

جامعة أكلي محند أولحاج - البويرة
Tasdawit Akli Muḥend Ulḥağ -Tubiret-
Université Akli Mohand Oulhadj – Bouira-



كلية الحقوق والعلوم السياسية
قسم القانون العام
مذكرة مكملة لمتطلبات نيل شهادة الماستر في القانون العام

جريمة التجسس الإلكتروني في التشريع الجزائري

تخصص: قانون جنائي وعلوم جنائية

تحت إشراف الأستاذ:
- مزهود حكيم

من إعداد الطالب:
- عكلوش محند

لجنة المناقشة:

رئيسا	جامعة البويرة	أ- د. خليفي سمير
مشرفا	جامعة البويرة	أ- مزهود حكيم
ممتحنا	جامعة البويرة	أ- د. زكاريّا بوعمامة

السنة الجامعية: 2026/2025

شكر وتقدير

Azul fellowen

السلام عليكم

أقدم بخالص الشكر والتقدير والامتنان للأستاذ المشرف مزهود حكيم،
على توجيهاته ودعمه لإعداد هذه المذكرة.

كما أشكر جميع الأساتذة الكرام في قسم الحقوق على ما قدموه من
علم ونصائح قيمة وسعيهم الجاد من أجل المعرفة، وكذا الطاقم الإداري
بكلية الحقوق.

ولا يسعني إلا أن أعبر عن امتناني لكل من ساهم أو مد لي العون في إنجاز
هذا العمل.

محمّد

إهداء

أهدي هذه المذكرة إلى أفراد عائلتي الأعزاء، الذين كانوا دائما مصدر دعم
وتشجيع في مسيرتي الأكاديمية والحياتية،

إلى والديا الحبيبين،

إلى زوجتي ذهبية وبناتي الغاليات إرزا، أميليا وماريس،

وأخواني الأعزاء أعمار وماسينيسا، وأخواتي العزيزات سامية، حسينة

وسعاد.

كما أهدىها إلى الأصدقاء والاحباب.

محمد

المقدمة

مقدمة

لا شك أن الثورة التكنولوجية والمعلوماتية الحالية تُعد من أبرز التحولات التي تركت آثارًا عميقة على مختلف جوانب الحياة، إذ أحدثت نمطًا متسارعًا للتعامل مع المعلومات والاتصالات، رافقته تحديات ومخاطر تمس سيادة الدول وحقوق الأفراد. فقد أوجدت هذه الثورة بيئة رقمية مفتوحة تيسر تبادل المعلومات والبيانات عبر الشبكات، وفي مقدمتها شبكة الإنترنت، غير أن هذه التطورات، رغم ما حققته من مزايا في مختلف المجالات، أفرزت في المقابل العديد من التحديات الأمنية والقانونية.¹

وفي هذا السياق، برز مفهوم الأمن المعلوماتي باعتباره أحد الركائز الأساسية لحماية البيانات والأنظمة الرقمية، ويقصد به مجموعة التدابير التقنية والقانونية والتنظيمية التي تهدف إلى ضمان سرية المعلومات وسلامتها وتوافرها، ومنع الوصول غير المشروع إليها أو التلاعب بها أو تعطيلها. وقد أصبح الأمن المعلوماتي ضرورة ملحة لحماية الأفراد والمؤسسات والدول في ظل التزايد المستمر للتهديدات السيبرانية وتطور أساليب الهجمات الإلكترونية.²

وقد تجلت هذه التحديات بشكل خاص في ظهور أنواع جديدة من الجرائم التي تستهدف الأنظمة المعلوماتية والبيانات الرقمية، ومن أبرزها جريمة التجسس الإلكتروني، التي أصبحت تشكل تهديدًا خطيرًا للأمن الشخصي والوطني على حد سواء.

¹ - عبد الفتاح بيومي حجازي، الحماية القانونية لأمن المعلومات عبر شبكة الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2007، ص 15.

² - عبد الفتاح بيومي حجازي، أمن المعلومات وحماية البيانات في عصر التكنولوجيا الرقمية، دار الفكر الجامعي، الإسكندرية، 2008، ص 21.

ويقصد بالتجسس الإلكتروني أي نشاط غير قانوني يستهدف اختراق الأنظمة المعلوماتية أو التقاط البيانات أو رصدها بدون إذن، بهدف الحصول على معلومات سرية أو حساسة. هذه الجريمة قد شهدت تطوراً مواكباً لتقدم التكنولوجيا، فهي لم تعد محصورة على الأفراد فقط، بل باتت تُمارس من قبل منظمات إجرامية وحتى كيانات رسمية، مما يزيد من حجم خطورتها وتعقيداتها.

وتكمن خطورة هذه الجريمة في أنها تنتهك خصوصية الأفراد، وتعرض الأمن الاقتصادي والسياسي للدول للخطر، بالإضافة إلى تأثيرها المباشر على الأمن الوطني.

في ظل هذه الظروف، بذلت مختلف الأنظمة القانونية المقارنة جهوداً لوضع إطار قانوني لمواجهة هذه الجرائم، عبر سن قوانين خاصة تتعلق بمكافحة الجرائم الإلكترونية وتحديد العقوبات المناسبة لها. تعد التشريعات الجزائرية من بين تلك التي تواكب هذا التقدم، حيث قام المشرع الجزائري بإدخال تعديلات على قانون العقوبات، إلى جانب سنّ قوانين خاصة تهدف إلى حماية أنظمة معالجة البيانات الآلية، ومكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات.¹

تسعى هذه الدراسة إلى الوقوف على النصوص التشريعية والأحكام القانونية الجزائرية المنظمة للجريمة الإلكترونية بصفة عامة وجريمة التجسس الإلكتروني بصفة خاصة ومعرفة مدى فعاليتها في التصدي للجريمة المعلوماتية والحد من خطورتها المتزايدة من خلال الكشف عن الأدلة والوسائل المستعملة التي ترتكب بها هذه الجريمة وكذا الوصول إلى مرتكبيها.

¹ - القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، سنة 2009،

إن اختيارنا لهذا الموضوع نابع من ميل شخصي للقانون الجنائي والاهتمام بالعلوم الجنائية ورغبتنا مني في إثراء المجال العلمي والأكاديمي وخصوصا المساهمة في ثراء ومواكبة التشريع الجزائري، لإيجاد الحلول القانونية لردع الجريمة المتصلة بالوساطة الالكترونية ومن اجل الدولة الجزائرية ومواطنيها.

كون جريمة التجسس الالكتروني بأنها من الجرائم المستحدثة في التشريع الجزائري وأنها من أحدث جريمة التي تعد خطيرة على السيادة الوطنية وتهدد امن الدولة الجزائرية، وكذا تمس بحريات وخصوصيات الافراد، ارتأينا ان ندرسها بدقة، من أجل ان نسلط الضوء على:

- النظرة التشريعية الجزائرية في معالجة ومواجهة الجريمة الالكترونية وخاصة جريمة التجسس الالكتروني،

-دراسة جريمة التجسس الالكتروني دراسة تحليلية بتوضيح الإطار المفاهيمي والقانوني، أركانها وخصائصها والآليات القانونية والإجرائية لمواجهتها.

وبناءً على ذلك، فإن دراسة جريمة التجسس الإلكتروني في القوانين الجزائرية تعتبر ذات أهمية كبيرة، بسبب تزايد الاعتماد على التكنولوجيا الرقمية في شتى المجالات، وما ينجم عن هذا من زيادة معدلات الجرائم الإلكترونية. تساهم هذه الدراسة أيضًا في إبراز مدى كفاية النصوص القانونية الراهنة في التصدي لهذا النوع من الجرائم، ومدى فاعليتها في تحقيق الردع العام والخاص.

تتمثل صعوبات الدراسة بشكل رئيسي في ضيق الوقت نظرا لتشعب موضوع الجرائم الإلكترونية وتسارعه، فهو موضوع يستحق وقتا أطول وتفرغا أكبر من أجل الإلمام بكل جزئياته.

وتكمن كذلك الصعوبات بمناسبة الدراسة، في قلة المراجع المتخصصة وخاصة الجزائرية في هذا الموضوع، سواءا من كتب أو أطروحات، وعلى هذا اعتمدنا أساسا

على أهم المصادر والمراجع المعتمدة والمتاحة لنا من، كتب ورسائل علمية جزائرية، رسائل دكتوراه وماجستير ومذكرات الماستر وبحوث ومقالات علمية وملتقيات دولية ووطنية منظمة في الجزائر، كذلك، اعتمدنا على منصات ومكتبات إلكترونية لجامعات جزائرية، كما تم الاعتماد على مواقع أنترنت عالمية متخصصة في الجريمة الإلكترونية والميدان السبراني.

وتتركز إشكالية دراستنا حول قدرة التشريع الجزائري على مواكبة التطور السريع لجريمة التجسس الإلكتروني، وذلك عبر طرحنا لهذا السؤال الرئيسي: إلى أي مدى نجح المشرع الجزائري في وضع إطار قانوني فعال لمكافحة جريمة التجسس الإلكتروني ومدى توصله لتفعيل هذه الآليات القانونية في مكافحة هذه الجريمة؟ والذي سنجيب عليه تحت مجموعة من التساؤلات الفرعية التالية:

- ما مفهوم جريمة التجسس الإلكتروني وأركانها؟

- وما هي صورها المتعددة؟

- وكيف تعامل معها المشرع الجزائري من الناحية الموضوعية والإجرائية؟

- هل العقوبات المقررة كافية لردع هذه الجريمة؟

ومن أجل هذا البحث العلمي، اعتمدنا أساسا على المنهج الوصفي التحليلي، وذلك من خلال وصف جريمة التجسس الإلكتروني وبيان خصائصها وأركانها القانونية. ثم تم تحليل النصوص التشريعية الجزائرية المنظمة لها، وتقييم مدى فعاليتها في مكافحتها. بالإضافة إلى المنهج الوصفي التحليلي، تم الاستعانة وتوظيف المنهج النقدي للكشف عن أوجه النقص والقصور التشريعي الجزائري، واقتراح الحلول والتوصيات المناسبة لتعزيز الحماية القانونية من جريمة التجسس الإلكتروني.

ومن أجل ذلك، قد قسمنا هذه الدراسة إلى فصلين رئيسيين؛ حيث يخصص الفصل الأول للإطار المفاهيمي والتجريمي لجريمة التجسس الإلكتروني، من حيث

تعريفها وخصائصها وأركانها وصورها، بينما يخصص الفصل الثاني لدراسة الأحكام القانونية لهذه الجريمة في التشريع الجزائري، من حيث النصوص المجرّمة والعقوبات المقررة، إضافة إلى الإجراءات المتبعة في الكشف عنها وملاحقة مرتكبيها.

وفي الأخير، يهدف موضوع مذكرتنا إلى تقديم تحليل قانوني دقيق لجريمة التجسس الإلكتروني، مع إبراز النقائص التي قد تشوب التشريع الجزائري في هذا الميدان، واقتراح بعض الحلول والتوصيات التي من شأنها تعزيز المنظومة القانونية الجزائية لمكافحة هذا النوع من الجرائم الخطيرة على الأمن والسيادة الوطنيين وكذلك خصوصيات الافراد، بحيث يتحقق التوازن بين حماية الأمن المعلوماتي وضمان الحقوق والحريات الفردية.

الفصل الأول:

الإطار المفاهيمي والتجريبي لجريمة
التجسس الإلكتروني

الفصل الأول

الإطار المفاهيمي والتجريمي لجريمة التجسس الإلكتروني

إن تشعب الوسائل الرقمية والتواصل الحديثة وتطور التكنولوجيا قد زاد من خطورة أفعال جريمة التجسس الإلكتروني وصعب من مهام الدول في حماية أمن مؤسساتها والبيانات ومحاربة الجرائم الإلكترونية والتصدي بالخصوص لجريمة التجسس عن طريق الآليات الإلكترونية، حيث أنه يصعب كشفها وإثباتها، بل وتتطلب استراتيجيات تقنية، تشريعات ومنظومة قانونية جادة لمواجهة، من أجل ولحماية أمن الدولة وخصوصية الأفراد في المجتمع.

فقد شهد العالم في السنوات الأخيرة عدة فضائح من جرائم التجسس الإلكتروني، هزت عدة دول العالم ومنها المتقدمة ولحققتها أضراراً جسيمة مستأمنها القومي ومؤسساتها، وكما تم اتهام دول أخرى إثر لجوئها إلى عمليات تجسس الإلكتروني، ونذكر هنا على سبيل المثال برنامج التجسس الإسرائيلي بيغاسوس للتجسس والتنصت والأمثلة كثيرة عن جرائم التجسس الإلكتروني.

ولدراسة هذه الجريمة قسمنا الفصل إلى مبحثين، سنتناول ماهية التجسس الإلكتروني وخصائصه (المبحث الأول)، وبعد ذلك سنتطرق إلى الأركان المكونة لجريمة التجسس الإلكتروني في القانون الجزائري (المبحث الثاني).

المبحث الأول

ماهية التجسس الإلكتروني وخصائصه

تعتبر الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الإطار التشريعي الأساسي الذي يندرج ضمنه التجسس الإلكتروني في الجزائر، على أساس أنها تعدّ من أبرز الجرائم المستجدة في وقتنا المعاصر، التي فرضتها الثورة الرقمية والتطور التكنولوجي المتسارع في استخدام الوسائط الإلكترونية.

وعليه سيتم الإلمام بمفهوم جريمة التجسس الإلكتروني في التشريع الجزائري من خلال تبين مفهوم التجسس الإلكتروني (المطلب الأول)، والتطرق إلى خصائصه وأهدافه (المطلب الثاني).

المطلب الأول

مفهوم جريمة التجسس الإلكتروني

مع التطور الرقمي المتسارع في عصرنا، إن استتغال ظاهرة التجسس الإلكتروني كنوع جديد من الجرائم الإلكترونية أو السيبرانية الخطيرة والتي تمس أمن الدولة وكيانها، والتي هي محل دراستنا، خصصنا هذا المطلب لتعريف التجسس الإلكتروني (الفرع الأول)، وذكر ما يميز هذه الجريمة عن الأعمال الإجرامية الأخرى، كالاختراق والسرقة المعلوماتية (الفرع الثاني).

الفرع الأول: تعريف التجسس الإلكتروني قانوناً ولغة واصطلاحاً وفقهاً

نتناول في هذا الفرع تعريف التجسس الإلكتروني لغة واصطلاحاً ومن الناحية القانونية ووجهة نظر الفقه.

(لا يوجد تعريف محدد للتجسس الإلكتروني، فالتجسس في حد ذاته كلمة متشعبة لا يمكن حصرها بتعريف واحد، إلا أنه يمكن أن نعرف التجسس الإلكتروني بأنه أحد صور الإرهاب الإلكتروني، يقوم باستخدام التكنولوجيا الضارة بشكل سلبي من أجل إحداث آثار مدمرة وأضرار بالغة وكبيرة لمحطات التحكم وأجهزة الكمبيوتر وشبكات الاتصال بدوافع سياسية أو عرقية أو دينية... ويمتد التجسس الإلكتروني إلى أبعد من هذا، حيث عرف أيضاً بأنه العدوان أو التخويف أو التهديد المادي أو

المعنوي باستخدام الوسائل الإلكترونية، الصادر من الدول أو الجماعات أو الأفراد على الإنسان بغير حق.¹

لقد تطرق الأستاذ أمير فرج يوسف الى شرح مدلول التجسس الالكتروني على أنه من " جرائم الكمبيوتر ضد الحكومة": (وتشمل هذه الطائفة كافة جرائم تعطيل الاعمال الحكومية، وتنفيذ القانون، والإخفاق في الإبلاغ عن جرائم الكمبيوتر، والحصول على معلومات سرية، والإرهاب الالكتروني وغيرها).²، وأدرجه ضمن خانة المخاطر الأمنية وهو من الاعمال الإرهابية الالكتروني، فحسب رأيه هو (الاعتداء على سرية المعلومات الموجودة على الحاسوب دون إذن صاحبها....)³.

(ان التجسس الالكتروني أو ما يعرف بحرب التجسس المعلوماتي، هو عبارة عن عدة طرق لاختراق المواقع الالكترونية ومن ثم سرقة بعض المعلومات او بأكملها والتي قد تكون في غاية الأهمية والخطورة للطرف المتلقي والمسروق منه وقد انتشرت في الالفية الجديدة بانتشار طرق الاختراق).⁴

وكما تم تعريفه أيضا، بأنه التلصص وسرقة المعلومات من الأفراد أو المؤسسات أول الدول أو المنظمات، والتجسس على هذه المعلومات أيا كان نوعها

¹ - نجاري بن حاج علي فايزة، دراسة جريمة التجسس الإلكتروني، مجلة ستراتيجيا، جامعة مولود معمري، تيزي وزو، مجلد 16، العدد 11 السداسي الأول 2019، ص64.

² - أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، بدون طبعة، دار المطبوعات الجامعية الإسكندرية، مصر، 2008، ص51.

³ - أمير فرج يوسف، مرجع سابق، ص60.

⁴ - أوشان حنان، وادي عماد الدين، التجسس الالكتروني واليات مكافحته في التشريع الجزائري، العدد الثاني، جويلية 2014، ص132.

يأخذ أبعاداً جديدة، فتعددت أهدافها من معلومات اقتصادية إلى معلومات سياسية وعسكرية وشخصية.¹

لا يختلف التجسس الإلكتروني عن التجسس التقليدي إلا في الأداة المستخدمة وهي تكنولوجيا المعلومات التي وفرت للجاسوس الإلكتروني الحرية والسهولة في التجسس بعيداً عن أعين الرقيب، بحيث أشار الأستاذ يوسف صغير إلى أن التجسس الواقع في الإنترنت على أمن الدولة أنه: (يقوم قراصنة الحاسوب باختراق المواقع أو الحواسيب الإلكترونية، باستخدام برامج للتجسس على شبكات والأنظمة الإلكترونية، والاعتداء على البنية التحتية للمؤسسات الحكومية والخاصة على حد سواء).²

وقد تباينت التعريفات القانونية للتجسس الإلكتروني بين من جعله عاماً يشمل الأفراد والجماعات والدول، وبين من حصره في نطاق الدولة وأسرارها فقط دون الأفراد، ولذلك عرفه الفريق الأول بأنه: (الاطلاع على معلومات خاصة بالغير محفوظة على جهاز إلكتروني وليس مسموحاً لغير المخولين بالاطلاع عليها، بينما عرفه الفريق الثاني بأنه: استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الإلكترونية الخاصة بالدول والحكومات والتتصت عليها بقصد الحصول على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها، تشمل جميع المعلومات العسكرية والأمنية، والسياسية، والاقتصادية، والعلمية، والاجتماعية).³

¹ - سامية بوشوشة، حياة سالماني، التجسس الإلكتروني وطرق مكافحته، مجلة العلوم الاجتماعية، مجلد 16، عدد 01، 2023، ص 52.

² - يوسف صغير، جرائم الأنترنت جرائم، حقيقية في عالم افتراضي، مجلة معارف لجامعة البويرة مجلد 17، عدد 2، 2022، ص 222.

³ - سامية بوشوشة، حياة سلاماني، مرجع سابق، ص 53.

أولاً- تعريف التجسس الإلكتروني من الناحية القانونية

إذا رجعنا لقانون العقوبات الجزائري سنلاحظ أن المشرع الجزائري لم يعطنا تعريفاً واضحاً ودقيقاً لجريمة التجسس الإلكتروني على خلاف التجسس التقليدي، لكن فيما بعد نص على تجريم التجسس الإلكتروني ومن بين مجموعة الأفعال المكونة لهذه الجريمة من خلال تعديل قانون العقوبات سنة 2024 وذلك ليواكب التطور الذي مس المجال التقني.¹

حيث وضع المشرع الجزائري القانون رقم 04-15 المعدل والمتمم لقانون العقوبات، الذي يجرم الأفعال التي ترتكب بواسطة الوسائل التقنية لأول مرة تحت اسم جرائم الماسة بأنظمة المعالجة الآلية للمعطيات من المادة 394 مكرر إلى غاية المادة 394 مكرر 2.7²

وينص مضمون المادة 394 مكرر 2 على أن: (تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد).³

يفهم من نص هذه المادة أنه إذا ارتكبت إحدى الجرائم الماسة بأمن الدولة من بينها التجسس باستخدام أنظمة المعالجة الآلية للمعطيات فإنه تطبق عليها عقوبة

¹ - نادية سلامي، آليات مكافحة التجسس الإلكتروني، رسالة دكتوراه، جامعة العربي التبسي، كمية الحقوق والعلوم السياسية، 2019، ص 23.

² - إلهام بن خليفة وجمال غريسي، التجسس الإلكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري، مجلة دفاتر السياسة والقانون، مجلد 14، عدد 01، 2022، ص 155.

³ - المادة 394 مكرر 2، قانون 04-15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66 - 156، المتضمن قانون العقوبات، جريدة رسمية عدد 71.

أشد، لأن جرائم المساس بأمن الدولة تكون عقوبتها أشد من العقوبات المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر^{1.2}.

يستخلص من مواد القسم السابع مكرر الذي ذكر سابقا أن الأفعال المكونة لجريمة التجسس الإلكتروني، يتمحور هدفها في الإضرار والمساس بالدفاع الوطني والأمن القومي وتتمثل في فعل الدخول والبقاء في المنظومة المعلوماتية وتخريبها أو إدخال أو إزالة أو تعديل المعطيات أو تصميم أو بحث أو توفير أو تجميع أو نشر أو الإتجار في المعطيات سواء كانت مخزنة أو معالجة أو مرسلّة بواسطة المنظومة المعلوماتية².

ولم ينص القانون الجزائري على توقيع عقوبة الإعدام على جريمة التجسس الإلكتروني صراحة، بل اكتفى بتسليط عقوبة الإعدام في الجرائم العادية على الجاسوس الاجنبي والتي تضمنتها المادة 64 من ق.ع.ج في نصها³.

أما المواطن الذي يحمل الجنسية الجزائرية وفي حالة ارتكابه جريمة الخيانة وأفعال التي تضمنها الفصل الأول "الجنايات والجناح ضد أمن الدولة" في القسم الأول من "جرائم الخيانة والتجسس"، أقر المشرع الجزائري على تسليط عقوبة الإعدام، على كل جزائري وكل عسكري أو بحار في خدمة الجزائر يرتكب فعل جريمة الخيانة. فجريمة الخيانة تشكل اعتداء مباشرا ومؤثرا على الوجود السياسي للدولة، بل يهدد وجودها ككيان سياسي دولي وتشكل خطرا على استقلالها وسلامة إقليمها أو

¹ - إلهام بن خليفة وجمال غريسي، مرجع السابق، ص 155.

² - هبة نبيلة هروال، جرائم الانترنت، دراسة مقارنة، رسالة دكتوراه، جامعة أبي بكر بالكايد، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2014، ص 376.

³ - المادة 64، القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006: يرتكب جريمة التجسس ويعاقب بالإعدام كل أجنبي يقوم بأحد الأفعال المنصوص عليها في الفقرات 2 و3 و4 من المادة 61 وفي المادتين 62 و63.

ويعاقب من يحرض على ارتكاب إحدى الجنايات المنصوص عليها في هذه المادة والمواد 61 و62 و63 أو يسهل ارتكابها بالعقوبة المقررة لها.

الانتقاص من سيادتها وتهديدا لنطاقها الحيوي الخارجي...، ونظرا لتعدد مظاهر وأشكال جرائم الخيانة فقد عالجها المشرع في المواد 61 و62 و63 من قانون العقوبات الجزائري.¹

ثانيا: التعريف اللغوي للتجسس الإلكتروني

التجسس الإلكتروني أو السبراني هو مصطلح مركب يجمع بين "التجسس" كفعل و "الإلكتروني" كوسيلة، فكلمة التجسس في اللغة يعني البحث عن شيء، فيقال جس أو اجتس أو تجسس الاخبار أي بحث عنها وتقصاها، ويعني كذلك التفتيش عن بواطن الأمور،² اما كلمة الإلكتروني فهي مشتقة من "إلكترون"، وهو ما يتعلق بالتقنيات الحديثة، الحاسب الآلي، وشبكات الاتصال، والإنترنت.³

ثالثا: التعريف الاصطلاحي للتجسس الإلكتروني

اما التجسس في معناه الاصطلاحي يقصد به البحث والتتقيب عما يتعلق بالعدو من معلومات سرية باستخدام الوسائل السرية والفنية او العملاء والجواسيس من اجل نقل هذه المعلومات للاستفادة منها في اعداد الخطط.⁴

¹ - بن مكي نجا، محمود بوقطف، الخيانة العظمى جريمة ماسة بأمن الدولة في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، مجلد 1، عدد 1، 2014، ص 126.

² - بوجوراف عبد الغني، التجسس كجريمة ماسة بأمن الدولة في ظل قانون العقوبات الجزائري، مجلة افاق للعلوم، جامعة الجلفة، مجلد 2، عدد 8، 2017، ص 339.

³ - **Cyber espionage:** Cyber espionage, cyber spying, or cyber-collection is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information using methods on the Internet, networks or individual computers through the use of proxy servers,[1] cracking techniques and malicious software including Trojan horses and spyware, https://en.wikipedia.org/wiki/Cyber_espionage , Lu 01h:00,22-03-2026.

⁴ - هاشمي رشيد وملياني عبد الوهاب، المواجهة التشريعية لجريمة التجسس الإلكتروني في ظل القانون 06-24، المجلد التاسع، العدد الأول، 2005، ص 540.

وانطلاقاً من التعريف السابق للتجسس، فإن التجسس الإلكتروني أو ما يعرف بحرب التجسس المعلوماتي هي عبارة عن عدة طرق لاختراق المواقع الإلكترونية ومن ثم سرقة بعض المعلومات والتي قد تكون في قائمة الأهمية والخطورة للطرف المتلقي المسروق منه.¹ وقد عرفته مدونة SentinelOne المتخصصة في الأمن السيبراني بأنه: (يُعد التجسس الإلكتروني أحد أخطر التهديدات في عالم متصل ورقمي بشكل متزايد).²

¹ – **Idem:** Cyber spying typically involves the use of such access to secrets and classified information or control of individual computers or whole networks for a strategic advantage and for psychological, political, and physical subversion activities and sabotage, Lu 1:30, 22-03-2026.

² – <https://www.sentinelone.com/> : Le cyberespionnage consiste à accéder sans autorisation à des informations confidentielles dans le but probable d'obtenir un avantage stratégique, politique ou financier. Ce type d'espionnage s'effectue dans le domaine numérique. Il est principalement mené par des groupes soutenus par des États ou des pirates informatiques indépendants qui infiltrent des systèmes informatiques, des réseaux ou des appareils dans le but de voler des informations sensibles, Lu 2h:40, 22-03-2026.

رابعاً: التعريف الفقهي للتجسس الإلكتروني

يتميز التجسس بالتطور والتغير لذلك من الصعب إيجاد تعريف موحد ومضبوط له، فهناك تعريف تقليدي له وتعريف حديث للتجسس، فالتعريف الفقهي التقليدي يعرفه بأنه: التجسس يتمثل في الحصول وتجميع معلومات سرية حول السياسة أو المواد العسكرية والتنظيم الدفاعي أو الهجومي لدولة أجنبية وتسليم هذه المعلومات إلى دولة أجنبية أخرى. أما التعريف الحديث للتجسس فيعرفه بأنه: نقل أو إفشاء خبر أو أمر من الأمور التي تعتبر سرا من أسرار الدولة، وكان من شأن ذلك الإضرار بمصلحة هذه الدولة، إلى أي جهة خارجية.¹

الفرع الثاني: تمييز التجسس الإلكتروني عن الاختراق والسرقة المعلوماتية

سوف نتطرق في هذا الفرع إلى ما يميز جريمة التجسس الإلكتروني عن الأعمال الإجرامية الأخرى المشابهة، كالاختراق والسرقة المعلوماتية، وسنقوم بتعريف كل فعل على حدة مع مقارنة أوجه الاختلاف مع التجسس الإلكتروني.

من التدقيق والملاحظة يظهر أن فعل التجسس الإلكتروني يتميز بالمراقبة والاستطلاع، وأنه يمكن أن يكون الاختراق خطوة أولى للتجسس أو السرقة، بينما السرقة المعلوماتية تتميز بالاستيلاء ونقل البيانات، والاختراق وهو كسر حماية النظام والدخول.

بحيث نظم المشرع الجزائري جرائم المعلوماتية والتقنيات الحديثة عبر نصوص متفرقة، أبرزها قانون العقوبات المعدل، خاصة المواد 394 مكرر وما يليها والقانون رقم 04-09.

¹ - بوجوراف عبد الغني، نفس المرجع، ص 339.

ان التمييز بين التجسس الإلكتروني، الاختراق، والسرقعة المعلوماتية يقوم على الهدف من الجريمة-القصد الجنائي والركن المادي.¹

ميز المشرع الجزائري في قانون العقوبات المعدل والمتمم في المواد 394 مكرر وما يليها، بين جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، بحيث تشكل كل من التجسس الإلكتروني، الاختراق، والسرقعة المعلوماتية أنماطاً مختلفة كل فعل على حدة من حيث الهدف والوسيلة والنتيجة، هذا وإن اشتركت في استخدام الوسائل التقنية.

أولاً: فعل الاختراق - الدخول والبقاء غير المشروع

فعل الاختراق/ الدخول والبقاء غير المشروع هو عبارة عن عملية دخول غير مصرح به إلى أجهزة أو شبكات إلكترونية، ويتم هذا بواسطة برامج متطورة يستخدمها كل من يملك الخبرة والقدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت لحماية تلك الحاسبات أو الشبكات.² إن هدف الاختراق هو التسلل وهو الدخول إلى نظام معالجة آلية للمعطيات حاسوب، شبكة أو البقاء فيه عن طريق الغش دون وجه حق، أو عبر التحايل وتجاوز تدابير الحماية، ويظهر الركن المادي لهذا الفعل من خلال فعل الدخول والبقاء في النظام، أما القصد الجنائي فيقع بمجرد مجرد الدخول غير المصرح.

أما التكييف القانوني والتجريمي الذي اقره المشرع الجزائري لهذا الفعل، يظهر في مضمون نص المادة 394 مكرر من قانون العقوبات والتي اقرت عقوبة الحبس

¹ - موقع <https://asjp.cerist.dz> ، تم التصفح على ساعة 16:00.

² - عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر مهني، جامعة قاصدي مرباح ورقلة، كلية العلوم الاقتصادية والعلوم التجارة وعلوم التسيير، قسم علوم التسيير، 2019، ص 8.

من شهرين إلى سنتين وغرامة مالية¹، وكما شدد وضاعف العقوبة إذا ترتب ذلك حذف أو تغيير لمعطيات المنظومة.²

ثانيا: فعل السرقة المعلوماتية - الاستيلاء على البيانات

إن الهدف من فعل الاختلاس/الاستيلاء على البيانات هو الحصول على معطيات أي النصب، وهي عملية اختلاس أو نقل أو استخدام بيانات ومعطيات معلوماتية (ملفات، أموال رقمية، برامج) من نظام معالجة آلي دون رضا صاحبها دون وجه حق، بالتالي، كذلك، يمكن القول ان فعل السرقة المعلوماتية/الاستيلاء على البيانات هو نقل الملكية المعلوماتية إلى الجاني، مما يترتب عليه خسارة للضحية وكسب غير مشروع للجاني. ومما سبق ذكره، نلاحظ انه يجب وقوع شرط فعل التعديل والمحو ونقل للمعلومات والبيانات لاكتمال الركن المادي.

اما التكييف القانوني فنجد في مضمون نص المادة 394 مكرر¹، حيث يعاقب على: (كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها)³ والتي اقرت عقوبة الحبس من سنة إلى ثلاث سنوات وغرامة مالية.⁴

¹ - المادة 394 مكرر: (يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 ألف دج إلى 200,000 ألف دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100,000 ألف دج إلى 300,000 ألف دج)، قانون العقوبات الجزائري، المعدل والمتمم بقانون 06-24 مؤرخ في 28 افريل 2024.

² - تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100,000 ألف دج إلى 300,000 ألف دج)، نفس المادة، الفقرة الثانية.

³ - المادة 394 مكرر¹، قانون العقوبات الجزائري، المعدل والمتمم بقانون 06-24 مؤرخ في 28 افريل 2024.

⁴ - المادة السابقة الذكر.

المطلب الثاني

خصائص التجسس الإلكتروني وأهدافه

بعدما تطرقنا الى مفهوم التجسس الإلكتروني كنوع جديد من الجرائم الالكترونية المستحدثة في التشريع الجزائي الخطيرة والتي تمس أمن الدولة وكيانها، بتعريفه الواسع، وذكر ما يميز هذه الجريمة عن الاعمال الاجرامية الأخرى، كالاختراق والسرقة المعلوماتية، سنتناول في هذا المطلب الثاني خصائص التجسس الإلكتروني (الفرع الأول)، ثم نتطرق الى أهدافه في (الفرع الثاني).

الفرع الأول: الخصائص-العابرة للحدود، صعوبة الإثبات، سرعة التنفيذ والتخفي، قلة الإبلاغ عنها، محل وقوع جريمة التجسس الإلكتروني

نتطرق في هذا الفرع لخصائص التجسس الإلكتروني، ويختلف هذا النوع من التجسس عن الجرائم السيبرانية في كونه غير مدفوع بالربح المادي الفوري، بل يركز على جمع المعلومات بعيدة المدى. ويختص التجسس الإلكتروني بمجموعة من الخصائص والمميزات التي يشترك فيها بصيغة شاملة مع الجريمة المعلوماتية وفيما يلي أبرز خصائصه.¹

أولاً: جريمة عابرة للأوطان-للحدود

نظرا للوسيلة المستعملة فيها وهي أجهزة الكمبيوتر، جعل من هذه الجريمة عابرة للحدود، لا ترتبط بإقليم جغرافي معين، تكفي توفر جهاز حاسوب في أي مكان في الكرة الأرضية، يكون مزودا بالشبكة المعلوماتية لارتكاب جريمة معلوماتية. هذا الوضع جعل أمام الدول اللجوء إلى حتمية التعاون والتنسيق الدوليين من أجل مكافحة هذه الجرائم بكافة الوسائل المتاحة بداية من خلال إبرام اتفاقيات ومعاهدات دولية،

¹ - <https://www.sentinelone.com/fr/cybersecurity-101/threat-intelligence/cyber-espionage>، Lu

وفتح المجال واسعا للقيام بإجراءات التحري والتدقيق اللازمين لكشف مرتكبي هذه الجرائم من خلال تحديد القانون الواجب التطبيق في هذه الحالات، وتحديد الدولة صاحبة الاختصاص القضائي.¹ إن الحديث عن صفة العالمية للجريمة المعلوماتية ارتبط بالتقنيات الحديثة، وما صاحبها من تطور في مجال الاتصال بحيث ألغى الحدود الجغرافية بين الدول، فتخطت بذلك الجريمة المعلوماتية حدود الدولة التي ترتكب فيها لتتعدى آثارها إلى عدة بلدان على مستوى العالم، فالتقنيات المتصلة عالميا قد جعلت من هذه الجريمة عابرة للحدود، وعليه فالطبيعة العالمية تمكن الجاني من ارتكاب الجريمة في دولة ما، وتؤثر على المجني عليه في دولة أخرى.²

إن جريمة التجسس الإلكتروني تشترك في الخصائص مع الجرائم الإلكترونية الأخرى فهي من أنواعها، وجريمة التجسس الإلكتروني لا تعترف بالحدود الجغرافية للدول، فهي عالمية، حيث يتم تنفيذها من مواقع بعيدة، ويتميز التجسس الإلكتروني بأنه عمل سري للغاية وطويل الأمد، لا يهدف لإحداث اضطراب مباشر، بل جمع معلومات استخباراتية.³

ثانيا: جريمة صعبة الإثبات

إثبات الجرائم الإلكترونية التي تمتاز بالنعومة و من بينها التجسس الإلكتروني، يواجه تحديات كبيرة نظرا لصعوبة تتبعها وكشفها، هذه الجرائم التي تتخذ شكل رقمي و افتراضي بحث، لا تترك أدلة ملموسة يمكن تتبعها، مما يجعل اكتشافها أمرا صعبا و عشوائيا في كثير من الأحيان وقد يحدث بعد فترة طويلة من وقوعها،

¹ - بن دراح علي إبراهيم، محاضرات في الجرائم المعلوماتية للسنة الثانية ماستر، معهد العلوم الحقوق والعلوم السياسية، قسم الحقوق، المركز الجامعي أفلو، الجزائر، 2020/2021، ص 7.

² - شوقي يعيش تمام، الجريمة المعلوماتية: دراسة تأصيلية مقارنة، مخبر أثر الاجتهاد القضائي على حركة التشريع، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الطبعة الأولى، 2019، ص 29.

³ - نجاري بن حاج علي فايزة، جريمة التجسس الإلكتروني، دراسة، ستراتيغيا، مجلة دراسات الدفاع ولاستقباله، العدد 11، السادس الأول، 2019، ص 68.

بالإضافة إلى ذلك، تفتقر هذه الجرائم إلى الأدلة المادية التقليدية مثل بصمات الأصابع، من ناحية أخرى، يتطلب التحقيق في جرائم المعلوماتية مهارات فنية متخصصة نادرا ما تتوفر لدى المحققين العاديين، مما يزيد من صعوبة التعامل معها، علاوة على ذلك...¹

لقد عرف عن التجسس الإلكتروني أنه لا يترك أي دليل مادي بعد ارتكاب الفعل الإجرامي ما يصعب معه عملية التعقب واكتشاف الجريمة أساسا. - إن التجسس الإلكتروني يحدث في بيئة هادئة لا تحتاج إلى القوة والعنف واستعمال الأسلحة، وإنما ما يحتاجه هو جهاز كمبيوتر وبعض البرامج وشبكة انترنت. - سهولة محو وإتلاف الأدلة التي من شأنها أن تؤدي إلى العثور واكتشاف مرتكب الفعل الجرمي والتمكن من إدانته...²، وهناك صعوبات أخرى أيضا تكمن في صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، إذ يستطيع المجرم المعلوماتي في أقل من ثانية أن يمحو أو يحرف، أو يغير البيانات و المعلومات الموجودة في الكمبيوتر، لذا فإن المصادفة وسواء الحظ دورا في اكتشافها، يفوق دور أساليب التدقيق والرقابة، ومعظم مرتكبيها الذين تم ضبطهم وفقا لما لاحظته أحد الخبراء في الجريمة المعلوماتية، إما أنهم تصرفوا بغباء، أو لم يستخدموا الأنظمة المعلوماتية بمهارة.³

ثالثا: جريمة سريعة التنفيذ والتخفي

لا شك في أن سرعة التنفيذ تمثل أحد أهم خصائص الجريمة السيبرانية، حيث يمكن للمجرم الجاسوس السيبراني تنفيذ الجريمة بسرعة فائقة إما من خلال استخدام

¹ - مقرر عبد الرؤوف، التجسس السيبراني الماس بأمن الدولة في التشريع الجزائري، مذكرة ماستر، جامعة برج بوعرييج، كلية الحقوق والعلوم السياسية، 2024، ص 11.

² - سامية بوشوشة، حياة سالماني، التجسس الإلكتروني وطرق مكافحته، مجلة العلوم الاجتماعية، مجلد 16، عدد 01، 2023، ص 54.

³ - عثمانى رضوان، مكافحة جرائم المعلوماتية في القانون الجزائري والدولي، رسالة دكتوراه، جامعة وهران 2-محمد بن أحمد، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2024، ص 15.

برامج مصممة خصيصا لهذا الغرض، بحيث يستخدم الجناة تقنيات متطورة مثل التشفير والشبكات المظلمة لإخفاء هويتهم ومكانهم. هذا الأسلوب يسمح للمجرم بالتحرك بسيرورة وبشكل خفي خارج مكان الجريمة مما يجعله غير ملحوظ.

يترتب على الخصائص المتقدمة المتعلقة بدولية هذه الجريمة، وصعوبة اكتشافها وهدوئها، ان هذه الجريمة يصعب إثباتها، وهذه الصعوبة راجعة إلى عدد من الأسباب، منها أنها جريمة لا تترك آثار مادية ملموسا، فضلا عن وقوعها في الغالب من قبل مجرمين محترفين، ... الجاني في هذه الجرائم في الغالب يقوم بإخفاء أو تدمير دليل إدانته في ثانية واحدة، مما يضيع معه دليل أو أدلة الجريمة، إضافة إلى أن هذا الجاني لا يقوم بمهاجمة ماديات جهاز الحاسب كما الجريمة التقليدية حتى يمكن القبض عليه، بل أنه يرتكب جريمته من خلال هذا الجهاز متخفيا، وربما يكون في دولة أخرى أو قارة أخرى.¹

رابعا: جريمة يقل الإبلاغ عنها

يعتبر عدم الإبلاغ عن الجرائم المعلوماتية من اهم العوامل التي تعيق اكتشافها وإثباتها، إن ضحايا هذه الجرائم يلعبون دورا هاما و رئيسيا في الإبلاغ عنها عند اكتشافها، فنجد العديد من الجهات (ضحايا) التي تتعرض لانتهاك أنظمتها المعلوماتية و تتكبد خسائر، يترددون في الإبلاغ عنها في حالة اكتشافها و تفضل عدم الكشف عنها حتى لموظفيها، بل تكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ للسلطات المختصة، ذلك لتجنب الضرر بسمعتها و الثقة في كفاءاتها، وبالتالي، يكون الإبلاغ عن هذه الجرائم قليلا مقارنة بالجرائم الأخرى، و هذا يعود الى المخاوف من التشهير و التأثير السلبي على سمعة المجني عليه في حالة الإبلاغ عن الجريمة.² بحيث يلجأ الضحايا الى الإحجام عن الإبلاغ عن هذه الجرائم في حال اكتشافها لخشية

¹ - عثمانى رضوان، نفس المرجع، ص 17.

² - مقرح عبد الرؤوف، نفس المرجع، ص 12.

المجني من فقد ثقة عملائها، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة.¹

خامسا: محل وقوع جريمة التجسس الإلكتروني

يُعد محل وقوع جريمة التجسس الإلكتروني في التشريع الجزائري من المسائل المعقدة نظراً لطبيعتها الافتراضية العابرة للحدود. بحيث يركز المشرع الجزائري على حماية أنظمة المعالجة الآلية للمعطيات (نظم المعلومات) بصفة عامة، وأسرار الدفاع الوطني بصفة خاصة.² إن محل الجريمة هو الشيء الذي ينصب عليه سلوك الجاني، انه السلوك المادي الذي يحدثه إزاء الدخول والتلاعب بالبيانات، المعلومات، النظام، ويشمل أنظمة المعالجة الآلية للمعطيات: تشمل الخوادم، الشبكات، أجهزة الحاسوب، ومواقع الإنترنت التابعة لمؤسسات الدولة، البنوك، أو الأفراد وأسرار الدفاع الوطني والاقتصاد الاستراتيجي: المعلومات الحساسة، الوثائق الرقمية، والخرائط العسكرية، حيث يشكل المساس بها جريمة تجسس ضد أمن الدولة و البيانات الشخصية: المعلومات المتعلقة بالأشخاص الطبيعيين في حال تم معالجتها بشكل غير مشروع.³

إن محل وقوع جريمة التجسس الإلكتروني هو الفضاء الافتراضي وليس مكاناً مادياً محدداً، حيث تتم عبر اختراق شبكات المعلومات، أنظمة المعالجة الآلية

¹ - عثمانى رضوان، المرجع السابق، ص 17.

² - <http://dspace.univ-skikda.dz> ، <http://dspace.univ-skikda.dz:4000/handle/123456789/2992> ، تم التصفح

2026-04-20 ، الساعة 1:00 .

³ - محمد خليفة، خصوصية الجريمة الالكترونية، وجهود المشرع الجزائري في مواجهتها، كلية الحقوق والآداب والعلوم الاجتماعية- جامعة 08 ماي 45 قالمه، موقع aspj، ص 343.

للبيانات، أو الشبكات السلكية واللاسلكية. قد تقع الجريمة في مكان غير مكان البث، حيث يتم اعتراض البيانات والوصول إليها عن بعد.¹

الفرع الثاني: أهداف التجسس الإلكتروني

يعتبر التجسس الإلكتروني أحد أبرز التهديدات السيبرانية الماسة بأمن الدول واقتصادها وخاصة الشركات في هذا العصر الرقمي، وهو عملية اختراق غير مشروع لأنظمة الحاسوب والشبكات لسرقة البيانات والمعلومات الحساسة، وغالباً ما يكون مدعوماً من دول أو مجموعات منظمة.² وتعد عملية التجسس أداة محورية في سياسات الدول منذ الأزل. حيث، مع تسارع التطور التكنولوجي وزيادة الاعتماد على الأنظمة الرقمية في شتى ميادين الحياة والتي أصبحت جزءاً لا يتجزأ من حياتنا اليومية، هذا الأمر أدى إلى بروز تحديات جديدة ازدادت معها المخاطر المصاحبة لها، مما فتح الباب أمام ظهور جريمة التجسس الإلكتروني، كأداة ناعمة للوصول إلى النتائج المرجوة، بحيث اشتد التنافس والتصادم خاصة بين الدول الكبرى.

وفي سياق أكاديمي، يمكن تصنيف أهداف التجسس الإلكتروني إلى ثلاثة محاور رئيسية والتي تشكل أعمدة الأمن القومي والقوة الدولية والتي سنتطرق إليها على التوالي.

أولاً: أهداف التجسس الإلكتروني السياسية

يهدف التجسس الإلكتروني في الميدان السياسي إلى تحقيق نفوذ استراتيجية ومن أجل اتخاذ قرارات دقيقة، أو إضعاف الخصوم. ومن الأهداف أيضاً، الاطلاع على الخطط الاستراتيجية والدبلوماسية عن طريق سرقة المراسلات الحكومية، وتقارير الاستخبارات، والسياسات الخارجية للدول المنافسة.

¹ - <https://asjp.cerist.dz/en/article/217145#> , lu le 26-03-2026, 23:00 .

²- <https://orionpolicy.org/cyber-espionage-and-u-s-policy-responses#/>, lu, 24-04-2026,20:56 .

وفي نفس السياق، ومن بين أهداف التجسس الإلكتروني، التدخل في العمليات السياسية لغاية التأثير على نتائج الانتخابات، أو التلاعب بالرأي العام في الدول المستهدفة، والابتزاز السياسي من أجل الحصول على معلومات حساسة تخص مسؤولين حكوميين لاستخدامها كأوراق ضغط، ولعل أحسن مثال في الموضوع هو التقرير الذي حذر من خلاله مسؤولو خبراء مجمع الاستخبارات الأمريكية CIA، أعضاء الكونغرس من أن روسيا تتدخل في الانتخابات الرئاسية لعام 2020 في محاولة لإعادة انتخاب ترامب.¹ ويعد أيضا جمع معلومات عن الوفود المفاوضة لمعرفة مواقف الدول الأخرى في المفاوضات الدولية (الاقتصادية، العسكرية، السياسية) للحصول على ميزة تفاوضية، كأداة ضغط.²

ثانيا: أهداف التجسس الإلكتروني العسكرية

يركز التجسس العسكري على جمع معلومات استخباراتية فورية تهدف إلى التفوق الميداني والردع.

ويرتكز التجسس على سرقة التكنولوجيا الدفاعية للحصول على تصميمات الأسلحة المتطورة، وأنظمة الدفاع الصاروخي، والبحوث العسكرية السرية وتتبع التحركات العسكرية ومراقبة تحركات القوات، والسفن، والطائرات، والتجسس على خطط الحروب والعمليات.

وكما يعتمد التجسس الإلكتروني على اختراق قيادات الدفاع من أجل استهداف وزارة الدفاع، وأجهزة الاستخبارات، والمقاولين الدفاعيين للحصول على معلومات موثقة

¹ – Desiderio, Andrew, Politico, **Russian interference in the 2020 United States elections**.

https://en.wikipedia.org/wiki/Russian_interference_in_the_2020_United_States_elections, consulté 26-03-2026, 23h:15.

² – <https://www.sentinelone.com/fr/cybersecurity-101/threat-intelligence/cyber-espionage/>

consulté le 29-03-2026, 20:h56.

وتجهيز ساحة المعركة وتحديد نقاط الضعف في شبكات القيادة والسيطرة للعدو لتسهيل ضربها في حال نشوب نزاع.¹

ثالثاً: أهداف التجسس الإلكتروني الاقتصادية والصناعية

يهدف التجسس الإلكتروني في الميدان الاقتصادي والصناعي إلى سرقة الملكية الفكرية والأسرار التجارية لمنح الشركات الوطنية أو الدولة ميزة تنافسية في السوق العالمي.² ومن بين العمليات التي تنفذ عن طريق التجسس الإلكتروني، نذكر سرقة الملكية الفكرية والأسرار التجارية: الاستيلاء على بحوث التنمية، وصفات المنتجات، وتصاميم الآلات، والخطط التسويقية للشركات المنافسة. ومن أجل سد الفجوة التكنولوجية يتم استخدام البيانات المسروقة لتطوير صناعات وطنية بسرعة دون الحاجة لاستثمار وقت وتكلفة في البحث والتطوير الاستحواذ على البيانات المالية بغية الوصول إلى المعلومات البنكية، والتعاقدات، ومصادر التمويل الخاصة بالشركات المنافسة أو البنوك، كذلك يستهدف التجسس الإلكتروني سلاسل الإمداد باختراق شركات أصغر أو أطراف ثالثة (Suppliers) للوصول إلى بيانات الشركات الكبرى كما في هجوم (SolarWinds).³

المبحث الثاني

الأركان المكونة لجريمة التجسس الإلكتروني

يتناول هذا المبحث العناصر الجوهرية التي تقوم عليها جريمة التجسس الإلكتروني، وهي الأركان القانونية التي لا تكتمل الجريمة ولا تترتب عنها المسؤولية الجزائية إلا بتوافرها مجتمعة، بدءاً من الأركان الثلاثة الأساسية و العامة ، المتمثلة في الركن الشرعي-النص القانوني و الركن المادي المتمثل في السلوك المادي

¹ - المرجع السابق.

² - <https://www.investopedia.com/terms/i/industrial-espionage.asp> #, consulté 29-03-2026, 20h :56.

³ - <https://skillogic.com/blog/what-is-cyber-espionage-in-cyber-security-types-prevention/>

consulté ,29-03-2026, 21:40.

للجريمة وهو مظهرها الخارجي، و الركن المعنوي الذي يجسد نية المعتدي وقصده الجنائي في اختراق الخصوصية أو المساس بأمن المعلومات، (المطلب الأول) و وصولاً الى الركن المستحدث فقهاً وهو- الركن الافتراضي المتمثل في البيئة الرقمية مثل الإنترنت والأجهزة الحاسوبية، مكان حدوث الجريمة وأداتها التنفيذية، (المطلب الثاني).

المطلب الأول

الأركان العامة لجريمة التجسس الإلكتروني

لقيام جريمة ما، لا بد أن تتوفر مجموعة من الأركان الأساسية التي يشكلها البناء القانوني لأي جريمة. وتتمثل هذه الأركان في الأساس بالركن الشرعي والركن المادي والركن المعنوي. ومن خلال هذه الأركان يتم تحديد المسؤولية الجزائية للشخص الذي يقوم بالجريمة. سنتناول هذا المطلب في ثلاثة فروع، الركن الشرعي- النص القانوني (الفرع الأول)، والركن المادي (الفرع الثاني)، والركن المعنوي في (الفرع الثالث).

الفرع الأول: الركن الشرعي- النص القانوني

الركن الشرعي للجريمة هو الأساس القانوني الذي يضيف وصف "الجريمة" على سلوك معين، ويعني خضوع الفعل لنص تجريم صريح وسابق في القانون، تجسداً لمبدأ "لا جريمة ولا عقوبة إلا بنص" كما هو منصوص عليه في الدستور الجزائري، خصوصاً في المادة 41: (كل شخص يُعتبر بريئاً حتى تثبت جهة قضائية إدانته، في إطار محاكمة عادلة).¹ و المادة 43 التي تنص على: (لا إدانة إلا بمقتضى قانون صادر قبل ارتكاب الفعل المجرّم).² و يعد هذا الركن حجر الزاوية في مبدأ

¹ - المادة 41، دستور الجمهورية الجزائرية الديمقراطية الشعبية، 2020، مرسوم رئاسي رقم 20-442 مؤرخ في 15 جمادى الأولى 1442 الموافق لـ 30 ديسمبر 2020، الجريدة الرسمية العدد 82، 30 ديسمبر 2020.

² - المادة 43، نفس المرجع.

الشرعية، حيث يضمن حماية حريات الأفراد من تحكم السلطة ببيان السلوك المباح من المحظور، و هذا ما ينص عليه الدستور الجزائري من خلال المادة 174 منه و التي تنص على: (يحمي القانون المتقاضي من أيّ تعسف يصدر عن القاضي)¹.

وتخضع العقوبات لمبدأ شرعية الجرائم والعقوبات بحيث: لا يجوز توقيع عقوبة أو تدبير أمن إلا بناءً على نص قانوني صريح يحدد الجريمة وعقوبتها قبل وقوعها، وهذا ما نص عليه قانون العقوبات في المادة الأولى: (لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون)².

وفي الأخير نستخلص ان الركن الشرعي هو النص القانوني الذي يقرر أن فعلاً معيناً هو جريمة أم لا، ويهدف الركن الشرعي إلى خلق توازن بين مصلحة الفرد ومصلحة المجتمع وهو تحديد السلوك الاجتماعي المقبول.

الفرع الثاني: الركن المادي - السلوك المادي

يعتبر الركن المادي هو السلوك المادي للجريمة وهو مظهرها الخارجي الذي يكون مدركاً بالحواس، بعض الفقه يسميه جسم الجريمة، في حين أن روح الجريمة هو عنصرها وركنها المعنوي.³ نتناول في هذا المطلب الاول السلوك الإجرامي لأفعال الدخول غير المصرح به، البقاء، والاعتراض (الفرع الأول)، ثم نتطرق الى محل الجريمة، المتمثلة في المعطيات المعلوماتية والنظم الرقمية.

أولاً: السلوك الإجرامي - الدخول غير المصرح به، البقاء غير المشروع، والاعتراض غير الشرعي

¹ - المادة 174، نفس المرجع.

² - المادة الأولى، قانون العقوبات الجزائري المعدل بالقانون 06-24، المؤرخ في 28 أبريل 2024، الجريدة الرسمية عدد 30، 2024.

³ - <https://univ-soukahrass.dz/moodle/pluginfile>، 22:17، 2026-03-29، على الساعة تم التصفح.

يتجسد السلوك الإجرامي في جريمة التجسس عبر ثلاث صور رئيسية حددها المشرع الجزائري لضمان شمولية الحماية القانونية للنظم المعلوماتية، والذي عبرت عنه صراحة المادة 394 مكرر من قانون العقوبات الجزائري (المعدلة بالقانون 04-15 و 06-24)، على معاقبة الدخول أو البقاء في أنظمة المعالجة الآلية للمعطيات وأقرت عقوبة الحبس من 3 أشهر إلى سنة، وغرامة مالية، أو بإحدى هاتين العقوبتين، لكل من دخل أو بقي عن طريق الغش في جزء من منظومة للمعالجة الآلية¹، إذن، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع، فيما الصورة المشددة، تتحقق بتوافر الظرف المشدد لها، و يكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.² وسنتناول هذه الأفعال بدقة.

1- فعل الدخول غير المصرح به

يقصد بالدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات³، ولم يحدد المشرع وسيلة الدخول أو طريقة لاتي يتم الدخول بها إلى النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر⁴. فعل الدخول هو تخطي الحواجز الأمنية للوصول إلى نظام

¹ - المادة 394 مكرر: (يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 ألف دج إلى 200,000 ألف دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100,000 ألف دج إلى 300,000 ألف دج).

² - مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، مجلة القانون، المجلد 09، العدد 01، 2020، ص 113.

³ - مراد مشوش، مرجع سابق، ص 113.

⁴ - مراد مشوش، نفس المرجع، ص 113.

معالجة آلية للبيانات دون وجه حق، حسب مضمون نص المادة 394 مكرر من قانون العقوبات¹.

2- فعل البقاء غير المشروع

وهو الاستمرار في التواجد داخل النظام بعد الدخول إليه بطريق الخطأ أو بعد انتهاء التصريح بالدخول. (ويقصد بفعل البقاء التواجد داخل النظام ضد إرادة من له الحق في السيطرة على هذا النظام وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول على النظام، ويقدر مجتمعان، ويكون البقاء معاقبا عليه حين يكون الدخول إلى النظام مشروعا، إذا كان يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورا، ويكون البقاء جريمة إذا تجاوز المتدخل المدة المسموحة بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية والاطلاع...) ²

3- فعل الاعتراض غير الشرعي

وهو استخدام وسائل تقنية لالتقاط بيانات مرسله عبر شبكة معلوماتية، وهو الجوهر الفني لعملية "التجسس". وعن اعتراض المراسلات السلكية واللاسلكية وعدم مشروعية الاعتراض والتتصت للبيانات والحق في حرمة الحياة الخاصة للأفراد، فإن المادة 47 من دستور 2020 تنص صراحة على أن: (لكل شخص الحق في حماية حياته الخاصة وشرفه. لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت. لا أساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر

¹ - المادة 394 مكرر، قانون العقوبات الجزائري المعدل بالقانون 06-24، المؤرخ في 28 أبريل 2024، الجريدة الرسمية عدد 30، 2024.

² - مراد مشوش، مرجع سابق، ص 114.

معلل من السلطة القضائية. حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. يعاقب القانون على كل انتهاك لهذه الحقوق).¹

انطلاقاً من نص هذه المادة فإن الدستور الجزائري يضمن سرية المكالمات الهاتفية وكل الاتصالات بأشكالها المختلفة من التنصت والمراقبة أو الاستماع أو النشر أو الاطلاع سواء كانت خطابات أو برقيات أو مستندات، وهذا كرسه قانون العقوبات الجزائري ضمناً بخصوص حق سرية المكالمات الهاتفية ما لم يتم الاعتراض بأمر قانوني، حيث أن المواد القانونية 107 و 137 من ق.ع.ج جاءت صريحة في تجريم فعل قيام الموظفين بالتعدي على حقوق الأفراد المشروعة منها الخاصة بمراسلاتهم بكل أنواعها و يليها ما نصت عليه المواد 303 و 303 مكرر وما يليها حول اعتراض المراسلات السلكية واللاسلكية. وأما نص المادة 12 من القانون 04-09 في فقرتيها "أ" و "ب" قد ألزمت مقدمي خدمة الإنترنت على (التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفة للقوانين و تخزينها او جعل الدخول إليها غير ممكن، وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول الى الموزعات التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامة و إخبار المشتركين لديهم بوجودها)².

وفي هذا الشأن عرفت اتفاقية بودابست للجريمة الإلكترونية المعروفة بـ اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية لسنة 2001 في المادة 03 الاعتراض غير شرعي على أنه (الاعتراض المقصود وغير القانوني الذي تم تنفيذه بالوسائل

¹ - دستور الجمهورية الجزائرية الديمقراطية الشعبية، 2020، مرسوم رئاسي رقم 20-442 مؤرخ في 15 جمادى الأولى 1442 الموافق لـ 30 ديسمبر 2020، الجريدة الرسمية العدد 82، 30 ديسمبر 2020.

² - قانون رقم 04-09، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات اللّم والاتصال ومكافحتها، جريدة الرسمية، 05 أوت 2009، الجزائر، عدد 47، ص 8.

التقنية، وبيانات الكمبيوتر، أثناء الإرسال غير العام أو من أو داخل نظام الكمبيوتر، بما في ذلك الانبعاثات الكهرومغناطيسية يحمل مثل هذه البيانات.¹

4- محل الجريمة - المعطيات المعلوماتية والنظم الرقمية

لا يقع التجسس الإلكتروني على أشياء مادية ملموسة، بل ينصب على كيانات افتراضية تمثل مستودع الأسرار في العصر الحديث وهي: المعطيات المعلوماتية التي تشمل كافة البيانات المخزنة أو المعالجة إلكترونياً، سواء كانت أسراراً عسكرية أو اقتصادية، وكما تشمل أيضاً النظم الرقمية المتمثلة في مجموع الوسائل التقنية من أجهزة وبرمجيات التي تشكل الوعاء الذي تجرى فيه عمليات التجسس، وسنتناول هذه العناصر بشرح دقيق.

أ- المعطيات المعلوماتية

تعرف بأنها كل تمثيل للوقائع أو المعلومات أو المفاهيم في شكل قابل للمعالجة بواسطة نظام معلوماتي، سواء كانت نصوصاً، صوراً، أصواتاً أو برامج.

إن المعطيات المعلوماتية تعتبر محل جريمة التجسس الإلكتروني فهي من العناصر غير المادية المرتبطة بالتكنولوجيا والتي تمثل الهدف المباشر للاعتداء.

وكما عرفت المادة الثانية الفقرة (ج) من القانون 04-09 المتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الأعلام والاتصال ومكافحتها، المعطيات المعلوماتية على أنها (أي عملية عرض للوقائع او المعلومات أو المفاهيم

¹ - L'article 3 de la convention du Budapest stipule que: "...l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques."

في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها).¹

وقد كرس القانون الجزائري حماية قانونية خاصة للمعطيات نظراً لخطورة الاعتداء عليها، وهذا، من خلال تجريم أفعال: لدخول غير المشروع إلى الأنظمة وحذف أو تعديل البيانات² واعتراض المعطيات أثناء نقلها.³

ب- النظم الرقمية - الأنظمة المعلوماتية

ويقصد به كل نظام لمعالجة المعطيات بطريقة آلية، ويشمل الأجهزة (Hardware) والبرمجيات (Software) وقواعد البيانات والشبكات (The Algerian legislator-defined the information system as any separate system or group of systems connected to each other or linked, one or more of which automatically processes the data in implementation of a specific program⁴، ويتكون النظام المعلوماتي من: الحواسيب والخوادم وشبكات الإنترنت، الشبكات الداخلية) والبرمجيات وقواعد البيانات.⁵ وعرف المشرع الجزائري الأنظمة المعلوماتية في المادة 2 الفقرة "ب" من القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنها: (أي نظام

¹ - المادة 02، قانون 04-09، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

ومكافحتها، جريدة الرسمية، 05 أوت 2009، الجزائر، عدد 47، ص 5.

² - المادة 394 مكرر، قانون العقوبات الجزائري المعدل بالقانون 06-24، المؤرخ في 28 أبريل 2024، الجريدة الرسمية عدد 30، 2024.

³ - المواد 394 مكرر-394 مكرر 7، مرجع سابق.

⁴ -BABAH Brahim, GHEHIOUECHE Alwalid, **The Legal Framework for The Inspection of Information Systems in Algerian Legislation**, Annals of Algiers University 1, Volume 39, N° 04, 2025, P 172.

⁵ - خالد رجم، محاضرات في نظام المعلومات، جذع مشترك علوم اقتصادية وتجارية وعلوم التسيير، السنة الثانية، معهد التكنولوجيا جامعة قاصدي مرباح ورقلة، 2018/2017، ص 12 و 13.

منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين)،¹

أما عن حماية الأنظمة المعلوماتية، فإن المشرع الجزائري قد أقر حمايتها من خلال المواد 394 مكرر 394 مكرر 7 من ق.ع.ج بتجريم أفعال: الولوج غير المشروع وتعطيل النظام وإدخال معطيات من شأنها الإضرار بوظيفته.²

الفرع الثالث: الركن المعنوي - القصد الجنائي

باعتبار التجسس الإلكتروني من الجرائم العمدية، فإن الركن المادي وحده لا يكفي للإدانة؛ بل يجب أن يقترن الفعل بتوجه إرادي آثم. ونظراً لخطورة هذه الجريمة، فإن القصد الجنائي فيها يتخذ أبعاداً مركبة تشمل العلم والإرادة والغاية.

أولاً: القصد العام - العلم والإرادة

يمثل القصد العام الحد الأدنى المطلوب لتوافر الركن المعنوي، حيث يجب أن تتجه إرادة الجاني إلى ارتكاب الفعل مع علمه بعدم شرعيته.

1- العلم: أن يدرك الجاني أن النظام الذي يخترقه غير مصرح له بالدخول إليه، وأن البيانات التي يعترضها محمية، وبالتالي فهو يقوم بفعل غير مشروع.

2- الإرادة: أن تتجه إرادته الحرة إلى تحقيق السلوك الإجرامي (الدخول أو الاعتراض) دون إكراه.

ثانياً: القصد الخاص - نية الإضرار بالمصلحة الوطنية والحصول على أسرار

لا يكتفي المشرع في جريمة التجسس بالقصد العام، بل يشترط توافر نية محددة تميز الجاسوس الإلكتروني عن الهاكر الهاوي.

¹ - المادة 2 الفقرة "ب"، نفس المرجع، ص 5.

² - المواد 394 مكرر - 394 مكرر 7، مرجع سابق.

1- نية الإضرار بالمصلحة الوطنية: إذا كان الهدف من التجسس إضعاف أمن الدولة أو الدفاع الوطني (المواد 61 و62 من قانون العقوبات).

2- نية الاستيلاء على الأسرار: الرغبة في كشف أسرار مهنية أو اقتصادية أو سياسية للاستفادة منها أو تسريبها لجهة معادية.

يتضح من دراسة هذا الفصل انه من الصعب إيجاد تعريف موحد وجامع للتجسس الإلكتروني متفق عليه، بحيث لا يختلف عن التجسس التقليدي الا في الوسيلة المستعملة للتجسس. ومن خلال هذا الفصل يظهر جليا ان التجسس المعلوماتي يمثل تهديدا للأمن القومي للدول، وذلك بسبب قدرته على اختراق الأنظمة وجمع معلومات حساسة بطرق غير قانونية، مما يتطلب مواجهة تشريعية جادة والتصدي لهذا النوع من الجرائم بتطوير استراتيجيات قانونية وتقنية فعالة لحماية الامن القومي للدولة والفضاء السيبراني وضمان سلامته.

وبعد دراسة معمقة لمحاور الفصل الأول، تبين لنا أن محل جريمة التجسس الإلكتروني في القانون الجزائري يتمثل في المعطيات المعلوماتية والنظم الرقمية، وهما عنصران يتمتعان بحماية قانونية مشددة نظراً لأهميتهما في الحفاظ على الأمن المعلوماتي والسيادة الرقمية للدولة ولأن جرائم المساس بأمن الدولة تكون عقوبتها أشد من العقوبات المنصوص عليها الدستور وخصوصا، في قانون العقوبات الجزائري ضمن أحكام المواد من 394 مكرر إلى 394 مكرر 2.

وأخيرا، نستنتج أن محل جريمة التجسس الإلكتروني في القانون الجزائري هو أن ترتكب جريمة التجسس الإلكتروني ضد المعطيات المعلوماتية والنظم الرقمية التي تمس وتستهدف أمن الدولة ومن بينها التجسس باستخدام أنظمة.

المطلب الثاني

الركن الافتراضي لجريمة التجسس الإلكتروني

الجريمة الإلكترونية تمثل ظاهرة حديثة دفعت الفكر القانوني لإعادة تقييم أركان الجريمة التقليدية المتمثلة في: الشرعي، المادي، والمعنوي، وفي هذا السياق، ظهر اقتراح فقهي بإضافة ركن افتراضي أو رقمي، يميز هذا النوع من الجرائم، بحيث لقيام الجريمة الإلكترونية يستلزم وجود نظام المعالجة الآلية للمعطيات كشرط أساسي¹، والذي سنعرفه في (الفرع الأول)، بعد ذلك سنتناول الحماية الفنية للنظام المعلوماتي كشرط لقيام المسؤولية الجزائية في (الفرع الثاني).

ويعني الركن الافتراضي البيئة الرقمية مثل الإنترنت والأجهزة الحاسوبية، التي تُعتبر مكان حدوث الجريمة وأداتها التنفيذية معاً. تتميز هذه الجرائم بارتباطها العميق بالتقنية، ما يجعلها غير ممكنة خارج السياق الرقمي - الافتراضي.

بخلاف الجرائم التقليدية التي تتطلب وجود موقع مادي، تكمن أهمية الركن الافتراضي في تحديد موقع الجريمة داخل الفضاء الإلكتروني. كما يرتبط هذا الركن بالركن المادي كوسيلة لتحقيق الجريمة عبر أساليب كاختراق البيانات أو تعديلها أو تدميرها. بهذا، تُكمل أركان الجريمة الإلكترونية من خلال الركن الشرعي المتمثل للنص القانوني، الركن المادي المتمثل بالفعل ونتائجه، الركن المعنوي القائم على القصد الجنائي، وأخيراً الركن الافتراضي الذي يوفر البيئة الرقمية لوقوع الجريمة.

ويمكن القول في الأخير، أن نظام المعالجة الآلية هو القلب التقني للجرائم المعلوماتية، وحمايته تهدف لضمان سرية وسلامة البيانات المخزنة أو المنقولة.

¹ - بن دراح علي إبراهيم، محاضرات في الجرائم المعلوماتية للسنة الثانية ماستر، معهد العلوم الحقوق والعلوم السياسية، قسم الحقوق، المركز الجامعي أفلو، الجزائر، 2020/2021، ص 9.

الفرع الأول: تعريف نظام المعالجة الآلية للمعطيات

يبدو أن المشرع الجزائري قد تأثر عند وضعه لتعريف نظام المعالجة الآلية للمعطيات الذي وضعته اتفاقية بودابست في المادة الأولى الفقرة "أ"، إذ عرفت النظام المعلوماتي بأنه: كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة، والتي يمكن أن تقوم سواء بمفردها. أو مع مجموعة عناصر أخرى، بتنفيذاً لبرنامج معين، بأداء معالجة آلية للبيانات¹، ثم عرفت المادة نفسها الفقرة "ب" المعطيات المعلوماتية بأنها: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.² يعرف نظام المعالجة الآلية للمعطيات (Système de traitement automatisé de données-STAD) في التشريع الجزائري، لا سيما في سياق مكافحة الجرائم المعلوماتية، بأنه كل مجموعة منفصلة أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين. بحيث عرفت المادة 2- الفقرة ب من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، النظام المعلوماتي (نظام المعالجة الآلية) بأنه: (أي نظام

¹ – L'article Article 1, alinéa (à) de la convention du Budapest stipule que : Aux fins de la présente Convention, a l'expression « système informatique » désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;

²– Alinéa (b): b l'expression « données informatiques » désigne toute représentation de faits, D'informations ou de concepts sous une forme qui se prête à un traitement Informatique, y compris un programme de nature à faire en sorte qu'un système Informatique exécute une fonction; op.cit.

منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين).¹

وبناءً على التعريفات القانونية، تتميز هذه الأنظمة لمعالجة الآلية للمعطيات بالخصائص التالية: الشمولية والتقنية أي انه النظام يشمل أي جهاز أو مجموعة أجهزة متصلة (حاسوب، خادم، شبكة) تقوم بمعالجة البيانات تلقائياً، وتتميز بالوظيفية (تنفيذ برامج) بحيث النظام مصمم لتنفيذ برامج معينة لإدخال، تخزين، حذف، أو تعديل المعطيات و ذو خاصية الحماية القانونية المزدوجة معناه أنه يضع القانون حماية على "النظام نفسه" (المنظومة المعلوماتية) و"المعطيات" (المعلومات المخزنة) التي يتضمنها و الصبغة غير المادية (للمعلومات) فالتعامل يتم مع معطيات رقمية غير ملموسة، مما يجعل الاعتداء عليها يحتاج لطرق تقنية خاصة.²

الفرع الثاني: الحماية الفنية للنظام المعلوماتي كشرط لقيام المسؤولية الجزائية

نظراً للحاجة الملحة لحماية الأنظمة المعلوماتية، أصبح من الضروري وجود نصوص قانونية خاصة بهذا المجال. وقد استجابت العديد من الدول لهذا التوجه من خلال إبرام اتفاقيات تهدف إلى مكافحة الجريمة المعلوماتية وحماية الأنظمة المعلوماتية. ومن بين هذه الاتفاقيات، تبرز معاهدة بودابست لعام 2001، التي تُعتبر أول معاهدة دولية شاملة لمكافحة الجرائم الإلكترونية، بالإضافة إلى الاتفاقية العربية لمكافحة الجريمة المعلوماتية، وكذلك اتفاقية الأمم المتحدة المقررة في عام 2024، التي تُعتبر معاهدة دولية شاملة لمواجهة الجرائم.

¹ - المادة 02 ، قانون 04-09 قانون رقم 04-09، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات اللام والاتصال ومكافحتها، جريدة الرسمية، 05 أوت 2009، الجزائر، عدد 47، ص 5.

² - يعيش تمام شوقي، خليفة محمد، نظام المعالجة الآلية للمعطيات الإلكترونية كأساس للحماية الجزائية في التشريع

الجزائري، جامعة بسكرة، مجلة جيل الأبحاث القانونية المعمقة، العدد 25، 2018، ص 11.

أما بالنسبة للمشرع الجزائري، فقد تدارك ولو نسبيا الفراغ القانوني في مجال الإجرام المعلوماتي، باستحداث نصوص تجرimeية بهدف توفير الحماية الجزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، فقام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون 04-15 مستعملا في ذلك التسمية التي "المساس بأنظمة المعالجة الآلية للمعطيات"¹. وقددر المشرع الجزائري من خلال هذا التعديل ان جوهر المعلوماتية هي المعطيات التي تدخل الى الحاسوب فتحولها الى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من عدة زوايا، وبصدور القانون 04-09 عبر المشرع على الجرائم المعلوماتية بتسمية "الجرائم المتصلة بتكنولوجيات الاعلام والاتصال".² أثار ركن الحماية الفنية للنظام المعلوماتي انقساما في الوسط الفقهي، حول اعتماده أم لا كشرط لقيام المسؤولية الجزائية في تكييف فعل انه جريمة الكترونية؛ "اختلف الفقه القانوني في مدى اعتبار الحماية الأمنية لنظام المعالجة الآلية للمعطيات كشرط ضروري كي يحظى هذا النظام بالحماية الجزائية من عدمها، فقد اعتبر جزء من الفقه الفرنسي إلى عدم اشتراط توفر الحماية الفنية للنظام المعلوماتي لقيام الجريمة المعلوماتية، وذلك رجع كون نظام الأمن والحماية الفنية أو التقنية لا يكون له سوى دور إيجابي ، وأن ثبوت سوء نية المنتهك لهذا النظام ودخوله إليه بطريقة غير شرعية هي متوفرة أساسا".³ "...في حين قسم اتجاه آخر من الفقه المتمسك بضرورة وجود نطاق كاف من الحماية الأمنية للمختلف الأنظمة المعلوماتية المعالجة آليا، مقسما هذه الأخيرة إلى ثلاث أصناف: -أنظمة مفتوحة للجمهور. - أنظمة قاصرة على أصحاب الحق فيها، ولكن دون حماية فنية. -أنظمة قاصرة على

¹ - حمز خضري، عشاش حمزة، خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، مجلد 6، عدد 2، 2020، ص 172.

² - حمز خضري، عشاش حمزة، نفس المرجع، ص 172.

³ - بن دراح علي إبراهيم، محاضرات في الجرائم المعلوماتية للسنة الثانية ماستر، معهد العلوم الحقوق والعلوم السياسية، قسم الحقوق، المركز الجامعي أفلو، الجزائر، 2020/2021، ص 11.

أصحاب الحق فيها، مع توفرها على حماية فنية لها. حيث اعتبر هذا الفقه أن النوع الأخير من الأنظمة المعلوماتية هو الذي يتمتع بالحماية الجنائية، وحجتهم في ذلك أن الحماية الجنائية يجب أن تقتصر على الأنظمة المحمية فنيا، لأنه من الطبيعي أن يقوم باستغلالها أي شخص، لذا فإن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم ويتوفر الحماية الأمنية ولو بقدر أدنى. لكن التساؤل المطروح في هذه الحالة حول إمكانية عدم توفر نظام معلوماتي على نظام حماية فنية على قدر ما ولو كان بسيطاً، ومنه من الناحية العملية أصبح من غير المعقول تقبل فكرة وجود نظام معلوماتي لا يحتوي على عنصر الحماية الفنية له، لذا فإن وجود هذه الحماية له دور كبير في تحديد القصد الجنائي لدى المجرم المعلوماتي...¹

أما الفقه الجزائري فهو يعتبر أن المشرع لم يشترط الحماية الفنية مثل (كلمات السر، وجدان الحماية) كشرط مسبق لتصنيف الفعل كجريمة، وهذا، من خلال اعتماده معيار "الوصول غير المصرح به" كعنصر أساسي وذلك استناداً إلى تفسير المواد (394 مكرر إلى 394 مكرر 7)، بحيث تنص المادة 394 مكرر على: (يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 ألف دج إلى 200,000 ألف دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100,000 ألف دج إلى 300,000 ألف دج)،² وتجدر الإشارة إلى أن المشرع الجزائري بالإضافة إلى ذلك، سوى بين النظام المحمي وغير المحمي من خلال الاكتفاء واعتماد على عنصر تجريم فعل "الشروع" في المادة 394

¹ - بن دراح علي إبراهيم، المرجع السابق الذكر، ص 11.

² - المادة 394 مكرر من قانون العقوبات الجزائري.

مكرر 7 التي تنص: (يعاقب على الشروع في ارتكاب الجнг المنصوص عليها في هذا القسم بالعقوبات المقررة للجنة ذاتها).¹

انطلاقا مما سبق شرحه ومن خلال الدراسات الجزائرية، ألتمسنا المشرع الجزائري قد سوى بين النظام المحمي وغير المحمي من خلال الاكتفاء واعتماد على عنصر تجريم فعل الشروع وعدم اشتراط الحماية التقنية، مما ساعد في توسيع نطاق الحماية القانونية وعدم ترك أي ثغرات للمخترقين.

¹ - المادة 394 مكرر 7، نفس المرجع.

الفصل الثاني:

الآليات الإجرائية والموضوعية للمكافحة في القانون الجزائري

الفصل الثاني

الآليات الإجرائية والموضوعية للمكافحة في القانون الجزائري

تعتبر جريمة التجسس الإلكتروني من التحديات المعاصرة التي تثير العديد من القضايا القانونية والإجرائية. الآن، في عصر الإنترنت، أصبح التجسس الإلكتروني خطراً حقيقياً على أماننا وأمان معلوماتنا، بحيث يصل المجرمين بطريقة متاحة وبسهولة الى اختراق الأنظمة، وبالتالي يسرقون المعلومات الخاصة ويسببون مشاكل كبيرة للأفراد والمؤسسات والدولة. لذلك، يجب أن يكون لدى الدولة الجزائرية بل كل الدول قوانين واضحة لمكافحة هذه الجرائم.

سنناقش القوانين والآليات الإجرائية والموضوعية في القانون الجزائري لمكافحة التجسس الإلكتروني، وكيفية مواجهة جريمة التجسس الإلكتروني وتطبيق هذه القوانين وكذلك طريقة عمل القضاء الجزائري في مراحل: التحقيقات، وكيف تجمع الأدلة الرقمية، وأهمية التعاون بين الشرطة والقضاء لمكافحة التجسس الإلكتروني، ولمعالجة كل هذه العناصر المكونة للفصل الثاني، سنتناول القواعد الإجرائية والوقائية لمواجهة التجسس الإلكتروني (المبحث الأول) والذي نعالج فيه أساليب البحث والتحري في الجرائم الإلكترونية (المطلب الأول) والتعاون الدولي في مجال مكافحة التجسس الرقمي (المطلب الثاني)، ونستعرض السياسة العقابية والمسؤولية عن جريمة التجسس الإلكتروني (المبحث الثاني) الذي يتكون من العناصر التالية، العقوبات المقررة للأشخاص الطبيعيين والمعنويين (المطلب الأول) و الظروف المشددة ومعوقات الملاحقة القضائية (المطلب الثاني).

المبحث الأول

القواعد الإجرائية والوقائية لمواجهة التجسس الإلكتروني

بسبب التطور السريع في التكنولوجيا، أصبح التجسس الإلكتروني يهدد خصوصية الافراد والأمن المؤسسي خاصة ولذلك، من المهم فهم القواعد والخطوات اللازمة لمواجهة هذا التهديد. وتتطلب مكافحة جريمة التجسس الإلكتروني تفعيل مجموعة متنوعة من القواعد القانونية والإجراءات التي تسهم في تعزيز الأمن الرقمي وحماية المعلومات الحساسة، وسنسلط الضوء على أهمية تطبيق القوانين المحلية والدولية في وضع استراتيجيات فعالة لمواجهة التهديدات الإلكترونية. سنقوم هنا بدراسة الطرق والأساليب المستخدمة في البحث والتحقيق في الجرائم الإلكترونية، بما في ذلك جمع الأدلة الرقمية وتحليل البيانات والإجراءات التي تتبعها الجهات المختصة في (المطلب الأول) وستناول دور التعاون الدولي بين الدول لمكافحة ظاهرة التجسس الإلكتروني الذي يعد عنصراً حيوياً في هذا الإطار (المطلب الثاني).

المطلب الأول

أساليب البحث والتحري في الجرائم الإلكترونية

تعتبر جرائم التجسس الإلكتروني من أكثر الجرائم تعقيدا بسبب صعوبة الكشف عنها وإثباتها، بالنظر إلى طابعها غير المادي واعتمادها على تقنيات رقمية متطورة تمكن مرتكبيها من إخفاء آثارهم والتنقل بين أنظمة معلوماتية متنوعة خلال وقت قصير. هذه الطبيعة الديناميكية لهذه الجرائم تجعل أدوات التحري التقليدية غير ملائمة لمواجهتها، مما دفع المشرع الجزائري إلى اعتماد آليات إجرائية حديثة تتماشى مع خصوصيات البيئة الرقمية، بما يتيح الكشف عن الأدلة الإلكترونية وتتبع مرتكبي تلك الجرائم بشكل فعال، من خلال تطوير قواعد قانون الإجراءات الجزائية وإدماج نصوص قانونية متخصصة، وخاصة من خلال القانون رقم 09-04، بحيث أتاح مجموعة من الوسائل التقنية والقانونية التي تمكن الجهات المختصة من القيام

بالتحريات بطريقة فعالة.¹ تناول هذا المطلب من خلال التطرق الى التفتيش الإلكتروني واعتراض الرسائل وفق قانون 04-09 (الفرع الاول) و دور الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها في (الفرع الثاني).

الفرع الأول: التفتيش الإلكتروني واعتراض الرسائل وفق قانون 04-09

التفتيش الإلكتروني إشكالية أفرزها التطور الحديث في الجريمة المعلوماتية، الذي يهدف إلى الوصول للأدلة المعلوماتية أو البيانات المخزنة في الوسائط الإلكترونية وأنظمة الحاسوب. وكونه إجراء ينتهك حياة الأفراد الخاصة، خاصة وأنه ينصب على المكونات المادية والمعنوية للحاسب الآلي، والتي تحتوي على كم هائل من أسرار الأشخاص، أخضعتة القوانين الإجرائية إلى ضوابط قانونية، يجب على القائمين به مراعاتها خلال التفتيش، وإلا كان إجراء باطلا.²

¹ -Bouder Hadjira : L'introduction, en 2004, de dispositions inédites dans le code pénal algérien, à savoir celles relatives à la criminalité liée aux TIC, a certainement suscité l'attention du législateur algérien quant à la nécessité D'adopter des règles procédurales adéquates... Le chapitre III de la loi 09-04 a mis en place des règles procédurales plus adaptées à la nature des délits informatiques, et à la particularité de l'environnement dans lequel ils sont perpétrés, Division Recherche et Développement en Sciences de l'Information, (CERIST), Bulletin d'information trimestriel, numéro 13, 2013, P P 17-20.

² - سهيلة طمين، إشكالية التفتيش في الجريمة المعلوماتية، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزيوزو، المجلد 20، العدد 1، 2025، ص 463.

أولا - تعريف التفتيش الإلكتروني

يشير إلى مجموعة الإجراءات القانونية التي تتخذ للوصول إلى البيانات والمعلومات المخزنة إلكترونيا. هذا النوع من التفتيش يتطلب دقة واحترافية في التعامل مع المعلومات الرقمية.

" التفتيش الإلكتروني عبر الدخول إلى منظومة معلوماتية أو الاطلاع على ما يحتويه جهاز الكمبيوتر أو الهاتف وذلك من ... وذلك بتسخير أشخاص على دراية بمهارات التعامل الإلكتروني حتى يتمكن من مساعدة الضبطية القضائية على جمع المعلومات والحصول على المعطيات اللازمة التحقيق، خاصة وأن هذه الأخيرة لا يمكن حجزها أو مصادرتها أي (المعلومة).¹

" لم يورد المشرع الجزائري تعريفا خاصا ودقيقا للتفتيش بقدر ما اعتبره إجراء من إجراءات التحقيق وإحاطته بضوابط صارمة نظرا لأهميته في كشف الأدلة وخطورته فيما قد يترتب عنه من مساس بحرية الأشخاص وبكرامتهم ومما يؤكد ذلك اهتمام الدستور الجزائري بهذه النقطة إذ نص في المادة 40 منه بالقول: (فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة).²

اعتمد المشرع الجزائري إجراءات خاصة تتجاوز المفهوم التقليدي للتفتيش، من خلال المادة الخامسة من القانون رقم 04-09 المؤرخ في 5 أوت 2009، الذي يحدد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي تنص: (يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4

¹ - مشري سلمى، محاضرات في مقياس الجريمة الإلكترونية السنة الثانية ماستر علوم جنائية، جامعة سطيف 2، ص 21.

² - زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص 130.

أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى: أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها. ب- منظومة تخزين معلوماتية...¹

ثانيا - شروط التفتيش الإلكتروني

حدد القانون الجزائري شروطا دقيقة لإجراء التفتيش الإلكتروني بصورة قانونية وصحيحة، ومن بين أهم هذه الشروط ما يلي: وجود جريمة أو أدلة قوية، لا يجوز اللجوء إلى التفتيش الإلكتروني إلا إذا توفرت أدلة جوهريّة أو شبهات جدية بارتكاب جريمة إلكترونية، مثل التجسس أو اختراق الأنظمة المعلوماتية. يتطلب التفتيش الإلكتروني الحصول على إذن مسبق من السلطات القضائية المختصة، مما يضمن احترام حقوق الأفراد وحمايتهم، كما اقتره المادة 40 من الدستور الجزائري السابقة الذكر وقانون الإجراءات الجزائية الجزائري، فإن التفتيش المنصب على المنظومة الإلكترونية يختلف عنه كليه من حيث الشروط الموضوعية والشكلية وكذا موضوع التفتيش،² لكل ذلك سوف نورد هذه العناصر ويمكن تقسيمها إلى قسمين:

1- القواعد الموضوعية للتفتيش الإلكتروني

وتتضمن عدة شروط وهي:

أ- وقوع الجريمة المعلوماتية بفعل غير مشروع مرتبط باستخدام الحاسوب لتحقيق أغراض غير مشروعة.

ب- تورط شخص أو اشخاص معينين في ارتكاب الجريمة الإلكترونية أو الاشتراك فيها:

يجب ان تتوافر لدى الشخص المراد تفتيش حاسوبه أو منزله، دلائل كافية لاعتقاد أنه قد ساهم في ارتكاب جريمة، سواء كان بصفته فاعل أصلي أو شريك، يستوجب اتهامه بها، ويقصد بالدلائل الكافية الإشارات التي تقوم على المضمون

¹ - المادة 5، القانون رقم 09-04، المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 47، اوت 2009.

² - زبيحة زيدان، نفس المرجع، ص 131.

العقلي والمنطقي لوقائع وملابسات الجريمة، وكذا خبرة وكفاءة القائم بالتفتيش والتي يمكن بها تأكيد نسبة الجريمة لفاعلها.¹

ج-توافر إشارات قوية أو قرائن على وجود اشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة:

قبل ان يقوم المحقق بعملية التفتيش أو يؤذن بها، يجب ان تتوفر دلائل قوية على أن المحل المراد تفتيشه أو الحاسب الالى المراد تفتيشه تتواجد فيهم وسائل او برامج استعملت لاقتراف الجريمة أو مستمدة منها، أو فيه مستندات معلوماتية تساعد على اكتشاف الحقيقة.²

د- محل التفتيش الالكتروني:

أن محل التفتيش الالكتروني هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به، ويقصد بمحل التفتيش الالكتروني ذلك المستودع الذي يحتفظ فيه الشخص بالأشياء التي تتضمن سره، وينصب هذا المحل في الجريمة المعلوماتية على جهاز نظام المعالجة الآلية بمكوناته وشبكات الاتصال الخاصة به أو المتعلقة بالوسائل المعلوماتية بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش، والأماكن التي توجد بها تلك الأشياء. والمحل في الجرائم المعلوماتية لا يكون قائما بذاته بل مقترنا إما بمكان معين كمسكن المتهم أو بشخص معين بصفته مالك أو حائز مثلما هو الشأن في الحاسب المحمول أو الهاتف النقال، لذلك فإنه يتعين قبل مباشرة إجراءات التفتيش مراعاة طبيعة المكان الذي تتواجد فيه

¹ - سهيلة طمين، المرجع السابق، 471.

² - سهيلة طمين، نفس المرجع، ص 472.

الوسائل المعلوماتية المراد تفتيشها وكذا الضمانات القانونية المحاطة به، لأن حكم تفتيش هذه الوسائل يتوقف غالبا على طبيعة المكان الذي تتواجد فيه.¹

هـ - السلطة المختصة بالتفتيش:

لا يعتبر التفتيش الإلكتروني صحيحا ومنتجا لآثاره إلا إذا تم القيام به من طرف الأشخاص أو الجهات المخول لها قانونا صلاحيات إجرائه، وبالنسبة للمشرع الجزائري فقد أوكل صلاحية إجراء التفتيش أو إلى السلطات القضائية المتمثلة في النيابة وكذا ضباط الشرطة القضائية وفقا لأحكام المادة 5 من القانون رقم 09/04 وبالنظر إلى المهارات الفنية التي تتطلبها الجريمة المعلوماتية فقد أجاز المشرع الجزائري للسلطات المكلفة بالتفتيش الاستعانة بخبير له دراية بالمعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها بهدف مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها، وذلك طبقا لمقتضبات المادة 5 الفقرة الأخيرة منها.²

2- القواعد الشكلية للتفتيش الإلكتروني

وتتضمن عدة شروط منها:

أ- أن يتم التفتيش بأسلوب آلي إلكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة:

يعد التفتيش الإلكتروني في القانون الجزائري إجراء استثنائيا ومعقدا يهدف إلى ضبط أدلة رقمية (بيانات، وثائق إلكترونية، أنظمة معلوماتية) المرتبطة بالجرائم المعلوماتية أو التقليدية التي استخدمت فيها الوسائط التكنولوجية. ان شرط التفتيش بأسلوب آلي إلكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة يعد جوهريا

¹ - كيحول عبد القادر، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية، شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، قسم الحقوق جامعة زيان عاشور الجلفة، 2020/2019، ص 13.

² - كيحول عبد القادر، نفس المرجع السابق، ص 14.

لخصوصية الأدلة الرقمية، بحيث لا يجوز لعون الضبط القضائي استخدام الطرق التقليدية لفحص الأجهزة، بل يجب استخدام برمجيات وأجهزة فحص متخصصة قادرة على قراءة البيانات، استرجاع المحذوف، وفحص الأقراص الصلبة دون تدميرها. نظرا لطبيعة الجرائم التقنية، أجازت المادة 46 من ق.إ.ج.ج. بضرورة الاستعانة بخبراء في المسائل التقنية- خبراء في الإعلام الآلي والتي تنص على: (يمكن النيابة العامة الاستعانة في المسائل الفنية بأشخاص مؤهلين، يتم اختيارهم من بين الأشخاص ذوي الاختصاص، وإذا تعذر ذلك يمكن اختيارهم من جدول الخبراء القضائيين)¹، كما تنص الفقرة الأخيرة من المادة 5 من قانون 04/09 في مضمونها على: (إمكانية تسخير يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدبير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها و تزويدها بكل المعلومات الضرورية لإنجاز مهمتها)² و في إطار عملية التحقيق، فإن التفتيش لا يجوز إلا بإذن كتابي مسبق من وكيل الجمهورية أو قاضي التحقيق كما هو منضم في المواد 44، 64، 75 من ق.إ.ج.ج. التي تنظم التفتيش، لذلك من أجل ضمان صحة الإجراء والسرعة في التنفيذ، وأن الاستعانة بخبراء متخصصين أمر مهم جدا يهدف الى حماية الأدلة الرقمية من المحو أو التعديل (Data Volatile)، لذلك، لمنع المتهم من تدمير الأدلة عن بعد أو عبر برمجيات التدمير الذاتي³، و في نفس السياق، ومن أجل استخلاص المعطيات بسرعة قبل إتلافها، سمح القانون بمباشرة التفتيش عن بعد (Search Remote) للأنظمة المعلوماتية.

¹ - المادة 46: قانون رقم 14-25 مؤرخ أوت 2025، يتضمن قانون الإجراءات الجزائية الجزائري، رقم 54.

² - المادة 5، القانون رقم 04-09 المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 47.

³ - مصارة انفال، محلول منال، إجراءات التفتيش الإلكتروني في التشريع الجزائري، ماستر أكاديمي القانون الجنائي والعلوم

الجنائية، كلية الحقوق والعلوم السياسية جامعة باتنة 1، <https://dspace.univ-batna.dz/items/ebe2c3e4-4b2f-4f5d-a731-b058940775c8>

ب- أن يكون أمر التفتيش مسببا أي يجب أن يتضمن الاسباب التي أدت الى إجراءه:

التفتيش هو إجراء خطير يمس بالخصوصية، لذا اشترط القانون وجوب التسبب أي الحصول على إذن كتابي مسبق من وكيل الجمهورية أو قاضي التحقيق هذا ما تضمنته المادة 75 من ق.إ.ج.ج: (لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب سابق صادر من وكيل الجمهورية أو قاضي التحقيق، مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشرع في التفتيش. ويكون الأمر كذلك في حالة التحري في الجنحة المتلبس بها أو التحقيق في إحدى الجرائم المذكورة في المادة 310 أدناه. يجب أن يتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي ستتم زيارتها أو تفتيشها وإجراء الحجز فيها، وذلك تحت طائلة البطلان. تنجز هذه العمليات تحت الإشراف المباشر للقاضي الذي أذن بها والذي يمكنه، عند الاقتضاء، أن ينتقل إلى عين المكان للسهر على احترام أحكام القانون. إذا اكتشفت أثناء هذه العمليات جرائم أخرى، من غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة.¹

ج- تكوين فريق التفتيش يجب أن يتضمن خبراء مسرح الجريمة من الفنيين والمختصين:

يجب أن يشمل تشكيل فريق التفتيش خبراء في مسرح الجريمة من الفنيين والمتخصصين على وأن يتمتعوا بمهارة ممتازة في الحاسوب والأنظمة الإلكترونية، بالإضافة إلى رجال الشرطة. يتكون الفريق من مشرف التحقيق، وفريق التفتيش

¹ - المادة 75: قانون رقم 25-14 مؤرخ أوت 2025، يتضمن قانون الإجراءات الجزائية الجزائري، رقم 54.

العملي المكون من خبراء الحاسوب، بالإضافة إلى فريق الأمن والحماية المكون من رجال الشرطة.¹

ثالثا - نتائج التفتيش الإلكتروني

يستند التفتيش الإلكتروني في الجزائر إلى ترسانة قانونية متكاملة توازن بين الردع والحماية، فوجد القانون رقم 04-09 هو المرجع الأساسي الذي يحدد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بحيث تنص المادة الثالث منه على: (...وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع و تسجيل محتواها في حينها و القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية).²، كما تنص المادة الخامسة من نفس القانون على: (يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، لأغراض التفتيش،³ و من اجل تحقيق أهداف التحقيق بفعالية، قد أدخل القانون 04-09 أدوات كآليات مستحدثة تمنح المحققين مرونة تتناسب مع الطبيعة الافتراضية للجريمة و هي التفتيش عن بعد ، أي انه أجاز المشرع للسلطات القضائية الولوج إلى الأنظمة المعلوماتية عن بعد لضبط البيانات المخزنة في " السحب- Cloud " أو خوادم خارج المكان المادي للتفتيش كما ينص الشطر الأخير من المادة 5 المذكورة من قانون 04-09 : (... و لو عن بعد، على: أ- منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها. ب- منظومة تخزين

¹ - بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة ماستر، جامعة محمد

البشير الابراهيمي برج بوعرييج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022، ص 53.

² - المادة 3 ، القانون رقم 04-09 الجزائري المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم

المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 47، اوت 2009.

³ - المادة 5، نفس المرجع.

معلوماتية¹). كما قرر قانون الإجراءات الجزائية في الفصل الثاني الذي يخص مهام النيابة العامة وأعوان الضبطية القضائية، ومن قواعد عامة في التحقيق وإجراء التفتيش خصوصاً في المواد 44، 47، و64 و75 والتي تطبق على التفتيش الإلكتروني بما لا يتعارض مع خصوصيته الرقمية ولكي تسهم إجراءات التفتيش الإلكتروني في ضمان حماية حقوق الأفراد وفي الوقت نفسه تحقيق أهداف التحقيق بصورة فعالة.

في القانون الجزائري، لا يعتبر التفتيش الإلكتروني مجرد إجراء تقني لجمع الأدلة، بل هو تقاطع دقيق بين حماية الحقوق الدستورية كحرمة الحياة الخاصة ومصصلحة المجتمع في مكافحة الجريمة المستحدثة، ونجد تأكيد هذا المبدأ من طرف الدستور الجزائري لسنة 2020 حين كرس حماية الحياة الخاصة وسرية المراسلات وحماية حقوق الأفراد -الضمانات القانونية، وكذا عدم جواز انتهاكها إلا بأمر مسبب من السلطة القضائية، ولضمان عدم تحول التفتيش إلى أداة تعسفية وضع المشرع الجزائري ضوابط صارمة لقيام وتنفيذ عملية التفتيش الإلكتروني واحترام التوقيت القانوني، حيث يخضع التفتيش للضوابط الزمنية العامة و ينفذ من 05:00 صباحاً إلى 20:00 مساءً إلا في حالات الاستثناء القانونية القصوى، و حضور المعني أو الشهود، أوجبت المادة 47 في مضمونها على: (لكل شخص الحق في حماية حياته الخاصة وشرفه. لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت. لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية. حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. يعاقب القانون على كل انتهاك لهذه الحقوق)² و في نفس السياق، يلتزم القائم بالتفتيش بعدم إفشاء الأسرار الشخصية التي لا علاقة لها بالجريمة محل التحقيق، وذلك تحت طائلة العقوبات الواردة في

¹ - المادة 5، نفس المرجع

² - المادة 47 ، دستور 2020 للجمهورية الجزائرية الديمقراطية الشعبية.

المادة 301 من قانون العقوبات في القسم الخامس - الاعتداءات على شرف و إعبار الأشخاص و على حياتهم الخاصة و إفشاء الاسرار و التي تنص : (يعاقب بالحبس من شهر إلى ستة أشهر وبغرامة من 20.000 إلى 100.000 دينار الأطباء والجراحون والصيادلة والقابلات أو غيرهم من الأشخاص الذين أودعت لديهم الأسرار، إما بسبب مهنهم أو صفتهم أو مهنهم الدائمة أو المؤقتة، والذين، خارج حالات إيجاب القانون عليهم أو ترخيصهم بذلك، يفشون هذه الأسرار).¹

ثانيا: اعتراض الرسائل

"اعتراض المراسلات الإلكترونية في الجزائر هو إجراء قانوني استثنائي، يسمح للضبطية القضائية تحت إشراف النيابة العامة أو قاضي التحقيق بمراقبة، تسجيل، أو التقاط المحادثات والمراسلات الرقمية (بريد إلكتروني، وسائل تواصل) للمشتبه بهم في جرائم خطيرة (إرهاب، جريمة منظمة، إلكترونية)، ويعد مساساً بحرمة الحياة الخاصة لا يجوز إلا بإذن قضائي كتابي".² و قد سمحت المادة 4 من قانون 04-09 للجهات القضائية المختصة بوضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، وذلك كإجراء وقائي أو للتحري عن الجرائم و التي تنص على: (يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية: (أ) - للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أو الجرائم الماسة بأمن الدولة. ب في حالة توفر معلومات عن احتمال ارتكاب الجرائم المذكورة في الفقرة (أ) أعلاه).³

¹ - المادة 301، قانون العقوبات الجزائري.

² - مقالاتي مونة، بوخميس سهيلة، الحق في اعتراض سرية الاتصالات والمراسلات في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية: مجلد 3، عدد 2، 2019، ص ص 122 - 148.

³ - المادة 3، القانون رقم 04-09 الجزائري المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 47، اوت 2009.

و تعد مراقبة الاتصالات الإلكترونية ونفتش النظم المعلوماتية من أهم وأخطر الإجراءات التي جاء بها قانون 09/04 ، فمثلا فهذين الإجراءين خلفا صراعا كبيرا في كثير من الدول الأوروبية، من بينها سويسرا وألمانيا لم تسمحا بالقيام بالمراقبة الإلكترونية والتفتيش في المنظومات المعلوماتية إلا إذا وقعت الجريمة فعلا، وليس كتدبير وقائي من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهذا لأن هذان الإجراءين يمسان بشكل مباشر الحياة الخاصة للأفراد، فكان جديرا بالمشرع وضع قيود قانونية لتبرير اللجوء إلى هذين الإجراءين كما هو الحال بالنسبة للحالة "أ" من المادة 04 من القانون 1.04/09¹

"ويجب ان يكون التفتيش الالكتروني مبنيا على إذن كتابي من السلطة القضائية، ويكون مبررا بضرورة التحقيق في جرائم خطيرة"² بهدف كشف الجرائم ومواجهة تطورها في افضاء الرقمي، تحديد الجناة، وجمع الأدلة الرقمية لضمان فعالية العدالة، و نظم المشرع الجزائري اعتراض المراسلات وتسجيل الاصوات والنقاط الصور ضمن قانون الإجراءات الجزائية وفي هذه السياق تنص المادة 114 منه على انه : (إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق بابتدائي في جرائم القتل العمدى، والمخدرات والمؤثرات العقلية، والجريمة المنظمة عبر الحدود الوطنية، الجرائم المتصلة بتكنولوجية الإعلام والاتصال، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، وجرائم الفساد، وجرائم التهريب، وجرائم الاتجار بالبشر، جرائم الاتجار بالأعضاء، وجرائم تهريب المهاجرين، وجرائم اختطاف الأشخاص، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي : -

¹ - أحمد مسعود مريم، قريشي محمد، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09، شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة قاصدي مرباح، الجلفة، 2013، ص108.

² - مقالاتي مونة، بوخميس سهيلة، نفس المرجع.

اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية...¹

و تعد مراقبة الاتصالات الإلكترونية وتفتش النظم المعلوماتية من أهم وأخطر الإجراءات التي جاء بها قانون 09/04 فهذين الإجراءين خلفا صراعا كبيرا في كثير من الدول الأوروبية في سويسرا وألمانيا و مثلا لم تسمح بالقيام بالمراقبة الإلكترونية والتفتيش في المنظومات المعلوماتية إلا إذا وقعت الجريمة فعلا، وليس كتدبير وقائي من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهذا لأن هذان الإجراءين يمسان بشكل مباشر الحياة الخاصة للأفراد، فكان جديرا بالمشروع وضع قيود قانونية لتبرير اللجوء إلى هذين الإجراءين كما هو الحال بالنسبة للحالة "أ" من المادة 04 من القانون 04/09². اما فيما يخص تقديم خدمات بكل أنواعها، لاحظنا كذلك بالنسبة لالتزامات مقدمي الخدمات بأنواعهم أن المشروع ألزمهم في المادة 12 من القانون 04/09 بسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفاتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، ولم يدرج المشروع أي مسؤولية على عاتقهم في حالة امتناعهم عن القيام بهذا الالتزام على عكس نظيره المشروع الفرنسي، لهذا كان حريا بالمشروع إدراج عقوبات جزائية على مقدمي الخدمات المقصرين في أداء واجبهم القانوني.³

¹ - قانون رقم 25-14، يتضمن قانون الإجراءات الجزائية، العدد 54، 2025، الجمهورية الجزائرية الديمقراطية الشعبية.

² - احمد مسعود مريم، قريشي محمد، المرجع السابق، ص108.

³ - المادة 12: زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات الإنترنت ما يأتي:
أ- التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفاتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، ب- وضع ترتيبات تقنية تسمح بحسر الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام والآداب العامة وإخبار المشتركين لديهم بوجودها. قانون رقم 09-04 الجزائري المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 47، اوت 2009.

1- عدم مشروعية التنصت في الدستور

إن المادة 39 من الدستور تنص صراحة على أن: (لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحييها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة)¹.

انطلاقاً من نص هذه المادة فإن الدستور الجزائري يضمن سرية المكالمات الهاتفية وكل الاتصالات بأشكالها المختلفة من التنصت والمراقبة أو الاستماع أو النشر أو الإطلاع سواء كانت خطابات أو برقيات أو مستندات الخ ...

لقد كرس قانون العقوبات الجزائري ما جاء في الدستور بخصوص حق سرية المكالمات الهاتفية ضمناً ما لم يتم الاعتراض بأمر قانوني حيث هناك مواد قانونية صريحة على معاقبة كل من يمس بحرمة الحياة الخاصة للأشخاص عبر تسجيل أو نقل المكالمات أو الأحاديث الخاصة أو السرية دون رضا صاحبها، بالحبس من 6 أشهر إلى 3 سنوات وغرامة مالية، بهدف حماية سرية الاتصالات، وتنص المادة 303 مكرر منه على: (يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه. يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة. إن صفح الضحية يضع حداً للمتابعة

¹ - المادة 39، دستور الجمهورية الجزائرية الديمقراطية لسنة 2020.

الجزائية)¹ كذلك، في هذا الشأن، تنص المادة منها المادة 137 ق ع ج التي تجرم قيام الموظفين بالتعدي على حقوق الأفراد المشروعة منها الخاصة بمراسلاتهم بكل أنواعها حول اعتراض المراسلات السلوكية واللاسلكية، وتنص على: (كل موظف عمومي أو وكيل عن الدولة أو عامل أو مستخدم في بريد الخدمة، يفتح رسائل موجهة للبريد أو يختلسها أو يتلفها أو يسهل فتحها أو اختلاسها أو إتلافها، يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات وبغرامة مالية من 500 إلى 1000 دج. ويعاقب بنفس العقوبة كل مستخدم أو عامل في خدمة البرق، يختلس أو يفشي أو يسهل اختلاس أو إفشاء برقية أو يلفها أو يعطلها).²

الفرع الثاني: دور الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها

تعد الهيئة الوطنية للوقاية من الجرائم الإلكترونية من المؤسسات الوطنية في الجزائر والتي تلعب دورًا هامًا في حماية الأمن السيبراني. هذه الهيئة مهمة بشكل خاص في مكافحة الجرائم الإلكترونية التي تهدد الأمن الوطني والاقتصاد الرقمي. ومن جانب آخر، تعمل الهيئة على توعية المواطنين والمستخدمين حول مخاطر التهديدات الإلكترونية، وتزويدهم بالمعرفة اللازمة لحماية بياناتهم الشخصية. كما تعمل الهيئة على تنسيق جهودها مع باقي الأجهزة الأمنية على المستوى المحلي والدولي لمكافحة الجرائم الإلكترونية.

أولاً- إنشاء الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها: تهدف الهيئة إلى تعزيز القدرات الوطنية لمكافحة الجرائم الرقمية، من خلال تطوير استراتيجيات فعالة وتوفير التدريب اللازم للجهات المعنية. وأنشئت هذه الهيئة بفضل القانون رقم 09-04 الجزائري المؤرخ في 5 غشت 2009،

¹ - المادة 303 مكرر، قانون العقوبات الجزائري 2024.

² - المادة 137، نفس المرجع.

المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 47، أوت 2009، في الفصل الخامس منه والذي يخص الهيئة الوطنية للوقاية، وذلك، لتوفير إطار قانوني وتنظيمي لمكافحة الجرائم الإلكترونية، بالتعاون مع باقي الأجهزة الأمنية والقضائية، بحيث، تنص المادة 13 على: (تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته).¹

ثانيا - مهام الهيئة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها: تشمل الهيئة مجموعة من المهام، مثل التوعية بمخاطر الجرائم الإلكترونية، إجراء التحليلات اللازمة، والتنسيق بين مختلف الجهات الحكومية والخاصة والتعاون وتبادل المعلومات مع نظيراتها في الخارج والتي اقترتها المادة 14 من قانون رقم 04-09 في مضمونها التالي: (تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصاً، المهام الآتية:

أ- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

ب- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك جمع المعلومات وإنجاز الخبرات القضائية- تبادل المعلومات مع السلطات الأمنية الجزائرية ونظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم).²

¹ - المادة 13، القانون رقم 04-09 الجزائري المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 47، أوت 2009.

² - المادة 14، نفس المرجع.

وكما " تضطلع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في الجزائر بدور مزدوج وقائي وتحريي، يهدف إلى حماية أمن الدولة من التهديدات الإلكترونية. تشمل مهامها الاستباقية مراقبة الفضاء الرقمي، والتحري التقني عن الجرائم، والتعاون مع السلطات القضائية لضبط مرتكبي الجرائم التخريبية والإرهابية عبر الإنترنت.¹

المطلب الثاني

التعاون الدولي في مجال مكافحة التجسس الإلكتروني

من خصائص جريمة التجسس الإلكتروني أنها عابرة للحدود والسيادة الإقليمية للدول، مستفيدة بشكل كبير من الطبيعة المفتوحة لشبكة الإنترنت وسرعة انتقال البيانات بين الأنظمة المعلوماتية المختلفة في زمن قياسي. ففي كثير من الحالات، يُرتكب الفعل الإجرامي في دولة معينة، بينما تُخزن البيانات المرتبطة به في دولة أخرى، فيما يتواجد الضحايا في دولة ثالثة، مما فرض التعاون الدولي على الدول كضرورة ملحة لمكافحة الجريمة الرقمية. أمام هذا الخطر، انخرطت الجزائر في المنظومة القانونية الدولية، حيث بادرت بالانضمام إلى عدد من الاتفاقيات الدولية والإقليمية المتعلقة بمكافحة الجرائم الرقمية. وسنتأول هذا المطلب من خلال التطرق إلى أهمية الإنابات القضائية الدولية في تعقب الجناة (الفرع الأول) وانضمام الجزائر للاتفاقيات الدولية في (الفرع الثاني).

الفرع الأول: أهمية الإنابات القضائية الدولية في تعقب الجناة

تعد الإنابة القضائية الدولية أداة أساسية في التعاون القضائي لمكافحة الجرائم العابرة للحدود، وخاصة الجرائم الإلكترونية مثل التجسس الإلكتروني. من خلال هذه

¹ - سهيلة بوزيرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات

الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، 'revue critique de droit et sciences politiques'، Volume 17، pp

<https://asjp.cerist.dz/en/article/209229> 30-12-2022، 560-575

الآلية، يمكن للدول طلب المساعدة من جهات قضائية أجنبية لإجراء التحقيقات أو تنفيذ الأحكام القضائية المتعلقة بالجرائم الرقمية. فالجرائم الإلكترونية تمتد إلى الفضاء الرقمي العالمي الذي يتجاوز الحدود التقليدية. وعليه، فإن جريمة التجسس الإلكتروني غالباً ما تتطلب التعاون بين الدول للوصول إلى الأدلة الإلكترونية التي تقع في دول أخرى نظراً لأهمية الإنابة القضائية الدولية كأداة فعالة لتسريع التحقيقات وتسليم المجرمين المتورطين. " وفي هذا الإطار عملت الجزائر على تطوير استراتيجية أمنية متعددة الجوانب تتناسب مع طبيعة هذه الجرائم، من خلال تعزيز منظومتها القانونية ومطابقتها للاتفاقيات الإقليمية والدولية، للرد على تحديات الإجرام السيبراني في مختلف المستويات. ونظراً لحدثة هذه الجرائم، وفي ظل غياب تعريف موحد ومحدد لها بما يسمح من تحديد آليات مكافحتها، أصبحت من الصعب على الدول مواجهتها بمفردها، مما يستوجب تعاوناً دولياً حقيقياً قائماً على أساس التنسيق المشترك وتبادل الخبرات والمعلومات.¹

أولاً: مفهوم الإنابة القضائية الدولية

الإنابة القضائية الدولية هي آلية قانونية يتم من خلالها طلب المساعدة القضائية من دولة أخرى في إطار التحقيقات الجنائية أو تنفيذ الأحكام القضائية. تشمل الإنابة القضائية الدولية مجموعة من الإجراءات التي تتيح تبادل المعلومات والوثائق، وتنفيذ أوامر التفتيش والحجز.

" يقصد بهذه الصورة طلب اتخاذ إجراء قضائي من إجراءات الدعوى العمومية تتقدم به الدولة الطالبة الى الدولة المطلوب إليها لضرورة ذلك عند الفصل في مسألة معروضة لدى السلطة القضائية في الدولة الطالبة لتعذر قيامها بهذا الإجراء ونفسها، وهدف هذه الصورة تسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات

¹ - آسيا لعمراني، التعاون الدولي في مواجهة الجرائم السيبرانية: الجزائر نموذجاً، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، المجلد 5، العدد 2، 2012، ص54.

الازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية، التي تمنع الدولة الأجنبية من ممارسة بعض الاعمال القضائية داخل أقاليم الدول الأخرى لسماع شهود أو إجراء تفتيش غيرها.¹

وتعتمد الإنابة القضائية الدولية على الاتفاقيات الدولية التي تعقدها الدول فيما بينها، مثل الاتفاقيات الإقليمية مثل معاهدة بودابست حول الجرائم الإلكترونية الاتفاقية العربية أو الاتفاقيات العالمية مثل اتفاقية الامم المتحدة لمكافحة الجرائم السيبرانية.

ثانيا: أهمية الإنابات القضائية الدولية

" تعد الإنابات القضائية الدولية ركيزة أساسية في التعاون القضائي الجزائري لمكافحة الجرائم السيبرانية العابرة للحدود، مثل التجسس الإلكتروني، حيث تتيح تجاوز عقبة الحدود الوطنية وتوفير الدعم اللوجستي والمعلوماتي اللازم لتعزيز فعالية الملاحقات القضائية.² وتكمن أهمية الإنابات القضائية الدولية في تيسير تبادل المعلومات وتوفير الدعم اللوجستي بين الدول لتعزيز فعالية الملاحقات القضائية. والملاحظ اليوم، ان في كثير من الحالات جرائم التجسس الإلكتروني قد لا تكون الأدلة أو المشتبه بهم موجودين في الحدود الوطنية للدولة المتضررة والأدلة الرقمية محفوظة في خوادم موجودة في دول أخرى، مما يصعب التحقيق المحلي، ففي هذه الحالة تتجلى أهمية الإنابة القضائية الدولية في توفير التعاون القضائي بين الدول لمتابعة الجريمة وتتبع الجناة، و هذا ما أقره قانون الإجراءات الجزائية الجزائري فيما يخص التعاون الدولي في المادة 883 التي تنص على: (في حالة المتابعات الجزائية، غير السياسية، في بلد أجنبي، تسلّم الإنابات القضائية الصادرة من

¹ - شويرب جيلالي، مراد فائزة، الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية، مجلة الدراسات القانونية والسياسية،

المجلد 9، العدد 02، 2023، ص 166.

² - آسيا لعمراني، المرجع السابق ص 54.

السلطة الأجنبية بالطريق الدبلوماسي وترسل إلى وزارة العدل بالأوضاع المنصوص عليها في المادة 865 أعلاه، وتنفذ الإنابات القضائية إذا كان لها حل وفق القانون الجزائري وكل ذلك بشرط المعاملة بالمثل.¹ وتتمثل أهمية الإنابة القضائية في عدة مجالات منها:

1- الحصول على الأدلة الإلكترونية المخزنة في خوادم تابعة لدول أخرى: إن المشرع الجزائري أقر إجراءات صارمة في مجال ملاحقة هذا النوع الجديد من الجرائم المعلوماتية، من ذلك أنه "وسع من نطاق التفتيش لو عن بعد حين رخص في المادة 5 من القانون 04-09 للسلطة القضائية المختصة وكذا لضباط الشرطة القضائية الدخول إلى المنظومة المعلوماتية وحتى وأن تبين لهذه السلطات أو وجد لديها اعتقاد بأن المعطيات محل البحث مخزنة في منظومة معلوماتية تقع خارج الإقليم فإن ذلك لا يمنع من تتبعها و الوصول إليها لكن في إطار المساعدة الأجنبية بسلطاتها المختصة..."²

2- طلب توقيف المشتبه بهم الذين يشتبه في تورطهم في جريمة التجسس الإلكتروني لتسليمهم إلى الدولة المتضررة: وهنا، فيما يخص طلب تسليم المجرمين، تشير المادة 865 الى انه: (يتولى وزير الشؤون الخارجية تحوي ل طلب التسليم، بعد فحص المستندات، ومعه الملف، إلى وزير العدل الذي يتحقق من سلامة الطلب ويعطيه التتبع الإجرائي الملائم الذي يتطلبه القانون).³

3- تنفيذ أوامر تفتيش وحجز على الأجهزة الإلكترونية في الدولة الأجنبية: فهي تمثل صورة من صور المساعدة القانونية المتبادلة للإنابات القضائية الدولية، بحيث تُرسل الطلبات عبر الطرق الدبلوماسية وتنفذ وفقاً للقانون الوطني بشرط

¹ - المادة 883، قانون رقم 25-14 ، 2025، المتضمن لقانون الإجراءات الجزئية.

² - زبيحة زيدان، المرجع السابق، ص 144.

³ - المادة 865، نفس المرجع.

المعاملة بالمثل عن طريق وتنص المادة 16 من قانون 04-09 على: (في إطار التحريات أو التحقيقات القضائية الجارية لمعينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني. يمكن في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه).¹

4- استجواب الشهود أو المحققين من الدول الأخرى للحصول على معلومات قد تكون حاسمة في التحقيقات.

ثالثا: دور الإنابة القضائية الدولية في مواجهة جريمة التجسس الإلكتروني

تعتبر الإنابة القضائية الدولية آلية قانونية جوهرية في مواجهة جرائم التجسس الإلكتروني في مواجهة هروب وتستر الجناة في دول أجنبية، بحيث يتمثل دورها في النقاط التالية ذكرها:

1- الحصول على الأدلة الرقمية: وهي موجودة على خوادم (Servers) خارج الجزائر، بحيث تمكن الإنابة القضائية قاضي التحقيق من مطالبة الدولة الأجنبية بضبط، تجميد، أو نسخ هذه البيانات وتقديمها كأدلة قانونية صالحة للإدانة في هذا الصدد تنص المادة 50 من ق.إ.ج.ج على: (يمكن تجميد و/أو حجز الممتلكات والأموال والعائدات غير المشروعة الناتجة عن ارتكاب جريمة أو أكثر من جرائم المخدرات والمؤثرات العقلية /أو جرائم التهريب و/أو جرائم الاتجار بالبشر و/أو جرائم الاتجار بالأعضاء و/أو جرائم تهريب المهاجرين و/أو اختطاف الأشخاص و/أو المضاربة غير المشروعة و/أو جرائم تبييض الأموال وتمويل الإرهاب وتمويل

¹ - المادة 16، القانون رقم 04-09 الجزائري المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 47، اوت 2009.

انتشار أسلحة الدمار الشامل و/أو جرائم الفساد و/أو جرائم مخالفة التشريع المتعلق بالصرف وحركة الأموال من وإلى الخارج و/أو جرائم مخالفة القانون النقدي والمصرفي و/أو جرائم التهرب والغش الضريبيين و/أو جرائم الإرهاب و/أو الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.¹

2- توقيف المشتبه بهم: ففي حالة تحديد هوية الجاسوس إلكتروني وتواجده خارج الحدود، يتم إرسال إنابة قضائية دولية تتضمن أمراً بالقبض عليه، بهدف توقيفه مؤقتاً تمهيداً لتسليمه أو محاكمته في الدولة التي وقع فيها الضرر. " ولا تقتصر مهمة استقصاء الأدلة واتخاذ إجراءات التحقيق على الإقليم الجزائري، ذلك أنه قد يستلزم التحقيق اتخاذ إجراء في إقليم دولة أجنبية..."²

3- تبادل الأدلة: تتيح الإنابة نقل الأدلة والوثائق الفنية من التقارير المخبرية، التسجيلات، نتائج فحص الأجهزة بين الدول بسرعة، لضمان عدم اندثارها وكما تشمل تبادل المعلومات حول أنماط التجسس المستخدمة. وفي إطار الجرائم الإلكترونية أقرت الاتفاقية الأوروبية حول الجريمة الافتراضية، تبادل المعلومات في المادة 23 مهنا، بنصها صراحة على وجوب توافر التعاون الدولي بين الدول الأطراف وتعميقه، وتقليل العوائق، بما أكبر قدر من السهولة والسرعة لتبادل المعلومات والأدلة بين الأطراف.³

رابعاً: آليات التعاون الدولي في الإنابة القضائية

¹ - قانون الإجراءات الجزائية الجزائري.

² - بن يمينة أمينة، إجراءات الإنابات القضائية بالجزائر في المواد الجزائية، أطروحة دكتوراه في القانون العم تخصص القانون الاجرائي، الكلية الحقوق والعلوم السياسية، جامعة وهران2، 2021/2020.

³ - فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والسياسية، المجلد 8، العدد1، 2022، ص 440.

فيما يخص الجزائر، فإن الإنابة القضائية الدولية تعتمد على جملة من القوانين الوطنية والدولية التي تُسهم في تعزيز التعاون في مجال الجرائم الإلكترونية. القانون الجزائري يحدد آليات التعاون القضائي في الجرائم العادية والإلكترونية من خلال:

1- قانون الإجراءات الجزائية: وهو يتضمن قواعد الاختصاص وكيفية تنفيذ آليات طلب الإنابة القضائية ومن خلاله يتم تنظيم تنفيذها مع الشركاء الدوليين في إطار التعاون الدولي.

2- القانون رقم 09-04: وهو المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ومجال التعاون والمساعدة القضائية الدولية والاختصاص القضائي وكذلك مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

3- الاتفاقيات الدولية: أما على المستوى الدولي، فتعد اتفاقية بودابست حول الجرائم الإلكترونية أهم اتفاقية إقليمية التي نظمت التعاون بين الدول لمكافحة الجرائم الإلكترونية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014 وكذلك الاتفاقية الأممية لمكافحة الجريمة السيبرانية التي وقعت عليها الجزائر رسميا بتاريخ 24 أكتوبر 2025.

خامسا: تحديات الإنابة القضائية في الجرائم الإلكترونية

على الرغم من أهمية الإنابة القضائية الدولية في مكافحة الجرائم الإلكترونية، إلا أن هناك عدة تحديات قانونية وتقنية قد تعيق فعالية هذا التعاون، مثل:

1- التباين في التشريعات: تختلف قوانين الدول فيما يتعلق بالجرائم الإلكترونية وطرق ملاحقتها.

2- السرية والخصوصية: قد تواجه الدول صعوبة في تبادل البيانات المتعلقة بالخصوصية الشخصية أو الأمن القومي.

3- القيود التقنية: تتطلب التحقيقات في الجرائم الإلكترونية تقنيات متقدمة للغاية.

من خلال هذا المنظار، تأتي أهمية تطوير الأطر القانونية والتقنية في الدول المعنية من خلال تحديث التشريعات، وتعزيز التعاون الدولي، وتدريب الكوادر الفنية ومن خلال تعزيز هذه الآلية، يمكن للجزائر والدول الأخرى التعامل مع الجرائم الإلكترونية بشكل أسرع وأكثر فعالية، مما يساهم في الحفاظ على الأمن الرقمي على الصعيدين الوطني والدولي.

الفرع الثاني: انضمام الجزائر للاتفاقيات الدولية

لم تعد القوانين الداخلية وحدها كافية لمواجهة هذه الجرائم، بل تتمثل الحاجة في إطار دولي منسق للتبادل المعلوماتي وتيسير الإجراءات القضائية وتوحيد المفاهيم القانونية بين الدول.

في هذا السياق، يمثل انضمام الجزائر إلى المعاهدات الدولية المتعلقة بمكافحة الجرائم المنظمة والجرائم السيبرانية خطوة استراتيجية ضمن سياستها الجنائية الحديثة. إن أهمية هذا الانضمام يكمن أخذ الجزائر بعين الاعتبار الزيادة المتسارعة في الجرائم المعلوماتية، منها التجسس الإلكتروني وأخطاره المربكة، هذا ما يفرض نمطا جديدا من التعاون القضائي والأمني. وقد ساهمت العديد من الاتفاقيات الدولية والإقليمية في دعم النظام القانوني الجزائري في هذا المجال والتي سنذكرها.

أولا: اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية

تعد اتفاقية الأمم المتحدة لعام 2000، التي صادقت عليها الجزائر في أكتوبر 2025، إحدى الركائز الأساسية للتعاون الدولي ضد مختلف أشكال الجرائم المنظمة

عبر الوطنية، بما في ذلك استخدام التقنيات الحديثة، فهي تقدم إطار عمل يمكن تطبيقه على جرائم التجسس الإلكتروني كإحدى صور الجريمة المنظمة. ويمكن القول، ان هذه الاتفاقية الأمامية توفر للجزائر آلية دولية لتتبع مرتكبي جرائم التجسس الإلكتروني، خاصة عندما تتخطى الحدود الداخلية أو تتصل بشبكات إجرامية دولية. كما يعكس هذا الانخراط التزام الجزائر بمواكبة التطورات العالمية في مجال مكافحة الجريمة السيبرانية، وتطوير منظومتها القانونية بما يتماشى مع المعايير الدولية.

ثانيا: الاتفاقية الأوروبية بودابست - اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية

تعد اتفاقية بودابست لعام 2001 هي أول اتفاقية دولية متخصصة في مكافحة الجرائم السيبرانية وقد أثرت بشكل كبير على التشريعات الوطنية الحديثة المتعلقة بالجريمة الإلكترونية. توفر هذه الاتفاقية إطارا جنائيا وإجرائيا للتعاون الدولي، وتساعد على تبادل الأدلة الرقمية وحماية البيانات الإلكترونية وتعزيز التعاون بين السلطات المعنية. بالرغم من أن الجزائر ليست طرفا رسميا في هذه الاتفاقية، إلا أن العديد من مبادئها انعكست بوضوح في التشريع الجزائري وخاصة في القانون 04-09 الذي اعتمد العديد من الآليات الحديثة المستوحاة من روح هذه الاتفاقية.

ثالثا - الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

تهدف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة على المستوى الإقليمي بالقاهرة بتاريخ 21 ديسمبر 2010، إلى تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم الإلكترونية بما في ذلك جرائم التجسس الإلكتروني وتوحيد الجهود التشريعية والأمنية وتسهيل التعاون القضائي في مجال الجرائم المعلوماتية، مما يساهم في تبادل الخبرات والمعلومات. ويمكن القول ان هذه الاتفاقية تقدم للجزائر إطارا إقليميا للتعاون والتنسيق في مجال مكافحة التجسس الإلكتروني.

المبحث الثاني

السياسة العقابية والمسؤولية عن جريمة التجسس الإلكتروني

التوازن بين الردع الفعال وحماية حقوق الأفراد، مثل حق الخصوصية، هو تحدي كبير في تحديد العقوبات المناسبة لجرائم التجسس الإلكتروني. تتطلب هذه الجرائم إطارا عقابيا خاصا بها، مما دفع المشرع الجزائري إلى إعادة النظر في سياساته لتعزيز الردع وحماية الأمن القومي من الأخطار السيبرانية. يتضمن التشريع الجزائري تجريم الأفعال الإلكترونية وإنشاء نظام عقابي يأخذ في الاعتبار خطورة الجريمة، بما في ذلك فرض عقوبات على الأشخاص والشركات وتوسيع المسؤولية الجنائية لتشمل جميع المشاركين، سواء كانوا مشاركين بشكل مباشر أو غير مباشر. سنتناول في هذا السياق العقوبات المقررة للأشخاص الطبيعيين والمعنويين (المطلب الأول)، الظروف المشددة ومعوقات الملاحقة القضائية في (المطلب الثاني).

المطلب الأول

العقوبات المقررة للشخص الطبيعي والمعنوي

تعد العقوبة في القانون الجزائري وسيلة أساسية يعتمد عليها المشرع بهدف حماية النظام العام والحد من السلوكيات الإجرامية. وتظهر أهمية هذه الوسيلة بصورة أوضح في التشريع الجزائري عند التعامل مع الجرائم الإلكترونية، وهذا لما تنطوي عليه من آثار مباشرة على أمن الدولة وسرية معلوماتها. وانطلاقا من هذا المفهوم، عمل المشرع الجزائري على تطوير منظومة قانونية متخصصة تتناسب مع الخصائص المختلفة للجرائم المعلوماتية.

في هذا الإطار، سنتناول هذا المطلب بعرض العقوبات الأصلية والتبعية للأشخاص الطبيعيين في (الفرع الأول)، ومسؤولية الأشخاص المعنوية وعقوباتها في الجرائم الإلكترونية في (الفرع الثاني).

الفرع الأول: العقوبات الأصلية والتبعية للشخص الطبيعي

يتعرض الشخص العادي الذي يرتكب جريمة التجسس الإلكتروني في الجزائر لمنظومة عقابية صارمة، تُظهر مدى خطورة هذا النوع من الجرائم التي تهدد سيادة الدولة وأمنها القومي واستقرار مؤسساتها. وقد سعى المشرع الجزائري، من خلال القوانين ذات الصلة، إلى فرض عقوبات رئيسية وأخرى تبعية، تهدف إلى تحقيق الردع، ويظهر جليا من خلال المواد 61 الى 64 من قانون العقوبات التي تعالج التجسس كجناية ضد أمن الدولة، والمواد 394 مكرر إلى 394 مكرر 7 من القانون رقم 04-09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أولا : العقوبات الأصلية

تتفاوت العقوبات بحسب جسامة الفعل، تجسس لصالح دولة أجنبية، أو قرصنة بيانات أفراد/مؤسسات وتشمل العقوبات المقررة مثل الحبس والغرامات المالية، التي تهدف إلى ردع مرتكبي هذه الجرائم وهي:

1- عقوبة الإعدام: فقد أقرت المواد 61 الى 64 من ق.ع.ج عقوبة الإعدام في حالة ارتكاب أفعال الخيانة والتخابر والتجسس والتي توصف بجرائم موجهة ضد أمن الدولة الجزائرية، بحيث تنص المادة 64 على: (يرتكب جريمة التجسس ويعاقب بالإعدام كل أجنبي يقوم بأحد الأفعال المنصوص عليها في الفقرات 2 و 3 و 4 من المادة 61 وفي المادتين 62 و 63. ويعاقب من يحرض على ارتكاب إحدى الجنايات المنصوص عليها في هذه المادة والمواد 61 و 62 و 63 أو يعرض ارتكابها بالعقوبة المقرر للجنايات ذاتها).¹

¹ - المادة 64، قانون العقوبات الجزائري.

2- عقوبة السجن المؤبد: ينص مضمون المادة 65 على: (يعاقب بالسجن المؤبد كل من يجمع معلومات أو أشياء أو وثائق أو تصميمات بغرض تسليمها إلى دولة أجنبية والذي يؤدي جمعها واستغلالها إلى الإضرار بمصالح الدفاع الوطني أو الاقتصاد الوطني).¹

3- عقوبة السجن المؤقت: تنص المادة 63 مكرر 1 على: (يعاقب بالسجن المؤقت من عشرين (20) سنة إلى ثلاثين (30) سنة، كل من يقوم بتسريب معلومات أو وثائق سرية تتعلق بالأمن الوطني و/أو الاقتصاد الوطني، عبر وسائل التواصل الاجتماعي، قصد الأضرار بمصالح الدولة الجزائرية أو باستقرار مؤسساتها).²

ثانيا: العقوبات التبعية: تتضمن الحرمان من بعض الحقوق المدنية، مما يساهم في تحقيق العدالة الاجتماعية ويعكس خطورة الجريمة المرتكبة وبموجب المواد 394 مكرر وما بعدها، يمكن للقاضي الجزائي الحكم بعقوبات تكميلية، وجوبية أو جوازية وهي:

1- مصادرة الأجهزة: مصادرة العتاد والبرمجيات والوسائل المستخدمة في ارتكاب الجريمة (أجهزة حاسوب، هواتف، خوادم).

2- إغلاق الموقع/المحل: إغلاق المحل أو المكان الذي استغل في ارتكاب الجريمة مثل مقهى إنترنت إذا ارتكبت بعلم مالكه.

3- المنع من مزاوله نشاط: منع المتورط من مزاوله بعض الأنشطة المهنية.

¹ - المادة 65، نفس المرجع.

² - المادة 63 مكرر 1، نفس المرجع الذكر.

4-نشر الحكم: نشر ملخص للحكم بالإدانة في الصحف أو الوسائل الإعلامية على نفقة المحكوم عليه.¹

الفرع الثاني: مسؤولية الشخص المعنوي وعقوباته في الجرائم الإلكترونية
أولاً: تعريف الشخص المعنوي:

إن مضمون نص المادة 49 من القانون المدني الجزائري يؤكد على، أن الأشخاص المعنوية تشمل كل من الكيانات القانونية مثل الدولة، الولاية، البلدية، المؤسسات العمومية ذات الطابع الإداري، الشركات المدنية والتجارية، الجمعيات والمؤسسات، الوقف وكل مجموعة من أشخاص أو أموال يمنحها القانون شخصية قانونية التي يمكن أن تكون مسؤولة عن الجرائم الإلكترونية.² " ويعرف الشخص الاعتباري على أنه مجموعة الأشخاص أو الأموال التي تهدف إلى تحقيق غرض معين يعترف لها بالشخصية القانونية بالقدر اللازم لتحقيق ذلك الغرض".³

ثانياً : العقوبات: قد تشمل الغرامات المالية الكبيرة أو حتى إغلاق المؤسسة، مما يبرز أهمية الالتزام بالقوانين واللوائح المعمول بها.

الغرامة المالية: المادة 394 مكرر 4 من قانون العقوبات تنص على أن الغرامة للشخص المعنوي تعادل خمسة أضعاف (5 مرات) الحد الأقصى للغرامة المقررة للشخص الطبيعي.

2-العقوبات التكميلية: يمكن الحكم بعقوبات إضافية تشمل:

¹ - مفدي الناجح، ملتقى الثقافة القانونية، 10 ديسمبر 2024،

<https://www.facebook.com/groups/1517128068580577/members>

² -المادة 49 معدلة: القانون المدني الجزائري: الأشخاص الاعتبارية هي: - الدولة، الولاية، البلدية، - المؤسسات العمومية ذات الطابع الإداري، - الشركات المدنية والتجارية، - الجمعيات والمؤسسات، - الوقف، - كل مجموعة من أشخاص أو أموال يمنحها القانون شخصية قانونية.

³ - نبيل إبراهيم سعد: المدخل إلى القانون، نظرية الحق، منشأة المعارف للنشر، 2001، مصر، ص 212.

أ- حل الشخص المعنوي

ب- غلق المؤسسة أو إحدى فروعها بصفة مؤقتة أو دائمة.

ج- المنع من ممارسة النشاط

د- نشر الحكم الصادر بالإدانة.

المطلب الثاني

الظروف المشددة ومعوقات الملاحقة القضائية

يعترف جل القانونيون أن الجرائم الإلكترونية، وخاصة جريمة التجسس الإلكتروني، تعد من أخطر التحديات التي نتجت عن التطور التكنولوجي السريع في عالمنا الحديث، حيث يمكن أن يعرض الأمن الوطني للخطر، يستهدف مؤسسات حيوية، أو يؤدي إلى تسريب بيانات استراتيجية مهمة. أمام هذه البيئة المتغيرة، يسعى المشرع لتغليظ العقوبات كإجراء ردعي يحمي المصالح الحيوية للدولة ويصون الأمن العام. من ناحية أخرى، لا يمكن إغفال الصعوبات العملية التي تعترض مسار الملاحقة القضائية في هذا النوع من الجرائم.

بناء على ذلك، سنتناول هذا المطلب بالتطرق الى الظروف المشددة - إذا مست الجريمة الدفاع الوطني أو الأمن القومي في (الفرع الأول)، وإلى معوقات الملاحقة - الحصانات الرقمية، تشفير البيانات في (الفرع الثاني).

الفرع الأول: الظروف المشددة - إذا مست الجريمة الدفاع الوطني أو الأمن القومي

يعتبر فعل التجسس الإلكتروني في الجزائر كامتداد حديث للجرائم الماسة بأمن الدولة و" يعد المساس بالدفاع الوطني أو الأمن القومي في التشريع الجزائري من أخطر الجرائم، نظرا لتهديدها المباشر لسيادة الدولة، وحدة أراضيها، واستقرار مؤسساتها. يتبنى المشرع الجزائري سياسة جنائية صارمة -سياسة زجرية- تعتمد على تشديد العقوبات أو الظروف المشددة، لردع كل من تسول له نفسه الإضرار

بالمصلحة الوطنية العليا.¹ من هذا المنظور، أولى المشرع الجزائري اهتماما كبيرا لمكافحة هذه الجريمة، بالتالي وضع إطارا قانونيا يتضمن أحكاما صارمة تعكس أهمية حماية أمن وسيادة الدولة، خصوصا عندما إذا مست الجريمة الدفاع الوطني أو الأمن القومي، و تضمن قانون العقوبات عقوبات مشددة منها الإعدام و المؤبد في المواد 63 مكرر و 64 و تنص المادة 77 منه على: (يعاقب بالإعدام الاعتداء الذي يكون الغرض منه إما القضاء على نظام الحكم أو تغييره، وإما تحريض المواطنين أو السكان على حمل السلاح ضد سلطة الدولة أو ضد بعضهم البعض، وإما المساس بوحدة التراب الوطني. ويعتبر في حكم الاعتداء تنفيذ الاعتداء أو محاولة تنفيذه)². ويشمل التجسس الإلكتروني التسلل إلى الأنظمة المعلوماتية للمؤسسات الاستراتيجية أو العسكرية أو السيادية، والحصول على معلومات سرية ونقلها أو إفشائها لصالح أطراف أجنبية، وتزداد العقوبات صرامة إذا كانت الجريمة مرتبطة بظروف مشددة، مثل ارتكاب الجرم لصالح دولة أجنبية أو تنظيم معاد أو إذا كانت الجريمة تستهدف منشآت ذات طابع عسكري أو أمني حساس، أو إذا استخدمت تقنيات عالية التطور، ففي هذا الإطار تنص المادة 394 مكرر على: (تضعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة...)³، و المادة 394 مكرر 3 التي تنص: (يعاقب بالحبس من سنتين (2) إلى عشر (10) سنوات وبغرامة من 700.000 دج إلى 2.000.000 دج، إذا استهدفت الجرائم المنصوص عليها في هذا القسم الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال

¹ - بولبراشر إسراء، خميس لبنى، دوب نصيرة، الجرائم الماسة بأمن الدولة الخارجي في التشريع الجزائري، مذكرة ماستر،

كلية الحقوق والعلوم السياسية، جامعة سكيكدة، 2025، ص 77.

² - المادة 77، قانون العقوبات الجزائري.

³ - المادة 394 مكرر، المرجع السابق.

بتطبيق العقوبات الأشد¹. وبالتالي، يتبين أن المشرع الجزائري اتبع نهجا صارما في تعامله مع جرائم التجسس الإلكتروني، معتمدا على التشديد في الإجراءات والعقوبات.

أولاً: تعريف الظروف المشددة

في القانون الجزائري تشير الظروف المشددة إلى الحالات التي تزيد من خطورة الجريمة، مثل تلك التي تهدد الأمن القومي أو الدفاع الوطني.

ثانياً : أثر الظروف المشددة

تؤدي هذه الظروف إلى زيادة العقوبات المقررة، مما يعكس الجدية في التعامل مع مثل هذه الجرائم في التشريع الجزائري المادة 394 مكرر السالفة الذكر.

الفرع الثاني: معوقات الملاحقة - الحصانات الرقمية، تشفير البيانات، وتنازع الاختصاص

تواجه الملاحقة القضائية في الجرائم الإلكترونية، وبالأخص جرائم التجسس الإلكتروني، عديدا من الصعوبات القانونية والتقنية التي تزيد من تعقيد عمليات التحقيق والكشف عن هذه الجرائم وملاحقة مرتكبيها مقارنة بالجرائم التقليدية. ويرجع ذلك إلى طبيعة الفضاء الرقمي الافتراضي الذي لا يتقيد بالحدود الجغرافية ويمكن مرتكبي الجرائم من إخفاء هويتهم وتغيير البيانات بسرعة كبيرة، الأمر الذي يحد من فعالية الأساليب التقليدية للعدالة الجنائية وتخلق عوائق أمام أجهزة الضبطية القضائية والنيابة العامة أثناء تحريك ومباشرة الدعوى العمومية، ويمكن تقسيم هذه المعوقات إلى ثلاث نقاط رئيسية:

أولاً: الحصانات الرقمية وتحدي تحديد هوية الجاني

" تشير إلى الحماية الممنوحة لبعض المعلومات، مما قد يعوق الوصول إليها أثناء التحقيقات. تعد الحصانات الرقمية من أبرز المعوقات أمام ملاحقة الجناة

¹ - 394 مكرر 3، نفس المرجع.

قضائيا. ولا تشير هذه الحصانات إلى المفهوم القانوني المتعارف عليه كالحصانة الدبلوماسية، بل إلى صعوبة تحديد هوية الفاعلين في العالم الرقمي. فمرتكبو جرائم التجسس الإلكتروني عادة ما يلجؤون إلى تقنيات متنوعة مثل:

- استخدام عناوين IP مزيفة أو متغيرة،
- الاعتماد على شبكات افتراضية خاصة (VPN)،
- توجيه أنشطتهم عبر خوادم وسيطة تقع في دول مختلفة.

هذا التعقيد يؤدي إلى صعوبة توجيه الاتهام لشخص معين، ما يتعارض مع المبدأ الأساسي في قانون الإجراءات الجزائية الجزائري القائم على شخصية المسؤولية الجزائية وضرورة الإثبات القطعي للإدانة.¹ وفي حماية وتشفير البيانات تنص المادة الأولى من رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، على وضع قواعد خاصة للوقاية من هذه الجرائم: (يهدف هذا القانون الى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها).² كذلك اقرت المادة 16- الفقرة الاولى من نفس القانون، في إطار المساعدة القضائية الدولية المتبادلة على: (في إطار التحريات أو التحقيقات القضائية الجارية لمعينة الجرائم المشمولة بهذا القانون و كشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في شكل الالكتروني).³ ورغم أن القانون الجزائري رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها قد

¹ - <https://www.google.com/search> .

² - المادة 3، قانون رقم 09-04 ، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

³ - المادة 16، المرجع السابق.

وضع آليات للبحث والتحري في الجرائم الإلكترونية، إلا أن التطبيق العملي لهذه الآليات يعوقه التطور السريع لتقنيات التمويه الرقمي.

ثانيا: تشفير البيانات وتحدي الحصول على الأدلة الرقمية

يعتبر تحديا كبيرا أمام السلطات، حيث يصعب الوصول إلى المعلومات اللازمة للتحقيق وكما يمثل تشفير البيانات عقبة تقنية رئيسية تعترض الأجهزة المكلفة بالتحقيق، حيث يتم تشفير البيانات وتحويلها إلى رموز لا يمكن قراءتها إلا بوجود مفاتيح خاصة، مما يصعب عملية جمع الأدلة الرقمية وخاصة أن تلك الأدلة تتميز بسهولة تغييرها أو فقدانها بسرعة، ما يستلزم تدخلا تقنيا فوريا لجمع وتحليل البيانات قبل ضياعها.

في جرائم التجسس الإلكتروني، يستخدم التشفير على نطاق واسع لإخفاء:

- محتوى الرسائل والمعلومات المتبادلة - البيانات المسروقة أثناء نقلها

- مسارات الهجمات الإلكترونية.

وبالرغم من أن القانون رقم 09-04 يسمح باتخاذ إجراءات خاصة مثل اعتراض الاتصالات الإلكترونية أو جمع الأدلة الرقمية تحت رقابة قضائية، إلا أن هذه التدابير تظهر محدوديتها عند مواجهة تقنيات التشفير الحديثة والمتطورة، التي قد تتطلب التعاون الدولي واستخدام معدات عالية الكفاءة لفك الشيفرات.

ثالثا: تنازع الاختصاص

قد يحدث عند وجود أكثر من جهة معنية بالتحقيق، مما يعرقل الإجراءات القانونية ويؤدي إلى عدم فعالية الملاحقات القضائية في الجرائم العابرة للحدود تشكل الطبيعة العابرة للحدود للجرائم الإلكترونية تحدياً قانونياً عويصاً. ففي حالة جرائم التجسس الإلكتروني، قد يتم تنفيذ الجريمة انطلاقا من دولة ما بينما تكون الخوادم

المستخدمة موجودة في دولة أخرى، في حين يقع الضحية في دولة ثالثة.¹ هذا الواقع يفتح الباب أمام إشكالات قانونية تتعلق بما يلي:

– تحديد الدولة المختصة بالتحقيق والإجراءات القضائية.

– تنوع القوانين المحلية بين الدول بخصوص تعريف الجرائم الإلكترونية وتجريمها، مما يصعب ويحول دون تنفيذ الأحكام القضائية عبر الحدود الدولية.

في هذا السياق، يعتمد القانون الجزائري على قواعد التعاون الدولي المنصوص عليها في قانون الإجراءات الجزائية الجزائري، إضافة إلى الاتفاقيات الدولية الثنائية ومتعددة الأطراف والتي تشمل المساعدة القضائية وتسليم المجرمين. كما تستلهم السلطات الجزائرية إجراءاتها من اتفاقية بودابست لعام 2001 الخاصة بالجريمة السيبرانية، والتي تعد مرجعا دوليا للتنسيق بين الدول لمواجهة الجرائم الإلكترونية.

تتطلب جريمة التجسس الإلكتروني استجابة قانونية متكاملة تشمل إجراءات صارمة وتعاون دولي فعال، كما ينبغي تحديث التشريعات وتفعيل الآليات القانونية لضمان حماية الأمن القومي والمعلومات الحساسة. إن التحسين المستمر للقدرات القانونية والإجرائية يعد أمرا حيويا في مواجهة التحديات المتزايدة التي تطرحها الجرائم الإلكترونية. تواجه ملاحقة الجرائم الإلكترونية العديد من المعوقات، مثل الحصانات الرقمية التي تحمي بعض الأشخاص من الملاحقة القضائية، واستخدام تقنيات تشفير البيانات التي قد تعيق الوصول إلى الأدلة.

ويتعين على المشرع الجزائري العمل على توسيع نطاق آليات التعاون الدولي وتعزيز الإمكانيات التقنية للتحقيق الرقمي وتحديث التشريعات لتواكب التطورات السريعة في مجال التكنولوجيا الرقمية القادرة على التصدي لهذا النوع المتقدم من

¹ – **Cybercrime jurisdiction: issues and options**, UNODC – United Nations Office on Drugs and Crime, <https://www.youtube.com/@UNODCHQ>

الجرائم الخطيرة على أمن الدولة الجزائرية وسيادتها الرقمية وحماية خصوصيات مواطنيها.

الختمة

خاتمة

في ختام هذه الدراسة التي تناولت موضوع جريمة التجسس الإلكتروني في التشريع الجزائري، يتضح أن هذه الجريمة تعد من أخطر الجرائم المستحدثة التي أفرزها التطور التكنولوجي، لما تنطوي عليه من مساس مباشر بخصوصية الأفراد، وتهديد لأمن المعلومات، بل وامتداد آثارها إلى الأمن الوطني والسيادة الرقمية للدولة. وقد أظهرت هذه الدراسة أن جريمة التجسس الإلكتروني تتميز بخصائص تجعلها تختلف عن الجرائم التقليدية، سواء من حيث طبيعتها غير المادية، أو صعوبة اكتشافها، أو الطابع العابر للحدود الذي يميزها.

ومن خلال تحليل النصوص القانونية ذات الصلة، تبين أن المشرع الجزائري قد خطى خطوات مهمة في سبيل مكافحة الجرائم المعلوماتية عموماً، ولم يكرس مواد قانونية مستقلة حول جريمة التجسس الإلكتروني على وجه الخصوص رغم خطورة هذه الجريمة على السيادة الوطنية والأمن الوطني، وذلك من خلال إدراج نصوص قانونية تجرم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، إلى جانب وضع عقوبات تهدف إلى تحقيق الردع. غير أن هذه الجهود، رغم أهميتها، لا تزال تواجه بعض التحديات المرتبطة بسرعة تطور الوسائل التكنولوجية، وهو ما قد يؤدي إلى ظهور أشكال جديدة من التجسس الإلكتروني لا تغطيها النصوص الحالية بشكل كاف.

كما أظهرت الدراسة أن فعالية مكافحة جريمة التجسس الإلكتروني في الجزائر لا تتوقف فقط على وجود نصوص قانونية، بل تتطلب أيضاً إرادة سياسية قوية وواضحة المعالم وكذلك تفعيل آليات التطبيق، من خلال تعزيز قدرات الجهات المختصة في مجال التحري الرقمي، وتوفير التكوين اللازم للأجهزة الأمنية والقضائية، فضلاً عن تطوير وسائل التعاون الدولي، نظراً للطابع العابر للحدود الذي يميز هذه الجرائم.

وفي الأخير، تبقى مكافحة جريمة التجسس الإلكتروني في بلادنا مسؤولية مشتركة بين المشرع، والجهات الأمنية، والمؤسسات، والأفراد، الأمر الذي يستدعي تبني مقاربة شاملة تجمع بين البعد القانوني والتقني والتوعوي، بهدف تحقيق حماية فعالة للفضاء الرقمي، وضمان أمن واستقرار المجتمع في ظل التحول الرقمي المتسارع.

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

وعليه يمكن استخلاص النتائج التالية:

مع التطور المتسارع للأنظمة الرقمية والوسائل الإلكترونية، أصبح مفهوم التجسس أكثر تعقيدًا وتشعبًا، وغياب تعريف موحد للتجسس الإلكتروني مما يزيد من صعوبة تحديد ماهية التجسس الإلكتروني وحدوده، خاصة في ظل التغيرات المستمرة في البيئة الرقمية.

تتنوع جرائم التجسس الإلكتروني تنوعًا كبيرًا، حيث تختلف باختلاف الأهداف التي تسعى إليها، والوسائل التقنية المتاحة لارتكابها، ولم ينص المشرع الجزائي على جريمة التجسس الإلكتروني بشكل مستقل، وإنما اعتبرها كجريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات تسري عليها نفس الأحكام الموضوعية والاجرائية التي تسري على هذه الجرائم في محاولة لمواجهة الجرائم الإلكترونية، ومن بينها التجسس الإلكتروني، قام المشرع الجزائي بحماية المعطيات التي تحتويها

أنظمة المعالجة الآلية عن طريق تجريم أي تلاعب أو عبث بها، وامتدت هذه الحماية لتشمل بذلك جميع أنواع المعطيات بغض النظر عن حالتها مخزنة أو مرسلة أو معالجة.

في سياق التطور المتسارع للتكنولوجيا وتزايد التهديدات التي تواجه الأمن المعلوماتي، عمل المشرع الجزائري على تطوير الإطار القانوني لحماية المعطيات الرقمية سعياً لتعزيز الحماية القانونية للأنظمة المعلوماتية، وقد تم ذلك من خلال تعديل القسم السابع مكرر قانون العقوبات بموجب القانون رقم 24 - 06، حيث قام من خلال هذا التعديل بتشديد العقوبات المقررة على جرائم المساس بهذه الأنظمة، و لكن دون ان يخصص نص أو مواد تراعي خطر التجسس الإلكتروني وأن تجرمه ، وكذلك، أحدث المشرع الجزائري قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، دون الإشارة و الحرص على هذه الجريمة الخطيرة.

شدد المشرع الجزائري العقوبة على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إذا استهدفت هذه الأفعال الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، يأتي هذا التشديد نظراً لخطورة هذه الجرائم باعتبارها تهديداً مباشراً لأمن الدولة واستقرارها، حيث يمكن أن تؤدي إلى تسريب معلومات حساسة أو تعطيل البنية التحتية الحيوية، وبالتالي فإن جريمة التجسس الإلكتروني التي تستهدف عادة أنظمة المعالجة الآلية للمعطيات الحكومية تخضع لهذه العقوبات المشددة.

تعد جريمة التجسس الإلكتروني من الجرائم العمدية التي تقوم بالقصد الجنائي العام بعنصره العلم والإرادة، فيجب ان يعلم الجاني بأن حصوله على تلك المعلومات او البيانات قد تم بوجه غير مشروع وضد إرادة ورغبة صاحب السيطرة عليها مع اتجاه إرادته الى إثبات السلوك المجرم .

على ضوء النتائج السابقة خلصت الدراسة الى جملة التوصيات التالية:

1- ان وضع تعريف شامل ودقيق للتجسس الإلكتروني يمثل تحديا كبيرا في ظل التطور المتسارع للتكنولوجيا، ومع ذلك فإن هذا التعريف ضروري لضمان تطبيق القانون بشكل عادل وفعال، مع ضرورة أن يغطي هذا التعريف جميع أشكاله وصوره للتجسس الإلكتروني، دون ذكر وسائل ارتكاب الجريمة وذلك لضمان شموله لكافة الأشكال المستقبلية لهذه الجرائم.

2- ندعو إلى تعزيز وتكثيف التعاون الدولي لإبرام اتفاقية دولية لمكافحة التجسس الإلكتروني، تهدف إلى توحيد الجهود الدولية وتبادل المعلومات والخبرات بين الدول الأعضاء.

3- ندعو المشرع الجزائري لتحديث النصوص القانونية والتشريعية المتعلقة بالجرائم المعلوماتية وذلك لمواكبة تطور قطاع تكنولوجيا الاعلام والاتصال، مع ضرورة استحداث مواد خاصة في قانون العقوبات وتعديل قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ليتضمن مواد أو بند مخصص لجريمة التجسس الإلكتروني، وهذا من أجل التصدي لهذه الجريمة الخطيرة وكذلك إضافة عنصر التسرب في نصوص معدلة جديدة.

4- تعزيز الوعي المجتمعي بمخاطر التجسس الإلكتروني وكذا سبل الوقاية منه.

5- يجب تشجيع البحث التكنولوجي والتعليم المكثف للعلوم الدقيقة وعلم الحاسوب و الاعلام الالي والذكاء الاصطناعي والمعلوماتي بصفة عامة، من أجل الوصول الى: صنع منتوج جزائري وطني من المعدات والأجهزة الالكترونية والحساسة والحواسيب والهواتف...إلخ، وهذا لتفادي الاختراق والتصدي لعمليات القرصنة

والتجسس على أسرار الدولة واعتراض المراسلات... إلخ، من طرف القوى الدولية ومختلف أجهزة المخابرات.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

المراجع العربية:

أولاً: الكتب

- 1- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، بدون طبعة، دار المطبوعات الجامعية الإسكندرية، مصر، 2008.
- 2- زبيحة زيدان الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى - عين مليلة الجزائر.
- 3- نبيل إبراهيم سعد: المدخل إلى القانون، نظرية الحق، منشأة المعارف للنشر، 2001، مصر.
- 4- شوقي يعيش تمام، الجريمة المعلوماتية: دراسة تأصيلية مقارنة.
- 5- عبد الفتاح بيومي حجازي، الحماية القانونية لأمن المعلومات عبر شبكة الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2007.
- 6- عبد الفتاح بيومي حجازي، أمن المعلومات وحماية البيانات في عصر التكنولوجيا الرقمية، دار الفكر الجامعي، الإسكندرية، 2008.

ثانياً: الرسائل العلمية

أ- رسائل الدكتوراه:

- 1- نادية سلامي، آليات مكافحة التجسس الالكتروني، رسالة دكتوراه، جامعة العربي التبسي، كمية الحقوق والعلوم السياسية، 2019.
- 2- هبة نبيلة هروال، جرائم الانترنت، دراسة مقارنة، رسالة دكتوراه، جامعة أبي بكر بالقائد، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2014.

3- بن يمينة أمينة، إجراءات الإنابات القضائية بالجزائر في المواد الجزائية، أطروحة دكتوراه في القانون العم تخصص القانون الاجرائي، الكلية الحقوق والعلوم السياسية، جامعة وهران2، 2021/2020.

4- عثمانى رضوان، مكافحة جرائم المعلوماتية في القانون الجزائري والدولي، رسالة دكتوراه، جامعة وهران 2-محمد بن أحمد، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2024.

ب- رسائل الماجستير:

1-أحمد مسعود مريم، قريشي مجمد، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09، شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة قاصدي مرباح، الجلفة.

ج-مذكرات الماستر:

1- بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة ماستر، جامعة محمد البشير الابراهيمي برج بوعرييج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022.

2- بولبراشن إسرائ، خميس لبنى، دوب نصيرة، الجرائم الماسة بأمن الدولة الخارجي في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة سكيكدة، 2025.

3- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر مهني، جامعة قاصدي مرباح ورقلة، كلية العلوم الاقتصادية والعلوم التجارة وعلوم التسيير، قسم علوم التسيير، 2019.

4- كيحول عبد القادر، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية، شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، قسم الحقوق، جامعة زيان عاشور الجلفة، 2020/2019.

- 5- مصارة انفال، محلول منال، اجراءات التفتيش الالكتروني في التشريع الجزائري، ماستر أكاديمي القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية جامعة باتنة 1.
- 6- مقرح عبد الرؤوف، التجسس السيبراني الماس بأمن الدولة في التشريع الجزائري، مذكرة ماستر، جامعة برج بوعرييج، كلية الحقوق والعلوم السياسية، 2024.

ثالثا: البحوث والمقالات

- 1- حمز خضري، عشاش حمزة، خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، مجلد 6، عدد 2، 2020.
- 2- سامية بوشوشة، حياة سالماني، التجسس الالكتروني وطرق مكافحته، مجلة العلوم الاجتماعية، مجلد 16، عدد 01، 2023.
- 3- شوقي يعيش تمام، الجريمة المعلوماتية: دراسة تأصيلية مقارنة، مخبر أثر الاجتهاد القضائي على حركة التشريع، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الطبعة الأولى، 2019.
- 4- آسيا لعمراني، التعاون الدولي في مواجهة الجرائم السيبرانية: الجزائر نموذجا، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، المجلد 5، العدد 2.
- 5- إلهام بن خليفة وجمال غريسي، التجسس الإلكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري، مجلة دفاتر السياسة والقانون، مجلد 14، عدد 01، 2022،
- 6- أوشان حنان، وادي عماد الدين، التجسس الالكتروني واليات مكافحته في التشريع الجزائري، العدد الثاني، جويلية 2014.
- 7- بن مكي نجاة، محمود بوقطف، الخيانة العظمى جريمة ماسة بأمن الدولة في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، مجلد 1، عدد 1، 2014.

- 8- بوجوراف عبد الغني، التجسس كجريمة ماسة بأمن الدولة في ظل قانون العقوبات الجزائري، مجلة افاق للعلوم، جامعة الجلفة، مجلد 2، عدد 8، 2017.
- 9- سهيلة طمين، إشكالية التفتيش في الجريمة المعلوماتية المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، المجلد 20، العدد 1، 2025.
- 10- شويرب جيلالي، مراد فائزة، الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية، مجلة الدراسات القانونية والسياسية، المجلد 9، العدد 02.
- 11- فريد ناشف، أليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والسياسية، المجلد 8، العدد 1، 2022.
- 12- محمد خليفة، خصوصية الجريمة الالكترونية، وجهود المشرع الجزائري في مواجهتها، كلية الحقوق والآداب والعلوم الاجتماعية- جامعة 08 ماي 45 قالمة، موقع aspj.
- 13- مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجية الاعلام والاتصال، مجلة القانون، المجلد 09، العدد 01، 2020.
- 14- مشري سلمى، محاضرات في مقياس الجريمة الالكترونية السنة الثانية ماستر علوم جنائية، جامعة سطيف2.
- 15- مقلاتي مونة، بوخميس سهيلة، الحق في اعتراض سرية الاتصالات والمراسلات في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية: مجلد 3، عدد 2، 2019.
- 16- نجاري بن حاج علي فائزة، دراسة جريمة التجسس الإلكتروني، مجلة ستراتيجيا، جامعة مولود معمري، تيزي وزو، مجلد 16، العدد 11 السداسي الأول 2019.
- 17- هاشمي رشيد وملياني عبد الوهاب، المواجهة التشريعية لجريمة التجسس الالكتروني في ظل القانون 06-24، المجلد التاسع، العدد الأول، 2005.

- 18- يعيش تمام شوقي، خليفة محمد، نظام المعالجة الآلية للمعطيات الالكترونية كأساس للحماية الجزائية في التشريع الجزائري، جامعة بسكرة، مجلة جيل الأبحاث القانونية المعمقة، العدد 25، 2018.
- 19- يوسف صغير، جرائم الأنترنت جرائم، حقيقة في عالم افتراضي، مجلة معارف لجامعة البويرة مجلد 17، عدد 2، 2022.
- 20- خالد رجم، محاضرات في نظام المعلومات، جذع مشترك علوم اقتصادية وتجارية وعلوم التسيير، السنة الثانية، معهد التكنولوجيا جامعة قاصدي مرباح ورقلة، 2018/2017.
- 21- بن دراح علي إبراهيم، محاضرات في الجرائم المعلوماتية للسنة الثانية ماستر، معهد العلوم الحقوق والعلوم السياسية، قسم الحقوق، المركز الجامعي أفلو، الجزائر، 2020/2021.
- رابعا: النصوص التشريعية والقانونية

أ- الاتفاقيات الدولية

- 1- اتفاقية بودابست للجريمة المعلوماتية، 23 نوفمبر 2001، المجر.

ب- النصوص التشريعية:

- 1- دستور الجمهورية الجزائرية الديمقراطية الشعبية، 2020، مرسوم رئاسي رقم 20-442 مؤرخ في 15 جمادى الأولى 1442 الموافق لـ 30 ديسمبر 2020، الجريدة رقم 75.
- 2- القانون رقم 07-05 المؤرخ في 25 ربيع الثاني عام 1428 الموافق 13 مايو سنة 2007، المعدل والمتمم للأمر رقم 75-58 المتضمن القانون المدني، الجريدة عدد 31، 2007.
- 3- قانون رقم 25-25 مؤرخ أوت 2025، يتضمن قانون الإجراءات الجزائية الجزائري، رقم 54.

4- قانون رقم 24-06 مؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، المعدل والمتمم، قانون رقم 66-156 المؤرخ في 18 صفر 1386 هـ الموافق لـ 08 يونيو 1966، يتضمن قانون العقوبات.

5- قانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، 05 أوت 2009، الجزائر، عدد 47.

خامسا: المراجع باللغة الأجنبية

1 - Boudier Hadjira, Division Recherche et Développement en Sciences de l'Information, (CERIST), Bulletin d'information trimestriel, numéro 13, 2013, P P 17-20.

2- La Convention de Budapest sur la cybercriminalité, 23 novembre 2001, Budapest Hongrie.

3-BABAH Brahim, GHEHIOUECHE Alwalid, The Legal Framework for The Inspection of Information Systems in Algerian Legislation, Annals of Algiers University 1, Volume 39, N° 04, 2025.

سادسا: المواقع الالكترونية

- https://en.wikipedia.org/wiki/Cyber_espionage
- <https://www.sentinelone.com/>
- <https://asjp.cerist.dz>
- <http://dspace.univ-skikda.dz>
- <https://www.sentinelone.com/fr/cybersecurity-101/threat-intelligence/cyberespionage>
- <https://asjp.cerist.dz/en/article/217145#>
- <https://orionpolicy.org/cyber-espionage-and-u-s-policy-responses/#>
- https://en.wikipedia.org/wiki/Russian_interference_in_the_2020_United_States_elections.
- <https://www.sentinelone.com/fr/cybersecurity-101/threat-intelligence/cyber-espionage/>

- <https://www.investopedia.com/terms/i/industrial-espionage.asp>
- <https://skillogic.com/blog/what-is-cyber-espionage-in-cyber-security-types-prevention>
- <https://univ-soukahrass.dz/moodle/pluginfile>
- <https://dspace.univ-batna.dz/items/ebe2c3e4-4b2f-4f5d-a731-b058940775c8>

– سهيلة بوزبرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: revue critique de droit et sciences politiques، Volume 17، pp 560–575 2022،
<https://asjp.cerist.dz/en/article/209229>.

– مفدي الناجح، ملتقى الثقافة القانونية، 10 ديسمبر 2024،

. <https://www.facebook.com/groups/1517128068580577/members>

– <https://www.google.com/search>.

– Cybercrime jurisdiction: issues and options, UNODC - United Nations Office on Drugs and Crime, <https://www.youtube.com/@UNODCHQ>.

الفهرس

الفهرس

أ-ج	مقدمة
1	الفصل الأول: الإطار المفاهيمي والتجريبي لجريمة التجسس الإلكتروني
1	المبحث الأول: ماهية التجسس الإلكتروني وخصائصه
2	المطلب الأول: مفهوم جريمة التجسس الإلكتروني
2	الفرع الأول: تعريف التجسس الإلكتروني قانوناً ولغة واصطلاحاً وفقهاً
9	الفرع الثاني: تمييز التجسس الإلكتروني عن الاختراق والسرقة المعلوماتية
12	المطلب الثاني: خصائص التجسس الإلكتروني وأهدافه
12	الفرع الأول: الخصائص-العابرة للحدود، صعوبة الإثبات، سرعة التنفيذ والتخفي، قلة الإبلاغ عنها، محل وقوع جريمة التجسس الإلكتروني
17	الفرع الثاني: أهداف التجسس الإلكتروني
19	المبحث الثاني: الأركان المكونة لجريمة التجسس الإلكتروني
20	المطلب الأول: الأركان العامة لجريمة التجسس الإلكتروني
20	الفرع الأول: الركن الشرعي- النص القانوني
21	الفرع الثاني: الركن المادي- السلوك المادي
27	الفرع الثالث: الركن المعنوي- القصد الجنائي
29	المطلب الثاني: الركن الافتراضي لجريمة التجسس الإلكتروني
30	الفرع الأول: تعريف نظام المعالجة الآلية للمعطيات
34	الفرع الثاني: الحماية الفنية للنظام المعلوماتي كشرط لقيام المسؤولية الجزائية
34	الفصل الثاني: الآليات الإجرائية والموضوعية للمكافحة في القانون الجزائري
35	المبحث الأول: القواعد الإجرائية والوقائية لمواجهة التجسس الإلكتروني
35	المطلب الأول: أساليب البحث والتحري في الجرائم الإلكترونية
36	الفرع الأول: التفتيش الإلكتروني واعتراض الرسائل وفق قانون 09-04
49	الفرع الثاني: دور الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها
51	المطلب الثاني: التعاون الدولي في مجال مكافحة التجسس الإلكتروني
51	الفرع الأول: أهمية الإنابات القضائية الدولية في تعقب الجناة

58	الفرع الثاني: انضمام الجزائر للاتفاقيات الدولية
60	المبحث الثاني: السياسة العقابية والمسؤولية عن جريمة التجسس الالكتروني
60	المطلب الأول: العقوبات المقررة للشخص الطبيعي والمعنوي
61	الفرع الأول: العقوبات الأصلية والتبعية للشخص الطبيعي
63	الفرع الثاني: مسؤولية الشخص المعنوي وعقوباته في الجرائم الإلكترونية
64	المطلب الثاني: الظروف المشددة ومعوقات الملاحقة القضائية
64	الفرع الأول: الظروف المشددة - إذا مست الجريمة الدفاع الوطني أو الأمن القومي
66	الفرع الثاني: معوقات الملاحقة - الحصانات الرقمية، تشفير البيانات، وتنازع الاختصاص
71	خاتمة
75	قائمة المصادر والمراجع
82	الفهرس
84	ملخص

ملخص

تناولت هذه الدراسة موضوع جريمة التجسس الإلكتروني، وهي واحدة من أخطر الجرائم المستجدة التي أفرزتها التكنولوجيا، حيث تهدف إلى كشف آليات المواجهة القانونية لهذا النشاط الإجرامي في ظل التشريع الجزائري. تكمن إشكالية الدراسة في مدى كفاية النصوص التشريعية والقانونية الجزائرية الحالية في استيعاب التطور المتسارع لأساليب التجسس الرقمي وحماية السيادة المعلوماتية والخصوصية. وخلصت إلى أن المشرع الجزائري خطى خطوات هامة من خلال تعديل قانون العقوبات (04-15) وصدر القانون 04-09، حيث جرم الدخول غير المصرح به لأنظمة المعالجة الآلية للمعطيات. ومع ذلك، لا تزال هناك تحديات تتعلق بصعوبة الإثبات الرقمي، وتداخل المفاهيم بين التجسس الذي يمس أمن الدولة والشخصي، مما يتطلب تحديثا مستمرا للمنظومة الإجرائية لمواكبة هذه الجريمة الخطيرة العابرة للحدود.

الكلمات المفتاحية: التجسس الإلكتروني، التشريع الجزائري، الجريمة المعلوماتية، أمن الأنظمة، القانون 04-09.

Abstract:

This study concludes that cyber espionage is considered one of the most dangerous crimes resulting from technological development. It examines the effectiveness of Algerian legislation in combating this phenomenon, particularly through the Penal Code, the Code of Criminal Procedure, and the law on the prevention and combating of crimes related to information and communication technologies. The study highlights the significant steps taken by the Algerian legislator through the amendment of the penal code under Law 15-04 and the enactment of Law 09-04, which criminalize unauthorized access to information systems. Nevertheless, challenges remain, especially regarding the difficulty of digital evidence and the continuous evolution of cyber espionage methods, which requires constant updates to the legal and procedural framework in order to protect the Algerian State's information sovereignty and individuals' privacy.

Keywords: Cyber Espionage, Algerian Legislation, Cybercrime, Systems Security, Law 09-04.