تأثير التجسس الالكتروني على الحق في الخصوصية المعلوماتية

The Impact of Cyber-Espionage on the Right to Information Privacy

فتيحة خالدي ♦
جامعة أكلي محند اولحاج- البويرة/ الجزائر
f.khaldi@univ-bouira.dz

تاريخ الإرسال: 2021/05/03 تاريخ القبول: 2021/05/20 تاريخ النشر: 2021/06/29

الملخص:

من إيجابيات التكنولوجيا؛ رقمنة كل ماهو ورقي، ليصبح متاحا للجميع، إلا أن من سلبياتها،أنه يشكل في حد ذاته تهديدا للأمن المعلوماتي،والحياة الخاصة ككل، لذلك يمثل التجسس الرقمي، أو الجوسسة الرقمية أحد المظاهر الخطيرة للاعتداء على حق الأفراد، والشركات، وحتى الدول في الخصوصية المعلوماتية.

من هنا تأتي أهمية هذه الورقة البحثية، التي تلقي الضوء على موضوع قديم مستحدث، لتوضيح مدى تأثير التجسس الإلكتروني على الحق في الخصوصية الرقمية، خاصة في ظل ما أتاحته ثورة الاتصالات والمعلومات من آفاق جديدة، أين لم يعد الجاسوس مجبرا على ارتداء أزياء التنكر، أو السفر لأجل القيام بمهمته، مثلما كان عليه الأمر في أساليب التجسس القديمة، إنما يحتاج فقط لجهاز كومبيوتر، وبرامج معينة، وشبكة انترنت.

الكلمات المفتاحية: الفضاء الرقمي؛ الخصوصية المعلوماتية؛ الجريمة الإلكترونية؛ التجسس الالكتروني.

Abstract:

One of the pros of technology is digitizing everything that is in paper, to be available to all. But one of its drawbacks, is that it itself poses a threat to information security, and private life as a whole. So digital espionage, or digital spies, is a serious manifestation of attacking the right of individuals, companies, and even states to information privacy.

Hence the importance of this research paper, which sheds the light on an old, new topic, to illustrate the impact of cyber-espionage on the right to digital privacy, especially in light of the new updates provided by the communications and information revolution, where the spy is no longer has to wear costumes of disguise, or travel to carry out his mission. Only needs a computer, certain programs, and the Net.

Keywords: Digital Space; Information Privacy; Cyber-Crime; Cyber-Espionage.

♦ المؤلف المرسل

تأثير التجسس الالكتروني على الحق في الخصوصية المعلوماتية

مقدمة:

يعد الحق في الخصوصية من الحقوق اللصيقة بالشخصية والملازمة للشخص باعتباره إنسانا، لذلك اتجهت التشريعات الدولية والوطنية إلى حمايته من أي انتهاك سواء كانت صادرة من سلطات الدولة أو من الأشخاص العاديين، حيث اعتبرته الشرعة الدولية حقا من حقوق الإنسان، من خلال حماية أي شخص يتعرض لأي نوع من أنواع التدخل التعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، أو تعرضه لحملات تمس شرفه وسمعته.

وبالرغم من إقرار الصكوك والاتفاقيات الدولية والدساتير الوطنية بحماية الحق في الخصوصية إلا إن هذا الحق تأثر بتطور الحياة، خاصة في ظل الفضاء الرقمي الذي يمثل مجالا واسعا يكثر فيه انتهاك هذا الحق والمساس بحرمة الحياة الخاصة، لدرجة ربط ظهور الحق في الخصوصية المعلوماتية بمخاطر تقنية المعلومات المتصلة بحماية بنوك المعلومات وعمليات المعالجة الآلية للبيانات.

ومن بين ما يهدد الحق في الخصوصية في الفضاء الرقمي، ما يسمى بالجوسسة الرقمية أو التجسس الرقمي أو الالكتروني، عن طريق اختراق المواقع الالكترونية والاعتداء على خصوصية الأفراد والمؤسسات الحكومية الذي أصبح يتزايد بفعل تطور السريع لتكنولوجيا المعلوماتية، خاصة بفعل الهواتف والأجهزة والكاميرات الذكية التي اجتاحت أسواق وحياة الأفراد والدول.

انتشرت ظاهرة التجسس الالكتروني مع نهاية القرن العشرين وبداية الالفية الجديدة بفعل الثورة التكنولوجية الهائلة في مجال المعلومات والاتصالات والتوسع في استخدام شبكة المعلوماتية(الانترنت) ، والتي غيرت أساليب التجسس التقليدية إلى طرق الكترونية حديثة سهلت مهمة الجاسوس في الوصول إلى المعلومات ي وقت قصير.

استنادا على ما سبق، فالتجسس الالكتروني أو الرقمي أصبح يشكل في ظل التطور التقني الهائل الذي نعيشه حربا للسيطرة على الأفراد والدول من خلال قرصنة المعلومات، إذ تعتمده الدول اليوم لحماية أمنها وتطوير اقتصادها من خلال الاطلاع على أسرار منافسيها.

بناء على ما تقدم، إذا كان العصر الحالي يعرف بعصر المعلومات الرقمية، لدرجة أن أهمية المعلومات باتت تمثل مصدر قوة الدولة الاقتصادية والاجتماعية والعسكرية ، وحيث أن التجسس ظاهرة لازمت المجتمعات وتطورت بتطورها، إلى أن أصبح يشكل تهديدا للبيانات والمعلومات الرقمية، واعتداء على حق الخصوصية المعلوماتية، **فكيف يمكن حماية وتأمين حق الخصوصية المعلوماتية في مواجهة ظاهرة التجسس الالكتروني ؟.**

اقتضت منا الإجابة عن الإشكال المطروح، توظيف المنهج الوصفي والتحليلي، من خلال التعرض إلى تحليل نقطتين، نتطرق في الأولى إلى مضمون التجسس الرقمي أو الالكتروني، من خلال التعرف على مفهومه وأنواعه، وخصائصه، لكي يسهل علينا توضيح في النقطة الثانية انتهاك التجسس الالكتروني لحق الخصوصية المعلوماتية، من خلال التعرف على مظاهر هذا الاعتداء وطرق مكافحته.

1. مضمون التجسس الالكتروني أو الرقمي

يقصد بالخصوصية المعلوماتية، حق الأفراد أو الجماعات أو المؤسسات أن يحددوا الوقت والكيفية التي تصل بها المعلومات الخاصة بهم إلى الآخرين[1]، لذلك فالخصوصية المعلوماتية أو الرقمية تفيد عد التعدي على البيانات الشخصية عبر الانترنت أو أي وسيط مماثل بالمعالجة أو الاستيلاء أو الاستخدام، وهو ما يفيد أن الخصوصية في العصر الرقمي تتصل بأمرين، الأول خصوصية المعلومات الشخصية، والثاني خصوصية الاتصالات[2].

في هذا الصدد يعد التجسس الرقمي أو الالكتروني احد أنماط التعدي على هذه الخصوصية، حيث دلت كتابات الفقهاء على أن التجسس من أقدم التصرفات التي مارسها الإنسان في سبيل الحصول على المعلومة،وقد تطور وتغير مفهومه بفعل التقدم التقني والتكنولوجي إذ يظهر في شكل أنواع بحسب الوسائل التكنولوجية التي يتم عبرها.

1.1. مفهوم التجسس الالكتروني

نتطرق من خلال هذا المطلب إلى تعريف التجسس (الفرع الأول)، ثم إلى توضيح الخصائص التي يتميز بها التجسس الرقمي باعتباره فعلا إجراميا(الفرع الثاني).

1.1.1. تعريف التجسس الالكتروني

التجسس لغة مشتق من الفعل جس وتجسس واجْتس الأخبار وتجسسها والأمور، بمعنى بحث عنها أو تفحصها وتتبعها، والجاسوس جمع جواسيس وهو الشخص الذي يتتبع الأخبار، والجاسوسية مهنة الجاسوس[3].

وقد جاء لفظ التجسس في قوله تعالى :" يا أيها الذين امنوا اجتنبوا كثيرا من الظن إن بعض الظن إثم ولا تجسسوا ولا يغتب بعضكم بعضا أيحب أحدكم أن يأكل لحم أخيه ميتا فكرهتموه واتقوا الله إن الله تواب رحيم"[4]، بمعنى لا تبحثوا عن عورات الناس وتكشفوا ما ستره الله، ونهى أيضا سبحانه وتعالى عن التجسس على دواخل الناس وإذاعتها وإشاعتها على فرض الاطلاع عليها [5].

وقوله صلوات الله عليه وسلم:" إياكم والظن فان الظن اكذب الحديث، ولا تحسسوا، ولا تجسسوا ولا تناجشوا، ولا تحاسدوا، ولا تباغضوا، ولا تدابروا، وكونوا عباد الله إخوانا"[6].

---

[1]- حسين ربيعي، المراقبة الالكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد1، 2016، ص 413.

[2]- سليم حميداني، اختراق الخصوصي في العالم الرقمي: حدود الظاهرة ومطالب الحماية القانونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد4، العدد2، 2019، ص ص35 -36.

[3]- المنجد في اللغة، طبعة 25، دون سنة، دون بلد، ص 90 مادة جس .

[4]- سورة الحجرات الآية 12.

[5]- حسين بدر نجف، التجسس والاطلاع على أسرار الغير-دراسة فقهية-، مجلة معين، العدد 7، 2017، ص 73.

[6]- الإمام البخاري، صحيح البخاري، مجلد (102/12)، رقم الحديث (6064).

والتجسس في معناه العام الاصطلاحي البحث والتنقيب عما يتعلق بالعدو من معلومات سرية باستخدام الوسائل السرية والفنية، أو العملاء والجواسيس من اجل نقل هذه المعلومات للاستفادة منها في إعداد الخطط، وقد أشار القانون الدولي إلى الجاسوس في زمن الحرب في نص المادة 19 من لائحة لاهاي بالقول: " يعد جاسوسا، من يعمل سرا أو من وراء ستار زائف للحصول على معلومات في منطقة العمليات، بنية تبليغها الفريق الخصم"، أما التجسس فعرفته المادة 29 من هذه اللائحة بالقول:" عملية جمع المعلومات التابعة لطرف في النزاع، عن طريق عمل من أعمال الزيف أو تعمد التخفي، بنية تبليغها للعدو" وهو التجسس الكلاسيكي الذي انتشر أثناء النزاعات المسلحة، على مدى عقود مضت[1].

وقد خلت اغلب التشريعات الوطنية من إعطاء تعريف للتجسس، نظرا لتعدد أفعاله، واكتفت فقط بتحديد صور السلوك المجرم للجريمة، في حين تباينت وتعددت مفاهيم الفقه الجنائي للتجسس كفعل مجرم، بين نظرة موسعة وأخرى مضيقة، فأما التعريف الضيق فيقصر التجسس على وقائع جمع المعلومات العسكرية التي تفيد العدو عن طريق استخدام طرق احتيالية، فيقصد بالتجسس :" قيام الأجنبي بجمع الوثائق والمعلومات السرية المتعلقة بالوضع السياسي والاقتصادي والموارد العسكرية والتنظيم الدفاعي والهجومي للدولة، وذلك بقصد تسليم الوثائق والمعلومات إلى الدولة الأجنبية سواء كان ذلك مجانا أو بمقابل".

ويقوم التعريف الواسع للتجسس على شمول التعريف لكل فعل يخدم مصالح الدول الأجنبية، فعرف وفق ذلك بأنه:" البحث عن أي نوع من المعلومات خفية، عن دولة معينة بهدف إيصالها إلى دولة أجنبية وذلك بنية الإضرار بالدولة التي يتجسس عليها"[2] .

ولا يختلف تعريف التجسس الرقمي أو الالكتروني عن تعريف التجسس العام إلا في الأداة المستعملة في التجسس التي وفرتها التكنولوجيا الحديثة، فيعني أن يقوم احد الأشخاص غير المصرح لهم بالدخول إلى نظام التشغيل بطريقة غير شرعية إلى أغراض غير شرعية، إما بالسرقة أو التخريب او عن طريق التحكم في نظام التشغيل، ويتحقق ذلك متى كان الدخول مخالفا لإرادة صاحب النظام، كاختراق البيانات الشخصية[3].

وهو بذلك يعتمد على استخدام التقنيات الالكترونية في الحصول على المعلومات، وفي مجال المحادثات الشخصية، يعني " عملية التنصت أو التقاط البيانات التي تنتقل بين جهازين عن بعد عبر شبكة الانترنيت" أو بترجمة الانبعاث الكهرومغناطيسي الصادر من الحاسوب إلى بيانات باستخدام الوسائل التقنية[4] .

---

[1]- ليث الدين صلاح حبيب، التجسس وأحكامه إبان النزاعات المسلحة الدولية، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلد1، العدد1 ص310.

[2]- إسراء يونس هادي، أسامة احمد النعيمي، جريمة التجسس الالكتروني في إطار مشروع قانون جرائم المعلوماتية العراقي لسنة 2011، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد10، العدد36، 2021، ص ص 35-36.

[3]- حفصي عباس، التجسس الالكتروني في الشريعة والقانون، مجلة الواحات للبحوث والدراسات، المجلد 12، العدد الأول، 2019، ص 273

[4]- الذهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الالكترونية،(دراسة مقارن)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الأول، العدد الثامن،جامعة المسيلة،2017، ص 147.

فالتجسس الالكتروني:" عبارة عن عدة طرق لاختراق المواقع الالكترونية ومن ثم سرقة بعض المعلومات التي قد تكون مهمة وخطيرة للطرف المتلقي والمسروق منه"[1] ؛ وهو ما ذهب اليه المشرع الاردني في قانون الجرائم الالكترونية عندما عرف التجسس الالكتروني بانه: " دخول الجاني الى الشبكة المعلوماتية، او نظام المعلومات او باي وسيلة كانت بهدف الاطلاع على بيانات او معلومات غير متاحة للجمهور تمس الامن الوطني او العلاقات الخارجية للمملكة او السلامة العامة او الاقتصاد الوطني"[2] .

والتجسس الالكتروني بالمعنى المذكور، يمثل شكل من أشكال الإرهاب باستخدام التكنولوجيا، بشكل سلبي من اجل إحداث أثار مدمرة لمحطات التحكم وشبكات الاتصال، لذلك هناك من يربط بين التجسس الالكتروني والإرهاب الالكتروني باعتبارهما يمثلان نوعا من العدوان او التخويف او التهديد المادي او المعنوي الصادر ممن الدول او الجماعات او الأفراد على الإنسان، في دينه او نفسه او عرضه او عقله او ماله بغير حق، عن طريق استخدام الإمكانيات العلمية والتقنية [3]

وتختلف جريمة التجسس الالكتروني عن جريمة القرصنة الالكترونية، في أن هذه الأخيرة تعتبر من الجرائم الواقعة على الملكية الفكرية، في حين التجسس الالكتروني أكثر شمولا يكون بقصد التنصت أو انتهاك سرية البيانات[4] .

2.1.1. خصائص التجسس الرقمي

يتميز التجسس الالكتروني بعدة خصائص وهي:

- يشكل فعل التجسس الرقمي أو الالكتروني جريمة معاقب عليها في القوانين الجنائية للدول، تتسم بحداثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفائها ومحو أثارها، لذلك تواجه الأجهزة الأمنية صعوبات كثيرة خاصة في مرحلة التحري والحقيق لان الأساليب التقليدية لا تصلح لكشف المجرم لذلك يقتضي أن يكون الجهات المكلفة بالتحقيق والتحري على معرفة بأنظمة المعلوماتية وبرامجها المتطورة[5] .
- التجسس الرقمي جريمة عابرة للحدود، بسبب استخدامه لشبكات المعلومات التي لا تعترف بالحدود الجغرافية، إذ أن المقدرة الهائلة التي تتمتع بها الحواسب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين الأنظمة المختلفة والبعيدة أدت إلى تأثر أشخاص كثيرة من دول مختلفة بالتجسس الالكتروني الذي قد يرتكب في حاسوب موجود في دولة معينة لكن النتيجة الإجرامية تتحقق في دولة أخرى[6] .

---

[1]- إسراء يونس هادي، أسامة احمد النعيمي، مرجع سابق، ص 37.

[2]- أبو ذر شاكر عبد، التجسس الالكتروني في ظل التشريع الأردني، مجلة العلوم السياسية والقانون، مجلد4،العدد26،المركز الديمقراطي العربي- برلين، المانيا، 2020، ص43.

[3]- عبد الهادي محمود الزيدي، التجسس الإسرائيلي الالكتروني على الدول العربية، مجلة دراسات دولية، العدد58، 2014، ص 140.

[4] - ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي، المركز العربي ، 2017، ص 96.

[5] - السيد عبد الحميد احمد، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولي، مكتبة الوفاء القانونية، الطبعة الأولى، الإسكندرية، 2018، ص 72.

[6]- اوشن حنان، وادي عماد الدين، التجسس الالكتروني واليات مكافحته في التشريع الجنائي الجزائري، مجلة الحقوق والعلوم السياسية،العدد2، جامعة عباس لغرور خنشلة، 2014، ص 132.

- تتنوع مجالات التجسس الرقمي إلى تجسس في المجال العسكري نظرا لأهمية الجانب العسكري في حفظ امن الدول وتجسس في المجال التجاري خاصة مع توسع التعامل بالتجارة الالكترونية[1]، بالإضافة إلى التجسس الشخصي الذي يعني التنصت ومراقبة شؤون الأفراد الخاصة في الفضاء الرقمي.
- إثبات جريمة التجسس في الفضاء الرقمي صعب شانها شان الجريمة المعلوماتية، باعتبار أن الركن المادي للجريمة يرتكب في إطار واقع غير ملموس، وهو مجال الحاسوب والانترنيت عبر النظام المعلوماتي، وهو ما يثير مشكلة تحديد الدولة صاحبة الاختصاص القضائي والقانون الواجب التطبيق وإجراءات الملاحقة القضائية[2].

2.1. أنواع التجسس الالكتروني أو الرقمي

للتجسس الالكتروني أنواع تختلف بالنظر للوسيلة الالكترونية التي يتم بها، فقد يتم التجسس على الأشخاص عبر شبكة الانترنت أو من خلال الشبكات السلكية واللاسلكية،أو عن طريق الهواتف النقالة أو الجوال، كما يمكن أن يحدث عبر الموجات والترددات، وكذلك التجسس الالكتروني من خلال الأقمار الصناعية.

1.2.1. التجسس الرقمي على الأشخاص عبر الانترنت

ينتشر هذا النوع من التجسس أثناء الاستخدام الشخصي للكمبيوتر، يستخدم الجاسوس او(الهكر) برامج خارجية ظاهرها تقديم خدمات مبنية على فكرة برنامج الخادم الذي يعمل في نظام الهدف ليقوم الهكر بالاتصال من خلال برنامج العميل او الخادم وهنا تبدأ عملية التجسس.

فقد تعرضت جمهورية كوريا الجنوبية سنة 2011 إلى خسارة كبيرة للبيانات الشخصية صنفت الأولى من نوعها في تاريخ البلاد، حيث تم اختراق المعلومات الخاصة ب35 مليون عميل وسرقة البيانات الشخصية[3].

2.2.1. التجسس الالكتروني عبر الشبكات السلكية واللاسلكية

يتم التجسس الالكتروني في الشبكات السلكية واللاسلكية، عن طريق اصطياد البيانات المرسلة من طرف المستخدمين في الشبكة، ومن أشهر التجسس بداخل الشبكات نجد برنامج (sniffer) الذي يصطاد حزم البيانات المرسلة، حيث تم تجربة احد أنواعه وهو مختص في باصطياد كلمات المرور في احد مقاهي الانترنيت وكانت النتيجة الحصول على كلمات المرور السرية لايميلات الأشخاص، ومن أشهر هذه البرامج لأنظمة ويندوز ولينكس نجد: برنامج ethereal وtcpdump وwindump وغيرها[4].

---

[1] - يهدف التجسس الاقتصادي إلى الحصول على نوعية وحجم الخدمات المقدمة من طرف شركات الدول، الحصول على البحوث والدراسات، التصنت على الاجتماعات الخاصة السرية.....، ويكثر هذا النوع خاصة عندما يحتدم التنافس الاقتصادي بين الشركات او الدول. اسراء يونس هادي، أسامة احمد النعيمي، مرجع سابق، ص 60.

[2] - معاشي سميرة، الجريمة المعلوماتية، مجلة المفكر، العدد 17، 2018، ص 410-412.

[3] - حسن بن احمد الشهري، الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس، المجلة العربية للدراسات الأمنية والتدريب، المجلد28، العدد56، 2012، ص 12

[4] - اوشن حنان، وادي عماد الدين، مرجع سابق، ص 133.

3.2.1. التجسس الالكتروني عن طريق الهاتف النقال

تعد تكنولوجيا الهواتف النقالة الرائدة في عصرنا الحالي، حيث تتيح الكثير من الخدمات في مجال الاتصالات ولعل أهمها الرسائل النصية القصيرةsms ، ثم تطور جهاز الهاتف وأصبح يسمح بتحميل حجم كبير من الملفات خاصة بعد إضافة إمكانية الدخول على الانترنت الأمر الذي سهل للأشخاص تصفح الكثير من المواقع والبريد الالكتروني والتواصل عبر خدمة المراسل الخطي وغيرها.

كل هذه التطبيقات المتاحة على الهاتف النقال سمحت بالتجسس على خصوصية الشخص، إذ بإمكان الجميع لتجسس على الجميع، وأكثر من ذلك أن التجسس أصبح مشروعا تتبناه كبرى دول العالم، فقد اقر الكونقرس قانون التنصت لعام 1994 أمر من خلاله جميع شركات صناعة الهواتف بتصنيع هواتف تسهل مراقبتها وتتبعها من قبل الأجهزة الحكومية[1].

4.2.1. التجسس الالكتروني عبر الموجات والترددات

تعد كل الموجات والترددات في العصر الحالي معروفة للجميع بإمكانهم استخدامهم في محطات الراديو او قنوات التلفزيون او الهواتف أو أجهزة الحاسوب، الا انه هناك بعض الموجات غير معروفة او ما يسمى بالترددات السرية الدولية وهي التي تكون محلا للتجسس، شرط امتلاك جهاز التقاط لاسلكي بموجات فوق متوسطية مع الحصول على مجال الترددات، بالإضافة الى امتلاك خبرة في مجال البرمجيات والتشفير[2].

5.2.1. التجسس الالكتروني عبر الأقمار الصناعية

برغم المزايا التي توفرها الأقمار الصناعية والتي من بينها مشاهدة البث التلفزيوني العابر للقارات وإجراء المكالمات الهاتفية لمسافات بعيدة، إلا أنها تخفي وراءها تطبيقات تتيح التجسس على حرمة الحياة الخاصة من خلال إمكانية تتبع حركة الهدف ومراقبة الشخص في أي نقطة يكون فيها .

فالقدرة والدقة الكبيرة التي تتميز بها الاقمار الصناعية المخصصة للتجسس جعلتها بامكانها مراقبة كل حركة من حركات الأشخاص المستهدفين في أي مكان يكونون، ومن ابرز الاقمار الصناعية التي استخدمت في التجسس نذكر[3]:

- أقمار التجسس الأمريكية، التي انطلقت في استخدامها مع نهاية الخمسينيات، مثل القمر الصناعي كورونا(corona) ، وساموس(Samos)، وارغوه (Argon) ولانيار(Lanyard) وغامبيت(gambit) وكريستال(crystal) وغيرها...
- أقمار التجسس التابعة للاتحاد السوفياتي سابقا، مثل كوسموس(cosmos)، رورسات(rorstal)، الماز(almaz)، إضافة إلى أقمار أطلقتها دول أخرى كبريطانيا والهند وألمانيا والصين وكوريا الجنوبية...

---

[1]- صبرينة بن سعد، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا الإعلام والاتصال، أطروحة دكتوراه، كلية الحقوق، جامعة باتنة، 2015، ص112.

[2]- اوشن حنان، وادي عماد الدين، مرجع سابق، ص 135.

[3]- عبير علي عبد العزيز شري، مشروعية التجسس عبر الأقمار الصناعية في القانون الدولي العام، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلد9، العدد2019،2، ص 788.

2. انتهاك التجسس الالكتروني لحق الخصوصية المعلوماتية

تعمد كبرى المؤسسات والشركات الدولية في العصر الرقمي إلى تجميع وتخزين البيانات الخاصة بالأفراد التي تتعلق بوضعهم الصحي أو التعليمي أو العائلي، في غياب توفير الأمان المطلق لسرية ما ينقل من بيانات، وهو ما يجعل فرص الوصول إلى هذه المعلومات سهل بصورة غير مشروعة ممكنا عن طريق التجسس الالكتروني وبالتالي المساس بخصوصية الأفراد، وعليه نتطرق إلى توضيح الأساليب المتاحة للتجسس الرقمي على خصوصيات الأشخاص، وطرق الحماية المتوفرة في العصر الحالي.

1.2. مظاهر اعتداء التجسس الرقمي على حق الخصوصية المعلوماتية

تستخدم العديد من الأساليب من اجل التجسس على الخصوصية المعلوماتية، منها زرع الفيروسات التي تعد من أهم الأساليب التي يتم بواسطتها التجسس على البيانات الشخصية في البيئة الرقمية(الفرع الأول)، وكذلك استخدام تقنيات أخرى كإخفاء المعلومات داخل المعلومات وتقنية أبواب المصيدة وغيرها(الفرع الثاني)

1.1.2. دس الفيروسات الالكترونية

يمثل الفيروس برنامج صغير يزرع في الاسطوانات والأقراص الخاصة بالحاسوب بقصد تخريبه، حيث تتكاثر هذه الفيروسات فتجعل الحاسوب خاملا ومن ثم يدمر البرامج والبيانات وكل المعلومات، وغالبا ما تنتقل الفيروسات إلى الحواسيب عبر شبكة الانترنيت[1] .

ونجد من بين الفيروسات المشهورة استخدام برنامج حصان طروادة بصورة خفية في البرامج التطبيقية وبالتالي يمكن الوصول إلى قاعدة البيانات الخاصة بالحاسوب، ومثالها إرسال الهاكر صورة أو ملف يحتوي على ذلك الفيروس عبر المحادثات أو الشات أو عبر رسالة في البريد الالكتروني، أو عن طريق إنزال برامج أو صور أو ملفات لمواقع مشبوهة كالمواقع الجنسية وغيرها[2] .

كما يعمل حصان طروادة على تغيير البرامج والبيانات والمعلومات داخل الحاسوب، وهذا النوع صعب الاكتشاف إذ بمجرد دخوله في جهاز الضحية من هيئته وأحيانا يدمر نفسه عند إتمام مهمته فيصعب تتبعه والقضاء عليه[3] .

يزرع الفيروس بالحاسوب بقصد الحصول على معلومات على الحياة الخاصة للشخص، ثم استخدام هذه المعلومات بصورة غير مشروعة، حيث يقوم الفيروس المزروع بمعالج المعلومات الاسمية للشخص من اجل الحصول على معلومات جديدة عنه باستخدام وسائل معينة، كالتقريب والمقابلة بين المعلومات وإعداد الإحصائيات وإدماج العناصر وربطها ببعضها لينتهي إلى ترجمة حياة الفرد في ثوان معدودة[4] .

---

[1] - شريفي الشريف، مدى احترام الحق في الخصوصية في الحسابات الالكترونية على الانترنت، مجلة القانون والمجتمع، المجلد4، العدد2019،1 ، ص 121.

[2] - هروال هبة نبيلة، جرائم الانترنت (دراسة مقارنة)، أطروحة دكتوراه،جامعة تلمسان، 2014/2013، ص 374.

[3] - صبرينة بن سعد، مرجع سابق، ص150.

[4] - سوزان عدنان الأستاذ، انتهاك حرمة الحياة الخاصة عبر الانترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية (دراسة مقارنة)، المجلد 29، لعدد 3، 2013، ص 435.

في هذا الصدد فان التطور الهائل لأساليب التجسس الالكتروني من خلال تطوير الفيروسات الالكترونية فاق تطور نظم الحماية الالكترونية، ففي دراسة أجرتها شركة كاسبرسكي لابkaspersky lab سنة 2014 في مجال مكافحة الفيروسات وحماية الأجهزة الالكترونية من هجمات الهاركز، أظهرت أن نحو 315 ألف تطبيق خبيث يحاول اختراق أجهزة الاتصالات الالكترونية يوميا، وهو ما يشكل تهديدا وخطرا على جميع المستخدمين[1] .

2.1.2. استخدام أساليب تقنية أخرى للتجسس الرقمي

نجد من بين الأساليب المستحدثة للتجسس على الخصوصية المعلوماتية استخدام التقنيات الآتية[2]:

- **إخفاء المعلومات داخل المعلومات** : يلجا المجرم من خلال هذا الأسلوب إلى إخفاء المعلومات المهمة بداخل معلومات أخرى عادية في الحاسوب، ثم يجد بعد ذلك وسيلة لتهريب هذه المعلومات الحساسة دون أن يشك أحدا، باعتبار أن الجاسوس لا يلجا إلى الطباعة المعلومات أو عرضها على الشاشة لان في ذلك مخاطرة في أن ينكشف آمره من طرف الضحية الذي يوقفها أو من طرف الحاسوب الذي يسجل محاولاته، ويتم غالبا بكتابة الجاسوس برنامجا وتنفيذه بسرية على حاسوب الضحية ، حيث يقوم البرنامج بفحص كل البيانات المخزنة على الحاسب ثم يومض المصابيح الموجودة على الحاسوب، ليتم بطريقة متخفية قراءة كل المعلومات الموجودة على الحاسوب دون استطاعة احد كشف ذلك[3].
- **استخدام تقنية الأبواب المصيدة أو الخفية**: استخدمت هاته التقنية من طرف احد المبرمجين الذي اعد بابا خفيا في البرنامج المستخدم من طرف إحدى الشركات التي تستخدم حاسب للمشاركة الزمنية وقد سمح له ذلك بالتقاط برامج وبيانات مستخدمين آخرين.
- **ربط الهوائيات مع حاسوب خاص**: يمكن عن طريق الهوائيات التقاط الموجات الكهرومغناطسية المنبعثة من الحاسب عن مسافة 300 قدم خلال فترة تشغيله مع إمكانية تسجيلها ثم معالجتها وترجمتها إلى معلومات.

2.2. وسائل حماية الخصوصية المعلوماتية من جريمة التجسس الالكتروني

أدى النقل الرقمي للبيانات إلى تسهيل التجسس الالكتروني، والسبب يعود بالدرجة الأولى إلى عدم قدرة شبكات الاتصال على توفير الأمان المطلق لسرية ما يتم نقله عبرها من معلومات، لذلك يتم اعتماد وسائل تقنية لمكافحة التجسس الالكتروني، كما أن هناك من التشريعات من تصدت له كفعل مجرم عن طريق مكافحته قانونيا.

1.2.2. الوسائل التقنية لمكافحة التجسس الالكتروني او الرقمي

من بين الوسائل التقنية التي تستخدم لمكافحة وكشف التجسس الرقمي نجد:

---

[1] - سليم حميداني، مرجع سابق، ص43.

[2] - هروال هبة نبيلة، مرجع سابق، ص ص 374-375.

[3] - المرجع نفسه، ص 373.

- **استخدام برنامج كشف ومقاومة الفيروساتAntivirus:** تعمل هذه البرامج على مكافحة الأضرار التي تخلفها الفيروسات وكشفها، لذلك أصبح هناك نوع من التسابق بين مطوري الفيروسات من جهة ومطوري المضادات من جانب أخر[1].

وهناك تقنيات وبرامج متطورة للحماية من التجسس الالكتروني او على الاقل التقليل من مخاطره، منها حماية الشبكات اللاسلكية الداخلية باستخدام تقنية (Mac addres) عوضا عن تقنية (IP Address)، إذ يستطيع مدير الشركة من خلالها تحديد عدد الأجهزة المصرح لها بالاتصال واستخدام الشبكة؛ بالإضافة إلى استخدام برامج متطورة شهيرة مثل[2] :

- برنامج (SPYWARY BLASTER) الذي يقوم بدور المراقب لمنع اية ملفات تجسس من اقتحام الجهاز او الشبكة ، إضافة الى القضاء على تلك البرامج.
- برنامج(AD AWARE) الشهير في مكافحة التجسس اذ يزيل ملفات التجسس غير المرغوب فيها مباشرة.
- برنامج(WEBROOT SPY SWEEPER) وهو برنامج قوي لمكافحة التجسس الالكتروني، فهو يعمل على مراقبة وازالة ملفات التجسس.

- **التشفير المعلوماتي:** وهو عبارة عن عملية تقنية سرية تؤدي الى تحويل المعلومات مفهومة مقروءة إلى إشارات غير مفهومة لا يمكن قراءتها، وبذلك يمكن المحافظة على سلامة البيانات وحمايتها من السرقة والتجسس والاختراق[3]، والتشفير بهذا المعنى نوعين[4] :

- التشفير المتماثل، او ما يسمى بالمفتاح السري، حيث يستخدم كل من المرسِل والمستقبِل المفتاح السري ذاته في تشفير الرسالة وفك تشفيرها، وقد تراجع استخدام هذا النزاع بسبب التبادل غير الامن للمفتاح السري.
- التشفير اللامتماثل، او ما يسمى بالمفتاح العام، فعوضا عن استخدام مفتاح واحد يستخدم مفتاحين اثنين احدهما عام والأخر خاص، تربط بينهما علاقة ، حيث يكون المفتاح الخاص معروفا من جهة المرسِل، يستخدم لتشفير الرسالة وفك شفرتها، أما المفتاح العام فيكون معروفا لدى أكثر من جهة او شخص، وقد تم تطوير هذا النوع ليصبح أكثر أمانا من خلال إضافة البصمة الالكترونية للرسالة.

وعلى العموم فان حماية البيانات ذات الطبيعة الالكترونية خاصة إذا كانت محفوظة على شبكة الانترنت لم تعد أمنة، لذلك يتطلب حمايتها من خلال ضمان دخول امن وحفظها بشكل سري باستعمال كلمة سر غامضة، تكون طويلة ومركبة من أحرف وأرقام ورموز، والابتعاد عن ان مكونة من بيانات شخصية كالاسم واللقب

[1] - صبرينة بن سعد، مرجع سابق، ص 205.
[2] - إسراء يونس هادي، أسامة احمد النعيمي، مرجع سابق، ص 44.
[3] - شريفي الشريف، مرجع سابق، ص ص 125-126.
[4] - حسن بن احمد الشهري، مرجع سابق، ص ص 23-24.

وتاريخ الميلاد او رقم الهاتف، ويجب تغييرها بعد فترة من الاستعمال، ولا ينصح باستعمال نفس كلمة السر لحسابات مختلفة[1] .

2.2.2. الوسائل القانونية لمكافحة التجسس الرقمي

تباين موقف التشريعات بخصوص مكافحة التجسس الالكتروني، فهناك من التشريعات من اكتفت بالنصوص التقليدية المجرمة للتجسس، وهناك من أصدرت تشريعات خاصة أقرت بموجبه حماية جنائية إزاء الاعتداءات على الخصوصية المعلوماتية، في حين قررت تشريعات أخرى تعديل قانون العقوبات بما يشمل تجريم مثل هذه الانتهاكات[2] .

كما أن التشريعات المقارنة استخدمت عبارات وألفاظ غير التجسس، منها التصنت ، الالتقاط، الاعتراض، الدخول دون تصريح وغيرها، وهذا دون تجريم خاص لفعل التجسس الرقمي، بالرغم من تجريمها التجسس التقليدي المتعارف عليه[3].

أما المشرع الجزائري فنجده هو الأخر اكتفى بتجريم فعل التجسس التقليدي في المادة 61 من قانون العقوبات دون الإشارة إلى هذا النوع الحديث للتجسس في البيئة الرقمية، غير انه من جانب أخر عمل على حماية خصوصية الأفراد بطرق قانونية، حيث نجده تمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر 156/66 المتضمن قانون العقوبات، بالقسم السابع مكرر المعنون بـــ(المساس بأنظمة المعالجة الآلية للمعطيات)، في المواد من 394 مكرر الى 394 مكرر7 [4].

الخاتمة

تعد جريمة التجسس الالكتروني مظهرا من مظاهر تهديد الحياة الخاصة في الفضاء الرقمي، إلا أن هذا النوع من الإجرام المستحدث يمس أكثر الدول ومصالحها السياسية والاقتصادية، كما يمس كذلك الحياة الخاصة للأشخاص، ورغم ذلك بقى محصورا ضمن دائرة الإجرام المعلوماتي ولم يجرم كفعل جرامي بشكل مستقل، بناء عليه توصلنا إلى جملة من النتائج نوردها في الأتي:

- يهدف التجسس الالكتروني إلى الحصول بطريقة غير مشروعة على بيانات ومعلومات سرية بطبيعتها، باستخدام أجهزة الحاسوب وبرامجه وأنظمته للاعتداء على شبكة المعلومات السرية.
- للتجسس الالكتروني مظاهر وأساليب ومجالات متنوعة، تسعى للوصول إلى المعلومات الاقتصادية او الاجتماعية أو السياسية...، غير المتاح الاطلاع عليها من طرف العامة، لذلك يصعب تعقب مرتكبيه واكتشافهم، بفعل محو أثاره المادية بعد ارتكابه.

---

[1] - سليم حميداني، مرجع سابق، ص44.

[2] - محمود احمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت (دراسة مقارنة)، دار الفكر والقانون، المنصورة، 2012،ص 61.

[3] - أبو ذر شاكر عبد، مرجع سابق، ص49- 51.

[4] - اوشن حنان، وادي عماد الدين، مرجع سابق، ص 139.

- يشكل التجسس الالكتروني فعلا مجرما، وقد أدرك المشرع الجزائري كغيره من التشريعات المقارنة خطورته من حيث انه يمثل اعتداء صارخ على الحق في الخصوصية المعلوماتية، فتصدى لمظاهره في إطار "المساس بأنظمة المعالجة الآلية للمعطيات" ، دون الإشارة إلي جريمة التجسس الالكتروني .

وعليه، ونظرا لخطورة التجسس الالكتروني وانتهاكه لأمن الأفراد والدول المعلوماتي، بفعل التطور المستمر لأساليبه، نقترح مايلي:

- على الدول عامة والجزائر على وجه الخصوص، القضاء على الأمية الرقمية، من خلال تعليم الشخص معنى الخصوصية الرقمية ورفع الوعي لديه بشان التقنيات الجديدة وهو ما يصطلح عليه بالثقافة الرقمية.
- وضع قوانين وتشريعات تقنن خصوصية البحث على الانترنيت.
- تنظيم مكافحة التجسس الالكتروني، بوضع نصوص واليات قانونية تحدد مظاهره، وأساليبه، وجزائه القانوني.
- تعزيز وتفعيل دور التعاون الدولي من اجل مكافحة التجسس الالكتروني، بما فيه تكريس مبدأ الاختصاص الجنائي العالمي.

قائمة المراجع

1- الكتب

- السيد عبد الحميد احمد، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولي، مكتبة الوفاء القانونية، الطبعة الأولى، الإسكندرية، 2018.
- ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي، المركز العربي ، 2017.
- محمود احمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت (دراسة مقارنة)، دار الفكر والقانون، المنصورة، 2012.

2- الرسائل والمذكرات

- صبرينة بن سعد، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا الإعلام والاتصال، أطروحة دكتوراه، كلية الحقوق، جامعة باتنة، 2015
- هبة نبيلة هروال، جرائم الانترنت (دراسة مقارنة)، أطروحة دكتوراه،جامعة تلمسان، 2014/2013.

3- المقالات

- أبو ذر شاكر عبد، التجسس الالكتروني في ظل التشريع الأردني، مجلة العلوم السياسية والقانون، مجلد4،العدد26،المركز الديمقراطي العربي-برلين، المانيا، 2020، ص 40-53.
- إسراء يونس هادي، أسامة احمد النعيمي، جريمة التجسس الالكتروني في إطار مشروع قانون جرائم المعلوماتية العراقي لسنة 2011، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد10، العدد36، 2021،ص 31-72.
- اوشن حنان، وادي عماد الدين، التجسس الالكتروني واليات مكافحته في التشريع الجنائي الجزائري، مجلة الحقوق والعلوم السياسية،العدد2، جامعة عباس لغرور خنشلة، 2014، ص 130-141.

- حسن بن احمد الشهري، الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس، المجلة العربية للدراسات الأمنية والتدريب، المجلد28، العدد56، 2012، ص 5-32.

- حسين بدر نجف، التجسس والاطلاع على أسرار الغير-دراسة فقهية-، مجلة معين، العدد 7، 2017، ص 71-88.

- حسين ربيعي، المراقبة الالكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد1، 2016، ص409-428.

- حفصي عباس، التجسس الالكتروني في الشريعة والقانون، مجلة الواحات للبحوث والدراسات، المجلد 12، العدد الأول، 2019، ص 270-292.

- الدهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الالكترونية،(دراسة مقارن)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الأول، العدد الثامن،جامعة المسيلة،2017، ص 143-160.

- سليم حميداني، اختراق الخصوصي في العالم الرقمي: حدود الظاهرة ومطالب الحماية القانونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد4، العدد2، 2019، ص 33-46.

- سوزان عدنان الأستاذ، انتهاك حرمة الحياة الخاصة عبر الانترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية (دراسة مقارنة)، المجلد 29، لعدد 3، 2013،ص 421-455.

- شريفي الشريف، مدى احترام الحق في الخصوصية في الحسابات الالكترونية على الانترنت، مجلة القانون والمجتمع، المجلد4، العدد2019،1، ص 161-183.

- عبد الهادي محمود الزيدي، التجسس الإسرائيلي الالكتروني على الدول العربية، مجلة دراسات دولية، العدد58، 2014، ص 137-160.

- عبير علي عبد العزيز شري، مشروعية التجسس عبر الأقمار الصناعية في القانون الدولي العام، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلد9، العدد2019،2، ص 781-809.

- ليث الدين صلاح حبيب، التجسس وأحكامه إبان النزاعات المسلحة الدولية، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلد1، العدد1 ص300-323.

- معاشي سميرة، الجريمة المعلوماتية، مجلة المفكر، العدد 17، 2018، ص 397-417.