مداخلة بعنوان :

الجهود الدولية لحماية الأمن الرقمي

من إعداد: لمنور مرمي

طالب دكتوراه- كلية الشريعة والاقتصاد

جامعة الأمير عبد القادر- قسنطينة

تحت إشراف: الدكتورة حفيظة مبارك

أستاذ محاضر (أ)

جامعة الأمير عبد القادر- قسنطينة

الملخص

تعالج هذه الدراسة الضمانات الدولية ، الإقليمية والعربية لحماية الأمن الرقمي من الجرائم الالكترونية، وذلك بسبب التطور الحاصل في مجال التكنولوجيا العالمية ، حيث أصبحت قضية الأمن الرقمي أو السيبراني من التحديات الكبرى التي تواجهها الدول على الصعيدين الإقليمي والعالمي لاسيما مع تزايد حجم التهديدات الأمنية التي تصيب أمن ومعلومات الدول مما يؤدي إلى اختراق أمنها الوطني وانهياره.

لذا سيتم التركيز في هذه الدراسة على مفهوم الأمن الرقمي، مفهوم الجرائم الالكترونية وأثرها على الأمن الرقمي للدول، ثم التعرف على الآليات والضمانات الدولية والإقليمية والعربية لحماية الأمن الرقمي .

Summary

This study deals with international, regional and Arab guarantees to protect digital security from cybercrime, due to the development taking place in the field of global technology, as the issue of digital or cyber security has become one of the major challenges faced by countries at the regional and global levels, especially with the increasing volume of security

threats affecting the security And the information of countries, which leads to the penetration and collapse of their national security.

Therefore, this study will focus on the concept of digital security, the concept of electronic crimes and their impact on the digital security of countries, and then identify the international, regional and Arab mechanisms and guarantees to protect digital security.

مقدّمة :

الحمد لله الذي خلق الإنسان من عدم وعلمه مالم يعلم، ورغّبه في العلم والتعليم، والصلاة والسلام على هادي البشرية ومعلم الإنسانية الذي أمر بالقراءة ورغّب في طلب العلم والتعلّم وحث عليه ،أما بعد :

يشهد المجتمع الدولي اليوم تطورا متسارعا لتكنولوجيا المعلومات والاتصالات، كما يعرف تزايدا وتنوعا في التطبيقات والخدمات الإلكترونية التي تعتمد الفضاء الرقمي أو السيبراني أساسا لها . ولأن تكنولوجيا المعلومات والاتصالات أصبحت الركيزة الأولى لبناء مجتمع المعرفة ولبنة أساسية في نموه وازدهاره، ذلك أن معظم فئاته من مستخدمي شبكة الأنترنت. حيث أصبحت الشبكة العنكبوتية فضاء كبير يوفر بيئة التواصل و العمل والتوثيق لكل المستخدمين من البشر ، و فاقت كل الإمكانيات التكنولوجية والرقمية .وأصبحت وسطا تنساب فيه البيانات المحتضنة وتتعدد الأخطار التي تهدد استقرار تلك الشبكات وأمنها كالإصابة بالفيروسات والبرامج الضارة لأغراض سرقة المعلومات وغيرها ، مما أدى إلى زيادة وسائل التجسس على الأفراد والمؤسسات لاختراق الأجهزة الأمنية .

فالتطور التكنولوجي السريع مثلما أصبح نقطة قوة متمثلة في توفير لوازم حماية هوية وبيانات الداخلين إليها وسرعة انتشارها واتساع نطاقها ، تحول إلى نقاط ضعف تغريهم بانتهاج هذا المسلك الإجرامي والاستمرار فيه وذلك لقلّة المخاطر التي يتعرضون إليها بالقياس مع ماهو حاصل في الجرائم العادية ، فلا يكون هناك تسلق يخشى منه كسر ولا مداهمة قد تعرض لإطلاق نار ،إضافة إلى بساطة الجهد المطلوب في ارتكاب الجريمة وصعوبة اعتراض السلوك المجرم في غياب وجود حواجز جغرافية ، ولغموض وتعقيد التقنيات المستخدمة في ارتكاب الجريمة وصعوبة التعرف على هويات مرتكبيها وسهولة إخفاء الطابع الجرمي، لما يقوم به هؤلاء من عمل بالغ الخطورة على المصلحة التي يستهدفونها ، إضافة إلى عدم علم الضحية بأنها مستهدفة إلى أن يتم الاعتداء عليها. وهذا النشاط الإجرامي سمي بما يعرف بالجريمة الإلكترونية والتي تعتبر جرائم جنائية ترتكب بواسطة الشبكة المعلوماتية والمعلومات الإلكترونية .

ومع تزايد حجم الجرائم الإلكترونية وخطورتها ،كان لابد من وضع حد لها ومحاربتها بشتى الطرق التي تكون غايتها حماية حسابات الأنترنت واستعمالها دون التعرض لأي تهديدات أو مراقبة تهدد سرية المعلومات ، وهو ما يعرف بالأمن الرقمي.

مما سبق ولمعالجة هذه الظاهرة ، نتوصل إلى طرح الإشكال الرئيسي التالي :

ماهي الضمانات التي تدعم الأمن الرقمي وتحميه من آثار وسلبيات الجرائم الالكترونية ؟

ويندرج تحت هذه الإشكالية جملة الأسئلة الفرعية التالية :

- ما مفهوم الأمن الرقمي ؟
- ما مفهوم الجريمة الإلكترونية ؟
- ماهي ضمانات الأمن الرقمي في الاتفاقيات الدولية ؟
- ماهي ضمانات الأمن الرقمي في الاتفاقيات الإقليمية ؟
- ماهي ضمانات الأمن الرقمي في الاتفاقيات العربية ؟

خطة البحث :

لقد قسمنا موضوع البحث إلى مقدمة ومبحثين وخاتمة، حيث تناولنا في المبحث الأول الاطار المفاهيمي للأمن الرقمي والجرائم الإلكترونية ، بحيث تم تقسيم هذا المبحث إلى مطلبين رئيسيين، الأول لتعريف الأمن الرقمي، أما المطلب الثاني خصص لمعرفة مفهوم الجريمة الالكترونية .

وتطرقنا في المبحث الثاني إلى الضمانات والاتفاقيات التي تتحكم في الأمن الرقمي على المستويات الدولية، الإقليمية والعربية، وسنذكر بجهود التشريع الجزائري في هذا المجال.

المبحث الأول : الإطار المفاهيمي للأمن الرقمي والجريمة الإلكترونية

يعتبر الأمن الرقمي الأساس في قطاع الاتصالات وتقنية المعلومات والتي تعتبر الحد الأدنى من السياسات الأساسية للأمن الرقمي والتي تساعد في تخفيف أثر التهديدات الأمنية الرقمية في قطاع الاتصالات وتقنية المعلومات إذا ما تم تطبيقها بفعالية .كما يعد التحول الرقمي ضرورة ملحة في الوقت الراهن في ظل الحاجة إلى تنويع كل القطاعات . سنقسم هذا المبحث إلى مطلبين أساسيين ؛ خصصنا الأول لمعرفة مفهوم الأمن الرقمي، أما المطلب الثاني فيتناول مفهوم الجريمة الإلكترونية.

المطلب الأول : مفهوم الأمن الرقمي

تتعدد تعريفات الأمن الرقمي وتتنوع حسب زاوية الرؤية ، فلو نظرنا من ***زاوية أكاديمية*** سنجد أنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها .

ومن ***زاوية تكنولوجية وفنية*** بحتة يمكن تعريفه على أنه : الوسائل والأدوات والإجراءات المطلوب توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية .

أما من ***الناحية القانونية*** نجد التعريف يأخذ منحى آخر لكونه يركز على التدابير والإجراءات التي من شأنها حماية سريّة وسلامة و خصوصية محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجَريمة المعلوماتية [1].

ويعرف الأمن الرقمي بأنه كيفية استخدام شبكة الانترنت استخداما فعالا بدون التعرض لأي تهديدات أو مخاطر أو مراقبة تهدّد خصوصية وسرية المعلومات. وفي إطار ثورة التكنولوجيا والتطور المتسارع للتقنيات الرقمية، أصبح أكثر من نصف سكان العالم يستخدمون الأنترنت ومواقع التواصل الاجتماعي بشكل يومي، وذلك كونها الوسائل الحديثة المستخدمة بطريقة أسهل وأسرع للتواصل بين الأفراد والمجتمعات لتبادل المعلومات سواء على الصعيد المهني أو الإنساني.

فقد أصبح النشاط الرقمي يحتكّ بالحريات والحق في الخصوصية والأمان ، في مقابل رغبة الدول في مراقبة مواطنيها والتحكّم في نشاطاتهم في إطار مايعرف بالمراقبة المخابراتية ، وهذا لرصد نشاط بعض الأفراد أو اختراق حساباتهم وذلك حفاظا على أمنها واستقرارها الداخلي. وفي ظل هذه التغيرات والحريات وصراعات القوى الدولية والأنظمة الدائمة مع الحقوق والحريات الإنسانية نشأ مفهوم الأمن الرقمي لحماية الأفراد والجماعات والمنظمات من التهديدات والمخاطر التي قد يواجهونها عند استخدام شبكة الأنترنت بصفة عامة [2].

وانطلاقا من أهدافه يمكن تعريف الأمن الرقمي بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن إمكانيات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن ، بحيث تتوقف عجلة الإنتاج، و لا تتحول الأضرار إلى خسائر دائمة . وهو النشاط أو العملية والقدرة أو نظم المعلومات واتصالات الدولة حيث تكون المعلومات الواردة فيه محمية من أي دافع من التلف والاستخدام غير المصرح به أو التعديل أو الاستغلال[3].

---

[1] جمال محمد غيطاس ،الأمن المعلوماتي والجرائم الإلكترونية ، أدوات جديدة للصراع ، مركز الجزيرة للدراسات، 29 فيفري 2012 ، الموقع http://studies.aljazeera.net/ar/issues/2012/02.

[2] مركز " هاردو " لدعم التعبير الرقمي؛ **الأمن الرقمي وحماية المعلومات، الحق في استخدام شبكة آمنة** ، القاهرة، 2017، ص6 ،(http://hrdo egypt.org)

[3] بارة سميرة ،الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر (الدور والتحديات) جامعة قاصدي مرباح ، ورقلة،الجزائر ، ص 427.

ومن الناحية العلمية الإجرائية يمكن تلخيص الأمن السيبراني على أنه لا يتعدى المفاهيم التالية :

- يتكون الأمن السيبراني إلى حد كبير من وسائل دفاعية تستخدم لكشف وإحباط المتسللين ؛
- الأمن السيبراني ينطوي على حماية شبكات الكمبيوتر و المعلومات التي تحتويها من الاختراق ومن الضرر الخبيث ومن التعطيل ؛
- كما ينطوي على الحد من هجوم المخاطر الخبيثة على البرمجيات وأجهزة الكمبيوتر والشبكات ، وهذا يشمل الأدوات المستخدمة للكشف عن اقتحام ووقف الفيروسات ، ومنع وصولها وفرض التوثيق وتمكين الاتصالات المشفرة [1].
- الأمن السيبراني هو : مجموعة من الأدوات والسياسات والمفاهيم والضمانات الأمنية والمبادئ التوجيهية من المخاطر المحدقة بالمعلومات، ومعالجتها والإجراءات والتدريب وأفضل الممارسات وضمانات التقنيات التي يمكن استخدامها لحماية البيئة الإلكترونية وتنظيم أصول المستخدم .
- هو القدرة على الحماية أو الدفاع عن استخدام الفضاء الإلكتروني من الهجمات السيبرانية ،وهو التكنولوجيات والعمليات والممارسات وتدابير الاستجابة والتخفيف والتي تهدف إلى حماية الشبكات وأجهزة الكمبيوتر والبيانات من هجوم أو تلف أو الوصول غير المصرح به، وذلك لضمان السرية والنزاهة [2].
- وللوصول إلى تعريف يتصف بالشمولية للأمن السيبراني يستدعي الوقوف عند مجموعة من العناصر تعد الفاعلة والمتحكمة في تحقيقه وهي (التكنولوجيا –الأحداث – الاستراتيجيات –العمليات والأساليب –الإنسان والمرجع الأمني) . وبالتمعن في هذه العناصر نتوصل إلى أن الأمن الرقمي يجب أن يتميز بمايلي :
- طابع متعدد التخصصات الاجتماعية والتقنية .
- كونه شبكة خالية من الحجم وقدرات الفاعلين يمكن أن تكون مماثلة على نطاق واسع .
- درجة عالية من التغيير والترابط وسرعة التفاعل .

ونخلص إلى أن الأمن الرقمي : هو عبارة عن برامج وآليات وقدرات بشرية تَفعل لمواجهة أي تعدي على المعلومات الإلكترونية بشتى أنواع الجريمة الإلكترونية .

---

[1] Douwe Korff ,CYBER SECURITY DEFINITIONS –a selection .P1,in :https://www.sbs.ox.ac.uk /cyberesecurity – capacity /system /fils /CPDP20201520 - KORFE Handout .pdf .

[2] منى الأشقر ،الأمن السيبراني –التحديات ومستلزمات المواجهة – اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني ، بيروت ، من 27 إلى 28 أوت 2012 م ،جامعة الدول العربية ، المركز العربي للبحوث القانونية والفضائية ، ص 15 .

و الأمن الرقمي هو كيفية استخدام شبكة الأنترنت استخداما فعالا بدون التعرض لأي تهديدات ، مخاطر أو مراقبة تهدد خصوصية وسرية المعلومات وهو استخدام المتعمد لأنظمة الحاسب الآلي ، الشبكات والجهات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية بهدف إحداث أضرار[1] .

المطلب الثاني : مفهوم الجريمة الإلكترونية

الجريمة الإلكترونية هي تلك الممارسات التي توقع ضد فرد أو مجموعة مع توفر باعث إجرامي بهدف التسبب بالأذى لسمعة الضحية عمدا ،أو إلحاق الضرر النفسي والبدني به سواء كان ذلك بأسلوب مباشر أو غير مباشر بالاستعانة بشبكات الاتصال الحديثة كالانترنت وما تتبعها من أدوات كالبريد الإلكتروني وغرف المحادثة والهواتف المحمولة [2].

يشار إليها أنها : إساءة استخدام تكنولوجيا المعلومات والاتصالات من قبل المجرمين بالتبادل على أنها جرائم انترنت أو إساءة استخدام الكمبيوتر والجريمة المرتبطة بالحاسب الآلي [3]، جريمة التكنولوجيا العالية والجريمة الإلكترونية كما عرفتها رابطة كبار ضباط الشرطة أنها :" تنطوي على استخدام الكمبيوتر أو الانترنت شبكات تكنولوجيا لارتكاب أو تسهيل ارتكاب الجريمة " ، أما المعهد الأسترالي لعلم الإجرام فيرى أنها "تسمية عامة لجرائم ارتكبت باستخدام تخزين البيانات الإلكترونية أو جهاز الاتصالات [4].

لا يوجد إجماع عل تعريف الجريمة الإلكترونية من حيث كيف تعرف أو ماهي الجرائم التي تتضمنها الجريمة الإلكترونية ، وكما يقول *[فان دير هلست و نيف]* :(هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة .. وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والالكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف)[5].

---

[1] بارة سميرة ، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر ، مرجع سابق ، ص 428 .

[2] مركز هردو لدعم التعبير الرقمي ، التنظيم القانوني والجرائم الإلكترونية –ما بين أمن المعلومات وتقييد الحريات – الإصدارة3 غير الموطنة القاهرة ،2018 ، ص 7 .

[3] بارة سميرة ، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر ، - الدور والتحديات - ،جامعة قاصدي مرباح ، ورقلة ص 428 .

[4] Cameron S.D Brown ,*Investigating and Prosecuting Cyber Crim :Forensic Dependencies and Barries and to justice *,International Journal of Cyber Criminology .Vol9 ,Jssue 1 ,january –june 2015 , p57 .

[5] Van der hulst & Neve, 2008, P.18

(ذياب موسى البداينة، الجرائم الإلكترونية ، المفهوم والأسباب، ورقة علمية مقدمة في الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية (7 إلى 1435/11/9هـ الموافق: 2 إلى 2014/9/4م) ، عمان ، المملكة الأردنية الهاشمية ، 2014 ، ص 3.)

ويتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية . وتعرف الجرائم الإلكترونية على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال[1].

وهناك من عرفها على أنها الجرائم ذات الطابع المادي التي تتمثل في كل سلوك غير قانوني من خلال استخدام الأجهزة الالكترونية ينتج منها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة، وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل السرقة أو إتلاف المعلومات الموجودة في الأجهزة، ومن ثم ابتزاز الأشخاص باستخدام تلك المعلومات.[2]

ولقد عرفها الأستاذ [جون فورستر] بأنها فعل إجرامي يستخدم الكمبيوتر في ارتكابها كأداة رئيسية.[3]

كما أن هناك جانب من الفقه لايهتم بالوسيلة أو موضوع الجريمة المعلوماتية ويعرفها بوصفها مرتبطة بالمعرفة الفنية والتقنية باستخدام الحاسب الآلي ، لذلك عرفت هذه الجريمة بأنّها أية جريمة يكون متطلب اقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب. وبذلك عرفها الدكتور هشام فريد رستم بأنها أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه.[4]

تتكون الجريمة الإلكترونية أو الافتراضية (cyber crimes) من مقطعين ،هما الجريمة(crime والالكترونية(cyber)؛

- ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات.
- أما الجريمة فهي السلوكيات والأفعال الخارجة عن القانون .

والجرائم الإلكترونية هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشرة أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت (كغرف الدردشة ، البريد الإلكتروني و الموبايل)[5].

---

[1] ذياب موسى البداينة ، ***الجرائم الإلكترونية –المفهوم والأسباب*** ،الملتقى العلمي : الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان ، 1435 هـ/ 2014 م ، ص 3.

[2] مجلة تكنولوجيا المعلومات، قسم نظم المعلومات، دون دار نشر. نقلا عن مختارية بوزيدي، ماهي الجريمة الالكترونية، سعيدة، الجزائر، 2017

[3] خالد عياد الحلبي، **إجراء التحري والتحقيق في جرائم الحاسوب والانترنت** ، دار الثقافة للنشر و التوزيع، الأردن، بدون طبعة، 2011، ص 29.

[4] عادل يوسف عبد النبي البشكري، **الجريمة المعلوماتية وأزمة الشرعية الجزائية**، العدد 7، الكوفة، العراق، ص113.

[5] Halder ,D. & jaishankar ,K. (2011): ***Cyber crime and the victimization of woman :Laws ,Rights and Regulations*** ,.Hershey ,PA ,USA :IGI Global .ISBN 978- 1- 60960 -830 -9 .

ومن التعريفات التي وضعها أنصار **الاتجاه الضيق** أن الجريمة الإلكترونية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر ، بقدر كبير، لازما من ناحية؛ وملاحقته من ناحية أخرى. كما عرفها هذا الاتجاه بأنها الجريمة التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط.

أما أصحاب **الاتجاه الموسع** يعرفونها بأنها كل سلوك إجرامي يتم بمساعدة أو باستخدام الكمبيوتر.[1]

كما عرفت بأنها الممارسات التي توقع ضد فرد أو مجموعة من الأفراد، مع توفر باعث إجرامي بهدف التسبب بالأذى لسمعة الضحية عمدا أو إلحاق الضرر النفسي والبدني به سواء كان ذلك بأسلوب مباشر أو غير مباشر بالاستعانة بشبكات الاتصال الحديثة كالانترنت وما تتبعها من أدوات كالبريد الإلكتروني وغرف المحادثة والهواتف المحمولة [2].

وأدت الحداثة التي تتميز بها الجريمة الإلكترونية واختلاف النظم القانونية والثقافية بين الدول إلى اختلاف في مفهوم الجريمة الالكترونية من بينها :

- حسب اللجنة الأوروبية فإن مصطلح الجريمة الإلكترونية يضم كل المظاهر التقليدية للجريمة مثل الغش وتزييف المعلومات ونشر مواد إلكترونية ذات محتوى مخل بالأخلاق أو دعوى لفتن طائفية .
- حسب وزارة العدل في الولايات المتحدة الأمريكية التي عرفت الجريمة عبر الأنترنت بأنها :"أي جريمة معرفة فنية بتقنية الحاسبات تمكنه من ارتكابها ".
- حسب منظمة التعاون الإقتصادي للجريمة المرتكبة عبر الأنترنت :" هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به ، يتعلق بمعالجة آلية للبيانات ونقلها" [3].

بعدما تم تحديد مفهوم الأمن الرقمي والجريمة الالكترونية ، سنتطرق إلى الضمانات والاتفاقيات التي تنظم الأمن الرقمي على المستويات الدولية، الإقليمية والعربية في ***المبحث الثاني***.

---

[1] محمود ابراهيم غازي؛ الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2014، ص 118.

[2] مركز هردو لدعم التعبير الرقمي ،التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات ،القاهرة ، 2017 ، الإصدار 3 ، ص 7. (http: www.hrdo egypt .org)

[3] الجريمة المعلوماتية، نقلا عن موقع :(http: ar.m.wikipedia.org)، تاريخ التصفح 2021/4/28.

المبحث الثاني : الأمن الرقمي في الاتفاقيات الدولية والإقليمية والتشريعات العربية

تعتبر هذه الاتفاقيات في مجملها كضمانات أساسية لحماية وتطوير الأمن الرقمي على المستويات الدولية والإقليمية، من أجل ذلك قسمنا هذا المبحث إلى ثلاث مطالب كالآتي؛

المطلب الأول : الأمن الرقمي في المواثيق و الاتفاقيات الدولية

إن مجمل المواثيق و الاتفاقيات الدولية المتعلقة بحقوق الإنسان تعبر عن التزام الدول باحترامها لخصوصية الأفراد، وذلك يثبت من خلال مراجعة النصوص الداخلية للدول وتعديلها حسب نصوص المواثيق والاتفاقيات الدولية والتي تكون الدولة طرفا فيها، ولقد أصبح الآن معروفا بأن بعض أحكام المواثيق والاتفاقيات قد ارتقت وأصبحت قواعد عرفية، ما يعني إلتزام الدول بها حتى ولو كانت غير موقعة عليها[1].

ومن أبرز هذه المواثيق **الإعلان العالمي لحقوق الإنسان** ، و الذي نص على: (لا يجوز أن يتعرض أحد للتدخل التعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو بحملات على شرفه وسمعته ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات) [2].

أما عن العهد الدولي للحقوق المدنية والسياسية فقد نص على ضرورة عدم التدخل بشكل تعسفي أو غير قانوني في خصوصيات الشخص وأسرته وحرمة مسكنه و **سرية مراسلاته والحفاظ على سمعته وشرفه**[3].

بالإضافة إلى المواثيق والاتفاقيات السالفة الذكر سوف نذكر بعض القرارات والمواثيق الدولية التي تدعم حماية الأمن الرقمي والخصوصية الرقمية، ومنها الآتي؛

الفرع الأول: قرار الجمعية العامة للأمم المتحدة بشأن حماية حق الخصوصية الرقمية

عندما أصبحت مناقشة الحقوق الرقمية تحتاج إلى تركيز خاص مباشرة وليس ربط بالحقوق الإنسانية الأصيلة التي تم إقرارها دوليا ، جاء قرار الجمعية العامة للأمم المتحدة رقم 166/69 بشأن الحق في الخصوصية في العصر الرقمي والذي جاء نصه :

"أن الجمعية العامة إذ تؤكد من جديد مقاصد ميثاق الأمم المتحدة ومبادئه ،وإذ تؤكد من جديد حقوق الإنسان والحريات الأساسية بصيغتها المكرسة في الإعلان العالمي لحقوق الإنسان ومعاهدات حقوق الإنسان الدولية ذات الصلة ، بما في ذلك العهد الدولي الخاص بالحقوق المدنية والسياسية والعهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، وإذ تؤكد من جديد كذلك إعلان وبرنامج فيينا ، وإذ تشير إلى قرارها 167/68 المؤرخ في 18 ديسمبر 2013 م ،بشأن

---

[1] رزق سلمودي وليندا ربايعة وآخرون؛ الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي، مجلة الجامعة العربية الأمريكية للبحوث، مجلد 3، العدد 2، 2017، ص9.

[2] المادة 12 من الإعلان العالمي لحقوق الانسان، الصادر في 10 ديسمبر 1948،هيئة الأمم المتحدة.

[3] المادة 17 من العهد الدولي للحقوق المدنية والسياسية الصادر 16 ديسمبر 1966، ودخل حيز التنفيذ سنة 1976، هيئة الأمم المتحدة.

الحق في الخصوصية في العصر الرقمي[1] .وإذ ترحب باتخاذ مجلس حقوق الإنسان القرار 13/26 المؤرخ في 26 حزيران 2014 بشأن تعزيز وحماية حقوق الإنسان على الأنترنت والتمتع بها[2].

أكدت الجمعية العامة على الحاجة إلى مواصلة القيام بمناقشة وتحليل المسائل المتصلة بتعزيز وحماية الحق في الخصوصية في العصر الرقمي ،والضمانات الإجرائية والرقابة وسبل الإنصاف المحلية الفعالة ، وأثر المراقبة على الحق في الخصوصية الرقمية وغيره من حقوق الإنسان .وسلمت بالتصدي بفعالية للتحديات المرتبطة بالحق في الخصوصية في سياق تكنولوجيا الاتصالات الحديثة والذي يوجب مواصلة العمل المتضافر من جانب أصحاب المصلحة المتعددين بشأن الانترنت في الاجتماع المعقود في ساو باولو في البرازيل في أفريل 2014 [3]. كما تجدر الإشارة إلى سرعة وتيرة التطور التكنولوجي والتي تمكن الأشخاص في العالم بأسره من استخدام تكنولوجيا المعلومات والاتصالات الجديدة ،وتعزز في الوقت نفسه قدرة الحكومات والشركات والأشخاص على مراقبة الاتصالات واعتراضها وجمع البيانات ،مما قد يؤدي إلى انتهاك حقوق الإنسان أو النيل منها ، ولا سيما الحق في الخصوصية على النحو المبين في المادة 16 من الإعلان العالمي لحقوق الانسان والمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية [4].

كما تلاحظ أن البيانات الوصفية يمكن أن تترتب عليها فوائد إذا تم تجميعها يمكن أن تكشف عن المعلومات الشخصية ويمكن أن يكتشف منه سلوك الشخص ،وعلاقاته الاجتماعية وأفضلياته الخاصة وهويته .وتؤكد على أن مراقبة الاتصالات الرقمية يجب أن تكون منسقة مع الالتزامات الدولية المتصلة بحقوق الإنسان وأن تتم بالاستناد إلى إطار قانوني متاح للعموم وواضح ودقيق وخال من التمييز .وعندما تعترض الاتصالات الرقمية للأشخاص وتجميع البيانات الشخصية عندما تتطلب الإفصاح عن البيانات الشخصية من أطراف ثالثة بما في ذلك الشركات الخاصة وجب على الدول الالتزام[5].

كما تسلم الجمعية العامة بالطبيعة العالمية والمفتوحة للانترنت وبالتقدم السريع في مجال تكنولوجيا المعلومات والاتصالات كقوة دافعة لتسريع خطى التقدم على طريق التنمية بمختلف أشكالها .كما تؤكد على أن الحقوق نفسها التي يتمتع بها الأشخاص خارج الأنترنت يجب أن تحظى بالحماية أيضا على الأنترنت بما في ذلك الحق في الخصوصية [6].

---

[1] الأمن الرقمي وحماية المعلومات ؛ الحق في استخدام شبكة آمنة ، مركز هردو لدعم التعبير الرقمي ، القاهرة ، 2017 ، ص 10 .

[2]الوثائق الرسمية للجمعية العامة ،الدورة التاسعة والستون ،الملحق رقم 53 ،(A53/69/)

[3] الوثائق الرسمية للجمعية العامة الدورة الثالثة والأربعون ، الملحق رقم 40 ،(A/43/40) المرفق السادس .

[4] قرار الجمعية العامة للأمم المتحدة رقم 166/69 ،الحق في الخصوصية في العصر الرقمي ،الصادر في 18 ديسمبر 2014 ، الدورة التاسعة والستون ، بناءا على تقرير اللجنة الثالثة ،البند 68/ ب من جدول الأعمال ،ص 2 و 3 .

[5] قرار الجمعية العامة للأمم المتحدة رقم 166/69 ،نفس المرجع ، ص 3 .

[6] المادة 2 و3 من قرار الجمعية العامة رقم 166/69 .

كما توجب احترام وحماية الحق في الخصوصية بما في ذلك سياق الاتصالات الرقمية واتخاذ التدابير اللازمة لوضع حد لانتهاكات ذلك الحق ، مع مراقبة الاتصالات وجمع البيانات الشخصية لضمان تنفيذ الالتزامات المترتبة عليها بموجب القانون الدولي لحقوق الإنسان[1] .

الفرع الثاني : إعلان القمة العالمية حول مجتمع المعلومات (wsis)

حيث تم عقدها عام 2003 حول مجتمع المعلومات تحت رعاية الأمم المتحدة ،تم خلالها تبني إعلان مبادئ القمة العالمية حول مجتمع المعلومات ،والذي يعيد التأكيد على شمولية حقوق الإنسان وحرياته الأساسية وعدم تجزئتها والترابط فيما بينها إضافة إلى الحوكمة الرشيدة على كل المستويات .كما يشير هذا الإعلان إلى أهمية حق حرية التعبير في مجتمع المعلومات .كما أقر أيضا بأنه من الضروري منع استخدام موارد وتقنيات المعلومات للأغراض الجنائية والإرهابية مع احترام حقوق الإنسان [2].

الفرع الثالث: ميثاق حقوق الأنترنت لجمعية الاتصالات المتقدمة (APC)

حيث تم وضع ميثاق حقوق الأنترنت على يد جمعية الاتصالات المتقدمة (APC) بأوربا في براغ ، في شهر فيفري 2001م . ويقوم هذا الميثاق على ميثاق الاتصالات الشعبي، ويهدف إلى تطوير الوصول إلى الانترنت للجميع وحرية التعبير وحرية التنظيم ، الوصول إلى المعارف والتعليم المشترك والتأليف ، وتطوير البرمجيات مفتوحة المصدر المجانية .

وتطوير التقنيات ،الخصوصية ،المراقبة والتشفير، تطوير حوكمة الأنترنت وحماية الوعي وإعمال حقوق الإنسان على النحو المجسد في الإعلان العالمي لحقوق الإنسان والعهد الدولي للحقوق المدنية والسياسية والعهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، واتفاقية القضاء على جميع أشكال التمييز ضد المرأة.[3]

المطلب الثاني : الأمن الرقمي في الاتفاقيات الإقليمية

لقد عرف الأمن الرقمي اهتماما واسعا على المستوى الاقليمي، لذلك قسمنا هذا المطلب إلى ثلاثة فروع ؛ تناولنا في الأول الأمن الرقمي في اتفاقية الاتحاد الإفريقي، الفرع الثاني يخص الأمن الرقمي في الاتفاقية الأوروبية،أما الفرع الثالث حول الأمن الرقمي في الاتفاقية الأمريكية ؛

---

[1] المادة 1/4 و 2/4 من قرار الجمعية العامة رقم 166/69

[2] مركز هردو ،الأمن الرقمي وحماية المعلومات ، مرجع سابق ، ص 9 ؛ نقلا عن
(klang, Mathias; Murray,Andrew ;human rights in the digital age, Routledge; 2005) ، ص1، مؤرشف من الأصل في 25 أكتوبر2013.

[3] مركز هردو ،الأمن الرقمي وحماية المعلومات ، مرجع سابق، ص 8 و 9 .

الفرع الأول : الأمن الرقمي في اتفاقية الإتحاد الإفريقي

اتفق قادة الاتحاد الإفريقي على اتفاقية تاريخية تؤثر على كثير من مناحي الحياة الرقمية ،حيث اجتمع قادة الاتحاد الإفريقي وكان عددهم 54 حكومة افريقية ، وتم تثبيت الاتفاقية من قبل دول الإتحاد الإفريقي بمناسبة انعقاد مؤتمره "23 " في دورته العادية بتاريخ 27 يونيو 2014 ، .والتي تغطي نطاق واسع من الأنشطة على الأنترنت متضمنة التجارة الإلكترونية وحماية البيانات والجرائم الإلكترونية والأمن السيبراني الوطني .وتعتبر هذه الاتفاقية قفزة إلى الأمام في تنظيم الأنترنت وتعرف أيضا باتفاقية مالابو [1].

نظمت هذه الاتفاقية بنص واحد من ثمانية وثلاثين (38) مادة ،أربعة مجالات تناولها المشروع الموريتاني بنصوص منفصلة وهذه المجالات هي :

- الجريمة السيبرانية بأبعادها المختلفة الموضوعية والإجرائية .
- تنظيم المبادلات الإلكترونية .
- حماية البيانات ذات الطابع الشخصي .
- رسم أهداف ووضع ضوابط وترقية مجتمع المعلوماتية في دول الاتحاد [2].

إضافة إلى أن الاتحاد الإفريقي طلب من كل دولة وضع إستراتيجية وطنية للأمن السيبراني وتمرير قوانين الجرائم الإلكترونية والتأكد من أن التجارة الإلكترونية تمارس بحرية . كما يطلب من كل دولة أن تكون لها سلطة حماية البيانات الوطنية لضمان أن البيانات الشخصية تعالج وفقا لأحكام الاتفاقية في غرض مشروع ويحدد حفظ البيانات بالوقت اللازم للغرض الذي تم معالجته مع وجود استثناءات للمصلحة العامة ، كما يجب اخبار أصحاب البيانات ببياناتهم قبل أن يتم مشاركتها مع أطراف ثالثة [3].

كما أدرجت الاتفاقية أن الخصوصية أمر مرحب به مع الوضع في الاعتبار أنه لم يتم العثور عليه صراحة في الميثاق الإفريقي[4] .كما ضمنت ثقافة الأمن السيبراني في المادة 26 [5].

كما تصر الاتفاقية على قواعد الأمن السيبراني والتي تدعم سيادة القانون وذلك لوضع معايير التبادل الدولي للبيانات بطريقة فعالة [6].كما يجب على الدول حماية البيانات وإعلام المستخدمين عن المخاطر التي تتعرض لها بياناتهم ونقلها لأطراف ثالثة حسب نص المادة 18 من الاتفاقية ،وهو البند الذي ينبغي أن يطبق على خرق البيانات والتحويلات الغير القانونية[7] .

---

[1] مدونة محمد ، الاتحاد الإفريقي يتبنى إطار بشأن الأمن السيبراني وحماية البيانات ، جانفي 2015 ،على الموقع . https://moeltaher.net

[2] سيدي محمد الأمين الراضي ،الجريمة السيبرانية وتكاملية النص الوطني ،الإقليمي والدولي ،مذكرة دكتوراه ،جامعة نواكشوط العصرية ،موريتانيا ،يوليو 2019 ، ص 10.

[3] المادة 18 ، من اتفاقية الإتحاد الإفريقي .

[4] المادة 25 من اتفاقية الاتحاد الإفريقي .

[5] المادة 26 من اتفاقية الاتحاد الإفريقي .

[6] المادة 28 من اتفاقية الاتحاد الإفريقي

[7] المادة 29 من اتفاقية الاتحاد الإفريقي .

الفرع الثاني: الأمن الرقمي في الاتفاقية الأوروبية

ولقد جاء النص على حق الخصوصية والأمن الرقميين في الاتفاقية الأوروبية لحقوق الإنسان في المادة 18 [1].

وبالرجوع إلى جوهر المادة 18 في فقرتها الأولى، يلاحظ أنها تضمنت احترام كل الحياة الخاصة والعائلية والمسكن والمراسلات لكل فرد يوجد على إقليم أي من الدول الأطراف، بمعنى أنها سوت بين مواطني الدولة التي يتم فيها خرق هذه الحقوق ومواطني الدول الأخرى الأطراف في هذه الاتفاقية، وحتى بين مواطني الدول غير الأعضاء فيها، طالما هم مقيمون في إحدى تلك الدول الأطراف [2]. أما الفقرة الثانية من المادة 18 من هذه الاتفاقية، فإنّها ترفض أي تدخل للسلطة العامة في كيفية ممارسة هذا الحق من طرف صاحبه كما لا تجيز للسلطة ذاتها تقييد ممارسته، إلا إذا كانت النصوص التشريعية للدول المعنية تجيز ذلك ، وبما لا يتعدّى القدر الضروري لتحقيق الأغراض التي من أجلها سمح بالتدخل [3].

على الرغم من أن المعايير الأمريكية توفر أساسا وضوابط واضحة للعمليات التجارية ، فقد أنشأ الاتحاد الأوربي لائحة أكثر ملاءمة للشركات التي تعمل داخل دول الاتحاد، وفي ضوء خروج بريطانيا من هذا الاتحاد كان من المهم النظر في كيفية العمل مع المملكة المتحدة للالتزام بهذه اللوائح الأمنية.

فقد تم تشريع ثلاثة قوانين أو لوائح رئيسية داخل الاتحاد الأوروبي (وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات"ENISA" في 2004/3/10؛ ثم تم وضع التوجيه الخاص بأمن أنظمة الشبكات والمعلومات "توجيه NIS "والذي دخل حيز التنفيذ في أوت 2016، ثم اللائحة العامة لحماية البيانات في الاتحاد الأوروبي والذي تم تنفيذه في 25 ماي 2018. [4]

الفرع الثالث: الأمن الرقمي في الاتفاقية الأمريكية

كما أن الاتفاقية الأمريكية لحقوق الإنسان هي الأخرى جاء النص فيها على حماية الحق في الخصوصية الرقمية من خلال احترام الفرد لشرفه وعدم الاعتداء عليه وصون كرامته، كما لا يجوز التدخل بشكل تعسفي في حياته الخاصة أو شؤون أسرته أو منزله أو مراسلاته ، وإن كان هناك تدخل أو اعتداء فالقانون يحميه [5].

ولقد حاولت حكومات الولايات المتحدة تحسين الأمن الرقمي من خلال زيادة ظهور الجمهور للشركات ذات الأمن الضعيف ، وفي سنة 2003 ،أقرت كاليفورنيا قانون الإخطار الأمني.[6]

---

[1] الاتفاقية الأوروبية لحقوق الإنسان الصادرة سنة 1950، المادة 18.

[2] حسين عمر؛ المنظمات الدولية ، دار الفكر العربي، القاهرة، ط1، 1993م.

[3] بارق منتظر عبد الوهاب لامي؛ جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط ، الأردن، 2017، ص76.

[4] EU GDPR Portal , "home page of EU GDPR" 28/8/2019 ، 2017/3/12، (http: ar.m.wikipedia.org)

[5] المادة 11 من الاتفاقية الأمريكية لحقوق الانسان، سان خوسيه، الصادرة في 11/22/ 1969م.

[6] Securely protect your self against cyber trespassAct(2005; 109th congress H.R.29) – Gov track.us مؤرشف في 26 أوت 2017 (http: ar.m.wikipedia.org)

وفي سنة 2004 خصص الكونغرس 4.7 مليار دولار للأمن السيبراني. ويحاول الكونغرس جعل المعلومات الرقمية أكثر شفافية بعد فشل قانون الأمن السيبراني لعام 2012، الذي كان سيخلق معيير طوعية لحماية البنية التحتية الحيوية، وفي أفريل 2013 أقر مجلس النواب قانون تقاسم وحماية الاستخبارات السيبرانية (CIPSA).

وفي شهر فيفري عام 2016، قام الرئيس الأمريكي أوباما، بتطوير خطة عمل الأمن القومي للأمن السيبراني (CNAP)، حيث تم وضع خطة طويلة المدى من أجل حماية الولايات المتحدة من التهديدات السيبرانية.[1]

المطلب الثالث: الأمن الرقمي في الاتفاقيات العربية

نظرا لما عرفه المجتمع الدولي من اهتمام بالأمن والخصوصية الرقمية، حاولت الدول العربية تكييف تشريعاتها بما يتماشى والاتفاقيات الدولية والإقليمية في هذا المجال، وذلك راجع أساسا لحماية أمنها واستقرارها الرقمي الوطني. سنحاول عرض هذه الجهود من خلال الفروع الآتية؛

الفرع الأول: الاتفاقية العربية لحماية الفضاء السيبراني

قطعت الخطوات التحضيرية لإبرام الاتفاقية العربية لحماية الفضاء السيبراني شوطا بعيدا من التمحيص والتعديل والأخذ بملاحظات الدول التي كانت تصب في الاتجاه الصحيح نحو وضع الإطار القومي الشامل لأمن وحماية الفضاء السيبراني الذي أصبح أهم مرتكزات بناء وتوفير الشروط السليمة للتنمية الشاملة المبنية على تداول آمن وتوفير مجد للمعلومات باستخدام الفضاء السيبراني وتكنولوجيا المعلومات كمعبر ووسيلة ومتن لهذا الكم الهائل من المعلومات [2].

كما تبين توصيات الإتحاد الدولي للاتصالات أن الأمن الرقمي يعتمد على مزيج مركب من التحديات التقنية السياسية والاجتماعية والثقافية . وبشكل أدق فإن صلاحية الأمن السيبراني الوطني تعتمد على الركائز الخمسة التالية :

- تطوير إستراتيجية وطنية للأمن السيبراني وحماية البنية التحتية للمعلومات الحساسة .
- إنشاء تعاون وطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات .
- ردع الجريمة السيبرانية .
- خلق قدرات وطنية لإدارة حوادث الحاسب الآلي.
- تحفيز ثقافة وطنية للأمن السيبراني [3].

---

[1] FACT SHEET: Cybersecurity National action PLAN; White house.gov ، مؤرشف من الأصل في 2019/8/7 (http: ar.m.wikipedia.org)

[2] الاتفاقية العربية لحماية الفضاء السيبراني –بين الواقع والطموح – ،المركز العربي للبحوث القانونية والقضائية ، مجلس وزراء العدل العرب ، جامعة الدول العربية ،بيروت ، 23 –25 يوليو 2018 ،ص 3 .

[3] الاتفاقية العربية لحماية الفضاء السيبراني –بين الواقع والطموح – ،نفس المرجع ، ص 4 – 5 .

سعت الدول العربية لحماية البيانات والمعلومات الخاصة بشبكتها الإلكترونية من أي اختراقات من أي جهة كانت، والتزاما بالمعاهدات والمواثيق العربية المتعلقة بحقوق الانسان ذات الصلة، وحفظا لحق الدول والمؤسسات والأفراد في حماية بياناتها وعدم تهديدها أو تعطيل مصالحها أو إلحاق الضرر بالمال العام وحفظا للخصوصية فقد اتفقت على مايلي :

الحفاظ على القوى العربية من أي اختراقات إلكترونية وكذلك الثروة التقنية والمالية والمعلوماتية للمؤسسات الحكومية والخاصة والأفراد من الهجمات والقرصنة الإلكترونية ، وحماية البيانات والبنى التحتية من الهجوم الإلكتروني مع وضع آلية قانونية تضمن استخدام الأمن السيبراني [1].

كما أكدت الاتفاقية على حق كل الدول في تطبيق أنظمتها في مجال الفضاء السيبراني[2]،كما تطبق أحكامها على جرائم تقنية المعلومات والجرائم المتعلقة بالفضاء السيبراني متى أضرت بأحد مصالحها وإذا تحققت النتيجة الجرمية في إقليمها[3]. وتتخذ الاتفاقية التدابير الاحترازية لحماية المنشآت الحرجة ولضمان سلامة البنية التحتية للاتصالات والمعلومات [4]، وتمتنع الدول العربية عن إجراء أي تعطيل للاتصالات أو البنية التحية لها أو تعرض أمن وسلامة الفضاء السيبراني لأي خطر كان[5].

وأكدت الاتفاقية على التعاون الدولي والإقليمي لحماية الفضاء السيبراني لا سيما اللجان التابعة للأمم المتحدة والاتحاد الدولي للاتصالات وغيرها من الهيئات ذات الاختصاص بمسائل الأمن السيبراني [6].

وخلاصة القول فقد تضمنت بنود الاتفاقية أحكام الأمن السيبراني وحمايته من كافة أشكال الاعتداء ، ومختلف أشكال الجرائم الإلكترونية وطريقة محاربتها وصد الاختراقات الإلكترونية للبنية التحتية للاتصالات والمؤثرة على الدولة والحكومات والأفراد . كما نصت على التعاون الأمني في مكافحة الجرائم الإلكترونية بما فيها المنظمة لاسيما الإرهابية منها وغسيل الأموال وعلى اتخاذ تدابير قانونية لحماية الفضاء السيبراني وتعزيز سبل المكافحة في المواد (16 و17)من الاتفاقية[7].

---

[1] المادة الأولى ، من الاتفاقية العربية لحماية الفضاء السيبراني –بين الواقع والطموح –المركز العربي للبحوث القانونية والقضائية ، مجلس وزراء العدل العرب ، جامعة الدول العربية ،بيروت 23 –25 يوليو 2018 ،ص 9 .

[2] المادة الثالثة من الاتفاقية العربية لحماية الفضاء السيبراني ص 12.

[3] المادة السادسة من الاتفاقية العربية لحماية الفضاء السيبراني ،ص 12 .

[4] المادة الرابعة من الاتفاقية العربية لحماية الفضاء السيبراني ، ص 14 .

[5] المادة التاسعة من الاتفاقية العربية لحماية الفضاء السيبراني ، ص 14.

[6] المادة الثالثة عشر من الاتفاقية العربية لحماية الأمن السيبراني ، ص 15 .

[7] المادة 16 –17 من الاتفاقية العربية .

- وأكدت على التنظيم الإداري لمتابعة شؤون الأمن السيبراني في موادها من (18 إلى 23) ،ونصت على الإطار التشريعي لحماية الفضاء السيبراني في وذلك استنادا إلى النصوص الدولية والاتفاقيات وبروتوكولات التعاون حول حماية الفضاء السيبراني المتعلقة بالجريمة السيبرانية والتعاون في الجرائم العابرة للحدود وكل المعايير الدولية المعتمدة في حماية البنية التحتية للاتصالات وأنظمة المعلومات [1].وتضمنت القواعد القانونية والتشريعات المناسبة لحماية الأمن السيبراني في المواد من (25 إلى 30).

وهكذا فقد نصت الاتفاقية العربية لحماية الفضاء السيبراني على الأمن السيبراني وحمايته من الاعتداءات والاختراقات التي يمكن أن يتعرض لها ، ويكون لها تأثير على الدولة والحكومة والفرد ،وتوفير التدابير اللازمة لحمية الفضاء السيبراني وذلك بالتعاون مع مختلف الهيئات الدولية والإقليمية ، كما أقرت تنظيم إداري لمتابعة شؤون الأمن السيبراني وإطار تشريعي لحمايته من الاعتداءات .

الفرع الثاني: الجهود الجزائرية لحماية الأمن الرقمي

أمام التهديدات والمخاطر المتزايدة والتي يخلفها استخدام التكنولوجيا الحديثة في الجزائر فقد بات لزاما اعتماد سياسة أمنية وطنية تضع مسألة توفير الأمن الرقمي أو السيبراني على رأس أولوياتها واستراتيجياتها ، وذلك من خلال البحث عن آليات فعالة يمكن من خلالها إدارة مختلف الحروب السيبرانية سواء باعتماد سياسات وقائية أحيانا أو سياسات علاجية أحيانا أخرى ،حيث احتلت الجزائر المرتبة 23 عالميا في مجال الأمن الرقمي [2].

بذلت الجزائر جملة جهود لحماية الأمن الرقمي حيث ركزت أساسا في مجال اتخاذ التدابير القانونية دون غيرها من التدابير الأخرى ، وذلك من خلال صدور القانون رقم 09-04 المؤرخ في 05 أوت 2009 ،الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،والذي تم فيه تحديد الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الإلكترونية [3].بناءا على ما ورد في المادة 4 التي نصت على :

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة .
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني [4].

---

[1] المادة 24 من الاتفاقية العربية لحماية الأمن السيبراني، ص 19 .

[2] الاتحاد الدولي للاتصالات ، تقرير حول الرقم القياسي للأمن السيبراني وسمات السلامة السيبرانية ، جينيف ، الإتحاد الدولي للاتصالات ، مكتب تنمية الاتصالات ، أفريل 2015 م ، ص 6.

[3] قانون رقم 09-04 المؤرخ في 14 شعبان 1430هـ الموافق ل 5أوت 2009 م ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، الجريدة الرسمية ، العدد 47 ، الصادرة في 25 شعبان 1430 هـ الموافق ل 16 أوت 2009 م ،ص 6.

[4] بن مرزوق عنترة ، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية ، جامعة محمد بوضياف ، الجزائر، ص 7.

- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية ،في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة [1].

بالإضافة إلى ذلك فإن المشرع الجزائري يعتبر صراحة أن المحادثات الشخصية وصورة الشخص مظهرين أساسيين للحق في الخصوصية ، وذلك حماية لما يدور من حديث وما يتخذه الشخص من أوضاع اعتمادا على أنه لا يطلع عليه أحد . ولقد حدد المشرع أشكال الاعتداء على الأحاديث الشخصية والسرية من خلال (المادة 303 مكرر، الفقرة 1) من قانون العقوبات الجزائري رقم 06-23 ([2]). ويتبين لنا أن المشرع قد اتخذ معيار خصوصية المحادثات ضابطا لا تتحقق دونه جريمة الاعتداء على الحق في الخصوصية [3]، فالعبرة ليست بحماية المكان وإنما بطبيعة الواقعة أو المحادثة، فحماية القانون تمتد لتشمل المكالمات وكل حديث خاص أو سري ولو كان قد أجري في مكان عام [4].

وفي إطار الأمن المعلوماتي دائما نص نظام بنك الجزائر رقم 12-03 مؤرخ في 28 نوفمبر 2012 والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما في المادة "17 "فقرة 2 ، فهذا الجهاز الآلي الذي يحوزه مسيرو النظام يدخل في سياق الأمن المعلوماتي وذلك لاكتشاف الزبائن والعمليات لكي لا يكون هناك تعد على العمليات [5].
وفي إطار القانون رقم 15 -04 المؤرخ في 2015/2/1 ، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين ، لقد ميز المشرع الجزائري، في المادة 2 الفقرتين 11 و12 من هذا القانون ،بين نوعين من الجهات المكلفة بالتصديق الإلكتروني؛ الجهة الأولى سميت بالطرف الثالث الموثوق(فقرة11)، والجهة الثانية أعطي لها تسمية مؤدي خدمات التصديق(فقرة12) [6]. والملاحظ أن المشرع أشار إلى وجوب حصول مؤدي هذه الخدمة على الترخيص لمزاولة نشاطها تمنحه السلطة الاقتصادية للتصديق الإلكتروني ، غير أنه لم يشر إلى وجوب حصول الطرف الثالث الموثوق والذي يقدم خدمات التصديق لصالح المتدخلون في الفرع الحكومي على ذلك من السلطة الحكومية للتصديق. ويعتبر اشتراط الحصول

---

[1] المادة "4" من القانون 09-04 المؤرخ في 05 أوت 2009 .

[2] قانون العقوبات رقم 06-23 المعدل والمتمم، المؤرخ في 2006/12/20، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية ، عدد 2006،84 ، ص 12.

[3] عائشة لخشين؛ حماية الحق في الخصوصية في العصر الرقمي في المواثيق الدولية، مقال نشر في مجلة جيل حقوق الانسان، عدد 39 ، 2021/3/2 ، ص109. (http:www. jilrc.com) ، تاريخ الاطلاع: 2021/4/27.

[4] بن حيدة محمد؛ الحق في الخصوصية في التشريع الجزائري(دراسة مقارنة)، رسالة ماجستير، كلية الآداب والعلوم الإنسانية، جامعة أحمد دراية، أدرار، 2009-2010، ص99

[5] إيلاف فاخر كاظم علي ، مخاطر العمليات المصرفية الإلكترونية ، المركز العربي للدراسات والبحوث العلمية ، جمهورية مصر العربية ،الطبعة الأولى، 2019 ، ص 62.

[6] القانون رقم 15-04 المؤرخ في 2015/02/1 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية ، عدد 6، بتاريخ 2015/02/10.

على الترخيص لمزاولة هذا النشاط أمر ضروري للحفاظ على مصالح المتعاملين الكترونيا لأنه يضفي نوعا من الثقة والأمان على عمل هذه الجهات من ناحية، ويقلل من إمكانية التعرض لاحتيال من ناحية أخرى [1].

ولقد جاء القانون رقم 18 -04 المؤرخ في 10 ماي 2018 والذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، حيث أشارت المادة 4 منه؛ على مسؤولية الدولة في تحديد وتطبيق معايير إنشاء واستغلال الخدمات المختلفة وأمن وسلامة شبكات الاتصالات الالكترونية[2].

خاتـمة

تتعرض ثقافة الأمن الرقمي في ظل التطور التكنولوجي المعاصر إلى تحديات كبيرة واختراقات متعددة سميت بالجريمة الإلكترونية مست الدولة والمؤسسة والفرد من خلال الاعتداء على البيانات الخاصة بهم ، لذلك كان لابد من وجود قواعد قانونية تفرض حماية الأمن الرقمي وتنظمه ،كما لوحظ وجود نقص في القواعد القانونية الحامية للأمن الرقمي وهو ما يرتب مسؤولية جزائية واضحة إزاء انتهاك الأمن السيبراني لأية دولة أو شخص طبيعي أو معنوي في العالم. فالمواثيق والاتفاقيات الدولية والإقليمية وحتى العربية قد وفرت الحماية ، لهذا الحق الرقمي،بشكل واسع لكنها لم تتعاطى أكثر مع إشكالية التطور التكنولوجي المتسارع للجرائم الإلكترونية والمعلوماتية والتي تعد أكثر الجرائم خطورة وتعقيدا في هذا العصر.

نتائج الدراسة:

من خلال هذه الدراسة توصلنا للنتائج التالية:

- أن الأمن الرقمي يتميز بعدة خصائص لعل أهمها ما يلي:
  1. هو ذو طابع متعدد التخصصات (الاجتماعية ،الاقتصادية والتقنية...)
  2. كون الأمن الرقمي شبكة خالية من الحجم وقدرات الفاعلين يمكن أن تكون مماثلة على نطاق واسع.
  3. له درجة عالية من التغيير والترابط وسرعة التفاعل .
- إن عدم إجماع الفقهاء على تعريف موحد للجريمة الالكترونية يعود إلى اختلاف تحديد نطاق هذه الجريمة ، وقد تبنى المشرع الجزائري الاتجاه الموسع ، باعتبار أن هذه الجريمة هي كل فعل غير مشروع يمس النظام المعلوماتي، أو أي جريمة ترتكب أو يستعمل في ارتكابها منظومة معلوماتية أو أي نظام للاتصالات ، وهذا التوسيع في المفهوم لا يتفق مع ماهية الجريمة الإلكترونية، باعتبارها تستهدف بالدرجة الأولى الجانب البرمجي للنظم المعلوماتية.

---

[1] رضوان قرواش ؛ هيئات التصديق الالكتروني في ظل القانون رقم 15-04 المؤرخ في 2015/02/1 ، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين (المفهوم والالتزامات)،كلية الحقوق والعلوم السياسية ، جامعة سطيف 2، الجزائر، مجلة العلوم الاجتماعية، العدد 24، جوان 2017 ، ص 413.

[2] القانون رقم 18 -04 المؤرخ في 10 ماي 2018 والذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية، عدد 27 ، بتاريخ 13 ماي 2018، ص5.

- صعوبة مكافحة الجريمة الإلكترونية باعتماد وسائل تقليدية، لذا وجب تجديد هذه الآليات وتحسينها بما يتماشى والتطور المتسارع الذي تتميز به الجرائم الالكترونية.
- أهمية الجانب التقني في مكافحة الجريمة الإلكترونية، لذا ينبغي الاهتمام به ومحاولة تطويره وتحيينه مع تطور هذه الجريمة .
- وأمام هذا الوضع بات لزاما على حكومات الدول الإسراع في اتخاذ الإجراءات الأمنية اللازمة لتطوير آليات التصدي لمثل هذه الجرائم المتطورة وتعزيز التعاون الدولي.

التوصيات والمقترحات:

وعليه لمسايرة تطور الجرائم الالكترونية ، نوصي بالحلول والمقترحات التالية:

- ضرورة تعديل وتحيين القوانين الداخلية للدول، كقانون العقوبات وقانون الإجراءات الجزائية والقانون التجاري... ، بما يتلاءم وأنواع الجرائم الالكترونية المستحدثة، ووضع طرق متطورة وفعالة لتتبعها ومكافحتها.
- إنشاء محاكم متخصصة بالجرائم الالكترونية في كل المجالس القضائية للسيطرة على هذه الظاهرة ومجابهتها وذلك حفاظا على الأمن الرقمي.
- ضرورة تخصيص جهاز شرطة علمية جنائية متخصصة في جرائم الانترنت في كل مقاطعة إدارية وتكوين لجان خبراء للمتابعة والتحري الالكتروني.
- تكوين هيئات وطنية استشارية متخصصة ، لمراقبة ومتابعة جرائم الانترنيت ، وتزويد البرلمان بكل التغيرات والتطورات الحاصلة .
- تعزيز التعاون والمساعدة الوطنية والدولية في مجال مكافحة الجرائم الالكترونية، وعقد وإبرام اتفاقيات تسمح بمتابعة رقمية آنية، وتسليم مرتكبي هذه الأعمال المؤثرة سلبا على الأمن الرقمي للدول.

قائمة المصادر والمراجع

أولا : الكتب العربية

- إيلاف فاخر كاظم علي ؛ مخاطر العمليات المصرفية الإلكترونية ، المركز العربي للدراسات والبحوث العلمية ،جمهورية مصر العربية ،الطبعة الأولى، 2019 .
- بن مرزوق عنترة ، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية ، جامعة محمد بوضياف ، الجزائر .
- حسين عمر؛ **المنظمات الدولية** ، دار الفكر العربي، القاهرة، ط1، 1993.
- خالد عياد الحلبي ؛ **إجراء التحري والتحقيق في جرائم الحاسوب والانترنت** ، دار الثقافة للنشر و التوزيع، الأردن، بدون طبعة، 2011 .
- ذياب موسى البداينة؛ الجرائم الإلكترونية ، المفهوم والأسباب، ورقة علمية مقدمة في الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية(7 إلى 1435/11/9هـ الموافق: 2 إلى 2014/9/4م) ،عمان، المملكة الأردنية الهاشمية ، 2014.
- محمود إبراهيم غازي؛ الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2014.

ثانيا : الكتب الأجنبية

- Douwe Korff ,CYBER SECURITY DEFINITIONS –a selection ; P1,in:https://www.sbs.ox.ac.uk /cyberesecurity – capacity /system /fils /CPDP20201520 - KORFE Handout .pdf
- Cameron S.D Brown ,*Investigating and Prosecuting Cyber Crim :Forensic Dependencies and Barries and to justice *,International Journal of Cyber Criminology .Vol9 ,Jssue 1 ,january –june 2015 .
- Van der hulst & Neve, 2008.
- Halder ,D. & jaishankar ,K. (2011): Cyber crime and the victimization of woman :Laws ,Rights and Regulations ,.Hershey ,PA ,USA :IGI Global .ISBN 978- 1-60960 -830 -9 .
- FACT SHEET: Cybersecurity National ; action Plan . White house.gov .
- klang, Mathias; Murray,Andrew ;human rights in the digital age, Routledge; 2005

ثالثا : المجلات والدوريات العلمية

- رزق سلمودي وليندا ربايعة وآخرون؛ الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي، مجلة الجامعة العربية الأمريكية للبحوث، مجلد 3، العدد 2، 2017 .
- عادل يوسف عبد النبي البشكري، **الجريمة المعلوماتية وأزمة الشرعية الجزائية**، العدد 7، الكوفة، العراق .
- بارة سميرة ،الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر – الدور والتحديات – جامعة قاصدي مرباح ورقلة ، الجزائر .
- مال محمد غيطاس ،الأمن المعلوماتي والجرائم الإلكترونية ، أدوات جديدة للصراع ، مركز الجزيرة للدراسات،نشر 29 فيفري 2012 م، على الموقع .http://studies.aljazeera.net/ar/issues/2012/02
- مدونة محمد ، الاتحاد الإفريقي يتبنى إطار بشأن الأمن السيبراني وحماية البيانات ، جانفي 2015 ،على الموقع https://moeltaher.net
- عائشة لخشين؛ حماية الحق في الخصوصية في العصر الرقمي في المواثيق الدولية، مقال في مجلة جيل حقوق الانسان، عدد 39 ، 2021/3/2 ، ص109. (http:www.jilrc.com) ، تاريخ الاطلاع: 2021/4/27.
- بن حيدة محمد؛ الحق في الخصوصية في التشريع الجزائري(دراسة مقارنة)، رسالة ماجستير، كلية الآداب والعلوم الإنسانية، جامعة أحمد دراية، أدرار، 2009-2010 .
- مركز " هردو " لدعم التعبير الرقمي؛ **الأمن الرقمي وحماية المعلومات، الحق في استخدام شبكة آمنة** ، القاهرة، 2017 ، (http://hrdo egypt.org)
- مجلة تكنولوجيا المعلومات، قسم نظم المعلومات، دون دار نشر. نقلا عن مختارية بوزيدي، ماهي الجريمة الالكترونية، سعيدة، الجزائر، 2017 .
- مركز هردو لدعم التعبير الرقمي ،التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات ،القاهرة ، 2017 ، الإصدار 3 .
- بارق منتظر عبد الوهاب لامي؛ جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط ، الأردن، 2017 .
- رضوان قرواش ؛ هيئات التصديق الالكتروني في ظل القانون رقم 15-04 المؤرخ في 2015/02/1 ، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين (المفهوم والالتزامات)،كلية الحقوق والعلوم السياسية،جامعة سطيف 2 ، الجزائر، مجلة العلوم الاجتماعية، العدد 24، جوان 2017 .
- سيدي محمد الأمين الراضي ،الجريمة السيبرانية وتكاملية النص الوطني ، الإقليمي والدولي ، مذكرة دكتوراه ، جامعة نواكشوط العصرية، موريتانيا ، يوليو 2019 .

رابعا :الملتقيات والمؤتمرات

- منى الأشقر ،الأمن السيبراني –التحديات ومستلزمات المواجهة – اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني ، بيروت ، من 27 - 28 أوت 2012 م ،جامعة الدول العربية ، المركز العربي للبحوث القانونية والفضائية .
- ذياب موسى البداينة ، *الجرائم الإلكترونية –المفهوم والأسباب* ،الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان ، 1435 هـ/ 2014 م.

ثالثا : المواقع الإلكترونية

- http: www.hrdo egypt .org
- http: ar.m.wikipedia.org
- EU GDPR Portal , "home page of EU GDPR" 28/8/2019
- http://studies.aljazeera.net/ar/issues/2012/02

رابعا : القوانين والاتفاقيات

- الاتفاقية العربية لحماية الفضاء السيبراني –بين الواقع والطموح - ،المركز العربي للبحوث القانونية والقضائية ، مجلس وزراء العدل العرب ، جامعة الدول العربية ،بيروت ، 23 -25 يوليو 2018 .
- الإعلان العالمي لحقوق الانسان، الصادر في 10 ديسمبر 1948،هيئة الأمم المتحدة.
- العهد الدولي للحقوق المدنية والسياسية الصادر 16 ديسمبر 1966، ودخل حيز التنفيذ سنة 1976، هيئة الأمم المتحدة.
- الوثائق الرسمية للجمعية العامة ،الدورة التاسعة والستون 69 ،الملحق رقم 53 ،(A53/69/)
- الوثائق الرسمية للجمعية العامة الدورة الثالثة والأربعون 43، الملحق رقم 40 ،(A/43/40) المرفق السادس .
- قرار الجمعية العامة للأمم المتحدة رقم 166/69 ،الحق في الخصوصية في العصر الرقمي ،الصادر في 18 ديسمبر 2014 ، الدورة التاسعة والستون ، بناءا على تقرير اللجنة الثالثة ،البند(68/ ب) من جدول الأعمال .
- الاتفاقية الأوروبية لحقوق الإنسان الصادرة سنة 1950.
- الاتفاقية الأمريكية لحقوق الانسان، سان خوسيه، الصادرة في 11/22/ 1969م.
- الاتحاد الدولي للاتصالات ، تقرير حول الرقم القياسي للأمن السيبراني وسمات السلامة السيبرانية ، جينيف ، الإتحاد الدولي للاتصالات ، مكتب تنمية الاتصالات ، أفريل 2015
- قانون رقم 09-04 المؤرخ في 14 شعبان 1430هـ الموافق 5 أوت 2009 م ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، الجريدة الرسمية ، العدد 47 ، الصادرة في 25 شعبان 1430 هـ الموافق ل 16 أوت 2009 م.

.

- قانون العقوبات رقم 06-23 المعدل والمتمم، المؤرخ في 2006/12/20، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية ، عدد 84. 2006.
- القانون رقم 15-04 المؤرخ في 2015/02/1 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية ، عدد 6، بتاريخ 2015/02/10.
- القانون رقم 18 -04 المؤرخ في 10 ماي 2018 والذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية للجمهورية الجزائرية ،عدد 27 ، بتاريخ 13 ماي 2018.