مجلة البحوث القانونية و الاقتصادية | المجلد 05/ العدد : 01 (2022) ، ص 302-322

تحديات الانترنت لسيادة الدول (السيادة الرقمية)

Internet Challenges to State Sovereignty (Digital Sovereignty)

ط.د/شحيرط أحمد (*)
مخبر الحقوق والعلوم السياسية
جامعة الأغواط، الجزائر
Ahmedchehiret1964@gmail.com

أ.د/ قريبيز مراد

مخبر الحقوق والعلوم السياسية

جامعة الاغواط، الجزائر

Gueribizuniv03@gmail.com

تاريخ الاستلام: 2021/05/01 تاريخ القبول للنشر: 2021/09/30

****

ملخص:

ارتبط المفهوم التقليدي للسيادة بعوامل تقليدية، لكن مع تطور الاتصالات حدثت تغييرات جذرية في مفهوم السيادة، وبات من الصعب السيطرة على المعلومات في ظل الارتباط بالشبكة الدولية للمعلومات، والتي شكلت رأس مال مهم يفوق الأهمية التي تتحلى بها رؤوس الأموال الاقتصادية في عصرنا الحالي، وهو الامر الدي تمخض عنه مفهوم السيادة الرقمية التي تؤطر معايير السيادة في عصر المعلومات، فلم يعد الامر مقتصرا على المحيط الجغرافي، حيث عملت وسائل الاتصال على خلق فضاء جديد، وفي طل التحول الرقمي المتسارع أصبح مفهوم السيادة الرقمية محط اهتمام أي دولة في العالم، وهو دفع المجتمع الدولي الى تجسيد التعاون على ارض الواقع، لذلك أبرمت العديد من الاتفاقيات الدولية في مجال التعاون الدولي من أجل مكافحة الإجرام السيبراني.

الكلمات المفتاحية: السيادة الرقمية، الانترنت، الدولة الالكترونية، حماية المعلومات والبيانات، الجرائم الالكترونية.

Abstract:

The traditional concept of sovereignty was linked to traditional factors, but with the development of communications, radical changes took place in the concept of sovereignty, and it became difficult to control information in light of the connection to the international network of information, which formed an important capital that outweighs the importance of economic capital in our current era, which

*ط.د/شحيرط احمد

formed an important capital that outweighs the importance of economic capital in our current era, which is the matter. My father gave birth to itThe concept of digital sovereignty that frames the standards of sovereignty in the information age, it is no longer confined to the geographical environment, as the means of communication have created a new space, and in the wake of the accelerated digital transformation, the concept of digital sovereignty has become the focus of attention of any country in the world, which is pushing the international community to embody Cooperation on the ground. Therefore, many international agreements have been concluded in the field of international cooperation in order to combat cybercrime.

key words: Digital sovereignty, the internet, the cyber state, information and data protection, cybercrime.

مقدّمة:

لفقد تغيرت مفاهيم السيادة في ظل العالم المعاصر، وذلك بفعل ظاهرة العولمة التي تصور منظروها العالم كقرية صغيرة، وبالتالي انتقل مفهوم السيادة إلى ساحة جديدة بفعل التطور التكنولوجي والإلكتروني الهائل، وهو الأمر الذي فرض على كثير من الدول إنشاء فضاءات جديدة تختزل بداخلها كمية معلومات هائلة تخص أمنها الداخلي، وبالتالي فقد شكلت معلومات الدولة الإلكترونية وضرورة حمايتها وتأمينها هاجسا جديدا في أي سياسة أمنية قد تتبناها هذه الدول، وقد نظرت بعض الدول لهذا الأمر بمثابة السيادة بمفهومها الجديد، هذه الأخيرة التي تواجه تحديات عدة تنبع من الأنشطة عبر الإنترنت، والتي يمكن ممارستها بأشكال غير منضبطة وغير مشروعة في أغلب الأحيان.

وتأكيدا على ذلك، فقد شكلت المعلومات الإلكترونية السارية في القنوات التكنولوجية رأس مال مهم يفوق الأهمية التي تتحلى بها رؤوس الأموال الاقتصادية في عصرنا الحالي، مما يدعو إلىضرورة حماية تلك المعلومات من أي هجوم قد تتعرض له البيئة التكنولوجية الحاضنة، والمليئة بالمخاطر والتهديدات، فعلى الرغم من التراجع التدريجي الذي لحق بهذا المفهوم عبر العصور، لهذا كان لا بد من التمييز بين السيادة كمفهوم قانوني والذي يعني الاعتراف بجميع الدول –قانونيا- بحقها في حماية مصالحها الوطنية. وبين السيادة كواقع سياسي، بمعنى القدرة الفعلية للدولة على إنفاذ إرادتها في المجال الدولي.

انطلاقا مما تقدم ذكرت يمكن ان نطرح الإشكالية الآتية:

ما مدى تأثير الانترنت على سيادة الدول؟

وللإجابة على هذه الإشكالية نقترح خطة تتكون من مبحثين، بحيث نتناول في المبحث الأول مفهوم السيادة الرقمية، اما المبحث الثاني نتناول فيه الجهود القانونية للدفاع عن السيادة الرقمية

المبحث الأول:مدلول السيادة الرقمية

مع التطور التكنولوجي وظهور العالم الافتراضي، تطور مفهوم السيادة ليشمل هذا النطاق على الأقل في إطار الحدود الوطنية للدولة وما يتبعها من منظومات معلوماتية تابعة لها فإن للدولة فرض وبسط سلطاتها على عالمها أو إقليمها الافتراضي، والمتمثل في قواعد البيانات والنظام أو المنظومة المعلوماتية الخاضع للدولة، وهو ما يعرف بالسيادة الرقمية، في ظل عدم امتلاك العديد من الدول للتكنولوجيات الحديثة((الاسكوا)، 2019،ص 93)والواقع ان السيادة الرقمية، لم تظهر الا بتخطي الأنترنت لسيادة الدول للحدود الواقعية والتي ساعدت فيها تطور الاتصالات الالكترونية وعبورها للحدود الوطنية، الذي مس بشكل واضح الحدود الإقليمية المادية، بعدما إنفتحت الدولة على تكنولوجيات الإعلام والاتصال وتبنت التخزين المعلوماتي أو الالكتروني للبيانات، هذه البيانات التي توجد في نطاقات تتحكم فيها دول أخرى بحكم أسبقيتها في مجال المعلومات.((الاسكوا)، 2019،ص 93) وعلى هذا الأساس ومما تقدم نعالج هذا المبحث من خلال مطلبين، بحيث نخصص المطلب الأول الى المقصود بالسيادة الرقمية، اما المطلب الثاني الى تدخل الانترنت في سيادة الدول.

المطلب الأول: مفهوم السيادة الرقمية

على الرغم من ان رابطة الهوية تتجسد في العالم المادي بواسطة وثيقة الهوية او أي وثيقة لإثبات هوية المواطن وارتباطه بدولة ما على هذا الأساس، والتي تعتبر سوى وثيقة تدين بشرعيتها للشخص الضامن لها وهو الدولة، فإن هذه الهوية على العكس من ذلك في العالم الرقمي او الافتراضي، حيث ان هذه الهوية غير مضمونة بسبب الضعف المتوطن في الانترنت .(Vers, 2005,P02)

الفرع الأول: المقصود بالسيادة الرقمية

إن ظهور السيادة الرقمية لم يتم إلا بسبب تخطي الانترنت لسيادة الدول التقليدية والتي تعدت فيها الشبكات الالكترونية للاتصالات الحدود الوطنية (Benyekhlef, 2002, p05)الامر الذي أدى بالبعض الى اعتبار ان الحفاظ على السيادة الرقمية لن يتحقق إلا من خلال الجهود الجماعية مستقبلا سواء على المستوى الصناعي او المستوى السياسي(Nathalie Kosciusko, 2009, p10)ومما سبق ذكره يمكن القول ان " كل منشأة يقال عنها انها ذات سيادة رقمية عندما تستطيع انشاء

توافقية interopérabilité، بين المنشآت الفرعية التي تشكلها وتجنب التوافقية الغير مرغوب فيها مع المنشآت التي تتبعها إليها". (سعادي،، 2014، ص 240)

وعلى هذا يمكن تعريف السيادة الرقمية على أنها قيام الدولة ببسط سيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل في الانترنت، حيث انه لا وجود للسيادة الرقمية لولا وجود الانترنت وتخطيه لحدود السيادة التقليدية المتمثلة في الفضاء المادي للدولة ضمن حدودها الإقليمية.

إن سيطرة الدولة وفرض ولايتها القضائية على الانترنت من خلال تنظيم فضائها الالكتروني سعيا منها للحفاظ عليه، يكون بعزمها على ضرورة مكافحة الأفعال التي تعرض ثقة وسلامة وامن المجتمع الافتراضي للخطر. (حمود، 1997، ص13)

الفرع الثاني: كيفيات الاعتداء على السيادة الرقمية

إن القيام ببعض الأفعال المرتبطة باستغلال الأدوات الاتصالية لا سيما الانترنت، هو اعتداء على السيادة الرقمية للدولة، إذ أصبحت هذه الأفعال اليوم تعتبر جرائم جديدة تتوفر على جميع أركان الجريمة وتسمى "الجريمة المعلوماتية ومن بينها:

أولا: الجرائم ضد السرية وسلامة وتوافرونظم المعلومات

هذا النوع من الجرائم يشمل الدخول الغير مشروع، الاعتراض الغير مشروع، المساس بسلامة البيانات، المساس بسلامة النظام، إساءة استخدام الأجهزة.

1-1: الدخول الغيرمشروع

نصت اتفاقية بودابست على هذه الجريمة في المادة الثانية تحت عنوان " الدخول غير القانوني"،وأشارت المذكرة التفسيرية لاتفاقية بودابست بأن الدخول غير المشروع يعد الجريمة الرئيسية التي تنطوي على التهديد والتعدي على الأمن المعلوماتي، بمعنى السرية والسلامة وإتاحة النظم والبيانات المعلوماتية، إذ أن هذا الدخول يمكن أن يترتب عليه الوصول إلى بيانات سرية مثل كلمة المرور (هلالي عبدالله.، 2003، ص69)، فتعرضت الكثير من أنظمة الحاسبات الآلية، وبصفة خاصة تلك التي تعمل من خلال شبكات المعلومات، إلى اختراق بواسطة أشخاص تقنية أنظمة المعلوماتية وما في حكمها لعام 2004في المادة الثالثة:" كل من دخل عمدا وبغير وجه حق موقعا أو نظاما معلوماتيا يعاقب بالحبس.. والغرامة.... أو بإحدى هاتين العقوبتين"وجرمت هذه الجريمة أيضا في المادة 06من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

1-2: الاعتراض غير المشروع

يمكن أن يطلق عليها تسمية جريمة التجسس المعلوماتي والاعتراض غير القانوني للبيانات وهي التسمية التي اعتمدتها اتفاقية بودابست، فالتجسس من العمليات القديمة حيث كان الإنسان يتجسس على أعدائه لمعرفة أخبارهم والخطط التي يعدونها لمهاجمته، ولهذا كان للتجسس أهميته الكبيرة على كافة مستويات النزاعات الإنسانية التي مر بها البشر منذ بدأ الخليقة، فتطورت عمليات التجسس طبقا لما يسود المجتمع من تطورات علمية وتكنولوجية.(ممدوح عبد الحميد ، 2006، ص106)

لقد كان نتيجة الثورة المعلوماتية وانتشار شبكات الاتصالات وتزاوجها مع شبكات المعلوماتية وظهور شبكة الانترنت هدفا للمحتالين ومحترفي الأعمال التجسسية(الرحيم، 2004، ص800.) ، فكان نتيجة استخدام الشبكات المعلوماتية (الحجاج.، 2010 ص 161)ومنه ازدهرت وتحولت وسائل التجسس والتصنت من الطرق التقليدية إلى الطرق الالكترونية (إبراهيم،، 2009 ص338)، فقد أدى الاستخدام المتزايد للحاسبات الآلية تضرر في المجال العسكري و الاقتصادي و السياسي و الصناعي و الإداري و حتى الشخصي(الحفيظ.، 2003، ص 153)، فبظهور الحسابات بدأت مسألة الحصول على المعلومات تأخذ أبعادا جديدة، حيث تطورت أساليب جمع هذه المعلومات حيث" باتت هذه الأساليب تعتمد اعتمادا كبيرا على التكنولوجيا الرقمية."

1-3: المساس بسلامة البيانات

إن ما يسمى "الخصوصية الرقمية" هي وصف لحماية البيانات الشخصية للفرد، والتي يتم نشرها وتداولها من خلال وسائط رقمية، وتتمثل البيانات الشخصية في كل البيانات التي نستخدمها في تفاعلنا على الإنترنت أثناء استخدامنا للحاسب الآلي أو أي من وسائل الاتصال الرقمي بالشبكة العنكبوتية، فسياسة التجسس الرقمي، التجسس، أو "المراقبة" – كما تطلق عليه الحكومات- هي متابعة ورصد لأداء وأنشطة الأفراد في تفاعلهم مع حياتهم اليومية، وقد توسع استخدام الحكومات للتجسس على مواطنيها أو حتى مواطنين دول أخري مع التطور التقني ، حيث انه في منتصف العقد الأخير من القرن العشرين تبنت الحكومات تقنيات أكثر تطوراً لمجاراة انتشار استخدام الهاتف المحمول والإنترنت.(Conflicts of Interest, 2004 May 3-5)

1-4: المساس بسلامة النظام

قد تستهدف الجرائم الواقعة على النظام المعلوماتي التي إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي، وهذه المكونات هي تلك المعدات

التي تستخدم في تشغيله كالأسطوانات و الشرائط و الكابلات...إلخ ، (الملط، 2006، ص176)كأن تكون محلا للسرقة أو الإتلاف العمدي كإحراقها او إفساد أسطوانات التشغيل المغناطيسي بتعريضها إلى أي مجال مغناطيس متلف (حسونة، 1993، ص471)، اما جرائم الاعتداء على المكونات المنطقية، فهي تقع إما على البرامج التطبيقية و إما على برامج التشغيل،أما جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي فتتم من خلال التلاعب بالمعلومة فيها أو عن طريق إتلافها.

1-5: إساءة استخدام الأجهزة

جرائم إساءة استعمال الأجهزة أو البرامج المعلوماتية وجرائم كل من قد م أو أنتج أو وزع أو حاز بغرض الاستخدام جهازا أو برنامجاً معلوماتيا أو أية بيانات معلوماتية معدة أو كلمات سر أو كودات دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقا. (الارشادالخامس، 2006، ص4)

المطلب الثاني: تدخل الانترنت في سيادة الدول

لم يعد مبدأ السيادة يقتصر على الأبعاد السياسية فحسب كما كان الحال عليه في القرنين الماضيين، بل تعداه اليوم ليشمل بعداً تقنياً جديداً يضاف إلى معناه الأصلي المتعارف، كما ان العولمة تؤثر على ثقافات دول العالم المختلفة ،(جاسم،، 2014، ص436.)فظهور التقنيات الحديثة أدى إلى سهولة النفاذ إلى حدود الدولة واختراق سيادتها وخاصة بالنسبة للدول النامية. (نعوس، 2012 ص6)

لقد كانت الدول قادرة على ضمان سيادتها قبل دخول المجتمعات البشرية عصر الرقمية إثر اختراع اول حاسوب ENIAC سنة 1946، فكانت تضمن معظم الاعمال بين الدول بواسطة الاتفاقات الدولية كما كانت تراقب حركات الافراد بواسطة بروتوكولات الهجرة (سعادي،، 2014، ص 240)، وقد اعتبرت شبكة الانترنت أداة أسطورية للاتصال.Ghernaouti-Hèlie(، 2010 , p24

هذا ويعتبر ميشال أليو ماري الانترنت مكانا لجميع الحريات وهو أيضا للأسف مكان للانحراف والجريمة في طريق النمو (Philippe Wolf, 2011, p787)، وفي السداسي الأول من سنة 2011، نشر مركز الاستعلام والبحث ومعالجة التوابع Centre d'Enseignement, de Recherche et de Traitement Addictions (CERTA)، 395 إعلان إعوار vulnèrabilitè من ضمنها أربع إنذارات خطر. Alertes(Philippe Wolf, 2011, p787)

وامام هذا الوضع يمكن انه إذا كانت سيادة الدولة تمارس على إقليم ما فإن الانترنت يجهل الحدود الدولية ,(Ghernaouti-Hèlie, p24 , 2010)وإذا كانت سيادة الدولة تطبق على شعب

معين، فإن الانترنت ينشئ مجموعة افتراضية ضمن شبكات اجتماعية ما وراء أي انتماء وطني (Michèle Alliot- Marie, 2009, p06)، كما نشير انه خلال فعاليات المؤتمر العالمي الذي جرت فعالياته في مقاطعة تشيجيان الصينية، تم منح المشاركين كلمات مرور خاصة ليتمكنوا من الالتفاف على جدار الحماية (firewall) المفروض في الصين.

بالرغم من التغيير الذي احدثه التقدم التقني الا انه لا يخلوا من التأثيرات السلبية التي تتجاوز حدود الدولة الواحدة (الأمم المتحدة، المجلس الاقتصادي والاجتماعي، 2005 ، ص 4)، كما أن فكرة النطاق المحفوظ إن كانت في ظاهرها تقوي مفهوم السيادة فهي تؤكد في ذات الوقت مبدأ الخضوع للقانون الدولي.

المبحث الثاني: الجهود القانونية للدفاع عن السيادة الرقمية

إن وجود تعاون دولي يتفق مع طبيعة الجرائم المتعلقة بالإنترنت، والتي تتميز بطابع خاص يقتضي أن يكون هناك ردود فعل سريعة، وترتيباً على ذلك فإن مكافحة جرائم الإنترنت على المستوى الوطني والدولي تقتضي توثيق روح التعاون بين الأنظمة القانونية الداخلية والخارجية وتظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص (Délégation de compétence) وفي اتخاذ إجراءات التحقيق وجمع الأدلة وتسليم المجرمين والاعتراف بالأحكام الجنائية،(فايز،، 2019، ص14)كما ان مكافحة الجرائم المعلوماتية لن يكون له تأثير يذكر إلا إذا كان هناك تعاوناً دولياً على أكبر قدر من التنسيق والتعاون. (تاينر، 2007، ص 262)

وعليه نعالج هذا المبحث من خلال مطلبين، نخصص المطلب الأول للجهود الوطنية للدفاع عن السيادة الرقمية، اما المطلب الثاني نخصصه للجهود الدولية للدفاع عن السيادة الرقمية.

المطلب الأول: الجهود الوطنية للدفاع عن السيادة الرقمية

إن المجهودات الوطنية التي قامت بها الدول للدفاع عن سيادتها الرقمية، تجسدت من خلال مبادرات التصدي للأعمال التي مستها وأضرت بها، نذكر منها بعض الدول على سبيل المثال وليس الحصر، مجهودات الجزائر للدفاع عن السيادة الرقمية (الفرع الأول)، ومجهودات الدول الأوروبية (الفرع الثاني).

الفرع الأول: جهود الجزائر للدفاع عن السيادة الرقمية

لقد أبدت الجزائر استعدادها منذ سنوات لمكافحة وحماية المعطيات الرقمية ضد جنح التقليد والتزوير واستخدام المزور، وكذلك مختلف الجرائم المعلوماتية (الامر 66-106، 1966)، وبالموازاة مع منافعها وخدماتها

أضحت التكنولوجيا والانترنت بصفة خاصة تستخدم لارتكاب الجرائم والاضرار بالأفراد والمؤسسات

وعلى ما تقدم نعرض المنظومة التشريعية للاختراق الرقمي في الجزائر ثم سياسة جهاز الدفاع الوطني في تحقيق الامن المعلوماتي.

أولا: المنظومة التشريعية للاختراق الرقمي في الجزائر

واجه التشريع الجزائري الجرائم السيبرانية، بإصدار قوانين عامة وخاصة، كما كفل الدستور الجزائري لسنة 2016 حماية الحقوق الأساسي والحريات الفردية، كما تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات وقانون الإجراءات الجزائية والتي تحظر كل مساس بهذه الحقوق.

1-1: قانون العقوبات

تطرق المشرع الجزائري الى تجريم الأفعال الماسة بأنظمة الحاسب الآلي، فعدل قانون العقوبات بموجب القانون رقم 04-10 المؤرخ في 10نوفمبر2004 المعدل والمتمم للأمر رقم 66-106 المتضمن قانون العقوبات، تحت عنوان: " المساس بأنظمة المعالجة الآلية للمعطيات، ويتضمن هذا القسم ثمانية مواد من المادة 394مكرر الى المادة 394مكرر7.

1-2: قانون الإجراءات الجزائية

تم في هذا القانون تمديد الاختصاص المحلي لوكيل الجمهورية في مجال الجرائم الالكترونية، طبقا للمادة 37فقرة2 من قانون الإجراءات الجزائية (الامر 15-02، 2015)، حيث يمتد الاختصاص المحلي إذا تعلق الامر بجرائم المخدرات او الجريمة المنظمة العابرة للحدود الوطنية او الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات او جرائم تبييض الأموال او الإرهاب او الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد والتهريب (اوهايبية،، 2018 ص358)، كما نص على التفتيش في المادة 45فقرة 2 من نفس القانون المعدل، كما نص أيضا بموجب المادة 65مكرر3فقرة 5 أنه في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإن وكيل الجمهورية المختص يقوم بوضع الترتيبات التقنية دون موافقة المعني، من أجل التقاط وتصبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة او سرية في أماكن خاصة او عامة، وفي عام 2006 قام المشرع بإدخال تعديل آخر على قانون العقوبات بموجب القانون رقم 16-

02المؤرخ في 19جويلية 2016(القـانـون رقم 02-16، 2016)، ضمن القسم السابع مكرر من قانون العقوبات بموجب المواد من 394مكرر الى المادة 394مكرر8، وضمن نطاق الفصل الثالث الخاص بالجنايات والجنح ضد الأموال.

1-3: القانون رقم 09-04

سعت الجزائر الى استدراك الفراغ القانوني من خلال تعزيز منظومتها التشريعية خاصة منذ 2009، حيث تم صدور القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها بتاريخ 05 اوت 2009. (قانون رقم 09-04، 2009)

كما احتوى هذا القانون على 19مادة موزعة على 06 فصول مستمدة من الاتفاقيات الدولية (اتفاقية بودابيست، 2001)، وجاء هذا القانون مطابقا للتشريعات الوطنية لا سيما تلك المتعلقة بمحاربة الفساد وتبييض الأموال وتمويل الإرهاب، حيث نص هذا القانون على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته.

ثانيا: سياسة جهاز الدفاع الوطني في تحقيق الامن المعلوماتي.

على غرار باقي الدول فقد وضعت قيادة الدفاع الوطني الجزائرية، الامن السيبراني أحد أولوياتها، إذ سارعت الى مراجعة سياستها الأمنية وأدرجت آليات جديدة تعنى بهذه المسائل وتجسيدا لذلك أعدت مؤسسة الدفاع الوطني برامج خاصة لمجابهة الجريمة الالكترونية والحد من انتشارها، وانشاء أجهزة تنسجم في أدوارها وتجهيزاتها مع المتغيرات الحاصلة في هذا المجال. (تاينر، 2007، ص 262)

2-1: الهياكل المنشأة لتقصي الجريمة السيبرانية

وتتمثل هذه الهياكل في الآتي:

أ- مركز الوقاية من جرائم الاعلام الآلي وجرائم المعلوماتية للدرك الوطني:

هذا المركز أنشئ سنة 2008 ببير مراد رايس، وهو بمثابة مركز توثيق ويهدف الى تامين منظومة المعلومات لخدمة الامن العمومي، كما يقوم بتحليل المعطيات والبيانات للجرائم المعلوماتية

ب- المعهد الوطني للأدلة الجنائية وعلم الاجرام

تم انشاء هذا المعهد ببو شاوي التابع للقيادة العامة للدرك الوطني قسم الاعلام والاتصال الالكتروني، وطلك بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26جويلية 2004، وعدل نظامه الأساسي بموجب المرسوم الرئاسي رقم 09-118 المؤرخ في 14 أفريل 2004.

ويتكون هذا الجهاز من 11 دائرة متخصصة في عدة مجالات متباينة، تضمن جميعها الخبرة والتكوين والتعليم وتقديم جميع المساعدات التقنية، كما ويحتوي هذا المعهد على العديد من الأقسام والمصالح المختصة ومن أهمها:

1-مصلحة البصمات: هذه المصلحة مجهزةبأنظمة التعرف الآلي على البصمات، وتقم المصلحة بمقارنة البصمات.

2-مصلحة الوثائق: يتم فيها التأكد من صحة الوثائق والامضاءات والتحقق من النقود والتأكد من صحة الوثائق السرية.

3- مصلحة الاعلام الآلي: يتم من خلالها رصد وتتبع ومراقبة عمليات الاختراق والقرصنة المعلوماتية واكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية.

4-مصلحة البيئة: تشرف على عمليات البحث في أسباب تلوث المياه والتربة والكشف عن المواد السامة المتواجدة في المحيط وأماكن العمل. (جاسم،، 2014، ص436.)

ج- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الامن الوطني:

قامت مصالح الامن بإنشاء المصلحة المركزية للجريمة الالكترونية سنة 2011 التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، وهي عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمنى خاص لمحاربة الجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني، وتم بعدها انشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

د- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها:

تشكلت بمقتضى المرسوم الرئاسي رقم 15-261 وهي سلطة إدارية مستقلة لدى وزير العدل تعمل تحت اشراف ومراقبة لجنة مديرية يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الامن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء، وتضم الهيئة قضاة وضباط واعوان من الشرطة القضائية تابعين لمصالح الاستعلامات العسكرية والدرك الوطني والامن الوطني وفقا لأحكام قانون الإجراءات الجزائية. (بوغرارة، 2018، ص112).

2-2: جهود الجيش الوطني الشعبي في الدفاع عن السيادة الرقمية

لقد قامت قيادة الجيش الوطني الشعبي بوضع استراتيجية دفاع سيبراني، تغطي كل الجوانب التي لها صلة بتحقيق نظام دفاع سيبراني متكامل، وتتمحور استراتيجية الدفاع السيبراني للجيش الوطني الشعبي حول سبعة محاور وهي:

أ-الجانب الوظيفي والتنظيمي: تكون اعمال الدفاع السيبرانيموجهة ومنفذة في إطار وظيفة او تنظيمية مكرسة لضمان تجانس وفعالية هذه الاعمال.

ب-الجانب القانوني: الاستمرار في تحيين وتعزيز الإطار القانوني المتعلق باستعمال تكنولوجيات الاعلام والاتصال عموما وتامين منظومات الاعلام خصوصا.

ج-جانب الموارد البشرية: الهدف منها جاهزية الموارد البشرية التقنية المعتبرة وذوي الكفاءات العالية في مجال الدفاع السيبراني.

د-الجانب التقني: تقوية وتكييف القدرات التقنية للحماية، والكشف والرد على الهجمات السيبرانية باستمرار.

هـ-جانب الوقاية والتحسيس: تحسيس مستخدمي الجيش الوطني الشعبي من المخاطر والتهديدات السيبرانية والوقاية منها.

و-جانب البحث والتطوير: ان استعمال هياكل البحث والتطوير للجيش الوطني الشعبي لوسائل تقنية خاصة او مشخصة يعد عنصرا حاسما في استراتيجية الدفاع السيبراني.

ي-جانب التعاون: تعزيز التعاون في مجال الدفاع السيبراني مع جيوش الدول الشريكة من اجل الاستفادة من الخبرات والوسائل التكنولوجية المتقدمة. (مجلةالجيش، 2011)

الفرع الثاني: مجهودات الدول الأوروبية

قامت فرنسا من خلال وزارتها الداخلية بمجموعة من المقترحات، تراها فعالة لحماية سيادتها الرقمية والدفاع عنها، حيث اقترحت فرنسا كيفية التدخل في الشبكة، وانه يجب ان تستفيد قوات الدولة الأمنية بتكوين متأقلم مع شبكات الاتصالات réseaux de télécommunications، وبطاقات الشرائح carte a' puces وعلم الحجب cryptologie، او الهواتف النقالة téléphones mobiles.

إن المقترح الفرنسي حسب وزير الداخلية، جاء فيه ان فرنسا لا تصبو الى المراقبة العامة على الفضاء الرقمي، ولكنها تريد ان تتزود بوسائل تجعل منه فضاء رقمي مضمون، فقد تكون هناك مساحة توازن بين شبكة بدون قواعد ولا مراقبة وبين شبكة تكون فيها المحتويات جائزة من طرف

الدولة، هذه المساحة تتمثل في دولة القانون (Michèle Alliot- Marie, 2009, p06)، ولذلك وجدت مجموعة من الوسائل:

أولا: الوسائل المستحدثة لمحاربة الجريمة المعلوماتية

1-1: الوسائل القانونية

وتكون من خلال تكوين محققي المعلوماتية cyber enquêteurs التابعين للشرطة والدرك الوطني وانشاء شهادة المحقق عن الجريمة المعلوماتية ووضع محققي المعلوماتية على مستوى مكتب مكافحة الجريمة المرتبطة بتكنولوجيا الاتصالات.

1-2: الوسائل الجديدة

تتمثل في وسائل جديدة للإشارة signalement، والحركة action حيث تنشأ وسائل الإشارة على أرضية وطنية للإشارة حول مواقع ومحتويات غير مشروعة على الانترنت مثل الموقع www.internt.signalement.gouv.fr، كما ان الإشارة الآلية لم تكن الا للمواقع الإباحية الطفولية، لذا تمنح هذه الأرضية لمستعملي الانترنت وسائل الإشارة آليا نحو أي شكل خبيث معاين على الانترنت وتعطي أيضا نصائح امنية للمستعملين. (سعادي،، 2014، ص 240)

1-3: الوسائل الجديدة للتحرك

وهي عبارة عن الوسائل المقدمة للعمال ضد الاحتيال escroqueries لا سيما على الانترنت ومحاربتها بوسائل الوقاية كإنشاء مركز نداءات هاتفية، والقمع كوضع مجموعة متخصصة ضد الاحتيال على الانترنت على المستوى المركزي لمحاربة الجريمة المرتبطة بتكنولوجيا الاعلام والاتصال للشرطة، التي تسمح بمركزة التحقيقات حول الاحتيال على الانترنت والمعرفة بقوة الشعب filières.

1-4: ابتكارعقوبات جديدة

وذلك من خلال تجميد المحتويات ذات الطابع اللاأخلاقي من طرف موردي الدخول الى الانترنت باعتبارها نشاطات إجرامية والتسجيل في مشروع قانون التوجيه والبرمجة من اجل تحسين أداء الامن الداخلي(القانون رقم 267/2011، 2013)، هو مبدا تجميد هذه المواقع ومحتوياتها، وقد قامت جميع الديمقراطيات في العالم بهذه الخطوة، حيث جمدت مواقع بأوروبا والولايات المتحدة الامريكية مما أدى الى توقيف المد المالي للمجموعات الاجرامية المستعملة للأطفال.

1-5: وضع وسائل تحقيق جديدة

من اجل تعزيز السيادة الرقمية ضد الجريمة المنظمة توصلت فرنسا الى تمكين التقاط صور او أصوات عن بعد بمجرد استصدار قرار من القاضي التحقيق لان الكاميرات والميكروفونات لم

تعد كافية، لطلك تم استخدام التطورات التكنولوجية لمعرفة ما يحضر من طرف المجرمين من خلال حواسيبهم الخاصة، فالتقاط معطيات رقمية عن بعد هي إمكانية تسمح للمحققين بالقبض على المعطيات في الوقت التي تنشر فيها على الشاشة او عندما ترقن على لوحة الحروف.

ثانيا: اقتراحات فرنسا لحماية سيادتها الرقمية

من اجل حماية السيادة الرقمية لفرنسا، اقترحت تدعيم ومضافة الوسائل البشرية والمادية والقانونية حتى يجعل من الانترنت فضاء للحريات والمسؤوليات وهذا بوجوب تفضيل تقارب شامل وعالمي وتقارب مؤسس على التعاون الدولي ضد اخطار تجاهل الحدود، مما يستوجب التحرك مع بعض فحماية السيادة الرقمية تعني ايضا الحفاظ على الشركات ضد التدخل و الجوسسة الصناعية ولذلك تم انشاء المجلس الاقتصادي للأمن على مستوى وزارة الداخلية للتمكن من تعيين الاخطار(Ghernaouti-Hèlie)2010،p24) ,كما فعلت المكتب المركزي لمحاربة الجريمة المرتبطة بتكنولوجيا المعلومات والاتصال Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication التابع للمديرية المركزية للشرطة القضائية.

وفي ذات السياق أنشئ في جويلية 2009 الوكالة الوطنية لأمن أنظمة المعلومات Agence nationale de sécurité des systémes d'information، التي لها صلاحيات وطنية وتابعة للأمن العام للدفاع (Michèle Alliot- Marie, 2009, p06)، بينما طالبت دول أوروبية تفعيل حقوق جديدة كحق التجميد droit a' la désactivationوحق صمت الشرائح droit au silence des puces، يسجل ضمن تمديد مبدا الموافقة القبلي المعمول به في أوروبا في ميدان التجارة الالكترونية، حيث يسمح للمواطنين بإعادة تنشيط الشرائح بصورة ارادية وحالة بحالة والملتقطين الموجودين في محيطهما.

المطلب الثاني: الجهود الدولية للدفاع عن السيادة الرقمية

إن مسألة الحفاظ على السيادة الوطنية واسترجاعها في مواجهة النشاطات الغير مشروعة هي مسألة يعترف بها الجميع وهي تفوق الحدود الوطنية وتتخطاها ولا يمكن التصدي لها إلا بالتعاون الدولي، لذلك ارتأت الدول من خلال تنظيماتها الدولية على كافة الأصعدة لإيجاد آليات تشريعية ومؤسساتية من اجل تحقيق مواجهة فعالة للأنشطة الغير مشروعة، لذلك نتناول في هذا المطلب الجهود العالمية والجهود الإقليمية للدفاع عن السيادة الرقمية من خلال فرعين.

الفرع الأول: الجهود العالمية للدفاع عن السيادة الرقمية

تجسدت هذه الجهود من خلال عمل منظمة الأمم المتحدة والاتحاد الدولي للاتصالات وكذا مجلس أوروبا.

أولا: جهود منظمة الأمم المتحدة للدفاع عن السيادة الرقمية

بدأ الاهتمام بالتصدي للأنشطة المخترقة للسيادة الرقمية على مستوى الأمم المتحدة أثناء المؤتمر الثامن للأمم المتحدة من اجل الوقاية من الجريمة ومعالجة المنحرفين المنعقدة بهافانا(كوبا) من 27اوت الى 7سبتمبر 1990، حيث تبنت فيه الجمعية العامة قرار يتعلق بالتشريع في مسألة الجريمة المعلوماتية، وقد تلت هذا المؤتمر العديد من الاعمال في مجال الدفاع عن السيادة الرقمية للدول، والتي نبدأها سنة 1994، وفي سنة 2005 أثناء المؤتمر الحادي عشر للأمم المتحدة حول الوقاية من الجريمة والعدالة الجنائية المنعقد في بانكوك (تايلاند)، تبنت الأمم المتحدة إعلانا حول ضرورة تجانس وتوحيد تشريعات محاربة الجريمة المعلوماتية، كما ان الأجهزة التابعة للأمم المتحدة تبنت هي أيضا العديد من القرارات في هذا الصدد ومن بينها:

لجنة الوقاية من الجريمة والعدالة الجنائية التابعة لمكتب الأمم المتحدة لمحاربة المخدرات والجريمة UNODC حيث اتخذت تدابير فعالة لمحاربة الاستغلال الجنسي للأطفال (2007).

المجلس الاقتصادي والاجتماعي للأمم المتحدة والذي تبنى قرارا حول التعاون الدولي في مسألة الوقاية والتحقيقات والمتابعات والعقوبات المتعلقة بالغش والتعسف والتزوير في الهوية لأغراض إجرامية والمخالفات الملحقة بها (2004).

ثانيا: جهود الاتحاد الدولي للاتصالات للدفاع عن السيادة الرقمية

إن الاتحاد الدولي للاتصالات يلعب دورا بارزا في تقعيد normalisation وتنمية الاتصالات ومسائل الامن المعلوماتي cybersécurité، حيث ان الاتحاد هو من بادر للقمتين العالميتين حول مجتمع المعلومات المنعقدتين في جنيف 2003 وتونس 2005، اللتين تمت فيهما مناقشة المواجهة الواجب اتباعها للمشاكل الجديدة المرتبطة بتطور المجتمع العالمي للمعلومات وكذا تطوير قواعد وقوانين ملائمة لها. (الأمم المتحدة،، 2005 ، ص 7)

هذا ونشير ان مخطط العمل لجنيف بين أهمية التدابير المتعلقة بمحاربة الجريمة المعلوماتية كما كانت قمة تونس العالمية حول مجتمع المعلومات فرصة لفحص مشكل الجريمة المعلوماتية وهو ما اظهرته اجندة تونس سنة 2005 حول مجتمع المعلومات وذلك بضرورة التعاون الدولي في محاربة الجريمة المعلوماتية، ثم تم إطلاق " البرنامج العالمي للأمن المعلوماتي للاتحاد الدولي للاتصالات"GCA، وفي إطار مجال العمل المعني ب "التدابير القانونية"، تضع "الهياكل التنظيمية"

إطار العمل وإستراتيجيات الاستجابة، فيما يتعلق بمنع الهجمات السيبرانية وتتبُّعها والردِ عليها(الاتحاد الدولي للاتصالات، 2007، ص38)، ويركز مجال "بناء القدرات" على وضع استراتيجيات لآليات بناء القدرات من أجل: زيادة الوعي و تعزيز الأمن السيبراني في إطار برنامج السياسات العامة الوطنية. (Framework, 2008)

ثالثا: جهود مجلس أوروبا للدفاع عن السيادة الرقمية

بين مجلس أوروبا الطابع الدولي للمخالفات المعلوماتية cyber délits، التي عالجها مؤتمر حول مختلف مظاهر الاجرام الاقتصادي، كما تلتها خطوات أخرى تمثلت في تعيين المجلس للجنة خبراء مكلفة بفحص المظاهر القانونية للجريمة المعلوماتية سنة 1985، كما وتبنت اللجنة الأوروبية حول المسائل الاجرامية " التقرير حول الجريمة المرتبطة بالحاسوب"، وهذا الأخير حللت فيه الاحكام القانونية للموضوع في القانون الجنائي. (سعادي،، 2014، ص 240)

الفرع الثاني: الجهود الإقليمية للدفاع عن السيادة الرقمية

تجسدت هذه الجهود من خلال مجموعة من المنظمات الإقليمية كالاتحاد الأوروبي ومنظمة التعاون والتنمية الاقتصادية ومنظمة التعاون الاقتصادي لآسيا والمحيط الهادي، ومنظمة الكومنولث، جامعة الدول العربية، مجلس التعاون الخليجي، منظمة الدول الامريكية.

أولا: جهود الاتحاد الأوروبي للدفاع عن السيادة الرقمية

تظهر جهود الاتحاد الأوروبي للدفاع عن السيادة الرقمية في تبني هذا الأخير بلاغ اللجنة communicationالأوروبية سنة 1999، المعنون" أوروبا الالكترونية 2005-مجتمع معلومات للجميع"، فكان المبادر بإطلاق فكرة "أوروبا الالكترونية "eEroupe، ثم بعد ذلك تبنى سنة 2000" مخطط العمل أوروبا الالكترونية" ، كما قامت اللجنة فيما بعد بنشر بلاغ سنة 2001 تضمن "امن الشبكات والمعلومات" والذي حللت فيه مشاكل الامن عبر الشبكات مقترحة خطوطا عريضة استراتيجية من اجل العمل في الميدان.

ثانيا: جهود منظمة التعاون والتنمية الاقتصادية للدفاع عن السيادة الرقمية

لقد بادرت منظمة التعاون الاقتصادي والتنمية في سنة 1983 بوضع دراسة حول إمكانية التجانس الدولي للقانون الجنائي من أجل مواجهة مشكل الجريمة المعلوماتية، حيث نشرت تقريرا متعلقا بتحليل التشريع ومقترحات محاربة الجريمة المنظمة خلال سنة 1985، كما أنشأت لجنة سياسة الاعلام والمعلوماتية والاتصالات PIIC سنة 1990، مجموعة خبراء مكلفة بإعداد حزمة من التوجيهات تسير أمن المعلومات التي سيتبناها مجلس منظمة التعاون والتنمية الاقتصادية سنة 1992(60)، كما ان المنظمة تبنت كذلك طبعة جديدة معنونة " الخطوط

التوجيهية لمنظمة التعاون والتنمية الاقتصادية المسيرة لأمن أنظمة وشبكات المعلومات نحو ثقافة الامن".

ثالثا: منظمة التعاون الاقتصادي لآسيا والمحيط الهادئ للدفاع عن السيادة الرقمية

كان موضوع المنتدى الإنمائي الأفريقي الأول، الذي نظمته اللجنة الاقتصادية لأفريقيا وعقد في أديس أبابا في تشرين الأول/أكتوبر1999، التحدي الذي تمثله العولمة وعصر المعلومات بالنسبة لأفريقيا"،وتشمل شبكة المنظمات غير الحكومية لأفريقيا(NGONET) بالإضافة إلى شبكة مراكز اتصال عن بعد، وبرنامج لتسخير الخبرات الرقمية لمغتربي أفريقيا وتشكيل تحالف دوائر الأعمال الأفريقية الذي يرمي إلى تشجيع تنمية الهياكل الأساسية للمعلومات والاتصالات في أفريقيا (الأمم المتحدة، 2000، ص42)، وفي المجال نفسه ساهمت مجموعة العمل الخاصة بالاتصالات والاعلام التابعة للمنظمة APEC-TEL، نشاط اعمال المنظمة التي ترمي الى مضاعفة الامن المعلوماتي، وتبنت استراتيجية الامن المعلوماتي سنة 2002. (الأمم المتحدة، 2010، ص8.)

رابعا: جهود منظمة الكومنولث للدفاع عن السيادة الرقمية

إن وزراء العدل بمنظمة الكومنولث قرروا انشاء مجموعة خبراء ترتكز في عملها على معاهدة مجلس أوروبا حول الجريمة المعلوماتية من اجل اعداد إطار قانوني لمحاربة هذا المرض، وقد قدمت تقريرا وتوصيات في هذا الصدد سنة 2002، كما قدمت المجموعة في نفس السنة مشروع قانون نموذج حول الجريمة المعلوماتية المرتبطة باستعمال الحاسوب الذي جاء متطابقا مع القواعد المحددة من طرف المعاهدة حول الجريمة المعلوماتية.

خامسا:جهود منظمة الدول الامريكية للدفاع عن السيادة الرقمية

تعمل منظمة الدول الامريكية منذ سنة 1999 بنشاط من أجل حل مسألة الجريمة المعلوماتية في المنطقة، حيث قامت المنظمة بالعديد من الاجتماعات في إطار عهدة وزراء العدل او النواب العامين للدول الامريكية REMIA، من اجل المطالبة بإنشاء مجموعة خبراء حكوميين حول الجريمة المعلوماتية التي كلفت ببعض المهام.

خاتمة

نخلص في الأخير الى القول بأن الانتشار الكثيف لتقنية المعلومات والاتصال عالميا فضلا عن غيرها من المؤشرات التي تعكس تنامي التجارة الالكترونية والاستخدامات المدنية استنادا على البنية التحتية المعلوماتية، ودورها في الاقتصاد والسياسة وفي عمل الحكومات والمرافق الحيوية، الامر الذي أدى الى تلاشي مفهوم سيادة الدول كما استقر عليه قبل المستحدثات التكنولوجية

الجديدة لا سيما الانترنت التي تخطت الحدود الجغرافية، إذ ان الدول بدخولها عصر الرقمية والانترنت على الخصوص فقدت هذه السيطرة على فضائها السيادي، مما شكل تصاعد الأهمية الإستراتيجية للمجال الرقمي، وعلى النحو من ذلك بات يعاني من تصاعد الهجمات السيبرانية وانتهاك الخصوصية وغيرها من المخاطر التي تهدد امن واستقرار المجال الرقمي وعلاقة ذلك بالثقة في التعاملات الرقمية، وهو ما دفع لأهمية وجود مبادرات إقليمية ودولية للعمل على تنظيم الحقوق والواجبات في المجال الرقمي ، وتوظيفه في مجال التنمية، فتم إطلاق العديد من المبادرات التي تقودها الأمم المتحدة لتحديد أفضل السبل لإدارة الحوكمة الرقمية ابتداء من عام 2002، كما تم إعلان القمة العالمية لمجتمع المعلومات في تونس عن إطلاق المنتدى العالمي لحوكمة الانترنت في عام 2005، ليكون منصة لكافة الشركاء في مجتمع المعلومات العالمي لوضع السياسات المثلي المتعلقة بالأنترنت، ومحاولات رصد التغيير الذي أحدثته التقنيات الرقمية في يوليو 2018 ،وتحسين الاستجابة في ظل توفير إطار عمل لتعزيز أهداف الأمم المتحدة للتنمية المستدامة 2030 وذلك من خلال التعاون الرقمي وحماية حقوق الإنسان والقيم على الإنترنت.

ومما تقدم ذكره نستنتج الآتي:

1-أن جميع دول العالم باتت مطالبة اليوم قبل غد، بإعلان سيادتها الرقمية على كامل أراضيها وتوجد بنية رقمية يتوجب حمايتها من الاختراق.

2-رغم الجهود الدولية والإقليمية المبذولة في مجال الدفاع عن السيادة الرقمية، إلا أنها لا تزال بعيدة عن الأهداف المرجوة خاصة أن الفضاء الالكتروني أصبح مكاناً خطراً بالنسبة للدول التي لم تتبنى وضع خطط استراتيجية سواء اكانت تلك الخطط قريبة أم متوسطة أم بعيدة المدى وذلك

لحماية بنيتها التحتية الالكترونية.

3-أصبح الفضاء الإلكتروني من أكثر الفضاءات أهمية وإستراتيجية والأكثر عرضة للاختراق وللتلاعب في أي لحظة، فقد باتت جرائمه تهدد امن المعلومات للقطاعات الحيوية المتعددة في الدول والمجتمعات، ومنها قطاع الإعلام والاتصالات، وقطاع المال والأعمال، وقطاع التجارة وقطاع الطاقة وغيرها من القطاعات.

4-إن من العوائق التي تواجه أمن الفضاء الالكتروني لمعظم الدول، هو انخفاض مستوى الوعي بأمن المعلومات، وقلة الكوادر المؤهلة لحماية فضاء الدول بخاصة دول العالم الثالث، بالإضافة لعدم وجود استراتيجية وطنية لحماية الفضاء الالكتروني في معظم الدول.

ومن خلال دراستنا للسيادة الرقمية نتوج بحثنا ببعض المقترحات:

1-ضرورة وضع تنظيم يتم من خلاله استحداث اساليب جديدة لحماية استخدام اجهزة الكومبيوتر وحماية البيانات المتصلة به تلك الاجهزة وحماية مؤسسات الدول.

2-يجب على الدول أن تتبنى وضع خطط استراتيجية سواء اكانت تلك الخطط قريبة أم متوسطة أم بعيدة المدى وذلك لحماية بنيتها التحتية الالكترونية.

3- ضرورة وضع تنظيم يمتد لتأسيس مفهوم السيادة الرقمية حول العالم والذي يكرس قواعد التعامل مع البيانات الرقمية المتعلقة بالأفراد ومختلف مؤسسات الدول.

4- ضرورة تفعيل استراتيجية لإدارة المخاطر، تراعي التوازن ما بين الحماية الالكترونية والمراقبة والاستجابة للحوادث، ذلك ان الحماية لا تتوقف فقط على الانظمة التقنية، بل هي منظومة متكاملة من خطط استراتيجية، وسياسيات، وحوكمة وعناصر بشرية، وذلك للحد من الهجمات الالكترونية

قائمة المراجع :

1- المؤلفات

-سعادي محمد (2003) ، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، الإسكندرية، مصر .

-هلالي عبد الله،(2003) الجوانب الإجرائية والموضوعية لجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية القاهرة، مصر .

- ممدوح عبد الحميد عبد المطلب(2006) ، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر .

-سلطان العلماءمحمد عبد الرحيم ،(2004) جرائم الانترنت والاحتساب عليها، بحوث مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثالث، العدد الثالث.

-يوسف أبو الحجاج،(2010) ، أشهر جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الكتاب العربي، القاهرة، مصر

- ممدوح إبراهيمخالد(2009) ، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي الإسكندرية، مصر.

-أيمن عبد الحفيظ،(2003) إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، الناشر هو المؤلف،

-احمد خليفة الملط(2006) ، الجرائم المعلوماتية، الطبعة الثالثة، دار الفكر الجامعي، القاهرة، مصر .

-حسام فايز(2019) ، الإرهاب الالكتروني والثورة الرقمية، الطبعة الأولى، مؤسسة طيبة للنشر والتوزيع، القاهرة، مصر .

2-االمؤلفات الأجنبية

أ- المؤلفات بالفرنسية

-Vers l'ètablissement(2005)d'une souveraineté nationale numèrique Revue Whiskey du 10 Juin .

- Karim Benyekhlef(2002) : L'Internet, un reflet de concurrence des Souverainetés, Revue Lex Electronica, Volume 8n'1 / Automne ..

- Nathalie Kosciusko(2009), Allocution aux actes du colloque du 17Juin, lintitulè : Souverainetènumèrique, Assemblèe nationale(2009) (France), dossier : fondation Prometheur, Juin .

-Laure ZICRY(2014) , Enjeux et maitrise des cyber-risques, largus, edition, France.

-Solange Ghernaouti-Hèlie(2010) , Comment lutter contre la cybercriminalité ? Revue Pour la Science n'391/Mai .

-Philippe Wolf / Lue Vallèe, Cyber-conflits, quelques clés de comprèhension : INHES/

ب- المؤلفات بالإنجليزية

-Conflicts of Interest, Privacy/Confidentialité, and Tissue Repositories : Protections, Policies, and Practical Strategies Conference co-sponsored (2004) by PRIM&R and the Columbia University Center of Bioethics. May 3-5 ; Boston, MA.

-The Global cybersécurité Agenda (GCA)،(2008)A Framework for International Cooperation in Cyber Security, International Télécommunication Union (ITU) ،April,

-الرسائل الجامعية

-جميل حمود(1997) ، تأثير التكنولوجيا الحديثة في العلاقات والقواعد الدولية، أطروحة مقدمة لنيل متطلبات شهادة الدكتوراه،كلية الحقوق، الجامعة اللبنانية، لبنان .

-أيمن عبد الحفيظ(2003) ، إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، أطروحة مقدمة لنيل متطلبات شهادة الدكتوراه في علوم الشرطة، كلية اقتصاد وعلومسياسية، جامعة القاهرة،مصر.

-المقالات

-فائز دنون جاسم(2014) ، تأثير الانترنت على مبدأ السيادة، مقال منشور في مجلة كلية الحقوق، ، ، العدد السابع، .

-عصام نعوسمصطفى (2012) ، سيادة الدولة في الفضاء الالكتروني، مقال منشور في مجلة الشريعة والقانون، ،المجلد السادس والعشرون، العدد الحادي والخمسون، .

-البحوث والمؤتمرات

-الأمم المتحدة(2010) ، مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، تقرير عن اجتماع الفريق العامل المعني بالتعاون الدولي، المعقود في فيينا يومي 27و28 تشرين الأول/أكتوبر

-المؤتمر الثامن1990) ، الذي عُقد في هافانا، المعاهدات النموذجية لتسليم المجرمين وتبادل المساعدة في المسائل الجنائية ونقل الإجراءات في المسائل الجنائية ونقل الإشراف على المجرمين المحكوم عليهم بأحكام مشروطة أو المفرج عنهم إفراجا مشروطاً، وقواعد الأمم المتحدة الدنيا النموذجية للتدابير غير الاحتجازية (قواعد طوكيو)، A/CONF.144/6.

- ذكي ذكي أمين حسونة(1993) جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، الفترة من 25الى 28 أكتوبر، القاهرة، .

-الأمم المتحدة(2006) ، المجلس الاقتصادي والاجتماعي، لجنة حقوق الإنسان، اللجنة الفرعية لتعزيز وحماية حقوق الإنسان، الدورة الثامنة والخمسون، البند الثالث من جدول الأعمال المؤقت، " إقامة العدل وسيادة القانون والديمقراطية"، ورقة عمل أعدها السيد فلاديمير كارتاشكين عملاً بمقرر اللجنة الفرعية 105/2005. E/CN.4/Sub.2/2006/7

-الارشاد الخامس(2006) ، الجرائم السيبرانية، ورقة بحثية خلفية لارشاد الجرائم السيبرانية، .

-الأمم المتحدة، تقرير الأمين العام عن اعمال المنظمة، تجسير الفجوة الرقمية، الدورة الخامسة والخمسون، الملحق رقم 1(**A/55/1**)، 2000.

-الأمم المتحدة(2005) ، الاتحاد الدولي للاتصالات، القمة العالمية لمجتمع المعلومات، الوثائق الصادرة عن القمة، جنيف 2003 -تونس 2005، ديسمبر .

-راسل تايلر(2007) ، أهمية التعاون الدولي في منع جرائم الإنترنت، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 06/19/ ، المملكة المغربية.

-الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الاسكوا)(2019) ، نشرة التكنولوجيا من أجل التنمية في المنطقة العربية، آفاق عالمية وتوجهات إقليمية بيروت، .

E/ESCWA/TDD/2019/4ONDRP-Rapport 2011.

-Michèle Alliot- Marie(2009) , Allocution aux actes du collque du 17 Juin 2009, Intitulè, Souverainetènumèrique, Assemblèe nationale (France), Dossier, Fondation Prometheus, Juin .

-الاتفاقيات الدوليةوالقوانين

أ- الاتفاقيات الدولية

-اتفاقية بودابيست (الاتفاقية الأوروبية المتعلقة بالجرائم المعلوماتية) بتاريخ 08 /11 2001.

-القانون العربي(2004) النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتي وما في حكمها لعام 2004والذي اعتمدته جامعة الدول العربية.

-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المؤرخة في ديسمبر2010.

ب-القوانين

-الامر 66-106، المؤرخ في 08جويلية 1966، المتضمن قانون العقوبات الجزائري المعدل والمتمم

-الامر 15-02، المؤرخ في 23 جويلية 2015 المعدل والمتمم للأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية كإجراء جديد لمواكبة السياسة الجزائية المعاصرة وتجسيد العدالة التصالحية التي تبنى على الرضائية والتفاوض تحقيقا للسلم الاجتماعي.

-القانون رقم 16- 02مؤرخ في 14رمضان عام 1437 الموافق ل 19يونيو سنة 2016، المتمم للأمر رقم 156-66المؤرخ في 18صفر عام 1386الموافق 8 يونيو سنة 1966والمتضمن قانون العقوبات.

-قانون رقم 09-04 مؤرخ في 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. (ج ر رقم 47 المؤرخة في 16 أوت2009.

-المواقع الالكترونية

http://www.itu.int/aboutitu/annual_report/2007/pdf/2007-ar.pdf

Http://www.itu.int/osg/csd/cybersecurity/gca/overview/index.html