جامعة 20 أوت 1955 سكيكدة

كلية الحقوق والعلوم السياسة

قسم الحقوق

التجسس الإلكتروني ضد أمن الدولة

مذكرة مكملة لنيل شهادة الماستر تخصص قانون جنائي وعلوم الجنائية

من تقديم الطالبتين:

كركابو فطيمة

بحري سندس

تحت إشراف:

موات مجيد

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الصفة
د/بوعزيز شهرزاد	أستاذ محاضر	رئيسا
د/موات مجيد	أستاذ محاضر	مشرفا ومقررا
د/مقدم عبد الرحيم	أستاذ محاضر	مناقشا

دورة سبتمبر 2024

شكر وتقدير

الحمد والشكر لله عز وجل الذي هدانا بعونه ووفقنا لإتمام هذا العمل
فما كان لشيء أن يجري الا بمشيئته جل جلاله

كما يسعدنا أن نتقدم بخالص الشكر والتقدير

لأستاذنا المشرف "**موات مجيد**" الذي تكرم بإشرافه على هذه المذكرة
ومرافقته لنا في اعدادها من خلال التوجيه والإرشاد

كما نتقدم بخالص الشكر والتقدير لأعضاء لجنة المناقشة

المحترمين على قبولهم مناقشة مذكراتنا وتقييمهم لمجهودنا

إهـداء

الحمد لله الذي ما تم جهد ولا ختم سعي إلا بفضله

وما تخطى العبد من عقبات وصعوبات إلا بتوفيقه

وأما بعد

أهدي فرحة تخرجي إلى والدي الكريمين

وبالأخص "**أمي**" العزيزة أسأل الله أن يشفيها ويطيل عمرها

إلى إخوتي الأعزاء "**جمال، مريم، محمد**"

إلى أبناء أختي وبالأخص عزيزتي "**إسراء**"

إلى كل من كان سندا لي في إنجاز هذه المذكرة

ولو بالدعاء والكلمة الطيبة

فطيمة

إهـداء

سبحان الذي كان سبب في نجاحي وتوفيقي وسدادي

هو وحده لا شريك له سبحانه وتعالى الذي أنار طريقنا

واخرجنا من الظلمات إلى النور

أتقدم بإهدائي هذا

إلى كل من ساهم في نجاحي

أولا أشكر الله سبحانه وحده الذي وفقني إلى الوصول إلى المراتب العليا

واشكر والدي الكريمين أدامهما الله لي لفضلهما الكبير

وإلى كل عائلتي وكل من علمني معنى الكفاح

وإلى استاذي الكريم "موات مجيد" مشرفنا

إلى كامل أسرة الحقوق

سندس

فهرس المحتويات

فهرس المحتويات

الفصل الثاني

آليات المتابعة الجزائية للتجسس الإلكتروني ضد أمن الدولة في التشريع الجزائري

مقدمة

مقدمة:

إن التجسس جريمة كانت موجودة منذ قدم البشرية إذ كانت ترتكب بواسطة وسائل تقليدية كإرسال الجواسيس من دولة إلى دولة أخرى لجمع المعلومات، لكن الأمر اختلف في عصرنا الحالي الذي شهد نقلة نوعية جد متسارعة في مجال التطور العلمي والتكنولوجي في جميع الميادين خاصة فيما تعلق منها بالشبكات الرقمية وتنقل المعلومات، و بات يعرف عصرنا اليوم بعصر المعلومات أو عصر العولمة، بحيث تلاشت الحدود الجغرافية بين الدول والشعوب والأفراد وأصبح العالم مجرد قرية صغيرة، وإثر هذا التطور الحاصل اقترنت بعض الجرائم التقليدية بالوسائل التكنولوجية من بينها جريمة التجسس.

حيث أصبحت ترتكب في عصرنا هذا بوسائل ومعدات جد متطورة إذ أصبحت بما يسمى التجسس الإلكتروني وبتطور وسائل ارتكابها ازداد حجم خطر هذه الجريمة التي أصبحت تهدد شعوب ومجتمعات وأفراد بل وحتى دول بأكملها، فالدمار الذي قد يلحقه التجسس الإلكتروني بأنظمة المعلومات قد تعطل حياة المجتمعات وتهدد استقرار الدول أما الخسائر التي قد تنجم عنه أكبر بكثير مما قد يتصوره العقل، إذ أصبح بإمكان الجاسوس اليوم التجسس على دولة من دولة أخرى دون أن يتواجد بالدولة المستهدفة، فقد طغى التجسس الإلكتروني بإمكانياته الهائلة ودقة نتائجه على أساليب التجسس القديم وأصبحت الدول والحكومات العظمى والمتطورة تستخدمه لمعرفة أسرار الخصم أو من تسعى السيطرة عليه فلم تصبح الحرب اليوم حرب جنود ودماء وأسلحة إنما أصبحت حرب معلومات تتفوق فيما الدول التي تملك أكثر أساليب التجسس تطورا، ولا يرتبط التجسس الإلكتروني بالأسرار العسكرية فقط بل يشمل الأسرار الاقتصادية والاجتماعية بل وحتى السياسية وقد كانت الجزائر من بين إحدى الدول التي وقعت ضحية لهذه الجريمة المستحدثة كما قد وضعتها تحت خانة الجرائم الالكترونية.

تكمن أهمية الموضوع في أن التجسس الإلكتروني إلى جانب اعتباره من الجرائم الالكترونية فهو يعتبر كذلك جريمة ماسة بأمن الدولة والتي تشكل خطرا يهدد مصالحها واستقرارها خصوصا في ظل عصر العولمة، وينبع الهدف من هذه الدراسة في محاولة

عرض مفهوم لجريمة التجسس بشكلها المستحدث وعرض جهود الدولة الجزائرية في مكافحة هذه الجريمة من الناحية الاجرائية سواء من خلال قانونها الداخلي أو بتعاونها الدولي من خلال الاتفاقيات الدولية.

ومن الأسباب التي دفعتنا لاختيار موضوع "التجسس الإلكتروني ضد أمن الدولة" الأهمية البالغة لأمن الدولة، إذ يعد أهم الأولويات الأساسية التي تسعى كل دولة لتأمينها وحفظها من شتى أشكال التهديدات التي يمكن أن تطالها.

ومن أهم الصعوبات التي واجهتنا أثناء إعداد هذه المذكرة قلة المراجع والمؤلفات المتخصصة التي تعالج موضوع التجسس الإلكتروني ضد أمن الدولة، ولو أن هناك مجموعة من المراجع قد تطرقت الموضوع بشكل جزئي وأحيانا في بضعة سطور وبشكل سطحي نظرا لحداثة هذا الموضوع بالتالي صعوبة الإلمام بالموضوع والحصول على المعلومات الكافية.

ومن الدراسات السابقة التي تناولت موضوع التجسس الإلكتروني:

-رسالة دكتوراه بعنوان "جرائم الانترنت" للباحثة نبيلة هروال، حيث تطرقت لموضوع التجسس الإلكتروني في الباب الثالث الذي عنوانه جرائم العدوان على أمن الدولة عبر الانترنت تحديدا في الفصل الثاني منه الذي عنوانه التجسس عبر الانترنت، لكنها لم تتطرق للموضوع بشكل مفصل، إذ أنها اكتفت بعرض مفهوم لهذه الجريمة، إلا أنها لم تتطرق للموضوع من الناحية الإجرائية، وهذا تطرقنا إليه في مذكرتنا "التجسس الإلكتروني ضد أمن الدولة"، في الفصل الثاني تحت عنوان آليات المتابعة الجزائية للتجسس الإلكتروني ضد أمن الدولة في التشريع الجزائري.

-رسالة دكتوراه بعنوان "آليات مكافحة التجسس الإلكتروني" للباحثة نادية سلامي، حيث ألمت بموضوع التجسس الإلكتروني من نواحي عديدة سواء من الناحية المفاهيمية أو الإجرائية.

ولعل أهم إشكال يطرح هذا الموضوع هو:

- إلى أي مدى استطاع المشرع الجزائري مواكبة تطور جريمة التجسس التي تستهدف أمن الدولة باستعمال وسائل مستحدثة؟ وما مدى فعالية النصوص القانونية التي أوجدها في مواجهة التجسس الإلكتروني وتحييد آثاره؟

بالنسبة للمنهج المعتمد في هذه الدراسة فقد اخترنا المنهج الوصفي التحليلي، إذ أنه وصفي من خلال التطرق من جهة لوصف جريمة التجسس الإلكتروني ذلك من خلال تعريفها وذكر خصائصها وأركانها، ومن جهة أخرى يضم التحليل من خلال دراسة الآليات التي استحدثها المشرع في متابعة التجسس الإلكتروني وهذا ما تم استخلاصه من خلال النصوص القانونية.

وللإجابة على إشكالية البحث تم تقسيم البحث إلى فصلين حيث تطرقنا في الفصل الأول إلى الأحكام العامة لجريمة التجسس الإلكتروني ضد أمن الدولة والذي قسمناه إلى مبحثين تناول كل منهما ماهية التجسس الإلكتروني ضد أمن الدولة، والإطار الموضوعي لجريمة التجسس الإلكتروني ضد أمن الدولة، أما الفصل الثاني فقد تناولنا فيه آليات المتابعة الجزائية للتجسس الإلكتروني ضد أمن الدولة في التشريع الجزائري، وقد قسمناه أيضا لمبحثين حيث تطرقنا في المبحث الأول لمتابعة التجسس الإلكتروني في ظل التشريع الجزائري، وتناولنا في المبحث الثاني مكافحة التجسس الإلكتروني في إطار الاتفاقيات الدولية.

الفصل الأول

الأحكام العامة لجريمة التجسس الإلكتروني ضد أمن الدولة

شهد العالم في عصرنا الحالي ثورة في الاتصالات والمعلومات أسهم ذلك في ظهور نمط جديد من الجرائم المستحدثة من بينها جريمة التجسس الإلكتروني، والتي تعتبر من بين أكثر الجرائم خطورة خاصة ذلك التجسس الذي يمس بأمن الدولة، حيث استخدمته الحكومات والدول لتجميع المعلومات الاستخبارية وأسرار أعدائها أو الدول التي تسعى للسيطرة عليها واستخدام هذه الأسرار والمعلومات لتدميرها فيما بعد، وقد انتشرت هذه الجريمة انتشارا واسعا في الآونة الأخيرة إذ أصبحت شبحا يهدد مصالح دول بأكملها سواء كانت متقدمة أو نامية على حد سواء.

ولدراسة هذه الجريمة قسمنا الفصل إلى مبحثين سنتناول ماهية التجسس الإلكتروني ضد أمن الدول (المبحث الأول)، ثم بعد ذلك سنتطرق إلى الإطار الموضوعي لجريمة التجسس الإلكتروني ضد أمن الدولة (المبحث الثاني).

المبحث الأول

ماهية التجسس الإلكتروني ضد أمن الدولة

بالرغم من ما قدمته التكنولوجيا الحديثة من ايجابيات ومنافع فقد منحت بالمقابل تقنيات متطورة استغلتها بعض الأطراف بشكل سلبي ودمجت بعض الجرائم بالتقنيات المتطورة لتصبح جرائم جديدة ذات مفاهيم مستحدثة، من بينها جريمة التجسس الالكتروني والتي تفرض وجوب تحليلها وبيان مدلولها، وعليه سيتم الإلمام بماهية التجسس الإلكتروني ضد أمن الدولة من خلال تبيان الملامح التعريفية للتجسس الإلكتروني و المقصود بأمن الدولة (المطلب الأول)، والتطرق إلى خصائص التجسس الإلكتروني (المطلب الثاني)، وسنتناول وسائل ارتكاب جريمة التجسس الالكتروني ضد أمن الدولة (المطلب الثالث).

المطلب الأول

تعريف التجسس الإلكتروني ضد أمن الدولة

تعتبر جريمة التجسس من الجرائم الماسة بأمن الدولة وكيانها سواء في التشريع الجزائري أو في التشريعات الأخرى وإثر اقتران هذه الجريمة بالوسائل التكنولوجية أصبحت بما يسمى التجسس الالكتروني ولضبط مفهوم هذه الجريمة قسمنا المطلب إلى فرعين حيث سنتناول تعريف التجسس الإلكتروني (الفرع الأول)، وسنتطرق إلى تعريف أمن الدولة (الفرع الثاني).

الفرع الأول

تعريف التجسس الإلكتروني

ندرس في هذا الفرع التجسس الإلكتروني من الناحية القانونية، ثم نحاول فحص مدلوله من وجهة نظر الفقه.

أولا–من الناحية القانونية:

إذا رجعنا لنص قانون العقوبات الجزائري سنلاحظ أن المشرع الجزائري لم يعطنا تعريفا واضحا ودقيقا لجريمة التجسس الإلكتروني على خلاف التجسس التقليدي، لكنه فيما بعد نص على تجريم التجسس الإلكتروني وبين مجموعة الأفعال المكونة لهذه الجريمة من خلال تعديل قانون العقوبات سنة 2004 وذلك ليواكب التطور الذي مس المجال التقني[1].

حيث وضع المشرع الجزائري القانون رقم 04–15 المعدل والمتمم لقانون العقوبات وجرم الأفعال التي ترتكب بواسطة الوسائل التقنية لأول مرة تحت اسم جرائم المساس بأنظمة المعالجة الآلية للمعطيات من المادة 394 مكرر إلى غاية المادة 394 مكرر 07[2].

و تجدر الإشارة أن المادة 394 مكرر3 تنص على أن: "**تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، دون الاخلال بتطبيق عقوبات أشد**"[3].

يفهم من نص هذه المادة أنه إذا ارتكبت إحدى الجرائم الماسة بأمن الدولة من بينها التجسس باستخدام أنظمة المعالجة الآلية المعطيات فإنه تطبق عليها عقوبتها لأن جرائم المساس بأمن الدولة تكون عقوبتها أشد من العقوبات المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر2.[4]

وتوقع عقوبة الإعدام على الجاسوس سواء ارتكب جريمة التجسس العادية كما حددت أركانها المادة 64 من قانون العقوبات وسواء ارتكبها بواسطة وسائل تقنية.[5]

(1) نادية سلامي، آليات مكافحة التجسس الالكتروني، رسالة دكتوراه، جامعة العربي التبسي، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2019، ص23.

(2) إلهام بن خليفة وجمال غريسي، "التجسس الإلكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري"، مجلة دفاتر السياسة والقانون، جامعة الشهيد حمة لخضر، الوادي، مجلد 14، عدد 01، 2022، ص 155.

(3) قانون رقم 04–15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004 المعدل والمتمم للأمر رقم66–156 المتضمن قانون العقوبات، جريدة رسمية، عدد71.

(4) إلهام بن خليفة وجمال غريسي، المرجع السابق، ص155.

(5) المرجع نفسه، ص156.

يستخلص من مواد القسم السابع مكرر الذي ذكر سابقا الأفعال المكونة لجريمة التجسس الإلكتروني، إذا كان هدفها الإضرار والمساس بالدفاع الوطني وتتمثل في فعل الدخول والبقاء في المنظومة المعلوماتية وتخريبها أو إدخال أو إزالة أو تعديل المعطيات أو تصميم أو بحث أو توفير أو تجميع أو نشر أو الإتجار في المعطيات سواء كانت مخزنة أو معالجة أو مرسلة بواسطة المنظومة المعلوماتية[1].

كما تناولت التشريعات الغربية والعربية جريمة التجسس الإلكتروني، فمثلا التشريع الفرنسي نص عليه من خلال المواد 411-6 إلى غاية 411-9 من قانون العقوبات الفرنسي الجديد، حيث جاء أن التجسس الالكتروني يمكن أن يرتكب عن طريق جمع أو إتلاف بيانات معلوماتية أو تسليم أو تسهيل تسليم إلى دولة أجنبية أو أحد عملائها قصد الاضرار بسلامة الدولة.[2]

ثانيا-من الناحية الفقهية:

تعددت تعاريف التجسس الإلكتروني، فمصطلح التجسس في حد ذاته متشعب ولا يمكن أن نحصره بتعريف واحد، إلا أنه عرفه البعض بأنه أحد صور الإرهاب الإلكتروني الذي يقوم باستعمال التكنولوجيا بشكل سلبي بغية إحداث أضرار وآثار مدمرة لمحطات التحكم والأجهزة التقنية وشبكات الاتصال سواء كان بدافع سياسي أوديني أو عرقي.[3]. وهناك من يعرف التجسس الإلكتروني على أنه: "استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الإلكترونية الخاصة بالدول والحكومات والتنصت عليها بقصد الحصول على ما لديها من معلومات مهمة تتعلق بنظامها

(1) نادية سلامي، المرجع السابق، ص24.

(2) هبة نبيلة هروال، جرائم الانترنت، دراسة مقارنة، رسالة دكتوراه، جامعة أبي بكر بلقايد، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2014، ص376.

(3) فايزة نجاري بن حاج علي، "جريمة التجسس الإلكتروني"، استراتيجيا مجلة دراسات الدفاع والاستقبالية، المعهد العسكري للوثائق و التقويم و الاستقبالية، لوزارة الدفاع الوطني، الجزائر، مجلد 6، عدد11، 2019، ص66.

وأسرارها، تشمل جميع المعلومات العسكرية والأمنية، والسياسية، والاقتصادية، والعلمية والاجتماعية".[1]

ربط هذا التعريف أمن الدولة بالمعلومات في المجال العسكري والأمني والسياسي والاقتصادي والعلمي والاجتماعي، حيث تعد هذه الأسرار دعامة وركيزة الدولة إذا كشفت صارت فريسة سهلة للدول المعادية.

ويمكن تعريفه أيضا بأنه: "العمليات التي تحصل من خلال الانترنت، لغرض جمع المعلومات الاستخبارية من أجهزة الكمبيوتر، أو أنظمة المعلومات أو الاتصالات أو الشبكات، من دون معرفة أو رضا الضحية".[2]

أو هو "أن يقوم أحد الأشخاص غير المصرح لهم بالدخول إلى نظام التشغيل بطريقة غير شرعية لتحقيق أغراض غير شرعية، إما بالسرقة أو التخريب أو عن طريق التحكم في نظام التشغيل، ويتحقق ذلك متى كان الدخول مخالف لإرادة صاحب النظام كاختراق البيانات الشخصية".[3]

وليس هناك اختلاف بين جريمة التجسس التقليدية وجريمة التجسس الإلكتروني سوى من ناحية الأداة المستخدمة، وهي تكنولوجيا المعلومات التي سهلت على الجاسوس تنفيذ جريمته بعيدا عن الأعين بسهولة وحرية.[4]

وتشبه عملية الاختراق في جريمة التجسس الإلكتروني الدخول إلى ذاكرة الإنسان، كما يمكن أن يكون للاختراق دليل مادي على أن الجاني اخترق بالفعل النظام المعلوماتي ويشترط أن يتحقق فعل الدخول بأي وسيلة تكنولوجية كانت سواء باستعمال كلمة سر حقيقية

(1) سامية بوشوشة وحياة سلماني، "التجسس الالكتروني وطرق مكافحته"، مجلة العلوم الاجتماعية والانسانية، جامعة باجي مختار، عنابة، مجلد 16، عدد 01 ،2023، ص53.

(2) فاطمة الظبيري، "القانون الدولي والهجمات الإلكترونية ما دون استخدام القوة"، المجلة الدولية للقانون، مجلد11، عدد1، 2022، ص232.

(3) فتيحة خالدي، "تأثير التجسس الالكتروني على الحق في الخصوصية المعلوماتية"، مجلة البحوث في الحقوق والعلوم السياسية، مجلد7، عدد1، 2021، ص305.

(4) سامية بوشوشة وحياة سلماني، المرجع السابق، ص52.

أو استعمال شفرة خاصة أو برنامج معين، ويتحقق الدخول غير المشروع متى كان يخالف إرادة صاحب النظام وكذلك مما يتعلق بأسرار الدولة ودفاعها.[1]

الفرع الثاني

تعريف أمن الدولة

يعرف البعض أمن الدولة انطلاقا من فكرة العناصر الثلاثة المكونة للدولة وهي: الاقليم الحكومة والشعب، وأمن الدولة يطاله الانتهاك إذا تم المساس بسلامة إقليمها واستقرار مؤسساتها الحكومية واحترام الحقوق الأساسية للشعب، وإذا تم الاعتداء على أحد هذه العناصر الثلاثة تكون الدول في حالة دفاع شرعي من أجل رد الاعتداء، وينتهك أمن الدولة من الخارج من خلال شن حرب عليها تهدد سلامتها الاقليمية، كما تطاله أيادي عدائية من الداخل لزعزعة أمنها واستقرارها من الداخل، ويعد الدفاع الوطني من أهم مرتكزات أمن الدولة.[2]

المطلب الثاني

خصائص التجسس الإلكتروني

باعتبار أن التجسس الإلكتروني هو صورة من صور التجسس التقليدي ظهر نتيجة التطور التكنولوجي فكلاهما يشتركان في خصائص ويختلفان في بعضها، ومن خلال هذا المطلب سنتطرق إلى الخصائص المشتركة بين التجسس الإلكتروني والتجسس التقليدي (الفرع الأول)، والخصائص المميزة للتجسس الإلكتروني عن التجسس التقليدي (الفرع الثاني).

(1) حفصي عباس، "التجسس الإلكتروني في الشريعة والقانون"، مجلة الواحات للبحوث والدراسات، مجلد12، عدد1، 2019، ص273.

(2) International Reviem of red crass, H. Montealegre Klenner: la sécurité de l'état et les droits de l'homme. https://www.google.com /search? client: fire fox-b. la sécurité + de + l'état+ et + les + droits + de + l'homme consulté le 25 mai 2024.

الفرع الأول

الخصائص المشتركة بين التجسس الإلكتروني والتجسس التقليدي

إن التجسس الإلكتروني يشترك مع التجسس التقليدي في كونهما كلاهما جريمتين تمسان بأمن الدولة فالدولة كما الأفراد لها قيم ومصالح وحقوق أساسية تعمد إلى صونها بالقانون الجزائي، وتنقسم الحقوق الأساسية للدولة لزمرتين، زمرة حقوق تشتقها الدولة من طبيعة كونها تجسيدا للأمة في علاقاتها مع الأمم الأخرى في الميدان الدولي وتستمد هذه الحقوق بصفتها شخصا من أشخاص القانون الدولي.[1]

وزمرة الحقوق التي لا غنى للدولة عن ممارستها وحمايتها لكي تتمكن أجهزتها من النهوض بأعباء الحكم والقيام بوظائفها الأساسية وتشتق الدولة هذه المهام من طبيعتها كحكومة وتمارس هذه الحقوق بصفتها شخصا من أشخاص القانون الداخلي، وتبعا لتقسيم حقوق الدولة لطائفتين جرائم أمن دولة داخلي وجرائم أمن دولة خارجي فيقصد بالجرائم الماسة بأمن الدولة الخارجي الأفعال المجرمة التي تقع على الدولة في علاقتها بالدول الأخرى ويراد منها زعزعة كيانها في المحيط الدولي ويندرج التجسس الإلكتروني ضمن طائفة الجرائم الماسة بأمن الدولة الخارجي شأنه شأن جريمة التجسس التقليدي.[2]

ويشترك التجسس الالكتروني مع التجسس التقليدي في كونهما يرتكبان من قبل فرد أجنبي بمعنى أن يكون الجاني حاملا لجنسية دولة أخرى، فقد ذهبت معظم التشريعات في هذا الصدد إلى الأخذ بمعيار جنسية الفرد كمعيار للتفرقة بين جريمة التجسس والخيانة، ومنها المشرع الجزائري فرباط الجنسية يفرض على المواطن واجب الولاء لدولته ومن أولويات هذا الولاء ألا يرتكب جريمة تؤثر على أمنها. فالمواطن الذي يخون هذا الواجب هو أشد

(1) نادية سلامي، المرجع السابق، ص31.

(2) المرجع نفسه، ص ص31-32.

إجراما وأكثر خطرا من ذلك الأجنبي الذي يقدم على إيذاء سلامة الدولة الأخرى لخدمة وطنه، فالأول خائن أما الثاني فيعتبر جاسوسا.[1]

الفرع الثاني

الخصائص المميزة للتجسس الإلكتروني عن التجسس التقليدي

تتميز الجريمة المعلوماتية بخصائص تختلف فيها عن الجريمة التقليدية باعتبار أن التجسس الإلكتروني يندرج تحت خانة الجرائم المعلوماتية.

فالجريمة المعلوماتية جريمة عابرة للحدود وتتسم غالبا بالطابع الدولي، مما جعل معظم دول العالم في حالة اتصال دائم على الخط مما سهل ذلك ارتكاب الجريمة من دولة لأخرى كونها جريمة عابرة القارات، حيث يمكن من خلال هذا النظام ارتكاب عدة جرائم مثال: الاحتيال المعلوماتي، سرقة بطاقات الائتمان، القرصنة وغسيل الأموال.[2]

وتتميز بكونها جرائم صعبة الاثبات فهي تعتبر جريمة مستحدثة تمثل ظاهرة اجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، كما تتسم بصعوبة اكتشافها ومتابعتها، بحيث لا تترك أثر فهي مجرد أرقام تتغير في السجلات. فمعظم الجرائم المعلوماتية تم اكتشافها فجأة وبعد وقت طويل من ارتكابها.[3]

تتميز بكونها صعبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، حيث أن الجاني المعلوماتي يستطيع أن يمحو ويغير البيانات والمعلومات الموجودة في الكمبيوتر لذلك فإن هناك دور للمصادفة وسوء الحظ في أساليب التدقيق والرقابة ومعظم الجناة الذي تم توقيفهم إما أنهم تصرفوا بغباء أو لم يستخدموا الأنظمة الالكترونية بمهارة وتدقيق.[4]

(1) نفس المرجع و الموضع.

(2) خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية شارع زكريا غنيم الابراهيمية، الإسكندرية، 2008، ص44.

(3) راوية هدى وجرادي فاطمة الزهراء، الإطار الموضوعي للجريمة المعلوماتية، مذكرة ماستر، جامعة ابن خلدون، كلية الحقوق والعلوم السياسية، قسم الحقوق،2019.

(4) خالد ممدوح إبراهيم، المرجع السابق، ص46.

كما أن التجسس الالكتروني جريمة ترتكبها فئة خاصة؛ فالجاسوس الإلكتروني يعتمد على الآلات وعلى مقدراته الذهنية، وأصبح الجاسوس يقاس بموهبته في قرصنة الشفرات والرموز الذي تتيح له الدخول لقواعد البيانات .[1]

المطلب الثالث

وسائل ارتكاب جريمة التجسس الإلكتروني ضد أمن الدولة

ذكرت المادة الثانية فقرة (أ) من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أن: "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية المعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".[2] وبحسب هذه المادة يمكن استخلاص أن التجسس الذي نص عليه المشرع في المادة 64 من قانون العقوبات يمكن ارتكابه باستخدام نظام اتصالات متطورة أو باستخدام أنظمة معالجة آلية للمعطيات.[3]، وهذا ما سنتطرق إليه من خلال التجسس المرتكب بأنظمة الاتصالات (الفرع الأول) والتجسس المرتكب بأنظمة المعالجة الآلية للمعطيات (الفرع الثاني).

(1) نادية سلامي، المرجع السابق، ص37.

(2) قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، جريدة رسمية، عدد47، الصادر بتاريخ 25 شعبان عام 1430 الموافق 16 غشت سنة 2009.

(3) إلهام بن خليفة وجمال غريسي، المرجع السابق، ص161.

الفرع الأول

التجسس المرتكب باستخدام أنظمة الاتصالات

تطورت وسائل التجسس الإلكتروني و أصبحت الدول المتطورة تعتمد على وسائل وأساليب جديدة متطورة تتيح لها اختراق كل حواجز أسرار الدول دون كشفها وقد تعددت هذه الوسائل.[1]، سنذكر بعضها:

أولا–التجسس باستخدام الأقمار الصناعية:

يقتصر التجسس الالكتروني باستعمال الأقمار الصناعية على الدول المتطورة فقط، والتي تتحكم في جميع البيانات في العالم حيث تقوم بابتكار أقمارها الصناعية بنفسها.[2]

وتعتبر الأقمار الصناعية من أهم وسائل التجسس في عصرنا الحالي ويرتبط عملها بالحواسيب والتي تقوم بتحليل ما يتم التقاطه، وقد تم اطلاق الأقمار الصناعية نتيجة التسابق نحو الفضاء الذي كان بين الولايات المتحدة الأمريكية والاتحاد السوفياتي فكان أول من أطلق قمرا صناعيا الإتحاد السوفياتي والذي أسماه "سبوتنيك1" في 4 أكتوبر1957، وقد أطلق قمرا آخر "سبوتنيك 2".[3]

وقد باتت أقمار التجسس وسيلة أساسية لتوفير مستوى كاف من المخزون المعلوماتي، فهي تحتوي على كاميرات عالية الدقة والقوة وأجهزة استشعار تعمل بواسطة الأشعة تحت الحمراء أو أجهزة استشعار حرارية وأجهزة كشف الحركة ليحدد بها مواقع الدبابات والصواريخ والسفن والطائرات الحربية، وتقوم برصد الرسائل اللاسلكية والميكروويفية من الأعداء ولا يخفى شيء عن هذه الجواسيس الصامتة في الفضاء.[4]

(1) المرجع نفسه، ص164.

(2) فايزة نجاري بن حاج علي، المرجع السابق، ص67.

(3) نادية سلامي، المرجع السابق، ص86.

(4) فتيحة مناد، "مدى شرعية الاستطلاع العسكري والتجسس من الفضاء الخارجي باستخدام الأقمار الصناعية–دراسة قانونية"، مجلة القانون العام الجزائري والمقارن، مجلد 4، عدد2، 2018، ص ص160–161.

كما تقوم الدول المتقدمة بمراقبة العالم باستخدام أقمارها الصناعية حيث وصلت أعدادها في العالم إلى 500 قمر صناعي عسكري وتمتلك الولايات المتحدة فقط حوالي 50 منها، تكلفتها ليست باهظة كما أن فترة صناعتها قصيرة لا تتعدى السنة. وتزعم هذه الدول أن الأقمار التي تقوم بإطلاقها مدنية وليست عسكرية لتقوم بخداع العالم وايهامه بأنها تطلق أقمارها ضمن حدودها لأغراض مدنية ولن تستخدمها لغرض التجسس على الدول الأخرى، ذلك أن القوانين قد حظرت إطلاق أقمار صناعية بدافع التجسس.[1]

كما تعد الأقمار الصناعية من أخطر الوسائل للتجسس ذلك أنه من الصعب تفادي التجسس بها لعدة أسباب من أهم هذه الأسباب أن هذه الوسيلة تمتلكها بعض الدول المتقدمة فقط، كما أنه يصعب الكشف عن هذه الأقمار بسبب أنها تمتلك الحرية في التجول في الفضاء لأن الفضاء لا يخضع لسيادة دولة محددة لذا لا يمكن التحجج بفكرة السيادة لمنع عمل تلك الأقمار الفضائية.[2]

ثانيا-التجسس باستخدام برنامج بيغاسوس:

تحتل اسرائيل المرتبة الأولى في عمليات التجسس الإلكتروني على الدول حيث تمتلك 27 شركة مختصة في هذا المجال، وحيث أن بريطانيا وأمريكيا وفرنسا وروسيا والصين لن تمتلك هذا العدد مجتمعة. كما تمتلك إسرائيل 8200 وحدة لتنفيذ الحرب الالكترونية والتجسس على الدول.[3]

ويعتبر برنامج بيغاسوس الإسرائيلي من الوسائل الحديثة الخطيرة والمتطورة في مجال التجسس، حيث يمكن أن يثبت على أجهزة بعض إصدارات نظام "آبل" أو نظام آخر من أجل التجسس على معلومات الشخص المستهدف بما فيها من ملفات وصور ووسائط، واكتشف هذا البرنامج في أغسطس 2016 ذلك بعد فشل في تثبيتها على هاتف أحد الناشطين حيث تفطنت الشركة لهذه الثغرة، وبشكل عام برنامج بيغاسوس بإمكانه تتبع

(1) الهام بن خليفة وجمال غريسي، المرجع السابق، ص164.

(2) نفس المرجع والموضع.

(3) مريم بناش وسعاد بولقرون، "التجسس وانتهاك حق الخصوصية في العصر الرقمي دراسة وصفية تحليلية لبرنامج (بيغاسوس)"، مجلة الدراسات الإعلامية والاتصالية، مجلد2، عدد3، 2022، ص70.

المكالمات والرسائل وجمع كلمات السر وتتبع الموقع وجمع المعلومات التي تقوم بتخزينها التطبيقات.[1]

ولا يعمل البرنامج من تلقاء نفسه بل يقوم بالاستهداف من خلال دفع الضحية للنقر على رابط خبيث مما يمكن من تحميل بيغاسوس الذي يكسر نظام "أي أو إس" على الجهاز المستهدف والتمكن من التجسس على ما يحتويه من بيانات ومعلومات.[2]

كما اشتهر هذا البرنامج في العديد من القضايا والفضائح حول العالم والتي تناقلتها مختلف وسائل الإعلام حول تسربات مست شخصيات معروفة كثيرة حول العالم ومست حتى دولا كبيرة، وساهمت في سقوط العديد من الشخصيات على الساحة الدولية مما سبب ذلك في خلق صراعات وأزمات داخل الدول.[3]

ثالثا-التجسس باستخدام حصان طروادة:

يعد حصان طروادة من بين برامج التجسس الإلكتروني الحديثة، حيث يمكن ارتكاب جريمة التجسس عن طريق إدخال ملف تجسسي إلى الضحية يدعى حصان طروادة ويعرف بأنه الحصان الخشبي الذي استعمل لمحاصرة طروادة وخداعه في الحرب، إذ لم يتمكن المهاجمون من اقتحام حصون طروادة فاستعملوا هذه الطريقة كفخ بترك الجيش بعد انسحابه حصانا خشبيا فأخذه أهل طروادة وأدخلوه الحصن ولم يكتشفوا أن جنود الأعداء مختبئون فيه.[4]

تماما كحالات التجسس الإلكتروني، يقوم الملف بالدخول لجهاز الشخص المستهدف ويغير من موقعه و هيئته، ولهذا السبب اعتبر حصان طروادة من أخطر وسائل التجسس ذلك أنها تدخل الأجهزة في صمت وهدوء دون الإنتباه لوجودها حتى في ظل وجود برامج

(1) نفس المرجع والموضع.

(2) المرجع نفسه، ص71.

(3) المرجع نفسه، ص73.

(4) عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، الطبعة الأولى، دار المستقبل للنشر والتوزيع، عمان، 2009، ص ص198-199.

مضادة للفيروسات، و لا يعتبر برنامج حصان طروادة فيروسا بل ملف تجسس حيث يمكن للمجرم من خلاله السيطرة بشكل كامل على جهاز الضحية بسهولة دون اكتشاف وجوده على الجهاز.[1]

وتعد تلك الانتهاكات التجسسية جرائما ترتكب في حق الأفراد وحتى الدول ، حيث أصبحت المجتمعات تشهد العشرات من هذه الجرائم التي تتم بواسطة الوسائل التقنية.[2]

رابعا–التجسس باستخدام أجهزة البوليمرات:

"تصنع أجهزة البوليمرات من مادة من نوع خاص من "البوليمرات" ابتكرها باحثون في الجمعية الكيميائية الأمريكية يمكن أن تدمر نفسها ذاتيا وتختفي من دون ترك أي أثر بعد أداء مهمتها السرية، وبمكن استخدمها لتصنيع أجهزة الاستشعار والتجسس الإلكترونية، حيث تلقى في أرض العدو للاستطلاع وتخزين المعلومات قبل تدمير نفسها والاختفاء كأنها لم تكن موجودة من الأساس، إذ أن هذه المادة لا تتحلل ببطء على مدار عام مثل المواد البلاستيكية بل تختفي في لحظات عندما تتلقى أمر التدمير الذاتي".[3]

خامسا–التجسس باستخدام تقنية البيوبوت:

المقصود بتقنية البيوبوت تسخير ما هو موجود في الطبيعة وإعداده تقنيا لتنفيذ مهام متنوعة يمكن أن تفيد البشرية لتنتج ما يسمى الأحياء الآلية "بيوبوت"، وهي عبارة عن كائنات يتم تسييرها بواسطة الوسائل التقنية أي أن أدمغتها مرتبطة بتقنيات لاستعمالها في تنفيذ مهام عديدة كالتجسس ومنها الصرصار الجاسوس والذي ابتكرته الباحثة "هونغ ليانغ" في جامعة تكساس.[4]

(1)عبد الحكيم رشيد توبة، المرجع السابق، ص201.

(2) نفس المرجع والموضع.

(3) إلهام بن خليفة وجمال غريسي، المرجع السابق، ص165.

(4) نفس المرجع والموضع.

الفرع الثاني

التجسس المرتكب بواسطة أنظمة المعالجة الآلية للمعطيات

إذا استهدف الجاسوس الأجنبي بمساسه لنظام المعالجة الآلية للمعطيات الدفاع الوطني فإنه بذلك يكون جاسوسا إلكترونيا وتوقع عليه عقوبة الإعدام، لأن العقوبة التي وصفها المشرع لجريمة التجسس أشد من مضاعفة عقوبات جرائم المساس بأنظمة المعالجة الآلية للمعطيات،[1] وقد ذكر المشرع ثلاث صور منها كالتالي:

أولا–الدخول أو البقاء في منظومة المعالجة الآلية للمعطيات:

تعد جريمة الدخول أو البقاء غير المشروع في منظومة المعالجة الآلية للمعطيات مرحلة تمهيدية تسبق الجرائم التي تستهدف البيانات الموجودة داخل هذا النظام كجريمة التجسس،[2] وقد نص على جريمة الدخول أو البقاء عن طريق الغش في نص المادة 394 مكرر كما يلي: "**يعاقب بالحبس من ثلاث (03) أشهر إلى سنة (1) وبغرامة من 50.000دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 إلى 150.000دج**".[3]

تتكون الجريمة من ركن مادي يتمثل في فعل الدخول أو البقاء في كل أو جزء من نظام المعالجة الآلية للمعطيات ويكفي قيام أحد الفعلين لتحقق الجريمة.[4]

(1) إلهام بن خليفة وجمال غريسي، المرجع السابق، ص161.

(2) نادية سلامي، المرجع السابق، ص208.

(3) قانون 04–15 المتضمن قانون العقوبات، المرجع السابق.

(4) إلهام بن خليفة وجمال غريسي، المرجع السابق، ص162.

أما الركن المعنوي يعد فعل الدخول أو البقاء جريمة عمدية تقوم على القصد الجنائي العام، والذي علم الجاني بأنه ليس له الحق بالدخول أو البقاء داخل النظام وأن فعله ضد رغبة مالك النظام، ومع ذلك تنصرف إرادته لإتيان هذا الفعل المخالف للقانون والمخالف لإرادة صاحب النظام.[1]

ثانيا-الاعتداء على سلامة المعطيات:

نص المشرع على الاعتداء على سلامة المعطيات في المادة 394 مكرر 1 بقوله: "**يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة مالية من 500.000 دج إلى 2.000.000دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها**".[2]

يتمثل الركن المادي لهذه الجريمة إما بصورة إجراء تعديلات أو تدميرها أو الإدخال غير المشروع للمعلومات داخل النظام.[3]

كما أن جريمة الإعتداء على سلامة المعطيات جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بأن تتجه إرادة الجاني لفعل من الأفعال المذكورة سابقا سواء إدخال، إزالة، تعديل مع علم الجاني بأن هذه الأفعال تشكل جريمة اعتداء.[4]

ثالثا-التعامل في معطيات غير مشروعة:

نص المشرع الجزائري على الأفعال التي تشكل هذه الجرائم في المادة 394 مكرر 2 من قانون العقوبات كالتالي: "**يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج، كل من يقوم عمدا وعن طريق الغش بما يلي:**

(1) نفس المرجع والموضع.

(2) قانون 04-15 المتضمن قانون العقوبات، المرجع السابق.

(3) بسمة مامن، "جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري"، مجلة الحقوق والعلوم السياسية، مجلد9، عدد1، 2022، ص485.

(4) نفس المرجع والموضع.

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار 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".[1]

ويتضح من خلال نص المادة أن جريمة التعامل في معطيات مشروعة لها صورتين:

أ-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 الماسة بأنظمة المعالجة الآلية للمعطيات:

تقوم الجريمة على ركن مادي يتمثل في أن الجاسوس يقوم بتصميم أو اختراع أو بحث أو تجميع أو توفير أو نشر أو بيع أو شراء بيانات معلوماتية شرط أن تكون مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية من شأنها تسهيل ارتكاب الجرائم الماسة بأنظمة المعالجة الآلية مثل تصميم الجاني لكود يمكن من خلاله الدخول لنظام المعالجة الآلية للمعطيات والتجسس على معلومات سرية تتعلق بدفاع الدولة ومن ثم اتلافها أو تغييرها بما يخدم مصالح الدول المعادية أو حتى تسليمها لها.[2]

ويقوم الركن المعنوي على قصد عام يتمثل في اتجاه إرادة الجاني لأي من الأفعال المذكورة سابقا مع علمه بأن نشاطه بشكل جريمة تعامل غير مشروع في المعطيات، ويتوفر على قصد جنائي خاص متمثل في استهدافه من وراء الأفعال المذكورة سابقا التمهيد لاستعمال المعطيات المترتبة عنها في ارتكاب جريمة تمس بأنظمة المعالجة الآلية للمعطيات.[3]

(1) قانون 04-15 المتضمن قانون العقوبات، المرجع السابق.

(2) إلهام بن خليفة وجمال غريسي، المرجع السابق، ص163.

(3) نادية سلامي، المرجع السابق، ص221.

ب-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم الماسة بنظام المعالجة الآلية للمعطيات:

يقوم الركن المادي لهذه الجريمة على توافر أحد الأفعال المذكورة في المادة سابقا، تتمثل هذه الأفعال في فعل الحيازة أو الإفشاء أو النشر أو الاستعمال، أما الركن المعنوي يتمثل في أنها جريمة عمدية تقوم على توافر القصد الجنائي العام لدى مرتكب الجريمة.[1]

المبحث الثاني

الإطار الموضوعي لجريمة التجسس الإلكتروني

جريمة التجسس الإلكتروني تعتبر تهديدا خطيرا لما لها من تداعيات تهدد استقرار الدول وعلى ضوء ذلك توجب علينا الإحاطة بموضوع هذه الجريمة الخطيرة بتبيان أركان التجسس (المطلب الأول)، والتطرق إلى محل التجسس الالكتروني (المطلب الثاني) وصولا إلى أبعاد التجسس الإلكتروني (المطلب الثالث):

المطلب الأول

أركان جريمة التجسس

بما أن جريمة التجسس الإلكتروني هي صورة من صور التجسس التقليدي تختلف فقط من حيث الوسيلة المستعملة وما ينطبق على جريمة التجسس من أركان نطبقه على الصورة المستحدثة للتجسس التي تتجلى في التجسس الإلكتروني، حيث سنتناول الركن المادي (الفرع الأول) والركن المعنوي (الفرع الثاني) ثم سنتطرق إلى الركن الشرعي لجريمة التجسس (الفرع الثالث).

الفرع الأول

الركن المادي

(1) نفس المرجع، ص223.

يتكون الركن المادي لجريمة التجسس كأي جريمة من ثلاثة عناصر تتمثل في النشاط الإجرامي والنتيجة والعلاقة السببية.

أولا-النشاط الجرمي:

هو توصل الفاعل لسرقة أو الحصول على ما يريده كما أن المشرع لم يحدد وسيلة معنية للسرقة أو الاستحصال سواء كان بطريقة مباشرة أو غير مباشرة أو بطريقة بسيطة أو معقدة أو صريحة أو ملتوية،[1] كما هو الحال في جريمة التجسس الالكتروني فالسرقة تحصل بوسائل الكترونية.

كما تجدر الإشارة أن المشرع لم يشترط صفة معنية في الفاعل، كما لم يشترط الوسيلة واكتفى بتمام الواقعة الاجرامية بحصول الجاني على السر.[2]

ثانيا-النتيجة:

لتمام الجريمة يجب أن تصل المعلومات إلى الدولة الأجنبية أو الفاعل الذي يعمل لصالحها والفعل هو التجسس أما النتيجة تتمثل في وصول المعلومة محل التجسس إلى الجهة التي رغبت في الوصول إليها بفعل التجسس.[3]

ثالثا-العلاقة السببية:

تتمثل العلاقة السببية في الصلة التي تربط بين الفعل والنتيجة وتبين أن ارتكاب الفعل هو الذي أدى لحدوث النتيجة.[1]

(1) آسية والي وسامية باشوش، الجرائم الماسة بأمن الدولة، مذكرة ماستر، جامعة آعلي محند أو لحاج، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2016، ص98.

(2) المرجع نفسه، ص99.

(3) نفس المرجع والموضع.

والسلوك الاجرامي في جريمة التجسس أدى لنتيجة معينة تتمثل في وصول المعلومة لجهة معنية أو دولة أجنبية، حيث لولا الفعل الإجرامي لما حصلت الدولة على المعلومة.[2]

الفرع الثاني

الركن المعنوي

يتخذ الركن المعنوي في غالبية الجرائم بصفة عامة صورة القصد الجنائي العام الذي يتحقق بتوافر عنصري العلم و الإرادة حيث يتطلب القصد الجنائي أن تتوفر الإرادة لدى الجاني لارتكاب الفعل المحظور قانونا وتحقيق النتيجة.[3]

كما لا تكفي الإرادة لتحقق القصد بل يجب أيضا توافر العلم بأركان الجريمة كما يتطلبها القانون.[4]

ويكفي في جناية التجسس القصد الجنائي العام الذي يتمثل في تعمد الفاعل ارتكاب فعل سرقة الأسرار مع علمه أن هذا الفعل مجرم قانونا ويعتبر مجرما كل شخص استحوذ على هذه الأسرار.[5]

أما القصد الجنائي الخاص فيتمثل في الغاية التي يقصدها الجاني من ارتكاب الجريمة.[6]

والقصد الجنائي الخاص في جريمة التجسس يتمثل في نية مرتكب الجريمة لتسليم وتبليغه السر الذي يحصل عليه إلى الدولة الأجنبية أو أي جهة يعمل لصالحها[1]، وذلك قصد الإضرار بالدولة التي يرتكب التجسس ضدها.

---

(1) حسام زغيدة وعمر بعلوج، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، جامعة الشاذلي بن جديد، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2023، ص23.

(2) آسية والي وسامية باشوش، المرجع السابق، ص100.

(3) أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة 15، دار هومة، 2019الجزائر، ص143.

(4) المرجع نفسه، ص144.

(5) آسية والي وسامية باشوش، المرجع السابق، ص100.

(6) أحسن بوسقيعة، المرجع السابق، ص147.

الفرع الثالث

الركن الشرعي

يستخلص الركن الشرعي لهذه الجريمة من المادة الأولى من قانون العقوبات التي تنص على أنه لا جريمة ولا عقوبة إلا بنص، فالمشرع الجزائري ينص على جريمة التجسس في المادة 64 من قانون العقوبات وكذلك في الفقرات 2، 3، 4 من المادة 61 والمواد 62، 63 من قانون العقوبات.[2]

وحسب ما نص عليه القانون 04-15 فقد نصت مواده على عقوبة المساس بأنظمة المعالجة الآلية للمعطيات سنذكر منها:

- **المادة 394 مكرر: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك.**
- **المادة 394 مكرر 2: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 500.000دج إلى 5.000.000 دج، كل من يقوم عمدا عن 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 فها 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.**

(1) آسية والي وسامية باشوش، المرجع السابق، ص101

(2) المرجع نفسه، ص ص97-98.

المادة 394 مكرر3: "تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، دون الاخلال بتطبيق عقوبات أشد".[1]

المطلب الثاني

محل التجسس الإلكتروني ضد أمن الدولة

إن الهدف من إقرار الدول أحكام صارمة للتجسس هو حماية أسرار أمنها الوطني من كافة أشكال التهديدات المحتملة نظرا لاختلاف وتشعب هذه الأسرار وتعلقها بكافة مجالات حياة الدولة سواء العسكرية أو السياسية أو الاقتصادية فكشف هذه الأسرار يهدد أمن الدول ومقوماتها، ومع الثورة التكنولوجية وانتشار استخدام الحواسيب وشبكات الاتصال اتجهت الدول الاستفادة من مزاياها وتخزين أسرارها بشكل رقمي إذ أصبحنا بصدد تجسس رقمي.[2]، وتشكل أسرار الدفاع الوطني محلا للتجسس الإلكتروني وعلى ضوء ذلك سنتناول تعريف أسرار الدفاع الوطني (الفرع الأول) وسنتطرق إلى أنواع أسرار الدفاع الوطني (الفرع الثاني).

الفرع الأول

تعريف أسرار الدفاع الوطني

تقع جريمة التجسس الإلكتروني على الأسرار المتعلقة بالدفاع الوطني، حيث "عرف المشرع الهولندي سر الدفاع بأنه المعلومات التي تخص الدولة وسلامتها، بينما عرفه المشرع

(1) قانون 04-15 المتضمن قانون العقوبات، المرجع السابق.

(2) نادية سلامي، المرجع السابق، ص102.

السويسري بأنها الوقائع والتصرفات التي تعتبر سرا وفقا لمصلحة الدفاع القومي، أما المشرع اليوغسلافي فقد عرف سر الدفاع بأنه الأسرار العسكرية والإقتصادية والرسمية".[1]

وبالرجوع لمواد قانون العقوبات الجزائري التي تحكم جريمة التجسس نجد المشرع قد تفادي إدراج تعريف لأسرار الدفاع في تلك المواد واكتفى بتعابير شاملة لها ينبغي كتمانه لمصلحة الدفاع الوطني دون تدخل في تفاصيل التعداد.[2]

فجعل السر إما أن يكون معلومات أو أشياء أو تصميمات أو مستندات ما لهذه التعابير من مرونة وغموض.[3]

وبما أن سر الدفاع الوطني يبقى نفسه في كل زمان فإن طريقة التعامل معه ومعالجته تتغير، فبعد أن كانت معالجة مادية بواسطة الإنسان أصبحت بمعالجة آلية بواسطة الآلة، وعليه فسر الدفاع الإلكتروني يعرف بأنه كل ما يتصل بمظاهر الدفاع الوطني المختلفة سواء عسكرية أو سياسية أو دبلوماسية أو اجتماعية حيث يعتمد في معالجته على أنظمة معالجة آلية للمعطيات وسيتوجب كتمانه للحفاظ على أمن الدولة.[4]

الفرع الثاني

أنواع أسرار الدفاع الوطني

تنقسم أسرار الدفاع الوطني إلى أسرار حقيقية وأسرار مفترضة:

(1) محمد عودة الجبور، الجرائم الواقعة على أمن الدولة وجرائم الإرهاب، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، 2011، ص192.

(2) نادية سلامي، المرجع السابق، ص115.

(3) نفس المرجع و الموضع.

(4) المرجع نفسه، ص ص124-125.

أولا-الأسرار الحقيقية:

حسب الفقيه الإيطالي مانزيتي تعني الأسرار المطلقة وهي تلك الأسرار التي لا يجب على أحد أن يعلم بها إلا من أوكلت إليه مهمة حفظها أو استعمالها ذلك حفاظا لمصلحة الدولة أو الأمن الخارجي الدولة، وهي وجوبية الكتمان وتشمل بدورها قطاعات مختلفة تتمثل في:[1]

أ-الأسرار العسكرية:

وهي تلك الأسرار المتعلقة بالشؤون العسكرية والتي يجب أن تبقى طي الكتمان لاعتبارات تخص الدفاع الوطني، سواء كانت الأسرار تخص القوات المسلحة العامة أو الاحتياطية كما أنها تشمل أيضا الكوادر التي تنظم أعمال وأنشطة القوات وتشمل البيانات والمعلومات حول المعدات ومقارنة وتوزيع تلك القوات سواء في الحدود السياسية للدولة أو في ميدان القتال، و تشمل أيضا الخطط الدفاعية وأساليب الاتصال والتشفير بين أجزاء المنظومة العسكرية.[2]

وتعتبر المؤسسات العسكرية من أهم المؤسسات في الدولة وأكثرها استخداما للوسائل التقنية ذلك ما جعلها مجالا خصبا للتجسس على أسرارها.[3]

والأسرار العسكرية تمثل المحور الأساسي للدولة و من ثم كان إنتهاك المعلومات العسكرية من أقدم الجرائم التي عرفتها التشريعات في نطاق حماية أمن الدولة وكيانها.[4]

ب-الأسرار الاقتصادية:

(1) رزق الله برهان، جريمة التجسس (أمن الدولة)، مذكرة ماستر، جامعة العربي التبسي ، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2018، ص16.

(2) المرجع نفسه، ص126.

(3) حنان أوشن وعماد الدين وادي، "التجسس الالكتروني وآليات مكافحته في التشريع الجنائي الجزائري"، مجلة الحقوق والعلوم السياسية، مجلد1، عدد2، 2014، ص 135.

(4) رزق الله برهان، المرجع السابق، ص17.

يقصد بها الأسرار التي تشمل كافة المعلومات والبيانات الخاصة باقتصاديات المؤسسات والدول وتضم المعلومات المتعلقة بقطاعات الاقتصاد والسياسات المالية للدول ومواردها الاقتصادية وحالة المواد التموينية والمخزون الاستراتيجي من كل مادة تموينية وطرق الصناعة والاختراعات العلمية.[1]

وتعتبر الأسرار الاقتصادية أحد الدعائم المهمة التي تستند عليها الدول في عصرنا الحالي ذلك أن الاقتصاد اليوم يلعب دورا هاما في تقرير مصير دول وأمم بأكملها، ومن هنا يأتي دور التجسس الاقتصادي كأداة ووظيفة أساسية.[2]

ويؤكد خبراء في مجال مكافحة الجاسوسية أهمية المعلومات الاقتصادية التي يتم جمعها عن الطرف المعادي لأثرها الحيوي الذي يمكن له تعطيل الجيش المعادي قبل تحركه وذلك لكشف مصادر المقاومة المتمثلة في إمكانيات البلاد في مجال الزراعة أو الصناعة والمعلومات والأسرار الاقتصادية لأهميتها الكبيرة في بناء خطة السوق ضد البلدان المعادية واستخدامها فيما بعد ضدها أثناء القتال.[3]

ج-الأسرار السياسية والدبلوماسية:

هي تلك الأسرار التي تتعلق بسياسة الدولة سواء الداخلية أو الخارجية وسواء كانت أسرار حالية أو خطوطا عريضة للسياسة المستقبلية للدولة عندما يكون موضوعها الدفاع الوطني بطريقة مباشرة أو غير مباشرة، وتشمل أيضا قرارات الحكومة ومواقفها اتجاه بعض الأحداث التي تجري في الدول الأخرى أو موقفها من دولة أجنبية أخرى، وتتضمن أيضا معلومات دبلوماسية كتقارير السفراء أو القناصل إلى وزير الخارجية لما تحوي هذه الخطابات والتقارير من خطة الدولة لبناء سياستها الخارجية.[4]

(1) نادية سلامي، المرجع السابق، ص127.

(2) رزق الله برهان، المرجع السابق، ص20.

(3) هبة نبيلة هروال، المرجع السابق، ص373.

(4) نادية سلامي، المرجع السابق، ص ص126-127.

ثانيا-الأسرار المفترضة:

هي ليست أسرار في حد ذاتها لكن القانون يفترض اعتبارها كذلك ويعطيها حكم سر الدفاع الوطني وتنقسم بدورها إلى أسرار حكمية وأسرار اعتبارية:

أ-الأسرار الحكمية:

الأسرار الحكمية تتمثل في الأشياء والمحررات والوثائق والرسوم والتصميمات والصور وغيرها التي يجب أن تظل تحت السرية لمصلحة الدولة وخشية أن تؤدي لإفشاء معلومات طبيعتها من الأسرار، فالسر الحكمي ليست سرا في حد ذاته إنما يعتبر وعاء للسر بطبيعته.[1]

ب-الأسرار الاعتبارية:

هي كل ما تعتبره السلطات الحكومية من أشياء أو معلومات أو وثائق أسرارا تتعلق بالدفاع الوطني، وذلك بموجب قرارات أو أوامر بمعنى أن تلك الأشياء أو المعلومات ليست سرية بطبيعتها قد تمثل واقعة معروفة مع ذلك ترى السلطات المعنية أنها أسرار لا يجب إفشاؤها.[2]

المشرع الجزائري عبر عن سر الدفاع الوطني الحقيقي والحكمي بأنه يتمثل في المعلومات والأشياء والمستندات والتصميمات وإن كانت تصلح كمحل التجسس التقليدي فالأمر مختلف بالنسبة للتجسس الإلكتروني، فرغم أن السر يبقى جوهره واحدا بالنسبة لكلا النوعين من التجسس إلا أن الفرق يكمن في شكل هذا السر وطريقة معالجته بحيث تصبح طبيعته إلكترونية يتعامل معه بواسطة نظام المعالجة الآلية للمعطيات، ويمكن إدخال مفهوم المعلومات ضمنها وأصناف السر الأخرى المتمثلة في الأشياء والمستندات والتصميمات رغم

(1) المرجع نفسه، ص135.

(2) رزق الله برهان، المرجع السابق، ص25.

كونها ذات طبيعة مادية، إلا أنه يمكن تحويلها لطبيعة إلكترونية أي لا مادية وذلك عن طريق إدخالها لنظام المعالجة الآلية للمعطيات.[1]

وليس بأمر جديد استخدام هذا النظام في حفظ الوثائق والمستندات والتصميمات، حيث يمكن تصويرها وإدخالها لهذا النظام كمثال الأسلحة لتسهيل إجراء تعديلات على تصميماتها أو حتى وضع تصاميم لأسلحة جديدة وبهذا يمكن المساس بهذه الأسلحة رغم كونها ذات طبيعة إلكترونية.[2]

المطلب الثالث

أبعاد التجسس الإلكتروني ضد أمن الدولة

إن لجريمة التجسس الإلكتروني أبعادا تشمل مجموعة الأسباب التي دفعت بالدول للتجسس على بعضها البعض والآثار المترتبة عن ذلك، وعلى إثر ذلك سنتناول أسباب التجسس الإلكتروني ضد أمن الدولة (الفرع الأول) وسنتطرق إلى الآثار المترتبة عن التجسس الالكتروني على سيادة الدولة (الفرع الثاني).

الفرع الأول

أسباب التجسس الإلكتروني ضد أمن الدولة

أضحى التجسس في عصرنا الحالي وخصوصا الحديث منه وسيلة ضرورية لا يمكن التغاضي عنها، فالتجسس اليوم أصبح الوسيلة اللازمة لاستمرار الدول كما أنها جريمة كانت

(1) نادية سلامي، المرجع السابق، 102.

(2) المرجع نفسه، ص139.

تمارس منذ قدم البشرية رغم أنها محظورة إلا أنه معترف بها ضمينا وتعتبر وسيلة الدول لفرض هيمنتها وإخضاع غيرها من الدول.[1]

تغيرت مفاهيم عديدة إثر الثورة المعلوماتية من بينها مفهوم الحرب، حيث يعتقد بعض المحللين أن ميدان المعركة المستقبلي سيكون الفضاء الإلكتروني لأن هذا الأخير يختصر التكلفة سواء المالية أو البشرية فالجندي أصبح يخوض حربا معلوماتية.[2]

وأكثر ما تتطلبه هذه الحرب المعلوماتية هو التحكم في تقنيات اختراق البنى التحتية الإحترافية عالية التطور والقدرة على تجاوز اجراءات التشفير والمراقبة والكشف عن مفاتيح القطاعات العسكرية والمدينة للخصوم.[3]

إن الدول العظمى في عصرنا الحالي هي من باتت تمتلك أكثر وسائل التجسس تطورا مما يتيح لها جمع أكبر قدر من المعلومات عن الدول ومعرفة استراتيجيتهم وخططهم للحرب.

وتشكل هذه المعلومات الحساسة قيمة ومصدرا للثروة كونها معلومات حساسة تسعى غالبية الدول للاحتفاظ بسرتيها من التهديدات الالكترونية المحتملة كالتجسس الإلكتروني، ذلك كون ان الفضاء الإلكتروني ليس حكرا على جهة أو دولة معنية مما أدى ذلك لظهور جهات كثيرة تمارس التجسس كجماعات الجريمة المنظمة والمنظمات الإرهابية.[4]

الفرع الثاني

الآثار المترتبة عن التجسس الإلكتروني على سيادة الدولة

(1) نادية سلامي، المرجع السابق، ص90.

(2) المرجع نفسه، ص91.

(3) نفس المرجع والموضع.

(4) المرجع نفسه، ص95.

يكمن الخطر الحقيقي لجريمة التجسس الإلكتروني الذي تقوم به الأجهزة الاستخبارية في الحصول على معلومات وأسرار دولة ما و من ثم إفشائها لدولة أخرى معادية لها أو استغلالها بما يضر المصلحة الوطنية لتلك الدولة.[1]

ومن المعروف أن هناك ارتباطا وثيقا بين أمن الدولة وسيادتها فالأول يعد مظهرا للثاني، إذ يمكن للدولة أن تتخذ كل ما تراه كفيلا بحماية أمنها ذلك استنادا للسيادة.[2]

حيث تغير مفهوم الاقليم والشعب الذي تمارس الدولة سيادتها عليهما فالإقليم لم تعد حدوده محصنة، إذ استطاعت ثورة المعلومات والاتصالات أن تخلق مجالات جديدة تمكن الدول المتطورة من تغيير هذا المفهوم أي لم تعد السيادة بالسياج المغلق حيث أصبحت المجالات الأساسية للسيادة الاقليمية متاحة لمن يملك الوسائل والأجهزة التقنية الحديثة كالتنصت عن طريق الأقمار الصناعية.[3]

إن جريمة التجسس الالكتروني تسعى لزعزعة الأمن ونشر الخوف والإخلال بنظام الدولة العام وتسعى لابتزاز وتهديد السلطات العامة وخلق حالة من الفوضى في الدولة.[4]

ولم تعد الحروب اليوم بالأسلحة التقليدية إنما باتت حرب معلومات تتفوق فيها الدول التي تحسن استغلالها في قلب موازين القوى لصالحها وضرب كيانات دول بأكملها.

(1) فاطمة الظبيري، المرجع السابق، ص59.

(2) نادية سلامي، المرجع السابق، ص97.

(3) المرجع نفسه، ص98.

(4) عبد الهادي محمود الزيدي، "التجسس الاسرائيلي على الدول العربية"، مجلة مركز الدراسات الاستراتيجية والدولية، مجلد1، عدد58، 2013، ص141.

الفصل الثاني

آليات المتابعة الجزائية للتجسس الإلكتروني ضد أمن الدولة في التشريع الجزائري

الفصل الثاني

آليات المتابعة الجزائية للتجسس الإلكتروني ضد أمن الدولة في التشريع الجزائري

إن اقتران جريمة التجسس بالوسائل الالكترونية جعله يعتبر من أكبر التحديات التي تواجه الدول دون استثناء، فالجرائم الالكترونية بصفة عامة تشكل صعوبة من حيث متابعتها نظرا لطبيعتها الإلكترونية والتي تتم في بيئة افتراضية لامادية إذ أن القواعد الإجرائية التقليدية لا يمكن تطبيقها على التجسس الإلكتروني لذا كان على الدولة أن تتدخل وتسن قواعد اجرائية جديدة، وخاصة تتماشى مع الجرائم الإلكترونية لتكمل نقص القواعد القديمة وباعتبار أن هذه الجريمة عابرة للحدود فإن جهود الدولة الداخلية لا تكفي، لذا كان على الجزائر أن تتعاون دوليا لمكافحة مثل هذه الجرائم إذ أن المشرع الجزائري أكد على ضرورة التعاون الدولي بموجب نصوص خاصة، وعليه قسمنا الفصل إلى مبحثين، حيث سنتناول متابعة التجسس الإلكتروني في ظل التشريع الجزائري (المبحث الأول) وسنتطرق إلى مكافحة التجسس الإلكتروني في إطار الاتفاقيات الدولية (المبحث الثاني).

الفصل الثاني

آليات المتابعة الجزائية للتجسس الإلكتروني ضد أمن الدولة في التشريع الجزائري

المبحث الأول

متابعة التجسس الإلكتروني في ظل التشريع الجزائري

تعتبر جريمة التجسس الإلكتروني جريمة واقعة على أمن الدولة فهي من أخطر الجرائم المستحدثة وتعتبر تهديدا كبيرا لأمن الدول، ومقابل ذلك كان التصدي لهذه الجريمة أمرا محتما على الدولة الجزائرية باعتباره خطرا يمس سيادتها وأمنها وكيانها كدولة ونظرا لطبيعة جريمة التجسس الإلكتروني والتي تعتبر من ضمن الجرائم الإلكترونية والتي تختلف عن الجرائم التقليدية في خصائصها نظرا لأنها جريمة عابرة الحدود فمتابعة هذه الجريمة تختلف عن متابعة الجرائم التقليدية، وبناء على ذلك سنتناول الاختصاص القضائي (المطلب الأول)، وسنتطرق إلى متابعة التجسس الإلكتروني في ظل قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال 09-04 (المطلب الثاني)، وسنتناول اجراءات التحري الخاصة بجريمة التجسس الإلكتروني ضد أمن الدولة (المطلب الثالث).

الفصل الثاني

آليات المتابعة الجزائية للتجسس الإلكتروني ضد أمن الدولة في التشريع الجزائري

المطلب الأول

الاختصاص القضائي

الاختصاص القضائي هو إدخال الجريمة في سلطة الجهات القضائية الجزائرية، وقد لا تطرح بعض الجرائم إشكالات في تحديد اختصاص هذه الجهات بالنظر فيها، بالمقابل قد يستعصي الأمر بخصوص بعض الجرائم منها جريمة التجسس الإلكتروني ضد أمن الدولة، نظرا لأنها تعتبر واحدة من الجرائم الإلكترونية العابرة للحدود لما فيها من مساس بمصالح الدولة بمعنى أنها تطرح إشكالا فيما يخص تطبيق المبادئ القانونية التي تنظم مسألة الاختصاص القضائي سواء كان مبدأ الإقليمية أو مبدأ العينية.[1]

وعلى إثر ذلك سنتناول إعمال مبدأ الإقليمية في متابعة جريمة التجسس الإلكتروني (الفرع الأول)، كما سنتطرق إلى إعمال مبدأ العينية في متابعة جريمة التجسس الإلكتروني (الفرع الثاني).

الفرع الأول

إعمال مبدأ الإقليمية في متابعة جريمة التجسس الإلكتروني

ويقصد بمبدأ إقليمية القانون الجزائي أن القانون الجزائي لدولة ما يطبق على كل جريمة ارتكبت على إقليم هذه الدولة سواء كان الجاني يحمل جنسية هذه الدولة أو يحمل جنسية دولة أجنبية، ووفق مبدأ الإقليمية فالمحكمة المختصة وسلطة التحقيق المختصة هي

(1) نادية سلامي، المرجع السابق، ص231.

محكمة المكان التي وقعت فيه الجريمة أو جزء منها بمعنى وقع فيها الركن المادي أو جزء منه.[1]

إن أحد أهم خصائص التجسس الالكتروني أن السلوكات الإجرامية المكونة لركنها المادي تتسم بطبيعة معنوية من جهة وإمكانية توزعها على أكثر من إقليم واحد، ومن جهة أخرى باعتبار أن التجسس الإلكتروني جريمة عابرة للحدود لا يشترط فيها الحضور المادي لمرتكبها في نفس الاقليم بل يكفي أن يستهدف جزء من المنظومة المعلوماتية الخاضعة لسيادة دولة معنية لوقوع الجريمة في إقليم هذه الدولة.[2]

وقد أدى هذا الطابع العابر للحدود إلى أن تصبح أكثر من دولة مختصة بالنظر في الجريمة، فقد يقوم الجاني من الدولة المتواجد بها ماديا بإرسال برامج تجسس عبر شبكة الانترنت إلى عدة أنظمة معلوماتية في الكثير من الدول أو قد يستهدف نظاما معينا في دولة معنية لكن هذه البرامج قد تمر بخوادم تتواجد بعدة دول مما يجعل الدولة الأولى التي انطلق منها البرنامج والدولة التي حدثت فيها النتيجة ودول العبور التي تحقق فيها جزء من الركن المادي للجريمة جميعها لديها اختصاص إقليمي للنظر في هذه الجريمة.[3]

في هذا الصدد انقسم رأي الفقهاء إلى ثلاثة اتجاهات لتحديد مكان وقوع الجريمة:

أولا–مذهب السلوك أو النشاط الاجرامي:

ووفقا لهذا المذهب ينعقد الاختصاص القضائي للمحكمة التي يقع في نطاقها السلوك الاجرامي وليس مكان تحقق النتيجة أو الأثار المترتبة عنه ذلك أن هذا المذهب يسهل عملية الإثبات وجمع أدلة الجريمة، كما أن المحكمة التي لها ولاية النظر في القضية تكون قريبة

(1) مريم عراب، "الاختصاص القضائي في الجرائم المعلوماتية"، مجلة حوليات كلية الحقوق والعلوم السياسية، مجلد7، عدد3، 2015، ص277.

(2) نادية سلامي، المرجع السابق، ص ص 235–236.

(3) نفس المرجع والموضع.

من مسرح الجريمة و تطبيق قانون الدولة التي تحققت فيها النتيجة لا يتفق واعتبارات العدالة ذلك أن الجاني لا يكون على دراية بقانون تلك الدولة.[1]

وهذا المعيار قد أخذ به المشرع الجزائري في نص المادة 586 من قانون الإجراءات الجزائية، حيث نصت على: "**تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر**".[2]

ثانيا-مذهب النتيجة الاجرامية:

هذا الاتجاه يأخذ بمبدأ وحدة الجريمة وعدم الفصل بين عناصرها، كذلك يمتاز في نظر المدافعين عنه بأنه أكثر واقعية على اعتبار أن الضرر له مظهر ملموس على خلاف السلوك الإجرامي الذي قد يتخذ فعل إيجابي كما قد يكون عبارة عن امتناع أي فعل سلبي، و تجدر الإشارة أن معظم الدول اعتمدت على مبدأ الإقليمية لحل مشكلة الاختصاص القضائي في الجرائم الالكترونية.[3]

ثالثا-المذهب المختلط:

برز اتجاه ثالث نتيجة الإنتقادات التي تعرض لها كلا المذهبين السابقين ومفاد هذا المذهب أن الجريمة تعد واقعة في مكان حصول الفعل الاجرامي وكذلك المكان الذي تحققت فيه النتيجة الإجرامية أو من المتوقع تحققها فيه، حيث حصل هذا الاتجاه على موافقة أغلب الفقه ويعد مبرره في أن الركن المادي للجريمة يقوم على ثلاثة عناصر: النشاط الاجرامي

(1) مريم عراب، المرجع السابق، ص277.

(2) الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون الاجراءات الجزائية المعدل والمتمم.

(3) عبد الرؤوف بوديسة بجاد، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة ماستر، جامعة محمد البشير الابراهيمي، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022، ص84.

والنتيجة والعلاقة السببية، مما يعني أن الجريمة وقعت في كل مكان تحقق فيه عنصر من عناصر الركن المادي للجريمة.[1]

وإذا كان من البساطة تطبيق المعايير السابقة في الجرائم العادية إلا أن الأمر يختلف بخصوص جريمة التجسس الإلكتروني بحيث أن لها من الخصوصية ما يصعب تطبيق المعايير السابقة لأسباب عدة ففيما يخص معيار السلوك الاجرامي مثلا فإن الجاني في جريمة التجسس الالكتروني قد يرتكب سلوكه الاجرامي انطلاقا من دولة أخرى غير الدولة المعتدى على أسرارها ونظرا لحساسية المحل فالدولة لا يمكنها أن تتنازل عن اختصاصها بمتابعة الجريمة أو أن تتشاركه مع دولة أخرى.[2]

أما من ناحية معيار تحقق النتيجة فيمكن أن يكون مقبولا، لأنه يمنح الاختصاص للدولة المتضررة بحيث لن تضطر الدولة لتقاسم النظر في جريمة تمس أمنها مع غيرها من الدول، لكن لا يمكن تطبيق ذلك فيما يخص جريمة التجسس الإلكتروني لأنها من جرائم السلوك المجرد ومعنى ذلك أن النتيجة تتحقق بمجرد القيام بالفعل الاجرامي دون انتظار تحقق نتيجة معنية.[3]

الفرع الثاني

إعمال مبدأ العينية في متابعة جريمة التجسس الإلكتروني

(1) نفس المرجع و الموضع.

(2) نادية سلامي، المرجع السابق، ص 237.

(3) نفس المرجع والموضع.

الفصل الثاني

آليات المتابعة الجزائية للتجسس الإلكتروني ضد أمن الدولة في التشريع الجزائري

يقصد بمبدأ العينة تطبيق القانون الجزائي على الجرائم التي تمس بالمصالح الأساسية للدولة والمرتكبة خارج إقليمها أيا كانت الجنسية التي يحملها مرتكب الجريمة وهذا المبدأ يفرضه حرص الدولة على حماية مصالحها الأساسية.[1]

فقد جاء هذا المبدأ لضرورة سد العجز الذي يكتنف مبدأ الإقليمية في جرائم الانترنت، ذلك أنه لم يكن بإمكانه حماية كل المصالح المتعلقة بالدولة وحماية سيادتها، ومبدأ العينية له ما يبرره إذا ما تعلق الأمر بحماية المصالح الوطنية خارج إقليم الدولة وإن كان افتراضي وهو حال مسرح الجريمة في الجرائم الإلكترونية.[2]

وعلى غرار باقي التشريعات أخذ المشرع الجزائري بمبدأ العينية لحماية المصالح الأساسية للدولة، لكن عرف مفهوم هذه المصالح وكيفية إعمال هذا المبدأ تغييرات تضمنتها مواد قانون الإجراءات الجزائية والمعدل سنة 2015 وكذا قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.[3]

ونصت المادة 588 المعدلة من قانون الاجراءات الجزائية على أنه: "**تجوز متابعة ومحاكمة كل أجنبي وفقا لأحكام القانون الجزائري ارتكب خارج الاقليم 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 إضرارا بمواطن جزائري**".[4]

(1) مريم عراب، المرجع السابق، ص279.

(2) عبد الرؤوف بوديسة بجاد، المرجع السابق، ص85.

(3) نادية سلامي، المرجع السابق، ص240.

(4) 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.

كما يتضح من خلال نص المادة المعدلة إلغاء المشرع الجزائري لشرط القبض على الجاني في الجزائر أو حصول الحكومة على تسليمه لها وعليه لا يشترط لمتابعة التجسس الإلكتروني توفر هذين الشرطين أي يمكن متابعته ومحاكمته غيابيا.[1]

إن إعمال مبدأ العينية على جريمة التجسس الإلكتروني تعترضه مجموعة من الصعوبات من أهمها عدم إمكانية تطبيقه وهذا راجع لصعوبة التوصل إلى الجاني وجعله يمثل أمام المحاكم الوطنية، ففي أغلب الحالات لا يمكن إلقاء القبض على الجاني في إقليم الدولة نظر لخفاء الجريمة ودرجة التكتم على تنفيذها إن تمت في الجزائر أو أصلا تمت خارج إقليم الجزائر بواسطة الدخول لأنظمة المعالجة الآلية للمعطيات عن بعد، وهذا الاحتمال الأرجح في حالة التجسس الإلكتروني وحتى في هذه الحالة لا يمكن الحصول على تسليم الجاني للسلطات الوطنية.[2]

المطلب الثاني

متابعة التجسس الإلكتروني في ظل قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال 09-04

بما أن التجسس الإلكتروني جريمة تندرج تحت خانة الجرائم الإلكترونية ونظرا لخصوصية هذه الجرائم وطبيعتها المختلفة عن الجرائم التقليدية فقد خصها المشرع الجزائري بإجراءات متابعة خاصة في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال 09-04 وعلى إثر ذلك سنتناول التفتيش والحجز (الفرع الأول)، ثم سنتناول المعاينة والمراقبة الإلكترونية (الفرع الثاني).

الفرع الأول

(1) نادية سلامي، المرجع السابق، ص242.

(2) المرجع نفسه، ص243.

التفتيش والحجز

إن الهدف من التفتيش هو البحث عن الأدلة التي تفيد في كشف الحقيقة وهو من بين الاجراءات التي نص عليها المشرع الجزائري من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال 09-04، أما الحجز أو الضبط كما أطلق عليه المشرع الجزائري في إطار هذا القانون 09-04 فهو إجراء جديد خاص بالمعطيات والذي يتناسب مع الطبيعة اللامادية للجرائم الإلكترونية.[1]

أولا-التفتيش في الجرائم الإلكترونية:

"هو إجراء من اجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص".

وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة"،[2] وقد نص المشرع الجزائري على إجراء تفتيش المنظومات المعلوماتية في المادة الخامسة من القانون الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وقد بين ضوابطه وشروط القيام به.[3]

1-مدى خضوع مكونات الحاسب المادية والمعنوية للتفتيش:

إن الولوج في المكونات المادية للحاسب بحثا عن شيء يتصل بجريمة إلكترونية وقعت ويفيد في كشف الحقيقة عن الجريمة وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى آخر فإن جواز التفتيش في تلك المكونات يتوقف على طبيعة

(1) عبد الرؤوف بوديسة بجاد، المرجع السابق، ص49.

(2) خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009، ص182.

(3) نادية سلامي، المرجع السابق، ص252.

المكان الموجود فيه إن كان مكانا عاما أو خاصا إذ أن لصفة المكان أهمية خاصة في مجال التفتيش فإذا كانت في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونا.[1]

أما بالنسبة لتفتيش مكونات الحاسب المعنوية فقد اختلفت الآراء بشأن جواز تفتيشها، فإذا كان الهدف من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الإلكترونية بأشكالها المختلفة.[2]

وأجاز المشرع الجزائري تفتيش المعطيات المعلوماتية بموجب المادة 05 من القانون 09-04، حيث أجازت هذه المادة للسلطات القضائية المختصة وكذلك ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات التي نصت عليها المادة 04 من نفس القانون والتي من بينها توافر معلومات عن احتمال اعتداء على منظومة معلوماتية يهدد النظام العام أو الاقتصاد الوطني.[3]

2-تفتيش منظومة المعلومات عن بعد في الجرائم الإلكترونية:

التفتيش في الجرائم الالكترونية يكون في حالتين:

أ-حالة جهاز متصل بجهاز المتهم داخل الدولة:

إن المشكلة في هذه الحالة عندما تقوم سلطة التحقيق بتفتيش جهاز متصل بجهاز المتهم يكون داخل الدولة وكذا تجاوز الاختصاص المكاني لسلطة التحقيق من ناحية والاعتداء على خصوصيات الغير من ناحية أخرى، ونظرا لوجود قصور تشريعي في

(1) أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2008، ص223.
(2) المرجع نفسه، ص224.
(3) عبد الرؤوف بوديسة بجاد، المرجع السابق، ص52.

نصوص قانون الإجراءات الجزائية لسنة 2006 تم مواجهة هذا القصور بالسماح للسلطات القضائية المختصة بتمديد التفتيش بسرعة وإلى أي منظومة معلوماتية أو جزء منها تقع داخل الإقليم الوطني، وهذا ماتضمنه الفقرة الثانية من المادة 05 من القانون رقم 09-04، وما يدخل ضمن نطاق الاستعجال في تمديد الاختصاص ذلك خشية من حدوث عبث بالأدلة الرقمية.[1]

ب-حالة جهاز متصل بجهاز المتهم خارج الدولة:

تكون الإشكالية أكبر في هذه الحالة عندما يكون الجهاز المطلوب تفتيشه يقع خارج الدولة إذ أنه في غالبية الأحيان يلجأ مرتكبي الجرائم الإلكترونية إلى تخزين البيانات الخاصة بهم والتي تعد أدلة إدانتهم في جرائم ارتكبوها خارج الدولة أما بالنسبة للمشرع الجزائري فقد تلافى مشكلة التفتيش خارج الإقليم الوطني بموجب الفقرة الثالثة من المادة 05 من قانون 09-04 حيث ذكرت أن التفتيش يكون بمساعدة السلطات الأجنبية المختصة وذلك طبقا للاتفاقيات الدولية.[2]

ثانيا-الحجز أو الضبط في الجرائم الإلكترونية:

إن الغرض من التفتيش هو ضبط الأدلة التي تفيد في ظهور الحقيقة فالضبط غرض التفتيش وإن لم يكن هو السبب الوحيد قد يتم الضبط استنادا لأسباب غير التفتيش كالمعاينة وما يقدمه المتهم والشهود للسلطات المختصة، وقد نص المشرع الجزائري على هذا الاجراء في المادة 06 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مستخدما مصطلح الحجز.[3]

1-اجراءات الحجز أو الضبط في الجرائم الإلكترونية:

(1) نفس المرجع و الموضع.

(2) المرجع نفسه، ص53.

(3) نادية سلامي، المرجع السابق، ص257.

نص المشرع الجزائر على حجز المعطيات من المواد 06 إلى 09 من القانون 09-04، وحسب المادة 06 عندما تكتشف السلطة المختصة بالتفتيش معطيات تفيد في كشف الجرائم أو مرتكبيها يتم نسخ المعطيات محل البحث على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الاجراءات الجزائية كما يجب على السلطة المختصة بالتفتيش والحجز أن تسهر على سلامة المعطيات في المنظومة المعلوماتية.[1]

الفرع الثاني

المعاينة والمراقبة الإلكترونية

أولا-المعاينة:

يقصد بالمعاينة الانتقال إلى الأماكن التي وقعت فيها الجريمة لإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الجريمة ومرتكبيها أي يجب على السلطات المختصة الإنتقال إلى أماكن وقوع الجريمة فور ارتكابها وإجراء المعاينة حتى لا يكون فارق زمني كبير بين إجراء المعاينة ووقت حدوث الجريمة لمنع الجاني من تغيير أو إزالة كل أو بعض الأثار المادية للجريمة وحتى لا يقع الشك في الدليل وهذا ما نصت عليه المادة 42 من قانون الإجراءات الجزائري.[2]

1-معاينة مسرح الجريمة الإلكترونية:

(1) صالح شنين، "اجراءات التحري والتحقيق في جرائم تكنولوجيات الإعلام والاتصال في التشريع الجزائري"، مجلة الدراسات القانونية، مجلد 1، عدد1، 2014، ص283.

(2) زهية معمش ونسيمة غانم، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة ماستر، جامعة عبد الرحمان ميرة، كلية الحقوق و العلوم السياسية، قسم القانون الخاص، 2013، ص ص 6-7.

يكون مسرح الجريمة داخل الحاسوب والبيانات الرقمية التي تكون داخل شبكاته وفي الأقراص وذاكرته المتواجدة بداخله، ويقصد بمعاينة مسرح الجريمة الالكترونية هو معاينة البصمات الإلكترونية والآثار التي يتركها مستخدم الشبكة المعلوماتية وتشمل الرسائل المرسلة منه والواردة إليه وجميع الاتصالات الالكترونية التي تتم من خلال الحاسوب.[1]

2-السلطة المختصة بإجراء المعاينة لمسرح الجريمة المعلوماتية:

الأصل أن انتقال المحقق الجنائي لإجراء المعاينة أو إجراء آخر أمر متروك للسلطة التقديرية له لا يقوم به إلا إذا كانت هناك مصلحة من ورائه، لذلك فالمعاينة هي إجراء من اجراءات التحقيق يترك أمر تقدير لزوم القيام بها إلى السلطة التي تباشر التحقيق، حيث نصت المواد 79، 80 و42 من قانون الاجراءات الجزائية الجزائري على أن المعاينة تجرى إما من طرف قاضي التحقيق ويكون ذلك بعد إخطار وكيل الجمهورية الذي له حق مرافقته، كما يسمح بتمديد اختصاص قاضي التحقيق إذا كانت هناك الضرورة لذلك، و يتم اجراء المعاينة من طرف ضابط الشرطة القضائية فور وصول خبر وقوع الجريمة إليهم و إنتقالهم إليها.[2]

ثانيا-المراقبة الإلكترونية:

تتمثل المراقبة الإلكترونية في كشف الجرائم قبل وقوعها، كما أنها وسيلة هامة من وسائل الارشاد الجنائي يقصد به المراقبة الأمنية التي محلها الاتصالات الإلكترونية والتي نص المشرع الجزائري على تعريفها من خلال القانون 09-04، وهي تراسل أو إرسال أو

(1) خضرة شنيتر، الآليات القانونية لمكافحة الجريمة الإلكترونية، رسالة دكتوراه، جامعة أحمد دراية، كلية الحقوق و العلوم السياسية، قسم الحقوق، 2021، ص ص64-65.

(2) زهية معمش ونسيمة غانم، المرجع السابق، ص9.

استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة باستعمال أي وسيلة إلكترونية.[1]

1-شروط المراقبة الإلكترونية:

وقد ذكرت المادة 04 من قانون 09-04 هذه الشروط والتي تتمثل في:

أ-**الإذن المكتوب:** فلا يجوز إجراء المراقبة إلا بإذن مكتوب من طرف السلطة القضائية المختصة.[2]

ب-شروط متعلقة بالجرائم الماسة بأمن الدولة: عندما يتعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية الذين ينتمون للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث يمنح الإذن لمدة 6 أشهر قابلة للتجديد على أساس يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.[3]

المطلب الثالث

إجراءات التحري الخاصة بجريمة التجسس الإلكتروني ضد أمن الدولة

تخضع جريمة التجسس الإلكتروني ضد أمن الدولة لإجراءات تحري خاصة نص عليها المشرع الجزائري في قانون الإجراءات الجزائية والمتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وعليه سنتناول اعتراض المراسلات وتسجيل الأصوات والتقاط الصور (الفرع الأول) وسنتطرق إلى اجراءات التسرب أو الاختراق (الفرع الثاني).

(1) عبد الرؤوف بوديسة بجاد، المرجع السابق، ص58.

(2) صالح شنين، المرجع السابق، ص279.

(3) المرجع نفسه، ص280.

الفصل الثاني

آليات المتابعة الجزائية للتجسس الإلكتروني ضد أمن الدولة في التشريع الجزائري

الفرع الأول

اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

أولا-اعتراض المراسلات:

من خلال نص المادة 65 مكرر 5 ن قانون الاجراءات الجزائية نجد أن المشرع الجزائري قد قصد باعتراض المراسلات اعتراض او تسجيل او نسخ المراسلات التي تتم عن طريق وسائل اتصال سلكية ولا سلكية وتكون بيانات قابلة للإنتاج والتوزيع، التخزين، الإستقبال والعرض واستثنى المراسلات الإلكترونية كونها يمكن أن تتم خارج النطاق السلكي واللاسلكي وقد أفرد لها مواد قانونية خاصة في إطار القانون 09-04.[1]

ثانيا-التسجيل الصوتي:

تسجيل الأصوات يقصد به تسجيل أحاديث المتهم وشركائه عن واقعة معنية من الوقائع التي نصت عليها المادة 65 مكرر 5 من قانون الاجراءات الجزائية خلسة، وبعد ما أعطى المشرع للمتهم الحق في الصمت فإنه وبشكل غير مباشر أورد استثناء عن هذا الحق وذلك بموجب المادة 65 مكرر التي ذكرناها سابقا، حيث أصبح من الممكن أخذ اعتراف الشخص ضد نفسه بشكل خفي ودون رضاه وموافقته عن طريق تسجيل كل ما يتفوه به من كلام بصفة خاصة سرية.[2]

ثالثا-التقاط الصور:

---

(1) عبد الرؤوف بوديسة بجاد، المرجع السابق، ص 62.

(2) فوزي عمارة، "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية"، مجلة العلوم الإنسانية، مجلد 21، عدد1، 2010، ص237.

لم يكتف المشرع بالسماح لقاضي التحقيق بتسجيل الأصوات فقط بل أيضا إمكانية التقاط الصور، فبموجب المادة 65 مكرر 5 أعطى المشرع الإذن لقاضي التحقيق أن يمد عين الكاميرا إلى الأماكن الخاصة التي تعتبر مستودعات أسرار المعنيين بالمراقبة.[1]

الفرع الثاني

إجراءات التسرب أو الاختراق

أورد المشرع الجزائري في نص المادة 65 مكرر 12 تعريفا للتسرب حيث نصت المادة "يقصد بالتسرب قيام ضباط أو عون الشرطة القضائية، 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".[2]

وحسب تعريف البعض بأنه أكثر وسائل التحري تعقيدا وخطورة ذلك أنه يتطلب من ضابط الشرطة القضائية وأعوانه القيام بمناورات توحي بأن القائم بها مساهم في ارتكاب الجريمة مع بقية أفراد العصابة لكنه يوهمهم ويخدعهم فقط بأنه فاعل وشريك لهم حتى يتسنى له أن يطلع على أسرارهم ويجمع الأدلة ويبلغ السلطات بذلك لضبط المجرمين ووضع حد للجريمة.[3]

إن الجرائم المعنية بالتسرب محددة على سبيل الحصر، وقد وردت في نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية ومن ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بحيث يمكن تصور القيام بعمليات تسرب في البيئة الحقيقية أو البيئة

(1) المرجع نفسه، ص238.

(2) قانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 66-155 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الاجراءات الجزائية، جريدة رسمية، عدد 14.

(3) عبد الرؤوف بوديسة بجاد، المرجع السابق، ص69.

الإلكترونية وذلك بقيام ضابط الشرطة القضائية بالدخول إلى العالم الافتراضي واشتراكه مثلا في محادثات غرف الدردشة أو الاتصال المباشر عن كيفية قيام أحدهم باختراق الشبكات.[1]

أولا-شروط التسرب:

ليكون التسرب ناجحا ونتائجه مقبولة كأدلة فرض لها المشرع شروطا إن لم تتوفر لا يمكن اللجوء إلى عملية التسرب أساسا، وحسب المادة 65 مكرر 11 يمكن القيام بالتسرب إذا اقتضت الضرورة في إحدى الجرائم المبينة في المادة 65 مكرر 5 من قانون الاجراءات الجزائية وهي جرائم محددة على سبيل الحصر وتتمثل في الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم المخدرات أو تبيض الأموال...[2]

وللقيام بإجراء التسرب يجب الحصول على إذن سابق يمنحه وكيل الجمهورية ويجب أن يخطر قاضي التحقيق وكيل الجمهورية بذلك قبل منح الإذن، كما يجب أن يكون الإذن مكتوبا ومسببا وذلك تحت طائلة البطلان و يجب أن تذكر الجريمة التي تبرر اللجوء لهذا الإجراء وهوية ضابط الشرطة القضائية الذي يباشر إجراء التسرب، ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر مع إمكانية التجديد إذا اقتضي ذلك وكذلك ضمن نفس الشروط سواء الشكلية أو الزمنية.[3]

المبحث الثاني

مكافحة التجسس الإلكتروني في إطار الاتفاقيات الدولية

(1) نادية سلامي، المرجع السابق، ص ص 270-271.

(2) عبد الرؤوف بوديسة بجاد، المرجع السابق، ص70.

(3) نادية سلامي، المرجع السابق، ص271.

الفصل الثاني

آليات المتابعة الجزائية للتجسس الإلكتروني ضد أمن الدولة في التشريع الجزائري

إن أسمى غايات أي دولة هو تحقيق الاستقرار والأمن ولأجل ذلك تبذل جهود وتوضع استراتيجيات وتسن قوانين فيتحقق بذلك أولى مستويات الأمن لكن في كثير من الأحيان لا يكون ذلك كافيا لبلوغ درجة الأمن المطلوبة إذ يرتبط بذلك ظروف خارجية لا يمكن للدولة وحدها أن تتعامل معها، لذا تلجأ لوضع أسس التعاون الدولي التي تتقاسم معها نفس التوجهات وعادة نفس النطاق الجغرافي والتي تشترك معها بنفس المخاطر والتهديدات لتعزز بذلك الدولة أمنها الوطني وتتمكن من وضع حد للجرائم العابرة للحدود كجريمة التجسس الإلكتروني و بناءا على ذلك سنتناول الاتفاقيات الدولية في مجال مكافحة التجسس الإلكتروني كجريمة الكترونية (المطلب الأول)، وسنتطرق إلى آليات التعاون الدولي في مواجهة الجريمة الالكترونية (المطلب الثاني)، وسنتناول الصعوبات التي تواجه التعاون الدولي في مكافحة الجريمة الالكترونية (المطلب الثالث).

المطلب الأول

الاتفاقيات الدولية في مجال مكافحة التجسس الإلكتروني كجريمة إلكترونية

تعد الاتفاقيات الدولية شكلا من أشكال التعاون الدولي في إطار مكافحة الجرائم الإلكترونية بصفة عامة، وباعتبار أن جريمة التجسس الإلكتروني التي نحن بصدد دراستها من الجرائم العابرة للحدود توجب على الجزائر أن تستعين بالاتفاقيات الدولية لمكافحة هذه الجريمة التي تهدد أمنها واستقرارها ورغم عدم إشارة هذه الاتفاقيات لجريمة التجسس الإلكتروني بشكل صريح وواضح إلا أنه يمكن أن تطبق عليها الأحكام العامة التي تطبق على كافة طوائف الجرائم الإلكترونية ومنه سنتناول اتفاقيتين مهمتين اعتمدت عليهما الجزائر في مكافحة جريمة التجسس الإلكتروني ضد أمن الدول، حيث سنتناول الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (الفرع الأول) واتفاقية بودابست (الفرع الثاني).

الفرع الأول

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ووقعت عليها الدول العربية ومن بينها الجزائر كرغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات والتي تعتبر تهديدا وخطرا على أمن ومصالح وسلامة مجتمعاتها ولضرورة الحاجة لتبني سياسة جنائية تشترك فيها الدول بهدف حماية المجتمع العربي من جرائم تقنية المعلومات.[1]

وقد نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على أحكام موضوعية وأخرى إجرائية لتكون بهذا قد أسست لسياسة جنائية عربية مشتركة تهدف للإحاطة بجميع عناصر مكافحة جرائم تقنية المعلومات ومن بينها جريمة التجسس الإلكتروني.[2]

جاء في نص المادة الخامسة من هذه الاتفاقية على ضرورة التزام كل دولة تعد طرفا في هذه الاتفاقية بتجريم الأفعال المبينة في الفصل الثاني منها، وذلك وفقا لتشريعاتها وأنظمتها الداخلية.[3]

ونصت في المادة السادسة منها على جريمة الدخول غير المشروع للنظام المعلوماتي بغرض الحصول على معلومات حكومية سرية والتي ما يعرف بالتجسس الإلكتروني كما قد شددت عقوبته في هذه الحالة.[4]

وإضافة لتجريم فعل الدخول غير المشروع فقد جرمت هذه الاتفاقية أيضا 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،

(1) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر سنة 2014.

(2) نادية سلامي، المرجع السابق، ص299.

(3) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المرجع السابق.

(4) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المرجع السابق.

وعليه يمكن القول أن الاتفاقية العربية قد جرمت جريمة التجسس الالكتروني من خلال تجريم فعل الدخول غير المشروع لمنظومة معلوماتية وكذلك من خلال تجريم فعل إساءة استخدام وسائل تقنية المعلومات.[1]

ومقارنة مع ما ورد في كل من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ونصوص قانون العقوبات الجزائري التي تجرم الأفعال الماسة بنظام المعالجة الآلية للمعطيات فقد توسع المشرع الجزائري في نطاق تجريم الأفعال التي قد تشكل جريمة تجسس إلكتروني، ولم يتم حصره فقط في فعل الدخول غير المشروع قصد الحصول على معلومات حكومية سرية بل شملت كل الأفعال الماسة بنظام المعالجة الآلية للمعطيات إذا كانت تستهدف الدفاع الوطني.[2]

وبالمقابل فقد قرر المشرع الجزائري أحكاما تتعلق بالاشتراك والشروع في ارتكاب الجرائم التي تمس نظام المعالجة الآلية المعطيات عموما كما أقر كذلك المسؤولية الجزائية للأشخاص المعنوية عن ذات الجرائم وهذا ما ينسجم مع ما أقرته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.[3]

كما نصت هذه الاتفاقية على أحكام إجرائية كان قد نص عليها المشرع الجزائري في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ووضع نظم وشروط وضوابط القيام بها مع الأخذ بعين الاعتبار أن القانون الجزائري قد صدر قبل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.[4]

الفرع الثاني

(1) نادية سلامي، المرجع السابق، ص300.

(2) المرجع نفسه، ص301.

(3) نفس المرجع و الموضع.

(4) المرجع نفسه، ص303.

اتفاقية بودابست

شكلت اتفاقية بودابست لمكافحة مختلف الجرائم المعلوماتية خطوة على مستوى التعاون الدولي وهي الوحيدة من حيث حجم الدول التي انظمت لها، و ترتكز أهمية هذه الاتفاقية بفعاليتها في إقرار إجراءات عملية تلتزم بها الدول المنظمة لها بإدراجها في قوانينها الوطنية والمشرع الجزائري رغم عدم المصادقة على هذه الاتفاقية إلا أنه نهج نهجها وتبنى تشريعها خاصة فيما يخص الجانب الموضوعي لمواجهة مثل هذه الجرائم.[1]

تضمنت اتفاقية بودابست 48 مادة كما أكدت الاتفاقية على ضرورة اتخاذ تدابير تشريعية لمكافحة الجرائم المعلوماتية ومخاطرها على الدول كما تضمنت عدة توصيات للدول الأعضاء لمكافحة الجريمة المعلوماتية، واعتبرت مرجعا مهما في مجال محاربة الجريمة السيبيرانية سواء بالنسبة للاتفاقيات اللاحقة لها أو بالنسبة للتشريعات الداخلية.[2]

وقد تناولت هذه الاتفاقية أحكاما موضوعية مفادها إلزام الدول الأطراف بتجريم مجموعة الأفعال التي تمس سرية وأمن بيانات الكمبيوتر ومنظوماته ومنها تحديدا فعل الدخول غير المشروع لمنظومة الكمبيوتر قصد الحصول على بيانات الكمبيوتر وفعل الاعتراض غير المشروع لخط سير البيانات باستعمال الوسائل التقنية بما في ذلك التقاط ما ينبعث من منظومة الكمبيوتر من موجات كهرومغناطيسية تحمل معها هذه البيانات، وفعل التدخل في البيانات الذي يقوم على إتلاف أو إلغاء أو إفساد أو تغيير أو تدمير للبيانات المتواجدة في الكمبيوتر وفعل إساءة استخدام الأجهزة، والملاحظ أن الأفعال المذكورة سابقا أفعال مشكلة للتجسس الالكتروني والذي جرمها المشرع الجزائري من خلال نصوص قانون

(1) سليمان قطاف وعبد الحليم بوقرين، "الآليات القانونية الموضوعية لمكافحة الجرائم السيبيرانية في ظل اتفاقية بودابست والتشريع الجزائري"، المجلة الأكاديمية للبحوث القانونية والسياسية، مجلد6، عدد1، 2022، ص334.

(2) المرجع نفسه، ص339.

العقوبات المنظمة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي اعتبرها تهديدا للدفاع الوطني.[1]

وبالعودة إلى الاتفاقية العربية نجد أنها قد نصت على ذات الأفعال السابقة باستخدام نفس المصطلحات لكن الفرق يمكن في أن الاتفاقية العربية قد نصت بشكل صريح وواضح على الحصول على معلومات سرية حكومية لكن بالمقابل أدرجت هذا الفعل ضمن النص الذي يتناول جريمة الدخول غير المشروع فقط، فهي بذلك قد جرمت سلوكا واحدا فقط من سلوكات التجسس الالكتروني وهو فعل الدخول غير المشروع لمنظمة معلوماتية بينما لم تحدد اتفاقية بودابست نوع البيانات أو المعلومات التي تتم عليها الاعتداءات أي لم تشترط أن تكون هذه المعلومات ذات طبيعة سرية أو غير سرية و تفادت الإشارة بشكل صريح للتجسس الإلكتروني وأدخلته ضمن الأحكام العامة المنصوص عليها فيها.[2]

ومن ناحية الأحكام الاجرائية فقد تضمنت هذه الاتفاقية كما هو الحال في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلزام الدول الأطراف بإدخال تعديلات على قوانينها الإجرائية الداخلية من حيث نصها على ضرورة تبني هذه الدول إجراءات التحري والتحقيق في البيئة الإلكترونية.[3]

وبالرغم من تأخر وعدم مصادقة العديد من الدول ومن بينها الجزائر على هذه الاتفاقية، إلا أنهم تقريبا تبنو نصوصها التجريمية في وضع نصوصهم الوطنية رغم عدم توقيعهم عليها لأسباب ربما ترتبط بمصالحهم السيادية وغيرها.[4]

المطلب الثاني

(1) نادية سلامي، المرجع السابق، ص307.

(2) المرجع نفسه، ص ص307-308.

(3) المرجع نفسه، ص308.

(4) سليمان قطاف وعبد الحليم بوقرين، المرجع السابق، ص253.

آليات التعاون الدولي في مواجهة الجريمة الإلكترونية

إن من خصائص التجسس الإلكتروني أنها جريمة إلكترونية عابرة للحدود الوطنية وعليه فمكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الاجرائي فمن المستحيل على الدولة مواجهة مثل هذه الجرائم ويتخذ التعاون الدولي عدة صور سنذكر صورتين منه، حيث سنتناول التعاون القضائي (الفرع الأول) وسنتطرق إلى تسليم المجرمين (الفرع الثاني).

الفرع الأول

التعاون القضائي

هي كل إجراء قضائي تقوم به الدولة لتسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم ويتعلق التعاون القضائي في مكافحة الجرائم في المجال الجنائي من خلال الاتفاقيات الدولية من خلال وجود الأدلة والقيام بالبحث وتقديم المعلومات.[1]

أولا-شروط التعاون القضائي:

1-تبادل المعلومات:

تتمثل في الأدلة والوثائق والمعلومات والمواد التي من شأنها أن تسهل مهمة المحاكمة ويشمل ذلك التبادل السوابق القضائية للجناة، ومكافحة الجرائم لا تتحقق إلا من خلال تعاون دولي حقيقي، وقد تبلور هذا النوع من التعاون منذ إنشاء المنظمة الدولية

(1) عادل عبد العال ابراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الاسكندرية، 2015، ص ص50-51.

للشرطة الجنائية كما تقوم هذه المنظمة بتشجيع التعاون الدولي بين أجهزة الشرطة في الدول الأطراف على نحو فعال في مكافحة الجريمة.[1]

2-نقل الاجراءات:

المقصود بنقل الاجراءات قيام إحدى الدول باتخاذ الاجراءات الجنائية بشأن جريمة ارتكبت داخل إقليم دولة أخرى، ولقد أقرت العديد من الاتفاقيات الدولية والإقليمية ذلك نذكر منها الاتفاقية النموذجية بشأن نقل الاجراءات في المسائل الجنائية واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطن والنموذج الاسترشادي لاتفاقية التعاون القانوني القضائي.[2]

3-الإنابة القضائية:

المقصود بالإنابة القضائية الدولية طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية بشأن جريمة ارتكبت في إقليم دولة أخرى، وتتقدم الدولة الطالبة إلى الدولة المطلوب إليها وذلك للفصل في مسألة معروضة على السلطة القضائية في الدول ويتعذر عليها القيام بها بنفسها، كما تهدف الإنابة إلى نقل الاجراءات في المسائل الجنائية لمواجهة ما تشهده الظواهر الاجرامية من تطور والتي تعترض سير الإجراءات الجنائية لقضايا تكون خارج الحدود الوطنية كما تستلزم الإنابة القضائية الدولية إرسال الملف الخاص بالدعوى الجنائية وتتضمن الاتفاقيات الدولية المبرمة في هذا العنصر شرطا باستبعاد وتنفيذ الأحكام في المجال السياسي والعسكري.[3]

الفرع الثاني

(1) عبد الرؤوف بوديسة بجاد، المرجع السابق، ص88.

(2) عادل عبد العال ابراهيم خراشي، المرجع السابق، ص ص54-55.

(3) المرجع نفسه، ص57-58.

تسليم المجرمين

يعرف تسليم المجرمين بأنه الإجراء الذي تقوم به الدولة استنادا لمعاهدة أو تأسيسا على المعاملة بالمثل، حيث تقوم دولة بطلب تسليم شخص من دولة أخرى لاتهامه أو لأنه محكوم عليه بعقوبة جنائية، كما قد تناولت العديد من الاتفاقيات والمؤتمرات الدولية موضوع تسليم المجرمين من أبرز هذه الاتفاقيات المؤتمر الأول للشرطة القضائية موناكو 1954، والمؤتمر الدولي للعقاب في لندن 1960.[1]

أولا-شروط تسليم المجرمين:

إن تسليم المجرمين يخضع للعديد من الشروط:

1-شرط التجريم المزدوج:

يقصد به أن يكون الفعل المطلوب التسليم من أجله مجرما في قوانين كلتا الدولتين الطالبة والمطلوب منها التسليم.[2]

والعبرة بالتجريم فقط دون الوصف القانوني للفعل لأنه من الممكن أن يختلف التكييف القانوني لفعل معين في الدول حسب تشريعاتها ويكون هذا الشرط في الدولة التي تطلب التسليم والدولة المطلوب منها التسليم ألا تكون الدعوى الجنائية قد انقضت أو سقطت بالتقادم وفق قانون إحدى الدولتين لأن غرض التسليم هو محاكمة الشخص أو تنفيذ عقوبة محكوم عليه بها، وهذا الإجراء يقوم أساسا على أن الدولة التي يتواجد على إقليمها المتهم

(1) المرجع نفسه، ص ص62-63.

(2) مليكة درياد، "أحكام تسليم المجرمين في قانون الاجراءات الجزائية"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد4، عدد1، 2019، ص10.

بارتكابه جريمة إلكترونية عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك أو تقوم بتسليمه لمحاكمته في دولة أخرى مختصة.[1]

2-الشروط المتعلقة بالأشخاص المطلوب تسليمهم:

عدم جواز تسليم الرعايا أيا كان نوع الجريمة المرتكبة من قبلهم في أي إقليم خارج دولتهم، كما لا يجوز تسليم ممنوحي حق اللجوء السياسي ومن تمت محاكمتهم عن ذات الجريمة المطلوب التسليم من أجلها.[2]

ثانيا-إجراءات تسليم المجرمين:

لا يمكن تسليم المجرمين إلا بناء على طلب تقدمه الدولة الطالبة إلى الدولة المطلوب منها التسليم كما تختلف الدول الطالبة بالنسبة للسلطة المختصة بالموافقة على طلب التسليم فالبعض يمنح للسلطة التنفيذية الاختصاص الكامل في هذا المجال، حيث تحيل الطلب إلى وزير العدل ليتحقق من سلامة الطلب ويبدي رأيه حوله ثم يحيله إلى رئيس الدولة الذي له الكلمة الأخيرة في اتخاذ قرار طلب التسليم والبعض الآخر من الدول لا تجيز تقديم طلب التسليم والبعض الآخر من الدول لا تجيز تقديم طلب التسليم إلا وفق حكم قضائي فإذا أصدر القضاء حكما يقضي بعدم التسليم امتنع على السلطة التنفيذية قرار طلب التسليم.[3]

المطلب الثالث

الصعوبات التي تواجه التعاون الدولي في مكافحة الجريمة الإلكترونية

(1) عبد الهادي حشيفة، التعاون الدولي في مجال الجرائم الالكترونية، مذكرة ماستر، جامعة زيان عاشور، كلية الحقوق و العلوم السياسية، قسم الحقوق، 2020، ص46.

(2) عادل عبد العال ابراهيم خراشي، المرجع السابق، ص69.

(3) مليكة درياد، المرجع السابق، ص13.

الفصل الثاني

آليات المتابعة الجزائية للتجسس الإلكتروني ضد أمن الدولة في التشريع الجزائري

إن التعاون الدولي في مواجهة الجرائم الإلكترونية العابرة للحدود كجريمة التجسس الإلكتروني ضد أمن الدولة رغم فعاليته في التصدي لمثل هذه الجريمة إلا أنه يواجه العديد من الصعوبات والعراقيل المختلفة والتي من شأنها أن تعطل تفعيله وتحول دون تحقيق أهداف هذا التعاون بالتالي ينتج عن ذلك إفلات المجرمين وعدم تحقيق العدالة الجنائية وإهدار لمصالح الدول والاخلال بنظامها الداخلي ولنستعرض هذه الصعوبات قسمنا المطلب لفرعين، حيث سنتناول الصعوبات في مكافحة الجريمة الإلكترونية على المستوى الوطني (الفرع الأول)، ثم نتطرق إلى الصعوبات في مكافحة الجريمة الالكترونية على المستوى الدولي (الفرع الثاني).

الفرع الأول

الصعوبات في مكافحة الجريمة الإلكترونية على المستوى الوطني

بما أن جريمة التجسس الإلكتروني تندرج تحت الجرائم الإلكترونية فأهم الصعوبات التي تواجه التعاون الدولي في مكافحة هذه الجريمة أنها صعبة الإثبات.

إذ أنه في الأصل تقع الجريمة في نفس مكان النشاط الجرمي، إلا أنه في الجريمة الالكتروني تقع الجريمة في كثير من الأحيان غير مكان البث مما يؤخر ذلك الجهات المختصة في اتخاذ ما يلزم من إجراءات التحقيق والاستدلال والتي تلعب دورا مهما في كشف الجريمة ذلك أن سلطات مكان البث لم يصل إلى علمها بعد وقوع الجريمة.[1]

(1) عزيزة لرقط، "التعاون الدولي في مكافحة الجرائم المعلوماتية"، مجلة التواصل في الاقتصاد وإدارة القانون، مجلد 25، عدد4، 2019، ص ص 3-4.

كما أن السلوك الجرمي في الجرائم الالكترونية ليس له أثر ملموس أي ولا وجود لأدلة مادية ملموسة يمكن أن تدرك بالحواس ذلك أن الدليل في مثل هذه الجرائم تكون عبارة عن نبضات إلكترونية لا مادية ذلك ما يتطلب قدرات في مجال المعلوماتية بالنسبة للمحقق حتى يستطيع أن يتعامل مع الأدلة و المحافظة عليها، إضافة لذلك فالفاعل في الجرائم الالكترونية كثيرا ما يأخذ احتياطاته التي تحول دون الوصول لكشف الجريمة ومعرفة الفاعل إذ أن باستطاعته تدمير دليل الإدانة بسهولة في ثوان معدودة بواسطة برامج متخصصة.[1]

فالمجرمين الذي يستخدمون الوسائل الالكترونية لارتكاب جرائهم يمتازون بالذكاء والإتقان في عملهم الذي يقومون به لذلك فهم يتمكنون من إخفاء أفعالهم غير المشروعة.[2]

وكثيرا ما يلجأ مرتكبو الجرائم الالكترونية لأهم الوسائل بهدف عرقلة جمع أدلة الإدانة ونجد من بين هذه الوسائل استخدام تقنية التشفير أو استعمالهم مسألة التدابير الأمنية لمنع مشكلة التفتيش والاطلاع على الأدلة وضبطها باستعمال كلمات السر أو إخفاء هويتهم خصوصا عند استخدامهم لشبكة الانترنت فيستعينون بالبرامج والتطبيقات التي تعمل على إخفاء وطمس هويتهم على شبكة الانترنت.[3]

ومن بين الصعوبات التي تواجه عملية استخلاص الدليل في الجريمة الإلكترونية نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة ذلك فيما يتعلق بثقافة الحاسوب والالمام بعناصر الجريمة الالكترونية وكيفية التعامل معها وذلك على الأقل بالنسبة للبلدان العربية.[4]

(1) المرجع نفسه، ص4.

(2) عماد بلغيث ويوسف جغلولي، "صعوبات التحقيق في الجرائم الالكترونية"، مجلة الرسالة للدراسات والبحوث الانسانية، مجلد6، عدد3، 2021، ص79.

(3) نفس المرجع والموضع.

(4) عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2007، ص122.

فالسلطات القائمة بالتحقيق بما لهم من خلفية قانونية تلعب دورا هاما في التحري والتحقيق في الجرائم التقليدية إلا أنهم لا يرتقون لنفس الدرجة من الخبرة عندما يتعلق الأمر بالجرائم الالكترونية وهذا نظرا لطبيعة الدليل الرقمي الذي يحتوي على مسائل فنية لا يقوى على فهمها سوى خبراء متخصصين.[1]

الفرع الثاني

الصعوبات في مكافحة الجريمة الإلكترونية على المستوى الدولي

يعترض التعاون الدولي في مجال مكافحة الجرائم الإلكترونية العديد من الاشكاليات والمعوقات التي تحول دون تحقيقه تتمثل في:

أولا–القصور التشريعي للدول:

إن اختلاف الدول في موروثها الثقافي والإجتماعي والإختلاف في المستوى السياسي أثر بشكل مباشر على السياسة التشريعية لكل دولة هذا ما جعل بعض الأنظمة القانونية تشكل عائقا كبيرا أمام التعاون الدولي، إذ أن هناك دولا تستشعر خطورة بعض الأفعال فتجرمها في قوانينها الداخلية ومن جهة أخرى هناك دول لم تجرم هذه الأفعال مما جعلها أفعالا مباحة تطبيقا لمبدأ الشرعية.[2]

كمثال في جريمة التجسس الإلكتروني التي تعتبر جريمة بموجب القانون الداخلي لكثير من الدول لكن القانون الدولي الإنساني قد عالج طريقة التعامل مع الجواسيس أثناء

(1) عماد بلغيث ويوسف جغلولي، المرجع السابق، ص80.

(2) عزيرة لرقط، المرجع السابق، ص4.

النزاعات المسلحة إلا أن الإشكالية عدم معالجة القانون الدولي لجريمة التجسس التي تحدث وقت السلم وهذا ما يجعلها أفعالا مباحة.[1]

ثانيا-تنازع الإختصاص القضائي الدولي:

ينجم عن اختلاف النظم والتشريعات القانونية تنازع في الاختصاص بين الدول خصوصا في إطار الجرائم التي تتعلق بالأنترنت التي تتميز بكونها جرائم عابرة للحدود فيحدث أن ترتكب الجريمة في إقليم دولة معنية من قبل أجبني هنا تخضع الجريمة الاختصاص الجنائي للدولة الثانية ذلك تطبيقا لمبدأ الاختصاص الشخصي وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل في اختصاصها استنادا لمبدأ العينية.[2]

مثل ما تم شرحه سابقا في إعمال مبدأ العينية على جريمة التجسس الإلكتروني، ويلاحظ أن اختصاص القضاء بنظر الجرائم التي تتم عبر الانترنت والقانون الواجب التطبيق على الفعل لا يتسم بالوضوح أمام حقيقة أن غالبية هذه الأفعال تتم من قبل أشخاص خارج حدود الدولة أو أنه تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام الدولة نفسها، وهذا ما يبرز أهمية اختبار مدى ملائمة قواعد الاختصاص والقانون الواجب تطبيقه وما إذا كانت القواعد والنظريات تطال هذه الجرائم أم يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها وما تثيره من مشكلات في مسألة الاختصاص القضائي.[3]

ثالثا-إشكالية الإنابة القضائية:

(1) فاطمة الظبيري، المرجع السابق، ص231.

(2) يوسف صغير، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2013، ص ص 135-136.

(3) المرجع نفسه، ص136.

تتمثل إشكالية الإنابة القضائية في إشكالية فكرة السيادة وكذا إشكالية البطء في الإجراءات، حيث تتمثل اشكالية فكرة السيادة في الحالة التي يرتكب فيها الجاني جريمة على إقليم دولة ما وتجرى محاكمته في دولة أخرى وحتى تقام محاكمة عادلة لابد من جمع الأدلة التي تثبت الجريمة لتنسب للجاني، وهذا لا يتحقق إلا على إقليم الدولة التي كانت مسرحا للجريمة وهذا ما يعرف بالتعاون القضائي الدولي، إلا أن هذا التعاون يصطدم مع فكرة السيادة التي تتمسك بها الدولة على إقليمها بحيث لا تسمح لدولة أخرى القيام بالإجراءات على إقليمها إنما تقوم بها عن طريق أجهزتها القضائية باعتبار أن لها الحق في الاختصاص بالفصل في كافة الجرائم المرتكبة على إقليمها اعتمادا على فكرة السيادة.[1]

أما عن إشكالية البطء في الإجراءات فإن طلبات الإنابة القضائية الدولية تسلم بالطرق الدبلوماسية وهذا يجعلها تتسم بالتعقيد والبطء والذي قد يتعارض مع طبيعة الجرائم المعلوماتية التي تتميز بالسرعة، هذا الأمر انعكس سلبا على التعاون الدولي في مكافحة مثل هذه الجرائم.[2]

رابعا-إشكاليات خاصة بتسليم المجرمين:

من الصعوبات التي تواجه التعاون الدولي في مكافحة الجرائم الالكترونية فيما يخص تسليم المجرمين نجد اشكاليتين:

1-إشكالية ازدواجية التجريم:

إن ازدواجية التجريم يعد شرطا مهما من شروط نظام تسليم المجرمين فذلك يعد عائقا أما التعاون الدولي في مجال محاربة الجرائم الالكترونية خاصة أن كثيرا من الدول لا تجرم هذه الجرائم بحيث تكون صعوبة في تحديد ما إذا يمكن تطبيق النصوص التقليدية على

(1) عزيزة لرقط، المرجع السابق، ص ص5-6.

(2) عبد الهادي حشيفة، المرجع السابق، ص51.

الجرائم المعلوماتية لدى الدولة المطلوب منها التسليم، وهذا ما يؤدي لعدم تفعيل الاتفاقيات الدولية في مجال تسليم المجرمين و بالتالي عدم تحقيق العدالة.[1]

2-التزاحم في طلبات التسليم:

المقصود بذلك قيام دولتين أو عدة دول بتقديم طلب التسليم عن نفس الشخص سواء كان الطلب متعلقا بذات الجريمة أو لجرائم أخرى، وتتحقق هذه الإشكالية في الجرائم الإلكترونية عندما يرتكب الجاني فعلا إجراميا يمس مصالح أساسية لأكثر من دولة وعليه فكل دولة تضررت من فعله الإجرامي يمكنها تقديم طلب التسليم إلى الدولة المطلوب منها، وطلب التسليم يجب أن يكون مبنيا على أدلة تثبت قيام الجاني بالأفعال التي نسبت إليه وليس مجرد إدعاء ويشترط أن يكون إرسال الطلب بصورة فعلية وليس مجرد تصريحات شفوية.[2]

(1) آسية صوان، التعاون الدولي في مكافحة الجرائم المعلوماتية، مذكرة ماستر، جامعة عبد الحميد بن باديس، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2022، ص78.

(2) عزيزة لرقط، المرجع السابق، ص6.

خاتمة

خاتمة:

في ختام دراستنا لموضوع التجسس الإلكتروني ضد أمن الدولة تبين لنا أن جريمة التجسس الإلكتروني هي في الواقع صورة مستحدثة لجريمة التجسس التقليدية، إلا أن ارتباطها بالوسائل التكنولوجية قد غير من طبيعتها لتصبح واحدة من الجرائم الالكترونية التي سعى المشرع الجزائري لمكافحتها نظرا لما لها من تأثير سلبي على استقرار الدولة وأمنها في ظل المفهوم الجديد والسائد لحرب التكنولوجيا في العصر الحالي.

وعلى ضوء ذلك توصلنا من خلال دراستنا لمجموعة من النتائج أهمها:

1. عدم وجود تعريف محدد وموحد لجريمة التجسس الإلكتروني وخصوصا في التشريع الجزائري الذي أدرج هذه الجريمة تحت اسم جرائم المساس بأنظمة المعالجة الآلية المعطيات.
2. أن للتجسس الإلكتروني خصائص مشتركة مع التجسس التقليدي فكلاهما يعتبر من الجرائم الماسة بأمن الدولة وكلاهما يرتكبها فرد أجنبي، كما يختلف التجسس الإلكتروني عن التجسس التقليدي في كونه جريمة عابرة للحدود وجريمة يصعب الكشف عنها واثباتها نظرا لطبيعتها.
3. أن وسائل ارتكاب التجسس الالكتروني عديدة منها ما يرتكب بواسطة أنظمة اتصالات، ومنها ما يرتكب بواسطة أنظمة المعالجة الآلية للمعطيات.
4. تشكل أسرار الدفاع الوطني المحل الذي ينصب عليه التجسس بصفة عامة والموضوع الذي تهدف الدولة لحمايته.
5. أقر المشرع الجزائري أحكاما إجرائية خاصة لمكافحة الجريمة الإلكترونية بصفة عامة، ومن ضمنها التجسس الإلكتروني ضد أمن الدولة وذلك في قانون الاجراءات الجزائية وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال 09-04.

وعلى ضوء النتائج المتوصل إليها يمكن وضع جملة من التوصيات تتمثل في:

1. يتعين على المشرع الجزائري سن نصوصا قانونية محددة وواضحة لجريمة التجسس الإلكتروني ضد أمن الدولة.
2. على الدولة الجزائرية أن تهتم بالجانب الوقائي إلى الجانب الإجرائي الردعي لوضع حد لهذه الجريمة الخطيرة.
3. على المشرع الجزائري أن يحدث نصوصا تشريعية متعلقة بالجرائم الالكترونية بصفة عامة لمواكبة التطور التكنولوجي، فجريمة التجسس الإلكتروني تشهد تطورا كل سنة في وسائل ارتكابها.
4. رسم سياسة دفاع إلكترونية وذلك بالاستفادة من تجارب وخبرات الدول المتقدمة في المجال التقني.

قائمة المراجع

قائمة المراجع والمصادر:

اولا-الاتفاقيات:

1. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر سنة 2014

ثانيا-القوانين:

1. الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون الاجراءات الجزائية المعدل والمتمم.
2. قانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156، المتضمن قانون العقوبات، جريدة رسمية، عدد71.
3. قانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 66-155 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الاجراءات الجزائية، جريدة رسمية، عدد 14.
4. قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، جريدة رسمية، عدد47، الصادر بتاريخ 25 شعبان عام 1430 الموافق 16 غشت سنة 2009.
5. 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.

ثالثا-الكتب:

1. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة 15، دار هومة، 2019.

2. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2008.
3. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية شارع زكريا غنيم الابراهيمية، الإسكندرية، 2008.
4. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009.
5. عادل عبد العال ابراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الاسكندرية، 2015.
6. عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، الطبعة الأولى، دار المستقبل للنشر والتوزيع، عمان، 2009.
7. عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2007.
8. محمد عودة الجبور، الجرائم الواقعة على أمن الدولة وجرائم الإرهاب، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، 2011.

رابعا-الرسائل الجامعية:

- **أطروحات الدكتوراه:**

1. نادية سلامي، آليات مكافحة التجسس الالكتروني، رسالة دكتوراه، جامعة العربي التبسي، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2019.
2. هبة نبيلة هروال، جرائم الانترنت دراسة مقارنة، رسالة دكتوراه، جامعة أبي بكر بلقايد، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2014.
3. خضرة شنيتر، الآليات القانونية لمكافحة الجريمة الإلكترونية، رسالة دكتوراه، جامعة احمد دراية، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021.

- **مذكرات الماجستير:**

1. يوسف صغير، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2013.

- **مذكرات الماستر:**

1. آسية صوان، التعاون الدولي في مكافحة الجرائم المعلوماتية، مذكرة ماستر، جامعة عبد الحميد بن باديس، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2022.
2. آسية والي وسامية باشوش، الجرائم الماسة بأمن الدولة، مذكرة ماستر، جامعة آعلي محند أو لحاج، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2016.
3. عبد الهادي حشيفة، التعاون الدولي في مجال الجرائم الالكترونية، مذكرة ماستر، جامعة زيان عاشور، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2020.
4. عبد الرؤوف بوديسة بجاد، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة ماستر، جامعة محمد البشير الابراهيمي، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022.
5. راوية هدى وجرادي فاطمة الزهراء، الإطار الموضوعي للجريمة المعلوماتية، مذكرة ماستر، جامعة ابن خلدون، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2019.
6. رزق الله برهان، جريمة التجسس (أمن الدولة)، مذكرة ماستر، جامعة العربي التبسي كلية الحقوق والعلوم السياسية، قسم الحقوق، 2018.
7. زهية معمش ونسيمة غانم، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة ماستر، جامعة عبد الرحمان ميرة، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، 2013.
8. حسام زغيدة وعمر بعلوج، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، جامعة الشاذلي بن جديد، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2023.

خامسا-المقالات:

قائمة المراجع

1. إلهام بن خليفة وجمال غريسي، "التجسس الإلكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري"، مجلة دفاتر السياسة والقانون، جامعة الشهيد حمة لخضر، الوادي، مجلد 14، عدد 1، 2022.
2. بسمة مامن، "جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري"، مجلة الحقوق والعلوم السياسية، مجلد9، عدد 1، 2022.
3. حفصي عباس، "التجسس الإلكتروني في الشريعة والقانون"، مجلة الواحات للبحوث والدراسات، مجلد12 عدد1، 2019.
4. حنان أوشن وعماد الدين وادي، "التجسس الالكتروني وآليات مكافحته في التشريع الجنائي الجزائري"، مجلة الحقوق والعلوم السياسية، مجلد1، عدد2، 2014.
5. سامية بوشوشة وحياة سلماني، "التجسس الالكتروني وطرق مكافحته"، مجلة العلوم الاجتماعية والانسانية، جامعة باجي مختار، عنابة، مجلد 16، عدد1، 2023.
6. سليمان قطاف وعبد الحليم بوقرين، "الآليات القانونية الموضوعية لمكافحة الجرائم السيبيرانية في ظل اتفاقية بودابست والتشريع الجزائري"، المجلة الأكادمية للبحوث القانونية والسياسية، مجلد6، عدد1، 2022.
7. صالح شنين، "اجراءات التحري والتحقيق في جرائم تكنولوجيات الإعلام والاتصال في التشريع الجزائري"، مجلة الدراسات القانونية، مجلد 1، عدد 1، 2014.
8. عبد الهادي محمود الزيدي، "التجسس الاسرائيلي على الدول العربية"، مجلة مركز الدراسات الاستراتيجية والدولية، مجلد1، عدد58، 2013.
9. عزيزة لرقط، "التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة التواصل في الاقتصاد وإدارة القانون، مجلد 25، عدد4، 2019.
10. عماد بلغيث ويوسف جغلولي، "صعوبات التحقيق في الجرائم الالكترونية"، مجلة الرسالة للدراسات والبحوث الانسانية، مجلد6، عدد3، 2021.
11. فاطمة الظبيري، "القانون الدولي والهجمات الإلكترونية ما دون استخدام القوة"، المجلة الدولية للقانون، مجلد11، عدد1، 2022.

12. فايزة نجاري بن حاج علي، "جريمة التجسس الإلكتروني"، استراتيجيا مجلة دراسات الدفاع والاستقبالية، مجلد6، عدد11، 2019.
13. فتيحة خالدي، "تأثير التجسس الالكتروني على الحق في الخصوصية المعلوماتية"، مجلة البحوث في الحقوق والعلوم السياسية، مجلد7، عدد1، 2021.
14. فتيحة مناد، "مدى شرعية الاستطلاع العسكري والتجسس من الفضاء الخارجي باستخدام الأقمار الصناعية–دراسة قانونية"، مجلة القانون العام الجزائري والمقارن، مجلد 4، عدد2، 2018.
15. فوزي عمارة، "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية"، مجلة العلوم الإنسانية، مجلد 21، عدد1،2010.
16. مريم بناش وسعاد بولقرون، "التجسس وانتهاك حق الخصوصية في العصر الرقمي دراسة وصفية تحليلية لبرنامج (بيغاسوس)"، مجلة الدراسات الإعلامية والاتصالية، مجلد2، عدد3، 2022.
17. مريم عراب، "الاختصاص القضائي في الجرائم المعلوماتية"، مجلة حوليات كلية الحقوق والعلوم السياسية، مجلد7، عدد3، 2015.
18. مليكة درياد، "أحكام تسليم المجرمين في قانون الاجراءات الجزائية"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد4، عدد1، 2019.

سادسا–المواقع:

1. International Reviem of red crass, H. Montealegre Klenner: la sécurité de l'état et les droits de l'homme. https://www.google.com /search? client: fire fox-b. la sécurité + de + l'état+ et + les + droits + de + l'homme consulté le 25 mai 2024.