جامعة عمار ثليجي الأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

بعنوان:

التعاون الإقليمي في مجال مكافحة الجريمة الإلكترونية

مذكرة ضمن متطلبات لنيل شهادة الماستر في الحقوق

التخصص :قانون جنائي وعلوم جنائية

إعداد الطلبة :

- خالدية قديري .
- حمزة دعماش.

إشراف الأستاذ:

- د.بن عرفة مُحَمَّد نذير .

لجنة المناقشة:

الإسم واللقب	الصفة
د.غريبي مُحَمَّد	رئيسا
أ.بن عرفه مُحَمَّد نذير	مشرفا ومقررا
د. سعودي علي	عضوا مناقشا

السنة الجامعية : 2025/2024م


بسم الله الرحمن الرحيم

وَلَا تَلْبِسُوا
ٱلْحَقَّ بِٱلْبَـٰطِلِ

إهداء

مهما كتبت من عبارات لن أجد أصدق من قول الله تعالى (يرفع الله الذين آمنوا منكم والذين نالوا العلم درجات » فحمدا كثيرا طيبا مباركا فيه.

ها قد طويت صفحة من صفحات الحياة كان فيها الجد والإجتهاد.

إلى نفسي التي قالت أنا لها سأنالها.

أنا اليوم أقف على عتبة تخرجي أقطف ثمار تعبي وأرفع قبعتي بكل فخر ....

إلى من جعل الجنة تحت أقدامها وسهلت لي الشدائد بدعائها.

الى الإنسانة العظيمة أمي الحبيبة.

إلى من كلل العرق جبينه...

إلى من علمني أن النجاح لا يأتي إلا بالصبر والاصرار....

إلى النور الذي أنار دربي والسرج الذي لا يضفي نوره.... إلى أعظم وأعز رجل في الكون أدامك الله لي طول العمر.....أبي الغالي .

. إلى الجوهرة النادر منبع الحنان ونبع العطاء جدتي الغالية غانية رحمها الله تعالى واسكنها فسيح جناته.

إلى مصدر قوتي والداعمين والساندين لي إلى ضلعي الثابت وامان أيامي إخواني الغاليين وأخواتي الغاليات.

إلى إخواني الذي سلكوا معي طريق النجاح حتى النهاية حيزية . هدى.....

إلى زوجة أخي نادية وكتاكيتها الصغار: ايمان – شهاب – بيان – يحي –رضوان.

إلى أعز صديقاتي اللواتي قضيت معهم أحلى اللحظات: وهبية – روبة – محجوبة – حبيبة – سارة – أصالة .

إهداء

الحمد لله الذي خلقني فسوى

خلقي والذي يصعد اليه الدعاء والذي كلما ذكرت اسمه شرح لي صدري فلك الحمد يا ذا الجلال والإكرام وصلى اللهم وسلم على سيدنا مُحَمَّد وعلى آله وصحبه أجمعين اهدي ثمرة مجهودي الى التي يعجز اللسان عن وصف فضلها والتي سهرت عليا الليالي وغمرتني بعطفها الى منبع الحنان ونور حياتي الى امي الغالية. كما أهديها الى من احمل اسمه بكل فخر حفظك الله ورعاك والدي والى سندي في حياة زوجتي الغالية واخوتي وأولادي كل واحد باسمه ادامكم الله نعمة وحفظك من كل شر واطال الله في أعماركم.

والى كل واحد ساعدني في انجاز هذا عمل

شكر وتقدير

الحمد لله على توفيقه وإحسانه والحمد لله على فضله وإنعامه

الحمد على وجوده وكرمه

اشكر الله عز وجل الذي أمدنا بعونه ووهبنا من فضله ومكننا من إنجاز هذا العمل

كما يسعنا أن نتقدم بجزيل الشكر إلى كل من ساهم في تكويننا ونخص بالذكر الأستاذ الفاضل

الدكتور **بن عرفة مُحَمَّد نذير**

الذي تكرم بالإشراف على هذه المذكرة ولم يبخل علينا بنصائحه الموجهة للخدمة فكان لنا

نِعْمَ الموجه والمرشد.

كما لا يفوتنا أن نشكر أعضاء لجنة المناقشة الذين تشرفوا بمعرفتهم وتقيمهم لمجهودنا.

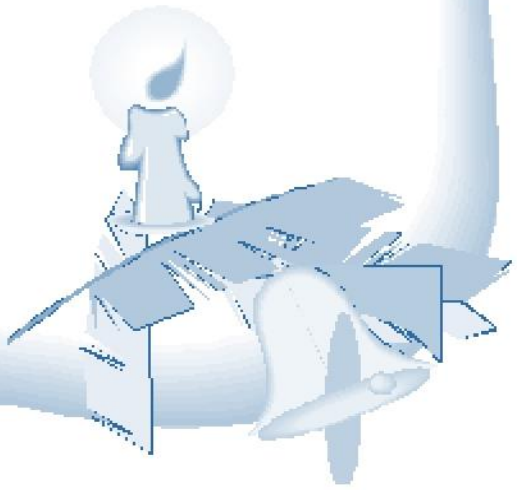
كما نتوجه بالشكر الخالص لكل أساتذة قسم الحقوق وإلى كل من ساعدنا من قريب أو بعيد

وساندنا في إنجاز هذا البحث حتى ولو بكلمة طيبة.

والشكر الكبير إلى كل من ساهم من قريب أو من بعيد لإتمام هذا العمل.

خالدية

حمزة



مقدمة:

شهد العالم تطور كبير في شتى المجالات الإقتصادية والاجتماعية والسياسية والثقافية والعلمية وغيرها، وتزامنا مع هذا التطور ظهرت بعض المسائل السلبية من بينها بهذا التطور ظاهرة الإجرام، فبعدما كان المجتمع يعرف الجريمة بمفهومها التقليدي، وكان يواجهها بالتشريعات والقوانين اللازمة في حينها، أصبح العالم الآن مع بزوغ فجر الثورة المعلوماتية وانتشار شبكة الأنترنت في جميع أقطاره يعرف جرائم جديدة لم يكن لها مثيل من قبل خاصة بعد توسع استخدام شبكة الأنترنت من جميع فئات المجتمع وفي شتى مجالاتها وهذه الجرائم يطلق عليها ما يسمى بالجرائم الإلكترونية أو المعلوماتية...

وبتزايد استخدام هذه التقنية من طرف القطاع العام والقطاع الخاص والمؤسسات الإقتصادية، وحتى المواطنين فيما بينهم، تزايد تطور أساليب هذه الجريمة والتي شملت عدة صور منها صناعة ونشر الفيروسات، الاختراقات، تعطيل الأجهزة، التجسس والتصنت، جرائم تبييض الأموال، والإتجار بالمخدرات، وجرائم الآداب العامة، وجرائم الإرهاب وغيرها....

لذا اصبح من الضروري التدخل التشريعي لدول العالم باستصدار قوانين وتشريعات لمواكبتها ومواجهتها بالإضافة إلى إبرام اتفاقيات بين الدول لمجابهة هذه الظاهرة وايجاد حلول تقنية وتكوينية لأجهزة الأمن والقضاء وغير ذلك.

وتوسيع مجالات التعاون البحث عن وسائل وسبل لمكافحة الجرائم الإلكترونية من اصدار لقوانين وتشريعات في هذا المجال، وابرام اتفاقيات مع دول أخرى .

تكمن اهمية دراستنا لهذا الموضوع بتسليط الضوء على الجريمة الالكترونية. وكذا الآليات القانونية لتأمين تكنولوجيا الاتصال الحديثة من الممارسات الإجرامية التي ارتبطت بها.

بالإضافة الى الفراغ القانوني المتعلق بهذا النوع من الجرائم وعدم قدرة النصوص العقابية على مسايرة التطور الغالب على هذا النوع من الجرائم وصعوبة اثباتها عن طريق الأدلة المتحصل عليها من الوسائل الإلكترونية مما يساهم بشكل كبير في فرار الجناة من العقاب.

كما تسمح لنا هذه الدراسة بقدر الإمكان معرفة هذا النوع من الجرائم، وبيان سبل مواجهتها تشريعيا سواء داخليا أو إقليميا حيث أن هذا الوضع أدى إلى قيام العديد من الدول بسن قوانين داخلية، وعقد اتفاقيات دولية لمواجهة هذا التطور المذهل والغير متكافئ في مجال المعلوماتية والاتصالات.

أما عن أسباب اختيار الموضوع فنرجع إلى الرغبة في التعرف على الجريمة الإلكترونية باعتبارها من الجرائم المستحدثة والمستفحلة في وقتنا الحالي وباعتبارها متعلقة بالعالم الافتراضي وكذا من اجل الزيادة في الرصيد المعرفي خصوصا لما لمسه من غموض ومستجدات واشكاليات افرزها في الواقع العملي .

أما الأسباب الموضوعية فتتمثل في انتشار وتفشي هذه الظاهرة على المستوى الوطني والإقليمي، باعتبارها ظاهرة لا تعرف الحدود التقليدية، وما يترتب عليها من أضرار جد خطيرة تمس شتى مجالات الحياة " الإقتصادية، الإجتماعية...،"، الأمر الذي استوجب الحسم في مواجهة هذه الظاهرة بإصدار أحدث التشريعات داخليا ودوليا.

ان الهدف من هذه الدراسة هو محاولة معرفة هذا النوع من الجرائم المستحدثة من خلال :

– تسليط الضوء على ظاهرة إجرامية تزداد بمعدلات قياسية خاصة مع الانتشار الهائل لاستعمال جهاز الكمبيوتر واستعمال المتزايد لاستعمال جهاز الكمبيوتر واستعمال المتزايد لشبكة الأنترنت .

– تحديد التعريفات الخاصة بالجريمة الإلكترونية وخاصة التعريف الفقهي والقانوني .

– إضافة إلى تحديد الخصائص التي تقوم عليها الجريمة الإلكترونية وتبيان البنيان القانوني لهذه الظاهرة من أركانها وانواعها.

–دراسة التشريع الجزائري وتبيان مدى تطور الآليات الدولية في معالجة الجريمة الإلكترونية وتبيان الإتفاقيات الدولية في مجال مكافحتها.

– تبيان مدى مساهمة التعاون الإقليمي في مكافحة الجريمة الإلكترونية .

رغم أن البحث في الجريمة الالكترونية ليس بالأمر الهين نظرا لحداثة هذا النوع من الجرائم وأنواعها المختلفة وما تتطلبه من معرفة ببعض الجوانب التقنية الدقيقة وفضلا عن صعوبة المصطلحات العلمية بالإضافة إلى انها لا تزال مجالا جديدا ضمن الدراسات المتعلقة بالقانون الجنائي والعلوم الجنائية في الجزائر ناهيك عن قلة الأحكام القضائية المتعلقة بالجرائم الإلكترونية وندرة التطبيقات المتعلقة بتفعيل آليات التعاون الإقليمي في هذا المجال .

وعليه فالإشكالية الرئيسية التي يمكن طرحها في هذا السياق:

–ما مدى فعالية آليات التعاون الإقليمي في مكافحة الجريمة الإلكترونية؟

– وللإجابة على هذه الإشكالية المطروحة قمنا بتقسيم البحث الى فصلين:

مقدمة:

الفصل الأول تطرقنا فيه إلى الإطار المفاهيمي للجريمة الالكترونية وذلك من خلال التعرض لمفهوم الجريمة الالكترونية في المبحث الاول والتعرض للمعالجة القانونية للجريمة الالكترونية في التشريع الجزائري في مبحث ثان.

اما الفصل الثاني فقمنا بالتطرق الى التعاون الثنائي والإقليمي لمكافحة الجريمة الإلكترونية بحيث خصصنا المبحث الاول لمجالات التعاون والمبحث الثاني لمدى فعالية التعاون الإقليمي لمكافحة الجريمة الإلكترونية.

واعتمدنا في دراستنا لهذا الموضوع على المنهج الوصفي ، وذلك من خلال تبيان ووصف وتشخيص موضوع البحث في مختلف جوانبه وابعاده.

الفصل الأول

الإطار المفاهيمي للجريمة الإلكترونية

تمهيد:

تعد الجرائم الإلكترونية صنفا مستحدثا من الجرائم التي وجب التنبه لمخاطرها وحجم الأضرار الناتجة عنها حيث أصبح الحاسب الآلي ركيزة أساسية في عصرنا فقد تعدى دوره إجراء العمليات الحسابية ليشمل مختلف مجالات الحياة ومن خلال الشبكات المتصلة به أصبح العالم عبارة عن قرية صغيرة يسهل فيها الحصول على المعلومات بسهولة وسرعة فائقة فقد أصبحت معظم القطاعات تعتمد على إستخدام الأنظمة المعلوماتية في أداء عملها وذلك لمعالجة ونقل وتخزين وتبادل المعلومات بين الأفراد والمؤسسات المختلفة في الدولة الواحدة أو بين مجموعة من الدول ,مما أدى لظهور الجريمة الإلكترونية وهذا ما يستلزم إعطاء صورة عامة لتحديد ماهيتها فاختلاف الاجتهادات للاتفاق على التعريف الموحد لها مرجعه سرعة تطورها وهذا ما دفع الجهات المعنية للتصدي لها سواء على الصعيد الوطني أو الإقليمي عن طريق التعاون الإقليمي في مكافحتها ومواجهة خطورتها لذلك سنحاول التطرق في هذا الفصل الى مفهوم الجريمة الإلكترونية في المبحث الاول والمبحث الثاني سنتطرق فيه الى المعالجة القانونية للجريمة الالكترونية في التشريع الجزائري.

المبحث الأول: مفهوم الجريمة الإلكترونية.

تتنوع الجرائم وتختلف بإختلاف وسائلها وطرقها ,وتعتبر الجرائم الإلكترونية من اخطرها وأصعبها كونها تعتمد على التكنولوجيا المتطورة وتخطيها للحدود الإقليمية وتغير اشكالها وتقنياتها وتعدد اركانها، هذا ما زاد من صعوبة تحديد تعريف واحد ومتفق عليه لها وضبط مفهومها وخصائصها وهو ما سنتطرق اليه في هذا المبحث

المطلب الأول: تعريف الجريمة الإلكترونية

الفرع الأول : تعريف الجريمة الإلكترونية فقها:

لقد اختلف الفقهاء حول وضع تعريف موحد للجريمة الإلكترونية ويعود ذلك الاختلاف حول تحديد نطاق هذه الجريمة فالبعض من الفقهاء ينظر إليها بمفهوم ضيق والبعض الآخر ينظر إليها بمفهوم موسع وهذا ما سيتم تبيانه من خلال :

أولا: الاتجاه المضيق من تعريف الجريمة الإلكترونية :

يعرفها أنصار هذا الاتجاه بأنها" كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم إرتكابها من ناحية ولملاحقته وتحقيقه من ناحية أخرى[1]."

فحسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لإرتكاب الجريمة بل كذلك لملاحقتها ، والتحقيق فيها وهذا التعريف يضيق بدرجة كبيرة من الجريمة الالكترونية، بمعنى يجب أن يتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة، والمختصين بملاحقتها من قضاة وضباط الشرطة وغيرهم. وهناك من يعرفها على أنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب أوهي الفعل الاجرامي الذي يستخدم في اقترافها الحاسوب باعتباره أداة رئيسية .

كما عرفها الأستاذ mass على أنها " الإعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح[2]."

---

[1] نايري عائشة ،**الجريمة الإلكترونية في التشريع الجزائري** ،مذكرة لنيل شهادة الماستر في القانون الإداري ،،جامعة أحمد دراية ،أدرار سنة 2016/2017 ص6 .

[2] بن منصور ،صالح .السلوك الإجرامي للمجرم المعلوماتي ،مذكرة لنيل شهادة ماستر في الحقوق ،جامعة عبد الرحمان ميرة ،بجاية ،سنة 2014/2015 ص8

اما الفقيـه الألمـاني tiedemann يرى انها " كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بإستخـدام الحاسب. بحيث يرتكز في تعريفه هذا على وسيلة إرتكاب الجريمة.

ويرى الأستاذ rosenblatt بأن الجريمة الإلكترونية :هي "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه".

حسب هذا التعريف فإن الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكابها تخرج من نطاق التجريم[1].

وعبر عنها البعض الآخر بأنها " جرائم الأموال وجرائم الأشخاص وجرائم المصلحة العامة التي تقع عن طريق إستعمال شبكة الانترنت سواء داخل البلاد أو خارجها نرى من خلال هذه التعريفات أن أصحاب الاتجاه المضيق في تعريفهم للجريمة الإكترونية أنهم أخذو الوسيلة كأداة لإرتكاب هذه الاخيرة.

ثانيا : الإتجاه الموسع من تعريف الجريمة الإلكترونية .

على عكس الإتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة، وبالتالي هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا، وذلك باستخدام شبكات الانترنت من خلال غرف الدردشة، واختراق البريد الإلكتروني ومختلف وسائل التواصل الإجتماعية، بهدف إلحاق الضرر لفرد أو مجموعة من الأفراد، وحتى لدولة من الدول تكون ضمن برنامج الإستهداف الحربي، أو الإقتصادي، أو الإضرار بسمعتها أو العكس، ويبقى الهدف واحد، وهو الكشف عن قضايا مستتر عليها، أو نشر معلومات لفائدة طرف أو أطراف اخرى من باب التسريب.

ويرى الخبير الأمريكي parker أن الجريمة الإكترونية هي" الأفعال الإجرامية المتعمدة ذات الصلة بالمعلوماتية التي يحقق منها الفاعل مكاسب وتلحق خسائر بالمجني عليه" .

كما عرفها البعض على أنها كل فعل أو امتناع عمدي ، ينشأ عن الإستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الإعتداء على الأموال أو الأشياء المعنوية .

ويعرفها الأستاذ vivant وhestanc :أنها مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب.

[1] بعرة سعيدة ، **الجريمة الإلكترونية في التشريع الجزائري** ،مذكرة لنيل شهادة ماستر في الحقوق ،جامعة محمد خيضر ،بسكرة ،سنة 2015/2016 ص10 .

الفرع الثاني : التعريف القانوني للجريمة الإلكترونية

عرفها المشرع الجزائري في المادة الثانية من القانون 04/09 والتي سماها " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بأنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الالكترونية "[1].

هنا المشرع الجزائري اعتمد في تعريف الجريمة المعلوماتية على معيارين هما، معيار موضوع الجريمة، ومعيار وسيلة ارتكاب الجريمة .

أولا :التعريف على أساس معيار موضوع الجريمة :

اعتمد المشرع الجزائري موضوع أو محل الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات كأساس لتحديد الجريمة المعلوماتية، وهي الجرائم المحددة في الفصل السابع مكرر من قانون العقوبات تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات "، والتي تحكمها المواد من 394مكرر إلى 394 مكرر 7 من هذا القانون .

ثانيا : التعريف على أساس معيار وسيلة ارتكاب الجريمة :

بالإضافة إلى الاستناد في تحديد الجريمة الإلكترونية على موضوع الجريمة، أضاف المشرع الجزائري معيار آخر لتحديدها وهو وسيلة ارتكاب الجريمة وتتمثل المنظومة المعلوماتية، أو نظام الإتصالات الالكترونية بقول " ...وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الاتصالات الالكترونية، فوسيلة ارتكاب الجريمة أو تسهيل ارتكابها في هذا التعريف هي محل اعتبار في تكييف الجريمة ، وهذا ما نص عليه الأمر رقم 11/21 المتمم للأمر رقم 66/155 والمتضمن قانون الإجراءات الجزائية، وذلك في المادة 211 مكرر 22 فقرة3 .

وهنا يمكن القول أن الجريمة الإلكترونية حسب القانون الجزائري تنقسم إلى قسمين القسم الأول يضم ، الجرائم التي ترتكب ضد نظام المعالجة الآلية للمعطيات، وتستهدف المساس الكلي أو الجزئي بهذه المنظومة[2]، وهي الجرائم المنصوص عليها في الفصل السابع مكرر من قانون العقوبات تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات "، فيما يتضمن القسم الثاني كل الجرائم الأخرى المنصوص

[1] القانون رقم 09/04 الصادر في 5اوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،ج، ر العدد 47.

[2] مسعود شهيرة ،**الجريمة الإلكترونية في التشريع الجزائري** ،مذكرة لنيل شهادة الماستر ،جامعة عبد الحميد بن باديس مستغانم ص9

عليها في قانون العقوبات، أو في القوانين الخاصة التي يتم ارتكابها، أو يتم تسهيل ارتكابها باستخدام منظومة معلوماتية.

الفرع الثاني : خصائص الجريمة الإلكترونية :

تتميز الجريمة الالكترونية بصفة عامة عن الجريمة التقليدية من عدة جوانب ،بمجموعة من الخصائص إذ أن التعرف على خصائص هذه الجريمة يمكن أن يساعد في إيجاد الحلول لمكافحتها ،وتتمثل فيما يلي[1]:

أولا: الجريمة الإلكترونية جريمة عابرة للحدود: اي انها غير مرتبطة بمنطقة جغرافية معينة بل تتخطى حدود الدولة فهي تتميز بالبعد الدولي بين الجاني والمجني عليه وهذا ما خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي والقانون الذي يجب تطبيقه لردع لهذه الجريمة.

✓ **خفاء الجريمة** :بحيث تفسر بأنها خفية ومستترة في أغلبها لأن الضحية لايلاحظها رغم أنها قد تقع أثناء وجوده على شبكة الاتصال ، ولأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة ، مثال عند ارسال الفيروسات المدمرة وسرقة الاموال والبيانات الخاصة أو اتلافها ، والتجسس عليها وسرقة المكالمات وغيرها.

ثانيا: سرعة تنفيذ الجريمة : اي انها لا تتطلب وقت طويل فقد تتم في ثانية أو جزء من الثانية في بعض الجرائم . فمثلا بضغطة واحدة على لوحة المفاتيح او عبر الهاتف يمكن للمجرم الالكتروني تحويل ملايين الدولارات من مكان الى آخر .

ثالثا: ترتكب في بيئة رقمية معلوماتية قوامها النظم المعلوماتية الحاسوبية: بمعنى تتم بواسطة المكونات المادية للحاسوب ومكوناته البرامجية.

رابعا: يقوم بها المجرم ذو طبيعة خاصة وإمكانات خاصة: بحيث يستخدم في ارتكاب جريمته الموارد المعرفية والأساليب الاحترافية.

خامسا: صعوبة الحصول على دليل مادي في مثل هذه الجرائم: حيث تغلب الطبيعة الالكترونية على الدليل المتوفر وتزداد صعوبة كشف الدليل بصورة خاصة متى ارتكبت هذه الجريمة في مجال العمل من قبل العاملين ضد المؤسسات التابعين لها ، فبحكم الثقة في هؤلاء يسهل عليهم اقتراف جرائمهم دون أن يتركوا آثارا تدل عليهم .

[1] فريد ناشف ،**آليات التعاون الدولي في مكافحة الجريمة الالكترونية** ،مجلة البحوث في الحقوق والعلوم السياسية المجلد 8 العدد1 سنة 2022 ص 435 .

سادسا: الجريمة الإكترونية تستلزم طرقا خاصة مستحدثة للإثبات: قوامها كالتعليم التدريب المتخصص المستمر لعلوم الحاسب الآلي ، لذا فإنها تقتضي وجود رجل شرطة إلكتروني ، ومحقق إلكتروني ، وقاضي إلكتروني ، فضلا عن الخبير الإلكتروني حتى يتم كشف الجريمة وتعقب الجناة فيها ومحاكمتهم ، وعليه فإن الاستعانة بالخبراء تصبح حتمية لكشف وتحليل وتفسير الدليل الجنائي ، الذي يثبت البراءة أو الادانة ، فهذه الجريمة لا يحدها مكان ، فهي عالمية إذ يمكن عن طريق الآلي أو في هاتف نقال لشخص في الصين مثال أن يرتكب جريمة تزوير أو سرقة معلومات أو نقود ، ضد شخص طبيعي أو معنوي في الو.م.أ أو العكس [1].

سابعا: تدني نسبة الابلاغ عن الجريمة من طرف المجني عليه: خاصة في حالة شركات ومؤسسات ، لتجنب الإساءة للسمعة و الرغبة في عدم زعزعة ثقة العملاء.

ثامنا:غالبا ما تكون الخسارة الناجمة عنها فادحة للمجني عليه.

تاسعا: الجريمة الالكترونية من الجرائم الناعمة: بحيث تبرز بوضوح في أسلوب ارتكابها و طريقتها ، فإن كانت الجريمة التقليدية تتطلب نوعا من أسلوب العضلي والعنف الذي قد يكون في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة .

فهي تتطلب الجهد الذهني من طرف المجرم وشبكة المعلومات الدولية – الانترنت –اي انه مع وجود مجرم محترف يوظف خبراته وقدراته على التعامل مع الشبكة ، للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير او السطو الالكتروني على أرصدة البنك. تتحقق الجريمة دون الحاجة لسفك الدماء.

عاشرا: الجريمة الإلكترونية تتم عادة بتعاون أكثر من شخص على ارتكابها اضرارا بالمجني عليه : وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت فيقوم بالجانب الفني من المشروع الإجرامي ، وشخص اخر من المحيط أو من خارج المؤسسة المجني عليها ، لتغطية عملية التلاعب و تحويل المكاسب .

المطلب الثاني : اركان الجريمة الالكترونية وانواعها.

الفرع الاول : اركان الجريمة الالكترونية:

اختلف الفقهاء في تحديد أركان الجريمة الإلكترونية حيث رأى بعضهم أن الجريمة تقوم على ركنين اثنين فقط هما الركن المادي والمعنوي , ويستبعد هذا الفقه الركن الشرعي باعتبار أن الصفة غير المشروعة

[1] داود وسيلة . **الجريمة الإلكترونية على ضوء القانون العقوبات الجزائري** ، مذكرة لنيل شهادة الماستر، جامعة عبد الحميد بن باديس ،مستغانم ،سنة 2019 ص 21.

للفعل تتجدد على ضوء نموذج الجريمة ,فهي العلاقة بين الفعل المرتكب والوصف القانوني، وبالتالي فهي تكشف عن وقوع الجريمة ولا تعتبر جزءا فيها ،ومن أنصار هذا الرأي ديكوك وجانديدي حيث ذكرا بأن النص القانوني ليس ركنا من أركان الجريمة إنما هو عامل الردع .

وذهب بعضهم إلى أن أركان الجريمة ثلاثة: الركن الشرعي ، المادي والمعنوي.

أولا: الركن الشرعي :

إن الجريمة هي نتيجة لأفعال مادية صادرة عن الإنسان فهي تختلف حسب نشاطاته.

مما جعل المشرع يتدخل لتجريم هذه الافعال الضارة بموجب نص قانوني يحدد فيها الفعل الضار أو المجرم والعقوبة المقررة لارتكابه .

ينطبق مبدأ الشرعية على تعريف الجرائم وعلى تحديد العقوبات وتدابير الأمن التي تطبق على شخص معين , فالقاعدة الأساسية الناتجة عن هذا المبدأ هي عدم رجعية القانون الجنائي فلا يجوز للقاضي تجريم الفعل ما لم يجرم بنص , ولا توقيع عقوبة.

فالقاضي الجنائي عند تفسيره لنصوص القانون يفسره تفسيرا ضيقا, أي عدم لجوء القاضي الجنائي لقياس فعل لم يرد نص بتجريمه على فعل و رد نص بتجريمه فيقرر القاضي الجنائي للأول عقوبة الثاني للتشابه بين الفعلين.

بحيث تستمد الجرائم الالكترونية شرعيتها من مختلف التشريعات الوطنية الصادرة بشأن الجريمة الالكترونية فقد بذلت هيئة الأمم المتحدة جهودا كبيرة إضافة إلى جهود المجلس الأوروبي لإقناع الدول بوضع تشريعات للتصدي ومواجهة ومكافحة جرائم الالكترونية وتعزيز التعاون الإقليمي في هذا المجال.

فعلى المستوى الوطني نجد أن معظم التشريعات الوطنية تناولت نصوص مستحدثة لمواجهة الإجرام الإلكتروني فمثلا التشريع الجزائري أصبحت المعلوماتية من وسائل ارتكاب الجرائم ,حيث عدل المشرع الجزائري قانون العقوبات من خلال القسم السابع منه ,حيث تناول جرائم المساس بأنظمة المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات ولم يكتف المشرع الجزائري بذلك فقد فرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون 06/23 المؤرخ في 20/12/2006 وإقراره بالمادة 303 مكرر إلى 03 للتصدي للاستخدام السيء لوسائل التكنولوجيا الحديثة[1].

[1] أحسن بوسقيعة ،**الوجيز في القانون الجزائري العام** ،ط3 ،دار هومة للنشر ،الجزائر 2006 ص 27 .

ثانيا الركن المادي:

هو كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا يؤدي إلى نتيجة تمس حقا من الحقوق , التي يكفلها الدستور والقانون .

فقد ذهب الدكتور رضا فرح إلى تقسيم الركن المادي في حد ذاته إلى ثلاث عناصر :

1/ السلوك الإجرامي : فقد يكون بفعل إيجابي وهو قيام الجاني بفعل إرادي بغية إحداث نتيجة معينة , كما يمكن أن يكون بفعل سلبي يأخذ وصف الامتناع عن إتيان أمر يوجبه المشرع . ففي الجريمة الإلكترونية يمكن أن نجده بنوعيه السلوك الإيجابي أو السلبي .

2/النتيجة الإجرامية: تقوم على أساس ما يعتد به المشرع ومايترتب عليه من نتائج بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى .

3/العلاقة السببية : تتمثل العلاقة السببية في الصلة التي تربط بين الفعل والنتيجة وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة وأهمية الرابطة السببية ترجح إلى إسناد النتيجة إلى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة وتحقق الرابطة السببية تلازما ماديا بين الفعل والنتيجة ذلك أنه لا شروع في الجرائم غير العمدية.

-يقوم الركن المادي للجريمة الإلكترونية على صورتين أساسيتين [1]:

أ/الصورة الأولى: متمثلة في الاعتداء على نظام المعالجة الآلية وتحتوي على نوعين من الإعتداء :

النوع الأول: وهو الدخول والبقاء الغير مشروع في نظام المعالجة الآلية يشمل هذا النوع ثلاث أفعال فعل الدخول والبقاء والعرقلة أو التعطيل .

النوع الثاني : متمثل في الاعتداء العمدي على نظام المعالجة الآلية للمعطيات وتندرج تحت هذا النوع كذلك ثلاث أفعال وهي فعل الإدخال والحذف والتعديل .

ب/الصورة الثانية متمثلة في الإعتداء على منتجات الإعلام الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي.

الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات :

نصت المادة 394 مكرر من قانون العقوبات الجزائري على أنه " يعاقب بالحبس من ثلاث أشهر إلى سنة وبغرامة من 50.000 دج إلى10.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك .

[1] بلعليات ابراهيم ،**اركان الجريمة وطرق اثباتها في قانون العقوبات الجزائري** ،ط1 دار الخلدونية ،الجزائر 2007 ص 17 .

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 إلى 150.000 دج نستخلص وجود صورتين لفعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات الصورة الأولى تتمثل في:

الصورة البسيطة : بحيث نجد النشاط الإجرامي في هذه الصورة في الأفعال التالية :

أ- فعل الدخول : يتحقق بمجرد الوصول إلى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبها لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن مقابل نفقات.

يرتكب فعل الدخول بأية طريقة أو وسيلة كانت لأن المشرع الجزائري لم يحددها.

إن جريمة دخول غير مصرح بها إلى نظام المعالجة الآلية للمعطيات يعد في التشريع الجزائري جريمة شكلية لانها لا تشترط تحقق النتيجة , يكفي الوصول إلى المعلومات المخزنة بداخل النظام فبمجرد الوصول إليها تقوم الجريمة.

ب / فعل البقاء : وهو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام ويتحقق هذا البقاء غير المشروع عند دخول شخص في نظام بتصريح ولكن تجاوز المدة المسموح له بالبقاء أو يقوم بطبع نسخة من المعلومات في حين سمح له بالرؤية فقط هنا تقوم جريمة البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

الصورة المشددة: إن ظرف تشديد ظرف مادي تربط بينه وبين الجريمة العمدية الأساسية علاقة سببية لكي نقول أن الشرط متوفر.

وقد نصت المادة394 مكرر الفقرة 2 و3 من قانون العقوبات الجزائري على ظروف تشديد عقوبة فعل الدخول والبقاء غير المشروع اذا ينتج عن هذين الفعلين إما محو أو تحويل للمعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائفه[1].

النوع الثاني : الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات :

بالنسبة للمشرع الجزائري لم يورد نصا خاصا بالاعتداء العمدي على سير النظام واكتفى بالنص على الإعتداء العمدي على المعطيات الموجودة داخل النظام وهذا راجع إلى تفسير أن الإعتداء على المعطيات قد يؤثر على صلاحية النظام ووظائفه.

[1] المادة 394 مكرر من قانون العقوبات الجزائري.

كذلك نصت المادة 394 مكرر 2 من قانون العقوبات الجزائري على الإعتداءات العمدية بنصها " يعاقب بالحبس من شهرين الى ثلاث سنوات وبغرامة من 1000000 إلى5000000 دج كل من يقوم عمدا أو عن طريق الغش بما يلي :

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم .

–حيازة أو إفشار أو نشر واستعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

1/الاعتداءات على منتوجات الإعلام الآلي والتزوير المعلوماتي :

هي الفعل الثاني لتحقق الركن المادي للجريمة الإلكترونية فيعد هذا الفعل من أخطر صور الغش المعلوماتي نظرا لما يتمتع به الحاسب الآلي من خطورة.

بحيث نجد أن المشرع الجزائري رغم تداركه من خلال القانون 04/15 المتضمن قانون العقوبات الفراغ القانوني في مجال الإجرام الإلكترونية وذلك بتجريم الاعتداءات الواردة على منتوجات الإعلام الآلي فلم يستحدث نصا خاصا بالتزوير المعلوماتي ولم يتبنى الاتجاه الذي تبنته التشريعات التي عملت على توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث .

ثالثا: الركن المعنوي:

هو العلاقة التي تربط ماديات الجريمة وشخصية الجاني فهو الحالة النفسية له.

ولقيام الركن المعنوي للجريمة الإلكترونية يكفي توافر العلم والإرادة أي القصد العام، والجريمة الإلكترونية كما سبق القول من الجرائم العمدية فمتى تطابق السلوك مع الصور التي تصلح تتشكل جريمة إلكترونية, حسب معايير كل دولة يتحقق الركن المعنوي. إلا أنه قد ترتكب هذه الجرائم عن غير قصد , فمثلا في جريمة الدخول غير المشروع إلى النظام يعتقد الجاني أنه مازال له حق الدخول إلى النظام الآلي كأن يكون قد سبق له الاشتراك في الدخول إلى البرنامج ولكن مدة الاشتراك قد انتهت ومع ذلك دخل إلى النظام استنادا إلى هذا الإعتقاد الخاطئ لأن الغلط في الأمر الجوهري ينفي القصد[1].

ويختلف الركن المعنوي للجريمة الإلكترونية باختلاف أنواعها وسنرى ذلك في ما يلي:

[1] حشيفة عبد الهادي' ، **التعاون الدولي في مكافحة الجرائم الإلكترونية**، مذكرة لنيل شهادة الماستر في الحقوق، جامعة زيان عاشور ،الجلفة سنة 2020 ص26 .ص 27

1.جريمة الدخول والبقاء غير المشروع داخل المعالجة الآلية للمعطيات :

تعتبر هذه الجريمة من الجرائم العمدية التي تتطلب قصدا جنائيا وذلك حسب نص المادة 394 مكرر قانون العقوبات الجزائري التي عبرت عن القصد الجنائي بنصها "كل من يدخل أو يبقى عن طريق الغش "ولا يتوافر القصد الجنائي إذا كان الجاني يعتقد أن دخوله أو بقاءه داخل النظام مسموح به أي مشروع أو كان الجاني يجهل بوجود حظر الدخول أو البقاء.

جريمة الإعتداءات على سير نظام المعالجة الآلية للمعطيات :تعد هذه الجريمة جريمة عمدية لأن أفعال العرقلة والتعطيل من الأفعال العمدية وهذا ما يميزه عن الإعتداء غير العمدي لسير النظام الذي يعتبر ظرف مشددا لجريمة الدخول والبقاء غير مشروع داخل النظام وعليه فالقصد الجنائي المفترض ينتج من

2.طبيعة الافعال المجرمة الإعتداءات العمدية على المعطيات :

هي جريمة عمدية يتخذ فيها القصد الجنائي بعنصرية العلم والإرادة فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يعلم الجاني بان نشاطه الإجرامي يترتب عليه التلاعب في المعطيات ويعلم أيضا أنه ليس له الحق في القيام بذلك وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته ويشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا انه ليس عنصرا في الجريمة[1].

3.استخدام المعطيات كوسيلة في إرتكاب الجرائم الماسة بالأنظمة الإلكترونية :

إن هذا الإستخدام يكون عمديا ويتمثل في التصميم أو البحث أو التجميع أو التوفير أو النشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية ويكون هذا الإستخدام عن طريق الغش فلذلك يتطلب القصد الجنائي العام بإضافة إلى القصد الجنائي الخاص المتمثل في نية الغش .

الفرع الثاني : أنواع الجرائم الإلكترونية:

إن تصنيف الجريمة الالكترونية أصعب من تصنيف الجريمة التقليدية وتستهدف الكثير من القطاعات، من أشخاص معنويين وطبيعيين وحتى الدول امنيا واقتصاديا لذا لم يستقر الفقهاء ورجال القانون على تصنيف واحد في تحديد أنواعها نظرا لسرعة تطورها.

فهناك من يعتمد على معيار الجرائم المعلوماتية المرتكبة على الحاسوباو بواسطته.

[1] حشيفة عبد الهادي ،مرجع سبق ذكره ،ص22.

وهناك من يعتمد معيار الدافع الإجرامي والباعث على ارتكابها .

واتجاه يعتمد على الوسيلة المستعملة والأسلوب المتبع لارتكاب الجريمة .

واتجاه آخر يأخذ بمعيار محل الجريمة أو الضحايا وهو الذي سنعتمده في دراستنا هذه كونه اوضح تقسيم وابسطه حيث تقسم كما يلي :

أولا: الجرائم الواقعة على الأشخاص والأموال:

1/الجرائم الواقعة على الأشخاص: هي الجرائم الإلكترونية التي يكون ضحاياها الأشخاص الطبيعيين يمكن اجمالها في:

أ/جرائم الملكية الفنية والأدبية: حيث يتم الإعتداء على الأشخاص بالاستيلاء على مجهود المؤلف عن طريق الإستيلاء على بيانات عمله المخزنة في نظام المعالجة الآلية(بنك المعلومات) وعلى حقوق الملكية الفكرية او حتى بالتقليد كما هو الحال في الملكية الصناعية .

ب/الإعتداء على حرمة الحياة الخاصة للأشخاص: هذه الجرائم تمس الأفراد سواء في خصوصياتهم أو في سلامة ابدانهم او شرفهم. حيث يحاول المجرم بعث الخوف في نفسية الضحية ببعث رسائل مجهولة المصدر عن طريق البريد الإلكتروني ، فتخاف الضحية من الفضيحة.

فحرمة الحياة الخاصة حق دستوري والمحافظة على الأسرار وعدم افشائها سواء كانت مكالمات او محادثات ، فلا يجوز اختراق شبكة الاتصالات والتصنت عليها وانتهاك الخصوصية ، حيث تتم عن طريق اعداد ملف يحتوي على معلومات الضحية بدون علمه او بعلمه مثل الأسرار التي يطلع عليها المحامي أو المحاسب أو الطبيب بمناسبة عمله ويستعملها ضده لابتزازه والتهديد.

ج/ انتحال الشخصية : وتطال هذه الجريمة الأشخاص وحتى المواقع ، حيث يستولي المجرم على البيانات والمعلومات الشخصية للضحية بعد اختراق المواقع بسبب سمعته او مكانته الاجتماعية والوظيفية اومن صلاحياته الاستفادة منها ماديا ومعنويا بالاستدراج والتغرير .

د /جرائم السب والقذف: هي أكثر الجرائم انتشارا على شبكة الأنترنت ، عن طريق وسائل الإتصال بالكتابة او البريد الإلكتروني او غرف المحادثة ، بتوجيه واسناد واقعة او خدش شرف الأشخاص او دون اسناد واقعة والهدف تشويه السمعة، كسب الرسول صلى الله عليه وسلم أو رئيس الجمهورية[1].

[1] غربي جميلة ،**آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري** ،مذكرة لنيل شهادة الماستر في القانون ،جامعة أكلي محند اولحاج ،بويرة سنة 2020/2021ص 18

ثانيا: الجرائم الواقعة على الأموال:

أ/ جريمة التحويل الإلكتروني للأموال: من أهم نشاطات البنوك الإلكترونية عمليات تحويل ونقل الأموال للزبائن من حساب بنكي الى حساب آخر، والمعلومات المتعلقة بعملية التحويل .

فيقوم البنك بتحويل الأموال من حساب المدين الى حساب الدائن، عن طريق المقاصة الإلكترونية خلافا للتحويلات التقليدية من طرف بنك مؤهل ومرخص له بذلك ، عن طريق اجهزة الحاسوب فالجريمة تكون عندما يكون هذا التحويل غير قانوني وغير مشروع فتحول الأموال من حساب الضحية الى حساب المعتدي او حساب مستفيد اجنبي عن طريق :

"التلاعب ببرامج التحويل الخاصة .

"استعمال بطاقة شخص لسحب امواله.

"استعمال البيانات والمعلومات الشخصية في اصدار بطاقة ممغنطة ثانية باسم الزبون الضحية للقيام بالجريمة .

ب/ جريمة غسيل الأموال :هي جريمة تقليدية تطورت عن طريق التطور التكنولوجي حيث يتم ارتكابها عن طريق تطهير الأمو ال ،التي يكون مصدرها غير مشروع ويتم استثمارها بطريقة شرعية عن طريق البنوك ، عن طريق نقلها بعملية اقتصادية ومالية للأموال من مصدر غير مشروع الى دائرة الإقتصاد الشرعي ، والمصدر غير الشرعي يكون من مخدرات او الإختلاس ، ويتمثل ضرر وخطورة تبييض الأموال في انها تدخل الى الاقتصاد حيث انها اموال غير مستقرة يمكن تحويلها الى الخارج في أي وقت كما انها جريمة مركبة حيث تغطي على الجريمة الأولى، ولها اضرار امنية واجتماعية وقانونية وسياسية.

ج/تجارة المخدرات عبر الأنترنت : بحيث نجد أنه هناك مواقع تروج لإستهلاك المخدرات وكيفية انتاجها وتعليم كيفية تصنيعها وطرق تسويقها .

د/السطو والسرقة الالكترونية : قرصنة ارقام البطاقات الممغنطة.

هـ/ التزوير الالكتروني : وهي تعد من بين أخطر الجرائم التي يقوم بها المجرم المعلوماتي نظرا لما يتمتع به الحاسب الآلي من خطورة ، فيتم التزوير عن طريق الوسائل المتطورة كتزوير العملة عن طريق الماسح الضوئي وما يسببه ذلك من اضرار بالاقتصاد الوطني ، او تقليد وتزييف الوثائق والمستندات الكترونيا او التوقيع على المحررات الرسمية[1].

[1] عقباش بريزة ،**آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري** ،مذكرة لنيل شهادة الماستر في الحقوق ،جامعة محمد البشير الابراهيمي ، برج بوعريريج ،سنة 2021/2022 ص 27.

الفرع الثاني : الجرائم الواقعة على الدولة :

وتتمثل اساسا في جريمتي المساس بأمن الدولة وكذلك الإرهاب الالكتروني:

اولا : الإرهاب الإلكتروني: وهو من اخطر الجرائم الإلكترونية فالانترنت اصبح مكانا لترويج أفكار المنظمات الإرهابية والتعبير عن معتقداتها، بمحاولة التأثير على المعتقدات الدينية لأفراد المجتمع وتقاليده مما يخلق الفوضى ويمس بأمن الدولة ، او تكون بتعاون بين عدة افراد قصد الإضرار بالبلد وقد تكون بالإشادة بالأفعال الإرهابية المرتكبة ضد الدولة او الحاق الأذى بالمؤسسة العسكرية، عن طريق زرع الفيروسات المخربة او تعطيل الأنظمة بالتنويه ضد دولة محددة واستغلال المؤيدين للمفكر المتطرف[1].

ثانيا: جريمة التجسس على الدولة :

ويكون في المجال الأمني والإقتصادي من طرف الدول المعادية بتجميع الأسرار وتموين الأخبار فيكون التجسس على الأسرار العسكرية تمس بأمن الدولة وتتم عن طريق اختراق المواقع الحكومية والرئاسية او قرصنتها وبالتالي الإطلاع عليها.

حيث ان استهداف الدفاع الوطني لدولة والهيئات عسكرية يتم بواسطة اشخاص او منظمات يتواجدون خارج البلاد والتجسس يكون على المواقع و المنظمات والشخصيات العسكرية.

-اما اقتصاديا: فيتم على المؤسسات الاقتصادية التابعة لدولة تكون من قبل عملاء من دولة معادية او حتى صديقة للكشف عن الأسرار الاقتصادية، او من شركة على شركة منافسة في نفس المجال فهي معلومات سرية مؤمنة لا يسمح بالاطلاع عليها أنها اسرار دولة[2].

المبحث الثاني: معالجة الجريمة الالكترونية في التشريع الجزائري.

على غرار التشريعات المقارنة التي تصدت للجريمة الإلكترونية فقد وجد المشرع الجزائري نفسه أمام صور جديدة للجريمة تختلف عن الجرائم التقليدية من حيث الوسائل المستخدمة وتتطلب تدخلا تشريعيا لمواجهتها لهذا سن تعديلا في قانون العقوبات رقم 04/15 الذي ادرج فيه مواد تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

---

[1] مصطفى يوسف كافي، **جرائم الفساد غسيل الأموال، السياحة الارهاب الالكتروني المعلوماتية** ، مكتبة المجتمع العربي للنشر والتوزيع ، الأردن ط1، 2014 ، ص 143.

[2] خالد حسن أحمد لطفي، **جرائم الأنترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني** ، دار الفكر الجامعي الاسكندرية ، د ذ ط ، 2019 ، ص 38.

المطلب الأول : المعالجة القانونية للجريمة الإلكترونية

الفرع الأول: نطاق المعالجة القانونية

اعتمد تدخل المشرع الجزائري في مواجهته للجرائم الإلكترونية على أسلوبين حسب طبيعة هذه الجرائم التي تأخذ شكلين :

الشكل الأول: يتجسد دفي صور الجرائم التقليدية يتم ارتكابها بوسائل إلكترونية في هذه الحالة فإن النصوص التقليدية يتم تطبيقها على الجرائم الإلكترونية ولا تعتبر الا صورة متطورة للجرائم التقليدية .

فالجرائم التي تمس الأموال مثل النصب والإحتيال عبر الانترنت تعد من قبيل الجرائم التقليدية التي تتم باستخدام وسائل تكنولوجية. فاذن تطبق عليها النصوص التقليدية .

وجرائم الإعتداء على الأشخاص مثل القذف والسب عبر الشبكات الاجتماعية تعد من قبيل الجرائم التقليدية التي تتم باستخدام التكنولوجيا .

وبالتالي فالنصوص الموجودة في مواجهة هذه الأفعال كفيلة لتلائم الأفعال المرتكبة بوسائل تكنولوجية .

ولا يوجد داع لإعادة صياغة نصوص جديدة لتجريم الأفعال المرتكبة بوسائل متطورة فالأمر لا يتطلب سن تشريعات جديدة .

اما بالنسبة للشكل الثاني فهو يأخذ صور جديدة لجرائم حديثة تتميز كليا عن الجرائم التقليدية وفي هذا الشكل لا يمكن بأي الحال الاعتماد على النصوص التقليدية لتجريم هذه الأفعال وبالتالي فإنه يتوقف على النصوص الجديدة أن تجرم أفعال التعدي على المعلوماتية[1].

والتي تتخذ شكل التعدي على البيانات المخزنة في ذاكرة الحاسوب مثل جرائم تدمير البيانات وإتلافها التي يعاقب عليها القانون في المادة 394 مكرر فقرة 2 [2].

وقد اعتمد المشرع الجزائري إصدار قوانين جديدة لتجريم أفعال تمس الإعتداء على أنظمة المعالجة الآلية للمعطيات. ليس في قانون جديد وانما أدرجها ضمن العقوبات ضمن الفصل الثالث القسم السابع مكرر بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات "وبالتالي فإن هذا القانون لاينطبق على الجرائم التقليدية التي يتم ارتكابها بواسطة التكنولوجيا.

إذ أن القانون الذي يضبطها هو النصوص التقليدية لقانون العقوبات .

---

[1] ياسين بن عمر ، **المعالجة القانونية للجرائم الإلكترونية في القانون الجزائري والتشريعات المقارنة** ،مجلة العلوم القانونية والسياسية المجلد 10 العدد 03 سنة ديسمبر 2019 ص 713.

[2] المادة 394 مكرر فقرة2 من قانون العقوبات الجزائري

ونلاحظ أن المشرع لم يشر إلى النصوص التي تطبق في حال ارتكاب أفعال تشكل جرائم تقليدية عن طريق أنظمة معلوماتية فلا يوجد إشارة تدل على تشديد العقوبة أو اعتبارها ظرف تشديد بشأن الجرائم المرتكبة بوسائل تكنولوجية.

إن هذا الفراغ يؤدي إلى حالة من التخبط في تكييف الأفعال التي تشكل جرائم تقليدية بوسائل أنظمة المعلوماتية المتطورة فهي من جهة تعد من أشكال الجرائم التي تم ارتكابها من خلال التغيير والتعديل في الأنظمة المعلوماتية مثل:

الاحتيال والتزوير وانتحال الصفة والسب والقذف والتي لها صور وتصنيف ضمن الجرائم التقليدية.

ومن جهة اخرى فإنها تعد من الجرائم التي تمس بأنظمة المعلوماتية وقد جاءت النصوص الجديدة لتجريمها .

مما يؤدي إلى تعارض النصوص الجزائية في تكييفها وتطبيق العقوبة على مرتكبيها.

الفرع الثاني : تجريم المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري:

جاءت مواد قانون العقوبات بعنوان القسم السابع مكرر 1 تحت الفصل الثالث المتعلقة بالجنايات و الجنح ضد الأموال، وإدراج هذه المواد في هذا الفصل دليل على أن موضوع الإعتداء هو الأموال، أو بالأحرى البيانات والمعطيات التي تأخذ صفة المال.

إن الدراسة القانونية لمواد قانون العقوبات المتعلقة بمعالجة الأنظمة الآلية للمعطيات، وهي المواد من 394 مكرر إلى غاية 394 مكرر 08 تعتبر إضافة جاء بها المشرع في سبيل مكافحة الجرائم الإلكترونية، إلا أن هذه النصوص بالرغم من إضافتها في مكافحتها لهذه الجرائم حملت غموضا كبيرا من حيث الصياغة، وبعد قراءة النصوص المتعلقة بتجريم الأفعال التي تمس نظام المعالجة الآلية للمعطيات نجد [1]:

1/من ناحية المصطلحات المستعملة:

نلاحظ غياب الكلمات المفتاحية في نصوص القانون، فقد جاءت نصوص مواد التجريم المتعلق بمعالجة الأنظمة الآلية للمعطيات غامضة، إذ لا يوجد ما يشرح الكلمات الدالة التي تبين كيفية قيام الركن المادي للجريمة، فهناك نقص فيما يخص كيفية ارتكاب الجريمة، وهذا يسبب اشكالا عند تطبيق النصوص، ومثاله المادة 394 مكرر 02 حيث جاءت عبارات النص مقتضبة وغامضة في تبيان السلوك المادي

[1] المواد من 394 مكرر إلى غاية 394 مكرر 08 من قانون العقوبات الجزائري.

للجريمة مثل: عبارات: بحث، تصميم، توفير، تجميع...أين يصعب تصور وقوع الجريمة من خلال هذه العبارات .

2/من ناحية التجريم :

نجد أن المشرع الجزائري لم يعمم صور الجرائم التقليدية، التي ترتكب بواسطة نظام معلوماتية، بل اقتصر على الجرائم التي تمس بالأنظمة المعلوماتية للمعطيات، بمعنى أن يكون محل الجريمة هو النظام المعلوماتي في حد ذاته، وهذا الأمر يجعل بعض النصوص التقليدية لا تنطبق على الجرائم التي ترتكب بواسطة التكنولوجيا، مثل: جريمة التزوير الإلكتروني.

اما من حيث التكرار في صور الجرائم و عدم توحيد المصطلحات: فالمادة 394 مكرر فقرة 01 والمادة 394 مكرر 1 تتشابهان لدرجة التطابق، حيث تناولت المادة الأولى تجريم الدخول أو البقاء عن طريق الغش في جزء من منظومة المعالجة الآلية للمعطيات، وتكلمت عن مضاعفة العقوبة، إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة، في حين نصت المادة 394 مكرر 01 على عقوبة من 06 أشهر إلى 03 سنوات .

والغرامة لكل من أدخل عن طريق الغش معطيات في نظام المعالجة الآلية، أو أزال أو عدل عن طريق الغش المعطيات التي يتضمنها.

فالمشرع مرة يتكلم عن نظام (المادة 394 مكرر 01) ومرة يتكلم عن منظومة (المادة 394 مكرر) ومرة يتكلم عن حذف أو تغيير (المادة 394 مكرر) ومرة يتكلم عن إزالة أو تعديل (394 مكرر 1) هو إختلاف في المفردات فقط مع اشتراكها في المعنى.

3/ من ناحية العقاب :

تميزت عقوبات التشريع الجزائري بتشديد العقوبات المالية مقارنة بالحبس، إذ تصل الغرامة إلى 4.000.000دج في جرائم إدخال أو تعديل أو إزالة معطيات عن طريق الغش (المادة 394 مكرر01) وتصل الغرامة حدها الأقصى إلى 10.000.000دج في الجرائم التي تناولتها المادة(394 مكرر 02) ورفع المشرع الجزائري من عقوبة الحبس في حالة واحدة، وهي الجرائم المتعلقة بتقديم المساعدة لإرتكاب أفعال إرهابية، وهي المنصوص عليها في المادتين 87 مكرر 11 و12 المعدلتين بموجب القانون رقم 16/02 أين يبلغ حدها الأقصى 10 سنوات سجنا[1].

[1] القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، ج ر ،العدد 71،ص ص 11-12.

وبالتالي يمكن القول أن العقوبات التي أقرها المشرع الجزائري تميزت بمضاعفة العقوبة في جانبها المالي أكثر من جانبها البدني، وهو ما يفقد من ميزة الردع، ويحد من سياسة مواجهة الجريمة الالكترونية.

المطلب الثاني: المعالجة الاجرائية للجريمة الإلكترونية:

إن الإشكال الذي يواجه أجهزة القضاء والشرطة القضائية لا يتمثل في الفراغ التشريعي للنصوص التجريمية بقدر ما هي كامنة في طرق ضبطها وإثباتها، وهو ما يرجع إلى افتقاد الآثار التقليدية التي قد تتركها أي جريمة ذات طبيعة معلوماتية، وإذا كان البحث في مسألة قدرة القواعد الاجرائية التقليدية في ضبط جريمة الإلكترونية أمرا صعبا، فهذا ما جعل مسألة ملائمة الإجراءات الجنائية في البحث والتحري مع خصوصية هذا النوع من الجرائم تستأثر باهتمام المشرعين.

وقد استحدث المشرع الجزائري نصوصا تنظم الإجراءات المتعلقة بالبحث والتحري في الجريمة الإلكترونية، وهو ما عرفه بصدور القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال رقم ،04/09 وهو مسلك انفرد به المشرع الجزائري دون غيره من التشريعات العربية، التي لم تورد قانونا خاصا إجرائيا في البحث والتحري على الجرائم الإلكترونية.

الفرع الأول: المعالجة الإجرائية واحترام مبدأ المشروعية

يشترط في إجراءات البحث والتحري في الجريمة عموما سلامتها ومشروعيتها، وموافقتها للقانون حتى تحقق العدالة منها وفي الجرائم الإلكترونية بالخصوص، لذا فإن الخصوصية التي تتميز بها تجعل من احترام مبدأ المشروعية وموافقة للقانون، تحديا للمشرعين بالنظر إلى أن القانون لم يعرف مثل هذه الإجراءات سابقا، إضافة إلى أن طبيعة آثار الجريمة تجعل التعامل معها وفق مبدأ المشروعية، والموافقة صعبا نوعا ما في ما يخص استخلاص الدليل الجنائي، وتتناول مسألة المشروعية عنصرين[1]:

مشروعية الإجراءات المتخذة في حد ذاتها ومشروعية استخلاص الدليل.

أولا: المشروعية في الإجراءات

أقر المشرع الجزائري مجموعة من الإجراءات لمواجهة الجريمة الالكترونية منها ذات طابع تقليدي على غرار التفتيش، ومنها ما هو مستحدث على غرار التسرب الإلكتروني.

[1] عز الدين عثماني، **إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الإتصال والمعلوماتية**، مجلة دائرة البحوث والدراسات القانونية والسياسية ،مخبر المؤسسات الدستورية والنظم السياسية ،العدد4،2018،ص56-57.

1/ المشروعية في إجراء التفتيش:

إن سهولة محو آثار الجريمة في جرائم المعلوماتية بصفة عامة، يتطلب السرعة في اتخاذ إجراءات التفتيش للحفاظ على أدلة الجريمة، إذ أن إتباع الإجراءات التقليدية المتمثلة في الحصول على الترخيص من السلطة القضائية قد يؤدي إلى ضياع دليل الجريمة هذا من جهة، ومن جهة أخرى فإن القفز على الضمانات القانونية لمشروعية التفتيش تؤدي إلى انتهاك الحريات، بدعوى خصوصية الجريمة الإلكترونية وإجراءاتها، ولذلك ينبغي إيجاد توازن بين خصوصية البحث والتحري في الجرائم الإلكترونية، مع الحفاظ على الحريات الأساسية، وقد حافظ المشرع على ضوابط التفتيش المنصوص عليها في قانون الإجراءات الجز ائية، وأعاد التذكير بها في قانون 04/09 في المادة 05 القيام بالتفتيش بناء على أمر من السلطة القضائية، وعليه فإن القانون 04/09 أحال على قانون الإجراءات الجزائية في مسألة تطبيق قواعد التفتيش، وأحاط إجراء التفتيش بضمانات؛ وهي أن يظل القائم بالتفتيش مقيدا إلى غاية صدور أمر بالتفتيش من القاضي المختص، وتراعى في عملية صدور الإذن استخدام أي وسيلة اتصال لإعلام المكلف بالتفتيش السماح له القيام بالتفتيش، خلافا لما هو معمول به في قانون الإجراءات الجزائية في الجرائم التقليدية، حيث يمكن الإستعانة بالفاكس أو رسالة نصية أو أي وسيلة الكترونية للتبليغ[1].

و بشأن مسألة تمديد التفتيش فقد نظم المشرع الجزائري مسألة تمديده في الجرائم الإلكترونية في المادة 05 فقرة 03" أجاز تمديد التفتيش لأنظمة معلوماتية خارج الإقليم الوطني، إذا دعت الضرورة ذلك، حيث تخول المادة للجهات المختصة توسيع نطاق التفتيش، ليشمل المعطيات المخزنة في منظومة معلوماتية تقع خارج القطر الوطني، وقد يشكل هذا الجواز انتهاكا لسيادة الدول، وتحسبا لذلك فقد ربط المشرع الجزائري اتخاذ هذه الإجراءات بوجود اتفاقيات بين الدول، في نطاق المساعدة القضائية المتبادلة ووفقا لمبدأ المعاملة بالمثل..

2/التسرب الإلكتروني:

عرف قانون الإجراءات الجزائية الجزائري التسرب في المادة 65 مكرر 12 بالقول: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف[2].

[1] عز الدين عثماني، مرجع سبق ذكره، ص 57.

[2] براهيمي جمال، **التحقيق الجنائي في الجرائم الإلكترونية**، اطروحة لنيل شهادة دكتوراه في العلوم تخصص قانون ،جامعة مولود معمري ،تيزي وزو سنة 2018 ص83.

وأجاز المشرع اللجوء إلى هذه الوسيلة، التي تعد أسلوبا من أساليب التحري الخاصة، في جرائم ذكرها المشرع على سبيل الحصر، وهي:

-الجرائم المتلبس بها.

-كجرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية، والجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب وجرائم الصرف، إضافة إلى جرائم الفساد ويتم اتخاذ الإجراءات بعد الحصول على إذن قضائي من وكيل الجمهورية أو قاضي التحقيق ويعد هذا ضابطا لوقوع هذه الإجراءات التي تمس بخصوصية الأفراد وتقع باطلا الإجراءات التي لم تتوفر فيها إذن من السلطة القضائية.

يخول القانون للمتسرب انتحال هوية مستعارة، كما يسمح له بارتكاب أعمال تعد جريمة في نظر القانون تحت ظرف الضرورة مثل :

اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم، أو مستعملة في ارتكابها.

ووسائل النقل أو التخزين أو الإيواء أو الحفظ والإتصال-استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي، وكذا ويتم التسرب من خلال استعمال العون المتسرب هوية مستعارة في مواقع الأنترنت، يشتبه قيام أصحابها بعمليات النصب والإحتيال، وفي إحدى العمليات تمكنت الشرطة القضائية الفرنسية عن طريق إجراء التسرب لأحد أعوانها، والذي قام بالدخول في موقع الكتروني، عبارة عن منتدى مخصص للحديث عن تقنيات تزوير البطاقات البنكية، وعن طريق هذا الموقع تمكنت الضبطية من الكشف عن هوية المحتالين على البطاقات البنكية، واستخدام محادثات الدردشة كدليل إثبات ضد الفاعلين[1].

الفرع الثاني: المشروعية في استخلاص الدليل نحو التخلي عن التمسك بمشروعية الدليل الجنائي في الجرائم الإلكترونية

أمام التحديات التي تطرحها الجرائم الالكترونية عامة، قد يصعب على الأجهزة المكلفة بالبحث والتحري التقيد ببعض المبادئ الإجرائية، التي تقتضيها عملية استيفاء الدليل الإلكتروني، الذي يقود إلى كشف الفاعل، مما دعى بعضهم إلى إعادة النظر في التمسك بمبدأ مشروعية الدليل، ومدى إمكانية ترجيح متطلبات العدالة على فكرة شرعية الدليل.

[1] ياسين بن عمر ، مرجع سبق ذكره، ص720.

حيث أن المشرع الوطني لم يتناول مسألة الدليل الالكتروني بالخصوص المقارنة بالأدلة الأخرى، إذ جميعها تخضع للمادة 212 من قانون الإجراءات الجزائية في مسألة الإثبات، بالرغم من أن المشرع الوطني نظم إجراءات المتابعة في الجرائم الإلكترونية، من خلال القانون 04/09 إلا أنه لا يوجد ما ينظم مسألة قيمة الدليل المستمد من الجرائم الالكترونية، ونطاق المشروعية في الحصول عليه.

إن خصوصية الدليل غير المادي في الجريمة الالكترونية، يحتم علينا إعادة النظر في التمسك بفكرة مشروعية الدليل، إذ أن إقصاء أي دليل لا يتوفر على المشروعية من شأنه أن ينجي الفاعل من العقوبة، ويسقط التهمة الموجهة إليه بناء على عدم وجود دليل مشروع، وهذا القول مناف لمتطلبات العدالة، التي تسعى إلى متابعة الجاني، والتمسك بالمشروعية في الجرائم التقليدية، إلا أن خصوصية الجريمة الإلكترونية تتطلب الأخذ بمبدأ المشروعية، بصورة نسبية وليست مطلقة، وتتمثل في قبول الدليل غير مشروع في حالة مناقشته وعدم استبعاده[1].

الفرع الثالث: المعالجة الإجرائية واحترام الحريات الأساسية :

تصطدم إجراءات البحث والتحري بمسألة تتعلق بالحريات الأساسية للأشخاص، وهي الضمانة التي كفلها الدستور إذ أن الحياة الخاصة تتعلق بحرمة السكن – والإستئثار بالبيانات الشخصية والإسمية – وسرية الإتصالات والمكالمات – والحق في حماية الصورة الشخصية، كل هذه العناصر تشكل الخصوصية للحياة الشخصية، ولا شك أن إجراءات التفتيش والبحث في البيانات وأدلة الجريمة المرتكبة بواسطة الكمبيوتر سيطال أحد عناصر هذه الخصوصية وعليه كان لزاما توافر ضمانات لحماية خصوصية الأفراد.

أولا: ضمانات حماية المعطيات الخاصة:

تعتبر قضية انتهاك الخصوصية من بين أهم القضايا المطروحة في مجال التحقيق في الجرائم المتعلقة بالأنترنت، خاصة فيما يتعلق بالتفتيش والمعاينة عبر الأنترنت، حيث يتطلب فحص مختلف المعاينات عبرها، بما في ذلك تفتيش البريد الالكتروني مثالا الأمر الذي يجعل خصوصيات الأفراد على المحك، خاصة إذا كان التفتيش والمعاينة متعلق بحسابات متصلة بالحاسوب محل التحقيق، فالحق في الخصوصية بمثابة عائق دون إجراء تحقيق على أكمل وجه، فيما يخص الجرائم المرتكبة عبر الأنترنت[2].

[1] المادة 212 من قانون الإجراءات الجزائية.

[2] عبد السلام طوبال ،**الضمانات القانونية لحماية المعطيات ذات الطابع الشخصي في التشريع الجزائري** ، مجلة العلوم القانونية والاجتماعية ،المجلد 5 ، العدد 2 سنة 2020 ص 269

إن حيز الإعتبار بالخصوصية في الجرائم الالكترونية والحياة الخاصة، أصبح ضيقا نظرا لصعوبة مكافحة الجريمة، دون الكشف عن سرية الاتصالات والبيانات المتعلقة بالمشتبه به، أو حتى ضمن دائرة الأشخاص الذين يتعاملون معه، وهي من دواعي البحث والتحقيق في الجريمة، إذ أن المعلومات التي يتم الكشف عنها ستظل سرية في التحقيق، ويضمن القانون عدم نشرها وكتمها، الأمر الذي يجعل الحياة الخاصة في هذه الحالة فقط مكشوفة من قبل رجال القضاء ومزودي الخدمة الملزمون بكتمان العمليات التي ينجزونها بناء على طلب المحققين، وكذا المعطيات التي يتحصلون عليها تحت طائلة العقوبة والمتابعة بتهمة إفشاء سرية التحقيق وقد حدد القانون مدة حفظ البيانات والتسجيلات المتعلقة بالأشخاص، والتي يلزم مقدمو الخدمات الإحتفاظ بها سنة واحدة ابتداء من تاريخ التسجيل.

وقد رتب المشرع الجزائري المسؤولية الجزائية لمن يقوم باستخدام المعلومات المتحصل عليها في غير الغرض الذي خصصت له، وقد أشار إلى ذلك في المادة 09 من القانون رقم 09-04 ولكن تبقى مسألة تجريم إفشاء الأسرار والبيانات المتحصل عليها غير كاف، مقارنة بما تسببه من أضرار نفسية على الأشخاص عند تداول معلوماتهم، ونظرا لما تمتلكه السلطات العامة من إمكانيات وأجهزة اتصالات تتيح لها التوصل إلى معلومات الأفراد والبيانات الشخصية، مما يشكل في بعض الأحيان تجاوزا لها من خلال الوصول بدون إذن لمعطيات خاصة، ونعتقد أن إنشاء هيئة إدارية مستقلة تعمل على مراقبة مدى احترام السلطات العامة لخصوصية الأفراد، يشكل ضمانا من تعدي أجهزة القضاء والشرطة عند البحث والتحري في الوقائع التي من المحتمل أن تشكل جرائم[1].

وفي هذا السياق صدر مؤخرا قانون رقم 18/07الذي يهدف إلى تحديد قواعد حماية الأشخاص الطبيعيين، في مجال معالجة المعطيات ذات الطابع الشخصي، والذي نص على إنشاء سلطة وطنية لحماية المعطيات ذات الطابع الشخصي في انتظار تنصيبها.

ثانيا : ضمانات المراقبة الإلكترونية

تعرف المراقبة الإلكترونية (électronique surveillance) بأنها عملية مراقبة شبكة الإتصالات باستخدام التقنية الإلكترونية، تجمع بواسطتها بيانات ومعلومات حول المشتبه فيه لتحقيق غرض أمني[2]. يقوم بها مراقب ذو كفاءة تتماشى مع نوع الجريمة التي يحقق فيها وهو إجراء وقائي يمكن أن تلجأ إليه

[1] قانون رقم 07/18 المؤرخ في 10 يونيو 2018،المتعلق بحماية الأشخاص الطبيعيين، في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] قيشاح نبيلة ،**ضمانات المراقبة الإلكترونية في التشريع الجزائري** ، مجلة الحقوق والعلوم السياسية جامعة خنشلة ،المجلد 10 العدد2 سنة 2023 ص1100.

السلطة القضائية حتى قبل وقوع الجريمة، في حالة اشتباه بارتكاب أفعال تمس بالنظام العام و الأمن كما نصت عليه المادة 04 فقرة (أ) و (ب) من القانون رقم 04/09 المتعلق بالوقاية من جرائم الإتصالات ومكافحتها[1].

ولقد قيد المشرع الجزائري في قانون 09/04 عمليات إجراء ومراقبة الاتصالات الإلكتروني بأمر من السلطة القضائية، لما لهذه الإجراءات من مساس بحقوق وحريات الأشخاص، وبالتالي لا يمكن إتخاذ إجراءات مراقبة الاتصالات الإلكترونية، وتسجيلها وتجميعها دون الحصول على إذن من السلطة القضائية، وهذا ما نصت عليه الفقرة 02 من المادة 04 من القانون سالف الذكر، لكن ما يلاحظ على هذه المادة أن المشرع لم يضع جزاء على مخالفة هذا الإجراء، واقتصر على عبارة "لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية"، وعلى خلاف ما هو موجود في قانون الإجراءات الجزائية، حيث رتب البطلان عند مخالفة الإجراءات الخاصة في متابعة الجرائم المذكورة. وعلى سبيل الحصر في المادة 65 مكرر 05 و التي من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، ونجد النص على البطلان في المادة 65 مكرر 15 .حيث يجب على المشرع ان يستدرك هاته النقطة ويشير إليها.

إضافة إلى ذلك فإنه أغفل ترتيب المسؤولية الجزائية في حالة القيام بإجراءات مراقبة الاتصالات الإلكترونية دون إذن من السلطة القضائية، إذ أنه يعد انتهاكا لحق الحياة الخاصة وهو حق دستوري كفله الدستور في المادة 46 منه والتي تنص: "لا يجوز انتهاك حرمة الحياة الخاصة وحرمة شرفه، يحميهما القانون، وسرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم".

فالدستور يحيل على القانون المعاقبة على انتهاك الحقوق و الحريات، في حالة مخالفتها لإجراءات .

وقد سبق قانون الإجراءات الجزائية أن نص على مشروعية إجراء تسجيل الأصوات واعتراض المراسلات والتقاط الصور، في تعديل له رقم 06/22 في المواد 65 مكرر 05 وما يليها، وهي إجراءات ترتبط بجرائم محددة على سبيل الحصر، وهي جرائم المخدرات – الجريمة المنظمة العابرة للحدود الوطنية – جرائم المساس بأنظمة المعالجة الآلية للمعطيات – تبييض الاموال – الإرهاب الجرائم المتعلقة بالتشريع الخاص بالصرف –جرائم الفساد[2].

[1] المادة 04 فقرة (أ) و (ب) من القانون رقم 04/09 المتعلق بالوقاية من جرائم الإتصالات ومكافحتها.

[2] القانون رقم 06/22 المؤرخ في 20-12-2006 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية ج ،ر، رقم 84

خلاصة الفصل الأول:

في ختام هذا الفصل يتضح لنا أن الجريمة الالكترونية هي جريمة وليدة التطور العلمي والتكنولوجي الذي وصلت إليه المجتمعات، فبرغم من الإيجابيات التي تطغى على هذا التقدم إلا أن الجانب السلبي له والذي يستعمل في أغراض سلبية يعرف انتشار كبيرا خاصة في أوساط الجيل الصاعد، فمرتكبي هذا النوع من الجرائم أو ما يعرفون بالمجرمين المعلوماتيين لهم قدرة كبيرة على تكيف بالمجتمعات الأخرى وكذا يتميزون بالذكاء والفطنة وهي أكبر مقومات ارتكاب هذا النوع من الجرائم.

كما أن صعوبة التي تحيط بالجريمة الالكترونية من حيث سرعة اكتشافها وصعوبة إثباتها تشكل أكبر عوائق التي تواجهنا لمكافحتها.

الفصل الثاني

التعاون الإقليمي لمكافحة الجريمة الإلكترونية

تمهيد

إن الحاجة إلى تنسيق دولي وثيق في مجالات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هو الحركة الكبيرة للمعلومات في الأنظمة المعلوماتية ،بحيث سمحت هذه الحركة بإرتكاب جرائم عن طريق جهاز الإعلام الآلي (الكمبيوتر) في دولة ما في حين أن نجاح الفعل الإجرامي يكون تنفيذه في دولة أخرى.

ولقد أدركت جميع الدول أنها مهما بلغت قوتها لا تستطيع بجهودها المنفردة القضاء على الجريمة الإلكترونية ,فكان من الضروري أن تدخل في علاقات تعاون متبادلة مع بعضها البعض بإعتبار هذا التعاون الإقليمي وسيلة لتحقيق درجة عالية من الإنسجام والتوافق مع اهداف المجتمع الدولي لمنع حدوث هذا النوع الجرائم أو الحد منها .فمن خلال هذا سنعرض في هذا الفصل الى مجالات التعاون في المبحث الأول أما المبحث الثاني فسنتطرق الى مدى فاعلية التعاون في مكافحة الجريمة الإلكترونية.

المبحث الأول: مجالات التعاون في مجال المكافحة الإلكترونية.

يهدف التعاون إلى التوفيق بين سيادة واستقلال كل دولة على حدى مع ضمان مزاولة كل واحدة منهما اختصاصها الجنائي على إقليمها وفي نفس الوقت إمكانية تنفيذ حقها في العقاب وتحقيق هذا لا يكون إلا بالتعاون ثنائي واقليمي من خلال هذا المنطلق سنتطرق اليه في:

المطلب الأول : التعاون الأمني.

الفرع الأول: مفهوم التعاون الأمني.

أولا : تعريف التعاون الأمني.

يعرف على أنه "تبادل العون والمساعدة وتظافر الجهود المشتركة بين طرفي دوليتين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال تصدي لمخاطر الإجرام وما يرتبط به من مجالات اخرى مثل مجال الأمن أو لتخطي مشكلات الحدود السيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين وتعقب مصادر التهديد سواء كانت مساعدة متبادلة قانونية أو قضائية أو شرطية وسواء اقتصرت على دولتين فقط أو امتدت إقليميا أو عالميا .

ويعد التعاون الأمني ثمرة تطور العلاقات الدولية ونتيجة حتمية لما تشهده الجريمة الإلكترونية من تطور وإنتشار حيث أضحت ظاهرة دولية [1].

ثانيا : أهمية التعاون الأمني.

لعلى شعور المجتمع بخطورة الجرائم الإلكترونية وتسارع نموها جعل التعاون الأمني لمكافحتها نقطة إلتقاء للجهود الدولية لاتخاذ تدابير تدعم سبل التعاون الإقليمي لمكافحتها .

وهو من بين أجهزة الشرطة الجنائية المتخصصة في مكافحة الجريمة الإلكترونية في الدول .

وأحد وسائلها الهامة التي يمكن من خلالها تفادي الجريمة او التقليل منها بحيث يستحيل على الدولة القضاء بمفردها على هذا النوع من الجرائم العابرة للحدود لأن جهاز الأمن في هذه دولة أو غيرها لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابعة لها .

فملاحقة مرتكبي هذه الجرائم وتقديمهم للعدالة لتوقيع العقاب يستلزم القيام بإجراء التحريات خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها ومن هذه الإجراءات معاينة مواقع الانترنت في الخارج أو ضبط الأقراص الصلبة أو تفتيش نظم الحاسوب.....الخ .

---

[1] سليمان ابو نمر ، **مكافحة الجريمة المعلوماتية في إطار القانون الدولي** ، مذكرة لنيل شهادة ماستر ،جامعة محمد خيضر، بسكرة ،سنة 2021 ص 23.

ومتى فرا المجرم خارج حدود الدولة يقف الجهاز الأمني عاجزا لذا أصبحت الحاجة ماسة إلى وجود تعاون دولي يأخذ على عاتقه القيام بهذه المهمة .

وتتضح أهمية التعاون الأمني من خلال تبني تكتيك متطور لإجراء التحريات والتحقيقات في مجال المكافحة الجريمة الإلكترونية بإستخدام التكنولوجيا الحديثة في الإتصال مثل الدوائر التلفزيونية، وإستخدام أساليب خاصة للتحري والمراقبة، واستحداث قنوات للاتصال، والتنسيق الأمني والقضائي بين الجهات المختصة عن طريق الأقمار الصناعية وشبكة الأنترنت لتبادل المعلومات سريعا، وانتقال القاضي إلى الدول المعنية للتحقيق ولاتخاذ ما يلزم من إجراءات، ليس فقط في مرحلة التحقيق الإبتدائي ولكن في مرحلة الحكم أيضا، ومراعاة تنفيذ الأحكام الاجنبية وفقا لضوابط تتفق عليها الدول فيما بينها، من خلال التوفيق بين الإجراءات الجنائية في كل من الدولتين، والإتفاق على معايير موحدة في هذا الشأن، كذلك الإتفاق على كيفية مصادرة الأموال محل الجريمة الإلكترونية عبر الحدود أو إرسال المسجونين [1].

ثالثا/ أسس التعاون الأمني لمكافحة الجريمة الإلكترونية :

نظرا للطبيعة الخاصة بالجريمة الإلكترونية فإنه ينبغي أن يبنى هذا التعاون على أسس معينة وهي كالآتي[2]:

1- الدراسة العلمية للبحث عن ظاهرة الجريمة الإلكترونية وتوفير البيانات الإحصائية المتعلقة بالجريمة وبمرتكبها لسير النظام القضائي الجنائي حيث أن هذه المعلومات تساعد بصورة فعالة على مكافحتها .

2- تحديد أساليب التعاون في مجال التدريب و تحقيق التكامل الأمني بين أجهزة الشرطة .

3- إعداد مشروع اتفاقية دولية تتضمن قانون موحد للجريمة الإلكترونية.

4- وضع إستراتيجيات وقائية واحترازية توفر الجو الملائم لمكافحة و انهاء انشطة المنظمات الإجرامية وزيادة الوعي العام لدى الأفراد بنشر البيانات اللازمة عن هذه الجريمة ومرتكبيها.

5_التنسيق بين المؤسسات الأمنية بآلياتها المختلفة في الساحات الأمنية والإقليمية والدولية بما يحقق حصر معدلات الجريمة ويحول دون استفحالها واستكمال أي نقص في المعلومات الأمنية، وذلك بالتعاون بتجميع عناصر تلك المعلومات، ليكتمل بها في النهاية كشف أبعاد الجرائم وخطط الإعداد لارتكابها، وإتاحة الفرصة لدراسة الثغرات الأمنية الدولية والعمل على ايجاد أفضل أساليب التصدي لها منعا للجريمة، وضبطا للجناة .

[1] حشيفة عبد الهادي، مرجع سبق ذكره ص 39.

[2] سليمان ابو نمر، مرجع سبق ذكره ،ص 25 .

فتبادل المعلومات والخبرات ونتائج البحوث والدراسات بخصوص الجرائم الإلكترونية يتيح حصر الأساليب والوسائل الجديدة المستخدمة لارتكابها ويوسع نطاق المعرفة بأنماط المجرمين وأنشطتهم الإجرامية .

رابعا : صور التعاون الأمني.

1/ربط شبكات الإتصال والمعلومات:

تحتاج الإتصالات الشرطية إلى وسائل الإتصال تحقق السرعة الملائمة لتتمكن أجهزة العدالة الجنائية من التواصل بين سلطات التحقيق والملاحقة المختلفة، لذا عمدت الدول والمنظمات الدولية تطوير الإتصال وتبادل المعلومات فيما بينها.

2-القيام ببعض العمليات الشرطية والأمنية المشتركة:

تعقب المجرم المعلوماتي وتعقب الأدلة الرقمية وضبطها، والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الإتصال بحثا عما قد تحتويه من أدلة وبراهين على ارتكاب الجريمة الإلكترونية، كلها أمور تستدعي القيام ببعض العمليات الشرطية والأمنية المشتركة بين الدول وذلك من أجل صقل مهارات وخبرات القائمين على مكافحة الجرائم والحد منها [1].

الفرع الثاني : جهود منظمة الأنتربول في مكافحة الجرائم الإلكترونية كنموذجا.

أولا : تعريف الأنتربول:

هو أكبر منظمة شرطية دولية أنشأت سنة 1929، مقرها الرئيسي في مدينة ليون بفرنسا، يتكون من الجمعية العامة، اللجنة التنفيذية، الأمانة العامة، المكاتب المركزية الوطنية، المستشارون، لجنة ضبط ملفات الأنتربول.

وكانت تسمى هذه المنظمة بالجنة الدولية للشرطة الجنائية وتضم في عضويها 182 دولة.

بحيث يكون العمل داخل المنظمة بتبادل اعضاء الشرطة الدولية المعلومات عن المجرمين الدوليين، ويتعاونون فيما بينهم في مكافحة الجرائم الدولية، مثل جرائم التهريب، وعمليات البيع والشراء غير المشروع للأسلحة، والجرائم الإلكترونية . وقد ركز الإنتربول في السنوات الأخيرة بصورة أساسية على الجريمة المنظمة والأنشطة الإجرامية ذات الصلة بها، مثل غسل الأموال[2].

---

[1] صوان آسيا ، **التعاون الدولي في مكافحة الجرائم المعلوماتية** ،،مذكرة لنيل شهادة ماستر جامعة عبد الحميد بن باديس, مستغانم سنة 2022 ص71.

[2] معتوق محمد اكلي ،**التعاون الدولي في مكافحة الجريمة الالكترونية** ، مذكرة لنيل شهادة الماستر في الحقوق ، جامعة محمد البشير الابراهيمي ،برج بوعريريج ،سنة 2023 ص 41.

ثانيا : إستراتيجيات الأنتربول في مكافحة الجرائم الإلكترونية:

أبدت هذه المنظمة جهود في مجال التصدي للجرائم المعلوماتية حيث أنشأت سنة 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا ونظمت تعاون مع مجموعة الدول الثماني الكبرى G8 بوضع استراتيجيات لمواجهة هذا النوع من الجرائم من خلال[1]:

1/ استحداث مركز اتصالات أمني عبر الشبكة على مستوى مصالح شرطة دول الأطراف ويعمل على مدار 24ساعة ولمدة 07 أيام في الأسبوع.

2/انتهاج وسائل حديثة في محاربة الجرائم المعلوماتية كاستخدام برنامج Excalibur الذي يحلل ويقارن بطريقة أوتوماتيكية الصور الإباحية من قبل دول الأطراف .

3/إنشاء كتيبات إرشادية حول الجرائم المعلوماتية وكيفيات التدريب على محاربتها والتحقيق فيها وتقديمها لشرطة دول الأطراف، كما عملت الأنتربول على إقامة علاقات بين الدول والمنظمة ومشاركة المعلومات مع سلطات تحقيق الدول التي تشهد انتشارا واسعا لهذا النوع من الجرائم .

4/بالإضافة إلى جهود الشرطة الدولية للويب IWP والتي تم إنشائها سنة 1987 تحت شعار "الخدمة والحماية" بحيث تتخصص هذه المنظمة في الحماية من الجرائم الإلكترونية والعمل على ردعها في كافة أنحاء العالم .

5/وأيضا جهود الأورجيست وهو عبارة عن جهاز يساهم على تعزيز التعاون القضائي والشرطي في مواجهة شتى أنواع الجرائم الخطيرة للأنترنت على المستوى الأوروبي، بجانب جهود الشرطة الأوروبية Europol التي تعمل على حفظ الأمن في أوروبا التي تعمل على التصدي للجرائم الإلكترونية وكذا فضاء شحن Schengen والذي سهل التعاون الشرطي من خلال مراقبة المشتبه فيهم عبر الحدود وملاحقتهم والتصدي للجرائم المعلوماتية .

أما على المستوى العربي عمل المجلس وزراء الداخلية للعرب و هو هيئة رئيسية تابعة لجامعة الدول العربية على تنسيق التعاون بين الدول العربية في مجال مكافحة الجرائم بشكل عام والجرائم المعلوماتية بشكل خاص[2].

[1] معتوق محمد اكلي ،مرجع سبق ذكره، ص 42

[2]

ثالثا : أهداف الأنتربول :

تستهدف هذه المنظمة تأكيد وتشجيع التعاون بين سلطات البوليس في الدول الأطراف وطبقا للمادة الثانية من ميثاق المنظمة تتمثل أهم أهدافها في:

أ-جمع المعلومات المتعلقة بالجرائم والمجرمين، وذلك عن طريق المعلومات التي تتسلمها المنظمة- بالمكتب الرئيسي في ليون الذي يعد من المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء ، ويتم ذلك عبر شبكة إتصالات حديثة.

ب-التعاون مع الدول الأعضاء في ضبط الهاربين والمطلوبين-أيا كانت جنسياتهم -والصادر ضدهم أحكام قضائية ، أو أوامر بالضبط والإحضار لمثولهم أمام جهات التحقيق ، وذلك من خلال إصدار النشرات الدولية المخصصة.

ج_ دعم جهود الشرطة في مكافحة الإجرام العابر للحدود، وتقديم الخدمات في مجال الأدلة الجنائية، كبصمات الأصابع، والحمض النووي .

د- إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام.

هـ-تأمين وتنمية التعاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان وبروح الإعلان العالمي لحقوق الإنسان[1].

العمل على تأمين وتنمية التعاون الدولي بين كافة أجهزة الشرطة الجنائية في الدول الأعضاء.

إنشاء وتفعيل كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام ومكافحتها.

العمل على منع الجرائم الدولية، أو الحد منها عن طريق مكافحة الإجرام العابر للحدود، وعن طريق تعقب المجرمين والجرائم المرتكبة، وتسهيل عمليات إلقاء القبض عليهم وتسليمهم إلى الجهات المختصة .

المطلب الثاني: التعاون القضائي.

الفرع الأول : تعريف المساعدة القضائية الدولية

تعرف المساعدة القضائية الدولية على أنها" كل فعل أو إجراء قضائي تقوم به الدولة من شأنها تسهيل مهمة المحاكمة في دولة اخرى بصدد جريمة من الجرائم.

[1] يوسف صغير، **آليات مكافحة الجريمة المرتكبة عبر الانترنت**، اطروحة لنيل درجة دكتوراه في العلوم تخصص قانون ، جامعة مولود معمري ،تيزي وزو ص73.

وتتم هذه المساعدة القضائية عبر المعاهدات الدولية بهدف التصدي للجرائم في إطار الجنائي وتتمثل في تجميع عناصر الأدلة من أجل الإعانة في المواد الجنائية، انجاز عمليات البحث، تسليم المعلومات والوثائق التي تلزم سلطة قضائية الأجنبية وكذا تقديم الوثائق المتعلقة بالحالة الجنائية[1].

الفرع الثاني : خطوات المساعدة القضائية:

إن انجاز هذه المساعد القضائية لايكمل إلا بإتمام ثلاث خطوات هي:

1/الطلب: هو طلب يتم تقدميه من طرف الدولة صاحبة الإختصاص الجنائي بالمحاكمة والتي تحتاج إلى المساعدة بهذا الشأن إلى الدولة التي ستقوم بإغاثتها ويتم الطلب حسب قانون الدولة الطالبة في إطار إتفاقية أو المعاهدة التي أبرمتها مع الدولة المساعدة والأصل أن هذه الطلبات تتم وفقا لسبل الدبلوماسية لكن بعض المعاهدات الدولية تتيح الفرصة للإتصال السريع والمباشر بين جهات العدل الدولتين لغاية ربح الوقت.

2/فحص الطلب: هو الخطوة الثانية لتحقيق المساعدة القضائية وهو إجراء تختص به الدولة التي ستقدم المساعدة ويتم ذلك من خلال التأكد ما إذا الواقعة المطلوب تحقيقها تعتبر فعلا مجرما طبقا لقانون الدولة الطالبة ودراسة مدى اختصاصها، أما الإجابة على هذا الطلب تكون بموجب ما نصت عليه بنود المعاهدات التي تمت مع الدولة الطالبة للمساعدة.

تنفيذ المساعدة القضائية: وهذه الخطوة تنفذ وفقا لقواعد قانون الدولة التي سوف تمد الإعانة[2].

الفرع الثالث : صور المساعدة القضائية.

إن المساعدة القضائية بعد استكمال شروطها تتخذ صور منها [3]:

أولا : تبادل المعلومات .

يقصد بتبادل المعلومات تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة من الجرائم عن الإتهامات التي وجهت إلى رعاياها في الخارج و الإجراءات التي اتخذت ضدهم.

وقد يتضمن مشاركة وتقديم السوابق القضائية للجناة، فمن خلالها تتعرف الجهات القضائية بدقة على الماضي الجنائي للفرد المحال إليها، وهي تساعد في تقرير الأحكام الخاصة بالعود، ووقف تنفيذ العقوبة.

---

[1] عثماني رضوان ،**مكافحة جرائم المعلوماتية في القانون الجزائري والدولي** ، اطروحة للحصول على شهادة دكتوراه في العلوم تخصص قانون جنائي ،جامعة محمد بن أحمد ،وهران 2 سنة 2024،ص 197.

[2] صوان آسيا ، مرجع سبق ذكره، ص 60.

[3] عثماني رضوان ،مرجع سبق ذكره، ص 198.

ولقد نصت المادة23 من الإتفاقية الأوروبية على هذا الإجراء بخصوص الجريمة الإفتراضية حيث نص بوضوح على ضرورة التعاون بين الدول الأطراف وبلورته والتخلص من القيود وذلك من اجل توفير السهولة والسرعة الممكنة لإتمام هذا إجراء تبادل المعلومات وتبادل الأدلة بين الطرفين.

ثانيا : نقل الإجراءات

يقصد به قيام إحدى الدول باتخاذ الإجراءات الجنائية بشأن جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه دولة بناءا على إتفاقية " وذلك إذا توافرت شروط معينة أهمها:

1-أن يكون الفعل المنسوب الى الشخص يشكل جريمة في الدولة الطالبة والمطلوب منها المساعدة القضائية.

2-أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدول المطلوب عن ذات الجريمة.

3-أن يكون الإجراء المطلوب اتخاذه يؤدي إلى الوصول إلى الحقيقة، كأن تكون أدلة الجريمة موجودة بالدولة المطلوب منها.

ولقد أقرت العديد من الإتفاقيات الدولية والإقليمية هذه الصورة كإحدى المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية [1].

ثالثا : الإنابة القضائية

تمثل صورة من صور التعاون الإقليمي بين الجهات القضائية، و يقصد بها تقديم طلب من دولة تريد المساعدة إلى الدولة المراد منها المساعدة بهدف اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية.

وذلك من أجل الفصل في مسألة المعروضة على السلطة القضائية الطالبة للمساعدة و التي لم تقدر على القيام بها لوحدها والمراد هو تسهيل الإجراءات الجنائية بين الدول فيما يخص إجراءات التحقيق وتقديم المتهمين للمحاكمة وكذا تجاوز مشكلة السيادة الإقليمية التي من شأنها إعاقة الدولة الأجنبية في مزاولة بعض الأعمال القضائية داخل أقاليم الدول الأخرى كإجراء التفتيش وسماع الشهود[2].

وبذلك فإن الغاية من الإنابة القضائية هو تبسيط الإجراءات وتأمين سرعة القيام بها والتقليص من الصعوبات التي تعيق تطبيق القوانين وأساس الإنابة القضائية في اتفاقيات الدولية والقوانين الوطنية ومبدأ المعاملة بالمثل.

---

[1] عثماني رضوان ،مرجع سبق ذكره، ص 198.

[2] رابيا نونور، **التعاون القضائي الدولي في مكافحة الجريمة المنظمة العابرة للحدود الوطنية** ، مذكرة لنيل شهادة الماستر في القانون ،جامعة مولود معمري ،تيزي وزو سنة 2016 ص 75.

وللإنابة القضائية في نطاق التصدي للجريمة ذات الطابع الدولي بشكل عام والجرائم الإلكترونية بشكل خاص عدة مميزات منها:

* الإهتمام بإحترام السيادة الوطنية والمحافظة عليها وذلك عن طريق تخويل أجهزة أمنية مختصة للقيام بالإجراءات المطلوبة على أرض الدولة دون تدخل من الأجهزة الأمنية التابعة للدولة الطالبة.

* مساهمة هذا التعاون في المحافظة على الأدلة وضمان عدم ضياعها وإتمام التحقيقات الواقعة الدولة الطالبة.

* يضمن هذا التعاون حقوق المتهمين من سرعة في المحاكمة وتامين عدم تركهم في السجن دون محاكمة ريثما تكتمل الإجراءات القانونية في دولة أخرى، تستدعي الإنابة القضائية أن يرسل الملف المتعلق بالدعوى الجنائية يتضمن مستندات ووثائق ومحاضر التحقيق التي نفذت بعلم السلطة القضائية في الدولة المطلوب منها اتخاذ بعض الإجراءات.

الفرع الرابع: تسليم المجرمين

هو إجراء قضائي في مجال التعاون القضائي ويقصد به قيام دولة ما (الدولة المطلوب منها التسليم) بتسليم الشخص المتواجد على إقليمها إلى للدولة الطالبة بناءا على طلبها بغرض محاكمته عن جريمة اتهم بارتكابها، او من اجل تنفيذ حكم الصادر في حقه من محاكم هذه الدولة أو المحكمة الدولية.

ومن أجل وضع حدود للعلاقة التي على أساسها يتم إجراء تسليم المجرمين بين دول الأطراف وجب توافر شروط أساسية المتمثلة في:

الشرط الأول: التجريم المزدوج ويقصد به أن يكون الفعل الذي يستدعي التسليم مجرما في قانون كلا الدولتين الطالبة والمطلوب إليها التسليم ، كما يشترط تبعا لشرط ازدواجية التجريم ألا تكون الدعوى الجنائية انقضت أو تقادمت طبقا لأي قانون من الدولتين لأن الهدف من إجراء تسليم المجرمين هو محاكمة الشخص أو تنفيذ العقوبة المقررة في حقه .

أما الشرط الثاني يتمثل في أن يكون الفعل المجرم من الجرائم الجائز بشأنها التسليم ويختلف تصنيف وتعريف الجرائم محل التسليم باختلاف نهج الاتفاقيات الدولية والقوانين الوطنية فهناك من ينتهج التعداد الحصر من خلال تحديد جرائم على سبيل الحصر وهناك من ينتهج وضع قائمة سلبية للجرائم او الحالات التي لا يجوز فيها التسليم وهذا النهج هو الأكثر شيوعا[1]. "

[1] وريدة جنيدلي ، **التعاون الدولي لمكافحة الجريمة المعلوماتية الفاعلية والتحديات** ،مجلة القانون والعلوم السياسية المجلد 10 العدد 02 سنة 2024 ص 329

أما إجراءات طلب التسليم تكون بعد إتباع الشروط المتعلقة بالأشخاص المطلوب تسليمهم، بحيث نصت اتفاقية بودابست الإجراءات التي يجب إتباعها في تسليم المجرمين من دولة إلى أخرى في المادة 24 فقرة 07 حيث نصت على:

ضرورة إخطار السكرتير العام لمجلس أوروبا بإسم وعنوان كل سلطة مسؤولة عن إصدار أو تلقي طلبات التسليم من قبل كل طرف عند التوقيع أو التصديق، أو يخطر أوامر الضبط التحفظي في حالة غياب للاتفاقية، إنشاء سجل جديد وخاص لسلطات المسؤولة التي تعينها الأطراف، وذلك من قبل السكرتير العام لمجلس أوروبا، مع التزام كل طرف بما يحتويه ذلك السجل باستمرار .

المبحث الثاني: مدى فعالية التعاون الإقليمي في مكافحة الجريمة الإلكترونية

يعد التعاون الإقليمي من الأدوات الأساسية التي تعتمدها الدول لمواجهة التحديات المتزايدة التي تفرضها الجرائم الإلكترونية، باعتبارها ظاهرة عابرة للحدود لا يمكن مواجهتها بجهود وطنية منفردة. وقد تم اعتماد عدة آليات إقليمية لتحقيق هذا الهدف، من أبرزها الاتفاقيات متعددة الأطراف كاتفاقية الجامعة العربية لمكافحة جرائم تقنية المعلومات (2010)، واتفاقية مالابو للاتحاد الإفريقي (2014)، إضافة إلى أجهزة الشرطة الإقليمية مثل الأفريبول والأوروبول التي سيتم التطرق لهم في المطلب الاول .

اما بالنسبة للمطلب الثاني فسنتطرق فيه الى مدى مساهمة التعاون لمكافحة الجريمة الالكترونية

المطلب الأول : آليات التعاون الإقليمي

الفرع الأول: الآليات المؤسساتية :

أولا/الشرطة الإفريقية الأفريبول (Afripol) :

هي منظمة الشرطة الجنائية للدول الإفريقية التي تم انشائها سنة 2015، يوجد مقرها بالجزائر العاصمة وتضم (41) دولة . وقد جاءت لتسهيل التعاون وتبادل المعلومات بين إدارات الشرطة الوطنية للدول الاعضاء في مكافحة الجرائم الدولية والارهاب المخدرات وتهريب الأسلحة والمتاجرة فيها على المستوى الإفريقي ومن أهم ما تهدف إليه المنظمة نذكر مايلي:

–وضع استراتيجية افريقية لمحاربة الإجرام.

–تعزيز القدرات التحليلية للشرطة الإفريقية في مجال تقدير المخاطر الإجرامية واقتراح الحلول المناسبة لها، وتحقيق التضامن والتعاون فيما بين إدارات الشرطة في إطار العمليات الأمنية[1].

[1] ثورية بوصلعة ،**السياسة الجنائية والامنية في مواجهة الجريمة العابرة للحدود**، اطروحة دكتوراه ،جامعة أبو بكر بلقايد ،تلمسان سنة 2018 ،ص190 –191

-تطوير الشرطة الإفريقية ماديا وبشريا من خلال ضمان الاطار التكويني الملائم والذي يتماشى وطبيعة القارة الإفريقية.

-وضع مركز افريقي خاص بالشرطة العلمية والتقنية والتحليل الجنائي ومحاربة الجريمة العابرة للحدود والمخدرات.

-تبني الطرق الصحيحة والمناسبة والعملية في مجال حوكمة الشرطة واحترام حقوق الانسان والتسيير الديمقراطي لمناهج الشرطة في كيفية التعامل في حالة الشغب واسترجاع النظام العام.

-توفير الوسائل العلمية والتكنولوجية ووسائل التدخل للشرطة الإفريقية وذلك من خلال المساعدة التقنية للاتصال وتبادل الخبرات العملية الخاصة بمكافحة الاجرام والتحليل الجنائي واستعمال التكنولوجيا وتبني طرق أمنية متجددة.

ثانيا : أجهزة آلية الاتحاد الافريقي للتعاون الشرطي:

تتشكل آلية "الأفريبول" من عدة أجهزة تتمثل في [1]:

1/ الجمعية العامة: تعتبر السلطة الفنية العليا في "الأفريبول" وتتكون من قادة الشرطة للدول الأعضاء وتضطلع بمسؤولية توفير التوجيه القيادي فيما يتعلق بالتعاون الشرطي في قارة إفريقيا، ولعل أهم المهام التي تناط بها والمتصلة بالردع الالكتروني تتمثل في :

وضع وتنفيذ والإشراف على السياسات المتعلقة بمجابهة الإجرام الالكتروني داخل القارة الإفريقية، وإعداد الخطوط التوجيهية وتحديد أولويات عمل "الأفريبول" في هذا المجال.

-بحث مشروع الميزانية والهيكل المقترح "للأفريبول"، من أجل تعزيز دور هذه الآلية في التصدي للجريمة الالكترونية وعرضهما على أجهزة السياسة للاتحاد الإفريقي وفقا للنظم واللوائح المالية للإتحاد.

-إعداد تقرير سنوي عن عملها وتقديمه إلى أجهزة صنع السياسة للإتحاد الإفريقي من خلال اللجنة الفنية المتخصصة للدفاع والسلامة والأمن.

2/لجنة التوجيه :تتشكل لجنة التوجيه لآلية الإتحاد الإفريقي للتعاون الشرطي" أفريبول" من الأعضاء الخمسة (5) لهيئة مكتب الجمعية العامة مفوض السلم والأمن للإتحاد الإفريقي رؤساء المنظمات الإقليمية للتعاون الشرطي المدير التنفيذي لآلية الإتحاد الإفريقي للتعاون الشرطي، ويقوم برئاسة لجنة

[1] عبد العزيز لزعر ،**آلية الاتحاد الإفريقي للتعاون الشرطي الأفروبول ودورها في مكافحة الجريمة الالكترونية**، مجلة المتون .جامعة مولاي الطاهر ،سعيدة سنة 2021 ص 255.

التوجيه رئيس الجمعية العامة، ويتم النص في قواعد الإجراءات على وظائف لجنة التوجيه ومعدلات اجتماعاتها وإجراءاتها.

3/ الأمانة : حيث نص النظام المنشأ لآلية "الأفريبول" على تأسيس أمانة خاصة بهذه الآلية.

بحيث يكون المدير هو المسؤول التنفيذي لهذه الآلية الإفريقية ويقوم بتقديم تقارير منتظمة إلى مفوضية الأمن والسلم بالإتحاد الإفريقي، على أن تعيين المدير يتم بواسطة الجمعية العامة التي تتكون من رؤساء الشرطة للدول الأعضاء بناءا على توصية من لجنة التوجيه، وتكلف الأمانة العامة بعدة مهام أهمها يتمثل في ضمان الإدارة الفعالة "الأفريبول"، بالإضافة إلى عقد وخدمة اجتماعات الجمعية العامة ولجنة التوجيه والاجتماعات الأخرى "للأفريبول" مع الإبقاء على اتصالات مع السلطات الوطنية والدولية المعنية بإنفاذ القانون.

ثانيا : الشرطة الأوروبية (EUROPOL)

يمثل الأوروبول جهاز الشرطة الجنائية على مستوى الاتحاد الأوروبي، انشأ في لكسمبورغ بموجب الاتفاقية 26 جويلية 1995 ودخل حيز الخدمة في عام 1999 بعد أن اتخذ مقره في مدينة لاهاي بهولندا، ليكون همزة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال ملاحقة الجرائم العابرة للحدود بما فيها جرائم الإرهاب والمخدرات الجريمة المنظمة، وكذا الجرائم الالكترونية .

ويهدف أساسا هذا الجهاز إلى تسهيل عملية البحث والتحري وتبادل المعلومات بين سلطات الأمن التابعة لدول الاتحاد، وتجميع، تخزين وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص جريمة من الجرائم المذكورة بما فيها الجريمة الالكترونية .

كما يتولى الأوروبول إسداء النصيحة وتقديم التوجيهات والإرشادات المفيدة ومختلف أنواع الدعم (المادي أو اللوجستيكي لهيئات التحقيق الوطنية.

ولتنفيذ هذه المهام يضمن هذا الجهاز اتصالا دائما ومتواصلا وسريعا مع السلطات المختصة في الدول الأعضاء عن طريق ما يسمى بنقاط اتصال[1].

وينشط الأوروبول في مجال مكافحة الجريمة الالكترونية مع نظام معلومات تشنجين (système d information Schengen) وهو نظام أنشأ في عام 1990 يتكون من قسم مركزي مقره مدينة ستراسبورغ و أقسام وطنية في كل دول المنظمة ، ويحد بنك معلومات ضخم تسجل فيه المعلومات التي ترسلها إليه قوات الشرطة القضائية من كل دولة عضو من بينها المعلومات المتعلقة بالأفراد المطلوب

[1] براهيمي جمال، مرجع سبق ذكره، ص 303.

تسليمهم من قبل دول أخرى، أو الممنوعين عن دخول أراضي دولة ما، أو المعلن اختفائهم أو المطلوب تقديمهم للعدالة بأمر قضائي لأي سبب كان .

كما يتفاعل الأوروبول في أداء مهامه مع جهاز الأوروجيست Eurojust) باعتباره وحدة للتعاون القضائي والتنسيق بين السلطات القضائية المكلفة بالتحقيق، وذلك عندما تمس الجريمة دولتين على الأقل من الدول في الاتحاد الأوروبي، أو دولة عضو مع دولة أخرى خارج الاتحاد فيتم تبادل المساعدات القضائية فيما بين الجهازين من خلال تبادل المعلومات تسهيل ونقل الإجراءات المتعلقة بالتحقيق والبحث في الجرائم العابرة للحدود تبادل الإنبات القضائية، تسليم المجرمين، وكذا التخفيف من مختلف العقبات والحواجز البيروقراطية التي تواجه سلطات إنفاذ القانون على المستوى الأوروبي .

ليس هذا فحسب، بل ولتفعيل وتوسيع التعاون الأمني عبر الحدود يتعامل الأوروبول مع وكالات استخباراتية متخصصة وأنظمة مراقبة ذات خبرة عالية، كوكالة فرانتكس (Frontex)، وهي وكالة أوروبية لإدارة التعاون العملياتي على الحدود الخارجية للدول أعضاء الاتحاد الأوروبي .

ونظام الأورودك (Eurodac)، وهو نظام معلوماتي واسع النطاق يحتوي على البصمات الرقمية لطالبي اللجوء والمهاجرين غير الشرعيين الموجودين على إقليم الاتحاد الأوروبي .

وكذا نظام الاوروسير (Eurosur)، وهو نظام لتبادل المعلومات بخصوص مراقبة الحدود الأوروبية، يشمل على برنامج مشترك لتكنولوجيا المعلومات و يعمل على تمكين السلطات المشاركة في إطاره من تقييم و رؤية الوضع على الفور في الاتحاد الأوروبي وما وراء الحدود الخارجية للإتحاد[1].

إلى جانب ذلك، استحدث جهاز على مستوى الأوروبول في عام 2010 أطلق عليه اسم (Internet Crime Reporting Online ICROS) مهمته توفير أكبر قدر ممكن من التعاون والتنسيق الأمني السريع في مجال مكافحة الجريمة الالكترونية بين دول الاتحاد الأوروبي وهو الجهاز الذي تم تدعيمه مؤخرا في جويلية 2017 بهيئة أخرى متخصصة تدعى المركز الأوروبي للجريمة الالكترونية (EC3)، والذي سيكون كما قال رئيسه ترويلس أو يرتينج)، همزة وصل بين الدول الاعضاء تنصهر فيها الجهود ومركزا للدعم الاستخباراتي والتشغيلي والقضائي يقوم بالرد على الجرائم الإلكترونية، بالإضافة إلى قدرته على تعبئة كل مصادر الدول الأعضاء في الاتحاد الأوروبي التي من شأنها تقليص والحد من آثار تهديدات المجرمين الإلكترونيين أينما حلوا وسيعمل على تزويد الشرطة وسلطات إنفاذ القانون في الدول

[1] براهيمي جمال، مرجع سبق ذكره، ص 304.

الأعضاء، بمعلومات حول اتجاهات الجرائم الإلكترونية الجارية، بالإضافة إلى تفاصيل عن التهديدات الناشئة .

مواصلة لهذه الجهود، فقد تم استحداث عدة آليات أخرى لتسهيل وتعزيز عملية التعاون الأمني على الصعيد الأوروبي، منها الاعتراف في عام 2002 بمذكرة القبض الأوروبية (Mandat d'arrêt européen) والتي دخلت حيز النفاذ في عام 2004 كإجراء يسمح لسلطات الضبط القضائي في أي دولة عضو في الاتحاد الأوروبي القبض على المتهم الهارب إلى إقليمها تنفيذا لحكم إدانة نهائي صادر عن هيئة قضائية لدولة أخرى عضو دون التقيد بشرط التجريم المزدوج، وتسليمه إلى هذه الأخيرة وفقا لشروط تسليم المجرمين .

الفرع الثاني: الآليات القانونية الإقليمية العربية و الإفريقية لمكافحة الجريمة المعلوماتية

أولا : الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

حررت هذه الاتفاقية بالقاهرة في 21 ديسمبر 2010 و هي تعتبر تتويجا لجهود الدول العربية ، وقد صادقت عليها الجزائر بموجب بالمرسوم الرئاسي رقم 14 252 المؤرخ في 08-09-2014، وكان الهدف منها التصدي لهذا النوع المستحدث من الجرائم، حيث أكدت هذه الاتفاقية في مقدمتها على أنها جاءت تجسيدا الرغبة هذه الدول في توطيد التعاون فيما بينها للقضاء على هذه الجرائم التي أضحت تهدد أمنها وسلامتها ، وتوحيد الروى وتوجيه الأفكار لأخذ بسياسة جنائية مشتركة و متقاربة ، هدفها الاسمى تحقيق حماية للمجتمع العربي ككل مع الأخذ في الحسبان طبيعة هذه المجتمعات، و ما يميزها من توجه ديني و أخلاقي الذي جاء به ديننا الحنيف، وكذا بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الإجرام وصوره ، مع الأخذ بالحسبان النظام العام لكل دولة، وفي هذا الصد نجد المادة الأولى منها قد أشارت أن هذه الاتفاقية جاءت لتوحيد جهود الدول العربية وتعزيز التعاون المتبادل فيما بينها بغية مجابهة الجرائم الإلكترونية والتصدي لمخاطرها الأمر الذي يعود بالفائدة على مصالحها مجتمعة خاصة من الناحية الأمنية في هذا المجال وسلامة الموطنين ، وقد تضمنت هذه الاتفاقية خمسة فصول بمجموع 42 مادة، شملت التعريف بالمصطلحات كما نصت على جرائم الاحتيال والتزوير الإلكتروني، وكذا جرائم الماسة بالحياة الخاصة وحرمة الإنسان والجرائم الإباحية ، وطرق التفتيش والتعاون القانوني والقضائي وتسليم المجرمين... إلخ[1].

[1] بن عبو عفيف **الآليات القانونية في الجزائر وتطورها في مكافحة الجريمة الالكترونية** ،مجلة حقوق الانسان والحريات العامة المجلد 9 العدد 1 سنة 2024 ص41 ص42.

ومن خلال استقرائنا لهذه الاتفاقية يتبين لنا بأنها تعتبر نقطة تحول هامة في مجال مكافحة جرائم تقنيات المعلومات، وحسنا ما فعل المشرع الجزائري عندما صادق عليها و أخذا بما جاء فيها، نظرا لأنها جاءت مدعمة لسياسته الجنائية التي سبق و إن لجأ اليها، كما تمثل أيضا تكملة للنقائص المسجلة في القوانيين السابقة، خاصة ما تعلق ببعض الجرائم مثل التزوير المعلوماتي والإباحية الإلكترونية.

ثانيا : إتفاقية الاتحاد الإفريقي (مالابو) :

في ظل تصاعد التهديدات المرتبطة بالفضاء السيبراني، سعى الاتحاد الإفريقي إلى وضع آلية قانونية إقليمية تهدف إلى تنسيق جهود الدول الأعضاء لمواجهة الجرائم الإلكترونية، وهو ما تُرجم باعتماد اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات ذات الطابع الشخصي، المعروفة بـ"اتفاقية مالابو"، بتاريخ 27 جوان 2014، خلال القمة الثالثة والعشرين للاتحاد الإفريقي المنعقدة بمدينة مالابو، عاصمة غينيا الاستوائية.

وتُعتبر هذه الاتفاقية من أبرز أدوات التعاون الإقليمي الإفريقي، حيث تهدف إلى:

... تعزيز ومواءمة التشريعات الحالية للدول الأعضاء والمجموعات الاقتصادية الإقليمية في مجال تكنولوجيا المعلومات والاتصالات، مع احترام الحريات الأساسية وحقوق الإنسان والشعوب.

.. إنشاء وثيقة معيارية مناسبة تتوافق مع البيئة القانونية والثقافية والاقتصادية والاجتماعية الإفريقية.

... التأكيد على حماية البيانات الشخصية والخصوصية وهي قضية رئيسية في مجتمع المعلومات، بحيث يجب أن تحترم أي معالجة للبيانات الشخصية التوازن بين الحريات الأساسية ومصالح الجهات الفاعلة العامة والخاصة

...تعزيز استخدام تكنولوجيا المعلومات والاتصالات، وزيادة التدفق وانقاص أسعار الأنترنيت ..العمل على تعهد كل دولة طرف باعتماد تدابير تشريعية أو تنظيمية لتحديد القطاعات التي تعتبر حساسة لأمنها القومي ورفاهية اقتصادها.

...العمل على تنظيم الاعتراف القانوني بالمعاملات التجارية والعقد والإمضاء الإلكترونيين، وإيجاد قواعد قانونية تحمي المستهلكين وحقوق الملكية الفكرية والبيانات الشخصية وأنظمة المعلومات، بالإضافة للتشريعات المتعلقة بالخدمات الهاتفية والعمل عن بعد وغيرها[1].

[1] مريم لوكال ،**قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014**، مجلة الدراسات القانونية والإقتصادية ، المجلد 4 ،العدد 3 سنة 2021.ص 661

كما تناولت هذه الاتفاقية ثلاثة محاور رئيسية:

1/تنظيم المعاملات الإلكترونية :

من خلال منح الوثائق الرقمية حجية قانونية، وضمان حقوق المستهلك في البيئة الإلكترونية .

2/ حماية البيانات ذات الطابع الشخصي : وذلك عبر إلزام المؤسسات بالحصول على موافقة الأفراد قبل جمع أو معالجة بياناتهم، وإنشاء هيئات وطنية مستقلة تشرف على احترام هذه المبادئ.

3/مكافحة الجرائم الإلكترونية: من خلال تجريم مجموعة من الأفعال مثل الدخول غير المشروع إلى الأنظمة المعلوماتية، الاحتيال عبر الإنترنت، ونشر المحتوى غير القانوني، مع التأكيد على أهمية التعاون وتبادل المعلومات بين الدول الأعضاء. ورغم أن الاتفاقية اعتُمدت منذ سنة 2014، إلا أن دخولها حيز التنفيذ بقي مشروطاً بمصادقة خمسة عشر دولة عضو، وهو ما تأخر نسبياً بسبب تفاوت جاهزية الدول الإفريقية من حيث البنية القانونية والمؤسساتية[1].

المطلب الثاني: مدى مساهمة التعاون في مكافحة الجريمة الإلكترونية.

الفرع الأول: اهداف التعاون الاقليمي في مكافحة الجريمة الالكترونية

تتمثل أوجه مساهمة التعاون لمكافحة الجريمة الالكترونية فيما بلي :

أولا: توحيد التشريعات بين الدول:

بحيث يساهم التعاون الإقليمي في دعم مواءمة التشريعات الوطنية حول الجريمة الإلكترونية لتقليص "الثغرات القانونية" التي قد تستغلها الشبكات الإجرامية.

ومثال ذلك : اتفاقية مالابو التي تُشجع الدول الإفريقية على سن قوانين تتطابق في تعريف الجريمة الإلكترونية والعقوبات،وهذا ما يسهل التعاون القضائي.

ثانيا:تعزيز تبادل المعلومات والتحقيقات:

لأن هذا التعاون يسمح بإنشاء قنوات لتبادل البيانات والمعلومات التقنية والاستخباراتية حول الهجمات السيبرانية، ما يُسرّع من تعقّب مرتكبيها. مثلا : إنشاء شبكات إقليمية بين أجهزة الشرطة (مثل AFRIPOL على مستوى إفريقيا) لتبادل المعلومات الفورية.

ثالثا: بناء القدرات وتكوين الموارد البشرية: وذلك من خلال التعاون بين الدول الذي يفتح المجال لتنظيم ورشات تدريب وتكوين ضباط أمن ومحققين في مجال الأدلة الرقمية.

[1] مريم لوكال، مرجع سبق ذكره، ص 662.

ومثال ذلك برامج التكوين التي ينظمها الاتحاد الأوروبي لدول البحر المتوسط، أو تلك الممولة من الاتحاد الإفريقي بالتعاون مع الاتحاد الدولي للاتصالات .

رابعا: حماية البنية التحتية الرقمية:

وذلك من خلال إنشاء استراتيجيات إقليمية للأمن السيبراني يتم التنسيق في حماية المنشآت الحيوية (بنوك، اتصالات، طاقة...). مثلا: الاستراتيجية السيبرانية للاتحاد الإفريقي التي تسعى لحماية البنى التحتية الإفريقية.

خامسا: التنسيق القضائي وتسليم المجرمين:

بحيث أنه يسهّل إجراءات تسليم مرتكبي الجرائم الإلكترونية عبر اتفاقيات ثنائية أو جماعية، خاصة وأن الجناة غالباً ما ينشطون من خارج حدود الدول المتضررة.

ومثال ذلك : التنسيق بين دول غرب إفريقيا لتسليم أفراد متورطين في جرائم الاحتيال الإلكتروني العابر للحدود .

سادسا:الاستجابة السريعة للحوادث السيبرانية

فالتعاون يتيح إنشاء فِرق استجابة طارئة إقليمية ، تتدخل بشكل جماعي لتقديم الدعم التقني للدول المتضررة من هجوم إلكتروني واسع. ففي حال حدوث هجوم إلكتروني على منشآت دولة ذات بنية ضعيفة، قد تتدخل فرق إقليمية للدعم الفني والتحقيق.

سابعا:تبادل الخبرات التشريعية والفنية :

يساعد التعاون في مشاركة التجارب الوطنية الناجحة في تطوير القوانين السيبرانية، ما يُسرّع من تحديث تشريعات الدول الأخرى. فمثلا نجد هناك بعض الدول الإفريقية مثل غانا قد استفادت من تجارب جنوب إفريقيا في إنشاء وحدات شرطة إلكترونية متخصصة[1].

الفرع الثاني : التحديات التي تعيق فاعلية التعاون الاقليمي:

يُعد التعاون الإقليمي أحد الركائز الأساسية لمواجهة الجرائم الإلكترونية ذات الطابع العابر للحدود، غير أن هذا التعاون يواجه جملة من التحديات التي تعيق فاعليته، ويمكن إبراز أهمها فيما يلي:

أولا: تفاوت التشريعات الوطنية: إن اختلاف الأطر التشريعية بين الدول الإقليمية بشأن تعريف الجريمة الإلكترونية وتجريمها، يُعد من أبرز العوائق التي تقف في وجه تفعيل التعاون الإقليمي، مما يُعقّد مسألة تسليم المجرمين والمساعدة القانونية المتبادلة، لغياب شرط ازدواجية التجريم في كثير من الأحيان.

[1] سليمان ابو نمر .مرجع سبق ذكره ص 56 -57.

ثانيا: قصور آليات التعاون القضائي: بحيث يُعاني التعاون القضائي الإقليمي من غياب هيئات تنسيقية دائمة ومحدودية فعالية الآليات القائمة، كالبطء في تنفيذ الإنابات القضائية، وصعوبة تبادل الأدلة الرقمية في ظل غياب اتفاقيات إجرائية تفصيلية تتضمن قواعد حماية المعطيات والخصوصية.

ثالثا: صعوبات في الاختصاص القضائي العابر للحدود: تطرح الجريمة الإلكترونية إشكالات قانونية متعلقة بتحديد الاختصاص الإقليمي، إذ قد تُرتكب الجريمة في إقليم دولة، بينما تقع نتائجها في إقليم دولة أخرى، ما يُولد تنازعًا في الاختصاص القضائي ويجعل من الضروري تطوير قواعد إقليمية موحدة في هذا المجال.

رابعا: ضعف تبادل المعلومات الاستخباراتية: رغم أهمية التعاون الأمني الوقائي، إلا أن تبادل المعلومات بين أجهزة الشرطة والأمن في الدول الإقليمية لا يزال محدودًا بسبب ضعف الثقة المتبادلة، والخشية من استغلال المعلومات لأغراض غير قانونية، إلى جانب غياب بنوك معلومات إقليمية مشتركة.

خامسا: الاختلاف في المعايير الإجرائية: يُعد اختلاف الإجراءات القضائية والضمانات القانونية (مثل شروط التفتيش الإلكتروني، ومدى حجية الدليل الرقمي) من العراقيل التي تُؤثر سلبًا على فعالية التعاون القضائي الإقليمي، مما يستدعي توحيد المعايير أو اعتماد اتفاقيات نموذجية إقليمية.

سادسا: محدودية الإطار المؤسساتي الإقليمي: تُواجه بعض المنظمات الإقليمية (مثل الأفريبول أو جامعة الدول العربية) قيودًا في الاختصاص التنفيذي أو التنسيقي، بسبب محدودية صلاحياتها أو الطابع غير الملزم لتوصياتها، مما يحد من قدرتها على الإشراف الفعلي على التعاون في مجال مكافحة الجرائم الإلكترونية.

سابعا: عدم كفاية الموارد التقنية والبشرية: تفتقر أغلب الدول الإقليمية إلى الكفاءات المتخصصة في الجريمة السيبرانية، وكذا إلى الوسائل التقنية اللازمة لرصد وتتبع الأدلة الرقمية وتقديم الدعم الفني للجهات القضائية، ما يُضعف من فعالية التعاون التقني والقضائي[1].

[1] ليندا شرابشة ، **السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية**، الاتجاهات الدولية في مكافحة الجريمة الالكترونية، ماجستير في قانون الدولي العام ،جامعة محمد شريف مساعدية، سوق اهراس، ص 249-251.

خلاصة الفصل الثاني :

يتّضح من خلال دراسة هذا الفصل أن الجريمة الإلكترونية تمثّل تهديدًا معقّدًا يتجاوز الحدود الوطنية، ويستلزم مواجهة جماعية تقوم على التعاون الثنائي والإقليمي بين الدول. وقد أثبت هذا التعاون، رغم بعض النقائص، أهميته البالغة في دعم الجهود الأمنية والقضائية، من خلال تبادل المعلومات، تنسيق التحقيقات، وتحديث الأطر القانونية، خاصة عبر آليات مثل المنظمات الإقليمية (كالأوروبول وأفريبول) والاتفاقيات متعددة الأطراف.

ورغم النجاحات المحققة، فإن فعالية هذا التعاون ما تزال نسبية، بسبب العوائق القانونية، التقنية، والسياسية التي تعترض سبيل التكامل بين الدول. فاختلاف التشريعات، وانعدام الثقة المتبادلة، ونقص الإمكانات التكنولوجية، تمثل تحديات رئيسية تُقلّل من فاعلية التصدي الجماعي لهذه الظاهرة.

لذلك، فإن تعزيز هذا التعاون يتطلب إرادة سياسية صادقة، وتوحيد الرؤى الاستراتيجية، وتطوير الآليات التقنية والقانونية الكفيلة ببناء جدار وقائي إقليمي مشترك ضد الجريمة الإلكترونية، يكون قادرًا على مجاراتها وملاحقة مرتكبيها بفعالية، حمايةً للأمن العام وسيادة القانون في الفضاء الرقمي.

خاتمة

خاتمة:

في ختام هذه الدراسة الخاصة بالتعاون الإقليمي في مجال مكافحة الجريمة الإلكترونية استخلصنا أن هذه الجريمة تختلف عن الجرائم التقليدية نظرا لعدم وضع تعريف جامع وموحد لها.

كما أن طبيعتها الخاصة تجسدت في خصائصها المتميزة والمتمثلة في أنها جريمة عابرة للحدود لكونها ترتكب بواسطة الحاسوب وفي مجال الحاسب الآلي، والسرعة في التنفيذ .

والتطور المستمر ومتسارع من حيث ارتكابها والخصوصية التي يتميز بها المجرم المعلوماتي ، باعتباره لا يلجا إلى العنف كما هو الحال في المجرم التقليدي، بل يتميز بالذكاء والمهارة والسلطة والمعرفة وهذا ما جعل القوانين الحالية عاجزة عن مكافحة هذا النوع من الجرائم نظرا لتطور الحاصل بالمجال تقنية المعلومات والمساس باهم الضمانات اللازمة لتطبيق مبدأ الشرعية الجزائية الذي مفاده "لا جريمة ولا عقوبة إلا بالنص " بحيث لا يمكن مساءلة شخص إلا عن سلوك حددت عناصره القانونية والعقوبة المقررة لها مسبقا، ليتمكن القضاة أيضا من إضفاء الصفة الجنائية على الفعل والتكييف القانوني للواقعة المجرمة.

هذا ما استدعى ضرورة التعاون الإقليمي والعمل على إيجاد قوانين وعقد مؤتمرات و إبرام اتفاقيات لتصدي لهذه الجرائم ذات البعد العالمي، غير أن اهتمام المشرع الجزائري بالجريمة الالكترونية وبالعقوبات المقررة لها من خلال النصوص القانونية لا يعد كافيا لمواجهة الإنتشار المخيف والتطور السريع لهذه الجريمة بل يجب إصدار قانون خاص بها يتضمن المصطلحات الخاصة بهذه الجريمة وأنواعها والعقوبات المقررة لها، مع وجوب تشديد العقوبات نظرا للأثار السلبية التي تخلفها على مؤسسات العامة والأشخاص وبصفة كبيرة على أمن الدولة.

ومن خلال دراستنا هذه توصلنا إلى جملة من النتائج التالية:

– نظرا لحداثة الجريمة الإلكترونية استحال وجود اجماع موحد على تعريفها.

– عالمية الجريمة الإلكترونية وطابعها العابر للحدود جعل من الصعب على الدول مواجهتها بشكل منفرد، ما فرض ضرورة اعتماد آليات التعاون الثنائي والإقليمي.

– الجرائم الإلكترونية لا تترك أثرا ماديا في مسرح الجريمة كما أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة.

–التعاون الإقليمي أثبت نجاعته النسبية من خلال إنشاء هياكل تنظيمية وأمنية مثل "الأوروبول" و"الأفريبول"، التي أسهمت في تسهيل تبادل المعلومات وتعزيز التنسيق بين الدول.

خاتمة:

-غياب تشريعات وطنية متوافقة مع الاتفاقيات الإقليمية يُعيق تنفيذ قرارات وآليات التعاون، ويخلق فراغًا قانونيًا في مواجهة المجرمين الإلكترونيين العابرين للحدود.

- وجود فجوة رقمية بين دول الإقليم الواحد يجعل من الصعب تحقيق تنسيق عملياتي متوازن وفعال، خاصة في مراحل التتبع والتحقيق والتحليل الرقمي.

وعلى ضوء دراستنا هذه ارتأينا الى بعض الاقتراحات تتمثل في:

1. العمل على إيجاد تعريف شامل وجامع للجريمة الالكترونية باختلاف أنواعها.

2. خلق ثقافة اجتماعية جديدة عن جريمة الالكترونية باعتبارها سلوك غير مشروع يترتب عنه عقوبات جزائية.

3.تعزيز الانضمام إلى الاتفاقيات الإقليمية والدولية المتخصصة في مكافحة الجريمة الإلكترونية، وعلى رأسها اتفاقية بودابست واتفاقية مالابو.

4.توسيع قاعدة تبادل المعلومات بين الدول في إطار من الثقة والاحترام المتبادل للسيادة، مع اعتماد آليات تشفير وأمن معلوماتي عالية مع ضرورة إنشاء قواعد بيانات إقليمية موحدة تتيح تتبع المجرمين الإلكترونيين والمشتبه فيهم، وتسهيل الوصول إلى المعلومات الأمنية ذات الصلة.

5.دعم الدول ذات الإمكانيات المحدودة تقنيًا وتشريعيًا، من خلال برامج إقليمية لبناء القدرات وتوفير الدعم اللوجيستي والفني.

6. ضرورة تدريس السلوكيات الإجرامية المتعلقة بالجريمة الالكترونية في كليات الحقوق والمعاهد القضائية ونشر الوعي القانوني .

قائمة المراجع

قائمة المصادر والمراجع :

أ) الإتفاقيات

2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 21-12-2010، والتي صادقت عليها الجزائر.

3. إتفاقية الاتحاد الإفريقي حول الأمن السيبيراني مالابو 2014 .

ب) النصوص القانونية:

4. .القانون رقم 09/04 الصادر في 5اوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،ج،ر العدد 47 .

5. القانون 18 – 07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية ،عدد 34، بتاريخ 10 يونيو 2018.

6. القانون رقم 06/22 المؤرخ في 20-12-2006 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية رقم 84.

7. القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، ج ر ،العدد 71،القسم السابع، مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.

ج) المراجع:

- الكتب :

8. أحسن بوسقيعة ،**الوجيز في القانون الجزائري العام** ،ط3 ،دار هومة للنشر ،الجزائر 2006 .

9. بلعليات ابراهيم،**أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري**،ط1 دار الخلدونية ،الجزائر 2007.

10. مصطفى يوسف كافي، **جرائم الفساد غسيل الأموال، السياحة الارهاب الالكتروني المعلوماتية ،** مكتبة المجتمع العربي للنشر والتوزيع ، الأردن ط1، 2014 .

11. خالد حسن أحمد لطفي، **جرائم الأنترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني** ، دار الفكر الجامعي الاسكندرية ، د ذ ط ، 2019 .

د) الرسائل والمذكرات :

-رسائل الدكتوراه :

12. براهيمي جمال، **التحقيق الجنائي في الجرائم الإلكترونية**، اطروحة لنيل شهادة دكتوراه في العلوم تخصص قانون ،جامعة مولود معمري ،تيزي وزو سنة 2018.

13. ثورية بوصلعة ،**السياسة الجنائية والامنية في مواجهة الجريمة العابرة للحدود**، اطروحة دكتوراه ،جامعة أبو بكر بلقايد ،تلمسان سنة 2018.

14. عثماني رضوان ،**مكافحة جرائم المعلوماتية في القانون الجزائري والدولي** ، اطروحة للحصول على شهادة دكتوراه في العلوم تخصص قانون جنائي ،جامعة محمد بن أحمد ،وهران 2 سنة 2024.

15. يوسف صغير، **آليات مكافحة الجريمة المرتكبة عبر الانترنت**، اطروحة لنيل درجة دكتوراه في العلوم تخصص قانون ، جامعة مولود معمري ،تيزي وزو .

- مذكرات الماستر :

16. معتوق محمد اكلي ،**التعاون الدولي في مكافحة الجريمة الالكترونية** ، مذكرة لنيل شهادة الماستر في الحقوق ، جامعة محمد البشير الابراهيمي ،برج بوعريريج ،سنة 2023 .

17. بن منصور ،صالح .**السلوك الإجرامي للمجرم المعلوماتي** ،مذكرة لنيل شهادة ماستر في الحقوق ،جامعة عبد الرحمان ميرة ،بجاية ،سنة 2014/2015 .

18. بعرة سعيدة ، **الجريمة الإلكترونية في التشريع الجزائري** ،مذكرة لنيل شهادة ماستر في الحقوق ،جامعة محمد خيضر ،بسكرة ،سنة 2015/2016 .

19. رابيا نونور ،**التعاون القضائي الدولي في مكافحة الجريمة المنظمة العابرة للحدود الوطنية** ، مذكرة لنيل شهادة الماستر في القانون ،جامعة مولود معمري ،تيزي وزو سنة 2016 .

20. حشيفة عبد الهادي' ، **التعاون الدولي في مكافحة الجرائم الإلكترونية**، مذكرة لنيل شهادة الماستر في الحقوق، جامعة زيان عاشور ،الجلفة سنة 2020.

21. عقباش بريزة ،**آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري** ،مذكرة لنيل شهادة الماستر في الحقوق ،جامعة محمد البشير الابراهيمي ، برج بوعريريج ،سنة 2021/2022 .

22. غربي جميلة ،**آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري** ،مذكرة لنيل شهادة الماستر في القانون ،جامعة أكلي محند اولحاج ،بويرة سنة 2020/2021.

23. سليمان ابو نمر ، **مكافحة الجريمة المعلوماتية في إطار القانون الدولي** ، مذكرة لنيل شهادة ماستر ،جامعة محمد خيضر، بسكرة ،سنة 2021.

24. صوان آسيا ، **التعاون الدولي في مكافحة الجرائم المعلوماتية** ،،مذكرة لنيل شهادة ماستر جامعة عبد الحميد بن باديس, مستغانم سنة 2022 .

25. نايري عائشة ،**الجريمة الإلكترونية في التشريع الجزائري** ،مذكرة لنيل شهادة الماستر في القانون الإداري ،جامعة أحمد دراية ،أدرار سنة 2016/2017 .

26. داود وسيلة ،**الجريمة الإلكترونية على ضوء قانون العقوبات الجزائري** ،مذكرة لنيل شهادة الماستر في الحقوق ،جامعة عبد الحميد بن باديس، مستغانم، سنة 2019

هـ)المجلات :

27. بن عبو عفيف **الآليات القانونية في الجزائر وتطورها في مكافحة الجريمة الالكترونية** ،مجلة حقوق الانسان والحريات العامة المجلد 9 العدد 1 سنة 2024 .

28. فريد ناشف ،**آليات التعاون الدولي في مكافحة الجريمة الالكترونية** ،مجلة البحوث في الحقوق والعلوم السياسية المجلد 8 العدد1 سنة 2022 .

29. مريم لوكال ،**قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014**،مجلة الدراسات القانونية والإقتصادية ، المجلد 4 ،العدد 3 سنة 2021.

30. عبد العزيز لزعر ،**آلية الاتحاد الإفريقي للتعاون الشرطي الأفروبول ودورها في مكافحة الجريمة الالكترونية**، مجلة المتون ،جامعة مولاي الطاهر ،سعيدة سنة 2021.

31. قيشاح نبيلة ،**ضمانات المراقبة الإلكترونية في التشريع الجزائري** ، مجلة الحقوق والعلوم السياسية جامعة خنشلة ،المجلد 10 العدد2 سنة 2023 .

32. عبد السلام طوبال ،**الضمانات القانونية لحماية المعطيات ذات الطابع الشخصي في التشريع الجزائري** ، مجلة العلوم القانونية والاجتماعية ،المجلد 5 ، العدد 2 سنة 2020 .

33. وريدة جنيدلي ، **التعاون الدولي لمكافحة الجريمة المعلوماتية الفاعلية والتحديات** .مجلة القانون والعلوم السياسية المجلد 10 العدد 02 سنة 2024 .

34. ياسين بن عمر ، **المعالجة القانونية للجرائم الإلكترونية في القانون الجزائري والتشريعات المقارنة** ،مجلة العلوم القانونية والسياسية المجلد 10 العدد 03 سنة ديسمبر 2019 .

35. عز الدين عثماني، **إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الإتصال والمعلوماتية**، مجلة دائرة البحوث والدراسات القانونية والسياسية ،مخبر المؤسسات الدستورية والنظم السياسية ،العدد4،2018.

فهرس المحتويات

قائمة المختصرات:..... Erreur ! Signet non défini.

مقدمة:..... Erreur ! Signet non défini.

الفصل الاول: الإطار المفاهيمي للجريمة الإلكترونية

المبحث الأول: مفهوم الجريمة الإلكترونية..... 6

المطلب الأول: تعريف الجريمة الإلكترونية..... 6

المطلب الثاني : اركان الجريمة الالكترونية وانواعها..... 10

المبحث الثاني: معالجة الجريمة الالكترونية في التشريع الجزائري..... 18

المطلب الأول : المعالجة القانونية للجريمة الإلكترونية..... 19

المطلب الثاني: المعالجة الاجرائية للجريمة الإلكترونية:..... 22

خلاصة الفصل الأول:..... 28

الفصل الثاني: التعاون الإقليمي لمكافحة الجريمة الإلكترونية

المبحث الأول: مجالات التعاون في مجال المكافحة الإلكترونية. 31

المطلب الأول : التعاون الأمني..... 31

المطلب الثاني: التعاون القضائي..... 35

المبحث الثاني: مدى فعالية التعاون الإقليمي في مكافحة الجريمة الإلكترونية..... 39

المطلب الأول : آليات التعاون الإقليمي..... 39

المطلب الثاني: مدى مساهمة التعاون في مكافحة الجريمة الإلكترونية..... 45

خلاصة الفصل الثاني : 48

خاتمة:..... 50

قائمة المصادر والمراجع : 53

الملخص: 58

الملخص

الملخص:

نظرا لاتساع نطاق الجرائم الإلكترونية تسعى الاتفاقيات والمنظمات الاقليمية بغض النظر عن اختلافها إلى جانب الدول لمكافحة هذا النوع من الجرائم.

سواء من خلال النص على الأفعال التي تعد جرائم إلكترونية ضمن مواثيقها ، وعقد المؤتمرات الخاصة بها أو من خلال تفعيل آليات التعاون الاقليمي بين الدول والزامها بها،

ورغم تعدد أشكال هذا التعاون في سبيل قمع هذه الجرائم والحد منها إلا أنه توجد عدة تحديات تواجه الدول في تحقيق مسعاها وتنقص من فعاليتها كقاعدة ازدواج التجريم ، ومسألة السيادة الوطنية.

كلمات مفتاحية: مكافحة ، الجريمة الإلكترونية ،الفاعلية ، التحديات، التعاون الإقليمي.

Abstract :

Due to the breadth of the scope of cybercrime, regional conventions and organizations, regardless of their differences, are working together with states to combat this type of crime .

Whether by stipulating acts that are considered cybercrimes within their charters , holding their own conferences, or by activating regional cooperation mechanisms between states and committing them،

Despite the multiplicity of forms of such cooperation in order to suppress and reduce these crimes, there are several challenges facing states in achieving their endeavor and reducing its effectiveness as a rule of double criminality and the issue of national sovereignty.

Keywords: counteraction, cybercrime, effectiveness, challenges, regional cooperation.