جـامعـة المنوفيـة
كلية الحقوق

الحماية الدستورية للأمن السيبراني وأثره على النظام العام

الدكتورة

ماجدة عبد الشافى محمد الهادى خالد منصور

مدرس القانون العام – جامعة بنها

الملخص

يهدف البحث إلى دراسة الأمن السيبراني الذي يعد جزء أساسي من أمن الدول، حيث يرتبط بالمسائل المتعلقة بحماية المعلومات على جميع الأنظمة والشبكات الإلكترونية، لعظم أهمية الأمن السيبراني وحاجة الناس إليه ولارتباطه بواقعنا المعاصر وعظم تأثيره على النظام العام، بات الحماية الدستورية للفضاء السيبراني وما يتعلق بها من حماية سيادة الدولة وحقوق الأفراد ضرورة لا غني.

وقد توصل البحث إلى العديد من النتائج منها أنه على الرغم من الكثير من الإيجابيات التي أسهمت في تحقيقها التكنولوجيا الرقمية إلا أنها أفرزت العديد من الآثار السلبية سواء على المستوى الأمن العسكري أو الاقتصادي أو الاجتماعي والثقافي.

وقد أوصى البحث بضرورة وضع الإطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية حماية للخصوصية، والهوية الرقمية، وأمن المعلومات، وذلك بمشاركة من الأطراف المعنيين، وأيضا ضرورة وضع وتنفيذ خطط وحملات للتوعية المجتمعية بأهمية الأمن السيبراني.

الكلمات المفتاحية: الأمن السيبراني ــ الحماية الدستوريةــ النظام العام

Abstract:

The research aims to study cyber security, which is an essential part of state security. It relates to the protection of information on all electronic systems and networks. Due to the great importance of cybersecurity and people's need for it, and its relevance to our contemporary reality, and the greatest impact on public order constitutional protection of cyberspace and what is related to it in terms of protecting state sovereignty and individual rights has become a necessity.

The research has reached many results, including that despite many positives that digital technology has contributed to, it has produced many negative effects, whether on the level of military, economic, social or cultural security.

The research recommended the need to develop the appropriate legislative framework for cyberspace security and combating cybercrime in order to protect privacy, digital identity, and information security, with the participation of the concerned parties, as well as the need to develop and implement plans and campaigns for community awareness of the importance of cybersecurity.

Keywords: cyber security – constitutional protection – public order

مقدمة

تعد التحولات التكنولوجية من أهم الركائز الأساسية للمجتمع في جميع المجالات، حيث أصبح العصر الحالي هو عصر الثورة الرقمية والإلكترونية التي تمارس نشاطها في الفضاء الإلكتروني الذي يعد أبعد من الأرض ويكون أكثر خطراً على سكانها حيث دخلت هذه الثورة في جميع المجالات الإنسانية.

يشهد المجتمع اليوم تطوراً متسارعاً لتكنولوجيا المعلومات والاتصالات، كما يشهد تزايداً وتنوعاً في التطبيقات والخدمات الإلكترونية التي تعتمد الفضاء السيبراني أساساً لها. ومن ثم فقد أصبحت تكنولوجيا المعلومات والاتصالات الركيزة الأولى لبناء مجتمع المعرفة ولبنة أساسية في نموه وازدهاره في ظل العولمة[١]، ولذلك تتطلع العديد من الدول اليوم، المتقدمة منها أو النامية، إلى بناء مجتمع معرفي جديد يعتمد على التنوع الاقتصادي، وعلى الابتكار والإبداع، وكذلك على التبادل المعرفي والفكري في المجالات الحيوية المختلفة.

وقد بدأت دول العالم في الدخول إلى عصر التحول الرقمي باعتماد استراتيجيات وطنية للتحول الرقمي، ومن ذلك الاستراتيجية الفرنسية للأمن الرقمي عام ٢٠١٥[٢] كما بدأت مصر في تطوير رؤية للدولة المصرية في إطار الرقمية رؤية مصر ٢٠٣٠، والتي تعتمد في أغلب جوانبها على تنمية البنية التحتية التكنولوجية واعتماد تكنولوجيا الاتصالات والمعلومات كوسيلة لإنجاز المهام المختلفة الحكومية وغير الحكومية.[٣]

([١])العولمة :Globalization هو مصطلح إنجليزي تم ترجمته إلى اللغة العربية، وتعني جعل الشيء عالميا من حيث النطاق أو التطبيق أو بمعنى آخر الظاهرة التي تشير إلى مرحلة من مراحل التطور التاريخي للمجتمعات الإنسانية (الاقتصادية والاجتماعية والثقافية والسياسية) فهذه الظاهرة تسعى إلى تذويب الحدود بين المجتمعات، بحيث تصبح جميع الأنشطة الإنسانية مفتوحة على بعضها البعض والمساواة بينها،" يمكن الرجوع في ذلك إلى

Bhagwat, Jagdihln, Defiance of Globalization, New York, Oxford University Pressm2004, p 29.

([2])Strategie Nationale pour La Securite Du Numerique, 2015

https://www.ssi.gouv.fr/

([٣]) تأكيدا على أهمية التحول الرقمي بادرت الحكومة المصرية بإنشاء كل من المجلس القومي للمدفوعات والمجلس الأعلى للتحول الرقمي والمجلس الأعلى للأمن السيبراني، ووضع خطة شاملة لنشر الوعي المجتمعي بأهمية التحول الرقمي وتحقيق طفرات على صعيد البنية التحتية الرقمية، فضلا عن إطلاق مصر الاستراتيجية الوطنية للتجارة الإلكترونية عام ٢٠١٧ م في إطار تشجيع التجارة الإلكترونية، بالتعاون مع منظمة الأمم المتحدة للتجارة والتنمية "الأونكتاد"، وكذلك تدشين مشروع البنية المعلوماتية المصرية لربط أكثر من ٧٠ قاعدة بيانات حكومية ببعضها، وتفعيل المحرك الرقمي القومي G2G، ومنصة تقديم الخدمات

ولقد انعكست تلك التطورات على الإدارة العمومية التي تعتبر هي الآلية التي تحرك عجلة التنمية في الدولة وتخدم المواطنين، بذلك تم إدراج البرمجة المعلوماتية داخل نسق عمل الإدارة، ساعدها في ذلك ظهور شبكة الإنترنت وما نتج عنها تأثير في تسهيل العمليات الإدارية، وتبسيط إجراءاتها وتقليل استخدام الورق فيها وتحقيق عدد من المزايا الأخرى، هذه التطورات كان لها الأثر البارز في إحداث تغيرات جذرية على أداء المؤسسات يأتي في مقدمة التحول الرقمي في الإدارة.

لقد أفضت الثورة المعلوماتية عن ظهور بيئة جديدة وهي الفضاء الإلكتروني، وهي تختلف عن البيئات الأخرى سواء الإقليم البري، البحري، الجوي أو الفضاء الخارجي كونها من صنع الإنسان ولكنها تشترك في بعض السمات والخصائص مع البيئات الأخرى، وأضحى الفضاء الإلكتروني عنصراُ مؤثراً في النظام الدولي وفي إدارة التفاعلات بين الدول وأصبح يلعب دوراً هاماً في التأثير على موازين القوة وتستخدم العديد من الدول القدرات التي يوفرها الفضاء الإلكتروني لاعتبارات في مقدمتها الأمن والقوة العسكرية.

تعد البيانات التي تنتجها الجهات الحكومية أو تتلقاها أو تتعامل معها أصولًا وطنية يمكن أن تساهم في تحسين الأداء والإنتاجية وتسهيل تقديم الخدمات العامة عن طريق دعم العمليات الفعالة لإدارة البيانات واتخاذ القرارات الاستراتيجية واستشراف المستقبل وتحقيق أعلى مستويات المسؤولية والشفافية كما تسعى الدول في جميع أنحاء العالم إلى الاستفادة من قيمة البيانات باعتبارها مورداً اقتصادياً يساعد على الابتكار ويساهم في دعم التحولات الاقتصادية وتعزيز المقومات التنافسية للدول، وعلى المستوى الوطني[1]، تقوم الجهات الحكومية بجمع ومعالجة كميات هائلة من البيانات يمكن الاستفادة منها للمساهمة في النمو الاقتصادي والارتقاء بالدولة المصرية إلى الريادة ضمن الاقتصادات القائمة على البيانات.

ونتيجة للتحول الرقمي في تنفيذ المهام والمسؤوليات المختلفة في كافة المرافق العامة التابعة للدولة فقد تعرضت لهجمات عدة منها الاحتيال وسرقة المعلومات وتغيير البيانات، حيث أن العمل الالكتروني معرض لتلك الهجمات، والتي ينظر إليها على أنها تحديات تحد من كفاءة الإدارة الرقمية وتقلل من فعاليتها لذا اتجهت الدولة المصرية أجل الحفاظ على النتائج والمكتسبات التي تحققت من تطبيق التحول الرقمي إلى البحث عن أساليب جديدة تدعم من

الحكومية إلى جانب منصة تقديم الدكتور/ محمد موسى على شحاته: انعكاسات تفعيل آليات التحول الرقمي في ضوء مبادرة الشمول المالي على تطبيقات الحكومة الإلكترونية بجمهورية مصر العربية، بحث منشور بمجلة الدراسات التجارية المعاصرة، العدد التاسع يناير – ٢٠٢٠، ص ٢٠٠.

([1])الهيئة السعودية للبيانات والذكاء الاصطناعي، سياسات حوكمة البيانات الوطنية، مكتب إدارة البيانات الوطنية، ٢٠٢١، ص ٨.

الخطوط الدفاعية في مواجهة تلك الهجمات وبحيث تعطي لها حصانة قوية للوقاية منها. وتسمى تلك الأساليب بإجراءات أو ممارسات أو برامج الأمن السيبراني*.

ومن ثم يحظى الأمن السيبراني بأهمية بالغة ذلك أن الحكومات والمؤسسات العسكرية والشركات والمؤسسات المالية والطبية وغيرها تقوم بجمع ومعالجة وتخزين كميات كبيرة جدا من البيانات على أجهزة الكمبيوتر والأجهزة الأخرى، وإن كثير من هذه البيانات معلومات حساسة كونها تتعلق بالملكية الفكرية أو معلومات أمنية أو شخصية أو بيانات مالية، إذ أن الدخول غير المصرح به إلى هذه المعلومات والبيانات له عواقب وخيمة، ولاسيما وأن هذه المعلومات تنتقل بين المؤسسات والشركات عبر الشبكات إلى أجهزة أخرى، ونظرا لارتفاع الهجمات الإلكترونية فإن الدول والمؤسسات والشركات تجد نفسها مضطرة لحماية بياناتها ومعلوماتها، بل أصبحت الهجمات والاختراقات الإلكترونية تهديدا حقيقيا للنظام العام في الدول.

واستهدفت رؤية مصر ٢٠٣٠ التطور الشامل للوطن وأمنه واقتصاده ورفاهية مواطنيه وعيشهم الكريم، ولذلك فمن الطبيعي أن يكون أحد مستهدفاتها التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية، بما يعبر عن مواكبة التقدم العالمي المتسارع في الخدمات الرقمية وفي الشبكات العالمية المتجددة، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ويتماشى مع تنامي قدرات المعالجة الحاسوبية وقدرات التخزين الهائلة للبيانات وتراسلها.

ومن ثم تم تشكيل المجلس الأعلى للأمن السيبراني بقرار من رئيس مجلس الوزراء بالعام ٢٠١٤ برئاسة وزير الاتصالات، وعضوية ممثلين عن كل من وزارات: البترول، الدفاع، الداخلية، الكهرباء، الخارجية، الصحة، التموين، الموارد المائية، البنك المركزي، جهاز المخابرات العامة، إضافة إلى ٣ أعضاء من ذوي الكفاءة والخبرة.(١)

*** الأمن السيبراني هو مفهوم ظهر بعد الحرب الباردة استجابة للمزيد من الابتكارات التكنولوجية والظروف الجيوسياسية المتغيرة، تم استخدامه لأول مرة من قبل علماء الكمبيوتر في أوائل التسعينات للتأكيد على سلسلة من حالات عدم الأمان المرتبطة بأجهزة الكمبيوتر لكنة تجاوز مفهومة التقني لأمن الكمبيوتر عند حث المؤيدين على أن التهديدات الناشئة عن التقنيات الرقمية يمكن أن يكون لها آثار اجتماعية مدمرة، يمكن الرجوع في ذلك إلى:**

Lene Hansen- Helen Nissenbaum, Digital Disaster, Cyber Security, and the Copenhagen School, International Studies Quarterly (2009) 53, 1155–1175

(١) قرار رئيس مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤.

المشكلة:

لقد أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة وزادت هيمنة تكنولوجيا المعلومات والاتصالات على نسق الحياة العام، وصاحب ظهور الحاسب الآلي والتوسع في استخدام شبكة الإنترنت في مجالات الحياة المختلفة ظهور بعض الآثار السلبية والمخاطر المترتبة على هذا التوسع الكبير؛ إذ كلما زاد الاعتماد على هذه التقنيات في التنمية زادت المخاطر الخاصة بحماية المعلومات، ومن هذه المخاطر التعرض للهجمات من خلال الفضاء السيبراني، إذ أصبح الفضاء السيبراني عرضة للانتهاكات من قبل محترقي الشبكات سواء أكانوا دولا أو غيرها مما يملكون هذه التقنيات المعلوماتية، فتوجهت الأنظار إلى الاهتمام وبشدة إلى الأمن السيبراني، وأصبح الحفاظ عليها حفاظا على الأمن القومي و النظام العام في الدول.

ومن ثم فإن الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن والذي يتعلق بتلك الدرجة التي تمكن الدولة من أن تصبح في مأمن من المخاطر التي تتعرض لها ومن حماية البنية التحتية للمنشآت الحيوية من الاستخدام غير المشروع لتكنولوجيا الاتصال والمعلومات بهدف محاوله السيطرة على الأجهزة وسرقة المعلومات وإفسادها أو تعطيلها.[1]

وتتمثل مشكلة البحث في السؤال الرئيسي التالي:

ما دور الحماية الدستورية للأمن السيبراني في الحفاظ على النظام العام؟ ويتفرع منه عدة أسئلة على النحو التالي:

١. ما أثر التحول الرقمي على النظام العام بعناصره المختلفة؟

٢. كيف يتم الموازنة بين مزايا التحول الرقمي وبين التهديدات التي تواجه أمن واستقرار المجتمع؟

٣. ما أثر الأمن السيبراني في مواجهة تلك التهديدات؟

هدف البحث: يهدف البحث الحالي إلى دراسة:

- التعرف على دوافع التحول الرقمي وأثره على النظام العام بعناصره المختلفة، وكذلك المخاطر التي تنشأ نتيجة لتطبيق التحول الرقمي في الدولة.
- الوقوف على دور الأمن السيبراني في مواجهة تلك التهديدات وحماية الحقوق الرقمية وكذلك حماية سيادة الدولة.

---

(١) د/ أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، المجلد الخامس والثلاثون، الجزء الثالث، ٢٠٢٠، ص ٣٧٧.

أهمية البحث:

تكمن الأهمية العلمية للبحث فيما يقدمه من معرفة شاملة حول أهمية تحقيق الأمن السيبراني للدولة كرد فعل ضروري للتحول الرقمي وما ينشأ عنه من تهديدات لأمن واستقرار الدول وذلك للوقوف حول كيفية مواجهة تلك التهديدات وصولا للحفاظ على النظام العام بعناصره المختلفة، والحفاظ على سيادة الدولة.

منهج البحث:

اعتمد البحث الحالي على المنهج الوصفي التحليلي الذي يركز على الوصف الدقيق والتفصيلي لظاهرة أو موضوع محدد للحصول على نتائج علمية دقيقة بطريقة موضوعية، ويتجلى اعتماد هذا المنهج من خلال السرد ووصف وتحليل أهم المفاهيم الخاصة بالتحول الرقمي والنظام العام وكذلك الأمن السيبراني، وكذلك تحدي ابعاد الأمن السيبراني ومتطلبات تطبيقه حماية للنظام العام، وفي ضوء أهداف البحث ومنهجه تم تقسيم البحث إلى فصليين، الأول يتضمن أثر التحول الرقمي على النظام العام، والثاني على الإطار الدستوري للأمن السيبراني وأثره على سيادة الدولة وحقوق الانسان.

الفصل الأول

أثر التحول الرقمي على النظام العام

أدى التطور التكنولوجي وتنامي الجهود نحو تطوير الاقتصاد المبني على المعرفة، إلى أن أصبحت تكنولوجيا المعلومات والاتصالات أداة رئيسية في توليد المعرفة، وحفظها، ومعالجتها، وتبادلها، وإتاحة فرص عمل جديدة للشباب، وتحفيز النمو الاقتصادي، مما استوجب على الدول ضرورة تبني الاتجاه نحو التحول الرقمي. وسوف نتناول ذلك فيما يلي:

المبحث الأول: مبررات وأهمية التحول الرقمي للمجتمع

المبحث الثاني: مخاطر التحول الرقمي التي تهدد النظام العام

المبحث الأول

مبررات وأهمية التحول الرقمي للمجتمع

شهد العالم حالياً العديد من التحولات العميقة؛ نتيجة النمو المُتسارع لحجم المعلومات والتي أدت بدورها لظهور عدد كبير من العلاقات والنشاطات المختلفة على المستوى العالمي، ومن أبرز هذه التحولات هي التكنولوجيا الحديثة التي تُعد من أهم الركائز الأساسية للمجتمع في جميع المجالات، مما أوجب على الدول ضرورة الاستجابة لها وسرعة التحول الرقمي لمواكبة تلك التغييرات، ومن ثم سوف نتناول مبررات وأهمية التحول الرقمي للمجتمع في مطلب أول، ثم بعد ذلك نتعرض إلى المخاطر التي تهدد النظام العام جراء التحول الرقمي في مطلب ثان على النحو التالي

المطلب الأول

مفهوم النظام العام والتحول الرقمي

أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة، فعلى المستوى الاجتماعي كان لها وقع كبير على سلوكيات المجتمع وهويته، وانتشار آليات الترابط بين المجموعات البشرية متمثلة في وسائل التواصل الاجتماعي، عبر أجهزة الحاسوب والهواتف المحمولة، مما ترتب عنه تغييرات كبرى في مرتكزات اجتماعية كبيرة كالخصوصية، الثقافة، الإعلام، التعارف وبناء العلاقات الاجتماعية، وبذلك فإن التحول الرقمي له تأثيرات عدة على النظام العام في المجتمع، ومن ثم سوف نعرض لمفهوم النظام العام وعناصره وبعد ذلك نتعرض لمفهوم التحول الرقمي على النحو التالي:

أولا: مفهوم وعناصر النظام العام:

يعتبر النظام العام فكرة مرنة تختلف باختلاف الزمان والمكان، فما يعتبر مخالفا للنظام العام في زمان أو مكان معينين قد لا يعد كذلك في زمان أو مكان آخرين، كما يختلف باختلاف الفلسفة السياسية والاقتصادية والاجتماعية السائدة في الدولة.

كما يعرف النظام العام بأنه قواعد يقصد بها تحقيق مصلحة عامة سياسية أو اجتماعية أو اقتصادية، تتعلق بنظام المجتمع الأعلى، وتعلو على مصلحة الأفراد، فيجب على جميع الأفراد مراعاة هذه المصلحة وتحقيقها، ولا يجوز لهم أن يناهضوها باتّفاقات فيما بينهم، حتى ولو حقّقت لهم مصالح فردية، لأن المصالح الفردية لا تقوم أمام المصلحة العامة.[1]

([1]) عبد العزيز أحمد السنهوري، الوسيط في شرح القانون المدني الجديد، نظرية الالتزام بوجه عام، مصادر الالتزام، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٠، ص ٣٩٩-٤٠٠.

عناصر النظام العام:

يجمع الفقه على ضرورة ربط النظام العام بالمصلحة العامة العليا للمجتمع في كل دولة على حده، غير أن معظم الفقهاء يتفقون على أن مفهوم النظام العام يتكون من ثلاثة عناصر ثابتة وهي: الأمن العام والصحة العامة والسكينة العامة، إلا أن مجلس الدولة الفرنسي أضاف في حكمه في قضية LUTETIA الآداب والأخلاق العامة كعنصر رابع من عناصر النظام العام.[١]

وسوف نتناول هذه العناصر على النحو التالي:

١- **الأمن العام:** " La securities publique" ويقصد به كل ما يطمئن به الإنسان على نفسه وماله. وبذلك يهدف الضبط الإداري لتحقيق الأمن العام للمواطنين وجعلهم يشعرون بأن أنفسهم وأموالهم وأغراضهم في مأمن من الاعتداءات والانتهاكات، على الإدارة واجب الحفاظ على النظام في الدولة كلها، بمنع الحركات الثورية، والمظاهرات، والتجمعات الخطرة في الطرق العامة على خلاف القانون. كما تلتزم الإدارة بالعمل علي توقي الكوارث العامة والتصدي لها حال حدوثها سواء كانت بفعل الطبيعة مثل الفيضانات والزلازل، أو كانت من صنع البشر كالجرائم مثل القتل والسرقة، فضلا عن المحافظة علي نظام المرور وحفظ البشر من الحيوانات الخطرة ....الخ.

٢- **الصحة العامة:** **'La salubrite publique**" تمثل الصحة العامة المظهر الثاني للنظام العام، ويقصد بها كل ما من شأنه أن يحفظ صحة الجمهور ويحميهم من أخطار الأمراض، ولهذا يقع على عاتق الإدارة مقاومة أسباب الأمراض باتخاذ الإجراءات الوقائية فيما يتعلق بمشرب الأفراد ومأكلهم ومسكنهم. إذ يجب على الإدارة أن تطعم الأفراد من الأمراض المعدية وأن تتخذ الإجراءات التي تمنع انتشارها وكذلك ضرورة مراقبة صلاحية الأغذية والتأكد من أن المحال العمومية تلتزم بالشروط الصحية.

٣- **السكينة العامة:** " **La tranquilite publique** " ويقصد بها المحافظة على حالة الهدوء والسكون في الطرق والأماكن العامة حتى لا يتعرض الأفراد لمضايقات الغير كالمتسولين أو من يستعملون مكبرات الصوت ...الخ. فهذه الأعمال ولو أنها لا ترقي إلى درجة الإخلال

---

(١) **c.E,18 decembre 1958,ste des films Lutetia,D 1960,171,note Weil.**

- **وخلاصة هذه القضية أن وزير الإعلام وافق على عرض أحد الأفلام السينمائية من قبل شركة لوتيتا بعد أن أجيز من قبل سلطة الرقابة، إلا أن عمدة المدينة المعنية والتي عرض فيها الفيلم أصدر أمرا بمنع عرض هذا الفيلم بسبب مخالفته للياقة والآداب العامة، لأن عرضه قد يثير الاضطرابات بسبب الطبيعة غير الأخلاقية للفيلم، حيث طعن بقرار المنع أمام القضاء الإداري، وقضى مجلس الدولة بأن من حق العمدة منع عرض الفيلم إذا تبين له بأن عرضه سوف يترتب عليه الإضرار بالنظام العام، وبذلك أضاف المجلس في حكمه، الآداب والأخلاق العامة إلى عناصر النظام العام لتصبح أربعة عناصر.**

بالنظام العام، إلا أنها قد تسبب مضايقات على درجة من الجسامة تستلزم تدخل الإدارة بناء على سلطات البوليس لإيقافها.

٤- **<u>الآداب والأخلاق العامة</u>:** توسعت أحكام مجلس الدولة الفرنسي الحديثة في مدلول النظام العام ليشمل المحافظة على النظام الأدبي، حيث قضت بشرعية قرار الإدارة بمنع عرض المطبوعات التي تصف الجرائم والفضائح في الأماكن العامة، كما قضت دائرة النقض الجنائية الفرنسية في حكمها الصادر في ١٨ يوليو ١٩٤١ بسلامة لائحة (بوليس) تحرم على النساء ارتداء ملابس الرجال، كما حكم مجلس الدولة الفرنسي بشرعية الإجراءات التي اتخذتها الإدارة لحماية أبناء المستعمرات من تأثير الخمور لأن ذلك يتعلق مباشرة بحماية النظام العام. [١]

ثانيا: مفهوم وخصائص التحول الرقمي: هناك العديد من التعريفات للتحول الرقمي نعرض للتعريف اللغوي ومن ثم المفهوم الاصطلاحي على النحو التالي:

١- مفهوم التحول الرقمي:

أ- المفهوم اللغوي:

التحول الرقمي هو مفهوم مركب مكون من شقين هما التحول والرقمي:

التحول في اللغة: تحوّل السيء أي تنقل من موضوع إلى موضوع آخر، أو من حال إلى حال، وتحول عن الشيء أي انصرف إلى غيره.

الرقمي: من الرقمنة وأصل الكلمة هي الرقم، والرقم هو العلامة، وفي علم الحساب هو الرمز المستعمل للتعبير عن أحد الأعداد البسيطة.

ب: مفهوم التحول الرقمي اصطلاحا:

التحول الرقمي Digital transformation or Digitization :بأنه استخدام المنظمة للتقنية في إدارة أعمالها وخدماتها وأنشطتها وفي معالجة وتحليل بياناتها وفي التواصل بين افرادها، وفي أداء تعاملاتها إلكترونيا بشكل كامل، ولابد أن يتم ذلك في بيئة تقنية أو رقمية، مؤمنة مستندة لقواعد بيانات محمية.[٢]

([١]) د/ سليمان محمد سليمان الطماوي: الضبط الإداري، دراسة مقارنة، مجلة الأمن والقانون، المجلد ١، العدد١، أكاديمية شرطة دبي، ١٩٩٣، ص ٢٧٥-٢٧٦.

([٢]) فاطمة الزهراء فرحات، دور التحول الرقمي في تحسين أداء وظائف العلاقات العامة في المؤسسات العمومية الجزائرية، دراسة تحليلية لصفحة فيسبوك مديرية الصحة والسكان لولاية أم البواقي، رسالة ماجستير، كلية العلوم الاجتماعية والإنسانية، جامعة العربي بن مهيدي- أم البواقي، الجزائر، ٢٠٢٠، ص ٦٣.

ويقصد به الاستثمار في الفكر وتغيير السلوك لإحداث تحول جذري في طريقة العمل، عن طريق الاستفادة من التطور التقني الكبير الحاصل لخدمة المستفيدين بشكل أسرع وأفضل.[١]

ويمكن تعريفه على أنه هو عملية الحصول على مجموعات النصوص الإلكترونية وإدارتها من خلال تحويل مصادر المعلومات المتاحة على وسائط تخزين تقليدية إلى صورة إلكترونية، وبالتالي يصبح المحتوى التقليدي محتوى رقمي يمكن الاطلاع عليه من خلال تطبيقات الحاسبات الآلية.[٢]

ويشير مفهوم "التحول الرقمي" إلى استخدام التكنولوجيا لدعم عمليات التغيير الجذري في العمليات المؤسسية.[٣]

كما أن هناك من عرف التحول الرقمي بأنه : "الانتقال من نظام تقليدي إلى نظام رقمي قائم على تكنولوجيا المعلومات والاتصالات في جميع مجالات العمل بالدولة، في ضوء مجموعة من المتطلبات المتمثلة في وضع استراتيجية للتحول الرقمي، ونشر ثقافة التحول الرقمي، وإدارة وتمويل التحول الرقمي، بالإضافة إلى المتطلبات البشرية، والتقنية، والأمنية، والتشريعية.[٤]

ومن خلال المفهوم السابق للتحول الرقمي يمكن استخلاص خصائص التحول الرقمي على النحو التالي:

٢- خصائص التحول الرقمي:

يساهم التحول الرقمي في تحقيق رفاهية المجتمعات والأفراد من خلال ما يوفره من خدمات متنوعة، وهو ما يوضح أهمية التحول الرقمي ودور في تسهيل عملية تبادل المعلومات والبيانات دون التعرض لحواجز مكانية أو زمانية ويعود هذا للخصائص التي يتميز بها التحول الرقمي ومن أهمها:

---

(1) https://www.my.gov.sa/wps/digitaltransformation , 1/1/2023.

(٢) أحمد فرج أحمد، الرقمنة داخل مؤسسات المعلومات أم خارجها؟ دراسة في الإشكاليات ومعايير الاختيار، مجلة دراسات المعلومات، تصدر عن جمعية المكتبات والمعلومات السعودية بالتعاون مع معهد الملك سلمان للدراسات والخدمات الاستشارية، العدد الرابع، يناير ٢٠٠٩، ص ١١.

(3)Maye, Terry & Others, Transforming Higher Education Through Technology-Enhanced Learning, The Higher Education Academy, York Science Park, Heslington, 2009,p11.

(٤) د/ مصطفى أحمد أمين، التحول الرقمي في الجامعات المصرية كمتطلب لتحقيق مجتمع المعرفة، مجلة الإدارة التربوية، العدد التاسع عشر، ٢٠١٨، ص٤٥.

- **التنوع في اشكال الاتصال المتاحة** من خلال وسيلة رقمية واحدة هي الحاسب الشخصي، والاختيار بين هذه الأشكال في الزمان والمكان الذي يحدده بناءا على حاجاته وظروفه الخاصة.
- **التنوع فب المحتوى الذي يختاره في المواقع** المختلفة المنتشرة على شبكة الانترنت سواء في وظائف هذا المحتوى أو مجالاته.
- **التكامل:** تمثل شبكة الانترنت مظلة اتصالية تجمع بين نظم الاتصال واشكالها، والوسائل الرقمية المختلفة والمحتوى بأشكاله في منظومة واحدة
- **توفر للمتلقي الخيارات المتعددة،** في اطار متكامل عن طريق توفير أساليب التعرض والاتاحة ووسائل التخزين بأسلوب متكامل خلال وقت التعرض على شبكة الانترنت ومواقعها المتعددة.[١]
- **تجاوز وحدتي المكان والزمان:** فالتحول الرقمي يتيح إمكانية الاتصال عن بعد وبالتالي لا يفترض فيه وجود عملية الاتصال في مكان واحد كما هو الاتصال بالمواجهة، والذي كان شرطا لتوفر عنصري المرونة والتفاعلية.
- **الاستغراق في عملية الاتصال:** من الخصائص المميزة للتحول الرقمي انخفاض تكلفة الاتصال أو الاستخدام نظرا لتوفر البنية الأساسية للاتصال وانتشار الأجهزة الرقمية، وكذلك تطور برامج المعلومات ونظم الاتصال بتكلفة زهيد مما يشجع المستخدمين لأجهزة الحاسب وبرامجه على الاستغراق في هذه البرامج بهدف التعلم لأوقات طويلة في إطار فردي، كما يساعد تطور برامج النصوص الفائقة والوسائل الفائقة على طول فترة التجول بين المعلومات والأفكار التي تتضمنها لأغراض اكتساب المعلومات أو التسلية، ولذلك فإن فترة استخدام الحاسب الآلي وبرامجه تفوق في كثير من الأحيان الوقت المستغرق في القراءة أو الاستمتاع أو المشاهدة، خصوصا بع أن أصبحت الشبكة العالمية مصدرا مضافا لعرض المواد الإعلامية التي تقدمها وسائل الإعلام على مواقعها في هذه الشبكة.[٢]

([١]) محمد عبد الحميد، نظريات الاعلام واتجاهات التأثير، ط٣، عالم الكتب، القاهرة، ٢٠٠٤، ص ١١٠-١١١.

([٢]) محمد عبد الحميد، المرجع السابق، ص ١١٥.

المطلب الثاني

مبررات التحول الرقمي

دفعت موجة التطور في مجال تكنولوجيا المعلومات والاتصال بجميع الدول للتحول نحو الإدارة الإلكترونية، تلبية لحاجة المواطنين إلى زيادة كفاءة الخدمات، ومواكبة التطور العالمي ومن أهم هذه الدوافع ما يلي:

- **تسارع التقدم التكنولوجي والثورة المعرفية المرتبطة به:** أدى إلى الرغبة في توظيف التكنولوجيا الحديثة لصالح المجتمع، وتمكينه من الحصول على فوائد كثيرة تساهم في تحسين أداء المؤسسات، وإتاحة الفرص للاستثمار في قطاع التكنولوجيا لتسهيل الحياة والاستفادة من المزايا التقنية المتوفرة على المستوى الدولي.
- **تطور الاتصالات:** في ظل الاتصالات الإلكترونية وجدت الإدارة نفسها في قلب الحدث العالمي وعلى اتصال مباشر بأطرافه مما يجعلها مطمئنة إلى صواب قراراتها وإجراءاتها مما يضعها على المحك على القرار العالمي بخصوص ما تتخذه من قرارات أو تنفذه من معاملات[١].
- **التحولات الديمقراطية:** وما رافقها من إصلاحات إدارية مطلوبة من كل دولة ترغب في الانضمام إلى منظمة التجارة العالمية أو تلبية مطالب جمعيات حقوق الإنسان المحلية والدولية.
- **أزمات القطاع العام:** كانت الخصخصة أول الخطوات التي سعى القطاع العام إلى التخفيف من الأعباء الإدارية وغرس ثقافة الترشيد في الوقت والموارد التي تتسرب في ظل عدم قدرة جهة الإدارة على السيطرة بيد أن بعض الإدارات الخدمية التي لا يمكن خصخصتها وجدت نفسها في مواجهة مباشرة ومقارنة غير متصفة مع إدارات مؤسسات القطاع الخاص التي وضعت قدمها في أرض التقنية واعتبرتها سبيلاً للسيطرة على مواردها وضبط عملية العمل بها، مما يمكنها من إعطاء قرارات صحيحة لموارد الإدارة الفعلية. لقد أصبحت التقنية معادلاً موضوعيا للترشيد في ظل الفكر الإداري الحديث سواء ترشيد نفقات أو ترشيد الأيدي العاملة الزائدة وتوجيهها إلى مواقع أخرى في حاجة إليها، كذلك أصبحت التقنية ملاذ لتلك الإدارات للتخلص من الصفوف الطويلة للمواطنين الذي يضع تلك الإدارات وموظفيها في ضغط مستمر وحرج كبير أمام الفئات المستهدفة فكانت التقنية البديل الأمثل. [٢]

([١]) محمد الطعامنة، طارق العلوش: الحكومة الإلكترونية وتطبيقاتها في الوطن العربي، المنظمة العربية للعلوم الإدارية، القاهرة، ٢٠٠٤، ص ٧٦.

([٢]) رأفت عبد الباقي رضوان: الإدارة الإلكترونية الإدارة والمتغيرات العالمية الجديدة، الملتقى الإداري الثاني، الجمعية السعودية للإدارة، الرياض، ١٦-١٧ محرم ١٤٢٥، ص ٥.

- **الحوار والتواصل:** الرغبة الشعبية للمجتمعات المعاصرة على الحوار الحضاري على نحو اجتماعي بين الشعوب شكلت عنصر دفع للجهات الإدارية إلى تطبيق تطبيقات التقنية بوصفها نافذة يطل منها على العالم ويتواصل إنسانيا ومعلوماتيا وإداريا بقدراتها وبوصفها أداة تواصل إلى جانب إنها أداء إنتاج.[١]

المطلب الثالث

أهمية التحول الرقمي

حفز التحول الرقمي انتقال المؤسسات من بيئة محلية داخلية إلى وضعية متميزة متكاملة مع البيئات الأخرى تولد انعكاسات مباشرة وتنتج نموا مستمرا. وبناء التميز يتطلب مساهمة جميع الفعاليات الوظيفية والإدارية والرقابية لإنتاج تفاعل طبيعي، وتحفيز متغيرات جذرية تنشئ حركية طوعية مستمرة وتولد نوعا من الاستقطاب الصحيح الذي يشغل قفزة انتقالية تؤدي إلى إدماج العديد من قطاعات الدولة. [٢]

وقد أطلق المنتدى الاقتصادي العالمي عام ٢٠١٥ مبادرة تسمى "مبادرة التحول الرقمي" The Digital Transformation Initiative (DT) مشروع أطلقه العالم كجزء من المبادرات المنظمة بشأن تشكيل المستقبل.[٣]

أهمية التحول الرقمي من الناحية العسكرية: أدي الاستخدام المكثف لتكنولوجيا المعلومات الجديدة في المجال العسكري إلى تعزيز القدرات القتالية للأسلحة التقليدية والتكنولوجيا العسكرية الأخرى، ولهذا السبب فإن العسكريين ينظرون إلى تكنولوجيا المعلومات والاتصالات على أنها سلاح وهدف في آن واحد. ففي نطاق المجال العسكري تعد العمليات التي تتم للحصول على تفوق المعلومات في نطاق حرب المعلومات.[٤]

---

(١) منال محمد الوكيل، تأثير الإدارة الإلكترونية على القرارات الإبداعية في المنظمات الحكومية مع دراسة تطبيقية على حي غرب مدينة نصر، المجلة العلمية لقطاع كليات التجارة، جامعة الأزهر، العدد ١٦، ٢٠١٦، ص ٦٤٦.

(٢) د/ محمد علي حسن شعلان، حوكمة التحول الرقمي في الرؤية السعودية ٢٠٣٠، مجلة المهندس، تصدر عن الهيئة السعودية للمهندسين، العدد ٩٩، ٢٠١٦، ص ٤٩.

(3)World Economic Forum , Digital Transformation Initiative Professional Services Industry, White Paper, Committed To Improving The State Of The World, January 2017, p2.

(٤) حمدون اتوريه، البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، ٢٠١١، ص٤٨.

أهمية التحول الرقمي من الناحية الاقتصادية: وعلى المستوى الاقتصادي، ساعدت تكنولوجيا المعلومات والاتصالات على الانتقال السريع نحو الاقتصاد الرقمي المبني على المعرفة، ودخلنا بذلك للعصر الرقمي، إذ يتم استخدام البرمجيات والتطبيقات الذكية لتحقيق نجاحات متعددة في ريادة الأعمال والإدارة، بالإضافة إلى تزايد استخدام الابتكارات التكنولوجية في قطاعات اقتصادية حيوية كالطاقة، السياحية، الخدمات المالية والمصرفية.

أهمية التحول الرقمي من الجوانب الاجتماعية والثقافية:

لقد أضفت التحول التكنولوجي بعدا إيجابيا جديدا على الملايين من البشر، وأحدثت تغييرات ثقافية واجتماعية وسياسية واقتصادية في حياة مجتمعات بأكملها. ومن أهم هذه الآثار الإيجابية:

• **تعزيز قيم المواطنة لدى الأفراد:** يمكن استخدام وسائل التواصل الاجتماعي كوسيلة إعلامية من الجهات المسؤولة بالدولة أو شخصيات المجتمع المؤثرة لإبراز الجوانب الإيجابية للوطن والتركيز عليها على نطاق واسع، وترسيخ المبادئ والقيم الوطنية بطريقة مباشرة أو غير مباشرة لدى شريحة كبيرة من مستخدمي هذه المواقع.

• **نافذة مطلة على العالم:** وجد الملايين من أبناء الشعوب الأجنبية والعربية في الشبكات الاجتماعية نافذة حرة لهم للاطلاع على أفكار وثقافات العالم بأسره.

• **فرصة لتعزيز الذات:** فمن لا يملك فرصة لإيجاد كيان مستقل في المجتمع يعبر به عن ذاته، فإنه عند التسجيل بمواقع التواصل الاجتماعي وتعبئة البيانات الشخصية، يصبح له كيان مستقل على الصعيد العالمي.

• **أكثر انفتاحا على الآخر:** إن التواصل مع الغير، سواء أكان ذلك الغير مختلفاً عنك في الدين والعقيدة والثقافة والعادات والتقاليد، واللون، والمظهر والميول، فإنك قد اكتسبت صديقا ذا هوية مختلفة عنك وقد يكون بالغرفة التي بجانبك أو على بعد آلاف الأميال في قارة أخرى.

• **منبر للرأي والرأي الآخر:** إن من أهم خصائص مواقع التواصل الاجتماعي سهولة التعديل على صفحاتها، وكذلك حرية إضافة المحتوى الذي يعبر عن الأفكار والمعتقدات التي قد تتعارض مع الغير، فالمجال مفتوح أمام حرية التعبير مما جعل مواقع التواصل الاجتماعي أداة قوية للتعبير عن الميول والاتجاهات والتوجهات الشخصية تجاه القضايا المختلفة.

• **التقليل من صراع الحضارات:** فقد تعزز مواقع التواصل الاجتماعي من ظاهرة العولمة الثقافية[1]

([1]) د.م ناصر محمد عبيد الساعدي، د/ هناء على محمد الضحوي، استراتيجية تعزيز المواطنة والاعتدال باستخدام وسائل التواصل الاجتماعي لمواجهة التحديات والتطرف والتكفير في دول مجلس التعاون الخليجي، بحث فائز بمسابقة جائزة الأمير خالد الفيصل للاعتدال، ٢٠١٧، ص ٢٦.

ومما سبق يتضح إن التحول الرقمي له العديد من الآثار الإيجابية على الصعيد العسكري، حيث ساعد على تعزيز القدرات العسكرية وزيادة كفاءة التسليح. وله أيضا العديد من الإيجابيات على الصعيد الثقافي والاجتماعي، إلا أنه في نفس الوقت له العديد من المخاطر التي قد تواجه المجتمع نتيجة للتزايد في استخدام تلك الوسائل التكنولوجية على النحو التالي.

المبحث الثاني

مخاطر التحول الرقمي التي تهدد النظام العام

لقد أدى التوسع في استخدام الفضاء السيبراني إلى ظهور العديد من المخاطر التي تواجه المجتمع في مختلف المجالات، فمنها مخاطر تهدد الأمن بجميع جوانبه، ولقد استعرضت استراتيجية مصر ٢٠١٧-٢٠٢١ بعض من هذه المخاطر التي سنعرضها على النحو التالي:

المطلب الأول

مخاطر التحول الرقمي من خلال استراتيجية مصر ٢٠١٧-٢٠٢١

حددت استراتيجية مصر ٢٠١٧- ٢٠٢١ أهم التحديات التي تواجه الأمن السيبراني فيما يلي:

١- خطر اختراق وتخريب البني التحتية للاتصالات وتكنولوجيا المعلومات:

ظهرت انماطا جديدة خطيرة للغاية من الهجمات السيبرانية تستهدف إعاقة الخدمات الحيوية، وكذلك نشر برمجيات خبيثة وفيروسات لتخريب أو تعطيل البني التحتية للاتصالات وتكنولوجيا المعلومات ونظم التحكم الصناعية الحيوية وخاصة في المرافق الهامة (منشآت الطاقة النووية والبترول والغاز الطبيعي والكهرباء والطيران والنقل بأنواعه وقواعد البيانات والمعلومات القومية والخدمات الحكومية والرعاية الصحية والاسعاف العاجل وغيرها)، وذلك عبر عدة قنوات تشمل الشبكات اللاسلكية والذاكرة النقالة بالإضافة إلى القنوات الأخرى الشائعة (البريد الالكتروني ومواقع الانترنت والشبكات الاجتماعية وشبكات الاتصالات السلكية)، مما يؤثر تأثيرا ملموسا على البني التحتية لتلك المنشآت والمرافق وعلى الخدمات والأعمال المرتبطة بها، وقد ثبت عمليا أنها ليست بمنأى عن التعرض للهجمات السيبرانية الشرسة حتي لو كانت غير متصلة بالإنترنت.[١]

٢- خطر سرقة الهوية الرقمية والبيانات الخاصة:

تعد سرقة الهوية الرقمية من أخطر الجرائم التي تهدد مستخدمي الانترنت ومستقبل الخدمات الالكترونية، حيث قد تتعرض البيانات الشخصية للمستخدم إلى السرقة بهدف انتحال شخصيته والاستيلاء على ممتلكاته وامواله أو للزج باسمه في تعاملات مشبوهة أو غير قانونية. وعادة ما يستعين سارق الهوية بمعلومات موجودة بالفعل علي الانترنت، وبخاصة علي مواقع شبكات التواصل الاجتماعية والمهنية المفتوحة أو قواعد البيانات والمعلومات القومية والشبكات الخاصة بالخدمات الحكومية وخدمات الضمان الاجتماعي وشبكات الرعاية الصحية ومواقع التجارة

---

(١) **الاستراتيجية الوطنية للأمن السيبراني في مصر ٢٠١٧-٢٠٢١**

الالكترونية والأسواق الافتراضية وشبكات المدفوعات الالكترونية والصرافات الآلية وبورصة الأوراق المالية، فضلا علي أنه قد تتعرض الأدوات والأنظمة المستخدمة في اجراء المعاملات الالكترونية للسرقة أو التخريب مما يشكل خطرا كبيرا علي مصالح المستخدمين ومستقبل الخدمات الالكترونية وقد تؤثر الهجمات الموسعة على القطاع المالي الوطني بوجه عام. كما قد تتعرض البيانات الخاصة بالمؤسسات العامة والشركات للسرقة مما يكبدها خسائر فادحة مادية وأدبية، فضلا عن الأضرار بسمعتها وخسارتها لعملائها وأصولها الأدبية، مما قد يضر بالاقتصاد الوطني بوجه عام.[١]

٣- خطر الارهاب والحرب السيبرانية

تزداد صعوبة توفير الأمن زيادة كبيرة في عالم بات يعتمد وبشكل متنامي على التكنولوجيا في كافة مناحي الحياة، وقد برهنت المجموعات الإرهابية على درايتها وسرعة تمكنها من التعامل مع تشكيلة عريضة من ابتكارات الاتصالات والتواصل الجديدة، من أبعد أركان الشبكة المظلمة إلى منصات التواصل الاجتماعي الشائعة المتاحة للجميع. وتسمح هذه الوسائل بالانتشار السريع للأفكار والتكتيكات والاستراتيجيات بوتيرة لم تكن ممكنة خلال العقود الماضية. ويضاف إلى ذلك استغلالها لنظم الرسائل المشفرة التي تعقد الجهود الرامية إلى تعقب الإرهابيين المشتبه فيهم، أو تحديد شركائهم وشبكاتهم واستراتيجياتهم.[٢]

انتشرت مؤخرا نوعية خطيرة من الهجمات والجرائم السيبرانية تعتمد علي تقنيات متقدمة(كالحوسبة السحابية والذكاء الاصطناعي وانترنت الأشياء)، وأجهزة تتصت علي شبكات الاتصال (السلكية واللاسلكية)، وبرمجيات لفك شفرة ولاختراق لأنظمة الشبكات والحاسبات وقواعد البيانات، وبرمجيات لتشفير العمليات المشبوهة، وبرمجيات خبيثة لاختراق أنظمة أمن الشبكات والحاسبات لتسخيرها في القيام بعمليات اجرامية وتعاملات مشبوهة دون علم أصحابها فيما يسمي بالشبكات الآلية، حيث يمكن أن تضم شبكة آلية واحدة عشرات أو مئات الألاف أو ملايين من الحواسب أو الأجهزة المتصلة بالإنترنت (انترنت الأشياء*) التي يمكن استخدامها

---

(١)الاستراتيجية الوطنية للأمن السيبراني في مصر ٢٠١٧-٢٠٢١

(٢) د/ سجان م. غوهيل & بيترك فوستر، المنهج المرجعي لمكافحة الإرهاب، ٢٠٢٠، الناتو،، ص ٥

*** يعتبر مفهوم إنترنت الأشياء IoT (Internet of Things) الجيل الجديد المتطور والمتنامي في شبكة الانترنت والذي يزيد من قدرة الأشياء المادية)الأدوات والأجهزة المختلفة التي تتميز بعنوان IP مخصص لها من الاتصال بشبكة الانترنت وتنظيم عملية التفاهم بين الأشياء المادية المترابطة مع بعضها والمتصلة عبر بروتوكول الانترنت. يمكِّن إنترنت الأشياء الإنسان من التحكّم بشكل فعاّل وسهل بالأشياء عن قرب وعن بُعد، فيستطيع المستخدم مثلاً تشغيل محرّك سيارته والتحكم فيها من جهازه الحاسوبي. يمكن الرجوع في ذلك إلى انترنت الأشياء على الموقع:**

لشن هجمات متنوعة، مثل الهجمات الموزعة لإعاقة الخدمات على شبكات ومواقع مستهدفة لأغراض اجرامية كالتخريب والإرهاب والتهديد والترهيب والابتزاز. وفي حين أنه من المرجح أن تطوير الفيروسات المعقدة والشرسة يتم علي مستوي متقدم ويستلزم منظومة خبرات مركبة لا تتوافر إلا في الدول المتقدمة تقنيا، وذلك لأغراض استراتيجية وحربية يمكن لتلك الدول استخدامها بدلا من(أو الي جانب) الهجمة العسكرية التقليدية فيما يسمي بالحروب السيبرانية، إلا أنه قد بدأ بالفعل نقل هذه الانماط واستنساخها من قبل التنظيمات الارهابية والتشكيلات العصابية الدولية للاستخدام في العمليات الارهابية وفي الجرائم المنظمة وفي تهديد وتعطيل البني التحتية للاتصالات والمعلومات، وبالتالي يتوقع العديد من الخبراء في مجال الأمن السيبراني تنامي انتشار الهجمات السيبرانية الشرسة في الفترة القادمة.

المطلب الثاني

مخاطر التحول الرقمي التي تهدد أمن واستقرار المجتمع

لم تعد القوة العسكرية وحدها هي المُهدد الوحيد للدول بل أصبح امتلاك الدول للقوة الإلكترونية يمثل خطراً أكبر على الدول المستهدفة ومن هنا جاء التحول في مفهوم الأمن، بحيث لم يعد أمن الدولة القومي مقتصر على الأمن العسكري بل أصبح هناك الأمن القومي السياسي، والذي يتلخص في المحتوى الأمني للبيانات الرقمية والمعلومات الإلكترونية التي تخص الأحزاب في الدولة إضافة للمعلومات التي تتعلق بالبرلمانات وأجهزة الدولة السيادية هي كلها معلومات حساسة قد يؤدي العبث بها لحروب أهلية داخل الدولة، وكذلك الأمن القومي الفكري والثقافي والذي يمثل ذروة الإنتاج الفكري لأي دولة والتي قد تساهم في رفع أو خفض مظاهر الأمن القومي للدولة، كالمظهر المادي المتعلق باستقرار المواطنين أو رفع الهواجس الأمنية في الدولة.

أولا: التهديدات العسكرية لأمن المجتمع

هناك العديد من التهديدات التي تستهدف المجتمع من الجانب العسكري ومنها الإرهاب السيبراني على النحو التالي:

---

https://ar.wikipedia.org/wiki/

أ- مفهوم الإرهاب السيبراني:

يعرف الإرهاب بصفة عامة أنه: استخدام طرق عنيفة كوسيلة الهدف منها نشر الرعب للإجبار على اتخاذ موقف معين أو الامتناع عن موقف معين. ومن هذا التعريف يتضح أن ملامح جريمة الإرهاب تختلف عن غيرها من الجرائم حيث أنها وسيلة وليست غاية، والوسائل المستخدمة عديدة ومتنوعة، وتتميز بطابع العنف وتخلق حالة من الفزع والخوف، وغالباً ما يكون الدافع من وراء جرائم الإرهاب المشاكل السياسية أو أن هناك فريقان مختلفان.[١]

ب-صور الإرهاب السيبراني:

يشمل الإرهاب السيبراني أي نشاط إجرامي يتم من خلال شبكة الإنترنت بهدف بث الأفكار المتطرفة، سواء كانت سياسية أو دينية أو عنصرية للسيطرة على وجدان الأفراد، وإفساد عقائدهم، وإذكاء تمردهم، واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصالح المجتمع.[٢]

١- استهداف النظم العسكرية

تستهدف هذه النوعية من الهجمات عادة الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات، من خلال سرقة المعلومات والبيانات العسكرية أو التلاعب بها وتعد هذه من أخطر الهجمات. ويتم من خلالها نقل كميات هائلة من المعلومات عبر شبكات المعلومات بصورة يومية، وتتميز كثير من هذه المعلومات بكونها على درجة كبيرة من الأهمية. وعلى الرغم من استخدام أجهزة تشفير تتولى تشفير الوسائل والمعلومات المهمة عند إرسالها وفك شفرتها عند استقبالها، إلا أن الاستيلاء على المعلومات التي يتم نقلها عبر شبكات المعلومات قد أصبح يشكل خراً كبيراً يهدد أمن وسلامة هذه المعلومات.[٣]

يعد هذا النوع من التهديدات من أخطر نماذج الإرهاب ومن أبرز السيناريوهات المحتملة التي تواجه المجتمع وتبدأ في مراحلها الأولى باختراق المنظومة الأمنية المتعلقة بالأسلحة الاستراتيجية ونظم الدفاع الجوي والصواريخ النووية وقد تقوم الجماعات الإرهابية بفك الشفرات السرية للتحكم في تشغيل منصات إطلاق الصواريخ الاستراتيجية مما يؤدى إلى خسائر فادحة ويقلل من قدرات الدولة العسكرية وحماية أراضيها ومنشآتها الحيوية ومواطنيها.

ويرجع السبب في شن تلك الهجمات لما تتميز به الحرب السيبرانية من خصائص تؤثر على البنية التحتية للمنشآت الحيوية، نتيجة اعتماد منشآت الطاقة والكهرباء على النظم المتقدمة في

---

(١) د أحمد محمد رفعت، الإرهاب الدولي، دار النهضة العربية، عام ٢٠٠٦، بدون رقم طبعة، ص ٢٢٦ وما بعدها.

(٢) د/ حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، ٢٠٠٦، ص ٥٤.

(٣) أميرة عبد العظيم محمد عبد الجواد، مرجع سابق ٤٣٢.

المعلومات. ولا يلقى هذا النمط الجديد من الصراع تنديدا دوليا مثل الهجوم التقليدي، وتتميز تلك الهجمات أنها سريعة الانتشار ورخيصة التكلفة وعدم معلومية مصدر الهجوم مما يؤدي إلى ارتباك الخصم وقد تتم تلك الهجمات عبر الشبكات عابرة الحدود الدولية.

١. **التجسس السيبراني:** يقصد به تلك المحاولات المتعمدة لاختراق أجهزة الكمبيوتر والمواقع الإلكترونية التابعة للدولة المناوئة أو الخصم بهدف سرقة معلومات سرية[١]، حيث أن التجسس المعتمد على المجال السيبراني يؤثر سلبا على المعلومات وأنظمة المعلومات، مما يتيح إمكانية تسريب أسرار ومعلومات حساسة للدول الأخرى[٢]

٢. **التحريض على ارتكاب اعمال عنف:** ومن أبرز نماذج الإرهاب السيبراني هو تحريض الجماعات الإرهابية على ارتكاب أعمال إرهابية تتعلق بالعنف. ومن أبرز القضايا في هذا الشأن: قضية الولايات المتحدة الأمريكية ضد إيمرسون وينفيلد بيغولي. فقد تم أتهام طالب أمريكي في الثانية والعشرين من عمره، بالضلوع في نشر معلومات على شبكة الإنترنت متعلقة بصنع القنابل والتحريض على ارتكاب أعمال عنف وجرائم أخرى. وكان إيمرسون يعرف باسم مستعار " أسد الله الشيشاني "، له دور نشط في المنتدى الجهادي المعروف دولياً والمسمى باللغة الإنجليزية " شبكة أنصار المجاهدين " وقد شارك في إدارته وعبر عن وجهة نظره المتطرفة، وقام بتشجيع الزائرين على ارتكاب أعمال إرهابية ضد الولايات المتحدة الأمريكية، ونشر أشرطة تحتوي على فيديوهات تبث كيفية تعلم صنع المتفجرات وقد وجهت إليه المحكمة المحلية الأمريكية للدائرة الشرقية بولاية فرجينيا في ١٤ يوليه عام ٢٠١١ عدة تهم منها النشر على المنتدى الإلكتروني عبارات تدعو إلى الإرهاب. [٣]

ثانيا التهديدات الاجتماعية والثقافية والأخلاقية لأمن المجتمع

على الرغم من الكثير من الإيجابيات التي أسهمت في تحقيقها التكنولوجيا الرقمية والتي أدت إلى مزيد من التقدم، فإن الواقع يبرز العديد من السلبيات، حيث أفرز العديد من المشكلات والآثار السلبية؛ كطمس الثقافات القومية والقضاءِ على خصوصياتها وفرضِ ثقافات دخيلة لشعوب معينة، وانتشار الممارسات السيئة لاستخدام التكنولوجيا بين الأفراد؛ مثل نشر المعلومات

---

(١) شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب "التفجير من الداخل" على الساحة الدولية، العربي للنشر والتوزيع، القاهرة، 2019، ص ١٠٦

(٢) شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد ١٥، العدد ٠١، ٢٠٢٢، ص ٢٩٥.

(٣) مكتب الأمم المتحدة المعنى بالمخدرات والجريمة، استخدام الإنترنت في أغراض إرهابية، بالتعاون مع فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ تدابير مكافحة الإرهاب، نيويورك، عام ٢٠١٣، ص ٤٠.

المضللة، أو الغريدات المسيئة، أو الدخول على المواقع الإلكترونية غيرِ اللائقة وغيرِ غير الأخلاقية، أو المواقع التي تتضمن محتويات وتيارات فكرية ضارة للمواطنة والهوية الثقافية. [١]

وتمتاز الهجمات المعلوماتية بالشراسة التي تمكن أن تمزق النسيج الاجتماعي للبلد، والقوة البلغة على إلحاق أضرار مادية واسعة.

تتجسد في تأثير المخاطر والتهديدات السيبرانية في تشكيل بنية المجتمع ومنها زيادة الجرائم المستحدثة، تهديد البنى التحتية، تهديد القيم والأخلاق، استهداف الأمن القومي، تصدير الأزمات. ويمكن توضيح ذلك على النحو التالي:

١- استحداث الجرائم السيبرانية وزيادة معدلاتها

أدى الاعتماد المتزايد في الحياة اليومية على الأنظمة المعلوماتية والأجهزة المتصلة بالإنترنت، وتشعب طبيعة تلك الأجهزة من هواتف خلوية، وأجهزة حوسبة شخصية، وكذلك تزايد عدد المتصلين بالفضاء السيبراني، كل ذلك أدى إلى تزايد احتمالا الاعتداءات وزيادة معدلات الجرائم.

٢- تهديد القيم والأخلاق

تؤدي التهديدات الاجتماعية السيبرانية إلى تدني المستويين القيمي والأخلاقي من خلال المحتويات غير المشروعة وغير المرغوب بها ذات تأثير سلبي على اخلاقيات المجتمع وعلى ارتفاع نسبة الممارسات الإجرامية كالإباحية، والترويج للإتجار بالممنوعات والدعارة والإرهاب [٢]

المطلب الثالث

تهديدات الصحة العامة للمجتمع

شهد العقد الماضي طفرة في استخدام التكنولوجيات الرقمية الجديدة داخل بيئات الرعاية الصحية كافة، ما أدى إلى إحداث تحسن كبير في إتاحة الوصول إليها وخدمات الرعاية المقدمة فيها. وبفضل هذه التكنولوجيات، أصبح في وسعنا جمع كم هائل من المعلومات ستسهم بلا شك في صياغة مستقبل جديد للرعاية الصحية وإدخال تحسينات جذرية على النتائج الصحية في جميع أنحاء العالم.

إلا أن ثمة واحد من أبرز التحديات في هذا السياق، ألا وهو كيفية الحفاظ على سلامة هذه البيانات وأمنها بما يضمن استمرار ثقة المرضى والجمهور في مؤسسات الرعاية الصحية

---

(١) محمد عبد البديع السيد، دور وسائل الإعلام الجديدة في دعم المواطنة الرقمية لدى طلاب الجامعة، مجلة بحوث العلاقات العامة، جامعة بنها، العدد ١٢، ٢٠١٦، ص ١٢٣.

(٢) اسلام فوزي، الأمن السيبراني: الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي، المجلة الاجتماعية القومية، المجلد السادس والخمسون، العدد الثاني، ٢٠١٩، ص ١١٢

التي تحتفظ بمعلومات غاية في السرية عن أنفسهم وعائلاتهم. وليس أيسر من فقدان هذه الثقة عندما نتساهل في حماية الأنظمة الأساسية أو عند ضياع البيانات الشخصية للأفراد.[١]

ولا يتوقف الأمر عند هذا الحد، حيث إن هناك الكثير من الأهداف الأخرى، التي يمكن استهدافها لإحداث الفوضى في الحياة المدنية. فهناك مثلاً شبكات المعلومات الطبية، والتي يمكن لمهاجمتها، واختراقها ومن ثم التلاعب بها أن يؤدي إلى خسائر في أرواح المرضى من المدنيين. كأن يتم النفاذ إلى سجلات المستشفيات والتلاعب بسجلات بها بشكل يؤدى إلى حقن هؤلاء بأدوية وعلاجات كانت مميتة بالنسبة لهم. حتى لو افترضنا أن شبكة المعلوماتية الخاصة بالمؤسسات الطبية منيعة، فإن رسالة واحدة تنشر مثلاً بالبريد السيبراني، مفادها أن هناك دماء ملوثة في المستشفيات وما إلى ذلك، يمكن لها أن تحدث آثاراً مدمرة على الصعيد الاجتماعي.[٢]

قد تخلف الجرائم السيبرانية في قطاع الرعاية الصحية تداعيات خطيرة على سلامة المرضى. ومع ذلك، فقد تبين ضعف جاهزية القطاع للجرائم السيبرانية وفق ما ورد رغم أنه أكثر ضعفًا أمامها مقارنة بغيره من القطاعات الحيوية. ويرجع السبب في ذلك إلى عدم وجود ما يضمن توفير التمويل اللازم للأمن السيبراني لا سيما الموجه للنظم الصحية في القطاع العام. ففي المملكة المتحدة مثلًا، لا تنفق كثير من صناديق هيئة الخدمات الصحية الوطنية إلا ١ إلى ٢% من ميزانيتها السنوية على البنية التحتية لتكنولوجيا المعلومات، مقارنة ب ٤ إلى ١٠ % في القطاعات الأخرى) مثل قطاعي التمويل والاتصالات

ويزداد الوضع صعوبة في الدول ذات الدخل المنخفض والمتوسط من حيث تمويل الأمن السيبراني في قطاع الرعاية الصحية، حيث تخصص الحكومات نسبة أقل من ناتجها المحلي الإجمالي لصالح قطاع الصحة بأكمله، فلا يتبقى سوى موارد زهيدة تخصص لأمن البيانات وبناء أنظمة صحية سيبرانية متينة. ونجد كذلك في هذه الفئة من الدول أن التبرعات تشكل أكثر من خمس التمويل الذي يتلقاه قطاع الصحة، ويتم توجيه الغالب الأعم من هذه الميزانيات لأمراض أو مبادرات بعينها وليس لترسيخ إدارة النظام الصحي أو بنيته التحتية.

---

(١) جاي مارتن& وآخرون، حماية نظم الرعاية الصحية، إطار عالمي للأمن السيبراني، تقرير شبكة الأنظمة الصحية الرائدة ٢٠٢٠، تقرير إليكتروني، معهد الابتكار في مجال الصحة العالمية في إمبريال كوليدج لندن، ٢٠٢٠،ص ٣.

(٢)د/ عادل عبد الصادق، القوة الالكترونية، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، قوانين وتشريعات، إصدارات مكتبة الإسكندرية، العدد ٢٣، ٢٠١٦ص ١١.

ارتفع عدد الهجمات السيبرانية الموجهة ضد مؤسسات الرعاية الصحية وزادت حدتها بدرجة كبيرة في جميع أنحاء العالم خلال العقد الماضي. [١]وثمة هجمات بعينها أسفرت عن تعطيل المؤسسات بشكل كبير، مما أدى إلى تعرضها لخسارات مالية وتعريض سلامة المرضى للخطر، ومن أمثلة تلك الهجمات ما يلي:

- **هجوم واناكراي مايو ٢٠١٧ على هيئة الخدمات الصحية الوطنية البريطانية***: أدى إلى حظر الوصول للأنظمة، مما منع الموظفين من الوصول إلى بيانات المرضى والخدمات الحيوية. ألغيت آلاف المواعيد والعمليات الجراحية.١٩
- **الهجوم على مجموعة سنغافورة للخدمات الصحية يونيو ٢٠١٨:** حيث تم سرقة البيانات الشخصية ل ١,٥ مليون مريض، بما في ذلك الوصفات الطبية لرئيس الوزراء لي هسين لونج.[٢]
- **الهجوم على النظام الصحي لمجمع مستشفيات درويد والمراكز الطبية الإقليمية (في الولايات المتحدة الأمريكية) ٢٠١٩:** حيث توقفت رعاية المرضى من ذوي الحالات غير الحرجة لمدة ١٠ أيام. تم دفع مبلغ فدية للمهاجمين لم يكشف عن حجمه لفك شفرة الملفات والسماح باستئناف الخدمات.[٣]

([1]) Ghafur S, et al. Improving Cyber Security in the NHS. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf

*** هيئة الخدمات الصحية الوطنية (بالإنجليزية: National Health System) وتختصر NHS «إن إتش إس» هي نظام تقديم الخدمات الصحية للمواطنين في إنكلترا وهو ممول من قبل العامة، ويجب عدم خلطها مع أجهزة الصحة الوطنية الثلاثة الأخرى التي تعمل عبر المملكة المتحدة في مقاطعاتها الخاصة ضمن حكوماتها الخاصة والتي طورت قوانين تختلف بعض الشيء عن بعضها البعض. أجهزة الخدمات الأربع تقدم خدمات من دون اختلاف في الحقوق لمواطني المقاطعات الأخرى كمقاطعاتهم.**

([2]) Tham I, et al. Sing Health cyber-attack: How it unfolded. The Straits Times, 20 July 2018: https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/ sg-cyber-breach/index.html

([3]) Eddy N. Alabama hospital system DCH pays to restore systems after ransomware attack. Healthcare IT News; 7 October 2019. www.healthcareitnews.com/news/alabama-hospital-system-dch-pays-restore-systems-after-ransomware-attack

- **الهجوم على عمليات تشغيل مجموعة لايف هيلث كير الجنوب إفريقية عام ٢٠٢٠:** أثر الهجوم على أنظمة دخول المرضى ومعالجة الأعمال، بالإضافة إلى خوادم البريد الإلكتروني، مما أدى إلى حدوث تأخيرات إدارية في خدمات المرضى.[١]

ومما سبق يتضح أن هناك علاقة وثيقة بين سلامة المرضى والأمن السيبراني، حيث أثبتت التداعيات الناجمة عن الهجوم السيبراني في المجال الصحي لها تأثير كبير على إمكانية وصول المرضى لخدمات الرعاية الصحية وتوقيتها المناسب، مما يهدد عنصر أساسي من عناصر النظام العام ألا وهو الصحة العامة.

([1]) **Miles R. Life Healthcare announces cyberattack. Intelligent CISO, 11 June 2020.**

www.intelligentciso.com/2020/06/11/life-healthcare-announces-cyberattack/

المبحث الثالث

متطلبات تحقيق التحول الرقمي

ترتبط السياسات الرقمية بالتحول الرقمي ارتباطًا وثيقًا، فالعلاقة بينهما لا تنفصل عراها؛ فإذا كان التحول الرقمي يسعى إلى تغيير طرق الإدارة التقليدية ونظمها بحيث تعتمد على التكنولوجيا الرقمية، بالشكل الذي يقود إلى تقديم الخدمات بشكل أيسر وأسرع وأسهل؛ فإن عملية صنع السياسات الرقمية تستهدف تحقيق هذا التحول بشكل فاعل ورصين. إن عملية التحول الرقمي في كل القطاعات ليست من السهولة بمكان، فهي بحاجة إلى سياسات اجتماعية رصينة، تلعب أدوارًا في هذا التحول، وتراعي عددًا من الأبعاد المهمة منها:

أولا: التطور المستمر للبنية التحتية: تحتاج التحولات الرقمية إلى بنية تحتية قوية، تسمح بإجراء العمليات التي تتم في إطارها، وذلك على مستوى البنية التحتية المرتبطة بالكابلات والكهرباء، والبنية التحتية الرقمية المتعلقة بالشبكات والتطبيقات، وهذه المسألة تحتاج إلى تخطيط استراتيجي يخرج من رحم سياسات اجتماعية رصينة، بحيث تقوم هذه السياسات بتحديد التقنيات التي يمكن التعامل من خلالها مع السحائب الإلكترونية، وإنترنت الأشياء والذكاء الاصطناعي، وكلها أمور مهمة من أجل تحقيق التحول الرقمي الفعَّال، فالمراد في هذا الصدد أن تقوم السياسات الرقمية بتبني رؤى تسعى ليس إلى توفير البنية التحتية فقط، ولكنها تستهدف مواكبة التطورات التقنية التي تطرأ على هذا الأمر، والاستمرار في هذا التطوير من أجل تحول رقمي آمن.[١]

ثانيا: السعي نحو تحقيق العدالة الرقمية: يرتبط ذلك بتحقيق قدر من العدالة الرقمية، حيث توفير سبل النفاذ إلى الشبكة لجميع المواطنين بأيسر السبل، وتعني العدالة الرقمية ببساطة بتوفير مساحة آمنة لجميع الفئات للتعامل مع المنظومة العامة للتحول الرقمي، فهي توفر –على نطاق واسع– عدالة الوصول إلى الخدمات الرقمية لجميع المواطنين دون تمييز، وفي سبيل ذلك لابد من توافر ثلاثة شروط: أولها يتمثل في توزيع عملية النفاذ والوصول إلى الخدمات الرقمية المقدمة، وثانيها يتمثل في الاعتراف بالتنوع داخل سياقات الرقمنة، وثالثها يتمثّل في المشاركة في المساحات المختلفة من الرقمنة، وبذلك تعد العدالة الرقمية من أهم مقومات السعي نحو تحول رقمي بنَّاء.[٢]

---

(١) د/ وليد رشاد زكي، السياسات الرقمية وترشيد صناعة القرار، إصدارات مركز المعلومات ودعم اتخاذ القرار، رئاسة مجلس الوزراء، ٢٠٢١، ص ٦.

(2)Kretschmer Tobias and Khashabi Pooyan, Digital Transformation and Organization Design: An Integrated Approach, California Management Review, Vol. 62(4) 86–104, 2020, p 87.

ثالثا: القضاء على الأمية الرقمية: من الأدوار المهمة عند صناعة السياسات الرقمية القضاء على الأمية الرقمية، بحيث يتم توفير السبل للمواطنين للوصول إلى الخدمات الرقمية، ويقصد بالأمية الرقمية «الافتقاد إلى مجموعة المهارات والمعارف والمواقف المطلوبة للوصول إلى المعلومات الرقمية، واستخدامها، وتقييمها بشكل فعَّال وكفاءة أخلاقية »، فمما لا شك فيه أن الأمية الرقمية تمثِّل حاجزًا كبيرًا للعبور إلى التحول الرقمي المطلوب، لذلك على السياسات الرقمية أن تفطن إلى هذا الأمر جيدًا، وللقضاء على الأمية الرقمية يجب التركيز على ثلاثة محاور أساسية:

يتمثّل الأول: في التعرف على مهارات تشغيل التقنيات الرقمية واستخدامها، مثل أجهزة الكمبيوتر، والأجهزة اللوحية، والهواتف الذكية، والثاني: مرتبط بمهارات الوصول إلى استخدام خدمات الحكومة الرقمية، ويتحدد

الثالث: في تقييم الخدمات الرقمية، وليس المقصود بالتقييم هنا التقييم الهدَّام، ولكن التقييم الذي يقود إلى تحسين الخدمات المقدمة للجمهور.[١]

رابعا: تحقيق الأمن السيبراني: يتحدد الأمن السيبراني في حماية الأفراد والجماعات والدول عبر الشبكة من التهديدات المحيطة بهم، وينقسم الأمن في هذا السياق إلى ثلاثة مستويات: الأول أمن الأفراد والمتعلق بالخصوصية وانتهاكها، وسرقة الحسابات الشخصية، بل وصل الأمر إلى تهديد الحياة الآمنة عبر اختراق الجسد عبر الإنترنت فيما يعرف بقضايا أمن إنترنت الأشياء internet of things، أما المستوى الثاني فهو المستوى المرتبط بالمؤسسات والتنظيمات، فثمّة تهديدات أمنية على أنظمة الشركات والمؤسسات واختراق خصوصيتها وأمنها المعلوماتي، بالشكل الذي يهدد المكاسب المرتبطة بها، أما المستوى الثالث فهو المستوى المرتبط بأمن المجتمعات نفسها؛[٢] حيث زاد الحديث عن مفاهيم جديدة مثل الإرهاب السيبراني، وهو نمطان: الأول مرتبط باستخدام الميديا الجديدة في حشد الأفراد وتعبئتهم وتجنيدهم، والتجسس... وغيرها، والثاني مرتبط بالإرهاب عبر الشبكة مثل اختراق الحواسيب الخاصة بالدول كالمستشفيات، ومحطات الطاقة، والمؤسسات العسكرية... وغيرها. وكلها تثير مجموعة من المشكلات الخاصة بأمن المجتمعات، هنا وجب عند وضع السياسات الرقمية التركيز بشكل كبير على تحقيق الأمن السيبراني على كل مستوياته

([1]) La Rose Tara and Detlor Brian, Research on Social Work Practice, 20(10, 2021, PP1-11.

([٢]) د/ وليد رشاد زكي، من الأمن الصحي إلى الأمن السيبراني، الأمن والحياة، جامعة نايف للعلوم الأمنية، المملكة العربية السعودية، 2020، العدد ٤٣٣، ص ٩٨.

الفصل الثاني

الإطار الدستوري للأمن السيبراني

وأثره على الدولة وحقوق الانسان

تعتمد المجتمعات الحديثة بشكل متنامي على تكنولوجيا الاتصالات والمعلومات المتصلة بالشبكة العالمية، غير أن هذا الاعتماد المطرد ترافقه مجموعة من المخاطر الناشئة والمحتملة التي تهدد وبشكل أساسي الشبكات وأمن المعلومات والمجتمع المعلوماتي وأعضاءه، حيث أن سوء الاستغلال اليومي للشبكات الإلكترونية لأهداف إجرامية يؤثر سلبا على سلامة البنى التحتية للمعلومات الوطنية الحساسة في كافة المجالات مما ينعكس على النظام العام بعناصره المختلفة، وهو ما جعل الأمن السيبراني يشكل جزء أساسيا من سياسة أمنية وطنية. وسوف نتناول ذلك على النحو التالي:

المبحث الأول: مفهوم وأهمية وأهداف الأمن السيبراني.

المبحث الثاني: الحماية الدستورية للحقوق الرقمية والأمن السيبراني

المبحث الثالث: دور الأمن السيبراني الحفاظ على سيادة الدولة ومتطلبات تحقيقه.

المبحث الأول

مفهوم وأهمية وأهداف الأمن السيبراني

يعتمد الفضاء المعلومات على نظم الكمبيوتر وشبكات الانترنت* ومخزون هائل من البيانات والمعلومات، بحيث يتم الاتصال بالشبكات غير الحواسيب أو الهواتف أو غيرها من دون التقيد بالحدود الجغرافية، ومن ثم فلقد أصبح الأمن السيبراني ركزة أساسية في كل المنظمات والمؤسسات بل وحتى الدول لموجهة الحروب الإلكترونية، ولذلك سوف نتناول التطور التاريخي للإنترنت والأمن السيبراني ومن ثم مفهوم الأمن السيبراني وبعد ذلك نبين أهم خصائصه على النحو التالي

المطلب الأول

مفهوم الأمن السيبراني والمفاهيم ذات العلاقة

ظهر مصطلح الفضاء السيبراني في ثمانينات القرن الماضي، ويعبر الأمن السيبراني عن ممارسات دقيقة لحماية الشبكات والأجهزة والبيانات من التلف أو الضياع أو السرقة أو الوصول غير المصرح به، وبذلك فإن الأمن السيبراني يحمي التقنيات الرقمية ومستخدميها من المخاطر الرقمية، من ثم فإن أصبح الأمن السيبراني ركزة أساسية في كل المنظمات والمؤسسات بل وحتى الدول لموجهة الحروب الإلكترونية، ولذلك سوف نتناول مفهوم الأمن السيبراني وبعد ذلك نبين أهم خصائصه على النحو التالي

أولا :المفهوم اللغوي للأمن السيبراني:

يتكون مفهوم الأمن السيبراني من كلمتي (الأمن) والسيبراني. فالأمن هو نقيض الخوف، أي بمعنى السلامة، والأمن مصدر الفعل أمن أمنا وأمانا وأمنة أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال أمن من الشر أي سلم منه.

كلمة السيبرانية، مشتقة من الكلمة اللاتينية" سايبر " Cyber" ومعناها تخيلي أو افتراضي، والسيبر كلمة يجري استخدامها لوصف الفضاء الذي يضم الشبكات العنكبوتية المحوسبة، ومنظومات الاتصال والمعلومات وأنظمة التحكم عن بعد. وتعني: كل ما يتعلق أو يرتبط

*** يرجع إنشاء الإنترنت في بادئ الأمر في الستينات من القرن الماضي نتاجًا لمشروع ARPA NET)) وكان ذلك بهدف تأمين شبكة اتصال خاصة لا يمكن إتلافها أو تدميرها في حال حدوث عمليات تخريب أو نشوب حرب مفاجئة وعهدت وزارة الدفاع بهذه المهمة إلى وكالة مشاريع الأبحاث المُتقدمة القادرة على مقاومة الكوارث والاستمرار في العمل في حالة حدوث هجوم. يمكن الرجوع في ذلك إلى:**

حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت "دراسة مقارنة "، رسالة قدمت لنيلِ درجة الدكتوراه في القانون من جامعة عين شمس، عام ٢٠٠٧ م، ص ١٢

بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، ومنها اشتقت صفة السيبرانية والسيبراني Cyberneticsوتعني علم التحكم الأوتوماتيكي، أو علم الضبط، كما تعني أيضا القيادة أو التوجيه، والذي يعني: "علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية[١]

ثانيا: المفهوم الاصطلاحي للأمن السيبراني:Cyber Security concept

يعد الأمن الفضائي السيبراني مجموع القواعد التي يضعها مسؤولو الأمن في أي مكان والتي يجب أن يتقيد بها جميع الاشخاص الذين يمكنهم الوصول إليه، فمفهوم الأمن مفهوم واسع يطال جميع عمليات الدخول والخروج والبقاء أو التصرف في مكان ما، وعليه يشمل الأمن في الفضاء السيبرني قواعد واصول ضبط الاتصال وانتقال المعلومات وتخزينها وحفظها، كما يشمل أمن المواقع وأمن الأنظمة الالكترونية وعمليات استثمارها اضافة الى أمن الاتصالات.[٢]

كما يمكن تعريفه بأنه مجموعة الأساليب التفاعلية التي يتم فيها تخصيص الموارد لحماية الأنظمة من التهديدات الالكترونية.[٣]

أو هو التقنيات والإجراءات التي تهدف إلى حماية أجهزة الكمبيوتر والشبكات والبيانات من الدخول غي القانوني ونقاط الضعف والهجمات المنقولة عبر الإنترنت نت قبل الجانحين.[٤]

يمكن تعريف الأمن الالكتروني بأنه: حماية البيانات الالكترونية والشبكات الالكترونية، وكذلك الاشخاص الذين يستخدمونها من أولئك الذين يعتزمون ممارسة الأذى أو الضرر أو السرقة أو المضايقة أو الأعمال المماثلة.[٥]

تعريف وزارة الدفاع الأمريكية تعريفا دقيقا للأمن السيبراني حيث اعتبرته" جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الجرائم، والهجمات، والتخريب والتجسس والحوادث.[١]

---

(١) منير البعلبكي، المورد قاموس إنكليزي عربي، دار العلم للملايين، بيروت، ٢٠٠٤، ص ٢٤٣& قاموس أكسفورد على الموقع: https: //en. oxforddictionaries. com/definition/cyber

(٢) يونس مؤيد يونس، استراتيجية الولايات المتحدة الامريكية لأمن السيبراني، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، بغداد، العدد ٥٥، ٢٠١٨، ص ١.

(3) Abdurrahman, O., & Omar, I. M.و The Impact of Applying Electronic Management System on the English Language Level: A Case study at Cihan University. International Journal of Research and Engineering, 5(7), 2018,p 457-464.

(4)K. K. Panigrahi, Information Security and Cyber Law , published by tutorials point ,2015 ,p.1.

(٥) جون باسيت، الحروب المستقبلية في القرن الحادي والعشرين، مركز الامارات للدراسات والبحوث الاستراتيجية أبو ظبي الامارات ٢٠١٤، ص ٥.

فالأمن السيبراني هو مزيج من العمليات والتقنيات تهدف إلى حماية البرامج والتطبيقات والشبكات وأجهزة الكمبيوتر والبيانات من الهجوم، ويشمل الأمن السيبراني الأمن المادي للشبكات وأجهزة الحاسب الآلي، وأمن غير مادي يتعلق بالبرامج والمعلومات والبيانات من أي هجوم وأضرار متعمدة والتحكم في الوصول الصحيح للأجهزة والشبكات لحمايتها من الضرر.[٢]

ويعرف البعض الأمن السيبراني بأنه: " عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة"[٣].

يتضح مما سبق بأن الأمن السيبراني مجموعة من التدابير والإجراءات التي تم تصميمها وتطبيقها لحماية الأنظمة الإلكترونية في الدولة والمعلومات الحساسة من الهجمات والتهديدات الالكترونية سواء كانت تلك التهديدات تنشأ من داخل أو خارج الدولة.

ثالثا: **خصائص الأمن السيبراني:** يتميز الأمن السيبراني بعدة سمات ومن أهمها:

- الأمن السيبراني ليس مسار عمل لمرة واحدة؛ إنما هو عملية مستمرة ويحتوي على آليات دفاع مبتكرة لكونه يواجه التهديدات التي تقع على الأنظمة والشبكات وغيرها.
- يعمل على خلق نظام بيئي سيبراني آمن وإنشاء نظام موثوق به.
- يقوم بعملية وقائية رقابية مسبقة بهدف البحث عن المخاطر والعمل على حلها وسد الثغرات.
- يعمل على الدفاع اللاحق والذي يتمثل في قاعدة إرجاع الوضع إلى ما كان عليه.
- يوفر خاصية التنبيه إلى وجود خطأ أو إساءة استخدام الشبكات التي تعرض البيانات والمعلومات إلى الخطر من داخل المؤسسات. وأيضاً تغطية المخاطر الخارجية ومراقبة التهديدات[٤]

رابعا: المفاهيم المرتبطة بالأمن السيبراني، هناك العديد من المفاهيم المرتبطة به ومن أهمها ما يلي:

<u>الفضاء السيبراني Cyberspace :</u>عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأنه: "فضاء التواصل المشكل من خلال الربط

([١]) يوسف بوغرارة، الأمن السيبراني" الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني، مجلة الدراسات الأفريقية وحوض النيل، المركز العربي، العدد الثالث، ٢٠١٨.

([٢]) مصطفى إبراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي"، مجلة العلوم القانونية والسياسية، م. ١٠، ع.١، ٢٠٢١، ص ١٥٧.

([3]) Richard A. Kemmerer, Cyber security, University of California, Santa Barbara Department of Computer Science, 2003, p 3.

([٤]) خالد ظاهر عبد الله جابر السهيل المطيري، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد ٣٨، ٢٠٢٢، ص ١٠٠٦.

البني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية". فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين. كما أن هناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة.[١]

ويعرف أيضا بأنه بيئة تفاعلية رقمية تشمل عناصر مادية وغير مادية، مكونة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين.

الهجمات السيبرانية: cyberattacksيمكن تعريفها بكونها: "فعلا يقوّض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام".[٢]

الجريمة السيبرانية:Cybercrime مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها". فهي الجريمة المتصلة باستخدام الكمبيوتر، أي تصرف غير قانوني، يرتكب باستخدام تقنيات المعلومات والاتصالات، بقصد السيطرة على نظام الدولة الإلكتروني.[٣]

مفهوم أمن المعلومات: هو مجموعة الإجراءات والتدابير الوقائية التي تستخدم للمحافظة على المعلومات وسريتها والمحافظة عليها من السرقة أو الاختراق.

كما يعرف أمن المعلومات بأنه نظام حماية المعلومات الرقمية، ويمكن من خلاله تشفير البيانات، وتوفير الشبكات والبنية التحتية التي تحتوي على معلومات شخصية، ومعلومات مالية، وبيانات خاصة بالشركات، وتكون كلها محمية بشكل مكثّف ضد أي اختراقات.[٤]

---

(١)د/ منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني، لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد ١١١، ص ٢٠٢٠.

(2)Matthew C. Waxman, "Cyber-Attacks and the Use of Force, The Yale Journal of International،Back to the Future of Article 2 (4), Vol. 36,2011,p 423.

(3) Catota, Frankie E ؛Morgan1, M. Granger and Douglas C. Sicker, Cybersecurity education in a developing nation: the Ecuadorian environment, Journal of Cybersecurity, 00(0), 2019, 1–19 doi: 10.1093/cybsec/tyz001.

(٤) د/ ميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد ٣٥، الجزء الثالث، ٢٠٢٠، ص ٣٨٨.

المطلب الثاني

أهداف وأهمية تحقيق الأمن السيبراني

أولا: أهداف الأمن السيبراني:

يعد الهدف الأسمى للأمن السيبراني هو القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات ويتطلب حماية الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به، ونتيجة لأهمية الأمن السيبراني في واقع مجتمعات اليوم فقد جعلته العديد من الدول على رأس أولوياتها، خاصة بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، في إشارة صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حروب جديدة هي الحروب الإلكترونية.

وهناك من يرى أن الأمن السيبراني يهدف إلى تحقيق ما يلي:

١. تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
٢. التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
٣. توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.
٤. صمود البنى التحتية الحساسة للهجمات الإلكترونية.
٥. توفير المتطلبات اللزمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
٦. سد الثغرات في أنظمة أمن المعلومات.
٧. مقاومة البرمجيات الخبيثة، وما تستهدفه من احداث اضرارا بالغة للمستخدمين.
٨. التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
٩. الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.
١٠. اتخاذ جميع التدابير الضرورية لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.
١١. تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق اجهزتهم التقنية بقصد الإضرار بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.[١]

---

(١) د/ منى عبد الله السمحان، مرجع سابق، ص ١٢.

يتضح مما سبق أن الأمن السيبراني يهدف إلى الوقاية أو منع وقوع التهديدات السيبرانية من الأساس، والتدخل فيها حال وقوعها بهدف التقليل والحد من آثارها، ومن ثم وضع إجراءات سريعة للتعافي والرجوع إلى الوضع الطبيعي. سواء كان ذلك عن طريق وضع خطط أو تنفيذ إجراءات أو رسم سيناريوهات لمواجهة مثل هذه التحديات.

ثانيا: أهمية الأمن السيبراني:

للأمن السيبراني أهمية بالغة في الدولة، خاصة ما يتعلق بالجانب الوقائي للبيانات والمعلومات، والاتصالات المختلفة وتكمن هذه الأهمية فيما يلي:

- يساعد على استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- يوفر بيئة عمل آمنة خلال العمل عبر الشبكة العنكبوتية.
- يعمل على الحفاظ على المعلومات وتجانسها وسلامتها وذلك بكف الأيادي من العبث بها وتحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.[1]
- يحمي الأمن السيبراني مختلف أنواع البيانات الحساسة والمهمة من تعرضها للسرقة أو الإتلاف.

تنبع أهمية الأمن السيبراني من ثلاثة محاور رئيسية هي:

- **السرية:** أي التحكم في الولوج إلى البيانات واتاحتها لمن يسمح لهم فقط.
- **السلامة:** الحفاظ على سلامة البيانات والمعلومات وحمايتها من الهجمات التخريبية أو السرقة.
- **الجاهزية:** جاهزية جميع الأنظمة والخدمات والمعلومات واتاحتها حسب الطلب.

([1]) منى عبد الله السمجان، مرجع سابق، ص ١٢.

المطلب الثالث

ابعاد الأمن السيبراني

البعد العسكري: تنشأ أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصرعات المسلحة، كما أنه يساعد في عملية تبادل المؤسسات العسكرية المعلومات الهامة بشكل إلكتروني افتراضي بدون اختراق هذا التواصل، مما ينعكس إيجابيا على تحقيق الأهداف العسكرية للدولة.

البعد الاجتماعي: يرتبط البعد الاجتماعي أيضاً بالمجالات العلمية، والثقافية، والخدمية، حيث تسمح التطور التكنولوجي بالوصول الى مناطق بعيدة، والى فئات محددة، ككبار السن، والمرضى، وغيرهم من ذوي الاحتياجات الخاصة. بالإضافة إلى الدور الذي يمكن أن يؤديه، في تبادل المعلومات، في أوقات الازمات الإنسانية والكوارث، ولا تقف الابعاد الاجتماعية عند حدود توفير اطمئنان المواطن إلى حياته اليومية، والاستفادة من طاقات تقنيات المعلومات والاتصالات، في تطوير نشاطاته المختلفة، بل تتعداها، إلى صيانة القيم الجوهرية في المجتمع: كالانتماء، وغيرها من المعتقدات.[١]

البعد السياسي: وهناك صراع سيبراني تحركه دوافع سياسية ويأخذ شكلا عسكريا ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني وذلك بهدف إفساد النظم المعلوماتية والشبكات والبنية التحتية وبما يتضمن استخدام أسلحة وأدوات إلكترونية من قبل فاعلين داخل المجتمع المعلوماتي أو من خلال التعاون ما بين قوى أخرى لتحقيق أهداف سياسية. [٢]

كما يشكل الأمن السيبراني دورا هاما في الحياة السياسية، حيث يتعاظم هذا الدور في ظل اعتماد المواطنين على مواقع التواصل الاجتماعي في حياتهم اليومية والتقنيات الحديثة. والأمن

([١])عبد الرحمن عاطف أبوزيد، بحث في الأمن السيبراني في الوطن العربي، دراسة حالة المملكة العربية السعودية، المركز العربي للبحوث والدراسات، العدد ٤٨، عام ٢٠١٩، ص ٥

([2]) Myriam Dunn, Information Age Conflicts, A Study of the, Center،Information Revolution and a Changing Operating Environment, ETH Zurich،for Security Studies (CSS, Issue No 64,2002,p14.

السيبراني له دور هام في الحملات الانتخابية البرلمانية، وكذلك الاحتجاجات الإلكترونية وغيرها.[١]

البعد الاقتصادي: يرتبط الأمن السيبراني، ارتباطاً وثيقاً بالاقتصاد، فالتلازم واضح، بين اقتصاد المعرفة، وتوسع استخدام تقنيات المعلومات والاتصالات، كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة، والمخزنة، والمستخدمة، على كل المستويات. كذلك تتيح تقنيات المعلومات والاتصالات، تعزيز التنمية الاقتصادية لبلدان كثيرة، عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى، التي تبحث عن إدارة كلفة إنتاجها، بأفضل الشروط. إلا أن هذا الواقع المشرق، يطرح مسائل مختلفة، سواء منها ما يتعلق بحماية مقدم الخدمة، والعمل أو بحماية المستهلك على الإنترنت.[٢]

ويضاف إلى ذلك، دخول العالم عصر المال الإلكتروني، ضمن بيئة تقنية متحركة، بعد إطلاق خدمات المحفظة الإلكترونية، إذ تتزايد استثمارات المصارف، والمؤسسات المالية، في مجال المال الرقمي، وتتنافس الشركات على إصدار تطبيقات تسمح بآليات دفع أمنة، ويحفظ المال في المحفظة الإلكترونية، وبالإيفاء من خلالها وباستخدامها كرصيد افتراضي. وقد وضعت بعض الدول تشريعات خاصة بهذا المال. وغنيّ عن القول، ما يمكن أن يثيره هذا الأمر من صعوبات وما يتطلبه من تشريعات للحد من بعض الجرائم الاقتصادية والمالية الخطرة، والعابرة للحدود، كتبييض الأموال، والتهرب من الضريبة.

الأبعاد القانونية: إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان إلى الأطر القانونية الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها.

ولعل من أبرز الممارسات القانونية في مجال الأمن السيبراني هو ضمان بعض الحقوق في هذا المجال كحق النفاذ إلى الشبكة العالمية للمعلومات، وأيضاً توسعت بعض المفاهيم لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الإلكترونية، والحق في إنشاء التجمعات يوجد إطار تشريعي في مجال الأمن السيبراني المصري وإن كان ضعيفا قبل صدور قانون ١٧٥المكافحة جرائم تقنية المعلومات ٢٠١٨، إلا أنه

---

(١) خالد ظاهر عبد الله جابر السهيل المطيري، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد الثامن والثلاثون، يوليو ٢٠٢٢، ص ١٠٠٧.

(٢) حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني، " دراسة مقارنة"، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، ٢٠٢١، ص ٢٩.

كان موجودا متمثلا في قانون الاتصالات رقم ١٠ لسنة ٢٠٠٣، وقانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤، وقانون حماية المستهلك رقم ٦٧ لسنة ٢٠٠٦ وقرار جمهوري رقم ٢٧٦ لسنة ٢٠١٤ بشأن انضمام مصر للاتفاقية العربية لمكافحة الجرائم التقنية، ثم جاء قانون تقنية المعلومات ٢٠١٨ لتشهد مصر حراكا قويا في مجال أمن المعلومات. على الإنترنت، وأيضاً الحق في حماية ملكية البرامج المعلوماتية.

المبحث الثاني

الحماية الدستورية للحقوق الرقمية والأمن السيبراني

أدى التحول الرقمي للدولة إلى ظهور ما يسمى بحقوق الإنسان الرقمية*، وهي حقوق الإنسان التي تسمح للفرد بالوصول إلى الإعلام الرقمي واستخدامه، وإنشائه ونشره، أو الوصول إلى أجهزة الحاسوب وغيرها من أنظمة التخزين والحوسبة المحليّة والسحابيّة، وأنظمة الاتصال التي توصل لها وما عليها من خدمات لنقل البيانات والمعلومات، وحقّ الوصول لها والأجهزة الإلكترونيّة، أو شبكات الاتصال واستخدامها، وحقه في شبكات بث تلفزيوني وإذاعي رقمية تنقل له المعلومات والأخبار والبرامج بكل أشكالها دون قيود وهذا الحق يرتبط بعدد أخر من الحقوق وحريات مثل الحق في حرية تداول المعلومات والحق في حرية الرأي والتعبير، والحق في الخصوصية. وسوف يتم تناول ذلك على النحو التالي:

- المطلب الأول: الحماية الدستورية للحق في الحصول على المعلومات والأمن السيبراني
- المطلب الثاني: الحماية الدستورية للحق في حرية التعبير والأمن السيبراني
- المطلب الثالث: الحماية الدستورية للحق في الخصوصية والأمن السيبراني

المطلب الأول

الحماية الدستورية للحق

في الحصول على المعلومات والأمن السيبراني

يعتبر حق الحصول على المعلومات من أبرز سمات ومعالم الثورة الرقمية، حيث أن عالم الانترنت وضع فرص متساوية أمام جميع البشر من حيث الوصول إلى الانترنت وإمكانية اقتناء وسائل النقل الرقمية، لذا فإن حق الحصول على المعلومات هي أحد حقوق الإنسان

*** تعتبر الحقوق الرقمية من حقوق الانسان الأساسية، إذ أقر مجلس حقوق الإنسان في عام ٢٠١٢ ولاحقا في عامي ٢٠١٤ و٢٠١٦أن نفس حقوق الإنسان المحمية في الواقع يجب أن تكون محمية عبر الإنترنت أيضا. وفي ذات السياق اصبحت القدرة على مشاركة المعلومات والتواصل بحرية باستخدام شبكة الإنترنت أمراً ضرورياً من أجل إعمال حقوق الإنسان على النحو المجسد في الاعلان العالمي لحقوق الإنسان والعهد الدولي الخاص بالحقوق المدنية والسياسية.**

حيث تنص المادة ١٩ من العهد الدولي الخاص بالحقوق المدنية والسياسية الفقرة ٢ على: «لكل إنسان حق في حرية التعبير. ويشمل هذا الحق حريته في التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين دونما اعتبار للحدود». كما أكد الإعلان العالمي لحقوق الانسان على هذه الحقوق والتي تؤكد على أن حق الوصول الى الانترنت والوصول الى المعلومات من خلاله هو حق من حقوق الإنسان الأساسية.

الرقمية. ولقد نص الدستور المصري على هذا الحق في المادة ٦٨[١]. وبذلك فإن أي حرمان من الوصول إلى المعلومات يعتبر من قبيل انتهاك حق الإنسان في العصر الرقمي، ويعتبر يعتبر حق الحصول على المعلومات حقا من الحقوق والحريات الأساسية التي نصت عليها القوانين والدساتير.

تعد الشفافية مكونا أساسيا في كل من الإدارة والتنظيم، وتتضمن نشر المعلومات وتداولها عن التمويل وخطوات صنع القرارات بين أصحاب المصالح الحقيقيين، من خلال نشر التقارير سواء إلكترونيا أو على هيئة نسخ مطبوعة سواء بصورة شهرية أو سنوية.[٢]

وتشترط الشفافية توفر المعلومات الدقيقة في مواقيتها وإفساح المجال أمام الجميع للاطلاع على المعلومات الضرورة والموثقة، ويجب أن تنشر بعلنية ودورية من أجل توسيع دائرة المشاركة والرقابة والمحاسبة ومحاصرة الفساد من جهة، والمساعدة على اتخاذ القرارات الصالحة في السياسات العامة من جهة أخرى.[٣]

وتقوم الشفافية بدور هام لاسيما فيما يتعلق بتعميم المعلومات المتعلقة بحقوق المواطنين والخدمات التي يحق لهم المطالبة بها وسبل الحصول على تلك الحقوق، كما تشمل كذلك الطرق التي تمارس بها السلطة من أجل تحقيق الصالح العام كقدرة الحكومة على إدارة مواردها بفاعلية وتنفيذ السياسات.[٤]

---

(١) دستور جمهورية مصر العربية ٢٠١٤ المادة ٦٨: المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب، والإفصاح عنها من مصادرها المختلفة، حق تكفله الدولة لكل مواطن، وتلتزم الدولة بتوفيرها وإتاحتها للمواطنين بشفافية..."

(٢) د/ سامر علي السيد السقا: استراتيجية مقترحة لتعزيز الشفافية في المجالس الشعبية المحلية: دراسة مطبقة على المجلس الشعبي المحلي لمركز طلخا، المؤتمر العلمي الدولي الرابع والعشرون للخدمة الاجتماعية" الخدمة الاجتماعية والعدالة الاجتماعية"، كلية الخدمة الاجتماعية، جامعة حلوان، المجلد ٣، ٢٠١١، ص١٠٠٩.

(٣) د/ حسن خميس ابراهيم نحلة: متطلبات دعم الشفافية بين القيادات التنفيذية وتأثيرها على برامج التنمية المحلية، مجلة دراسات في الخدمة الاجتماعية والعلوم الإنسانية، المجلد ٤، العدد ٣٥،٢٠١٣، ص ١٩٠٤.

(4) Ropport De Synthese : Décentralisation Et Gouvernance Locale en Afrique: Etude Comparative Sur L'Appropriation De La Reforme Par Les Communautés Rurales Au Mali et au Burkina Faso, Center For Research on Local Knowledge,2007 ,p 5.

ولذلك فقد نص الدستور المصري لسنة ٢٠١٤ في المادة ٦٨ على أن" المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب، والافصاح عنها من مصادرها المختلفة، حق تكفله الدولة لكل مواطن، وتلتزم الدولة بتوفيرها وإتاحتها للمواطنين بشفافية....."

يعد الحصول على المعلومات والإحصائيات وإمكانية الوصول إليها بوضوح وبدون غموض وتسهيل إجراءات الحصول عليها أمرا ضروريا لتحقيق الشفافية الإدارية.[١]

ويهدف الأمن السيبراني إلى تعزيز حماية جميع ما يتعلق بالدولة والأفراد إلكترونياً لحماية هذه الأنظمة الإلكترونية وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية وجميع مكوناتها المحيطة بالمجتمع من أجهزة وبرمجيات ومعدات وجميع ما يؤثر على تقديم هذه الخدمات، وما تحويه من بيانات، فأصبحت هذه أيضًا من أهم الأولويات المهمة والحيوية لجميع دول العالم للحفاظ على بيانات مواطنيهم وحفظ ممتلكاتهم وبياناتهم الإلكترونية عن طريق:

- حماية شبكة المعلومات والاتصالات والتي تلعب كبيرا في تدفق خط سير تدفق البيانات بين المواطنين والدولة ومن طرف إلى طرف آخر، والتي إذا تعرضت إلى تخريب أو تدمير أو اختراق حتماً قد يؤثِّر ويقطع هذه الاتصالات ويتوقف سير العمل وتتوقف الخدمات.
- حماية شبكة المعلومات من أي هجوم وذلك بمعرفة آخر التقنيات الموجود في هذا المجال ومن أهمها كشف أهداف رسائل هذا العدو والتعرّف على طبيعة هذا المهاجم وذلك وماذا يريد من خلال معرفة اساليبه المستخدمة والأساليب المختلفة لكي يتم العمل على إيقاف هذا الهجوم بأسلوب علمي وتقني مُحكم يمنع هذا الهجوم

المطلب الثاني
الحماية الدستورية للحق
في حرية التعبير والأمن السيبراني

تعد حرية التعبير عن الرأي من الحقوق الاساسية التي اقرتها مختلف المواثيق الدولية[٢] وكرستها دساتير الدول منها الدستور المصري الصادر ٢٠١٤ في المادة ٦٥.[١] إن هذه المادة

---

(١) **Amosa Desmond Uelese: Local Government and Good Governance: the Case of Samoa, Commonwealth Journal of Local governance, Issue 7, 2010, p10.**

(٢) **يخضع هذا الحق لمبادئ الإعلان العالمي لحقوق الإنسان والعهدين الدوليين الخاصين بحقوق الإنسان تحت باب الحق في حرية التعبير عن الرأي، ويقتضي هذا الحق في ممارسة كل شخص لحقه في التعبير عن رأيه دون أن يتعارض ذلك مع حقوق وحريات الغير أو النظام العام، وتعتبر حرية التعبير الرقمية من أسمى الحقوق التي نادت بها القوانين والتي يجب العمل على حمايتها ورعايتها نظراً لما يتعرض له هذا الحق من**

تقر بالحرية المطلقة لكل شخص في التعبير ونقل الافكار والأنباء والآراء بواسطة أي وسيلة كانت من دون أي قيد أو شرط، وبهذا المعنى قد يشكل ممارسة هذا الحق تهديدا لأمن الدول وسيادته.

بدأت الحكومات، ولاسيما في البلدان المتقدمة في مجال التقنيات الرقمية مثل إستونيا وكوريا وسنغافورة، تستغل تحليل البيانات والمنصات الرقمية في جعل عملية وضع السياسات أسرع وتيرة وأكثر استنارة وتكاملا. ويفتح الإنترنت أيضا سبلا جديدة للديمقراطية التشاركية. فقد شهدت أيسلندا تجربة إعادة كتابة دستورها من خلال استلهام آراء الجمهور، واستكشفت البرازيل وإستونيا سبلا تشاركية لوضع القوانين. وتساعد وسائل التواصل الاجتماعي على تذليل الحواجز التقليدية في طريق العمل الجماعي للمواطنين، وذلك عن طريق الخفض الشديد لتكلفة الاتصال والتنسيق. ويظهر عدد متزايد من الكتابات التجريبية أيضا أن الهواتف المحمولة واستخدام موقعي توتير فيسبوك ساعدت الاحتجاجات أثناء أحداث الربيع العربي في مصر [٢] والمظاهرات المناهضة للحرب في الولايات المتحدة [٣] وجهود تعبئة المواطنين في أنحاء أفريقيا. [٤]

انتهاك من قبل السلطات والأنظمة الحاكمة بموجب القوانين الجائرة التي يتم سنها تحت بند قوانين مكافحة الجرائم الالكترونية.

(١) دستور جمهورية مصر العربية ٢٠١٤المادة ٦٥تنص على: حرية الفكر والرأي مكفولة. ولكل إنسان حق التعبير عن رأيه بالقول، أو بالكتابة أو التصوير، أو غير ذلك من وسائل التعبير والنشر.

(2) Acemoglu, Hasan, and Tahoun, The Power of the Street: Evidence from Egypt's Arab Spring." NBER Working Paper 20665, National Bureau of Economic Research, Cambridge, MA, 2014,

(3)Bennet, Breunig and Givens, Communication and Political Mobilization: Digital Media and the Organization of Anti-Iraq War Demonstrations." Political Communication 25 (3),2008,p 269–89.

(4)Hollenbach, Florian, and Jan Pierskalla, Voicing Discontent: Communication Technology and Protest." APSA Annual Meeting paper,2014,

http://papers.ssrn.com/ sol3/papers.cfm?abstract_id=2452306

المطلب الثالث

الحماية الدستورية للحق

في الخصوصية والأمن السيبراني

يقصد بالخصوصية حق الفرد في حفظ بيناته ومعلوماته الشخصية وحياته الخاصة والتحكم فيمن يمكنه الوصول لها سواء كانوا افرادا آخرين أو حكومات. ومن ثم فقد نص الدستور المصري على أن للحياة الخاصة حرمة وهي مصونة لا تمس وذلك في المادة ٥٧.[١]

هناك العديد من المتغيرات التي أدت إلى زياد الشعور بأهمية الخصوصية لدى مستخدمي الانترنت والاتصالات، وكذلك مستخدمي شبكات التواصل الاجتماعي، كوسيلة للحشد والتأييد في الفاعليات السياسية، بالإضافة إلى التزايد المستمر في عدد الفيروسات والبرمجيات الخبيثة، مما يشكل خطرا على المعلومات الخاصة بالأفراد. وتعد الرقابة على الانترنت أحد انتهاكات الخصوصية التي يمكن أن تقوم بها الحكومات لفرض سيطرتها على مجتمع مفتوح لا يمكن السيطرة عليه.[٢]

---

(١) دستور جمهورية مصر العربية، المادة ٥٧: للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها....

(٢) محمد الطاهر، الحريات الرقمية "المفاهيم الأساسية"، مؤسسة حرية الفكر والتعبير، القاهرة، ٢٠١٣،ص٦.

المبحث الثالث

دور الأمن السيبراني الحفاظ

على سيادة الدولة ومتطلبات تحقيقه.

تعتبر السيادة القوة والسيطرة الكاملة النهائية غير القابلة للنقاش وعادة ما تمارس الدول سيادتها على إقليم معين، ويرتبط مفهوم السيادة بفكرة الدولة وقدرتها على فرض سيطرتها على أراضيها وشعبها وسيادتها أيضا التي يتم التعبير عنها في حريتها في التعامل مع الدول الأخرى وعدم قدرة أيٍّ من الدول فرض سيطرتها على إقليم دولة أخرى، وعادة ما يتم الإشارة إلى مفهوم السيادة مقترنًا بفكرة الاستقلال؛ حيث إن الاستقلال هو أهم العوامل التي تتيح للدولة ممارسة أنشتطها على المستوى الداخلي والخارجي، فغالبًا ما يكون الاستقلال داعمً لمفهوم السيادة.

يضع الدستور الإطار العام لمفهوم الدولة ولنظامها السياسي الداخلي والذي يعد الأساس لمضمونه ومحوره وإطار ما فيه من حقوق وحريات وكيفية تكوين السلطات فيها وعلاقتها ببعضها البعض.

يعد الأمن السيبراني جزء أساسي من أمن الدول، يرتبط بالمسائل المتعلقة بحماية المعلومات على جميع أنظمة الحوسبة والشبكات الإلكترونية، لعظم أهمية الأمن السيبراني وحاجة الناس إليه ولارتباطه بواقعنا المعاصر، بات حماية الفضاء السيبراني ضرورة لا غني عنها؛ لأن حربه حرب عبر القارات، وهي أخطر الحروب، وتزداد خطورته كلما زاد التقدم في المجال المعلوماتي، وبذلك أصبح الأمن السيبراني ضرورة لحماية القطاعات الحيوية. ولقد أكد الدستور المصري ٢٠١٤ في المادة ٣١ على أن أمن الفضاء المعلوماتي جزء من الأمن القومي المصري. وسوف يتم تناول ذلك على النحو التالي:

المطلب الأول: دور الأمن السيبراني في الحفاظ على سيادة الدولة

المطلب الثاني: دور الأمن السيبراني تدعيم المواطنة

المطلب الثالث: متطلبات تحقيق الأمن السيبراني.

المطلب الأول

دور الأمن السيبراني في الحفاظ على سيادة الدولة

تشكل السيادة أحد الأركان الجوهرية التي تبنى عليها نظرية الدولة في الفكر السياسي والقانون إذ تعد السيادة ملازمة لحياة الدولة ومرتبطة بوجودها. فالسيادة مفهوم قانوني– سياسي يتعلق بالدولة باعتبارها تشكل أحد أهم خصائصها وشروطها الأساسية، كما انها تعد من المحددات السياسية والقانونية المركزية لمفهوم الدولة الوطنية ومن خلالها يتجسد واقعيا الوجود القانوني والسياسي للدولة كعضو في المجتمع الدولي.

وقد نص دستور مصر على أن السيادة للشعب وحده، يمارسها ويحميها، وهو مصدر السلطات، ويصون وحدته الوطنية التي تقوم على مبادئ المساواة والعدل وتكافؤ الفرص بين جميع المواطنين.[١]

أولا: مفهوم السيادة:

تشكل السيادة أحد الأركان الجوهرية التي تبنى عليها نظرية الدولة في الفكر السياسي والقانوني ولذلك فإنه هناك العديد من التعريفات للسيادة نذكر منها:

تعد السيادة القوة المطلقة التي تربط الأفراد، وكذلك الكيانات الأخرى داخل الدولة، وتعدُّ ركنًا من أركان قيام الدولة، وممارستها تمنح الدولة السلطة العُليا المطلقة على إقليمها وشعبها في مختلف أمورها سواء داخليًا أو خارجيًا على حدٍ سواء. [٢]

ويعتبر مفهوم السيادة ليس من المفاهيم المتفق عليها، وعلى الرغم من أن هذا المفهوم في جوهره، وبموجب القانون الدولي، هو قوة وحق، معترف به أو مؤكد بشكل فعّال فيما يتعلق بجزء محدد من العالم، وذلك لترتيب شؤون الحكم، منعًا لاحتلال الأمم أو الشعوب بعضها لبعض. وفي هذا السياق، يمكن القول بأنه يصعب الحديث عن السيادة باعتبارها "قوة" و" حق" فقط دون معرفة أوجه تطور مفهوم السيادة من النواحي اللغوية والسياسية والقانونية، وفي الإطار القانوني على النحو التالي:

أ- مفهوم السيادة من الناحية اللغوية:

يحتاج ضبط مفهوم فكرة السيادة إلى بيان أصل هذه الكلمة، فكلمة "السيادة" هي اصطلاح قانوني مترجم من كلمة فرنسية هي (souverainete)، ومشتقة من الأصل اللاتيني (Superanus)، ومعناها "الأعلى"، وفي اللغة العربية هي من أصل فعل "ساد" أو "يسود"، والخلاصة هي أن المعني اللغوي سواء كان في اللغات الأجنبية أو العربية يدل على أن كلمة السيادة تدل على المنزلة والقوة والغلبة.[٣]

ب-مفهوم السيادة من الناحية السياسية والقانوني:

يعد السيادة مفهوم غير متفق عليه من نهاية تحديده، ولكن بالنظر إلى الطبيعة القانونية للدول، اتفق الفقهاء على أن قيام الدولة المعاصرة بأركانها الثلاثة: الشعب، والإقليم، والسلطة

---

(١) المادة ٤ من دستور جمهورية مصر العربية.

(2) Raia Prokhovnik Internal/external: The state of sovereignty, Contemporary Politics, 1996, Vol. 2, Issue 3، PP. 7-20, Available on: https://www.tandfonline.com/doi/abs/10.1080/13569779608454736

(٣)حسن رزق سليمان عبدو، النظام العالمي ومستقبل الدولة في الشرق الأوسط، رسالة ماجستير، كلية الآداب والعلوم الإنسانية، جامعة الأزهر، فلسطين، غزة ٢٠١٠، ٤٦.

السياسية، يترتب عليه تميزها بأمرين أساسيين؛ الأول هو تمتعها بالشخصية القانونية الاعتبارية، والثاني هو أن السلطة السياسية يجب أن تكون فيها ذات سيادة، وعلى هذا النحو، تفهم السيادة في مبادئ القانون العام الدولي –وبالمعني البسيط– على أنها وصف لدولة لها سيطرة كاملة على أراضيها ولا تخضع لأي سيطرة دولة أخرى ولا تلتزم إلا بقواعد القانون الدولي العام.[١]

ثانيا: تغير مفهوم السيادة في الفضاء السيبراني:

أدى التطور الناجم عن التكنولوجيا الحديثة في مجال الإنترنت والفضاء السيبراني بالتبعية إلى ضرورة تغير مفهوم السيادة، فلم تعد فكرة السيادة مرتبطة بالمفهوم التقليدي للإقليم. إذ أثر التقدم التكنولوجي على اتصالاتنا اليومية على نطاق واسع، وفي مجال التواصل بين الأفراد، خلقت التكنولوجيا عالمها الخاص ووسائط الاتصال الممثلة في الفضاء السيبراني، وأدى اتساع شبكة الإنترنت العالمية إلى خلق عالم افتراضي، معروف باسم «الفضاء الإلكتروني» يمكن الوصول إليه بسهولة من خلال أجهزة الكمبيوتر وغيرها من وسائط تكنولوجيا المعلومات. وفي هذا الفضاء، ظهرت المواقع الإلكترونية والمدونات والرسائل الإلكترونية والشبكات الاجتماعية التي تُسرع الاتصالات بين الناس، وتُسهل معاملاتهم، تروي عطشهم للمعرفة والترفيه. ومع ذلك، يجب الأخذ في الاعتبار أن بيئة الفضاء الإلكتروني معقدة، ولا حدود لها، وليس له موقع مكاني معين.[٢]

تعد الدولة جزء من بنية الأمن السيبراني التي تهدف الى تخفيف المخاطر السياسية الناشئة عبر الانترنيت، والأهم من ذلك هي سيادة الدولة وبما أن البنية التحتية لتقنية المعلومات والاتصالات أسست لحركة تدفق المعلومات عبر الحدود الجغرافية بين الدول محولة العالم الى قرية كونية لذا فرض ذلك واقعاً جديداً على السيادة الوطنية، الأمر الذي جعل الدولة تعاني من مشاكل أشد وأخطر من تلك التي واجهتها من قبل، فتحولت من مسائل الأمن عبر الحدود ومسائل الأمن التقليدية برزت مشكلة السيادة على الفضاء السيبراني وعلى العلاقات التي تحاك عبر الانترنيت بين اشخاص موجودين على أراضي مختلفة خاضعة لعدد من السيادات أي يختلف بلد مصدر العمل وبلد تحقق نتائجه والبلاد التي تمر عبرها البيانات فالفضاء السيبراني مكان مختلف لكنه شديد الارتباط بالعالم المادي وليس مستقلا عنه. وهذا يعني أن الأمن

([١])مروه زين العابدين سعد، تأثير تغير مفهوم السيادة على الاختصاص القضائي في الجرائم السيبرانية، المجلة الدولية للفقه والقضاء والتشريع، المجلد ٣، العدد ٣، ٢٠٢٢، ص ٦٨٦.

([2])Jyoti Rattan and Vijay Rattan, Cyber Laws & Information Technology, Bharat Law House, Delhi , 2014, p. 48

السيبراني أثر في سيادة الدولة ولم يلغيها وإنما غير وظيفتها حيث فرض وضائف جديدة على سيادة الدولة.[١]

وبذلك فإن الأمن السيبراني له تأثير على قوة الدولة من خلال ظهور شكل جديد للقوة وهو القوة الافتراضية والتي تعرف بالقدرة على الحصول على النتائج المرجوة من خلال مصادر المعلومات الإلكترونية.

وذلك نظرا للتطورات المتلاحقة في النظام الدولي، والتي ساهمت في تحول السيادة من صفة «المطلق» إلى «النسبي»، ولعل الفضاء السيبراني كان من أبرز التطورات، والذي شكل تحديًا كبيرًا لمفهوم «السيادة» بمعناها التقليدي في القانون الدولي، وفيما يلي أبرز الدلالات على ذلك:

- ظهور نوعية جديدة من المشكلات الدولية التي تستلزم تكثيف الجهود الدولية لاحتوائها، ولعل أهمها القرصنة الإلكترونية والحرب الإلكترونية وعمليات الاختراق.
- ساهم التطور الهائل في وسائل الاتصالات وتكنولوجيا المعلومات في اختراق سيادة الدول ومن ثم لم يعد باستطاعة الدول احتكار الإعلام، وذلك بسبب الكم الهائل من المعلومات والبيانات والأفكار التي تنتشر دون قيود أو شروط.
- أصبحت المنتجات المعلوماتية غير مقتصرة على دولة بعينها، فلم يُعد في مقدور أية دولة الاكتفاء بما انتجته من معلومات، ولكن أصبح يُحتم على الحكومات الاستعانة بالقطاع الخاص متمثلً في شركات تكنولوجيا المعلومات لإدارة وتنظيم الكم الهائل والمكثف من البيانات والمعلومات.
- أحدث الفضاء السيبراني تغييرات في مهام ووظائف الدولة، إذ لم تُعد القوات المسلحة بالمعنى التقليدي هي الفاعل الوحيد الذي يتولى وظيفة الدفاع الخارجي، وبالتالي، حماية أراضي الدولة ومواطنيها من أي عدوان خارجي، ويرجع ذلك إلى وجود أنماط جديدة من العدوان لم تكن فيما قبل، ولعل جميعها ترتبط بشبكات الاتصالات والمعلومات؛ حيث يمكن لاختراق إلكتروني أن يتسبب في تعطيل البنية التحتية لمنشأة حيوية دون التعرف على تحديد مصدر الهجمات وكيفية الرد عليها بصورة سريعة.
- أضحى الفضاء السيبراني أداة مهمة لدعم الفاعلين من غير الدول، وذلك لمواجهة الدول، أي أن الفضاء السيبراني ساهم في تقوية الحركات الانفصالية والجماعات الإرهابية، وبالتالي، أثر أيضًا على الهُوية الوطنية للأفراد.

---

(١) د/ تغريد معين حسن المشهدي، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، العدد ٣٠، ص ٢٢٤.

- وأخيرًا، تضاؤل دور الدولة القومية، بل وأصبح من الصعب اعتبارها الفاعل الوحيد في العلاقات الدولية.[١]

المطلب الثاني

دور الأمن السيبراني تدعيم المواطنة

تعتبر المواطنة حالة نفسية تعكس العلاقة بين الوطن والمواطن بما تتضمنها من علاقات بين الأفراد ودولتهم وعلاقات الأفراد ببعضهم البعض وبين المؤسسات الدستورية.[٢]

وإمعاناً من المشرع الدستوري بإن المواطنة هي أحد الركائز الاساسية للمجتمع، فقد تضمنت المادة الأولى من دستور ٢٠١٤ على أن جمهورية مصر العربية دولة ذات سيادة موحده لا تقبل التجزئة، ولا ينزل عن شيء منها، نظامها جمهوري ديمقراطي يقوم على اساس المواطنة وسيادة القانون.. "، كما نصت المادة ٢١ من ذات الدستور على جعل مفاهيم المواطنة والتسامح وعدم التمييز والحفاظ على الوحدة الوطنية من أهدف التعليم، إلا أن النصوص الدستورية التي تقرر مبادئ المواطنة لا قيمة لها مالم تصاحبها ضمانات حقيقية وطنية ودولية تكفل تطبيق هذه النصوص تطبيقاً فعلياً.

تتطلب المواطنة تحقيق المساواة بين المواطنين مالم توجد أسباب موضوعية تبرر اتخاذ إجراءات للتمييز في أمور بعينها، ورغم ذلك لا يمكن التسليم أو القول بأن ثبوت صفة المواطنة تعني التمتع الآلي أو التلقائي بالحق في المساواة، بل يعد ذلك للتشريعات القائمة.[٣] ومن ثم فأن القيمة الدستورية للمواطنة لا مرية فيها، فهي جزء لا يتجزأ من مقومات المجتمع، التي تكفلها الحماية الدستورية[٤]. ويترتب على الحماية الدستورية للمواطنة وجود التزام بحمايتها وتكريسها، وإيجاد آليات لتعزيزها ومنع انتهاكها وإيقاف ما قد يقع من تطبيقات تخل من مضمونها.

أولا: مفهوم المواطنة: مفهوم المواطنة لغة: مشتقة من الوطن، والوطن هو المنزل الذي يقيم فيه الانسان، والجمع أوطان، ويقال وطن بالمكان، وأوطن به أقام، وأوطنه اتخذه وطنا، وأوطن فلان

---

(١) أنديرا عراجي، القوة في الفضاء السيبراني؛ فصل عصري من التحدي والاستجابة، بيروت؛ دار ميرزا للطباعة والنشر والتوزيع، ٢٠١٩، ص ٨٣ –

(٢) د/ أشرف عبد الفتاح أبو المجد، التنظيم الدستوري للحقوق والحريات الاقتصادية، منشأة المعارف، ٢٠٠٩، ص ٦٢.

(٣) د/ حسام فرحات أبو يوسف، الحماية الدستورية في المساواة، دراسة مقارنة، دار النهضة العربية، ٢٠٠٤، ص ١٧٥.

(٤) الدستور المصري الصادر ٢٠١٤ المادة ٥٣: " المواطنون لدى القانون سواء، وهم متساوون في الحقوق والحريات والواجبات العامة، لا تمييز بينهم بسبب الدين أو العقيدة أو ..."

أرض كذا وكذا أي اتخذها مسكنا يقيم فيه، أما الموطن فكل مقام قام به الإنسان لأمر ما فهو موطن له.[١]

أ- مفهوم المواطنة اصطلاحا:

يحدد مفهوم المواطنة اصطلاحا طبيعة الرابطة القانونية بين الفرد والدولة التي يعيش فيها، فالمواطنة تمثل الحق القانوني للشخص الذي يعيش في بلد ما كي يكون مواطنا في هذا البلد.

كما يمكن تعريف المواطنة على أنها صفة المواطن التي تحدد حقوقه وواجباته الوطنية ويعرف الفرد حقوقه ويؤدي واجباته عن طريق التربية الوطنية، وتتميز المواطنة بنوع خاص من ولاء المواطن لوطنه وخدمته في أوقات السلم والحرب.[٢]

المواطنة تعني أن كل مواطن يتساوى مع كل مواطن آخر في الحقوق والواجبات، ما داموا في مراكز قانونية واحدة.[٣]

ثانيا: تأثير التحول الرقمي على المواطنة

ساهم هذا التضخم الهائل في استخدام وسائل التواصل الاجتماعي في ظهور وانتشار العديد من الظواهر السلبية المعاصرة، كانتشار الجماعات المتطرفة على شبكات التواصل الاجتماعي، واستخدام هذه المنصات الحديثة في تجنيد الإرهابيين والمتطرفين بالإضافة إلى تفشي العنصرية الطائفية، والعرقية، والمذهبية، والتحرش بالآخرين من خال محاولات تشويه السمعة، إذ يقوم البعض بالتستر خلف ستار أسماء وحسابات وهمية في هذا الفضاء الإلكتروني الكبير، ومن ثم يطلقون العنان لبث أفكارهم ومعتقداتهم دون الأخذ في الاعتبار مدى الإضرار بأمنهم وأمن أوطانهم، ومما لا شك فيه أن العديد من رموز الفكر التكفيري وأصحاب العقائد الفاسدة قاموا باستخدام مواقع التواصل الاجتماعي لتجنيد الإرهابيين بواسطة الخطاب الفكري الاسلامي، واستطاعوا بأساليبهم التحريضية الجذابة، وخطبهم الرنانة، ومعرفتهم بمواطن الضعف لدى الشباب، استقطاب العديد من الأتباع وتوجيههم حسب رغباتهم.

من هذا المنطلق ظهرت لدينا الحاجة لتعزيز قيم المواطنة، ليس بشكلها التقليدي فحسب، بل باستخدام منصات التواصل الاجتماعي الحديثة. فإذا كانت المواطنة هي منظومة المبادئ والقيم والحقوق والواجبات المترتبة على المواطن تجاه وطنه وأمته، فإن المواطنة الرقمية أو الإلكترونية هي أحد أشكال التعبير عنها ولكن بشكل افتراضي وعلى نطاقات كبيرة مما يجعل المسؤولية الوطنية أكبر، مما يدعم ظهور المواطنة الرقمية.

---

(١) أبو الفضل محمد مكرم بن منظور، لسان العرب، دار صادر للطبع والنشر، بيروت، ٢٠٠، ص ٢٣٩.

(٢) زكى بدوي، معجم مصطلحات العلوم الاجتماعية، مكتبة لبنان، بيروت، ص ١٩٨٦، ص ٦٠.

(٣) د. يحي الجمل، مبدأ المواطنة والتعديلات الدستورية، مقال بجريدة المصري اليوم، العدد٩٥٣، ٢٢ يناير ٢٠٠٧، ص٧.

هي تفاعل الفرد مع غيره باستخدام الأدوات والمصادر الرقمية مثل الحاسوب بصوره المختلفة، وشبكات المعلومات، كوسيلة للاتصال مع الآخرين، باستخدام العديد من الوسائل أو البرامج مثل: البريد الإلكتروني، المدونات، ومختلف مواقع شبكات التواصل الاجتماعي[١]. فهي تعرف بأنها مجموع القواعد، والضوابط، والمعايير، والأعراف، والأفكار، والمبادئ المتبعة في الاستخدام الأمثل والقويم للتكنولوجيا، التي يحتاجها المواطنون صغارا وكبارا من أجل المساهمة في رقي الوطن، فالمواطنة الرقمية باختصار هي توجيه وحماية: توجيه نحو منافع التقنيات الحديثة، وحماية من أخطارها، أو باختصار أكثر دقة هي التعامل الذكي مع التكنولوجيا.

ينعكس تأثير الوسائل التكنولوجية ومنها وسائل التواصل الاجتماعي على المواطنة بارتباطها بتشكيل هوية الشباب الوطنية – أكبر فئة من مستخدمي وسائل التواصل الاجتماعي – في أبعادها الترويحية، والفكرية، والثقافية، والتعليمية، والتشريعية، والتحفيزية، وترسيخ مستويات عالية من الثقة في كفاءة الشباب وبناء قدراته، وما تتطلبه المواطنة من فكر واعٍ مدرك لمسؤولياته، وشعور بواجب التضحية والعمل من أجل الوطن، وتعزيز قيم المواطنة عبر توظيف هذه المواقع التفاعلية لمواجهة حالات التشاؤم، والإحباط، والسلبية، والنظرة الضيقة، في ثقافة بعضهم، وحواراته وردود الفعل التي تتخذ مواقف مغايرة، خاصة عندما يكون الحديث عن المواطنة الحقوق والواجبات والمسؤوليات.[٢]

يعد المواطنة بذلك إطار لاكتشاف توجهات الشباب ومواطن القلق لديهم، لتضع عليها مؤسسات الدولة يدها ومن ثم العمل على مساعدتهم على تجاوزها، وتوجيه طاقاتهم نحو تعميق ثقافة الابتكار والاختراع والموهبة، ومن ثم بناء المناخات الاعلامية والتوعوية والتثقيفية الداعمة للشباب، كتعزيز جودة التعليم، وترقية أساليب التوعية والتثقيف وإيجاد حاضنات للشباب تستقطب أفكارهم وتتيح لهم فرص النقاش وإبداء الرأي، وتمنحهم الثقة في أنفسهم، والمرونة في التشريعات الداعمة لعمل الشباب.[٣] ومما سبق نستنتج أن الأمن السيبراني ضرورة ملحة للدولة لا تقل أهمية عن الأمن العسكري وغيره، وبذلك يستلزم الأمر البحث في متطلبات تحقيقه

---

(١) محمد شرف صبحي الدمرداش، معايير التربية على المواطنة الرقمية وتطبيقاتها في المناهج الدراسية، المؤتمر الدولي السادس لضمان جودة التعليم، أنماط التعليم ومعايير الرقابة على الجودة فيه. مسقط، ٢٠١٤، ص ١٣٩ – ١٤٧.

(٢) رجب بن على العيسوي، "شبكات التواصل الاجتماعي وصناعة المواطنة"، الوطن. عمان، ٢٠١٦، متاح على:/http://alwatan.com/details

(٣) رجب بن على العيسوي، المرجع السابق.

المطلب الثالث

متطلبات تحقيق الأمن السيبراني.

حددت الاستراتيجية الوطنية للأمن السيبراني في مصر ٢٠١٧-٢٠٢١ أهم الركائز للاستعداد لمواجهة الأخطار السيبرانية فيما يلي: [١]

الدعم السياسي والمؤسسي والتنفيذي: ويشمل ذلك الوعي بخطورة التهديدات السيبرانية وضرورة التعامل معها كألوية وبأعلى قدر من الجدية، مع الاهتمام بالاستعداد المسبق بما يشمل الخطط الاستراتيجية والتنفيذية وخطط الطوارئ وآليات التنسيق العرضي واعداد الكوادر والتجهيزات التقنية واللوجستية.

الإطار التشريعي: وضع الإطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية وأمن المعلومات، وذلك بمشاركة من الأطراف المعنيين، وذوي الخبرة في القطاع الخاص ومؤسسات المجتمع المدني، مع الاسترشاد بالخبرات والتجارب والبرامج الدولية ذات الصلة، مع اعداد وتدريب المتخصصين في انفاذ القانون في الجهات القضائية والشرطية.

الإطار التنظيمي والتنفيذي: وضع الإطار التنظيمي وانشاء منظومة وطنية لحماية أمن الفضاء السيبراني، وتأمين البنى التحتية للاتصالات وتكنولوجيا المعلومات ونظم وقواعد البيانات والمعلومات القومية وبوابات الخدمة الحكومية والمراقع الحكومية على الإنترنت، وذلك بإعداد وتفعيل ما يعرف بفرق الاستعداد والاستجابة لطوارئ الحاسبات والشبكات، والشبكات في القطاعات الحيوية على المستوى الوطني، انطلاقا من التجربة الرائدة في قطاع الاتصالات وتكنولوجيا المعلومات. تكون هذه الفرق مسئولة عن اعمال المتابعة الأمنية لشبكات الاتصالات والمعلومات الوطنية والحواسب المتصلة بها، وعن التعامل مع أية أخطار سيبرانية تهددها أو هجمات سيبرانية توجه إليها.، وعن التوعية والاعداد لمواجهتها.

البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني: تشجيع ودعم وتنمية البحث العلمي والتطوير ودعم التعاون بين الجهات البحثية والشركات الوطنية خاصة في مجال تحليل البرمجيات الخبيثة المتقدمة ومجال تحليل الأدلة الرقمية، وفي مجال حماية وتأمين نظم التحكم الصناعية، ومجال تطوير أجهزة وأنظمة تأمين النظم والشبكات ومجال التشفير والتوقيع الإلكتروني، ومجال حماية البنى التحتية للاتصالات وتكنولوجيا المعلومات، ومجال تأمين الحواسب السحابية وحماية قواعد البيانات الكبرى ومجال الذكاء الاصطناعي وانتر نت الأشياء.

([١]) الاستراتيجية الوطنية للأمن السيبراني في مصر ٢٠١٧-٢٠٢١.

تنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات بالتعاون والشراكة مع القطاع الخاص والجامعات ومؤسسات المجتمع المدني.

التعاون مع الدول الصديقة والمنظمات الدولية والإقليمية ذات الصلة: وتشمل تبادل الخبرات وتنسيق المواقف في مجال أمن الفضاء السيبراني ومكافحة الجرائم السيبرانية حيث أن تلك الجرائم لا تعترف بالحدود الجغرافية أو السياسية.

التوعية المجتمعية: وضع الخطط وتنفيذ خطط وحملات للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية المؤمنة للأفراد والمؤسسات وبأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها فضلا عن حماية الخصوصية وإطلاق برامج حماية الأطفال والنشء على الانترنت.

النتائج والتوصيات:

أولا النتائج:

١. ساهم التحول الرقمي في تحقيق رفاهية المجتمعات والأفراد من خلال ما يوفره من خدمات متنوعة، وهو ما يوضح أهمية التحول الرقمي ودور في تسهيل عملية تبادل المعلومات والبيانات دون التعرض لحواجز مكانية أو زمانية.

٢. على الرغم من الكثير من الإيجابيات التي أسهمت في تحقيقها التكنولوجيا الرقمية إلا أنها أفرزت العديد من المشكلات والآثار السلبية؛ كطمس الثقافات القومية والقضاءِ على خصوصياتها وفرضِ ثقافات دخيلة لشعوب معينة.

٣. لم تعد القوة العسكرية وحدها هي المُهدد الوحيد للدول بل أصبح امتلاك الدول للقوة الإلكترونية يمثل خطراً أكبر على الدول المستهدفة ومن هنا جاء التحول في مفهوم الأمن، بحيث لم يعد أمن الدولة القومي مقتصر على الأمن العسكري بل أصبح يشمل كافة جوانب الحياة في المجتمع.

٤. يهدف الأمن السيبراني إلى تعزيز حماية جميع ما يتعلق بالدولة والأفراد إلكترونياً لحماية هذه الأنظمة الإلكترونية وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية وجميع مكوناتها.

٥. يرتبط الأمن السيبراني بجميع المسائل الاقتصادية، والاجتماعية والسياسية، والإنسانية، وذلك انطلاقاً من التعريف المعطى له، على أنه قدرة الدولة على حماية مصالحها وشعبها، في مختلف مجالات حياته اليومية، ومسيرته نحو التقدم، بأمان، من جهة أولى، ومن كونه يرتبط ارتباطاً وثيقاً بسلامة مصادر الثروة في العصر الحالي، ونعني بها، البيانات، والمعلومات، والقدرة على الاتصال والتواصل، وهي المحور الذي يتكون حوله الإنتاج، والإبداع، والقدرة على المنافسة، من جهة ثانية.

ثانيا التوصيات:

١. ضرورة أن تقوم السياسات الرقمية بتبني رؤى تسعى ليس إلى توفير البنية التحتية فقط، ولكنها تستهدف مواكبة التطورات التقنية التي تطرأ على هذا الأمر، والاستمرار في هذا التطوير من أجل تحول رقمي آمن.
٢. لابد من بناء مجتمع مسئول ومدرك لمخاطر الفضاء السيبراني، قادر على التعامل مع قواعد السلامة ومدرك للعواقب القانونية التي يمكن أن تترتب على التعرض لسلامة الأفراد والمؤسسات.
٣. ضرورة ترسيخ جذور الثقافة المتعلقة بالأمن السيبراني وتحفيزها.
٤. ضرورة العمل مليًا على تطوير الاستراتيجيات الوطنية ذات العلاقة وتوفير الحماية الفائقة للبنية التحتية لأكثر المعلومات حساسية.

قائمة المراجع

أولا: القواميس:

١. أبو الفضل محمد مكرم بن منظور، لسان العرب، دار صادر للطبع والنشر، بيروت، ٢٠٠.

٢. زكى بدوي، معجم مصطلحات العلوم الاجتماعية، مكتبة لبنان، بيروت، ص ١٩٨٦.

٣. منير البعلبكي، المورد قاموس إنكليزي عربي، دار العلم للملايين، بيروت، ٢٠٠٤.

ثانيا: المراجع باللغة العربية

١.أحمد فرج أحمد، الرقمنة داخل مؤسسات المعلومات أم خارجها؟ دراسة في الإشكاليات ومعايير الاختيار، مجلة دراسات المعلومات، تصدر عن جمعية المكتبات والمعلومات السعودية بالتعاون مع معهد الملك سلمان للدراسات والخدمات الاستشارية، العدد الرابع، يناير ٢٠٠٩.

٢.أحمد محمد رفعت، الإرهاب الدولي، دار النهضة العربية، بدون رقم طبعة، عام ٢٠٠٦.

٣.اسلام فوزي، الأمن السيبراني: الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي، المجلة الاجتماعية القومية، المجلد السادس والخمسون، العدد الثاني، ٢٠١٩.

٤.أشرف عبد الفتاح أبو المجد، التنظيم الدستوري للحقوق والحريات الاقتصادية، منشأة المعارف، ٢٠٠٩.

٥.أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، المجلد الخامس والثلاثون، الجزء الثالث، ٢٠٢٠.

٦.أنديرا عراجي، القوة في الفضاء السيبراني؛ فصل عصري من التحدي والاستجابة، بيروت؛ دار ميرزا للطباعة والنشر والتوزيع، ٢٠١٩.

٧. تغريد معين حسن المشهدي، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، العدد ٣٠.

٨. جون باسيت، الحروب المستقبلية في القرن الحادي والعشرين، مركز الامارات للدراسات والبحوث الاستراتيجية أبو ظبي الامارات ٢٠١٤، ص ٥.

٩. حسام فرحات أبو يوسف، الحماية الدستورية في المساواة، دراسة مقارنة، دار النهضة العربية، ٢٠٠٤.

١٠. حسن رزق سليمان عبدو، النظام العالمي ومستقبل الدولة في الشرق الأوسط، رسالة ماجستير، كلية الآداب والعلوم الإنسانية، جامعة الأزهر، فلسطين، غزة ٢٠١٠.

١١. حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، ٢٠٠٦.

١٢. حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت "دراسة مقارنة "، رسالة قدمت لنيلِ درجة الدكتوراه في القانون من جامعة عين شمس، عام ٢٠٠٧ م.

١٣. حمد الطعامنة، طارق العلوش: الحكومة الإلكترونية وتطبيقاتها في الوطن العربي، المنظمة العربية للعلوم الإدارية، القاهرة، ٢٠٠٤.

١٤. حمدون اتوريه، البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، ٢٠١١.

١٥. حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني، " دراسة مقارنة"، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، ٢٠٢١.

١٦. خالد ظاهر عبد الله جابر السهيل المطيري، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد ٣٨، ٢٠٢٢.

١٧. رأفت عبد الباقي رضوان: الإدارة الإلكترونية الإدارة والمتغيرات العالمية الجديدة، الملتقى الإداري الثاني، الجمعية السعودية للإدارة، الرياض، ١٦-١٧ محرم ١٤٢٥. منال محمد الوكيل، تأثير الإدارة الإلكترونية على القرارات الإبداعية في المنظمات الحكومية مع دراسة تطبيقية على حي غرب مدينة نصر، المجلة العلمية لقطاع كليات التجارة، جامعة الأزهر، العدد ١٦، ٢٠١٦.

١٨. سامر علي السيد السقا، استراتيجية مقترحة لتعزيز الشفافية في المجالس الشعبية المحلية: دراسة مطبقة على المجلس الشعبي المحلي لمركز طلخا، المؤتمر العلمي الدولي الرابع والعشرون للخدمة الاجتماعية" الخدمة الاجتماعية والعدالة الاجتماعية"، كلية الخدمة الاجتماعية، جامعة حلوان، المجلد ٣، ٢٠١١.

١٩. سجان م. غوهيل & بيترك فوستر، المنهج المرجعي لمكافحة الإرهاب، ٢٠٢٠الناتو.

٢٠. سليمان محمد سليمان الطماوي: الضبط الإداري، دراسة مقارنة، مجلة الأمن والقانون، المجلد ١، العدد١، أكاديمية شرطة دبي، ١٩٩٣.

٢١. شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب "التفجير من الداخل" على الساحة الدولية، العربي للنشر والتوزيع، القاهرة، ٢٠١٩.

٢٢. شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد ١٥، العدد ٠١، ٢٠٢٢.

٢٣. عادل عبد الصادق، القوة الالكترونية، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، قوانين وتشريعات، إصدارات مكتبة الإسكندرية، العدد ٢٣، ٢٠١٦.

٢٤. عبد الرحمن عاطف أبوزيد، بحث في الأمن السيبراني في الوطن العربي، دراسة حالة المملكة العربية السعودية، المركز العربي للبحوث والدراسات، العدد ٤٨، عام ٢٠١٩.

٢٥. عبد العزيز أحمد السنهوري، الوسيط في شرح القانون المدني الجديد، نظرية الالتزام بوجه عام، مصادر الالتزام، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٠.

٢٦. فاطمة الزهراء فرحات، دور التحول الرقمي في تحسين أداء وظائف العلاقات العامة في المؤسسات العمومية الجزائرية، دراسة تحليلية لصفحة فيسبوك مديرية الصحة والسكان لولاية أم البواقي، رسالة ماجستير، كلية العلوم الاجتماعية والإنسانية، جامعة العربي بن مهيدي– أم البواقي، الجزائر، ٢٠٢٠.

٢٧. محمد الطاهر، الحريات الرقمية "المفاهيم الأساسية"، مؤسسة حرية الفكر والتعبير، القاهرة، ٢٠١٣.

٢٨. محمد شرف صبحي الدمرداش، معايير التربية على المواطنة الرقمية وتطبيقاتها في المناهج الدراسية، المؤتمر الدولي السادس لضمان جودة التعليم، أنماط التعليم ومعايير الرقابة على الجودة فيه. مسقط، ٢٠١٤

٢٩. محمد عبد البديع السيد، دور وسائل الإعلام الجديدة في دعم المواطنة الرقمية لدى طلاب الجامعة، مجلة بحوث العلاقات العامة، جامعة بنها، العدد ١٢، ٢٠١٦.

٣٠. محمد عبد الحميد، نظريات الاعلام واتجاهات التأثير، ط٣، عالم الكتب، القاهرة، ٢٠٠٤.

٣١. محمد علي حسن شعلان، حوكمة التحول الرقمي في الرؤية السعودية ٢٠٣٠، مجلة المهندس، تصدر عن الهيئة السعودية للمهندسين، العدد ٩٩، ٢٠١٦.

٣٢. محمد موسى على شحاته: انعكاسات تفعيل آليات التحول الرقمي في ضوء مبادرة الشمول المالي على تطبيقات الحكومة الإلكترونية بجمهورية مصر العربية، بحث منشور بمجلة الدراسات التجارية المعاصرة، العدد التاسع يناير ٢٠٢٠.

٣٣. مروه زين العابدين سعد، تأثير تغير مفهوم السيادة على الاختصاص القضائي في الجرائم السيبرانية، المجلة الدولية للفقه والقضاء والتشريع، المجلد ٣، العدد ٣، ٢٠٢٢.

٣٤. مصطفى إبراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي"، مجلة العلوم القانونية والسياسية، مجلد ١٠، العدد الأول، ٢٠٢١.

٣٥. مصطفى أحمد أمين، التحول الرقمي في الجامعات المصرية كمتطلب لتحقيق مجتمع المعرفة، مجلة الإدارة التربوية، العدد التاسع عشر، ٢٠١٨.

٣٦. منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني، لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد ١١١، ٢٠٢٠.

٣٧. ناصر محمد عبيد الساعدي، د/ هناء على محمد الضحوي، استراتيجية تعزيز المواطنة والاعتدال باستخدام وسائل التواصل الاجتماعي لمواجهة التحديات والتطرف والتكفير في دول مجلس التعاون الخليجي، بحث فائز بمسابقة جائزة الأمير خالد الفيصل للاعتدال، ٢٠١٧.

٣٨. الهيئة السعودية للبيانات والذكاء الاصطناعي، سياسات حوكمة البيانات الوطنية، مكتب إدارة البيانات الوطنية، ٢٠٢١.

٣٩. وليد رشاد زكي، السياسات الرقمية وترشيد صناعة القرار، إصدارات مركز المعلومات ودعم اتخاذ القرار، رئاسة مجلس الوزراء، ٢٠٢١.

٤٠. ـــــــــ، من الأمن الصحي إلى الأمن السيبراني، الأمن والحياة، جامعة نايف للعلوم الأمنية، المملكة العربية السعودية، ٢٠٢٠، العدد ٤٣٣.

٤١. يحي الجمل، مبدأ المواطنة والتعديلات الدستورية، مقال بجريدة المصري اليوم، العدد٩٥٣، ٢٢ يناير ٢٠٠٧

٤٢. يوسف بوغرارة، الأمن السيبراني" الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني، مجلة الدراسات الأفريقية وحوض النيل، المركز العربي، العدد الثالث، ٢٠١٨.

٤٣. يونس مؤيد يونس، استراتيجية الولايات المتحدة الامريكية لأمن السيبراني، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، بغداد، العدد ٥٥، ٢٠١٨.

ثالثا: القوانين

١. دستور جمهورية مصر العربية ٢٠١٤

رابعا: القرارات:

١. قرار رئيس مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤

خامسا التقارير:

١. مكتب الأمم المتحدة المعنى بالمخدرات والجريمة، استخدام الإنترنت في أغراض إرهابية، بالتعاون مع فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ تدابير مكافحة الإرهاب، نيويورك، عام ٢٠١٣.

٢. جاي مارتن& وآخرون، حماية نظم الرعاية الصحية، إطار عالمي للأمن السيبراني، تقرير شبكة الأنظمة الصحية الرائدة ٢٠٢٠، تقرير إليكتروني، معهد الابتكار في مجال الصحة العالمية في إمبريال كوليدج لندن، ٢٠٢٠.

٣. الاستراتيجية الوطنية للأمن السيبراني في مصر ٢٠١٧-٢٠٢١.

سادسا: المراجع باللغة الإنجليزية

1. Abdurrahman, O., & Omar, I. M. و The Impact of Applying Electronic Management System on the English Language Level: A Case study at Cihan University. International Journal of Research and Engineering, 5(7), 2018.
2. Acemoglu, Hasan, and Tahoun, The Power of the Street: Evidence from Egypt's Arab Spring." NBER Working Paper 20665, National Bureau of Economic Research, Cambridge, MA, 2014,
3. Amosa Desmond Uelese, Local Government and Good Governance: the Case of Samoa, Commonwealth Journal of Local governance, Issue 7, 2010.
4. Bennet, Breunig and Givens, Communication and Political Mobilization: Digital Media and the Organization of Anti-Iraq War Demonstrations." Political Communication 25 (3), 2008.
5. Bhagwat, Jagdihln, Defiance of Globalization, New York, Oxford University Pressm, 2004.
6. Catota, Frankie E ؛Morgan1, M. Granger and Douglas C. Sicker, Cybersecurity education in a developing nation, the Ecuadorian environment, Journal of Cybersecurity, 00(0), 2019.
7. Jyoti Rattan and Vijay Rattan, Cyber Laws & Information Technology, Bharat Law House, Delhi, 2014.
8. K. K. Panigrahi, Information Security and Cyber Law , published by tutorials point ,2015
9. Kretschmer Tobias and Khashabi Pooyan, Digital Transformation and Organization Design: An Integrated Approach, California Management Review, Vol. 62(4) 86–104, 2020.
10. Lene Hansen– Helen Nissenbaum, Digital Disaster, Cyber Security, and the Copenhagen School, International Studies Quarterly, 2009.

11. Matthew C. Waxman, "Cyber-Attacks and the Use of Force, The Yale Journal of International،Back to the Future of Article 2 (4), Vol. 36, 2011.
12. Maye, Terry & Others, Transforming Higher Education through Technology-Enhanced Learning, the Higher Education Academy, York Science Park, Heslington, 2009.
13. Myriam Dunn, Information Age Conflicts, A Study of the, Center،Information Revolution and a Changing Operating Environment, ETH Zurich،for Security Studies (CSS, Issue No 64,2002.
14. Richard A. Kemmerer, Cyber security, University of California, Santa Barbara Department of Computer Science, 2003.
15. World Economic Forum, Digital Transformation Initiative Professional Services Industry, White Paper, Committed To Improving The State Of The World, January 2017.

سابعا: المراجع الفرنسية:

1. La Rose Tara and Detlor Brian, Research on Social Work Practice, 2021.
2. Ropport De Synthes, Décentralisation Et Gouvernance Locale en Afrique, Etude Comparative Sur L'Appropriation De La Reforme Par Les Communautés Rurales Au Mali et au Burkina Faso, Center For Research on Local Knowledge,2007.

ثامنا: مواقع النت:

1. Strategie Nationale pour La Securite Du Numerique, 2015 https://www.ssi.gouv.fr/
2. Hollenbach, Florian, and Jan Pierskalla, Voicing Discontent: Communication Technology and Protest." APSA Annual Meeting paper,2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2452306
3. https://www.my.gov.sa/wps/digitaltransformation , 1/1/2023.
4. https://ar.wikipedia.org/wiki/
5. Ghafur S, et al. Improving Cyber Security in the NHS. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/ imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf
6. Tham I, et al. Sing Health cyber-attack: How it unfolded. The Straits Times, 20 July 2018:

https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/ sg-cyber-breach/index.html

7. Eddy N. Alabama hospital system DCH pays to restore systems after ransomware attack. Healthcare IT News; 7 October 2019. www.healthcareitnews.com/news/ alabama-hospital-system-dch-pays-restore-systems-after-ransomware-attack

8. Miles R. Life Healthcare announces cyberattack. Intelligent CISO, 11 June 2020.

www.intelligentciso.com/2020/06/11/life-healthcare-announces-cyberattack/

9. Https: //en. oxforddictionaries. com/definition/cyber

10. Raia Prokhovnik Internal/external: The state of sovereignty, Contemporary Politics, 1996, Vol. 2, Issue 3، PP. 7-20, Available on:https://www.tandfonline.com/doi/abs/10.1080/13569779608454736

11. Http://alwatan.com/details