



جامعة أحمد درايعية - أدرار
كلية العلوم الإنسانية والاجتماعية
والعلوم الإسلامية
قسم العلوم الانسانية



مذكرة بعنوان:

دور الإعلام الرقمي في الحد من الجرائم السيبرانية
موقعي "الشروق" و"أخبار الوطن" أونلاين أنموذجا

مقدمة لنيل شهادة الماستر في علوم الإعلام والاتصال
تخصص صحافة مطبوعة وإلكترونية

إشراف البروفيسور:
مشاور صيفي

إعداد الطالبتين:
• باحمد نعيمة
• الطيبي أمينة

لجنة المناقشة

الاسم واللقب	الصفة
الدكتور كعواش عبدالرحمن	رئيسا
البروفيسور مشاور صيفي	مشرفا ومقررا
الدكتور سباعي أحمد	عضوا ومناقشا

السنة الجامعية: 1443-1444 هـ / 2022-2023



إذن بالطبع والإيداع

أنا الأستاذ (ة): أ. د. مستشار حسيبي
المشرف مذكرة تالمستر الموسومة: "دراسة في عدم الرقعة الحمراء من الجرائم السيبرانية
موقعها" السروقة لمرأ خبار الوطن - أ. د. مكيون أمور زجا

من إنجاز الطالب (ة): س. أحمد نجيدة

و الطالب (ة): الطيب أمنة

كلية: العلوم الإنسانية والاجتماعية والعلوم الإسلامية

القسم: العلوم الإنسانية

التخصص: صحافة مكتوبة وكتر ميديا

تاريخ المناقشة: 2023 / 06 / 04

أشهد أن الطلبة قد قاموا بالتدريبات والتصحيفات المطلوبة من طرف لجنة التقييم / المناقشة، وعليه أُرخص لهم بطبع
المذكرة وإيداعها بالمكتبة المركزية للجامعة.

- إمام المشرف:

أ. د. حسيبي

آدرار في: 2023 / 06 / 18

مساعد رئيس القسم:

مساعد رئيس قسم العلوم الإنسانية
مكلف بمهام التدريس والبحث العلمي

د. بابا عبد الله

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

شكر وتقدير

ونتقدم بالشكر الجزيل "للبروفيسور" مشاور صيفي" الذي رافقنا طيلة هذا البحث وأمدنا بالمعلومات والنصائح القيمة، و التوجيهات السديدة ، و دعمه الكبير لنا لإتمام هذا العمل و إخراجہ في حلتہ الأخيرة؛ فله فائق التقدير والإحترام ، راجين من الله أن يسدد خطاه ويحقق مناه فجزاه الله عنا كل خير .

كما نشكر أعضاء لجنة المناقشة لقبولهم مناقشة هذا العمل. كما نتقدم بجزيل الشكر والعرفان للسيد: "رياض هويلي" المدير التنفيذي مسؤول النشر بشبكة "أخبار الوطن" على مساعدته القيمة لنا.

إهداء

الحمد لله الذي بنعمته تتم الصالحات والذي وهبنا هذا التوفيق والسداد ومنحنا الثبات
واعاننا على إتمام هذا العمل فها هي ثمار جهدنا قد أينعت وحن قطافها ...إنها لحظة
تخرجي ولأنكم إحدى أركانها فلإني اهدي هذا العمل المتواضع الى أمي وأبي الغاليين
حفظهما الرحمان وأطال في عمرهما شكرا على كل ما بذلتموه من تضحيات وجهود
لتربيتي وتعليمي إنما أنا اليوم بسببكم أنتم إن كلمات دعائي وشكري لا توافيكم
حقكم ومنزلتكم وقدركم فأترك الأمر لتقدير العليم الحكيم ليقدم لكما ما يسر
قلوبكما في الدنيا والآخرة والى من تربيت معهم سندي في هذه الحياة إخوتي كل واحد باسمه .
وإلى زميلتي بالدراسة أمنة الطيبي.
وأخيراً لا يفوتنا أن نعبر عن بالغ تحياتنا الى كل من ساعدنا من قريب او من بعيد في
إنجاز هذا البحث واسأل الله عز وجل ان يوفقنا لما يحب ويرضى .

باحمد نعيمة



إهداء

الحمد لله والشكر لله الذي أنار لي طريقي وكان لي خير عوناً، بفضل الله أتممت اليوم مرحلة الماستر ، ورفعت قبعتي مودعاً للسنين التي مضت أهدي تخرجي وثمره تعي إلى أمي وأبي يا من أحمل اسمكما بكل افتخار إليكما يا قدوتي ونبراسي الذي ينير دربي إليكما يا من أعطيتموني ولا زال عطاؤكما بلا حدود فمهما وصفت فيكم أو عبرت عن مشاعري فلم أوفى حقكم فأنتم رحمة الله لي في هذه الحياه يا من أدين لكم بحياتي إلى من أحبها الى نبض قلبي إلى من تستقبلني بابتسامه وتودعني بدعوة ”أمي الغالية_الحاجة سولة“ أسأل الله أن يحفظها لي، وإلى حبيبي و أماني وحزام ظهري وسر وجودي ”أبي الغالي الحاج إسماعيل“ وإلى رفيق دربي زوجي عيسى وإلى ملاذ حياتي إبني حبيبي طه ، وإليكم يا سندي و رزاح ظهري إخوتي وأخوتي وإلى من ساندوني ووقفوا معي وإلى رفيقي بالمشوار الدراسي باخذ نعيمة إلى من كل أحببتهم عائلتي و أصدقائي وإلى كل الأساتذة الذين قدموا يد المساعدة وإلى كل من ساندنا وبالنصح دعمنا وإلى الخير أرشدنا ، وأسأل الله عز وجل أن يوفقنا الى ما يحبه ويرضاه.

الطبي أمنة

خطة الدراسة

مقدمة

الفصل الأول :الإطار المفاهيمي للدراسة

المبحث الأول : مفهوم الإعلام الرقمي

المطلب الثاني : أنواع ووسائل الإعلام الرقمي

المطلب الثالث : وظائف وأهمية الإعلام الرقمي

المبحث الثاني : مفهوم الجرائم السيبرانية

المطلب الأول : تعريف الجرائم السيبرانية وخصائصها

المطلب الثاني : أسباب الجرائم السيبرانية

المطلب الثالث : طرق وأشكال الجرائم السيبرانية

المبحث الثالث : المجرم السيبراني

المطلب الأول : تعريف المجرم السيبراني وسماته

المطلب الثاني : فئات المجرم السيبراني

المطلب الثالث : أدوات وأساليب المجرم السيبراني

الفصل الثاني : أهمية الإعلام في الحد من الجرائم السيبرانية

المبحث الأول : دور التشريعات في الحد من الجرائم السيبرانية

المطلب الأول : تشريعات الجرائم السيبرانية في الجزائر

المطلب الثاني : تشريعات الجرائم السيبرانية في بعض الدول العربية والغربية

المطلب الثالث : الاتفاقيات الإقليمية في الجريمة السيبرانية

المبحث الثاني : أهمية الإعلام الرقمي في الحد من الجرائم السيبرانية

المطلب الأول : الوعي بالجريمة السيبرانية

المطلب الثاني : حماية خصوصية مستخدم الشبكات الاجتماعية

المطلب الثالث : معوقات الإعلام الرقمي في الحد من الجرائم السيبرانية

المطلب الأول : مخاطر التطور التكنولوجي

المطلب الثاني : ضعف التنسيق والتعاون الدولي لمكافحة الجريمة السيبرانية

المطلب الثالث : صعوبة الإثبات بالدليل الرقمي

الفصل الثالث : دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم

السيبرانية

المبحث الأول : دور موقع الشروق أونلاين في الحد من الجرائم السيبرانية

المطلب الأول : نبذة تعريفية لموقع الشروق أونلاين

المطلب الثاني : أهداف موقع الشروق أونلاين

المطلب الثالث : دور موقع الشروق أونلاين في الحد من الجرائم السيبرانية

المبحث الثاني : دور موقع أخبار الوطن أونلاين في الحد من الجرائم السيبرانية

المطلب الأول : نبذة تعريفية لموقع أخبار الوطن أونلاين

المطلب الثاني : أهداف موقع أخبار الوطن أونلاين

المطلب الثالث : دور موقع أخبار الوطن أونلاين في الحد من الجرائم السيبرانية

الخاتمة

مقدمة

مقدمة:

إن ظهور الإعلام الرقمي وماتج عنه من تحولات واستحداثات في عصر المعلومات شكل تغييرا في طريقة حياة المجتمع، من حيث التعليم والترفيه وطريقة التعامل وتفاعل الناس مع بعضهم البعض، ذلك أن الإعلام الرقمي يعتمد على التقنيات الجديدة الرقمية وعلى التفاعل بين التكنولوجيا والصور والصوت ، وهذا ما يجعل وسائل الإعلام الرقمي تتغير باستمرار مع تطور التكنولوجيا الجديدة، ويعتبر دور الإعلام الرقمي جزءاً مهماً في زيادة الوعي بالجرائم السيبرانية حيث لديه القدرة على إعلام وتنقيف وتنبه الأفراد والمجتمعات من خطورة الجرائم السيبرانية، فعلى الرغم من التطور التكنولوجي والمعلوماتي الذي صاحب الإعلام الرقمي إلا أنه من خلال استخدام التقنيات الحديثة بات ارتكاب الجرائم الالكترونية أكثر انتشارا وتفاقما خصوصا وأن العالم يشهد اليوم نقلة نوعية في مجال المعاملات السيبرانية.

حيث عرفت الفترة الأخيرة تطورا إلكترونيا مذهلا رافقه تداخل وتباين المعاملات الاقتصادية والاجتماعية والتجارية والإدارية ، وهذا يعني أن العالم قد تغير من نمط مساحة مغلقة إلى نمط مساحة مفتوحة في كل المجالات وعلى كل المستويات، وتعتبر الجرائم السيبرانية من أهم الاهتمامات التي باتت تطارد المواطن في حياته الشخصية والدول في سيادتها وأمنها ، بالنظر إلى التطور التكنولوجي والرقمي الهائل وما صاحبه من تأثير على كل المستويات أثر بشكل أو بآخر على أمن واستقرار الشعوب من جهة والمساس بحرمة وخصوصية المواطن من جهة أخرى، بل وأصبحت تداعيات هذه الثورة التكنولوجية هاجساً يهدد أمن واستقرار الدول والمواطن على حد سواء، ولذا تسعى هذه الدراسة للكشف عن دور الإعلام الرقمي في الوقاية من الجريمة السيبرانية من خلال مجابهة الفكر الإجرامي وتوعية أفراد المجتمع ضد الجريمة السيبرانية .

➤ إشكالية الدراسة:

يتبلور دور وسلطة وسائل الإعلام عامة والإعلام الرقمي خاصة في التأثير المباشر على أفكار وسلوكيات الأفراد والمجتمعات، بما في ذلك أمنهم وسلامتهم، خصوصا في مجال ارتفاع معدلات الجرائم الالكترونية ؛ حيث أضحي الناس يدمنون شبكة الأنترنت حتى أصبحت جزءا لا يتجزأ من حياتهم اليومية، ونتيجة لهذا فقد خلق الإعلام الرقمي مشاكل لا متناهية ؛ فعلى الرغم من إيجابيات

التطور التكنولوجي والرقمي إلا أنه بالمقابل شكلت مجموعة من السلبيات أهمها ما يعرف بالجرائم السيبرانية .

ويتجلى دور الإعلام الرقمي في توعية أفراد المجتمع ،وتعزيز الوعي الأمني المعلوماتي لديهم، ليكون الفرد قادراً على تحصين نفسه ضد أي خطر أو فكر إجرامي إلكتروني وانطلاقاً من فعالية وسائل الإعلام الرقمي في التأثير على الأمن المعلوماتي تتمحور إشكالية الدراسة في السؤال الرئيسي التالي :

كيف يساهم الإعلام الرقمي في الحد من الجرائم السيبرانية ؟

➤ الأسئلة الفرعية :

- و تتفرع عن هذه الإشكالية التساؤلات الفرعية التالية:
- ✓ ما المقصود بالإعلام الرقمي و الجرائم السيبرانية؟
- ✓ هل للإعلام الرقمي دور فعال في الحد من انتشار الجرائم السيبرانية ؟
- ✓ كيف تساهم مؤسستي الشروق وأخبار الوطن أونلاين في توعية الأفراد بمخاطر الجرائم السيبرانية؟

➤ فرضيات الدراسة:

- للإجابة على الأسئلة نقدم الفرضيات التالية:
- ✓ للإعلام الرقمي دور مهم و فعّال في الحد من الجرائم السيبرانية .
- ✓ للإعلام الرقمي استراتيجيات وقائية في مكافحة الجرائم السيبرانية .
- ✓ تلعب مؤسستي الشروق وأخبار الوطن أونلاين دوراً توعوياً فعّالاً في الحد من مخاطر الجرائم السيبرانية.

➤ أهمية الدراسة :

إن أهمية الدراسة من أهمية الموضوع الذي تعالجه وما يمكن أن تقدمه من فوائد، ومع ظهور الإعلام الرقمي والتطورات المصاحبة له، ونظراً لأهمية خصوصية الأفراد ومعلوماتهم الشخصية التي تحتاج من طرف مجرمين في الفضاء السيبراني نسعى إلى تقديم نظرة شاملة عن دور وأهمية الإعلام الرقمي في الوقاية والحماية للحد من الجرائم السيبرانية والتهديدات الناجمة عنها، وأهم

الطرق والسبل المتبعة لمكافحة هذه الجرائم، وتتجلى أهمية دراستنا في المساهمة القيمة لموقعي الشروق وأخبار الوطن أونلاين في نشر الوعي لمواجهة الجرائم والتهديدات السيبرانية .

➤ أهداف الدراسة:

تسعى هذه الدراسة إلى التعرف على دور الإعلام الرقمي في الحد من انتشار وتفاقم الجرائم السيبرانية، من خلال التعرف على مفهوم الإعلام الرقمي ومدى نجاعة مؤسستي الشروق وأخبار الوطن أونلاين في توعية المواطنين حول مخاطر الجرائم السيبرانية، بالإضافة إلى إبراز :

- الخصائص والمميزات التي يحظى بها الإعلام الرقمي في معالجة الجرائم السيبرانية.
- الأهمية التي يختص بها الإعلام الرقمي في الوقاية من الجرائم السيبرانية .
- التعرف على الدور الذي يلعبه الإعلام الرقمي للحماية والحد من ارتفاع معدلات الجرائم السيبرانية .

- الكشف عن طرق الإعلام الرقمي في الحد من انتشار الجرائم السيبرانية .
- المعوقات التي تحد من فعالية الإعلام الرقمي في الوقاية والحد من الجرائم السيبرانية.

➤ **دوافع اختيار الموضوع :** يرجع اختيار الموضوع إلى أسباب موضوعية وأخرى ذاتية نذكر منها:

➤ الدوافع الموضوعية :

- أهمية الموضوع ،والوقوف على الدور الذي يلعبه الإعلام الرقمي في الحد من الجرائم السيبرانية.
- انتشار واستفحال ظاهرة الجرائم السيبرانية في الآونة الأخيرة.
- جدية وخطورة الموضوع تستحق الدراسة والبحث في حيثياتها.

➤ الدوافع الذاتية :

- الرغبة الشخصية في البحث في مثل هذه المواضيع باعتباره موضوعا حساسا .
- كون الموضوع يصب في مجال دراستنا ،وله علاقة بتخصص علوم الإعلام والاتصال ومؤسستي الشروق وأخبار الوطن أونلاين تتناسب وموضوع الدراسة،باعتبارها مؤسسات رقمية ذات صلة بالموضوع .
- الفضول العلمي وحب الاستكشاف والاطّلاع على مواضيع الساعة.

➤ حدود الدراسة: تتضح حدود الدراسة فيما يلي :

- **الحدود المكانية:** أجريت الدراسة على مؤسستي الشروق وأخبار الوطن أونلاين الجزائريتين، باعتبارهما مؤسستين رقميتين تسعى إلى توعية وتنوير وإرشاد القراء والمواطنين، بكل ما يخص الجرائم السيبرانية و كل ما يطرأ عليها من جديد.

- **الحدود الزمانية:** أجريت دراستنا على مجموعة مقالات من مؤسسة الشروق وأخبار الوطن أونلاين الجزائريتين، فقد اخترنا الفترة الزمنية للمقالات التي تقوم عليها الدراسة من سنة 2020 إلى يومنا هذا ماي 2023، وقد اعتمدنا هذه الفترة لتزايد الاهتمام بالمواضيع المتعلقة بالجرائم السيبرانية.

الإطار المنهجي للدراسة

منهج الدراسة :

➤ منهج الدراسة :

اعتمدنا في دراستنا على المنهج الوصفي التحليلي؛ باعتباره المنهج الأنسب لخدمة هذا البحث؛ حيث نقوم بوصف الظاهرة و تحليلها التحليل الدقيق و المناسب؛ خاصة و أنه يتناسب بشكل واضح مع موضوع دراستنا، كما أعتمدنا على المنهج الإحصائي في دراستنا لنموذجي الشروق و أخبار الوطن أونلاين الجزائريتين.

➤ أداة جمع البيانات .

اعتمدنا في دراستنا على أداة تحليل مضمون موقعي الشروق وأخبار الوطن أونلاين الجزائريتين، فمن خلال هذه الأداة تعرفنا على مضمون الموقعين وكيف تناولوا موضوع الجرائم السيبرانية وتهديداتها من خلال القيام بدراسة تحليلية لمضمون مجموعة من المقالات والفيديوهات وفق فترة زمنية مبررة، حيث ساعدتنا في الوصول إلى نتائج علمية دقيقة من خلال نتائج علمية دقيقة من خلال المعلومات التي جمعناها لإثراء بحثنا العلمي .

➤ عينة الدراسة :

اعتمدنا في دراستنا على عينة من المقالات من موقعي الشروق وأخبار الوطن أونلاين للقيام بالدراسة عليها وتحليلها، وكان اختيارنا لهذه العينة معايير علمية دقيقة بهدف الوصول إلى

نتائج حقيقية لإثراء الرصيد المعرفي للقراء، فقد اعتمدنا على كل المقالات التي تناولت موضوع الجرائم السيبرانية في الفترة من 2020 إلى يومنا هذا (ماي 2023).

➤ تبرير خطة الدراسة:

لمعالجة هذا الموضوع ودراسته من مختلف الجوانب، قسمناه إلى ثلاثة فصول، في الفصل الأول تناولنا المفاهيم العامة حول الإعلام الرقمي والجرائم السيبرانية، قسمناه إلى ثلاثة مباحث، المبحث الأول تطرقنا فيه إلى تعريف الإعلام الرقمي وخصائصه وأنواعه وأهدافه، بينما تضمن المبحث الثاني تعريف الجرائم السيبرانية وخصائصها، أسبابها وتداعياتها وطرق وأشكاله، وبالنسبة للمبحث الثالث تحدثنا فيه عن الجرم السيبراني تعريفه وسماته وأصنافه وأدواته.

أما الفصل الثاني فقد خصص لأهمية الإعلام الرقمي في الحد من الجرائم السيبرانية وقد قسم هو الآخر إلى ثلاثة مباحث، المبحث الأول تضمن دور التشريعات في الحد من الجرائم السيبرانية والمبحث الثاني أهمية الإعلام الرقمي في الحد من الجرائم السيبرانية والمبحث الأخير أهم المعوقات التي تواجه الإعلام الرقمي في الحد من الجرائم السيبرانية.

و في الفصل الثالث عرضنا من خلاله دور مؤسستي الشروق وأخبار الوطن أونلاين الجزائيتين، في توعية الأفراد و المجتمع و المؤسسات، بمخاطر الجرائم السيبرانية وطرق الوقاية منها.

➤ الدراسات السابقة:

من خلال دراستنا لحثيات الموضوع والبحث فيه توصلنا لمجموعة من الدراسات السابقة التي تناولت الإعلام الرقمي والجرائم السيبرانية نذكر منها :

- الدراسة الأولى: سلطان مطلق ناصر أبو ثنين السبيعي، دور الإعلام الرقمي في الحد من الجرائم السيبرانية في المملكة العربية السعودية، الرياض 2020 .

ناقش الباحث موضوع الإعلام الرقمي والجرائم السيبرانية وسبل الإعلام الرقمي في الحد من هاته الجرائم .

فقد تطرق الباحث من خلال دراسته في القسم الأول إلى الإعلام الرقمي مفهومه أدواته وخصائصه وعناصره ونظرياته، أما القسم الثاني فقد خصصه للجرائم السيبرانية ماهيتها وخصائصها

ودور الاتحاد السعودي للأمن السيبراني والبرمجة، بينما القسم الثالث اختص بعرض وتحليل بيانات الدراسة ومناقشة نتائجها¹.

- الدراسة الثانية: جابري سارة، الإعلام الجديد.. دراسة في المداخل والتأثيرات في ظل الألفية الثالثة .

هدفت الباحثة من خلال هذه الدراسة إلى تسليط الضوء على الإعلام الجديد والتأثيرات المصاحبة له، حيث أثار هذا الأخير ضجة كبيرة وأحدث تغيرات كثيرة في الساحة الإعلامية على المستويين الإصطلاحي والتأثيري، ذاكرة الأشكال المختلفة والمتنوعة. بالإضافة إلى ضبط المفاهيم والمصطلحات الخاصة بالإعلام الجديد والتطرق إلى الآثار المترتبة عن استخدام وسائل الإعلام الجديد².

- الدراسة الثالثة: مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، دراسة شاملة عن الجريمة السيبرانية ، مسودة - شباط/فبراير، 2013 .

تناولت الدراسة 8 فصول ، كل فصل يعالج جانب من جوانب الجرائم السيبرانية فالفصل الأول عن الموصولية والجريمة السيبرانية ،الفصل الثاني الصورة العالمية والفصل الثالث حول التشريع وأطر العمل ، رابع فصل ناقش استعراض عام للتجريم ، الفصل الخامس تضمن إنفاذ القانون والتحقيقات، سادس فصل يحتوي على الأدلة الإلكترونية والعدالة الجنائية أما الفصل السابع التعاون الدولي بينما الفصل الثامن والأخير سبل منع الجريمة السيبرانية³.

¹ سلطان مطلق ناصر أبو ثنين السبيعي ، دور الإعلام الرقمي في الحد من الجرائم السيبرانية في المملكة العربية السعودية، مذكرة مكملة لنيل شهادة الماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2020 .

² جابري سارة ، "الإعلام الجديد دراسة في المداخل والتأثيرات في ظل الألفية الثالثة"، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 03، العدد 02، جامعة العربي التبسي، تبسة، جوان 2020 .

³ الأمم المتحدة، دراسة شاملة عن الجريمة السيبرانية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فبراير 2013 .

➤ صعوبات البحث :

لا يخلُ أي بحث من بعض الصعوبات ومن بين أهم الصعوبات التي واجهتنا أثناء انجاز هذا البحث:

- صعوبة الحصول على المراجع التي تحدثت عن الإعلام الرقمي والجرائم السيبرانية على حد سواء على مستوى مكاتب ولاية أدرار، أما رقميا لم تتمكن من العثور على جل المراجع المطلوبة .
- مدة إعداد الرسالة غير كافية بتاتا لإنجاز دراسة مفصلة وشاملة مما وضعنا تحت ضغط شديد .

➤ مصطلحات أكثر تداولاً في الدراسة :

(1) **الإعلام الرقمي** : هو الإعلام الإلكتروني الحديث الذي جاء بديلا عن الإعلام الورقي، يعتمد الإعلام الرقمي على الوسائط المختلفة التي تستخدم الأجهزة التكنولوجية، ويعتبر هذا الأخير الإعلام الذي يستخدم كافة الوسائل الاتصالية المتاحة للوصول إلى الأجهزة أينما كان وكيفما يريد¹ .

(2) **الجريمة السيبرانية** : أو الجريمة الإلكترونية وهي جميع الأنشطة الغير قانونية التي تنفذ باستخدام التكنولوجيا (كالاحتيال الإلكتروني والاختراق... إلخ)

(3) مفهوم التهديدات السيبرانية:

"هناك من يعرف التهديد السيبراني على أنه هو برنامج مضر مصدره الفضاء الإلكتروني يسعى إلى المساس بأمن الحاسبات الآلية والهواتف الذكية والأجهزة اللوحية وشبكات المعلومات وغيرها من الأشياء المتصلة بالإنترنت² .

(4) المفهوم الإجرائي للتهديدات السيبرانية :

هي تلك الجرائم والهجمات الإلكترونية التي تحدث في الفضاء السيبراني تهدف إلى إختراق البنية المعلوماتية لإشخاص أو المؤسسات وتدميرها.

¹ تسنيم الكفاوي، "تعريف الإعلام الرقمي"، من موقع : www.mawdoo3.com، بتاريخ 29 ماي 2023 علي الساعة 18:20.

² ساعد بوقرص، "الأمن السيبراني": مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة"، مجلة الأبحاث في الحماية الاجتماعية، العدد 01، جامعة العلوم والتكنولوجيا هواري بومدين، 2022، ص 65.

الفصل الأول

مدخل مفاهيمي حول الإعلام الرقمي والجرائم السيبرانية

المبحث الأول: مفهوم الإعلام الرقمي

إن الثورة التكنولوجية الحاصلة في مختلف المجالات والتخصصات عامة والمجال الإعلامي خاصة والتطور الذي صاحبها أسفرت عن ولادة تخصص جديد تحت مسمى الإعلام الرقمي الذي أحدث نقلة نوعية في مجال الإعلام والاتصال .

المطلب الأول: تعريف الإعلام الرقمي وخصائصه

❖ أولاً: تعريف الإعلام الرقمي (Digital Media) :

هو مجموعة من الأساليب والأنشطة الرقمية الجديدة التي تمكننا من إنتاج ونشر المحتوى الإعلامي وتلقيه بمختلف أشكاله من خلال الأجهزة الإلكترونية (الوسائط) المتصلة أو غير متصلة بالإنترنت في عملية تفاعلية بين المرسل والمستقبل¹.

وفي تعريف آخر :

يعرف الإعلام الرقمي بأنه أي وسائل إعلام ترمز وتقرأ بشكل آلي، ويمكن إنتاجه ورؤيته وتوزيعه وإجراء التغييرات عليه وحفظه على الكمبيوتر مثل الصورة الرقمية (digital Imagery)، والفيديو الرقمي (digital video)، وصفحات الويب (Web page)، والويب سايت (Web sites)، وتعد وسائل التواصل الاجتماعي (Social media)، والبيانات وقواعد البيانات (Data an databases)، والصوت الرقمي (Digital audio) مثل ملفات (Mp 3) والكتب الإلكترونية (e-books) كمثال على الإعلام الرقمي وهي تتناقض مع وسائل الإعلام التقليدي مثل الصحافة المطبوعة والأشرطة والأفلام².

ويشترط (جيمس) إتحادها مع الحوسبة الشخصية لكي يتحقق مفهوم الإعلام الرقمي، وهو يستثني التلفزيون الذي يستخدم التقنية الرقمي وكذلك الراديو، ولكنه يعد التلفزيون والراديو الذي ييثر بواسطة الإنترنت جزء من الإعلام الرقمي وهذه الرؤية تتناقض مع ماذهب إليه عدد من الباحثين الذين يعدون الوسائل الإعلامية كافة التي تستخدم التقنية الرقمية تندرج ضمن الإعلام

¹منصور حسام، "الإعلام الرقمي: مفهومه، وسائله، نظرياته"، مجلة بحوث ودراسات في الميديا الجديدة، المجلد 03، العدد 02، 2022، ص 89.

²غالب كاظم جبال الدعيمي، الإعلام الجديد اعتمادية متصاعدة- وسائل متجددة، دار أمجد للنشر والتوزيع، الأردن، 2017، ص 60-61.

الرقمي بما فيها وسائل الإعلام التقليدي ومنها الراديو والتلفزيون اللذين يستخدمون النظم التقنية الرقمية في العملية الإنتاجية للمحتوى الإعلامي.¹

تسميات الإعلام الرقمي :

أطلقت تسميات عدة وكثيرة على مفهوم الإعلام الرقمي وهي كالآتي:

1) الإعلام الجديد (New Media) :

قدم خبراء الإعلام بهذا المجال تعريفات عدة لمفهوم الإعلام تعريفات عدة لمفهوم الإعلام الجديد منطلقين من فهمهم لهذا المصطلح الجديد فبعضهم يعده تطورا ينسجم مع ما آلت إليه الثورة التكنولوجية وآخرون يعدونه أنموذجا لبرامج التلفزيون والراديو التفاعلية التي ظهرت وانتشرت مع بدء حقبة الخمسينيات والستينيات مثل برامج (TalkShow) وأوبرا وصباح الخير اميريكا وغيرها من البرامج، في حين يعده آخرون تعبيراً عن استخدام منصة الإنترنت الناتج عن اندماج وسائل عدة متمثلة بالنص والصورة والصوت، إذ يعرفه قاموس التكنولوجيا الحديثة (High-Tech Dictionary) بأنه اندماج أو تكامل بين أجهزة الكمبيوتر (The integration of computers والشبكات الكمبيوترية (computers networking) والوسائط المتعددة .

2) الإعلام التفاعلي (Interactive media) :

تعرف موسوعة (Investopedia) الإعلام التفاعلي بأنه وسيلة للتواصل تعتمد فيها مخرجات إنتاج البرامج الإعلامية على مدخلات المستخدمين مثل المواقع والألعاب وشبكات التواصل الاجتماعي في حين أن الأفلام وأغلب برامج التلفزيون لا تعد برامج تفاعلية، وتتجسد التفاعلية كسمة عامة في الشبكات التواصل الاجتماعي بشكل مطلق وليس جزئياً كما في التلفزيون والراديو وعلى وفق تعريف هذه الموسوعة فإن استخدام الصور والنصوص والحديث مع الأصدقاء هي إحدى مظاهر التفاعلية ولا بد من أن تقترن بالاستجابة لمضمون ما ينشر وتحقيق الاستجابة لكي ندرجه في مسمى الإعلام التفاعلي.²

¹ غالب كاظم جواد الدعيمي، المرجع السابق، ص 61 .

² المرجع نفسه، ص 61 .

(3) الإعلام الآلي (Media automated) :

ذهب بعض أقسام الإعلام في الجامعات إلى تسمية القسم المختص بدراسة الإعلام الجديد بالإعلام الآلي، لاسيما جامعات الجزائر وأحيانا يدمج مع الأقسام العلمية كما في جامعة بومدين كلية الالكترونك والإعلام الآلي وتتفق هذه مع مدخل كروسي للإعلام الجديد الذي يعد الوسائل كافة ماهي إلا آلات وليس وسائل إعلام وفقا لرؤيته التي ستعرضها لاحقا .

(4) الإعلام الشبكي (Online media) :

جاءت تسميته بالإعلام الشبكي لإمكانية استخدام الشبكة العنكبوتية لنقل الأحداث والقضايا التي تتعلق بالجمهور عن طريق أجهزة الحاسوب والموبايل وعبر تطبيقات متعددة، كما بات بالإمكان مراقبة ما يجري في العالم من البيت أو العمل وتحميل الصور والتواصل مع الآخرين بسهولة ويسر، فضلا عن إمكانية تحميل الأفلام واللقطات التي يرغب الفرد بأن يطلع عليها المستخدمون¹ .

(5) إعلام المعلومات (Information media) :

ويطلق عليه أيضا إعلام المعلومات والتكنولوجيا، ويشير إلى الإفادة القصوى من تكنولوجيا الاتصال في بث المعلومات وإنتاجها وتوزيعها على جمهور واسع وكبير عابر للقومية والجغرافية فضلا عن التواصل مع الآخرين عبر تطبيقات متنوعة وفرتها التكنولوجيا الحديثة وهذه التسمية تنطلق من خاصية تزويد الجمهور بالمعلومات المتنوعة .

(6) الإعلام البديل (Alternative media) :

يرى كريس آتون أن مصطلح الإعلام البديل يشير إلى عدد من المشروعات والممارسات والشبكات التي تعمل في مواجهة الأساليب الشائعة للإعلام، وتسعى في الوقت نفسه لتطوير أشكال مختلفة من الممارسة الإعلامية² .

(7) إعلام المجتمع (Society media) :

¹ غالب كاظم جواد الدعيمي، المرجع السابق، ص.ص. 55- 62 .

² خالد جمال عبده، الإعلام البديل على الانترنت فلسفة جديدة في الاعلام والاتصال، الناشر المكتب العربي للمعارف، ط1، القاهرة، 2016، ص.24.

انطلقت هذه التسمية من مشاركة الأفراد في إنتاج المضمون وصياغته وبثه بواسطة شبكات التواصل الاجتماعي مثل المدونات والفيديو بوك وتويتر واليوتيوب وغرف الدردشة والمنتديات وغيرها من وسائل التواصل الاجتماعي إذ بات متاحا للجمهور امتلاك أدوات إنتاج المضمون الإعلامي عن طريق امتلاك أجهزة متوافرة تعمل بالتقنية الرقمية مثل الكاميرا الرقمية والموبايل الذي يتميز بخواص متعددة وهذه التسمية تقترب كثيرا من الإعلام التفاعلي، وأسهمت التكنولوجيا بظهور ما يعرف بالمواطن الرقمي وهو في الغالب الذي نشأ في زمن التكنولوجيا الرقمية، واعتاد على استخدامها بشكل مفرط لإنجاز متطلبات حياته اليومية وهو يكون متصلا بالشبكة العنكبوتية طوال الوقت عبر أجهزة الموبايل أو الحاسوب وتباین نسبة المواطنين الرقميين من بلد إلى آخر بحسب المستوى المعاشي ودرجة التطور وفي الغالب تزداد النسبة لدى الشباب .

8) الوسائط المتعددة (multimedia) :

تشير هذه التسمية إلى عملية اندماج النص مع الصوت والفيديو والصور مع بعضها لتكون رسالة مفهومة تفاعلية، تسهم في خدمة قطاعات متنوعة اقتصادية وتجارية وإعلامية، وبحلول 2000 دخلت الحقبة الثانية من استخدام التكنولوجيا الرقمية في الوسائط المتعددة لتشمل نواحي الحياة كافة، وساعدت قدرة هذه الأجهزة الدقيقة على تخزين معلومات لاتعد ولا تحصى بتقديم خدمة الجمهور كبيرة للجمهور .

الإعلام الإلكتروني (Electroniccommunication):

يشير هذا المفهوم الواسع الذي نتج عن اندماج التكنولوجيا الحديثة مع منصة الإنترنت إلى وسائل عدة يمكن لها أن تقدم المعلومات والأخبار بشأن الأحداث الجارية إلى قطاعات عريضة من الجمهور بهدف التأثير في معتقداتهم وتحقيق الترفيه والتعليم مثل الصحافة الإلكترونية بأشكالها شتى والمدونات ووسائل التواصل الاجتماعي، وبهذا التعريف فإن مفهوم الإعلام الإلكتروني لا يتعد في معناه عن التسميات الأخرى .

وكان مصطلح الإعلام الإلكتروني في مطلع 1940 يشير إلى الراديو والتلفزيون لتمييزها عن الصحافة المطبوعة بأشكالها شتى إلا أنه وبعد حصول النقلة التكنولوجية في مجال الاتصال استخدام هذا المصطلح للدلالة على معنى آخر غير المعنى السابق¹ .

¹ غالب كاظم جواد الدعيمي، مرجع السابق، ص.ص. 55 - 62 .

9) الوسائط المتشعبة (Hypermedia) :

تد نلسون (Ted nelson) الرائد في التكنولوجيا المعلومات وهو أول من استخدم هذا المصطلح في 1965 بعد أن صاغه من مصطلحي (Hypertext) و (Hypermedia) في 1963 وتعني الوسائط المتشعبة عملية ربط بين النصوص والصور والكرافيك والصوت بواسطة روابط متشعبة، وفي هذه الحالة فهي تتيح للمضمون الإبحار في العالم الافتراضي عن طريق وصلات متشعبة، وتختلف عن الوسائط المتعددة كون إعلام الوسائط ينتج عن عملية اندماج بين ثلاث وسائط متمثلة بالنص والصورة والصوت ومن ثم خلق حالات تفاعلية (Interactivity) بين المضمون المنتج المعروض عبر الحاسوب والمستخدم، فضلا عن أن الوسائط المتعددة تسير بشكل خطي في حين الوسائط المتشعبة تتشعب بمستوى غير محدود.

10) إعلام الفضاء السيبراني (CyberSpace) :

ويعرف الفضاء السيبراني بأنه البيئة الافتراضية التي تحدث فيها عمليات الاتصال في ظل الانترنت على شاشة الكمبيوتر، وأصبحت هذه المفردة مشهورة بشكل كبير عندما بدأ استخدام الانترنت والتقنية الرقمية في التسعينات وكانت تشير إلى أفكار وظواهر جديدة عدة وأصل هذه المفردة يعود للفنون البصرية، وأول من استخدمها هو الرسامة الدنماركية سوزاني (Susanne) في أواخر 1960 مع زميلتها المهندسة كاستنهوف (Carsten Hoff) واستخدمت لاحقا 1980 في مجال العمل على لسان كاتب الخيال وليم جيبسون (William Gibson)، ومن ثم وردت في قصة قصيرة للكاتب نفسه 1982، في حين يشير الدكتور عباس مصطفى صادق في كتابه (الإعلام الجديد المفاهيم والوسائل والتطبيقات) إلى أنها استخدمت أول مرة من جيبسون لكن في روايته (Necromancer) التي كتبها 1984.

11) الإعلام التشاركي (Participatory media) :

توصف وسائل الإعلام التشاركية بأنها وسائل الإعلام التي تتيح للجمهور عن طريقها أن يؤدي دورا في عملية جمع المعلومات وإعدادها وتحليلها ونشر المضمون، وتمثل صحافة المواطن جزءا منها واستخدام هذا المفهوم لأول مرة في 2006¹.

¹ المرجع السابق، ص.ص. 55 - 62 .

ثانيا : خصائص الإعلام الرقمي (الإعلام الجديد) :

- (1) **السرعة** : أصبح من الواضح أن مستخدم الوسائل الجديدة الحاسوب والهاتف والراديو الرقمي والتلفزيون الرقمي والهاتف المحمول، يستطيع تبادل رسائله وخطابه مع الطرف الآخر بصورة أكثر سرعة من المرحلة التي سبقت ظهور الإنترنت والأقمار الاصطناعية .
- (2) **الشمول** : لقد اتسعت استخدامات الوسائل التقليدية كالصحافة والتلفون والإذاعة والتلفزيون في ظل التكنولوجيا الجديدة، كما اتسعت رقعة انتشارها لتضم زوايا العالم كله أرضا وجوا وبحرا .
- (3) **الجودة** : هناك تطور ملموس في جودة الصوت والصورة ووضوحهما في البث الإذاعي والتلفزيوني والاتصالات الهاتفية والتبادل الإخباري والتراسل النصي عبر الإنترنت والهواتف المحمولة والتلكس وغيرها، وهو ماكانت الاتصالات المتاحة سابقا تشكو من عدم توفره لعقود طويلة مما يتسبب في عرقلة عملية الاتصال عبر هذه الوسائل أو تشويشها أو انقطاعها .
- (4) **التنافذ** : إن التآزر بين وسائل الاتصال بما يؤمن دعم خصائص كل منها للآخر أصبح سمة مميزة لوسائل الاتصال اليوم في ظل التقنية الجديدة، فالحاسوب يدعم جودة إنتاج الصحيفة الإلكترونية والقمر الاصطناعي يدعم جودة الصوت والصورة التي نداولها عبر الإنترنت والهاتف صار يستفيد من تطبيقات الحاسوب والإنترنت والكاميرا .
- (5) **التأثير** : إن ما تتمتع به الوسائل الحديثة من إمكانيات استخدام الوسائط المتعددة، الصوت والصورة واللون والحركة والنص، قد فاقت كثيرا ما سبق أن امتلكنه الوسائل التي سبقتها. وتشير الدراسات إلى أن واقع التلقي يؤشر حالة من الانبهار بما تقدمه وسائل الاتصال الحديثة لدى شرائح واسعة من الجمهور بصورة تدعو الكثير من الإعلاميين والمربين إلى القلق مما يمكن أن تشكله ثقافة الصورة من مخاطر على فئات الأطفال والشباب خاصة¹.
- (6) **التحكم** : تميزت وسائل الاتصال في هذه المرحلة بقدرة متجددة على التكيف لرغبات المستخدم من حيث التحكم بالوقت أو الشكل أو المضمون الذي يرغب في التعامل معه ، كما يحقق للمتلقي قدرا عاليا من الخصوصية وهي صفة تسجل لهذه الوسائل وعليها في وقت واحد،

¹ حارث عبود، مظهر العاني، الإعلام والهجرة الى العصر الرقمي، دار الحامد للنشر والتوزيع، ط1، الأردن، 2015، ص.ص.70-72.

من جهة أخرى فقد أصبح بمقدور الجمهور أن يكون هو نفسه مصدرا للأخبار والوثيقة الميدانية باستخدام هاتفه النقال بكل سهولة ويسر، ولم يعد من الصعب على المتلقي أن يرسل وثيقة نصية أو صوتية إلى وكالات الأنباء أو مواقع الإنترنت لتكون خلال لحظات أمام العالم كله بوسائل عدة وبأشكال عدة. وقد استخدمت العديد من المحطات الإذاعية والتلفزيونية ووكالات الأنباء والصحف هذه الإمكانية في تغطية وقائع أحداث ساخنة في مواقع عديدة في العالم وقت واحد بالاستعانة بجمهورها في رصد الأحداث ونقلها من أماكن الأحداث.

(7) **التفاعل** : وهي صفة أنتجتها القدرات الجديدة لوسائل الاتصال بحيث ألغت نمط التلقي السلبي غير التفاعلي الذي كان يعاني منه الجمهور في تعامله مع الوسائل السابقة، فقارئ الصحيفة الإلكترونية أو مشاهد التلفزيون، أو مستخدم الإنترنت يستطيع أن يوصل رأيه للكاتب أو المقدم بصورة ميسرة وسريعة .

(8) **التنوع** : إن قدرة الإنترنت والأقمار الاصطناعية على نقل ملايين الرسائل والمواد السمعية والصورية في وقت واحد أتاحت للمتلقي نوافذ بالغة التنوع لتلبي طيفا واسعا من الرغبات في مختلف التخصصات، بل إننا نجد محطات تلفزيونية مثلا تتخصص بالأطفال أو المرأة أو الرياضة أو الطبخ أو الرحلات أو غيرها .

(9) **التكامل** : تتكامل عناصر التقنية في الوسائل التي تتيحها البيئة الاتصالية المعاصرة بما يسهل مهمة المستخدم بصور مختلفة¹ ، وربما يبرز ذلك بصورة جلية اليوم في الهواتف الذكية التي تمكن المستخدم من الكتابة والتصوير والتراسل والتشارك بالوثائق والتحدث بالصورة والصوت وتخزين المعلومات بأشكالها المختلفة ومتابعة المحطات الإذاعية والتلفزيونية المفضلة وغير ذلك من جهاز الهاتف الشخصي دون عناء يذكر.

(10) **العالمية** : لم تعد الرسائل المتبادلة بين جمهور وسائل الاتصال حبيسة النطاق المحلي أو الإقليمي بل اتسعت لتشمل العالم كله، ولم يعد غريبا أن تجد ابنك ذا السنوات العشر قد ارتبط بصداقات عديدة في البلدان أخرى قد لا يعلم مواقعها على خارطة العالم وهو مؤشر يتصل بجوانب تربوية واجتماعية وثقافية عديدة .

¹ حارث عبود، مزهر العاني، المرجع السابق ص73-74.

11) **المرونة** : تتسابق شركات صناعة المعلومات ووسائل تداولها على توفير خدماتها بأسرع وقت وأفضل صورة الفوز بثقة جمهورها وتحقيق أفضل عائد اقتصادي في النهاية، لذلك فهي دائمة السعي إلى تحقيق رغبات جمهورها والتكيف لظروفه وجدول نشاطه اليومي في البيت ومكان العمل وفي الشارع والأماكن العامة بما يحقق للمستخدم أعلى مرونة ممكنة في استخدام تكنولوجيا الاتصال للتواصل مع الأخبار والأحداث وتقلبات الأسعار والأنواء الجوية وما يفضل من برامج تلفزيونية وغيرها، وعلى سبيل المثال فقد ذهبت إحدى محطات التلفزيون إلى إنتاج برامج خاصة لتعليم اللغة بالصوت والصورة ووزعتها لمستخدمي الهاتف المحمول لغرض تعلم اللغة من خلال هواتفهم في أوقات فراغهم وهم في محطة القطار أو مكان العمل .

12) **التزامن** : من المعلوم أن جل وسائل الاتصال في المرحلة التي سبقت ظهور الحاسوب والانترنت كانت غير قادرة على التراسل المتزامن بين المرسل والمستقبل باستثناء المورس والهاتف . أما في المرحلة التي أعقبت ظهورهما فإن التواصل المتزامن أصبح سمة مميزة إنه يتم باستخدام الصوت والصورة والنص في وقت واحد .

13) **الشيوع** : لم تعد الوسائل الحديثة مقتصرة على الميسورين من الناس ، فقد سعت شركات الإنتاج إلى عرض منتجاتها منها بأسعار تنافسية، وعلى الرغم من ذلك فإن الوسائل الحديثة تتطلب من مستخدميها اكتساب قدر من المهارات التي تمكنه من استخدامها على عكس الوسائل التي سبقتها، ومع ذلك فإن استخدام وسائل الاتصال الحديثة هو اليوم أكثر شيوعاً بكثير من ذي قبل .

14) **التخزين** : إذا كانت أولوية معظم وسائل الاتصال في المرحلة السابقة تعنى بإيصال الأخبار والوثائق ولا تعنى بتوثيق المعلومات باستثناء بعضها فإن أولوية الحاسوب والانترنت هي تخزين كم هائل من المعلومات المصنفة طبقاً لاحتياجات المستخدم، والمتاحة وقت الطلب وهو ما يجعلها مصدراً أساسياً للمعرفة والإعلام في مختلف الميادين هذا فضلاً عن سهولة الوصول إليها وتعدد الأشكال التي تحفظ بها هذه المعلومات ¹.

¹ المرجع السابق ص 73-74 .

15) تجاوز الرقابة : لم تعد الرقابة مهيمنة على مضامين الاتصال ومكوناته وأصبح التراسل حراً طليقاً في أغلبية وهو آخذ في هذا المسار بشكل يكاد يكون متكاملًا، وذلك مع تطور تقنيات الاتصال وصعوبة تقييد مضامينها وذلك على مستوى العالم أجمع.

16) تكاليف محدودة : إن تكاليف النشر الإلكتروني بل والبث صوتاً وصورة أصبح من السهولة بمكان، وتكاليف تعد زهيدة مقارنة بالوسائل التقليدية وهي مازالت في انخفاض مستمر .

17) ملكية للجميع : أصبحت ملكية هذه الوسائل متاحة للجميع، فأى فرد بإمكانه أن يقوم بامتلاك وسائله وبمبالغ زهيدة بحيث يستطيع أن ينشر ويرسل ويستقبل بل ويحظى بالإقبال الجماهيري والمتابعة متى ما كان موضوعه جذاباً وموجهاً للجماهير ذات علاقة .¹

ومن أهم الظواهر التي صاحبت الإعلام الرقمي (الجديد) :

- كسر احتكار المؤسسات الإعلامية الكبرى .
- ظهور طبقة جديدة من الإعلاميين، وأحياناً من غير المتخصصين في الإعلام قد يتفوقون على أهل الاختصاص الأصليين .
- ظهور منابر جديدة للحوار .
- ظهور إعلام الجمهور إلى الجمهور .
- ظهور مضامين ثقافية وإعلامية جديدة .
- مشاركة المجتمع في تسليط الضوء على قضايا إعلامية .
- نشوء ظاهرة المجتمع الافتراضي والشبكات الاجتماعية .
- تفتت الجماهير وانتقال الإعلام من حالة الجماهير العريضة لوسائل الإعلام التقليدية إلى مرحلة الإعلام الفئوي والإعلام المتخصص .²

¹ عبد اللطيف بن ديبان العوفي، التوعية الإعلامية الأسس النظرية والاجراءات التطبيقية، النشر العلمي والمطابع، الرياض، جامعة الملك سعود، 2012، ص 225-226 .

² انتصار محمد القحطاني، الإعلام الرقمي، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد الثامن، 2019/2، ص 11، 12 .

المطلب الثاني : أنواع ووسائل الإعلام الرقمي

❖ أولا :أنواع الإعلام الرقمي

الإعلام الرقمي المملوك :

هو أي أصول عبر الانترنت تتحكم فيها ، عادة ما يكون هذا النوع من الوسائط فريدا لعلامة تجارية وتشمل منصات الوسائط الرقمية موقع الويب الخاص بك وقنوات التواصل الاجتماعي والمدونات ومقاطع الفيديو وما إلى ذلك . إذا قمت بتحسين الإعلام الرقمي المملوك لك لتحسين محركات البحث فسيظهر عملك عندما يبحث العملاء المحتملون عن موضوعات ذات صلة بما تقدمه كلما زادت ملكية الوسائط الرقمية التي تنشئها أصبح عملك أكثر وضوحا ويمنح هذا سلطة علامتك التجارية وبالتالي يزيد ترتيبك على صفحة نتائج محرك البحث .

الإعلام الرقمي المدفوع :

تروج الوسائط المدفوعة للمحتوى الخاص بك عبر الانترنت لتحسين حركة المرور إلى أصول الوسائط المملوكة لك ، يتضمن هذا النوع من الوسائط عادة إعلانات البحث المدفوعة والإعلانات الصورية وإعلانات Facebook .

على الرغم من أن الوسائط المدفوعة تعتبر نفقات عند استخدامها بشكل صحيح فإنها تعرض المحتوى والعلامة التجارية الخاصة بك إلى جمهور أوسع يمكن لوكالة التسويق الجيدة استخدام الوسائط المدفوعة لتوجيه العملاء المناسبين إلى موقع الويب الخاص بك ، ويمكن أيضا أن تقدم إعلانات الوسائط الرقمية المدفوعة نتائج مهمة وقابلة للقياس داخل الحملة وبالتالي تدعم استراتيجية التسويق الشاملة وهذا يعتبر إحدى نظريات الإعلام الجديد.

الإعلام الرقمي المكتسب :

هو إعلانات يتم إنشاؤها بواسطة عملائك عندما يدافع العملاء عن علامتك التجارية عبر الكلام الشفهي أو وسائل التواصل الاجتماعي أو المراجعات أو الشهادات أو المشاركات، أو إعادة النشر وما إلى ذلك فهذا هو أفضل شكل من أشكال التأييد الذي يمكن أن تحصل عليه الشركة ويعد الإعلام الرقمي المكتسب طريقة فعالة لتنمية العلامات التجارية مع تقليل تكاليف

اكتساب العملاء ومع ذلك يتعين مراقبة ذلك بانتظام لأنه على عكس الوسائط الرقمية المملوكة لا يوجد سيطرة عليه¹.

❖ ثانياً: وسائل وأدوات الإعلام الرقمي:

تعددت وسائل الإعلام الرقمي وأدواته، وتزداد تنوعاً ونمواً مع مرور الوقت ومن هذه الوسائل:

- الشبكات الاجتماعية:

عبارة عن مواقع ويب تقدم مجموعة من الخدمات للمستخدمين مثل المحادثة الفورية، والرسائل الخاصة، والبريد الإلكتروني، والفيديو، والتدوين، ومشاركة الملفات، وغيرها من الخدمات. ومن أشهر الشبكات الاجتماعية الموجودة حالياً:

- الفيس بوك .
- تويتر .

وقد حاول العرب الاستفادة من فكرة الشبكات الاجتماعية لإنشاء شبكات اجتماعية عربية لكنها لم تصل إلى شهرة الفيس بوك، تويتر، ومنها :

- شبكة فرند أوي .
- شبكة أرابز .

- المفضلات الاجتماعية:

وهي مواقع تسمح لك بإنشاء مفضلاتك وأرشفتها وحتى مشاركتها مع باقي الأعضاء المسجلون في هذه المواقع، هي مفضلة لا ترتبط بجهازك كما هي العادة بل هي مفضلة موجودة على شبكة الإنترنت ومن أشهر أمثلتها موقع ديفغ، وظهرت عدة مواقع عربية توفر خدمة المفضلات الاجتماعية مثل: موقع ضريت، موقع أفلق، حفار المدونات.

- مواقع استضافة المدونات المجانية، ومنها :

- الورد برس .
- بلوجر .
- تمبلر .¹

¹ دينا محمود، تعريف الإعلام الرقمي وأنواعه وأهميته، www.Almrsal.com، أوت 2022، 03:34 .

- مشاركة الفيديوهاات والصور :

مواقع مشاركة الفيديوهاات هي مواقع إعلام جديد تتيح لك مشاركة مقاطع الفيديو الخاصة بك، وصورك مع أصدقائك على الموقع، وأشهر تلك المواقع، اليوتيوب، جوجل فيديو .

- مواقع مشاركة الصور :

مواقع مشاركة الصور تسمح لك برفع صورك إلى الموقع ومشاركتها مع الآخرين مثل: ليكر كما توجد مواقع أخرى عديدة لمشاركة الصور وتخزينها منها: سلايد، فوتولوغ، فوتوكي².

- موقع ماي سبيس(MySpace):

هو أكبر موئل في شبكة الانترنت للتشبيك الاجتماعي للأصدقاء وما اليهم وقت كتابة هذا النص وهو يقدم لهم أركاناً خاصة لتقديم لمحات من حياتهم الشخصية، ومدوناتهم، ومجموعاتهم، وصورهم، وموسيقاهم، ومقاطع الفيديو التي يعرضونها في الموقع ، ويحتوي ماي سبيس على محرك بحث خاص بعرض ونظام بريد الكتروني داخلي ويستطيع الناس من جميع أنحاء العالم صنع ملفات الكترونية عن حياتهم، والالتحاق بمجتمع خاص وتحديد مواعيد للإلتقاء والتشابك المهني والترويج للأعمال ومشاركة الاهتمامات والعثور على أصدقاء الدراسة القدامى والأصحاب كما يمد الموقع مستخدميه بمساحة للخصوصية والاندماج الثقافي ويتحاور ملايين الشباب مع الإعلام من خلاله ويعبرون عن قيمهم الشخصية والثقافية من خلال شبكة ماي سبيس الاجتماعية³.

-المدونات:

هي يوميات شخصية على الشبكة يتم إدراجها بواسطة برامج بسيطة تسمح بطبع نص على الحاسوب وإرساله فور الاتصال بالشبكة ليظهر على صفحة الموقع المعني وهي تمزج عمداً بين المعلومات والآراء كما تترافق مع ربط بمصدر أصيل أو بمفكرة أخرى أو بمقالة ينصح بها كاتب

¹ ماهر عودة، وآخرون، الإعلام الرقمي الجديد، دار الإعصار العلمي للنشر والتوزيع، ط1، عمان-الأردن، 2015، ص33، 34.

² المرجع نفسه، ص33، 34 .

³ نسرين حسونة، الإعلام الجديد المفهوم والوسائل والرسائل والخصائص والوظائف، متاح على الرابط. www.alukah.net ، 31 بتاريخ. -03، على الساعة: 22:12، 2023، ص4 .

اليوميات أو يعلق عليها، وأول مدونة من هذا الصنف ترجع إلى 7 تشرين/ أكتوبر 1994 وهي منسوبة إلى دايفوينر، مبرمج أحد البرامج الإلكترونية الأكثر شيوعاً ومطورة تحت اسم منيلا . ويعرف (سليمان، 2009، 134) المدونة بأنها تطبيق من تطبيقات الإنترنت، يعمل من خلال نظام إدارة المحتوى، وفي أبسط صورة عبارة عن صفحة ويب على شبكة الإنترنت تظهر عليها تدوينات (مدخلات) مؤرخة ومرتبطة ترتيباً زمنياً تصاعدياً ينشر منها عدد محدد يتحكم فيه مدير أو ناشر المدونة، كما يتضمن النظام آلية لأرشفة المدخلات القديمة، ويكون لكل مدخلة منها مسار دائم لا يتغير منذ لحظة نشرها يمكن القارئ من الرجوع إلى تدوينة معينة في وقت لاحق عندما لا تعود متاحة في الصفحة الأولى للمدونة، كما يضمن ثبات الروابط ويحول دون تحللها .

إن مدونات الإنترنت تعتبر واحداً من أهم تطبيقات الإعلام الجديد هو البلوغ Blog أو ويب لوج Weblog ما أطلق عليه عربياً المدونة وهي عبارة عن موقع على الإنترنت يستخدم كصحيفة يوميات إلكترونية فردية تعبر عن صاحبها وتركز على موضوع معين، مثل السياسة أو الأخبار المحلية، ويمكن أن تكون عبارة عن مذكرات يومية، وهي تنشر بالنصوص، والصور والفيديو والصوتيات وتحمل وصلات لمدونات أخرى، مواقع إنترنت أو وسائط أخرى متعلقة بالمقالة .

- الويكي Wiki:

هي عبارة عن مواقع ويب تسمح للمستخدمين بإضافة محتويات وتعديل الموجود منها، حيث تلعب دور قاعدة بيانات مشتركة جماعية، أشهر هذه المواقع، موقع Wikipedia وهو الموسوعة التي تضم ملايين المقالات بمعظم لغات العالم .

كلمة الويكي Wiki بلغة شعب جزر هاواي الأصليين تعني: بسرعة، أما بلغة التكنولوجيا فهي تعني نوع بسيط من قواعد البيانات التي تعمل في شبكة الانترنت. وفي عام 1995 قام كل وارد كينغهام وبوليوف بإنشاء أول موقع ويكي وهو WikiwikiWeb والذي شكل مجتمعاً متعاوناً مفتوحاً للجميع، حيث يمكن لأي شخص أن يشارك في تطوير وزيادة محتويات الموقع منذ ذلك الوقت وحتى اليوم ظهرت برامج ويكي كثيرة واعتمدت الكثير من المواقع على هذه البرامج والهدف هو تبسيط عملية المشاركة والتعاون في تطوير المحتويات إلى أقصى حد ممكن¹.

¹ نسرين حسونة، مرجع السابق ، ص 5 .

-البودكاست:

هي خدمة تتيح الحصول على الملفات الصوت والفيديو من موقع معين بمجرد أن تدرج فيه دون الحاجة الى زيارته في كل مرة وتحمل المحتوى يدوياً فالمستخدم الذي يملك تطبيقاً على جهازه كتطبيق (Apple Itunes) مثلاً يمكنه الاشتراك في خدمة البودكاست لأي موقع يريد بشرط أن يقدم الموقع هذه الخدمة، ثم يقوم ال itunes بتحميل الملفات الجديدة أوتوماتيكياً في حال توفرها .

-المنتديات:

هي عبارة عن برامج خاصة تعمل على الموقع الإعلامي أو أي مواقع أخرى ذات طابع خاص أو عام على شبكة الانترنت مثل المواقع المتخصصة وتسمح بعرض الأفكار والآراء في القضايا أو الموضوعات المطروحة للمناقشة على الموقع وإتاحة الفرصة للمستخدمين أو المشاركين في الرد عليها ومناقشتها فوراً سواء كان ذلك مع أو ضد الآراء أو الأفكار المطروحة دون قيود على المشاركين باستثناء القيود التي يضعها مسئولو المنتدى من خلال نظام الضبط والتحكم المقام على البرنامج .

وهي واحدة من تطبيقات المشاركة والتفاعل والإعلام البديل التي جاءت بها الشبكة بما يحقق للجميع اسماع أصواتهم، وهي في الوقت نفسه مجموعة من البرامج المختلفة تعمل على تطبيق هذا النوع من التواجد الحي للتجمعات على الانترنت وهي نشاط يعود إلى حوالي عام 1995 العام الذي بدأت فيه المنتديات في الظهور، وتمثل مرحلة انتقالية أو تطويرية من النشرات الالكترونية BBS ومجموعات الأخبار التي سادت في الثمانينات وبداية التسعينات، لتخلق نوعاً من المجتمعات الافتراضية التي تدور غالباً حول موضوع معين أو بلد أو مجموعة من الموضوعات .

-مجتمعات المحتوى :

هي مجتمعات (موقع) على الشبكة تسمح بتنظيم ومشاركة أنواع من المحتويات أشهر المجتمعات تهتم بالصور كموقع Flickr، وحفظ الروابط Bookmakr Links كموقع Del.icio.us، والفيديو كموقع Youtube¹ .

¹نسرين حسونة، مرجع السابق، ص 6-7 .

-موقع يوتيوب :

هو أحد أشهر المواقع الإلكترونية على شبكة الإنترنت وعنوانه www.youtube.com، وتقوم فكرة الموقع على إمكانية إرفاق أي ملفات تتكون من مقاطع الفيديو على شبكة الإنترنت دون أي تكلفة مالية، فبمجرد أن يقوم المستخدم بالتسجيل في الموقع يتمكن من إرفاق أي عدد من هذه الملفات ليراها ملايين الأشخاص حول العالم، كما يتمكن المشاهدون من إدارة حوار جماعي حول مقطع الفيديو من خلال إضافة التعليقات المصاحبة فضلاً عن تقييم ملف الفيديو من خلال إعطائه قيمة نسبية مكونة من خمس درجات لتعبر عن مدى أهمية ملف الفيديو من وجهة نظر مستخدم الموقع .

وطبقاً لتصنيف أليكسا العالمي فإن موقع يوتيوب يأتي في المركز الثالث من حيث أكثر المواقع العالمية مشاهدة، بعد كل من : ياهو، وجوجل.

-موقع Flickr :

يعتبر موقع Flickr نموذجاً لواحدة من أهم التطبيقات صحافة الجمهور في بعدها المتمثل في توزيع الصور، وقد أسهم الموقع في مناسبات مختلفة في أن يكون بديلاً حياً لوكالات الأنباء مثلما حدث أيام تفجيرات قطارات الإنفاق في لندن وفي أحداث تسونامي. فهو موقع لمشاركة الصور وحفظها وتنظيمها وهو أيضاً جمعية لهواة التصوير على الإنترنت بالإضافة إلى كونه موقعاً مشهوراً للتشارك في الصور الشخصية ، يتم استخدام الموقع من قبل المدونين من خلال إعادة استخدام الصور الموجودة فيه، أخذ الموقع شهرته من خلال ابتكاراته كإضافة التعليقات (Comments) من قبل الزائرين وكلمات المفاتيح Tags .

- التدوين المصغر Microblogging :

هو عبارة عن خدمات تقدمها شبكات اجتماعية تسمح بإنشاء حسابات وصفحات شخصية تعتبر بمثابة مدونات، غير أن التدوينات هي عبارة عن رسائل قصيرة لا تتجاوز 140 حرفاً لعرضها ومشاركتها على الويب وعلى أجهزة الهواتف المحمولة ، ويتم التدوين إما عبر الويب سواء عبر الموقع نفسه أو عبر مختلف التطبيقات المكتبية المطورة بناء على منصة تطوير الموقع أو

عبر الرسائل القصيرة (SMS) ويعتبر Twitter أشهر موقع للتدوين المصغر بالإضافة الى Jaiku و Pownce¹.

- البريد الإلكتروني (EMAIL) :

البريد الإلكتروني (EMAIL) هو من أشهر الخدمات التي تقدمها الشبكة المعلوماتية في الوقت الحالي اخترع عام 1972 من طريق رايدكومنسون الذي تمكن من إرسال أول رسالة إلكترونية، واليوم وبعد مرور حوالي 45 سنة أصبح ضرورة اتصالية حقيقية ومن مميزاته إمكانية إرسال الرسائل مرفقة بصورة أو وثائق....، بالإضافة الى توفير العديد من المواقع والخدمات بالمجان وهي وسيلة سهلة وبسيطة وفي متناول الجميع².

- الصحافة الإلكترونية :

شهد المجتمع المعاصر مع نهاية القرن العشرين تطورات سريعة في كافة جوانب الحياة الاقتصادية والسياسية والتكنولوجية ، ويعتبر مجال الاتصال والإعلام من أهم الجوانب التي تأثرت بهذا التطور حيث لعبت الحاسبات الآلية والأقمار الصناعية وخاصة الأنترنت دورا هاما في نقل المعرفة والمعلومات وكافة مواد الاتصال بين المجتمعات بشكل مباشر، في وقت قريب كانت الصحافة الورقية أو المكتوبة تشكل المصدر الأول للمعلومات والأخبار لدى الجمهور إلى أن دخل مصطلح جديد إلى عالم الإعلام أطلق عليه "الصحافة الإلكترونية" واكتسب هذا النوع الجديد أهمية بالغة من ظهوره أوائل التسعينات من القرن الماضي، وتزايدت أهمية الصحافة الإلكترونية مع توالي الأعوام انتشار الانترنت وتضاعف أعداد مستخدميه فأصبحت غالب المؤسسات الصحفية على الصعيدين العالمي والعربي تمتلك مواقع إلكترونية لمطبوعاتها الورقية، لكن الجديد هو ظهور نوع جديد من الصحف غير التقليدية وهو ما عرف بالصحف الإلكترونية والتي يقتصر إصدارها على النسخة الإلكترونية دون المطبوعة .

وتعرف الصحافة الإلكترونية بأنها منشور إلكتروني دوري يحتوي على الأحداث الجارية سواء المرتبطة بموضوعات عامة أو بموضوعات ذات طبيعة خاصة ويتم قراءتها من خلال جهاز كمبيوتر

¹ نسرین حسونة، مرجع السابق، ص 7 .

² خضر إبراهيم حيدر، الميديا مفهومها المعاصر وعلاقتها بالإعلام الكلاسيكي، المركز الإسلامي للدراسات الإستراتيجية، ط1، القبة العباسية المقدسة، 2018، ص 156، 157 .

عبر شبكة الإنترنت وتتمثل الفكرة الأساسية في الصحيفة الإلكترونية في توفير المادة الصحفية (خبر، تعليق، تقرير، تحقيق...) على إحدى شبكات الخدمة التجارية الفورية . كما تتميز الصحافة الإلكترونية بمجموعة من الخصائص نوردتها فيما يلي : الوصلات الشعبية، الإشارة إلى المواقع ذات صلة بالموضوع ، أداة البحث في الموقع وجود أرشيف للموضوعات والأعداد السابقة المباشرة والتحديث المستمر، التفاعلية¹ .

- الإذاعة الرقمية :

- الراديو الرقمي الفضائي :

يعد البث الإذاعي الفضائي ثورة في عالم الراديو حيث تنقله من النظام القديم والموجة المتوسطة والقصيرة إلى عصر الفضاء ، وتربطه بتكنولوجيا الاتصال الحديثة مما يشكل بعثا جديدا لجهاز الراديو يعتمد على الاستقبال المباشر من القمر الصناعي دون اللجوء إلى محطات تقوية عالية التكاليف ومحدودة الأثر .

والراديو الفضائي أو راديو الأقمار الصناعية أو راديو الاشتراك هو راديو رقمي يستقبل إشارات البث من الأقمار الصناعية التي تغطي مجالا أرضيا جغرافيا واسعا لا يقارن معها البث الإذاعي الأرضي بأي حال من الأحوال إذ يستطيع المستمع متابعة إشارات البث في مجال تغطيتها بصرف النظر عن الموقع، كما يقوم نظام البث الإذاعي الرقمي المباشر عن طريق إرسال الإشارات إلى الملايين من أجهزة الاستقبال (الراديو الفضائي) ولا يحتاج التقاط إشارات القمر الصناعي إلى أرضية بل هناك هوائيات صغيرة مثبتة في كل جهاز راديو تلتقط الإشارة مباشرة .

وظهرت المنظومة الجديدة للراديو الرقمي الفضائي من خلال شركة "وورلد سبيس" الأمريكية التي أسسها الدكتور نوح عزمي سماره عام 1990 بهدف إنشاء شبكة فضائية عربية تستطيع أن تغطي إفريقيا والشرق الأوسط وأمريكا الجنوبية الوسطى باستخدام البث الرقمي ، وحصلت هذه الشركة على موافقة الاتحاد الدولي للاتصالات السلكية واللاسلكية عام 1993 .

ويتميز الراديو الفضائي بأنه مؤمن من التداخل والتشويش ، كما أن عملية اختيار المحطة التي يراد الاستماع إليها لا يتم بتحريك المؤشر كما هو الحال في الأجهزة التقليدية وإنما بتحديد رقم

¹ منصور حسام، مرجع السابق، ص 93 .

المحطة المعنية ، كما تسعى هذه الوسيلة الإعلامية الى تحقيق التنمية في عديد البلدان الفقيرة من خلال تخصيص بعض قنوات البيئة ، الصحة ، التعليم الجامعي ¹.

-راديو الأنترنت :

راديو الأنترنت هو عبارة عن برامج صوتية يتم بثها عبر توصيلات الأنترنت، وهو نظام لا يشبه طريقة البث التقليدية عبر الفضاء بواسطة الإشاعات الكهرومغناطيسية، هو خدمة إذاعية تبث عن طريق الشبكة ويمكن لأي مشترك في الأنترنت القيام بها كما يمكنه الاستماع لأي محطة موجودة على الأنترنت فقد أمكن لأي شخص أن يصبح مالكا لمحطة إذاعية على الشبكة حتى ولو كان مركزها في البيت فكل ما يحتاجه هو أن يملك شخصا صوتا يستطيع من خلاله توصيل رسالته ومواد إذاعية وكمبيوتر ، فالعديد من المحطات الإذاعة في الأنترنت مستقلة تماما عن المحطات التقليدية بل هي وسيلة بث متخصصة وموجودة فقط على شبكة تعرض أفقا واسعا من الخدمات الإخبارية ، الرياضية، الحوارية، الموسيقى ، المواد الصوتية والأرشفة ولأن الإشارة الإذاعية تنتقل على شبكة الأنترنت بلا حدود فمن الممكن الحصول على خدماتها في جميع أنحاء العالم ، فعلى سبيل المثال يمكن الاستماع الى محطة إذاعة أسترالية في أوروبا وإفريقيا .

- التلفزيون الفضائي الرقمي :

يعتبر البث الرقمي نقلة مفصلية في تاريخ التلفزيون ، لأنه أنهى عصر ندرة البث الإذاعي والتلفزيوني أو محدوديته التي ميزت البث التناظري من جهة وفتح الأبواب على مصارعها من جهة أخرى ، لاستثمار الطاقات التي تحملها الموائمة التقنية التي سمحت ببث المادة الإعلامية أو الثقافية أو التعليمية ذاتها عبر العديد من المحامل والشاشات: التلفزيون، الكمبيوتر، الهاتف، جهاز (DVD)المحمول، جهاز(Ipad)انطلاقا من قاعدة أن الوسائط المتعددة ليست دجما للوسائط بل إنها تكامل الوسائط المختلفة لإنتاج مادة تلتقي فيها أنماط الاتصال المختلفة باستثمار طاقتها التوصيلية والتعبيرية والجمالية .

ولقد أحدثت شبكة الأنترنت تغييرا كبيرا في الوضع الاقتصادي و الاجتماعي والإعلامي في التلفزيون الكلاسيكي حيث أصبحت شريكه في بث مواده السمعية والبصرية بشكل مباشر

¹منصور حسام، المرجع نفسه، ص93 .

(live streaming) أو إعادة بثها ففي هذا الصدد يمكن التأكيد أن قناة mbc الأمريكية هي أول قناة عرضت برامجها على شبكة اليوتيوب.

كما برزت الانترنت كفاعل جديد في مجال البث السمعي البصري، وهذا ما يبيته تزايد عدد القنوات التلفزيونية التي تبث عبر شبكة الانترنت بجانب الشركات الاقتصادية، والمؤسسات الإدارية، والهيئات الثقافية والاجتماعية والسياسية والمهنية التي أصبحت تبث شرائط الفيديو في مواقع الانترنت لغايات تجارية وتواصلية ونضالية¹.

ومن مزايا التلفزيون الرقمي نجد :

-سهولة التخطيط وإمكانية اللجوء إلى الشبكات أحادية الموجات أي بث البرامج انطلاقاً من نقاط متعددة على الموجة نفسها وهو غير متوافر في البث التناظري أو التماثلي.

-يمكن للتلفزيون الرقمي تقديم خدمات وسائط متعددة تشتمل على الصوت والصورة والبيانات والنصوص .

-توافر خدمات تفاعلية متعددة مثل البريد الإلكتروني والانترنت وخدمات التفاعل مع البرامج .

-توافر خيارات متعددة وكثيرة من القوالب والبرامج .

-إمكانية الحصول على الصورة عالية الوضوح .

-إلغاء الحدود الفاصلة بين الكمبيوتر والتلفزيون فأصبح بإمكان استخدام التلفزيون الرقمي للقيام بأي وظيفة من وظائف الكمبيوتر والعكس².

¹ المرجع السابق، ص 94، 95 .

² المرجع نفسه، ص 95 .

المطلب الثالث : وظائف وأهمية الإعلام الرقمي

❖ أولاً :وظائف الإعلام الرقمي

حدد (شرام) و(لا سويل) عدداً من الوظائف الرئيسية والفرعية للإعلام في المجتمعات ، ووجد ولبر شرام هناك أربع عشرة وظيفة أو مهمة رئيسة أو فرعية لوسائل الاتصال الجماهيري وهي :

مراقبة الناس والتعلم منهم، توسع آفاق التعرف على العالم، توسيع التركيز والاهتمام، رفع معنوية الناس، خلق الأجواء الملائمة للتنمية، يساعد بصورة غير مباشرة على تغيير الاتجاه، يغذي قنوات الاتصال بين الأشخاص، تدعيم الحالة الاجتماعية، توسيع نطاق الحوار السياسي، تقوية المعايير الاجتماعية، تنمية أشكال التذوق الفني والأدبي، يؤثر في الاتجاهات الضعيفة ويقويها، يعمل مدرسا ويساعد في جميع أنواع التعليم، وقد ولد تطور الحاجات الاجتماعية والسياسية والاقتصادية للمجتمعات المختلفة وظائف للإعلام الجديد المعاصر منها :

1. تجاوز قيود العزلة التي يفرضها الاتصال الرقمي، حيث يتعامل الفرد لساعات طويلة مع الحاسب الشخصي بعيداً عن الاتصال بالآخرين في الواقع الحقيقي، وتجاوز قيود العزلة هذه يتم بالاتصال بالآخرين من خلال برامج الحاسوب أو الشبكات في إطار واقع وهمي أو افتراضي يرسم أطراف الاتصال، حيث لا يتم الاتصال وجها لوجه ولكن من خلال المحادثات والحوارات والبريد الإلكتروني، ومع آخرين يعرف بعضهم البعض و لا تجمعهم سمات خاصة سوى ما يفرضه هذا الواقع وحاجاته .

2. سهولة الاتصال بالمواقع الإخبارية وفورية الإعلام، حيث تتوافر الآلاف من المواقع الإعلامية التي تقدم الوظيفة الإخبارية، وتنشر الوقائع والأحداث التي تتم في بقاع كثيرة من العالم في لحظة وقوعها .

3. القدرة على القيام بالتعبئة لتأييد الأفكار التي تنادي بها، ومناهضة غيرها من الأفكار بحيث يمكن أن تسهم في تكوين رأي عام إقليمي أو عالمي نحو المواقف والقضايا والأفراد في وقت معين، يتكون من فئات المستخدمين لشبكة الانترنت وبصفة خاصة المواقع الإعلامية المنتشرة فيها مما يجعلنا نطلق على هذه المواقع "المواقع الرقمية التعبوية" التي تعمل بمعزل عن كل النظم والأشكال التنظيمية المتاحة في المجتمعات وبالتالي تسهم في تنمية المشاركة الديمقراطية .

4. غياب المصادر وتحري المصادقية تسهم في تدعيم وظيفة الدعاية التي تسهم في جانبها السلبي في تحقيق الغزو الثقافي والهيمنة الثقافية والتبعية الثقافية¹.
5. تقديم المعلومات المتعددة والمتنوعة التي تتميز بالضخامة بشكل غير مسبوق نتيجة الخصائص التي تميزت بها تكنولوجيا الاتصال والمعلومات، وأهمها سعة التخزين وسهولة الإتاحة.
6. نجد أن هناك توسعاً في استخدام وسائل الإعلام الجديد في التعليم، ففي مجال التعليم عن بعد حققت دول العالم تقدماً ملموساً للاستفادة من شبكة الانترنت في تقديم الخدمة التعليمية للمستويات التعليمية المختلفة، وانتشرت المفاهيم والاستراتيجيات الخاصة بالتعليم عن بعد والتعلم من خلال الشبكات والتعليم الافتراضي والفصول الافتراضية وغيرها التي تشير الى وظيفة الحواسيب والشبكات في التعليم.
7. أصبحت وظيفة التسويق و الإعلان تجدد صدًى كبيراً لدى المعلنين وخصوصاً بالنسبة للمواقع التي تحقق نسبة أكبر في الاستخدام والدخول عليها، شأنها في ذلك شأن وسائل الإعلام الأخرى، ويعتبر تحقيق هذه الوظيفة بالنسبة لجمهور المتلقين دليلاً إلى اتخاذ القرارات الشرائية بجانب أنها تحقق تمويلاً لهذه المواقع والشركات التي تقدم الخدمات المتعددة سواء كانت مجانية أو مدفوعة.
8. مع انتشار برامج المسابقات والألعاب على مواقع شبكة الانترنت أو في البرامج الرقمية التي تعد لهذا الغرض وتناسب فئات مستويات عمرية عديدة، أسهم الإعلام الجديد في ذلك بتحقيق وظيفة التسلية والترفيه التي أصبحت تجذب مستويات عمرية مختلفة، بجانب ما تقدمه المواقع الإعلامية من إذاعة للمواد الإعلامية التي تسهم في تحقيق هذه الوظيفة وحاجات جمهور المستخدمين منها².

❖ ثانياً : أهمية الإعلام الرقمي

تزداد أهمية الإعلام الرقمي يوماً بعد يوم، وذلك للأسباب الآتية :

- يتضمن الإعلام الرقمي خصائص الإعلام التقليدي كافة، بالإضافة الى العديد من المزايا والإمكانيات الجديدة التي لا تتوفر في التقليدي .

¹ نسرین حسونة، مرجع السابق، ص12، 13 .

² المرجع السابق، ص 13 .

- تأتي أهمية الإعلام الرقمي من كونه إعلاماً عالمياً، بمعنى أنه يصل إلى كل مكان في العالم عبر الانترنت، كما أنه يتجاوز مشكلة اللغة إذ يتيح الإنترنت ترجمة أي محتوى يعرض من خلاله، إلى مختلف لغات العالم .
- بات الإعلام الرقمي أو الإلكتروني أكثر مصداقية وحيادية من الإعلام التقليدي اليوم، فهو لا يرتبط بقيود يفرضها الملاك أو الحكومات التي عادةً ما تسيطر على الإعلام التقليدي .
- يتناسب محتوى الإعلام الرقمي مع اهتمامات الجمهور، فإن لم يمكن المحتوى من الموضوعات التي تكثر عمليات البحث ضعيفاً ولا ينتشر¹ .
- يتيح الإعلام الرقمي الحرية المطلقة للمشاهد، في اختيار المحتوى الذي يريد في الوقت الذي يريد، وإمكانية إيقاف التشغيل والمتابعة متى يريد، بالإضافة إلى حفظ المحتوى والعودة إليه في وقت لاحق، وهذا ما جعل الكثير من الناس اليوم يتعدون عن مشاهدة التلفاز، واستبدالها بالإنترنت كاليوتيوب الذي يعرض ما يريده المشاهد وفي الوقت الذي يرغب فيه .
- كما يتيح الإعلام الرقمي إمكانية متابعة الأخبار على مدار اليوم، دون الحاجة إلى شراء الصحف الورقية وانتظار طباعتها وهذا يوفر على الشخص الوقت والجهد والمال .
- يمتاز الإعلام الرقمي بالانفتاح، إذ تتدفق فيه المعلومات من أطراف عدة .
- يمتاز الإعلام الرقمي بمواكبته للأحداث، فهو إعلام لحظي يتجدد على مدار الساعة.²

¹ الإعلام الرقمي: مفهومه وأهميته وأنواعه، متاح على الرابط: www.annajah.net، 30-03-2023، 09:15 .

² المرجع السابق، 30-03-2023، 09:15 .

المبحث الثاني: مفهوم الجرائم السيبرانية

المطلب الأول : تعريف الجرائم السيبرانية وخصائصها

للجريمة السيبرانية مجموعة من التعاريف ويمكن التعرف عليها فيما يلي:

❖ أولاً: تعريف الجرائم السيبرانية (الإلكترونية)

تعتبر الجريمة المعلوماتية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها التي ارتبطت بتقنية المعلومات، فقد اصطلح على تسميتها بداية بـ "إساءة استخدام الكمبيوتر"، ثم "احتيال الكمبيوتر"، فالجريمة المعلوماتية بعدها "جرائم الكمبيوتر"، جرائم التقنية العالية إلى "جرائم الهاكرز"، "فجرائم الانترنت" وأخيراً "السيبركرايم".

وقد وصفت هذه الجريمة بأنها مقاومة للتعريف لكثرة ما تناولته الكتابات عنها شرحاً وتوضيحاً فمنهم من نظر إليها من خلال وسيلة ارتكابها، ومنهم من خلال موضوعها، ومنهم من خلال توافر المعرفة بتقنية المعلومات، حيث يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها: "الجريمة التي تلعب فيها البيانات الحاسوبية والبرامج المعلوماتية دوراً رئيسياً، أو"كل فعل إجرامي متعمد أياً كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالجنح عليه¹، أو كسب يحققه الفاعل، وقد اتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمة التعاون الاقتصادي والتنمية (OCDE) للجريمة المعلوماتية في اجتماع باريس عام 1983 بأنها "كل سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به، يتعلق بالمعالجة الآتية للبيانات أو نقلها²

الجريمة السيبرانية لغة واصطلاحاً:

- الجريمة في اللغة : جمع جريمة، والجريمة أصل واحد يرجع إليه الفروع فالجرم القطع وجرم كسب والجريمة الذنب .
- الجريمة في الاصطلاح :

الاصطلاح الفقهي : محظورات شرعية زجر الله تعالى عنها بحد أو تعزير.

¹ عائشة عبد الحميد، ملوك نوال، "الإجرام السيبراني وأثره على تهديد الأمن الثقافي في الجزائر"، مجلة المفكر للدراسات القانونية

والسياسية، المجلد 3، العدد 3، سبتمبر 2020، ص 216 .

² عائشة عبد الحميد، ملوك نوال، مرجع السابق، ص 216.

الاصطلاح القانوني : لفعل أو ترك الذي نص القانون على عقوبة مقدرة له .

• السيرانية في اللغة و الاصطلاح :

السيرانية كلمة إنجليزية مشتقة من كلمة (Cyber) وتعني : مرتبط بالحاسوب أو شبكات الحاسوب، وقيل تعني : فضاء الانترنت، وقيل : كلمة يونانية مشتقة من كلمة (Kybernetes) وتعني : الشخص الذي يدير دفة السفينة، مجازاً للمتحكم.¹

• كما يمكن أن نعرف الجريمة بأنها كل سلوك أو نشاط أو فعل مخالف للقيم والقواعد العامة السائدة ومعايير المجتمع والصادر من الإنسان مقصوداً أو تحت تأثير عامل معين والذي يحدث الضرر بالفرد ومؤسسات المجتمع والبناء الاجتماعي من جهة والذي يؤدي الى خلق نوع من الاضطرابات السلوكية ونشر الذعر والقلق والخوف بين أفراد المجتمع من جهة أخرى.²

• تعريف الجريمة السيبرانية (الإلكترونية) فقهاً وقانوناً :

أ- التعريف الفقهي : انقسم الفقه إلى عدة آراء منهم من ضيق من مفهوم الجريمة الإلكترونية ومنهم من وسع من مفهومها، الاتجاه الذي يضيق من مفهوم الجريمة الإلكترونية، يذهب أنصار هذا الاتجاه إلى حصر الجريمة الإلكترونية في الحالات التي تتطلب قدراً كبيراً من المعرفة التقنية في ارتكابها، ومن التعريفات إلى وضعها أنصار هذا الاتجاه أن الجريمة الإلكترونية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية وملاحقته وتحقيقه من ناحية أخرى .

ب- التعريف القانوني :

أما بالنسبة للتعريف الذي جاء به المشرع الجزائري للجرائم المتصلة للتكنولوجيات الإعلام والاتصال فإنه يعرفها بأنها : "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية".³

¹ عبد العزيز بن فهد بن محمد بن داود، "الجرائم السيبرانية : دراسة تأصيلية مقارنة"، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 09، العدد 03، 2020، ص 148 .

² نوري ياسين هرزاني، الإعلام والجريمة، مطبعة جامعة صلاح الدين، أربيل، 2005، ص 29 .

³ محمد بوعمر، سيد علي بنينال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة أكلبي محمد أولحاج، البويرة، 2020/2019، ص 4، 5 .

-وتعرف الجريمة عموماً في نطاق القانون الجنائي بأنها فعل غير مشروع صادر عن ارادة جنائية يقرر له القانون عقوبة أو تدبيراً احترازياً¹.

الجريمة السيبرانية :

إن مصطلح الجرائم السيبرانية هو إحدى المصطلحات الحديثة والمستخدمه عن جرائم الإنترنت الذي تعددت مصطلحاته وذلك لنشأة وتطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات .

لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تتم الجريمة الإلكترونية وكما يقول فان دير هيلست و ونيف "هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف" .

ويتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية كما تعرف الجرائم الإلكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال².

كما يعرف بعض الفقهاء مصطلح السيبرانية بأنها "هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع الكترونية أو بنى تحتية محمية الكترونياً لتعطيلها أو تدميرها أو الإضرار بها" ويعرفه آخرون بأنها "هجوم عبر الانترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها" كما تم تعريف مصطلح السيبرانية في ورشة عمل بعنوان "الأمن الرقمي وحماية المستخدم من مخاطر الانترنت والذي نفذته هيئة الاتصالات وتقنية المعلومات المنعقد بتاريخ(2018/04/26) "بأنها مأخوذة من كلمة (سيبر) Cyber، وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي ، فالسيبرانية تعني : (فضاء الانترنت) .

ويعرف أيضاً بأنه "المجال الجديد الخامس للحروب الحديثة بعد البر والبحر والجو والفضاء الحقيقي وهو يمثل جميع شبكات الحاسب الآلي الموجودة حول العالم ويشمل ذلك الأجهزة

¹ محمد نصر محمد، الوسيط في الجرائم المعلوماتية، مركز الدراسات العربية للنشر والتوزيع، ط1، مصر، 2015، ص15 .

² راضية حميدة، "الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي نحو تفعيل دور الأمن السيبراني المعلوماتي"، مجلة الإعلام والمجتمع، المجلد 05، العدد 02، ديسمبر 2021، ص341 .

الالكترونية المرتبطة من خلال شبكة الألياف البصرية والشبكات اللاسلكية الفضاء السيبراني ليس الإنترنت فقط وإنما شبكات أخرى كثيرة متصلة مثل : gos/pstn/Gsm/Swift/Acars أما تعريف مصطلح الجريمة السيبرانية "هو السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية العالمية .

ويعرف مايكل آرون دينس الجريمة السيبرانية بأنها "هي جرائم سيبرانية، والتي أيضا جرائم الكمبيوتر ويتم استخدام الحاسب الآلي والانترنت فيها كأداة لتحقيق أهداف غير قانونية، مثل ارتكاب الاحتيال، والاتجار في المواد الإباحية للأطفال والملكية الفكرية، وسرقة الهويات، أو انتهاك الخصوصية".¹

ويعرفها الفقيه (merwe) أنها كل فعل غير مشروع الذي يتورط في ارتكابه الحاسب الآلي أو هو الفعل الإجرامي الذي يستخدم في اقتوافه الحاسب الآلي كأداة رئيسية.² لقد اختلفت تعريفات لمصطلح الجريمة السيبرانية، مما يصعب معه تقرير بإمكان إيجاد تعريف موحد باعتبار أن هذه الظاهرة حديثة نسبياً مما يحشى حصرها في نطاق واحد وبالتالي يصعب وضع تعريف جامع مانع للجريمة السيبرانية إذ أنها كما قيل تقاوم التعريف ولا يوجد لديها تعريف متفق عليه للدلالة عليها.³

كما أن تعدد المصطلحات المستخدمة للتعبير عن هذه الجرائم يعد دليلاً على مدى أهمية هذا الموضوع⁴، وعليه للجريمة السيبرانية مسميات عدة منها:

- ✓ جرائم الحاسوب والانترنت .
- ✓ جرائم التقنية العالية.
- ✓ الجريمة الإلكترونية .

¹ زياد بن محمد عادي العتيبي، "جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث : أشكالها ، خصائصها، أركانها والدوافع من ارتكابها"، المجلة الأكاديمية العالمية للدراسات القانونية، المجلد 3، العدد 1، 2020، ص 4 .

² عبد العال الديري، محمد صادق اسماعيل، الجرائم الإلكترونية (دراسة قانونية قضائية مقارنة)، المركز القومي للإصدارات القانونية، ط 1، القاهرة، 2012، ص 40 .

³ محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، دار النهضة العربية، القاهرة، 2009، ص 34.

⁴ أيمن عبد الله فكري، الجرائم المعلوماتية (دراسة مقارنة في التشريعات العربية والاجنبية)، مكتبة القانون والإقتصاد، ط 1، الرياض، 2014، ص 84 .

✓ جرائم أصحاب الياقات البيضاء¹.

❖ ثانياً : خصائص الجرائم السيبرانية

تتميز الجريمة السيبرانية بالعديد من الخصائص التي تميزها عن غيرها من الجرائم التقليدية ومن أبرز الخصائص التي تتميز بها الجريمة السيبرانية هي على النحو الآتي :

1. الحاسب الآلي هي الأداة الرئيسية في ارتكاب الجرائم السيبرانية:

لا يستطيع المجرم السيبراني بتنفيذ هجماته في بيئة سيبرانية إلا باستخدام أجهزة الحاسب الآلي المتصلة بشبكة الإنترنت فارتكاب هذه الجريمة تتطلب توفر وسائل التقنية الحديثة التي لا بد أن يكون لدى المجرم المعرفة والدراية في كيفية التعامل معها، وتعد أجهزة الكمبيوتر العادية والمحمولة وكذلك الأجهزة الذكية، وهي الأداة الرئيسية لارتكاب هذه الجرائم .

2. الجريمة السيبرانية جريمة خفية يصعب اكتشافها :

تختص الجريمة السيبرانية بالخفاء لأنها تقع في بيئة رقمية أو فضاء سيبراني لحدود له وفي الغالب لا يشعر بها المجني عليه كسرقة البيانات أو إرسال الفيروسات إلى جهاز المضيف، فمن ناحية تقنية يتم نقل المعلومات بواسطة النبضات الإلكترونية في صيغة أوامر رقمية². يلاحظ بأنها جرائم تفتقد إلى الآثار التقليدية، كما أن التخلص من تلك الأوامر الرقمية أمر في غاية البساطة خصوصاً عندما تكون الجريمة واقعية بسلوك جرمي واحد يمثل الضغط على أحد أزرار لوحة التحكم في الحاسب الآلي إلا أنها تقود إلى مشكلة أخرى أعقد وأخطر وهي صعوبة تحديد الفاعل وكشفه مما يجعل الصدفية المحضة الوسيلة لذلك كما يلاحظ بأن الأدلة التقليدية لا تنجح في إثبات هذه الجريمة، لأن الجرائم السيبرانية لا يمكن إثباتها إلا بدليل ذو طبيعة خاصة تنتمي إلى نفس الفضاء السيبراني التي تقع على الجريمة، ويحرص على عدم الظهور في مسرح الجريمة ومواجهة المجني عليه أو الجهة المستهدفة لخوفه من اكتشاف هويته .

¹ إسراء جبريل رشاد مرعي، "الجرائم الإلكترونية (الأهداف - الأسباب - طرق الجريمة ومعالجتها)"، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد 1، يناير 2018، ص 427.

² زياد بن محمد عادي العتيبي، المرجع السابق، ص 9-10 .

3. جريمة عابرة للحدود الوطنية والقارات :

وهذه هي إحدى الخصائص الهامة التي تتميز بها الجرائم السيبرانية، حيث أن المسرح الجنائي الخاص بها لا ينحصر في مكان معين أو دولة معينة، لأنها تتم في بيئة افتراضية لا حدود لها وبالتالي يعد الفضاء السيبراني حول العالم كله مسرحاً لها، وبإمكان المجرم السيبراني تنفيذ هجماته في أي مكان وزمان بالعالم، وهذا الأمر يعد بحد ذاته تحدي كبير في حقل الاختصاص القضائي والقانوني الواجب التطبيق من حيث الملاحقة والتحقيق والضبط والتفتيش، وعليه فإن الوصول إلى الحقيقة يستوجب الاستعانة بخبرة فنية ذات مهارة عالية وتكافل بين الدول عن طريق عقد الاتفاقيات المنظمة لهذا الشأن .

فلا يتواجد الفاعل في مسرح الجريمة، حيث تتباعد المسافات بين الفاعل والنتيجة، وهذه المسافات لا تقف كما أسلفنا عند حدود دولية معينة بل تمتد إلى النطاق الإقليمي لدول أخرى مما يضعف صعوبة اكتشافها أو ملاحقتها¹.

4. الجريمة السيبرانية جريمة ناعمة :

جرى تسمية الجرائم السيبرانية أو المعلوماتية للجرائم الناعمة، لأنها لا تتطلب استخدام الأساليب التقليدية في ارتكاب الجريمة وأيضاً لا تحتاج إلى مجهود بدني لارتكابها كما هو حال الجرائم التقليدية فلا يوجد دماء أو أسلحة مادية نتيجة لارتكابها بل تعتمد على تخطيط منظم ومعرفة باستخدام الأجهزة الذكية .

ويلاحظ بأن هذه الجرائم تتميز بأنها ترتكب بسرعة فائقة وفي وقت قصير وبأسلوب هادئ فهي لا تحتاج إلى العنف كالجرائم التقليدية، لذلك لا يتم اكتشافها إلى بعد مدة زمنية فهي تنصب على البيانات والمعلومات المخزنة في نظام المعلومات مما ينفي وجود أي أثر مادي أو تقليدي يمكن الاستعانة به في إثباتها، فالجرائم المعلوماتية ينتفي فيها العنف ولا توجد فيها آثار كما ذكرنا أعلاه وإنما هي أوامر وأرقام ودلالات تتغير أو تمسح من السجلات أو تستولي على البيانات وغيرها من الصور التي لا يمكن حصرها .

¹ المرجع السابق، ص 10 .

5. صعوبة إثبات الجريمة :

تختص الجرائم المرتكبة عبر استخدام شبكات الإنترنت بالغموض وصعوبة اكتشافها وفي رأي الباحث تكمن الصعوبة لأنها لا تترك أثراً تقليدياً كال بصمات فمعظم هذه الجرائم يتم اكتشافها على محض الصدفة وبعد وقت طويل من ارتكابها مما يشكل إلى صعوبة معرفة وإلمام ومهارة كافية في تقنية وعلوم الحاسب الآلي حتى يمكن اكتشافها وتتبعها¹.

6. التحديات والصعوبات القانونية :

التحديات والصعوبات القانونية التي تعرقل عملية متابعة الجناة التي تنجم عن مشاكل الحدود والولايات القضائية وذلك نظراً لكون الجريمة السيبرانية من طائفة الجرائم عابرة الحدود الوطنية.²

المطلب الثاني : أسباب الجرائم السيبرانية

هناك عدد من الأسباب التي يمكن حصرها كأسباب للجريمة السيبرانية (الإلكترونية) منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي. كما أن أسباب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه فردي، مجتمعي، كوني . فجرائم الشباب والهواة والصغار تختلف عن أسباب جرائم المحترفين، وتختلف وفق هدفها سرقة أو معلومات أو تجارة بالمعلومات أو الشخصية . ونذكر بعضاً من تلك الأسباب فيما يلي :

1. الرغبة في جمع المعلومات وتعلمها:

وأولئك الذين يرتكبون هذه الجرائم يقدمون عليها بغية الحصول على الجديد من المعلومات وقد أشار الأستاذ ليفي في أحد مؤلفاته الخاصة بقرصنة الأنظمة (HACKERS) إلى (أن أخلاقيات هؤلاء القراصنة تركز على مبدئين أساسيين هما الأول: أن الدخول إلى أنظمة الحاسب الآلي يمكن أن يعلمك كيف يسير العالم، والثاني أن جمع المعلومات يجب أن يكون غير خاضع للقيود). ومن وجهة نظر هؤلاء القراصنة فإن جميع المعلومات المفيدة بوجه عام يجب أن تكون

¹ زيد بن محمد العتيبي، مرجع السابق، ص 10 .

² محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية دراسة مقارنة، دار الفكر والقانون للنشر وتوزيع، ط1، المنصورة، 2021، ص 19 .

غير خاضعة للقيود وبعبارة أخرى أن تتاح حرية نسخها وجعلها تتناسب مع استخدامات الأشخاص. وكثيراً ما نجد أن قراصنة الأنظمة يعلنون أن هدفهم من الوصول للمعلومات ودخولهم للشبكات والحواسيب الإلكترونية هو التعلم فقط. فهم يتعاونون في البحث على شكل جماعات ويتقاسمون المعلومات والخبرات التي يحصلون عليها ويستفيدون منها في أنشطة هادفة ولو بطرق غير مشروعة .

2. الاستيلاء على المعلومات:

الإقدام على ارتكاب هذا الجرم بواسطة تقنية المعلومات بهدف الحصول على المعلومة ذاتها والاستيلاء عليها والتصرف فيها يتمثل ذلك في الحصول على المعلومة المحفوظة في الحاسب الآلي أو المنقولة أو تغييرها أو إلغائها نهائياً من النظام. ويختلف الدافع لهذا التصرف فقد يكون دافع تنافسي أو سببه الابتزاز أو الحصول على مزايا ومكاسب اقتصادية، كثيراً ما يكون هدف هذه الجرائم ذو طابع سياسي أو اقتصادي .

3. قهر النظام وإثبات التفوق على تطور وسائل التقنية:

في بعض الأحيان يكون الدافع وراء ارتكاب هذه الجرائم هو قهر النظام وإثبات قدرة الجاني وتفوقه على تعقيدات وتطور وسائل التقنية الحديثة، حيث يمضي كل وقته أمام شاشات أجهزته لكسر الحواجز الأمنية للأنظمة الإلكترونية واختراقها ليثبت براعته في القدرة على التحدي أي تطور جديد في عالم التقنية والتكنولوجيا. ويرتفع مؤشر الزيادة لدى فئات صغار السن من مرتكبي هذه الجرائم¹.

4. إلحاق الأذى بأشخاص أو جهات:

بعض المجرمين الذين يقدمون على ارتكاب الجريمة عبر شبكة المعلومات العالمية وتقنية المعلومات بالصورة عامة يركز الدافع من وراءها على إلحاق الأذى بأشخاص محددين أو جهات معينة، وغالبا ما تكون تلك الجرائم مباشرة تتمثل في صورة ابتزاز أو تهديد أو تشهير كما حصل في القضية التي ضبطها بإمارة دبي بدولة الإمارات العربية المتحدة عندما أقدم الجاني فيها ويلقب "بقرصان صور الفتيات" بالسطو على البريد الإلكتروني لمجموعة من الفتيات بتلك الدولة

¹ مجلس التعاون لدول الخليج العربية، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، 2016، ص 28 .

والاستيلاء غير مشروع على صورهن الشخصية وتعتمد نشرها على موقع خاص بشبكة الانترنت مع مجموعة الصور الإباحية . وكما يمكن ان تكون هذه الجرائم غير مباشرة وتتمثل في الحصول على البيانات والمعلومات الخاصة بتلك الجهات أو الأشخاص لاستخدامها فيما بعد في ارتكاب جرائم مباشرة .

5. تحقيق أرباح ومكاسب مادية:

هناك بعض الجرائم الالكترونية التي ترتكب يكون الدافع منها تحقيق أرباح ومكاسب مادية كاستخدام شبكة الانترنت للإعلان عن صفقات تجارية غير مشروعة كصفقات المخدرات والاتجار بالبشر وقد وردت في بحث أعده هشام بشير المستشار الإعلامي للجمعية المصرية لمكافحة جرائم الانترنت أن عصابات الإجرام المنظم استغلت التكنولوجيا الحديثة في تيسير شؤون الاتجار في البشر ويرى الباحث أن الاتجار بالبشر عبر الانترنت هو تجارة الإلكترونية حيث أن تعريف التجارة الإلكترونية تلك التعاملات التي تتم الكترونيا عبر شبكة المعلومات العالمية (الأنترنت).

6. تهديد الأمن القومي والعسكري :

بعض الجرائم الإلكترونية الهدف منها أسباب ودوافع سياسية كتهديد الأمن القومي والعسكري ومن ذلك ظهر ما يعرف بالتجسس الإلكتروني والإرهاب الإلكتروني والحرب المعلوماتية كما هو الحاصل بين الدول المتقدمة إلكترونيا¹.

7. ضعف تنفيذ القانون وتطبيقه في الجريمة الإلكترونية :

هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مجارة التقدم في الجرائم الإلكترونية وأساليبها . وهذا لا يتوقف عند التشريعات وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني، كما هو الحالي على المستوى الدولي. فما يغذي الجريمة الإلكترونية غياب التشريعات الجزائية والجنائية وضعف الممارسات العدلية والشرطية².

¹ مجلس التعاون لدول الخليج العربية، مرجع السابق، ص 29، 30 .

² المرجع السابق، ص 29، 30 .

8. التحول الرقمي للمجتمع :

دخل المجتمع اليوم عصر المعلوماتية الجديدة (أي فضاء الإلكتروني أو العالم الافتراضي). فالناس يقضون جزءاً من حياتهم اليومية في الفضاء الإلكتروني ينشئون الشبكات والمواقع ويتمتعون بأنواع جديدة من العلاقات الاجتماعية، وهم على تواصل مع ما يجري في العالم الخارجي، والقيام ببعض الأعمال. كل من هذه الأنشطة قد جعلت من الممكن للجميع وبوجود جهاز كمبيوتر أو مودوم مع معرفة التقنية القليلة. وبعبارة أخرى، فإن شبكة الانترنت هي من خلقت ما يعرف الآن باسم الفضاء الإلكتروني، أو العالم الافتراضي. يحتاج المجتمع لكي يقوم بوظائفه الى أن يعم الأمن والأمان وان يتحقق النظام والاستمرارية. ولا يتوقف توفر الأمن والأمان في الواقع المادي للمجتمع بل انتقل ليشمل العالم الافتراضي.

وهناك أسباب تتعلق بخصائص الجريمة الإلكترونية في حد ذاتها وفي ما يلي مجموعة من خصائص الجرائم الإلكترونية والتي تؤدي إلى ارتكاب الجريمة الإلكترونية منها :

- الإزالة Remivable : الجريمة الإلكترونية لا تتطلب الإزالة فيمكن نسخها فقط .
- التوافر Available : المعلومات في كل مكان، جاهزة لتستفيد منها الجريمة .
- القيمة Valuable : معلومات بطاقات الائتمان والحسابات المصرفية والتصاميم...
- الديمومة Durable : المعدات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة .
- سرعة التنفيذ : لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكثير وبضغط واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان الى آخر. وهذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة والتنفيذ عن بعد إذ لا تتطلب الجريمة الإلكترونية في أغلبها (إلى جرائم سرقة معدات الحاسب) وجود الفاعل في مكان الجريمة¹.

¹ راضية حميدة، مرجع السابق، ص 345، 346 .

المطلب الثالث : طرق وأشكال الجرائم السيبرانية

❖ أولاً : طرق الجرائم السيبرانية

وتشمل وليس حصراً على :

1. تخريب المعلومات وإساءة استخدامها ويشمل ذلك قواعد المعلومات المكتبات تمزيق الكتب تحريف السجلات الرسمية... إلخ .
2. سرقة المعلومات ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني أو الصناعي أو العسكري أو تخريبها أو تدميرها... إلخ .
3. تزوير المعلومات ويشمل الدخول لقواعد في النظم التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب .
4. تزيف المعلومات وتشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها .
5. انتهاك الخصوصية ويشمل نشر المعلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم أو وضع معلومات تخص تاريخ الأفراد ونشرها.
6. التصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف .
7. التجسس ويشمل اعتراض المعلومات ومحاوله معرفة ما يقوم به الأفراد .
8. التشهير ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة .
9. السرقة العلمية الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية .
10. سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها .
11. الدخول غير القانوني للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات .
12. قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى¹ .

¹ اسراء جبريل رشاد مرعي، مرجع السابق، ص. 441-443.

13. قرصنة البيانات والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر .
14. خلاعة الأطفال وتشمل نشر الصور خاصة للأطفال "الجنس السياحي" للأطفال خاصة وللإناث على الشبكات بشكل عام ونشر الجنس التخليبي .
15. القنابل البريدية وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة إلكترونية .
16. إفشاء الأسرار وتشمل الحصول على معلومات خاصة جداً ونشرها على الشبكة .
17. الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو المالية أو الهاتف... إلخ .
18. سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان .
19. التحرش الجنسي ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة أو المحادثة أو الملامسة .
20. المطاردة والملاحقة والابتزاز وتشمل ملاحقة الذكور للإناث أو العكس والتتبع بقصد فرض إقامة علاقة ما وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل .
21. الإرهاب الإلكتروني ويشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب ومصادرة هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني¹.

ثانياً : أشكال الجرائم السيبرانية

1) الجرائم الاقتصادية :

تتنوع الجرائم الاقتصادية بتنوع النظام السائد في الدولة فعلى سبيل المثال في الدول الرأسمالية نجد أن أغلب الجرائم الاقتصادية تتمحور حول الاحتكارات والتهرب الضريبي والجمركي والسطو على المصارف وتجارة الرقيق الأبيض و الاطفال، في حين تتمحور تلك الجرائم في النظام الاشتراكي على الرشوة والاختلاس والسوق السوداء، وهذا لا يعني بالضرورة أنه لا يمكن ارتكاب كل أنواع

¹المرجع السابق، ص 441- 443 .

الجرائم في مجتمع واحد حيث يمكن أن نجد في المجتمع الرأسمالي مثلاً جرائم رشوة واختلاسات والعكس صحيح .

وكما في الجرائم الأخرى فإن الانترنت ساهم في تطوير طرق وأساليب ارتكاب هذه الجرائم وتوسيع منطقة عملها خاصة مع توجه الكثير من الدول في التحول إلى الحكومات الإلكترونية كما في دولة الإمارات العربية المتحدة مثلاً، حيث استفاد المجرمون من التقدم التقني في اختلاس الأموال وتحويل الأرصدة النقدية وكذلك في سرقة التيار الكهربائي والمياه وخطوط الهاتف والعبث بها وإتلافها .

وتتعدد الآثار السلبية لهذا النوع من الجرائم، فمن الناحية الاقتصادية تكلف الدول أموالاً طائلة حيث قدرت الخسارة العالمية الناجمة عن تلك الجرائم عام 2007 بنحو 200 مليار، وتقدر خسائر الأمريكيين وحدهم بحوالي 240 مليون دولار¹ .

وتتمثل انعكاسات الجريمة الإلكترونية على الاقتصاد العالمي ب :

أ : الخسارة المالية بسبب الابتزاز :

تمت في مصر عملية ابتزاز عن طريق الشبكة العنكبوتية وذلك بتهديد شركة مياه غازية بنشر صورة لأحد منتجاتها وبداخلها حشرة، ولكن لم ترضخ الشركة إلى تهديد ونشر المبتزون الصورة وشاهدها 3700 شخص وتم التعرف على المبتزون واعترفوا بجرمهم .

ب : الخسارة المالية بعض الموظفين المطرودين :

"تيموثي ألن ليود" هو مصمم ومبرمج فصل من عمله، فما كان منه إلا أن أطلق قنبلة إلكترونية ألغت كافة التصاميم وبرامج الانتاج لأحد أكبر مصانع التقنية العالية في نيوجرسي التي تعمل لحساب وكالة الفضاء NASA والبحرية الأمريكية .

ج : الخسارة المالية بسبب سرقة المعلومات الشخصية :

في بنك لويدز في امستردام تم تحويل مبلغ 8.4 مليون دولار الى بنك في سويسرا من قبل شاب عمره 26 عام .

¹ بشرى حسين الحمداني، القرصنة الإلكترونية أسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، ط1 ، الأردن - عمان ، 2014 ، ص62.

في عام 200م ، جرى السطو على 33 ألف جهاز صرف آلي ATM في بريطانيا، وقد كانت الخسارة المالية كبيرة بنحو 15 مليون جنيه إسترليني .

ولا يزال هناك قلق عالي كبير على المستوى الأمني والاقتصادي والإداري نتيجة الاختراقات الإلكترونية المتعددة التي تشهدها المنشآت مما جعل من أمن المعلومات هاجسا لدى الدول والشعوب والمنظمات والشركات والمنشآت الاقتصادية وذلك على كافة المستويات الأمنية والإدارية والاقتصادية .

وطالب خبراء اقتصاديون ومختصون في أمن المعلومات بضرورة تطبيق معايير عالية في مجال حماية المعلومات في كافة المنشآت الوطنية خاصة البنوك والمنشآت التي يحتم عليها حفظ معلومات ضخمة سواء للأفراد أو المنشآت .¹

(2) الجرائم الاجتماعية :

■ الهندسة الاجتماعية:

وهي شكل من أشكال جرائم الابتزاز الإلكتروني تقوم على التلاعب النفسي بالأشخاص لإرغامهم على فعل أنشطة غير قانونية أو الإفشاء عن معلومات سرية وهي من أشهر أنواع الاحتيال .

■ لعبة القمار :

تنتشر اندية القمار على الإنترنت وعادة ما تكون محل اشتباه ومراقبة من قبل السلطات الأمريكية وبالرغم من أن سوق القمار في أمريكا يعتبر الأسرع نموا على الإطلاق إلا أن المشكلة القانونية التي تواجه أصحاب مواقع القمار الافتراضية على الإنترنت أنها غير مصرح لها حتى الآن في أمريكا بعكس نوادي القمار الحقيقية كالمنتشرة في لاس فيجاس وغيرها، ولذلك يلجأ بعض أصحاب تلك المواقع الافتراضية على الإنترنت إلى انشائها وإدارتها من أماكن مجاورة لأمريكا وخاصة في جزيرة انتيجوا على الكاريبي².

ويوجد على الإنترنت أكثر من ألف موقع للقمار يسمح لمرتاديه من مستخدمي الإنترنت بممارسة جميع أنواع القمار التي توفرها المواقع الحقيقية ومن المتوقع أن ينفق الأمريكيون ما يزيد

¹ المرجع السابق، ص. 71-73.

² أنواع الجرائم الإلكترونية، www.cyberone.com، بتاريخ: 2023/04/1، على الساعة: 13:41 .

عن (600) مليار دولار سنويا في اندية القمار وسيكون نصيب مواقع الانترنت منها حوالي مليار دولار .

ولقد حاول المشرعون الأمريكيون تحريك مشروع قانون يمنع المقامرة عبر الانترنت ويسمح بملاحقة الذين يستخدمون المقامرة السلكية أو الذين يروجون لها سواء كانت هذه المواقع في امريكا أو خارجها .

■ تجارة المخدرات :

لم تقتصر المواقع المنتشرة على الانترنت بالترويج للمخدرات بل تعداه الى تعليم كيفية زراعة وصناعة المخدرات بكافة اصنافها وان انواعها وبأبسط الوسائل المتاحة، والأمر الذي يدفع بالقارئ ومعظمهم من المراهقين الى تطبيق ما يقرأه .

ويؤكد هذه المخاوف أحد الخبراء التربويين في بالولايات المتحدة والذي أكد أن ثمة علاقة يمكن ملاحظتها بين ثالث المراهقة والمخدرات.

ولا تقتصر ثقافة المخدرات على تلك المواقع فقط بل تساهم المنتديات وغرف الدردشة في ذلك أيضا.

وبالرغم من انتشار المواقع الخاصة بالترويج للمخدرات وتعليم كيفية صنعها إلا أن هذه المواقع لم تدق جرس الإنذار بعد ولم يهتم بآثارها السلبية وخاصة على الشيء كما فعلته المواقع الاباحية وخاصة في الدول التي تعرف باسم الدول المتقدمة .

■ جرائم الاتجار بالبشر عن طريق الانترنت :

وتتمثل هذه الجريمة بإنشاء أو نشر موقع على شبكة الانترنت بقصد الاتجار بالبشر أو تسهيل التعامل به بأي شكل من الإشكال أو روج له أو ساعد على ذلك أو تعاقد أو تعامل أو تفاوض بقصد إبرام الصفقات المتعلقة بالاتجار بالبشر أن المخاوف من استخدام الانترنت لا تقتصر على ارتكاب الجريمة بل تساهم بعض المواقع في انحراف الشباب وخصوصا من المراهقين، وذلك من خلال إنشاء مواقع الالكترونية بقصد الاتجار بالمخدرات أو المؤثرات العقلية أو الترويج لها أو تعاطيها أو سهل التعامل فيها أو تعاقد أو تعامل أو تفاوض بقصد إبرام الصفقات المتعلقة بالاتجار بها بأي شكل من الإشكال¹.

¹ بشرى حسين الحمداني، مرجع السابق، ص.75-78.

(3) الجرائم الثقافية :

تعرف الجرائم الثقافية على أنها استيلاء المجرم على الحقوق الفكرية ونسبها له من دون موافقة الضحية فمن الممكن أن تكون أحد الصور التالية :

- قرصنة البرمجيات : هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على أسطوانات وبيعها للناس بسعر أقل .
 - التعدي على القنوات الفضائية المشفرة وإتاحتها عن طريق الانترنت عن طريق تقنية (soft copy).
 - جرمية نسخ المؤلفات العلمية والأدبية بالطرق الالكترونية المستخدمة .
- جرائم قرصنة البرامج :

تعرف قرصنة البرامج بأنها الاعتداء بالنسخ أو الاستعمال غير المشروع لبرامج الكمبيوتر المحمية بموجب قوانين حق المؤلف، وطبقا لإحصائية اتحاد منتجي البرامج لعام 200 تصل نسبة القرصنة إلى 56% بينما تقدر الخسائر بـ 12 مليون دولار وتلحق قرصنة البرامج الضرر بكل الشركات المنتجة لبرامج الكمبيوتر بالإضافة إلى المستخدمين أنفسهم، وهي تؤدي إلى ارتفاع أسعار البرامج بالنسبة إلى المستخدمين وإلى انخفاض مستوى الدعم الفني للبرامج كما أنها تتسبب في تأخير تمويل عمليات تطوير برامج جديدة مما يؤدي بالتالي إلى تدهور مستوى صناعة البرامج ككل.

كذلك تلحق القرصنة أضراراً بكل من ناشري وموزعي برامج الكمبيوتر أيا كان حجمهم، فمطورو البرامج ينفقون أعواماً لتطوير برنامج، وهناك جزء من المقابل المالي الذي يحصل عليه مطورو البرنامج يوجه إلى تطوير برامج جديدة بحيث تستمر تلك البرامج في التطور والتقدم نحو الأفضل .

وكشفت جمعية منتجي برامج الحاسوب التجارية (بي.أس.أي) عن تفاصيل الدراسة العالمية السنوية التاسعة حول قرصنة البرمجيات، حيث ظهر أن المعدل الإجمالي لقرصنة البرمجيات في الشرق الأوسط وإفريقيا بلغ 58% عام 2011، في حين وصلت القيمة التجارية للبرمجيات غير المرخصة نحو 4.2 مليارات دولار¹.

¹ المرجع السابق، ص. 75-78 .

■ انتهاك الخصوصية :

تتفق التشريعات السماوية والأنظمة الوضعية على ضرورة احترام خصوصية الفرد ويعتبر مجرد التطفل على تلك المعلومات سواء كانت مخزنة في الحاسب الآلي أو في بريده الإلكتروني أو في أي مكان آخر انتهاكاً لخصوصيته الفردية .

وأدى انتشار الأنترنت إلى تعرض الكثير من مستخدمي الأنترنت لانتهاك خصوصياتهم الفردية سواء عمداً أو مصادفة، فبكل بساطة ما أن يزور مستخدم الأنترنت أي موقع على شبكة الأنترنت حتى يقوم ذلك الموقع بإصدار نسختين من الكعكة الخاصة بأجهزتهم (Cookies) وهي نصوص صغيرة يرسلها العديد من مواقع الويب لتخزينها في جهاز من يزور تلك المواقع لعدة أسباب لعل منها التعرف على من يكرر الزيارة للموقع أو لأسباب أخرى، وتبقى واحدة من الكعكات في الخادم (السيرفر) الخاص بهم والأخرى يتم تخزينها على القرص الصلب لجهاز الزائر للموقع في أحد الملفات التي قامت الموقع الأخرى بتخزينها من قبل دون أن يشعر صاحب الجهاز بذلك أو حتى الاستئذان منه، وفورا يتم اصدار رقم خاص ليميز ذلك الزائر عن غيره من الزوار وتبدأ الكعكة بأداء مهمتها بجمع المعلومات وإرسالها الى مصدرها أو إحدى شركات الجمع والتحليل للمعلومات وهي عادة ما تكون شركات دعاية وإعلان وكلما قام ذلك الشخص بزيارة الموقع يتم إرسال المعلومات وتحديد النسخة الموجودة لديهم ويقوم المتصفح لديه بعمل المهمة المطلوبة منه ما لم يقوم صاحب الجهاز بتعديل وضعها وقد تستغل بعض المواقع المشبوهة هذه الكعكات بنسخ تلك الملفات والاستفادة منها بطريقة أو بأخرى .

كما قد يحصل أصحاب المواقع على معلومات شخصية لصاحب الجهاز طوعا حيث يكون الشخص عادة اقل ترددا عندما يفشى معلوماته الشخصية من خلال تعامله مع جهاز الحاسب الآلي بعكس لو كان الذي يتعامل معه إنسان آخر¹.

وهناك وسائل لحماية الخصوصية أثناء تصفح الأنترنت، ولكن " من الصعب جدا السيطرة على ما يحدث للمعلومة بمجرد خروجها من جهاز الحاسب الآلي وعلى ذلك فإن حماية الخصوصية

¹ المرجع السابق، ص 79.

يجب أن تبدأ من البداية بتحديد نوعية البيانات التي لا ينبغي أن تصبح عامة ومشاعة ثم بتقييد الوصول الى تلك المعلومات"¹.

والخصوصية حق مستقل يحمي الفرد من الاعتداءات المادية والمعنوية التي تطال حياته الخاصة.²

4) الابتزاز الإلكتروني :

الابتزاز الإلكتروني هو إحدى الجرائم المستحدثة التي يقوم فيها الجاني باستخدام مهاراته الفنية ومعرفته بخبايا التكنولوجيا، وعن طريق امتلاكه لبرمجيات متطورة تستطيع اختراق المواقع الشخصية أو البيانات المخزنة على أي أداة متصلة بالانترنت أو بأي شبكة محلية أو دولية أخرى يستطيع الحصول بواسطتها على بيانات بمختلف أشكالها سواء من أفراد أو من منظمات، بهدف استخدام هذه البيانات للحصول عن طريق الابتزاز على ما يريد سواء لغاية شخصية في نفسه أو لتحقيق غاية يطلبها طرف آخر منه وتنفيذ طلبات لمصلحة جهة أخرى.³

5) الجرائم السياسية :

تتعدد أشكال الجريمة السياسية :

- تستخدم المجموعات المسلحة حالياً تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل : الاتصالات والتنسيق وبث الأخبار المغلوطة وتوظيف بعض صغار السن وتحويل بعض الأموال في سبيل تحقيق أهدافهم " .
- الاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات وذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية والسهلة الاستخدام والتي يمكن تحميلها مجاناً .
- نشر الأفكار الخاطئة بين الشباب كالإرهاب والإدمان والزنا لفساد الدولة لأسباب سياسية واقتصادية بالدرجة الأولى .

المرجع السابق، ص. 79-84.¹

² مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الإتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، ط1، مصر، 2016، ص39 .

³ زهراء عادل سلي، جريمة الابتزاز الإلكتروني دراسة مقارنة، شركة دار الأكاديميون للنشر والتوزيع، ط1، الأردن، 2020 ، ص36.

المواقع المعادية :

يكثر انتشار الكثير من المواقع الغير المرغوب فيها على شبكة الإنترنت فمصطلح المواقع المعادية هو مصطلح حديث بدأ استخدامه بعد هذا التطور التكنولوجي في مجال شبكة الإنترنت فقام مصممي المواقع المعادية باستغلال التكنولوجيا لخدمة أغراضهم الشخصية، ومن هذه المواقع ما يكون موجهاً ضد سياسية دولة أو ضد عقيدة أو مذهب أو حتى ضد شخص ما، وهي تهدف في المقام الأول إلى تشويه صورة الدولة أو المعتقد أو الشخص المستهدف، وتصنف المواقع المعادية وفقاً للغرض منها كآتي :

● المواقع السياسية المعادية :

قد ينظر البعض إلى إنشاء تلك المواقع كظاهرة حضارية تتمشى مع الديمقراطية والحرية الشخصية، ولكن الواقع غالباً ما يكون الغرض من وراء إنشائها هي معارضة النظام السياسي القائم في بلد ما فيحاولون من خلال تلك المواقع نشر الأخبار الفاسدة التي تنشر بين الفرقة بين أفراد الشعب ونظامه السياسي القائم¹.

فقد صدق مكتب التصديق على الأحكام بمجلس الوزراء على الحكم الذي أصدرته محكمة أمن الدولة العليا ضد جميع المتهمين في قضية حزب التحرير والبالغ عددهم 26 منهما وعاقبت المحكمة 12 منهما بينهم ثلاثة بريطانيين بالسجن 5 سنوات، 7 متهمين بالسجن، وسنة واحدة لـ 7 متهمين آخرين، حيث انه في عام 2002م اتهمت نيابة أمن الدولة العليا المذكورين بالترويج بالقول والكتابة لأغراض جماعة أسست على خلاف أحكام القانون تسمى حزب التحرير، وتدعو إلى تعطيل أحكام الدستور والقانون، ومنع مؤسسات الدولة من مباشرة عملها والترويج لأفكار الحزب عبر المنشورات وإنشاء موقع على شبكة الإنترنت يدعو لهذه الأفكار وتكفير النظم الحاكمة.

● المواقع الدينية المعادية :

ويكون الغرض من إنشاءها الإساءة إلى دين معين من الأديان ونشر الأفكار السيئة عنه وحث الناس على الابتعاد عنه، وتلك المواقع غالباً يكون القائمين عليها من معتنقي الديانات الأخرى المتشددون في دينهم أو أن يكون هدفهم بث الشقاق والخلاف في ما بين أفراد الشعب

¹ بشرى حسين الحمداني، المرجع السابق، ص 62.

الواحد فيحاولون إثارة الفتنة عن طريق نشر الأخبار الكاذبة والمندسوسة وذلك لتحقيق هدفهم الخبيث .

● المواقع المعادية للأشخاص أو الجهات :

وهي تشبه إلى حد كبير بالمواقع المخصصة للقدف، حيث تهدف أساساً لتشويه سمعة الشخص أو الجهة .

انتحال الشخصية وينقسم إلى نوعين :

أ- انتحال شخصية الفرد :

تعتبر جرائم انتحال الشخصية من الجرائم القديمة إلا أن التنامي المتزايد لشبكة الإنترنت أعطى المجرمين قدرة أكبر على جمع المعلومات الشخصية المطلوبة عن الضحية والاستفادة منها في ارتكاب جرائمهم فتنتشر في شبكة الانترنت الكثير من الإعلانات المشبوهة والتي حاول البعض الاستيلاء على معلومات اختيارية من الضحية، فهناك مثلاً اعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية والذي يتطلب بطبيعة الحال الإفصاح عن بعض المعلومات الشخصية كالاسم والعنوان والأهم رقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية، وبالرغم من أن مثل هذا الإعلان من الواضح بمكان أنه عملية نصب واحتيال إلا أنه ليس من المستبعد أن يقع ضحيته الكثير من مستخدمي الإنترنت¹.

ويمكن أن تؤدي جريمة انتحال الشخصية الى الاستيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية أو حتى الإساءة إلى سمعة الضحية².

ب- انتحال شخصية المواقع :

مع أن هذا الأسلوب يعتبر حديث نسبياً إلا أنه أشد خطورة وأكثر صعوبة في اكتشافه من انتحال شخصية الأفراد، حيث يمكن تنفيذ هذا الأسلوب حتى مع المواقع التي يتم الاتصال بها من خلال نظم الاتصال الآمن (Secured Server) حيث يمكن وبسهولة اختراق مثل هذا الحاجز الأمني وتتم عملية الانتحال بهجوم يشنه المجرم على المواقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بديل، أو يحاول المجرم اختراق موقع لأحد مقدمي الخدمة المشهورين ثم يقوم بتركيب

¹المرجع السابق، ص. 71-73 .

²المرجع نفسه ، ص73.

البرنامج الخاص به هناك مما يؤدي الى توجيه أي شخص الى موقعه بمجرد كتابة اسم الموقع المشهور.

ويتوقع أن يكثر استخدام أسلوب انتحال شخصية المواقع في المستقبل نظراً لصعوبة اكتشافها .

ج- استخدام الانترنت في ارتكاب الجريمة المنظمة :

وهي استخدام شبكة الانترنت بقصد إشاعة الفوضى بقصد إضعاف النظام أو الثقة بالنظام الالكتروني للدولة أو إتلاف وتعطيل أو إعاقة أو الأضرار بأنظمة الحاسوب أو شبكة المعلومات العائدة للدولة بقصد إضعاف الثقة بالنظام المالي الالكتروني أو الأوراق التجارية والمالية للدولة واستخدام الانترنت في ارتكاب جرائم غسيل الأموال حيث يأخذ المجرمون بأحدث التقنيات لغرض خدمة نشاطاتهم سيما وأن جرائم غسيل الأموال عابرة للحدود .

تزوير البيانات من الجرائم المعلوماتية الأكثر انتشاراً فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من أشكال التزوير للبيانات من خلال تزوير أو تقليد أو اصطناع توقيع أو سند أو كتابة الكترونية أو أية وسيلة أخرى أو استعمال البطاقة الالكترونية المقلدة أو المزورة مع علمه بذلك أو اصطناع عمداً وثائق أو سجلات أو قيود الكترونية أو أحدث تغييراً أو تلاعب في سند الكتروني صحيح و الاستيلاء عمداً على توقيع أو كتابة أو سند واستخدامها لمصلحته الشخصية .

6) الجرائم الجنسية :

هذا النوع من الجريمة يمكن أن يتمثل بإحدى الصور التالية :

- **التغريب والإستدراج** : في العادة تتواجد هذه الصورة عندما يتعرف أحد الشبان على إحدى الفتيات في الشات أو في برامج المحادثة ويكون علاقة معها ثم يستدرجها بالكلام المعسول ويوهمها بالزواج لكي تثق به ومن ثم يقوم بتهديدها وفضيحتها بما يملكه من يملكه من صور أو تسجيلات لصوتها إن لم تستجيب لطالباته .

- **انتشار الصور ومقاطع الفيديو المخلة بالآداب على مواقع الانترنت :**

من قبل الغزو الفكري لكي يتداولها الشبان والشابات وإفساد أفكارهم وإضعاف إيمانهم¹ .

¹ بشرى حسين الحمداني، نفس المرجع السابق ، ص 71-62-73.

(7) الجريمة المادية (Financial Crime) :

وهي التي تسبب أضراراً مالية على الضحية أو المستهدف من عملية النصب وتأخذ واحدة من الأشكال الثلاثة التي سوف استعرضها بشرح مختصر مثل :

- عملية السرقة الإلكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك كتلك المنتشرة الآن في الكثير من الدول الإفريقية وخاصة جنوب إفريقيا وفيها يتم نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية .
- إنشاء صفحة انترنت مماثلة جداً لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة (Phishing) لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها .

- رسائل البريد الواردة من مصادر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج مع الوعد بنسبة من المبلغ، أو تلك التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي .

● الإغراق بالرسائل :

يلجأ بعض الأشخاص إلى ارسال مئات الرسائل إلى البريد الإلكتروني لشخص ما يقصد الاضرار به حيث يؤدي ذلك إلى تعطيل الشبكة وعدم امكانية استقبال أي رسائل فضلاً عن امكانية انقطاع الخدمة .

واذا ما تعرض الشخص العادي لمحاولة الاغراق بالرسائل حيث لن يصمد بريده طويلاً امام السيل المنهمر من الرسائل عديمة الفائدة أو التي قد يصاحبها فيروسات أو صور أو ملفات كبيرة الحجم، خاصة اذا علمنا أن مزود الخدمة عادة يعطي مساحة محددة للبريد لا تتجاوز عشرة "ميغا" كحد أعلى¹.

¹ المرجع السابق ص 88، 89 .

المبحث الثالث : المجرم السيبراني

المطلب الأول : تعريف المجرم السيبراني وسماته

❖ أولاً : تعريف المجرم السيبراني (المعلوماتي)

لا شك أن الشخص الذي يرتكب الفعل غير المشروع ويعتدي فيه على حق من حقوق الغير بالمعنى الواسع، يعد في نظر القانون مجرماً ويتعرض للعقاب إذا ما اقترف جريمته، ولذلك فإن العقوبة لكي تحقق هدفها المباشر أو غير المباشر أي تحقيق هدفها في مجال الردع العام أو الخاص، وإذا كنا في مجال الإجرام المعلوماتي من حيث الظروف التي دفعته لارتكاب جريمته وأسبابها وصفاته وذلك حتى يمكن إعادة تأهيله اجتماعياً ويعود إلى حظيرة المجتمع كمواطن صالح ينفع المجتمع ولا يضره.

والمجرم المعلوماتي هو المجرم الذي له القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الالكتروني الرقمي وملحقاته ووسائل الاتصال الرقمية وذلك بأداء فعل أو الامتناع عنه مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محلياً أو دولياً .

والمجرم المعلوماتي يحتاج لممارسة جريمته إلى الولوج غير المشروع على ذاكرة الحاسب الآلي لكي يلتقط المعلومات المخزنة أو يعدل عليها .

ولطالما ارتبطت شخصية المجرم المعلوماتي بصورة الطالب في مجال العلوم المعلوماتية أو في صورة ذلك الشخص المهووس تقنية المعلوماتية، والذي لا يستهدف من خلاله فعله سوى اختبار قدراته في مواجهة النظم المعلوماتية، غير أن التحول الجذري من حيث مدى خطورة هذه الأفعال دفع وبصفة تدريجية إلى تصنيفها ضمن مجال الاعتداءات التي تدرج في صنف الجريمة المنظمة¹ .

❖ ثانياً : سمات المجرم السيبراني

لم يكن لارتباط الجريمة المعلوماتية بالحاسوب والإنترنت أثراً على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثر أيضاً على تمييز المجرم المعلوماتي عن غيره من

¹ عامر محمد الحبيب عبد القادر، المجرم المعلوماتي، مذكرة شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2018/2019.

المجرمين واتصافه بسمات معينة جعلت منه محلاً للعديد من الأبحاث والدراسات، ويتميز المجرم المعلوماتي بعدد من السمات والخصائص هي :

(1) المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء :

يتمتع مجرمو المعلوماتية بقدر لا يستهان به من المهارة والمعرفة بتقنيات الحاسوب والانترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آلياً. فتنفيذ الجريمة المعلوماتية يتطلب قدراً من المهارة لدى الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات .

إن المجرم المعلوماتي يمكن أن يكون تصوراً كاملاً لجريمته، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته، وذلك حتى لا يفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو الكشف عنها .

يتميز المجرم المعلوماتي غالباً بالذكاء، حيث أن الجريمة المعلوماتية تتطلب مقدرة عقلية وذهنية عميقة خاصة في الجرائم المالية التي تؤدي إلى خسارة مادية كبيرة تلحق بالجنح عليه، فالمجرم المعلوماتي يستخدم قدرته العقلية ولا يلجأ الى استخدام العنف أو الإكراه بل يحاول أن يحقق أهدافه بهدوء .

الإجرام المعلوماتي هو إجرام الأذكى بالمقارنة بالإجرام التقليدي الذي يميل الى العنف، فالمجرم المعلوماتي يسعى بشغف إلى معرفة طرق جديدة مبتكرة لا يعرفها احد سواء وذلك من اجل اختراق الحواجز الأمنية في البيئة الالكترونية ومن ثم نيل مبتغاه¹ .

(2) المجرم المعلوماتي يبرر ارتكابه لجريمته :

يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي أن مال يقوم به لا يدخل في عداد الجرائم أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في الأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصادياً تحمل نتائج تلاعبهم .

¹ نخلا عبد القادر مومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، ط1، ط2، عمان، 2008/2010، ص.ص 77-83.

فهؤلاء الأشخاص لا يدركون أن سلوكهم يستحق العقاب، ويبدو أن الاستخدام المتزايد للأنظمة المعلوماتية قد انشأ مناخاً نفسياً موائماً لتصوير استبعاد فكرة الخير والشر وقد ساعد على ذلك عدم وجود احتكاك مباشر بالأشخاص، ومما لا شك فيه أن هذا التباعد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل ففي كثير من الأحيان يقوم العاملون بالمؤسسات المختلفة باستخدام أجهزة الحاسوب لأغراض شخصية بوصفه سلوكاً شائعاً بين الجميع ولا ينظر إليه بوصفه فعلاً إجرامياً .

إلا أن ذلك لا يعني أن عدم الشعور بعدم أخلاقية هذه الأفعال الإجرامية المعلوماتية لدى فئة كبيرة ينفي وجود مجرمين يرتكبون الإجرام المعلوماتي وهم على علم وإدراك بعدم مشروعية وأخلاقية هذا الفعل، فهناك فئة لديها اتجاه إجرامي خطير وسوء نية واضح وهم على إدراك بخطورة أفعالهم .

(3) المجرم المعلوماتي إنسان اجتماعي :

المجرم المعلوماتي هو عادة إنسان اجتماعي قادر على التكيف في بيئته الاجتماعية بل إن بعضهم يتمتع بثقة كبيرة في مجال عمله، فالمجرم المعلوماتي يتميز بأنه لا يضع نفسه في حالة عداء مع المجتمع الذي يحيطه بل إنه إنسان قادر على التوافق والتصالح مع مجتمعه . فهو إنسان مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع، فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف ولا يعني ذلك تقليل من شأن المجرم المعلوماتي بل إن خطورته الإجرامية قد تزداد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه . شعور المجرم أنه محل ثقة من مجتمعه وشعوره بأنه خارج إطار الشبهات قد يدفعه إلى التمادي في ارتكاب جرائمه التي قد لا تكتشف، وإذا اكتشفت فإنها تواجه صعوبة الإثبات ونقص الأدلة ونقص الخبرة لدى المحققين ولدى رجال القضاء¹ .

¹ أهلا عبد القادر مومني، مرجع السابق، ص.ص 77-83 .

(4) خوف المجرم المعلوماتي من كشف جريمته :

يتصف مجرمو المعلوماتية بالخوف من كشف جرائمهم وافتضاح أمرهم، وبالرغم من أن هذه الخشية تصاحب المجرمين على اختلاف أنماطهم إلا أنها تميز مجرمي المعلوماتية بصفة خاصة لما يترتب على كشف أمرهم من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان . ويساعد مجرمي المعلوماتية على الحفاظ على سرية أفعالهم طبيعة الأنظمة المعلوماتية نفسها، ذلك أن أكثر ما يعرض المجرم إلى اكتشاف أمره هو أن يطرأ أثناء تنفيذه لجريمته عوامل غير متوقعة لا يمكن التنبؤ بها، في حين أن أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي أن الحواسيب إنما تؤدي عملها غالباً بطريقة آلية بحيث لا تتغير المراحل المختلفة التي تمر بها أي من العمليات التي يقوم بها من مرة إلى أخرى وهو ما يساعد على عدم كشف الجريمة طالما أن جميع خطوات التنفيذ معروفة مسبقاً حيث لا يحتمل أن تتدخل عوامل غير متوقعة يكون من شأنها الكشف عن الجريمة .

وهذه الخشية لدى مجرمي المعلوماتية من اكتشاف أفعالهم مردها انتماؤهم في الغالب الأعم إلى وسط اجتماعي متميز، سواء من حيث التعليم أو الثقافة أو المستوى المهني وطبيعة العمل . أثبتت الدراسات أن غالبية مرتكبي الجرائم المعلوماتية غير قادرين على ارتكاب الجرائم التقليدية خاصة لتلك التي تتطلب مواجهة مع المجني عليه فالجرم المعلوماتي لا يستطيع الاعتداء على المجني عليه بطريقة مباشرة إلا أنه لا يرى غضاضة في أن يكون هذا الاعتداء عن طريق البيئة الالكترونية.

(5) المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي :

ويقصد بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي التي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الشيفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات، والتي تعطي الفاعل مزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو المعلومات أو تعديلها¹ .

¹ المرجع السابق، ص.ص 77-83.

وقد تتمثل هذه السلطة في الحق في استعمال الأنظمة المعلوماتية، أو إجراء بعض التعاملات، أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة .

المطلب الثاني : فئات المجرم السيبراني

إن التسارع المذهل الذي يشهده عالم المعلوماتية والتقنيات الرقمية الحديثة انعكس بدوره على الجرائم التي ترتكب في البيئة التقنية الالكترونية فأصبحنا أمام جرائم مستحدثة سريعة التطور مرتكبوها ماهرون في ابتكار الأساليب الحديثة لخرق الحواجز الأمنية في هذا العالم الرقمي مستخدمين خبراتهم ومهاراتهم الذهنية والعقلية .

وأمام هذا التطور والتغير السريع في أنماط الجريمة المعلوماتية وصورها فقد يكون من الصعب وضع تصنيف ثابت لطوائف مجرمي المعلوماتية، ولكن يمكن لنا وفقاً لما توصلت له الدراسات والأبحاث التي تناولت مجرمي المعلوماتية أن نبين بعض هذه الأنماط لهؤلاء المجرمين، ولكن لا بد من الإشارة أولاً إلى أن هذه التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة محددة دون غيرها من الفئات المذكورة بل يمكن أن يكون المجرم الواحد مزيجاً من أكثر من طائفة أو فئة .

■ الفئة الأولى : صغار مجرمي المعلوماتية :

كما يسميهم البعض صغار نوابغ المعلوماتية ويقصد بهم الشباب البالغ المفتون بالمعلوماتية وأنظمتها .

وقد تباينت الآراء بالنسبة لهذه الطائفة، حيث يرى البعض أنه لا يبدو من المناسب أن نصنف هؤلاء الشباب في طائفة أو أخرى من الطوائف الإجرامية لأن لديهم ببساطة ميلاً للمغامرة والتحدي والرغبة في الاكتشاف ونادراً ما تكون أهداف أفعالهم المحظورة غير شريفة وهم لا يدركون ولا يقدرّون مطلقاً النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشأة أو شركة تجارية¹ .

بينما هناك اتجاه آخر يناصر هذه الفئة ويعتبرها ممن يقدم خدمة لأمن المعلومات ووسائل الحماية ويصفهم بالأخبار ويتمادى هذا الاتجاه في تقديره لهذه الفئة باعتبارهم لا يسببون ضرراً

¹ خلا عبد القادر مومني، مرجع السابق، ص.ص-78-83.

للنظام ولا يقومون بأعمال احتيال وينسب إليهم الفضل في كشف الثغرات الأمنية في تقنية المعلومات .

أما الاتجاه الأخير فيرى أن هذه الطائفة تصنف ضمن مجرمي المعلوماتية مثل غيرهم من المجرمين حيث أن أفعالهم المتمثلة في انتهاك الأنظمة واختراق الحواجز الأمنية في البيئة الالكترونية تعد أفعالاً خطيرة من الناحية العملية، بل إن أفعالهم لا تقف عند حدود دولة ما بل إنها تتعدى الحواجز الجغرافية .

وفي الواقع فإنه يجب عدم التقليل من خطورة هؤلاء الأشخاص فهذه الفئة قد تتعدى مرحلة الهواية والعبث لتدخل مرحلة متقدمة أكثر في مجال ارتكاب الجرائم المعلوماتية وهي مرحلة الاحتراف لهذه الجرائم، كما أن هناك مخاوف تتمثل في احتضان منظمات الجريمة المنظمة لهذه الفئة للاستفادة من مهاراتهم وتطويرها من أجل تحقيق مآربهم وغاياتهم الإجرامية من خلال التقنيات الحديثة .

حيث أن هذه الفئة تكون أكثر تقبلاً لأي أفكار تعرض أو تفرض عليها خاصة إذا كانت تحمل المغامرة والإثارة والتحدي في طياتها¹ .

■ الفئة الثانية : القراصنة

قراصنة المعلومات هم عادة مبرمجون من أصحاب الخبرة يهدفون إلى الدخول إلى الأنظمة المعلوماتية غير المسموح لهم بالدخول إليها وكسر الحواجز الأمنية المحيطة بهذه الأنظمة ويمكن تصنيف القراصنة إلى صنفين هما :

1. القراصنة الهواة العابثون أو الهاكرز (Hackers) :

وهم فئة المجرمين الأقل خطورة والذين تتوافر لديهم خبرة معتبرة في مجال الحاسب الآلي ووظائفه ومكوناته، ونظم المعلوماتية، ومعرفة البرامج التي يجري العمل بها كالبرامج المحاسبية، وبما أن هؤلاء يمارسون مواهبهم لغرض الولوج إلى نظم المعلومات بدافع الفضول أو اللهو، فهم لا يدركون ولا يقدرّون النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة لذلك فإن هذه الفئة تعد أقل خطورة ولكن مع ذلك يلاحظ أن ازدياد الأعداد المستخدمة لتكنولوجيا الإعلام

¹ المرجع السابق، ص. 78-83.

والاتصال، وما يتبعه من ازدياد نسبة الجرائم في هذا المجال، فلا يستبعد معه احتمال انزلاق هذه الفئة من مجرد هوة للأفعال غير المشروعة إلى محترفين.¹

هذا القسم من القراصنة أو ما اصطلح على تسميتهم "بالهاكرز" يرون في اختراق الأنظمة المعلوماتية تحدياً لقدراتهم الذاتية، وهذه الطائفة غالباً ما تكون من هوة الحاسوب فيقومون بأعمالهم هذه لمجرد إظهارهم أنهم قادرون على اقتحام المواقع الأمنية أحياناً أو لمجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع أحياناً أخرى.

وهم يدعون أنه لا توجد هناك دوافع تخريبية وراء أعمالهم، بل قد يكون الفضول وحب المعرفة والتعمق في عمل الأنظمة المعلوماتية هو دافعهم الأول ومجرمو المعلوماتية من هذا الصنف هم عادة أشخاص عاديون يشغلون مناصب محل ثقة ولديهم الكفاءة الخاصة والمعرفة والمهارة المطلوبة في مجال الحواسيب والشبكات الالكترونية.

فعلى سبيل المثال خرق استشاري تقنية معلومات أحد الأنظمة الأمنية لشبكة الإنترنت البريطانية لمجرد كشف الفجوات الأمنية بها وقد نجح في الحصول على أسماء لأكثر من 24 ألف شخص وعناوينهم وكلمات السر ومعلومات البطاقات الائتمانية من بينهم خبراء عسكريون وموظفون حكوميون وكبار مديري الشركات.

وهناك القراصنة الأخلاقيون الذين يقولون أنهم يعملون من أجل المصلحة العامة، فشكّلوا لهم منظمات خاصة مثل منظمة القراصنة ضد مواقع إباحية الأطفال التي استطاعت القيام بمحلات تأديبية لتعطيل قدرة بعض المواقع الالكترونية عن عرض مواد غير أخلاقية.

وفي الحقيقة هناك سمة مميزة لهذه الفئة من القراصنة إلا وهي تبادلهم للمعلومات فيما بينهم وتحديدًا التشارك في وسائل الاختراق وآليات نجاحها في مواطن الضعف في نظم الحاسوب والشبكات خاصة عن طريق النشرات الإعلامية الالكترونية ومجموعات الأخبار.

إلا أن الحقيقة التي يجب أن لا نخفيها هي أن هؤلاء القراصنة الهواة ساهموا في كشف الفجوات الأمنية للأنظمة المعلوماتية في المؤسسات المالية وغيرها الأمر الذي ساهم في تطوير نظم الأمن ضد الاختراقات الأمنية التي قد يقوم بها مجرمو المعلوماتية.

¹ يعيش تمام شوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، مطبعة الرمال، ط1، ط2، الوادي-الجزائر، 2019، ص22-23.

ويشاع في بعض المنشآت التي يضبط بها أحد قراصنة المعلومات أن يتم إلحاقه بالفريق المعلوماتي المكلف بأمن النظام المعلوماتي فيها .

2. القراصنة المحترفون (Crackers) :

هذه الفئة تعكس اعتداءاتهم ميولاً إجرامية خطيرة تنبئ عن رغبتها في إحداث التخريب. ويتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول فقد يحدثون إضراراً كبيرة .

وعادة ما يعود المجرم المحترف بالجريمة المعلوماتية إلى ارتكاب الجريمة مرة أخرى حيث تزداد سوابقه القضائية وهو يعيش لسنوات طويلة من عائد جرائمه وهذا المجرم لا يفضل الأفكار المتطرفة وإنما الأفكار التي تدر عليه الأرباح الشخصية¹ .

توضح الدراسات التي أجراها معهد (Stand Ford Research) أن محترفي الجرائم المعلوماتية من الجيل الحديث هم غالبا من الشباب الذين تتراوح أعمارهم من 25 الى 45 وتبين الإحصاءات في هذا المجال مايلي :

- أن 25% من أفعال الغش المعلوماتي أو الجريمة المعلوماتية يرتكبها المحلل.
- أن 18% من هذه الأفعال يرتكبها المبرمج .
- أن 17% يرتكبها المستخدم الذي لديه أفكار خاصة بنظم المعلومات .
- أن 12% يرتكبها الشخص الأجنبي عن المكان الذي تتواجد فيه نظم المعلومات .
- وإن 11% من هذه الأفعال يرتكبها فني التشغيل .

■ الفئة الثالثة : الموظفون العاملون في مجال الأنظمة المعلوماتية

بحكم طبيعة عمل هؤلاء الموظفين ونظراً لأن النظام المعلوماتي هو مجال عملهم الأساسي ونظراً للمهارات والمعرفة التقنية التي يتمتعون بها فإنهم يقتربون بعض الجرائم المعلوماتية التي من الممكن أن تحقق أهدافهم الشخصية، وأهمها الكسب المادي فالعلاقة الوظيفية التي تربط بين الموظف والمجني عليه تجعل عملية ارتكابه للجريمة المعلوماتية أسهل نظراً للثقة التي يتمتع بها .

¹ نهلا عبد القادر مومني، مرجع السابق، ص.ص 83-89.

وهناك فئة من الموظفين الحاقدين على عملهم أو على مؤسساتهم الذين قد يقومون بأفعال إجرامية لا تهدف إلى الكسب المادي بل هدفها الانتقام والثأر من أصحاب عملهم وهذه الفئة يذهب البعض إلى تسميتها "بفئة مجرمي المعلوماتية الحاقدين".

■ الفئة الرابعة : مجرمو المعلوماتية أصحاب الآراء المتطرفة

تتألف هذه الفئة من الجماعات الإرهابية أو المتطرفة التي تتكون من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو أساسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحياناً إلى النشاط الإجرامي ويتركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه وبدأ اهتمام هذه الجماعات وخاصة تلك التي تتمتع بدرجة عالية من التنظيم يتجه إلى نوع جديد من النشاط الإجرامي ألا وهو الجريمة المعلوماتية¹.

فهذه الجماعات تدافع عن قضية أو معتقد معين ولا تهدف ابتداءً إلى تحقيق الربح المادي وفي هذا تختلف هذه المنظمات المتطرفة عن المنظمات الإجرامية المنظمة، حيث تهدف الأخيرة إلى تحقيق مصالحها الشخصية المباشرة وتحديدًا تحقيق الربح المادي.

قامت جماعات تنتمي إلى منظمات إرهابية دولية من اليمين المتطرف واليسار مثل جماعة الألوية الحمراء الإيطالية ومنظمة (LECLODO) وهي : منظمة فرنسية متخصصة في تدمير نظم المعلومات وغيرها من المنظمات الأخرى بارتكاب أفعال اعتداء على أنظمة المعلومات المنتشرة في أوروبا ابتداءً من عام 1978.

وقد تعرضت وزارات وجامعات ومؤسسات مالية لهجمات الألوية الحمراء، ومن هذا أيقنت المنظمات الإرهابية أن في استطاعتها بمجهود بسيط أن تلحق أضراراً ضخمة داخل أي مشروع عن طريق تدمير المركز المعلوماتي له، لذا أصدرت الألوية الحمراء في فبراير 1998 منشوراً شرحت فيه إستراتيجيتها وأهدافها من الجرم على النظم المعلوماتية.

■ الفئة الخامسة : مجرمو المعلوماتية في إطار الجريمة المنظمة

في عالم الشبكات الإلكترونية كما هو الحال في العالم الحقيقي يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة وقد يكون أفضل ما توصف به هذه الأعمال أنها جرائم غير منظمة إلا

¹ المرجع السابق، ص. 83-89.

أن مجموعات الجريمة المنظمة بدأت بشكل متزايد باستغلال الفرص الجديدة التي يوفرها العالم الرقمي .

ومن التعريفات التي قيلت في الجريمة المنظمة أنها: "تعبير عن مجتمع إجرامي يعمل خارج إطار الشعب والحكومة ويضم بين طياته آلاف المجرمين الذين يعملون وفقاً لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المؤسسات تطوراً وتقدماً، كما يخضع أفرادها لأحكام قانونية سنوها لأنفسهم وتفرض أحكاماً بالغة القسوة على من يخرج عن ناموس الجماعة ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة مدروسة يلتزمون بها ويجنون من ورائها الأموال الطائلة¹ .

وعرفت هذه الجريمة كذلك من قبل الوفد المصري في المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين أنها: "مشروع إجرامي يمارسه مجموعة من الأفراد بتنظيم مؤسس ثابت له بناء هرمي ومستويات للتنفيذ وفرص للتزويج ويحكمه نظام داخلي صارم ويستخدم الإجرام والعنف والتهديد والابتزاز والرشوة في إفساد المسؤولين وفرض السطوة بهدف تحقيق أرباح طائلة بوسائل غير مشروعة حتى ولو اتخذ قالباً شرعياً من الناحية القانونية .

فالجريمة المنظمة تسعى في المقام الأول إلى الإفادة المادية أو تحقيق الأرباح الطائلة من خلال مواصلة العمل عبر وسائل إجرامية متنوعة، وهذه الجريمة تعد من جرائم ذوي النفوذ والسلطان التي قد يتورط فيها رجال السياسة وأصحاب المناصب الرفيعة فهي تعد بالفعل من جرائم ذوي الياقات البيضاء .

منظمات الجريمة المنظمة تطور أساليب عملها باستمرار بما يحقق أهدافها وغاياتها والعوامل المساعدة في تطوير هذه المنظمات لطرق عملها الموائمة المالية والاقتصادية التي تتمتع بها، فهي تسعى دوماً إلى استغلال الوسائل التقنية الحديثة في القيام بنشاطاتها فاستفادت هذه المنظمات عبر سنوات عملها من أحدث وسائل الاتصال حتى تؤمن الترابط بين أفرادها وجماعاتها .

وسعت وتسعى هذه المنظمات إلى الاستفادة من أجهزة التقنية المعلوماتية الحديثة المتمثلة في جهاز الحاسوب وشبكة الانترنت لتسوية أعمالها وتسهيل تنفيذها فلقد وجدت هذه المنظمات في شبكة الانترنت وسيلة لا تضاهي للقيام بعمليات غسيل الأموال على نطاق واسع وكذلك لتدعيم تجارة الرقيق الأبيض وتجارة الأعضاء البشرية عبر إنشاء مواقع خاصة بهذه الأعمال وهذه التقنيات

¹ المرجع السابق، ص. 83-89.

الحديثة تتناسب مع طبيعة النشاطات الإجرامية لجماعات الجريمة المنظمة التي تعد من الجرائم العابرة للحدود .

تقوم جماعات الجريمة المنظمة بتبني أصحاب الكفاءات وأصحاب الخبرة والمهوبين في مجال تقنية المعلومات وذلك بإغرائهم بالمال لينضموا إلى صفوفها وتقوم بتدريبهم وزيادة مهاراتهم في هذا المجال لخلق مجرمين متخصصين في الجرائم المعلوماتية في إطار هذه المنظمات ويمارس مجرمو المعلوماتية في نطاق هذه المنظمات نشاطات تدر على المنظمة أرباحاً هائلة فيقومون بتزوير البرامج وتقليدها واختراق شبكات المعلومات الخاصة بالدول والمؤسسات المالية الكبرى العالمية، كما يمارسون أعمال التجسس الصناعي والتجاري .

الجرائم المعلوماتية تشكل عامل جذب كبير لهذه المنظمات الإجرامية فبالإضافة إلى الأرباح المرتفعة التي تنتج من هذه الجرائم فإن صعوبة الكشف عنها وصعوبة إثباتها بالمقارنة مع الجرائم التقليدية، كذلك فإن بطء في التحقيق في هذه الجرائم نتيجة لعدم التعاون الدولي الكافي في هذا المجال جعل منها مادة إجرامية دسمة تغري هذه الجماعات باقترافها .

تجدر الإشارة إلى أن نسبة هذا النمط من الجرائم المعلوماتية التي تدخل في إطار الجريمة المنظمة مازالت منخفضة بالمقارنة بالأنماط الأخرى ويرجع ذلك بصفة أساسية لما تتطلبه هذه الجريمة من توافر درجة عالية من المعرفة والخبرة بتقنيات الحاسوب والإنترنت .¹

■ الفئة السادسة : الحاقدون

هذه الطائفة لا يسعون إلى إثبات القدرات التقنية و المهنية وفي نفس الوقت لا يسعون إلى مكاسب مادية أو سياسية إنما يحرك أنشطتهم الرغبة في الانتقام والثأر من تصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها .²

¹ هـلا عبد القادر مومني، مرجع السابق، ص. 83-89.

² غادة نصار، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، ط1، القاهرة، 2017، ص 51 .

المطلب الثالث : أدوات وأساليب المجرم السيبراني

❖ أولاً : أدوات المجرم السيبراني

حتى يتمكن القراصنة (Hachers) من تنفيذ جريمتهم الإلكترونية يستلزم ذلك توفر أدوات لذلك ومن أبرزها :

- الاتصال بشبكة الإنترنت وتعتبر أداة رئيسية لتنفيذ الجريمة .
- توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب .
- وسائل التجسس ومنها ربط الكاميرات بخطوط الاتصال الهاتفي .
- البار كود وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز .
- طابعات (Printers) .
- هواتف رقمية ونقالة .
- برامج ضارة ومنها (Trojan horse) إذ تتمثل وظيفته بخداع الضحية وتشجيعه على تشغيله فيلحق الضرر الشامل بالحاسوب والملفات الموجودة عليه .¹

❖ ثانياً : أساليب المجرم السيبراني

يستخدم المجرم السيبراني تقنية الاختراق لتنفيذ جريمته وذلك من خلال التحايل على الأنظمة المعلوماتية، فيكون الاختراق بالقدرة على وصول هدف معين عن طريق ثغرات في نظام الحماية الخاصة، وتتم عن طريق برنامجين الأول الخادم وهو بجهاز الضحية إذ ينفذ المهام الموكلة إليه والثاني يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد، كما أنهم يستخدمون عدة برامج منها :

1. حصان طروادة: وهو عبارة عن برنامج صغير مختبئ ببرنامج أكبر وتؤدي مهامها بشكل خفي في إطلاق الفيروسات والدودة التي تقوم بإرسال البيانات عن الثغرات الموجودة في النظام، و إرسال كلمات المرور السرية الخاصة بالهدف، ومن أنواعه القنابل المنطقية التي يزرعها المبرمج داخل النظام الذي يطوره .

2. فيروسات الكمبيوتر: وهي برامج صغيرة تستخدم لتعطيل شبكات الخدمات .

3. الديدان: وهي تتكاثر عن طريق نسخ نفسها عن طريق الشبكات وهدفها الشبكات المالية مثل البورصات .

¹ أسراء جبريل رشاد مرعي، مرجع السابق، ص 431 .

4. الأبواب الخلفية : وهي ثغرة تترك عن عمد من مصمم النظام للتسلل إليه وقت الحاجة .
5. الاختناق المروري السيبراني : وهو سد وخنق الاتصالات لدى المستهدف بحيث يمكنه من تبادل المعلومات .
6. القصف السيبراني : وهو الهجوم على شبكة المعلومات بحيث يسبب ضغط كبير على الموقع فيفقد قدرة الموقع على استقبال الرسائل من العملاء وبالتالي يوقف عن العمل تماماً .¹

¹ راضية حميدة، مرجع السابق، ص 343، 344 .

الفصل الثاني:

أهمية الإعلام الرقمي في الحد من الجرائم
السيبراني

المبحث الأول : دور التشريعات في الحد من الجرائم السيبرانية

المطلب الأول : تشريعات الجرائم السيبرانية في الجزائر

للجزائر مجموعة من القوانين والتشريعات التي تم سنّها بخصوص الجرائم السيبرانية وتتجلى فيما يلي :

الجرائم السيبرانية (المعلوماتية) قبل صدور القانون 04-09 :

اعتبر المشرع الجزائري برامج الحاسب الآلي من المصنفات الأدبية والفنية، وفي ذلك نصت المادة 4 من الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة على اعتبار برامج الحاسب الآلي كمصنف أدبي مكتوب محمي بهذا القانون، فالحقوق المادية أو المالية هي الإطار الذي يمكن صاحب الحق من استغلال برنامجه بشتى الطرق دون غيره أو لمن يخوله هو نفسه هذا الحق، وله في ذلك إبلاغه للجمهور بأية منظومة معالجة معلوماتية ويترتب على ذلك حقوق مادية للمؤلف صاحب البرنامج بالاستغلال التجاري له ولورثته بمختلف الطرق .

وقد حدد هذا الأمر أحكام جزائية تنص على جنحة التقليد والعقوبات المقررة لها بموجب المواد من 151 إلى 160 من هذا الأمر، ومع هذه البداية دخلت مجموعة تعديلات أخرى على قانون العقوبات والإجراءات .

تعديل قانون العقوبات :

بدأ المشرع الجزائري في مواكبة التطورات التكنولوجية من خلال إدخاله لمجموعة تعديلات على قانون العقوبات بإدراج قسم خاص يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004 ، ثم توالي التعديلات وإدراج بعض السلوكيات الإجرامية المتعلقة بذلك بموجب القانون 06-23 المؤرخ في 20 ديسمبر 2006 ، منها الدخول والبقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، أو الإدخال عن طريق الغش معطيات في النظام المعالجة الآلية أو الإزالة أو التعديل بطرق الغش لبعض المعطيات¹، أو في حالة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو

¹ مهدي رضا، "الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري"، مجلة إيليزا للبحوث والدراسات، المجلد 06، العدد 02، ص.ص 116-118.

مرسلة عن طريق منظومة معلوماتية أو حيازة أو إفشاء أو نشر أو استعمال المعطيات بطريق الغش، كما تشدد العقوبة في حالة حذف أو تغيير المعطيات أو تخريب نظام اشتغال المنظومة . ورغم نص المشرع الجزائري على هذه المواد إلا أنه لم يتطرق إلى جرائم القذف والسب الالكتروني أو المطاردة عبر الانترنت أو الغش المعلوماتي وإنما اكتفى بالنصوص العقابية التقليدية التي لا تتوافق مع طبيعة الجرائم السيبرانية ولا تتماشى مع مبدأ شرعية الجرائم والعقوبات وحظر القياس .

كما جرم المشرع الجزائري المساس بحمة الحياة الخاصة بموجب المواد من 303 مكرر إلى 03 من هذا القانون، غير أنه لم يضع الآليات القانونية المعتمدة للتصدي لهذه الجرائم .

تعديل قانون الإجراءات الجزائية :

استحدث المشرع الجزائري بموجب قانون الإجراءات الجزائية مجموعة من الإجراءات الخاصة التي تتماشى مع العالم الافتراضي وتتمثل في اعتراض المراسلات والتقاط الصور وتسجيل الأصوات وإجراء التسرب .

حيث سمح المشرع الجزائري باللجوء إلى اعتراض المراسلات والتقاط الصور وتسجيل الأصوات لمقتضيات التحري والتحقيق في جرائم محددة حصراً ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ولابد أن تراعي في ذلك شروط محددة قانوناً، والمتمثلة في الإذن وطبيعة الجريمة وكتمان السر المهني وتحرير محضر من طرف ضابط الشرطة القضائية المأذون له بالعملية .

وأشار المشرع بموجب المادة الثالثة من القانون 09-04 إلى ضرورة احترام سرية المراسلات وعرف الاتصالات الالكترونية في المادة الأولى من نفس القانون بأنها : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة لأي رسالة الكترونية.

وكإجراء آخر فقد أجاز المشرع اللجوء إلى التسرب بموجب المادة 65 مكرر 11 قانون إجراءات جزائية جزائري، وذلك إذا اقتضت ضرورة التحري والتحقيق ذلك في الجرائم المحدد حصراً ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات¹، حيث يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب

¹ المرجع السابق، ص.ص 116-118.

باحترام الضمانات والشروط المقررة قانوناً، والمتمثلة في احترام شرط الإذن المكتوب والمسبب ومن ثم يمكن استخدام هوية مستعارة للقيام بالتسرب في مدة زمنية محددة تقدر بأربعة أشهر قابلة للتجديد، ويجزر تقريراً يتضمن أهم العناصر الضرورية لمعينة الجريمة .

ويعرف التسرب بأنه : قيام ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف(المادة 65 مكرر 12 قانون إجراءات جزائية جزائري) .

آليات مكافحة الجرائم السيبرانية على ضوء القانون 04-09 :

كخطوة جديدة قام المشرع الجزائري بسن القانون 04-09 المتعلق بالوقاية من تكنولوجيا الإعلام والاتصال ومكافحتها، وإن كان تجسيد بنوده علة أرض الواقع مازال ضعيفا الى حد الساعة نتيجة إهمال الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وفي تحديد العقوبة المناسبة في حق مرتكبيها، حيث تقتصر العقوبات في غالبية الأحيان على الغرامة المالية فقط .

غير أنه وضع مجموعة من تدابير وقائية من هذه الجرائم ومكافحتها وأهمها :¹

(1) التدابير الوقائية :

أ. المراقبة الإلكترونية :

يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 04 من القانون 04-09 في

الحالات التالية :

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة .
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني .
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول الى نتيجة تم الأبحاث الجارية دون اللجوء الى المراقبة الإلكترونية .
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة .²

¹ المرجع السابق، ص.ص 116-118 .

² عبد الكريم مورك، تشريعات الجرائم الإلكترونية في الجزائر والدول العربية، دار علي بن زيد للطباعة والنشر، ط1، الجزائر، 2020، ص 11-12 .

ب : الاستعانة بمزودي الخدمات للوقاية من الجرائم السيبرانية :

ويكون ذلك من خلال تقديم مزودي الخدمات المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها ويوضع المعطيات تحت تصرف السلطات،(المادة 11 من القانون 09-04) وتشمل هذه المعطيات :

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة .
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال .
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال .
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها .
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصالات وكذا عناوين المواقع المطلع عليه .

ويشترط التزام مقدمي الخدمات بحفظ هذه المعطيات وأطلق عليها: المعطيات المتعلقة بحركة السير، ولم يغفل تعريفها بموجب المادة الأولى من هذا القانون بأنها : أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات وتوضع مصدر الاتصال والوجهة المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة .

زيادة على ذلك أفرد المشرع الجزائري مجموعة التزامات خاصة بمقدمي خدمات الانترنت (المادة 12 من القانون 09-04) تشمل التدخل الفوري لسحب المحتويات المخالفة للقوانين وتخزينها أو حضر الدخول إليها، إضافة إلى الالتزام بموضع ترتيبات تقنية تحصر إمكانية الدخول إلى الموزعات التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامة¹ .

¹ المرجع السابق، ص. 118-122.

2) التدابير الإجرائية :

أ : تفتيش وحجز المنظومة المعلوماتية

فلمقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية، ثم وضع مجموعة ترتيبات تقنية لمراقبة الاتصالات الالكترونية، وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية (المادة 03 من القانون 09-04) .

غير أن إجراء الحجز قد تصادفه عدة إشكالات لأسباب تقنية مما يتعين على السلطات التي تقوم بالتفتيش استعمال تقنيات مناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو الى نسخها الموضوعية تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة (المادة 07 من القانون 09-04) .

وجدير بالذكر أن هذا القانون أجاز اللجوء إلى التفتيش ولو عن بعد بسرعة إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، كما يمكن التفتيش عن بعد في منظومة تخزين معلوماتية، ويمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل معلومات ضرورية .

ب : تمديد الاختصاص بنظر هذه الجرائم

حيث يؤول الاختصاص للمحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، في حالة ارتكاب الجريمة من أجنبي وكانت الجريمة تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني .

ج : تبادل المساعدة القضائية الدولية

سمح المشرع الجزائري بإمكانية تبادل المساعدة القضائية الدولية لجمع الأدلة المتعلقة بالجريمة في شكلها الالكتروني، ومن الممكن الاستجابة لطلبات المساعدة الرامية إلى تبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية أو وفقا لمبدأ المعاملة بالمثل¹ .

¹ المرجع السابق، ص.ص 118-122 .

د :الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث استحدثت هذه الهيئة بموجب القانون 09-04 وبقيت تشكيلتها وتنظيمها و كفاءات سيرها لتحديد عن طريق التنظيم والذي توالى فيه التغيرات ابتداء من المرسوم الرئاسي لسنة 2015 ثم سنة 2019 ليأتي المرسوم الرئاسي لسنة 2020 ليعيد تنظيم الهيئة، وعرفها بأنها : سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة رئيس الجمهورية، ويحدد مقرها في الجزائر العاصمة¹، ويمكن نقله الى أي مكان من التراب الوطني بموجب مرسوم رئاسي وتتكون الهيئة من مجلس توجيه ومديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية ويقدمان عرضا عن نشاطاتهما(مرسوم رئاسي رقم 20-183 المؤرخ في 13 يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر، عدد 40، الصادرة بتاريخ 18 يوليو 2020) .

ومما سبق نلاحظ أن المشرع الجزائري خطى خطوة ايجابية بسن هذا القانون وتنظيمه إلا انه لا يكفي لمواجهة خطورة الجرائم السيبرانية مما يتطلب مواكبة التطورات التكنولوجية باستمرار .

(3) القوانين اللاحقة المدعمة للقانون 09-04 للحد من الإجرام السيبراني

● القانون 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية

حيث استحدث هذا القانون ووضع مجموعة آليات للتصدي للجرائم المتعلقة بالعالم الافتراضي منها، استحدثت سلطة ضبط من بين مهامها السهر على احترام متعاملي البريد والاتصالات الالكترونية للأحكام القانونية والتنظيمية المتعلقة بالبريد والاتصالات الالكترونية والأمن السيبراني (المادة 13 من القانون 18-04 المؤرخ في 10 مايو 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، جر، عدد 27، الصادرة بتاريخ 13 مايو 2018).

تجريم انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الالكترونية أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل أو المرسل إليه أو الأخبار بوجودها وتجريم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة، وسنت مجموعة من العقوبات ضمن المواد من 164 إلى 188 من هذا القانون.

¹المرجع السابق، ص. ص. 118-122.

● القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات

الطابع الشخصي

وضع المشرع الجزائري مجموعة من الآليات المتعلقة بالعالم الافتراضي والتي يمكن إيجازها في عدة نقاط :

- استحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي .
- وضع مجموعة التزامات ملقاة على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي .
- اتخاذ السلطة الوطنية لمجموعة إجراءات إدارية في حالة خرق أحكام القانون من طرف المسؤول عن المعالجة .
- يمكن للسلطة الوطنية القيام بالتحريات ومعاينة المحلات والأماكن التي تتم فيها المعالجة باستثناء محلات السكن، كما يمكنها اللجوء إلى المعطيات المعالجة وجميع المعلومات والوثائق أيا كانت دعائمها .
- تأهيل أعوان رقابة للقيام ببحث ومعاينة الجرائم المتعلقة بالمعطيات ذات طابع شخصي تحت إشراف وكسل الجمهورية .
- يمكن للمدعي بالمساس بحق من حقوقه المنصوص عليها في هذا القانون أن يطلب من الجهة القضائية اتخاذ أي إجراءات تحفظية للحد من التعدي أو للحصول على تعويض .
- تختص الجهة القضائية الجزائرية بمتابعة هذه الجرائم التي ترتكب خارج إقليم الجمهورية من طرف جزائري أو شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للقانون الجزائري، كمل تختص بمتابعة الجرائم المنصوص عليها في هذا القانون وفقا لقواعد الاختصاص المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية (المادة 53 من القانون 18-07، المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات طابع شخصي ج ر، عدد 34، الصادرة بتاريخ 10 يونيو 2018) .
- تجريم الاعتداء على المعطيات ذات الطابع الشخصي بإفراد عقوبات مالية وأخرى سالبة للحرية وفقا للمواد من 54 إلى 74 من هذا القانون¹.

¹ مهدي رضا، مرجع السابق، ص 118-122.

المطلب الثاني : تشريعات الجرائم السيبرانية في بعض الدول العربية والغربية

❖ أولاً: تشريعات في بعض الدول العربية

كان للدول العربية تشريعات مهمة جدا حول الجرائم السيبرانية والمتمثلة فيما يلي:

1. تشريعات الجرائم السيبرانية في المملكة العربية السعودية :

المملكة العربية السعودية من الدول النامية التي تتميز بتطور سريع للغاية في البنية التحتية الحيوية لشبكات الاتصالات والمعلومات، ويتزامن هذا التطور الهائل مع تزايد الاعتماد على أنظمة الكمبيوتر والأنظمة الالكترونية خاصة في المؤسسات الحكومية وشركات النفط والخدمات المصرفية، مما يؤهلها للعب دورا رياديا محليا وإقليميا وعربيا في حماية سوق الطاقة العالمية، وهذا ما يعرضها للهجمات الإرهابية الالكترونية التي كبدت الدولة خسائر تقدر بملايير الدولارات .

ولقد صدرت في المملكة العربية السعودية بعض الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الالكترونية والإرهاب الالكتروني، ونصت تلك الأنظمة على عقوبات في حال مخالفتها، وجاء قرار مجلس الوزراء رقم 163 بتاريخ 24 أكتوبر 1996، الذي ينص على بعض الضوابط المنظمة لاستخدام شبكة الانترنت والاشتراك فيها ومن ذلك :

- الامتناع عن الوصول أو محاولة الوصول إلى أي من أنظمة الحاسبات الآلية الموصولة بشبكة الانترنت .
- الامتناع عن إرسال أو استقبال معلومات مشفرة إلا بترخيص .
- الامتناع عن الدخول إلى حسابات الآخرين، أو محاولة استخدامها بدون تصريح .
- الالتزام باحترام الأنظمة الداخلية للشبكات المحلية والدولية عند النفاذ إليها .
- الامتناع عن تعريض الشبكة الداخلية للخطر¹ .

وفي مكافحة للإرهاب الالكتروني تم عام 2007 سن نظام مكافحة جرائم المعلومات بحيث تنص المادة السابعة منه على : "يعاقب بالسجن مدة لاتزيد على 10 سنوات وبغرامة مالية لاتزيد عن 5 ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية التالية :

¹عبد الكريم مروت، الإرهاب الإلكتروني وآليات مكافحته، دار علي بن زيد للطباعة ونشر، ط1، بسكرة-الجزائر، 2020،

- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، لتسهيل الاتصال بقيادات الأجهزة الحارقة أو المتفجرات أو أي مادة تستخدم في الأعمال الإرهابية .

- الدخول غير المشروع إلى موقع الكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني¹ .

وفي عام 2014 صدر نظام مكافحة الإرهاب ومن خلاله تم تجريم كل من يقوم بفعل إرهابي باستعمال الوسائل الالكترونية حيث نصت المادة 36 منه على "يعاقب بالسجن لمدة لا تزيد عن 20 سنة ولا تقل عن 10 سنوات كل من قام لارتكاب أي من الجرائم المنصوص عليها في النظام بأحد الأفعال التالية :

درب أو تدريب أو مول التدريب على أي مما يأتي :

"استخدام أي من وسائل الاتصالات السلكية أو اللاسلكية أو الالكترونية " .

كما نصت المادة 39 من نظام مكافحة الإرهاب على معاقبة كل من هرب أيا من الأسلحة أو الذخائر أو المتفجرات، أو أيا من وسائل الاتصال السلكية أو اللاسلكية أو الالكترونية، بقصد استخدامها في ارتكاب أي من الجرائم المنصوص عليها في النظام .

ونصت المادة 44 من النظام على معاقبة كل من أذاع أو نشر بأية وسيلة خبرا أو بيانا أو إشاعة كاذبة أو مغرضة أو نحو ذلك بقصد تنفيذ جريمة إرهابية ومعنى ذلك انه يعاقب كل من قام بالأفعال السابقة الذكر باستخدام الوسائل الالكترونية مثل البريد الالكتروني ومواقع التواصل الاجتماعي أو أية وسيلة تعتمد على الانترنت، وفي نفس المنحى نصت المادة 47 من النظام على معاقبة كل من استعمل وسيلة الكترونية في تمويل الجرائم الإرهابية داخل المملكة أو خارجها أو استعمال هاته الأموال من قبل كيان إرهابي أو إرهابي .

إلى جانب هذا تعتبر المملكة العربية السعودية إحدى الدول الموقعة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في 21 ديسمبر 2010، وفي سعيها للتصدي للإرهاب الالكتروني أنشأت المملكة السعودية جهاز رئاسة أمن الدولة و أنيطت له مسؤولية مكافحة الارهاب والأمن

¹ المرجع السابق، ص.ص 103-107 .

الالكتروني والاستخبارات الداخلية إلى تعزيز الاستعداد الالكتروني من خلال تطوير إطار وإستراتيجية الأمن الالكتروني وزيادة الوعي والقدرة على الأمن الالكتروني.

ولقد وضعت وزارة الاتصالات وتكنولوجيا المعلومات عام 2011، وهي إحدى الوكالات الحكومية المسؤولة عن الأمن الالكتروني و رقمنة الخدمات الحكومية في المملكة العربية السعودية إستراتيجية وطنية لأمن المعلومات وذلك رداً على الهجمات الالكترونية التي تعرضت لها السعودية. وفي أكتوبر 2017 نظمت المملكة العربية السعودية فعاليات المؤتمر العالمي الثاني لحلول القيادة والسيطرة والذي استقطب أكثر من 30 خبيراً و1000 مشارك على المستوى الدولي ومن بين المواضيع التي ناقشها المؤتمر الحرب الرقمية والصمود ضد الهجمات السيبرانية، حلول القيادة والسيطرة لمكافحة الإرهاب السيبراني وإدارة الأزمات والإرهاب التكنو-اجتماعي .

ويشكل موضوع حماية البنية الحيوية من الإرهاب الالكتروني أحد المواضيع الرئيسية التي ناقشها المؤتمر كونها من أولويات الحكومات والشركات في العالم، وإحدى ركائز الاستقرار والتطور الاقتصادي في ظل تصاعد الهجمات الإجرامية والإرهابية أهمها القرصنة والاختراقات الإلكترونية والإرهاب الالكتروني، وقد صبت حكومة المملكة العربية السعودية كل جهودها في حماية البنية الحيوية للقطاعات الاقتصادية الإستراتيجية وذلك من خلال تطوير أنظمة الحماية ومكافحة الإرهاب الالكتروني.¹

2. تشريعات الجرائم السيبرانية في الأردن :

قانون رقم 27 لسنة 2015 قانون الجرائم الالكترونية :

المادة 3 :

أ- يعاقب كل من دخل قصداً الى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، بالحبس مدة لا تقل عن أسبوع ولا تزيد ثلاثة أشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين .

ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو

¹ المرجع السابق، ص.ص 103-107.

إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد (1000) ألف دينار .

ت- يعاقب كل من دخل قصداً الى موقع الكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار .

المادة 4 : يعاقب كل من ادخل أو نشر أو استخدم قصداً برنامجاً عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول اليه أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار .

المادة 5 :

يعاقب كل من قام قصداً بالتقاط أو باعتراض أو بالتصنت أو أعاق أو حور أو شطب محتويات على ماهو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار¹ .

¹ المرجع السابق، ص. 357-370.

المادة 6 :

يعاقب كل من حصل قصداً دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) ألفي دينار¹.

المادة 8 :

تضاعف العقوبة على الجرائم المنصوص عليها في المواد من (3) الى (6) من هذا القانون بحق كل من قام بارتكاب أي منها بسبب تأديته وظيفته أو عمله أو باستغلال أي منهما .
قانون رقم (15) لسنة 2015 قانون المعاملات الالكترونية :

المادة 24 :

يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على ثلاث سنوات أو بغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار أو بكليتا هاتين العقوبتين كل من :

أ- أنشا أو نشر أو قدم شهادة توثيق الكتروني بغرض احتيالي أو لأي غرض غير مشروع.

ب- قدم إلى جهة التوثيق الالكتروني معلومات غير صحيحة بقصد إصدار شهادة توثيق أو وقف سريانها أو إلغائها .

المادة 25 :

تعاقب أي من جهات التوثيق الالكتروني المرخصة أو المعتمدة بغرامة لا تقل عن (50000) خمسين ألف دينار ولا تزيد على (100000) مائة ألف دينار بالإضافة إلى إلغاء ترخيصها أو اعتمادها إذا قدمت معلومات غير صحيحة في طلب الترخيص أو الاعتماد أو أفشت أسرار أحد عملائها أو استغلت المعلومات المتوفرة لديها عن طالب شهادة التوثيق

¹ المرجع السابق، ص، ص 357-370.

الالكتروني لأغراض أخرى غير أنشطة التوثيق الالكتروني دون الحصول على موافقة طالب الشهادة الخطية المسبقة.

المادة 26 :

يعاقب كل من يمارس نشاط جهات التوثيق الالكتروني داخل المملكة، دون الحصول على ترخيص أو اعتماد وفقا لأحكام هذا القانون والأنظمة الصادرة بمقتضاه بغرامة لا تقل عن (50000) خمسين ألف دينار ولا تزيد على (100000) مائة ألف دينار¹.

قانون رقم (16) لسنة 2019 قانون الأمن السيبراني :

المادة 3 :

أ- يشكل في المملكة مجلس يسمى (المجلس الوطني للأمن السيبراني) يتألف من رئيس يعين بإرادة ملكية سامية وعدد من الاعضاء يمثلون الجهات التالية :

- وزارة الاقتصاد الرقمي والريادة .
- البنك المركزي الأردني .
- القوات المسلحة الاردنية -الجيش العربي .
- دائرة المخابرات العامة .
- المركز الوطني للأمن وإدارة الأزمات .
- ثلاثة أعضاء يسميهم مجلس الوزراء بناء على تنصيب رئيس المجلس لمدة سنتين قابلة للتجديد لمرة واحدة على ان يكون اثنان منهم من ذوي الخبرة من القطاع الخاص .
- يختار المجلس من بين أعضائه في أول اجتماع يعقده نائباً لرئيس المجلس يقوم مقامه في حال غيابه .
- يجتمع المجلس بدعوة من رئيسه أو نائبه أربع مرات في السنة أو كلما دعت الحاجة ويكون اجتماعه قانونياً بحضور ما لا يقل عن ثلثي أعضائه ويتخذ قراراته بأغلبية أصوات أعضائه الحاضرين .
- لرئيس المجلس دعوة أي شخص لحضور اجتماع المجلس للاستئناس برأيه في الأمور المعروضة عليه دون أن يكون له حق التصويت .

¹ المرجع السابق، ص.ص 357-370.

- يحضر رئيس المركز اجتماعات المجلس دون أن يكون له حق التصويت .
 - يسمى رئيس المركز أحد موظفي المركز أمنيا لسر المجلس يتولى تنظيم جدول أعماله وتدوين محاضر جلساته وحفظ قيوده وسجلاته ومتابعة تنفيذ قراراته وأي أعمال يكلفه بها رئيس المجلس¹ .
 - على الرغم مما ورد في الفقرة (ج) من هذه المادة وفي حالات استثنائية يقدرها رئيس المجلس أو نائبه عند غيابه، يجوز أن ينعقد اجتماع المجلس بحضور أربعة على الأقل من الأعضاء المنصوص عليهم في البنود من (1) إلى (6) من الفقرة (أ) من هذه المادة ويكون القرار قانونيا ملزما على أن يحاط باقي أعضاء المجلس علما به في أول اجتماع تال له يكتمل فيه النصاب.
- المادة 4 : يتولى المجلس المهام والصلاحيات التالية :
- أ- إقرار الاستراتيجيات والسياسات والمعايير المتعلقة بالأمن السيبراني .
 - ب- إقرار الخطط والبرامج اللازمة لقيام المركز بمهامه وواجباته بما فيها برامج التعاون الدولي والإقليمي .
 - ت- اعتماد التقارير ربع السنوية عن الوضع الأمني السيبراني للمملكة والتقارير السنوي عن أعمال المركز .
 - ث- تشكيل اللجان التنسيقية من ذوي العلاقة لتمكين المركز من تحقيق أهدافه على أن تحدد في قرار تشكيلها مهامها وواجباتها وكيفية انعقاد اجتماعها واتخاذ قراراتها .
 - ج- إقرار الموازنة السنوية للمركز.

المادة 5 :

- أ- ينشأ في المملكة مركز يسمى (المركز الوطني للأمن السيبراني) يتمتع بشخصية اعتبارية ذات استقلال مالي وإداري وله بهذه الصفة تملك الاموال المنقولة وغير المنقولة والقيام بجميع التصرفات القانونية اللازمة لتحقيق أهدافه بما في ذلك ابرام العقود وله حق التقاضي و ينوب عنه في الإجراءات القضائية وكيل إدارة قضايا الدولة.
- يرتبط المركز برئيس الوزراء .

¹ المرجع السابق، ص. 357-370.

ب- يكون مقر المركز في مدينة عمان وله فتح فروع في محافظات المملكة .

المادة 10 :

أ- يحظر على أي شخص أو جهة تقديم أي من خدمات الأمن السيبراني دون الحصول على الترخيص اللازم وفقا لأحكام هذا القانون والأنظمة والتعليمات الصادرة بمقتضاه.

ب- على الجهات والأشخاص التي تقدم خدمات الأمن السيبراني في المملكة تصويب أوضاعها وفق أحكام هذا القانون والأنظمة والتعليمات الصادرة بمقتضاه¹ .

❖ ثانيا : تشريعات الجرائم السيبرانية في بعض الدول الأجنبية

كان للدول الأجنبية تشريعات صارمة ورادعة للجرائم السيبرانية وهذا ما سنتناوله من خلال بعض الدول الأجنبية والمتمثلة فيما يلي:

1. تشريع الجرائم السيبرانية في الولايات المتحدة الأمريكية :

قررت الولايات المتحدة الأمريكية إجراء خطوات تنفيذية لمكافحة الإرهاب الالكتروني في عهد الرئيس "بيل كلينتون" وبالتحديد في عام 1996 وذلك بإنشاء لجنة حماية البنية الحساسة، وفي مارس 1998 بدأ البنتاغون في التحري عن أخطر الهجمات على أنظمة الكمبيوتر الأمريكية فيما سمي "متاهة ضوء القمر"، وفي 1999 تم الانطلاق في تدريب آخر سمي "نجم القمة" وهو كيفية التصدي للصواريخ التي قاتلوا بمهاجمة أنظمة القوى التي تعدي عددا من القواعد العسكرية الأمريكية نتج عنه إرباك أنظمة الطوارئ في محطات الطاقة .

وتعتبر أحداث 11 سبتمبر 2001 نقطة تحول في مكافحة الإرهاب في العالم عامة وفي الولايات المتحدة الأمريكية خاصة، بحيث بعد أحداث مهاجمة برججي مركز التجارة الدولية بمنهاتن ومقر وزارة الدفاع الأمريكية (البنتاجون)، وضع هذا الأخير خطة تستهدف مراقبة الانترنت والتعامل معها كمنظومة سلاح معادية، وعليها تم إنشاء مكتب الأمن للفضاء الالكتروني، وإنشاء مركز حرب المعلومات يتناول جوانب الإرهاب الالكتروني، إلى جانب مبادرات أخرى كإنشاء المركز القومي لحماية البنية التحتية ومركز تحليل وتبادل المعلومات وبرنامج حراسة البنية التحتية وغيرها، وانتشرت في أجهزة الأمن الأمريكية المختلفة وحدات خاصة بالإرهاب الالكتروني وقيام

¹ المرجع السابق، ص.ص 357-370.

مكتب التحقيقات الفدرالي بملاحقة الإرهابيين الإلكترونيين وكذا قيام أجهزة الخدمات السرية بملاحقة الإرهاب الإلكتروني .

وفي أقل من شهرين من أحداث 11 سبتمبر 2001، وبالتحديد 26 أكتوبر 2001 ظهرت أول اتفاقية أمريكية لمكافحة الإرهاب الإلكتروني والتي بمقتضاها عززت سلطات البحث والتحقيق وتوسيع صلاحيات المراقبة الإلكترونية، ومنه خولت بعض النصوص الاتفاقية لقاضي النيابة ومكتب التحقيقات الفدرالي بالتقاط الرسائل المشتبه فيه، دون الحصول على إذن، إذا كان الأمر يتعلق بقضية مكافحة الإرهاب، كما تسمح للنائب الفدرالي أو العام بمراقبة أنشطة المشتبه فيهم على شبكة الانترنت دون الحصول على إذن مسبق¹، أما القانون الأمريكي الخاص بالمراقبة الإلكترونية فيجبر مقدمي الانترنت وشركات استغلال خطوط الهاتف بتقديم جميع المعلومات المطلوبة عن الزبائن المشتبه فيهم، خاصة إذا كانت هذه التسجيلات لها علاقة بأبحاث وتحقيقات المسموح بها في إطار الوقاية من الإرهاب الدولي.

غير أن هذه الجهود التي تبذلها الحكومة الأمريكية للحد من ظاهرة الإرهاب الإلكتروني تشكل تهديدا مباشرا على الحريات الشخصية والمدنية للمواطنين. وتميزت الإستراتيجية الأمريكية في مكافحة الإرهاب الإلكتروني بطابع استباق الهجمات المحتملة وذلك عن طريق رصد الهجوم الإلكتروني وتعتمد بالأساس على تطوير تقنيات الحرب المعلوماتية لشن هجمات استباقية تستهدف شبكات الإرهابيين والدول المعادية، وتسمح بالمقابل بتعزيز دفاعها ضد الهجمات الإلكترونية والإرهاب الإلكتروني .

في 2009 أنشأت الولايات المتحدة قيادة الكترونية أمريكية، وهي عبارة عن بنية عسكرية رسمية مكرسة للدفاع ضد الهجمات الإلكترونية وتنفيذ الهجمات ضد شبكات الكمبيوتر العدو .

وعمدت الإدارة الأمريكية في عهد الرئيس اوباما إلى اتخاذ التدابير الآتية :

- تعزيز الإطار القانوني والتشريعي، عبر إصدار قانون خاص لمكافحة الإرهاب الإلكتروني عرف بقانون حماية الشبكات السيبرانية .
- تعزيز دور مركز الاتصالات الاستراتيجي لمكافحة الإرهاب التابع لوزارة الخارجية

¹عبد الكريم مروت، الإرهاب الإلكتروني وآليات مكافحته، مرجع السابق، ص. 89-92.

الأمريكية، حيث يعمل عدد من المتخصصين في تقنيات المعلومات والاتصالات يجيدون عدد من اللغات من بينها العربية، وينشط هذا المركز عبر توثيق ونشر مواد مناهضة للإرهاب، وإعادة نشر ما ينشر من قبل جهات متعاطفة مع حركة مكافحته سواء كانت دولاً أم منظمات أم أفراد ويرأس هذا المركز مسلم، يحتل منصب المبعوث الخاص لمنظمة التعاون الإسلامي .

- إطلاق مشروع مخصص للتصدي للهجمات الإرهابية ومحاولات التجنيد على الانترنت يعتمد على بث تغريدات مضادة للإرهاب إضافة إلى استهداف حسابات الجهاديين .

- إرساء قواعد التعاون مع بلدان أخرى، من خلال عدد المبادرات أهمها تفعيل التعاون وتبادل المعلومات بين أجهزة طوارئ الانترنت، أو إنشاء خلايا مشتركة تعمل على رصد التهديدات السيبرانية وتبادل المعلومات بشأنها¹ .

ويقوم جهاز من المتجسسين في الولايات المتحدة الأمريكية بتمشيط مواقع التواصل الاجتماعي منقبين في البيانات التي ينشرها الإرهابيون عن أنفسهم سعياً إلى توقع خطتهم وتتبع تحركاتهم.

في ضوء إستراتيجية ترامب للأمن القومي وفيما يخص الإرهاب الإلكتروني عزز الأمن السيبراني من خلال الاستفادة من المجتمع المفتوح والتقدم في تشفير الاتصالات والانترنت بهدف مواجهة استخدام الإرهابيين للانترنت في التجنيد والتعبئة والتمويل للقيام بعملياتها الإرهابية داخل الولايات المتحدة، ومحاربة داعش والجماعات الإرهابية حتى بعد هزيمتهم الميدانية في سوريا والعراق. ولقد اتخذت الولايات المتحدة الأمريكية خطوات من أجل منع الجرائم الإرهابية الإلكترونية لإقناع الشركات والوكالات الحكومية لتبادل المعلومات مع وكالات إنفاذ القانون حول الخروقات الأمنية. ومن شأن تشريع أكثر إثارة للجدل أن يسمح لوكالات إنفاذ القانون في الولايات المتحدة بقراءة رسائل ورسائل مشفرة إلكترونياً، في ظل نفس الحالات التي يسمح لها باستخدام الهواتف. كما بدأ القطاع الخاص في حماية نفسه من خلال تشكيل منظمات مثل فريق الاستجابة للطوارئ في الكمبيوتر، التي تتعامل مع الاستجابة للحوادث الأمنية للنظام² .

¹ المرجع السابق، ص.ص 89-92.

² المرجع نفسه ، ص.ص 89-92 .

2. التشريع البريطاني في مكافحة الجرائم السيبرانية:

تعتبر المملكة المتحدة من الدول القلائل التي وضعت قانوناً لمكافحة الإرهاب يستهدف خصيصاً استخدام الإرهابيين للإنترنت ففي قانون مكافحة الإرهاب لعام 2000، تعاطي مع موضوع الإرهاب الإلكتروني من خلال التعريف الموسع للإرهاب، بحيث شمل أفعال القرصنة المعلوماتية التي من شأنها إزعاج أو خلق اضطراب داخل النظام الإلكتروني وكذا الأفعال والأقوال المناصرة للإرهاب عبر شبكة الانترنت، وتحريض الغير على ارتكاب عمل إرهابي خارج المملكة عن طريق إنشاء مواقع الكترونية وكان البرلمان البريطاني قد صادق على قانون يجبر الجهات والمقاولات المتخصصة على حفظ معطيات ربط الاتصال وفي 2002 توالى عملية استصدار إجراءات المراقبة الإلكترونية .

كما يشمل الإجراءات المحظورة المدرجة في القانون كتعريض حياة شخص للخطر أو خلق خطر جسيم على الصحة العامة أو السلامة العامة، أو الأعمال المصممة للتدخل بشكل خطير في النظام الإلكتروني أو تعطيله والأعمال التي تنطوي على عنف خطير أو وفاة لشخص آخر أو إلحاق ضرر جسيم بالممتلكات، ويصف قانون الإرهاب لعام 2000 العمل الإرهابي بأنه مصمم بشكل جاد للتدخل في نظام إلكتروني أو تعطيله بشكل خطير، كما يعتبره جانب من الفقهاء بمثابة التصدي للإرهاب الإلكتروني، ويستشهدون بالهجمات على الخدمات المصرفية عبر الانترنت وتدمير البيانات المخزنة بالحاسوب، ويرون كذلك أن التركيز على كلمة "جاد" مهم لأن "الإزعاج الباهظ" لا يرقى إلى مستوى الإرهاب الإلكتروني .

وفي أعقاب تفجيرات لندن عام 2005 سنت الحكومة قانون الإرهاب في عام 2006 يتضمن الجزء الأول منه أحكاماً تتناول خصيصاً الأنشطة التي تعتمد على الانترنت والتي يرجح أن تشجع على ارتكاب أعمال إرهابية أو تساعد في ذلك، إلى جانب قانون إساءة استخدام الحاسوب لسنة 1990 والذي يتناول الجرائم السيبرانية عموماً¹ .

ثم جاء قانون مكافحة الإرهاب والأمن لعام 2015 عززت قدرة أجهزة الاستخبارات لديها وبخاصة وصول إلى البيانات الصدد، تحديد الموقع الجغرافي، اعتراض الأمن ومواقع السلطة والمركبات، التقاط الصور وبيانات الكمبيوتر. منح للمرة الأولى الإطار القانوني لعمل الخدمات وقد

¹ المرجع السابق، ص.ص 92-95.

عرف ذلك في هذه العمليات وتعيين لمتابعة تنفيذها، سلطة إدارية مستقلة جديدة واللجنة الوطنية لمراقبة تقنيات الذكاء الذي ينجح مع سلطات أوسع إلى اللجنة الوطنية لمراقبة اعتراض الأمن كما تم فرض أوامر الاستبعاد المؤقتة، بحيث يجوز لوزارة الخارجية فرض أمر استبعاد مؤقت على فرد إذا تم استيفاء الشروط التالية :

- الشرط (أ) هو أن وزير الدولة يشتهه بشكل معقول أن الفرد شارك في النشاط المتعلق بالإرهاب خارج المملكة المتحدة .
 - الشرط (ب) هو أن وزيرة الخارجية تعتبر ذلك ضروري، لأغراض مرتبطة بحماية أعضاء الجمهور في المملكة المتحدة من خطر الإرهاب من أجل أمر استبعاد مؤقت ليتم فرضها على الفرد .
- وتسعى حكومة المملكة المتحدة إلى اتخاذ تدابير وقائية ضد التهديد الإرهابي الإلكتروني ردا على الاستخدام المتزايد للإرهابيين للتكنولوجيا عبر الانترنت في شن الهجمات الإرهابية الإلكترونية ، الشيء الذي أدى ببعض الشركات البريطانية المعنية بتكنولوجيا المعلومات والاتصالات على حث حكومة المملكة المتحدة على إنشاء وكالة لمنع الهجمات السيبرانية من أجل توفير حماية فعالة للبنية التحتية الحيوية الوطنية ضد الإرهاب الإلكتروني وهذا ما أدى بالحكومة البريطانية الى إطلاق إستراتيجية لمكافحة الإرهاب ومواكبة التطور التكنولوجي ومواجهة التطرف على الانترنت وأنشأت حكومة المملكة المتحدة المركز الوطني للمساعدة التقنية وهو عبارة عن موقف للاستشارة والاعتراض والمراقبة وتثقيف الجمهور العام حول الإرهاب الإلكتروني وتطوير الشراكة بين القطاعين العام والخاص لمعالجة الاستراتيجيات الأمنية في صناعة الكمبيوتر .

وأصدرت الحكومة البريطانية برنامج جديد، يمكن أن يكشف تلقائيا المحتوى الإرهابي على أية منصة على الانترنت بدقة خارقة كما يمكنه إيقاف الفيديوهات الإرهابية عند رفعها على الانترنت وحتى قبل نشرها وهذا البرنامج التكنولوجي وضع من طرف وزارة الداخلية البريطانية وشركة الذكاء الاصطناعي لعلوم البيانات، ويقوم بتحليل كل المواد المرئية والصوتية المسجلة¹.

¹عبد الكريم مروت، المرجع نفسه، ص 92-93-94-95 .

المطلب الثالث : الاتفاقيات الإقليمية في الجريمة السيبرانية

لقد كان للاتفاقيات الإقليمية أهمية كبيرة في ردع الجريمة السيبرانية، وفي ما يلي سنتناول أهم الاتفاقيات الإقليمية في الجريمة السيبرانية.

1) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات :

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حُررت بالقاهرة بتاريخ 15/1/1432هـ الموافق لـ 2010/12/21م ، إن الدول العربية الموقعة رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعاً منها بضرورة الحاجة الى تبني سياسية جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات. وأخذاً بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية وكذلك بالتراث الإنساني للأمم العربية التي تبذل كل أشكال الجرائم ومع مراعاة النظام العام لكل دولة والتزاماً بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها ، فقد اتفقت على مجموعة من المواد والقوانين من بينها :

المادة 3 : مجالات تطبيق الاتفاقية

تنطبق هذه الاتفاقية مالم ينص على خلاف ذلك على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات التالية :

- ارتكبت في أكثر من دولة .
- ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى .
- ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة .
- ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى¹ .

المادة 6 : جريمة الدخول غير المشروع

الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار بهذا الاتصال :

¹عبد الكريم مروك، الجريمة السيبرانية في الاتفاقيات والصكوك الدولية، مؤسسة نقطة بوك للنشر و التوزيع، ط1، 2021، ص.ص167-186.

- محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين و المستفيدين.
- الحصول على معلومات حكومية سرية .

المادة 7 : جريمة الاعتراض غير المشروع

الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات .

ومن بين الأحكام الختامية لهذه الاتفاقية مايلي :

1. تعمل الجهات المختصة لدى الدول الأطراف على اتخاذ الإجراءات الداخلية اللازمة لوضع هذه الاتفاقية موضع التنفيذ .

2. تكون هذه الاتفاقية محلا للتصديق عليها أو قبولها أو إقرارها من الدول الموقعة وتودع وثائق التصديق أو القبول أو الإقرار لدى الأمانة العامة لجامعة الدول العربية في موعد أقصاه ثلاثون يوما من تاريخ التصديق أو القبول أو الإقرار وعلى الأمانة العامة إبلاغ سائر الدول الأعضاء والأمانة العامة لمجلس وزراء الداخلية العرب بكل إيداع لتلك الوثائق وتاريخه .

3. تسري هذه الاتفاقية بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من يبع دول عربية .

4. يجوز لأي دولة من دول الجامعة العربية غير الموقعة على هذه الاتفاقية أن تنضم إليها وتعتبر الدولة طرفا في هذه الاتفاقية بمجرد إيداع وثيقة التصديق أو القبول أو الإقرار أو الانضمام لدى الأمانة العامة لجامعة الدول العربية ومضي ثلاثين يوما على تاريخ الإيداع¹.

5. مع مراعاة ما نصت عليه الفقرة (3) من المادة التاسعة عشر إذا تعارضت أحكام هذه الاتفاقية مع أحكام أية اتفاقية خاصة سابقة يطبق النص الأكثر تحقيقا لمكافحة جرائم تقنية المعلومات.

6. لا يجوز لأية دولة من الدول الأطراف أن تبدي أي تحفظ ينطوي على مخالفة لنصوص هذه الاتفاقية أو خروج على أهدافها .

¹المرجع السابق، ص.ص 167-186.

7. يجوز للدولة الطرف أن تقترح تعديل أي نص من نصوص هذه الاتفاقية وتحويله إلى الأمين العام لجامعة الدول العربية الذي يقوم بإبلاغه إلى الدول الأطراف في الاتفاقية لاتخاذ قرار باعتماده بأغلبية ثلثي الدول الأطراف ويصبح هذا التعديل نافذاً بعد مضي ثلاثين يوماً من تاريخ إيداع وثائق التصديق أو القبول أو الإقرار من سبع دول أطراف لدى الأمانة العامة لجامعة الدول العربية .

8. يمكن لأية دولة طرف أن تنسحب من هذه الاتفاقية بناءً على طلب كتابي ترسله إلى الأمين العام لجامعة الدول العربية .

ويرتب الانسحاب أثره بعد مضي ستة أشهر من تاريخ إرسال الطلب إلى الأمين العام لجامعة الدول العربية .

(2) قانون الإمارات العربي القانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية

المعلومات وما في حكمها :

ونص هذا القانون على 27 مادة، نذكر بعض منها، وهي كالآتي :

المادة (3) : كل من دخل عمداً وبغير وجه حق موقعا أو نظاما معلوماتيا يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين .

المادة (6) : كل من ادخل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في ذلك حكمها ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات بغرض ذلك ولم يتحقق غرضه يعاقب بالحبس...والغرامة...أو بإحدى هاتين العقوبتين¹ .

المادة (9) : كل من استعمل الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها في تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه ولو كان هذا الفعل أو الامتناع مشروعاً يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين.

المادة (26) : تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه حتى ولو ارتكبت كلياً أو جزئياً خارج إقليم الدولة متى أضرت بأحد مصالحها ويختص القضاء الوطني بنظر الدعاوى المترتبة عليها .

¹ المرجع السابق، ص.ص 188-200.

المادة (27) :فضلا عن العقوبات المنصوص عليها في هذا القانون تقضي المحكمة بإبعاد أجنبي الذي يحكم عليه وفقا لمواد (22.16).

(3) وثيقة الرياض (قانون) للنظام الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية 2012 :

تحتوي هذه الوثيقة على 39 مادة ومن بين هذه المواد مايلي :

المادة (2) : مع عدم الإخلال بالاتفاقية الثنائية والجماعية المنظمة للاختصاص القضائي الدولي وتسليم المطلوبين بين دول التعاون تسري أحكام هذا النظام (القانون) على الجرائم المنصوص عليها فيه حتى ولو ارتكبت كليا أو جزئيا خارج إقليم الدولة، متى أضرت بأحد مصالحها أو تحققت نتيجة الفعل في الدولة أو كان يراد أن تتحقق فيها، ويختص القضاء الوطني بنظر الدعاوى المترتبة عليها .

المادة (34) : يجوز للمحكمة بدلا من الحكم بأي عقوبة منصوص عليها في هذا النظام (القانون) ان تأمر بوضع المحكوم عليه تحت المراقبة أو حرمانه من استخدام وسائل تقنية المعلومات أو إلزامه بأداء عمل لمدة لا تزيد على (...) أو وضعه في مأوى علاجي .

المادة (38) : يعفى من العقوبات المقررة للجرائم المنصوص عليها في هذا النظام (القانون) كل من بادر من الجناة بإبلاغ الجهات المختصة بما يعلمه عنها قبل البدء في تنفيذ الجريمة وكان من شأن ذلك اكتشاف الجريمة قبل وقوعها أو الحيلولة دون إتمامها أو ضبط مرتكبها¹.

(4) إتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي:

اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، تم اعتمادها في الدورة الثالثة والثلاثون لقمة رؤساء دول وحكومات الاتحاد الإفريقي المنعقدة في ملايو، غينيا الاستوائية في 27 جوان 2014 .

إن الدول الأعضاء في الاتحاد الإفريقي اذ تسترشد بالقانون التأسيسي للاتحاد الإفريقي المعتمد في عام 2000 وإذ تأخذ بعين الاعتبار ان هذه الاتفاقية المتعلقة باعتماد إطار قانوني للأمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي تتكفل بالالتزامات الحالية للدول

¹ المرجع السابق، ص.ص 188-200.

الأعضاء في الاتحاد الإفريقي على المستويات الإقليمية الفرعية والإقليمية والدولية لبناء مجتمع المعلومات .

وإذ تشير إلى أنها تهدف إلى محاولة تحديد الأهداف والتوجيهات الرئيسية لمجتمع المعلومات في افريقيا وتعزيز التشريعات والأنظمة الحالية الخاصة بتكنولوجيا المعلومات والاتصالات للدول الاعضاء والمجموعات الاقتصادية الإقليمية .

وتؤكد مجدداً تمسك الدول الأعضاء في الاتحاد الإفريقي بالحريات الأساسية وحقوق الإنسان والشعوب الواردة في الإعلانات والاتفاقيات وغيرها من الصكوك المعتمدة في إطار الاتحاد الإفريقي والامم المتحدة .

تضمنت اتفاقية الاتحاد الإفريقي 38 مادة بشأن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي، ومن بين أهم هذه المواد نجد :

المادة 8 : أهداف هذه الاتفاقية بخصوص البيانات ذات الطابع الشخصي :

- تلتزم كل دولة طرف بوضع إطار قانوني يهدف الى تعزيز الحقوق الأساسية والحريات العامة لاسيما حماية البيانات الفعلية وقمع اية جريمة متعلقة بانتهاك الخصوصية والمعاقبة عليها دون المساس بمبدأ حرية حركة البيانات ذات الطابع الشخصي .
- يجب أن تضمن هذه الآلية المنشئة أن أي نوع من معالجة للبيانات يجب أن يحترم الحريات والحقوق الأساسية للأشخاص الطبيعيين مع الأخذ بعين الاعتبار صلاحيات الدولة وحقوق المجتمعات المحلية والأهداف التي أنشئت من اجلها المشاريع التجارية¹ .

المادة 32 : التدابير الواجب اتخاذها على مستوى الاتحاد الإفريقي :

على رئيس مفوضية الاتحاد الإفريقي أن يقدم تقريراً لرؤساء الدول والحكومات الإفريقية بشأن إنشاء ورصد الآلية التنفيذية لهذه الاتفاقية .

وستسعى آلية الرصد المقرر إنشاؤها إلى تحقيق ما يلي :

¹ المرجع السابق، ص، ص 188-200 .

✓ تعزيز وتشجيع القارة الإفريقية على اعتماد وتنفيذ تدابير لتعزيز أمن الفضاء الإلكتروني في الخدمات الإلكترونية وفي مكافحة الجريمة الإلكترونية وانتهاكات حقوق الإنسان في الفضاء الإلكتروني .

✓ جمع الوثائق والمعلومات بشأن احتياجات أمن الفضاء الإلكتروني وكذلك حول طبيعة وحجم الجريمة الإلكترونية وانتهاكات حقوق الإنسان في الفضاء الإلكتروني .

✓ العمل على وضع الطرق لتحليل احتياجات أمن الفضاء الإلكتروني وحول طبيعة وحجم الجريمة الإلكترونية وانتهاكات حقوق الإنسان في الفضاء الإلكتروني ونشر المعلومات وتوعية الجمهور بشأن الآثار السلبية لهذه الظاهرة .

✓ تقديم المشورة للحكومات الإفريقية بشأن أفضل السبل لتعزيز أمن الفضاء الإلكتروني ومكافحة آفة الجريمة الإلكترونية وانتهاكات حقوق الإنسان في الفضاء الإلكتروني على المستوى الوطني¹ .

✓ جمع المعلومات وإجراء التحاليل حول السلوك الإجرامي لمستخدمي شبكات المعلومات وأنظمة الكمبيوتر العاملة في إفريقيا ونقل هذه المعلومات إلى السلطات الوطنية المختصة .

✓ صياغة وتشجيع اعتماد مدونات قواعد السلوك لتكون موائمة للاستخدام من قبل الموظفين العموميين في مجال أمن الفضاء الإلكتروني .

✓ إقامة شركات مع المفوضية والمحكمة الإفريقية لحقوق الإنسان والشعوب، والمجتمع المدني الإفريقي، والمنظمات الحكومية، والمنظمات الحكومية الدولية، والمنظمات غير الحكومية بغية تسهيل الحوار بشأن مكافحة الجريمة الإلكترونية وانتهاكات حقوق الإنسان في الفضاء الإلكتروني .

✓ تقديم تقارير منتظمة إلى المجلس التنفيذي للاتحاد الإفريقي حول التقدم الذي أحرزته كل دولة طرف في تنفيذ أحكام هذه الاتفاقية .

✓ القيام بأي مهام أخرى تتعلق بالجريمة الإلكترونية وانتهاكات حقوق الأفراد في الفضاء الإلكتروني والتي قد تسند إليها من قبل أجهزة صنع السيارات في الاتحاد الإفريقي .

5) اتفاقية بودابست لمكافحة الجرائم المعلوماتية :

¹ عبد الكريم مروت، مرجع السابق، ص.ص 201-270.

اتفاقية بودابست لمكافحة الجرائم المعلوماتية حررت في بودابست في 2001/11/23 .
إن الدول الأعضاء بالمجلس الأوروبي وغيرها من الدول الأخرى الموقعة على هذه الاتفاقية الخاصة بالإجرام السيبراني .
اهتماما من جانبها بأن المجلس الأوروبي هدفه تحقيق الوحدة الكبرى بين أعضائها، واعترافا منها بقيمة رعاية التعاون مع الدول الأخرى أطراف هذه الاتفاقية .
واقترعا منها بضرورة الحاجة لإتباع سياسة جنائية مشتركة تهدف في المقام الأول إلى حماية المجتمع من الإجرام السيبراني، وذلك من خلال إقرار التشريع الملئم ورعاية التعاون الدولي ودعمه .
وإدراكا منها بعمق التغييرات التي أحدثتها عمليات التقييم والتقارب واستمرار عولمة شبكات الكمبيوتر .
و إيماننا منها بأن المكافحة الفعالة للإجرام السيبراني تستلزم زيادة وسرعة وتفعيل التعاون الدولي في الأمور الجنائية تفعيلا جيدا.

فقد تم الاتفاق من جانبهم على مجموعة من المواد،ومن نتائج هذه الاتفاقية :

المادة 39 : نتائج الاتفاقية

1. إن الغرض من الاتفاقية الحالية هو استكمال المعاهدات أو الاتفاقيات المتعددة الأطراف أو الثنائية فيما بين الدول الأطراف بالاتفاقية بما في ذلك النصوص الخاصة:
- بالاتفاقية الأوروبية الخاصة بتسليم المجرمين والتي أصبحت جاهزة على التوقيع في 13 ديسمبر 1957 رقم (Est24) .
- الاتفاقية الأوروبية الخاصة بتبادل المساعدات في الأمور الجنائية والذي أصبح جاهزا على التوقيع بستراسبورغ في 20 أبريل 1959 رقم (Est30)¹ .
2. وفي حالة سابقة قيام دولتين أو أكثر من الدول الأطراف بالاتفاقية بإبرام اتفاقية أو معاهدة تتعلق بالأمور التي يتم التعامل فيها بهذه الاتفاقية أو بالأحرى قيامها بإقامة علاقاتها بناء على مثل هذه الأمور، أو في حالة قيامها بعمل ذلك مستقبلا وبالتالي فإنه سيحق لها قانونا تطبيق تلك الاتفاقية أو المعاهدة أو تنظيم تلك العلاقات إلا أنه في حالة قيام الدول الأطراف بالاتفاقية بتأسيس علاقاتها فيما يتعلق بالأمور التي يتم التعامل فيها بهذه الاتفاقية الحالية فضلا عما تحكم

¹ المرجع السابق، ص.ص 201-270.

اللوائح الخاصة بها، فقد تعمل تلك الدول ذلك بطريقة قد لا تتفق والأهداف والمبادئ الخاصة بالاتفاقية .

3. لن يؤثر أي شيء بهذه الاتفاقية على الحقوق والقيود والالتزامات والمسؤوليات وغير ذلك من تلك الأمور الخاصة بأية دولة من الدول الأطراف بالاتفاقية¹ .

المبحث الثاني : أهمية الإعلام الرقمي في الحد من الجرائم السيبرانية

المطلب الأول : الوعي بالجريمة السيبرانية

تبين الاستقصاءات، بما في ذلك في البلدان النامية، أن معظم مستخدمي الإنترنت من الأفراد في الوقت الراهن يتخذون احتياطات أمنية أساسية .

يسلط جميع أصحاب المصلحة الضوء على الأهمية المستمرة لحملة رفع الوعي العام، بما في ذلك تلك التي تغطي التهديدات الناشئة، وتلك التي تستهدف جماهير محددة، مثل الأطفال. تثقيف المستخدم يكون أكثر فعالية عندما يتم دمج مع أنظمة تساعد المستخدمين على تحقيق أهدافهم بطريقة آمنة.

زيادة الوعي:

تسلط مبادئ الأمم المتحدة التوجيهية لمنع الجريمة الضوء على أهمية تثقيف الجمهور وتوعيته. حيث تمثل زيادة الوعي العام بمخاطر الاحتيال والتدابير الوقائية التي يمكن اتخاذها إستراتيجية هامة في الوقاية من أي نوع من أنواع الجريمة. وبالإضافة إلى الحكومات أثناء جمع المعلومات للدراسة سلطت منظمات القطاع الخاص أيضا الضوء على أهمية الوعي العام والمشارك فيما يتعلق بالجريمة السيبرانية. كما نوهت إحدى شركات الاتصالات الكبرى، على سبيل المثال، قائلة: "يجب علينا تثقيف الناس بخصوص الأمن الأساسي. إن مالكي الأجهزة التي ليس لها أمن أساسي، أو رقع، أو تحديثات، يتكون أبواهم مفتوحة على مصاريعها. ينبغي أن تكون الحملة جزءا من دور الحكومة كذلك، إن علينا إرسال رسائل بشكل مستمر عن أناس يحققون أفضل حماية لأنفسهم".

أشارت العديد من البلدان إلى مبادرات رفع الوعي. فقد أشارت إحدى البلدان المجيبة عن الاستبيان في الأمريكيتين، على سبيل المثال، إلى أهمية الحملات الإعلانية في الإعلام، وتشغيل بوابات (24/7) الدردشة التفاعلية على الإنترنت و تعزيز الشبكات والمواقع الاجتماعية " كما

¹ المرجع السابق، ص.ص 201-270 .

نوه عدد من البلدان في أوروبا والأمريكيتين أيضا إلى أنها وضعت استراتيجيات لرفع الوعي من خلال حملات لفترات محددة مثل "شهر التوعية بالأمن السيبراني" و "يوم السلامة على الإنترنت". ذكرت إحدى البلدان علاوة على ذلك أنها أنشأت صفحة على فيس بوك، والتي تنشر... نصائح أمن سيبراني على الإنترنت ولها وصلات إلى بوابة للإبلاغ عن الشكاوى. هناك أيضا رقم هاتف الجرائم 1800- للإبلاغ عن حوادث الجريمة السيبرانية " كما أشارت إحدى البلدان في أوروبا إلى أن التدابير الرامية إلى تحسين الإبلاغ عن الجريمة السيبرانية قد تم تطويرها بشكل إضافي في 2007 مع إنشاء موقع متخصص على الإنترنت... هذا الموقع ع كمنصة معلوماتية ثنائية الاتجاه، حيث يمكن للشخص أن على معلومات بالأخطار التي تواجهه فضاء الانترنت، ومن ناحية أخرى إرسال تقارير عن جرائم مرتكبة. ويتم توجيه التقارير بشكل مباشر إلى مسؤولي الشرطة ... وفي الوقت الراهن، يتم استلام قرابة 150 تقريرا بشكل شهري عبر الموقع... من المتوقع عقب انطلاق الحملة للترويج للموقع أن يتزايد عدد الزيارات وعدد التقارير المقدمة يلخص الجدول أدناه تفاصيل أربع حملات توعية تم ذكرها أثناء جمع المعلومات للدراسة¹.

ملامح حملات التوعية:

على الصعيد العالمي، تناول استعراض دولي بشأن التوعية بالأمن السيبراني والمبادرات التثقيفية في 2011. 68 من هذه الحملات، والتي استخدمت كلها الإنترنت كوسائل للاتصال. قدّم أكثر من ثلث الحملات منشورات، ونحو 30 في المائة ضمّن أيام أو أسابيع أو أشهر لرفع الوعي بالإضافة إلى ندوات تدريبية وكتب إرشادية. كما استخدم الربع فيديوهات و ألعاب أو مسابقات. وقد تمت استضافة معظم الحملات من قبل وكالات حكومية، وإن جاءت غالبا كجزء من اتحاد يشمل شركاء من القطاع الخاص والمؤسسات غير الربحية.

وبينما يتم تنظيم العديد من حملات التوعية على المستوى الوطني، يوجد أيضا عدد صغير من الأمثلة الإقليمية. نظام الإنذار وتبادل المعلومات الأوروبي، على سبيل المثال، أنشئ عام 2006. جمعت هذه الحملة معلومات ومواد تعليمية من أفرقة الاستجابة للطوارئ الحاسوبية ومجتمعات أمنية أخرى من بلدان في أوروبا. تمت ملائمة المواد بعد ذلك لمختلف فئات المواطنين

¹ الأمم المتحدة، دراسة شاملة عن الجريمة السيبرانية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فيفري 2015، ص. 330-333.

والشركات الصغيرة ومتوسطة الحجم في كل بلد البلدان من المشاركة. وتم نشر المواد بواسطة وسائل الإعلام الاجتماعية ومواقع الإنترنت والقوائم البريدية. كما ركز نطاق واسع تجريبي على الوعي بالروبوتات وسرقة الهوية، وتهديدات الهندسة الاجتماعية، وصلت إلى أكثر من 1,500 شخصا. أدارت شركات التكنولوجيا والجماعات غير الربحية أيضا حملات التوعية الخاصة بها. فحملة جوجل "من الجيد أن تعرف على سبيل المثال، نفّذت بحوالي 40 لغة منذ 2011. كما تعطي الإعلانات في الصحف والمجلات وعلى الإنترنت ووسائل النقل العام نصائح أمنية توضح بعض خصائص الإنترنت الأساسية مثل ملفات تعريف الارتباط وعناوين بروتوكول الإنترنت. عمل معهد سلامة الأسرة على الإنترنت أيضا مع التكنولوجيا لتجميع مواد تثقيفية تعليمية للوالدين والأطفال والمعلمين في موقعهم "Platform for Good". أدار كييفستار (Kyivstar)، مشغل اتصالات في أوروبا الشرقية حملة "أخبر طفلك عن أمان الإنترنت" في نيسان/أبريل 2012، مع إعلانات في وسائل الإعلام المطبوعة، وعلى السيارات، وعلى الإنترنت، وأيضا مع متطوعين يقدمون دورات معلوماتية في المدارس، وأما بالنسبة للجمهور الأصغر سنا فقد أدارت ديسني (Disney)، حملة سلامة تلفزيونية ومن خلال موقع على الإنترنت ومجلة في 2012 هدفت للوصول إلى 100 من الأطفال والأهل في أوروبا، والشرق الأوسط، وأفريقيا¹. وعلى الرغم من العدد المتزايد لهذه الحملات إلا أن عددا من البلدان نوّه إلى فكرة أن "حملات التوعية العامة ستستغرق بعض الوقت لتبني ثقة العامة من أجل زيادة الإبلاغ. الجريمة السيبرانية". وأثبت الاستعراض الدولي 2011 للحملات كذلك أن القليل من الحملات تضمنت عنصر التقييم. كما سلّط الضوء أيضا على التحديات التي تواجه تطوير الحملات الملائمة والفعالة من حيث التكلفة، وأشار أيضا إلى أن تقديم المعلومات للمستخدمين دون أنشطة تدريب واكتساب مهارات إضافية يكون تأثيره محدودا على سلوكياتهم على الإنترنت. وختم الاستعراض بأن حملات بسيطة مركزة على مجموعات مستهدفة محددة يكون لها تأثير أكثر فعالية، على ما يبدو، من حيث التكلفة².

¹ المرجع السابق، ص.ص. 330-333.

² المرجع السابق، ص.ص. 332-333.

المطلب الثاني : حماية خصوصية مستخدم الشبكات الاجتماعية

- وللحيلولة دون انتهاك الخصوصية في الشبكات الاجتماعية فلا بد من إتباع النصائح الآتية :
- 1 - الاختيار الدقيق للمعلومات الحساسة التي تكتبها أو الصور والفيديوهات التي ترفعها على حسابك فلا تكتب أي شيء في صفحة الملف الشخصي لوحة الإعلانات والرسائل الفورية أو أي نوع آخر من أشكال المشاركة والنشر الإلكتروني على الانترنت من شأنه أن يعرضك لإمكانية سرقة الهوية أو التهديدات الأمنية. وهذا يتضمن الأسماء الشخصية والتجارية والعناوين وأرقام الهاتف، والمسميات الوظيفية، وتواريخ الميلاد، وتفاصيل جدولك الزمني والأعمال الروتينية اليومية أو معلوماتك الأسرية. فمن الأفضل أن تحتفظ بهذه المعلومات بدلاً من أن تستخدم ضدك يوماً ما.
 - 2 - الحذر عند قبول طلبات الصداقة و التحقق ممن أرسل الطلبات و معرفة أنك لست ملزماً بمصادقة كل من طلب منك ذلك.
 - 3 - الحذر عند إعطاء الصلاحيات للبرامج و قراءة ما التراخيص التي يريدها البرنامج ولا تثق بكل البرامج والتطبيقات فبعضها وجد بغاية أخذ معلوماتك و معلومات أصدقائك.
 - 4 - من البديهي أنك يجب أن تضبط إعدادات الخصوصية حسب ما يناسبك و أن لا تعطي الكثير من المعلومات الشخصية عنك للعموم.
 - 5 - الأهم حماية كلمة السر و الحذر من التروجان و الفايروسات و الحيل التي وجدت بغرض سرقة كلمات السر مثل أن يدعي شخص أنه ممثل الدعم في شركة الفيس بوك و يطلب منك أن تضغط على رابط مرسل بالإيميل يطلب منك فيه تعديل معلوماتك لضمان عدم إغلاق حسابك، وهنا يجب الحذر أن الموقع الرئيسي المرسل هو somedomain.com مثلاً و ليس facebook و الفيس بوك هنا عبارة عن مجلد فرعي فيه، وتكون واجهة الموقع المرسل عبارة عن واجهة مطابقة 100% لواجهة الموقع المراد سرقة كلمة سره ، و لكن عند إدخال اسم المستخدم والإيميل يقوم هذا الموقع المزيف بإرسال معلوماتك للمخترق بدلاً من إدخالك للموقع، هذا ما يسمى الصيد أو phishing.
 - 6 - الضغط الدائم على الشبكات الاجتماعية كي تعطي المزيد من الخصوصية للمستخدمين.
 - 7 - عدم نشر ما قد يسيء إليك".

- 8- القيام بضبط وتعديل إجراءات الحماية الخاصة بالخصوصيات في الشبكات الاجتماعية.
- 9 - تأكد من إرسال معلوماتك الشخصية عبر اتصال آمن، فلدى إرسال أرقام بطاقة التأمين أو المعلومات المصرفية، أو كلمات السر، تحقق من وجود صورة قفل على شريط عنوان المتصفح. فمثل هذه التقنية تقوم بتشفير البيانات التي ترسلها وتتلقاها، مما يجعل من الصعب على أي شخص التجسس على الخط للوصول إلى هذه المعلومات.
- 10-الهروب من تعقب الإعلانات لك، فغالباً ما تقوم شبكات الإعلانات بتركيب ملف صغير على كومبيوترات الأشخاص الذين يقومون بزيارة مواقع شبكية معينة.
- 11 - يجب على كل من يدخل ويتصفح الإنترنت أن يكون لديه أربعة أنواع من البرامج وهي: م مضاد فيروسات قوي، فاحص وماسح برامج التجسس والكوكيز، فاحص وماسح أحصنة طروادة Trojan ، كما وعليك تحديث هذه البرامج كل شهر وأخيراً تجنّب الدخول بكثرة الى المواقع التجارية التي تقدم خدمات مجانية.
- 12 -وإذا كنت تستخدم خطأً سريعاً مثل ADSL أو DSL فاعلم بأن نسبة الخطورة أكثر ونسبة إصابتك أكبر ممن يستخدمون الخطوط البطيئة فكن حذراً حتى لا تقول وداعاً للخصوصية.
- كن متشككاً بما تستقبله من معلومات فمواقع الشبكات الاجتماعية مليئة بالمعلومات التجارية المفيدة، فضلاً عن كميات كبيرة من التضليل عديم الفائدة، فكر بمصادقية وواقعية في كل ما تقرأه في الإنترنت سواء كانت نصائح لمضاربي الأسهم، أو الأخبار العاجلة، أو فضائح سياسية، أو إشاعاتمنتشرة. فبعض الناس سوف يكذب من أجل كسب مصلحة خاصة فيهم، والبعض الآخر قد يكون مجرد بغاء لا يعي ما يردده من القيل والقال¹.
- 13 - كن عميق التفكير فلا أحد يحب كثير الكلام أو من يتكلم بما لا يعرف أو يدعي ما لا يملك، ولكن في الانترنت قد يخلع بعض الأشخاص الأقنعة المزيفة التي كانوا يرتدونها في الحياة الواقعية، ليظهروا على حقيقتهم. فمن أسهل الأشياء في الإنترنت و من ضمنه الشبكات الاجتماعية التخفي خلف الأسماء المستعارة، والخوض في كل شيء محذور من الكذب و الفحش و نشر الفضائح فتجنب زلات لوحة مفاتيحك ولا تكتب أي شيء يمكن أن يضرك

¹ بشري حسين الحمداني، مرجع السابق، ص.ص 165-170.

فيما بعد. و فكر مرتين قبل الكتابة. قال تعالى : (ما يلفظ مِنْ قَوْلٍ إِلَّا لَدَيْهِ رَقِيبٌ عَتِيدٌ) (سورة ق الآية 18).

14 - كن ذواقاً مهذباً فإذا أردت نشر صورة أو فيديو أو حتى كتابة رسالة في الشبكات الاجتماعية فتأكد من أنه سيظهر في أجمل شكل ممكن لأنه في النهاية يعبر عنك وعن آرائك ومعتقداتك.

15 - فلا تظهر بشكل محل بالأدب ولا ترتدي قبعة المهرج. كن متيقظاً فطناً فالكثير من الناس في الشبكات الاجتماعية قد يظهر و بصورة مغايرة تماماً لواقعهم. فإذا كنت تدرش مع المدير التنفيذي لشركة مرموقة ففي الواقع قد تكون تتحدث إلى طفل مراهق أو سجين محكوم عليه بالإعدام. فتأكد دائماً من هوية الأشخاص الذين تتعامل معهم و اجث عنهم و تحقق من المعلومات التي يرسلونها لك.

الخصوصية الشخصية الخاصة أو الخصوصية الاعتبارية للمواقع من الحقوق المحفوظة والتي يعتبر الاعتداء عليها جرماً يستحق صاحبها العقاب والتجريم، وقد أدى انتشار الشبكة وخاصة الاجتماعية - بما تحمله من خصوصية اجتماعية للشخص والمواقع - إلى سهولة هتك ستار الحقوق والتلاعب بها إما بالتعطيل أو التغيير أو بالاستغلال السلي لها ولمعلوماتها، وانتهاك الخصوصية يتم ذلك من عدة طرق منها انتحال الشخصية الخاصة للأفراد أو الاعتبارية للمواقع والشركات، فلكل شخصية فردية واعتبارية حقوقها المحفوظة، وخاصة الشخصيات المهمة والمتميزة وأصحاب الرئاسات الكبرى، وكذلك الحال مع المواقع الشهيرة والمتميزة، استغلالاً للنفوذ والشهرة والثقة الاعتبارية لكثير من الشخصيات والمواقع¹.

ولتأمين الحقوق الخاصة للأفراد والمواقع، لابد من معرفة ما يلي:

1- ليس كل ما يعرف يكتب على الحاسب وينشر على الشبكة، فحاول أن تكون لك أسرارك الخاصة التي تحتفظ بها في غير جهاز الحاسب، أو اجعل لها جهازاً خاصة لا يكون متصل بالشبكة.

2 - شفر معلوماتك الخاصة، أي أجعل لها شفرة خاصة من رقم أو نحوه يصعب تخمينها، وحاول تغييرها كل فترة معينة، والبرامج التي تخدم في التشفير كثيرة.

¹ المرجع السابق، ص.ص 165 - 170.

- 3- اعرف من تضيفهم كأصدقاء أو مشاركين ومطلعين على ملفاتك ومعلوماتك.
- 4 - أعط صلاحية خاصة لأشخاص معروفين بالاطلاع على الملفات الخاصة، أو استخدامها في أضيق نطاق ممكن .
- 5 -احتفظ بنسخ احتياطية من أعمالك أو موقعك أو بياناتك في مكان آمن لا يصل له غيرك أو من تحوله بذلك تحت إشرافك
- 6 - زود جهازك ببرنامج حماية قوي وفعال ،داوم على الاطلاع على ملفاتك وتفقدتها باستمرار، أو وكل من تثق به في ذلك .¹

المطلب الثالث : الوقاية والتأمين بالبرامج والوسائل التقنية

أولاً : الوقاية بالبرامج

- توجد برامج متنوعة للوقاية من الجرائم السيبرانية، حيث تتباين هذه البرامج بدرجة فاعليتها وذلك حسب البرامج المصممة لهذا الغرض، ومن بين هذه البرامج :
- عمل نسخ من ملفات البيانات Backups .
 - استخدام البرامج المضادة للفيروسات Anti-Virus software .
 - برامج جدران النار Firewalls sifware ، نظام أو برامج حماية تحجز بيانات بين الشبكة الداخلية والشبكة الخارجية أي هو الجهاز الذي يتحكم في تدفق المعلومات بين جهاز الحاسوب والإنترنت، والهدف هو حجز كل ما هو غير مرغوب فيه من خارج البيئة المحمية، يستطيع المستخدم إذن الخروج إلى عالم الإنترنت ولكن لا يستطيع من في الخارج الدخول إلى الجهاز من خلاله .
 - استخدام الخصائص الفسيولوجية fingerprintBiometrics - لحماية النظام مثل بصمة الإبهام، حدة العين، الصوت وغيرها .
 - التشفير Encryption : وتستخدم معظم نظم المعلومات الإدارية الشبكية برامج جدران النار والبرامج المضادة للفيروسات بالإضافة الى تشفير لحماية الرسائل والملفات المخفية، وهناك تشفير باستخدام المفتاح العام Public Key Encryption المعروف اختصاراً باسم

¹ بشرى حسين الحمداني، مرجع السابق، ص.ص 165-170 .

(PKE) وهو نظام تشفير يستخدم مفتاحين، مفتاح رئيسي يمكن أن يستخدم أو أن يحصل عليه أي شخص ومفتاح خاص Privete Key للشخص المستلم فقط.¹

ثانياً : تأمين بالوسائل التقنية

ويتم ذلك على أربعة مستويات هي:

أ- تأمين وحماية الحاسبات الشخصية والحاسبات الخادمة.

ب تأمين وحماية شبكة الربط بالإنترنت.

ج- تأمين المعلومات المتداولة.

د - الحماية من التهديدات والاختراقات.²

المبحث الثالث: معوقات الإعلام الرقمي في الحد من الجرائم السيبرانية

رغم التطور الذي صاحب الإعلام الرقمي، إلا أن هناك مجموعة من العوائق التي تعيق دوره في

الحد من الجرائم السيبرانية وهذا ماستتقرق إليه من خلال المطالب التالية :

المطلب الأول : مخاطر التطور التكنولوجي

تتعدد آثار ومخاطر التكنولوجيا الجديدة للإعلام والاتصال، حيث تشكل عائق أمام الإعلام

الرقمي في الحد من الجرائم السيبرانية، وتتمثل هذه المخاطر فيما يلي :

1. صعوبة حماية المعلومات :

تشمل مجالين :

حفظ المؤلفات وحقوق المؤلف : تكاد التكنولوجيا الجديدة للإعلام والاتصال تعيد النظر في

مفهوم المؤلف والحقوق المرتبطة بالتأليف وذلك بطرق عدة :

أولاً : كيف تحدد مستحقات المؤلفين؟ إن تطور الطرق السريعة للمعلومات التي توفر بنوك الصور

والأصوات والمعطيات، سيجعل النشر الإلكتروني مهيمنا على توزيع الدعائم (الأوعية) المادية. إن

¹ عبد السلام محمد المايل، عادل محمد الشرجي، "الجريمة الإلكترونية في الفضاء الإلكتروني: المفهوم- الأسباب- سبل المكافحة مع التعرض لحالة ليبيا"، مجلة آفاق للبحوث والدراسات سداسية-دولية محكمة، العدد 04 جوان 2019، المركز الجامعي ايليزي، ص 251 .

² مجلس التعاون الدول الخليج العربية، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، 2016، ص 44.

حقوق المؤلف التي تعتمد أساسا على نموذج الكتاب يجب أن تكيف أخذه بعين الاعتبار الطبيعة اللامادية للمعلومات. ومع ذلك فهل سيسمح هذا التكيف بمراقبة استعمال عبر الشبكات الدولية حيث تقررصن وتستنسخ بواسطة أجهزة فعالة وغير مكلفة؟ وهل سيسمح بالحقوق المادية للمؤلفين؟ كيف يمكن بعد ذلك حفظ الحقوق المعنوية للمؤلفين؟ حيث أصبح من الشائع حاليا تغيير ألوان الأفلام والمقاطع الموسيقية ومحتويات المقالات والنصوص عبر الشبكة العنكبوتية .

2. مجال سرية المعطيات الشخصية وخصوصيتها :

تحدد التكنولوجيا الجديدة للإعلام والاتصال الحياة الخاصة لمستعملها. فبعدما أضحت تفاعلية أصبحت الشبكات الاتصالية تتيح المعرفة الفورية للبرامج المشاهدة من طرف الجمهور وللمعلومات التي اطلع عليها الانترنتيون وحتى تشخيص الحواسيب المتصلة بها . وبالطبع قد تستعمل هذه المعلومات الخاصة لأغراض تجارية لمعرفة خصائص المستهلكين كما قد تستعمل لأغراض سياسية أو عسكرية أو أمنية¹ .

المطلب الثاني : ضعف التنسيق والتعاون الدولي لمكافحة الجريمة السيبرانية

على الرغم من الخطورة التي تكتسبها جرائم المعلومات، إلا أن التنسيق والتعاون الدوليين بشأنها لم يبلغ درجة الاهتمام الذي تشهده بعض الجرائم الدولية على غرار الجرائم الإرهابية، لذا يكون من الأهمية بمكان توسيع نطاق هذا التنسيق والتعاون إلى جميع الجرائم التي تهدد المصلحة العامة والأشخاص والأموال، بما فيها الجرائم المعلوماتية، من خلال ربط اتفاقيات تعاون بين الدول، بما يتيح إمكانية تقديم طلب إلى سلطات الدولة المعنية من أجل تزويدهم بالمعلومات والأدلة في مرحلتي التحري والتحقيق.

فإذا كانت الجريمة المعلوماتية تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، فإن ذلك يبرز أهمية امتهان قواعد الاختصاص والقانون الواجب التطبيق، فيما إذا كانت النظريات والقواعد القائمة في هذا الحقل تطال هذه الجرائم أم يتعين أفراد قواعد خاصة بها في ضوء خصوصيتها، وما تثيره من مشكلات في مجال الاختصاص القضائي، مع ملاحظة أن هذا الإشكال يتفاقم أكثر في ظل

¹ فضيل دليو، التكنولوجيا الجديدة للإعلام والاتصال مفاهيم-نظريات-مبادئ-استعمالات-آفاق، دار الفايز للطباعة والنشر، ط1، الجزائر، 2010، ص 45 .

امتداد الملاحقة والتحري والضبط والتفتيش خارج الحدود، الأمر الذي يتطلب وجود تعاون دولي يكفل مكافحة الجريمة الإلكترونية من جهة، ولا ينتهك مبدأ سيادة الدول على إقليمها من جهة ثانية.

والواقع أن خاصية العالمية التي تميز جرائم المعلوماتية قد دفعت رجال القانون والفقهاء إلى الدعوة لمواجهتها من خلال وضع قواعد اتفاقية تعبر عن تصور دولي موحد من شأنه تدارك النقائص والثغرات التي تعترى منظومة القوانين الداخلية للدول وذلك بهدف التقليل من حدة آثار هذه الجريمة.

وفي هذا الإطار تضافرت الجهود من أجل وضع إطار قانوني اتفاقي يسمح بمتابعة مرتكبي جرائم المعلوماتية ومعاقبتهم، وهو الأمر الذي تجسد في اتفاقيات ثنائية ومتعددة الأطراف متعلقة بالمسألة سواء على المستويين الدولي أو الإقليمي¹.

فمن المعلوم أن الجرائم المعلوماتية ظهرت في الدول المتقدمة، ولا غرابة في ذلك على اعتبار أن تلك الدول كانت سباقة إلى استخدام البيئة الرقمية في تعاملاتها العادية والتجارية والمالية وغيرها، لذا برزت الحاجة إلى توحيد الجهود الدولية في هذا المجال، وهو ما تجسد فعلاً بعقد الكثير من المؤتمرات المتعلقة بالموضوع وإبرام اتفاقيات تخص المسألة، وعلاوة على ذلك تم وضع قوانين نموذجية لمواجهة هذه الجرائم في مجالات متعددة، ومن أجل بيان تلك الجهود من الأهمية بمكان الإشارة إلى بعضها بإيجاز فيما يأتي :

1- المؤتمر الدولي لحقوق الإنسان الخاص لسنة 1968:

يعتبر هذا المؤتمر من أول المؤتمرات التي تعكس الجهود الدولية في مكافحة جرائم الأنترنت، حيث عقد بالعاصمة الإيرانية في نهاية ستينيات القرن الماضي، وقد أكدت الفقرة 18 من هذا الإعلان صراحة إلى أن التقدم العلمي والتقني يمكن أن يعرض حقوق وحريات الفرد للخطر، وهو الأمر الذي لقي صدى واسعاً من طرف الغالبية العظمى من الدول المتقدمة، وذلك من خلال التجسيد الفعلي لمضمون هذه التوصية في تشريعاتها الداخلية.

ب قانون الأونسيتال النموذجي للتجارة الإلكترونية لسنة: 1996

علاوة عن المؤتمر السابق الإشارة إليه، يعد هذا القانون من أهم الجهود الدولية في مجال

¹ يعيش تمام شوقي، مرجع السابق، ص.ص 42-48.

مكافحة الجرائم المتعلقة بالمعلوماتية على المستوى الدولي، وقد كان لبنة للعمل الكبير الذي قامت به "الأنسترال" في سبيل وضع نصوص نموذجية لتزويد المشرعين الوطنيين بمجموعة قواعد مقبولة دولياً ترمي إلى تدليل العقوبات القانونية وتعزيز القدرة على التنبؤ بالتطورات القانونية في مجال التجارة الإلكترونية لمواجهة جرائم المعلوماتية في مجال التجارة الإلكترونية، وقد لقي هذا القانون قبولاً من طرف مشرعي الدول والمتعاملين لاسيما بعد أن اعتمدته لجنة الأمم المتحدة سنة 1996.¹

ج- القانون النموذجي المتعلق بالتوقيع الإلكتروني لسنة 2001 .

يعتبر هذا القانون تكملة للجهود التي بذلتها لجنة "الأنسترال" في سبيل مكافحة الجرائم المعلوماتية المتعلقة بالتجارة الدولية، حيث تكفل بوضع قواعد موحدة من شأنها حماية التوقيع الإلكتروني، وهو ما كرسته الكثير من الدول في تشريعاتها الداخلية.

علاوة عن الجهود الدولية لمواجهة الجرائم المعلوماتية عكفت الكثير من الدول إلى معالجة هذه الجرائم على المستوى الإقليمي، وهذا ما يتضح من خلال النموذجين التاليين:

أ - الاتفاقية الأوروبية لجرائم الانترنت لسنة 2001

دخلت هذه الاتفاقية حيز التنفيذ سنة 2004، ويطلق عليها البعض تسمية اتفاقية بودابست وقد جاءت تنويعاً للجهود التي بذلها المجلس الأوروبي في سبيل التوصل إلى وضع إطار اتفاقي فعال لمكافحة الجرائم المعلوماتية، ومن أهم الدول التي وقعت عليها خارج دول الاتحاد الأوروبي نذكر جنوب إفريقيا واليابان والولايات المتحدة الأمريكية.

وتأتي أهمية هذه الاتفاقية في كونها اتفاقية تهدف إلى توفير إطار دولي مشترك للتعامل مع الجرائم الإلكترونية حيث تلتزم الدول الموقعة عليها بتعديل تشريعاتها لمواجهة التحديات التي تفرضها تكنولوجيا المعلومات، إذ تولت تحديد الجرائم المعلوماتية، واعتماد أدوات إجرائية لمكافحة الجريمة المعلوماتية وضبط مرتكبيها .

وتتكون الاتفاقية من 44 مادة موزعة على عدد من الأبواب، بحيث جاء الباب الأول منها محددًا للتعريفات وضبط المصطلحات، أما الباب الثاني فخصص للحديث عن التدابير الواجب اتخاذها على الصعيد الوطني، والباب الثالث يتعلق بالولاية القضائية والتعاون الدولي، والباب الرابع

¹ يعيش تمام شوقي، مرجع السابق، ص. 42-48.

يتضمن الأحكام الختامية .

ب- قانون عربي استرشادي لمكافحة الجريمة المعلوماتية:

تم اعتماد مشروع هذا القانون في الدورة التاسعة عشر لمجلس وزراء العدل العرب سنة 2003، قبل أن يعتمده وزراء الداخلية العرب سنة 2004.

والملاحظ أن هذا القانون أشار لأنواع الجرائم التي تقع عن طريق الكمبيوتر والانترنت بصفة عامة، وأحال إلى التشريعات الداخلية كلما يتعلق الأمر بأركان هذه الجرائم وكذلك العقوبات التي تطبق عليها، وفي هذا السياق تضمن الباب السابع من هذا القانون فصلا خاصا يتعلق بالجرائم المعلوماتية الواقعة على حقوق الأشخاص، حيث أدرجت فيه أربعة مواد (من المادة 461 إلى المادة 464 منه، وأشارت إلى حماية خصوصية الأشخاص من خطر الجرائم المعلوماتية وكيفية تتبع المجرمين والعقوبات المقررة لهذه الجرائم¹).

رغم ذلك يبقى هذا القانون فضفاض ولم يعط الجريمة المعلوماتية ماتستحقه من الاهتمام الأمر الذي جعل أحكامه عاجزة عن مواجهة خطر الجرائم المعلوماتية.

الجدير بالإشارة أن الاهتمام على المستوى المحلي بمكافحة الجريمة المعلوماتية قد زاد مع استشعار دول الجوار خطر الإرهاب الدولي وفي هذا السياق اجتمع في ماي 2002 وزراء دول الثمانية بمدينة ترومبكن بكندا لإصدار وثيقة تتضمن مجموعة من التوصيات حول تعقب آثار الاتصالات الهاتفية عبر الحدود من أجل مكافحة الأعمال الإرهابية، وفي ماي 2004 أصدرت دول الثمانية بيانا مشترك صدر بعنوان مواصلة تعزيز القوانين المحلية، وأوصى جميع الدول أن تواصل تحسين القوانين التي تجرم إساءة استخدام الشبكات الالكترونية، والتي تسمح بسرعة التعاون بشأن التحقيقات المتصلة بالإنترنت.

ولعل أفضل وأنسب أنواع التعاون هو التعاون الثنائي الذي ساعد ومن المنتظر أن يضل محافظا على تلك الصفة في مكافحة الجريمة الالكترونية².

¹ المرجع السابق، ص.ص. 42-48.

² المرجع نفسه، ص.ص. 42-48.

المطلب الثالث : الإثبات بالدليل الرقمي

تثير جرائم المعلومات إشكالاً خاصاً يتعلق بمسألة إثباتها، فلا يزال هذا الموضوع مجالاً خصباً للنقاش والتحليل من لدن رجال القضاء والقانون على السواء، وقد برزت أهمية موضوع دليل الإثبات الإلكتروني للجريمة المعلوماتية بفعل قصور وسائل الإثبات الإجرائية المعمول بها في دائرة الجرائم العادية التي تتم في البيئة المادية، عن إثبات الجرائم التي ترتكب في البيئة الافتراضية.

من المفيد التنويه في هذا الإطار إلى أن مواجهة إشكالية إثبات الجريمة المعلوماتية أصبح يتطلب تضافر جهود القانونيين وأجهزة البحث والتحري على المستويين الوطني والدولي، فإذا كان لا يتعذر في الكثير من الأحيان الوصول إلى الدليل المادي بشأن الجرائم العادية فإنه من الصعوبة بمكان إثباته فيما يخص الجريمة المعلوماتية، لاسيما في ظل التطورات التكنولوجية التي يشهدها عالمنا المعاصر، والتي ساعدت على ارتكاب هذه الجرائم دون ترك أي دليل مادي يمكن أجهزة الضبط والتحري من متابعه مرتكبيها باستخدام الوسائل الإجرائية العادية، ولا غرابة في ذلك طالما أنه يرتكبها مجرم يستفيد من الأساليب والتقنيات التكنولوجية الحديثة لتنفيذ الأعمال الإجرامية في مختلف أنحاء العالم عبر شبكة الانترنت، فضلا عن استخدامه ذكائه وإمكانياته العلمية والعملية التي تمكنه من محو الآثار التي يمكن التعرف عليهم من خلالها.

ومهما يكن من أمر يبقى الدليل الرقمي هو المعول عليه في إثبات ارتكاب جريمة معلوماتية معينة في زمان ومكان محددين، لهذا يكون من الضروري علينا ضبط مدلوله والصعوبات المرتبطة به، فضلا على قيمته في الإثبات.¹

¹ يعيش تمام شوقي، مرجع السابق، ص 49-50 .

الفصل الثالث :

دور موقع الشروق و أخبار الوطن

أونلاين في الحد من الجرائم

السيبرانية

المبحث الأول : دور موقع الشروق أونلاين في الحد من الجرائم السيبرانية

المطلب الأول : نبذة تعريفية لموقع الشروق أونلاين

الشروق أونلاين هي موقع إخباري، يومية مستقلة تهتم بالأخبار المحلية والاجتماعية والسياسية والعالمية والرياضية والثقافية وغيرها من الأخبار كالأعياد والإجازات والمنتجعات والعقارات والممتلكات الى جانب التقارير المالية، وسوق الأسهم والاستثمارات والبورصة، وتتطلع أيضاً للمسرح والسينما والثقافة والترفيه .

لقد أطلق مجمع الشروق موقعه الرسمي في حلة جديدة بواجهة عصرية، سهلة التصفح وسريعة الأداء، ووضع بين يدي الجمهور خدمات مميزة تمنح له السبق في الحصول على الخبر . وجعل موقع الشروق خدمة القارئ وتسهيل الوصول للمعلومة على رأس أهدافه، مع التركيز على المصداقية، حاملاً شعار عينك على الجزائر، الوطن العربي والعالم .

وقدم الموقع تركيبة فريدة تمزج بين تقديم الخدمة الإخبارية بسرعة ومهنية عالية، وتوفير أدوات التواصل الاجتماعي بشكل آني وتفاعلي كما تقدم خدمة البث الحي للشروق نيوز والشروق العامة بقلب جديد ومتميز متوافق مع جميع الأجهزة الذكية . وتم إطلاق الموقع الأربعاء، في حفل جمع إدارة المجمع بالصحفيين والتقنيين الذين ساهموا في إخراج الموقع في حلته الجديدة للجمهور الواسع . وأكد مدير مجمع الشروق "رشيد فضيل"، أن الموقع كان فكرة ركز عليها المدير الراحل علي فضيل وسار على نهجها مجموعة من الصحفيين بعده واستكمل المسيرة طاقم شبابي استطاع أن يحقق الهدف الذي رسمه المجمع وهو التموقع محلياً وعربياً والوصول الى الريادة .

ونوه المدير العام بجهود الفريق العامل الذي رفع سقف التحدي عالياً لجعل الموقع على رأس المواقع الإخبارية الجزائرية .

من جهته أكد مدير القطاع الرقمي . سمير فارس . أن العمل جاء نتاج مجهودات فريق متكامل استطاع أن يحقق قفزة نوعية في ظرف وجيز وتمكن من الوصول الى مراتب متقدمة¹ .

¹ مريم حاجي، إستخدام الشباب الجزائري لقناة الشروق و الإشباعات المحققة منها دراسة ميدانية على عينة من شباب مدينة أم البواقي، مذكرة ماستر في علوم الإعلام والاتصال تخصص صحافة وإعلام إلكتروني، جامعة العربي بن مهيدي - أم البواقي، -2016-2017، ص114.

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

كما أثنت مديرة قناة الشروق سلسبيل فضيل ، على مجهودات المبدولة مؤكدة أن الطريق لا يزال مفتوحاً أمام الموقع لإثبات تفوقه بالحرص على المصداقية والسرعة في معالجة الخبر .

ويتميز موقع الشروق أونلاين ببعض الخصائص نذكر منها :

- خدمة إخبارية على مدار الساعة .
- واجهة حديثة وعصرية .
- سهل التصفح وسريع الأداء .
- خدمة البث الحي .

المطلب الثاني : أهداف موقع الشروق أونلاين

من المعروف أن المؤسسات الإعلامية أونلاين تحتوي على رسالة محددة جيداً لها أغراض سامية وهادفة، ومن بين هذه المؤسسات مؤسسة الشروق أونلاين والتي هي الأخرى لها أغراض وأهداف ذات قيم ومبادئ نبيلة وسامية، وتتمثل أهداف هذه الأخيرة فيما يلي :

- ✓ نقل الأخبار والأحداث والمستجدات الوطنية والدولية برؤية موضوعية وحيادية .
- ✓ تغطية الأحداث الوطنية والدولية بكل مهنية واحترافية بعيداً عن التزيف أو التحريف .
- ✓ ترسيخ الهوية والوحدة الوطنية وكذلك إسماع صوت الجزائر في العالم .
- ✓ أن تكون المؤسسة ناقلة للجمهور الجزائري بكل ما يدور حوله في العالم .
- ✓ الدفاع عن مصلحة الوطن والمواطن ونقل الحقيقة كما هي خدمة للجزائر وحرية التعبير.¹
- ✓ فتح مجالها الرقمي الإلكتروني لكل الآراء والتيارات والتوجهات والفعاليات من أجل النقاش الهادف والتحليل البناء .

✓ التوعية والإرشاد جميع الأصعدة العالمية والدولية والوطنية والمحلية، وفي مختلف المجالات السياسية منها والاجتماعية والاقتصادية.... الخ .

✓ رصد ومعالجة كل الظواهر الاجتماعية والاهتمامات التي يواجهها المجتمع الجزائري ومختلف المجتمعات بأسلوب تربوي وأخلاقي، بهدف المساهمة في معالجة الأمراض التي تنخر حياة الأفراد

¹ مريم حاجي، إستخدام الشباب الجزائري لقناة الشروق والإشباع الحقة منها دراسة ميدانية على عينة من شباب

مدينة أم البواقي، مذكرة لنيل شهادة الماستر في علوم الإعلام والاتصال تخصص صحافة وإعلام إلكتروني، جامعة العربي بن مهيدي- أم البواقي، -، 2016-2017، ص114.

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

والجماعات .

- ✓ ستكون مؤسسة الشروق أونلاين لسان حال المواطنين والغلابي و"الزوالية"، وتكون منبراً مفتوحاً للمواطن وانشغالاته ومشاكله مع ضمان نقلها دون تزيف أو تحريف .
- ✓ تزويد المتابعين بالسبق والمساهمة في إضافة الجديد في إطار الرأي والرأي الآخر .
- ✓ ضمان حق المتابع والمشاهد في الإعلام والكلمة الحرة بعيداً عن التجريح والسب والقذف والإساءة وبعيداً عن تصفية الحسابات وترويج المزاعم وتلفيق الاتهامات بلا دليل ولا حجة .
- ✓ ستكون أيضاً مرآة عاكسة للواقع والمشهد الجزائري بلا تضخيم ولا تعميم وبيتنا مفتوحاً لكل الملاحظات والإضافات والانتقادات .

المطلب الثالث : دور موقع الشروق أونلاين في الحد من الجرائم السيبرانية

لمؤسسة الشروق أونلاين دور مهم وفعال في الحد من الجرائم السيبرانية، وذلك من خلال التوعية أونلاين عبر صفحتها الرقمية بخطورة هذه الجرائم وبالتهديدات والأضرار التي تنجم عنها بنشر كل ما يخص وكل ماهو جديد في عالم الجرائم السيبرانية من مقالات ومواضيع وحملات توعوية ومؤتمرات ونشاطاتالخ، وفيما يأتي سنحاول سرد أهم المقالات التي تعاملت معها الشروق أونلاين في مكافحة الجريمة السيبرانية ونشر الوعي بمدى خطورتها واتساع مجالاتها وآفاقها :

❖ نشرت الشروق أونلاين عبر صفحتها الرقمية بتاريخ 2015/08/09 مقال بعنوان " إرانيون ينقلون تجربتهم إلى الشرطة الجزائرية حول الجرائم السيبرانية" حيث شرع وفد من خبراء الشرطة الإيرانية في دورة تكوينية لفائدة إطارات متخصصة من الشرطة الجزائرية، حول الوقاية ومكافحة الجريمة السيبرانية، وعلى مدار 5 أيام، حيث سيتم تبادل الخبرات عن التشريعات الدولية وأفضل الممارسات والمساعدة التقنية والتعاون الدولي، بغية تعزيز سبل مكافحة هذا النوع من الجرائم الحديثة¹.

¹ إيرانيون ينقلون تجربتهم إلى الشرطة الجزائرية، من الموقع: Echourouk online.com

، بتاريخ 2023/03/23، على الساعة: 11:30 .

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

❖ وفي نفس السنة حررت الشروق يوم 2015/10/08 مقال بعنوان "إنشاء هيئة وطنية للوقاية من الجرائم الإلكترونية" فقد قام رئيس الجمهورية عبد العزيز بوتفليقة، على مرسوم رئاسي يتضمن إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وخلص البيان إلى أن هذه التغييرات وعمليات إعادة التنظيم تهدف إلى تعزيز قدرة وفعالية مصالح الاستعلام الوطنية وتكييفها مع التحولات السياسية الوطنية¹.

نشرت الشروق أونلاين مقالا بتاريخ 2016/05/24 تحت عنوان: "الإرهاب الإلكتروني والهجمات السيبرانية" تهدد الأمن والاستقرار؛ حيث أشار اللواء مناد نوبة، قائد الدرك الوطني، من تنامي الجرائم الإلكترونية وتهديداتها، فقد أصبحت تشكل خطرا حقيقيا على أمن الدول من خلال محاولات الاختراق الأمني للمؤسسات العامة والحيوية، واختراق أنظمة البنوك والأفراد وسرقة البيانات والتجسس الصناعي للمواقع الحساسة، كمادعا إلى سن تشريعات جديدة لكشف الجناة وملاحقتهم، وتشديد الرقابة على أجهزة الدولة والشركات والبنوك، وذلك في إطار مقارنة شاملة².

❖ وفي نفس السياق تم نشر مقال في 02/01/2016 تغطية لما صرحت به وزارة الدفاع في مجال مكافحة الجرائم السيبرانية تحت عنوان: "وزارة الدفاع تحبط 12 مليون محاولة اختراق لمواقعها"، فقد صرحت وزارة الدفاع الوطني صرحت بإحباط أزيد من 12 مليون محاولة اختراق لقيادات قواتها ومديريتها المركزية سنة 2016، بمعدل 32 ألف محاولة اختراق يوميا، من قبل عصابات "الهاكرز" من مختلف دول العالم، في إطار ما يعرف بـ "الحرب والإرهاب الإلكتروني"، إلا أن ضباطا أكفاء وقفوا باحترافية لكل المحاولات من خلال التجند المستمر لحماية بنوكها المعلوماتية من أي محاولات اختراق لمواقعها حفاظا على أسرار الدولة الجزائرية.

❖ كما تناول موقع الشروق أونلاين مقالا آخر بتاريخ 2017/01/02 يحمل عنوان "وزارة الدفاع تحبط 12 مليون محاولة إختراق لمواقعها" حيث أحبطت وزارة الدفاع الوطني أزيد من

¹ إنشاء هيئة وطنية للوقاية من الجرائم الإلكترونية، Echourouk online.com بتاريخ 2023/03/24، على الساعة: 09:13.

² الإرهاب الإلكتروني والهجمات السيبرانية تهدد الأمن والاستقرار، Echourouk online.com، بتاريخ 2023/5/15، على الساعة: 15:45.

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

12 مليون محاولة اختراق لقيادات قواتها ومديريتها المركزية سنة 2016، بمعدل 32 ألف محاولة اختراق يوميًا من قبل عصابات "الهاكرز" من مختلف دول العالم، في إطار ما يعرف بـ "الحرب والإرهاب الإلكتروني"، إلا أن ضباطا أكفاء وقفوا باحترافية لكل المحاولات من خلال التجند المستمر لحماية بنوكها المعلوماتية من أي محاولات اختراق لمواقعها حفاظًا على أسرار الدولة الجزائرية¹.

❖ كما ورد في مقال نشر يوم 2017/05/15 تغطية ملتقى بعنوان : "الدفاع السيبراني مكون أساسي للأمن والدفاع الوطني" ، الذي نظّمته مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لدائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي يومي 15-16 ماي 2017 بالنادي الوطني للجيش ببني مسوس، حيث أكد اللواء زراد الشريف رئيس دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي، أن تنظيم الملتقى الأول حول الأمن السيبراني والدفاع السيبراني بالجزائر تحت شعار: "الدفاع السيبراني: مكون أساسي للأمن والدفاع الوطني"، يأتي من أجل خلق فضاء نقاش بين مختلف الفاعلين في الفضاء السيبراني على المستوى الوطني، لفهم أفضل رهانات الأمن السيبراني والدفاع السيبراني².

❖ وفي 2017/10/12 الشروق أونلاين نشرت مقال تحت عنوان: "الجيش يدخل حرب الفضاء الإلكتروني ومكافحة الجوسسة" لقد قررت القيادة العليا للجيش، استحداث مصلحة "الدفاع السيبراني ومراقبة أمن الأنظمة" على مستوى دائرة الاستعمال والتحضير لأركان الجيش

¹ وزارة الدفاع تحبط 12 مليون محاولة الإختراق لمواقعها، Echourouk online.co، بتاريخ: 2023/05/09 ، على الساعة: 9:50 .

² الدفاع السيبراني مكون أساسي للأمن والدفاع الوطني، من الموقع Echourouk online.com ، بتاريخ: 2023/05/09 ، على الساعة: 11:30 .

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

بهدف تأمين وحماية المنظومات والمنشآت الحيوية للبلاد ضد التهديدات والإرهاب الإلكتروني والجوسسة على أسرار الدولة الجزائرية¹.

❖ وتناول الموقع مقالا آخر نشر بتاريخ 2018/04/06 من طرف الصحفي "أحسن حراش" بعنوان "جوسسة إلكترونية تستهدف الوزراء وإطارات الدولة" حيث حذرت مصالح الوزارة الأولى عبر مراسلة رسمية كافة الوزارات وأعضاء الحكومة ومن خلالها موظفي وإطارات الدولة، من انتشار تطبيق خبيث جديد عبر شبكة الإنترنت وبالتحديد بموقع الفيسبوك والمسنجر، حيث يعتمد التطبيق على هويات نسائية وهمية ويستهدف سرقة جميع بيانات الضحايا من رسائل وصور وحتى تحديد مواقعهم. وحسب مراسلة رسمية وجهها الوزير الأول أحمد أويحيى إلى أعضاء طاقم الحكومة، والتي تحوز الشروق نسخة منها، فإن التحذير جاء بناء على تقرير وتنبية وصل مصالحه من المصالح المؤهلة بوزارة الدفاع الوطني يشير إلى حملة جديدة للتجسس السيبرانية تسمى temptingcedar وتستهدف عدة دول منها الجزائر².

❖ كما ورد في مقال نشر من قبل الصحيفة "نواة باشوش" يوم 2018/03/27 بعنوان "اللواء نوبة: الجريمة الإلكترونية والهجمات السيبرانية تهدد الأمن العمومي" فقد صرح مؤكداً اللواء مناد نوبة قائد الدرك، على ضرورة تكثيف الجهود للوقاية من الجريمة الإلكترونية ومكافحتها والتي أصبحت تهدد أمن الدول بأكملها. وجاء في بيان لوزارة الدفاع، أن قيادة الدرك نظمت يومي 27 و28 مارس 2018 بالنادي الوطني للجيش ببني مسوس، الطبعة الثانية من الندوة الدولية حول الأمن السيبراني تحت عنوان "الخدمات الإلكترونية والأمن العمومي"³.

¹ الجيش يدخل حرب الفضاء الإلكتروني ومكافحة الجوسسة، من موقع: echourouk online، بتاريخ: 2023/4/01، على الساعة: 05:30.

² أحسن حراش، جوسسة إلكترونية تستهدف الوزراء وإطارات الدولة، من موقع: echourouk online.com، بتاريخ: 2023/04/03، على الساعة: 04:16.

³ نواة باشوش، اللواء نوبة: الجريمة الإلكترونية والهجمات السيبرانية تهدد الأمن العمومي، من موقع: echourouk online.com، بتاريخ: 2023/04/12، على الساعة: 10:01.

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

❖ وفي نفس السياق قام الصحفي "مُحمَّد مسلم" بنشر مقال يوم 2018/05/07 بعنوان "لوح يدعو إلى اتفاقية دولية لمحاربة الجرائم الإلكترونية" فقد دعا وزير العدل حافظ الأختام الطيب لوح، إلى بذل الجهود من أجل الوصول إلى اتفاقية دولية للوقاية ومحاربة الجريمة الإلكترونية، وذلك عبر تعزيز آليات التنسيق والتعاون بين الدول، لمواجهة مثل هذه الأخطار¹.

❖ وفي نفس المجال نشر موقع الشروق أونلاين مقال بتاريخ 2019/11/14 تحت عنوان "جهود لمواجهة الجرائم الإلكترونية" بأن خبراء في أمن المعلومات دعوا إلى ضرورة توحيد الجهود الخليجية لمواجهة تحديات التكنولوجيا وتوفير الحماية اللازمة للبيانات والمعلومات الحساسة الخاصة بدول مجلس التعاون الخليجي عبر وضع إستراتيجيات وطنية لمواجهة تلك التحديات².

❖ وجاء في مقال آخر حرر من طرف موقع الشروق أونلاين بـ 2021/01/13 المنطوي تحت عنوان: "151 متورط.. كورونا ترفع الجرائم السيبرانية"، مع الإنتشار الهائل لوباء كورونا وتزامناً مع الحجر الصحي الذي فرضه هذا الأخير نتج عنه تورط 1514 شخص في 2026 جريمة سيبرانية، على مستوى منطقة وسط البلاد، خلال سنة 2020، حسب حصيلة كشف عنها المفتش الجهوي لشرطة منطقة الوسط بن شيخ فريد زين الدين³.

❖ كما نشر الصحفي "عمار يزلي" مقالا بتاريخ 2021/02/12، يحمل عنوان "رهان آبي لأمننا السيبراني" فالحديث عن "الأمن السيبراني"، حاضر اليوم في كل بقعة بعدما صار مطلباً رئيساً وملحاً إثر انفلات الأمور من بين أيدي المروجين له والمنتجين والمستهلكين

¹ مُحمَّد مسلم، لوح يدعو إلى إتفاقية دولية لمحاربة الجريمة الإلكترونية، من موقع echourouk online.com ، بتاريخ: 202/04/13، على الساعة: 07:20 .

² جهود لمواجهة الجرائم الإلكترونية، من موقع: echourouk online.com ، بتاريخ: 2023/04/15، على الساعة: 06:00.

³ 1514 متورط كورونا ترفع التحدي، من موقع: echourouk online.com ، 17 بتاريخ: 2023/04/، على الساعة: 20:14.

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

لبرامج برمجيات الاتصال الحديث ومنصات التواصل الاجتماعي، غير أن هذه الوسائط و"منصات الإطلاق". هو سلاح ذو حدين تتمتع به هذه الوسائط، وهو يستعمل اليوم على نطاق أوسع بفعل انتشار الأنترنت وتطوره جيلا بعد جيل. كل أشكال الجريمة صارت اليوم حاضرة في هذا الفضاء، إن لم نعرف كيف نتحصن بالتطوير الدائم والمستمر والمستमित لأنظمتنا الدفاعية ضد الغزو السيبراني من جهة، وضد الجريمة الفردية والمنظمة من جهة أخرى، في زمن نراهن فيه على دخول سوق الاقتصاد والتبادل من بوابة الإنترنت¹.

❖ ونظراً لارتفاع حصيلة المتورطين في الجرائم السيبرانية نشرت الشروق أونلاين في 2021/05/23 مقال يتناول تصريح من الفريق شنقريجة تحت عنوان "أحبطنا كافة الهجمات السيبرانية ضد الجزائر"، قال رئيس أركان الجيش الوطني الشعبي، الفريق سعيد شنقريجة، إن الجزائر تمكنت من إحباط كل الهجمات السيبرانية والمؤامرات المنفذة عبر فضاء الأنترنت والتي زادت حدتها خلال الآونة الأخيرة بعد تجاوزت البلاد لأزمته².

❖ نشر الصحفي "خالد.م" يوم 2021/06/16 مقال بعنوان "بلحيمر: ضمان سيادة سيبرانية أولوية لتحسين الشباب العربي" فقد أكد وزير الاتصال، الناطق الرسمي للحكومة، عمار بلحيمر، بالقاهرة أن الجزائر تولي أهمية خاصة لدور الإعلام في التكفل بالشأن الداخلي والدفع بالقضايا العربية وذلك من خلال سياسة اتصال حديثة تعتمد على توظيف الرقمنة والإعلام الإلكتروني على أوسع نطاق³.

❖ كما ورد في مقال نشره موقع الشروق أونلاين يوم 2021/07/02 تحت عنوان "الحرب السيبرانية : الإستعداد لقيادة المعارك العسكرية في الميدان الخامس" حيث أصدر مركز المستقبل

¹ عمار يزلي، رهان آني لأمننا السيبراني، من موقع: echourouk online.com، بتاريخ: 2023/04/18، على الساعة: 21:23.

² أحبطنا كافة الهجمات السيبرانية ضد الجزائر، من موقع: Echourouk online.com، بتاريخ: 2023/04/02، على الساعة: 23:02.

³ خالد.م، بلحيمر: ضمان سيادة سيبرانية أولوية لتحسين الشباب العرب، Echourouk online.com، 2023/04/21، 13:13.

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

للأبحاث والدراسات المتقدمة، ضمن إصداراته سلسلة "كتب المستقبل"، كتاباً جديداً بعنوان "الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس"، من تأليف الدكتور إيهاب خليفة، رئيس وحدة التطورات التكنولوجية بالمركز، ليلقي الضوء على مفهوم الحرب السيبرانية والمقصود بها وتحديد أبعادها وخصائصها والأسلحة المستخدمة فيها، ويوضح كيفية قياس التهديدات السيبرانية والتي يمكن من خلالها التفريق بين حالة الخطر وحالة التهديد وحالة الحرب، ويستعرض أهم نماذج الجيوش السيبرانية في العالم، كما يستعرض مفاهيم الأمن والدفاع والردع السيبراني¹.

❖ وفي 2021/8/23 كتب "مُجدّ مسلم" مسؤول الملف السياسي بجريدة الشروق مقال تحت عنوان "محرابة الجرائم الرقمية يجب أن تتحول الى ثقافة وتعليم"، حيث جاء في بيان اجتماع مجلس الوزراء الأخير حديث عن "تثمين إنشاء القطب المتخصص في الجرائم السيبرانية، كمكسب لقطاع العدالة على غرار القطب المتخصص في الجرائم الاقتصادية، مع التشديد على الإسراع في تنصيب القطب الجديد ومعالجة الجرائم السيبرانية المعروضة حالياً، أمام العدالة"².

❖ وفي نفس المجال نشر الموقع مقال آخر يوم 2021/09/08 بعنوان "الشرطة تعلن عن مخطط جديد لمواجهة الجريمة الإلكترونية" حيث كشفت المديرية العامة للأمن الوطني عن وضع مخطط جديد لمواجهة الجريمة الإلكترونية التي تجاوزت في 2020 الخمسة آلاف جريمة. وقال الملازم الأول "مطمط أمين" في تصريح للإذاعة الجزائرية، أن الشرطة خصصت فرقا خاصة بمكافحة الجريمة المعلوماتية، مضيفاً أن المصلحة المركزية لمكافحة الأمن المعلوماتي تسهر عبر فرقها الموجودة على مستوى 58 ولاية³.

Echourouk ، الحرب السيبرانية : الإستعداد لقيادة المعارك العسكرية في الميدان الخامس، 2023/04/22، 14:14.

online.com¹

²مُجدّ مسلم، محاربة الجرائم الرقمية يجب أن تتحول إلى ثقافة وتعليم، echourouk online.com، 2023/04/22، 9:50.

³ الشرطة تعلن عن مخطط جديد لمواجهة الجريمة الإلكترونية، 2023/04/24، 08:10. echourouk online.com

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

❖ وتبعاً لمواضيع الجرائم السيبرانية وخطورتها تم إنشاء قطب جزائي من قبل رئيس الجمهورية لردع هاته الجرائم وهو ما حررته "إلهام بوثلجة" إحدى صحفيات جريدة الشروق في مقال بتاريخ 2021/8/6 تحت عنوان "استحداث قطب جزائي متخصص سيكبح الجرائم السيبرانية"، لقد ثمن خبراء في القانون قرار رئيس الجمهورية عبد المجيد تبون خلال اجتماع المجلس الأعلى للأمن، والرامي إلى استحداث قطب جزائي جديد مكلف بمتابعة الجرائم السيبرانية ومكافحتها، فضلاً عن متابعة المتورطين في نشر الأخبار الكاذبة عبر منصات التواصل الاجتماعي بغرض التهويل، معتبرين بأنه سيحد من الانتشار الفادح للجرائم الإلكترونية وحتى بالنسبة للأخبار الزائفة التي انتشرت كالنار في الهشيم عبر فيسبوك وتويتر¹.

❖ مع التطور التكنولوجي الحاصل أدى إلى ارتفاع كبير جداً في معدل الجرائم السيبرانية وهذا ما تحدث عنه الصحفية الشروق "نؤارة باشوش" في مقال نشرته يوم 2021/11/23 بعنوان "الإجرام الإلكتروني ... أرقام مرعبة" حيث أشارت إلى ما قاله وزير العدل حافظ الأختام عبد الرشيد طبي على تشديد العقوبات ضدّ الجرائم السيبرانية، من خلال إنشاء القطب الوطني المتخصص في محاربة الجريمة الإلكترونية، فيما حذرت المصالح الأمنية من ارتفاع الجرائم الإلكترونية في الجزائر، بعد أن قفزت الجريمة من العالم الحقيقي إلى الافتراضي العابر للحدود نظراً لسرعة تنفيذها، حيث سجلت مصالح الدرك والشرطة ما يربو عن 8 آلاف جريمة إلكترونية خلال 2020 مما جعلها تنافس الجريمة التقليدية².

❖ نشر الصحفي "منير ركاب" بتاريخ 2022/01/17 مقال بعنوان "الدفاع السيبراني طرف فعال في العمليات العسكرية" لقد أكد اللواء "محمد عمر"، قائد مدرسة القيادة والأركان، الشهيد حمودة أحمد المدعو "سي الحواس"، بتمتفوستن بالناحية العسكرية الأولى في العاصمة، على أهمية الدفاع السيبراني ومراقبة أمن الأنظمة، والذي يهدف إلى حماية المنشآت الحيوية والمؤسساتية وتأمينها ضد التهديدات الخارجية والداخلية، من خلال استحداث مصلحة لتلقين الضباط

¹ إلهام بوثلجة، استحداث قطب جزائي متخصص سيكبح الجرائم السيبرانية، من موقع echourouk . 03:09، 2023/04/25، online

² نؤارة باشوش، الإجرام الإلكتروني أرقام مرعبة، echourouk online.com، 2023/04/26، 15:15.

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

المتربصين وكيفية صد الضربات الإلكترونية الخارجية التي تستهدف أنظمة المعلومات، ومنظومات الاتصال، ومختلف مصالح وقيادات الجيش الوطني الشعبي، بضربات مضادة، بعد تكوين جاد يستفيد منه الضباط المتربصون، المتخرجون من الأكاديمية العسكرية لمختلف الأسلحة بشرشال¹.

❖ تماشياً مع الارتفاع المتزايد في نسب الجرائم السيبرانية قادة الجزائر بنجاح مسار لمكافحة هاته الجرائم، وهو ماتم الإعلان عنه في مقال يوم 2022/3/16 عبر الشروق أونلاين اندرج تحت عنوان " الجزائر تقود بنجاح المسار الأممي لمكافحة الجرائم السيبرانية"، فقد حققت الجزائر نجاحا دبلوماسيا لافتا خلال ترأسها للدورة الأولى للجنة الأمية المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية، المنعقدة مؤخرا بمقر الأمم المتحدة بنيويورك².

❖ كما ورد في مقال لصحفي "بلقاسم حوام" نُشر يوم 2022/3/28 تحت عنوان " أول مركز للتكوين في الأمن السيبراني بالجزائر قريبا"، حيث أعلنت "فلة قوار"، رئيسة شركة "INTELLIGENT NETWORK" عن فتح أول مركز وطني للتكوين في قضايا الأمن السيبراني في الجزائر من طرف المنظمات الدولية، والذي يهدف حسبها إلى تعزيز تقنيات الدفاع والحماية ضد مختلف أنواع الهجمات السيبرانية التي تتعرض لها مختلف المؤسسات والبنى التحتية وحتى الأشخاص في الجزائر³.

❖ وفي نفس المجال تم نشر مقال في 2022/5/30 من طرف "أمين شاوش" أحد الصحفيين بمؤسسة الشروق أونلاين يحمل عنوان: "مختصون: هكذا يتم مواجهة الإرهاب السيبراني وتحقيق السيادة الرقمية في الجزائر" حيث حرر هذا الأخير بأنه قد أجمع المشاركون في

¹ منير ركاب، الدفاع السيبراني طرف فعال في العمليات العسكرية، من موقع echourouk online.com، 2023/04/27، 12:30.

² الجزائر تقود بنجاح المسار الأممي لمكافحة الجرائم السيبرانية، 2023/5/9، 9:50، Echourouk online.com.

³ بلقاسم حوام، أول مركز للتكوين في الأمن السيبراني في الجزائر، 2023/04/28، 01:12.

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

الملتقى الوطني الافتراضي حول التهديدات السيبرانية وتداعياتها على الأمن الوطني الجزائري على ضرورة تطوير آليات تحقيق الأمن السيبراني والسيادة الرقمية¹.

❖ وفي المجال السيبراني أيضا نشر موقع الشروق أونلاين مقال يوم 2022/08/28 تحت عنوان "اتصالات الجزائر تضم مكتشف ثغرة آبل إلى مركزها للدفاع السيبراني" أعلن المدير العام لاتصالات الجزائر عادل بن تومي يوم الأحد، عن التحاق الشاب عبد القادر مواز الذي اكتشف ثغرة أمنية في موقع شركة "آبل"، للعمل بمركز الدفاع السيبراني للمؤسسة العمومية، وأكد المسؤول في ذات المنشور توصل اتصالات الجزائر إلى اتفاق مع الشاب مواز، لانضمامه إلى مركز الدفاع السيبراني للشركة، تعزيزا لصفوفها، ولتطوير مؤهلاته في المجال².

وفي نفس السياق نشرت الشروق أونلاين مقال يوم 2022/11/10 يندرج تحت عنوان "قضية بيغاسوس: يونيسكو تعزل موظفة مغربية بعد تجنيدها من قبل مخابرات الرباط" فقد أصدرت منظمة الأمم المتحدة للثقافة والعلوم يونيسكو، قرارا بعزل موظفة من جنسية مغربية، بعد تحقيق داخلي أثبت تجنيدها من قبل مخابرات الرباط في قضية تجسس تخص ملف برنامج بيغاسوس. وحسب ما نقل موقع "أفريكأنتيليجونس" الفرنسي، فإن موظفة من جنسية مغربية تسمى "وفاء.ب"، تم عزلها من منصبها كمديرة لوحدة إدارية بمنظمة اليونسكو، عقب تحقيق إداري دام أشهر، أظهر عملها لصالح المخابرات المغربية بتسريب معلومات حول منطمتين حقوقيتين فجرتا عام 2021، فضيحة التجسس باستعمال برنامج بيغاسوس والتي تورطت فيها الرباط³.

¹ أمين شاوش، مختصون: هكذا يتم مواجهة الإرهاب السيبراني وتحقيق السيادة الرقمية في الجزائر، echourouk online.com، 2023/04/29، 11:45.

Echourouk ، اتصالات الجزائر تضم مكتشف ثغرة آبل إلى مركزها للدفاع السيبراني، 2023، 17:06/04/29 .
online.com²

³ ، قضية بيغاسوس: يونيسكو تعزل موظفة مغربية بعد تجنيدها من قبل مخابرات الرباط، 2023/04/30، 09:09.
Echourouk online.com

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

❖ نشر الصحفي "ع.س" يوم 2022/12/18 مقال بعنوان "قبة حديدية سيبرانية مشتركة بين المخزن والكيان الصهيوني" حيث أعلن الكيان الصهيوني شروعه في العمل مع المغرب ودولتين عربيتين أخريين على مشروع "القبة الحديدية السيبرانية"، بزعم إنشاء منصة دفاعية مشتركة ضد الهجمات الإلكترونية المتوقعة من قراصنة "الأعداء المشتركين"، الأمر الذي يمهّد لإنشاء أول منظومة دفاعية مشتركة في هذا المجال بين الدول التي تعتبرها دولة الاحتلال جزءاً من معاهدات السلام التي تطلق عليها اسم "اتفاقيات أبراهام"¹.

❖ وفي 2023/01/17 نشر موقع الشروق مقال تحت عنوان "المنشآت الطاقوية في الجزائر مؤمنة ضد الهجمات السيبرانية" أكد مدير الأمن الداخلي لدى مجمع سوناطراك منير بلحسين أن الشركة تتبنى أنظمة للوقاية ومكافحة الهجمات السيبرانية التي تستهدف المعطيات الإستراتيجية. وقد تمكّنت سوناطراك، "بفضل الوسائل التكنولوجية المتطورة التي بحوزتها، من أن تواجه هذا النوع من الهجمات بكل جدارة"، يقول المسؤول ذاته².

وتناولت الشروق أونلاين في مقال آخر نشر بتاريخ 2023/02/12 تحت عنوان "هجمات سيبرانية حادة من المغرب والكيان الصهيوني على وكالة الأنباء الجزائرية" بأن الموقع الإلكتروني لوكالة الأنباء الجزائرية تعرض منذ ساعات، إلى سلسلة من الهجمات السيبرانية "الحادة"، حسب ما ذكرته الوكالة. وقامت وكالة الأنباء الجزائرية بحجب موقعها الإلكتروني بشكل مؤقت، جراء الهجمات التي كانت تستهدف اختراقه، حسب المصدر. وقالت الوكالة إن سلسلة من الهجمات الحادة، اتّضح أن مصادرها الجغرافية من الكيان الصهيوني، والمغرب، وبعض المناطق في أوروبا، قد تمّ رصدّها.

❖ كما نجد في مقال آخر حرر بتاريخ 2023/2/15 "... الدرك الوطني يكشف عن حصيلة الجرائم السيبرانية بالجزائر عامي 2022 و 2023"، حيث كشف الرائد "فريد درامشية"

¹ ع.س، قبة حديدية سيبرانية مشتركة بين المخزن والكيان الصهيوني، من موقع echourouk online.com، 22:30، 2023/05/01،

² المنشآت الطاقوية في الجزائر مؤمنة ضد الهجمات السيبرانية، 18:18، 2023/05/02، Echourouk online.com

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

المختص في الإجرام السيبراني بقيادة الدرك الوطني عن معالجة 500 جريمة سيبرانية منذ بدء سنة 2023، كما نبّه درامية إلى أنّ الإجرام الإلكتروني في تزايد مستمر، حيث قفز من 2838 جريمة في 2021، إلى 4600 قضية في 2022، مسجلاً 500 قضية إجرام إلكتروني منذ انطلاق العام الحالي¹.

❖ وفي نفس اليوم تم نشر مقال من طرف الصحفية "نؤارة باشوش" 2023/02/15 بعنوان "الجريمة السيبرانية أسلحة الجناة الجديدة لضرب الأشخاص والإقتصاد" حذرت المصالح الأمنية والجهات القضائية من ارتفاع الجرائم الإلكترونية أو ما يعرف بالجرائم "السيبرانية"، إذ سجلت مصالح الدرك والشرطة والأمن العسكري قرابة 12 ألف جريمة إلكترونية خلال سنة 2022 وشهر جانفي من سنة 2023، شملت اختراق مواقع مؤسسات وشركات عمومية وخاصة وكذا الجرائم المالية والاقتصادية، خاصة العابرة للحدود وتلك المستحدثة، إلى جانب الابتزاز، التهديد والتشهير، المساس بالحريات الشخصية والحياة الخاصة عبر شبكات التواصل الاجتماعي، إلى جانب نشر المعلومات الزائفة والمضللة، القرصنة والتحرش الإلكتروني والنصب والاحتيال².

❖ وفي نفس المجال تناول الصحفي "عبد الحميد عثمان" حوار لصحفي والحقوقي "منصور قدور بن عطية" يوم 2023/05/06 بعنوان "بيغاسوس كل تفاصيل ملكة التجسس بالوثائق" بمناسبة صدور مؤخرًا كتاب توثيقي جد مهم، بعنوان "بيغاسوس ملكة التجسس"، للصحفي والحقوقي الجزائري منصور قدور بن عطية، عن دار الوعي للنشر والتوزيع بالجزائر العاصمة، وهو أول عمل جزائري يسلط الضوء بشكل مكثف حول فضيحة التجسس باستخدام برنامج بيغاسوس الذي طورته الشركة الإسرائيلية "أن أس

¹ الدرك الوطني يكشف حصيلة الجرائم السيبرانية بالجزائر عامي 2022 و2023، 2023/05/05، 19:00 . Echourouk online.com.

² نؤارة باشوش، الجريمة السيبرانية أسلحة الجناة الجديدة لضرب الأشخاص والإقتصاد ' echouriuk . 12:08، 2023/05/06، online.com

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

أو“ واستعمله المخزن ودول أخرى عن كتب للتطفل على الأصدقاء، والجيران قبل الخصوم السياسيين¹.

❖ كما ورد في مقال للصحفي "حسان حويشة" يوم 2023/05/12 يحمل عنوان "إحباط قرابة 30 مليون تهديد سيبراني ضد الجزائر" فقد أظهر تقرير حديث لرائد عالمي في الأمن السيبراني أن برمجياته الدفاعية أحبطت ما لا يقل عن 29.7 مليون هجمة ضد الجزائر في عام 2022، منها أكثر من 19 مليون تهديد طال عناوين بريد إلكتروني جزائرية.

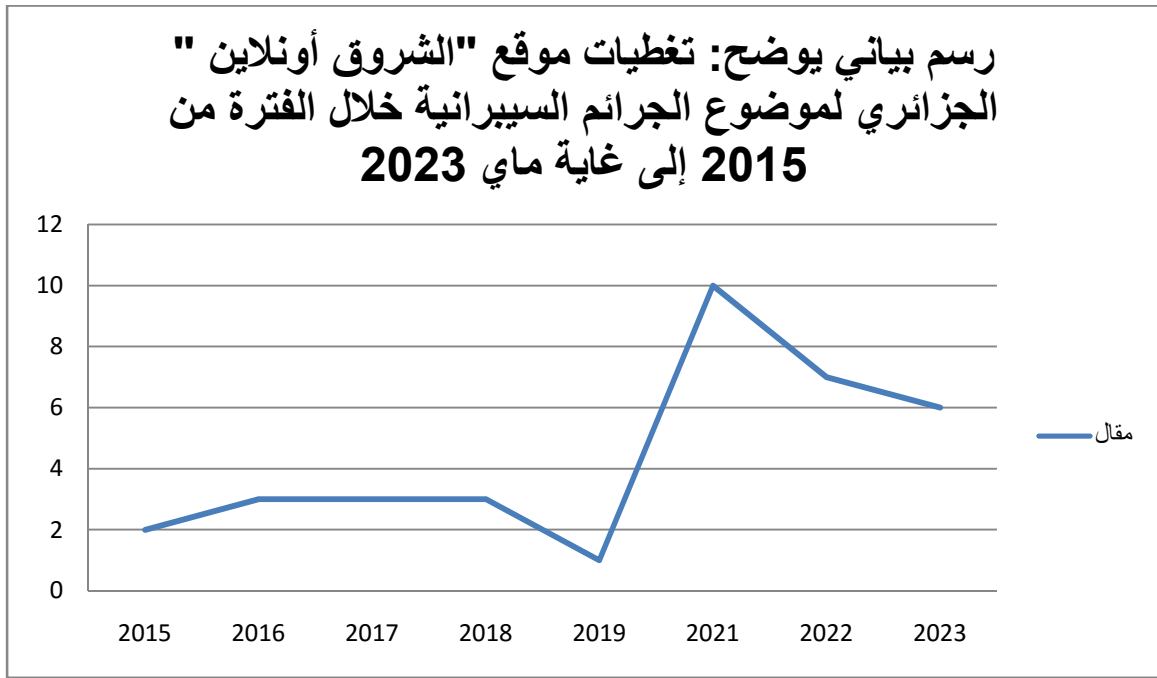
جدول: يبين مختلف التغطيات الإعلامية لموقع "الشروق أونلاين" حول الجرائم السيبرانية خلال الفترة من 2015 إلى غاية ماي 2023

السنة	نوع التغطية	عددها
2015	- مقال صحفي	02
2016	- مقال صحفي	03
2017	- مقال صحفي	03
2018	- مقال صحفي	03
2019	- مقال صحفي	01
2021	- مقال صحفي	10
2022	- مقال صحفي	07

¹ عبد الحميد عثمان، بيغاسوس كل تفاصيل مملكة التجسس بالوثائق، من موقع echourouk online.com ، 07:04، 2023/05/07 .

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

05 01	- مقال صحفي - حوار	2023
37 مقالا 01 حوار	المجموع	



المصدر: تغطيات موقع "الشروق أونلاين" الجزائري لموضوع الجرائم السيبرانية خلال الفترة من 2015 إلى غاية ماي 2023 (الطالبتان بتصرف)

نستنتج من الجدول و الرسم البياني أعلاه ،أن موقع "الشروق أونلاين" ، عرض وعالج مختلف التغطيات الإعلامية حول الجرائم السيبرانية خلال الفترة من 2015 إلى غاية ماي 2023، فقد تم اختيار هاته الفترة لأنها عرفت اهتماما بالمواضيع المتعلقة بالجرائم السيبرانية.

حيث نسجل أن موقع "الشروق أونلاين" في تغطيته لموضوع الجرائم السيبرانية في الفترة المدروسة (2015 إلى غاية ماي 2023) ؛فقد عرف في بداية الفترة تدبدا نوعا في التغطية الإعلامية للموضوع ، بينما شهدت الفترة الأخيرة ارتفاع نسبة التغطية الإعلامية للموضوع ، و هذا ما يبين

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

زيادة اهتمام موقع "الشروق أونلاين" بالجريمة السيبرانية ؛ و هذا ما يساهم في زيادة الوعي بمخاطرها و الحد منها.

ففي سنة 2015 سجلنا مقالين تناولوا الجرائم السيبرانية، الشيء نفسه سجلناه سنة 2016. بينما في سنتي 2017 و 2018 فقد اختلف الأمر قليلا عن سابقه وارتفع إرتفاعا طفيفا إلى 3 مقالات في كل سنة. أما في سنة 2019 لم ينشر الموقع مقالا واحدا فقط، ويمكن تفسير هذا النقص بأن الموقع آنذاك كان مهتما بمواضيع أخرى أكثر على غرار المجال السيبراني، كمواضيع الحراك في الجزائر، و أزمة وباء كورونا.

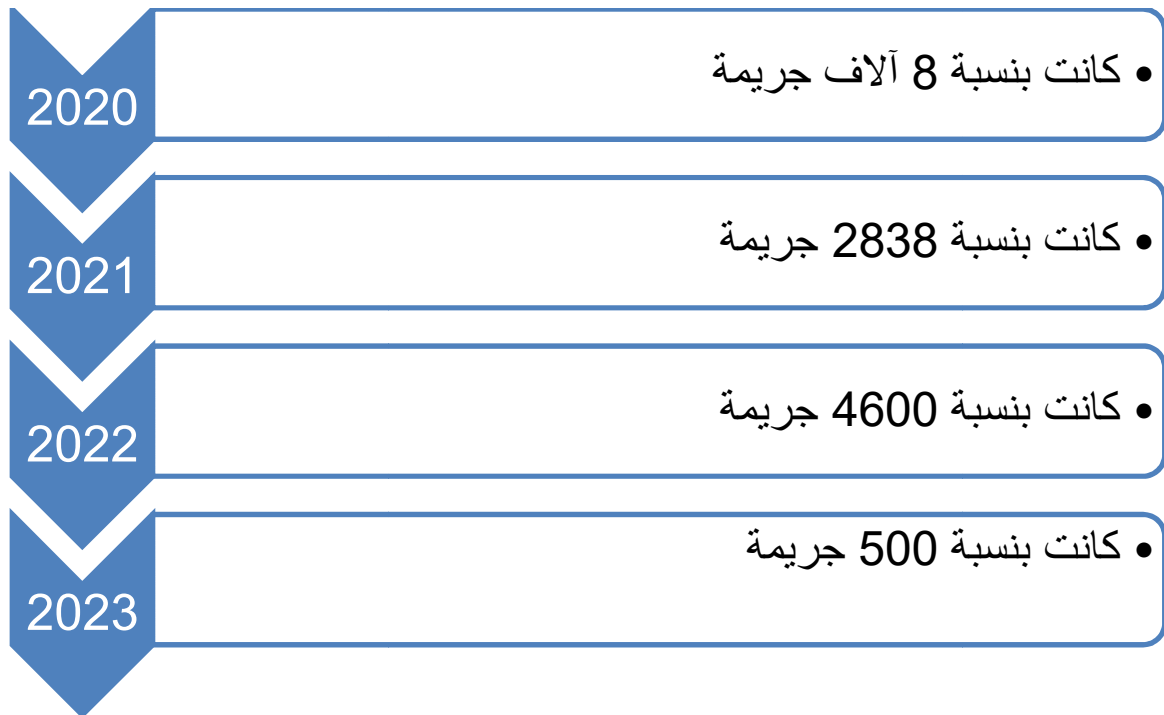
أما سنة 2020 لم نسجل أي مقال بخصوص الجرائم السيبرانية، ويمكن تبرير ذلك بإنشغال الموقع برصد أخبار جائحة كورونا التي اجتاحت العالم أجمع؛ حيث أن هذه الأخيرة لم تشغل موقع "الشروق أونلاين" فقط بل العالم ككل. فقد كانت مادة دسمة لمختلف المواقع الإلكترونية و وسائل الإعلام المختلفة التي أصبحت شغلهم الشاغل.

أما بالنسبة لسنة 2021 فقد اختلف الأمر كثيرا عن السنوات الماضية، حيث نشر موقع الشروق أونلاين 10 مقالات حول الجرائم السيبرانية فشهدت هذه الفترة ارتفاع ملحوظ من ناحية عدد المقالات ومن ناحية اهتمام الموقع بموضوع التهديدات و الجرائم السيبرانية على حد سواء، فقد أصبح الموقع يبدى اهتماما أكثر بموضوع الجرائم السيبرانية ، من خلال التغطية الإعلامية لجميع الملتقيات والمؤتمرات والندوات. ومواكبة كل ما هو جديد ويخص المجال السيبراني. كما تابع الموقع نشره لمواضيع حول الجرائم السيبرانية .

نفس الشيء نسجله سنة 2022 ، بمواصلة موقع "الشروق أونلاين" تغطيته لمواضيع الجرائم السيبرانية بـ 7 مقالات. أما في سنة 2023 و إلى غاية ماي 2023 ؛ فنسجل أرتفاعا لا بأس به في نسبة تغطية موقع "الشروق أونلاين" لموضوع الجرائم السيبرانية ، و هذا ما يبين من جهة ارتفاع نسبة الجرائم السيبرانية ، و من جهة أخرى زيادة اهتمام موقع "الشروق أونلاين" بالتغطية الإعلامية لمواضيع الجريمة السيبرانية ، و هذا ما يساهم بشكل أو بآخر في الحد منها و نشر الوعي الوطني بمخاطرها.

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

مخطط يبين نسبة الجرائم السيبرانية من سنة 2020 إلى سنة 2023



المصدر : من موقع Echourouk online.com

المبحث الثاني : دور موقع أخبار الوطن أونلاين في الحد من الجرائم السيبرانية

المطلب الأول : نبذة تعريفية لموقع أخبار الوطن أونلاين

أخبار الوطن شبكة إخبارية جزائرية متعددة الوسائط، أصدرها صحفيون جزائريون شباب في خضم الحراك الشعبي السلمي، تهدف إلى إعادة الاعتبار للممارسة العالمية وإحداث اتصال بين القارئ والمشاهد والصحافة من خلال المعلومة الصادقة والخبر اليقين، والتحليل الموضوعي والمنهجي وفق القيم المهنية المتعارف عليها عالميا.

فهي شبكة إخبارية جزائرية تأسست يوم 05-10-2019 ، معتمدة من قبل وزارة الاتصال.
* نبذة تاريخية:

- ولأن كل مشروع هو عبارة عن حلم، قبل أن يتشكل في فكرة، ليولد ويتجسد على الأرض كجسد ملموس، كذلك أخبار الوطن.

فقد كانت حلم حملة صحفيون أصدقاء، كانوا يتطلعون إلى ممارسة مهنية مغايرة على تلك التي اختبروها في مختلف المؤسسات الإعلامية التي مروا منها أو سيروا تحريرها أو ساهموا في تأسيسها، اذ لعبت الخبرة والكفاءة والاحترافية دورها الفعال في رسم شكل ومسار شبكة أخبار الوطن، هيكلية وتأطيرا وسياسة تحريرية، وعلاقات عامة¹.

في الخامس من أكتوبر عام 2019، وفي أوج الحراك الشعبي المبارك الذي انطلق في الثاني والعشرين من شهر فبراير عام 2019، ولدت شبكة أخبار الوطن الجزائرية، في ظروف سياسية

¹ رياض هويلي، المدير التنفيذي مسؤول النشر بشبكة اخبار الوطن، "نبذة تاريخية عن شبكة أخبار الوطن"، مقال مرسل عن طريق البريد الإلكتروني للأستاذ المشرف ، بتاريخ 2023/05/28، الساعة : 15:30

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

وإعلامية يميزها مطالبة الجزائريين بالتغيير السلمي وبناء دولة المؤسسات، وتنظيم الحياة العامة بما يمليه القانون.

في هذه الأجواء، اختار مجموعة من الصحفيين المحترفين، إطلاق "شبكة أخبار الوطن"، آخذين بالحسبان حاجة الجزائريين الى إعلام بديل وموضوعي وحر ومسؤول و نزيه، يقدم خدمة عمومية محترفة، يدافع عن الوطن ضد الهجمات السيبرانية، ويقدم للمواطن المعلومة الصادقة الصحيحة والتحليل الواعي بعيدا عن أي تكلس إيديولوجي أو تقوقع مصلحي أو انحياز فتوي¹.

ولأن هؤلاء الصحفيين المحترفين، ملمون بالتحولات التي تعرفها الساحة الاعلامية وطنيا ودوليا، فقد تم اختيار شبكة وليس مجرد جريدة او موقع الكتروني . والشبكة هي خدمات اعلامية متكاملة ومتشابكة: جريدة ورقية، موقع الكتروني باللغتين العربية والفرنسية، مع تلفزة رقمية web tv . ووفق هذه الرؤية، استطاعت شبكة اخبار الوطن ان تحتل مكانة لا بأس بها في الساحة الاعلامية الجزائرية وتتصدر المشهد في الكثير من الاحيان نظرا لتكامل مجالات نشاطها وتنوعها بين الصحافة المكتوبة و الصحافة الالكترونية التي تستخدم الوسائل التكنولوجية الحديثة علاوة الى التوظيف الايجابي لوسائل التواصل الاجتماعي، وكذلك خدة السمعي البصري، وهو ما جعل جمهورها متنوع ومتعدد، ونوعي أيضا².

اعتمدت أخبار الوطن على طاقم شاب، وادخلت واستخدمت لأول مرة غرفة أخبار مدجة وتفاعلية، إذ أصبح الصحفي في أخبار الوطن يختلف عن الصحفي التقليدي، فهو يمارس كل الانواع الصحفية وكل الفروع في وقت واحد/ صحافة مكتوبة، الكترونية وسمعية بصرية.

ترفع أخبار الوطن شعار المصادقية قبل السبق، وهو ما جعلها تكتسب مكانة هامة لدى القراء وصناع القرار والنخب السياسية والعلمية، حيث تمكنت من فتح فضاءاتها للكتاب والمثقفين

¹ المرجع السابق.

² المرجع نفسه.

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

والسياسيين والمسؤولين، وباتت قبلتهم في استقاء الاخبار ومتابعة التحاليل ومختلف الأنشطة التي تهم المواطن والمجتمع على حد سواء.

المطلب الثاني : أهداف موقع أخبار الوطن أونلاين

بطبيعة الحال، لكل وسيلة إعلامية أهداف مسطرة من قبل المؤسسين، إن كانت إعلامية أو سياسية أو إيديولوجية، أو تجارية. ومن هذا المنطلق، وبما أن "أخبار الوطن" أسسها صحفيون، فقد تجلت أهدافها فيما يلي¹:

- إعطاء دفعا قويا ونفسا جديدا للممارسة المهنية وفق رؤية تأخذ بعين الاعتبار التحولات الجارية في الساحتين الدولية والوطنية وما صاحبهما من إفرازات التطور التكنولوجي والرقمي على الأداء الصحفي بشكل عام
- تقديم خدمة اعلامية متميزة، وفق المعطيات السالفة الذكر، ومنه المساهمة في صناعة مشهد إعلامي تنافسي.
- المساهمة في الدفاع عن ثوابت المجتمع الجزائري وصيانة أركان الدولة، أمام تزايد الحروب الناعمة التي يستخدم فيها الإعلام كسلاح فتاك.
- إبراز الثقافة الجزائرية وبعدها التاريخي والحضاري بين الأمم ورد الحملات التضليلية التي تستهدف الجزائر شعبا ودولة
- خلق وعي وطني جزائري حول القضايا المصيرية التي تهم البلد والمجتمع.
- المساهمة في بلورة مشروع وطني من خلال فتح النقاش المسؤول أمام النخب ومنه استكشاف الكفاءات الوطنية.

¹ رياض هويلي، المدير التنفيذي مسؤول النشر بشبكة اخبار الوطن، " أهداف شبكة أخبار الوطن "، مقال مرسل عن طريق البريد الإلكتروني للأستاذ المشرف ، بتاريخ 2023/05/28، الساعة : 15:30

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

- المساهمة في تكريس مبدأ التعددية الاعلامية والسياسية بحسب مضمون الدستور الجزائري ومنه تكوين وعي مواطناتي قائم على الحوار والتعايش.
- كما يمكن تلخيص مجمل أهداف " أخبار الوطن " فيما يلي¹:
- نقل الأخبار والأحداث والتطورات الوطنية والدولية.
- تغطية الفعاليات الوطنية والدولية باحتراف وموضوعية.
- نقل كل ما يجر حول العالم للجمهور الجزائري.
- التوعية والارشاد على جميع المستويات السياسية والاقتصادية والاجتماعية وغيرها من المجالات.
- فتح مجالها الرقمي الإلكتروني أمام كافة الآراء والتيارات والاتجاهات والاحداث للنقاش والبناء.
- منح المتابعين السبق في كل ما هو جديد على الصعيد الوطني والمحلي.

¹ الطالبتان بتصرف، من الموقع: <https://akhbarelwatane.dz/apropos/> ، بتاريخ: 2023/04/27 ، على الساعة: 22:10 .

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

المطلب الثالث : دور موقع أخبار الوطن أونلاين في الحد من الجرائم السيبرانية

انطلاقاً من دورها المهني أولاً، ثم من شعارها (المصدقية قبل السبق)، ثم من قناعتها بالاحترافية والمسؤولية الاخلاقية، قامت "أخبار الوطن" بالرد على الحملات التي تستهدف الجزائر من خلال بث أخبار مضللة وكاذبة تستهدف مؤسسات الدولة، سيما وأن هذه الحملات في الغالب مصدرها قوى خارجية: لوبيات سياسية واقتصادية وثقافية، تكتلات، منظمات، نشطاء، وفي كل الحالات تقف وراءهم حكومات لها خطط لاضعاف الدولة الجزائرية، جراء مواقفها السيادية أو لغناها الطبيعي (ثروات متنوعة)، أو لحسابات جيو-سياسية.

عملت أخبار الوطن من خلال نهج تحريري واضح ودقيق على إبراز المعلومة الصحيحة والدقيقة وإعطائها للمواطن في وقتها مع تنبيهه إلى التضليل الذي تهدف إليه المعلومة المضادة؛ بحيث فتحت المجال للخبراء والأكاديميين والسياسيين والاقتصاديين والدبلوماسيين الجزائريين كل في اختصاصه من إعطاء المعلومات الصحيحة والرسمية، التي تهم الوطن والمواطن في الوقت المناسب، بغرض تحقيق الاكتفاء المعلوماتي للمواطن وتحقيق الأمن الاعلامي للوطن ملتقى حول مخاطر الفضاء السيبراني على الوحدة الوطنية¹.

و في هذا الصدد نسجل الاهتمام الكبير "لشبكة أخبار الوطن" بموضوع الجرائم السيبرانية رغم حداثتها ، و قد تنوعت تغطياتها الإعلامية من أخبار و مقالات إلى فيديوهات ، خاصة في تغطيتها للملتقيات العلمية الخاصة بموضوع الجرائم و التهديدات السيبرانية. و يمكن إجمال مختلف هذه التغطيات في الآتي:

¹ رياض هويلي، المدير التنفيذي مسؤول النشر بشبكة اخبار الوطن، " دور أخبار الوطن في الحروب السيبرانية"، مقال مرسل عن طريق البريد الإلكتروني للأستاذ المشرف ، بتاريخ 2023/05/28، الساعة : 15:30

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

❖ نسجل تغطية لشبكة " أخبار الوطن " عبر قناتها على YouTube بتاريخ 2022/05/11 للملتقى الدولي بعنوان "الجزائر والتهديدات السيبرانية: نحو مستقبل آمن سيبرانيا"، والذي تم تنظيمه بجامعة أحمد درايعية أدرار بمبادرة من البروفيسور "مشاور صيفي"، بمشاركة العديد من الدول تونس ومصر والأردن والعراق وسلطنة عمان وتركيا وذلك عبر مداخلات عن بعد، كما كان للأجهزة الأمنية حضور بارز ومهم، حيث تم من خلال الملتقى إبراز أهم التهديدات السيبرانية وآليات التصدي لها ، و هذا ما يساهم في نشر الثقافة السيبرانية و نشر الوعي الوطني بمخاطر الجرائم السيبرانية¹.

❖ كما سجلت "أخبار الوطن" تغطية إعلامية أخرى عبر قناتها على YouTube بتاريخ 2022/03/06 للملتقى بعنوان "الجريمة السيبرانية محور ملتقى جهوي بمجلس قضاء البليدة" بمشاركة مجموعة من الفاعلين أساتذة جامعيين وقضاة والشرطة والدرك الوطني، حيث جاء محتوى الملتقى حول الجريمة السيبرانية، كما تم الإشارة إلى أنه حان الوقت أن يكون هناك منظومة قانونية لمواكبة ودراسة ومعالجة الجريمة السيبرانية والخروج بتوصيات وإقتراحات لإيجاد حلول أخرى ونصوص أكثر للتصدي للجرائم السيبرانية وتهديداتها².

أما بالنسبة للمقالات فنسجل تغطية إعلامية لمقالين وهما كالآتي:

❖ حيث تناولت الصحفية "ضيرة أوراغي" مقال بتاريخ 2022/12/01 تحت عنوان "ملتقى حول مخاطر الفضاء السيبراني على الوحدة الوطنية" فقد نظمت قيادة الناحية العسكرية السادسة يومي 27 و 28 نوفمبر 2022 على مستوى مقر قيادة الناحية ملتقى جهوي تحسيسي حيث شارك في الملتقى إطارات الناحية، أساتذة جامعيين،

¹علي غنامي، الجزائر والتهديدات السيبرانية : نحو مستقبل آمن سيبرانيا، أخبار الوطن، من الرابط ، <https://www.youtube.com> ، بتاريخ 2023/05/17 ، على الساعة: 09:15 .

²أخبار الوطن، الجريمة السيبرانية محور ملتقى جهوي بمجلس قضاء البليدة، من الرابط <https://www.youtube.com> ، بتاريخ 2023/04/20 ، على الساعة: 10:10 .

الفصل الثالث: دور موقعي الشروق وأخبار الوطن أونلاين في الحد من الجرائم السيبرانية

السلطات المحلية وممثلي الأسرة التربوية لولاية تمنراست .وتضمن الملتقى إلقاء مجموعة من المحاضرات من طرف أساتذة مختصين، تخللته مناقشات ثرية¹.

❖ كما نشر موقع أخبار الوطن أونلاين يوم 2023/04/27 مقال حول ملتقى وطني بعنوان "تحديات وأفاق الدفاع السيبراني في إطار الحروب الهجينة"، حيث نظمت مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لدائرة الاستعمال والتحضير أركان الجيش الوطني الشعبي، الطبعة الرابعة للملتقى الوطني حول الدفاع السيبراني، يومي 26 و 27 أفريل 2023 على مستوى نادي الموقع للجيش بعين النعجة .استهل هذا الملتقى الذي عرف حضور عدد من ضباط وعمداء وإطارات وخبراء من الجيش الوطني الشعبي، بكلمة افتتاحية ألقاها رئيس مصلحة الجغرافيا والكشف عن بعد نيابة عن السيد دائرة الاستعمال والتحضير أركان الجيش الوطني الشعبي، أكد فيها على أهمية هذا الحدث والغاية من تنظيمه، مبرزا أن مهمة تأمين والدفاع عن فضائنا السيبراني هي مسؤولية جماعية تستدعي انخراط جميع الفاعلين المعنيين .يعالج هذا الملتقى على مدار يومين سبل تعزيز الأمن السيبراني الأنظمة المعلومات وخلق فضاء للنقاش وتبادل المعارف بين مختلف الجهات الفاعلة في الفضاء السيبراني، من أجل الإلمام الجيد برهانات وتحديات الدفاع السيبراني .

¹ ضيرة أوراغي، مخاطر الفضاء السيبراني على الوحدة الوطنية، أخبار الوطن، من الرابط <https://www.youtube.com> ، بتاريخ 2023/04/04 ،على الساعة:13:10 .

الخاتمة

الخاتمة :

من خلال بحثنا هذا المنطوي حول " دور الإعلام الرقمي في الحد من الجرائم السيبرانية موقعي الشروق وأخبار الوطن أونلاين" نستطيع القول بأن الإعلام الرقمي شكل إضافة قيمة في مجال الإعلام والاتصال نظراً لتطبيقاته ووسائله وخصائصه المختلفة، كما أن لهذا الأخير دور بارز وفعال جداً ومهم في الوقاية من الجرائم السيبرانية، حيث تعتبر هذه الأخيرة من بين الجرائم المعاصرة التي لها أشكال متنوعة ومتعددة وإحدى أهم المخاوف التي أصبحت تؤرق أفراد المجتمع وتهدد حياتهم الشخصية. ولا تقتصر خطورة هاته الجرائم على الأفراد فقط بل طالت حتى الدول وباتت تهدد أمنها واستقرارها، واعتباراً لطبيعة الجريمة السيبرانية العابرة للحدود وإمكانية ارتكابها من أي مكان في العالم وبما أنها تفتعل إلكترونياً فهنا يبرز دور الإعلام الرقمي في التصدي لهذه الجرائم بأرقى السبل منها الوقائية والتوعية ويتجلى ذلك عبر نشر الوعي بمدى خطورة هاته الجرائم بالإضافة الى نشر سبل وطرق وبرامج الحماية والتأمين ضد الجرائم السيبرانية.

وفي ظل المجهودات التي يبذلها الإعلام الرقمي للحد ومجابهة هذه الجرائم، فقد تضافرت مجهودات الدول العربية والغربية ومن بينهم الجزائر لوضع حد لهذه الجرائم من خلال إبرام اتفاقيات و سن مجموعة من القوانين والتشريعات لردع ومحاربة الجرائم السيبرانية والتي من شأنها أن تقلل من انتشارها بفضل العقوبات الصارمة التي تم سنها .

وانطلاقاً مما سبق يمكن رصد بعض الاقتراحات والتي يمكن حصرها فيما يلي :

- تكثيف الحملات والمحاضرات والمؤتمرات للتوعية والاطلاع على كل ماهو جديد في المجال السيبراني .

- السعي إلى بناء منظومة وعي وطنية ، بمساهمة مؤسسات التنشئة الاجتماعية ، على رأسهم الإعلام بشكل عام و الرقمي بشكل خاص.

- إنشاء مراكز لاستقبال البلاغات المتعلقة بالجرائم السيبرانية، تحت إشراف كوادر متخصصة من أجل الحد و التصدي لمختلف الهجمات و التهديدات و الجرائم السيبرانية في وقتها ، و الوقاية من وقوعها.

- الاستعانة بمجموعة من التقنيين والفنيين ذو خبرة ومهارة عالية في المجال السيبراني .

- إنشاء معاهد ومدارس لتكوين في المجال الأمن السيبراني .

- مناشدة الدول العربية لتكثيف العمل والتنسيق فيما بينهم لوضع واستحداث قوانين متعلقة بتسليم المجرمين وتبادل المساعدة فيما بينهم وتقديم الدعم اللازم لبعضهم البعض فيما يخص الجرائم السيبرانية.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولاً: المصادر

1. الأمم المتحدة، دراسة شاملة عن الجريمة السيبرانية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فبراير 2013 .

ثانياً : الكتب

1. بن ديان العوفي عبد اللطيف ،التوعية الإعلامية الأسس النظرية والإجراءات التطبيقية،النشر العلمي والمطابع،الرياض جامعة الملك سعود،2012 .
2. جمال عبده خالد ،الإعلام البديل على الإنترنت فلسفة جديدة في الإعلام والاتصال،الناشر المكتب العربي للمعارف،ط1،مصر،2016 .
3. جواد الدعيمي غالب كاظم ،الإعلام الجديد اعتمادية متصاعدة وسائل متجددة،دار أمجد للنشر والتوزيع،الأردن،2017 .
4. حسين الحمداني بشرى ،القرصنة الإلكترونية أسلحة الحرب الحديثة،دار أسامة للنشر والتوزيع،ط1،عمان-الأردن،2014 .
5. حيدر خضر إبراهيم ،الميدان مفهومها المعاصر وعلاقتها بالإعلام الكلاسيكي،المركز الإسلامي للدراسات الإستراتيجية،ط1،القبة العباسية المقدسة،2018 .
6. دليو فضيل ،التكنولوجيا الجديدة للإعلام والاتصال(مفاهيم-نظريات-مبادئ-استعمالات-آفاق)،دار الفايز للطباعة والنشر،ط1،قسنطينة(الجزائر)،2010 .
7. الديري عبد العال ،مُجد صادق اسماعيل، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة،المركز القومي للإصدارات القانونية،ط1،القاهرة،2012 .

8. زين العابدين صالح مروة ،الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني،مركز الدراسات العربية للنشر والتوزيع،ط1،مصر،2016.
9. شوقي يعيش تمام ،الجريمة المعلوماتية دراسة تأصيلية مقارنة،مطبعة الرمال، ط1، ط2، الجزائر،2019 .
10. عادل سلمي زهراء ،جريمة الإبتزاز الإلكتروني دراسة مقارنة،شركة دار الأكاديميون للنشر والتوزيع،ط1،الأردن،2020 .
11. عبد القادر مومني نحلة ،الجرائم المعلوماتية،دار الثقافة للنشر والتوزيع ،ط1، ط2، عمان،2010 .
12. عبود حارث،العاني مزهر،الإعلام والهجرة الى العصر الرقمي،دار الحامد للنشر والتوزيع،ط1،الأردن،2015 .
13. فكري أيمن عبد الله، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية،مكتبة القانون والإقتصاد،ط1،الرياض،2014 .
14. ماهر عودة و آخرون،الإعلام الرقمي الجديد،دار الإعصار العلمي للنشر والتوزيع،ط1،عمان(الأردن)،2015 .
15. محمد عبيد الكعبي،الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة،دار النهضة العربية،القاهرة،2009 .
16. محمد نصر محمد،الوسيط في الجرائم المعلوماتية،مركز الدراسات العربية للنشر والتوزيع،ط1،مصر،2015.
17. محمود الدسوقي محمد كمال ،الحماية الجنائية لسرية المعلومات الإلكترونية دراسة مقارنة،دار الفكر والقانون للنشر والتوزيع،ط1،المنصورة،2021 .

18. مروت عبد الكريم، الإرهاب الإلكتروني وآليات مكافحته، دار علي بن زيد للطباعة والنشر، ط1، بسكرة (الجزائر)، 2020 .
 19. مروت عبد الكريم، الجريمة السيبرانية في الاتفاقيات والصكوك الدولية، مؤسسة نقطة بوك للنشر والتوزيع، ط1، 2021 .
 20. مروت عبد الكريم، تشريعات الجرائم الإلكترونية في الجزائر والدول العربية، دار علي بن زيد للطباعة والنشر، ط1، الجزائر، 2020 .
 21. نصار غادة، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، ط1، القاهرة، 2017 .
 22. هرزاني نوري ياسين، الإعلام والجريمة، مطبعة جامعة صلاح الدين، أربيل، 2005 .
- ثانيا: الدوريات**
23. بن فهد بن محمد بن داود عبد العزيز، الجرائم السيبرانية: دراسة تأصيلية مقارنة، مجلة الإجتهد للدراسات القانونية والإقتصادية، المجلد 09، العدد 03، 2020 .
 24. جبريل رشاد مرعي اسراء، "الجرائم الإلكترونية (الأهداف- الأسباب- طرق الجريمة ومعالجتها)"، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير 2018 .
 25. حسام منصور، الاعلام الرقمي (مفهومه- وسائله- نظرياته)، مجلة بحوث ودراسات في الميديا الجديدة، المجلد 03، العدد 02، 2022 .
 26. حميدة راضية، "الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي نحو تفعيل دور الأمن السيبراني بالمعلوماتي"، مجلة الإعلام والمجتمع، المجلد 05، العدد 02، ديسمبر 2021 .
 27. رضا مهدي، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة ايليزي للبحوث والدراسات، المجلد 06، العدد 02، 2021 .

28. ساعد بوقرص، "الأمن السيبراني": مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة"، مجلة الأبحاث في الحماية الاجتماعية، العدد 01، جامعة العلوم والتكنولوجيا هواري بومدين، 2022، ص 65.
29. عبد الحميد عائشة ، نوال ملوك ، "الإجرام السيبراني وأثره على تهديد الأمن الثقافي في الجزائر"، مجلة المفكر للدراسات القانونية والسياسية، الجزائر، المجلد 3 ، العدد 3، سبتمبر 2020 .
30. العتيبي زياد بن محمد عادي ، "الجرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهوميها من حيث: (أشكالها-خصائصها-أركانها والدوافع من ارتكابها)"، المجلة الأكاديمية العالمية للدراسات القانونية، المجلد 03، العدد 01، 2020 .
31. القحطاني انتصار محمد ، "الإعلام الرقمي"، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد الثامن، 2019 .
32. مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، نزوى سلطنة عمان، 2016 .
33. محمد المايل عبد السلام ، الشرجبي عادل محمد ، الجريمة الإلكترونية: المفهوم-الأسباب-سبل المكافحة مع التعرض لحالة ليبيا، آفاق للبحوث والدراسات سداسية دولية محكمة، العدد 4، المركز الجامعي إيليزي، جوان 2019 .
34. مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دراسة شاملة عن الجريمة السيبرانية، مسودة شباط، نيويورك، 2013 .

ثالثا: المذكرات والرسائل الجامعية

35. حبيب عبد القادر عامر مُجَد ، **المجرم المعلوماتي**، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2019/2018 .
36. بوعمرة مُجَد ، **بنينال سيد علي ، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري**، مذكرة تخرج شهادة الماستر في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، 2020/2019 .
37. حاجي مريم ، **إستخدام الشباب الجزائري لقناة الشروق والاشباعات المحققة منها دراسة ميدانية على عينة من شباب مدينة أم البواقي**، مذكرة تخرج لنيل شهادة الماستر في علوم الإعلام والاتصال تخصص صحافة وإعلام إلكتروني، جامعة العربي بن مهيدي- أم البواقي، 2017/2016 .

رابعا: مقالات مرسلّة عبر الإيميل

38. رياض هويلي، المدير التنفيذي مسؤول النشر بشبكة اخبار الوطن، "نبذة تاريخية عن شبكة أخبار الوطن"، مقال مرسل عن طريق البريد الإلكتروني للأستاذ المشرف ، بتاريخ 2023/05/28، الساعة : 15:30
39. رياض هويلي، المدير التنفيذي مسؤول النشر بشبكة اخبار الوطن، " أهداف شبكة أخبار الوطن "، مقال مرسل عن طريق البريد الإلكتروني للأستاذ المشرف ، بتاريخ 2023/05/28، الساعة : 15:30
40. رياض هويلي، المدير التنفيذي مسؤول النشر بشبكة اخبار الوطن، " دور أخبار الوطن في الحروب السيبرانية"، مقال مرسل عن طريق البريد الإلكتروني للأستاذ المشرف ، بتاريخ 2023/05/28، الساعة : 15:30.

خامساً : الأنترنت:

41. رنيا محمود، تعريف الإعلام الرقمي وأنواعه وأهميته، من الموقع: www.Almrsal.com، بتاريخ: 2023/04/28، على الساعة: 03:34 .
42. نسرين حسونة، الإعلام الجديد المفهوم والوسائل والخصائص والوظائف، من الموقع: www.alukah.net ، بتاريخ: 2023/03/31، على الساعة: 12:22 .
43. الإعلام الرقمي مفهومه وأهميته وأنواعه، من الموقع: www.annajah.net ، بتاريخ: 2023/3/30، على الساعة: 9:15 .
44. أنواع الجرائم الإلكترونية، من الموقع: www.cyberone.com ، بتاريخ: 2023/4/01، على الساعة: 13:41 .
45. إيرانيون ينقلون تجربتهم إلى الشرطة الجزائرية، من الموقع: Echourouk online.com ، بتاريخ: 2023/03/23، على الساعة: 11:30 .
46. إنشاء هيئة وطنية للوقاية من الجرائم الإلكترونية، Echourouk online.com بتاريخ: 2023/03/24، على الساعة: 09:13 .
47. الإرهاب الإلكتروني والهجمات السيبرانية تهدد الأمن والاستقرار، echourouk online.com، بتاريخ: 2023/5/15، على الساعة: 15:45 .
48. وزارة الدفاع تحبط 12 مليون محاولة الإختراق لمواقعها، Echourouk online.com، بتاريخ: 2023/05/09، على الساعة: 9:50 .
49. الدفاع السيبراني مكون أساسي للأمن والدفاع الوطني، من الموقع Echourouk online.com ، بتاريخ: 2023/05/09 ، على الساعة: 11:30 .
50. الجيش يدخل حرب الفضاء الإلكتروني ومكافحة الجوسسة ، من موقع: echourouk online، بتاريخ: 2023/4/01، على الساعة: 05:30 .

51. أحسن حراش، جوسسة إلكترونية تستهدف الوزراء وإطارات الدولة، من موقع: echourouk online.com، بتاريخ: 2023/04/03، على الساعة: 04:16.
52. نورة باشوش، اللواء نوبة: الجريمة الإلكترونية والهجمات السيبرانية تهدد الأمن العمومي، من موقع: echourouk online.com، بتاريخ: 2023/04/12، على الساعة: 10:01.
53. محمد مسلم، لوح يدعو إلى إتفاقية دولية لمحاربة الجريمة الإلكترونية، من موقع echourouk online.com، بتاريخ: 2023/04/13، على الساعة: 07:20.
54. جهود لمواجهة الجرائم الإلكترونية، من موقع: echourouk online.com، بتاريخ: 2023/04/15، على الساعة: 06:00.
55. 1514 متورط كورونا ترفع التحدي، من موقع: echourouk online.com، بتاريخ: 2023/04/17، على الساعة: 20:14.
56. عمار يزلي، رهان آني لأمننا السيبراني، من موقع: echourouk online.com، بتاريخ: 2023/04/18، على الساعة: 21:23.
57. أحبطنا كافة الهجمات السيبرانية ضد الجزائر، من موقع: Echourouk online.com، بتاريخ: 2023/04/02، على الساعة: 23:02.
58. خالد.م، بلحيمر: ضمان سيادة سيبرانية أولوية لتحسين الشباب العرب، Echourouk online.com، 2023/04/21، 13:13.
59. الحرب السيبرانية : الإستعداد لقيادة المعارك العسكرية في الميدان الخامس، من الموقع Echourouk online.com، بتاريخ: 2023/04/22، على الساعة: 14:14.
60. محمد مسلم، محاربة الجرائم الرقمية يجب أن تتحول إلى ثقافة وتعليم، echourouk online.com، 2023/04/22، 9:50.
61. الشرطة تعلن عن مخطط جديد لمواجهة الجريمة الإلكترونية، echourouk الموقع: online.com، بتاريخ: 2023/04/24، على الساعة: 08:10.

62. إلهام بوثلجة، استحداث قطب جزائي متخصص سيكبح الجرائم السيبرانية، من موقع echourouk online، 2023/04/25، 03:09.
63. نورة باشوش، الإجرام الإلكتروني أرقام مرعبة، echourouk online.com، 2023/04/26، 15:15.
64. منير ركاب، الدفاع السيبراني طرف فعال في العمليات العسكرية، من موقع echourouk online.com، 2023/04/27، 12:30.
65. الجزائر تقود بنجاح المسار الأمني لمكافحة الجرائم السيبرانية، من الموقع: Echourouk online.com، بتاريخ: 2023/5/9، على الساعة: 9:50.
66. بلقاسم حوام، أول مركز للتكوين في الأمن السيبراني في الجزائر، من الموقع: Echourouk online.com، بتاريخ: 2023/04/28، على الساعة: 01:12.
67. أمين شاوش، مختصون: هكذا يتم مواجهة الإرهاب السيبراني وتحقيق السيادة الرقمية في الجزائر، من الموقع: echourouk online.com، بتاريخ: 2023/04/29، على الساعة: 11:45.
68. اتصالات الجزائر تضم مكتشف ثغرة آبل إلى مركزها للدفاع السيبراني، Echourouk online.com، بتاريخ: 2023/04/29، على الساعة: 17:06.
69. قضية بيغاسوس: يونيسكو تعزل موظفة مغربية بعد تجنيديها من قبل مخابرات الرباط، من الموقع: Echourouk online.com، بتاريخ: 2023/04/30، على الساعة: 09:09.
70. ع.س، قبة حديدية سيبرانية مشتركة بين المخزن والكيان الصهيوني، من الموقع: echourouk online.com، بتاريخ: 2023/05/01، على الساعة: 22:30.
71. المنشآت الطاقوية في الجزائر مؤمنة ضد الهجمات السيبرانية، من الموقع: Echourouk online.com، بتاريخ: 2023 /05/ 02، على الساعة: 18:18.

72. الدرك الوطني يكشف حصيلة الجرائم السيبرانية بالجزائر عامي 2022 و 2023، من الموقع: Echourouk online.com بتاريخ: 2023/05/05، على الساعة: 19:00
73. نورة باشوش، الجريمة السيبرانية أسلحة الجناة الجديدة لضرب الأشخاص والإقتصاد، من الموقع: echouriuk online.com، بتاريخ: 2023/05/06، على الساعة: 12:08.
74. عبد الحميد عثمان، بيغاسوس كل تفاصيل مملكة التجسس بالوثائق، من الموقع echourouk online.com ، 2023/05/07 ، 07:04 .
75. الطالبتان بتصرف، من الموقع: <https://akhbarelwatane.dz/apropos/> ، بتاريخ: 2023/04/27 ، على الساعة: 22:10 .
76. علي غنامي، تغطية: الملتقى الدولي "الجزائر والتهديدات السيبرانية : نحو مستقبل آمن سيبرانيا"، جامعة أدرار يومي 12/11 ماي 2022، أخبار الوطن، من الرابط ، <https://www.youtube.com> ، بتاريخ 2023/05/11 ، على الساعة: 09:15 .
77. أخبار الوطن، "الجريمة السيبرانية محور ملتقى جهوي بمجلس قضاء البلدية"، من الرابط <https://www.youtube.com> ، بتاريخ 2023/04/20 ، على الساعة: 10:10.
78. ضيرة أوراغي، مخاطر الفضاء السيبراني على الوحدة الوطنية، أخبار الوطن، من الرابط <https://www.youtube.com> ، بتاريخ 2023/04/04 ، على الساعة: 13:10 .
79. تسنيم الكفاوي، "تعريف الإعلام الرقمي"، من موقع www.mawdoo3.com ، بتاريخ 29 ماي 2023 علي الساعة 18:20.

الملاحق



الشروق

العالم

للدفاع ضد الهجمات الإلكترونية من
قراصنة "الأعداء"

قبة حديدية سيبرانية مشاركة بين المخزن والكيان الصهيوني

ع.س

0 | 1975 | 2022/12/18



© أرشيف



الشروق

الجزائر

بمنطقة وسط البلاد خلال سنة 2020:

1514 متورط.. كورونا ترفع الجرائم السيبرانية!

الشروق أونلاين

0

571

2021/01/13



© أرشيف



الشروق

الجزائر

المنشآت الطاقوية في الجزائر "مؤمنة" ضد الهجمات السيبرانية

الشروق أونلاين

0



370



2023/01/17



© أرشيف

بعض مقالات موقع "الشروق أونلاين" حول الجرائم السيبرانية



الشروق

الجزائر

رئيس دائرة الاستعمال والتحضير لأركان
الجيش:

نعمل لتحسين المعارف في مجال مكافحة التهديدات السيبرانية

الشروق أونلاين

0



2494



2017/05/15





منوعات

جديد مركز المستقبل للأبحاث والدراسات
المتقدمة

الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس

الشروق

4

1931

2021/07/02





الجزائر

تسجيل 12 ألف حالة خلال العام الماضي
وشهر جانفي 2013

الجريمة السيبرانية.. أسلحة الجنّة الجديدة لضرب الأشخاص والاقتصاد

نؤارة باشوش



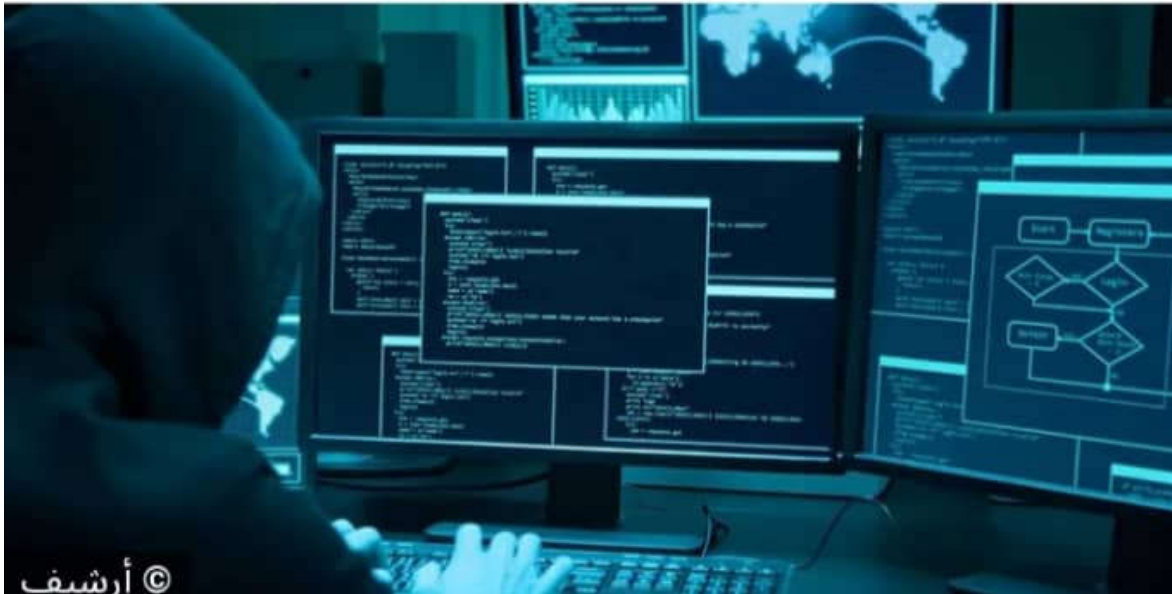
0



522



2023/02/15





الشروق

الجزائر

الفريق شنقرية: أحبطنا كافة الهجمات السيبرانية ضد الجزائر

الشروق أونلاين

2



1922



2021/05/23





الشروق

الجزائر

تقرير دولي حول الأمن الرقمي في 2022
يكشف:

إحباط قرابة 30 مليون تهديد سيبراني ضد الجزائر

حسان حويشة



0

1083

2023/05/12



© أرشيف



الشروق

الجزائر

قائد مدرسة القيادة والأركان، اللواء محمد
عمر، لـ "الشروق":

الدفاع السيبراني طرف فعال في العمليات العسكرية

منير ركاب



0



1425



2022/01/17



© أرشيف



النشروفي

الجزائر

مختصون: هكذا يتم مواجهة الإرهاب السيبراني وتحقيق السيادة الرقمية في الجزائر

أمين شاوش

0



1808



2022/05/30





أخبار الجزائر

ملتقى وطني تحت عنوان "تحديات وأفاق الدفاع السيبراني في إطار الحروب الهجينة"

التحرير • 27 أبريل، 2023



نظمت مصلحة الدفاع السيبراني
ومراقبة أمن الأنظمة لدائرة





أخبار الجزائر

ملتقى حول مخاطر الفضاء السيبراني على الوحدة الوطنية

نضيرة أوراغي • 1 ديسمبر، 2022



نظمت قيادة الناحية العسكرية
السادسة يومي 27 و28 نوفمبر
2022، على مستوى مقر قيادة
الناحية ملتقى جهوي تحسيسي



فهرس المحتويات

فهرس المحتويات

7	مقدمة:
31	الفصل الأول مدخل مفاهيمي حول الإعلام الرقمي والجرائم السيبرانية
14	المبحث الأول: مفهوم الإعلام الرقمي
14	المطلب الأول: تعريف الإعلام الرقمي وخصائصه
23	المطلب الثاني : أنواع ووسائل الإعلام الرقمي

المطلب الثالث : وظائف وأهمية الإعلام الرقمي	33
المبحث الثاني : مفهوم الجرائم السيبرانية	36
المطلب الأول : تعريف الجرائم السيبرانية وخصائصها	36
المطلب الثاني : أسباب الجرائم السيبرانية	42
المطلب الثالث : طرق وأشكال الجرائم السيبرانية	46
المبحث الثالث : المجرم السيبراني	58
المطلب الأول : تعريف المجرم السيبراني وسماته	58
المطلب الثاني : فئات المجرم السيبراني	62
المطلب الثالث : أدوات وأساليب المجرم السيبراني	69
الفصل الثاني: أهمية الإعلام الرقمي في الحد من الجرائم السيبرانية	71
المبحث الأول : دور التشريعات في الحد من الجرائم السيبرانية	72
المطلب الأول : تشريعات الجرائم السيبرانية في الجزائر	72
المطلب الثاني : تشريعات الجرائم السيبرانية في بعض الدول العربية والغربية	79
المطلب الثالث : الإتفاقيات الإقليمية في الجريمة السيبرانية	91
المبحث الثاني : أهمية الإعلام الرقمي في الحد من الجرائم السيبرانية	98
المطلب الأول : الوعي بالجريمة السيبرانية	98
المطلب الثاني : حماية خصوصية مستخدم الشبكات الاجتماعية	101
المطلب الثالث : الوقاية والتأمين بالبرامج والوسائل التقنية	104
المبحث الثالث: معوقات الإعلام الرقمي في الحد من الجرائم السيبرانية	105
المطلب الأول :مخاطر التطور التكنولوجي	105

المطلب الثاني : ضعف التنسيق والتعاون الدولي لمكافحة الجريمة السيبرانية	106
المطلب الثالث : الاثبات بالدليل الرقمي	110
الفصل الثالث : دور موقع الشروق و أخبار الوطن أونلاين في الحد من الجرائم السيبرانية	111
المبحث الأول : دور موقع الشروق أونلاين في الحد من الجرائم السيبرانية	112
المطلب الأول : نبذة تعريفية لموقع الشروق أونلاين	112
المطلب الثاني : أهداف موقع الشروق أونلاين	113
المطلب الثالث : دور موقع الشروق أونلاين في الحد من الجرائم السيبرانية	114
المبحث الثاني : دور موقع أخبار الوطن أونلاين في الحد من الجرائم السيبرانية	130
المطلب الأول : نبذة تعريفية لموقع أخبار الوطن أونلاين	130
المطلب الثاني : أهداف موقع أخبارالوطن أونلاين	132
المطلب الثالث : دور موقع أخبار الوطن أونلاين في الحد من الجرائم السيبرانية	134
الخاتمة	137
قائمة المصادر والمراجع	140

الملخص :

تهدف هذه الدراسة إلى التعرف على الإعلام الرقمي والإضافات المتنوعة والمميزة التي أحدثتها في مجال الإعلام والاتصال، وكذا التعرف على دوره في مكافحة الجرائم السيبرانية، وأهمية التشريعات والقوانين التي سنتها الجزائر وبعض الدول العربية والغربية، بالإضافة إلى الإتفاقيات الإقليمية المبرمة حول الجريمة السيبرانية للحد منها .

وقد اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، لإبراز دور الإعلام الرقمي في التصدي ومواجهة الجرائم السيبرانية من خلال مختلف التطبيقات والبرامج المعروفة والمستخدمه عالمياً.

وقد بينت الدراسة أهمية المؤسسات الرقمية ومن بينها مؤسستي الشروق وأخبار الوطن أونلاين في مكافحة الجرائم السيبرانية عبر بناء الوعي لدى الأفراد بمخاطر هذه الجرائم وذلك من خلال نشر الحملات والإعلانات والمحاضرات التوعوية، وتقديم بعض التدابير والإجراءات الاحترازية للوقاية والحماية ضد الجرائم السيبرانية .

الكلمات المفتاحية: الرقمنة، الإعلام الرقمي، الجريمة، الجرائم السيبرانية.

Abstract :

This study aims to identify the digital media and the various and distinctive additions that it has been made in the field of media and communication, as well as its role in combating cybercrime, the importance of legislation and laws enacted by Algeria and some Arab and Western countries, in addition to the regional agreements concluded on cybercrime to reduce it.

This study relied on the analytical descriptive approach to highlight the role of digital media in addressing and combating cybercrime through various applications and known programs and used globally.

The study showed the importance of digital institutions, including Al-Shorouk and Akhbar Al-Watan Online websites, in combating cybercrime by building awareness among individuals of the dangers of these crimes, by publishing campaigns, advertisements and educational lectures, and providing some precautionary measures and procedures for prevention and protection against cybercrime.

Key words: Digitization/ Digital media/ The crime/ Cyber crime.