلاً يمكن لكل الناس شراؤها والاطلاع عليها، مع الإشارة إلى أن السرية هنا ترفع فقط على جزء المعلومة الذي تم نشره دون الأجزاء الأخرى التي تبقى محتفظة بطابعها السري هذا في حالة ما إذا كانت المعلومة تشتمل على عديد الجزئيات، لكن تعدد الحفظة للسر أو من لهم صفة العلم به لا يعني ذيوعه فيبقى محتفظاً بطبيعته حتى إذا تحصل عليه جاسوس ما؛ لأنه يبقى في دائرة محدودة من الأشخاص، فضلاً عن كونه ما زال باقياً على أصله من حظر إذاعته أو تناقله[2].

---

[1]- محمد الفاضل، مرجع سابق، ص. 345.

[2]- عبد المهيمن بكر، مرجع سابق، ص. 178.

ومن الجدير بالذكر أن صفة السرية ليست مفهوماً مطلقاً وإنما هي مفهوم نسبي قد يتسع وقد يضيق بالنسبة لزمان اقتراف جريمة التجسس أ في السلم هو أم في زمن الحرب؟، وبالنسبة أيضاً لصفة الدولة التي تم لمصلحتها الإفشاء أ حليفة هي أم معادية؟، فما يجب كتمانه على الدولة المعادية يُباح معرفته من قبل الدولة الحليفة[1].

الفـــرع الثانـــي: الأســـرار المفترضـــــة.

الأسرار المفترضة ليست أسراراً في ذاتها ولكن القانون يفترض اعتبارها كذلك ويمكن إعطائها حكم سر الدفاع الوطني، وهذه الفئة من الأسرار تنقسم إلى فصيلتين: أولاهما تشمل الأسرار الحكمية، أما الثانية فتتعلق بالأسرار الاعتبارية[2]؛ وعليه سيتم التطرق لكل فئة من هتين الفئتين في عنصر مستقل كالآتي:

أولاً- الأســـرار الحكميـــــة:

سيتم التطرق إلى الأسرار الحكمية من خلال عنصرين: يتناول الأول تعريف الأسرار الحكمية وشروطها، بينما يتناول الثاني موقف المشرع الجزائري من الأسرار الحكمية؛ لأنه وبخلاف الأسرار الحقيقية هناك ملاحظات يجب إبدائها وخصها ببعض الشرح، وهذا كالآتي:

أ- تعـريف الأسـرار الحكميـة وشروطهـــا:

الأسرار الحكمية هي: الأشياء أو المحررات والوثائق والرسوم والتصميمات والصور وغيرها من الأشياء التي يجب لمصلحة الدفاع عن البلاد إلا يعلم بها إلا من يناط به حفظها أو استعمالها والتي يجب أن تبقى سراً على من عداهم خشية أن تؤدي إلى إفشاء معلومات "بطبيعتها مـن الأسـرار"، أي لتجنب أن تؤدي إلى الوقوف على سر للدفاع القومي بطبيعته كالمعلومات الحربية أو الصناعية أو السياسية المتعلقة بالدفاع الوطني[3]؛ وعليه فالسر الحكمي ليس سراً في حد ذاته ولكنه يمكن أن يؤدي إلى كشف سر من الأسرار الحقيقية.

---

[1]- محمد الفاضل، مرجع سابق، ص. 349.

[2]- محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 472.

[3]- عبد المهيمن بكر، مرجع سابق، ص. 180.

ويشترط لقيام السر الحكمي ضرورة توافر عنصرين: أولهما أن تكون هناك علاقة أو صلة مباشرة بين السر الحكمي وبين السر الحقيقي، وثانيهما أن يكون السر الحكمي بمثابة وعاء للسر بطبيعته، وهذا كالأتي:

1- وجـود علاقـة بين السر الحكمـي والسـر الحقيقـي:

يشترط لقيام السر الحكمي أن تكون هناك علاقة مباشرة بينه وبين سر من الأسرار الحقيقية بحيث يكون من شأن هذه العلاقة أن تؤدي إلى تمكين الذي يلم بالسر الحكمي من الإحاطة بحقيقة السر الفعلي، ويرجع الفضل في قيام فكرة السر الحكمي إلى القضاء الفرنسي في نهاية القرن التاسع عشر وذلك رغم عدم وجود نصوص قانونية صريحة حول هذه الفئة من الأسرار؛ حيث أدخل القضاء الفرنسي السر الحكمي في مفهوم سر الدفاع الوطني، وفي ذلك قضت محكمة النقض الفرنسية بأن معنى الوثيقة والتي تشكل سراً من أسرار الدفاع يشمل كل الأشياء أو المعلومات التي بطبيعتها تشير أو تعلن عن شيء أو ظرف أو واقعة معينة، بمعنى أن الأشياء أو المعلومات التي تؤدي بصورة تلقائية إلى معرفة حقيقة سر بطبيعته تدخل في حكم الأسرار المحمية جنائيا وذلك نظراً للصلة الوثيقة التي تربط بينهما، وفي ذلك تنص المادة 9/413 في بندها الثاني من قانون العقوبات الفرنسي الجديد أنه يمكن أن تكون موضوعاً لتلك التدابير – تدابير حماية سر الدفاع الوطني – البيانات والأساليب والأشياء والوثائق والمعطيات المبرمجة أو الفهارس التي يكون إفشاءها ضاراً بالدفاع الوطني أو تلك التي يمكن أن تؤدي إلى الكشف عن سر الدفاع الوطني، أما في حالة ما إذا انتفت هذه العلاقة فلا وجود للسر الحكمي[1].

2- وجـوب أن يكون السـر الحكمـي وعـاءً للسـر الفعلـي:

يشترط كذلك لقيام السر الحكمي أن يكون هذا السر سواء كان متمثلاً في وثيقة أو معلومة أو أي شيء آخر، بمثابة وعاء للسر الفعلي؛ فالأسرار الحكمية ليست في الواقع سوى أوعية تحوي الأسرار الفعلية، ومن هنا يمكن وصفها بالأسرار "اللصيقة"؛ ولهذا يتعين أن تكون هذه الأوعية محجوبة عن كل

[1]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 268-269.

من ليست له صفة في الإحاطة بها وأن تظل سرية في مواجهة غير المأذون لهم بمهمة حفظها أو استعمالها أو حيازتها[1].

من الواضح إمكانية أن تكون الأشياء أو الوثائق أو التصميمات أو الصور وغيرها وعاء للسر لأنها من طبيعة مادية وهي تحوي السر وتتضمنه ويجب التمعن فيها للوصول إلى السر الحقيقي، لكن التساؤل يثور بشأن المعلومات إذ أنها من طبيعة معنوية وهي مستحصلة من الأمور المادية السابق ذكرها؛ وعليه فالحصول على المعلومة يعني الحصول على السر الحقيقي وبعبارة أخرى فإن المعلومة هي وعاء للمعلومة ذاتها ولا يمكن الفصل بينهما، ولكن يمكن القول هنا أن هناك معلومات لا يمكن التوصل إلى دلالتها على سر حقيقي إلا بجمعها وربطها بمعلومات أخرى جزئية فالمعلومات السرية هي سلسلة من وقائع متشعبة وقد تكون هذه الوقائع مرتبطة بالإحاطة بوثيقة أو بتصميم أو بشيء؛ ومن هذا المنطلق قد يكون للمعلومة وعاء ولو كان متميزاً عن الأوعية السابق ذكرها.

إن التحقق من توافر شرطي ضرورة وجود علاقة بين السر الحكمي والسر الحقيقي، وكذا ضرورة أن يكون السر الحكمي وعاءً للسر الفعلي يعتبر مسألة تدخل في صميم اختصاص قاضي الموضوع؛ لأن تحديد ما إذا كانت الوثائق أو المعلومات أو الأشياء موضوع الدعوى مرتبطة بسر حقيقي أو تشكل وعاء له أمر يرجع تقديره إلى محكمة الموضوع والتي لها أن تستأنس برأي السلطات المختصة على أن هذا الرأي إذا قُدم إليها لا يلزمها في شيء فلها أن تأخذ به أو تطرحه جانبا شأنه في ذلك شأن أي عنصر من عناصر الدعوى يقبل التمحيص وإثبات العكس[2].

ب- مـــوقف المشـــرع الجزائري مـــن الأســـرار الحكميـــة:

بالرجوع إلى قانون العقوبات الجزائري بغية استجلاء موقف المشرع الجزائري من مسألة تعريف السر الدفاع الوطني الحكمي وتحديد شروطه نجد أنه ضمن مواد القسم الأول الخاص بتجريم سلوكات الخيانة والتجسس من الفصل الأول المتضمن الجنايات والجنح ضد أمن الدولة، تعريف سر الدفاع الوطني الحقيقي كما سبق توضيحه في أكثر من موضع دون تضمين ذات المواد المتعلقة بالتجسس لتعريف لسر الدفاع الوطني الحكمي، ولكن بالرجوع إلى القسم الثاني من ذات الفصل والمتعلق بجرائم

[1]- محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. ص. 474-475.

[2]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 270.

التعدي الأخرى على الدفاع الوطني أو الاقتصاد الوطني يمكننا الوقوف على أن المشرع الجزائري قد اعترف بالأسرار الحكمية وأشار إليها في أكثر من مادة من هذا القسم وباستقرائها والربط بينها يمكن التوصل إلى تعريف للسر الحكمي؛ بحيث نص على أنه يعاقب بالسجن المؤقت من عشر سنوات إلى عشرين سنة كل حارس وكل أمين بحكم وظيفته أو بحكم صفته على معلومات أو أشياء أو مستندات أو تصميمات يجب أن تحفظ تحت ستار السرية لمصلحة الدفاع الوطني **أو يمكن أن تؤدي معرفتها إلى الكشف عن سر من أسرار الدفاع الوطني** يكون قد قام بغير قصد الخيانة أو التجسس بما يلي ...[1]، كما نص أيضاً على أنه يعاقب بالسجن المؤقت من خمس إلى عشر سنوات كل شخص عدا من ذكروا في المادة 66 يكون بغير قصد الخيانة أو التجسس قد ارتكب الأفعال الآتية: 1- الاستحواذ على معلومات أو أشياء أو مستندات أو تصميمات يجب أن تحفظ تحت ستار السرية لمصلحة الدفاع الوطني **أو يمكن أن تؤدي معرفتها إلى الكشف عن سر من أسرار الدفاع الوطني**[2]، ويمكن استخلاص عدة أمور مهمة من استعراض هذين النصين هي:

1- المشرع الجزائري عرف السر الحكمي بأنه المعلومات أو الأشياء أو المستندات أو التصميمات التي يمكن أن تؤدي معرفتها إلى الكشف عن سر من أسرار الدفاع الوطني، وهو ذات التعريف المتداول فقهاً.

2- المشرع الجزائري ربط بين تعريف سر الدفاع الوطني الحقيقي وتعريف سر الدفاع الوطني الحكمي، وهو بذلك يشير إلى العلاقة الوطيدة والارتباط الوثيق بينهما وجعل السر الحكمي تابعاً للسر الحقيقي فوجوده أو انتفاءه مرتبط به وهو ما يعتبر من شروط قيام السر الحكمي الذي سيتم تناوله لاحقاً.

3- المشرع الجزائري من خلال مواد القسم الثاني المتعلق بالاعتداءات الأخرى على الدفاع الوطني وكما سبقت الإشارة إليه يعترف ضمناً بأن الخيانة و التجسس المنصوص عليها في القسم الأول هي نوع من الاعتداءات الماسة بالدفاع الوطني، وهو ما تدل عليه صياغة عنوان القسم الثاني "جرائم الاعتداءات **الأخرى** على الدفاع الوطني أو الاقتصاد الوطني" فقط الفرق بين القسمين هو في التكييف ورغبة المشرع بتخصيص طائفة من الأفعال الخطيرة بأوصاف محددة وبعقوبات صارمة، ومناط هذا

[1]- المادة 66 من قانون العقوبات.

[2]- المادة 67 من نفس القانون.

التفريق هو قصد الفاعل من وراء ارتكاب الأفعال المنصوص عليها من خلالهما، فتكون بذلك معظم الجرائم المنصوص عليها في القسم الثاني جرائم اعتداء على الدفاع الوطني إذا انتفى قصد الخيانة أو التجسس بينما تكون جرائم خيانة أو تجسس إذا توافر قصد الخيانة أو التجسس؛ وعليه لا يجب الذهاب إلى أن المشرع الجزائري قد اعترف فقط بالسر الحقيقي بشأن جرائم التجسس لأنه عرفه ضمن مواد القسم الأول المتعلقة بهذه الجرائم بينما السر الحكمي لا يؤدي المساس به لارتكاب جريمة تجسس بل لارتكاب جرائم تعدي على الدفاع الوطني، فالأسرار التي تكون محل التجسس لا تقتصر على الحقيقية منها بل تشمل أيضا الحكمية وهذا ما تأكده صياغة المادتين 66 و67 أعلاه وذلك من خلال إيراد المشرع لتعريف سر الدفاع الوطني الحقيقي عن طريق النقل الحرفي له من المادة 63 المتعلقة بالتجسس ثم إتباعه مباشرة بتعريف سر الدفاع الوطني الحكمي، كما يستنبط ذلك أيضا من خلال ربط هذين التعريفين بعبارة "بغير قصد الخيانة أو التجسس" الواردة في المادتين 66 و67 إذ وبمفهوم المخالفة يصبح المساس بذات الطائفتين من الأسرار تجسساً إذا كان قصد الفاعل كذلك؛ وعليه فمحل التجسس هو كل الأسرار سواء حقيقية أم حكمية.

4- المشرع الجزائري استخدم تعابير المعلومات والأشياء والمستندات والتصميمات لتعريف سر الدفاع الوطني الحقيقي والحكمي وهي وإن كانت تصلح لتكون محلاً للتجسس التقليدي فإن الأمر يختلف بالنسبة للتجسس الإلكتروني؛ فبالرغم من التأكيد على أن السر يبقى جوهره واحداً بالنسبة لنوعي التجسس والفرق ينحصر في شكل هذا السر وطريقة معالجته بحيث يصبح ذا طبيعة إلكترونية ويُتعامل معه بواسطة نظام المعالجة الآلية للمعطيات، وإذا كان بالإمكان إدخال مفهوم المعلومات ضمنها لأن طبيعتها معنوية وتُستقى من أصناف السر الأخرى وهي الأشياء والمستندات والتصميمات، فإن هذه الأخيرة ذات طبيعة مادية، ورغم أن الأمر ليس بهذا التعقيد إذ أن هذه الأصناف ورغم طبيعتها المادية يمكن تحويلها إلى صورة إلكترونية أي صورة لامادية عن طريق إدخالها إلى نظام المعالجة الآلية؛ إذ أنه ليس بجديد استخدام هذه الأنظمة في حفظ الوثائق والمستندات والتصميمات بعد تصويرها وحتى الأشياء التي من أمثلتها الأسلحة فيمكن تصويرها وإدخالها في هذه الأنظمة مما يسهل إدخال تعديلات في التصميم عليها أو حتى وضع تصاميم لأسلحة جديدة بواسطتها ليبقى فقط التجسيد الفعلي في الواقع لتلك التصاميم؛ وعليه يمكن المساس بهذه الأسلحة وهي بشكل إلكتروني دون إغفال الإشارة إلى أن الأسلحة الحديثة يتم التحكم فيها باستخدام أنظمة تحكم إلكترونية، لكن الإشكال الذي يطرح هنا هو بخصوص موقف المشرع

الجزائري الذي يبقى قديماً لا يساير التطورات فعليه في هذا الإطار مسايرة التشريعات التي أدخلت تعديلات على مفهومها لسر الدفاع وعلى رأسها التشريع الفرنسي الذي اعترف صراحة بالسر الإلكتروني، لذا على المشرع الجزائري أن ينص صراحة على السر الإلكتروني في المواد التي تحكم التجسس بصفة عامة دون الاكتفاء بالنصوص المستحدثة التي تنص على مفهوم المعطيات المعالجة آليا بصفة عامة وتخصيصها فيما بعد في الحالة التي تستهدف الجرائم الماسة بهذه المعطيات الدفاع الوطني كما جاء في المادة 394 مكرر3 من قانون العقوبات؛ وهذا بالنظر إلى أن التجسس الإلكتروني يبقى فرعا تابعاً للأصل ألا وهو التجسس الذي تحكمه مواد القسم الأول خاصة من الفصل الأول المتضمن جرائم أمن الدولة.

لقد تم عرض هذا الكلام بمناسبة الحديث عن الأسرار الحكمية وليس قبلاً (وإن كان ينطبق على سر الدفاع الوطني بصفة عامة) لأن هذه الأسرار ليست في الواقع سوى وعاء يحوي الأسرار الحقيقية؛ بحيث أنه في حالة الاطلاع على ما يوجد داخلها سنكون بصدد سر حقيقي وليس سر حكمي، وهذا الوعاء أو الشكل هو جوهر الاختلاف بين سر الدفاع التقليدي وسر الدفاع الإلكتروني؛ بحيث أصبحت الأوعية الآن تتمثل في الوثائق أو التصميمات الإلكترونية وحتى مفهوم الشيء التقليدي أصبح حالياً عبارة عن وثيقة أو تصميم إلكتروني؛ وعليه فالتوصل لهذه الأوعية يعتبر توصلاً لأسرار حكمية.

ثانيـاً- الأســرار الاعتباريـــة:

سيتم التطرق إلى الأسرار الاعتبارية في عنصرين: يتناول العنصر الأول تعريف الأسرار الاعتبارية و الفرق بينها وبين الأصناف الأخرى من الأسرار، بينما يتناول العنصر الثاني موقف المشرع الجزائري من تعريف الأسرار الاعتبارية، وهذا كالآتي:

أ- تعريـف الأســرار الاعتباريــة والفرق بينـها وبيـن الأصنـاف الأخـرى مـن الأســرار:

الأسرار الاعتبارية هي تلك المعلومات أو الوثائق أو غير ذلك من الأشياء التي ليست بطبيعتها سراً وإنما اعتبرت من الأسرار بناء على أمر من السلطة المختصة[1]، ولا يشترط لقيام السر الاعتباري أو كما يطلق عليه أيضا "السر المتحفظ عليه" أن يكون سراً بمعنى الكلمة بل قد يكون غير ذلك أي قد يمثل

[1]- عماد الدين محمد كامل الجمل، مرجع سابق، ص. 87.

واقعة معروفة لدى قطاع كبير من الناس ومع ذلك ترى السلطات المعنية بالأمر اعتبار مثل تلك الواقعة سراً[1].

ولكون السر الاعتباري تحدده جهات تنتمي إلى السلطة التنفيذية فإن هذا يؤدي إلى القول بأن الجرائم التي تقوم على أساس انتهاك الأسرار الاعتبارية تمثل في حقيقة الأمر جرائم من خلق هذه السلطة وليس من صنع السلطة التشريعية وهو الأمر الذي يخالف مبدأ الفصل بين السلطات، وكان يتعين أن يتم الرجوع لسلطة التشريع في كل مرة يرى فيها ضرورة تجريم وقائع معينة لا أن يتم ذلك من خلال السلطة التنفيذية وبإرادتها المنفردة وبصورة مباشرة، كما أن منح هذه السلطة مثل هذه الصلاحيات يعرض الحريات العامة وحقوق الأفراد للانتهاك؛ لذا فقد توجهت عدة تشريعات إلى إلغاء فكرة السر الاعتباري وأسقطت التجريمات التي ترتكز عليه، ومن أهم هذه التشريعات نجد القانون الإيطالي الذي يعتبر أول قانون يتناول هذا الصنف من الأسرار لكنه قام بإلغاء التمييز التقليدي الذي سبق أن أخذ به بين السر الاعتباري والسر الطبيعي أو الفعلي؛ بحيث نص على أن أسرار الدولة تتحدد في الوثائق والمستندات والمعلومات والأنشطة وكل ما يضر نشره بالدولة الديمقراطية بما في ذلك المعاهدات الدولية والدفاع عن المؤسسات الدستورية والممارسة الحرة للوظائف الأساسية للهيئات الدستورية واستقلال الدولة في مواجهة الدول الأخرى وعلاقتها معها والاستعدادات الدفاعية والعسكرية للدولة، فهذه الأشياء فقط هي التي تدخل في مفهوم سر الدولة[2].

ويختلف السر الاعتباري عن السر الحقيقي، في كون الأول ليس سراً بطبيعته ولكنه إعتُبر كذلك بمقتضى أمر من السلطة المختصة في الدولة وذلك على عكس الحال بالنسبة إلى السر الحقيقي الذي هو سر بطبيعته ويستمد سريته من ذاتيته التي تنبئ عن ذلك تلقائيا ودون حاجة إلى صدور قرار أو أمر من السلطة الحكومية، كما يختلف كذلك السر الاعتباري عن السر الحكمي، فهذا الأخير كما سبقت الإشارة إليه يمثل في الواقع معلومات أو وثائق أو أشياء ترتبط على نحو وثيق بسر حقيقي بحيث يمكن القول بوجود علاقة عضوية بينهما تبرر إخضاعهما لأحكام واحدة، أما السر الاعتباري فليس كذلك؛ إذ أنه لا يتناول مسائل سرية بطبيعتها ولا يرتبط بها بصورة مباشرة؛ ولهذا كان يشترط دائما لقيام السر

[1]– محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 467.

[2]– محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. ص. 279-280.

الاعتباري ضرورة تدخل السلطة الإدارية المختصة بالإعلان عنه وذلك عن طريق اعتبار واقعة ما أو شيء ما ضمن سر الدفاع بخلاف السر الحكمي الذي لا يتطلب مثل هذا التدخل، وغاية ما يتطلبه هذا السر لكي يكون موجوداً أن تكون هناك علاقة تربط بينه وبين سر حقيقي وبحيث تؤدي هذه العلاقة إلى إمكان الكشف عن السر الحقيقي عن طريق الإلمام بالسر الحكمي؛ وعليه فالسر الحكمي يستمد وجوده من القانون مباشرةً وليس من خلال تدخل السلطة الإدارية ، لكن تشترك كل من الأسرار الحقيقية والأسرار الحكمية والأسرار الاعتبارية في موضوعها وما تشتمل عليه بحيث تضم جميعاً طوائف المعلومات والأشياء والوثائق فقط يشترط بالنسبة للسر الاعتباري ألا تكون ذات طبيعة سرية؛ لأنها لو كانت كذلك لتعلق الأمر بسر حقيقي[1].

ب- موقـف المشـرع الجزائـري مـن تعريـف الأسرار الاعتباريـة:

يصدق ما تم توضيحه بخصوص موقف المشرع الجزائري من تعريف الأسرار الحكمية على موقفه بخصوص تعريف الأسرار الاعتبارية؛ وذلك من حيث أنه لم يتطرق لها من خلال نصوص المواد التي تحكم التجسس لأن هذه النصوص قد تضمنت تعريف سر الدفاع الوطني الحقيقي فقط، ولكن بالرجوع إلى نصوص المواد التي تحكم جرائم التعدي الأخرى على الدفاع الوطني أو الاقتصاد الوطني يمكن استخلاص عناصر تمثل جوهر السر الاعتباري رغم أن المشرع الجزائري لم يُعَرف هذا الصنف من الأسرار صراحة.

بحيث باستقراء قانون العقوبات الذي يُقر المعاقبة بالسجن المؤقت من عشر سنوات إلى عشرين سنة لكل من سلم بغير إذن سابق من السلطة المختصة إلى شخص يعمل لحساب دولة أو مؤسسة أجنبية اختراعاً يهم الدفاع الوطني أو معلومات أو دراسات أو طريقة صنع تتصل باختراع من هذا النوع أو بتطبيقات صناعية تهم الدفاع الوطني أو يفشي إليه شيئاً من ذلك[2]؛ نستنتج أن مثـل هـذه المعلومات والأشياء ليست سرية بطبيعتها ولو كان الأمر كذلك لما تمت مناقشة أمر وجود إذن من عدمه بإفشائها أو تسليمها لطرف أجنبي، كما يؤدي التمعن في هذا النص إلى القول بأنه إذا كانت هذه السلطات تملك منح مثل هذا الإذن فهي ذاتها السلطة التي لها صلاحية اعتبار هذه الوقائع أسراراً غير قابلة للتداول، بتعبير

[1]- محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. ص. 478-479.

[2]- المادة 68 من قانون العقوبات.

آخر هي من تمنح واقعة معينة وصف سر وهي من تخلع عنها ذات الوصف وهو جوهر السر الاعتباري.

كما أنه باستقراء قانون العقوبات الذي يُقر المعاقبة بالحبس من سنة إلى خمس سنوات كل من يقدم معلومات عسكرية لم تجعلها السلطة المختصة علنية وكان من شأن ذيوعها أن يؤدي بجلاء إلى الإضرار بالدفاع الوطني إلى علم شخص لا صفة له في الاطلاع عليها أو إلى علم الجمهور دون أن تكون لديه نية الخيانة أو التجسس[1]؛ نستنتج أن مثل هذه المعلومات العسكرية الصالحة لأن تكون علنية بمعنى تقبل إمكانية النشر والتداول هي من حيث طبيعتها غير سرية ولو كان الأمر عكس ذلك لما وضع المشرع الجزائري مثل هذا النص ولاكتفى بنص المادة 63 التي تنص على الأسرار الحقيقية أي الأسرار بطبيعتها؛ خاصة وأن المعلومات ذات الطابع العسكري هي معلومات حساسة يمتنع في أغلب الأحيان من يعلم بها عن نشرها؛ وعليه فهذه المادة كسابقتها تعترف لبعض الجهات المختصة والتي تنتمي إلى السلطة التنفيذية بصلاحية إعتبار واقعة من الوقائع سراً، وبعبارة أخرى فالمشرع الجزائري يعترف بفكرة السر الاعتباري.

الفـــرع الثالـــث: الأســرار ذات الطبيعـــة الخاصـــة.

الأصل أن إفشاء المعلومات التي تتعلق بإجراءات التحري والتحقيق يشكل انتهاكاً للسر المهني باعتبار أن هذه الإجراءات تتسم بالسرية ويستوجب على كل من يعلم بها أو ببعضها عدم إذاعتها ووجوب كتمان السر المهني تحت طائلة العقاب إلا في حالات استثنائية محددة حصراً في القانون[2]، كما أن الأصل في المحاكمة أن تتم جلساتها بشكل علني تحت طائلة البطلان إلا ما تعلق منها بالنظام العام أو

---

[1]– المادة 69 من قانون العقوبات.

[2]– تنص المادة 11 من الأمر رقم 15–02 المؤرخ في 23 يوليو سنة 2015 المعدل والمتمم للأمر رقم 66–155 المؤرخ في 08 يوليو 1966 والمتضمن قانون الإجراءات الجزائية على: "تكون إجراءات التحري والتحقيق سرية ما لم ينص القانون على خلاف ذلك ودون إضرار بحقوق الدفاع.

كل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها فيه.

غير أنه تفادياً لإنتشار معلومات غير كاملة أو غير صحيحة أو لوضع حد للإخلال بالنظام العام يجوز لممثل النيابة العامة أو لضابط الشرطة القضائية بعد الحصول على إذن مكتوب من وكيل الجمهورية أن يطلع الرأي العام بعناصر موضوعية مستخلصة من الإجراءات على أن لا تتضمن أي تقييم للأعباء المتمسك بها ضد الأشخاص المتورطين.

الآداب و كذا محاكمة الأحداث، غير أن الأمر إذا تعلق بجريمة تجسس فإنه يخضع لأحكام خاصة نص عليها قانون العقوبات الجزائري حيث ورد فيه تجريم فعل الإفشاء إلى شخص لا صفة له، وفعل الإذاعة علنا لطائفة من المعلومات تشمل ما يلي:

أولاً– المعلومات المتعلقة بالتدابير التي تتخذ لكشف مرتكبي جريمة التجسس (وكل الجرائم المنصوص عليها في القسم المنصوص عليها في القسم الأول والقسم الثاني من الفصل الأول المتضمن الجنايات و الجنح ضد أمن الدولة) وكذا لكشف شركائهم وللقبض عليهم.

ثانيـــاً– المعلومات المتعلقة بسير إجراءات المتابعة والتحقيق.

ثالثـــاً– المعلومات المتعلقة بسير المحاكمة أمام جهات القضاء[1].

المعلومات السابق إيرادها تمثل أسرارا ذات طبيعة خاصة إذ لا تندرج ضمن الأسرار الحقيقية أو الأسرار المفترضة، لكنها تمثل خروجاً عن القواعد العامة في التحري والتحقيق والمحاكمة أقرها المشرع ومنحها صفة السر خدمة لأغراض الدفاع الوطني ومنعاً لإفلات الجناة أو شركائهم من العقاب؛ وذلك لكون جرائم أمن الدولة الخارجي التي قررت بشأنها هذه الأحكام تشكل خطورة بالغة باعتبارها اعتداءً على شخصية الدولة وكيانها، وفي إفشاء المعلومات المتعلقة بمتابعة هؤلاء الجناة ما يفيدهم أو بعضهم في تجنب القبض عليهم ومحاكمتهم وتوقيع العقاب المستحق عليهم، أو يمكنهم من طمس الأدلة وإتلافها؛ وبالتالي إعاقة العدالة.

تجدر الإشارة في هذا الصدد إلى وجود ارتباط بين حماية أسرار الدفاع الوطني عموماً من جهة والعمل الإعلامي والصحفي من جهة أخرى؛ بحيث إذا كان إفشاء الأفراد لهذه الأسرار يؤدي إلى مساس كبير بأمن الدولة فإن خطورة هذا الإفشاء تكون أكثر وضوحاً وأبلغ أثراً في حالة وقوع مثل هذا الإفشاء أو الإذاعة من خلال وسائل الإعلام المختلفة بالنظر إلى عاملي السرعة في الانتشار واتساع الرقعة المكانية للإذاعة؛ لذا فقد ضمن المشرع الجزائري القوانين التي تنظم العمل الصحفي أحكاماً توضح حدود هذا العمل وطبيعة المعلومة المحظورة عن النشر والإذاعة، فقد نص قانون الإعلام على أن نشاط الإعلام الذي يتضمن كل نشر أو بث لوقائع أو أحداث أو رسائل أو آراء أو أفكار أو معارف وذلك عبر أية

[1]– البند السادس من الفقرة الأولى من المادة 70 من قانون العقوبات.

وسلة مكتوبة أو مسموعة أو متلفزة أو إلكترونية[1]، يُمارس بحرية ولكن مع وجوب احترام مجموعة من القيم والضوابط أهمها السيادة الوطنية والوحدة الوطنية ومتطلبات أمن الدولة والدفاع الوطني والمصالح الاقتصادية للبلاد وسرية التحقيق القضائي[2]، كما أقـــر ذات القانـــون للصحفـــي المحترف بحق الوصول إلى مصدر الخبر ماعدا في الحالة التي يتعلق فيها الخبر بسر الدفاع الوطني أو عندما يمس الخبر بأمن الدولة و/ أو السيادة الوطنية مساساً واضحاً، أو عندما يتعلق الخبر بسر البحث والتحقيق القضائي، أو عندما يتعلق الخبر بسر اقتصادي إستراتيجي، أو عندما يكون من شأن الخبر المساس بالسياسة الخارجية والمصالح الاقتصادية للبلاد[3]، كما عاد المشرع الجزائري ونص في القانون المتعلق بالنشاط السمعي البصري على أن هذا النشاط يمارس بحرية لكن مع ضرورة احترام مجموعة القيم والضوابط التي أقرها قانون الإعلام والمذكورة أعلاه[4]، كما نص على أن دفتر الشروط العامة المتضمن للقواعد العامة المفروضة على كل خدمة للبث التلفزيوني أو للبث الإذاعي يتضمن التزامات احترام متطلبات الوحدة الوطنية والأمن والدفاع الوطنيين، وكذا احترام المصالح الاقتصادية والدبلوماسية للبلاد، وكذا احترام سرية التحقيق القضائي[5].

المبحـــث الثانـــي: وعـــاء ســـر الدفـــاع الوطنـــي الإلكترونـــي وشكلـــه.

رغم الطبيعة الخاصة ومجموعة الميزات التي تكسب التجسس الإلكتروني ذاتيته المستقلة وتفرده عن التجسس التقليدي في عدة مسائل، إلا أنه يبقى تابعاً للتجسس لأنه أحد مراحل تطوره التي استفادت من التقنيات التكنولوجية الحديثة بحيث يظل خاضعاً في كثير من القواعد والأحكام لتلك التي تنظم التجسس عموماً ومنها تحديداً فكرة الدفاع الوطني من حيث المفهوم و الأنواع؛ وعليه فجوهر ومحل التجسس ذاته بالنسبة للإثنين، لكن ما يصنع الفرق بينهما هو وعاء سر الدفاع الإلكتروني؛ بحيث ينصب التجسس الإلكتروني على نظام المعالجة الآلية الذي أصبح البديل عن الإنسان في التعامل مع أسرار الدفاع الوطني التي تم تحويل شكلها لا موضوعها –المدروس سابقاً– من صورة مادية محسوسة إلى

[1]– المادة الثالثة من القانون العضوي رقم 12–05 المؤرخ في 12 يناير من سنة 2012 المتعلق بالإعلام.

[2]– المادة الثانية من نفس القانون.

[3]– المادة 84 من نفس القانون.

[4]– المادة الثانية من القانون رقم 14–04 المؤرخ في 24 فبراير من سنة 2014 المتعلق بالنشاط السمعي البصري.

[5]– المادة 48 من نفس القانون.

صورة إلكترونية لامادية وغير محسوسة فأخذت شكل معلومات إلكترونية، هذه الأخيرة التي تعد العنصر أو الكيان المعنوي لنظام المعالجة فهي جزء أساسي فيه، ونظراً لتبعية المعلومة لنظام المعالجة الآلية فسيتم التطرق بدايةً وذلك في المطلب الأول لوعاء سر الدفاع الوطني الإلكتروني أي نظام المعالجة الآلية للمعطيات، ثم تخصيص المطلب الثاني لشكل سر الدفاع الوطني الإلكتروني ألا وهي المعلومات الإلكترونية.

المطلـــب الأول: وعـــاء ســـر الدفـــاع الوطنـــي الإلكترونـــي.

يمثل نظام المعالجة الآلية للمعطيات الوعاء الجديد والمستودع الذي يحوي ويشمل كل أنواع سر الدفاع الوطني؛ إذ اتجهت كل الدول إلى الاستفادة من خصائص هذه التقنية التي تسهل عمليات التخزين باختزالها للمساحة، فالكم الكبير من أسرار الدفاع من وثائق وتصميمات ومعلومات وحتى تلك التي تدخل في عداد الأشياء أي ذات الطبيعة المادية كالأسلحة مثلا أصبح استحداثها وتصميمها والتعامل معها والتحكم فيها يتم بواسطة هذا النظام، بالإضافة إلى إمكانية استرجاعها وكذا نقلها بسهولة؛ فأصبح الاستغناء عن هذه الميزة التكنولوجية كليا أمراً مستبعداً، وأصبح أيضاً الاكتفاء بمفهوم سر الدفاع الوطني منقوصاً دون دراسة هذه التقنية التي تمنح لهذا السر وصفة الإلكتروني شأنه في ذلك شأن كل المفاهيم القانونية في عصر تكنولوجيا المعلومات والاتصالات؛ وعليه للإحاطة بمفهوم نظام المعالجة الآلية للمعطيات سيتم تناول هذا المطلب في فرعين: يعرض الفرع الأول تعريف نظام المعالجة الآلية للمعطيات، بينما يعرض الفرع الثاني عناصر نظام المعالجة الآلية للمعطيات.

الفـــرع الأول: تعريـف نظـام المعالجـة الآليـة للمعطيـات.

إن تعبير نظام المعالجة الآلية للمعطيات تعبير فني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلاً عن أنه تعبير متغير يخضع للتطورات السريعة ليس في مجال الحاسبات الآلية فقط بل في مجال كل التجهيزات ذات الطابع الإلكتروني، إلا أن الأمر على صعوبته يحتم ضرورة وضع تعريف لهذا النظام لأهمية هذا الأخير والدور الذي يلعبه بالنسبة للدولة أو الأفراد، من سرعة في إنجاز المعاملات، ودقة في الأداء، وتوفير للجهود، وحجم المعلومات والوثائق الضخم التي يمكن تخزينها، وسهولة استرجاع للمعلومات المخزنة[1]، بالإضافة إلى أن نظام المعالجة الآلية للمعطيات يعتبر الشرط

[1]– خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص. 29.

الأولي للبحث في توافر أو عدم توافر جرائم الاعتداء على نظام المعالجة الآلية للمعطيات ومنها جريمة التجسس الإلكتروني، ونظراً لتعدد التعاريف في هذا الشأن وبالمقابل عدم وجود اتفاق بل في أحيان أخرى نقف على التناقض في التعاريف؛ يجب التطرق إلى رأي الفقه، ثم تحديد موقف المشرع منها؛ وعليه ستتم دراسة تعريف نظام المعالجة الآلية للمعطيات من خلال عنصرين: يتناول العنصر الأول التعريف الفقهي لنظام المعالجة الآلية للمعطيات، والعنصر الثاني التعريف القانوني لنظام المعالجة الآلية للمعطيات.

أولاً- التعريف الفقهي لنظام المعالجة الآلية للمعطيات:

لم تكن عملية تحديد تعريف لمصطلح نظام المعالجة الآلية للمعطيات بالشيء البسيط؛ وهذا نظراً لوجود عدة مصطلحات علمية متداخلة ويرتبط كل منها بالآخر، وبعضها مجرد تعبير مرادف للآخر، ورغم ذلك فهناك عدم اتفاق حول المقصود منها؛ لذا تستخدم من طرف كل باحث للدلالة على معنى مختلف عما يرمي إليه غيره؛ الأمر الذي اقتضى ضرورة تتبع منشأ وتطور هذا المصطلح لتجاوز هذه الصعوبات.

فمنذ أن وُجد الإنسان وهدفه التعرف على المحيط الذي ينتمي إليه وسبل التعامل معه؛ لذا شكلت هذه المعارف مجموعة معلومات ذات قيمة وأهمية بالغة في حياته لذا اجتهد على مر العصور في إيجاد طرق أو أنظمة للتعامل مع هذه المعلومات ومعالجتها؛ وعليه فقد سعى إلى جمعها وتسجيلها على وسائط حفظ مختلفة بدءاً من جدران المقابر والمعابد وأوراق البردي إلى أن تم اختراع الورق[1] ليسهل بالنسبة لذلك العصر ولعصور تلته عملية معالجة هذه المعلومات تخزيناً واسترجاعاً ونقلاً؛ وعليه فأنظمة معالجة المعلومات أو المعطيات قديمة قدم وقوف الإنسان على أهمية المعلومة فهذه الأخيرة تبقى ذاتها، المتغير هو الأسلوب المتبع في معالجتها والذي أصبح في المرحلة الحالية يعتمد على الآلة هذه الأخيرة التي كان لها دور أساسي في تغيير مفهوم هذا النظام وتطوره تبعاً لتطورها.

فالنظام اصطلاحاً لفظ مشتق من الكلمة اللاتينية "systema" التي تعني الكل المركب من عدد من الأجزاء، وبالرجوع إلى المعاجم العلمية المتخصصة نجد منها من تعرف النظام بأنه: عنصر مركب يتم تشكيله من عدة وحدات متميزة متصلة مع بعضها البعض بواسطة عدد من العلاقات التي تنشأ لتحقيق التفاهم والترابط بين هذه المكونات أو الوحدات المختلفة، ومنها من يعرف النظام على أنه:

[1]- ياسين قوتال، مرجع سابق.

مجموعة من العناصر التي تمارس وظائفها من خلال علاقاتها بطريقة مماثلة أو أنه مجموعة الأوامر التي تتم بوسائل متعددة من أجل الحصول على نتائج محددة.

وليس هناك تعريف دقيق للنظام لدى ذوي الاختصاص؛ وذلك بسبب تعدد الاستعمال ووجود أنظمة كبيرة تظم بداخلها أنظمة أصغر منها؛ وهذا ما دفع بعض الفقهاء إلى القول بأن النظام يمثل نظرية الانتساب، فالنظام كمفهوم علمي عام لا يختلف من مجال إلى آخر وإنما النظام ذاته يختلف باختلاف المجال الذي ينتمي إليه؛ وعليه فقد تم تعريفه على أنه: مجموعة المكونات ذات علاقة متداخلة مع بعضها تعمل على نحو متكامل داخل حدود معينة لتحقيق هدف أو أهداف مشتركة في بيئة ما وفي سبيل ذلك يقبل مدخلات ويقوم بالعمليات[1] وينتج مخرجات، ومن نفس المنطلق عُرف بأنـــه: كيـــان مرتبط أو متصل بكيانات أخرى والتي تشمل العتاد والتجهيزات والبرامج وحتى البشر والعالم الفيزيائي بظواهره الطبيعية[2] (وهذا ما يفسر أن خطط الأمن المعلوماتي لحماية أنظمة المعالجة في مجال ما، تشمل القواعد الخاصة بالتجهيزات والبرامج والمستخدمين وغيرهم، وكذا تجنب تأثيرات البيئة الطبيعية).

وفي إطار تشعب الأنظمة وتطورها المستمر تبعاً لحاجة الأفراد فإن ذات الحاجة إلى آلية منظمة تتولى عمليات جمع وتوفير المعلومات اللازمة ومعالجتها أدت إلى ظهور مصطلح نظم المعلومات التي تُعرف بأنها: عبارة عن آلية وإجراءات منظمة تسمح بتجميع وتصنيف وفرز البيانات ومعالجتها ومن ثم تحويلها إلى معلومات يسترجعها الإنسان عند الحاجة ليتمكن من إنجاز عمل أو إتخاذ قرار أو القيام بأية وظيفة عن طريق المعرفة التي سيحصل عليها من المعلومات المسترجعة من النظام، وقد يتم استرجاع المعلومات في نظام المعلومات **يدويا** أو **ميكانيكيا** أو **إلكترونيا** وهو الغالب في نظم المعلومات المعاصرة[3]، بمعنى أن مصطلح نظم المعلومات مصطلح واسع جداً يغطي طرق المعالجة التقليدية وكذا العصرية للمعلومات؛ فبعد أن كان نظام المعلومات يقوم على التعامل اليدوي مع المعلومات أصبح يعتمد على التعامل الآلي معها؛ إذ بعد ظهور الحاسبات الآلية ظهر كذلك مصطلح نظم المعلومات المبنية على الحاسبات الآلية أو ما يسمى بنظام المعلومات المحوسبة الذي يرمز إليه بـ "cbis" ، وهو نظام

[1]– رشيدة بوكر، مرجع سابق، ص. ص. 49 –50.

[2]- Fernand Lone Sang, protection des systèmes informatiques contre les attaques par entrées-sorties, thèse du doctorat université de Toulouse, 2012, p .6, mémoire publiée sur le site: www.tel.archives-ouvertes.fr, le site a été visité le: 23/11/2015.

[3]– خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص. 23.

يعتمد على المكونات المادية أو الأجهزة والمكونات البرمجية للحاسوب في معالجة المعطيات وبث واسترجاع المعلومات، وقد تم تعريفه على أنه: عبارة عن آلية وإجراءات منظمة تسمح بتجميع وتصنيف وفرز البيانات ومعالجتها ومن ثم تحويلها إلى معلومات يسترجعها الإنسان عند الحاجة ليتمكن من انجاز عمل أو اتخاذ قرار أو القيام بأية وظيفة عن طريق المعرفة التي سيحصل عليها من المعلومات المسترجعة من النظام.

إلا أنه منذ السبعينات من القرن الماضي وما تطلبه التطور التقني من ضرورة القيام بمهام توفير وجمع ومعالجة وتبادل المعلومات في نفس الوقت؛ فقد ظهر مصطلح نظام المعالجة الآلية باعتباره الواسطة التي أفرزتها عمليات الدمج بين كل من وسائل الحوسبة والاتصال والوسائط المتعددة؛ وعليه فمصطلح نظام المعالجة الآلية هو مصطلح نشأ بهدف وصف الحالة التي نتجت عن اندمـــاج تقنية عملاقة هي تقنية نظم المعلومات وتقنية الاتصالات عن بعد وهندسة التحكم[1]، رغم أنه تجب الإشارة هنا إلى أن مصطلح نظام المعالجة الآلية للمعطيات يغطي ويشمل كذلك النظام التقليدي المسمى بنظام المعلومات المحوسبة القائم على الحواسيب بمفردها دون أن تكون مرتبطة بوسيلة اتصال؛ وعليه فنظام المعالجة الآلية للمعطيات يشتمل على الحواسيب أو التجهيزات الأخرى التي تؤدي ذات الغرض كالهواتف المحمولة حالياً والتي تقوم بعمليات إلكترونية دون الحاجة إلى الربط، كما يشمل الحواسيب والتجهيزات الإلكترونية الأخرى المتصلة ببعضها عن طريق تقنيات الاتصالات.

يذهب جانب كبير من الفقهاء وكذا المشرعين إلى استخدام مصطلح تقنية المعلومات للدلالة على مصطلح نظم المعالجة الآلية للمعطيات وهو حال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وكذا القانون العربي الإسترشادي لمكافحة تقنية أنظمة المعلومات وما في حكمها، والتي سيتم التطرق إليها في التعريف القانوني لنظام المعالجة الآلية للمعطيات، أما من الجانب الفقهي فنقف على عديد التعاريف لتقنية المعلومات والتي تنطبق على تعريف نظام المعالجة الآلية للمعطيات؛ بحيث تعرف تقنية المعلومات الحديثة على أنها: نظام ألي أو إلكتروني تحقق نتيجة الدمج بين تقنية الحوسبة وتقنية الاتصال ذو قدرة على رقمنة الصوت والصورة وتحويلها إلى مادة تفاعل بين المستخدم وبين المحتوى والتعامل مع المعلومات إدخالاً ومعالجةً واسترجاعاً ونقلاً وتبادلاً وتفاعلاً، أو بتعبير آخر تقنية المعلومات الحديثة هي:

[1]– رشيدة بوكر، مرجع سابق، ص. ص. 51–52.

الاستخدام العلمي للحوسبة والإلكترونيات والاتصالات لمعالجة وتوزيع البيانات والمعلومات بصيغها المختلفة[1]، بينما يذهب آخرون إلى تعريف تقنية المعلومات بأنها: تغذية ومعالجة وتخزين ثم بث واستخدام المعلومات الرقمية والنصية والمصورة والصوتية عن طريق تقنيات الحاسب الآلي والاتصالات، وفي إطار وظيفتها عُرفت بأنها: توظيف أدوات وأوعية وأساليب ووسائل وتجهيزات متطورة لنقل المعلومات من المرسل إلى المستقبل بأقل وقت وجهد وتكلفة وبأقصى قدر من الدقة، وعلى ضوء مكوناتها عُرفت بأنها: تشتمل على الأجهزة وما يتعلق بها من شبكات ونظم التشغيل والبرامج ومن أهم الأجهزة الحاسب الآلي، وبصفة عامة هي: نظم تشغيل وتقنيات اتصال وبرمجيات متطورة تسهم في دعم إمكانات الحاسب الآلي بأساليب متطورة تعتمد على العلم والخبرة والمعرفة وتوفر الوقت والجهد والتكلفة وأقصى قدر من الدقة لتغذيـــة ومعالجـــة وتخزيـــن وبـــث استخدام ونقل المعلومات والبيانات وحمايتها[2].

يظهر في هذا الإطار أيضاً مصطلح المعلوماتية كأحد أكثر المصطلحات انتشاراً واستخداماً؛ بحيث يستخدم من قبل البعض للدلالة على نظام المعالجة الآلية للمعطيات، فمصطلح المعلوماتية اختصار مزجي لكلمتي معلومة "information"، وكلمة آلي "automatique" وهي تعني بذلك المعالجة الآلية للمعلومة[3] كما تعني تكنولوجيا معالجة وإرسال المعلومات بواسطة الكمبيوتر، أو هي التزاوج والالتحام بين تقنيات الأنظمة المعلوماتية والاتصالات والاستعمال المتزايد للإلكترونيات[4]، فمن وجهة النظر هذه تكون المعلوماتية مرادفة من حيث المعنى لنظام المعالجة الآلية للمعطيات، لكن المتفحص لمجموعة أخرى من التعاريف الفقهية والأكاديمية يلاحظ الاختلاف بين هذه التعاريف والتعاريف السابق إيرادها؛ بحيث عرفت المعلوماتية بأنها: علم يهتم بالموضوعات والمعارف المتصلة بتحصيل المعلومات وتجميعها وتنظيمها واختزانها واسترجاعها وتفسيرها وبثها وتحويلها واستخدامها، كما يتضمن البحث عن

---

[1]– علي جعفر، مرجع سابق، ص. 31.

[2]– منصور بن سعد القحطاني، مهددات الأمن المعلوماتي وسبل مواجهتها (دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض)، مذكرة ماجستير في العلوم الإدارية، مقدمة لقسم العلوم الإدارية بكلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2008، ص. ص. 17– 18.

[3]– عمر بن محمد العتيبي، الأمن المعلوماتي في المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، أطروحة دكتوراه، مقدمة لقسم العلوم الإدارية بكلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010، ص. 18.

[4]– مسعود خثير، الحماية الجنائية لبرامج الكمبيوتر (أساليب وثغرات)، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2010، ص. 20.

تمثيل المعلومات في النظم الطبيعية والصناعية والإدارية واستخدام الرموز والمفاتيح في نقل الرسالة والتعبير عنها بكفاءة فضلاً عن الاهتمام بدراسة أساليب معالجة المعلومات والأنظمة المعلوماتية ونظم البرمجة، فهي كعلم تتصل بالعديد من العلوم الأخرى لعل أهمها علوم الأنظمة المعلوماتية وعلوم المكتبات والتوثيق وعلوم اللغويات والإحصاء والرياضيات والإدارة ونظريات النظم والاتصالات[1]، كما عُرفت المعلوماتية بأنها: علم التعامل المنطقي مع المعلومات باعتبارها ناقلة للمعارف الإنسانية سواء كانت ذات صبغة تقنية أو اقتصادية أو اجتماعية وذلك من خلال أجهزة أوتوماتيكية وفورية[2]، ولليونسكو تعريف موسع وأكثر حداثة للمعلوماتية بحيث يُدرج في مفهومها الفروع العلمية والتقنية والهندسية وأساليب الإدارة الفنيـة المستخدمـة فـي تـداول ومعالجة المعلومات وتصنيفها والمتعلقة كذلك بالأنظمة المعلوماتية وتفاعلها مع الإنسان والآلات وما يرتبط بذلك من أمور اجتماعية واقتصادية وثقافية[3].

ويتبين من عرض مختلف التعاريف السابقة بشأن المعلوماتية أنها علم واسع يحتوي عديد المفاهيم ويغطي عديد المجالات ويعد نظام المعالجة الآلية أهمها لذا لا يمكن إختزال المعلوماتية في أحد جزئياتها وتعريفها بدلالته.

ثانيـاً- التعريـف القانونـي لنظام المعالجـة الآليـة للمعطيـات:

استخدم المشرع الجزائري تعبير أنظمة المعالجة الآلية للمعطيات لأول مرة في قانون العقوبات وذلك بمناسبة تعديله بموجب القانون 04-15 المؤرخ في العاشر من نوفمبر سنة 2004، لكنه لم يتصدى لها بالتعريف واكتفى بالنص على مجموعة الجرائم التي تشكل مساساً بهذه الأنظمة، لكن بصدور القانون رقم 09-04 المؤرخ في 5 أوت من سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والتي تشمل جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها سابقاً في قانون العقوبات، يمكننا الوقوف على إتجاه المشرع الجزائري إلى محاولة ضبط بعض المصطلحات آخذاً بذلك مسلك معظم التشريعات بخصوص تنظيم المسائل ذات الصلة باستخدام تكنولوجيا المعلومات والاتصالات عامة؛ بحيث خصص المادة الثانية منه لهذا الغرض

[1]- مسعود خثير، مرجع سابق، ص. 19.

[2]- محمد علي العريان، مرجع سابق، ص. 39.

[3]- مسعود خثير، مرجع سابق، ص. 20.

ومن خلال استقراء ما جاء في هذه المادة يمكن تحديد موقف المشرع الجزائري من مسألة تعريف نظام المعالجة الآلية للمعطيات.

تناول المشرع الجزائري في المادة الثانية من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الاتصال والإعلام ومكافحتها مجموعة من المصطلحات التقنية محاولاً وضع تعاريف لها لغرض ذات القانون لكنه لم يخص مصطلح نظام المعالجة الآلية بالشرح المستقل بل ذكره كعنصر من عناصر تعريف بقية المصطلحات الواردة في هذه المادة لكن باستقرائها يمكن الخروج بجملة الملاحظات الآتية:

أ- المشرع الجزائري اعترف بوجود طائفة جديدة من الجرائم كانت نتاج التزاوج بين تكنولوجيا المعلومات وتكنولوجيا الاتصالات؛ وهو ما يتبين من تسمية هذا القانون، وكذا من تعريفه لهذه الطائفة من الجرائم في الفقرة(أ) من المادة الثانية من ذات القانون واعتباره للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تندرج ضمن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بحسب تعبير المشرع الجزائري، والمحاولات الفقهية بصدد تعريف نظام المعالجة الآلية للمعطيات توصلت إلى ذات النتيجة كما سبق عرضه سابقاً.

ب- المشرع الجزائري عرف في الفقرة ب من المادة الثانية مصطلح المنظومة المعلوماتية بأنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة بعضها البعض أو المرتبطة يقوم واحد منها أو أكثـــر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين"، وفي هذا الإطار يذهب بعض الباحثين إلى الإستناد إلى هذه الفقرة للقول بأن المشرع الجزائري قد عرف نظام المعالجة الآلية للمعطيات[1]، وجعلوا بذلك نظام المعالجة الآلية للمعطيات مرادفاً لمصطلح النظام المعلوماتي، وبالتدقيق في معنى المصطلحين نجد تطابقاً من حيث موضوع وجوهر كليهما؛ فنظام المعالجة الآلية للمعطيات يقوم على وجود حاسوب أو مجموعة حواسيب متصلة ببعضها تقوم بعمليات هي جوهر المعالجة الآلية، وهي إدخال المعطيات ومعالجتها وفقاً لبرنامج معين وتحليلها وإخراجها بالصورة المرغوبة، بالإضافة إلى أن هذا التعريف الذي أورده المشرع الجزائري للمنظومة المعلوماتية هو ذاته تعريف النظام المعلوماتي الذي أوردته اتفاقية بودابست، والتي تنص على أنه: "كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذاً لبرنامج معين بأداء معالجة آلية

[1]- رشيدة بوكر، مرجع سابق، ص. 52.

للبيانات"[1]، وإذا كان محتوى تعريف النظام المعلوماتي هو ذاته محتوى تعريف نظام المعالجة الآلية للمعطيات إلا أنه لا يمكن الجزم بأن مصطلح النظام المعلوماتي كلفظ أو كتعبير يُرادف مصطلح نظام المعالجة الآلية للمعطيات أيضاً كلفظ وكتعبير؛ وذلك بالنظر للأسلوب المستعمل من طرف المشرع الجزائري في الفقرة الأولى من المادة الثانية حيث نص بقوله: "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية"؛ بحيث نص على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وعلى الجرائم التي ترتكب عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية كل على حدة وبشكل منفصل ولو رمى إلى عدم التفريق بين مصطلحي نظام معالجة آلية للمعطيات ومنظومة معلوماتية لاستخدم مصطلحاً واحداً، كما يمكن الوقوف على ما يؤيد هذا التوجه وذلك بالرجوع إلى نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 ، والتي صادقت عليها الجزائر سنة 2014، وتجب قبلاً الإشارة و التذكير هنا بأن هذه الاتفاقية استخدمت تعبير تقنية المعلومات للدلالة على نظام المعالجة الآلية للمعطيات، حيث نصت هذه الاتفاقية على أن مصطلح تقنية المعلومات يُقصد به: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا"[2]، وهذا التعريف لمصطلح تقنية المعلومات هو ذاته تعريف نظام المعالجة الآلية للمعطيات بحسب التفسير الوارد سابقا، لتعود وتعرف النظام المعلوماتي في الفقرة الخامسة من نفس المادة بأنه: "مجموعة برامج و أدوات معدة لمعالجة وإدارة البيانات والمعلومات"، دون إشارة منها هنا لضرورة وجود وسيلة ربط أو اتصال، بينما أشارت للتجهيزات المادية والمعنوية وكذا شبكات الاتصالات والربط بين هذه التجهيزات في تعريفها لتقنية المعلومات؛ ما يؤدي للقول بوجود تناقض واضح بين نصوص القانون الجزائري الداخلي رقم 09-04 والاتفاقية العربية المصادق عليها، وفي هذه الحالة يكون الأخذ بالاتفاقية العربية لأنها تسمو

[1]- المادة الأولى من اتفاقية بودابست الأوروبية حول الإجرام المعلوماتي مصادق عليها أمام المجلس الأوروبي في بودابست بتاريخ 23 نوفمبر 2001.

[2]- الفقرة الأولى من المادة الثانية من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010 وقد صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر سنة 2014.

في التطبيق على القانون الداخلي[1]؛ فيكون بذلك نظام المعالجة الآلية للمعطيات غير النظام المعلوماتي، كما أن القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها تضمن ذات التعريف الذي أوردته الاتفاقية العربية إذ نص القانون على أن النظام المعلوماتي هو: "مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات"[2]، دون إشارة إلى تجهيزات الاتصال التي بدونها لا نكون بصدد نظام معالجة آلية.

يستنتج مما سبق عرضه بأن المشرع الجزائري لم يتناول مصطلح نظام المعالجة الآلية للمعطيات بالتعريف صراحةً ولكنه قام بتعريف مصطلح النظام المعلوماتي، وبالتدقيق في فحوى هذا التعريف نجد أنه يصلح كتعريف لنظام المعالجة الآلية، لأنه يقوم على العناصر الضرورية له وهي التجهيزات بمفردها أو مع وسائل الاتصال، رغم ما وقفنا عليه من اختلاف بين مصطلحي نظام المعالجة الآلية والنظام المعلوماتي كتعابير بالاستناد لما جاء في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وكذا القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

ورجوعاً للتشريعات الأخرى بحثاً عن موقفها من تعريف نظام المعالجة الآلية للمعطيات، ومنها القانون الفرنسي خاصة نجده لم يتطرق إلى تحديد مفهوم نظام المعالجة الآلية للمعطيات موكلاً مهمة ذلك إلى الفقه والقضاء، لكن تجدر الإشارة إلى أن مجلس الشيوخ الفرنسي كان قد اقترح تعريفاً لنظام المعالجة الآلية عند تبنيه للقانون رقم 19/88 المعروف بقانون "Godfrain" الصادر بتاريخ 1988/01/05 والمتعلق بمحاربة الغش المعلوماتي وذلك خلال الأعمال التحضيرية[3]، إذ عـَرف نظام المعالجة الآلية للمعطيات بأنه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي يربط بينها

[1]– تنص المادة 150 من الدستور الجزائري (الصادر بموجب المرسوم الرئاسي رقم 96–438 المؤرخ في 07 ديسمبر سنة 1996 المعدل بموجب القانون رقم 16–01 المؤرخ في 06 مارس 2016) على: "المعاهدات التي يصادق عليها رئيس الجمهورية، حسب الشروط المنصوص عليها في الدستور، تسمو على القانون".

[2]– المادة الأولى من القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها المعتمد من طرف مجلس وزراء العرب بتاريخ 2003/10/08 ومجلس وزراء الداخلية العرب بتاريخ 2004/04/21.

[3]– غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، أطروحة دكتوراه، مقدمة لكلية الحقوق، جامعة باجي مختار، عنابة، 2010–2011، ص. 125.

مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا للحماية الفنية"[1].

إن المفهوم السابق الذي يقترحه مجلس الشيوخ الفرنسي يتضمن عنصرين:

العنصـــر الأول: مجموعــة من المكونات المادية والمعنوية المرتبطة ببعضها البعض بعلاقات أو روابط تؤدي إلى تحقيق نتيجة معينــة:

بحيث يتكون نظام المعالجة الآلية من مكونات مادية، ومثالها وحدات الإدخال والإخراج وأسلاك الاتصال، ومن مكونات غير مادية، كاللوغاريتمات التي تشكل البرامج والمعلومات المشفرة في شكل معطيات[2]، فالملاحظ على هذا التعريف أنه يعتمد على أسلوب التمثيل وليس سرد مكونات نظام المعالجة الآلية على سبيل الحصر أي أنه اكتفى بضرورة توافر بعض العناصر كحد أدنى في نظام ما حتى يمكن أن يكون محلاً للحماية الجزائية، وهو مسلك صائب؛ ذلك أن العناصر التي يتكون منها نظام المعالجة الآلية في حالة تطور تكنولوجي مستمر وسريع الأمر الذي يتطلب عدم تقييد التعريف بالعناصر التي وردت فيه، علاوة على أنه لم يحدد وسائل تحقيق المعالجة وعلى رأسها الحاسب الآلي وإنما اكتفى بالإشارة إلى النتائج المحددة، ويُفهم من ذلك أن توافر هذه المكونات في أي جهاز أو آلة تقوم بالمعالجة الآلية ينطبق عليه وفقا لذلك مفهوم نظام المعالجة الآلية، وهو ما حدث بالفعل؛ حيث أثبت العلم أن هناك عناصر أخرى مدمجة بالحواسيب يمكن اعتبارها نظاماً كالهواتف المحمولة؛ لذا فقد اكتفى بتحديد النتيجة من خلال وجود العناصر المادية والعناصر المعنوية المرتبطة ببعضها وهذه النتيجة هي القيام بعملية المعالجة الآلية، وفي هذا الإطار عرف القانون الفرنسي المتعلق بالحريات والمعلوماتية عملية المعالجة الآلية بأنها: عبارة عن مجموعة من العمليات التي تتم آليا وتتعلق بالتجميع والتسجيل والإعداد والتعديل والاسترجاع والاحتفاظ ومحو المعلومات ومجموعة العمليات التي تتم آليا بغرض استغلال المعلومات وخصوصا عمليات الربط والتقريب وانتقال المعلومات ودمجها مع بيانات أخرى أو تحليلها للحصول على معلومات ذات دلالة خاصة[3].

---

[1]– وهيبة رابح، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد الرابع، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، ديسمبر 2014، ص. ص. 321–322.

[2]– غنية باطلي، الجريمة الإلكترونية، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015، ص. 139.

[3]– رشيدة بوكر، مرجع سابق، ص. ص. 53–54.

العنصـر الثاني: ضرورة خضوع النظام للحماية الفنية حتى يتمتع بالحماية القانونية الجنائيـة:

فالحماية الجنائية يجب أن تقتصر على الأنظمة المحمية فنياً؛ لأنه من الطبيعي أن من يقوم باستغلال نظام للمعالجة الآلية للمعطيات يضع الوسائل الفنية اللازمة لمنع الغش، وأن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم وليس من يُهمل منهم توفير الحد الأدنى للحماية، كما أن ضرورة تطلب حماية فنية سيدفع مُستغلي تلك الأنظمة إلى استخدام الحماية الفنية ويكون دور القانون الجنائي في هذه الحالة دور وقائي وهذا أيضاً ما يتفق وسياسة المشرع الجنائي[1]، لكن هذا الشرط رغم مبرراته إلا أنه غير معمول به في معظم التشريعات المنظمة للجرائم الواقعة على أنظمة المعالجة الآلية للمعطيات، فلا يشترط لقيام هذه الأخيرة وجود نظام حماية فنية معين، وهو ذات مسلك المشرع الجزائري، ولكن إذا كان يمكن التخلي عن مثل هذا الشرط بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي تستهدف الأفراد فإن الأمر يجب أن يُراجع بالنسبة لهذه الجرائم في حال مساسها بالدفاع الوطني؛ لأنه من المفترض أن صيانة الأمن الخارجي للدولة والمنصب تحديداً على حماية أسرار دفاعها الوطني تستلزم قيام الدولة بإحاطة مثل هذه الأسرار بسياج من الحماية وفي حالة العكس سيؤدي هذا إلى الاعتقاد بأن هذه الأسرار مباحة للاطلاع والنشر والإذاعة.

إذا كان تعريف مجلس الشيوخ الفرنسي لنظام المعالجة الآلية للمعطيات غير ملزم لأنه حذف من النص النهائي، إلا أنه يمكن للقضاء أن يستهدي به فيما يعرض عليه من منازعات في هذا الخصوص؛ باعتبار أن هذا التعريف يعتبر من الأعمال التحضيرية التي يمكن الاستعانة بها في تفسير غموض النص أو غموض بعض عباراته، وهذا ما يستفاد فعلا من أحكام القضاء الفرنسي حيث أخذ بالمفهوم الموسع للنظام حيث قضى في بعض أحكامه باعتبار شبكة الاتصال وقرص صلب وحاسوب محمول وهاتف محمول من النظام[2].

يستنتج من عرض مجموعة التعاريف الفقهية والموقف التشريعي من عملية تعريف نظام المعالجة الآلية للمعطيات أنه برغم عدم الاتفاق على تعريف واحد لهذا النظام وحتى عدم الاتفاق على مصطلح

[1]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، لبنان، 1999، ص. 123.

[2]– رشيدة بوكر، مرجع سابق، ص. 55.

موحد في هذا الإطار إلا أن العناصر الرئيسية التي تشكل جوهر هذا المصطلح واحدة، وعلى ضوءها يمكن اقتراح التعريف التالي:

نظام المعالجة الآلية للمعطيات هو نظام مكون من مجموعة عناصر مادية وعناصر معنوية مرتبطة ببعضها لآجل تخزين ومعالجة وتعديل واسترجاع ونقل وتبادل المعطيات مهما كان نوعها، وسواء كان هذا النظام منفصلاً أو متصلاً بغيره من الأنظمة الشبيهة بواسطة تقنيات الاتصالات المختلفة.

الفـــرع الثانـــي: عناصـــر نظـــام المعالجـــة الآليـــة للمعطيـــات.

يقوم نظام المعالجة الآلية للمعطيات على ثلاثة عناصر: العناصر المادية وهي مجموع العناصر التي لها وجود ملموس في العالم الخارجي، وتشمل وحدات الإدخال ووحدة المعالجة المركزية ووحدات الإخراج، والعناصر المعنوية وهي مجموعة المكونات من طبيعة لامادية تشمل خاصة المعلومات الإلكترونية، هذه الأخيرة تمثل شكل سر الدفاع الوطني الإلكتروني؛ لذا ورغم كونها من عناصر نظام المعالجة الآلية للمعطيات إلا أنه نظراً لأهميتها الخاصة للدراسة؛ فسيتم تناولها في عنصر مستقل لاحق كما كان الشأن بالنسبة لنظام المعالجة، أما العنصر الثالث فهو عنصر الشبكات أو تجهيزات الربط، وتجدر الإشارة هنا إلى أن كل عنصر من العناصر السابقة يمثل مرحلة من مراحل عملية المعالجة الآلية للمعطيات بالإضافة إلى أن عمليات التجسس الإلكتروني غير محصورة في مرحلة دون الأخرى؛ إذ يمكن القيام بأي سلوك مشكل للجريمة في أي منها، سواء في مرحلة إدخال المعطيات، أو مرحلة معالجتها، أو في مرحلة الإخراج، أو عند القيام بنقل هذه المعطيات من جهاز إلى أخر متصل بالشبكة مهما كان نوع هذه الشبكة وامتدادها ومهما كانت طريقة الربط سلكية أو لاسلكية؛ وعليه سيتم تناول المكونات المادية والشبكات كلٌ في عنصر مستقل، مع تبيان كيف تتم عمليات التجسس الإلكتروني باستغلال هذه العناصر، كالآتي:

أولاً- العناصـــر الماديـــة لنظـــام المعالجـــة الآليـــة للمعطيـــات:

تشمل العناصر أو المكونات المادية لنظام المعالجة الآلية للمعطيات الحاسب الآلي والوحدات التابعة له من وحدات إدخال ووحدة المعالجة المركزية ووحدات الإخراج، وهذا على التفصيل الآتي:

أ- الحـــاسب الآلـــي:

يعد الحاسب الآلي المحور والركيزة الأساسية في أنظمة المعالجة الآلية للمعطيات، وكما تمت الإشارة إليه مراراً من أن التطورات التكنولوجية قد أدت إلى إحداث ثورة على مستوى المصطلح وفي كل المجالات إذ مست هذه التطورات مفهوم الحاسب الآلي كذلك؛ بحيث لم يعد يُمثِل ذلك الجهاز الذي يَمثُل في الذهن عند ذكر هذا التعبير؛ لأن مصطلح الحاسب الآلي أصبح له مدلول شامل يتسع ليحوي مجموعة أخرى من الأجهزة غير الحاسوب بالمعنى التقليدي والضيق للكلمة؛ فالحاسب الآلي بهذا المعنى هو آلة حاسبة إلكترونية تستقبل البيانات ثم تقوم عن طريق الاستعانة ببرنامج معين بعملية تشغيل هذه البيانات للوصول إلى النتائج المطلوبة[1]، وبتعريف آخر هو عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات بطريقة ما وذلك بتنفيذ ثلاث عمليات أساسية هي: استقبال البيانات المدخلة ومعالجة البيانات إلى معلومات وإظهار المعلومات المخرجة[2]، أما التعريف الحالي فيستغرق هذه التعاريف الضيقة للحاسوب، ويتبين ذلك من خلال جملة التعاريف التشريعية التالية:

1- عرف المشرع الأمريكي الحاسوب بأنه: أداة إلكترونية مغناطيسية مرئية وكيميائية أو أية أداة ذات سرعة عالية في معالجة البيانات تؤدي عمليات منطقية رياضية أو عمليات تخزين أو تتضمن أية تسهيلات لتخزين البيانات أو تسهيلات اتصالية[3].

2- عرف نظام مكافحة الجرائم المعلوماتية السعودي الحاسب الآلي بأنه: أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات أو تخزينها أو إرسالها أو استقبالها أو تصفحها ، يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له[4].

---

[1]- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2003، ص. 22.

[2]- نهلا عبد القادر المومني، مرجع سابق، ص. 20.

[3]- علي جبار الحسيناوي، جرائم الحاسوب والأنترنت، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2009، ص. 22.

[4]- الفقرة السادسة من المادة الأولى من نظام مكافحة الجرائم المعلوماتية للمملكة العربية السعودية رقم م/17 وتاريخ 1428/03/08.

3- عرف القانون المتعلق بتنظيم التواصل على الشبكة والجريمة المعلوماتية السوري لسنة 2012 الحاسب الآلي بأنه: أي جهاز يستخدم التقانات الإلكترونية أو الكهرطيسية أو الضوئية أو الرقمية أو أية تقانات أخرى مشابهة بغرض توليد معلومات أو جمعها أو حفظها أو الوصول إليها أو معالجتها أو توجيهها أو تبادلها[1].

نستنتج من استعراض التعاريف التشريعية السابقة للحاسب الآلي أن مفهوم هذا الأخير أصبح يشمل بالإضافة إلى الحاسب الآلي بمفهومه التقليدي كل جهاز آخر يمكنه إجراء عمليات معالجة آلية، أي أنه يتسع ليشمل كل الأجهزة المتولدة عن التطورات العلمية، ويُلاحظ أن التعريف الحديث للحاسب الآلي يطابق تعريف الوسيط الإلكتروني السابق عرضه بمناسبة تعريف التجسس الإلكتروني؛ بحيث يُقصد بالوسيط الإلكتروني كل ما يتصل بالتكنولوجـــيا الحديثـــة وذو قـــدرات كهربائيـــة أو رقميـــة أومغناطيسية أو لاسلكية أو بصرية أو كهرومغناطيسية أو مؤتمتة أو ضوئية أو ما شابه ذلك، وفي إطار شرح هذا التعريف يقصد بالأتمتة العمل بطريقة ذاتية وتلقائية دون اعتماد على الجهد البشري، ومن أمثلة الأجهزة ذات القدرات الكهربائية نجد الحاسب الآلي، ومن أمثلة القدرات الرقمية الحاسب الشخصي المحمول، ومن أمثلة القدرات المغناطيسية أو اللاسلكية نجد الهاتف العادي أو الهاتف المحمول، ومن أمثلة القدرات البصرية الكاميرات الرقمية[2]؛ وعليه فقد أصبح المفهوم الجديد للحاسب الآلي أشمل بكثير من مفهومه التقليدي، بل يحتويه كجهاز فقط من بين أجهزة كثيرة أخرى؛ مما حذا بتشريعات أخرى لتجاوز هذا المصطلح بسبب الخلط الذي قد يسببه واستخدام مصطلحات أخرى لكنها تشير إلى ذات المقصود الحديث بمصطلح الحاسب الآلي، ومنها القانون الإماراتي بشأن مكافحة جرائم تقنية المعلومات حيث استخدم مصطلح "وسيلة تقنية المعلومات" لهذا الغرض حيث يقصد بها: أية أداة إلكترونية مغناطيسية، بصرية، كهروكيميائية أو أية أداة أخرى تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية ويشمل أية قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الأداة[3].

---

[1]- سوزان عدنان الأستاذ، مرجع سابق، ص. 432.

[2]- علي جعفر، مرجع سابق، ص. 33.

[3]- المادة الأولى من القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة.

إن كل الوسائط الإلكترونية أو الحواسيب الآلية بمفهومها الحالي تستلزم ذات العناصر المادية والعناصر المعنوية وكذا تجهيزات الربط لتعد أنظمة للمعالجة الآلية للمعطيات؛ لأنها من حيث طريقة العمل ومبدأ التشغيل، متشابهة، بل يُعد الحاسب الآلي بمفهومه الضيق أفضل مثال من بينها؛ لذا سيتم التركيز على العناصر المادية المتعلقة به.

ب- وحـــدات الإدخـــال:

وهي الوحدات المسؤولة عن مرحلة إدخال المعطيات إلى نظام المعالجة الآلية، ومن أمثلتها لوحة المفاتيح، ومشغل الأقراص المغناطيسية، ومشغل شرائط التخزين أو الأقراص المغناطيسية الصلبة، والفأرة، وتستخدم حالياً وحدات إدخال عالية الكفاءة والسرعة في إدخال المعطيات، ومن أمثلتها أجهزة المسح الإلكتروني التي تقوم بقراءة الوثائق المكتوبة والخرائط المرسومة والصور التي تحولها إلى إشارات ترسلها إلى أجهزة نظام المعالجة الآلية لقراءتها والتعامل معها، كما توجد بعض التجهيزات الأخرى تستخدم للإدخال تتعرف على مطبوعات الحبر المغناطيسي، كما توجد وحدات للتعرف على الحروف والعلامات ضوئيا[1].

يمكن أن ترتكب عمليات التجسس الإلكتروني في مرحلة الإدخال؛ إذ في هذه المرحلة حيث تترجم المعلومات إلى لغة مفهومة من قبل الآلة يكون من السهل إدخال بيانات جديدة لا علاقة لها بالمعطيات القائمة ومحو البيانات الأساسية المطلوب إدخالها[2]؛ بحيث يتم إدخال بيانات وهمية في نظام المعالجة الآلية لم تكن موجودة في من قبل، وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة، أو عن طريق إدخال معلومات مزورة بحيث يتم وضع معلومات بديلة للمعلومات الحقيقية عن طريق الحذف بإزالة كلمة أو رمز معين أو عن طريق الإضافة بزيادة بيانات غير صحيحة[3]، كما يمكن في هذه المرحلة معرفة المعلومات التي يتم إدخالها وهذا عن طريق تسجيل ما يكتب على لوحة المفاتيح من خلال اعتراض الإشارات الكهرومغناطيسية الصادرة عنها عن طريق تجهيزات وبرمجيات معينة.

---

[1]- رشيدة بوكر، مرجع سابق، ص. 58.

[2]- خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص. 85.

[3]- محمد أمين الشوابكة، مرجع سابق، ص. 232.

ج- وحـــدة المعالجـــة المركزيـــة:

تعتبر هذه الوحدة بمثابة العقل المفكر والمسيطر على باقي الوحدات المكونة لنظام المعالجة الآلية أو كما توصف بالعمود الفقري الذي لا وجود لنظام المعالجة الآلية بدونه، وتعمل هذه الوحدة عل تنفيذ جميع العمليات الخاصة بالتشغيل وعمليات المقارنة المنطقية والعمليات الحسابية الموجودة في البرنامج المراد تنفيذه، كما تقوم بتنفيذ المعطيات من وإلى الوحدات المساعدة مع ضمان تحرك المعلومات من وإلى الذاكرة الرئيسية[1].

وفي مرحلة المعالجة التي تقوم بها وحدة المعالجة المركزية وتحديداً من خلال أجزائها الرئيسية يمكن أن يقوم الجاني بالتدخل في الكيان المنطقي للحاسوب والذي يتمثل في مجموعة البرامج المخصصة للقيام بمعالجة المعطيات – تشكل البرامج العنصر الرئيس للتعامل مع المعطيات بحيث لا وجود لمعطيات إلكترونية دون برامج وسيتم التطرق لها في عنصر شكل سر الدفاع الوطني الإلكتروني – ويتخذ هذا التدخل إما صورة تعديل البرنامج القائم أو صورة خلق برنامج جديد؛ بحيث تأخذ صورة تعديل البرامج القائمة إحدى أوجه ثلاث: فتكون إما عن طريق التلاعب في البرنامج، ويتم ذلك ببرمجة النظام بشكل يؤدي إلى اختفاء البيانات بشكل كلي أو جزئي، أو يتم ذلك باختلاس المعلومات عن طريق وضع برامج خاصة بالتقاط البيانات، أو عن طريق تغيير نظام التشغيل وهذا عن طريق تزويد برنامج نظام التشغيل بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة كلمة السر أو مفتاح الشيفرة أو أداة الربط بحيث تتيح الوصول إلى جميع المعطيات التي يتضمنها الحاسب الآلي[2]، ومن الأمثلة عـن هذه الحالة قيام وكالة الأمن القومي الأمريكي NSA بزراعة مفتاح في نظام التشغيل الشهير ويندوز وهو أحد الأسباب التي دعت الحكومة الألمانية لإعلانها في الآونة الأخيرة عن استبدالها لنظام التشغيل ويندوز بأنظمة أخرى[3]، بينما تأخذ صورة خلق برنامج جديد إحدى إحتمالين، فإما أن يكون هذا البرنامج الجديد برنامجاً وهمياً، بمعنى اصطناع برنامج كامل ومخصص فقط لارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات، أو أن يكون هذا البرنامج الجديد برنامجاً ناقصاً من الناحية الفنية، وفي هذا الفرض يقوم الجاني وهو غالباً المبرمج بإدخال فجوات في برنامج الحاسب الآلي حتى يتمكن من تنفيذ التعديلات

[1]- رشيدة بوكر، مرجع سابق، ص. 59.

[2]- محمد أمين الشوابكة، مرجع سابق، ص. 236.

[3]- يوسف حسن يوسف، مرجع سابق، ص. 132.

الضرورية بإدخال رموز "code" إضافية أو إحداث مخارج وسيطة، وإذا كان يفترض في المبرمج نزع هذه الفجوات عند الإنتهاء من البرمجة إلا أن سيئي النية من المبرمجين قد يتغاضون عن استبعاد هذه الفجوات لارتكاب الجرائم، أو أنها قد تُنسى بطريقة الخطأ بسبب عيب مما يتيح للجاني فرصة الدخول من خلالها[1]، أو قد يتم التدخل في مرحلة المعالجة هذه بواسطة إدخال برامج للفيروسات تقوم إما بإتلاف المعطيات أو الحصول عليها، ومثاله فيروس فلام "flame" الذي استخدم لسرقة البيانات والمعطيات في ماي من سنة 2012 من أجهزة كمبيوتر خاصة بعديد من المسؤولين الإيرانيين[2]، كما أنه يمكن التدخل في هذه المرحلة ليس بالاعتماد على البرامج وإنما باستعمال تجهيزات تقنية خاصة تمكن من التقاط الموجات الكهرومغناطيسية المنبعثة من الحاسوب خلال فترة تشغيله مع إمكانية تسجيلها ومعالجتها وترجمتها إلى معلومات تتسم بالوضوح[3].

د- وحـــدات الإخـــراج :

وهي الوحدات التي يتم بواسطتها إخراج المعطيات التي تم معالجتها، ومن أمثلتها شاشات العرض، ووحدات تخزين المعلومات على الأقراص الممغنطة، والطابعات، وأجهزة الرسم.

في مرحلة الإخراج يمكن للجاسوس الإلكتروني القيام بالتلاعب في النتائج التي يخرجها النظام؛ بحيث يتم الحصول على معلومات غير تلك المعالجة مما يؤدي إلى أضرار هائلة، وذلك حين استخدام هذه المعلومات أو توظيفها مع مجموعة معلومات أخرى صحيحة، أو عند إعادة إدخالها مجدداً للنظام للاستفادة منها في عمليات أخرى، كما أنه حالياً توجد طابعات ليزر ثلاثية الأبعاد تقوم بالتجسيد المادي للتصاميم التي يتم القيام بها على الحاسوب وإعطاء تعليمات خاطئة لتلك الطابعات يؤدي إلى الحصول على منتجات غير مطابقة للتصميم الأصلي مع ما لهذا من أضرار واضحة، كما يمكن أيضا التجسس على المعلومات التي يتم طباعتها عن طريق اعتراض ما يصدر عن هذه الطابعات من إشارات كهرومغناطيسية باستخدام وسائل تقنية مختلفة[4].

---

[1]- محمد أمين الشوابكة، مرجع سابق، ص. 237.

[2]- بشرى حسين الحمداني، مرجع سابق، ص. 114.

[3]- نهلا عبد القادر المومني، مرجع سابق، ص. 216.

[4]- ذياب البداينة، الأمن وحرب المعلومات، مرجع سابق، ص. 285.

ثانيـاً- تجهيـــزات الربـــط أو الشبكـــات:

الشبكة بصفة عامة مجموعة من النقاط التي تمثل عناصر كهربائية، أو عناصر إلكترونية، أو نهايات طرفية، أو حاسبات يتصل بعضها بوصلات كما في الشبكات الكهربائية وشبكات الحاسب الآلي وشبكات الاتصال.

ويلاحظ أن معظم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات شائعة الوقوع في نطاق شبكات الحاسب الآلي وشبكات الاتصال[1]، والشبكة على هذا التخصيص عبارة عن أداة ربط بين حاسبين أو أكثر، هذه الرابطة يمكن أن تكون أرضية كالسلك أو الكابل، كما يمكن أن تكون لا سلكية مثل الراديو والأشعة تحت الحمراء والقمر الصناعي، أو كليهما معا أي سلكية ولاسلكية[2]، مع ملاحظة التوجه المتزايد إلى استخدام الشبكات اللاسلكية واستبدال النظام السلكي الذي تم الاعتماد عليه في العقود الماضية، والشبكة اللاسلكية هي الشبكة التي تستعمل الموجات الإلكترومغناطيسية في توصيل المعلومات من نقطة لأخرى دون الاعتماد على أي اتصال مادي، بل بالاعتماد على الأمواج الراديوية، أو الأشعة تحت الحمراء لنقل البيانات[3].

تتعدد أصناف الشبكات فهناك شبكة الأنترانت، وهي عبارة عن شبكة من الحاسبات الآلية الخاصة بمؤسسة واحدة ولا يمكن لأحد الوصول إليها إلا لمن يعمل داخل المؤسسة ولديه كلمة السر، وهناك شبكة الإكسترانت التي تشير إلى شبكة من الحاسبات الخاصة بمجموعة من المؤسسات ولا يمكن لأحد الوصول إليها إلا لمن يعمل ويتعامل مع إحدى هذه المؤسسات ولديه كلمة السر للدخول إليها، وتعد شبكة الأنترنت الطريق السريع للمعلومات، الأكبر والأوسع امتداداً بين كل الشبكات؛ إذ تغطي جميع أنحاء العالم وتصل بين حواسيب شخصية وشبكات محلية وشبكات عامة كما تسمح بانضمام شبكات معلوماتية ذات أنساق مختلفة في إطارها[4]؛ وهي بهذا أكثر الشبكات تعرضاً لمخاطر التجسس وسرقة المعلومات.

---

[1]- عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، مرجع سابق، ص. 56.

[2]- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقاً عليها، دار النهضة العربية، مصر، 2007، ص. 20.

[3]- ضياء مصطفى عثمان، السرقة الإلكترونية، دار النفائس للنشر والتوزيع، الأردن، 2011، ص. 177.

[4] - رشيدة بوكر، مرجع سابق، ص. 87.

تشكل مرحلة نقل وتبادل المعطيات بمختلف صورها مرحلة مهمة في عمليات التجسس؛ إذ يمكن معرفة محتوى اتصال قد يتم داخل نظام حاسوب واحد أو بين نظامين مختلفين أو بين عدة أنظمة ترتبط بينها من خلال شبكة اتصالات، وذلك بالتقاط المعلومات التي يتضمنها هذا الاتصال، ويُعد التقاط الموجات الكهربائية الصادرة عن النظام المعلوماتي الوسيلة الأساسية لاعتراض المعلومات المتنقلة عبر النظام، كما يمكن استخدام أجهزة التقاط خاملة لا تصدر أية إشارات لاسلكية لاعتراض وصلات الموجات القصيرة التي تحتوي على بيانات؛ حيث يمكن بهذه الطريقة اعتراض ما يجري من اتصالات بين المحطات الأرضية والأقمار الصناعية[1]، كما يمكن التجسس على الاتصالات التي تتم سلكياً أي عن طريق الكوابل، رغم أن هذه الطريقة في التجسس الإلكتروني تعتبر تقليدية مقارنة بأساليب التجسس الحالية؛ وهذا بالنظر إلى الاعتماد المتزايد على الاتصالات اللاسلكية[2].

ملاحظـــــة:

يذهب البعض إلى عدم الاكتفاء بالعناصر السابقة للقول بتمام نظام المعالجة الآلية؛ فلا يكفي توافر العناصر المادية والعناصر المعنوية وكذا شبكات الربط، بل يجب أيضا توافر عنصر رابع يعد مهما وأساسيا وهو العنصر البشري "humanware" كمحللي النظم ومطوري البرمجيات ومشغـــلي النظام

---

[1]– نهلا عبد القادر المومني، مرجع سابق، ص. 217–218.

[2]– كمثال على التجسس على الاتصالات اللاسلكية تم في سنة 2006 الكشف عن تفاصيل عملية تجسس على اتصالات لاسلكية من طرف وكالة المخابرات المركزية الأمريكية على الاتصالات الهاتفية العسكرية السوفياتية؛ إذ في بداية الخمسينات من القرن الماضي كانت برلين الرباعية الأجزاء مركز شبكة واسعة من الخطوط الهاتفية والبرقية التي تمتد من غرب فرنسا إلى روسيا، وكانت تتم الاتصالات العسكرية السوفياتية عبر مجموعة من الكابلات التي خُبيء بعضها في باطن برلين، وبناء على اقتراح الأجهزة البريطانية درست الوكالة الأمريكية إمكانية زرع نظام تنصت على هذه الكابلات التي تمر تحت الأرض، وقد تطلب الأمر حفر نفق طوله 450 متر وعمقه ستة أمتار من برلين الغربية حتى الكابلات الواقعة في المنطقة الخاضعة للنفوذ السوفياتي، وكان لابد من اتخاذ الكثير من الاحتياطات لاسيما إزالة قرابة الثلاثة آلاف طن من الرمل دون إثارة الشبهات؛ ولذا قامت الوكالة بالادعاء بأنها تقوم بإنشاء رادار جديد لسلاح الجو، وانطلق المشروع في يناير من سنة 1954، وتم في الشتاء تركيب نظام تبريد داخل الحفرة لأنها تظهر إذا ما ذابت الثلوج بفعل حرارة الإنسان، وقد مكنت هذه العملية من تسجيل أربعين ألف ساعة من الاتصالات المتبادلة بين الأجهزة السوفياتية خلال عام واحد من هذه الاتصالات سمحت للوكالة بالاطلاع على خطط الاتحاد السوفياتي الحربية، ولكن جهاز الكاجي بي كان على علم بالعملية حتى قبل تنفيذها عن طريق دبلوماسي بريطاني أقنعه الكا جي بي بالعمل لحسابه لكنها تركت الأمور تأخذ مجراها رغبة في عدم فضح هذا العميل بالنظر لأهميته الكبرى، ليقرر فيما بعد وضع حد لهذه النشاطات عن طريق تنظيم أعمال حفر فوق النفق في سنة 1956، أنظر: فرانك دانينو، مرجع سابق، ص. ص. 110–111.

وخبراء البرمجة ومهندسي الصيانة[1]؛ إذ بالرغم من أن أهم خاصية لنظام المعالجة الآلية للمعطيات هي الأتمتة أي أن النظام يقوم بوظائفه بشكل تلقائي دون تدخل العامل البشري، إلا أن هذا ليس بصورة مطلقة فمهما بلغت درجة تطور هذه الأنظمة فهي بحاجة دوما لإشراف خبراء في هذا المجال ولمراقبة سلامة سير النظام والتدخل لمواجهة أي طارئ.

المطلـــب الثانـــي: شكـــل ســـر الدفـــاع الوطنـــي الإلكترونـــي.

أدت التسهيلات التي وفرتها أنظمة المعالجة الآلية للمعطيات إلى تزايد تبعية الدول لها واعتمادها عليها في التعامل مع معلوماتها حتى الحساسة منها فأصبحت هناك بنوك للمعلومات تحوي أسرار الدولة المتعلقة بدفاعها الوطني، ومن البديهي أن التحول من طرائق المعالجة اليدوية المنصبة على هذه الأسرار بشكلها التقليدي المادي إلى طرائق المعالجة الآلية قد أنتج شكلاً حديثاً غير مادي يتماشى مع خصوصيات هذه الطرائق المستحدثة؛ بحيث أصبحت أسرار الدفاع الوطني تأخذ شكل معلومات إلكترونية؛ الأمر الذي يحتم ضرورة الإحاطة بهذا الشكل الجديد وإن كان جوهر أسرار الدفاع الوطني واحداً مهما كان شكل هذا السر مادياً أم معنوياً؛ وعليه لتحقيق هذه الغاية سيتم تقسيم هذا المطلب إلى فرعين: يتناول الفرع الأول تعريف المعلومات الإلكترونية وطبيعتها القانونية، ويتناول الفرع الثاني أنواع المعلومات الإلكترونية وخصائصها.

الفـــرع الأول: تعريـف المعلومـات الإلكترونيـة وطبيعتهـا القانونيـة.

تعد المعلومات الإلكترونية ركيزة أساسية في تكوين أنظمة المعالجة الآلية للمعطيات؛ لذا فقد حضي هذا المصطلح من ناحية محاولة تعريفه باهتمام على المستوى الفقهي وعلى المستوى القانوني رغم تعدد أوجه هذه المحاولة وعدم الاتفاق على العناصر الرئيسية التي يشتمل عليها هذا المصطلح، كما أن الجدل والاختلاف ثار بشأن تحديد الطبيعة القانونية للمعلومات الإلكترونية وذلك بغية تحديد القواعد القانونية التي تطبق عليها؛ وعليه سيتم تناول كل من تعريف المعلومات الإلكترونية والطبيعة القانونية للمعلومات الإلكترونية على حدة في عنصر مستقل كالآتي:

[1]– خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص. 26.

أولاً- تعـــريف المعلومـــات الإلكترونيـــة:

لقد تعددت التعريفات بخصوص المعلومات سواء من الناحية الفقهية أو القانونية؛ وعليه سيتم بداية تناول التعاريف الفقهية، ثم تناول التعاريف القانونية، وهذا كالآتي:

أ- التعريـف الفقهـي للمعلومـات الإلكترونيـة:

نقف من الناحية الفقهية على عديد التعاريف التي تتناول المعلومة بصفة عامة وبغض النظر عن شكلها، فالمعلومة بحسب مصدرها اللغوي المأخوذ من كلمة "informer" تعني: القابلية لاتخاذ شكل معين وبذلك يتم توصيل الفكرة إلى الغير[1]، وهو التعريف الذي بنيت على أساسه عديد التعاريف الاصطلاحية؛ فالمعلومة بالنسبة للبعض هي: تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير بفضل علامة أو إشارة من شأنها أن توصل المعلومة لهذا الغير[2]، وهناك تعاريف أخرى أكثر شمولاً واتساعاً ودلالةً على مختلف أنواع المعلومات؛ بحيث تُعرف في هذا الإطار بأنها: مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل أو الاتصال أو للتفسير والتأويل أو للمعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها و نقلها بوسائل وأشكال مختلفة[3].

ب- التعريـف القانونـي للمعلومـات الإلكترونيـة:

سيتم بدايةً عرض تعريف المعلومات الإلكترونية في مختلف القوانين المقارنة، ثم على ضوء ما سيتم عرضه سيُحلل موقف المشرع الجزائري من تعريف المعلومات الإلكترونية، وهذا كالآتي:

1- تعريـف المعلومـات الإلكترونيـة في القوانين المقارنـة:

بالرجوع إلى النصوص القانونية المقارنة لمعرفة موقف المشرعين من هذا المستجد الإلكتروني؛ نجد كذلك مجموعة كبيرة من التعاريف، لكن ما يلاحظ عليها أنها أكثر تخصيصاً من التعاريف الفقهية إذ تتناول المعلومة الإلكترونية تحديداً، ويمكن إيراد أهمها فيما يلي:

---

[1]- سليم عبد الله الجبوري، مرجع سابق، ص. 35.

[2]- غنية باطلي، الجريمة الإلكترونية، الدار الجزائرية للنشر والتوزيع، مرجع سابق، ص. 59.

[3]- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، مصر، 2010، ص. 27.

– عرف المشرع الفرنسي المعلومة في القانون الخاص بالاتصالات السمعية والبصرية الصادر في 29 جويلية من سنة 1982، بأنها: رنين صور الوثائق والبيانات أو الرسائل من أي نوع[1].

– عرف المشرع الأمريكي المعلومة الإلكترونية في قانون المعاملات التجارية الإلكترونية لسنة 1999، بأنها: تشمل البيانات والكلمات والصور والأصوات وبرامج الكمبيوتر والبرامج الموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك[2].

– عرف المشرع الإماراتي المعلومات الإلكترونية في قانون مكافحة جرائم تقنية المعلومات بأنها: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات، وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها[3].

– عرف المشرع الأردني المعلومات الإلكترونية في قانون جرائم أنظمة المعلومات بأنها: البيانات التي تمت معالجتها وأصبح لها دلالة[4].

– عرف المشرع السوري المعلومات الإلكترونية في القانون المتعلق بتنظيم التواصل على الشبكة والجريمة المعلوماتية بأنها: العلامات أو الإشارات أو النصوص أو الرسائل أو الأصوات أو الصور الثابتة أو المتحركة التي لها معنى قابل للإدراك مرتبط بسياق محدد[5].

ما يلاحظ على التعاريف السابقة أنها حاولت تعريف المعلومات الإلكترونية عن طريق تعداد ما يندرج ضمنها على سبيل المثال متفاديةً إعطاء معنى محدد ومباشر لها يشرح طبيعتها ويميزها عن المعلومات العادية، لكن أغلب هذه التعاريف على قدر من التناقض وعدم الاتفاق ليس فقط على تحديد تعريف للمعلومة الإلكترونية بل وعلى استخدام المصطلحات في هذا الشأن، فمنها من يعرف المعلومات بدلالة البيانات، ومنها من يقوم بتعريف البيانات بدلالة المعلومات، ومنها من يعرف المعلومات بدلالة

---

[1]– مسعود خثير، مرجع سابق، ص. 15.

[2]– خالد ممدوح إبراهيم، الجريمة المعلوماتية، مرجع سابق، ص. 50.

[3]– المادة الأولى من القانون الاتحادي رقم 2 لسنة 2006 في شان مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة.

[4]– المادة الثانية من قانون جرائم أنظمة المعلومات الأردني رقم 30 لسنة 2010.

[5]– المادة الأولى من المرسوم التشريعي رقم 17 المؤرخ في الثامن من شباط سنة 2012 المتعلق بقانون تنظيم التواصل على الشبكة والجريمة المعلوماتية لدولة سوريا.

البرامج وهو ما يبدو جلياً من التعاريف التي أوردها كل من المشرع الفرنسي والمشرع الأمريكي وكذا المشرع الإماراتي (لأن تعريفه للمعلومات الإلكترونية هو ذاته تعريف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[1])؛ بمعنى أن هذه القوانين لم تعط أي أهمية للفروقات الفنية بين مصطلحات المعلومات والبيانات والبرامج، بينما تجنب التعريف الممنوح للمعلومات الإلكترونية من طرف كل من المشرع الأردني والسوري هذا الخلط واعتد بالفرق الفني بين المعلومات والبيانات، ولا يمكن توضيح هذا بشكل كاف دونما وضع حدود للعلاقة بين كل من المعلومات والبيانات والبرامج من الناحية الفنية، وهذا ما سيتم من خلال العناصر الآتية:

- الفـــرق بيـن المعلومـات والبيانـات:

تجدر الإشارة بدايةً إلى أن المشرع الجزائري قد فضل استخدام مصطلح المعطيات بدلاً من مصطلح البيانات، ولا يوجد فرق بينهما إذ أن المعطيات لغة تعني البيانات؛ وعليه فالفرق الذي يكون بين المعلومات والبيانات هو ذاته الفرق بين المعلومات والمعطيات.

فالبيانات لغةً تعني: شيء مُعطى أو مُسلم به، وشيء ما معروف أو مسلم بصحته كحقيقة أو واقعة[2]. أما في الاصطلاح فلها عديد التعاريف يُكتفى منها بتلك التي توضح العلاقة بينها وبين المعلومة، فيعرفها البعض بأنها: مجموعة من الحقائق أو القياسات أو المعطيات التي تتخذ صورةً، أو أرقاماً، أو حروفاً، أو رموزاً، أو أشكالاً خاصةً، وتصف فكرةً، أو موضوعاً، أو حدثاً، أو هدفاً معيناً، ويتم تحويلها كمواد خام لغرض استخراج معلومات معينة[3]، بينما عرفها البعض بطريقة أكثر تركيزاً بأنها: مجموعة الحقائق والأفكار التي لم تتم معالجتها، أو بأنها المادة الخام للمعلومات، وحتى تصبح البيانات معلومات لابد أن تعالج هذه البيانات بطريقة معينة[4]، وفي حالتنا هي المعالجة الآلية.

---

[1]- تُعرِف الفقرة الثالثة من المادة الثانية من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، البيانات بأنها: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات كالأرقام والحروف والرموز وما إليها....

[2]- هشام محمد فريد رستم، مرجع سابق، ص. 25.

[3]- رشيدة بوكر، مرجع سابق، ص. ص. 66-67.

[4]- عبد الرحمان شعبان عطيات، أمن الوثائق والمعلومات، جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، 2004، ص. 122.

وعليه فالبيانات أو المعطيات عبارة عن حقائق يمكن لآحاد الناس قراءتها وفهم دلالتها البسيطة دون الدخول في عمليات استنتاجية واستقرائية لدلالتها المعقدة سواء من حيث الربط بين أكثر من بيان منها أو استخلاص أية نتيجة مترتبة عليها (وهذا ما يطابق المقصود منها لغوياً)، فإن تم ذلك بدء الدخول في منطقة أخرى وهي منطقة المعلومات؛ فالمعلومات وفقاً لذلك هي كل نتيجة مبدئية، أو نهائية مترتبة على تشغيل المعطيات، أو تحليلها، أو استقراء دلالتها، واستنتاج ما يمكن استنتاجه منها وحدها، أو مترافقة مع غيرها، أو تفسيرها على نحو يثري معرفة مستخدمي القرار ويساعدهم على الحكم السديد على الظواهر والمشاهدات[1]، ولكن هذا لا يعني استقلالية كل من المعطيات والمعلومات فهناك علاقة وثيقة يُعبر عنها بالدورة الإسترجاعية للمعلومات؛ إذ يتم تجميع وتشغيل البيانات والحصول على معلومات ثم تستخدم هذه المعلومات في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من البيانات التي يتم تجميعها ومعالجتها مرة أخرى للحصول على معلومات إضافية يُعتمد عليها في إصدار قرارات جديدة[2]، وهذا ربما ما يفسر اختلاف نظرة القوانين إلى هذا الموضوع؛ فمن القوانين من يُعرف المعلومات بدلالة المعطيات كما هو شأن القانون الأمريكي، وهناك من يعرف البيانات بدلالة المعلومات كما هو شأن القانون السعودي؛ إذ عرف نظام مكافحة جرائم المعلوماتية البيانات وأورد المعلومات الإلكترونية كجزء منها، ونص بأن البيانات هي المعلومات أو الأوامر أو الرسائل أو المواصلات أو الأصوات أو الصور التي تعد أو التي سبق إعدادها لاستخدامها في الحاسب الآلي وكل ما يمكن تخزينه ومعالجته كالأرقام والحروف والرموز وغيرها[3]، وهناك من القوانين من تمنح أهمية للتفريق بين المعلومات والبيانات وهو تفريق ذو طابع فني، ومنها القانون السوري والقانون الأردني الذي نص صراحة على أن المعلومات هي البيانات التي تمت معالجتها.

- **الفـــرق بيـن المعلومـــات والبرامـــج:**

تشكل كل من المعلومات والبرامج المكونات غير المادية للحاسب الآلي والتي لا يمكن بدونها لهذا الأخير أن يؤدي وظائفه، وللبرامج تحديداً أهمية أساسية؛ إذ تمثل ما يمكن أن يُسمى بفكر الحاسب؛

---

[1]- رشيدة بوكر، مرجع سابق، ص. 67.

[2]- نهلا عبد القادر المومني، مرجع سابق، ص. 102.

[3]- الفقرة الرابعة من المادة الأولى من نظام مكافحة الجرائم المعلوماتية للمملكة العربية السعودية رقم م/17 و تاريخ 1428/03/08.

فهي التي تحدد له العمليات المطلوب انجازها وترتيب وكيفية أدائها، وبدونها لا يعدو الحاسب أن يكون مجموعة معدات إلكترونية عاطلة عن الاستخدام؛ ومن هذا المنطلق تعرف البرامج على أنها: مجموعة التعليمات التي يخاطب بها الإنسان الآلة فتسمح بأداء مهمة محددة[1]؛ ومن هنا يتبين الدور الرئيسي لهذا المكون بحيث أنه بدون برامج لا يمكن الحديث عن معالجة آلية للمعطيات ولا عن معلومات إلكترونية أصلاً.

ومن الناحية القانونية نرصد عديد التعاريف للبرامج؛ إذ نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن البرنامج المعلوماتي هو: مجموعة من التعليمات والأوامر قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما[2]، وهو ذات التعريف الذي أوردته المادة الثانية من قانون جرائم أنظمة المعلومات الأردني، وكذا المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي.

إذا كانت المعلومات إلى جانب البرامج تشكل المكونات غير المادية لنظام المعالجة الآلية للمعطيات وهما بالنسبة له بمثابة الروح من الجسد، إلا أن الفرق بينهما يكمن في الغاية منهما، فالغاية من البرنامج في حد ذاته هو الوظيفة التي يقدمها والتي تتمثل في تشغل نظام المعالجة الآلية وتوجيهه إلى حل المشاكل ووضع الخطط المناسبة فضلاً عن اضطلاعه بمهمة المعالجة الآلية لإفراز المعلومات الإلكترونية المتداولة؛ بحيث بغيابه يصير نظام المعالجة الآلية مجرد كتلة حديدية صماء كباقي الآلات، أما المعلومات فالغاية من وجودها تكمن فيها في حد ذاتها؛ إذ ليس لها دور معين في تشغيل نظام المعالجة الآلية، وإنما يعتبر هذا الأخير بمثابة المستودع أو الوعاء الذي يتم فيه معالجة هذه المعلومات وتخزينها ثم إتاحتها عند طلبها واسترجاعها وذلك بالاطلاع عليها وتكوين معرفة أو دراية توفرها هذه المعلومات[3].

2- تعـريف المعلومـات الإلكترونيـة في القانـون الجزائـري:

لم يتضمن قانون العقوبات ولا قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أي تعريف للمعلومات الإلكترونية، واكتفى المشرع الجزائري بتعريف المعطيات المعلوماتية وذلك في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث نص على

[1]- مسعود خثير، مرجع سابق، ص. 27.

[2]- الفقرة الرابعة من المادة الثانية من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3]- رشيدة بوكر، مرجع سابق، ص. 74.

أن المعطيات المعلوماتية هي: "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"[1]، وكما سبقت الإشارة فإن المشرع الجزائري يستخدم مصطلح المعطيات بدلا عن البيانات لأن معناهما واحد، ويستنتج من التعريف أعلاه أن المشرع الجزائري لا يعير أهمية للتفرقة الفنية بين المعلومات والمعطيات والبرامج بل جعلها مرتبطة من حيث النتيجة القانونية إذ تخضع جميعها لذات الحماية القانونية الجزائية المقررة بموجب قانون العقوبات، وعدم التفرقة هذه تظهر من خلال المعنى الموسع للمعطيات فهي تشمل المعلومات وكذلك البرامج، وهو ذات إتجاه المشرع الأمريكي، وإن كانت هناك فروقات فنية أساسية بين المعطيات والبرامج والمعلومات بحسب التوضيح السابق، فإن المشرع في هذه الحالة غير ملزم بأن يكون تابعاً للقواعد العلمية في هذه الحالة، بالرغم من أننا بصدد دراسة مصطلحات تقنية بحتة، لكن الفرق بينها من الناحية الفنية لا يؤثر في تطبيق النص الجزائي؛ لأن النتيجة واحدة في كل الحالات وهي المساس بنظام المعالجة الآلية للمعطيات، بل بالعكس قد يؤدي اعتماد المشرع لهذه التفرقة إلى صعوبة بالغة في تطبيق النص الجزائي خاصة في مجال أسرار الدفاع الوطني التي تتخذ هنا شكل معلومات إلكترونية؛ فبإعتبار أن البيانات هي مُدخلات نظام المعالجة الآلية فأسرار الدفاع الوطني عندما يتم إدخالها لنظام المعالجة بأية وسيلة إدخال مما تم التطرق له سابقاً، تعتبر بيانات وإذا كان القانون يقيم وزناً للتفرقة الفنية وهي عادة ليست بالبساطة المعروضة سابقاً لأنها مرتبطة بعمليات رياضية معقدة، فستخرج هذه الأسرار في هذه المرحلة من نطاق الحماية الجزائية وسيكون أي سلوك يهدف للحصول عليها أو تعديلها أو تغييرها في مرحلة الإدخال لا يشكل سلوك تجسس إلكتروني؛ لأنه غير منصب على معلومات إلكترونية وإنما عـــلى بيانات إلكترونية، ونفس الشيء لو إعتمد التفرقة بين المعلومات الإلكترونية والبرامج، فكما تم توضيحه فالتعامل مع المعلومات يتم بواسطة البرامج بمعنى القدرة على المساس بهذه المعلومات التي هي أسرار دفاع وطني وذلك عن طريق هذه البرامج أو عن طريق الإعتداء على هذه البرامج ذاتها بواسطة تعديل هذه البرامج أو اصطناع برامج وهمية كما تم شرحه سابقا، وفي حالة التفرقة بين المعلومات والبرامج فسيؤدي هذا أيضا إلى خروج السلوكات التي يكون محلها البرامج من نطاق تطبيق النص الجزائي المتعلق بحماية الدفاع الوطني المستهدف عن طريق المساس بأنظمة المعالجة الآلية للمعطيات؛ وعليه فمسلك المشرع الجزائري من حيث عدم الأخذ بالتفرقة

[1]– الفقرة (ج) من المادة 2 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفنية بين كل من المعلومات والمعطيات والبرامج مسلك سديد، بالرغم من أن التشريعات التي أخذت بذات التفرقة ووضعت تعاريف لكل من المعلومات والبيانات والبرامج لم تُقم وزنا لهذه التفرقة حين تطبيق النص القانوني على الاعتداءات الماسة بها.

مما سبق عرضه يمكن إقتراح التعريف التالي:

المعلومات الإلكترونية هي كل النصوص والتصاميم والأصوات والصور الثابتة والمتحركة والرموز والأرقام وغيرها، وتشمل الصورة التي تكون عليها في مرحلتي الإدخال والمعالجة وهي صورة بيانات (معطيات) إلكترونية، كما تشمل الوسائل المستخدمة في معالجة البيانات وهي البرامج.

وإذا كان سر الدفاع الوطني الإلكتروني يأخذ في البيئة الإلكترونية شكل معلومات إلكترونية فإنه بالتعدي يأخذ الصور التي تأخذها؛ بمعنى أنه قد يكون نصاً، أو تصميماً، أو صوتاً، أو صورةً ثابتةً أو متحركةً، أو رمزاً، أو رقماً، وغيرها، كما يشمل الصورة التي يكون عليها في مرحلتي الإدخال والمعالجة وهي صورة بيانات، كما يشمل الوسائل المستخدمة في معالجته عندما يكون بصورة بيانات وهي البرامج.

ثانيـاً- الطبيعـــة القانونيـــة للمعلومـات الإلكترونيـــة:

بتحول أسرار الدفاع الوطني من الصورة المادية إلى أسرار إلكترونية تأخذ شكل معلومات إلكترونية بصورتها اللامادية؛ فقد أصبحت بهذا الشكل الجديد المحل والهدف الرئيسي لعمليات التجسس الإلكتروني، سواء للدول أو لجماعات الجريمة المنظمة أو للجماعات الإرهابية أو حتى للأفراد؛ وذلك نتيجة للقيمة الاقتصادية العالية التي تمثلها إذ تفوق قيمة الأموال المادية مما جعل البعض يطلق عليها تسمية البترول الرمادي ويقرر وجود سوق سوداء للمعلومات والذي من خلاله يمكن الوصول للمعلومات التجارية و الصناعية والشخصية كما يمكن الوصول للمعلومات العسكرية[1]، ورغم القيمة المالية التي تمثلها هذه المعلومات الإلكترونية إلا أن هذه المعلومات في حالتها المجردة مـــن الوسائـــط المادية تثير عدة مشاكل في تحديد محل الجريمة باعتبارها مجرد إشارات أو نبضات إلكترونية غير مرئية تنساب عبر أجزاء نظام المعالجة الآلية وشبكات الاتصال العالمية بصورة آلية وليست ذات كيان مادي؛ مما خلق مواقف فقهية متباينة في تحديد الطبيعة القانونية لها[2]؛ فظهر بذلك إتجاهان:

---

[1]- ضياء مصطفى عثمان، مرجع سابق، ص. 96.

[2]- رشيدة بوكر، مرجع سابق، ص. 90.

أ- الإتجـــاه الأول:

يرفض أنصار هذا الإتجاه إدراج المعلومات الإلكترونية ضمن القيم المالية التي يمكن الاعتداء عليها، ويرى أنه وفقا للقواعد العامة فإن الأشياء المادية وحدها هي التي تقبل الاستحواذ، ولما كانت المعلومة الإلكترونية ذات طبيعة معنوية ولا يمكن اعتبارها من قبل القيم القابلة للحيازة والاستحواذ إلا في ضوء حقوق الملكية الفكرية لذلك تستبعد المعلومات من مجال السرقة ما لم تكن مسجلة على دعامة مادية[1]، فإذا تم الاستحواذ على هذه الدعامات فلا تثور مشكلة قانونية في تكييف الواقعة على أنها فعل استحواذ على معلومات تهم الدفاع الوطني، وتطبق هنا الفقرة الثانية من المادة 63 من قانون العقوبات المتعلقة بجريمة التجسس التقليدي والتي تنص على "الاستحواذ بأية وسيلة كانت على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها أي دولة أجنبية أو إلى أحد عملائها".

ب- الإتجـــاه الثانـي:

يذهب هذا الإتجاه إلى أن المعلومات الإلكترونية ما هي إلا مجموعة مستحدثة من القيم قابلة للاستحواذ مستقلة عن دعامتها المادية وهذا بإعمال معيار القيمة الاقتصادية للشيء، حيث يعتبر الشيء مالاً ليس بالنظر إلى ما له من كيان مادي ملموس وإنما بالنظر إلى قيمته الاقتصادية وأن القانون الذي يرفض إسباغ صفة المال على شيء له قيمة اقتصادية هو بلا جدال كما قال الفقيه الفرنسي "كاربونيي carbonnier" قانون منفصل تماماً عن الواقع[2]؛ ولهذا يرى أصحاب هذا الإتجاه أنه يكون مقبولاً أن يكون موضوع المال شيئاً غير مادي متى كانت له قيمة اقتصادية ومن ثم فلا مانع من إضفاء وصف المال على المعلومات ومعاملتها على أساس ذلك ما دام أنها تتمتع بقيمة اقتصادية بل إنها ذات قيمة اقتصادية عالية[3].

وعلى الصعيد نفسه ثمة من يقول بأن هناك مال معلوماتي مادي فقط ولا يمكن أن يخرج عن هذه الطبيعة، وهي أدوات الحاسب الآلي مثل وحدة العرض البصري ووحدة الإدخال، وأن هناك من المال المعلوماتي المادي ما يحتوي على مضمون معنوي هو الذي يعطيه القيمة الحقيقية، ومثال هذا المال

[1]- مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة بحثية مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنظم بتاريخ: 23-25 سبتمبر 2012.

[2]- عفيفي كامل عفيفي، مرجع سابق، ص. 130.

[3]- رشيدة بوكر، مرجع سابق، ص. 92.

المعلوماتي المادي الشريط الممغنط أو الذاكرة أو الأسلاك التي تنبعث منها الإشارات، فمن المنطق القول أنه إذا حدثت سرقة، فإنه لا يسرق المال المسجل عليه المعلومة لقيمته هو وإنما يسرق ما هو مسجل عليها من معلومات إلكترونية، هذه الأخيرة يمكن الاستحواذ عليها بتشغيل جهاز قارئ ورؤيتها على الشاشة مترجمة إلى أفكار تنتقل من الجهاز إلى ذهن المتلقي، وطالما أن موضوع الحيازة (أي المعلومات الإلكترونية) غير مادي فإن الحيازة تكون من نفس الطبيعة أي غير مادية (ذهنية)؛ وبالتالي يمكن حيازة المعلومات بواسطة الالتقاط الذهني عن طريق البصر[1] إذا كانت قد ظهرت على الشاشة بشكل مرئي أو بعد وصولها إلى الأذن في صورة صوتية صادرة من الأجهزة، ومن الفقهاء الذين قالوا بهذا الفقيه "M.Devese" بحيث يرى أن الالتقاط الذهني للمعلومات الموجودة على الشاشة يمكن أن يندرج ضمن قانون العقوبات؛ فبقدر ما يعاقب القانون الفاعل الذي يلتقط بطريقة غير مشروعة المعلومات ويقوم بحفظها على دعامة مادية يمكن معاقبة الشخص الذي يقوم بالتقاط المعلومات ولكن يحفظها في ذاكرته، وفي نفس السياق يرى الفقيه "M.Bahnam" أن الالتقاط الذهني بدون وجه حق لمعلومات محفوظة على دعامة مادية يطبق عليه القانون الجنائي حتى ولو لم يتم إنتقال هذه الدعامة، أي حتى لو لم تخرج من حيازته[2].

لقد اعترف المشرع الجزائري بأن المعلومات الإلكترونية تصنف ضمن طائفة الأموال؛ وهذا ما يستنتج من خلال إدراجه للجرائم الماسة أنظمة المعالجة الآلية للمعطيات ضمن الجرائم ضد الأموال في قانون العقوبات، كما يستنتج من النصوص التي تجرم الممارسات الماسة بأنظمة المعالجة الآلية للمعطيات أن المشرع الجزائري قد اعترف كذلك بفكرة الالتقاط الذهني للمعلومات؛ وهذا من خلال تجريمه لفعل حيازة المعطيات المتحصلة من إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وهذا في الفقرة الثانية من المادة 394 مكرر 2 من قانون العقوبات؛ وعليه يمكن القول أن المعلومات الإلكترونية أو أسرار الدفاع الوطني الإلكتروني هي أموال معلوماتية ذات طبيعة معنوية قابلة لأن تكون محلاً للاستحواذ والحيازة والإفشاء والنشر، وكل أنواع الاعتداءات التي يمكن أن تنصب على الأشياء ذات الطبيعة المادية .

[1]– مفتاح بوبكر المطردي، مرجع سابق.

[2]– غنية باطلي، الجريمة الإلكترونية، أطروحة دكتوراه، مرجع سابق، ص. ص. 76–77.

الفـــرع الثانـي: أنـــواع المعلومـات الإلكترونيـــة وخصائصهـا.

أن وجود كم هائل من المعلومات الإلكترونية التي تخص حياة ونشاط الأفراد كما الدول دفع إلى ضرورة تصنيف هذه المعلومات بغرض تحديد الأهم والجدير بالحماية القانونية منها، وكذا تحديد نوع هذه الحماية التي تختلف تبعاً للضرر الذي يمكن أن يترتب عن الاعتداء عليها، ومن جانب آخر لا يكفي مجرد التصنيف هذا للاستفادة من الحماية القانونية، بل يجب أن تتوافر في المعلومات الإلكترونية مجموعة خصائص محددة بإكتمالها تصبح المعلومة محل حماية قانونية؛ وعليه سيتم تناول أنواع المعلومات الإلكترونية وخصائص المعلومات الإلكترونية كل في عنصر مستقل، مع محاولة إسقاط هذه القواعد العامة على المعلومات الإلكترونية التي تحوي سراً من أسرار الدفاع الوطني، وهذا كالآتي:

أولاً- أنـــواع المعلومـــات الإلكترونيـــة:

تبرز بصدد تحديد أنواع المعلومات الإلكترونية عديد التقسيمات تختلف باختلاف الأساس المعتمد عليه في التقسيم، بحسب التفصيل التالي:

أ- تقسيـم المعلومـات الإلكترونية على أساس الجهة التـي تتبعهـا:

تنقسم المعلومات الإلكترونية من حيث الجهة التي تتبعها هذه المعلومات إلى: معلومات خاصة بالأفراد، ومعلومات خاصة بالدولة، هذه الأخيرة تنقسم بدورها إلى: معلومات مباحة، ومعلومات سرية سواء كانت هذه المعلومات السرية أسراراً حقيقية أم مفترضة أم ذات طبيعة خاصة وهذا الصنف تحديداً هو المعني بالحماية القانونية في إطار النصوص التي تجرم التجسس، أما المعلومات الخاصة بالأفراد فهي تخضع من حيث المبدأ لنصوص قانونية غير تلك التي تحكم أسرار الدولة.

ب- تقسيـم المعلومـات الإلكترونيـة على أساس طبيعتهـا:

تنقسم المعلومات الإلكترونية بحسب طبيعتها إلى: معلومات إلكترونية إسمية أو شخصية، ومعلومات إلكترونية موضوعية أو غير شخصية، ويقصد بالأولى المعلومات المرتبطة بالشخص المخاطب بها كإسمه وحالته الاجتماعية وموطنه وصحيفة السوابق القضائية الخاصة به، أما ماعدا ذلك فهي معلومات غير شخصية[1]، هذا النوع من المعلومات الإلكترونية ليست له علاقة مباشرة بالدفاع

[1]- رشيدة بوكر، مرجع سابق، ص. 78.

الوطني ولا يخضع من حيث الأصل لنصوص قانون العقوبات التي تحكم التجسس، ولكن هذه المعلومات قد ترتبط بالدفاع الوطني في حالة ما إذا ارتبطت بمعلومات شخصية لأفراد محل متابعة في أحد جرائم التجسس فنكون هنا بصدد أسرار الدفاع الوطني ذات الطبيعة الخاصة الموضحة سابقاً، وفي هذا الإطار هناك من القوانين من تعتبر المعلومات الإلكترونية الخاصة بالحالة المدنية سراً قومياً، ومنها المشرع المصري الذي نص في قانون الأحوال المدنية رقم 143 لسنة 1994 على اعتبار البيانات أو المعلومات أو الإحصائيات المجمعة التي تشتمل عليها السجلات والدفاتر الإلكترونية أو الحاسبات الآلية أو وسائط التخزين الملحقة سراً قومياً لا يجوز الاطلاع عليه أو نشره إلا لمصلحة قومية أو علمية وبإذن كتابي، وعاقب بالأشغال الشاقة المؤقتة كل من يخترق أو يحاول اختراق سرية هذه المعلومات بأية صورة من الصور، وتكون العقوبة الأشغال المؤبدة إذا وقعت الجريمة في زمن الحرب[1].

ج- تقسيـم المعلومـات الإلكترونية على أساس الصورة التي تظهـر بهـا:

تقسم المعلومات الإلكترونية على أساس الصورة التي تظهر بها إلى: معلومات إلكترونية مشفرة، ومعلومات إلكترونية غير مشفرة، فالمعلومات عبارة نبضات إلكترونية يمكن التقاطها ولحمايتها من مخاطر الاعتداء والاطلاع عليها يجب أن توفر لها الحماية، ويعتبر التشفير أهم وسيلة لذلك؛ إذ يؤدي إلى حجب المعلومات عن الغير ممن ليس لهم الحق في الاطلاع عليها ويجعل الوصول إلى المعلومات المشفرة أصعب بكثير من الوصول إلى المعلومات غير المشفرة، وغني عن البيان أن أسرار الدولة يجب أن تكون مشفرة لضمان حمايتها.

د- تقسيـم المعلومـات الإلكترونيـة على أساس إتاحتهـا وتقييدهـا:

تقسم المعلومات الإلكترونية على أساس إتاحتها وتقييدها إلى: معلومات متاحة، ومعلومات غير متاحة أي مقيدة، ويقصد بالصنف الأول المعلومات التي يتاح للكافة الحصول عليها دون حاجة لإذن شخص معين، أما الصنف الثاني فيشير إلى المعلومات التي لا يمكن الاطلاع عليها إلا من طرف أشخاص معينين[2]، وأسرار الدفاع الوطني تأخذ شكل معلومات إلكترونية مقيدة أي غير متاحة.

---

[1]- محمد محمد صالح الألفي، مرجع سابق، ص. 256.

[2]- غنية باطلي، الجريمة الإلكترونية، أطروحة دكتوراه، مرجع سابق، ص. 55.

هـ- تقسيـم المعلومـات الإلكترونيـة على أساس حركتهـا:

تقسم المعلومات الإلكترونية على أساس حركتها إلى: معلومات متحركة، ومعلومات ساكنة، فالمعلومات الإلكترونية لا تتخذ نفس الوضعية داخل نظام المعالجة الآلية للمعطيات فقد تكون ساكنة داخله أو في حالة حركة من نظام معالجة آلية إلى آخر وذلك عبر شبكة من الشبكات[1]، ومن المعروف أن المعلومات الإلكترونية الساكنة داخل نظام معالجة آلية للمعطيات هي الأكثر أمنا من تلك المتحركة، لأن الاعتداء عليها يقتضي من المعتدي التواجد في المكان الذي يتواجد به الحاسب الآلي وهو أمر صعب؛ وعليه فإن المعلومات الساكنة تحتاج حمايتها إلى إجراءات أمنية محـدودة بينمـا تلك المتحركة التي تنتقل عبر شبكات الاتصال فتحتاج إلى إجراءات أمنية أكبر[2]، والدول رغبة في حماية أسرار دفاعها الوطني تلجأ عادة إلى تخزينها في نظام معالجة آلية منفصل أي غير مرتبط بالشبكة، إلا أن هذا العزل ورغم أنه وسيلة حماية فعالة إلا أنها غير مطلقة، وهذا ما أثبتته قضية فيروس "ستكسنت" السابق إيرادها، كما أن الاعتماد شبه الكلي على أنظمة المعالجة الآلية أدى إلى استخدامها في كل مجالات نشاط الدولة مما منح فرصة للجواسيس للتوصل إلى أسرار الدول عبر الثغرات التي يمكن إيجادها في هذه الأنظمة، والأمثلة الواقعية على هذه الحالات كثيرة.

ثانيـاً- خصائـص المعلومـات الإلكترونيـة:

لتتمتع المعلومات الإلكترونية عامة بالحماية القانونية يستوجب أن تتصف بمجموعة من الخصائص، يمكن إجمالها في العناصر الآتية:

أ- خاصيـة التحـديد:

يُعد التحديد خصيصة أساسية فبانعدامها لا نكون أمام معلومة حقيقية؛ وعليه فالمعلومة ترتبط بالتحديد وجوداً وعدماً وهذا ما يذهب إليه الفقيه "كاتالا catala"؛ بحيث يشير إلى أن المعلومة قبل كل شيء تعبير وصياغة متخصصة من أجل تبليغ رسالة، ويكون هذا التبليغ عن طريق علامات أو إشارات مختارة لكي تحمل الرسالة إلى الغير[3]، أما المعلومة غير المحددة فهي مجرد أخبار يتداولها الجميع دون

---

[1]- رشيدة بوكر، مرجع سابق، ص. 82.

[2]- غنية باطلي، الجريمة الإلكترونية، الدار الجزائرية للنشر والتوزيع، مرجع سابق، ص. 65.

[3]- سليم عبد الله الجبوري، مرجع سابق، ص. 39.

القدرة على تحديد إطارها العام فتخرج بذلك من مجال الحماية القانونية لأنها لا توصل فكرة محددة للمخاطب بها.

ب- خاصيــة السريــة:

وهي الخاصية التي بمقتضاها تكون المعلومة غير قابلة للكشف وللإظهار لغير المرخص لهم بمعرفتها، وهذا يعني بأن النظام المعلوماتي يجب أن يمنع المستخدمين من قراءة معلومة سرية إذا كانوا غير مرخصين ومنع المستخدمين المرخص لهم بالاطلاع على المعلومة من إذاعتها وإفشاءها للغير[1]، فالمعلومة غير السرية هي معلومة مكشوفة ومجال حركتها غير محدد بمجموعة من الأشخاص وتكون قابلة للتداول؛ فلا يمكن الحديث عندئذ عن اعتداء عليها بسرقتها أو الاطلاع عليها بدون وجه حق لأنها بمنأى عن أية حيازة، وتكون المعلومات سرية حينما تكون متواجدة داخل نظام معالجة آلية مغلق لا يمكن الدخول إليه إلا من قبل الأشخاص الذين يملكون صلاحيات الدخول، سواء كان ذلك لكل النظام أو لجزء منه فقط[2]، وللسرية ثلاثة ضوابط:

1- الجـــديــة: والجدية المقصودة هنا هي الجدية النسبية وليست المطلقة؛ لأن المعلومة قد تكون معروفة لعدد قليل من الأشخاص ومع ذلك تبقى محتفظة بطابع السرية[3].

2- أن تكـون للمعلومـة قيمة معتبرة فـي مجالهـا: بمعنى أن تكون المعلومات مهمة وأساسية في المجال الذي تتبعه، سواء كان هذا المجال عسكرياً أو سياسياً أو دبلوماسياً أو اقتصادياً، رغم أن المعلومة قد لا تكون ذات قيمة كبيرة بالنسبة لمجال أو قطاع واحد فقط؛ فالمعلومة الاقتصادية مثلا قد يكون لها أهمية عسكرية، بالإضافة إلى وجود علاقة وثيقة بين سرية وقيمة المعلومات؛ فكلما كان من الصعب الحصول على المعلومات نظراً لكونها سرية زادت قيمتها، وكلما زادت قيمة المعلومات زادت الرغبة في إبقائها سرية ورغبة الجواسيس في الحصول عليها وهكذا.

3- أن تُتخـذ تدابيـر للمحافظة على سرية المعلومـات: فلا يكفي لاعتبار السرية في المعلومات التعامل معها بجدية وأن يكون لها قيمة معتبرة في مجالها، بل لابد من اتخاذ تدابير وإجراءات

---

[1]- Fernand Lone Sang, op. cit, p. 9.

[2]- رشيدة بوكر، مرجع سابق، ص. ص. 83-84.

[3]- ضياء مصطفى عثمان، مرجع سابق، ص. 98.

معقولة من قبل حائزها للمحافظة على سريتها، والمعقولية في اتخاذ الإجراءات تختلف باختلاف طبيعة المعلومات ودرجة أهميتها وقيمتها وحسب نوع النشاط المستخدمة فيه؛ فالإجراءات البسيطة التي يتخذها صاحب مشروع صغير مثل وضع المعلومات في مكان مغلق قد تكون كافية للمحافظة على الأسرار، بينما لا تكفي هذه الإجراءات لحماية أسرار المشروعات الكبيرة أو المنشآت العسكرية التي تحتاج إلى إجراءات أمنية أكثر تعقيداً[1].

ج- خاصيـــة الاستئثـــار:

تعد خاصية الاستئثار بالمعلومة أمراً ضرورياً لتتمتع المعلومة الإلكترونية بالحماية القانونية؛ لأنه في مختلف الجرائم التي تنطوي على اعتداء على الأموال، وباعتبار أن المعلومات تعد مالاً معلوماتياً معنوياً، فإن الفاعل يعتدي على حق يخص الغير على سبيل الاستئثار، ويتوافر للمعلومة هذه الصفة إذا كان الوصول إليها غير مصرح به إلا لأشخاص محددين[2].

إن الخصائص التي تم ذكرها أعلاه تنطبق على أسرار الدفاع الوطني مهما كان شكلها، سواء كان ذلك الشكل تقليدياً متمثلاً في معلومات أو أشياء أو مستندات أو تصميمات، أو كان ذلك الشكل إلكترونياً متمثلاً في نصوص أو تصاميم أو أصوات أو صور ثابتة ومتحركة أو رموز أو أرقام.

[1]-ضياء مصطفى عثمان، مرجع سابق، ص. 99.

[2]- خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص. 60.

خلاصـــة البـــاب الأول

إن التسهيلات التي وفرتها ثورة المعلومات والاتصالات على مستوى توفير الجهد والوقت والدقة في الأداء؛ أدت إلى إنتشار استخدام تقنياتها وتجهيزاتها في معالجة مختلف المسائل وتسهيل مختلف المعاملات خاصة للدولة، وقد أدى اعتماد هذه الأخيرة حتى في معالجة أسرار دفاعها الوطني على أنظمة المعالجة الآلية للمعطيات إلى ظهور صنف جديد من الجرائم التي تستهدف هذه الأسرار؛ بحيث برز التجسس الإلكتروني كنمط مستحدث من التجسس بصفة عامة وكمرحلة من مراحل تطوره التاريخي، ورغم كون التجسس الإلكتروني نوع من أنواع التجسس بصفة عامة بمعنى وجود قواعد مشتركة بينه وبين التجسس التقليدي، إلا أن التجسس الإلكتروني ينفرد بعديد الأحكام التي تشكل ذاتيته كجريمة مستحدثة، ويمكن توضيح ذلك من خلال العناصر الآتية:

1- التجسس الإلكتروني هو كل سلوك يرتكبه أجنبي ويستهدف أنظمة المعالجة الآلية للمعطيات أو يستخدمها كوسيلة ومن شأنه المساس بسر من أسرار الدفاع الوطني التي تتجسد في شكل معلومات إلكترونية بغض النظر عن طبيعة مرتكبه والجهة المستفيدة منه سواء كانت دولة أو مؤسسة أو جماعة إجرامية أو فرداً عادياً، أما التجسس التقليدي فهو كل نشاط يقوم به أجنبي يكون من شأنه انتهاك أو خرق قواعد المحافظة التي تحيط بالأسرار المتعلقة بالدفاع الوطني.

2- التجسس الإلكتروني جريمة من الجرائم الماسة بأمن الدولة الخارجي التي يرتكبها أجنبي، وهو في هذا يتفق مع التجسس التقليدي، لكنه ينفرد عنه بكونه يعتبر أحد الجرائم الإلكترونية، بمعنى أنه يستخدم أنظمة المعالجة الآلية للمعطيات أو يستهدفها، وبأنه أحد تقنيات وأساليب الإرهاب الإلكتروني، وبكونه أيضا أحد أساليب وتقنيات الحرب الإلكترونية.

3- التجسس الإلكتروني من حيث الموضوع له عدة صور تتنوع بحسب المجال ونوع سر الدفاع الوطني المستهدف، فنجد التجسس العسكري والتجسس السياسي والدبلوماسي والتجسس الاقتصادي كأهم نوع من أنواع التجسس في الوقت الراهن، وصور التجسس الإلكتروني هذه من حيث الموضوع هي ذاتها أنواع التجسس التقليدي، لكن التقسيم الذي ينفرد به التجسس الإلكتروني فهو ذلك المبني على أساس الوسيلة، وفي هذا الإطار نجد التجسس عن طريق الحواسيب والأنترنت، والتجسس عن طريق الهواتف النقالة، والتجسس عن طريق الأقمار الصناعية.

4- التجسس الإلكتروني جاء نتيجة لعدة ظروف وأسباب أهمها رغبة الدولة في حفظ أمنها وهو تبرير تقليدي للتجسس بصفة عامة ولا يقتصر على الإلكتروني منه، لكن هذا الأخير يجد أسباب إضافية في الظروف الراهنة؛ فهو يمارس بمبرر مواجهة الإرهاب والتصدي له، وبتغير نمط الحرب والقوة إلى حرب معلوماتية وقوة ناعمة، بالإضافة إلى مراقبة السباق الدولي نحو التسلح ومنع الدول الأخرى من الريادة في هذا المجال، كما جاء التجسس الإلكتروني نتيجة للثورة التكنولوجية والتحول إلى الفضاء الإلكتروني، كما أسهم في تزايد أنشطته ظهور فاعلين جدد يبحثون عن استغلال المعلومة لإنجاح مخططاتهم كما هو الحال بالنسبة للمنظمات الإرهابية، أو بحثاً عن الثروة كما هو الحال بالنسبة لجماعات الجريمة المنظمة، أو بحثاً عن الثروة أو الشهرة أو الانتقام كما هو الحال بالنسبة للأفراد الذين يمارسون التجسس لحسابهم الخاص.

5- التجسس الإلكتروني له آثار تمس الدولة كما تمس الأفراد، وإذا كان النمط التقليدي من التجسس يمس الدولة كما الأفراد إلا أن أبعاد هذا التأثير قد تغيرت؛ بحيث يمس التجسس الإلكتروني بالدولة تحديداً في سيادتها لكن مفهوم هذه الأخيرة تغير نتيجة إلى الانتقال إلى الفضاء الإلكتروني الذي له مفهومه الخاص للإقليم والشعب وحتى السلطة، ومن جهة أخرى فلتجسس الإلكتروني أثره على الحياة الخاصة للأفراد؛ إذ لم يعد هناك شيء يمكن للفرد إخفاءه في ظل التطور الملفت للوسائط الإلكترونية ناهيك عن قيام الأفراد ذواتهم بكشف خصوصياتهم وآراءهم عبر شبكات التواصل تحديداً؛ مما يمنح الفرص لتجميع كم هائل من المعلومات عن التركيبة الاجتماعية للدول وأراء الشعوب وتوجهاتها.

6- التجسس الإلكتروني يستهدف أسرار الدفاع الوطني، هذه الأخيرة هي ذاتها محل التجسس التقليدي بحيث أن جوهرها واحد بالنسبة للطائفتين لكنها تنفرد في حالة التجسس الإلكتروني بالمكان أو المستودع أو الوعاء الجديد الذي يحتويها؛ بحيث تتواجد أسرار الدفاع الوطني في أنظمة المعالجة الآلية للمعطيات وهذا الأخير هو المستهدف بأنشطة التجسس الإلكتروني، بينما يستهدف نشاط التجسس التقليدي أسرار الدفاع الوطني بصورتها الطبيعية الملموسة والمحفوظة في أوعية تخزين مادية.

7- تأخذ أسرار الدفاع الوطني المتواجدة بأنظمة المعالجة الآلية شكل معلومات إلكترونية أي كيانات معنوية غير ملموسة؛ بحيث تشمل هذه الأخيرة النصوص، والتصاميم، والأصوات، والصور ثابتة كانت أو متحركة، والرموز، والأرقام، وغيرها، بينما تأخذ أسرار الدفاع الوطني العادية شكل معلومات، أو مستندات، أو أشياء، أو تصاميم، بمعنى كيانات مادية ملموسة، لكن المحتوى في الحالتين واحد؛ وعليه

فما يمنح سر الدفاع الوطني وصفه الإلكتروني هو شكله والوعاء الجديد الذي يحويه، أما جوهره وموضوعه فيبقى واحداً لا يتغير بتغير نوع التجسس.

البـــاب الثانـــي: الجهـــود الوطنيـــة والجهـــود الدوليـــة لمكافحـــة التجـسس الإلكتـرونـــي.

الفـصل الأول: الجهـود الوطنيـة لمكافحـة التجـسس الإلكترونـي.

الفـصل الثاني: الجهـود الدوليـة لمكافحـة التـجسس الإلكتروني.

البـــاب الثانـــي:

الجهـود الوطنيـة والجهـود الدوليـة لمكافحـة التجـسس الإلكترونـــي.

تُعد ممارسة التجسس واستقصاء الأخبار أقدم النشاطات التي مارسها الإنسان لأسباب متعددة أهمها التحوط لأي مخاطر قد تلحقه، وبظهور التجمعات وبروز الدولة كأرقى كيان بينها وأكثرها تنظيماً وتطوراً؛ تبنت ذات الممارسات بغرض معرفة كل ما يتعلق بالدول الأخرى، وخاصة تلك المعلومات التي تحاول إخفائها وتعتبرها أسراراً لا يجب على غيرها الوصول إليها؛ فكانت الدول بذلك تنظر للتجسس على أنه أحد حقوقها المشروعة بل واجب عليها القيام به حفاظاً على أمنها واستقلالها في مواجهة الدول الأخرى، لكنها في ذات الوقت لا تتردد في اعتباره أخطر الجرائم وأشدها تأثيراً، وفي إقرار أحكام صارمة له، بل وفي كثير من الأحيان استثنائية تخرج عما هو مألوف بالنسبة لطوائف الجرائم الأخرى، وهذا في حالة ما إذا كانت هي المستهدفة به؛ وعليه ارتبط التجسس دوماً ومنذ القدم بوجود أحكام لمكافحته، وإذا كانت الدول لوقت قريب تكرس قوانينها للتصدي للتجسس الممارس من طرف الدول الأخرى فقط فإن الوضع حالياً قد تغير بظهور عوامل جديدة أوجبت ضرورة إعادة النظر في أطر الحماية المرصودة؛ بحيث أدت ثورة المعلومات والاتصالات إلى منح الأفراد ذات قدرات الدول في التجسس وذات الحظوظ في التوصل إلى أسرار الدفاع الوطني الخاصة بهذه الدول؛ إذ بقيام هذه الأخيرة بحفظ أسرارها بشكل إلكتروني تكون قد وفرت فرصاً للوصول إليها بطرائق من ذات الطبيعة؛ خاصة في ظل الإنتشار الواسع للتكنولوجيات التي تتيح هذا، وكذا في ظل تبادل المعارف حول أساليب القيام بالتجسس، لدرجة أن المخترقين وقراصنة الشبكات اليوم يضعون كسر إجراءات الحماية التي تحيط بأسرار الدول والوصول إليها رهاناً للكسب أو حتى تسلية لتمضية الوقت؛ وعليه فبعد أن كانت الدولة في سبيل مكافحتها للتجسس تواجه خصماً واحداً هو الدول الأخرى، أضحت في ظل الظروف الحالية تواجه بالإضافة للدول خصوماً جدد هم الأفراد وجماعات الجريمة المنظمة والمنظمات الإرهابية، وحتى بعض المؤسسات والكيانات التي تعتدي على سرية معلومات الدولة تحت مبررات متعددة، مع ضرورة الإشارة إلى أن الدولة قد تستفيد هي ذاتها من خدمات هذه الأطراف الجديدة في الوصول إلى أسرار الدول الأخرى؛ فتكون بذلك لدراسة ورصد الجهود المبذولة من طرف الدولة الواحدة، أو تلك المبذولة من طرف عديد الدول في إطار التعاون الدولي أهمية كبيرة وواضحة؛ وعليه سيتم تقسيم هذا الباب إلى فصلين: يتناول الفصل الأول بالدراسة الجهود

الوطنية لمكافحة التجسس الإلكتروني، ويتناول الفصل الثاني الجهود الدولية لمكافحة التجسس الإلكتروني.

الفصـــل الأول:

الجهــود الوطنيــة لمكافحــة التجــسس الإلكترونـــي.

يعتبر التجسس أحد الجرائم الخطيرة لكونه اعتداء يمس أمن الدولة الخارجي، بمعنى أنه اعتداء يمس الدولة بصفتها شخصاً من أشخاص القانون الدولي؛ فيشكل بذلك أهم مصادر الخطر التي تهدد وجودها واستقلالها وسيادتها وكيانها في المحيط الدولي؛ لذا كان التصدي للتجسس والمحافظة على الاستقلال الوطني أحد أهم قضايا الدولة الأساسية المنصوص عليها دستورياً؛ بحيث عني الدستور باعتباره أسمي قوانين الدولة بإقرار واجب حماية وصيانة استقلال البلاد وسيادتها وسلامة ترابها ووحدة شعبها وجميع رموز الدولة على كافة المواطنين، كما أقر العقاب الصارم على جميع الجرائم المرتكبة ضد أمن الدولة وعلى رأسها التجسس[1]، وبناءاً على الدستور فقد تم رصد عديد القوانين لغرض تجريم نشاطات التجسس وإقرار أشد العقوبات لها ووضع القواعد الإجرائية الخاصة لمتابعتها؛ وعليه وبغية الإلمام بهذه القوانين المرصودة كجهود لمكافحة جرائم التجسس بصفة عامة، والتجسس الإلكتروني كصنف منها؛ سيتم تقسيم هذا الفصل إلى مبحثين: يتناول المبحث الأول الجهود الوطنية الموضوعية لمكافحة التجسس الإلكتروني، بينما يتناول المبحث الثاني الجهود الوطنية الإجرائية لمكافحة التجسس الإلكتروني.

المبــحث الأول: الجهــود الوطنيــة الموضوعيــة لمكافحــة التجــسس الإلكترونــي.

تشكل القواعد المتعلقة بالتجريم والعقاب أهم القواعد الموضوعية التي تقررها أية دولة لمواجهة الأنشطة التي تمس بها أو تلك التي تمس بالأفراد؛ فهي وسيلتها الأنجع لتحقيق غايات المكافحة، والتجسس لا يخرج عن هذه القاعدة، وفي هذا الإطار يُعد قانون العقوبات الشريعة العامة في التجريم والعقاب؛ بحيث يضمنه المشرع معظم الجرائم، وقد يضيف في نفس القانون تجريم أنشطة مستحدثة لها علاقة بالأنشطة المجرمة التقليدية كما هو شأن التجسس؛ بحيث بالإضافة إلى النصوص القديمة التي تحكم التجسس بصفة عامة ونظراً لتأثير التكنولوج...يات الحديثة على طرق ارتكاب الجرائم التقليدية؛ فقد قام المشرع الجزائري باستحداث مواد جديدة تجرم طائفة من الأفعال الماسة بأنظمة المعالجة الآلية

[1]– تنص المادة 75 من الدستور على: "– يجب على كل مواطن أن يحمي ويصون استقلال البلاد وسيادتها وسلامة ترابها الوطني ووحدة شعبها وجميع رموز الدولة.
– يعاقب القانون بكل صرامة على الخيانة والتجسس والولاء للعدو وعلى جميع الجرائم المرتكبة ضد أمن الدولة".

للمعطيات، ونص فيها على حالة ما إذا كانت هذه الأفعال موجهة لاستهداف الدفاع الوطني؛ مما يجعلنا أمام طائفتين من النصوص نصوص تقليدية تحكم التجسس بصفة عامة، ونصوص مستحدثة جاءت أساساً لمكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات مع تضمنها لحالة المساس بالدفاع الوطني، وكما سبقت الإشارة إليه فإن المشرع الجزائري هنا لا يجرم كل الجرائم الإلكترونية؛ إذ يقتصر تجريمه على تلك الأفعال التي تمس أنظمة المعالجة الآلية للمعطيات بمعنى تلك السلوكات التي يكون هذا النظام هدفاً لها فقط؛ وعليه لا تطبق هذه النصوص على الجرائم التي يكون نظام المعالجة الآلية للمعطيات وسيلة لارتكابها كأصل عام[1]، رغم أن المشرع الجزائري استدرك الأمر في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بحيث نص على أن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تشمل جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية[2]، بمعنى أن المشرع الجزائري يعترف بالمفهوم الكامل للجريمة الإلكترونية ويتخذ عن طريق هذا القانون كل التدابير الإجرائية لمكافحتها لكنه في ذات الوقت وفي إطار قانون العقوبات يجرم فقط جزءاً منها وهي السلوكات التي تستهدف نظام المعالجة، أما السلوكات التي ترتكب بواسطته فإن المشرع هنا تركها عموماً لتندرج ضمن النصوص التقليدية فيه، وهو أمر يستوجب إعادة النظر إذ لا يمكن الاستناد إلى قانون إجرائي بالأساس لتجريم أفعال تندرج ضمن قانون العقوبات، لكن في إطار الوضع الحالي وباعتبار التجسس الإلكتروني جريمة إلكترونية فهي إما أن ترتكب مساساً بأنظمة المعالجة الآلية للمعطيات، وإما أن ترتكب بواسطة هذه الأنظمة والنصوص المستحدثة في قانون العقوبات تتضمن الجزء الأول كقاعدة عامة، الأمر الذي يستوجب دراسة ما إذا كانت النصوص التقليدية التي تحكم التجسس عامة صالحة لأن تطبق على أنشطة التجسس الإلكتروني المرتكبة عن طريق الوسائط الإلكترونية؛ وعليه سيتم تناول كل من النصوص القديمة والنصوص المستحدثة في قانون العقوبات بالدراسة وبالتحليل لاستخلاص القواعد التي تحكم التجسس الإلكتروني؛ ومنه سيقسم هذا المبحث إلى مطلبين: يتناول المطلب الأول الجهود الموضوعية لمكافحة التجسس الإلكتروني في إطار قواعد قانون العقوبات التقليدية،

[1]– يستثنى من هذا الأصل العام حالة حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وهي الجريمة المنصوص عليها في المادة 394مكرر2 من قانون العقوبات.

[2]– الفقرة (أ) من المادة الثانية من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

بينما يتناول المطلب الثاني الجهود الموضوعية لمكافحة التجسس الإلكتروني في إطار قواعد قانون العقوبات المستحدثة.

المطلب الأول: الجهود الموضوعية لمكافحة التجسس الإلكتروني في إطار قواعد قانون العقوبات التقليدية.

قام المشرع الجزائري بتحديد أحكام التجريم والعقاب الخاصة بالتجسس في القسم الأول المعنون بالخيانة والتجسس، وكذا في القسم السادس المتضمن أحكام مختلفة تطبق على كل جرائم أمن الدولة من الفصل الأول الخاص بالجنايات والجنح ضد أمن الدولة من الباب الأول المتضمن الجنايات والجنح ضد الشيء العمومي من الكتاب الثالث المتعلق بالجنايات والجنح وعقوباتها من الجزء الثاني المعنون بالتجريم من قانون العقوبات، بالرغم من وجود بعض الأحكام ذات الصلة بالتجسس في القسم الثاني المتضمن جرائم التعدي الأخرى على الدفاع الوطني أو الاقتصاد الوطني من ذات الفصل السابق إيراده، ويحوي القسم الأول مجموعة نصوص تتضمن الجرائم المعتبرة جرائم تجسس بصفة عامة، وللإحاطة بالإحكام التي تنطبق منها على التجسس الإلكتروني سيتم تقسيم هذا المطلب إلى فرعين: يتناول الفرع الأول أحكام تجريم نشاطات التجسس، ويتناول الفرع الثاني أحكام العقاب على جرائم التجسس.

الفرع الأول: أحكام تجريم نشاطات التجسس.

تتعدد جرائم التجسس التي نص عليها القسم الأول المشار إليه أعلاه من قانون العقوبات؛ إذ تشمل طائفة كبيرة لا يمكن تطبيق أحكام بعضها على التجسس الإلكتروني بالنظر إلى أن ما يميز نشاطات هذا الأخير، كونها ذات طبيعة لا مادية لأنها تتم في بيئة افتراضية؛ لذا لا يمكن تطبيق النصوص التي تتضمن سلوكات تجسس لا يتصور قيامها إلا بصورة مادية فقط عليها، ومن هذا المنظور يمكن تقسيم جرائم التجسس التي تنص عليها القواعد التقليدية لقانون العقوبات إلى طائفتين:

- **الطائفة الأولى:** وتشمل مجموعة الجرائم التي لا تقوم إلا عن طريق سلوك مادي بحت؛ وعليه لا يمكن تطبيق أحكامها على التجسس الإلكتروني، وتتضمن هذه الطائفة الجرائم التالية:

* تسليم قوات جزائرية أو أراض أو مدن أو حصون أو منشآت أو مراكز أو مخازن أو مستودعات حربية أو عتاد أو ذخائر أو مبان أو سفن أو مركبات للملاحة الجوية مملوكة للجزائر أو مخصصة للدفاع عنها إلى دولة أجنبية أو إلى عملائها[1].

* إتلاف أو إفساد سفينة أو سفن أو مركبات للملاحة الجوية أو عتاد أو مؤن أو مبان أو إنشاءات من أي نوع كانت وذلك بقصد الإضرار بالدفاع الوطني أو إدخال عيوب عليها أو التسبب في وقوع حادث وذلك تحقيقاً لنفس القصد[2].

* عرقلة مرور العتاد الحربي[3].

* إتلاف معلومات أو أشياء أو مستندات أو تصميمات سرية بقصد معاونة دولة أجنبية أو ترك الغير يتلفها[4].

- **الطائفـــة الثانيـــة:** وتشمل مجموعة من الجرائم التي لم يحدد فيها المشرع الجزائري طريقة قيام ركنها المادي بل وسع في كثير من المواد من صور ارتكاب هذا السلوك صراحة، بينما هناك مجموعة أخرى من الجرائم يمكن إدراجها ضمن هذه الطائفة يحتمل ارتكاب سلوكها الإجرامي بصورة مادية كما يحتمل ارتكابه بصورة لامادية؛ وعليه يمكن تطبيق هذه النصوص على التجسس الذي يتم عن طريق وسائط إلكترونية، وتتضمن هذه الطائفة الجرائم التالية:

* التخابر مع دولة أجنبية بقصد حملها على القيام بأعمال عدوانية ضد الجزائر[5].

* التخابر مع دولة أجنبية أو مع أحد عملائها بقصد معاونة هذه الدولة في خططها ضد الجزائر[6].

---

[1]- البند الثالث من الفقرة الأولى من المادة 61 من قانون العقوبات.

[2]- البند الرابع من الفقرة الأولى من المادة 61 من نفس القانون.

[3]- البند الثالث من المادة 62 من نفس القانون.

[4]- البند الثالث من المادة 63 من نفس القانون.

[5]- البند الثاني من الفقرة الأولى من المادة 61 من نفس القانون.

[6]- البند الثاني من المادة 62 من نفس القانون.

* تحريض العسكريين أو البحارة على الانضمام إلى دولة أجنبية أو تسهيل السبيل لهم إلى ذلك والقيام بعمليات تجنيد لحساب دولة في حرب مع الجزائر[1].

* المساهمة في مشروع لإضعاف الروح المعنوية للجيش أو للأمة يكون الغرض منه الإضرار بالدفاع الوطني مع علمه بذلك[2].

* تسليم معلومات أو أشياء أو مستندات أو تصميمات يجب أن تحفظ تحت ستار من السرية لمصلحة الدفاع الوطني إلى دولة أجنبية أو أحد عملائها على أية صورة ما وبأية وسيلة كانت[3].

* الاستحواذ بأية وسيلة كانت على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو إلى أحد عملائها[4].

وعليه ستقتصر الدراسة على الجرائم التي تندرج ضمن الطائفة الثانية؛ بحيث سيتم التطرق بداية إلى جريمة التخابر مع دولة أجنبية بصورتيها، ثم التطرق إلى جريمة تحريض العسكريين أو البحارة على الانضمام إلى دولة أجنبية، ثم إلى جريمة القيام بعمليات تجنيد لحساب دولة في حرب مع الجزائر، ثم إلى جريمة إضعاف الروح المعنوية للجيش أو للأمة، ومن ثم إلى جريمة التسليم أو الاستحواذ على أسرار الدفاع الوطني، وهذا في العناصر الآتية:

أولاً- جريمة التخابر مع دولة أجنبية:

تأخذ جريمة التخابر في قانون العقوبات الجزائري صورتين تتفقان في بعض الأحكام وتختلفان في أخرى، وهو ما سيتم توضيحه من خلال التطرق إلى كل جريمة وأركانها كل على حدة:

أ- جريمة التخابر مع دولة أجنبية بقصد حملها على القيام بأعمال عدوانية ضد الجزائر:

تم النص على هذه الجريمة في البند الثاني من الفقرة الأولى من المادة 61 من قانون العقوبات بقولها: "يرتكب جريمة الخيانة ويعاقب بالإعدام كل جزائري وكل عسكري أو بحار في خدمة الجزائر يقوم بأحد الأعمال الآتية: ...2- القيام بالتخابر مع دولة أجنبية بقصد حملها على القيام بأعمال عدوانية ضد

[1]- البند الأول من المادة 62 من قانون العقوبات.

[2]- البند الرابع من المادة 62 من نفس القانون.

[3]- البند الأول من المادة 63 من نفس القانون.

[4]- البند الثاني من المادة 63 من نفس القانون.

الجزائر أو تقديم الوسائل اللازمة لذلك سواء بتسهيل دخول القوات الأجنبية إلى الأرض الجزائرية أو بزعزعة ولاء القوات البرية أو البحرية أو الجوية أو بأية طريقة أخرى"، ومن هذا النص نستنتج أن هذه الجريمة تقوم على ثلاثة أركان هي الركن المفترض والركن المادي والركن المعنوي:

1- الركـــن المفتـــرض: تجدر الإشارة إلى أن كلاً من جريمة الخيانة وجريمة التجسس متطابقان في التجريم والعقاب بحيث نص المشرع عليهما في ذات المواد لكن معيار التفرقة بينهما هي جنسية الفاعل، وقد تم النص على هذا المعيار في المادة 64 من قانون العقوبات بحيث يتغير تكييف ذات الفعل بحسب جنسية مرتكبه فيعتبر خيانة إذا ارتكبه جزائري و يعتبر تجسساً إذا ارتكبه أجنبي[1]، ورغم وضوح المعيار وبساطته إلا أن تطبيقه يطرح بعض الصعوبات؛ فبالنسبة لهذه الجريمة نص المشرع على أنها تعد خيانة إذا ارتكبها جزائري أو عسكري أو بحار في خدمة الجزائر؛ وعليه لتكون تجسساً يجب أن يكون الفاعل أجنبياً باستثناء فئة العسكريين أو البحارة الذين في هم في خدمة الجزائر حتى لو كانوا أجانب، والإشكالية المطروحة هنا ما هو وضع مزدوجي الجنسية، أو الذين سحبت منهم الجنسية أو تنازلوا عنها وحالة عديمي الجنسية؟.

2- الركـــن المـــــادي: تقوم جريمة التخابر مع دولة أجنبية بقصد حملها على القيام بأعمال عدوانية ضد الجزائر على السلوك الإجرامي المتمثل في فعل التخابر، وهنا تجدر الإشارة إلى أن هذا الفعل هو ذاته المشكل للسلوك الإجرامي لجريمة التخابر مع دولة أجنبية أو مع أحد عملائها بقصد معاونتها في خططها ضد الجزائر، ويقصد بالتخابر الاتصال بين شخصين أو كيانين وحصول التفاهم بينهما وهو ذات المقصود بالنسبة لجرائم أمن الدولة؛ إذ يعني في هذا الإطار حصول التفاهم المتبادل بين الجاني وبين الدولة الأجنبية فالتخابر لا يتحقق إلا بوجود الاتفاق أي بتلاقي إرادتين متقابلتين[2]، ومعنى ذلك أنه إذا عرض شخص ما خدماته على دولة أجنبية كان فعله عرضاً فردياً من جانب واحد ويسمى في هذه الحالة سعياً؛ لذا لا تكتفي بعض التشريعات بالنص على التخابر فقط كما فعل المشرع الجزائري بل تنص زيادة عليه على فعل السعي، وعند قيام التفاهم أو الاتفاق على الغرض الإجرامي بين الجاني

[1]- باستثناء الفعل المنصوص عليه في البند الأول ومن الفقرة الأولى من المادة 61 من قانون العقوبات وهو فعل حمل السلاح ضد الجزائر إذ يكيف دائما على أساس أنه خيانة.

[2]- عثمان يحي أحمد أبو مسامح، جريمة التخابر وإجراءات محاكمة مرتكبيها في التشريع الفلسطيني (دراسة تحليلية مقارنة)، مذكرة ماجستير، مقدمة لقسم القانون العام بكلية الشريعة والقانون، الجامعة الإسلامية، غزة، فلسطين، 2014، ص. 7.

والدولة الأجنبية لا عبرة عندئذ بمن حرك الأسباب التي تحققه إذ يستوي أن يكون الجاني هو الذي عرض على ممثل الدولة الأجنبية أو العكس[1]. والاتصال بالدولة الأجنبية يشمل كل أنواع المراسلات والمحادثات والاتصالات، وقد يكون مباشراً يقوم به الشخص نفسه وقد يكون الاتصال عن طريق الوسطاء أو العملاء[2]، ومن الجلي أنه في ظل تكنولوجيا الاتصالات الحديثة وما توفره من وسائط إلكترونية مختلفة أصبح القيام بالتخابر أكثر سهولة.

وحسب ظاهر النص يجب أن يتم التخابر مع الدولة الأجنبية فقط بمعنى أن يكون الاتصال مباشرةً بها أي مع أحد ممثليها والقائمين بشؤونها كوزراء الحكومة أو ممثليها السياسيين أو سائر موظفيها ورجالها المدنيين أو العسكريين، بيد أن الموظفين الرسميين للدولة الأجنبية قلما يقومون هم بأنفسهم بمثل هذا الدور الذي يتنافى وأصول اللياقة في إطار العلاقات الدولية[3]؛ لذا كان على المشرع الجزائري أن لا يحصر الجهة التي يتم الاتصال بها في الموظفين الرسميين للدولة، ومن جهة أخرى يشترط النص أن يكون غرض الجاني من وراء تخابره بالدولة الأجنبية هو حملها على القيام بأعمال عدوانية ضد الجزائر مما يفترض أن العلاقة بين الجزائر وبين هذه الدولة الأجنبية قبل ممارسة الجاني لنشاطه الإجرامي كانت علاقة طبيعية سعى الجاني إلى تحويلها إلى علاقة عدوانية؛ وعليه فمحل الحماية الجنائية هو مصلحة الدولة في المحافظة على العلاقات العادية بينها وبين الدول الأخرى. وإذا كان موضوع الحماية هو المحافظة على الحالة العادية للعلاقات الدولية، فإن هذا النص يحمي هذه العلاقات بالمعنى الموضوعي، فهو لا يحمي روابط الود أو الشعور بالتعاطف بين الجزائر والدولة الأجنبية تلك الروابط التي يكون لها أثر في تقوية التحالف مع هذه الدولة، ولكنها تمنع التخابر معها لتجنب قيامها بأعمال مادية أو موضوعية عدائية، بمعنى أنها تنظر إلى النشاط المادي العدواني للدولة الأجنبية لا إلى شعورها الخفي بالعداء أو عدم الثقة[4]، رغم أن التخابر هنا قد يعاقب عليه بالاستناد إلى نصوص أخرى بحيث لا يمكن

---

[1]– سعد إبراهيم الأعظمي، مرجع سابق، ص. ص. 96– 97.

[2]– عبد القادر الشيخ، شرح قانون العقوبات القسم الخاص (الجرائم الواقعة على أمن الدولة)، منشورات جامعة حلب، مديرية الكتب والمطبوعات الجامعية، سوريا، 2006، ص. 65.

[3]– محمد الفاضل، مرجع سابق، ص. 177.

[4]– عبد المهيمن بكر، مرجع سابق، ص. 64.

ترك الجناة يعكرون صفو العلاقات بين الدول دون عقاب[1]. وليس بلازم أن تتخذ الأعمال العدوانية صورة إعلان الحرب؛ ففي هذا الإطار عرفت محكمة أمن الدولة العليا لمصر العمل العدائي بأنه: كل عمل تتأذى به الوداعة والعلاقة الطيبة بين الدول أو يتضرر به السلم القائم بينها[2]، كالقيام باستعراض بحري أو قطع للعلاقات الدبلوماسية، ولا يشترط لقيام الجريمة أن يتحقق شيء من ذلك فعلاً فيكفي أن تكون تلك هي الغاية التي رمى إليها الجاني[3]. ولا يشترط أيضا لتحقق هذه الجريمة ظرف زمني معين فقد تتم في زمن السلم كما في زمن الحرب.

3- الركـن المعنـــوي: جريمة التخابر جريمة عمدية تتطلب لقيامها ضرورة توافر القصد الجنائي بصورتيه العام والخاص؛ بحيث يجب أن تتجه إرادة الجاني إلى الاتصال بالدولة الأجنبية مهما كانت وسيلة هذا الاتصال مع علمه بأن فعله هذا يشكل جريمة معاقب عليها قانوناً وهو القصد الجنائي العام، أما القصد الجنائي الخاص فيتمثل في إتجاه إرادة الجاني إلى تحقيق نتيجة معينة وهي حمل الدولة الأجنبية التي تم الاتصال معها إلى القيام بأعمال عدوانية ضد الجزائر، أو قصد تقديم الوسائل اللازمة للعدوان، وتعبير وسائل العدوان تعبير واسع النطاق يشمل أي أمر من شأنه أن يساعد الدولة الأجنبية في عدوانها، وقد تضمن البند الثاني من الفقرة الأولى من المادة 61 مثالين، المثال الأول هو تسهيل دخول القوات الأجنبية إلى الأرض الجزائرية، ويتصور هنا أن يقوم الفاعل باستغلال التجهيزات الإلكترونية الحديثة في تصوير الأماكن أو وإرسال الخرائط الدقيقة عنها، والمثال الثاني هو زعزعة ولاء القوات البرية أو البحرية أو الجوية، وقد يتم ذلك بعدة طرق كنشر المقالات الإلكترونية أو بث الشائعات المغرضة والأكاذيب عبر مواقع التواصل الاجتماعي وغيرها من الطرق الإلكترونية، وترك المشرع المجال مفتوحا ليتضمن أي وسيلة أخرى بإمكان الجاني أن يساعد بها الدولة الأجنبية وذلك بصريح العبارة "... أو بأية طريقة أخرى"، ويكفي لقيام الجريمة تحقق أي من القصدين، لكن ما يميزهما أنه يفترض أن تكون العلاقات ودية بين الجزائر والدولة الأجنبية في حالة إتجاه إرادة الجاني إلى حمل هذه الأخيرة على القيام بأعمال عدوانية ضد الجزائر، بينما في الصورة الثانية فتكون الدولة الأجنبية أصلاً تضمر نوايا سيئة

---

[1]- تنص المادة 71 من قانون العقوبات على: "يعاقب بالسجن المؤقت من عشر سنوات إلى عشرين سنة كل من ...(3)- يجري مع عملاء دولة أجنبية مخابرات من شأنها الإضرار بالمركز العسكري أو الدبلوماسي للجزائر أو بمصالحها الإقتصادية الجوهرية"

[2]- عبد الحكم فودة، مرجع سابق، ص. 521.

[3]- عثمان يحي أحمد أبو مسامح، مرجع سابق، ص. 78.

للجزائر وأنها بحاجة إلى اختلاق الذرائع لمباشرة ما تنوي القيام به من عدوان فيتجه قصد الجاني من وراء المخابرات التي يجريها معها إلى تقديم الوسائل اللازمة لذلك العدوان[1].

ب- جريمة التخابر مع دولة أجنبية أو مع أحد عملائها بقصد معاونة هذه الدولة في خططها ضد الجزائر:

تم النص على هذه الجريمة في البند الثاني من المادة 62 من قانون العقوبات بقولها: "يرتكب جريمة الخيانة ويعاقب بالإعدام كل جزائري وكل عسكري أو بحار في خدمة الجزائر يقوم في وقت الحرب بأحد الأعمال الآتية :... 2- القيام بالتخابر مع دولة أجنبية أو مع أحد عملائها بقصد معاونة هذه الدولة في خططها ضد الجزائر"، وانطلاقاً من هذا النص نخلص إلى أن الجريمة تقوم على ثلاثة أركان كسابقتها، وهي:

1- الركن المفترض: لكي تقوم هذه الجريمة لابد بحسب النص من توافر شرطين هما:

- يجب أن يكون الفاعل أجنبياً باستثناء فئة العسكريين والبحارة الذين هم في خدمة الجزائر بحيث يكيف الفعل بالنسبة لهم كخيانة، وفي هذا تشترك هذه الصورة من التخابر مع الصورة الأولى.

- يجب أن تكون هناك حالة حرب للقول بقيام هذه الجريمة وهذا بعكس الجريمة السابقة التي لا يشترط فيها زمن معين فهي ترتكب في السلم كما في الحرب، ويقصد بالحرب وفقا لأحكام القانون الدولي كل نزاع مسلح بين دولتين[2]، فالمقصود بالحرب هنا الحرب الخارجية كما أن حالة الحرب تتضمن في نطاقها إلى جانب الحرب الفعلية أو الحقيقية الفترة التي يوقف فيها القتال نتيجة هدنة[3].

2- الركن المادي: إن السلوك الإجرامي لهذه الجريمة والمتمثل في التخابر أي إجراء الاتصالات بأية طريقة كانت هو ذاته السلوك الإجرامي للجريمة السابقة، والاختلاف بينهما يكمن في الجهة التي يتم معها التخابر؛ بحيث بالإضافة إلى القيام بالتخابر مع الدولة مباشرة بمعنى مع موظفيها وممثليها الرسميين يمكن أن يتم التخابر أيضا مع أحد عملائها أي مع شخص يعمل لمصلحتها، ولا

[1]- محمد عودة الجبور، الجرائم الواقعة على أمن الدولة وجرائم الإرهاب، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص. 136.

[2]- مصطفى مجدي هرجة، مرجع سابق، ص. 8.

[3]- عبد المهيمن بكر، مرجع سابق، ص. 28.

يشترط هنا وجود توكيل رسمي له من هذه الدولة وإنما يكفي أن تدل الظروف والملابسات على أنه يعمل لمصلحتها ولقاضي الموضوع سلطة تقدير هذا[1]، كما يكمن الاختلاف أيضا بين صورتي الجريمة في غرض الجاني من التخابر مع الدولة الأجنبية وهو في هذه الحالة معاونتها في خططها ضد الجزائر، بمعنى أن هذه الدولة في حالة عداء مع الجزائر بعكس الصورة الأولى والجاني هنا يرمي إلى معاونة هذه الدولة المعادية في خططها المرسومة ضد الجزائر، وقد تركت المادة المجال مفتوحاً ليشمل أية صورة من صور المعاونة وبأية طريقة كانت.

3- الركـــن المعنـــوي: جريمة التخابر مع دولة أجنبية بصورتها هذه جريمة عمدية تستوجب لقيامها القصد الجنائي العام، بمعنى إتجاه إرادة الجاني للتخابر مع دولة أجنبية مع علمه بأن ما يقوم به جريمة معاقب عليها قانوناً. كما تتطلب هذه الجريمة القصد الجنائي الخاص؛ بحيث يجب أن تكون غاية الجاني من قيامه بالاتصالات مع الدولة الأجنبية هي معاونتها في خططها ضد الجزائر.

ثانيـاً- جريمـة تحريض العسكريين أو البحـارة على الانضمام إلى دولـة أجنبيـة:

نص المشرع الجزائري على هذه الجريمة في البند الأول من المادة 62 من قانون العقوبات بقوله: "يرتكب جريمة الخيانة ويعاقب بالإعدام كل جزائري وكل عسكري أو بحار في خدمة الجزائر يقوم في وقت الحرب بأحد الأعمال الآتية: 1- تحريض العسكريين أو البحارة على الانضمام إلى دولة أجنبية أو تسهيل السبيل لهم إلى ذلك"؛ ومن خلال هذا النص نستنتج أن جريمة تحريض العسكريين أو البحارة على الانضمام إلى دولة أجنبية تقوم على ثلاثة أركان هي:

أ- الركـــن المفتـــرض: يشترط لقيام هذه الجريمة ضرورة توافر عنصرين:

1- يجب أن يكون الفاعل أجنبياً باستثناء العسكريين أو البحارة الذين هم في خدمة الجزائر فلا عبرة بجنسيتهم إذ يعتبر الفعل بالنسبة إليهم خيانة في كل الأحوال.

2- يجب أن تكون هناك حالة حرب للقول بقيام هذه الجريمة بحسب الشرح السابق.

ب- الركـــن المـــادي: يتحقق السلوك الإجرامي الذي يقوم عليه الركن المادي لهذه الجريمة بتحقق أحد فعلين:

[1]- سعد إبراهيم الأعظمي، مرجع سابق، ص. 100.

1- تحريض العسكريين أو البحارة على الانضمام إلى دولة أجنبية: ويقع فعل التحريض بكل ما من شأنه أن يؤثر على هؤلاء العسكريين أو البحارة لدفعهم إلى الانخراط في صفوف دولة أجنبية، ولم يشر المشرع الجزائري إلى السبل التي يمكن عن طريقها جعل هؤلاء ينضمون إلى دولة أجنبية ولو على سبيل المثال وترك المجال مفتوحاً ليضم كل الطرق التي يمكن استحداثها، وإذا كان التحريض مسبقاً قد يتم بالمخاطبة العادية أو بالمحاضرات العامة أو بواسطة توزيع المنشورات ولصق الإعلانات، فإنه وإن بقي المبدأ نفسه فإن الوسيلة قد تغيرت؛ بحيث يمكن استغلال المزايا التي توفرها الوسائط الإلكترونية الحديثة كالأنترنت والهواتف الذكية في إغراء الجنود للانضمام للدول أخرى عن طريق البريد الإلكتروني، أو الرسائل القصيرة، أو منتديات الحوار، أو مواقع التواصل الاجتماعي.

والسائد فقهاً أن المقصود بالجنود عموماً الجنود العاملون فعلاً أي الذين يباشرون العمل العسكري سواء في البر أو البحر أو الجو، فلا يدخل في معناهم جنود الاحتياط لأنهم لا يقومون بالخدمة فعلاً وإن كانوا قد أُعِدوا للقيام بها عند الاستدعاء[1]. كما يشترط لقيام الجريمة أن يكون التحريض منصباً على تحقيق غرض معين هو دفع العسكريين والبحارة للانضمام لخدمة دولة أجنبية، ولم يشترط المشرع الجزائري أن تكون هذه الدولة في حالة عداء أم لا مع الجزائر، كما لا يشترط تحقق الغرض من التحريض فهو لخطره على مصلحة الدولة جريمة في ذاته وإن خاب أثره.

2- تسهيل السبيل للعسكريين أو البحارة للانضمام إلى دولة أجنبية: ويختلف فعل التسهيل عن فعل التحريض من حيث أن المحرض يعمل على إستمالة العسكريين والبحارة أو إغوائهم بترك الخدمة والانخراط لدى دولة أخرى، أما التسهيل فالمفروض فيه أن هؤلاء قد رغبوا أو صمموا تلقائياً أو بتحريض الغير على الالتحاق بخدمة دولة أجنبية فيقدم لهم الجاني وسائل العون التي من شأنها أن تسهل لهم تحقيق هذا الغرض[2]، ولا يشترط في هذه الصورة أن يتم تسهيل انضمام العسكريين والبحارة لصالح دولة معادية فقد تكون كذلك وقد لا تكون، كما لا يشترط في هذه الصورة أيضا أن يتحقق غرض الجاني فيكفي قيامه بكل ما من شأنه أن يسهل الانضمام لهؤلاء العسكريين والبحارة، كما لم يشترط المشرع أن يتم التسهيل بوسيلة معينة فقد يتم بكل وسيلة مهما كانت، ومثاله أن يتولى الوساطة بين الطرفين عن طريق الاتصالات التي يجريها بالدولة الأجنبية.

---

[1]- عبد المهيمن بكر، مرجع سابق، ص. ص.121- 122.

[2]- نفس المرجع، ص. 122.

ج- الـــركن المعنـــوي: جريمة تحريض العسكريين أو البحارة أو تسهيل السبيل لهم للانضمام إلى دولة أجنبية جريمة عمدية تقوم على عنصري القصد الجنائي العام والقصد الجنائي الخاص؛ بحيث يجب أن تتجه إرادة الجاني إلى القيام بعمل تحريض أو تسهيل مهما كان نوعه مع علمه أنه يقوم بالتحريض أو التسهيل على الانضمام إلى دولة أجنبية، بمعنى علمه أن ما يقوم به من أفعال تشكل جريمة معاقب عليها قانوناً، بالإضافة إلى ضرورة أن تكون غايته من وراء هذه الأفعال هو جعل العسكريين أو البحارة ينظمون إلى دولة أجنبية ولا يهم بعد ذلك إن تحققت غايته أم لم تتحقق.

ثالثـــاً- جريمـة التجنيـد لحســاب دولــة فـي حرب مع الجزائـــر:

نص المشرع الجزائري على هذه الجريمة في البند الأول من المادة 62 من قانون العقوبات وهو ذات البند الذي تضمن جريمة التحريض أعلاه لكن لوجود اختلافات جوهرية استوجب الأمر تخصيص هذا الفعل بعنصر مستقل؛ بحيث تنص هذه المادة على: "يرتكب جريمة الخيانة ويعاقب بالإعدام كل جزائري وكل عسكري أو بحار في خدمة الجزائر يقوم في وقت الحرب بأحد الأعمال الآتية: 1-...القيام بعمليات تجنيد لحساب دولة في حرب مع الجزائر"، وتشترك هذه الجريمة مع جريمة تحريض العسكريين أو البحارة على الانضمام إلى دولة أجنبية في الركن المفترض؛ لذا سيتم تناول كل من الركن المادي والركن المعنوي فقط، وهذا كالآتي:

أ- الركـــن المـــــادي: يتمثل السلوك الإجرامي الذي يقوم عليه الركن المادي لهذه الجريمة في فعل التجنيد، وإذا كان التحريض أو التسهيل كسلوكات يمكن أن تندرج ضمن مفهوم التجنيد، إلا أن ما يميز جريمة التجنيد عن جريمة التحريض والتسهيل أن هذه الأخيرة تستهدف العسكريين أو البحارة بينما التجنيد قد يشمل إضافة إلى العسكريين والبحارة المدنيين[1]، ويقصد بالتجنيد جمع الجند أو الرجال، وهو الاتفاق مع الأشخاص مهما كانت صفتهم على الالتحاق بوصفهم جنوداً أو عمالاً لخدمة العدو سواء بمقابل أو بدونه وسواء كانوا رجالاً أم نساءً، كما لا يشترط ليتم الركن المادي أن يبدأ هؤلاء المجندين الخدمة فعلياً؛ إذ يكفي أن يكونوا جاهزين للقيام بها بمجرد الاستدعاء[2]. وتعتبر وسائل الاتصال الحديثة أهم طرق التجنيد على الإطلاق خاصة عن طريق فتح مواقع متخصصة بهذا الموضوع، ويشترط لقيام

[1]- عبد الله سليمان، مرجع سابق، ص. 27.

[2]- عبد المهيمن بكر، مرجع سابق، ص. ص. 124- 125.

هذه الجريمة أن يتم التجنيد لصالح دولة معادية بمعنى دولة في حالة حرب مع الجزائر[1] بعكس الجريمة السابقة التي لا تشترط هذا لقيامها. والملاحظ أن المشرع يشترط القيام بعدة عمليات تجنيد للقول بقيام الجريمة وهو مسلك منتقد؛ إذ يكفي قيام الفاعل بنشاطات من شأنها أن تقود للتجنيد، كفتح موقع إلكتروني وإغراء الأشخاص بالانضمام إلى دولة معادية بشتى الأساليب، سواء تحقق غرضه أو لم يتحقق، وبغض النظر عن عدد المجندين.

ب- الـــركن المعنـــوي: جريمة التجنيد لصالح دولة في حرب مع الجزائر جريمة عمدية يجب لقيامها توافر القصد الجنائي العام لدى الجاني، بمعنى يجب أن تتجه إرادته إلى القيام بفعل من أفعال التجنيد مع علمه بالظروف التي يقترف فيها جريمته، وبأن ما يقوم به يشكل جريمة معاقب عليها قانوناً، ويكتفي بعض الشُراح بهذا القصد لقيام الجريمة، بينما يذهب جانب آخر إلى استلزام وجود القصد الجنائي الخاص، وهو استهداف الجاني غاية معاونة العدو، واثبات هذه الغاية بسيط لأن علم الجاني بحالة الحرب أثناء قيامه بالتجنيد قرينة على انتوائه مساعدة العدو[2]، وأوافق الرأي الأول، فالجريمة تقوم بمجرد اقتران إرادة الجاني بعلمه بأن ما يقوم به جريمة وبحالة الحرب القائمة ولا يهم غايته في هذا الإطار.

رابعـاً- جريمـة إضعـاف الـروح المعنويـة للجيش أو للأمـــة:

نص المشرع الجزائري على هذه الجريمة في البند الرابع من المادة 62 من قانون العقوبات بقوله: "يرتكب جريمة الخيانة ويعاقب بالإعدام كل جزائري وكل عسكري أو بحار في خدمة الجزائر يقوم وقت الحرب بأحد الأعمال الآتية: 4- المساهمة في مشروع لإضعاف الروح المعنوية للجيش أو للأمة يكون الغرض منه الإضرار بالدفاع الوطني مع علمه بذلك"، وتشترك هذه الجريمة مع الجريمة السابقة في الركن المفترض؛ وعليه سيتم فقط تناول الركن المادي والركن المعنوي.

أ- الـــركن المـــــادي: يتحقق الركن المادي لهذه الجريمة بأي فعل يشارك أو يساهم به الجاني في مشروع لإضعاف الروح المعنوية للجيش أو للأمة، والملاحظ هنا أن النص قد استخدم تعبير"المشروع" وهذا يدل على اشتراطه وجود خطة أو تدبير وهو الأمر الذي يستلزم نوعاً من التنظيم الهادئ للخطة المرسومة كما يستلزم مدة زمنية معينة ، بالإضافة إلى ضرورة أن يكون هناك أكثر من شخص؛ فإذا قام

[1]- تعاقب المادة 76 من قانون العقوبات بالحبس من سنتين إلى عشر سنوات وبغرامة من 10000 إلى 100000 دج كل من يقوم في وقت السلم بتجنيد متطوعين أو مرتزقة لصالح دولة أجنبية في أرض الجزائر.

[2]- عبد المهيمن بكر، مرجع سابق، ص. 129.

الفاعل منفرداً بأي سلوك من شأنه زعزعة أو إضعاف الروح المعنوية للشعب أو الجيش فلا تقع هذه الجريمة [1]، ولا يشترط المشرع هنا نوعاً معيناً من النشاط بل وسع من دائرته ليشمل كل ما من شأنه أن يضعف الروح المعنوية للجيش أو الأمة؛ فيتحقق ذلك باللجوء إلى الدعاية المثيرة أو ما يعرف بحرب الأعصاب أو الحرب النفسية بإذاعة الأخبار أو البيانات أو الإشاعات الكاذبة، كأن يزعم بأن العدو يستخدم الغازات السامة، أو بأن قنبلة قد قتلت ألف شخص مع أن حصيلتها وجود عدد قليل من القتلى[2]، وتعد وسائل الاتصال الإلكترونية الحديثة من أهم الوسائل في الحرب النفسية نظراً لانتشار استخدامها وسرعة نقل المعلومة عبرها وتجاوزها لكل الحدود الجغرافية. ويشترط المشرع أن تتم هذه الأفعال في زمن الحرب لتقع تحت طائلة العقاب المقرر في هذه المادة[3].

ب- الـــركن المعنـــوي: جريمة إضعاف الروح المعنوية للجيش أو الأمة جريمة عمدية يتطلب لقيامها القصد الجنائي العام؛ بحيث يستوجب إتجاه إرادة الجاني إلى القيام بفعل معين مع علمه من جهة بأنه يساهم به في مشروع لإضعاف الروح المعنوية للجيش أو للأمة، وكذا ضرورة علمه من جهة أخرى بأن هذا المشروع الغرض منه الإضرار بالدفاع الوطني وقد ركز المشرع على عنصر العلم هذا صراحة، كما تتطلب الجريمة لقيامها أيضا قصداً جنائياً خاصاً يتمثل في ضرورة أن يستهدف الجاني من خلال مساهمته في مثل هذا المشروع الإضرار بالدفاع الوطني.

خامسـاً- جريمـة التسليـم أو الاستحـواذ على أسـرار الدفاع الوطنـي:

نص المشرع الجزائري على هذه الجريمة في البندين الأول والثاني من المادة 63 من قانون العقوبات بقوله: "يكون مرتكبا للخيانة ويعاقب بالإعدام كل جزائري يقوم:

---

[1]- محمد صبحي نجم، شرح قانون العقوبات الجزائري(القسم الخاص)، ط 6، ديوان المطبوعات الجامعية، الجزائر، 2005، ص. 198.

[2]- عدلي أمير خالد، الجرائم الضارة بالوطن من الداخل والخارج في ضوء المستحدث من قوانين وأحكام النقض والدستور، دار الفكر الجامعي، مصر، 2013، ص. 625.

[3]- تنص المادة 75 من قانون العقوبات على أنه: "يعاقب بالسجن المؤقت من خمس إلى عشر سنوات كل من يساهم وقت السلم في مشروع لإضعاف الروح المعنوية للجيش يكون الغرض منه الإضرار بالدفاع الوطني وهو عالم بذلك".

1- بتسليم معلومات أو أشياء أو مستندات أو تصميمات يجب أن تحفظ تحت ستار من السرية لمصلحة الدفاع الوطني أو الاقتصاد الوطني إلى دولة أجنبية أو أحد عملائها على أية صورة ما وبأية وسيلة كانت.

2- الاستحواذ بأية وسيلة كانت على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو إلى أحد عملائها".

من خلال هذا النص نستخلص الأركان المتطلبة لقيام الجريمة، وهي ثلاثة كالآتي:

أ- **الـــركن المفتـــرض:** يستلزم في فاعل الجريمة أن يكون أجنبياً، وعلى خلاف الجرائم السابقة لم يستثن المشرع الجزائري العسكريين أو البحارة الذين هم في خدمة الجزائر فكل الأجانب في هذه الحالة يعاقبون إذا ما ارتكبوا الأفعال المنصوص عليها في هذه المادة على أساس التجسس.

ب- الـــركن المـــادي: يقوم الركن المادي للجريمة على أحد السلوكين الآتيين:

1- تسليـم أســرار الدفــاع الوطنــي: ويقصد بالتسليم الإعطاء ونقل الحيازة المادية لمحل السر إن كان للسر محل مادي، أو نقل الحيازة المعنوية إن لم يكن للسر حيازة مادية[1]، ويسمى في هذه الحالة إفشاءً، ويقصد به الإفضاء بالسر إلى الغير أو تمكينه من الإطلاع على مضمونه دون نقل وعائه المادي إلى حيازة الغير[2]؛ وعليه ففعل التسليم يتسع ليشمل كل فعل من شأنه جعل الدولة الأجنبية أو أحد عملائها يطلعون على السر، ولا تهم الصورة التي يكون عليها فقد يكون السر عبارة عن كتابة أو رسم أو صورة أو حتى عن طريق تبليغه مشافهة، كما لا تهم الوسيلة التي يتم بها التسليم فقد تتم بالوسائل التقليدية أو بالوسائل الإلكترونية الحديثة كإرسال الوثائق المكتوبة أو التي تحوي صوراً وتصاميم أو خرائط مشفرة عبر البريد الإلكتروني مثلاً، أو حتى عن طريق طبعها على وسائط تخزين إلكترونية يتم قراءتها فيما بعد بواسطة جهاز الحاسوب أو أي جهاز إلكتروني آخر، ولم يشترط المشرع زمناً معيناً لقيام الجريمة إذ يستوي ارتكابها في زمن السلم كما في زمن الحرب، لكنه اشترط أن يكون محل الجريمة معلومات أو أشياء أو مستندات أو تصميمات سرية ومتعلقة بالدفاع الوطني أو الاقتصاد الوطني، ولمحكمة الموضوع

[1]- فريد ولد حسين، جرائم التجسس، مذكرة ماجستير في القانون الجنائي الدولي، مقدمة لمعهد العلوم القانونية الإدارية، المركز الجامعي عباس لغرور، خنشلة، 2010- 2011، ص. 74.

[2]- عدلي أمير خالد، مرجع سابق، ص. 616.

في هذا الشأن تقدير كون الأمور السابقة ذات طبيعة سرية، وكذا تقدير مدى تعلقها بالدفاع الوطني، كما لها في سبيل ذلك الاستئناس برأي من ترى الاستعانة به[1]، كما يشترط المشرع أيضا أن يتم التسليم إلى الدولة الأجنبية سواء كان ذلك التسليم مباشراً أي لأحد موظفيها أو ممثليها الرسميين أو لأحد عملائها.

2- الاستحواذ على أسرار الدفاع الوطني: ويقصد بالاستحواذ الحصول على السر بمعنى الوصول إليه والاطلاع عليه والتمكن من إحرازه معنويا أو ماديا[2]؛ فالالتقاط الذهني للمعلومات من شاشة كومبيوتر وحفظها في الذاكرة عبارة عن إحراز معنوي وتخزينها في وسائط تخزين إلكترونية أو في حاسوب أو هاتف ذكي يعد إحرازاً مادياً، والمشرع في هذا لم يحصر وسائل الاستحواذ أو الحصول على السر فقد تكون بأي وسيلة كانت، فقط يشترط أن يتم الاستحواذ على سر من أسرار الدفاع الوطني بقصد تسليمه إلى دولة أجنبية أو إلى أحد عملائها.

تجب الإشارة هنا إلى أنه بالرغم من حصر المشرع الجزائري للجريمة الإلكترونية في إطار قانون العقوبات في تلك التي يكون نظام المعالجة الآلية هدفاً لها وتغاضى عن تجريم الأفعال التي يكون ذات النظام وسيلة لارتكابها، فإنه قد خرج عن هذه القاعدة حين نصه في المادة 394 مكرر2 على تجريم أفعال الحيازة أو الإفشاء أو النشر أو الإستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم الماسة بنظام المعالجة الآلية؛ وهو بهذا يجعل هذا النظام وسيلة لارتكاب الجريمة الإلكترونية والتجسس الإلكتروني منها؛ وعليه يمكن تطبيق النص التقليدي والنص المستحدث معاً في هذه الجريمة.

ب- الركن المعنوي: جريمة التسليم أو الاستحواذ على أسرار الدفاع الوطني جريمة عمدية تتطلب لقيامها في صورتي التسليم والاستحواذ ضرورة توافر القصد الجنائي العام لدى مرتكبها، بمعنى أن تتجه إرادته إلى التسليم أو الاستحواذ بأي طريقة على أسرار الدفاع الوطني مع علمه بأن ما يقوم به جريمة وإحاطته بكل عناصرها، أما في صورة الاستحواذ فتتطلب إضافة إلى القصد الجنائي العام قصداً جنائياً خاصاً، وهو أن يرمي الجاني من وراء استحواذه على سر من أسرار الدفاع الوطني تسليمه إلى دولة أجنبية أو إلى أحد عملائها، ومهما يكن فإنه في حالة تخلف القصد الجنائي العام والخاص حسب

[1]- أحمد محمود خليل، جرائم أمن الدولة العليا معلقاً عليها بأحكام محكمة النقض المصرية، المكتب الجامعي الحديث، مصر، 2009، ص. 26.

[2]- محمد صبحي نجم، مرجع سابق، ص. 200.

الحالة لا تقوم الجريمة الحالية لكن قد يندرج تجريم ذات الأفعال ضمن نصوص أخرى من قانون العقوبات؛ لأن الأمر يتعلق بأفعال تستهدف محلاً حساساً له صلة مباشرة بأمن الدولة الخارجي هو أسرار الدفاع الوطني ولا يمكن تجاوز تقرير الحماية له بغض النظر عن الظروف التي يقع فيها المساس بهذا المحل[1].

الفـــرع الثانـــي: أحكـــام العقـــاب علـــى جرائـــم التجـــسس.

نص المشرع الجزائري على أغلب أحكام العقاب المتعلقة بجريمة التجسس في القسم السادس من الفصل الأول المتعلق بالجنايات والجنح ضد أمن الدولة، ومن هذه الإحكام ما هو متعلق بالشخص الطبيعي، ومنها ما هو متعلق بالشخص المعنوي؛ وعليه سيتم عرض أحكام العقاب المقررة للشخص الطبيعي أولاً، ثم أحكام العقاب المقررة للشخص المعنوي ثانياً.

أولاً- أحكـــام العقـــاب المقـــررة للشخـــص الطبيعـــي:

قرر المشرع الجزائري على غرار كل التشريعات الأخرى عقوبة الإعدام لمرتكبي الجرائم السابق عرضها؛ وعليه سيتم الاكتفاء في هذا العنصر بدراسة الأحكام المتعلقة بالإعفاء من العقوبة وتخفيفها والأحكام المتعلقة بالإشتراك لأنها تختلف عما هو مقرر لجملة الجرائم العادية، وهذا كما يأتي:

أ- أحكـــام الإعفـــاء والتخفيـــف مـــن العقـــاب: الأصل أن العقاب يعتبر من لوازم التجريم فلا جريمة بلا عقوبة، إلا أن سياسة المشرع ولاعتبارات متعددة اقتضت أن يكون هناك تسامح يصل إلى درجة الإعفاء الكلي من العقاب بتوافر شروط معينة، ولقد أخذت الكثير من التشريعات بهذه السياسة التي ترمي في الأساس إلى تشجيع الأفراد على التبليغ عن الجرائم التي يتم التحضير لها أو تلك التي ساهموا في ارتكابها؛ وهذا بالنظر لكونها جرائم تتسم بالخفاء وتتجرد من المظاهر المادية التي تلفت نظر السلطات بالإضافة إلى كونها جرائم خطيرة يتكيف الكشف عنها بالخدمة الحقيقية للمجتمع[2]، ويصبح الأمر أكثر إلحاحاً بالنسبة لجرائم التجسس كونها تختلف عن بقية الجرائم التي ينص عليها قانون العقوبات وهذا بسبب طبيعتها الخاصة؛ لأنها في الغالب ترتكب من طرف دولة ضد دولة أخرى وتقع

[1]- تضمنت المادة 66 والمادة 67 من قانون العقوبات تجريم أفعال الاستحواذ والإبلاغ وغيرها من الأفعال التي يكون محلها سراً من أسرار الدفاع الوطني بتوافر شروط معينة، لكن البارز فيها أن المشرع الجزائري اشترط أن تتم هذه الأفعال دون قصد التجسس.

[2]- محمد عودة الجبور، مرجع سابق، ص. 64.

على الأسرار المتصلة بالدفاع الوطني والأمن الخارجي للدولة؛ ولهذا فإن المشرع يقبل الخروج على مبدأ عموم العقاب لمن يبادر إلى الإبلاغ عن هذه الجرائم وذلك حتى تتمكن السلطات العامة في الدولة من معرفة الأسرار التي انتهكت وأن تحد بالتالي من الآثار المترتبة على معرفة الدول الأجنبية بتلك الأسرار، فالخطر لا يكمن في انتهاك السر الوطني فقط ولكن أيضاً في جهل السلطات الوطنية بحقيقة حدوث ذلك الانتهاك[1]، وقد يستفيد المبلغ عن جريمة التجسس إما من الإعفاء أو التخفيف في العقوبة وذلك بحسب ظروف معينة تم إيرادها في قانون العقوبات:

1- شـــروط الإعفـــاء مـــن العقـــاب: نص قانون العقوبات على الإعفاء من العقوبة المقررة لكل من يبلغ السلطات الإدارية أو القضائية عن جناية أو جنحة ضد أمن الدولة قبل البدء في تنفيذها أو الشروع فيها[2]، ومن هذا النص تُستخلص شروط الاستفادة من الإعفاء من عقوبة التجسس وهي:

- **المبـــادرة بتبليـــغ السلطـــات الإداريـــة أو القضائيـــة:** بمعنى قيام الشريك بإخبار السلطة الإدارية أو السلطة القضائية بجريمة التجسس التي يتم التحضير لارتكابها، وهذا يفترض أن هذه السلطات تجهل أمر هذه الجريمة، ويجب أن يكون ذلك الإبلاغ مفصلاً ومطابقاً للحقيقة بحيث يؤدي إلى الغرض الذي ينشده المشرع في تمكين السلطات المختصة من أداء مهمتها في تجنب وقوع التجسس، وهذا يعني أن الإبلاغ الذي لا يتضمن تفصيلات الواقعة وبيان ظروفها وأدلتها وتحديد أشخاص مرتكبيها لا يصلح أن يكون سبباً للإعفاء من العقاب، ولا يكفي فقط مجرد الإبلاغ على هذا النحو بل يجب أن يكون المبلغ هو البادئ بإبلاغ تلك السلطات عن الجريمة[3].

- **بجـــب أن يحـــدث التبليـــغ قبـــل تنفيـــذ الجريمـــة أو الشروع فيهـــا:** وقد تعرض هذا الشرط لانتقادات من جانب الفقه بدعوى أنه لا يتفق مع منطق الأشياء؛ إذ كيف يمكن القول بإعفاء شخص من العقوبة في الوقت الذي لم تقع فيه الجريمة أصلاً، غير أن هناك فريقاً من الفقه يرى بأن هذا الشرط لا يحول دون الاستفادة من النص في حالات معينة ومثاله حالة الإبلاغ عن الجريمة الأصلية قبل وقوعها

[1]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 504.

[2]- الفقرة الأولى من المادة 92 من قانون العقوبات.

[3]- محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 225.

وكان المُبلِغ مساهماً في جريمة لم تقع بعد بأن كان عالما بنيات الجاسوس وقدم له إعانة أو مساعدة أو وسيلة للتعيش أو السكنى[1].

2- شروط التخفيف من العقاب: نص قانون العقوبات على حالتين مختلفتين للتخفيف هما:

- **الحالة الأولى:** تخفيض العقوبة درجة واحدة إذا كان الإبلاغ قد حصل بعد إنتهاء التنفيذ أو الشروع فيه لكن قبل بدء المتابعات[2]، وبالرجوع إلى نصوص قانون العقوبات التي تحدد كيفية احتساب التخفيض، وباعتبار أن عقوبة التجسس هي الإعدام؛ تصبح العقوبة بعد التخفيض عشر سنوات سجنا[3].

- **الحالة الثانية:** تخفض العقوبة درجة واحدة بالنسبة للفاعل إذا مكن من القبض على الفاعلين أو الشركاء في نفس الجريمة أو في جرائم أخرى من نفس النوع ونفس الخطورة وذلك بعد بدء المتابعات[4]، وفي هذه الحالة يفترض أن يكون الإبلاغ قد حصل بعد إنتهاء التنفيذ أو الشروع فيه، كما يفترض أنه تم بعد بدء المتابعات بمعنى أن السلطات في هذه الحالة على علم بموضوع الجريمة وباشرت التحقيقات فيها ولكن تعذر عليها الوصول إلى الجناة فيقوم المبلغ هنا بتمكينها من الوصول إليهم والقبض عليهم، أو أن المبلغ قد مكن من القبض على الفاعلين أو الشركاء في جريمة أخرى من نفس الخطورة ومن نفس النوع، بمعنى يجب أن تكون جريمة من جرائم التجسس في هذه الحالة، لكن هنا نكون أمام إحتمالين: إما أن تكون السلطات قد ألقت القبض على كل الجناة وليس من سبيل للمبلغ إلا أن يمكن المبلغ من القبض على جناة آخرين ارتكبوا جريمة من نفس درجة الخطورة، وإما أن لا تكون السلطات قد ألقت القبض على كل الجناة في الجريمة التي شارك فيها المبلغ ولكن المبلغ لا يعرف هوية كل الشركاء معه مما اضطره بغية الحصول على التخفيف أن يقدم المساعدة للسلطات المعنية فقام بتمكينها من القبض على مرتكبي جريمة أخرى من نفس مستوى خطورة جريمة التجسس التي شارك في ارتكابها.

ب- الأحكام المتعلقة بالإشتراك: لم يكتف المشرع الجزائري بما تم تقريره كقاعدة عامة في قانون العقوبات بشأن الإشتراك[5]، ولكنه قام بالمقابل بالنص على حالات محددة يعتبر فاعلها شريكاً

---

[1]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 509.

[2]- الفقرة الثانية من المادة 92 من قانون العقوبات.

[3]- المادة 53 من نفس القانون.

[4]- الفقرة الثالثة من المادة 92 من نفس القانون.

[5]- أنظر المادة 42 من نفس القانون.

ويعاقب بالإعدام نظيرها وهذا في الفقرة الثانية من المادة 91 من قانون العقوبات، رغم أن المتمعن فيها لا يجد أية خصوصية لخصها بنص مستقل بل يمكن إدراجها في نطاق النصوص العامة التي تحكم الإشتراك، وربما لجأ المشرع لهذا المسلك ليس لخصوصية أفعال الاشتراك ذاتها ولكن لخصوصية الجريمة الأصلية وخطورتها على أمن الدولة الخارجي فأراد بذلك أن يحتاط لإمكانية وجود ثغرات تعيق تطبيق القواعد العامة في الإشتراك وللتأكيد على أفعال معينة بالذات، وتطرح هذه المادة عدة نقاط إستفهام عند قراءتها؛ بحيث تنص على أنه: "علاوة على الأشخاص المبينين في المادة 42 يعاقب باعتباره شريكاً من يرتكب دون أن يكون فاعلاً أو شريكاً أحد الأفعال الآتية:

1- تزويد مرتكبي الجنايات والجنح ضد أمن الدولة بالمؤن أو وسائل المعيشة وتهيئة مساكن لهم أو أماكن لاختفائهم أو لتجمعهم وذلك دون أن يكون قد وقع عليه إكراه ومع علمه بنواياهم.

2- حمل مراسلات مرتكبي هذه الجنايات وتلك الجنح وتسهيل الوصول إلى موضوع الجناية أو الجنحة أو إخفائه أو نقله أو توصيله وذلك بأية طريقة كانت مع علمه بذلك".

وأول ما يثير التساؤل في هذه المادة هو مقدمتها إذ تفترض بحسب صياغتها بأن من يقوم بالأفعال المذكورة في هذه المادة بحسب الأصل ليس شريكاً لو تعلقت بجرائم غير جرائم أمن الدولة ولكن هذه الأفعال لا تخرج عن المألوف وعن ما هو منصوص في المادة 42 فهي عبارة عن وسائل مساعدة للفاعلين لارتكاب جرائمهم ويعتبر فاعلها شريكاً بغض النظر عن نوع الجريمة المرتبطة بها، كما توحي ذات الصياغة بأن الأشخاص الذين يقومون بالأفعال المنصوص عليها في هذه المادة لا يقعون ضمن دائرة العقاب؛ لأنه لا تكييف لأفعالهم فتدخل المشرع واعتبرهم شركاء رغم أن الواضح أنهم شركاء دون الحاجة إلى مثل هذا التنصيص، باستثناء حالة إخفاء موضوع الجريمة الوارد النص عليه في البند الثاني فبحسب الأصل يكون فاعلها مرتكباً لجريمة الإخفاء، ولكن لخطورة موضوع الجريمة وهو في حالة التجسس سر من أسرار الدفاع الوطني؛ ارتأى المشرع أن يعتبر فاعلها شريكاً لتشدد عليه العقوبة وتصل الإعدام، بالإضافة إلى أن المشرع قد اعتبر بعض الأفعال الواردة في هذه المادة كأفعال اشتراك في 43 من قانون العقوبات وهي حالة من يقدم مسكناً أو ملجأً أو مكاناً للاجتماع لبعض المجرمين.

ثانياً- أحكام العقاب المقررة للشخص المعنوي:

في مقابل إعتراف المشرع الجزائري بالمسؤولية الجزائية للشخص المعنوي[1] فإنه نص على عدم إمكانية مساءلة هذا الشخص المعنوي عن أي جريمة إلا إذا نص القانون على ذلك صراحة[2]، وفي هذا الإطار أقر المشرع الجزائري صراحة المسؤولية الجنائية للشخص المعنوي عن جرائم التجسس وذلك في المادة 96 مكرر من قانون العقوبات[3] بحسب الشروط العامة المنصوص عليها في المادة 51 مكرر، وهو مسلك صائب فقد أخذت كثير من التشريعات بمبدأ المسؤولية الجنائية للشخص المعنوي لاسيما في نطاق الجرائم الماسة بأمن الدولة بعد أن ثبت على نحو قاطع أن كثير من هذه الأشخاص التي ترمي في الظاهر إلى تحقيق غايات مشروعة قد تكون ستاراً ترتكب من ورائه جرائم خطيرة كالتجسس؛ فالشخص المعنوي يستطيع بإمكانياته الضخمة أن يرتكب الجرائم بصورة أكثر خطراً وضرراً مما لو ارتكبها الأفراد، يضاف إلى ذلك ظهور العديد من الشركات والمؤسسات العالمية التي تخصصت بالفعل في حقل التجسس الدولي عن طريق الأقمار الصناعية التي تملكها[4]، وكذلك المؤسسات العالمية لتصنيع الهواتف النقالة والأجهزة الإلكترونية، وتنقسم العقوبات المقررة للشخص المعنوي عن جريمة التجسس إلى نوعين كالآتي:

أ- **العقوبات الأصلية:** تطبق على الشخص المعنوي عقوبة الغرامة حسب الكيفيات المنصوص عليها في المادة 18 مكرر2 من قانون العقوبات، وبالرجوع إليها نجدها تقرر عقوبة الغرامة المقدرة بمليونيّ (2.000.000) دينار عندما تكون الجناية معاقبا عليها بالإعدام[5].

---

[1]- إعترف المشرع الجزائري بالمسؤولية الجزائية للشخص المعنوي بموجب القانون رقم 04-15 المؤرخ في العاشر نوفمبر من سنة 2004 المعدل والمتمم لقانون العقوبات في المادة 51 مكرر منه

[2]- وهو الشرط الوارد في المادة 51 مكرر من قانون العقوبات التي تنص على: " باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام يكون الشخص المعنوي مسؤولاً جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك".

[3]- تم إضافة هذه المادة بموجب القانون رقم 06-23 المؤرخ في العشرين من ديسمبر سنة 2006 المعدل والمتمم لقانون العقوبات

[4]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 483.

[5]- الفقرة الثانية من المادة 96 مكرر من قانون العقوبات.

ب- العقوبات التكميلية: يتعرض الشخص المعنوي علاوة على عقوبة الغرامة السابقة الذكر لواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 18 مكرر[1]، وهي:

- حل الشخص المعنوي.
- غلق المؤسسة أو فروعها لمدة لا تتجاوز خمس (5) سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (5) سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس (5) سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر وتعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (5) سنوات وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

إن الطبيعة الخاصة لجرائم التجسس من حيث إتسامها بالخفاء وصعوبة الكشف وكذا ارتكابها من قبل أجنبي تجعل من الصعب تطبيق هذه الأحكام سواء بالنسبة للشخص الطبيعي أو بالنسبة للشخص المعنوي.

المطلب الثاني: الجهود الموضوعية لمكافحة التجسس الإلكتروني في إطار قواعد قانون العقوبات المستحدثة.

أدى ظهور الجرائم الإلكترونية كطائفة جديدة من الجرائم المختلفة في الوسيلة والهدف إلى ضرورة مواجهتها بقواعد تتلائم مع خصوصية أنشطتها اللامادية وبيئتها الإفتراضية التي تخرج في كثير من الأحيان عن مجال تطبيق النصوص التقليدية، وإن كان التجسس الإلكتروني كجريمة إلكترونية ماسة بأمن الدولة يخضع في بعض حالاته للنصوص العامة التي تحكم التجسس التقليدي إلا أن هناك من سلوكاته الإجرامية ما لا يمكن إخضاعه لهذه النصوص؛ لذا قام المشرع الجزائري باستحداث نصوص جديدة في

[1]- الفقرة الثالثة من المادة 96 مكرر من قانون العقوبات.

قانون العقوبات ذاته تنص على تجريم الأنشطة الماسة بأنظمة المعالجة الآلية للمعطيات[1]، ونص فيها على حالة استهداف الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الدفاع الوطني وأحال على تطبيق عقوبات أشد إذا اقتضت الحالة ذلك، وباعتبار أن أسرار الدفاع الوطني تعد جوهر ومحور الدفاع الوطني فإن الجرائم المنصوص عليها هنا تعد جرائم تجسس إلكتروني إذا استهدفت هذه الأسرار، لكن الصعوبة لا تثور بشأن عنصر التجريم بقدر ما تتعلق بعنصر العقاب خاصة في ظل غموض المصطلحات التي استخدمها المشرع في هذا الصدد؛ وعليه سيتم تقسيم هذا المطلب إلى فرعين: يتناول الفرع الأول الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات مع إسقاط عناصر الدراسة على الحالة التي تكون فيها معطيات النظام متعلقة بسر من أسرار الدفاع الوطني، بينما يتناول الفرع الثاني العقوبات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات مع عرض إشكالية تطبيق هذه العقوبات في حالة ما إذا كانت هذه الجرائم تستهدف الدفاع الوطني.

الفـــرع الأول: الجرائـم الماســة بأنظمـة المعالجــة الآليــة للمعطيــات.

تضم الجرائم الماسة بأنظمة المعالجة قسمين رئيسيين: الأول يحوي جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات، والثاني يحوي الجرائم المترتبة على جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات، وستتم دراستها كالآتي:

أولاً- جريمـة الدخـول أو البقـاء غير المشروع في نظام المعالجة الآليــة للمعطيــات:

تُعد جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية أو كما تسمى أيضا بجريمة الاختراق الإلكتروني أكثر الجرائم إنتشاراً وخطورة وكذا أهمية؛ لأنها تعبر عن المرحلة التمهيدية لبقية الجرائم الأخرى التي تستهدف المعطيات الموجودة في هذا النظام، وقد نص المشرع الجزائري على جريمة الدخول أو البقاء غير المشروع أو كما عبر عن هذا الأخير بلفظ "عن طريق الغش"، في المادة 394 مكرر بقوله: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

[1]- تم استحداث النصوص التي تجرم الأنشطة الماسة بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04-15 المؤرخ في العاشر من نوفمبر سنة 2004 المعدل والمتمم لقانون العقوبات.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) و الغرامة من 50.000 إلى 150.000 دج ".

وحسب هذا النص يتبين أن لجريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات صورتان: صورة بسيطة تتمثل في مجرد الدخول أو البقاء غير المشروع ونصت عليها الفقرة الأولى، وصورة مشددة تتحقق إذا ما نتج عن الدخول أو البقاء غير المشروع إما حذف أو تغيير في المعطيات أو تخريب لنظام إشتغال المنظومة، ونصت على هذه الصورة كل من الفقرتين الثانية والثالثة، وستتم دراسة كل صورة على حدة كالآتي:

أ- جريمة الدخول أو البقاء غير المشروع في صورتها البسيطة:

تقوم جريمة الدخول أو البقاء غير المشروع في صورتها البسيطة على ركنين يستنتجان من خلال الفقرة الأولى من المادة 394 مكرر كالآتي:

1- الركن المادي: السلوك الإجرامي لجريمة الدخول أو البقاء غير المشروع في صورتها البسيطة نوعان: سلوك إيجابي وسلوك سلبي، فالأول يتمثل في فعل الدخول، والثاني يتمثل في فعل الامتناع عن الخروج من نظام المعالجة الآلية للمعطيات أو البقاء فيه في الوقت الذي كان من المفروض عليه المغادرة[1]:

- **المقصود بفعل الدخول غير المشروع (الدخول عن طريق الغش):** يعرف هذا الفعل بأنه: عملية ولوج غير شرعي إلى نظام التشغيل في الحاسب من قبل أشخاص لا يملكون سماحيات الدخول وذلك بهدف القيام بأعمال غير قانونية مثل التجسس أو السرقة أو التخريب، أو أنه الولوج إلى المعلومات داخل نطاق الاختراق الذي يحدث للنظام المعلوماتي بأكمله أو لجزء منه أياً كان سواء كان جزءاً مادياً أو برامج جزئية أو مجرد بيانات مخزنة في نظام التنصيب عن طريق التوصل إلى الأرقام أو الكلمات أو الشفرات أو الحروف أو المعلومات السرية[2]، وهذا التعريف الأخير يعد الأشمل لحالات انتهاك نظام المعالجة الآلية؛ بحيث يتضمن كل عناصر هذا النظام وكذا مراحل الاختراق تبعاً لها، وقد تم التطرق

[1]- غنية باطلي، الجريمة الإلكترونية، أطروحة دكتوراه، مرجع سابق، ص. 138.

[2]- رشيدة بوكر، مرجع سابق، ص. ص. 178- 179.

سابقاً بنوع من التفصيل إلى أن النظام المعلوماتي له عناصر مادية كوحدات الإدخال والمعالجة والإخراج، وأن عملية الدخول والتجسس قد تتم على مستوى أي من هذه العناصر المادية وتستهدف أسرار الدفاع الوطني التي تأخذ شكل معلومات إلكترونية، هذه الأخيرة تتسع لتشمل إضافة إلى المعلومات بالمفهوم الفني البرامج و البيانات، وهي أي المعلومات والبيانات والبرامج تكون العناصر المعنوية للنظام، وتشكل العناصر المادية والعناصر المعنوية بالإضافة إلى وسائل الاتصالات أو الشبكات نظام المعالجة الآلية للمعطيات الذي يمثل بدوره محل هذه الجريمة، ولا يشترط تبعاً لما سبق ليتحقق الدخول أن يكون في كل النظام بل حتى لجزء منه فقط، ويجب النظر هنا إلى الدخول كظاهرة معنوية تشابه تلك التي نعرفها عندما نتكلم عن الدخول إلى فكر أو إلى ملكة التفكير لدى الإنسان أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة[1]، ووفقا لهذا التصور المعنوي لفكرة الدخول فإنه يتحقق بأي طريقة والمشرع أحسن فعلاً حينما لم يحدد طرق الدخول ولم يعط حتى مجرد أمثلة عنها باعتبار تعدد وسائل الاختراق وتطورها المستمر، وعلى كل فإن الدخول قد يتم بطريقة مباشرة عن طريق نظام المعالجة الآلية الذي يحتوي على المعلومات وهذا باستعمال الرمز السري أو كلمة المرور الصحيحة أو القيام بإدخال برنامج التجسس في نظام المعالجة مباشرة باليد[2]، إلا أن هذه الطريقة من النادر أن تنجح لسبب بسيط هو عدم القدرة على الوصول المادي إلى أنظمة المعالجة الآلية التي تحوي أسرار الدفاع لوجودها في أماكن تتمتع بتقنيات حماية عالية الكفاءة إلا إذا افترضنا وجود متعاونين من المستخدمين الداخليين أنفسهم كما كان الشأن بالنسبة لقضية المفاعل النووي الإيراني، وقد يتم الدخول بطريقة غير مباشرة عندما يصل الفاعل إلى المعلومات أو النظام عن طريق نظام آخر يتصل بالأول بواسطة شبكة الاتصالات، وهو الإحتمال الأقوى فجُل المخاطر مصدرها الشبكة، وتقنيات الدخول إلى النظام هنا متعددة ومتغيرة باستمرار ولقد تم التطرق لبعضها سابقا، ومنها تقنية أبواب المصيدة وتقنية لوحة المفاتيح، بالإضافة إلى استخدام برنامج لكسر الشفرات، أو برنامج لزرع فيروس تجسس معين، أو عن طريق التقاط أو اعتراض الموجات الكهربائية المنبعثة عن نظم المعالجة الآلية أثناء اشتغالها بواسطة استخدام وسائل فنية معينة ثم إعادة بناء تلك الموجات أو الذبذبات للحصول على معلومات واضحة ومفهومة، وتعتبر هذه التقنية من أهم التقنيات المستخدمة في التجسس المعلوماتي ورغم أن هناك من التشريعات من تعتبر الاعتراض جريمة

[1]– علي عبد القادر القهوجي، مرجع سابق، ص. 131.

[2]– غنية باطلي، الجريمة الإلكترونية، الدار الجزائرية للنشر والتوزيع، مرجع سابق، ص. 152.

مستقلة عن الدخول إلا أن الراجح فقهاً أن هذا الفعل يندرج ضمن جريمة الدخول غير المشروع وهو مسلك المشرع الجزائري. ولم يشترط المشرع صفة معينة في الشخص ليكون جانياً وبالتالي تقع الجريمة من أي شخص مهما كانت صفته، وإنما يكفي أن يكون من أولئك الذين ليس لهم حق أو تصريح بالدخول إلى هذا النظام[1]، لكنه تجاوزه مخالفاً بذلك إرادة صاحب حق السيطرة على النظام الذي يعرف بأنه كل شخص طبيعي أو معنوي أو سلطة عامة أو كل مؤسسة أو جهاز يكون له سلطة التصرف في نظام الحاسب الآلي التابع له وتقرير مضمونه أو محتواه وكيفية تنظيمه والهدف منه[2].

- **المقصود بفعل البقاء غير المشروع (البقاء عن طريق الغش):** يعرف البقاء غير المشروع بأنه: التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام[3]، أو بأنه: التواجد من قبل الجاني داخل نظام المعالجة الآلية والتجول بين الملفات والمجلدات والبيانات والمعلومات والانتقال من جزء إلى جزء آخر داخل النظام وبصفة مستمرة، أو بأنه: فعل الاتصال بعد أن توافر للشخص العلم بكونه نظاماً ممنوعاً عليه الدخول إليه وإتجاه إرادته إلى الإبقاء على هذا الاتصال الذي حدث بطريق الخطأ[4]، ومن هذه التعاريف يمكن القول أن البقاء المعاقب عليه داخل النظام قد يتحقق مستقلاً عن فعل الدخول إلى النظام وقد يجتمع معه ويكون البقاء معاقباً عليه استقلالاً، حين يكون الدخول غير مجرم، ومثاله إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو فيكون من الواجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فوراً فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع فقط، وقد يجتمع الدخول إلى النظام والبقاء غير المشروع معاً وذلك في الفرض الذي لا يكون فيه للجاني حق الدخول إلى النظام لكنه يدخل إليه فعلاً ضد إرادة من له حق السيطرة عليه ثم يبقى في النظام[5] ليحقق أغراضه وهي إحتمالات واردة جداً في حالة ارتكاب التجسس؛ فقد يدخل الفاعل صدفة إلى نظام المعالجة الآلية الممنوع عليه الدخول إليه وهي حالة من يشغل برامج معلوماتية لأغراض معينة لكن قد يُدخل أوامر عن طريق الخطأ والصدفة فيجد نفسه قد

---

[1]- رشيدة بوكر، مرجع سابق، ص. 190.

[2]- غنية باطلي، أطروحة دكتوراه، مرجع سابق، ص. 141.

[3]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار النهضة العربية، مصر، 2009، ص. 360.

[4] - رشيدة بوكر، مرجع سابق، ص . 213 .

[5]- علي عبد القادر القهوجي، مرجع سابق، ص. 133.

توصل إلى الدخول إلى نظام ممنوع ولكن بدل أن يخرج يستمر في التجوال في النظام مما يتيح له الإطلاع على معلومات حساسة، أو قد يعلم أصلاً بتحريم الدخول إلى أنظمة معينة ورغم ذلك يقوم باستغلال مختلف التقنيات لذلك وهو بالأصل يقوم بالدخول لغرض البقاء والبحث عن المعلومات التي يريد، والفرق بين الاحتمالين أن الجاني في الحالة الأولى غالباً ما يكون من الهواة المدفوعين بباعث حب المغامرة بعكس الثاني الذي يعتبر في الغالب من المجرمين المحترفين وتقوم الجريمة في كل الحالات فلا عبرة هنا بالباعث، وفي هذا الفرض الأخير نكون بصدد تحقق الاجتماع المادي للجرائم بين جريمتي الدخول والبقاء وهنا ثار الخلاف الفقهي حول تحديد متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء؛ فيذهب البعض إلى تحديد اللحظة بالوقت الذي يعلم فيه المتدخل أن بقاءه في النظام غير مشروع وهو أمر يصعب إثباته، بينما يذهب البعض إلى تحديد العلم منذ اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع ومع ذلك يظل داخل النظام[1]، وهذا يفترض وجود أجهزة إنذار تقوم بهذه المهمة وهو متطلب فني متوفر عند المؤسسات الكبيرة فقط، وهناك رأي يعتبر أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام فإذا دخل وظل ساكناً تظل الجريمة جريمة دخول إلى النظام أما إذا بدء في التجول فإن جريمة البقاء داخل النظام تبدأ منذ تلك اللحظة[2]، ويمكن تحديد هذا بوسائل الحماية الفنية، وكلا الرأيين الأخيرين صائب. ومحل جريمة البقاء غير المشروع هو ذاته محل جريمة الدخول غير المشروع أي نظام المعالجة الآلية بكل عناصره المادية والمعنوية وشبكات الاتصال؛ وعليه كما في جريمة الدخول غير المشروع يستوي أن يكون البقاء قد تم في كل نظام المعالجة الآلية أو في جزء منه فقط كما نصت المادة 394 مكرر في فقرتها الأولى.

وجريمة الدخول غير المشروع جريمة شكلية لا يلزم لقيامها تحقق نتيجة معينة[3]، فلا يهم أن يكون الجاني قد تحصل على سر من أسرار الدفاع الوطني، ونفس الشيء بالنسبة لجريمة البقاء غير المشروع فهي مجرمة لذاتها وبغض النظر عن النتائج سواء ترتب عن بقاء الجاني في النظام والتجوال فيه إعتداء مهما كان نوعه على سر الدفاع الوطني.

---

[1]– محمد أمين الشوابكة، مرجع سابق، ص. 25.

[2]– علي عبد القادر القهوجي، مرجع سابق، ص. 134.

[3]– جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة (الجرائم الناشئة عن استخدام الحاسب الآلي)، دار النهضة العربية، مصر، 1996، ص. 150.

المشرع الجزائري لم يكتف بتجريم الدخول أو البقاء غير المشروعين في نظام المعالجة الآلية بل تجاوز ذلك إلى تجريم مجرد المحاولة وذلك حسب العبارة الواردة في نص المادة السابقة بالقول: "... أو يحاول ذلك"، غير أن ما يمكن إثارته هنا هو صعوبة الإثبات[1]، فإن كان من الممكن تصور وجود محاولة للدخول من خلال محاولة تخطي الإجراءات الفنية التي توضع لغرض منع الإختراقات فالأمر يبدو صعباً للغاية بالنسبة للبقاء بحيث لا يمكن تصور وجود محاولة للبقاء، فإما أن يكون هناك بقاء أو لا يكون فعلى المشرع هنا مراجعة مصطلحاته.

2- الـــركن المعنـــوي: جريمة الدخول أو البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات في صورتها البسيطة جريمة عمدية ركنها المعنوي القصد الجنائي العام الذي يتطلب اتجاه إرادة الجاني إلى ارتكاب الجريمة مع علمه بعناصرها، بمعنى علمه بأنه يدخل إلى نظام معالجة خاص بالغير، أو أنه يتجول فيه دون أن يكون له الحق في ذلك أي ليس له حق الدخول أو البقاء فيه، ويستدل على توافر سوء النية لدى الجاني إذا كان دخوله إلى النظام جاء نتيجة إختراقه لجهاز الأمن الذي يحمي هذا النظام أو عن طريق توصله إلى كلمة السر أو الشيفرة ودخل بها إلى النظام[2]، أو عن طريق استخدامه لتجهيزات تقنية وفنية مخصصة لأغراض الاختراق.

ب- جريمـة الدخـول أو البقـــاء غير المشـروع في صورتها المشـــددة:

تصبح جريمة الدخول أو البقاء غير المشروع جريمة مشددة وتضاعف تبعاً لذلك عقوبتها إذا ترتب عنها إحدى النتيجتين الآتيتين:

- **النتيجـة الأولـى: حـذف أو تغييـر معطيـات النظـام:** وتم النص عليها في الفقرة الثانية من المادة 394 مكرر، ومصطلح الحذف يشير إلى إزالة المعلومات الموجودة داخل نظام المعالجة وهو أقصى أنواع الضرر، أما مصطلح التغيير فيشير إلى إحداث تعديلات فحسب على المعطيات دون أن يصل الأمر إلى حد إزالتها بحيث تظل المعلومة موجودة ولكن بدون معنى أو فائدة أو لها معنى ولكنه مغاير للمعنى الأصلي الذي كانت عليه قبل هذا الفعل[3].

---

[1]- زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011، ص. 51.

[2]- جميل عبد الباقي الصغير، مرجع سابق، ص. 151.

[3]- رشيدة بوكر، مرجع سابق، ص. 231.

- **النتيجة الثانية: تخريب نظام إشتغال المنظومة:** وتم النص عليها في الفقرة الثالثة من المادة 394 مكرر، ويقصد بالتخريب كل فعل من شأنه إعاقة أو إفساد نظام التشغيل، وتتحقق الإعاقة بكل سلوك يتسبب في تباطؤ أو إرباك عمل نظام المعالجة، ويتحقق الإفساد أو التعييب بجعل النظام غير قادر على الاستعمال السليم وذلك بأن يُعطي نتائج غير تلك التي كان من الواجب الحصول عليها، ولا يشترط أن تكون الإعاقة أو الإفساد بصورة كلية بل يمكن أن يؤدي النشاط إلى إعاقة أو إفساد جزئي للنظام[1]، ومن أفضل الأساليب المستخدمة لتخريب نظام اشتغال المنظومة برامج الدودة، وهي عبارة عن برامج تستهدف جزءاً محدداً من نظام المعالجة الآلية للمعطيات وهو الجزء الخاص بنظام التشغيل، بحيث تقوم بإصدار معلومات غير صحيحة تؤدي في النهاية إلى تعطيل وإيقاف النظام المعلوماتي بصورة كاملة[2].

إن النتيجة المترتبة على جريمة الدخول أو البقاء غير المشروع والتي تعتبر ظرف تشديد هي نتيجة غير عمدية وغير مقصودة حيث لم تتجه نية الفاعل إلى الإضرار بنظام التشغيل أو بمعطياته فهذه النتيجة وقعت على سبيل الخطأ غير العمدي والذي يتخذ صورة الإهمال أو عدم الإحتراز أو الرعونة؛ وعليه فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة القصدية الأساسية وهي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره إلا إذا اثبت الجاني إنتفاء تلك العلاقة[3] كأن يثبت أن الحذف أو التغيير في المعطيات أو التخريب في نظام اشتغال المنظومة لم يكن بسبب دخوله أو بقاءه غير المشروع وإنما كان بسبب فعل خارجي من طرف آخر.

إن النتيجتين السابقتين جاءتا غير مقصودتين أي عن طريق الخطأ أما لو قصد الجاني إحداثهما فنكون بصدد جريمة الإعتداء العمدي على المعطيات المجرمة بموجب المادة 394 مكرر1 فيما يتعلق بفعلي التعديل والإزالة، أما الفعل المتمثل في تخريب نظام اشتغال المنظومة فلم ينص المشرع الجزائري عليها كجريمة عمدية وهي ثغرة قانونية على المشرع الجزائري سدها وذلك بتجريمها كما فعل المشرع الفرنسي في المادة 2/323 من قانون العقوبات الفرنسي.

---

[1]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، مرجع سابق، ص. ص. 372- 374.

[2]- نهلا عبد القادر المومني، مرجع سابق، ص. 131.

[3]- علي عبد القادر القهوجي، مرجع سابق، ص. 137.

ثانيـاً- الجرائـم المترتبة على جريمـة الدخول أو البقاء غيـر المشـروع في نظام المعالجة الآلية للمعطيـات:

يترتب على الدخول أو البقاء غير المشروع في نظام المعالجة الآلية سلوكات إجرامية أخرى تمس أساساً بالمعطيات التي يحويها هذا النظام، وبالرجوع إلى ما نص عليه المشرع الجزائري يمكن إجمال هذه السلوكات في قسمين: يحوي الأول جريمة الإعتداء على المعطيات، والثاني مجموعة نشاطات تتمحور حول التعامل غير المشروع في المعطيات، وسيتم تناول كل منهما في عنصر مستقل كالآتي:

أ- جريمـة الإعتـداء علـى المعطيـات:

نص المشرع الجزائري على هذه الجريمة في المادة 394 مكرر1 من قانون العقوبات بقوله: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"، وانطلاقا من هذه المادة نستنتج الأركان التي تقوم علها الجريمة وهي:

1- الـركن المـــادي: تقوم جريمة الإعتداء على المعطيات بارتكاب الجاني لأحد الأفعال الثلاثة الآتية:

- **فعـل الإدخـــال:** يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية أو كان يوجد عليها معطيات من قبل، وقد يتم الفعل بإدخال معطيات وهمية إلى النظام المعلوماتي[1] أو بإدخال معطيات صحيحة ولكن من شأنها التشويش على المعطيات الموجودة قبلاً في النظام، كما يشمل فعل إدخال المعطيات إدراج برنامج ما والذي هو عبارة عن تعليمات بلغة ما توجه إلى كيان الحاسوب بغرض الوصول إلى نتيجة معينة هي بمثابة هدف الجاني، وتعتبر مرحلة إدخال البيانات أو البرامج أو المعطيات الجديدة كما سماها المشرع الجزائري أهم المراحل في الجريمة الإلكترونية فهي تمهد لمرحلة أخطر وهي مرحلة استغلال البيانات[2] سواء بتعديلها أو إزالتها، ولا يمكن الفصل هنا بين إدخال المعطيات أو البيانات وإدخال البرامج؛ لأن الجاني قد يستخدم لغرض إدخال المعطيات برامج معينة أو أنه يقوم مباشرة بإدخال برنامج معين كبرنامج تجسس أو برنامج لفيروس هدفه إزالة أو تعديل ما

[1]- غنية باطلي، الجريمة الإلكترونية، أطروحة دكتوراه، مرجع سابق، ص. 161.

[2]- زيدان زيبحة، مرجع سابق، ص. 54.

يوجد أصلاً من معطيات أي بغرض القيام بالسلوكات الإجرامية اللاحقة، لكن المشرع إعتبر إدخال مثل هذا البرنامج إدخالا لمعطيات في نظام المعالجة، ومن التطبيقات القضائية في هذا الشأن أنه قضي في فرنسا بأنه يقع تحت طائلة نص المادة 323-3 من قانون العقوبات والتي تقابلها المادة 349 مكرر 1 من قانون العقوبات الجزائري تعمد إدخال فيروس في برنامج الغير وكذا الإمتناع عن إخبار هذا الأخير بإدخال مثل هذا الفيروس ولو حصل ذلك بصفة عرضية[1].

- **فعـــل الإزالـــــة:** وتستخدم عديد المصطلحات للتعبير عنه كالتدمير والمحو والإتلاف والطمس، ويقصد بفعل الإزالة عموماً محو جزء من المعطيات المسجلة على الدعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[2]، وانطلاقاً من هذا التعريف فإزالة المعطيات قد تكون بصفة جزئية أو بصفة كلية من الدعامة الموجودة في النظام، ولا يقصد بتحطيم هذه الدعامة التحطيم المادي لأن هذا يدخل في إطار النصوص التقليدية التي تحكم الإتلاف المادي، لكن المقصود هنا التحطيم أو الإتلاف المعنوي، ومثاله في هذه الحالة إتلاف القرص الصلب للحاسوب عن طريق فيروس خاص لهذا الغرض، كما يقصد بالإزالة أيضا عملية نقل المعطيات وتخزينها في منطقة من الذاكرة؛ فكما هو معروف فوحدة الذاكرة الموجودة في وحدة المعالجة المركزية لها أقسام فيقوم الجاني بنقل المعطيات وتخزينها في الملائم منها.

- **فعـــل التعديـــل:** يقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، ويتحقق التعديل كما الإزالة عن طريق العديد من البرامج الضارة أهمها الفيروسات والقنابل الزمنية والمنطقية[3].

ومحل النشاطات الجرمية السابقة يقتصر على المعطيات الموجودة داخل النظام فقط أما التي لم تدخل النظام أو عولجت وانفصلت عنه فتخرج من نطاق الحماية المقرر بموجب هذه المادة، وهو ما يثير التساؤل حول وضعية المعلومات المخزنة على دعامات إلكترونية ففي حالة كون هذه المعلومات تخص الدفاع الوطني هل إتلافها يبقى بدون متابعة؟ وإن تم الاتفاق على أن إتلاف مثل هذه الدعامات هو

[1]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص (الجرائم ضد الأشخاص والجرائم ضد الأموال)، ط 7، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، ص. 446.

[2]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، مرجع سابق، ص. 383.

[3]- هشام محمد فريد رستم، مرجع سابق، ص. 158.

إتلاف مادي فهل يمكن تطبيق النص التقليدي الذي يحكم إتلاف أسرار الدفاع الوطني عليها؟ بالرجوع إلى البند الثالث من المادة 63 من قانون العقوبات التي تنص على: "إتلاف مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد معاونة دولة أجنبية أو ترك الغير يتلفها" نجد أنها حددت أشكال سر الدفاع الوطني في المعلومات والأشياء والمستندات والتصميمات فبحسب الظاهر من النص لا حماية لهذه الأسرار نفسها لو كانت مخزنة على دعامة إلكترونية رغم أن لها ذات الأهمية كالأولى لكن بالرجوع إلى البند الأول من نفس المادة نجد المشرع قد وسع من الأشكال التي يمكن أن تكون عليها هذه الأسرار بقوله: "... معلومات أو أشياء أو مستندات أو تصميمات ... على أية صورة ما وبأية وسيلة كانت"؛ نستخلص أن المشرع الجزائري قد إعترف بوجود أوعية أخرى يمكن أن تحوي الأسرار ولم يعط مثالاً عليها بل ترك النص مفتوحاً ليشمل كل التطورات، لكن حتى وإن سلمنا بهذا فهناك إشكالية أخرى تطرح نفسها بحيث أن الهدف من تجريم إتلاف الأوعية التي تحوي أسرار الدفاع الوطني مهما كانت هو المحافظة على هذه الأسرار من الزوال والفقدان النهائي لكن في حالة وجود سر الدفاع الوطني على دعامة إلكترونية فإن تحطيم هذه الدعامة لا يؤدي إلى فقدان وزوال السر؛ لأنه من الممكن جداً أن توجد نسخ أخرى من هذه الدعامة بالإضافة إلى تخزين نسخ أخرى في نظام المعالجة الآلية.

2- الـــركن المعنـــوي: جريمة الإعتداء على معطيات نظام المعالجة الآلية جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي العام، بمعنى ضرورة أن تتجه إرادة الجاني إلى ارتكاب واحد أو أكثر من السلوكات الإجرامية المكونة للركن المادي وهي الإدخال والإزالة والتعديل مع علمه بأن هذه السلوكات تشكل جريمة الإعتداء على معطيات نظام معالجة آلية تابع للغير، والقصد الجنائي العام كاف لقيام الجريمة؛ إذ لا يتطلب وجود نية أو غاية خاصة لدى الجاني بإلحاق الضرر بالجهة صاحبة النظام.

ب- جرائـم التعامـل غيـر المشـروع فـي المعطيـات:

نص المشرع الجزائري على السلوكات التي تشكل هذه الجرائم في المادة 394 مكرر2 من قانون العقوبات بقوله: "يعاقب بالحبس من شهرين (2) إلى ثلاثة (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمداً وعن طريق الغش بما يلي:

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

يتبين أن المشرع الجزائري يحاول من خلال سنه لهذا النص أن يضع مجموعة من التدابير الوقائية لحصر نطاق الجرائم الماسة بأنظمة المعالجة الآلية والحد من أثارها ومخلفاتها من خلال تجريمه لكل النشاطات التي تهدف إلى توفير وسائل ارتكاب هذه الجرائم من جهة، وتجريم كل النشاطات التي تهدف إلى استغلال منتوج هذه الجرائم من جهة أخرى، وهو ما سيتم تناوله فيما يلي:

1- جريمة التعامل غير المشروع في معطيات صالحة لارتكاب جرائم المساس بأنظمة المعالجة الآلية:

تقوم هذه الجريمة على ركنين يستخلصان من الفقرة الأولى للمادة 394 مكرر 2 المذكورة أعلاه وهما:

- **الركن المادي:** يقوم الركن المادي لهذه الجريمة على توافر واحد أو أكثر من السلوكات الإجرامية الآتية:

* **التصميم:** يقصد به إعداد برامج وتقنيات صالحة لارتكاب الجريمة، ويقوم بهذا الفعل في الأغلب المتخصصون أو الذين لديهم قدرات فنية في تصميم المعطيات والبرامج، ومثاله تصميم البرامج الخبيثة[1] كبرامج الفيروسات والقنابل المنطقية والزمنية أو برامج الاختراق والتجسس المعلوماتي.

* **البحث:** إن تعبير البحث تعبير مرن وله دلالات متعددة فقد يشير إلى البحث عن المعطيات التي يمكن أن ترتكب بها الجريمة أو يشير إلى البحث في كيفية تصميم برامج لارتكاب الجريمة، والبحث بالمفهوم الأول قد يقوم به كل الناس خاصةً في ظل ما تقدمة شبكة الأنترنت ومحركات البحث فيها من خيارات الوصول للمعلومة المطلوبة حتى لو كانت غير مشروعة ومن هذا المنطلق لا يمكن متابعة الجميع بجرم البحث؛ لذا فإن المقصود بالبحث هنا هو ذلك الذي ينصب على كيفية تصميم البرامج وتطويرها وإعداد نسخ مستحدثة منها.

[1]- غنية باطلي، الجريمة الإلكترونية، الدار الجزائرية للنشر والتوزيع، ص. 187.

* **التجميع:** يقصد به القيام بجمع قدر كبير من المعلومات التي تشكل خطراً كبيراً والتي من الممكن أن ترتكب بها إحدى جرائم الإعتداء على نظم المعالجة الآلية، ولعل استخدام المشرع لهذا المصطلح بصيغة الجمع له ما يبرره؛ ذلك أن تعدد المعلومات من شأنه أن يركز أو يرفع من درجة الخطورة التي تشكلها، فما من شك أن هناك فرق بين من يحوز على المعلومة وبين من يسعى إلى تجميعها[1]، ونلاحظ هنا أن المشرع أراد أن يحتاط لنشاط البحث المنظم والمحترف والمنصب على موضوع محدد الذي يقوم به أفراد معينون فالبحث في هذه الحالة يدخل في نطاق التجميع وليس في نطاق البحث بمفهومه السابق.

* **التوفير:** يشير هذا المصطلح إلى عرض المعلومات وإتاحتها وجعلها في متناول الغير، ومن قبيل ذلك كلمة المرور وشفرة الدخول أو أية بيانات مشابهة تسمح بالولوج لكل أو جزء من نظام المعالجة، ويشمل كذلك الكشف أو الإفشاء العلني للثغرات الأمنية في النظام، والتوفير بهذا المعنى يختلف نطاقه من حيث الأشخاص عن التجميع؛ فهذا الأخير لا تتعدى فيه عملية حيازة المعلومات والتصرف فيها القائم بها بينما في التوفير فإن الأشخاص الذين سيحصلون على المعلومات ويتصرفون فيها تتعدى دائرتهم ذلك الشخص وتتسع لغيره[2].

* **النشر:** يقصد به إعلام وإذاعة المعطيات وتمكين الغير من الاطلاع عليها، ويتم بمختلف الوسائل بحيث يمتد ليشمل كل نشاط من شأنه نقل البيانات للآخرين[3] وتوسيع دائرة العالمين بها، وربما الفرق بين التوفير والنشر يكمن في إتساع دائرة الأشخاص الذين يمكنهم أن يعرفوا بهذه المعطيات؛ فالتوفير ينحصر في عدد معين من الأفراد قد يكونون مثلاً فريقاً من المخترقين ومعروف تبادل مثل هؤلاء لما يتوصلون إليه، أما النشر فلا يشترط فيه وجود روابط معينة بين الأشخاص بحيث يتم جعل المعطيات متاحة للجميع وبدون ضوابط معينة.

* **الإتجار:** ويشمل أي تصرف من شأنه توفير عائد أو منفعة مادية نظير تقديم المعطيات للغير كالإنتاج والبيع والاستيراد والتصدير.

---

[1]– رشيدة بوكر، مرجع سابق، ص. 281.

[2]– نفس المرجع، ص. 283.

[3]– غنية باطلي، الجريمة الإلكترونية، أطروحة دكتوراه، مرجع سابق، ص. 176.

والملاحظ في هذه الجريمة أن المشرع الجزائري قد توسع في محلها مقارنة بالجرائم السابقة؛ فهي تشمل كل أنواع المعطيات ومهما كانت الصورة الموجودة عليها سواء كانت مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، فتشمل مثلا تحميل برامج يمكن أن تستخدم في ارتكاب الجريمة على دعامة إلكترونية فهذه الدعامة مستقلة عن نظام المعالجة لكن المشرع شملها بالتجريم، ويذهب المشرع الفرنسي إلى أبعد من هذا بحيث لم يقصر محل الجريمة على المعطيات فقط بل أيضا التجهيزات أو الأدوات التي تكون معدة ومصممة لارتكاب واحدة أو أكثر من الجرائم الماسة بأنظمة المعالجة الآلية.

تجدر الإشارة في هذا الإطار إلى أن المشرع الجزائري قد قام بسن المرسوم التنفيذي رقم 09-410 المؤرخ في العاشر ديسمبر من سنة 2009 الذي يحدد قواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة، ويقصد بهذه الأخيرة كل عتاد يمس استعماله غير المشروع بالأمن الوطني وبالنظام العام[1]، وقد قام هذا المرسوم بتحديد قائمة هذه التجهيزات في الملحق الأول منه وجعلها قابلة للتحين بقرار مشترك بين الوزراء المكلفين بالدفاع الوطني والداخلية والنقل وتكنولوجيات الإعلام والاتصال[2]، ومن أمثلتها تجهيزات الاتصالات المستعملة لإرسال الصورة أو الصوت أو الفيديو أو المعطيات عبر القمر الصناعي وأنظمة المتوقع عن طريق القمر الصناعي التي تعمل عبر شبكات الهاتف النقال وكذلك التجهيزات والبرامج المعلوماتية للترميز، واعتبر أيضا البطاقات المسبقة والمؤجلة الدفع كتجهيزات حساسة[3]، وأخضع ذات المرسوم كل أنشطة الاتجار والاقتناء والحيازة والاستعمال المنصبة على هذه التجهيزات للشروط المحددة فيه وكذا لنصوصه التطبيقية[4]، ورغم أهمية هذا المرسوم وسده لثغرة عدم نص المشرع الجزائري في قانون العقوبات على مثل هذه التجهيزات إلا أن ذلك لا يُغني المشرع عن ضرورة أن يذكرها صراحة في صلب المادة 394 مكرر 2 ومن ثم يحيل على المرسوم أعلاه لتبينها.

---

[1]- الفقرة الأولى من المادة الثانية من المرسوم التنفيذي رقم 09-410 المؤرخ في العاشر ديسمبر من سنة 2009 يحدد قواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة.

[2]- الفقرة الثانية من نفس المرسوم التنفيذي.

[3]- القسم أ من الملحق الأول للمرسوم التنفيذي رقم 09-410 المحدد لقواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة.

[4]- المادة الثالثة من نفس المرسوم التنفيذي.

- **الـــركن المعنـــوي:** جريمة التعامل غير المشروع في معطيات صالحة لارتكاب جرائم المساس بأنظمة المعالجة الآلية جريمة عمدية تتطلب لقيامها توافر القصد الجنائي العام، بمعنى إتجاه إرادة الجاني إلى ارتكاب واحد أو أكثر من نشاطات التصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مع علمه بأن نشاطه يشكل جريمة تعامل غير مشروع في معطيات يمكن أن ترتكب بها جريمة ماسة بأنظمة المعالجة الآلية، كما يتطلب لقيام الجريمة القصد الجنائي الخاص والمتمثل في استهدافه من وراء السلوكات السابقة الإعداد أو التمهيد لاستعمال المعطيات المترتبة عنها في ارتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية، وبهذا يستثني من يقوم بإعداد هذه المعطيات أو التمهيد لاستعمالها في أغراض مشروعة كالأغراض العلمية أو أغراض الحماية الفنية لنظام معلوماتي.

2- جريمـة التعامـل غيـر المشـروع في معطيات متحصل عليها من جرائم المساس بأنظمـة المعالجـة الآليـة:

تقوم هذه الجريمة على ركنين يستخلصان من الفقرة الثانية للمادة 394 مكرر 2 المذكورة أعلاه وهما:

- **الـــركن المـــادي:** يقوم الركن المادي لهذه الجريمة على توافر واحد أو أكثر من السلوكات الإجرامية الآتية:

* **الـحيـــازة:** تعرف الحيازة بأنها سيطرة واقعية وإرادية للحائز على المنقول تخوله الانتفاع به، تعديل كيانه، تحطيمه أو نقله، وباعتبارها مركزاً واقعياً فهي لهذا السبب قد تكون مشروعة تستند إلى سبب صحيح قانونا كما قد تكون غير مشروعة كما هو الحال هنا؛ إذ تتعلق الحيازة بمعطيات متحصل عليها من إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ولا تقوم الحيازة إلا بسيطرة الحائز على المعطيات، ويقصد بذلك استطاعة التأثير عليها تأثيراً يتفاوت حجمه تبعاً لنوع الحيازة إذ قد تكون السيطرة مطلقة يستطيع معها الحائز أن يفني المعلومات أو يعدل فيها أو ينتفع بها أو يستعملها أو يوجهها، كما قد تكون هذه السيطرة من الناحية الواقعية محدودة تمكنه فقط من استغلال المعطيات على وجه معين، ولا تكفي مجرد السيطرة على المعطيات للقول بوجودها، بل يجب أن تكون هذه السيطرة إرادية أي مقترنة بنية إحتباس المعطيات، وهذا لا يتحقق إذا كان تمتع الحائز بسلطاته على المعطيات لم يكن إلا أمراً عرضياً

أوجدته المصادفة أو تم بنية عدم التكرار؛ لأنه يلزم أن تكون سيطرة الشخص على المعطيات مقترنة بنية احتباسها واستمرار احتباسها أبداً أو لمدة مؤقتة[1]، وهذه الشروط تنطبق في حالة حيازة معطيات حساسة متعلقة بأسرار الدفاع الوطني فسيطرة الجاني عليها قد تكون مطلقة أي يمكنه حتى أن يتلفها ويفنيها أو يستعملها في الحصول على معلومات أخرى أو لارتكاب جريمة أخرى، كما قد تكون سيطرته عليها محدودة تقتصر على إخضاعها لعمليات تهيئة لإرسالها للجهة المطلوبة، أما فيما يخص نية الإحتباس فالأمر هنا فيه بعض الخصوصية وإن كان يتبع الشروط العامة السابق ذكرها؛ إذ أن الجاني حائز السر إنما يحتبسه لديه لحساب طرف آخر قد يكون دولة عميل لها أو أية جهة أخرى تدفع مقابلاً للحصول على هذا السر.

* **الإفشـــاء:** تتمتع أنظمة المعالجة الآلية للمعطيات بقدرة تخزين هائلة للمعطيات سواء المتعلقة بالأفراد أو الدولة؛ مما ضاعف من إمكانية الحصول عليها عن طريق اختراق هذه الأنظمة ومن ثم إفشاءها لأغراض مختلفة، وقد تم التطرق لذات السلوك حين دراسة جريمة تسليم أسرار الدفاع الوطني في القواعد التقليدية التي تحكم التجسس وتمت الإشارة حينها إلى أن مصطلح التسليم يشمل الإفشاء والإذاعة؛ وعليه فالإفشاء في هذا الإطار يحمل مدلول التسليم والإذاعة وكل ما من شأنه التعبير عن نقل المعلومة إلى طرف معين.

* **النشـــر:** يأخذ هذا المصطلح ذات معنى مصطلح النشر الوارد في الجريمة السابقة الفرق بينهما يكمن في المحل الذي ينصب عليه هذا الفعل، ففي حين انصب في الحالة السابقة على المعطيات الصالحة لارتكاب جرائم المساس بأنظمة المعالجة الآلية، ينصب في هذه الحالة على المعطيات المتحصلة من هذه الجرائم، ولم يحدد المشرع الجزائري طريقة معينة للنشر فقد يكون بطريقة إلكترونية أو بطريقة تقليدية كالكتابة مثلا.

* **الاستعمـــال:** يعتبر الاستعمال أخطر سلوك يمكن أن يقع على المعطيات المحصل عليها من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ومثاله استعمال دولة معينة لأسرار التصنيع النووي لدولة أخرى والمتحصل عليها من اختراق منظومتها المعلوماتية في تطوير برنامجها الخاص، لكن إذا كان من السهل اكتشاف وإثبات مثل هذا الفعل بالنسبة للجرائم التي تستهدف الأفراد فإن احتمال اكتشاف

[1]– رشيدة بوكر، مرجع سابق، ص. ص. 285– 286.

ذات الفعل أو إثباته في حالة أسرار الدفاع الوطني للدول المتحصلة من الجرائم الإلكترونية شبه مستحيل؛ على اعتبار صعوبة اكتشاف الجريمة الأصلية المترتب عليها المعطيات المستعملة ابتداء.

ولم يشترط المشرع الجزائري ضرورة وجود ضرر لتقوم الجريمة؛ فيكفي في ذلك إتيان الجاني لأحد الأفعال السابقة لتقوم الجريمة.

- **الـــركن المعنـــوي:** جريمة التعامل غير المشروع في معطيات متحصلة من الجرائم الماسة بأنظمة المعالجة الآلية جريمة عمدية تقوم على توافر القصد الجنائي العام فقط لدى مرتكبها، بمعنى إتجاه إرادته إلى القيام بأحد السلوكات الإجرامية المتمثلة في حيازة أو إفشاء أو نشر أو استعمال معطيات مع علمه بأنها معطيات غير مشروعة لأنها متحصلة من إحدى الجرائم الماسة بأنظمة المعالجة الآلية.

وتجدر الإشارة هنا إلى أن المشرع الجزائري وبغرض الحد من آثار جرائم التعامل غير المشروع في المعطيات سواء كانت هذه المعطيات صالحة لارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات أو كانت متحصل عليها من هذه الجرائم؛ قد قام بموجب القانون رقم 16- 02 المؤرخ في 19 يونيو سنة 2016 المتمم لقانون العقوبات باستحداث المادة 394 مكرر 8 والتي تجرم وتعاقب إمتناع مقدمي خدمات الأنترنت رغم إعذارهم من قبل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أو رغم صدور أمر أو حكم قضائي يلزمهم بذلك، عن القيام بالتدخل الفوري لسحب أو تخزين المحتويات التي تشكل جرائم منصوص عليها قانونا أو لجعل الدخول إليها غير ممكن، كما تجرم امتناعهم عن القيام بوضع ترتيبات تقنية تسمح بذلك، إذ من شأن هذه المادة أن تدفع مقدمي خدمات الأنترنت إلى المساهمة المؤكدة في مواجهة الجرائم الإلكترونية كافة ومنها جريمة التجسس الإلكتروني خاصة؛ بحيث تحد من إمكانية التعامل غير المشروع في تلك المعطيات التي تمكن من ارتكاب التجسس الإلكتروني وذلك من خلال منع تجميعها أو توفيرها أو نشرها أو الاتجار فيها كما هو الحال بالنسبة لتقنيات وبرامج الاختراق الإلكتروني، كما تحد من إمكانية التعامل غير المشروع في معطيات متحصلة من التجسس الإلكتروني وهي في هذه الحالة عبارة عن أسرار دفاع وطني عن طريق منع نشرها أو إفشاءها ومن ثم منع إمكانية استعمالها[1].

[1]- راجع بخصوص نص المادة 394 مكرر8 من قانون العقوبات ، ما ورد في هامش الصفحة 66 من هذه الرسالة.

الفـــرع الثانـــي: العقوبـات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيـات.

إذا كانت عملية تحديد العقوبات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في حالتها العادية لا تطرح إشكاليات؛ بإعتبار أن النصوص القانونية السابق إدراجها قد تضمنتها صراحة، فإن الإشكاليات تطرح بصدد تطبيق هذه العقوبات في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المستهدفة للدفاع الوطني؛ ولتوضيح أبعاد هذه الإشكالية يستوجب بدايةً تحديد العقوبات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في الأحوال العادية، ثم التطرق لإشكالية تطبيق هذه العقوبات في حالة استهداف الدفاع الوطني، وهذا في العنصرين الآتيين.

أولاً- تحديـد العقوبـات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيـات:

سيتم بدايةً التطرق إلى العقوبات المقررة للشخص الطبيعي، ثم العقوبات المقررة للشخص المعنوي كالآتي:

أ- **العقوبـات المقـررة للشخـص الطبيعـي:** تنقسم العقوبات المقررة للشخص الطبيعي إلى عقوبات أصلية، وعقوبات تكميلية:

1- **العقوبـات الأصليـــة:** تختلف العقوبات الأصلية باختلاف الجريمة لكنها تضم في كل الحالات الحبس والغرامة، وهذا على التحديد الآتي:

- **العقوبـة المقررة لجريمـة الدخول أو البقاء غير المشروع في نظـام معالجـة آليـة للمعطيـات:** تختلف العقوبة المقررة لهذه الجريمة تبعاً لصورتها؛ بحيث يعاقب على الجريمة في صورتها البسيطة أي على الدخول أو البقاء المجرد الذي لا يترتب عنه أي ضرر بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج[1]، بينما تضاعف العقوبة على الجريمة في صورتها المشددة فتصبح في حالة ما إذا ترتب عن الجريمة حذف أو تغيير لمعطيات المنظومة[2] الحبس من ستة أشهر إلى سنتين و الغرامة من 100.000 دج إلى 200.000 دج، وتصبح في حالة ما إذا ترتب عن الجريمة تخريب نظام اشتغال المنظومة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى

[1]- الفقرة الأولى من المادة 394 مكرر من قانون العقوبات.

[2]- الفقرة الثانية من المادة 394 مكرر من نفس القانون.

150.000 دج[1]، وتضاعف كل هذه العقوبات سواء للجريمة في صورتها البسيطة أو المشددة في حالة ما إذا استهدفت هذه الجرائم الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام[2]، فتصبح في صورة الجريمة البسيطة الحبس من ستة أشهر إلى سنتين والغرامة من 100.000 دج إلى 200.000 دج، وتصبح العقوبة في صورة الجريمة المشددة إذا ترتب عنها حذف أو تغيير لمعطيات المنظومة الخاصة بالدفاع الوطني أو بالهيئات والمؤسسات الخاضعة للقانون العام الحبس من سنة إلى أربعة سنوات والغرامة من 200.000 دج إلى 400.000 دج، وإذا ترتب عن الجريمة تخريب نظام اشتغال المنظومة الخاصة بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام فالعقوبة تكون الحبس من سنة إلى أربعة سنوات والغرامة من 100.000 دج إلى 300.000 دج.

- **العقوبة المقررة لجريمة الاعتداء على المعطيات:** يعاقب فاعل هذه الجريمة بالحبس من ستة أشهر إلى ثلاثة سنوات وبالغرامة من 500.000 دج إلى 2.000.000 دج[3]، وتضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام فتصبح الحبس من سنة إلى ستة سنوات والغرامة من 1.000.000 دج إلى 4.000.000 دج.

- **العقوبة المقررة لجرائم التعامل غير المشروع في المعطيات:** يعاقب فاعل هذه الجرائم بغض النظر عن صورها المحددة سابقاً بالحبس من شهرين إلى ثلاث سنوات وبالغرامة من 1.000.000 دج إلى 5.000.000 دج، وتضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام فتصبح الحبس من أربعة أشهر إلى ستة سنوات والغرامة من 2.000.000 دج إلى 10.000.000 دج.

2- العقوبات التكميلية: قد تكون العقوبات التكميلية المنصوص عليها إلزامية أو إختيارية، وتتمثل العقوبات التكميلية الإلزامية التي يجب على القاضي الحكم بها في حالة ارتكاب إحدى الجرائم السابق في مصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة، وكذا في إغلاق المواقع التي تكون محلاً لهذه الجرائم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت

[1]- الفقرة الثالثة من المادة 394 مكرر من قانون العقوبات.

[2]- المادة 394 مكرر3 من نفس القانون.

[3]- المادة 394 مكرر1 من نفس القانون.

بعلم مالكها، وهاتين العقوبتين تطبقان مع احترام حقوق الغير حسن النية[1]، أما العقوبات الإختيارية فهي تلك العقوبات المنصوص عليها في المادة التاسعة من قانون العقوبات بحيث يجوز للقاضي الحكم بواحدة أو أكثر منها على مرتكب جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وتشمل هذه العقوبات الحجر القانوني، والحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية، وتحديد الإقامة، والمنع من الإقامة، والمصادرة الجزئية للأموال، والمنع المؤقت من ممارسة مهنة أو نشاط، وإغلاق المؤسسة، والإقصاء من الصفقات العمومية، والحظر من إصدار الشيكات و/ أو استعمال بطاقات الدفع، وتعليق أو سحب رخصة السياقة أو إلغاؤها مع المنع من استصدار رخصة جديدة، وسحب جواز السفر، ونشر أو تعليق حكم أو قرار الإدانة، مع ضرورة الإشارة إلى أن العقوبات المنصوص عليها سابقاً في حالة التشديد تصبح عقوبات جنائية؛ وفي هذه الحالة تصبح عقوبتي الحجر القانوني والحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية عقوبات تكميلية إلزامية على القاضي النطق بها[2].

ب- العقوبات المقررة للشخص المعنوي: أقر المشرع الجزائري المسؤولية الجزائية للشخص المعنوي عن ارتكاب أحد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وذلك في المادة 394 مكرر 5 من قانون العقوبات، وكما في حالة الشخص الطبيعي تنقسم العقوبات المقررة للشخص المعنوي إلى عقوبات أصلية وعقوبات تكميلية كالآتي:

1- العقوبات الأصلية: لم يكتف المشرع الجزائري بالنص العام الذي يحدد مقدار الغرامة المقررة للشخص المعنوي[3]، بل أعاد تكرار نفس الحكم في المادة 394 مكرر5 السابقة؛ بحيث يعاقب الشخص المعنوي المرتكب لإحدى الجرائم السابقة بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، وتختلف هذه الغرامة باختلاف تلك المقررة للشخص الطبيعي وذلك تبعاً لوجود أو عدم وجود ظروف التشديد وعليه تشدد غرامة الشخص المعنوي تبعاً لتشديد غرامة الشخص الطبيعي.

2-العقوبات التكميلية: بالإضافة لعقوبة الغرامة تطبق على الشخص المعنوي واحدة أو أكثر من العقوبات التكميلية المتمثلة في حل الشخص المعنوي، وغلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات، والإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات، والمنع من مزاولة

[1]- المادة 394 مكرر6 من قانون العقوبات.

[2]- الفقرة الثانية من المادة 9 مكرر1 من نفس القانون.

[3]- وهو نص المادة 18 مكرر من نفس القانون.

نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس سنوات، ومصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها، ونشر وتعليق حكم الإدانة، والوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات[1].

ج- أحكام الإشتراك والشروع: فيما يخص الإشتراك فإن كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وكان هذا التحضير مجسداً بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها[2]، بينما يعاقب على الشروع في ارتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بالعقوبات المقررة للجريمة ذاتها[3].

ثانياً- إشكالية تطبيق العقوبات المقررة للجرائم الماسة بأنظمة المعالجة الآلية في حالة إستهداف الدفاع الوطني:

ينص المشرع الجزائري في المادة 394 مكرر3 من قانون العقوبات على أنه: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد"، إلا أن تطبيق هذا النص يطرح عديد الإشكاليات فالمصطلحات التي استخدمها المشرع في هذه المادة على بساطتها الظاهرية إلا أنها من الاتساع والمرونة والغموض ما يجعل من تحديد العقوبات التي يقصدها المشرع أمراً على قدر من الصعوبة، فأي معيار يتم إتباعه لتحديد الحالات التي تضاعف فيها العقوبات والحالات التي نطبق فيها العقوبات الأشد؟ ثم أي عقوبات أشد يقصدها المشرع من خلال هذا النص؟ إذ أن هناك عقوبات تتعدد وتختلف بحسب نوع الجريمة المستهدفة للدفاع الوطني سواء تلك المنظمة تحت عنوان جرائم الخيانة والتجسس أو تلك المنظمة تحت عنوان جرائم التعدي الأخرى على الدفاع الوطني بحيث قد تصل العقوبة إلى الإعدام، فالتشديد هنا من الخطورة بمكان على الأفراد الأمر الذي كان يفترض تحديد المقصود بلفظ "الأشد" بصورة صريحة، كما أن المشرع لم يحدد لنا الأساس الذي انطلاقاً منه نطابق بصورة دقيقة بين جريمة ماسة بأنظمة

[1]- المادة 18 مكرر من قانون العقوبات.

[2]- المادة 394 مكرر5 من نفس القانون.

[3]- المادة 394 مكرر7 من نفس القانون.

المعالجة الآلية وأخرى تستهدف الدفاع الوطني للقول بأن عقوبة الثانية مستحقة للأولى، ولإبراز هذه الصعوبات في التطبيق نورد الأمثلة الآتية:

أ- بالنسبة لجريمة الإعتداء على المعطيات والتي تتضمن أفعال الإدخال والإزالة والتعديل لمعطيات نظام المعالجة الآلية للمعطيات، فإن كل هذه الأفعال تؤدي إلى إفساد وإتلاف وتعييب المعطيات الموجودة في النظام بشكل يجعلها غير صالحة كلياً أو جزئياً للاستغلال، وهو أسوء ما يمكن أن تتعرض له هذه المعطيات من أشكال الإعتداء، وبحسب المادة 394 مكرر3 قد تكون هذه المعطيات متعلقة بالدفاع الوطني أي أن لها طابع السرية، وبالرجوع إلى القواعد التي تحكم جرائم الإعتداء على الدفاع الوطني وتحديداً جرائم التجسس نجد أن المشرع قد نص على المعاقبة بالإعدام على إتلاف المعلومات أو الأشياء أو المستندات أو التصميمات التي يجب أن تحفظ تحت ستار من السرية لمصلحة الدفاع الوطني بقصد معاونة دولة أجنبية أو ترك الغير يتلفها[1]، والإتلاف المقصود هنا هو الإتلاف المادي ويقصد به إعدام (الإتلاف الكلي أو الإزالة أو المحو) أو تعييب (الإتلاف الجزئي) الوعاء المستوعب لسر من أسرار الدفاع سواء كان هذا الوعاء متمثلا في وثيقة أو مخطط أو صورة أو جهاز أو آلة لتخزين المعلومات[2]، أما الإتلاف المنصوص عليه في المادة 394 مكرر1 فهو إتلاف معنوي ينصب على أسرار الدفاع الوطني التي تأخذ شكل معلومات إلكترونية، وكما سبق توضيحه تعاقب هذه المادة على مثل هذا الإتلاف في الأحوال العادية بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج وإذا استهدف الدفاع الوطني فبحسب المادة 394 مكرر 3 تضاعف العقوبة فتصبح الحبس من سنة إلى ستة سنوات والغرامة من 100.000 دج إلى 4.000.000 دج أما العقوبة الأشد فتنص عليها المادة 63 من قانون العقوبات التي تحكم الإتلاف التقليدي وهي الإعدام وإذا كان المشرع قد أصاب في تجريم الإتلاف المعنوي كما الإتلاف المادي لأن كلاهما يمثل أخطر أنواع الإعتداء على سر الدفاع الوطني فإن تقرير الإعدام كعقوبة أشد قد يثير بعض الغموض؛ فالمشرع يجرم ويعاقب على الإتلاف بالإعدام لما يشكله هذا الفعل من خطورة إذ يعدم السر ويزيله من الوجود أو يجعله غير صالح، أما الإتلاف المعنوي والذي تمثله جريمة الإعتداء على

[1]- البند الثالث من المادة 63 من قانون العقوبات.

[2]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 498-499.

المعطيات فرغم أنه هو الآخر يعدم سر الدفاع الوطني الذي يأخذ شكل معلومات إلكترونية لكن يجب الأخذ بعين الإعتبار أن هذا الإتلاف لا يلغي وجود السر نهائياً إذ تبقى هناك نسخ لهذا السر سواء كانت إلكترونية أم نسخاً أصلية مادية مما يجعل مساواة الإتلاف في الحالتين من حيث العقوبة شيئاً يدعو للنظر، فهل تُطبق في هذه الحالة العقوبة المضاعفة أم العقوبة الأشد؟.

ب- فيما يخص جريمة التعامل غير المشروع في معطيات يمكن أن ترتكب بها أحد جرائم المساس بأنظمة المعالجة الآلية للمعطيات والتي تشمل أفعال التصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار، فالمشرع يقصد من وراء تجريمه لها توفير الحماية الوقائية لأنظمة المعالجة وما تحويه من معطيات حساسة وذلك عن طريق منع ارتكاب الجرائم الماسة بها، وبالبحث في النصوص التقليدية عن مثل هذه السلوكات والتي قد تؤدي إلى ارتكاب جرائم تمس بالدفاع الوطني لنطبق من خلالها ما قصد به المشرع بتعبير العقوبات الأشد الوارد في المادة 394 مكرر3؛ نجد تجريم المشرع الجزائري لفعل جمع معلومات أو أشياء أو وثائق أو تصميمات يؤدي جمعها واستغلالها إلى الإضرار بمصالح الدفاع الوطني مقرراً عقوبة السجن المؤبد له[1]، وفعل الجمع هنا يشبه فعل تجميع معطيات يمكن أن ترتكب بها جريمة ماسة بأنظمة المعالجة الآلية للمعطيات تستهدف الدفاع الوطني فالفعل نفسه في الحالتين والنتيجة أيضا نفسها في الحالتين، وبالرجوع إلى العقوبات نجد المشرع الجزائري قد قرر في المادة 394 مكرر 2 لجريمة التعامل غير المشروع في معطيات يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية في الأحوال العادية عقوبة الحبس من شهرين إلى ثلاث سنوات والغرامة من 1.000.000دج إلى 5.000.000 دج وتضاعف في حالة استهداف الدفاع الوطني لتصبح الحبس من أربعة أشهر إلى ستة سنوات والغرامة من 2.000.000 دج إلى 10.000.000 دج، فهل تُطبق في هذه الحالة العقوبة المضاعفة أم تطبق العقوبة الأشد؟.

ج- بالنسبة لجريمة التعامل غير المشروع في معطيات متحصلة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي تشمل أفعال الحيازة أو الإفشاء أو النشر أو الاستعمال، فيمكن أن تكون هذه المعطيات متعلقة بالدفاع الوطني أي ذات طبيعة سرية وحيازتها أو إفشاؤها أو نشرها أو استعمالها يؤدي بدون شك لإلحاق ضرر كبير بالدفاع الوطني، ويقابل هذه الأنشطة في النصوص التقليدية كل من

[1]- المادة 65 من قانون العقوبات.

فعل التسليم والذي يشمل الإفشاء وفعل الاستحواذ الذي يشمل الحيازة كما تم شرحه في عناصر سابقة[1]، وتنصب هذه الأفعال على أسرار الدفاع الوطني وهذا لصالح دولة أجنبية أو أحد عملائها، ويقرر المشرع الجزائري في الأحوال العادية لجريمة التعامل غير المشروع في المعطيات وذلك بموجب المادة 394 مكرر2 عقوبة الحبس من شهرين إلى ثلاث سنوات والغرامة من 1.000.000 دج إلى 5.000.000 دج، وفي حالة استهداف الجريمة للدفاع الوطني تضاعف العقوبة بحسب المادة 394 مكرر3 لتصبح الحبس من أربعة أشهر إلى ستة سنوات والغرامة من 2.000.000 دج إلى 10.000.000 دج، أما العقوبة الأشد فهي ما تم النص عليه في المادة 63 من قانون العقوبات بحيث تكيف الجريمة على أنها تجسس ويعاقب فاعلها تبعا لذلك بالإعدام، فهل تُطبق العقوبة المضاعفة أم العقوبة الأشد؟.

يتبين من العرض السابق صعوبة تحديد العقوبات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في حالة استهدافها للدفاع الوطني وهذا يرجع بالأساس لمرونة وغموض المصطلحات التي استخدمها المشرع؛ ومما لاشك فيه أنه بهذا يمنح للقضاء سلطة واسعة في تقرير نوع العقوبة تبعاً لسلطته الواسعة في تفسير النص التجريمي المستحدث والقديم، ويفسر الكثير المرونة التي تكاد تكون الصفة الأساسية للنصوص ذات الصلة بأمن الدولة برغبة المشرع ذاته في إعطاء القاضي حرية التقدير، فالمشرع إنما يأتي بعبارات مرنة كي يسمح للقاضي بأن يعمل عقيدته وتقديره لكل جريمة على حدة وفقاً لظروفها الموضوعية الخاصة، رغم أن الإعتماد على القاضي في تحديد الجريمة الماسة بأمن الدولة من سواها قد يؤدي إلى خرق مبدأ المشروعية[2]، وقد يعرض حقوق الأفراد للانتهاك، وإذا كانت الجرائم الماسة بأمن الدولة في جل التشريعات تتسم بذات المرونة والاتساع لاعتبارات يرجحها المشرع، فإنه من غير الواجب تمديد هذه المرونة لتشمل جرائم موجهة ضد الأفراد بالأساس كالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بحيث يفترض على المشرع أن يحدد بدقة العقوبات المقررة لها في حالة مساسها بالدفاع الوطني وأن لا يترك النص على هذا الغموض والمرونة.

[1]– المادة 63 من قانون العقوبات.

[2]– محمد علي السيد، الوجيز في الجريمة السياسية، منشورات الحلبي الحقوقي، لبنان، 2003، ص. 62.

المبحث الثاني: الجهود الوطنية الإجرائية لمكافحة التجسس الإلكتروني.

لا تكون القواعد الموضوعية ذات جدوى بدون أن تجد طريقها للتطبيق؛ لذا تشكل القواعد الإجرائية المحور الثاني المكمل لأي سياسة وطنية ترمي لمكافحة الجريمة؛ إذ توفر القواعد الإجرائية وسائل كشفها وإثباتها ومتابعتها، ونظراً للطبيعة الخاصة للتجسس الإلكتروني من حيث كونه جريمة تتم في بيئة افتراضية لامادية فقد تعجز القواعد الإجرائية التقليدية المنصوص عليها في قانون الإجراءات الجزائية عن الإلمام بكل ظروفها وعناصرها؛ الأمر الذي أدى بالمشرع الجزائري تحسباً للصعوبات التي قد تعترض تطبيق النصوص الإجرائية التقليدية، إلى سن قواعد إجرائية جديدة تتماشى والجرائم المرتكبة في البيئة الإلكترونية وتكمل النقص في القواعد القديمة؛ وذلك من خلال إصدار قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ويحدد هذا القانون بعض قواعد الاختصاص القضائي في نظر الجرائم الماسة بالدفاع الوطني بالإضافة إلى نصه على بعض إجراءات التحري والتحقيق المستحدثة، وتشكل هذه المحاور أهم العناصر الإجرائية في مكافحة التجسس الإلكتروني؛ وعليه فستتم دراسة هذا المبحث من خلال ثلاثة مطالب: يتناول المطلب الأول قواعد الاختصاص القضائي في متابعة جرائم التجسس الإلكتروني، والمطلب الثاني إجراءات متابعة جرائم التجسس الإلكتروني في ظل قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والمطلب الثالث إجراءات متابعة جرائم التجسس الإلكتروني في ظل قانون الإجراءات الجزائية.

المطلب الأول: قواعد الاختصاص القضائي في متابعة جرائم التجسس الإلكتروني.

تقتضي متابعة أي جريمة تحديد الاختصاص القضائي بها ابتداءً، بمعنى إدخالها في سلطة الجهات القضائية الجزائرية، وقد لا تطرح بعض الجرائم إشكالات في تحديد اختصاص هذه الجهات بنظرها، وبالمقابل قد يستعصي الأمر بخصوص بعض الجرائم، وفي هذا الإطار تشكل جرائم التجسس إلكتروني أحد أكثر الجرائم التي تثير مسألة تحديد الاختصاص القضائي؛ بالنظر إلى أنها تجمع بين عدة خصائص، فهي جريمة إلكترونية عابرة للحدود بمعنى تخطيها للحواجز الإقليمية ومرتكبها لا تربطه بالجزائر أية رابطة قانونية فهو في كل الحالات أجنبي، كما أن هذه الجرائم –وهو الأمر الأخطر– تمس بالدفاع الوطني وبمصالح أساسية للجزائر، بمعنى أنها تطرح صعوبات فيما يخص تطبيق المبادئ القانونية التي تنظم مسألة الاختصاص القضائي سواء كان مبدأ الإقليمية أو مبدأ العينية؛ على اعتبار أن المبدئين المتبقيين المتمثلين في مبدأ الشخصية ومبدأ العالمية لا مجال لإعمالهما بخصوص التجسس

الإلكتروني؛ وعليه لتحديد كيفية إعمال مبدئي الإقليمية والعينية على جرائم التجسس الإلكتروني لتحديد الاختصاص القضائي بها تجب دراسة وتحليل كل مبدأ منها على حدة؛ وتبعا لذلك سيتناول الفرع الأول تطبيق مبدأ الإقليمية على جرائم التجسس الإلكتروني، ويتناول الفرع الثاني تطبيق مبدأ العينية على جرائم التجسس الإلكتروني.

الفـــرع الأول: تطبيــق مبـدأ الإقليمية على جرائـم التجـسس الإلكترونـي.

يرتبط مبدأ الإقليمية إرتباطاً وثيقا بسيادة الدولة فهو من يرسم حدودها وهذه الأخيرة عرفت تحولاً ملفتاً في المفهوم بظهور الفضاء الإلكتروني الذي أدى كذلك إلى تغيير في طبيعة السلوكات الإجرامية المرتكبة ومنها التجسس؛ مما يطرح إشكالية كيفية إعمال مبدأ الإقليمية عليها، وللإجابة عن هذه الإشكالية يستوجب الإحاطة بالمفاهيم المطروحة؛ وعليه سيتم التطرق بدايةً لمبدأ الإقليمية والسيادة في الفضاء الإلكتروني، ومن ثم التطرق إلى أثر خصوصية جرائم التجسس الإلكتروني على إعمال مبدأ الإقليمية.

أولاً- مبـدأ الإقليميـة والسيـادة فـي الفضـاء الإلكترونـي:

يُقصد بمبدأ الإقليمية تطبيق التشريع العقابي الوطني على كافة الجرائم المرتكبة على إقليم الدولة بصرف النظر عن جنسية الجاني أو المجني عليه؛ حيث يستوي أن يكون وطنياً أو أجنبياً، وبصرف النظر أيضاً عن المصلحة التي أهدرتها الجريمة ولو كانت مصلحة دولة أجنبية[1]، ومن هذا التعريف يتبين أن للمبدأ شقان أو مظهران هما:

أ- **المظهـر الإيجابـي:** ويتمثل في أن القانون الوطني وحده الذي يطبق في حدود إقليم الدولة، وأن لهذه الأخيرة أن تسن من التشريعات ما تراه لازماً لمصلحتها وأن تخضع لشرائعها جميع المقيمين على إقليمها رعايا وأجانب؛ ويترتب على هذا أنه لا يسمح بتطبيق أي تشريع أجنبي داخل الإقليم الوطني حتى لو كان ذلك عن طريق المحاكم الوطنية وإلا كان ذلك إعتداء على السيادة الوطنية للدولة؛ وعليه فالذي يرتكب التجسس داخل إقليم الدولة يخضع لقانون هذه الدولة أيا كانت جنسيته[2].

[1]- رفعت رشوان، مبدأ إقليمية قانون العقوبات في ضوء قواعد القانون الجنائي الداخلي والدولي، دار الجامعة الجديدة، مصر، 2008، ص. 13.

[2]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 461.

ب- المظهر السلبي: ويقصد به عدم إمتداد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقا لحدودها المعترف بها في القانون الدولي[1]، وهذا يفترض أن أحكام التجسس لا تسري على الجرائم التي تقع خارج إقليم الدولة؛ لأن ذلك يدخل في اختصاص الدولة صاحبة الإقليم التي تنفرد بمباشرة هذا الحق ويمتنع على غيرها من الدول الأخرى أن تمارس اختصاصاً من هذا النوع على إقليم ليس تابعاً لها؛ فليس لسلطة أجنبية أن تأمر بالقبض على متهمين مقيمين بإقليم دولة أخرى حتى لو كان هؤلاء قد ارتكبوا جرائم على إقليمها[2].

يتبين مما سبق الإرتباط الوثيق بين السيادة ومبدأ الإقليمية فإحترام الأولى يتطلب إعمال الثاني هذا من جهة، ومن جهة ثانية فالإقليم هو الذي يحدد المجال الذي تمارس فيه الدولة سيادتها، وعندما يتعلق الأمر بالحدود التقليدية للإقليم ومن ثم السيادة فلا تُطرح صعوبات كثيرة من حيث إشتمال الإقليم كما حدده الدستور[3] على المجال البري والمجال البحري والمجال الجوي بالإضافة إلى الحالات التي يتم فيها تمديد هذا الإقليم ليشمل السفن والطائرات الجزائرية، لكن الصعوبة تثور بخصوص مجال آخر مستحدث هو المجال أو الفضاء الإلكتروني، وهو البعد الذي أصبحت تمارس عبره كل أنواع الجريمة ذات الطابع الإلكتروني ومنها التجسس، وهذا البعد من الإتساع بحيث أضحى يشكل عالماً آخر موازٍ للعالم الافتراضي؛ إذ يضم كل الأفراد وكل الدول التي تتعامل عبره ويلغي بذلك الحدود الإقليمية التقليدية ليكون محيطاً ممتداً بدون حواجز، فلا يكون الجاسوس مضطراً للحضور جسدياً على إقليم دولة معينة ليمارس أنشطته التجسسية ما دام الفضاء الإلكتروني يختزل المسافات ويوفر له إمكانية الوصول إلى غاياته من أي مكان كان فيه.

ويكمن تفرد الفضاء الإلكتروني في أنه ورغم كونه بيئة وعالم جديد مختلف تماماً عن العالم الواقعي، إلا أنه يرتبط به ويتم استغلال عناصره لإدارته والتحكم فيه؛ وذلك من حيث كونه المجال الذي

---

[1]- موسى أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة عبر الوطنية، مداخلة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28- 29/ 10/ 2009.

[2]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 462.

[3]- تنص المادة 13 من الدستور على:

"- تمارس سيادة الدولة على مجالها البري ومجالها الجوي وعلى مياهها.

- كما تمارس الدولة حقها السيد الذي يقره القانون الدولي على كل منطقة من مختلف مناطق المجال البحري التي ترجع إليها".

يتميز باستخدام الإلكترونيات والمجال الكهرومغناطيسي لتخزين أو تعديل أو تغيير البيانات عن طريق النظم المتصلة والمرتبطة بالبنية التحتية الطبيعية[1]؛ مما يجعل هذا الفضاء الغير مرئي والمتصل في ذات الوقت بالبيئة الحقيقية الطبيعية مكاناً نقل إليه الأفراد والدول كل نشاطاتهم، حتى الغير مشروعة منها للاستفادة من مزايا الخفاء والسهولة في الوصول إلى الأهداف. ونظراً لارتباط هذا الفضاء بالبُنى التحتية الطبيعية التابعة لإقليم دولة معينة كان من المفروض أن يعتبر هذا الفضاء إمتداداً لذات الإقليم وأي سلوك غير مشروع يرتكب مساساً به كان يجب أن يعتبر مساساً بإقليم الدولة وسيادتها عليه، وهو الأمر الذي أثار التساؤل حول طبيعة هذا الفضاء الجديد، فهناك من يعتبره ملكاً دولياً مشتركاً، بمعنى عدم خضوعه لسيادة أية دولة، وتتم الدعوة إلى الاستخدام السلمي له وعدم عسكرته وهو بذلك يشبه الفضاء الخارجي ومنطقة أعالي البحار[2]، لكن إشتراك كل الدول في استخدام هذا الفضاء بدون أن يخضع لأي تحديد فيه مساس خطير بسيادتها بإعتبار أن هذا الفضاء متصل بشكل وطيد بالبُنى الطبيعية الإقليمية للدولة والقول باعتباره مجالاً مفتوحاً يؤدي بالضرورة إلى القول بإباحة انتهاك الحدود الإقليمية للدولة؛ الأمر الذي يستوجب وضع حدود للفضاء الإلكتروني كما كان الأمر بالنسبة للمجال الأرضي والبحري والجوي؛ إذ تقاسمت الدول فيما بينها هذه المجالات الثلاث وتركت منها أجزاءً عدتها ملكاً مشتركاً للإنسانية كما كان بالنسبة للقارة القطبية ولأعالي البحار وللفضاء الخارجي، وفي هذا الإطار لم يتم الوقوف على وجود جهود على المستوى الدولي في هذا الخصوص؛ ربما لأن الموضوع حديث جداً ويطرح إشكالات على المستوى التقني والفني ويتطلب إرادة سياسية دولية جادة؛ فمسألة ترسيم الحدود التقليدية ما زالت تطرح إشكاليات على المستوى الدولي فما بالك بمسألة ترسيم الحدود الإلكترونية، إلا أن هناك جهوداً على المستوى الداخلي يمكن القول أنها تصب في إتجاه مثل هذا التحديد وإن كانت في بداياتها؛ وذلك بسبب اقتناع الدول بخطورة ترك هذا الفضاء بدون تنظيم أو رقابة، وفي هذا الإطار نجد أن بعض الدول قد إتجهت للاعتماد على قدراتها الخاصة في وضع شبكات معلوماتية لها استقلاليتها عن الشبكة العالمية للمعلومات؛ وهذا رغبة في تقليص مساحة الانكشاف، ونسجل هنا تجربة الإتحاد الأوروبي في التعامل مع أمن المعلومات القومية من خلال وضع ما يعرف بالشبكة الأوروبية للوصول المباشر

[1]– عادل عبد الصادق محمد الجخة، مرجع سابق، ص. 29.

[2]– نفس المرجع، ص. 224.

للمعلومات "الأورونت Euro Net"[1]، وفي مجال مراقبة الدول لمجالها الإلكتروني نجد أنه من بين ما يقارب الأربعين حكومة التي تراقب فعلياً بيئتها الافتراضية تعد الصين أكثرها نجاحاً في هذا الخصوص[2]، فكما وضعت في السابق صورها العظيم كآلية لرسم وحماية حدودها، قامت حالياً – نسبة إلى أحد أهم تقنيات الأمن الإلكتروني وهي الجدران النارية – بوضع ما يعرف بصور الصين الناري العظيم " grand muraille pare-feu de chine"[3] لمراقبة مجالها الإلكتروني، وبإعتبار الفضاء الإلكتروني أساساً عبارة عن حقول من الترددات والأمواج الكهرومغناطيسية فقد أدى ذلك بالدول إلى محاولة بسط سيادتها عليها؛ وهذا ما إتجه إليه المشرع الجزائري من خلال القانون المتعلق بالبريد وبالمواصلات السلكية واللاسلكية حيث نص على أن الدولة تضطلع في إطار ممارسة صلاحياتها المتعلقة بمراقبة المواصلات السلكية واللاسلكية بممارسة السيادة طبقا للأحكام الدستورية على كامل فضائها الهيرتزي وبالإنفراد باستعمال طيف الذبذبات اللاسلكية الكهربائية والإشراف على استغلالها من طرف المتعاملين وموفري الخدمات والمرتفقين المباشرين[4].

مما سبق نخلص إلى أن مبدأ الإقليمية الذي يرتبط بسيادة الدولة على مجالها الإقليمي لا يجب أن يُحصر فقط في المجالات التقليدية؛ فبالإضافة إلى المجال البري والبحري والجوي، يمكن إضافة المجال أو الفضاء الإلكتروني كبعد رابع مستحدث، هذا البعد هو في الحقيقة ما يخلق الصعوبات في صدد إعمال مبدأ الإقليمية على جرائم التجسس الإلكتروني؛ لأنه هو ما يمنح للتجسس خصوصيته الإلكترونية وما يترتب عن هذه الخصوصية.

ثانيـاً– أثـر خصوصيـة جرائم التجسس الإلكتروني على إعمال مبـدأ الإقليميـة:

إن أحد أهم خصائص التجسس الإلكتروني أن السلوكات الإجرامية المكونة لركنها المادي تتسم بطبيعة معنوية من جهة، مع إمكانية توزعها على أكثر من إقليم واحد من جهة أخرى؛ وهذا على اعتبار أن التجسس الإلكتروني جريمة عابرة للحدود لا يشترط فيها الحضور المادي لمرتكبها في ذات الإقليم بل

[1]– وليد غسان جلعود، مرجع سابق، ص. 65.

[2]-Nir Kshetri, les activités d'espionnages électronique et contrôle d'internet A l'ére de l'infonuagique: le cas de la chine, Télescope, vol 18, n°=1-2, printemps-été 2012, p . 169.

[3]- ibid, p. 181.

[4]– المادة السادسة من القانون رقم 2000–03 المؤرخ في الخامس أوت من سنة 2000 المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية.

يكفي أن يُستهدف الجزء من الفضاء الإلكتروني الخاضع لسيادة الدولة المعنية للقول بوقوع الجريمة في إقليم هذه الدولة، وقد أدى هذا الطابع العابر للحدود إلى أن تصبح أكثر من دولة مختصة بالنظر في الجريمة؛ فقد يقوم الجاني من دولة تواجده المادي بإرسال برنامج تجسس عبر شبكة الأنترنت إلى عدة أنظمة معلوماتية في عديد الدول، أو قد يستهدف نظاماً معيناً في دولة معينة لكن هذا البرنامج قد يمر بخوادم موجودة في عدة دول؛ مما يجعل الدولة الأولى التي انطلق منها البرنامج والدولة التي حدثت فيها النتيجة ودول العبور التي تحقق بها بعض الركن المادي للجريمة جميعاً لها اختصاص إقليمي بنظر هذه الجريمة، وقد تدخل الفقه ليضع معايير يمكن الاستناد إليها لتحديد الاختصاص القضائي بمتابعة الجرائم ذات الطابع العابر للحدود بصفة عامة، وهي ثلاثة، يتم استعراضها ثم تحديد إن كان يصلح تطبيقها في حالة جرائم التجسس الإلكتروني:

أ- معيار السلوك أو النشاط الإجرامي: ووفقا لهذا المعيار ينعقد الاختصاص للمحكمة التي يقع في نطاقها النشاط الإجرامي؛ لأن هذا يؤدي إلى تيسير عملية الإثبات وجمع أدلة الجريمة وأن المحكمة التي لها ولاية نظر الدعوى تكون قريبة من مسرح الجريمة، ناهيك عن أن الحكم الذي يصدر في الواقعة يكون أكثر فعالية ويسهل معه ملاحقة الجناة، وهو المعيار الذي أخذ به المشرع الجزائري في قانون الإجراءات الجزائية؛ حيث نص بأنه تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر[1].

ب- معيار مكان تحقق النتيجة: تعرض المعيار الأول لعدة إنتقادات من جانب آخر من الفقه؛ من حيث أنه لا يعير اهتماماً للمكان الذي تحقق فيه الضرر أو أثر النشاط الإجرامي الذي كان الجاني يسعى إلى تحقيقه فالآثار الضارة هي التي تبعث الفزع في النفوس في حين أن مكان وقوع السلوك لا يعدو أن يكون مصدر الضرر ليس إلا[2]، ومن التشريعات التي تأخذ بهذا الإتجاه التشريع الأمريكي الذي يعطي الاختصاص لمحاكمه الجنائية بمجرد حدوث آثار الجريمة على إقليمها ، فقد قضى في أمريكا بأنه إذا تم إدخال بيانات من مكان معين وكانت تتضمن ما يشكل جريمة إلكترونية وكانت هذه البيانات مقروءة في دولة أخرى فإن الاختصاص ينعقد لمحاكم الدولة التي يمكن الإطلاع على تلك

[1]- المادة 586 من قانون الإجراءات الجزائية.

[2]- موسى مسعود أرحومة، مرجع سابق.

البيانات في إقليمها[1]، كما تم إعتبار مجرد مكالمة هاتفية مع شخص في دولة أخرى مبرراً لإعتبار الجريمة قد وقعت بالفعل فوق إقليم الدولة[2].

ج- المعيار المختلط: ومفاده أن الجريمة تعد واقعة في مكان حصول النشاط وكذلك في المكان الذي تحققت فيه النتيجة أو الذي من المتوقع أو من المنتظر تحققها فيه، ويتم تغليب قانون محل تحقق النتيجة إذا كانت الجريمة تامة، في حين يفضل مكان النشاط أو السلوك إذا كانت الجريمة قد وقفت عند حد الشروع أو كانت من قبيل جرائم السلوك المجرد[3].

إذا كان من البساطة تطبيق المعايير السابقة والأخذ بها في الجرائم العادية فإن جريمة التجسس الإلكتروني لها من الخصوصية ما يصعب تطبيق المعايير السابقة عليها وهذا للأسباب الآتية:

- فيما يخص معيار مكان السلوك الإجرامي فإن الجاني في جريمة التجسس الإلكتروني قد يرتكب سلوكه الإجرامي إنطلاقاً من دولة أخرى غير الدولة المستهدفة بالإعتداء على أسرارها، وبالنظر إلى حساسية هذا المحل؛ فالدولة لا يمكنها بأي حال أن تتنازل عن اختصاصها بمتابعة الجريمة أو أن تتشاركه مع دولة أخرى فالاختصاص يعود إليها بغض النظر عن مكان وقوع الجريمة، مع الأخذ بعين الاعتبار وجود حالات لا يمكن معها تحديد المكان الذي ارتكب فيه النشاط الإجرامي.

- يبدو معيار مكان تحقق النتيجة مقبولاً ظاهرياً لأنه يمنح الاختصاص للدولة المتضررة وفي هذه الحالة لن تضطر الدولة لتقاسم النظر في جريمة تمس أمنها مع غيرها من الدول، لكن لا يمكن تطبيق ذلك فيما يخص التجسس الالكتروني لأنه يعد من جرائم السلوك المجرد بحيث تتحقق الجريمة بمجرد القيام بالسلوك دون التوقف على تحقق نتيجة معينة، كما تثار هنا مسألة الإفلات من العقاب في حالة الشروع؛ وعليه فالدولة التي يستهدفها التجسس يجب أن يؤول لها الاختصاص بغض النظر عن حدوث نتيجة من عدمها.

- في ظل خصوصية التجسس الإلكتروني فقد يحتمل أن تُستهدف أسرار أكثر من دولة؛ وهي الحالة التي يكون فيها الجاني فرداً يعمل لحسابه الخاص أو في حالة جماعات الجريمة المنظمة أو

---

[1]- نسيم سعيداني، مرجع سابق، ص. 100.

[2]- مفتاح بوبكر المطردي، مرجع سابق.

[3]- موسى مسعود أرحومة، مرجع سابق.

المنظمات الإرهابية، فهنا يثبت لكل تلك الدول الاختصاص لأن محل الجريمة على ذات الدرجة من الحساسية والأهمية للجميع ويصبح إعمال معيار مكان تحقق النتيجة دون فائدة؛ لأن السلوك يتسبب في ضرر لعدة دول، كما أن معيار مكان السلوك قد يمنح الاختصاص لدولة حصل فيها مجرد السلوك الإجرامي وهي بذلك لن تُقدر محل الجريمة كالدولة المتضررة ذاتها، بالإضافة إلى عراقيل أخرى لها أهميتها كعدم تجريم قانون الدولة التي تم فيها السلوك لهذا السلوك، أو عدم إعتبارها لمحل الجريمة سراً في قانونها، وتمتنع مع هذا عن تسليم الجاني إلى الدولة الطالبة.

مما سبق نخلص إلى أن هناك تغييراً كبيراً في مفهوم مبدأ الإقليمية بظهور الفضاء الإلكتروني كمجال سيادة جديد للدولة يُستهدف بسلوكات إجرامية ذات طبيعة معنوية تتوزع على أقاليم أكثر من دولة؛ مما أعطى لهذا المبدأ أبعاداً جديدة تطرح إشكالات لم تكن معروفة من قبل؛ فالقول بأن اختصاص الدولة بنظر التجسس الإلكتروني يتحدد بحصول أحد سلوكاته الإجرامية على إقليمها قول يتجاوز البساطة التي يبدو عليها، وإذا كان النقد التقليدي الموجه لمبدأ الإقليمية من حيث كونه يقف عاجزاً عن أداء دوره في معاقبة المجرمين الذين ارتكبوا جرائمهم خارج الإقليم ومن ثم يقف عقبة في سبيل المحافظة على المصالح الأساسية للدولة[1]، فإن ظهور الفضاء الإلكتروني ومن ثم التغييرات التي طرأت على مفهوم الإقليم قد تجعل مبدأ الإقليمية عاجزاً كذلك حتى عن أداء دوره الكامل في معاقبة المجرمين الذين ارتكبوا جرائمهم داخل الإقليم بمفهومه الجديد الذي لا يشترط الوجود المادي لهؤلاء المجرمين.

الفـــرع الثانـــي: تطبيـق مبدأ العينيـة على جرائـم التجـسس الإلكترونـــي.

رغم كون مبدأ الإقليمية المبدأ الأساسي المتبع لتحدد الاختصاص القضائي في كل التشريعات واعتبار المبادئ الأخرى مبادئ احتياطية، إلا أن مبدأ العينية يحتل تلك المكانة والأهمية في حالة المساس بالمصالح الأساسية للدولة، وقد عرف هذا المبدأ تطوراً في ظل تعديل قانون الإجراءات الجزائية لسنة 2015، وكذا في ظل قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ وعليه سيتم بداية التطرق لمدلول ومبررات تطبيق مبدأ العينية، ثم التطرق لكيفية إعمال مبدأ العينية على جرائم التجسس الإلكتروني في ظل القوانين الإجرائية الجديدة.

[1]– زكي زكي حسين زيدان، مرجع سابق، ص. 151.

أولاً- مدلول ومبررات تطبيق مبدأ العينية: سيتم عرض مدلول مبدأ العينية، ومن ثم مبررات تطبيقه كالآتي:

أ- مدلول مبدأ العينية: يقصد بمبدأ العينية أو كما يسميه البعض بمبدأ الذاتية[1]، تطبيق أحكام القانون الجنائي على كل جريمة تمس مصلحة أساسية للدولة أياً كان مكان ارتكابها أو جنسية فاعلها، فالضابط في هذا المبدأ يكمن في أهمية المصلحة التي تهدرها الجريمة، وأساس هذا المبدأ يتمثل في أن الدولة لا يمكن أن تترك لغيرها من الدول الأخرى مهمة العناية بمصالحها الحيوية الشخصية البحتة بل إن جوهر المبدأ يكون أظهر عندما لا يعد الفعل جريمة في محل وقوعه وذلك حتى تطمئن كل دولة أن كل عدوان يلحق مصالحها الأساسية خارج إقليمها الوطني لن يمر بغير عقاب، ولذلك يعد مبدأ العينية مبدأ المصلحة في صورتها المجردة[2].

ب- مبررات تطبيق مبدأ العينية: يستند الأخذ بمبدأ العينية على عدة مبررات يمكن إجمالها فيما يلي:

1- مبدأ حماية المصالح الأساسية للدولة: بحيث توجد للدولة مصالح وحقوق تسعى إلى حمايتها عن طريق تجريم الأفعال التي تضر بها وهذه المصالح والحقوق فئتان: الفئة الأولى والتي تنبثق عن كيان الدولة ذاته كشخص من أشخاص القانون الدولي، أو عن استقلالها وسيادتها وسلامتها، أو عن علاقاتها الدولية، والفئة الثانية تنبثق عن الدستور ونظام الحكم الداخلي للدولة وسلطاتها العامة، وعن وحدة الشعب وأمنه وعدم النيل منها[3]، ويندرج التجسس الإلكتروني ضمن الطائفة الأولى من الحقوق الأساسية التي تسعى الدولة لحمايتها ومن ثم تجريم هذا السلوك وإتخاذ كل ما يلزم لمتابعته؛ خاصة أن متابعة ذات السلوك قد لا تلقى الإهتمام اللازم من جانب الدول الأجنبية التي يقع فيها، بل قد تكون هذه الدول هي المستفيدة منه؛ ولهذا تأخذ مختلف التشريعات بمبدأ العينية في نطاق الجرائم المضرة بالمصالح الحيوية للدولة عندما ترتكب في الخارج سواء كانت هذه الجرائم معاقباً عليها في البلد الأجنبي الذي وقعت

[1]- فهد ناصر عيسى بن صليهم، مبدأ العينية وأثره في مكافحة الجرائم العابرة للحدود الدولية، مذكرة ماجستير في العدالة الجنائية ، مقدمة لكلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص. 31.

[2]- زكي زكي حسين زيدان، مرجع سابق، ص. 152.

[3]- فهد ناصر عيسى بن صليهم، مرجع سابق، ص. 41.

فيه وبنفس الوصف الذي تخضع له في القانون الوطني للدولة المتضررة[1]، أو كانت هذه السلوكات لا تشكل جرائم في هذا البلد الأجنبي؛ وذلك من منطلق أنه لا توجد دولة بإمكانها أن تُقدر أهمية المحل الذي إنصبت عليه الجريمة أو أن تُقدر درجة حساسية المصالح المستهدفة بالعدوان كالدولة المتضررة ذاتها، كما أن طبيعة محل الجريمة من الخصوصية والارتباط الوطيد بالدولة ما يمنع أن تتنازل الدولة عن حقها في المتابعة لدولة أخرى؛ لأن هذا يعني تنازلها عن سيادتها.

2- مبدأ سيادة الدولة ودفاعها عن النفس: إن التطورات التقنية الحديثة في مجال تكنولوجيات المعلومات والاتصالات أدت إلى زيادة فرص ارتكاب الجرائم انطلاقاً من دول أخرى؛ مما حذا بالدولة أن تواجه خطرها على دفاعها الوطني عن طريق التوسع في بسط تطبيق قوانينها العقابية خارج إقليمها مستندة في ذلك على ما لها من سيادة دون أن تكترث للدول الأخرى؛ فقانون الدولة هو وحده الذي يحدد النطاق المكاني الذي تنفذ إليه قواعد قانونها الجنائي وأنه ليس ثمة قانون يمنع الدولة من أن تمارس حقها في عقاب أي عدوان ضدها، ولئن كان من المؤكد أن الدولة إذ تطالب بهذا الحق سوف تصطدم بغيرها من الدول، إلا أن حقها في العقاب يتوقف دائما على إرادتها وحدها بوصفها صاحبة السيادة لا على أي قواعد أخرى فالدولة بحكم سيادتها تأبى الخضوع لإرادة خارجية على أمنها[2]، وبالإضافة إلى حقها في السيادة تستند الدولة في تبريرها لمد اختصاصها القضائي خارج حدودها الإقليمية المادية على حق آخر مقرر في القانون الدولي وهو حقها في الدفاع عن النفس ضد الاعتداءات التي تطال مصالحها الأساسية؛ فلا يمكن لها أن توكل أو تعتمد على غيرها في الدفاع عنها.

ثانياً- إعمال مبدأ العينية على جرائم التجسس الإلكتروني في ظل القوانين الإجرائية الجديدة:

على غرار باقي التشريعات أخذ المشرع الجزائري بمبدأ العينية لحماية المصالح الأساسية للدولة الجزائرية، لكن عرف مفهوم هذه المصالح وكذا كيفية إعمال هذا المبدأ تغييرات تضمنتها مواد قانون الإجراءات الجزائية المعدل في سنة 2015 وكذا قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذه المواد هي التي تحدد إطار تطبيق مبدأ العينية في القانون الجزائري؛ وعليه

[1]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 466.

[2]- فهد ناصر عيسى بن صليهم، مرجع سابق، ص. 102.

سيتم بداية تناول شروط إعمال مبدأ العينية على جرائم التجسس الإلكتروني في القانون الجزائري، ثم سيتم التطرق إلى صعوبات إعمال مبدأ العينية على جرائم التجسس الإلكتروني في القانون الجزائري.

أ- شـــروط إعمال مبدأ العينيـة على جرائم التجسس الإلكتروني في القانون الجزائـري:

عرف مبدأ العينية في القانون الجزائري تطوراً على مستوى المفهوم وشروط الإعمال، بل إن هذا المفهوم ذاته تم النص عليه في كل من قانون الإجراءات الجزائية المعدل في سنة 2015[1]، وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بحيث تنص المادة 588 المعدلة من قانون الإجراءات الجزائية على أنه: "تجوز متابعة ومحاكمة كل أجنبي وفقا لأحكام القانون الجزائري ارتكب خارج الإقليم الجزائري بصفة فاعل أصلي أو شريك في جناية أو جنحة ضد أمن الدولة الجزائرية أو مصالحها الأساسية أو المحلات الدبلوماسية والقنصلية الجزائرية أو أعوانها أو تزييفا لنقود أو أوراق مصرفية وطنية متداولة قانونا في الجزائر أو أي جناية أو جنحة ترتكب إضراراً بمواطن جزائري"، بينما تنص المادة 15 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه: "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبياً وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني"، ومن خلال هذين النصين يتم إستخلاص شروط إعمال مبدأ العينية على جرائم التجسس الإلكتروني تحديداً مع المقارنة بما كان منصوصاً عليه في المادة 588 من قانون الإجراءات الجزائية القديم[2]، وهذا كالآتي:

1- يشترط لإعمال مبدأ العينية أن تكون الجريمة المرتكبة مكيفة على أنها جناية أو جنحة وأن تشكل اعتداءاً على محال محددة على سبيل الحصر، رغم أن قائمة الجرائم هذه قد عرفت توسيعاً وتغييراً

[1]- الأمر رقم 15-02 المؤرخ في 23 يوليو سنة 2015 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية.

[2]- تنص المادة 588 من قانون الإجراءات الجزائية قبل تعديلها على: "كل أجنبي ارتكب خارج الإقليم الجزائري بصفة فاعل أصلي أو شريك جناية أو جنحة ضد سلامة الدولة الجزائرية أو تزييفاً لنقود أو أوراق مصرفية وطنية متداولة قانوناً بالجزائر تجوز متابعته ومحاكمته وفقاً لأحكام القانون الجزائري إذا القي القبض عليه في الجزائر أو حصلت الحكومة على تسليمه"

بعد التعديل الذي عرفته المادة 588 فقد كانت تضم قبل تعديلها، كل اعتداء ضد سلامة الدولة الجزائرية أو تزييفاً لنقود أو أوراق مصرفية وطنية متداولة قانوناً بالجزائر، لتضم في ظل المادة 588 المعدلة كل إعتداء على أمن الدولة الجزائرية أو مصالحها الأساسية أو المحلات الدبلوماسية والقنصلية أو أعوانها أو تزييفاً لنقود أو أوراق مصرفية وطنية متداولة قانوناً في الجزائر، ويلاحظ تخلي المشرع الجزائري عن تعبير سلامة الدولة الجزائرية والذي يعتبر تعبيراً فضفاضاً يتسع ليشمل كل المصطلحات الجديدة التي جاء بها المشرع الجزائري، لكنه فضل تعويضه بهذه المصطلحات الجديدة، وفي هذا الإطار كان المشرع الجزائري قبل تعديل قانون الإجراءات الجزائية قد عدل طائفة هذه الجرائم بموجب المادة 15 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ليضيف بذلك الجرائم المتصلة بتكنولوجيات الإعلام والاتصال لنطاق إعمال مبدأ العينية مع اشتراط أن تستهدف هذه الجرائم مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني، ويستحسن بالمشرع الجزائري هنا توحيد المصطلحات المستعملة درءاً لأي غموض أو تداخل في المفاهيم، والتجسس الإلكتروني يجد سنده في إعمال مبدأ العينية عليه في كلا القانونين وفي كلتا المادتين فهو جريمة ماسة بأمن الدولة وكذا جريمة من جرائم تكنولوجيات الإعلام والاتصال المستهدفة للدفاع الوطني.

2- كان المشرع الجزائري في ظل المادة 588 قبل تعديلها يشترط لإعمال مبدأ العينية ومتابعة الجاني ومحاكمته وفقا لأحكام القانون الجزائري، إما أن يتم القبض على الجاني في الجزائر أو حصول الحكومة على تسليمه لها، لكن التعديل الجوهري في هذه المادة يكمن في إلغاء المشرع الجزائري لهذا الشرط؛ وعليه لا يشترط لمتابعة مرتكب التجسس الإلكتروني أن يتم القبض عليه في الجزائر أو أن يتم تسليمه للجزائر؛ فيمكن إذاً متابعته ومحاكمته غيابياً.

3- لم يضع المشرع الجزائري سواء من خلال المادة 588 من قانون الإجراءات الجزائية أو المادة 15 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ضوابط معينة لتختص المحاكم الجزائرية بمحاكمة الجاني عن الجرائم المنصوص عليها فيها ومنها التجسس الإلكتروني؛ فالاختصاص يعود إليها في جرائم التجسس الإلكتروني المرتكبة في الخارج سواء كانت السلوكات المكونة لها تمثل جرائم في ظل تشريع الدولة التي ارتكبت فوق إقليمها أو لم تكن كذلك وسواء تمت محاكمة المتهمين عن هذه الأفعال أمام القضاء الأجنبي أو لم تتم، كما أن الأحكام الصادرة عن المحاكم الأجنبية

سواء بالبراءة أو الإدانة لا تغل يد القاضي الوطني في الفصل في الواقعة المعروضة عليه متى كانت تشكل جريمة من جرائم التجسس وفقا لأحكام القانون الوطني[1].

4- لم يجعل المشرع الجزائري ممارسة الاختصاص بمتابعة ومحاكمة الجاني عن أفعال التجسس الإلكتروني أمراً إلزامياً على الجهات القضائية الجزائرية، فالمادة 588 من قانون الإجراءات الجزائية في صيغتها القديمة وكذا في صيغتها المعدلة تجعل ممارسة هذا الاختصاص أمراً جوازياً وذلك بصريح العبارة ، لكن المشرع لم يستخدم تعبير "تجوز متابعة أو محاكمة ..." في المادة 15 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بل جاءت صيغة المادة دالة على وجوبية اختصاص المحاكم الجزائرية بنظر الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة بالخارج والمستهدفة للدفاع الوطني، ولا يمكن الجزم إذا كان المشرع يقصد إخراج هذا النوع من الجرائم من نطاق الجوازية ليجعل الاختصاص القضائي الجزائري به وجوبي، أم أنه أراد من خلال المادة 15 أن يضيف هذا النوع من الجرائم إلى طائفة الجرائم التي تدخل في نطاق إعمال مبدأ العينية دون نية خصها بوجوبية ممارسة الاختصاص بشأنها، وهذين الاحتمالين يُستقرءان من الصيغة التعبيرية التي استخدمها المشرع الجزائري في المادة 15 بحيث جاء فيها "**زيادة على قواعد الاختصاص** المنصوص عليها في قانون الإجراءات الجزائية، **تختص المحاكم الجزائرية بالنظر** في الجرائم المتصلة بتكنولوجيات ...".

ب- صعوبات إعمال مبدأ العينية على جرائم التجسس الإلكتروني في القانون الجزائري:

إن أهم الصعوبات التي تقف في وجه إعمال مبدأ العينية هو عدم إمكانية تطبيقه؛ وهذا يرجع إلى صعوبة التوصل إلى الجاني وجعله يمثل أمام المحاكم الوطنية، فلا يمكن في أغلب الحالات إلقاء القبض على الجاني في إقليم الدولة الجزائرية؛ نظراً لخفاء الجريمة ودرجة التكتم على تنفيذها إن تمت في الجزائر، أو أنها أصلاً تتم خارج الإقليم الجزائري بواسطة الدخول إلى أنظمة المعالجة الآلية للمعطيات عن بعد وهو الاحتمال الأرجح في حالة التجسس الإلكتروني، وحتى في هذه الحالة لا يمكن في أغلب إن لم نقل في كل الحالات الحصول على تسليم هذا الجاني للسلطات الوطنية؛ لأن الكثير من الدول ونظراً لحساسية موضوع ومحل التجسس وهو أسرار الدفاع الوطني ترفض التسليم بدعوى عدم وجود ضمانات للمحاكمة العادلة أو أن تتمسك بعدم التسليم لأن قانونها لا يعتبر الفعل الذي أقدم عليه الجاني جريمة؛

[1]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 468.

وهذا يرجع أساساً إلى أن فكرة المصالح الأساسية للدولة أو الإستراتيجية أو حتى ما يعتبر أمراً ماساً بأمن الدولة موضوع نسبي التجريم فما تعتبره دولة من المصالح الأساسية قد لا تعتبره دولة أخرى كذلك، هذا دون تجاهل الإحتمال الذي تكون الدولة التي ارتكب على إقليمها التجسس هي ذاتها دولة الجاني فيستحيل معه أن تسلم الدولة أحد رعاياها وهذه قاعدة قانونية ثابتة في كل التشريعات، أو هي ذاتها الدولة التي تم التجسس لمصلحتها فيكون أيضا من المستحيل تسليم الجاني الذي قدم لها مثل هذه الخدمات الجليلة في نظرها، وقد تكون هذه الأسباب هي التي دفعت المشرع الجزائري إلى إلغاء شرط إلقاء القبض على الجاني في الجزائر أو الحصول على تسليمه لإعمال مبدأ العينية فيمكن متابعته ومحاكمته غيابياً؛ كل هذه الصعوبات أدت بالبعض للقول أن الفائدة من وراء النص على هذا المبدأ لا تعدو مجرد التخويف[1].

المطلـــب الثانـي: إجراءات متابعـة جرائم التجسس الإلكتروني في ظل قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهـــا.

تبدأ إجراءات متابعة الجريمة بصفة عامة من لحظة العلم بوقوعها إلى غاية صدور حكم بات فيها، وتخضع جرائم التجسس الإلكتروني شأنها شأن باقي الجرائم لذات هذه الإجراءات، غير أنها تنفرد بخصوصية إجراءات التحري والتحقيق فيها وهذا لخصوصية وسائل ومخلفات ارتكابها والبيئة التي تتم فيها؛ مما يجعل الإجراءات التقليدية المقررة للجرائم العادية عاجزة عن كشف أداة الجريمة وفاعلها الإلكتروني؛ ولهذا فقد أفرد لها المشرع الجزائري مجموعة إجراءات خاصة تتلائم مع البيئة الإلكترونية التي تتم على مستواها ولها القدرة على التعامل مع الدليل الإلكتروني الناجم عنها، وباعتبار جرائم التجسس الإلكتروني من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المستهدفة لأمن الدولة وللدفاع الوطني؛ فقد خصها قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بمجموعة من إجراءات التحقيق والتحري الخاصة ونص صراحة على ارتباط هذه الإجراءات بالمساس بأمن الدولة وبالدفاع الوطني؛ لذا سيتم تركيز الدراسة عليها في هذا المطلب، وعليه يقسم هذا الأخير إلى ثلاثة فروع: يتناول الفرع الأول مراقبة الاتصالات الإلكترونية، ويتناول الفرع الثاني تفتيش المنظومات المعلوماتية

[1]– محمود سليمان موسى، الجرائم الماسة بأمن الدولة، مرجع سابق، ص. 112.

وحجز المعطيات المعلوماتية، بينما يتناول الفرع الثالث حفظ المعطيات المتعلقة بحركة السير واعتراض المعطيات المتعلقة بالمحتوى.

الفـــرع الأول: مراقبـــة الاتصـــالات الإلكترونيـــة.

يُعد إجراء مراقبة الاتصالات الإلكترونية أكثر الإجراءات المستحدثة أهمية نظراً لدوره المزدوج في الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا في مكافحتها، وتظهر هذه الأهمية من خلال تنظيم المشرع الجزائري لها من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومن خلال تخصيص أكثر مواد المرسوم الرئاسي المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لهذا الإجراء، وسيتم تناوله من خلال عنصرين: يعرض الأول تعريف مراقبة الاتصالات الإلكترونية، والثاني ضوابط مراقبة الاتصالات الإلكترونية.

أولاً- تعريـف مراقبـة الاتصـالات الإلكترونيـة:

نص المشرع الجزائري على إجراء مراقبة الاتصالات الإلكترونية من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، لكنه لم يتطرق شأنه شأن أغلب التشريعات إلى تحديد المقصود بمراقبة الاتصالات الإلكترونية، مكتفياً في ذلك بتعريف الاتصالات الإلكترونية فقط بأنها: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية[2]، وقد يثير هذا التعريف القانوني التساؤل حول العلاقة بين إجراء مراقبة الاتصالات الإلكترونية وإجراء اعتراض المراسلات السلكية واللاسلكية الوارد في المادة 65 مكرر 5 من قانون الإجراءات الجزائية، خاصةً في ظل الخلط الكبير الذي يتم الوقوف عليه حين الرجوع إلى تعريف المراقبة الإلكترونية فقهاً فتعرف الثانية بدلالة الأولى أو العكس، ولتبيين الفرق بين الإجرائين نرجع إلى قانون البريد والمواصلات السلكية واللاسلكية بحثاً عن تعريف للاتصالات السلكية واللاسلكية لبحث الفرق بينها وبين الاتصالات الإلكترونية الواردة في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ؛ فنجده يُعرف المواصلات السلكية واللاسلكية بأنها: كل تراسل أو إرسال أو

[1]- المادة الرابعة من قانون الوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]- الفقرة "و" من المادة الثانية من نفس القانون.

استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية[1]، والملاحظ على التعريفين التطابق التام في موضوع الاتصال لكن الاختلاف يكمن في وسيلة الاتصال، ففي حالة الاتصالات الإلكترونية وسع المشرع الجزائري من مفهومها ومحتواها لتشمل أية وسيلة إلكترونية بينما حددها المشرع في حالة الاتصالات السلكية واللاسلكية عموماً في أي وسيلة سلكية أو لاسلكية كهربائية أو كهربائية مغناطيسية، وتبدو هذه المصطلحات التقنية صعبة الإدراك بعض الشيء لكن ليس الغرض هنا هو فهم المقصود العلمي بهذه التجهيزات وإنما وضع الحدود الفاصلة بين كل من إجراء مراقبة الاتصالات الإلكترونية وإجراء مراقبة أو اعتراض المراسلات السلكية واللاسلكية، ولأجل هذا نرجع إلى التعريف الممنوح سابقاً للفظة "إلكتروني" لنستخلص المقصود بوسيلة إلكترونية، بحيث تم إبراز أن لفظة "إلكتروني" يعني كل ما يتصل بالتكنولوجيا الحديثة وذو قدرات كهربائية أو رقمية أو مغناطيسية أو لاسلكية أو بصرية أو كهرومغناطيسية أو مؤتمتة أو ضوئية أو ما شابه ذلك"[2]، ويتضح من خلال هذا التعريف أن الاتصالات الإلكترونية أوسع من الاتصالات السلكية واللاسلكية؛ بحيث تتضمن الوسائل التي تقوم عليها الثانية وتتجاوزها، فتشمل بذلك الهاتف الثابت والهاتف المحمول والبريد الإلكتروني ومواقع التواصل الاجتماعي ومنتديات النقاش الإلكترونية وغيرها من الوسائل الإلكترونية المستخدمة للتواصل بين الناس التي لم يشأ المشرع حصرها؛ وعليه يتضح أن إجراء مراقبة الاتصالات الإلكترونية أوسع من إجراء مراقبة الاتصالات السلكية واللاسلكية ويتضمنه، وفي المقابل لا يمكن القول بأن الإجرائين منفصلان ولكل منهما مجاله الخاص بحيث إذا كان إجراء اعتراض الاتصالات السلكية واللاسلكية محصوراً حسب البعض في التنصت التليفوني أي في مراقبة المكالمات الهاتفية فقط[3]، فيتم بالموازاة مع ذلك حصر مراقبة الاتصالات الإلكترونية في تلك التي تتم عبر الأنظمة الحاسوبية، والدليل أن المشرع الجزائري قد تفطن لهذه الثغرة وتدارك الأمر في المرسوم الرئاسي المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ بحيث أعاد تعريف الاتصالات الإلكترونية من خلاله

---

[1]– الفقرة 21 من المادة الثامنة من القانون رقم 2000–03 المؤرخ في الخامس أوت من سنة 2000 المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية.

[2]– علي جعفر، مرجع سابق، ص. 32.

[3]– هشام ساحلي، أساليب التحري الخاصة ومدى مساسها بحرمة تنقل الفرد في التشريع الجزائري، مجلة الحقوق للبحوث القانونية والاقتصادية، العدد الثاني، كلية الحقوق، جامعة الإسكندرية، مصر، 2014، ص. 864.

بالقول بأنها: كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية بما في ذلك وسائل الهاتف الثابت والنقال[1].

من خلال إبراز العلاقة بين إجرائي مراقبة الاتصالات الإلكترونية ومراقبة الاتصالات السلكية واللاسلكية، يمكن القول بأن المحاولات الفقهية لتعريف المراقبة الإلكترونية التي تم الوقوف عليها في معظمها محل نقد بسبب خلطها ليس فقط بين الإجرائين السابقين، ولكن لخلطها أيضا بين إجراء المراقبة الإلكترونية وإجراء تسجيل الأصوات والأحاديث الخاصة، وفي هذا الإطار يذهب البعض إلى حد القول بأن الاختلاف بينها يكمن في التسمية فقط[2]؛ وعليه يتم تعريف إجراءات مختلفة على أساس أنها ذاتها إجراء مراقبة إلكترونية، ومنها تعريف المراقبة بأنها: تعمد الإنصات والتسجيل ومحلها المحادثات الخاصة سواء كانت مباشرة أو غير مباشرة أي سواء كانت مما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكية واللاسلكية، أو تعريف المراقبة بأنها: التنصت ومحلها المحادثات التي تدور بين أكثر من شخص سواء بواسطة الأجهزة التليفونية أو اللاسلكية أو أجهزة الشفرة أو كانت مباشرة بين شخصين أو أكثر وكانت بطريقة يقصد بها أطرافها ألا تكون مسموعة للغير، أو بأنها: نوع خاص من استراق السمع يسلط على الأحاديث الشخصية والمحادثات التلفونية خلسة دون علم صاحبها بواسطة أجهزة إلكترونية أسفر عنها النشاط العلمي الحديث فهو ينصب على أي حديث شخصي يكون للإنسان مع نفسه أو مع غيره ويكون له صفة شخصية كما ينصب على المكالمات التلفونية التي تدور بين أطرافها ويمتد مفهوم المكالمات التلفونية ليشمل المكالمات اللاسلكية أيضا[3]، لكن بالمقابل هناك بعض المحاولات ترمي إلى تعريف مراقبة الاتصالات الإلكترونية كإجراء قائم بذاته، فمنها من يعرفه بأنه: مراقبة شبكة الاتصالات، ومنها من يعرفه بأنه: العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكاناً أو شيئاً حسب طبيعته مرتبط بالزمن (التاريخ و الوقت) لتحقيق غرض أمني أو لأي غرض آخر[4]، لكن ما يؤخذ على التعريف الأول أنه من الاتساع وعدم التحديد ما يجعله غير مستوف للغرض منه وغير دال على المقصود به، ونفس الشيء

---

[1]– المادة الخامسة من المرسوم الرئاسي رقم 15–261 المؤرخ في الثامن أكتوبر من سنة 2015 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

[2]– ياسر الأمير فاروق، مرجع سابق، ص. ص. 20– 21.

[3]– نفس المرجع، ص. ص. 139– 140.

[4]– رشيدة بوكر، مرجع سابق، ص. 370.

بالنسبة للتعريف الثاني فقد توسع ليشمل عناصر ليست مستهدفة بصفة مباشرة بالمراقبة كالأمكنة مثلا كما توسع في الغرض منها لتشمل أغراض غير التي ينص عليها القانون في هذا الشأن والمحصورة في الوقاية ومكافحة جرائم محددة على سبيل الحصر[1].

محاولةً لاقتراح تعريف لإجراء مراقبة الاتصالات الإلكترونية استناداً لما جاء في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها يمكن القول بأنه:

ذلك الإجراء القائم على مجموعة من الشروط القانونية المحددة يهدف إلى تتبع وتفحص أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة تتم بواسطة أية وسيلة إلكترونية وذلك باستخدام التقنيات التكنولوجية الإلكترونية الحديثة، بغرض الوقاية من مجموعة جرائم محددة قانوناً على سبيل الحصر أو مكافحتها؛ وعليه هناك شرطان أساسيان للقول بوجود مراقبة إلكترونية للاتصالات وهما: وجوب أن تكون وسيلة الاتصال إلكترونية فيخرج الاتصال المباشر والعادي من هذا الإجراء ويدخل ضمن إجراء تسجيل الأصوات الذي سيتم التطرق له لاحقا، وكذلك وجوب أن تكون وسيلة المراقبة إلكترونية.

ثانيـاً- ضوابـط مراقبـة الاتصـالات الإلكترونيـة:

مما لا شك فيه أن إجراء مراقبة الاتصالات الإلكترونية يمس بحق الإنسان في الخصوصية وبحرمة مراسلاته وإتصالاته المحمية بموجب الدستور والمواثيق الدولية[2]، إلا أن هذا الحق المقرر للأفراد

---

[1]- تجدر الإشارة هنا إلى أن بعض الباحثين يستخدمون مصطلح المراقبة الإلكترونية للدلالة على معان وإجراءات مختلفة تماماً عما هو مقرر في القانون رقم 09-04، ومنها استخدامه للتعبير عن إجراء الترصد الإلكتروني، والذي يقصد به الإجراء القائم على استخدام تقنيات إلكترونية تتمثل عادةً في وضع طوق لا يمكن العبث به سواء في الرجل أو المعصم ويقوم برصد تحركات الشخص المراقب الذي يكون عادة متهماً أو محكوماً عليه لكن غير محبوس لمعرفة مكان تواجده وكذا الأمكنة التي يتردد عليها، كما قد يستخدم مصطلح المراقبة الإلكترونية للدلالة على الإجراءات والتقنيات المستخدمة عبر المطارات والموانئ أو حتى المحطات البرية للسفر بغرض مراقبة المسافرين وتحديد المشتبه فيهم والمبحوث عنهم ومنها تقنية برنامج حدقة العين والنظام القزحي، وتقنية برنامج بصمات الأصابع العشر وتقنية برنامج الاستهداف الآلي، راجع بخصوص هذه التقنيات وكذا المراقبة الجزائية الإلكترونية (الترصد الإلكتروني) الباحث: مصطفى محمد موسى، التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي، كتاب بدون دار أو بلد نشر، 2011، ص. ص. 280- 285.

[2]- تنص المادة 46 من الدستور على: "- لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون.
- سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.
- لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم".=

ليس حقاً مطلقاً بل يتم تقييده في كثير من الأحيان بمقتضيات حماية أمن الدولة والمجتمع ككل، لكن هذا التقييد يراعي دوما احترام هذا الحق من خلال حرص المشرع على إحاطة ممارسة هذا الإجراء بمجموعة ضوابط قانونية تضمن شرعيته، وهذه الضوابط تم النص على بعضها في المادة الرابعة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وأحال ذات القانون على قانون الإجراءات الجزائية فيما يخص البعض الآخر[1]، ويمكن إجمال هذه الضوابط فيما يلي:

أ- **الحالات التي يتم فيها اللجوء إلى مراقبة الاتصالات الإلكترونية:** بحيث قام المشرع الجزائري بتحديد الحالات التي يتم فيها اللجوء إلى مراقبة الاتصالات الإلكترونية وذلك على سبيل الحصر في متن المادة الرابعة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وهي:

1- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

2- في حالة توفر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني.

3- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

4- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[2].

ب- الإذن: بحيث نصت الفقرة الثانية من المادة الرابعة على أنه لا يمكن إجراء عمليات المراقبة في الحالات الذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة، ولم تحدد المقصود بالسلطة

= كما نصت المادة 12 من الإعلان العالمي لحقوق الإنسان على "لا يجوز أن يتعرض أحد لتدخل تعسفي في حياته الخاصة أو مراسلاته ولكل شخص الحق في الحماية القانونية ضد هذا التدخل".

[1]- تنص المادة الثالثة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على: "مع مراعاة الإحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

[2]- مع الأخذ بعين الاعتبار لما جاء في المادة 18 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تنص على: " يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام".

القضائية المختصة إلا فيما يخص حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة؛ بحيث تعود سلطة منح الإذن بإجراء المراقبة الإلكترونية للنائب العام لدى مجلس قضاء الجزائر وهذا لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، ولمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها[1]، وفي هذا الإطار نص المرسوم الرئاسي المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه تكلف مديرية المراقبة الوقائية واليقظة الإلكترونية التابعة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته بتنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها[2]، وفيما يخص الحالات الأخرى التي يتقرر فيها السماح بإجراء المراقبة الإلكترونية فيتم الرجوع إلى القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية لتحديد الجهة المختصة بمنح الإذن ومدته، فتكون هذه الجهة هي وكيل الجمهورية في حالة التحري وقاضي التحقيق في حالة فتح تحقيق قضائي ويتم منح هذا الإذن لضباط الشرطة القضائية، وتنفذ العمليات المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية في حالة التحري وتحت المراقبة المباشرة لقاضي التحقيق في حالة التحقيق القضائي، ويجب أن يتضمن الإذن تعريفاً بالعملية وطبيعة الجريمة التي تبرر الإجراء مع العلم بأنه إذا اكتشفت جرائم أخرى غير تلك الواردة في الإذن فهذا لا يكون سبباً لبطلان الإجراءات العارضة، ويسمح هذا الإذن لضابط الشرطة القضائية بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها وفي أي وقت شاء وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن، لكن دون المساس بالسر المهني، ويسلم الإذن مكتوباً لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق وضمن نفس الشروط الشكلية والزمنية[3]، ولكن وخلافاً لما نصت عليه المادة 65 مكرر 8 من قانون الإجراءات الجزائية والتي تجيز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر كل

[1]– الفقرة الثالثة من المادة الرابعة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]– المادة 11 من المرسوم الرئاسي رقم 15–261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3]– المواد 65 مكرر5 و 65 مكرر6 و65 مكرر7 من قانون الإجراءات الجزائية.

عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعملية المراد القيام بها، فإن المادة 41 من المرسوم الرئاسي رقم 15-261 المذكور سابقاً تنص على تولي الأعوان المؤهلين في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته ووحداتها المكلفة بالمراقبة لصالح ضباط الشرطة القضائية الجوانب التقنية للعمليات المنصوص عليها في قانون الإجراءات الجزائية؛ على اعتبار أنه لا يمكن تطبيق المادة 11 من ذات المرسوم والذكورة أعلاه لأنها وبحسب ما جاء فيها فهي مقررة فقط لحالة المراقبة الوقائية بمعنى تطبيقها فقط في الجرائم المنصوص عليها في الفقرة أ من المادة الرابعة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها دون بقية الجرائم الواردة في ذات المادة.

إن جرائم التجسس الإلكتروني عبارة عن جرائم ماسة بأمن الدولة من جهة وجرائم تستهدف منظومة معلوماتية على نحو يهدد الدفاع الوطني بمعنى أنها تطرح إشكالية الأحكام التي تخضع لها بخصوص الجهة مانحة الإذن هل هو النائب العام لدى مجلس قضاء الجزائر أم وكيل الجمهورية وقاضي التحقيق حسب الحالة، وهذه الإشكالية لا تطرح فقط بالنسبة للتجسس الإلكتروني بل تشمل كل الجرائم الإلكترونية الماسة بأمن الدولة ومنها مثلا الإرهاب الإلكتروني.

ج- الغـرض من المراقبـة الإلكترونيـة: يؤكد المشرع الجزائري من خلال الفقرة الأخيرة من المادة الرابعة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أن الغرض من الترتيبات الموضوعة لغرض الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة يجب أن تكون موجهة حصرياً لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير[1]، ولم يؤكد على هذا الغرض بالنسبة لبقية الحالات التي يلتجأ فيها إلى المراقبة التقنية لأن الجريمة فيها محددة بوضوح، بعكس الحالة التي أكد عليها المشرع؛ إذ أن الجريمة فيها غير قائمة أصلاً ويتم اللجوء للمراقبة الإلكترونية للوقاية من حدوثها،

[1]- تنص المادة 303 مكرر من قانون العقوبات على: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك: 1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه، 2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه، يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة....".

وفي كل الحالات لا يجوز استعمال المعلومات المتحصل عليها إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية[1].

الفـــرع الثانـــي: تفتيـش المنظومـات المعلوماتيـة وحجـز المعطيـات المعلوماتيـة.

يرتبط إجرائي تفتيش المنظومات المعلوماتية، وحجز أو ضبط المعطيات المعلوماتية من حيث كون الثاني غرض الأول وهدفه، كما يعتبر كلاهما إجراءً خاصاً ومختلفاً عن التفتيش والحجز التقليدي، وسيتم تبيان هذه الخصوصية من خلال تناول كل واحد من الإجرائين في عنصر مستقل.

أولاً- تفتيـش المنظومـات المعلوماتيـــة:

التفتيش عموماً هو البحث عن أدلة الجريمة وعن كل ما يمكن من نسبتها إلى شخص معين، وتفتيش المنظومات المعلوماتية لا يخرج عن هذا الإطار، لكن ما يميزه هو المحل الذي ينصب عليه والمتمثل في المنظومة المعلوماتية بكل مكوناتها المادية والمعنوية وسواء كانت هذه المنظومة منفصلة أم متصلة بغيرها من المنظومات عن طريق الشبكات الإلكترونية؛ فيكون بذلك إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات ودعامات تخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون جناية أو جنحة، والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها[2]، وقد نص المشرع الجزائري على إجراء تفتيش المنظومات المعلوماتية في المادة الخامسة من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وضمنها ضوابطه وشروط القيام به، ومحيلاً فيها كذلك على الأحكام العامة الواردة في قانون الإجراءات الجزائية، ويمكن إجمال هذه الشروط فيما يلي:

أ- ســبب التفتيـش فـي البيئـة الإلكترونيـة: يتمثل سبب التفتيش وفق القواعد العامة في وقوع جريمة ما جناية أو جنحة واتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها وتوافر قرائن وإمارات قوية على وجود أشياء تفيد في كشف الحقيقة لدى المتهم أو في مسكنه أو بشخص غيره أو

[1]- المادة التاسعة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]- عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، مداخلة مقدمة في المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 12- 14/ 11/ 2007.

مسكنه[1]، وهذه القواعد العامة لا تكون في أغلب الحالات سبباً لتفتيش النظم المعلوماتية بحيث تقرر المادة الخامسة من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أن الحالات التي يتم فيها التفتيش هي ذاتها المنصوص عليها في المادة الرابعة المتعلقة بالمراقبة الإلكترونية، وهذه الحالات كما سبق عرضه فيها ما يتعلق بجرائم لم تحدث بعد ولا وجود لمتهمين فيها وهي حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وحالة توفر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني، ويُعد التفتيش الممارس في هذه الحالة تفتيشاً وقائياً لا يتوقف على توافر الأسباب التي تدعو للتفتيش عادةً، أما الحالتين المتبقيتين وهما حالة التفتيش لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى تفتيش المنظومات المعلوماتية، وحالة التفتيش في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، فتخضع لضرورة توافر الأسباب العامة مذكورة سابقاً؛ وعليه فالتفتيش في حالة جرائم التجسس الإلكتروني لا يتطلب حودثاً فعلياً لها بل هو مجرد إجراء يهدف للوقاية منها ومنع حدوثها.

ب- محـــل التفتيـــش: محل التفتيش هو المنظومة المعلوماتية، وقد تم التوضيح سابقاً بأن هذه المنظومة تتكون من عناصر مادية وعناصر معنوية ولا توجد أي صعوبة بالنسبة للتفتيش الذي ينصب على المكونات المادية للنظام فهو يخضع للقواعد العامة المنصوص عليها في قانون الإجراءات الجزائية، وباعتبار التفتيش هنا يتعلق بجرائم ماسة بأنظمة المعالجة الآلية للمعطيات فهو يتجاوز الضمانات المقررة لتفتيش المساكن التي يمكن أن توجد بها مثل هذه المكونات المادية للنظام؛ بحيث لا يشترط حضور الشخص الذي يشتبه في أنه ساهم في ارتكاب الجريمة عند تفتيش مسكنه، كما أنه يجوز القيام بإجراء التفتيش في كل ساعة من ساعات النهار أو الليل ودون حاجة إلى رضائه عند القيام بهذا الإجراء[2]، وبالرجوع إلى المادة الخامسة من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نجد أن المشرع الجزائري قد ركز على تفتيش المكونات

[1]- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، مصر، 2010، ص. 99.

[2]- الفقرة الأخيرة من المادة 45 ، والفقرة الثالثة والرابعة من المادة 47 والفقرة الأخيرة من المادة 64 من قانون الإجراءات الجزائية.

المعنوية للمنظومة المعلوماتية وهذا ما يستفاد من صياغة المادة بقولها "يجوز ... **الدخول** بغرض **التفتيش** ولو عن بعد إلى: أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها . ب- منظومة تخزين معلوماتية" ، وقد استخدم المشرع هنا مصطلحي الدخول والتفتيش، ويتضمن هذا الأخير مفاهيم قراءة وتمحيص وبحث وفحص البيانات، وعلى العكس فإن كلمة الدخول وإن كانت ذات معنى محايد (بمعنى اشتمالها للتفتيش وغيره من المصطلحات) إلا أنها أكثر إلتصاقاً بالمصطلحات المعلوماتية، ويتم استخدام المصطلحين عموماً من أجل تنسيق المفاهيم التقليدية والمصطلحات الحديثة[1]، وباعتبار الدخول هنا مصطلح معلوماتي؛ فهو يستخدم للبيئة الإلكترونية وليس المادية، ويكون المشرع الجزائري بهذا قد حسم أمر الخلاف الفقهي حول صلاحية المكونات المعنوية للمنظومة للتفتيش[2] بإفرادها بنص خاص في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، آخذاً بالرأي الذي يقرر بأن معطيات الحاسوب قابلة للتفتيش لأنها عبارة عن نبضات أو ذبذبات إلكترونية وإشارات أو موجات كهرومغناطيسية قابلة لأن تسجل وتخزن على وسائط معينة ويمكن قياسها[3]، سواء كانت هذه الوسائط موجودة في ذات المنظومة المعلوماتية أو في منظومة تخزين مستقلة، وهي الحالات التي وضحها المشرع الجزائري في المادة الخامسة من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وبإعتبار أن المنظومة المعلوماتية قد تكون منفصلة كما قد تكون متصلة بغيرها من المنظومات مشكلة شبكة من المنظومات، فقد تكون هذه الأخيرة محصورة في المكان وبذلك لا تتجاوز حدود الدولة الواحدة، أو ممتدة في المكان فتكون بذلك موزعة على أكثر من دولة واحدة، فإن هناك إحتمال بأن الجاني لم يقم بتخزين المعطيات المبحوث عنها في المنظومة المعلوماتية التي يتم التفتيش فيها ولكن في منظومة معلوماتية أخرى متصلة بها سواء كانت واقعة في ذات الدولة أو كانت واقعة في دولة أخرى، والمشرع الجزائري قد تناول هذين الاحتمالين ونص على إمكانية إجراء التفتيش عن بعد مقرراً شروطاً خاصة بكل احتمال على حدة، وهذا كالآتي:

---

[1]- هلالي عبد اللاه أحمد، مرجع سابق، ص. ص. 248- 249.

[2]- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، مصر، 2010، ص. ص. 223- 224 .

[3]- عفيفي كامل عفيفي، مرجع سابق، ص. 364.

- **الحالة التي تكون فيها المنظومات المعلوماتية موجودة في الجزائر**: بحيث إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقاً من المنظومة الأولى فيجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقاً بذلك[1]، والملاحظ هنا أن المشرع لم يشترط أن تكون المنظومة المعلوماتية الثانية ملكاً للمتهم فقد تكون له أو لشخص آخر يعلم أو لا يعلم بوجود هذه المعطيات في منظومته، وتجب الإشارة هنا إلى إمكانية تعدد المنظومة الثانية، كما أن هناك ملاحظات تُبدى بشأن السلطات التي يتم إعلامها سيتم التطرق إليها في صدد الحديث عن الإذن.

- **الحالة التي تكون فيها المنظومات موزعة بين الجزائر ودولة أخرى**: بحيث إذا تبين بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقاً من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة ووفقاً لمبدأ المعاملة بالمثل[2]، وما يثير التساؤل هنا هو الحالة التي يكون التفتيش فيها وقائياً فهل يمكن إعمال هذه الإجراءات بشأنه خاصة لتعلقه بمعطيات لها صلة بأمن الدولة والدفاع الوطني، وهو الأمر المستبعد.

ج- السلطة المختصة بالتفتيش: لم تتضمن المادة الخامسة المنظمة لإجراء التفتيش النص على السلطات القائمة به، ولا على ضرورة وجود إذن بتفتيش المنظومة المعلوماتية، واكتفت بالإحالة على قانون الإجراءات الجزائية، فجاء بذلك النص غامضاً غير محدد المعاني؛ إذ تنص الفقرة الأولى من المادة الخامسة من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية ..."، وقد تدخل المشرع الجزائري لاستجلاء هذا الغموض بعض الشئ من خلال المرسوم الرئاسي المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ليحدد السلطة المختصة بالتفتيش، ولكن في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة فقط، بمعنى في حالة التفتيش الوقائي تكون الهيئة هي السلطة المكلفة والمخولة بذلك، لكن المادة لم تشر صراحةً إلى مديرية المراقبة

[1]- الفقرة الثانية من المادة الخامسة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]- الفقرة الثالثة من المادة الخامسة من نفس القانون.

الوقائية واليقظة الإلكترونية بذلك التكليف، لكن يفهم من سياق النص أنها المقصودة بذلك[1]، وبحسب ذات المادة فإن التفتيش يتم تحت سلطة قاض مختص وفقاً للأحكام المنصوص عليها في المادة الرابعة من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ وعليه بالرجوع لهذه المادة فالقاضي المختص هو النائب العام لدى مجلس قضاء الجزائر، أما في حالة الجرائم الأخرى فيتم الرجوع فيها إلى قانون الإجراءات الجزائية والذي نجده ينظم مسألة تفتيش المساكن مما يوحي بأن الإذن بتفتيش المسكن ينصرف إلى ما يحويه هذا المسكن ومنه المنظومة المعلوماتية، فتكون السلطة المختصة بالتفتيش إما قاضي التحقيق أو وكيل الجمهورية واللذان يأذنان لضباط الشرطة القضائية بالقيام به، على أن يكون الإذن مكتوباً مع وجوب استظهاره قبل الدخول إلى المنزل أو الشروع في التفتيش، وأن يكون هذا الإذن متضمناً تحت طائلة البطلان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي ستتم زيارتها وتفتيشها[2]. إلا أن القيام بتفتيش المنظومة المعلوماتية يطرح عديد الصعوبات والإشكالات التي لا يمكن الاستناد لحلها على قانون الإجراءات الجزائية، فالإذن يستوجب تحت طائلة البطلان أن يحدد بدقة الأماكن التي سيتم تفتيشها لكن البيئة الرقمية من الإتساع بحيث تخزن ملايين البيانات والملفات المرتبطة ببعضها مما يستحيل معه التحديد، كما أن التفتيش قد يمتد لمنظومة معلوماتية موجودة في مسكن آخر مما يستلزم نص الإذن على ذلك أو استصدار إذن جديد، لكن المشرع تدخل هنا باستبعاد استصدار إذن جديد بحيث قرر في المادة الخامسة من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الاكتفاء بمجرد إعلام السلطات المختصة مسبقاً بتمديد التفتيش، ويتضح من هذا أن قواعد التفتيش المنصوص عليها في قانون الإجراءات الجزائية قررت أساساً لتفتيش المساكن وليس لتفتيش المنظومة المعلوماتية؛ مما يستلزم معه أن يحدد المشرع قواعد خاصة لها تنفصل عن القواعد التقليدية.

---

[1]– حيث تنص المادة 21 من المرسوم الرئاسي رقم 15–261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على: "قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة تكلف الهيئة حصرياً بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية تحت سلطة قاض مختص ووفقاً للأحكام المنصوص عليها في المادة الرابعة من القانون رقم 09–04"، وعليه بما أن الجهة المكلفة داخل الهيئة بالمراقبة الإلكترونية هي مديرية المراقبة الوقائية واليقظة الإلكترونية فينسحب ذلك على جميع الإجراءات الأخرى لأن المشرع ذكرها جميعا في ذات النص ولم يخص المراقبة الإلكترونية بنص خاص بها.

[2]– المادة 44 من قانون الإجراءات الجزائية.

د- التسخير: بحيث يمكن للسلطات المختصة بالتفتيش، وهي وكيل الجمهورية أو قاضي التحقيق وكذا لضباط الشرطة القضائية المأذون لهم، أن يكلفوا أي شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو له دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها[1].

ثانياً- حجز المعطيات المعلوماتية:

إن الغرض من التفتيش هو ضبط الأدلة التي تفيد في ظهور الحقيقة، فالضبط في معظم الأحوال هو غرض التفتيش وإن لم يكن هو السبب الوحيد؛ فقد يتم الضبط استناداً لأسباب أخرى غير التفتيش كالمعاينة وما يقدمه المتهم والشهود للسلطات المختصة[2]، وقد نص المشرع الجزائري على هذا الإجراء في المادة السادسة من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مستخدماً مصطلح الحجز، حاسماً بذلك الجدل القائم حول مدى قابلية المعطيات المعلوماتية للحجز[3]، مقرراً صلاحيتها لذلك، وهذا باعتبار أن المكونات المادية للنظام لا يثير حجزها أي إشكالية فهي تخضع للقواعد العامة المقررة في قانون الإجراءات الجزائية، وباعتبار أن المعطيات المعلوماتية عبارة عن ذبذبات إلكترونية فلا يمكن حجزها بالطرق التقليدية؛ لذا فقد نص المشرع الجزائري على أساليب حجزها في المادة السادسة ذاتها، ويمكن إجمالها في عنصرين هما:

أ- أسلوب نسخ المعطيات المعلوماتية: فعندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة؛ يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها كالبرامج مثلا على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز[4].

ب- الحجز عن طريق منع الوصول إلى المعطيات: ويسمى هذا الأسلوب كذلك بالتجميد، بحيث إذا استحال إجراء الحجز وفقاً لطريقة النسخ لأسباب تقنية، يستوجب على السلطة القائمة بالتفتيش

---

[1]- الفقرة الأخيرة من المادة الخامسة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2007، ص. 207.

[3]- زيدان زيبحة، مرجع سابق، ص. 149.

[4]- الفقرة الأولى من المادة السادسة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة[1]، كما أجاز المشرع الجزائري للسلطات القائمة بالتفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك[2].

الفـــرع الثالـث: حفظ المعطيات المتعلقـة بحركة السير واعتراض المعطيات المتعلقة بالمحتـوى.

يُعد إجرائي حفظ المعطيات المتعلقة بحركة السير واعتراض المعطيات المتعلقة بالمحتوى أكثر الإجراءات حداثة فيما يخص الوقاية والمكافحة في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال عموماً، وسيتم تناول كل إجراء في عنصر مستقل.

أولاً- حفــظ المعطيـات المتعلقـة بحركــة السيـــر:

وهو إجراء إستحدثه المشرع الجزائري ونص عليه في المادة 11 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لكنه لم يعرفه، وعموماً يقصد بحفظ المعطيات المتعلقة بحركة السير أو ما يسمى كذلك بمعطيات المرور، تجميع أو تسجيل البيانات المتعلقة بخط سير البيانات في الوقت الفعلي عن طريق إلزام مقدم الخدمة بذلك في حدود قدرته الفنية بهدف تسهيل مهمة الجهات القائمة بجمع الأدلة في التعرف على مرتكب الجريمة الإلكترونية والمساهمين معه في ارتكابها[3]. وقد اكتفى المشرع الجزائري في ذلك بتعريف مقدمي الخدمة وكذا المعطيات المتعلقة بحركة السير بحيث عرف هذه الأخيرة في الفقرة "ه" من المادة الثانية من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنها: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءاً من حلقة اتصالات توضح مصدر الاتصال والوجهة المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة، بينما عرف مقدمي الخدمات في الفقرة "د" من ذات المادة بأنهم: أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات، وأي كيان آخر

[1]- المادة السابعة من قانون الوقاية من االجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]- المادة الثامنة من نفس القانون.

[3]- مفتاح بوبكر المطردي، مرجع سابق.

يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها، ورغم قيام المشرع بتعريف المعطيات المتعلقة بحركة السير إلا أنه عاد وحدد نوع المعطيات التي يجب على مقدمي الخدمات أن يحفظوها، وهي المعطيات التي تسمح بالتعرف على مستعملي الخدمة والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال والخصائص التقنية وكذا تاريخ ووقت ومدة الاتصال والمعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها والمعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها[1]، وفي هذا الإطار لم يكتف المشرع الجزائري بإلزام مقدمي خدمات الأنترنت بحفظ هذه المعطيات وإنما ألزم كذلك متعاملي الهاتف بذلك رغم أن إلتزامهم أكثر تحديداً وحصراً؛ بحيث يلزمون فقط بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة وكذلك تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه[2]، وقد حددت المادة 11 مدة حفظ المعطيات بالنسبة لكل من مقدمي الخدمة ومتعاملي الهاتف بسنة واحدة تحتسب ابتداءً من تاريخ التسجيل[3].

ثانيـاً- اعتـراض المعطيـات المتعلقـة بالمحتـوى:

نص المشرع الجزائري على هذا الإجراء بطريقة غير مباشرة من خلال المادة العاشرة من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بحيث نص على أنه: "يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها ..."، ويقصد باعتراض المعطيات المتعلقة بالمحتوى تجميع البيانات التي تشير إلى المحتوى الإخباري للاتصال، بمعنى مضمون الاتصال أو

---

[1]- الفقرة الأولى من المادة 11 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]- الفقرة الثانية من المادة 11 من نفس القانون.

[3]- نظراً لأهمية إجراء حفظ المعطيات المتعلقة بحركة السير فقد قرر المشرع الجزائري عقوبات لمقدمي الخدمة ومتعاملي الهاتف نظير عدم احترام الالتزامات المقررة في المادة 11 من القانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ بحيث نصت في فقرتيها ما قبل الأخيرة والأخيرة على: "دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية ويعاقب الشخص الطبيعي بالحبس من ستة أشهر إلى خمس سنوات وبغرامة من 50.000 دج إلى 500.000 دج. يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات ...".

الرسالة أو المعلومات المنقولة عن طريق الاتصال[1]؛ وعليه يكمن الفرق بين المعطيات المتعلقة بالمرور والمعطيات المتعلقة بالمحتوى في أن الأولى تغطي فقط المعطيات المنتجة خلال نقل المعطيات ولكن لا تغطي المعطيات المنقولة بمعنى الكلمة، كما أن الدخول إلى المعطيات المتعلقة بالمحتوى يمكن السلطات من تفحص طبيعة الرسائل والملفات المتبادلة أما معطيات المرور فتمكن من كشف هوية مرتكب الجريمة دون معرفة محتوى الاتصال، كما أن الصعوبات التي تواجه إجراء حفظ المعطيات المتعلقة بالمرور تتمثل في إمكانية استخدام الجناة لخدمات على الأنترنت تسمح بإجراء اتصالات مجهولة وسرية أو استخدام نهايات طرفية عمومية (كالاتصال من مقهى أنترنت مثلاً) فهذا الإجراء لن يمكن من كشف المرسل[2]، أما أهم الصعوبات التي تواجه إجراء اعتراض المعطيات المتعلقة بالمحتوى فهو لجوء الجناة إلى تكنولوجيا التشفير مما يسمح لهم حماية المحتويات المتبادلة بصورة يستحيل معها على سلطات التحقيق الدخول إليها، كما أن فك الشفرات قد يتطلب وقتاً طويلاً[3]، ورغم خصوصية هذا الإجراء فالمادة العاشرة التي نصت عليه جاءت عامة ولم تتضمن شروطه أو ضوابطه كما أن صياغتها لا تدل بشكل قاطع على الإحالة إلى المادة 11 السابقة الذكر فيما يخص إخضاعه لذات الشروط التي يخضع لها إجراء حفظ معطيات المرور، وكل ما نصت عليه المادة العاشرة هو إلزام مقدمي الخدمات بكتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، لكن المشرع الجزائري عاد ونص في المادة 21 من المرسوم الرئاسي المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أن الهيئة هي المكلفة حصرياً بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، وذلك في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة.

[1]– هلالي عبد اللاه أحمد، مرجع سابق، ص. 266.

[2]-Marco Gerck, comprendre la cybercriminalité: guide pour les pays en développement, union Internationale des télécommunications, suisse, 2009, p. 222-223, ouvrage publié sur le site:www.itu.int/ITU-D/cyb/cybersecurity/législation.html, le site a été visité le: 04/02/2015.

[3]- Ibid, p. 226.

المطلب الثالث: إجراءات متابعة جرائم التجسس الإلكتروني في ظل قانون الإجراءات الجزائية.

تُعد الإجراءات السابق دراستها في المطلب الثاني إجراءات خاصة نص عليها المشرع في قانون خاص أيضا؛ وعليه تبقى جرائم التجسس الإلكتروني تخضع لإجراءات التحري والتحقيق الأخرى المنصوص عليها في قانون الإجراءات الجزائية، رغم أن هذا الأخير أيضاً قد خص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بقواعد تخرج عما هو مألوف ومقرر لبقية الجرائم والمتمثلة في إجراءات التحري الخاصة، وفي مقابل هذه القواعد الجديدة والخاصة هناك قواعد تقليدية لكن ما يجعلها هي الأخرى خاصة هو تطبيقها على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؛ وعليه سيتم تقسيم هذا المطلب لفرعين: يتناول الفرع الأول إجراءات التحري والتحقيق التقليدية في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ويتناول الفرع الثاني إجراءات التحري الخاصة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

الفرع الأول: إجراءات التحري والتحقيق التقليدية في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

يتضمن قانون الإجراءات الجزائية كقاعدة عامة النص على الإجراءات المتبعة في شأن كل الجرائم دون استثناء، لكن بالمقابل هناك جرائم تفرض وتضفي طابعاً خاصاً على هذه الإجراءات التقليدية؛ فتصبح بذلك إجراءات خاصة نظراً لخصوصية الجريمة المتبعة بمناسبتها، ومن أبرز هذه الإجراءات الشهادة والخبرة، والتي سيتم تناول كل واحدة منها في عنصر مستقل.

أولاً- الشهادة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

تُعرف الشهادة بصفة عامة بأنها: الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته منها.

تُعد الشهادة من أقدم وأبرز وسائل الإثبات والحصول على الأدلة في كافة طوائف الجرائم، وهي من حيث الأهمية لا تختلف بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، لكنها تصبح في هذا الصدد ذات طبيعة خاصة ترجع إلى خصوصية الشاهد فيها؛ بحيث يختلف من حيث صفته عن

غيره من الشهود في الجرائم التقليدية؛ فغالباً ما يكون من أصحاب المعرفة التقنية بالنظام المعلوماتي وذلك بحكم عمله ولا يقصد بذلك أن يكون الشاهد خبيراً بل كلاهما يختلف عن الآخر حيث يقدم هذا الأخير تقارير وآراء توصل إليها بتطبيق قوانين علمية وأصول علمية أما الشاهد فيقدم معلومات حصلها بالملاحظة الحسية[1].

يُقصد بالشاهد في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي والذي تكون لديه معلومات جوهرية ولازمة للدخول في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب على أدلة الجريمة داخله ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي[2]، والشاهد بهذا المعنى يشمل عديد الطوائف أهمها: مشغلوا الحاسب الآلي وخبراء البرمجة والمحللون ومهندسوا الصيانة والاتصالات ومديروا النظم[3]، وبالإضافة إلى هذه الفئة هناك أشخاص آخرون يعدون بمثابة شهود في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بحكم دورهم في توصيل طالب الخدمة أو المستهلك إلى شبكة الأنترنت وهم مقدموا الخدمات الوسيطة في مجال المعلوماتية والأنترنت ومن هؤلاء متعهدوا الوصول ومتعهدوا الإيواء وناقلوا المعلومات على شبكة الأنترنت ومتعهد الخدمات ومورد المعلومات ومؤلف الرسالة[4].

ويخضع الشهود المعلوماتيون لذات القواعد العامة والمعروفة لسماع الشهود بغض النظر عن صفتهم والمقررة في قانون الإجراءات الجزائية في المواد من 88 إلى 99، لكن تجب الإشارة هنا إلى

---

[1]– عائشة بن قارة مصطفى، مرجع سابق، ص. ص. 125– 126.

[2]– إبراهيم محمد منصور الشحات، الجريمة الإلكترونية (في الشريعة الإسلامية والقوانين الوضعية)، دار الفكر الجامعي، مصر ، 2011، ص. 197.

[3]– يُقصد بمشغلي الحاسب الآلي الخبراء الذين تكون لهم الدرية التامة بتشغيل جهاز الحاسب الآلي والمعدات المتصلة به واستخدام لوحة المفاتيح في إدخال البيانات وتكون لديهم معلومات عن قواعد كتابة البرامج، أما خبراء البرمجة فهم الأشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين: الفئة الأولى تتضمن مخططي برامج التطبيقات ومخططي برامج النظم، أما المحللون فهم الأشخاص الذين يحللون الخطوات ويقومون بتجميع بيانات نظام معين وتحليلها إلى وحدات منفصلة واستنتاج العلاقات الوظيفية منها كما يقومون بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات، أما مهندسوا الصيانة والاتصالات فهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به، أما مديروا النظم فهم الذين توكل لهم أعمال الإدارة في النظم المعلوماتية، أنظر: عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري ، مرجع سابق.

[4]– عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص. ص. 39– 41.

طبيعة التزامات الشاهد في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؛ فكون الشاهد المعلوماتي الشخص الوحيد الذي بإمكانه معرفة كلمات المرور والشفرات الخاصة بالبرامج المختلفة التي استعان بها الجاني لارتكاب جريمته والتي قد لا يمكن للخبير المنتدب من الجهة القضائية أن يعرفها أو يتمكن من التوصل إليها في الوقت اللازم مما قد يؤدي إلى تضييع الأدلة وإفلات الجاني؛ قد أثار الجدل حول مدى إمكانية إلزام هذا الشاهد على تقديم الدليل الفني في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فيذهب إتجاه للقول أنه ليس من واجب الشاهد وفقاً للالتزامات التقليدية للشهادة أن يقوم بطباعة البيانات المخزنة في ذاكرة الحاسوب أو تحليل ذاكرة النظام المعلوماتي ليكشف له عن آثار بعض البيانات، أو تقديم المعلومات اللازمة لاختراقه كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة، بينما يذهب إتجاه آخر إلى عكس هذا فيجعل من كل هذه الأمور التزامات تقع على عاتق الشاهد المعلوماتي باستثناء حالات المحافظة على سر المهنة فإنه يكون في حل من هذه الالتزامات[1]. وبالرجوع إلى مواد قانون الإجراءات الجزائية نجد أن المشرع الجزائري قد ألزم الشاهد بالحضور وبأداء اليمين عند الاقتضاء وبالإدلاء بشهادته لكنه لم يتضمن أي نص صريح يلزم الشاهد بالقيام بعمل معين؛ لذا ينبغي التدخل بخص الشاهد المعلوماتي بنصوص قانونية تلزمه بتقديم المساعدة للجهات القضائية وبالمحافظة على سرية الإجراءات التي يقوم بها نظراً لخصوصية وتفرد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ومنها تحديداً التجسس الإلكتروني، وذلك عن طريق إضافة التزام جديد ومستقل عن بقية التزامات الشاهد التقليدية، وهو ما يعرف فقهاً بالالتزام بالإعلام، ويعني أنه ومتى كان الشاهد حائزاً على معلومات لازمة لاختراق نظام معالجة آلية للمعطيات بحثاً عن أدلة للجريمة داخله تتطلبها مصلحة التحقيق، فإنه يكون مطالباً بأن يعلم بها السلطات القائمة على التحقيق على سبيل الإلزام، ويتضمن هذا الإعلام طبع ملفات البيانات المخزنة في ذاكرة الحاسب الآلي أو حاملات البيانات الثانوية طالما اقتضت مصلحة التحقيق ذلك، وكذلك الإفصاح عن كلمات المرور السرية والكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة[2].

[1]– عائشة بن قارة مصطفى، مرجع سابق، ص. ص. 130– 131.

[2]– عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص. ص. 340– 345.

ثانياً- الخبرة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

إن خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تنبع كما سبق توضيحه من لامادية سلوكاتها الإجرامية والتي تنفذ في بيئة غير مرئية؛ الأمر الذي استتبع أن تكون مخلفات هذه الجريمة أيضا لا مادية وغير ملموسة؛ الأمر الذي بدوره ألزم الاستناد في إثبات وقوع هذه الجرائم ونسبتها إلى فاعلين معينين على أدلة من ذات الطبيعة ومستخرجة من ذات البيئة؛ فالأدلة بهذا الشأن عبارة عن دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة، وهي ليست كما يقول البعض أقل مادية من الأدلة المادية فحسب بل تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعين[1]؛ وعليه تطرح هذه الأدلة الإلكترونية أو الرقمية صعوبة التعامل معها إن في مرحلة جمعها أو تخزينها أو إعادة بناءها لتقديمها لقضاء الحكم لتكون بذلك دلائل لها حجية مطلقة لا يرقى إليها الشك في مدى صحتها وإثباتها للجرائم؛ لذا يتم الاستناد في جميع مراحل التعامل المذكورة معها إلى وجود خبراء متخصصين في هذا المجال، فالخبرة في إطار الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تتجاوز من حيث الأهمية تلك المرتبطة بالجرائم التقليدية؛ لأن هذه الأخيرة تنتج آثاراً مادية يمكن التعامل معها بسهولة مقارنة مع الآثار اللامادية التي تتطلب خبرة في ذلك، كما لا يتحدد دور الخبرة هنا بمرحلة معينة من الدعوى العمومية بل هي إجراء لصيق بكل مراحلها ولا يمكن الاستغناء عنها فهي متطلبة من لحظة تجميع الأدلة إلى لحظة عرضها على قضاة الحكم، ونظراً لأهمية المعرفة الفنية في هذا المجال وعدم إمكانية الاعتماد الكلي على الخبراء في هذا المجال؛ فالأمر يتطلب تأهيل رجال الضبط وسلطات التحقيق لإنجاح متابعة مثل هذه الجرائم؛ وهذا درءاً لما ينادي به البعض من أنه يمكن للخبير نفسه أن يحدد إطار مهمته إذ أن هذا الأمر من شأنه تقويض دور المحقق والقاضي في الدعوى الجنائية[2]، وجعلهم تابعين لآراء أفراد لا يعدون جزءاً من جهاز العدالة وإن كانوا مساعدين له، حتى أنه قد وجدت شركات عالمية متخصصة في تحقيق الجرائم المعلوماتية حققت نجاحاً في كثير من المجالات لكن الأمر فيه تنازل واضح عن سلطات منوطة بالأساس بجهاز العدالة وبالدولة وفيه مخاطرة بالمساس بأسرار قضايا حساسة؛ وهذا ما دفع كل الدول إلى العمل على تأهيل أفراد السلطة القضائية في هذا المجال لإكسابهم المهارات والمعرفة الفنية

[1]- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص. 235.

[2]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص. 329.

بكل ما يتصل بتقنية المعلومات والاتصالات[1]، بل وأصبح للسلطة القضائية أجهزة خاصة مكلفة بإنجاز الخبرات في هذا المجال، وهو ذات التوجه الذي أخذ به المشرع الجزائري، بحيث أحدث المعهد الوطني للأدلة الجنائية وعلم الإجرام[2] وهو مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي تعمل تحت وصاية وزير الدفاع الوطني ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه وبهذه الصفة فإنه يخضع إلى جميع الأحكام التشريعية والتنظيمية المطبقة على المؤسسات العسكرية[3]، ويكلف هذا المعهد بناء على طلب من القضاة والمحققين أو السلطات المؤهلة بإجراء الخبرات والفحوص العلمية التي تخضع لاختصاص كل طرف في إطار التحريات الأولية والتحقيقات القضائية بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح[4]، ويحتوي هذا المعهد على قسم الإعلام الآلي يختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية وإلى جانبه يوجد مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية تابع أيضا لقيادة الدرك الوطني أما على مستوى المديرية العامة للأمن الوطني فتوجد مخابر الشرطة العلمية التابعة لمديرية الشرطة القضائية، ومن الفروع التقنية التي تضمها هذه المخابر خلية الإعلام الآلي والتي تختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية بناء على تسخيرات أو إنابات قضائية[5]، وحتى تكتمل قدرات هذه الأجهزة فقد تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته[6]، ومن بين مهام هذه الهيئة مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية[7]، كما نص المرسوم الرئاسي المحدد لتشكيلة وتنظيم وكيفيات سير هذه الهيئة، على تكليفها بمساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال الخبرات

---

[1]– راجع أكثر كتاب خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص. ص. 182– 189.

[2]- أحدث المشرع الجزائري المعهد الوطني للأدلة الجنائية وعلم الإجرام بموجب المرسوم الرئاسي رقم 04 – 183 المؤرخ في 26 يونيو من سنة 2004

[3]– المادة الثانية من نفس المرسوم الرئاسي.

[4]– المادة الرابعة من نفس المرسوم الرئاسي.

[5]– نسيم سعيداني، مرجع سابق، ص. 189.

[6]– تم إنشاء هذه الهيئة تطبيقاً المادة 13 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[7]– المادة 14 من نفس القانون.

القضائية وكذلك المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال[1].

تلعب الأجهزة السابقة دوراً مهما في مساعدة السلطات القضائية في التحري والتحقيق في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من خلال بحث وإعداد الدليل الإلكتروني الذي يؤدي إلى إثبات الجريمة ومدى نسبتها إلى شخص معين، لكن بالرغم من ذلك تبقى دوماً أعمال الخبرة آراءً إستشارية لإنارة القاضي ولا تقيده فيجوز له أن يأخذ بها أو يطرحها[2].

الفـــرع الثانـــي: إجـراءات التحـري الخاصـة في الجرائـم الماسة بأنظمة المعالجـة الآليـة للمعطيـات.

إجراءات التحري الخاصة وكما تشير إلى ذلك تسميتها هي إجراءات استثنائية قررها المشرع لطوائف من الجرائم محددة على سبيل الحصر ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؛ بحيث تخرج هذه الإجراءات في ممارستها عن الضوابط المقررة لبقية الإجراءات، وسيخصص هذا الفرع لدراسة إجراءات تسجيل الأصوات والتقاط الصور والتسرب، وسيتم خص كل واحد منها بعنصر مستقل.

أولاً- إجـراء تسجيـل الأصـوات وإجـراء التقـاط الصـور:

نص المشرع الجزائري على هذين الإجرائين في المادة 65 مكرر5 من قانون الإجراءات الجزائية، وما يميزهما عن إجراء المراقبة الإلكترونية وكذا اعتراض المراسلات السلكية واللاسلكية أنهما لا يتضمنان أي نوع من الاتصالات التي تتم عن طريق الوسائل الإلكترونية مهما كان نوعها بحيث يتمان في حالة شخص متواجد بمفرده أو عدة أشخاص في حالة تواصل عادي بدون الاعتماد على وسيلة اتصال كواسطة بينهم.

ويقصد بإجراء تسجيل الأصوات حسب ذات المادة: وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه بصفة خاصة أو سرية من طرف شخص أو عدة

[1]- المادة الرابعة من المرسوم الرئاسي المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]- رشيدة بوكر، مرجع سابق، ص. 429.

أشخاص في أماكن خاصة أو عمومية، ومن خلال هذا التعريف القانوني يستنتج أن الإجراء يستهدف أغراض معينة، ومحلاً معيناً، ويتم بوسائل معينة، حسب التوضيح التالي:

أ- أغراض إجراء تسجيل الأصوات: يهدف هذا الإجراء إلى الالتقاط، ويقصد به التنصت، وهو الاستماع إلى الحديث خلسة، وإلى البث ويقصد به نقل الحديث الذي تم الاستماع إليه أو تسجيله من المكان الذي يتم فيه التسجيل إلى مكان آخر باستخدام وسيلة تقنية، ويقصد بالتسجيل حفظ الحديث على الأشرطة المخصصة لذلك لإعادة الاستماع إليها من بعد، وهو بهذا يشير إلى ذات المقصود بالتثبيت رغم أن هذا المصطلح قد يتعلق بالصورة أكثر من الصوت بحيث يجعلها غير متحركة أي ثابتة من حيث المكان والزمان.

ب- محل إجراء تسجيل الأصوات: ينصب هذا الإجراء على الأحاديث الخاصة والسرية دون العامة، ويعني الحديث كل صوت له دلالة التعبير عن معنى أو مجموعة من المعاني والأفكار المترابطة سواء كانت هذه الدلالة مفهومة لجمهور الناس أو لفئة محددة منهم، ومن ثم يُعد حديثاً ذلك الذي يتم بلغة أجنبية أو باستعمال الشفرة[1]، والملاحظ أن المشرع لم يقصر هذا الإجراء على الأحاديث التي تدور بين شخصين أو أكثر بل يشتمل أيضاً على حديث الشخص بمفرده وهي حالة من يفكر بصوت مرتفع، كما لم يشترط مكاناً معيناً يتم في هذا الحديث فيستوي أن يكون مكاناً خاصاً أو عاماً كالمساكن وملحقاتها والشوارع والحدائق والمطارات والمنشات الرياضية وغيرها.

ج- وسائل إجراء تسجيل الأصوات: يستوجب المشرع أن يتم هذا الإجراء بواسطة أدوات تقنية مخصصة لهذا الغرض؛ وعليه لا يعتد بالتقاط الأحاديث باستخدام الأذن، وقد شهدت هذه الأدوات التقنية تطوراً ملفتاً في الشكل والكفاءة[2].

ويُقصد بإجراء التقاط الصور حسب المادة السابقة وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص، وعرفه البعض بأنه: استعمال وسائل تقنية أو معدات تمكن من أخذ صور للمتورطين في جرائم محددة سواء من خلال آلة للتصوير أو كاميرا فيديو للحصول على فيلم يسمح بمعاينة الأحداث مرة ثانية من خلال تقنية الإعادة البطيئة التي

[1]- ياسر الأمير فاروق، مرجع سابق، ص. ص 145- 146.

[2]- كوثر أحمد خالند، الإثبات الجنائي بالوسائل العلمية، مكتب التفسير للنشر والإعلان، أربيل، 2007، ص. 223.

يمكن الوقوف من خلالها على كل ما يهم في التحري والتحقيق[1]؛ وعليه فغرض هذا الإجراء هو التقاط الصور وبداهة يختلف مفهوم الالتقاط هنا عن ذلك المقصود بإجراء تسجيل الأصوات، ولم يشترط المشرع وسيلة تقنية معينة لالتقاط الصور فلا تنحصر في مجرد آلات التصوير العادية التي تثبت الصورة، ولكن تشمل أساساً كاميرات الفيديو، وعادة ما تقوم تقنيات المراقبة البصرية هذه بالتقاط الصورة والصوت معاً[2]. أما محل هذا الإجراء فهو القيام بتصوير شخص واحد أو مجموعة من الأشخاص. وبعكس إجراء التقاط الأصوات فقد حصر المشرع إجراء التقاط الصور في الأماكن الخاصة دون العامة، وفي هذا الإطار تجدر الإشارة إلى أن المشرع الجزائري قد نظم عمليات التقاط الصور إن صح التعبير في الأماكن العامة ولأغراض محددة، وذلك بموجب المرسوم الرئاسي المحدد للقواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو وسيره[3]، ويشكل هذا النظام حسب ذات المرسوم أداة تقنية للاطلاع والاستباق تهدف إلى المساهمة في عديد المجالات وتحديداً في مكافحة الإرهاب والوقاية من الأعمال الإجرامية وتأمين البنايات والمواقع الحساسة وذلك من خلال تحسين مستوى عمل الجهات المختصة عبر تزويدها في الوقت الحقيقي بالأخبار والمعلومات الكفيلة بمنع ارتكاب الجرائم أو الجنح أو مكافحتها بفعالية و/ أو تسهيل التعرف على مرتكبيها وإلقاء القبض عليهم[4].

إن كلاً من إجراء تسجيل الأصوات، وإجراء التقاط الصور يحكمهما مجموعة من الضوابط، يمكن إجمالها في العناصر الآتية:

أ- **الجرائم المعنية بالإجرائين:** إن الجرائم التي يتم بمناسبتها القيام بإجرائي تسجيل الأصوات والتقاط الصور محددة على سبيل الحصر ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ب- الإذن: بحيث يستلزم القيام بالإجرائين ضرورة وجود إذن مسبق بذلك يمنح لصالح ضابط الشرطة القضائية الذي يباشرهما، ويتم منح هذا الإذن في حالة التحري من قبل وكيل الجمهورية المختص والذي يتولى المراقبة المباشرة للعمليات المأذون بها، وفي حالة فتح تحقيق قضائي يتم منح الإذن من قبل

---

[1]- هشام ساحلي، أساليب التحري الخاصة ومدى مساسها بحرمة تنقل الفرد في التشريع الجزائري، مجلة الحقوق للبحوث القانونية والاقتصادية، العدد الثاني، كلية الحقوق، جامعة الإسكندرية، مصر، 2014، ص. 865.

[2]- كوثر أحمد خالند، مرجع سابق، ص. 226.

[3]- المرسوم الرئاسي رقم 15- 228 المؤرخ في 22 أوت من سنة 2015 والذي يحدد القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو وسيره

[4]- المادة الثانية والمادة الثالثة من نفس المرسوم الرئاسي.

قاضي التحقيق والذي يتولى أيضاً المراقبة المباشرة للعمليات المأذون بها، وفي الحالتين يسمح الإذن الممنوح بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من قانون الإجراءات الجزائية أي قبل الساعة الخامسة صباحاً وبعد الساعة الثامنة مساءاً، وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن[1]، لكن دون المساس بالسر المهني[2]، ويجب أن يتضمن هذا الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، ويسلم الإذن مكتوباً لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية[3].

ج- المكلفون بالجوانب التقنية لعمليات تسجيل الأصوات والتقاط الصور: حسب المرسوم الرئاسي المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يتولى الأعوان المؤهلون في الهيئة ووحداتها المكلفة بالمراقبة لصالح ضباط الشرطة القضائية الجوانب التقنية للعمليات المنصوص عليها في قانون الإجراءات الجزائية[4]، ومن بينها بداهة إجرائي تسجيل الأصوات والتقاط الصور، وهنا يثور التساؤل حول جدوى نص المادة 65 مكرر 8 التي تجيز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر 5، في ظل وجود نص جديد يحدد الجهة التي تقوم بوضع هذه الترتيبات.

د- محضر العمليات: بحيث يستوجب على ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص أن يحرر محضراً عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط

---

[1]- المادة 65 مكرر5 من قانون الإجراءات الجزائية.

[2]- الفقرة الأولى من المادة 65 مكرر6 من نفس القانون.

[3]- المادة 65 مكرر7 من نفس القانون.

[4]- الفقرة الثالثة من المادة 41 من المرسوم الرئاسي المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

والتثبيت والتسجيل الصوتي أو السمعي البصري، وأن يذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها[1]، وذلك لتكون العمليات متطابقة مع الإذن الممنوح.

ثانياً- إجراء التسرب:

التسرب في اللغة يعني الدخول بطريقة متخفية إلى مكان ما أو داخل جماعة ما، أما اصطلاحاً فهو عملية ميدانية يقوم بها أشخاص مؤهلون لذلك تحت إشراف ورقابة الجهات القضائية المختصة، تقوم على اختراق وتغلغل المتسرب داخل مكان أو هدف أو تنظيم يصعب الدخول إليه أو ما يسمى بالمكان المغلق للجماعات الإجرامية، بهدف الكشف عن الجرائم الخطيرة والمتورطين فيها والحد من تأثيرها على المجتمع، فهو في الغالب عملية تتطلب أن يدخل العون المكلف بالعملية في اتصال بالأشخاص المعنيين ويربط معهم علاقات ضيقة ويحافظ على السر المهني لغاية تحقيق الهدف النهائي من العملية، وهي تتطلب على الخصوص المشاركة المباشرة في نشاط الخلية الإجرامية التي تسرب إليها والذي يكون أحياناً ضرورة لقبوله[2].

وقد عرف المشرع الجزائري التسرب في قانون الإجراءات الجزائية بأنه: قيام ضابط أو عون الشرطة القضائي تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف[3]، ونظراً لخصوصية هذا الإجراء فقد أحاطه المشرع من خلال قانون الإجراءات الجزائية بمجموعة ضوابط وشروط يمكن تلخيصها في العناصر الآتية:

أ- **الجرائم المعنية بالتسرب:** وهي مجموعة جرائم محددة على سبيل الحصر واردة في المادة 65 مكرر 5 من قانون الإجراءات الجزائية، ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؛ بحيث يمكن تصور القيام بعمليات تسرب في البيئة الحقيقية أو القيام بعمليات تسرب في البيئة الإلكترونية، وهذا بقيام ضابط أو عون الشرطة القضائية بالدخول إلى العالم الافتراضي وإشتراكه مثلاً في

[1]- المادة 65 مكرر 9 من قانون الإجراءات الجزائية.

[2]- هشام ساحلي، مرجع سابق، ص. ص. 871- 872.

[3]- المادة 65 مكرر 12 من قانون الإجراءات الجزائية.

محادثات غرف الدردشة أو حلقات النقاش والاتصال المباشر عن كيفية قيام أحدهم باختراق الشبكات أو بث الفيروسات[1].

ب- الإذن: بحيث يستلزم القيام بإجراء التسرب وجود إذن سابق بذلك يمنحه في حالة التحري وكيل الجمهورية، وفي حالة فتح تحقيق قضائي قاضي التحقيق، لكن بعكس كل الإجراءات السابق دراستها يجب على قاضي التحقيق قبل منح الإذن أن يخطر وكيل الجمهورية بذلك، وفي الحالتين يتم إجراء التسرب تحت الرقابة المباشرة لمانح الإذن حسب الحالة[2]، ويجب أن يكون هذا الإذن مكتوباً ومسبباً وذلك تحت طائلة البطلان، ويجب أن يتضمن ذكراً للجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر مع إمكانية التجديد حسب مقتضيات التحري والتحقيق ضمن نفس الشروط الشكلية والزمنية، كما يجوز للقاضي الذي رخص بإجراء عملية التسرب أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة ولا تودع الرخصة في ملف الإجراءات إلا بعد الإنتهاء من عملية التسرب حفاظاً على سرية الإجراء وسرية هوية القائم به[3].

ج- الأشخاص القائمون بإجراء التسرب: بعكس الإجراءات السابق دراستها والتي يجب أن يقوم بها ضابط شرطة قضائية، فإنه يمكن تكليف إما ضابط شرطة قضائية أو عون شرطة قضائية بالقيام بالتسرب وهذا تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية[4]، ويفهم من المادة 65 مكرر 14 أنه بإمكان ضباط أو أعوان الشرطة القضائية أن يُسَخِروا بعض الأشخاص للقيام بالتسرب، ولم تحدد المادة إن كان بالإمكان أن يكون من ضمن هؤلاء الأشخاص أفراد من الجماعة الإجرامية التي يتم التسرب فيها، لكن الأكيد أنهم يقومون بنشاطهم تحت رقابة وإشراف من سخرهم وكذلك تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية.

د- دور المتسرب في عملية التسرب: لتحقيق الأغراض المرسومة لعملية التسرب يمكن لضابط أو عون الشرطة القضائية المتسرب أن يوهم الأشخاص المشتبه في ارتكابهم جناية أو جنحة أنه

---

[1]- رشيدة بوكر، مرجع سابق، ص. 434.

[2]- المادة 65 مكرر 11 من قانون الإجراءات الجزائية.

[3]- المادة 65 مكرر 15 من نفس القانون.

[4]- المادة 65 مكرر 12 من نفس القانون.

فاعل معهم أو شريك لهم أو خاف، وبحسب قانون العقوبات يعتبر فاعلاً كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة استعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي[1]، لكن بالرجوع إلى قانون الإجراءات الجزائية نجده ينص على: "... أن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضاً على ارتكاب جرائم"[2]، وفي هذا الإطار يذهب البعض إلى ضرورة التمييز بين من يقوم بإيهام غيره ومن يحرضهم على القيام بذلك؛ لأن المقصود بالإيهام هو مسايرة المشتبه فيه في مسلكه الإجرامي حتى يُضبط ويداه في الجرم، فيجوز لرجال الشرطة تشجيع من يتوفر لديهم الإستعداد لارتكاب الجريمة بقصد ضبطهم، كما أن التحريض لا يتوفر إلا إذا كان هو الدافع إلى الجريمة، وأما تدخل رجل السلطة العامة لكشف الجريمة لا يعد تحريضاً[3]، لكن وضع حدود دقيقة بين ما يعتبر فعل تحريض وما لا يعتبر كذلك أمر صعب، وبحسب قانون العقوبات يعتبر شريكاً في الجريمة من لم يشترك اشتراكاً مباشراً و لكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك[4]، ومثاله قيام المتسرب بتزويد المشتبه فيهم بالمؤن أو بأن يوفر لهم مسكناً أو مكاناً للاجتماع، وبالإضافة إلى إيهام المتسرب للمشتبه فيهم بأنه فاعل أو شريك يوهمهم كذلك بإخفاء الأشياء المتحصلة من الجرائم المرتكبة كما جاء في قانون العقوبات عند نصه على العقاب على إخفاء الأشياء[5].

هـ- الأفعـال المـأذون بهـا للمتسـرب: وهي مجموعة من الأفعال يمكن للفرد المتسرب القيام بها دون أن تقوم مسؤوليته الجزائية، وهي:

1- إقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

---

[1]- المادة 41 من قانون العقوبات.

[2]- الفقرة الثانية من المادة 65 مكرر12 من قانون الإجراءات الجزائية.

[3]- هشام ساحلي، مرجع سابق، ص. 876.

[4]- المادة 42 من قانون العقوبات.

[5]- أنظر المادة 387 من نفس القانون.

2- إستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني (والمقصود هنا توفير الوثائق الرسمية إن كان هناك ضرورة لذلك كاستخراج بطاقة تعريف أو رخصة سياقة أو بطاقة رمادية)، أو الطابع المالي، وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال[1].

ولأجل قيام العون المتسرب بمهامه يسمح له باستخدام هوية مستعارة، ولا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات ويعاقب من يقوم بكشفها بالحبس من سنتين إلى خمس سنوات وبغرامة من 50.000 دج إلى 200.000 دج، وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس إلى عشر سنوات والغرامة من 200.000 دج إلى 500.000 دج، وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من عشر إلى عشرين سنة والغرامة من 500.000 دج إلى 1.000.000 دج دون الإخلال بتطبيق الأحكام الواردة في قانون العقوبات والمتعلقة بالجنايات والجنح ضد الأشخاص[2].

[1]- المادة 65 مكرر 14 من قانون الإجراءات الجزائية.

[2]- المادة 65 مكرر 16 من نفس القانون.

الفصـــل الثانـــي:

الجهــود الدوليــة لمكافحــة التجــسس الإلكترونــي.

حالة الأمن هي أسمى غايات أية دولة ولأجلها تبذل الجهود وتضع الإستراتيجيات وتسن القوانين الوطنية؛ فيكون بذلك أول مستويات الأمن قد تحقق، لكن في كثير من الأحيان لا يكون هذا كافياً لبلوغ درجة الأمن المطلوبة؛ إذ يكون ذلك مرتبطاً بظروف ومعطيات خارجية لا يمكن للدولة بمفردها الإحاطة بها؛ لذا تلجأ لوضع أسس التعاون مع الدول التي تتقاسم معها نفس التوجهات وعادة نفس المجال الجغرافي وتواجه كما هي ذات المخاطر فتعزز بذلك الدولة أمنها الوطني عبر ضمان مستوى آخر من الأمن هو الأمن الإقليمي، وقد يتجاوز تهديد معين مستوى الدولة الواحدة ومستوى مجموعة محددة من الدول فيصبح إنشغال المجتمع الدولي ككل، فلا يتحقق بذلك الأمن الوطني إلا بتحقق أمن كل الدول، أي أن أمن الدولة لا يتحقق إلا في إطار الأمن الجماعي لكل الدول الأخرى، وهو الوضع الذي فرضته أشكال الجريمة الحديثة المعتمدة أساساً على تكنولوجيات المعلومات والاتصالات؛ إذ لم تعد أي دولة بمنأى عنها، لكن إذا كان من الممكن إخضاع معظم الجرائم الإلكترونية لأشكال التعاون الإقليمي أو الدولي فإن التجسس الإلكتروني يعد الاستثناء الأبرز من هذه القاعدة، وذلك بالنظر لخصوصيته وازدواجية النظرة إليه والتعامل معه، فالدولة تعتبره حقاً وتصرفاً مشروعاً من قبلها وجريمة شديدة الخطورة إذا ما ارتكبتها دولة أخرى ضدها، لذلك يصبح أشبه بالمستحيل أن يتم وضع اتفاقية دولية لمكافحته، رغم أن ظهور فواعل دولية جديدة إلى جانب الدولة قد يؤدي إلى التفكير في إعادة النظر في الأطر الدولية التي تحكم التجسس عامة، ورغم عدم وجود اتفاقية إقليمية أو اتفاقية دولية لمواجهته صراحة، يمكن في المقابل استنباط أحكام تنطبق عليه من خلال اتفاقيات إقليمية ودولية وُضعت أساساً لتنظيم مواضيع أخرى، وتُرصد بهذا الصدد أيضاً جهود بعض المنظمات الإقليمية والمنظمات الدولية على رأسها منظمة الأمم المتحدة؛ وعليه بغية الإحاطة بهذه العناصر سيتم تقسيم هذا الفصل إلى مبحثين: يتناول المبحث الأول جهود مكافحة التجسس الإلكتروني في إطار المنظمات الإقليمية والاتفاقيات الإقليمية، ويتناول المبحث الثاني جهود مكافحة التجسس الإلكتروني في إطار المنظمات الدولية والاتفاقيات الدولية.

المبحث الأول: جهود مكافحة التجسس الإلكتروني في إطار المنظمات الإقليمية والاتفاقيات الإقليمية.

يُعد الأمن الإقليمي أحد أهم مستويات الأمن التي تتفق الدول على أهميتها، وتعمل على إتخاذ الإجراءات بغية حفظها؛ وهذا بالنظر لعدة إعتبارات أهمها ارتباط الأمن الإقليمي بالأمن الوطني وإعتباره امتداداً له، بالإضافة إلى قدرة الدول التي تجمعها روابط مشتركة كالرقعة الجغرافية أو المرجعية الفكرية أو الدينية أو اللغوية على فهم وتقييم التحديات التي تواجهها، لذا تلجأ الدول إلى تفعيل التعاون الإقليمي لمواجهة المخاطر والتهديدات المشتركة، وفي هذا الإطار يعد تشكيل و تأسيس المنظمات الإقليمية أو الانضمام إليها أهم أوجه هذا التعاون، وتترجم جهود هذه المنظمات خاصة في شكل اتفاقيات ونصوص قانونية تنظم مكافحة الجرائم التي تهدد مجموع الدول الأعضاء، وسيتم بحث جهود مكافحة التجسس الإلكتروني من خلال عمل المنظمات الإقليمية وكذا من خلال أحكام الاتفاقيات الإقليمية؛ وعليه سيقسم هذا المبحث إلى مطلبين: يتناول المطلب الأول جهود مكافحة التجسس الإلكتروني في إطار المنظمات الإقليمية، ويتناول المطلب الثاني جهود مكافحة التجسس الإلكتروني في إطار الاتفاقيات الإقليمية.

المطلب الأول: جهود مكافحة التجسس الإلكتروني في إطار المنظمات الإقليمية.

يشكل التجسس الإلكتروني كأحد أبرز تأثيرات الجريمة الإلكترونية على أمن الدولة، أكبر التحديات التي تواجه الدول دون استثناء وإن كان ذلك بدرجات متفاوتة، لذلك تعمل معظم الدول في إطار منظماتها الإقليمية على تحيين سياساتها للتصدي للظواهر الإجرامية لتتماشى خصوصاً مع معطيات الثورة التكنولوجية، وفي هذا الإطار سيتم التركيز بالدراسة على عينة من المنظمات الإقليمية سواء بالنظر لارتباطنا بها أو بالنظر لأهميتها؛ وعليه سيتناول الفرع الأول جهود مكافحة التجسس الإلكتروني في إطار جامعة الدول العربية، ويتناول الفرع الثاني جهود مكافحة التجسس الإلكتروني في إطار الإتحاد الأوروبي، بينما يتناول الفرع الثالث جهود مكافحة التجسس الإلكتروني في إطار حلف شمال الأطلسي.

الفرع الأول: جهود مكافحة التجسس الإلكتروني في إطار جامعة الدول العربية.

نشأت جامعة الدول العربية بموجب التوقيع على ميثاقها بتاريخ 22 مارس من سنة 1945، والذي دخل حيز التنفيذ في 11 ماي من ذات السنة، وقد تضمن هذا الميثاق بالإضافة إلى مواد معاهدة الدفاع المشترك والتعاون الاقتصادي للجامعة العربية تحديد الأهداف الرئيسية التي تسعى هذه الأخيرة

لتحقيقيها، وعلى ضوء هذه الأهداف سيتم بحث جهود مكافحة التجسس الإلكتروني، ولذلك ستُعرض بداية أهداف جامعة الدول العربية ومن ثم تقييم عمل جامعة الدول العربية.

أولاً- أهداف جامعة الدول العربية:

جاءت أهداف جامعة الدول العربية موزعة بين مواد ميثاقها، وكذا ما أضافته مواد معاهدة الدفاع المشترك والتعاون الاقتصادي، إذ ترتكز بحسب المادة الثانية من ميثاق الجامعة على توثيق الصلات بين الدول الأعضاء وتنسيق خططها السياسية تحقيقا للتعاون بينها وصيانة لاستقلالها وسيادتها والنظر بصفة عامة في شؤون البلاد العربية ومصالحها، بينما أكدت معاهدة الدفاع المشترك والتعاون الاقتصادي[1] بين دول الجامعة العربية في ديباجتها على الرغبة في تقوية الروابط وتوثيق التعاون بين دول الجامعة حرصاً على استقلالها ومحافظة على تراثها المشترك وكذلك ضم الصفوف لتحقيق الدفاع المشترك عن كيانها وصيانة الأمن والسلام وتعزيز الاستقرار والطمأنينة وتوفير أسباب الرفاهية والعمران في بلادها، وانطلاقاً من هذه الأهداف التي تمثل في مجموعها مبادئ عامة يمكن إجمال هذه الأهداف والمبادئ العامة في عنصرين رئيسيين هما: تحقيق الأمن القومي العربي وتوثيق الصلات وبناء تحالف بين الدول العربية:

أ- تحقيق الأمن القومي العربي:

منذ بدايات الاستقلال العربي عن الاستعمار الأوروبي في أواسط القرن الماضي أدركت معظم الدول العربية أهمية ارتباطها ووحدتها؛ فكان الأمن القومي العربي من الأسس التي بنيت عليها فلسفة الوحدة العربية، وعلى الرغم من قيام النظام العربي السياسي على قاعدة "الدول القطرية"، غير أن معظم الدول العربية كانت تعتبر الأمن القومي العربي ضرورة مهمة لأمنها القطري؛ بالنظر إلى عدة إعتبارات أبرزها وحدة مصدر التهديد الخارجي لمجموع الدول العربية في وقت واحد، والقدرة على مواجهة التكتلات الدولية المختلفة الطامعة في المنطقة سواءً على صعيد الأمن الاقتصادي أو العسكري أو السياسي، ورصد تعاون الشبكات المعادية التي تبث عملاءها في المنطقة ومنعها من النيل من الأمن القطري عبر

[1]- معاهدة الدفاع المشترك والتعاون الإقتصادي بين دول الجامعة العربية وملحقها العسكري الموقعة بتاريخ 17 جوان سنة 1950، والتي أصبحت نافذة المفعول في 23 أوت سنة 1952.

التعاون العربي المشترك[1]؛ فكانت جامعة الدول العربية وميثاقها ومعاهداتها الملحقة الإطار القانوني لتحقيق الأمن القومي العربي.

ويُعرف الأمن القومي عموماً والذي يمكن إسقاطه على الحالة العربية بأنه ما تقوم به الدولة أو مجموعة الدول التي يضمها نظام جماعي واحد من إجراءات في حدود طاقتها للحفاظ على كيانها ومصالحها في الحاضر والمستقبل مع مراعاة التغييرات المحلية والدولية[2]، وبناءاً على هذا الشرط الأخير أي تغير الإجراءات المتبعة لتحقيق الأمن القومي تبعاً لتغير الظروف المحلية والدولية؛ فقد عرفت إستراتيجيات عمل الجامعة لذات الغرض تحيينات وتطويرات متواصلة تتماشى مع المعطيات المستجدة، وفي هذا الإطار يتم رصد مستويين أو صنفين من الإستراتجيات: أولاهما الإستراتيجية الأمنية العربية التي تحوي المبادئ العامة المستقاة من أهداف الجامعة العربية دون تحديد مجال معين؛ وعليه فهي تشمل كل النواحي التي يمكن أن تمس بالأمن القومي العربي، وثانيهما الإستراتيجية العربية لمكافحة جرائم تقنية المعلومات كأنموذج لمواجهة المخاطر التي تمس بالأمن القومي العربي، وسيتم التعرض لكلا الإستراتيجيتين في الآتي:

1- الإستراتيجيـة الأمنيــة العربيــة:

تعبر الإستراتيجية الأمنية العربية عن مجموعة من الإجراءات التي تهدف إلى تحقيق الأمن القومي العربي ومواجهة مجموع المهددات المحتملة له والتي من أبرزها الإختراقات من قبل المخابرات العالمية بقصد التحكم السياسي والسيطرة المعلوماتية وكذلك إحتكار العلوم والتقانة العالية، ولقد تم إقرار هذه الإستراتيجية من قبل مجلس وزراء الداخلية العرب سنة 1983، مع ضرورة الإشارة إلى أنه يجري تطويرها سنوياً لتتماشى مع التحولات والظروف السائدة، ويمكن إجمال أهم بنود هذه الإستراتيجية التي لها علاقة بالتجسس الإلكتروني في النقاط التالية:

- تحقيق التكامل الأمني العربي تبعاً لوحدة الأمن العربي؛ ذلك لأن الأمن الداخلي أو الخارجي لكل دولة عربية مرتبط بالأمن العربي الجماعي، وأن الإخلال بالأمن الداخلي في أية دولة منها تتعدى

[1]- جواد الحمد، مستقبل الأمن القومي العربي في ظل السلام مع إسرائيل، ط2، مركز دراسات الشرق الأوسط، الأردن، 1999، ص. ص. 11- 13.

[2]- معمر بوزنادة، مرجع سابق، ص. 18.

آثاره بالضرورة إلى الإخلال باستقرارها السياسي والاقتصادي والاجتماعي وقدرتها العسكرية مما يؤثر بالتالي على محصلة القوة الذاتية للأمة العربية وعلى جهودها من أجل التحرير والتنمية والرخاء ومجابهة التهديدات التي تواجهها.

– مكافحة الجريمة بكل أشكالها وصورها القديمة والمستحدثة في المجتمع العربي وتطهيره من مختلف أنواع الانحرافات السلوكية.

– الحفاظ على أمن المؤسسات والهيئات والمرافق العامة في الوطن العربي وحمايتها من محاولات العدوان على سلامتها.

– الحفاظ على أمن الفرد في الوطن العربي وضمان شخصيته وحريته وحقوقه وممتلكاته.

– حماية المصالح العربية خارج الوطن العربي.

– بناء قدرات أمنية عسكرية ومدنية لحماية أمن الوطن العربي الداخلي والخارجي[1].

2– الإستراتيجيـة الأمنيـة العربيـة لمكافحـة جرائم تقنيـة المعلومـات:

إن الجرائم الإلكترونية كما تمس الحقوق والحريات الشخصية فهي تهدد الأمن القومي والسيادة الوطنية، ونظراً لارتفاع مؤشر هذه الجرائم وتضاعف أعدادها وتطور أساليبها بسبب التطور المتسارع في تكنولوجيا المعلومات، حرصت الأمانة العامة لمجلس وزراء الداخلية العرب على مكافحة هذه الجرائم بوضع إستراتيجية عربية تنبثق من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (نصت هذه الاتفاقية بشكل صريح على تجريم المساس بالأسرار الحكومية، وسيتم التطرق إليها بالتفصيل لاحقاً) التي اعتمدها مجلس وزراء الداخلية العرب في القاهرة في دورته الحادية والثلاثين بتاريخ 21 ديسمبر من سنة 2010، وقد رأت الأمانة العامة عند إعداد هذه الإستراتيجية أن التصدي لجرائم تقنية المعلومات بإعتبارها من الجرائم العابرة للحدود الوطنية في كثير من أدوارها يتطلب تعاوناً استراتيجياً مشتركاً على كافة الأصعدة الوطنية والعربية وحتى الدولية، ومن هذا المنطلق تبلورت مجالات تنفيذ هذه الإستراتيجية فيما شكلت الجهود الوطنية في كل بلد عربي حجر الأساس في التصدي لمثل هذا النوع من الجرائم؛ بحيث حرصت

[1]– محمد الأمين البشري، مؤسسات المجتمع المدني والأمن القومي العربي، مداخلة مقدمة في إطار الندوة العلمية حول دور مؤسسات المجتمع المدني في التوعية الأمنية، قسم الندوات واللقاءات العلمية، مركز الدراسات والبحوث، 12– 14/ 05/ 2009.

هذه الإستراتيجية على إيجاد آلية وطنية للتعاون والتنسيق بين الجهات المعنية بمكافحة هذه الجرائم، ابتداءً من مرحلة تقييم المخاطر ورصد ومتابعة تلك الجرائم وتبادل المعلومات بشأنها، مروراً بعمليات التحري والملاحقة والتحقيق وتبادل المعلومات، وانتهاءً بتقديم مرتكبيها إلى المحاكمة، مع التعاون والتنسيق مع جميع وسائل الإعلام المرئية والمسموعة والمقروءة لتوعية المواطنين بأخطار جرائم المعلومات وتوعية العاملين بمراكز المعلومات والاتصالات ومستخدمي الشبكة العنكبوتية ومواقع التواصل الاجتماعي بالأساليب والوسائل التي يتبعها قراصنة المعلومات لتحقيق أهدافهم والسبل الكفيلة بكشفها، وذلك من خلال النشرات التوعوية والمحاضرات العلمية المتخصصة بهذا الشأن، بالإضافة إلى ضرورة الاستفادة مما تعده المنظمات والهيئات الدولية المتخصصة بمكافحة مثل هذه الجرائم، وكذلك متابعة التطورات في مجال التقنيات الرقمية والجرائم المتعلقة بها وتوظيف أحدث المستجدات الدولية بهذا الشأن في العمل الأمني بما يسهم في الكشف عن جرائم تقنية المعلومات ويقود إلى التوصل لمعرفة مرتكبيها[1].

وتحقيقاً لجهود التوعية من جهة ورصد ومسايرة التطورات والمستجدات على المستوى التقني والتشريعي، وكذلك لدراسة وتحليل جرائم تقنية المعلومات وتحديد السبل الإجرائية المناسبة لمتابعتها من جهة أخرى؛ فقد قامت الأمانة العامة لمجلس وزراء الداخلية العرب وكذلك الهيئات العلمية والأكاديمية والمنظمات العربية لتكنولوجيات الاتصال والإعلام ومختلف الهيئات العربية الأخرى ذات العلاقة بتنفيذ فعاليات وبرامج وملتقيات ومؤتمرات خاصة تهدف لمواجهة ومكافحة جرائم تقنية المعلومات بصفة عامة وإتاحة خلاصة تلك الأعمال للأجهزة الأمنية في الدول العربية للاستفادة منها، مع ضرورة الإشارة هنا إلى أن هذه الفعاليات المدرجة في إطار إستراتيجية الأمانة العامة لمجلس وزراء الداخلية العرب تعبر عن استمرارية الجهود العلمية المعروفة حتى قبل صدور الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ومن بين هذه الفعاليات تلك الندوات واللقاءات العلمية التي تنظمها جامعة نايف العربية للعلوم الأمنية ضمن خطط سنوية معتمدة من مجلس وزراء الداخلية العرب ومنها ندوة دراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها المنظمة من طرف هذه الجامعة بتونس سنة 2000، وكذلك مؤتمر أمن المعلومات العربية وسبل مواجهة التحديات المستقبلية المنظم بالقاهرة في نوفمبر من سنة 2002، وندوة الجرائم الإلكترونية وجرائم أمن الدولة المنظم بجامعة مسقط في أكتوبر من سنة 2002، وندوة مكافحة الجريمة

[1]– محمد أحمد السويحلي، تكاثف الجهود العربية لمكافحة الجريمة الإلكترونية، مجلة الدراسات المالية والمصرفية، العدد الأول، المجلد الثالث والعشرون، الأكاديمية العربية للعلوم المالية والمصرفية، الأردن، مارس سنة 2015، ص. 6.

عبر الأنترنت على المستوى العربي المنعقدة في شرم الشيخ سنة 2008 والمنظمة من طرف المنظمة العربية للتنمية الإدارية التابعة لجامعة الدول العربية، والمؤتمر العربي الإفريقي الثالث حول قرصنة الشبكات وحماية أمن المعلومات التحديات التقنية والقانونية المنظم بالتعاون مع عديد الأطراف منها جامعة الدول العربية وجامعة عين شمس في ديسمبر سنة 2010[1].

ب- توثيق الصلات وبناء تحالف بين الدول العربية:

يشير كل من ميثاق جامعة الدول العربية ومعاهدة الدفاع المشترك والتعاون الاقتصادي إلى رغبة الجامعة في توثيق الصلات بين الدول المشتركة فيها، وكذلك تقوية الروابط وتوثيق التعاون بينها حرصاً على استقلالها، وكذلك ضم الصفوف لتحقيق الدفاع المشترك عن كيانها وصيانة الأمن والسلام فيها، وقد ترتب عن الجهود المبذولة لتحقيق هذه الأهداف عدة نتائج على الصعيد العملي منها تقديم المساعدات المالية وبروز اتفاقيات تعاون إن في المجال التفافي أو التجاري أو الصحي وغيرها من المجالات، وبالموازاة مع هذا وفيما يخص أغراض هذه الدراسة فقد وضعت الأهداف السابقة أسس تحالف بين الدول العربية يتم بموجبه مواجهة التهديدات المشتركة، بل وتطبيقاً له إلتزمت الكثير من الدول العربية بحماية الأمن الخارجي للدول العربية الأخرى ومنها تعرضها للتجسس وتجسيد ذلك من خلال نصوص قوانينها العقابية، وبتعبير آخر فقد فَعَّل هذا التحالف مبدأ التضامن الدولي المشترك بين الدول العربية لمكافحة الجرائم الماسة بأمن الدولة الخارجي بصفة عامة.

فقد يحدث وأن تقع أفعال معينة لا تدخل في معنى الجريمة في مفهوم القانون الوطني لعدم توافر أركانها أو شروطها القانونية، ولكنها تمثل في نفس الوقت جرائم مضرة بأمن دولة أجنبية طبقاً لقانون هذه الدولة، ففي الأحوال العادية لا يهتم القانون الداخلي بها لأنها لا تمس بالمصالح الوطنية، إلا أن هناك حالات ينص القانون فيها على خضوع الجرائم التي تتضمن إخلالاً بالأمن الخارجي لدولة أجنبية معينة ومنها جرائم التجسس أياً كان مكان وقوعها لسلطان هذا القانون كما لو كانت هذه الجرائم قد وقعت على الدولة التي تسري فيها أحكام ذلك القانون، ويكون هذا في حالة وجود معاهدات دولية للدفاع المشترك أو التحالف، وهذا هو مضمون مبدأ التضامن الدولي المشترك الذي يقضي بسريان أحكام القانون الوطني لدولة معينة على الجرائم التي تقع إضراراً بأمن دولة أخرى بصرف النظر عن مكان وقوع

[1]- محمد محمد صالح الألفي، مرجع سابق، ص. ص. 288- 290.

الفعل أو جنسية الفاعل طالما أن الدولة المعتدى عليها مرتبطة بمعاهدة تحالف مع الدولة الأولى[1]، وتفسير ذلك يرجع إلى طبيعة وتطور العلاقات الدولية من جهة وتنوع وتشعب الوسائل المستعملة في الصراعات الدولية وتأثيراتها غير المحدودة بحيث إتخذت أشكالا عديدة ومعقدة؛ وقد ترتب على ذلك كله أن أمن الدولة الوطني لم يعد بمعزل عن الأمن الإقليمي بل وحتى الدولي بل يتأثر به على نحو مباشر، ويصبح أمن الدولة مرتبطاً على نحو وثيق بأمن دولة أو عدة دول أخرى في حالة الأحلاف العسكرية أو الارتباط بمعاهدة دفاع مشترك، ومن أمثلته على الصعيد العربي والإقليمي معاهدة الدفاع المشترك بين دول الجامعة العربية، هذه المعاهدة التي أقامت في نفس الوقت وفي مادتها الثانية أساس تحالف عسكري بين الدول العربية إذ نصت على: "تعتبر الدول المتعاقدة كل اعتداء مسلح يقع على أية دولة أو أكثر منها أو على قواتها إعتداء عليها جميعاً"[2].

بالرجوع إلى القوانين العقابية للدول العربية نجد معظمها يأخذ بمبدأ التضامن الدولي المشترك وبصورة صريحة، وينص على سريان أحكام القانون الوطني المتعلقة بجرائم أمن الدولة على الجرائم المخلة بأمن الدول الحليفة أو المرتبط معها بمعاهدة دفاع، رغم أن بعض هذه التشريعات تضع شروطاً لذلك كوجوب وقوع الجريمة المضرة بأمن الدولة الحليفة في زمن الحرب، أو أن تكون هذه الجريمة من الجرائم المضرة بأمن الدولة الخارجي دون الداخلي كما هو شأن التشريع الأردني[3]، وبعضها يقرر إعتبار الجرائم المخلة بأمن الدول الحليفة بمثابة جرائم تقع على أمن الدولة سواء من الخارج أو الداخل، ومنها من تقرر إعتبار المسألة جوازية لرئيس الدولة، ومن التشريعات التي أخذت بمبدأ التضامن الدولي المشترك بشكل مطلق وغير مشروط نجد قانون العقوبات التونسي[4]، وقد أخذ المشرع الجزائري بذات المبدأ وذلك في قانون العقوبات بحيث نص على: "يجوز للحكومة بمرسوم تصدره أن تخضع الأفعال التي ترتكب ضد أمن الدول الحليفة أو الصديقة للجزائر لكل أو بعض الأحكام الخاصة بالجنايات أو الجنح ضد أمن الدولة سواء في وقت الحرب أو السلم"[5]، وعليه فالمشرع الجزائري قد قرر حماية أمن الدول الحليفة أو الصديقة من كل الجرائم المخلة به ولم يقصر هذه الحماية على الأمن الخارجي دون الداخلي

[1]– محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 479.

[2]– محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 129.

[3]– أحمد محمد الرفاعي، مرجع سابق، ص. 25.

[4]– محمود سليمان موسى، الجرائم الواقعة على أمن الدولة، مرجع سابق، ص. 125.

[5]– المادة 94 من قانون العقوبات.

أو العكس، كما مد هذه الحماية من حيث الزمن بحيث يقرر إخضاع الجرائم الماسة بأمن الدولة الحليفة أو الصديقة ومنها التجسس لأحكام قانون العقوبات المقررة لهذه الطائفة من الجرائم سواء ارتكبت في وقت الحرب أو وقت السلم، لكن المشرع الجزائري جعل الأخذ بمبدأ التضامن الدولي المشترك جوازياً تاركاً أمر تقريره للحكومة وذلك بموجب مرسوم، كما منحها كذلك حق إخضاع الجرائم الماسة بأمن الدولة الحليفة أو الصديقة لكل أو لبعض أحكام التجريم والعقاب الخاصة بذات الجرائم والمقررة في قانون العقوبات الجزائري بحسب ما تراه مناسبا للتطبيق على كل حالة.

ثانياً- تقييم عمل جامعة الدول العربية:

لطالما تعرضت جامعة الدول العربية وكيفية تسييرها للازمات والقضايا العربية وكذلك كيفية تعاطيها مع المستجدات الدولية للنقد، للحد الذي برزت معه عديد المبادرات الرامية لإصلاح هذه المنظمة التي يفترض أنها تجسد التعاون والوحدة العربية وتمثل الإطار القانوني الذي يوفر الحماية للمصالح الحيوية والأمن القومي العربي، ويمكن أن تنطبق هذه الانتقادات العامة الموجهة لسير جامعة الدول العربية على حالة الجهود الإقليمية لتحقيق الأمن القومي العربي عموماً ومكافحة التجسس كمطلب مدمج ضمن ذات الهدف، وفي هذا الإطار سيتم تقييم عمل جامعة الدول العربية من خلال عنصرين: يتضمن العنصر الأول غموض مفهوم العدوان في إطار ميثاق جامعة الدول العربية، بينما يتضمن العنصر الثاني مدى شمول معاهدة الدفاع المشترك للعمليات في الفضاء الإلكتروني.

أ- غموض مفهوم العدوان في إطار ميثاق جامعة الدول العربية:

نص ميثاق جامعة الدول العربية على إجراءات مواجهة العدوان الذي قد تتعرض له أية دولة عربية، سواء كان هذا الإعتداء موجهاً لها من طرف دولة عربية أخرى عضو في الجامعة أو من طرف دولة أجنبية ، بحيث قرر أنه:

"إذا وقع إعتداء من دولة على دولة من أعضاء الجامعة أو خشي وقوعه فللدولة المعتدى عليها أو المهددة بالإعتداء أن تطلب دعوة المجلس للانعقاد فوراً.

ويقرر المجلس التدابير اللازمة لدفع هذا الإعتداء ويصدر القرار بالإجماع، فإذا كان الإعتداء من إحدى دول الجامعة لا يدخل في حساب الإجماع رأي الدولة المعتدية"[1].

وباستقراء هذا النص يلحظ الغموض الذي تتسم به تلك الإجراءات، ويبرز هذا الغموض من خلال ما يلي:

1- عدم تحديد نوع العدوان المقصود في المادة، بحيث جاءت الصيغة عامة ومن الاتساع بحيث يمكن أن تتسع لكل فعل يؤدي إلى إلحاق ضرر بالدولة المستهدفة مما يُفهم منه إمكانية شموله للإعتداءات الإلكترونية على البُنى الحساسة والسرية للدول الأخرى، بمعنى قيام دولة معينة سواء كانت دولة عربية عضو في الجامعة أم دولة أجنبية بارتكاب جريمة من جرائم التجسس الإلكتروني أدت إلى الحصول على أسرار الدفاع الوطني للدولة الثانية أو أدت لإذاعتها أو لإفشائها أو أدت لتدميرها، فكل هذه الأفعال وكما أثبته الواقع يترتب عنها أضرار بالغة بالدولة المستهدفة، لكن حتى في حالة افتراض إندراج الإعتداءات الإلكترونية ضمن مفهوم العدوان[2]، فإن تقرير ذلك يخضع لقاعدة الإجماع، بحيث تسري قاعدة الإجماع على القرار الخاص بتقدير نوع القضية التي تدرس وما إذا كانت عدواناً أم لا فإذا حدث خلاف بخصوص ذلك فإن القضية لا تناقش أصلاً، وهذا ما يؤدي إلى صعوبة طرح قضية التجسس الإلكتروني على جامعة الدول العربية.

2- نصت المادة السادسة من ميثاق جامعة الدول العربية على أن مجلس الجامعة يقرر التدابير اللازمة لرد الإعتداء لكنه لم يحدد نوع هذه التدابير مما يُفهم منه أن هذا المجلس يقرر تدابيراً بحسب الحالة والظروف مما قد يجعل نفس الفعل يخضع لتدابير مختلفة وهو ما قد يكرس التمييز في التعامل مع الدول رغم كون جوهر الفعل واحداً، هذا بالإضافة إلى أن تقرير هذه التدابير يخضع هو الآخر لقاعدة الإجماع بحيث تعطي هذه القاعدة لكل دولة حق الاعتراض على القرارات التي يتوصل إليها مجلس

[1]- المادة السادسة من ميثاق جامعة الدول العربية.

[2]- Ron smith et scott knight, l'application des solutions de la guerre Electronique a la sécurité des réseaux, revue militaire canadienne, automne 2005, p. 50, article publié sur le site www.journal.forces.gc.ca, le site a été visité le: 23/11/2015.

الجامعة بشأن رد الاعتداء الذي يقع على دولة أخرى عضو، مما يؤدي إلى صعوبة في اتخاذ القرارات بشأن مواجهة الاعتداء الإلكتروني وليأخذ هنا صورة التجسس الإلكتروني.

3- في حالة تجاوز الصعوبات السابقة بمعنى إمكانية طرح قضية الإعتداء الإلكتروني على مجلس الجامعة والاتفاق بالإجماع على القرارات المتضمنة التدابير المتخذة لمواجهته، فإن تنفيذ هذه القرارات يصطدم بعدم وجود آليات وأجهزة تكفل تنفيذ هذه القرارات، مما يُشكك في فعاليتها وكذلك في طابعها الإلزامي.

وعليه يمكن القول أن مواجهة التجسس الإلكتروني باعتباره نوعاً من أنواع الإعتداءات يصطدم بجملة عراقيل وصعوبات في إطار ميثاق جامعة الدول العربية، وتظهر هذه الصعوبات على كل مستويات متابعة هذه القضية سواء كان ذلك على مستوى طرحها أو على مستوى إتخاذ قرار بشأنها أو على مستوى تنفيذ هذه القرارات، هذا بالإضافة إلى أن الدول العربية لم تتوصل إلى إجماع حول مواجهة الإعتداءات التقليدية فما بالك بالاتفاق حول مواجهة الإعتداءات الإلكترونية.

ب- مـدى شمـول معاهـدة الدفـاع المشتـرك للعمليات فـي الفضاء الإلكترونـي:

سبقت الإشارة إلى أن الدول حالياً تعتبر الفضاء الإلكتروني ميداناً خامساً للعمليات العسكرية إلى جانب البر والبحر والجو والفضاء وأن اللجوء إلى استخدام هذا الفضاء والموجودات الرقمية كأسلحة أو كأدوات استخبار أصبح يتطور بسرعة[1]، مما سمح بظهور صنف جديد من الحروب هي الحروب الإلكترونية التي تظهر كقطيعة مع الصراعات والحروب الكلاسيكية بسبب خصائصها المتمثلة في عالمية ميدان التحرك وتعدد فرص النجاح للهجمات؛ مما دفع عدداً معتبراً من المحللين إلى التوصل إلى ذات النتيجة السابقة من أن ميدان المعركة المستقبلي سيكون الفضاء الإلكتروني[2]، وما يدعم هذا الطرح توجه عديد الدول إلى تطوير قدراتها العسكرية لصد الهجومات الإلكترونية وبناء سياسات للدفاع الإلكتروني، ودعم الأمن المعلوماتي لبناها الحساسة[3]، وهي كلها معطيات تشير إلى تبني السياسات الأمنية لكل الدول

[1]- The Defence cyberstrategy, op. cit, p. 4.

[2]- Irnerio Seminatore, op. cit.

[3]- تُعتبر الولايات المتحدة الأمريكية من الدول الأوائل الذين اعتبروا الأمن الإلكتروني مسألة أمن وطني وأعدوا إستراتيجية تهدف إلى مكافحة سلسلة التهديدات المرافقة، وما يلاحظ حول هذه الإستراتيجية ربطها دوماً بالمجال العسكري؛ فقد قامت إدارة كلنتون في نهاية تسعينات القرن الماضي بتأسيس لجنة لبحث مسألة الأمن الإلكتروني تولى قيادتها جنرال من القوات المسلحة الأمريكية، وقد أسست مجموع التوصيات التي خرجت بها هذه اللجنة إلى إقامة كل الإستراتيجيات الأمريكية في=

للفضاء الإلكتروني كبعد إستراتيجي لعملياتها العسكرية واعترافها بأن الهجمات الإلكترونية لها نفس أثار وأضرار الهجمات الكلاسيكية، بحيث وكمثال قامت وزارة الدفاع الأمريكية في ماي من سنة 1999 بإصدار إرشادات حذرت فيها من سوء استخدام هجمات المعلومات والتي يمكن أن تعرض الولايات المتحدة لمسؤولية جنائية تتعلق بالإتهام بارتكاب جرائم حرب، وحثت القادة العسكريين على تطبيق نفس مبادئ قانون الحرب[1].

وبإسقاط الوقائع السابقة على حالة التحالف العربي العسكري المؤسس بموجب معاهدة الدفاع المشترك وملحقها العسكري نجدها لا تتطرق صراحة لهذا الصنف الجديد من التهديدات الإلكترونية، إذ اكتفت بالنص في مادتها الثانية على أن تعتبر الدول المتعاقدة كل إعتداء مسلح يقع على أية دولة أو أكثر منها أو على قواتها إعتداءً عليها جميعاً، وهي ذات الصيغة المستخدمة في معاهدة حلف شمال الأطلسي لكن الدول المنظمة إلى هذا الحلف وبالاستناد إلى ذات مواد هذه المعاهدة اعترفت بالهجمات الإلكترونية وبالتجسس الإلكتروني كتهديد أو كإعتداء جدي ضدها واتخذت إجراءات عديدة لمواجهته

=مجال الأمن الإلكتروني، والتي عرفت عديد التحيينات وذلك عن طريق إخضاعها للمراجعة الدورية بحيث كانت من بين أول الإجراءات التي اتخذها باراك أوباما بصفته رئيساً للولايات المتحدة القيام بإجراء فحص لـ (60) يوماً للسياسة الأمريكية للأمن الإلكتروني، لأكثر تفاصيل أنظر:

-Holly Porteous, cybersécurité et renseignement de sécurité : L'approche des Etats – Unis, étude générale, bibliothèque du parlement, Canada, publication n° 2010-02-F révisée le 15 juin 2011, p. p. 1– 5.

– فمثلاً في 08 جانفي من سنة 2014 أطلقت قوات الطيران الأمريكية عرضاً لأجل تكوين ألف (1000) خبير في المعارك الإلكترونية، وبتاريخ 18 فيفري من ذات السنة أكدت القوات المسلحة الإيرانية استعدادها لمواجهة أي هجوم إلكتروني يستهدفها، وبتاريخ 25 ماي من ذات السنة أعلنت اندونيسيا عن إنشاء قيادة عملياتية للدفاع المعلوماتي في إطار جيشها يدعى"مركز العمليات الإلكترونية le cyber opération center" ، وإعلان الجيش الشعبي للتحرير للصين في الأول من جويلية من ذات السنة عن إنشاء مركز للأبحاث حول الفضاء الإلكتروني يدعى "مركز الأبحاث الاستخباراتية الإستراتيجية للفضاء الإلكتروني cyberspace strategic intellegence research center"، وقيام الولايات المتحدة الأمريكية بتاريخ 17 جويلية من ذات السنة بتنظيم تمرين دفاع إلكتروني معنون بـ "ceber Guard 14–1" تضمن (500) مشارك ومختلف الكيانات المدنية والعسكرية، وإعلان الجيش الأمريكي بتاريخ العاشر من سبتمبر من ذات السنة عن تفعيل لوائه الأول للحماية الإلكترونية في فورت هود، هذه الوحدة هي الأولى في سلسلة عشرين (20) وحدة موضوعة تحت القيادة الإلكترونية للولايات المتحدة، وإعلان روسيا في السادس من نوفمبر من ذات السنة عن نيتها في إنشاء وحدة جديدة للدفاع الإلكتروني مختصة في مراقبة الشبكات العسكرية، أنظر:

-Ryan Burton, op. cit, p. p. 4 –13.

[1]– عادل عبد الصادق محمد الجخة، مرجع سابق، ص. 201.

وذلك في إطار التعاون الذي يجمعها بموجب عضويتها في حلف شمال الأطلسي، والتي سيتم دراستها في حينها؛ وعليه ومن حيث المبدأ يمكن التوسيع في نطاق نصوص معاهدة الدفاع المشترك لتشمل هجمات الإلكترونية، وتعزيز التعاون الإقليمي العربي لمواجهتها خاصة وأن صياغة مواد هذه المعاهدة وملحقها العسكري تسمح بمثل هذا التوسيع، فعلى سبيل المثال لا الحصر تنص المادة الثالثة من المعاهدة على أن تتشاور الدول المتعاقدة فيما بينها بناء على طلب إحداها كلما هددت سلامة أراضي أية واحدة منها أو استقلالها أو أمنها، وغني عن البيان أن الهجمات الإلكترونية ومنها تحديداً أفعال التجسس الإلكتروني تشكل في الوقت الحالي أحد أهم التهديدات لأمن الدول الخارجي، كذلك فقد وضعت المادة الخامسة من المعاهدة الأساس القانوني لتأليف اللجنة العسكرية الدائمة وأحالت على ملحق المعاهدة العسكري لتحديد مهامها واختصاصاتها، وبالرجوع إلى البند الأول من هذا الملحق نجد أن من بين اختصاصات اللجنة العسكرية الدائمة تقديم المقترحات لزيادة كفاية قوات الدول المتعاقدة من حيث تسليحها وتنظيمها وتدريبها لتتماشى مع أحدث الأساليب والتطورات العسكرية وتنسيق كل ذلك وتوحيده، كما تختص بتنظيم تبادل البعثات التدريبية وتهيئة الخطط للتمارين والمناورات المشتركة بين قوات الدول المتعاقدة وحضور هذه التمارين والمناورات ودراسة نتائجها بقصد اقتراح ما يلزم لتحسين وسائل التعاون في الميدان بين هذه القوات والبلوغ بكفايتها إلى أعلى درجة، وكلها مواد تمنح الأساس القانوني لتعاون إقليمي أمني يمكن توسيعه ليشمل مواجهة التهديدات الإلكترونية؛ فالعديد من المنظمات قامت بوضع خطط دفاع إلكتروني، وبإجراء تمارين، وتنفيذ عمليات للتصدي للهجمات في الفضاء الإلكتروني، كما هو حال الإتحاد الأوروبي أو حلف شمال الأطلسي، أو حتى كما هو ملاحظ حالياً من خلال إتجاه بعض الدول نحو التعاون الثنائي في مجال الدفاع الإلكتروني.

مما سبق نخلص إلى أن مواد معاهدة الدفاع المشترك وملحقها العسكري تُعد أساساً قانونياً مناسباً لبناء تعاون إقليمي عربي من شأنه مواجهة مختلف أصناف الاعتداءات الجديدة التي يعرفها الفضاء الإلكتروني ومنها عمليات التجسس الإلكتروني، لكن لا يوجد في الممارسة العملية ما يدل على هذا التوجه؛ وعليه يمكن القول أن هذه النصوص تبقى مجرد إجراءات نظرية يعوزها التفعيل خاصة في ظل تغلب المنطق القطري على المنطق القومي التوحيدي داخل جامعة الدول العربية.

الفـــرع الثانـــي: جهـــود مكافحـة التجـسس الإلكتروني في إطـار الإتحـاد الأوروبـــي.

تتجلى جهود الإتحاد الأوروبي في مكافحة الجريمة الإلكترونية بصفة عامة ومنها التجسس الإلكتروني في محورين رئيسيين: الأول نظري يبرز من خلال إتخاذ إجراءات قانونية لمكافحة الإجرام الإلكتروني ولدعم الأمن المعلوماتي عموماً، والثاني عملي يبرز من خلال إتخاذ إجراءات عملية وملموسة لمكافحة التجسس الإلكتروني تحديداً، وسيتم التطرق للمحورين كل على حدة في العنصرين الآتيين:

أ- الإجـراءات القانونيـة لمكافحـة الإجرام الإلكترونـي عمومـاً ولدعم الأمن المعلوماتـي على مستـوى الإتحـاد الأوروبـي:

بالرغم من كون اختصاصات الإتحاد الأوروبي في مجال التشريع الجزائي محدودة، إلا أن له القدرة على إتخاذ الإجراءات اللازمة لتنسيق التشريعات الوطنية في المادة الجزائية في حالات معينة ومنها الإجرام الإلكتروني، وفي هذا الإطار نقف على جملة من النصوص القانونية التي تهدف أساساً لدعم الأمن الإلكتروني للأنظمة والشبكات المعلوماتية، حيث أصدرت اللجنة الأوروبية في سنة 2001 نشريتين: الأولى معنونة بـ "خلق مجتمع معلومات أكثر أماناً وذلك عن طريق تقوية أمن البنى التحتية للمعلومات ومكافحة الإجرام المعلوماتي"، وقد حللت هذه النشرية وحاولت وضع حلول لمشكلة الإجرام المعلوماتي من خلال الإشارة تحديداً إلى ضرورة العمل الفعال لأجل محاربة التهديدات التي تمس بتكاملية وتوافرية وكذلك بأمن الوظائف الخاصة بالأنظمة المعلوماتية والشبكات، أما النشرية الثانية فكانت حول "أمن الشبكات والمعلومات" والتي قامت بتحليل إشكاليات الأمن في الشبكات وقدمت مقترحاً يتضمن الخطوط العريضة الإستراتيجية لرد الفعل في هذا المجال، هاتان النشريتان أشارتا إلى ضرورة التقارب بين التشريعات الموضوعية للقانون الجزائي على مستوى الإتحاد الأوروبي خاصة ما تعلق منها بالهجومات التي تستهدف الأنظمة المعلوماتية، فمثل هذا التقارب والتنسيق بين التشريعات هو العنصر المفتاح لكل المشاريع المباشرة على مستوى الإتحاد الأوروبي لمكافحة الإجرام المعلوماتي، ولذلك وبناءاً على ما سبق فقد قامت اللجنة الأوروبية في سنة 2002 بعرض مقترح حول قرار إطار يتعلق بالهجمات المستهدفة للأنظمة المعلوماتية، هذا المقترح تم تعديله جزئيا ثم تم تبنيه من طرف المجلس الأوروبي بموجب القرار رقم 2005/ 222 بتاريخ 24 فيفري سنة 2005 حول الإعتداءات ضد الأنظمة المعلوماتية، وقد استند هذا القرار الإطار على اتفاقية مجلس أوروبا حول الإجرام المعلوماتي المعروفة باتفاقية بودابست، مع تركيزه على ضرورة تنسيق النصوص الموضوعية للقانون الجزائي التي تهدف إلى حماية البنى التحتية، إذ

ركزت مواد هذا القرار الإطار على تجريم أفعال الدخول غير المشروع للأنظمة المعلوماتية والإعتداء على تكاملية النظام والإعتداء على تكاملية المعطيات، وحث الدول على الأخذ والالتزام بها، ونظراً لأن هذا القرار الإطار لم يدمج ضمن أحكامه العناصر المتعلقة بقانون الإجراءات الجزائية وتحديداً ما يتعلق بتنسيق الآليات الضرورية من أجل التحقيق حول الجرائم الإلكترونية ومتابعة مرتكبيها أمام القضاء؛ فقد أعدت اللجنة في سنة 2005 مقترحاً للإتحاد الأوروبي متعلق بحفظ المعطيات والذي تبناه بعد ثلاثة أشهر فقط من عرضه عليه، ويُلزم المقترح الجديد ممولي خدمات الأنترنت بتخزين معطيات المرور الضرورية من أجل كشف وتحديد هوية المجرمين في الفضاء الإلكتروني[1]، وتجدر الإشارة هنا إلى أن القرار الإطار للإتحاد الأوروبي له أهمية تفوق تلك المقررة لاتفاقية بودابست التي تم وضعها في إطار مجلس أوروبا، ولا يُنظر للأهمية هنا من زاوية شمول المواد للجرائم الإلكترونية كافة، ولكن من زاوية حجية تلك المواد بالنسبة للدول؛ بحيث أن مجلس أوروبا لا يمكنه إجبار أحد الدول الأعضاء فيه على توقيع اتفاقية بودابست كما لا يمكنه إجبار دولة موقعة على المصادقة على الاتفاقية، وبعكس مجلس أوروبا فإن الإتحاد الأوروبي له وسائل إجبار الدول الأعضاء لتطبيق القرارات التي تتخذ فيه؛ وهذا ما يفسر لما كثير من دول الإتحاد الأوروبي التي وقعت على اتفاقية بودابست لسنة 2001 ولكن لم تصادق عليها بعد ولكنها بالرغم من ذلك تطبق القرار الإطار للإتحاد الأوروبي المتعلق بالإعتداءات ضد الأنظمة المعلوماتية لسنة 2005[2]، لذلك فإن الإتحاد الأوروبي وكما سبقت الإشارة إليه ورغم سلطاته المحدودة في مجال التشريع إلا أن له القدرة على تنسيق التشريعات الوطنية للدول الأعضاء فيه من خلال وضع أطر قانونية تسترشد بها هذه الدول عند صياغة قوانينها الداخلية مما يؤدي من حيث النتيجة إلى توحيد المواد القانونية، وعليه القدرة على ضمان فعالية أكبر لمواجهة الجرائم الإلكترونية بصفة عامة.

كما قامت اللجنة الأوروبية في سنة 2007 بوضع نشرية معنونة بـ "نحو سياسة عامة في مجال مكافحة الإجرام الإلكتروني"، أشارت إلى أهمية اتفاقية مجلس أوروبا كأداة دولية أساسية لمكافحة الإجرام الإلكتروني، كما تضمنت الإشارة إلى الإشكالات والمواضيع التي تحتل مكاناً مركزياً في الأنشطة المستقبلية للجنة خاصةً ما تعلق منها بتقوية التعاون الدولي لمكافحة الإجرام المعلوماتي، وتنسيق الدعم المالي لأنشطة التكوين، وتنظيم إجتماع للخبراء في مجال مكافحة ومتابعة هذه الجرائم، ومراقبة تطور

[1]- Marco Gercke, op. cit, p. p. 115 –116.
[2]- Ibid, p. 128.

التهديدات الإلكترونية بهدف تقدير الحاجة إلى وضع تشريع مكمل، بالإضافة إلى تقوية وتدعيم الحوار مع القطاع الصناعي[1]، وبخصوص هذه النقطة الأخيرة فقد نادى الإتحاد الأوروبي بضرورة إعتبار الصناعة الإلكترونية صناعة إستراتيجية، وهي الفكرة التي تشير إلى تجربة الإتحاد الأوروبي في مجال أمنية المعلومات القومية بحيث اشتمل تطبيق هذه التجربة على القطاعين العام والخاص في أوروبا والتي أصبحت تنافس وبشكل قوي تجربة الولايات المتحدة الأمريكية ومن بعدها اليابان[2]، وهذا بالنظر لما يمثله الاستقلال في مجال الصناعات الإلكترونية والتخلص من التبعية للتجهيزات الأجنبية من دور مهم في سياسة حماية المعلومات القومية وسد الثغرات التي يمكن أن تشكل تهديداً لهذه المعلومات.

ب- الإجراءات العملية لمكافحة التجسس الإلكتروني على مستوى الإتحاد الأوروبي:

سبقت الإشارة إلى أن نظام التجسس الإلكتروني عبر الأقمار الصناعية المعروف باسم "إيشلون" والذي جاء نتيجة لاتفاقية أُبرمت سنة 1947 بين كل من الولايات المتحدة الأمريكية وبريطانيا وأنظمت إليها فيما بعد كل من كندا واستراليا ونيوزلندا، لم يتم الكشف عنه للعلن ولم يتعرف عليه العالم إلا بعد صدور تقرير اللجنة البرلمانية الأوروبية حول تطور تقنيات الرقابة السياسية الموضوع من طرف آلان بومبيدو ، والمعنون بـ "تقييم تقنيات التحكم السياسي" في ديسمبر من سنة 1997، وفي إطار ردة فعل الإتحاد الأوروبي على عمليات التجسس الأمريكية التي تتم عن طريق نظام إيشلون والتي تم إعادة توجهيها لأغراض التجسس الاقتصادي تحديداً بعدما كانت محصورة في المجال العسكري فقط؛ فقد قام الإتحاد الأوروبي في أفريل من سنة 2004 بإطلاق برنامج يُدعى "كوانتوم Quantum"، والذي يهدف إلى مساعدة المؤسسات الأوروبية لتوفير حماية أفضل لأنشطتها من التجسس الصناعي؛ بحيث قام المشروع بتسخير خبراء تطوير برمجيات في الإلكترونيك وفي التشفير وكذلك مختصين في تقنيات الأمن الإلكتروني، رغم أن البعض يرى أن هذا المشروع جاء متأخراً جداً لأن الأضرار في معظم الحالات كانت قد حدثت بالفعل[3]، هذا بالإضافة إلى الإشكاليات المعقدة التي يثيرها الإنتماء المزدوج لعديد الدول للإتحاد الأوروبي من جهة ولاتفاق "UKUSA" الذي ترتب عنه نظام إيشلون من جهة ثانية، كما هو الحال بالنسبة لبريطانيا (كعضو سابق للإتحاد الأوروبي)، وبعض الدول المشاركة في هذا النظام بشكل غير مباشر كألمانيا.

---

[1]- Marco Gercke, op. cit, p. 117.

[2]- وليد غسان سعيد جلعود، مرجع سابق، ص. 65.

[3]- Frédéric Charpier, op. cit, p. 25.

وفي إطار السعي إلى مكافحة الإرهاب الإلكتروني ومن خلاله مواجهة عمليات التجسس الإلكتروني فقد أعلنت ألمانيا عن إعدادها لبرنامج لتطوير فيروسات، وقيامها من خلاله بتطوير فيروسات حاسوب تهدف إلى مراقبة من تصفهم بالإرهابيين ورصد أي هجمات محتملة والمراقبة الجنائية عن طريق الأنترنت لمن يشتبه فيهم بالإرهاب، مع ضرورة الإشارة إلى أن هذا البرنامج قد واجه عراقيل متعلقة بانتهاكه لحقوق الإنسان وذلك بعد إقرار محكمة ألمانية في فيفري من سنة 2007 بأن التجسس عبر الأنترنت يحتاج إلى منح سلطة قانونية خاصة[1]، لكن بالرغم من ذلك فقد اتفقت دول الإتحاد الأوروبي في الثلاثين من شهر ماي من سنة 2007 بقيادة ألمانيا على مسودة تفاهم لمراقبة الإرهاب عبر الأنترنت[2].

وفي إطار عمل الإتحاد الأوروبي على تعزيز الوحدة بين دوله الأعضاء من خلال استهداف إقامة آلية اتصال معلوماتية تجمع كل هذه الدول فقد استثمر في هيئات البريد والبرق والهاتف التي كانت تعمل في أوروبا ليزيد من قدرتها المعلوماتية بشكل كبير ويحولها إلى ما يعرف بالشبكة الأوروبية للوصول المباشر للمعلومات "أورونت EURO NET"[3]، وبالمقابل ورغبة في تحقيق الأمن المعلوماتي القومي من خلال مراقبة الشبكة المعلوماتية الأوروبية فقد تم إنشاء شبكة خاصة تدعى "الوكالة الأوروبية لأمن المعلومات–The European Network and information sécurity Agency – ENISA " ومقرها أثينا باليونان مكلفة بمراقبة القرصنة الإلكترونية داخل المجال الأمني الأوروبي[4].

من ناحية أخرى فقد عمل الإتحاد الأوروبي على تطوير قدراته الإلكترونية لمواجهة الهجمات عبر الفضاء الإلكتروني من خلال تنظيمه لتمارين للدفاع الإلكتروني، ومثال ذلك قيامه بإعداد تمارين لإدارة و تسيير الأزمات الإلكترونية في سنة 2014 تحت مُسمى "cyber Europe 2014"[5].

الفـــرع الثالـــث: جهـود مكافحـة التجـسس الإلكتروني فـي إطـار حلـف شمـال الأطلسـي.

تعد منظمة حلف شمال الأطلسي (الناتو) أشهر المنظمات الدولية التي تأسست بهدف تعزيز الأمن الإقليمي – رغم أن مجال عمله يتسع ليشمل العالم ككل – كما يعتبر أكثر المنظمات الأمنية

[1]– عادل عبد الصادق محمد الجخة، مرجع سابق، ص. 261.

[2]– نفس المرجع، ص. 259.

[3]– وليد غسان سعيد جلعود، مرجع سابق، ص. 65.

[4]– عادل عبد الصادق محمد الجخة، مرجع سابق، ص. 261.

[5]- Ryan Burton, op. cit, p. 2.

العسكرية الإقليمية قوةً وتكاملاً إلى حد بعيد، وهذا يرجع إلى دور الولايات المتحدة بصفتها القوة المسيطرة فيه وكذلك إلى الخبرة الطويلة المتوفرة لدى هذه المنظمة في تشغيل هيكل قيادي متكامل على نحو سليم[1]، وقد نشأ هذا الحلف كإمتداد لاتفاق أمني أوروبي ليتوسع فيما بعد بدخول الولايات المتحدة الأمريكية كعضو فعال فيه وليؤسس لتعاون في المجال الأمني بين أوروبا والولايات المتحدة الأمريكية وذلك بموجب معاهدة حلف شمال الأطلسي الموقعة في واشنطن في الرابع أفريل من سنة 1949[2]، والتي تشكل المادة الخامسة منها محور التعاون الأمني بين الدول الأعضاء وركيزة الالتزام بمبدأ الدفاع المشترك بينها، وقد كان للتطورات التقنية وظهور الفضاء الإلكتروني وزيادة التهديدات الناشئة عنه أثر بارز على الخطط الأمنية لحلف الناتو من ناحيتين، الأولى تتعلق بتغيير مفهوم الدفاع المشترك بحيث أصبح يشمل الهجمات الإلكترونية والإتجاه نحو إعتبار هذه الأخيرة بمثابة إعتداء شأنها شأن الإعتداءات التقليدية، والثانية تتجسد من خلال العمل على إتخاذ إجراءات تتماشى مع طبيعة الفضاء الإلكتروني لغرض مواجهة الهجمات الصادرة عنه ومنها التجسس الإلكتروني تحديداً، وسيتم تفصيل كلتا الناحيتين في العنصرين الآتيين:

أ- تغييـر مفهوم الدفاع المشتـرك فـي ظل ميثـاق شمـال الأطلســي:

لقد شكلت هجمات الحادي عشر سبتمبر من سنة 2001 نقطة التحول في بناء الإستراتيجيات الأمنية لحلف الناتو من خلال منح أهمية بالغة للفضاء الإلكتروني كبعد جديد للنشاطات الإجرامية، وكمصدر مُتفرد لتهديدات مستجدة تحتاج إلى إعادة النظر فيها بما يتناسب والخطر التي تمثله، فقبل هذا التاريخ كانت تتم مناقشة المخاطر الإلكترونية والتحديات الأمنية في إطار مجموعات صغيرة من خبراء التقنية لكن منذ ذات التاريخ بات من الواضح أن عالم الأنترنت تحديداً يمثل مواطن ضعف خطيرة للمجتمعات المترابطة إلكترونياً وبشكل متزايد، كما لم يكن حلف الناتو يُعط الهجمات الإلكترونية التي كان يتعرض لها قبل هذا التاريخ تلك الأهمية التي تستحق، فأثناء أزمة كوسوفو سنة 1999 واجه الناتو أول حادث خطير من الهجمات الإلكترونية وقد أدى من بين أمور كثيرة إلى غلق حساب البريد الإلكتروني للحلف لعدة أيام أمام الزوار الخارجيين، كما أدى كذلك إلى العطل المتكرر لموقع الحلف إلا أنه في هذا

[1]- بول ويلكنسون، مرجع سابق، ص. 81.

[2]- محمد حسون، الإستراتيجية التوسعية لحلف الناتو وأثرها على الأمن القومي العربي، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد الثاني، المجلد السادس والعشرون، 2010، ص. ص. 336- 337.

الوقت كان يعتبر تلك الهجمات مجرد حملة لمنع معلوماته وبأنها خطر لكن محدود النطاق والأثر مما تطلب حينها استجابات تقنية محدودة، لتبدأ النظرة في التغير بعد تاريخ 2001، ولتشكل حوادث إستونيا في سنة 2007 الموضوع الذي جذب أخيراً الانتباه السياسي لهذا التهديد المتزايد على الأمن العام واستقرار الدول، وفي عام 2008 انطلقت واحدة من أخطر الهجمات الإلكترونية ضد أنظمة حواسيب الجيش الأمريكي من خلال وصلة (USB) بسيطة متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الأوسط بحيث تم نشر برامج تجسس في كل من الأنظمة السرية والغير سرية والتي لم تكتشف رغم تشكيل ما يشبه جسر رقمي تم من خلاله نقل الآلاف من ملفات البيانات إلى خوادم خارجية، ومنذ ذلك الحين أصبح التجسس الإلكتروني يشكل أحد التهديدات الدائمة لدول حلف الناتو جميعاً والتي شهدت حوادث مماثلة أدت إلى سرقة أسرار وطنية رغم وضعها تحت حراسة مشددة[1]، وهذا ما أدى بدول الحلف إلى التفكير في تغيير سياستها الأمنية وفي توسيع مفهوم الدفاع المشترك الوارد في المادة الخامسة من معاهدة حلف شمال الأطلسي، والتي تنص على أن "تتفق الأطراف على أن أي هجوم مسلح ضد أي منها في أوروبا أو أمريكا الشمالية سوف يعتبر هجوماً عليها جميعاً وبالتالي فإنها تتفق على أنه في حالة حدوث مثل هذا الهجوم فإن كلاً منها – تطبيقاً للحق الفردي والجماعي في الدفاع عن الذات– وفقا للبند 51 من ميثاق الأمم المتحدة سوف تساعد الطرف أو الأطراف التي تتعرض للهجوم وذلك بإتخاذ إجراء منفرد أو بالتنسيق مع الأطراف الأخرى بالصورة التي تراها ضرورية بما في ذلك استخدام القوة المسلحة من أجل استعادة أمن منطقة شمالي الأطلنطي والحفاظ عليها ..."، وعليه طُرحت إمكانية إعتبار الهجمات الإلكترونية مهما كان نوعها تدخل ضمن الإعتداءات التي تستوجب إعمال نص هذه المادة بشأنها، لكن مع ضرورة تقييد هذه الإمكانية بشروط محددة؛ إذ إعتبرت دول الحلف أن الهجوم الإلكتروني لا يكون كعمل عسكري إلا إذا تم تحديد مسؤولية مرتكبيه[2]، وقد أعادت دول الحلف تبني المفهوم الجديد للدفاع المشترك حديثاً وبشكل صريح إذ أعلن مسؤولوا الناتو في الخامس من سبتمبر من سنة 2014 عن تبنيهم لإجراء يدعم نص الدفاع المشترك يتضمن تقرير أنه في حالة ما إذا كانت أحد الدول الثمان والعشرين (28) لحلف الناتو ضحية لهجوم إلكتروني فإن هذا الأخير سيعتبر كمساس

[1]– أولاف تايلر، التهديدات الجديدة: الأبعاد الإلكترونية، مجلة الناتو، مقال منشور على الموقع الإلكتروني: http://www.nato.int/docu/review/2011/11september/cyber-threads/files/1679.jpg، تمت زيارة الموقع بتاريخ: 2016/06/26.

[2]– عادل عبد الصادق محمد الجخة، مرجع سابق، ص. 267.

وإعتداء على مجموع أعضاء الناتو[1]، لكن يبقى التساؤل المطروح هنا يدور حول كيفية الرد على مثل هذا الهجوم؛ إذ بالرجوع إلى المادة الخامسة ذاتها من معاهدة الحلف الأطلسي نجدها تنص على الرد المسلح أي الرد العسكري، كما يفهم من صياغتها إمكانية إتخاذ إجراءات أخرى تركت أمر تحديدها للدول الأعضاء في الحلف، لكن إذا كان الرد المسلح على الإعتداءات التقليدية يمكن تبريره قانوناً لوضوح عناصره كتحديد الجهة المعتدية والجهات المساهمة في الإعتداء وحجم الأضرار الناجمة عنه فالأمر ليس بذات البساطة بالنسبة للهجمات الإلكترونية؛ إذ لا يمكن في معظم الحالات التحديد الدقيق للمسؤول عن الإعتداء الإلكتروني أو مكان انطلاقه أو المساهمين فيه أو الأضرار المترتبة عنه، بل ولا يمكن في حالات أخرى تحديد عناصر أسلوب ووسيلة الهجوم بشكل مفصل وكامل مما يجعل الالتزام بقواعد القانون الدولي وخاصة ميثاق هيئة الأمم المتحدة الذي يمنح حق الدفاع عن النفس إتجاه الإعتداء الصادر من دولة محددة أمراً صعباً للغاية؛ وعليه يمثل أي شكل من أشكال الرد العسكري مشكلة كبيرة من الناحية القانونية والسياسية.

ب- الإجراءات المتخذة من طرف حلف الناتو لمواجهة الهجمات الإلكترونية بصفة عامة:

في ظل الصعوبة البالغة التي تعترض اللجوء إلى الحل العسكري لمواجهة الهجمات الإلكترونية، فإن الإجراءات المتخذة من قبل حلف الناتو قد ركزت أساساً على بناء سياسة للدفاع الإلكتروني والعمل على تطويرها باستمرار، ومن بين ما تتضمنه هذه السياسة العمل على تدعيم إجراءات الأمن المعلوماتي من جهة، وتعزيز التعاون في مجال تبادل المعلومات حول التهديدات الإلكترونية المحتملة، ومراقبة النشاطات الممارسة في الفضاء الإلكتروني، وتطوير القدرات الإلكترونية للكشف والرد على تلك الهجمات من جهة أخرى.

بالاستناد إلى معاهدة حلف شمال الأطلسي وتحديداً مادتها الخامسة، ومادتها الرابعة التي تقر بحق الأطراف في التشاور فيما بينها حينما يكون هناك في رأيها تهديد للسيادة أو الاستقلال السياسي أو الأمني لأي منها، فقد كان للحلف عقد الاجتماعات الدورية لبحث المسائل التي تندرج ضمن المحاور الواردة في هذه المادة والمتعلقة بسيادة وأمن دول الحلف ولبناء الإستراتيجيات الأمنية للتصدي لمختلف أشكال التهديدات التي قد تمس بها وتقرير الإجراءات الضرورية حيالها، ويندرج إقرار سياسة الدفاع

[1]- Ryan Burton, op. cit, p. 12.

الإلكتروني ضمن طائفة الإجراءات المقررة للتصدي للهجمات الإلكترونية بصفة عامة بإعتبارها تمثل أحد أخطر التهديدات لسيادة وأمن الدول الأعضاء في حلف الناتو، ولقد بدأت المعالم الأولى لسياسة حلف الناتو للدفاع الإلكتروني تظهر بعد سنة 2001، وكما سبقت الإشارة إليه فإن إهتمام حلف الناتو بالفضاء الإلكتروني كمصدر جدي للمساس بأمن الدول الأعضاء فيه كان مع هجمات الحادي عشر سبتمبر؛ إذ بعد عام واحد منها أطلق حلف الناتو دعوة هامة لتحسين قدراته الدفاعية ضد الهجمات الإلكترونية وكان ذلك كجزء أساسي من التزام براغ الذي تم الموافقة عليه في نوفمبر من سنة 2002[1]، ليتم العمل فيما بعد على ترجمة هذه الدعوة إلى خطوات عملية تمثلت بداية في إصدار نص الدليل السياسي الشامل لحلف الناتو والذي تبناه رؤساء دول وحكومات الحلف في نوفمبر من سنة 2006، الذي يدور حول تعزيز القدرة على حماية أنظمة المعلومات ذات الأهمية الكبيرة بالنسبة للحلف ضد الهجمات على الأنترنت، وبعد تعرض استونيا لهجمات إلكترونية كبيرة قام حلف الناتو بدعوة وزراء دفاعه إلى تطوير سياسات دفاعية خاصة بشأن الهجمات الإلكترونية في أكتوبر من سنة 2007، ليقوم الحلف فيما بعد وللمرة الأولى في تاريخه بوضع سياسة رسمية للدفاع الإلكتروني وذلك في قمة بوخارست في سنة 2008؛ وعليه فقد تم تشكيل قيادة دفاع وفرق خاصة عبر الفضاء الإلكتروني للتصدي لأية محاولة لشن هجمات عبر الأنترنت وذلك للتنسيق فيما بين دول الحلف في حال تعرض إحداها لهجمات مصدرها الفضاء الإلكتروني والتعاون الأمني لحماية بنياتها الأساسية، وفي ماي من نفس السنة وقعت سبعة دول من أعضاء حلف الناتو على وثيقة تقضي بإنشاء دفاع مشترك إلكتروني وإنشاء مركز للخبرة والتدريب في عاصمة استونيا، ويهدف مركز الخبرة هذا إلى البحث والتدريب والتطوير المشترك فيما يخص حرب الفضاء الإلكتروني، كما أشار الحلف إلى ضرورة تبادل المعلومات على مستوى دوله وعلى ضرورة وجود آلية للإنذار المبكر حول أي نشاط مريب والكشف عن أي هجوم معلوماتي محتمل[2].

وفي إطار تفعيل حلف الناتو لسياسته الخاصة بالدفاع الإلكتروني وتطوير قدراته لصد هجمات الفضاء الإلكتروني فقد قام بإجراء عديد التمارين المتعلقة بإدارة وتسيير الأزمات الإلكترونية، ومنها قيامه في الثامن عشر من نوفمبر من سنة 2014 بإطلاق تمرين للدفاع الإلكتروني سُمي بـ" cyber

[1]– أولاف تايلر، مرجع سابق.

[2]– عادل عبد الصادق محمد الجخة، مرجع سابق، ص. ص. 266– 268.

coalition 2014"، والذي ضم أربع مئة (400) خبير عضو من الدول الأعضاء والدول الشريكة للحلف[1].

المطلب الثاني: جهود مكافحة التجسس الإلكتروني في إطار الاتفاقيات الإقليمية.

المتفحص للاتفاقيات الإقليمية المتعلقة بمكافحة الجريمة بمختلف أشكالها لا يقف على تخصيص أي واحدة منها مباشرة لغرض مكافحة التجسس الإلكتروني بمعنى عدم وجود اتفاقيات على المستوى الإقليمي تنظم أحكام هذه الجرائم على وجه التحديد وهو ذات السائد على الصعيد الدولي، لكن في المقابل وباعتبار التجسس الإلكتروني جريمة إلكترونية وبالبحث في الاتفاقيات الإقليمية المنظمة لهذا الموضوع نجد أن منها ما يتضمن مواد تنظم وبشكل صريح حالة مساس الجرائم الإلكترونية بالأمن الخارجي للدولة وبالمعلومات الإلكترونية الحكومية ذات الطابع السري؛ وعليه فهي تتضمن آليا الإشارة إلى التجسس الإلكتروني، ومنها ما يتضمن أحكاماً عامة تطبق على كافة طوائف الجريمة الإلكترونية بدون تخصيص فيمكن لذلك تطبيقها على حالة التجسس الإلكتروني، وفي هذا الإطار نقف على نموذجين مهمين للاتفاقيات الإقليمية الموجهة لمكافحة الجريمة الإلكترونية: النموذج الأول يرتبط بالتعاون العربي والمجسد من خلال القانون الاسترشادي لمكافحة جرائم تقنية المعلومات وكذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، أما النموذج الثاني فيرتبط بالتعاون الأوروبي والمجسد في اتفاقية بودابست حول الإجرام المعلوماتي، ومنه سيتناول الفرع الأول القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بينما يتناول الفرع الثاني الاتفاقية الأوروبية حول الإجرام المعلوماتي.

الفرع الأول: القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات والاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

لم تكن الدول العربية بمنأى عن مخاطر الجرائم الإلكترونية؛ نظراً لكونها من المستخدمين لتقنيات المعلومات والاتصالات الحديثة شأنها في ذلك شأن كل دول العالم، وهو ما دفع إلى التفكير في إطار جامعة الدول العربية – باعتبارها الإطار المجسد للتعاون العربي – في وضع نصوص قانونية لمواجهة هذه المخاطر والتهديدات التي تمس الأفراد كما تمس بسيادة وأمن الدول ذاتها، وبالنتيجة فقد تم

[1]- Ryan Burton, op. cit, p. 15.

التوصل إلى الاتفاق على وضع إطارين قانونيين يتم العمل من خلالهما على مكافحة الجرائم الإلكترونية بصفة عامة وضمنها تخصيص حالة المساس بالأمن الخارجي للدول وأسرارها القومية بنصوص صريحة، ويتعلق الأمر هنا بكل من القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي ستتم دراسة كل منهما في عنصر مستقل كما يلي:

أولاً- القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات:

يمثل القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات أولى مظاهر العمل لخلق تنسيق عربي وتوحيد جهود مواجهة الجرائم الإلكترونية، وذلك تحديداً من خلال التوصل إلى توحيد نظرة القوانين الوطنية الداخلية لهذه الجرائم؛ إذ يوفر هذا القانون مرجعية لكافة مشرعي الدول العربية لسن قوانينها المتعلقة بالتصدي لهذه الجرائم المستحدثة وخاصة منها التي تشكل تهديداً ومساساً بالأمن الخارجي للدولة كحالة التجسس الإلكتروني، وقد صدر القانون العربي النموذجي أو الاسترشادي في شأن مكافحة جرائم تقنية المعلومات كثمرة عمل مشترك بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية بعد أن تبين أن كليهما قدم مشروعاً في هذا الخصوص، وتم اجتماعهما المشترك خلال يومي 21 و22 من شهر ماي من سنة 2003 حيث تم النظر في المشروعين اللذين تم إعدادهما في نطاق المجلسين، وتم إعداد مشروع قانون مشترك عرض على المجلسين في الدورة العادية لكل منهما[1]، بحيث اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشر بموجب القرار رقم (495- د 19) بتاريخ الثامن أكتوبر من سنة 2003، واعتمده مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بموجب القرار رقم (417- د 21) بتاريخ 21 أفريل من سنة 2004، ويضم هذا القانون سبع وعشرين مادة تمثل النموذج القانوني الذي على الدول العربية الاسترشاد به لتجريم الأفعال المشكلة للجرائم الإلكترونية بصفة عامة ومنها تلك الماسة بالأمن الخارجي لها وتحديداً ما تعلق بالتجسس الإلكتروني، بينما تركت أمر تقدير العقوبة المناسبة لكل دولة بحسب ظروفها الداخلية، وفي هذا الإطار نص القانون العربي الاسترشادي على أن "كل من دخل عمداً وبغير وجه حق موقعاً أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني يعاقب بالسجن ... فإذا كان الدخول بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو بث أفكار تمس ذلك يكون الحد

[1]- رشيدة بوكر، مرجع سابق، ص. 134.

الأدنى للعقوبة السجن ..."[1]؛ وعليه يتبين من هذه المادة اعتراف القانون العربي الاسترشادي بالتهديد الذي تمثله تكنولوجيات المعلومات والاتصالات على أمن الدولة الخارجي وعلى أسرار دفاعها الوطني ودعوته الصريحة للتشريعات الداخلية لتتبنى تجريم أفعال التجسس الإلكتروني حين وضعها لقوانين مكافحة الجرائم الالكترونية؛ وقد استجابت عديد الدول العربية فعلاً لهذه الدعوة وهو ما يتجلى من خلال تضمينها لقوانينها المستحدثة والخاصة بمكافحة الجرائم الإلكترونية نصوصاً تتضمن تجريم المساس بأمن الدولة الخارجي والحصول على أسرار الدولة أو الإعتداء عليها عن طريق تكنولوجيات المعلومات والاتصالات، ومن أمثلة هذه القوانين نجد:

أ- نظام مكافحة جرائم المعلوماتية السعودي، والذي حدد بداية وقبل الشروع في تقرير أحكام التجريم والعقاب المقررة لهذه الجرائم، أهدافه العامة والمتمثلة خصوصاً في المساعدة على تحقيق الأمن المعلوماتي وحماية المصلحة العامة وحماية الاقتصاد الوطني[2]، بمعنى السعي خاصة للحفاظ على أمن وسرية المعلومات في وقت اعترف العالم كله والتشريعات الوطنية والدولية بقيم المعلومات التي قد تؤدي إلى حد نشوب حروب بين الدول ومن ذلك المعلومات التي تتعلق بأسرار هذه الدول؛ سيما وأن المعلومة قد زادت أهميتها في ظل ثورة تقنية المعلومات وتعدد الوسائط الإلكترونية التي يحتفظ عليها بهذه البيانات والمعلومات[3]؛ ولذلك فقد نصت المادة السابعة من ذات النظام على أنه: "يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: (1)- ... (2)- الدخول غير المشروع إلى موقع إلكتروني/ أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني".

ب- القانون الاتحادي المعدل في شأن مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة، حيث ينص على "يعاقب بالسجن كل من دخل وبغير وجه حق موقعاً أو نظاماً مباشرةً أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات

---

[1]- المادة 22 من القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات.

[2]- المادة الثانية من نظام مكافحة الجرائم المعلوماتية السعودي الصادر بقرار مجلس الوزراء رقم 79 وتاريخ 07/ 03 /1428 هجرية والذي تمت المصادقة عليه بموجب المرسوم الملكي رقم (م/ 17) و تاريخ 08/ 03/ 1428 هجرية.

[3]- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والأنترنت في التشريعات العربية (دراسة مقارنة مع التطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية)، دار النهضة العربية، مصر، 2009، ص. 13.

حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك. فإذا ترتب على الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها تكون العقوبة السجن مدة لا تقل عن خمس سنوات."[1].

ج- قانون جرائم المعلوماتية السوداني لسنة 2007، والذي ينص في مادته السابعة على: "كل من يدخل عمداً موقعاً أو نظاماً مباشرةً أو عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها بغرض:- الحصول على بيانات أو معلومات تمس الأمن القومي للبلاد أو الاقتصاد الوطني يعاقب بالسجن مدة لا تتجاوز السبع سنوات أو بالغرامة أو بالعقوبتين معا؛ إلغاء بيانات أو معلومات تمس الأمن القومي للبلاد أو الاقتصاد الوطني أو حذفها أو تدميرها أو تغييرها، يعاقب بالسجن مدة لا تتجاوز العشر سنوات أو بالغرامة أو بالعقوبتين معاً"[2].

د- قانون جرائم أنظمة المعلومات الأردني ، والذي ينص على: "(أ)- كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع إلكتروني أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني يعاقب بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن خمسمائة دينار ولا تزيد على خمسة آلاف دينار. (ب)- إذا كان الدخول المشار إليه في الفقرة (أ) من هذه المادة بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن ألف دينار ولا تزيد على خمسة آلاف دينار"[3].

وبالإضافة إلى تضمين القانون العربي الاسترشادي المادة الثانية والعشرين منه لتجريم التجسس الإلكتروني، فقد قام بتقرير عديد الأحكام الأخرى المتعلقة بالعقاب على ذات الأفعال ومنها معاقبة الشريك في ارتكاب الجرائم المنصوص عليها في المادة أعلاه بذات العقوبة المقررة لها[4]، والمعاقبة على الشروع في ارتكاب هذه الجرائم بذات العقوبة المقررة للجريمة التامة[5]، كما أقرت الحكم بمصادرة الأجهزة أو

---

[1]- المادة 22 من القانون الاتحادي رقم (2) لسنة 2006 المعدل في شأن مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة

[2]- هبة نبيلة هروال، مرجع سابق، ص. 382.

[3]- المادة 11 من قانون جرائم أنظمة المعلومات الأردني رقم (30) لسنة 2010.

[4]- المادة 23 من القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات.

[5]- المادة 24 من نفس القانون.

البرامج أو الوسائل المستخدمة في ارتكاب في ارتكاب هذه الجرائم وكذلك الأموال المتحصلة منها، بالإضافة إلى الحكم بإغلاق المحل أو المشروع الذي يكون محلاً لارتكاب هذه الجرائم[1]، كما يلاحظ أن القانون العربي الاسترشادي قد جاء بحكم جديد فيما يخص العقوبات، إذ قرر بأنه وفضلاً عن العقوبات المنصوص عليها في هذا القانون تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه وفقا للمادة الثانية والعشرين[2] أي يحكم عليه بسبب ارتكابه لفعل من أفعال تجسس إلكتروني.

من جهة ثانية فقد نص القانون العربي الاسترشادي على تقرير حق الدولة في إعمال مبدأ العينية، ومنح الاختصاص القضائي للدولة التي تضررت مصالحها بفعل أحد الجرائم المنصوص عليها في هذا القانون، ومنها تحديداً تلك الماسة بأمنها الخارجي وفي مقدمتها التجسس الإلكتروني، وهذا بغض النظر عن مكان ارتكابها، بحيث نص في مادته السادسة والعشرون على أن "تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه حتى ولو ارتكبت كلياً أو جزئياً خارج إقليم الدولة متى أضرت بأحد مصالحها ويختص القضاء الوطني بنظر الدعاوى المترتبة عليها".

ثانيـاً- الاتفاقيـة العربيـة لمكافحـة جرائـم تقنيـة المعلومـات:

جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات كتعبير عن رغبة الدول العربية في تعزيز التعاون فيما بينها لمكافحة هذه الطائفة من الجرائم التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعاً منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضدها[3]، وفي هذا الإطار لم تكتف الاتفاقية بتقرير الأحكام الموضوعية لمكافحة جرائم تقنية المعلومات فقط كما هو الشأن بالنسبة للقانون العربي الاسترشادي بل تضمنت فضلاً عنها تفصيلاً للأحكام الإجرائية التي تضمن تطبيق تلك الأحكام الموضوعية؛ وبهذا تكون الاتفاقية قد أسست لسياسة جنائية عربية مشتركة ترمي إلى الإحاطة بجميع عناصر مكافحة جرائم تقنية المعلومات ومنها جريمة التجسس الإلكتروني، وسيتم تناول الأحكام الموضوعية والأحكام الإجرائية لمكافحة التجسس الإلكتروني في إطار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات كل في عنصر مستقل كالآتي:

---

[1]- المادة 25 من القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات.

[2]- المادة 27 من نفس القانون.

[3]- أنظر الديباجة والمادة الأولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010 والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14- 252 المؤرخ في 08 سبتمبر سنة 2014.

أ- الأحكام الموضوعية لمكافحة التجسس الإلكتروني في إطار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

تضمنت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلزام الدول على تجريم الأفعال التي تم تبيينها في الفصل الثاني منها، وذلك وفقاً لتشريعاتها وأنظمتها الداخلية[1]، ومن بين هذه الأفعال نجد فعل الدخول غير المشروع لمنظومة معلوماتية والذي يشكل تجسساً إلكترونياً في حالة ما إذا ترتب عنه الحصول على معلومات حكومية سرية، وهذا ما يتبين من استقراء نص المادة السادسة من الاتفاقية العربية المتضمنة لجريمة الدخول غير المشروع و التي جاء فيها: "1- الدخول أو البقاء وكل إتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

2- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الإتصال أو الاستمرار بهذا الإتصال:

أ) ... ب) الحصول على معلومات حكومية سرية.".

وبالإضافة إلى تجريم فعل الدخول غير المشروع فقد جرم المشرع العربي بالمقابل فعل إساءة استخدام وسائل تقنية المعلومات والتي يقابلها في القانون الجزائري فعل التعامل غير المشروع في معطيات صالحة لارتكاب جرائم المساس بأنظمة المعالجة الآلية، بحيث تشمل جريمة إساءة استخدام وسائل تقنية المعلومات إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير أو حيازة، من جهة لأية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب جريمة الدخول غير المشروع، ومن جهة ثانية لكلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد ارتكاب جريمة الدخول غير المشروع[2]؛ وعليه يمكن القول بأن الاتفاقية العربية جرمت التجسس الإلكتروني من خلال تجريم فعل الدخول غير المشروع لمنظومة معلوماتية وكذلك من خلال تجريم فعل إساءة استخدام وسائل تقنية المعلومات.

[1]- المادة الخامسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2]- المادة التاسعة من نفس الاتفاقية.

بالإضافة إلى إلزام الاتفاقية العربية للدول على تجريم الأفعال السابقة فقد نصت على إلزامها كذلك بوضع أحكام تنظم الشروع والإشتراك في ارتكاب تلك الأفعال[1]، والعمل على تقرير المسؤولية الجنائية للأشخاص المعنوية عن ذات الأفعال[2].

بإجراء مقارنة بين ما ورد في كل من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ونصوص قانون العقوبات الجزائري المتعلقة بتجريم الأفعال التي تشكل مساساً بأنظمة المعالجة الآلية للمعطيات، يمكن القول أن المشرع الجزائري قد توسع في نطاق تجريم الأفعال التي قد تشكل تجسساً إلكترونياً ولم يحصره فقط في فعل الدخول غير المشروع بغرض الحصول على معلومات حكومية سرية، بل مده ليشمل كما سبق دراسته كل الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات إذا كانت تستهدف الدفاع الوطني، كما لم يقتصر تجريمه كما جاء في الاتفاقية العربية على فعل إساءة استخدام وسائل تقنية المعلومات والتي يقابلها في القانون الجزائري فعل التعامل غير المشروع في معطيات صالحة لارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات، بل جرم أيضا فعل التعامل غير المشروع في معطيات متحصل عليها من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، لكن بالمقابل فقد قرر المشرع الجزائري أحكاماً تتعلق بالإشتراك والشروع في ارتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات عموماً، كما أقر المسؤولية الجزائية للأشخاص المعنوية عن ذات الجرائم وهو ما ينسجم مع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

ب- الأحكام الإجرائية لمكافحة التجسس الإلكتروني في إطار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

في مقابل تجريم التجسس الإلكتروني فقد عملت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على توفير آليات تطبيق ذلك التجريم من خلال تقرير مجموعة من الأحكام الإجرائية تضمن متابعة المتهمين وتوفير أدلة إثبات ارتكابهم لتلك الأفعال، وباستقراء مواد الاتفاقية نلحظ عمل المشرع العربي على مستويين: يتعلق المستوى الأول بإلزام الدول بإدخال تعديلات على قوانينها الإجرائية الداخلية لكي تتماشى مع البيئة الجديدة لارتكاب الجرائم الإلكترونية، ويتعلق المستوى الثاني بتقرير إجراءات للتعاون

[1]- المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2]- المادة 20 من نفس الاتفاقية.

القانوني والقضائي بين الدول العربية لمكافحة ذات الجرائم؛ بحيث لا يمكن الحديث عن تعاون خارجي فعال بين الدول دون وجود قوانين داخلية تسمح بذلك التعاون وتوفر عوامل نجاحه، وسيتم التطرق لكلا المستويين في الآتي:

1- إلـزام الـدول الأطـراف علـى إدخـال تعديـلات علـى قوانينهـا الإجرائيـة الداخليـة: بحيث تضمنت الاتفاقية عديد النصوص التي تحث الدول العربية على وجوب تبني إجراءات للتحري والتحقيق في مجال جرائم تقنية المعلومات، ومنها:

- **تفتيـش المعلومـات المخزنـة:** بحيث ألزمت الاتفاقية كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها، وكذلك التفتيش أو الوصول إلى بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه، بالإضافة إلى إتخاذ الإجراءات الضرورية لتمكين السلطات المختصة من تمديد التفتيش إلى تقنية معلومات أخرى أو جزء منها متواجدة في إقليمها[1].

- **ضبـط المعلومـات المخزنـة:** بحيث ألزمت الاتفاقية كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها بعد القيام بالتفتيش الإلكتروني[2].

- **الجمـع الفـوري لمعلومـات تتبـع المستخدميـن:** بحيث ألزمت الاتفاقية كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من جمع أو تسجيل بواسطة الوسائل الفنية على إقليمها لمعلومات تتبع المستخدمين، والعمل على إلزام مزود الخدمة بذلك مع وجوب احتفاظه بسرية أية معلومة يطلع عليها عند تنفيذه لالتزاماته[3].

- **إعتـراض معلومـات المحتـوى:** بحيث ألزمت الاتفاقية كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من الجمع أو التسجيل بواسطة الوسائل الفنية على إقليمها

[1]- المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2]- المادة 27 من نفس الاتفاقية.

[3]- المادة 28 من نفس الاتفاقية.

لمعلومات محتوى الاتصالات المعينة، والعمل كذلك على إلزام مزود الخدمة بذلك مع وجوب احتفاظه بسرية أية معلومة يطلع عليها عند تنفيذه لالتزاماته[1].

بالرجوع إلى القانون الجزائري وتحديداً قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نلحظ أن هذا الأخير قد نص على كل هذه الإجراءات ونظم شروط وضوابط القيام بها، مع الأخذ بعين الإعتبار أن القانون الجزائري سابق من حيث الصدور على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

2- تقرير إجراءات التعاون القانوني والقضائي بين الدول العربية لمكافحة جرائم تقنية المعلومات: جاءت نصوص الاتفاقية التي تقرر إجراءات التعاون الإقليمي العربي فيما يخص مكافحة جرائم تقنية المعلومات كافة ومنها التجسس الإلكتروني بعد تلك المقررة لضرورة تبني الدول العربية في تشريعاتها الداخلية لإجراءات التحري والتحقيق الإلكترونية، وهو مسعى يهدف إلى ضمان إنجاح هذا التعاون العربي، وباستقراء نصوص الاتفاقية نجدها ترتكز بهذا الخصوص على ثلاثة محاور أساسية هي:

- **قواعد الاختصاص القضائي:** بحيث تضمنت الاتفاقية الحديث عن كل المبادئ القانونية التي يتم الاستناد إليها لتحديد الاختصاص القضائي للدولة بمتابعة جرائم تقنية المعلومات؛ إذ تضمنت النص على مبدأ الإقليمية من خلال تقرير حق الدولة في مد اختصاصها القضائي إذا ارتكبت إحدى تلك الجرائم ومنها التجسس الإلكتروني كلياً أو جزئياً أو تحققت في إقليمها أو على متن سفينة تحمل علمها أو على متن طائرة مسجلة تحت قوانينها، كما تضمنت النص على مبدأ الشخصية من خلال تقرير حق الدولة في مد اختصاصها القضائي إذا ارتكبت تلك الجرائم من قبل أحد مواطنيها، وهو المبدأ الذي لا محل لإعماله بالنسبة لجرائم التجسس الإلكتروني بالنسبة للقانون الجزائري باعتبار أن فاعلها يجب أن يكون أجنبياً لكن هذا لا يمنع من وجود قوانين عربية تنص على خلاف ذلك ولا تتبنى معيار الجنسية للتفريق بين ما يعتبر خيانةً وما يعتبر تجسساً، كما تضمنت النص على مبدأ العينية من خلال تقرير حق الدولة في مد اختصاصها القضائي إذا كانت الجريمة المرتكبة تمس أحد المصالح العليا للدولة[2]، وعليه يكون للدولة بموجب المبادئ السابقة الحصول على حق متابعة مرتكب جريمة التجسس الإلكتروني في حالة تواجده على إقليم دولة عربية أخرى طرف في الاتفاقية من خلال الحصول على تسليمه لها، وفي

[1]- المادة 29 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2]- الفقرة الأولى من المادة 30 من نفس الاتفاقية.

هذا الشأن تعرضت الاتفاقية العربية لاحتمال إدعاء أكثر من دولة طرف بالاختصاص القضائي بالجرائم المنصوص عليها فيها فقررت تقديم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها، وفي حالة إتحاد الظروف فتقدم الدولة الأسبق في طلب التسليم[1]، وعليه تتبين رغبة المشرع العربي في إعطاء الأولوية لمكافحة تلك الجرائم التي تمس بمصالح الدولة وتشكل تهديداً لأمنها ولعل الحصول على أسرار تلك الدول والذي يعتبر أحد غايات التجسس الإلكتروني أهم التهديدات والمخاطر التي تواجه أمنها، وهذا ما يتجلى من خلال تقديم إعمال مبدأ العينية على بقية المبادئ القانونية الأخرى بشأن تحديد الاختصاص القضائي للدولة المتضررة.

– **تسليـم المجرميـن:** يعد إجراء تسليم المجرمين أهم الإجراءات التي تمكن من مكافحة الجرائم بصفة عامة والتجسس الإلكتروني بصفة خاصة، وقد أقرت الاتفاقية العربية إمكانية التسليم بخصوص كل الجرائم الواردة فيها بدون استثناء، وأقرت بأن هذه الجرائم تعتبر قابلة للتسليم في أي معاهدة لتسليم المجرمين تكون قائمة بين الدول الأطراف، بل وأقرت بأن تُعد هي ذاتها كأساس قانوني لتسليم المجرمين بخصوص الجرائم الواردة فيها في حالة عدم وجود معاهدة تسليم بين دولتين عربيتين وكانت الدولة المطلوب منها التسليم تشترط وجود مثل هذه المعاهدة في حين لا يكون لدى الدولة الطالبة معاهدة للتسليم، بينما في الحالة التي لا تشترط فيها الدول الأطراف وجود معاهدة لتبادل المجرمين فيجب أن تعتبر الجرائم المنصوص عليها في الاتفاقية العربية قابلة لتسليم المجرمين بينها، وقد أخضعت الاتفاقية العربية تسليم المجرمين للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدة التسليم المطبقة بما في ذلك الأسس التي يمكن للدولة الطرف الاستناد عليها لرفض تسليم المجرمين، ومن السائد أن كافة الدول ترفض تسليم مواطنيها لغرض متابعتهم أمام الجهات القضائية لدولة أخرى؛ وقد اعترفت الاتفاقية العربية بهذا الأمر لكنها في المقابل نصت على أن تتعهد تلك الدولة الرافضة وفي الحدود التي يمتد إليها اختصاصها بتوجيه الاتهام ضد من يرتكب من مواطنيها لدى أي من الدول الأطراف الأخرى جرائم معاقب عليها في قانون كل من الدولتين بعقوبة سالبة للحرية مدتها سنة أو بعقوبة أشد، وذلك إذا ما وجهت إليها الدولة الطرف الأخرى طلباً بالملاحقة[2].

[1]– الفقرة الثالثة من المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2]– المادة 31 من نفس الاتفاقية.

- **المساعدة المتبادلة:** بحيث قررت الاتفاقية العربية وجوب قيام جميع الدول الأطراف بتبادل المساعدة فيما بينها وبأقصى الحدود الممكنة لغايات التحقيقات أو الإجراءات أو لجمع الأدلة الإلكترونية المتعلقة بالجرائم المنصوص عليها فيها بدون استثناء، مع إخضاعها للمساعدة بشكل رئيسي للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة أو في معاهدات المساعدة المتبادلة بما في ذلك الأسس التي تعتمد عليها الدولة المطلوب منها المساعدة لرفض التعاون[1]، وقد شملت الاتفاقية عديد المجالات التي يمكن أن تمتد إليها المساعدة، ومن أمثلتها التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة؛ إذ منحت الاتفاقية إمكانية أن تطلب دولة طرف من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضي الدولة الطرف المطلوب منها[2]، وكذلك ضرورة قيام الدول الأطراف بتوفير المساعدة الثنائية لبعضها البعض بخصوص الجمع الفوري لمعلومات تتبع المستخدمين المصاحبة لاتصالات معينة في أقاليمها والتي تبث بواسطة تقنية المعلومات[3]، بالإضافة إلى ضرورة قيام الدول الأطراف بتوفير المساعدة الثنائية لبعضها فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معينة تبث بواسطة تقنية المعلومات في الحدود المسموح بها[4].

بالرجوع إلى قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نجده يقضي بإمكانية تبادل السلطات المختصة المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني[5]، لكنه بالمقابل يقضي برفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام[6]، وهو نفس ما أقرته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بحيث أجازت للدولة الطرف المطلوب منها المساعدة أن ترفضها إذا إعتبرت أن تنفيذ الطلب يمكن أن يشكل انتهاكاً لسيادتها أو أمنها أو نظامها أو مصالحها الأساسية، إلا أنها أضافت سبباً آخر يمكن للدولة

---

[1]- المادة 32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2]- المادة 39 من نفس الاتفاقية.

[3]- المادة 41 من نفس الاتفاقية.

[4]- المادة 42 من نفس الاتفاقية.

[5]- المادة 16 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[6]- المادة 18 من نفس القانون.

المطلوب منها المساعدة أن تستند إليه لرفض تلبية طلب المساعدة وهو حالة ما إذا كان الطلب متعلقاً بجريمة تعتبرها هذه الدولة جريمة سياسية[1].

الفـــرع الثانـــي: الاتفاقيـة الأوروبيـة حـول الإجـرام المعلوماتـي (اتفاقيـة بودابسـت):

تعد الاتفاقية الأوروبية حول الإجرام المعلوماتي أحد المرجعيات المهمة للتصدي للجريمة الإلكترونية بمختلف أشكالها على المستوى الأوروبي وحتى على المستوى الدولي، وتجدر الإشارة في هذا الإطار إلى أنه ورغم قيام عديد الدول غير الأوروبية بالإشتراك فيها كالولايات المتحدة الأمريكية واليابان وكندا وجنوب إفريقيا إلا أنها لا تشكل اتفاقية دولية بحق إذ لم تشارك فيها أية دولة نامية[2]، كما أنها شكلت بالأساس ثمرة جهود قام بها مجلس أوروبا على مدار سنوات[3].

تشكل اتفاقية بودابست نموذجاً قانونياً شاملاً نص على كل عناصر ومتطلبات مواجهة الجرائم الإلكترونية بصفة عامة ابتداءً من تقريرها لمجموعة من الأحكام الموضوعية والإجرائية التي على الدول

---

[1]– المادة 35 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2]– إيهاب ماهر السنباطي، الجرائم الإلكترونية (الجرائم السيبيرية): قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد، مداخلة مقدمة في إطار الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19– 20 أفريل 2007.

[3]– تعود بدايات إهتمام مجلس أوروبا بموضوع الجريمة الإلكترونية إلى انعقاد المؤتمر الثاني عشر لمديري معاهد الأبحاث الإجرامية حول المظاهر الإجرامية للجريمة الإقتصادية المنعقد في ستراسبورغ سنة 1976؛ إذ أشار المجلس إلى الطابع العالمي للجرائم الإلكترونية، ومنذ ذلك الحين أصبح هذا الموضوع انشغالاً أقصى للمنظمة؛ إذ قام مجلس أوروبا سنة 1985 بإنشاء لجنة خبراء مكلفة بدراسة المظاهر القانونية للإجرام الإلكتروني، وفي سنة 1989 تبنت اللجنة الأوروبية للمسائل الجنائية تقريراً حول الإجرام ذو الصلة بالحاسوب و درست نصوصا قانونية موضوعية في القانون الجزائي والتي يعد تطبيقها ضرورياً من أجل مكافحة الأشكال الجديدة للجرائم الإلكترونية، وبتاريخ 13 سبتمبر من سنة 1989 تبنت لجنة الوزراء لمجلس أوروبا توصية تحت رقم (89/ 9) تؤكد الطابع العالمي والعابر للحدود للإجرام الإلكتروني وضرورة التنسيق بين التشريعات وتطوير التعاون القانوني الدولي ووحدت فيها مجموعة توجيهات للدول الأعضاء، كما اتخذت نفس اللجنة في سنة 1995 توصية جديدة تحت رقم (95/ 13) تعالج نتائج الإجرام المعلوماتي العابر للحدود، وفي سنة 1996 قررت اللجنة الأوروبية للمسائل الجنائية إنشاء لجنة خبراء مكلفة بالإجرام المعلوماتي وكان الهدف من إنشاءها لا يتعلق باتخاذ توصية جديدة ولكن بإعداد اتفاقية، وتوالت فيما بعد اجتماعات هذه اللجنة بين سنوات 1997 و2000 للتوصل للنسخة النهائية لمشروع الاتفاقية في أفريل سنة 2001، ثم عرض النص على لجنة الوزراء لتتبناه ولفتحه للتوقيع وهذا ما تم في العاصمة المجرية بودابست بتاريخ 23 نوفمبر سنة 2001، أنظر لأكثر تفاصيل:
- Marco Gercke, op. cit, p. p. 110 - 112.

الأطراف الاستناد إليها حين صياغة تشريعاتها الداخلية وصولاً إلى تحديد مبادئ التعاون الدولي لضمان فعالية جهود مكافحة هذه الجرائم، والملاحظ عند استقراء نصوص هذه الاتفاقية أن معظم الأحكام الواردة فيها تتطابق إلى حد بعيد مع ما هو مقرر في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات باستثناء بعض الأحكام التي انفردت هذه الأخيرة بالنص عليها، وباعتبار أن الاتفاقية الأوروبية قد تضمنت النص على أحكام مكافحة الجريمة الإلكترونية بصفة عامة وبدون تخصيص؛ فسيتم بحث مكافحة التجسس الإلكتروني في إطار تلك الأحكام العامة من منطلق كونه أحد صور هذه الجرائم مع إجراء مقارنة بين ما ورد في الاتفاقية الأوروبية والاتفاقية العربية في ذات الشأن وهذا من خلال العنصرين الآتيين:

أولاً- الأحكام الموضوعية لمكافحة الجرائم الالكترونية في إطار الاتفاقية الأوروبية حول الإجرام المعلوماتي:

من ناحية الأحكام الموضوعية تناولت الاتفاقية الأوروبية إلزام الدول الأطراف على تجريم مجموعة من الأفعال التي تمس سرية وأمن وسلامة وتوافر بيانات الكمبيوتر ومنظوماته، ومنها تحديداً فعل الدخول غير المشروع على منظومة الكمبيوتر بقصد الحصول على بيانات الكمبيوتر[1]، وفعل الاعتراض غير المشروع لخط سير البيانات باستخدام الوسائل الفنية بما في ذلك التقاط ما ينبعث من منظومة الكمبيوتر من موجات كهرومغناطيسية تحمل معها هذه البيانات[2]، وفعل التدخل في البيانات الذي يقوم على إتلاف أو إلغاء أو إفساد أو تغيير أو تدمير البيانات الموجودة بالكمبيوتر[3]، وفعل إساءة استخدام الأجهزة و الذي يقوم على إنتاج أو بيع أو حيازة أو الحصول على جهاز أو برنامج كومبيوتر يتم تصميمه أساساً بغرض ارتكاب إحدى الجرائم السابقة[4]، والملاحظ أن كل هذه الأفعال تشكل جوهر التجسس الإلكتروني والذي قام المشرع الجزائري بتجريمها من خلال نصوص قانون العقوبات المنظمة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات واعتبرها مصدراً لتهديد الدفاع الوطني، وبإجراء مقارنة بين مذهب الاتفاقية الأوروبية ومذهب الاتفاقية العربية في التجريم نجد أن هذه الأخيرة قد نصت على ذات الأفعال السابقة وباستخدام نفس المصطلحات، لكن الفرق بينهما يكمن في أن الاتفاقية العربية نصت

[1]- المادة الثانية من الاتفاقية الأوروبية حول الإجرام المعلوماتي.

[2]- المادة الثالثة من نفس الاتفاقية.

[3]- المادة الرابعة من نفس الاتفاقية.

[4]- المادة السادسة من نفس الاتفاقية.

بشكل صريح على الحصول على المعلومات الحكومية السرية لكنها بالمقابل أدرجت هذا الفعل ضمن النص الذي يتناول جريمة الدخول غير المشروع فقط؛ فهي بذلك تجرم سلوكاً واحدا فقط من سلوكات التجسس الإلكتروني وهو الدخول غير المشروع لمنظومة معلوماتية، بينما الاتفاقية الأوروبية لم تحدد نوع البيانات أو المعلومات التي تقع عليها مختلف الاعتداءات السابقة أي لم تشترط أن تكون هذه المعلومات ذات طبيعة سرية أو غير سرية بمعنى تفادت الإشارة بشكل صريح للتجسس الإلكتروني وتركته يدخل ضمن الأحكام العامة المنصوص عليها فيها.

ثانياً- الأحكام الإجرائية لمكافحة الجرائم الإلكترونية في إطار الاتفاقية الأوروبية حول الإجرام المعلوماتي:

من ناحية الأحكام الإجرائية تضمنت الاتفاقية الأوروبية وكما هو الشأن تماماً في الاتفاقية العربية، من جهة، إلزام الدول الأطراف على إدخال تعديلات على قوانينها الإجرائية الداخلية من حيث نصها على ضرورة قيام هذه الدول بتبني إجراءات التحري والتحقيق في البيئة الإلكترونية، ويتعلق الأمر هنا بالنص على إجراء تفتيش وحجز منظومة الكمبيوتر[1]، وإجراء تجميع بيانات الكمبيوتر في الوقت الصحيح[2]، والذي يقابله إجراء الجمع الفوري لمعلومات تتبع المستخدمين المنصوص عليه في المادة 28 من الاتفاقية العربية، وإجراء اعتراض مضمون البيانات[3]، والذي يقابله إجراء اعتراض معلومات المحتوى المنصوص عليه في المادة 29 من الاتفاقية العربية، ومن جهة ثانية تقرير إجراءات التعاون الدولي من حيث إلزام الاتفاقية للدول الأطراف بضرورة تفعيل إجراء تسليم المجرمين[4]، وكذلك تبادل المساعدة إلى أقصى حد ممكن فيما يخص القيام بعمليات التحقيق والإجراءات المتعلقة بالجرائم الإلكترونية ومثالها تبادل المساعدات في تجميع البيانات خلال خط سيرها وكذلك في تجميع أو تسجيل مضمون البيانات الخاصة باتصالات معينة[5]، لكن الاختلاف المسجل فيما يخص الأحكام الإجرائية يتعلق بالنص الذي يحدد قواعد الاختصاص القضائي بمتابعة الجرائم الإلكترونية؛ بحيث تضمنت الاتفاقية الأوروبية في

[1]- المادة 19 من الاتفاقية الأوروبية حول الإجرام المعلوماتي.

[2]- المادة 20 من نفس الاتفاقية.

[3]- المادة 21 من نفس الاتفاقية.

[4]- المادة 24 من نفس الاتفاقية.

[5]- المواد 25 و33 و34 من نفس الاتفاقية.

مادتها الثانية والعشرين النص فقط على مبدأي الإقليمية والشخصية بينما كانت الاتفاقية العربية أكثر شمولاً؛ بحيث تضمنت النص كذلك على إعمال مبدأ العينية والذي يكون للدولة بموجبه الاختصاص بمتابعة الجرائم الإلكترونية في حالة مساسها بأحد مصالحها العليا وتشكيلها تهديداً لأمنها؛ وعليه يمكن القول بأن الاتفاقية العربية قد اعترفت وبشكل صريح بخطورة بعض الجرائم الإلكترونية على أمن الدولة ووفرت بذلك سنداً قانونياً يمكن الدولة من متابعة هذا الصنف من الجرائم ومنها التجسس الإلكتروني، بل ومنحته الأولوية في تقرير الدولة الأحق بالحصول على تسليم المجرمين، بعكس الاتفاقية الأوروبية التي تفادت النص على هذا المبدأ؛ ويمكن رد ذلك إلى طبيعة هذه الاتفاقية في حد ذاتها فهي إن صح التعبير اتفاقية إقليمية ذات بعد دولي، بحيث تضم فضلاً عن الدول الأوروبية عديد الدول الأخرى كالولايات المتحدة الأمريكية وكندا واليابان وجنوب إفريقيا وغيرها مع إقرارها بإمكانية انضمام أية دولة أخرى لها؛ لذا يشكل الاعتراف بمبدأ العينية ومن خلاله حق الدولة في الحصول على الجواسيس مساساً بسلوكات التجسس التي تقوم بها هذه الدول وعلى رأسها الولايات المتحدة، ويكرس إتجاه تجريم التجسس كسلوك غير مشروع على المستوى الدولي وهو الأمر الذي تتعمد الدول عدم إقراره وذلك ما يفسر من جهة أخرى عدم وجود اتفاقية دولية لمكافحة التجسس لحد الآن.

المبحث الثاني: جهود مكافحة التجسس الإلكتروني في إطار المنظمات الدولية والاتفاقيات الدولية.

تنطلق عادة كل المبادرات الرامية لوضع أحكام خاصة بموضوع معين من خلال استشعار أهميته ومدى اتساع تأثيراته على المستوى الدولي؛ فيتم طرحه على الجهات والتنظيمات التي يدخل هذا الموضوع ضمن دائرة اهتمامها، فتبدأ بذلك الدراسة الجدية والمركزة للموضوع لتحديد إطار قانوني يحكمه، وذلك من خلال تنظيم الملتقيات وإصدار القرارات والتوصيات، وعادة ما تنتهي هذه الجهود وتترجم إلى اتفاقيات دولية تنظم المسألة المطروحة صراحةً أو تتضمن أحكاماً جزئية تتعلق بموضوع آخر ذو صلة بالموضوع الأساسي للاتفاقية، وهذا ما نلحظه تحديداً بخصوص التجسس الإلكتروني والذي تتوزع أحكام مكافحته على اتفاقيات تنظم بالأساس مسائل أخرى؛ وعليه سيتم تناول هذا المبحث من خلال مطلبين: يتضمن المطلب الأول جهود مكافحة التجسس الإلكتروني في إطار المنظمات الدولية، ويتضمن المطلب الثاني جهود مكافحة التجسس الإلكتروني في إطار الاتفاقيات الدولية.

المطلب الأول: جهود مكافحة التجسس الإلكتروني في إطار المنظمات الدولية.

تعد هيئة الأمم المتحدة المنظمة الدولية الأهم التي يتم عبرها وعبر وكالاتها المتخصصة وضع كل الإستراتيجيات الدولية لمكافحة مختلف التهديدات والمخاطر التي تواجه المجتمع الدولي ككل، وفي إطار الإجرام الإلكتروني كان لكل هذه الكيانات دور في إرساء قواعد ومبادئ دولية تهدف للتصدي لمخاطر هذا الإجرام على أمن الدول جميعاً دون استثناء، وإن كانت هذه المبادرات في أغلبها تركز على فكرة الأمن المعلوماتي وتجعله محوراً لها، باعتبار أن الأمن المعلوماتي يلعب الدور الرئيس في منع حدوث كل أنواع الجرائم الإلكترونية دون استثناء، فيكون بذلك نقطة إلتقاء بين الدول فيما يخص مكافحة التجسس الإلكتروني ولو كان ذلك بطريقة غير مباشرة وبشكل غير صريح؛ وعليه سيتم في الفرع الأول تناول جهود مكافحة التجسس الإلكتروني في إطار منظمة الأمم المتحدة، وفي الفرع الثاني تناول جهود مكافحة التجسس الإلكتروني في إطار الوكالات المتخصصة التابعة لهيئة الأمم المتحدة، ثم تخصيص الفرع الثالث للأمن المعلوماتي كمحور إلتقاء توصيات المنظمات الدولية لمكافحة التجسس الإلكتروني.

الفـــرع الأول: جهود مكافحة التجسس الإلكتروني في إطار منظمة الأمم المتحدة.

يمكن استخلاص الجهود الدولية لمكافحة التجسس الإلكتروني من خلال القرارات والتوصيات التي خرجت بها الأعمال المختلفة لهيئة الأمم المتحدة، وإن كان طرح وتناول هذه المسألة لم يتم بشكل مباشر، إلا أن تلك القرارات فيها ما يشكل إطاراً دولياً قد يسهم في مواجهة التهديدات التي يشكلها التجسس الإلكتروني بالنسبة للدول، وهذا ما يتضح من خلال الجهود الرامية لدعم الاستخدام السلمي للفضاء الإلكتروني أو من خلال الجهود الرامية إلى تحقيق الإدارة المشتركة للأنترنت وإنهاء هيمنة وسيطرة بعض الأطراف على هذه الشبكة والتي تم طرحها وتناولها من طرف القمة العالمية لمجتمع المعلومات وإدارة الأنترنت.

أولاً- جهود الأمم المتحدة لدعم الاستخدام السلمي للفضاء الإلكتروني:

أصبح حالياً الفضاء الإلكتروني المجال الخامس (بعد المجال البري والبحري والجوي والفضائي) الذي تسعى الدول لإيجاد موقع لها فيه؛ وذلك بغية استغلاله لأغراض عديدة أهمها القيام بشن حروب معلوماتية؛ لما يوفره من وسائل يمكن استغلالها للوصول إلى المعلومات الحساسة والسرية للدول الأخرى ومن ثم سرقتها أو تدميرها أو منع أصحابها من استغلالها، فلا يمكن الإنكار أن الأنترنت اليوم قد

أصبحت جزءاً مهما من الُبنى التحتية العسكرية الإستراتيجية الأمر الذي جلب الانتباه إلى مسألة استخدام الفضاء الإلكتروني لأغراض غير سلمية بعكس طبيعته الأصلية، فنادى البعض بمنع عسكرة الفضاء الإلكتروني بينما يؤكد البعض الآخر عدم إمكانية تجنب الأمر[1]، خاصة بعد توجه غير الدول لاستخدام ميزات هذا الفضاء لتحقيق أهدافها كالمنظمات الإرهابية خاصة؛ لذا حاول البعض الآخر أن يجد سنداً قانونياً دولياً لتجريم الاستخدام غير السلمي للفضاء الإلكتروني، فذهب إلى أن ميثاق هيئة الأمم المتحدة وإن لم ينص صراحة على تجريم استخدام حرب المعلومات فإن روح الميثاق يتفق مع تجريم استخدامه، باعتباره يمثل انتهاكاً لما ورد في الميثاق بخصوص التهديد واستخدام القوة ضد أية دولة، كما أن الميثاق ذاته في مادته الثانية قد أوصى الدول الأعضاء بأن يفضوا منازعاتهم الدولية بالوسائل السلمية على وجه لا يجعل السلم والأمن والعدل الدولي عرضة للخطر؛ ومن ثم فإن التجاء الدول إلى تسوية منازعاتها وصراعاتها عبر الفضاء الإلكتروني يعرض الأمن والسلم الدولي والطابع السلمي للعلاقات الدولية للخطر[2].

إن مسألة الاستخدام السلمي للفضاء الإلكتروني عرفت بدايات طرحها عالمياً في منتصف سبعينات القرن الماضي، وكان ذلك من خلال الإعلان الخاص باستخدام التقدم العلمي والتكنولوجي لصالح السلم وخير البشرية، والذي تم تبنيه بموجب قرار الجمعية العامة للأمم المتحدة في العاشر نوفمبر من سنة 1975، والذي أكد على أن جميع الدول يجب أن تنهض بالتعاون الدولي لضمان استخدام نتائج التطورات العلمية والتكنولوجية لصالح تدعيم السلم والأمن الدوليين، وأن تمتنع الدول عن أية أعمال تستخدم فيها المنجزات العلمية والتكنولوجية لأغراض انتهاك سيادة الدول الأخرى وسلامتها الإقليمية أو التدخل في شؤونها الداخلية أو شن الحروب العدوانية، وأن هذه الأعمال لا تمثل خرقاً صارخاً لميثاق الأمم المتحدة ومبادئ القانون الدولي فحسب، بل تشكل أيضا تشويها غير مقبول للمقاصد التي ينبغي أن توجه التطورات العلمية والتكنولوجية لخير البشرية[3].

من جهة أخرى فقد أصدرت هيئة الأمم المتحدة عبر جمعيتها العامة عدداً من القرارات التي توضح مدى تصاعد الإهتمام العالمي باستخدام تكنولوجيا الاتصال والمعلومات استخداماً غير سلمي؛

---

[1]- Ron Smith et Scott Knight, op. cit, p. 49.

[2]– محمد محمد صالح الألفي، مرجع سابق، ص. 278.

[3]– عادل عبد الصادق محمد الجخة، مرجع سابق، ص. ص. 234– 235.

بحيث تمت الإشارة لأول مرة إلى الاستخدام العسكري المحتمل لتكنولوجيا الاتصال والمعلومات في قرار الجمعية العامة في الدورة 49/54 في الأول ديسمبر من سنة 1999، ثم توالت القرارات التي تناولت ذات الموضوع ومنها قرار الجمعية العامة في الدورة 28/55 في ديسمبر من سنة 2000 والدورة 19/56 في 19 ديسمبر من سنة 2001 بشأن إرساء الأساس القانوني لمكافحة إساءة استعمال تكنولوجيا الاتصال والمعلومات في أعمال إجرامية، وركزت تلك القرارات على أن التطورات العلمية والتكنولوجية يمكن أن يكون لها تطبيقات مدنية وعسكرية على السواء، وبأنه يلزم مواصلة وتشجيع التقدم المحرز في تسخير العلم والتكنولوجيا لأغراض التطبيقات المدنية، وفي هذا السياق إتخذت الجمعية العامة للأمم المتحدة في الدورة 258/56 بتاريخ 31 يناير سنة 2002 قراراً يدعو إلى استخدام تكنولوجيا الاتصال والمعلومات من أجل التنمية.

ويُذكر هنا أن روسيا قد قدمت في ديسمبر 1998 اقتراحاً للجمعية العامة للأمم المتحدة طالبت فيه بوضع مسودة قرار يتعلق بأمن المعلومات حمل مسمى "التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي" وتبنتها بالإجماع الجمعية العامة للأمم المتحدة في الدورة 70/53 المنعقدة في الرابع من ديسمبر 1998، ودعا القرار أعضاء الأمم المتحدة لترسيخ التعاون الثنائي والمتعدد الأطراف والأخذ بعين الاعتبار الأخطار المحتملة والقائمة في مجال أمن المعلومات، ودعا القرار أيضا كل الدول لإبلاغ الأمين العام للأمم المتحدة بوجهات نظرهم حول تحديد الأفكار الأساسية المرتبطة بقضايا أمن المعلومات والعمل على تطوير المبادئ الدولية التي من شأنها دعم أمن نظم المعلومات والاتصالات الدولية والمساعدة في مكافحة الاستخدام الإرهابي والإجرامي لها، هذا وقد كانت روسيا قد قدمت للجمعية العامة قراراً سعى إلى تطوير اتفاقيات الحد من التسلح لكي تشمل عمليات شبكات المعلومات، وحملت مسودة القرار الروسي في الدورة 70/53 للجمعية العامة للأمم المتحدة دعوة الدول الأعضاء لدعم اتجاهات الأخذ في الاعتبار الأخطار القائمة والمحتملة في مجال أمن المعلومات، والتقدم في مجال تنمية المبادئ الدولية التي يمكن أن تدعم أمن نظم المعلومات والاتصالات العالمية، والمساعدة في مكافحة الإرهاب المعلوماتي والجريمة، وأشار القرار الروسي إلى أهمية إدراك أن استخدام أسلحة المعلومات ضد البنية التحتية الحيوية يأتي مشابها لنتائج استخدام أسلحة الدمار الشامل، كما تبنت الأمم المتحدة إقتراحاً روسيا في ماي من سنة 2000 يدعو إلى "تحديد المفاهيم المرتبطة بأمن المعلومات والتي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية"، وفي عام 2001 وافق أعضاء الأمم المتحدة على إنشاء

مجموعة الخبراء الحكومية التي بدأت عملها في عام 2004 بهدف مناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات الدولي والإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية، وتعد تلك أول مرة يتم إتخاذ قرار سياسي على المستوى الدولي لترجمة الجهود الدولية إلى خطوات عملية[1]، ولكن على الرغم من إجتماع مجموعة الخبراء في عامي 2004 و2005 بهدف وضع ترتيبات لمسودة قرار يقدم للأمانة العامة للأمم المتحدة إلا أنها فشلت في التوصل إلى مسودة للقرار واصطدمت بإشكالية إذا ما كان القانون الدولي الإنساني أو القانون الدولي تحديداً يمكنه أن ينظم الأبعاد الأمنية للعلاقات الدولية في حالة الاستخدام العدائي لتكنولوجيا الاتصال والمعلومات عن طريق توظيفها للأغراض العسكرية والسياسية[2].

ثانيـاً- القمـة العالميـة لمجتمـع المعلومـات وإدارة الأنترنـت:

بالإضافة إلى الجهود السابقة فقد إتجهت جهود أخرى إلى العمل على إنهاء هيمنة الولايات المتحدة الأمريكية على عمل شبكة الأنترنت؛ بحيث تسيطر هذه الدولة على النظام الذي يوزع أسماء المواقع ونطاق عملها والشفرة الرقمية التي توصل أجهزة الكمبيوتر إليها عبر برامج متخصصة مما يمكنها وبشكل حصري من إدارة الشبكة ومراقبتها، وهو موقف تراه الكثير من الدول غير عادل؛ ومن ثم تنادي بنوع من الإدارة المشتركة للشبكة بما يجعلها غير مرهونة بدولة بعينها وإنما بمجموع إرادات الدول المستخدمة لها، مع المشاركة في وضع المعايير التي تحدد الإباحة والحظر في استخدام الشبكة، ومدى حقوق الأفراد والجماعات في الوصول إلى مصادر المعلومات وفي تداولها، خاصة مع شيوع ما يسمى بضرورات الأمن مقابل اعتبارات الحرية[3].

ترى الدول النامية خصوصاً، أن الأنترنت أصبحت مرفقاً عالمياً وليس خاصاً بالولايات المتحدة، وأنها من أهم الركائز الأساسية لإقامة مجتمع المعلومات القطري أو الإقليمي أو العالمي؛ وبالتالي هناك أهمية قصوى لمناقشة وضبط الطريقة التي تدار بها الشبكة والجهة التي تسيطر عليها، وأن منظمة الإيكان لا تخضع لأية اتفاقيات دولية تتعلق بسياسة إدارة الأنترنت، مما يعني أن تكون عرضة لقرارات تعسفية أحادية الجانب بدون أن يكون لأية دولة حق الرفض، وأن ترك الوضع على ما هو عليه سيضع

[1]- عادل عبد الصادق محمد الجخة، مرجع سابق، ص. ص. 240- 242.

[2]- محمد محمد صالح الألفي، مرجع سابق، ص. ص. 279- 280.

[3]- عادل عبد الصادق محمد الجخة، مرجع سابق، ص. ص. 242- 243.

في يد الولايات المتحدة أوراق ضغط إضافية على العالم ربما تتطور إلى إجراءات قد تضر بالآخرين، وترى ذات الدول أن سيطرة أي طرف على إدارة الأنترنت بدون ضوابط يجعلها عرضة للتلصص والتجسس، ومن ذلك المحاولات التي تم اتخاذها بدعوى مكافحة الإرهاب؛ حيث أخذت شكل إجراءات رسمية حكومية علنية بعد أن كانت مثل هذه الإجراءات محصورة في أعمال أجهزة الاستخبارات وحسب.

ولقد تم طرح مسألة إدارة الأنترنت من خلال القمة العالمية لمجتمع المعلومات والتي عقدت دورتها الأولى في جنيف سنة 2003 ودورتها الثانية في تونس سنة 2005 وذلك برعاية الأمم المتحدة، بحيث اتفقت جميع الحكومات في المرحلة الأولى للقمة العالمية على أن السلطة السياسية على قضايا السياسات العامة المتصلة بالأنترنت تعتبر حقاً سيادياً للدول لذا طالبت الأمين العام للأمم المتحدة بضرورة البحث في مسألة إدارة الأنترنت، بدأً من صياغة تعريف لهذه العبارة كنقطة انطلاق للبحث في غير ذلك من الموضوعات، ليشكل ذات الموضوع أي إدارة شبكة الأنترنت المحور المسيطر على أعمال قمة تونس وذلك لتحولها من البعد التقني والفني إلى أن تصبح ذات بعد سياسي واجتماعي[1].

لهذا الغرض فقد شكلت الأمانة العامة لهيئة الأمم المتحدة فريقاً دولياً لدراسة قضية إدارة الأنترنت؛ وقد انتهى فريق العمل إلى إيجاد بعض التصورات بهذا الخصوص، يتمثل التصور الأول في إقامة مجلس عالمي للأنترنت يتألف من أعضاء الحكومات، ويوفر تمثيلاً مناسباً عن كل منطقة، ويكون له علاقة بمؤسسات الأنترنت، وربطه بالأمم المتحدة، وأن يكون للقطاع الحكومي دور قيادي وللقطاع الخاص والمدني دور استشاري، ويتمثل التصور الثاني في تشكيل مجلس دولي للأنترنت ينهض فيما يتعلق بالسياسات التي تمس المصالح الوطنية للدول عبر الوظائف الموازية لاختصاص هيئة الأنترنت، أما التصور الثالث فقد اقترح إقامة ثلاثة كيانات مؤسسية عالمية لمعالجة وإدارة ورسم السياسات والإشراف على الهيئة والتنسيق العالمي[2].

وقد جاء في إعلان المبادئ أن الأنترنت قد تطورت لتصبح مرفقاً عالمياً متاحاً للعامة، وينبغي أن تشكل إدارتها قضية مركزية في جدول أعمال مجتمع المعلومات، وينبغي أن تكون الإدارة الدولية للأنترنت متعددة الأطراف وشفافة وديمقراطية وبمشاركة كاملة من الحكومات والقطاع الخاص والمجتمع المدني والمنظمات الدولية، كما جاء فيه أن إدارة الأنترنت تنطوي على قضايا تقنية وقضايا تتعلق

[1]– محمد محمد صالح الألفي، مرجع سابق، ص. ص. 280– 281.

[2]– عادل عبد الصادق محمد الجخة، مرجع سابق، ص. ص. 242– 243.

بالسياسات العامة على حد سواء وينبغي أن يشترك فيها جميع أصحاب المصلحة والمنظمات الدولية الحكومية والمنظمات الدولية ذات الصلة[1].

إن الموضوعات والمسائل التي أثارتها هيئة الأمم المتحدة من خلال قراراتها ومؤتمراتها جد مهمة ومؤثرة في مجال مكافحة التجسس الإلكتروني؛ فطرح قضية عسكرة الفضاء الإلكتروني واستخدامه غير السلمي واعتبار وسائله وتقنياته بمثابة أسلحة مما يجعله يعرض السلم والأمن الدوليين للخطر، هو بمثابة اعتراف بعدم مشروعية التجسس الإلكتروني وبكونه عملاً عدائياً من دولة ضد دولة أخرى، وكذلك طرح مسألة التخلص من السيطرة والهيمنة الأحادية الجانب على الأنترنت من شأنه أن يحد من سلطة جانب معين وتحكمه في مراقبة معلومات الأنترنت؛ بحيث يعد إشراك الدول في الإدارة والإشراف بمثابة ضمانة لحماية الموارد المعلوماتية الحيوية لكل دولة، لكن تبقى التوصيات والقرارات الصادرة بهذا الشأن غير معبرة ولا مترجمة لأهمية تلك الموضوعات والمسائل؛ فهي في معظمها مجرد أفكار عامة أقرب للمبادئ الأخلاقية و الفلسفية منها لقواعد دولية ملزمة وقابلة للتطبيق؛ وعليه يمكن القول أن هذه الجهود عبارة عن عرض أفكار وليس تقديم حلول ورسم سياسات قابلة للتجسيد.

الفـــرع الثانـــي: جهـود مكافحـة التجـسس الإلكترونـي في إطـار الوكـالات المتخصصـة لهيئـة الأمـم المتحـدة.

تلعب الوكالات المتخصصة التابعة لهيئة الأمم المتحدة دوراً ملحوظاً في مجال مكافحة الجريمة الإلكترونية بصفة عامة، والعمل على تعزيز الأمن المعلوماتي من جانب آخر، وفي هذا الصدد نقف على جهود جهازين هما: الإتحاد الدولي للاتصالات والوكالة الدولية للطاقة الذرية.

أولاً- الإتحـاد الدولـي للاتصـــالات[2]:

في ختام أشغال القمة العالمية لمجتمع المعلومات تم تعيين الإتحاد الدولي للاتصالات كمنسق لتطبيق التوجهات الكبرى المتعلقة ببناء الثقة والأمن في استخدام تكنولوجيا الاتصال والمعلومات؛ وانطلاقاً من ذلك قام الإتحاد الدولي بدعم التعاون ما بين الشركات الخاصة والقطاع العام من أجل تنسيق الجهود

[1]- عادل عبد الصادق محمد الجخة، مرجع سابق، ص. 248.

[2]- الإتحاد الدولي للاتصالات وكالة متخصصة تابعة لهيئة الأمم المتحدة مقره جنيف تأسس بداية كإتحاد دولي للتيليغراف في 1865، ويضم حالياً 191 دولة عضو وأكثر من 700 قطاع وجمعية: Marco Gercke, op. cit, p. 125 .

والعمل على تبني إستراتيجية عالمية للأمن الإلكتروني وإنشاء بوابة إلكترونية للأمن الإلكتروني؛ وأصبح الإتحاد الدولي للاتصالات بمثابة ملتقى دولي رئيسي لهذه الأنشطة، وفي هذا الإطار أعلنت الأمانة العامة للإتحاد عن إطلاق البرنامج الدولي للأمن المعلوماتي الذي يتضمن سبعة أهداف إستراتيجية، هي:

– وضع إستراتيجيات من أجل إستحداث تشريع نموذجي في مجال الإجرام المعلوماتي يكون قابلاً للتطبيق على المستوى الدولي ويتماشى مع النصوص السارية المفعول على المستوى الوطني والإقليمي.

– وضع إستراتيجيات من أجل خلق بُنى تنظيمية وسياسات مناسبة على المستوى الوطني والإقليمي في مجال الإجرام الإلكتروني.

– وضع إستراتيجية لصياغة معايير أمنية دنيا وخطط إعتماد للأجهزة والبرمجيات والأنظمة تكون مقبولة عالمياً.

– وضع إستراتيجيات لإيجاد إطار عالمي للرصد والإنذار والاستجابة للحوادث لضمان التنسيق عبر الحدود بين المبادرات الجديدة والقائمة.

– وضع استراتيجيات عالمية لإنشاء وإقرار نظام هوية رقمية عام وعالمي والهياكل التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية عبر الحدود الجغرافية.

– وضع إستراتيجية عالمية تهدف لتقوية القدرات البشرية والمؤسساتية من أجل تعزيز المعارف على كل المستويات وفي كل الميادين المذكورة أعلاه.

– عرض إقتراحات بشأن إطار لإستراتيجية دولية متعددة الأطراف لتحقيق التعاون والحوار والتنسيق على المستوى العالمي في كل الميادين والمجالات المذكورة أعلاه[1].

بالإضافة إلى ذلك فقد استحدث الإتحاد الدولي للاتصالات دليلاً إلكترونياً لتتبع المعايير الأمنية الخاصة بتكنولوجيات المعلومات والاتصالات لمكافحة الجريمة عبر الأنترنت، ووصف هذا الدليل بأنه خريطة الطريق فيما يتعلق بمعايير الأمن الخاصة بتكنولوجيات المعلومات والاتصالات؛ حيث يستطيع أن يلاحق المعلومات عن أحدث المعايير الأمنية المتجددة باستمرار، ثم يصبها في قاعدة بيانات تفتح أمام

[1]- Marco Gercke, op. cit, p. 110.

المعنيين؛ ما يسهل مهمة البحث عن المعلومات المطلوبة. وقد تم وضع الدليل بالتعاون المشترك بين الإتحاد الدولي للاتصالات والوكالة الأوروبية المختصة بأمن الشبكات والمعلومات وأطراف دولية أخرى مهتمة بشؤون الأمن المعلوماتي على شبكة الأنترنت. ويعرض الدليل أسماء المنظمات المعنية بتطوير المعايير وما تنشره من صيغ خاصة بأمن الأنترنت؛ ما يجنب تكرار الجهود كما يسهل مهمة مهندسي أمن الشبكات الإلكترونية في كشف الثغرات التي تمكن العابثين من استغلالها[1].

ثانيـاً- الوكالـة الدوليـة للطاقـة الذريـة[2]:

للوكالة الدولية للطاقة الذرية جهود ملحوظة في مجال مكافحة التجسس الإلكتروني وبصورة واضحة وصريحة، إلا أن هذه الحماية تستهدف نوعاً معيناً من الأسرار، هي الأسرار النووية لمختلف الدول والتي ترد إليها من خلال تطبيق ما يعرف بنظم الضمانات النووية.

بحيث تنص الفقرة (باء) من المادة الثالثة من الدستور الأساسي للوكالة الدولية للطاقة الذرية على أنها تعمل وفقا لمقاصد الأمم المتحدة ومبادئها التي ترمي إلى تقرير السلم والتعاون الدولي؛ وانطلاقاً من هذا المبدأ تعمل الوكالة على مراقبة أغراض استخدامات الطاقة النووية والعمل على ضمان أن تنحصر في الغايات السلمية وذلك من خلال تطبيق ما يسمى بنظم الضمانات النووية، هذه الأخيرة عبارة عن مجموعة من القواعد القانونية والفنية التي فرضتها الوكالة على الدول الأعضاء فيها بموجب معاهدة منع إنتشار الأسلحة النووية والتي تهدف إلى ضمان أن المواد النووية والتجهيزات والمعدات والمشروعات والخدمات في مجال الطاقة النووية؛ تستخدم في المجال السلمي ولن يتم تحويلها إلى أسلحة نووية أو أجهزة تفجير نووية أو أي غرض عسكري آخر[3]. وتعد نظم محاسبة ومراجعة المواد النووية وكذلك نظم التحقيق والتفتيش الذي تجريه الوكالة على المنشآت النووية للدول الأعضاء من الأساسيات التي يقوم عليها نظام الضمانات، والذي تدعم أيضاً بإبرام الوكالة لاتفاقية للحماية المادية للمواد النووية في مارس من سنة 1980، ووفقا لأحكام اتفاقية الضمانات الشاملة والتي يشار إليها بالوثيقة INFCIRC /153

---

[1]- عبد الصبور عبد القوي علي، الجريمة الإلكترونية والجهود الدولية للحد منها، مجلة الدراسات المالية والمصرفية، العدد الأول، المجلد الثالث والعشرون، الأكاديمية العربية للعلوم المالية والمصرفية، الأردن، مارس 2015، ص. 15.

[2]- الوكالة الدولية للطاقة الذرية منظمة دولية تابعة للأمم المتحدة تأسست في 23 أكتوبر من سنة 1956 وبدء نفاذ دستورها في 29 يوليو من سنة 1975، وهي الجهاز الأساسي المختص والمركز العالمي لتحقيق التعاون بين الدول في مجال الاستخدامات السلمية للطاقة النووية والعمل على منع استخدامها في الأغراض العسكرية.

[3]- عماد الدين محمد كامل الجمل، مرجع سابق، ص. 146.

لسنة 1971؛ فالدولة الطرف ملزمة بتزويد الوكالة الدولية للطاقة الذرية بمعلومات وصفية عن المرافق النووية سواء الموجودة منها فعلياً أو المقرر تدشينه[1]، كما أنه وبناء على تنفيذ أحكام اتفاقية الحماية المادية للمواد النووية المشار إليها أعلاه؛ تدفق إلى الوكالة كم هائل من المعلومات عن الحماية المادية للمنشآت النووية والمواد النووية لدى الدول الأعضاء في الاتفاقية، إلا أن ذلك كان مشروطاً دائماً وحسبما ورد في الاتفاقية بدعوة الدول الأطراف فيها باتخاذ الخطوات الملائمة والمتفقة مع قوانينها الوطنية لحماية سرية أي معلومات مقدمة سواء إلى الهيئات الدولية أو إلى أية دولة طرف في الاتفاقية، تكون قد سلمتها بطريقة سرية من دولة طرف أخرى أو تلقتها تلك الدولة عن طريق المشاركة في أي نشاط لتنفيذ هذه المعاهدة، وأنه لن يطلب من تلك الدول الأطراف في الاتفاقية تقديم أي معلومات لا يسمح لها بإفشائها طبقاً لقوانينها الوطنية أو التي تخل بأمن تلك الدول أو الحماية المادية للمواد النووية[2]، وقد أدى قيام الدول بتطبيق الالتزامات المفروضة عليها إلى تدفق الكثير من المعلومات النووية على الوكالة الدولية للطاقة الذرية؛ الأمر الذي دفعها إلى إنشاء نظام يعتمد على تخزين هذه المعلومات في حاسبات ذات سعة كبيرة ومجهزة لمعالجة هذه المعلومات للمقارنة واكتشاف الغير عادي بها؛ وقد أُنشئ قسم ضمن أقسام الضمانات بالوكالة خصيصاً لهذا الغرض يقوم المختصون فيه بتلقي المعلومات ومعالجتها بالوكالة، على أن تلك المعلومات المخزنة في الحاسبات الإلكترونية قد فُرض عليها سياج منيع من الحماية المادية والإلكترونية والقانونية؛ بحيث يقتصر العلم بها على الأشخاص المختصين دون غيرهم وكل في مجاله وتخصصه ودون أن يتخطى علمه بالمعلومات إلى غيره من التخصصات والأقسام، كما قامت الوكالة بالتعاقد مع إحدى الشركات العالمية لإجراء تقييم لأمن المعلومات النووية ووضع إجراءات أمن معلوماتي جديدة تتضمن استخدام كلمات سر أكثر مناعة وإعادة تصميم الحلقة الأمنية للحد من الوصول إلى بيانات قسم الضمانات وتشفير شرائط النظم الاحتياطية، كما تم تحديث تصاريح الوصول إلى قواعد البيانات الرقابية السرية عند نقل الموظفين إلى مواقع أخرى أو انتهاء عملهم، ووضع سياسة لحماية الحاسبات من الفيروسات، ووضع خطط أمنية لمنع الوصول للمعلومات عن بعد، وتأمين الاتصالات الخاصة ببيانات المفتشين، واستخدام سياسة محددة للتحقق من هوية المستخدمين، فضلا عن وضع نظام للتحقق والكشف عن التداول غير السليم للمعلومات الرقابية السرية وأمن كلمات السر، وفحص وتوثيق

[1]– المادة الثامنة من اتفاقية الضمانات الشاملة والتي يشار إليها بالوثيقة INFCIRC /153 لسنة 1971.

[2]– المادة السادسة من اتفاقية الحماية المادية للمواد النووية لسنة 1971.

الحاسبات المحمولة ومحطات العمل الموجودة في الشبكة، وإعداد وتنفيذ برامج للتدريب والوعي في مجال الأمن وإنشاء برنامج تدريب دوري إجباري لجميع أفراد إدارة الضمانات.

لم تقصر الوكالة الدولية للطاقة الذرية حمايتها لأسرار الدفاع النووية الخاصة بالدول الأعضاء على تلك الأسرار المخزنة في الحاسبات لديها، بل امتدت حمايتها إلى تلك الأسرار وهي في نطاق وداخل دولها؛ بأن فرضت مجموعة من الالتزامات على الموظفين لديها وخاصة المفتشين الدوليين، قوامها الحفاظ على تلك الأسرار وعدم إفشائها إذا تعلق علمهم بها أثناء عملهم لحساب الوكالة في الدول الأعضاء؛ فهناك التزام عام يقع على عاتق الوكالة وموظفيها ورد في المادة السابعة من دستور الوكالة بعدم إفشاء أي سر صناعي أو أية معلومات أخرى سرية يطلعون عليها بمقتضى عملهم الرسمي في الوكالة[1].

الفـــرع الثالــث: الأمـن المعلوماتـي كمحور إلتقاء توصيات المنظمات الدولية لمكافحة التجسس الإلكتروني.

المتتبع لكل الجهود المبذولة من طرف هيئة الأمم المتحدة أو وكالاتها المتخصصة لمكافحة كل أشكال الجريمة الإلكترونية دون استثناء، ومنها التجسس الإلكتروني؛ يجد أنها تدور حول محور واحد وهو الأمن المعلوماتي، واهتمام هذه المنظمات بمسألة الأمن المعلوماتي؛ نابع من كونه أكثر الإجراءات فعالية في التصدي لمخاطر الإجرام الإلكتروني وإن كانت نتائجه غير مطلقة وكذلك لكونه أكثر الإجراءات التي يمكن أن تحقق الإجماع الدولي، وكذا نظراً للطبيعة التقنية والعملية لأساليبه؛ فهي لا تحتاج لمناقشات أو اجتماعات طويلة لمناقشة الأخذ أو عدم الأخذ بها بعكس ما يلاحظ بشأن إتخاذ قرار بشأن مسألة قانونية معينة؛ ما يجعل من الأمن المعلوماتي أفضل الحلول المتوافرة حالياً لمواجهة التجسس الإلكتروني لذا تستوجب دراسته بشيء من التفصيل.

يُعبر مصطلح الأمن المعلوماتي عن سياسة تقليص مساحة تهديدات الإجرام المعلوماتي المرتبط باستخدام التكنولوجيات الحديثة[2]، وعن الحالة المبحوث عنها لأجل نظام معلوماتي يسمح بمقاومة الحوادث النابعة من الفضاء الإلكتروني القادرة على أن تعرض للخطر توافرية أو تكاملية أو سرية

[1]– عماد الدين محمد كامل الجمل، مرجع سابق، ص. ص. 222– 226.

[2]-Anne SOUVIRA, la cybersecurité des enterprises, revue LAMY droit des affaires (RRDA), numéro 87, Walters Kluwer, France, November 2013, p. 95.

المعطيات المخزنة أو المعالجة أو المنقولة وكذا الخدمات المرتبطة التي تمنحها هذه الأنظمة أو التي تجعلها متاحة[1]، ويقوم على مجموعة الإجراءات والقواعد والتشريعات التي توضع للحفاظ على سلامة وتكامل نظام المعلومات من التخريب والعبث والفقدان وكذلك من التغيير والاستعمال غير المسموح به، سواء كان هذا التغيير أو التخريب مقصوداً أم غير مقصود[2]، وستتم الإحاطة بمفهوم الأمن المعلوماتي من خلال عنصرين: يتناول العنصر الأول أهداف الأمن المعلوماتي، والعنصر الثاني إجراءات الأمن المعلوماتي.

أولاً- أهـــداف الأمـــن المعلوماتـــي:

لابد بدايةً من الإشارة إلى أن تحقيق الأمن بصورة شاملة وأكيدة ومضمونة ليس موجوداً؛ فلكل نظام نقاط ضعف خاصة به جعلت البعض يعتبرون أن قوة أي نظام إنما تقاس بقوة أضعف نقطة فيه، وبالمقابل لابد من المقارنة بين كلفة الأمن وقيمة الحماية بمعنى قيمة ما يراد حمايته؛ فمما لاشك فيه أن اهتمامات الأمن تختلف باختلاف المواد والموارد المعرضة للتهديد[3]، فتأتي حماية المواد والموارد الحساسة ذات الطبيعة السرية المرتبطة بالدفاع الوطني في صدارة تلك الاهتمامات مع ملاحظة التغيير الذي عرفه سلم ترتيب الأسرار المستهدفة؛ إذ أصبحت مصالح الاستعلامات تكرس نسبة كبيرة من أنشطتها للبحث عن المعلومة العلمية والاقتصادية والتكنولوجية[4]، وما يحدد قيمة هذه المعلومة وغيرها هي ثلاثية السرية والتكاملية والتوافرية؛ لذا تهدف كل سياسات الأمن المعلوماتي إلى حماية هذه الثلاثية.

وتُشير السرية إلى أن المعلومة غير قابلة للكشف وللإظهار لمستخدمين غير مرخص لهم بمعرفتها، وهذا يعني بأن النظام يجب أن يمنع المستخدمين من قراءة معلومة سرية إذا كانوا غير مرخصين ومنع المستخدمين المرخص لهم بقراءة المعلومة من إذاعتها وإفشاءها لغيرهم من المستخدمين الغير مرخص لهم. أما التكاملية فتشير إلى عدم قابلية المعلومة للإتلاف، وهذا يعني بأن النظام

[1]- Myriam QUEMENER, la coopération entre des organes de lutte contre la cybercréminalité, revue LAMY driot des affaires (RRDA), numéro 87, Walters Kluwer, France, novembre 2013, p.101.

[2]- عبد الرحمن شعبان عطيات، مرجع سابق، ص. 122.

[3]- منى الأشقر جبور وعزيز ملحم بربر، مرجع سابق.

[4]- Robert Longeon et jean luc Archimbaud, Guide de la sécurité des systems d'information, centre national de la recherche scientifique, France, 1999, p. 31, ouvrage le site: http//www.cnrs.fr/infosecu, le site a été visité le:04/02/2015.

المعلوماتي يجب أن يمنع تعديلها من طرف المستخدمين غير المرخص لهم بذلك أو تعديلها غير الصحيح من طرف مستخدمين مرخص لهم بذلك، ومصطلح التعديل هنا يجب أخذه بمعناه الواسع والذي يتضمن خلق معلومة جديدة أو تحيين معلومة أو إتلاف معلومة موجودة مسبقا. أما التوافرية فتشير إلى سهولة الوصول إلى المعلومة عندما يحتاج إليها المستخدم وهذا يعني أن النظام المعلوماتي يجب أن يمنح الدخول إلى المعلومة من أجل أن يتمكن المستخدم المرخص له من قراءتها أو تعديلها[1].

وبالرجوع إلى بعض التعريفات الممنوحة للأمن المعلوماتي نجد من بينها ما يُعرفه بدلالة أهدافه، ويجمع من خلاله مجموعة الأهداف المذكورة أعلاه، ومنها تعريف توصيات أمن المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة لأمن أنظمة المعلومات بأنه: حماية أنظمة المعلومات ضد أي وصول غير مرخص إلى أو تعديل المعلومات أثناء حفظها، معالجتها أو نقلها؛ وضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، بما في ذلك جميع الإجراءات الضرورية لكشف، توثيق، ومواجهة هذه التهديدات[2].

ثانيـــاً- إجـــراءات الأمـــن المعلوماتـــي:

يمكن تقسيم إجراءات الأمن إلى ثلاثة أقسام رئيسية: بحيث يتمحور القسم الأول حول إجراءات الأمن البشري، والقسم الثاني حول إجراءات الأمن المادي، والقسم الثالث حول إجراءات الأمن المعنوي.

أ- إجـــراءات الأمـــن البشـــري:

وهي إجراءات موضوعها جميع الأفراد العاملين في المركز من المدير والإدارة والمهندسين ومحللي النظم والمبرمجين والمشغلين والسكرتارية وعمال الصيانة وعمال النظافة، وتشمل تلك الإجراءات أمن العاملين والأمن منهم؛ إذ أن أهم مصدر لتهديد مركز المعلومات هو من العاملين فيه[3]، فخطر التصرف المتعمد والسيئ النية من قبل أولئك الذين يعملون خاصة في المؤسسات الاقتصادية خطر واقعي؛ حيث قد يُسهل مستخدم ما سرقة المراسلات أو تسريب المعطيات المعلوماتية المالية أو الشخصية

[1]- Fernand lone sang, op. cit, p. 10.

[2]- سليمة سعيدي وبلال حجاز، جرائم المعلوماتي والشبكات في العصر الرقمي، دار الفكر الجامعي،مصر،2017، ص. 114.

[3]- عبد الرحمن شعبان عطيات، مرجع سابق، ص. 125.

أو المتعلقة بأسرار التصنيع[1]؛ لذا فإن الاهتمام بالمستخدمين مطلب جوهري في أي سياسة أمن معلوماتي لهذا يجب أن يركز في تدريب العاملين في مركز المعلومات على حثهم بأنه يجب أن تكون مهمتهم الحفاظ على أمن الحواسيب من الطامعين بسرقة أسرارها أو العبث بما تحتويه من برمجيات، ولا يُكتفى فقط بتحسيس المستخدمين بل يتعدى الأمر إلى إتباع مجموعة من القواعد الخاصة لضمان تأمين المعلومات من المستخدمين ذاتهم لأن الشخص مهما كان موثوقاً به سيكون عرضة لكثير من الإغراءات، ومثالها جعل رمز سري لكل شخص عامل يمكنه من الدخول على الجزء الذي يهمه فقط من النظام المعلوماتي دون أن يتمكن من الاطلاع على ملفات غيره الذين يملكون بدورهم مفاتيح أخرى خاصة بهم، وكذلك تصميم النظم بحيث لا يمكن التغيير في المعلومات والبيانات إلا من قبل لجنة خاصة لهذا الغرض يملك كل عضو فيها جزءاً من كلمات المفتاح لا يعرفه غيره؛ وبالتالي يفتح النظام فقط بحضورهم جميعاً، بالإضافة إلى تكليف عدد من العاملين وعدم الاكتفاء بتكليف منتسب واحد فقط للقيام بالواجبات المهمة؛ وذلك لمنع الاستغلال والتفرد، ومنها ربط أجهزة الحاسوب ووضع خطة الطوارئ وإلغاؤها وتصميم وبرمجة النظام الأمني ومعالجة المعلومات السرية وفحص الأجهزة والبرمجيات بعد التعاقد على شرائها[2].

ب- إجـراءات الأمــن المــادي (الفيزيقــي):

وهي إجراءات موضوعها تأمين المبنى وغرفة الحاسب والحاسب نفسه وهدفها المنع من الوصول إلى مكان التواجد المادي للنظام المعلوماتي، وتبدأ من اختيار موقع المبنى وإحاطته بإجراءات لمنع اختراقه، مثل بناء الأسيجة، ووضع أجهزة المراقبة الإلكترونية، والحراسة المشددة، ووضع الضوابط الملائمة للدخول لضمان اقتصار الدخول إليها على الأشخاص المصرح لهم بذلك فقط، وكذلك وضع إجراءات خاصة بالتنقل والدخول إلى الأجزاء المختلفة للمبنى في حد ذاته من طرف المستخدمين أنفسهم؛ إذ يحدد لهم المجال المكاني الذي يحق لم التواجد فيه. بالإضافة إلى إجراءات الحماية ضد التهديدات البيئية كالحرائق والفيضانات والزلازل، أي كل أنواع الكوارث سواء كانت طبيعية أو بفعل الإنسان. وكذلك المراقبة والتحكم في نقاط الدخول مثل مناطق التوريد والتحميل والنقاط الأخرى التي يحتمل دخول الأشخاص غير المصرح لهم من خلالها وإن أمكن عزلها عن مناطق تواجد مرافق معالجة المعلومات[3].

---

[1]- Anne Souvira, op. cit, p. 96.

[2]- عبد الرحمن شعبان عطيات، مرجع سابق، ص. 127.

[3]- عمر بن محمد العتيبي، مرجع سابق، ص. 91.

بالإضافة إلى إتباع إجراءات بخصوص مرافقة ومراقبة الأشخاص من غير المستخدمين الحاصلين على إذن بدخول المبنى، ومثاله حالة تأمين مخابر الأبحاث العلمية الوطنية؛ بحيث تشكل اتفاقيات التعاون الدولي وإرسال المتربصين إلى هذه المواقع فرصة للحصول على المعلومة العلمية، الأمر الذي يفرض ابتداءً البقاء في حالة يقظة؛ لأن العلاقة بين مشروع البحث وجنسية الشريك تمثل حساسية خاصة وهو السبب الذي لأجله يتم إجراء رقابة مسبقة على طلبات التربص الخاصة بالباحثين وحول مشاريع الشراكة الدولية[1]، وتمتد الرقابة إلى التواجد داخل هذه المختبرات وإلى غاية مغادرتها. كما تشمل هذه الإجراءات المادية الحواسيب وملحقاتها انطلاقاً من تحديد مواقعها داخل المبنى وحتى داخل الغرف في حد ذاتها وحماية تمديدات الكوابل الخاصة بالكهرباء والاتصالات المستخدمة في نقل المعلومات[2]، وإتخاذ الإجراءات اللازمة لمنع رصد والتقاط الإشعاع الكهرومغناطيسي المنبعث من الحواسيب أثناء عملها[3]. وكذلك منع نقل الأجهزة خارج موقعها دون إذن مسبق، وضرورة القيام بصيانة ومراقبة دورية للأجهزة وتأمين عملية التخلص منها، بحيث يستوجب التأكد من إزالة أية بيانات حساسة أو طمسها قبل ذلك[4]؛ باعتبار توفر برمجيات تمكن من استرجاع البيانات من وسائط التخزين بعد مسحها.

ج- إجـراءات الأمــن المعنــوي:

وهي إجراءات موضوعها المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات أو التي يتم نقلها من نظام إلى آخر عبر شبكات الربط والاتصالات، وتهدف هذه الإجراءات إلى منع غير المرخص لهم من الوصول إليها. ويأتي في مقدمة هذه الإجراءات: التشفير أو ما يعرف أيضاً بالتعمية، التي تقوم على خلط المعلومات الإلكترونية بحيث لا يمكن إعادة ترتيبها إلا باستخدام مفتاح معين بحيث تكون هذه المعلومات المخلوطة غير مفهومة بتاتاً للشخص الذي لا يملك المفتاح[5]. وهناك العديد من أنــواع التشفير

[1]- Robert Longeon et gean luc Archimbaud, op. cit, p. 32.

[2]- عمر بن محمد العتيبي، مرجع سابق، ص. 91.

[3]- عبد الرحمن شعبان عطيات، مرجع سابق، ص. 137.

[4]- عمر بن محمد العتيبي، مرجع سابق، ص. 92.

[5]- عبد الرحمن شعبان عطيات، مرجع سابق، ص. 130.

كالتشفير المتناظر أو المتماثل، والتشفير غير المتناظر أو بمفتاح عام، والتشفير الهجين[1]. ورغم اعتبار التشفير أحسن الحلول لحفظ المعطيات السرية إلا أن عيبه الوحيد كونه تقنية عامة لا يقتصر استخدامه على الدولة فقط، بل يستغله أيضا المجرمون لإخفاء محتوى اتصالاتهم؛ فيصبح بذلك أفضل وسيلة للأمن المعلوماتي سواء للدولة أو للمجرمين[2]. أما التقنية الثانية المستخدمة بغرض توفير الأمن المعنوي وتحديداً للشبكات فهي تقنية الجدران النارية، وهي عبارة عن مجموعة من البرمجيات والأجهزة التي يتم إعدادها لتحتل الحدود بين الشبكة المراد حمايتها والشبكة التي يراد الحماية منها، والهدف من هذه الجدران هو التغلب على أكبر قدر ممكن من الثغرات الأمنية من خلال بناء قناة اتصال توجه إليها المراسلات والمعلومات المتبادلة مع الشبكات لمراقبتها والسيطرة على خروجها أو دخولها من وإلى الشبكة المراد حمايتها، وبشكل عام فإن الجدران النارية هي عبارة عن برامج تقوم بصد محاولات الاختراق أو الهجوم الوافد من الشبكات وخاصة الأنترنت[3]. وإضافة إلى هاتين التقنيتين هناك الكثير غيرها التي لا يمكن حصرها جميعاً لتطورها المستمر، لكن في المقابل يمكن حصر مستويات أو أنواع الأمن داخل النظام في ثلاثة نقاط هي:

---

[1]– يقوم التشفير المتناظر أو المتماثل أو بمفتاح سري (la cryptographie symétrique) على وجود مفتاح واحد هو الذي يشفر نصاً ويفك تشفيره. أما التشفير غير المتناظر (la cryptographie asymétrique) فيقوم على استخدام مفتاحين الأول سري والثاني عمومي؛ فلإرسال رسالة لمالك المفتاح السري يكفي تشفير الرسالة بالمفتاح العمومي المناسب ووحده مالك المفتاح السري يمكنه فك شفرة الرسالة. أما التشفير الهجين (la cryptographie hybride) فيقوم على مزج نوعي التشفير السابقين؛ بحيث يتم تشفير الرسالة بواسطة طريقة التناظر بمساعدة مفتاح سري وبعد هذا يتم تشفير المفتاح ذاته بطريقة التشفير غير المتناظر وبعد إرسالها يقوم متلقيها بفك شفرة المفتاح ثم يقوم باستخدام هذا المفتاح لفك شفرة الرسالة، والاتصالات التي تتم عن طريق الأنترنت يتم تأمينها بواسطة بروتوكولات تستخدم التشفير الهجين، أنظر:

- Abderrahmane Nitaj, op. cit, p. p. 2 – 3.

[2]– إن تشفير المعطيات المعلوماتية من طرف الجناة يُعقد عمل مصالح المكافحة والتي يجب عليها لأجل الدخول إلى تلك المعطيات أن تفك التشفير ابتداءً، وهي عملية عادة ما تتسم بالصعوبة والبطء؛ فالوقت الضروري لكسر شيفرة يعتمد على تقنية التشفير المستخدمة وكذا على طول المفتاح، فاستخدام برنامج تشفير بطول مفتاح يبلغ 20 بايت يستطيع حاسوب حديث يجري مليون عملية في الثانية أن يكسر الشفرة في أقل من ثانية، وبتشفير بطول مفتاح بـ 40 بايت يصبح الوقت اللازم لذلك حولي أسبوعين، ومن أجل مفتاح بطول 56 يتطلب الأمر 2285 عاماً، ومن أجل 128 بايت وبواسطة مليار حاسوب مخصصة لهذه العملية يستلزم الأمر ملايير السنين، غير أن طبعة برنامج التشفير الشهير (PGP) تسمح بالتشفير المعطيات بواسطة مفتاح بطول 1024 بايت، أنظر:

- Marco Gercke, op. cit, p. 91.

[3]– جعفر حسن جاسم الطائي، مرجع سابق، ص. 246.

1- أمن الدخول: ويهتم بحماية مدخل النظم.

2- أمن نظام الملف: ويتضمن التحكم في الوصول إلى ملفات النظام.

3- أمن الحاسب الخادم: ويتضمن التحكم في حماية الحاسوب الموزع[1].

المطلب الثاني: جهود مكافحة التجسس الإلكتروني في إطار الاتفاقيات الدولية.

المتفحص للقانون الدولي لا يعثر على أية اتفاقية دولية وضعت تحديداً لتنظيم أحكام التجسس بصورة عامة، ولا التجسس الإلكتروني بصفة خاصة، إلا أن هناك بعض الاتفاقيات التي حَوَت في نصوصها أحكاماً تتعلق مباشرةً بالتجسس الممارس في زمن الحرب، كما هو الحال بالنسبة لاتفاقيات القانون الدولي الإنساني، وهناك اتفاقيات أخرى تنظم مجالات لها صلة معروفة بالتجسس، كتلك المنظمة للعمل الدبلوماسي أو تلك المنظمة للنشاطات في الفضاء الخارجي أو تلك المنظمة لاستخدام الطاقة النووية؛ وعليه سيقسم هذا المطلب إلى أربعة فروع: يتناول الفرع الأول جهود مكافحة التجسس الإلكتروني في إطار اتفاقيات القانون الدولي الإنساني، ويتناول الفرع الثاني جهود مكافحة التجسس الإلكتروني في إطار اتفاقيات القانون الدولي للفضاء الخارجي، ويتناول الفرع الثالث جهود مكافحة التجسس الإلكتروني في إطار الاتفاقيات المنظمة لاستخدام الطاقة النووية، بينما يتناول الفرع الرابع جهود مكافحة التجسس الإلكتروني في إطار اتفاقية فيينا للعلاقات الدبلوماسية.

الفرع الأول: جهود مكافحة التجسس الإلكتروني في إطار اتفاقيات القانون الدولي الإنساني.

لا تهتم اتفاقيات القانون الدولي بصفة عامة بالتجسس الممارس في زمن السلم؛ فذلك من اختصاص التشريعات الوطنية فلكل دولة حق سن القواعد التي تراها كفيلة بحفظ أمنها انطلاقاً من تمتعها بالسيادة الكاملة على إقليمها، أما التجسس الواقع في زمن الحرب فإنه يدخل ضمن نطاق اهتمامات القانون الدولي الإنساني تحديداً، ولعل أبرز اتفاقياته في هذا الخصوص اتفاقية لاهاي لسنة 1907، واتفاقيتي جنيف الثالثة والرابعة، والبروتوكول الأول الإضافي لاتفاقيات جنيف لسنة 1977، والتي اهتمت بتحديد وضع الجاسوس والأحكام التي يخضع لها في حالة القبض عليه، وللإحاطة بهذه الأحكام سيتم بدايةً عرض تعريف التجسس في إطار اتفاقيات القانون الدولي الإنساني، ثم شروط التجسس في إطار

[1]- سليمة سعيدي وبلال حجاز، مرجع سابق، ص. 124.

اتفاقيات القانون الدولي الإنساني، ثم معاملة الجاسوس في إطار اتفاقيات القانون الدولي الإنساني، ومن ثم يتم تناول تقييم لاتفاقيات القانون الدولي الإنساني وإسقاط أحكامها على التجسس الإلكتروني.

أولاً- تعريف التجسس في إطار اتفاقيات القانون الدولي الإنساني:

تضمنت النصوص القانونية المتعلقة بالتجسس تعريف فاعله أي تعريف الجاسوس؛ بحيث نصت اتفاقية لاهاي المتعلقة بقوانين وأعراف الحرب على الأرض على أنه: "لا يمكن أن يعتبر كجاسوس إلا الفرد الذي يعمل في الخفاء أو تحت ستار كاذب لجمع المعلومات أو محاولة جمع المعلومات في منطقة العمليات الحربية لإحدى الدول المتحاربة بنية إيصالها للطرف المعادي"[1]، وهو ذات المفهوم الذي عرفه القانون الدولي العرفي[2]، كما نصت الفقرة الثانية من ذات المادة على أنه: "لا يعتبر جاسوساً العسكريون الغير متنكرين الذين يتوغلون في منطقة العمليات للجيش المعادي لأجل جمع المعلومات وكذلك لا يعتبر كجواسيس العسكريون وغير العسكريين الذين يقومون بشكل علني بمهامهم المتعلقة بنقل البريد سواء إلى جيشهم الخاص أو للجيش المعادي وكذلك ينتمي إلى هذه الفئة من يشتغل كواسطة اتصال بين وحدات الجيش أو بين أجزاء الأقاليم المختلفة".

كما نص البروتوكول الأول إلى اتفاقيات جنيف المتعلق بحماية ضحايا المنازعات الدولية المسلحة على أنه: "لا يعد مقارفاً للتجسس فرد القوات المسلحة لطرف في النزاع الذي يقوم بجمع أو يحاول جمع معلومات لصالح ذلك الطرف في إقليم يسيطر عليه الخصم إذا إرتدى زي قواته المسلحة أثناء أدائه لهذا العمل، كما لا يعد مقارفاً للتجسس فرد القوات المسلحة لطرف في النزاع الذي يقيم في

[1]- المادة 29 من اتفاقية لاهاي المتعلقة بقوانين وأعراف الحرب على الأرض الموقعة في 18 أكتوبر من سنة 1907 والتي دخلت حيز التطبيق في 26 جوان 1910.

[2]- تم تعريف الجواسيس في القانون الدولي العرفي أي قبل تقنينه في اتفاقيات دولية، لكن الملاحظ التعريف لم يشهد تغييراً بل بقي ذاته، فمثلاً عُرِف التجسس في إعلان بروكسيل لسنة 1874 بشأن أحكام القانون العسكري بأنه: القيام بجمع أو محاولة جمع معلومات في إقليم تحت سيطرة طرف معادي بالتصرف بشكل خفي أو تحت ذرائع كاذبة:

-Jean –Marie Henckaerts et Louise Doswald– Beck, Droit international humanitaire coutumier, volume 1: Régles, Bruylant, Belgique, 2006, p. 516.

إقليم يحتله الخصم والذي يقوم لصالح الخصم الذي يتبعه بجمع أو محاولة جمع معلومات ذات قيمة عسكرية داخل ذلك الإقليم ما لم يرتكب ذلك عن طريق عمل من أعمال الزيف أو تعمد التخفي"[1].

من استقراء المادتين أعلاه؛ يمكن القول أن التجسس هو الفعل الذي يقوم به فرد سواء كان عسكريا أم لا ويهدف إلى جمع أو محاولة جمع المعلومات داخل إقليم الخصم وذلك خفية أو تحت ستار كاذب.

ثانياً- شروط التجسس في إطار اتفاقيات القانون الدولي الإنساني:

بالاستناد إلى المادتين 29 من اتفاقية لاهاي و46 من البروتوكول الإضافي الأول لاتفاقيات جنيف؛ نستنتج أنه لكي نكون أمام واقعة تجسس لابد من توافر مجموعة من الشروط يمكن إجمالها في العناصر الآتية:

أ- **جمع المعلومات:** بحيث تشترط المادتين أن يمارس شخص ما نشاطاً من شأنه الحصول على معلومات معينة أو يحاول ذلك بنية نقلها للطرف المعادي الذي يتبعه، ومعنى ذلك أنه إذا ثبت أن النشاط الذي قام لا يتعلق بجمع معلومات أو محاولة ذلك فإنه لا يعتبر جاسوساً، كمن يقوم بأعمال تخريبية أو إنتحارية ضد القوات المعادية، كما لا يعد جاسوساً ذلك الذي يقوم بعملية نقل المعلومات من مكان إلى آخر إذا لم يكن هو الذي قام بتجميعها[2].

ب- **أن يكون الفاعل متنكراً:** بحيث اشترط البروتوكول الإضافي الأول لاتفاقيات جنيف لكي يتابع الجاني بتهمة التجسس أن يكون عسكرياً متنكراً، أي أن لا يكون مرتدياً لزي قواته المسلحة أثناء قيامه بجمع أو محاولة جمع المعلومات، فإذا قام الفاعل بذلك وهو مرتد لزيه العسكري فلا يعد مقترفاً لفعل التجسس[3]، بل يعامل على أساس أنه أسير حرب؛ وهذا يعني أن المشرع الدولي إعتد بمعيار المظهر المادي كقرينة على وجود أو انتفاء عنصر التخفي والتنكر ومنه التفرقة بين مركز الجاسوس ومركز أسير الحرب.

---

[1]- المادة 46 من البروتوكول الأول الإضافي إلى اتفاقيات جنيف المعقودة في 12 أوت من سنة 1949 والمتعلق بحماية ضحايا المنازعات الدولية المسلحة لسنة 1977.

[2]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. 357.

[3]- الفقرة الثانية من المادة 46 من البروتوكول الأول الإضافي لاتفاقيات جنيف.

ج- أن يقع جمع أو محاولة جمع المعلومات في إقليم يسيطر عليه طرف معادي: بحيث نصت المادة 46 من البروتوكول الأول الإضافي لاتفاقيات جنيف على ضرورة أن تتم عمليات التجسس في إقليم يسيطر عليه العدو، ويلاحظ هنا توسع هذه المادة في المجال المكاني الذي يمكن اقتراف التجسس فيه مقارنة بما نصت عليه المادة 29 من اتفاقية لاهاي والتي حصرته في منطقة العمليات الحربية لإحدى الدول المتحاربة، ويمكن القول أن التجديد الذي تضمنه البروتوكول الأول الإضافي يعتبر في الواقع إجراء كاشف لقاعدة دولية عرفية عدلت تلقائياً اتفاقية لاهاي، بحيث يراد بمنطقة العمليات كل إقليم الدولة طبقاً لما استقر عليه العرف الدولي إعتباراً من بداية القرن العشرين، وتطبيقاً لذلك قضت إحدى المحاكم الأمريكية بأن مدينة نيويورك تقع ضمن منطقة عمليات الحرب العالمية الأولى رغم أن الاشتباكات كانت دائرة في قارة أخرى[1]، وبالإضافة إلى الإقليم الأصلي التابع للدولة فإن تعبير "إقليم يسيطر عليه العدو" يتسع ليشمل أي حيز مكاني تحتله الدولة ويصبح بذلك تحت سيطرتها.

د- أن يتم جمع أو محاولة جمع المعلومات لمصلحة دولة معادية: وهو الشرط المنصوص عليه صراحة في كل من المادة 29 من اتفاقية لاهاي والمادة 64 من البروتوكول الإضافي الأول لاتفاقيات جنيف.

هـ- شرط التلبس بالنسبة للجاسوس المقيم: بحيث تضمن البروتوكول الإضافي الأول لاتفاقيات جنيف النص على حالة خاصة تتعلق بفرد القوات المسلحة الذي يقيم في إقليم يحتله الخصم، والذي لا يعتبر جاسوساً إلا إذا قام بجمع أو محاولة جمع معلومات ذات قيمة عسكرية (أي الأسرار العسكرية فقط فتخرج بذلك طوائف المعلومات الأخرى من التجريم) داخل ذلك الإقليم عن طريق عمل من أعمال الزيف أو تعمد التخفي، ورغم اعتبار هذا العسكري جاسوساً، إلا أنه لا يفقد حقه في التمتع بوضع أسير الحرب ولا تجوز معاملته كجاسوس إلا إذا قبض عليه أثناء قيامه بالتجسس أي وهو متلبس بفعل جمع المعلومات العسكرية[2].

---

[1]- ولقد عللت المحكمة حكمها هذا بقولها: "أنه نتيجة التقدم الذي حدث في وسائل نقل معدات التخريب والتدمير، فإنه من المؤكد أن أراضي الولايات المتحدة الأمريكية تعتبر ضمن منطقة العمليات الايجابية للحرب، هذا بالإضافة إلى أن أعداداً كبيرة من القوات الأمريكية والمعدات العسكرية ترسل يومياً إلى جبهات القتال عن طريق ميناء نيويورك، ويكفي لاعتبار الشخص جاسوساً أن يأتي إلى الولايات المتحدة في مهمة تجسس ويرسل المعلومات التي يجمعها إلى العدو" : محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 361- 362.

[2]- الفقرة الثالثة من المادة 46 من البروتوكول الأول الإضافي لاتفاقيات جنيف.

ثالثاً- معاملة الجاسوس في إطار اتفاقيات القانون الدولي الإنساني:

سبق القول أن المعيار الذي يتم على أساسه التفريق بين الجاسوس وغير الجاسوس ليس محل الفعل رغم استهدافه لأسرار الدولة، ولكنه مظهر الفاعل، فإذا كان مرتدياً زيه العسكري عُد أسير حرب يستفيد طبقا لذلك من القواعد المقررة لمعاملة أسرى الحرب في اتفاقية لاهاي واتفاقية جنيف الثالثة بشأن معاملة أسرى الحرب[1]، أما إذا كان الفاعل متنكراً بزي غير زي قواته العسكرية أو كان مدنياً يعمل بخفاء فيعامل معاملة الجاسوس ويخضع للقواعد المقررة في كل من اتفاقية لاهاي وكذا البروتوكول الإضافي الأول لاتفاقيات جنيف وكذلك اتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب، بحيث تعد هذه القواعد بمثابة ضمانات لمعاملة الجواسيس؛ وعليه فالشخص الذي يقوم بجمع أو محاولة جمع معلومات عن العدو لا تخرج معاملته عن أحد احتمالات ثلاث هي:

- **الإحتمال الأول: أسير الحرب:** يستفيد من هذا الوضع كل من له صفة عسكرية فقط وقام بجمع المعلومات في منطقة الخصم مرتدياً زيه الرسمي، وكذلك العسكري المقيم في إقليم الخصم رغم جمعه للمعلومات وهو متنكر بشرط عدم إلقاء القبض عليه متلبساً بذلك، ويخضع الفرد هنا إلى ما جاء في اتفاقية لاهاي واتفاقية جنيف الثالثة بشأن معاملة أسرى الحرب.

- **الإحتمال الثاني: الجاسوس المحارب:** وهو كل من له صفة عسكرية وقام بجمع المعلومات في منطقة الخصم باستخدام التنكر والتخفي وكذلك العسكري المقيم في إقليم الخصم المقبوض عليه متلبساً بجمع المعلومات، ويخضع الفرد هنا إلى اتفاقية لاهاي وكذا البروتوكول الإضافي الأول لاتفاقيات جنيف.

- **الإحتمال الثالث: الجاسوس غير المحارب:** وهو كل مدني تابع لطرف يقوم بجمع المعلومات في منطقة العمليات التابعة للخصم، ويخضع الجاسوس هنا للأحكام الواردة في اتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب.

ويمكن إجمال ضمانات معاملة الجاسوس بصنفيه في العناصر التالية:

[1]- المواد من 4 إلى 20 من اتفاقية لاهاي ومواد اتفاقية جنيف الثالثة بشأن معاملة أسرى الحرب المؤرخة في 12 أوت سنة 1949.

أ- الحق في محاكمة عادلة: إذ أقرت المادة 30 من اتفاقية لاهاي عدم إمكانية معاقبة الجاسوس دون محاكمة مسبقة[1]، كما نصت اتفاقية جنيف الرابعة على مجموعة من الضمانات التي يستفيد منها مرتكب التجسس مع ملاحظة أن الأحكام المقررة في هذه الاتفاقية جاءت لصالح الأشخاص المحميين بها أي المدنيون، فأقرت ضرورة معاملة الأشخاص المتهمين بالتجسس بإنسانية، وفي حالة ملاحقتهم قضائياً لا يحرمون من حقهم في محاكمة عادلة قانونية على النحو المنصوص عليه في ذات الاتفاقية[2]، بحيث نصت هذه الأخيرة على مجموعة ضمانات كالآتي:

1- يستوجب دون إبطاء إبلاغ أي متهم تحاكمه دولة الاحتلال كتابة وبلغة يفهمها بتفاصيل الإتهامات الموجهة إليه، وينظر في الدعوى بأسرع ما يمكن، ويتم إبلاغ الدولة الحامية بأي محاكمة تجريها دولة الاحتلال لأشخاص محميين بتهم تكون عقوبتها الإعدام ويكون لها في كل الأوقات الحصول على معلومات عن سير الإجراءات[3].

2- للمتهم بالتجسس الحق في تقديم الأدلة اللازمة لدفاعه وعلى الأخص استدعاء الشهود، وله حق الاستعانة بمحام مؤهل يختاره يستطيع زيارته بحرية وتوفر له التسهيلات اللازمة لإعداد دفاعه، وإذا لم يقدم المتهم على اختيار محام تعين له الدولة الحامية محامياً وفي حالة عدم وجود دولة حامية يتعين على دولة الاحتلال أن تنتدب له محامياً شريطة موافقة المتهم، كما يحق لأي متهم -إلا إذا تخلى بمحض إرادته عن هذا الحق- أن يستعين بمترجم سواء أثناء التحقيق أو جلسات المحكمة وله في أي وقت أن يعترض على المترجم أو يطلب تغييره[4].

---

[1]- "إن المحاربين المقبوض عليهم خلال قيامهم بنشاطات تجسس ليس لهم الحق في مركز أسير حرب ولا يمكن إدانتهم بدون محاكمة مسبقة" هذه القاعدة عرفية وكانت معروفة من قبل التقنين في اتفاقية لاهاي والبروتوكول الإضافي الأول لاتفاقيات جنيف؛ فقد كان منصوصاً عليها مثلا في إعلان بروكسل لسنة 1874 بشأن تدوين أحكام القانون العسكري في المادتين 20 و21:

-jean - Marie Henckaerts et Louise Doswald – Beck, op. cit, p. p. 515 – 516.

[2]- الفقرة الثالثة من المادة الخامسة من اتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب المؤرخة في 12 أوت من سنة 1949 كما نصت الفقرة الأولى من المادة 70 أيضاً على أنه: "لا يجوز للمحاكم المختصة التابعة لدولة الاحتلال إصدار أي حكم إلا إذا سبقته محاكمة قانونية".

[3]- الفقرة الثانية من المادة 71 من نفس الاتفاقية.

[4]- المادة 73 من من نفس الاتفاقية.

3- يجوز الحكم بالإعدام في حالة الإدانة بالجاسوسية، لكن يشترط أن يكون الإعدام هو عقوبة هذه التهمة بمقتضى التشريع الذي كان سارياً في الأراضي المحتلة قبل بدء الاحتلال، كما أنه لا يجوز إصدار حكم الإعدام إلا بعد توجيه نظر المحكمة بصفة خاصة إلى أن المتهم ليس من رعايا دولة الاحتلال؛ وهو لذلك غير ملزم بأي واجب للولاء نحوها، كما لا يجوز بأي حال إصدار حكم الإعدام على شخص يقل سنه عن الثامنة عشر سنة وقت اقتراف الجريمة[1].

4- يجب أن تبلغ الدولة الحامية بأسرع ما يمكن بجميع الأحكام التي تصدر بتطبيق عقوبة الإعدام، بحيث لا تبدأ مهلة الاستئناف في حالة الحكم بالإعدام إلا بعد وصول إخطار بالحكم إلى الدولة الحامية[2].

5- للشخص المحكوم عليه حق استخدام وسائل الاستئناف التي يقررها التشريع الذي تطبقه المحكمة، ويبلغ بكامل حقوقه في الاستئناف والمهلة المقررة لممارسة هذه الحقوق، كما لا يحرم الشخص المحكوم عليه بالإعدام بأي حال من حق رفع التماس بالعفو أو بإرجاء العقوبة[3].

6- لا ينفذ حكم الإعدام قبل مضي مدة لا تقل عن ستة شهور من تاريخ استلام الدولة الحامية للإخطار المتعلق بالحكم النهائي الذي يؤيد عقوبة الإعدام أو بقرار رفض التماس العفو أو إرجاء العقوبة، رغم أنه يجوز خفض مهلة الستة شهور هذه في حالات محددة عندما يترتب على وجود ظروف خطيرة وحرجة تهديد منظم لأمن دولة الاحتلال أو قواتها المسلحة، لكن يجب أن تتلقى الدولة الحامية دائماً إخطار بخفض المهلة وتُعطى لها الفرصة دائماً لإرسال ملاحظاتها في الوقت المناسب بشأن أحكام الإعدام هذه إلى سلطات الاحتلال المختصة[4].

ب- الحق في انقضاء المسؤولية عن أفعال التجسس في حالات معينة: بحيث تقرر اتفاقية لاهاي أن الجاسوس الذي التحق بالجيش الذي ينتمي إليه وتم القبض عليه لاحقاً من طرف العدو يعامل كأسير حرب ولا يكون محل مسؤولية عن أفعال التجسس السابقة[5]، ولقد ثار الجدل بين الفقهاء

---

[1]- المادة 68 من اتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب.

[2]- الفقرة الثانية من المادة 74 من نفس الاتفاقية.

[3]- الفقرة الأولى من المادة 75 من نفس الاتفاقية.

[4]- الفقرة الثانية والثالثة من المادة 75 من نفس الاتفاقية اتفاقية.

[5]- المادة 31 من اتفاقية لاهاي المتعلقة بقوانين وأعراف الحرب على الأرض.

حول السبب في إقرار مثل هذا المبدأ؛ فيذهب جانب للقول بأن السبب يرجع إلى صعوبة إثبات واقعة التجسس بعد أن يكون الجاسوس قد تمكن من العودة إلى صفوف جيشه. بينما يرى البعض الآخر أن الجاسوسية هي إحدى خدع الحرب المسموح بها وأن التهديد بإيقاع عقوبة شديدة على الجاسوس يعتبر عاملاً مانعاً من محاولة البعض القيام بها وبالتالي تعتبر هذه العقوبة غير ذات موضوع بعد وقوع الفعل وإتمامه. بينما يرى جانب آخر من الفقه أن الجاسوسية تشكل خطراً شديداً على الدولة وكيانها وهذا الخطر هو الذي يبرر للدولة معاقبة الجاسوس، فإذا تمكن الجاسوس من العودة إلى صفوف جيشه بعد أن قام بنشاطه التجسسي، فإن الخطر في هذه الحالة ينعدم ويتلاشى ومن ثم تنتفي حالة الدفاع الشرعي للدولة في مواجهة الجاسوس. بينما يقرر فقهاء آخرون أن الأشخاص الذين قاموا بأعمال البحث والاستطلاع عن العدو هم في الأصل جنود ملزمون بالقيام بتلك الأعمال بحكم طبيعة النظام العسكري الذي يخضعون له وليس بناء على مواقفهم أو رغباتهم الشخصية ومن ثم يجب ألا يعاملوا معاملة المجرمين، بل يجب إعتبارهم أسرى حرب شأنهم في ذلك شأن بقية العسكريين إذا وقعوا في قبضة الطرف المعادي[1].

رابعـاً- تقييم اتفاقيات القانون الدولي الإنساني وإسقاط أحكامها على التجسس الإلكتروني:

بداية سيتم تناول تقييم اتفاقيات القانون الدولي الإنساني في مواجهة التجسس، ومن ثم إسقاط أحكام اتفاقيات القانون الدولي الإنساني على التجسس الإلكتروني كالآتي:

أ- تقييم اتفاقيات القانون الدولي الإنساني في مواجهة التجسس: الملاحظ بعد عرض وتحليل مواد اتفاقيات القانون الدولي الإنساني المنظمة للتجسس في زمن الحرب، أنها تنظم أحكام فعل واحد وهو جمع المعلومات عن الخصم بطريقتين مختلفتين، فهي تعتبره من ناحية تجسس إذا ما تم باستخدام وسائل التنكر وتقرر له معاملة خاصة، ولا تعتبره من ناحية أخرى تجسساً إذا ما قام به العسكري وهو بزيه الرسمي وتقرر له كذلك في هذه الحالة معاملة مختلفة، ومن هذا المنطلق الذي يقوم على عدم النص صراحة على تجريم جوهر التجسس المتمثل في جمع المعلومات السرية؛ نجد الفقه قد إنقسم إلى فريقين: فريق يؤكد مشروعية التجسس، وفريق آخر يؤكد عدم مشروعية التجسس لكن ما يجمع

[1]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 369-370.

الفريقين أن كلاهما إستند إلى ذات الاتفاقيات السابقة لتبرير وجهة نظره، وسيتم عرض مذهب كل منها في الآتي:

1- مذهب مشروعية التجسس: يرى جانب من الفقه أن اتفاقيات القانون الدولي الإنساني المنظمة للتجسس تنظر إليه كنشاط مشروع؛ إذ أنها لم تجرمه ولم تمنع استخدامه، فاتفاقية لاهاي قد حددت ما يُمنع على الطرفين المتحاربين القيام به ولم تذكر التجسس من بينها[1]، كما أنها قد نصت صراحةً على أن حيل وخدع الحرب واستخدام الوسائل الضرورية للحصول على المعلومات عن العدو تعتبر مشروعة[2]، وقد أصبح الآن معترفاً بحق المتحاربين في استخدام الجواسيس كحيلة شرعية من حيل الحرب[3]، بالإضافة إلى أن ذات الاتفاقية قد نصت على أن الجاسوس الذي يعود وينضم إلى الجيش الذي ينتمي إليه ثم يقع في أسر العدو بعد ذلك يعامل كأسير حرب ولا مسؤولية عليه عن أعماله التجسسية السابقة[4]، فهذا النص وكما سبقت الإشارة إليه يسقط العقوبة عن الجاسوس الذي ينجح في العودة إلى جيشه إذا ما وقع في قبضة الطرف المعادي فيما بعد؛ مما يستدل معه على أن التجسس ليس جريمة في قانون الحرب وإلا كيف يمكن اعتبار نجاح الجاسوس في العودة إلى الطرف الذي ينتمي إليه سبباً من أسباب عدم المسؤولية[5]، هذا بالإضافة إلى الحكم الخاص الذي قرره البروتوكول الأول الإضافي لاتفاقيات جنيف والتي ورغم إعتبارها للفرد العسكري المقيم في إقليم الطرف المعادي جاسوساً، إلا أنه لا تجب معاملته كجاسوس بل كأسير حرب إلا إذا قُبض عليه متلبساً بجمع المعلومات[6].

وعموماً يذهب العديد من الفقهاء إلى تقرير أن مشروعية التجسس في زمن الحرب جاءت من عدم وجود أية التزامات عامة على المتحاربين بإحترام إقليم أو حكومة الدولة المعادية، وكذلك من انعدام وجود أية اتفاقيات دولية خاصة تنص على عدم مشروعية التجسس[7]، وهو الرأي الذي أخذت به كذلك

---

[1]- المادة 23 من اتفاقية لاهاي.

[2]- المادة 24 من نفس الاتفاقية.

[3]-Graig Brown, espionage in international law: a necessary evil, university of western ontario, 1999, p. 23.

[4]- المادة 31 من اتفاقية لاهاي.

[5]- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، مرجع سابق، ص. 184.

[6]- الفقرة الثالثة من المادة 46 من البروتوكول الأول الإضافي لاتفاقيات جنيف.

[7]- Graig Brown, op. cit, p. 23.

بعض المحاكم فقد ذهبت محكمة النقض الهولندية (الدائرة الجنائية) إلى أن القانون الدولي لا يعتبر التجسس جريمة حرب كما أن هذا القانون لا يجرمه كذلك[1].

2- مذهب عدم مشروعية التجسس: يتجه المؤيدون لهذا الإتجاه إلى أنه ليس هناك نص أو حكم في القانون الدولي يسمح بممارسة التجسس صراحةً أو ضمناً لاسيما معاهدة لاهاي، والقول بأنها قد عددت النواهي المحظورة في زمن الحرب ولم تكن أعمال التجسس من بينها، مردود عليه بأن المعاهدة لم تذكر النواهي على سبيل الحصر وإنما جاءت على سبيل المثال، كما أن نص المادة 24 من ذات المعاهدة يكشف عن مبدأ قديم متعارف عليه يقضي بمشروعية الاستطلاع العسكري في مناطق العمليات ولكنه لا يفيد إباحة التجسس، كما يذهب أنصار هذا المذهب إلى أن التجسس دائماً يشكل نشاطاً غير مشروع لأنه يظهر عن طريق ممارسة أعمال مستهجنة وبأساليب ذميمة يقوم بها الجواسيس، وأنه حتى لو افترض وجود هدف مشروع للتجسس، فإن عدم مشروعية الوسيلة المستعملة في التجسس تظل قائمة وكافية لإسقاط أي مظهر من مظاهر الشرعية عن هذا النشاط ذلك؛ لأن الجاسوس لا يبلغ هدفه إلا باستعمال الغدر والمكيدة والتدليس[2].

يمكن الرد على حجج هذه الإتجاه بالقول أن التجسس من الأعمال البارزة والأكثر أهمية وممارسة من طرف الدول؛ لذا لا يمكن تفسير عدم تضمن المادة 24 من اتفاقية لاهاي له بأنها عرضت بعض النواهي على سبيل المثال؛ لأن طبيعة ومكانة التجسس تفرض التطرق له لذا فالمرجح أن إغفال هذه المادة للنص عليه إنما هو إغفال مقصود يرمي إلى إبعاده من قائمة الأعمال المحظور القيام بها في الحرب، كما أنه لا يمكن رسم حدود دقيقة للتفريق بين الاستطلاع العسكري والتجسس فهما مفهومان متداخلان جداً، كما أن ربط التجسس باستعمال الغدر والمكيدة والتدليس يتماشى مع ما نصت عليه مواد الاتفاقيات السابق دراستها بإعتباره شرطاً ضرورياً لإعتبار الفرد جاسوس؛ الشيء الذي يدفع للقول بأن التجسس مشروع، فقط بشرط أن يقوم به العسكري بزيه الرسمي؛ لأنه يمكنه في حالة القبض عليه من الاستفادة من مركز أسير الحرب شأنه شأن بقية العسكريين وأفراد القوات المتحاربة إذا وقعوا في قبضة العدو فتكون أمامه فرصة العودة مجدداً إلى وطنه.

[1]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. 346.

[2] - نفس المرجع، ص. ص. 350- 352.

مما سبق يمكن القول بأن اتفاقيات القانون الدولي الإنساني المنظمة لأحكام التجسس قد أباحت جمع المعلومات السرية عن العدو وهو جوهر التجسس؛ ما يستفاد منه أنها لا تجرم التجسس في حد ذاته ولكنها تضع شروطاً للقيام به، وهي عدم استخدام التنكر أو التخفي تحت ستار كاذب ليصبح كأي تصرف أخر عادي تلجأ إليه الدول للفوز بمعاركها، بل وتحمي العسكري الجاسوس غير المتنكر وتعتبره أسير حرب.

ب- إسقاط أحكام اتفاقيات القانون الدولي الإنساني على التجسس الإلكتروني: إن الأحكام التي نظمتها مواد اتفاقيات القانون الدولي الإنساني ذات الصلة بالتجسس قد قُررت لتنظم التجسس الممارس في زمن الحرب بصفة عامة ودون تخصيص لنوع منه، وبإسقاطها على حالة التجسس الإلكتروني يمكن تسجيل الملاحظات الآتية:

1- لقد تم وضع اتفاقيات القانون الدولي الإنساني لتنظيم علاقات الدول ومراكز الأفراد وسلوكاتهم أثناء زمن الحرب، والحرب المقصودة هنا هي الحرب الواقعة في الإقليم المعروف والذي يشمل تقليديا المجال البري والبحري والجوي، وليس لتنظيم الحرب المعلوماتية التي تتم في الفضاء الإلكتروني والتي يعد التجسس الإلكتروني أهم أساليبها.

2- أغلب الأحكام المنظمة للتجسس قديمة جداً خاصة تلك الواردة في اتفاقية لاهاي، والدول تتفادى تحيينها رغم التغيير الجذري الذي عرفته أغلب العناصر الأساسية المستلزمة لقيام التجسس، فشرط التواجد بإقليم الخصم لم يعد له ذات الدلالة حالياً؛ إذ بانتقال الأفراد كما الدول إلى الفضاء الإلكتروني حيث لا توجد أهمية للحدود الجغرافية أصبح الحضور الفيزيقي للجواسيس في الإقليم الأجنبي غير ذي أهمية ما دام بالإمكان تعويضه بالحضور المعنوي، وما دامت النتيجة واحدة هي الحصول على أسرار الدولة الخصم.

3- ركزت الأحكام السابقة على ضرورة القيام بالتجسس باستخدام التخفي والتنكر، لكن حالياً أصبح للتخفي بعد آخر أكثر تعقيداً، فإذا كان كشف التنكر سابقاً في متناول الدولة بالنظر للحضور الشخصي للفرد الجاسوس فيها، ففي المقابل توفر اليوم تقنيات المعلومات والاتصالات بشكل بديهي عنصر الخفاء وتجعل الجواسيس الإلكترونيين في مأمن من الكشف؛ لذلك لم يعد جوهر الجوسسة الآن التنكر والادعاءات الكاذبة ولكن مجرد إذاعة وإعلان المعلومات بشكل غير مرخص، لذلك أضحت مسألة

عدم القدرة على مراقبة انسيابية المعلومة أهم قضية للدولة الحديثة إذ أصبحت تركز مجهوداتها على توفير الحماية الوقائية لمعلوماتها أكثر من العمل على إظهار وكشف الجواسيس الأجانب[1].

4- الشرط الأساسي الذي قررته مواد الاتفاقيات السابقة لغرض تحديد وضعية الشخص القائم بعملية جمع المعلومات من حيث إعتباره جاسوساً فيعامل على هذا الأساس، أو أسير حرب فيستفيد مما هو مقرر لهذه الفئة، هو ضرورة التمييز بين المحارب وغير المحارب[2]، وهذا التمييز يجب أن يكون على أساس ارتداء الزي العسكري، هذا الشرط جوهري لتطبيق كل اتفاقيات القانون الدولي الإنساني لكن لا يمكن إعماله في حالة التجسس الإلكتروني؛ لأن هذا الأخير يتم في الخفاء ونشاطاته غير مادية تعتمد على الحضور المعنوي للفرد سواء عسكري أو مدني في إقليم الخصم لذا لا يمكن الجزم بأن الشخص الذي يقوم بجمع المعلومات مدني أو عسكري، وحتى لو فرضنا أنه أمكن القبض على هذا الشخص فلا يمكن إثبات أنه كان يرتدي زيا عسكريا أم لا.

5- القواعد السابقة سُنت لتنظيم أحكام التجسس الذي تقوم به الدول إتجاه بعضها والذي يمارسه لحسابها الأفراد سواء كانوا عسكريين أم مدنيين بدافع خدمة الوطن أساساً، لكن حاليا أصبح التجسس مصدراً للثراء يمتهنه الأفراد لصالحهم الخاص بحيث لم يعد الهدف من جمع المعلومات إيصالها للدولة التي يعمل الجاسوس لصالحها وإنما أصبح الهدف هو المتاجرة بالأسرار ولا يهم الطرف الذي سيستفيد منها سواء كانت دولة أو جماعة إرهابية أو أفراد آخرين؛ وعليه فالأحكام السابقة قديمة ولا تصلح للتطبيق في حالة التجسس الذي يقوم به الأفراد والمؤسسات وجماعات الجريمة المنظمة والمنظمات الإرهابية،

---

[1]- Graig Brown, op. cit, p. 9.

[2]- إن مقتضى أن يكون المحارب متميزاً عن الشعب المدني هو في الأصل قاعدة قديمة للقانون الدولي العرفي، وكانت معروفة في إعلان بروكسل لسنة 1874 بشأن تدوين أحكام القانون العسكري في مادته التاسعة، وفي دليل الحرب البحرية المعروف بدليل أكسفورد لسنة 1880 في مادته الثانية ، ثم تم تقنينها فيما بعد في اتفاقية لاهاي في المادة الأولى والاتفاقية الثالثة لجنيف في المادة الرابعة وفي البروتوكول الإضافي الأول في المادة 44، وتطبيقات الدول تبرز أنه لأجل تمييز الشعب المدني فإن المحاربين ملزمون بارتداء زي أو علامة مميزة وحمل الأسلحة بشكل صريح، لكن أصبح الأمر مقتصراً بمقتضى اتفاقية لاهاي والبروتوكول الإضافي الأول على ارتداء الزي العسكري، كما يعد أيضاً ضمن طائفة المحاربين ويستفيد وفقاً لذلك من قانون أسرى الحرب السكان المدنيون الذين يحملون السلاح تلقائيا لأجل مقاومة المحتل أي ما يُعرف بحالة النفير، وهذه القاعدة عرفية تضمنتها المادة العاشرة من إعلان بروكسل والمادة الثانية من اتفاقية لاهاي والمادة الرابعة من اتفاقية جنيف الثالثة:

-Jean –Marie Henckaerts et Louise Doswald –Beck, op. cit, p. p. 510 – 512.

ويعبر بعض الكتاب عن الوضع الجديد بالقول: "العالم وطبيعة الصراع تغيرا وطرق خوض الحرب كذلك تغيرت فالصراعات الحالية والمستقبلية عالمية وعابرة للحدود والجيل الرابع للحرب يظهر جلياً من خلال خصم مفترس يعمل ويتحرك في عالم الشبكات بعيداً عن القوالب التقليدية للدول، فالإرهابيون والمجرمون والعصابات أصبحوا يشتغلون وبشكل واسع على النهايات الطرفية للتكنولوجيا الافتراضية والدخول إلى عالم المعلوماتية أصبح يسيراً بفضل الأموال الناتجة عن الجريمة المنظمة والعابرة للحدود وليس من الصعب تخيل هذه الكيانات وعبر إمكانياتها التي تجاري الحكومات في مراقبة الدول ومقدرتها الحربية في جعل أهدافها أكثر بُعداً ..."[1].

الفـــرع الثانـي: جهـود مكافحـة التجـسس الإلكترونـي في إطار اتفاقيات القانـون الدولـي للفضـاء الخارجـي.

شكل النصف الثاني من القرن العشرين بداية سباق عالمي كبير لاكتشاف الفضاء الخارجي واستغلال الميزات التي يمنحها، ليتحول بعد سنوات قليلة من ذلك إلى ساحة كبيرة تتزاحم فيها الأقمار الصناعية والأجسام الفضائية سواء المخصصة للأبحاث العلمية أو للاتصالات أو للبث التليفزيوني أو مراقبة الطقس؛ الأمر الذي حتم على الدول وضع إطار قانوني دولي ينظم حدود استخدامات الفضاء خاصة في ظل إعراب الكثير من الدول النامية –تحديداً– عن قلقها وتخوفها إزاء استخدام هذه الأقمار للتجسس إلكترونياً عليها؛ وبناء عليه فقد تم وضع عديد الاتفاقيات الدولية التي شكلت في مجموعها ما يُعرف بالقانون الدولي للفضاء الخارجي، القائم أساساً على مبدأ حرية استكشاف واستخدام الفضاء الخارجي؛ وعليه سيتم عرض هذا المبدأ ثم القيود الواردة عليه في ظل اتفاقيات الفضاء الخارجي لإبراز دورها في مكافحة التجسس الإلكتروني.

أولاً– مبـدأ حريـة استكشـاف واستخـدام الفضـاء الخارجـي:

نصت اتفاقية المبادئ المنظمة لنشاطات الدول في ميدان استكشاف واستخدام الفضاء الخارجي (تسمى أيضا اتفاقية الفضاء) على أن لجميع الدول حرية استكشاف واستخدام الفضاء الخارجي بما في ذلك القمر والأجرام السماوية الأخرى دون أي تمييز وعلى قدم المساواة ووفقا للقانون الدولي، ويكون حراً الوصول إلى جميع مناطق الأجرام السماوية، كما نصت كذلك على حرية إجراء الأبحاث العلمية في

[1]- Louise I . Gerdes, op. cit, p. p. 154– 155.

الفضاء الخارجي بما في ذلك القمر والإجرام السماوية الأخرى، وتراعي الدول تيسير وتشجيع التعاون في مثل هذه الأبحاث[1]، ومع أن النص صريح الدلالة على تقرير مبدأ حرية الاستكشاف والاستخدام بالنسبة لكافة الدول دون تمييز وعلى قدم المساواة، إلا أنه في حقيقة الأمر ليس إلا مبدأ صورياً بحتاً؛ لأن هذه الحرية لا يمكن ممارستها عملياً إلا بالنسبة لعدد قليل ومحدود من الدول مما يجعلها تهيمن على الفضاء الخارجي لامتلاكها التكنولوجيا والإمكانيات المادية لذلك، وقد تنبه المجتمع الدولي لهذه الحقيقة إذ مع إقراره لمبدأ حرية الاستكشاف والاستخدام لم يعط الدول الفضائية أي حق أو إدعاء السيادة أو التملك بالنسبة للفضاء الخارجي[2]، ولأجل ذلك تنص اتفاقية الفضاء على عدم جواز التملك القومي للفضاء الخارجي بما في ذلك القمر والأجرام السماوية الأخرى بدعوى السيادة أو بطريق الاستخدام أو وضع اليد أو بأية وسيلة أخرى[3]، وهو نفس ما نص عليه الاتفاق المنظم لأنشطة الدول على سطح القمر أو الأجرام السماوية، من أن القمر وموارده الطبيعية يعتبر تراثاً مشتركاً للإنسانية ولا يجوز إخضاعه للتملك الوطني بدعوى السيادة أو عن طريق الاستخدام أو الاحتلال أو بأية وسيلة أخرى[4]، وبهذا تكون هذه الاتفاقيات قد حسمت الجدل القائم حول السيادة وتطبيقها على الفضاء الخارجي[5]، ومن هذه النصوص يستنتج أن الفضاء الخارجي ملك للبشرية جمعاء وعلى وجه الدوام؛ فيكون لكل دولة تمتلك الإمكانيات اللازمة الحق

---

[1]– الفقرة الثانية والثالثة من المادة الأولى من معاهدة المبادئ المنظمة لنشاطات الدول في ميدان استكشاف واستخدام الفضاء الخارجي بما في ذلك القمر والأجرام السماوية الأخرى التي اعتمدتها الجمعية العامة للأمم المتحدة بقرارها رقم 2222 (د 21) والتي جرى توقيعها في لندن وموسكو وواشنطن في 27 جانفي سنة 1967 ودخلت حيز التنفيذ في 10 أكتوبر سنة 1967، وقد صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 342/91 المؤرخ في 28 سبتمبر سنة 1991.

[2]– محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. 390.

[3]– المادة الثانية من اتفاقية الفضاء الخارجي.

[4]– المادة 11 من الاتفاق المنظم لأنشطة الدول على سطح القمر أو الأجرام السماوية المعتمد من قبل الجمعية العامة للأمم المتحدة في قرارها رقم (34–68) الصادر في 18 ديسمبر سنة 1979 والذي دخل حيز التنفيذ ابتداءً من 11 يوليو سنة 1984.

[5]– في هذا الإطار ظهر اتجاهان فقهيان: اتجاه يؤيد مبدأ سيادة الدولة على كل ما يعلو إقليمها من فضاء ويمثله قلة من الفقهاء وهم أنصار مبدأ الامتداد اللانهائي للسيادة في الفضاء، واتجاه آخر يأخذ بمبدأ حرية الفضاء الخارجي أي استبعاد امتداد السيادة الإقليمية للفضاء الخارجي وهو توجه الفقه والعمل الدوليين (راجع أكثر ليلى بن حمودة، مرجع سابق، ص. ص. 45– 49) .

في استخدام هذا الفضاء للأغراض التي تريدها مع ضرورة إحترام ما تم تقريره في الاتفاقيات التي تحكمه والتي تشكل قيوداً على هذا المبدأ.

ثانياً- القيود الواردة على مبدأ حرية استكشاف واستخدام الفضاء الخارجي:

إذا كان المجتمع الدولي قد تراضى على تبني مبدأ حرية استكشاف واستخدام الفضاء الخارجي وعدم خضوعه للسيادة أو التملك أو الحيازة من قبل أية دولة، فإنه في المقابل لم يقبل أن تكون تلك الحرية مطلقة من كل قيد بحيث تستطيع كل دولة أن تفعل ما تشاء بدون ضوابط أو شروط؛ بالنظر إلى الأخطار التي يمكن أن تحدث انطلاقاً من الفضاء الخارجي، فعنصر المسافات والبعد عن الأرض لم يعد عنصراً مخففاً من درجة الخطورة، بل العكس؛ فالأبعاد المترامية والسحيقة للفضاء جعلت إمكانية اكتشاف أو تحديد مصدر الخطر أمراً بالغ الصعوبة إن لم يكن مستحيلاً بالنسبة للدولة المتجسس عليها، وما يزيد من خطورة الوضع أن العديد من الشركات والمنظمات الخاصة ذات النشاط التجاري والاستثماري قد دخلت بدورها في مجال الاستطلاع الفضائي وهذا في حد ذاته يعرض المصالح السياسية والاقتصادية والعسكرية للدول المتجسس عليها لمخاطر وأضرار حقيقية، ومن أجل ذلك فإن المجتمع الدولي عندما قبل بمبدأ حرية استكشاف واستخدام الفضاء قد قيده ببعض الشروط والضوابط، وذلك بأن تكون الاستخدامات الفضائية ذات طبيعة سلمية، وأن يكون هدفها تحقيق فائدة ومصلحة كافة الدول[1]، وهي القيود التي سيتم تفصيلها ومحاولة تقييمها في الآتي:

أ- **قيد الاستخدامات السلمية:** تنص الفقرة الثانية من المادة الرابعة من اتفاقية الفضاء الخارجي على ضرورة أن تراعي جميع الدول الأطراف في المعاهدة قصر استخدامها للقمر والأجرام السماوية الأخرى على الأغراض السلمية، وقد أثارت صياغة هذه المادة الكثير من الجدل والنقاش من طرف الفقهاء، ولقد انصب هذا النقاش تحديداً على المقصود بتعبير "الأغراض السلمية"؛ فانقسم الفقه إلى إتجاهين: إتجاه يفسره بغير العسكري، أي منع استخدام الفضاء الخارجي لأغراض عسكرية، بينما يذهب الإتجاه الثاني إلى أن المقصود بتعبير الأغراض السلمية هو الغير عدواني والذي يشير إلى عدم اللجوء إلى حالة الحرب وعدم التهديد أو استخدام القوة العسكرية؛ لذلك فإن إطلاق الأقمار الصناعية الاستطلاعية لغايات عسكرية أو أمنية يمكن عدها جميعاً أعمالاً سلمية وليست عدوانية ما دامت الدولة

[1]- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 392-393.

لم تقم بعدوان عسكري على دولة أخرى، ويدعم هذا التوجه أن كلاً من الولايات المتحدة الأمريكية وروسيا ما فتأتا تقومان بأعمال عسكرية في الفضاء الخارجي مع تمسكهما الدائم بأنهما لم يخرجا في أي وقت عن الاستخدام السلمي للفضاء الخارجي، ما يفهم منه إتجاههما إلى تفسير الاستعمال السلمي للفضاء الخارجي بعدم العدوان[1]؛ ويترتب على النقاش والجدل بخصوص تفسير النص أن التجسس الذي يقع عن طريق الأجهزة الفضائية يعتبر عملاً غير مشروع طبقاً للإتجاه الأول، وعملاً مشروعاً طبقاً للإتجاه الثاني وهو الإتجاه الغالب.

ب- قيد تحقيق فائدة ومصلحة كافة الدول: بحيث يكون استخدام الفضاء الخارجي مشروعاً طبقا للقانون الدولي، إذا كان يرمي إلى تحقيق المصلحة المشتركة التي تعود بالفائدة على الإنسانية جمعاء، بل ويستوجب تشجيع العمل المشترك والتعاون الدولي لبلوغ هذه الهدف، وفي هذا الإطار تنص الفقرة الأولى من المادة الأولى من اتفاقية الفضاء الخارجي على أن يباشر استكشاف واستخدام الفضاء الخارجي لتحقيق فائدة ومصالح جميع البلدان أياً كانت درجة نمائها الاقتصادي أو العلمي، كما أضافت الفقرة الثالثة من ذات المادة أن إجراء الأبحاث العلمية في الفضاء الخارجي يكون حراً مع الحث على أن تراعي الدول تيسير وتشجيع التعاون الدولي في مثل هذه الأبحاث، كما تضمنت المادة الخامسة من ذات الاتفاقية حث الملاحين الفضائيين التابعين لأية دولة من الدول الأطراف على تقديم كل مساعدة ممكنة عند مباشرة أية نشاطات في الفضاء الخارجي إلى الملاحين الفضائيين التابعين للدول الأطراف الأخرى، كما اعتبرت ذات المادة بأن الملاحين الفضائيين يعدون بمثابة مبعوثي الإنسانية في الفضاء الخارجي لذلك يجب تزويدهم بكل مساعدة ممكنة عند حصول أي حادث أو هبوط اضطراري في إقليم أية دولة من الدول الأطراف أو في أعالي البحار، والمبادرة في حالة هبوط الملاحين الفضائيين اضطراراً إلى إعادتهم سالمين إلى الدول المسجلة فيها مركبتهم الفضائية، ولم تكتف الدول بخصوص هذا الموضوع بإقرار مبدأ مساعدة الملاحين الفضائيين في اتفاقية الفضاء الخارجي بل خصصت له اتفاقية مستقلة تتضمن الإحاطة به وإقرار كل الأحكام ذات الصلة بإنقاذ الملاحين الفضائيين وكذا إعادتهم ورد

[1]- سهى حميد سليم الجمعة، تلوث بيئة الفضاء الخارجي في القانون الدولي العام، دار المطبوعات الجامعية، مصر، 2009، ص. ص. 69- 70.

الأجسام المطلقة في الفضاء، وهذا نابع كما جاء في ديباجة هذه الاتفاقية والتي تسمى باتفاقية الإنقاذ والإعادة اختصاراً، من رغبة الدول في تعزيز التعاون الدولي والتي تحدوها إلى ذلك المشاعر الإنسانية[1].

وانطلاقاً من هذا يكون على الدول أن تمتنع عن استخدام الفضاء الخارجي لمصلحتها الخاصة إضراراً ببقية الدول، وباعتبار التجسس وبشكل قاطع وبديهي لا يحقق فائدة لكافة الدول؛ فهو من هذا المنظور يشكل نشاطاً غير مشروع، وهو الرأي الذي تبناه وسانده الإتحاد السوفيتي في فترة الحرب الباردة؛ بحيث أبدى منذ سنة 1962 تحفظه على هذه الأنشطة في مشروعه المقدم للجنة الاستخدامات السلمية للفضاء الخارجي للأمم المتحدة بشأن إعلان المبادئ الأساسية التي تحكم الفضاء الخارجي معتبراً أن استخدام الأقمار الصناعية كوسيلة من وسائل المخابرات وجمع المعلومات عن أقاليم الدول الأخرى لا يتفق وأهداف البشرية في غزو وارتياد الفضاء الخارجي، كما تضمن نصاً يمنع استخدام الأقمار الصناعية لجمع المعلومات السرية، وترى وجهة النظر السوفياتية أن الاستطلاع من الفضاء الخارجي يُعد مخالفةً خطيرةً للقانون الدولي؛ على أساس أن موضوع النشاط والغرض منه هو الذي يحدد مشروعيته وليس المكان الذي يتم فيه، كما أن المشروع السوفياتي لاتفاقية مساعدة وإنقاذ رواد الفضاء وإعادة الأجسام الفضائية قد تضمن النص على أن الأقمار الصناعية التي تستخدم لهذا الغرض تكون محلاً للمصادرة إذا سقطت في الإقليم الذي تجمع المعلومات عنه[2]، لكن اتفاقية الإنقاذ والإعادة لم تتضمن في نسختها النهائية مثل هذا النص؛ مما يدفع للقول بأنه حتى في الحالة التي تكون فيها الدولة متأكدة بأن الملاحين الفضائيين وكذا الأجسام الفضائية كان هدفها التجسس، فبموجب مصادقتها على اتفاقية الإنقاذ والإعادة تكون ملزمة بإنقاذ الملاحين الفضائيين وتزويدهم بكل مساعدة لازمة[3]، كما تكون ملزمة بمساعدة السلطة المُطلِقة لاسترجاع أي جسم فضائي أو أي جزء من أجزائه سقط على إقليمها[4]، بمعنى أن هذه الاتفاقية لا تعتبر التجسس مشروعاً وفقط بل وتلزم الدول على السكوت عنه والاشتراك في ممارسته، ويصبح الأمر أكثر غرابة حينما تضطر دولة مُتجسس عليها إلى إنقاذ ومساعدة الملاحين الفضائيين

---

[1]– اتفاقية إنقاذ الملاحين الفضائيين وإعادة الملاحين الفضائيين ورد الأجسام المطلقة في الفضاء الصادرة بمقتضى قرار الجمعية العامة للأمم المتحدة رقم 2345 (د. 22) بتاريخ 19 ديسمبر سنة 1967، والتي تم فتحها للتوقيع بلندن وموسكو وواشنطن في 22 أفريل سنة 1968 ودخلت حيز التنفيذ في 3 ديسمبر سنة 1968، والجزائر لم توقع ولم تصادق عليها.

[2]– ليلى بن حمودة، مرجع سابق، ص. 234.

[3]– المادة الثانية من اتفاقية إنقاذ الملاحين الفضائيين وإعادة الملاحين الفضائيين ورد الأجسام المطلقة في الفضاء.

[4]– المادة الخامسة من نفس الاتفاقية.

وإعادة المركبات الفضائية التي تجسست عليها إلى دولها الأصلية، ولا يكون للدولة المتجسس عليها إلا الحق في مطالبة الدولة المُطلِقة بالتعويض عن الأضرار التي تسببها أجسامها الفضائية تطبيقاً لاتفاقية المسؤولية الدولية عن الأضرار التي تحدثها الأجسام الفضائية[1]، ولا تشمل بطبيعة الحال الأضرار هنا التجسس، بل يُقصد بها الخسارة في الأرواح أو الإصابة الشخصية أو أي ضرر آخر بالصحة أو الخسارة أو الضرر الذي يلحق بممتلكات الدولة أو ممتلكات الأشخاص الطبيعيين أو المعنويين[2].

نجد في المقابل دولاً أخرى تذهب إلى حد القول بأن التجسس الفضائي يحقق مصلحة وفائدة البشرية جمعاء ومن ثم كان استخدامه مشروعاً؛ لأنه وسيلة فعالة في حماية الأمن والسلم الدوليين لاسيما في مرحلة الرعب النووي التي مازال العالم يعيش في ظلها حالياً، إذ أن الاستعدادات العسكرية في المجتمعات والدول النووية تتم في سرية كاملة ولا سبيل للتعرف عليها إلا عن طريق التجسس الفضائي، كما أن عمليات نزع السلاح النووي تحتاج إلى معرفة هذه الأسلحة وإلى القدرة على مراقبة تنفيذ ما تضمنته المعاهدات الخاصة بذلك، وهذا أمر لا يمكن تحقيقه بصورة فعالة إلا عن طريق التجسس الفضائي[3]، لكن تجب الإشارة هنا إلى أن ما يحدد مشروعية أو عدم مشروعية التجسس الفضائي ليس كونه يحقق أو لا يحقق مصلحة البشرية جمعاء وإنما وضعية الدولة ودرجة تقدمها، فالواقع يشهد بأن الدول التي تتمسك بمبدأ عدم المشروعية هي عادة دول لا تمتلك المقدرة العلمية أو التقنية لاستكشاف أو استخدام الفضاء الخارجي، لكن بمجرد أن تصل إلى درجة تستطيع معها إرتياد الفضاء يتغير موقفها وتصبح ضمن الفريق الذي يدافع عن التجسس عبر الأقمار الصناعية، وهو ما حدث بالفعل مع بعض الدول ومنها البرازيل والإتحاد السوفياتي[4].

---

[1]– المادة الثامنة من اتفاقية المسؤولية الدولية عن الأضرار التي تحدثها الأجسام الفضائية (وافقت عليها الجمعية العامة للأمم المتحدة بقرارها رقم 2777 (د. 26) بتاريخ 29 نوفمبر سنة 1971، وعرضت للتوقيع بلندن وموسكو وواشنطن بتاريخ 29 مارس سنة 1972، ودخلت حيز التنفيذ بتاريخ 1 سبتمبر سنة 1972، وقد تم التوقيع عليها من طرف الجزائر في 20 أفريل سنة 1972 ولكنها لم تصادق عليها).

[2]– المادة الأولى من نفس الاتفاقية.

[3]– محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مرجع سابق، ص. ص. 396–397.

[4]– ليلى بن حمودة، مرجع سابق، ص. 247.

من ناحية أخرى ذهب بعض الفقهاء بغرض ضمان أن يتم استخدام الفضاء الخارجي لمصلحة البشرية جمعاء إلى التفكير في تدويل نشاطات الفضاء كلياً، وهذا عن طريق إنشاء منظمة دولية تتولى إطلاق السفن الفضائية واستخدامها فضلاً عن تصنيعها، وفي هذه الحالة يخضع الفضاء إلى نظام وإدارة عامة تتصاع الدول لأوامرها، وعلى الرغم من أن المداولات بشأن إنشاء سلطة دولية عليا مطروح الآن على طاولة المفاوضات في لجنة الاستخدام السلمي للفضاء الخارجي، إلا أن الشكوك حول مدى نجاحها قائمة؛ إذ هل بوسع روسيا الإتحادية أو الولايات المتحدة الأمريكية مثلاً التخلي عن أسرار صنع أقمارها الصناعية وبرامج إطلاقها لمصلحة منظمة دولية أو سلطة عليا تشرف على الأنشطة الفضائية[1]، كما أنه من المستحيل أن تتنازل هاتين الدولتين عن هيمنتهما على استخدام الفضاء الخارجي لتحقيق مصالحهما واستغلاله في التجسس الإلكتروني على بقية الدول، خاصة وأنهما تستفيدان من القصور في كل الاتفاقيات المنظمة لاستخدام الفضاء الخارجي هذا القصور الذي لعبتا الدور الأساسي في وجوده من خلال إسهامهما وبشكل رئيسي في وضع هذه الاتفاقيات خدمة لمصالحهما، وهذا ما يفسر عدم خضوع هذه الاتفاقيات للتعديل أو التغيير لحد اليوم؛ وعليه يبقى التجسس الإلكتروني في إطارها نشاطاً مسموحاً به لكل دولة لها المقدرة والإمكانيات على إرتياد الفضاء ما يحتم على أية دولة ترغب في حماية أمنها أن تقوم سواء بمفردها أو في إطار التعاون الدولي بتطور قدراتها لتصبح هي الأخرى ضمن الدول التي لها مكان في الفضاء الخارجي؛ خاصةً وأن اتفاقية الفضاء الخارجي تعد أساساً قانونيا لذلك من خلال نصها على مبدأ حرية استكشاف واستخدام الفضاء الخارجي وتشجيعها على التعاون الدولي في هذا الإطار.

الفـــرع الثالـــث: جهود مكافحة التجسس الإلكتروني في إطار الاتفاقيات المنظمة لاستخدام الطاقـة النوويـــة.

تحقيقاً للحد من إنتشار الأسلحة النووية؛ تم وضع نظام دولي شامل للضمانات النووية، وقد حددت معالم هذا النظام مواد معاهدة عدم إنتشار الأسلحة النووية وجملة من الوثائق الصادرة تطبيقاً لها[2]،

---

[1]– سهى حميد سليم الجمعة، مرجع سابق، ص. 10.

[2]– جاء في ديباجة معاهدة عدم إنتشار الأسلحة النووية (المعتمدة بموجب قرار الجمعية العامة للأمم المتحدة 2373 (د. 22) المؤرخ في 12 يونيو/ حزيران سنة 1968، وجرى توقيعها في كل من لندن وموسكو وواشنطن في 1 تموز/يوليو سنة 1968، ودخلت حيز التنفيذ في مارس سنة 1970)؛ تعهد الدول الأطراف في المعاهدة بالتعاون في تسهيل تطبيق ضمانات الوكالة الدولية للطاقة الذرية على النشاطات الدولية السلمية، كما فرضت في مادتها الثالثة التزاماً على كل دولة غير حائزة للأسلحة النووية تكون طرفاً في المعاهدة بقبول الضمانات المنصوص عليها في اتفاق يجري التفاوض عليه= =

وبموجب هذا النظام يكون على الدولة تزويد الوكالة الدولية للطاقة الذرية بمعلومات عن سير برنامجها السلمي لاستخدام الطاقة النووية، كما تلتزم من جانب آخر باستقبال موظفي هذه الوكالة المكلفون بتفتيش المواقع النووية للدول الأطراف، وهذين الالتزامين يؤديان بشكل أكيد إلى علم الوكالة بمعلومات ذات طابع سري ولها ارتباط وطيد بالدفاع الوطني؛ لذا يقع على الوكالة كما على موظفيها التزام الحفاظ على الأسرار التي تصل إلى علمها نتيجة تطبيق نظام الضمانات ويكون على موظف الوكالة الذي يخل بهذا الالتزام تحمل نتائج قيامه بإفشاء أسرار الدفاع الوطني النووية المتعلقة بدولة ما طرف في الاتفاقية الدولية للحد من إنتشار الأسلحة النووية والاتفاقيات ذات الصلة بها؛ وعليه سيتم التطرق بداية إلى واجب حفظ أسرار الدفاع الوطني النووية، ومن ثم إلى أثر الإخلال بواجب حفظ أسرار الدفاع الوطني النووية.

أولاً- واجب حفظ أسرار الدفاع الوطني النووية:

يرد إلى الوكالة الدولية للطاقة الذرية كم هائل من المعلومات من طرف الدول الخاضعة لنظام الضمانات والتي تعد في معظمها سرية متعلقة بدفاعها الوطني، وتقوم الوكالة بتخزينها في حاسبات خاصة لدى إدارة الضمانات لديها، ولإدراك الوكالة للطابع الحساس لهذه المعلومات فقد أقرت أنظمة حماية تتركز على الأمن المعلوماتي -كما سبق عرضه من قبل- والوكالة في هذا الإطار لم تقصر حمايتها لأسرار الدفاع النووية الخاصة بالدول الأعضاء على تلك المخزنة في حاسباتها بل امتدت حمايتها إليها وهي داخل دولها بأن فرضت مجموعة من الالتزامات على الموظفين لديها وخاصة المفتشين الدوليين قوامها الحفاظ على تلك الأسرار وعدم إفشائها إذا تعلق علمهم بها أثناء عملهم لحساب الوكالة في الدول الأعضاء، فهناك التزام عام يقع على عاتق الوكالة وموظفيها ورد في المادة السابعة من

وعقده مع الوكالة الدولية للطاقة الذرية وفقاً لنظام الوكالة الأساسي ونظام ضماناتها، وتكون الغاية الوحيدة من ذلك تحري تنفيذ تلك الدولة للالتزامات المترتبة عليها بموجب هذه المعاهدة؛ منعاً لتحويل استخدام الطاقة النووية من الأغراض السلمية إلى الأسلحة النووية؛ وبناءً على ما ورد في هذه المعاهدة قامت الوكالة الدولية للطاقة الذرية من جانبها في ماي سنة 1971 بإقرار وثيقة للضمانات تنفذ في إطار معاهدة منع إنتشار الأسلحة النووية بعنوان هيكل ومضمون الاتفاقات التي تعقد بين الوكالة والدول بموجب معاهدة عدم إنتشار الأسلحة النووية، وهي الوثيقة INFCIRC /153 والتي تعرف باتفاقية الضمانات الشاملة، وبغرض زيادة فعالية الضمانات النووية جاءت الوثيقة INFCIRC /540 بعنوان البروتوكول النموذجي الإضافي للاتفاق(ات) المعقود(ة) بين الدولة (الدول) والوكالة الدولية للطاقة الذرية من أجل تطبيق الضمانات، وقد صدرت هذه الوثيقة عن الوكالة في سبتمبر سنة 1997، وهذه الوثيقة مصممة للدول التي لديها اتفاقات ضمانات مع الوكالة الدولية للطاقة الذرية من أجل توطيد فعالية نظام الضمانات وتحسين كفاءته كمساهمة في سبيل أهداف عدم الانتشار النووي العالمي.

القانون الأساسي للوكالة بعدم إفشاء أي سر صناعي أو أية معلومات أخرى سرية يطلعون عليها بمقتض عملهم الرسمي في الوكالة[1]، كما ورد هذا الالتزام في عديد الاتفاقيات المنظمة لاستخدام الطاقة النووية الصادرة عن الوكالة، فقد نصت الوثيقة (INFCIRC/153) المعروفة باتفاقية الضمانات الشاملة على وجوب أن تتخذ الوكالة الدولية للطاقة الذرية كافة الاحتياطات التي تتطلبها حماية الأسرار التجارية والصناعية وغيرها من المعلومات السرية التي تصل إلى علمها من خلال تنفيذ اتفاق الضمانات، وليس للوكالة أن تنشر أو تبلغ أية دولة أو أية منظمة أو أي شخص أية معلومات حصلت عليها من خلال تنفيذ اتفاق الضمانات، إلا أن لها أن تبلغ معلومات محددة تتصل بتنفيذ هذا الاتفاق إلى مجلس المحافظين، وإلى موظفي الوكالة الذين تتطلب مهامهم الرسمية المتعلقة بالضمانات أن يكونوا على بينة من هذه المعلومات، شريطة أن يكون ذلك في الحدود الدنيا التي يتطلبها إيفاء الوكالة لمسؤولياتها في تنفيذ الاتفاق، ويجوز نشر معلومات موجزة عن المواد النووية الموضوعة تحت ضمانات الوكالة بموجب الاتفاق بناءً على قرار يتخذه المجلس إذا وافقت على ذلك الدولة المعنية مباشرة[2]، كما نصت ذات الوثيقة على إلزام الدولة بأن تتخذ الخطوات اللازمة التي تكفل تمكين مفتشي الوكالة من الاضطلاع على نحو فعال بوظائفهم التي يقضي بها الاتفاق، وفي المقابل يجب أن يتم ترتيب زيارات مفتشي الوكالة وأنشطتهم على نحو يقلص إلى الحد الأدنى من احتمالات الإزعاج والإرباك للدولة وللأنشطة النووية السلمية محل التفتيش، ويكفل حماية الأسرار الصناعية محل التفتيش أو أية معلومات سرية أخرى تتناهى إلى علم المفتش[3]، كما ورد التزام عام بحماية أسرار الدفاع النووية في اتفاقية الحماية المادية للمواد النووية والمرافق النووية، إذ نصت على ضرورة أن تتخذ الدول الأطراف ما يقتضيه الحال من التدابير المتماشية مع قوانينها الوطنية لحماية سرية أية معلومات تتلقاها بوصفها موضع ثقة بفضل أحكام هذه الاتفاقية من دولة طرف أخرى، أو من خلال اشتراكها في أي نشاط مضطلع به تنفيذاً لهذه الاتفاقية، وإذا أسرّت دول أطراف بمعلومات إلى منظمات دولية، تعين إتخاذ خطوات لحماية سرية تلك المعلومات، كما أقرت هذه الاتفاقية بعدم إلزام الدول الأطراف بتقديم أية معلومات لا تسمح لها قوانينها الوطنية الإفضاء بها أو أية

[1]– عماد الدين محمد كامل الجمل، مرجع سابق، ص. 226.

[2]– المادة الخامسة من الوثيقة رقم INFCIRC /153 بعنوان هيكل ومضمون الاتفاقيات التي تعقد بين الوكالة الدولية للطاقة الذرية والدول بموجب معاهدة عدم انتشار الأسلحة النووية، المعروفة باتفاقية الضمانات الشاملة، الصادرة عن الوكالة الدولية للطاقة الذرية في ماي سنة 1971.

[3]– المادة التاسعة من نفس الوثيقة.

معلومات من شأنها أن تعرّض للخطر أمن الدولة المعنية أو الحماية المادية للمواد النووية[1]، كما تضمنت الوثيقة رقم (INFCIRC /540)[2] النص على الالتزام بالمحافظة على الأسرار النووية، إذ أقرت في ديباجتها إلزام الوكالة بإتخاذ جميع الاحتياطات التي تكفل حماية الأسرار التجارية والتكنولوجية والصناعية وغير ذلك من المعلومات السرية التي تتناهى إلى علمها، كما عادت وأكدت ذات الالتزام في المادة 15 منها، بحيث تنص الفقرة الأولى من هذه المادة على وجوب أن تطبق الوكالة نظاماً صارماً يكفل الحماية الفعالة ضد إفشاء الأسرار التجارية والتكنولوجية والصناعية وغير ذلك من المعلومات التي تتناهى إلى علمها، بينما نصت فقرتها الثانية على أن نظام الحماية المذكور يجب أن يتضمن أحكاماً تتعلق بالمبادئ العامة والتدابير المرتبطة بها للتعامل مع المعلومات السرية، وكذلك أن يتضمن شروط استخدام الموظفين فيما يتعلق بحماية المعلومات السرية، وكذلك الإجراءات التي تتخذ في حالات انتهاك السرية أو إدعاءات انتهاكها.

ثانياً- أثر الإخلال بواجب حفظ أسرار الدفاع الوطني النووية:

بالنظر إلى حساسية المعلومات التي تصل إلى علم الوكالة وارتباطها بأمن الدولة التي تسهم في توفيرها، فإن الوكالة وفي حالة ما إذا أخل أحد موظفيها أو أحد مفتشيها بالالتزام بالحفاظ على سرية المعلومات النووية التي توصل إليها بمناسبة عمله بالوكالة، وذلك بأن أفشى ذلك السر أو سلمه إلى دولته أو إلى إحدى الدول أو المنظمات أو أية جهة أو إلى أي شخص يعمل لحساب هؤلاء جميعاً؛ شكل هذا العمل جريمة تنشئ حقاً للدولة الواقع عليها الإعتداء بمحاكمة هذا الشخص فضلاً عن كونه يعد انتهاكاً صارخاً للامتيازات والحصانات التي قررتها الوكالة لهؤلاء للقيام بمهام عملهم، وتجدر الإشارة في هذا الإطار إلى أن الوكالة الدولية للطاقة الذرية قد قررت لموظفيها ومفتشيها جملة من الإمتيازات والحصانات لكي تؤهلهم للقيام بمهام أعمالهم و لم تكتف بتقرير تلك الإمتيازات والحصانات في صلب دستورها أو في الوثائق الصادرة عنها، بل عقدت اتفاقية بهذه الإمتيازات والحصانات وألزمت الدول الأعضاء فيها بالتوقيع عليها وذلك في يوليو من سنة 1960، لكن في حالة تجاوز هؤلاء الموظفين والمفتشين لما تقرر لهم من

[1]- المادة السادسة من اتفاقية الحماية المادية للمواد النووية (الموقعة في فيينا ونيويورك في 3 مارس سنة 1980 ودخلت حيز التنفيذ في 8 فبراير سنة 1987، وأصبحت بعد عقد المؤتمر الدبلوماسي لتعديل الاتفاقية وتعزيز أحكامها في سنة 2005 تسمى باتفاقية الحماية المادية للمواد النووية والمرافق النووية، وقع عليها لغاية سنة 2014، 149 دولة) .

[2]- الوثيقة INFCIRC /540 المعنونة بالبروتوكول النموذجي الإضافي للاتفاق(ات) العقود(ة) بين الدولة (الدول) والوكالة الدولية للطاقة الذرية من أجل تطبيق الضمانات، الصادرة عن الوكالة الدولية للطاقة الذرية في سبتمبر 1997.

إمتيازات وحصانات بأن جاءت أعمالهم لحسابهم الخاص أو لحساب دولهم أو لحساب أي شخص أو أية منظمة أو جهة كانت، نكون بصدد إساءة استعمال الإمتيازات والحصانات المقررة بما تمثله من خرق لدستور الوكالة والوثائق الصادرة عنها خاصة اتفاقية الحصانات والإمتيازات[1]، وفي هذه الحالة يقع على الوكالة التزام عام بالتعاون مع السلطات المختصة في الدول الأعضاء لضمان سير العدالة وتجنب كل إساءة لاستعمال الإمتيازات والحصانات والتسهيلات التي قررتها الاتفاقية، فيكون على الوكالة واجب رفع الحصانة عن أي موظف تابع لها في جميع الحالات التي ترى فيها أن الحصانة تحول دون أخذ العدالة مجراها وأن رفعها لا يضر بمصالح الوكالة[2]، وعدم الاكتفاء فقط بالفصل؛ إذ أن فصله في الأحول التي بلغت فيها إساءته للدرجة التي يستحق معها ذلك الجزاء كقيامه بإفشاء أو تسليم سر من أسرار الدفاع النووية لأحد الدول الأعضاء يكون قد علمه أو حصل عليه بمناسبة قيامه عمله لحساب الوكالة؛ غير كاف لإمكان محاكمته عن جرائمه لكونه يتمتع بحصانة تحول دون ذلك حتى بعد انتهاء وظيفته إذا تعلقت المخالفة بمهام عمله كمفتش أو موظف تابع للوكالة؛ لذا فإنه يجب على الوكالة ومن منطلق التزامها بالتعاون مع سلطات الدول الأعضاء لتحقيق العدالة أن ترفع عنه الحصانة في تلك الأحوال حتى يمكن محاكمته عن جرائمه وفقا لقانون الدولة الواقع عليها الإعتداء.

إن الحقوق والإمتيازات والحصانات المقررة لموظفي الوكالة ومفتشيها لم تقرر لمصلحتهم الخاصة ولا لمصالح دولهم وإنما تقررت لصالح الوكالة ولتحقيق أهدافها، فإذا خرج الموظف (المفتش) عن نطاق وظيفته، بأن أفشى سراً من أسرار الدفاع النووية لإحدى الدول كان قد علمه بسبب وظيفته، كان على الدولة التي وقع عليها الإعتداء إتخاذ كافة الإجراءات التحفظية اللازمة وإعلان الوكالة بالأمر لسحب الإمتيازات والحصانات المقررة لهذا المخالف، وعلى الوكالة من جانبها ومن واقع التزامها بالتعاون مع الدول الأعضاء فيها لتحقيق سير العدالة، أن ترفع الحصانة عن ذلك الموظف (المفتش) تمهيداً لحاكمته وفقا لقواعد الاختصاص المقررة في الدولة الواقع عليها الإعتداء، وطالما أن ذلك جزء من التزام الوكالة تجاه الدول الأعضاء فيها وأنه يحقق العدالة؛ فإنه من الطبيعي ألا يمثل ذلك عرقلة لسير عمل الوكالة أو يمثل ذلك منعاً من تأدية وظائفها الأصلية[3].

---

[1]– عماد الدين محمد كامل الجمل، مرجع سابق، ص. ص. 228– 229.

[2]– المادة السادسة من اتفاقية الحصانات والإمتيازات للوكالة الدولية للطاقة الذرية الموقعة في يوليو سنة 1960.

[3]– عماد الدين محمد كامل الجمل، مرجع سابق، ص. ص. 230– 231.

إن متابعة موظفي أو مفتشي الوكالة الدولية للطاقة الذرية في حالة إفشاءهم لأسرار الدفاع الوطني للدول الأعضاء في اتفاقية منع إنتشار الأسلحة النووية واتفاقياتها للضمانات يبدوا صعباً للغاية بالنظر لعديد الأمور: أولها أن المتابعة مشروطة برفع الوكالة للحصانة على موظفها أو مفتشها، وهو بحسب المادة السادسة السابق ذكرها ليس أمراً تلقائياً يتم بشكل آلي بمجرد إفشاء هؤلاء لأسرار الدولة، ولكن يخضع للسلطة التقديرية للوكالة، وذلك إذا رأت أن الحصانة تحول دون أخذ العدالة مجراها وأن رفعها لا يضر بمصالح الوكالة فلهذه الأخيرة وحدها تقرير ما قد يضر وما قد لا يضر بمصالحها، وحتى في الحالة التي ترفع فيها الوكالة الحصانة عن موظفها أو مفتشها تتطلب متابعتهم ضرورة تواجدهم في إقليم الدولة حين إفشاءهم لأسرارها وعلمهم بذلك، وإذا كان من الممكن تحقق هذا الفرض في حالة المفتش لأن عمله يقتضي التواجد في إقليم الدولة المعنية، فإنه من الصعب تحققه في حالة الموظف لأن عمله عادة ما يتم على مستوى الوكالة وعلمه بأسرار الدولة يتم من خلال عمله فيها وليس من خلال تواجده في الدولة المعنية ويستلزم لمتابعته حصول الدولة على تسليمه، وفي هذا الإطار لا يوجد أي نص في كل اتفاقيات الوكالة يتحدث عن مثل هذا الأمر، وكل ما هنالك هو إمكانية فصله ورفع الحصانة عليه دون تسليمه؛ فتصبح الدولة من جديد أمام مشكلة تطبيق مبدأ العينية وما يطرحه من صعوبات، وهناك إشكالية أخرى تتعلق بإمكانية إتهام مفتش الوكالة الدولية للطاقة الذرية بإفشاء أسرار الدفاع النووية للدولة المعنية، وهي إشكالية أوجدها البروتوكول النموذجي الإضافي أو الوثيقة رقم (INFCIRC /540) والذي يمنح لمفتش الوكالة حق إبلاغ الوكالة بنتائج التفتيش عبر وسائل الاتصالات الحديثة الأمر الذي يمكنه من إرسال المعلومات إلى طرف ثالث في غضون ثوان قليلة الأمر الذي يحول دون اكتشاف الإفشاء أو القدرة على إثباته، هذا دون الحديث عن إمكانية الاختراق والتجسس عن بعد من قبل أطراف أخرى، وهذا رغم نص ذات البروتوكول على ضرورة مراعاة الحاجة لحماية الممتلكات أو المعلومات الحساسة عند توصيل وإرسال المعلومات بالطرق الحديثة[1].

الفـــرع الرابـــع: جهـود مكافحـة التجـسس الإلكتروني في إطار اتفاقيـة فيينـــا للعلاقـات الدبلوماسيـة.

يُعد إستقبال الدولة لممثلين عن دول أخرى وخصهم بمركز قانوني متميز تخرج أحكامه عن ما هو مقرر لبقية الأشخاص من حيث منحهم حصانات شاملة لهم ولمقرهم ولمراسلاتهم، أهم أوجه التعاون

[1]– المادة 14 من الوثيقة رقم INFCIRC /540.

بين الدول وأكثر مظاهر توطيد العلاقات بينها، لكن قد يستغل الممثلون الدبلوماسيون هذه الحصانات كغطاء لممارسة التجسس تحديداً؛ فأصبح العمل الدبلوماسي مرتبطاً تقليدياً بالجوسسة، وفي ظل عدم تمكن الدولة المضيفة غالباً من متابعة هؤلاء الدبلوماسيين أو إنزال العقاب بهم في إطار قضائها الخاص، فقد أوجدت – بالمقابل– اتفاقية فيينا للعلاقات الدبلوماسية بعض الوسائل لمواجهة التصرفات غير الشرعية للمبعوثين الدبلوماسيين وهي الوسائل التي تتجه الدول لإعمالها بغية تحقيق التوازن بين مقتضيات حماية أمن الدولة ومكافحة التجسس وبين الحصانة الدبلوماسية؛ وعليه يتم بداية تناول عنصر حدود العلاقة بين العمل الدبلوماسي والتجسس الإلكتروني، ثم عرض وسائل تحقيق التوازن بين مقتضيات مكافحة التجسس الإلكتروني والحصانة الدبلوماسية.

أولاً– حـدود العلاقـة بيـن العمـل الدبلوماسـي والتجـسس الإلكترونـي:

لقد جرت العادة على أن من بين مهام الممثلين الدبلوماسيين العمل على تزويد دولهم بتقارير دقيقة وموثوق فيها عن الدول الموفدين إليها؛ إذ ليس هناك في التشريعات الداخلية ولا في الأعراف الدولية ما يبيح سؤال الممثل الدبلوماسي الذي يراقب ما يجري في البلاد التي يعمل بها ثم ينقل إلى حكومة بلاده نتائج ملاحظاته مهما تكن هذه الملاحظات ومهما تنطوي عليه من أسرار تتصل بتلك الدولة وهذا ما أقره القانون الدولي كذلك[1]، بحيث أكدت اتفاقية فيينا للعلاقات الدبلوماسية على أن من أهم وظائف البعثة الدبلوماسية استطلاع الأحوال والتطورات في الدولة المعتمد لديها بجميع الوسائل المشروعة وتقديم التقارير اللازمة عنها إلى حكومة الدولة المعتمدة[2]، غير أن هذا النص يثير إشكالاً يتعلق بحدود استطلاع الأحوال والتطورات في الدولة المضيفة وتقديم التقارير عنها والتمييز بين الوسائل المشروعة والوسائل غير المشروعة، وهذا ما أكدته محكمة العدل الدولية حينما اعترفت بوجود صعوبة في إثبات وقوع تعسف في كل حالة أو تحديده حتى يمكن اعتبار استطلاع الأحول والتطورات في الدولة المضيفة وتقديم التقارير عنها تجسساً أو تدخلاً في شؤونها الداخلية[3]، لكن يبقى وضع الحدود الفاصلة بين

---

[1]– أحمد محمد الرفاعي، مرجع سابق، ص. 124.

[2]– المادة الثانية من اتفاقية فيينا للعلاقات الدبلوماسية المحررة في فيينا في 18 أفريل من سنة 1961، والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 64/ 74 المؤرخ في 2 مارس من سنة 1964.

[3]– رؤوف بوسعدية ومنى غبولي، مواجهة المشرع الجزائري لأفعال التجسس الصادرة عن أفراد البعثات الدبلوماسية، مداخلة مقدمة في إطار الملتقى الوطني حول الجرائم الماسة بأمن الدولة، معهد العلوم القانونية والإدارية، المركز الجامعي عباس لغرور، خنشلة، 12– 13 ديسمبر سنة 2011.

الحصول على المعلومات كعمل مصرح به وبين التجسس على أسرار الدولة الموفد إليها مسألة رهينة بالحذق والحصافة الدبلوماسية[1]، إذ أن الممثل الدبلوماسي يجب أن يتحلى بالقواعد الخلقية الحسنة خلال قيامه بواجبه، وهذا ما يسمى الخُلق الدولي، والدبلوماسي الذي يحرض على التجسس أو يقدم الرشوة للموظفين أو يبتاع الأسرار المتصلة بسلامة الدولة التي يمثل بلاده لديها بالنقود أو الوعود يخرق حرمة الخلق الدولي ويقترف جرماً صريحاً[2] هو التجسس.

لكن رغم ما سبق قوله يشهد الواقع العملي على الارتباط التقليدي الموجود بين العمل الدبلوماسي والتجسس، من خلال استخدام أجهزة المخابرات لسفارات دولها في الخارج كغطاء دبلوماسي لبعض ضباطها، والذي أصبح عرفاً مستقراً في العلاقات الدولية[3]، والأمر الذي يساعد على هذا: الوضع القانوني الخاص المعترف به سواء للمبعوثين الدبلوماسيين أو لمقر البعثة الدبلوماسية أو للمراسلات الدبلوماسية، والمترجم بالحصانة الدبلوماسية، إذ يقصد بحصانة المبعوث الدبلوماسي حرمته ضد سريان القانون الوطني في مواجهته وتعطيل اختصاص المحاكم الوطنية في ممارسة ولايتها القضائية، فلا يمكن القبض عليه والقيام بإجراء التحقيق معه أو حبسه حبساً احتياطياً أو إحالته أمام المحاكم الوطنية بسبب جريمة ارتكبها[4]، وقد قررت اتفاقية فيينا هذا الحق ونصت على تمتع المبعوث الدبلوماسي بالحصانة القضائية فيما يتعلق بالقضاء الجنائي للدولة المعتمد لديها[5]، ويلاحظ من خلال هذا النص عدم جواز إخضاع المبعوث الدبلوماسي لقضاء الدولة المضيفة مهما بلغت شدة الجرم؛ إذ جاء النص مطلقًا ولم يُشر إلى استثناءات لنطاق تطبيقه، وهو ذات التوجه الذي أخذ به أغلب الفقهاء أيضاً؛ إذ اتفقوا على منح المبعوث الدبلوماسي حصانة مطلقة حيال الجزاء عن جميع الأفعال الصادرة عنه داخل إقليم الدولة المستقبلة مهما بلغت جسامتها، فيستوي أن يكون الجرم المرتكب من قبله خطِراً أو غير ذلك، كما يستوي أن يكون متلبساً به أو لا، أو أن يكون مُرتكباً بإيعاز من دولته، وسواء كان الجرم جناية أو جنحة أو مخالفة ارتكبها بصفته الرسمية أو الخاصة، ويُكتفى في حالة ارتكاب جريمة ضد أمن الدولة باتخاذ بعض التدابير منها

---

[1]– عاطف فهد المغاريز، مرجع سابق، ص. 153.

[2]– أحمد محمد الرفاعي، مرجع سابق، ص. 125.

[3]– محمد عدنان عثمان، مرجع سابق، ص. 71.

[4]– شادية رحاب، الحصانة القضائية الجزائية للمبعوث الدبلوماسي، أطروحة دكتوراه في العلوم القانونية، مقدمة لقسم العلوم القانونية بكلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2006، ص. 13.

[5]– الفقرة أ من المدة 31 من اتفاقية فيينا للعلاقات الدبلوماسية.

استدعاء المبعوث أو طرده أو إبعاده عن إقليم الدولة المعتمد لديها[1]؛ والعلة في تقرير هذه الحصانة كون المبعوثين الدبلوماسيين يمثلون دولاً ذات سيادة، بالإضافة إلى أن كفالة الحرية والاستقلال المتطلبين لأدائهم أعمالهم تقتضي إقرار هذه الحصانة، فلا يُتصور إمكان ضمان استقلال المبعوث تجاه الدولة المعتمد لديها إذا كان خاضعاً في أعماله أو تصرفاته لاختصاصها القضائي، إذ يكون عندئذ عرضة لأن تُتخذ قِبله كافة الإجراءات القضائية التي تُتخذ قِبل عموم الأفراد؛ مما قد يؤدي إلى المساس باستقلاله والإخلال بطمأنينته وعرقلة المهام التي يضطلع بها[2]. أما على مستوى الممارسة الدولية فيلاحظ خروج الدول في بعض الأحيان عن قاعدة الحصانة الجزائية المطلقة للمبعوثين الدبلوماسيين عند ارتكاب جرائم التجسس بالنظر إلى بلوغ هذه الجرائم حداً من الكثرة أثارت سُخط بعض الدول التي وجدت نفسها مضطرة لأن تمارس اختصاصها القضائي فعلياً حيال بعض الدبلوماسيين المعتمدين لديها قناعة منها بعدم جدوى الطرد، ومثاله ممارسة المحاكم السويسرية اختصاصها الجنائي حيال المستشار الاقتصادي الأول في السفارة الفرنسية بسويسرا سنة 1959 بعد اتهامه بالتجسس، وحكمت عليه بالحبس لمدة 18 شهراً والإبعاد من سويسرا لمدة 15 عاما، وكذلك ما حدث في سنة 1970 حيث تم القبض على موظفة بالسفارة الفرنسية بتشيكوسلوفاكيا سابقاً بتهمة التجسس وحكم عليها بالسجن لمدة عشر سنوات ثم أفرج عنها وطردت من البلاد سنة 1972[3].

ومن جهة ثانية تتطلب طبيعة المهام المتصلة بالتمثيل الدبلوماسي وتعدد الأعمال المتفرعة عنها، أن يكون لكل بعثة دبلوماسية مقر خاص بها في إقليم الدولة المعتمدة لديها تمارس فيه مهامها وتحتفظ فيه بالوثائق الخاصة بها وتتخذ منه مركزاً لها في علاقاتها بحكومة الدولة الموفدة لديها، والقاعدة العامة في القانون الدولي أن دور البعثات الدبلوماسية تتمتع بحصانة تامة ومطلقة ضماناً لاستقلال المبعوثين من ناحية، واحتراماً لسيادة الدولة التي يمثلها كل منهم من ناحية أخرى[4]، وقد أكدت اتفاقية فيينا للعلاقات الدبلوماسية هذه القاعدة ونصت على أن تكون حرمة دار البعثة مصونة، ولا يجوز لمأموري الدولة المعتمد لديها دخولها إلا برضاء رئيس البعثة، وبأنه يترتب على الدولة المعتمد لديها التزام خاص باتخاذ جميع التدابير المناسبة لحماية دار البعثة من أي اقتحام أو ضرر ومنع أي إخلال بأمن البعثة أو

[1]– شادية رحاب، مرجع سابق، ص. 109.

[2]– رفعت رشوان، مرجع سابق، ص. 26.

[3]– شادية رحاب، مرجع سابق، ص. ص. 169– 171.

[4]– رفعت رشوان، مرجع سابق، ص. 47.

مساس بكرامتها، وبأن تعفى دار البعثة وأثاثها وأموالها الأخرى الموجودة فيها ووسائل النقل التابعة لها من إجراءات التفتيش أو الاستيلاء أو الحجز أو التنفيذ[1]، ومن أبرز الأمثلة حالياً على حصانة مقر البعثة الدبلوماسية قضية "ويكيليكس"، إذ لا يزال مؤسس هذا الموقع والمطلوب من طرف الولايات المتحدة الأمريكية بتهمة نشر وثائق سرية محتميا بسفارة الإكوادور في لندن منذ جوان من سنة 2012، والتي منحته اللجوء السياسي لكن السلطات البريطانية ترفض السماح له بمغادرة أراضيها وتوعدته بإلقاء القبض عليه في حالة مغادرته لمقر السفارة ، هذا وقد كانت بريطانيا قد هددت بإمكانية مداهمة سفارة الإكوادور للقبض على المطلوب لكن ذلك أثار استنكاراً شديداً من قبل حكومة الإكوادور التي اعتبرت الأمر تهديداً بالإعتداء على سيادتها ومخالفة للقانون الدولي[2]، وبالإضافة إلى الحصانة التي يتمتع بها المبعوث الدبلوماسي ومقر البعثة الدبلوماسية، تحضى أيضا اتصالات ومراسلات المبعوث الدبلوماسي بذات الحصانة، وهذا ما أقرته اتفاقية فيينا للعلاقات الدبلوماسية بنصها على أن تجيز وأن تصون الدولة

---

[1]– المادة 22 من اتفاقية فيينا للعلاقات الدبلوماسية.

[2]– جوليان أسانج مبرمج أسترالي وصحفي وناشط في الأنترنت، أسس موقع ويكيليكس سنة 2006 والذي أصبح معروفاً ابتداء من سنة 2010 بسبب نشره لوثائق عسكرية ودبلوماسية سرية أثارت حرجا للولايات المتحدة الأمريكية وللعديد من الدول؛ لذلك تحاول الولايات المتحدة خاصة الحصول على تسليمه لمقاضاته بنشر أسرارها، وقد أدرجته الأنتربول على لائحة أكثر المطلوبين لديها وذلك بناء على إصدار محكمة ستوكهولم الجنائية مذكرة اعتقال دولية بدعوى أنه مشتبه فيه في جرائم تحرش جنسي واغتصاب وليس بسبب اتهامات تتعلق بنشره لأسرار متعلقة بعدة دول؛ وبناء عليه فقد اعتقلته بريطانيا في السابع من ديسمبر سنة 2010 وأمضى حوالي الأسبوع في السجن قبل إطلاق سراحه ووضعه تحت الإقامة الجبرية، وقضى أسانج الشهور التالية في معركة قضائية لرفض تسليمه للسويد؛ لخشيته بأن تقوم هذه الأخيرة بتسليمه إلى الولايات المتحدة الأمريكية، وصرح بأن هناك دوافع سياسية تقف وراء الاتهامات الموجهة إليه وبأنها جزء من حملة التشويه ضده وضد موقعه، لكن حكم القضاء البريطاني بتسليمه إلى السويد في فبراير من سنة 2012 وهو ما أيدته المحكمة العليا لاحقا، وفي 14 جوان/ يونيو من سنة 2012 رفضت المحكمة العليا طلبه لإعادة النظر في الطعن المقدم في القضية وبأن له الحق في الطعن في القرار أمام المحكمة الأوروبية لحقوق الإنسان، لكن أسانج فضل عدم الرجوع إلى المحكمة الأوروبية ولجأ في 19 جوان 2012 إلى سفارة الإكوادور في لندن وطلب اللجوء السياسي؛ لتمنحه إياه بتاريخ 16 أغسطس/ أوت من سنة 2012، لكن بالمقابل صرحت الحكومة البريطانية بأنها لن تسمح له بخروج آمن إلى الإكوادور لأنها ملزمة من الناحية القانونية بتسليمه إلى السويد، وفي سبتمبر من سنة 2014 تقدم أسانج بشكوى إلى الأمم المتحدة فحواها أنه محتجز تعسفياً لأنه لا يمكنه المغادرة دون أن يُعتقل؛ لتصدر اللجنة الأممية قراراً لصالحه في فبراير من سنة 2016 جاء فيه أنه اعتقل تعسفياً وأن له الحق في التحرك بحرية وفي الحصول على تعويض بسبب حرمانه من الحرية، لكن وزارة الخارجية البريطانية صرحت بأن هذا القرار لن يغير شيئاً وبأنها ستعتقل أسانج إذا غادر السفارة التي يمكث بها:
– من هو جوليان أسانج مؤسس ويكيليكس، مقال منشور على الموقع الالكتروني:
http://www.bbc.com/arabic/worldnews/2016/ 160204 ، تمت زيارة الموقع بتاريخ 21 / 08 / 2016.

المعتمد لديها للبعثة حرية الاتصال لجميع الأغراض الرسمية وأن للبعثة عند اتصالها بحكومة الدولة وبعثها وقنصلياتها الأخرى أينما وجدت أن تستخدم جميع الوسائل المناسبة بما في ذلك الرسل الدبلوماسيون والرسائل المرسلة بالرمز أو الشفرة أو استخدام جهاز إرسال لاسلكي[1]، لكن يشترط في الحالة الأخيرة الحصول على إذن من الدولة المعتمد لديها، كما أقرت اتفاقية فيينا الحصانة للحقيبة الدبلوماسية ونصت على عدم جواز فتحها أو حجزها[2]، وتجدر الإشارة هنا إلى أن الحقيبة الدبلوماسية تشير إلى الطرود التي تحتوي على المراسلات الرسمية وكذلك الوثائق والأشياء الموجهة حصراً للاستعمال الرسمي؛ لذا يعتبر في حكمها كل ما يرسل مغلفاً برسم البعثة الدبلوماسية[3]، وكما أقرت اتفاقية فيينا بعدم جواز فتح الحقيبة الدبلوماسية أو حجزها وهذا لصالح الدولة الموفدة، عادت وأقرت من ناحية أخرى عدم جواز احتواء الحقيبة الدبلوماسية إلا الوثائق الدبلوماسية والمواد المعدة للاستعمال الرسمي[4]، وهذا لصالح أمن الدولة المضيفة، وهذا ما يُفهم منه أن لهذه الأخيرة حق فتح هذه الحقيبة إذا كان لديها معلومات مؤكدة على احتواءها لما يمس بأمنها، ومثاله وسائط تخزين إلكترونية تحوي أسرار دفاع وطني متعلقة بالدولة المضيفة.

ثانياً- وسائل تحقيق التوازن بين مقتضيات مكافحة التجسس الإلكتروني والحصانة الدبلوماسية:

إن الحصانات السابق عرضها سواء تعلقت بالمبعوث الدبلوماسي أو تعلقت باتصالاته ومراسلاته أو تعلقت بمقر البعثة الدبلوماسية، كلها ظروف قد تُستغل لارتكاب التجسس الإلكتروني بفاعلية دون أن يكون للدولة في أغلب الأحيان القدرة على إخضاع مرتكبيه لاختصاصها القضائي أو معاقبتهم وفقاً لقانونها الداخلي، لكن تبقى هذه الحصانات كما يذهب إليه الرأي الغالب في الفقه ذات طبيعة إجرائية؛ فهي وإن كانت تحول دون ملاحقة الجاني ومعاقبته أمام محاكم دولة الإقليم فهي لا تبيح الفعل[5]، لذلك يكون أمام الدولة القدرة على الالتجاء إلى مجموعة الإجراءات القانونية التي قررتها اتفاقية فيينا للعلاقات الدبلوماسية لمواجهة جرائم المبعوثين الدبلوماسيين، بحيث تشكل هذه الإجراءات وسائل الدولة لتحقيق

[1]- الفقرة الأولى من المادة 27 من اتفاقية فيينا للعلاقات الدبلوماسية.

[2]- الفقرة الثالثة من المادة 27 من نفس الاتفاقية.

[3]- عاطف فهد المغاريز، مرجع سابق، ص. 99.

[4]- الفقرة الرابعة من المادة 27 من اتفاقية فيينا للعلاقات الدبلوماسية.

[5]- رفعت رشوان ، مرجع سابق ، ص . 28.

التوازن بين مقتضيات مكافحة التجسس الإلكتروني والحصانة الدبلوماسية، ويمكن إجمال هذه الإجراءات في العناصر الآتية:

أ- إعلان أحد المبعوثين الدبلوماسيين شخصاً غير مرغوب فيه:

يُعد هذا الإجراء أهم الإجراءات التي قررتها اتفاقية فيينا للعلاقات الدبلوماسية والتي يمكن للدولة اللجوء إليها لمواجهة جرائم التجسس بصفة عامة التي يقوم بها المبعوث الدبلوماسي، كما يمكن للدولة أن تُعلن المبعوث الدبلوماسي شخصاً غير مرغوبً فيه حتى قبل وصوله إلى إقليمها، إذا رأت بأن هذا الشخص قد يُعرض أمنها الوطني للخطر، وهذا الإعلان لا يلزم الدولة بتسبيبه أو احترام شروط زمنية معينة، إذ تنص اتفاقية فيينا على أنه يجوز للدولة المعتمد لديها في جميع الأوقات ودون بيان أسباب قرارها أن تعلن للدولة المعتمدة أن رئيس البعثة أو أي موظف دبلوماسي فيها شخص غير مرغوب فيه أو أن أي موظف آخر فيها غير مقبول (الموظف هنا لا يتمتع بالحصانة الدبلوماسية كما هو الشأن بالنسبة للمبعوث الدبلوماسي لذا لا يُعلن شخصا غير مرغوب فيه وإنما شخص غير مقبول)، وفي هذه الحالة تقوم الدولة المعتمدة حسب الاقتضاء إما باستدعاء الشخص المعني أو بإنهاء خدمته في البعثة، وتشهد الممارسة الدولية على كون هذا الإجراء أكثر الإجراءات التي تلجأ إليها الدولة لمواجهة جرائم التجسس بصفة عامة، ومن الأمثلة على ذلك قيام بريطانيا بطلب سحب بعض موظفي البعثة الدبلوماسية للإتحاد السوفياتي سنة 1970 لثبوت اتهامهم بالتجسس غير أن الطلب رُفض؛ فقامت الحكومة البريطانية على إثر ذلك بطرد مئة وخمسة (105) من الدبلوماسيين الروس؛ الأمر الذي أدى إلى تأزم العلاقات بين الدولتين لمدة طويلة[1]، وقيام واشنطن في 21 آذار سنة 2001 بإعلان خمسين (50) دبلوماسياً روسياً أشخاصاً غير مرغوب فيهم وقامت بطردهم، فردت موسكو في 23 آذار سنة 2001 بطرد أربعة دبلوماسيين أمريكان بتهمة التجسس[2].

يُعتبر إعلان الشخص غير مرغوب فيه سلاحاً تلجأ إليه كل دولة مضيفة تريد التخلص من كل مبعوث دبلوماسي لا ترغب في بقائه على إقليمها، لكن رغم ذلك لا يُعد إجراءاً فعالاً أو رادعاً للحد من التصرفات غير الشرعية التي يقوم بها المبعوثون الدبلوماسيون على إقليم الدولة المضيفة؛ حيث أنه بالرغم من العدد الهائل للمثلين الدبلوماسيين الذين تم اعتبارهم أشخاصاً غير مرغوب فيهم، إلا أن ذلك لم

[1]- شادية رحاب، مرجع سابق، ص. ص. 169- 170.

[2]- عاطف فهد المغاريز، مرجع سابق، ص. 185.

يوقف التجسس، بل أدى إلى تأزم العلاقات بين الدول، إضافة إلى ذلك فكثيراً ما نجد أن الشخص الغير مرغوب فيه في دولة ما يمكن أن تعينه دولته كسفير لدى دولة أخرى، ما يؤدي إلى استمرار الدبلوماسي في التعسف في استعمال حصانته لأغراض غير شرعية لإدراكه أن أقصى عقوبة سوف يتعرض لها هي الطرد مع عدم خضوعه للقضاء الإقليمي للدولة المضيفة، وحتى في الحالات القليلة التي تخضعه الدولة لمحاكمها فعادة ما ينتهي الأمر بإعادة الإفراج عنه وطرده، كما هو موضح في أمثلة سابقة، كما تظهر عدم فاعلية هذا الإجراء أيضاً في أنه عندما تلجأ الدولة المضيفة إلى إعلان المبعوث الدبلوماسي شخصاً غير مرغوب فيه فإن الدولة المعتمدة تسارع إلى اتخاذ نفس الإجراء استناداً إلى مبدأ المعاملة بالمثل لمواجهة عملية طرد ممثليها؛ وبالتالي يصبح التصرف الذي قامت به الدولة المضيفة غير مجد[1].

ب- تخفيض حجم البعثة الدبلوماسية:

إن ازدياد عدد أفراد البعثة الدبلوماسية قد يؤدي إلى صعوبة مراقبة ما تقوم به من أفعال وصعوبة التحقق من القائم بفعل التجسس بصورة دقيقة؛ لذا استقر الرأي على أنه يحق للدولة المضيفة استناداً إلى مقتضيات أمنها الوطني أن تطالب بتخفيض عدد المبعوثين الدبلوماسيين إلى الحد المعقول وأن ترفض ما يزيد عن هذا الحد[2]، واستخدام الدولة المضيفة لهذا الحق – التخفيض- قد يكون كرد فعل منها يعقب إعلان دبلوماسي أو أكثر من دبلوماسيي الدولة الموفدة كأشخاص غير مرغوب فيهم وطردهم من إقليمها بتهمة التجسس، كما قد يكون دون أن يثبت قيام هؤلاء بأعمال تهدد أمن الدولة المضيفة، وذلك نتيجة مغالاة بعض الدول في عدد الأشخاص الذين تضمهم بعثاتها الدبلوماسية، الأمر الذي يحمل الدولة المضيفة على الشك بقيام هؤلاء بنشاط آخر خارج المهام المُعترف بها، كالقيام بأعمال التجسسية[3] (أي يمكن اعتباره تخفيضاً وقائياً). وقد حددت اتفاقية فيينا للعلاقات الدبلوماسية بعض الأحكام المتعلقة بحجم البعثة، إذ نصت على أن للدولة المعتمد لديها عند عدم اتفاق صريح بشأن عدد أفراد البعثة الاحتفاظ بعدد أفراد البعثة في حدود ما تراه معقولاً وعادياً مع مراعاة الظروف والأحوال السائدة في الدولة المعتمد لديها وحاجات البعثة المعنية، كما يجوز للدولة المعتمد لديها أن ترفض ضمن هذه الحدود قبول أي

[1]- شادية رحاب، مرجع سابق، ص. ص. 224- 225.

[2]- رؤوف بوسعدية ومنى غبولي، مرجع سابق.

[3]- محمد عدنان عثمان، مرجع سابق، ص. ص. 129- 130.

موظفين من فئة معينة[1]، وفي ذات الصدد ولنفس الأغراض نصت اتفاقية فيينا على أن للدولة المعتمد لديها أن تقضي في حالة الملحقين العسكريين أو البحريين أو الجويين موافاتها بأسمائهم مقدماً للموافقة عليها[2]، ومثاله طلب الرئيس الكوبي السابق كاسترو تخفيض عدد موظفي السفارة الأمريكية في كوبا إلى ثلاثين موظفا مبرراً طلبه باحتفاظ الولايات المتحدة الأمريكية بحوالي 300 موظفا يتخفى 80% منهم وراء الحصانة الدبلوماسية للقيام بأعمال تجسس، وكذلك إعلان الكونغرس الأمريكي سنة 1985 من خلال قانون خاص قرر فيه بأن عدد أعضاء البعثة الدبلوماسية التابعة للإتحاد السوفياتي في واشنطن يجب أن يكون مساوياً لعدد أعضاء البعثة الممثلة للولايات المتحدة الأمريكية في موسكو[3].

إن اللجوء إلى إجراء تخفيض البعثة الدبلوماسية قد يؤدي إلى الحد من عمليات التجسس؛ لأنه يمكن الدولة المعتمد لديها من أن تراقب المبعوثين الدبلوماسيين لديها، لكن هذا الإجراء يصطدم ببعض الصعوبات، منها لجوء الدولة المعتمدة إليه تطبيقاً لمبدأ المعاملة بالمثل، كما أن تزايد عدد أفراد البعثات ليس في ذاته السبب في ارتكاب التجسس، وإنما يعود ذلك إلى سلوكهم ومدى انضباطهم واحترامهم لقوانين الدولة المضيفة[4].

ج- تقييد حرية تنقل أعضاء البعثات الدبلوماسية في إقليم الدولة الموفدين إليها:

بالرجوع إلى اتفاقية فيينا نجدها قد أقرت حق التنقل لأفراد البعثات الدبلوماسية، لكنها بالمقابل وضعت قيوداً على هذا الحق، إذ تنص على أن تكفل الدولة المعتمد لديها حرية التنقل والسفر في إقليمها لجميع أفراد البعثة مع عدم الإخلال بقوانينها وأنظمتها المتعلقة بالمناطق المحظورة أو المنظم دخولها لأسباب تتعلق بالأمن القومي[5]؛ وعليه فهذا الإجراء يهدف بالدرجة الأولى إلى المحافظة على الأمن القومي للدولة المضيفة، إذ تقوم هذه الأخيرة بتحديد المجال الذي يستطيع الدبلوماسيون التنقل ضمنه وخارج هذا المجال يجب الحصول على إذن خاص، وقد تتخذ الدول إجراءات أكثر تشدداً ضد حركة

[1]- المادة 11 من اتفاقية فيينا للعلاقات الدبلوماسية.

[2]- المادة السابعة من نفس الاتفاقية.

[3]- عاطف فهد المغاريز، مرجع سابق، ص. 190.

[4]- رؤوف بوسعدية ومنى غبولي، مرجع سابق.

[5]- المادة 26 من اتفاقية فيينا للعلاقات الدبلوماسية.

المبعوثين، حيث قد يصل الأمر حد منعهم من الخروج من مقراتهم الدبلوماسية وهو ما حصل في حالة تأزم العلاقات الفرنسية الإيرانية سنة 1987[1].

د- قطع العلاقات الدبلوماسية:

يُعد قطع العلاقات الدبلوماسية أخطر مظاهر سوء العلاقات الدبلوماسية بين دولتين، ولا يتم اتخاذ مثل هذا القرار إلا إذا رأت الدولة الموفد إليها أن مصالحها قد تضررت وأن هناك داعياً جدياً لقطع العلاقات، ويُعرف القطع بأنه تعبير إنفرادي عن إرادة دولة ما في وضع حد لوسيلة الاتصال العادية بينها وبين دولة أخرى وذلك باستدعاء البعثة الدبلوماسية المعتمدة لدى كل منهما، ويُعد مظهراً من مظاهر حرص الدولة على أمنها[2]، ولم تخصص اتفاقية فيينا مادة مستقلة للحديث عن هذا الإجراء لكن يمكن القول أن هذا الإجراء يجد سنده القانوني في المادة الثانية من اتفاقية فيينا التي تنص على أن تقام العلاقات الدبلوماسية وتنشأ البعثات الدبلوماسية الدائمة بالرضا المتبادل؛ وعليه يفهم أن للدولة حق إنهاء هذه العلاقات متى ارتأت ضرورة ذلك، كما اكتفت اتفاقية فيينا في هذا الإطار بتحديد الآثار المترتبة على قطع العلاقات الدبلوماسية فقط[3].

وعلى صعيد الممارسة الدولية نجد أن الدول نادراً ما تلجأ إليه؛ وذلك حرصاً على استقرار الصلات الودية بينها، وما يؤكد ذلك عدم لجوء كل من الولايات المتحدة الأمريكية وروسيا إليه رغم كثرة حالات التجسس بينهما[4].

---

[1]- رؤوف بوسعدية ومنى غبولي، مرجع سابق.

[2]- عاطف فهد المغاريز، مرجع سابق، ص. 197.

[3]- تنص المادة 45 من اتفاقية فيينا للعلاقات الدبلوماسية على أنه: "تراعى في حالة قطع العلاقات الدبلوماسية بين دولتين أو الاستدعاء المؤقت أو الدائم لإحدى البعثات الأحكام التالية:

أ- يجب على الدولة المعتمد لديها حتى في حالة وجود نزاع مسلح احترام وحماية دار البعثة وكذلك أموالها ومحفوظاتها.

ب- يجوز للدولة المعتمدة أن تعهد بحراسة دار البعثة وكذلك أموالها ومحفوظاتها إلى دولة ثالثة تقبل بها الدولة المعتمد لديها.

ج- يجوز للدولة المعتمدة أن تعهد بحماية مصالحها ومصالح مواطنيها إلى دولة ثالثة تقبل بها الدولة المعتمد لديها".

[4]- رؤوف بوسعدية ومنى غبولي، مرجع سابق.

هـ- مساءلة المبعوث الدبلوماسي:

أقرت اتفاقية فيينا طريقتين لمساءلة المبعوث الدبلوماسي عن الجرائم التي يرتكبها إضراراً بالدولة المضيفة: تتمثل الطريقة الأولى في رفع الحصانة القضائية عنه لتتمكن الدولة المضيفة من متابعته أمام محاكمها، بحيث نصت ذات الاتفاقية على أنه يجوز للدولة المعتمدة أن تتنازل عن الحصانة القضائية التي يتمتع بها المبعوثون الدبلوماسيون[1]، وتتمثل الطريقة الثانية في قيام الدولة المضيفة باللجوء إلى الدولة التي يمثلها المبعوث الدبلوماسي لمقاضاته أمام محاكمها بالاستناد إلى نص اتفاقية فيينا، على أن تمتع المبعوث الدبلوماسي بالحصانة القضائية في الدولة المعتمد لديها لا يعفيه من قضاء الدولة المعتمدة[2]، إلا أنه لا توجد أية سابقة تشير إلى قيام الدولة برفع الحصانة عن ممثلها الدبلوماسي لتحاكمه الدولة المضيفة، ولا قيامها هي بمحاكمته عن أفعال التجسس التي يقوم بها؛ إذ أنه عادة ما يقوم المبعوث الدبلوماسي بنقل أسرار الدولة المضيفة تطبيقاً لإملاءات دولته فلا يتصور أن تقوم بمحاكمته أو أن تمنح ذلك الحق لغيرها.

[1]- الفقرة الأولى من المادة 32 من اتفاقية فيينا للعلاقات الدبلوماسية.

[2]- الفقرة الرابعة من المادة 31 من نفس الاتفاقية.

خلاصـــة البـــاب الثانـــي

تمثل حماية أمن الدولة بصفة عامة، أولوية بالنسبة للمشرع في كل دول العالم؛ وذلك لكونه يشكل جوهر وجود واستمرارية هذه الدول، ويعبر عن مدى قوتها وتأثيرها في مواجهة غيرها؛ لذا تعمل ذات الدول على صعيد قانونها الداخلي على إقرار مجموعة من الأحكام الاستثنائية سواء الموضوعية أو الإجرائية منها لمكافحة كل ما يمس بهذا الأمن من جرائم، وتحاول من خلال التعاون الإقليمي أو الدولي أن توحد جهود التصدي لها وتضمن من وراء ذلك فعالية قواعد قانونها الوطني، ومن خلال ما تم تفصيله في هذا الباب يمكن تلخيص وإجمال الجهود المرصودة لمكافحة التجسس الإلكتروني فيما يلي:

1- على المستـوى الوطنـي: أقر المشرع الجزائري من خلال عديد القوانين حماية الدفاع الوطني بصفة عامة ومن وراءه مكافحة التجسس الإلكتروني بصفة خاصة؛ ويظهر هذا من مجموعة القواعد الموضوعية والقواعد الإجرائية المرصودة لذلك. فمن الناحية الموضوعية يلاحظ توزع أحكام تجريم وعقاب التجسس الإلكتروني بين النصوص التقليدية التي تحكم التجسس التقليدي وبين النصوص المستحدثة التي تحكم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وبالرجوع إلى النصوص التقليدية يلاحظ أن عديدها جاء بصياغة عامة ومرنة تحدد القواعد العامة التي تحكم جرائم التجسس دون تخصيص، مع ذكر وسائل هذه الجرائم على سبيل المثال وترك المجال مفتوحاً لضم ما يُستحدث منها؛ فيدخل التجسس الإلكتروني بذلك في مجال تطبيقها، ومن حيث العقوبات أقر المشرع الجزائري أقصاها لمرتكب جرائم التجسس بحيث حدد الإعدام كجزاء لها، وأفرد قسماً خاصاً يتضمن إقرار المسؤولية الجنائية للشخص المعنوي عن جرائم التجسس وأحكام الإشتراك والإعفاء والتخفيض للعقوبات، ولم يُحِلْ في ذلك على القواعد العامة، مما يدل على العناية الخاصة التي أولاها المشرع لهذه الطائفة من الجرائم، أما بالرجوع إلى النصوص المستحدثة المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؛ فقد نص المشرع الجزائري على حالة استهداف هذه الجرائم للدفاع الوطني، فتُشكل بذلك هذه الجرائم تجسساً إلكترونياً إذا مست بأسرار الدفاع الوطني والتي تأخذ في هذه الحالة شكل معطيات إلكترونية، أما فيما يخص العقوبات فلم يكتف المشرع بالعقوبات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بصفة عامة، وإنما نص على الإحالة على تطبيق عقوبات أشد؛ وهو ما طرح إشكالية كيفية تقرير العقوبات. أما من الناحية الإجرائية فقد قرر المشرع الجزائري إخضاع الجرائم الإلكترونية ومنها تلك الماسة بأمن الدولة لمجموعة قواعد استثنائية تم النص عليها في قانون الإجراءات الجزائية وفي القانون

رقم 09-04 المتضمن تحديد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ليساير بذلك الوارد في الاتفاقيات الدولية لمكافحة الجرائم الإلكترونية.

2- على المستوى الإقليمي: تظهر جهود مكافحة التجسس الإلكتروني على الصعيد الإقليمي من خلال عمل المنظمات وكذلك من خلال أحكام الاتفاقيات الإقليمية. فمن جانب عمل المنظمات الإقليمية نلحظ على المستوى العربي توفر منظمة جامعة الدول العربية على مجموعة قواعد يمكن الاستناد إليها للتصدي للتجسس الإلكتروني بإعتباره أحد الأخطار التي تهدد الأمن القومي العربي، هذه القواعد التي تضمنها تحديداً ميثاق الجامعة وكذلك معاهدة الدفاع المشترك تبقى رغم ذلك بعيدة عن التطبيق والتفعيل، بعكس ما هو ملاحظ على المستوى الأوروبي وتحديداً من خلال عمل الإتحاد الأوروبي؛ إذ تظهر جلية الجهود العملية لتدعيم الأمن المعلوماتي وبناء تعاون إقليمي لمواجهة ممارسات التجسس الإلكتروني رغم العوائق المواجهة في هذا الصدد، أو من خلال عمل حلف الناتو الذي يشكل المظلة الأمنية للقارة الأوروبية والذي نجح إلى حد ما في تفعيل نصوص الدفاع المشترك لمواجهة الهجمات الإلكترونية ومنها التجسس. أما من جانب الاتفاقيات الإقليمية فيمكن القول أن الدول العربية تمتلك إطاراً قانونياً متميزاً لمواجهة التجسس الإلكتروني تحديداً الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي تناولت صراحةً جريمة الدخول غير المشروع لمنظومة معلوماتية بغرض الحصول على معلومات حكومية سرية، وأقرت حق الدول في مد اختصاصها القضائي في حالة المساس بأمنها وبمصالحها العليا، بعكس الاتفاقية الأوروبية حول الإجرام المعلوماتي التي خلت من مثل هذين الحكمين المهمين واكتفت بالنص على الجرائم الإلكترونية بصفة عامة وبدون تخصيص.

3- على المستوى الدولي: المتفحص لعمل المنظمات الدولية وعلى رأسها هيئة الأمم المتحدة ومنظماتها المتخصصة؛ يجدها تركز جهودها لمكافحة الجرائم الإلكترونية عموماً ومنها التجسس الإلكتروني على تدعيم الأمن المعلوماتي لمنع المجرمين من التوصل إلى المنظومات المعلوماتية الحساسة، ليشكل عمل الوكالة الدولية للطاقة الذرية في هذا الإطار حالة خاصة بتقريرها ضرورة حماية أسرار الدفاع الوطني النووية صراحةً. أما من ناحية الاتفاقيات الدولية وكما هو الشأن على الصعيد الإقليمي لا توجد اتفاقية دولية مخصصة تحديداً لتنظيم أحكام التجسس، ولكن يمكن استخلاص ذات الأحكام بالرجوع إلى عديد الاتفاقيات الأخرى، ومنها اتفاقيات القانون الدولي الإنساني، واتفاقيات الفضاء الخارجي، والاتفاقيات المنظمة لاستخدام الطاقة النووية، والاتفاقيات المنظمة للعمل الدبلوماسي، ورغم

معالجة هذه الاتفاقيات لمسألة التجسس بصفة مباشرة إلا أن القواعد المقررة فيها لا يمكن الاستناد عليها لمكافحة التجسس الإلكتروني بالنظر خاصة لعدم فعالية الإجراءات المقررة فيها.

الخـــــاتمـــــــة

الخاتمـــــــــة:

تُشكل حماية البنية الإلكترونية الحساسة أهم تحديات الدول في عصرنا الحالي؛ أين أصبح الاعتماد شبه المطلق والتبعية لتكنولوجيات الإعلام والاتصال الميزة الغالبة في أسلوب إدارتها وتسييرها لكافة نشاطاتها وشؤونها باختلاف مظاهرها، الأمر الذي سهل في المقابل إمكانية وصول الغير إلى ما يعتبر بالنسبة إليها أسرار دفاع وطني وباستغلال ذات الوسائل والتكنولوجيات؛ وعليه فقد سعت هذه الدول ومن خلال بناء أُطر حماية تتماشى مع أشكال التهديدات المستحدثة التي تتخذ من الفضاء الإلكتروني بيئة النشاط ومنطلق وهدف الهجمات، إلى مكافحة هذه التهديدات وفي مقدمتها التجسس الإلكتروني، وبعد تخصيص هذه الدراسة لتحليل هذا الأخير ورصد آليات مكافحته؛ تم التوصل إلى جملة من النتائج، وتقرير بعض التوصيات تُعرض في الآتي:

أولاً- نتائـــج الدراســـــة: يمكن إجمال نتائج الدراسة في النقاط الآتية:

1- إذا كان التجسس التقليدي يُعرف بأنه كل نشاط يقوم به أجنبي يكون من شأنه إنتهاك أو خرق قواعد المحافظة التي تحيط بالأسرار المتعلقة بالدفاع الوطني، فإن التجسس الإلكتروني هو كل سلوك يرتكبه أجنبي، ويستهدف أنظمة المعالجة الآلية للمعطيات أو يستخدمها كوسيلة، ومن شأنه المساس بسر من أسرار الدفاع الوطني التي تتجسد في شكل معلومات إلكترونية، بغض النظر عن طبيعة مرتكبه والجهة المستفيدة منه سواء كانت دولة أو مؤسسة أو جماعة إجرامية أو فرداً؛ وعليه فكلا المفهومين يشتركان في صفة الفاعل الذي يجب أن يكون أجنبياً، وفي المحل الذي يقع عليه التجسس وهو أسرار الدفاع الوطني، لكنهما يتمايزان أولاً من حيث الوسيلة والهدف؛ إذ يجب إستخدام أنظمة المعالجة الآلية للمعطيات كوسيلة في التجسس الإلكتروني أو جعلها هدفاً له، وثانياً من حيث شكل أسرار الدفاع الوطني المستهدفة؛ والتي تأخذ شكل معلومات إلكترونية في الأصل أو يتم تحويلها إلى هذا الشكل عن طريق استخدام نظام معالجة آلية للمعطيات في نقلها أو تخزينها أو إعادة استرجاعها، وثالثاً من حيث مرتكبيه والجهات المستفيدة منه؛ بحيث لم تعد الدولة أو الفرد – لحساب الدولة – لا الممارس ولا الطرف الأوحد المستفيد منه، بل أضحى الأفراد كما المؤسسات الاقتصادية بالدرجة الأولى كما جماعات الجريمة المنظمة أو الجماعات الإرهابية تمثل الجهات الجديدة الفاعلة والمستفيدة منه شأنها في ذلك شأن الدول.

2- يُعد التجسس الإلكتروني امتداداً للتجسس بصفة عامة وآخر محطات تطوره التاريخي حالياً، لذا ورغم تميز الصورة التقليدية له عن المستحدثة منه فلا يمكن الفصل التام بينهما، وهذا ما يظهر من خلال مجموعة الخصائص التي يتسم بها التجسس الإلكتروني؛ بحيث منها ما يجمعه بالصورة التقليدية للتجسس ومنها ما يرسم ذاتيته واستقلاله عنها، فمن ناحية يُعتبر كما التجسس التقليدي جريمة من جرائم أمن الدولة الخارجي المشروط ارتكابها من طرف شخص أجنبي، ومن ناحية ثانية ينفرد بكونه نتاج التطور الحاصل على مستوى تكنولوجيات المعلومات والاتصالات والانتقال إلى العصر الإلكتروني الأمر الذي جعل التجسس في ظله يصبح جريمة إلكترونية يتصف بصفاتها، وفي مقدمة هاته الصفات ارتكابها من قبل طائفة مميزة من المجرمين إصطلح على تسميتها بالمجرمين الإلكترونيين؛ وعليه وفي مقابل ارتكاب التجسس التقليدي من قِبل الجاسوس التقليدي أصبح إرتكاب التجسس الإلكتروني رهناً على وجود طائفة جديدة من الجواسيس هم الجواسيس الإلكترونيون العارفون بكيفيات إستغلال التكنولوجيات الحديثة للمساس بأسرار الدفاع الوطني لمختلف الدول، كما يتصف التجسس الإلكتروني تحديداً بكونه أهم تقنيات الحرب الإلكترونية سواء في نمطها الدفاعي أو الهجومي، بالإضافة إلى إعتباره أحد الأساليب التي يعتمدها الإرهاب الإلكتروني من خلال إستخدام نظم المعلومات لتجميع الإستخبارات لغرض إستغلالها في الهجمات الإلكترونية أو المتاجرة بها.

3- تتعدد صور التجسس الإلكتروني إن بالنظر إلى موضوعه أي إلى طبيعة المعلومة المستهدفة به، أو بالنظر إلى الوسيلة المعتمدة لممارسته، فمن الزاوية الأولى يأخذ التجسس الإلكتروني ذات صور التجسس التقليدي المعروفة فينقسم إلى تجسس عسكري وتجسس سياسي وتجسس دبلوماسي وتجسس اقتصادي، مع ملاحظة بروز هذا الأخير حالياً بعدما كان التجسس على المعلومة العسكرية يحتل صدارة أولويات الدول سابقاً، أما من الزاوية الثانية فنلحظ أن ما يميز التجسس الإلكتروني عن التقليدي هو وسيلة ممارسته، وفي هذا الشأن نميز بين ثلاثة أنماط منه: التجسس عن طريق الحواسيب والأنترنت، والتجسس عن طريق الهواتف، والتجسس عن طريق الأقمار الصناعية، مع ملاحظة أنه إذا كان بالإمكان التصدي للتجسس عن طريق الحواسيب أو الهواتف فإن الأمر يصبح أكثر صعوبة بالنسبة لذلك الممارس عبر الأقمار الصناعية لارتباط ذلك بضرورة توفر قدرات علمية وتجهيزات تكنولوجية ليست في متناول أغلب الدول.

4- يعتبر التجسس الإلكتروني أحد أكثر المواضيع القانونية جدلاً وغموضاً؛ لأنه يجمع بين الشيء ونقيضه، فالدولة الواحدة تنظر إليه كتصرف مشروع وغير مشروع في ذات الحين، مشروع إن كانت هي القائم به وغير مشروع إن كانت هي ضحيته، وفي هذا الإطار تبرر لجوءها إليه بسعيها إلى حفظ أمنها وتبرر مكافحتها له أيضا بسعيها إلى حفظ أمنها، وحتى في هذه الحالة الأخيرة يُعد التجسس أهم أساليب مكافحة التجسس وبالنتيجة أهم أدوات حفظ أمن الدولة؛ وعليه ورصداً لأسباب التجسس الإلكتروني يحتل حفظ أمن الدولة والتصدي لكل التهديدات المحتملة له خاصة في عصرنا الحالي صدارة هذه الأسباب، ومن بين هذه التهديدات تلك التي يشكلها الإرهاب، واللجوء كما الاعتماد المتزايد على تقنيات الحرب المعلوماتية، زيادة على رغبة الدول في مراقبة السباق التكنولوجي والعلمي في مجال التسلح. وبالإضافة إلى حفظ أمن الدولة هناك عديد الأسباب التي أسهمت في بروز نمط التجسس الإلكتروني، منها أساساً الثورة التكنولوجية والتحول إلى الفضاء الإلكتروني، وبروز فواعل دولية جديدة تسعى للحصول على المعلومات الحساسة نظراً لقيمتها المالية الكبيرة والطلب المستمر والمتزايد عليها. وفي مقابل تعدد أسباب اللجوء إلى التجسس الإلكتروني فقد كانت له آثاره الملحوظة إن على الدولة من خلال مساسه بسيادتها، أو على الأفراد من خلال مساسه بحقهم في الحياة الخاصة.

5- تشكل أسرار الدفاع الوطني للدولة المحل الذي ينصب عليه التجسس بصفة عامة والموضوع الذي تهدف الدولة إلى حمايته، وهو لا يختلف من حيث الجوهر باختلاف صور التجسس إذ يبقى دالاً على ذات المحتوى، كما لا يختلف من حيث الأنواع إذ ينقسم إلى أسرار حقيقية وأسرار مفترضة وأسرار ذات طبيعة خاصة، لكن ما يميز سر الدفاع الوطني كمحل للتجسس الإلكتروني هو الوعاء المحتوي له والشكل الذي يظهر عليه؛ بحيث يأخذ في هذه الحالة شكل معلومات إلكترونية مخزنة في أنظمة معالجة آلية للمعطيات فيصبح بذلك سراً إلكترونياً غير ملموس بخلاف الصورة المادية الملموسة التي يوجد عليها سر الدفاع الوطني التقليدي عادةً، وفي هذا الإطار يمكن تعريف سر الدفاع الوطني الإلكتروني بأنه كل ما يتصل بمظاهر الدفاع الوطني المختلفة (عسكرية أو اقتصادية أو سياسية أو دبلوماسية أو اجتماعية) والذي يعتمد في معالجته (تخزيناً واسترجاعاً وتعديلاً ونقلاً) على أنظمة المعالجة الآلية للمعطيات، ويستوجب إبقاءه مكتوماً لمصلحة أمن الدولة.

6- كان لظهور تكنولوجيات المعلومات والاتصالات وتبني الجزائر لها كغيرها من دول العالم أثره البارز على تطور التشريع الجزائي في شقيه الموضوعي والإجرائي، سواء كان ذلك من خلال إضافة

مواد جديدة في صلب القوانين الموجودة، وهو أساساً حال التعديل الذي عرفه قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في العاشر نوفمبر من سنة 2004 بتجريم الأفعال التي تشكل مساساً بأنظمة المعالجة الآلية للمعطيات، ونصه صراحةً على مضاعفة العقوبات المنصوص عليها بشأنها إذا إستهدفت الجريمة الدفاع الوطني وذلك دون الإخلال بتطبيق عقوبات أشد؛ وحال التعديل الذي عرفه قانون الإجراءات الجزائية بإدخال إضافات جوهرية تجلت خاصةً من خلال إجراءات التحري والتحقيق في هذه الطائفة من الجرائم، والتي جاء بها القانون رقم 06-22 المؤرخ في العشرين ديسمبر من سنة 2006، وكذلك من خلال تعديل مفهوم وشروط إعمال مبدأ العينية المنصوص عليه في تعديل قانون الإجراءات الجزائية الذي كان بموجب الأمر رقم 15-02 المؤرخ في 23 يوليو من سنة 2015؛ أو سواء كان ذلك من خلال إستحداث قوانين جديدة مخصصة تحديداً لمكافحة الجريمة الإلكترونية بمختلف صورها، وأبرزها إطلاقاً القانون رقم 09-04 المؤرخ في الخامس أوت من سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والذي نص على الإجراءات الحديثة في مجال التحري والتحقيق في الجريمة الإلكترونية، وكذا على مجال إعماله والذي يشمل الجرائم الماسة بأمن الدولة وتلك التي تشكل تهديداً للنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

7- في إطار معالجة المشرع الجزائري للجريمة الإلكترونية بصفة عامة -واعتبار التجسس الإلكتروني أحد صورها- يُلاحظ إستخدامه لمصطلحين متمايزين للدلالة عليها، بحيث عبر عنها حين إستحداثها لأول مرة بموجب تعديل قانون العقوبات رقم 04-15 بمصطلح "الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات" وهو المصطلح الذي يحصر الجريمة الإلكترونية أساساً في مجموع الأفعال التي تستهدف هذه الأنظمة، ليتدارك النقص بمناسبة وضعه للقانون رقم 09-04 بإستخدامه لمصطلح جديد هو "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، وبنصه صراحة في المادة الثانية منه على أن هذه الجرائم تشمل جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهُل ارتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية؛ وعليه تصبح الجريمة الإلكترونية بصفة عامة شاملة لمجموع الأفعال التي يكون فيها نظام المعالجة الآلية وسيلة لارتكاب الجريمة أو هدفاً للجريمة، وفي هذا الإطار نكون أمام تجسس إلكتروني في حالتين: الحالة الأولى تتعلق بالاعتداء على أسرار الدفاع الوطني باستخدام أنظمة المعالجة الآلية للمعطيات، وهنا يندرج تجريم هذا الإعتداء في إطار النصوص التقليدية في قانون العقوبات والتي تحكم التجسس بصفة عامة

لأن هذه النصوص وفي كثير منها قد جاءت بألفاظ مرنة لم تحدد الوسيلة المتطلبة لارتكاب التجسس فنكون في هذه الحالة أمام جريمة تجسس تقليدية باستخدام أنظمة معالجة آلية للمعطيات، أما الحالة الثانية فتتعلق بالاعتداء على أسرار الدفاع الوطني المخزنة في أنظمة المعالجة الآلية للمعطيات، ويندرج تجريم هذا الاعتداء ضمن النصوص المستحدثة في قانون العقوبات والمتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات خاصة وأن المادة 394 مكرر 3 منه تنص صراحة على حالة استهداف الجريمة للدفاع الوطني.

8- تتسم سياسة المشرع الجزائري لمكافحة التجسس الإلكتروني في شقها الموضوعي المتعلق بالتجريم والعقاب بخصوصية بارزة، وهذا من حيث تعدد النصوص القانونية التي يمكن أن تندرج ضمنها نشاطات التجسس الإلكتروني كما سبق تبيانه في العنصر السابق؛ بحيث نجد أن التجسس الإلكتروني الذي يستخدم أنظمة المعالجة الآلية للمعطيات كوسيلة يخضع للنصوص التقليدية التي تحكم التجسس بصفة عامة والمتمثلة في المواد من 61 إلى 63 من قانون العقوبات والمتعلقة تحديداً بجريمة التخابر مع دولة أجنبية، وجريمة تحريض العسكريين أو البحارة على الانضمام إلى دولة أجنبية، وجريمة التجنيد لحساب دولة في حرب مع الجزائر، وجريمة إضعاف الروح المعنوية للجيش أو للأمة، وكل هذه الجرائم يُتصور استخدام التقنيات الإلكترونية لارتكابها خاصة في ظل مرونة صياغة المواد السابقة وعدم حصرها لوسيلة ارتكاب الجرائم المنصوص عليها ضمنها، أما التجسس الإلكتروني الذي يستهدف أنظمة المعالجة الآلية للمعطيات فيخضع في تجريمه للنصوص المستحدثة التي تحكم الجريمة الإلكترونية بصفة عامة والمتمثلة في المواد من 394 مكرر إلى 394 مكرر 2 من قانون العقوبات والمتعلقة بجريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات، وجريمة الإعتداء على المعطيات، وجريمة التعامل غير المشروع في المعطيات، وهذا في حالة استهداف هذه الجرائم للدفاع الوطني كما نصت عليه المادة 394 مكرر 3 من قانون العقوبات.

9- إذا كان تجريم نشاطات التجسس الإلكتروني سواء تلك المندرجة ضمن النصوص التقليدية أو النصوص المستحدثة من قانون العقوبات يطرح بعض الإشكالات المتعلقة إما بمرونة المصطلح والتي تُبرَر عادة بطبيعة الجريمة – جريمة أمن الدولة – وإما بغموض المصطلح التقني، فإن التساؤل يُثار حقيقة بشأن تطبيق العقوبات في حالة جرائم التجسس الإلكتروني الخاضعة للنصوص المستحدثة، إذ ينص المشرع الجزائري في المادة 394 مكرر3 على: "تضاعف العقوبات المنصوص عليها في هذا

القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد"، فالمصطلحات التي استخدمها المشرع هنا من الاتساع والغموض ما يجعل من تحديد العقوبات التي يقصدها أمراً بالغ الصعوبة، فأي معيار يتم إتباعه لتحديد الحالات التي تضاعف فيها العقوبات والحالات التي تُطبق فيها العقوبات الأشد؟ فهذه الأخيرة قد تصل إلى الإعدام بالرجوع إلى النصوص التقليدية التي تحكم التجسس بصفة عامة ما يَفترِض تحديد المقصود بلفظ "الأشد" بصورة دقيقة وصريحة حفاظاً على حقوق الأفراد، كما أن المشرع لم يحدد لنا الأساس أو المعيار الذي انطلاقاً منه نطابق بصورة دقيقة بين جريمة ماسة بأنظمة المعالجة الآلية للمعطيات وأخرى تستهدف الدفاع الوطني للقول بأن عقوبة الثانية مستحقة للأولى.

10- أقر المشرع الجزائري في إطار مكافحته للجريمة الإلكترونية بصفة عامة ومن ضمنها التجسس الإلكتروني أحكاماً إجرائية خاصة تخرج عن تلك المقررة لطوائف الجرائم المعُتبرة عادية، وتبرز هذه الأحكام إبتداءاً فيما نص عليه قانون الإجراءات الجزائية بمناسبة التحري والتحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ونظراً لخصوصية وسائل ومخلفات ارتكاب هذه الجرائم والبيئة الالكترونية التي تتم على مستواها فقد خصها المشرع الجزائري بقانون مستقل تضمن مجموعة إجراءات جد استثنائية تتلائم مع هذه البيئة ولها القدرة على التعامل مع الدليل الإلكتروني الناجم عنها، هو القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والذي نص على الحالات التي يمكن اللجوء فيها لهذه الإجراءات والمتعلقة أساساً بالجرائم الماسة بأمن الدولة وبالدفاع الوطني، وتتمثل في إجراء مراقبة الإتصالات الإلكترونية وإجراء تفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية وإجراء حفظ المعطيات المتعلقة بحركة السير واعتراض المعطيات المتعلقة بالمحتوى، ومنح المشرع من خلال المرسوم الرئاسي رقم 15-261 المؤرخ في الثامن أكتوبر من سنة 2015 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لهذه الهيئة اختصاص وسلطة ضبط سير هذه الإجراءات.

11- باستقراء جهود مكافحة التجسس الإلكتروني على المستوى الإقليمي؛ يتم الوقوف على الوضوح والتحديد النسبي لهذه الجهود مقارنة بما هو موجود على المستوى الدولي؛ ويعود هذا إلى طبيعة العلاقات ووحدة المصالح بين الدول التي تجمعها روابط مشتركة ترتكز في أغلبها على الإقليم، وفي هذا

الإطار وبالرجوع إلى المنظمات الإقليمية نجد مثلاً أن سياسة الإتحاد الأوروبي في هذا الخصوص قد قامت على محورين رئيسيين: الأول نظري يبرز من خلال إتخاذ إجراءات قانونية لمكافحة الإجرام الإلكتروني ولدعم الأمن المعلوماتي بصفة عامة، والثاني عملي من خلال إتخاذ إجراءات عملية لمكافحة التجسس الإلكتروني تحديداً كإطلاق برنامج "كوانتوم" كرد فعل على نظام التجسس الإلكتروني العالمي "إيشلون"، أما فيما يخص مكافحة التجسس الإلكتروني في ظل جامعة الدول العربية ورغم أن ميثاقها ومعاهداتها الملحقة تشكل الإطار القانوني لتحقيق الأمن القومي العربي ولبناء تحالف بين الدول العربية قائم على مبدأ التضامن الدولي المشترك – الذي أخذت به فعلياً معظم الدول العربية في قوانينها العقابية الداخلية لمواجهة الجرائم الماسة بأمن الدولة الخارجي ومنها التجسس– إلا أن الجامعة العربية لم تتمكن من تفعيل هذا المبدأ ليشمل الاعتداءات الإلكترونية التي تتخذ من الفضاء الإلكتروني بيئة للنشاط، وهذا بعكس الحاصل في إطار منظمة حلف شمال الأطلسي؛ بحيث تغير في ظل ميثاقها مفهوم الدفاع المشترك، إذ تجاوز مفهوم العدوان التقليدي ليعتبر بأن الهجومات الإلكترونية بمختلف صورها أحد أنواع الاعتداءات، وفي ظل الصعوبة الراهنة لتطبيق هذا المفهوم الجديد فقد ركز الحلف على بناء سياسة للدفاع الإلكتروني تقوم على تدعيم إجراءات الأمن المعلوماتي وتعزيز التعاون في مجال تبادل المعلومات حول التهديدات الإلكترونية ومراقبة النشاطات الممارسة في الفضاء الإلكتروني، أما فيما يخص الجهود المبذولة لمكافحة التجسس الإلكتروني في إطار الاتفاقيات الإقليمية ورغم عدم وجود اتفاقية خاصة بعنوان هذه المكافحة، إلا أنه وفي ظل الجهود العربية لمكافحة الجريمة الإلكترونية تم النص صراحة على جريمة التجسس الإلكتروني، وهذا ما يظهر سواء من خلال القانون العربي الإسترشادي لمكافحة جرائم تقنية المعلومات –الذي أخذت به عديد الدول العربية حين وضعها لقوانينها الداخلية لمكافحة الجريمة الإلكترونية– أو من خلال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي نصت صراحة على حالة المساس بمنظومة معلوماتية بغرض الحصول على أسرار حكومية أو بيانات ومعلومات تمس الأمن الخارجي للدولة، وتعد الاتفاقية العربية تحديداً إطاراً قانونياً متكاملاً يضم الشق الموضوعي وكذا الشق الإجرائي لمكافحة جرائم تقنية المعلومات ومنها التجسس الإلكتروني، وللإشارة فإن معظم الإجراءات الواردة في هذه الاتفاقية قد تضمنها قَبلاً القانون الجزائري رقم 09–04، وما يمكن ملاحظته أيضاً بشأن الاتفاقية العربية هو التطابق الكبير بين ما ورد فيها وما ورد في الاتفاقية الأوروبية حول الإجرام المعلوماتي، غير أن الإختلاف يبرز في تفادي هذه الأخيرة للتطرق مباشرة إلى موضوع المساس بالأسرار

والمعطيات الإلكترونية الحساسة للدول إذ جاءت نصوصها بألفاظها عامة وشاملة، وربما يرجع السبب إلى كون هذه الاتفاقية ذات أبعاد دولية نظراً لمشاركة بعض الدول غير الأوروبية فيها ما يؤكد فكرة تفادي الدول لتجريم التجسس الإلكتروني بشكل صريح في الممارسة الدولية.

12- باستقراء جهود مكافحة التجسس الإلكتروني على المستوى الدولي وبالرجوع بداية إلى أعمال المنظمات الدولية الممثلة في هيئة الأمم المتحدة وبعض وكالاتها المتخصصة نجدها تركز أساساً على موضوع تعزيز الأمن في الفضاء الإلكتروني بغرض منع المجرمين من الوصول إلى النظم المعلوماتية الحساسة بالإضافة إلى دراسة مدى إعتبار الاعتداءات التي تتم في الفضاء الإلكتروني مساساً بميثاق الهيئة وتهديداً للأمن والسلم الدوليين وكذا دعم مسألة الإستخدام السلمي للفضاء الإلكتروني، أما بالرجوع إلى الاتفاقيات الدولية، وفي ظل عدم وجود اتفاقيات تتضمن بصريح العبارة والإشارة إلى التجسس سواء بصفة عامة أو التجسس الإلكتروني بصفة خاصة؛ فيمكن تجميع الأحكام المتعلقة بمكافحة التجسس عامة من خلال مجموعة اتفاقيات جاءت أساساً لتنظيم مواضيع أخرى، فاتفاقيات القانون الدولي الإنساني تضمنت تعريف الجاسوس وبينت الأحكام التي يخضع لها في حالة القبض عليه، لكن ميزتها الغالبة تنظيمها للتجسس التقليدي بمعنى عدم صلاحيتها للتطبيق على التجسس الإلكتروني لاختلاف أطراف ووسائل وبيئة النشاط بين الشكلين، أما اتفاقيات القانون الدولي للفضاء الخارجي ومع تقريرها لمبدأ حرية استكشاف واستخدام الفضاء الخارجي ورغم تقييدها لهذه الحرية بقيد الاستخدامات السلمية وقيد تحقيق فائدة ومصلحة كافة الدول؛ فإن العقبة في سبيل مكافحة التجسس عبر الأقمار الصناعية تتمثل في تفسير وإعطاء مدلول لهذين القيدين فالدول المالكة للثروة وللتكنولوجيا التي تسمح لها وبشكل حصري من استغلال الفضاء الخارجي تذهب إلى أن إطلاق الأقمار الاستطلاعية لغايات عسكرية وأمنية تعد جميعاً أعمالاً سلمية وليست عدوانية ما دامت الدولة لم تقم بعدوان عسكري على دولة أخرى، كما تذهب نفس الدول إلى القول بأن التجسس الفضائي يحقق مصلحة البشرية جمعاء وأنه وسيلة فعالة في حماية الأمن والسلم الدوليين لاسيما في مرحلة الرعب النووي والتهديدات الإرهابية!، أما الاتفاقيات المنظمة لاستخدام الطاقة النووية فقد أقرت واجب حفظ أسرار الدفاع الوطني النووية على موظفيها ومفتشيها تحت طائلة تحمل هؤلاء للمسؤولية أمام الدولة المُعتدى عليها بالإضافة إلى رفع الحصانة عنهم، إلا أن اقتضاء الدولة لحقها صعب جداً من الناحية العملية؛ نظراً لكون رفع الحصانة يخضع للسلطة التقديرية للوكالة الدولية للطاقة الذرية من جهة، ولكون سلطة هذه الأخيرة لا يتعدى رفع

الحصانة إلى التسليم؛ وهذا ما يحول دون قدرة الدولة على المحاكمة الحضورية والفعالة، أما بالرجوع إلى اتفاقيات القانون الدولي الدبلوماسي وتحديداً اتفاقية فيينا للعلاقات الدبلوماسية وبالنظر إلى الارتباط التقليدي بين العمل الدبلوماسي والعمل المخابراتي من جهة، وفكرة الحصانة الدبلوماسية؛ فقد قررت هذه الاتفاقية جملة من الجزاءات تشكل وسائل تحقيق التوازن بين مقتضيات حماية أمن الدولة والحصانة الدبلوماسية، إلا أنه ومن الناحية العملية تبقى هذه الجزاءات بعيدة عن تحقيق الغرض منها.

13- يتسم التجسس الإلكتروني بخصوصية بارزة تظهر تحديداً من خلال ازدواجية نظرة الدولة الواحدة له، فهو في الآن ذاته أكثر الجرائم خطورة والماسة بأمنها وأكثر الوسائل التي تلجأ إليها للحفاظ على هذا الأمن، لذلك فاعتبار التجسس سلوكاً مجرماً ومشروعاً في نفس الوقت كان له أثره على جهود مكافحته، وفي هذا الإطار يُلاحظ تجنب دراسة وتناول هذا الموضوع بشكل مباشر على المستوى الدولي سواء من خلال أعمال المنظمات الدولية المختلفة أو من خلال إفراده باتفاقية دولية تنظم أحكامه بشكل صريح، والمتوفر في هذا الشأن هو مجموعة أحكام متفرقة تُستنبط من استقراء توصيات المنظمات أو مواد الاتفاقيات ذات صلة، مع ملاحظة اختلاف في مستوى الإهتمام بين ما هو موجود على المستوى الدولي وما هو موجود على المستوى الإقليمي؛ وعليه بإجراء مقارنة بين مُعطى مستوى الأمن – وطني، إقليمي، دولي– وبين معطى مكافحة التجسس، نجد أنه كلما تم الإنتقال من مستوى أمن إلى آخر (بإتباع نفس الترتيب المذكور آنفاً) كلما أصبحت آليات المكافحة أضعف، وهذا راجع من جهة لدرجة أهمية ذلك المستوى، فكل دولة تحرص على بذل الجهود لحماية أمنها القطري كأولوية ثم يأتي السعي لحماية الأمن الإقليمي نظراً للروابط والمصالح العديدة التي تجمعها مع الدول الأخرى التي تتقاسم وإياها الانتماء لذات الإقليم ليأتي بعد هذين المستويين الأمن الدولي؛ وكذلك لاعتبارها أفعال التجسس المُمارسة من طرفها نابعة من حقها في الحفاظ على بقاءها وتلك الممارسة ضدها أشد أنواع الاعتداءات التي يمكن أن تتعرض لها ومنه يستوجب عليها رصد كافة الآليات الممكنة لمكافحتها، من جهة ثانية.

ثانيـاً- توصيـــات الدراســـة: خرجت الدراسة بجملة من التوصيات يمكن تبيانها في الآتي:

1- تعديل المادة رقم 394 مكرر 3 من قانون العقوبات وذلك بحذف مصطلح "الدفاع الوطني" الوارد فيها لسببين أساسيين؛ السبب الأول يتعلق بعدم إمكانية تجريم الأفعال التي تمس بالدفاع الوطني وهي في حقيقتها جرائم أمن دولة وموقعها الطبيعي هو الفصل الناص على الجنايات والجنح ضد أمن

الدولة ضمن قانون العقوبات، وليس كما ورد في هذا الأخير ضمن الفصل الناص على الجنايات والجنح ضد الأموال، والسبب الثاني- كما سبق توضيحه في متن الدراسة- يتعلق بالعقوبات المقررة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات المستهدفة للدفاع الوطني، إذ لم يتم تحديدها بدقة واكتفى المشرع هنا باستخدام تعابير مرنة تمثلت في النص على مضاعفة العقوبات الواردة في القسم المتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات دون الإخلال بتطبيق عقوبات أشد، ولم يوضح المشرع أي عقوبات أشد يقصدها على وجه التحديد، إذ بالرجوع إلى الفصل المتعلق بجرائم المساس بأمن الدولة وبالدفاع الوطني نجد أن العقوبات قد تصل حد الإعدام الأمر الذي كان يوجب على المشرع الجزائري أن يكون دقيقاً في تقرير العقوبات وعدم ترك ذلك لتقدير القضاء؛ لأن الأمر يتعلق بمبدأ المشروعية من جهة، وبحفظ حقوق الأفراد من جهة ثانية.

2- إدخال تعديلات على الفصل المتضمن الجنايات والجنح ضد أمن الدولة من قانون العقوبات، أولاً بالنص صراحةً على الأسرار ذات الطبيعة الإلكترونية ضمن أصناف أسرار الدفاع الوطني الوارد ذكرها في المادة 63 من قانون العقوبات، وهو مسلك عديد التشريعات العقابية الأجنبية على رأسها قانون العقوبات الفرنسي الجديد الذي أضاف مفهوم "المعطيات المعلوماتية" ضمن طوائف أسرار الدفاع الوطني وذلك في المواد من 411-6 إلى 411-8، وثانياً إضافة مادة للفصل أعلاه تتضمن تجريم وعقاب الأفعال التي تشكل مساساً بأنظمة المعالجة الآلية للمعطيات المتعلقة بأمن الدولة الخارجي وبأسرار دفاعها الوطني ومنها الدخول أو البقاء غير المشروع في النظام، مع تضمين هذه المادة شروطاً خاصة تميزها عن ذات الأفعال الغير مستهدفة للدفاع الوطني كاشتراط ضرورة وجود حماية فنية للنظام المعلوماتي المُعتدى عليه؛ وهذا تماشياً والمسلك الذي اعتمده عندما نص على تجريم ما يُعرف بالإرهاب الإلكتروني بموجب المادتين 87 مكرر 11 و87 مكرر 12 من القانون رقم 16-02 المؤرخ في 19 جوان سنة 2016 المعدل لقانون العقوبات، وعدم اكتفاءه في هذا الإطار بالنصوص التي تحكم الإرهاب في صورته التقليدية التي لا تتضمن استغلال تكنولوجيات الإعلام والاتصال لارتكابه.

3- تدعيم أُطر التعاون الإقليمي خاصةً في ظل عدم القدرة على الإعتماد على التعاون ذو البعد الدولي لصعوبة الاتفاق تحديداً على تجريم التجسس، وهذا مثلاً عن طريق تفعيل نصوص الدفاع العربي المشترك وبناء سياسة مشتركة للدفاع الإلكتروني كما هو الأمر بالنسبة للتجمعات الإقليمية الأخرى، والالتزام بتجسيد بنود الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تُعد إطار تعاون شامل بما

تتضمنه من أحكام خاصة بحماية الأسرار الإلكترونية الحكومية موضوعياً وإجرائياً، ونصها خاصة على إقرار مبدأ العينية وتسليم المجرمين بشأنها، مع ضرورة تبني الإتجاه السائد الذي يُخرج جرائم أمن الدولة الخارجي من طائفة الجرائم السياسية؛ باعتبار أن الاتفاقية العربية تخرج هذه الطائفة من مجال تطبيق إجراءات التعاون.

4- إذا كان من الصعب تفعيل التعاون في شقه الدولي بالنظر إلى أن كُل دولة تعتبر جمع المعلومات حتى السرية منها عن الدول الأخرى فعلاً مشروعاً نابعاً من الدفاع عن حقها في البقاء، فإنه وفي ظل التطور الذي عرفه التجسس من حيث ظهور فواعل جديدة إلى جانب الدول تمارسه لحسابها ولإغراضها الخاصة – الأفراد، المنظمات الإرهابية، جماعات الجريمة المنظمة- يُفترض في الدول ألا تمنح ذات الإمتيازات التي تقررها لنفسها لهؤلاء؛ وعليه وجب عليها أن تعمل على صياغة آليات تعاون دولي لمكافحة التجسس الإلكتروني المُمارس من قبلهم.

5- ضرورة إشراك خبراء المعلوماتية والاتصالات في إعداد النصوص القانونية؛ فكل القوانين حالياً لها بُعد تقني ما يجعل حركة التشريع في تبعية مباشرة لما يستجد على المستوى التكنولوجي، ويحتم على واضعي القانون ليس مجرد استشارة أهل الخبرة وإنما إلزامية الأخذ برأيهم تحديداً في ضبط المصطلحات؛ بحيث أصبح للمصطلح القانوني الإلكتروني مدلول مطابق لذلك التقني وأي إنفراد بصياغة المادة القانونية قد يؤدي إلى التناقض ومخالفة الحقيقة والبعد عن الواقع ما يمس في النهاية بتحقيق العدالة ومكافحة الجريمة بمختلف صورها، وفي مقابل ذلك ضرورة إجراء دورات تكوينية متواصلة خاصة للقضاة لغرض تحيين معارفهم ومواكبة – على الأقل – ما هو ظاهر من التطورات التكنولوجية في مجال الإعلام والاتصال، والإلمام بالتقنيات والأساليب المتطورة باستمرار لارتكاب التجسس الإلكتروني.

6- في ظل عجز النصوص القانونية بمفردها عن مكافحة التجسس الإلكتروني؛ بالنظر لعدة أسباب أهمها: صعوبة اكتشاف وقوعه، أو تحديد مرتكبيه، أو القبض عليهم؛ يُصبح من إتخاذ تدابير وقائية للحيلولة دون الوصول إلى الأنظمة المعلوماتية أكثر من ضرورة، وهذا لا يتم إلا عن طريق أمرين هما:

أ- بناء منظومة متكاملة للأمن المعلوماتي، تشمل الجانب البشري والجانب المادي والجانب التقني، مع تحيينها بشكل مستمر، ورسم سياسة دفاع إلكتروني مسايرة للنهج الذي تبنته اليوم عديد الدول والمنظمات.

ب- دعم البحث العلمي واستغلال نتائجه في بناء صناعات وطنية مستقلة، والتخلص من التبعية في مجال التقنية للدول الأجنبية؛ فالواقع أثبت أن كثيراً من حالات التجسس الإلكتروني جاءت نتيجة ثغرات موجودة إما على مستوى التجهيزات أو أنظمة التشغيل المعلوماتية.

7- ضرورة الإهتمام بدراسة تأثير التكنولوجيات الحديثة على أمن الدولة، والمعالجة الدقيقة لكل جوانب هذا التأثير خاصة في ظل افتقار المكتبة الجامعية لمثل هذه الدراسات من جهة، وكونها مجالاً خصباً للبحث؛ بالنظر للإشكالات الكثيرة والدقيقة التي تطرحها سواء من ناحية فهم وتطبيق القواعد القانونية الموضوعية أو الإجرائية.

قـــائـــمة المصادر والمراجـــع

قائمة المصادر والمراجع باللغة العربيـــة:

أولاً- النصوص القانونيـــة:

أ- الدساتيـــر:

1- الدستور الجزائري الصادر بموجب المرسوم الرئاسي رقم 96–438 المؤرخ في 7 ديسمبر سنة 1996 المعدل بموجب القانون رقم 16– 01 المؤرخ في 6 مارس سنة 2016.

ب- الإتفاقيات والمواثيق الدوليـــة:

1- إتفاقية لاهاي المتعلقة بقوانين وأعراف الحرب في البر المؤرخة في 18 أكتوبر سنة 1907.

2- ميثاق جامعة الدول العربية المحرر بالقاهرة بتاريخ 22 مارس سنة 1945.

3- إتفاقية جنيف الثالثة بشأن معاملة أسرى الحرب المؤرخة في 12 أوت 1949.

4- إتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب المؤرخة في 12 أوت سنة 1949.

5- معاهدة الدفاع المشترك والتعاون الإقتصادي بين دول الجامعة العربية وملحقها العسكري الموقعة بتاريخ 17 جوان سنة 1950 والتي دخلت حيز التنفيذ في 23 أوت 1952.

6- إتفاقية فيينا للعلاقات الدبلوماسية المحررة بفيينا بتاريخ 18 أفريل سنة 1961.

7- معاهدة المبادئ المنظمة لنشاطات الدول في ميدان استكشاف واستخدام الفضاء الخارجي بما في ذلك القمر والأجرام السماوية الأخرى الموقعة في كل من لندن وموسكو وواشنطن في 27 جانفي سنة 1967 والتي دخلت حيز التنفيذ في 10 أكتوبر سنة 1967.

8- إتفاقية إنقاذ الملاحين الفضائيين وإعادة الملاحين الفضائيين ورد الأجسام المطلقة في الفضاء الموقعة في كل من لندن وموسكو وواشنطن في 22 أفريل سنة 1968 والتي دخلت حيز التنفيذ في 03 ديسمبر سنة 1968.

9- معاهدة عدم إنتشار الأسلحة النووية الموقعة في كل من لندن وموسكو وواشنطن في 01 يوليو سنة 1968 والتي دخلت حيز التنفيذ في مارس سنة 1970.

10- الوثيقة رقم "INFCIRC/153" بعنوان هيكل ومضمون الاتفاقيات التي تعقد بين الوكالة الدولية للطاقة الذرية والدول بموجب معاهدة عدم انتشار الأسلحة النووية، المعروفة باتفاقية الضمانات الشاملة، الصادرة عن الوكالة الدولية للطاقة الذرية في ماي سنة 1971.

11- إتفاقية المسؤولية الدولية عن الأضرار التي تحدثها الأجسام الفضائية الموقعة في 29 مارس سنة 1972 والتي دخلت حيز التنفيذ في 01 سبتمبر سنة 1972.

12- البروتوكول الأول الإضافي إلى إتفاقيات جنيف والمتعلق بحماية ضحايا المنازعات الدولية المسلحة لسنة 1977.

13- الاتفاقية المنظمة لأنشطة الدول على سطح القمر والأجرام السماوية الصادرة في 18 ديسمبر سنة 1979 والتي دخلت حيز التنفيذ في 11 يوليو سنة 1984.

14- اتفاقية الحماية المادية للمواد النووية الموقعة في كل من فيينا ونيويورك في 03 مارس سنة 1980 والتي دخلت حيز التنفيذ في 08 فبراير سنة 1987.

15- الوثيقة رقم "INFCIRC/540" بعنوان البروتوكول النموذجي الإضافي للاتفاق(ات) المعقود(ة) بين الدولة (الدول) والوكالة الدولية للطاقة الذرية من أجل تطبيق الضمانات ، صادرة عن الوكالة الدولية للطاقة الذرية في سبتمبر سنة 1997.

16- إتفاقية بودابست الأوروبية حول الإجرام المعلوماتي الموقعة في بودابست في 23 نوفمبر سنة 2001.

17- القانون العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها المعتمد من طرف مجلس وزراء العدل العرب بتاريخ 08 أكتوبر 2003 ومجلس وزراء الداخلية العرب بتاريخ 21 أفريل سنة 2004.

18- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010.

ج- القوانين العضويـــة:

1- القانون العضوي رقم 12-05 المؤرخ في 12 يناير سنة 2012 المتعلق بالإعلام.

د- القوانين العاديـــة:

1- الأمر رقم 66–155 المؤرخ في 08 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم بموجب القانون رقم 17-07 المؤرخ في 27 مارس سنة 2017.

2- الأمر رقم 66–156 المؤرخ في 08 يونيو سنة 1966 المتضمن قانون العقوبات، المتمم بموجب القانون رقم 16–02 المؤرخ في 19 يونيو سنة 2016.

3- القانون رقم 2000–03 المؤرخ في 05 أوت سنة 2000 يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية.

4- القانون رقم 09–04 المؤرخ في 05 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

5- القانون رقم 14–04 المؤرخ في 24 فبراير سنة 2014 يتعلق بالنشاط السمعي البصري.

ه- المراسيـــم :

1- المرسوم الرئاسي رقم 04–183 المؤرخ في 26 يونيو سنة 2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي.

2- المرسوم الرئاسي رقم 15–228 المؤرخ في 22 أوت سنة 2015 يحدد القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو وسيره.

3- المرسوم الرئاسي رقم 15–261 المؤرخ في 08 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

و- قوانين عربيـــة:

1- القانون الاتحادي رقم 02 لسنة 2006 المعدل، في شأن مكافحة جرائم تقنية المعلومات، لدولة الإمارات العربية المتحدة.

2- نظام مكافحة الجرائم المعلوماتية الصادر بموجب المرسوم الملكي رقم م/17 وتاريخ 1428/03/08، للمملكة العربية السعودية.

3- قانون جرائم أنظمة المعلومات رقم 30 لسنة 2010، لدولة الكويت.

4- المرسوم التشريعي رقم 17 المؤرخ في 08 شباط (فيفري) سنة 2012 المتعلق بتنظيم التواصل على الشبكة والجريمة المعلوماتية، لدولة سوريا.

ثانيـــاً- الكتب:

1- إبراهيم شاكر محمود الجبوري، جرائم الإعتداء على أمن الدولة من الداخل والخارج، المركز القومي للإصدارات القانونية، مصر، 2011.

2- إبراهيم محمد منصور الشحات، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، دار الفكر الجامعي، مصر، 2011.

3- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ط 7، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007.

4- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط 5، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007.

5- أحمد محمود خليل، جرائم أمن الدولة العليا، المكتب الجامعي الحديث، مصر، 2004.

6- أحمد محمد الرفاعي، الجرائم الواقعة على أمن الدولة (الجرائم الواقعة على أمن الدولة الخارجي)، دار البشير للنشر والتوزيع، الأردن، 1990.

7- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، مصر، 2010.

8- بشرى حسين الحمداني، القرصنة الإلكترونية وأسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، الأردن، 2014.

9- بول ويلكينسن، العلاقات الدولية، ترجمة لبنى عماد تركي، مؤسسة هنداوي للتعليم والثقافة، مصر،2013 .

10- ثامر كامل محمد، تداعيات عاصفة الأبراج (الإستراتيجية الدولية في عصر العولمة)، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2002.

11- جاك يوسف الحكيم ورياض الخاني، شرح قانون العقوبات القسم الخاص (الجرائم الواقعة على أمن الدولة الخارجي)، منشورات جامعة دمشق، كلية الحقوق، 2009.

12- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، دار البداية، الأردن، 2010.

13- جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، الأردن، 2010.

14- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، مصر، 1996.

15- جواد الحمد، مستقبل الأمن القومي العربي في ظل السلام مع إسرائيل، ط 2، مركز دراسات الشرق الأوسط، الأردن، 1999.

16- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، دار النهضة العربية، مصر، 2009.

17- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2011.

18- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعة، مصر، 2010.

19- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2009.

20- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، مصر، 2009.

21- ذياب البداينة، الأمن و حرب المعلومات، دار الشروق للنشر و التوزيع، الأردن، 2006.

22- رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، 2012.

23- رفعت رشوان، مبدأ إقليمية قانون العقوبات في ضوء قواعد القانون الجنائي الداخلي والدولي، دار الجامعة الجديدة، مصر، 2008.

24- زكي زكي حسين زيدان، الإستخبارات العسكرية ودورها في تحقيق الأمن القومي للدولة في الفقه الإسلامي والقانون الوضعي، دار الكتاب القانوني، مصر، 2009.

25- زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011.

26- سعد إبراهيم الأعظمي، جرائم التجسس في التشريع العراقي، دون بلد نشر، 1981.

27- سليمة سعيدي وبلال حجاز، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، مصر، 2017.

28- سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، منشورات الحلبي الحقوقية، لبنان، 2011.

29- سهى حميد سليم جمعة، تلوث بيئة الفضاء الخارجي في القانون الدولي العام، دار المطبوعات الجامعية، مصر، 2009.

30- ضياء مصطفى عثمان، السرقة الإلكترونية، دار النفائس للنشر والتوزيع، الأردن، 2011.

31- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، مصر، 2010.

32- عاطف فهد المغاريز، الحصانة الدبلوماسية بين النظرية والتطبيق، دار الثقافة للنشر والتوزيع، الأردن، 2009.

33- عبد الحكم فودة، الموسوعة الجنائية الحديثة، دار الفكر والقانون، مصر، 2002.

34- عبد الرحمان شعبان عطيات، أمن الوثائق والمعلومات، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

35- عبد الصبور عبد القوي علي مصري، الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، مصر، 2008.

36- عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، مصر، 2011.

37- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والأنترنت في التشريعات العربية، دار النهضة العربية، مصر، 2009.

38– عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2007.

39- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، دار النهضة العربية، مصر، 2009.

40- عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، مصر، 2009.

41- عبد الفتاح مصطفى الصيفي، قانون العقوبات اللبناني (جرائم الاعتداء على أمن الدولة وعلى الأموال)، دار النهضة العربية للطباعة والنشر، لبنان، 1972.

42- عبد القادر الشيخ، شرح قانون العقوبات القسم الخاص (الجرائم الواقعة على أمن الدولة)، منشورات جامعة حلب، كلية الحقوق، مديرية الكتب والمطبوعات الجامعية، 2006.

43- عبد الله سليمان، دروس في شرح قانون العقوبات الجزائري القسم الخاص، ط 2، ديوان المطبوعات الجامعية، الجزائر، 1989.

44- عبد المهيمن بكر، جرائم أمن الدولة الخارجي (دراسة معمقة في القانون الكويتي والمقارن)، دار النهضة العربية، مصر، 1976.

45- عدلي أمير خالد، الجرائم الضارة بالوطن من الداخل والخارج في ضوء المستحدث من قوانين وأحكام النقض و الدستورية، دار الفكر الجامعي، مصر، 2013.

46- عدنان الخالدي، موسوعة أشهر جواسيس العالم، دار أسامة للنشر والتوزيع، الأردن، 2010.

47- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2003.

48- علي جبار الحسيناوي، جرائم الحاسوب والأنترنت، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2009.

49- علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، دون بلد نشر، 2013.

50- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعة للطباعة والنشر، لبنان، 1999.

51- غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015.

52- فاوي الملاح، سلطات الأمن والحصانات والإمتيازات الدبلوماسية، دار المطبوعات الجامعية، مصر، 1993 .

53- فرانك دانينو، وكالة الاستخبارات المركزية الأمريكية CIA حكاية سياسية 1947-2007، ترجمة عبير المنذر، مؤسسة الانتشار العربي، لبنان، 2009.

54- كوثر أحمد خالند، الإثبات الجنائي بالوسائل العلمية، مكتب التفسير للنشر والإعلان، أربيل، 2006.

55- ليلى بن حمودة، الاستخدام السلمي للفضاء الخارجي، المؤسسة الجامعية للدراسات والنشر والتوزيع، لبنان، 2008.

56- مجدي محب حافظ، الحماية الجنائية لأسرار الدولة، الهيئة المصرية العامة للكتاب، مصر، 1997.

57- مجدي محمود محب حافظ، موسوعة جرائم الخيانة والتجسس (دراسة في التشريع المصري والتشريعات العربية والتشريعات الأجنبية والشريعة الإسلامية)، دار محمود للنشر والتوزيع، مصر، 2010.

58- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

59- محمد الفاضل، الجرائم الواقعة على أمن الدولة، ط 4، المطبعة الجديدة، سوريا، 1978.

60- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2009.

61- محمد راكان الدغمي، التجسس وأحكامه في الشريعة الإسلامية، ط 2، دار السلام للطباعة والنشر والتوزيع والترجمة، مصر، 1985.

62- محمد صبحي نجم، شرح قانون العقوبات الجزائري (القسم الخاص)، ط 6، ديوان المطبوعات الجامعية، الجزائر، 2005.

63- محمد علي السيد، الوجيز في الجريمة السياسية، منشورات الحلبي الحقوقية، لبنان، 2003.

64- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، مصر، 2004.

65- محمد عودة الجبور، الجرائم الواقعة على أمن الدولة وجرائم الإرهاب، دار الثقافة للنشر والتوزيع، الأردن، 2009.

66- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، مصر، 2001.

67- محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة (دراسة مقارنة في التشريعات العربية والقانونين الفرنسي والإيطالي)، دار المطبوعات الجامعية، مصر، 2014.

68- محمود سليمان موسى، الجرائم الواقعة على أمن الدولة (دراسة مقارنة في التشريعات العربية والقانونين الفرنسي والإيطالي في ضوء المفاهيم الديمقراطية والدستورية ومبادئ حقوق الإنسان)، دار المطبوعات الجامعية، مصر، 2009.

69- مسعود خثير، الحماية الجنائية لبرامج الكمبيوتر (أساليب وثغرات)، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2010.

70- مصطفى مجدي هرجة، التعليق على قانون العقوبات، المجلد الثاني، دار محمود للنشر والتوزيع، مصر، دون تاريخ نشر.

71- مصطفى محمد مرسي، التحري في جرائم مجتمع المعلومات و المجتمع الافتراضي، دون دار وبلد نشر، 2011.

72- معمر بوزنادة، المنظمات الإقليمية ونظام الأمن الجماعي، دار المطبوعات الجامعية ، الجزائر، 1992.

73- ممدوح الشيخ، التجسس التكنولوجي (سرقة الأسرار الاقتصادية والتقنية)، مكتبة بيروت، مصر، 2007.

74- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2008.

75- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، مصر، 1994.

76- هلالي عبد الله أحمد، إتفاقية بودابست لمكافحة جرائم المعلومات معلقاً عليها، دار النهضة العربية، دون بلد نشر، 2007.

77- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية (دراسة تأصيلية تحليلية ومقارنة للتنصت على المحادثات التليفونية والتي تجري عبر الأنترنت والأحاديث الشخصية نظرياً وعملياً)، دار المطبوعات الجامعية، مصر، 2009.

78- يوسف حسن يوسف، الجرائم الدولية للأنترنت، المركز القومي للإصدارات القانونية، مصر، 2011.

ثالثـــاً- الرسائـــل الجامعيـــة:

أ- أطروحات الدكتـــوراه:

1- تنوير أحمد بن محمد نذير، حق الخصوصية (دراسة مقارنة بين الفقه الإسلامي والقانون الإنجليزي)، أطروحة دكتوراه في الفقه الإسلامي، مقدمة لكلية الشريعة والقانون، الجامعة الإسلامية العالمية بإسلام آباد، 2007.

2- شادية رحاب، الحصانة القضائية الجزائية للمبعوث الدبلوماسي، أطروحة دكتوراه في العلوم القانونية، قسم العلوم القانونية، مقدمة لكلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2006.

3- صبرينة بن سعيد، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا "الإعلام والاتصال"، أطروحة دكتوراه في القانون الدستوري، قسم الحقوق، مقدمة لكلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2014-2015.

4- صفية بشاتن، الحماية القانونية للحياة الخاصة، أطروحة دكتوراه، مقدمة لكلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012.

5- عماد الدين محمد كامل الجمل، الحماية الجنائية لأسرار الدفاع في مواجهة التقدم التكنولوجي الحديث، أطروحة دكتوراه في الحقوق، مقدمة لكلية الحقوق، جامعة القاهرة، دون تاريخ مناقشة.

6- عمر بن محمد العتيبي، الأمن المعلوماتي في المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، أطروحة دكتوراه، قسم العلوم الإدارية، مقدمة لكلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010.

7- غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، أطروحة دكتوراه، مقدمة لكلية الحقوق، جامعة باجي مختار، عنابة، 2010-2011.

8- محمد بن محمد سالم عدود، الجرائم المضرة بأمن الدولة الداخلي وعقوباتها في القانون الموريتاني، أطروحة دكتوراه الفلسفة في العلوم الأمنية، مقدمة لقسم العدالة الجنائية بكلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010.

9- محمد محمد صالح الألفي، الجرائم المضرة بأمن الدولة عبر الأنترنت، أطروحة دكتوراه، مقدمة لكلية الحقوق، جامعة القاهرة، 2011.

10- محمود سليمان موسى، النظرية العامة لجرائم التجسس في القانون الليبي والتشريع المقارن، أطروحة دكتوراه، مقدمة لكلية الحقوق، جامعة الإسكندرية، 1997.

11- هبة نبيلة هروال، جرائم الأنترنت (دراسة مقارنة)، أطروحة دكتوراه، مقدمة لكلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2013-2014.

ب- مذكرات الماجستيـــر:

1- عادل عبد الصادق محمد الجخة، أثر الإرهاب الإلكتروني على مبدأ إستخدام القوة في العلاقات الدولية، مذكرة ماجستير، مقدمة لقسم العلوم السياسية بكلية الإقتصاد والعلوم السياسية، جامعة القاهرة، 2009.

2- عبد الكريم عاشور، دور الإدارة الالكترونية في ترشيد الخدمة العمومية في الولايات المتحدة الأمريكية والجزائر، مذكرة ماجستير في العلوم السياسية والعلاقات الدولية، مقدمة لقسم العلوم السياسية والعلاقات الدولية بكلية الحقوق والعلوم السياسية، جامعة منتوري، قسنطينة، 2009-2010.

3- عثمان يحي أحمد أبو مسامح، جريمة التخابر وإجراءات محاكمة مرتكبيها في التشريع الفلسطيني (دراسة تحليلية مقارنة)، مذكرة ماجستير في القانون العام، مقدمة لقسم القانون العام بكلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2014.

4- فريد ولد حسين، جرائم التجسس، مذكرة ماجستير في القانون الجنائي الدولي، مقدمة لمعهد العلوم القانونية والإدارية بالمركز الجامعي عباس لغرور، خنشلة، 2010-2011.

5- فهد ناصر عيسى بن صليهم، مبدأ العينية وأثره في مكافحة الجرائم العابرة للحدود الدولية(دراسة مقارنة)، مذكرة ماجستير في العدالة الجنائية، قسم العدالة الجنائية، مقدمة لكلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

6- محمد عدنان عثمان، دور القانون الدولي في مواجهة التجسس الدبلوماسي، مذكرة ماجستير في القانون العام، مقدمة لقسم القانون العام بكلية الحقوق، جامعة الشرق الأوسط، دون بلد، 2015.

7- منصور بن سعيد القحطاني، مهددات الأمن المعلوماتي وسبل مواجهتها (دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض)، مذكرة ماجستير في العلوم

الإدارية، مقدمة لقسم العلوم الإدارية بكلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2008.

8- نسيم سعيداني، آليات البحث والتحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة ماجستير في العلوم الجنائية، مقدمة لقسم الحقوق بكلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012–2013.

9- وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، مذكرة ماجستير في التخطيط والتنمية السياسية، مقدمة لكلية الدراسات العليا بجامعة النجاح الوطنية، نابلس، فلسطين، 2013.

رابعـــاً- المؤتمـــرات والملتقيـــات والنـــدوات والحلقـــات العلميـــة:

1- إيهاب ماهر السنباطي، الجرائم الإلكترونية (الجرائم السيبيرية): قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد، مداخلة مقدمة في إطار الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19-20 يونيو 2007.

2- حنان أوشن ووادي عماد، التجسس الإلكتروني وآليات مكافحته في التشريع الجنائي الجزائري، مداخلة مقدمة في إطار الملتقى الوطني حول الجرائم الماسة بأمن الدولة، معهد العلوم القانونية والإدارية، المركز الجامعي عباس لغرور، خنشلة، 12–13 ديسمبر 2011.

3- ذياب موسى البداينة، الإرهاب المعلوماتي، مداخلة مقدمة في إطار الحلقة العلمية الموسومة بـــ"الأنترنت والإرهاب"، قسم البرامج التدريبية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، القاهرة، 15–19 نوفمبر 2008.

4- رؤوف بوسعدية ومنى غبولي، مواجهة المشرع الجزائري لأفعال التجسس الصادرة عن أفراد البعثات الدبلوماسية، مداخلة مقدمة في إطار الملتقى الوطني حول الجرائم الماسة بأمن الدولة، معهد العلوم القانونية والإدارية، المركز الجامعي عباس لغرور، خنشلة، 12–13 ديسمبر 2011.

5- عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة تطبيقية مقارنة)، مداخلة مقدمة في إطار المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 12–14 نوفمبر 2007.

6– محمد أمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الأنترنت، مداخلة مقدمة في إطار الحلقة العلمية الموسومة بـــ "الانترنت والإرهاب"، قسم البرامج التدريبية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، القاهرة، 15–19 نوفمبر 2008.

7- محمد أمين البشري، مؤسسات المجتمع المدني والأمن القومي العربي، مداخلة مقدمة في إطار الندوة العلمية حول دور مؤسسات المجتمع المدني في التوعية الأمنية، قسم الندوات واللقاءات العلمية، مركز الدراسات والبحوث، 12–14 ماي 2009.

8- مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، 23–25 سبتمبر 2012.

9- منى الأشقر جبور وعزيز ملحم بربر، أمن الشبكات والإنترنت، مداخلة مقدمة في إطار الحلقة العلمية الموسومة بـــ "الانترنت والإرهاب" ، قسم البرامج التدريبية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، القاهرة، 15–19 نوفمبر 2008.

10- موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة عبر الوطنية، مداخلة مقدمة في إطار المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28–29 أكتوبر 2009.

11- ياسين قوتال، جريمة التجسس الالكتروني ومخاطرها على أمن الدولة، مداخلة مقدمة في إطار الملتقى الوطني حول الجرائم الماسة بأمن الدولة، معهد العلوم القانونية والإدارية، المركز الجامعي عباس لغرور، خنشلة، 12–13 ديسمبر 2011.

خامســاً- المقــالات:

1- أروى محمد تقوى، مدى مسؤولية مشغلي الهاتف النقال عن إساءة إستخدامه في الاتصال بالأنترنت، مجلة الحقوق، المجلد الحادي عشر، العدد الثاني، سوريا.

2- أولاف تايلر، التهديدات الجديدة: الأبعاد الإلكترونية، مجلة الناتو، مقال منشور على الموقع الالكتروني:

http://www.nato.int/docu/review/2011/11september/cyber-threads/files/1679.jpg

تمت زيارة الموقع بتاريخ: 2016/06/26.

3- جمال علي زهران، الأمن الإقليمي: التهديدات والتحديات في ظل الأمن القومي العربي، مجلة الغدير، العدد الرابع والستون، دار الفلاح للنشر والتوزيع، لبنان، خريف 2013.

4- حنان أوشن ووادي عماد الدين، التجسس الالكتروني وآليات مكافحته في التشريع الجنائي الجزائري، مجلة الحقوق والعلوم السياسية، العدد الثاني، جامعة عباس لغرور، خنشلة، أكتوبر 2014.

5- سوزان عدنان الأستاذ، إنتهاك حرمة الحياة الخاصة عبر الأنترنت (دراسة مقارنة)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد التاسع والعشرون، العدد الثالث، سوريا، 2013.

6- عبد الصبور عبد القوي علي، الجريمة الالكترونية والجهود الدولية للحد منها، مجلة الدراسات المالية والمصرفية، العدد الأول، المجلد الثالث والعشرون، الأكاديمية العربية للعلوم المالية والمصرفية، الأردن، السنة الثالثة والعشرون، مارس 2015.

7- ليتيم فتيحة وليتيم نادية، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة الفكر، العدد الثاني عشر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، دون تاريخ نشر.

8- محمد أحمد السويحلي، تكاتف الجهود العربية لمكافحة الجريمة الإلكترونية، مجلة الدراسات المالية والمصرفية، العدد الأول، المجلد الثالث والعشرون، الأكاديمية العربية للعلوم المالية والمصرفية، الأردن، السنة الثالثة والعشرون، مارس 2015.

9- محمد حسون، الإستراتيجية التوسعية لحلف الناتو وأثرها على الأمن القومي العربي، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد السادس والعشرون، العدد الثاني، سوريا، 2010.

10- هشام ساحلي، أساليب التحري الخاصة ومدى مساسها بحرمة تنقل الفرد في التشريع الجزائري، مجلة الحقوق للبحوث القانونية والاقتصادية، العدد الثاني، كلية الحقوق، جامعة الإسكندرية، مصر، 2014.

11- وهيبة رابح، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد الرابع، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، ديسمبر 2014.

12- يونس الزرهوني، القصة الكاملة لمفجر أكبر فضيحة خيانة في التاريخ الأمريكي: إدوارد سنودن، مقال منشور على الموقع الالكتروني: www.the3professional.com/2013/08/blog-post-html ، تمت زيارة الموقع بتاريخ: 2016/08/21.

سادســاً- المعاجـــم و القوامـــيس:

1- أبي الفضل جمال الدين محمد بن مكرم ابن منظور الإفريقي المصري، لسان العرب، ط 4، المجلد الثالث، دار صادر للطباعة والنشر، لبنان، 2005.

2- أحمد مختار عمر، معجم اللغة العربية المعاصرة، المجلد الأول، عالم الكتب للنشر والتوزيع والطباعة، مصر، 2008.

3- يوسف محمد رضا، معجم العربية الكلاسيكية والمعاصرة، مكتبة لبنان ناشرون، لبنان، 2006.

قائمـــة المراجـــع باللغـــة الفرنسيـــة:

1/ les ouvrages:

1- Allen M. Lenden et autres, les crimes contre l'Etat, commission de réforme du droit du Canada, Canada 1986.

2- Frédéric Chapier, l'économie c'est la guèrre: les agents secrets au service du big business, édition du seuil, paris.

3- Gerard Peliks, la cybercriminalité, livres blanc de forum ATENA, France, Mai 2013.

4- Jean. Marie Henckaerts et Luise Doswald-Beck, droit international humanitaire coutumier, volume 1: règles, bruylant, Belgique, 2006.

5- Marco Gerck, comprendre la cybercriminalité: guide pour les pays en développement, union internationale des télécommunication, Suisse, 2009 ouvrage publié sur le site:www.itu.int/ITU-D/cyb/cybersecurity/législation.html, le site a été visité le: 04/02/2015.

6- Koenraad Dassen, sûreté du l'Etat, Bruxelles, Belgique, 2005, ouvrage publie sur le site: http//www.suretedeletat.be, le site a été visité le:07/02/2015.

7- Robert Longeon et Jean-Luc Archimbaud, guide de la sécurité des systèmes d'information, centre national de la recherche scientifique, France, 1999, ouvrage publié sur le site: http//www.cnrs.fr/infosecu, le site a été visité le: 04/02/2015.

2/ les thèses :

1- Fernand Lone Sang, protection des systèmes informatiques contre les attaques par entrées-sorties, thèse du doctorat université de Toulouse,2012, mémoire publiée sur le site: www.tel.archives-ouvertes.fr, le site a été visité le: 23/11/2015.

2- Joëlle Noailly, l'espionnage industriel au cour de la guerre mondiale du renseignement économique, mémoire de maitrise, université Lyon 2,1996-1997, mémoire publiée sur le site: www.strategique,free.fr, le site a été visité le: 04/02/2015.

3/ les articles :

1- Anne Souvira, la cybersécurité des entreprises, revue LAMY droit des affaires (RRDA), numéro 87, Walters Kluwer, France, novembre 2013.

2- Bernard Carayon, secret des affaires (protéger le secret des affaires: un enjeu national): bulletin du droit des secret d'affaires-BSA-n°=1,publication de l'institut de l'IE, paris, trimestre 3, novembre 2012, publié sur le site: www.institut-ie.fr, le site a été visité le: 04/02/2015.

3- Bertrand Warusfel, la loi américaine sur l'espionnage économique, revue droit te défense, paris, 1997, publié sur le site: www.driot.univ-paris5.fr,le site a été visité le: 23/11/2015.

4- Cecile Doutriausc, donnés personnelles et cybersurveillance, la RDN, chaire cyber-défense et cyber-sécurité, n°=775, paris, décembre 2014, publié sur le site: www.chaire-cyber.fr, le site a été visité le: 23/11/2015.

5- Daniel Tant, guerre électronique et chiffrement, association des réservistes de chiffre et de la sécurité de l'information(ARCSI), France, publié sur le site: www.arcsi.fr, le site a été visité le: 23/11/2015.

6- Daniel Ventre, cyberespionnage et diplomatie : l'exemple des tentions Chine/Etats-Unis, les grands dossiers de diplomatie, n°=23, article publié sur le site: www.chaire-cyber.fr, le site a été visité le: 23/11/2015.

7- Dany Deschenes, le système échelon : une nouvelle donne dans l'espionnage électronique, bulletin le maintien de la paix, n°=50, université Laval, Québec, Canada, janvier 2001, publié sur le site: http//:www.ulaval.ca/ikhei, le site a été visité le: 04/02/2015.

8- Emmanuele Daoud et autres, libertés fondamentales et protection des données personnelles, revue LAMY droit des affaires (RRDA), numéro 87, Walters Kluwer, France, novembre 2013.

9-Laurent Murawiec, la cyber guerre, publie sure le site: www.societestrategie.fr, le site a été visité le: 23/11/2015.

10- Myriam Quemener, la coopération entre des organes de lutte contre la cybercriminalité, revue LAMY droit des affaires (RRDA), numéro 87, Walters Kluwer, France, novembre 2013.

11- Nir Kshetri, les activités d'espionnage électronique et contrôle d'internet A l'ère de l'infonuagique : le cas de la chine, Télescope, vol 18, n°=1-2, printemps-été 2012.

12- Pierre Caron, la guerre électronique n'aura pas lieu, association des anciens de l'école de guerre économique, publié sure le site: www.bdc.aege.fr, le site a été visité le: 23/11/2015.

13- Ron Smith et Scott Knight, l'application des solution de la guerre électronique a la sécurité des réseaux, revu militaire Canadienne, Canada, automne 2005, publié sur le site: www.journal.forces.gc.ca, le site a été visité le: 23/11/2015.

14- L'affaire Snowden et la nouvelle géopolitique du cyberespionnage, article publier sur le site: http://la-rem.eu, le site a été visité le: 23/11/2015.

4/ les séminaires, les études, les rapports et les publications:

1- Abderrahmane Nitaj, la cryptographie et la confiance numérique, étude, université de Caen basse, Normandie, 23 mars 2013.

2- Alexandre Lienard, lutter contre l'espionnage industriel, réseau vincibilis, étude publié sur le site: www.utbm.fr, le site a été visité le: 23/11/2015.

3- François-Bernard Huyghe, qu'est-ce que la guerre de l'information?, étude publié sur le site: http// www. Huyghe.fr, le site a été visité le: 04/02/2015.

4- Holly Porteous, cybersécurité et renseignement de sécurité: l'approche des Etat unis, étude générale, bibliothèque du parlement, canada, 15 juin 2011.

5- Irnerio Seminatore, la géopolitique a l'âge numérique, sixième conférence de la onzième année de l'academia diplomatica europaea, institut européen des relations internationales, Bruxelles, 13/02/2014, publie sur le site: www.ieri.be, le site a été visité le: 04/02/2015.

6- Jean –Baptiste De Fontenilles et autres, la course technologique en matière d'armement: une nécessité qui peut être métriser ou, au contraire, un risque technologique déconnecté de la réalité opérationnelle et géostratégique, rapport sur les travaux de la comité n°=7 à la 45eme session national, 2009, rapport publié sur le site: www.chear,france/wiheden.fr, le site a été visité le: 23/11/2015.

7- Jean-Jacques Gagnepain, les révolutions technologiques qui préparent le futur, actes de la rencontre internationale de prospective du sénat intitulé "la guerre du futur: analyse prospective de l'avenir des conflits, palais du Luxembourg, jeudi 27 novembre 2003, publié sur le site: www.penseemiliterre.fr, le site a été visité le: 23/11/2015.

8- Rayan Burton, 2014 une année d'actualité cyber, publication de cellule cyberdéfense, France, 22 janvier 2015, publier sur le site: www.cil.cnrs.fr, le site a été visité le: 23/11/2015.
9- René Trégouet, présentation de colloques: introduction générale, actes de la rencontre internationale de prospective du sénat intitulé "la guerre du futur: analyse prospective de l'avenir des conflits, palais du Luxembourg, jeudi 27 novembre 2003, publié sur le site: www.penseemiliterre.fr, le site a été visité le: 23/11/2015.
10- Saida Bedar, perspectives et prospectives du contexte stratégique, actes de la rencontre internationale de prospective du sénat intitulé "la guerre du futur: analyse prospective de l'avenir des conflits, palais du Luxembourg, jeudi 27 novembre 2003, publié sur le site: www.penseemiliterre.fr, le site a été visité le: 23/11/2015.

5/ dictionnaires:

1- Alain Rey, le Robert micro, dictionnaire de la langue française, 3eme édition, Paris, 1998.
2- Yves Garnier, dictionnaire encyclopédique, Larousse, Paris, France, 2001.

قائمـــة المراجـــع باللغـــة الإنجليزيـــة:

1/ Books:

1- Daniel Domsheit-berg, inside wikileaks, crown publishers, New York, United States, 2011.
2- Louise I Gerdes, Espionage and intelligence Gathering, Greenhaven press, United States of America, 2004.

2/ conférences and stadys and publications:

1- Graig Brown, Espionage in international Law: a Necessary Evil, stady university of western Ontario, 1999.
2- Kevin A. O'Brien, cyber-intelligence: for threat profiling of sub-state actors in the information Age, rand Europe, Cambridge, united kingdom, study published on: www.isodarco.it, 23/11/2015.
3- Tim Maurer, Wikileaks2010: A Glimpse of future, discussion paper, explorated in cyber international relations discussion paper series, Belfer center for science and international Affaires, Harvard Kennedy school, USA, August

2011 , Publier sur le site: www.maurer-dp-2011-10-wikileaks-final , le site a été visité le: 23-11-2015.

4- Troy Townsend and others, SEI Emerging Technology center: Cyber intelligence Tradecraft project, Software Engineering Institute, Carnegie Mellon University, USA, 2013, etude publier sur le site: www.sei.cmu.edu, le site a été visité le: 23/11/2015.

5- Cyberespionage: the harsh reality of advanced security threats, publication of DELOITTE (centre for security and privacy solution), 2011, study published on: www.isaca.org, 23/11/2015.

6- Cyberthreat intelligence and the lessons from Law enforcement, publication of KPMG, Suisse, May 2013, publié sur le site: wwwkpmg.com, le site a été visité le: 23/11/2015.

7- Strategic Cyber Intelligence, publication of the intelligence and national security alliance (INSA), Arlington, USA, March 2014, etude publier sur le site: www.insaonline.org, le site a été visité le: 23/11/2015.

8- The Defence cyber strategy, publication of the Netherlands ministry of defence , Netherlands , September 2012 , publier sur le site: www.ccdcoe.org, le site a été visité le: 23/11/2015.

فـــهـــــــرس الـــمـــوضـوعـــات

- فـهـرس المـوضـوعـات –

ملخــص البحـــــث.

1- ملخص البحث بالعربيــة.

2- ملخص البحث بالفرنسية.

1- ملخص البحث بالعربية:

أسهم إنتشار التكنولوجيات الحديثة في تغيير طرق ممارسة الدول لأنشطتها وإدارة مرافقها بتدرج مستويات أهميتها وحساسيتها، بتبنيها النمط الإلكتروني في الإدارة والاعتماد على أنظمة المعالجة الآلية للمعطيات في معالجة معلوماتها حتى السرية منها، إن تخزيناً أو إسترجاعاً أو نقلاً أو تبادلاً؛ مما استتبع تغير طرق الإعتداء على هذه المعلومات؛ لتتحول إلى طرق إلكترونية تتماشى مع الأساليب الحديثة في حفظ الأسرار، فظهر بذلك التجسس الإلكتروني في البيئة الإلكترونية كنشاط مواز للتجسس التقليدي في البيئة العادية، يطرح عديد الإشكاليات ويثير كثير الصعوبات لدراسته، تتعلق ابتداءً بغموض مفهومه وجدة الأطر التي تحكمه، كما أنه ونظراً لخصوصية البيئة الجديدة التي يرتكب فيها هذا النشاط فإن الطرق والآليات التقليدية لمكافحة التجسس لم تعد في أغلبها قادرة على مواكبة التغيير الحاصل؛ لأن كلا من السلوك الإجرامي ووسيلة ارتكابه والبيئة التي يتم على مستواها تغيرت لتأخذ شكلاً إلكترونياً غير محسوس، مع عدم القدرة على التحديد الدقيق للأضرار الحاصلة؛ وعليه كانت هذه الدراسة محاولةً للإحاطة بمفهوم هذا المصطلح المستجد، وتحديد مفرداته الأساسية، وكذا محاولةً لرصد الجهود المبذولة لمكافحته، سواء كانت جهوداً وطنية، أم جهوداً دولية، وذلك من خلال الإجابة على الإشكالية الآتية:

ما مدى فعالية الآليات الوطنية والإقليمية والدولية في مكافحة التجسس الإلكتروني، في ظل إزدواجية نظرة وتعامل الدولة الواحدة مع التجسس الإلكتروني من جهة، وتأثير التباين في أهمية مستويات الأمن (أمن وطني – أمن إقليمي– أمن دولي) من جهة أخرى؟.

2- Résumé de la recherche en français:

La propagation des nouvelles technologies a participé au changement des méthodes d'exercice des états de leurs activités, et à la gestion de leurs secteurs, selon leur degrés d'importance et de sensibilité, en adoptant le régime électronique dans l'administration, et en basant sur les systèmes de traitement automatique des donnés dans le traitement de leur information, y compris ceux qui sont secrètes, que ce soit dans le stockage, la récupération, le transfert ou l'échange, ce qui a conduit au changement des méthodes de portée atteinte à ces informations, par des méthodes électroniques, suivant les modalités modernes qui visent à préserver ses secrets. ainsi l'espionnage électronique est apparu sur l'environnement électronique comme activité parallèle à l'espionnage traditionnel dans l'environnement ordinaire, posant divers problématiques, et plusieurs difficultés, ayant relation initialement avec l'ambiguïté de son concept, et avec la nouveauté des règlement qui le gèrent. de ce fait et devant la particularité de l'environnement dans lequel déroule cette activité, les méthode traditionnelle de la lutte contre l'espionnage ne sont plus capable dans leurs majorité à suivre le rythme de changement effectif, à cause de comportement criminel et ses moyens, et l'environnement dans le quel il se déroule se sont transformés vers un modèle électronique non concret, avec l'incapacité de la détermination exacte des dommages engendrés. Ainsi cette étude a essayé d'entourer le concept de ce nouveau terme, et de précisé ses éléments essentiels, et a essayé aussi de quantifier les efforts déployés pour lutter contre ce phénomène, que ceux soient nationaux ou internationaux, et ceci en répondant au problématique suivant: quelle est l'envergure de l'efficacité des mécanismes, nationaux, territoriaux, et internationaux dans la lutte contre l'espionnage électronique, dans l'ombre du dédoublement de la vue, et du comportement de l'état unique face à l'espionnage électronique d'une part, et de l'influence de la différence de l'importance des niveaux de sécurité (sécurité nationale territoriale et internationale) d'autre part.