الجرائم السيبرانية وآثارها على الأمن المجتمعى
فى ضوء القانون الدولى العام

د. مسعد عبدالرحمن زيدان قاسم زيدان
دكتوراه في القانون الدولي العام كلية الحقوق- جامعة القاهرة
أستاذ القانون الدولي المشارك بجامعة نايف العربية للعلوم الأمنية سابقا

مقدمة

بادئ ذى بدء لابد ، أن ننوه الى أنها الحقيقة عندما نقول بأن التطورات التكنولوجية المعاصرة سواء على المستوى الوطنى أو الدولى كشفت العديد من الجرائم السيبرانية[١] التي لا يعوقها الحدود السياسية للدول ،ومن ثم تزايد خطورتها لتنوعها وفق الهدف الذى تسعى اليه سواء كانت أهداف اقتصادية أو إجتماعية أو سياسية وتكون تبعاتها بعيدة الأثر وسريعة ومدمرة بالنسبة لضحاياها في ظل درجة عالية من الإفلات من العقاب ، وهو ما توكده الاحصاءات سواء وقت السلم[٢] أو الحرب[٣] أو الأزمات [٤] . نتيجة

---

(١) وتشمل : ١- جرائم اختراق الحواسب ومراكز المعلومات مثل تغيير وثيقة ملكية أو تغيير بيانات ضرائبية ،٢- وجرائم شبكات الانترنت مثل :التشهير وتشويه السمعة،والسطو على أرقام البيطاقات الائتمانية.٣- الاشكال الجديدة والمستجده من الجريمة السيبرانية مثل إساءة استعمال العملات المشفرة، والجرائم المرتكبة على الشبكة الخفية وإنترنت الأشياء، والتصيد الاحتيالي، ونشر البرامجيات الخبيثة .

انظر : نشرة الاتحاد المصرى للتأمين،عدد اسبوعي،رقم ٦٧ ، سنة ٢٠١٩.بعنوان"الهجمات الالكترونية (السيبرانية) والتأمي.https://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244&PageDetailID=1324

انظر ايضا : فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية ، فيينا، ٦-٨ نيسان/أبريل٢٠٢١ .

UNODC/CCPCJ/EG.4/2021/CRP.1 17 February 2021

(٢) حيث تتراوح معدلات التأذي، من تزوير بطاقات الائتمان وانتحال الشخصية على الإنترنت والوقوع ضحية لمحاولات تصيد احتيالي ومحاولات اطلاع دون إذن على حسابات البريد الإلكتروني، بين ١ و ١٧ في المائة من نسبة السكان الذين يستخدمون الإنترنت في ٣٠ بلدا في جميع أنحاء العالم ، ويقدَّر أنَّ حوالي ٢٤ في المائة من إجمالي حركة الإنترنت العالمية تنتهك حقوق النشر.

انظر : مكتب الأمم المتحدة المعني بالمخدرات والجريمة – فيينا ، دراسة شاملة عن الجريمة السيبرانية ، نيويورك ، مسودة شباط/فبراير ٢٠١٣ .ص ٢٤ .

(٣) كلما زادت رقمنة الجيش، زادت نظريا مساحة الهجوم التي يوفرها ، فمن خلال أسلوب الحرب المختلطة أو ما يعرف بالهجينة عن طريق توجيه الهجمات إلى البنية التحتية لتكنولوجيا المعلومات وتوجيه المعلومات الكاذبة كجزء من الحرب النفسية الحديثة يتم اختراق بيانات وزارات الدفاع ، فبحسب وزارة الدفاع الروسية، تم تدمير ١٦١٢ موقعا بينها ٥٤ مركز قيادة ونقطة اتصالات تابعة للجيش الأوكراني، بالإضافة إلى ٣٩ منظومة مضادة للجو من طرازات "إس-٣٠٠" و"بوك إم-١" و"أوسا"، إلى جانب إلى ٥٢ محطة رادار.وتم تدمير ٢٠٧ طائرات بدون طيار و١٤٦٧ دبابة و ١٤٨ قاذفة صواريخ متعددة.انظر : https://al-ain.com/article/russian-ukrainian-war-in-numbers

(٤) ازداد عدد النطاقات المسجلة بالكلمتين الرنيسيتين ' COVID' أو' corona' من أجل استغلال تزايد عدد الأشخاص الباحثين عن معلومات عن كوفيد - ١٩ . ويُعتبر الكثير من هذه النطاقات مستحدثا لتحقيق مآرب خبيثة. فنقلا عن Alto Palo Networks ،اكتشف في نهاية شهر آذار/مارس ٢٠٢٠ نطاقا خبيثا و٢٦١ ٤٠ نطاقا شديد الخطورة مسجلة حديثا.انظر: التهديدات السيبرانية المرتبطة بكوفيد - ١٩ في العالم ، الانتربول ، نيسان/أبريل ٢٠٢٠ ، ص ٢ .

https://www.interpol.int/ar/4/6/19

لتزايد عدد مستخدمى الانترنت حيث بلغ ٤.٩ مليارمشترك بنسبة ٦٣% من سكان العالم، وبحلول عام ٢٠٢٢، سيتم توصيل ما يقدر بنحو ٢٨.٥ مليار جهاز بالإنترنت.[١] ولذلك يجب تعزيز ثقافة المساءلة والالتزام بالمعايير والقواعد والمبادئ الناشئة بشأن السلوك المسؤول في الفضاء السيبراني.

ولقد كشفت الجرائم السيبرانية خاصة المتعلقة بالإرهاب والحروب و التجسس السيبراني [٢] وسرقة الأموال العامة والخاصة ، وتدمير القيم والمبادئ التى تحكم سلوك الأفراد فى المجتمعات المختلفة عن مدى خطورتها على الأمن المجتمعى للدول. فظهر الاهتمام بالأساليب والآليات التقنية والبشرية اللازمة لمواجهة هذا النوع من الجرائم التى تهدد الأمن القومى للدول سواء على مستوى المنظمات الدولية الحكومية[٣] وغير الحكومية، وعلى مستوى الهيئات المعنية داخل الدول[٤] من أجل حماية الأمن السيبرانى ومن ثم حماية الأمن المجتمعى، والحفاظ على التقدم والاستقرار للدول ، وحفظ السلم والأمن الدوليين.

ولقد شهد العقد الأخير تطورات مهمة على صعيد إصدار الصكوك الدولية والإقليمية الملزمة وغير الملزمة الرامية إلى التصدّي للجرائم السيبرانية. وتشمل مجلس أوروبا أو الاتحاد الأوروبي، وكومنولث الدول المستقلة أو منظمة شنغهاي للتعاون، والمنظمات الأفريقية الحكومية الدولية، وجامعة الدول العربية، والأمم المتحدة.[٥]

ونحاول في هذه الدراسة أن نقف على ماهية الأمن السيبرانى والجرائم السيبرانية وعلاقاتها بالأمن المجتمعى والأسس القانونية التى تحكمها وآليات حماية الأمن المجتمعى من الجرائم السيبرانية والتى تشكل خطورة على الدول والسلم والأمن الدوليين.

المشكلة

لا شك أن التطورات العلمية وما أفرزته من تقدم فى مجال الاتصالات ووسائل التواصل الاجتماعى كان لها آثارها السياسية والاقتصادية والاجتماعية على المجتمعات والدول، ورغم أهمية هذا التطور إلا أنه سلاح ذو حدين فيه الخير للبشرية، وأيضاً يحمل

---

(١) دعوة أممية إلى البقاء يقظين حيال التكنولوجيات الخبيثة التي يمكن أن تعرض الأجيال القادمة للخطر، الامم المتحدة ، ٢٩ حزيران/يونيه ٢٠٢١ - السلم والأمن ، انظر :https://news.un.org/ar/story/2021/06/1078872

(٢) الهيئة العامة للاستعلامات المصرية :الأمن السيبرانى .. بيئة تكنولوجية أكثر أمناً -الإثنين، ٢٦ فبراير ٢٠١٨ - ١٢:١٠ م انظر : https://sis.gov.eg/Story/159921?lang=ar

(٣) قرار الجمعية العامة في الدورة ٥٥/٢٨ في ديسمبر ٢٠٠٠، والدورة ٥٦/١٩ في ١٩ من ديسمبر ٢٠٠١ بشأن إرساء الأساس القانوني لمكافحة إساءة استعمال تكنولوجيا الاتصال والمعلومات في أعمال إجرامية. وجاءت القرارات في الدورة ٥٣/٧٠ في ٤ من ديسمبر ١٩٩٨ وفي الدورة ٥٤/٤٩ في الاول من ديسمبر ١٩٩٩، والدورة ٥٥/٢٨ في ٢٠ من نوفمبر ٢٠٠٠، والدورة ٥٦/١٩ في ٢٩ من نوفمبر ٢٠٠١، والدورة ٥٧/٥٣ في ٢٢ من نوفمبر ٢٠٠٢ بشأن التطورات الحادثة والمتوقعة في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. بالإضافة إلى كل من: قرار الجمعية العامة للأمم المتحدة في الدورة ٥٧/٢٣٩ في ٢٠ من ديسمبر ٢٠٠٢ بشأن إرساء ثقافة عالمية لأمن الفضاء الإلكتروني، ٥٥/٧٣ في ٤ من ديسمبر ٢٠٠٠، ٥٦/١٢١ في ١٩ من ديسمبر ٢٠٠١، الدورة ٥٨/١٩٩ في ٢٣ من ديسمبر ٢٠٠٣.

(٤) جمهورية مصر العربية ، رئاسة مجلس الوزراء - المجلس الأعلى للأمن السيبراني ، https://escc.gov.eg/index.html

(٥) فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية ، فيينا، ٢٥ -٢٨ شباط/فبراير ٢٠١٣. UNODC/CCPCJ/EG.4/2013/2

الشر فى جوانب أخرى إذا استخدم لتهديد الأمن المجتمعى ونشر الفوضى والتأثير على السياسات المختلفة التى تتخذها الدول بقصد تحقيق التنمية والأمن لشعوبها خاصة فى الدول النامية.

فرضيات البحث

١. تخلف بعض الدول فى مجال تكنولوجيا الاتصالات والانترنت.
٢. عدم وجود التشريعات الفاعلة التى تعمل على الاستفادة من الانترنت وفى نفس الوقت تواجه الجرائم التى قد ترتكب سواء من الأفراد أو الجماعات أو الدول .
٣. عدم تحقيق التعاون الكافى على المستوى الدولى لمواجهة الجرائم السبيرانية .
٤. غياب الكوادر الفنية اللازمة لمواجهة الجرائم السبيرانية التى قد تهدد الأمن المجتمعى للدول .

١. الصراعات العسكرية وغير العسكرية بين الدول واستخدام الجرائم السبيرانية فى هذه الصراعات لسيطرة بعض الدول على الأخرى.
٢. غياب الاستقرار السياسى والاقتصادى قد يدفع بعض الأفراد والجماعات داخل الدولة لاستغلال هذا المناخ لارتكاب الجرائم السبيرانية لاشباع رغباتهم الاقتصادية أو السياسية على حساب الأمن المجتمعى.

الهدف من البحث

دراسة الهيكل القانوني الدولى والمحلى، وتعمل هذه الدراسة على أهمية الاستفادة بوسائل التواصل الاجتماعى بما يخدم الأمن المجتمعى بمفهومه الشامل الاقتصادى والسياسى والاجتماعى والثقافى وفى نفس الوقت مواجهة الجرائم السبيرانية أياً كان نوعها ومصدرها سواء كان ذلك من مخاطر داخلية أو خارجية لتحقيق الأمن المجتمعى واستقرار المجتمع وتقدمه.

المنهج المستخدم

المنهج التحليلى الوصفي لتحليل مختلف القوانين الدولية والمحلية والتشريعات الصادرة المعنية بالجرائم السيبرانية و الحفاظ على الأمن المجتمعى. على أمل التوصل إلى إدخال تحسينات على التشريعات الحالية لتعزيز الأمن المجتمعى بجانب تحقيق التوازن بين الأمن المجتمعى، و الاستفادة من التطورات التكنولوجية.

الخطة

المبحث الأول : ماهية الأمن المجتمعى والجرائم السبيرانية.
المطلب الأول: ماهية الأمن المجتمعى.
المطلب الثانى: ماهية الجرائم السبيرانية.
المبحث الثانى :الأساس القانونى للأمن المجتمعى وعلاقته بالأمن السيبرانى .
المطلب الأول:الأساس القانونى الدولى للأمن المجتمعى وعلاقته بالأمن السيبرانى .
المطلب الثانى : الأساس القانونى الوطنى للأمن المجتمعى وعلاقته بالأمن السيبرانى .
المبحث الثالث :آليات تفعيل الحماية للأمن المجتمعى فى مواجهة الجرائم السيبرانية دولياً ومحلياً.
المطلب الأول : الآليات الوقائية لحماية الأمن المجتمعى فى مواجهة الجرائم السيبرانية .
المطلب الثانى : الآليات العلاجية لحماية الأمن المجتمعى فى مواجهة الجرائم السيبرانية .
وأخيراً :النتائج والتوصيات

المبحث الأول : ماهية الأمن المجتمعى والجرائم السبيرانية

تمهيد:

من المخاطر الحديثة التى تهدد الأمن المجتمعى هى تلك الجرائم التى ترتكب عبر شبكة الانترنت وتهديد الأمن السبيرانى من خلال إلقاء الرعب والفزع لدى الأفراد والجماعات بالتهديد فى أموالهم وأنفسهم وسمعتهم بطريقة مباشرة أو غير مباشرة ، ولذا عملت الدول جاهدة من خلال إصدار التشريعات الداخلية والمشاركة فى عقد الاتفاقيات الدولية التى تعمل على حمايتها من المخاطر السيبرانية التى تهدد الأمن المجتمعى لها [١].

وتوكد المادة الأولى من الميثاق العالمى للطبيعة الصادر من الجمعية العامة للأمم المتحدة ١٩٨٢ على أن " للإنسان حقاً أساسياً فى الحرية والمساواه فى ظروف معيشية مُرضيه وفى بيئة تسمح له بالحياة الكريمة والرفاهية ، وعلى الانسان واجب مقدس فى حماية وتحسين البيئة للأجيال الحاضرة والمستقبلية ".[٢]

ويعتبر عام ٢٠١٨ عام الاختراقات الأمنية حيث شهد العالم خلاله ارتفاعاً كبيراً فى عملية إختراق أنظمة الأمن الالكترونية وتسريب البيانات الخاصة لملايين المستخدمين ، وهذا الوضع أدى الى ارتفاع أسعار التأمين السيبرانى لقلة عدد الشركات العاملة فى هذا المجال ،ولعدم اليقين فى تقدير الخسائر التى تحدثها الجرائم السيبرانية [٣]؛ وفى ضوء ما سبق فإننا سنتصدى لهذا المبحث من خلال المطلبين التاليين :-

المطلب الأول : ماهية الأمن المجتمعى .

المطلب الثانى: ماهية الجرائم السيبرانية.

المطلب الأول : ماهية الأمن المجتمعى

فى عصرنا الحالى بات الأمن المجتمعى من أكثر الأمور أهمية بالنسبة للشعوب والحكومات خاصة فى كل التغيرات والتطورات المتسارعة والانفتاح الكبير على الدول الأخرى ، وهو ما أدى الى تهديد الأمن المجتمعى خاصة فى الصراعات المسلحة الدولية وغير ذات الطابع الدولى وفى أوقات السلم من خلال الغزو الثقافى وتهديد مؤسسات الدول من خلال استخدام وسائل التواصل الاجتماعى على شبكات الانترنت ، وهو ما يعرف بالجرائم السيبرانية .

و يعد الأمن المجتمعى ضمانة أساسية للاستقرار البشرى حتى يتسنى له ممارسة نشاطهم الانسانى فى جو من الأمن والطمأنينة والاستقرار ، ولذا أخذ الله تعالى على الانسان العهد بعدم الافساد فى الأرض وفى ذلك يقول الله تعالى " ثُمَّ أَنتُمْ هَؤُلَاءِ تَقْتُلُونَ أَنفُسَكُمْ وَتُخْرِجُونَ فَرِيقًا مِّنكُم مِّن دِيَارِهِمْ تَظَاهَرُونَ عَلَيْهِم بِالْإِثْمِ وَالْعُدْوَانِ..." [٤]، ولقد كشفت التطورات التكنولوجية الحديثة مدى المخاطر التى تصيب البشر جراء الجرائم

---

(١) د./ محمد أحمد منتصر : جريمة التهديد بالقتل عبر شبكة الانترنت ، مصر المعاصرة ، ع ٥١٨. ، ابريل ٢٠١٥ ، ص٩٢ .

(٢) الميثاق العلمى للطبيعة الصادر من الجمعية العامة للأمم المتحدة عام ١٩٨٢ .

(٣) نشرة الاتحاد المصرى للتأمين والهجمات الالكترونية (السيبرانية) والتأمين ، عدد أسبوعى رقم ٦٧ لعم ٢٠١٧ .

(٤) سورة البقرة ، الآية ٨٥ .

السيبرانية ([١]) ، وأثرها على الأمن المجتمعى الذى آثار الفقه فى الكثير من العلوم والاختصاصات المختلفة ، وحاول الجميع وضع تعريف للأمن المجتمعى على النحو الأتى :

يرى إتجاه أن المقصود بالأمن المجتمعى اصطلاحا هو " عدم توقع مكروه فى الزمان الآنى" والمراد به هنا الحاضر والمستقبل .

ويرى اتجاه أن الأمن المجتمعى يعنى " وصف للسلوك أو التصرف نحو الأخرين ويعنى المواقف التى معها تأثير متبادل بين فرقاء تربطهم روابط وعلاقات معينه " . ويضيف هذا الاتجاه بأن مصطلح الأمن المجتمعى مركب تركيباً وصفياً ، وهو مصطلح معاصر وعرف بعدة تعريفات :

١. الطمأنينة التي تمنع الخوف والفزع عن الانسان فرداً أو جماعة فى سائر ميادين الحياة .
٢. والطمأنينة التي يشعر بها أفراد المجتمع الناتجة عن مساهمة مؤسسات التنمية والتنشئة الاجتماعية فى تفعيل جميع الاستراتيجيات والامكانيات والممارسات التى تحقق للفرد الشعور بعدم الخوف فى حاضره ومستقبله ، وتؤكده له الاعتراف بوجوده ومكانته فى المجتمع ومشاركته الايجابية .

وينتهى هذا الاتجاه الى أن الأمن المجتمعى يدور حول توفير حالة الأمن والاستقرار والطمأنينة فى المجتمع، وعدم القلق على مستقبله السياسى والاقتصادى والاجتماعى .([٢]) ([٢]).

ويقول إتجاه آخر بأن المفهوم العام للأمن المجتمعى يشمل الاكتفاء المعيشى والاقتصادى والاستقرار في الحياة للمواطن بحيث يشعر بأن له ركائز ثابتة فى مجتمعه تحفظ له وجوده وكيانه وتؤدى الى تعلقه بأرضه ووطنه ، ويعتبر الاستقرار فى حياة الفرد عامل ضرورى لحفظ توازنه العاطفى والنفسى ومن ثم تعلقه بجزوره العائلية والثقافية والعقائدية والوطنية .([٣])

وفى ضوء ما سبق من تعريفات للأمن المجتمعى فإننا نرى أن الامن المجتمعى يعنى توفير حالة من الأمن والاستقرار لجميع أفراد المجتمع أياً كانت إنتمائتهم السياسية أو العقائدية أو العرقية على المستوى السياسى أو الاقتصادى أو الاجتماعى وتحقيق اهداف الجميع سواءعلى المستوى الشخصى أو الجماعى فى الحاضر والمستقبل.

وفى عصرنا الحالى بات الأمن المجتمعى من أكثر الأمور أهمية بالنسبة للشعوب والحكومات خاصة فى ظل التغيرات والتطورات المتسارعة والانفتاح الكبير على الدول الأخرى ، والتقدم الهائل فى مجال تكنولوجيا الاتصالات ، وأثر ذلك على الدول سواء فى وقت السلم أو الحرب ، وعمليات الغزو الثقافى ، وتدمير البنية التحتية

([١]) د./ عبد الوهاب بن رجب هاشم : جرائم البيئة وسبل المواجهة ، مركز البحوث والدراسات بجامعة نايف العربية للعلوم الأمنية ، الرياض ، ٢٠٠٦ مـ -١٤٢٧ هـ، ص١٦ .

([٢]) د./ عبدالله محمد الربايعه : السياسة الشرعية وأهميتها فى تحقيق الأمن المجتمعى ، المجلة العربية للدراسات الأمنية والتدريب ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، المجلد رقم ٣٠ ، ع. ٥٩ ، جمادى الأول لعام ١٤٣٥ هـ، ص١٠.

([٣]) المرجع السابق ، ص ١٢ .

للشعوب باستخدام شبكات الانترنت أو ما يطلق عليه بالجرائم السيبرانية ، والتى أدت الى تفكك الدول وانهيارها خاصة فى الآونة الأخيرة ، وهو ما سنتناوله فى المطلب الثانى .

المطلب الثانى : ماهية الجرائم السيبرانية.

تمهيد :

تكمن أهمية الأمن السيبرانى كقضية ناشئة فى حقل العلاقات الدولية من خلال حداثة هذا المجال ، فهناك تاريخ طويل من التخمينات حول دور التكنولوجيا الرقمية فى الدراسات الأمنية والتى يعود منشأها الى Arqulla and Ronfeldlrs 1993 من خلال حرب الانترنت والحرب السيبرانية، وقد كان هناك تاريخ واسع من الاختبارات النظرية والأخلاقية بشأن المخاوف المتعلقة بالأمن السيبرانى .

ومع نهاية الحرب الباردة حدثت تحولات تدريجية ظهرت على مستوى التفكير فى الدراسات الأمنية خاصة ما يتعلق بالأمن السيبرانى ، وهو ما تجلى فى أعمال مدرسة كوبن هجن وروادها أمثال " بارى بوزان" و"أولى ويفير" حيث اكتسبت أعمالهما أهمية كبرى خاصة عند التفكير فى الأمن السيبرانى لأن تركيزهما لم يكن على محاولة موضوعية بتصنيف ماهو تهديد أو ماهى الثغرة الأمنية المترتبة على الجرائم السيبرانية ،ولذا كانت هناك حاجة لتحديد ماهية هذه الجرائم حتى يمكن التعامل معها .([1])

ومن الاهمية بمكان قبل الخوض في تعريف الجرائم السيبرانية يجب تحديد ماهية الأمن السيبراني علي النحو التالي :-

الأمن السيبرانى وهو من المفاهيم والمصطلاحات التى تشكل تحدياً يواجه الباحثين والدارسين فى مختلف التخصصات لما يطرحه من إشكاليات تجعل من الصعوبة بمكان الإتفاق على تعريفات واضحة وشاملة بين أعضاء المجتمع العلمى ، ويعد الأمن السيبرانى واحداً من المفاهيم المعقدة خاصة حال محاولة الربط بينها وبين الأمن المجتمعى .([2])

وهناك العديد من التعاريف التى قدمت لمفهوم الأمن السيبرانى **حيث عرفه اتجاه** بأنه " مجموعة من الاجراءات المتخذة فى مجال الدفاع ضد الهجمات السيبرانية ونتائجها التى تشمل تنفيذ التدابير المضادة المطلوبة ".

ويقول إتجاه أن الأمن السيبرانى" عبارة عن مجموعة من الاجراءات التى إتخذت فى الدفاع ضد هجامات قراصنة الكمبيوتر وعواقبها ، ويتضمن تنفيذ التدابير المضادة المطلوبة ".

ويقول إدوار أمورسونAmoroso Edward بأن الأمن السيبرانى هو إجراءات من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات وتشمل تلك الوسائل الأدوات المستخدمة فى مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة .

([1]) اللجنة الدولية للصليب الأحمر ، مقالة، ٢٥ فبراير ٢٠٢١ ، بعنوان " الحرب السيبرانية والقانون الدولى الانسانى "

(٢) اللجنة الدولية للصليب الأحمر، مقالة، بعنوان "الحرب السيبرانية والقانون الدولى الانسانى "، ٢٥ فبراير لعام ٢٠٢١.

ويقول إتجاه بأن الأمن السيبرانى " مجموعة من الاجراءات مثل تجميع وسائل وسياسات واجراءات أمنية ومبادئ توجيهيه ومقاربات لإدارة المخاطر وتدريبات وممارسات فعلية وتقنيات يمكن إستخدامها لحماية البنية السيبرانية وموجودات المؤسسات والمستخدمين .([1])

وتقول وزارة الدفاع الأمريكية بأن الأمن السيبرانى هو جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والالكترونية من مختلف الجرائم والتى تشمل الهجمات والتخريب والتجسس والحوادث التى تؤثر على الأمن القومى .

ويرى الاعلان الأوروبى للأمن السيبرانى أنه قدرة النظام المعلوماتى على مقاومة محاولات الاختراق التى تستهدف البيانات الالكترونية . ويميز الاعلان الأوروبى بين الأمن السيبرانى وأمن المعلومات حيث يرى أن الأمن السيبرانى له مفهوم أوسع من أمن المعلومات لأن أمن المعلومات يهتم بأمن المعلومات الفيزيائية والورقية بينما لا يهتم الأمن السيبرانى بذلك .

المفاهيم المرتبطة بالأمن السيبرانى:-

١. **الفضاء السيبرانى:** الذى عرفته الوكالة الفرنسية لأمن أنظمة الاعلام ANSSI - وهى وكالة حكومية مكلفة بالدفاع السيبرانى الفرنسى – بأنه فضاء التواصل المشكل من خلال الربط العالمى لمعدات المعالجة الآلية للمعطيات الرقمية فهو البيئة التفاعلية الحديثة والتى تشمل عناصر مادية وغير مادية مكونة من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات والمستخدمين سواء مستخدمين أو مشغلين.ويقول إتجاه أن الفضاء السيبرانى هو الذراع الرابعة للجيوش الحديثة والتى يمكنها حسم المعارك العسكرية .

٢. **الهجمات السيبرانية:** هى كل عمل يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومى أو سياسى من خلال إستغلال نقطة ضعف واهيه يمكن للمهاجم التلاعب بالنظام السيبرانى وتهديد الأمن المجتمعى .

٣. الردع السيبرانى :وهو مواجهة الهجمات السيبرانية تجاه الدول لحماية الأمن القومى من خلال منع الأعمال الضارة ضد الأصول الوطنية فى الفضاء ، والأصول التى تدعم العمليات الفضائية .

ومركز الردع السيبرانى يرتكز على ثلاث ركائز هى

أ. مصداقية الدفاع

ب. قدرة على الانتقام

ج. الرغبة فى الانتقام من مرتكبى الهجمات السيبرانية التى تؤثر على الأمن المجتمعى أياً كانت صوره .

---

(١)التقرير الصادر عن الاتحاد الدولى للاتصالات حول اتجاهات الاصلاح فى الاتصالات لعام ٢٠٢١:٢٠١٠.

أبعاد الأمن السيبرانى وفق تطبيقات الاعلام الأمنى ([1])

يعتمد الأمن السيبراني على أجهزة وشبكات يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتاف قد يحدث، وقد يعتمد الأمن السيبراني على مجموعة أبعاد تتمثل في التالى :

١- الأبعاد العسكرية :تتمثل في قدرتها على ربط الوحدات العسكرية ببعضها بما يسمح بسهولة تبادل المعلومات والسرعة في اتخاذ القرارات العسكرية وتدمير الأهداف عن بُعد، وفى المقابل يمكن تعطيل قدرة الدولة، وقطع أنظمة الاتصال بين الوحدات العسكرية وقيادتها وتعطيل شبكات الإنترنت، وفى مجال التطبيقات العسكرية استطاعت إسرائيل انتاج طائرة Harpy، والتي اقتربت إلى حد كبير من التخلي عن التدخل البشري، حيث يُترك للطائرة تحديد الأهداف ومهاجمتها، وقد صُممت الطائرة لتدمير الدفاعات الجوية بشكل انتحاري.

٢- الأبعاد الاقتصادية :يرتبط الأمن السيبراني ارتباطاً وثيقاً بالاقتصاد القومي، حيث تتنافس الشركات على إصدار تطبيقات تسمح بآليات دفع آمنة، ووضعت بعض الدول تشريعات خاصة بحماية أموالها والحد من بعض الجرائم الاقتصادية العابرة للحدود مثل الإرهاب الإلكتروني، وغسيل الأموال، والتجارة بالبشر وغيرها.

٣- الأبعاد الاجتماعية :حيث تُسهم وسائل الاعلام وشبكات التواصل الاجتماعي في فتح المجال للأفراد للتعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية بأشكال مختلفة، وتبادل الخبرات والأفكار وتكوين الصداقات بين أفراد المجتمعات الأخرى.

٤- الأبعاد السياسية : وتعنى حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية، حيث أصبح بإمكان الفرد المشاركة في صناعة القرار السياسي، والاطاع على خلفيات ومبررات القرارات السياسية التي تتخذها حكومته عبر الكم الهائل من المعلومات التي يمكنه الوصول إليها.

٥- الأبعاد القانونية :تُعد العلاقة بين القانون والتكنولوجيا علاقة تبادلية، فالتطورات الحديثة تفرض وضع أطر وتشريعات للأعمال غير القانونية حيث تفتقد الجريمة الالكترونية للأطر القانونية، ويعود ذلك إلى طبيعة الجريمة الإلكترونية في حد ذاتها، وصعوبة تحديد هوية مرتكبي تلك الجرائم، إلى جانب ذلك فإن الجرائم عبر الانترنت غير مقيدة بحدود الدول، الأمر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافحتها.

ومما سبق كان هناك محاولات عدة لوضع تعريف للجرائم السيبرانية على النحو الآتى :

يرى إتجاه أن الجريمة السيبرانية تتوقف على الغرض من استخدامها حيث أن الجريمة السيبرانية الحالية تتمثل فى عدد محدود من الأعمال التى تمس سرية البيانات أو النظم الحاسوبية وسلاماتها أو إحداث أضرار لمحتوى الحواسب .

---

(١) د./ مجدي الداغر: اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وانعكاساته على دعم وتعزيز الأمن السيبرانى في مصر، (دراسة ميدانية) ، المجلة العربية لبحوث الاعلام والاتصال - العدد ٣٣ ابريل/ يونيو٢٠٢١ ، ص ٣٧ .

ويرى اتجاه ثانى :أن الجريمة السيبرانية لا تتسم بنفس القدر من الأهمية فيما يخص الأغراض الأخرى كتحديد صلاحيات الهيئات المختصة بالتحريات والتعاون الدولى حيث يفضل التركيز على الأدلة الالكترونية فيما يخص أى جريمة بدلا من التركيز على تركيبة واسعة واصطناعية للجريمة السيبرانية .([١])

ويرى اتجاه ثالث: أن الجريمة السيبرانية هى مجموعة الأفعال غير القانونية التى تتم عبر معدات أو أجهزة إلالكترونية أو شبكة الانترنت أو تبث عبرها محتويات وتتطلب الالمام بمقتضيات الحاسب الألى ونظم المعلومات مما يترتب عليها مقاضات فاعلها.

ويرى إتجاه أخر: أن الجريمة السيبرانية هى كل فعل ضار بالآخرين عبر استعمال الوسائط الالكترونية مثل الحواسب، أجهزة المحمول، شبكات الاتصال الهاتفية ، شبكات نقل المعلومات، والاستخدامات غير القانونية للبيانات الحاسوبية أو الالكترونية عموماً.([٢])

والمادة الثانية من اتفاقية منظمة شنغهاي للتعاون، تنص بأن الجريمة السيبرانية باعتبارها" تهديدا كبيرا "لأمن المعلومات على الصعيد الدولي .كما عرف ملحق الاتفاقية الجريمة السيبرانية بأنها" استعمال موارد المعلومات في أغراض غير مشروعة و(أو) تأثير ذلك عليها في الفضاء المعلوماتي".

وفى ضوء ما سبق من تعريفات للجريمة السيبرانية فإننا نرى أن الجريمة السيبرانية هى كل فعل ضار بالآخرين عبر استخدام الفضاء الالكترونى أياً كانت الوسيلة المستخدمة بالمخالفة للقواعد القانونية الذى تحكم استخدام هذه الوسائل الالكترونية ولها آثار مباشرة أو غير مباشرة على الأمن المجتمعى.

أنواع الجرائم السيبرانية :

١. الوصول للبيانات بشكل غير قانونى والاطلاع عليها أو التلاعب فيها .
٢. استخدام الحواسب وشبكة الانترنت للتخطيط لجريمة كالسرقة أو الاختلاس وتزوير المستندات واستغلال الأطفال والفتيات .
٣. تدمير المواقع الالكترونية أو إيقافها وسرقتها والتشهير وتشويه السمعة وتزوير التوقيع الالكترونى .
٤. إختلاس أموال البنوك والوسائط والمستندات المالية وكلها تؤثر بشكل مباشر أو غير مباشر على الأمن المجتمعى وحياة الأفراد.

الجهات الاقتصادية الأكثر تعرضاً للجرائم السيبرانية

١- البنوك .
٢- المراكز الطبية .
٣- قطاع التأمين .

وذلك لأن الجرائم السيبرانية والهجمات الالكترونية تتطور بسرعه بسبب التحول الرقمي المتنامي واستخدام الانترنت علي نطاق واسع ، وبالتالي الخسائر الناجمه عن هذه

([١]) المرجع السابق .

([٢]) نشرة الاتحاد المصرى للتأمين : الهجمات الالكترونية (السيبرانية) والتأمين ، عدد إسبوعى ، رقم ٦٧ ، ٢٠١٧-٢٠٢١ .

الجرائم تتزايد سواء من الناحية المالية أو المادية للهيئات الاقتصادية العامه أو الافراد علي حد سواء ، وبالتالي تؤثر علي الامن المجتمعي بصفة مباشرة أو غير مباشرة .
وفى ضوء تحقق ماهية الأمن المجتمعى والجرائم السيبرانية فإننا سنتناول فى المبحث التالى : الأساس القانونى للجرائم السيبرانية وعلاقتها بالأمن المجتمعى .

المبحث الثانى : الأسس القانونية الدولية والوطنية للجرائم السيبرانية وعلاقاتها بالأمن المجتمعى

تمهيد:-

شهدت مرات عدة زيادة هائلة فى جرائم الانترنت على المستوى الدولى نتيجة لتحولات الاقتصادية والديموغرافية حيث لاحظ العاملون فى مجال انفاذ القانون ارتفاع مستوى الجرائم السيبرانية وأثر ذلك على الأمن المجتمعى حيث يستغل الأفراد والجماعات الاجرامية المنظمة الفرص الجديدة المتاحة لإرتكاب الجرائم السيبرانية لتحقيق الأرباح حيث تشير التقديرات أن أكثر من ٨٠% من الجرائم السيبرانية هو شكل من أشكال النشاط الإجرامى المنظم.

حيث تقوم الأسواق السوداء للجرائم السيبرانية بإعداد البرمجيات الخبيثة والفيروسات وبيع البيانات . وكان لهذه الاحصاءات فى مجال الجرائم السيبرانية أهميتها لوضع السياسات على المستوى الوطنى لمواجهة هذه الجرائم التي تؤثر بالسلب على الأمن المجتمعى .(١)

التركيز الموضوعي لصكوك الجريمة السيبرانية

وفى ضوء ما سبق إتخذت الدول والمنظمات الدولية التشريعات والاتفاقيات الدولية التى من شأنها مواجهة الجرائم السيبرانية وحماية الأمن المجتمعى للدول وهو ماسنحاول عرضه على النحو التالى :-

المطلب الأول : الأسس القانونية الدولية للأمن المجتمعى وعلاقته بالأمن السيبرانى

المطلب الثانى : الأسس القانونية الوطنية للأمن المجتمعى وعلاقته بالأمن السيبرانى

---

(1) UNODC/CCPCJ/EG4/2013/23Jauary,2013

المطلب الأول: الأسس القانونية الدولية للأمن المجتمعى وعلاقته بالأمن السيبرانى
أولاً: جهود الجمعية العامة فى مجال مكافحة الجرائم السيبرانية

طلبت الجمعية العامة فى قرارها٢٣٠/٦٥ الى لجنة منع الجريمة والعدالة الجنائية أن تنشأ وفقاً للفقرة ٤٢ من إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية من أجل إجراء دراسة شاملة لمشكلة الجريمة السيبرانية ، والتدابير التى تتخذها الدول الأعضاء والمجتمع الدولى والقطاع الخاص لتبادل المعلومات عن التشريعات الوطنية وأفضل ممارسات والمساعدة التقنية والتعاون الدولى بغية دراسة الاختيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطنى والدولى للتصدى للجرائم السيبرانية ، وإقتراح تدابير جديدة ، وعلاوة على ذلك أحاطت الجمعية العامة علماً مع التقرير فى قرارها ١٨٩/٦٧ الخاص بفريق الخبراء الحكومى الدولى المفتوح العضوية المعنى باجراء دراسة شاملة عن مشكلة الجرائم السيبرانية وأثرها على الأمن المجتمعى .

كما عقدت الدورة الأولى لفريق الخبراء فى فينا خلال الفترة من ١٧-٢١ يناير ٢٠١١ وقام الفريق خلال هذه الدورة بتوزيع استبيان على الدول الأعضاء والمنظمات الحكومية الدولية وممثلى القطاع الخاص والمؤسسات الأكادمية وأظهر الاستبيان أن ماهية الجريمة السيبرانية يتوقف على الغرض من إرتكابها وما يترتب على ذلك من أعمال تمس سرية البيانات والنظم وسلامة الحواسب والسعى نحو تحقيق مكاسب شخصية أو مالية أو إحداث أضرار بالبيانات والأجهزة المعنية . ([1])

وأظهرت الدراسات التباين بين الدول فى مجال مكافحة الجرائم السيبرانية حيث أن الدول الأوروبية توجد بها تشريعات بلغت أكثر من ثلثي الدول ، وتعد كافية لمواجهة الجرائم السيبرانية فى حين أن الأمر مختلف فى الدول النامية بأفريقيا وأمريكا اللاتينية وأسيا حيث يرى الباحثين أن أكثر من ثلثي تشريعاتها غير كافية لمواجهة الجرائم السيبرانية ومن ثم حماية الأمن المجتمعى ، وهى فى حاجة لمزيد من التشريعات .

ثانياً : الجهود الاقليمية فى مجال إصدار الاتفاقيات المتعلقة بالجرائم السيبرانية

شهد العالم فى الآونة الأخيرة على المستوى الاقليمى إصدار العديد من الاتفاقيات الاقليمية الملزمة وغير الملزمة التى تتصدى للجرائم السيبرانية فى إطار التجمعات الأتية:([2])

١. مجلس الاتحاد الأوروبى .
٢. دول الكومنولث المستقلة أو منظمة شنغهاى.
٣. المنظمات الحكومية الأفريقية الدولية .
٤. الجامعة العربية .

ويعمل القانون الدولى لحقوق الانسان بمثابة سيف ودرع على حد سواء، إذ أنه يقضى بتجريم أشكال وتصرفات معينة ويحمى أشكال وتصرفات أخرى ، ولذا على

([1]) UNODC/CCPCJ/EG4/2013/23Jauary,2013,p.2.
([2]) UNODC/CCPCJ/EG4/2013/23Jauary,2013,p3.

الدول أن تنظم هذه الأمور من خلال تشريعات تنظم حرية التعبير وتمنع التحريض على الابادة الجماعية والكراهية والتمييز والارهاب والعمل على إحترام ثقافة الشعوب والتقاليد والعادات السائدة التى تنظمها الشرائع السماوية .

وعلى الدول وضع القواعد الاجرائية التى تحكم عمليات جمع الأدلة الالكترونية ذات الصلة بالجرائم السيبرانية والتى قد تؤدى الى براءة الفرد الذى يحاكم أو إدانته من خلال محاكمة قانونية تأخذ فى الاعتبار مصداقية الأدلة الالكترونية التى تكون مخزنة فى الأجهزة الالكترونية وملحقاتها وهى أدلة تتسم بسرعة الزوال وسهولة التلاعب بها من قبل المتهمين ؛ والأمر يحتاج الى محققين مدربين لديهم القدرة على تحميل وتحليل البيانات الالكترونية لحماية الأمن المجتمعى ضد الجرائم السيبرانية .

وينشأ البعد الدولى للجرائم السيبرانية عندما يكون للجريمة المعنية عنصر أو أخر مهم فى إقليم دولة أخرى أو يكون أحد جوانب تنفيذ الجريمة قد تم فى إقليم أخر ، وينص القانون الدولى على عدد من الأسس المتعلقة بالولاية القضائية بأن الأفعال المعنية لما فى ذلك الولايات القضائية التى تستند الى الاقليم أو الجنسية التى يحملها المتهم ، وهذا يستلزم بعض صور التعاون الدولى .

ويشمل صور التعاون الدولى فى مجال الجرائم السيبرانية لحماية الأمن المجتمعى ؛-

١. تسليم المطلوبين .
٢. تبادل المساعدات القانونية.
٣. الاعتراف المتبادل بالأحكام الأجنبية والتعاون بين أجهزة الشرطة .

ونظراً لطبيعة الأدلة الالكترونية التى يسهل زوالها والتلاعب فيها يتطلب ذلك التعاون الفعال وإتخاذ الاجراءات فى أسرع وقت ممكن ، وتوضح الاحصاءات الدولية أن أكثر من ٧٠% من الدول طلبت المساعدة القانونية المتبادلة ، وطلبت تعاون فى مجال الأدلة الجنائية بين الدول الأفريقية وأمريكا وأوروبا نحو ٦٠% فى مجال الجرائم السيبرانية.

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

وتنفيذاً لما سبق نصت المادة ٢٢ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن الدول الأطراف تلتزم بأن يتبنى قانونها الداخلى الاجراءات الضرورية لتحديد الصلاحيات والاجراءات التى تشجع على التعاون فى مجال الجرائم السيبرانية لحماية الأمن المجتمعى ، ونصت المادة ٢٦ على أن كل دولة إفريقية عليها إتخاذ الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش على تقنية المعلومات أو جزء منها والمعلومات المخزنة بالأجهزة ، ونصت المادة ٣١ على تبادل المجرمين بين الدول الأطراف فى الاتفاقية العربية ، ويقدم الطلب فى هذا الصدد كتابتاً ويجوز أن يقدم بشكل عاجل .([1])

([1]) الاتفاقية العربية لمكافحة تقنية المعلومات ، الصادر فى ٢٠١٠/١٢/٢١ .

الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية

ويعد الاتحاد الأوروبى من أوائل التنظيمات الإقليمية التى تعاملت مع الجرائم السيبرانية وذلك للأضرار الاجتماعية والاقتصادية التى أصابت الأفراد والهيئات سواء الحكومية وغير الحكومية نتيجة لعدم الوعى بالإذاء الناجم عن هذه الجرائم أو لشعور الضحايا بالخجل والارتباك وتخوف من الابلاغ عن بعض الجرائم السيبرانية . كما قد يترتب على ذلك من خسائر اقتصادية كما هو الحال فى الجرائم التى ترتكب فى مواجهة البنوك أو المؤسسات الاقتصادية خشية إهتزاز المراكز المالية لها ، ولكن مع تزايد هذه الجرائم والآثار الاقتصادية والاجتماعية الخطيرة التى تترتب عنها مما دفع الدول الأوروبية الى وضع المعاهدات الدولية والتشريعات الداخلية التى تستخدم لمعالجة حوادث معينه والقيام بتحقيقات تكتيكية على المدى المتوسط والبعيد من خلال التعاون بين الدول المختلفة خاصة فيما يتعلق بالجرائم السيبرانية العابرة للحدود.

وهو ما نصت عليه المادة ٢٣ من الاتفاقية الأوروبية المتعلقة بالجريمة الألكترونية لعام ٢٠٠١ والتى تلزم الدول بضرورة التعاون الدولى فى المسائل المتعلقة بالجرائم السيبرانية ، والمادة ٢٤ تتعلق بالتعاون فى مجال تسليم المجرمين ، والمساعدة المتبادلة ، والمادة ٢٨ نصت علي المعاملة بالمثل . كما حثت المادة الثانية الدول الأطراف القيام بوضع التشريعات الداخلية التى تجرم الأفعال المتعلقة بالجرائم السيبرانية خاصة ما يتعلق باتلاف بيانات الحاسوب أو حذفها أو تعديلها أو القيام بالتزوير أو نشر المواد الاباحية للأطفال والفتيات ([1]).

اتفاقية الاتحاد الأفريقى بشأن الفضاء الالكترونى وحماية البيانات ذات الطابع الشخصى

ولقد إسترشدت اتفاقية الاتحاد الأفريقى بشأن الفضاء الالكترونى وحماية البيانات ذات الطابع الشخصى بالقانون التأسيسى للاتحاد الأفريقى المعتمد عام ٢٠٠٠ والتى نصت فى ديباجتها أن الاتفاقية تأخذ فى الاعتبار الإطار القانونى للأمن فى الفضاء الالكترونى وحماية البيانات ذات الطابع الشخصى ، وتتكفل بالالتزامات الواقعة على الدول الأعضاء فى الاتحاذ الافريقى على المستويات الاقليمية الفرعية والاقليمية والعالمية لحماية المجتمع السيبرانى . مع الأخذ فى الاعتبار الحريات الأساسية وحقوق الانسان والشعوب الواردة فى الاعلانات والاتفاقيات المعتمدة فى إطار الاتحاد الأفريقى والأمم المتحدة .

وتشير الاتفاقية الى الاعلان الصادر عن الدورة الرابعة عشر لمؤتمر رؤساء دول وحكومات الاتحاد الأفريقى بشأن تكنولوجيا المعلومات والاتصالات فى أفريقيا " التحديات والأفاق المستقبلية للتنمية " ([2])

([1]) الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية الصادرة فى ٢٠٠١/١١/٢٣.

([2]) الاعلان الصادر عن الدورة الرابعة عشر لمؤتمر رؤساء دول وحكومات الاتحاد الافريقى بشأن تكنولوجيا المعلومات والاتصالات فى أفريقيا " التحديات والآفاق المستقبلية للتنمية " المنعقد فى أديس أبابا ، أثيوبيا ، فى الفترة من ٣١ يناير الى ٢ فبراير عام ٢٠١٠ .

وأخذت الاتفاقية في الاعتبار اعلان "اوليفر نامبو "الذي اعتمده مؤتمر الاتحاد الافريقي الاستثنائي للوزراء المسئوولين عن تكنولوجيا المعلومات والاتصالات والجرائم التي ترتكب والاثار الاقتصادية والسياسية والاجتماعية والامن المجتمعي للدول الافريقية وكيفية مواجهتها . ([1])

وفي ضوء ما سبق نصت الماده الثامنة من الاتفاقية الافريقية علي التزام الدول الاطراف بوضع اطار قانوني يهدف الي تعزيز الحقوق الاساسية والحريات العامه لا سيما حماية البيانات الالكترونية ، وقمع اي جريمة متعلقه بانتهاك الخصوصية والعقاب عليها . ويقع علي الدول الاطراف وفقا لهذه الاتفاقية واجب حماية البيانات السيبرانية دون تهديد الحريات العامه للمواطنين وحياتهم الخاصه . ([2])

المطلب الثاني: الاسس القانونية الوطنية للأمن المجتمعي وعلاقته بالأمن السيبراني

دفع الاستخدام المتزايد لوسائل التواصل الاجتماعي ، ومحتوي الانترنت الذي ينتجه الافراد بأنفسهم والحكومات الي اتخاذ تدابير تنظيمية من بينها اللجوء الي القانون الجنائي والدعوه الي احترام الحق في التعبير، وبعض الدول تضع قيود فيما يتعلق بالتشهير والاهانه والتهديد والتحريض علي الكراهية واهانة المشاعر الدينية، ونشر المواد التي تشيع الفاحشة وتقوض دور الدوله ومؤسساتها .

ومن اهم أنماط التهديدات السيبرانية التي تتعرض لها مصر بعد 2013 م كما تراها النخبة ([3])

التهديدات	النخبة الامنية		النخبة الاعلامية		النخبة الاكاديمية		الاجمالي	
	ك	%	ك	%	ك	%	ك	%
الارهاب الالكتروني	١٦	٦٦.٦	١٥	٤٢.٨	٢٢	٤٦.٨	٥٣	٥٠.٠
الجرائم الالكترونية	٥	٢٠.٨	١٢	٣٤.٤	١٤	٢٩.٧	٣١	٢٩.٣
الحروب الالكترونية	٣	١٢.٦	٨	٢٢.٨	١١	٥١.٥	٢٢	٢٠.٧
الاجمالي	٢٤	١٠٠	٣٥	١٠٠	٤٧	١٠٠	١٠٦	١٠٠

وتختلف المقتضيات القانونية الوطنية والسياسات المتبعه في القطاع الخاص بشأن الاحتفاظ بالبيانات وافشائها اختلافا كبيرا حسب النظام القانوني وتطوره خاصه في مجال استخدام البيانات علي الشبكه الالكترونية حيث بلغت بعض الدول الي مستوي متقدم من الاوامر القضائية التي تسمح بالحصول علي البيانات من مقدمى الخدمة وبيانات المشاركين المخزنة على الأجهزة الالكترونية بصورة يراعى فيها التوازن بين

([1]) إعلان أوليفرتامبو الذى اعتمده مؤتمر الاتحاد الأفريقى الاستثنائى للوزراء المسئولين عن تكنولوجيا المعلومات والاتصالات المنعقد فى جنوب أفريقيا بجوهانسبيرج فى ٥ فبراير عام ٢٠٠٩ . أنظر أيضاً : اعلان أبيدجان المعتمد فى ٢٢ فبرايرعام ٢٠١٢ وإعلان أديس أبابا المعتمد فى ٢٢ يونيو عام ٢٠١٢ حول مواءمة تشريعات الفضاء الالكترونى فى أفريقيا .

(٢) اتفاقية الاتحاد الأفريقى بشأن أمن الفضاء الالكترونى وحماية البيانات ذات الطابع الشخصى المعتمدة بمالابو" غنيا الاستوائية فى ٢٧ يونيو٢٠١٤ .

([3]) د./ مجدي الداغر: اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وانعكاساته على دعم وتعزيز الأمن السيبرانى في مصر، (دراسة ميدانية) ، مرجع سابق، ص ٤٩ .

الخصوصية ومراعاة الأصول القانونية بما يسهل عمليات التحقيق الفعال فى الجرائم السيبرانية لتحقيق الأمن المجتمعى وحماية الأمن القومى .

وفى ذلك يقول الأمين العام للأمم المتحدة السابق كوفى عنان بأنه ينبغى أن ينظر الى اسهام المجتمع المدنى فى مجال مكافحة الجرائم السيبرانية لا بوصفه محاولة لاغتصاب دور الحكومات بل كطريقة لإضافة نوعية وقيمة الى قرارات وقوانين الدول ، ومشاركة المجتمع المدنى ليست غاية فى حد ذاتها كما أنها ليست علاجاً لجميع المشاكل ولكنها ذات أهمية حيوية لتحقيق الأمن المجتمعى .([١])

ومن الملاحظ :-

١- ان الجرائم السيبرانية ليست هي السبب الوحيد الذي يتسبب في اتلاف وضياع البيانات الالكترونية او اتلافها لانه قد يكون وارد ذلك ارتفاع مبالغ فيه بالنسبه للطاقه التي تغذي الاجهزه او الكوارث الطبيعية التي تؤدي الي اتلاف الاجهزه والكابلات المغذية لهذه الاجهزة الالكترونية بشكل يؤثر علي أمن الافراد والامن المجتمعي سواء من الناحية الاقتصادية او السياسية او الاجتماعية .

٢- وكما يرتكب الافراد والجماعات المختلفه أفعال تؤثر على الأمن السيبرانى، وكذا الأمن المجتمعى بصوره المختلفة، فإن الدول أصبحت تستخدم الانترنت كوسيلة من وسائل الحرب الحديثة بقصد ضرب الأهداف الاقتصادية من خلال التأثير فى البنية الأساسية لقاعدة البيانات التى تنظم عمل المنشأت الاقتصادية والصناعية والخدمية للدول لإضعاف الروح المعنوية للشعوب من خلال ما يعرف بالحرب السيبرانية ، وهى إحدى صور الحرب الحديثة والتى تلعب دور كبير فى تهديد الأمن المجتمعى للدول حيث يقوم مرتكب هذه الجرائم بالعمل على إتلاف أو السيطرة على البيانات الالكترونية عبر الحدود الدولية باستهداف مواطن الضعف فى البنية التحتية الالكترونية لدول أخرى من خلال جهات حكومية أو غير حكومية بما يشكل تهديد للأمن القومى للدولة المستهدفة وبالتالي التأثير على الأمن المجتمعي.([٢])

والدستور المصري لعام ٢٠١٤ ([٣]) جعل حماية الفضاء المعلوماتى إلتزام على الدولة لما له من ضرورة لحماية الأمن القومى بصفة عامة والأمن المجتمعى بصفة خاصة ، وهى فى سبيل تحقيق هذه الغاية عليها مراعاة الاتي :-

١. الاجراءات التى من شأنها مواجهة مشكلات العصر بروح منفتحة ومؤثرة وفق منظومة شاملة تثبت دعائم الأمن والنظام لمواجهة الجرائم المعاصرة ، ومنها الجرائم المتعلقة بتطورات التكنولوجية خاصة الجرائم السيبرانية مع تحقيق الحماية لحقوق الانسان وفرض هيبة الدولة .
٢. مراعاة الأهم ثم المهم لأن الأمور التى تحقق المصالح للأمه ليس كلها على درجة واحدة والأصل تحقيقها كلها لتحقيق الأمن المجتمعى لجميع أفراد الدولة خاصة فى مجال الأمن السيبرانى .

([١]) كلمة الأمين العام كوفى عنان أمام مجلس الأمن التابع للأمم المتحدة بالجلسة ٢٢ يونيو ٢٠٠٤ .S/PV.4993

([٢]) تقرير سويس رى Swiss Re لعام ٢٠١٧ ، ص ص ٢٣:٢٢ .

([٣]) الدستور المصرى لعام ٢٠١٤ ، المادة ٣١ .

ونظراً لأهمية الأمن السيبرانى وأثره على الأمن المجتمعى فإن الدستور المصرى الصادر ٢٠١٤ فى المادة ٣١ منه نصت على أن "أمن الفضاء المعلوماتى جزء أساسي من منظومة الإقتصاد والأمن القومى وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذى ينظمه القانون ".

وفى ضوء هذه المادة تأسس المركز المصرى للاستجابة لطوارئ الانترنت والحاسب ، والمجلس الأعلى للأمن السيبرانى التابع لوزارة الاتصالات وتكنولوجيا المعلومات لجمهورية مصر العربية ، والمسئول عن أمن المعلومات وتوفير الدعم والدفاع والتحليل فى مجال الهجمات السيبرانية ، ويوفر المركز الانذار المبكر ضد انتشار البرمجيات الخبيثة والهجمات السيبرانية ضد البنية التحتية للاتصالات فى مصر .

وفي اطار دعم الامن القومي بصفة عامة والامن المجتمعي بصفة خاصة وتزايد التهديدات والتحديات المستقبلية في مجال الامن السيبراني ولرصد ومجابهة المخاطر والتهديدات المتزايده قام المجلس الاعلي للأمن السيبراني التابع لمجلس الوزراء برئاسة وزير الاتصالات بوضع الاستراتيجية الوطنية للأمن السيبراني ٢٠١٧: ٢٠٢١ ، وأصدر قانون مكافحة جرائم تقنية المعلومات المعروف بمكافحة الجرائم السيبرانية .([1])

ولقد صدر القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات ، وفي المادة ٣/٢ تنص علي أنه مع مراعاة الحياة الخاصة للأفراد التي يكفلها الدستور يلتزم مقدمو الخدمه والتابعون لهم أن يوفروا حال طلب جهات الامن القومي ، ووفقا لاحتياجاتها كافة الامكانيات الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها وفقا للقانون لتحقيق الامن المجتمعي .

وفي الماده ٤ تعمل السلطات المصرية علي التعاون مع الدول الاخري في اطار الاتفاقيات الدولية والاقليمية والثنائية تطبيقا لمبدأ المعاملة بالمثل بتبادل المعلومات لمواجهة الجرائم السيبرانية لحماية الامن المجتمعي .

وقرر القانون عقوبات جنائية كما هو الحال في المادة ١٧ والتي نصت علي يعاقب بالحبس مده لا تقل عن سنتين وبغرامة لا تقل عن مائة الف جنية ، ولا تجاوز خمسمائة الف جنية أو بإحدي هاتين العقوبتين كل من اتلف او عطل او عدل مسار او الغي كليا او جزئيا متعمدا وبدون وجه حق البرامج والبيانات او المعلومات المخزنة او المعالجة علي اي نظام معلوماتي ايا كانت الوسيلة المستخدمة في الجريمة . ([2])

ونصت الماده ٣٤ علي الظروف المشدده في الجرائم السيبرانية بأنه " اذا وقعت اي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الاخلال بالنظام العام او تعريض سلامة المجتمع وامنه للخطر او الاضرار بالامن القومي للبلاد او بمركزها الاقتصادي او منع او عرقلة ممارسة السلطات العامة لاعمالها او تعطيل احكام الدستور

---

(١) نشرة الاتحاد المصرى للتأمين : الهجمات الالكترونية (السيبرانية) والتأمين ، عدد إسبوعى ، رقم ٦٧ ، ٢٠١٧- ٢٠٢١ .

(٢) الجريدة الرسمية ، ع ٣٢ مكرر ج ، ١٤ أغسطس ٢٠١٨ ، ص١٥ .

او القوانين او اللوائح او الاضرار بالوحده الوطنية والسلام الاجتماعي تكون العقوبة السجن المشدد .([1])

وفي ضوء ما سبق يتضح لنا الجهود التشريعية علي المستوي الوطني لمواجهة الجرائم السيبرانية لحماية الامن المجتمعي للدول ، ومن ثم يلزم اجتهاد الدراسة لوضع الآليات اللازمة لمواجهة هذه الجرائم من خلال الاجراءات الوقائية والعلاجية لتحقيق الامن المجتمعي بصورة بفعالة علي النحو التالي .

المبحث الثالث: آليات تفعيل حماية الامن المجتمعي في مواجهة الجرائم السيبرانية الدولية والوطنية

بعد العرض السابق لتحديد ماهية الجرائم السيبرانية والأمن المجتمعى والأساس القانونى سواء على المستوى الداخلى أو الدولى فالمنطق يستلزم ضرورة البحث فى آليات مواجهة خطر الجرائم السيبرانية وذلك لتحقيق الأمن المجتمعى على النحو الآتى :-

المطلب الأول : الآليات الوقائية لحماية الأمن المجتمعى فى مواجهة الجرائم السيبرانية الدولية والوطنية المطلب الثانى: الآليات العلاجية لحماية الأمن المجتمعى فى مواجهة الجرائم السيبرانية الدولية والوطنية

المطلب الأول: الآليات الوقائية لحماية الأمن المجتمعى فى مواجهة الجرائم السيبرانية الدولية والوطنية

من المعلوم أن الوقاية خير من العلاج ، ولذا يجب الاهتمام بالاجراءات الوقائية لحماية الامن المجتمعي من الجرائم السيبرانية سواء علي المستوي الوطني او الدولي وهو ما نتناوله من خلال التالي :-

أولاً: الآليات الوقائية الوطنية لحماية الأمن المجتمعى فى مواجهة الجرائم السيبرانية .

يرى جانب من الفقه التركيز على الآليات الآتية :

١. برنامج لدعم البحث العلمى والتطوير وتنمية صناعة الأجهزة التى تعزز الأمن السيبرانى من خلال دعم برامج ومشروعات التعاون بين الجهات البحثية والشركات الوطنية خاصة فى مجال تحليل البرمجيات الحديثة المتقدمة ، ومجال تحليل الأدلة الرقمية وتأمين النظم والشبكات وحماية البنية التحتية لنظم الالكترونية .
٢. التوعية المجتمعية للفرص والمزايا التى تقدمها الخدمات الالكترونية للأفراد والمؤسسات والجهات الحكومية بأهمية الأمن السيبرانى لحمايتها من المخاطر التى تواجهها.
٣. مواجهة الأخطار المترتبة على الجرائم السيبرانية ، وتحقيق الشراكة المجتمعية والتي تشمل الجهات الحكومية والقطاع الخاص والمؤسسات البحثية والمجتمع المدنى لتعظيم الاستفادة وحماية الأمن المجتمعى .

([1]) الجريدة الرسمية ، ع ٣٢ مكرر ج ، مرجع سابق ، ص٢١ .

ولقد زخرت الدراسات فى السنوات الأخيرة بإجتهادات المفكريين والعلماء حول التنمية بمفهومها الحديث والمعاصر المرتبط بالانسان وتمكينه من حقوقة السياسية والاجتماعية والاقتصادية والثقافية ، وفقاً لما تقتضية فلسفة الحكم الرشيد ، ولأنها تشكل اهم الشروط لتنمية الدول وتحسين أوضاعها فى ظل التقدم التكنولوجى الهائل والذى كشف عن عدد هائل من الجرائم السيبرانية وأثرها على الأمن المجتمعى .([١])

وهذا الأمر فى حاجة ليس فقط لآصدار القواعد القانونية ، بل لتفعيل أحكامه لآنه لاقيمة للقانون مالم تحترم أحكامه من قبل المخاطبين به حكام ومحكومين أو القائمين على تنفيذه ، ولاقيمة لأحكامه بدون تنفيذها لأن كل متقاضى يسعى من وراء دعواه الحصول على الحكم الذى يحمى حقوقه وتنفيذه على أرض الواقع لأن عدم تنفيذ الأحكام يضرب فى الصميم حرمة القانون وأحكام القضاء ويزرع الشك حول فاعلية جدواه خاصة فيما يتعلق بمواجهة الجرائم السيبرانية وتحقيق الأمن المجتمعى .([٢])

ثانيا: الآليات الوقائية الدولية لحماية الأمن المجتمعى فى مواجهة الجرائم السيبرانية

١. تعد الدبلوماسية الشعبية بين الدول خاصة على المستوى الاقليمى لها أهميتها خاصة عندما تستهدف الجماهير ومخاطبتهم من خلال وسائل الاعلام المختلفه من خلال المنابر المتعددة التى تركز أساساً على العمل الأهلى والمجتمع المدنى غير الحكومى وتبذل هذه الجهود سواء من خلال اشرف السفارات والبعاثات الدبلوماسية الرسمية أو بجهود بعيدة عن العمل الرسمى مستخدمة كل الامكانيات من خلال النقابات العمالية والمهنية التى تعمل على مواجهة الجرائم السيبرانية وحماية الأمن المجتمعى.([٣])

٢. الجهود الدولية من خلال المنظمات غير الحكومية التى تركز على تطور الأسلحة ذاتية التشغيل دون تدخل البشر واستخدامها من خلال أجهزة الاستشعار عن بعد والبرمجيات التى أصبحت تهدد المدنيين بشكل كبير وتخالف أحكام القانون الدولى الانسانى باستخدام الذكاء الاصطناعى . مما دفع اللجنة الدولية للصليب الأحمر الى إعتماد قواعد جديدة ملزمة لتنظيم إستخدام هذه الأسلحة ، وأهمية التفاوض بين الدول بشأن تشغيلها سواء فى حال قيام نزاع مسلح دولى أو غير ذى طابع دولى لتحقيق الحماية للمدنيين والأعيان المدنية وتحقيق الأمن المجتمعى .([٤])

([١]) د./ نهتاف موردة، وأخرون : الحكم الرشيد والتنمية البشرية فى دول الشسرق الأوسط وشمال أفريقيا ، دراسة قياسية باستخدام نماذج البيانات الطولية ، مصر المعاصرة عدد ٥١٦ ، أكتوبر ٢٠١٤ ، القاهرة ، ص٤٢٥ .

([٢]) د./ على محمد عبدالفتاح محمد خليل : سلطة قاضى الالغاء فى توجيه أوامر الادارة واستخدام التهديد المالى ضدها لضمان تنفيذها حكمه (دراسة مقارنة) ، مصر المعاصرة ، ع ٥١٩ ، يوليو ٢٠١٥ ، ص١٠٨ .

([٣]) د./ محمد سليمان طابع : سيناريوهات الصراع والتعاون حول المياه فى الشرق الأوسط ، دراسة حالة حوض النيل ، مصر المعاصرة ، ع٥١٥ ، يوليو ٢٠١٤ ، القاهرة ، ص٢٧١ .

(٤) كلمة الممثل العام للجنة اللدولية لصليب الأحمر أمام الجمعية العامة للأمم المتحدة فى الدورة ٧٦ اللجنة الأولى عند المناقشة العامة لنزع السلاح والأمن الدولى فى ٢١ أكتور ٢٠٢١ .

المطلب الثانى: الآليات العلاجية لحماية الأمن المجتمعى فى مواجهة الجرائم السيبرانية الدولية والوطنية

مما لا شك فيه أنه يجب الاهتمام بالاجراءات العلاجية لحماية الامن المجتمعي من الجرائم السيبرانية سواء علي المستوي الوطني او الدولي وهوما نتناوله من خلال التالي:

أولاً : آليات علاجية دولية لحماية الأمن المجتمعى فى مواجهة الأمن السيبرانى:

لعل تزايد مخاطر الأعمال العدائية فى الفضاء الخارجى هى مصدر قلق إنسانى خطير لأن العمليات العسكرية فى الفضاء الخارجى لا تحدث فى فراغ قانونى لأنها مقيدة بالقوانين القائمة لا سيما معاهدة الفضاء الخارجى وميثاق الأمم المتحدة وقواعد القانون الدولى الانسانى والتى تعمل على حماية المدنيين والأعيان المدنية فى الصراعات المسلحة ([1])

وأضاف ممثل اللجنة الدولية للصليب الأحمر أمام الجمعية العامة الأعمال التى تشكل تهديداً للفضاء الخارجى والتى بناء عليها صدرت توصيات من قبل الأمين العام للأمم المتحدة بالتقرير المعنون بالحد من التهديدات الفضائية عن طريق معايير، وقواعد، ومبادئ تضبط أنماط السلوك المسئول بالقرار رقم A/7G/77 والآثار الخطيرة المحتملة لاستخدام الأسلحة فى الفضاء الخارجى وقد حذر السيد/تيلمانرو دنهاوزر خبير الحرب السيبرانية التهديدات التى تؤثر قى الفضاء السيبرانى ودور القانون الدولى الانسانى فى تفادى التهديدات الخطيرة على المدنيين([2])

ونظراً لتزايد التهديدات التكنولوجية فى مجال الجرائم السيبرانية خلال أكثر من عقد من الزمان قامت فرق الخبراء على المستوى الحكومى بدراسة وتقديم توجيهات للتصدى لمخاطر تكنولوجيا المعلومات والاتصالات الحالية والناشئة، وأثرها على الأمن الدولى بما فى ذلك تدابير بناء الثقة وبناء القدرات والتعاون. فى حين أن الفريق العامل مفتوح العضوية قد إعتمد توصيات ملموسة وعملية كما أكدت على ذلك الممثلة السامية لشئون نزع السلاح بالأمم المتحدة . وأضافت بأن المنظمات الاقليمية تبذل جهوداً بدءاً من تنفيذ القواعد الطوعية غير الملزمة للدول وانتهاءً باتخاذ التدابير الاقليمية الرائدة لبناء الثقة واعتماد أدوات اقليمية للحد من الجرائم السيبرانية وأثرها على الأمن المجتمعى ([3])

ثانياً الآليات العلاجية الوطنية لحماية الأمن المجتمعى فى مواجهة الأمن السيبرانى:

على الرغم من الجهود الدولية السالفة الذكر إلا أن الجهود الوطنية لا يمكن تجاهلها لمواجهة الجرائم السيبرانية والتى تؤثر سلباً على الأمن المجتمعى سواء فى المجالات السياسية والاقتصادية والاجتماعية والتى تتطلب اتخاذ الأليات الأتية :-

---

(١)وقد صاغت اللجنة الدولية للصليب الأحمر هذه الآراء فى ورقة تحمل عنوان " التكلفة البشرية المحتملة لاستخدام الأسلحة فى الفضاء الخارجى والحماية التى يوفرها القانون الدولى ، والتى نشرت فى ابريل ٢٠٢١ بالجمعية العامة وتم الأخذ بها فى قرارها ٧٥/٣٦ .

(٢)اللجنة الدولية للصليب الأحمر ، مقال بعنوان " الحرب السيبرانية والقانون الدولى الانسانى الصادر فى ٢٥ فبراير٢٠٢١

(٣) السيدة أيزومي ناكاميتو، وكيل الأمين العام لشئون نزع السلاح فى تقريرها أمام مجلس الأمن تحت عنوان " دعوة أممية الى البقاء يقظين حيال التكنولوجيات الخبيثة التى يمكن أن تعرض الأجيال القادمة للخطر " بتاريخ ٢٩ يونيو ٢٠٢١ .

١. إتخاذ الاجراءات التى تشارك فيها جميع الأطراف لتحقيق التعاون الدولى بين الدول فيما يتعلق بجمع الأدلة الالكترونية وتحليلها حال إرتكاب الجرائم السيبرانية.
٢. توفير المساعدات الفنية والتقنية التى من شأنها العمل على كشف الجرائم السيبرانية وتحليل الأدلة الالكترونية مما يساعد على ضبط الجناه .
٣. اعتماد المعايير اللازمة التى من شأنها المساعدة فى إجراء التحقيقات ونفاذ القانون وتبادل المعلومات بين الجهات المعنية داخل الدولة .
٤. وضع الاحصاءات الدقيقة للجرائم السيبرانية لبيان إتجاه هذه الجرائم ، وبيان مؤشرات الزيادة أو النقص حتى يتمكن متخذ القرار والمسئولين من إتخاذ القرارات ، ورسم السياسات اللازمة لمواجهة هذه الجرائم وعلاج أسبابها ، وآثارها بما يحقق الأمن المجتمعى بصورة فاعلة .
٥. تعويض ضحايا الجرائم السيبرانية والعمل على إصلاح الأضرار التى أصابت الأجهزة والوسائل المستخدمة والشبكة الالكترونية ومساعدة المستخدمين المتضررين فنياً لتلافى الأخطار التى نتجت عن هذه الجرائم .([1])

وفى ضوء ما سبق يقول" جون لوك" أحد علماء الفكر السياسى الأوروبى أن الحرية لا تعنى الاباحة ولكن المساواة التى لا تؤدى إلى حرب الجميع ضد الجميع ، والعقل الطبيعى يقول أن البشر جميعاً متساويين ومستقلين ، ولا يجوز لأحد أن يسئ الى الأخر ولا يجوز التعدى على حقوق الأخرين ، والمنطق الطبيعى يقول بأنه يجب حماية البرئ وعقاب المذنب .

ويقول " جان جاك رسو " بأن العقد الاجتماعى يعنى الحرية التى يتم إعطائها للأفراد دون تأثير على الادارة العامة بالسلب بمعنى حماية المجتمع ضد كل فعل ضار ومنها بطبيعة الحال الجرائم السيبرانية لما لها من أثر على الأمن المجتمعى ([2])

الخاتمة

لقد تناولت الدراسة الجرائم السيبرانية وأثرها على الأمن المجتمعى فى ثلاث مباحث ، فالمبحث الأول يتضمن ماهية الجرائم السيبرانية والأمن المجتمعى ، وتعرضت الدراسة لموقف الفقه من تحديد ماهية الأمن المجتمعى وانتهت الى أنه يعنى توفير حالة من الأمن والاستقرار لجميع أفراد المجتمع أياً كان انتمائتهم السياسية أو العقائدية أو العرفية سواء على المستوى الاقتصادى أو الاجتماعى أو السياسى ، وتحقيق أهداف الجميع علي المستوى الشخصى أو الجماعى فى الحاضر والمستقبل.

كما تعرضت الدراسة لماهية الجرائم السيبرانية وانتهت الى أنها كل فعل ضار بالأخرين عبر استخدام الفضاء الالكترونى أياً كانت الوسيلة المستخدمة بالمخالفة للقواعد القانونية التى تحكم استخدام هذه الوسائل الالكترونية ولها آثار مباشرة أو غير مباشر على الأمن المجتمعى

([1]) مكتب الأمم المتحدة المعنى بالمخدرات : دراسة شاملة عن الجريمة السيبرانية ، فبراير ٢٠١٣ ،الأمم المتحدة ، نيويويرك، ص xv .

([2]) د./ يوسف حسين محمد البشير : المواجهات الأخلاقية لحقوق الانسان فى المرجعية الفكرية الاسلامية ، مصر المعاصرة ، ع ٥٣٣ ، القاهرة ، يناير ٢٠١٩ ، ص٤٠٩.

والمحث الثاني تضمن الأسس القانونية الدولية والوطنية التى تحكم الجرائم السيبرانية وتعمل على حماية الأمن المجتمعى سواء من خلال سن التشريعات والاجراءات الوقائية والعلاجية من خلال الجهات المعنية لنفاذ القانون .
كما تعرض الباحث في المبحث الثالث الى الآليات الوطنية والدولية التى من شأنها مواجهة الجرائم السيبرانية والحد منها والعمل على حماية الأمن المجتمعى ، وإنتهت الدراسة الى وضع النتائج التى أسفرت عنها الدراسة وكذا التوصيات التى يرى الباحث أهمية الأخذ بها للحد من الجرائم السيبرانية وحماية الأمن المجتمعى على النحو التالى :-

أولاً النتائج :

١. في ظل عالم تسوده العولمة، فإن أغلبية القوانين تتضرر من التداخل بين النظم القانونية الوطنية والإقليمية والدولية، وعادة ما يحدث تفاعلات بين هذه النظم على مستويات متعددة، تؤدي إلى تعارض الأحكام لبعضها البعض في بعض الأحيان، أو اصطدامات بين القوانين، أو الإخفاق في التوافق بينهما بشكل كاف، أو تحدث فجوات قضائية عند تناول الجريمة السيبرانية.
٢. التشرذم الذى يطبع الساحة الدولية وتنوع القوانين المحلية المتعلقة بالجريمة السيبرانية والأمن المجتمعى لإختلاف النطاق الموضوعى والجغرافى .
٣. الاختلافات التشريعية وإنعكاس الاختلافات الاجتماعية والثقافية مما أدى الى إختلاف فى مجال الصلاحيات والاجراءات والأحكام المتعلقة بالتعاون الدولى فى مجال الجرائم السيبرانية والأمن المجتمعى .
٤. الاعتماد على الوسائل التقليدية للتعاون الدولى الرسمى فى مجالات مستحدثة كالجرائم السيبرانية وأثرها على الأمن المجتمعى والتى تحتاج الى سرعة فى الاجراءات والامكانيات لسرعة زوال الأدلة الالكترونية .
٥. عدم التوافق بين الأطر القانونية الوطنية التى تحكم الجرائم السيبرانية وصلاحيات التحقيق وقواعد حقوق الانسان التى تحكم مسألة التجريم والاجراءات الجنائية الحاكمة .
٦. عدم توافر المساعدات الفنية والتقنية اللازمة لسلطات انفاذ القانون من المدعين العموم والسلطات القضائية ومأمورى الضبط القضائى علي الوجه المستدام لمواجهة الجرائم السيبرانية وحماية الأمن المجتمعى .
٧. عدم كفاية التعاون بين الجهات المختلفة لتعزيز الشركات لمواجهة الجرائم السيبرانية من قبل الحكومات والقطاع الخاص والمجتمع المدنى والمؤسسات الأكاديمية من أجل حماية الأمن المجتمعى.

ثانياً : توصيات البحث

١. يجب أن تتناول التدابير القانونية لمنع الجريمة السيبرانية ومكافحتها من كافة المجالات المعنية بالتجريم ومنح الصلاحيات الإجرائية وتحديد الاختصاص القضائي والتعاون الدولي، بالإضافة إلى المسؤولية والتبعية التي يتحملها مقدم خدمة الإنترنت.

٢. أهمية التعاون بين الدول فى مجال مواجهة الجرائم السيبرانية خاصة تلك التى تؤثر على الأمن المجتمعى من خلال وضع الاتفاقيات الدولية التى من شأنها الزام الدول الأطراف بصك التشريعات اللازمة سواء على مستوى القواعد الموضوعية أو الاجرائية موضع التنفيذ .
٣. ينبغي للدول الأعضاء أن تكفل صمود أحكامها التشريعية أمام اختبار الزمن فيما يتعلق بالتطورات المستقبلية في مجال التكنولوجيا عن طريق اشتراع قوانين تعتمد صياغات محايدة من الناحية التكنولوجية وتجرم النشاط الذى يعتبر غير قانوني بدلا من تجريم الوسائل المستخدمة في ممارسته
٤. ينبغي للدول الأعضاء أن تنظر في وضع مصطلاحات متسقة لوصف أنشطة الجريمة السيبرانية ، وأن تقوم قدر الإمكان بتيسير التفسير الدقيق للقوانين ذات الصلة من جانب أجهزة إنفاذ القانون والسلطات القضائية.
٥. ينبغي للدول الأعضاء أن تحترم الحقوق السيادية للدول الأخري لدى صياغة السياسات والتشريعات التي تناسب أوضاعها الوطنية وتفي باحتياجاتها الوطنية فيما يتعلق بالتصدي للجريمة السيبرانية. وتعزيز التعاون الدولي على مكافحة الجريمة السيبرانية
٦. مساعدة الدول المتقدمة فى مجال التطوير التكنولوجى للدول النامية بحيث يسهل عليها اكتشاف الجرائم السيبرانية ومواجهتها فى أسرع وقت ممكن قبل اخفاء الأدلة الالكترونية .
٧. عقد دورات تدريبية و فنية للقضاه ومساعدى القضاه فى مجال الأمن السيبرانى لمسايرة التطورات التكنولوجية فى مجال تجميع الأدلة الالكترونية وحمايتها من الضياع أو التلاعب بها من جانب الجناه .
٨. أهمية تفعيل المعاهدات على المستوى الاقليمى لمواجهة الجرائم السيبرانية وحماية الأمن المجتمعى بصفة خاصة والأمن القومى بصفة عامة .
٩. إتخاذ الإجراءات الوقائية على المستوى الوطنى والدولى لمواجهة الجرائم السيبرانية وحماية الأمن المجتمعى للدول لتحقيق الاستقرار السياسى والاقتصادى والاجتماعى .

وفى الختام لا يسعنى إلا أن أقول " إِنْ أُرِيدُ إِلَّا الْإِصْلَاحَ مَا اسْتَطَعْتُ ۚ وَمَا تَوْفِيقِي إِلَّا بِاللَّهِ ۚ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ "

المراجع

أولا :- القرءان الكريم

١. سورة البقرة ، الآية ٨٥ .

ثانيا :- الاتفاقات والاعلانات والتقارير والدساتير

١. اتفاقية الاتحاد الأفريقى بشأن أمن الفضاء الالكترونى وحماية البيانات ذات الطابع الشخصى المعتمدة بمالابو" غنيا الاستوائية فى ٢٧ يونيو٢٠١٤ .
٢. الميثاق العلمى للطبيعة الصادر من الجمعية العامة للأمم المتحدة عام ١٩٨٢ .
٣. الاتفاقية العربية لمكافحة تقنية المعلومات ، الصادر فى ٢٠١٠/١٢/٢١ .
٤. الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية الصادرة فى ٢٠٠١/١١/٢٣.

٥. الاعلان الصادر عن الدورة الرابعة عشر لمؤتمر رؤساء دول وحكومات الاتحاد الافريقى بشأن تكنولوجيا المعلومات والاتصالات فى أفريقيا " التحديات والآفاق المستقبلية للتنمية " المنعقد فى أديس أبابا ، أثيوبيا ، فى الفترة من ٣١ يناير الى ٢ فبراير عام ٢٠١٠ .
٦. إعلان أوليفرتامبو الذى اعتمده مؤتمر الاتحاد الأفريقى الاستثنائى للوزراء المسئولين عن تكنولوجيا المعلومات والاتصالات المنعقد فى جنوب أفريقيا بجوهانسبيرج فى ٥ فبراير عام ٢٠٠٩ .
٧. اعلان أبيدجان المعتمد فى ٢٢ فبراير عام ٢٠١٢ وإعلان أديس أبابا المعتمد فى ٢٢ يونيو عام ٢٠١٢ حول مواءمة تشريعات الفضاء الالكترونى فى أفريقيا .
٨. التقرير الصادر عن الاتحاد الدولى للاتصالات حول اتجاهات الاصلاح فى الاتصالات لعام ٢٠٢١:٢٠١٠.
٩. تقرير سويسرى SwissRe لعام ٢٠١٧ .
١٠. كلمة الأمين العام كوفى عنان أمام مجلس الأمن التابع للأمم المتحدة بالجلسة ٢٢ يونيو ٢٠٠٤ S/PV.4993.
١١. فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية ، فيينا، ٦-٨ نيسان/أبريل٢٠٢١ . UNODC/CCPCJ/EG.4/2021/CRP.1 17 February 2021
١٢. فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية ، فيينا، ٢٥ -٢٨ شباط/فبراير ٢٠١٣ UNODC/CCPCJ/EG.4/2013/2.
١٣. UNODC/CCPCJ/EG4/2013/23Jauary,2013
١٤. مكتب الأمم المتحدة المعنى بالمخدرات : دراسة شاملة عن الجريمة السيبرانية ،الأمم المتحدة ، نيويورك، فبراير ٢٠١٣.
١٥. الدستور المصرى لعام ٢٠١٤ ، المادة ٣١ .
١٦. الجريدة الرسمية ، ع ٣٢ مكرر ج ، ١٤ أغسطس ٢٠١٨ .

ثالثا :- الصليب الاحمر

١. اللجنة الدولية للصليب الأحمر ، مقالة ، بعنوان " الحرب السيبرانية والقانون الدولى الانسانى " ، ٢٥ فبراير لعام ٢٠٢١ .
٢. وقد صاغت اللجنة الدولية للصليب الأحمر هذه الآراء فى ورقة تحمل عنوان " التكلفة البشرية المحتملة لاستخدام الأسلحة فى الفضاء الخارجى والحماية التى يوفرها القانون الدولى ، والتى نشرت فى ابريل ٢٠٢١ بالجمعية العامة وتم الأخذ بها فى قرارها ٧٥/٣٦ .
٣. كلمة الممثل العام للجنة اللدولية لصليب الأحمر أمام الجمعية العامة للأمم المتحدة فى الدورة ٧٦ اللجنة الأولى عند المناقشة العامة لنزع السلاح والأمن الدولى فى ٢١ أكتور ٢٠٢١ .

رابعا : الكتب العربية

١. السيدة أيزومي ناكاميتو، وكيل الأمين العام لشئون نزع السلاح فى تقريرها أمام مجلس الأمن تحت عنوان " دعوة أممية الى البقاء يقظين حيال التكنولوجيات الخبيثة التى يمكن أن تعرض الأجيال القادمة للخطر " بتاريخ ٢٩ يونيو٢٠٢١ .
٢. د./ عبدالله محمد الربايعه : السياسة الشرعية وأهميتها فى تحقيق الأمن المجتمعى ، المجلة العربية للدراسات الأمنية والتدريب ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، المجلد رقم ٣٠ ، ع. ٥٩ ، جمادى الأول لعام ١٤٣٥ هـ .
٣. د./ عبد الوهاب بن رجب هاشم : جرائم البيئة وسبل المواجهة ، مركز البحوث والدراسات بجامعة نايف العربية للعلوم الأمنية ، الرياض ، ٢٠٠٦ مـ -١٤٢٧ هـ .
٤. د./ على محمد عبدالفتاح محمد خليل : سلطة قاضى الالغاء فى توجيه أوامر الادارة واستخدام التهديد المالى ضدها لضمان تنفيذها حكمه (دراسة مقارنة) ، مصر المعاصرة ، ع ٥١٩ ، يوليو ٢٠١٥
٥. د./ نهتاف موردة، وأخرون : الحكم الرشيد والتنمية البشرية فى دول الشسرق الأوسط وشمال أفريقيا ، دراسة قياسية باستخدام نماذج البيانات الطولية ، مصر المعاصرة عدد ٥١٦ ، أكتوبر ٢٠١٤ ، القاهرة .
٦. د./ مجدي الداغر: اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وانعكاساته على دعم وتعزيز الأمن السيبرانى في مصر، (دراسة ميدانية) ، المجلة العربية لبحوث الاعلام والاتصال - العدد ٣٣ ابريل/ يونيو٢٠٢١ .

٧. د./ محمد أحمد منتصر : جريمة التهديد بالقتل عبر شبكة الانترنت ، مصر المعاصرة ، ع .٥١٨ ، ابريل ٢٠١٥ .
٨. د./ محمد سليمان طايع : سيناريوهات الصراع والتعاون حول المياه فى الشرق الأوسط ، دراسة حالة حوض النيل ، القاهرة ، مصر المعاصرة ، ع٥١٥ ، يوليو ٢٠١٤ .
٩. د./ يوسف حسين محمد البشير : المواجهات الأخلاقية لحقوق الانسان فى المرجعية الفكرية الاسلامية ، مصر المعاصرة ، ع ٥٣٣ ، القاهرة ، يناير ٢٠١٩ .

خامسا :- المواقع

١. نشرة الاتحاد المصرى للتأمين ، عدد اسبوعي ، رقم ٦٧ ، سنة ٢٠١٩ . بعنوان " الهجمات الالكترونية (السيبرانية) والتأمين .
https://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244&PageDetailID=1324
٢. مكتب الأمم المتحدة المعني بالمخدرات والجريمة – فيينا ، دراسة شاملة عن الجريمة السيبرانية ، نيويورك ، مسودة شباط/فبراير ٢٠١٣ .
https://al-ain.com/article/russian-ukrainian-war-in-numbers
٣. التهديدات السيبرانية المرتبطة بكوفيد - ١٩ في العالم ، الانتربول ، نيسان/أبريل ٢٠٢٠ .
https://www.interpol.int/ar/4/6/19
٤. دعوة أممية إلى البقاء يقظين حيال التكنولوجيات الخبيثة التي يمكن أن تعرض الأجيال القادمة للخطر، الامم المتحدة ، ٢٩ حزيران/يونيه ٢٠٢١ - السلم والأمن ،
https://news.un.org/ar/story/2021/06/1078872
٥. الهيئة العامة للاستعلامات المصرية :الأمن السيبرانى .. بيئة تكنولوجية أكثر أمناً -الإثنين، ٢٦ فبراير ٢٠١٨ - ١٢:١٠ م
https://sis.gov.eg/Story/159921?lang=ar
٦. جمهورية مصر العربية ، رئاسة مجلس الوزراء - المجلس الأعلى للأمن السيبراني ،
https://escc.gov.eg/index.html