التجسس وانتهاك حق الخصوصية في العصر الرقمي
دراسة وصفية تحليلية لبرنامج "بيغاسوس"

Espionage and violation of the right to privacy in the digital
Subtitle A descriptive and analytical study of the "Pegasus" program;

مريم نباش
جامعة الجزائر 3 (الجزائر)
nebbache.meriem@univ-alger3.dz

سعاد بولقرون
جامعة الجزائر 3 (الجزائر)
Boulgoune.souaad@univ-alger3.dz

ملخص

تهدف هذه الدراسة إلى معرفة مدى أهمية أمن وخصوصية المعلومات في العصر الرقمي أمام ظاهرة التجسس الالكتروني وتأثيرها على الحق في الخصوصية، وهذا ما يتطلب توفير آليات حماية المعلومات الشخصية وتأمينها، وقد اعتمدنا على المنهج الوصفي والمنهج التحليلي من خلال التعرض إلى تحليل مضمون التجسس الرقمي أنواعه وخصائصه، والذي سيوضح لنا بدوره انتهاك حق الخصوصية المعلوماتية من طرف برامج التجسس والبحث أيضا في آليات وطرق مكافحتها. كما قمنا بعرض بعض النماذج التي تم فيها اختراق بعض الشبكات والهواتف الذكية من طرف برامج التجسس " بيغاسوس" لنبين في الأخير أهمية أمن الشبكات الالكترونية من المخاطر التي يمكن أن تحدث في حالة عدم توفره، وقد توصلت الدراسة إلى ضرورة اعتماد خطوات عاجلة من أجل التصدي لتفشي برامج التجسس، بالإضافة إلى وقف استخدام وبيع أدوات اختراق الأجهزة الشخصية إلى أن يتم وضع نظام ضمانات كافية لحماية حقوق الإنسان.

كلمات مفتاحية: الخصوصية- برامج التجسس- العصر الرقمي.

Abstract

This study aims to know the importance of information security and privacy in the digital age in front of the phenomenon of electronic espionage and its impact on the right to privacy, and this requires the provision of mechanisms to protect and secure personal information. , which in turn will explain to us the violation of the right of information privacy by spyware and also search in the mechanisms and methods of combating it, and we have presented some models in which some networks and smartphones were hacked by the "Pegasus" spyware, to show in the last the importance of the security of electronic networks from the risks that It can occur if it is not available, and the study found the need to adopt urgent steps to counter the spread of spyware, in addition to stopping the use and sale of hacking tools for personal devices until a system of adequate safeguards is put in place to protect human rights.

Keywords: Espionage prigrams, Spying prigrams. The digital age.

رقمنة
مجلة الدراسات الإعلامية والاتصالية

المجلد 02 | العدد 03
ديسمبر 2022
الصفحات 63 - 78

ردمد |ISSN-2773-4285
2830-8417|EISSN
الإيداع القانوني |07/2021
العنوان |11، طريق دودو مختار، بن عكنون، الجزائر العاصمة.
الفاكس |50 88 23 (023)
الهاتف | 75 29 62 (0561)

تاريخ الاستلام 2022/12/10
تاريخ القبول 2022/12/15
تاريخ النشر 2022/12/31

المؤلف المرسل |
مريم نباش
جامعة الجزائر3 (الجزائر)
الإيميل المهني: nebbache.meriem@univ-alger3.dz

1. مقدمة:

أحدث التطورات الحديثة في تقنيات المعلومات والاتصالات تغيرات جذرية على مستوى جميع المجالات، تجسدت في انتشار استخدام تقنيات وشبكات المعلومات من طرف الشركات والمؤسسات والحكومات وبالتالي ازدياد حجم البيانات التي تعالج وتخزن وتسترجع عند الحاجة إليها، إذ أضحت شبكة الأنترنيت من الضروريات الحاصلة في عصرنا الحديث، بل وحتى في حياتنا اليومية، حيث تنقل عديد من شبكات الحواسيب كما هائلا من المعلومات والبيانات بين الأشخاص والمؤسسات على مستوى العالم، وتتنوع هذه المعلومات والبيانات في أهميتها ودرجة سريتها وخصوصيتها من العامة والعلمية والمعلومات المتعلقة بالإحصائيات الحكومية وكذا والمعلومات الاستخباراتية ذات طابع سري.

وتعمل المنظمات المعاصرة في هذا الإطار على إدارة وتخزين هذه المعلومات والتحكم في الوصول إليها بشكل فعال وتوفير الحماية والأمن من المخاطر والهجمات التي قد تتعرض لها هذه المعلومات من خلال وضع الإجراءات اللازمة لضمان أمن وخصوصيه المعلومة، خاصة وأن هذه الأخيرة تشكل البنية التحتية الأساس في نجاح صنع القرارات وعليه فان للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها وتداولها ووضع السبل الكفيلة بحيازتها، وقد أثار موضوع الحصول على البيانات الشخصية الموجودة في العديد من الملفات المحوسبة وقواعد البيانات الاهتمام لمشكلتي الخصوصية والسرية، إذ تعمل نظم المعلومات على زيادة إنتاج وتوفر البيانات على الجماعات والأفراد، ومن ثم زيادة التحكم في الجماعات والأفراد.

اليوم ومع تدفق المعلومات والبيانات الهائل في الفضاء الرقمي وهيمنة العالم الافتراضي على جميع المجالات، ظهرت ثورة رقمية شاملة لكل المستويات استطاعت جذب كافة شرائح المجتمعات وتقديمها لبدائل تواصلية مجانية وفعّالة، وهذا ما أفرز بدوره تحديات جديدة مرتبطة بمدى حماية البيانات والمعلومات الخاصة عن الأفراد لاسيما مع ظهور الأجهزة الذكية وما تحمله من تطبيقات مبهرة ومتنوعة، حيث أصبحت هذه البيانات الآن معرضة لكشفها والوصول إليها عن طريق هجمات الفضاء السيبرانيوالاستحواذ على المعلومات والتسابق المحموم للسيطرة على هذا الفضاء لاسيما وأنه أصبح يشكل عنصرا حيويا لأمن الدول كما يعتبر أحد أكبر التحديات الخطيرة ، بعد دخول المجال الرقمي ضمن المحددات الجديدة لمؤشرات القوة وأبعادها الجديدة من حيث طبيعتها وأنماط استخدامها، بل وأيضا طبيعة الفاعلين، وهو ما كان له انعكاس على قدرات الدول وعلاقاتها الخارجية.

فالخصوصية تعتبر حق من الحقوق اللصيقة بالشخصية والملازمة للشخص باعتباره إنسانا، لذلك اتجهت التشريعات الدولية إلى حمايته من أي انتهاك سواء كانت صادرة من سلطات الدولة أو أشخاص عاديين، إلا أن هذا الحق تأثر بالتطور الرقمي الذي يمثل مجالا واسعا يكثر فيه انتهاك هذا الحق، ومن بين ما يهدد هذا الحق ما يسمى بالجوسسة الرقمية أو الإلكترونية عن طريق اختراق المواقع الالكترونية والاعتداء على خصوصية الأفراد والمؤسسات الحكومية بفعل التطور السريع لتكنولوجيا المعلومات خاصة بفعل الهواتف والأجهزة والكاميرات الذكية.

وهناك دول من أساءت إلى استخدام أدوات الاختراق الحاسوبي الاقتحامية "برامج التجسس"، باستعمال لأدوات المراقبة على غرار برنامج "بيغاسوس"، الذي اثار الكثر من الجدول إذ بدايته ظهوره و استخدامه، أين يعمل على تحويل الهواتف الذكية إلى "أجهزة مراقبة تعمل على مدار الساعة"، بذريعة الحفاظ على الأمن العام، وبهذا يصبح الحق في الخصوصية معرض للخطر اليوم أكثر من أي وقت مضى، فيما حذر تقرير للأمم المتحدة من تفاقم المخاطر التي تهدّد الخصوصية وحقوق الإنسان من خلال استخدام برامج التجسس والمراقبة، وفي هذه الورقة البحثية سنحاول الإجابة على الإشكالية التالية : **فما مدى تأثير برامج التجسس والمر اقبة على الحق في الخصوصية ؟**

<u>التساؤلات الفرعية</u>

- **ما هي التكنولوجيا الرقمية التجسسية وأخطر أدواتها في انتهاك الخصوصية؟**
- ما مدى أهمية أمن وخصوصية المعلومات في العصر الرقمي؟
- كيف يمكن حماية وتأمين حق الخصوصية المعلوماتية أمام ظاهرة التجسس الالكتروني ؟.
- ما هي التحديات التي تواجه الخصوصية في العصر الرقمي؟

2. الجانب المنهجي

1.2 أهداف الدراسة :

يهدف هذا البحث الموسوم ب " التجسس وانتهاك حق الخصوصية في العصر الرقمي، دراسة وصفية تحليلية لبرنامج "بيغاسوس" إلى معرفة مدى أهمية أمن وخصوصية المعلومات في العصر الرقمي في العصر الراهن الذي يعيش ضمن ثورة معلوماتية القوي يأكل الضعيف وظهور أهمية الفائقة للمعلومة بالنسبة للدول من اجل حماسة سيادتها ومصالحها هذا من جهة من جهة أخرى حتى المؤسسات الاقتصادية الكبرى تسعى إلى البحث عن احتياجات وتفضيلات جماهيرها من أجل استهداف بالشكل المطلوب من خلال هذا طرحت فكرة الخصوصية والأمن المعلوماتي ، بالإضافة إلى ذلك من أهمية الموضوع هو الحاجة الماسة ماسة للمعلومات إذ أنه يهدف هذا الموضوع إلى تبيان أهمية أمن الشبكات الالكترونية والمخاطر التي يمكن أن تحدث في حالة عدم توفره، في حماية المعلومات الشخصية وكيف يمكن وتأمين حق الخصوصية المعلوماتية أمام ظاهرة التجسس الالكتروني.

2.2 منهج الدراسة:

اقتضت منا الإجابة على الإشكال المطروح وفق أهداف وطبيعة الدراسة توظيف المنهج الوصفي والتحليلي، من خلال التعرض إلى تحليل النظري التجسس الرقمي أنواعه وخصائصه، والذي سيوضح لنا بدوره انتهاك حق الخصوصية المعلوماتية من طرف برامج التجسس والحث أيضا في آليات وطرق مكافحتها ،هذا من جهة من جهة أخرى التعرض والوقوف على مدرى خطورة هذا البرنامج عل خصوصية الأفراد وعلى تهديد أمن واستقرار الدول و للإجابة على هذا السؤال الرئيسي لابد لنا أن نعرض بعض النماذج التي تم فيها اختراق بعض الشبكات والهواتف الذكية من طرف برامج التجسس لنبين أهمية أمن الشبكات الالكترونية والمخاطر التي يمكن أن تحدث في حالة عدم توفره.

3.2 أدوات جمع البيانات :

الأدوات المستخدمة في هذا هو أداة المقابلة العلمية مع مجموعة من الخبراء في أمن المعلوماتي للإفادة حول برنامج "بيغاسوس" وعن التكنولوجيات المستخدمة في هذا النوع من الاختراق وكذا على الآليات التي يمكن من خلالها التصدي لمثل هذه الهجمات بالإضافة للاستفادة عن الطرق الواجب اتباعها لحماية الفرد نفسه من الاختراق والجوسسة التي يتعرض لها، بالإضافة إلى استخدام أداة تحليل الوثائق عن طريق الاطلاق عن جل المواثيق والقوانين الدولية والوطنية في أمن وحماية خصوصية الأفراد والدول وحتى المؤسسات.

4.2 مصطلحات الدراسة:

اختلف مفهوم الخصوصية حسب العصور، المؤسسات والأفراد، حيث أن الخصوصية ليست حقيقة طبيعية ثابتة وأن إعادة تعريف حدودها يتم باستمرار، لقد تمكن أرسطو من التمييز الكلاسيكي:

1- خصوصية المعلومات:

ذكر زي حسن الوردي الخصوصية ضمن إطار تقنية المعلومات تعني كيفية جمع واستخدام وحماية المعلومات الشخصية وقد أدت القدرات الهائلة لتقنية المعلومات في خزن واسترجاع المعلومات إلى ظهور الحاجة لحماية الخصوصية الشخصية وقد اعتبر هذا الموضوع من أهم موضوعات التسعينيات واكثرها سخونة ومن بينها على سبيل المثال : هل يعد استخدام المعدات المؤتمنة في تحديد مصدر الاتصال الهاتفي أو المعلومات عن الاتصال المدفوع انتهاكا للخصوصية؟ هل يمكن عد بعض قدرات شركات الهاتف لمعرفة موقع الشخص الذي يقوم بالاتصال انتهاكا للخصوصية ؟ (منال وجيه - محمد سيد أحمد، 2014)

يرتبط موضوع الخصوصية إرتباطا وثيقا بتطور ونمو الاجتماعي الذي يضعف معه الاهتمام به في المجتمعات البسيطة، لكن الأمر يختلف في المجتمعات الحديثة، حيث تتميز بضخامة أعدادها وضعف الروابط فيها بين أفرادها، واضمحلال التضامن الاجتماعي، مما يجعل كل فرد حريص على أن يغلف حياته الخاصة في إطار من السرية، أين يطرح هذا الأمر الحالي في وقت الانترنت والعالم الافتراضي هذا العالم الذي تسبح فيه حياتنا الخاصة ومعطياتها وفق البرامج الالكترونية والرقمية و خاصة المنصات الاجتماعية التي تخزن البيانات الخاصة للمستعمل أو الفرد السابح في العالم الافتراضي وهنا مكمن الأخطار التي تهدد حق الخصوصية للفرد فأصبح بذلك الحق في الخصوصية يستجيب لمتطلبات لوضعيات ومتطلبات جديدة أفرزتها البيئة الرقمية التكنولوجية.(نساخ، 2022)

وقد أثار موضوع الحصول على البيانات الشخصية الموجودة في العديد من الملفات المحوسبة وقواعد البيانات الاهتمام لمشكلة الخصوصية والسرية، إذ تعمل نظم المعلومات على زيادة إنتاج وتوفر البيانات على الجماعات والأفراد، ومن ثم زيادة التحكم في الجماعات والأفراد، فالبيانات الخاصة عن الأفراد أصبحت الآن معرضة لكشفها والوصول إليها عبر الوصول العام.

وترتبط الخصوصية بالسرية لكنهما يختلفان في المعنى، فالسرية تعني أو تدل على أن هناك موضوعا معينا لا يجوز نشره وبثه للآخرين لأنه يتضمن معاملات تجارية أو استراتيجية عسكرية أما الخصوصية فتدل على القيود الخاصة بالبيانات الشخصية، وضرورة إتاحتها أو الوصول إليها بالطرق العامة الشائعة، وبأي في هذا الإطار موضوع التحكم في المعلومات والذي يتضمن وجوده منافذ للحد من وعي الأفراد وهنا كأسباب وراء هذه القيود قد تكون عامة أو خاصة . (منال وجيه - محمد سيد أحمد، 2014)

فقد لا ترغب الدولة في تعريف الجمهور العام في كيفية مواجهتها للعدو فقد ترغب شركة في حجب معلومات معينة عن أحد الاختراعات بعيد عن منافسيهم وقد يرغب أحد الأثرياء في عدم معرفة الناس بوضعه المالي وعاداته في الإنفاق وقد يكون العكس هو الصحيح. فعل سبيل المثال قد ترغب بعض الدول المتقدمة في نشر تقارير عن قوتها العسكرية كقوة ردع للأفعال المعادية وقد يرغب أحد أفراد المجتمع في تعريف الجميع بثروته وذلك للتأثر على وضعه، أي أن التحكم في المعلومات يتضمن القدرة على نشر المعلومات ومنعها في الوقت نفسه.

إن الدول المتقدمة التي قطعت شوط أكبر في استخدام الحواسيب وبنوك المعلومات قد تفطنت إلى هذه الناحية وسنت التشريعات للمحافظة على هذه الخصوصية. فقد صدر في الولايات المتحدة الأمريكية عام 1974قانون حماية الخصوصية الذي قامت بإعداده لجنةمتخصصة، وحددت فيه عدة مبادئ لحماية الخصوصية منها :

- لا يجوز القيام بإعداد شبكات سرية للمعلومات تحتوي على بيانات الأفراد .
- من حق الفرد أن يعلم ويرى محتويات أي سجل يحتوي بياناته الشخصية وأين وكيف تستخدم.
- كما أن من حقه أن يمنع استخدام بياناته الشخصية في الأغراض التي جمعت من أجلها.
- من حقه أن يصحح البيانات أو يعدلها في حال وقوع خطأ من قبل الآخرين عند تسجيلها أو إعدادها.

- وأخيرا فإن من يستخدم البيانات الشخصية يكون مسؤولا عن تصحيحها أو استخدامها استخداما غير صحيح .(منال وجيه - محمد سيد أحمد، 2014)

2. **الخصوصية الرقمية:**

وكتب الفقيه الفرنسي ميلر عام 1972 معلقا على انتهاك الحواسيب لحاتنا الشخصية: " إنّ الحاسوب بشراهته لجمع المعلومات على نحو لا يمكن وضع حد لها، وما يتصف به من دقة ومن عدم نسيان ما يخزن فيه قد يقلب حياتنا على عقب، يخضع فيها الأفراد لنظام رقابة صارم، ويتحول المجتمع بذلك إلى عالم شفاف ، تصبح فيه بيوتنا ومعالنتها المالية وحياتنا العقلية والجسمانية عارية لأي مشاهد.(يحي الشريف نصير - مزغيش عبير، 2022)

وقد اتجه الفقيه الأمريكي ويليام بروسر في تعريفه إلى الابتعاد عن التعريف المجرد للخصوصية، بل اعتمد على تعدد العناصر التي تدخل في إطارها، وتكوم ما يمكن تسميته بالحياة الخاصة، أين اعتبر أنه يمكن رفع دعوى قضائية مدينة لدفع الاعتداء الذي يقع على الحياة في الحالات أربع:

- انتهاك أو اقتحام عزلة أو خلوة الفرد بالاعتداء على حرمة مسكنه، أو التصنت على محادثاته، أو تصويره.
- إفشاء العلني للوقائع الخاصة والماسة باحترام الشخص العادي.تشويه سمعة شخص في نظر الآخرين .
- استخدام اسم الفرد أو صورته أو ملامحه لكسب تجاري دون موافقته .

كل هذه لتعاريف كانت لمعاني الخصوصية لمفهومها الواسع: أما الحق في الخصوصية الرقمية فهو مفهوم يقترن بالمعلوماتية ومختلف استخداماتها، كون هذه الأخيرة اليوم تحتل جانبا هاما من الحياة الخاصة للأراد بداية من الستينات من القرن الماضي .(يحي الشريف نصير - مزغيش عبير، 2022)

وتم تعريف الخصوصية الرقمية على أنها تعني حماية جميع البيانات التي ينشئها المستخدم أو ينقلها أثناء تصفح الويب من خلال جهاز محمول أو سطح مكتب، أو بأنها قدرة على التحكم بدورة المعلومات المتعلقة بهم، أي أنها تحكم الأفراد في مدى توقيف وظروف مشاركة حياتهم، فهي تمكين المستخدمين وحدهم من منع الآخرين أو السماح لهم بالاطلاع على البيانات الرقمية المتعلقة بحياتهم الخاصة، فهي تشكل مستحدث للخصوصية لها علاقة مباشرة بالمعلومات الرقمية، لأن جانبا مهما من المعلومات الحاسة والخاصة بالأفراد قد أضحى اليوم متاحا عبر الأنظمة المعلوماتية والانترنت خاصة، بحيث يصعب تعقبه أو استرجاعه .(يحي الشريف نصير - مزغيش عبير، 2022)

ونظرا لتغير المشهد مع إنشاء الإنترنت ووسائل التواصل الاجتماعي، فقد اختلف مفهوم الخصوصية عما كان عليه قبل قرن أو حتى أربعين عاما، مما جعل قوانين الخصوصية الحالية و أضرارها غير كافية الإطلاق لمعالجة مشاكل و آثار الخصوصية الرقمية .(يحي الشريف نصير - مزغيش عبير، 2022).

3. **صور انتهاك الحق الخصوصية :** يأخذ انتهاك الحق في الخصوصية طرقا عديدة وأشكالا متنوعة تحت مسمى مقتضيات حماية الأمن الوطني يمكن أن نوجزها فيما يلي: (خليف، دت)

- جمع وتخزين بيانات شخصية صحيحة على نحو غير مشروع: إذ يحدث أنّ تقود الجهات الأمنية حملة بحث عن مشتبه فيهم افتراضيين دون الرجوع إلى سلطة قضائية لمنحها الإذن في مباشرة ترصد وتعقيب الأفراد وبالتالي يكون أمام فعل واضح لانتهاك الحق الحق في الحياة الخاصة للأفراد في عملية جمع وتخزين بيانات صحيحة عنهم، لكن على نحو غير مشروع وغير قانوني، ويستمد هذا الجمع أو التخزين صفته فجوة غير المشروعة: ومن بين نلك الأساليب ما يلي: مراقبة أو اعتراض والتقاط وتفريغ الرسائل المتبادلة عن طريق البريد الالكتروني، توصيل أسلاك بطريقة خفية إلى الحاسب الآلي الذي تخزن داخل البيانات المطلوب الاستيلاء عليها .

- التجسس الرقمي على الحياة الخاصة: : ذلك باستعمال التقريب والمقابلة بين مستعمل برامج الإحصائيات في نطاق أمني مشترك ثم ربطها ببعضها البعض ومنه الحصول على ترجمة فورية لحياة لفرد مثل الحصول على رقم رصيده البنكي عمولاته وتواريخ تذاكر سفره رقم التأمين الاجتماعي لخاص مع إمكانية وقوع هذه المعلومات في أيدي غير مختصة أو مرتبطة بأجهزة الأمن لأنه في بعض الأحيان تستعمل هذه الأجهزة عملاء مدنيين أو مؤقتين أو الاستعانة بشركات أمنية خاصة . وتزداد الأمور تعقيدا عندما يتم التطفل على البريد الالكتروني من الجهات الرسمية بداع التصدي لقضايا حماية الأمن الوطني أو الحفاظ على النظام العام، وعلى سبيل المثال نجد أنه صدر قانون التصنت الأمريكي الذي يسمح لوكالة الاستخبارات الأمريكية بمراقبة المكالمات الهاتفية فيه والبريد الالكتروني الخاص بالأجانب وبالمقيمين في الولايات المتحدة الأمريكية دون إذن قضائي ويمنح السلطات الأمريكية حق التحري على كل المكالمات .
- الإفشاء غير المشروع للبيانات وإساءة استعمالها: إنّ الطرق والأساليب التي تستخدمها أجهزة الأمن الحكومية تعتمد في غالبها على نشر البيانات المحصل عليها رقميا على أوسع نطاق مما يجعل هذه الأجهزة تقع تحت طائلة إفشاء غير المشروع لبيانات رقمية لعديد الأفراد ومن المتصور في هذه الحالة أنّ يتم الجمع والتخزين والمعالجة لبيانات شخصية بصورة مشروعة ولكن على العكس من ذلك يتم إفشائها من قبل القائمين على حفظها بصورة غير مشروعة أو قد يساء استخدامها من قبلهم بشكل و بآخر .
- عدم الالتزام بالقواعد الإجرائية في عملية جمع ومعالجة ونشر البيانات الشخصية : فقد تضطر الحكومات إلى الاستعانة بقطاعات أخرى اقتصادية أو إدارية لها صلاحيات معالجة بيانات رقمية شخصية للمواطنين أو غير مواطني تلك الدولة فتأخذ هذه البيانات وتعالجها رغم أنّ القانون قد يوجب ضرورة قيام الجهات الراغبة في جمع وتخزين ومعالجة بيانات شخصية شخصية ضرورة الحصول على ترخيص مسبق لممارسة هذا النشاط قبل مزاولتها إياه، وعليه فأي عدم التزام بما تنص عليه القوانين ذات الصلة بالخصوصية للبيانات الشخصية ستعتبر انتهاكا صارخا لحق الخصوصية للأفراد والجماعات
- التسلل الرقمي: حيث تمارس بعض الدول بحجة حماية الأمن القومي عن طريق التسلل داخل بيانات الشركات و المؤسسات العامة والخاصة بغية أخذ معلومات شخصية تمس حياة الموظفين والعمال والاطلاع على ملفاتهم دون إذن بذلك ، فإذا انطوت المراقبة على ممارسة الدولة للسلطة أو للسيطرة الفعلية فيما يتعلق بالهياكل الأساسية للاتصالات الرقمية، يجب على الدول أن تتقيد بالتزاماتها المتعلقة بحقوق الإنسان كلما قامت بهذه المرابة .ويشمل ذلك مثلا، التصنت المباشر على الهياكل الأساسية للاتصالات أو اختراقها، وممارسة الدولة للولاية التنظيمية على طرف ثالث يتحكم ماديا في البيانات، ونسخ كل البيانات الرقمية والمعلوماتية لهذه الشركات والمؤسسات واستغلالها في عمليات أبحاث أمنية أو استخباراتية .(خليف، دت)

3. الحماية الدولية للحق في الخصوصية الفردية:

أدى النمو العالمي في الاتصالات الرقمية إلى زيادة ممارسات المراقبة الجديدة على الانترنت، ولقد تم تبرير استخدام ولقد تم تبرير استخدام هذه الأساليب في ظل أطر قانونية عفي عليها الزمن إلى تدخلات واسعة ومخالفة في حق الخصوصية خاصة الرقمية منها، مما استدعى بذل الكثير من الجهود سواء على مستوى الاتفاقيات الدولية ومختلف المواثيق أو على مستوى التشريعات الداخلية، بما يتماشى وحماية حق الخصوصية في المجال الالكتروني أو استحداث تشريعات خاصة تغطي هذه الحماية . (بلعسل بنت نبي ياسمين- مقدر نبيل، 2021)

4. أثر الوسائل التقنية للمعلومات الحديثة على الحق في الخصوصية:

نظرا لما توصل إليه العلم الحديث من وسائل وتقنيات جديدة فينقل المعلومات أو كشفها خلف هذا أثر على خصوصية البشر، منها ما هو إيجابي، ومنها ما هو سلبي، وهذا ما سوف نتطرق إليه على التوالي:

1.4 الآثار الإيجابية لوسائل تقنية المعلومات الحديثة على الحق في الخصوصية:

أصبح عالمنا فائق السرعة من خلال عصر المعلوماتية، وهذا من خلال تطور وسائل الاتصال الحديثة ومنها الشبكة العنكبوتية والهاتف المحمول، وكذلك الاتصال عبر الأقمار الصناعية والذي يعرف اليوم باسم الانسياب الدولي للمعلومات. هذه الوسائل الاتصالية الحديثة أضحت تؤدي خدمات جليلة للبشرية، لا غنى لأي مجتمع عنها، وتبرز آثارها الإيجابية على الحق في الخصوصية، وإن من حق مستخدمي وسائل الاتصال الحفاظ على سرية معلوماته وبياناته وسرية الاتصالات التي يجريها، حيث أصبحت خصوصيات الأفراد وأسرارهم ومعلوماته الخاصة داخل الأجهزة الإلكترونية وشبكات المعلومات، حيث أن المعاملات اليومية صارت تعتمد على شبكة الانترنيت بصفة شبه أساسية. فلوسائل تقنية المعلومات الحديثة القدرة الفائقة في عملية تحليل واسترجاع المعلومات، وهذا ماجعل الدول إلى إنشاء قواعد البيانات لتنظيم عملها، كما أن استخدام هذه الوسائل اتسع في جمع وتخزين ومعالجة البيانات الشخصية لأغراض متعددة، خاصة وأن كافة المعلومات المتعلقة بجميع جوانب الحياة الخاصة يمكن جمعها وخزنها لفترة غير محدودة، كما يمكن الرجوع إليها جميعا بمنتهى السرعة والسهولة.(لخشين، 2021)

2.4 الآثار السلبية لوسائل تقنية المعلومات الحديثة على الحق في الخصوصية:

على الرغم من أهمية وسائل تقنية المعلومات الحديثة، ومالها من آثار إيجابية سبق بيانها، إلا أن هنالك مخاطر عديدة تواجه الحق في الخصوصية بالنظر لإمكانية انتهاكه عبر وسائل تقنية المعلومات الحديثة، ذلك أن سهولة عمليات التخزين والمعالجة الالكترونية وازدياد تدفق المعلومات التي تتم عبر وسائل تقنية المعلومات الحديثة، تضعف قدرة الفرد على التحكم في تدفق المعلومات الخاصة به، إذ أصبحت المعلومات الشخصية في ظل الشبكة العالمية متوفرة مايؤدي إلى ازدياد التهديدات لخصوصية الناس، وقد أصبح الوصول إلى المعلومات الشخصية بصورة غير مشروعة أكثر من ذي قبل، وازدادت فرص إساءة استخدامها.(لخشين، 2021)

إضافة إلى ذلك فقد ازدادت عمليات مراقبة الأفراد وملاحقتهم، وعمليات التعدي على خصوصياتهم من خلال الوصول إلى سجلات البيانات المخزنة، كما أن وسائل تقنية المعلومات الحديثة ساعدت على عولمة المعلومات والاتصالات عبر الحدود دون اعتبار للجغرافية والسيادة بحيث تعطى المعلومات لجهات داخلية وخارجية بل وتعطى لجهات مجهولة وهو ما يثير إساءة استخدام البيانات خاصة في الدول التي لا توفر حماية قانونية للبيانات الشخصية أو أنها لا تستطيع توفيرها فانتشار النقل الرقمي للمعلومات والبيانات الشخصية أدى إلى ظهور جرائم ماسة بحرمة الحياة الخاصة عبر وسائل تقنية المعلومات الحديثة كالتجسس الإلكتروني، وتعدد تصوره منها ماهو بواسطة الهاتف.

فأنشطة الاختراق امتدت بشكل كبير إلى نظم الهاتف، ومنها من خلال البريد الإلكتروني، حيث يحدث التجسس الإلكتروني بواسطة البريد الإلكتروني من خلال القيام بإرسال ملفات مرفقة ضمن رسالة عادية والتي تكون في الغالب مجهولة المصدر بالنسبة للضحية، وعند فتح هذه المرفقات يتم الدخول على جميع الملفات الموجودة في جهاز الكمبيوتر وتتبّع حركات صاحب الحساب ونشاطه. إذ أن الوسائل الإلكترونية أتاحت وسائل رقابة عالية سمعية ومرئية ومقروءة فأصبحت هنا كقدرة عالية على جمع المعلومات ومعالجتها إلكترونيا.

وبالنظر لانتشار استخدام وسائل تقنية المعلومات الحديثة فقد ازدادت جرائم الاعتداء على البيانات الشخصية وبصورة متعددة الأمر الذي يبرز أهمية التوفيق بين ضرورة وأهمية وفائدة وسائل تقنية المعلومات الحديثة، وبين تفادي ما يمكن أن يصيب الأفراد من أضرار في خصوصياتهم من استخدام هذه الوسائل. (لخشين، 2021)

5. التجسس الالكتروني:

تُعدّ الجاسوسية مهنة من أقدم المهن التي مارسها الإنسان داخل المجتمعات البشرية منذ فجر التاريخ الإنساني، فكانت تدفعه إليها غريزته الفطرية للحصول على المعرفة ومحاولة استقراء المجهول وكشف أسراره التي قد تشكل خطرًا يترصد به في المستقبل.

فاليوم ونحن في القرن 21م،أصبح للتجسس الإلكتروني أبرز التهديدات الأمنية الحديثة التي تتعرض لها الحكومات والمواطنون من طرف استخبارات خارجية أو أخرى داخلية تجاه مواطنيها على حدسواء. وقد تضاعفت عمليات التجسس الإلكتروني مع التطور التكنولوجي الحاصل في خوادم الإنترنيت، حتى أن هناك من الحكومات من شرّعت بشكل غير مباشر للتجسس الإلكتروني داخليا وخارجيا على المؤسسات والمواطنين.

والتجسس الإلكتروني أو ما يعرف بحرب التجسس المعلوماتي هي عبارة عن عدة طرق لاختراق المواقع الرقمية ومن ثم سرقة بعض المعلومات والتي قد تكون في قائمة الأهمية والخطورة للطرف المتلقي والمسروق منه وقد انتشرت في الألفية الجديدة بانتشار طرق الاختراق وأحيانا قد يكون الاختراق من أشخاص عابثين ليس إلا وأحيانا بغرض سرقة معلومات مهمة مثلما حدث لوزارة الدفاع الأمريكية البنتاغون في السنوات الماضية من قبل أشخاص لا يتبعون لأي تنظيم إرهابي أو ثوري بل أشخاص عابثين. وكما تم اختراق موقع وزارة الدفاع الفرنسية سابقا بغرض سرقة معلومات عن الاستطلاعات والمناورات والنظام الصاروخي الفرنسي. وليس الاختراق محصورا على المؤسسات العسكرية فكذلك قد تتعرض له المؤسسات النقدية وخصوصا البنوك المركزية والمؤسسات العملاقة.(الجوسسة ارقمية والأمن القومي: برنامج بيغاسوس الاسرائيلي نموذجا ، 2021-7-22)

6. الموقف القانوني والدولي من برنامج بيغاسوس

1.6 برنامج بيغاسوس:

تعتبر "إسرائيل" الأولى عالميًا في عمليات التجسس الإلكتروني وتمتلك 27 شركة متخصصة في هذا المجال، والغريب أن أمريكا وبريطانيا وفرنسا وروسيا والصين لا تمتلك مجتمعة هذا العدد، حيث تمتلك "إسرائيل" 8200 وحدة لتنفيذ الحرب الإلكترونية والتجسس الإلكتروني، وعند تقاعد خبراء هذه الوحدة الفنية عالية التدريب يتم اجتذاب شخوصها إلى الشركات الإسرائيلية المختصة في هذا المجال لتدريبهم مجموعات جديدة.(الجوسسة ارقمية والأمن القومي: برنامج بيغاسوس الاسرائيلي نموذجا ، 22-7-2021)

ولعل برنامج **بيغاسوس الاسرائيلي** هو من أحدث و أخطر البرامج التجسسية و أكثر تطورا، حيث يُمكِن تثبيته على أجهزة تشغيل بعض إصدارات نظام آي أو إس (أبل) أو أي نظام آخر، من أجل التجسس على الشخص المستهدف ومعرفة ما يقوم به على هاتفه المحمول والاطلاع على ملفاته وكل الصور أو الوسائط التي يحتفظ بها في الجوال. اكتُشفت هذه البرمجية في آب/أغسطس 2016 وذلكَ بعد فشل تثبيتها على أيفون أحد النشطاء في مجال حقوق الإنسان الإماراتي "أحمد منصور"، ما مكَّن شركة أبل من الانتباه لها والانتباه لاستغلالها الثغرات الأمنية بهدف الاختراق والتجسّس.بشكلٍ عام فبرمجيّة بيغاسوس قادرة على قراءة الرسائل النصية، تتبع المكالمات، جمع كلمات السر، تتبع موقع أو مكان الهاتف وكذا جمع كلّ المعلومات التي تُخزنها التطبيقات. حينَ اكتشاف البرمجيّة؛ أصدرت شركة أبل نسخة 9.3.5 وذلكَ بهدفِ إصلاح نقاط الضعف التي احتوت عليها النسخة السابقة. حظيت هذه البرمجيّة بشهرة كبيرة وبتغطيّة إعلاميّة خاصة بعدما انتشرت أخبار تُفيد باستعمالها في التجسس على شخصيات مهمة في مُختلف المجالات. أَطلقت عليها بعضُ وسائل الإعلام لقبَ «البرمجيّة الأكثر تطورًا» وذلك بعدَ نجاحها في التجسس على هواتف أيفون المعروفة بقوّة حمايتها لبيانات المستخدم مقارنة بأنظمة تشغيل أخرى. من ناحية أخرى؛ ذكرت الشركة المصنعة للبرمجيّة وهي شركة إن إس أو أنّ لها إذنًا من بعض الحكومات للاستمرار في صناعة البرنامج وذلك للمساعدة على مكافحة الإرهاب والجريمة على حد زعمها.

عمليًا؛ البرنامج لا يعمل من تلقاء نفسه بل يستهدف المستخدم من خِلال دفعه بطريقة من الطرق إلى النقر على رابط خبيث مما يُمكّن من تحميل بيغاسوس التي يتمثلُ دورها في كسر آي أو إس على الجهاز وبالتالي التمكن من قراءة الرسائل النصية، المكالمات، جمع كلمات المرور، تتبع موقع الهاتف،جمع بيانات التطبيقات بما في ذلكَ جي ميل، فايبر، فيسبوك، واتساب، تيليجرام وسكايب.(الجوسسة ارقمية والأمن القومي: برنامج بيغاسوس الاسرائيلي نموذجا ، 2021-7-22)

2.6 كيف يخترق "بيغاسوس" الهواتف؟

يعتقد الباحثون أن الإصدارات المبكرة من برنامج القرصنة التي كشفت لأول مرة عام 2016، استخدمت رسائل نصية مفخخة لتثبيتها على هواتف المستهدفين. ويجب أن ينقر المستهدف على الرابط الذي وصله في الرسالة حتى يتم تحميل برنامج التجسس، لكن لذلك حدا في فرص التثبيت الناجح لاسيما مع تزايد حذر مستخدمي الهواتف من النقر على الروابط المشبوهة.

خلافا لذلك، استغلت الإصدارات الأحدث من "بيغاسوس" الذي طورته شركة "إن إس أو غروب" الإسرائيلية ثغرات في تطبيقات الهواتف النقالة واسعة الانتشار.ففي عام 2019، رفع تطبيق المراسلة "واتس آب" دعوى قضائية ضد الشركة الإسرائيلية قال فيها إنها استخدمت إحدى الثغرات المعروفة بـ"ثغرة يوم الصفر" في نظام التشغيل الخاص به لتثبيت برامج التجسس على نحو 1400 هاتف، وبمجرد الاتصال بالشخص المستهدف عبر "واتس آب"، يمكن أن ينزل "بيغاسوس" سرا على هاتفه حتى لو لم يرد على المكالمة، وورد في الآونة الأخيرة أن "بيغاسوس" استغل ثغرة في تطبيق "آيميساج" الذي طورته شركة "آبل"، ومن المحتمل أن ذلك منحها إمكان الوصول تلقائيا إلى مليار جهاز "آيفون" قيد الاستخدام حاليا.(الجوسسة ارقمية والأمن القومي: برنامج بيغاسوس الاسرائيلي نموذجا ، 22-7-2021)

3.6 ماذا يفعل البرنامج إثر تنزيله؟

يشرح أستاذ الأمن الإلكتروني في جامعة University of Surrey في المملكة المتحدة آلانوودوارد، أن "بيغاسوس" هو على الأرجح إحدى أكثر أدوات الوصول عن بعد كفاءة."وقال: "فكر في الأمر كما لو أنك وضعت هاتفك بين يدي شخص آخر، يمكن استخدام البرنامج للاطلاع على رسائل الهاتف والبريد الإلكتروني للضحايا، وإلقاء نظرة على الصور التي التقطوها، والتنصت على مكالماتهم، وتتبع موقعهم وحتى تصويرهم عبر كاميرات هواتفهم."(الجوسسة ارقمية والأمن القومي: برنامج بيغاسوس الاسرائيلي نموذجا ، 22-7-2021)

تعريف رامي رؤوف عن برنامج بيغاسوس:برنامج بيغاسوس من البرامج الخبيثة التي تعمل بطرق مختلفة وجزء من تطويرها يتعلق بتطوير آليات الاستهداف. ففي السابق كان يتم استهداف الأشخاص من خلال رابط أو رسالة، ولكن مع بيغاسوس هناك أنماط استهداف حديثة، إذ يكفي أن تقوم جهة ما بالاتصال بالشخص المستهدف لفترة ما بين 8 و10 ثوان، ليتم تنزيل وتثبيت البرنامج حتى لو لم يرد على المكالمة، وعادة هناك طرق معينة يمكن للشخص اكتشاف استهدافه، ولكن برنامج بيغاسوس لكونه برنامجا ذكيا جدا، فيصعب على شخص غير تقني أو مهندس كشفه. ففي برامج التجسس الرخيصة والتقليدية هناك مؤشرات معينة، مثل عمل ضوء كاميرا الهاتف في أوقات غير متوقعة، أو ارتفاع حرارة الجهاز بشكل أعلى من الطبيعي، أو استهلاك البطارية بسرعة أكبر أو تغير خلفية الشاشة، أو ظهور برامج جديدة بشكل مفاجئ، أو يتم استهلاك مساحة التخزين بشكل سريع، ولكن مع بيغاسوس المؤشرات التقنية يصعب على غير الخبير كشفها، لأن الاختراق الناجح، هو الاختراق الصامت الذي لا يمكن الكشف عنه. إذ أن في قائمة الضحايا التي تعاملنا معها، رأينا أن بعضهم خضع للمراقبة منذ 3 سنوات دون دراية منهم، لأنه صعب استنباطه.(سالم، 21-7-2021)

4.6 طريقة الكشف عنه:

الطريقة الأولى هي أن الخبراء يستطيعون الكشف عن بيغاسوس من خلال البصمة الإلكترونية. فلكل برنامج على الإنترنت بصمة إلكترونية مثل بصمة اليد، ومن خلال التسريبات التقنية والإصدارات القديمة لبيغاسوساستطعنا الحصول على البصمة الإلكترونية للبرنامج، ونستطيع من خلال برامج مشروعة ومقارنة البصمات أن نكشف عن وجوده، طبعا في مجال أمن المعلومات هناك مكاتب حرة المصدر، توثق البرمجيات الخبيثة وتعمل على تحرير جميع المعلومات المتعلقة بها، وبهذه الطريقة يمكن الكشف عن البرامج الخبيئة على الهواتف، بمعنى آخر وبشكل أكثر وضوحا؛ فإنه يتم جمع قاعدة بيانات متعلقة بأجهزة تم اختراقها وبصمات الكترونية معينة، ومن ثم تحليلها، واستخدامها لمعرفة إن كان أي جهاز قد تم اختراقه أم لا.

الطريقة الثانية؛ هي أن المجتمع الأكاديمي والمعامل التقنية، لديها معلومات سابقة حول طريقة اختراق بيغاسوس للهواتف، مثلا نعرف أن هناك جهة معينة تستهدف الأفراد من خلال رسالة تحتوي على عنوان نطاق (دومين) معين أو رابط معين، فنبحث عن هذه المؤشرات أيضا ونحذر المستخدم، ولكن هناك نقطة معينة يجب التأكيد عليها، وهي أنه لو فحصنا هاتفا ما ولم نجد برنامج بيغاسوس عليه، هذا لا يعني أنه لم يصب. لأن من ميزات الإصابة الذكية هي حذف الاختراق بحد ذاته، فيمكن أن يقوم البرنامج على اختراق جهاز ما وبعد فترة يحذف نفسه تلقائيا. وبالتالي صعب جدا تأكيد إصابة الجهاز أو عدم إصابته.

5.6 الهواتف الأكثر عرضة للاختراق:

وفقا للأبحاث والمؤشرات لا نعرف إن كان هناك إصدار يستهدف الكمبيوترات حتى الآن، يمكن أن يكون موجودا ولكن لم نكتشفه بعد. وبالنسبة للهواتف فهناك إصدارات مختلفة منه، لهواتف نوكيا وآيفونوأندرويد، وبلاك بيري وغيرها، وعادة شركات التقنية المختصة بالتجسس يكون لديها اختصاص معين، إما بالحواسيب أو بالهواتف، فالبرمجيات الخبيثة لا تعمل بذات الآلية، وتختلف بحسب الأجهزة. فالشركة التي أنتجت بيغاسوس هيNSO ، وهي مختصة ببرامج اختراق الهواتف، لأن استهدافها أرخص من استهداف الكمبيوترات، إذ أن اختراق الهاتف لا يعتمد على استجابة الضحية للاختراق، فيمكن استهدافه من خلال "مكالمة لم يرد عليها"، ولكن في عالم الحواسيب يجب أن يقوم الشخص بأمر ما ليتم اختراق جهازه، وبالتالي الجهد والتقنية مختلفة.(سالم، 21-7-2021)

6.6 أثار برنامج بيغاسوس:

أكدت الكثير من التحقيقات الصحفية أن نشطاء وصحفيين وسياسيين حول العالم استهدفوا بعمليات تجسس بواسطة برنامج خبيث للهواتف الخلوية طورته شركة NSO الإسرائيلية كما أنه يتم استخدام برامج ضارة من الدرجة العسكرية من مجموعة NSO ومقرها إسرائيل للتجسس على الصحفيين ونشطاء حقوق الإنسان والمعارضين السياسيين. ويقول اتحاد 17 مؤسسة إخبارية، إنه حدد أكثر من ألف فرد في 50 دولة اختارهم عملاء "إن إس أو" منذ 2016 للمراقبة المحتملة، بينهم قرابة 200 صحفي.

- رُخّص بيع برنامج بيغاسوس من قبل حكومة إسرائيل للمملكة العربية السعودية، وذلك للتجسس على هاتف الصحفي السعودي جمال خاشقجي وتتبع اتصالاته، والذي اغتيل في عام 2018.
- في الهند في أواخر عام 2019، رفعت فيسبوك دعوى قضائية ضد مجموعة إن إس أو، مدعيه أنه تم استخدام تطبيق الواتساب لاختراق عدد من النشطاء والصحفيين والبيروقراطيين في الهند، مما أدى إلى اتهامات للحكومة الهندية بالتورط .
- بين التحقيق الاستقصائي للعديد من الصحفيين بأن برناجبيغاسوسلديه كثير من خبايا حيث أشار إليه موقع الجزيرة الأخبارية الذي عرضته قناة في حلقة 2020/12/20 "شركاء التجسس" لقطات حصرية يعرضها بينت

اختراق هواتف إعلاميين ونشطاء، منهم صحفيون من قناة الجزيرة والتلفزيون العربي، تستخدمه إسرائيل أو تبيعه للحكومات للتنصت على معارضيها وحتى حلفاؤها.

- في عام 2021، أعلن زعيم حزب "غد الثورة" المصري أيمن نور عن تلقيه إخطارات عديدة بتعرض هاتفه لاختراق من خلال برنامج بيغاسوس، وقال في تغريدة على تويتر عنونها بوسم "فضيحة تجسس" إن شركة بريطانية وجهة أميركية ومختبر كندي أبلغوه بقيام جهة استخباراتية باختراق هاتفه، وأوضح أن ذلك تم "من خلال شفرة ماكرة وبرنامج بيغاسوس لشركة إن إس أو الإسرائيلية والمبيع لأجهزة استخباراتية عربية"

- استخدم برنامج بيغاسوس من قبل عصابات المخدرات المكسيكية لاستهداف وترهيب الصحفيين المكسيكيين والجهات الحكومية .في 18 يوليو 2021 كُشف عن التجسس على المعارضين السياسيين والصحفيين والنشطاء من قبل عدة دول باستخدام بيغاسوس.(الجوسسة ارقمية والأمن القومي: برنامج بيغاسوس الاسرائيلي نموذجا ، 22-7-2021)

7.6 أبرز قضايا التجسس المتعلقة ببرنامج "بيغاسوس":

برز برنامج بيغاسوس في العديد من القضايا العالمية والفضائح التي تناولتها وسائل الإعلام العالمية أين أثارت وأسالت الكثير من الحبر حول محتويات وتسربات مست العديد من الشخصيات المعروفة حول العالم و حتى دول بقيمتها ساهمت في سقوط العديد من الأسماء على الساحة الدولية مما سبب وخلق أزمات حادة وصراعات داخل الدول وبينها يذكر أنّ برنامج «بيغاسوس» في السنة 2021 بعد انتشار لائحة تضم 50 ألف جهة تعرضت للتجسس في مختلف أنحاء العالم، من بينهم صحافيون وشخصيات سياسية وناشطون حقوقيون .(العربي، 2022)

كما وقد أشير كشف عن صفقات بيع أسلحة إسرائيلية لأنظمة استبدادية ارتكبت بواسطتها مذابح وجرائم حرب، كشف أنه طلب من المدعي العام الإسرائيلي فتح تحقيق في كيفية السماح لشركة «أن أس أو» ببيع برنامجها التجسسي في بودابست، موضحا أنه قدم هذا الطلب بالتعاون مع الاتحاد المجري للحريات المدنية الذي يؤكد أن «بيغاسوس» استهدف أربعة صحافيين هنغاريين، فهذا البرنامج التجسّسي يستطيع أن يخترق كاميرا أو ميكروفون هاتف نقال، ويحصل على بياناته كاملة.(العربي، 2022)

ونشرت المفوضية الأوروبية العديد من التقارير الصحفية من المفوضية الاتحاد الأوروبي عن الانتهاكات التي مست العديد من الدول والمؤسسات أن ذكرت التقارير الصحفية إلى إقدام الاتحاد المجري للحرّيات المدنية بتقديم شكاوى إلى الوزراء المجريين الذين يشرفون على المخابرات، وإلى المفوضية الأوروبية،إذ تم رفع عدد كبير من الدعاوى القضائية أمام المحكمة الأوروبية لحقوق الإنسان، مشرين إلى أن جميع الوسائل القانونية ستستخدم من أجل فرض احترام حقوق الذين تمّ التجسس عليهم بشكل غير قانوني. ويمكن الإشارة إلى أنه في نوفمبر/ تشرين الثاني 2021، أكد لاغوس كوسا العضو البارز في الحزب الحاكم بالمجر أن بلاده استخدمت «بيغاسوس» مؤكدًا أن الهدف من ذلك لم يكن التجسس بشكل غير قانوني على المواطنين المجريين. (العربي، 2022)

وفي هذا السياق كشف تقرير صحيفة «نيويورك تايمز» عن صراع أمريكي . إسرائيلي على السيطرة على هذه البرمجية. أين ذكرت بعض التصاريح الصحفية التي نقلت على لسان مراسل الإسرائيلي للشؤون الاستخباراتية رونين بيرغمان إنه «بكل ما يتعلق بالحكومتين الأمريكية والإسرائيلية، فالحديث يدور عن صراع حول من يسيطر على برنامج بيغاسوس، وهو سلاح السايبر الأقوى والأفضل في العالم، وعن الجهة التي تستحوذ عليه ومن يملك الصلاحية بأن يقرر لمن يسمح باقتنائه ومن لا». (العربي، 2022)

7. الوقاية من هذا النوع من البرامج.

الوقاية في مجال أمن المعلومات موضوع كبير جدا، لأن هناك وقاية للأشخاص العاديين، ووقاية للصحفيين أو العاملين في مجال حقوق الإنسان، وهم الأكثر عرضة للاختراق. يجب أن نتذكر أن المراقبة والاستهداف لا يحدثان بشكل تقني فقط، بل هناك أبعاد هندسية وإنسانية. فالوقاية لا تحميك دائما، حتى لو كانت لديك أجهزة لحماية هاتفك، ولو كان الشخص المستهدف مطلعا ولديه معرفة كافية بالتقنيات. فهذا لا يعني أنه أقل عرضة للاختراق.

لأن الاختراق الآن لا يعتمد على الهاتف فقط، بل يعتمد على استخدام الشبكة الوطنية للاتصالات والبنية التحتية. فمثلا في مصر وشمال أفريقيا؛ الشركات المشغلة للإنترنت أو خدمات الهاتف هي شركات تابعة للدولة، فلو كان لديك هاتف وبه شريحة محمول من شركة ما، فالبنية التحتية ملك للدولة، وبالتالي يصبح استهداف الأفراد أسهل من خلال هذه البنية التحتية.

ولكن أهم قاعدة للوقاية هي: لا تضغط على أي رابط، لأن الروابط هي بشكل أساسي الطريقة الأولى لاختراق الهواتف. ويجب أن يكون هناك حذر من استقبال روابط حتى من أشخاص تعرفهم، لأن "الجهات الشريرة" بإمكانها انتحال هويات أشخاص آخرين. وإذا قمت بالضغط على الرابط، فسيتم تسريبه لباقي الأشخاص على هاتفك، ولكن إن شعر الفرد أنه قد تم استهدافه، فبإمكانه "إعادة تهيئة الجهاز" مرتين، لأن هناك برمجيات ذكية يصعب محوها من عملية إعادة تهيئة الهاتف لمرة واحدة فقط. ومع بيغاسوس بالإمكان أن يتم حذف البرنامج إن قمت بإعادة تهيئة الجهاز مرتين.(سالم، 21-7-2021)

1.7 المواثيق القوانين الدولية الوطنية:

بحسب تقرير المفوضية الأمم المتحدة الصادر لسنة 2022، جنيف (في 16 أيلول/ سبتمبر 2022) – فقد حذّر تقرير جديد صدر عن الأمم المتحدة من أن حق الناس في الخصوصية يتعرض لضغوط متزايدة بسبب استخدام التكنولوجيات الرقمية الحديثة المتصلة بالشبكات، التي حوّلتها خصائصها إلى أدوات هائلة للمراقبة والسيطرة والقمع.(المتحدة، أيلول سبتمبر 2022)

وهو آخر تقرير بشأن الخصوصية في العصر الرقمي أعدّته مفوضيّة الأمم المتّحدة السامية لحقوق الإنسان: ثلاثة مجالات أساسية هي: إساءة سلطات الدولة استخدام أدوات الاختراق الحاسوبي الاقتحامية ("برامج التجسس")، والدور الرئيسي للتشفير القوي في ضمان حماية حقوق الإنسان عبر الإنترنت، وآثار تفشي الرصد الرقمي للأماكن العامة، سواء على شبكة الإنترنت أو خارجها

وأوضح التقرير كيف يمكن لأدوات المراقبة مثل برنامج "بيغاسوس"، أن تحول معظم الهواتف الذكية إلى "أجهزة مراقبة تعمل على مدار الساعة"، ما يسمح للجهة "الدخيلة" بالوصول إلى كل ما تحويه هواتفنا المحمولة وباستخدامها كسلاح للتجسس على حياتنا.في حين يُزعَم أنّ أدوات التجسس هذه تُستَخدَم لمكافحة الإرهاب والجريمة، فإنها كثيرًا ما تُستخدم لأسباب غير مشروعة.

وقد أكّد التقرير أنّه من الضروري للغاية اعتماد خطوات عاجلة من أجل التصدي لتفشي برامج التجسس، كما كرّر الدعوة إلى وقف استخدام وبيع أدوات الاختراق الحاسوبي إلى أن يتم وضع نظام ضمانات كافية لحماية حقوق الإنسان. ويجب ضمان ألا تستخدم السلطات عمليات الاختراق الحاسوبي للأجهزة الشخصية إلا كملاذ أخير وأن تستخدمه فقط "لمنع فعل معين يرقى إلى مستوى تهديد خطير للأمن القومي أو جريمة خطيرة محددة أو لأغراض التحقيق في ذلك،" على حدّ ما جاء في التقرير.(المتحدة، أيلول سبتمبر 2022)

والتشفير هو عامل تمكين رئيسي للخصوصية وحقوق الإنسان في الفضاء الرقمي، إلاّ أنّه يتمّ تقويضه حاليًا. ويدعو التقرير الدول إلى تفادي اتخاذ الخطوات التي يمكن أن تضعف التشفير، بما في ذلك فرض ما يُعرَف بالأبواب الخلفية التي

تتيح الوصول إلى البيانات المشفرة للأشخاص أو التفتيش المنهجي في الأجهزة الشخصية، المعروف بالمسح من جانب العميل.(المتحدة، أيلول سبتمبر 2022)

كما دقّ التقرير ناقوس الخطر بشأن المراقبة المتزايدة للأماكن العامة. فقد تم التخلص من القيود العملية المفروضة سابقًا على المراقبة من خلال جمع البيانات آليًا وتحليلها على نطاق واسع، بالإضافة إلى أنظمة الهوية الرقمية الجديدة وقواعد البيانات البيو مترية الشاملة التي تسهّل إلى حد كبير اتساع نطاق تدابير المراقبة هذه.

كما مكّنت التكنولوجيات الجديدة المراقبة المنهجية لما يقوله الناس عبر الإنترنت، بما في ذلك من خلال جمع وتحليل منشورات وسائل التواصل الاجتماعي.وغالبًا ما تفشل الحكومات في إبلاغ الجمهور بشكل كافٍ عن أنشطة المراقبة التي تمارسها. وحتى عندما يتم نشر أدوات المراقبة في البداية لخدمة أغراض مشروعة، يمكن بسهولة تغيير وجهة استخدامها فتخدم غايات لم تكن مخصصة لها في الأصل.(المتحدة، أيلول سبتمبر 2022).

2.7 موقف المشرع الجز ائري من حماية الحق في الخصوصية في مظهرها:" البيانات ذات الطابع الشخصي:

عمل التشريع الجزائري كغيره من التشريعات المقارنة على الاعتراف بحق الخصوصية بشكل عام كمبدأ دستوري من خلال نص المادة 39 بنص صريح " لا يجوز انتهاك حرمة المواطن الخاصة وحرمة بشكل عام كمبدأ ددستوري من خلال نص المادة 39 بنص صريح لا يجوز انتهاك حرمة المواطن الخاصة وحرمة شرفه ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل اشكالها مضمونة"، وقد كرس مبدأ الحماية الجنائية بموجب نص المادة 303 من قانون العقوبات التي نصت على أم يعاقب بالحبس من 6 أشهر إلى 3 سنوات كل من تعمد المساس بحرمة الحياة الخاصة بأي تقنية كانت ذلك:

. التقاط أو تسجيل أو نقل مكالمات أو محادثات خاصة أو سرية بغير إذن صاحبها أو رضاه.

التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها وحمل هذا النص في طياته الحماية المرنة التي تمتد إلى أي طبيعة لحق الخصوصية أو الحديث وهذا باستخدام عبارة أي " تقنية كانت" وعلى الرغم من النص غير المباشر على حق الخصوصية وحق الخصوصية الكترونيا نجد أنه لم يتجه إلى إصدار قانون بالحماية للخصوصية في المجال الرقمي، إلا أن المشرع اكتفى بمواكبة محاربة جريمة المساس بالحق في الخصوصية في العالم الرقمي بموجب رقم 15-04 المتضمن تعديل قانون العقوبات في القسم المعنون" المساس بأنظمة المعالجة الآلية للمعطيات" من خلال نص المادة 39 يعاقب بالحبس من 3 أشهر إلى سنة أو بغرامة من 50 إلى 100 ألف كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.، وكذا جرم عمليات تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو إفشاء أو استعمالها لأي غرض كل المعطيات المتحصل عليها من الجرائم المنصوص عليها في هذا القسم. من جهته فقد وفر المشرع الحماية الجنائية لحق الخصوصية بموجب المادة 04 من القانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهذا بضمان عدم المساس بالحياة الخاصة للأفراد في حالة قيام السلطات المختصة بالقيام بعمليات المراقبة لكل الاتصالات الرقمية بهدف من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة .(خدوجة، 2017)

شرع المشرع الجزائري فيما يخص حماية الخصوصية الخاصة بالأفراد إذ كان صريحا في مثل هذه المسائل أين أصدر قانون 07/18 الخاص بحماية المعطيات الشخصية. تجسيدا لما جاء في الدستور الجزائري من حق الأفراد في حماية حياة الأفراد الخاصة، وبذلك أقر بموجب هذا القانون حماية للأفراد وتجريم كل انتهاك يقع عليها، لكن لابد انّ نقول انّ المعطيات الخاصة للأفراد مظهر من مظاهر الحياة الخاصة للأفراد، وبذلك اختلاف وارد في هذا الجانب فمبدأ حماية البيانات الشخصية يعد منبثقا من الخصوصية وتعد خصوصية البيانات الشخصية أحدث أنواع الخصوصيات .(نساخ، 2022)

وتفطن بذلك رجال الفقه والقانون إلى خطورة العقول الالكترونية على الحياة الخاصة للأفراد، وذلك في قدرتها على الجمع وتخزين الكم الهائل للمعلومات والبيانات الخاصة للأفراد، وإعادة توظيفها، لأغراض أخرى، من طرف هذه الشركات سواء أغراض تجارية مادية بحثية أو علمية وبذلك يكون الاعتداء على خصوصية الأفراد .

انطلاقا من هذه الانشغالات عكفت التشريعات الوضعية على وضع آليات قانونية لحماية الحق فيالخصوصية للأفراد في أحد أنواع الخصوصية وهي البيانات الخاصة، ولحق المشرع الجزائري بالركب أخيرا وصدر القانون لحماية البيانات الشخصية للأفراد 07/18، يؤكد هذا الموقف من المشرع رغبته في حمية الشخص من المساس بخصوصية من قبل الغير وذلك في مواجهة تحديات العصر الرقمي.(نساخ، 2022)

بداية نعرج على المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي وفق المشرع الجزائري المعتمد على القانون 07/18 بدراسة الموافقة المسبقة ونوعية المعطيات، ومن هذه المبادئ الموافقة المسبقة من طرف الشخص المعني وذلك لمعالجة المعطيات ذات الطابع الشخصي وذلك وفق المادة السابعة من القانون 07/18 وللشخص الرجوع عن موافقته في أي وقت .

إلا أنّ المشرع لم يجعل الموافقة واجبة في حالة ما إذا كانت الضرورة وفق المادة السابعة من القانون ومنها حالة احترام الالتزام القانوني الذي يخضع له الشخص المعني أو المسؤول عن المعالجة أو لحماية حياة الشخص المعني أو تنفيذ لعقد يكون الشخص المعني طرفا فيه أو لتنفيذ إجراءات سابقة للعقد اتخذت على طلبه أو للحفاظ على المصالح الحيوية للشخص المعني، إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه وغيرها من الاستثناءات التي أوردها المشرع في طيات هذا القانون.(نساخ، 2022)

إلا أن المشرع بمقتضى هذا القانون وضع قيودا في معالجة هذه المعطيات الخاصة منها أنه لابد أن تكون معالجة المعطيات الشخصية بطريقة مشروعة ونزيهة، ولابد أن يكون تجميع هذه المعطيات لغايات محددة، وواضحة ومشروعة، وعدم معالجتها مرة أخرى، بطريقة تتنافى مع هذه الغايات المشروعة ولابد أن تكون المعطيات الشخصية كاملة و محينة إذا اقتضى الأمر مع ضرورة أن تكون المعطيات الشخصية محفوظة بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة الأزمة لإنجاز الأغراض التي من أجلها تم جمعها ومعالجتها .

أضف إلى جملة القيود الواردة على لمعالج عند معالجة المعطيات ذات الطابع الشخصي وضع المشرع هيئة مختصة، " السلطة الوطنية" التي تعتبر السلطة المختصة التي تودع لديها التصريح المسبق الذي موضوعه إجراء المعالجة، واشترط المشرع جملة من الشروط في هذا التصريح وفق المادة 14 من قانون 07/18، أضف إلى ذلك فإن للسلطة الوطنية أنّ تقرر إخضاع المعالجة لنظام الترخيص وذلك في حالة إذا كانت المعالجة تمثل أخطارا على الحياة الخاصة وذلك وفق المادة 17 من القانون 07/18.(نساخ، 2022)

- حقوق الشخص المعني بالمعطيات ذات الطابع الشخصي والتزامات المسؤول عن المعالجة

نتناول جملة الحقوق المقررة للمعني بالمعطيات ذات الطابع الشخصي ثم نحدد جملة الالتزامات التي تقع على المسؤول بالمعالجة للمعطيات ذات الطابع الشخصي .

أ. حقوق المعني بالمعطيات الشخصية :حدد المشرع حقوقا للشخص المعني بالمعطيات حيث منح المشرع الجزائري وفق قانون 18-07 للمعنيين بمعالجة المعطيات ذات الطابع الشخصي مجموعة من الحقوق وذلك لدفع الاعتداء على معطيات من طرف المسؤول عن المعالجة وذلك لحماية حياتهم الخاصة، وحدد المشرع هذه الحقوق للشخص المعني في الباب من القانون 18-07 المتمثلة في:

الحق في الإعلام- الحق في الإيلاج– الحق في التصحيح – الحق في الاعتراض- الحق في منع الاكتشاف المباشر .(نساخ، 2022)

ب. الالتزامات الواقعة على المسؤول عن كمعالجة المعطيات ذات الطابع الشخصي:

قرر المشرع إلى جانب حقوق المعني بالمعطيات الشخصية جملة من الالتزامات على عاتق المسؤول عن المعالجة حيث يقع على المسؤول عن المعالجة حماية المعطيات ذات لطابع الشخصي من إتلاف العرضي أو غير المشروع أو الضياع ا أو التلف أو النشر أو الولوج غير المرخصين وذلك بوضع التدابير التقنية والتنظيمية الملائمة ، وبقع لزاما على ذلك المسؤول عن المعالجة اختيار معالج من الباطن الذي يقدم الضمانات الكافية المتعلق بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها ويسهر على احترامها وتقوم المعالجة من الباطن بموجب عقد بين المعالج من الباطن والمسؤول عن المعالجة ، وبمقتضى هذا العقد ليس للمعالج من الباطن بين التصرف إلا بناءا على تعليمات من المسؤول عن المعالجة ، كذلك التزام المسؤول عن المعالجة والأشخاص الذي اطلعوا على المعطيات ذات الطابع الشخصي بالسر المهني حتى بعد انتهاء مهامهم .(نساخ، 2022).

8. خاتمة

في ختام هذه الورقة البحثية، نستخلص أن اختراق الخصوصية في العالم الرقمي هو موضوع هام وخطير في نفس الوقت لا سيما مع تطور البرمجيات والتطبيقات الحديثة والمتطورة والتي أبرزت واجهة المخاوف المتعلقة بالحقوق والحريات الشخصية للفرد، بحيث تتعرض بيانات ومعلومات الأشخاص للتجسس والقرصنة والاستغلال غير المشروع والتوظيف السيئ لها، مما يقتضي إيجاد آليات الحماية القانونية للخصوصية، من خلال تصدي الجهات القانونية بصرامة لجرائم التجسس، والدعوة إلى وقف استخدام وبيع أدوات الاختراق الحاسوبي إلى أن يتم وضع نظام ضمانات كافية لحماية سرية الخصوصية المعلوماتية وتطوير آليات نظم الحماية والنقل الآمن للبيانات، على أن تبقى ثقافة احترام الخصوصيات ومراعاة الشأن الخاص من أهم المبادئ التي يجب أن تسود في المجتمعات الرقمية.

9. قائمة المراجع:

- الجوسسة الرقمية والأمن القومي: برنامج بيغاسوس الاسرائيلي نموذجا .***(22-7-2021)*** . موقع الموسوعة الجزائرية للدراسات السياسية والاستراتيجية ***Consulté le*** .تاريخ زيارة الموقع 24-11-2022 الساعة 15:45
- العربي, م. ا ,***(2022)*** .جانفي 31 .***(***ملخص ملف التجسس" بيغاسوس: 450 ضحية حول العالم، والتجسس يطال الاسرائليين أيضا . موقع القدس العربي ***Consulté le*** .تاريخ الزيارة 24-11-2022 الساعة 16:06
- المتحدة, م. ا ***(*** .أيلول سبتمبر 2022 ***).***برامج التجسس والمراقبة: تقرير للأمم المتحدة يحذر من تفاقم المخاطر التي تهدّد الخصوصية وحقوق الإنسان .موقع الجزيرة الاخبارية***Consulté le 2022*** .
- بلعسل بنت نبي ياسمين- مقدر نبيل .***(2021)*** .الحق في الخصوصية الرقمية .مجلة المستقبل للدراسات القانونية والسياسية ,المجلد 05) العدد 01***3865-2543 .Récupéré sur pp. 10-22),***
- خدوجة, ا ,***(2017)*** .ديسمبر .***(***حق الخصوصية في مواجهة الاعتداءات الالكترونية (دراسة مقارنة) .مجلة الأستاذ الباحث للدراسات القانونية والسياسية ,المجلد الأول) العدد 08***158 -140 .pp),***

- خليف, خ) .دت .(الحق في الخصوصية الرقمية في مواجهة مقتضيات حماية الأمن الوطني .القانون الدولي العام.182 -174 .pp ,
- سالم, م .(2021-7-21) .برناج " بيغاسوس"التجسسي ذكي جدا وكشفه صعب .موقع الرسمي موقع2022 ,24 11 le Consulté .dw
- لخشين, ع .(2 3 ,2021) .حماية الحق في الخصوصية في العصر الرقمي في المواثيق الدولية .ممجلة جيل حقوق الانسان) العدد 39.p ,(109.
- منال وجيه - محمد سيد أحمد .(2014) .المعلومات والاتصالات (النظريات والتطبيق).مصر : كلية العلوم والدراسات الانسانية جامعة الشقراء.
- نساخ, ف ,2022) .نوفمبر .(حماية الحق في الخصوصية في ظل البيئة الرقمية .المجلة الأكاديمية للبحث القانوني ,المجلد 13) العدد 01) 427 - 414 .pp ,(ص 5.(
- يحي الشريف نصير -مزغيش عبير .(2022) .الآليات القانونية المكرسة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري . مجلة البحوث في العقود وقانون الأعمال ,المجلد 07 (العدد02.213-192 .pp)