جامعـــة أكـــلي محند أولحـــاج – البـــويـــرة–

كلية الحقوق والعلوم السياسية

قسم القانون العام

التصدي لجريمة التجسس السيبراني في إطار التشريع الجزائري والاتفاقيات الدولية

مذكرة ضمن متطلبات نيل شهادة الماستر في القانون العام

تخصص: قانون جنائي وعلوم جنائية

من إعداد الطالبة:

– معقاسي ريهام

تحت إشراف الدكتور:

– أ. د. زعادي محمد جلول

أعضاء اللجنة		
مزهود حكيم	جامعة البويرة	رئيسا
زعادي محمد جلول	جامعة البويرة	مشرفا
نبهي محمد	جامعة البويرة	ممتحنا

السنة الجامعية: 2026/2025

شكر وعرفان

الحمد لله أولاً وقبل كل شيء، الحمد لله الذي بنعمته وتوفيقه تم هذا العمل، والحمد لله الذي منحني القوة والصبر لأصل إلى نهاية هذا المشوار.

أتقدم بأسمى عبارات الشكر والامتنان إلى أستاذي الفاضل والمشرف **(زعادي محمد جلول)**، الذي لم يكن مجرد مشرف فحسب، بل أستاذًا رافقني بالتعليم والتوجيه طوال سنوات دراستي الجامعية، فكان نعم السند العلمي والناصح طوال فترة إعداد هذا العمل. كما يمتد شكري إلى كل أساتذتي الأفاضل، الذين كانوا سببًا في إنارة طريقنا بالمعرفة، ولهم الفضل الكبير في تلقينا التكوين العلمي وأدوات البحث التي مكنتنا من إنجاز هذا العمل.

وأتقدم بخالص الشكر وعظيم الامتنان إلى والديّ العزيزين، اللذين لا تكفي الكلمات ولا العبارات لرد جزء بسيط من فضلهما عليّ، فقد كانا السند الحقيقي في كل مراحل حياتي، وتحملًا معي التعب والضغط بصبر ومحبة دون كلل. وكان دعاؤهما الدائم يرافقني في كل خطوة، وكان وجودهما مصدر قوة وطمأنينة في أصعب اللحظات، فلهما مني كل الحب والامتنان والعرفان.

كما أشكر من أعماق قلبي عائلتي الغالية؛ إخوتي وأخواتي، كلٌّ باسمه، على دعمهم المتواصل ووقوفهم إلى جانبي في كل الظروف، وعلى كل كلمة تشجيع وكل موقف جميل خفف عني تعب هذا المشوار، فكنتم خير سند وخير رفقة في طريق الوصول إلى هذا النجاح.

وفي الختام، أتوجه بكل الشكر والمحبة إلى صديقاتي والمقربين مني، الذين شاركوني تفاصيل هذه الرحلة بكل ما حملته من تعب وضغط وفرح ونجاح، شكرًا لوجودكم الدائم إلى جانبي، ولدعمكم وتشجيعكم الذي كان يهون عليّ الكثير من اللحظات الصعبة،

إهـــــــــــــــــــــــــــــــداء

أهدي عملي الذي انتظرته طويلاً إلى من كانوا الدعم والعطاء

إلى من بذلوا جهد السنين من أجلي

أهدي هذا العمل إلى من كان يترقب هذه اللحظة بشغف

إلى أول سند في حياتي، إلى الروح الطاهرة التي غادرتنا قبل أن تشهد هذا اليوم، إلى من تمنيت أن يكون واقفًا بجانبي ليرى ثمرة دعائه وتشجيعه.. أبي الغالي رحمه الله.

أهدي له هذا العمل راجية من المولى أن يتغمده برحمته، وأن يكون فخوراً بما حققته اليوم.

إلى أمي السند الثابت في الحياة من سهرت وتعبت، منبع العطاء الصامت والقلب الكبير، من أبصرت بها طريق حياتي واعتزازي بذاتي، فلولا دعاؤها ما وصلت اليوم إلى هنا.

أهدي هذا العمل إلى كل من آمن بي وكان السند الذي لا يميل، إلى كل من ساندني طوال مسيرتي الدراسية.

إلى نفسي

في الختام أقف وقفة اعتزاز بنفسي، أهدي هذا العمل لنفسي تقديراً لكل مجهود بذلته، ولكل سنوات التعب التي عشتها لأصل إلى هذه المرتبة اليوم.

هذا النجاح لكم بقدر ما هو لي.

قائمة المختصرات

ص	صفحة
ص ص	من الصفحة إلى الصفحة
ج.ر	الجريدة الرسمية
د.ط	دون طبعة
ق.ع	قانون العقوبات
ق.إ.ج	قانون الإجراءات الجزائية

مقدمة

تتسارع الابتكارات التكنولوجية في عصرنا الحالي لتفرض واقع جديد أعاد تشكيل البنى التحتية للمجتمعات، حيث تحولت الشبكة العنكبوتية من مجرد أداة للتواصل إلى أساس تعتمد عليه الدول في تسيير أدق تفاصيلها الأمنية، السياسية والاقتصادية. وفي ظل هذا التحول، أصبحت المعلومات والبيانات في الوقت الراهن من أكثر الموارد قيمة؛ إذ لم يعد التنافس يقتصر على امتلاك الثروات الطبيعية أو القدرات العسكرية التقليدية فحسب، بل امتد ليشمل القدرة على الوصول إلى المعلومة للتحكم فيها وحمايتها. ومع هذا التوسع المتزايد وانتقال جانب كبير من الأنشطة الحيوية إلى البيئة الرقمية، برز الفضاء السيبراني كمجال جديد تتداخل فيه المصالح الاستراتيجية، وتتم من خلاله إدارة وتخزين كميات هائلة من البيانات التي تمس الأفراد والدول على حد سواء، لتصبح الأنظمة المعلوماتية والشبكات الرقمية الركيزة الأساسية للإدارات العمومية، المؤسسات الاقتصادية، والمنشآت الأمنية والعسكرية.

غير أن هذه المزايا والمنافع الرقمية رافقها بروز تحديات أمنية تمثلت في تنامي الجريمة المستحدثة العابرة للحدود، مما وفر للجماعات الإجرامية المنظمة بيئة افتراضية ملائمة لممارسة أنشطة غير مشروعة يصعب تتبعها أو كشف مرتكبيها، ولم تعد هذه الجرائم السيبرانية مقتصرة على ممارسات فردية عشوائية بدافع الكسب المالي أو التخريب، بل تقاطعت مع صراعات النفوذ الدولي، لتصبح الدول نفسها فاعلاً أساسياً في هذا الفضاء، تستخدمه كساحة حرب غير معلنة لضرب مصالح خصومها والاستيلاء على معلوماتها الحساسة.

وفي عمق هذه المواجهة الرقمية، ظهرت جريمة التجسس السيبراني كتهديد جديد يمس مباشرة سيادة الدول وأمنها القومي. وتتجاوز خطورة هذا السلوك الإجرامي حدود الأضرار التقنية أو المادية المباشرة، كونه يتحرك في الخفاء عبر خوارزميات وبرمجيات خبيثة تخترق الأنظمة الحيوية دون ترك أثر ملموس، مما يصعّب كشف هوية الفاعل وإثبات الجريمة، فهو بمثابة سلاح صامت قادر على زعزعة استقرار الدول وتدمير أمنها الداخلي دون إطلاق رصاصة واحدة. كما تتميز هذه الجريمة بخصوصية فريدة تميزها عن صور التجسس التقليدي، إذ لم يعد الجاني بحاجة إلى التواجد المادي داخل الإقليم المستهدف، بل أصبح بإمكانه اختراق أعمق أسرار الدولة عن بعد مستغلاً الوسائل التقنية الحديثة.

وأمام هذا التطور المتسارع والأخطار المتنامية للتجسس السيبراني، وجدت الدول نفسها أمام تحديات قانونية وأمنية غير مسبوقة، فرضت عليها ضرورة تحديث منظوماتها التشريعية

وآلياتها الوقائية والإجرائية، بالتوازي مع تعزيز أطر التعاون القضائي والأمني الدولي عبر الاتفاقيات الدولية والمنظمات المختصة لمجابهة هذا الخطر العابر للحدود.

ولم يكن المشرع الجزائري بمعزل عن هذه التحولات؛ إذ سعى جاهداً إلى مواكبة الطفرة التكنولوجية عبر استحداث ترسانة من النصوص القانونية والتدابير التنظيمية والإجرائية الرامية إلى حماية الأنظمة المعلوماتية الوطنية والتصدي للأفعال التي تستهدفها، والانخراط في الجهود الدولية والإقليمية ذات الصلة. ومع ذلك، فإن الطبيعة المتطورة باستمرار لأساليب التجسس السيبراني، وخصوصيته الإجرائية، تظل تثير عدة تساؤلات حول مدى كفاية وفعالية هذه الآليات القانونية المقررة لمواجهته وقمع أشكاله المختلفة على المستويين الوطني والدولي.

تكمن الأسباب الرئيسية في اختيار هذا الموضوع فيما يلي:

1. الأسباب الذاتية:

– الرغبة في دراسة جريمة حديثة وخطيرة فالتجسس السيبراني ليس مجرد جريمة فردية، بل تهديد يمس سيادة الدول وأمن المجتمعات، وهذا ما دفع إلى دراسته والتعمق فيه.

– الاهتمام بالمجال السيبراني وما يثيره من إشكالات قانونية وجنائية معاصرة.

– السعي إلى التعمق في موضوع يجمع بين الجوانب القانونية والتقنية والأمنية.

– الدافع العلمي للبحث في مجالات لها قيمة ميدانية وتطبيقية في الواقع الجزائري.

2. الأسباب الموضوعية:

– الإحساس بوجود فراغ علمي بسبب عدم وجود دراسات مقارنة جادة تجمع بين البعد الدولي والتشريع الجزائري في هذا الموضوع تحديداً.

– التطور المستمر لأساليب الاعتداءات السيبرانية مما يجعل الموضوع ذا أهمية علمية وقانونية.

– تنامي خطر التجسس الرقمي وتحوله إلى أداة أساسية في الصراعات الدولية الراهنة، مما يهدد السيادة الوطنية والبيانات الحساسة للدول.

وتتجلى أهمية دراسة هذا الموضوع فيما يأتي:

– تسليط الضوء على نوع من الجرائم لا يزال يتطور بسرعة تفوق قدرة التشريعات على مواكبته، مما يجعل البحث فيه ضرورة أكاديمية وعملية في آن واحد.

– إبراز خطورة التجسس السيبراني وأثره الكبير على الدول.

تتمثل الأهداف المرجوة من هذا البحث فيما يلي:

– تأطير مفهوم التجسس السيبراني تأطيراً قانونياً يميزه عن غيره من الجرائم.

– تحديد أركان الجريمة وفق المنظومة القانونية الجنائية الكلاسيكية وتكييفها مع خصوصية الفضاء الرقمي.

– رصد موقف المجتمع الدولي من هذه الجريمة من خلال الاتفاقيات والمعاهدات الدولية ذات الصلة.

– تبيان الموقف التشريعي الجزائري ومدى كفاءته في مواجهة التجسس السيبراني وتجريمه ومكافحته.

بينما تسعى المنظومة الدولية وتتطلع التشريعات الوطنية وفي مقدمتها المشرع الجزائري إلى صياغة أركان قانونية حاسمة وآليات إجرائية وتقنية قادرة على تحصين الأمن القومي المعلوماتي؛ فإن معضلة التجسس السيبراني تظل تتحدى هذا الاستقرار القانوني، وهو ما يطرح الإشكالية المحورية التالية: **ما مدى فعالية المنظومة القانونية المتبناة دولياً ووطنياً للتصدي للممارسات اللصيقة للتجسس السيبراني؟**

وللإجابة عن هذه الإشكالية، تم تقسيم هذه الدراسة إلى فصلين؛ خصص الفصل الأول للإطار النظري لجريمة التجسس السيبراني، وقسم إلى مبحثين، بحيث يتمحور المبحث الأول حول مفهوم هذه الجريمة، خصائصها، وتمييزها عن الجرائم المشابهة، بالإضافة إلى أبرز أساليب ارتكابها. بينما ركز المبحث الثاني على دراسة أركانها القانونية والإشكالات المرتبطة بها. أما الفصل الثاني، فقد خصص للبحث في استراتيجيات مكافحة هذه الجريمة؛ حيث خصص المبحث الأول لرصد الاستراتيجية الدولية والآليات المعتمدة، في حين ركز المبحث الثاني على الاستراتيجية الجزائرية والجهود الوطنية المبذولة للتصدي لجريمة التجسس السيبراني

ولمعالجة الإشكالية المطروحة في الدراسة تم الاعتماد على المنهج الوصفي لعرض مختلف المفاهيم المرتبطة بالموضوع، والمنهج التحليلي لدراسة النصوص القانونية الوطنية والدولية ذات الصلة وتحليلها، مع الاستعانة بالمنهج المقارن كلما اقتضت طبيعة الدراسة ذلك.

الفصل الأول

الإطار النظري لجريمة التجسس السيبرانى

تتسم حياتنا المعاصرة بتقدم تكنولوجي مذهل غير طريقة تعاملنا مع المعلومات، إلى درجة أصبح لا يمكن الاستغناء عن التكنولوجيا. فلم يعد تبادل المعلومات والوثائق ينفذ عبر الأساليب القديمة التي تتطلب وقتًا طويلاً، بل أصبحت هذه العملية تنجز بسرعة فائقة وبوسائل رقمية متقدمة تتيح للمستخدم الوصول إليها في أي وقت. ومع هذا التقدم الهائل ظهرت ممارسات سلبية تحمل في طياتها تهديدات جسيمة تهدد مستخدمي هذه التكنولوجيا.

نجد في مقدمة هذه التهديدات جريمة التجسس السيبراني، التي تعد من أخطر التحديات المعاصرة، لا سيما أنها مفهوم حديث على المجتمع الدولي، إضافة إلى صعوبة كشف مرتكبيها وتحميلهم المسؤولية القانونية. لم تعد هذه الجريمة مجرد أفعال فردية يقوم بها أشخاص بغرض الحصول على معلومات لخدمة مصالح شخصية أو لتحقيق ربح مادي فقط، بل تحولت إلى ساحة صراع بين الدول فيما بينها، حيث توظف هذه الأخيرة خبراء محترفين في المجال التقني للقيام بأعمال غير قانونية تهدف إلى كشف نقاط القوة والضعف لدى الدول المنافسة.

شهدت السنوات الأخيرة تصاعداً ملحوظًا لعمليات التجسس السيبراني، حيث باتت بعض الدول توظف قدراتها التقنية للوصول إلى بيانات حساسة تخص الدول الأخرى، وتجاوزت هذه الممارسات الغرض الدفاعي التقليدي، الذي كان يقتصر على كشف خطط الخصوم، ليصبح التجسس أداة هجومية تهدف إلى إلحاق الضرر بالدول، وأمام هذا الواقع بات من الضروري على المجتمع الدولي ومختلف التشريعات الوطنية لكل دولة تكييف وتطوير أطر قانونية تتلاءم مع طبيعة هذه الجرائم، مع وضع آليات ردع فعالة لمواجهة هذه التحديات المتزايدة.

ومن هذا المنطلق، ولفهم أعمق لهذه الجريمة، تم تقسيم الفصل الأول إلى مبحثين، بحيث خصص **(المبحث الأول)** لدراسة المفاهيم النظرية للتجسس السيبراني وما يحيط بها، بينما نسلط الضوء في **(المبحث الثاني)** على الأركان الأساسية التي تقوم عليها هذه الجريمة.

المبحث الأول

مفهوم جريمة التجسس السيبراني

يشكل التجسس أحد الأفعال المعروفة منذ القدم في تاريخ البشرية الطويل والمليء بالصراعات، استعملته الممالك والإمبراطوريات للإيقاع ببعضها البعض واستباق الخصوم لمعرفة خططهم بدقة قبل حدوثها أو الشروع في تنفيذها، واستخدمت فيه طرق تقليدية متنوعة مثل التنصت خلف الجدران العالية أو التفتيش السري في الأماكن المخفية بعناية أو حتى التسلل إلى الأماكن بهويات مزيفة، مما جعله أداة استراتيجية حاسمة في الصراعات القديمة بين الممالك.

تتجسس الدول في الوقت الحاضر على بعضها البعض في وقت وجيز، دون الحاجة إلى الدخول لساحة القتال كما كان في السابق أو تعريض عناصرها أو عملائها للخطر، فيكفي تكليف أشخاص ذوي كفاءة عالية وخبرة متخصصة في مجال الأنظمة المعلوماتية، وهم من يسمون بالجواسيس الإلكترونيين المحترفين الذين يعتمدون على أحدث البرمجيات والأدوات الرقمية في تنفيذ هذه العمليات.

لفهم هذه الجريمة، تم تقسيم هذا المبحث إلى مطلبين، بحيث خصص **(المطلب الأول)** لتقديم مختلف الجوانب المفاهيمية والقانونية للتجسس السيبراني، أما **(المطلب الثاني)** تم التركيز فيه على الجوانب العملية لتنفيذ هذه الجريمة.

المطلب الأول

تعريف جريمة التجسس السيبراني

التجسس السيبراني هو فعل غير قانوني يندرج ضمن الهجمات السيبرانية التي تستهدف أو تستخدم الشبكات المعلوماتية للحصول على بيانات سرية أو تعديلها أو حتى تدميرها دون وجه حق، وتتمثل خطورته في التعدي على أمن الدول، لذا تصنف هذه الجريمة من أخطر الجرائم التي يسعى القانون الدولي للحد منها ومعاقبة مرتكبيها. حاولت عدة تشريعات وطنية التصدي لهذه الجريمة، بما في ذلك المشرع الجزائري الذي أولى لهذه الجريمة أهمية بالغة،

إذ صنفها ضمن الجرائم الخطيرة من الدرجة الأولى لأنها تهدد السيادة الوطنية، غير أن المشرع الجزائري لم يقدم تعريفًا شاملاً لها، وهذا ما يزيد من صعوبة الإحاطة بها وبحدودها القانونية.

استناداً إلى ذلك، ينقسم هذا المطلب إلى فرعين، يتمحور **(الفرع الأول)** حول تقديم مختلف التعاريف المقترحة لهذه الجريمة، بينما يتمحور **(الفرع الثاني)** حول أهم خصائص هذه الجريمة وتمييزها عن الجرائم المشابهة.

الفرع الأول: معنى جريمة التجسس السيبراني

التجسس السيبراني من أخطر التحديات الرقمية الحديثة، وهو مصطلح حديث يكتنفه الغموض بسبب غياب تعريف محدد له في أغلب التشريعات، وهو الأمر الذي أدى إلى تضاعف الجهود على المستوى الفقهي لسد هذا الفراغ.

أولا: المعنى القانوني لجريمة التجسس السيبراني

يتبين عند دراسة قانون العقوبات الجزائري أن المشرع لم ينص على جريمة التجسس السيبراني، بل اكتفى بذكر التجسس بصفة عامة ضمن الجرائم الماسة بأمن الدولة في القسم الأول المتعلق بجرائم الخيانة والتجسس في المادة 64، حيث حددت هذه المادة الأفعال التي تدخل في حكم التجسس وتستوجب المساءلة الجنائية، إذ أشارت إلى أن الأفعال التي تدخل ضمن المواد 61 و62 و63 والتي تتعلق بالخيانة تشمل أيضا التجسس، وأقر المشرع الجزائري عقوبات صارمة على من يرتكب هذه الأفعال[1].

تشكل هذه الجريمة اعتداءً على مختلف قطاعات الدولة متى انصبت على الحصول على معلومات حساسة للإضرار بها، ويعد القطاع العسكري من أخطر ما يمكن المساس به لما يمثله من تهديد لقدرات الدولة الدفاعية. لذلك نص المشرع على هذه الجريمة في قانون القضاء العسكري في القسم الثاني المعنون بـــ"الخيانة والتجسس والمؤامرة العسكرية" من المواد 280

[1]– المادة 64 من أمر رقم 66–156 مؤرخ في 18 صفر عام 1386 الموافق 8 يونيو عام 1966، المتضمن قانون العقوبات، ج ر العدد 49، صادر في 21 صفر عام 1386 الموافق 11 يونيو سنة 1966، المعدل والمتمم.

إلى 282، حيث أقر عقوبة الإعدام لمن ورد ذكرهم في المادة 280 من القانون السالف الذكر[1] في حالة ارتكابهم جريمة التجسس، وعليه فإن المشرع الجزائري لم يقدم تعريفًا لهذه الجريمة.

ثانيا: المعنى الفقهي لجريمة التجسس السيبراني.

قبل التطرق إلى معنى التجسس السيبراني يجب أولا الوقوف عند التجسس التقليدي.

1. التجسس التقليدي.

يعرف (محمد الفاضل) التجسس بأنه كل سعي غير مشروع يهدف للحصول على معلومات أو وثائق تتعلق بأمن الدول، من شأنها كشف نقاط القوة والضعف للدولة المتجسس عليها[2].

في حين يرى (مناصرة عبد الله) أنه "كل فعل يقوم به شخص بمحض إرادته، بمعاونة دولة أخرى تسعى إلى الاطلاع على أسرار دولة أخرى، بكافة الوسائل المتاحة"[3].

بالنسبة (ليوسف الشفرة) فيرى أن التجسس يتمثل في القيام بأعمال احتيالية للوصول إلى معلومات محظورة يجب أن تبقى سرية، ثم نقلها وإعطائها إلى شخص أو جهة لا يخول لها أن تكون بحوزتها، أو التصرف فيها بنحو غير قانوني[4].

من خلال ما تم ذكره سابقا، يمكن تعريف التجسس بأنه كل نشاط محظور قانوناً يقوم به شخص بمعاونة دولة أخرى بالقيام بمجموعة من الأفعال التي تمكنه من الاستحواذ على معطيات سرية تضر بالدولة وأمنها القومي وذلك لتسليمها للدولة الأجنبية التي تساعده.

2. التجسس السيبراني

---

[1]– المادة 280 من أمر رقم 71–28، مؤرخ في 26 صفر عام 1391 الموافق 22 أبريل سنة 1971 يتضمن قانون القضاء العسكري، ج ر العدد 38، الصادر في 11 الثلاثاء 16 ربيع الأول عام 1391 الموافق 11 مايو 1971، المعدل والمتمم.

[2]– محمد الفاضل، الجرائم الواقعة على أمن الدول، الجزء الأول، الطبعة الثانية، مطبعة جامعة دمشق للنشر، سوريا، 1963 ص290.

[3]– مناصرة عبد الله، الاستخبارات العسكرية في الإسلام، الطبعة الثانية، دار الرسالة للنشر والتوزيع، بيروت، لبنان، 1991، ص15.

[4]– فريد ولد حسين، جرائم التجسس، مذكرة مقدمة لنيل شهادة الماجيستر في القانون الدولي الجنائي، مدرسة الدكتوراه، القانون الجنائي الدولي، معهد العلوم القانونية والإدارية، المركز الجامعي عباس لغرور –خنشلة–، 2011/2010، ص20.

اختلف الفقه في وضع تعريف جامع للتجسس السيبراني، الأمر الذي أدى إلى انقسامه إلى عدة اتجاهات رئيسية:

أ) الاتجاه الأول: التعريف الموسع.

يعتمد أنصار هذا الاتجاه على توسيع مفهوم التجسس السيبراني ليشمل كافة الأنشطة الإلكترونية الرامية إلى جمع المعلومات لصالح دولة أجنبية، بغض النظر عن طبيعة هذه المعلومات، سواء كانت أمنية أو سياسية أو اقتصادية أو غير ذلك. ويستند هذا الاتجاه إلى أن أي معلومة تكتسب بوسائل غير مشروعة وتمس بأمن الدولة تدخل ضمن نطاق هذه الجريمة[1].

في هذا الصدد، عرف (سليم عبد الله الجبوري) التجسس السيبراني بأنه: القيام بالاعتداء على منظومة معلوماتية بأية وسيلة وحيازة مختلف المعلومات التي تمس بالدولة[2].

ب) الاتجاه الثاني: التعريف الضيق

يذهب أنصار هذا الاتجاه إلى حصر مفهوم التجسس السيبراني في الأفعال السيبرانية التي تهدف إلى الحصول على معلومات عسكرية فقط، من خلال الدخول بدون وجه حق إلى أنظمة معلوماتية قصد الحصول إلى بيانات حساسة، باعتبارها الهدف الأساسي للدول المعادية، ويبررون ذلك بأن الاطلاع على هذه المعلومات يمكن أن يساعد العدو على فرض سيطرته على الدولة المستهدفة أكثر من المعلومات الأخرى، مما يشكل خطراً على أمن الدولة[3].

ت) الاتجاه الثالث: حسب طبيعة الجهة المستهدفة

يرتكز هذا الاتجاه على طبيعة الجهة المستهدفة، حيث ينقسم الفقه بين من يرى أن التجسس السيبراني ينصب على التعدي على المعطيات الشخصية للأفراد، بينما ترى الفئة الثانية بأنه فعل يستهدف الدول وسيادتها فقط.

- التعدي على معطيات شخصية

---

[1]- كركابو فطيمة، بحري سندس، التجسس الإلكتروني ضد امن الدولة، مذكرة مكملة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 -سكيكدة-، سبتمبر 2024، ص8.

[2]- سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، د ط، منشورات الحلبي الحقوقية للنشر، لبنان، 2011، ص325.

[3]- فتيحة خالدي، تأثير التجسس الإلكتروني على الحق في الخصوصية المعلوماتية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 07، العدد 01، جامعة ابن خلدون تيارت، السنة 2021، ص305.

يركز هذا الاتجاه على الأفعال التي تتضمن الدخول غير المشروع إلى أجهزة معلوماتية تخص أفراد أو منظمات، بهدف التجسس أو تحقيق مصالح شخصية أو مالية. ويرى أنصار هذا الاتجاه أن التجسس لا يقتصر على الحكومات فقط، بل يمكن أن يشمل الأشخاص، لكن انتقد هذا الاتجاه بحجة أن التجسس على الأفراد يشكل جريمة مستقلة، ولا يدخل بالضرورة ضمن جريمة التجسس، التي ترتبط أساسا بالدول، كما أن فاعلها غالبا ما يكون أجنبي.

وقد وصف (رمضان حسن ضاحي عبد الحافظ) في هذا الصدد التجسس السيبراني بأنه اختلاس معلومات تخص الأفراد أو المنظمات من خلال التطفل لاستغلالها بطرق غير مشروعة[1].

- الاستهداف السيادي

يرى أنصار هذا الاتجاه أن التجسس السيبراني يتمثل في سعي جهة أجنبية للوصول باستخدام الوسائل الإلكترونية، إلى معلومات أو بيانات حساسة تخص الدولة أو الجهات الرسمية أو الحكومات، بغرض الحصول على معلومات سرية يمكن استغلالها لتحقيق مصالحها أو إضعاف قدرات الدولة المستهدفة[2].

يعرف (علي جعفر) التجسس السيبراني في هذا الصدد بأنه الدخول غير القانوني باللجوء إلى مختلف التقنيات إلى الأنظمة المعلوماتية للدول والحكومات قصد أخذ كل ما يتعلق بأمنها ودفاعها أو أي مجال قد تستفيد منه الدولة الأجنبية في الإطاحة بالدولة المتجسس عليها.[3]

بناءً على ما سبق، يمكن تعريف التجسس السيبراني بأنه كل نشاط غير مشروع تقوم به جهة أجنبية، باستخدام الوسائل الرقمية والتقنية أو من خلال استهداف نظام معلوماتي، بقصد

---

[1]- رمضان حسن ضاحي عبد الحافظ، التجسس الإلكتروني عبر تقنيات الذكاء الاصطناعي "دراسة فقهية"، مجلة كلية الدراسات الإسلامية والعربية للبنات بسوهاج، العدد الحادي والثلاثون، الإصدار الأول، جامعة الأزهر، يونيو2025، ص791.

[2]- محمد عدنان عثمان، دور القانون الدولي في مواجهة التجسس الديبلوماسي، رسالة لنيل متطلبات الحصول على درجة الماجيستر في القانون العام، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط، يناير 2015، ص 16.

[3]- علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، د ط، منشورات زين الحقوقية، لبنان، 2013، ص 569.

الحصول على معلومات سرية تخص دولة، بهدف الكشف عن أسرارها أو الإضرار بمصالحها أو لتحقيق منفعة خاصة بالدولة الأجنبية.

يتشارك التجسس التقليدي والتجسس السيبراني في الهدف المرجو، وهو الحصول على معلومات حساسة للدول وتسليمها للغير، غير أنهما يختلفان في بعض الأمور منها:

التجسس التقليدي غالباً ما يعتمد على أساليب محدودة تقوم على الفعل المادي والوجود الفعلي في مكان الجريمة، مثل التسلل بصفة رسمية بهوية مزيفة إلى مكان تواجد المعلومات، في حين يتميز التجسس السيبراني بتعدد أساليبه وتطوره المستمر. كما يعد هذا الأخير أكثر تعقيداً لاعتماده على برمجيات ووسائل رقمية يصعب اكتشافها، مما يتطلب امتلاك الجاسوس مهارات تقنية عالية لتحكم في هذه البرمجيات، إضافة إلى صعوبة إثباته لأنه يتم بسرعة داخل الفضاء الإلكتروني[1].

أما التجسس التقليدي، فيكون أسهل من حيث الإثبات، كحالة ضبط الجاني أثناء تواجده في مكان الجريمة أو وجود أدلة ملموسة أو شهود، كما أن نطاقه غالباً ما يرتبط بوجود الجاسوس داخل الدولة المستهدفة، بخلاف التجسس السيبراني الذي يمكن ارتكابه عن بعد[2].

الفرع الثاني: خصائص وتمييز جريمة التجسس السيبراني بما يماثلها من جرائم

جريمة التجسس السيبراني من الجرائم التي تستمد خصائصها من البيئة الرقمية التي تنفذ فيها، مما يجعلها تختلف عن الجرائم التقليدية. كما تتميز هذه الجريمة بسمات تميزها عن غيرها من الجرائم المشابهة، لذلك خصص هذا الجزء من الدراسة لعرض أهم خصائص جريمة التجسس السيبراني والتمييز بينها وبين الجرائم المشابهة لها.

أولا: خصائص جريمة التجسس السيبراني

لجريمة التجسس السيبراني جملة من الخصائص كغيرها من الجرائم الإلكتروني، والتي تتمثل في:

1. جريمة عابرة للحدود

[1]– محمد بدوسي، الحماية الجنائية للأسرار الخاصة بأمن الدولة من التجسس الإلكتروني "دراسة مقارنة بين التشريعين الفلسطيني والأردني"، مجلة جامعة الاستقلال للأبحاث، مجلد10، عدد خاص، جامعة الاستقلال، آب 2025، ص11.

[2]– محمد بدوسي، المرجع السابق، ص12.

جريمة التجسس السيبراني لا ترتبط بمكان جغرافي محدود، فهي عابرة للحدود الدولية، لكونها تتم في الفضاء الرقمي، فلا يشترط من الجاسوس أن يكون في مكان تواجد المعلومات، بل يكفي أن تتوفر لديه الوسائل التقنية اللازمة مثل الحاسوب لارتكابها، لكن هذا لا ينفي أن يتواجد الجاسوس في المكان الذي يحتوي على نظام معلوماتي، فيدخل بطريقة خفية[1].

2. صعوبة الاكتشاف والإثبات

التجسس السيبراني من الجرائم الإلكترونية التي يصعب على الجهات المختصة كشفها وإثباتها، ويعود ذلك لاحترافية الجواسيس الذين يستخدمون وسائل حجب متطورة، تمكنهم من الدخول إلى النظام بطريقة سرية، دون ترك أي دليل مادي واضح. يعود ذلك لتنفيذ العملية بسرعة كبيرة لتجنب ترك ما يدينهم، وحتى عند كشف العملية يظل جمع الأدلة والتحقيق صعباً نظرا لمحو الأدلة ولقصور بعض تقنيات مكافحة هذا النوع من الجرائم، مما يتطلب من الجهات المختصة دائماً الحذر والحيطة[2].

3. الطابع الاستراتيجي لجريمة التجسس السيبراني

هذه الجريمة من الجرائم المنظمة القائمة على السرية والتخطيط المسبق، فيتم ارتكابها وفق استراتيجيات وخطط محددة مسبقًا، مع دراسة كل خطوة قبل بدء التنفيذ بعناية فائقة، وهذا بسبب أهمية المعلومات الحساسة المراد أخذها، وهو ما يميزها عن بعض الجرائم الإلكترونية الأخرى. فيمكن أن ترتكب هذه الأخيرة بطرق عشوائية دون تخطيط مسبق في بعض الحالات، بينما يقوم التجسس السيبراني على التخطيط والسرية لتحقيق أهداف ومصالح استراتيجية[3].

4. المجرم ذكي ومتخصص

---

[1]– حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجيستر في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر –باتنة–، 2012/2011، ص 17.

[2]– معاشي سميرة، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة الفكر، العدد السابع عشر، جامعة محمد خيضر بسكرة، جوان2018، ص 412.

[3]– مسكين سعيدة، الإطار القانوني للجريمة الإلكترونية في التشريع الوطني والدولي، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي في الحقوق، تخصص قانون الإنترنت والإعلام الآلي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي –برج بوعريريج–، 2025/2024 ص19.

على عكس الجرائم التقليدية التي يمكن لأي شخص تنفيذها، سواء في حالة غضب أو حتى بتخطيط مسبق، فإن الجاسوس السيبراني يجب أن تتوفر فيه مجموعة من الصفات، مثل الذكاء العالي إذ يعرف متى وكيف يدخل إلى النظام، إضافة إلى التخطيط بطريقة استراتيجية لتجنب كشفه. كما يجب أن يكون متخصصاً في التقنيات والمجال الرقمي، ملماً بكيفية استخدام البرامج والأنظمة التي تمكنه من الوصول إلى النظام المعلوماتي، أي أن هذا النوع من الانتهاكات الرقمية يتطلب كفاءات عالية ومهارات متقدمة[1].

5. التجسس السيبراني جريمة ناعمة

جريمة التجسس السيبراني ينعدم فيها العنف الجسدي، فهي جريمة هادئة تنفذ في الخفاء باستعمال البرمجيات الخبيثة والوسائل التقنية، ما يعني أنها تحتاج جهد ذهني أكبر من الجهد العضلي، عكس بعض الجرائم التي تعتمد على العنف وترك أثار ملموسة، ومع ذلك لا يمكن إنكار حقيقة الضرر الكبير الذي تسببه هذه الجريمة، والذي يكون أشد حدة من الجرائم العنيفة[2].

ثانيا: تمييز التجسس السيبراني عن الجرائم المماثلة له

يواجه الباحثين صعوبة في التفريق بين الجرائم المتشابهة، مما يعقد فهم طبيعة كل جريمة على حدة، لذلك من الضروري توضيح الفرق بين التجسس السيبراني وما يشابهه من جرائم.

1. التمييز بين جريمة التجسس السيبراني وجريمة الخيانة

بالرغم من أن المشرع الجزائري أدرج كلتا الجريمتين ضمن قسم واحد لارتباطهما بالمساس بأمن الدولة، إلا أنهما يختلفان من حيث عدة جوانب.

قبل معرفة كيفية التفريق بينهما يجب أولاً الوقوف عند تعريف جريمة الخيانة.

---

[1]– رحموني محمد، خصائص الجريمة المعلوماتية ومجالات استخدامها، مجلة الحقيقة، العدد 41، جامعة احمد دراية أدرار، 2018، ص443.

[2]– المرجع نفسه، ص 442.

تعرف جريمة الخيانة بأنها كل فعل يقوم به شخص يمتلك جنسية الدولة أي مواطن بحكم قوانينها بالتعامل مع دول أجنبية، سواء بإرادته أو تحت الإكراه، ويشمل ذلك تسليم كل ما قد يضر بدولته وذلك إما بمقابل أو بدون مقابل[1].

وللتمييز بين هاتين الجريمتين، لابد من دراسة عدة معايير تتمثل في:

أ) المعيار الذاتي

وفق هذا المعيار، يمكن التمييز بين الجريمتين بالاعتماد على القصد الجنائي للجاني أو الباعث، فإذا كان الهدف هو الحصول على معلومات لتحقيق منافع مادية، هنا الفعل يكيف على أنها جريمة تجسس. أما إذا ارتكبت بدافع الإضرار بالدولة فهي جريمة الخيانة. غير أن هذا المعيار يصعب تطبيقه، لكون الجريمتين يمكن ارتكابهما للحصول على مزايا مختلفة، كما يشتركان في المساس العمدي بمصالح الدولة، بالإضافة إلى ذلك من الصعب تحديد نوايا الجناة لمعرفة الباعث وراء جريمتهم[2]، ولذلك لا يمكن الأخذ بهذا المعيار، وخاصة إذا نظرنا إلى التشريع الجزائري الذي صنفهما على أنهما جريمتي المساس بأمن الدولة.

ب) المعيار الموضوعي

يقوم هذا المعيار على التمييز بين جريمتي التجسس السيبراني والخيانة من خلال طبيعة السلوك المرتكب، فالتجسس يتمثل في البحث عن المعلومات وجمعها باللجوء إلى مختلف الوسائل، في حين أن الخيانة تقوم على تسليم معلومات سرية إلى جهة أجنبية. غير أن هذا المعيار يعد غير عملي في الواقع، ذلك أن عملية البحث عن المعلومات غالبًا ما تتبعها عملية تسليم المعلومات المتحصل عليها، مما يجعل التجسس وفق هذا المعيار بمثابة أعمال تحضيرية تسبق الخيانة، وهو ما يؤدي إلى تداخل بين الجريمتين بدل الفصل بينهما[3].

---

[1]–عليلي عماد الدين، بن قسيس زين الدين، جرائم الخيانة وتسريب المعلومات والوثائق السرية على ضوء القانون 24-06 المعدل والمتمم لقانون العقوبات، مذكرة مكملة لمتطلبات نيل شهادة الماستر، تخصص قانون أعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 –قالمة–، 2025/2024، ص7.

[2]– بوشعبة محمد، الخيانة والتجسس في قانون القضاء العسكري، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة يحي فارس –المدية–، 2022/2021، ص9.

[3]– بوجوراف عبد الغاني، التجسس كجريمة ماسة بأمن الدولة في ظل قانون العقوبات الجزائري، **مجلة أفاق العلوم**، الجزء 01، العدد الثامن، جامعة الجلفة، جوان2017، ص ص338– 348 ص340.

ت) معيار الجنسية

يستند هذا المعيار إلى الاعتداد بجنسية الجاني كعنصر حاسم في التكييف القانوني للجريمة، بحيث يعد المساس بأمن الدولة خيانة إذا صدر عن أحد مواطنيها، في حين يكيف الفعل ذاته على أنه تجسس إذا ارتكبه أجنبي ليس له صلة بالدولة المستهدفة. تبنى المشرع الجزائري هذا المعيار، وهو ما يتجلى في المواد المنظمة لهاتين الجريمتين في قانون العقوبات، إذ نص على أن الخيانة تتمثل في الأفعال التي تصدر عن مواطن جزائري وتمس بالدولة، بينما التجسس هو كل فعل مماثل يصدر عن أجنبي[1].

2. التمييز بين جريمة التجسس السيبراني وجريمة الإرهاب الإلكتروني

تأثر الإرهاب بالتطور التكنولوجي المعاصر، فظهر نمط جديد يعرف بالإرهاب الإلكتروني، الذي يتم في الفضاء السيبراني، فلم يعد النشاط الإرهابي يقتصر على الأساليب التقليدية كالتفجير والتخريب المادي لممتلكات الدول، بل امتد ليشمل استغلال الأنظمة المعلوماتية وشبكات الاتصال في بث الرعب وشن الحروب على الدول.

يقصد بالإرهاب الإلكتروني اللجوء إلى الوسائل المستحدثة الرقمية في تنفيذ أعمال ذات طابع إرهابي، عن طريق استهداف الأنظمة بالتعطيل أو التخريب، أو توظيف البيانات في التحضير للهجمات الإرهابية أو تنفيذها، بما يهدف في النهاية إلى الضغط على الدول، أو ترهيب الأفراد لتحقيق أغراض معينة[2].

ورغم التشابه بين الجريمتين في بعض المسائل مثل استهداف الدول عبر استخدام وسائل إلكترونية، إلا أن هذا التشابه لا يعني تطابقهما من الناحية القانونية، فالاختلاف بينهما يبقى قائما في بعض الجوانب منها:

التجسس السيبراني يمس أمن الدولة الخارجي ويهدف إلى المساس بالمعطيات الإلكترونية لتسليمها إلى دول أجنبية، بينما الإرهاب يستهدف الأمن الداخلي ويهدف بالأساس إلى بث الرعب وزعزعة الأمن القومي وإثارة الفزع بين المواطنين ومحاولة الإضرار بالمجتمع.

---

[1]– بوعلي هالة، جريمة الخيانة والتجسس في التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي –تبسة–، 2022/2021، ص 55.

[2]– سليماني مباركة، الإرهاب الإلكتروني وطرق مكافحته، مجلة الحقوق والعلوم السياسية، المجلد 01، العدد 08، جامعة عباس لغرور –خنشلة–، جوان 2017، ص 343.

حتى المعلومات التي يجمعها الإرهابيون تستغل في التخطيط والتهديد، كما أن الإرهاب الإلكتروني غالبا ما يرتكب علناً ومن قبل جماعات منظمة، يوزع أفرادها الأدوار فيما بينهم بشكل منظم، في حين يمكن للتجسس أن ينفذه شخص واحد بسرية تامة دون الحاجة إلى دعم الأخرين[1].

قد يتقاطع التجسس السيبراني والإرهاب الإلكتروني في بعض الحالات، إذ قد يلجأ الإرهابيون إلى التجسس لتقصي عن المعلومات قبل تنفيذ هجماتهم، غير أن ذلك لا يعني أن كل فعل تجسس يعد عملاً إرهابياً، لأنه غالباً ما تلجأ إليه الدول للسيطرة أو التجسس ضد بعضها.

المطلب الثاني

أسس وأساليب تنفيذ جريمة التجسس السيبراني

يشكل التجسس السيبراني أخطر صور الإجرام المعلوماتي المستحدث، بالنظر إلى ما يترتب عنه من مساس بمصالح الدول، وذلك من خلال استهداف المعطيات ذات الطابع السري.

يقوم هذا الفعل على مجموعة من الأسس التي تبين طبيعة الجريمة ذاتها، إلى جانب اعتماد تقنيات حديثة تمكن الجاسوس من اختراق الأنظمة المعلوماتية أو استخدامها للوصول إلى البيانات المستهدفة والحصول عليها.

وعليه فإن دراسة التجسس السيبراني لا تقتصر على فهم ماهيته فقط، بل تشمل أيضاً تحليل الأسس التي يستند إليها لقيام الجريمة، مع الوقوف على أهم الوسائل المعتمدة في تنفيذ التجسس السيبراني.

للإلمام بالجريمة بشكل أدق يجب التركيز على الأسس التي تقوم عليهم الجريمة في **(الفرع الأول)**، ووسائل تنفيذها في **(الفرع الثاني)**.

الفرع الأول: أسس قيام جريمة التجسس السيبراني

جريمة التجسس السيبراني من الجرائم المعقدة التي تتطلب تحقق أسس معينة حتى يتم تصنيف الفعل المرتكب على أنه تجسس سيبراني، ولا يتحقق هذا الوصف إلا بتوافر أسس معينة.

[1]– نادية سلامي، آليات مكافحة التجسس الإلكتروني، أطروحة مقدمة لنيل شهادة دكتوراه في العلوم في القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي –تبسة–، 2019/2018، ص41.

أولا: الجاسوس السيبراني

لتحديد من هو الجاسوس السيبراني، يجب أولاً الوقوف على تعريفه، ثم معرفة كيفية تكوينه.

1. تعريف الجاسوس

مصطلح جاسوس مشتق من التجسس. ظهر لأول مرة في المادة 88 من قانون ليبر لعام 1863، الذي وقعه الرئيس الأمريكي أبراهام لينكولن خلال الحرب الأهلية الأمريكية.

تُعرف هذه المادة الجاسوس بأنه كل شخص يتسلل خفية أو يلجأ إلى وسائل الغش والخداع، بقصد الحصول على معلومات تتعلق بالعدو ونقلها إلى الطرف المعادي[1].

تناولت اتفاقية لاهاي لسنة 1907 هذا المصطلح في المادة 29، على أنه إذا استخدم شخص ما أساليب سرية للحصول على معلومات قد تضر بدولة ما، فإن هذا الشخص يعد جاسوسا، مع نصها على استثناء مفاده أنه إذا حصلت دولة أخرى على معلومات علناً، فإن ذلك لا يعد تجسساً، لأن جوهر التجسس يكمن في السرية[2].

يقصد بالجاسوس كل شخص يتسلل بطرق غير مشروعة للأنظمة الإلكترونية، مستعملاً وسائل تقنية خفية، بقصد الحصول على أسرار حساسة واستغلالها، وقد يكون مجند لدى الدولة ضمن أجهزة الاستخبارات، أو يتم الاستعانة به بصفة عرضية عند الحاجة.

يختلف الجواسيس من حيث درجة الاحتراف ومستوى المهارة التقنية، فمنهم من يمتلك قدرات محدودة لا ترتقي للأعمال المعقدة مثل التجسس، ومنهم من يتمتع بخبرة عالية تمكنه من دخول الأنظمة المعقدة وتجاوز وسائل الحماية، مما يجعل مواجهتهم أكثر صعوبة[3].

يتطلب التجسس السيبراني ذكاءً ومعرفة تقنية كبيرة لتجاوز الإجراءات الأمنية والحصول على المعلومات دون الكشف عن الهوية. كما يتطلب هذا النوع من الجرائم مهارات تحليلية وتخطيطية، بما في ذلك اختيار الأهداف المناسبة واستغلال الثغرات الأمنية، ولا يشترط

---

[1]– أحمد عبد السلام، الجاسوس في القانون الدولي، جوان 2019، مقال منشور على الموقع https://jordan-lawyer.com/ تاريخ الاطلاع 23 فيفري 2026، على الساعة 14:27.

[2]– المادة 29 من اتفاقية لاهاي الرابعة المتعلقة بقوانين وأعراف الحرب البرية واللوائح المرفقة بها، المعتمدة في 18 أكتوبر1907، دخلت حيز النفاذ في 26 يناير 1910.

[3]– بن شهرة شول، مراد مشوش، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية والسياسية، مجلد 04، العدد 01، المركز الجامعي بآفلو، جوان 2020، ص15.

للمخترق أن يكون محترفًا تلقى تعليمًا في هذا المجال، فقد يكتسب هذه المهارات مع الوقت. دون أن ننسى الباعث وراء فعله، سواء بدافع الولاء لدولته أو السعي وراء مصالح شخصية[1].

2. تكوين الجاسوس السيبراني

يمكن أن يكون الجاسوس السيبراني فرداً يعمل بمفرده، أو مجموعة من الأفراد الذين يتحكمون في استخدام التكنولوجيا، حيث تلجأ إليهم الدول للقيام نيابة عنها بالتنقيب عن معلومات تخص دول منافسة لها، كما قد يعمل لصالح الدولة نفسها التي تتولى تكوينه وتدريبه لخدمة مصالحها.

وفي هذه الحالة يخضع لتدريب منظم تشرف عليه أجهزة الاستخبارات، ليتعلم المهارات اللازمة لتنفيذ العمليات وطرق الاتصال السري المشفر مع الجهة التي يعمل لصالحها، إضافة إلى توفير تقنيات وأدوات يصعب تتبعها. ولا يقتصر التكوين على الجانب التقني فقط، بل يشمل أيضًا التأهيل النفسي، مثل التحفظ وعدم كشف المعلومات في حال القبض عليه، وقد يتم هذا التكوين بشكل فردي أو ضمن شبكات متصلة ببعضها البعض يشرف عليها شخص واحد[2].

لم يعتمد المشرع الجزائري مصطلح الجاسوس كوصف قانوني صريح في ق ع، وإنما ذكر صفة الأجنبي الذي يرتكب الأفعال التي تصنف في حكم التجسس، الأمر الذي يجعل صفة الجاسوس تستخلص من خلال السلوك الإجرامي المرتكب.

ثانيا: محل الجريمة

ترتكب جريمة التجسس السيبراني ضد جميع المصالح التي تمس بأمن الدولة، والمخزنة داخل الشبكات الإلكترونية أو كما يسميها المشرع الجزائري أنظمة المعالجة الألية للمعطيات، والتي لا يسمح لأي شخص الاطلاع عليها، إلا المخولون قانونًا بموجب مهامهم.

1. تعريف أسرار الدولة

[1]– بن شهرة شول، المرجع السابق، ص14.

[2]– سعودي رضا، قمع جريمة التجسس في التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماستر، تخصص سياسة جنائية وعقابية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي –تبسة–، 2017/2016، ص 36.

يقصد بأسرار الدولة تلك المعلومات والبيانات التي تمتلكها الدول وتحرص على إبقائها سرية لما لها أهمية في خدمة الدولة، وتشمل سجلات مكتوبة، صور، فيديوهات، ملفات تقنية وملفات صوتية وغيرها، تكون متصلة بمختلف المجالات، ويؤدي كشفها من طرف جهات معادية إلى تهديد سيادة الدولة وأمنها القومي، لذلك تعد هذه الأسرار الهدف الرئيسي الذي يسعى إليها الجواسيس والدول الأجنبية[1].

2. أنواع المعلومات المتجسس عليها

يمكن للجاسوس الوصول إلى مختلف المعلومات، والتي قد تتضمن:

أ) معلومات عسكرية: هي مختلف المعلومات التي تتعلق بالشق العسكري للبلاد من عتاد، أو فيديوهات لتكوين الجيش، أو عددهم وكيفية تدريبهم، أو نقاط ضعف المنشآت العسكرية، الأسلحة التي تمتلكها الدول ومواقعها، وغيرها من المعلومات التي تدخل ضمن هذا المجال وتعتبر هذه المعلومات من أخطر المعلومات التي اذا تسربت يقع ضرر كبير على الدولة[2].

ب) معلومات سياسية: تتمثل في البيانات التي تكشف الأحزاب السياسية وتوجهات الدولة لمعرفة كيف يمكن التأثير عليها، كذلك القرارات الداخلية والخارجية والسياسات العامة، والخطط الدبلوماسية التي تبين مواطن علاقات الدولة مع الدول الأخرى، والتي يكون كشفها قادر على صنع قرارات سياسية جديدة بين الدول[3].

ت) معلومات اقتصادية: هي كل معلومة من شأنها الإضرار باقتصاد الدولة، وتشمل خصوصاً الأسرار الصناعية والتجارية، مثل خطط الإنتاج، طرق التصنيع والتقنيات التكنولوجية، إضافة إلى الاستراتيجيات التسويقية ودراسات السوق، قوائم الزبائن والموردين والصفقات والعقود التجارية، وكذا البيانات المالية والتوقعات الاقتصادية المستقبلية للمؤسسات. ويؤدي تسريب

[1]– نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، 2010، ص211.

[2]– بولبراشن إسراء، خميس لبنى، الجرائم الماسة بأمن الدولة الخارجي في التشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 –سكيكدة–، جوان2025، ص 47.

[3]– المرجع نفسه، ص47.

مثل هذه المعلومات إلى إضعاف القدرة التنافسية للمؤسسات والقضاء على مكانتها في السوق العالمي[1].

ث) معلومات علمية وتكنولوجية: تخص الأعمال البحثية والتطورات التي حققتها المؤسسات في المجالات الطبية التقنية وغيرها، مثل الاختراعات، الابتكارات، التجارب العلمية أو التقنيات المتطورة، بهدف سرقة ما سبق ذكره إما لمنافسة الدول في السوق أو لتطوير ما تم سرقته لأخذ الأفضلية أو لتعزيز القدرات العلمية والتقنية على المستوى الوطني والدولي[2].

لا يقتصر التجسس على هذه المجالات فقط، بل يمتد إلى مجالات أخرى مثل التجسس الإعلامي الذي يستهدف وسائل الإعلام والتأثير في الرأي العام، والتجسس الثقافي الذي يهتم بدراسة توجهات المجتمعات وقيمها. غير أن هذه الدراسة تقتصر على أهم المجالات التي تمس بأمن الدولة.

الفرع الثاني: أساليب تنفيذ جريمة التجسس السيبراني

شهد مجال التجسس السيبراني تطور ملحوظ بسبب التكنولوجيا، مما أدى إلى تعدد الأساليب المستخدمة في هذه الجريمة، والتي تنقسم بشكل رئيسي إلى نوعين؛ الأول يتمثل في اختراق الأنظمة المعلوماتية للوصول إلى البيانات المخزنة، والثاني يعتمد على استخدام تقنيات حديثة لمراقبة الهدف وجمع المعلومات عنه دون الحاجة لدخول إلى الأنظمة، ومن أبرز هذه الأساليب:

أولا: الأساليب التي تستهدف الأنظمة المعلوماتية

هي مختلف الأساليب التي يلجأ إليها الجاسوس للدخول إلى نظام معلوماتي لأخذ المعلومات المرادة، هذه الأساليب متعددة نذكر منها:

1. التجسس بواسطة البرمجيات الخبيثة

هي برامج صنعت خصيصا لإلحاق الضرر بالمستخدمين، وهي من أكثر الأساليب المستخدمة في التجسس، يقوم الجاسوس بإدخالها في النظام بطريقة سرية دون معرفة المستخدم

[1]– هروال هبة نبيلة، جرائم الأنترنت" دراسة مقارنة"، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2014/2013، ص 373.

[2]– محمد عدنان عثمان، المرجع السابق، ص 33.

عن طريق استغلال الثغرات الأمنية، أو حتى إخضاع المستخدم على تحميل برامج ضارة في ظاهرها برامج مشروعة دون أن يعلم، وهي أنواع متعددة مثل:

برنامج الروتكيت (ROOTKIT) وهو برنامج يستخدم لإخفاء البرمجيات الضارة ومنع اكتشافها بوسائل الحماية. ثانيا برامج التجسس (SPYWARE) الهدف منها أخذ أكبر قدر ممكن من المعلومات، كذلك ما يسمى بالديدان الإلكترونية (WORMS) التي تتكاثر في الجهاز بسرعة كبيرة، بحيث تتسلل أولاً الدودة المضيفة إلى النظام، ثم تقوم بنسخ نفسها مرات عديدة مستغلة الثغرات الأمنية لتصل إلى أكبر قدر ممكن من المعلومات. كذلك أشهر البرامج وهو حصان طروادة (trojan horse) المبنى على الأسطورة الشهيرة، حيث يخفي نفسه في برنامج عادي، بحيث يقوم المستخدم بتثبيته دون أن يعلم حقيقته، وبعد التثبيت يتم تفعيل الشفرة الخبيثة، والتي تتيح للجاسوس الدخول إلى النظام والتحكم فيه عن بعد فيقوم بأخذ المعلومات أو التعديل فيها[1].

1. التجسس عن طريق برنامج بيغاسوس

يعتبر هذا البرنامج من أخطر البرامج، طورته شركة NSO GROUP الإسرائيلية للتجسس على الأجهزة الذكية عن طريق استغلال الثغرات الأمنية في أنظمة التشغيل، يمنح البرنامج للجاسوس صلاحيات واسعة في الوصول لكل محتويات الجهاز من رسائل ومكالمات وغيرها، وحتى تشغيل الكاميرا وتحويل المعلومات إلى خوادم أخرى دون معرفة المستخدم[2].

الجزائر من إحدى الدول التي تعرضت لهذا البرنامج، حيث كشف مقال صحفي على أنه تم استهداف كبار الشخصيات السياسية والعسكرية في الفترة بين 2017-2019، ومن أبرز

---

[1]- Advance DataSec، ما هو فيروس التجسس وكيف يختلف عن البرامج الضارة الأخرى، سبتمبر2025، مقال منشور على الموقع https://advance-datasec.com/، تاريخ الاطلاع 2026/03/11، على الساعة 7:43.

[2]- مريم نباش، سعاد بولقرون، التجسس وانتهاك حق الخصوصية في العصر الرقمي دراسة وصفية تحليلية لبرنامج "بيغاسوس"، مجلة الدراسات الإعلامية والاتصالية، مجلد 02، العدد 03، جامعة الجزائر 3، ديسمبر 2022، ص ص63-78، ص 8.

الشخصيات الرئيس السابق عبد العزيز بوتفليقة وعائلته، وبعض القادة والجنرالات مثل الفريق الأول أحمد صالح والجنرال واسيني بوعزة، إضافة إلى الوزير الأول السابق نور الدين بدوي[1].

ثانيا: الأساليب التي تستخدم التكنولوجيا لجمع المعلومات

في هذا الصدد، يقوم الجاسوس باستخدام وسائل تقنية لمراقبة الأهداف أو لجمع المعلومات دون الدخول إلى الأنظمة المعلوماتية، تتمثل هذه الأساليب في:

1. التجسس بواسطة الأقمار الصناعية

تعد الأقمار الصناعية اليوم من الوسائل الأكثر شيوعاً في ميدان التجسس، حيث تقوم بجمع معلومات عن مناطق أو أنظمة معلوماتية يصعب الوصول إليها. وتختلف أنواع القمر الصناعي باختلاف الهدف من إطلاقها، مثل أقمار المراقبة، وأقمار الاستطلاع، وأقمار الملاحة الجوية، لكن الأكثر أهمية هي الأقمار المخصصة للتجسس بين الدول، والتي تحتوي على مستشعرات وكاميرات عالية الدقة وأنظمة معالجة متطورة لنقل البيانات. يقوم القمر الصناعي أثناء مروره بمنطقة معينة التقاط الصور والإشارات وغيرها من المعطيات، من خلال اعتراض المراسلات واعتراض الاتصالات اللاسلكية، مع القدرة على العمل تحت مختلف الظروف بفضل التقنيات المتطورة التي يمتلكها. كما ترسل البيانات إلى محطات أرضية عبر اتصالات لا سلكية مشفرة لا يمكن فكها إلى من الجهة المرسلة للقمر لضمان السرية[2].

2. التجسس بواسطة أجهزة البوليمرات:

تنفذ الجريمة عبر أجهزة مصنوعة من مواد بوليمرية قابلة للتحلل، يتم تصنيع أجهزة استشعار ودوائر إلكترونية دقيقة يمكن دمجها داخل الأجهزة المستهدفة، فتقوم بتحليل المتغيرات في البيئة الموجودة فيها، ثم تقول بتحويلها لإشارات كهربائية التي تعالج وتنقل على شكل بيانات ترسل إلى الجاسوس، مما يسمح له بالحصول على ما يريد، قبل أن تتحلل أو تتفكك

---

[1] – تاهمي مصطفى، مستقبل الأمن القومي الجزائري في ظل التطورات التكنولوجية وحروب المعلومات، أطروحة مقدمة لاستكمال متطلبات شهادة الدكتوراه في العلوم السياسية وعلاقات دولية، تخصص علاقات دولية واستشراف، قسم الدراسات الدولية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، 2024/2023، ص 155.

[2]– مناد فتيحة، مدى شرعية الاستطلاع العسكري والتجسس من الفضاء الخارجي باستخدام الأقمار الصناعية –دراسة قانونية–، مجلة القانون العام الجزائري والمقارن، المجلد الرابع، العدد الثاني، جامعة الجيلالي اليابس سيدي بلعباس، 2018، ص 160-161.

بعد فترة محددة أو عند تلقى إشارة معينة. ظهرت هذه التقنية أول مرة في الولايات المتحدة الأمريكية في أبحاث علمية بطلب من وزارة الدفاع، وذلك لاستغلالها في جمع المعلومات بسبب سرعتها في التحلل بعد تحقيق الهدف[1]. فعلى سبيل المثال، يمكن دمج هذه التقنية داخل جهاز إلكتروني في غرفة اجتماعات، حيث تقوم بالتقاط الاهتزازات الناتجة عن الكلام، ثم تحويلها إلى إشارات كهربائية تُرسل إلى نظام آخر يقوم بتحليلها لمعرفة ما يحدث داخل الغرفة.

3. التجسس عن طريق طائرات بدون طيار (الدرون)

هي طائرات ذات حجم صغير تسير بدون طيار يتم التحكم فيها عن بعد، ترسلها الجهة الأجنبية للتجسس، وذلك لأغراض منها الاستطلاع والاستكشاف، من خلال الكاميرات وأجهزة الاستشعار المثبتة فيها، يمكنها التجسس على مختلف منشآت الدولة والمواقع الحساسة التابعة لها، مثل تسييرها فوق موقع عسكري أو سفارة لمعرفة هيكل المنشاة، كما يمكن في بعض الحالات تزويدها بأجهزة إلكترونية تمكن من التقاط بعض الإشارات أو محاولة الوصول إلى الشبكات اللاسلكية القريبة منها، ويتم التحكم فيها عن بعد بواسطة أنظمة اتصال لاسلكية أو عبر الأقمار الصناعية[2].

4. التجسس بواسطة تقنية البيوبوت

تمثل هذه التقنية واحدة من أكثر التقنيات الحديثة إثارة في مجال التجسس، حيث يتم دمج التكنولوجيا بالطبيعة، فيمكن تزويد بعض الحشرات بمكونات إلكترونية دقيقة مثل المستشعرات وأجهزة الاتصال، مما يسمح بالتحكم فيها عن بعد. تتم هذه العملية إما بتصميم روبوتات تكاد لا ترى تحاكي شكل الحشرات الحقيقية، أو بزرع أجهزة داخل حشرات حية، ثم توجيهها

---

[1]– ديلي ميل، أجهزة تجسس أمريكية من نوع غريب، أوت 2019، مقال منشور على الموقع https://arabic.rt.com/world، تاريخ الاطلاع 2026/02/29، على الساعة 10:13.

[2]– مصطفى شريف، اقتحام الدرونات لعالم التجسس والاختراق السيبراني، مقال منشور على الموقع https://itach.dk/drone-between-hacking-and-espionage/، تاريخ الاطلاع 2026/03/01، على الساعة 21:55.

للهدف لمراقبته والحصول على المعلومات، تقوم هذه الكائنات بنقل البيانات والصور إلى الجهة المرسلة التي تتحكم فيها عبر إشارات لاسلكية[1].

5. التجسس بواسطة الذكاء الاصطناعي

مع التطور السريع لتقنيات الذكاء الاصطناعي، أصبح يستعمل حتى في عمليات التجسس السيبراني. ويقصد به مجموعة من الأنظمة الذكية القادرة على معالجة كميات هائلة من المعلومات بسرعة فائقة، والتعرف على أنماط وسلوكيات في البيانات لا يستطيع البشر اكتشافها بسهولة، مما يعزز قدرات الحكومات على فهم تحركات الخصوم واتخاذ قرارات استراتيجية أسرع وأدق. كما يمكن استغلال أنظمة الذكاء في تنفيذ هجمات تجسسية معقدة أو تحسين قدرات المتسللين[2].

المبحث الثاني

أركان جريمة التجسس السيبراني

يستلزم التحديد القانوني لأي فعل قانوني، الانتقال من مرحلة ضبط المفاهيم المتعلقة بالفعل إلى مرحلة حصر أركان الجريمة؛ باعتبارها الركيزة الأساسية للتكييف القانوني الصحيح، والمنطلق الرئيسي لإسناد المسؤولية الجنائية.

---

[1]– الهام بن خليفة، جمال غريسي، التجسس الإلكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري، مجلة دفاتر السياسة والقانون، مجلد 14، عدد 01، جامعة قاصدي مرباح ورقلة، 2022، ص 165.

[2]– *اندبندنت العربية، التجسس والذكاء الاصطناعي... من الإنسان وعنه وعليه، افريل 2025، مقال منشور على الموقع* https://www.independentarabia.com/، *تاريخ الاطلاع 2026/03/11، على الساعة 7:52.*

فبعد توضيح مفهوم جريمة التجسس السيبراني في المبحث السابق، تبرز الحاجة الآن إلى البحث في بنيتها القانونية؛ إذ لا يمكن معاقبة الجاني أو توصيف فعله بأنه اعتداء غير مشروع إلا إذا توفرت في فعله أركان محددة ينص عليها القانون

وتأسيساً على ذلك، فإن قيام جريمة التجسس السيبراني مرهون بتوفر ثلاثة أركان متمثلة في الركن الشرعي والمادي والمعنوي، وتعد هذه الأركان ضرورية لقيام الجريمة، غير أن تطبيقها في المجال السيبراني يثير عدة صعوبات، خاصة فيما يتعلق بتحديد السلوك الإجرامي بدقة وإثبات القصد الجنائي، نظراً لخصوصية البيئة الرقمية وتعقيدها.

وعليه، يهدف هذا المبحث إلى استجلاء أركان هذه الجريمة، من خلال تخصيص **(المطلب الأول)** لدراسة الركن الشرعي، أما **(المطلب الثاني)** فللركن المادي، وأخيراً **(المطلب الثالث)** للركن المعنوي.

المطلب الأول

الركن الشرعي لجريمة التجسس السيبراني

يعد الركن الشرعي أساس قيام الجريمة في القانون الجنائي، وهو التجسيد الفعلي لمبدأ الشرعية الذي يقتضي وجود نص سابق يجرم الفعل ويحدد العقوبة المقررة له، مع عدم خضوع الفعل لسبب من أسباب الإباحة. غير أن إعمال هذا المبدأ في مجال التجسس السيبراني يثير إشكال عملي، بسبب الطبيعة الخاصة لهذه الجريمة التي ترتكب داخل بيئة رقمية عابرة للحدود، إضافة إلى التطور المتسارع للتكنولوجيا الذي يفوق قدرة النصوص القانونية على مواكبة أفعال الجريمة وضبط نطاقها بدقة، مما قد يؤدي إلى فراغ تشريعي.

انطلاقًا من هذا، ولدراسة هذا الركن يقتضي البحث في المصادر القانونية التي تجرم التجسس السيبراني، سواء على المستوى الوطني أو الدولي، وذلك من خلال التطرق إلى الإطار التشريعي الجزائري في **(الفرع الأول)**، والاتفاقيات الدولية ذات الصلة في **(الفرع الثاني)**.

الفرع الأول: الإطار التشريعي الجزائري

كرس المشرع الجزائري مبدأ الشرعية من خلال عدة نصوص، لا سيما المادة 43 من التعديل الدستوري لسنة 2020 التي تنص على أنه "لا يمكن إدانة أي شخص إلا بقانون صدر

قبل ارتكابه للفعل"[1]، وكذا المادة الأولى من قانون العقوبات التي تؤكد المبدأ ذاته، وبموجب هذا المبدأ، وبسبب غياب نص خاص يجرم التجسس السيبراني بصفة مستقلة، وجد المشرع الجزائري نفسه أمام حتمية معالجة هذه الأفعال ضمن النصوص الموجودة في ق ع، من خلال تجريمها ضمن أحكام المواد التي تتقاطع أفعالها مع صور السلوك الإجرامي لهذه الجريمة.

أولا: تجريم التجسس السيبراني من خلال قانون العقوبات الجزائري

جرم المشرع الجزائري جريمة التجسس ضمن المواد التي تجرم أفعال المساس بالدفاع الوطني للدولة. لكن ليست كل هذه الأفعال تندرج ضمن التجسس السيبراني، بسبب طبيعته المرتبطة بالفضاء السيبراني، ومع ذلك فإن اعتماد المشرع لعبارة "بأي وسيلة كانت" في بعض الأفعال يسمح بتوسيع نطاق التجريم ليشمل مختلف الأفعال والوسائل المرتكبة إلكترونيا، إلى جانب الوسائل التقليدية في تنفيذ الجريمة[2].

على هذا الأساس يمكن تقسيم أفعال التجسس التي جاءت بها هذه المواد إلى صورتين:

الصورة الأولى يكون فيها التجسس محصور في الإطار التقليدي المحض فلا يمكن تصوره بطريقة أخرى، والصورة الثانية يمكن أن تتحقق عبر الوسائط الرقمية، مثل التخابر مع دولة أجنبية الذي يحتمل وقوعه بطرق تقليدية مثل الاجتماعات السرية، أو عبر وسائل الاتصال الحديث، وهو ما يفهم ضمنياً من عدم تحديد الوسيلة المستعملة في النص، مما يفتح المجال لإدراج الوسائل الإلكترونية ضمنها.

وكذلك الأفعال التي تتعلق بالحصول أو نقل أو إتلاف معلومات من شأنها الإضرار بالدولة، بأي طريقة كالدخول وتخريب منظومة معلوماتية تابعة لجهات حكومية وتمكين الغير منها[3].

ويلاحظ أن المشرع لم يربط قيام الجريمة بظرفي السلم أو الحرب، فالقانون الجزائري يجرم هذه الأفعال في كل الأحوال متى تم المساس بالدولة، بغض النظر عن طريقة ارتكاب الفعل كيف تم أو الوسيلة المستعملة.

---

[1]– المادة 43 من مرسوم رئاسي رقم 22–442 مؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر لسنة 2020، يتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر سنة 2020، ج ر العدد 82.

[2]– نادية سلامي، المرجع السابق، ص 188.

[3]– المادة 63 من أمر رقم 66–156 المتضمن قانون العقوبات، السالف الذكر.

غير أن هذه الأحكام، رغم دورها تبقى غير كافية لمواجهة الأشكال المستحدثة لهذا النوع من الجرائم، وهو ما دفع المشرع إلى إدخال تعديلات على ق ع بالقانون رقم 04-15[1]، حيث تم بموجبه استحداث القسم السابع مكرر والمتعلق بالجرائم التي تمس أنظمة المعالجة الألية للمعطيات، والذي أدرج من خلاله العديد من الأفعال التي تعتبر جرائم إلكترونية، في محاولة لإدماج البعد التقني ضمن التجريم. ويفهم من ذلك اتجاه المشرع نحو توسيع نطاق التجريم ليشمل السلوكيات التي تضر بالأنظمة المعلوماتية.

وفي ذات السياق، عزز المشرع الجزائري ظروفاً مشددة للعقوبة، عندما تكون الأفعال المذكورة في هذا القسم موجهة ضد الدفاع الوطني والهيئات الخاضعة للقانون العام[2]، وهو ما يدل على اهتمامه بحماية المصالح الأساسية للدولة من هذه الأفعال. ومن شأن هذا التشديد أن يشمل بعض الأفعال التي تتجاوز مجرد الاعتداء على الأنظمة المعلوماتية لتطال مصالح الدولة، وهو ما يسمح بإدراج جريمة التجسس السيبراني ضمن هذه النصوص، لكن ما يعاب على هذه المواد أنها تنطوي فقط على الأفعال التي تمس بالأنظمة المعلوماتية، مما قد يؤدي إلى عدم شمول بعض صور التجسس السيبراني التي ترتكب بطرق لا تستلزم المساس بالأنظمة المعلوماتية، وإنما تستهدف الحصول على المعلومات بطرق أخرى، مثل استعمال الدرون[3].

حتى التعديلات اللاحقة لــق ع التي أضافها المشرع لم تمس مضمون الأفعال المجرمة، بل انصبت على تشديد الجزاءات، وهو ما يعكس استمرار النقص على مستوى التأطير التشريعي، مما دفع المشرع لإصدار قانون خاص ينظم هذا المجال.

ثانيا: قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيا الأعلام والاتصال ومكافحتها

جاء هذا النص لسد النقص، باعتباره أول إطار قانوني خاص يجرم مختلف الجرائم المعلوماتية، حيث وسع من الأفعال التي يمكن أن تدرج ضمن هذا المجال، فجرم هذا القانون

---

[1]- قانون رقم 04-15 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر العدد 71.

[2]- المادة 394 مكرر 3 من قانون 04-15 المتضمن تعديل قانون العقوبات، السالف الذكر.

[3]- سامية بوشوشة، حياة سلماني، التجسس الإلكتروني وطرق مكافحته، **مجلة العلوم الاجتماعية والإنسانية**، المجلد 16، العدد 01، جامعة تبسة، جوان 2023، ص64.

كل فعل يمس بالأنظمة المعلوماتية المذكور في ق ع، بالإضافة إلى كل فعل يرتكب أو يسهل ارتكابه باللجوء إلى هذه الأنظمة أو أي وسيلة أخرى[1].

في السابق كان المشرع يجرم أفعال التجسس السيبراني التي تندرج فقط في نطاق المساس بالأنظمة، أما مع هذا التعديل وسع من التجريم ليحيط بكل أفعال التجسس السيبراني التي ترتكب أو يسهل القيام بها بواسطة منظومة معلوماتية. فأصبحت تعد كل جريمة وقعت على نظام معلوماتي أو استعملت فيها أي وسيلة تندرج ضمن جرائم تكنولوجيا الإعلام والاتصال[2].

ومع هذا، يبقى غياب تنظيم صريح ومستقل لجريمة التجسس السيبراني قائماً، ما يطرح إشكالات عديدة من ضمنها تحديد عناصرها بدقة إلى غير ذلك، ما يستدعي تدخلاً تشريعياً يراعي خصوصية هذه الجريمة ويضبط نطاقها بشكل أوضح.

الفرع الثاني: الاتفاقيات الدولية ذات الصلة

يطرح التجسس السيبراني فراغ قانوني ناتج عن عدم التوازن بين خطورته العملية وغياب تأطير دولي صريح له، حيث لا توجد لحد اليوم اتفاقية دولية تفرده بالتجريم بشكل مستقل، رغم مخاطره الوخيمة على الأمن القومي والتي تتجاوز الحدود الوطنية للدول، بما قد يؤدي إلى زعزعة العلاقات الدولية، وعلى هذا الأساس يتم استنباط الإطار القانوني المنظم له بشكل غير مباشر من خلال مجموعة من الاتفاقيات التي تعالج الأفعال التي قد تتقاطع معه في المجال السيبراني.

في هذا الصدد، يتناول هذا الفرع الإطار القانوني لجريمة التجسس السيبراني، من خلال عرض أهم الاتفاقيات الولية ذات الصلة.

أولا: الاتفاقية المتعلقة بالجريمة الإلكترونية

هي أول إطار دولي شامل وضعه مجلس أوروبا سنة 2001 لمكافحة الجرائم المرتكبة عبر الأنظمة المعلوماتية، دخلت حيز التنفيذ سنة 2004، وتهدف إلى توحيد قواعد التجريم وتعزيز

---

[1]– المادة 2 من قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 47، الصادرة في 25 شعبان عام 1430 الموافق لـــ 16 غشت سنة 2009.

[2]– حابت أمال، الجريمة المعلوماتية في التشريع الجزائري: بين قانوني 04-15، و09-04، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، المجلد 7، العدد 25، مؤسسة هيرودوت للبحث العلمي والتكوين، 2023، ص59.

التعاون الدولي، ورغم عدم تطرقها للتجسس السيبراني بشكل مباشر، إلا أنها عالجت العديد من السلوكيات التي تشكل وسائل تقنية لارتكابه، مثل الدخول غير المشروع واعتراض البيانات، وهو ما سمح بتوفير إطار قانوني لتجريم هذه الأفعال[1].

جرمت هذه الاتفاقية مجموعة من الجرائم المعلوماتية، بما في ذلك صور المشاركة الجنائية مثل التحريض والمساعدة، كما ألزمت الدول الأطراف من خلال المادة 13 بتجريم كل الأفعال التي نصت عليها ضمن تشريعاتها الوطنية، فتركت السلطة التقديرية لتقدير العقوبات والتدابير لكل دولة وفق نظامها الداخلي[2].

ويلاحظ أن الجزائر من الدول التي لم تنضم لهذه الاتفاقية، بالرغم من أهميتها المرجعية في هذا المجال.

ثانيا: اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية 2024

تم اعتماد هذه الاتفاقية تحت إشراف الجمعية العامة للأمم المتحدة في تاريخ 24 ديسمبر 2024، بموجب القرار رقم 79/243، بهدف التعاون الدولي وتوحيد الجهود في مواجهة الجرائم السيبرانية. تم اعتماد على الاتفاقية كإطار ملزم للدول الأطراف، وفتح باب التوقيع عليها ابتداءً من 25 أكتوبر 2025[3].

اتخذت هذه الاتفاقية شأنها شأن الاتفاقيات الأخرى، على عدم التنصيص على التجسس السيبراني بشكل مباشر، ومقاربته مع بعض الأفعال، في الفصل الثاني المعنون بالتجريم، مما قد يجعلها مرجع يلجأ إليه في هذه الحالة، وأقرت هذه الاتفاقية إلزامية الدول الأطراف بتجريم الأفعال التي نص عليها هذا الفصل في تشريعاتها الداخلية[4].

ثالثا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

---

[1]– سامية بوشوشة، المرجع السابق، ص 63.

[2]– المادة 13 من اتفاقية بودابست المتعلقة بالجرائم الإلكترونية، الموقعة في بودابست من طرف مجلس أوروبا في 23 نوفمبر 2001، دخلت حيز التنفيذ في 1 يوليو 2004.

[3]– أبرز بنود اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية، 2025، مقال منشور على الموقع، https://www.aljazeera.net/، تاريخ الاطلاع 2026/03/29، على الساعة 17:13.

[4]– المواد من 7 إلى 11 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، تم تبنيها في 24 ديسمبر 2024، الموقعة في هانوي والمعتمدة من طرف الجمعية العامة للأمم المتحدة، موقعة في 25 أكتوبر 2025.

تندرج الاتفاقية ضمن المساعي الإقليمية الرامية لمواجهة التهديدات المتزايدة المتعلقة بالفضاء السيبراني، تم اعتمادها سنة 2010 من طرف جامعة الدول العربية، بهدف توحيد السياسات التشريعية العربية في هذا المجال. تعكس هذه الاتفاقية التعامل مع الظواهر الإجرامية المعلوماتية؛ إذ ركزت على تجريم الأفعال التقنية المختلفة، دون الارتقاء إلى معالجة الظواهر الإجرامية المعقدة بشكل مباشر مثل التجسس السيبراني.

صادقت الجزائر عليها من خلال المرسوم الرئاسي رقم 14-252. ألزمت هذه الاتفاقية مثل غيرها، الدول الأطراف في إضفاء الطابع التجريمي للأفعال التقنية ضمن تشريعاتها الداخلية، ومن بين الأفعال التي يمكن إسقاطها عل التجسس السيبراني في هذه الاتفاقية هو الدخول والاعتراض غير المشروع للأنظمة المعلوماتية التي نصت عليهم المواد 6 و7[1].

رابعا: دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية

هو ليس اتفاقية دولية، بل دليل أنشأه خبراء القانون الدولي من حلف الشمال الأطلسي، وهو مجرد مرجع تفسيري فقهي وليس ملزم، أنشأ بسبب الهجمات السيبرانية التي ازداد عددها في الآونة الأخيرة، هناك نسختين منه ما صدر في 2013 وما صدر في 2017، وبما أن هذه الوثيقة ليست رسمية فهناك دول رفضت العمل به مثل روسيا بسبب حجيته الغير إلزامية[2].

تضمن هذا الدليل جملة من المبادئ، لاسيما مبدأ سيادة الدولة على بنيتها الرقمية، ومسؤولية الدول عن الهجمات السيبرانية. غير أن الأهمية القانونية لهذا الدليل تبرز أساساً في تعامله مع جريمة التجسس السيبراني، إذ أشار في المادة 66[3] منه، على أن هذا الفعل لا يعد خرقًا لقواعد القانون الدولي في حالة النزاعات المسلحة.

---

[1]- المواد 6 و7 من المرسوم الرئاسي رقم 14-252 مؤرخ في ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، ج ر 57، الصادر في 4 ذو الحجة عام 1435، الموافق لـــ 28 سبتمبر سنة 2014.

[2]- محمد الأبيض، دليل تالين والقواعد المطبقة على الهجمات السيبرانية، **مجلة العلوم القانونية والاجتماعية**، المجلد العاشر، العدد الرابع، جامعة زيان عاشور –الجلفة–، ديسمبر 2025، ص796-797.

[3]- المادة 66 من دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية، أُعد من قبل مجموعة من الخبراء الدوليين بدعوة من قبل (THE NATO cooperative cyber defence center of excellence)، المحرر من طرف MICHEAL N. SCHMITT، ترجمة على محمد كاظم الموسوي، في كتابه الموسوم بـــ(المشاركة المباشرة في الهجمات السيبرانية)، المطبوع في شركة المؤسسة الحديثة للكتاب عام 2019.

غير أن هذا التوجه يطرح إشكال قانوني عميق، يتمثل في أن التجسس السيبراني يعد من الناحية العملية فعلاً بالغ الخطورة على استقرار الدول، وكان من المفترض أن يخضع لتأطير قانوني واضح على المستوى الدولي، غير أن الواقع يظهر غياب هذا النص، وهو ما يؤدي إلى فراغ تشريعي على مستوى الركن الشرعي لهذه الجريمة.

ومن ثم، فإن هذا الدليل، بدل أن يؤكد على تجريم هذا الفعل جعله مشروعاً في نطاق معين، وهذا ما يبرز التناقض بين خطورة هذا الفعل وغياب تجريمه في قواعد القانون الدولي.

المطلب الثاني

الركن المادي لجريمة التجسس السيبراني

يمثل الركن المادي الدعامة الواقعية والمظهر الخارجي الملموس الذي تخرج من خلاله الجريمة من حيز النوايا الباطنية إلى حيز الوجود الفعلي، إذ لا يعاقب القانون على مجرد الأفكار ما لم تقترن بسلوك مادي يمس بالمصالح التي يحميها. وإذا كان هذا الركن يتخذ في الجرائم التقليدية طابع مادي ذو أفعال ملموسة، فإنه في البيئة الرقمية يكتسي طبيعة خاصة تتلاءم معها؛ حيث يبرز في جريمة التجسس السيبراني عبر منظومة من الأفعال الإلكترونية غير المشروعة التي يستهدف بها الجاسوس اختراق الأنظمة المعلوماتية وتجاوز تدابير حمايتها للحصول على ما يريد.

يتشكل هذا الركن من عناصر مادية متكاملة، تنطلق بالسلوك الموجه نحو النظام المعلوماتي، لتفضي إلى نتيجة الوصول إلى المعلومات واستغلالها.

ومن ثم، فإن تحديد مضمونه يقتضي الوقوف على السلوك الإجرامي في **(الفرع الأول)**، وتبيان النتيجة المترتبة والعلاقة التي تربط بينهما في **(الفرع الثاني)**.

الفرع الأول: السلوك الإجرامي

يقتضي تكييف التجسس السيبراني كجريمة، أن تتجه إرادة الجاسوس إلى إتيان نشاط خارجي، يتم داخل البيئة الرقمية، بغرض تحقيق نتيجة معينة، ويعد هذا النشاط هو السلوك الإجرامي في هذه الجريمة، حيث يتخذ عدة صور يمكن حصر أهمها فيما يلي:

أولا: فعل التخابر

فعل التخابر هو الركيزة الأساسية والمنطلق الأول لجريمة التجسس، ويتجلى هذا السلوك في صورة تواطؤ الجاسوس مع جهات أجنبية بهدف تنسيق أعمال عدائية تستهدف السيادة الوطنية[1]، وذلك عبر ربط قنوات اتصال بشتى الطرق الممكنة، فهو سلوك إيجابي يقدم من خلاله الجاني معلومات محفزة للعدو، فيجسد هذا الفعل التعاون غير القانوني الذي يتيح نقل أو تبادل المعلومات ذات الطابع الحساس[2].

يمكن أن يسبق هذا الفعل عملية التجسس من حيث كونه وسيلة للحصول على الدعم أو التوجيه، ويمتد إلى حين تزويد الجهة الأجنبية بالمعطيات المطلوبة، بما يجعله يرتبط بمراحل التجسس قبل التنفيذ وأثناء القيام به وحتى الانتهاء منه.

ثانيا: فعل الدخول أو البقاء غير المصرح به

يفترض لتنفيذ عملية التجسس التسلل إلى البيئة المعلوماتية المستهدفة، وهو ما يتحقق عبر صورتين، وهما الدخول أو البقاء غير المصرح بهما.

1. فعل الدخول:

يعد هذا الفعل من أبرز صور الاعتداء على الشبكات المعلوماتية، وقد أولاه المشرع الجزائري أهمية خاصة، بالنظر لكونه يشكل المدخل التقني الأول للولوج لأي نظام. جرمته المادة 394 مكرر من ق ع، والتي تقضي بمعاقبة كل من يدخل دون وجه حق إلى نظام معلوماتي، بعقوبات سالبة للحرية وغرامات مالية، دون اشتراط تحقق نتيجة ضارة لاحقة لهذا

[1]– المادة 62 من الأمر 66–156 المتضمن قانون العقوبات السالف الذكر.

[2]– اوشن حنان، وادي عماد الدين، التجسس الإلكتروني وآليات مكافحته في التشريع الجنائي الجزائري، مجلة الحقوق والعلوم السياسية، المجلد 01، العدد 02، جامعة عباس لغرور –خنشلة–، جويلية 2014، ص136.

الفعل[1]. ويتميز هذا الفعل بكونه جريمة قائمة بذاتها، فتقوم بمجرد الدخول بصرف النظر عن النتائج المترتبة عنها[2]. كما لم يحدد المشرع وسيلة معينة للولوج، الأمر الذي يجعل صور تنفيذه متعددة، ومن الناحية العملية، يمكن أن يتم الدخول بطريقتين:

أ) الدخول المباشر: ويقصد به الولوج إلى النظام في شكل مباشر أمام الجهاز المستهدف، من خلال إدخال كلمات مرور أو رموز أو استعمال وسائط مادية أو برمجيات[3]، فيمكن للجاسوس التواجد أمام الجهاز المطلوب وإدخال أي وسيلة تساعده في كسر جدار الحماية.

ب) الدخول عن بعد: ويقصد به ارتكاب الجريمة من مكان أخر، باستعمال أي وسيلة إلكترونية من شأنها المساعدة في الدخول، مثل إرسال برامج تجسسية أو حصان طروادة الذي يخدع المستخدم لإحالته لمساعدة الجاسوس بالدخول[4].

وتجدر الإشارة أن المشرع لم يشترط تحقق ضرر فعلي لقيام هذه الجريمة، إذ يكفي مجرد الدخول غير المشروع. كما تقوم المسؤولية الجنائية متى ثبتت إرادة الجاني، أما حالة الخطأ فهي حالة نادرة في المجال السيبراني، بالنظر إلى طبيعة المعلومات شديدة الحماية، وهو ما يستوجب في حال حدوث خطأ الخروج الفوري وإلا قامت المسؤولية الجنائية[5].

---

[1]– المادة 394 مكرر من القانون 24–06، مؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، يعدل ويتمم الأمر 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر العدد 30، الصادر بـــ 21 شوال عام 1445 الموافق لـــ 30 أبريل سنة 2024.

[2]– حمزة بن عقون، المرجع السابق، ص 183.

[3]–عزالدين عثماني، صور الركن المادي في الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 03، جامعة الشهيد حمه لخضر –الوادي–، ديسمبر 2028، ص ص612–625، ص 616.

[4]– قسمية محمد، خضري حمزة، مكافحة الجرائم الماسة بنظام المعالجة الألية للمعلومات في قانون العقوبات، مجلة صوت القانون، المجلد السابع، العدد 2، جامعة خميس مليانة، نوفمبر 2020، ص ص126–150، ص ص131–132.

[5]– المرجع نفسه، ص 134.

2. فعل البقاء

يقصد بالبقاء استمرار الشخص بالتواجد دون وجه حق في النظام، والامتناع عن الخروج رغم علمه بانعدام السند القانوني الذي يجيز له البقاء. وتقوم هذه الصورة متى تحقق عنصر الاستمرار الإرادي داخل النظام خلافًا لإرادة صاحب الحق[1].

ولم يربط المشرع الجزائري هذه الجريمة بجريمة الدخول، فيمكن أن يكون الدخول عن غير قصد أو بصفة مشروعة مثل العامل الذي يحق له أن يدخل إلى النظام لكن لوقت وجيز ثم يخرج منه إلا أنه يقرر البقاء، كما يمكن أن يتصل البقاء بالولوج في حالة ما إذا كان لشخص نية الدخول والبقاء من الأول[2].

وتعد جريمة الدخول من الجرائم الوقتية التي تكتمل بمجرد تحققها، في حين يأخذ فعل البقاء طابع الجريمة المستمرة التي تمتد أثارها طوال فترة التواجد داخل النظام، وتنتهي بخروج الشخص أو إنهاء تواجده بأي وسيلة كانت[3].

ثالثا: التلاعب العمدي بالمعطيات

التلاعب العمدي بالمعطيات هو النتيجة المترتبة عن الأفعال المذكورة سابقا، جرمها المشرع في المادة 394 مكرر1[4]، وتتحقق هذه الأفعال حتى وإن كان الدخول في أصله مشروعا، كأن يستغل موظف صلاحياته في الدخول إلى نظام مؤسسته، ثم يقوم بأفعال تتجاوز حدود الغرض من دخوله، مما يحول سلوكه من فعل مشروع إلى نشاط إجرامي متمثل في الصور الأتية:

1. فعل الإدخال: هو إدراج شيء جديد للدعامة المعلوماتية، ويكون إما قبل الدخول أو بعده.

أ) قبل الدخول: هو فعل سابق لفعل الدخول، فيقوم الجاني بإدراج برامج خبيثة في النظام أو في الحاسوب تمكنه من الدخول كفك الشفرات وذلك لتسهيل عملية الدخول.

---

[1]– آية بن ميسية، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة ضمن متطلبات نيل شهادة الماستر، تخصص قانون جنائي، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف–ميلة–، 2025/2024، ص 22.

[2]– نعمان عبد الكريم، الدخول أو البقاء عن طريق الغش في نظام المعالجة الألية للمعطيات، مجلة حوليات جامعة الجزائر 1، المجلد 38، العدد 02، جامعة الجزائر 1، 2024، ص ص36–56، ص 43.

[3]– نعمان عبد الكريم، المرجع السابق، ص 44.

[4]– المادة 394 مكرر1 من القانون 24–06 المتضمن تعديل قانون العقوبات، السالف الذكر.

ب) بعد الدخول: وهو إضافة معطيات وبيانات جديدة للنظام، تهدف إلى التشويش على عمل الجهاز، أو توجيه النظام لتحقيق نتائج معينة، أو حتى إدراج حسابات لمستخدمين أخرين لتمكينهم من الولوج فيما بعد[1].

2. فعل الإزالة: هو المحو الكلي أو الجزئي للمعطيات المخزنة في الدعامة داخل وسائط التخزين، ولا يقتصر الأمر على الحذف النهائي بل يشمل أيضاً نقل المعطيات من مكانها الأصلي، أو إزاحتها بقصد إخفائها، أو جعل الوصول إليها أمرا مستحيلاً[2].

3. فعل التعديل: هو تغيير ماهية المعطيات واستبدالها ببيانات مغايرة للحقيقة دون علم أو موافقة الجهات المتحكمة في النظام. يتم ذلك باستخدام الفيروسات أو البرامج التخريبية، ويهدف الجاني من خلاله إلى تزييف الحقائق الرقمية لتحقيق غاياته الإجرامية[3].

رابعا: التعامل في معطيات غير المشروعة

يقصد بالتعامل في المعطيات غير المشروعة كافة السلوكيات الرقمية والأنشطة الإجرامية التي استهدفتها المادة 394 مكرر2[4]. ولا يقتصر هذا التجريم على المساس بالبيانات فحسب، بل يمتد ليشمل كافة الوسائط والأدوات التي تسهل الاعتداء على الأنظمة، ويمكن تقسيم هذه الأفعال كما يلي:

1. التعامل في معطيات صالحة لارتكاب الجريمة

تشمل هذه الفئة الأنشطة التحضيرية والوسائل التقنية التي تسبق عملية الولوج أو الاعتداء الفعلي، أو حتى تتم أثناء سير عملية التجسس، حيث تتعلق أساساً بتهيئة الوسائل التقنية اللازمة لتنفيذ الفعل الإجرامي، ابتداءً من إعدادها وصولًا إلى نشرها وإتاحتها للغير. وتتجلى صور هذا التعامل فيما يلي:

---

[1]– جدي نسيمة، جرائم المساس بأنظمة المعالجة الألية للمعطيات، مذكرة لنيل شهادة الماجيستر في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014/2013، ص65.

[2]– بودواب سمير، لبديوي فؤاد، جرائم المساس بأنظمة المعالجة الألية للمعطيات، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 –سكيكدة–، 2024، ص27.

[3]– عياشي عاشور، يعيش عبد الحق، آليات مكافحة جريمة التجسس السيبراني في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي في الحقوق، تخصص قانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي–برج بوعريريج–، 2024/2023، ص 19.

[4]– المادة 394 مكرر 2 من القانون 24–06 المتضمن تعديل قانون العقوبات السالف الذكر.

أ) التصميم: يتمثل في إنشاء أو تطوير أدوات وبرمجيات تستخدم في تنفيذ جريمة التجسس السيبراني، كإعداد البرامج الخبيثة التي تمكن من الولوج إلى الأماكن المحظورة، أو تعطيلها أو التحكم فيها[1].

ب) البحث: ينصرف إلى القيام بعمليات استقصاء تقنية، سواء داخل الشبكات بهدف اكتشاف الثغرات الأمنية أو الوصول إلى البيانات، أو التعرف على الأساليب التي تسهل القيام بالعملية ككل.

ت) التجميع: يتحقق عند قيام الجاني بتجميع الوسائل والمعطيات التي تسهل عليه ارتكاب الجريمة، وتنظيمها في شكل قابل للاستغلال، سواء بغرض نقلها أو تخزينها أو استعمالها [2].

2. التعامل في معطيات متحصلة من الجريمة

يتعلق هذا النوع من الأفعال بالمرحلة اللاحقة لارتكاب الجريمة، حيث يتم التصرف في المعطيات بما يحقق الغاية النهائية من الفعل الإجرامي، ويتخذ هذا التعامل عدة صور، من بينها

أ. الحيازة: تتمثل في بسط السيطرة الفعلية على المعطيات والاحتفاظ بها، بما يتيح للجاني إمكانية التصرف فيها.

ب. الإفشاء: هو كشف المعطيات أو نقلها للغير دون وجه حق، بما يؤدي إلى اطلاع أشخاص غير مخولين عليها، وهو ما يشكل مساساً بسرية المعلومات[3].

ت. الاستعمال: يتجسد في توظيف المعطيات المتحصل، كاستغلالها من قبل جهات أجنبية أو مؤسسات منافسة، بما يحقق لها منفعة على حساب الجهة المتضررة[4]. مثل تجسس شركة على شركة أخرى لتكتشف أسرار صناعة منتج ما، وأخذ تلك الأسرار وتطبيقها في صناعة المنتج.

---

[1]– بوذراع عبد العزيز، خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجيستر في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، 2012/2011، ص68.

[2]– بن بادة عبد الحليم، بوحادة محمد سعد، (جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة) –دراسة سياسية قانونية–، الملتقى الدولي الأول الموسوم بـــ: أمن المعلومات في الفضاء الإلكتروني: الرهانات والتحديات في شمال إفريقيا، المنعقد يومي: 17و18 فيفري 2020، كلية الحقوق والعلوم السياسية، –جامعة غرداية–، ص19.

[3]– بوذراع عبد العزيز، المرجع السابق، ص 69.

[4]– قسمية محمد، خضري حمزة، المرجع السابق، ص 141.

وقد جرم المشرع الجزائري هذه الأفعال أيضا في المادة 63 من ق ع التي تنص على معاقبة كل من يقوم بالاستحواذ على كل ما يتعلق بسرية الدولة، أو تسليمه للغير دون وجه حق[1].

الفرع الثاني: النتيجة والعلاقة السببية

يعد تحقق الأثر المترتب عن السلوك الإجرامي، إلى جانب قيام الرابطة القانونية التي تصل هذا السلوك بنتيجته، من المقومات الجوهرية لقيام الركن المادي للجريمة؛ إذ لا يكفي مجرد صدور فعل من الجاني، بل يجب أن يفضي هذا الفعل إلى نتيجة يعتد بها قانوناً، وأن تثبت الصلة بينهما.

وعلى هذا الأساس، تبرز أهمية تحديد طبيعة النتيجة المتحققة في جريمة التجسس السيبراني، وكذا تبيان مدى توافر العلاقة السببية بين الفعل المرتكب والضرر الناتج عنه، بما يسمح بإسناد المسؤولية الجزائية للجاني.

أولا: النتيجة الإجرامية

تتمثل النتيجة الإجرامية في جرائم التجسس السيبراني في الاعتداء على أمن النظام المعلوماتي وسرية المعطيات محل الحماية، باعتبارها المصلحة الجوهرية التي يسعى المشرع إلى صونها. وتتحقق هذه النتيجة بمجرد وقوع أي مساس بهذه المصالح، سواء تمثل ذلك في تعريض النظام أو المعطيات للخطر، أو كشفها فعلياً وإتاحتها لجهات غير مخولة قانوناً، بما يؤدي إلى الإخلال بطابعها السري وانعدام الحماية المقررة لها[2].

ولا يشترط لقيام هذه النتيجة تحقق ضرر مادي ملموس أو استعمال فعلي للمعطيات من قبل الغير، بل يكفي أن يثبت أن سلوك الجاني قد أدى إلى المساس بأمن النظام المعلوماتي أو سرية المعطيات، بوضعها في حالة تسمح بالاطلاع عليها أو الوصول إليها دون وجه حق، وهو ما يعد في حد ذاته اعتداءً قائماً من الناحية القانونية[3].

---

[1]– المادة 63 من أمر رقم 66–156 المتضمن قانون العقوبات، السالف الذكر.

[2]– بوشعبة محمد، المرجع السابق، ص 30.

[3]– محمد بدوسي، المرجع السابق، ص 17.

ثانيا: العلاقة السببية

لا يكفي لقيام الركن المادي في جريمة التجسس السيبراني مجرد تحقق سلوك إجرامي ونتيجة ضارة، بل يتعين أن تقوم بينهما علاقة سببية تسند بموجبها النتيجة إلى الفعل. وتتحقق هذه الرابطة متى ثبت أن النتيجة لم تكن لتقع لولا الفعل، وأن هذا الأخير كان سبباً كافياً في إحداثها.

ففي حالة اعتراض البيانات مثلاً، لا يعتد بقيام المسؤولية الجنائية إلا إذا كان كشف المعطيات أو المساس بسريتها نتيجة طبيعية ومترتبة عن هذا الفعل، لا عن عوامل أجنبية مستقلة. أما إذا تدخل سبب أجنبي كافٍ لقطع هذه الرابطة، فهنا تنقطع وتنتفي المسؤولية[1].

المطلب الثالث

الركن المعنوي لجريمة التجسس السيبراني

تصنف جريمة التجسس السيبراني ضمن طائفة الجرائم العمدية التي تفترض توافر إرادة واعية لدى الجاني، نظراً للوسائل المستخدمة في الجريمة المعقدة والمدروسة بعناية. ومن ثم يستبعد فيها قيام الخطأ، إذ لا يمكن تصور وقوع جريمة التجسس نتيجة إهمال، بل تقوم على نشاط ذهني منظم يسبق التنفيذ الفعلي ويواكبه.

ولا يقتصر الركن المعنوي في هذا الإطار على مجرد الإدراك بطبيعة السلوك الإجرامي، وإنما يمتد ليشمل نية خاصة تتجسد في استهداف مصالح الدولة أو العمل لصالح جهة أجنبية. وعليه، يقتضي تحليل الركن المعنوي في جريمة التجسس السيبراني الوقوف على عناصر القصد الجنائي العام من حيث العلم والإرادة في **(الفرع الأول)**، ثم بيان القصد الجنائي الخاص باعتباره نية الجاني لتحقيق غرض معين في **(الفرع الثاني)**.

الفرع الأول: القصد الجنائي العام

[1]– مقرح عبد الرؤوف، التجسس السيبراني الماس بأمن الدولة في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق، تخصص قانون الإعلام الآلي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي–برج بوعريريج–، 2024/2023، ص 24.

تفرض جرائم التجسس دراسة البعد النفسي لسلوك الجاني، لأن خطورتها لا تنحصر في الفعل المادي وحده، بل تمتد إلى إرادة واعية تتجه نحو الإضرار بمصالح الدولة المحمية قانوناً. ويجسد هذا في القصد الجنائي العام، الذي يربط بين السلوك الإجرامي والنية الداخلية للجاني، ويستدل من خلاله على قيام المسؤولية الجزائية.

يتأسس هذا القصد على عنصرين مترابطين هما العلم والإرادة؛ فلا يكفي تحقق الفعل ما لم يكن الجاني مدركاً لوقائعه وظروفه التي يجرمها القانون، ومتجهاً بإرادته إلى تحقيقه. ومن خلال هذا الترابط يتحدد البناء النفسي للجريمة من خلال ما يلي:

أولا: العلم

هو إدراك الجاني إدراك يقيني بطبيعة فعله غير المشروع، بحيث يكون واعيًا بأنه بصدد المساس بنظام معلوماتي محمي قانونًا، وأن محل الاعتداء لا يقتصر على مجرد بيانات عادية، بل قد يشمل معطيات ذات طابع حساس أو استراتيجي يترتب على كشفها ضرر فعلي[1].

ولا يقتصر هذا العلم على معرفة الفعل في حد ذاته، بل يمتد ليشمل الإحاطة الكاملة بعناصره التقنية، كمعرفة الوسيلة المستخدمة مع علمه بعدم مشروعيتها في ظل التنظيم القانوني والضوابط التقنية المعمول بها. كما يتطلب هذا العنصر أن يكون الجاني مدركًا للنتائج المحتملة المترتبة عن سلوكه، كإفشاء البيانات، أو استغلالها من طرف الغير[2].

ثانيا: الإرادة

يقصد بالإرادة هنا اتجاه نية الجاني بحرية واختيار نحو ارتكاب الفعل الإجرامي، أي أنه لا يكتفي بمجرد العلم بطبيعة السلوك غير المشروع، بل يتجاوز ذلك إلى اتخاذ قرار بتنفيذه.

وتعبر الإرادة هنا عن عنصر السيطرة النفسية على السلوك، بحيث يكون الفعل ناتجًا عن اختيار شخصي مستقل، لا عن إكراه مادي أو معنوي أو خطأ غير مقصود. فالجاني يباشر سلوكه الإجرامي عن قصد وتوجيه مسبق نحو تحقيق النتيجة. وعليه، فإن اجتماع عنصري

---

[1]– علاء الدين محمد عفيف نابلسي، السياسة الجنائية في مواجهة جرائم التجسس "دراسة مقارنة"، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة الماجيستر في القانون الجنائي، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس فلسطين، 2020، ص42.

[2]– المرجع نفسه، ص42.

العلم والإرادة يكوّنان القصد الجنائي العام، الذي يعد الأساس لقيام المسؤولية الجنائية في جريمة التجسس السيبراني[1].

الفرع الثاني: القصد الجنائي الخاص

يتميز الركن المعنوي في جريمة التجسس السيبراني بخصوصية واضحة، إذ لا يقتصر على توافر القصد الجنائي العام المتمثل في العلم والإرادة، بل يتطلب توافر قصد جنائي خاص يتمثل في اتجاه إرادة الجاني نحو تحقيق غاية محددة تمس بمصالح الدولة. وعليه فإن السلوك الإجرامي في جريمة التجسس السيبراني ليس مجرد فعل إرادي، بل هو نشاط موجه نحو هدف معين يكشف عن خطورة النية الإجرامية.

ولهذا، يقتضي الأمر بيان صور القصد الجنائي الخاص على النحو الآتي:

أولا: نية الأضرار بمصالح الدول

تتحقق هذه الصورة من القصد الجنائي الخاص عندما تتجه إرادة الجاني إلى المساس بالمصالح الجوهرية للدولة، وعلى رأسها أمنها القومي وسلامتها، واستقرار مؤسساتها، فالجاني لا يكتفي بمجرد المساس بالنظام، بل يسعى من خلال فعله إلى إحداث ضرر فعلي أو محتمل، كنية إضعاف القدرات الدفاعية للدولة، أو زعزعة أمنها الداخلي. ولا يشترط لتحقق المسؤولية الجنائية أن يقع الضرر فعلاً، بل يكفي ثبوت اتجاه إرادة الجاني نحو تحقيقه، لأن العبرة في الجرائم العمدية تكون بالقصد لا بالنتيجة الإجرامية[2].

ثانيا: نية الحصول على معلومات سرية

يقوم هذا القصد عندما ينصرف سلوك الجاني نحو استهداف معلومات بسبب طبيعتها السرية، بحيث لا يكون محل الاعتداء بيانات عادية، وإنما معطيات تكتسي أهمية بالغة للدولة. فمحور هذا القصد لا يتعلق بالفعل في حد ذاته، بل بالمحل الذي ينصب عليه، وهو المعلومات[3].

---

[1]– المرجع نفسه، ص 42.

[2]– محمد الفاضل، المرجع السابق، ص 360.

[3]– منيرة صديقي، خديجة سعيدات، تجريم الأفعال الماسة بأمن الدولة والوحدة الوطنية، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر أكاديمي في الحقوق، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة –غرداية–، 2022/2021، ص88.

ومن ثم، فإن الطابع التجسسي للفعل يظهر من خلال نوعية المعلومات المستهدفة، حيث تكشف طبيعتها عن الغاية الحقيقية للجاني، كما قد يتخذ هذا الفعل صور متعددة، مثل السعي للاحتفاظ بهذه المعلومات أو استغلالها أو إعطاؤها إلى جهات أخرى، وهو ما يعكس اتجاه واضح نحو توظيفها خارج إطارها المشروع[1].

[1]– محمد الفاضل، المرجع السابق، ص 361.

الفصل الثاني

استراتيجية مكافحة التجسس السيبراني في الإطار الدولي والتشريع الجزائري

تستدعي الخطورة المتزايدة لجريمة التجسس السيبراني وما تخلفه من انعكاسات على أمن الدول وسيادتها، الوقوف على الجهود المبذولة لمكافحتها والتصدي لها. فالتسارع الرهيب الذي تشهده تكنولوجيا المعلومات اليوم، والاعتماد شبه الكلي على الفضاء الرقمي، جعل من هذه الجريمة هاجس أمني يهدد المصالح الحيوية والسيادية للدول، الأمر الذي عجل بضرورة بناء آليات قانونية ومؤسساتية قادرة على مواكبة هذه التحديات والتصدي لها.

ولم تعد مواجهة التجسس السيبراني مسؤولية دولة واحدة فحسب، بل أصبحت تتطلب تعاون دولي واسعاً نظراً للطابع العابر للحدود الذي تتسم به هذه الجريمة، حيث يمكن أن ترتكب من إقليم دولة وتستهدف أنظمة معلوماتية موجودة في دولة أخرى، وهو ما يصعب من إجراءات الكشف عن مرتكبيها وملاحقتهم. لذلك اتجه المجتمع الدولي إلى إرساء مجموعة من الاتفاقيات والآليات الرامية إلى تعزيز التعاون وتوحيد الجهود في مجال مكافحة الجرائم السيبرانية بصفة عامة، والتجسس السيبراني بصفة خاصة.

وبالتوازي مع هذه الجهود الدولية، سعت الجزائر إلى مواكبة التطورات المتسارعة التي يشهدها المجال الرقمي من خلال تبني منظومة قانونية ومؤسساتية تهدف إلى حماية أنظمتها المعلوماتية وتعزيز أمنها السيبراني، وذلك عبر سنّ نصوص تشريعية متخصصة واستحداث هيئات وآليات مكلفة بالوقاية من التهديدات السيبرانية والتصدي لها.

وعليه، يقتضي تناول موضوع مكافحة التجسس السيبراني دراسة مختلف الجهود والآليات المعتمدة على المستويين الدولي والوطني، وهو ما تم تخصيص هذا الفصل من أجله، وذلك لبيان آليات مكافحة التجسس السيبراني في الإطار الدولي في (المبحث الأول)، ثم الوقوف على الجهود التي اعتمدها المشرع الجزائري للتصدي لهذه الجريمة ومواجهة مخاطرها في (المبحث الثاني).

المبحث الأول

استراتيجية مكافحة التجسس السيبراني في الإطار الدولي

تتجاوز مكافحة التجسس السيبراني حدود المقاربات الوطنية الفردية للدول، ليصبح قضية دولية تفرضها الطبيعة العابرة للحدود لهذه الجريمة، وقدرة اقترانها بالتقنيات المعقدة التي تسمح باستهداف المنشآت الحيوية وسرقة البيانات السيادية من أي مكان في العالم دون ترك أثر صريح للجناة.

وأمام هذا التهديد الشامل، تزايدت القناعة الدولية بعدم كفاية التدابير الداخلية الوطنية، مما استدعى إرساء استراتيجيات جماعية عبر اتفاقيات ومؤسسات دولية وإقليمية؛ ولم تقتصر هذه الجهود على صياغة أطر التعاون المشترك فحسب، بل امتدت لتلزم الدول الأطراف بضرورة تحديث تشريعاتها الوطنية وتكييفها لمجابهة هذه الاعتداءات كالتزام دولي أساسي.

وعليه وتماشياً مع هذا التوجه، خصص هذا المبحث لدراسة كيف يتم مكافحة التجسس السيبراني في الإطار الدولي عبر مطلبين؛ بحيث تناول **(المطلب الأول)** الأطر القانونية والمؤسساتية للاتفاقيات والمنظمات الدولية والإقليمية، في حين يعرض في **(المطلب الثاني)** آليات التعاون الدولي، مع بيان أحكام المسؤولية الدولية المترتبة عن التجسس الرقمي.

المطلب الأول

الجهود الدولية والإقليمية في مكافحة التجسس السيبراني

يمثل التشريع الدولي والإقليمي خط الدفاع القانوني الأول ضد قراصنة وجواسيس المعلومات، حيث تسعى القواعد والاتفاقيات الصادرة عن المنظمات إلى توحيد المفاهيم الإجرائية والموضوعية وتحديد التزامات الدول في مواجهة المخاطر السيبرانية الماسة بالبنية التحتية للدول، بهدف سد الثغرات القانونية وتعزيز التعاون الدولي لمنع الإفلات من العقاب.

ولإعطاء صورة متكاملة عن هذه الجهود، قسم هذا المطلب إلى فرعين؛ يتمثل **(الفرع الأول)** في دراسة الجهود الدولية والعالمية المتمثلة في منظمة الأمم المتحدة، ثم نعرج في **(الفرع الثاني)** على دراسة الجهود الإقليمية من خلال استعراض استراتيجية المجلس الأوروبي والاستراتيجية المعتمدة في إطار جامعة الدول العربية، لبيان كيفية التنسيق بين هذه المستويات المختلفة لمكافحة هذه الجرائم

الفرع الأول: جهود منظمة الأمم المتحدة لمكافحة التجسس السيبراني

تكتسي الجهود الصادرة عن المنظمات ذات الطابع العالمي أهمية بالغة بالنظر لشمولية أحكامها وقدرتها على صياغة معاهدات ملزمة لعدد واسع من الدول. وهذا ما ينطبق على مساعي منظمة الأمم المتحدة، التي سعت منذ سنوات طويلة على مكافحة الجرائم السيبرانية بشتى الطرق عبر عدة قرارات واتفاقيات.

أولا: المبادرات والقرارات الأممية لمواجهة التهديدات الرقمية

تندرج القرارات الدولية الصادرة في هذا السياق ضمن المساعي الرامية إلى تعزيز الأمن السيبراني ومكافحة الجريمة المعلوماتية بكافة أشكالها، بما فيها الهجمات الإلكترونية وأنشطة التجسس التي تهدد استقرار الدول وبنيتها التحتية الحيوية. وتتبلور هذه الجهود في:

1. **التوجه الوقائي المبكر وحماية الخصوصية:** تبنت الجمعية العامة للأمم المتحدة توصيات مؤتمر طهران الدولي الأول لحقوق الإنسان لعام 1968، والتي حذرت بشكل صريح من خطورة الحاسبات الإلكترونية وأجهزة المراقبة وأدوات التطفل الحديثة إذا ما استغلت في تخزين البيانات الشخصية وتحليلها، معتبرةً هذا السلوك تهديداً مباشر لحرمة الحياة الخاصة ومساس غير مشروع للبيانات[1].

2. **تطوير المنظومة التشريعية العالمية:** تأسيساً على هذا المنظور الوقائي، تبلورت الرؤية الأممية عبر قراري الجمعية العامة رقم (55/63) لعام 2000 ورقم (56/121) لعام 2001 بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات، واللذين شكلا منطلقاً لحث الدول الأعضاء على وضع تشريعات وطنية تتماشى مع خطورة الاعتداءات الرقمية. وبحلول عامي 2003 و2004، عززت المنظمة هذا التوجه بإصدار القرارين (57/239) و(58/199) بهدف إرساء ثقافة عالمية للأمن السيبراني هدفها حماية البنى التحتية المعلوماتية[2].

3. **تطوير القواعد الإجرائية والملاحقة القضائية:** لم يقتصر الدور الأممي على الجوانب الوقائية والتوعوية، بل امتد ليتناول الأبعاد الإجرائية والموضوعية لملاحقة الجرائم العابرة للحدود؛ إذ وضع مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين (هافانا 1990)

---

[1]– بقدار شيماء، آليات مكافحة الجريمة الإلكترونية على المستويين الدولي والوطني، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس –مستغانم–، 2023، ص 45.

[2]– بقدار شيماء، المرجع السابق، ص 45.

القواعد الأساسية لتطوير القوانين الإجرائية، داعياً إلى تمكين سلطات التحقيق والقضاء من صلاحيات مرنة ومناسبة لجمع الأدلة الرقمية والتعامل مع الطبيعة المعقدة للأنشطة المعلوماتية غير المشروعة. كما شدد المؤتمر على ضرورة تفعيل آليات المساعدة القضائية وتبادل المعلومات وتسهيل إجراءات تسليم المجرمين بين الدول الأطراف، وهي ذات الآليات القانونية التي تتقاطع مع متطلبات مكافحة التجسس السيبراني العابر للحدود[1].

4. **اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية 2024:** لمواكبة التطورات المتسارعة، اعتمدت الجمعية العامة للأمم المتحدة بموجب قرارها 79/243 الصادر في ديسمبر 2024 النص النهائي لأول معاهدة دولية ملزمة عالمياً لمكافحة الجرائم المعلوماتية. وتضع هذه الاتفاقية إطار قانوني موحد لتسهيل المساعدة القانونية المتبادلة العابرة للحدود وضبط الأدلة الرقمية المرتبطة بالولوج غير الشرعي للأنظمة والاعتراض غير المشروع للبيانات، وهي الممارسات التقنية الأساسية المعتمدة في التجسس السيبراني[2].

ثانيا: الالتزامات الدولية المفروضة على الدول الأعضاء لمكافحة التجسس السيبراني

لضمان مكافحة فعالة للجرائم الإلكترونية، أقرت اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية 2024 مجموعة من الالتزامات والإجراءات المحورية التي يتوجب على الدول القيام بها. كتجريم العديد من الأفعال التي تشكل الركن المادي للتجسس، وفرضت الالتزامات الآتية:

1. الالتزامات التشريعية (التجريم)

أ. تلزم الدول بتجريم أي جريمة منصوص عليها في اتفاقيات أخرى متى ارتكبت بواسطة تكنولوجيا المعلومات، مما يمتد ليشمل التجسس المرتبط بالإرهاب أو الجرائم الدولية.

ب. إلزام الدول بتجريم الجرائم الإلكترونية بما فيها التي تشكل فعل من أفعال التجسس السيبراني.

ت. تقرير مسؤولية الشركات والمؤسسات جنائياً أو مدنياً عن جرائم الاتفاقية، ويشمل شركات التجسس الخاصة وموردي برامج المراقبة.

ث. تجريم المساهمة والتحريض والشروع في ارتكاب أي جريمة من جرائم الاتفاقية.

---

[1]– بقدار شيماء، المرجع السابق، ص 46.

[2]– أبرز بنود اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية، المرجع السابق.

ج. إلزام الدول الأعضاء بتأسيس ولايتها القضائية على الجرائم المرتكبة في إقليمها أو من قبل مواطنيها أو ضدها، مما يتيح ملاحقة الجواسيس السيبرانيين حتى لو كانوا خارج البلاد.

ح. إلزام الدول بتبني فترات تقادم طويلة للجرائم السيبرانية، وذلك لعدم فرار الجناة[1].

لكن في هذا الصدد نجد أن المشرع الجزائري قد تبنى مقاربة أكثر صرامة وحماية لأمنه السيبراني والقومي؛ فحينما يتعلق الأمر بالتجسس السيبراني، فإن المشرع الجزائري استبعد نظام التقادم في الجرائم الماسة بأمن الدولة وجعل الدعوى العمومية غير قابلة للسقوط بمرور الزمن، وهو ما يتجاوز الحد الأدنى الذي طالبت به الاتفاقية ويضمن ملاحقة الجناة مهما طال الزمن، وهذا حسب ما نصت عليه المادة 12 من قانون الإجراءات الجزائية 25-14[2].

2. الالتزامات الإجرائية

أ. سن صلاحيات وإجراءات للتحقيق في الجرائم الإلكترونية وجمع الأدلة الرقمية، وتسري هذه الإجراءات على أي جريمة ترتكب بواسطة التكنولوجيا.

ب. إلزام الدول عن طريق سلطاتها المختصة في الأمر بحفظ البيانات الإلكترونية فوراً لمنع ضياع الأدلة، ويكون الاحتفاظ لمدة 3 أشهر لحماية الدليل من الضياع.

ت. الحفاظ على بيانات المرور بشكل عاجل والكشف عن مزود الخدمة المعني، وهي أداة جوهرية لتحديد مصدر هجمات التجسس وتتبع مساراتها.

ث. يمكن للسلطات إلزام أي شخص أو مزود خدمة بتسليم بيانات إلكترونية محددة، مما يمكن الحصول عليه من سجلات الاتصالات في التحقيقات.

ج. يمكن لسلطات الدول تفتيش الأنظمة المعلوماتية وضبط البيانات الإلكترونية، ويطبق هذا الإجراء عند اكتشاف خوادم أو أجهزة مستخدمة في عمليات التجسس.

ح. السماح بإمكانية مراقبة بيانات المرور وجمعها في الزمن الحقيقي، مما يتيح تتبع الاتصالات الجارية في عمليات التجسس السيبراني[3].

---

[1]- المواد 4، 18، 19، 22، 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، السالفة الذكر.

[2]- المادة 12 من قانون رقم 25-14 مؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، يتضمن قانون الإجراءات الجزائية، ج ر العدد 54، الصادر في 19 صفر عام 1447 الموافق 13 غشت سنة 2025.

[33]- المواد من 23 إلى 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، السالفة لذكر.

خ. القيام بالاعتراض القانوني للاتصالات، حيث تُلزم الدول الأطراف بتبني تدابير تشريعية وتقنية تمنح السلطات المختصة صلاحية جمع وتسجيل بيانات محتوى الاتصالات الإلكترونية في الوقت الحقيقي، أو إجبار مزودي الخدمة على التعاون في ذلك، في الجرائم الخطيرة مثل التجسس السيبراني، مع فرض سرية تامة على التنفيذ. وتطبق على اعتراض رسائل ومكالمات الجواسيس لمعرفة خططهم[1].

3. الضمانات القانونية.

أ. احترام سيادة الدول وعدم التدخل في شؤونها وعليه يحظر على أي دولة ممارسة صلاحياتها في مكافحة الجريمة المعلوماتية في إقليم دولة أخرى دون إذنها.

ب. تنفيذ الالتزامات المفروضة على الدول في إطار احترام حقوق الإنسان.

ت. يجب أن تخضع جميع التدابير الإجرائية للرقابة القضائية وأن تخضع لمبدأ التناسب، وتحديد مدة الإجراءات وأسبابها، لحماية الحقوق الرقمية للأفراد[2].

4. التعاون الدولي في مجال المكافحة

أ. تلتزم الدول بتقديم المساعدة القانونية المتبادلة للحصول على أدلة رقمية تفيد في كشف الجرائم.

ب. تسليم المشتبه في ارتكابهم جريمة من الجرائم المنصوص عليها، مما يمكن من تسليم الجواسيس السيبرانيين، لكن هذا التسليم يجب أن يخضع لشروط حتى يستوفي مشروعيته.

ت. تلتزم الدول باتخاذ تدابير وقائية وتعزيز قدراتها الدفاعية ضد الجرائم الإلكترونية، ومحاولة إرساء ثقافة الوقاية من الجرائم الإلكترونية وخاصة التجسس السيبراني على المستوى الوطني[3].

الفرع الثاني: جهود المنظمات الإقليمية لمكافحة التجسس السيبراني

تشكل الجهود الإقليمية ركيزة أساسية مكملة للمساعي الدولية في مكافحة الجرائم الإلكترونية؛ نظراً لمرونتها وقدرتها على صياغة قواعد تشريعية تتلاءم مع الخصوصيات الجغرافية والسياسية للدول الأعضاء. فالتكامل والتقارب بين دول الإقليم الواحد يمكن

---

[1]– المادة 30 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، السالفة الذكر.

[2]– المواد 5، 6، 24 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، السالفة الذكر.

[3]– المواد 35، 37، 53 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، السالفة الذكر.

المنظمات الإقليمية من توحيد الرؤى الأمنية والقانونية بشكل أسرع لمجابهة الاعتداءات الرقمية.

وفي هذا الصدد خصص هذا الجزء لدراسة جهود المجلس الأوروبي باعتباره الرائد في وضع أولى الاتفاقيات الملزمة عالمياً، والجهود المبذولة في فضاء جامعة الدول العربية.

أولا: جهود المجلس الأوروبي

يعتبر المجلس الأوروبي من أبرز الهيئات الإقليمية التي ساهمت في إرساء أطر قانونية لمواجهة الإجرام المعلوماتي، عبر حزمة من الآليات التشريعية والإجرائية الهادفة إلى كبح المخاطر الناجمة عن التكنولوجيا. وتتمثل هذه المساعي بإصدار التوصية رقم (95/13) المؤرخة في 11 سبتمبر 1995، والمتعلقة بالمشاكل الإجرائية الجنائية المرتبطة بتكنولوجيا المعلومات؛ إذ استهدفت دعم السلطات القضائية وأجهزة التحقيق في مجابهة هذه الجرائم. وتضمنت التوصية جملة من التدابير المحورية كتفتيش أنظمة الحاسوب، وتأكيدها على إلزامية تعاون مزودي خدمات الاتصالات مع الجهات المختصة، وحث الدول على تعديل قوانينها الإجرائية بما يضمن الحصول على الأدلة الرقمية ومحاسبة الجناة[1].

وفي سياق تطوير هذه العقيدة القانونية، اعتمد المجلس اتفاقية بودابست لمكافحة الجرائم الإلكترونية لعام 2001، بوصفها أول وثيقة دولية متخصصة في هذا المجال، واستهدفت الاتفاقية توحيد القواعد الموضوعية والإجرائية وتعزيز التعاون العابر للحدود؛ حيث ألزمت الدول الأطراف بتجريم الأفعال التي تستهدف سلامة الأنظمة، وهي ذاتها الأساليب التقنية المحورية المعتمدة في التجسس السيبراني. كما وضعت الاتفاقية ركائز مرنة للمساعدة القضائية المتبادلة[2].

وتعزيزاً للمواكبة التشريعية أمام تطور أساليب الجريمة الإلكترونية، طور المجلس الأوروبي أدواته عبر صياغة البروتوكول الإضافي الثاني لاتفاقية بودابست، وجاء هذا

[1]– لعور مرزوق، تازولت أكرم سيف الدين، الجرائم الإلكترونية والأمن السيبراني في الاتفاقيات الدولية والتشريع الجزائري، مذكرة مكملة لنيل شهادة الماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور –خنشلة–، 2024/2023، ص 58–59.

[2]– المرجع نفسه، ص 60.

البروتوكول كآلية مستحدثة لتجاوز بطء إجراءات المساعدة القضائية التقليدية التي كانت تتسبب في تلف أدلة التجسس الرقمي أو محوها. ومن أبرز آلياته الحديثة؛ السماح للسلطات القضائية بالاتصال المباشر بمزودي الخدمة ومسجلي النطاقات في الدول الأخرى لطلب بيانات المشتركين وكشف هويات المخترقين، بالإضافة إلى وضع قواعد للتعاون السريع في حالات الطوارئ التي تهدد الأمن القومي، وتشكيل فرق تحقيق مشتركة بين الدول. هذا إلى جانب استمرار جهود المجلس في تنظيم برامج تدريبية لتمكين القضاة والمحققين من التعامل مع الأدلة الرقمية وتفتيش الأنظمة السحابية مع الحفاظ على سرية البيانات[1].

ثانيا: جهود مكافحة التجسس السيبراني في إطار جامعة الدول العربية

تأسست جامعة الدول العربية بموجب ميثاقها في 22 مارس 1945، وعززت بمعاهدة الدفاع المشترك والتعاون الاقتصادي 17 جوان 1950. وتتمحور أهدافها الاستراتيجية حول توثيق علاقات الدول وتأمين الاستقرار الإقليمي[2]، وهي غايات تندرج ضمن محورين:

1. تحقيق الأمن القومي العربي

اقترن الأمن القومي العربي بالعمل الجماعي لمواجهة التهديدات الخارجية الموحدة، وصد التكتلات الطامعة، وتتبع الشبكات التخريبية المعادية وصدها. ويمثل الأمن القومي المنظومة الدفاعية المشتركة لحماية المصالح العليا. وامتثالاً للمتغيرات الرقمية المتسارعة، أقرت الجامعة نمطين من الخطط الأمنية وهي:

أ. الاستراتيجية الأمنية العربية: أقرها مجلس وزراء الداخلية العرب عام 1983 وتُحدث سنوياً. تتقاطع مع مكافحة التجسس الرقمي من خلال بنود أساسية أهمها:

– ترسيخ وحدة الأمن العربي والتكامل الدفاعي؛ لأن المساس باستقرار أي دولة يمتد لباقي المنظومة.

– مجابهة الأنماط الإجرامية المستحدثة وتطهير البيئة العربية من الانحرافات المهددة للاستقرار.

– تأمين البنى التحتية والمنشآت العامة ضد أي استهداف أو عدوان خارجي.

---

[1]– إلينا بليكسيدا، التعليقات على البروتكول الإضافي الثاني لاتفاقية الجريمة الإلكترونية تنتهي في أوائل مايو، 2021، مقال منشور على الموقع https://www.icann.org/، تاريخ الاطلاع 2026/05/16، على الساعة 13:34.

[2]– نادية سلامي، المرجع السابق، ص 275.

– كفالة الحماية القانونية للأفراد، وصيانة حرياتهم، وسلامة ممتلكاتهم.
– بسط الحماية الأمنية على المصالح الحيوية العربية خارج النطاق الجغرافي الإقليمي.
– تطوير القدرات الدفاعية الأمنية لردع جميع التهديدات[1].

ب. الاستراتيجية العربية لمكافحة جرائم تقنية المعلومات: اعتمدها مجلس وزراء الداخلية العرب بالقاهرة في 21 ديسمبر 2010، كآلية منبثقة عن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ونصت صراحة على تجريم الاعتداء على الأسرار الحكومية[2].

وتتحدد آليات المكافحة والتعاون الدولي بموجب هذه الاتفاقية في النقاط التالية:

– **توسيع الاختصاص القضائي:** ليشمل الجرائم المرتكبة داخل إقليم الدولة، أو على متن سفنها وطائراتها، أو من قبل مواطنيها في الخارج، أو الماسة بمصالحها العليا.
– **تسليم المجرمين والمساعدة القضائية:** تسهيل تبادل المتهمين، وتقديم أقصى دعم لنجاح التحقيقات القضائية وجمع الأدلة الإلكترونية، والتبادل السريع للمعلومات.
– **التدابير الرقمية المستعجلة: مثل** الحفظ المؤقت السريع للبيانات المخزنة منعاً لضياعها، والتعاون في التتبع عبر الحدود، والجمع الفوري لبيانات الاتصالات[3].
– **الجهود العلمية الاستباقية :**نشطت الأمانة العامة للمجلس مع المنظمات الأكاديمية مثل جامعة نايف العربية للعلوم الأمنية لتنظيم مؤتمرات لشرح الظواهر الإجرامية الرقمية، ومن أبرزها؛ ندوة تونس (2000)، مؤتمر القاهرة (2002)، ندوة شرم الشيخ (2008)، والمؤتمر العربي الأفريقي الثالث بالقاهرة (2010)[4].

2. توثيق الصلات وبناء تحالف بين الدول العربية

تتلاقى نصوص ميثاق جامعة الدول العربية ومعاهدة الدفاع المشترك عند رغبة تشكيل جبهة موحدة تصون السلام الداخلي وتحقق الدفاع الجماعي ضد أي تهديد يمس كيان الأمة العربية. وعلى الصعيد العملي، أثمر هذا التحالف التزامات قانونية متبادلة لحماية الأمن

[1]– المرجع نفسه، ص 277.
[2]– نادية سلامي، المرجع السابق، ص 278.
[3]– أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث، تخصص القانون الخاص، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج، 2021/2020، ص 200–201.
[4]– سلامي نادية، المرجع السابق، ص 279–280.

الخارجي للدول الأعضاء عبر إدراج نصوص عقابية تتصدى لأعمال التجسس الموجهة ضد الدول الحليفة، تفعيلاً لمبدأ "التضامن الدولي المشترك" لمكافحة الجرائم الماسة بالأمن الخارجي بصفة عامة[1].

فمن الناحية القانونية، قد ترتكب سلوكيات لا تجرمها القوانين الداخلية لعدم مساسها المباشر بالمصالح الوطنية، لكنها تصنف كجرائم خطيرة تضر بأمن دولة عربية وفق تشريعها الخاص، وهي أفعال لا يهتم بها القانون الداخلي في الأحوال العادية. إلا أنه في إطار التحالفات وعقود الدفاع المشترك، يتم بسط الاختصاص العقابي الوطني للنظر في تلك الجرائم أياً كان مكان اقترافها أو جنسية مرتكبها، حمايةً لأمن الدولة الشريكة. ويجد هذا التوجه تفسيره في ترابط المنظومة الأمنية العصرية؛ وعند مراجعة المنظومة الجنائية العربية، يتضح تبني هذا التضامن العقابي بنسب متفاوتة؛ فبينما يشترط التشريع الأردني وقوع الجريمة المخلة بأمن الدولة الحليفة في زمن الحرب مع اقتصارها على الأمن الخارجي، يتبنى قانون العقوبات التونسي المبدأ بشكل مطلق وبلا شروط[2].

ومن جهة أجاز المشرع الجزائري في إطار التحالف مع الدول العربية حماية أمن الدولة الحليفة من كل الجرائم المخلة به، فتخضع لأحكام الجنايات والجنح الماسة بأمن الدولة سواء وقت السلم أو الحرب، وشملت الحماية الأمنين الداخلي والخارجي، غير أن المشرع أبقى على الطابع الجوازي لهذه الآلية القانونية واشترط صدور مرسوم تنفيذي يحدد الأحكام وهذا ما أقرته المادة 94 من ق.ع[3].

المطلب الثاني

آليات التعاون الدولي وإقرار المسؤولية الدولية عن التجسس السيبراني

إن وجود النصوص القانونية والاتفاقيات الدولية لا يشكل وحده حلاً كافياً لمواجهة التجسس السيبراني؛ فالطبيعة العابرة لهذه الجريمة تجعل من المستحيل على أي دولة مواجهتها بمفردها. ومن هذا المنطلق، يكمن التحدي الحقيقي في الانتقال من مرحلة النصوص النظرية إلى مرحلة التطبيق الميداني، وهو ما يتطلب تفعيل آليات مرنة وسريعة للتعاون الدولي لتبادل

---

[1]– المرجع نفسه، ص 280.

[2]– سلامي نادية، المرجع السابق، ص 281.

[3]– المادة 94 من الأمر رقم 66–156 المتضمن قانون العقوبات الجزائري، السالف الذكر.

المعلومات وجمع الأدلة الرقمية قبل محوها. غير أن هذا التعاون الإجرائي لا يكتمل إلا بإرساء قواعد صارمة لإقرار المسؤولية الدولية، بما يضمن ملاحقة الجناة بفاعلية وضمان عدم إفلاتهم من العقاب تحت غطاء الحدود الجغرافية.

وتأسيساً على ذلك، تقتضي الإحاطة بأبعاد هذا الموضوع تقسيمه إلى فرعين، **(الفرع الأول)** يستقصي آليات التعاون الدولي كأداة للمواجهة والوقاية؛ و**(الفرع الثاني)** إلى بحث النظام القانوني للمسؤولية الدولية في الفضاء السيبراني.

الفرع الأول: آليات التعاون الدولي

يستلزم مكافحة جريمة التجسس السيبراني على الصعيد الدولي تقصي أثارها من مكان ووقت ارتكاب الجريمة، إلى تحقق نتيجتها، ولا يتحقق هذا الأمر إلا بشيء واحد وهو التعاون الدولي بين الدول التي طالتها هذه الجريمة، وهذا التعاون يكون عن طريق:

أولا: التعاون القضائي الدولي

يعتبر التعاون القضائي من أبرز الآليات الفعالة في الحد من الجرائم الإلكترونية التي ترتكب في دولة وتمتد أثارها لتمس سيادة دولة أخرى. غير أن هذا التعاون يصطدم بإشكالية تتمثل في الاختصاص القضائي والقانون الواجب التطبيق.

1. إشكالية تنازع الاختصاص القضائي

تثير الجرائم الإلكترونية العابرة للحدود إشكالية قانونية معقدة تتعلق بتنازع الاختصاص القضائي بين الدول، بحيث يثير الإشكال حول من هي الدولة صاحبة الاختصاص هل هي الدولة التي ارتكبت فيها الجريمة أو التي يحمل الجاني جنسيتها أو الدولة الضحية، حيث تجد الجهات القضائية الداخلية للدول نفسها أمام تداخل في معايير إسناد الاختصاص. فمن جهة يتم التمسك بمبدأ إقليمية النص الجنائي باعتباره المعيار الأصلي الذي بموجبه ينعقد اختصاص الدولة التي وقعت الجريمة فوق ترابها أو استغلت بنيتها الرقمية في الهجوم. ومن جهة أخرى تظهر المبادئ الاحتياطية كبديل إجرائي؛ حيث نجد مبدأ الشخصية وهو تطبيق قانون الدولة التي يحمل الجاني جنسيتها لحمايته أو محاكمته، في حين يشكل مبدأ العينية الأداة السيادية الأبرز التي تتيح للدول ملاحقة الجرائم التي تستهدف أمنها ومصالحها الحيوية حتى وإن

ارتكبها أجانب وخارج حدودها. هذا التعدد في المبادئ غالباً ما يضع القضاء الدولي في حالة تصادم وازدواجية حول تحديد الجهة القضائية ذات الأحقية في الاختصاص[1].

أ. معايير تحديد الأولوية القضائية في حال تنازع الاختصاص الدولي

لحسم هذا النزاع وفي حالة وجود جريمة ارتكبت في دولة وامتدت أثارها لدولة أخرى وكان مرتكبها ينتمي لدولة أخرى، وضعت المعاهدات الدولية قواعد تدرجية واضحة. ومن ذلك ما كرسته المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي منحت الأولوية المطلقة لـــ "معيار المصلحة المعتدى عليها" والذي يمثل المبدأ العيني؛ فمتى استهدفت الهجمات السيبرانية المواقع الحكومية الحساسة أو قواعد البيانات السيادية لدولة ما، فإن حقها في حماية أمنها القومي يتقدم قانوناً على المبدأين الإقليمي والشخصي[2].

ب. موقف المشرع الجزائري: كرس المشرع الجزائري المبدأ العيني في المادة 15 من القانون رقم 09-04، مانحاً المحاكم الجزائرية الولاية القضائية الكاملة للفصل في الجرائم الرقمية المرتكبة خارج الإقليم الوطني من طرف أجانب، متى استهدفت مؤسسات الدولة، أو الدفاع الوطني، أو المصالح الاستراتيجية[3].

أما في الأحوال التي لا تشكل فيها الجريمة المعلوماتية مساساً مباشراً بأمن دولة بعينها، فإن الاختصاص يعود للترتيب التقليدي بالاحتكام أولاً إلى مبدأ الإقليمية، ثم مبدأ الشخصية، وصولاً إلى معيار الأسبقية في تقديم طلب التسليم عند اتحاد الظروف[4].

وبناءً على هذا، فإن حل هذا التنازع والبدء في الملاحقة الفعلية لا يتحقق إلا بالانتقال إلى الآليات الإجرائية للتعاون القضائي.

2. الآليات الإجرائية للتعاون القضائي الدولي

---

[1]- بطيحي نسيمة، محاضرات في مقياس الوقاية من الجرائم الإلكترونية، مطبوعة مقدمة لطلبة السنة ثانية ماستر، تخصص إدارة إلكترونية وخدمات رقمية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين-سطيف2-، 2022/2021، ص 72.

[2]- بطيحي نسيمة، المرجع السابق، ص 74.

[3]- المادة 15 من قانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر.

[4]- بطيحي نسيمة، المرجع السابق، ص 75.

لتجسيد التعاون القضائي على أرض الواقع وتجاوز عقبات السيادة، تستعين الدول بحزمة من التدابير القانونية المرنة أبرزها:

أ. الإنابة القضائية

يقصد بالإنابة القضائية الدولية تلك الآلية القانونية التي تتيح للسلطات القضائية في دولة ما أن تطلب من سلطات قضائية في دولة أخرى تنفيذ إجراء قضائي معين نيابةً عنها بسبب تعذر القيام بالإجراء بنفسها، سواء تعلق الأمر بتبليغ أوراق قضائية، أو القيام بإجراءات البحث والتحري أو التحقيق[1]، وتجد هذه الآلية مبررها في مبدأ السيادة الإقليمية الذي يقيد صلاحيات القاضي داخل حدود دولته، فلا يملك الحق بالقيام بإجراء يفيد في الكشف عن الحقيقة في دولة أخرى إلا عن طريق الإنابة، مما يجعل التعاون القضائي الدولي ضرورة لا غنى عنها لضمان حسن سير العدالة في القضايا ذات الطابع العابر للحدود. وتندرج هذه العملية عادةً في إطار اتفاقيات ثنائية أو متعددة الأطراف، وتوجه طلبات الإنابة عبر القنوات الدبلوماسية أو جهات مختصة، وتنفذ وفق قانون الدولة الموجه إليها الطلب، مع مراعاة الشروط والقيود التي قد تشترطها تلك الدولة للاستجابة لمثل هذه الطلبات[2].

ب. تبادل المعلومات

يقصد بتبادل المعلومات قيام الأجهزة القضائية والأمنية في دول مختلفة بالتواصل المباشر لتقديم البيانات، الوثائق، والمواد الاستدلالية التي تطلبها الدولة الأخرى لتساعدها في التحقيق. غير أن اشتراط الطلب المسبق قد لا يتلاءم مع سرعة التهديدات الرقمية؛ ولذلك جاءت المادة 26 من بودابست لعام 2001 لتنص على إمكانية تبادل المعلومات بدون طلب، إذ تخطت المفهوم التقليدي للتبادل القائم على الطلب، وكرست مبدأ "التدفق التلقائي للمعلومات" بين الدول الأطراف. وبموجب هذا المقتضى المستحدث، يحق لأي دولة من تلقاء نفسها وبمبادرة ذاتية أن تحيل إلى دولة أخرى ما رصدته أجهزتها الاستخباراتية والأمنية من

---

[1]– عمارة زينب، الوقاية من الجرائم الإلكترونية، مطبوعة بيداغوجية ألقيت على طلبة السنة ثانية ماستر للسداسي الثالث، تخصص إعلام ألي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج، 2022/2021، ص 57–58.

[2]– عثماني رضوان، مكافحة جرائم المعلوماتية في القانون الجزائري والدولي، أطروحة مقدمة للحصول على شهادة الدكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد 2 وهران، 2024/2023، ص201

معطيات رقمية، متى تبين لها أن هذه البيانات ستفيد الطرف الآخر في كشف هجمات سيبرانية أو عمليات تجسس تستهدف بنيته التحتية الحيوية أو منظومته المعلوماتية السيادية[1].

ت. نقل الإجراءات

يقصد بنقل الإجراءات قيام دولة ما استناداً إلى اتفاقية أو معاهدة دولية بتبني واتخاذ حزمة من الإجراءات الجنائية المتعلقة بجريمة نفذت أركانها فوق إقليم دولة أخرى، على أن تباشر الدولة المنقول إليها هذه الملاحقة لمصلحة الدولة الطالبة. ويشترط لقيام هذه الآلية توفر عدة شروط منها شرط التجريم المزدوج الذي يستوجب أن يكون الفعل مجرماً في كلا الدولتين، وضرورة أن تكون الإجراءات تكتسي طابع المشروعية، بحيث تتوافق التدابير المراد اتخاذها مع النظام القانوني والتشريعي للدولة المطلوب منها تنفيذ الإجراءات، وأن تكتسي الإجراءات طابع الجدية والأهمية وذلك بأن تنطوي التدابير المطلوبة على أهمية بالغة تمكن فعلياً من كشف ملابسات الجريمة والوصول إلى حقائقها الفاصلة[2].

نصت العديد من الاتفاقيات الدولية على هذا الإجراء؛ كاتفاقية بودابست المتعلقة بمكافحة الجرائم المعلوماتية في المادة 23[3].

ث. تسليم المجرمين كآلية لمكافحة جريمة التجسس السيبراني

يقصد بتسليم المجرمين تخلي الدولة التي لجأ إليها المتهم أو المحكوم عليه في جريمة معلوماتية عنه، وتسليمه إلى الدولة التي تطلبه بقصد محاكمته أو تنفيذ العقوبة بحقه. ويتوقف هذا الإجراء على شروط محددة[4].

– شروط تسليم المجرمين

تتأسس آلية التعاون الدولي لتسليم المتهمين على مجموعة من الشروط الموضوعية التي تحكم قبول الطلب أو رفضه. فبموجب الفقرة الأولى من المادة 37، يشترط لقيام عملية التسليم تحقق مبدأ الازدواجية الجنائية، بحيث يكون فعل التجسس مجرماً ومعاقباً عليه في

---

[1]– المادة 26 من اتفاقية مكافحة الجريمة المعلوماتية بودابست السالفة الذكر.

[2]– قزران مصطفى، زرقين عبد القادر، الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، المجلد الثامن، العدد 02، جامعة الجيلالي بونعامة خميس مليانة، 2022، ص ص1222–1244، ص 1227.

[3]– المرجع نفسه، ص 1228.

[4]– خرشي عثمان، تسليم المجرمين كآلية دولية لمكافحة الجرائم المعلوماتية، مجلة البحوث القانونية والسياسة، العدد العاشر، جامعة مولاي الطاهر بسعيدة، جوان 2018، ص 930.

قانون الدولة الطالبة والدولة متلقية الطلب معاً. ومع ذلك منحت الفقرة الثانية مرونة اختيارية للدول بأن تتجاوز عن هذا الشرط وتوافق على التسليم إذا كان قانونها الداخلي يسمح بملاحقة هذه الأفعال الخطيرة حتى لو لم تكن مجرمة لديها. وفي حالة تشابك الجرائم، تجيز الفقرة الثالثة جمع الجرائم المرتبطة بالتجسس السيبراني في ملف واحد وتسليم المتهم عنها حزمة واحدة لمنع تجزئة العدالة[1].

ولسد الفراغ القانوني عند غياب المعاهدات، نصت الفقرة الرابعة على إدراج هذه الجرائم تلقائياً في أي اتفاقية تسليم قائمة، بينما سمحت الفقرة الخامسة باتخاذ هذه الاتفاقية الدولية كقاعدة وأساس قانوني مباشر لإتمام التسليم بين الدول التي لا ترتبط بمعاهدات ثنائية، في حين اعتبرت الفقرة السابعة الجريمة السيبرانية موجبة للتسليم تلقائياً بين الدول التي لا تشترط وجود معاهدات أصلاً[2].

ويحق للدول رفض تسليم مواطنيها بحسب الفقرة الحادية عشرة، لكن تصبح الدولة ملزمة بإحالة القضية فوراً لقضائها الوطني لمحاكمته محلياً تفعيلاً لمبدأ "إما التسليم أو المحاكمة". أو النظر وفقاً للفقرة الثالثة عشرة في تنفيذ الحكم الأجنبي داخل سجونها الوطنية إذا كان المطلوب مواطناً[3].

- **إجراءات القيام بالتسليم**

تمر العملية الإجرائية للتسليم بخطوات صارمة تتلاءم مع سرعة الجريمة الرقمية العابرة للحدود؛ حيث ألزمت الفقرة التاسعة الدول الأعضاء بتبسيط الإجراءات والتعجيل فيها لتفادي ضياع الدليل. وتنفيذاً لذلك منحت الفقرة العاشرة الدولة الطالبة الحق في الالتماس المستعجل للاعتقال الاحتياطي للمتهم لضمان عدم فراره أو تدميره للأدلة، وهو إجراء يتم تفعيله بمرونة عبر قنوات منظمة الشرطة الجنائية الدولية (الإنتربول)، مع كفالة المعاملة المنصفة وضمانات الدفاع للمتهم بموجب الفقرة الرابعة عشرة[4].

وقبل اتخاذ أي قرار نهائي بالرفض، فرضت الفقرة السابعة عشرة التزاماً إجرائياً يقضي بوجوب فتح باب التشاور بين الدولتين لمنح الدولة الطالبة فرصة كافية لتقديم أدلتها الفنية

---

[1]– المادة 37 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، السالفة الذكر.

[2]– المادة 37 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، السالفة الذكر.

[3]– المادة 37 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، السالفة الذكر.

[4]– المادة 37 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، السالفة الذكر.

وتقارير الفحص الرقمي، على أن تقوم الدولة متلقية الطلب بإبلاغ الطرف الآخر بقرارها النهائي وأسبابه فور صدوره تفعيلاً للفقرة الثامنة عشرة. وتكتمل هذه المنظومة بموجب الفقرة التاسعة عشرة التي تفرض على كل دولة تحديد "سلطة مركزية" رسمية تتولى حصرياً مسؤولية طلبات التسليم، مع حث الدول في الفقرة العشرين والأخيرة على إبرام اتفاقيات ثنائية لتعزيز فاعلية هذه الإجراءات

ثانيا: التعاون الأمني والفني الدولي لمكافحة التجسس السيبراني

بسبب خطورة التجسس السيبراني على الدول بات من الضروري تفعيل التعاون الدولي الأمني والفني لإضفاء الفعالية اللازمة على آليات التصدي لهذه الظاهرة.

1. التعاون الأمني

يتجسد التعاون الدولي في الشق الأمني من خلال إنشاء شبكات متخصصة، وتفعيل دور المنظمات الدولية والإقليمية لتنسيق الجهود وملاحقة الجناة عبر الحدود، وذلك وفق الآليات التالية:

أ. إنشاء مكاتب وشبكات متخصصة لتبادل المعلومات: من خلال تأسيس مراكز وطنية ونقاط اتصال أمنية دورها جمع وتحليل البيانات المتعلقة بمرتكبي الجرائم السيبرانية، وتوفير المساعدة التقنية وتبادل الخبرات بين الدول (مثل شبكة النقطة المضيئة 7/24)[1].

ب. التعاون في إطار المنظمة الدولية للشرطة الجنائية (الإنتربول):

تعد المنظمة الدولية للشرطة الجنائية (الإنتربول) منظمة حكومية دولية تضم في عضويتها 196بلداً، وتتخذ من مدينة ليون بفرنسة مقراً لأمانتها العامة، إلى جانب مجمّعها العالمي للابتكار في سنغافورة .تهدف المنظمة أساساً إلى تيسير التعاون الأمني العابر للحدود وتبادل البيانات الجنائية لتعزيز الأمن العالمي[2]. وتعتمد في هيكلها التشغيلي على المكاتب المركزية الوطنية كحلقة وصل أساسية في كل دولة عضو، وترتبط هذه المكاتب عبر شبكة

[1]– شرويلي فاطمة، ديدي فضيلة، آليات مكافحة الجريمة الإلكترونية، مذكرة مقدمة لنيل شهادة الماستر، تخصص قانون أعمال، قسم القانون، معهد الحقوق، المركز الجامعي صالحي أحمد –النعامة–، 2023/2022، ص 39.

[2]– المادة 1، 2 من القانون الأساسي للمنظمة الدولية الشرطية الجنائية الإنتربول، اعتمد أثناء الدورة الـــ 25 للجمعية العامة فيينا 1956، متاح على الموقع https://www.legal-tools.org/، تاريخ الاطلاع 2026/05/18، على الساعة 2:42.

اتصالات عالمية آمنة التي تتيح الوصول الفوري لقواعد البيانات الشرطية. وتتمتع المنظمة بـــالحياد التام، مما يسمح للدول بالتعاون الأمني حتى في غياب العلاقات الدبلوماسية بينها.

أنشأت المنظمة خلال عام 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا، كما قامت بالتعاون مع مجموعة الدول الثمانية الكبرى (G8) بوضع استراتيجيات لمواجهة هذه الجرائم من خلال إنشاء مركز اتصالات أمني عبر الشبكة يعمل على مدار 7/24على مستوى مصالح الشرطة في الدول الأطراف. واعتمدت المنظمة في هذه المكافحة على استخدام وسائل تقنية حديثة، وتزويد شرطة الدول بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب والتحقيق فيها، مما سمح بتحقيق إنجازات هامة بالاشتراك مع المباحث الفيدرالية الأمريكية والشرطة الإنجليزية والألمانية، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء لملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة[1].

– المنصات الرقمية المتخصصة

توفر المنظمة عبر موقعها الرسمي منظومة متكاملة من خدمات الدعم والتعاون لمواجهة التهديدات الرقمية، وتعتمد في ذلك على منصتين دورهما التنسيق بين الدول الأعضاء والشركاء.

منصة تبادل المعارف المتصلة بالجريمة السيبرانية: وهي فضاء آمن يجمع أجهزة إنفاذ القانون والخبراء الدوليين. وترتكز وظيفتها الأساسية على تبادل المعلومات والخبرات غير العملياتية، ونشر تقارير التهديدات السيبرانية الناشئة، وتعميم أفضل الممارسات والأساليب التحقيقية لمساعدة الدول على فهم الأنماط الإجرامية الحديثة وبناء قدراتها الوقائية، أي دورها وقائي وتوعوي، تستعمل لتبادل التقارير والخبرات، وأفضل الأساليب لمكافحة الجرائم، ومحاولة فهم الجرائم السيبرانية الناشئة لوضع لها استراتيجية للتصدي لها[2].

منصة التعاون لمكافحة الجريمة السيبرانية: وهي منصة عملياتية ذات طابع سري ومقيد، يقتصر الدخول إليها على الأطراف والجهات المعنية بالعمليات الميدانية فقط. وتستخدم هذه

---

[1]– الطاهر ياكر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، المجلد 4، العدد 4، 2022جامعة الجيلالي بونعامة خميس مليانة، ص 16.

[2]– خدمات التعاون في مجال مكافحة الجريمة السيبرانية، موقع الإنتربول الرسمي، https://www.interpol.int/، تاريخ الاطلاع 2026/05/18، على الساعة 10:53.

المنصة كأداة للتنسيق الفوري في التحقيقات الجنائية العابرة للحدود، حيث تسمح بتبادل البيانات الحساسة والأدلة الرقمية وتوحيد الجهود لتفكيك الشبكات الإجرامية وإسقاط بنياها التحتية[1].

أما فيما يتعلق بالحد من التجسس السيبراني، فإن دور هاتين المنصتين يتجلى بوضوح في جانب المكافحة الإجرائية والتقنية؛ حيث تتيح منصة المعارف للدول الأعضاء رصد وتحليل الأفعال والأساليب المكونة للجريمة، بينما تستغل منصة العمليات في تتبع الآثار الرقمية لمرتكبي هذه الاعتداءات، وتنسيق الجهود الشرطية الدولية المشتركة لتعطيل هذه المنظومات التخريبية وضبط المتورطين فيها.

– وسائل الإنتربول لمكافحة جريمة التجسس السيبراني

تساهم منظمة الإنتربول بشكل كبير وفعال في ملاحقة مرتكبي الجرائم الإلكترونية وتفكيك شبكاتهم عبر توظيف وسائل وآليات دولية تتيح لها هذه الملاحقة، وتعتبر النشرات الدولية من أهم الأدوات الدولية الحاسمة في هذا المجال، وفي مقدمتها النشرة الحمراء التي تتيح ملاحقة الجناة الرقميين المطلوبين دولياً الصادرة بحقهم أحكام وقرارات توقيف قضائية. كما تلعب النشرة الزرقاء دور وقائي هام يتمثل في تتبع حركات المتورطين أو المشتبه فيهم ارتكاب أنشطة التجسس وتحديد مواقعهم عند محاولتهم مغادرة الدول أو دخولها. وبما أن هذه الجرائم تعتمد في ارتكابها على أدوات وبرمجيات خبيثة فإن النشرة البنفسجية تنشرها المنظمة لإعطاء معلومات دورية للدول حول الأساليب المستخدمة في هذه الجرائم[2].

ت. تنفيذ العمليات الأمنية المشتركة: ويتمثل ذلك في تنسيق الجهود بين الدول عند وقوع جريمة سيبرانية عابرة للحدود لتتبع الجناة وملاحقتهم؛ بحيث تلتزم كل دولة بمباشرة إجراءات البحث والتحري والتحقيق الأولي وضبط الأدلة الرقمية وفقاً لاختصاصها الإقليمي، بما يضمن تكامل الأدوار وسرعة التصدي للجريمة[3].

ث. الاتحاد الإفريقي للتعاون الشرطي الأفريبول

---

[1]– المرجع نفسه.

[2]– بوعكاز أسماء، مباركي دليلة، الإنتربول ودوره في تنفيذ اتفاقيات تسليم المجرمين في إطار مكافحة الجريمة المنظمة، مجلة الباحث للدراسات الأكاديمية، المجلد 08، العدد 03، جامعة باتنة 1، 2022، ص130–131.

[3]– شرويلي فاطمة، ديدي فضيلة، مرجع سابق، ص 39.

تعتبر آلية الاتحاد الإفريقي للتعاون الشرطي الأفريبول آلية إقليمية ومؤسسة تقنية حديثة استحدثت لتعزيز التعاون الأمني بين الدول الإفريقية والحد من الجرائم، حيث بدأت فكرة إنشائها في سبتمبر عام 2013 بوهران، وتمت الموافقة على أن تكون الجزائر مقراً لها في فيفري عام 2014، ليتم بعد ذلك اعتماد نظامها الأساسي رسمياً من قبل مؤتمر الاتحاد الإفريقي بأديس أبابا في عام 2017. وتهدف هذه الآلية بشكل أساسي إلى وضع استراتيجية إفريقية منسقة لمنع الجرائم الخطيرة وتطوير قدرات أجهزة الشرطة الوطنية، ومساعدة الشرطة الوطنية للدول أو القارية أو الدولية مثل الإنتربول، وتسهيل المساعدة القانونية المتبادلة وتيسير تبادل المعلومات، ووضع استراتيجيات ونظم وقواعد بيانات ملائمة في المجالات الأمنية لتنفيذ المهام المذكورة أعلاه[1].

2. التعاون الفني والتقني

بسبب التطور المتسارع للمنظومة الرقمية، لم يعد التعاون القضائي والأمني الدولي كافيا، بل أصبح من الواجب بناء منظومة تعاون فني وتقني تضمن الاستجابة الفورية لبناء القدرات الاستباقية، وتتجلى هذه المنظومة في:

أ. الاتحاد الدولي للاتصالات

يعد الاتحاد الدولي للاتصالات باعتباره وكالة متخصصة تابعة للأمم المتحدة النقطة المركزية لتوجيه التعاون الدولي بين الحكومات والقطاع الخاص في مجال تكنولوجيا المعلومات. وفي إطار مكافحة التهديدات الأمنية والتجسس السيبراني، يرتكز دور الاتحاد على تنفيذ المخطط العالمي لتعزيز الأمن السيبراني من خلال تعزيز الأمن بوضع استراتيجيات متكاملة فيما بينها؛ تشمل تطوير النظم التشريعية وتوحيدها وجعلها قابلة للتطبيق وطنيًا ودوليًا، وتهيئة البيئات التنظيمية والسياسية لمكافحة الجرائم المعلوماتية، مع وضع الحد الأدنى لمعايير الأمن التقني عالميًا. كما تمتد هذه الجهود لتأسيس آليات دولية للمراقبة والإنذار المبكر والتنسيق العابر للحدود، وبناء نظام عالمي موثوق للهوية الرقمية والاعتراف بالوثائق

[1]– ودرار أمين، الشرطة الجنائية الإفريقية "الأفريبول"، حوليات جامعة الجزائر 01، المجلد 34، العدد 01، جامعة الجزائر 01، لسنة 2020، ص ص137–140.

الإلكترونية، فضلاً عن التركيز على بناء القدرات البشرية والمؤسسية، وتقديم المشورة الفنية لتعزيز الحوار والشراكة الاستراتيجية بين جميع أصحاب المصلحة على المستوى الدولي[1].

ب. تفعيل منظومة الإنذار المبكر السيبراني كآلية دفاعية دولية استباقية

يعد الإنذار المبكر السيبراني في السياق الدولي أحد أبرز ركائز الأمن السيبراني الجماعي الوقائي في مواجهة جرائم التجسس الرقمي واختراق سيادة الدول. ويقصد به تلك الآلية التقنية والإجرائية القائمة على الرصد المستمر وتبادل المعلومات الرقمية بين الدول بصفة فورية، للتنبؤ بالتهديدات والبرمجيات الخبيثة الموجهة ضد الأنظمة الحساسة قبل اكتمال ركنها المادي.

وتكمن أهمية هذه المنظومة في طابعها الوقائي الذي يتجاوز فكرة رد الفعل بعد وقوع الجريمة، إلى فكرة الوقاية والتحصين حيث تلتزم الدول عبر مراكز الاستجابة للطوارئ المعلوماتية المشتركة (CERT) بالإخطار المتبادل عن أي مؤشرات اختراق أو ثغرات أمنية تستغلها الجماعات الإجرامية، وعزل الأنظمة المعلوماتية التي طالها الهجوم لمحاولة توقيفه قبل أن يمتد إلى أنظمة أخرى، وتفعيل خطط الطوارئ لهذه الأوقات[2].

ت. التدريب كآلية فنية لتفعيل مكافحة التجسس السيبراني

يقصد بـــنظام التدريب إخضاع عناصر تنفيذ القانون من مصالح قضائية ومختصين فنيين لتكوين تقني متخصص ومستمر في مجال الأمن السيبراني والأدلة الرقمية. ويشمل هذا التدريب ماهية المخاطر المستحدثة للتكنولوجيا وأنماط القيام بهذه الجرائم، ومحاكاة طرق التجسس الإلكتروني، والتعرف على أساليب زرع برمجيات التجسس، وكيفية القيام بإجراءات التحقيق المستحدثة وكيفية فحص الشبكات واستخراج الأدلة الرقمية وتأمينها بطرق علمية وقانونية. وتكتسي هذه الآلية طابعاً وقائياً من خلال تمكين الجهات المختصة من الرصد الاستباقي للثغرات الأمنية ومحاولات التسلل غير المشروعة وقبل وقوع عملية تسريب

---

[1]– علوي علي أحمد الشارفي، الوجيز في جرائم تقنية المعلومات، الطبعة الأولى، المركز الديمقراطي للنشر برلين، ألمانيا، 2024، ص 117.

[2]– أمحمد إسماعيل، زوبيري عبد الحليم، دور التكنولوجيا الحديثة في ارتكاب الجرائم الإلكترونية وسبل مكافحتها، مذكرة تخرج لنيل شهادة الماستر تخصص قانون جنائي والعلوم الجنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2025/2024، ص 78.

البيانات، بالإضافة إلى تحقيق الردع التقني الذي يقلل من احتمالية استهداف البنى التحتية المعلوماتية الحيوية للدولة[1].

الفرع الثاني: إقرار المسؤولية الدولية للدول عن أعمال التجسس السيبراني

لا يقتصر تصدي القانون الدولي العام لظاهرة التجسس السيبراني على الملاحقة الجنائية للجواسيس فقط، بل يمتد ليشمل مساءلة الدول باعتبارها الأشخاص الرئيسة للقانون الدولي في حال ثبوت تورطها المباشر أو تقصيرها السيادي.

أولاً: أساس قيام المسؤولية الدولية وشروط إسناد الفعل الرقمي للدولة

لقيام المسؤولية الدولية للدول التي ترتكب جريمة التجسس السيبراني يجب أن تتوفر عدة شروط وهي:

1. **وجود فعل غير قانوني ينتهك قواعد القانون الدولي:** ويقصد به ارتكاب فعل مخالف للالتزامات الدولية والذي يشكل ضرراً على الأخرين، وفي جريمة التجسس السيبراني يعتبر كل فعل من شأنه الحصول على معلومات أو معطيات بغية استعمالها بطريقة غير مشروعة جريمة يعاقب عليها القانون الدولي أو القوانين الداخلية[2].

2. **نسبة الفعل إلى أحد أشخاص القانون الدولي:** لكي تترتب المسؤولية الدولية عن الدول في حال ارتكابهم جريمة التجسس يجب أن يسند هذا الفعل إلى دولة ما أو شخص من أشخاص القانون الدولي الذي يتمتع بالسيادة الكاملة، فلا يمكن مسائلة دولة لا تمتلك سيادة فهي لا حقوق لها، ومن المعروف أن التجسس السيبراني تقوم به الدول ذات الإمكانيات الكبيرة والتكنولوجيا المتطورة والتي بطبيعة الحال تمتلك سيادة[3].

---

[1]– بوحزمة نصيرة، التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس–سيدي بلعباس–، 2022/2021، ص 282–283.

[2]– أحمد سعيد أحمد، المسؤولية الدولية الناتجة عن الجرائم السيبرانية، مجلة الباحث العلمي، مجلة الباحث العربي، مجلد 6، عدد 04، جامعة الدول العربية –مجلس وزراء العدل العرب– المركز العربي للبحوث القانونية والقضائية، 2025، ص 9.

[3]– المرجع نفسه، ص 9.

3. وقوع ضرر يمس بالمصلحة العامة: ويتمثل هذا الضرر في المساس بأمن الدولة أو كيانها أو أحد مؤسساتها، ويجب أن يكون الضرر نتيجة للفعل، فعند ارتكاب جريمة التجسس السيبراني لا بد أن يشكل ضرر على الدولة الضحية[1].

فإذا توافرت هذه الشروط وثبت أن الدولة محل الشبهة هي من ارتكبت التجسس السيبراني تقوم عليها المسؤولية الجنائية الدولية.

ثانيا: إشكالية إثبات التجسس السيبراني

تتمحور الإشكالية الكبيرة في إقرار المسؤولية الدولية عن فعل التجسس السيبراني حول صعوبة توقيف الجناة، وسرعة محو الدليل الرقمي، لكن العقبة الرئيسية تكمن في العنصر الشخصي، أي إسناد الفعل إلى الدولة التي ارتكبت الفعل إما عبر جواسيس محترفين أو عبر أجهزتها الاستخباراتية. وذلك بسبب أن الدولة التي ترسل الجاسوس تنكر عادةً معرفتها به فور القبض عليه، ولهذا فالدول التي تقف وراء الهجمات السيبرانية تلجأ إلى ما يعرف بالأنكار مستغلةً صعوبة التحقق التقني من مصدر الهجوم وهوية منفّذه الحقيقي.

ومع ذلك، فإن الفقه الدولي يقر بإمكانية إسناد الفعل إلى الدولة متى ثبت أن القائمين بالهجمات السيبرانية كانوا يتلقون تعليمات وتوجيهات من قبلها أو يعملون تحت رقابتها، وهو ما نصت عليه المادة 8 من مسودة لجنة القانون الدولي حول مسؤولية الدول، على أن الفعل يعتبر صادراً عن الدولة إذا كان الأشخاص يتصرفون في الواقع بناءً على تعليمات تلك الدولة أو بتوجيهات منها وتحت رقابتها، فإذا ثبت أن الجاسوس أخذ تعليماته من تلك الدولة أو عمل تحت رقابتها، فهنا تقوم المسؤولية الجنائية الدولية للدولة ولا يمكنها التهرب من تحمل المسؤولية[2].

[1]– المرجع نفسه، ص 10.

[2]– خالد وليد شوشان، التجسس في القانون الدولي، مجلة الحقوق، العدد 4، جامعة الكويت، 2016، ص316–317.

المبحث الثاني

استراتيجية مكافحة التجسس السيبراني على المستوى الوطني

تلزم الاتفاقيات الدولية الدول الأعضاء بتبني تشريعات داخلية للحد من الجرائم المعلوماتية؛ وهو ما ينطبق على الجزائر التي تواجه جريمة التجسس السيبراني كأحد أخطر التحديات التي تمس أمنها ومعطياتها الحساسة. وفي هذا السياق، تعكس المؤشرات الحديثة حجم التهديد الذي تواجهه الجزائر في هذا المجال، حيث صنفت ضمن أكثر الدول استهدافاً بالهجمات السيبرانية، واحتلت المرتبة 19 عالمياً كأكثر الدول استهدافاً بالهجمات السيبرانية، بنحو 70 مليون هجمة استهدفت قطاعات حيوية كالحكومة والمال والمحروقات.

هذا الواقع فرض على الجزائر تبني تدابير وطنية وتفعيل هياكل مؤسساتية لحماية فضائها الرقمي، ورغم أنها لم تفرد استراتيجية مستقلة لقمع جريمة التجسس السيبراني، إلا أنها أدرجتها ضمن جهودها العامة لمكافحة الجريمة المعلوماتية.

وتأسيساً على ذلك، تقتضي دراسة هذه الآليات تقسيم هذا المبحث إلى مطلبين؛ يركز **(المطلب الأول)** على استراتيجيات مكافحة التجسس السيبراني، بينما يدرس في **(المطلب الثاني)** إجراءات المتابعة القضائية لجريمة التجسس السيبراني.

المطلب الأول

استراتيجيات مكافحة جريمة التجسس السيبراني

لمواجهة جريمة التجسس السيبراني، لم يكتفي المشرع الجزائري بالجانب التشريعي فقط، بل اعتمد منظومة ترتكز على استراتيجية وطنية قادرة على التعامل مع مختلف الجرائم الإلكترونية، وخاصة الجرائم المعقدة مثل التجسس السيبراني. فخصوصية هذا النوع من الجرائم، فرض على الدولة اللجوء إلى حلول متعددة تشمل بالدرجة الأولى تفعيل أجهزة ومؤسسات خاصة، إلى جانب ذلك تدابير احترازية وتقنية.

ويقتضي الأمر دراسة هذه الاستراتيجيات كل واحدة على حدة، بحيث خصص **(الفرع الأول)** للآليات المؤسساتية للوقاية من جريمة التجسس السيبراني، أما **(الفرع الثاني)** خصص للتدابير الوقائية وأخيراً **(الفرع الثالث)** خصص للتدابير التقنية.

الفرع الأول: الآليات المؤسساتية لمكافحة جريمة التجسس السيبراني

لا يمكن أن تكتسي الاستراتيجية الوطنية لمكافحة جريمة التجسس السيبراني طابع الفعالية، إلا من خلال تجسيدها ميدانياً عبر أجهزة مختصة، تتولى تنفيذ آليات التصدي وذلك لرصد التهديدات الواقعة على الفضاء السيبراني وردعها. ولذلك اعتمدت الجزائر على جملة من المؤسسات التي يتكامل دورها بين الوقاية والمراقبة والتنسيق مع المصالح القضائية، وتتمثل هذه الأجهزة في:

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

تمثل هذه الهيئة الجهاز المركزي المكلف بمواجهة التهديدات السيبرانية. وقد أنشئت بموجب القانون 09-04[1]، وقد شهدت لاحقاً إعادة هيكلة جذرية لتعزيز فعاليتها.

1. الطبيعة القانونية:

[1]- المادة 13 من قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف الذكر.

بموجب المرسوم الرئاسي رقم 21-439[1] المعدل والمتمم بالمرسوم الرئاسي 24-381[2]، تم تكريس الهيئة كسلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، وتوضع لدى رئاسة الجمهورية، مما يمنحها صلاحيات واسعة ومرونة في التنسيق بين الأجهزة.

2. الصلاحيات والاختصاصات الاستراتيجية

تتولى الهيئة مهام محورية تتوزع بين الجوانب الوقائية والتقنية والقضائية أبرزها:

أ. إعداد الاستراتيجية الوطنية للوقاية من الجرائم المعلوماتية والإشراف على تنفيذها.

ب. المراقبة الوقائية للاتصالات: للكشف المبكر عن الجرائم المعلوماتية الخطيرة، وذلك تحت إشراف السلطة القضائية المختصة.

ت. التنسيق العسكري والأمني: التعاون مع مصالح وزارة الدفاع الوطني في مجالات المراقبة الإلكترونية التي تقع ضمن اختصاص الجيش الوطني.

ث. الدعم التقني والقضائي: مساعدة الجهات القضائية عبر تقديم الخبرات الفنية، وذلك عن طريق جمع الأدلة الرقمية.

ج. التكوين والتطوير: المساهمة في تكوين المتخصصين في مجال التحريات الرقمية[3].

ح. تجهيز البنية التحتية: اقتناء الوسائل والتجهيزات والحلول التقنية اللازمة، لمراقبة الاتصالات الإلكترونية وصيانتها[4].

---

[1]- مرسوم رئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 86، الصادرة في 6 ربيع الثاني عام 1443 الموافق 11 نوفمبر سنة 2021.

[2]- مرسوم رئاسي رقم 24-381 مؤرخ في 25 جمادى الأولى عام 1446 الموافق 27 نوفمبر سنة 2024، يتمم المرسوم الرئاسي رقم 21-439 المؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021 والمتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 80، الصادر في 2 جمادى الثانية عام 1446 الموافق 4 ديسمبر سنة 2024.

[3]- المادة 04 من مرسوم رئاسي رقم 21-439 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر.

[4]- المادة 33 مكرر من مرسوم رئاسي رقم 24- 381 يتمم المرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر.

خ. البعد الدولي والتعاون العابر للحدود: بسبب الطبيعة العابرة للحدود للجرائم الإلكترونية تضطلع الهيئة بما يلي:

- السهر على تنفيذ طلبات المساعدة القضائية الدولية الصادرة عن الدول الأجنبية.
- تبادل المعلومات والخبرات مع الهيئات الدولية المماثلة، لتحديد هوية الجناة وتتبع الهجمات السيبرانية[1].

يظهر دور الهيئة في جريمة التجسس السيبراني من خلال صلاحياتها الممنوحة لها للتصدي لهذه الجريمة، بهدف الكشف المبكر عن التهديدات. غير أن هذه الصلاحيات تمارس وفق ضوابط قانونية، من بينها الحصول على إذن من الجهة القضائية المختصة في حالات خاصة مثل المراقبة الإلكترونية، وتنفيذها من طرف أعوان مؤهلين، مع احترام حدود استعمال المعطيات وعدم إفشائها[2].

ثانيا: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية

أنشئ هذا لمركز سنة 2008 ومقره في بئر مراد رايس، وهدفه تأمين الفضاء المعلوماتي الوطني. وتتمحور مهامه الأساسية حول تحليل الجرائم المرتكبة وتحديد مرتكبيها[3].

ويتولى تقديم المساعدة للمحققين باستخدام التكنولوجيا الحديثة لمعاينة الجرائم والمراقبة والبحث عن الأدلة، لا سيما في الجرائم التي تمس بالدولة مثل الإرهاب أو التجسس. كما يقوم بالرقابة الدائمة على شبكة الأنترنت، والمشاركة في عمليات التحري والتسرب بالتنسيق مع السلطات القضائية، بالإضافة إلى دوره في تبادل الخبرات الدولية لمواجهة هذه التحديات[4].

ثالثا: المعهد الوطني للأدلة الجنائية وعلم الإجرام التابع للدرك الوطني

---

[1]– المادة 04 من مرسوم رئاسي 21–439 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر.

[2]– عياشي عاشور، يعيش عبد الحق، المرجع السابق، ص 58.

[3]– سميحة بلقاسم، حميد بوشوشه، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر.. واقعها وآليات مجابهتها، مجلة العلوم الإنسانية، المجلد 10، العدد 01، جامعة أم البواقي، جوان 2023، ص551.

[4]– المرجع نفسه، ص 552.

أنشئ هذا المعهد بالمرسوم الرئاسي 04-183، وهو مؤسسة عمومية ذات طابع إداري تحت وصاية وزير الدفاع الوطني[1]، يتكفل بتقديم الدعم العلمي والتقني للجهات القضائية خلال مراحل التحري والتحقيق.

ويلعب هذا المعهد دوراً محورياً في مكافحة الجرائم السيبرانية من خلال دعم أجهزة التحقيق، عن طريق دائرة الإعلام الآلي المتواجدة فيه والتي تقوم بمعالجة وتحليل الأدلة الرقمية وإعداد الخبرات التقنية. كما يساهم في تعزيز اليقظة التكنولوجية لمواكبة تطور أساليب الجريمة وتحديث تقنيات الكشف عن هذه الجرائم[2].

رابعا: المصلحة المركزية لمكافحة جرائم تكنولوجيا الإعلام والاتصال

تم تأسيس هذه المصلحة من طرف المديرية العامة للأمن الوطني، لكن مع بدايتها في 2011 أنشأت على شكل فصيلة أمنية على مستوى المديرية لمواجهة الإجرام الإلكتروني، لتصبح فيما بعد مصلحة مركزية متصلة بمديرية الشرطة القضائية. وتتمتع هذه المصلحة بمهام عديدة تشمل تقديم الدعم التقني للمصالح القضائية، ومباشرة التحريات في الجرائم المعلوماتية ذات البعد الوطني أو الدولي، مع اليقظة الرقمية المستمرة لرصد المحتويات المخالفة للقانون. ويمتد هيكل المصلحة لشمل فرقاً متخصصة عبر ولايات الوطن مكلفة باستقبال الشكاوى والبحث والتحري تحت إشراف الجهات المختصة، كما يتكامل هذا الدور في التنسيق الدولي مع شرطة الإنتربول لتسهيل ملاحقة المجرمين وتبادل المعلومات[3].

خامسا: مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة

يشكل استحداث مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة خطوة عملية لحماية أسرار الدولة الحساسة من التهديدات السيبرانية؛ حيث تعد هذه المصلحة خطوة استراتيجية في مواجهة هذه التهديدات في المجال العسكري، وخاصة الهجمات ذات الطابع الإرهابي أو

---

[1]- المادة 02 من مرسوم رئاسي رقم 04-183 مؤرخ في 8 جمادى الأولى عام 1425 الموافق 26 يونيو سنة 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الأجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر العدد 41، الصادر في 9 جمادى الأولى عام 1425 الموافق 27 يونيو سنة 2004، ص 18.

[2]- سويسي فتيحة، التكييف القانوني لجرائم المعلوماتية والإشكالات العلمية المترتبة عنها، مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية بتاريخ 18 جانفي 2022، ص 17.

[3]- بارة سمير، الأمن السيبراني (cyber Security) في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن السيبراني، العدد 04، جامعة الحاج لخضر -باتنة-، جويلية 2017، ص272.

التجسسي، وتختص المصلحة بتخطيط ومتابعة تنفيذ سياسة ردعية شاملة تهدف إلى صد محاولات المساس بمنظومات أو منشآت الدولة الحساسة[1].

وتتمحور استراتيجيتها في الدفاع السيبراني على سبعة محاور تتمثل في؛ الجانب الوظيفي والتنظيمي لضمان سلسلة عمل موحدة في المنظومة العسكرية، بما يضمن توزيع المهام بسلاسة وسرعة الاستجابة للهجمات السيبراني؛ وتطوير ومراجعة الإطار التشريعي في هذا المجال؛ وكذلك تأهيل الجانب البشري لتكوين كفاءات ذات خبرة عالية؛ وتطوير الوسائل التقنية المستعملة في التصدي لهذه التهديدات. كما تولي المصلحة أهمية كبيرة للجانب الوقائي والتحسيسي لمستخدمي الجيش ضد مخاطر استعمال هذه التكنولوجيا بشكل خاطئ، وتعزيز التعاون مع جيوش الدول الشريكة من أجل الاستفادة من الخبرات التقنية المتقدمة[2].

سادسا: مركز الاستجابة لطوارئ الحاسوب (CERT ALGERIA)

هو فريق أمني مختص بتكنولوجيا المعلومات، يعمل تحت إشراف مركز البحث في الإعلام العلمي والتقني (CERIST). ويتخذ دور وقائي تقني لرصد التهديدات السيبرانية وتحليل الحوادث الرقمية والاستجابة لها في الوقت المناسب[3]؛ من خلال إصدار التنبيهات الأمنية، وتحليل البرمجيات الخبيثة وتفكيك شيفرات التسلل، وتقديم الدعم الفني للمؤسسات، والتنسيق بين الهيئات والمؤسسات الوطنية في حالة وجود هجوم أو مشكل أمني، فعند تعرض مؤسسة حكومية لمحاولة اختراق للتجسس يتدخل المركز تقنياً لوقف تسريب البيانات، وتحديد مصدر الهجمات وتوعية الجهات المعنية بكيفية غلق مسار الهجوم. كما تمتد فاعليته إلى الصعيد الدولي وذلك عبر التنسيق مع مختلف الهيئات العالمية والإقليمية، مثل (FIRST) و(AFRICACERT)، مما يعزز قدرة الجزائر في التصدي لمختلف التهديدات السيبرانية[4].

سابعا: منظومة أمن الأنظمة المعلوماتية

---

[1]– استحداث مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة، أكتوبر 2017، مقال منشور على موقع منتدى التكنولوجيا العسكرية والفضاء https://army-tech.net/، تاريخ الاطلاع 2026/04/24، على الساعة 17:27.

[2]– المرجع نفسه.

[3]– الفريق الجزائري للاستجابة لطوارئ الحاسوب، موقع مركز البحث في الإعلام العلمي والتقني، https://www.cerist.dz/، تاريخ الاطلاع2026/04/24، على الساعة 18:39.

[4]– أمحمد إسماعيل، زوبيري عبد الحليم، المرجع السابق، ص 28.

تشكل الهجمات السيبرانية المدعومة من طرف الدول، خاصة الموجهة لأغراض التجسس أو الاستعلام للحصول على معلومات حساسة، من أبرز التهديدات التي أصبحت تواجه الجزائر في المجال الرقمي. وهو ما دفع المشرع الجزائري إلى استحداث آلية جديدة تتمثل في المنظومة الوطنية لأمن الأنظمة المعلوماتية، الموضوعة تحت وصاية وزارة الدفاع الوطني، بهدف حماية الأنظمة المعلوماتية الوطنية[1].

تتكون هذه المنظومة من جهازين رئيسيين هما:

1. **المجلس الوطني لأمن الأنظمة المعلوماتية:** يعتبر الهيئة العليا في هذا المجال، حيث يرأسه وزير الدفاع الوطني أو ممثله، ويتولى المصادقة على الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من طرف الوكالة، والموافقة على توجهاتها العامة، إلى جانب إبداء رأيه بشأن مشاريع النصوص القانونية والتنظيمية المرتبطة بالمجال، والمصادقة على اتفاقيات التعاون الدولي ذات الصلة. واقتراح التدابير اللازمة لحماية البنى التحتية والأنظمة الحساسة، مع متابعة تنفيذ الاستراتيجية الوطنية وتقييم التهديدات الرقمية التي قد تمس أمن الدولة[2].
2. **وكالة أمن الأنظمة المعلوماتية:** هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية، وتعتبر الجهاز التنفيذي للمنظومة، إذ تضم مركز وطني ومديريات ومصالح متخصصة، وتشرف عليها لجنة توجيه ولجنة علمية، كما تعمل بالتنسيق مع مسؤولي أمن الأنظمة المعلوماتية في مختلف المؤسسات والهيئات[3].

وتتوزع مهامها بين إعداد الاستراتيجية الوطنية وتنسيق تنفيذها، وجمع وتحليل المعطيات المتعلقة بالتهديدات السيبرانية، وإجراء التحقيقات الرقمية عند وقوع الهجمات الإلكترونية، إضافة إلى اقتراح النصوص القانونية والتنظيمية المتعلقة بالمجال. كما تتولى مراقبة الثغرات الأمنية داخل الأنظمة المعلوماتية، وإصدار التنبيهات والإنذارات المبكرة عند

---

[1]– حزام فتيحة، الحماية المؤسساتية للأنظمة الرقمية في الفترة التشريعية الممتدة من 2009–2020، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد 13، العدد 01، جامعة حسيبة بن بوعلي –الشلف–، 2021، ص280

[2]– المادة 4 من مرسوم رئاسي رقم 20–05 مؤرخ في 24جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر العدد 04، الصادر في أولى جمادى الثانية عام 1441 الموافق 26 جانفي سنة 2020.

[3]– مقري صونيا، بن لعامر وليد، المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقاً للمرسوم الرئاسي رقم 20–05، مجلة البحوث في العقود وقانون الأعمال، المجلد 10، العدد 02، جامعة الأخوة منتوري –قسنطينة–، 2025، ص139.

رصد تهديدات محتملة، إلى جانب ضمان اليقظة التكنولوجية والأمنية وتعزيز التكوين والتوعية والتحسيس والبحث والتطوير في مجال الأمن السيبراني[1].

ثامنا: هيكل أمن الأنظمة

بما أن جل المؤسسات العمومية أصبحت تتخذ الأنظمة الرقمية داخل مرافقها، فإنها عرضة بالدرجة الأولى لمختلف الهجمات السيبرانية، خاصة فيما يتعلق بالوصول غير المشروع للبيانات للاطلاع عليها. وهنا تدخل المشرع الجزائري من خلال استحداث هيكل خاص داخل المؤسسات والإدارات العمومية يتولى مهمة تأمين البيانات وحماية الأنظمة، ويلزم على كل هذه الجهات إنشاء هيكل وتعيين له مسؤول مختص، مع إلحاقه مباشرة بالمسؤول الأول للمؤسسة[2]. وهذا التنظيم يساعد على أداء الهيكل لمهامه بموضوعية، خاصة فيما يتعلق بمراقبة مدى احترام قواعد الأمن.

وتتمثل مهامه في إعداد سياسة خاصة بأمن الأنظمة للجهة التابع لها والسهر على تطبيقها، بالإضافة إلى وضع تدابير للوقاية من المخاطر التي قد تتعرض لها البيانات. كما يعمل على متابعة الأمن المعلوماتي بشكل مستمر، والتنسيق مع مختلف المصالح، إلى جانب القيام بعمليات تحسيس لفائدة الموظفين للجهة التابع لها حول مخاطر الاستعمال غير الأمن للأنظمة[3].

ولهذا، يمكن اعتبار هذا الهيكل وسيلة جديدة تهدف إلى حماية المعطيات داخل الجهات التابعة للدولة، والمساهمة في الوقاية من الجرائم المعلوماتية وخاصة التجسس السيبراني.

الفرع الثاني: التدابير الوقائية

---

[1]– المادة 18 من مرسوم رئاسي رقم 20–05 يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، السالف الذكر.

[2]– المادة 2 من مرسوم رئاسي رقم 26–07 مؤرخ في 18 رجب عام 1447 الموافق 7 جانفي سنة 2026، يتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية، وتحديد مهامه وتنظيمه وسيره، ج ر العدد 04، الصادر في 29 رجب عام 1447 الموافق 18 جانفي سنة 2026.

[3]– المادة 4 من مرسوم رئاسي رقم 26–07 مؤرخ في 18 رجب عام 1447 الموافق 7 جانفي سنة 2026، يتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية، وتحديد مهامه وتنظيمه وسيره، السالف الذكر.

لا تقتصر الحماية من هذه الجرائم في وضع مؤسسات خاصة للوقاية منها ولا معاقبة مرتكبيها بعد حدوثها، بل يجب أيضا وضع تدابير احترازية هدفها الحد من العوامل التي تؤدي إلى ارتكاب هذه الجرائم وهي:

أولا: الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029

في إطار تبني استراتيجية وقائية واستباقية لمواجهة التهديدات السيبرانية، شرعت الجزائر في السنوات الأخيرة في إعداد الاستراتيجية الوطنية للأمن السيبراني للفترة 2025-2029، التي صادق عليها رسمياً رئيس الجمهورية في 30 ديسمبر 2025[1]، والتي تم تفعيلها رسمياً ضمن توجه الدولة نحو تعزيز السيادة الرقمية وحماية الأنظمة المعلوماتية الوطنية. وقد جاءت هذه الاستراتيجية نتيجة جملة من المعطيات، أبرزها مخرجات الملتقى الوطني للأمن السيبراني المنعقد في جوان 2023 تحت إشراف رئيس الجمهورية، إضافة إلى استغلال نتائج إحصاء الأنظمة المعلوماتية الوطنية والاستفادة من تجارب الدول الرائدة وتوصيات الاتحاد الدولي للاتصالات. وتشرف الوكالة الوطنية لأمن الأنظمة المعلوماتية على تنفيذ هذه الاستراتيجية التي تهدف إلى حماية البنى التحتية الحساسة وتعزيز قدرات الوقاية والكشف والاستجابة للحوادث السيبرانية، مع التركيز على بناء المورد البشري باعتباره العنصر الأساسي في الأمن السيبراني، وهو ما تجسد من خلال إنشاء مؤسسات تكوين متخصصة كالمدرسة العليا للأمن السيبراني والمدرسة العليا للذكاء الاصطناعي. كما تقوم هذه الاستراتيجية على تعزيز التعاون الوطني والدولي ودعم البحث والتطوير والابتكار في مجال الأمن السيبراني[2].

ثانيا: التوعية والتحسيس بمخاطر الجرائم المعلوماتية

أقرت الدولة الجزائرية عبر مؤسساتها المختصة، خاصة وزارة العدل ووزارة الرقمنة، أهمية التوعية الجماهيرية من خلال تنظيم حملات إعلامية تحسيسية موجهة لفئات المجتمع كافة، حول مخاطر استعمال الأنترنت بشكل خاطئ، وكيفية حماية البيانات الشخصية، ويعد

---

[1]- المادة 01 من مرسوم رئاسي رقم 25-321 مؤرخ في 10 رجب عام 1447 الموافق 30 ديسمبر سنة 2025، يتضمن المصادقة على الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية للفترة 2025-2029، ج ر العدد 87، الصادر في 10 رجب عام 1447 مؤرخ في 30 ديسمبر سنة 2025.

[2]- الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، منشورة في موقع وزارة الدفاع الوطني الجزائر، على الموقع https://www.mdn.dz/، تاريخ الاطلاع 2026/04/25، على الساعة 14:35.

هذا التوجه جزءاً من السياسية الوطنية للوقاية من الجريمة المكرسة في الاستراتيجية العامة للوقاية من الجرائم المعلوماتية [1].

ثالثا: حوكمة البيانات كآلية وقائية للحد من التجسس السيبراني

تندرج حوكمة البيانات ضمن الآليات الوقائية الحديثة التي اعتمدها المشرع الجزائري في إطار تعزيز أمن المعلومات، والحد من مخاطر التهديدات السيبرانية. وتقوم هذه الحوكمة على وضع إطار تنظيمي شامل يضبط مختلف مراحل التعامل مع البيانات، بدءاً من جمعها ومعالجتها وصولاً إلى تخزينها وتبادلها بين الهيئات، بما يضمن التحكم فيها بشكل دقيق[2].

ويترتب على هذا الإطار فرض التزامات على كل المؤسسات التابعة للدولة للقيام بما جاء في أحكام هذه الاستراتيجية في أجال محددة، من تصنيف بياناتها وفهرسة مصادرها، والتصنيف يكون بحسب درجة خطورة البيانات، من درجة عامة إلى سرية وسرية للغاية، وهذا التصنيف هو الخطوة الأولى لمكافحة التجسس، لأنه يسمح للمؤسسات بتركيز مواردها الدفاعية على البيانات التي تكون هدفاً للجواسيس، بدلاً من تشتيت الجهود على بيانات غير مهمة. كما تساهم في تعزيز التنسيق بين مختلف الهيئات، وتوحيد أساليب التعامل مع البيانات[3].

وتتداخل هذه الحوكمة مع منظومة أمن الأنظمة، بحيث يتولى المجلس الوطني لأمن الأنظمة البت في مسائلها، وتبت الوكالة في إطار مهامها في تصنيف مستوى أمن البيانات، ومراقبة تطبيق معايير الحماية داخل المؤسسات[4].

رابعا: الالتزامات المفروضة على عاتق مقدمي الخدمات

---

[1]– بلعباس أحمد، بلعباس محمد نذير، الوقاية من الجرائم المعلوماتية في القانون، مذكرة ضمن متطلبات نيل شهادة الماستر في القانون، تخصص قانون جنائي، قسم العام، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور بالجلفة، 2025/2024، ص 40.

[2]– المادة 2 من مرسوم رئاسي رقم 25–320 مؤرخ في 10 رجب عام 1447 الموافق 30 ديسمبر سنة 2025، يتضمن وضع منظومة وطنية لحوكمة البيانات، ج ر العدد 87، الصادرة في 10 رجب عام 1447 الموافق 30 ديسمبر لسنة 2025.

[3]– وضع المنظومة الوطنية لحوكمة البيانات حيز الخدمة ركيزة أساسية لبناء دولة عصرية، فيفري 2026، مقال منشور على الموقع https://www.aps.dz/، تاريخ الاطلاع 2026/04/25، على الساعة 17:48.

[4]– المادة 14 و16 من مرسوم رئاسي رقم 25–320 يتضمن وضع منظومة وطنية لحوكمة البيانات، السالف الذكر.

مزودي الخدمة مثل اتصالات الجزائر فرض عليهم المشرع الجزائري مجموعة من الالتزامات في إطار الوقاية، وتتمثل هذه الالتزامات في:

التعاون مع السلطات المختصة في إطار مكافحة الجرائم المعلوماتية، وذلك عبر الاحتفاظ بالبيانات التقنية الضرورية لتتبع الاتصالات وتحديد أصحابها. وتشمل هذه البيانات المعلومات الكفيلة بالتعرف على هوية المستخدمين، والمعطيات المتعلقة بالأجهزة المستخدمة، وخصائص الاتصالات من حيث التوقيت والمدة والطبيعة التقنية، إضافة إلى البيانات المرتبطة بالخدمات والجهات المستفيدة منها، فضلاً عن المعلومات التي تسمح بتحديد الأطراف المتصلة والمواقع الإلكترونية التي تمت زيارتها. كما ألزم متعاملي الهاتف بحفظ البيانات التي تتيح تحديد مصدر الاتصال ومساره، على أن تبقى هذه المعطيات محفوظة لمدة سنة كاملة ابتداءً من تاريخ تسجيلها، وأن يحتفظ مزودي الخدمة بسرية المعلومات عن المستخدمين وعدم إفشائها للغير إلا فيما ينص عليه القانون[1].

ومن أجل ضمان فعالية هذا الالتزام، أقام المشرع الجزائري مسؤولية جزائية في حالة الإخلال بهذه الالتزامات متى ترتب عن ذلك عرقلة التحريات القضائية، حيث أخضع الأشخاص الطبيعيين لعقوبات سالبة للحرية وغرامات مالية، في حين تطبق على الأشخاص المعنويين عقوبات مالية[2].

فرض كذلك المشرع الجزائري على مقدمي خدمات الإنترنت الالتزام بنفس التعليمات المفروضة على مقدمي الخدمات، واتخاذ تدابير تقنية عاجلة تتمثل في إزالة أو تعطيل الوصول إلى المحتويات المخالفة للقانون فور العلم بها. ويعكس هذا التوجه رغبة المشرع الجزائري في تدعيم الرقابة الرقمية وتعزيز آليات التتبع الإلكتروني[3].

الفرع الثالث: التدابير التقنية لحماية الأنظمة المعلوماتية من التجسس السيبراني

في ظل تطور أساليب التجسس السيبراني، أصبحت التدابير التقنية تمثل خط الدفاع الأساسي لحماية الأنظمة المعلوماتية من الحصول غير المشروع للمعلومات. وتقوم هذه التدابير على مجموعة من الوسائل التقنية والبرمجية التي تهدف إلى تأمين الشبكات

---

[1]– المواد 10 و11 من قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف الذكر.

[2]– المادة 11 من قانون 09-04 السالف الذكر.

[3]– المادة 12 من قانون 09-04 السالف الذكر.

والمعلومات، ومراقبة الأنشطة المشبوهة، بما يحد من قدرة الجهات المعادية على المساس بالأنظمة المعلوماتية.

أولاً: تقنيات تأمين الاتصالات وحماية البيانات

من أبرز التقنيات الحديثة لحماية البيانات والاتصالات أثناء تداولها بين الشبكات هي

1. التشفير المعلوماتي

يعتبر التشفير من أهم الوسائل التقنية المستعملة لحماية المعلومات من التجسس السيبراني، إذ يقوم على تحويل البيانات إلى رموز وإشارات غير مفهومة لا يمكن الاطلاع عليها إلا من قبل الأشخاص المصرح لهم. ويساهم هذا التشفير في حماية سرية البيانات ومنع اعتراضها أثناء التخزين أو النقل عبر الشبكات[1].

وينقسم التشفير إلى نوعين:

أ. التشفير المتماثل: يعتمد على استعمال مفتاح سري واحد في عملية التشفير وفك التشفير، غير أن فعاليته تبقى مرتبطة بمدى أمن عملية تبادل المفتاح بين الأطراف .

ب. التشفير اللامتماثل: يقوم على استخدام مفتاحين مختلفين، أحدهما عام والآخر خاص، بما يسمح بتأمين الاتصالات الإلكترونية وتقليل مخاطر اعتراض المفاتيح السرية[2]

2. بروتوكولات تأمين الاتصالات

تستخدم مجموعة من البروتوكولات التقنية لتأمين نقل البيانات عبر الشبكات والحد من عمليات التجسس أو اعتراض المعلومات، ومن أهمها:

أ. بروتوكولTLS : يضمن تشفير البيانات المتبادلة بين المستخدم والخادم، يقوم بإنشاء مصافحة أولية بين الطرفين للتفاوض على الخوارزميات، ثم يقوم بإنشاء مفتاح مشترك، بما يحافظ على سرية الاتصالات الإلكترونية[3].

ب. بروتوكولIPSEC : يوفر حماية على مستوى الشبكات ويستعمل خاصة في تأمين الشبكات الافتراضية الخاصة[4].

---

[1]– فتيحة خالدي، المرجع السابق، ص 311.

[2]– المرجع نفسه، ص 331.

[3]– أمحمد إسماعيل، زوبيري عبد الحليم، المرجع السابق، ص 71.

[4]– المرجع نفسه، ص 72.

ت. بروتوكولSSH : يسمح بإدارة الخوادم عن بعد عبر قناة اتصال مشفرة وآمنة [1].

ث. بروتوكولDNSSEC : يهدف إلى حماية نظام أسماء النطاقات من عمليات الاختراق[2]

3. حماية الشبكات السلكية واللاسلكية

تشمل حماية الشبكات اللاسلكية الداخلية مجموعة من التدابير التقنية التي تهدف إلى الحد من الوصول غير المشروع، من بينها تقييد الأجهزة المصرح لها بالاتصال عبر تقنية عنوانMAC ADDRESS ، هذه التقنية تحمل أرقاماً لا تتكرر أبداً ويستطيع المسؤول عن الشبكة من خلالها تحديد عدد الأجهزة المصرح لها بالاتصال واستخدام الشبكة[3].

ثانيا: أنظمة المراقبة والدفاع عن الشبكات

تعتمد الجهات المختصة في مراقبة الأنظمة على وسائل تقنية متطورة لمراقبة حركة الشبكات، والكشف المبكر عن كل محاولات المساس بالنظام عن طريق:

1. الجدران النارية

تمثل الجدران النارية خط الدفاع الأول ضد محاولات الدخول أو أي مساس بالأنظمة، حيث تعمل على مراقبة حركة البيانات الواردة والصادرة والتحكم في الاتصالات غير المصرح بها وفق قواعد أمنية محددة[4].

2. أنظمة كشف ومنع التسلل (IDS\IPS)

تساهم هذه الأنظمة في رصد الأنشطة غير الطبيعية ومحاولات الولوج داخل الشبكات، كما تسمح باتخاذ إجراءات تلقائية لمنع الهجمات السيبرانية والتقليل من آثارها، وفي حال كشف أي تسلل للأنظمة يقوم هذا النظام بإنذار فوري مما يسمح التصدي المبكر لكل الهجمات[5].

2. أنظمة إدارة الأحداث الأمنيةSIEM

---

[1]– عبد السلام أحمد، بروتوكولات الأمان في شبكان الأنترنت، الطبعة الثانية، دار الأشجار للنشر، الأردن، 2018، ص 78.

[2]– أمحمد إسماعيل، زوبيري عبد الحليم، المرجع السابق، ص 71–73.

[3]– سامية بوشوشة، حياة سلماني، المرجع السابق، ص 66.

[4]– أمحمد إسماعيل، زوبيري عبد الحليم، المرجع السابق، ص 73.

[5]– خالد علي نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، مجلة البحوث القانونية والاقتصادية، مجلد 2022، عدد 79، جامعة المنصورة، لسنة 2022، ص 38.

تقوم هذه الأنظمة بجمع وتحليل السجلات الأمنية الصادرة عن مختلف الأجهزة والخوادم، بما يسمح بالكشف المبكر عن الأنشطة المشبوهة المرتبطة بالتجسس السيبراني[1].

ثالثا: البرمجيات المتخصصة في مكافحة التجسس السيبراني

هدف هذه البرمجيات هو التصدي لكل محاولات التجسس السيبراني على الأنظمة المعلوماتية، تتمثل هذه البرمجيات في:

1. برامج مكافحة التجسس

استخدام برامج مكافحة التجسس مثل spyware blaster الذي لا يقتصر دوره فقط القضاء على التجسس بل يقوم بدور المراقب لمنع أية ملفات من اقتحام الجهاز أو الشبكة ومراقبة الأنشطة غير الطبيعة[2].

2. أنظمة منع تسرب البيانات والشبكات الافتراضية الخاصة

تساهم أنظمة منع فقدان البيانات DLP في مراقبة تداول المعلومات الحساسة ومنع تسريبها خارج الشبكة، في حين توفر الشبكات الافتراضية الخاصة VPN اتصالاً مشفراً يحد من مخاطر اعتراض البيانات أثناء الاتصال بالإنترنت[3]

المطلب الثاني

المكافحة الإجرائية لجريمة التجسس السيبراني

يستلزم التصدي لجريمة التجسس السيبراني اعتماد منظومة متكاملة لا تقتصر على التجريم والوقاية فقط، بل تمتد إلى وضع مختلف الآليات القانونية التي تسمح بكشف هذه الجريمة والتحري عنها ومتابعة مرتكبيها أمام القضاء. لذلك أحاط المشرع هذا النوع من الجرائم بمجموعة من الإجراءات الخاصة التي تتماشى مع طبيعتها التقنية، وتبدأ من إجراءات البحث والتحري وجمع الأدلة الرقمية، مروراً إلى الجهة القضائية المختصة بها، وصولًا إلى تقرير الجزاءات المناسبة لمرتكب هذه الجريمة. ويهدف هذا التنظيم إلى ضمان فعالية المتابعة القضائية وتحقيق الردع في مواجهة هذا النمط المستحدث من الإجرام.

---

[1]– أمحمد إسماعيل، زوبيري عبد الحليم، المرجع السابق، ص 74.

[2]– سامية بوشوشة، المرجع السابق، ص 66.

[3]– أمحمد إسماعيل، زوبيري عبد الحليم، المرجع السابق، ص 75.

في هذا السياق، يتجه هذا المطلب لتبيان إجراءات البحث والتحري في (الفرع الأول)، والاختصاص القضائي والجزاءات المقررة لهذه الجريمة في (الفرع الثاني).

الفرع الأول: الآليات الإجرائية للكشف عن جريمة التجسس السيبراني

تفرض جريمة التجسس السيبراني خصوصية إجرائية عند ملاحقة مرتكبيها، وذلك بسبب طبيعتها الرقمية المعقدة وصعوبة الكشف عن أدلتها الرقمية، مما استدعى اعتماد إجراءات بحث وتحقيق تتلاءم مع طبيعتها الخاصة. وقد نظم المشرع هذه الإجراءات ضمن قانون 09-04 وقانون الإجراءات الجزائية.

أولا: الإجراءات المستحدثة ضمن قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال

استحدث المشرع بموجب هذا القانون مجموعة من الإجراءات الخاصة التي تهدف إلى الكشف عن الجرائم المعلوماتية وجمع الأدلة الرقمية. وتتجسد هذه الإجراءات في

1. المراقبة الإلكترونية

تشكل المراقبة الإلكترونية إحدى أهم الوسائل التي اعتمدها المشرع الجزائري لمواجهة الجرائم الإلكترونية، لاسيما التجسس السيبراني أو أي جريمة تمس بأمن الدولة، ويقوم بها ضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها بإذن من النائب العام لدى مجلس قضاء الجزائر، بمتابعة الاتصالات والبيانات المتبادلة عبر الأنظمة والشبكات المعلوماتية، مع إمكانية جمعها وتسجيلها باستعمال وسائل تقنية مخصصة لذلك. غير أن المشرع أحاط هذا الإجراء بجملة من الضمانات، من خلال اشتراط إذن مسبق، مع ضرورة احترام حدود الغرض الذي أذن من أجله حفاظاً على الحياة الخاصة للأفراد[1].

2. التفتيش

[1]- المادة 04 من قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف الذكر.

يبرز التفتيش كإجراء محوري يهدف إلى البحث والكشف عن الأدلة الرقمية في البيئة الافتراضية، وهو إجراء يمس بحرية وحرمة الأخرين، ولهذا قام المشرع بتنظيمه، ووضع شروط لصحته وتوكيل القيام به إلى أشخاص محددين قانوناً[1].

خول القانون صلاحية القيام بهذا الإجراء إلى السلطات القضائية المختصة وضباط الشرطة القضائية، وكذا الاستعانة بالأشخاص ذوي الخبرة في المجال لمساعدتهم في القيام به[2].

1. نطاق التفتيش

يمتد إجراء التفتيش ولو عن بعد الولوج إلى الأنظمة المعلوماتية وما تحتويه من بيانات ومعطيات إلكترونية مخزنة فيها، وقد يمتد إلى الحواسيب والأجهزة المرتبطة بالشبكة والأقراص الصلبة والخوادم، بل وحتى الأنظمة المرتبطة بالمنظومة الرئيسية محل التفتيش متى وجدت مؤشرات على اتصالها بالجريمة، وذلك بعد إعلام السلطة القضائية المختصة[3].

2. شروط التفتيش

يشترط لصحة التفتيش من الناحية القانونية توافر:

- **ضرورة توفر سبب للتفتيش**

يقع التفتيش على جريمة قد وقعت فعلاً وتشكل فعل غير مشروع، أو قد يكون إجراء وقائي يسبق الجريمة في حالة شك أن جريمة تجسس ستحدث. وأن يكون هناك شخص توجه له التهمة، بسبب ارتكابه الجريمة، أو وجود ما يدعو الظن بارتكابها، وإذا لم يتوفر شخص توجه له التهمة يرفع ضد مجهول لحين اكتشاف الفاعل. كما يشترط توفر دلائل ترجح ارتباط الوسائل أو الأنظمة المعلوماتية المراد تفتيشها بالجريمة محل التحقيق[4].

---

[1]– إدريس قرفي، تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية: بين اتفاقية بودابست والتشريع الجزائري، مجلة الحقوق والحريات، المجلد 02، العدد 02، جامعة محمد خيضر بسكرة، 2014، ص100.

[2]– المادة 05 من قانون 09-04 السالف الذكر.

[3]– يعيش تمام شوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، الطبعة الأولى، مطبعة الرمال (الوادي) للنشر، الجزائر، 2019، ص 66.

[4]– صغير يوسف، التفتيش كآلية لإثبات جرائم نظم المعلوماتية، المجلة النقدية للقانون والعلوم السياسية، المجلد 16، العدد 04، جامعة تيزي وزو، سنة 2021، ص 603.

- **ضوابط مباشرة التفتيش**

يشترط لمباشرة التفتيش في الجرائم السيبرانية صدور إذن قضائي مسبق عن الجهة المختصة، باعتباره الضمانة الأساسية لمشروعية هذا الإجراء. غير أن المشرع، مراعاةً لخصوصية هذه الجرائم، أجاز تنفيذه في أي وقت ليلاً أو نهاراً وفي أي مكان خاص أو عام متى اقتضت ضرورة التحري ذلك، مع منح قاضي التحقيق صلاحية الأمر به عبر كامل التراب الوطني واتخاذ التدابير التحفظية اللازمة. كما خفف من القواعد الشكلية للتفتيش، إذ لا يشترط حضور المعني أو ممثله أو شاهد أثناء القيام به في جرائم تكنولوجيا الإعلام والاتصال[1].

- **التفتيش في المسائل ذات البعد الدولي**

في حال كانت المنظومة المعلوماتية موضوع التفتيش تقع خارج الإطار الإقليمي للجزائر، فإن التفتيش يجرى بالتنسيق مع السلطات الأجنبية المختصة، وفقاً للاتفاقيات الدولية ذات الصلة أو مبدأ المعاملة بالمثل. وهذا بسبب الطبيعة العابرة للحدود للجرائم المعلوماتية[2].

3. الحجز المعلوماتي

يعتبر الحجز المعلوماتي إجراء لاحق للتفتيش، فبعد قيام السلطات المختصة بالتفتيش وإيجاد معلومات تدخل في إطار الجريمة أو كيفية ارتكابها، يتعين حفظها في مكان آمن للرجوع إليها واستعمالها كدليل. ويخول للجهات المختصة ضبط ومصادرة كل ما له علاقة بالجريمة أو يساعد في إثبات مرتكبيها لاحقاً. لكشف الجريمة ومنع إتلاف الدليل، ولا يقتصر على الأجهزة المادية كالحواسيب أو الأقراص، بل يمتد ليشمل أيضاً الأنظمة المعلوماتية[3].

ولا يشترط حجز كل المنظومة المعلوماتية، بل يمكن نسخ المعطيات المفيدة واللازمة في دعامة تخزين إلكترونية أخرى كالأقراص الصلبة أو الحواسيب. كما نص المشرع على

---

[1]– المواد 75و76 و78 من قانون رقم 25–14 يتضمن قانون الإجراءات الجزائية، السالف الذكر.

[2]– المادة 05 من قانون 09–04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف الذكر.

[3]– يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، عدد 48، جامعة باجي مختار عنابة، ديسمبر 2016، ص 90.

ضرورة حماية المعطيات محل الحجز من التلف أو الضياع، فيجب على السلطة المختصة الحفاظ على سلامة المعطيات داخل المنظومة المعلوماتية بكل الوسائل[1].

وفقاً للمادة 07 إذا تعذر القيام بعملية الحجز لأسباب مختلفة أو تقنية مثل وجود أنظمة حماية عالية في النظام، فإنه يجب على السلطات اللجوء إلى الحجز عن طريق منع الوصول إلى تلك المعلومات بأي وسيلة تقنية كانت، بحيث يتم تقييد وصول المجرم إلى المعلومات فلا يمكن لأي أحد الوصول إليها وحتى الأشخاص الذين لهم الحق في الدخول إليها وذلك لتفادي تعديلها أو محوها أو إتلافها[2].

ثانيا: الإجراءات المنصوص عليها في قانون الإجراءات الجزائية

تطبق أيضا في مجال الجرائم الإلكترونية أحكام قانون الإجراءات الجزائية باعتباره الإطار العام الذي ينظم إجراءات البحث والتحري وجمع الأدلة، وتقسم هذه الإجراءات إلى إجراءات كلاسيكية عامة، وأخرى استثنائية نص عليها القانون ويلجأ إليها في الجرائم الخطيرة.

1. المعاينة

تعتبر المعاينة إجراء مهم جداً في البحث والتحري عن الجرائم، سواء التقليدية أو الرقمية، فتهدف إلى التحقق المباشر من وقوع الجريمة وتحديد آثارها وتقييم أضرارها. ونظراً للطبيعة الافتراضية وغير المادية للأدلة المعلوماتية وسرعة تعرضها للمحو أو التعديل، فإن هذه العملية لا تقتصر على الانتقال المادي إلى مسرح الجريمة التقليدي، بل تمتد لتشمل المعاينة الرقمية للأنظمة، والشبكات، والخوادم المستهدفة أو التي كانت وسيلة للتنفيذ، وتجرى عادة في المراحل المبكرة للتحقيق وتسبق عمليات التفتيش الإلكتروني والحجز الرقمي لضمان الحفاظ على الحالة الأولية للنظام[3]. وفي ظل التشريع الجزائري كرس المشرع منظومة إجرائية خاصة أسند بموجبها صلاحية المعاينة لجهات متخصصة تمتلك الكفاءة

---

[1]– المادة 06 من قانون 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف الذكر.

[2]– المادة 07 من قانون 09-04 السالف الذكر.

[3]– بوفروك هند، سعيود بشرى، إجراءات المعاينة، التفتيش، والحجز داخل المنظومة المعلوماتية، مذكرة مكملة لنيل شهادة الماستر تخصص القانون الجنائي والعلوم الجنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 سكيكدة، 2025، ص 39.

التقنية، من ضباط الشرطة القضائية تحت إشراف وكيل الجمهورية أو قاضي التحقيق، وبدعم من الهيئات الوطنية المتخصصة[1]، مع إمكانية الاستعانة بالخبراء والتقنيين في الإعلام الآلي لتفكيك الأنظمة المعقدة أو البيانات المشفرة أو في حالة إجراء معاينة استعجالية لا يمكن تأخيرها[2].

ينصب موضوع المعاينة على فحص الحواسيب والشبكات والأقراص الصلبة، لمحاولة إيجاد أي دليل يكشف الفاعل أو يدينه وذلك عبر الأثار والبصمات الإلكترونية التي يتركها المستخدم كالرسائل الصادرة والواردة، تصفح المواقع والملفات المحمولة، وتتميز المعاينة الإلكترونية بمرونتها إذ لا ترتبط بالانتقال المادي بل يمكن القيام بها بعدة طرق سواء من مقر الشرطة القضائية عبر الحواسيب الموجودة هناك، أو الحاسوب الشخصي لضابط الشرطة القضائية، أو مقاهي الإنترنت أو عبر مزودي الخدمة[3].

2. الخبرة الفنية

خول القانون للجهات المختصة الاستعانة بخبير فني كلما اقتضت الحاجة إلى ذلك[4]، وهذا الخبير في إطار الصلاحيات الممنوحة له يقوم بإعداد خبرة فنية، والتي هي وسيلة شبه ضرورية في التحقيق في الجرائم المعلوماتية، وذلك بسبب الطبيعة المعقدة لهذه الجرائم والتي لا يمكن لغير الخبير تحليلها. لذلك يستعان بخبير أمن المعلومات أو خبير في الأدلة الجنائية الرقمية لتحديد مصدر الهجوم، وتحليل الأجهزة والشبكات والخوادم لفهم طريقة التجسس وطبيعة البرامج المستخدمة. ويقوم بإعداد تقرير مفصل حول ما قام به وما وجده ليساهم في تكوين قناعة القاضي. وكذلك يضمن الخبير حسب خبرته سلامة الدليل الرقمي من أي شيء قد يضره أو يمس به[5].

---

[1]– قلات سومية، حاحة عبد العالي، مقتضيات المعاينة المعلوماتية في التشريع الجزائري، مجلة الحقوق والحريات، المجلد 11، العدد 1، جامعة محمد خيضر –بسكرة–، السنة 2023، ص 524.

[2]– المادة 81 من قانون رقم 25–14 يتضمن قانون الإجراءات الجزائية، السالف الذكر.

[3]– عياشي عاشور، يعيش عبد الحق، المرجع السابق، ص 73.

[4]– المادة 239 من قانون رقم 25–14 يتضمن قانون الإجراءات الجزائية، السالف الذكر.

[5]– صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجيستر في القانون، تخصص القانون الدولي للأعمال، مدرسة الدكتوراه "القانون الأساسي والعلوم السياسية"، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013، ص 89–90

والخبير يجب أن يكون شخص يضطلع بعدة أمور في هذا المجال، من التحكم في الأجهزة والحواسيب والمعرفة الكافية التي تخول له التصرف فيها بطريقة صحيحة، دون أن يقوم بأي ضرر يمس الأجهزة أو يدمر الدليل[1].

ولتكون الخبرة لها حجيتها القانونية لابد للخبير أن يتبع مجموعة من الواجبات بداية من حلف اليمين في حال كان أول مرة يقيد في جدول الخبراء لضمان نزاهته، وإنجاز الخبرة الموكلة إليه بنفسه والقيام بكل ما يلزم به القانون، وأن يبقى في الفترة المنتدب فيها تحت الرقابة القضائية للجهة القضائية المسؤولة عن انتدابه وذلك لإحاطتها بكافة التطورات في الأعمال التي يقوم بها، ويجب أن يحترم فترة الخبرة التي يحددها القانون وأن يقدمها في الوقت المناسب، وتتضمن هذه الخبرة كل ما توصل إليه بالتفصيل[2].

ومن أهم الخبراء في مجال القيام بالخبرة هو المعهد الوطني للأدلة الجنائية وعلم الإجرام بالجزائر، بحيث يساعد هذا المعهد في تقديم المساعدة في القضايا الرقمية المعقدة من خلال أجهزته الداخلية الملمة بجميع المعلومات اللازمة في التعامل مع الدليل الإلكتروني، ومحاولة الوصول إليه[3].

3. التسرب الإلكتروني

التسرب الإلكتروني هو تقنية حديثة تسمح لضباط وأعوان الشرطة القضائية التوغل إلى مجموعات إجرامية بعد التنسيق والتحضير المسبق بين السلطات الخاصة، بهدف مراقبة أشخاص مشتبه فيهم والتوغل بينهم لكشف أنشطتهم الإجرامية، وإيهامهم أن المتسرب شريك أو فاعل معهم[4]. وتعد هذه التقنية من أخطر الإجراءات التي تقوم بها الشرطة القضائية للكشف عن الجرائم الخطيرة، بسبب أن المتسرب يحتك احتكاك مباشر مع المشتبه فيهم، مما يعرض حياته وحياة عائلته للخطر في حال كشف هويته.

---

[1]– صغير يوسف، المرجع السابق، ص 91.

[2]– عماد يوسف، لزهر ضربان، إجراءات التحري في الجرائم الإلكترونية، مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر، تخصص قانون قضائي مهني، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، 2023/2022، ص 48.

[3]– بن علال بومدين، التحقيق الجنائي في الجرائم الناشئة عن المعاملات الإلكترونية في ضوء التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماستر في القانون العام، قسم الحقوق، معهد الحقوق والعلوم السياسية، المركز الجامعي مغنية، 2021/2020، ص 46.

[4]– المادة 121 من قانون رقم 25–14 يتضمن قانون الإجراءات الجزائية، السالف الذكر.

أ. أنواع التسرب

بسبب التطور الحاصل في عالم الإجرام والجريمة، لم تعد ترتكب الجرائم بوسائل تقليدية، مما جعل التسرب التقليدي المعروف من قبل لم يعد كافياً للتصدي لهذه الأفعال مما أوجب أن يقوم المشرع باستحداث نوع جديد من التسرب، ولذلك هناك نوعين من التسرب:

- **التسرب التقليدي:** وهو قيام المتسرب بعملية التسرب بطريقة ميدانية، أين يتوغل في الجماعات الإجرامية شخصياً في أماكنهم، بحيث يستطيع أن يعيش معهم وأن يتنقل معهم وإلى غير ذلك، فالتسرب التقليدي هو استعمال طرق معروفة لدخول بين المشتبه فيهم[1].
- **التسرب الإلكتروني:** استحدث المشرع الجزائري هذا الإجراء في قانون 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية، والقانون 20-15 المتعلق بالوقاية من جرائم اختطاف الأشخاص ومكافحتها، بحيث نص على أن هذا الإجراء يكون ضمن هذه الجرائم فقط، وهو ما يترك تساؤل حول إمكانية تطبيق هذا الإجراء في جرائم أخرى مثل التجسس السيبراني. لكن بالرجوع إلى القواعد العامة في ق.إ.ج. وتحديداً الجرائم التي يجوز فيها اللجوء إلى التسرب المادي، نجد من بينها جرائم تكنولوجيا الإعلام والاتصال؛ ونظراً للطبيعة الرقمية لهذه الجرائم، فإنه من غير الممكن منطقياً معاينتها أو اختراقها ميدانياً وجهاً لوجه، مما يستوجب حتماً إعمال آلية التسرب بالوسائل والتقنيات الرقمية كأداة ضرورية لكشف هذه الجرائم والتصدي لها[2].

ويحاط بجملة من الحماية القانونية من إعفاء من المسؤولية الجزائية عن الأفعال التي يقوم بها تنفيذاً لعملية التسرب، فيقوم المتسرب بمساعدة الجماعة التي توغل فيها بكافة الطرق ليثبت لهم أنه واحداً منهم فيقوم بأي فعل ضروري لمساعدتهم من أموال أو ملفات أو وسائل تقنية...إلخ[3].

بسبب الخطورة العالية التي يشكلها هذا الإجراء على حياة ضابط الشرطة القضائية، ألزم القانون له عدة شروط يجب التقيد بها أو اعتبر إجراء باطل.

---

[1]- راوية مطماطي، نبيل بن عديدة، عملية التسرب على ضوء قانون الإجراءات الجزائية 25-14، مجلة حقوق الإنسان والحريات العامة، المجلد 10، العدد 02، -جامعة مستغانم-، سنة 2025، ص 402.

[2]- سارة قريمس، التسرب الإلكتروني كآلية إجرائية مستحدثة للتحري والتحقيق الجنائي الرقمي على ضوء التشريع الجزائري، مجلة الفكر القانوني والسياسي، المجلد التاسع، العدد الثاني، جامعة عمار ثليجي -الأغواط-، 2025، ص1243.

[3]- المادة 123 من قانون رقم 25-14، يتضمن قانون الإجراءات الجزائية، السالف الذكر.

بداية يجب أن يحرر المتسرب تقرير مسبق يتضمن جميع المعلومات التي تخص العملية من ذكر الجريمة التي بسببها سيقام التسرب وصفة من سيقوم به. والإذن بمباشرة عملية التسرب من السلطات المختصة مع تبرير اللجوء إلى هذه العملية، وذكر مدة العملية وهي 4 أشهر قابلة للتجديد عن اللزوم ولا يجوز كشف هوية المتسرب ويعاقب بعقوبات صارمة كل من كشف هوية المتسرب وتسبب بأذى له أو لعائلته[1].

4. اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

تعتبر هذه الإجراءات انتهاكات صارخة لحرمة الحياة الخاصة للأشخاص والتي كفلها الدستور لكل فرد، إلا أنه ولمقتضيات خاصة أدرجها المشرع ضمن إجراءات البحث والتحري والتحقيق كإجراءات مستحدثة في بعض الجرائم الخطيرة.

أ. اعتراض المراسلات

يعتبر هذا الإجراء وسيلة استثنائية تتسم بالطابع السري، تستخدم خلال مراحل البحث أو التحري أو التحقيق الابتدائي، ولا يسمح باللجوء إليها إلا في نطاق الجرائم الخطيرة التي يحددها القانون. ويقوم هذا التدبير على مراقبة اتصالات شخص أو مجموعة يشتبه في ارتكابهم نشاط إجرامي، فيتم الاطلاع على محتوى التواصل بينهم دون إعلامهم أو الحصول على موافقتهم، بهدف استخراج الأدلة. وتشمل هذه العملية جميع أشكال المراسلات دون استثناء، سواء تعلق الأمر بالرسائل البريدية التقليدية أو الاتصالات الهاتفية أو الرسائل النصية أو البريد الإلكتروني[2].

ب. تسجيل الأصوات

يتمثل هذا الإجراء في عملية تقنية تهدف إلى التقاط الأصوات بكل خصائصها الصوتية، بما في ذلك نبرة المتكلم وعيوب النطق، ثم تحويلها إلى إشارات مخزنة على وسائط تسجيل تسمح بالرجوع إليها لاحقًا وسماع محتواها. ويمكن تطبيق هذا الإجراء في مختلف الفضاءات سواء كانت خاصة أو عمومية. ويتم الاعتماد في ذلك على أجهزة متطورة للتسجيل، من بينها أجهزة تعتمد على الربط السلكي أو اللاسلكي حيث تخفى داخل المكان المستهدف وتوصل

---

[1]– المواد 120، 122، 124، 125 من قانون رقم 25–14، يتضمن قانون الإجراءات الجزائية، السالف الذكر.

[2]– لبنى عبد الكريم، مطبوعة بيداغوجية في مقياس قانون الإجراءات الجزائية المعمق، محاضرات موجهة لطلبة السنة الأولى ماستر تخصص قانون جنائي وعلوم جنائية، السداسي الأول، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي –جيجل–، 2026/2025، ص 36.

بجهاز استقبال خارجي، إضافة إلى أجهزة تستعمل من داخل الموقع المطلوب عبر حملها أو تثبيتها بشكل غير ظاهر، وأخرى تستخدم من خارج المكان وتتيح التقاط المحادثات حتى داخل الفضاءات المغلقة دون الحاجة إلى الولوج إليها[1].

ت. التقاط الصور

يقوم هذا الإجراء على توظيف وسائل تقنية حديثة تسمح بتصوير الأشخاص المشتبه فيهم، بغرض توثيق وقائع أو سلوكيات ذات صلة بالتحقيق. ويشمل التصوير عدة صور، أبرزها التصوير الثابت الذي يعتمد على التقاط صورة واحدة بواسطة آلة تصوير لتثبيت المعلومة، إضافة إلى التصوير السمعي البصري الذي يقوم على تسجيل مشاهد متحركة مصحوبة بالصوت، بما يتيح إعادة تحليلها لاحقًا من طرف الجهات المختصة واستخلاص كل ما قد يفيد في إثبات الجريمة[2].

ج. الإطار القانوني لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور

تعتبر هذه الإجراءات ذات طبيعة استثنائية، ولا يمكن اعتبارها مشروعة إلا إذا تم تنفيذها وفق الضوابط القانونية المحددة، وذلك بسبب مساسها بشكل مباشر بحرية وحرمة الأفراد في حياتهم الخاصة. ولذلك فإن استعمالها من طرف الضبطية القضائية في مرحلة التحري يخضع لإشراف وموافقة وكيل الجمهورية، بينما يشترط في مرحلة التحقيق القضائي الحصول على إذن صادر عن قاضي التحقيق وتحت رقابته. كما يمكن تفعيل الوسائل التقنية في أي زمان أو مكان دون إعلام المعنيين، بما في ذلك خارج الأوقات العادية المحددة قانونًا[3].

ويشترط أن يشمل الإذن بهذه العمليات كل العناصر المطلوب القيام بها، والجريمة التي تبرر اللجوء إلى مثل هذه الإجراءات ومدتها، على أن يصدر بشكل مكتوب ولمدة لا تتجاوز أربعة أشهر قابلة للتجديد عند الاقتضاء. كما يجوز للسلطات المختصة الاستعانة

---

[1]– بن يونس فريدة، استحداث قطب جزائي وطني لمكافحة الجرائم السيبرانية ومتابعتها –قراءة في الأمر 21–11–، مجلة الدراسات القانونية والاقتصادية، المجلد 05، العدد 01، المركز الجامعي بريكة، سنة 2022، ص 1715.

[2]– المرجع نفسه، ص 1716.

[3]– المادة 114 من قانون رقم 25–14 يتضمن قانون الإجراءات الجزائية، السالف الذكر.

بجهات فنية أو خبراء أو هيئات عمومية أو خاصة متخصصة من أجل ضمان التنفيذ التقني لهذه العمليات[1].

وعند الانتهاء يتعين على ضابط الشرطة القضائية إعداد محضر مفصل يوثق جميع مراحل التنفيذ، مع تحديد دقيق لتوقيت بداية ونهاية كل عملية. ويتم كذلك استخراج التسجيلات أو الصور أو المحادثات ذات الصلة بالقضية وضمها إلى ملف الإجراءات على وسائط إلكترونية مرفقة كأدلة مادية[2].

الفرع الثاني: الاختصاص القضائي والجزاءات المقررة لجريمة التجسس السيبراني

تتطلب مكافحة جريمة التجسس السيبراني تحديد الجهة القضائية المختصة بالنظر فيها، بما يضمن فعالية المتابعة وتقرير عقوبات صارمة تتناسب مع خطورة الجريمة، بهدف ردع مرتكبيها وحماية الأنظمة المعلوماتية والبيانات من الاعتداءات.

أولا: الاختصاص القضائي لجريمة التجسس السيبراني

أهم ما يميز الجرائم المعلوماتية عن الجرائم الأخرى هو تمديد الاختصاص المحلي للجهات القضائية وذلك بسبب تعقيد هذه الجرائم وطابعها العابر للحدود وخطورتها على أمن واستقرار الدولة.

1. اختصاص جهاز الشرطة القضائية

تتولى الشرطة القضائية مهمة البحث والتحري في مختلف الجرائم، بما فيها الجرائم المعلوماتية، وتتكون من ضباط وأعوان الشرطة القضائية التابعيين لجهازي الأمن الوطني والدرك الوطني، إضافة إلى الفئات التي خول لها القانون هذه الصفة[3]. كما تضم مصالح الشرطة القضائية فرق ووحدات متخصصة في مكافحة الجريمة المعلوماتية وهي المختصة في البحث والتحري في هذه الجرائم.

يجوز تمديد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني في الجرائم المعلوماتية[4].

---

[1]– المادة 116 و117 من قانون رقم 25–14 مؤرخ في 9 صفر عام 1447 الموافق 3 غشت 2025، يتضمن قانون الإجراءات الجزائية، السالف الذكر.

[2]– المادة 118 و119 من قانون رقم 25–14، يتضمن قانون الإجراءات الجزائية، السالف الذكر.

[3]– المادة 20 من قانون رقم 25–025، يتضمن قانون الإجراءات الجزائية، السالف الذكر.

[4]– المادة 24 من قانون رقم 25–14 يتضمن قانون الإجراءات الجزائية، السالف الذكر.

وبما أن هذه الجرائم تقع في فضاء رقمي يصعب التعامل معه، فيلزم أن تكون الجهات المختصة في البحث والتحري عنه ملمة بهذا المجال بـــالمعرفة الكافية في مجال الشبكات وتشغيل الحواسيب والقدرة على التعامل مع أنظمتها المختلفة، والقدرة على التعامل مع الأمن المعلوماتي وطرق التجسس مع استخدام برامج الوقاية من الفيروسات وغيرها[1].

2. اختصاص الجهات القضائية

وسع المشرع الجزائري من اختصاص المحاكم ووكلاء الجمهورية وقضاة التحقيق في عدة جرائم منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات إلى اختصاص دوائر محاكم أخرى[2].

وتختص الجهات القضائية بالنظر إلى الجرائم المعلوماتية المرتكبة خارج الإقليم الوطني، متى كانت الأفعال المرتكبة مجرمة بالقانون الجزائري، وارتكبت خارج الجزائر، وكان مرتكبها أجنبي يستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني[3].

3. اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

يقع مقر هذا القطب في دائرة اختصاص مجلس قضاء الجزائر العاصمة[4]، ويختص في متابعة ومكافحة بعض الجرائم المعلوماتية المنصوص عليها قانوناً، لاسيما جريمة التجسس السيبراني التي تندرج ضمن هذه الجرائم. ويمارس كل من وكيل الجمهورية وقاضي التحقيق ورئيس ذات القطب التابعين للقطب اختصاصهم عبر كامل الإقليم الوطني[5]، نظراً لأن الجرائم التي يختص بها هذا القطب هي جرائم معقدة وغير محددة الرقعة.

---

[1]– جراد سميرة، قتال جمال، خصوصية المتابعة الجزائية للجرائم الإلكترونية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 14، العدد 01، جامعة تامنغست، للسنة 2025، ص 343.

[2]– المادة 01 من مرسوم تنفيذي رقم 06-348 مؤرخ في 12 رمضان عام 1427 الموافق 5 أكتوبر سنة 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر العدد 63، الصادر في 15 رمضان عام 1427 الموافق 18 أكتوبر 2006، ص 30.

[3]– المادة 15 من قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف الذكر.

[4]– المادة 335 من قانون رقم 25-14 يتضمن قانون الإجراءات الجزائية، السالف الذكر.

[5]– المادة 337 من قانون رقم 25-14، يتضمن قانون الإجراءات الجزائية، السالف الذكر.

أ. اتصال القطب بملف القضية

يتصل هذا القطب الجزائي بملف القضية بعدة طرق تتمثل في:

- **تواجد ملف الدعوى بحوزة الضبطية القضائية أو النيابة العامة**

إذا كانت القضية في مرحلة البحث والتحري في الجرائم التي يختص بها القطب لدى مصالح الضبطية القضائية، فينبغي إرسال جميع المحاضر والتقارير الإخبارية وكافة إجراءات التحقيق المنجزة مباشرة إلى وكيل الجمهورية لدى القطب الجزائي. وفي هذه الحالة يصبح ضباط الشرطة القضائية خاضعين لسلطة وكيل الجمهورية لدى القطب ويتلقون تعليماتهم منه مباشرة، وفي حال تقرر فتح تحقيق قضائي في القضية، فإنهم ينفذون الإنابات القضائية الصادرة عن قاضي التحقيق المخطر بالملف لدى القطب[1].

وفي حالة كان الملف في يد النيابة العامة على مستوى إحدى المحاكم الوطنية، فعلى وكيل الجمهورية المختص فيها إصدار قرار بالتخلي عن الملف وإحالته إلى وكيل الجمهورية التابع للقطب[2]. وفي المقابل إذا تبين لوكيل الجمهورية لدى القطب أن الوقائع المعروضة عليه لا تدخل ضمن اختصاصه النوعي، فإنه يصدر بدوره قراراً بالتخلي لصالح وكيل الجمهورية المختص إقليمياً[3].

- **تواجد الملف في مرحلة التحقيق لدى المحاكم العادية**

إذا تبين لقاضي التحقيق بالمحاكم العادية أن القضية تقع ضمن صلاحيات القطب، فإنه يصدر أمر بعدم الاختصاص النوعي، سواء من تلقاء نفسه أو بطلب من وكيل الجمهورية، ثم يحال الملف بعد ذلك إلى قاضي التحقيق لدى القطب.

وتبقى الأوامر الصادرة من قاضي التحقيق الأول قائمة ومنتجة لأثارها القانونية، ما لم يصدر قرار مخالف من قاضي التحقيق لدى القطب[4].

---

[1]– المادة 346 من قانون رقم 25–14، يتضمن قانون الإجراءات الجزائية، السالف الذكر.

[2]– عون فاطمة الزهراء، الإجراءات التشريعية المستحدثة في مواجهة الجريمة الإلكترونية في القانون الجزائري –القطب الجزائي الوطني نموذجاً–، مجلة حقوق الإنسان والحريات العامة، المجلد 07، العدد 02، جامعة عبد الحميد بن باديس مستغانم،2022، ص 566.

[3]– المادة 347 من قانون رقم 25–14، يتضمن قانون الإجراءات الجزائية، السالف الذكر.

[4]– المادة 348 من قانون رقم 25–14، يتضمن قانون الإجراءات الجزائية، السالف الذكر.

ويختص وكيل الجمهورية وقاضي التحقيق ورئيس ذات القطب بكامل الصلاحيات التي تخول لهم البحث والتحري ومتابعة الجريمة المعروضة أمامهم، بالاستعانة بالشرطة القضائية أو أي جهة يمكنها المساعدة، فيمكن للجهات المختصة للقطب إما متابعة الإجراءات التي قام بها ضباط الشرطة من قبل أو قاضي التحقيق، أو القيام بأي إجراء يرونه ضروري في كشف ملابسات القضية[1].

ثانيا: العقوبات المقررة لجريمة التجسس السيبراني

تعتبر جريمة التجسس السيبراني من أخطر الجرائم التي يمكن أن تمس النظام العام للدولة، ولذلك أقر لها المشرع الجزائري عقوبات صارمة وذلك للحد منها وحماية أمن الدولة.

أقر المشرع الجزائري عقوبة التجسس بالنظر إلى طبيعة المصلحة المعتدى عليها، والمتمثلة في أسرار الدفاع الوطني والمعطيات ذات الطابع الاستراتيجي أو الأمني، فقد نصت المادة 64 من ق.ع على عقوبة الإعدام لكل من يرتكب أو يحرض أو يعرض بنفسه ارتكاب أفعال التجسس أو يساهم فيها متى تعلقت بأمن الدولة أو مصالحها العليا[2]، ولا يختلف الأمر إذا ارتكبت الجريمة باستعمال الوسائل المعلوماتية، لأن استخدام الحاسوب أو الشبكات الإلكترونية لا يغير من الطبيعة القانونية للفعل متى كان الهدف منه الحصول على معلومات سرية أو بيانات حساسة بقصد إفشائها أو تسليمها لدولة أجنبية أو جهة معادية أو استعمالها للإضرار بالأمن الوطني.

ويتحقق الركن المادي للتجسس السيبراني من خلال عدة أفعال تقنية نظمها المشرع ضمن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، كالدخول غير المشروع إلى الأنظمة المعلوماتية، وهي الأفعال المنصوص عليها في المواد 394 مكرر وما يليها من ق.ع. غير أن هذه الأفعال لا تعد تجسس بمجرد وقوعها، وإنما يشترط أن يقترن ارتكابها بقصد جنائي خاص يتمثل في استهداف أمن الدولة أو المساس بمصالحها، أو تمكين جهة أجنبية من معلومات ذات طابع سري. أما إذا اقتصر الفعل على مجرد اختراق أو مساس بالنظام المعلوماتي دون توافر هذه الغاية، فإن التكييف القانوني ينصرف إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات، والتي رتب لها المشرع عقوبة الحبس والغرامة المالية. وبالتالي

[1]– المادة 337 قانون رقم 25–14، يتضمن قانون الإجراءات الجزائية، السالف الذكر.

[2]– المادة 64 من الأمر 66–156 المتضمن قانون العقوبات السالف الذكر.

قد تتشابه الأفعال المادية في الجريمتين، غير أن معيار التفرقة بينهما يتمثل في الغاية الحقيقية من السلوك الإجرامي وطبيعة المصلحة المعتدى عليها، إذ تتحول الجريمة المعلوماتية العادية إلى جريمة تجسس سيبراني متى استهدفت أسرار الدولة أو أمنها الداخلي أو الخارجي، وهو ما يبرر إخضاعها للعقوبات الأشد المقررة ضمن جرائم أمن الدولة.

العقوبات التكميلية

علاوة على الأحكام الأصلية لجريمة التجسس يمكن أن تحكم الجهة المختصة بمصادرة الأجهزة والبرامج والوسائل المستخدمة في الجريمة من أقراص صلبة أو حواسيب، مع إغلاق المواقع التي تكون محلاً للجريمة من الجرائم المعاقب عليها في هذا القسم والتي تدخل في حكم التجسس[1].

الإعفاء والتخفيف من عقوبة التجسس السيبراني

إذا قام الشخص بتبليغ السلطات الإدارية أو القضائية عن جريمة تمس بأمن الدولة كجريمة التجسس السيبراني قبل البدء في التخطيط لها أو تنفيذها، في هذه الحالة يتم إعفاؤه تماما من العقوبة المقررة للجريمة. ويستفيد أيضا من تخفيف العقوبة بدرجة واحدة في حالة التبليغ المتأخر عن الجريمة وذلك بعد ارتكابها، ولكن قبل أن تبدأ السلطات القضائية في المتابعة الجزائية. وكذلك يستفيد منها في حالة المساعدة في القبض على المتورطين في الجريمة إذا ساعد بكل الطرق السلطات وقدم لهم معلومات تمكنهم من القبض على الفاعلين الأخرين أو شركائهم، بشرط أن يكون ذلك قبل المتابعة القضائية[2].

[1]– المادة 394 مكرر 6 من قانون 04-15، المتضمن تعديل قانون العقوبات السالف الذكر.

[2]– المادة 92 من الأمر 66-156 المتضمن قانون العقوبات السالف الذكر.

خاتمة

في الختام، وبعد الإلمام الشامل بالموضوع، يتضح أن التجسس السيبراني لم يعد مجرد تهديد تقني عابر، بل أصبح إحدى الأدوات التي تستغل في الصراعات الحديثة بين الدول، لما ينطوي عليه من مخاطر تمس أمن واستقرار الدول. وقد أظهرت الدراسة أن هذه الجريمة باتت من أبرز التهديدات التي تواجه الدول والمؤسسات في ظل الاعتماد المتزايد على التكنولوجيا والأنظمة الرقمية، إذ لا يقتصر خطرها على استهداف البيانات والمعلومات الحساسة فحسب، بل يمتد ليشمل المساس بالأمن الوطني والمصالح الاستراتيجية للدول وعلاقاتها.

ولهذا سعى كل من المجتمع الدولي والمشرع الجزائري إلى وضع استراتيجية قانونية ومؤسساتية وتقنية لمواجهة هذه الجريمة، من خلال الاتفاقيات الدولية، وآليات التعاون الدولي، والتشريعات الوطنية، والهيئات المختصة بالأمن السيبراني. غير أن تحليل مختلف هذه الآليات أظهر أن فعاليتها تبقى نسبية، إذ ورغم مساهمتها في الحد من بعض الممارسات المرتبطة بالتجسس السيبراني، إلا أنها ما تزال تواجه عدة تحديات قانونية وتقنية وعملية تحد من قدرتها على تحقيق مواجهة كاملة وفعالة لهذه الجريمة.

وعليه، يمكن الإجابة عن الإشكالية المطروحة بالقول إن المنظومة المتبناة دولياً ووطنياً للتصدي للممارسات اللصيقة بالتجسس السيبراني أسهمت في تعزيز الحماية القانونية والأمنية للفضاء السيبراني، إلا أن فعاليتها لا تزال غير كافية بالنظر إلى الطبيعة المتطورة للتجسس السيبراني، وسرعة تطور وسائله، والطابع العابر للحدود الذي تتسم به هذه الجريمة.

هذا الواقع يجعلنا نقف على مجموعة من النتائج الحتمية المستخرجة من الموضع محل الدراسة، وصولاً إلى طرح حلول وتوصيات عملية يمكن تطبيقها في واقعنا الحالي.

وبالتالي وبعد دراسة معمقة لموضوع التجسس السيبراني تم استخراج النتائج الأتية:

-التجسس السيبراني ليس مجرد جريمة معلوماتية عادية، بل هو عمل منظم يعتمد على أساليب تقنية محددة يستهدف الحصول على معلومات سرية بطرق إلكترونية خفية، وكثيراً ما تكون الجهات الحكومية طرفاً فيه. ونظراً لطابعه العابر للحدود، فإن نسبته إلى جهة معينة تعتبر صعبة من الناحية القانونية والتقنية.

-تتميز أساليب التجسس الرقمي بالتنوع المستمر والتطور الدائم، مما يجعل التعريفات القانونية الجامدة عاجزة عن مواكبته وملاحقة واقعه المتغير.

–لا توجد حتى الآن معاهدة دولية ملزمة وشاملة تتعلق تحديداً بالتجسس السيبراني، مما يترك فراغاً قانونياً واضحاً على المستوى الدولي، والتعاون الدولي في مجال مكافحة التجسس السيبراني لا يزال محدوداً، ويغلب عليه الطابع السياسي أكثر من الطابع القانوني والتقني.

بناءً على ما تم ملاحظته من نتائج، سنقدم الحلول والتوصيات الأتية:

– بالنظر إلى الصعوبات التشريعية المتمثلة في غياب تعريف قانوني موحد متفق عليه للتجسس السيبراني دولياً، وعدم وضع المشرع الجزائري لتعريف أو قانون خاص ينظمه، مما يفتح ثغرات لإفلات الجناة من العقاب؛ فإننا نوصي بالعمل الجاد على صياغة اتفاقية دولية ملزمة تحدد بوضوح الأفعال المحظورة، مع قيام المشرع الجزائري بمراجعة قوانين الجرائم المعلوماتية وتحديثها لتشمل أحكاماً صريحة تفصل في التجسس السيبراني بمفهومه الشامل دون الاكتفاء بالقواعد العامة.

– انطلاقاً من واقع ضعف إجراءات الحماية والوعي الرقمي في المؤسسات الجزائرية الحساسة التي لا تزال تستخدم الطرق التقليدية وتعتمد على برمجيات وأنظمة تشغيل مستوردة من شركات أجنبية قد تحوي ثغرات تجسس؛ فإننا ندعو إلى فرض فحص تقني صارم على كافة البرمجيات المستوردة قبل تشغيلها، موازاة مع تبني خيار "إنشاء شبكة وطنية مغلقة للبيانات السيادية "تضمن عزل أنظمة معلومات الدولة الحساسة (مثل بيانات الدفاع، العدالة، والمؤسسات الاقتصادية الكبرى) تماماً عن شبكة الإنترنت العالمية.

– استجابةً للعقبات التقنية والإجرائية الكبيرة المحيطة بـــ "صعوبة الإسناد الرقمي"، واستخدام الجناة لتقنيات إخفاء الهوية عبر خوادم وسيطة، ورفض بعض الدول التعاون القضائي بحجة السيادة الرقمية أو إنكار علاقتها بالهجوم؛ فإننا نقترح إنشاء هيئة دولية تقنية محايدة للتحقيق في هذه الحوادث العابرة للحدود، مع تفعيل إمكانية فرض غرامات مالية أو عقوبات صارمة على الدول التي ترفض التعاون القضائي، موازاة مع تبسيط وتسريع الإجراءات القانونية وطنياً ودولياً لتفادي محو الأدلة الرقمية.

– لمواجهة الصعوبة الناتجة عن سرعة التطور التقني لأدوات التجسس التي تتجدد بوتيرة أسرع من القوانين وتجعل التشريعات متأخرة دائماً؛ فإننا نوصي بوضع أطر قانونية مرنة تعتمد على المعايير التقنية المتغيرة، وتعزيز تبادل المعلومات الاستخباراتية والتحذيرات

الاستباقية بشأن التهديدات السيبرانية بين الدول لضمان الجاهزية التشريعية والدفاعية قبل وقوع الفعل.

– بالنظر إلى افتقار الكثير من الدول للخبراء القادرين على التحقيق في جرائم التجسس السيبراني وملاحقتها قضائياً؛ فإننا نحث على الاستثمار الحقيقي في تأهيل الكوادر البشرية من خلال إدراج برامج تكوين تخصصية في أمن المعلومات والتحقيق الرقمي على مستوى الجامعات والمعاهد الوطنية، وتبني مهارات الشباب الجزائري الموهوب في الحماية والاختراق وتوظيفهم في الهيئات الأمنية بامتيازات ومحفزات مادية تمنع هجرتهم إلى الخارج.

– بما أن بناء أنظمة دفاعية قوية يتطلب ميزانيات مالية ضخمة جداً لتحديثها دورياً مما يعيق الدول للحفاظ على أمنها؛ فإننا نوصي بتشجيع الابتكار الوطني وتطوير برمجيات حماية محلية الصنع (مفتوحة المصدر ومؤمنة)، والاعتماد على الشراكات التقنية الإقليمية لتقاسم تكاليف التحديث، مما يضمن حماية المنظومة الأمنية بأقل التكاليف المالية الممكنة.

قائمة المراجع

قائمة المراجع:

أولا: الكتب

1. دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية، أُعد من قبل مجموعة من الخبراء الدوليين بدعوة من قبل (THE NATO cooperative cyber defence center of excellence)، المحرر من طرف MICHEAL N. SCHMITT، ترجمة على محمد كاظم الموسوي، في كتابه الموسوم بـــ(المشاركة المباشرة في الهجمات السيبرانية)، المطبوع في شركة المؤسسة الحديثة للكتاب عام 2019.

2. سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، د ط، منشورات الحلبي الحقوقية للنشر، لبنان، 2011.

3. عبد السلام أحمد، بروتوكولات الأمان في شبكان الأنترنت، الطبعة الثانية، دار الأشجار للنشر، الأردن، 2018.

4. علوي علي أحمد الشارفي، الوجيز في جرائم تقنية المعلومات، الطبعة الأولى، المركز الديمقراطي للنشر برلين، ألمانيا، 2024.

5. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، د ط، منشورات زين الحقوقية، لبنان، 2013.

6. محمد الفاضل، الجرائم الواقعة على أمن الدول، الجزء الأول، الطبعة الثانية، مطبعة جامعة دمشق للنشر، سوريا، 1963.

7. مناصرة عبد الله، الاستخبارات العسكرية في الإسلام، الطبعة الثانية، دار الرسالة للنشر والتوزيع، بيروت، لبنان، 1991.

8. نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، 2010.

9. يعيش تمام شوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، الطبعة الأولى، مطبعة الرمال (الوادي) للنشر، الجزائر، 2019.

ثانيا: الرسائل والمذكرات الجامعية

- رسائل الدكتوراه

1. أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث، تخصص القانون الخاص، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج، 2021/2020.
2. تاهمي مصطفى، مستقبل الأمن القومي الجزائري في ظل التطورات التكنولوجية وحروب المعلومات، أطروحة مقدمة لاستكمال متطلبات شهادة الدكتوراه في العلوم السياسية وعلاقات دولية، تخصص علاقات دولية واستشراف، قسم الدراسات الدولية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، 2024/2023.
3. عثماني رضوان، مكافحة جرائم المعلوماتية في القانون الجزائري والدولي، أطروحة مقدمة للحصول على شهادة الدكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد 2 وهران، 2024/2023.
4. نادية سلامي، آليات مكافحة التجسس الإلكتروني، أطروحة مقدمة لنيل شهادة دكتوراه في العلوم في القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي –تبسة–، 2019/2018.
5. هروال هبة نبيلة، جرائم الأنترنت" دراسة مقارنة"، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2014/2013.

– رسائل الماجيستر

1. بوذراع عبد العزيز، خصوصية الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، مذكرة لنيل شهادة الماجيستر في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، 2012/2011.
2. جدي نسيمة، جرائم المساس بأنظمة المعالجة الألية للمعطيات، مذكرة لنيل شهادة الماجيستر في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014/2013.
3. حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجيستر في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر –باتنة–، 2012/2011.

4. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجيستر في القانون، تخصص القانون الدولي للأعمال، مدرسة الدكتوراه "القانون الأساسي والعلوم السياسية"، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013.
5. علاء الدين محمد عفيف نابلسي، السياسة الجنائية في مواجهة جرائم التجسس "دراسة مقارنة"، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة الماجيستر في القانون الجنائي، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس فلسطين، 2020.
6. فريد ولد حسين، جرائم التجسس، مذكرة مقدمة لنيل شهادة الماجيستر في القانون الدولي الجنائي، مدرسة الدكتوراه، القانون الجنائي الدولي، معهد العلوم القانونية والإدارية، المركز الجامعي عباس لغرور –خنشلة–، 2011/2010.
7. محمد عدنان عثمان، دور القانون الدولي في مواجهة التجسس الديبلوماسي، رسالة لنيل متطلبات الحصول على درجة الماجيستر في القانون العام، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط، يناير 2015.

– مذكرات الماستر

1. أمحمد إسماعيل، زوبيري عبد الحليم، دور التكنولوجيا الحديثة في ارتكاب الجرائم الإلكترونية وسبل مكافحتها، مذكرة تخرج لنيل شهادة الماستر تخصص قانون جنائي والعلوم الجنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2025/2024.
2. آية بن ميسية، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة ضمن متطلبات نيل شهادة الماستر، تخصص قانون جنائي، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف–ميلة–، 2025/2024.
3. بقدار شيماء، آليات مكافحة الجريمة الإلكترونية على المستويين الدولي والوطني، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس –مستغانم–، 2023.
4. بلعباس أحمد، بلعباس محمد نذير، الوقاية من الجرائم المعلوماتية في القانون، مذكرة ضمن متطلبات نيل شهادة الماستر في القانون، تخصص قانون جنائي، قسم العام، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور بالجلفة، 2025/2024.

5. بن علال بومدين، التحقيق الجنائي في الجرائم الناشئة عن المعاملات الإلكترونية في ضوء التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماستر في القانون العام، قسم الحقوق، معهد الحقوق والعلوم السياسية، المركز الجامعي مغنية، 2021/2020.

6. بودواب سمير، لبديوي فؤاد، جرائم المساس بأنظمة المعالجة الألية للمعطيات، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 –سكيكدة–، 2024.

7. بوشعبة محمد، الخيانة والتجسس في قانون القضاء العسكري، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة يحي فارس –المدية–، 2022/2021.

8. بوعلي هالة، جريمة الخيانة والتجسس في التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي –تبسة–، 2022/2021.

9. بوفروك هند، سعيود بشرى، إجراءات المعاينة، التفتيش، والحجز داخل المنظومة المعلوماتية، مذكرة مكملة لنيل شهادة الماستر تخصص القانون الجنائي والعلوم الجنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 سكيكدة، 2025.

10. بولبراشن إسراء، خميس لبنى، الجرائم الماسة بأمن الدولة الخارجي في التشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 –سكيكدة–، جوان2025.

11. سعودي رضا، قمع جريمة التجسس في التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماستر، تخصص سياسة جنائية وعقابية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي –تبسة–، 2017/2016.

12. عليلي عماد الدين، بن قسيس زين الدين، جرائم الخيانة وتسريب المعلومات والوثائق السرية على ضوء القانون 24–06 المعدل والمتمم لقانون العقوبات، مذكرة مكملة لمتطلبات نيل شهادة الماستر، تخصص قانون أعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 –قالمة–، 2025/2024.

13. عماد يوسف، لزهر ضربان، إجراءات التحري في الجرائم الإلكترونية، مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر، تخصص قانون قضائي مهني، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، 2023/2022.

14. عياشي عاشور، يعيش عبد الحق، آليات مكافحة جريمة التجسس السيبراني في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي في الحقوق، تخصص قانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي-برج بوعريريج-، 2024/2023.

15. كركابو فطيمة، بحري سندس، التجسس الإلكتروني ضد امن الدولة، مذكرة مكملة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 -سكيكدة-، سبتمبر 2024.

16. لعور مرزوق، تازولت أكرم سيف الدين، الجرائم الإلكترونية والأمن السيبراني في الاتفاقيات الدولية والتشريع الجزائري، مذكرة مكملة لنيل شهادة الماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور -خنشلة-، 2024/2023.

17. مسكين سعيدة، الإطار القانوني للجريمة الإلكترونية في التشريع الوطني والدولي، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي في الحقوق، تخصص قانون الإنترنت والإعلام الآلي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي -برج بوعريريج-، 2025/2024.

18. مقرح عبد الرؤوف، التجسس السيبراني الماس بأمن الدولة في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق، تخصص قانون الإعلام الآلي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي-برج بوعريريج- ، 2024/2023.

19. منيرة صديقي، خديجة سعيدات، تجريم الأفعال الماسة بأمن الدولة والوحدة الوطنية، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر أكاديمي في الحقوق، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة -غرداية-، 2022/2021.

ثالثا: المقالات العلمية

1. أحمد سعيد أحمد، المسؤولية الدولية الناتجة عن الجرائم السيبرانية، مجلة الباحث العلمي، **مجلة الباحث العربي**، مجلد 6، عدد 04، جامعة الدول العربية –مجلس وزراء العدل العرب– المركز العربي للبحوث القانونية والقضائية، 2025، ص ص1–18.

2. صغير يوسف، التفتيش كآلية لإثبات جرائم نظم المعلوماتية، المجلة النقدية للقانون والعلوم السياسية، المجلد 16، العدد 04، جامعة تيزي وزو، سنة 2021، ص ص595–606.

3. إدريس قرفي، تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية: بين اتفاقية بودابست والتشريع الجزائري، **مجلة الحقوق والحريات**، المجلد 02، العدد 02، جامعة محمد خيضر بسكرة، 2014، ص ص99–112.

4. اوشن حنان، وادي عماد الدين، التجسس الإلكتروني وآليات مكافحته في التشريع الجنائي الجزائري، **مجلة الحقوق والعلوم السياسية**، المجلد 01، العدد 02، جامعة عباس لغرور – خنشلة–، جويلية 2014، ص ص130–141.

5. بارة سمير، الأمن السيبراني (cyber Security) في الجزائر: السياسات والمؤسسات، **المجلة الجزائرية للأمن السيبراني**، العدد 04، جامعة الحاج لخضر –باتنة–، جويلية 2017، ص ص255–280.

6. بن شهرة شول، مراد مشوش، السمات الخاصة للجريمة المعلوماتية، **مجلة المستقبل للدراسات القانونية والسياسية**، مجلد 04، العدد 01، المركز الجامعي بآفلو، جوان 2020، ص ص3–21.

7. بن يونس فريدة، استحداث قطب جزائي وطني لمكافحة الجرائم السيبرانية ومتابعتها – قراءة في الأمر 21–11–، **مجلة الدراسات القانونية والاقتصادية**، المجلد 05، العدد 01، المركز الجامعي بريكة، سنة 2022، ص ص1707–1727.

8. بوجوراف عبد الغاني، التجسس كجريمة ماسة بأمن الدولة في ظل قانون العقوبات الجزائري، **مجلة أفاق العلوم**، الجزء 01، العدد الثامن، جامعة الجلفة، جوان2017، ص ص338– 348.

9. بوعكاز أسماء، مباركي دليلة، الإنتربول ودوره في تنفيذ اتفاقيات تسليم المجرمين في إطار مكافحة الجريمة المنظمة، **مجلة الباحث للدراسات الأكاديمية**، المجلد 08، العدد 03، جامعة باتنة 1، 2022، ص ص118–141.

10. جراد سميرة، قتال جمال، خصوصية المتابعة الجزائية للجرائم الإلكترونية، **مجلة الاجتهاد للدراسات القانونية والاقتصادية**، المجلد 14، العدد 01، جامعة تامنغست، للسنة 2025، ص ص333-355.

11. حابت أمال، الجريمة المعلوماتية في التشريع الجزائري: بين قانوني 04-15، و09-04، **مجلة هيرودوت للعلوم الإنسانية والاجتماعية**، المجلد 7، العدد 25، مؤسسة هيرودوت للبحث العلمي والتكوين، 2023، ص ص53-68.

12. حزام فتيحة، الحماية المؤسساتية للأنظمة الرقمية في الفترة التشريعية الممتدة من 2009-2020، **مجلة الأكاديمية للدراسات الاجتماعية والإنسانية**، المجلد 13، العدد 01، جامعة حسيبة بن بوعلي –الشلف–، 2021، ص ص273-283.

13. خالد علي نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، **مجلة البحوث القانونية والاقتصادية**، مجلد 2022، عدد 79، جامعة المنصورة، لسنة 2022، ص ص1-50.

14. خالد وليد شوشان، التجسس في القانون الدولي، **مجلة الحقوق**، العدد 4، جامعة الكويت، 2016، ص ص395-428.

15. خرشي عثمان، تسليم المجرمين كآلية دولية لمكافحة الجرائم المعلوماتية، **مجلة البحوث القانونية والسياسة**، العدد العاشر، جامعة مولاي الطاهر بسعيدة، جوان 2018، ص ص916-942.

16. راوية مطماطي، نبيل بن عديدة، عملية التسرب على ضوء قانون الإجراءات الجزائية 25-14، **مجلة حقوق الإنسان والحريات العامة**، المجلد 10، العدد 02، –جامعة مستغانم–، سنة 2025، ص ص397-427.

17. رحموني محمد، خصائص الجريمة المعلوماتية ومجالات استخدامها، **مجلة الحقيقة**، العدد 41، جامعة احمد دراية أدرار، 2018، ص ص432 -451.

18. رمضان حسن ضاحي عبد الحافظ، التجسس الإلكتروني عبر تقنيات الذكاء الاصطناعي "دراسة فقهية"، **مجلة كلية الدراسات الإسلامية والعربية للبنات بسوهاج**، العدد الحادي والثلاثون، الإصدار الأول، جامعة الأزهر، يونيو2025، ص ص762-794.

19. سارة قريمس، التسرب الإلكتروني كآلية إجرائية مستحدثة للتحري والتحقيق الجنائي الرقمي على ضوء التشريع الجزائري، **مجلة الفكر القانوني والسياسي**، المجلد التاسع، العدد الثاني، جامعة عمار ثليجي –الأغواط–، 2025، ص ص1232–1248.

20. سامية بوشوشة، حياة سلماني، التجسس الإلكتروني وطرق مكافحته، **مجلة العلوم الاجتماعية والإنسانية**، المجلد 16، العدد 01، جامعة تبسة، جوان 2023، ص ص49–74.

21. سليماني مباركة، الإرهاب الإلكتروني وطرق مكافحته، **مجلة الحقوق والعلوم السياسية**، المجلد 01، العدد 08، جامعة عباس لغرور –خنشلة–، جوان 2017، ص ص340–355.

22. سميحة بلقاسم، حميد بوشوشه، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر.. واقعها وآليات مجابهتها، **مجلة العلوم الإنسانية**، المجلد 10، العدد 01، جامعة أم البواقي، جوان 2023، ص ص533–561.

23. الطاهر ياكر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، **مجلة الصدى للدراسات القانونية والسياسية**، المجلد 4، العدد 4، 2022جامعة الجيلالي بونعامة خميس مليانة، ص ص1–39.

24. عزالدين عثماني، صور الركن المادي في الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، **مجلة العلوم القانونية والسياسية**، المجلد 09، العدد 03، جامعة الشهيد حمه لخضر –الوادي–، ديسمبر 2028، ص ص612–625.

25. عون فاطمة الزهراء، الإجراءات التشريعية المستحدثة في مواجهة الجريمة الإلكترونية في القانون الجزائري –القطب الجزائي الوطني نموذجاً–، **مجلة حقوق الإنسان والحريات العامة**، المجلد 07، العدد 02، جامعة عبد الحميد بن باديس مستغانم،2022، ص ص554–576.

26. فتيحة خالدي، تأثير التجسس الإلكتروني على الحق في الخصوصية المعلوماتية، **مجلة البحوث في الحقوق والعلوم السياسية**، المجلد 07، العدد 01، جامعة ابن خلدون تيارت، السنة 2021، ص ص302–314.

27. قزران مصطفى، زرقين عبد القادر، الآليات الدولية لمكافحة الجريمة الإلكترونية، **مجلة صوت القانون**، المجلد الثامن، العدد 02، جامعة الجيلالي بونعامة خميس مليانة، 2022، ص ص1222–1244.

28. قسمية محمد، خضري حمزة، مكافحة الجرائم الماسة بنظام المعالجة الألية للمعلومات في قانون العقوبات، **مجلة صوت القانون**، المجلد السابع، العدد 2، جامعة خميس مليانة، نوفمبر 2020، ص ص126-150.

29. قلات سومية، حاحة عبد العالي، مقتضيات المعاينة المعلوماتية في التشريع الجزائري، **مجلة الحقوق والحريات**، المجلد 11، العدد 1، جامعة محمد خيضر –بسكرة–، السنة 2023، ص ص519-551.

30. محمد الأبيض، دليل تالين والقواعد المطبقة على الهجمات السيبرانية، **مجلة العلوم القانونية والاجتماعية**، المجلد العاشر، العدد الرابع، جامعة زيان عاشور –الجلفة–، ديسمبر 2025، ص ص792-803.

31. محمد بدوسي، الحماية الجنائية للأسرار الخاصة بأمن الدولة من التجسس الإلكتروني "دراسة مقارنة بين التشريعين الفلسطيني والأردني"، **مجلة جامعة الاستقلال للأبحاث**، مجلد10، عدد خاص، جامعة الاستقلال، آب 2025، ص ص1-26.

32. مريم نباش، سعاد بولقرون، التجسس وانتهاك حق الخصوصية في العصر الرقمي دراسة وصفية تحليلية لبرنامج "بيغاسوس"، **مجلة الدراسات الإعلامية والاتصالية**، مجلد 02، العدد 03، جامعة الجزائر 3، ديسمبر 2022، ص ص63-78.

33. معاشي سميرة، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، **مجلة الفكر**، العدد السابع عشر، جامعة محمد خيضر بسكرة، جوان2018، ص ص398-417.

34. مقري صونيا، بن لعامر وليد، المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقاً للمرسوم الرئاسي رقم 20-05، **مجلة البحوث في العقود وقانون الأعمال**، المجلد 10، العدد 02، جامعة الأخوة منتوري –قسنطينة–، 2025، ص ص129-150.

35. مناد فتيحة، مدى شرعية الاستطلاع العسكري والتجسس من الفضاء الخارجي باستخدام الأقمار الصناعية –دراسة قانونية–، **مجلة القانون العام الجزائري والمقارن**، المجلد الرابع، العدد الثاني، جامعة الجيلالي اليابس سيدي بلعباس، 2018، ص ص154-171.

36. نعمان عبد الكريم، الدخول أو البقاء عن طريق الغش في نظام المعالجة الألية للمعطيات، **مجلة حوليات جامعة الجزائر 1**، المجلد 38، العدد 02، جامعة الجزائر 1، 2024، ص ص36-56.

37. الهام بن خليفة، جمال غريسي، التجسس الإلكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري، **مجلة دفاتر السياسة والقانون**، مجلد 14، عدد 01، جامعة قاصدي مرباح ورقلة، 2022، ص ص154-167.

38. ودرار أمين، الشرطة الجنائية الإفريقية "الأفريبول"، **حوليات جامعة الجزائر 01**، المجلد 34، العدد 01، جامعة الجزائر 01، لسنة 2020، ص ص135-149.

39. يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، **مجلة التواصل في الاقتصاد والإدارة والقانون**، عدد 48، جامعة باجي مختار عنابة، ديسمبر 2016، ص ص82-94.

رابعا: النصوص القانونية

الاتفاقيات الدولية

1. اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، تم تبنيها في 24 ديسمبر 2024، الموقعة في هانوي والمعتمدة من طرف الجمعية العامة للأمم المتحدة، موقعة في 25 أكتوبر 2025.

2. اتفاقية بودابست المتعلقة بالجرائم الإلكترونية، الموقعة في بودابست من طرف مجلس أوروبا في 23 نوفمبر 2001، دخلت حيز التنفيذ في 1 يوليو 2004.

3. اتفاقية لاهاي الرابعة المتعلقة بقوانين وأعراف الحرب البرية واللوائح المرفقة بها، المعتمدة في 18 أكتوبر1907، دخلت حيز النفاذ في 26 يناير 1910.

القوانين

1. قانون رقم 04-15 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر العدد 71.

2. قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

ومكافحتها، ج ر العدد 47، الصادرة في 25 شعبان عام 1430 الموافق لـــ 16 غشت سنة 2009.

3. قانون رقم 24-06، مؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، يعدل ويتمم الأمر 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر العدد 30، الصادر بـــ 21 شوال عام 1445 الموافق لـــ 30 أبريل سنة 2024.

4. قانون رقم 25-14 مؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، يتضمن قانون الإجراءات الجزائية، ج ر العدد 54، الصادر في 19 صفر عام 1447 الموافق 13 غشت سنة 2025.

الأوامر

1. أمر رقم 66-156 مؤرخ في 18 صفر عام 1386 الموافق 8 يونيو عام 1966، المتضمن قانون العقوبات، ج ر العدد 49، صادر في 21 صفر عام 1386 الموافق 11 يونيو سنة 1966، المعدل والمتمم.

2. أمر رقم 71-28، مؤرخ في 26 صفر عام 1391 الموافق 22 أبريل سنة 1971 يتضمن قانون القضاء العسكري، ج ر العدد 38، الصادر في 11 الثلاثاء 16 ربيع الأول عام 1391 الموافق 11 مايو 1971، المعدل والمتمم.

المراسيم الرئاسية

1. مرسوم رئاسي رقم 04-183 مؤرخ في 8 جمادى الأولى عام 1425 الموافق 26 يونيو سنة 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الأجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر العدد 41، الصادر في 9 جمادى الأولى عام 1425 الموافق 27 يونيو سنة 2004.

2. مرسوم رئاسي رقم 14-252 مؤرخ في ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، ج ر 57، الصادر في 4 ذو الحجة عام 1435، الموافق لـــ 28 سبتمبر سنة 2014.

3. مرسوم رئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 86، الصادرة في 6 ربيع الثاني عام 1443 الموافق 11 نوفمبر سنة 2021.

4. مرسوم رئاسي رقم 22-442 مؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر لسنة 2020، يتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر سنة 2020، ج ر العدد 82.

5. مرسوم رئاسي رقم 24-381 مؤرخ في 25 جمادى الأولى عام 1446 الموافق 27 نوفمبر سنة 2024، يتمم المرسوم الرئاسي رقم 21-439 المؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021 والمتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 80، الصادر في 2 جمادى الثانية عام 1446 الموافق 4 ديسمبر سنة 2024.

6. مرسوم رئاسي رقم 25-321 مؤرخ في 10 رجب عام 1447 الموافق 30 ديسمبر سنة 2025، يتضمن المصادقة على الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية للفترة 2025-2029، ج ر العدد 87، الصادر في 10 رجب عام 1447 مؤرخ في 30 ديسمبر سنة 2025.

7. مرسوم رئاسي رقم 26-07 مؤرخ في 18 رجب عام 1447 الموافق 7 جانفي سنة 2026، يتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية، وتحديد مهامه وتنظيمه وسيره، ج ر العدد 04، الصادر في 29 رجب عام 1447 الموافق 18 جانفي سنة 2026.

المراسيم التنفيذية

1. مرسوم تنفيذي رقم 06-348 مؤرخ في 12 رمضان عام 1427 الموافق 5 أكتوبر سنة 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر العدد 63، الصادر في 15 رمضان عام 1427 الموافق 18 أكتوبر 2006.

خامسا: المطبوعات الجامعية

1. بطيحي نسيمة، محاضرات في مقياس الوقاية من الجرائم الإلكترونية، مطبوعة مقدمة لطلبة السنة ثانية ماستر، تخصص إدارة إلكترونية وخدمات رقمية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين–سطيف2–، 2022/2021.

2. عمارة زينب، الوقاية من الجرائم الإلكترونية، مطبوعة بيداغوجية ألقيت على طلبة السنة ثانية ماستر للسداسي الثالث، تخصص إعلام ألي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج، 2022/2021.

3. لبنى عبد الكريم، مطبوعة بيداغوجية في مقياس قانون الإجراءات الجزائية المعمق، محاضرات موجهة لطلبة السنة الأولى ماستر تخصص قانون جنائي وعلوم جنائية، السداسي الأول، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي –جيجل–، 2026/2025.

سادسا: المداخلات والملتقيات العلمية

المداخلات العلمية

1. سويسي فتيحة، التكييف القانوني لجرائم المعلوماتية والإشكالات العلمية المترتبة عنها، مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية بتاريخ 18 جانفي 2022.

الملتقيات العلمية

1. بن بادة عبد الحليم، بوحادة محمد سعد، (جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة) –دراسة سياسية قانونية–، الملتقى الدولي الأول الموسوم بـــ: أمن المعلومات في الفضاء الإلكتروني: الرهانات والتحديات في شمال إفريقيا، المنعقد يومي: 17و18 فيفري 2020، كلية الحقوق والعلوم السياسية، –جامعة غرداية–.

سابعا: المواقع الإلكترونية

1. أبرز بنود اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية، 2025، مقال منشور على الموقع، https://www.aljazeera.net/، تاريخ الاطلاع 2026/03/29، على الساعة 17:13.

2. Advance DataSe، ما هو فيروس التجسس وكيف يختلف عن البرامج الضارة الأخرى، سبتمبر2025، مقال منشور على الموقع https://advance-datasec.com/، تاريخ الاطلاع 2026/03/11، على الساعة 7:43.

3. أحمد عبد السلام، الجاسوس في القانون الدولي، جوان 2019، مقال منشور على الموقع https://jordan-lawyer.com/ تاريخ الاطلاع 23 فيفري 2026، على الساعة 14:27.

4. استحداث مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة، أكتوبر 2017، مقال منشور على موقع منتدى التكنولوجيا العسكرية والفضاء https://army-tech.net/، تاريخ الاطلاع 2026/04/24، على الساعة 17:27.

5. الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، منشورة في موقع وزارة الدفاع الوطني الجزائر، على الموقع https://www.mdn.dz/، تاريخ الاطلاع 2026/04/25، على الساعة 14:35.

6. إلينا بليكسيدا، التعليقات على البروتكول الإضافي الثاني لاتفاقية الجريمة الإلكترونية تنتهي في أوائل مايو، 2021، مقال منشور على الموقع https://www.icann.org/، تاريخ الاطلاع 2026/05/16، على الساعة 13:34.

7. *اندبندنت العربية، التجسس والذكاء الاصطناعي... من الإنسان وعنه وعليه، افريل 2025، مقال منشور على الموقع https://www.independentarabia.com/، تاريخ الاطلاع 2026/03/11، على الساعة 7:52.*

8. خدمات التعاون في مجال مكافحة الجريمة السيبرانية، موقع الإنتربول الرسمي، https://www.interpol.int/، تاريخ الاطلاع 2026/05/18، على الساعة 10:53.

9. ديلي ميل، أجهزة تجسس أمريكية من نوع غريب، أوت 2019، مقال منشور على الموقع https://arabic.rt.com/world، تاريخ الاطلاع 2026/02/29، على الساعة 10:13.

10. الفريق الجزائري للاستجابة لطوارئ الحاسوب، موقع مركز البحث في الإعلام العلمي والتقني، https://www.cerist.dz/، تاريخ الاطلاع2026/04/24، على الساعة 18:39.

11. المادة 1، 2 من القانون الأساسي للمنظمة الدولية الشرطية الجنائية الإنتربول، اعتمد أثناء الدورة الـــ 25 للجمعية العامة فيينا 1956، متاح على الموقع https://www.legal-tools.org/، تاريخ الاطلاع 2026/05/18، على الساعة 2:42.

12. المركز الأوروبي لدراسة مكافحة الإرهاب والاستخبارات- ألمانيا وهولندا-، "الذكاء الاصطناعي هل يغير قواعد التجسس التقليدية؟"، نوفمبر 2025، منشور على موقع https://www.europarabct.com/، تاريخ الاطلاع 2026/03/12، على الساعة 5:53.

13. مصطفى شريف، اقتحام الدرونات لعالم التجسس والاختراق السيبراني، مقال منشور على الموقع https://itach.dk/drone-between-hacking-and-espionage/، تاريخ الاطلاع 2026/03/01، على الساعة 21:55.

14. وضع المنظومة الوطنية لحوكمة البيانات حيز الخدمة ركيزة أساسية لبناء دولة عصرية، فيفري 2026، مقال منشور على الموقع https://www.aps.dz/، تاريخ الاطلاع 2026/04/25، على الساعة 17:48.

فهرس المحتويات

فهرس المحتويات: