جرائم الأنترنت وتحديات الأمن السيبراني: دراسة في متغيرات الجريمة ومقارباتها العلاجية.

Internet crimes and cyber security challenges : a study of crime variables and their therapeutic approaches

حرزالله محمد لخضر
كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة(الجزائر)
mohamed.harz@yahoo.fr

تاريخ الاستلام: 2021/07/25 تاريخ القبول: 29/05/ 2023 تاريخ النشر: 15/06/ 2023

الملخص:

إن التحديات الأمنية التي فرضتها التكنولوجيات الحديثة والوسائط الاتصالية الرقمية، وما أنتجته من مظاهر جديدة للجريمة والانحراف المرتبط بالأنترنت وبسوء استخدام تكنولوجيا المعلومات، تدفع نحو ضرورة البحث عن مقاربات جديدة تناسب التعامل مع هذا النموذج الجديد من المجتمع الشبكي المفتوح.

وعليه تهدف هذه الدراسة للبحث في خصائص الجرائم المتصلة بالأنترنت واستراتيجية الوقاية منها بطرح آليات وتصورات عملية تهدف إلى تحقيق الأمن السيبراني وصيانة الأمن الفكري والمجتمعي.

الكلمات المفتاحية: جرائم الأنترنت، تكنولوجيا المعلوماتية، الأمن السيبراني، البيئة الرقمية، الأمن الإعلامي والفكري.

Abstract:

The security challenges posed by modern technologies and digital media, and its new manifestations of crime and delinquency associated with the misuse of information technology, prompt the search for new approaches that are appropriate to deal with this new paradigm of open-network society.

Therefore this study aims to search in the characteristics of crimes related to the Internet, and its prevention strategy, by proposing practical mechanisms and scenarios aimed at to achieve cybersecurity and maintaining intellectual and societal security.

Keywords: Internet crimes, information technology, Cybersecurity, Digital environment, Media and intellectual security.

المقدمة:

لقد أفرز التطور التقني والرقمي الحديث سلوكات ومظاهر جديدة في مختلف مناحي الحياة، فظهرت على إثر ذلك مصطلحات وصناعات ومكتسبات مستحدثة ومفيدة للإنسانية؛

كالتجارة والإدارة الإلكترونية، والكتب الرقمية والتعليم الإلكتروني والجامعة الافتراضية، والاقتصاد الرقمي والتحاضر المرئي عن بعد، والسلع والعملات الإلكترونية..الخ. كما كان لهذا التقدم التكنولوجي تبعات على المستوى الأمني، حيث برزت أشكال جديدة لجرائم مرتبطة بسوء استخدام تكنولوجيات الإعلام والاتصال والشبكة المعلوماتية، من بينها: جرائم التجارة الإلكترونية، شبكات التجنيد عبر الأنترنت، الإغراء والفساد الأخلاقي، الانتحال والقرصنة الإلكترونية، الاعتداء على خصوصيات الأشخاص، جرائم الإرهاب الإلكتروني، تخريب الأنظمة المعلوماتية والحاسوبية (الفيروسات)، اختراق المواقع الرسمية، والتغرير بالأحداث وتلقينهم السلوك الإجرامي؛ كصناعة المتفجرات والمخدرات، وتعليم أساليب التحايل المختلفة...الخ.

وقد مثلت مظاهر الاندماج الكوني والتثاقف والانكشاف الإعلامي بيئة خصبة لتنامي ظاهرة الغزو السيبراني Cyber invasion ، فأضحت الفضاءات الداخلية للمجتمعات منفتحة بجميع تفاعلاتها على العالم الخارجي، مما أفضى إلى عدم القدرة على التحكم في سعة وحجم التدفقات المعرفية وقوتها التأثيرية على عقول وسلوك المتلقين، بسبب الاتصال الشبكي المعقد بين الأشخاص، فأصبحت الأحداث الواقعة في أقاصي الأرض تلقي بظلالها وآثارها على الجانب الآخر منها في غضون دقائق معدودة، وظهرت التنظيمات والترابطات الشبكية العابرة للحدود، التي شكلت تحديا كبيرا على المؤسسات الأمنية والتعليمية والاجتماعية، ووضعت الأمن المجتمعي والفكري الإلكتروني في قلب العاصفة.

وعليه أصبح من الضروري البحث عن مقاربات أمنية أكثر فاعلية في درء آثار التوظيف السيئ للأنترنت وتحجيم تبعاتها، مقارباتٍ تكون أكثر اقترابا من مسرح الجرائم الإلكترونية، مع ضرورة إشراك المواطن في العمل التوعوي والفعاليات المدنية، وتنمية حسه وثقافته الأمنية وإشعاره بمسؤوليته المدنية في التأسيس لمفهوم **"الأمن الجماعي التشاركي Participatory collective security "**، على اعتبار أن الأمن هو كلٌّ لا يتجزأ ويتضامن في تحقيقه جميع أفراد المجتمع.

1- الإشكالية والتساؤلات الفرعية:

لمعالجة هذا الموضوع فإننا نطرح الإشكالية التالية:

ما هي الخصوصيات المميزة للفعل الإجرامي المرتكب عبر الأنترنت؟ وما مقاربات إرساء الأمن السيبراني؟

- ما المقصود بجرائم الأنترنت ؟ وما هي الخصوصيات المميزة لها؟
- ما هي أبرز إشكالات تكييف ومتابعة جرائم الأنترنت ؟
- كيف تهدد جرائم الأنترنت الكيان المجتمعي والأمن الفكري النظام المعلوماتي للأفراد والمؤسسات؟
- ما هي أهم المقاربات الوقائية والعلاجية لإرساء الأمن السيبراني ؟

2- فرضية الدراسة:

كلما تم ترسيخ الوعي الرقمي عبر المؤسسات التربوية وتفعيل الإرشاد الأسري وتبني مقاربة الشرطة المجتمعية، كلما ساهم ذلك في إرساء مقومات الأمن السيبراني وتحجيم تبعات جرائم الأنترنت والتحكم في آثارها.

3- أهمية الدراسة:

تعالج هذه الدراسة موضوعا حساسا فرض نفسه على أدبيات العلوم الإنسانية المعاصرة، فالتعامل مع التكنولوجيات الحديثة وتوظيفاتها على مستوى الحياة العامة والخاصة بات حتمية لا مفر منها، وأصبح يشكل معلما من معالم مجتمع المعلومات الرقمي المعاصر، غير أنَّ لهذا التحول تداعيات سلبية قد تعتبر "ضريبة لازمة" لطغيان التوجه الرقمي والتكنولوجي وتحكمه في مسلكيات المجتمعات الرقمية، أين يكون الإنسان مجبرا على مواجهة أنماط جديدة من الجرائم والتهديدات الخطرة والفتاكة، فتصبح الحياة الشخصية للأفراد والأنظمة المعلوماتية للمؤسسات في مرمى الاستهداف، ما يجعل من مسألة "الأمن السيبراني" تحديا يشغل اهتمام الدول والمنظمات والأفراد.

4- أهداف الدراسة:

1- استجلاء خطورة جرائم الأنترنت وطبيعتها التهديدية لاسيما على فئة الأحداث والشباب.

2- ترسيخ الوعي بأهمية إدراك الأساليب الحديثة للجريمة الإلكترونية وتبعاتها على الفكر والسلوك والمجتمع.

3- عرض مقاربات وقائية وعلاجية لتحقيق الأمن السيبراني كمقدمة شرطية لإرساء دعائم الأمن الفكري والمجتمعي.

5- منهج الدراسة:

بما أن الدراسة تنتمي إلى حقل العلوم الاجتماعية والإنسانية، فقد تم استخدام المنهج الوصفي في معالجة متغيرات الدراسة، من خلال جمع المادة العلمية المستهدفة، وترتيبها في سياق منهجي متكامل، قصد تحليل العلاقة بين متغيرات الدراسة، وصولا إلى نتائج علمية ذات بعد عملي.

6- تقسيم الدراسة:

للإجابة على إشكالية الدراسة فقد اعتمد الباحث على الخطة المنهجية التالية:

1- ملامح ومتغيرات البيئة الرقمية الحديثة.
2- المهددات الأمنية الناجمة عن تكنولوجيا المعلوماتية.
3- الأنترنت والجريمة الإلكترونية: التحول في طبيعة التهديدات.
4- خصائص الجرائم المتصلة بالأنترنت.
5- التدابير التقنية والفنية لتحقيق الأمن السيبراني.
6- تدابير إرساء الأمن الفكري والإعلامي للحد من جرائم الأنترنت.

1- ملامح ومتغيرات البيئة الرقمية الحديثة.

لقد حقق الإنسان على مدى العصور الماضية تطورا هائلا في مجال تقنية المعلومات والاتصالات،" خاصة مع وجود شبكة الأنترنت، التي زادت من حجم المعلومات المتاحة

وتعدد أشكالها، فشبكة الأنترنت تعد البيئة المثالية لاحتضان وإتاحة الدخول إلى المعلومات الرقمية، التي تقوم بتوفير أوعية ومصادر المعلومات على وسائط رقمية مخزنة في قواعد المعلومات، بحيث تتيح للمستفيدين الإطلاع والحصول على هذه الأوعية من خلال نهايات طرفية مرتبطة بقواعد المعلومات، وبهذه الطريقة تمكن الباحثون من الحصول على أوعية ومصادر المعلومات في أي وقت ومن أي مكان تتوفر فيه نهايات طرفية مرتبطة بتلك القواعد المعلوماتية، ومما سبق يمكن اعتبار أن البيئة الرقمية Digital environment الحديثة عبارة عن:" مزيج من الأنشطة والخدمات التي تكتسي طابعا رقميا تبعا للوسائل والإمكانات المتاحة، وتتفاعل فيها العديد من التقنيات التي تساهم في تغيير ملامح الخدمات المقدمة، فهي ترتكز على شبكات المعلومات وعلى رأسها شبكة الأنترنت وكذا مختلف مخرجات تكنولوجيا المعلومات من أدوات وتقنيات تجهيزية وبرمجية."(لحواطي،2014، ص49).

إن المعرفة الإنسانية في نمو مطرد ومتسارع، وتطالعنا المجلات العلمية ووسائل الإعلام يوميا بأبحاث وفتوحات معرفية جديدة،" وما تم تحقيقه فقط في العقود القليلة الماضية على سبيل المثال، يتجاوز بكثير المعرفة التي تراكمت خلال آلاف السنين قبل ذلك، فكمية المعلومات في كل نشاط بشري معين كبيرة جدًا، لدرجة أنه بدون فهم وإدارة هذه المعلومات بشكل صحيح، فإننا نفقد مسار ما نعرفه وإلى أين نتجه. ونظرًا لأن المعلومات تنمو بشكل كبير، فقد برزت الحاجة إلى موضوع جديد كامل اسمه"تكنولوجيا المعلومات"، يتعامل مع مثل هذا الكم الهائل من المعلومات." (Damjanovski, 2005, P 377)

فتكنولوجيا المعلومات تهدف أساسا إلى تنظيم واستغلال المعلومات المتدفقة بشكل لحظِي، والتي تتجاوز قدرة الإنسان على التحكم فيها، ومن هذا المنطلق فهي تعرف بأنها عبارة عن:" مجموعة من الأجهزة والخدمات التي تقوم بالتقاط البيانات والمعلومات وإرسالها وعرضها بشكل إلكتروني. وهي تشمل الحواسيب الشخصية (PC) والأجهزة الملحقة وشبكات الاتصالات عريضة النطاق وأجهزة ومراكز البيانات." (الإتحاد الدولي للإتصالات،2011، ص02) ويمكن القول أن تكنولوجيا المعلومات تتضمن ثلاثة أبعاد رئيسية وهي:

1- منظومات حاسوبية Computer systems
2- شبكات اتصالات Communication networks
3- المعرفة بالتكنولوجيا Knowledge of technology (حواس وحبوشي، 2017، ص 106.)

ومن هذا المنطلق يؤكد الكثير من الخبراء" أن التحول الرقمي في عصر الاتصال الفائق يعمل كمحرك رئيسي للتغيير في كل من بيئة الأعمال والبيئات الاجتماعية." (Srdjan Krčo and Others, 2019, P 84) وكان من نتاج هذا التغيير حدوث تحولات كثيرة على عدة مستويات ومجالات علمية وعملية وممارسات سلوكية، ويجمع الكثير من الباحثين" أن النصف الثاني من القرن العشرين شهد ظهور **ثورة الاتصال الخامسة** والذي شهد ابتكارات فاقت كل الابتكارات السابقة، وذلك بموجب الاندماج التاريخي بين ظاهرتي تفجير المعلومات والمعرفة وثورة الاتصال، والتي نتج عنها التكنولوجيات الاتصالية الحديثة

التي تتمثل أساسا في الأجهزة الحاسبة وملحقاتها والبرمجيات المتطورة، التي أدت إلى تحكمٍ أكثر في المعلومات من حيث التجميع والمعالجة والتخزين. وبالفعل فقد أفرزت تكنولوجيا الاتصال الحديثة ثورة حقيقية في نقل المعلومات وتخزينها، كما مكنت من بروز وظهور خدمات جديدة لنقل المعلومات وتداولها زادت من فعالية هذه التكنولوجيا، وانتشر بين المثقفين الكتاب الإلكتروني محل التقليدي، أما في مجالي التجارة والاقتصاد فقد برزت مصطلحات تخصهم نذكر منها: التجارة الإلكترونية والاقتصاد اللامادي."(بولعويدات، 2007، ص82).

ومن التكنولوجيات الحديثة للاتصال **"التّطبيقات الحديثة"** التي انتشرت بشكل واسع سواء على الهاتف المنقول أو الحاسب الآلي، إذ أنّها تشهد تزايدا وإقبالا كبيرا بسبب تطوّر التّقنية، وازدياد أساليب التّواصل: كالفايسبوك، الواتساب، الإيميل، الأنستغرام، الفايبر، تويتر....الخ). ناهيك عن الآلاف من البرامج الإلكترونية التي أصبحت تتحكم في أساليب إدارة الحياة العصرية، ويُلاحظ أنّ تخصُّصات البرمجة أصبحت مَرغوبة وبكثرة بسبب تزايد الأفكار والحاجة لتطبيقها بصورة رقميّة ومبرمجة.

إلا أنه في خضم هذا التحول الرقمي الكبير في الحياة العصرية ستزداد قيمة المعرفة، وتتضاعف البيانات وتداول المعلومات بشكل لم يسبق له مثيل،" فالهواتف الذكية والتطبيقات المرتبطة بها تولد كميات هائلة من البيانات، وقد نما عدد الهواتف الذكية بنسبة 50٪ تقريبًا في السنوات الثلاث الماضية. ومع ذلك، فإن الأجهزة المتصلة الأخرى تنمو بمعدل أعلى، وتوجد أجهزة استشعار متصلة في كل شيء من الساعات والملابس والسلع الرياضية والسيارات والأجهزة. نحن نعيش في أوقات شديدة الترابط، وسيستمر هذا المستوى من النمو بمعدل متسارع في المستقبل المنظور." (Steven M. Stone,2019, P 15)

ولا بد من الإقرار هنا بأن" بقاء **الهوة التكنولوجية Technological gap** بين الدول المتقدمة والدول النامية سيُبقي الهيمنة الإعلامية للدول الصناعية في مجالات الإعلام والمعلومات، وسوف تتضرر بذلك الدول النامية، حيث تصبح غير قادرة على حفظ استقلالها السياسي وأمنها الثقافي بسبب التفوق التكنولوجي للغرب، بل ستصبح معرضة للاختراقات المستمرة والخطيرة لمعتقداتٍ وأفكارٍ وقيمٍ تتعارض مع أنظمتها السياسية والاجتماعية والثقافية."(زرزايحي، 2010، ص 254) كما يشير الكثير من الباحثين إلى الدور الخطير الذي تلعبه **العولمة الإعلامية Media globalization** في إضعاف القيم المحلية وضمورها واستلاب الذات وخطف ولاء وانتماء المواطنين لأوطانهم، وإغرائهم بمظاهر الحضارة الغيرية، وهذا ما سماه المفكر محمد عابد الجابري ب" **الاختراق الثقافي Cultural hack**" حيث يؤكد في هذا السياق:" أن العولمة تعني نفي الآخر، وإحلال الاختراق الثقافي والهيمنة، وفرض نمط واحد للاستهلاك والسلوك."(سنان، 2017، ص 36)

وتبعا لكل ما سبق تبيانه، طرأ تغيير واسع في مفهوم الأمن وأخذ أبعادا جديدة تستند على المعطى الرقمي والتكنولوجي، وبرزت إزاء ذلك أنماط جديدة من الجرائم لا تقل خطورة عن الجرائم التقليدية بل قد تتفوق عليها، فتكنولوجيات الإعلام والاتصال الحديثة تعتبر سلاحا ثنائي الاستخدام في المجال الأمني تحديدا، إذ يمكن استغلالها في ابتزاز

الضحايا أو تجنيدهم و شحن أفكارهم وإقناعهم برؤى وأفكار خطيرة، أو التأثير فيهم من أطراف مجهولة أو استعمالها كأداة للجرم أو مسرحا للجريمة. كما يمكن استثمارها في الدعاية الإيجابية وتحقيق الأمن الفكري والديني والثقافي، والمحافظة على هوية واستقرار المجتمع وصيانة وتدعيم منظومة القيم والأخلاق، ولتحقيق هذه الأهداف لا بد من اكتمال الوعي بطبيعة التكنولوجيات الحديثة وأساليبها ومخاطرها ومحاذيرها على النفس والفكر والسلوك والمجتمع.

2- المهددات الأمنية الناجمة عن تكنولوجيا المعلوماتية.

لقد أفرزت التكنولوجيات الجديدة للاتصال والمعلومات عدة تهديدات تتسم بالخطورة والجدية والسرعة والشمولية، وهو ما جعلها لصيقة الصلة بالجانب الأمني، ومن أبرز هذه التهديدات الأمنية:

1) التحديات التقنية Technical challenges: وتتمثل في استخدام التقنيات الحديثة في تهديد الأمن، واستغلالها في تنظيم المجموعات الإرهابية وجماعات الجريمة المنظمة والجريمة العابرة للحدود الوطنية ...الخ.

2) التحديات الثقافية Cultural challenges: فالمهددات الأمنية في عصر العولمة تتطلب تحصينا أمنيا ومشاركة اجتماعية وتكوين ثقافة نابذة للعنف والجريمة.

3) التهديد باستغلال المعلومات الحساسة والملكية الفكرية والمعلومات السرية: إن سرقة المعلومات أو الاحتيال أو الجرائم الفضائية لها آثار سلبية على المستوى الفردي، وعلى المستوى المؤسسي (سرقة بطاقات الائتمان) وعلى المستوى الوطني (المعلومات السرية للدولة).

4) التهديد بانتقاء المعلومات لأغراض سياسية أو اقتصادية أو عسكرية.

5) التهديد بتدمير المعلومات أو تدمير مكونات البناء المعلوماتي التحتي الحساس، ولهذا نتائج سلبية كبيرة على الاقتصاد والأمن الوطني(الفيروسات).

6) التهديد عن بعد: لا تتطلب التهديدات الأمنية الوجود الفيزيقي للجناة وإنما يمكن التخطيط و التنظيم والتنفيذ عن بعد، وهذه التهديدات عابرة للحدود الوطنية.

7) تمتاز التهديدات الأمنية بسهولة خفاء الفاعلين وسهولة التنفيذ وانخفاض التكاليف.

8) تهديد البنية المعلوماتية الحساسة التي تشمل الاتصالات، والبنوك والمال والطاقة الكهربائية، وتوزيع الوقود والغاز، والتخزين ومصادر المياه والمواصلات وخدمات الطوارئ والخدمات الحكومية.(البداينة، 2011، ص69)

إن هذه المهددات الأمنية الجديدة لتكنولوجيا المعلومات أعادت صياغة مفهوم جديد للجريمة، يختلف عن المفهوم التقليدي من حيث: طبيعته وأدواته وآثاره، وباستقراء الواقع يمكننا أن نلاحظ جملة من الآثار الناجمة عن تكنولوجيا المعلومات الحديثة والمهددة للأمن الفكري والمجتمعي، ومن أبرزها بحسب الباحث:

1) الاحتيال Fraud: فقد أصبحت وسائل التّواصل الاجتماعيّة مَنصّةً للعديد من ضِعاف النفُوس الذين يستخدموها بطريقة سلبيّة ومنها الاحتيال، ومعظم وسائل الاحتيال تتمّ

عن طريق سرقة النّقود من خلال مواقع البيع والشّراء غير القانونيّة وغير المَوثوقة، أو تقمص شخصيات وهمية أو حسابات مجهولة المصدر.

2) الانكشافية وغياب الخصوصية Absence of privacy : فقد أدى الاتصال الجماعي والتشارك في استعمال التطبيقات المختلفة التي أتاحتها التكنولوجيات والبرمجيات عبر الأنترنت، إلى تراجع مبدأ السرية والخصوصيات الشخصية، فأصبح من الممكن الإطلاع على أسرار الغير من خلال نشر الفضائح والأسرار الشخصية أو عن طريق الاختراق.

3) البرمجة اللغوية والسلوكية Linguistic and behavioral programming: من خلال غرس قيمٍ وسلوكاتٍ منحرفة أو لغات هجينة، فكثرة الصور والفيديوهات والأخبار المكررة عن القتل وصور العدوان، كرست ممارسات عدوانية في لغة وسلوك الأفراد خاصة الشباب منهم.

4) ضعف الحياة الاجتماعية: حيث تراجعت العلاقات الحميمية بين الناس والجيران والأقارب، من خلال الزيارات وتقوية العلاقات الاجتماعية، وحلت محلها العزلة والانغماس في العالم الافتراضي.

5) غياب التثبت والمصداقية Lack of credibility : من خلال المبالغة في نقل الأحداث والأخبار وكثرة الإشاعات والتسرع في مشاركة المعلومات المغلوطة، وغياب التثبت من المصادر الموثوقة والأصلية.

6) تهديدات الهوية Identity threats: ويتمثل هذا الخطر في التأثير سلبا على الهوية الثقافية واللغوية والدينية والأخلاقية، من خلال الانبهار بالغير وفضول الاكتشاف، والتقليد الأعمى لسلوك المنحرفين عبر عمليات الغرس الثقافي والحرب الناعمة وتأثير منصات التواصل وشبكة الأفلام والألعاب ودور السينما.

إن هذه المخاطر الناجمة عن الطفرة الهائلة لتكنولوجيات الاتصال، أصبحت تشكل تحديا خطيرا على الدول والمجتمعات، حيث أضحت تهدد أمنها المجتمعي والثقافي وتساهم في نشر الفوضى والفتن بين أفرادها، خاصة في ظل غياب الوعي وترشيد استغلال هذه الوسائط لدى مختلف فئات المجتمع، ولا أدل على ذلك من تفشي الجرائم الإلكترونية والألعاب الخطيرة المؤدية إلى القتل أو الفساد الأخلاقي، كلعبة الحوت الأزرق التي ظهرت في السنوات الماضية، وعملت على تهيئة وتطويع المراهقين لجرّهم نحو الانتحار، من خلال مراحل وعمليات نفسية مقصودة، الأمر الذي يدفعنا لزاما نحو ضرورة الوعي بحجم وآثار هذه المخاطر، والعمل على تأسيس منظومة حمائية تهدف إلى تأمين العقول والقيم والهوية الثقافية ضد قوى التشويه والاغتراب والاستيلاب.

3- الأنترنت والجريمة الإلكترونية: التحول في طبيعة التهديدات.

لقد جسدت الأنترنت ثورة حقيقية في ميدان المعرفة والتقنية، ومثلت على مدى الخمسين سنة الماضية أعظم إنجاز توصلت إليه البشرية، ساهم بشكل عميق في إعادة صياغة مفاهيم جديدة للعلاقات الدولية والتنظيمات الاجتماعية والسلوكات الإنسانية، فأسس لمفهوم مجتمع المعرفة والاقتصاد الرقمي، وساعد على اندماج المعارف الإنسانية، وما ترتب عن ذلك من تطوير الأفكار وسرعة الابتكارات وتفتق عبقرية العقل البشري في التحليل والإبداع.

والإنترنت Internet هي:" كلمة إنجليزية مختزلة لعبارة "Work net of Interconnection" وهي تتجزأ إلى كلمتين "Interconnection" : وتعني الربط بين عنصرين أو شيئين و "Work Net" وتعني الشبكة. وشبكة الإنترنت عبارة عن مئات الملايين من الحاسبات الآلية حول العالم مرتبطة ببعضها البعض، ومع ترابط هذا العدد الهائل من الحاسبات أمكن إرسال الرسائل الإلكترونية بينها بلمح البصر، بالإضافة إلى تبادل الملفات والصور الثابتة أو المتحركة أو الأصوات، وتتجلى أبرز خدماتها التواصلية: البريد الإلكترونيE-mail، التخاطب والدردشة Chat ، تلفون الانترنت، نقل الإخبار والمعلومات، التيلينت Télé net، بروتوكول نقل الملفات FTP وهو اختصار ل File transfer protocol."(الروقي، 2015، ص 60)

وتعرف الأنترنت أيضا بأنها:" عبارة عن شبكة للمعلومات العالمية، التي يتم فيها ربط مجموعة شبكات مع بعضها البعض في العديد من الدول عن طريق الهاتف والأقمار الصناعية، ويكون لها القدرة على تبادل المعلومات بينها من خلال أجهزة كمبيوتر مركزية تسمى أجهزة الخادم SERVER التي تستطيع تخزين المعلومات الأساسية فيها والتحكم في الشبكة بصورة عامة، كما تسمى أجهزة الكمبيوتر التي يستخدمها الفرد باسم أجهزة المستخدمين USER." (خريسات، (د ت ن) ص45)

وترى **فريحة كريم** أن الأنترنت:" تعبر عن عالم افتراضي عبر جهاز الحاسوب، أين يتحرر الفرد من جسده وعقله وينعزل تماما عن واقعه، وتضيف أنه يمكن تعريف الأنترنت باعتبارها: مجموعة الشبكات المتداخلة التي تمثل منتدى عالمي لكل الثقافات والآراء والنشاطات، والتي تقوم على فكرة تفاعل المعلومات التي تتم بين طرفين كل منهما مرسل في الوقت نفسه."(صافة، 2016، ص 26.)

فالأنترنت أضافت "**البعد الكوني**" للمجال الفكري للإنسان المعاصر، وأسست لواقع سوسيولوجي مستحدث، من خلال استعمالاتها المتنوعة وواسعة النطاق، والتي تشمل" مختلف نشاطات الإنسان التجارية بالإضافة إلى مجالات التعليم والترفيه، ولقد أخذت آثارها في البروز بشكل جلي في مجال الاتصالات، وتبادل الأفكار والمعلومات بشكل جعل الحدود الجغرافية تنعدم وتتلاشى، ومن خلال هذا النشاط الإنساني عبر شبكة الانترنت ظهرت الأنشطة الإجرامية...وتطورت الجريمة المرتكبة عبر الأنترنت بشكل رهيب في المدة الأخيرة، وذلك بالنظر إلى التطور المستمر والمتسارع لشبكة الأنترنت، مما جعل هذه الشبكة وسيلة مثالية لتنفيذ العديد من الجرائم بعيدا عن أعين الجهات الأمنية، حيث مكنت الأنترنت العديد من المجرمين والجماعات الإجرامية من القيام بعدة أفعال غير مشروعة، مستغلين مختلف التسهيلات التي تقدمها هذه الشبكة، وذلك دون أدنى مجهود ودون الخوف من العقاب."(بن صغير، 2015، ص 02)

وتأسيسا على ما سبق فإنه يطلق على الجرائم المتصلة بالأنترنت وبالوسائل التكنولوجية الحديثة وعلى رأسها الحاسوب الآلي والهواتف الذكية **بالجرائم الإلكترونية Cyber Crime أو الجرائم عبر الأنترنت**، وتعرف على أنها:" نشاط إجرامي تستخدم فيه التقنية الإلكترونية – الحاسوب الآلي والرقمي وشبكة الأنترنت- بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف." وبصياغة أخرى عرفها البعض الآخر

بأنها:" جرائم الشبكة العالمية التي يستخدم الحاسب وشبكاته العامة كوسيلة مساعدة لارتكاب الجريمة، مثل استخدامه في النصب والاحتيال وغسل الأموال وتشويه السمعة والسب"...وتعد جرائم الأنترنت من هذا المنطلق: أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية، أو بمعنى آخر: هي كل فعل غير مشروع يكون علم تكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه."(بن صغير، 2015، ص 05)

وقد نبه المفكر عابد الجابري منذ أمد إلى المخاوف المنتظرة جراء سوء استخدام الأنترنت وتعميمها في ظل ضعف الوازع الفكري والانفلات المعلوماتي، فقال:" في مجال المعلوماتية وتكنولوجيا الاتصال السمعي والبصري عبر الأقمار الصناعية والاتصال حول شبكة الطرق السيارة للمعلومات، فإن عملية "هتك الحرمات" تتسع وفي نفس الوقت يتضاءل الأمل في تدارك الموقف وإمكانية التحكم...فما يقذف اليوم في شبكة الأنترنت من صور وممارسات تدخل في مجال "الخلاعة" وما يبث فيها من معلومات وتقنيات خاصة بصنع القنابل وتشكيل العصابات وغير ذلك، مما يتنافى مع القيم والمعايير الأخلاقية يثير المخاوف بشكل جدي." (الجابري،1997،ص 38)

فالاستخدام السيئ للأنترنت ساهم في إعادة هندسة مفهوم جديد للتهديد، وتغيرت بفعل ذلك طبيعته وتنوعت أساليبه وازدادت ضراوة، وإذا شئنا أن نميز أبرز الجرائم المتصلة بالأنترنت فسنحددها في ما يلي:

1- جرائم العرض Honor crimes : وتتمثل في المواد الإباحية المعروضة على شبكة الانترنت.

2- النصب والاحتيال Fraud : ويأخذ النصب والاحتيال صورا عديدة مثل: بيع سلع أو خدمات وهمية أو المساهمة في مشاريع استثمارية وهمية أو سرقة معلومات البطاقات الائتمانية واستخدامها.

3- انتهاك حقوق الملكية الفكرية على شبكة الانترنت: يعد مجال الملكية الفكرية Intellectual property في الإبداع من الأمور التي يحاول إنسان القرن الحادي والعشرين وضع حدود وقوانين لها، وإن كان انتهاك الملكية الفكرية ظاهرة قديمة، إلا أنها انتشرت بشدة على شبكة الأنترنت للانفتاح الذي تنتجه الشبكة على كل المواد الإبداعية.

4- صناعة ونشر الفيروسات Industry viruses and publish : وهي أكثر جرائم الانترنت انتشارا وتأثيرا خاصة في السنوات الأخيرة، حيث أصبحت الأنترنت وسيلة فعالة وسريعة في نشر الفيروسات...فإن الهدف المباشر للفيروسات هي المعلومات المخزنة على الأجهزة المقتحمة، حيث تقوم بتغييرها أو حذفها أو سرقتها أو نقلها إلى أجهزة أخرى، كما أنها قد تسبب أخطارا رهيبة لملفات الكمبيوتر الشخصي، والفيروس هو عبارة عن شفرة كمبيوتر تكتب لتسبب المقاطعة أو الضرر عند تنفيذها.

5- انتحال الشخصية Identity theft : تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية، وتهدف إما لغرض الاستفادة من مكانة تلك الهوية أي الضحية أو لإخفاء هوية شخصية المجرم لتسهيل ارتكابه جرائم أخرى.

6- استخدام المواقع المتخصصة في القذف وتشويه سمعة الأشخاص: تعمل هذه المواقع على إبراز سلبيات الشخص المستهدف ونشر أسراره والتي قد يتم الحصول عليها بطريقة

غير مشروعة، بعد الدخول إلى جهازه أو بتلفيق الأخبار عنه. وحوادث التشهير والقذف في شبكة الانترنت كثيرة، فقد وجد ضعفاء النفوس في شبكة الانترنت وفي ظل غياب الضوابط النظامية والجهات المسؤولة عن متابعة السلبيات التي تحدث أثناء استخدام الانترنت متنفسا لأحقادهم.(صافة، 2016، ص83-87 بتصرف)

7- الاختراقات Penetrations: تتمثل في الدخول غير المصرح به إلى أجهزة أو شبكات الحاسب الآلي، فجُل عمليات الاختراق (أو محاولات الاختراق) تتم من خلال برامج متوفرة على الأنترنت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير، وهنا تكمن الخطورة، وتختلف الأهداف المباشرة للاختراقات، فقد تكون المعلومات هي الهدف المباشر، حيث يسعى المخترِق لتغيير أو سرقة أو إزالة معلومات معينة، وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه، كأن يقوم المخترِق بعمليته بقصد إبراز قدراته "الاختراقية" أو لإثبات وجود ثغرات في الجهاز المخترَق.

8- تعطيل الأجهزة Disable hardware : كثر مؤخرا ارتكاب مثل هذه العمليات، حيث يقوم مرتكبوها بتعطيل أجهزة أو شبكات عن تأدية عملها بدون أن تتم عملية اختراق فعلية لتلك الأجهزة. وتتم عملية التعطيل بإرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها الأمر الذي يعيقها عن تأدية عملها.

9- التغرير والاستدراج Deception and enticement: غالب ضحايا هذا النوع من الجرائم هم من صغار السن من مستخدمي الشبكة، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة على الأنترنت والتي قد تتطور إلى التقاء مادي بين الطرفين. إن مجرمي التغرير و الاستدراج على شبكة الأنترنت يمكن لهم أن يتجاوزوا الحدود السياسية، فقد يكون المجرم في بلد والضحية في بلد آخر، وكون معظم الضحايا هم من صغار السن فإن كثيرا من الحوادث لا يتم الإبلاغ عنها، حيث لا يدرك كثير من الضحايا أنهم قد غُرر بهم. (الهاجري، 2004، ص144-145)

10- ألعاب القمار Slot games : ظاهرة نوادي القمار عبر الأنترنت تتداخل مع ظاهرة غسل الأموال باعتبار أن كليهما من صور الجريمة المنظمة Organized crime... وهي مواقع صممت على غرار - كازينو لاس فيغاس - الذي يوفر كل أنواع القمار وألعابه بدءا بألعاب القمار وانتهاء بآلات المقامرة، وهذه النوادي هي على شبكة الأنترنت، ويديرها أفراد قلائل من منازلهم أو مكاتبهم الصغيرة، ويدفعون رسوما للحكومات تصل إلى 85 ألف دولار للمراهنات الرياضية، وأكثر منها للكازينوهات الرياضية، وذلك يوفر فرصة للقائمين على جريمة غسل الأموال غير المشروعة من خلال شبكة الانترنت.

11- الابتزاز عبر الأنترنت Blackmail online :ونقصد بهذا استخدام الأنترنت لمضايقة أو تهديد شخص ما بصفة مستمرة، كما يتضمن تعقب هذا الشخص في الحياة الواقعية والظهور في منزل هذا الشخص وعمله مهددين أملاكه بل وعائلته، أي يمكننا القول أنها عملية تهديد إلكترونية وفعلية للضحية. وقد لا يكون التهديد في البداية عبر الأنترنت اتصالا فعليا، إلا أنه يمكن أن يتطور وقد يؤدي لاستخدام العنف، ولهذا السبب فهي جريمة خطيرة.(صافة، 2016، ص 83-87.)

إن التوظيف السلبي لمختلف الوسائط الرقمية له تبعات خطيرة على الوعي والفكر وعلى الآصرة المجتمعية، ويعود ذلك غالبا إلى جهالة أساليبها الذكية في التأثير على الرأي العام وتشكيل المفاهيم وإعادة هندسة الأفكار وتأطيرها، ودفعها نحو المسارات والأهداف التي يريدها أصحابها، وهذا يحيلنا إلى التعرف على خصائص الجرائم التي تعتبر الأنترنت إما وسيلة أو مسرحا لها.

4- خصائص الجرائم المتصلة بالأنترنت.

تتسم الجرائم المتصلة بالأنترنت بطبيعة خاصة وهي ذات توصيف قانوني وإجرائي مختلف عن الجرائم التقليدية، وهذا يعود للخصائص المستحدثة التي يمتاز بها الجرم وماهية مرتكبه ونوعية ضحاياه،" فكل ما تحتاجه جرائم الأنترنت هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الأنترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين، فمن هذا المنطلق تعد الجريمة المرتكبة عبر الأنترنت من الجرائم النظيفة، فلا آثار فيها لأي عنف أو دماء، وإنما هي مجرد أرقام وبيانات يتم تغييرها من السجلات المخزونة في ذاكرة الحاسبات الآلية، وليس لها أثر خارجي مادي." (بن صغير، 2015، ص 09)

وبناء عليه تتسم الجرائم المتصلة بالأنترنت بخصائص متفردة تختص بها عن غيرها من الجرائم التقليدية، ويمكن أن نحددها في ما يلي:

1- خفاء الجريمة وسرعة التطور في ارتكابها: فهي خفية ومتسترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من اقتراف جريمته بدقة، مثلا: إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وسرعة المكالمات وغيرها من الجرائم...ويستفيد المجرمون في مختلف أنحاء العالم من الشبكة في تبادل الأفكار والخبرات الإجرامية في ما بينهم، ويظهر لنا ذلك جليا في مختلف المواقع الإلكترونية ومنتديات القراصنة (الهاكرز)، التي تضمن لهم الاتصال فيما بينهم، من أجل تبادل المعارف والخبرات في مجال القرصنة وذلك من أجل ارتكابهم لجرائمهم بعيدا عن أعين الأمن.

2- اعتبارها أقل عنفا في التنفيذ: لا تتطلب جرائم الأنترنت عنفا لتنفيذها أو مجهودا كبيرا فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية، التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صور ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف..الخ.

3- جريمة عابرة للحدود: بعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات، وتبادلها بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها: أن أماكن متعددة في دول مختلفة وعبر الأنظمة التقنية الحديثة، جعل بالإمكان عن طريق حاسوب موجود في دولة معينة ارتكاب الفعل الإجرامي في دولة أخرى، وذلك راجع إلى مجتمع المعلومات الذي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود.

4- سرعة محو الدليل لتوفر وسائل تقنية تعرقل الوصول إليه: البيانات والمعلومات المتداولة عبر شبكة الأنترنت تكون على هيئة رموز مخزنة على وسائط تخزين ممغنطة لا تقرأ إلا بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه إلى الجاني يبدو أمرا صعبا لاسيما وأن الجاني يتعمد عدم ترك أي أثر لجريمته... وتتم الجريمة المرتكبة عبر الأنترنت خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والأنترنت، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل في غاية السهولة. فالمجرم في جرائم الأنترنت يعيق سلطات التحقيق في الوصول إلى الدليل بشتى الوسائل، كمسح برامج أو وضع كلمات سرية ورموز، وقد يلجأ لتشفير التعليمات لمنع إيجاد أي دليل يدينه.

5- صعوبة الوصول إلى الدليل: وذلك نتيجة قيام كبرى المواقع العالمية على الأنترنت بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية الفنية لمنع التسلل والوصول غير المشروع إليها لتدميرها أو تبديلها أو الاطلاع عليها أو نسخها، هذا من جهة، ومن جهة أخرى يمكن للمجرم زيادة صعوبة عملية ضبط أي دليل يدينه وذلك من خلال: استخدامه كلمات مرور بعد تخريب الموقع مثلا أو استخدام تقنيات التشفير.

6- صعوبات شديدة في ضبط وتوصيف جرائم المعلوماتية: لا مراء في أن رجال الضبطية القضائية والمحققين والقضاة يصادفون صعوبات جمة فيما يتعلق بإجراءات ضبط جرائم المعلوماتية، وإضفاء الوصف القانوني المناسب على الوقائع المتعلقة بها، ولعل مرد ذلك يرجع إلى الطبيعة الخاصة لهذه الجرائم، فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود.

7- فكرة الاختصاص والطبيعة الدولية للجرائم المعلوماتية: الجرائم المعلوماتية تتم - في الغالب الأعم- بأفعال ترتكب من قبل أشخاص خارج الحدود، كما أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود، الأمر الذي يثير التساؤل حول الاختصاص القضائي لهذه الجرائم، علاوة على أن امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود، أمر يحتاج إلى تعاون دولي شامل يستهدف تحقيق مكافحة هذه الجرائم، مع احترام السيادة الوطنية للدول المعنية.(بن صغير، 2015، ص 09-11.)

إن نوعية الجرائم الإلكترونية الجديدة وما تتميز به من خصائص تشكل تحديا كبيرا على الأمن الفكري والأخلاقي و المعلوماتي والاجتماعي للأفراد والمجتمعات، خاصة تلك التي تعاني من ضعف تكنولوجي واتساع الفجوة الرقمية The digital divide. وهذا يتطلب إعادة مراجعة المنظومة التعليمية والقانونية والقضائية والأمنية والإعلامية، وتطوير أدائها بما يتناسب مع طبيعة وحجم التحديات التي فرضتها البيئة الرقمية بوسائلها الذكية وعالمها الافتراضي، ومنطقها المتميز بالسرعة والتغير المستمر في المضامين والوسائل والقوة التأثيرية بفعل جاذبية التقنيات الحديثة والتطبيقات الإلكترونية واستقطابها لعقول المستخدمين وتوجيهها لسلوكهم.

وللوقاية من تبعات الاستخدام السيئ للأنترنت وتكنولوجيا المعلومات والاتصالات وإرساء مقومات الأمن السيبراني، لا بد من اتخاذ تدابير ضرورية على المستوى التقني والفني، وأخرى على المستوى المعرفي والتعليمي والتربوي لصيانة الأمن الفكري والإعلامي، الذي يمثل بعدا أساسيا في ترسيخ الأمن المجتمعي بمفهومه الشامل.

5- التدابير التقنية والفنية لتحقيق الأمن السيبراني.

إن الوقاية من مختلف الجرائم الإلكترونية السابقة يتطلب "معرفة متخصصة" بأحدث تقنيات الحماية والأمن السيبراني Cybersecurity، التي تشهد تطورا مطردا وتحديثا متجددا،" ويتطلب الوفاء بهذه المسؤولية التزامًا بنهج دفاعي متعمق لأمن المعلومات، يستخدم ضوابط أمنية متعددة ومتداخلة لتحقيق كل هدف من أهداف الأمن السيبراني. كما يتطلب أيضًا أن يكون لدى المحللين فهم قوي لبيئة التهديد التي تواجه مؤسستهم، من أجل تطوير مجموعة من الضوابط القادرة على الارتقاء إلى مستوى الحدث والرد على تلك التهديدات." (Chapple, Seidl, 2017,P 63) ونورد هنا أهم التدابير التقنية والفنية لتفادي الجرائم الإلكترونية وهي:

1- استعمال البرمجيات المضادة للاعتداءات الإلكترونية وهي تعمل على البحث وتحطيم البرامج الخبيثة التي يمكن أن تتواجد بذاكرة الحاسب أو بأحد وسائط التخزين...كما تعمل على إيقاف أغلب الاعتداءات الأخرى كاستعمال برامج الجوسسة.

2- تطوير وسائل الدفع المالي كالبطاقة الائتمانية التي تعتبر من أكثر الوسائل أمانا.

3- إنشاء نسخ احتياطية من المعلومات العامة والخاصة بالمستهلكين في المنظمة والمتجر بحيث يمكن استرجاعها لو فقدت.

4- التحكم بدخول المستخدمين باستخدام الجدار الناري أو جدار الحماية (Fire-wall) وهذا لمقاومة أخطار المتطفلين وتوفير الحماية للمنظمات. **والجدار الناري** عبارة عن مكونات مادية وبرمجيات خاصة توضع بين الشبكة الداخلية للمنظمة من جهة وبين الشبكات الخارجية ويعمل على منع أي من المستخدمين الخارجيين من التوغل في الشبكات الخاصة والدخول غير المرخص.

5- تشفير الملفات File encryption أي تحويل محتوى الرسائل بشكل يصعب على الغير معرفة المحتوى الأساس، أو إعادته إلى وضعه الأصلي، ولا يقوم بذلك إلا من يعرف كيف يتم تحويره. فالتشفير هو عبارة عن تغيير صيغة الكتابة من صيغة مفهومة إلى أخرى غير مفهومة من قبل عامة الناس.

6- التوقيع الإلكتروني Electronic signature وهو استخدام طريقة للتحقق من أن صاحب المعاملة هو نفس الشخص الذي قام بإرسالها أو تنفيذها، كما يطلق عليه بالبصمة الإلكترونية، ويتم تشفير التوقيع الإلكتروني باستخدام نظام التشفير عن طريق المفتاح العام المزدوج.

7- طمس البيانات فالبيانات لا تحذف من الجهاز بمجرد حذف الملف أو تفريغ سلة المهملات، فهذا لا يعني الإتلاف النهائي للملفات، بل يتم ذلك عن طريق حذف المؤشر الذي يدل عليه وليس الملف نفسه، أي أن محتويات الملف تظل في وحدة التخزين ولكن على هيئة

مساحة فارغة يمكن الكتابة عليها، وبهذا يمكن بواسطة برامج استرجاع متخصصة استرجاع ذلك الملف.

8- حماية البرمجيات فهناك بعض العناصر المستخدمة في أمن البرمجيات منها:

أ- وضع كلمة مرور تكون قوية بحيث: لا تكون مكونة من كلمة واحدة، أو تتضمن معلومات شخصية كالاسم وتاريخ الميلاد، لا تقل عن 10 خانات، تكون خليطا من الحروف الصغيرة والكبيرة والأرقام والرموز، وتحديثها بشكل مستمر.

ب- استخدام برامج مضادة للفيروسات وتحديثها باستمرار.

ت- التحديث المستمر للبرمجيات كبرنامج Windows فبسبب التحسين المستمر لهذه البرامج قد تظهر عليها ثغرات أمنية تعرض الجهاز للاختراق، ولتلافي ذلك فلابد من تحديث هذه البرامج باستمرار.

ث- حماية البرمجيات، فعلى المستخدم أو المنظمة أن تراعي ما يلي:

- وضع قوانين إدارية أمنية لاستخدام الحواسيب المحمولة وكلمات المرور؛
- تجنب أي شيء ليس له علاقة بما يبحث عنه؛
- المراقبة التقنية الدورية للتركيبة الحاسوبية؛
- المراقبة الفنية الدورية للبرامج الحاسوبية. (حواس وحبوشي، 2017، ص 115. بتصرف)

إن إرساء الثقافة الرقمية أصبحت معطى أساسيا في مجتمع المعلومات، الذي فرض واقعا جديدا يتطلب من الجميع التكيف معه ومسايرة تداعياته، وعليه صار لزاما على المؤسسات في مختلف المجالات لاسيما الأمنية منها، تخصيص تكوينات متميزة في أساليب الوقاية من الجرائم الإلكترونية، كما على المؤسسات الإعلامية التربوية والجامعية المساهمة بقسط وافر في نشر الوعي الرقمي وتدابير الحماية اللازمة وتحديثها باستمرار، لتحقيق الأمن السيبراني والحد أو التحكم في تبعات الهجمات والجرائم الإلكترونية.

6- تدابير إرساء الأمن الفكري والإعلامي للحد من جرائم الأنترنت.

يُجمع العديد من الباحثين والمفكرين أن التحديات الجديدة التي فرضتها تقنيات الاتصال الذكية في ظل بيئة العولمة تفرض على الدول اتخاذ الاستراتيجيات الضرورية والملائمة لتجسيد متطلبات الأمن المعلوماتي Information security تحقيقا للغاية الكبرى وهي الأمن المجتمعي العام والشامل. وفي هذا السياق تُعزى العديد من مظاهر الجريمة وأسبابها إلى المواد الإعلامية المنكشفة والميسَّرة لكافة فئات المجتمع لاسيما المراهقين منهم، عن طريق الأنترنت أو القنوات الإعلامية ذات الخط الافتتاحي والتوجه الإعلامي غير المتحفظ، ومن هذه المواد الإعلامية: أفلام الأكشن والدراما والمواقع الإرهابية والإباحية..الخ، والتي تعمل على التوجيه اللاإرادي لوعي وسلوك المشاهدين نحو طباع العنف وسلوك الإجرام، من خلال ترويض النفوس على صور القتل والدم والمخدرات والعلاقات الجنسية حتى تَهُونَ حرمتها في النفوس، ويَسْتَسْهِل الشباب ارتكابها.

وعليه طرح العديد من العلماء **مقاربة العلاج بالداء نفسه**، أي تحويل الداء إلى دواء، بحيث إذا اعتبرنا الإعلام هو الداء في بعض جوانبه فلابد أن نجعل منه دواء من خلال تبني

مفهوم"**الأمن الإعلامي التنافسي Competitive media security** " كأحد أهم أبعاد الأمن المجتمعي في عصر العولمة والغزو الثقافي، وفي هذا السياق يكننا أن نقدم تعريفا إجرائيا للأمن الإعلامي باعتباره:" **استراتيجية شاملة وواعية تتخذها الجهات الرسمية في الدولة لتأمين المقومات الوطنية والقيم الدينية والأخلاقية واللغوية والعادات الأصيلة للمجتمع، من كل التيارات المعادية والساعية لتفكيك الكيان المجتمعي، والتشكيك في الحقائق والمبادئ العامة للمجتمع، وذلك من خلال وضع قواعد ومبادئ واضحة لميثاق أخلاقيات الإعلام الوطني وبيان موضوعه وغايته وطبيعته ومجاله ورسالته والالتزام بالدفاع عنها، باستخدام التكنولوجيا الحديثة للمعلومات والاتصالات.**" وينظر للأمن الإعلامي اليوم كأحد الغايات الإستراتيجية لأي مجتمع، فهو يهدف لتأمين الجبهة الداخلية للدولة وصد ما تتعرض له من جبهتها الخارجية من محاولات للتشويه أو الاغتراب والاستيلاب.

ولتحقيق الأمن الإعلامي فلابد من اتخاذ مجموعة من التدابير الاستباقية والاستشرافية التي تشكل متكاملة: **استراتيجية لتحقيق الأمن الفكري والإعلامي،** وفي هذا الصدد يقترح الباحث التدابير التالية**:**

1- إعادة مراجعة المنظومة القانونية المتعلقة بالجرائم والجنح والجنايات وتكييفها مع مستجدات الواقع التكنولوجي الجديد.

2- تكثيف برامج التكوين للهيئات التعليمية والأمنية والقضائية في تكنولوجيا المعلوماتية والرقمية وتزويدهم بالمهارات اللازمة، قصد التحيين الدوري لمعارفهم وتمكينهم من معالجة الوضعيات التي تعترضهم بكفاءة أكثر.

3- ترقية الثقافة الرقمية Digital culture لدى المجتمع من خلال تكثيف الحصص والبرامج التي تشرح مخاطر التوظيف السيئ للتكنولوجيا على الأفراد والأطفال خصوصا، وأساليب التحايل الرقمي في شتى الميادين: التجارة والأموال، الابتزاز، انتحال الشخصية، التشهير، القرصنة، الاختراق، الألعاب، المواقع الجهادية والإباحية...الخ، مع تقديم إرشادات هامة حول الإجراءات اللازم اتخاذها للوقاية منها أو تدابير الحماية حال التعرض لمثل هذه الحالات.

4- تكييف المناهج الدراسية مع مستجدات البيئة الرقمية خاصة في المراحل الابتدائية، بإقرار مواد تُعنى بالوعي الرقمي والتربية التكنولوجية وتعليم التلاميذ الاستعمالات الجيدة والسليمة للتكنولوجيا، وتحذيرهم من عواقب وخطورة التوظيف الخاطئ لها.

5- ضرورة التركيز على التكوين المتخصص في "الإعلام الأمني Security media " وترقية مهارات رجال الأمن والشرطة القضائية والعلمية في مجال التكنولوجيات وبشكل مستمر، لمواكبة التحديثات المستجدة ومعرفة تقنيات التعامل مع الجرائم الإلكترونية.

6- وضع إطار تعريفي شامل للجرائم الحديثة المتعلقة بمخاطر الأنترنت وتوعية الآباء بمدى خطورتها وعواقبها وطبيعتها وآثارها النفسية والاجتماعية والأخلاقية والأمنية على أبنائهم.

7- تنقيح وتهذيب المحتوى الإعلامي المقدم سواء على التلفزيون أو شبكات التواصل والأنترنت، كحجب المواقع الإباحية والجهادية، ومنع الأفلام التي تروج للصور الوحشية والابتذال الأخلاقي.

8- تكوين الأساتذة في مجال علم النفس التربوي Educational psychology وعلم نفس المراهق ومجال الإعلام الآلي، لبيان آثار التكنولوجيات الرقمية الحديثة وسبل استثمارها في الميدان المعرفي والعلمي، وكشف مخاطرها مع الاستماع لانشغالات الطلبة وتوجيههم ومرافقتهم بيداغوجيا ونفسيا.

9- ضرورة الانتقال من الاستراتيجية الدفاعية إلى الاستراتيجية الوقائية والتنافسية والاستباقية، ومن الأمن بمفهومه التقليدي، إلى الأمن الفكري والمعلوماتي والسيبراني، فمنطلق كل جريمة هو انحراف على مستوى الفكر.

10- التسويق الإعلامي التنافسي للقيم الوطنية وتشجيع الجمعيات الشبابية التي تعنى بقضايا الشباب وتطلعاتهم، وإنشاء خلايا الاستماع والتوجيه والنصح للشباب بما فيهم المنحرف، وذلك للانتقال من دور المتلقي والمتأثر إلى دور المرسل والمؤثر.

الخاتمة:

إن أكبر تحدٍّ أمني في العصر الرقمي الحديث الذي يشهد ثورة معلوماتية متزايدة ومتسارعة هو تحقيق شروط ومقومات الأمن السيبراني، باعتباره مقدمة شرطية لتحقيق الأمن الفكري والديني والثقافي والاجتماعي، فالفكرة تقاوم بالفكرة وليس بالرصاصة أو القانون فقط، فامتلاك المقدرة التكنولوجية وكفاءة الإقناع ومعرفة المداخل الحديثة للتأثير في توجهات الشباب وتعديلها هو كفيل بترسيخ ركائز الأمن المجتمعي الشامل.

وإثراءً لما تم تفصيله في هذه الدراسة يتقدم الباحث بجملة التوصيات التالية :

1- ضرورة العمل الجاد على تحديث وتطوير أساليب العمل الإعلامي والأمني ومواكبة العصرنة، مع صيانة المنظومة القيمية والوطنية.

2- العمل على تحديث الذهنيات وأنماط التفكير خاصة لدى المستويات القيادية والإدارية ومراكز اتخاذ القرار، لمواجهة التحديات الجديدة بعقلية أكثر انفتاحا على مختلف شرائح المجتمع، والسعي إلى تطبيق سياسة الاحتواء والاندماج وسط المحيط الاجتماعي، واستقطاب الشباب وفق مقاربات علمية فعالة (مثل تبني استراتيجية الشرطة المجتمعية).

3- عدم التركيز على آليات العقاب أو التخويف والزجر فقط، لأن جيل العصر الرقمي المنفتح على ما وراء الحدود السياسية والجغرافية، لا يتقبل كثيرا أسلوب الانصياع والتهديد والزجر بقدر ما يتفاعل بإيجابية مع أساليب التواصل الجيدة والفعالة، وهذا هو المدخل الحديث لتحقيق الأمن الإعلامي والرقمي، والاستثمار في تكنولوجيات الإعلام والاتصال بما يحقق التشاركية والثقة بين المواطن ومؤسسات دولته لاسيما الأمنية منها.

4- لابد من تكريس ثقافة المواطنة بكافة أبعادها الحضارية وتوعية المواطن بأنه شريك في تحقيق الأمن الرقمي والتنمية الشاملة، لأنه المستفيد الأول والأخير من توفر الأمن والمتضرر الأول من غيابه.

5- يجب على الحكومات والدول إعادة النظر في السياسات الأمنية والتعليمية وتحديثها بما يجعلها قادرة على استيعاب المتغيرات الحديثة، وتطوير كفاءات المؤسسات لتكون قادرة على مجابهة ومعالجة الأنماط الجديدة للانحرافات والجرائم الإلكترونية، التي تتسم بخصائص أكثر دقة وذكاء وخفاء وسرعة وتأثيرا على نفوس وعقول فئة الشباب خصوصا، الذين هم أكثر ضحايا هذه الوسائط الجديدة ومن أشد المتفاعلين معها.

مراجع الدراسة:

أولا/ باللغة العربية:

1- محمد عابد الجابري. **قضايا في الفكر المعاصر.** (بيروت: منشورات مركز دراسات الوحدة العربية، 1997).

2- إياس بن سمير الهاجري. **أمن المعلومات على شبكة الأنترنت.** (الرياض: منشورات جامعة نايف للعلوم الأمنية، 2004).

3- برا سنان. **إشكالية المواطنة: الرعية في التراث السياسي الإسلامي**. (برلين(ألمانيا): المركز الديمقراطي العربي للنشر ، 2017).

4- سعد بن معتاد الروقي. **مدى استخدام تقنية المعلومات والاتصالات في تحسين أداء إدارات الموارد البشرية.** (الرياض: دار جامعة نايف للنشر ، 2015).

5- عبد الله خريسات. **التطبيق العملي للمكتبة و البحث العلمي،** (الأردن: دار عالم الثقافة، (د ت ن).

6- ذياب موسى البداينة. **الأمن الوطني في عصر العولمة.** (ط1، الرياض: منشورات جامعة نايف العربية للعلوم الأمنية، 2011).

7- لحواطي عتيقة. استرجاع المعلومات العلمية والتقنية في ظل البيئة الرقمية ودوره في دعم الاتصال العلمي بين الباحثين: دراسة ميدانية مع أساتذة الباحثين بجامعة محمد الصديق بن يحي –جيجل-.(**أطروحة دكتوراه،** جامعة قسنطينة، معهد علم المكتبات والتوثيق، 2013-2014).

8- صافة أمينة. آثار استعمال التكنولوجيا على أفراد الأسرة الجزائرية: دراسة للتأثيرات النفسية والاجتماعية والأخلاقية والصحية لاستعمال الأنترنت على أبناء الاسرة الجزائرية أنموذجا. (**أطروحة دكتوراه،** قسم علم النفس وعلوم التربية والأرطوفونيا، كلية العلوم الاجتماعية، جامعة وهران (الجزائر) ،2015-2016).

9- حورية بولعويدات." استخدام تكنولوجيا الاتصال الحديثة في المؤسسة الاقتصادية الجزائرية." (**مذكرة ماجستير،** جامعة منتوري قسنطينة، كلية العلوم الانسانية، والعلوم الاجتماعية، قسم علوم الاعلام والاتصال، 2007).

10- حواس مولود وحبوشي عبد الناصر. التحديات الأمنية لتكنولوجيا المعلومات. (**مجلة الآفاق للدراسات الاقتصادية،** كلية العلوم الاقتصادية والتجارية وعلوم التسيير. جامعة تبسة، المجلد 3 العدد 1، 2017).

11- زوبير زرزايحي. العولمة الإعلامية والهوية الثقافية في الجزائر، (**سلسلة أعمال الملتقيات: العولمة والهوية الثقافية،** جامعة منتوري قسنطينة: مخبر علم اجتماع الاتصال للبحث والترجمة، 2010).

12- عبد المؤمن بن صغير. الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن. **ورقة بحثية** مقدمة ضمن الملتقى الوطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة. (جامعة بسكرة، كلية الحقوق والعلوم السياسية، 16-17 نوفمبر 2015).

13- تقرير الإتحاد الدولي للاتصالات، **"استعمال تكنولوجيا المعلومات والاتصالات لمعالجة مسألة تغير المناخ"**. (أمانة المبادرة العالمية للاستدامة الإلكترونية، بلجيكا، فبراير 2011).

ثانيا/ باللغة الأجنبية:

1- Mike Chapple, David Seidl, **Cybersecurity Analyst (CSA+™)**. (USA: Wiley by John Wiley & Sons , 2017)

2- Srdjan Krčo and Others, **Digitization of Value Chains and Ecosystems**. (From a collective book entitled: Digital Business Models Driving Transformation and Innovation. Editor: Annabeth Aagaard, Publishing Springer Nature, 2019.)

3- Steven M. Stone. **Digitally Deaf Why Organizations Struggle with Digital Transformation**. (Switzerland: Springer Nature, 2019).

4- Vlado Damjanovski. **Networking and Digital Technology**. (Second Edition, USA: Elsevier Butterworth–Heinemann, 2005).