مجلة الحكمة للدراسات الاعلامية و الاتصالية
Eissn :2600-6863 Issn : 2353-0502
المجلد 10 / العـدد 04 (2022)، ص: 56- 74

التدابير الأمنية لحماية المؤسسات الإعلامية من الجريمة الإلكترونية

Security measures to protect media organizations from cybercrime

خديجة الرياط [1]،

[1] معهد الصحافة وعلوم الأخبار جامعة منوبة –(تونس)،

butmaamer@yahoo.fr

تاريخ الاستلام: 2022/11/21 تاريخ القبول: 2022/11/24 تاريخ النشر: 2022/12/09

ملخص:

تهدف هذه الدراسة البحثية إلى محاولة تسليط الضوء على ما هي أهم المعايير والتدابير الأمنية التي من شأنها زيادة فعالية نظام الحماية من الجريمة الإلكترونية في المؤسسات الإعلامية، والذي يعطيها حصانة من محاولات الاختراق والولوج إلى المعلومات.

وتم التوصل إلى أن هناك ضعف على مستوى البنية التحتية الذي لا تتواكب مع البيئة الرقمية الدولية، كما أن الإجراءات القانونية في حال وجود اختراق معلوماتي لا ترقى لمتطلبات الحماية الإلكترونية مما يؤدي إلى سهولة استهداف المعلومات (المؤسساتية والحكومية)

كلمات مفتاحية: الجريمة الإلكترونية، المؤسسات الإعلامية، الأمن المعلوماتي.

Abstract:

This research study aims to try to shed light on what are the most important security standards and measures that will increase the effectiveness of the cybercrime protection system in media institutions, which gives them immunity from hacking attempts and access to information.

It was concluded that there is a weakness in the level of infrastructure that does not keep pace with the international digital environment, and that legal procedures in the event of an

information breach do not meet the requirements of electronic protection, which leads to easy targeting of information (institutional and governmental).

Keywords: cybercrime, media institutions, information security.

***المؤلف المرسل:** خديجة الرباط

1. مقدمة

إن القرصنة الالكترونية في دول العالم تعتبر من بين الإشكالات التي أصبحت عائقا يهدد الأمن المعلوماتي لها، حيث أصبح هاجس الجريمة الإلكترونية ينموا شيئا فشيئا ويتطور مع تطور الأساليب الحديثة في مجال الإعلام، مما سهل على مرتكبي القرصنة الحصول على المعلومات من أي بلد دون عناء، بل تعدى ذلك ليصبح مفهوم الجريمة الإلكترونية مفهوما ذو دلالة مؤسساتية وأبعاد تشكل إن لم تصنع وعيا ناتجا عن تعبئة ممنهجة. ورغم وجود قوانين تجرم هذه العملية إلا أنه لا يزال هنالك نقص في بعض الحالات التي يسهل التحكم فيها والتي تمس أمن الدولة في حد ذاتها. وعليه نجد أن المؤسسات الإعلامية في الجزائر خاصة وفي الوطن العربي عامة عرضة للقرصنة مما يجعلنا في بحثنا هذا نسعى إلى ضرورة البحث عن آليات لمحاربة القرصنة الإلكترونية لهذه المؤسسات وحماية المعلومات والحفاظ على أمنها. وللإجابة على هذا الموضوع نطرح الإشكال الرئيسي الآتي:

إشكالية البحث: وللإجابة على هذا الموضوع نطرح الإشكال الرئيسي الآتي:

ما مدى فاعلية التدابير الأمنية لمكافحة الجريمة الإلكترونية للمؤسسات الإعلامية ؟

وللإحاطة أكثر تم تجزئة الإشكالية الرئيسية إلى الإشكاليات الفرعية التالية:

- ما مدى تأثير الجريمة الإلكترونية على أمن المعلومات لدى المؤسسات الإعلامية؟

- هل التدابير الأمنية المعمول بها حاليا كافية للحفاظ على أمن معلومات المؤسسات الإعلامية؟

الفرضيات: بغية الإجابة على الأسئلة السابقة قمنا بصياغة الفرضيات التالية:

- في بعض الأحيان لا يمكن حماية معلومات المؤسسات الإعلامية من الجريمة والقرصنة الإلكترونية ذات المستوى العالي؛

- للوصول إلى فعالية الآليات المتبعة لمحاربة الجرائم المتصلة بأمن معلومات المؤسسات الإعلامية لابد من تطوير برامج حماية ذلت تقنية عالية؛

أهمية الموضوع: يشكل موضوع التدابير الأمنية لحماية المؤسسات الإعلامية من الجريمة الإلكترونية أهمية كبيرة في مجال أمن وسرية المعلومات لهذه المؤسسات عامة وأسرار الهيئات العمومية خاصة، حيث تقوم هذه المؤسسات بإيجاد آليات وتدابير للقضاء على الجريمة الإلكترونية.

أهداف الموضوع: إن لهذا الموضوع عدة أهداف تبدأ بتحليل وتشخيص ظاهرة الجريمة الإلكترونية، الوقوف على آليات مكافحتها، والبحث عن مدى فاعلية هذه الآليات في المؤسسات الاعلامية، وبيان دور المؤسسات الإعلامية في الحفاظ على أمن وسرية المعلومات الخاصة بها.

منهجية البحث: تم الاعتماد في هذه الدراسة على المنهج الوصفي في عرض مفاهيم أساسية لها.

2. الاطر النظرية للجريمة الإلكترونية:

من خلال هذا العنصر سنطرق على المفاهيم العامة للجريمة الإلكترونية من عدة زوايا كما يلي:

1.2 التعريف القانوني للجريمة الالكترونية:

عرف المشرع الجزائري الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية"، وبهذا فقد وفق المشرع برأينا في تعريفه لأنه جمع الحالات التي تكون فيها نظم المعلوماتية و شبكات الاتصال إما موضوعا للجريمة أو وسيلة أو دعامة لجرائم تقليدية، ولولا هذه النظم المعلوماتية و شبكات الاتصالات ما كان أن نصبغ صفة المعلوماتية على هذه الجرائم. وعلى خلاف المشرع الفرنسي الذي لم يعطي تعريفا للجريمة الالكترونية فإن المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب المادة الثانية من القانون 09-04 على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية". ويلاحظ على هذا التعريف ما يلي :

- إن المشرع الجزائري قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الالكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الالكترونية، وثانيها معيار موضوع الجريمة المساس بأنظمة المعالجة الآلية

للمعطيات وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

- كما حدد المشرع الجزائري نطاق الجريمة الالكترونية وذلك عن طريق إقراره بأن الجريمة الالكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الالكترونية في القانون الجزائري (بوضياف، 2018، ص ص352-353).

2.2 خصائص الجرائم الالكترونية:

تنفرد الجريمة الالكترونية بمجموعة من الخصائص التي تميزها عن الجرائم التقليدية، ومن أبرز هذه الخصائص(غدير، 2020، ص234):

- سرعة التنفيذ؛
- التنفيذ عن بعد؛
- عابرة للدول؛
- جرائم ناعمة؛
- صعوبة متابعتها وإثباتها.

3.2 دوافع ارتكاب الجرائم الالكترونية:

هنالك العديد من الدوافع اهمها ما يلي(غدير، 2020، ص234):

- الولع في جمع المعلومات؛
- حب المغامرة و الإثارة؛
- الدوافع الشخصية؛
- تحقيق المكاسب المالية؛
- الدوافع السياسية.

3. المؤسسات الإعلامية والأمن المعلوماتي:

أصبحت قضية الأمن المعلوماتي من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لاسيما في ظل تنامي التهديدات الأمنية الالكترونية على مستوى

الدول والمؤسسات العامة والحكومية والخاصة سواء بالنظر لعدد الهجمات أو الاضرار الناجمة عنها، غير أن مسألة الأمن المعلوماتي مسألة قانونية أكثر منها مسألة تقنية لتعلقها بمجالات الخصوصية وأمن المعلومات فلابد أن تعد الجهات الادارية حزمة قوانين منظمة للأمن المعلوماتي وأن يكون للقانونيين دور في تصميم الاجراءات والتدريب وتقديرات المخاطر السيبيرية. لذا إن لم يكن الفضاء الالكتروني والمعلوماتي وسيلة موثوقة بها للاتصال أو التجارة فسيعرض الأفراد كما الشركات عن الاستثمار ويزيد من احتمالية ذلك الفرض التقاعس الحكومي في دول العالم خاصة العالم الثالث عن توفير و تطبيق الاجراءات الدفاعية اللازمة. ويتهدد الأمن المعلوماتي للإدارة بصورة كبيرة لاعتماد الإدارة في الوقت الحالي في إدارتها لمرافقها على نظام الحكومة الالكترونية، وقد يصل الأمر لانتهاك أمن الدولة الوطني كالإطلاع على معلومات تمس أمن الدولة أو الوصول إلى أنظمة التحكم في محطات المفاعلات النووية (رجب، 2021، ص 118).

1.3 أهمية الإدارة للمؤسسات الإعلامية:

إن النجاح الذي تحققه مؤسسات الأعمال والتي باتت من ضمنها اليوم المؤسسات الإعلامية يعود بالأساس إلى وجود إدارات قديرة، وقوية، ومتفهمة لطبيعة مهامها وأعمالها، وواعية للبيئة المحيطة بها. لذلك، فإن المهمة الأساسية للإدارة تتمثل في جعل المؤسسة بكاملها تستهدف إلى الإنجاز العالي من خلال أفضل تطويع للموارد كافة. وإذا أمعنا النظر في حياتنا اليومية، فإننا نجد أن الإدارة تمارس أولا على المستوى الشخصي من خلال إدارة الفرد لشؤون معيشته، ومن ناحية أخرى سنجد أن الإدارة مطبقة على المستوى الجماعي من خلال ممارسة مختلف أنواع مؤسسات الأعمال للأنشطة الإدارية. أي أن للإدارة مكانا في كافة أنشطة حياتنا اليومية.. ولقد نتج عن التطور الصناعي والتكنولوجي الهائل اتجاهات حديثة لتغيير أساليب إدارة الأعمال في المؤسسات الإعلامية، الصحفية، ومن أهم هذه الاتجاهات ما يأتي (زامل، 2017، ص ص16-17):

- الإيمان بأهمية رأس المال الفكري والمعرفي؛

- الإيمان بأهمية التكنولوجيا بشكل كبير في دعم الإدارة داخل المؤسسة الاعلامية؛
- تغيير مفاهيم الرقابة على العمل الإعلامي؛
- التركيز على بناء فرق العمل المنتجة في المؤسسات الإعلامية على اختلاف أنواعها.
- الاهتمام بالموازنة بين حياة الأفراد وعملهم؛
- التركيز على السرعة في الإنجاز مع الكفاءة.

إذن الإدارة تعد ذات أهمية بالغة، لأنها الضمان الوحيد لإنجاز الواجبات والحصول على النتائج المطلوبة وفق عملية متقنة، فهي تتضمن القيام بدور إشرافي مرن وواسع المدى، والتركيز على الآخرين وأدائهم، وتعلم المهارات الجديدة وتطوير المهارات القديمة، وإعطاء وتلقي الآراء حول العمل، والتخطيط للمستقبل، وتفويض المهام، والكثير من الممارسات التي تتوسع وتتعقد مع ازدياد الخبرات في العمل.

2.3 تعريف الأمن المعلوماتي:

وسوف نتطرق إلى الأمن المعلوماتي من عدة أوجه كما يلي:

وردت كلمة " أمن " في معجم لسان العرب لابن منظور " بمعنى الأمانة و الأمان، أي أمنت فأنا آمن وآمنت غيري من الأمن، والأمن ضد الكفر ويقال آمن فلان يأمن أمنا و أمنا، وشتق مصطلح الأمن من securitas المتكونة من sini بمعنى غير و فكرة cura بمعنى غياب السلامة والأمن أما معجم " بلاكويل " فيعرف الأمن على أنه مفهوم يرد في المناقشات التي تدور حول السياسة الخارجية لكنه يطبق على أوضاع الأفراد والدول وهو لابد أن يكون من جهة مسألة إدراك حسي ومسألة ظروف مادية من جهة أخرى ومن خلال ذلك يبدو أن هناك ارتباط بين مفهوم الأمن والسيادة (قادة، 2021، ص8.).

ويعرف الأمن المعلوماتي بأنه مجموعة من الإجراءات و التدابير الوقائية التي تستعمل سواء في المجال الفني أو الوقائي لصيانة المعلومات الخاصة بالإدارة الالكترونية، والإجراءات القانونية التي تتخذ، تحمي من حدوث أي تدخلات غير مشروعة سواء عن طريق الصدفة أو بشكل متعمد. ويثير موضوع أمن المعلومات العديد من القضايا القانونية الهامة والتي تؤثر على الحياة العامة والخاصة، فأمن المعلومات يؤثر على حقوق الملكية الفكرية والسرية والخصوصية وحماية البيانات والحق في حرمة الحياة الخاصة، ولقد استحدثت مجموعة من الجرائم بفعل أنظمة المعلومات نذكر على سبيل المثال: الاحتيال المصرفي والمالي، الإرهاب الالكتروني، القرصنة والفيروسات التي تخرب نظم المعلومات وتفسد البيانات(حمودي، 2020، ص95).

3.3 خصائص ومميزات أمن المعلومات:

يتميز أمن المعلومات بعدة خصائص وهي كالآتي(الدوسري، العريشي، بدون سنة، ص10):

- يجب أن تكون مناسبة اقتصاديا أي ذات جدوى اقتصادية؛
- يجب أن تكون مفهومة للمستخدمين؛
- يجب أن تكون واقعية تتناسب مع واقع المنظمة؛
- يجب أن تكون متناغمة مع اهداف المنظمة؛
- يجب أن تكون مرنة و قابلة للمعالجة؛
- يجب أن توفر حماية معقولة لأهداف الإدارة المعلنة؛
- يجب أن تكون مستقلة أي لا تعتمد على أجهزة **Hardware** ولا برامج **Software** محددة.

4.3 أهمية أمن المعلومات:

تكمن فيما يلي(قدايفة، بدون سنة، ص 165):

- القطاعات الاقتصادية تعتمد على صحة ودقة المعلومات؛

- حاجة الدول لوجود إجراءات أمنية قابلة للتطبيق، تغطي المخاطر التي يمكن أن تظهر عند التعامل مع الأطراف الاخرى؛
- الحاجة المتزايدة لإنشاء بيئة الكترونية آمنة تخدم القطاعين الخاص والعام؛
- النمو السريع في استخدامات التطبيقات الالكترونية والتي تتطلب بيئة آمنة؛
- الحاجة إلى حماية البنية التحتية للشبكة المعلوماتية من أجل استمرارية الأعمال التجارية؛
- مع تطور التقنية المعلوماتية وازدهارها توفرت فرص للإجرام الالكتروني.

4. التدابير الأمنية للحماية من الجريمة الإلكترونية:

ونصت المادة 11 من مبادئ الأمم المتحدة التوجيهية لمنع الجريمة بضرورة أن تستند الاستراتيجيات والسياسات والبرامج و التدابير المتعلقة بمنع الجريمة إلى " أساس عريض متعدد التخصصات من المعرفة بمشاكل الجريمة "، يجب أن تتضمن هذه القاعدة المعرفية إنشاء نظم البيانات و يعتبر جمع البيانات لإعداد إجراءات التدخل لمنع الجريمة والحد منها عملية لا تقل أهمية عن الجريمة السيبرانية كما هو الحال بالنسبة لأنواع الجرائم الأخرى ويتبلور استخدام قياس الجريمة السيبرانية للإعلام عن مبادرات الحد من الجريمة في تعزيز الاستجابات المحلية والوطنية والإقليمية والدولية، وتحديد الفجوات في الاستجابات وتوفير معلومات استخباراتية وتقييم للمخاطر وتثقيف وتوعية الجمهور. ويسلط العديد من المعلقين الضوء على التحديات الخاصة التي تعترض سبيل جمع المعلومات بشأن مجال و طبيعة الجريمة السيبرانية وتشتمل هذه التحديات على إشكالية تحديد ما يشكل الجريمة السيبرانية في المقام الأول والتحديات المتعلقة بالنقص في التقارير المقدمة وتسجيل أعداد نقل عن العدد الحقيقي واستعراض القضايا

المنهجية والوعي، واحتمال حدوث تضارب في المصالح للبيانات الخاصة بالقطاع الخاص (مكتب الأمم المتحدة، 2013، ص34).

1.4الجدار الناري:

تعتبر من أهم الأدوات المستخدمة في تأمين الشبكات ومنع الاتصالات الخارجية المرتبة في الانترنت من وصول إلى داخل الشبكة إضافة إلى قيامها بفلترة الاتصالات الخارجية لبعض الخدمات المتوفرة على الشبكة الدولية، و ظهرت تقنية الجدار الناري في أواخر الثمانينات عام 1988 عندما قام مهندسون من **DEC** بتنظيم نظام فلترة عرف باسم جدار النار بنظام فلترة العبوة والجدران النارية والتي تدعى كذلك بجدران الحماية، والتي تتمثل في أدوات الكترونية أمنية تمنع الوصول الغير مسموح به إلى الحاسب الشخصي وذلك عن طريق إقامة حاجز يفصل بين الشبكة و الحواسيب الشخصية، تجبر به جميع عمليات الدخول والخروج للمرور عبر هذا الجدار الذي يتصدى لجميع محاولات الدخول بدون صفة(حمودي، **2020**، ص ص98-99).

2.4 الحلول العملية فيما يتعلق ببعض الإجراءات المتطلبة لمكافحة الجريمة الالكترونية:

يطرح بعض الفقه حلولا عملية لمواجهة تحديات ومشكلات الجرائم الالكترونية، وتتمثل بالآتي (العجمي، 2014، ص110):

لابد من اتخاذ وسائل الحيطة و الحذر في تعامل البنوك مع الأنشطة المصرفية التي تتم عبر الإنترنت نظرا لأن تركيز غاسلي الأموال يتم على هذه البنوك و بهذه الأساليب باعتبارها مرتعا خصبا لتجارتهم خصوصا إذا كانت الدولة التي ترعى هذه البنوك أو التي في ضيافتها تعاني من عجز في النظام الرقابي العام للدولة؛

- إصدار قوانين واضحة وصارمة تلزم جميع المصارف بوضع الخطوات العملية الضرورية لمنع غسل الأموال فيها خاصة تلك الأموال التي يتم التعامل بها عبر الأنترنت؛

- ضرورة قيام المصارف بتدابير عملية من شأنها تكشف محاولات غسل الأموال فيها، ومراقبة جميع التعاملات الالكترونية؛

- ضرورة قيام المصارف بإنشاء أجهزة أو إدارات تتولى مراقبة و متابعة البلاغات التي تصلها عن أي عملية أو نشاط مشبوه و بالتالي الإبلاغ عنها للجهات المختصة في الدولة خاصة إن كانت تلك العمليات المصرفية تتعلق تتم عبر الانترنت؛

- ضرورة تدريب المحققين على القيام بالكشف عما تحتويه أجهزة الكمبيوتر من برامج مخزنة عند الضرورة مما ييسر عمليات التفتيش التي تتم على كمبيوتر المتهم؛

- ضرورة تدريب العاملين في المباحث الجنائية على تفحص الأدلة الالكترونية؛

- ضرورة الاستعانة بخبراء في الكمبيوتر والشبكات أثناء عمليات التقصي والتحقيق في الجرائم المعلوماتية والانترنت.

3.4 الإجراءات والتدابير الإدارية الواجب اتخاذها لحماية المعلومات الحكومية:

هناك مجموعة من الإجراءات الإدارية التي يمكن استعمالها في هذا الصدد لتحقيق أمن المعلومات، حيث على الحكومات التي تتبنى تقديم خدماتها الالكترونية للمواطنين القيام بعدة مهام اتجاه أمن المعلومات كالرقابة والإشراف على أمن المعلومات وسوف يتم استعراض مهام رئيسية يجب عليها القيام بها وهي كالآتي (يحياوي بدون سنة، ص11):

- **توفير أمن الأجهزة:** لتأمين الأجهزة لابد من تأمين المبنى كعدم السماح لغير المصرح لهم بالدخول إلى غرفة الحاسب الآلي ومخزن وسائط التخزين،

ويفضل استخدام التكنولوجيا الحديثة للدخول على الأنظمة (بصمة الأصبع، بصمة العين، البطاقة الممغنطة ...)؛

- **توفير أمن البيانات:** يتوجب على الإدارة توزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني وتقليص الجرائم ووضع آلية يتم تنفيذها للقيام بالنسخ الاحتياطي وتأمين وسائط الحفظ الخارجية بما يكفل أمنها وتحديثها ويجب صياغة الضوابط المنظمة لعمليات التشغيل ولمبرمجي قواعد البيانات ومدرائها ولإدارة الشبكات وخطوط الاتصال ولعمليات الإدخال و الإخراج والضوابط الأمنية لبناء وتشغيل البرامج التطبيقية؛

- **توفير أمن الأفراد:** عندما تريد الإدارة حماية معلوماتها عليها اتباع الإجراءات الإدارية في مجال أمن الأفراد على النحو التالي:

- منع التوظيف المؤقت نهائيا و مراعاة إجراءات إنهاء خدمة الموظف بطلب تسليم كل ما كان بحوزته كالمفاتيح و البطاقات الممغنطة و تغيير كلمة المرور قبل مغادرته؛
- متابعة العاملين و نقلهم إجباريا بين الأقسام المختلفة في الإدارة و ملاحظة الذين لا يطلبون إجازة بإجبارهم على الإجازة ومراقبة النظام بعد ذلك للتأكد من عدم وجود خلل كانوا يتفادونه بوجودهم؛
- عقد ندوات ومؤتمرات ومحاضرات بشكل دوري في مجال أمن المعلومات وعرض النشرات الداخلية وتعليمات الإدارة التي تتضمن اطلاع الأفراد على المعلومات المهمة في مجال الأمن لإلزام العاملين بالنظم الإدارية المحددة؛
- دفع العاملين لحضور المعارض العالمية للأجهزة والبرامج، وإرسالهم إلى الدورات المتخصصة بأمن المعلومات ليكون لديهم خلفية قوية بما يكفل تحقيق أمن المعلومات؛
- منح الحوافز وربط الترقية والدورات بمدى التقيد بأمن المعلومات؛

- **توفير قسم متخصص بأمن المعلومات:** تقوم المؤسسة الكبيرة بتعيين مدير أمن نظم المعلومات يرتبط بالإدارة العليا مباشرة لأهمية التقارير الاي يعدها ويرأس مدير الأمن قسما مستقلا من المتخصصين في مجال أمن المعلومات ومن ذوي الخبرة الفنية والأمنية في معالجة البيانات والبرمجة حسب نظم التشغيل ولغات البرمجة وقواعد البيانات المستخدمة في المؤسسة، ومدربين على التنسيق الأمني ولديهم المقدرة الكافية للتعامل مع جرائم نظم المعلومات والحالات الطارئة.

4.4 الآليات المؤسساتية لمكافحة التقليد والقرصنة:

إن الحماية الداخلية للملكية الفكرية عن طريق سن قوانين وعقوبات قد تكون غير كافية، لذلك لابد من إنشاء أجهزة للرقابة وذلك لضمان حماية فعالة. ونظرا للأهمية البالغة التي تكتسيها الملكية الفكرية فلقد سعت معظم الدول إلى إنشاء مؤسسات ومراكز وطنية متخصصة لتوفير حماية الحقوق ودعم القدرات الابتكارية والإبداعية ورغم اختلاف التسميات التي منحت لهذه المؤسسات بحسب التشريعات الوطنية إلى أن هدفها واحد و هو ترقية الملكية الفكرية. ولقد اهتمت الجزائر بالملكية الفكرية عن طريق إنشاء"المكتب الوطني للملكية الصناعية" ONPI بمقتضى المرسوم رقم 63-248 وكانت صلاحياته تتمثل في الملكية الصناعية والتجارية وكا ما يتعلق بالسجل التجاري ثم أنشئ" المعهد الجزائري للتوحيد الصناعي والملكية الصناعية" بمقتضى أمر 73-62 و لقد حل محل هذا المعهد " المعهد الوطني الجزائري للملكية الصناعية" بمرسوم تنفيذي 98-68 واعتبار هذا الأخير الهيئة المكلفة بكافة عناصر الملكية الصناعية. وفي مجال الملكية الأدبية و الفنية فلقد تم إنشاء " الديوان الوطني لحق المؤلف " بمقتضى أمر 73-46 غير أن مهامه كانت محدودة و ناقصة فأنشئ بذلك " الديوان الوطني لحقوق المؤلف والحقوق المجاورة" بمقتضى مرسوم تنفيذي 98-366 حيث أضيفت لصلاحياته حماية حقوق الفنانين والمؤلفين بعد أن كانت مقتصرة على المؤلفين فقط، والملاحظ أن هاتين الهيئتين لا تعدان الوحيدتين لحماية الملكية الفكرية على المستوى الوطني، بل توجد إلى جانبهما هيئات أخرى لا

تقل أهمية عنهما وهي: إدارة الجمارك ومصلحة مراقبة الجودة وقمع الغش (زواني، 2022، ص70).

5.4 الإجراءات المتخذة على المستوى العربي والعالمي لمكافحة جرائم الانترنت والحاسوب:

سنت عدد من الدول الأوروبية قوانين خاصة بجرائم الانترنت والحاسوب مثل بريطانيا وهولندا وفرنسا والدنمارك والمجر وبولندا واليابان وكندا، كما اهتمت البلدان الغربية بإنشاء أقسام خاصة بمكافحة جرائم الانترنت بل إنها خطت خطوة إلى الأمام و ذلك بإنشاء مراكز لاستقبال ضحايا تلك الجرائم. وعلى مستوى الدول العربية لم تقم أي دولة عربية بسن قوانين خاصة بجرائم الحاسب الآلي والانترنت، ففي مصر مثلا لا يوجد نظام قانوني خاص بجرائم المعلومات إلا أن القانون المصري يجتهد بتطبيق القانون الجنائي التقليدي على الجرائم المعلوماتية و التي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية ة اتخاذ إجراءات فورية اتجاه المخالفين في المواقع الالكترونية ويتم تدميرها إذا ثبت إضرارها بمصلحة الأمن القومي أو الآداب العامة .وشهدت فعاليات المؤتمر الإقليمي الأول حول الجريمة الالكترونية " تحديات تكنولوجيا المعلومات والتنمية الاقتصادية " العديد من المطالب، دعا عدد من رجال القانون والقضاة وأعضاء النيتبة العامة والمتخصصين في مجال الجريمة الالكترونية إلى ضرورة وضع تشريعات وقوانين تعاقب مرتكبي جرائم الانترنت والمعلومات والبيانات على شبكة المعلومات الدولية وتطوير التشريعات الموجودة حاليا بما يواكب التطور العلمي والتكنولوجي بما يكفل حقوق المواطنين المستخدمين شبكة المعلومات الدولية وتحدد واجباتهم. وإن التأثير المجتمعي الذي يحدثه التقدم التكنولوجي يحتاج إلى تنظيم قانوني يضع إطارا للعلاقات التي تترتب على استخدامه بما يكفل حماية الحقوق المترتبة على هذا الاستعمال، ويحدد الواجبات اتجاهها فلابد للتقدم العلمي والتكنولوجي أن يواكبه تكيف في القواعد القانونية إذ لا يجوز للقانون أن يقف صامتا مكتوف الأيدي حيال أساليب انتشار هذا التقدم و حيال القيم التي يروجها. ولا يقف دور

القانون على مجرد تنظيم العلاقات المترتبة على التقدم التكنولوجي بل إنه يجب أن يحمي القيم التي تحيط باستخدام التكنولوجيا، ويحدد المسار الصحيح الذي يجب أن يسلكه التقدم التكنولوجي حتى لا يتخذه المجرمون أداة لتطوير وسائل إجرامهم بل يكون على العكس من ذلك وسيلة لمحاربة هذا الإجرام وهو ما يوجب على القانون أن تمتد نصوصه إلى الأنشطة الجديدة التي تفرزها التكنولوجيا حتى تحدد الجريمة في نصوص منضبطة واضحة ولا يترك بحثها إلى نصوص قانون العقوبات التقليدي التي قد تتسم بعدم اليقين القانوني أو لا تتسع لملاحقة الأنماط الجديدة من الإجرام. وقد تتجاوز نتائج هذه الجرائم إلى وقوع جرائم اخرى تهدد الحق في الحياة و السلامة البدينة إذا ما أدى العبث في المعلومات على تغيير طريق العلاج أو تركيبة الدواء. وقد تؤثر على نطاق الخدمات الالكترونية وقطاعات التنمية الاقتصادية وتكنولوجيا المعلومات، الأمر الذي يتطلب إعادة هيكلة قطاع الاتصال، وتدعيم دور الدولة في حماية المستخدمين تكنولوجيا الاتصالات من خلال إجراءات تتميز بالشفافية الكاملة، خاصة أننا نواجه تحديات جديدة بما يعرف بالجريمة الالكترونية التي يجب مكافحتها لتشجيع الاستثمار وحماية حقوق الملكية الفكرية، الأمر الذي يستلزم ألا يتم بمعزل الثوابت التشريعية والقانونية. و إن التقدم التكنولوجي أفرز أنماطا جديدة من الجريمة و كذا من المجرمين فكان للتقدم في العلوم المختلفة أثره على نوعية الجرائم و استغل المجرم ثمرات هذه العلوم في تطويع المخترعات العلمية الحديثة لخدمة أهدافه الإجرامية، فالمشكلة الرئيسية لا تكمن في استغلال المجرمين الانترنت وإنما في عجز أجهزة العدالة عن ملاحقتهم وعدم ملاحقة القانون لهم ومسايرة التكنولوجيا الجديدة لتشريعاته (سعدون ، 2011، ص5).

5. خاتمة

من خلال عرضنا لموضوع التدابير الأمنية لحماية المؤسسات الإعلامية من الجريمة الإلكترونية، من خلال طرح الأطر النظرية للجريمة الإلكترونية بدءا بالتعريف القانوني للجريمة الالكترونية، والخصائص والدوافع التي أدت إلى ارتكاب مثل هذه الجرائم، ولحماية هاته المؤسسات لا بد من توفير الأمن

المعلوماتي ووضع التدابير الأمنية للحماية من الجريمة الإلكترونية، إضافة إلى ذلك توفير الحلول العملية فيما يتعلق ببعض الإجراءات المتطلبة لمكافحة مثل هاته الجرائم، باستعمال الجدار الناري، وتوفير الإجراءات والتدابير الإدارية الواجب اتخاذها لحماية المعلومات الحكومية، إضافة إلى ذلك وضع الآليات المؤسساتية لمكافحة التقليد والقرصنة، مع ضرورة إعداد الإجراءات اللازمة على المستوى العربي والعالمي لمكافحة جرائم الانترنت والحاسوب.

نتائج البحث:

- ضعف البنية التحتية حيث أنها لا تواكب سرعة تدفق النت دوليا وتعد من أضعف السرعات على مستوى العالم، مما يعرقل نقل المعلومات بالشكل الملائم؛
- عدم مواكبة الإجراءات القانونية لتطورات الجريمة الإلكترونية، حيث أنها تفتقر إلى سن قوانين تتماشى مع طبيعة الجرائم الحديثة، إذ وجب صياغة قوانين تستجيب لصفة الردع بالنسبة لمرتكبي هذه الجريمة؛
- سهولة استهداف المعلومات (المؤسساتية والحكومية)، إذ ان عمليات اختراق أنظمة المعلومات يرجع لعدة عوامل منها عدم توفير أجهزة تقنية ذات التدفق العالي من ناحية، ومن ناحية أخرى عدم الجدية في إنشاء خلايا للأمن المعلوماتي داخل هاته المؤسسات.

التوصيات:

- سن التشريعات القانونية التي تحافظ على أمن المعلومات بما يحفظ هاته الأخيرة من أي تهديد خارجي، مما يوجب تفعيل استراتيجيات إدارية أكثر فاعلية؛
- تفعيل الاتفاقيات الدولية لمكافحة الجريمة الإلكترونية؛

- وضع استراتيجية لتحديث الأجهزة داخل المؤسسة أكثر فاعلية سواء من حيث الحواسيب أو من حيث البرامج الحمائية؛
- تطوير البنية التحتية من خلال تطوير أنظمة الاتصال من الكابلات العادية إلى كابلات الألياف الزجاجية.

آفاق البحث:

- أنظمة الحماية الإلكترونية بين الواقع والمأمول؛
- تطور الجرائم الإلكترونية في الدول العربية؛
- القرصنة الإلكترونية في المجتمع الدولي؛
- الاتفاقيات الدولية لمكافحة القرصنة الإلكترونية.

6. قائمة المراجع:

الكتب:

1. سلام منعم زامل، الاتجاهات الحديثة في إدارة المؤسسات الصحفية، دار نور للنشر، الطبعة الأولى، 2017.

المذكرات:

2. عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية – دراسة مقارنة-، مذكرة مقدمة ضمن متطلبات نيل شهادة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014.

المجلات:

3. بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، سبتمبر 2018.

4. سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن، ألجريمة ألالكترونية عبر الانترنيت أثرها وسبل مواجهتها، تاريخ النشر 5/4/ 2011.

5. غدير برنس الزبن، عبد الكريم عوده الله الخرابشة، الجرائم الإلكترونية ومستوى الوعي بخطورتها دراسة ميدانية على عينة من الشباب الجامعي الأردني، مجلة الجامعة الإسلامية للدراسات الانسانية، 2020.

6. فريدة حمودي، الأمن المعلوماتي في الجزائر بين التطورات التكنولوجية وضعف البيئة الرقمية، المجال المصرفي نموذجا" دراسة قانونية"، مجلة جيل، الأبحاث القانونية المعمقة، مجلة علمية دولية محكمة تصدر دوريا عن مركز جيل البحث العلمي، العام الخامس - العدد - 41 يوليو2020 .

7. ياسر محمد عبد السلام رجب، التطورات التشريعية المستحدثة في مجال الأمن المعلوماتي- دراسة مقارنة، المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والعلوم والآداب، مصر، 2021.

المطبوعات:

8. زواني نادية، محاضرات في مكافحة التقليد والقرصنة: مطبوعة مقدمة لطلبة الماستر تخصص الملكية الفكرية، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر 1، 2022.

9. قادة بن عبد الله عائشة، محاضرات في مقياس الأمن الوطني الجزائري، قسم العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد تلمسان، الجزائر، 2020-2021.

بحوث علمية:

10. سلمى عبد الرحمن الدوسري، جبريل حسن محمد العريشي، دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع، جامعة الأميرة نورة بنت عبد الرحمان.

11. قدايفة أمينة، استراتيجية أمن المعلومات.

12. مكتب الأمم المتحدة المعني بالمخدرات والجريمة فيينا، دراسة شاملة عن الجريمة، الأمم المتحدة، نيويورك، 2013.

13. يحياوي محمد، مخاطر القرصنة المعلوماتية على الحكومة الالكترونية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة البويرة، الجزائر.