الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of algeria
وزارة التعليم العالي والبحث العلمي
Ministray of higher education and scientific research
جامعة محمد البشير الإبراهيمي- برج بوعريريج-
University of mohammed Al-bachir Al –Ibrahimi-BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

**مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق**

**تخصص: قانون الاعلام الآلي**

**الموسومة بـ :**

# التجسس السيبراني الماس بامن الدولة في التشريع الجزائري

**إعداد الطالب :** **إشراف الدكتورة:**

- **مقرح عبد الرؤوف** **خرباش جميلة**

**نوقشت وأجيزت يوم: 20-06-2024**

**لجنة المناقشة**

| (اللقب والاسم) | (الرتبة) | (الصفة) |
|---|---|---|
| • مهناوي سارة | أستاذ مساعد قسم –ب– | رئيسا |
| • خرباش جميلة | أستاذ مساعد قسم –أ– | مشرفا |
| • دريسي عبد الله | أستاذ مساعد قسم –ب– | ممتحنا |

**السنة الجامعية : 2024/2023**

الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of higher education and scientific research
جامعة محمد البشير الإبراهيمي – برج بوعريريج
University Of Mohamed Al-Bashir Al-Ibrahimi - BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

# إذن بالإيـــداع

أنا الممضي أسفله الأستاذ : حسباين جميلة

الرتبة : أستاذة مساعدة أ

المشرف على مذكرة الماستر الموسومة بـ : التجسس السيبراني المباس بأمن الدولة في التشريع الجزائري

من إعـــداد :

الطالب الأول : مفرح عبد الرؤوف

الطالب الثاني : /

**أوافق على إيداع الطالب (الطالبين) لمذكرة التخرج لدى الإدارة من أجل برمجتها للمناقشة.**

إمضاء الأستاذ المشرف

ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

## نموذج التصريح الشرفي
## الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

**(الطالب الأول)**

أنا الممضي أسفله،

السيد(ة): مشرح ع الرؤوف ..... الصفة: طالب، أستاذ، باحث ..... طالب .....

الحامل(ة) لبطاقة التعريف الوطنية رقم 400402394 والصادرة بتاريخ 19.01.2022 .....

المسجل(ة) بكلية / معهد الحقوق ..... قسم العلوم السياسية .....

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

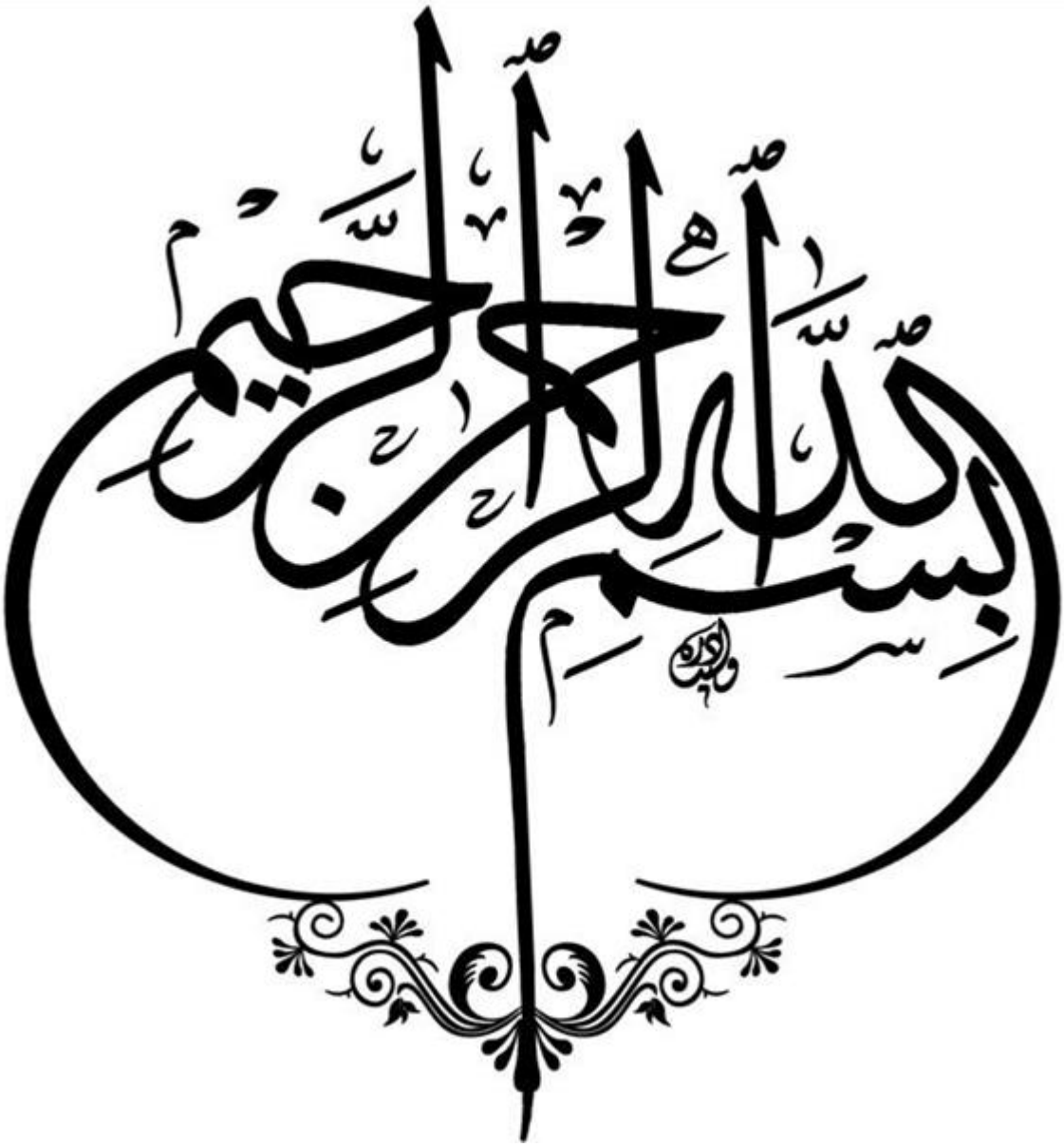
عنوانها: الجهد الجزائي للمسيرين في ظل الدولة في التشريع الجزائري .....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: ....09.06.2024....

توقيع المعني (ة)

لدى مجلس المعني للتنكير وبتفويض منه
ضابط الحالة المدنية
حروز زهير


بسم الله الرحمن الرحيم

# مقدمة

ان استخدام الانترنت يعد من اهم مظاهر عصرنا الراهن حيث صاحب زيادة الأفراد المستخدمين لها جرائم الكترونية لم تكن موجودة ولم يعرفها العالم لولا الانفجار الكبير للتكنولوجيا المعلومات و الاتصال اذ ان الجرائم الماسة بأمن الدولة تعد اخطر واشد الجرائم التي تهدد كيان الدولة وسلامتها فهذه الفئة من الجرائم تعتبر جريمة دولة على يد فرد او مجموعة من الافراد فمن بين هذه الجرائم جريمة التجسس التي هي احدى الجرائم التي تصدى لها المشرع الجزائري في قانون العقوبات بكل شدة لكن بقر هذا النوع من الجرائم يتصنف بالخطورة والتطور المستمر جراء استخدام أساليب جديدة يصعب كشفها خاصة مع التكور الهائل للتكنولوجيا في شتى المجالات فهي تشكل اغشداءا مباشرا ومؤثرا على سياسة الدولة ذلك بتهديد استقلالها وسلامة اراصيتها وتنقاص من سيادتها وتهدد نطاقها الحيوي الخارجي بالاعتماد على الجواسيس لعيون والأرصاد واستخدام الاجهزة المتقدمة تكنولوجيا سواء كانت سرية او علنية لذا منحها المشرع الاسبقية و الأولوية نظرا كخطورتها وأهمية المصالح التي تحميها .

تكتسي هذا الموضوع ي أهمية كبيرة لكونه من الموضوعات الحديثة والمنتشرة على نطاق واسع في التشريعات الأجنبية والعربية، بما في ذلك التشريع الجزائري، حيث يعكس الاهتمام المتزايد بهذا المجال وضرورة مواكبة التطورات الحاصلة فيه.

تعددت الأسباب التي دفعتنا لاختيار هذا الموضوع، فمن الناحية الذاتية، يعود ذلك إلى الميول الشخصي والشغف بدراسة المواضيع الحديثة والمتعلقة بالجرائم الرقمية والمجال السيبراني، حيث دفعنا هذا الاهتمام إلى اختيار هذا الموضوع من قائمة المواضيع المقترحة من قبل الأستاذ المشرف.

أما من الناحية الموضوعية، فنظرًا لتنوع أنواع الجرائم وظهور الجرائم السيبرانية كفئة جديدة، رأينا ضرورة دراسة هذا الموضوع بشكل معمق لتمييز الجرائم السيبرانية عن غيرها

من الجرائم التقليدية، وكشف الغموض الذي يكتنف هذا النوع الجديد من الإجرام والذي يختلف في طبيعته وخصائصه عن الجرائم التقليدية.

تسعى هذه الدراسة إلى تحقيق الأهداف التالية:

- الإلمام بمفهوم جريمة التجسس سيبرانية الماسة بأمن الدولة وتحديد دلالاتها ومضامينها بشكل دقيق.
- استكشاف طبيعة بمفهوم جريمة التجسس السيبيراني الماسة بأمن الدولة وخصائصها المميزة التي تفرقها عن الجرائم التقليدية.
- التعرف على الآليات والاستراتيجيات المختلفة لمكافحة الجرائم السيب راني الماسة بأمن الدولة والحد من انتشارها.
- تسليط الضوء على الإطار التشريعي والقانوني المتعلق بالجرائم السيبرانية الماسة بأمن الدولة وكيفية التصدي لها بفعالية.

بناءا على ما سبق فإن الإشكالية الرئيسية لهذه الدراسة هي:

**كيف نظم المشرع الجزائري آليات مكافحة جريمة التجسس السيبراني؟**

وبناءً على ما تقدم و للإجابة عن الإشكالية المطروحة وللإحاطة بمضامين الموضوع اعتمدنا على المنهج الوصفي بغرض وصف الجريمة السيبرانية من خلال تعريفها وتبيان خصائصها وصورها وكذا التعرف على مرتكبها، كما اعتمدنا على المنهج التحليلي بغرض تحليل النصوص القانونية ودراسة آليات وأساليب التحري عن الجريمة السيبراينة.

قسمنا الموضوع إلى فصلين، خصصنا الفصل الأول لدراسة ماهية الجريمة السيبرانية، أما الفصل الثاني فقد خصص إلى دراسة آليات مكافحة التصدي للجريمة السيبرانية في التشريع الجزائري.

# الفصل الأول:

# ماهية التجسس السيبيراني الماس بأمن الدولة

في العصر الرقمي الحديث، أضحى الفضاء السيبراني جزءًا لا يتجزأ من حياتنا اليومية، سواء في المجالات الشخصية أو المهنية أو الحكومية. هذا الفضاء الجديد جاء بمزايا عديدة مثل السرعة والراحة في تبادل المعلومات، ولكنه في الوقت نفسه أوجد نوعًا جديدًا من التهديدات والمخاطر. من بين هذه المخاطر تبرز الجريمة السيبرانية بأشكالها المتعددة، التي لا تؤثر فقط على الأفراد والشركات، بل تمتد تأثيراتها لتشمل أمن الدولة واستقرارها.

إن التحولات السريعة في تكنولوجيا المعلومات والاتصالات قد أدت إلى ظهور مفاهيم وأساليب جديدة في ارتكاب الجرائم. من بين هذه الجرائم، يبرز التجسس السيبراني كواحد من أخطر التهديدات التي تواجه الدول في العصر الحالي، فالتجسس السيبراني لا يقتصر على جمع المعلومات بطرق تقليدية، بل يتعدى ذلك إلى اختراق الأنظمة الإلكترونية والاستيلاء على بيانات حساسة قد تهدد الأمن القومي.

سنسلط الضوء في هذا الفصل على ماهية التجسس السيبراني الماس بأمن الدولة، من خلال عرض الإطار المفاهيمي للجريمة السيبرانية والطبيعة القانونية لها، وكذلك التطرق إلى مفهوم التجسس عبر الإنترنت ووسائله المختلفة. سوف نتناول هذه المواضيع بشكل منهجي ومنظم، لنقدم رؤية شاملة وعميقة حول هذا الموضوع الحيوي والهام.

# المبحث الأول: الإطار المفاهيمي للجريمة السيبرانية

بلا شك، تُعد الجرائم الإلكترونية من أبرز التحديات السلبية التي تواجه مختلف جوانب الحياة في العصر الحديث، هذه الجرائم، التي تحولت إلى مصدر قلق كبير لدول العالم، شهدت ارتفاعاً ملحوظاً في معدلات انتشارها وتطور أشكالها وتزايد أعدادها، بالإضافة إلى تنوع الطرق المستخدمة في ارتكابها لذا، من الضروري فهم هذه الظاهرة الإجرامية بعمق لكي نتمكن من تطوير حلول فعالة للحد منها.

لهذا الغرض، قمنا بتقسيم هذا القسم إلى فقرتين، حيث أول فقرة مخصصة لفهم مفهوم الجريمة الإلكترونية، بينما الفقرة الثانية تركز على أشكال الجريمة الإلكترونية.

## المطلب الأول: مفهوم الجريمة السيبرانية

مع تطور التكنولوجيا المتسارع في العصر الحالي، ظهر نوع جديد من الجرائم يُعرف بالجرائم الإلكترونية أو السيبرانية، وعليه خصصنا هذا المطلب لتعريف الجريمة السيبرانية (الفرع الأول)، ثم تحديد خصائصها (الفرع الثاني)، والتطرق لتحديد طبيعتها القانونية في (الفرع الثالث).

### الفرع الأول: تعريف الجريمة السيبرانية

تعددت وتباينت تعريفات الجريمة السيبرانية، وسنستعرض في هذا الفرع مختلف هذه التعريفات، وعليه تناولنا في هذا الفرع التعريف اللغوي للجريمة السيبرانية (أولا)، ثم نتطرق إلى التعريف الإصطلاحي (ثانيا).

**أولا: التعريف اللغوي للجريمة السيبرانية**

تعرف الجريمة السيبرانية في اللغة على أنها:

السيبرانية هي كلمة إنجليزية ناشئة عن كلمة(cyber) ، والتي تشير إلى الارتباط بالحواسيب أو شبكات الحواسيب، وغالباً ما يُقال إنها تشير إلى مجال الإنترنت، كما يُقال إنها كلمة يونانية ناشئة عن كلمة(kybernetes) ، والتي تعني الشخص المسؤول عن القبة التي تدير السفينة، مما يشير بشكل مجازي إلى المتحكم [1]، وسيبرانية هي كلمة مشتقة من كلمة (cybetneties) أي علم الضبط[2].

**ثانيا:التعريف الإصطلاحي**

إن مصطلح الجريمة السيبرانية ينقسم في شقيه إلى مصطلح الجريمة أولا فالجريمة فمصطلح الجريمة في اللغة هو الجرم والتعدي أو الذنب وجمعها إجرام أو جروم وهو الجريمة وفي نطاق القانون الجنائي هي فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدابير إحتيازيا.[3]

أما مصطلح الجريمة السيبرانية هو إحدى المصطلحات الحديثة والمستخدمة عن جرائم الأنترنت الذي تعددت مصطلحاته وذلك لنشأة تطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات، وقد صيغ مصطلح الجريمة السيبرانية لأول مرة من قبل ويليام جيبسون* عام 1982 ومنذ ذلك الحين اتسعت الحدود التي تحدد الجريمة السيبرانية، وخلال نشأتها فضل الأجيال الأولى من العلماء والمنظمات مصطلح جرائم الكومبيوتر بالمعنى الضيق للجريمة السيبرانية على مصطلح الجريمة السيبرانية بالمعنى الأوسع للكلمة، ومع تطور المصطلحات

---

[1] خرشف فاطمة ولزار سميرة، الإطار المفاهيمي والقانوني لمواجهة الجرائم السيبرانية، مجلة سوسيولوجيا للجريمة مخبر الجريمة والإنحراف بين الثقافة و التمثلات الإجتماعية، جامعة علي لونيسي البليدة2، مجلد 2، عدد 1،2021 ، ص60.

[2] منير البعلبكي، المورد قاموس إنجليزي–عربي، دار العلم للملايين، د.ط، بيروت، 2022 ،ص241.

[3] أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة بين التشريعات العربية والأجنبية، الطبعة الأولى، مكتبة القانون والإقتصاد،الرياض،2014، ص82.

* ويليام فورد جيبسون ولد في 17 مارس 1948 هو روائي أمريكي كندي له طابع خيالي تأملي ويدعى (بالرسول الأسود) أدخل ويليام جيبسون مصطلح الفضاء الإلكتروني في قصته القصيرة (الكروم المحترق) ثم أشاع هذا المفهوم في روايته الأولى نيورومانسر التي أصدرت عام 1948.

المستخدمة جرى بذل جهود أكاديمية لتعريف الجريمة السيبرانية، ولابد لأي نهج عصري في هذا الشأن أن يسلم بأن تعبير الجريمة السيبرانية ليس مصطلح قانوني قائم بذاته بل هو تعبير جامع يشمل مجموعة أفعال مرتكبة ضد بيانات أو نظم حاسوبية أو على استخدام موارد المعلومات لأغراض غير مشروعة.[1]

تمتاز الجريمة السيبرانية بتنوع التعاريف التي يتم تطبيقها عليها، يمكن وصفها بأنها استغلال غير قانوني للتقنيات المعلوماتية، سواء من خلال الاعتداء على برامج وبيانات الحاسب الآلي أو بواسطة استخدام التكنولوجيا بطرق غير مشروعة،

**ثالثا: التعريف الفقهي:**

تم تعريف الجريمة السيبرانية بتعريفات مختلفة، منها تعريف الأستاذ روزنبلات الذي وصفها بأنها: أي نشاط غير مشروع يستهدف نسخًا أو تغييرًا أو حذفًا أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي يتم الوصول إليها من خلاله، وعرفها الأستاذ ليزلي د، بول بأنها: فعل إجرامي يستخدم الحاسوب كأداة رئيسية في تنفيذه [2]، قد تبدو تعاريف الجريمة السيبرانية محدودة لأنها غالباً ما تقتصر على المعرفة العميقة في مجال الإعلام الآلي، على الرغم من وجود حالات تتضمن فيها ارتكاب هذه الجريمة باستخدام معرفة بسيطة فقط، لذا، ظهرت مظاهر فقهية تهدف إلى توسيع مفهوم الجريمة السيبرانية، من بين هذه التعاريف الفقهية الموسعة، نجد تعريف الفقيه كلاوس تايدومان الذي يعرف الجريمة السيبرانية على أنها: كافة أشكال السلوك الغير مشروع الذي يتم ارتكابه باستخدام

[1] ماينو جيلالي و عروس كوثر، الجريمة السيبرانية في صورها المستحدثة، مجلة القانون والتنمية، مخبر القانون والتنمية، جامعة طاهري محمد بشار، المجلد4، العدد1، جويلية 2023، ص53.

[2] صدام حسين ياسين العابدي، جرائم الأنترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعية، د.ط، المركز العربي للتوزيع،القاهرة،2018، ص43.

الحاسوب الآلي، وتعريف الأستاذين كليمنس مارتن وبرناديت هي، شيل على أنها: الجريمة المتعلقة بتكنولوجيا الحاسوب والإنترنت، وتشمل أيضاً الأفعال التي تعتبر جرائم سيبرانية مثل الدخول أو النسخ غير المشروع، وسرقة وسائل الإتصالات، والتشويش، والترهيب لفئة معينة من الناس أو المؤسسات، بالإضافة إلى الإرهاب السيبراني[1].

**رابعا: التعريف القانوني**

وفقًا للمادة الثانية من القانون رقم 04/09 الصادر في الجزائر، يُعرف المشرع الجزائري الجريمة السيبرانية، التي يُشير إليها بـ"الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات"، بأنها: الأفعال الإجرامية التي تستهدف أنظمة معالجة البيانات الآلية المحددة في قانون العقوبات، بالإضافة إلى أي جريمة تُرتكب باستخدام أو تسهيل من خلال شبكة معلوماتية أو نظام اتصالات إلكتروني، [2]

من خلال تحليل المادة المذكورة، يتضح أن المشرع الجزائري قد اعتمد على معيارين رئيسيين في تحديد الجريمة السيبرانية:

أ) التعريف بناءً على معيار الموضوع الجرمي: حيث يُعتبر الموضوع الجرمي هنا هو الاعتداء على أنظمة معالجة البيانات الآلية، وهو العنصر الأساسي في تحديد طبيعة الجريمة السيبرانية، هذه الجرائم محددة ضمن الفصل السابع المكرر من قانون العقوبات،

[1] طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر،2011-2012، ص ص3-4.

[2] المادة 2 من القانون09-04 المؤرخ في 13شعبان 1430 الموافق ل5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد 47، المؤرخة في 25 شعبان 1430هـ الموافق ل 15 غشت 2009، ص5.

تحت عنوان "الاعتداء على أنظمة معالجة البيانات الآلية"، وتشمل المواد من 394 مكرر إلى 394 مكرر7 من القانون المذكور .[1]

ب) بالنظر إلى الوسيلة المستخدمة في ارتكاب الجريمة، يمكن للمشرع أن يُضيف معياراً إضافياً لتحديد الجريمة السيبرانية، وهو البيئة المعلوماتية التي تم استخدامها*، تعتبر وسيلة ارتكاب الجريمة مؤثرة في تحديد نوع الجريمة ومعاقبتها.

وبالتبعية، يمكن تصنيف الجريمة السيبرانية وفقًا للتشريعات الجزائرية إلى فئتين، الفئة الأولى تشمل الجرائم التي تستهدف نظام معالجة البيانات وتهدف إلى التلاعب بالنظام بشكل كلي أو جزئي، وتُعاقب عليها وفقًا للمادة السابعة المكررة من قانون العقوبات، أما الفئة الثانية فتضم جميع الجرائم الأخرى المنصوص عليها في قانون العقوبات أو القوانين الخاصة، التي يتم ارتكابها أو تيسير ارتكابها باستخدام أنظمة المعلومات أو أي أنظمة اتصالات.[2]

## الفرع الثاني: خصائص الجريمة السيبرانية

تختص الجريمة السيبرانية بمجموعة من الخصائص والمميزات نذكرها على النحو التالي:

**أولا: الجريمة السيبرانية عابرة للحدود**

تتميز الجريمة السيبرانية بقدرتها على العبور بين الحدود الوطنية، وذلك بفضل التقدم التكنولوجي واستخدام الحاسوب الآلي في مختلف مجالات الحياة، لم تعد هذه الجرائم محصورة داخل حدود دولة معينة؛ بل أصبحت بالإمكان ارتكابها عبر الإنترنت،

[1] عميمر عبد القادر، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري، دراسة مقارنة، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر1، 2019-2020، ص19.

[2] المرجع نفسه، ص20.

مثل اختراق حواسيب في دولة ما وتدمير بياناتها، مما يجعل التعرض للهجوم ممكنًا في دولة مختلفة تمامًا، مثال على ذلك هو حالة هاوي في أوروبا الذي استطاع فك شفرة حاسوب في مركز معلومات في البنتاجون، مما أتاح له الوصول والتلاعب ببيانات هذا المركز، [1]

**ثانيا: الجريمة السيبرانية صعبة الإثبات**

إثبات جرائم الإنترنت يواجه تحديات كبيرة نظرًا لصعوبة تتبعها وكشفها، هذه الجرائم، التي تتخذ شكل رقمي بحت، لا تترك أدلة ملموسة يمكن تتبعها، مما يجعل اكتشافها أمرًا عشوائيًا في كثير من الأحيان وقد يحدث بعد فترة طويلة من وقوعها، بالإضافة إلى ذلك، تفتقر هذه الجرائم إلى الأدلة المادية التقليدية مثل البصمات الأصابع، من ناحية أخرى، يتطلب التحقيق في جرائم الإنترنت مهارات فنية متخصصة نادرًا ما تتوفر لدى المحققين العاديين، مما يزيد من صعوبة التعامل معها، علاوة على ذلك، يسعى مرتكبو هذه الجرائم بشكل متعمد إلى استخدام تقنيات التمويه والتضليل والاحتيال لتجنب الكشف عن هويتهم. [2]

**ثالثا: الجريمة السيبرانية سريعة التنفيذ والإخفاء**

لا شك في أن سرعة التنفيذ تمثل أحد أهم خصائص الجريمة السيبرانية، حيث يمكن للمجرم تنفيذ الجريمة بسرعة فائقة إما بنفسه أو من خلال استخدام برامج مصممة خصيصًا لهذا الغرض، هذا الأسلوب يسمح للمجرم بالتحرك بسرورية وبشكل خفي خارج

[1] غانم مرضي الشمري، الجرائم المعلوماتية، ماهيتها، خصائصها، كيفية التصدي لها قانونيا، ، الطبعة الأولى، الدار العلمية والدولية للنشر والتوزيع، عمان، 2016، ص37.

[2] رحوني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة أحمدة دراية–أدرار– د.ج، العدد41، د.ت، ص ص442_443.

مكان الجريمة، مما يجعله غير ملحوظ لدى الضحية، إضافة إلى ذلك، التقدم التكنولوجي قد أنتج العديد من الأدوات والبرامج التي تعزز سرعة تنفيذ الجريمة السيبرانية.[1]

**رابعا: قلة الإبلاغ عنها**

يعتبر عدم الإبلاغ عن الجرائم السيبرانية من أهم العوامل التي تعيق اكتشافها وإثباتها، ضحايا هذه الجرائم، وهم المجني عليهم، يلعبون دورًا رئيسيًا في ذلك، حيث يترددون في الإبلاغ عنها في حالة اكتشافها، العديد من الجهات التي تتعرض لانتهاك أنظمتها المعلوماتية أو تتكبد خسائر فادحة تفضل عدم الكشف عنها، حتى لموظفيها، وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ للسلطات المختصة، وذلك لتجنب الضرر بسمعتها والثقة في كفاءتها، وبالتالي، يكون الإبلاغ عن هذه الجرائم قليلًا مقارنة بالجرائم الأخرى، وهذا يعود إلى المخاوف من التشهير والتأثير السلبي على سمعة المجني عليه في حالة الإبلاغ عن الجريمة. [2]

**خامسا: محل وقوع الجريمة السيبرانية**

الجريمة السيبرانية لا تحدث في بيئة مادية ملموسة، بل تتم في بيئة الحاسوب وشبكة الإنترنت الافتراضية، مما يزيد من تعقيد التعامل معها لدى السلطات، في هذه البيئة، البيانات والمعلومات هي نبضات إلكترونية غير مرئية، مما يجعل من السهل على المجرم طمس الدليل أو محوه، الجريمة السيبرانية تحدث في العالم الافتراضي، من خلال بيئة المعالجة الآلية للمعطيات، مما يجعل من الصعب تحديد مكان وقوع الجريمة

[1] عبد الله بن حسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية، رسالة الماجستير في قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2014،ص33.

[2] قاسحي فيروز، الجريمة الإلكترونية عبر مواقع التواصل الإجتماعي، مجلة الرسالة للدراسات والبحوث الإنسانية جامعة الجزائر3، المجلد7، العدد8، فيفري2023 ، ص ص 206_207.

والتعامل معها، هذا يؤدي إلى صعوبة في جمع الأدلة وتحديدها، نظرًا لطبيعة محل وقوع الجريمة السيبرانية.[1]

## المطلب الثاني: الطبيعة القانونية للجريمة السيبرانية وصورها

تتميز الجريمة السيبرانية عن الجرائم التقليدية باعتبارها جريمة مستحدثة، مما يمنحها طابعًا قانونيًا خاصًا بها، وهذا ما سنناقشه في هذا المطلب.

### الفرع الأول: الطبيعة القانون للجريمة السيبيرانية

**أولا: الطبيعة القانونية الخاصة بالجريمة السيبرانية**

تتميز الجرائم السيبرانية بكونها لا تقتصر على أساليب تقليدية بل تستخدم تقنيات متقدمة وحديثة، مما يميزها عن الجرائم الأخرى، هذه الجرائم تنشأ وتتطور بفضل تكنولوجيا المعلومات، وبالتالي ترتبط ارتباطًا وثيقًا بها، هذا الارتباط يمنحها خصائص وسمات قانونية فريدة تميزها عن الجرائم التقليدية، بينما تخضع الجرائم بشكل عام للقانون الجنائي، فإن الجرائم السيبرانية غالبًا ما تتعلق بما يعرف بالقانون الجنائي السيبراني، هذه الخصوصية تضفي على هذا النوع من الجرائم طابعًا قانونيًا مميزًا، سواء فيما يتعلق بطبيعة الجريمة نفسها أو فيما يتعلق بخصوصية الأهداف التي تتعرض للاعتداء في إطار ارتكاب هذه الجرائم.[2]

**ثانيا: موقف المشرع الجزائري من الجريمة السيبرانية**

لم يجد المشرع الجزائري بدًّا من تعديل قانون العقوبات لسد الفراغ القانوني في هذا المجال، وذلك بموجب القانون 15/04 المتضمن قانون العقوبات، حيث أضاف القسم

[1] عبد الله بن حسين آل حجراف القحطاني، المرجع السابق، ص33.

[2] سعيداني نعيم، آليات البحث والتحري في الجريمة المعلوماتية في القانون الجزائري، مذكرة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر –باتنة–، 2013/2012، ص30.

السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، وقد ورد في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى ظهور أشكال جديدة من الإجرام، وقد رأى المشرع الجزائري أن جوهر المعلوماتية يكمن في المعطيات التي تدخل إلى الحاسب الآلي وتتحول إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات بطرق متعددة، لذلك فضل المشرع الجزائري استخدام مصطلح "المساس بنظم المعالجة الآلية للمعطيات"، والذي يشمل المعلومات والنظام الذي يحتويها، بما في ذلك شبكات المعلومات، مما يجعل نطاق التجريم يقتصر على الأفعال التي تشكل اعتداءً على النظام المعلوماتي.[1]

## الفرع الثاني: صور الجريمة السيبرانية

بلا شك، تطوَر تكنولوجيا الحواسيب، بما في ذلك طابعات الليزر والماسحات المتقدمة، قد ساهم بشكل كبير في تزوير المعلومات المخزنة في أنظمة الحواسيب، نظرًا لاعتمادنا المتزايد على هذه الأنظمة في تخزين ومعالجة البيانات الحساسة مثل بيانات الولادة والوفاة وجوازات السفر ورخص القيادة، أصبح من الضروري حماية هذه المعلومات من التلاعب.

تتخذ عمليات التزوير المعلوماتي صورتين رئيسيتين، الأولى تتمثل في تلاعب في المعلومات داخل نظام الحاسوب، وذلك لتغيير الحقيقة في هذه المعلومات، يمكن أن يتم ذلك عن طريق تعديل المعلومات، أو حذف أجزاء منها، أو تعطيل وظائفها.

الصورة الثانية للتزوير المعلوماتي تتمثل في تزوير المعلومات نفسها، سواء كان ذلك عن طريق إنشاء معلومات مزيفة أو تعديل المعلومات الأصلية بطريقة تغير معناها أو تشوهها.

[1] حشمان عمار، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، كلية العلوم الإقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح–ورقلة–2018_2019، ص17.

بالتالي، أصبح من الضروري تطوير تدابير أمنية قوية لحماية المعلومات المخزنة في أنظمة الحواسيب من التلاعب والتزوير، وتعزيز الوعي بأهمية الأمان السيبراني للحفاظ على سلامة وصحة المعلومات.

في السياق الثاني، يتم تحويل معلومات غير صحيحة لإنشاء وثيقة مزيفة، ويتم هذا التحويل بنية استخدام المعلومات بطريقة غير مشروعة، ويتم ذلك باستخدام التكنولوجيا الحاسوبية لتزوير الوثائق.[1]

## أولا: على مستوى الجامب التشريعي

تعتبر التجسس بشكل عام من المجالات المثيرة للجريمة السيبرانية، حيث يُعتبر من الجرائم التي يمكن تنفيذها بسهولة عبر الحواسيب، يتوسع نطاق التجسس في مجال السيبرانية ليشمل أنواعًا متنوعة من المعلومات، بما في ذلك الأسرار الحكومية في عدة مجالات، بالإضافة إلى المعلومات الصناعية.[2] عندما يُستخدم التجسس السيبراني، يتم الهدف منه الحصول على معلومات سرية غير مشروعة بهدف تحقيق أفضلية استراتيجية أو اقتصادية أو عسكرية، يمكن تعريف التجسس السيبراني على أنه استخدام تقنيات التكنولوجيا للحصول على المعلومات، ويختلف نوع التجسس، حيث يمكن أن يكون عبر الأفراد أو عبر شبكات الاتصالات السلكية أو حتى من خلال الأقمار الصناعية.[3]

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، دراسة نظرية تطبيقية، ، الطبعة الأولى، منشورات الحلبي الحقوقية، القاهرة، 2015، ص270.

[2] نائلة عادل محمد فريد قورة ، المرجع نفسه، ص 273.

[3] قطاف سليمان و بوقرين عبد الحليم، مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية، مجلة البحوث القانونية والإقتصادية، مخبر البحث في الحقوق والعلوم السياسية جامعة عمار ثليجي–الأغواط–، المجلد5، العدد2 2022، ص72.

### ثانيا: سرقة المعلومات

سرقة المعلومات تختلف عن السرقة التقليدية بسبب طبيعتها الخاصة وعدم قابليتها للانتقال من حيازة إلى أخرى، يمكن تجريم الحصول غير المشروع على المعلومات المبرمجة آليًا حتى لو لم يتم نسخها أو طباعتها، قد يكون الحصول على المعلومات بهدف ارتكاب جريمة أخرى أو بهدف الحصول عليها بحد ذاتها، تجريم سرقة المعلومات يهدف إلى حماية المعلومات المبرمجة آليًا وإقامة توازن بين حماية المعلومات وحق الوصول إليها، الإطلاع على المعلومات دون نية غير مشروعة لا يعتبر سرقة المعلومات، وهذا يميزها عن جريمة الدخول غير المصرح به لنظام الحاسب الآلي. [1]

### ثالثا: الإرهاب السيبراني (cyber terrorism)

يمثل الفضاء السيبراني عنصرًا جذبًا للتنظيمات الإرهابية المتنوعة والمختلفة في الإيديولوجيات، نظرًا لما يوفره من وسائل إعلام دولية وأدوات قوة، يمكن للأطراف المختلفة استخدام هذا الفضاء، وقد أثبت تنظيم "داعش" أنه التنظيم الإرهابي الأكثر تهديدًا لسلامة شبكة الإنترنت العالمية، حيث استخدم الفضاء السيبراني في الدعاية والتمويل والتجنيد وجمع المعلومات وتنسيق الهجمات الإرهابية، كما يستخدم هذا التنظيم وسائل التكنولوجيا للتجنيد ونشر أفكاره في أوساط الشباب، وكانت حملاته في بعض الأحيان قادرة على إثارة العنف والخوف والرعب في الدول والمجتمعات.[2]

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص 269.

[2] غريب حكيم، الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديد وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، المجلد5، العدد2،ص ص103-104.

# المبحث الثاني: ماهية التجسس عبر الانترنت الماس بأن الدولة

يتناول المبحث الثاني ماهية التجسس عبر الإنترنت الذي يمس بالدولة، حيث يستعرض المطلب الأول جريمة التجسس الكلاسيكي، بينما يركز المطلب الثاني على التجسس السيبراني.

## المطلب الأول: جريمة التجسس الكلاسيكي

يتناول المطلب الأول جريمة التجسس الكلاسيكي، حيث يستعرض الفرع الأول تعريف جريمة التجسس، بينما يركز الفرع الثاني على أركان جريمة التجسس.

### الفرع الأول: تعريف جريمة التجسس

**أولا: التعريف اللغوي**

**التجسس** : كلمة مأخوذة من الجذر "جسس" وتعني التحقق من شخص ما عبر النظر إليه بدقة لفهمه بشكل أفضل، يشير الجَسُ إلى الفحص والبحث، فالجس يعني البحث عن شيء ما أو التحقق منه، نقول: "تحسست فلانًا" أو "تحسست من فلان" بمعنى بحثت عنه أو عنه بشكل دقيق، أما التجسس، فهو البحث عن الأمور المخفية، وغالبًا ما يستخدم في سياق الأمور السيئة [1] فعل التجسس يعني استكشاف الأخبار والبحث عنها بطرق غير مشروعة، وهو سلوك مرفوض نهانا الله عن ممارسته لقوله تعالى بعد بسم الله الرحمان الرحيم "يَا أَيُّهَا اللذين آمنوا اجتنبوا كثيرًا من الظَّن إن بعض الظن إثم ولا تَجَسَّسُوا وَلا يَغْتَب بَعْضُكُم بعْضًا أيحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ"[2]

[1] أمل جبر عبد الخالق إشتوي ، التجسس عبر التصوير في الفقه الإسلامي ، ( رسالة ماجستر) في الفقه المقارن ، كلية الشريعة والقانون ، غزة، د س ن ص 17

[2] سورة الحجرات ، الآية 12

وقوله صلى الله عليه و سلم "إنا قد نهينا عن التجسس ولكن إن يظهر لنا شيء تأخذ به".[1]

**ثانيا: التعريف القانوني لجريمة التجسس**

**أ- تعريف جريمة التجسس في قانون العقوبات الجزائري:**

لم يقم المشرعون في الجزائر بتحديد تعريف لجريمة التجسس، بل اعتمدوا على العقوبة المرتبطة بها في نص المادة 64 من قانون العقوبات التالي:

يتعرض للإعدام أي شخص أجنبي يرتكب جريمة التجسس عندما يقوم بأي من الأفعال المذكورة في الفقرات 2 و 3 و 4 من المادة 61، وفي المادتين 62 و 63، أيضًا، يتعرض المضطهدون للعقوبة المقررة لهذه الجرائم إذا حثوا على ارتكاب أي من الجرائم المذكورة في المادة 64 والمواد 61، 62، 63.

**ب- تعريف جريمة التجسس في القانون الدولي العام**

توجد اختلافات في تعريف التجسس بين فترات الحرب والسلم، يشير القانون الدولي الإنساني إلى التجسس خلال فترات الحرب بشكل واضح ومفصل، فقد نصت المادة 29 من اتفاقية لاهاي لعام 1907 على تعريف الجاسوس بشكل صريح: يُعتبر شخصًا جاسوسًا إذا قام بجمع المعلومات بطريقة سرية في منطقة الأعمال الحربية بهدف توصيلها إلى العدو، [2]

[1] حديث شريف علاء الدين بن محمد بن إبراهيم البغدادي، تفسير الخازن لباب التأويل في معاني التنزيل، جزء 5 ، دار الكتب العلمية بيروت، لبنان.

[2] فواز البقور ، التجسس في التشريع الأردني دراسة مقارنة، دار النشر، الطبعة الثالثة، عمان، 1993، ص 25.

من خلال هذا النص، يمكننا استنتاج تعريف للتجسس خلال الحرب، وهو يتضمن استخدام جميع طرق الخداع والكذب المحظورة في سياق النزاع، بما في ذلك نقل أو نشر أي معلومات أو أوامر تعتبر من المعلومات السرية للدولة مع الهدف الوصول بها إلى العدو، [1]

تجد في القوانين الدولية نقصاً في التطرق إلى ممارسة التجسس خلال فترات السلم، حيث لم يتم الإشارة إليها بوضوح، ولا وجود لأي نصوص تلزم الدول بمنع التجسس على بعضها خلال هذه الفترات، يعود ذلك جزئياً إلى عدم وجود اتفاقيات تنص على حظر التجسس في هذه الظروف، مما يجعل هذا المجال غير محدد بشكل واضح في الأنظمة القانونية الدولية، [2] فيما يتعلق بالتجسس خلال فترات السلم، قدم الفقهاء تعريفات متعددة، بشكل عام، يُعتبر التجسس، وفقًا لغالبية فقهاء القانون الدولي، سلوكًا يخالف الأسس القانونية الدولية لأنه يشكل تهديدًا لأمن الدول واستقلالها، [3] بعض الفقهاء يرون أن التجسس ينتهك القواعد القانونية الدولية إذا استخدمت فيه وسائل وأساليب غير مشروعة بموجب القانون الدولي، مثل انتهاك السيادة الإقليمية، بالإضافة إلى الفعل نفسه للتجسس،[4]

## الفرع الثاني: أركان جريمة التجسس

### أولا: الركن الشرعي لجريمة التجسس.

سيتم تعريف الركن الشرعي كالتالي:

[1] عبد الغني بوجراف، التجسس كجريمة ماسة بأمن الدولة في ظل قانون العقوبات الجزائري، مجلة أفاق العلوم، الجلفة الجزء الأول، العدد الثامن 2017، ص 339

[2] صلاح نصر ، الحرب الخفية تاريخ المخابرات، دار الخيال الجزء الأول، الطبعة الأولى، القاهرة، 2002، ص 81.

[3] عبد الرحمان لحرش، التجسس والحصانة الديبلوماسية، مجلة الحقوق، جامعة الكويت، العدد الرابع، السنة السابعة والعشرون ، 2003، ص 179.

[4] عبد الرحمان الحرش ، المرجع نفسه، ص 182.

النص الذي يُجرّم الفعل المرتكب والمحدد في قانون العقوبات أو في نصوص الشريعة الإسلامية، حيث ينص قانون العقوبات على أنه لا توجد جريمة أو عقوبة أو إجراء أمني إلا بموجب نص قانوني، بناءً على ذلك، فإن أي فعل غير مُجرَّم في قانون العقوبات يُعتبر مباحًا حتى لو رفضته الأخلاق والعادات والتقاليد.

يشير المبدأ القانوني للشرعية إلى أن القانون يجب أن يحدد ويجرم الأفعال الجرمية، حيث يعتبر الأصل في الإنسان البراءة وفي الأشياء الإباحة، يختلف الفقه الجنائي في تحديد مدى وجود هذا الركن، حيث يوجد من يعتبر الجريمة تتألف من الركن المادي والمعنوي فقط، وبناءً على أن العمل الضار لا يعتبر جريمة إلا بوجود نص قانوني يحدده، فإنه يصبح ضرورياً لوجود الجريمة أن يكون هناك نص قانوني يحددها.

وقد تم تأكيد مبدأ الشرعية في إعلان حقوق الإنسان الصادر بعد الثورة الفرنسية عام 1789، وفي المادة 11 من الإعلان العالمي لحقوق الإنسان لعام 1948، كما تم تضمين هذا المبدأ في جميع المصادر القانونية العالمية والدساتير الوطنية، وبالتالي، لا يمكن للقاضي الجنائي إصدار حكمه إلا بناءً على النصوص القانونية المحددة، [1]

يقوم الركن الشرعي على عنصرين أساسين تتمثل فيما يلي:

### 1 – خضوع الفعل لنص تجريمي:

ينبغي أن يكون التهمة والعقوبة محصورين في نطاق النصوص القانونية المكتوبة، أي ينبغي أن يكون التهمة والعقوبة موضوع لنص مجلس النواب المكتوب، وإذا كانت السلطة التشريعية

[1] عبد الله سليمان، شرح قانون العقوبات الجزائري القسم العام، ديوان المطبوعات الجامعية، الجزء الأول (الجريمة)، د ط، 1995، ص 68.

هي المسؤولة عن تحديد التهمة والعقوبة، بينما السلطة القضائية مسؤولة عن تطبيق القانون، فإن السلطة التنفيذية لها الصلاحية للتشريع في مجال المخالفات من خلال إصدار توجيهات تسمى توجيهات الضبط.

**2 – عدم وجود سبب من أسباب الإباحة:**

هذا العنصر يلغي الخصائص الجنائية للفعل ويجعله مقبولاً، حيث يُمكن أن يُحول وجود أحد الأسباب المبررة الفعل إلى خارج نطاق الجريمة، ويُزيل الشبهة غير المشروعة منه، وبالتالي يعود الفعل إلى قانونيته بعد أن كان مُحكوماً، والسبب في ذلك هو أن انعدام سبب التجريم لا يجعل الفعل يحمل طابع العدوان إذا تم ارتكابه في ظروف معينة تبرر إباحته.

وتندرج تحت ثلاثة عناصر:

- **تنفيذ الأوامر القانونية:** على سبيل المثال، لا يُعتبر فعل الموظف الذي ينفذ حكم الإعدام جريمة قتل، ولا تسري عليه أحكام قانون العقوبات.
- **استخدام السلطة التقديرية:** يُسمح للموظفين العموميين باستخدام سلطاتهم التقديرية وممارسة الحقوق الممنوحة لهم بموجب القانون.
- **الدفاع الشرعي:** يُعترف بحق الدفاع عن النفس في القانون، ويُسمح باستخدام القوة الضرورية في حالات محددة، شريطة أن تكون هذه القوة متناسبة مع خطورة الاعتداء وألا تتجاوز الحدود اللازمة للدفاع، يُفرق القانون بوضوح بين الدفاع الشرعي وأعمال الانتقام أو القصاص الذاتي.[1]

**ثانيا: الركن المفترض لجريمة التجسس.**

سنتطرق إلى الركن المفترض لجريمة التجسس وفق ما يلي:

[1] عبد الله سليمان، مرجع سابق، ص 70.

**تعريف الركن المفترض** :لكي تُعطى الجريمة الجنائية وصفها الصحيح، وحتى يمكن اعتبار الفعل الإجرامي جريمة وفق القانون، يتطلب القانون أحيانًا توافر شروط معينة عند ارتكاب الفعل الإجرامي،

ظهرت فكرة الركن المفترض لأول مرة من قبل الفقيه "مانزيني"، الذي أسس الفكرة بوجود ركن آخر إلى جانب الأركان التقليدية اللازمة لإكتمال الجريمة، يعرّف الفقيه "مانزيني" الأركان المفترضة على أنها: "ظروف أو عناصر إيجابية أو سلبية يجب توافرها قبل أو أثناء الفعل المادي لتكوين الجريمة."[1]

يميز الفقيه بين نوعين من الركن المفترض، حيث يوجد النوع الأول في الركن المفترض للجريمة، في هذه الحالة، عدم وجود الركن أثناء إجراء الفعل الجنائي لا يجعل الجريمة غير صالحة، بل يغير وصفها وتحولها إلى جريمة ذات وصف مختلف، مثال على ذلك هو صفة الموظف في جريمة استيلاء على أموال الدولة، حيث يزول صفة الموظف.

**ثالثا: الركن المادي لجريمة التجسس في التشريع الجزائري**

لا يمكن وجود جريمة إلا بتوافر ركنين أساسيين: الركن المادي والركن المعنوي، الركن المادي يتألف من ثلاثة عناصر رئيسية: السلوك الإجرامي، النتيجة، والرابطة السببية بينهما، وفقًا للقانون، يجب توافر هذه العناصر مجتمعة في بعض الجرائم مثل القتل والسرقة والضرب، وتعرف هذه الجرائم بالجرائم المادية، ومن ناحية أخرى، لا يشترط وجود النتيجة

[1] عبد الغني بوجراف، مرجع سابق، ص 341.

في بعض الجرائم الأخرى مثل حمل السلاح بدون ترخيص، وتعرف هذه الجرائم بالجرائم الشكلية.

وبالإضافة إلى ذلك، يجب أن يتوافر الركن المعنوي لقيام الجريمة، والذي يتمثل في نية الجاني وإصراره على ارتكاب الجريمة، فالقانون لا يعاقب على النوايا والأفكار فحسب، بل يتطلب وجود سلوك فعلي ضار ونية جرمية لتوجيه العقاب، [1]

يتمثل الجزء المادي في جريمة التجسس في مجموعة من السلوكيات الجنائية، سواء كانت إيجابية أو سلبية، التي يقوم بها المتهم أو مجموعة من المتهمين، وهو ما تنص عليه المادة 64 من قانون العقوبات والمادة 66، يُفترض أن يكون قد ارتكب الخيانة أو التجسس عن عمد، وكل من ارتكب أيًا من الأفعال المبينة في الفقرات 2، 3، 4 من المادة 63.

**1-السلوك الإجرامي:**

ويتعلق هذا بحركة الشخص المتسبب في الجريمة، حيث يسعى للحصول على معلومات أو أسرار دولية، وهي جزء أساسي من عنصر السلوك في جريمة التجسس، لم يحدد التشريع الجزائري وسيلة محددة لاكتساب هذه المعلومات، سواء كانت ذلك بطرق مباشرة أو غير مباشرة، بسيطة أو معقدة، صريحة أو غير ملتوية، ومع ذلك، تختلف هذه الطرق باختلاف الأماكن؛ حيث يوجد اختلاف بين الأماكن العسكرية وطريقة الحصول على الأسرار، سواء كانت معروضة أو مخبأة عادةً في المكاتب، يمكن أن يشمل هذا الحصول على مراحل مختلفة حتى يتم الوصول إلى النتيجة المرغوبة.

**2-النتيجة:**

[1] منصور رجماني، المرجع السابق، ص 69-70.

لكي تكتمل جريمة التجسس، يجب أن تصل المعلومات المستهدفة إلى الدولة الأجنبية أو الشخص الذي يعمل نيابةً عنها، العنصر الأساسي في هذه الجريمة هو عملية التجسس نفسها، بينما النتيجة المتوقعة هي تسليم المعلومات المجسس عليها إلى الجهة التي تسعى للحصول عليها من خلال هذه الأنشطة.

**3-العلاقة السببية:**

تعني أن السلوك الإجرامي نتج عنه وصول معلومة محددة إلى جهة دولة أجنبية، وبذلك، لولا الفعل الإجرامي لما حصلت الدولة على هذه المعلومة، وعليه، فإن العلاقة السببية تكمن في الربط بين الفعل والنتيجة، وهي مكملة للركن المادي، فلا يكفي الفعل وحده لقيام الجريمة، ولا يكفي وجود النتيجة وحدها، بل يجب أن يكون هناك ارتباط سببي بينهما[1].

تعريف الركن المعنوي: يرتبط الركن المعنوي بالقصد الجنائي، وهناك عدة تعريفات للقصد الجنائي، على سبيل المثال، عرفه الأستاذ عبد الله سليمان بأنه العلم بعناصر الجريمة وإرادة إرتكابها، [2] ويوجد تأكيد واضح في العديد من نصوص قانون العقوبات الجزائري على توافر القصد الجنائي عند توافر عنصري العلم والإرادة، مثل ما هو منصوص عليه في المادة 73 من قانون العقوبات التي تعاقب بالسجن من سنة إلى خمس سنوات وبغرامة من 3,000 إلى 30,000 دج كل من ارتكب عمدا..، وكذلك المادة 254 التي تصف القتل بأنه "إزالة روح إنسان عمدا"، والمادة 180..، كل من أخفى عمدا..، كما لا يلاحظ أن المشرع الجزائري استخدم عبارة "مع علمه بذلك" للدلالة على توافر عنصر العلم، في المادة 42/2 من قانون العقوبات التي تنص على ذلك.

[1] محمد بوشعبة، مذكرة ماجيستير بعنوان الخيانة والتجسس في قانون القضاء العسكري الجزائري، قانون جنائي، جامعة يحي فارس، المدية، 2022، ص 29.

[2] عبد الله سليمان، مرجع سابق، ص 249.

يُعتبر شخصًا شريكًا في الجريمة إذا لم يشترك مباشرةً في ارتكابها، ولكنه قدم المساعدة للفاعل أو الفاعلين في الأفعال التحضيرية أو المسهلة أو المنفذة للجريمة، مع علمه بذلك، "[1]

فيما يتعلق بالركن المعنوي لجريمة التجسس، يكفي وجود القصد الجنائي العام، أي تعمد الفاعل ارتكاب جريمة سرقة الأسرار أو الحصول عليها بطريقة غير مشروعة، مع العلم بأن المشرع يجرم هذه الأفعال، يُعتبر مجرمًا كل شخص يستولي على هذه الأسرار بطريقة غير مشروعة.

يتضمن القصد الجنائي الخاص أنه إذا توافر، فإنه يؤدي إلى نتيجة واحدة هي تثبيت العقوبة وتصنيف الفعل كجريمة، والدافع أو المُبعث لارتكاب الجريمة يُحتسب للقاضي لتقييمه، يجدر بالإشارة إلى أن القصد الجنائي العام يتكون من عنصرين: العلم والإرادة، أي أن يكون المتهم على علم بأركان الجريمة وعناصرها، إذا كان المتهم جاهلاً بهذه الأمور، فإن القصد الجنائي يختفي، مما يؤدي إلى إزالة الجريمة وترك الجزء المعنوي.

توافر القصد العام لا يعني بالضرورة توافر القصد الخاص لدى المتهم، ولكن يفترض وجوده ما لم يثبت المتهم عدم وجود النية، [2]

## المطلب الثاني : التجسس السيبيراني

نتناول في هذا المطلب مفهوم التجسس السيبراني في الفرع الأول، ثم نتطرق إلى وسائل ارتكاب التجسس الإلكتروني في الفرع الثاني.

[1] إبراهيم بلعليات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الطبعة الأولى، الجزائر، 2007، ص 119.

[2] أسية والي، سامية باشوش، مرجع سابق، ص.101.

## الفرع الأول: مفهوم التجسس السيبيراني

تستحوذ مواضيع التجسس الإلكتروني اهتمام جيل اليوم خاصة الدخول إلى عالم الهاكرز الذي يعتبر حلماً يسعى إليه الكثير من الشباب، أما شبكة الإنترنت فهي ميدان صراعات من نوع جديد حملت كل أدوات التدمير الإلكتروني كالتجسس والاختراق وتدمير المواقع الإلكترونية الحكومية وغير الحكومية، والتحكم في تغيير قواعد بيانات قد تصل خطورتها إلى تهديد الأمن القومي لبعض الدول، مما دفع بعض خبراء الإنترنت للاعتقاد أن الشبكة العنكبوتية أصبحت على حافة الانهيار، ولخص بعض تقنيي الإعلام

الآلي لدى شركة (Kaspersky) ما يحدث بقولهم: إن التكنولوجيا يأكل بعضها بعضا، جريمة التجسس الإلكتروني ولعل أصعب ما يمكن الاستدلال به كبداية لفهم هذه الظاهرة هو تقديم تعريف لها أو على الأقل إعطاء تفسير لها، بحكم أن كل ما ينشط في العالم الافتراض يصعب تحديد ماهيته.

### أولاً: تعريف التجسس الإلكتروني

لا يوجد تعريف دقيق للتجسس الإلكتروني، إذ يشكل التجسس مفهومًا شاملاً لا يمكن تحديده بتعريف واحد، يمكن وصف التجسس الإلكتروني بأنه شكل من أشكال الإرهاب الإلكتروني، حيث يتم استخدام التكنولوجيا بشكل سلبي لإحداث آثار مدمرة وأضرار جسيمة على أنظمة التحكم وأجهزة الكمبيوتر وشبكات الاتصال، بغرض سياسي أو عرقي أو ديني، وما إلى ذلك، ويمتد نطاق التجسس الإلكتروني ليشمل العدوان أو التخويف أو التهديد، سواء كان ذلك من دول أو جماعات أو أفراد، باستخدام الوسائل الإلكترونية للإضرار بالأفراد بشكل مادي أو معنوي بطرق غير قانونية»[1]

[1] https://www.facebook.com/realestateKhal/posts

يمكن تعريف برامج التجسس على أنها أدوات تستخدم لمراقبة وتتبع سلوك الحاسوب، بما في ذلك ما يكتبه المستخدم والمواقع التي يزورها، بهدف سرقة معلومات حساسة مثل كلمات المرور، الغرض الأساسي من هذه البرامج هو مراقبة وتسجيل كافة الأنشطة التي تحدث على الجهاز، بمجرد تثبيت برنامج التجسس، يبدأ في إخفاء نفسه داخل النظام، مما يجعل من الصعب على المستخدم اكتشاف وجوده، [1]هناك أنواع أخرى من برامج التجسس تؤثر سلبًا على أداء جهاز الكمبيوتر ونظام التشغيل، حيث يمكن أن تتسبب في إبطاء الجهاز أو تعطيله أو حتى إلحاق الضرر بنظام التشغيل، بالإضافة إلى ذلك، تمتلك هذه البرامج القدرة على تغيير الصفحة الرئيسية أو صفحة البحث الافتراضية في متصفحات الويب، أو حتى إضافة مكونات غير ضرورية أو غير مرغوب فيها إلى المتصفح، قد تجعل هذه البرامج أيضًا من الصعب تغيير الإعدادات وإعادتها إلى حالتها الأصلية، وفقًا للتقييمات الحديثة، تم الكشف عن أن أكثر من ثلثي الحواسيب الشخصية تتأثر بأحد أنواع برامج التجسس [2].

**ثانيا: أنواع التجسس**

من الصعب تحديد أو إحصاء جميع أنواع التجسس الإلكتروني، ومع ذلك، سنحاول سرد بعض الأنواع الرئيسية لهذا النوع من الاختراق:

**1-التجسس عن طريق الشبكات السلكية واللاسلكية**

لقد ظهرت أنواع جديدة من التجسس الإلكتروني في الشركات والمؤسسات التي تستخدم الشبكات بجميع أشكالها، سواء كانت سلكية أو لاسلكية، صغيرة أو كبيرة، ومن بين أكثر أساليب التجسس شيوعًا داخل الشبكات ما يُعرف بـ "Sniffer" أو اصطياد حزم البيانات

[1] سالم منصور، ماهي برامج التجسس؟ وكيف تتسل لأجهزتنا؟على الموقع
http://www.arabs2day.ws/forums/lofiversion/index.php/t172.htm أطلع عليه بتاريخ 2024/05/19 على الساعة 21:00.

[2]نوف علي الشنيفي، البرامج التجسسية أنواعها وطرق الحماية منها، مركز التميز الأمن المعلوماتي، مصر.2011.

المرسلة، ومن بين البرامج الشهيرة المستخدمة لهذا الغرض في أنظمة ويندوز ولينكس هو برنامج "Ethereal" للشبكات الداخلية، بالإضافة إلى برامج مثل "Tcpdump" و "WinDump"وغيرها، تتيح هذه البرامج للمستخدمين اصطياد البيانات المرسلة داخل الشبكة ومراقبة معظم البروتوكولات، مما يعني أن أي شخص داخل شبكة محلية يمكنه التجسس على بقية المستخدمين، وقد تم إجراء تجربة على أحد أنواع "Sniffer" المتخصصة في اصطياد كلمات المرور في إحدى مقاهي الإنترنت، وكانت النتيجة الحصول على كلمات المرور السرية لحسابات البريد الإلكتروني للأشخاص الذين قاموا بتسجيل الدخول، [1]

**2-التجسس بواسطة الأقمار الصناعية**

هذا النوع من التجسس الإلكتروني يتميز بطابع دولي ويعتمد على استخدام تقنيات وأجهزة متطورة للغاية، وعلى الرغم من أن المصادر المتاحة حول هذا الموضوع قليلة، إلا أنه يمكن القول أن التجسس عبر الأقمار الصناعية يتطلب قدرات تكنولوجية وتقنية عالية ويقتصر على الدول المتقدمة التي تمتلك القدرة على تطوير وإطلاق الأقمار الصناعية بنفسها، تتميز هذه الأقمار الصناعية بأحدث التقنيات والبرامج المتاحة، وعادة ما يتم إطلاقها أمام الرأي العام بأسباب إنسانية أو علمية، ولكن الدولة المسؤولة عن إطلاق القمر الصناعي تكون وحدها على علم بالغاية والهدف الحقيقي للمهمة، وخاصة إذا كان القمر الصناعي مُرسلًا بهدف التجسس.

**3-التجسس بالاستعمال شبكات الهاتف النقال**

في عام 2006، قدمت شركة كنديك الأوروبية المعروفة في مجال التجسس العسكري والإرهاب، برنامجًا رقميًا يُسمى(CrytoPro GSM A5) ، والذي كشف عن إمكانية اختراق تشفير الأنظمة الإلكترونية المستخدمة لحفظ وحماية سرية المعلومات خلال المكالمات

[1] حسن بن أحمد الشهيري، «الأنظمة الإلكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس» المجلة العربية للدراسات الأمنية والتدريب المجلد ،28العدد ،56 ص 13-14.

الهاتفية أو الرسائل النصية، يمكن للبرنامج الوصول إلى المحتوى وتغييره أو حذفه، تظهر صورة من البرنامج توضح قدرته على التقاط المحادثات والرسائل النصية بدقة عالية، يدعم البرنامج نظام اليونكود المختلف اللغات، وتوجد نسخة مخصصة لشبكات GSM ونسخة أخرى لشبكة الثريا، هذا يعني أنه بمجرد الحصول على هذا البرنامج وتثبيته على جهاز يحتوي على وصلة لاسلكية، يمكن لأي شخص التجسس على شبكةGSM ، [1]

## الفرع الثاني: وسائل ارتكاب التجسس الإلكتروني

وفقًا لنص المادة الثانية الفقرة "أ" من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق نظام معلوماتي أو نظام للاتصالات الإلكترونية"، وعلى ذلك، يمكن القول أن التجسس الإلكتروني المذكور في المادة 64 يمكن أن يرتكب بواسطة نظم معالجة آلية للبيانات، ويمكن أن يرتكب بوسائل اتصال متقدمة، حتى بدون استخدام العنصر البشري الأجنبي، يمكن توضيح ذلك كما يلي:

**أولا: التجسس المرتكب بواسطة أنظمة المعالجة الآلية للمعطيات**

وفقًا للمادة 394 مكرر 3 في القانون الجزائري، يتم تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، وذلك دون الإخلال بتطبيق عقوبات أشد، إذا كان الأجنبي يستهدف نظام المعالجة الآلية للمعطيات الخاص بالدفاع الوطني، فإنه يعتبر جاسوسًا إلكترونيًا وتكون عقوبته الإعدام، حيث أن العقوبة المنصوص عليها لجريمة التجسس أشد من مضاعفة عقوبات جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وقد حدد المشرع ثلاث صور لهذه الجرائم وسنتناولها في النقاط التالية:

[1] نوف علي الشنيفي، مرجع سابق، ص15.

**1-الآلية للمعطيات**

وفقا للمادة 394 مكرر من قانون العقوبات الجزائري، يتم معاقبة أي شخص يقوم بالدخول أو البقاء بطريقة غير مشروعة في نظام المعالجة الآلية للمعطيات، أو يحاول ذلك، بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية تتراوح بين 50,000 دج و100,000 دج، تتضاعف هذه العقوبة إذا تسببت هذه الأفعال في حذف أو تغيير المعطيات الموجودة في النظام، وفي حالة تسببت هذه الأفعال في تخريب نظام العمل للمنظومة، تصبح العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50,000 دج إلى 150,000 دج، تتكون هذه الجريمة من ركن مادي (الدخول أو البقاء غير المشروع في النظام) وركن معنوي (القصد الجنائي)، وسنتناولهما في النقاط التالية:

- **الركن المادي**

يقوم الركن المادي في هذه الجريمة على فعل الدخول أو على فعل البقاء في كل أو جزء من نظام معالجة آلية للمعطيات ويكفي قيام أحدهما على جزء أو كل النظام لتحقق الجريمة.

والدخول هو حسب الفقه الفرنسي [1]، لهذا الفعل مدلولان، مادي ومعنوي، المدلول المادي يكون عندما يحاول الجاني دخول النظام الإلكتروني، أو يدخل بالفعل إليه، أما المدلول المعنوي فيتمثل في الدخول في العمليات الذهنية التي يقوم بها النظام، ويمكن أن يتم الدخول بأي وسيلة، فمثلاً يمكن للجاسوس أن يقوم بالتلاعب بعناصر الأنظمة الدفاعية

[1] عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت، في القانون العرب النموذج. مصر مطابع شتات،2007، ص 62.

الإلكترونية للدولة للحصول على المعلومات التي تمكنه من القيام بالتجسس، أو يمكنه ربط النظام بجهاز تصنت أو اعتراض للوصول إلى المعلومات السرية، وقد يتم ذلك عن طريق برنامج فيروسات مثل برنامج حصان طراودة الذي يساعد المستخدم على الحصول على كلمة السر ودخول النظام دون اكتشاف، وبالتالي، يُعتبر هذا البرنامج فعالًا في عمليات التجسس، [1]؛ ويتحقق الدخول متى كان غير مشروعا، أي مخالفا لإرادة صاحب النظام أو من له حق السيطرة عليه، فالدخول على الأنظمة التي تتعلق بأسرار الدولة الدفاعية أو العسكرية هو دخول غير مشروع [2]

البقاء في النظام يعني التواجد داخل نظام المعالجة الآلية للبيانات دون موافقة من يمتلك السيطرة على هذا النظام، يتحقق البقاء حتى لو كان الدخول قانونياً ولكن البقاء غير مسموح به، ويتحقق ذلك إذا استمر الجاني في التواجد داخل النظام بعد انتهاء المدة المسموح بها للبقاء، يكفي هذا البقاء لتحقيق الركن المادي، دون الحاجة إلى التقاط معلومات، يهدف المشرع من تجريم البقاء في النظام حماية النظام وكل مكوناته، بما في ذلك المعطيات المعالجة، والتي قد تتضمن أسرار الدولة الدفاعية، إذا نجح الجاسوس في الوصول إليها، فإن ذلك يعتبر تجسساً يمس بأمن الدولة الجزائرية، سواء كان هدفه الاستحواذ عليها، أو تسليمها للدولة الأجنبية المعادية للجزائر، أو تدميرها.

- **الركن المعنوي**

تعد جريمة الدخول أو البقاء في النظام من الجرائم العمدية، حيث يقوم الجاني بقصد جنائي عام، والذي يتطلب أن يكون على علم بأنه غير مسموح له بالدخول أو البقاء داخل النظام، وأن ذلك يتعارض مع إرادة مالك النظام أو المسؤول عنه، وعلى الرغم من ذلك، يقوم الجاني بالتصرف بطريقة مخالفة للقانون ومخالفة لإرادة صاحب النظام، وتنص القوانين

[1] عماد مجدي عبد الملك، جرائم الكومبيوتر والانترنت .الإسكندرية دار المطبوعات الجامعية،2011، ص 43.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص 63.

الجزائرية على أن الدخول أو البقاء داخل نظام المعالجة الآلية للبيانات بطريقة غش يعتبر غير مشروع، ولذا يتعين على الشخص المتورط أن ينسحب فوراً، فإذا استمر في التواجد داخل النظام فإن فعله يُعتبر جريمة قابلة للمحاسبة، وعلى الرغم من وجود آراء قانونية تخالف هذا الرأي وتعتبر الدخول بسبب الصدفة أو السهو أو الخطأ فعلاً مشروعاً وغير قابل للمحاسبة، إلا أن الرأي السائد يعتبر الدخول بسبب الصدفة أو السهو أو الخطأ فعلاً غير مشروع وقابل للمحاسبة [1].

ويمكن القول إزاء ذلك أن هذا الدخول أو البقاء سهوا أو خطأ أو صدفة إذا كان يتعلق بنظام معالجة آلية لأسرار الدولة

الدفاعية أو العسكرية فإنه يفترض أن يعتبر غير مشروع، ب الاعتداء على سلامة المعطيات في نظام المعالجة الآلية للمعطيات جاء في نص المادة 394 مكرر 1 من قانون العقوبات الوطني أنه يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"، ليتضح من ذلك أن الجريمة تقوم على ركن مادي ومعنوي، نفصل فيهما كما يلي:

تتألف الجريمة من التغيير في البيانات الموجودة في نظام المعالجة الآلية للبيانات عن طريق الغش، ويحدث هذا التغيير من قبل مجرم غير مرخص له بالوصول إلى النظام، سواء من خلال الإدخال أو التعديل أو المحو أو الإزالة، يكفي لتحقيق الجريمة قيام المتهم بأحد هذه الأفعال، [2] يُقصد بالإدخال، وفقًا للفقه، إضافة معطيات جديدة على الدعامة الخاصة بها، سواء كانت فارغة أم كانت تحتوي بالفعل على معطيات، أو تغذية النظام بالمعلومات المراد معالجتها أو بالتعليمات اللازمة لعملية المعالجة، أما التعديل، فيشير إلى

[1] عبد الفتاح بيومي حجازي، مرجع نفسه، ص ص 63.

[2] Eric A.Capriolisystem de traitement automatiser de données .*revue jurisclasseu*. Yves Mayaud . 2011 .*code penal*.Paris: dalloz.

استبدال المعطيات الموجودة في النظام بمعطيات أخرى، ومن المحو أو الإزالة، يُفهم إزالة جزء من المعطيات المسجلة على الدعامة والموجودة في النظام، أو تحطيم تلك الدعامة، أو نقل أو تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة،[1]

يُقصد بالإدخال، وفقًا للفقه، إضافة معطيات جديدة على الدعامة الخاصة بها، سواء كانت فارغة أم كانت تحتوي بالفعل على معطيات، أو تغذية النظام بالمعلومات المراد معالجتها أو بالتعليمات اللازمة لعملية المعالجة، أما التعديل، فيشير إلى استبدال المعطيات الموجودة في النظام بمعطيات أخرى، ومن المحو أو الإزالة، يُفهم إزالة جزء من المعطيات المسجلة على الدعامة والموجودة في النظام، أو تحطيم تلك الدعامة، أو نقل أو تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

- **التعامل في معطيات غير مشروعة**

قد حدد المشرع الجزائري جريمة التعامل مع بيانات غير مشروعة في المادة 394 مكرر 2 من قانون العقوبات الجزائري، والتي تنص على ما يلي: "يُعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة تتراوح بين 1,000,000 دينار جزائري و5,000,000 دينار جزائري، كل من يقوم عمدًا وبطريقة مخادعة بأي من الأفعال التالية":

يمكن تنفيذ الجرائم المذكورة في هذا القسم عن طريق تصميم أو بحث أو تجميع أو توفير أو نشر أو التجارة في البيانات المخزنة أو المعالجة أو المرسلة عبر نظام معلوماتي.

حيازة أو إفشاء أو نشر أو استخدام البيانات التي تم الحصول عليها من إحدى الجرائم المذكورة في هذا القسم لأي غرض.

يتضح من المادة أن جريمة استغلال البيانات المعالجة عبر نظام آلي للبيانات تأتي على شكلين، ويمكن توضيحهما كما يلي.

[1] إلهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزور .باتنة: جامعة الحاج لخضر،2016، ص 41.

**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 الماسة بأنظمة المعالجة الآلية للمعطيات**

تقوم هذه الجريمة على ركنين مادي ومعنوي، يتمثل الركن المادي في قيام الجاسوس بإنتاج أو تصميم أو اختراع أو بحث أو تجميع أو توفير أو نشر أو بيع أو شراء معطيات معلوماتية، سواء كانت مخزنة أو معالجة أو مرسلة عبر نظام معلوماتي، مما يسمح بارتكاب الجرائم التي تستهدف أنظمة المعالجة الآلية للبيانات، مثال على ذلك هو تصميم الجاسوس لكود أو شفرة تمكنه من الدخول إلى النظام والاطلاع على معلومات سرية تتعلق بدفاع الدولة الجزائرية، ثم إتلافها أو تغييرها أو تسليمها لدولة معادية.

أما الركن المعنوي، فيقوم على القصد العام، حيث يتجه إرادة الجاني نحو ابتكار أو توفير أو البحث عن معطيات أو الاتجار فيها مع علمه بكافة عناصر الجريمة، بالإضافة إلى قصد جنائي خاص يتمثل في ارتكاب أحد الجرائم التي تمس أنظمة المعالجة الآلية للبيانات، إذا كان هدف الجاني هو حماية الأنظمة الآلية فنياً دون نية ارتكاب جرائم، فلا جريمة عليه، اتفاقية بودابست تشترط أن يكون ارتكاب هذه الأفعال بنية ارتكاب الجرائم المعلوماتية[1].

**2 - حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**

تتضمن هذه الصورة ركنًا ماديًا وركنًا معنويًا، يتطلب الركن المادي وجود معلومات معلوماتية غير مشروعة بحوزة الجاني، وأن يقوم بإبقائها لديه أو إفشائها أو نشرها أو استخدامها، يعكس هذا الركن نية الجاني في الاستفادة من هذه المعلومات غير المشروعة.

[1] محمد خلّفة،دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلّة للمعطّات، في قانون العقوبات الجزائري .المجلة النقدية للقانون والعلوم السياسية،2018.

أما الركن المعنوي، فيتطلب قصدًا جنائيًا عامًا يتمثل في إرادة الجاني لحيازة أو إفشاء أو نشر أو استخدام المعلومات غير المشروعة، مع علمه بطبيعتها غير المشروعة وتأثيرها الضار، يهدف هذا التجريم إلى تضييق نطاق الأشخاص الذين يمكنهم الاطلاع على هذه المعلومات وتقليل انتشارها.

على سبيل المثال، إذا حصل الجاني على كلمة مرور عن طريق ارتكاب جريمة غير مصرح بها في نظام المعالجة الآلية للمعلومات، وقام بحيازتها أو نشرها أو إفشائها أو استخدامها لصالح دولة معادية للجزائر، فإنه يتحمل المسؤولية الجنائية عن هذا الفعل.

**ثانيا: التجسس المرتكب بواسطة أنظمة الاتصالات**

أصبح الحديث عن التجسس عبر البريد الإلكتروني والهاتف وغرف الدردشة شيئاً من الماضي، حيث تعتمد الدول المتقدمة الآن على أساليب أكثر تطوراً ونجحت في تطويرها إلى درجة تستطيع بها اختراق كافة حواجز أسرار الدول دون أن يتم رصد هذا الاختراق، هذه الأساليب متنوعة وكثيرة، ولكن سنناقش أهمها في النقاط التالية.

**1-التجسس بواسطة الأقمار الصناعية**

تستخدم الدول العظمى الأقمار الصناعية لمراقبة العالم، حيث يوجد حوالي 500 قمر صناعي عسكري تابع لها، تمتلك الولايات المتحدة الأمريكية 50 منها، وتكلفتها ليست عالية وتعمل لمدة تصل إلى سنة واحدة، تدعي هذه الدول أن الأقمار التي أطلقتها هي أقمار مدنية وليست عسكرية، بهدف إيهام العالم بأن استخدامها يقتصر على الأغراض المدنية داخل حدودها وأنها لن تستخدمها للتجسس على الدول الأخرى، ومع ذلك، تستخدم هذه الأقمار في الحروب لمراقبة الأعداء على مدار 24 ساعة والتعرف على إمكاناتهم واستعداداتهم للحرب، وعلى الرغم من أن القوانين تحظر إطلاق أقمار صناعية عسكرية

لأغراض التجسس في القضاء، إلا أن الواقع يشير إلى استخدامها في هذا السياق، [1]، تسمح هذه الطرق باكتشاف نقاط داخل المناطق التي تتعرض للمراقبة المكثفة، ويمكنها الرؤية تحت السحب وفي الليل، بالإضافة إلى اكتشاف التحركات تحت سطح الأرض، تعتبر الأقمار الصناعية أخطر وسيلة للتجسس نظرًا لأنه من الصعب تجنب التجسس بها، نظرًا لأن هذه التكنولوجيا متخصصة في قلة من الدول المتقدمة فقط، وصعوبة تفادي الكشف عن هذه الأقمار بسبب استفادتها من حرية الملاحة الفضائية، الفضاء الخارجي لا يخضع لسيادة دولة معينة، وبالتالي لا يمكن استخدام مفهوم السيادة لإلغاء عمل هذه الأقمار. [2]

**2- التجسس بواسطة أجهزة البوليمرات**

تُصنع أجهزة البوليمرات من نوع خاص من "البوليمرات" التي طورها باحثون في الجمعية الكيميائية الأمريكية، تتميز هذه البوليمرات بقدرتها على تدمير نفسها ذاتيًا والاختفاء تمامًا دون ترك أي أثر بعد إتمام مهمتها السرية، يمكن استخدامها في تصنيع أجهزة الاستشعار والتجسس الإلكترونية التي تُلقى في مناطق العدو لجمع وتخزين المعلومات، ثم تدمر نفسها وتختفي كأنها لم تكن موجودة أصلاً، على عكس المواد البلاستيكية التي تتحلل ببطء على مدار عام، تختفي هذه المادة في لحظات عندما تتلقى أمر التدمير الذاتي.

**3- التجسس بواسطة الطائرات المصغرة المسيرة "ميكرو دورن سوارم"**

في يناير 2017، أعلنت وزارة الدفاع الأمريكية نجاح أول تجربة لمنظومة جديدة طورها مكتب القدرات الإستراتيجية، حيث أُطلق سرب ذكي من الطائرات المسيرة المصغرة من على متن ثلاث طائراتF/A-18 Super Hornets ، استخدمت التجربة 103

[1] طه الراوي. 28 فيفري 2020 كيف غيرت التكنولوجيا أساليب التجسس.تاريخ الاسترداد 14-05-2024 . https://www.noonpost.com/content/36070.

[2] سلامي نادية، التجسس الإلكتروني كأثر للاستخدام غير المشروع للفضاء الإلكتروني على أمن الدولة الخارجي، مجلة دراسات، 2017

طائرات مصغرة تُدعى"Perdix" ، تتحرك بشكل مشابه للأسراب الحية في الطبيعة، وتتواصل مع بعضها ضمن عقل مركزي لصناعة قرار جماعي بعد جمع المعلومات الميدانية عبر المجسات الخاصة، هذا النظام المستقل يقلل من الحاجة للتوجيه البشري المباشر، مما يعزز ريادة الولايات المتحدة في مجال الأنظمة ذاتية التحكم، ويميز الطائرات المسيرة بقدراتها الاستطلاعية وصغر حجمها الذي يسمح لها بالإفلات من أنظمة الرصد الرادارية واختراق موجات الاتصالات للقوات المعادية، [1]

**4-التجسس بواسطة تقنية البيوبوت**

تتمثل تقنية البيوبوت في استغلال العناصر الطبيعية الموجودة في الحياة وتطويرها تكنولوجيًا لأداء مهام متنوعة تعود بالنفع على البشرية، هذا التطور يؤدي إلى إنشاء ما يُعرف بالكائنات الحية الآلية أو "البيوبوتس"، والتي تتكون من كائنات حية تُدار إلكترونيًا، أي أن أنظمتها العصبية مرتبطة بتقنيات متقدمة وخوارزميات لتنفيذ مجموعة واسعة من المهام، بما في ذلك الصراصير الجواسيس، فكرة هذه الصراصير تعود إلى الباحثة "هونغ ليانغ" من جامعة تكساس، التي اختارت الصراصير المنتشرة في أمريكا اللاتينية لأنها متوفرة بكثرة ولديها قدرة عالية على الشفاء السريع، بالإضافة إلى حجمها الكبير وحركتها البطيئة، مما يجعلها مثالية لحمل حقائب مزودة بتقنيات متطورة يمكن استخدامها في مجالات التجسس وغيرها، كما يتم استخدام اليعسوب في التجسس أيضًا، حيث تساعده عضلاته الموجودة تحت أجنحته على الطيران، وبفضل التيار الكهربائي، يمكن التحكم في تحركاته

[1] بلال العضايلة 02 نوفمبر 2019 كيف تحسم التكنولوجيا العسكرية الحروب قبل بدايتها .تاريخ الاطلاع 20 أوت 2024 على الساعة 18:00 من https://strategiecs.com/ar/analyses/how-can-military-technology-be-the-decisive-factor-in-wars-before-their-eruption

للطيران والهبوط وتغيير اتجاهه يمينًا أو يسارًا أثناء الطيران دون المخاطرة بفقدان توازنه، حيث تضمن التقنيات المستخدمة الحفاظ على توازنه بكفاءة، [1]

**خلاصة الفصل:**

يتضح من خلال هذا الفصل أن التجسس السيبراني يمثل تهديدًا كبيرًا للأمن القومي للدول، وذلك بسبب قدرته على اختراق الأنظمة وجمع معلومات حساسة بطرق غير قانونية، يتطلب التصدي لهذا النوع من الجرائم تطوير استراتيجيات قانونية وتقنية فعالة لحماية الفضاء السيبراني وضمان سلامته.

[1] طه الراوي، مرجع السابق، ص 26.

# الفصل الثاني:

# الاليات الردعية  للتجسس السيبيراني الماس بأمن الدولة

في عصرنا الرقمي المتسارع، يشكل الأمن السيبراني محوراً أساسياً لضمان استقرار الدول وحمايتها من التهديدات الخارجية والداخلية. التجسس السيبراني، باعتباره أحد أخطر التهديدات، يستهدف اختراق الأنظمة الإلكترونية الحكومية والعسكرية والاقتصادية لجمع معلومات حساسة واستغلالها للإضرار بمصالح الدول. للرد على هذا التهديد، تتطلب الدول وضع آليات ردعية فعالة تتضمن استراتيجيات عملياتية وقانونية.

يتناول الفصل الثاني من هذا البحث الآليات الردعية لمواجهة التجسس السيبراني الذي يهدد أمن الدولة. يبدأ المبحث الأول باستعراض الآليات العملياتية لردع التجسس السيبراني، حيث يتم التركيز على الأجهزة المختصة بالأمن السيبراني على المستويين الوطني والدولي، ثم الانتقال إلى الاستراتيجيات الأمنية المتبعة لمكافحة التهديدات السيبرانية، والتي تشمل جهود التعاون الدولي والوطني.

في المبحث الثاني، يتم مناقشة الآليات القانونية والتحديات التي تواجه تحقيق الأمن السيبراني، يتم التطرق إلى الآليات القانونية العامة والخاصة لردع جريمة التجسس عبر الإنترنت، بالإضافة إلى استعراض معيقات تحقيق الأمن السيبراني في الجزائر، وتقديم رؤية مستقبلية لتعزيز هذا الأمن في ظل التحديات الأمنية المتزايدة.

# المبحث الأول: الاليات العملياتية لردع التجسس السيبيراني

يتناول المبحث الأول الآليات العملياتية لردع التجسس السيبراني، حيث يركز المطلب الأول على الأجهزة العملياتية المختصة في الأمن السيبراني، بينما يتناول المطلب الثاني الاستراتيجيات الأمنية لمكافحة التهديدات السيبرانية.

## المطلب الأول: الأجهزة العملياتية المختصة في الأمن السيبراني

يتناول المطلب الأول الأجهزة العملياتية المختصة في الأمن السيبراني، حيث يستعرض الفرع الأول الأجهزة على المستوى الوطني، بينما يركز الفرع الثاني على الأجهزة على المستوى الدولي.

### الفرع الأول: على المستوى الوطني

**1- مركز الوقاية من جرائم الإعلام الآلي لدرك الوطني:**

تم إنشاء هذا المركز في بئر مراد رايس عام 2008 كجهاز يهدف إلى تعزيز أمان وأمان نظام المعلومات وخدمة الأمن العام، يقوم المركز بتحليل البيانات والمعلومات المتعلقة بالجرائم الإلكترونية، ويسعى لتحديد هوية الجناة، سواء كانوا أفرادًا أو عصابات أو أطراف أخرى، [1]

يهدف هذا المركز إلى تقديم الدعم للأجهزة الأمنية الأخرى من خلال التعاون المشترك لمكافحة الجرائم السيبرانية، يركز المركز على تطوير استراتيجيات للتعامل مع هذه الجرائم ووضع تشريعات لتنظيم استخدام المعلومات، بالتنسيق مع وزارة العدل ومعهد متخصص في علم الجريمة لتحسين مستوى التعامل مع الجريمة بشكل عام والجريمة السيبرانية بشكل

[1] سمير بارة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني (Cyber Security) في الجزائر الدور والتحديات"، جامعة قاصدي مرباح، ورقلة ، ص 445.

خاص، تسعى الجزائر بجد للاستفادة من خبرات الدول الأخرى في تأمين النظم المعلوماتية وحمايتها من الجرائم، وذلك من خلال مجموعة من العناصر الرئيسية، أبرزها:

**الوقاية:** وتتضمن الحملة التوعوية والتثقيفية، التي تنفذ بالتنسيق مع وزارة التضامن الوطني والأسرة، تنظيم ملتقيات ومحاضرات وأيام دراسية ومنتديات دولية، والمشاركة في منتديات صحفية وبرامج تلفزيونية وإذاعية، بالإضافة إلى استخدام مختلف وسائل النشر والإعلان الأخرى.

– **المكافحة** تعزز الوعي الجزائري من خلال استخدام شبكات التواصل والإنترنت، حيث يعلق المواطنون بشأن القضايا المحلية ويعرفون الأخطار المتعلقة بالسلوكيات المشبوهة أو الاعتداءات التي قد تظهر على شكل فيديوهات منشورة على الإنترنت، هذا النشاط يسهل التحقيق والتعامل مع الجهات المختصة للقبض على المشبوهين والمجرمين في الوقت المناسب، [1]

**2– المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:**

يعتبر هذا المعهد واحدًا من المشاريع التي تم تنفيذها في إطار تطوير قطاع الدرك الوطني بوشاوي، تم إنشاؤه بموجب مرسوم رئاسي مؤرخ في 26 جوان 2004، وبدأ العمل به رسميًا في الأول من جانفي 2009، وقد كانت الفترة بين عامي 2004 و2009 مخصصة لتدريب الموارد البشرية وتجهيز المعهد بالمعدات والتقنيات الضرورية، يقوم المعهد

[1] سهام بو عموشة، " الفضاء السبراني يتميز بانفتاح شبكة المعلوماتية وانعدام الحواجز الجغرافية"، جريدة الشعب، العدد 17، 24 ماي 2024، الكويت، ص06.

بأداء مهام عديدة تلبي احتياجات السلطة القضائية وضباط الشرطة القضائية والجهات المؤهلة قانونيًا، خاصة أثناء التعامل مع القضايا المعقدة، "[1]

**مصلحة الاعلام الآلي :**

تابع لإدارة البحث الجنائي والتحليل الجنائي في الدرك الوطني، وعلى مستوى هذا التابع، يتم تتبع ومراقبة ورصد عمليات اختراق واختراق الأمن السيبراني، واكتشاف البيانات المسروقة وتحليل البرمجيات الخبيثة، ومن بين مهام هذا التابع ما يلي: [2]

يعمل على إكمال نظام الاتصال الآلي عبر شبكة تربط مختلف وحدات وهياكل الدرك الوطني، والتي تمكن من نقل المعلومات بسرعة وسهولة بين الوحدات أفقيًا وعموديًا، هذا يسهل على المحققين التحري بفعالية حول الجرائم وتتبع المشتبه بهم.

يتم العمل على تنظيم هياكل ووحدات متخصصة في ممارسة الشرطة القضائية بطريقة تعزز تخصصها، بما في ذلك إنشاء فرق متخصصة في مجالات مثل المخدرات والتزوير وجرائم الإعلام الآلي وغيرها من الجرائم المعقدة التي تقوم بها شبكات منظمة وتصنف على أنها إجرام منظم، [3]

**3 المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:**

تم إنشاء المصلحة المركزية لمكافحة الجريمة الإلكترونية في عام 2011 استجابةً لمتطلبات الأمن المعلوماتي ومكافحة التهديدات الأمنية الناتجة عن الجرائم الإلكترونية،

[1] نسيمة سحواذ،" الطموح لتوسيع دائرة الاعتماد المتبادل بإدراج طرق تحليلية لفائدة مخابر أخرى"، في 02 مارس // http Dikanews.com13:63/2024

[2] بارة سمير ، مرجع سابق، ص 436

[3] أحمد غاي، تكييف الشرطة القضائية مع متطلبات إصلاح العدالة، تقييم وآفاق"، في 03 مارس2024/14:13 w.w.w.mjustice.dg

عملت هذه المصلحة على تعديل الهيكل الأمني لمديرية الشرطة القضائية، وقد كانت هذه المصلحة في البداية عبارة عن وحدة صغيرة شكلت النواة الأولى لتشكيل أمني متخصص في مكافحة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني، [1]

أكدت مديرية الأمن في سياق موضوع الجرائم المستحدثة على ضرورة استعداد وجاهزية كافة وحدات جهاز الشرطة بتخصصاتها المختلفة لمواجهة الجرائم الجديدة المرتبطة بالمعلوماتية والشبكة العنكبوتية، وأشارت المديرية إلى أهمية تطوير أساليب مكافحة هذه الظاهرة العابرة للحدود، والمعروفة الآن باسم "الجريمة السيبرانية"، بهدف تشكيل جبهة أمنية فعالة للتصدي لهذه الآفة التي تتزايد خطورتها سنة بعد أخرى.

في المراحل الأولى من الأمن الوطني، كانت المؤسسات العامة تسعى لوضع خطط عمل لتعزيز يقظة جهاز الشرطة والمصالح المختصة في متابعة الجرائم المعلوماتية، هذا التقدم يرجع إلى استخدام وسائل وآليات التحكم في تكنولوجيا الإعلام والاتصال لقطع مسار هذا النوع من الجرائم، [2]

**4 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.**

نصت المادة 13 من القانون 09/04 الصادر في أغسطس إلى إنشاء هيئة وطنية متخصصة، وتنظيمها وكيفية عملها يتم تحديده عن طريق اللوائح التنظيمية، أما مهام هذه الهيئة فقد تناولتها المادة 14 من نفس القانون، وتتمثل في الوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، تشمل إجراءات الوقاية توعية مستخدمي هذه التكنولوجيات بمخاطر الجرائم التي قد يتعرضون لها أثناء التصفح أو الاستخدام، ومن أبرز هذه الجرائم:

[1] عبد القادر سعيدي المصلحة المركزية الالكترونية في مواجهة مجرمي العالم الافتراضي، في 03 مارس 17:42/2024 www.essalamonline.com

[2] – راضية مناد، تطوير قدرات الشرطة في مواجهة الجريمة الالكترونية ، أمن واستراتيجية 03 مارس www.dgayerinfo.com.21:19/2024

التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء، اختراق أنظمة الشركات والمؤسسات الرئيسية أو الجهات الحكومية، وغيرها.

**5-مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال** بحسب نص المادة 14 من القانون09/04 هناك نوعان من المكافحة تقوم بهما هذه الهيئة :

أ، تقديم الدعم للسلطات القضائية ووحدات الشرطة القضائية في إجراء التحقيقات المتعلقة بالجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات، بما في ذلك جمع المعلومات وإجراء التحليلات القانونية والفنية المطلوبة، (المادة 14، الفقرة (ب) من القانون 09/04)

أ- تبادل المعلومات مع الجهات المماثلة في الخارج بهدف جمع جميع البيانات الضرورية لتحديد المسؤولين عن الجرائم المرتبطة بتقنيات الاتصالات والمعلومات ومكافحتها[1] يقترح المشروع في هذا القسم إنشاء هيئة وطنية متخصصة تضطلع بمهام رئيسية، ومن بينها تنشيط وتنسيق عملية الوقاية من الجرائم المعلوماتية، وتقديم الدعم للسلطات القضائية ومصالح الشرطة القضائية في التحريات المتعلقة بهذه الجرائم، كما تقوم الهيئة أيضًا بجمع المعلومات من هيئاتها المماثلة في الخارج لمكافحة هذا النوع الخطير من الجريمة.[2]

[1] أحمد مسعود مريم آليات مكافحة جرائم تكنولوجيا الاعلام والاتصال في ضوء القانون رقم 09/04، رسالة ماجستير، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية قسم الحقوق 2012-2013)، ص 45-44

[2] الجريدة الرسمية، القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وطرق مكافحتها، الفترة التشريعية السادسة، السنة الثالثة الدورة الرابعة، رقم 122 ( 27 يونيو (2009)، ص 04

## الفرع الثاني: على المستوى الدولي

على المستوى الدولي، تنص المادة (16) من القانون (و) على أنه في إطار التحقيقات أو الاستقصاءات القضائية المتعلقة بالجرائم المشمولة بالقانون وكشف مرتكبيها، يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الإلكترونية المتعلقة بالجريمة، بهدف تبادل المعلومات بين الدول فيما يتعلق بالجريمة الإلكترونية وتحديد هوية الجناة ومواقعهم، تشارك الهيئة الجزائرية في الأعمال التحضيرية الضرورية مع الهيئات الدولية المماثلة لها، بهدف البحث والتعرف على الجرائم الإلكترونية ومرتكبيها وتحديد مواقعهم.

تسعى الجزائر لتعزيز تبادل المعلومات بين الدول، وتركز بشكل خاص على المنظمة الدولية للشرطة الجنائية، نظرًا لكونها أبرز جهاز دولي في مكافحة الجريمة، بما في ذلك الجرائم المعلوماتية، كما تعمل على تعزيز التعاون الدولي بين أجهزة الشرطة من خلال تعيين قائمة تضم ضباطًا مختصين في مجال البحث والتحري بشأن الجرائم المعلوماتية.

الدول يمكنها الاعتماد عليهم لتسهيل الإجراءات القضائية المتعلقة بتسليم الأشخاص المطلوبين، وتنفيذ الأوامر القضائية الدولية، بما في ذلك نشر أوامر القبض الدولية للمطلوبين والمطالبة بتسليمهم، [1]

من خلال التعاون الفعال بين دوائر الشرطة والمنظمة الدولية للشرطة الجنائية (الإنتربول)، تم تنظيم دورات تدريبية متعددة لموظفي الشرطة في العديد من البلدان، بالإضافة إلى تبادل المعلومات وإنشاء قواعد بيانات للصور وبرامج لتحديد هوية الضحايا، تم أيضًا إنشاء نظام لرصد "استغلال الأطفال" وغيرها من الإجراءات المماثلة، في إطار هذا

[1] – إيمان بن سالم جريمة التجنيد الالكتروني للإرهاب وفقا لقانون العقوبات الجزائري ، ( برلين، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية ، 2008)، ص 80

التعاون، تم استجابة البلدان التالية (روسيا، الولايات المتحدة، اليابان، اليونان، إسبانيا، أستراليا، ألمانيا، الإمارات العربية المتحدة، إندونيسيا، تونس، الجزائر، العراق، عمان، مصر، المغرب، قطر، سويسرا، البرتغال، إيطاليا وغيرها من الدول) لاستبيان وجهته الإنتربول، وذلك بهدف وضع قوانين وتطبيق عقوبات على مرتكبي استغلال الأطفال في المواد الإباحية عبر الإنترنت.[1]

## المطلب الثاني : الإستراتيجيات الأمنية لمكافحة التهديدات السيبرانية

يتناول المطلب الثاني الاستراتيجيات الأمنية لمكافحة التهديدات السيبرانية، حيث يركز الفرع الأول على الاستراتيجيات على المستوى الدولي، بينما يستعرض الفرع الثاني الاستراتيجيات على المستوى الوطني.

### الفرع الأول: على المستوى الدولي

نتطرق من خلال هذا الفرع إلى الندوة الدولية حول الأمن السيبراني في الجزائر (أولا)، ثم نتطرق إلى إستراتيجية التعاون الدولي للوقاية من الجرائم السيبرانية (ثانيا)

**أولا: الندوة الدولية حول الأمن السيبراني في الجزائر**

اعتمدت الجزائر نهجًا شاملًا يجمع بين الأمن الوطني والأمن السيبراني لمكافحة الجرائم السيبرانية التي تتجاوز الحدود، يتضمن هذا النهج التعاون العملي لفهم أفضل للتحديات الكبيرة على المستوى العالمي، خاصة في ظل تزايد التهديدات الأمنية الإلكترونية والأضرار الجسيمة الناتجة عنها، مثل الاختراقات الأمنية التي ضربت العديد من الدول وأثرت على أمنها واستقرارها وبنيتها التحتية.

[1] نجاة معلا مجيد تعزيز وحماية جميع حقوق الانسان بما في ذلك الحق في التنمية"، الجمعية العامة، الأمم المتحدة، الدورة الثانية عشر، البند 03 من جدول الأعمال، ص 24

في شهر مايو 2016، نظمت الجزائر ندوة دولية حول الأمن السيبراني، حضرها أكثر من 15 دولة وأكثر من 50 خبيرًا دوليًا في مجال الأمن السيبراني، تمت مناقشة حالة التطور التكنولوجي والتشريعات المتعلقة بالفضاء السيبراني، بالإضافة إلى السياسات المتعلقة بالأمن السيبراني وأمن المنشآت الحساسة والوقاية من جرائم الإنترنت ومكافحتها.

توصل الخبراء المشاركون في الندوة إلى ضرورة إقامة تعاون حقيقي بين الدول لمكافحة الجريمة الرقمية التي تؤثر على الأفراد والمؤسسات على حد سواء، تم التأكيد على أهمية تبادل المعلومات وتطوير إجراءات مشتركة للتصدي للتهديدات السيبرانية وحماية البنية التحتية الحيوية والمعلومات الحساسة.[1]

شهد هذا الملتقى مشاركة خبراء عسكريين ومدنيين في مجال الأمن والدفاع السيبراني، وكانت فرصة للمشاركين لتبادل الخبرات والمعارف، ومناقشة التطورات والمستجدات في هذا المجال من خلال محاضرات وورش عمل تطبيقية تقدم نظرة شاملة عن "التهديدات السيبرانية"، بالإضافة إلى استعراض التشريعات المتعلقة بالفضاء السيبراني، ومن المتوقع أن تسفر هذه المناقشات عن توصيات فيما يتعلق بإدارة الأزمات السيبرانية وتعزيز استراتيجية الدفاع الوطني لمكافحة التهديدات السيبرانية، "[2]

**ثانيا: إستراتيجية التعاون الدولي للوقاية من الجرائم السيبرانية**

ممثلو قادة الجيوش الأمريكية والفرنسية والكندية أكدوا أن الفضاء السيبراني يشكل خطرًا على مؤسسات الدول وبنيتها الحساسة، وأنه يعتبر الوسيلة المفضلة للجماعات

[1] – مصطفى عباني، التدابير الأخرى في مجال نزع السلاح والأمن الدولي، اللجنة الأولى للدورة الـ 71 الجمعية العامة للأمم المتحدة، بعثة الجزائر الدائمة لدى الأمم المتحدة، نيويورك، 24 أكتوبر 2016، ص 02.

[2] – سليمة مقراني الجيش الوطني الشعبي : ملتقى حول الدفاع السيبراني، مكون أساسي للأمن والدفاع الوطني في 07 مارس

hltps:www.eljoumhouria.dg. 17:51/2024

الإرهابية لاستهداف وجذب أعداد كبيرة من الشباب والنساء، وشددوا على أهمية تعزيز الحصانة الأمنية لمؤسسات الدول ضد "الإرهاب الإلكتروني".

**كندا:** حيث ذكر ممثلها على هامش الندوة التي نظمتها قيادة الدرك الوطني حول الجريمة المعلوماتية، أن الإنترنت والخدمات الإلكترونية وفرت مجالاً واسعاً للجماعات المتطرفة والعنيفة، حيث أتاحت لهم فرصاً للنشر والتواصل بطرق لم تكن متاحة سابقاً للتنظيمات الخارجة عن القانون، كما أصبحت مواقع التواصل الاجتماعي مثل "فيسبوك" وسيلة لتجنيد الإرهابيين والتنظيمات الإرهابية.

**فرنسا:** من جانبها، أكد اللواء مارك وتين أو غوراد، ممثل الجيش الفرنسي، أن الجرائم الإلكترونية أصبحت الآن عابرة للحدود، وبناءً على ذلك، فإنه يتعين على جميع الدول العمل بطريقة دقيقة وذكية لمواجهتها، واقترح استقطاب المخترقين المؤسسات والبنوك، المعروفين بـ "الهاركرز"، واستخدامهم في مجال تأمين المؤسسات، حيث يعتبرون من الأشخاص الذكياء والماهرين في هذا المجال.

**الولايات المتحدة الأمريكية:** أشار اللواء جون بول باليميروا، ممثل الولايات المتحدة في الندوة، إلى أن الجرائم الإلكترونية تُعَد من أخطر التهديدات التي تواجه دول العالم، حيث تؤثر على أمنها واستقرارها، وأوضح أن هذه الجرائم تُعتبر إحدى وسائل الإرهاب، حيث يتم استخدامها لاختراق المؤسسات العامة والحيوية."[1]

[1] عبد الرحمان بن حمادي الفضاء الأزرق أصبح مكانا مثاليا للقيام بأعمال غير مشروعة"، معرض الصحافة تجزئة سعيد بن حداد الشراقة ، الجزائر 25 ماي 2016، ص 4-5.

## الفرع الثاني: على المستوى الوطني

### أولا: اليقضة الإسراتيجية التابعة لمركز الوقاية

تُعد مهمة المسؤولين عن إستراتيجيات مطاردة وتتبع ورصد جميع أشكال المخالفات والجرائم التي تتم عبر شبكة الإنترنت، مثل التهديدات والإبتزاز والقرصنة المعلوماتية والتحرش وسرقة الهوية وإنتحال الشخصية وعرض المنتجات الممنوعة للبيع عبر المواقع التجارية والدعاية المغرضة والإرهاب، لمكافحة هذه الجرائم المعلوماتية، يتم وضع إستراتيجيات لمراقبة الإنترنت والتعامل مع الجهات المختصة ومعاقبة المتهمين، [1]

**اليقضة الأمنية** : بفضلها، يُمكن متابعة تطور الإحرام وأساليبه بصفة عامة، والخطط العملية التي ينتهجها المحرمون لتحضير وتجنيد الأفراد بشكل أفضل، وتوفير الوسائل لمواجهة هذا النوع من الجرائم.

**اليقضة التكنولوجية والعلمية** : تتمثل المهمة في جمع المعلومات والبيانات التي تساعد على متابعة التطورات والابتكارات في المجالات التكنولوجية والعلمية، والتي تهم قوى الأمن بمختلف أنواعها بما في ذلك الدرك الوطني والجيش الوطني.

**3 اليقضة الإجتماعية** وتتولى متابعة التحليل والدراسات المختلفة المتعلقة بالمجتمع وتطوراته، والمعايير التي تحكمها وعلاقتها بالأمن العام.

**4 اليقضة القانونية** : تركز على متابعة التطورات في المجال القانوني والنصوص التشريعية المتعلقة بمختلف المهام والنشاطات المتصلة بمهام الدرك الوطني، خاصة فيما يتعلق بحفظ الأمن العام.

[1] إسماعيل جنة حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون"، مجلة الجيش ، العدد 599 جوان 2013، ص14.

**5 اليقضة الاقتصادية** تركز على الجوانب الاقتصادية وتطورات السوق الوطنية والدولية، وتهدف إلى حماية المصالح في سياق توقيع العقود أو اتفاقيات الشراكة الاقتصادية، بعد هذه الاستراتيجيات، يُعد تقرير تقني يُرسل إلى قيادة الدرك الوطني التي تقوم بدورها بنشره وتوزيعه على المستوى المركزي (مثل الهيئات التابعة لقيادة الدرك الوطني وقيادة مجموعات حرس الحدود)، أو المستوى الجهوي (مثل المجموعات الإقليمية والقيادة الجهوية لحرس الحدود)، أو المستوى المحلي (مثل الكتائب وفصائل البحث والتحريات).[1]

**ثانيا: إستراتيجية حفظ النظام والأمن العموميين**

أكد قائد سلاح الدرك الوطني، اللواء مناد نوبة، في كلمته خلال افتتاح الندوة الدولية حول الأمن السيبراني بعنوان "الفضاء السيبراني: رهانات وتحديات"، على ضرورة وضع خطط استراتيجية لمكافحة الجريمة المعلوماتية والمنظمة بكافة السبل، وأوضح أن مؤسسة الدرك الوطني تضطلع بمهام الأمن العام، وتوفر لتحقيق ذلك وسائل متقدمة في مجالات الشرطة العلمية والتقنية والخبرة الجنائية، وأكد أن الجهاز يعمل على حفظ النظام والأمن العام من خلال اتخاذ إجراءات وقائية عبر الرصد المستمر، كما يضمن الأمن العام بحماية الممتلكات وحرية التنقل عبر وسائل الاتصال، ويحرص على التطبيق الدائم للقوانين والأنظمة ضمن نطاق الوطن

**ثالثا: إستراتيجية إنشاء تشريعات جديدة متعلقة بالتهديدات السيبرانية:**

نظرًا لتزايد الجرائم الإلكترونية، دعا السيد مناد نوبة إلى وضع تشريعات جديدة لكشف المجرمين وملاحقتهم وتشديد الرقابة على الأجهزة الحكومية والشركات والبنوك، كما أكد على ضرورة حماية الأفراد من أن يكونوا ضحايا لهؤلاء المجرمين، وأشار إلى أن تجريد الفعل

[1] – إسماعيل جنة حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون، المرجع السابق، ص 15.

الإجرامي من شكله المادي يتطلب من الدرك إنشاء هيكل تنظيمي جديد وتوفير وسائل مناسبة وإجراءات عملية فعالة، وذلك ضمن نهج شامل للحد من انتشار الجرائم الإلكترونية وتحديد طبيعتها المتغيرة، وأشار إلى أن هذه الجرائم تشكل تهديدًا حقيقيًا لأمن الدولة من خلال محاولات اختراق المؤسسات الحكومية الحيوية وسرقة البيانات والتجسس والتأثير على النظام العام.

**رابعا: إستراتيجيات الدفاع السيبراني ومراقبة الأنظمة:**

قررت القيادة العليا للجيش إنشاء قسم الدفاع السيبراني ومراقبة أمن الأنظمة ضمن هيكل دائرة الاستخدام والتحضير لأركان الجيش، يهدف هذا القسم إلى تأمين وحماية المنظومات والمنشآت الحيوية في الجزائر من التهديدات السيبرانية والإرهاب الإلكتروني والتجسس على أسرار الدولة.

من خلال إنشاء قسم الدفاع السيبراني ومراقبة الأنظمة، سيتم تغطية جميع الجوانب المتعلقة بتحقيق نظام دفاعي شامل وفعال لحماية المنظومات والمنشآت الحيوية والحساسة في الجزائر من التهديدات السيبرانية والإرهاب الإلكتروني وإحباط أي محاولة للتجسس على أسرار الدولة.

ومن بين المهام الرئيسية لقسم الدفاع السيبراني ومراقبة الأنظمة تشمل:

تتضمن مهام المصلحة المتعلقة بالدفاع السيبراني ومراقبة الأنظمة تخطيط وتنفيذ ومتابعة النشاطات التي تتمثل في تطبيق السياسة الشاملة للدفاع السيبراني، والتي تهدف إلى ضمان فعالية الحماية ضد التهديدات السيبرانية الموجهة لأنظمة المعلومات والإتصالات ومنظومات الأسلحة للجيش، أهم محاور إستراتيجية الدفاع السيبراني للجيش تشمل:

1. يتعين تنظيم الجانب الوظيفي والتنظيمي لضمان تنفيذ أعمال الدفاع السيبراني بطريقة متناسقة وفعالة ضمن إطار وظيفي أو تنظيمي متكامل، مما يضمن تجانسها وفاعليتها.
2. يتم تكليف الجانب القانوني بتحسين وتعزيز بشكل مستمر الإطار القانوني المتعلق بالاستخدامات الشاملة لتكنولوجيا المعلومات والاتصالات، وتأمين أنظمة المعلومات بشكل خاص.
3. يشكل جانب الموارد البشرية هدفًا أساسيًا، حيث يتطلب وجود مورد بشري تقني متميز وذو كفاءة عالية في مجال الدفاع السيبراني، لضمان نجاح دمج هذا المجال في الأنشطة التشغيلية وإدارة الجيش.
4. تكليف الجانب التقني بتعزيز وتعديل القدرات التقنية للحماية والكشف والرد على الهجمات السيبرانية بشكل دائم، مع الحفاظ على يقظة مستمرة فيما يتعلق بالأساليب والوسائل المستخدمة من قبل المهاجمين.
5. الجانب الوقائي يتعلق بحماية وتوعية مستخدمي الجيش الوطني الشعبي من المخاطر والتهديدات التي تنشأ نتيجة استخدام تكنولوجيا المعلومات والاتصالات سواء في السياق المهني أو الشخصي بشكل دائم.
6. يتمثل جانب البحث والتطوير في استخدام وسائل تقنية متخصصة وشخصية من قبل هياكل البحث والتطوير للجيش الوطني الشعبي، وخاصة تلك المستخدمة لتعزيز الحماية ضد التهديدات السيبرانية، وهو عنصر حيوي في استراتيجية الدفاع السيبراني.
7. تهدف جهود تعزيز التعاون إلى تمكين القوات الجزائرية من الاستفادة من خبرات الدول الشريكة ومن الوسائل التكنولوجية المتقدمة بشكل كبير.[1]

[1] نوارة باشوش الجيش يدخل الحرب الفضاء الالكتروني في: 8 أفريل 2024 www.ehoroukonline.com

**خامسا: إستراتيجيات المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني**

1. سعت المديرية العامة للأمن الوطني إلى وضع خطط عمل ميدانية لتعزيز يقظة الجهاز والمصالح المختصة في مجال مكافحة الجريمة المعلوماتية، باستخدام وسائل وآليات التحكم في تكنولوجيا الإعلام والاتصال.
2. تم إنشاء ندوات أمنية لتسليط الضوء بشكل أكبر على الجرائم المستجدة، وخاصة في السياق الجزائري، حيث تمثل فرصة لتبادل الخبرات والأفكار مع المتخصصين لفهم هذه الظاهرة بشكل شامل.
3. قامت المديرية العامة للأمن الوطني ببرمجة دورات تكنولوجية متقدمة حول موضوع "الوقاية السيبرانية"، تهدف هذه الدورات إلى تزويد المشاركين بالمعرفة والمهارات اللازمة في مجال مكافحة الجريمة الإلكترونية ومواكبة تطورات التكنولوجيا، تشمل هذه الدورات تدريب فرق المحققين في الشرطة على استخدام التقنيات الحديثة والتحكم فيها، بالإضافة إلى تعريفهم بالأساليب المعتمدة دوليًا في الوقاية والمكافحة للجرائم الإلكترونية الهدامة.

وضع خطط إستراتيجية في المجال الوقاية والتحسس من هذه الجرائم الناجمة عن سوء استعمال الشبكات العنكبوتية خاصة من طرف الشباب والأطفال باللجوء إلى العمل الإستباقي لإزالة الأخطار المحتملة وحماية الأفراد والمجتمع من هذا النوع من الجرائم

## المبحث الثاني: الاليات القانونية ومعيقات تحقيق الامن السيبيراني

يتناول المبحث الثاني الآليات القانونية ومعيقات تحقيق الأمن السيبراني، حيث يتمحور المطلب الأول حول الآليات القانونية لردع جريمة التجسس عبر الإنترنت، ويتضمن الفرع الأول الآليات القانونية العامة مثل قانون العقوبات، بينما يركز الفرع الثاني على الآليات

القانونية الخاصة. أما المطلب الثاني فيسلط الضوء على معيقات تحقيق الأمن السيبراني الجزائري في ظل التحديات الأمنية والمستقبلية، ويشمل الفرع الأول معيقات تحقيق الأمن السيبراني الجزائري، ويقدم الفرع الثاني رؤية مستقبلية للأمن السيبراني الجزائري.

## المطلب الأول : الاليات القانونية لردع جريمة التجسس عبر الانترنت

يتناول المطلب الأول الآليات القانونية لردع جريمة التجسس عبر الإنترنت، حيث يُستعرض في الفرع الأول الآليات القانونية العامة مثل قانون العقوبات، بينما يُركز الفرع الثاني على الآليات القانونية الخاصة.

### الفرع الأول: الاليات القانونية العامة (قانون العقوبات)

تنص المادة 64 من قانون العقوبات على أن يُعاقَب بالإعدام كل أجنبي يرتكب التجسس، بموجب ما هو منصوص عليه في الفقرات 2 و 3 و 4 من المادة 61 وفي المادتين 62 و 63، ومن المادة يُفهم أن التجسس يتم من قبل أجنبي، وهو شرط لا يُفتَرض أن يؤدي إلى انعدام الجريمة، بل يُعتَبر في حال تخلفها محل جريمة أخرى، وهي جريمة الخيانة [1]حتى لو كان الجاني جزائري الجنسية وليس أجنبيًا، فإن المادة تشير إلى وقوع الجريمة من قبل الأجنبي بشكل عام، لا يهم جنس الجاني أو ما إذا كان مدنيًا أو عسكريًا، إذا كان للجاني شركاء جزائريين، فإنهم يتحملون المسؤولية عن جريمة التجسس وليس خيانة وطنية.[2]

#### أولا: أفعال التجسس وفقا للمادة 61

[1]بو جوراف عبد الغانيً جوان التجسس كجريمة ماسة بأمن الدولة في ظل قانون العقوبات الجزائري .مجلة آفاق للعلوم 2017، ص560.

[2]اسحاق ابراهًيم منصور، شرح قانون العقوبات الجزائري .الجزائر: ديوان المطبوعات الجامعية. الأمر رقم 156/66المؤرخ في8 يونيو 1966 قانون العقوبات .الجزائر: الجرّيدة الرسمية، 1988.

حسب المادة 61، يمكن تقسيم جريمة التجسس إلى ثلاث صور:

- التخابر مع دولة أجنبية.
- تسليم قوات أو ممتلكات جزائرية إلى دولة أجنبية أو عملائها.
- الإضرار بالدفاع الوطني.

وتحدد عناصر كل صورة كما يلي:

**1- القيام بالتخابر مع دولة أجنبية**

وفقًا للمادة 64 والفقرة رقم 01 من المادة 61، يُعتبر شخصًا مرتكبًا لجريمة التجسس إذا كان أجنبيًا وقام بالتخابر مع دولة أجنبية بنية حثها على ارتكاب أعمال عدوانية ضد الجزائر، أو توفير الوسائل اللازمة لذلك، سواء عن طريق تسهيل دخول القوات الأجنبية إلى الأراضي الجزائرية، أو بزعزعة ولاء القوات البرية أو البحرية أو الجوية، أو بأي طريقة أخرى، يتضح من ذلك أن جريمة التجسس تتألف من ركن مادي (التخابر وتوفير الوسائل) وركن معنوي (النية العدوانية ضد الجزائر)

- **الركن المادي**

الركن المادي لجريمة التجسس يتمثل في قيام الجاني بفعل التخابر مع دولة أجنبية، وهذا يعني وجود اتفاق غير مشروع بين الجاسوس والدولة الأجنبية، يهدف إلى تقديم أسرار الدفاع الخاصة بالدولة الجزائرية إلى الدولة الأجنبية، يكفي إثبات وقوع الاتفاق، سواء كان ذلك في العلن أو الخفاء، صراحة أو ضمنيًا، شفهيًا أو كتابيًا، أو إذا قام الجاني بالاتصال بالدولة الأجنبية أو إذا قامت الدولة الأجنبية بالاتصال به، ويتم تحقيق الركن المادي للجريمة بمجرد وقوع الاتفاق، دون الحاجة إلى تحقيق النتيجة المتمثلة في القيام بأعمال عدوانية ضد الجزائر [1]، وسواء تم الاتصال مباشرة أو عن طريق المراسلة، سواء عن طريق البريد أو اللاسلكي أو الهاتف أو التلغراف أو أي وسيلة اتصال أخرى تم تطويرها بفضل التقدم

[1] محمد صبحي نجم، شرح قانون العقوبات الجزائري القسم الخاص .الجزائر: ديوان المطبوعات الجامعّية،2000، ص 49.

التكنولوجي، ويستوي ذلك سواء وقع التخابر داخل الجزائر أو خارجها، يجب أن يتم إثبات وجود هذا الاتصال بغض النظر عن الطريقة التي تمت بها.

- **الركن المعنوي**

يتألف الركن المعنوي لجريمة التجسس من قصد جنائي عام وقصد جنائي خاص، يتمثل القصد الجنائي العام في أن يكون لدى الجاني نية متجهة نحو ارتكاب التخابر مع دولة أجنبية معادية للجزائر، وأن يكون على علم بأن فعله يُعتبر تجسسًا يُعاقب عليه القانون، إذا تبين أن المتهم لم يكن على علم بأن الشخص الذي تخابر معه هو ممثل لدولة أجنبية معادية للجزائر أو أنه يعمل لصالحها، فإن القصد الجنائي العام لا يتوفر لديه[1]،القصد الجنائي الخاص في التجسس يتمثل في أن يكون الغرض من تجسس الفرد على الجزائر هو دفع دولة أجنبية لاتخاذ إجراءات عدائية ضدها، مثل إعلان الحرب عليها، أو قطع العلاقات الدبلوماسية أو الاقتصادية معها، قد يكون الهدف أيضًا توفير الوسائل الضرورية لتنفيذ هذه الأعمال العدائية، سواء بتسهيل دخول القوات الأجنبية إلى الأراضي الجزائرية، أو بزعزعة الولاء داخل القوات المسلحة البرية، البحرية، أو الجوية، أو من خلال أساليب أخرى، الغاية من التجسس هنا تتمثل في مراقبة العدو وتعزيز قدراته على حساب الدفاع الوطني، والقوات، والمنشآت، والموارد العسكرية الوطنية.

**2- تسليم قوات أو ممتلكات جزائرية إلى دولة أجنبية أو عملائها**

وفقًا للفقرة الثالثة من المادة 61، يُعتبر الشخص الذي يقوم بتسليم قوات عسكرية جزائرية، أو أراضٍ، أو مبانٍ، أو حصون، أو منشآت، أو مراكز، أو مخازن، أو مستودعات حربية، أو معدات، أو ذخائر، أو مبانٍ، أو سفن، أو وسائل نقل جوي تابعة للجزائر أو

[1]أحمد فتحً سرور، الوسّط في قانون العقوبات القسم الخاص .القاهرة: دار النهضة العربّة،2013، ص 55.

مخصصة لحمايتها، إلى دولة أجنبية أو إلى أحد وكلائها، جاسوسًا بموجب المادة 64، تتألف هذه الجريمة من عنصر مادي وعنصر معنوي.

- **الركن المادي**

ترتكز هذه الجريمة على سلوك إجرامي صريح يتمثل في تسليم قوات عسكرية جزائرية، سواء كانت برية أو بحرية أو جوية، أو تسليم ممتلكات عسكرية مخصصة لحماية الجزائر، إلى دولة أجنبية أو إلى أحد وكلائها، ويُعتبر التسليم هو نقل ملكية هذه القوات أو الممتلكات من الدولة الجزائرية إلى قوات العدو ليتمكنوا من السيطرة عليها، [1] ،تتحقق الجريمة سواء دخلت القوات العسكرية في البلاد أم لم تدخل، ولا يلزم أن يكون هذا السلوك في زمن الحرب؛ بل قد يحدث أيضًا في زمن السلام.

- **الركن المعنوي**

تُعتبر هذه الجريمة جريمة متعمدة، تحدث بمجرد توافر النية الجنائية العامة لدى الجاني، دون الحاجة إلى التحقق من النية الجنائية الخاصة، يتطلب ذلك أن تكون إرادة الجاسوس موجهة نحو نقل ملكية القوات البحرية أو الجوية أو البرية، أو نقل ملكية الممتلكات العسكرية المخصصة للدفاع عن الوطن، إلى دولة أجنبية أو إلى أحد وكلائها، مع العلم الكامل بذلك.

### 3- الإضرار بالدفاع الوطني

وفقًا للمادة 61، الفقرة 3، وبموجب المادة 64، يُعتبر شخصًا جاسوسًا إذا قام بتدمير أو إتلاف سفينة أو عدة سفن، أو وسائل النقل الجوي، أو معدات، أو مؤن، أو مبانٍ، أو

[1] محمد صبحي نجم، مرجع السابق، ص 53.

منشآت بأي نوع كان، بنية إلحاق الضرر بالدفاع الوطني، أو إحداث عيوب فيها، أو تسبب في وقوع حادث، وذلك بنفس النية، تتألف هذه الجريمة من عنصر مادي وعنصر معنوي.

- **الركن المادي**

تتمثل الجريمة في سلوك إجرامي يأخذ أشكالاً متعددة، مثل التدمير أو الفساد، وقد يشمل إدخال عيوب أو التسبب في حوادث، لا يلزم لتحقيق الجريمة أن تتضمن جميع هذه الأشكال؛ تكفي تحقق إحداها، تشمل الهدف من هذه السلوكيات المركبات البحرية أو الجوية، والمعدات، والمواد، والمباني، والأعمال الهندسية، وكل ما يتعلق بالدفاع عن الوطن.

يتمثل التدمير في تحطيم الأشياء أو تدميرها، مثل هدم المباني الدفاعية أو حرق السفن، الفساد يتضمن التدخل لجعل الأشياء غير صالحة لغرضها، مثل تخريب محرك السفينة، إدخال العيوب يعني التدخل الإرادي لجعل الأشياء غير فعالة بالطريقة التي كانت مصممة عليها، مثل العبث في تركيب الأجهزة.[1]

- **الركن المعنوي**

تتألف الجريمة من قصد جنائي عام يتجه نحو اعتداء على السفن أو المركبات الجوية المحمية، أو المعدات، أو المواد، أو المباني، أو الأعمال الهندسية التي تخدم الدفاع الوطني، وذلك إما بتدميرها أو تلفها أو إدخال عيوب عليها أو التسبب في حوادث لها، مع علم الجاسوس بأن هذا الفعل يضر بالدفاع الوطني، يتطلب الأمر وجود قصد جنائي خاص يتمثل في أن الهدف الأساسي من هذا الفعل هو إلحاق الضرر بالدفاع الوطني.

**ثانيا: أفعال التجسس وفقا للمادة 62**

يتم تحديد التجسس وفقًا للمادة 62 في أربع أشكال يفترض تحقيقها خلال فترة الحرب، وهي تشمل تشجيع الجنود أو البحارة على الانضمام إلى دولة أجنبية، والتجاوزات

[1] بو جوراف عبد الغاني، مرجع السابق، ص 563.

مع دولة أجنبية ضد الجزائر، وتعطيل مرور المعدات العسكرية وتقويض الروح المعنوية للجيش أو الأمة، يمكن تفصيل هذه الأشكال كما يلي:

**1- تحريض العسكريين أو البحارة على الانضمام إلى دولة أجنبية**

يعتبر مرتكبًا للتجسس وفقًا للمادة 64 والمادة 62 في الفقرة الأولى أي شخص يشجع الجنود أو البحارة على الانضمام إلى دولة أجنبية أو يسهل طريقهم لذلك، ويشارك في عمليات تجنيد لصالح دولة في حرب مع الجزائر، تتألف الجريمة من عنصر مادي ومعنوي، ويمكن تفصيل هذين الجانبين كما يلي:

- **الركن المادي**

تتألف الجريمة من سلوك إجرامي يأخذ ثلاثة أشكال، ويكفي تحقيق إحداها لتكون الجريمة كاملة، الأولى هي تحريض الجنود أو البحارة الجزائريين على الانضمام إلى دولة أجنبية معادية للجزائر، ويترتب على ذلك التعامل مع التحريض وفقًا للقواعد العامة في المادة 41 من قانون العقوبات، التي تحدد الطرق المتاحة للتحريض مثل الهبة أو الوعد أو التهديد أو إساءة استخدام السلطة أو الولاية أو التحايل أو التدليس الإجرامي، الصورة الثانية هي تسهيل الطريق لهؤلاء الجنود أو البحارة الجزائريين للانضمام إلى دولة أجنبية معادية للجزائر، ويترتب على ذلك عدم تحديد طرق التسهيل من قبل المشرع، مما يعني أنه يمكن تنفيذ ذلك بأي طريقة، مثل الاتصالات اللازمة وتأمين طريق الوصول وعقد الاتفاقات بينهم وبين الدولة الأجنبية [1].

والصورة الثالثة هي إجراء عمليات تجنيد لصالح دولة في حرب مع الجزائر، حيث لا يكفي المتهم بالاتصال فقط مع الجنود أو البحارة، بل يجب أن يعمل على تجنيدهم لصالح الدولة المعادية، سواء كان ذلك داخل البلاد أو في الخارج، في الصورتين الأولى والثانية، لا

[1] بن مكي نجاة، محمود بوقطب.فيفري 2014 الخيانة العظمى كجريمة من الجرائم الماسة بأمن الدولة .مجلة الحقوق والعلوم السياسية، ص1150.

يهم إذا كان الانضمام قد حدث فعليًا، أما في الصورة الأخيرة، فمن الضروري أن يحدث التجنيد بالفعل، [1]

- **الركن المعنوي**

في هذه الصورة، يكفي تحقق القصد الجنائي العام، وذلك من خلال اتجاه إرادة المتهم نحو ارتكاب إحدى صور السلوك الإجرامي التي حددتها المادة، مع علمه بأركان الجريمة، بعد ذلك، لا يهم الهدف وراء ارتكاب الجريمة، سواء كان المتهم يسعى للمال، أو يخطط للتآمر ضد الجزائر، أو يهدف لأي غرض آخر، [2]

**2- التخابر مع دولة أجنبية ضد الجزائر**

يعتبر مرتكبًا للتجسس وفقًا للمادة 64 والمادة 62 في الفقرة الثانية أي شخص يتخاذ إجراءات للتجاذب مع دولة أجنبية أو أحد عملائها بهدف مساعدة هذه الدولة في خططها ضد الجزائر، تتألف الجريمة من عنصر مادي ومعنوي، ويمكن توضيح هذين الجانبين كما يلي:

- **الركن المادي**

يتم تحقيق السلوك الإجرامي في هذه الصورة من خلال اتفاق الجاسوس مع دولة معادية للجزائر أو أحد عملائها أثناء حرب بينهما، للتفاهم والتباحث بشأن مساعدتها في تنفيذ مخططاتها العسكرية داخل الجزائر، في هذا السيناريو، يضع الجاسوس نفسه تحت تصرف العدو أو أحد حلفائه، ويقوم بأداء المهام المطلوبة منه لتحقيق الأهداف المخطط لها.

[1] عبدالله سليمان، دروس في شرح قانون العقوبات الجزائري القسم الخاص .الجزائر: ديوان المطبوعات الجامعية،1996، ص 20.

[2] عبدالله سليمان، مرجع نفسه، ص 20.

- **الركن المعنوي**

يعتمد الجانب المعنوي لهذه الجريمة على وجود قصد عام وقصد جنائي خاص، يتطلب الأمر أن تكون إرادة المتهم موجهة نحو الاتفاق مع دولة معادية للجزائر، مع علمه بأن هذا الفعل يضع أمن الدولة الجزائري في خطر، كما يتطلب أن يكون الهدف الأساسي من هذا الاتفاق هو مساعدة هذه الدولة في تنفيذ خططها ضد الجزائر.

**3- عرقلة مرور العتاد الحربي**

يعتبر مرتكبًا للتجسس أي شخص قام بعرقلة مرور المعدات العسكرية، وفقًا لنص المادة 64 والفقرة الثالثة من المادة 62، تتألف هذه الصورة من عنصر مادي وعنصر معنوي، ويمكن تفصيل هذين الجانبين كما يلي:

- **الركن المادي**

في وقت الحرب، يهم كل دولة ضمان وصول المعدات العسكرية في الوقت والمكان المناسب، بهدف تزويد جيشها بالذخائر والمواد الملائمة والملابس والمعدات اللازمة للقتال، مما يسمح بتهيئته وتمكينه من الدفاع، إذا قام الأجنبي بأفعال تعرقل مرور هذه المعدات إلى الجيش الوطني، فإنه يعتبر من قبل المشرع الجزائري مرتكبًا للتجسس، نظرًا لتعطيل خطط الدفاع وتعرض الجيش للهزيمة، تعتبر الجريمة هذه اعتداءً على وسائل الدفاع الوطني، وقد أشار المشرع إلى أهميتها من خلال نص خاص.

- **الركن المعنوي**

يعتمد الجانب المعنوي على وجود قصد جنائي عام فقط، وهو اتجاه إرادة المتهم نحو عرقلة مرور المعدات العسكرية، مع علمه بأنه يرتكب الجريمة وفقًا للمتطلبات القانونية، لا يهم القاضي الهدف وراء ارتكاب الجريمة، سواء كان الهدف هو العداء والانتقام من الجزائر، أو الحصول على مبلغ مالي، أو مساعدة الدولة المعادية في تنفيذ خططها أو غير ذلك.

**4- إضعاف الروح المعنوية للجيش أو الأمة**

في الفقرة الرابعة من المادة 62 والمادة 64، ذكر أنه يعتبر مرتكبًا للتجسس أي شخص يساهم في مشروع إضعاف الروح المعنوية للجيش أو الأمة، بهدف إلحاق الضرر بالدفاع الوطني، مع علمه بذلك، تعتمد هذه الجريمة على عنصر مادي وعنصر معنوي، ويمكن دراستهما كما يلي:

- **الركن المادي**

تتألف الجريمة من السلوك المحض الذي يتمثل في أن يكون الجاسوس مساهمًا في مشروع مخطط لإضعاف الروح المعنوية للجيش الوطني أو للأمة الجزائرية، يفترض أن هذه الجريمة تتم في إطار عصابة أو مجموعة من الناس تهدف لإلحاق الضرر بالدفاع الوطني عن طريق تهديد إخلاص القوات المسلحة للدولة أو إضعاف روحها المعنوية، مما يؤدي إلى قتل روح الشجاعة والإقدام وحب الاستبسال لدى الجنود، وذلك من خلال زعزعة الأمن والإثارة للخوف والفزع في قلوبهم قبل وأثناء مواجهة العدو، كما قد يتخطى لإضعاف الروح المعنوية للأمة، مما يؤدي إلى تقويض ثقة الشعب في قدرة الجيش، وخلق شعور بالخوف، وبث روح الإنهزامية في أوساط الشعب الجزائري،[1] وعلى ذلك فيمكن أن يكون الجاسوس فاعلا أصليا أو شريكا أو محرضا في هذه المجموعة.

- **الركن المعنوي**

يتطلب القانون في هذه الجريمة وجود قصد جنائي عام وقصد جنائي خاص، القصد الجنائي العام يتمثل في اتجاه إرادة المتهم نحو الانضمام إلى المجموعة التي تهدف لتنفيذ مشروع لإضعاف الروح المعنوية للجيش أو للأمة، مع علمه بأركانها القانونية، القصد الجنائي الخاص هو أن تكون نية المتهم من وراء هذا الانضمام هي إلحاق الضرر بالدفاع الوطني، مع علمه بذلك.

## ثالثًا: أركان أفعال التجسس وفقًا للمادة 63

[1] بو جوراف عبد الغاني، المرجع السابق، ص 580.

تنص المادة 63 على أنه يتعلق بصورة أخرى من صور التجسس، وهي انتهاك أسرار الدفاع الوطني، تنص المادة على أنه يعتبر جاسوسًا أي شخص أجنبي يقوم بتسليم معلومات أو أشياء أو مستندات أو تصميمات تحتاج إلى الحفاظ على سريتها لمصلحة الدفاع الوطني أو الاقتصاد الوطني إلى دولة أجنبية أو أحد عملائها، بأي طريقة مادية أو معنوية، أو يقوم بالاستحواذ على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بهدف تسليمها لدولة أجنبية أو أحد عملائها، أو يقوم بتدمير مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بهدف مساعدة دولة أجنبية أو ترك الغير يتلفها، ولهذه الجريمة عنصر مادي وعنصر معنوي، ويمكن تفصيلهما كما يلي:

**1-انتهاك أسرار الدفاع الوطني**

ليُحمَّل الجاني مسؤولية ارتكاب انتهاك أسرار الدفاع الوطني، يجب أن يُدين بتسليم معلومات أو أشياء أو مستندات أو تصميمات إلى العدو أو أحد عملائه، والتي من المفترض أن تُحفَظ سراً لصالح الدفاع الوطني أو الاقتصاد الوطني، ولا يُشترط أن يكون الحفظ ورقياً فقط، بل يمكن أن يكون الحفظ في أنظمة معالجة البيانات الإلكترونية، مثل نظام المعالجة الآلية للبيانات، أو في وسائط تخزين البيانات مثل الأقراص المدمجة، أو الأشرطة الممغنطة، أو أشرطة الفيديو، ويُفهم بـ"فعل التسليم" نقل الحيازة المادية أو المعنوية للمعلومات السرية إلى العدو أو أحد عملائه.[1] يتحقق هذا الفعل بالتعامل المادي مع السر أو بتمكين الآخرين من الاستيلاء عليه، مثل ترك المستودع المحتوي على السر مفتوحًا أو ظاهرًا أو بدون حراسة، مما يُمكن الآخرين من الوصول إليه، أو تصويره، أو نسخه، [2]، ولا يشترط المشرع أن يكون التسليم بوسيلة معينة، بل نص على أنه يتم بأي وسيلة كانت، سواء كانت تقليدية مثل اليد، أو الهاتف، أو البريد العادي، أو عن طريق أحد العملاء الغاني، أو

[1] محمد صبحي نجم، مرجع السابق، ص 54.

[2] أحمد فتح سرور، مرجع السابق، 60.

بوسائل حديثة مثل البريد الإلكتروني، أو تطبيقات التراسل الفوري مثل السكايب، أو المنصات الاجتماعية كالماستجر وغيرها، ومحل التسليم يمكن أن يكون معطيات تتعلق بالدفاع، والتي يمكن أن تكون مخزنة في الحاسوب الآلي، أو الأقراص المدمجة، أو الأشرطة الممغنطة، أو أشرطة الفيديو، حيث يقوم الجاني بتسليمها باليد أو بإرسالها إلكترونيًا.

**2- الاستحواذ على معلومات سرية تتعلق بالدفاع الوطني**

يشير مصطلح "الاستحواذ" إلى الحصول على المعلومات السرية، سواء كان ذلك من خلال الوصول إلى المحتوى المادي للمعلومات السرية أو فهم مضمونها أو معناها، سواء تم تسليمها أو إتلافها أم لا، وفقًا للمشرع الجزائري، يمكن أن يكون الاستحواذ على المعلومات السرية بطرق مختلفة، سواء كان ذلك عن طريق الاطلاع على المعلومات السرية المكتوبة أو المحفوظة إلكترونيًا وحفظها في الذاكرة، وهذا يعتبر استحواذًا معنويًا، أما إذا تم الحصول على المعلومات السرية بواسطة اليد أو تم نسخها أو حفظها في وسائل إلكترونية، فإنه يعتبر استحواذًا ماديًا، لم يحدد المشرع الجزائري أي طريقة محددة للاستحواذ، بل يمكن أن يكون بأي وسيلة تكنولوجية أو أخرى، وبالتالي، يمكن القول أن النص القانوني يترك المجال مفتوحًا لاستيعاب أي وسيلة أخرى قد تظهر في المستقبل.

**3- إتلاف معلومات سرية تتعلق بالدفاع الوطني**

يقصد بإتلاف محل السر إعدام ذاتيته وإنهاء كيانه وهو لا يتحقق إلا على الوعاء المادي الحامل له [1]، سواء كانت المعلومات السرية محمولة على وثائق ورقية أو وسائط إلكترونية، يتم تحقيق إتلافها عن طريق تمزيق الوثائق الورقية أو حرقها أو مسح المحتوى المكتوب، وبالنسبة للوسائط الإلكترونية، يتم تدميرها إلكترونيًا باستخدام فيروسات إلكترونية، لا يشترط أن يقوم الجاني بإتلاف المعلومات السرية بنفسه، بل يمكن أن يتحقق الإتلاف عن

[1] محمد صبحي نجم، مرجع السابق، ص 55.

طريق تمكين الآخرين من القيام بهذا الفعل، وبالتالي، يتم تدمير المعلومات السرية بطرق مختلفة بناءً على الوعاء المادي الذي يحملها.

**4- الركن المعنوي**

يتطلب التوافر في الصور الثلاثة لانتهاك أسرار الدفاع الوطني وجود القصد الجنائي العام، وهو ما يتطلب إرادة وعلم من المتهم، يجب أن تكون إرادة المتهم الواعية موجهة نحو انتهاك أسرار الدفاع الوطني عبر التسليم أو الاستحواذ أو الإتلاف، مع علمه بذلك، يكون القاضي ملزمًا بالبحث عن القصد الجنائي الخاص في فعل الاستحواذ والإتلاف، إذا وجد القاضي أن غاية الجاسوس من وراء الاستحواذ هي تسليم محل السر إلى دولة أجنبية أو أحد عملائها، فإن الجانب المعنوي يتحقق، وإذا كان قصد المتهم من وراء الإتلاف هو مساعدة دولة أجنبية ضد الجزائر، فإن الجانب المعنوي يتحقق أيضًا.

## الفرع الثاني: الاليات القانونية القانونية الخاصة

تركزت الجهود بشكل رئيسي على اتخاذ التدابير القانونية دون إيلاء الاهتمام الكافي للتدابير الأخرى. يتجلى هذا التوجه بوضوح في صدور القانون رقم 09-04 المؤرخ في 05 أغسطس 2009، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. يتناول هذا القانون تحديد الحالات التي تبرر اللجوء إلى مراقبة الاتصالات الإلكترونية.

بناء على ما ورد في المادة 4 التي نصت على ما يلي: "[1]

للوقاية من الأفعال المصنفة كجرائم إرهابية أو تخريبية والجرائم التي تمس أمن الدولة، يُسمح بمراقبة الاتصالات الإلكترونية في حالة وجود معلومات عن احتمال اعتداء على

[1] قانون رقم 9-4 المؤرخ في 14 شعبان 1430 الموافق 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية العدد 47، الصادرة بتاريخ 25 شعبان1430 الموافق لـ 16 أوت 2009، ص06.

منظومة معلوماتية تهدد النظام العام، الدفاع الوطني، مؤسسات الدولة، أو الاقتصاد الوطني. تشمل هذه التدابير التحريات والتحقيقات القضائية التي يكون من الصعب تحقيق نتائجها دون اللجوء إلى المراقبة الإلكترونية، وذلك في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما نصت المادة 13 على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهو ما تم بالفعل بصدور المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، الذي يحدد تشكيل وتنظيم وكيفية سير عمل هذه الهيئة. تتضمن مهام الهيئة، وفقاً للمادة 4 من المرسوم، مجموعة من الإجراءات والأنشطة الرامية إلى الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:[1]

-

- تنسيق الجهود الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بين مختلف الجهات المعنية.
- تقديم الدعم والمساعدة للسلطات القضائية وأجهزة إنفاذ القانون في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك جمع وتوفير المعلومات والخبرات القانونية.
- ضمان المراقبة الوقائية للاتصالات الإلكترونية لاكتشاف الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت إشراف القضاء المختص وباستثناء أي جهات أخرى.

[1] – الجمهورية الجزائرية الديمقراطية الشعبية مرسوم رئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436، مرجع سابق، ص16-17

- جمع وتسجيل وحفظ البيانات الرقمية، وتحديد مصدرها ومسارها لاستخدامها في الإجراءات القضائية.
- المساهمة في تدريب وتأهيل المحققين المتخصصين في مجال التحقيقات التقنية المتعلقة بتكنولوجيات الإعلام والاتصال.
- المساهمة في تحديث وتطوير المعايير القانونية والتشريعات في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.، [1]

إلى جانب الاهتمام بالجوانب القانونية والمؤسساتية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، نظمت مديرية الاتصال والإعلام والتوجيه التابعة لأركان الجيش الوطني الشعبي سلسلة من الملتقيات حول رهانات تداول المعلومات عبر شبكات التواصل الاجتماعي. وقد أجمع المشاركون في هذه الملتقيات على ضرورة تعزيز العقيدة الأمنية الجزائرية بالمزيد من اليقظة والتحكم في التكنولوجيات الحديثة، والتنبيه لمخاطر سوء استخدامها. كما دعوا إلى توسيع دائرة المشاركة لتشمل فواعل جدد من خارج المؤسسة العسكرية، بهدف المساهمة في صيانة عقيدة الدفاع الوطني، نظرًا لأن الفضاء السيبراني أصبح أحد الميادين الأكثر أهمية، ويحتل المرتبة الخامسة للنزاعات بعد البر والبحر والجو والفضاء.[2]

[1] ب، بوعلام، ملتقى حول الجيش الوطني الشعبي ورهانات تداول المعلومات عبر شبكات التواصل الاجتماعي"، مجلة الجيش، (مؤسسة المنشورات العسكرية، العدد 630 جانفي 2016)، ص 39.

[2] ب، بوعلام، مرجع سابق، ص ص 38-39.

## المطلب الثاني: معيقات تحقيق الأمن السيبراني الجزائري في ظل التحديات الأمنية والمستقبلية

يتناول المطلب الثاني معيقات تحقيق الأمن السيبراني الجزائري في ظل التحديات الأمنية والمستقبلية، حيث يستعرض الفرع الأول معيقات تحقيق الأمن السيبراني الجزائري، بينما يقدم الفرع الثاني رؤية مستقبلية للأمن السيبراني في الجزائر.

### الفرع الأول: معيقات تحقيق الأمن السيبراني الجزائري

إن التطورات الحديثة في مفهوم الأمن تستدعي منا إعادة النظر في هذا المفهوم بما يتماشى مع التغيرات المتسارعة في العالم، خاصة في ظل التقدم الهائل في مجالات الإعلام الآلي وتكنولوجيا المعلومات والاتصالات. حيث أدى هذا التطور إلى ظهور مفهوم "المدن الذكية" التي تحولت فيها الخدمات من الشكل التقليدي إلى الإلكتروني، مما خلق حقلًا جديدًا يختلف عن سابقيه. ورغم الفوائد العديدة لهذا التحول، إلا أنه يتطلب توفير الأمن اللازم لضمان نجاح هذه الخدمات. لذلك، يجب علينا إعادة تعريف مفهوم الأمن ليتواءم مع هذا الواقع الجديد، وضمان حماية البنية التحتية الرقمية والخدمات الإلكترونية من أي تهديدات أو مخاطر محتملة.

والجزائر كغيرها من الدول تسعى نحو تبني مقاربة الحوكمة الالكترونية * وعلى الرغم من حداثة التوجه، إلا أن عدد الجرائم المرتكبة يوحي بحجم الأخطار التي تتربصها، وهو ما يجعل مؤسسة الدفاع الوطني أمام تحديات وعوائق جديدة وهو تحقيق الأمن السيبراني حاليا ومستقبلا، تواجه مصالح الدرك الوطني ومصالح الأمن الوطني العديد من العوائق والتحديات التي تعيقها في تحقيق الأمن السيبراني في الجزائر، يمكن أن تذكر أهمها بما يلي:

- مع زيادة عدد المشتركين في شبكة الإنترنت في الجزائر إلى أكثر من 10 ملايين مشترك، تزداد المخاطر المرتبطة باستخدام الشبكة. ومع تزايد عدد مستخدمي الإنترنت، يصبح اكتشاف هوية مرتكبي الجرائم الإلكترونية تحدياً كبيراً بسبب صعوبة البحث والتحري ضمن هذا العدد الهائل والمتزايد باستمرار من المستخدمين.
- يساهم انتشار تكنولوجيا الإنترنت فائقة السرعة مثل VSAT وADSL وSDSL في تسهيل ارتكاب الجرائم الإلكترونية بسرعة أكبر، مما يضع الجهات الأمنية المتخصصة أمام تحديات كبيرة تتعلق بسرعة مباشرة التحقيقات ومتابعة الجناة. يتطلب ذلك التسلح بالأجهزة المتطورة والبرامج الحديثة عالية الأداء لمواجهة هذه التحديات بفعالية.
- مع التطور التكنولوجي وظهور تقنيات الإنترنت مثل WiFi وG3 وG4، لم يعد المجرمون بحاجة للجلوس خلف الحواسيب الموصولة سلكياً بشبكة الإنترنت لارتكاب جرائمهم. هذا يستدعي من الجهات الأمنية رفع مستوى التحدي والاستعداد بأحدث التقنيات لمواجهة هذه التطورات والتصدي لها بفعالية.
- تزايد عدد مستخدمي شبكات التواصل الاجتماعي في الجزائر إلى أكثر من 7 ملايين مستخدم أسهم بشكل كبير في زيادة أنواع متعددة من الجرائم الإلكترونية، مثل التحرش الجنسي والقذف واستغلال القصر، وغيرها. هذا يستدعي وضع استراتيجيات متكاملة لضمان الأمن السيبراني عند استخدام مواقع التواصل الاجتماعي.

تُعتبر عمليات التخفي أثناء استخدام خدمات شبكة الإنترنت (مثل استخدام بروكسي Proxy) من أكبر التحديات التي تواجه الجهات المتخصصة في التحقيقات الرقمية. ويتطلب التصدي لهذه الإشكالية تعاونًا وثيقًا بين مختلف الجهات ذات الصلة، إلى جانب التزود بأحدث الوسائل التقنية القادرة على رصد الجزئيات وفك التشفير، وتطوير البنى التحتية

للمعلومات وتحديثها باستمرار. كما يتعين تصميم برامج متطورة ومتخصصة في مجال مكافحة هذه الأنشطة التخفية على الإنترنت.

يجب على الجهات المعنية اتخاذ إجراءات فعالة لمواجهة تحدي التخفي عبر الإنترنت، والذي يمثل عائقًا كبيرًا أمام التحقيقات الجنائية في مجال الجرائم الإلكترونية. ويتطلب ذلك توفير الموارد البشرية والمادية اللازمة، وتعزيز التعاون والتنسيق بين مختلف الأطراف المعنية، بهدف تطوير القدرات التقنية والمهنية للتصدي لهذا التحدي بشكل فعال.

تشكل المشكلة الرئيسية في مكافحة الجرائم الإلكترونية هي طبيعتها العابرة للحدود والقارات. حيث يستطيع مرتكبو هذه الجرائم النفاذ إلى أنظمة الحاسوب في دولة ما، والتلاعب واختراق البيانات في دولة أخرى، وتسجيل النتائج في دولة ثالثة. كما يمكنهم إخفاء هوياتهم ونقل الموارد عبر قنوات موجودة في دول مختلفة. وبفضل قدرتهم على التنقل إلكترونيًا من شبكة إلى أخرى والوصول إلى قواعد البيانات في قارات متعددة، تصبح العديد من الدول والمحاكم والقوانين معنية بهذه الجرائم، مما يشكل تحديًا حقيقيًا.

لذلك، فإن المكافحة الفعالة للجرائم الإلكترونية تتطلب تعاونًا متزايدًا وسريعًا وفعالًا على أعلى درجات التنسيق بين الدول والحكومات. حيث يجب على الدول تبادل المعلومات والخبرات، وتنسيق الجهود، وتوحيد التشريعات والإجراءات القانونية، وتعزيز التعاون القضائي والشرطي عبر الحدود، من أجل مواجهة هذا التحدي بشكل فعال وحاسم.[1]

مع التقدم التكنولوجي السريع في مجالات الإنترنت والاتصالات، أصبح من الضروري على الأجهزة الأمنية المتخصصة مواكبة هذه التطورات. يشمل ذلك ليس فقط

[1] كريستينا سكولمان " الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية"، برنامج الأمم المتحدة، برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة أعمال الندوة الإقليمية حول الجرائم المتصلة 119 بالكمبيوتر، المملكة المغربية، يونيو 2007، ص19-20.

اقتناء التكنولوجيا الحديثة، بل أيضًا تعلم كيفية استخدامها واستغلالها بفعالية. هذا التحدي يضع ضغطًا كبيرًا على الميزانيات المحدودة، مما يستدعي توجيه جميع الموارد المادية، المالية، والبشرية نحو تعزيز الأمن السيبراني.

بالإضافة إلى ذلك، يعتبر نشر الوعي حول مفهوم الأمن السيبراني بين مستخدمي الإنترنت أمرًا حاسمًا. يتطلب ذلك تنظيم حملات توعية لتعليم المستخدمين اتخاذ الإجراءات الضرورية لضمان مستوى أمان مقبول، وترسيخ أهمية الإبلاغ الفوري عن أي مخاطر لتمكين السلطات المعنية من التحرك في الوقت المناسب وتحديد مرتكبي الجرائم الإلكترونية.

للحد من انتشار الجريمة الإلكترونية، يجب تفعيل القوانين بشكل فعال وتطبيقها بصرامة. أحد العوامل الرئيسية التي تسهم في زيادة هذه الجرائم هو الإفلات من العقاب والتأخير في تنفيذ القوانين، مما يمنح المجرمين فرصة تكرار جرائمهم. لذا، من الضروري التأكيد على تطبيق القوانين بشكل صحيح. بالإضافة إلى ذلك، يجب أن تتكيف النصوص القانونية مع التغيرات المستمرة في هذا المجال. كما يُنصح بإنشاء محاكم متخصصة بالجرائم الإلكترونية نظرًا للانتشار الواسع لهذه الجرائم وتعقيدها الفني، مما يتطلب خبرة قضائية متخصصة للتعامل معها بشكل فعال.[1]

## الفرع الثاني: رؤية مستقبلية للأمن السبراني الجزائري

في ظل التطورات السريعة في مجالات الإعلام الآلي، تكنولوجيا الاتصالات، والمعلومات، أصبح من الضروري إعادة النظر في مفاهيم الأمن بما يتماشى مع هذه التغيرات. خاصة مع الاتجاه نحو إنشاء "المدن الذكية"، حيث تحولت الخدمات من التقليدية إلى الإلكترونية، مما أنشأ مجالًا جديدًا يتطلب توفير أمن مختلف عن السابق. على الرغم

[1] – بارة سمير، مرجع سابق، ص18.

من الفوائد العديدة لهذه التطورات، إلا أنها تستلزم توفير أمن فعال لضمان نجاح هذه الخدمات.

الجزائر، مثل باقي الدول، مطالبة بتبني مقاربة الحكومة الإلكترونية. على الرغم من حداثة هذا التوجه، إلا أن ارتفاع عدد الجرائم الإلكترونية يشير إلى الأخطار الكبيرة المحدقة. هذا يضع مؤسسات الدفاع الوطني أمام تحدي جديد، وهو ضمان الأمن السيبراني الآن وفي المستقبل.[1]

[1] بن مرزوق عنترة وآخرون، البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"، مجلة العلوم الإنسانية، العدد38، الصادرة بتاريخ جوان 2018، ص 41.

**خلاصة الفصل:**

تناولنا الفصل الثاني آليات الردع المختلفة لمواجهة التجسس السيبراني الذي يمثل تهديدًا حقيقيًا لأمن الدولة واستقرارها، يتم تقسيم هذا الفصل إلى مباحث ومطالب متعددة تركز على الجوانب العملياتية والقانونية لمكافحة هذه الجرائم السيبرانية.

# خاتمة

ان جريمة التجسس في تطور مستمر لاستخدامها احدث التقنيات والاساليب التي توصلت اليها التكنولوجيا في جميع الميادين لذلك لزم على المشرع الجزائري مواكبة ذلك لمواجهة هذه الجريمة باستحداث آليات اخرى أكثر تطورا ودقة.

وبعد تحليلنا للنصوص القانونية للتجسس توصلنا الى النتائج التالية :

- المشرع الجزائري لم يحدد وسائل التجسس الالكتروني وأن يمكن ارتكابه بواسطة أنظمة المعالجة الآلية للمعطيات أو بواسطة أنظمة اتصالات الكترونية لأن وسائل ارتكاب التجسس الالكتروني في تطور مستمر لا يكاد يمر يوما على العالم الى ويسمع بوسائل جديدة في الدقة والاتقان حيث احتكرتها الدول الكبرى وتعمل على تطويرها بواسطة خبراء مختصين .

**اقتراحات:**

- يحب على المشرف ان يكيف قانوني داخلي مع اتفاقية عربية بمكافحة جرائم تقنية المعلومات وذلك من خلال النصوص، صرحة دون أي غموض يستدعي التأويل أما القيس على تشديد العقاب على اي جريمة تقليدية بما فيها التجسس بواسطة منظمة المعلومات أو نظام اتصالات الالكترونية.
- تشديد اجراءات ووسائل حماية المنظومة الدفاعية المتضمنة معطيات سرية للدفاع الوطني.

# قائمة المصادر والمراجع

**قائمة المراجع والمصادر:**

**أولا: القرآن الكريم:**

سورة الحجرات ، الآية 12.

**ثانيا: النصوص القانونية:**

**1-القوانين:**

- الجريدة الرسمية، القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وطرق مكافحتها، الفترة التشريعية السادسة، السنة الثالثة الدورة الرابعة، رقم 122 27 يونيو (2009).

- الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 04/09 المؤرخ في 14 شعبان 1430 الموافق 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية العدد 47، الصادرة بتاريخ 25 شعبان1430 الموافق لـ 16 أوت 2009.

**2-الأوامر:**

- المادة 2، القانون09-04 المؤرخ في 13شعبان 1430 الموافق ل5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد 47، المؤرخة في 25 شعبان 1430هـ الموافق ل 15 غشت 2009.

**ثالثا: الكتب**

- إبراهيم بلعليات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الطبعة الأولى، الجزائر، 2007.

– أحمد فتحً سرور، الوسيط في قانون العقوبات القسم الخاص، القاهرة: دار النهضة العربٌة، 2013.

– اسحاق ابراهٌيم منصور 1988 شرح قانون العقوبات الجزائري، الجزائر: ديوان المطبوعات الجامعية، الأمر رقم 66/156 المؤرخ في 8 يونيو 1966 قانون العقوبات، الجزائر: الجرٌيدة الرسمية.

– إلهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزور، جامعة الحاج لخضر، باتنة، 2016.

– أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة بين التشريعات العربية والأجنبية، الطبعة الأولى، مكتبة القانون والإقتصاد، الرياض، 2014.

– حديث شريف علاء الدين بن محمد بن إبراهيم البغدادي، تفسير الخازن لباب التأويل في معاني التنزيل، جزء 5 ، دار الكتب العلمية بيروت، لبنان، 2009.

– سهام بو عموشة، "الفضاء السبراني يتميز بانفتاح شبكة المعلوماتية وانعدام الحواجز الجغرافية"، جريدة الشعب، العدد 17345، 24 ماي (2017).

– صدام حسين ياسين العابدي، جرائم الأنترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعية، د.ط، المركز العربي للتوزيع،القاهرة، 2018.

– صلاح نصر، الحرب الخفية تاريخ المخابرات، دار الخيال الجزء الأول، الطبعة الأولى، القاهرة، 2002.

– عبد الرحمان بن حمادي الفضاء الأزرق أصبح مكانا مثاليا للقيام بأعمال غير مشروعة"، معرض الصحافة تجزئة سعيد بن حداد الشراقة ، الجزائر ، 25 ماي 2016.

– عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت، في القانون العرب النموذج، مصر مطابع شتات، 2007.

– عبد الله سليمان، شرح قانون العقوبات الجزائري القسم العام، ديوان المطبوعات الجامعية، الجزء الأول (الجريمة)، (دون طبعة)، 1995.

– عماد مجدي عبد الملك، جرائم الكومبيوتر والانترنت، الإسكندرية دار المطبوعات الجامعية، 2011.

– غانم مرضي الشمري، الجرائم المعلوماتية، ماهيتها، خصائصها، كيفية التصدي لها قانونيا، الطبعة الأولى، الدار العلمية والدولية للنشر والتوزيع، عمان، 2016.

– فواز البقور، التجسس في التشريع الأردني دراسة مقارنة، دار النشر، الطبعة الثالثة، عمان، 1993.

– كريستينا سكولمان "الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية"، في برنامج الأمم المتحدة، برنامج الأمم المتحدة، برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة أعمال الندوة الإقليمية حول الجرائم المتصلة 119 بالكمبيوتر، المملكة المغربية، يونيو 2007.

– محمد صبحي نجم، شرح قانون العقوبات الجزائري القسم الخاص، الجزائر: ديوان المطبوعات الجامعيّة، 2000.

– مصطفى عباني، التدابير الأخرى في مجال نزع السلاح والأمن الدولي، اللجنة الأولى للدورة الـ 71 الجمعية العامة للأمم المتحدة، بعثة الجزائر الدائمة لدى الأمم المتحدة، نيويورك، 24 أكتوبر 2016.

– منير البعلبكي، المورد قاموس إنجليزي–عربي، دار العلم للملايين، د.ط، بيروت، 2022.

– نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، دراسة نظرية تطبيقية، الطبعة الأولى، منشورات الحلبي الحقوقية، القاهرة، 2015.

- نجاة معلا مجيد تعزيز وحماية جميع حقوق الانسان بما في ذلك الحق في التنمية"، الجمعية العامة، الأمم المتحدة، الدورة الثانية عشر، البند 03 من جدول الأعمال.

- نوف علي الشنيفي، البرامج التجسسية أنواعها وطرق الحماية منها، مركز التميز الأمن المعلوماتي، مصر.2011.

**رابعا: المجلات**

- إيمان بن سالم جريمة التجنيد الالكتروني للإرهاب وفقا لقانون العقوبات الجزائري، برلين، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية ، 2008.

- حسن بن أحمد الشهيري، «الأنظمة الإلكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس» المجلة العربية للدراسات الأمنية والتدريب المجلد 28، العدد 56.

- إسماعيل جنة حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون"، مجلة الجيش، العدد 599 جوان (2013).

- بن مرزوق عنترة وآخرون البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"، مجلة العلوم الإنسانية، العدد 38، جوان 2018.

- بن مكي نجاة، محمود بوقطب، فيفري 2014 الخيانة العظمى كجريمة من الجرائم الماسة بأمن الدولة، مجلة الحقوق والعلوم السياسية.

- بو جوراف عبد الغانيً جوان التجسس كجريمة ماسة بأمن الدولة في ظل قانون العقوبات الجزائري، مجلة آفاق للعلوم 2017.

- ب، بوعلام ملتقى حول الجيش الوطني الشعبي ورهانات تداول المعلومات عبر شبكات التواصل الاجتماعي"، مجلة الجيش، (مؤسسة المنشورات العسكرية، العدد 630 جانفي 2016).

- رحوني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة أحمدة دراية–أدرار– د.ج، العدد 41، د.ت.
- خرشف فاطمة ولزار سميرة، الإطار المفاهيمي والقانوني لمواجهة الجرائم السيبرانية، مجلة سوسيولوجيا للجريمة مخبر الجريمة والإنحراف بين الثقافة و التمثلات الإجتماعية، جامعة علي لونيسي البليدة2، مجلد 2، عدد 1،2021 .
- سلامي نادية، التجسس الإلكتروني كأثر للاستخدام غير المشروع للفضاء الإلكتروني على أمن الدولة الخارجي، مجلة دراسات ،2017
- عبد الرحمان لحرش، التجسس والحصانة الديبلوماسية، مجلة الحقوق، جامعة الكويت، العدد الرابع، السنة السابعة والعشرون ، 2003.
- عبد الغني بوجراف، التجسس كجريمة ماسة بأمن الدولة في ظل قانون العقوبات الجزائري، مجلة أفاق العلوم، الجلفة الجزء الأول، العدد الثامن 2017.
- غريب حكيم، الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديد وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، المجلد5، العدد2.
- سمير بارة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني (Cyber Security) في الجزائر الدور والتحديات"، جامعة قاصدي مرباح ورقلة، د س.
- قاسحي فيروز، الجريمة الإلكترونية عبر مواقع التواصل الإجتماعي، مجلة الرسالة للدراسات والبحوث الإنسانية جامعة الجزائر3، المجلد7، العدد8، فيفري 2023.
- قطاف سليمان وبوقرين عبد الحليم، مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية، مجلة البحوث القانونية والإقتصادية، مخبر البحث في الحقوق والعلوم السياسية جامعة عمار ثليجي–الأغواط، المجلد 5، العدد 2، 2022.

- ماينو جيلالي وعروس كوثر، الجريمة السيبرانية في صورها المستحدثة، مجلة القانون والتنمية، مخبر القانون والتنمية، جامعة طاهري محمد بشار، المجلد 4، العدد1، جويلية 2023.

- محمد خلّفة، دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلّة للمعطّات، في قانون العقوبات الجزائري، المجلة النقدية للقانون والعلوم السياسية، 2018.

**خامسا: الرسائل الجامعية:**

**1-أطروحات دكتوراه:**

- عميمر عبد القادر، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري، دراسة مقارنة، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 1، 2019-2020.

**2-رسائل الماجيستر:**

- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الاعلام والاتصال في ضوء القانون رقم 09/04، رسالة ماجستير، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012-2013.

- أمل جبر عبد الخالق، التجسس عبر التصوير في الفقه الإسلامي، رسالة ماجستر في الفقه المقارن ، كلية الشريعة والقانون ، غزة، د س ن.

- سعيداني نعيم، آليات البحث والتحري في الجريمة المعلوماتية في القانون الجزائري، مذكرة الماجيستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر-باتنة-، 2013/2012.

- عبد الله بن حسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية، رسالة الماجيستير في قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2014.

- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة الماجيستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر،2011-2012.

- محمد بوشعبة، مذكرة ماجيستير بعنوان الخيانة والتجسس في قانون القضاء العسكري الجزائري، قانون جنائي، جامعة يحي فارس، المدية، 2022.

**3-المذكرات:**

- حشمان عمار، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، كلية العلوم الإقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح-ورقلة- 2019_2018.

**سادسا: المواقع الالكترونية:**

- https://strategiecs.com/ar/analyses/how-can-military-technology-be-the-decisive-factor-in . تاريخ الاطلاع 20 أوت 2024 على الساعة 18:00
- http://www.arabs2day.ws/forums/lofiversion/index.php/t172.htm أطلع عليه بتاريخ 2024/05/19 على الساعة 21:00
- hltps: www.eljoumhouria.dg أطلع عليه بتاريخ 2024/05/19 على الساعة 21:00
- https://www.noonpost.com/content/36070 أطلع عليه بتاريخ 2024/05/19 على الساعة 22:00
-
- www.essalamonline.com أطلع عليه بتاريخ 2024/05/19 على الساعة 22:00

- www.ehoroukonline.com أطلع عليه بتاريخ 2024/05/26 على الساعة 21:00
- https://www.facebook.com/realestateKhal/posts أطلع عليه بتاريخ 2024/05/29 على الساعة 20:00

**سابعا: المراجع باللغة الأجنبية**

- Eric A.Caprioli( .février, 2011) system de traitement automatiser de données .revue jurisclasseu.
- sunil.c.pawer,dr.s.mente, cyber crime,cyber space and effects of cyber crime, international journal of scientifics research in computer science engineering and information technology, Punyashlok Ahilyadevi Holkar Solapur University Solapur, Maharashtra, India volume7, issue1, 2021, p211.
- wars-before-their-eruption
- Yves Mayaud (2011) .code penal.Paris: dalloz.

# فهرس المحتويات

## فهرس المحتويات

مقدمة .....1

الفصل الأول:

ماهية التجسس السيبيراني الماس بأمن الدولة

المبحث الأول: الإطار المفاهيمي للجريمة السيبرانية..... 5

المطلب الأول: مفهوم الجريمة السيبرانية..... 6

الفرع الأول: تعريف الجريمة السيبرانية..... 6

الفرع الثاني: خصائص الجريمة السيبرانية..... 10

المطلب الثاني: الطبيعة القانونية للجريمة السيبرانية وصورها ..... 13

الفرع الأول: الطبيعة القانون للجريمة السيبيرانية..... 13

الفرع الثاني: صور الجريمة السيبرانية..... 14

المبحث الثاني: ماهية التجسس عبر الانترنت الماس بأن الدولة..... 17

المطلب الأول: جريمة التجسس الكلاسيكي ..... 17

الفرع الأول: تعريف جريمة التجسس..... 17

الفرع الثاني: أركان جريمة التجسس ..... 19

المطلب الثاني : التجسس السيبيراني ..... 25

الفرع الأول: مفهوم التجسس السيبيراني..... 26

الفرع الثاني: وسائل ارتكاب التجسس الإلكتروني..... 29

الفصل الثاني:

الاليات الردعية للتجسس السيبيراني الماس بأمن الدولة

المبحث الأول: الاليات العملياتية لردع التجسس السيبيراني ..... 41

المطلب الأول: الأجهزة العملياتية المختصة في الأمن السيبراني..... 42

الفرع الأول: على المستوى الوطني..... 42

الفرع الثاني: على المستوى الدولي..... 47

المطلب الثاني : الإستراتيجيات الأمنية لمكافحة التهديدات السيبرانية..... 48

الفرع الأول: على المستوى الدولي..... 48

أولا: الندوة الدولية حول الأمن السيبراني في الجزائر ..... 48

ثانيا: إستراتيجية التعاون الدولي للوقاية من الجرائم السيبرانية..... 49

الفرع الثاني: على المستوى الوطني..... 51

المبحث الثاني: الاليات القانونية ومعيقات تحقيق الامن السيبيراني..... 55

المطلب الأول : الاليات القانونية لردع جريمة التجسس عبر الانترنت ..... 56

الفرع الأول: الاليات القانونية العامة (قانون العقوبات)..... 56

الفرع الثاني: الاليات القانونية القانونية الخاصة..... 67

المطلب الثاني: معيقات تحقيق الأمن السيبراني الجزائري في ظل التحديات الأمنية والمستقبلية..... 70

الفرع الأول: معيقات تحقيق الأمن السيبراني الجزائري ..... 70

الفرع الثاني: رؤية مستقبلية للأمن السبراني الجزائري ..... 73

خاتمة.....76

قائمة المصادر والمراجع.....78