الأمن المعلوماتي في مواجهة القرصنة الالكترونية

Information security in the face of electronic piracy

مريم بالطة[1]، آسيا برغيت[2]

[1]جامعة 20 اوت 1955 سكيكدة (الجزائر)، m.balta@univ-skikda.dz

[2]جامعة 20 اوت 1955 سكيكدة (الجزائر) brighetassia2020@yahoo.com

تاريخ الاستلام:2021/12/11 تاريخ القبول:2021/12/29 تاريخ النشر:2022/06/30

الملخص:

أدت التكنولوجيا الحديثة إلى تقريب المسافات بين الشعوب وذلك من خلال توفير العديد من وسائط الاتصال الجديدة التي لم تكن معروفة من قبل، كما نجد أن تلك التكنولوجيات أفرزت الكثير من السلبيات والمخاطر ولعل أهمها هي صعوبة تحكم واحتفاظ الفرد بخصوصياته جراء انتشار الكثير من الوسائل السهلة لقرصنة التطبيقات الالكترونية. ومن خلال هذا المقال سوف نبرز مختلف التحديات والصعوبات التي يواجهها الأمن المعلوماتي في مواجهة القرصنة الإلكترونية.

الكلمات المفتاحية: الامن المعلوماتي، القرصنة الالكترونية، تكنولوجيا الاتصال، الانترنت.

Abstract :

Modern technology has brought the distances between peoples closer by providing many new means of communication that were not known before, and we find that these technologies have produced many negatives and risks, perhaps the most important of which is the difficulty of controlling and preserving the individual's privacy due to the spread of many easy methods for piracy of applications And through this article, we will highlight the various challenges and difficulties that information security faces in the face of electronic piracy.

Keywords: information security, electronic piracy, communication technology, the Internet.

المؤلف المرسل(1)

1.مقدمة:

شهد القرن الواحد والعشرين ثورة متفردة في عالم تكنولوجيا الإعلام والاتصال، إلى الحد الذي اعد فيه بعض الخبراء والمختصين المجال المعلوماتي الالكتروني الميدان الخامس للنزاعات بعد الأرض والبحر والجو والفضاء، و لربما يعود ذلك إلى درجة الانتشار والتطور السريعين لهذه التقنية، إذ لا يكاد مجال من مجالات الحياة إلا وارتكز على هذه الأخيرة في ظل التحول التي قلصت الجهد، الوقت، التكلفة وساهمت بسرعتها ومرونتها في تلبية الحاجيات وأمام تغيير منطق الحروب حاليا إلى الاتجاه اللاتماثلي.

غير وانه على الرغم من ايجابيات التي حملتها الانترنت، إلا أنها حملت معها العديد من التهديدات والمخاطر الذي ترجمت في جرائم الكترونية، لم تفرق بين الأشخاص والمؤسسات والدول، ناهيك عن التهديدات التي قد تطال امن واستقرار الدول، إذ لا ينكر احد الدور المتعاظم لشبكة الانترنت في الثورات العربية.

إن هذه الجرائم تتميز بطبيعة خاصة تختلف عن الجرائم العادية فهي لا تترك آثار مادية يمكن من خلالها التوصل إلى الجاني كما في الجرائم العادية، كما انه إتلاف أو تغيير الأدلة في هذه الجرائم خلال لحظات دون أن يترك هذا التغيير آثار مادي يجعلها أكثر صعوبة وقد تزداد هذه مع الطبيعة الافتراضية الرقمية التي يرتكب فيها المجرم جريمته ومدى السهولة التي توفرها له في ارتكابها حيث انه من نقرة واحدة بسيطة على الكمبيوتر كافية للوصول إلى الضحية المحتمل، كما أنها في كثير من الأحيان لا تتم في خفاء فالمجرم يتعمد ذلك من خلال اللعب في البيانات وتدمير الدلائل إن أراد ذلك.

وعلى ضوء ذلك فان الظاهرة الإجرامية المعلوماتية باتت تشكل بعض التحديات القانونية والعملية التي وجب على الدول والمؤسسات والأفراد بشكل عام أن تتكاتف من اجل وضع سبل لكيفية الحد من هذه الظواهر وحماية حقوق الأفراد وحياتهم وبياناتهم وقد تظهر جليا بالجزائر في الوظائف المتعلقة بالأمن الوطني والدرك الوطني وضرورة تحقيق الأمن المعلوماتي للأفراد والمنظمات على حد سواء واعتباره إحدى المهام الأساسية والرئيسية التي يمكن أن تهدد امن واستقرار الوطن، فقد تتعلق بأفراد عاديين كما قد تمس امن الدولة كافة لذلك وجب العمل على وضع استراتيجيات وأساليب تتماشى مع التقنيات الجديدة التي يستخدمها المجرمين المقرصنين.

وبناء على ما سبق يمكن طرح الإشكالية التالية : **ما هي التحديات والصعوبات التي يواجهها الأمن المعلوماتي في مواجهة القرصنة الإلكترونية؟**

2. تحديد المفاهيم

1.2 الأمن المعلوماتي:

يشمل الأمن المعلوماتي الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية من أجهزة وبرمجيات وبيانات وأفراد من التجاوزات والتدخلات الغير مشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلل، أو كنتيجة لإجراءات خاطئة أو غير الوافية المستخدمة عن إدارة هذه المصادر وعليه فان موضوع امن المعلومات يشمل المحاور التالية :

- ✓ الأخطاء العفوية غير المعتمدة أثناء تجهيز البيانات لإدخالها على الحاسبة.
- ✓ حوادث فقدان أو تغيير المعلومات بسبب تعطل الأجهزة أو حصول خلل في البرامج.
- ✓ سرقة المعلومات أو التقاطها أو تغييرها بشكل غير مأذون وما ينتج عن هذا من سوء استخدام المصادر.
- ✓ فقدان قدرات إدارة المعلومات نتيجة وقوع بعض الكوارث الطبيعية (صادق، 2008).

2.2 الجريمة الالكترونية

تعرف الجريمة الالكترونية على أنها : " كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الالكترونية بقدر كبير لازم لارتكابه من ناحية، لملاحقته وتحقيقه من ناحية أخرى "، كما تعرف على أنها :" الفعل الغير مشروع الذي يتورط في ارتكابه الحاسب، أو هي الفعل الاجرامي الذي يستخدم في اقتراف الحاسوب باعتباره ادة رئيسية **(عقون، 2011)**."

3.2. الهجمات الالكترونية :

بعبارة بسيطة تعرف الهجمات الالكترونية على أنها عبارة عن هجوم يتم شنه من احد أجهزة الكمبيوتر أو مجموعة من الأجهزة على جهاز كمبيوتر آخر أو عدة أجهزة كمبيوتر أو شبكات، ويمكن تقسيمها إلى نوعين رئيسين على النحو التالي : "هجمات يكمن الهدف من ورائها تعطيل جهاز الكمبيوتر المستهدف أو هجمات يكون الغرض منها الوصول إلى بيانات جهاز الكمبيوتر المستهدف وربما الحصول على امتيازات المسؤول عنه" **(امؤسسة غانم).**

3.3.القرصنة الالكترونية :

عملية اختراق لأجهزة الحاسوب أو المواقع تتم عبر شبكة الانترنت غالبا لان اغلب حواسيب العالم مرتبطة عبر هذه الشبكة أو حتى عبر شبكات داخلية يرتبط بها أكثر من جهاز حاسوب ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في اختراق برامج الحاسوب وطرق ادارتها أي أنهم مبرمجون ذو مستوى عال يستطيعون بواسطة برامج مساعدة الحاسوب اختراق حاسوب معين للتعرف على محتوياته ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة **(الخلايلة، 2005)**.

3.عناصر الأمن المعلوماتي

1.3.السرية أو الموثوقية : وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين لذلك.

2.3.التكامل وسلامة المحتوى: التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث فيه، وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث فيه في أي مرحلة.

3.3.استمرارية توفر المعلومات أو الخدمة : التأكد من استمرارية عمل النظام المعلوماتي واستمرارية القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.

4.3.عدم إنكار التصرف المرتبط بالمعلومات ممن قام به : ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها انه هو الذي قام بهذا التصرف بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت ما (محمد، 2009).

4. القرصنة الالكترونية في الجزائر :

ان القرصنة الالكترونية في الجزائر يمكن أن تدخل على المدى القريب أو المتوسط من مؤثراتها، فتأثيرها يشابه والأزمة المالية العالمية المستفحلة حاليا فقد تم دق ناقوس الخطر بمناسبة تسليم شهادات الكفاءة لممثلي شركة IpBAICK، هذه الشركة العالمية المتخصصة في امن الشبكات المعلوماتية ضمن تكوين مهندسين في الإعلام الآلي، ومن

هنا تجلت الخدمات المضمونة لهذه الشركة في ميدان امن الشبكات المعلوماتية، حيث أوضح ممثلو هذه الشركة أن خدماتهم تضمن أقصى الأمن في تسيير شبكات المؤسسات.
أما في الجزائر أراد ممثلو هذه الشركة إجراء عملية تحسيس حول الظروف وإشكالية تامين الشبكات المعلوماتية في الجزائر ثم مناقشتها بقوة، حيث أوضحوا أن في الجزائر خطر كبير في الاعتداء المعلوماتي، وأوضحوا أن خطر الاعتداءات المعلوماتية ضد مواقع رسمية جزائرية يشكل تهديدا واقعا، ولحد الآن لا يوجد أي برنامج خاص بالجزائر مما يثير مخاوف أن تكون منظومتنا المعلوماتية لدى المؤسسات مقرصنة ومعتدى عليها.

وأضافوا أن أخطار القرصنة في الجزائر موجود في اي زمان ومكان ومنذ عامين تمكن الجزائريون من حل شفرة TPS رغم انه حتى الحين كان الروس في الطليعة في هذا الميدان.

كما أوضح الرئيس ومدير العام لشركة التعليم والتكوين " نوار حرز الله " منذ وقت بان المواقع الالكترونية لمؤسسات الدولة مستهدفة في حين موضحا بان عدد الاعتداءات على مختلف مواقع WEB قد بغت 3000 اعتداء في الشهر آنذاك، وفي هذا الميدان فان بعض المعتدين والهكرز يظهرون وبعضهم يبدي افتخارا بإمضاء قرصنته لأكبر عدد من المواقع وذلك الغرور تسبب لهؤلاء الأشخاص بعقوبات مستحقة.

إن المتتبع لظاهرة القرصنة الالكترونية في الجزائر يدرك التناقض الذي يميز هذه الظاهرة في حين لازال تصنيفها في مؤخرة التقنية التكنولوجية، تبقى تحتل المراتب الأولى في مجال القرصنة الالكترونية، حيث تشير التقارير والمعطيات المنشورة من قبل الهيئات المختصة والصحافة الوطنية إلى أن الجزائر تأتي على رأس البلدان العربية في ميدان القرصنة.

كما أن اختراق البرامج المعلوماتية يهم القراصنة الجزائريين وذلك لنوع الشفرة لباقي القنوات التلفزيونية مثلا، فعلى سبيل المثال تبادل شفرات الدخول للباقات التلفزيونية المشفرة فان الجزائريين يستعملون القرصنة كلمات سرية عن طريق برامج معروفة في هذا الميدان والتواجد في السوق الوطنية.

ويرى الخبير في مجال تكنولوجيا الإعلام والاتصال " السيد قرار يونس " إن تطور تكنولوجيا الإعلام والاتصال وما صاحبه من أضرار كالقرصنة الالكترونية وفي السياق ذكر

المتحدث أن درجة خطورة القرصنة في الجزائر قليلة مقارنة بمثيلاتها من الدول خاصة في مجال التجارة الالكترونية التي لم تشرع بعد في استعمالها، إلا انه الم على ضرورة التفكير من الآن في تنظيم هذه العملية وتحصين المواقع وتأمينها من خلال التطبيق الصارم للإجراءات خاصة ما تعلق بقرصنة البرامج، حيث يبقى تطبيق عقوبات على المخالفين متفاوت رغم أن القانون يمنع أي نوع من القرصنة سواء أن كانت الكترونية أو كلاسيكية.

وحسب السيد " قرار يونس " ففان التكتم على ظاهرة القرصنة وعدم التبليغ وتقديم الشكاوي عن حالات القرصنة خوفا من المشاكل التي قد يواجهها القائمون على الانترنت، يبقى عائقا أمام محاربة هذه الظاهرة.

من جهتها قالت الباحثة " هجيرة بودر" بمركز البحث في الإعلام العلمي والتقني أن القرصنة الالكترونية في الجزائر منتشرة بصفة واسعة، وان معظم البرامج المستعملة من قبل الجزائريين في برامج مقرصنة ابتداء من أنظمة " الونداوز" ومختلف طبعاته المستعملة، و ذكرت للمساء أن استعمال البرامج غير المقرصنة يعد جد ضئيل في الجزائر، ويقتصر عن بعض مؤسسات الدولة والذي يبقى غير كاف لان البرامج القرصنة تباع في الأماكن العمومية دون حسيب أو رقيب تقني بسهولة، كما أن الإقبال عليها واسع نظرا لثمنها الزهيد مقارنة بتلك الأصلية.

يعود ذلك أيضا إلى عدم استيعاب أهمية الأمن المعلوماتي والثغرات والعيوب التي تحتوي عليها البرامج المقرصنة والتي تهدد امن الأنظمة المعلوماتية، بينما يجب حسبها الذهاب نحو مصادر مجانية Open source المعروفة بأمنها وإمكانية معرفة ثغراتها (massa.com/or/content/view/27763).

5. تطور القرصنة الإلكترونية في ظل تطور تكنولوجيا الهواتف الذكية :

يتوقع خبراء التكنولوجيا الحديثة أن يسجل ازدياد كبير في هجمات القرصنة على أجهزة الهواتف الذكية في السنوات المقبلة والسبب أن سوق الأجهزة النقالة يعني بازدياد الوظائف وهو ما يفيد في التسويق، أكثر ما ينبغي بالسلامة واحترام خصوصية المستخدمين ويتوقع الخبراء تسجيل ازدياد كبير في هجمات القرصنة على أجهزة الهواتف الذكية في السنوات المقبلة، فعلى هامش المؤتمر الدولي حول الهواتف النقالة الذي انعقد في برشلونة لخص "جيمس لين " المسؤول عن السلامة في مجموعة " سوفوس" هذه المسالة بالقول أن

سوق الأجهزة النقالة يعني بزيادة الوظائف وهو ما يفيد في التسويق أكثر مما يعني بالسلامة واحترام خصوصية المستخدمين.

ويشير هذا الخبير بشكل خاص إلى مسؤولية مصنعي الأجهزة عن عدم توعية المستخدمين حول حماية الخصوصية، لافتا إلى أن 40 بالمئة فقط من المستخدمين يعتمدون مفتاح " بين كود " لحماية أجهزتهم.

مجموعة " سامسونغ مثلا ركزت في عرضها لهاتفها الذكي الجديد " اس 6" على مظهره ووضوح الصور التي يلتقطها، دون الالتفات إلى شؤون السلامة وحماية الخصوصية. فمستخدمي الهواتف الذكية اليوم يعانون اليوم ما كان يعانيه مستخدمو أجهزة الكمبيوتر الشخصية قبل 15 عاما، مع المخاطر المتزايدة الناجمة عن كون هذه الهواتف في حقيقة الأمر أجهزة الكمبيوتر متصلة بشكل دائم بشبكة الانترنت، كما يقول " تانغي دو كوتبون " المدير العام لمجموعة " كاسبيرسكي " المتخصصة في البرامج المضادة للفيروسات الالكترونية، أن 28 بالمئة من المستخدمين لا يعرفون شيئا عن البرامج المؤذية لأجهزتهم ما يجعلها مستباحة أمام هجمات القرصنة الالكترونية المعلوماتية.

وبحسب مجموعة " الكاتيل " فان 16 مليون شخص وقعوا ضحية هجمات القرصنة في 2014.

ويرى " دافيد غرو " مدير إقليم جنوب أوروبا في " انتيل سيكيوريتي " أن خطر القرصنة يسجل تصاعدا لان القراصنة يمكنهم من خلال عملياتهم الحصول على معلومات شخصية ولا سيما البيانات المالية للمستخدمين.

ولا ترعي الأجيال الجديدة من الهواتف الذكية مسالة السلامة، ماعدا بعض النماذج النادرة مثل بلاكفون2 بحيث يمنح هذا الهاتف لمستخدميه الحماية من الهجمات المعلوماتية وكذلك مراقبة أجهزة الاستخبارات، وفي هذا الإطار أيضا عرضت مجموعة " سي اس كومينيكاسيون ايه سيستم " الفرنسية شريحة ذاكرة توصل بالهاتف فتحول دون قدر احد على الولوج إلى المحادثات والبيانات المرسلة منه.

وبحسب الخبراء فان الهجمات تتركز على الأجهزة العاملة بنظام الأندرويد، الذي يسيطر على 80 بالمئة من السوق، غير أن نظام " اي ا واس " من ابل والذي كان ينظر إليه على انه أكثر أمنا من نظام غوغل لا يبدو انه بممنأى عن الهجمات، ويمكن لبعض

الفيروسات أن تسرق البيانات من جهاز الكمبيوتر وكذلك من الهاتف الذكي بعد ذلك يطلب القراصنة " فدية " لإعادة هذه البيانات، وفي كثير من الأحيان تدفع الفدية ولا تعود البيانات.، وإلى حين التوصل إلى حل جذري لمشكلة القرصنة للمعلومات يوصي الخبراء بتحميل برامج مضادة للفيروسات وعدم تحميل أي بيانات إلا من المواقع الرسمية المعروفة (www.france24.com).

6. سبل الوقاية من القرصنة الالكترونية عبر جهاز الهاتف النقال :

نشرت مجلة "ريدرز داجيست " في نسختها الاسترالية، تقريرا تحدثت فيه عن امن الهاتف، الذي لا يعد مجرد هاتف للتواصل وإنما بنتا نودع فيه صورنا ومختلف البيانات الشخصية، لذلك من المهم الحفاظ عليها من الاختراق.

وذكرت المجلة أن ما يجب القيام به هو تثبيت مضاد للفيروسات، حيث أن الهاتف الذكي يجب أن يعامل معاملة الكمبيوتر المحمول أو المكتبي من حيث ضرورة احتوائه على تطبيق ضد الفيروسات حفاظا عليه من القرصنة.

1.6.الحماية من الفيروسات : وترجع أهمية الحماية من الفيروسات لما تحتويه هواتفنا من معلومات شخصية مرتبطة بالحياة الخاصة والعمل، ويجب حمايتها دائما وأبدا من القرصنة الالكترونية لذلك يمكن اعتبار الحماية من الفيروسات هو خط دفاعك الأول ضد هذه القرصنة.

2.6.تشفير الرسائل النصية : وأيا كان نوع هاتفك الذكي أو مدى أهمية الرسائل النصية والمكالمات وحساسيتها لابد أن تجعلها دائما في وضع الإخفاء، ويتم ذلك عن طريق استخدام خاصية التشفير سواء لرسائلك النصية أو مكالماتك الخاصة.

3.6.قفل الشاشة : تشير التقارير إلى أن ما يقارب من 40 بالمئة من مالكي الهواتف الذكية لا يهتمون بقفل الشاشة أو ميزات الأمان الأخرى مع أن قفل الشاشة الرئيسية هي الطريقة الأسهل والأكثر وضوحا للحفاظ على حماية هاتفك بانتظام، بالإضافة إلى ذلك يوصي الخبراء بان تبذل قصارى جهدك لتأكد من عدم وجود كلمة مرور ضعيفة وتعلم كيفية قفل التطبيقات على هاتفك.

4.6.شبكات الانترنت العامة : قد تكون في مكان عام أو في احد الكافيهات والتي تسمح لك باستخدام شبكة الانترنت بالمكان ولكنها تشترط عليك ادخال بياناتك أو حتى بريدك

الالكتروني الخاص بك أن يجعل هاتفك عرضة للمتسللين الخبثاء الذين يمكنهم اختراق جهازك إذا لم تكن حريصا لهذا الأمر.

5.6. تطبيق الوصول إلى الهاتف المفقود : قد يتعرض جهازك إلى الفقد أو السرقة، و هو أمر وارد الحدوث لذلك يجب أن تكون مستعدا لمثل هذا الموقف واستخدام التطبيقات التي تساعدك للوصول إلى المعلومات الخاصة بك على جهازك المفقود، فعلى سبيل المثال يساعدك تطبيق find my iphone المدمج في إعادة الاتصال بهاتفك المفقود.

6.6.كسر الحماية : لا تفكر أبدا في كسر الحماية الخاصة بجهازك حتى يكون محررا من أي قيود مفروضة عليك من قبل هذا التصرف يخرج هاتفك أولا من فترة الضمان إن كنت قد حصلت عليه في وقت قريب وثانيا والاهم يصبح جهازك فريسة سهلة للقراصنة حيث يسهل عملية اختراقه (http://gate.ahram.org).

7.قانون القرصنة الالكترونية في الجزائر :

لقد استحدث المشرع الجزائري في تعديله لقانون العقوبات بمقتضى القانون 15/04 المؤرخ في 10 نوفمبر 2004 بإدراج القسم السابع مكرر وخصصه للاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات حيث جرم بعض الأفعال وحدد لها عقوبات :

1.7 جريمة الدخول والبقاء الغير مشروع إلى نظام المعالجة الآلية :لقد نص المشرع على فعل الدخول l acces في المادة 394 مكرر2 " يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة مالية من 50.000 إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل او جزء من منظمة المعالجة الآلية للمعطيات أو يحاول ذلك " ويقصد بالدخول هو ذلك النشاط المتمثل في الاتصال بنظام الكمبيوتر بهدف الفاعل من خلاله إلى الاطلاع على المعلومات التي يحتويها النظام وحسب نص المادة المذكورة أعلاه لكي يكون الدخول مجرما لا يشترط أن يقع على كامل النظام، بل يكفي أن يقع الدخول على جزء منه واشترط كذلك أن يكون الدخول من الغش غير انه لم يحدد وسائل وطرق الغش.

فضلا عن الدخول في النظام فان المشرع أضاف ما يعرف بالبقاء le maintien في نظام المعالجة الآلية للمعطيات ويتمثل هذا النشاط في مكوث الفاعل واستمراره داخل نظام الكمبيوتر بعد دخوله ولو عرضا أو يجاوز الوقت المسموح به للبقاء.

وقد نصت الفقرة الثانية من المادة 394 مكرر على تضاعف العقوبة إذا ترتب على ذلك حذف أو حذف المعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتعال المنظومة تكون العقوبة من 6 أشهر إلى 3 سنوات وبغرامة مالية 500.000 دج إلى 400.000 دج كل من ادخل بطريقة الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريقة الغش المعطيات التي يتضمنها " فقد تختلف أسباب الاختراق باختلاف أهداف المخترق فمنهم من يخترق لمجرد الفضول والبعض الذي يخترق لسرقة المعلومات من حواسيب الغير قد يكونوا عرضوها مقابل بدل مالي للاطلاع عليها، أما سبب الاختراق الذي أشار إليه المشرع فيكمن في نية المخترق في تبديل أو تحريف أو إزالة المعلومات في أجهزة الغير وهذا اخطر أنواع الاختراق.

2.7 جريمة الاستعمال الغير المشرع لأنظمة المعالجة الآلية للمعطيات :

نصت المادة 394 مكرر2 من قانون العقوبات " يعاقب بالحبس من 2 شهرين إلى 3 سنوات وبغرامة مالية من 1.000.000 كل من يقوم عمدا وعن طريق الغش بما يأتي :

- ✓ تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها جرائم المنصوص عليها في هذا القسم.
- ✓ حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها في هذا القسم.

وعليه يعد مرتكبا لهذه الجريمة كل من يستخدم البرامج المخزنة آليا بقصد الحصول على منفعة غير مشروعة، بمعنى الاستخدام الغير مصرح به لإمكانيات نظام المعالجة الآلية للمعطيات من اجل تحقيق منفعة شخصية.

- التشديد في حالة المساس بالمصالح العليا للوطن : نص المشرع الجزائري في المادة 394 مكرر3 تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات اشد.

3.7 الجرائم المعلوماتية الخاصة بالأشخاص:

لقد أتاحت الثورة الرقمية للمجرم المعلوماتي تسخير الحاسوب لتحقيق اغلب صور الاعتداء على الأشخاص وذلك بأبسط الأساليب من خلال التلاعب بالأنظمة المعالجة الآلية للمعطيات .

7-3-1 جرائم السب والقذف في صورتها المعلوماتية :

تعد جرائم السب والقذف من أكثر الجرائم انتشارا، وهي جرائم المساس بشرف الغير وسمعتهم ويكون عن طريق القذف أو السب كتابيا أو عن طريق المطبوعات أو رسومات، عبر البريد الالكتروني أو صفحات الويب بعبارات تمس الشرف ولقد اعتبر المشرع الجزائري صراحة أن من بين مكونات الركن المادي لارتكاب هذه الجريمة أن تكون موجهة لشخص الرئيس لاعتبار هذا الأخير من رموز السادة الوطنية وهذا ما نصت عليه المادة 144 مكرر3 " يعاقب بغرامة من 100.000 إلى 500.000 دج كل من أساء إلى الرئيس بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان عن طريق الكتابة أو الرسم أو التصريح أو بأية وسيلة أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة الكترونية أو معلوماتية أو إعلامية."

7-3-2 جرائم الاعتداء على حرمة الحياة الخاصة :

تعد جرائم الاعتداء على الحياة الخاصة من الجرائم القديمة التي عرفتها المجتمعات الإنسانية القديمة ولكنها سرعان ما تطورت نظرا للتقدم التكنولوجي الذي لعب دورا في سرعة وسهولة انتشار الأخبار والصور الذي من شانه أن يمثل تهديدا لخصوصية الأشخاص وسهولة الاعتداء على حرمة حياتهم الخاصة ومن هنا كانت الحاجة إلى وجود حماية قانونية صارمة تساهم في الحد من هذه الجرائم، وهذا ما نصت عليه المادة 303 مكرر2 يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك :

- بالالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.
- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.

8.عوائق تحقيق الأمن المعلوماتي في الجزائر في ظل الآنية والمستقبلية

تواجه مصالح الدرك الوطني والأمن الوطني العديد من العوائق والتحديات التي تعيقها في تحقيق الأمن المعلوماتي الالكتروني، يمكن أن نذكر أهمها فيما يلي :

- زيادة عدد المشتركين في شبكة الانترنت أكثر من 10 ملايين مشترك بالجزائر، مع زيادة عدد المستخدمين في الشبكة تزداد المخاطر، لتتحول عملية اكتشاف هوية مرتكبي الجرائم الالكترونية تحدي بسبب صعوبة البحث والتحري ضمن هذا العدد الهائل والمتجه للارتفاع باستمرار.
- انتشار تكنولوجيا الانترنت فائقة السرعة والتدفق ADLS/ VSAT /SDSL تسهم التكنولوجيا المتطورة في سرعة انجاز الجريمة، وهذا يضع الجهات الأمنية المختصة أمام تحدي مباشرة التحقيقات ومتابعة الجناة، والتسلح بالأجهزة المتطورة والبرامج الحديثة السريعة الخدمة (سمير، 2017).
- التطور التكنولوجي وظهور الانترنت اللاسلكي WIFI/ 3G/4G عبر هذه التقنيات لم يعد المجرم يحتاج الجلوس أمام الحواسيب الموصولة سلكيا بشبكة الانترنت للقيام بجريمته، مما يستدعي من الجهات الامنية رفع التحدي والاستعداد بأحدث التقنيات لمواجهة والتصدي لهذه التطورات.
- الاستعمال الواسع لشبكات التواصل الاجتماعي إذ وصل عدد مستخدمي هذه المواقع في الجزائر إلى أكثر من 7 ملاين مستعمل، وهو ماساهم بشكل كبير في ارتفاع أنواع متعددة من الجرائم الالكترونية، مثل القذف، التحرش الجنسي، استغلال القصر، و غيرها وهذا ما يستوجب وضع استراتيجيات جد محكمة لضمان الأمن المعلوماتي عند استخدام مواقع التواصل الاجتماعي.
- عمليات التخفي عند استعمال خدمات شبكة الانترنت PROXY وهي من اكبر الإشكاليات التي تواجهها الجهات المختصة بالتحقيق، ويتطلب تعاون جهات متعددة والتسلح بالوسائل المتطورة التي يمكن لها رصد الجزئيات وفك الشفرات وتطوير البنى التحتية الخاصة بالمعلومات وتحديثها باستمرار وتصميم برامج عالية التطور.

- التطور التكنولوجي في مجال الانترنت والاتصالات وهو ما يفرض على الأجهزة الأمنية المختصة بان تساير هذا التطور، سواء من حيث اكتساب التكنولوجية التقنية أو من حيث التمكن في استخدامها واستثمارها بالشكل اللازم، وهذا قد يرهق ميزانيتها المحدودة، لذلك يتوجب توفير جميع الإمكانيات المادية والمالية والبشرية اللازمة لتحقيق الأمن المعلوماتي.
- نشر توعية الأمن المعلوماتي لمستخدمي شبكة الانترنت وهو ما يستوجب القيام بحملات توعوية بين مستخدمي شبكة الانترنت لاتخاذ التدابير اللازمة لضمان الحد الأدنى من الأمان وتعليمهم آليات التشفير والاحتياط الواجب توفيرها عند استخدام مواقع التواصل الاجتماعي، كما يجب توعيتهم بضرورة التحلي بثقافة التبليغ في الوقت اللازم لتتمكن الجهات المعنية من القيام بدورها في الوقت المناسب والتوصل إلى مرتكبي الجرائم.
- تفعيل القوانين على ارض الواقع وتطبيقها بصرامة، إذ من بين اكبر الإشكالات التي تسهم في انتشار الجريمة الالكترونية هو الإفلات من العقاب والتأخر في تفعيل القوانين، وهو ما يمنح المجرم فرصا لتكرار جرائمه، ولذلك من الضروري تأكيد تطبيق القوانين كما يجب أن تتكيف النصوص القانونية مع التغيرات الحاصلة في هذا المجال، كما تتوجب إنشاء محاكم متخصصة بالجرائم الالكترونية نظرا للانتشار الواسع لهذه الجرائم (سمير، المرجع نفسه).

8.خاتمة:

خلصت الدراسة إلى أن أبرز الهجمات الإلكترونية تعود للمهاجمين الذين لديهم خيارات عديدة أثناء اختيار الهجمات لاختراق أنظمة المعلومات وتعطيلها. وكذلك يتعين علينا أن نتخذ إجراءات استباقية في حماية شبكتنا وتأمينها.

الاستمرار في تحديث برامج حماية الفيروسات بقاعدة البيانات، وضع كلمة مرور قوية، واستخدام نموذج بيئة تكنولوجيا معلومات ذو امتيازات منخفضة لحماية أنفسنا من القرصنة الإلكترونية.

وهناك بعض البرامج ايضا التى توفر لنا حماية اضافية وتقف كحائط ضد القرصنة الالكترونية.

قائمة المراجع:

الكتب:

1. الخلايلة، عايد رجال. (2005). تأليف *المسؤولية التقصيرية الالكترونية*. دار الثقافة للنشر والتوزيع.
2. دلال، صادق. (2008). تأليف *امن المعلومات* (صفحة 12). دار اليازوري العلمية للنشر والتوزيع. الاردن.

الأطروحات:

3. بن عقون، حمزة. (11 01, 2011). السلوك الاجرامي للمجرم المعلومات. جامعة باتنة، بحث مكمل لنيل شهادة الماجستر في العلوم القانونية، الجزائر.

المقالات:

4. بارة، سمير. (2017). الامن المعلوماتي في الجزائر السياسات والتحديات. *المجلة الجزائرية للامن الانساني، 04*، 275-276
5. علوطي، محمد. (2009). تحديات الامن الالكتروني في المؤسسة. *مجلة ابحاث اقتصادية وادارية، العدد6*، 168
6. حوالف، حليمة. معالم الجريمة الالكترونية في القانون الجزائري. *مجلة البحوث القانونية والسياسية، 03* (16)، 146-150
7. http://gate.ahram.org. (بلا تاريخ). تاريخ الاسترداد 28 10, 2021
8. www.el massa.com/or/content/view/27763. (بلا تاريخ). تاريخ الاسترداد 28 10, 2021، من
9. www.el massa.com/or/content/view/27763.
10. www.france24.com. (بلا تاريخ). تاريخ الاسترداد 26 10, 2021
11. للحاسب الالي امؤسسة غانم. (بلا تاريخ). http:// www.it.pillars.com. تاريخ الاسترداد 26 10, 2021، من http:// www.it.pillars.com.