

تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية



Cybercrime and legal mechanisms to address it In light of the geopolitical shifts

اسم الباحث: أ.سميرة بيطام

جهة الإنتساب: كلية الحقوق بن يوسف بن خدة - جامعة الجزائر

Author's name: Samira Bitam

Affiliation: Faculty of Law Ben Youssef Ben Khadda - University of Algiers

E-mail: kimatatae@gmail.com

work type: research paper

نوع العمل العلمي: بحث

discipline: public law, criminal law

مجال العمل: قانون عام - قانون جنائي

Doi: <https://doi.org/10.61279/0mnksv66>

Issue No. & date: Issue 22 - Oct. 2023 رقم العدد وتاريخه: العدد الثاني والعشرين - تشرين الاول - ٢٠٢٣

Received: 10/5/2023

تاريخ الاستلام: ٢٠٢٣/٥/١٠

Acceptance date: 10/8/2023

تاريخ القبول: ٢٠٢٣/٨/١٠

Published Online: 25 Oct 2023

تاريخ النشر: ٢٥ تشرين الاول ٢٠٢٣

© Printing rights are reserved to the Journal
of the College of Law and Political Science at
Aliraqia University

© حقوق الطباعة محفوظة لدى مجلة كلية القانون
والعلوم السياسية في الجامعة العراقية

Intellectual property rights are reserved to the
author

حقوق الملكية الفكرية محفوظة للمؤلف
حقوق النشر محفوظة للناشر (كلية القانون والعلوم
السياسية - الجامعة العراقية)

Copyright reserved to the publisher (College of
Law and Political Science - Aliraqia University)

نسب المصنّف - غير تجاري - منع الاشتقاق ٤,٠ دولي
للمزيد من المعلومات يرجى مراجعة الحقوق والترخيص

Attribution – NonCommercial - NoDerivs 4.0

International

For more information, please review the rights
and license



CC BY-NC-ND 4.0 DEED



تاريخ التقديم ٢٠٢٣/٥/١٠ تاريخ القبول ٢٠٢٣/٨/١٠
تاريخ النشر ٢٠٢٣/١٠/٢٥

تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية

Cybercrime and legal mechanisms to address it
In light of the geopolitical shifts

أ.سميرة بيطام

باحثة أكاديمية في القانون الجنائي (الحمض النووي والجريمة)

كلية الحقوق بن يوسف بن خدة - جامعة الجزائر

Samira Bitam

Academic Researcher in Criminal Law (DNA and Crime)

Faculty of Law Ben Youssef Ben Khadda - University of Algiers

kimatatae@gmail.com



المستخلص:

في السنوات الأخيرة تشهد الدول تحولات جيوسياسية كبيرة ومؤثرة، بدأت بتغيير توجه النظام العالمي المتسم بأحادية القطب، ما جعل الدول تتأهب لأن تحمي نفسها واقتصادها وحقوق مواطنيها ضد ما يسمى بالجريمة السيبرانية والتي تُعتبر حرباً جديدة الأسلوب والنتائج ان هي قُورنت بالحرب الكلاسيكية والبيولوجية .

فقد أفرزت التحولات التكنولوجية والتقنية الحديثة تطورات في استخدام وسائل التواصل وكذا المنصات الرقمية من أجل تسهيل عملية الوصول للآخر، هذا الوصول الذي يكون في بعض الأحيان غير مشروع نظراً لما يسببه من تهديدات أمنية سواء على الشخص الطبيعي أو المعنوي، ما جعل الجريمة المعاصرة تأخذ لها شكلاً ومنحى جديداً ذو طابع معقد ومتعدد المجالات بواسطة الفضاء الافتراضي.

وهذا ما دفع المؤسسات الأمنية لجميع الدول ان تكون في حالة استنفار في مجال الرقمنة الأمنية حماية للمعلومات وصونا للحقوق سواء الفكرية أو المالية أو الإقليمية في شقها الأمني، ما جعل نوع التدابير المتخذة مغاير تماماً للجريمة العادية سواء (سرقة أو قتل أو إرهاب حقيقي) لأن مسرح الجريمة اليوم لم يبق في شكله التقليدي الذي يستلزم تطويقه والحفاظ عليه لتحريز الأدلة منه، بل تغير الى مسرح جريمة افتراضي يستلزم آليات جديدة لاكتشاف هذا النوع من الاجرام ووضع الخطط البديلة للتصدي له .

الكلمات المفتاحية: الجرائم المتصلة، المعلوماتية والجرائم، جرائم المساس.

Abstract

In recent years, countries have witnessed major and influential geopolitical shifts, which began to change the orientation of the unipolar world system, which made countries prepare to protect themselves, their economy, and the rights of their citizens against the so-called cybercrime, which is considered a new war of method and results if it is compared to classical and biological warfare.

Modern technological and technical transformations have resulted in developments in the use of communication means as well as digital platforms in order to facilitate the process of reaching the other, this access, which is sometimes illegal due to the security threats it causes, whether on the natural or legal person, is what made contemporary crime take its toll. A new shape and direction with a complex and multi-field nature mediated by the virtual space.

This is what made the security institutions of all countries in a state of alert in the field of security digitization to protect information and safeguard rights, whether

تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية **الملف القانوني**

intellectual, financial or regional in the security aspect, which made the type of measures taken completely different from ordinary crime, whether (theft, murder or real terrorism) because the crime scene today It did not remain in its traditional form, which requires enclosing and preserving it in order to obtain evidence from it, but rather changed to a virtual crime scene that requires new mechanisms to detect this type of crime and develop alternative plans to address it.

key words: Related crimes, Informatics and crimes, Infringement crimes

مقدمة :

لقد تحول العالم في الألفية الأخيرة بشكل سريع وملحوظ فيما يخص جوانب استخدام التقنية وطريقة التعامل مع الرهانات المفروضة بسبب عوامل وظروف ، منها الحرب وكذا النقائص التي تعانيها دول العالم من مصادر للطاقة وموارد غذائية ومائية، وقد تكون هذه النقائص بمثابة الغنائم لدى من ينتهزون الفرص من أجل الحاق الأذى بالآخر والتمكن من ثرواته ومصادر العيش لديه ، وهو ما يمثل فكرة الاستعمار الجديد التي فتحت أبوابها أمام الجريمة السيبرانية في ثوبها المعاصر، ولا يخفى على أحد أن جناة هذه الجريمة هم محترفون ومتمكنون من التقنية الحديثة ويتلونون في أساليب الاختراق سواء لحسابات أو البنى التحتية لمؤسسات الدول ، وبالتالي تعد الجريمة السيبرانية في مفهومها المعاصر بمثابة صفقات مربحة لمن يجيد الاحترافية فيها .

وعلى اختلاف التسمية من جريمة سيبرانية الى الكترونية يكون مسرحها واحد والاختلاف في التسمية فقط، ففي ظل التحدي الرقمي والتكنولوجي سعت التشريعات و محاولات أهل التخصص في علم الاجرام لأن يضعوا مفهوما للجريمة السيبرانية بما يتوافق وطرق ارتكابها والمجال الذي تطبق فيه هذه الجريمة خطط الاعتداء على الآخر، ومن هنا تبدو أهمية هذا الموضوع في ضرورة البحث عن منبع هذه الجريمة وكيف تمكن مرتكبوها من اقتفافها لأجل الإطاحة بسياسات دول وبرامج حكومية وكذا برامج استثمارية عن طريق البنوك ناهيك عن جر الشباب الى بؤر الافلاس والانحلال الخلقي.

المبحث الأول

مفهوم الجريمة السيبرانية ومجالاتها

في الحقيقة لو تأملنا نجد بأن مصطلح الجرائم السيبرانية (Crime Cyber) مصطلح غير عربي، لكنه هو المتداول والمستخدم حديثا في وقتنا الحالي في هيئة الاتصالات وتقنية المعلومات وكذلك المؤتمرات والندوات كملتقى الجرائم السيبرانية والأدلة الرقمية الذي نظّمته جامعة الأمير نايف العربية للعلوم الأمنية في مدينة الرياض عام ٢٠١٣.

فالجريمة السيبرانية أي (الالكترونية) شكل متطور من أشكال الجريمة عبر الوطنية، وتزايد ضلوع جماعات الجريمة المنظمة يزيد من تفاقم الطابع المعقد لهذه الجريمة التي تحدث في مجال الفضاء الالكتروني الذي لا حدود له، ويمكن لمركبي الجرائم السيبرانية وضحاياهم أن يتواجدوا في مناطق مختلفة، كما يمكن أن تتمدد آثار الجريمة عبر المجتمعات في جميع أنحاء العالم، مما يبرز الحاجة الى وضع استجابة عاجلة وديناميكية ودولية^١.

المطلب الأول: خصائص الجريمة السيبرانية وآليات مكافحتها

يمكن اجمال هذه الخصائص في عدة نقاط^٢:

أ- جرائم تتم باستخدام الحاسب الآلي كأداة لارتكاب الجريمة، وتستخدم شبكة الأنترنت كوسيلة لذلك (هروال ٢٠١٣-٢٠١٤، ص ٣٧).

ب- جرائم لا يتم في أغلب الأحيان التبليغ عنها، خاصة اذا تعلق الأمر بالمؤسسات والشركات التجارية، تجنبا للإساءة للسمعة أو اهتزاز ثقة العملاء (الأسدي، ٢٠١٥، ص ٢٥).

ج- جرائم صعبة الاكتشاف لعدم تركها لآثار مادية يمكن من خلالها حل القضية ويطلق على هذه الآثار المعلوماتية الرقمية.

د- جرائم غامضة لصعوبة اثباتها وذلك بسبب غياب الدليل المرئي ولأن أغلب البيانات عبارة عن رموز لا يمكن قراءتها.

هـ- جرائم عابرة للحدود الوطنية تلحق أضرارا جسيمة تمس عدة أقاليم.

و- جرائم تستدعي المام مرتكبيها بالمعرفة التقنية والخبرة الفائقة في مجال الحاسب الألي.

ي- جرائم لا تمتاز بالعنف، لا يستخدم مرتكبوها القوة الجسدية أو العضلية للقيام بالجريمة

(١) روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الالكترونية الشاملة المتعددة التخصصات، العدد ٢٤، شهر ماي، ٢٠٢٠، ص ٥.

(٢) الجريمة السيبرانية، مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة للشرق الأوسط وشمال افريقيا، رابط المقال: <https://www.unodc.org/romena/ar/cybercrime.html/14:59/2023/06/10>.

(٣) مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة اليزا للبحوث والدراسات، المجلد ٦، العدد ٢، الجزائر، ٢٠٢١، ص ١١٤.

أولاً: التعاون الدولي للوقاية من الجريمة السيبرانية

لقد أوصت بعض الدول بأن الانضمام الى اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية من شأنه تعزيز التعاون الدولي واتساق القوانين المتعلقة بالجريمة السيبرانية، في حين أن بعض الدول الأخرى أوصت بأنه يمكن تعزيز مواثمة التشريعات من خلال وضع أحكام قانونية نموذجية على مستوى الأمم المتحدة^٤.

كما طلبت الجمعية العامة في قرارها ٢٣٠/٦٥ الى لجنة منع الجريمة والعدالة الجنائية أن تنشئ وفقاً للفقرة ٢٢ من اعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية: نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير، فريق خبراء حكومي دولي مفتوح العضوية من أجل اجراء دراسة شاملة لمشكلة الجريمة السيبرانية وللتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، بما في ذلك تبادل المعلومات عن التشريعات الوطنية وأفضل الممارسات والمساعدة الفنية والتعاون الدولي، بغية دراسة الاختيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني و الدولي^٥. وهناك استنتاجات رئيسية وخيارات، من خلال اعداد مشروع دراسة الجريمة السيبرانية تتعلق بقضايا^٦ منها:

١. تأثير عدم اتساق الإجراءات على الصعيد الدولي وتنوع القوانين المحلية المتعلقة بالجريمة السيبرانية على التعاون الدولي.
٢. الاعتماد على الوسائل التقليدية للتعاون الدولي الرسمي في المسائل الجنائية التي تنطوي على جرائم الأنترنت والأدلة السيبرانية لجميع الجرائم.
٣. دور موقع الأدلة.
٤. تنسيق الأطر القانونية الوطنية.
٥. سلطات انفاذ القانون وقدرات العدالة الجنائية.
٦. أنشطة منع الجريمة السيبرانية.

ثانياً: التشريعات والأطر الإجرائية

تؤدي التدابير القانونية دوراً رئيسياً في منع الجريمة السيبرانية ومكافحتها، وهذه التدابير ضرورية في جميع المجالات، بما في ذلك التجريم والصلاحيات الإجرائية والولاية القضائية

(٤) دراسة شاملة عن الجريمة السيبرانية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فبراير ٢٠١٣، ص XVI.

(٥) مرفق قرار الجمعية العامة ٢٣٠/٦٥.

(٦) دراسة شاملة عن الجريمة السيبرانية، المرجع السابق، ص XVI.

والتعاون الدولي، ومسؤولية مقدمي خدمات الأنترنت ، وعلى الصعيد الوطني كثيرا ما تتعلق قوانين الجريمة السيبرانية القائمة والجديدة، (أو المخطط لها) على حد سواء بالتجريم ، مما يدل على التركيز بصفة رئيسية على تجريم أفعال متخصصة تغطي الجريمة السيبرانية الأساسية^٧.

ونشيد بالتذكير في هذا السياق الى أن الولايات المتحدة الأمريكية هي ثاني دولة وضعت قانون لمكافحة الاجرام السيبراني وتم تقديم هذا القانون من قبل السيناتور Abi Ribicoff وفتت المصادقة عليه باسم «أنظمة الكمبيوتر الفيدرالية» ضمن قانون الحماية لعام ١٩٧٧ ، من خلال أحداث معزولة تم ادخال الكمبيوتر في الطب الشرعي والطب الشرعي الرقمي وكلاهما يعتبر علم وفن ، وقد كان روبرت موريس جونيور هو أول من قام بمحاكمة مجرم الكتروني في ٢٦ يوليو ١٩٨٩ بموجب قانون الاحتيال وإساءة استخدام الكمبيوتر^٨.

ومنه تواترت الإجراءات القانونية بشأن مكافحة الجريمة السيبرانية، اذا يتم تقديم تقرير حديث من جمعية الإنترنت فيها إحصاءات واتجاهات رئيسية جديدة بالاهتمام منها:

١. هناك ٣ مليارات مستخدم للإنترنت في مايو ٢٠١٥.

٢. سيصل انتشار الإنترنت عبر الهاتف المحمول إلى ٧١٪ سنة ٢٠١٩.

٣. قامت ١٩٢ دولة بتنفيذ قامت ١٩٢ دولة بتنفيذ 3G Mobile للشبكات.

٤. في الوقت الحاضر يتجاوز العدد الحالي للتطبيقات ١ مليون تم تنزيلها أكثر من ١٠٠ مرة.

ومن هذا البيانات شاع مصطلح الهاكر ، هذا المسمى الذي تغير على مدار عقود ماضية ، بحيث صار يُنظر لأنشطة المجموعة التي تخترق الحواسيب على أنها شريرة تعمل تحت الأرض لحدوث ضرر ضد نظم معلومات المجتمع ، ومن يمارسون الاختراق هم قرصنة ، يمكن أن تكون دوافعهم لمجرد الاستمتاع مثل سيناريو Kiddies لتشويه المواقع والوصول الى كلمات السر^٩.

وعلى اختلاف الغاية من الهجمات الالكترونية ، يتم تصنيف الهجمات والجرائم الالكترونية بناء على ثقافة الهاكرز الفرعية والمخاطر والتأثير والتكنولوجيا وعوامل بشرية أخرى، مع وضع هذه المبادئ في الاعتبار بحيث يجب أن تكون الجهود موجهة نحو الصون من ثلوث الأمن السيبراني الذي يحيط السرية والنزاهة^{١٠}.

المطلب الثاني: أنواع الجرائم السيبرانية

(٧) دراسة شاملة عن الجريمة السيبرانية، المرجع السابق، ص XXIII.

(8) REGNER SABILLON, JEIMY CANO , VICTOR CAVALLER , JORDI SERRA, Cybercrime and Cybercriminals: A Comprehensive Study , R. Sabillon et. al / International Journal of Computer Networks and Communications Security, 6) 4), June 2016 ,p 165.

(9) Ibid , p166.

(10) Ibid , p 168.

ينص مشروع اعداد إرشادات اليسكوا للتشريعات السيبرانية على أن تؤخذ بعين الاعتبار الخبرات الدولية والإقليمية المتراكمة مع تركيز خاص على توجهات الاتحاد الأوروبي في هذا المجال لأجل صياغة الارشاد الخاص بالجرائم السيبرانية، ومنها على التنوع^{١١} :

١- جرائم التعدي على البيانات المعلوماتية:

شملت الجرائم التي يكون موضوعها البيانات المعلوماتية أي التي تقع على بيانات معلوماتية، وهي جرائم التعرض للبيانات المعلوماتية وجرائم اعتراض بيانات معلوماتية.

٢- جرائم التعدي على الأنظمة المعلوماتية:

وتتناول جرائم الولوج غير المشروع الى نظام معلوماتي أو المكوث فيه وجرائم الولوج غير المشروع الى نظام معلوماتي أو المكوث فيه مع التعرض للبيانات المعلوماتية وجرائم إعاقة عمل نظام معلوماتي.

٣- إساءة استعمال الأجهزة أو البرامج المعلوماتية :

تتناول إساءة استعمال الأجهزة او البرامج المعلوماتية وجرائم كل من قدم او انتج أو وزع او حاز غرض الاستخدام جهازا أو برنامجا معلوماتيا أو أية بيانات معلوماتية معدة او كلمات سر أو كودات دخول، وذلك بغرض اقرار أي من الجرائم المنصوص عليها سابقا.

٤- الجرائم على الأموال :

تشمل جرائم الاحتيال أو الغش بوسيلة معلوماتية وجرم التزوير المعلوماتي وجرم الاختلاس أو سرقة أموال بوسيلة معلوماتية وجرم أعمال التسويق والترويج غير المرغوب فيها وجرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي والاستخدام غير المشروع لها وجرم الاطلاع على معلومات سرية أو حساسة أو افشائها.

٥- جرائم الاستغلال الجنسي للقاصرين:

وهي الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية ، وتشمل الرسوم أو الصور أو الكتابات أو الأفلام أو الإشارات أو أية أعمال اباحية يشارك فيها قاصرون أو تتعلق باستغلال القاصرين في المواد الإباحية، وتشمل أيضا انتاج مواد اباحية للقاصرين بقصد بثها بواسطة نظام معلوماتي.

٦- جرائم التعدي على الملكية الفكرية للأعمال الرقمية:

تشمل الجرائم التالية: جرم وضع اسم مختلس على عمل، وجرم تقليد امضاء المؤلف أو ختمه وجرم تقليد عمل رقمي أو قرصنة البرمجيات وجرم بيع أو عرض عمل مقلد أو وضعه في التداول ، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة.

(١١) الجرائم السيبرانية، الارشاد الخامس، رابط الورقة البحثية :

٧-الجرائم التي تمس المعلومات الشخصية:

تشمل الأفعال الاجرامية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح أو ترخيص مسبق يتيح القيام بالمعالجة وافشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليه.

الى جانب أنواع أخرى من الجريمة السيبرانية، وهناك من يشير الى أنواعها بحسب قصد الجاني فيصنفها الى:عمدية وغير عمدية،وبالنظر الى وقت الجريمة الى : متلبس بها وغير متلبس بها،وبالنظر الى جسامتها : جسيمة وغير جسيمة ، وبالنظر الى مصدرها: وطنية في حال أن منصات الهجوم أو القائمين عليها داخل البلد المستهدف و-عالمية- في حال أن منصات الهجوم أو القائمين عليها خارج البلد المستهدف^{١٢}.

(١٢) عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية: دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد ٩، العدد ٣، جامعة تامراغست، الجزائر، ٢٠٢٠، ص ١٥٩.

المبحث الثاني

مدى تأثر الجريمة السيبرانية بالتحويلات الجيوسياسية

قدم الجغرافي الفرنسي «Yves Lacoste» في كتابه «géopolitique de la méditerranée» تحليلًا جيوسياسيًا للمتوسط بحيث يتقاطع والتقسيم الذي اعتمده إلى فضاءين متميزين هما المتوسط الغربي والمتوسط الشرقي بفواعل مختلفة وبقضايا جيوسياسية متباينة، حيث جسد الكاتب من خلال تحليله التفاعلات الحاصلة في البحر المتوسط والتي ينظر إليها على أساس أفضل مثال بين حجم الشروحات الحاصلة بين الشمال والجنوب، وهذا بعد التحول الاستراتيجي للصراع الدولي من صراع إيديولوجي شرق غرب إلى صراع حضاري وتنموي شمال جنوب^{١٣}.

ومن هنا برز مفهوم الجيواقتصاد لتفسري حجم التحول في مضمون القوة، وكذا في طبيعة التنافس الجديد الذي نشأ بين القوى لتحقيق مصالحها المرتبطة أساسًا بالقضايا الاقتصادية، من أسواق رؤوس أموال، مواد طاقوية وكذا ثورة معرفية وتكنولوجية، حيث عبر «ألبن توفلر» في كتاب له يحمل عنوان «تحول السلطة» أنه ونتيجة للثورة التكنولوجية، فإن العالم سيشهد تغيرًا وتصنيفًا جديدًا، غير مبني على أساس عالم متقدم وآخر متخلف، أو عالم رأسمالي وآخر اشتراكي، بل أن التصنيف الجديد سيكون على أساس وجود عالم سريع وآخر بطيء^{١٤}.

المطلب الأول : ملامح الجريمة السيبرانية في ظل التحويلات الجيوسياسية العالمية

سوف يصبح النشاط السيبراني المتزايد للدولة القومية أكثر وضوحًا، ولكن ليس بالضرورة أن يُعزى قانونيًا وستظل القوى الكبرى تسعى إلى تجنب الانتقام المباشر الذي يمكن أن يتصاعد إلى حرب حركية إضافية. يحذر أندرو بارات، نائب الرئيس في شركة Coalfire، قائلاً: «إن حقيقة هجمات الدول القومية هي أنك قد لا تعرف أبدًا أنك تعرضت لضربة واحدة حتى تحددتها وكالة استخبارات دولة أخرى بشكل فعال»، إذ «يعتبر إسناد الهجمات إلى أطراف معينة مجالًا مثيرًا للجدل إلى حد كبير به مجال كبير للخطأ والإنكار، فما نحتاجه حقًا هو الانتقال من شركاء المخابرات العسكرية الودودين لدعم استنتاج معقول»^{١٥}.

ربما هو التحليل الواقعي لعلاقة التحويلات الجيوسياسية في العالم بالجريمة السيبرانية، وبالإمكان الاستشهاد بدليل حي من الواقع، أين ركزت كاميرات الأخبار على الحرب الحركية

(١٣) ناصر بوعلام، التحديات الأمنية والتفاعلات الجيوسياسية في غرب المتوسط والساحل الإفريقي وتداعياتها على الأمن الإقليمي للجزائر، أطروحة دكتوراه في العلوم السياسية والعلاقات الدولية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر ٣، ماي ٢٠٢٢، ص ٣٠.

(١٤) ألبن توفلر، تحول السلطة، ط ٢، ترجمة: لبنى الريدي، مصر: الهيئة المصرية العامة للكتاب، ١٩٩٧، ص ١٩٧.

(١٥) Kevin Townsend, Cyber Insights 2023, The Geopolitical Effect, An article published through this Link :

<https://www.securityweek.com/cyber-insights-2023-the-geopolitical-effect/12:11/2023/05/29>.

التي أثارها الغزو الروسي لأوكرانيا منذ ما يقرب من عام ، لكن محلي الأمن السيبراني لديهم مخاوف أخرى - على وجه التحديد ، أن التصعيد الحتمي للهجمات الإلكترونية يمكن أن ينتشر إلى العالم الأوسع^{١٦} .

لكن من الذي شجع على ظهور الآخر ، هل هي الجريمة السيبرانية أم التحولات الجيوسياسية؟، ما يبدو واضحا أن هناك علاقة بينهما وربما يتم توظيف الجريمة السيبرانية لأغراض توسعية عالمية لتحقيق ما يسمى العالم المتعدد الأقطاب.

أولا: مفهوم التحولات الجيوسياسية

لعل من التعريفات نجد أنها : علم علاقة الأرض بالعمليات السياسية ، وأن موضوعها يقوم على قاعدة التوسع الجغرافي لاسيما على تداخل الجيوسياسية والجغرافيا السياسية، وهي النظرية التي تبحث في قوة الدولة بالنسبة للأرض، كما أنها العلم الذي يبحث في المنظمات السياسية للمجال الأرضي وتكوينها، والجيوسياسية أيضا هي الأساس العلمي الذي يقوم على فن العمل السياسي للدولة في كفاها المमित من أجل حصولها على مجالها الحيوي ، وتشير الى الروابط والعلاقات السببية بين السلطة بين السلطة السياسية والحيز الجغرافي^{١٧}.

وقد كرّست اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) جزءاً من أنشطتها لتطوير نهج متقدم لوضع التشريعات السيبرانية يقوم على التنسيق على الصعيد الإقليمي للتصدي لهذه الظاهرة، فأصدرت في عام ٢٠٠٧ دراسة بعنوان «نماذج تشريعات الفضاء السيبراني في البلدان الأعضاء في الإسكوا» وقامت بتحليل التشريعات المعتمدة في هذه البلدان ومقارنتها مع التشريعات السيبرانية المطبقة في عدد من البلدان الأخرى. وفي عام ٢٠٠٩، أطلقت مشروع «تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية» الذي يهدف إلى تحسين التكامل الإقليمي وتعزيز قدرة البلدان الأعضاء على بناء قطاع قوي ومستدام لتكنولوجيا المعلومات والاتصالات.

ولعل أهم ما اتفق عليه أغلبية الباحثين في هذا الصدد أنه يصعب تحديد بداية التحولات ومنتهاها بشكل دقيق، كما أنه يصعب اعتماد مؤشرات قياس موحدة للتغيير الاجتماعي، خاصة فيما يتعلق بحيثياته السياسية والثقافية المرتبطة بشرعية الحكم والولاية^{١٨} .

فنحن أمام ثورة قيمية نعيشها بدون قدرة مؤسسات الدولة على التحكم في سرعة

(16) David Braue , How Geopolitics Affects Cybersecurity , Melbourne, Australia – Jan. 2023 , 19 : <https://cybersecurityventures.com/how-geopolitics-affects-cybersecurity/10:57/2023/06/01>.

(١٧) محمد احمد السامرائي، موسوعة المصطلحات العلمية في الجغرافيا السياسية والجيوبوليتيك ، بغداد الذاكرة للنشر والتوزيع، ط ١، ٢٠١٢، دص وأيضاً: أحمد سعيان ، قاموس المصطلحات السياسية والدستورية والدولية ، عربي انجليزي - فرنسي ، لبنان، مكتبة ناشرون ، ط ١، ٢٠٠٤، ص ١٣٨.

(١٨) مصطفى يحيوي ، التحولات الاجتماعية والثقافية والسياسية خلال العقدين الأولين من القرن ٢١: المقاربة الترابية بعد عشرين سنة من التجريب، Friedrich Ebert Stiftung، ديسمبر ٢٠٢٢، ص ٨.

انسيابها داخل جسم الانسان، وبدون امتلاكها لمعرفة دقيقة لحشيات تشكلها تمكنها من سرعة احتوائها، ولعل أهم مظاهرها هو بداية عودة شرخ الثقة بين الهامش والمركز^{١٩}.

ثانيا: مدى ارتباط الجريمة السيبرانية بالتحويلات الجيوسياسية

بالرجوع الى التشريع الجزائري نجده لم يستقر على استخدام مصطلح واحد على هذه الجرائم، حيث سماها بموجب القانون ٠٤-١٥ المتضمن قانون العقوبات بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، ثم بموجب القانون ٠٩-٠٤ المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، استخدم مصطلح الجرائم المتصلة بتكنولوجيات الاعلام والاتصال للدلالة على هذه الجرائم، وعرفها بجرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وبأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم الاتصالات الالكترونية (المادة ٠١ من القانون ٠٩-٠٤ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها^{٢٠}.

وفي بحث نشرته الأستاذة أميرة محمد محمد سيد في مجلة البحوث الإعلامية^{٢١} وعند تطرقها لمشكلة الدراسة، حيث مع بروز الحوسبة وتأثر الفضاء السيبراني بشكل واضح بجائحة كورونا ١٩، وزيادة معدل التهديدات والهجمات السيبرانية، وفي ظل زيادة توجه الدول لمواكبة التطور التقني والمعلوماتي وتغلغل وسائل تقنية المعلومات والاتصالات في مناحي الحياة بعالمنا المعاصر وتعزيز النفاذ إليها، وفي ظل التحول الرقمي للمؤسسات وقطاعات الدول زاد من حجم انتشار البيانات والمعلومات وتبادلها، الأمر الذي ساعد في زيادة حجم الاختراقات حتى أصبح الفضاء السيبراني بيئة خصبة للحروب والجرائم^{٢٢}، من قبل المتسللين السيبرانيين سواء كانوا أفرادا أم مجموعات منظمة إلى جانب النشاطات الإرهابية الممولة من قبل بعض الدول، نتيجة للطابع المفتوح لتلك الساحة الافتراضية وعدم وجود رقابة قانونية محكمة عليها.

اذن، غياب الرقابة القانونية وبروز العولمة الرقمية ساهم في انتشار الجريمة السيبرانية، حيث تؤثر تلك الجرائم بشكل كبير على خصوصية الأفراد لأنها تنطوي على وصول غير قانوني واستخدام ضار للبيانات من قبل المهاجمين، فتلك الجرائم مرتبطة باختراق كلمات المرور أو المواقع الإلكترونية أو شبكات الدول أو المنظمات ومن هنا يظهر الارتباط الوثيق بين التحويلات الجيوسياسية والجرائم السيبرانية، إذ يستغل المجرمون الإلكترونيون الحرب والنزاعات

(١٩) مصطفى يحيوي، المرجع السابق، ص ١١.

(٢٠) مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات، المجلد ٠٦، العدد ٠٢، جامعة محمد بوضياف، المسيلة، ٢٠٢١، ص ١١٣.

(٢١) أميرة محمد محمد سيد، استراتيجيات مكافحة الجريمة الإلكترونية في العصر المعلوماتي تعزيزا لرؤية مصر ٢٠٣٠، دراسة استشرافية، مجلة البحوث الإعلامية، العدد ٥٨، الجزء الرابع، كلية الاعلام، جامعة الأزهر، يوليو ٢٠٢١، ص ١٧٧٢.

(٢٢) المرجع نفسه، ص ١٧٧٩.

تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية **الملف القانوني**

مستخدمين في ذلك أسلوب الاختراقات الآلية للحواسيب وبالتالي زادت حدة الحروب زادت الجرائم الالكترونية لأنه تعتبر شكلا من أشكال الهجمات الحربية .

المطلب الثاني: آليات محاربة الجريمة السيبرانية في ظل التحولات الجيوسياسية

استنادا الى توجيهات الخبراء الإقليميين والأطر الدولية والإقليمية بشأن الأمن السيبراني^{٣٣}، فقد حددت جمعية الأنترنت ISOC المبادئ الأساسية التالية لتأمين شبكة الأنترنت (مجتمع الأنترنت ، مارس ٢٠٢٠، ص ٢):

-الوعي : يتعين على جميع الجهات المعنية في كل من القطاعين العام والخاص فهم المخاطر التي تهدد أمنها ، ومدى تأثير تلك المخاطر عليها وعلى الآخرين في النظام البيئي الخاص بالبنية التحتية لشبكة الأنترنت.

-المسؤولية: يجب على جميع الجهات المعنية تحمل مسؤولية مواجهة المخاطر الأمنية في اطار أدوارها ومؤسساتها، مع الأخذ في الاعتبار الآثار المترتبة على اتخاذ اجراء ما أو التقاعس عن تنفيذه.

-التعاون: يجب اشراك جميع الجهات المعنية ، بما في ذلك الأطراف المعنية خارج الحدود ، في حوار مستمر حول الأمن السيبراني لمواجهة التهديدات الجديدة والمستمرة مواجهة فعالة .

وهناك معايير ثلاثة اتفق عليها الخبراء منذ البداية لضمان المعلومات ويشار اليها بمثلث أو ثلاثي CIA وهي السرية والأمانة والتوافر (مركز هيدرو ، ٢٠١٧، ص ٧).

أولا: التنسيق فيما بين التشريعات لمكافحة الجريمة السيبرانية

سن القوانين السيبرانية وتنفيذها هو من القضايا التي تكتسب مزيداً من الأهمية مع انتشار استخدام تكنولوجيا المعلومات والاتصالات وتطبيقاتها في مختلف القطاعات الاقتصادية، والاجتماعية، والعلمية، والتجارية، وذلك في الخدمات الحكومية وفي علاقات التفاعل بين الأفراد والمؤسسات^{٣٤} .

ومن أنشطة مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة

العربية مايلي^{٣٥}:

(٢٣) بن علية بن جدو، تحديات الأمن السيبراني لمواجهة الجريمة الالكترونية، المجلد ٧، العدد ٢، الجزائر، مخبر الأمن السيبراني، جامعة باتنة ١، الجزائر، جويلية ٢٠٢٢، ص ٣٠٣.

(٢٤) نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية، اللجنة الاقتصادية والاجتماعية لغربي آسيا(الاسكوا)، الأمم المتحدة، نيويورك، ٢٠١٢، ص ٧.

(٢٥) نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية، المرجع السابق، ص ٨.

١. إعداد تقارير حول وضع التشريعات السيبرانية في المنطقة العربية واقتراح إطار عام لتطوير وتنسيق التشريعات السيبرانية في العالم العربي.
٢. وضع إرشادات للتشريعات السيبرانية بالاعتماد على التجارب الإقليمية والدولية، وخاصة التجربة الأوروبية، مع أخذ خصوصيات المنطقة العربية في الاعتبار.
٣. تنظيم اجتماع للخبراء شارك فيه الأخصائيون من المؤسسات الحكومية والمنظمات غير الحكومية والقطاع الخاص، لاستعراض ومناقشة مسودة إرشادات الإسكوا للتشريعات السيبرانية.
٤. تنظيم ورشتي عمل إقليميتين لتوفير التدريب العملي لصانعي القرار والسياسات حول إرشادات الإسكوا للتشريعات السيبرانية وتطبيقها على المستويين الوطني والإقليمي.
٥. تقديم خدمات استشارية للدول العربية من أجل تطوير تشريعاتها السيبرانية بالتوافق مع إرشادات الإسكوا.
٦. إنشاء شبكة افتراضية من الخبراء لإطلاق النقاش والحوار حول تطبيق إرشادات الإسكوا للتشريعات السيبرانية في المنطقة العربية، بحيث تشكل هذه الشبكة قاعدة لتبادل المعرفة وأداة لاستدامة المشروع.
٧. تنظيم ندوة حول المتطلبات القانونية والتنظيمية لإقامة مجتمع معرفة مستدام في المنطقة العربية، واستعراض نتائج المشروع وصياغة توصيات لضمان استدامة العمل في مجال تنسيق التشريعات السيبرانية على المستويين الوطني والإقليمي.

ثانياً: مواكبة التغيرات الجيوسياسية بالمصادقة على الاتفاقيات الخاصة بالإجرام المعلوماتي

لقد بلورت ورش العمل والخدمات الاستشارية الجانب التطبيقي لمشروع « تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية »، حيث أتاحت الفرصة للفرقاء المعنيين من وزارات تكنولوجيا المعلومات والاتصالات، ووزارات العدل، وذلك الجهات الأكاديمية والمجتمع المدني، للاطلاع عن قرب على أنشطة المشروع وخاصة إرشادات الإسكوا للتشريعات السيبرانية. وقد تمكنت الأردن، والبحرين، والجمهورية العربية السورية، وعمان، وفلسطين من الاستفادة من الخدمات الاستشارية التي قدمتها الإسكوا بالتعاون مع الخبراء القانونيين، وقد شملت هذه الخدمات الاستشارية مراجعة مسودات القوانين السيبرانية التي أعدتها هذه الدول، وتقيماً لوضع التشريعات السيبرانية في الدولة، ودراسة للفوارق بينها وبين إرشادات الإسكوا في هذا المجال^{٣٦}.

(٣٦) نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية، المرجع السابق، ص ٩.

كما أولى المشروع أهمية لاستدامة العمل ولضمان استمرار الاهتمام والاستخدام الفعلي للمخرجات، وخاصة إرشادات الإسكوا للتشريعات السيبرانية. وللوصول لهذا الهدف، عملت الإسكوا على انشاء بوابة الكترونية^{٢٧} تشكل مخزناً للمعلومات والمعرفة، وتهدف إلى التوعية بأهمية التشريعات السيبرانية ودعم متخذي القرار في الدول العربية في عملية وضع الأطر القانونية الخاصة بالفضاء السيبراني، وتهدف إلى التوعية بأهمية التشريعات السيبرانية ودعم متخذي القرار في الدول العربية في عملية وضع الأطر القانونية الخاصة بالفضاء السيبراني.

(٢٧) نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية ، المرجع السابق، ص ١١.

الخاتمة :

يبدو أن التحولات الجيوسياسية وحتى التغيرات المناخية أثرت بشكل واسع على مسار التفاعل السياسي والاقتصادي والاجتماعي للدول إزاء ما يحدث في العالم كله من مناورات للتموقع الجيد بحسب ما يقتضيه الحال من ضرورة مواكبة التطور الذي لا ينفك يتوقف لأن الدول كلها في أهبة تامة لأجل ضمان أمن عام وفي جميع القطاعات ، وعليه يمكن استنتاج بعض النتائج من خلال مضمون هذا البحث في توضيح التفاعل بين التغيرات الجيوسياسية والجريمة السيبرانية التي باتت تهدد اليوم الأمن القومي.

الاستنتاجات :

١. الجريمة السيبرانية جريمة عابرة للقارات ولا تتخذ لها شكلا معينا وتتنوع بحسب الهدف و الشيء المستهدف سواء أشخاص او مؤسسات أو اعتمادات مالية أو منصات رقمية، العبرة هي بتهديد الخصوصية الفردية وسلامة المعلومات والبيانات .

٢. تقح مهاجمة الدول قيد الحروب بأفعال سيبرانية مخالفة للقانون والأعراف الدولية، والمعروف على طبيعة وسائل الجريمة السيبرانية من تقنيات وطرق الكترونية هي منخفضة التكلفة مقارنة بتكلفة الأسلحة التقليدية، لكن تأثيرها الخطير يمتد حتى لهزيمة القوات العسكرية، يعني شكل الهجمات الحديثة أثر على التحولات الجيوسياسية بطريقة تبعث على عدم الاطمئنان ،وهو ما دفع بالدول الى دراسة الأمن السيبراني من جميع جوانبه خاصة منها طرق ارتكاب الجريمة السيبرانية .

٣. هناك صعوبة في اكتشاف الأدلة المادية لارتكاب الجريمة السيبرانية ،لأن الذين يرتكبون الجرائم أنفسهم يحتاطون بإجراءات امنية تزيد من صعوبة التعرف عليهم واكتشاف هويتهم، خاصة أنهم يرتادون الفضاء الالكتروني بأسماء مستعارة .

٤. تعتبر الجريمة السيبرانية من الجرائم متنوعة الأساليب وسريعة التطور بسبب تطور التكنولوجيا والتقنية، وعليه فان الاعتماد على الحاسوب لوحده ضاعف من نسبة ارتكابها لأن مسرح الجريمة الالكتروني ليس كمسرح الجريمة التقليدي وبالتالي يصعب ضبط الجناة بالترصد لهم مثل ما يحدث في الجرائم التقليدية.

٥. يمكن ان تغير الجريمة السيبرانية نتائج حرب كاملة في لحظات فارقة بسبب مفاجآت الاختراق وتغيير المعلومات وكذا الحصول على البيانات بطريق الدخول الغير مشروع للحسابات والأرصدة وغيره من منصات التفاعل الرقمي الحديث.

المقترحات :

١. على حكومات الدول أن تحين تشريعاتها من فترة لأخرى بحسب تطورات الجريمة السيبرانية وما يتبعها من أضرار على أكثر من صعيد خاصة ماي تعلق بحماية الخصوصية الفردية وكذا الأمن القومي للبلد.
٢. لا بد من اتخاذ تدابير الوقاية والأمن مع مراعاة حقوق الانسان في نفس الوقت .
٣. رفع مستوى الوعي لدى مرتادي وسائل التواصل الاجتماعي وكذا مستخدمي الأنترنت بصفة عامة بما يحقق الثقافة الكافية لمخاطر الجريمة السيبرانية خاصة لفئة المراهقين.
٤. توفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات.
٥. تفعيل الاتفاقيات الدولية بضرورة المصادقة عليها وسن قوانين وطنية امتثالاً لما تم المصادقة عليه في الاتفاقيات الخاصة بالمعالجة الآلية للمعلومات والأمن السيبراني.
٦. جمع الأدلة الاثباتية الالكترونية للجرائم السيبرانية المعروفة ووضع دليل قانون خاص بها لاستخدامه فور اكتشاف الجريمة .
٧. ضرورة تشديد بعض العقوبات الخاصة بحقوق المؤلفين والملكية الفكرية التي يمكن السطو عليها او تغييرها من خلال الاختراقات الالكترونية.
٨. توسيع صلاحيات الشرطة الالكترونية الى ضرورة المتابعة الدائمة لمن هم محل شك أو شبهة..منعا لوقوع الجريمة السيبرانية .
٩. ضرورة التكوين المستمر لجهاز الأمن السيبراني مراعاة لتطورات الحرب او النزاعات وما قد يحدثه من هجمات وتعطيل للبنى التحتية للمؤسسات والإدارات ..فبقدر تطوير وتنمية المعرفة بقدر ما يتم التعرف بسرعة عن الجناة وكشف أساليبهم حتى لو كانت باحترافية منهم.