مجلة العلوم الاجتماعية والإنسانية
Available online at https://www.asjp.cerist.dz/en/PresentationRevue/65

رت م د: 1112-685x
رت م د إ: 2588-2236

المجلد: 16 / العدد: 01 / جـوان 2023
ص ص: 49 ـ 74

التجسس الإلكتروني وطرق مكافحته

Cyber-Espionage and Ways to Combat it

سامية بوشوشة *
جامعة باجي مختار
عنابة / الجزائر
Selmanihayette@rocketmail.com

حياة سلماني
جامعة باجي مختار
عنابة / الجزائر
Samiabouchoucha23@yahoo.com

تاريخ الارسال: 2021/08/15 تاريخ القبول: 2023/05/22 تاريخ النشر: 2023/06/08

الملخص:

في ظل عصر السرعة والثورة المعلوماتية لا يمكن إنكار أهمية الانترنت، لأنها أحد دعائم تكنولوجيا الاتصال والمعلومات، ومع ذلك فإن لها آثار سلبية، فقد تسببت في ظهور نوع جديد من الجرائم المعلوماتية، والتي نجد من بينها جرائم التجسس على الآخرين سواء كانوا أشخاص طبيعيين أو اعتباريين.

وقد تطورت عمليات التجسس طبقا لما يسود المجتمع من تطورات علمية وتكنولوجية وتقنية، فظهر بذلك ما يعرف اليوم بالتجسس الإلكتروني، الذي تختلف خطورته بحسب ما إذا كان موجها ضد الأشخاص العاديين (الطبيعيين) أو الأشخاص الاعتباريين، فمع توسع التجارة الإلكترونية عبر شبكة الإنترنيت تحولت الكثير من مصادر المعلومات إلى أهداف للتجسس، ونظرا لخطورة هذه الجريمة سواء على المستوى الداخلي أو الدولي، سيتم من خلال هذا المقال إبراز سبل مكافحتها، والتخفيف من وطأتها.

الكلمات المفتاحية: التجسس الإلكتروني، شبكة الانترنت، المعاملات الإلكترونية، الجرائم الإلكترونية، النظام الإلكتروني.

Abstract:

In the age of speed and information revolution, the importance of the Internet cannot be denied, because it is one of the pillars of information and communication technology.

Espionage operations have evolved according to the prevailing scientific, technological and technological developments in society. Sources of information to targets of espionage, and given the seriousness of this crime,

* المؤلف المرسل.

both domestically and internationally, through this article will highlight ways to combat, and mitigate.
Key words: Cyber-espionage, Internet, Electronic transactions, Cybercrime, Electronic system.

1. مقدمـة

إن عمليات التجسس والتنصت من أجل الحصول على المعلومات هي عمليات قديمة قدم البشرية، وقدم النزاعات بينها فمنذ عصور مضت كان الإنسان يتجسس على أعدائه لمعرفة أخبارهم، والخطط التي يعدونها لمهاجمته ولهذا كان للتجسس أهميته الكبرى على كافة مستويات النزاعات الإنسانية التي مر بها البشر منذ بدء الخليقة، إلا أنه وبظهور عصر المعلومات والاتصالات وازدهاره تحولت وسائل التجسس والتنصت من الطرق التقليدية إلى الطرق الإلكترونية، لاسيما مع استخدام شبكة الانترنت وانتشارها الواسع عربيا وعالميا.

ويرتبط التجسس الإلكتروني بالتطورات التي تحدث في مجتمع المعلومات، فهو يزداد خطورة كلما زاد التقدم في المجال المعلوماتي، فالاكتشاف والتطور والبناء حتما يقابله التجسس والتخلف والهدم، فالدمار الذي قد يلحقه التجسس الالكتروني بأنظمة المعلومات التي تتحكم في كل مرافق الحياة في هذه المجتمعات التي تعتمد على الكمبيوتر والإنترنت اعتمادا مطلقا قد يعطل حياة مجتمعات بأكملها، والخسائر التي قد تنجم عن مثل هذا التجسس هي أكبر بكثير مما قد يتصوره العقل إذا لم يدرس ويخطط لوقوعه.

لذا لابد من دراسة هذا الأمر دراسة مبكرة والأخذ بالاعتبار أسوأ المخاطر المحتملة التي تترتب عليه، حتى نبني تقنياتنا وحضارتنا بشكل آمن متوازن، وكذلك ضرورة التعاون بين الدول في إنشاء مراكز وطنية تهتم بقضايا التجسس الإلكتروني والجرائم الإلكترونية التي اكتسحت عالم الإنترنت والتقنية ودراستها من النواحي التشريعية والقانونية وبيان أثرها السياسي والاقتصادي والاجتماعي، وكذلك توفير أشخاص ذوو خبرة في مجال التقنية للتصدي لمثل هذه الهجمات في أي وقت أو مكان، وذلك حتى نحد من هذه الاعتداءات وننعم بمجتمع ومنشآت ومؤسسات محمية من هذه الاعتداءات.

ولخطورة التجسس الالكتروني على المجتمعات الإنسانية ارتأينا من خلال هذا المقال، البحث في سبل مكافحته والتخفيف من وطأته على المستوى الوطني والدولي، من خلال محاولة الإجابة عن الإشكالية التالية:

ما مدى نجاعة التشريعات الوطنية والدولية في مجابهة التجسس الالكتروني؟

وللإجابة عن الإشكالية السابق ذكرها تم توخي خطة البحث التالية:

- مفهوم التجسس الإلكتروني
- مخاطر التجسس الإلكتروني وأساليب مكافحته

وفي دراسة موضوع التجسس الإلكتروني تم الاستعانة بمنهجين لتناسبهما مع طبيعة الموضوع وهما المنهج الوصفي، الذي تم من خلاله إعطاء وصف دقيق للظاهرة وبيان عناصرها وتجلى ذلك بشكل واضح من خلال القسم الأول من الدراسة، وتم أيضا الاستعانة بالمنهج التحليلي، لأن دراسة الموضوع تطلبت الاطلاع على النصوص القانونية المختلفة سواء منها الوطنية أو الدولية، أين تم تحليلها للوقوف على عناصر التجريم والعقوبات المقررة لجريمة التجسس الإلكتروني، وهذا ما تجلى بشكل واضح في القسم الثاني من الدراسة.

2. مفهوم التجسس الإلكتروني

في ظل التطور الهائل الذي شهده مجال الإعلام والاتصال والذي رافقه التطور الكبير في تكنولوجيات الحواسيب والأجهزة الذكية، أدى ذلك إلى ظهور أدوات واختراعات وخدمات جديدة نتج عنها نوع جديد من المعاملات يسمى بالمعاملات الإلكترونية والتي يقصد بها كل المعاملات التي تتم عبر أجهزة إلكترونية مثل الحاسوب، شبكة الانترنيت، الهاتف المحمول (الهواتف الذكية)، ونتيجة التطور الكبير والسريع لهذه الأجهزة وضعف القدرة على المرافقة والمراقبة والتحكم، ظهر نوع جديد من الجرائم يسمى بالجريمة الإلكترونية أو المعلوماتية أو التقنية، والتي هي عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي أو الهواتف الذكية الموصولة بشبكة الانترنيت بطريقة مباشرة أو غير مباشرة لتنفيذ الفعل الإجرامي. وأصبحت هذه الجرائم في وقتنا الراهن تهدد أمن وسلامة الأفراد أو المؤسسات أو حتى الحكومات،[1] والتي نجد من بينها جريمة التجسس الإلكتروني أو المعلوماتي، سنتطرق من خلال هذا العنوان لتعريف التجسس الإلكتروني، ثم بيان خصائصه.

أ. التعريف القانوني للتجسس الإلكتروني:

تعد شبكة الانترنت أحد تقنيات المعلوماتية والاتصالات في العصر الحالي، لما لها من دور كبير في نشر المعلومات بين البشر في كافة أنحاء العالم، وظهرت الشبكات العملاقة التي تعمل في مجال صناعة الشبكات، وأصبح هناك تنافس شديد بين هذه الشركات، وقد ساهمت هذه الشبكة في تطوير الفكر والثقافة وإحداث التقارب بين شعوب العالم. وبالتالي لا يمكننا

نكران الفوائد التي عادت على العالم من وراء هذه الشبكة. أي هناك فوائد إيجابية، لكن مع مرور الزمن ظهر الجانب السلبي للشبكة.

وذلك مع بزوغ فجر الثورة المعلوماتية، وتوسع استخدام شبكة الانترنيت وبدأ استخدامها في المعلومات التجارية ودخول جميع فئات المجتمع إلى قائمة المستخدمين، فبدأت تظهر أنماط إجرامية مستحدثة على هذه الشبكة.[2]

فالتجسس نمط من أنماط السلوك الإنساني رافق نشوء المجتمعات منذ القدم وتطور بتطورها حتى غدا له في عصرنا الحاضر شأن كبير وأهمية بالغة، وهو قديم قدم البشرية فقد عرفه الفراعنة، وكذلك الصينيون فيقول حكيمهم "سان سو":" إن ما يمكن الملك الحكيم والقائد الصالح من إنزال الضربة والانتصار وبلوغ ما يتجاوز حدود الرجل العادي هو المعلومات السابقة"، ولم تزدهر الجاسوسية وتنظم إلا مع بداية الحرب العالمية الثانية، فلم يعد التجسس قاصرا على الأسرار بل تعداه إلى المعلومات الصناعية والعلمية، وأسهم بذلك التقدم العلمي وبلوغ أجهزة التجسس درجة عالية من الكفاءة.[3]

والمعنى الاصطلاحي للتجسس يأتي في سياق المعنى اللغوي ولم يخرج عنه، فقد عرفه الغزالي بقوله:" طلب الأمارات المعرفة"، والجاسوس هو شخص يرسله الإمام ليطلع على عورات العدو ويعلم حالهم، وقد ورد التجسس صراحة في القرآن الكريم في قولة تعالى:" يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَاتَّقُوا اللَّهَ ۚ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ ." (الحجرات: 12) والنهي وإن كان موجها لآحاد المسلمين عن تتبع عورات المسلمين والبحث عنها دون مسوغ شرعي، إلا أنه يتناول الجماعات والمؤسسات والدول أيضا بأي صورة أو سبب غير مشروع يهدف إلى كشف أسرار الأفراد أو الجماعات أو الدول.[4]

إن التجسس الإلكتروني هو التلصص وسرقة المعلومات من الأفراد أو المؤسسات أو الدول أو المنظمات، والتجسس على هذه المعلومات أيا كان نوعها يأخذ أبعادا جديدة، فتعددت أهدافها من معلومات اقتصادية إلى معلومات سياسية وعسكرية وشخصية.[5]

ولا يختلف التجسس الإلكتروني عن التجسس التقليدي إلا في الأداة المستخدمة وهي تكنولوجيا المعلومات التي وفرت للجاسوس الإلكتروني الحرية والسهولة في التجسس بعيدا عن أعين الرقيب، وقد تباينت تعريفات القانونيين للتجسس الإلكتروني بين جعله عاما يشمل الأفراد والجماعات والدول، وبين حصره في نطاق الدولة وأسرارها فقط دون الأفراد، ولذلك

عرفه الفريق الأول بأنه:" الإطلاع على معلومات خاصة بالغير محفوظة على جهاز إلكتروني وليس مسموحا لغير المخولين بالاطلاع عليها"، بينما عرفه الفريق الثاني بأنه:" استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الإلكترونية الخاصة بالدول والحكومات والتنصت عليها بقصد الحصول على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها، تشمل جميع المعلومات العسكرية والأمنية، والسياسية، والاقتصادية، والعلمية، والاجتماعية".[6]

وعليه فجرائم التجسس الإلكتروني تشمل اختراق المواقع والصفحات الإلكترونية على الانترنيت بغرض التجسس أو التنصت على ما تحتويه من بيانات ومعلومات (نصية، أو صوتية، أو مرئية) تهم الجهة المستفيدة من التجسس (جهات اقتصادية وتجارية، أو سياسية، أو أمنية). كذلك إرسال رسائل بريد إلكترونية لمستخدمي الانترنت تتضمن على ملفات برمجية لديها القدرة على الإرسال بشكل آلي للمعلومات المتوفرة على جهاز المستخدم من ملفات (نصية، أو صوتية، أو مرئية). كما لديها القدرة على إرسال أي معلومات تتعلق بمستخدم الانترنيت مثل سجل زياراته لمواقع الانترنت والبيانات التي يدخلها المستخدم في مواقع الانترنيت كاسم المستخدم وكلمة السر، بالإضافة إلى كلمات البحث التي يدخلها المستخدم في محركات البحث العالمية، واستخدام البرامج المتخصصة باختراق أجهزة الحاسبات الآلية المرتبطة بالانترنت بهدف التجسس على ما تحتويه من معلومات وبيانات.[7]

وتجدر الإشارة في هذا المجال إلى أن جريمة التجسس المعلوماتي بمختلف صورها يمكن أن ترتكب بأي وسيلة، ومنها أبواب المصيدة (الأبواب الخلفية أو الخفية)، وهي ممرات خالية متروكة في برنامج ما، فالبرامج في نسختها الأولى تحوي على ثغرات وعيوب فنية معينة، أو أن هذه الثغرات قد تركت عمدا من قبل صانعو هذه البرامج، لينفذوا من خلالها إلى النظام المعلوماتي للتجسس على معلومات المؤسسات.[8]

إن البعض لا يرى بأن هناك فرق بين التجسس الإلكتروني وبين القرصنة الإلكترونية فكلاهما عبارة عن ممارسات غير مشروعة تتم عبر شبكة الانترنت، وتستهدف المعلومات الموجودة في أجهزة الحاسب الآلي، غير أن الكثير من فقهاء القانون يتجهون إلى التفريق بينهما من حيث الجهة المنفذة لكل منهما في الغالب ومقدار الخطر المترتب بواسطتهما.[9]

ب. خصائص التجسس الإلكتروني وصوره:

تتمثل أهم خصائص التجسس الإلكتروني في ما يلي:

- التجسس الإلكتروني لا يترك أي دليل مادي بعد ارتكاب الفعل الإجرامي ما يصعب معه عملية التعقب واكتشاف الجريمة أساسا.
- إن التجسس الإلكتروني يحدث في بيئة هادئة لا تحتاج إلى القوة والعنف واستعمال الأسلحة، وإنما ما يحتاجه هو جهاز كمبيوتر وبعض البرامج وشبكة انترنت.
- سهولة محو وإتلاف الأدلة التي من شأنها أن تؤدي إلى العثور واكتشاف مرتكب الفعل الجرمي والتمكن من إدانته.
- إن مستخدمي هذا النوع من التجسس يمتازون بخبرات وتقنيات هائلة في استخدام الأجهزة الإلكترونية الحديثة، من جهة أخرى نجد نقص إلى حد ما في الخبرات لدى الجهات الأمنية المعنية بالكشف عن هذه المخططات وكبحها.[10]

لقد أصبح التجسس في العصر الحالي شاملا لمختلف المجالات فلم يعد يقتصر على النواحي العسكرية والحربية، وإن كان هذا النوع من التجسس يمثل أهم أنواع التجسس وأخطرها، إلا أن المعلومة المطلوبة الآن تختلف عنها في الماضي، فلم تعد أعداد الجيوش وتجهيزاتها التقليدية من الأمور السرية، بل إننا نجد أن مثل هذه المعطيات تتداولها صفحات الصحف والبرامج التلفزيونية، عندما يحدث أزمة في منطقة معينة ويتم إرسال خرائط تمثل حجم القوات في الدول المجاورة لمناطق الصراع.

ولكن هناك تجسس عسكري يكون بصورة عميقة خاصة بين الدول الكبرى، فتسعى هذه الدول للحصول على أسرار حربية تكنولوجية، لكي تقف على مدى التقدم الذي وصلت إليه غيرها من الدول.[11]

ولقد سهلت شبكة الانترنت الأعمال التجسسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلوماتية ثلاث أهداف رئيسية وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي.[12]

ومن أهم ما يندرج تحت مسمى جرائم التجسس الإلكتروني ما يلي:

- **جرائم التجسس الاقتصادية والتجارية:** وهي جرائم التجسس التي يكون الهدف منها الحصول على معلومات اقتصادية وتجارية.

- **جرائم التجسس العسكرية والأمنية والسياسية:** وهي جرائم التجسس التي يكون الهدف منها الحصول على معلومات عسكرية أو أمنية أو سياسية.
- **جرائم التجسس الثقافية والتعليمية:** وهي جرائم التجسس التي يكون الهدف منها الحصول على معلومات ثقافية وتعليمية، ومن أمثلتها التجسس على الأبحاث والمخترعات والدراسات العلمية والتعاون الثقافي والتعليمي بين الدول.[13]

فلا يمكن حصر التجسس الإلكتروني في نطاق الدول والجماعات فقط لاسيما وأن التجسس على الأفراد قد يشكل أهمية قصوى للجهة المتجسسة نتيجة للأسرار البالغة الحساسية التي يحتفظون بها، فضلا عن أن الكثير من الجماعات الإرهابية قد تعول على المعلومات الشخصية للأفراد في سبيل استقطابهم وتجنيدهم ضمن تنظيماتهم وجماعاتهم الإرهابية.[14]

قد يكون التجسس سياسيا لمعرفة المواقف السياسية لصناع القرار في الدولة والمعلومات التي تتعلق بالسياسة الداخلية والخارجية المتبعة، أو التي تنوي الدولة السير عليها. وقد يكون التجسس معنويا ونفسيا لشعوب الدول وقادتها ومعرفة مواطن القوة والضعف في شخصية أفراد الشعب، وعوامل الوحدة والتفرقة والقيم السائدة في المجتمع، التيارات الحزبية والدينية ومدى تأثيرها في الأزمات، ومقدار العزيمة لدى شعب دولة ما، فالحرب المعنوية من أهم الحروب فمن خلال هذه المعلومات تستطيع الدولة المعادية استخدام السلاح المعنوي وتحطيم الروح المعنوية للشعب مما يسهل عليها كسب المعركة.[15]

وهناك تجسس اقتصادي لمعرفة موارد الدولة وحجم إنتاجها، وميزانها التجاري والاحتياطي لديها، والمدة التي تستطيع خلالها الاعتماد على ذاتها إذا تم حصارها، وكذلك معرفة المرافق الاقتصادية الحيوية لديها ومواقعها وكذلك ديونها الخارجية.

كما أن التجسس قد ينصب على المعلومات الصناعية والعلمية من خلال معرفة أسرار الصناعات والأبحاث العلمية، خاصة إذا كانت هذه الصناعات تتعلق بالدفاع الوطني، فهناك شركات تسهم في الإنتاج الحربي وتطوير الأسلحة، وقد يكون التجسس العلمي لمعرفة الدراسات العلمية في المجالات الزراعية، أو الهندسية، أو الصحية.[16]

ومن خلال ما سبق يتجلى لنا بأن جميع المعلومات السرية سواء كانت عسكرية أو سياسية أو اقتصادية من الممكن أن تكون على شكل محتوى إلكتروني، وحتى لو كان هذا المحتوى محاط بوسائل الأمن المعلوماتي، فإن المخزون الإلكتروني الموجود فيه عرضة

للتجسس الإلكتروني على تلك المعلومات واختراقها والحصول عليها وإفشاءها، خاصة وأن جميع دول العالم بعد التطور التكنولوجي الذي طرأ على أنظمة المعلومات أصبحت تعتمد على أجهزة الحاسب الآلي، والشبكة المعلوماتية في تسيير أمورها الداخلية والخارجية، حيث أصبح الحاسب الآلي أداة ضرورية لا يمكن الاستغناء عنها، من أجل حفظ البيانات والمعلومات والوثائق الخاصة بكل دولة، كما أن هذه المعلومات ذات أهمية كبيرة فهي تمس أمن الدولة وعلى درجة كبيرة من الخطورة.[17]

ج. أركان جريمة التجسس الإلكتروني

لقد نصت المادة الثالثة من اتفاقية بودابست المبرمة في 23 نوفمبر 2001م بشأن الجريمـة الإلكترونيـة على بعض صـور جرائـم التجسس الإلكـتروني، والتي يمكـن إجمالها في صورتين:

- جريمة الاعتراض غير القانوني لانتقال البيانات
- جريمة الولوج والبقاء غير المشروع في نظام المعالجة الآلية للبيانات[18]

وسنحاول أن نبين الركن المادي والمعنوي لجريمة التجسس الإلكتروني وفقا للصورتين السابق ذكرهما:

فالركن المادي في جريمة التجسس الإلكتروني عبارة عن السلوك الجرمي الذي يتبعه المجرم في جمعه للمعلومات المهمة والحساسة، بطريقة غير مشروعة وباستخدام وسائل تقنية المعلومات لتحقيق النتيجة التي يصبو إليها، والمتمثلة في استخدام هذه المعلومات لأغراض إرهابية ضد الدول أو المؤسسات أو الأفراد، ولا يتصور السلوك الجرمي في هذه الجريمة بدون وجود الوسائل التي ينتهجها ويستخدمها المجرمون للتجسس والحصول على المعلومات والأسرار، والمجالات التي يركز عليها مجرمو التقنية في تجسسهم. [19]

يتمثل الركن المادي في جريمة الاعتراض غير القانوني للبيانات في فعل الاعتراض، والذي يقوم به الجاني في الجريمة بدون وجه حق باستخدام الوسائل الفنية غير العلنية، وهذا يفترض توافر عدة شروط نصت المادة الثالثة من اتفاقية بودابست عليها، إلا أنها أجازت للدول الأعضاء إضافة شروط أخرى في حالة تجريمهم لفعل الاعتراض غير القانوني للبيانات في قوانينهم الداخلية.

ويشترط في فعل الاعتراض أن يتم باستخدام وسائل فنية غير علنية، كذلك يجب أن يتم فعل الاعتراض بدون حق.[20]

والصورة الثانية لجريمة التجسس الالكتروني المذكورة في الاتفاقية السابق ذكرها، هي جريمة الدخول في نظام المعالجة الآلية للبيانات، فقد أشارت إلى خطورتها باعتبارها تشكل تهديدا لأمن وسلامة النظم والبيانات والمعلومات، خاصة وأن هناك حاجة ضرورية لتوفير حماية ملائمة لمصالح المنظمات، وبالأخص لرجال الإدارة حتى يكون بمقدورهم أن يديروا ويستثمروا، ويتحكموا في أنظمتهم بدون تشويش أو عقبة من أي نوع، ولقيام الولوج والبقاء غير المشروع في أنظمة المعالجة الآلية للبيانات لابد من توفر ثلاثة شروط وهي:

- ضرورة وجود نظام معالجة آلية للبيانات
- أن يكون هذا النظام مشمولا بنظام حماية
- أن يكون الولوج بدون حق أو سند من القانون أو بناء على عقد أو اتفاق.[21]

والسلوك في جريمة الولوج غير المصرح به سلوك إيجابي أو ما يطلق عليه بالفعل وهو الذي يتمثل في فعل الدخول، والسلوك الإيجابي عبارة عن حركات إرادية من شأنها أن تحدث تغييرا في العالم الخارجي، وهذا التغيير يكون ملموسا في العالم المعلوماتي بالنسبة لجريمة الدخول.[22]

وتعتبر جريمة التجسس الإلكتروني من الجرائم العمدية التي تتطلب قصدا عاما يتمثل في العلم والإرادة، علم الجاني بأنه يأتي فعلا مخالفا للقانون، وذلك بولوجه إلى نظام إلكتروني بطريقة غير مصرح بها وإطلاعه على معلومات سرية تتعلق بالاقتصاد أو الأمن والدفاع أو السياسة أو السكان لبلد ما، فالجاني يعلم بأنه يعتدي على حق حماه القانون وعاقب على انتهاكه يتمثل في معلومات ووثائق سرية لا يحق له الاطلاع عليها، وتكون إرادته متجهة إلى إحداث النتيجة الجرمية المقصودة المتمثلة في دخول النظام الإلكتروني بغير حق والاطلاع على معلومات سرية حماها القانون وغير متاحة للجمهور، كما تتطلب هذه الجريمة قصدا خاصا يتمثل في قصد الجاني من دخوله إلى النظام الالكتروني المحمي الاطلاع على معلومات سرية لا يجوز له الاطلاع عليها.[23]

وجريمة الاعتراض غير القانوني للمحادثات الشخصية، ولنقل البيانات المعلوماتية من الجرائم العمدية التي يتطلب فيها القصد الجنائي بشقيه العلم والإرادة، فلابد أن يعلم الجاني أنه يقوم بالتصنت على المكالمات والأحاديث الشخصية وتسجيل ونقل البيانات المعلوماتية

بغير رضا أطراف الاتصال أو سند من القانون وإلا انتفى عنصر العلم وبالتالي لا قيام للركن المعنوي، كذلك لابد أن تتجه إرادة الجاني إلى إتيان السلوك المادي الذي يشكل جريمة الاعتراض كالتصنت والنقل...فإذا ما أكره من طرف الآخرين على ذلك لما لديه من خبرة ومهارة في استخدام أجهزة التصنت أو التسجيل، أو كان دخوله غير إرادي عن طريق المصادفة المحضة، أو تحت تأثير أي من وسائل الدفع والإكراه المعنوي والمادي الأخرى نحو الجريمة فإنه لا قيام للقصد الجنائي، وبالتالي لا جريمة.[24]

كما تعتبر جريمة الدخول غير المشروع لنظام المعالجة الآلية للبيانات من الجرائم العمدية، يتطلب لقيامها القصد الجنائي بعنصريه العلم والإرادة، العلم بمكونات الجريمة والإرادة المتجهة إلى ارتكاب السلوك الإجرامي لهذه الجريمة.

فلابد أن يلم الجاني بكل واقعة يتطلبها القانون لبناء أركان الجريمة واستكمال عناصرها، فضلا عن ذلك لابد أن يشمل العلم أيضا التكييف الذي تتصف به بعض هذه الوقائع وتكتسب به أهميتها في نظر القانون، وأن يعلم بخطورة الفعل الذي يقوم به على المصلحة التي يحميها القانون، كما يتطلب القصد الجنائي لجريمة الدخول غير المشروع لنظم المعالجة الآلية للبيانات، أن تتجه إرادة الجاني إلى فعل الدخول وإلى النتيجة الإجرامية، وهي الاطلاع أو التجول خلال المواقع والمعلومات والأسرار المعلوماتية بدون حق.[25]

3. مخاطر التجسس الإلكتروني وأساليب مكافحته

إن تطور الحضارة يعتمد على الاقتصاد، وعالم الاقتصاد تطور بتطور الحضارة البشرية، فكل حقبة زمنية طويلة تتميز عن غيرها، فأساس الاقتصاد الأول لحضارات العالم اعتمد على الملكية والزراعة لذا كانت الجرائم الاقتصادية تتمحور حول الزراعة، وفي عصر النهضة بل وحتى وقتنا الحالي مازالت الصناعة وعالم الشركات متعددة الجنسيات يلعب دورا مؤثرا وحيويا في الاقتصاد العالمي، وتوجد جرائم اقتصادية تتعلق بسرقة الاختراعات والتجسس الاقتصادي، ومخالفة أنظمة الدول بل وتطور الأمر إلى جرائم عابرة للقارات فيما عرف بغسل الأموال وتمويل الإرهاب.[26]

أ. مدى خطورة التجسس الإلكتروني

لقد تغيرت أدوات وأساليب التجسس وذلك نتيجة للثورة التكنولوجية والمعلوماتية في مجال الاتصالات، فأصبح العالم قرية صغيرة، وأصبحت كل المعلومات السياسية

والاقتصادية وأحيانا العسكرية معلومة للكافة، وبعد أن أصبحت الولايات المتحدة الأمريكية القوة العظمى الوحيدة في العالم فإنها تعمل جاهدة على التجسس على كل دول العالم للحفاظ على تفردها بقيادة العالم، ولأنها أكثر تقدما فإن لها قدرات خارقة على التجسس من خلال أقمار التجسس ومحطات التنصت الضخمة وحاملات الطائرات المرتبطة بالأقمار الصناعية، وتعد السفارات مراكز تجسس مشروعة فكل الدول تعتمد على سفاراتها في الحصول على معلومات عن البلد الذي توجد فيه السفارة وفي كافة المجالات، وترصد ميزانيات بأرقام خيالية للقيام بذلك من الدول الكبرى، وأكثر الدول التي تتجسس دبلوماسيا الاتحاد السوفياتي سابقا والولايات المتحدة الأمريكية.[27]

ففي عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن حدود الدولة مستباحة بأقمار التجسس والبث الثقافي، ولقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الالكترونية خاصة مع استخدام الانترنت وانتشاره عالميا.

ولا يقتصر الخطر على محاولة اختراق الشبكات والمواقع على العابثين من مخترقي الأنظمة، فمخاطر هؤلاء محدودة وتقتصر غالبا على العبث أو إتلاف المحتويات، والتي يمكن التغلب عليها باستعارة نسخة أخرى مخزنة، أما الخطر الحقيقي فيكمن في عمليات التجسس التي تقوم بها الأجهزة الاستخبارية للحصول على أسرار ومعلومات الدولة ثم إفشاءها لدولة أخرى تكون عادة معادية، أو استغلالها بما يضر المصلحة الوطنية للدولة.[28]

ولا تكمن الخطورة في استخدام الانترنت ولكن ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات، وتشارك في تلك العمليات شبكة إشيلون المستخدمة في التجسس على المكالمات ورسائل الفاكس والبريد الإلكتروني. ويندرج تحته الاقتناء عن طريق وسائل غير مشروعة أو الإفشاء أو النقل أو الاستعمال بدون وجه حق أو مبرر قانوني.[29]

ويمكن القول على أن التجسس الإلكتروني يرتبط بشكل واضح بالتطورات التي تحدث في البيئة الرقمية، فهو يزداد خطورة كلما ازداد التقدم في المجال المعلوماتي، فالتطور والاكتشاف والبناء حتما يقابله التخلف والتجسس والهدم.

فالتجسس الإلكتروني يعتمد على برامج تقوم بالتتبع والاطلاع على سلوك الجهاز من الكتابة إلى مراقبة المواقع التي يزورها المستخدم وذلك لسرقة معلومات سرية، ومراقبة وتسجيل جميع التحركات والأفعال التي تتم على جهاز، فبعد أن يتم تثبيت البرنامج

على جهاز الكمبيوتر، يقوم البرنامج بإخفاء نفسه من النظام بحيث يصعب على المستخدم اكتشاف وجوده.[30]

والجدير بالذكر أن عمليات التجسس، أصبحت اليوم كما يقول بعض الخبراء من أهم وأخطر الأسلحة بيد العديد من الأفراد وكذا الدول والحكومات، التي تسعى من خلال هذه العمليـات إلى الكشف عن معلومات إضافية تمكنها من تحقيق انتصارات جديدة خصوصا مع اتسـاع رقعـة الخلافـات الفرديـة وتزايد الأزمات الدولية التي أفقدت العالم الثقة بكل شيء تقريبا، فالتجسس الإلكتروني كما يقول بعض المراقبين هو نوع جديد من حروب السيطـرة على الأشخـاص والدول، ازدادت وتيرته بشكل كبير في ظل التطور التقني الهائل الذي نعيشه.[31]

ويشكل التجسس الإلكتروني خطورة على الإدارة الإلكترونية هو تعرض أرشيفها الإلكتروني لمخاطر كبيرة تكمن في التجسس على هذه الوثائق وكشفها ونقلها وحتى إتلافها، لذلك فهناك مخاطر كبيرة من الناحية الأمنية على معلومات ووثائق وأرشيف الإدارة سواء المتعلقة بالأشخاص أو الشركات أو الإدارات أو حتى الدول.[32]

ومصدر خطر التجسس الإلكتروني في هذا المجال يأتي غالبا من ثلاث فئات:

- الفئة الأولى هي الأفراد العاديين؛
- الفئة الثانية هي الهاكرز (القراصنة)؛
- الفئة الثالثة هي أجهزة الاستخبارات العالمية للدول.[33]

فالتجسس الالكتروني يتم من خلاله اختراق الأجهزة والقيام بعملية التجسس على المستخدم بطرق غير شرعية ولأغراض غير سوية كي يسرق معلومات تتعلق به سواء على الصعيد الشخصي أو السياسي، أو العملي أو الاجتماعي أو لسرقة حسابه، أو بهدف التخريب، أو بهدف معرفة معلومات تتعلق بالجانب المادي وغيرها من الجوانب الأخرى، حيث لم يعد هناك سرية يمكن الاحتفاظ بها من دون أن يقوم الشخص بعمليات كثيرة لتجنب عمليات التجسس أو "الهاكرز"، وكشفت الوثائق أن وكالة الأمن القومي الأمريكية تجسست على حوالي 125 مليار اتصال هاتفي، ورسائل نصية في فترة شهر جانفي من العام 2013، وكانت غالبيتها من دول شرق أوسطية.[34]

ومن خلال ما سبق بيانه عن مخاطر التجسس الالكتروني يتبين لنا بأن غاياته وأهدافه تتجلى من خلال ما يلي:

- زعزعة الأمن ونشر الخوف والرعب في نفوس الأفراد وكذا الدول والحكومات، بحيث يصبح الفرد وكذا الدول والحكومات في قلق تام بشأن معلوماته السرية التي لا ترغب في إطلاع أحد عليها؛
- تهديد وابتزاز الأشخاص والسلطات العامة والمنظمات الدولية، بموجبها يصبح الفرد تحت رحمة المتجسس، الذي يطلب أموال طائلة بغية الحفاظ على سرية المعلومات التي توصل إليها؛
- السطو وجمع الأموال، إما انتقاما من الشخص أو الدولة المعنية، وإما بحثا عن الثراء السريع، أو التحكم في الأنشطة الاقتصادية؛ [35]
- الاطلاع على معلومات سرية لصفقة أو مناقصة أو أصول تسويقية خاصة والاستفادة منها؛
- اختراق الموقع الالكتروني الخاص بالشركة.[36]

وفي هذا الصدد لابد من الإشارة إلى أن زعماء "بريكس" يصفون التجسس الإلكتروني بأنه نوع من الإرهاب، إذ صرح المتحدث الرسمي باسم الكرملين دميتري بيسكوف أن زعماء مجموعة "بريكس" قدموا تقييما شديد اللهجة لوقائع التجسس بما في ذلك التجسس الإلكتروني ووصفوه بأنه إرهاب، وأكد زعماء المجموعة على ضرورة ألا تشكل الحرية في الفضاء الإلكتروني الكمبيوتري خطرا على الأمن.[37]

ب. تجريم التجسس الإلكتروني في المواثيق الدولية والتشريعات الوطنية

في ظل التطور الهائل الذي يشهده العالم في مجال تقنية المعلومات أصبحت الحاجة ماسة وضرورية إلى حماية المعلومات الإلكترونية خاصة ما يتسم منها بطابع السرية، حيث برزت العديد من الجرائم الإلكترونية التي لم تكن موجودة في السابق، ولعل التجسس الإلكتروني يأتي في مقدمة هذه الجرائم التي وضعت المجتمع الدولي في تحد كبير للحد منه على أقل تقدير.[38]

ومع ظهور أنظمة المعلومات الإلكترونية أصبحت الحاجة ماسة إلى حماية هذه المعلومات، من أن تطالها يد المجرمين من العابثين والإرهابيين وأجهزة الاستخبارات المعادية، الأمر الذي دفع بالكثير من الدول إلى تعديل قوانينها وخاصة تلك التي تتعلق

بالتجسس والدفاع عن أمن الدولة، والانضمام إلى الاتفاقيات الدولية التي تعالج جرائم تقنية المعلومات الحديثة. (39)

ولقد بذلت الأمم المتحدة مجهودات كبيرة في مجال مكافحة استعمال تكنولوجيا المعلومات لأغراض إجرامية، حيث أصدرت الجمعية العامة قرارها رقم 63/55 بتاريخ 04 ديسمبر 2000، والمعنون بـ: مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية،حيث أعربت فيه عن قلقها إزاء الإمكانيات الجديدة التي يتيحها التقدم التكنولوجي للنشاط الإجرامي، ولا سيما إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، ولقد أقرت الجمعية العامة جملة من التدابير في هذا المجال نذكر منها:

- ينبغي للدول أن تكفل عدم توفير قوانينها وممارساتها ملاذا آمنا للذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية.
- ينبغي للنظم القانونية أن تحمي سرية البيانات ونظم الحواسيب وسلامتها وتوافرها، من أي عرقلة غير مأذون بها، وأن تضمن معاقبة من يقوم بإساءة استعمالها لأغراض إجرامية.(40)

على الرغم من عدم وجود سلطة قانونية عليا مباشرة تحكم استخدام الفضاء الإلكتروني، أو تمنع ممارسة أنشطة التجسس على الدول من خلاله، فإن هناك بعض الاتفاقيات والمعاهدات الدولية التقليدية التي تمنع أو تنظم عملية التجسس التقليدية، ويمكن أن ينسحب عليها تشريعيا ممارسة هذا النوع من التجسس عبر الانترنت. (41)

ومن بين الاتفاقيات الدولية نجد الاتفاقية الأوروبية لمكافحة جرائم الانترنت (اتفاقية بودابست 2001) التي نصت على:" يقوم كل طرف من الدول الأطراف في الاتفاقية بإقرار هذه الإجراءات وغيرها من الإجراءات الأخرى كلما كان ذلك ضروريا لإصدار نص قانوني أو تشريعي بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها، وذلك من حيث اعتراض خط سير البيانات دون وجه حق ويتم ذلك بالوسائل الفنية لقطع عمليات البث والإرسال غير العمومية لبيانات الكمبيوتر إلى أو من أو داخل منظومة الكمبيوتر بما في ذلك ما ينبعث من منظومة الكمبيوتر من موجات كهرومغناطيسية تحمل معها البيانات..." (42)

لقد عالجت الاتفاقية تسع جرائم منها: الدخول غير القانوني المتعمد، والاعتراض غير القانوني، كما أوجبت على الدول الأعضاء اتخاذ التدابير التشريعية اللازمة لتضمين قوانينها موضوع المسؤولية عن الشروع والتحريض والتدخل في ارتكاب هذه الجرائم من قبل

الأشخاص الطبيعية أو المعنوية، والملاحظ أن هذه الاتفاقية لم تنص صراحة على جريمة التجسس الالكتروني بمفهومها المتعارف عليه، بل أوردتها ضمن نصوص المواد التي تتعلق بالدخول والاعتراض غير المصرح بهما الأمر الذي يفتح المجال للتأويلات المختلفة على نحو يكرس لمفهوم المصالح وتجاذباتها السياسية عند تطبيق نصوص الاتفاقية.[43]

ومن خلال قرار الجمعية العامة 247/74 المعتمد في 27 ديسمبر 2019، قررت إنشاء لجنة خبراء حكومية دولية مخصصة مفتوحة العضوية ممثلة لجميع المناطق، لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، مع المراعاة التامة للصكوك والجهود الدولية القائمة على المستويات الوطنية والإقليمية والدولية بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، ولا سيما عمل ونتائج فريق الخبراء الحكومي الدولي المفتوح العضوية لإجراء دراسة شاملة عن الجريمة السيبرانية.[44]

وفقا للقرار السابق ذكره فاللجنة المخصصة مكلفة بوضع الاتفاقية من أجل الوفاء بولايتها، ويجوز لها النظر في عقد ثماني دورات في فيينا، من أوت 2021 إلى نهاية جوان 2024، لوضع الاتفاقية والموافقة عليها وتقديم مشروع قرار إلى الجمعية العامة للنظر فيه في دورتها التاسعة والسبعين المقرر عقدها في عام 2024[45].

وبالنسبة للتشريعات الوطنية نجد مثلا التشريع الأردني نص على جرائم التجسس في المواد من 114 إلى 116 من قانون حماية أسرار ووثائق الدولة لسنة 1971 وهي جريمة الدخول أو محاولة الدخول إلى أماكن محظورة بقصد الحصول على أسرار تتعلق بسلامة الدولة، وجريمة سرقة الأسرار التي تتعلق بسلامة الدولة أو الحصول عليها وجريمة إبلاغ الأسرار المتعلقة بأمن الدولة أو إفشاؤها دون سبب مشروع، كذلك نصت المادة 12 من قانون الجرائم الإلكترونية لسنة 2015 على جرائم التجسس الإلكتروني باعتبارها جريمة تمس ببيانات أو معلومات (محتوى إلكتروني) غير متاحة للجمهور تمس بالأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني.[46]

أما القانون العماني المعني بموضوع التجسس الإلكتروني هو قانون "مكافحة جرائم تقنية المعلومات" الصادر بالمرسوم السلطاني رقم: 2011/12 بتاريخ 2011/2/6، وقد عالج موضوع التجسس الإلكتروني في المواد (6) و (8) وفق النص التالي:" يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة

آلاف ريال عماني أو بإحدى هاتين العقوبتين كل من دخل عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا بقصد الحصول على بيانات أو معلومات إلكترونية حكومية سرية بطبيعتها أو بموجب تعليمات صادرة بذلك...، وتعد البيانات والمعلومات الإلكترونية السرية الخاصة بالمصارف والمؤسسات المالية في حكم البيانات والمعلومات الإلكترونية الحكومية السرية في نطاق تطبيق حكم هذه المادة". (47)

وتم النص كذلك على أنه:" يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على سنة وبغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد عن ألفي ريال عماني، أو بإحدى هاتين العقوبتين كل من اعترض عمدا ودون وجه حق باستخدام وسائل تقنية المعلومات خط سير البيانات أو المعلومات الإلكترونية المرسلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات، أو قطع بثها أو استقبالها أو تنصت عليها."(48)

وبالرجوع إلى قانون العقوبات الجزائري نجد أن المشرع اكتفى بالمساواة بين جريمة التجسس التقليدية وخيانة الأمانة من الناحية العقابية، دون الإشارة إلى هذا النوع الجديد من الجرائم الماسة بأمن الدولة الخارجي بل حتى الداخلي، في الكثير من الحالات مما يدفعنا إلى التساؤل هل يمكن القياس على العقوبة المقررة للجريمة التقليدية، فنجيب بالقول بأن القاضي لا يستطيع الاعتماد على القياس في الجانب الجزائي، كما أنه لا يستطيع تجريم فعل لم يجرمه المشرع، لذا استدرك المشرع الجزائري الفراغ القانوني من خلال تعديل قانون العقوبات فتمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر (156/66) بالقسم السابع مكرر، عنوانه:" المساس بأنظمة المعالجة الآلية للمعطيات"، ويشمل المواد من 394 مكرر إلى المادة 394 مكرر7 دون الإشارة المباشرة منه إلى جريمة التجسس الإلكتروني.(49)

فقد جرمت المادة 394 مكرر 2 من قانون العقوبات الجزائري أفعال الحيازة، الإفشاء، النشر، والاستعمال أيا كان الغرض من هذه الجرائم الواردة في القسم السابع مكرر من ذات القانون عندما يكون الهدف من ذلك المنافسة غير المشروعة، الجوسسة، الإرهاب أو التحريض على الفسق.(50)

غير أنه يمكن القول أن المشرع الجزائري بتحديده لثلاث صور فقط من هذه الجرائم المستحدثة، سوف يؤدي لا محالة إلى إفلات الكثير من مجرمي المعلوماتية من العقاب، نظرا لأن الجرائم التي ارتكبوها لا تدخل في نطاق أي صورة من الصور المحددة قانونا ومن بينها جريمة التجسس الإلكتروني، لأن تكنولوجيا الإعلام والاتصال في تزايد مستمر فكل يوم هناك

اكتشاف لوسائل حديثة يستغلها الجناة لارتكاب جرائم غير منصوص عليها في القانون، كما أن القضاة ملزمين باحترام مبدأ الشرعية الجنائية.[51]

لقد تبنى المشرع الجزائري الحماية الجزائية للمعلوماتية بموجب القانون رقم 09-04 الصادر بتاريخ: 9 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث جرم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات وجريمة الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي، وحدد لكل نوع من الجرائم السابق ذكرها أركانها والعقوبة المقررة لها.[52]

فحسب هذا القانون فالمقصود بالجرائم التي ترتكب بواسطة أنظمة الحوسبة والاتصالات هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات السابق ذكرها، وأي جريمة ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وإذا كانت الجرائم الأولى واضحة المعالم ومحددة عقوباتها، والتساؤل يطرح في هذا المجال عن الجريمة التي ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية، فالمشرع يقصد بأن أي جريمة محددة في قانون العقوبات أو أحد القوانين المكملة له إن ارتكبت بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية، فإنها تطبق عليها العقوبة المحددة في القانون، سواء ارتكبت بوسيلة إلكترونية أو بدونها.[53]

ولقد صادقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2014، والتي توصي في مادتها 21 على أن تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات.[54]

ج. الآليات والوسائل التقنية لحصر جريمة التجسس الإلكتروني

تعتبر جرائم التجسس الإلكتروني من الجرائم العابرة للحدود الوطنية للدول، أي أنها لا تتم ولا تنتهي في أراضي دولة محددة، وعليه فالحديث عن ضرورة إيجاد إستراتيجية تقنية وقانونية لمحاربتها وتأمين البيئة الإلكترونية، يأتي نظرا لتزايد عدد الهجمات على المستوى الدولي لأسباب عديدة أبرزها التحديات والعوائق لمحاربة هذه الظاهرة خاصة في المجال الأمني، وهو أحد أهم الأسباب في نجاح الجواسيس في استغلال التكنولوجيا في أنشطتهم، بالإضافة إلى ضعف التشريعات والعقوبات المخصصة لهذا النوع الجديد من الجرائم المستحدثة.[55]

ومن الوسائل التقنية المستعملة للتصدي لجريمة التجسس الإلكتروني نجد:

- استخدام تقنية (Mac Address) عوضا عن (Ip Address) لحماية الشبكات اللاسلكية الداخلية، لأنه يصعب اختراقها، فهي تحمل أرقاما لا تتكرر أبدا ويستطيع مدير الشبكة من خلالها تحديد عدد الأجهزة المصرح لها بالاتصال واستخدام الشبكة.[56]
- استعمال وسيلة الجدار الناري لحماية الشبكات الخاصة من الدخول ومنع الوصول غير المشروع لها، من خلال حماية وحدات التحكم والإرسال في الانترنت

ومن مزايا هذه الوسيلة أنها توفر الحماية اللازمة للشبكة والمعلومات والحد من تعرضها للأخطار ومتابعة المستخدمين للشبكة ومن يحاول العبث بها، وتسجيل وقائع الاستخدام بدقة طالما أن كل الرسائل والأوامر تمر به عند خروجها أو دخولها الانترنت، وكذلك تسجيل كافة المعلومات عن حركة مرور المعلومات.[57]

- تشفير البيانات باستخدام تقنية (Wired Equivalent Privacy) وباستخدام مفتاح كبير للتشفير يصعب كسره واختراقه، على أن يتم تغييره بشكل دوري.
- استخدام بعض برامج مكافحة التجسس مثل: Spyware Blaster الذي لا يقتصر دوره فقط على القضاء على برامج التجسس الالكتروني بل يقوم بدور المراقب لمنع أية ملفات من اقتحام الجهاز أو الشبكة.[58]
- ونجد كذلك نظام المعاملات الإلكترونية الآمنة باعتباره أهم بروتوكول متعلق بالنواحي الأمنية، وهدفه الأساسي هو تأمين عملية الوفاء والمعاملات المالية. ومن أهم مميزاته أنه يضمن كون طلب الشراء المرسل هو نفسه الطلب الذي يستقبله صاحب المشروع أو التاجر، من خلال بصمة ورقية معينة تكون مميزة لهذا الطلب، كما أنه يضمن سرية طلب الشراء عن طريق تشفير المعلومات التي يشملها الطلب، وكذلك البيانات الخاصة بعمليات الوفاء.

ويضمن كذلك للتاجر أو صاحب المشروع أن حامل البطاقة البنكية هو الشخص نفسـه عن طريق الشهادة التي يحملها والصادرة عن البنك الضامن أو شركة الائتمان الضامنة له.[59]

- أما نظام التأمين (SSL) تكمن مهمته في تشفير جميع الاتصالات في برامج التصفح أو النوافذ على شبكة المعلومات (Bowser) وأحد المواقع أو مقر المعلومات على

خادم الشبكة (Server)، وبالتالي فهو يقلل من فرصة وقوع المعلومات أثناء عملية انتقالها في أيدي أي شخص غير مرغوب فيه إلى أن تصل إلى المستقبل النهائي.[60]

4. خاتمة

من خلال التطرق لموضوع " التجسس الالكتروني وطرق مكافحته"، تبين أن هذه الممارسة التي ارتقت لكونها جريمة في العديد من تشريعات الدول، حيث تم الإشارة إلى ذلك في بعض المواثيق والاتفاقيات الدولية ومنها الاتفاقية الأوروبية لمكافحة جرائم الانترنت 2001، كما أوصت الجمعية العامة للأمم المتحدة في قراراتها بضرورة صياغة اتفاقية دولية شاملة بشأن استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية. ولا ننسى في هذا المجال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي أشارت بطريقة غير مباشرة للتجسس الإلكتروني.

أما بالنسبة للتشريعات الوطنية فنجد قانون مكافحة جرائم تقنية المعلومات العماني لسنة 2011 نص في المادتين: 6 و 8 على التجسس الإلكتروني، أما التشريع الأردني فقد أشار لهذه الجريمة في المادة 12 من قانون الجرائم الإلكترونية لسنة 2012، أما قانون العقوبات الجزائري فقد كان يجرم التجسس التقليدي الماس بأمن الدولة، ولكن كنتيجة للتطورات التي لحقت تكنولوجيا الإعلام والاتصال التي أصبحت تستخدم كوسيلة للجريمة، ظهرت العديد من الجرائم المستحدثة، تم إدخال تعديلات على هذا القانون شملت صور لجرائم تشكل مساسا بأنظمة المعالجة الآلية للمعطيات، ولكنه لم يشر بصفة مباشرة إلى جريمة التجسس الإلكتروني، كما تم إصدار القانون رقم 04/09 لسنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ومن خلال ما سبق الإشارة إليه تم التوصل إلى جملة من النتائج والاقتراحات نذكر منها:

أ. النتائج

- ✓ لا يختلف مفهوم التجسس الاصطلاحي عن مفهومه اللغوي، فكلاهما يهدف للكشف عن أمور مخفية، كما لا يختلف مفهوم التجسس الإلكتروني عن التجسس التقليدي إلا من حيث الأداة المستخدمة فقط وهي تكنولوجيا المعلومات.

- ✓ تتعدد صور ومجالات التجسس الإلكتروني، بين التجسس العسكري، السياسي، والاقتصادي هذا الأخير الذي يؤثر سلبا على المؤسسات الاقتصادية.
- ✓ تعتبر جرائم التجسس الإلكتروني من الجرائم العابرة للحدود، وتتطلب لقيامها توافر ثلاثة أركان وهي الركن المادي، الركن المعنوي والركن الشرعي، والتي تختلف بحسب صور الجريمة ومنها ما ذكر في المادة الثالثة من اتفاقية بودابست.
- ✓ المشرع الجزائري لم يضع تعريفا محددا للتجسس الدولي، وكذلك التجسس الإلكتروني لكي لا يحصره في مجال محدد.
- ✓ المشرع الجزائري لم يضع آليات قانونية ولا جنائية لمحاربة هذه الظاهرة الإجرامية رغم خطورتها.
- ✓ لم يفرد القانون الدولي جريمة التجسس بنص خاص، بل أوردها ضمن عموم جرائم الحاسب الآلي وهو قصور يفتح المجال واسعا للتأويل وفقا للمصالح السياسية وغيرها لبعض الدول.
- ✓ إن مكافحة جريمة التجسس الإلكتروني تتطلب من الدول إتباع أساليب ووسائل تقنية معينة منها: الجدار الناري، نظام المعاملات الإلكترونية الآمنة، نظام التأمين...والتي تهدف كلها لحصر هذه الجريمة ومجابهة مخاطرها.

ب. الاقتراحـات

- ✓ تعزيز وتفعيل التعاون الدولي لمكافحة جرائم التجسس الإلكتروني، بما في ذلك تكريس مبدأ الاختصاص الجنائي العالمي.
- ✓ ضرورة تكييف المشرع الوطني لقانونه الداخلي مع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال النص صراحة على تشديد العقوبات بالنسبة للجرائم المرتكبة باستعمال وسائط إلكترونية ومنها جريمة التجسس الإلكتروني.
- ✓ تشديد الدول لإجراءات ووسائل حماية أنظمتها الدفاعية المحتوية لمعلومات سرية في مختلف المجالات.
- ✓ إنشاء هيئات وطنية مهمتها مراقبة المواقع الإلكترونية عبر شبكة الانترنت لحجب المواقع المشبوهة التي تهدد أمن واستقرار المجتمع.

5. قائمة المصادر والمراجع

أولا/ المصادر

أ. الاتفاقيات والمواثيق الدولية

[1] الاتفاقية الأوروبية لمكافحة جرائم الانترنت لعام 2001.

[2] UN.DOC. A/RES/55/63, 22 January 2001.

[3] UN.DOC. A/AC.291/2, 15 June 2020.

ب. القوانين الوطنية

[1] القانون الأردني رقم 50 لسنة 1971 المتعلق بحماية أسرار ووثائق الدولة، الجريدة الرسمية للمملكة الأردنية الهاشمية، العدد 2315، الصادرة بتاريخ: 1971/08/01، الصفحة 1164.

[2] القانون الأردني رقم 27 لسنة 2015 المتعلق بالجرائم الإلكترونية، الجريدة الرسمية للمملكة الأردنية الهاشمية، العدد 5343، الصادرة بتاريخ: 2015/01/06، الصفحة 5631.

[3] قانون العقوبات الجزائري الذي تمم الفصل الثالث منه بالقانون رقم: 04-15 الصادر في: 10 نوفمبر 2004، ويتضمن المواد من 394 مكرر إلى 394 مكرر 7، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 71، الصادر بتاريخ: 10 نوفمبر 2014.

[4] القانون رقم 09-04 الصادر في: 9 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر بتاريخ: 16 أوت 2009.

[5] المرسوم السلطاني رقم: 2011/12 الصادر بتاريخ 2011/2/6 المتضمن قانون "مكافحة جرائم تقنية المعلومات"، الجريدة الرسمية لسلطنة عمان، العدد 969، الصادرة بتاريخ: 2011/02/15.

ثانيا/ المراجع

أ. الكتب

[1] خليفة إيهاب، القوة الإلكترونية (كيف يمكن أن تدير الدول شؤونها في عصر الانترنت)، العربي للنشر والتوزيع، القاهرة ،2017.

[2] صفاء فتوح جمعة، مسؤولية الموظف العام في إطار تطبيق الإدارة الإلكترونية، دار الفكر والقانون، المنصورة، 2014.

[3] ضرغام جابر عطوش، جريمة التجسس المعلوماتي: دراسة مقارنة، المركز العربي للدراسات والبحوث العلمية، القاهرة، 2017.

[4] غادة نصار، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، القاهرة، 2017.

[5] كافي مصطفى يوسف، الإدارة الإلكترونية، دار ومؤسسة رسلان للطباعة والنشر والتوزيع، سوريا، 2011.

ب. الأطروحات والرسائل الجامعية:

[1] فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الانترنيت، مذكرة لنيل شهادة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد –تلمسان- الجزائر، 2011-2012.

[2] مولود بوعقادة، الجرائم الاقتصادية والمالية وسبل محاربتها دوليا ووطنيا، مذكرة ماستر في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة خميس مليانة، الجزائر، 2014.

ج. المقـالات العلميـة

[1] إلهام بن خليفة، جمال غريسي، التجسس الإلكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري، مجلة دفاتر السياسة والقانون، الصادرة عن جامعة قاصدي مرباح، ورقلة، المجلد 14، العدد 1، 2022.

[2] بونعارة ياسمينة، الجريمة الالكترونية، المعيار، كلية أصول الدين، جامعة الأمير عبد القادر، المجلد 20، العدد 39، 2015.

[3] حنان أوشن، وادي عماد الدين، التجسس الإلكتروني وآليات مكافحته في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور، خنشلة، العدد الثاني، 2014.

[4] شاكر عبد أبو ذر، التجسس الإلكتروني في ظل التشريع الأردني، مجلة العلوم السياسية والقانون، العدد 26، 2020.

[5] عبد الإله محمد النوايسة، ممدوح حسن العدوان، جرائم التجسس الإلكتروني في التشريع الأردني (دراسة تحليلية)، دراسات، علوم الشريعة والقانون، الجامعة الأردنية، المجلد 46، عدد 1، ملحق 1، 2019.

[6] عبير علي حسين الورفلي، جرائم التجسس الإلكتروني للمعلومات الشخصية في إطار اتفاقية بودابست بشأن الجريمة الإلكترونية، مجلة أبحاث بكلية الآداب، جامعة سرت، العدد 15، الجزء 1، مارس 2023.

[7] علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في الشريعة الإسلامية مقارنا بالقانون الدولي، مجلة أصول الشريعة للأبحاث التخصصية، المجلد 4، العدد 4، أكتوبر 2018.

[8] نجاري بن حاج علي فايزة، جريمة التجسس الإلكتروني، ستراتيجيا: مجلة دراسات الدفاع والاستقبالية، العدد 11، السداسي الأول، 2019.

د. المداخـلات في الملتقيـات العلميـة

[1] بوزيدي مختارية، ماهية الجريمة الإلكترونية، مداخلة قدمت ضمن أعمال الملتقى الوطني:" آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري"، مركز جيل البحث العلمي بالتعاون مع مخبر بحث الحوكمة العمومية والاقتصاد الاجتماعي بجامعة تلمسان، الجزائر، 2017.

[2] حفوظة الأمير عبد القادر، غرداين حسام، الجريمة الإلكترونية وآليات التصدي لها، مداخلة قدمت ضمن أعمال الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي بالتعاون مع مخبر بحث الحوكمة العمومية والاقتصاد الاجتماعي بجامعة تلمسان، الجزائر، 2017.

[3] علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في القانون العماني مقارنة بالشريعة الإسلامية والقانون الجنائي الدولي، مداخلة قدمت في المؤتمر الدولي الأول: العلوم الشرعية تحديات الواقع وآفاق المستقبل، كلية العلوم الشرعية، سلطنة عمان، 2018.

[4] محمد محمد الألفي، ورقة عمل حول: تشريعات مكافحة جرائم الإرهاب الإلكتروني "الأحكام الموضوعية والأنماط"، الندوة العلمية حول: القوانين العربية والدولية في مكافحة الإرهاب، الرياض، المملكة العربية السعودية، 2013.

ه. المواقع الالكترونية

[1] عادل الأبيوكي، الجريمة الاقتصادية، مركز الإعلام الأمني، 2011.
https://www.policemc.gov. (consulté le:10/09/2019)

[2] فؤاد برامي، التجسس الإلكتروني خاصياته وأهدافه، 2018.
https://www.akhbarona.com/writers/260026.html (consulté le:10/09/2019)

[3] هشام بشير، الإرهاب الإلكتروني في ظل ثورة المعلومات، آراء حول الخليج، العدد 92، 2019.
http://araa.sa/index.php?view=article&id=244:2014-06-13-16-21-31&option=com_content (consulté le:10/09/2019)

Ad hoc committee established by General Assembly resolution 74/247 . https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html (consulté le:10/12/2020)

التهميش والاقتباس

(1) الأمير عبد القادر حفوظة، حسام غرداين، الجريمة الإلكترونية وآليات التصدي لها، مداخلة قدمت ضمن أعمال الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي بالتعاون مع مخبر بحث الحوكمة العمومية والاقتصاد الاجتماعي بجامعة تلمسان، الجزائر، 2017، ص 84.

(2) فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الانترنيت، مذكرة لنيل شهادة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد –تلمسان- الجزائر، 2011-2012، ص 1.

(3) التجسس في اللغة هو من الجس وهو اللمس باليد ويقال يجسه جسا واجتسه أي مسه ولمسه، أما الجاسوس فهو العين يتجسس الأخبار، وجمعها جواسيس ومنه الجساس، وهو وصف للمبالغة. وقد حاول الفقه وضع تعريف للتجسس إلا أن هذه التعريفات متباينة وتعتمد على طبيعة السلوك المجرم في التشريع محل الدراسة، لأن السياسة التشريعية تختلف من دولة لأخرى، كما أن جرائم التجسس تختلف من تشريع لآخر، لذا تأتي هذه التعريفات مختلفة. أنظر: عبد الإله محمد النوايسة، ممدوح حسن العدوان، جرائم التجسس الإلكتروني في التشريع الأردني (دراسة

تحليلية)، دراسات، علوم الشريعة والقانون، الجامعة الأردنية، المجلد 46، عدد 1، ملحق 1، 2019، ص ص 468-469.

(4) علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في القانون العماني مقارنة بالشريعة الإسلامية والقانون الجنائي الدولي، مداخلة قدمت في المؤتمر الدولي الأول: العلوم الشرعية تحديات الواقع وآفاق المستقبل، كلية العلوم الشرعية، سلطنة عمان، 2018، ص 1274.

(5) هشام بشير، الإرهاب الإلكتروني في ظل ثورة المعلومات، آراء حول الخليج، العدد 92، 2012.
http://araa.sa/index.php?view=article&id=244:2014-06-13-16-21-31&option=com_content (consulté le:10/09/2019)

(6) علي بن محمد بن سالم العدوي، المقال السابق، ص 1274.

(7) محمد محمد الألفي، ورقة عمل حول: تشريعات مكافحة جرائم الإرهاب الإلكتروني "الأحكام الموضوعية والأنماط"، الندوة العلمية حول: القوانين العربية والدولية في مكافحة الإرهاب، الرياض، المملكة العربية السعودية، 2013، ص 16.

(8) ضرغام جابر عطوش، جريمة التجسس المعلوماتي: دراسة مقارنة، المركز العربي للدراسات والبحوث العلمية، القاهرة، 2017، ص 178.

(9) فالقرصنة عادة ما ينفذها الهواة العابثون من محترفي الأنظمة المعلوماتية الذين يبحثون عن التسلية أو إثبات قدراتهم أو العبث وإتلاف المحتويات التي يمكن التغلب عليها من خلال استعادة نسخة أخرى من البرنامج مخزنة في مكان آمن، بينما يقتصر التجسس الإلكتروني في الغالب على التنظيمات الإرهابية وأجهزة الاستخبارات، التي تسعى للحصول على المعلومات والأسرار المتعلقة بدولة ما بشتى الطرق من أجل استغلالها بما يضر مصلحة تلك الدولة أو بيعها لدولة معادية لها، وعليه فإن مقدار الخطر يكون فيها أشد وحجم الضرر فيها أكبر وبالتالي لا توصف القرصنة الإلكترونية إرهابا كما يوصف بها التجسس الإلكتروني، على أن القرصنة عندما بدأت لم تكن تأخذ الطابع السلبي في بداية الأمر، بل كانت تطلق على من لديه عبقرية في ابتكار برامج سريعة ومدهشة في أنظمة الحواسيب ثم تدرج الأمر إلى أن طغى عليها الجانب السلبي في وقتنا الحالي. أنظر: علي بن محمد بن سالم العدوي، المقال السابق، ص 1275.

(10) فؤاد برامي، التجسس الإلكتروني خاصياته وأهدافه، أنفاس بريس، 2018.
https://anfaspress.com/news/voir/45767-2018-12-15-04-20-06 (consulté le:10/09/2019)

(11) عبد الإله محمد النوايسة، ممدوح حسن العدوان، المقال السابق، ص 470.

(12) الأمير عبد القادر حفوظة، حسام غرداين، المقال السابق، ص 94.

(13) محمد محمد الألفي، المقال السابق، ص 16.

(14) علي بن محمد بن سالم العدوي، المقال السابق، ص 1275.

(15) عبد الإله محمد النوايسة، ممدوح حسن العدوان، المقال السابق، ص 470.

(16) المقال نفسه، ص 470.

(17) شاكر عبد أبو ذر، التجسس الإلكتروني في ظل التشريع الأردني، مجلة العلوم السياسية والقانون، العدد 26، 2020، ص ص 44-45.

(18) عبير علي حسين الورفلي، جرائم التجسس الإلكتروني للمعلومات الشخصية في إطار اتفاقية بودابست بشأن الجريمة الإلكترونية، مجلة أبحاث بكلية الآداب، جامعة سرت، العدد 15، الجزء 1، مارس 2023، ص 134.

[19] علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في الشريعة الإسلامية مقارنا بالقانون الدولي، مجلة أصول الشريعة للأبحاث التخصصية، المجلد 4، العدد 4، أكتوبر 2018، ص 172.

[20] عبير علي حسين الورفلي، المقال السابق، ص ص 134-135.

[21] المقال نفسه، ص ص 136-137.

[22] المقال نفسه، ص 141.

[23] علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في الشريعة الإسلامية مقارنا بالقانون الدولي، المقال السابق، ص 179.

[24] عبير علي حسين الورفلي، المقال السابق، ص 136.

[25] المقال نفسه، ص ص 143-144.

[26] عادل الأبيوكي، الجريمة الاقتصادية، مركز الإعلام الأمني، 2011، ص ص 2-3.
https://www.policemc.gov. (consulté le:10/09/2019)

[27] عبد الإله محمد النوايسة، ممدوح حسن العدوان، المقال السابق، ص 469.

[28] فتيحة رصاع، المذكرة السابقة، ص ص 76-77.

[29] غادة نصار، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، القاهرة، 2017، ص 30.

[30] فؤاد برامي، المقال السابق.

[31] المقال نفسه.

[32] مصطفى يوسف كافي، الإدارة الإلكترونية، دار رسلان، سوريا، 2011، ص 73.

[33] صفاء فتوح جمعة، مسؤولية الموظف العام في إطار تطبيق الإدارة الإلكترونية، دار الفكر والقانون، المنصورة، 2014، ص76.

[34] ياسمينة بونعارة،الجريمة الالكترونية، المعيار، كلية أصول الدين، جامعة الأمير عبد القادر، قسنطينة، المجلد 20، العدد 39، 2015، ص 300.

[35] فؤاد برامي، المقال السابق.

[36] مولود بوعقادة، الجرائم الاقتصادية والمالية وسبل محاربتها دوليا ووطنيا، مذكرة ماستر في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة خميس مليانة، الجزائر، 2013-2014، ص 48.

[37] فؤاد برامي، المقال السابق.

[38] علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في القانون العماني مقارنة بالشريعة الإسلامية والقانون الجنائي الدولي، المقال السابق، ص 1273.

[39] المقال نفسه.

[40] UN.DOC. A/RES/55/63, 22 January 2001, p 1-3.

[41] إيهاب خليفة، القوة الإلكترونية (كيف يمكن أن تدير الدول شؤونها في عصر الانترنت)، العربي للنشر والتوزيع، القاهرة، 2017، ص164.

[42] المادة 3 من الاتفاقية الأوروبية لمكافحة جرائم الانترنت لعام 2001.

[43] علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في القانون العماني مقارنة بالشريعة الإسلامية والقانون الجنائي الدولي، المقال السابق، ص 1285.

(44) Ad hoc committee established by General Assembly resolution 74/247 . https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html (consulté le:10/12/2020)

(45) UN.DOC. A/AC.291/2, 15 June 2020. P 2.

(46) عبد الإله محمد النوايسة، ممدوح حسن العدوان، المقال السابق، ص ص 471-472.

(47) علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في القانون العماني مقارنة بالشريعة الإسلامية والقانون الجنائي الدولي، المقال السابق، ص ص 1275-1276.

(48) المقال نفسه، ص 1276.

(49) حنان أوشن، وادي عماد الدين، التجسس الإلكتروني وآليات مكافحته في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور، خنشلة، العدد الثاني، 2014، ص 139.

(50) بوزيدي مختارية، ماهية الجريمة الإلكترونية، مداخلة قدمت ضمن أعمال الملتقى الوطني:" آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري"، مركز جيل البحث العلمي بالتعاون مع مخبر بحث الحوكمة العمومية والاقتصاد الاجتماعي بجامعة تلمسان، الجزائر، 2017، ص 18.

(51) إلهام بن خليفة، جمال غريسي، التجسس الإلكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري، مجلة دفاتر السياسة والقانون، الصادرة عن جامعة قاصدي مرباح، ورقلة، المجلد 14، العدد 1، 2022، ص 155.

(52) بوزيدي مختارية، المقال السابق، ص 7.

(53) إلهام بن خليفة، جمال غريسي، المقال السابق، ص 155.

(54) المقال نفسه، ص 156.

(55) نجاري بن حاج علي فايزة، جريمة التجسس الإلكتروني، ستراتيجيا: مجلة دراسات الدفاع والاستقبالية، العدد 11، السداسي الأول، 2019، ص 68.

(56) علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في الشريعة الإسلامية مقارنا بالقانون الدولي، المقال السابق، ص 184.

(57) نجاري بن حاج علي فايزة، المقال السابق، ص 69.

(58) علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في الشريعة الإسلامية مقارنا بالقانون الدولي، المقال السابق، ص 185.

(59) نجاري بن حاج علي فايزة، المقال السابق، ص ص 69-70.

(60) المقال نفسه، ص 70.