الأمن السيبراني إشكالية المصطلح وتحديات المرحلة.

Cyber security: problematic of the term and its challenges stage.

عمار بن جدة

طالب دكتوراه بجامعة الأمير عبد القادر للعلوم الإسلامية – قسنطينة –

فرقة البحث" الحقوق والحريات الرقمية "

مخبر الدراسات الشرعية بجامعة الأمير عبد القادر للعلوم الإسلامية .

ammarbendjedda4@gmail.com

الملخص:

من اكبر التحديات التي تواجه الدول في مكافحة الجرائم الإلكترونية ومختلف تهديدات الفضاء السيبراني هو إعتماد التشريعات الفعالة لمواجهته ووضع مقاربات واجتهادات تواكب على الأقل السرعة والفعالية التي تعرفها الجرائم الإلكترونية يوما بعد يوما.

وأول خطوة في هذا المسار هو ضرورة وضع تصور شامل لمختلف تلك التحديات والعقبات التي تحول دون وضع تشريع دقيق و فعال للتقليل من الأخطار التي تهدد الفضاء الرقمي سواء على المستوى الدولي أو الوطني .

لذلك على صناع القرار والمشرعين وجهات نفاذ القانون التعرف على هذه التحديات حتى يمكن تجاوزها من خلال تشريعات غير تقليدية تواكب التطور الحاصل في الفضاء الرقمي وقادرة على الوقوف على مختلف التهديدات السيبرانية .

في هذا السياق ومن اجل تحقيق نسق تكاملي بين البعد المفاهيمي للأمن السيبراني ومختلف التحديات الفنية والقانونية (الموضوعية والإجرائية) التي تواجهنا في تحقيقه، جاءت هذه الورقة البحثية لوضع مقاربة قانونية قد تساهم في وضع القواعد القانونية من أجل تحقيق هذا الأمن المنشود .

المقدمة :

بعد انفجار الثورة المعلوماتية والتطور الهائل الذي عرفته تكنولوجية الإعلام والاتصال ودخول العالم العصر الرقمي بكل آثاره الايجابية والسلبية، وجدت البشرية نفسها أمام واقع جديد مليئ بمختلف التحديات والتهديدات، فصرنا نسمع عن التهديدات السيبرانية والهجمات الإلكترونية التي هددت الأمن القومي للدول بشكل لم تشهده البشرية من قبل.

وأمام هذا الوضع صار لزاما على الحكومات وجهات نفاذ القانون التحرك بسرعة من أجل البحث عن حلول قانونية للحد من هذا النوع من التهديد، لأن التشريعات الحالية لم تعد باستطاعتها مواكبة هذا النوع من الجرائم والتهديدات، خاصة مع سرعة منفذي الجرائم الالكترونية وجمود القوانين.

لكن قبل أن نطلب من المشرع الوطني أو الدولي البحث عن حلول قانونية، لابد لنا أن نشرح ونحلل هذه الظاهرة الجديدة بكل أبعادها التقنية والقانونية، حتى نستطيع وضع ا الحلول المناسبة لمواجهة مختلف التهديدات الناجمة عنها.

لذلك جاء هذا البحث للإجابة عن الإشكالية التالية :

ما هو مفهوم الأمن السيبراني و أهم الإشكاليات والتحديات التي يثيرها على المستوى الوطني والدولي ؟

وللإجابة عن هذه الإشكالية إعتمدت الخطة الثنائية التي أراها مناسبة لمثل هذه المواضيع من خلال مبحثين ، عالجت في المبحث الأول مفهوم الأمن السيبراني وعلاقته بالمصطلحات ذات الدلالة المتقاربة كالأمن الرقمي والجريمة الإلكترونية، ومختلف التهديدات التي يمكن أن تنتج عن هذه المتغيرات.

وفي المبحث الثاني حاولت الوقوف على مختلف الإشكالات والتحديات الفنية والقانونية التي يثيرها الفضاء السيبراني والتي يساعد فهمها في وضع التشريعات و القوانين المناسبة.

واعتمدت بشكل رئيس على تقرير الخبراء المقدم إلى الأمم المتحدة حول الأمن السيبراني ، خاصة تقرير سنة 2011 و آخر تقرير لسنة 2019 و 2020 الخاص بالأمن السيبراني .

المبحث الأول : مفهوم السيبرانية و أبعادها الأمنية

سنحاول من خلال هذا المبحث الوقوف على مختلف المفاهيم والمصطلحات المتعلقة بالفضاء السيبراني وأهم التهديدات التي يمكن أن يشكلها كمايلي :

المطلب الأول : الإطار المفاهيمي :

إن مسألة ضبط المصطلحات في المجال القانوني أمر مهم ويشكل تحديا جوهريا لرجال القانون، بإعتبار أن هذه المصطلحات والمفاهيم ستترجم إلى تشريعات وقوانين تعبر عن إرادة المجتمع ، ويزداد الأمر صعوبة وتعقيدا وحساسية إذا كنا بصدد الحديث عن التشريعات الجنائية .

ويعد الأمن السيبراني والمفاهيم القريبة منه، واحدا من المفاهيم المعقدة التي قدمت لها العديد من التعريف المختلفة والإسقاطات الواقعية التي صارت تصنع عالمنا الرقمي.

أولا : الأمن السيبراني :cyber Security

1- السيبر : CYBER و السبرانية أو **علم التَّربن** بالإنجليزية Cybernetics

كلمة سايبر Cyber مشتقة من Cybernetic وأصلها يوناني وتعني التوجيه والسيطرة، وعرفها Norbert Wiener [1] في عام 1984م "الدراسة العلمية للسيطرة على الأحياء والآلات وآلية التواصل بينها"،وهي بذلك تعني " : علم الاتصالات وأنظمة التحكم الآلي Cybernetics أو التوجيه، ومصدرها في كل من الآلات والأشياء الحية علم التحكم الذاتي.[2]

وتعرف كذلك بالقوة السيبرانية : Cyber Power حيث عرفها Joseph S. Nye, Jr. بأنها " تلك الموارد التي تتعلق بإنشاء المعلومات الإلكترونية والحاسوبية والتحكم فيها والاتصال بها، والتي تتشكل من البنية التحتية والشبكات والبرمجيات والمهارات البشرية. وهذا يشمل الإنترنت وأجهزة الكمبيوتر المتصلة بالشبكة ، وكذلك الشبكات الداخلية والتقنيات الخلوية والاتصالات الفضائية."

وتعرف القوة الإلكترونية من الناحية السلوكية بأنها القدرة على الحصول على النتائج المفضلة من خلال استخدام موارد المعلومات المترابطة إلكترونيا في المجال السيبراني. في أحد التعريفات المستخدمة على نطاق واسع ، فإن القوة السيبرانية هي "القدرة على استخدام الفضاء السيبراني لخلق مزايا والتأثير على الأحداث في بيئات تشغيلية أخرى وعبر أدوات القوة[3].

---

[1] **وربرت فينز** Norbert Wiener : عالم رياضيات أمريكي 1894-1964.

[2] قاموس أكسفورد : على موقع الإنترنت
https://www.oxfordlearnersdictionaries.com/definition/english/cybe

[3] Cyber Power By Joseph S. Nye, Jr. 1Joseph S.Nye JR , Cyber Power, Harvard Kennedy School, 2010, P: 03

2-الأمن السيبراني :

عرفت هيئة الاتصالات وتقنية المعلومات الأمن السيبراني بنفس تعريف الهيئة الوطنية للأمن السيبراني: "هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة (عتاد) وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك". [4]

ويمكن تعريف الأمن السيبراني انطلاقا من أهدافه بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات و المعلومات و يضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات ، حيث يهدف إلى حماية شبكات الكومبيوتر والمعلومات التي تحتويها من الضرر الخبيث أو التعطيل.[5]

ورغم تزايد الوعي بأهمية الأمن السيبراني، فإن إمكانيات تطبيق القانون الدولي لتنظيم سلوك الدول في الفضاء السيبراني تظل محدودة. ولقد دارت عدة نقاشات بشأن قدرة القانون الدولي على ضبط أنشطة الدول في الفضاء السيبراني. و من الحلول المطروحة من أجل التحكم في هذا الفضاء هو ضرورة التأكيد على أهمية تطوير أعراف مشتركة تسهل الوصول إلى تفاهم بين الدول. ومع ذلك، بالنظر إلى التحديات المرتبطة بتحديد المسؤوليات والتعاريف المتناقضة حول المعنى الحقيقي للأنشطة "السيبرانية"، فإن الموافقة على هذه الأعراف – أي فهم طريقة تطبيقها – وقبولها وتعزيزها كلها من طرف الدول ما تزال تسير بإيقاع بطيء[6] .

3- ظهور فكرة الأمن السيبراني :

أما على مستوى الجانب الممارساتي للدول، فقد ارتبط ظهور الأمن السيبراني بظهور الهجمات السيبرانية والتي حدثت بسبب عاملين أساسين:

الأول باستحداث أجهزة الكمبيوتر في منتصف الخمسينيات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقمياً(Digital) ، رافقه تظافر جهود عدد من الشركات الخاصة والعامة، توج بتطوير وحدة المعالجة المركزية(CPU) ، وذلك لتسهيل المهام الموكلة له، وقد تطور ذلك بصورة جذرية في العقود

---

[4] موقع الوينار (وزارة التقنية و الإتصالات السعودية) : https://attaa.sa/library/view/868

[5] بارة سميرة : **الأمن السيبراني (cyber Security) في الجزائر:السياسات و المؤسسات** ، المجلة الجزائرية للأمن الإنساني، جامعة الحاج لخضر،باتنة ،العدد الرابع : جويلية 2017 ، ص 257.

[6] **دوريات – قضايا إستراتيجية ، تحديات القوانين: الفضاء الافتراضي والقانون الدولي : المركز العربي لأبحاث الفضاء الإلكتروني** السبت،25 نوفمبر 2017 - 02:13

اللاحقة، حتى أصبح جهاز الكمبيوتر أساسا في عمل الكثير من المؤسسات الخاصة والعامة، فضلا عن الحياة اليومية.

أما الثاني فهو ظهور الشبكة العنكبوتية (الإنترنت)، الذي أحدث انقلابا مثيرا في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة، وقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري في مطلع التسعينيات من القرن المنصرم، وذلك حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة Cyber Cold War أو سباق التسلح السيبراني Cyber arms race .[7]

ثانيا :مفاهيم ذات صلة :

1- **الفضاء الرقمي:** يطلق على هذا الفضاء عدة مصطلحات منها العالم الافتراضي أو الفضاء السيربراني أو العالم الالكتروني، كلها مصطلحات نستخدمها بمعنى واحد وهو الاتصال المستمر بين سكان الأرض على مستوى شبكة الانترنت ، مما يقتضي التزامنية[8] .

ويعتبره البعض أنه مصطلح يوصف به حق الأفراد والتجمعات في التعبير عن آرائهم بالطريقة والكيفية التي يريدونها عبر استخدام أي أجهزة من أجهزة الاتصال المتاحة عبر الانترنت، والتي تستخدم مختلف التطبيقات المتاحة كالمدونات والشبكات الإجتماعية ومواقع مشاركة الصور ومقاطع الفيديو بالإضافة إلى المواقع الإخبارية و الصحف الالكترونية و غيرها.[9]

2- **الفضاء السيبراني :** عرفته الوكالة الفرنسة لأمن أنظمة الإعلامANSSI ، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأنه" :فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية ."فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون 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[10].

وعرفته الهيئة الوطنية للأمن السيبراني "بالشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات، وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، إلى جانب المعالجات

---

[7] الموسوعة السياسية poltical encylopedia، https://political-encyclopedia.org/dictionary

[8] محمد طوالبية: **إيديولوجية الفضاء الرقمي**، دراسة في الخلفيات المرجعية الأكاديمية للدراسات الاجتماعية والإنسانية، قسم العلوم الاجتماعية العدد 21 ، جانفي 2019 . ص 47 ..

[9] محمد الطاهر : **الحريات الرقمية، المفاهيم الأساسية**، مؤسسة حرية الفكر والتعبير، القاهرة، الطبعة الأولى،السنة 2012 ص 8.

[10] الموسوعة السياسية poltical encylopedia، https://political-encyclopedia.org/dictionary

وأجهزة التحكم المرتبطة بها، كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرد". [11]

3- الجريمة الإلكترونية:

و يستخدم كذلك مصطلح "الجريمة الحاسوبية"، وبصفة أكثر تحديدا "الجريمة السيبرانية"، لوصف فئة معينة من السلوك الإجرامي. وتتصف هذه الفئة من السلوك الإجرامي بعدة تحديات من ضمنها على السواء اتساع نطاق الجرائم المندرجة فيها والتطور الدينامي للأساليب الجديدة في ارتكاب الجرائم[12].

4- الفرق بين أمن المعلومات والأمن الإلكتروني

حدد خبراء التقنية عدة فروقات بين أمن المعلومات والأمن الإلكتروني ، بداية من ناحية المفهوم نجد أن أمن المعلومات هدفه المعلومة في حد ذاتها سواء أكانت رقمية أو ورقية أما الأمن الالكتروني فهو يعنى بحماية البيانات ،كل التقنيات المتعلقة بها وكل ما هو موجود في الفضاء الرقمي وحمايتها من أي هجمات إلكترونية على إختلافها .[13]

وعليه يمكن ان نعتبر أن هذه المفاهيم قريبة في مدلولاتها و استعمالاتها ، تاتي في الغالب بمعنى واحد فالعالم الافتراضي أو الفضاء السيبراني أو العالم الالكتروني كلها مصطلحات نستخدمها بمعنى واحد وهو الاتصال المستمر بني سكان الأرض على مستوى شبكة الانترنت، مما يقتضي التزامنية[14].

المطلب الثاني : مظاهر التهديدات في الفضاء السيبراني :

ظهرت عدة تهديدات متعلقة بالفضاء السيبراني وصلت إلى درجة الحروب بين الدول ، حيث شملت مجالها السيبراني ، حيث كان لها آثارا على أمن و اقتصاديات تلك الدول ، ضف إلى الهجمات التي يقوم بها الأفراد العاديين لأغراض ذاتية و مصالح شخصية ، و بيان ذلك فيمايلي :

أولا : حروب الفضاء السيبراني :

---

[11] موقع الوينار (وزارة التقنية و الغتصال السعودية) : https://attaa.sa/library/view/868

[12] الأمم المتحدة : المجلس الاقتصادي و الاجتماعي، **اتجاهات الجريمة على الصعيد العالمي والمسائل المستجدّة وتدابير التصدّي في مجال منع الجريمة والعدالة الجنائية**، لجنة منع الجريمة والعدالة الجنائية الدورة العشرون ، تقرير فريق الخبراء الحكومي الدولي المفتوح العضوَية عن الدراسة الشاملة لمشكلة الجريمة السيبرانية وتدابير التصدّي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص ، E/CN.15/2011/19، ص 6.

[13] https://attaa.sa/library/view/868 موقع العطاء الرقمي ، وزارة الإتصالات و تقنية المعلومات ، المملكة العربية السعودية .

[14] حمد طوالبية : **مرجع سابق** ، ص 03.

بعد أحداث 11 سبتمبر 2001 بدأ التركيز على الفضاء الإلكتروني كتهديد أمني جديد بفعل أحداث دولية كان أبرزها استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة ، وفي عام 2007 برز بوضوح دور الفضاء الإلكتروني كمجال جديد في العمليات العدائية في الصراع بين استونيا وروسيا وفي 2008 في الحرب بين روسيا و جورجيا،وجاء الهجوم الإلكتروني بفيروس "ستاكسنت "على برنامج إيران النووي عام 2010 ليمثل نقلة هامة بالتطور في مجال الأسلحة الإلكترونية . وعلى الرغم من الدور السياسي الذي لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في مطلع عام 2011، إلا أنها مثلت نقطة هامة لدعم الاهتمام الدولي بأمن الفضاء الإلكتروني ، وبرزت محاولات للسيطرة عليها بعد تصاعد الاحتجاجات في أكثر البلدان ديمقراطية وهي بريطانيا والولايات المتحدة.

وهو ما يعزز في ذات الوقت من انتشار الأنشطة غير السلمية للفضاء الإلكتروني، الذي يتجاوز الحدود الدولية[15].

ثانيا : تهديد الأمن الإقتصادي للدول :

صارت بيانات ومعلومات رواد الإنترنت و مستخدميه سلعة بملايير الدولارات ،و تجارة رائجة بأبعاد اقتصادية وفي بعض الأحيان استخباراتية ، كما حدث مع تطبيق ''مسلم برو'' الذي قام ببيع بيانات المستخدمين إلى الجيش الأمريكي وقيادة العمليات الخاصة تحديدا، وهو ما أسفر عن استخدامها في عمليات التصفية الأمريكية حول العالم. كما حذرت خدمة بث الصوتيات ''سبوتيفاي'' مستخدميها من تسريب بعض بيانات تسجيل المستخدمين (مثل: عناوين البريد الإلكتروني، وكلمات المرور، والجنس، وتواريخ الميلاد) لجهات خارجية بسبب ثغرة في البرنامج. كما تمكن أحد القراصنة من بيع كلمات المرور لمئات من المديرين التنفيذيين حول العالم، وذلك لأحد منتديات القراصنة المعروف باسم (Exploit.in.) بأسعار تتراوح بين 100 دولار و1500 دولار. وعلى صعيد متصل، أزالت ''جوجل'' في شهر أكتوبر 2020 تطبيقين من تطبيقات ''أندرويد'' الشهيرة من متجر الألعاب بسبب جمع بيانات المستخدمين الحساسة[16].

ثالثا : تهديد الأمن القومي للدول :

---

[15] نورة شلوش: **القرصنة الالكترونية في الفضاء السيبراني ا ربي التهديد المتصاعد لأمن الدول** ، مجلة بابل للدراسات الحضارية والتاريخية ، جامعة بابل ، العدد 02، ص 2.

[16] رغدة البهي : **الأمن السيبراني في 2020: بين الفرص والتحديات المركز المصري للفكر و الدراسات الاستراتيجية** ، مقال منشور بتاريخ January 11, 2021 بموقع : https://www.ecsstudies.com/13106/ تاريخ الدخول 25 مارس 2021 ، 22:00 سا.

في ظل التقدم التكنولوجي المهول الذي عرفته البشرية خاصة في بداية القرن الواحد والعشرين، ظهر نوع جديد من الحروب غير التقليدية مهددا لأمن الدول واستقرارها بإستعمال أسلحة إلكترونية لا تقل فتكا عن الأسلحة الكلاسيكية مع تنوع ما يسمى الفاعلين الالكترونيين في ساحة حرب لامتناهية في الزمان والمكان عبر الفضاء الإلكتروني . Conflict Cyber الذي يستخدم إما كوسيط للأعمال العدائية أو كحامل وناقل لحركة التفاعلات الصراعية أو بتحول الفضاء الإلكتروني إلى عنصر هام في القوة العسكرية من خلال تحوله إلى مجال لتطوير الأسلحة الإلكترونية أو السيبرانية Weapon Cyber ،والتي تعد شكلا جديدا من أشكال الأسلحة.

لذلك ذهب بعض الخبراء في الفضاء السيبراني إلى ضرورة وضع قانون خاص بهذا الفضاء من أجل السيطرة على الأنشطة غير السلمية في هذا الفضاء وفرض الاستخدام السلبي للتقدم التكنولوجي ووضع مصادر لهذا القانون تكون ملزمة للجميع.[17]

تعتبر الولايات المتحدة الأمريكية من الدول العظمى التي تملك أحدث التقنيات في المتعلقة بالفضاء السيبرياني ومن الدول القوية التي يمكنها مواجهة أي تهديد ، ومع ذلك نجد أنها قد تعرضت لأكبر الهجمات الالكترونية إلى درجة التأثير في نتائج انتخابات أكبر دولة ديمقراطية في العالم.

و هذا إن دل على شيئ فإنما يدل على أن لا استثناء لباقي الدول الأقل تقدما و ازدهرا في هذا المجال .

ونظرا لخطورة هذه المسألة على الأمن القومي للولايات المتحدة فقد التقت شركات التكنولوجيا الأمريكية بما فى ذلك فيسبوك وجوجل ومايكروسوفت وتويتر مع وكالات الاستخبارات الأمريكية مؤخرا لمناقشة استراتيجيات الأمن قبل الانتخابات الأمريكية نوفمبر 2020.

وبحسب موقع gadgetsnow الهندي، فقد التقت فرق أمن الشركات بممثلين من مكتب التحقيقات الفيدرالى، ومكتب مدير الاستخبارات الوطنية، وإدارة الأمن الداخلي، وذلك بمقر فيس

وقال ريتشارد سالجادو، مدير القانون فى جوجل، "فى شركتنا، استثمرنا فى أنظمة قوية لاكتشاف محاولات الخداع والقرصنة، وتحديد التدخل الأجنبي على منصاتنا، وحماية الحملات من الهجمات الرقمية، لكن التكنولوجيا ليست سوى جزء من الحل، فمن الأهمية بمكان أن تتعاون الصناعة وإنفاذ القانون وغيرهم لمنع أي تهديدات لنزاهة انتخاباتنا".

ويمكن أن يستخدم الفضاء الإلكتروني كوسيلة من وسائل الصراع داخل الدولة Inte–State بين مكوناتها على أساس طائفي أو اقتصادي أو ديني ، وهو ما يساعد على كشف ، ديناميكيات التفاعل الداخلي إلى الخارج بما يسهل من عملية الاختراق الخارجي عبر شبكات الاتصال بدعم أحد أطراف الصراع بأدوات غير قتالية[18].

---

[17] عادل عبد الصادق : **أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني**، سلسلة أوراق العدد 23: وحدة الدراسات المستقبلية مكتبة الإسكندرية ، ص 10.

المبحث الثاني : التحديات الفنية والقانونية للفضاء السيبراني.

نظرا لأهمية هذا الموضوع كما أشرنا آنفا ، فقد أقرت الجمعية العامة، في قرارها 230/65 ، إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية، حيث طلبت إلى لجنة التحديات العالمية، أن تنشئ، وفقا للفقرة 42 من إعلان سلفادور، فريق خبراء حكوميا دوليا مفتوح العضوية من أجل إجراء دراسة شاملة عن **مشكلة الجريمة السبرانية** والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، بما في ذلك تبادل المعلومات عن التشريعات الوطنية والممارسات الفضلى والمساعدة التقنية والتعاون الدولي، بغية دراسة الخيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجريمة السيبرانية واقتراح تدابير جديدة في هذا الشأن

وعقد الاجتماع الأول لفريق الخبراء في فيينا في الفترة من 17 إلى 21 جانفي 2011 والاجتماع السادس لفريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية في فيينا، 6-8 أبريل 2020، UNODC/CCPCJ/EG.4/2020/1 ، 7 January 2020.[19]

ومن خلال هذه التقارير يمكن أن نقف على أهم التحديات التي تواجه رجال القانون من التحديات التقنية والفنية التي تحيط الفضاء الرقمي وكذلك التحديات القانونية ذات الطابع الموضوعي والإجرائي والتي سوف نقف عليها فيمايلي :

المطلب الأول : التحديات التقنية والفنية .

إن قائمة التحديات التقنية والقانونية الفريدة المتصلة بالجريمة السيبرانية طويلة. ورغم أن مستخدمي خدمات الإنترنت يخلفون آثارا متعددة، فإنه يمكن للمجرمين عرقلة التحقيقات بتمويه هويتهم. فعلى سبيل المثال، إذا ارتكب أشخاص جرائم باستخدام مرافق طرفية عمومية لخدمات الإنترنت أو شبكات لاسلكية مفتوحة، فقد يصعب تحديد هويتهم. ومنشأ التحدي الأعم الذي يعترض سبيل التحقيق في الجريمة السيبرانية هو أنَّ الإنترنت توفر، من الناحية التكنولوجية، القليل من أدوات المراقبة التي يمكن أن تستخدمها سلطات إنفاذ القانون. فقد صممت الإنترنت أصلا كشبكة عسكرية تستند إلى بنية شبكية لا مركزية، الهدف منها هو الحفاظ على القدرة التشغيلية الرئيسية حتى في حال تعرض عناصر من الشبكة لهجمات. ولم يكن هذا النهج

---

[18] نورة شلوش : **مرجع سابق** ، ص 12 .

[19] الاجتماع السادس لفريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية ، فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية فيينا، أبريل، تحت رقم 2020 ، UNODC/CCPCJ/EG.4/2020/1 .

اللامركزي مصمما أصلا لتيسير التحقيقات الجنائية أو منع الهجمات من داخل الشبكة، كما أن تدابير التحقيق التي تستلزم وسائل للمراقبة تثير تحديات فريدة في هذا السياق[20].

ويمكن أن نحدد أهم هذه التحديات التقنية والفنية التي لها تأثيراتها المباشرة على الجوانب القانونية فيمايلي :

أولا : غياب الإحصاءات الدقيقة المتعلقة بالتهديدات السيبرانية :

إن وجود الإحصاءات المتعلقة بعدد الهجمات الالكترونية وعمليات القرصنة سواء تعلقت بالأفراد أو الدول، يساعد في رسم السياسات الجنائية وإعداد توصيات السياسات العامة.إلا أن الإشكال يطرح في عدم دقة هذه الإحصاءات كما ونوعا، لأنها تجسد إلا الجرائم المكتشفة والمبلغ عنها، وهناك مخاوف من أن عدد الحالات غير المبلغ كبير جدا وسبب عدم التبليغ في الغالب خشية المؤسسات التجارية أن يؤثر هذا النوع من الدعاية السلبية على سمعتها ، فحين تعلن شركة أن هناك من نجح في اختراق خادومها Serveur، فقد يفقد الزبائن الثقة هبا، مما يترتب عليه تكاليف قد تتجاوز حتى الخسائر الناجمة عن الاختراق .ولكن إذا لم يجر الإبلاغ عن الجرائم وملاحقة مرتكبيها قضائيا، فقد يعمد الجناة إلى تكرارها. وقد لا يعتقد الضحايا أن هيئات إنفاذ القانون ستتمكن من معرفة هوية الجناة.[21]

ثانيا :سيطرة القطاع الخاص على الفضاء الرقمي :

من التحديات التي تواجه جهات نفاذ القانون في التعامل مع التهديدات السيبرانية هو أن اغلب مقدمي خدمات الانترنت من القطاع الخاص، و هدفهم الأول هو الربح و كسب اكبر مساحات جديدة أمام المنافسين مما يصعب الوصول إلى البيانات المتعلقة بمنفذي الهجمات الالكترونية ، و هنا تظهر أهمية تعزيز وتوطيد التعاون بين السلطات الوطنية والقطاع الخاص[22].

والأخطر في الأمر أن القطاع الخاص في حد ذاته قد يكون تهديدا لأمن الفضاء الرقمي، فهنالك شركات تكنولوجيا المعلومات و شركات الاتصالات لديها علاقة وثيقة مع بعض الدول، وتعتمد عليها تلك الدول في الحصول على تراخيص تتيح لها الوصول إلى بيانات المستخدمين وتوفر المبادئ التوجيهية بشأن الأعمال

---

[20] الأمم المتحدة، المجلس الاقتصادي والاجتماعي، **تقرير فريق الخبراء الحكومي الدولي المفتوح العضوية عن الدراسة الشاملة لمشكلة الجريمة السيبرانية وتدابير التصدي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص**، رقم E/CN.15/2011/ 19 ، الدورة العشرون أفريل 2011م ،ص 16،

[21] الأمم المتحدة، المجلس الاقتصادي والاجتماعي، **تقرير فريق الخبراء الحكومي الدولي المفتوح العضوية عن الدراسة الشاملة لمشكلة الجريمة السيبرانية وتدابير التصدي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص**، لسنة 2011م، ص 10.

[22] الأمم المتحدة: **تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية**، فيينا مارس2019 ، رقم : UNODC/CCPCJ/EG.4/2019/2 المؤرخ في : 12 April 2019 ، ص 18..

التجارية وحقوق الإنسان، التي دعمها مجلس حقوق الإنسان في عام2011، من معايير عالمية لمنع ومواجهة الآثار الضارة على حقوق الإنسان المرتبطة بنشاط الأعمال التجارية.[23]

فكما هو معلوم فإنه يتوقف منع الجرائم السيبرانية والتحقيق فيها على عدد من العناصر المختلفة، حيث أن ارتكاب جريمة سيبرانية، حتى وإن كان الجاني يعمل بمفرده، يشمل تلقائيا عددا من الأشخاص والمؤسسات التجارية ، وبينما كثيرا ما يجري التركيز على كفالة وجود التشريعات المناسبة، فإن قطاع الصناعة الخاص يواصل أداء دور هام في منع الجريمة السيبرانية والمساعدة في التحقيقات ذات الصلة على السواء. بيد أن مشاركته في التحقيقات المتصلة بالجريمة السيبرانية محفوفة بعدد من التحديات[24].

لذلك نجد أن الدول المتقدمة سعت إلى عقد إتفاقيات مختلفة مع مقدمي خدمات الانترنت بما يحافظ على الأمن القومي للدول و حمايتها من أي هجمات إلكترونية ،بالرغم من الانتقادات الشديدة التي طالت مثل هذه الاتفاقيات بحجة أنها تشكل تهديد للحريات المدنية وإمكانية استغلال السلطات لها للتجسس على المواطنين وانتهاك خصوصياتهم .

ومن أحسن الأمثلة في هذا المجال قانون مشاركة وحماية المعلومات الرقمية Cyber Intelligence Sharing and Protection Act) ويعرف اختصارا اسم سيسبا (CISPA) وهو قانون اقترح في الولايات المتحدة يسمح بمشاركة معلومات حركة الإنترنت بين الحكومة الأمريكية و شركات التقنية والتصنيع. والهدف المعلن من هذه الوثيقة هو أن يساعد الحكومة الأمريكية على تحري تهديدات الإنترنت وضمان أمن الشبكات ضد الهجمات على الإنترنت.[25]

ثالثا : الطبيعة الخاصة للأدلة الرقمية :

بعض القضاة ليسوا على دراية بالأدلة الرقمية ومميزاتها وتعقيداتها التكنولوجية ، ونتيجة لذلك، يخضع هذا النوع من الأدلة في كثير من الأحيان لمعايير أعلى فيما يتعلق بالتوثيق و الحفظ، ينبغي إبلاء الاعتبار إلى عدم وجود أسباب عملية لفرض معايير أعلى فيما يتعلق بسلامة الأدلة الرقمية مقارنة بالأدلة التقليدية .لذلك تعمل الكثير من الدول على تجميد الأدلة الإلكترونية لمنع الإضافة أو الحذف أو التعديل عن طريق تدابير مثل

---

[23] فرانك لا رو : **تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير** Distr * الجمعية العامة 17 April 2013 ، Aالمتحدة الأممHRC/23/40 / ص 27.

[24] الأمم المتحدة، المجلس الاقتصادي والاجتماعي، **تقرير فريق الخبراء الحكومي الدولي المفتوح العضوية عن الدراسة الشاملة لمشكلة الجريمة السيبرانية وتدابير التصدي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص**، سنة 2011 ، مرجع سابق ، ص 23.

[25] ويكيبديا الموسوعة الحرة ، https://ar.wikipedia.org/wiki

حساب تدقيق المجموع للتأكد من صحة الأدلة الإلكترونية، وغلق الحسابات المفتوحة على التطبيقات الشبكية، واعتماد آلية الحماية ضد الكتابة على الأدلة.[26]

المطلب الثاني : التحديات القانونية

كما هو معلوم فالشرعية الجنائية تقوم على شقين مهمين هما الشرعية الموضوعية والشرعية الإجرائية ،وكلاهما ضروريين من اجل محاربة الجريمة وفرض القانون .لذلك يجب الوقوف على الإشكالات والتحديات التي لها علاقة بهما، من اجل تحقيق النجاعة والفعالية و بيان ذلك فيمايلي:

أولا : التحديات القانونية الموضوعية :

لقد زاد حجم الجرائم المعلوماتية وتنوعت أساليبها وتعدد اتجاهاتها وتعاظمت خسائرها، حتى صارت مصدر تهديد مباشر للأمن القومي للدول، وأمام هذا النمط الإجرامي الجديد الذي يعتمد على التقنية المتطورة في تحقيق أغراضه، يكون للتشريع الجنائي الموضوعي والإجرائي دورا هاما في الردع والحماية .

ولكن بالرجوع إلى خصائص هذا النمط الجديد من الجرائم ، نجد أن التشريع بصفة عامة في حالته الراهنة لا يبدو كافيا ولا فعالا بالدرجة المطلوبة والفعالة ، سواء في توصيف هذه الجرائم و تحديد أركانها أم في إجراءات متابعتها و مكافحتها، فاغلب النصوص القانونية الجنائية موروثة من القرن الماضي، حيث لم يكن هناك متخصصين أو فقهاء تشريعيين قادرين على التنبؤ بما سيحدث مستقبلا من سلوك إجرامي في حجم الجرائم الإلكترونية.[27]

1- الطبيعة القانونية للفضاء الرقمي ومعاييرها :

الفضاء الالكتروني عبارة عن مجال طبيعي ومادي ، ويرى آخرون انه ذو طابع افتراضي حيث يرونه انه تلك البنية الافتراضية التي تعمل بها المعلومات الالكترونية والتي تتصل عن طريق شبكات الكمبيوتر.كما يعرف انه ذلك المجال الذي يتميز باستخدام الالكترونيات والمجال الكهرومغناطيسي لتخزين و تعديل تغيير البيانات عن طريق النظم المتصلة و المرتبطة بالبنية التحتية الطبيعية .

ويدور الخلاف حول طبيعة الفضاء الالكتروني ما بين طبيعة افتراضية و أخرى مادية .ويحسم هذا الخلاف أن الفضاء الالكتروني له طبيعة مادية و أخرى افتراضية تظهر في كونه مجالا للحرب والقتال، حيث تتحرك عمليات المعلومات التي تشير إلى البيئة التي يمكن من خلالها شن عمليات الهجوم والدفاع والتي تكون متصلة ومستخدمة عبر الشبكات.

---

[26] الأمم المتحدة **تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية**، فيينا مارس2019 ، رقم : UNODC/CCPCJ/EG.4/2019/2 المؤرخ في : 12 April 2019 ، ص 10.

[27] طارق إبراهيم الدسوقي عطية : **الموسوعة الأمنية ، الأمن المعلوماتي والنظام القانوني لحماية المعلوماتية** ، دار الجامعة الجديدة ، الإسكندرية ، دط، 2015، ص 34.

بالتالي فحتى ولو اعتبرنا أن هذا الفضاء يبقى افتراضيا ومتجاوزا للزمان والمكان إلا انه من الناحية العملية يبقى ميدانا للكثير من الصراعات الحقيقة والتي تظهر آثارها الاجتماعية والسياسية والاقتصادية وحتى العسكرية ، حيث أقرت هيئة ا لأركان الأمريكية تعريفا للفضاء الالكتروني من وجهة نظر عسكرية بأنه مجال يتميز بإستخدام الالكترونيات والكهرومغناطيسية وتخزين تأثيرات متحركة أو ساكنة ضد الإشارات (الرادار ، أجهزة الاتصال) و نقاط ربط وشبكات النظام الدفاعي، حيث يتم الوصول إلى الهدف بسرعة الصوت والضوء عند استعمال قدرتها الفضائية الالكترونية "[28]

2-مسألة التجريم وعائق الشرعية:

يعتبر مبدأ شرعية الجريمة والعقوبة مبدأ مهم في حماية المتهمين بأي جريمة كانت، لكنه يمكن أن يكون ثغرة تسمح للمجرمين الإفلات من العقاب، خاصة إذا تعلق الأمر بالجرائم المستحدثة والتي تتطور كل يوم بحيث لا يمكن للتشريعات اللحاق بها ، غير أن تلك السلوكيات والوقائع تبقي بعيدة عن المتابعة في اغلب الدول، مما يستوجب ضرورة الإسراع وتدارك هذا النقص التشريعي في القريب العاجل، رغم أن مرجعيتها تقوم على جرائم شائعة كالنصب والاحتيال والسرقة والتزوير إلا أنها تبقى بعيدة عن المتابعة لانعدام الشرعية القانونية.[29]

كذلك يتطلب التحقيق في الجريمة السيبرانية وملاحقة مرتكبيها بصورة فعالة تجريم أفعال جديدة إذا كانت سلوكيات معينة غير مشمولة أصلا بالتشريعات القائمة. فوجود تشريعات مناسبة ضروري ليس فقط من أجل إجراء تحقيقات وطنية، بل لأنه يمكن أن يؤثر أيضا على التعاون الدولي،فيجب ان يشمل القانون الجنائي الموضوعي الوطني على معظم الأطر الإقليمية الشاملة التي وضعت للتصدي للجريمة السيبرانية من اجل سد الثغرات الموجودة في التشريعات الوطنية[30].

3- الموازنة بين إنفاذ القانون وإحترام المعايير المتعلقة بحقوق الإنسان :

إن مواجهة تهديدات الفضاء السيبراني يستلزم ضرورة تحقيق التوازن بين الحاجة إلى تدابير فعالة في إطار إنفاذ القانون للتصدي للجريمة السيبرانية وحماية حقوق الإنسان الأساسية، وخاصة الحق في الخصوصية. وقيل إن القواعد المتعلقة بالاحتفاظ بالبيانات قد تمثل نهجا عمليا لضمان قدرة مقدمي خدمات الاتصالات على الاضطلاع بدور أكبر في التصدي للجريمة السيبرانية من خلال تعزيز التعاون مع أجهزة إنفاذ القانون، شريطة أن يراعي تنفيذ هذه القوانين الضمانات الإجرائية وإجراءات حماية الخصوصية الواجبة و بالرغم من المجهودات الدولية في هذا المجال نجد أن تحقيق هذا التوازن لا زلا مفقودا بسبب تضارب المصالح و تنوع

---

[28] عادل صادق :**استخدام الإرهاب الالكتروني في الصراع الدولي** ، دار الكتاب الحديث ، القاهرة ، الطبعة الأولى ، 2015.ص 29 .

[29] لموسخ محمد :**تنازع الاختصاص في الجرائم الالكترونية** ، مجلة دفاتر، جامعة قاصدي مرباح ورقلة ، العدد 02 ، سنة 2009م، **ص 25**.

[30] الأمم المتحدة، المجلس الاقتصادي والاجتماعي، **تقرير فريق الخبراء الحكومي الدولي المفتوح العضوية عن الدراسة الشاملة لمشكلة الجريمة السيبرانية وتدابير التصدي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص**، سنة 2011 ، مرجع سابق ، ص 32.

الثقافات بين الشعوب و تعقيدات الفضاء الرقمي مع فرض القوى العظمى سيطرتها على كل المعايير التي تخدم مصالحها.[31]

4-إشكاليات التعاون الدولي :

مع إنعدام الاتفاقيات الدولية في مجال مكافحة الهجوم السيبراني خاصة تلك المتعلقة بتسليم المجرمين ، صارت مسألة التعاون الدولي في مكافحة التهديدات السيبرانية مسألة مهمة جدا في ظل الاختلافات القائمة بين الدول خاصة تلك المتعلقة بحقوق الإنسان .فالاتفاقيات الثنائية المتعلقة بتسليم المجرمين بشكلها التقليدي لم تعد كافية وغير فعالة نظرا للطابع المتطور والمعقد وعبر الوطني للجريمة السيبرانية ، لذلك نجد أن نظام تسليم المتهمين خاصة في الجرائم الإلكترونية السيبرانية لهو الحل الأمثل واللازم اتخاذه في شأن مكافحة الهجوم السيبراني وما يترتب عن تلك الجريمة من خسائر للمؤسسات العامة والخاصة، فما الفائدة من تحديد مرتكب الجريمة وتحديد مكانه دون القدرة على محاكمته ومعاقبته عما اقترفه من جرائم .فالتسليم يعد وسيلة أساسية للحد من الهجوم السيبراني[32].

ويمكن أن يبرز دور المجتمع الدولي في مواجهة تلك الجرائم من خال التعاون الدولي القضائي من خال تبادل المعلومات والوثائق التي تطلبها السلطات القضائية الأجنبية بصدد جريمة من الجرائم وكذا نقل الإجراءات وذلك من خال قيام الدولة بناء على اتفاق باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى، وتفعيل الإنابة القضائية التي تجعل دولة ما تتمكن من الاستفادة من السلطات العامة في دولة أخرى إذا ما حالت الحدود الإقليمية دون نفاذ قانونها تجاه المجرم[33].

لذلك فقد اقترحت بعض الدول الأعضاء أنه نظرا للطابع المتطور والمعقد وعبر الوطني للجريمة السيبرانية، سيكون من السابق لأوانه مناقشة معايير مشتركة في التعاون الدولي .ولذلك، ينبغي للدول الأعضاء أن تسعى إلى إرساء تدابير دولية جديدة لمكافحة الجريمة السيبرانية من خلال النظر في التفاوض على صك قانوني عالمي جديد بشأن الجريمة السيبرانية في إطار الأمم المتحدة.[34]

ونظرا لأهمية الموضوع فهناك عملية تفاوض جارية من أجل اعتماد بروتوكول إضافي ثان لاتفاقية بودابست للجريمة الإلكترونية [35] بهدف توفير قواعد واضحة وإجراءات أكثر فعالية بشأن الأحكام التي تجعل التعاون الدولي أكثر فعالية وسرعة؛ والأحكام التي تتيح التعاون المباشر مع مقدمي الخدمات في ولايات

---

[31] فرانك لا رو : **مرجع سابق** ،ص 15.

[32] شيخه حسني الزهراني : **التعاون الدولي في مواجهة الهجوم السيبراني**، مجلة جامعة الشارقة ، المجلد 17 ، العدد 1 شوال 1441 هـ /2020م الترقيم الدولي المعياري للدوريات 1996-2320 كلية القانون – جامعة الشارقة الشارقة – الإمارات العربية المتحدة ص 24.

[33] شيخه حسني الزهراني: **مرجع سابق** ،ص 27.

[34] الأمم المتحدة **تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية**، فيينا مارس2019 ، رقم : UNODC/CCPCJ/EG.4/2019/2 المؤرخ في : 12 April 2019 ، ص 03.

[35] تعد معاهدة **بودابست لمكافحة جرائم الإنترنت** أولى المعاهدات المتعلقة بتلك الجرائم والتي تمت في العاصمة المجرية بودابست في 23/11/001 ،والتي تبرز التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية،

قضائية أخرى فيما يتعلق بطلبات المعلومات عن المشتركين، وطلبات حفظ البيانات، والطلبات الطارئة والإطار والضمانات القوية للممارسات التي تنطوي على إمكانية الوصول إلى البيانات عبر الحدود، بما في ذلك متطلبات حماية البيانات[36].

ثانيا: التحديات القانونية الإجرائية :

إن القواعد الإجرائية التقليدية تبدو قاصرة إزاء ملاحقة مرتكب الجريمة المعلوماتية مما شكل صعوبات ميدانية في جمع الأدلة وإجراء التحقيقات الجنائية وملاحقة المجرمين بسبب البيئة الرقمية ذات الطبيعة الخاصة والتي تحتاج إلى إجراءات خاصة تتماشى مع متطلبات البيئة الرقمية، كل هذه التعقيدات تفرض على المشرع تطوير أساليب التحقيق والكشف عن الجريمة و تحديد الأساليب الإجرائية في مجال الجريمة المعلوماتية .[37]

1-تنازع الاختصاص القضائي :

إن اختلاف التشريعات والنظم القانونية يؤدي إلى تنازع في الاختصاص القضائي بين الدول مما يعوق التعاون الدولي، فتنتج عنه تحديات ناشئة عن النزاعات بشأن الولاية القضائية المعنية بالإنفاذ، وخصوصا، على سبيل المثال، في الحالات التي قد يكون فيها لمقدم الخدمة مقر في إحدى الولايات القضائية، ويكون المتحكم في البيانات موجودا في بلد آخر أو تكون البيانات مخزنة في ولاية قضائية أخرى أو في ولايات قضائية متعددة .و مع ظهور الحوسبة السحابية[38] تثار تحديات عملية وقانونية إضافية أمام التحقيقات الجنائية و إذا هناك مساعدات قضائية دولية إلا أن آلية تنفيذها يتم عن طريق دبلوماسي يتميز بالبطء والتعقيد الذي يتعارض مع طبيعة الجريمة السيبرانية والإنترنت الذي يتميز بالسرعة و اللازمانية .[39]

كذلك فإن جود شرط التجريم المزدوج الواجب توافره لا نفاذ تسليم المتهمين يعد عائقا يحول دون إنفاذه لأنه قد يجرم فعل في دولة دون الأخرى مما يترتب معه عدم إمكانية تسليم المجرم[40].

وما زاد الأمر تعقيدا أن هذه الجرائم المستحدثة سريعة الحدوث وفي عديد من الدول (الجريمة العابرة للحدود)، وما تطرحه هذه الجرائم من مشاكل قانونية خصوصا في مجال الاختصاص من حيث الجهات المخول لها متابعة

---

[36] تقرير خبراء الأمم المتحدة 2019 : **مرجع سابق** ص 12.

[37] طارق إبراهيم الدسوقي عطية : **الموسوعة الأمنية ، الأمن المعلوماتي والنظام القانوني لحماية المعلوماتية** ، دار الجامعة الجديدة ، الإسكندرية ، دط، 2015، ص 331.

[38] **الحوسبة السحابية** Cloud computing هي مصطلح يشير إلى المصادر والأنظمة الحاسوبية المتوافرة تحت الطلب عبر الشبكة والتي تستطيع توفير عدد من الخدمات الحاسوبية المتكاملة دون التقيد بالموارد المحلية بهدف التيسير على المستخدم، وتشمل تلك الموارد مساحة لتخزين البيانات والنسخ الاحتياطي والمزامنة الذاتية، كما تشمل قدرات معالجة برمجية وجدولة للمهام ودفع البريد الإلكتروني والطباعة عن بعد، ويستطيع المستخدم عند اتصاله بالشبكة التحكم في هذه الموارد عن طريق واجهة برمجية سهلة تسهل وتتجاهل الكثير من التفاصيل والعمليات الداخلية.

[39] الأمم المتحدة، **تقرير اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية**، فيينا مارس 2019 ، رقم UNODC/CCPCJ/EG.4/2019/2 ، ص 13.

[40] جهينة حسين البهلواني : **مرجع سابق** ، ص 28

المجرم، أو من خلال المحكمة المختصة فقد ترتكب الجريمة في دولة و تكون آثارها في دولة أخرى، وقد يكون الجاني يحمل جنسية دولة أخرى وتكون أدلة الجريمة موجودة في دولة أخرى وخارج النطاق الإقليمي لجهة التحقيق، فكيف يتم جمع الأدلة وضبطها وما هو القانون الواجب التطبيق، و هذا ما يحتم علينا ضرورة البحث عن الاختصاص في جرائم المعلوماتية العابرة للحدود على المستوى الداخلي، وكذا على المستوى الدولي من خلال التعاون الاتفاقي والقضائي للحد من هذه الظاهرة الإجرامية الخطيرة .[41]

2- مسألة الأدلة الإلكترونية وتعقيداتها :

إن القيمة القانونية للدليل الرقمي في مجال الإثبات الجنائي تتمثل في مشروعية الدليل الرقمي وحجيته.فطبقا لمبدأ الشرعية الإجرائية فلا يكون الدليل مقبولا في عملية الإثبات إلا إذا كان مشروعا،بأن تم البحث عنه والحصول عليه وفقا لطرق مشروعة، وعلى هذا الأساس فإن إجراءات جمع الأدلة الرقمية المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة ، ومشروعية الدليل تتطلب صدقه في مضمونه، وأن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة تدل على الأمانة والنزاهة من حيث طرق الحصول عليه، وهو ما يرتب عدم القبول بدليل رقمي تم الحصول عليه من إجراء التسرب جرى القيام به دون مراعاة الشروط الشكلية والموضوعية للإذن بمباشرة هذا الإجراء، أو كان الدليل متحصلا عليه عن طريق إكراه المتهم من أجل فك شفرة للدخول إلى النظم المعلوماتية أو كلمة السر اللازمة للدخول إلى ملفات المعلومات المختزنة، أو القيام بإجراء لتنصت أو المراقبة الإلكترونية عن بعد دون سند قانوني[42].

3- صلاحيات الإجراءات والتحقيق :

تحتاج هيئات إنفاذ القانون، من أجل إجراء تحقيقات فعالة، إلى إجراءات تحقيق تمكنها من اتخاذ التدابير اللازمة لتحديد هوية الجناة وجمع الأدلة المطلوبة للدعوى الجنائية .ويمكن أن تكون هذه التدابير هي نفسها التدابير المستخدمة في التحقيقات التقليدية غير المرتبطة بالجريمة السيبرانية. ولكن، بالنظر إلى أنه ليس من الضروري أن يكون الجاني حاضرا في مسرح الجريمة أو حتى على مقربة منه، فإنه من المرجح أن تجرى التحقيقات في الجرائم السيبرانية بطريقة مختلفة عن التحقيقات التقليدية.

إضافة إلى الأحكام المتعلقة بالجرائم السيبرانية الرئيسية، تتضمن أيضا معظم الأطر الإقليمية الشاملة التي وضعت للتصدي للجريمة السيبرانية مجموعة من الأحكام المصممة خصيصا لتيسير التحقيقات في الجرائم السيبرانية. وتتضمن الأحكام القياسية إجراءات محددة للتفتيش والضبط، والتعجيل في صون البيانات الحاسوبية، والكشف عن البيانات المخزونة، واعتراض بيانات المحتويات، وجمع البيانات عن حركة المعلومات،

---

[41] لموسخ محمد : **مرجع سابق** ، ص 12.

[42] آمال فكيري : **إشكالات الإثبات والإختصاص في جرائم تكنلوجيا الإعلام والإتصال العابرة للحدود** ، مجلة العلوم القانونية و السياسية، جامعة الوادي ، عدد17 ، جانفي 2018م. ص 633.

لذلك تواجه هيئات إنفاذ القانون في المرحلة الحالية تكنولوجيات مطورة حديثا ذات تأثير سلبي على أساليب التحقيق التقليدية. والكثير من تلك التحديات لم يتم التصدي لها بعد[43].

4- السيادة الإقليمة والسيادة السيبرانية وتضارب المصالح :

من تداعيات وآثار الفضاء الرقمي بكل تعقيداته نجد ظهر مفهم جديد لسيادة الدولة وهو السيادة السيبرانية ، ويعنى خضوع الفضاء السيبراني لمصالح وقيم الدولة، أي قدرة الدول في التحكم في مجالها السيبراني بما يضمن أنه يتبع نفس القواعد والقيم والاعتبارات من بقية المجتمع ، فهي عبارة تستخدم في مجال حوكمة الانترنت لوصف رغبة الحكومات في ممارسة السيطرة على الانترنت داخل الحدود الوطنية التابعة لهذه الحكومات ، لكن في المقابل صارت السيادة الإقليمية مفتوحة ومباحة بفعل التقدم التكنولوجي وصارت مهددة من طرف الدول والأفراد على حد سواء.

فضلا عما سبق نجد أن هذا المفهوم ليس محل إتفاق بين الدول بسبب التفاوت في إمتلاك التكنولوجيا الرقمية، فعلى سبيل المثال ترى الولايات المتحدة الأمريكية أن الفضاء السيبراني هو من المشاعات العالمية، وبالتالي لا مجال للحديث عن السيادة في هذا الفضاء ، في المقابل نجد أن الكثير من الدول كالصين و ألمانيا ترى أنه يجب وضع حدود و معالم في هذا الفضاء للتقليل من أخطاره وتهديداته.[44]

5- طلب الإنابة القضائية :

تعتبر طلب الإنابة القضائية من أهم الوسائل الناجعة في مكافحة الجرائم السيبرانية ، وهنا تظهر أهمية التعاون الدولي في التحقيق في الجرائم السيبرانية وملاحقة مرتكبيها قضائيا عبر الحدود .فعدد طلبات المساعدة القانونية المتبادلة للحصول على أدلة إثبات إلكترونية وحفظها يتزايد بسرعة، لأن طرائق التعاون التقليدية، وبوجه خاص الإجراءات المتعلقة بتبادل المساعدة تستغرق وقت طويلا، لا تسهل الوصول السريع إلى البيانات .بالتالي فالمساعدة القانونية المتبادلة لا تزال أداة بالغة الأهمية لتبادل البيانات عبر الحدود، لذلك فلا بد لا بد للقوانين الإجرائية المحلية من أن تواكب التقدم التكنولوجي وأن تضمن تزويد أجهزة إنفاذ القانون بالموارد الكافية لمكافحة جرائم الإنترنت .

---

[43] الأمم المتحدة، المجلس الاقتصادي والاجتماعي، **تقرير فريق الخبراء الحكومي الدولي المفتوح العضوية عن الدراسة الشاملة لمشكلة الجريمة السيبرانية وتدابير التصدي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص**، رقم E/CN.15/2011/ 19 ، الدورة العشرون أفريل 2011م، ص 26.

[44] بيرم فاطمة : **السيادة الوطنية السيبرانية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجا**، المجلة الجزائرية للأمن الإنساني ، جامعة الحاج لخضر باتنة ، العدد 1 ،جانفي 2020م ، ص 633.

وينبغي صوغ القوانين ذات الصلة على نحو يراعي المفاهيم التقنية المطبقة ويفي بالاحتياجات العملية للمحققين في الجرائم السيبرانية ويتسق مع ضمانات اتباع الأصول القانونية الواجبة ويحقق المصالح المتعلقة بالخصوصية ويضمن الحريات المدنية وحقوق الإنسان ويمتثل لمبدأي التناسب والولاية الاحتياطية ويكفل الإشراف القضائي .[45]

الخاتمة :

في ختام هذا البحث أكون قد توصلت إلى مجموعة من النتائج المهمة كمايلي :

- من الناحية المفاهمية والإصطلاحية نجد أن هناك تقارب المفاهيم المتعلقة بالفضاء السيبراني وتعقيداتها ، بسبب التطور السريع الذي يشهده العالم في مجال تكنولوجية الإعلام و الاتصال، الأمر الذي صعب من مهمة المشرعين وجهات نفاذ القانون الساهرين على تحقيق الأمن في الفضاء السيبراني.
- ظهور مصطلحات ومفاهيم جديدة لمفهوم " سيادة الدول " في القانون الدولي ، بعد ان تحول الفضاء السيبراني إلى ساحة حروب و صراع و تهديد لأمن الدول و انتهاك سيادتها ، بشكل لا يقل خطورة عن الحروب الكلاسيكية وآثارها المدمرة.
- وبالرجوع إلى مختلف التهديدات السيبرانية ، توصلت إلى وجود العديد من التحديات التي تحول دون تحقيق النجاعة والفعالية في محاربتها، منها ما هو تقني وفني ومنها ما هو قانوني بشقيه الموضوعي والإجرائي.
- من العراقيل التي تحول دون تنظيم الفضاء السيبراني والحد من التهديدات التي تطوله هو تضارب المصالح الدولية وبروز الازدواجية في معايير حقوق الإنسان في الفضاء الرقمي، عطل الكثير من الجهود الدولية خاصة تلك الصادرة عن هيئة الأمم المتحدة .

لذلك لا مناص من تكثيف الجهود الولية و نبذ الخلافات الإيديولوجية وتضارب المصالح، من اجل سلم سيبراني عالمي يحفظ حقوق الجميع أفراد ومنظمات ودول.

---

[45] الأمم المتحدة، **تقرير اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية**، فيينا مارس 2019 ، رقم UNODC/CCPCJ/EG.4/2019/2 ص 7.

قائمة المراجع و المصادر

أولا : المواثيق الدولية :

1- **مجلس حقوق الإنسان الدورة السابعة عشرة** البند 3 من جدول الأعمال **تعزيز وحماية جميع حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية** ،تقرير رقم A/HRC/17/27 للمقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، فرانك لا رو* **لسنة 2011م** .

2- الأمم المتحدة **تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية**، فيينا مارس2019 ، رقم :UNODC/CCPCJ/EG.4/2019/2 المؤرخ في : 12 April 2019 .

3- الأمم المتحدة، المجلس الاقتصادي والاجتماعي، **تقرير فريق الخبراء الحكومي الدولي المفتوح العضوية عن الدراسة الشاملة لمشكلة الجريمة السيبرانية وتدابير التصدي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص**، رقم E/CN.15/2011/ 19 ، الدورة العشرون أفريل 2011.

4- الاجتماع السادس لفريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية ، فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية فيينا، أبريل، تحت رقم 2020 ، UNODC/CCPCJ/EG.4/2020/1 .

5- فرانك لا رو : **تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير** * Distr الجمعية العامة 17 April 2013 ، Aالمتحدة الأمم40/23/HRC /

ثانيا : المؤلفات:

6- طارق إبراهيم الدسوقي عطية : **الموسوعة الأمنية ، الأمن المعلوماتي والنظام القانوني لحماية المعلوماتية ،** دار الجامعة الجديدة ، الإسكندرية ، دط، 2015، ص 331.

7- عادل صادق :**استخدام الارهاب الالكتروني في الصراع الدولي** ، دار الكتاب الحديث ، القاهرة ، الطبعة الأولى

8- Cyber Power By Joseph S. Nye, Jr. 1Joseph S.Nye JR , Cyber Power, Harvard Kennedy School, 2010،

ثالثا : المقالات

9- بارة سميرة : **الأمن السيبراني (cyper Security) في الجزائر:السياسات و المؤسسات** ، المجلة الجزائرية للأمن الإنساني، جامعة الحاج لخضر،باتنة ،العدد الرابع : جويلية 2017 ، ص 257.

10- بيرم فاطمة : **السيادة الوطنية السيبرانية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجا،** المجلة الجزائرية للأمن الإنساني ، جامعة الحاج لخضر باتنة ، العدد 1 ،جانفي 2020م ، ص 633.

11- حمد طوالبية : **أيديولوجية الفضاء الرقمي دراسة يف الخلفيات المرجعية** ، الاكاديمية للدراسات الاجتماعية و الإنسانية ، الأكاديمية للدراسات الاجتماعية والإنسانية ج/قسم العلوم االجتماعية العدد 21 – جانفي 2019 .

12- رغدة البهي : الأمن السيبراني في 2020: بين الفرص والتحديات المركز المصري للفكر و الدراسات الاستراتيجية ، مقال منشور بتاريخ January 11, 2021 بموقع : https://www.ecsstudies.com/13106/ تاريخ الدخول 25 مارس 2021.

13- نورة شلوش: **القرصنة الالكترونية في الفضاء السيبراني ا ربي التهديد المتصاعد لأمن الدول** ، مجلة بابل للدراسات الحضارية والتاريخية ، جامعة بابل ، العدد 02،

14- شيخه حسني الزهراني : **التعاون الدولي في مواجهة الهجوم السيبراني،** مجلة جامعة الشارقة ، المجلد 17 ، العدد 1 شوال 1441 هـ /2020م الترقيم الدولي المعياري للدوريات 1996-2320 كلية القانون – جامعة الشارقة – الإمارات العربية المتحدة

15- محمد الطاهر : **الحريات الرقمية، المفاهيم الأساسية،** مؤسسة حرية الفكر والتعبير، القاهرة، الطبعة الأولى،السنة 2012م.

16- محمد طوالبية: **إيديولوجية الفضاء الرقمي،** دراسة في الخلفيات المرجعية الأكاديمية للدراسات الاجتماعية والإنسانية، قسم العلوم الاجتماعية العدد 21 ، جانفي 2019 .

17- **لموسخ محمد :تنازع الاختصاص في الجرائم الالكترونية ، مجلة دفاتر، جامعة قاصدي مرباح ورقلة ، العدد 02 ، سنة 2009م،**

18- **دوريات – قضايا إستراتيجية ، تحديات القوانين: الفضاء الافتراضي والقانون الدولي : المركز العربي لأبحاث الفضاء الإلكتروني** السبت،25 نوفمبر 2017 - 02:13

19- آمال فكيري : **إشكالات الإثبات والاختصاص في جرائم تكنولوجيا الإعلام والإتصال العابرة للحدود** ، مجلة العلوم القانونية و السياسية، جامعة الوادي ، عدد17 ، جانفي 2018م.

المواقع الإلكترونية:

20- قاموس أكسفورد : على موقع الإنترنت
https://www.oxfordlearnersdictionaries.com/definition/english/cyber

21- موقع الوينار : https://attaa.sa/library/view/868

22- موقع العطاء الرقمي ، وزارة الإتصالات و تقنية المعلومات ، المملكة العربية السعودية ،
https://attaa.sa/library/view/868

23- الموسوعة السياسية poltical encylopedia، https://political-encyclopedia.org/dictionary

24- ويكيبديا الموسوعة الحرة ، https://ar.wikipedia.org/wiki