المواجهة التشريعية لجريمة التجسس الالكتروني في ظل القانون 24-06

The legislative confrontation of cyber espionage crime in light of law 26-04

هاشمي رشيدة*، مخبر بحث الحقوق والعلوم السياسية، جامعة عمار ثليجي -الأغواط-
r.hachemi@lagh-univ.dz
مليايني عبد الوهاب، مخبر بحث الحقوق والعلوم السياسية، جامعة عمار ثليجي -الأغواط-
abdel.meliani@lagh-univ.dz

تاريخ إرسال المقال: 30/ 01/ 2025 تاريخ قبول المقال: 29/ 04/ 2025 تاريخ نشر المقال: 13/ 05/ 2025

الملخص:

مع تسارع التطور التكنولوجي وزيادة الاعتماد على الأنظمة الرقمية في شتى ميادين الحياة والتي أصبحت جزءا لا يتجزأ من حياتنا اليومية، الامر الذي أدى الى بروز تحديات جديدة ازدادت معها المخاطر المصاحبة لها، مما فتح الباب امام ظهور جرائم جديدة وأخرى مستحدثة، أبرزها جريمة التجسس الالكتروني التي اصبحت تشكل تهديدا حقيقيا يواجه الأفراد والمؤسسات، فالتجسس الذي كان يقتصر سابقا على العالم المادي انتقل اليوم إلى الفضاء الرقمي، مما سهل اختراق الأنظمة وسرقة البيانات الحساسة والتلاعب بها، وبالتالي أضحى يشكل تهديدا خطيرا على الأمن القومي والاقتصادي والاضرار بالمصالح الحيوية للدول.

الكلمات المفتاحية: التجسس، التجسس الالكتروني، الجريمة الالكترونية، الفضاء الرقمي.

Abstract:

The rapid advancement of technology has led to an increased reliance on digital systems in all aspects of life, making them an integral part of our daily routines. With this evolution, new challenges have emerged and risks have escalated, giving rise to novel and sophisticated crimes, most notably cyberespionage. This crime poses a significant threat to individuals and organizations alike, as espionage, once confined to the physical world, has now migrated to the digital realm, facilitating the infiltration of systems, theft of sensitive data, and manipulation thereof. Such actions pose a serious threat to national and economic security.

Key words: Cyber espionage, Cybercrime, Cyberspace, Espionage

المقدمة:

لقد أحدثت الثورة التكنولوجية تحولا جذريا في طبيعة الجرائم التقليدية عامة وجريمة التجسس خاصة، فبعد أن كانت مقتصرة على جمع المعلومات بطرق تقليدية، أصبحت الان تستغل أحدث التقنيات والبرمجيات لاختراق الأنظمة الحاسوبية وسرقة البيانات الحساسة، وقد أدى هذا التحول الى تطور طبيعة مرتكبي جرائم التجسس، فبعد أن كان الجاسوس شخصية تقليدية تعمل في الخفاء، ظهرت فئة جديدة من

* المؤلف المرسل.

المجرمين أصحاب الكفاءات التقنية العالية الذين يستغلون مهاراتهم في مجال الحاسوب لارتكاب هذه الجرائم والذين يطلق عليهم اسم "ذوي الياقات البيضاء".

تعد جريمة التجسس الالكتروني انتهاكا غير مشروع للأنظمة الحاسوبية وشبكات الاتصالات بهدف الحصول على معلومات سرية أو حساسة، وتتنوع أشكال هذه الجريمة، بدءا من اختراق حسابات الأفراد وسرقة معلوماتهم وانتهاءا باختراق أنظمة الحكومات والشركات الكبرى للاستيلاء على أسرارها التجارية والعسكرية.

امام خطورة الجرائم الالكترونية المتزايدة، سارعت العديد من التشريعات المقارنة إلى وضع أنظمة وقوانين لحماية المعلومات الرقمية من الاختراق والتلاعب، والمشرع الجزائري بدوره سارع بسن أحكام قانونية لمواجهة الجرائم الالكترونية عامة بما فيها جريمة التجسس الالكتروني، وفي ظل غياب نص صريح ينظم جريمة التجسس الالكتروني بشكل مستقل، يلجأ الفقه والقضاء إلى تكييف هذه الأفعال ضمن أحكام المواد من 394 مكرر إلى 394 مكرر7 من قانون العقوبات المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات المستحدثة بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004 والمعدلة بموجب القانون 24-06 المؤرخ في 28 أفريل 2024، هذا التكييف يثير تساؤلات حول: **مدى كفايته في تغطية كافة جوانب التجسس الإلكتروني خاصة في ظل التطور المتسارع للتكنولوجيا؟**

وللإجابة على الاشكال المطروح اعتمدنا في دراستنا على المنهج الوصفي التحليلي، من خلال استعراض تعريف التجسس عامة والتجسس الالكتروني خاصة وتبيان خصائصه وذكر أنواعه (المبحث الأول)، ومن ثم تحليل السياسة الموضوعية للمشرع الجزائري في مواجهة جريمة التجسس الالكتروني من خلال تحليل نصوص القسم السابع مكرر من قانون العقوبات الجزائري حتى يتسنى لنا معرفة العناصر المكونة لجريمة التجسس الالكتروني والعقوبات المقررة لها (المبحث الثاني).

المبحث الأول: الإطار المفاهيمي للتجسس الالكتروني

مع تطور التكنولوجيا وتوسع نطاق استخدام شبكة الانترنت، تحول التجسس من مجرد نشاط تقليدي إلى تهديد إلكتروني متطور يستهدف الوصول الى المعلومات الشخصية او السرية بطرق غير مشروعة، هذا النشاط يتطلب درجة عالية من التقنية والمعرفة التكنولوجية، يعتمد فيه المجرمون مجموعة متنوعة من الأساليب التكنولوجية المتطورة للقيام بجرائم التجسس الالكتروني كما يستغلون الثغرات الأمنية في البرامج والتطبيقات الشائعة للوصول الى البيانات الحساسة هذه الأساليب تتطور باستمرار لتواكب التقدم التكنولوجي وهو ما يجعل مكافحتها تحديا كبيرا، مما يقتضي بيان مفهوم التجسس عامة وتبيان المقصود بالتجسس الالكتروني خاصة (المطلب الأول)، ومن ثم التعرف على أبرز أنواع التجسس الالكتروني (المطلب الثاني).

المطلب الأول: مفهوم التجسس الالكتروني

مع تزايد الاعتماد العالمي على شبكة الانترنت في شتى الميادين والمجالات، أصبح التجسس الالكتروني يشكل تهديدا متناميا للأفراد والمؤسسات والدول، مما زادت معه الحاجة إلى فهم طبيعة هذا النوع من التجسس وكيفية مواجهته، وعليه فإن تحديد مفهوم التجسس المعلوماتي يتطلب فهم التجسس بصفة عامة، ثم تبيان المقصود بالتجسس الالكتروني واستكشاف الخصائص المميزة له.

الفرع الأول: تعريف التجسس الالكتروني

سنتناول تعريف التجسس بصفة عامة (أولا)، ومن ثم تبيان المقصود بالتجسس الالكتروني (ثانيا)

أولا: تعريف التجسس عامة

التجسس لغة مشتق من الفعل جس يجس جسست جسا، فهو جاسوس والمفعول مجسوس، والجس هو جس الخبر، وتجسسه بحث عنه، أي تفحصه، ومنه الجاسوس، وجس الشخص بعينه أحد النظر اليه ليستبينه ويستثبته[1]، والتجسس بالجيم التفتيش عن بواطن الأمور، والجاسوس هو صاحب سر الشر، وهو العين الذي يتجسس الاخبار[2].

كما عرفه قاموس Oxford بأنه نشاط للحصول السري على معلومات سياسية او عسكرية مهمة عن دولة اخرى او اكتشاف اسرار شركة أخرى باستخدام الجواسيس[3] اما قاموس Merriam Webster عرفه على انه ممارسة التجسس او استخدام الجواسيس للحصول على معلومات حول خطط وانشطة حكومة اجنبية او شركة منافسة بشكل خاص. [4]

اما التجسس في معناه الاصطلاحي يقصد به البحث والتنقيب عما يتعلق بالعدو من معلومات سرية باستخدام الوسائل السرية والفنية او العملاء والجواسيس من اجل نقل هذه المعلومات للاستفادة منها في اعداد الخطط. [5]

ولقد تعددت التعريفات القانونية للتجسس، فالبعض عرفه بأنه الدخول أو محاولة الدخول الى الأماكن المحظورة للحصول على أشياء او وثائق او معلومات يجب أن تبقى مكتوبة حرصا على سلامة الدولة او سرقة هذه الأشياء او الاستحصال عليها او انشاؤها او ابلاغها دون سبب مشروع.[6]

وعرف بانه البحث عن أي نوع من المعلومات خفية عن دولة معينة بهدف ايصالها الى دولة اجنبية وذلك بنية الاضرار بالدولة التي يتجسس عليها.[7]

وبأنه نوع من أنواع العمل الاستخباري هدفه البحث والحصول على المعلومات المتعلقة بدولة ما ونقلها بطرق سرية خاصة من مكانها الى مكان اخر بواسطة عملاء دولة أخرى.[8]

بالرغم من اعتبار التجسس كتهديد للأمن القومي، إلا أن التشريعات الدولية والمحلية تفتقر إلى تعريف جامع وشامل له، وغالبا ما تكتفي هذه التشريعات بتحديد مجموعة من الأفعال التي تعتبر جرائم تجسس، دون الدخول في تفاصيل دقيقة حول ماهية التجسس بحد ذاته، والمشرع الجزائري لم يعطي تعريفا للتجسس على

غرار باقي التشريعات الوطنية كالمشرع المصري والعراقي والفرنسي واكتفى فقط بتحديد صور السلوك المجرم للجريمة.

ثانيا: تعريف التجسس الالكتروني

لا يختلف التجسس الالكتروني جوهريا عن التجسس التقليدي من حيث الهدف، ألا وهو الحصول على معلومات سرية بشكل غير مشروع، إلا أنه يختلف عنه في الأداة المستخدمة، وهي تكنولوجيا المعلومات التي تتيح للجاسوس الإلكتروني الوصول إلى كم هائل من البيانات بسرعة وسهولة، مما يجعل عملية التجسس أكثر تعقيدا وصعوبة في الكشف عنها.

وقد تباينت آراء الفقهاء حول تعريف التجسس الالكتروني ، فمنهم من يرى أنه يشمل أي فرد أو مجموعة أو دولة تقوم بجمع معلومات بطرق غير مشروعة، ومنهم من يضيق هذا التعريف ليشمل فقط الدول والجهات الرسمية.[9]

عرفه البعض الاخر بأنه استغلال التكنولوجيا الحديثة للدخول غير مشروع لأنظمة المعلومات الالكترونية الحساسة التابعة للدول أو المؤسسات، بهدف الحصول على معلومات سرية ذات قيمة استراتيجية، مثل المعلومات العسكرية والأمنية والسياسية والاقتصادية والعلمية.[10]

كما عرف التجسس الالكتروني بأنه استخدام التقنيات الحديثة لاختراق الأنظمة المعلوماتية والحصول على معلومات حساسة بشكل غير مشروع، بهدف التلاعب بالبيانات والمعلومات المخزنة فيها، ويتضمن ذلك نقل الملفات، وحذفها، وإضافتها، والتحكم في عمليات الجهاز مثل الطباعة والتصوير والتخزين، ويهدف هذا النوع من التجسس، سواء كان فرديًا أو منظمًا، إلى جمع معلومات حساسة عن الأفراد أو الدول أو المنظمات او المؤسسات، وذلك باستخدام الأدوات التقنية المتاحة في عصر المعلومات.[11]

يعد التجسس الالكتروني شكل من اشكال الإرهاب الالكتروني فهما نوع من العدوان او التخويف او التهديد المادي او المعنوي الصادر من الدول او الجماعات او الافراد على الانسان في دينه او نفسه او عرضه او عقله او ماله بغير حق باستخدام الموارد المعلوماتية والوسائل الالكترونية بشكل سلبي من اجل احداث اثار مدمرة واضرار بالغة وكبيرة لمحطات التحكم وأجهزة الكمبيوتر وشبكات الاتصال بدوافع مختلفة. [12]، فالدمار الذي يلحقه الهجوم الإرهابي بأنظمة المعلومات التي تتحكم في كل مرافق الحياة قد يعطل حياة مجتمع بأكمله، وعليه فانه من المتوقع ان تكون الطرق الالكترونية للتجسس على المعلومات أكثر الطرق استخداما في المستقبل من قبل التنظيمات الإرهابية نظرا لأهمية المعلومات خاصة المعلومات السياسية والعسكرية والاقتصادية، فالحصول على هذه المعلومات واستغلالها يضر بالمصلحة العامة والوحدة الوطنية للدولة.[13]

من خلال ما سبق يمكننا القول أن جريمة التجسس الالكتروني هي جريمة عابرة للحدود الوطنية، تستغل التكنولوجيا الحديثة للوصول غير المشروع الى الأنظمة الحاسوبية وسرقة البيانات الحساسة، وعلى الرغم من

اختلاف وسائل تنفيذها عن التجسس التقليدي، الا انها تتفق معه في الهدف الأساسي وهو الحصول على معلومات سرية بشكل غير مشروع.

الفرع الثاني: خصائص التجسس الالكتروني

يتميز التجسس المعلوماتي بعدة خصائص من بينها:

- تعد جريمة التجسس المعلوماتي من الجرائم الناعمة التي لا تستدعي استعمال العنف والقوة بل تحتاج الى مجهود ذهني وجهاز كمبيوتر وشبكة انترنت وبعض البرامج فقط.
- تتميز جريمة التجسس الالكتروني بطبيعتها العابرة للحدود بسبب استخدام شبكة الانترنت التي لا تعترف بالحدود الجغرافية، فالمقدرة الهائلة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين الأنظمة المختلفة والبعيدة أدت الى تأثر اشخاص كثيرة من دول مختلفة بالتجسس المعلوماتي الذي قد يرتكب في حاسوب موجود في دولة معينة لكن النتيجة الاجرامية تتحقق في دولة أخرى.[14]
- صعوبة اكتشاف جريمة التجسس الالكتروني لعدم وجود أي دليل مادي ملموس من جهة، ومن جهة أخرى امتناع المجني عليه عن تقديم شكوى في غالب الأحيان خاصة الشركات التجارية خشية الاضرار بسمعتهم وأعمالهم.
- تعد جريمة التجسس الالكتروني من الجرائم صعبة الاثبات باعتبار ان الركن المادي للجريمة يرتكب في إطار واقع غير ملموس وهو مجال الحاسوب والانترنت عبر النظام المعلوماتي، وهو ما يثير مشكلة تحديد الدولة صاحبة الاختصاص القضائي والقانون الواجب التطبيق وإجراءات الملاحقة القضائية.[15]

المطلب الثاني: أنواع التجسس الالكتروني

التجسس الالكتروني هو مصطلح واسع يشمل مجموعة متنوعة من الأنشطة غير المشروعة التي تهدف إلى الحصول على معلومات حساسة بشكل غير قانوني عبر الأنظمة الرقمية، يمكن تصنيف هذه الأنشطة إلى عدة أنواع سواءا من ناحية المعلومات المستهدفة (الفرع الأول)، او من ناحية الوسيلة المستعملة (الفرع الثاني).

الفرع الأول: أنواع التجسس الالكتروني حسب المعلومات المستهدفة

يرى الأستاذ Ulrich sieber أن المعلومات ليست مجرد عنصر مساعد بل هي عامل أساسي في عالمنا المعاصر، شأنه شأن الطاقة والمادة، وتؤكد الأبحاث أن قيمة المعلومات تتجاوز كونها مجرد أداة اقتصادية أو ثقافية أو سياسية، بل إنها تشكل قوة محركة ذات قدرة على خلق مخاطر استثنائية. [16]

وفي سياق جريمة التجسس الالكتروني، تعد المعلومات العسكرية والاقتصادية والاجتماعية والعلمية هدفا رئيسيا للجواسيس الالكترونيين الذين يسعون للاستفادة منها لتحقيق مكاسب غير مشروعة.

أولا: التجسس العسكري

تعتبر المعلومات العسكرية من أكثر الأنواع حساسية وسرية، حيث تشمل كل ما يتعلق بالجيوش والقوات المسلحة، بما في ذلك الخطط الحربية، الأسلحة، المعدات، التكنولوجيا العسكرية، والمواقع الاستراتيجية. هذه المعلومات ذات أهمية قصوى للأمن القومي للدولة، وتسريبها قد يؤدي إلى عواقب وخيمة.[17]

من بين الحالات التي تم اكتشافها، في عام 1989 قام 3 طلبة ألمان بالعمل لحساب المخابرات السوفياتية حيث قاموا بمدها بالشيفرات الخاصة بأنظمة حاسبات غاية في الأهمية ومنها نظام الحاسوب الخاص بوزارة الدفاع الامريكية ومعمل للأبحاث في لو لاموس واحدى الشركات الفرنسية ومعاهد علمية متفرقة في أوروبا وامريكا الشمالية واليابان، وتمكن الجناة من الدخول الى أنظمة الحاسبات سالفة الذكر عبر شبكات المعلومات وتمكنوا من استغلال بعض الثغرات التي تعتري الإجراءات الأمنية لهذه الأنظمة للحصول على الشيفرات الخاصة بها، ولقد تم اكتشاف الجناة بالصدفة واستغرقت عملية تتبعهم عاما كاملا قدموا بعده للمحاكمة امام القضاء الألماني ووجهت لهم تهمة التجسس لصالح دولة اجنبية .[18]

ثانيا: التجسس الاقتصادي والتجاري

يعد الاقتصاد الركيزة الأساسية لأمن الدول واستقرارها، يهدف هذا النوع من التجسس الى الحصول على معلومات حساسة حول الموارد الطبيعية، والبنى التحتية، والسياسات الاقتصادية، والأسرار التجارية للدول المنافسة، والهدف من وراء ذلك هو تقييم القوة الاقتصادية لهذه الدول، وتحديد نقاط ضعفها، واستغلال هذه المعلومات لتحقيق مكاسب عسكرية او صناعية او تجارية.[19]

من بين الحالات التي تم الكشف عنها سنة 1990 ان مكتب التحقيقات الفيدرالي الأمريكي ووكالة الاستخبارات المركزية ألقت القبض على أعضاء في جهاز الاستخبارات الفرنسية بعد ان ضبطوا متلبسين بجريمة التجسس على أكبر شركات الحاسوب الامريكية وخصوصا شركتي IBM وT exas Instruments ويذكر ان الجواسيس الفرنسيين قد تمكنوا من الدخول الى قواعد البيانات الخاصة بالمعلومات الداخلية للشركتين وذلك بغية الكشف عن خططهما وأسرارهما الصناعية.[20]

ثالثا: التجسس السكاني والاجتماعي

تجمع الدول كمًا هائلا من البيانات الديمغرافية والاجتماعية لتخطيط مستقبلها، تشمل هذه البيانات معلومات حول عدد السكان، توزيعهم الجغرافي، دينهم، أصلهم، مستويات معيشتهم، ونسبة الجنسين، ويتم تخزين هذه البيانات الحساسة في أنظمة معلومات إلكترونية، مما يجعلها عرضة للاختراق والاستغلال من قبل جهات داخلية أو خارجية تسعى لاستخدامها في تحقيق أغراض خاصة.[21]

من بين الحالات التي تم الكشف عنها، قيام موظفين من العاملين بمركز حاسوب في السويد بنسخ برامج مسجل عليها إحصاءات وبيانات سكانية، حيث قاما ببيعها بعد ذلك الى أحد المكاتب الخاصة بالإحصاءات والبيانات مقابل ثمن رخيص.[22]

رابعا: التجسس العلمي

تهدف الدول وخاصة الكبرى، إلى التجسس العلمي للحصول بشكل غير مشروع على معلومات سرية عن الأبحاث والدراسات والاختراعات في مختلف المجالات، سواء كانت عسكرية أو صناعية أو طبية أو غيرها، ويسعى هذا النوع من التجسس إما إلى الاستفادة من هذه المعلومات أو إلى منع الاخرين من الاستفادة منها.[23]

الفرع الثاني: أنواع التجسس الالكتروني حسب الوسيلة المستعملة

تختلف انواع التجسس الالكتروني باختلاف الوسيلة الالكترونية التي تتم بها الجريمة فقد يتم التجسس بواسطة الشبكات السلكية واللاسلكية، او عن طريق شبكات الهاتف النقال، او عن طريق الأقمار الصناعية، او بواسطة البريد الالكتروني، او عن طريق تقنية البوليمرات، او بواسطة الطائرات المسيرة، او عن طريق تقنية البيوبوت.

أولا: التجسس بواسطة الشبكات السلكية واللاسلكية وشبكات الهاتف النقال

انتشرت أساليب التجسس الإلكتروني بشكل كبير في البيئات الشبكية، سواء كانت شبكات شركات صغيرة أو كبيرة، سلكية أو لاسلكية، ومن أشهر هذه الأساليب هو ما يعرف بـ "اصطياد حزم البيانات" Sniffing وأيضا البرامج مثل Ethereal وTc dump وWin dump التي تتيح للمتسللين اعتراض وتحليل حركة البيانات داخل الشبكة، مما يسمح لهم بسرقة كلمات المرور والمعلومات الحساسة، وبالتالي فإن أي مستخدم داخل شبكة محلية قد يقوم بالتجسس على الاخرين أو معرض لخطر التجسس من قبل الآخرين، وقد تمت تجربة بعض أنواع Sniffer وهو مختص في اصطياد كلمات المرور في احدى مقاهي الانترنت فكانت النتيجة الحصول على كلمات المرور السرية لإيميلات الأشخاص الذين سجلوا الدخول.[24]

يشكل التجسس عبر شبكات الهاتف النقال هو الاخر تهديدا خطيرا للخصوصية والأمن، فبفضل التقدم التكنولوجي بات من الممكن فك تشفير الرسائل النصية والمكالمات الهاتفية، مما يسمح للمتسللين بالاطلاع على محتواها أو حتى تعديلها او حذفها وقد أثبتت برامج تجسس متخصصة، مثل برنامج Crytopro GSM A5، إمكانية اختراق أنظمة التشفير في شبكات الجيل الثاني (GSM) وشبكات الأقمار الصناعية (ثريا)، مما يهدد ملايين المستخدمين حول العالم[25]

ثانيا: التجسس بواسطة الأقمار الصناعية

يعتبر هذا النوع من التجسس عالميا بامتياز، ويتطلب استخدام أجهزة وتقنيات متطورة للغاية لا يمكن لأفراد أو منظمات عادية الحصول عليها،[26]ويقتصر تنفيذ هذه العمليات على الدول المتقدمة التي تمتلك قدرات تقنية هائلة، بما في ذلك أقمار صناعية مزودة بأحدث الأجهزة والبرامج، وعلى الرغم من أن إطلاق هذه الأقمار يتم عادة لأسباب معلنة مثل الأبحاث العلمية أو المساعدات الإنسانية، إلا أن الغرض الحقيقي منها قد يكون التجسس، حيث تتحكم الدولة في البيانات التي تجمعها هذه الأقمار وتحدد استخدامها.

في سنة 2023 أطلق الجيش الإسرائيلي القمر الصناعي التجسسي "أفق 13" والذي يمثل قفزة نوعية في قدرات المراقبة الإسرائيلية حيث يتميز هذا القمر بنظام رادار متطور يتيح له التقاط صور عالية الدقة في جميع الظروف الجوية، وبغض النظر عن حالة الغطاء السحابي، وعلى خلاف الأقمار الصناعية السابقة التي تعتمد على الضوء، فإن "أفق 13" قادر على اختراق الغيوم والظلام، مما يجعله أداة استخباراتية أكثر فاعلية، تم تصميم هذا القمر لينفذ مهام مراقبة دقيقة فوق مناطق حساسة مثل سوريا وإيران، ويأتي إطلاق هذا القمر في إطار سعي إسرائيل المستمر لتعزيز قدراتها الاستخباراتية والعسكرية[27]

ثالثا: التجسس بواسطة البريد الالكتروني

أصبح البريد الإلكتروني أداة أساسية في التواصل والتبادل المعلوماتي خاصة في بيئة العمل، على الرغم من شيوعه، لا يزال العديد من المستخدمين يتجاهلون أهمية تأمين حساباتهم الإلكترونية.

حذر خبراء الأمن السيبراني من أن كشف عنوان بريدك الإلكتروني يعد بمثابة مفتاح يفتح بابا واسعا للمتسللين للوصول إلى معلوماتك الشخصية، فبمجرد حصولهم على عنوان بريدك، يبدأون في استخدام أساليب مختلفة مثل التصيد الاحتيالي لخداعك للحصول على كلمة المرور الخاصة بك، مما يتيح لهم السيطرة على حساباتك وبياناتك الحساسة يتم ذلك عن طريق إرسال رسائل بريد إلكتروني مزيفة تحاكي مواقع معروفة، بهدف إقناع المستخدمين بإدخال بيانات تسجيل الدخول الخاصة بهم على مواقع وهمية، وبمجرد حصول المتسلل على هذه البيانات، يصبح لديه صلاحية الوصول إلى جميع حسابات الضحية.[28]

رابعا: التجسس بواسطة البوليمرات وتقنية البيوبوت

هي عبارة عن أجهزة مصنوعة من مادة من نوع خاص من "البوليمرات"، ابتكرها باحثون في الجمعية الكيميائية الأمريكية، تم تطويرها بناء على طلب من وزارة الدفاع الأمريكية وهي قادرة على تدمير نفسها ذاتيا بعد إتمام مهمتها، يمكن استخدام هذه المادة لصنع أجهزة تجسس صغيرة الحجم ترسل إلى مناطق معادية لجمع المعلومات ثم تختفي دون أن تترك وراءها أي أثر، اذ ان هذه المادة لا تتحلل ببطء على مدار عام مثل المواد البلاستيكية بل تختفي في لحظات عندما تتلقى امر التدمير الذاتي أو عندما تتعرض للشمس.[29]

أما تقنية البيوبوت فهي تهدف إلى دمج الكائنات الحية مع التكنولوجيا لخلق كائنات حية هجينة قادرة على تنفيذ مهام محددة، ويتم ذلك عن طريق تعديل الكائنات الحية وراثيا أو آليا، مما يمنحها قدرات جديدة ووظائف متخصصة، ومن بين هذه الكائنات الصرصار الجاسوس حيث اختارت الباحثة في جامعة تكساس "هوانغ ليانغ" الصراصير اللاتينية لتكون أساسا لروبوتات تجسس، وذلك بفضل قدرتها على التحمل، ويمكن استخدام هذه الصراصير الآلية في مهام متنوعة مثل البحث عن الناجين تحت الأنقاض أو التجسس على الأماكن الخطرة، الا أن هذه التقنية تثير مخاوف أخلاقية حول إمكانية استخدامها في مراقبة المواطنين، وكذلك اليعسوب التجسسي الذي يستخدم كجاسوس بفضل بنيته الفريدة، فعضلات أجنحته القوية تتيح له التحكم الدقيق

في حركته أثناء الطيران، وباستخدام التحفيز الكهربائي، يمكن توجيهه لتنفيذ مهام استطلاعية دقيقة، مثل الطيران في اتجاهات محددة أو الهبوط في أماكن معينة.[30]

خامسا: التجسس بواسطة الطائرات المصغرة المسيرة

أعلن مسؤولون في وزارة الدفاع الأمريكية سنة 2017 عن نجاح أول اختبار لسرب ذكي من الطائرات المسيرة المصغرة والتي جرت التجربة عليها في كاليفورنيا وشملت 103 طائرات مسيرة مصغرة أطلق عليها اسم perdix أطلقت من 3 طائرات fantôme F/A-18، تعمل هذه الطائرات كسرب واحد تتواصل فيما بينها وتتخذ القرارات الجماعية مما يجعلها أداة قوية في جمع المعلومات الاستخباراتية، وتعد هذه التقنية الجديدة بمثابة قفزة نوعية في مجال الطائرات المسيرة، حيث تسمح بتنفيذ مهام استطلاعية معقدة بكفاءة عالية وبتكلفة أقل.[31]

المبحث الثاني: تحليل السياسة الموضوعية للمشرع الجزائري في التصدي لجريمة التجسس الالكتروني

لقد قامت اغلب الدول بسن القوانين والأنظمة الكفيلة بمكافحة التجسس الالكتروني والوقاية منه، حيث اختلفت الدول بين من احاطتها بنصوص خاصة، وبين من اعتبرها نوعا من الجرائم الماسة بأنظمة المعالجة الالية للمعطيات، ومن الدول التي اعتبرها كذلك نجد المشرع الجزائري الذي كيف التجسس الالكتروني على أنه جريمة معلوماتية، ولهذا سنتطرق ضمن هذا المبحث الى السياسة الموضوعية للمشرع الجزائري في التصدي لجريمة التجسس الالكتروني باعتبارها جريمة من جرائم المساس بأنظمة المعالجة الالية للمعطيات من خلال التعرف على صور المساس بأنظمة المعالجة الالية للمعطيات المنصوص عليها في قانون العقوبات حتى يتسنى لنا معرفة العناصر المادية المكونة لجريمة التجسس الالكتروني (المطلب الأول)، ومن ثم التطرق الى الجزاءات المقررة لهذه الجرائم حسب التعديل الأخير 24-06 (المطلب الثاني).

المطلب الأول: صور المساس بأنظمة المعالجة الالية للمعطيات

نص المشرع الجزائري على جريمة التجسس في قانون العقوبات الصادر بموجب الأمر 66-156، ضمن الفصل الأول من الباب الأول تحت عنوان "الجنايات والجنح ضد أمن الدولة" في المواد من 61 الى 64، وباستقراء نصوص هذه المواد نجد ان المشرع الجزائري قد بين الافعال المكونة للركن المادي لجريمة الخيانة والتجسس، كما قام المشرع الجزائري من خلال التعديل الأخير لقانون العقوبات رقم 24-06 بإدراج المادتين 63 مكرر و63 مكرر 1 التي تنص على معاقبة كل من يقوم بتسريب معلومات أو وثائق سرية تتعلق بالأمن الوطني والدفاع الوطني والاقتصاد الوطني، عبر وسائل التواصل الاجتماعي لصالح دولة أجنبية أو أحد عملائها أو قصد الاضرار بمصالح الدولة او باستقرار مؤسساتها، ومع ذلك لم يتطرق المشرع الى جريمة التجسس الالكتروني ضمن النصوص التقليدية لجريمة التجسس الا في نص م63 مكرر المذكورة أعلاه، ولم يتطرق اليها كجريمة مستقلة بذاتها على غرار باقي التشريعات العربية الأخرى، وهو الامر الذي يحيلنا حتما إلى المواد من 394 مكرر إلى 394 مكرر 8 من ق ع ج رقم 04-15، المعدلة بموجب القانون 06-23والقانون

16-02 ومن ثم القانون 24-06[32]، والتي تعد الإطار القانوني العام للجرائم المرتكبة ضد أنظمة المعالجة الآلية للمعطيات او ما يسمى بالجرائم المعلوماتية، وبما أن المشرع لم ينص على جريمة التجسس الإلكتروني بشكل مستقل، يتم تصنيفها ضمن نطاق الجرائم المعلوماتية التي تنظمها في هذه المواد ولتي سنتناولها بالتفصيل فيما يلي.

الفرع الأول: جريمة الدخول أو البقاء عن طريق الغش

تعد جريمة الدخول أو البقاء غير المشروع الى نظام المعالجة الالية للمعطيات، المرحلة الأولى للعديد من الجرائم الالكترونية، بما في ذلك جريمة التجسس الإلكتروني، حيث تعتبر هذه الأفعال بمثابة التمهيد لارتكاب جرائم أخرى أكثر خطورة.

أولا: الركن المادي للجريمة

باستقراء نص م 394 مكرر ق ع ج يتضح لنا أن الركن المادي للجريمة يتكون من عنصرين هما الدخول أو البقاء عن طريق الغش الى نظام المعالجة الالية للمعطيات.

الدخول في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يوجد فيه الحاسوب، بل يقصد به الدخول إلى النظام المعلوماتي نفسه باستخدام التقنيات الحديثة، هذا الدخول يمكن أن يتم بطرق متنوعة، مثل الاتصال المباشر بالنظام أو الاعتراض غير المشروع للاتصالات، ويكون الدخول غير مشروع عندما يتم دون إذن من صاحب النظام أو مخالفًا للشروط التي وضعها صاحب النظام أو من يملك السيطرة على هذا النظام.[33]

وقد استعمل المشرع الجزائري في الفقرة الأولى من م 394 مكرر من ق ع ج عبارة "كل من يدخل او يبقى عن طريق الغش ..." والتي كان يقصد بها الدخول إلى نظام معلوماتي دون توفر الحق القانوني لذلك، وعليه فإن الدخول إلى جهاز حكومي يكون مشروعا إذا كان هناك رضا صريح أو ضمني من طرف الجهة صاحبة السيطرة على النظام، ويفهم من الرضا الضمني، على سبيل المثال، إمكانية الوصول إلى أجهزة متصلة بنفس الشبكة الداخلية، حيث يفترض أن العاملين في هذه الشبكة لديهم الصلاحية للوصول إلى الأجهزة الأخرى المنتمية الى ذات الشبكة.[34]

أما البقاء غير المشروع يقصد به التواجد المستمر داخل نظام معلوماتي بعد الدخول إليه، سواء كان هذا الدخول مشروعا أم غير مشروع، ويتحقق البقاء غير المشروع عندما يتجاوز الفاعل المدة المسموحة له بالبقاء داخل النظام ويستمر في التواجد داخله، وبالتالي فإن البقاء غير المشروع قد يكون نتيجة مباشرة للدخول غير المشروع، أو قد يحدث بعد دخول مشروع ولكنه تجاوز الحدود المسموحة.[35]

يكفي لقيام جريمة الدخول او البقاء غير المشروع الى نظام معلوماتي، أن يتمكن الفاعل من الدخول الى النظام فقط حتى ولو لم يتمكن من الوصول الى المعلومات الموجودة داخل هذا النظام، ذلك لأن هذه الجريمة تعتبر من الجرائم الشكلية التي تكتمل بارتكاب الفعل المجرم بغض النظر عن النتائج التي ترتبت عليه.[36]

وعليه فان السلوك الاجرامي في جريمة التجسس الإلكتروني يتمثل في قيام الجاني بالدخول غير المشروع لأنظمة المعلومات الحكومية أو التنصت عليها بوسائل تقنية حديثة، وذلك بهدف الحصول على معلومات سرية خاصة بالدولة، سواء كانت عسكرية، أمنية، سياسية، اقتصادية، علمية، مالية أو غيرها، وحتى لو لم يتمكن الفاعل من الحصول على هذه المعلومات، فإن مجرد نية الدخول للحصول على هذه المعلومات تكفي لاعتبار الجريمة تامة.[37]

ثانيا: الركن المعنوي للجريمة

باستقراء نص م 394 مكرر ق ع ج يتضح لنا ان جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات هي جريمة عمدية يشترط لقيامها توافر القصد الجنائي العام فقط بعنصريه العلم والإرادة، يتجلى هذا القصد في علم الجاني بأن فعله موجه إلى نظام معلوماتي، وبأنه يدخل أو يبقى فيه بطريقة غير مشروعة، وبالتالي فإن الجهل بحقيقة النظام أو الدخول اليه عن طريق الخطأ أو الاعتقاد بوجود تصريح بالدخول او بأن الموقع متاح للجمهور انتفى القصد الجنائي، ومع ذلك، إذا استمر الجاني في البقاء في النظام بعد علمه بعدم مشروعية دخوله، فإن ذلك يدل على توافر القصد الجنائي ويعد مرتكبا للجريمة منذ اللحظة التي تحقق فيها العلم.[38]

لا يكفي لقيام القصد الجنائي توافر عنصر العلم لدى الجاني فقط، بل يجب أن يتوافر أيضا عنصر الإرادة الجنائية، هذه الإرادة تتجلى في القرار الواعي والمتعمد بارتكاب السلوك الاجرامي، وهو الدخول أو البقاء غير المشروع داخل نظام المعالجة الالية للمعطيات، وبما أن هذه الجريمة تعد من الجرائم الشكلية التي لا يتطلب لقيامها نتيجة معينة، فان الإرادة هنا تقتصر على ارتكاب السلوك الاجرامي ولا تمتد الى النتيجة الاجرامية أي إرادة الدخول أو البقاء داخل النظام المعلوماتي.[39]

الفرع الثاني: جريمة التلاعب بمعطيات الحاسب الالي

جرم المشرع الجزائري التلاعب العمدي بالمعطيات بموجب م 394 مكرر 01 من ق ع ج، عن طريق إدخال معلومات زائفة، أو حذف معلومات صحيحة، أو تعديل المعلومات القائمة بطريقة غير مشروعة، ولقيام هذه الجريمة يكفي أن يقوم الجاني بفعل واحد فقط من هذه الأفعال فقط، ولا يشترط اجتماعها جميعا.[40]

أولا: الركن المادي للجريمة

يتكون الركن المادي لجريمة التلاعب بمعطيات الحاسب الالي من مجموعة من الأفعال والتي سنتناولها فيما يلي:

أ- الإدخال

يقصد به أي تغيير أو إضافة يتم إجراؤه على المعطيات الموجودة في نظام المعلومات، سواء كان هذا النظام فارغا أم يحتوي على معطيات مسبقة، ويشمل ذلك إدخال بيانات خاطئة أو ضارة، أو إضافة برامج

ضارة تهدف إلى التجسس أو التخريب، ويعد هذا الفعل جريمة سواء كان مرتكبه شخصا ليس له حق الوصول إلى النظام أو شخصا مخولا بالوصول ولكنه استغل صلاحياته بشكل غير مشروع.[41]

ب- المحو أو الازالة

يتحقق عن طريق فقدان جزء أو كل المعطيات المخزنة على أي وسيلة تخزين مرتبطة بالنظام، سواء تم ذلك عن طريق حذف البيانات أو تدمير الوسيلة نفسها أو نقلها إلى مكان غير متاح[42] ، وتستخدم هذه العمليات عادة برامج خبيثة مثل فيروس الدودة وحصان طروادة.[43]

ج- التعديل

يتحقق عن طريق إدخال تغييرات غير مشروعة على المعطيات الموجودة داخل النظام المعلوماتي واستبدالها بمعطيات أخرى بهدف تغيير سلوك النظام أو الحصول على نتائج غير مرغوبة، يتم ذلك عادة باستخدام برمجيات خبيثة مثل الفيروسات والقنابل المعلوماتية التي تعمل على تعطيل النظام.[44]

ثانيا: الركن المعنوي للجريمة

من خلال استقراء م 394 مكرر 01 ق ع ج يتضح لنا أن جريمة التلاعب بمعطيات الحاسب الآلي هي جريمة من الجرائم العمدية التي يشترط فيها توافر القصد الجنائي العام بعنصريه العلم والإرادة حيث جاء في نص المادة السالفة الذكر "كل من أدخل او أزال أو عدل عن طريق الغش..."، والذي يتطلب من الجاني أن يكون على علم بأن فعله غير مشروع وأن هدفه هو التلاعب بالمعطيات دون حق عن طريق ادخال او تعديل او إزالة معطيات، وبالتالي إلحاق الضرر بصاحب الحق في هذه المعطيات، والى جانب عنصر العلم يجب أن تتجه ارادة الجاني الى ارتكاب السلوك المجرم بإحدى الصور السالفة الذكر حتى يكتمل الركن المعنوي للجريمة.[45]

الفرع الثالث: جريمة التعامل في معطيات غير مشروعة

تعتبر جريمة التعامل في معطيات غير مشروعة المنصوص عليها في المادة 394 مكرر02 من ق ع ج من أخطر الجرائم التي تستهدف أمن المعلومات، ويتخذ السلوك الاجرامي في هذه الجريمة صورتين رئيسيتين، الأولى هي التعامل في معطيات صالحة لارتكاب جريمة، والثانية هي التعامل بمعطيات متحصل عليها من جريمة، والهدف من تجريم هذه الأفعال هو منع وقوع الجرائم ومنع استغلال المعلومات المسروقة.[46]

أولا: الركن المادي للجريمة

يتكون الركن المادي لجريمة التعامل في معطيات غير مشروعة من صورتين رئيسيتين سنتناولهما بالشرح فيما يلي:

أ- جريمة التعامل في معطيات صالحة لارتكاب جريمة

نصت الفقرة الأولى من م 394 مكرر 2 من ق ع ج على جريمة التعامل في معطيات صالحة لارتكاب جريمة من خلال تجريم مجموعة من الأفعال التي جاءت على سبيل الحصر والمتمثلة في التصميم، البحث،

التجميع، التوفير، النشر، الاتجار بمعلومات أو بيانات يمكن استخدامها في ارتكاب جريمة من جرائم المساس بأنظمة المعالجة الالية للمعطيات، ولقيام الجريمة يكفي أن يقوم الفاعل بأحد هذه الأفعال ولا يشترط توافرها جميعا، وفيما يلي سنقوم بشرح كل فعل على حدة:[47]

التصميم: يقصد به أي عمل مسبق يهدف إلى تهيئة الظروف لارتكاب جريمة من جرائم المساس بأنظمة المعالجة الالية للمعطيات من خلال إنشاء أو تطوير أدوات أو برامج أو تقنيات جديدة لاستخدامها في تنفيذ الجريمة، وعادة ما يقوم بتصميم هذه الأدوات أشخاص ذوي خبرة تقنية، مثل المبرمجين والمهندسين المتخصصين في الأمن السيبراني الذين يستخدمون مهاراتهم بطريقة غير مشروعة، ويشمل ذلك على سبيل المثال تصميم الفيروسات والبرامج الضارة وبرامج الاختراق والتجسس،

البحث: لا يقصد به مجرد البحث عن هذه المعطيات، بل يتعدى ذلك الى البحث في الطرق والأساليب المستخدمة في إنشاء المعطيات وتجهيزها للاستخدام كالبحث في طرق تصميم برنامج تجسس،

التجميع: نعني به جمع البيانات والمعلومات المختلفة التي يمكن استخدامها بشكل غير مشروع للدخول الى أنظمة المعلومات أو التلاعب بها،

التوفير: هو تقديم أو تسهيل حصول شخص آخر على معطيات يمكن استخدامها بشكل غير مشروع للدخول الى أنظمة المعالجة الالية للمعطيات أو التلاعب بها مما يؤدي الى اتساع دائرة الخطورة،

النشر: يقصد به جعل المعلومات المتعلقة بالجريمة متاحة للآخرين عبر أي وسيلة من وسائل النشر، هذا الفعل يعتبر من أخطر الأفعال لأنه يوسع نطاق انتشار هذه المعلومات، مما يزيد من احتمال استخدامها لأغراض إجرامية،

الاتجار: يقصد به بيع وشراء أو تبادل المعطيات الصالحة لارتكاب جريمة، وهو يختلف عن التوفير الذي قد يكون دون مقابل،

ب-التعامل في معطيات متحصل عليها من ارتكاب جريمة

تقع هذه الجريمة بارتكاب أحد الأفعال المذكورة في الفقرة الثانية من المادة 394 مكرر 2 من ق ع ج، المتمثلة في حيازة، إفشاء، نشر، أو استعمال أي معطيات تم الحصول عليها بشكل غير قانوني من خلال ارتكاب أحد الجرائم الماسة بأنظمة المعالجة الالية للمعطيات وسنقوم فيما يلي بعرض لكل واحد من هذه الأفعال على حدة:[48]

الحيازة: تعني الحيازة في هذه الجريمة السيطرة الفعلية على معطيات تم الحصول عليها بطرق غير مشروعة من خلال الاعتداء على أنظمة المعالجة الالية للمعطيات كحيازة المعطيات المتحصل عليها من عملية التجسس، هذه السيطرة تمنح الحائز حق التصرف في هذه المعطيات، سواء بتعديلها، أو نقلها، أو حتى تدميرها، وبالتالي فإن مجرد حيازة هذه المعطيات يعتبر جريمة بحد ذاتها،

الافشاء: يقصد به نقل المعطيات من حيازة الشخص الذي تحصل عليها بطريقة غير مشروعة عن طريق التجسس مثلا إلى حيازة شخص آخر، ولا يشترط أن يكون الشخص الذي يقوم بالإفشاء ملزم قانونا بكتمان هذه المعطيات، إذ قد يكون هو نفسه قد حصل عليها بطريقة غير مشروعة،

النشر: يشمل مفهوم النشر كما سبق ذكره، أي فعل يهدف إلى نشر المعطيات الصالحة لارتكاب جريمة، سواء كان هذا النشر مجانيا أو بمقابل، كما أن م 394 مكرر02 ق ع ج لم تحدد وسيلة معينة للنشر، وبالتالي فان النشر يشمل جميع الوسائل سواء كانت تقليدية كالكتابة مثلا او حديثة مثل شبكة الانترنت أو الأقراص المضغوطة،

الاستعمال: يشمل الاستعمال في هذه الجريمة أي استخدام أو استعمال للمعطيات التي تم الحصول عليها بطريقة غير مشروعة، بغض النظر عن الغرض من هذا الاستعمال أو طبيعته، ولا يهم عدد مرات الاستعمال حتى لو تم الاستعمال لمرة واحدة فقط، كأن تستعمل شركة معلومات سرية تم التحصل عليها من خلال التجسس على شركة منافسة لها.

ثانيا: الركن المعنوي للجريمة

جريمة التعامل في معطيات غير مشروعة من الجرائم العمدية التي يشترط فيها القصد الجنائي العام بعنصريه العلم والإرادة وهو ما يستشف من نص م 394 مكرر 02 ق ع ج ، فلابد ان يكون الجاني على علم انه يتعامل في معطيات غير مشروعة او معطيات متحصل عليها من احدى جرائم الاعتداء على نظام المعالجة الالية للمعطيات، واذا انتفى العلم بأحد العناصر السابقة انتفى القصد الجنائي، ولا يكفي أن يكون الجاني عالما بالعناصر المكونة للجريمة، بل يجب ان تتجه ارادته الى إتيان السلوك المجرم ممثلا في الأفعال السالفة الذكر.

لا يكفي لقيام الصورة الأولى من الجريمة المتمثلة في التعامل في معطيات صالحة لارتكاب جريمة ان يتوافر لدى الجاني القصد الجنائي العام فقط، بل يشترط كذلك توافر القصد الجنائي الخاص لدى الجاني أي اتجاه العلم والارادة الى وقائع معينة لا تدخل في تكوين اركان الجريمة، ولا بد ان يكون بقصد الاعداد او التمهيد لاستعمال هذه المعطيات في ارتكاب جريمة كجريمة التجسس الالكتروني، اما الصورة الثانية للجريمة المتمثلة في التعامل في معطيات متحصل عليها من ارتكاب جريمة فيكفي لقيامها توافر القصد الجنائي العام فقط.[49] على سبيل المثال في جريمة التجسس الإلكتروني، إذا قام شخص بجمع معلومات عن نظام حماية معين لشركة ما بهدف اختراقه، فإنه يكون قد ارتكب الصورة الأولى للجريمة اي جريمة التعامل في معطيات صالحة لارتكاب جريمة، حيث يتوافر لديه القصد الجنائي الخاص، أما إذا قام شخص آخر بشراء قاعدة بيانات تحتوي على معلومات شخصية دون معرفة كيفية استخدامها، ولكنه يعلم أنها يمكن استخدامها في ارتكاب جرائم، فإنه يكون قد ارتكب الصورة الثانية للجريمة أي التعامل في معطيات متحصل عليها من ارتكاب جريمة حيث يكفي وجود القصد الجنائي العام بعنصريه فقط.

المطلب الثاني: الجزاءات المقررة للجرائم الواقعة على أنظمة المعالجة الالية للمعطيات

تهدف العقوبة الجنائية الى ردع الجاني عن تكرار الجريمة من جهة ومن جهة أخرى ردع الآخرين عن ارتكاب جرائم مشابهة، وفي سياق الجرائم الماسة بأنظمة المعالجة الالية للمعطيات عامة وجريمة التجسس الالكتروني خاصة، تلعب العقوبة دورا حاسما في حماية المجتمع من الأضرار الاقتصادية والأمنية التي تترتب على هذه الجرائم، ولذلك تم توسيع نطاق المسؤولية الجنائية لتشمل بذلك كل من يشارك في ارتكاب هذه الجرائم سواء كان شخصا طبيعيا أو شخصا معنويا، وفي سبيل تعزيز الحماية القانونية من الجرائم الماسة بأنظمة المعالجة الالية للمعطيات قام المشرع الجزائري بتعديل بعض نصوص القسم السابع مكرر بموجب القانون رقم 24-06 المؤرخ في 28 أفريل 2024، وقد تضمنت هذه التعديلات تشديد عقوبة الحبس على اغلب الجرائم المنصوص عليها في هذا القسم وتشديد عقوبة الغرامة في بعض الجرائم، وسنتناول ذلك بالشرح فيما يلي.

الفرع الأول: العقوبات المقررة للشخص الطبيعي

تنقسم العقوبات المقررة للشخص الطبيعي الى عقوبات أصلية وأخرى تكميلية

أولا: العقوبات الأصلية

تشمل العقوبات البسيطة والعقوبات المشددة

1- العقوبات البسيطة

باستقراء نصوص المواد من 394 مكرر الى 394 مكرر02 من ق ع ج 24-06 نجد ان المشرع الجزائري قد نص على:

- معاقبة كل من قام بالدخول او البقاء عن طريق الغش في كل او جزء من منظومة للمعالجة الالية للمعطيات او يحاول ذلك بالحبس من ستة أشهر الى سنتين وبغرامة تصل الى 200.000 دج، والملاحظ هنا ان المشرع الجزائري بموجب التعديل الأخير قام برفع الحد الأدنى والاقصى للعقوبة كما قام برفع الحد الأدنى والاقصى للغرامة.
- معاقبة كل من يقوم بإدخال معطيات في نظام المعالجة الالية أو يزيل او يعدل بطريق الغش المعطيات التي يتضمنها بالحبس من سنة الى ثلاث سنوات وغرامة تصل الى 2.000.000 دج، ومنه نجد أن المشرع الجزائري بموجب التعديل الأخير قام برفع الحد الأدنى للعقوبة مع الإبقاء على الحد الأقصى للعقوبة مع الإبقاء على نفس مقدار الغرامة.
- معاقبة كل من يرتكب جريمة التعامل في معطيات غير مشروعة بصورتيها بالحبس من سنة الى خمس سنوات وبغرامة تصل الى 5.000.000 دج، وعليه نجد ان المشرع الجزائري بموجب التعديل الأخير قام برفع الحد الأدنى والاقصى للعقوبة مع الإبقاء على نفس مقدار الغرامة.

2- ظروف تشديد العقوبة

باستقراء نصوص المادتين 394 مكرر و394 مكرر03 من ق ع ج 24-06، نلاحظ ان المشرع الجزائري نص على حالات تشدد فيها العقوبة على الجرائم المنصوص عليها في القسم السابع مكرر على النحو التالي:

- إذا ترتب على الدخول او البقاء حذف او تغيير لمعطيات المنظومة فتصبح العقوبة ضعف تلك المنصوص عليها في جريمة الدخول او البقاء غير المشروع في صورتها البسيطة، فتصبح العقوبة الحبس من سنة الى أربع سنوات وغرامة تصل الى 400.000 دج.
- اما إذا ترتب على الدخول او البقاء تخريب نظام اشتغال المنظومة تضاعف العقوبة الى الحبس من سنة الى ثلاث سنوات وغرامة تصل الى 300.000 دج، حيث قام المشرع بالرفع من الحد الأدنى والاقصى للعقوبة والغرامة.
- أما إذا استهدفت هذه الجرائم الدفاع الوطني او الهيئات والمؤسسات الخاضعة للقانون العام تكون العقوبة الحبس من سنتين الى عشر سنوات وبغرامة تصل الى 2.000.000 دج دون الاخلال بتطبيق العقوبات الأشد، قبل تعديل قانون العقوبات 24-06 لم ينص المشرع على مدة العقوبة ومقدار الغرامة وانما نص على مضاعفة العقوبات فقط دون الاخلال بتطبيق العقوبات الأشد.

ثانيا: العقوبات التكميلية

إضافة الى العقوبات الاصلية المذكورة أعلاه، نص المشرع الجزائري على عقوبات تكميلية وجوبية في نص م 394 مكرر06 ق ع ج من القانون 04-15، والمتمثلة في المصادرة والغلق، كل الأجهزة والبرامج والوسائل المستخدمة في الجريمة مع اغلاق المواقع التي تكون محلا للجريمة، علاوة على اغلاق المحل او مكان الاستغلال إذا كانت الجريمة قد اركبت بعلم مالكها دون الاخلال بحقوق الغير حسن النية.

الفرع الثاني: العقوبات المقررة للشخص المعنوي

تشمل العقوبات المقررة للشخص الطبيعي العقوبات الاصلية وأخرى تكميلية

أولا: العقوبات الاصلية

يعاقب الشخص المعنوي الذي يرتكب جريمة من جرائم المساس بأنظمة المعالجة الالية للمعطيات بغرامة تعادل 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وذلك بموجب م 394 مكرر 04 ق ع ج من القانون 04-15، باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام التي لا تخضع للمساءلة الجزائية.

ثانيا: العقوبات التكميلية

تطبق على الشخص المعنوي نفس العقوبات التكميلية الوجوبية المنصوص عليها في م 394 مكرر06 ق ع ج والمتمثلة في المصادرة والغلق التي سبق لنا شرحها.

الفرع الثالث: الجزاء المقرر للاتفاق الجنائي والشروع

نصت م 394 مكرر 5 ق ع ج على معاقبة كل من يشارك في مجموعة او اتفاق بغرض التحضير للجرائم الماسة بأنظمة المعالجة الالية للمعطيات بنفس العقوبة المقررة للجريمة التي تم التحضير لها وذلك بشروط تتمثل في:

- يشترط المشاركة في مجموعة أو اتفاق
- أن يكون الغرض من المجموعة هو الاعداد لارتكاب جريمة من الجرائم المنصوص عليها في القسم السابع مكرر
- أن يجسد التحضير بفعل أو عدة أفعال مادية
- توفر القصد الجنائي بعنصريه لدى افراد المجموعة أي العلم بالعضوية في المجموعة واتجاه الإرادة للقيام بالأعمال التحضيرية

أما م 394 مكرر 07 ق ع ج فقد نصت على عقوبة الشروع في جريمة من جرائم المساس بأنظمة المعالجة الالية للمعطيات حيث تكون العقوبة المقررة للشروع في الجريمة هي نفسها العقوبة المقررة للجريمة ذاتها.

الخاتمة:

وفي ختام بحثنا يمكننا القول أن التطور التكنولوجي المتسارع وإن كان يحمل معه العديد من الفوائد، إلا أنه فتح الباب أمام تهديدات جديدة أبرزها الجرائم الإلكترونية، وتحديدا جريمة التجسس الإلكتروني، هذا النوع من الجرائم يستغل الثغرات الأمنية للحصول على المعلومات الحساسة وتعطيل الخدمات الحيوية، مما يشكل تهديدا مباشرا للأمن القومي والاقتصادي للدول والمؤسسات والأفراد على حد سواء.

وعليه يمكن استخلاص النتائج التالية:

- مع التطور المتسارع للأنظمة الرقمية والوسائل الإلكترونية، أصبح مفهوم التجسس أكثر تعقيدا وتشعبا، وغياب تعريف موحد للتجسس التقليدي يزيد من صعوبة تحديد ماهية التجسس الإلكتروني وحدوده، خاصة في ظل التغيرات المستمرة في البيئة الرقمية.
- تتنوع جرائم التجسس الإلكتروني تنوعا كبيرا، حيث تختلف باختلاف الأهداف التي تسعى إليها، والوسائل التقنية المتاحة لارتكابها.
- لم ينص المشرع الجزائري على جريمة التجسس الالكتروني بشكل مستقل، وانما اعتبرها كجريمة من جرائم المساس بأنظمة المعالجة الالية للمعطيات تسري عليها نفس الاحكام الموضوعية والاجرائية التي تسري على هذه الجرائم.

- في محاولة لمواجهة الجرائم الإلكترونية، ومن بينها التجسس الإلكتروني، قام المشرع الجزائري بحماية المعطيات التي تحتويها أنظمة المعالجة الالية عن طريق تجريم أي تلاعب أو عبث بها، وامتدت هذه الحماية لتشمل بذلك جميع أنواع المعطيات بغض النظر عن حالتها مخزنة أو مرسلة أو معالجة.
- في سياق التطور المتسارع للتكنولوجيا وتزايد التهديدات التي تواجه الأمن السيبراني، عمل المشرع الجزائري على تطوير الإطار القانوني لحماية المعطيات الرقمية سعيا لتعزيز الحماية القانونية للأنظمة المعلوماتية، وقد تم ذلك من خلال تعديل القسم السابع مكرر بموجب القانون رقم 24-06، حيث قام المشرع الجزائري من خلال هذا التعديل بتشديد العقوبات المقررة على جرائم المساس بهذه الأنظمة.
- شدد المشرع الجزائري العقوبة على الجرائم الماسة بأنظمة المعالجة الالية للمعطيات اذا استهدفت هذه الجرائم الدفاع الوطني او الهيئات والمؤسسات الخاضعة للقانون العام، يأتي هذا التشديد نظرا لخطورة هذه الجرائم باعتبارها تهديدا مباشرا لأمن الدولة واستقرارها، حيث يمكن أن تؤدي إلى تسريب معلومات حساسة أو تعطيل البنية التحتية الحيوية، وبالتالي فإن جريمة التجسس الإلكتروني التي تستهدف عادة أنظمة المعالجة الالية للمعطيات الحكومية تخضع لهذه العقوبات المشددة.
- تعد جريمة التجسس الالكتروني من الجرائم العمدية التي تقوم بالقصد الجنائي العام بعنصريه العلم والارادة، فيجب ان يعلم الجاني بأن حصوله على تلك المعلومات او البيانات قد تم بوجه غير مشروع وضد إرادة ورغبة صاحب السيطرة عليها مع اتجاه اراداته الى إتيان السلوك المجرم وبمخالفة إرادة صاحب المعلومات والبيانات.

على ضوء النتائج السابقة خلصت الدراسة الى جملة التوصيات التالية:

- ان وضع تعريف شامل ودقيق للتجسس الإلكتروني يمثل تحديا كبيرا في ظل التطور المتسارع للتكنولوجيا، ومع ذلك فإن هذا التعريف ضروري لضمان تطبيق القانون بشكل عادل وفعال، مع ضرورة أن يغطي هذا التعريف جميع أشكاله وصور للتجسس الإلكتروني، دون ذكر وسائل ارتكاب الجريمة، وذلك لضمان شموله لكافة الأشكال المستقبلية لهذه الجرائم.
- ندعو إلى التعاون الدولي لإبرام اتفاقية دولية لمكافحة التجسس، تهدف إلى توحيد الجهود الدولية في مكافحة هذه الجريمة، وتبادل المعلومات والخبرات بين الدول الأعضاء.
- ندعو المشرع الجزائري لتحديث نصوصه التشريعية المتعلقة بالجرائم المعلوماتية وذلك لمواكبة تطور قطاع تكنولوجيا الاعلام والاتصال، مع النص على جريمة التجسس الالكتروني بشكل مستقل.

الهوامش:

[1] ابن منظور، معجم لسان العرب، المجلد 3، دار صادر، بيروت، ص 147

[2] ضرغام جابر عطوش ال مواش، جريمة التجسس المعلوماتي دراسة مقارنة، مكتبة دار السلام القانونية، 2017، العراق، ص 87

[3] Espionage , oxford learners dictionaries, www.oxfordlearnersdictionaries.com

[4] Espionage, merriam-webster, www.merriam-webster.com

[5] فتيحة خالدي، تأثير التجسس الالكتروني على الحق في الخصوصية المعلوماتية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 07، العدد 01، الجزائر، 2021، ص 30

[6] علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة دراسو مقارنة، منشورات زين الحقوقية، الطبعة الأولى، 2013، ص 567 568

[7] فتيحة خالدي، المرجع السابق، ص 305.

[8] علي عبود جعفر، المرجع السابق، ص 567 568

[9] سامية بوشوشة، التجسس الالكتروني وطرق مكافحته، مجلة العلوم الاجتماعية والإنسانية، المجلد 16، العدد 01، الجزائر، 2023، ص52

[10] علي عبود جعفر، المرجع السابق، ص 569

[11] سامية بوشوشة، المرجع السابق، ص 53

[12] محمد الشوابكة، جرائم الحاسوب والانترنت: الجريمة المعلوماتية، دار الثقافة، عمان، 2009، ص 29.

[13] المعتصم منجي محمود القطيشات، جريمة الإرهاب باستخدام الوسائل الالكترونية، رسالة ماجستير في القانون العام، جامعة الاسراء، الأردن، 2022، ص41.

[14] اوشن حنان، التجسس الالكتروني واليات مكافحته في التشريع الجنائي الجزائري، مجلة الحقوق والعلوم السياسية، المجلد 1، العدد 2، 2014، ص 132.

[15] فتيحة خالدي، المرجع السابق، ص 306.

[16] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، 2010، ص 211.

[17] نادر عبد العزيز شافي، جرائم التجسس، تاريخ الاطلاع: 2024/08/17، على الساعة 17:40 https://www.lebarmy.gov.lb

[18] نهلا عبد القادر مومني، المرجع السابق، ص 212

[19] Andrew jones , Industrial espionage in a hi-tech world, Computer Fraud & Security , Volume 2008,Issue 01, 2008, page 08.

[20] نهلا عبد القادر مومني، المرجع السابق، ص 215.

[21] علي عبود جعفر، المرجع السابق، ص 571

[22] نهلا عبد القادر مومني، المرجع السابق، ص 216.

[23] نادر عبد العزيز شافي، جرائم التجسس، تاريخ الاطلاع: 2024/08/17، على الساعة 17:40 https://www.lebarmy.gov.lb

[24] اوشن حنان، التجسس بين الإباحية والتجريم، دار اليازوري العلمية، عمان، 2022، 177 178

[25] حسنين شفيق، الاعلام الجديد والجرائم الالكترونية، دار فكر وفن للطباعة والنشر والتوزيع، 2015، ص171

[26] اوشن حنان، المرجع السابق، ص179

[27] محمد وتد، "أفق 13" أحدث أقمار التجسس الإسرائيلية.. تعرف عليه، تاريخ الاطلاع 2024/08/09، على الساعة 20:45،
https://www.aljazeera.net/

[28] احذر هذه الخدع القراصنة لا يحتاجون أكثر من بريدك الإلكتروني لإيذائك، تاريخ الاطلاع 2024/08/17، على الساعة 18:05
https://www.aljazeera.net/

[29] شاهد أجهزة تجسس أمريكية من نوع غريب تاريخ الاطلاع 2024/08/05 على الساعة 19:36
https://arabic.rt.com/world//

[30] طه الراوي، كيف غيرت التكنولوجيا أساليب التجسس، تاريخ الاطلاع 2024/08/07 على الساعة 19:42
https://www.noonpost.com/36070/

[31] االبنتاغون يطور طائرات بدون طيار على شكل أسراب، تاريخ الاطلاع: 2024/08/07، على الساعة 18:30
https://arabi21.com/story/977208/

[32] القانون رقم 24-06، المؤرخ في 28 أفريل 2024، المعدل والمتمم للأمر 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات الجزائري، ج ر، العدد 30، المؤرخ في 30 أفريل 2024.

[33] بن مكي نجاة، السياسة الجنائية لمكافحة الجرائم المعلوماتية، دار الخلدونية، الجزائر، 2017، ص 179 180

[34] علي عبود جعفر، المرجع السابق، ص 581.

[35] عبد الفتاح بيومي الحجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي)، دار الكتب القانونية، مصر، 2007، ص 360 361.

[36] بن مكي نجاة، المرجع السابق، ص 180 184.

[37] علي عبود جعفر، المرجع السابق، ص580.

[38] بن مكي نجاة، المرجع السابق، ص 182 185

[39] بن مكي نجاة، المرجع السابق، ص 183

[40] بن مكي نجاة، المرجع السابق، ص 187 188

[41] جدي نسيمة، جرائم المساس بأنظمة المعالجة الالية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2013-2014، ص 64.

[42] امال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، 2007، الجزائر، ص 122

[43] عبد الفتاح بيومي الحجازي، المرجع السابق، ص 387

[44] عبد الفتاح بيومي الحجازي، المرجع نفسه.

[45] جدي نسيمة، المرجع السابق، ص 68 69

[46] رابحي عزيزة، الاسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة دكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2017–2018، ص 170.

[47] بن مكي نجاة، المرجع السابق، ص 194 195

[48] بن مكي نجاة ، المرجع السابق، ص 198 199

[49] بن مكي نجاة، المرجع السابق، ص 201 202.