مجلة الدراسات القانونية والسياسية

المجلد 09 العدد 02 جوان 2023 | ص ص:154-171

الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية

International And National Mechanisms To Combat Cyber Crime

شويرب جيلالي

جامعة عمار ثليجي، الأغواط

djelloulchouireb1979@gmail.com

مراد فائزة*

جامعة الدكتور يحي فارس، المدية

مخبر السيادة والعولمة

merad.faiza@univ-medea.dz

- تاريخ الإرسال: 2023/03/24 - تاريخ القبول: 2023/05/30 - تاريخ النشر: 2023/06/05

ملخص:

تعتبر الجريمة السيبرانية الوجه الحديث للإجرام والذي يشكل استخدام البيانات الإلكترونية ركنه المادي، وقد كافحت الدول من خلال الإتفاقيات والمعاهدات الدولية والتحالفات الإقليمية هذا النوع من الجريمة ومن أهم الإتفاقيات إتفاقية بودابست لمكافحة جرائم الفضاء المعلوماتي 2001،كما تناولها المشرع الجزائري في قانون العقوبات وما تلاه من قوانين، فضلا لما للآليات المؤسساتية الإجرائية من دور هام وقائي وردعي للجريمة الإلكترونية، مثل التعاون القضائي الدولي وتسليم المجرمين والإنابة القضائية وكذا جهود الهيئات الوطنية التي تلاحق المجرمين وتعاقبهم .

الكلمات المفتاحية: الجريمة السيبرانية، القوانين الدولية، التشريع الوطني، الآليات ،الردع.

Abstract :

Cybercrime is the new face of crime, when the use of data constitutes its material pillar, all the nations of the world have fought against this type of crime through international rules and conventions, such as the Budapest Convention 2001, and this which followed as well as the national legislation with what it contains the Algerian penal code and the special laws. In addition the institutional mechanisms of prevention and deterrence Such as international judicial cooperation, extradition of criminals, as well as national bodies that prosecute and punish criminals

Key words: cybercrime, international laws, national legislation, mechanisms, deterrence.

* -المؤلف المرسل:

مقدمة:

تختلف الجرائم السيبرانية عن الجرائم العادية إختلافًا جوهريًا من حيث طبيعتها ونطاقها وأساليبها والأدلة المتاحة لمكافحتها، فهي ظاهرة إجرامية جديدة تنطوي على هجمات وإختراقات داخل أنظمة المعلومات، إما بغرض تدمير تلك الأنظمة أو الحصول على معلومات سرية، ونتيجة للتطور السريع في مجال تكنولوجيا المعلومات والاتصالات والإنترنت ظهرت هذه الجرائم وشكلت سوء إستخدام للتكنولوجيا منبهة بمخاطر عسكرية واقتصادية وسياسية على المستويين الوطني والعالمي، مما أوجب إيجاد تدابير للتخفيف من هذه المشكلة.

تعد طبيعة السرية من سمات الجريمة السيبرانية،كما لا توجد قيود جغرافية أو زمنية لمثل هذه الجرائم، وعليه يمكن أن يعاني عدد لا يحصى من الضحايا من ضرر سريع، فضلا على أن إشكالية أمن المعلومات باتت تتجاوز مفهومها التقني لتشمل الأبعاد الأمنية والدفاعية والاستراتيجية، كما أصبحت جزءًا لا يتجزأ من خطط الأمن القومي والإتفاقات الدفاعية للتحالفات العسكرية.

ولذا كان لزاما على المجتمع الدولي أن يسعى لتظافر الجهود من أجل مكافحة هذا النوع من الإجرام عبر إتفاقيات وآليات دولية، ولم يغفل التشريع الوطني هذا النوع الجديد من الجرائم فتوسع في دائرة التجريم في مجال هذه الأفعال سواء كانت ماسة بالنظام نفسه أو من خلال إستعمال تكنولوجيا المعلومات في الجرائم التقليدية

تنبع أهمية هذه الدراسة من كونها تتناول الجريمة السيبرانية التي باتت تمس جميع مجالات الحياة، كما تلقي الضوء على جهود المشرع الدولي والوطني في التصدي لهذا النوع من الإجرام.

كما تكمن أهدافها في أن الإهتمام بمكافحة الجرائم السيبيرانية، يتطلب وضع إستراتيجية وإيجاد الحلول من خلال إبراز الدور الفعال لآليات مكافحة الجريمة السيبرانية على المستوى الدولي والوطني.

وبناء على ما تقدم تتمثل إشكالية الدراسة في التساؤل التالي: **ماهي مراحل تقنين ومحاربة الجرائم السيبرانية دوليا ووطنيا ؟**

وتتفرع عن هذه الإشكالية أسئلة فرعية

-ما مفهوم الجريمة السيبرانية في التشريعات الدولية والوطنية ؟

- ما مدى تكريس آليات تنفيذية دولية ووطنية لمكافحتها ؟

وقد تناولنا هذه الدراسة من خلال مبحثين، كمبحث أول تناولنا مفهوم الجريمة السيبرانية وتقنينها دوليا وإقليميا في المطلب الأول لنفصل في المطلب الثاني في مدى تناول التشريع الوطني للجريمة الإلكترونية وفي المبحث الثاني حاولنا عرض الآليات المؤسساتية والإجرائية التنفيذية لمحاربة الجريمة الإلكترونية من خلال الآليات الدولية في المطلب الأول والآليات الوطنية في المطلب الثاني، مستخدمين المنهج الوصفي في عرض المعلومات وتحليلها كما استخدمنا المنهج التاريخي عند تقديمنا لنظرة شاملة في بعض الأجزاء من الدراسة.

المبحث الأول مفهوم الجريمة السيبيرانية وتطورها دوليا وإقليميا:

بالرغم من أن الجرائم الإلكترونية أو جرائم الحاسوب هي ظاهرة محلية ودولية إلا أن التنبيه لخطورتها إنتشر على النطاق الدولي بل إن الخوف من مخاطرها تزايد لما تجاوزت الحدود الوطنية وأصبحت جريمة منظمة عابرة للحدود، فتناولها الفقه والقانون والقضاء والإعلام والدراسات المختلفة الاقتصادية والأمنية والسياسية والقانونية وعليه لابد أن نتعرف على مفهوم هذه الجرائم لنفصل بعد ذلك في وسائل مكافحتها وطنيا إقليميا ودوليا .

المطلب الأول مفهوم الجريمة السيبرانية ومراحل وجودها :

نتناول مفهومها أولا ثم تطورها ومراحل وجودها

الفرع الأول تعريف الجريمة السيبرانية

نعني بالجريمة السيبيرانية بصفة عامة إساءة استخدام تكنولوجيا المعلومات والإتصالات بين المجرمين بالتبادل، أو إساءة إستخدام الكمبيوتر أو" إستخدام الكمبيوتر أو الإنترنت لارتكاب أو تسهيل ارتكاب الجريمة، أما المعهد الأسترالي لعلم الإجرام فيرى بأنها" تسمية عامة لجرائم ارتكبت باستخدام تخزين البيانات الإلكترونية أو جهاز الإتصالات[1]"

وعرفها الأستاذ هلالي عبد الله أحمد بقوله: "عمل أو امتناع عن عمل يأتيه الإنسان إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض للاعتداء عليها عقابا"[2]

كما عرفها مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين بأنها "أية جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية ،والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية"[3]

فهي إذن جريمة لها عناصرها تصنع خصوصيتها إذ لابد من توفر وسائل إلكترونية من حاسوب وشبكة إنترنت تستخدم لأغراض إجرامية أي قصد الإضرار بالأفراد أو مؤسسات دولية تمتلك تلك المعلومات التي تستخدم ضدها أو يتم إتلافها أو تسريبها إلى العدو .

الفرع الثاني مكافحة الجريمة السيبرانية دوليا

في مجال مكافحة الجرائم السيبرانية بصفة عامة عقدت المعاهدات والاتفاقيات التي تعمل على تكريس التعاون الدولي في مجال مكافحة الجرائم الإلكترونية نذكر منها على سبيل المثال

[1] Cameron S. D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", International Journal of Cyber Criminology. Vol9, Issue 1, January – June 2015, p 57

[2] عبد الله أحمد هلالي، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي –دراسة مقارنة–، دار النهضةالعربية، القاهرة، 2000، ص. 105 و106.

[3] مونة مقلاتي .راضية مشري،الجريمة الإلكترونية دلالة المفهوم وفاعلية المعالجة القانونية، مجلة أبحاث قانونية وسياسية،المجلد 6 العدد 1،جامعة 8ماي 1945،قالمة،جوان 2021،ص 494

معاهدة بودابست لمكافحة جرائم الإنترنت ،توصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، كما ننوه بمساعي الجمعية العامة للأمم المتحدة لدراسة الوضع بشأن الجريمة السيبرانية ونبينهما فيما يلي:

أولا معاهدة بودابست لمكافحة جرائم الإنترنت

تعد معاهدة بودابست لمكافحة جرائم الإنترنت أولى المعاهدات المتعلقة بتلك الجرائم والتي تمت في العاصمة المجرية بودابست في 2001/11/23، والتي تبرز التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الإنترنت، وقد وقعت على تلك المعاهدة 26 دولة أوروبية بالإضافة إلى كندا واليابان، وجنوب أفريقيا، والولايات المتحدة الأمريكية، وتوفر المعاهدة أسس الأمن العام وتتضمن 48 مادة مقسمة على أربعة فصول.[1]

وتهدف الاتفاقية إلى:

-توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.

-توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيًا بواسطة الكمبيوتر.

-تعيين نظام سريع وفعال للتعاون الدولي.

-الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.

-جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها.

نرى من خلال مبادئ معاهدة بودابست حرصها على التعاون الدولي من خلال القوانين الجزائية الوطنية المتعلقة بهذا النوع من الجرائم بإعتبار كل دولة تحاول الحفاظ على أمنها القومي وإقتصادها وإستقرار نظامها السياسي من خلال العمل على أمنها السيبراني أي حماية قاعدة بياناتها،ولما كانت الجريم السيبرانية عابرة للحدود فمن المنطقي أن تنطلق في دولة وتنتهي في أخرى،مما جعل التعاون لمكافتحها وملاحقة المجرمين ضرورة لا مفر منها .

ثانيا مكافحة الجريمة الإلكترونية من خلال هيئة الأمم المتحدة

طلبت الجمعية العامة، في قرارها 65-230 من لجنة منع الجريمة والعدالة الجنائية أن تنشئ، وفقا للفقرة 42 من إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية:

نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغيرمن خلال تكوين فريق خبراء حكومي دولي مفتوح العضوية من أجل إجراء دراسة شاملة لمشكلة الجريمة السيبيرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، بما في ذلك تبادل المعلومات عن التشريعات الوطنية وأفضل الممارسات والمساعدة الفنية

[1]، عبد الله أحمد هلالي، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست 2001) دارالنهضة العربية، ط 2001، ص 30.

والتعاون الدولي، بغية دراسة الخيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجرائم السيبرانية وإقتراح تدابير جديدة في هذا الشأن[1]

أحاطت الجمعية العامة علما في قرارها **67-189** بعمل فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية، وشجعته على تحسين الجهود التي يبذلها من أجل إنجاز أعماله وعرض نتائج الدراسة في الوقت المناسب على لجنة منع الجريمة والعدالة الجنائية.

و عقدت الدورة الأولى لفريق الخبراء في فيينا في الفترة الممتدة من 17 الى 21 جانفي2011 وقام خلالها فريق الخبراء باستعراض واعتماد مجموعة من المواضيع وكذلك منهجية للدارسة تضمنت مجموعة المواضيع المطروحة للنظر فيها ضمن إطار الدراسة الشاملة للجريمة السيبرانية، مشكلة الجريمة السيبرانية، وتدابير التصدي القانونية للجريمة السيبرانية، وقدرات منع الجريمة والعدالة الجنائية وتدابير التصدي الأخرى للجريمة السيبرانية، والمنظمات الدولية، والمساعدة الفنية .ثم قسمت هذه الموضوعات الى 12 موضوعا فرعيا تناول هذه الموضوعات في سياق هذه الدراسة في ثمانية فصول.

وفي إطار منهجية الدراسة؛ كلف مكتب الأمم المتحدة المعني بالمخدرات والجريمة بإعداد الدراسة، بما في ذلك إعداد استبيان بهدف جمع المعلومات، وجمع البيانات وتحليلها، وإعداد مشروع لنص الدراسة.

وتقرَّر في إطار جمع المعلومات وفقا لمنهجية الدراسة التي أعدها مكتب الأمم المتحدة المعني بالمخدرات والجريمة، توزيع استبيان على الدول الأعضاء والمنظمات الحكومية الدولية وممثلين عن القطاع الخاص والمؤسسات الأكاديمية من شهر فيفري 2012 الى غاية جويلية 2012 وقد وردت إلى مكتب الأمم المتحدة المعني بالمخدرات والجريمة معلومات من 69 دولة عضوا. واستعرضت الأمانة أيضا أكثر من 500 وثيقة من مصادر مفتوحة .ويتضمن الملحق الخامس بهذه الدراسة مزيدا من التفاصيل بشأن المنهجية.

تناولت الدراسة مشكلة الجريمة السيبرانية من خلال منظور الحكومات، والقطاع الخاص، والأوساط الأكاديمية، والمنظمات الدولية، وقد تم طرح النتائج في ثمانية فصول تناولت الموص ولية الخاصة بشبكة الإنترنت والجريمة السيبرانية، والصورة العالمية للجريمة السيبرانية، وأطر وتشريعات مكافحة الجريمة السيبرانية، وتجريم الجريمة السيبرانية، وإنفاذ القانون والتحقيقات في الجريمة السيبرانية، والأدلة الإلكترونية والعدالة الجنائية، والتعاون الدولي في المسائل الجنائية التي تنطوي على جريمة سيبرانية، والوقاية الجريمة السيبرانية[2]

الفرع الثالث الآليات القانونية الإقليمية لمكافحة الجريمة الإلكترونية

[1] دراسة شاملة عن الجريمة السيبرانية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فينا، 2013، ص 13

[2] دراسة شاملة عن الجريمة السيبرانية، مرجع سابق، ص 14

يأخذ التعاون الدولي شكلا دوليا أو إقليميا داخل تحالفات مثل ما هو عليه الإتحاد الأوروبي والذي عمل على مكافحة الجريمة السيبرانية على المستوى الإقليمي وأصدر توصيات في هذا الشأن من خلال المجلس الأوروبي بإعتبارها هيئة إستراتيجية توجه السياسات العامة للإتحاد الأوروبي هذه التوصيات التي سنتناولها في الفرع الآتي

أولا توصيات المجلس الأوروبي

أدى التطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجزائية في هذا المجال إلى إصدار المجلس الأوروبي التوصية رقم 95/13 المؤرخ في 1995/09/11 في شأن مشاكل الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات، وحث الدول الأعضاء بمراجعة قوانين الإجراءات الجزائية الوطنية لكي تتلاءم من التطور في هذا المجال، ومن أهم ما ورد بتوصية المجلس الأوروبي ما يلي:

1.أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها.

2.أن تسمح الإجراءات الجزائية الوطنية لجهات التفتيش ضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية ويتعين إخطار الشخص القائم على الأجهزة بأن النظام كان محلا للتفتيش مع بيان المعلومات التي تم ضبطها، ويسمح بإتخاذ إجراءات الطعن العادية في قرارات الضبط والتفتيش.

3.أن يسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع إحترام الضمانات المقررة بمد التفتيش إلى أنظمة الكمبيوتر الأخرى في دائرة إختصاصهم والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات، بشرط ان يكون هذا الإجراء ضروريا.

4.أن يوضح قانون الإجراءات الجزائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجودة بأجهزة الكمبيوتر.

5.تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات ويتعين توفير السرية والإحترام للمعلومات التي يفرض القانون لها حماية خاصة.

6. يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لإجراء المراقبة والتسجيل.

7.يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات سواء كانت برامج أم قواعد أم بيانات، تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.

8.يتعين إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحتويه من معلومات باتخاذ الازم للسماح لرجال التحقيق بالاطلاع عليها، وأن تخول سلطات التحقيق بإصدار أوامر مماثلة لأي شخص لديه معلومات عن طريق التشغيل والمحافظة على المعلومات.

9.يجب تطوير وتوحيد أنظمة التعامل مع الأدلة الإلكترونية، وحتى يتم الاعتراف بها بين الدول المختلفة ويتعين أيضا تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة الإلكترونية.

10. يجب تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.

11. قد تتطلب إجراءات التحقيق مد الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة وتفترض التدخل السريع، وحتى لا يمثل هذا الأمر اعتداء على سيادة الدولة والقانون الدولي، يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك كانت الحاجة إلى عقد اتفاقيات تنظم كيفية اتخاذ مثل هذه الإجراءات.

12.يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع ادله معينة ويتعين عندئذ ان تسمح السلطة الأخيرة بإجراءات التفتيش والضبط .ويتعين كذلك السماح لهذه السلطة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدرها ولذلك يتعين تطوير اتفاقيات التعاون الدولي القائمة[1]

ثانيا إتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية

أقرت جامعة الدول العربية قانونا استرشاديا لمكافحة جرائم الفضاء السيبيراني، وقد سعت الدول العربية لتقنين وتجريم الأعمال الغير مشروعة المرتكبة من خلال إستخدام الفضاء السيبيراني بالتوقيع على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات من أجل تعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبيرانية والحفاظ على أمنها وسلامة مجتمعاتها، حيث دعا المجلس، إلى موافاة الأمانة الفنية للمجلس ما إتخذته من إجراءات لموائمة تشريعاتها مع أحكام الإتفاقية وتجريم الصور المستحدثة من الجرائم الإلكترونية لمنع الإرهابيين من إستخدام الإنترنت وتعزيز التعاون مع المنظمات الدولية والإقليمية المعنية بمواجهة كافة أشكال جرائم الإرهاب الإلكترونية.

كما دعا المجلس الى تفعيل التعاون لمنع المجرمين من استغلال تكنولوجيا المعلومات والاتصالات والإنترنت للتحريض على دعم أعمالهم الإرهابية وتمويل أنشطتهم والتخطيط والإعداد لها، وأكد المجلس على أهمية تعزيز التعاون مع المنظمات والوكالات الدولية المتخصصة للحصول على المساعدات المطلوبة في بناء القدرات اللازمة لمواجهة خطر استخدام الإرهابيين لأسلحة الدمار الشامل أو مكوناتها، ودعم أمن المطارات والموانئ والحدود.

[1] مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ط2000 ، ص80

بالرغم من كل هذه الجهود الدولية سواء على مستوى الأمم المتحدة والمنظمات الدولية وعلى المستوى الإقليمي وخاصة إتفاقية بودابست التي تعتبر بمثابة دعوة للدول لإعادة النظر في تشريعاتها الداخلية والدعوة إلى التعاون الدولي لأجل مكافحة الجرائم السيبرانية التي لا تعرف الحدود الجغرافية .إلا هناك صعوبات تواجه هذه الجهود[1].

المطلب الثاني مكافحة الجريمة السيبيرانية في التشريع الجزائري :

يطلق المشرع الجزائري على الجريمة السيبيرانية مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات شرطا اساسيا في الجريمة السيبرانية[2]

الفرع الأول الإطار التشريعي

تضمنت عدة قوانين موضوع مكافحة الجريمة المعلوماتية أما بإقرار أحكام موضوعية تشكل مساسا بالنظام الآلي أو بما يحتويه من معلومات وهو ما سوف نبينه من خلال العناصر الموالية:

أولا في قانون العقوبات

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون بموجب القانون العقوبات رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم لأمر رقم- 66-156 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات " ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394المادة مكرر7.

وفي عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون- رقم 06-23 المؤرخ في 20 ديسمبر 2006 حيث مس هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص، الواردة في هذا القسم من القانون 04-15 وربما يرجع سبب هذا التعديل إلى إزدياد الوعي بخطورة هذا النوع المستحدث من الإجرام بإعتباره يؤثر على الإقتصاد الوطني بالدرجة الأولى وشيوع إرتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل تكنولوجيا المعلومات وإنتشار الأنترنت كوسيلة لنقل المعلومات.

ثانيا القوانين اللاحقة للقانون 09-04

لم يكتفي المشرع الجزائري بالقانون 09-04 بل جاءت بعده عدة قوانين تعالج نفس المضمون وهي ما سوف نتطرق اليه في النقاط التالية:

أ) القانون 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد والإتصالات الالكترونية

[1] قطاف سليمان، بوقرين عبد الحليم، مواجهة الجرائم السيبرانية في ظل الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية ،المجلد 05، العدد 02، 2022، ص 81

[2] قانون رقم 09-04 مرجع سابق، ص 5.

.حيث إستحدث هذا القانون مجموعة آليات للتصدي للجرائم المتعلقة بالعالم الإفتراضي منها إستحداث سلطة ضبط من بين مهامها السهر على إحترام متعاملي البريد والإتصالات الإلكترونية من خلال أحكام قانونية وتنظيمية تتعلق بالأمن السيبراني

الأمن السيبراني[1]

وعليه جرمت إنتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الالكترونية أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل أو المرسل إليه أو الأخبار بوجودها، وتجريم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة، وسنت مجموعة من العقوبات[2]

ب) القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

فقد عرف المعطيات ذات الطابع الشخصي في المادة الثالثة من القانون رقم 18-07 المتعلق بحماية المعطيات الشخصية بأنها كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه "الشخص المعني " بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.

الا أن هذه المعايير للمعطيات الشخصية التي جاء بها قانون 18-07 تواجه صعوبات كثيرة يمكن أن تطرح أمام القضاء الذي يملك سلطة تقديرية في تحديد مدى توافر الطابع الشخصي لمعلومة معينة، مما يستلزم تقدير كل حالة على حدة بحسب ظروفها وملابساتها، مع الأخذ بعين الاعتبار ضرورة التوفيق بين حماية الحياة الخاصة والتدفق الحر للمعلومات، وكذلك تطور تكنولوجيا المعلومات والاتصالات الحديثة[3]

وأقر هذا القانون المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي فنجد المادة 7 من القانون 18-07 تنص على ضرورة إبداء الموافقة الصريحة للشخص المعني من أجل السماح بمعالجة معطياته الشخصية، وله التراجع عن موافقته في أي وقت، غير أن موافقته لا تكون ضرورية متى تعلق الأمر باحترام التزام قانوني يخضع له المعني.

ولم يغفل المشرع في القانون 18-07 حماية المعطيات الخاصة بالأطفال فقد جاءت المادة 8 من نفس القانون متوقفة على موافقة ممثله الشرعي أو بترخيص من القاضي المختص عند الاقتضاء أو يمكن لهذا الأخير الترخيص حتى

[1] المادة 13 من القانون 18-04 المرخ في في 10 مايو2018 ، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر، عدد27 ، الصادرة بتاريخ 13 ماي2018

[2] المواد من 164 الى 188 من نفس القانون

[3] تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على الضوء القانوني رقم 18-07، دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية المجلد 04، جامعة مسيلة، الجزائر، 2019، ص1528.

بدون موافقة ممثله الشرعي متى استدعت مصلحة الطفل الفضلى ذلك، وبالنسبة لطريقة المعالجة يجب أن تكون أغراض المعالجة واضحة ومحددة ومشروعة ومحترمة طوال فترة استمرار عملية استخدام المعلومات والاحتفاظ بها.

وتضمن نصوص القانون 18-07 إجراءات الحصول على التصريح من خلال ضرورة إيداع التصريح المسبق الذي يتضمن الالتزام بإجراء المعالجة لدى السلطة الوطنية، كما يمكن تقديمه بالطريق الإلكتروني، فورا أو في أجل أقصاه يومين، ويمكن للمسؤول عن المعالجة أن يباشر عملية المعالجة فور استلام وصل الإيداع[1].

كما أن السلطة الوطنية تُخضع أي معالجة تتضمن أخطارا ظاهرة على احترام وحماية الحياة الخاصة لترخيص مسبق بواسطة قرار مسبب يُبلغ إلى المسؤول عن المعالجة في أجل 10 أيام من تاريخ إيداع التصريح، كما يمنح الترخيص بمعالجة المعطيات الحساسة في حالة ما إذا كانت المعالجة ضرورية لحماية المصالح الحيوية للشخص المعني أو لشخص آخر[2]. كما منح هذا القانون ممارسة حق التصحيح أو التحيين أو مسح أو إغلاق المعطيات الشخصية عندما يتبين له أن هذه المعطيات غير مكتملة أو غير صحيحة أو لكون معالجتها ممنوعة قانونا[3].

وأضافت المادة 36 من القانون 18-07 حق الشخص في الاعتراض على معالجة معطياته الشخصية، خاصة إذ تعلق الأمر بأغراض دعائية أو تجارية.

وألزم المسؤول عن المعالجة باتخاذ كل التدابير التقنية والاحترازات اللازمة من أجل حماية وتأمين المعطيات ذات الطابع الشخصي من القرصنة والتلف وكل استخدام غير مشروع، كما ألزمته بالسر المهني وعدم إفشاء المعطيات التي وصلت إلى علمه[4]

ثانيا وضع إستراتيجية أمنية

وهذا من خلال مجموعة مواد منها المادة 2 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مسميا إياه": المنظومة المعلوماتية "وهي مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين "[5]

وجرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية وبأشكال جديدة من الإجرام لم تشهدها البشرية من قبل وهذا دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04 -15المؤرخ في العاشر من نوفمبر 2004المتمم للأمر رقم 66-156المتضمن قانون العقوبات والذي أفرد القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات. والذي تضمن ثمانية(8)مواد من المادة

[1] المادة 13 من القانون 18-07، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] نصت المادة 17 من نفس القانون

[3] المادة 35 من نفس القانون

[4] المادة 40 نفس القانون

[5] نشناش منية، مداخلة حول الركن المفترض في الجريمة المعلوماتية، جامعة بسكرة 2015ـ 2016،، ص 4.

394مكرر وحتى المادة 394مكرر 07. فالمشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات مقارنة مع التشريعات الأخرى إشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها، وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل من المعالجة الآلية للمعطيات[1]

من خلال ما تقدم نستنتج مواكبة المشرع الجزائري للتطور التكنولوجي بتعديل قانون العقوبات لسد الفراغ القانوني في هذا المجال ويخرج بذلك من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة ارتكابها وحصرها فقط في صور الأفعال التي تشكل إعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها .

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحولها إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة.

المبحث الثاني الآليات المؤسساتية لمكافحة الجريمة السيبيرانية :

لا يمكن الحديث عن مكافحة الجريمة السيبيرانية دون آليات تنفيذية دولية ووطنية يمكن من خلالها مجابهة الجريمة الإلكترونية وسوف نتطرق للآليات الدولية لمكافحة الجريمة السيبرانية في إطار التعاون الدولي ثم للآليات الوطنية الإجرائية والمؤسساتية.

المطلب الأول الآليات المؤسساتية الدولية لمكافحة الجريمة السيبرانية في إطار التعاون الدولي:

أصبح التعاون الدولي ضرورة ملحة لمكافحة الأفعال الإجرامية العابرة للحدود، حيث أثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة المعلوماتية، خاصة مع التطور الملموس والمذهل في الإتصالات وتكنولوجيات المعلومات فإن كان من الضروري أن تمتلك الدول الإمكانات التشريعية والقضائية والفنية لمكافحة الجريمة المعلوماتية، فان الأهم من ذلك أن تكون تلك القوانين متوائمة ومتجانسة بين مختلف الدول، إذ هي تحمي مصلحة مشتركة. والتعاون الدولي في مجال مكافحة الجرائم المعلوماتية قد يأخذ عدة أوجه منها ما يتعلق بضرورة التعاون في إنفاذ قانون لملاحقة ومتابعة ومعاقبة المجرمين ويتمثل هذا في التعاون القضائي وتسليم المجرمين، ومنها ما يتعلق بالسعي إلى إتخاذ الإجراءات والآليات ذات الطبيعة التقنية الفنية التي تكفل منع إرتكاب الجريمة في مرحلة التنفيذ نوضح ذلك فيما يلي:[2]

الفرع الأول: الوسائل العملية لمكافحة الجرائم السيبرانية

أولا: التعاون القضائي

من أهم الآليات الرئيسية للكفاح ضد الجريمة العابرة للحدود الوطنية بجميع أبعادها نجد التعاون القضائي الدولي، ففيما يتعلق بالجريمة المعلوماتية فإن فعالية التحقيق والملاحقة القضائية غالبا ما تقتضي الحاجة إلى مساعدة من السلطات في البلد الذي كان منشأ للجريمة، أو من السلطات في البلد الذي عبر من خلاله النشاط المجرم وهو في

[1] نشناش منية، المرجع نفسه 4 .

[2] صورية بوربابة، التعاون الدولي في مكافحة الجريمة المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد01، 2019، ص95

طريقه إلى الهدف، أو حيث توجد أدلة الجريمة، فقد يكون مرتكب الجريمة المعلوماتية من جنسية دولة ما مستعملا في جريمته حواسيب موجودة في دولة أخرى وتقع آثار جريمته في دولة ثالثة. ومن البديهي أن يقف مبدأ السيادة ومشاكل الحدود والولايات القضائية عقبة أمام إكتشاف هذه الجرائم ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المعلوماتية ومتابعة مرتكبيها قضائيا تؤكد على أهمية المساعدة القضائية المتبادلة بين الدول .

ثانيا: تبادل المعلومات

تشكل المعلومة، أساس لكل خطوة بالإتجاه الصحيح لمواجهة أية ظاهرة أو لتحقيق أي انجاز على أرض الواقع، والدول من جهتها تدرك قيمة وأهمية ذلك في علاقتها مع الدول الأخرى وباقي أشخاص القانون الدولي، وهي حريصة على كسب الكثير من المعلومات أكثر مما تقدمه لغيرها ورغم ما تضمه الإتفاقيات الدولية من نصوص تلزم الدول وتدفعها إلى التعاون إلا أن الواقع يشير للكثير من الإحباط في هذا المجال، سيما إذا ما تعلق الأمر بالإجرام الذي يتعدى نطاق الدولة الواحدة، ذلك أن المعلومات ذات الصلة في هذا الجانب ترتبط بصورة أو أخرى بأمن الدولة القومي وسيادتها التي لا تريد أن تفرط بها، وتبالغ الدول عادة في الدفاع عن تلك السيادة.

أقرت العديد من الإتفاقيات هذا النمط من التعاون، أهمها ما ورد في الفقرة الثانية(2) من المادة الأولى(1) لمعاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية [1] وكذا ما ورد في البند الثالث والرابع والخامس من المادة الثامنة (8)لإتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، إذ أوجبت على الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي . ونفس الأمر أيضا على ما قضت به المادة الأولى(1) من إتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية، وفي هذا الإطار أيضا صاغ إتفاق شنغن للإتحاد الأوروبي نظاما متكاملا لتبادل المعلومات[2]

ثالثا نقل الإجراءات

وهو يقضي بقيام دولة ما بمقتضى إتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد التحقيق في جريمة معلوماتية ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توفرت مجموعة من الشروط، أهمها التجريم المزدوج والذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب نقل الإجراءات إليها بالإضافة إلى شرعية الإجراءات المطلوب إتخاذها، بمعنى أن تكون مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة وأن تكون هذه الإجراءات ذات أهمية من شأنها أن تؤدي دورا مهما في الوصول إلى الحقيقة. ولقد أقرت العديد من الإتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية، منها

[1] شريف علتم، محمد ماهر عبد الواحد، موسوعة اتفاقيات القانون الدولي الانساني، النصوص الرسمية للإتفاقيات والدول المصدقة والموقعة، لجنة الصليب الاحمر، 2022، ص 282

[2] المادة 43 الفقرة الثاني من االبروتوكول الاول الاضافي الى اتفاقية جنيف 1949 المتعلقة بحماية ضحايا المنازعات الدولية المسلحة 1977

معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية "، وكذا إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية"[1].

رابعا الإنابة القضائية الدولية

يقصد بهذه الصورة طلب إتخاذ إجراء قضائي من إجراءات الدعوى العمومية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك عند الفصل في مسألة معروضة لدى السلطة القضائية في الدولة الطالبة لتعذر قيامها بهذا الإجراء بنفسها، وهدف هذه الصورة تسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية، التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى لسماع شهود أو إجراء تفتيش أو غيرها[2]

ويحدث بدرجة متزايدة أن تشترط المعاهدات والإتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن : تعين سلطة مركزية عادة ما تكون وزارة العدل ترسل إليها الطلبات مباشرة بدلا من المرور عبر القنوات الدبلوماسية، وذلك بغرض التسريع في الإجراءات[3].

خامسا تسليم المجرمين

تسليم المجرمين صورة من صور المساعدة القضائية تهدف إلى تسليم شخص من طرف دولة إلى دولة أخرى من أجل محاكمته قضائيا أو تنفيذ لحكم جزائي حاز لقوة الشيء المقضى به، هذا النوع من التعاون بين الدول غير مؤسس على الصداقة كما كان عليه الحال من قبل لكن يهدف اليوم إلى التعاون من أجل مكافحة الإجرام الدولي مع ضمان حماية لحقوق الإنسان[4] .

ويعتبر تسليم المجرمين جزء مما أوصى به؛ مؤتمر الأطراف في إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة فضلا عن اقتفاء أثر الأسلحة النارية والذخيرة، باعتبارها مساهمة من الدول في مكافحة الإتجار غير المشروع بالأسلحة النارية وإرتباطه بالجريمة المنظمة.[5]

وهو نتيجة طبيعية للتطورات التي حدثت في كافة المجالات ومنها مجال الإتصالات وتقنية المعلومات، حيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم، كما أن نشاطهم الإجرامي لم يعد قاصرا على

[1] نعمان عطاء الله الهيتي، قانون الحرب او القانون الدولي الانساني، دار مؤسسة رسلان للطباعة والنشر والتوزيع، دمشق، 2008، ص 75

[2] نعمان عطاء الله الهيتي،نفس المرجع،ص 75

[3] صورية بورباية، المرجع سابق، ص 97

[4] فايزة ميموني، تسليم المتهمين بين مقتضيات التعاون القضائي الدولي وحقوق الانسان، مجلة الحقوق والعلوم الإنسانية، المجلد / 15 ،العدد01 : ص 1218

[5] مؤتمر الأطراف في : اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية التحديات القائمة والممارسات الجيدة في مجال مكافحة صنع الأسلحة النارية وأجزائها ومكوناتها والذخيرة والاتجار بها بصورة غير مشروعة والتدابير اللازمة التيسير تنفيذ بروتوكول المكمل الاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، ورقة معلومات أساسية من إعداد الأمانة العامة الأمم المتحدة في 11 ابريل 2014. الوثيقة رقم:CTOC COR WG2014/2

إقليم معين بل امتد إلى أكثر من إقليم، حيث بات المجرم منهم يشرع في التحضير لإرتكاب جريمته في دولة معينة ويقبل على تنفيذها في بلد آخر، وقد يفر إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة، فالمجرم المعلوماتي أصبح بالتبعية مجرما دوليا ولكون أنه لا يمكن لأي دولة أن تجاوز حدودها الإقليمية لممارسة أعمالها القضائية على المجرمين الفارين، كان لابد من إيجاد آلية معينة للتعاون مع الدولة التي ينبغي إتخاذ الإجراءات القضائية فوق إقليمها، تتمثل في تسليم المجرمين الفارين لسلطاتها وهذا الإجراء يقوم أساسا على أن الدولة التي يتواجد على إقليمها المتهم بإرتكاب جريمة معلوماتية عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة، فهو يحقق بذلك مصلحة الدولتين الأطراف في عملية التسليم، إذ يحقق مصلحة الدولة الأولى في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وفي ذات الوقت يحقق مصلحة الدولة الثانية المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون.

ولذلك فقد حرصت معظم الدول على سن التشريعات الخاصة بتسليم المجرمين ومنها المشرع الجزائري الذي أخذ بهذا الإجراء كمظهر من مظاهر التعاون الدولي بين السلطات القضائية الأجنبية في قانون الإجراءات الجزائية في المواد 694 وما يليها. ولقد تناولت اتفاقية بودابست الإجراءات الواجب اتباعها في تسليم المجرمين من دولة إلى أخرى بموجب المادة 24 فقرة 7 بقولها :" يقدم كل طرف وقت التوقيع أو عند إبداع وثيقة التصديق أو القبول، أو الموافقة أو الانضمام بإخطار السكرتير العام لمجلس أوروبا باسم وعنوان كل سلطة مسؤولة عن إصدار أو تلقي طلبات التسليم، أو أوامر الضبط التحفظي في حالة عدم وجود اتفاقية[1]

الفرع الثاني التعاون الفني أو التقني الدولي في مواجهة الجريمة السيبيرانية

لا يقتصر التعاون الدولي في مجال مواجهة الجريمة على المساعدة القضائية المتبادلة فحسب، وإنما يشمل كذلك المساعدة التقنية وتبادل الخبرات بين الدول، ذلك أن العنصر البشري سواء على مستوى الأجهزة القضائية أو الأجهزة الأمنية [2]ليس بذات الجاهزية والمستوى لمواجهة الجريمة المعلوماتية، وإنما يختلف من دولة إلى أخرى بحسب تقدم تلك الدولة ورقيها[3].

ونجد أن جميع الاتفاقيات الدولية أو الإقليمية ذات الصلة قد دعت صراحة إلى ضرورة وجود تعاون دولي في مجال التدريب ونقل الخبرات فيما بينها[4]، ذلك أن التقدم المتواصل في تكنولوجيات المعلومات يفرض على الجهات

[1] مرسوم رئاسي رقم 20-183 المؤرخ في 13 يوليو2020 ، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد40 ، الصادرة بتاريخ 2020/07/18.

[2] حيدر كاضم عبد علي، مبدأ التمييز بين المدنيين والمقاتلين، دراسة على ضوء القانون الدولي الانساني، مجلة الكلية الاسلامية الجامعة، النجف، العدد22، 2013، ص 419

[3] صورية بورباية، مرجع سابق، ص 98

[4] حيدر كاضم عبد علي، المرجع سابق، ص 422

القضائية والأمنية أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ،ومن ناحية أخرى إن إعمال القانون في مواجهة الجرائم المعلوماتية يستلزم إتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية لما تقسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها ومحو آثارها، وبالتالي فإن ظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئا ثقيلا على عاتق الأجهزة القضائية المختصة من قضاة تحقيق وقضاة حكم وكذا رجال الضبطية القضائية، لأجل ذلك كان لابد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة والقدرة في التعامل مع الجريمة المعلوماتية والمجرم المعلوماتي.

وعلى هذا الأساس كانت الدعوة إلى ضرورة وجود تعاون دولي في مجال تدريب رجال القضاء والضبطية القضائية للإستفادة من مهارات وتجارب الآخرين من خلال أشخاص أكفاء ومؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهلة ميسرة والتدريب المقصود هنا ليس التدريب التقليدي فحسب، فلا يكف أن تتوافر لدى رجال القضاء الخلفية القانونية، بل لابد من إكسابهم خبرة فنية في مجال الجريمة المعلوماتية.

وهذه الأخيرة لا تتأتى دون تدريب تخصصي يراعى فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب وبالنسبة للمنهج التدريبي فيجب أن يشمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الإختراقات الشبكة المعلومات وأجهزة الحاسب الآلي وتحديد أنماط ونوعية الجرائم المعلوماتية، وبيانا لأهم الصفات التي يتميز بها المجرم المعلوماتي والدوافع وراء ارتكابه للجريمة المعلوماتية

المطلب الثاني الآليات المؤسساتية الوطنية لمكافحة الجريمة السيبرانية:

خلال السنوات الأخيرة أصبح استعمال تكنولوجيا المعلومات والاتصال لأهداف إجرامية يشكل تحديا حقيقيا لجل الدول، والجزائر في إطار إستراتيجيتها الأمنية المبنية على مواكبة التطورات الحاصلة أنشأت مجموعة من الأجهزة تعد آليات تنفيذ للنصوص القانونية والتي من شأنها وضع حد والتقليل من هذه الجرائم السيبرانية نذكر منها :

الفرع الأول الهيئات الوقائية

1.مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية التابعة للدرك الوطني

:أنشئ هذا المركز سنة 2008 ويعتبر الجهاز الوحيد المتخصص لهذا المجال في الجزائر ويهدف أساسا الى تامين منظومة المعلومات لخدمه الامن العمومي من خلال مكافحته للجرائم المعلوماتية[1] .

2.المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني:

يعتبر مؤسسه عموميه ذات طابع اداري انشئ بموجب المرسوم الرئاسي رقم04-183 المؤرخ في 26 جوان 2004ومن مهامه:

[1] نبيل ق.ج، إنشاء مركز لمكافحة الجريمة المعلوماتية في الجزائر،تاريخ النشر 2008/05/17 تاريخ الإطلاع 2023/02/15 سا 15:10 Djazairess.com/alfadjr/71333

– القيام بالخبرات العلمية او خبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة من اجل كشف الحقيقة بالأدلة العلمية لتحديد هوية مرتكبي الجنايات والجنح .

– العمل على ترقية البحوث التطبيقية وأساليب التحريات التي اثبتت فعاليتها في ميادين علمي الاجرام والأدلة الجنائية على الصعيدين الوطني والدولي .

3. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها:[1]

حيث استحدثت هذه الهيئة بموجب القانون **09-04** وبقيت تشكيلتها وتنظيمها وكيفيات سيرها لتحدد عن طريق التنظيم والذي توالت فيه التغييرات ابتداء من المرسوم الرئاسي لسنة 2015 ثم سنة 2019 المرسوم الرئاسي لسنة 2020 ليعيد تنظيم الهيئة، وعرفها بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والإستقلالية المالية توضع تحت سلطة رئيس الجمهورية، ويحدد مقرها في الجزائر العاصمة، ويمكن نقله الى أي مكان من التراب الوطني بموجب مرسوم رئاسي، وتتكون الهيئة من مجلس توجيه ومديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية ويقدمان عرضا عن نشاطاتها[2]

الفرع الثاني: الهيئات الردعية

المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الامن الوطني: كما تبنى المشرع الجزائري إستراتيجية جديدة لمكافحة الجرائم المعلوماتية حيث قام بإنشاء منظومة وطنية لأمن الانظمة المعلوماتية بموجب المرسوم الرئاسي رقم20-05 مؤرخ في20 جانفي2020 ، وتعتبر هذه المنظومة اداة الدولة في مجال امن الانظمة المعلوماتية وتشكل الاطار التنظيمي لإعداد الاستراتيجية الوطنية لأمن الانظمة المعلوماتية وتنسيق تنفيذها.

وتشمل المنظومة الوطنية لأمن الانظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني على كل من مجلس وطني لأمن الانظمة المعلوماتية مهمته اعداد الاستراتيجية الوطنيه لأمن الانظمة المعلوماتية، والموافقة عليها وتوجيهها، وكذلك على وكالة لأمن الانظمة المعلوماتية، تكلف بتنسيق وتنفيذ الاستراتيجية الوطنية لأمن الانظمة المعلوماتية[3].

الخاتمة:

نخلص إلى أن الجرائم السيبرانية جرائم يصعب التحكم فيها والتصدى لها نظرا لخصوصيتها بإعتبارها جرائم عابرة للجغرافيا وأيضا بإعتبار أن التطور المذهل في الجانب التكنولوجي والإلكتروني صعب هو الآخر من مهمة مكافحة هذه الجريمة.

والدولة كعضو في المجتمع الدولي لا تستطيع بمفردها التصدي لمثل هذه الجرائم، فرغم المساعي الدولية للتعاون في شكل إتحادات إقليمية وعالمية للتصدي لهذه الجرائم السيبرانية إلا أن التحدي كان أكبر والخسائر في إرتفاع مستمر بجميع أشكالاها

[1] مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات المجلد/ 06 العدد02 ، 2021، ص 120

[2] المرسوم الرئاسي السابق رقم 20-183 المؤرخ في 13 يوليو 2020 .

[3] أنشأت بموجب –المرسوم رئاسي رقم 20-05 مؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

وعلى المستوى الوطني فإن سعي المشرع الجزائري في وضع منظومة تشريعية ومؤسساتية للتصدى لمثل هكذا جرائم، إلا أن الظاهرة في إنتشار مخيف خاصة بسبب نقص التكوين لمكافحتها وآليات التصدي لها، زد على ذلك تطور وسائل الإجرام بسبب تطور الآليات الإلكترونية والرقمية.

وعليه فإنه لا مفر من تضافر الجهود بين الدول ومواصلتها لتطوير القدرة على التعاون الدولي في مختلف مجالاته التشريعية والقضائية والأمنية .

– كما لابد من العمل على وضع ضوابط إسناد جنائية لتحديد الإختصاص الموضوعي والإجرائي وأن يتم صياغتها في إطار إتفاقيات دولية، وبشكل يسمح بتبادل التعاون سواء كان ذلك على مستوى جمع الأدلة أو تسليم المجرمين.

– توحيد أنماط وأشكال الجريمة المعلوماتية بتحديد معالمها الرئيسية على مستوى القوانين الوطنية للدول.

– إستجابة الدول لمكافحة الجريمة المعلوماتية يجب أن يكون بشكل أسرع لأن حفظ الأدلة المعلوماتية يتطلب ذلك كما يبرر هذا الأمر سهولة إخفائها من قبل الجناة أو تلاعبهم وإتلافهم لها.

– وضع نظام إتصال دولي يساعد جهات الشرطة والتي تعمل على التحقيق في الجريمة المعلوماتية الإتصال مباشرة بجهات أجنبية لجمع الأدلة والمعلومات مع سرعة الإستجابة

–تكريس التعاون بين الدول المتقدمة والدول النامية في مجال التدريب على التكنولوجيا الحديثة.

– على الدول العربية عقد المزيد من الإتفاقيات الدولية والإقليمية في إطار التعاون على المستوى التشريعي والقضائي والأمني وتبادل الخبرات.

قائمة المصادر المراجع

المصادر

.النصوص الدولية

1–البروتوكول الإضافي الأول 1977 لإتفاقية جنيف 1949 المتعلقة بحماية ضحايا المنازعات الدولية المسلحة

2–الأمانة العامة الأمم المتحدة في 11 ابريل 2014. الوثيقة رقم:CTOC COR WG2014/2

.النصوص الوطنية

1–القانون 18–04 المرخ في في 10 مايو2018 ، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر، عدد27 ، الصادرة بتاريخ 13 ماي 2018

2–القانون 18–07، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

3–القانون رقم 09–04المؤرخ في 14شعبان 1430سنة 2009يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ح ر ع 47صادر بتاريخ 2009/08/16

4– المرسوم رئاسي رقم 20–05 مؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية

5–المرسوم رئاسي رقم 20–183 المؤرخ في 13 يوليو2020 ، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد40 ، الصادرة بتاريخ 2020/07/18.

المـراجــع:

الكتب

1. شريف علتم، محمد ماهر عبد الواحد، **موسوعة اتفاقيات القانون الدولي الانساني**، النصوص الرسمية **للإتفاقيات** والدول المصدقة والموقعة، لجنة الصليب الاحمر، 2022.

2. عبد الله أحمد هلالي، **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة)**، دار النهضة العربية، القاهرة، 2000.

3. مدحت رمضان، **جرائم الاعتداء على الأشخاص والإنترنت**، دار النهضة العربية، 2000 .

4. نعمان عطاء الله الهيتي، **قانون الحرب او االقانون الدولي الانساني**، دار مؤسسة رسلان للطباعة والنشر والتوزيع، دمسق، 2008، ص 75

5. هلالي عبد اللاه أحمد، **الجوانب الموضوعية والإجرائية للجرائم المعلوماتية(على ضوء اتفاقية بودابست 2001)** دار النهضة العربية، ط 2001

المقالات

1. تومي يحي، **الحماية القانونية للمعطيات ذات الطابع الشخصي على الضوء القانوني رقم 18-07، دراسة تحليلية**، مجلةالأستاذ الباحث للدراسات القانونية والسياسية المجلد 04، جامعة مسيلة، الجزائر، 2019

2. حيدر كاضم عبد علي، **مبدأ التمييز بين المدنيين والمقاتلين، دراسة على ضوء القانون الدولي الانساني**، مجلة الكلية الاسلامية الجامعة، النجف، العدد22، 2013

3. صورية بوربابة، **التعاون الدولي في مكافحة الجريمة المعلوماتية**، مجلة القانون الدولي للدراسات البحثية، العدد01، 2019

4. فايزة ميموني، **تسليم المتهمين بين مقتضيات التعاون القضائي الدولي وحقوق الانسان**، مجلة الحقوق والعلوم الإنسانية، المجلد / 15 ،العدد01 .

5. قطاف سليمان، بوقرين عبد الحليم، **مواجهة الجرائم السيبرانية في ظل الاتفاقيات الدولية**، مجلة البحوث القانونية والاقتصادية ،المجلد 05، العدد 02، 2022.

6. مهدي رضا، **الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري**، مجلة إيليزا للبحوث والدراسات المجلد/ 06 العدد : 02، 2021.

7. مونة مقلاتي .راضية مشري،الجريمة الإلكترونية دلالة المفهوم وفاعلية المعالجة القانونية، مجلة أبحاث قانونية وسياسية،المجلد 6 العدد 1،جامعة 8ماي 1945،قالمة،جوان 2021

8. نشناش منية، **مداخلة حول الركن المفترض في الجريمة المعلوماتية**، جامعة بسكرة 2015ـ 2016،

التقـاريــر

1.**دراسة شاملة عن الجريمة السيبرانية**، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فيينا، 2013

المواقع الإلكترونية نبيل ق.ج، إنشاء مركز لمكافحة الجريمة المعلوماتية في الجزائر،تاريخ النشر 2008/05/17 تاريخ الإطلاع 2023/02/15 سا 15:10 Djazairess.com/alfadjr/71333

المراجع الاجنبية:

1. Cameron S. D. Brown**, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice",** International Journal of Cyber Criminology**.** Vol9, Issue 1, January – June 2015, p 57