التعدي على الخصوصية وتحديات الأمن المعلوماتي
Infringement of privacy and information security challenges

أ.د. دليلة خينش

جامعة محمد خيضر – بسكرة (الجزائر)

d.khineche@univ-biskra.dz

ط.د سعاد خينش

مخبر علم النفس العصبي المعرفي والاجتماعي - جامعة حمة لخضر- الوادي (الجزائر)

Khineche-souad@univ-eloued.dz

الملخص:

يهدف البحث إلى تحديد إطار مفاهيمي حول الخصوصية والاختراق والأمن المعلوماتي ووصف أشكال الاختراق والتعدي على خصوصية الفرد الناتجة عن سوء استخدام الوسائط الحديثة وإلحاق الضرر المادى والمعنوي للمستخدم وتهديد أمنه المعلوماتي، وتعتمد الدراسة على المنهج الوصفي في وصف وتحليل أثر التهديدات الالكترونية على خصوصية الفرد في ظل البيئة الرقمية وتزويد المستخدم بحلول لمواجهة خطرها وتحقيق الأمن المعلوماتي، وبينت نتائج الدراسة أنه على الرغم من تطور آليات حماية المعلومات يبقى الاختراق والتعدي على خصوصية الفرد جريمة الكترونية تتطلب تكثيف عنصر التحسيس واليقظة وتعزيز سبل الحماية القانونية والتقنية لبيانات وخصوصية المستخدم.

كلمات مفتاحية: الخصوصية، الاختراق، الأمن المعلوماتي،

Abstract :

The research aims to define a conceptual framework around privacy , penetration and information security, describe the forms of penetration and infringement on the privacy of the individual resulting from the misuse of modern media to damage material and moral of user and threat his information security.the study adopted on the descriptive approach for describing and analyzing the impact of electronic threats on the privacy of the individual in light of the digital environment and it providing some solutions for confront their danger and achieve information security. The results ofthis study showed that despite the development of information protection mechanisms, hacking and infringement of an individual's privacy remains an electronic crime that requires intensifying of awareness and strengthening the means of legal and technical protection of the user's data and privacy.

Keywords: Privacy, Penetration, Information Security



رقمنة

مجلة الدراسات الإعلامية والاتصالية

المجلد03| العدد 01
مارس 2023
الصفحات 44 - 56

ردمد |ISSN-2773-4285
EISSN| 2830-8417
الإيداع القانوني |03/2023
العنوان |11، طريق دودو مختار، بن عكنون، الجزائر العاصمة.
الفاكس |50 88 23 (023)
الهاتف | 75 29 62 (0561)

تاريخ الاستلام 2022/11/20
تاريخ القبول 2022/12/25
تاريخ النشر 2023/03/18

أ.د. دليلة خينش |
جامعة محمد خيضر – بسكرة (الجزائر)
d.khineche@univ-biskra.dz

1. مقدمة:

قدمت الانترنت والتكنولوجيات الحديثة خدمة للإنسانية عن طريق منحها تأشيرة للانفتاح على العالم، كما أتاحت لها أشكال جديدة من الاتصال والتعامل مع البيانات والمعلومات، وسهلت من مستوى الخدمات الالكترونية وسرعتها، في المقابل أفرزت هذه البيئة الرقمية العديد من المشاكل الغير قانونية والغير أخلاقية كثيرا ما أثرت على النفس والعقل وسلوك الفرد والجماعة.

صاحب تطور الأجهزة الرقمية وسيادة الانترنت عبر العالم تغير في منظومة القيم والمفاهيم والسلوك، وباتت البيئة الالكترونية تشكل تهديدا على الفرد والمجتمع عن طريق ما تتيحه لمستخدمي الانترنت من ميزة الشعور بالحرية وإمكانية التخفي والتعدي على الآخرين، الأمر الذي أتاح لبعض المجرمين إطلاق أحكام سيئة ونظرة دونية نحو الآخرين، وإرسال مضامين مشبعة بقيم واتجاهات عنصرية تسيء للأفراد من حيث لون البشرة وشكل الشخص وعرقه وانتمائه الثقافي ومحيطه الاجتماعي ومجاله المكاني ومستواه الاجتماعي والتعليمي، بل تمكنهم عن طريق التحايل الالكتروني إلى النفاذ والاستيلاء على البيانات الخاصة للأفراد وتهديد خصوصيتهم.

ارتبط مفهوم الخصوصية بمفهوم حماية المعلومات حديثا و وضعت الخصوصية في إطار الحق في حماية البيانات الخاصة، وحدد المختصون أن الخصوصية هي الحد الفاصل بين حق الفرد المطلق وبين حق المجتمع. وفي عام 1980 ذهب القاضي الأمريكي (Brandeis Louis) قاضي المحكمة العليا إلى أن الخصوصية هي حق الفرد في أن يترك ليكون وحيدًا، لذا حددت الخصوصية كواحد من سمات المجتمع الديمقراطي. في عام 1967 عرف (Alan Westin) الخصوصية بأنها رغبة الأفراد في الاختيار الحر للآليات التي يعبرون بها عن أنفسهم ورغباتها. وتضمن مفهوم **خصوصية المعلومات (Information Privacy)** خصوصية المعلومات القواعد التي تحكم جمع وإدارة البيانات الخاصة (معلومات طبية، معلومات مالية، بطاقات هوية)، لكن رغم الاستخدام الواسع للتكنولوجيات الحديثة لتسهيل عملية الاتصال والتعاملات الالكترونية لا تزال أسرار الأفراد وخصوصياتهم في خطر، وتعتبر عملية حماية الخصوصية في البيئة الرقمية والتحكم في الإجراءات التقنية لتحقيق الأمن المعلوماتي من أهم القضايا التي تشغل بال الهيئات العلمية والرسمية والدولية.

مع التطور المتزايد لتكنولوجيا الإعلام والاتصال وزيادة الحاجة الماسة لاستخدام وسائلها تعددت التهديدات الالكترونية التي مست خصوصية الأفراد والجماعات وحتى هوية الدول، وأصبحت جريمة الاختراق والاعتداء على الخصوصية من أخطر الجرائم التي يمكن أن تقع عن طريق الانترنت نظرًا لعدم وجود الحماية التقنية الفاعلة لما يتم تداوله من معلومات وأسرار ومراسلات عن طريق الانترنت، وتشمل جريمة الاعتداء على الخصوصية الاعتداء بالتنصت أو التسجيل، أو نقل بواسطة جهاز معين، أو التقاط صورة دون علم ورضى بقصد إلحاق الضرر المادي والمعنوي بالجهة المستهدفة، من هنا برزت الحاجة الماسة لإيجاد حلول تهدف إلى حماية الخصوصية وتحقيق الأمن المعلوماتي، وجاءت هذه الورقة العلمية تحاول الإجابة على التساؤل الرئيسي التالي:

- **ما هي التهديدات الالكترونية التي تمس بالخصوصية وما تحديات الأمن المعلوماتي؟**

وللإجابة على هذا التساؤل جاءت التساؤلات الفرعية التالية:

1- **ما مفهوم الخصوصية؟**
2- **ما هي أشكال التعدي على الخصوصية وما هي وسائلها؟**
3- **ما سبل مكافحة التعدي على الخصوصية وحماية الأمن المعلوماتي؟**

2. أهداف الدراسة:

تهدف الدراسة إلى تحديد إطار مفاهيمي حول مفهوم الخصوصية والاختراق والأمن المعلوماتي في محاولة لتحليل أثر التهديدات الالكترونية على خصوصية الفرد في ظل الانتشار الواسع للتكنولوجيا الحديثة واستخدامها في الاتصال والتعاملات الإدارية والتجارية. وهذا قصد إبراز مخاطر الاختراق على بيانات المستخدم واقتراح حلول تجنب المستخدم من عملية الاختراق وتحقق الأمن المعلوماتي.

3. أهمية الدراسة:

تكمن أهمية هذه الدراسة في محاولة لتحديد مفاهيم حديثة أفرزتها البيئة الرقمية وبينت أثرها السلبي على أمن الفرد والمجتمع ألا وهي الخصوصية والاختراق والأمن المعلوماتي، في محاولة لتقديم إضافة علمية تسهم في إثراء الحقل المعرفي المتخصص في مجال العلوم الاجتماعية والإنسانية وحتى السياسية. وتقديم رؤية سوسيولوجية تعتمد على وصف وتحليل مخاطر الاختراق والتعدي على الخصوصية وأثرها على خصوصية الأفراد وأمنهم المعلوماتي تسهم في توعية الفرد وتمده بسبل وقائية لتحقيق الأمن المعلوماتي.

4. مفهوم الخصوصية:

ارتبط مفهوم الخصوصية بمفهوم حماية المعلومات حديثا ووضع الخصوصية في إطار الحق في حماية البيانات الخاصة، وحدد المختصون أن الخصوصية هي الحد الفاصل بين حق الفرد المطلق وبين حق المجتمع. وفي عام 1980 ذهب القاضي الأمريكي (Brandeis Louis) قاضي المحكمة العليا إلى أن الخصوصية هي حق الفرد في أن يترك ليكون وحيدًا، لذا حددت الخصوصية كواحد من سمات المجتمع الديمقراطي. في عام 1967 عرف (Alan Westin) الخصوصية بأنها رغبة الأفراد في الاختيار الحر للآليات التي يعبرون بها عن أنفسهم ورغباتها.

ويمكننا هنا التعرف على عدة أنواع للخصوصية وهي:

- **خصوصية المعلومات (Information Privacy)**: وتتضمن خصوصية المعلومات القواعد التي تحكم جمع وإدارة البيانات الخاصة (معلومات طبية، معلومات مالية، بطاقات هوية).
- **الخصوصية الجسدية أو المادية (Body Privacy)**: وتتعلق بالحماية ضد أي اعتداءات تمس النواحي الجسدية مثل فحوصات الجينات وفحص المخدرات والمؤثرات العقلية.
- **خصوصية الاتصالات (Communication Privacy)**: وتعني بسرية وخصوصية الاتصالات والمراسلات الهاتفية والبريد الإلكتروني وغيرها من الاتصالات **(سيفون، 2016، صفحة 154)**.

صاحب الانتشار الواسع للمعلومات في الوطن العربي انتشار شتى أنواع الجرائم الإلكترونية فحاولت هذه الدول إيجاد سبل تشريعية وإجرائية ناجعة لمواجهة الجرائم المعلوماتية من تلك الجهود القرار الصادر عن مجلس وزراء العدل العرب الخاص بإصدار القانون الجزائي الموحد كقانون عربي نموذجي حيث تضمن الباب السابع الخاص بالجرائم ضد الأشخاص فصل خاص بالاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية، وذلك في المواد 461-464 التي أشارت على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات الاسمية وكيفية الاطلاع عليها والعقاب المطبق في حال ارتكاب هذه الجرائم **(المويشر، 2009، صفحة 175)**.

تشير أحدث تقارير الخصوصية إلى أنه لا تزال أسرار الأفراد وخصوصياتهم في خطر، وتعتبر عملية حماية الخصوصية في البيئة الرقمية من أهم الوسائل والإجراءات التقنية بوصفها عملية تكاملية محكومة بإستراتيجية محددة العناصر، ومن الخطأ مجرد الاعتقاد بأن استخدام بعض التقنيات يحمي البيانات الشخصية حماية كاملة. وبالإضافة إلى ذلك يجب عدم

إغفال أهمية الحماية القانونية والتشريعية وتكاملها مع الحماية التقنية والتنظيمية، إذ قد ثبت أن الولايات المتحدة الأمريكية تمارس الرقابة على الانترنت وتقوم باختراق الاتصالات العالمية عبرها **(سيفون، 2016، صفحة 155)** من خلال وكالة الأمن القومي (NSA).

وقد كشف هذه الفضيحة المعروفة بشبكة (Echelon) الصحفي الاسكتلندي (Ducan Cambell)، كما تبين كذلك أن أكبر المؤسسات الأمريكية لأجهزة الإعلام الآلي تقوم بزرع بعض البرمجيات في ذاكرة الحواسيب التي تسمح بمتابعة استعمالات صاحب الحاسوب على شبكة الانترنت، ومعرفة المواقع والخدمات التي يزورها. وهو ما يمكنها من التعرف على شخصيته وعلى معلوماته الشخصية، التي تستخدم في دراسات السوق والأنشطة التجارية (التسويق، الإشهار)، ومن أمثلة هذه الشركات شركة (Doubleclick). وهذا ما أدى بالعديد من الجمعيات وأعضاء المجتمع المدني إلى التعبير عن رفضهم وتخوفهم من استغلال البيانات الشخصية للأفراد لأغراض أخرى (تجارية، سياسية...).

5. وسائط الاختراق الالكتروني لخصوصية الفرد:

أ- البريد الإلكتروني (Electronic Mail):

وهو أكثر استخدامات الانترنت شيوعًا، يتكون المصطلح من جزأين رئيسيين هما رأس (Header) ونص (Body)، ويحتوي الرأس على معلومات حول المرسل والمتلقي والمعلومات اللازمة لتوصيل الرسالة إلى العنوان المناسب، ويحتوي النص على الرسالة التي تم تكوينها **(الشوابكة، 2007، الصفحات 32-33)**.

ويستطيع الجاني من خلال البريد الإلكتروني أن يرسل مادة معينة إلى شخص ما بغرض النيل من شرفه أو كرامته أو تعرضه إلى بغض الناس واحتقارهم. فإذا ما استخدم البريد الإلكتروني للقيام بالأفعال السابقة عُدّ مرتكبا لجريمة الذم والقدح **(الشوابكة، 2007، صفحة 33)**. ويعد الهجوم عبر البريد الالكتروني والمواقع الإلكترونية من أفضل الطرق للهجمات على الأجهزة الإلكترونية بصورة عامة حيث أن عمليات الاحتيال وعمليات السرقة الإلكترونية تكون في الغالب عبر البريد والمواقع الإلكترونية، وسرقة كلمة المرور (Password Sniffing) باستخدام برامج لاقطة (Sniffer) أثناء الاتصال بالانترنت، حيث يتمكن المجرم من التقاط كلمة المرور أو محاولة تخمينها وهنا يتم اختراق المعلومات الخاصة بالمستخدمين أو المؤسسات وفي هذا الشأن لم تسلم حتى المؤسسات التعليمية والجامعية من الهجوم أو الاحتيال الإلكتروني، حيث أوضح المسؤولون الأمريكيون أن قراصنة الكمبيوتر (Hackers) تمكنوا من التسلل إلى سجلات بعض أشهر الكليات والجامعات الأمريكية والعبث بها، مثل تعرض كلية إدارة الأعمال جامعة هارفرد بالولايات المتحدة الأمريكية إلى اختراق **(طالب، 2007، صفحة 45)**.

والاستيلاء على كلمة المرور يمكن المجرم من انتحال شخصية (IP Spoofing) العديد من الشخصيات البارزة والمرموقة، والذين يملكون آلاف من الأتباع على الشبكات الاجتماعية وحدث ذلك غالبا على "تويتر" مما ألحق الحرج بالشخصيات. ولكي تتناقل الأجهزة المعلومات عبر الشبكة فإنها تربط (IP) بـ (MAS) أي لكل جهاز (IP) عنوان فريد لا يتكرر ويمكن للأجهزة الأخرى مراسلته به، إضافة إلى وجود عنوان آخر يسمى بـ (MAC).

ب- شبكة الويب العالمية (World Wide Web):

يمكن تعريف شبكة الويب العالمية (www أو Web) بأنها عبارة عن كم هائل من المستندات المحفوظة في شبكة الحاسوب، والتي تتيح لأي شخص أو لأي جهة الاطلاع على معلومات تخص جهات أخرى أو أشخاص آخرين قاموا بوضعها على هذه الخدمة، حيث تقدم خدمة معلومات واسعة النطاق من خلال خاصية الخطوط المحورية المتعددة والتي تسمح للمستخدمين بالارتباط عبر أنظمتها بالنصوص والملفات، للحصول على المعلومات التي يعلق عليها النص المحوري (Hyper Texte) **(الشوابكة، 2007، الصفحات 37-38)**.

ويمكن لأي مستخدم لشبكة الانترنت أن ينشئ له موقع (Site) على شبكة الويب العالمية، يتضمن معلومات يمكن إعادة تخزينها. فقد يرتكب الذم والقدح والتحقير عبر شبكة الويب العالمية من خلال إسناد مادة كتابية، أوصوتية، فيديو (سمعية

بصرية) تسيء إلى أحد الأشخاص، ومن شأنها أن تنال من شرفه أو كرامته أو تعرضه إلى بغض الناس واحتقارهم، وكذلك فإن الجرائد الإلكترونية أخذت حيزها على شبكة الويب العالمية لارتكاب أفعال الذم والقدح والتحقير من خلالها.

ج- الأخبار (News Groups):

مجموعات الأخبار عبارة عن مناطق مناقشات عامة عبر الانترنت، يمكن من خلالها التحدث حول أي موضوع، مع إمكانية تبادل الصور والمعلومات المقروءة أو المكتوبة، ويتم ذلك من خلال (News Groups) أو نظام يوزنت (Usenet) وكلاهما عبارة عن مجموعات أخبار. حيث أن عبارات الذم والقدح والتحقير تنشر وتذاع بين الناس عبر حلقات النقاش هذه، أو قد توزع على فئة منهم على شكل كتابات أو صور استهزائية أو مسودات الرسوم أو قد ترسل إلى بريدهم الإلكتروني.

د- غرف المحادثات والدردشة (Chat Rooms):

غرف المحادثة أو الثرثرة عبارة عن مساحات معروفة في الفضاء الإلكتروني (Cyber Space) تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض، بإرسال البريد الإلكتروني الذي يمكن قراءته من قبل الشخص المشترك في غرفة المحادثة. وفي الواقع عندما نتخاطب عبر الانترنت فإن ما يحدث هو أنك تكتب رسالة باستخدام لوحة المفاتيح، حيث يمكن للآخرين رؤية ما تكتب **(الشوابكة، 2007، الصفحات 38-45)**.

6. الجرائم الالكترونية التي تهدد الخصوصية:

بتطور وشيوع استخدام الانترنت ووسائل التكنولوجيا تعددت أشكال الجرائم الإلكترونية التي يتعرض لها الأفراد والمنظمات والدول ونوضح أهمها كالتالي:

أ- سرقة المال المعلوماتي المعنوي (Identity Theft):

أو سرقة الهوية وهي جريمة تأخذ صورة اختلاس البيانات والمعلومات والإفادة منها باستخدام السارق للمعلومات الشخصية- مثل الاسم، العنوان، الأرقام السرية- الخاصة بالمجني عليهم، والاستخدام غير الشرعي لشخصية المجني عليه ليبدأ بها عمليات السرقة المتخفية عبر الانترنت بحيث تؤدي بالغير إلى تقديم الأموال- الإلكترونية أو المادية- إلى الجاني- عن طريق التحويل البنكي **(الشوابكة، 2007، صفحة 138)**. هذا النوع من الجرائم يعتبر من أبرز أشكال الجرائم الإلكترونية وأكثرها خطورة، وتشير سرقة الهوية إلى تلك العمليات التي تتم من خلالها سرقة معلومات شخصية عن الهوية تستخدم للاحتيال والقيام بأعمال غير قانونية واستغلال هذه المعلومات لتحقيق مكاسب مالية. فعند إصابة جهاز الحاسب الآلي بأحد البرامج الخبيثة، قد يقوم هذا البرنامج بالبحث في الجهاز عن بيانات شخصية، مثل الاسم أو العنوان أو مكان الميلاد أو رقم الهاتف أو رقم بطاقة الهوية أو أرقام بطاقات الائتمان إلى آخره من معلومات، ثم يتم استخدامها في تزوير بطاقات الهوية وشهادات ميلاد وكشوف حسابات البنوك وسرقة الأموال.

ب- الاحتيال عبر الانترنت (Internet Fraud):

الاحتيال الإلكتروني هو نوع من الاحتيال يتم فيه استخدام الانترنت ووسائطه المختلفة كالمواقع الإلكترونية والبريد الإلكتروني للقيام بعمليات احتيالية لتحقيق مكاسب مالية. يتمثل الاحتيال بإغراء المتلقي بالاستجابة لطلبات المتصل في الحصول على معلومات شخصية، أو العنوان البريدي الإلكتروني ليتمكن من الدخول واستخدام البريد الإلكتروني في أعمال تخصه باسم صاحب البريد الإلكتروني. وبسبب تزايد أعداد المستخدمين للانترنت على مستوى العالم، ازدادت مخاطر تعرض الأفراد والشركات والمنظمات والحكومات لعمليات الاحتيال عبر الانترنت.

يعرّف الاحتيال بأنه كل تظاهر أو إيحاء يكون صالحًا لإيقاع المجني عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي، أي أن المجني عليه في جريمة الاحتيال هو من جازت عليه حيلة الجاني فانخدع بها وسلمه ماله **(الشوابكة، 2007، صفحة 185)**.

وقد أصبح للاحتيال الإلكتروني أبعاد خطيرة على المستوى العالمي وبات يؤثر في عالم المال والأعمال والبنوك بشكل جدي؛ حيث وصل الأمر إلى طرح دروس مجانية للمبتدئين في عالم الجرائم الاحتيالية الإلكترونية في مواقع معينة عبر الانترنت، وأصبحت البنوك تواجه مشاكل حقيقية في هذا الميدان، وقد نبه الخبراء ومنذ سنة 1997 إلى استفحال ظاهرة الاحتيال الإلكتروني وبخاصة منذ ذلك النوع (من الاحتيال الإلكتروني) الذي يضرب البنوك التجارية **(طالب، 2007، صفحة 41)**.

وجاء في تقريرين أصدرهما اتحاد البنوك الهولندية، والبنوك البلجيكية تضمن التقريران ما يقارب من (200) أسلوب وطريقة للنصب والاحتيال الإلكتروني على البنوك، وهذه الأساليب والطرق المعتمدة في النصب والاحتيال الإلكتروني تعتمد من قبل كل من العصابات الإجرامية المحترفة والأفراد، وكذلك عصابات المخدرات والعصابات المختصة في تبييض الأموال، وحذر التقريران من كارثة اقتصادية كبرى إذا لم يوضع حد لمثل هذه الأساليب الاحتيالية الخطيرة.

ومن الأمثلة على وسائل الاحتيال الإلكتروني وسيلة "الشيك وشنك" (Cheque- Washing) وهو عبارة عن شيك مصنوع من أشعة رملية دقيقة أعد في الأساس لتصعيب تزويره أو العبث به، حيث تمت سرقة هذا النوع من الشيكات وتم تزويره (تزوير بياناته) وتم فعلاً سحب مبالغ كبيرة بواسطة هذا الشيك الذي كان يعد إلى أمد قصير من أفضل أنواع الشيكات الآمنة على الإطلاق. ولم تنجح الوسائل التكنولوجية المعتمدة من قبل البنوك في اكتشاف التزوير والتعديل في بياناته، واتضح (بعد عدة عمليات تزوير) أن الطريقة الصحيحة للتأكد من صحة مثل هذا النوع من الشيكات هي ليست الوسائل الإلكترونية المعتمدة في هذا الميدان، بقدر ما هي العدسات المكبرة (العادية) التي بواسطتها يتم فعلا اكتشاف التزوير أو التعديل الإجرامي في بياناته **(طالب، 2007، صفحة 42)**.

تعددت أشكال جرائم الاحتيال عبر الانترنت ومن أهمها القيام ببيع سلع وهمية (Rogue Traders) أو سرقة معلومات البطاقات الائتمانية واستخدامها (Credit Card Fraud)، أو توجيه المستخدم إلى موقع خاطئ الغرض منه التحايل أو الاصطياد الاحتيالي والذي يتعرض فيه الأفراد للخداع عن طريق توجيههم إلى مواقع يتم فيها الحصول على أكبر قدر من المعلومات الخاصة بهم، ثم استخدامها من قبل القائم بالجريمة لتحقيق مكاسب مالية.

ج- الاختراق (Hacking):

يحدث الاختراق ثغرات في نظام الحماية الخاصة بالهدف، فيتمكن المخترق من الوصول إلى المعلومات بشكل غير قانوني، فيقوم بالاستيلاء على المعلومات ونشرها بعد تحريفها، أو حذفها مكان الموقع بما يحقق أهداف تخريبية يسعى إليها المتصل.

هجومات الاختراق (Penetration Attacks) هي تلك الهجمات التي يتم من خلالها الدخول غير المشروع إلى الأنظمة الآلية وتخطي نظام التأمين الخاص بها، وفي حالات الاختراق الكامل يتمكن المهاجم من السيطرة الكاملة على الحاسب الآلي وتغيير البيانات أو تبديلها، أو زرع برامج خبيثة داخل الجهاز. وفي بعض الحالات يقوم المخترق (Intruder) باستخدام الحاسب الآلي الذي تم اختراقه كأداة لشن هجوم إلكتروني على جهاز آخر خاصة وإن كانا متصلين بشبكة واحدة **(شفيق، 2016، الصفحات 33-34)**.

أبسط هذا النوع من الجرائم هو الدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة والخروج دون إحداث أي تأثير سلبي عليها، ويقوم بذلك النوع من الأنشطة ما يطلق عليهم "المخترقون ذوي القبعات البيضاء" (White Hat Hackers) الذين يقومون بالدخول بطريقة غير مشروعة على أنظمة الحاسب أو شبكات المعلومات أو مواقع الانترنت مستغلين بعض الثغرات في تلك النظم مخترقين بذلك كل سياسات وإجراءات امن المعلومات التي يقوم بها مديري تلك الأنظمة والشبكات (System and Network Administrators) ونتيجة عدم ارتباط ذلك النشاط بالشبكات؛ بمعنى اختراق أمن أجهزة الحاسب التي تحتوي على بيانات هامة بالرغم من وجود إجراءات أمنية لمنع الوصول إليها، أي وصول شخص غير مصرح به ودخوله إلى حجرة الحواسب المركزية بالمؤسسة، ثم خروجه دون إحداث أي أضرار. كل هذا يعتبر خرق لسياسة وإجراءات امن المعلومات بتلك المؤسسة.

الاختراق يتم باستخدام الشبكات وبصفة خاصة شبكة الانترنت في الدخول على قواعد البيانات أو مواقع الانترنت والحصول على معلومات غير المسموح بها أو إمكانية السيطرة التامة على تلك الأنظمة بالرغم من وجود إجراءات حماية متعددة الدرجات من أنظمة الكشف، وآليات تشفير البيانات، وكلمات السر المعقدة. فتخطي كل هذه الحواجز والدخول على أنظمة المعلومات والخروج دون إحداث أي تغيير أو إتلاف فان حالة الاختراق هذه تهدد مديري النظم وأمن المعلومات بأن سياساتهم وإجراءاتهم التنفيذية لأمن المعلومات بحاجة إلى التعديل والتغيير وأنه يتعين عليهم البدء مرة أخرى في عمل اختبار وتحليل للتهديدات ونقاط الضعف الموجودة بأنظمتهم (Risk Assessment) لإعادة بناء النظام الأمني مرة أخرى وأيضا العمل على إجراء ذلك الاختبار بصورة دورية لمواكبة الأساليب الجديدة في الاختراق.

د- جرائم الإضرار بالبيانات:

تعتبر جريمة الإضرار بالبيانات من أخطر الجرائم الإلكترونية نظرا للخسائر التي تلحق بالأفراد أو المؤسسات، وتشمل الجريمة كل عملية الكترونية تهدف إلى تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة إلكترونية (Digital Form) على الحواسيب الآلية المتصلة بشبكات المعلومات أو مجرد محاولة الدخول بطريقة غير مشروعة إليها **(محمد، 2016، صفحة 12)**.

تقع جريمة الإضرار أو الإتلاف في نطاق المعلوماتية عندما يتم الاعتداء على الوظائف الطبيعية للحاسب الآلي، وذلك بالتعدي على البرامج (Logical) والبيانات (Data) المخزنة والمتبادلة بين الحواسيب وشبكاته- الداخلية (المحلية) أو العالمية (الانترنت)- ويكون ذلك عن طريق التلاعب بالبيانات سواء بإدخال معلومات مصطنعة أو بإتلاف المعلومات المخزنة بالحواسيب والمتبادلة عبر الشبكة العالمية (Global Net) بمحوها أو تعديلها أو تغيير نتائجها أو التشويش على النظام المعلوماتي، الأمر الذي يؤدي إلى إعاقة سير عمل النظام الآلي.

ويكون الإتلاف العمدي للبرامج والبيانات بمحوها كلية أو تدميرها إلكترونيا أو تشويهها؛ مما يجعلها غير صالحة للاستعمال **(الشوابكة، 2007، صفحة 216)**. وذكر الماجد إبراهيم سنة 2005م في مقال له في مجلة (Digital- World) مايلي: "لم تسلم جهة من التخريب الإلكتروني والتعطيل والمشكلات، فحتى البنتاغون معقل (أقوى جيوش العالم) وأكثرها تطورًا تم اختراقه مرارًا، فكيف الأمر بالنسبة إلى الشركات والمؤسسات العامة في مختلف بلدان العالم" **(طالب، 2007، صفحة 44)**.

أما بالنسبة إلى تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل لنظم المعلومات فإن تلك الأنشطة تتم بواسطة أفراد هواة أو محترفون يطلق عليهم المخترقون ذوي القبعات السوداء (Black Hat Hackers) الذين قد يقومون بهذه الأعمال بغرض الاستفادة المادية أو المعنوية من البيانات والمعلومات التي يقومون بالاستيلاء عليها أو بغرض الإضرار بالجهة صاحبة تلك الأنظمة لوجود كره شخصي أو قبلي أو سياسي أو ديني أو القيام بذلك لحسابات أحد المؤسسات المنافسة.

هـ- الاعتداء على الملكية الفكرية لأسماء مواقع الانترنت:

من صور الاعتداء الأخرى التي تمثل اعتداء على الملكية الفكرية للأسماء ما يحدث من اعتداءات على أسماء مواقع الانترنت (Domain Names) حيث أن القاعدة العالمية في تسجيل أسماء النطاقات (والتي تتم أيضا باستخدام بطاقات الائتمان من خلال شبكة الانترنت).

من الجرائم الأخرى المتعلقة بأسماء النطاقات على شبكة الانترنت ما يعرف بإعادة التوجيه (Redirection) مثلما حدث لموقع شركة (Nike) في شهر يونيو عام 2000، حيث قامت جماعة من المحترفين بالدخول على موقع شركة تسجيل النطاقات الشهيرة والمعروفة باسم (Network Solutions) وتغيير بيانات النطاق لضعف إجراءات أمن المعلومات بالشركة في ذلك الحين، وبذلك تم إعادة توجيه مستخدمي الانترنت إلى موقع لشركة انترنت في اسكوتلاندا **(محمد، 2016، الصفحات 13-17)**.

و- الالتقاط غير المشروع للبيانات:

ويشمل الدخول غير المصرح به محاولة أي شخص الاستيلاء على أنظمة ومعلومات الغير ولو على سبيل إشباع الفضول والمتعة والإثارة أو تحديث أنظمة حماية الحاسبات الآلية **(الشاعر، 2015، صفحة 53)**.

إن الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن، يتيح للمجرم المعلوماتي ممارسة نشاطاته الإجرامية من أجل تحقيق مكاسب شخصية متباينة ومتعلقة بذات المجرم. بحيث تمكنه من التقاط البيانات المخزنة في قواعد البيانات أو المتبادلة عبر قنوات الانترنت واستخدامها بطرق غير مشروعة.

ويتمكن المجرم المعلوماتي من التقاط البيانات- بعد الدخول غير المشروع إلى النظام أو البقاء فيه- إما عن طريق التجسس المعلوماتي (Informatique espionnage) أو عن طريق الاحتيال (الخداع Spoofing) أو عن طريق تفجير الموقع المستهدف **(الشوابكة، 2007، صفحة 166)**.

ز- التحويل الإلكتروني غير المشروع للأموال:

اكتسب التعامل بالأموال في عصر المعلوماتية صفة البيانات الإلكترونية المخزنة في ذاكرة الحاسب الآلي، وأدت الثورة الرقمية إلى إمكانية إجراء تحويلات ومبادلات لهذه الأموال من أي مكان في العالم. وتكمن خطورة الأمر في إمكانية تلاعب الجاني بهذه البيانات المخزنة في ذاكرة الحاسب الآلي أو في برامجه وإجراء تحويلات في كل أو بعض أرصدة الغير أو فوائدها وتحويلها إلى حسابه أو حسابات أخرى.

وغالبا ما يتم ولوج مخترقي شبكات الانترنت إلى بيانات حساب الآخرين من خلال الحصول على كلمة مرور (Password) مدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجني عليه، فإذا تم الاستيلاء على كلمة المرور وإدخالها في أنظمة الحاسب الآلي فإنها- إذا ما كانت مدرجة وملائمة- سوف تنسجم وتقترن بالملف ومن ثم تسمح للمستخدم بالولوج إلى النظام المعلوماتي **(الشوابكة، 2007، صفحة 178)**.

ح- الاحتيال باستخدام بطاقات الدفع الإلكتروني عبر الانترنت:

يعتمد نظام بطاقة الدفع الإلكترونية على عمليات التحويل الإلكترونية من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر بالبنك الذي يوجد به حسابه، وذلك من خلال شبكة التسوية الإلكترونية للهيئات الدولية. وتعطي بطاقة الدفع الإلكتروني الحق للعميل في الحصول على السلع والخدمات عبر شبكة الانترنت عن طريق تصريح كتابي أو تليفوني بخصم القيمة على حساب بطاقة الدفع الإلكتروني الخاصة به **(الشوابكة، 2007، صفحة 193)**.

وقد أتاحت الثورة الرقمية لقراصنة المعلوماتية إمكانية تخليق أرقام البطاقات الائتمانية بواسطة برامج تشغيل، تتيح إمكانية تخليق أرقام بطاقات بنك معين من خلال تزويد الحاسب بالرقم الخاص بالبنك مصدر البطاقة، علاوة على إمكانية التقاط هذه الأرقام عبر قنوات الانترنت المفتوحة واستخدامها بطريقة غير مشروعة في عمليات التسوق عبر الشبكة، بحيث يتم خصم قيمة السلع من العملاء الشرعيين لهذه البطاقات.

7. أشكال التعدي على خصوصية الفرد:

تتعرض عملية تبادل المعلومات على الشبكة العالمية لمحاولات هجوم بأشكال مختلفة، ويكون بعضها بشكل مباشر أو بشكل غير مباشر من خلال وسيط واحد أو أكثر. وتعارف الخبراء على تسمية هذا الهجوم بالاختراق. ومواقع التواصل الاجتماعي ليست بمنأى عن هذه الاختراقات فحسابات المستخدمين لمواقع التواصل الاجتماعي عرضة للدخول إليها وانتحال شخصية منشئها وابتزازه وكثيرا من الحوادث حصلت نتيجة الدخول غير المشروع لمواقع الغير.

فالاختراق هو المرور أو التسلل إلى نظام الحاسب لإلحاق الضرر بالمعلومات المخزنة فيه أو سرقتها والاستيلاء عليها أو نشر الفيروسات فيها. ويمكن تقسيم الأشخاص الذين يقومون بعملية "الاختراق" إلى أربع فئات وهي: **(الشاعر، 2015، الصفحات 53-54)**

أ. **الفئة الأولى: الفضوليون / المخترقون (Hackers):** وهم الذين يقومون بالاستمتاع بتنفيذ المهمات الصعبة بل المستحيلة واقتحام اعقد الأنظمة على سبيل الهواية، بهدف إثبات الذات أو بنوايا إجرامية كتدمير البيانات أو الابتزاز.

ب. **الفئة الثانية: المتلصصون (Crackers):** وهم الفئة التي تحاول الدخول إلى أنظمة الحاسوب الآلي بسوء نية وبشكل غير قانوني بغرض التخريب، وذلك بتغيير المعلومات أو بحذفها أو إضافة معلومات تخدم هدفًا معيناً.

ج. **الفئة الثالثة: العابثون (Vandals):** وهم الفئة التي تخترق النظام بدافع العبث، وينقسمون إلى مجموعتين هما: مجموعة تشكل بعض المستخدمين الذين لهم حق الدخول في النظام، والمجموعة الثانية من الغرباء الذين لهم حق استخدلم النظام أو الدخول فيه، وفي كلتا الحالتين يدخل العابثون بهدف العبث واللهو ويعتقدون أن ما يقومون به من أعمال غير معاقب عليها وهي مباحة.

ومن أهم صور الاعتداء الالكتروني على خصوصية بالأفراد نذكر ما يلي:

- **الاعتداء على الحياة الخاصة للفرد:** حظيت الحياة الخاصة للأفراد بحماية دستورية وقانونية في مختلف تشريعات الدول المتقدمة، لما لخصوصية الأفراد من أهمية قصوى على كيان الفرد والمجتمع معًا. والحق في الخصوصية هو أحد الحقوق اللصيقة التي تثبت للإنسان، والتي غالبا ما يصعب حصر الجوانب المختلفة لها، والتمييز بحدود واضحة بين ما يعد من الحياة الخاصة للإنسان وما يعد من الحياة العامة له. ولما كانت الحياة الخاصة للأفراد بصورتها المستحدثة والمتمثلة في بنوك المعلومات المرتبطة بالتكنولوجيا مهددة بالعديد من الانتهاكات والاعتداءات، ولاسيما بظهور شبكة الانترنت والأجهزة التكنولوجية الحديثة، فإن النصوص التقليدية تقف عاجزة أمام هذه الاعتداءات على خصوصية الأفراد وأسرارهم **(الشوابكة، 2007، الصفحات 58-59)**.

إن المعلومات المجهولة- التي لا تدل على من تتعلق به- لا تثير أية صعوبة، حيث أن المجهول لا خصوصية له، ولكن الأمر يدق في حالة المساس بالمعلومات المتعلقة بأفراد معروفين، مما يؤدي إلى المساس بخصوصياتهم، فتكون بذلك المعلومات اسمية، إذ إنها تسمح بالتعرف على الشخص محل هذه المعلومة بطريقة مباشرة أو غير مباشرة.

وتعرف البيانات الاسمية على أنها البيانات الشخصية التي تتعلق بالحق في الحياة الخاصة للمرء، كالبيانات الخاصة بحالته الصحية والمالية والوظيفية والمهنية والعائلية، عندما تكون هذه البيانات محلاً للمعالجة الآلية **(الشوابكة، 2007، صفحة 63)**. وتعرض البيانات الاسمية للاختراق قد يعرض صاحبها إلى الاستغلال أو الابتزاز أو أي ضرر مادي أو معنوي يؤثر على أمن خصوصية.

- **نشر وإعلان معلومات تتعلق بالحياة الخاصة للفرد:** حيث يتم نشر معلومات حول الحياة الخاصة بالفرد عبر مختلف وسائل التكنولوجيا دون موافقته الصريحة، أو عدم الالتزام بحدود هذا الرضاء فيما يتعلق بالتعامل مع المعلومات الشخصية وطرق المعالجة الإلكترونية لها، وما يتعلق من معلومات مثل الحالة الصحية والاجتماعية والأسرية وفي هذا الشأن استقر القضاء على أن لكل شخص حقا مطلقا، وقاصر على صورته وعن استعمالها وأن الاعتداء على صورة الشخص يكون الاعتداء على جزء هام من الخصوصية، وهو الأمر الذي يستوجب المسؤولية والعقاب بحسب النشاط المخالف للحق في الخصوصية **(محمد، 2016، صفحة 30)**.
- **التنصت على الآخرين:** يتنصت المجرم الالكتروني على الحياة الخاصة بالآخرين عن طريق استخدام برنامج معين يقوم بفتح منفذ في جهاز الشخص المعتدي عليه، يمكن من خلاله الاطلاع والاستماع إلى جميع المحادثات والمراسلات الصادرة من الشخص المعتدي عليه ويتم إدخال هذا الملف إلى الجهاز المعتدي عليه عن طريق البريد الإلكتروني أو عن طريق مواقع مغرية يزورها المعتدي عليه **(محمد، 2016، صفحة 41)**.

- **جرائم الذم والتحقير عبر الانترنت:** تعد جرائم الذم والقدح* والتحقير من أكثر الجرائم شيوعًا في نطاق شبكة الانترنت، إذ يساء استخدامها للنيل من شرف الغير أو كرامته أو تعرضه إلى بغض الناس واحتقارهم، بما يتم إسناده للمجني عليه على شكل رسالة بيانات **(الشوابكة، 2007، صفحة 30)**.

وتتنوع صور الذم والقدح والتحقير بتنوع الغرض من استخدام الانترنت، والطريقة التي يستخدم بها، فقد يكون الذم والقدح والتحقير وجاهيًا عبر وسائل الاتصال المباشر، أو قد يكون كتابيًا أو قد يكون غيابيًا، أو قد يكون بواسطة المطبوعات، وجميع هذه الصور ترتكب عبر الانترنت من خلال المبادلات الإلكترونية الكتابية أو الصوتية أو التصويرية، وهي إما أن تكون بين طرفيات انترنت (Internet Terminal) متصلة (الحواسيب)، وإما أن تكون بواسطة طرفية انترنت منفصلة (مستقلة) **(الشوابكة، 2007، صفحة 31)**، أو عبر ما تبثه شبكات التواصل الاجتماعي من مضامين مباشرة أو غير مباشرة باستخدام الأجهزة الذكية.

- **التشهير (Cyber Defamation)**: التشهير وتشويه السمعة في مواقع التواصل الاجتماعي سهل وميسر للعابثين وذلك بالقيام بنشر معلومات حصل عليها المتصل بطريقة غير مشروعة أو معلومات مغلوطة وتهدف إلى كسب مادي أو سياسي أو اجتماعي معين.

8. حجم الاختراق والتعدي على الخصوصية في الجزائر:

أسست الجزائر سنة 2009 قسم خاص لمكافحة الجريمة المعلوماتية متخصص في استغلال الأدلة المعلوماتية ضمن المديرية الفرعية للشرطة العلمية والتقنية، وتمكنت مصالح المديرية العامة للأمن الوطني خلال السداسي الأول من سنة 2013 معالجة ما مجموعه 383 قضية تتعلق بالجريمة الالكترونية، في حين تم معالجة 515 قضية خلال سنة 2012، ويتعلق الأمر بـ 126 قضية خاصة بالاستغلال غير القانوني للأداة المعلوماتية، و154 تتعلق بالهاتف النقال، و103 تخص الصور الفوتوغرافية والفيديو.

في هذا الصدد عالجت الخلية المركزية لمكافحة الجريمة الالكترونية خلال السداسي الأول من نفس السنة 15 قضية تتعلق بانتهاك خصوصية الحياة الشخصية (معالجة 6 قضايا سنة 2012) وأربعة خاصة بالتشهير (8 قضايا سنة 2012) و11 بسبب الابتزاز (4 قضايا سنة 2012) وواحدة خاصة بانتحال الشخصية (4 قضايا سنة 2012) و24 تتعلق بالقرصنة (10 قضايا سنة 2012)، ويشير القسم المختص في استغلال الأدلة المعلوماتية أن غالبية المخالفات تتعلق بالتكنولوجيات الجديدة سيما بواسطة الحواسيب والانترنت والهواتف النقالة. وتم كذلك تسجيل أزيد من 100 قضية خلال 9 أشهر من سنة 2014 ومعظمها تتعلق بالنصب والاحتيال على الأشخاص.

أما في السداسي الأول من سنة 2015 سجلت مصالح الأمن 417 قضية تتعلق بالجريمة الالكترونية، شملت انتحال الشخصية، النصب والاحتيال التزوير الإلكتروني تخريب بيانات شخصية وعامة، الابتزاز بصور أو معلومات مقرصنة، التشهير، السرقة الالكترونية.

يلاحظ من الإحصائيات أن نسبة الجرائم الالكترونية شهدت ارتفاعا مستمرا، ففي السداسي الأول من سنة 2015 فاقت الجرائم الالكترونية ما تم تسجيله في السنوات (2012، 2013 و2014) وهذا نظرا للارتفاع المتزايد لاستخدام شبكة الانترنت من قبل جميع الفئات الاجتماعية، وبالتالي ازدياد عدد ضحايا القرصنة والنصب والاحتيال ومختلف أشكال الجرائم الالكترونية الأخرى مع ارتفاع عدد مجرمي الانترنت (لطرش و بن عزوز، 2016).

* **القدح**: هو الاعتداء على كرامة الغير أو شرفه أو اعتباره، ولو في معرض الشك والاستفهام- من دون بيانات مادة معينة.

في حين سجلت سنة 2018 أكبر نسبة في قضايا القذف حيث احتلت نسبة 13.54% بمجموع 42 جريمة شملت قذف أشخاص وتشويه سمعتهم تليها نسبة 7.41% بمجموع 23 جريمة تمثلت في قضايا السب سواء بطريقة كتابية أو عن طريق رسوم ومطبوعات عبر البريد الالكتروني أو الصوتي، واحتلت قضايا التشهير نسبة 6.77 بمجموع 21 قضية وذلك بنشر معلومات مغلوطة عن أشخاص أو مؤسسات للتشهير بهم ونشر إشاعات و17 قضية بنسبة 5.58% من صنف المساس بخصوصية الأشخاص دون علمه ورضاه ووضع تعليقات مسيئة لهم أو التهديد والابتزاز (بن عابد و بن عابد، 2022، الصفحات 275-276).

من خلال النسب يتبين أن أكثر أشكال الجريمة الالكترونية في السنوات الأخيرة تمثل في جريمة القذف والسب وهذا نتيجة خاصية التخفي التي يمنحها الفضاء الالكتروني للمجرمين، وكذا بسبب عدم التبليغ عن الجريمة من قبل الضحايا خاصة أن اغلب الجناة من فئة أقارب الضحية، وكذا نقص الوعي بالقوانين التي تشرع للأمن السيبراني وتعاقب كل من يسيء استخدام التكنولوجيا الحديثة.

9. أشكال التهديدات التي تواجه أمن المعلومات:

يُعرف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. والمعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات، وضمان أصالة وصحة هذه الاتصالات مع الحماية من المخاطر المحتملة والناتجة عن استغلال ثغرات وضعف النظام.

تتزايد التهديدات التي تواجه أمن المعلومات نتيجة التطور المتسارع في الأساليب التي يمكن من خلالها الوصول لبيانات ومعلومات سرية خاصة بهدف تعديلها أو سرقتها أو حتى تدميرها. ويمكن تصنيف أساليب التهديد بهدف الحصول على المعلومات بأسلوب غير مصرح به إلى ما يلي:

أ. **اختراق الشبكات (Hacking)**: تتم عملية الاختراق من خلال سرقة كلمة السر (Password Cracking) أو التعرض للاختراق أثناء محاولة معالجة اختراق سابق (Zero-Day Attack) أو هجمات حقن قواعد البيانات أو (Structured Query Language Injection Attack).

ب. **الهندسة الاجتماعية (Social Engineering)**: ليس لمصطلح الهندسة الاجتماعية معنى متفق عليه، ولكن من أقرب التعريفات أن نقول إنها استخدام المهاجم لحيل نفسية كي يخدع مستخدمي الحاسوب ليمكنوه من الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها. وخلافاً لما قد يتوهم بعض الناس، فإن الهندسة الاجتماعية يجب أن تكون على رأس قائمة وسائل الهجوم التي تتطلب حماية المعلومات منها **(شوابكة، 2019، صفحة 170)**، والسبب في ذلك يرجع إلى الآتي:

- أن الهندسة الاجتماعية من أنجح الوسائل التي يستخدمها المهاجم لسهولتها مقارنة بالوسائل التقنية الأخرى.
- أن المتخصصين في مجال أمن المعلومات وكذلك مستخدمي الحاسوب لا يعيرون خطر الهندسة الاجتماعية في اهتمامهم **(الغثير، 2009، صفحة 31)**.

فالهندسة الاجتماعية يقصد بها تحفيز المستخدم على الإفصاح عن بيانات سريتها من خلال طرح أسئلة بهدف جمع معلومات دون إثارة أي شبهة، ويحتوي هذا الأسلوب على عدة تقنيات منها مايلي:

- **التوأمة الشريرة (Evil Twin)**: أي ادعاء جهة معينة بأنها جهة موثوق منها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به.
- **سرقة الهوية (Identity Theft)**: أي ادعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يكون الطلب منه تقديم المعلومات بشكل مباشر.

- **التصيد (Phishing)**: ويقصد منها وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة.

ج. **البرمجيات الضارة (Malwar)**: تتم عملية الاختراق من خلال برامج متخصصة لتسهيل التسلل إلى النظام أو الشبكة بهدف تدمير البيانات، وما أن يتم تثبيت البرمجية الضارة فإنه من الصعب جدًا إزالتها، ويحتوي هذا الأسلوب على عدة تقنيات منها:

- **حصان طروادة (Trojan Horse)**: برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم.
- **الفيروسات (Viruses)**: برامج تدخل إلى الحاسوب وتتصل بالملفات المخزنة به ثم يكرر نفسه بحيث يتم تدمير هذه الملفات.
- **برامج التجسس (Spywar)**: برمجيات تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب، وغالبا ما يتم تنزيلها بشكل سري تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الانترنت.

10. **التعدي على الخصوصية و الامن المعلوماتي:**

تعتبر جريمة الاعتداء على خصوصية الأفراد من أخطر الجرائم التي يمكن أن تقع عن طريق الانترنت نظرًا لعدم وجود الحماية التقنية الفاعلة لما يتم تداوله من معلومات وأسرار ومراسلات عن طريق الانترنت، وتشمل جريمة الاعتداء على الحياة الخاصة الاعتداء بالتنصت أو التسجيل، أو نقل لحديث صدر عن شخص أو مراسلة دون رضاه بواسطة جهاز معين، أو التقاط أو نقل صورة شخص تواجد في مكان معين دون رضاه، وإلحاق الضرر المادي والمعنوي عليه، وتشير أحدث تقارير الخصوصية إلى أنه لا تزال أسرار الأفراد وخصوصياتهم في خطر، وتعتبر عملية حماية الخصوصية في البيئة الرقمية من أهم الوسائل والإجراءات التقنية بوصفها عملية تكاملية محكومة بإستراتيجية محددة العناصر، ومن الخطأ مجرد الاعتقاد بأن استخدام بعض التقنيات يحمي البيانات الشخصية حماية كاملة. وبالإضافة إلى ذلك يجب عدم إغفال أهمية الحماية القانونية والتشريعية وتكاملها مع الحماية التقنية والتنظيمية.

الأمن المعلوماتي هو حماية للمعلومات من الوصول و الولوج اليها من قبل الاستخدام الغير مصرح به بالتالي يلعب دور في حماية البيانات الشخصية ومنه حماية الخصوصية باستخدام أساليب متبعة كالتشفير لحماية المعلومات و تصميم أنظمة تكنولوجية المعلومات تحافظ على الخصوصية مع احداث برمجيات توفر شكلا من اشكال حماية الخصوصية لمستخدميها و هي عبارة عن أدوات لإخفاء الهوية في مجال الاتصالات بالتالي تصفح المستخدمين للويب بشكل مجهول و دون الكشف عن هويتهم، وثمة خيار آخر لتوفير تقنية إخفاء الهوية يتمثل في إخفاء هوية البيانات من خلال برامج خاصة، حيث توجد أدوات تزيل أسماء المرضى وتجعل بيانات العمر تظهر كفترات زمنية: كأن يتم تمثيل من يبلغون 35 عامًا بأن عمرهم يقع ضمن الفئة العمرية 30-40. وتكمن الفكرة وراء برامج إخفاء الهوية هذه في عدم إمكانية ربط السجلات بالأفراد وعدم التمكن من الوصول لمعلومات الخاصة بالأفراد و المؤسسات و حماية خصوصياتهم من الاختراق و التعدي .

وفي الأخير يمكن القول أن التطور في التكنولوجيا على قدر ايجابياته للفرد والمجتمع إلا أن مصاحبته للكثير من السلبيات خلق لا أمن للفرد والمجتمع الأمر الذي يتطلب مرارا تطور متلازم ومتزامن لآليات تحفظ أمن وسرية المعلومات الشخصية للفرد والمنظمة والمجتمع، مع توجيه اهتمام المختصين نحو مخاطر وتهديدات الهندسة الاجتماعية والعمل على تنمية الوعي حول الاستخدام الآمن لوسائل التكنولوجيا خاصة في مجال المعلومات والمعاملات الالكترونية.

11. خاتمة:

تتضمن الخصوصية خصوصية المعلومات والخصوصية الجسدية أو المادية وخصوصية الاتصالات والمراسلات الهاتفية والبريد الإلكتروني ، وتشير الدراسات أن أسرار الأفراد وخصوصياتهم في الفضاء السيبراني لا تزال تتعرض للاختراق و للتهديد

الالكتروني، وتعتبر عملية حماية الخصوصية في البيئة الرقمية من أهم القضايا التي تشغل بال كل المهتمين بالأمن المعلوماتي والسيبراني.

تكمن وسائط الاختراق الالكتروني لخصوصية الفرد في البريد الإلكتروني، وشبكة الويب العالمية،و الأخبار،و غرف المحادثات والدردشة ويخلف هذا التنوع في الوسائط تنوعا في أشكال الجرائم الالكترونية التي تهدد الخصوصية وذلك حسب طبيعة الجهة المستهدفة فقد يكون الهدف سرقة المال المعلوماتي المعنوي، أو الاحتيال عبر الانترنت، أو الاختراق والدخول غير المشروع إلى الأنظمة الآلية، وتخطي نظام التأمين الخاص بها أو جرائم الإضرار بالبيانات أو الاعتداء على الملكية الفكرية لأسماء مواقع الانترنت أو الالتقاط غير المشروع للبيانات، أو التحويل الإلكتروني غير المشروع للأموال أو الاحتيال باستخدام بطاقات الدفع الإلكتروني عبر الانترنت.

تتحدد أشكال التعدي على خصوصية الفرد في اختراق حساب المستخدم وانتحال شخصيته وابتزازه، وكذا الاعتداء على الحياة الخاصة للفرد ونشر معلومات تتعلق بحياته الخاصة عبر مختلف وسائل التكنولوجيا دون موافقته، وكذا التنصت على الآخرين وتهديدهم أو تعريضهم إلى الذم والتحقير و التشهير عبر الانترنت.

نتيجة التطور المتسارع في الأساليب التي يمكن من خلالها الوصول لبيانات ومعلومات سرية خاصة بهدف تعديلها أو سرقتها أو حتى تدميرها تتزايد التهديدات التي تمس بالأمن المعلوماتي و تتحدد أساليب التهديد بهدف الحصول على المعلومات بأسلوب غير مصرح به في الهندسة الاجتماعية بمختلف تقنياتها واختراق الشبكات، و في خاتمة هذه الورقة العلمية نستخلص أهم التوصيات:

- تكثيف الدراسات والأبحاث حول مفهوم الخصوصية في البيئة الرقمية وسبل حمايتها التقنية والقانونية.
- تطوير التشريعات السيبرانية تماشيا مع التطورات الحاصلة في عالم التكنولوجيا.
- الانضمام إلى الاتفاقيات الدولية في مجال حماية خصوصية الأفراد والأنظمة المعلوماتية مما يحفز على التنسيق والتعاون مع الناشطين من خبراء في مجال الأمن المعلوماتي والسيبراني .
- التوعية والتحسيس من مخاطر التكنولوجيا الحديثة وخاصة تلك التي تهدد خصوصية الفرد والمنظمة وهوية الدول.
- توعية الأفراد من خلال نشر ثقافة التبليغ في حالة أي تهديد الكتروني يمس بخصوصياتهم.
- الاهتمام بالتربية الإعلامية والتعريف بمخاطر التكنولوجيا التي تواجه كل فئات المجتمع وتضمينها في المناهج الدراسية والمؤسسات التعليمية.

12.قائمة المراجع:

- **المؤلفات:**

1. طالب، أحسن مبارك، (2007)، **جرائم الاحتيال والعوامل الاجتماعية والنفسية المهيئة لها**، الرياض، جامعة نايف العربية للعلوم الأمنية.
2. سيفون، باية، (2016)، **الانترنت والصحافة الإلكترونية (دراسة في طبيعة العلاقة والتأثير)**، ط1، الجزائر، دار الخلدونية.
3. الغثير، خالد بن سليمان، (2009)، **أمن المعلومات: بلغة مسيرة**، تقديم محمد بن إبراهيم السويل، ط1، الرياض، مكتبة الملك فهد الوطنية.
4. الشاعر، عبد الرحمان بن إبراهيم، (2015)، **مواقع التواصل الاجتماعي والسلوك الإنساني**، عمان، الأردن، دار صفاء للنشر والتوزيع.
5. الشوابكة، محمد أمين، (2007)، **جرائم الحاسوب والانترنت- الجريمة المعلوماتية**، عمان، الأردن، دار الثقافة للنشر والتوزيع.

6. **محمد**، نصر محمد، (2016)، **المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية (دراسة مقارنة)**، ط1، مصر، مركز الدراسات العربية والتوزيع.

7. شفيق، نوران، (2016)، **أثر التهديد ات الإلكترونية على العلاقات الدولية (دراسة في ابعاد الامن الإلكتروني)**، ط1، القاهرة، مصر، المكتب العربي للمعارف.

- **الأطروحات:**

8. المويشر، تركي بن عبد الرحمان، (2009)، **بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته**، أطروحة دكتوراه في الفلسفة الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، السعودية.

- **المقالات:**

9. شوابكة، عدنان عواد، (2019)، **دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف**، مجلة دراسات وأبحاث، المجلد11، العدد04، 170.