جامعة وهران 2-محمـــد بـن أحمـد

كلية الحقوق والعلوم السياسية

أطروحة

مقدمة للحصول على شهادة دكتوراه في العلوم

تخصص قانون جنائي

مكافحة جرائم المعلوماتية في القانون الجزائري والدولي

مقدمة ومناقشة علنا من طرف

الطالب: عثماني رضوان

أمام لجنة المناقشة:

الاسم واللقب	الرتبة	المؤسسة الأصلية	الصفة
أ.د.العربي شحط عبد القادر	أستاذ	جامعة وهران 2	رئيسا
أ.د.قمراوي عز الدين	أستاذ	جامعة وهران 2	مشرفا ومقررا
د.بربيح محي الدين	أستاذ محاضر أ	جامعة وهران 2	مناقشا
أ.د.ادريس خوجة نظيرة	أستاذة	جامعة سيدي بلعباس	مناقشا
أ.د.عيساني رفيقة	أستاذة	جامعة مستغانم	مناقشا
د.عمامرة حسان	أستاذ محاضر أ	جامعة الشلف	مناقشا

السنة الجامعية: 2024/2023

جامعة وهران 2-محمـــد بـــن أحمـــد

كلية الحقوق والعلوم السياسية

أطروحة

مقدمة للحصول على شهادة دكتوراه في العلوم

تخصص قانون جنائي

مكافحة جرائم المعلوماتية في القانون الجزائري والدولي

مقدمة ومناقشة علنا من طرف

الطالب: عثماني رضوان

أمام لجنة المناقشة:

الاسم واللقب	الرتبة	المؤسسة الأصلية	الصفة
أ.د.العربي شحط عبد القادر	أستاذ	جامعة وهران 2	رئيسا
أ.د.قمراوي عز الدين	أستاذ	جامعة وهران 2	مشرفا ومقررا
د.بربيح محي الدين	أستاذ محاضر أ	جامعة وهران 2	مناقشا
أ.د.ادريس خوجة نظيرة	أستاذة	جامعة سيدي بلعباس	مناقشا
أ.د.عيساني رفيقة	أستاذة	جامعة مستغانم	مناقشا
د.عمامرة حسان	أستاذ محاضر أ	جامعة الشلف	مناقشا

السنة الجامعية: 2024/2023

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

﴿ رَبِّ إِنِّي لِمَآ أَنزَلۡتَ إِلَيَّ مِنۡ خَيۡرٖ فَقِيرٞ ٢٤ ﴾

صدق الله العظيم

سورة القصص آية(24)

شكر و تقدير

الحمد الله حمدا يوافي ما تزايد من النعم والشكر له على ما أولاني من الفضل والكرم ....الذي وفقني لانجاز هده الرسالة .....

وعملا بقوله صلى الله عليه وسلم " من لم يشكر الناس لم يشكر الله "

وبعد أداء واجب الاحترام و التقدير

أتوجه بخالص شكري وامتناني وعرفاني لأستاذي الفاضل الموقر قمراوي عز الدين الذي تفضل بقبول الإشراف على هذه الرسالة منذ أن كانت فكرة إلى أن صارت بحثا، فتعلمت معه أبجديات البحث العلمي، وكان حريصا على الدقة والموضوعية بحسن التوجيه ودفعي للأمام...وكان صبورا علي علما وعملا رغم وقته الضيق و التزاماته الكثيرة ... أسأل الله أن يجزيه عني خير الجزاء

كما أتقدم بجزيل الشكر إلى كل الأساتذة أعضاء لجنة المناقشة

كل باسمه ومقامه... على جهودهم في قراءة الرسالة وتصويبها، وتحملهم عناء المناقشة، فجزاهم الله عني خير الجزاء...

كما أحمل الشكر والعرفان إلى كل من أمدني بالعلم، والمعرفة،وأسدى لي النصح والتوجيه، والى ذلك الصرح العلمي الشامخ متمثلا في جامعة وهران -2- محمد بن أحمد ،وأخص بالذكر كلية الحقوق والعلوم السياسية و القائمين عليها ...

كما أتوجه بالشكر إلى كل من ساندني بدعواته الصادقة، أو تمنياته المخلصة... أشكرهم جميعا وأتمنى من الله عز وجل أن يجعل ذلك في موازين حسناتهم .

إهـداء

أهدي ثمرة جهدي

إلى روح الحبيب المصطفى الهادي الأحب إلي من نفسي التي بين جنبي النبي الأمي القائد والمعلم الدال الراشد إلى الصراط المستقيم (محمد) صلى الله عليه وسلم

إلى قائدي وقدوتي والدي العزيز.....فالله يجزي أبي من

فضل نعمته خير الجزاء بما أولى وما قصدا

..... إلى والدتي .. نبع الحنان ... وبر الأمان

إلى من كانت لي سند في انجاز هذا البحث إليك زوجتي حفظك الله

إلى ثمرة حياتي فاطمة الزهراء، نهال، سارة حفظكم الله

إلى من أمدوني بالعون، شقيقي وشقيقاتي وكل العائلة الكبيرة

إليك لمن علمني حرفا، وأخذ بيدي في سبيل تحصيل العلم والمعرفة ..

عثماني رضوان

قائمة المختصرات

ج ر ج ج : الجريدة الرسمية للجمهورية الجزائرية

ق ع ج : قانون العقوبات الجزائري

ق إ ج ج : قانون الإجراءات الجزائية الجزائري

ج : الجزء

س : السنة

ع : العدد

ص : الصفحة

م : ميلادي

ط : الطبعة

مقدمـــــة

بمرور الزمن و بتعاقب الأجيال شهد العالم تطور كبير في شتى المجالات الاقتصادية والاجتماعية والسياسية والثقافية والعلمية وغيرها، وتزامنا مع هذا التطور عرف العالم نقلة نوعية مست ظاهرة صحية لصيقة بالمجتمع ألا وهي 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 الإنترنت في جميع أقطار المعمورة، يعرف جرائم جديدة لم يكن لها مثيل من قبل خاصة بعد توسع استخدام شبكة الإنترنت من جميع فئات المجتمع وفي شتى المجالات، وهذه الجرائم يطلق عليها مسمى الجرائم الإلكترونية أو المعلوماتية...

وبتزايد استخدام الدوائر الحكومية ومؤسسات الدولة بمختلف أقطارها لهذه التقنية للقيام بوظائفها وإبداء خدماتها سواء فيما بينها أو بينها وبين الجهات غير الحكومية كالمواطنين.

وبتزايد استخدام هذه التقنية من طرف القطاع العام والقطاع الخاص والمؤسسات الاقتصادية ، 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، والاتجار بالمخدرات، وجرائم الآداب العامة، وجرائم الإرهاب وغيرها....

وفي ظل هذا التطور السريع والرهيب وتحدي مقترفي مثل هذه الجرائم لأجهزة الأمن والقضاء وتشريعات الدول، التي أصبحت غير مواكبة لمثل هذا التطور، الأمر الذي دفع مشرعي دول العالم الإسراع إلى استصدار قوانين وتشريعات لمواكبة ومواجهة مثل هذه الجرائم، بالإضافة إلى إبرام اتفاقيات بين الدول لمجابهة هذه الظاهرة، وإيجاد حلول تقنية وتكوينية لأجهزة الأمن والقضاء وغير ذلك.

والجزائر مثلها مثل باقي دول العالم ليست بمنأى عن هذه الظاهرة رغم محدودية درجة انتشار التعامل بتقنية المعلوماتية إذا ما قرناها ببعض دول العالم، إلا أنه ورغم محدودية التعامل بهذه التقنية، شهدت الجزائر عدة جرائم كاختراق المواقع والأنظمة المعلوماتية، نشر الفيروسات، وغيرها من الجرائم التي مست مؤسسات واقتصاد الدولة، وكبدتها بعض الخسائر المادية، كما كذلك مست الحريات الخاصة للأفراد كالتشهير وتشويه السمعة، بالإضافة إلى عدة جرائم إلكترونية كجرائم الإرهاب وغيرها، وهذا ما دفع بالدولة الجزائرية إلى البحث عن وسائل وسبل لمكافحة الجرائم الإلكترونية من استصدار قوانين وتشريعات في هذا المجال، وإبرام اتفاقيات مع دول أخرى كمجال للتعاون وتبادل المعلومات،

بالإضافة إلى إجراء دورات تكوينية لأجهزة الأمن والقضاء محلية ودولية، بالإضافة إلى إيجاد حلول تقنية للتصدي لهذا النوع من الجرائم وغير ذلك من الحلول....

أهمية الموضوع:

ألقى التطور العلمي بظلاله على المعمورة وخاصة في مجال الاتصالات، حيث ألغى تلك الحدود الوهمية بين الدول، بحيث أصبح العالم كقرية صغيرة تواصليا ببزوغ هذه الثورة المعلوماتية، مخترقا وضاربا عرض الحائط كل الأعراف التقليدية في الجانب التواصلي بين الدول والشعوب.

إن التطور الذي عرفه المجتمع الدولي في مجال تكنولوجيا الاتصالات، وخاصة بظهور الإنترنت مس شتى مجالات الحياة، اقتصاديا، اجتماعيا، ثقافيا، علميا وغيرها، وكان له دور إيجابي وفعال، ولكن نظرا لانتقال المجتمعات إلى عصر المعلومات، وزيادة الترابط الإلكتروني، والذي سهل بدوره ارتكاب الجريمة المستحدثة.

إن دراستنا لهذا الموضوع له أهمية بمكان، وذلك بتسليط الضوء على هذا النوع من الجرائم ألا وهي الجريمة المعلوماتية، وذلك باعتبارها من الجرائم المستحدثة المتطورة غير راكدة التي تحتاج منا المواكبة، وهذه الدراسة سوف تسمح لنا بقدر الإمكان معرفة هذا النوع من الجرائم، وفي المقابل بيان سبل مواجهتها تشريعيا سواء داخليا أو دوليا حيث أن هذا الوضع أدى إلى قيام العديد من الدول بسن قوانين داخلية، وعقد اتفاقيات دولية لمجابهة هذا التطور المذهل والغير متكافئ في مجال المعلوماتية والاتصالات.

أهداف الدراسة:

إن الهدف من هذه الدراسة هو محاولة معرفة هذا النوع من الجرائم المستحدثة، ألا وهي الجريمة المعلوماتية من خلال التطرق للإطار المفاهيمي لهذا النوع من الجرائم، وكذا التطرق لسبل مواجهتها ومكافحتها من خلال أحدث التشريعات التي صخرتها الجزائر لمواكبتها هذا من جهة، ومن جهة أخرى محاولة معرفة القوانين الداخلية لبعض الدول محل الدراسة في هذا الموضوع، وكذا التعاون الدولي بإبراز بعض الاتفاقيات الثنائية والإقليمية والدولية في هذا المجال، وعليه فإن هذه الدراسة تهدف إلى:

- تحديد التعريفات الخاصة بالجريمة المعلوماتية وخاصة التعريف الفقهي والقانوني .

– تحديد الخصائص التي تقوم عليها الجريمة المعلوماتية وتبيان البنيان القانوني لهذه الظاهرة من أركانها وتقسيماتها.

– معرفة المجرم المعلوماتي والسمات التي يتصف بها وأهم دوافعه لارتكاب الجريمة المعلوماتية.

– تحديد واقع الجريمة المعلوماتية في الجزائر وأهم الإحصائيات المتعلقة بها .

– دراسة التشريع الجزائري وتبيان مدى تطوره في معالجة الجريمة المعلوماتية بالمقارنة مع بعض التشريعات الوطنية الأخرى، وكذا تبيان القوانين والاتفاقيات الدولية في مجال مكافحة هذه الظاهرة .

– تبيان إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية، وكذا تبيان الأرضية التي من المفترض أن تبنى عليها اتفاقية عالمية لمكافحة الجريمة السيبرانية برعاية الأمم المتحدة .

ولقد جاء اهتمامنا بهذا الموضوع نتيجة لمجموعة من الأسباب، العملية منها والعلمية.

أما الأسباب العملية فتتمثل في انتشار وتفشي هذه الظاهرة على المستوى الوطني والدولي، باعتبارها ظاهرة لا تعرف الحدود التقليدية، وما يترتب عليها من أضرار جد خطيرة تمس شتى مجالات الحياة " الاقتصادية، الاجتماعية،..."، الأمر الذي استوجب الحسم في مواجهة هذه الظاهرة بإصدار أحدث التشريعات داخليا و ارصاص الصفوف بالتعاون الدون مصلحي دوليا.

أما الأسباب العلمية فترجع إلى قلة الدراسات المتخصصة وطنيا، وكذا الأهمية المتزايدة على المستوى الدولي بهذه الظاهرة في ظل الصراع بين القوى الدولية الروسية الصينية من جهة و الأمريكية الأوروبية من جهة أخرى، كما تتضح الدراسة العلمية لهذا الموضوع على اكتشاف تشريعات الدول الأخرى في هذه الدراسة، وكذا الاتفاقيات الدولية لما لها من انعكاس إيجابي على التشريع الجزائري.

الإشكالية:

من هنا سنحاول البحث في هذه الرسالة من خلال الإشكالية التالية:

ما مدى كفاية القانون الجزائري والقوانين الوطنية محل الدراسة والقانون الدولي في الحد من ظاهرة الجريمة المعلوماتية؟

المنهج المتبع:

للإجابة على هذه الإشكالية المطروحة ارتأينا في دراستنا الاستناد على عدة مناهج، وهذا لما يتطلبه طبيعة هذا الموضوع منها:

1- المنهج المقارن الذي يعتبر من أهم المناهج في هذه الدراسة بالتطرق لعدة قوانين دول محل الدراسة مثل الجزائر ومصر وقطر وغيرها من الدول، وكذلك برجوعنا لعدة اتفاقيات سواء ثنائية أو إقليمية أو دولية لما لها من إيجابيات على القوانين الوطنية، وخاصة القانون الجزائري، والعكس صحيح.

2- المنهج الوصفي والتحليلي، وذلك من خلال وصف وتشخيص موضوع البحث في مختلف جوانبه وأبعاده .

3- المنهج الاستقرائي، وذلك من خلال استقراء النصوص القانونية سواء في التشريع الجزائري أو تشريعات الدول الأخرى، وكذا الاتفاقيات الثنائية والإقليمية والدولية.

خطة الدراسة:

من خلال ما سبق بيانه قمنا بتقسيم رسالتنا هذه إلى بابين، الباب الأول تم تخصيصه للإطار المفاهيمي للجريمة المعلوماتية وسبل مكافحتها في القانون الجزائري، والذي بدوره قسمناه إلى فصلين، الفصل الأول تطرقنا فيه للإطار المفاهيمي للجريمة المعلوماتية، أما الفصل الثاني خصصناه لمكافحة الجريمة المعلوماتية في القانون الجزائري.

وبدورنا الباب الثاني أعطيناه عنوان مكافحة جرائم المعلوماتية دوليا، وعالجناه في فصلين، الفصل الأول تطرقنا فيه للقوانين والاتفاقيات الدولية في مجال مكافحة الجريمة المعلوماتية، أما الفصل الثاني تطرقنا فيه للاتجاهات الدولية في مجال مكافحة الجريمة المعلوماتية، والذي عالجنا فيه موضوع التعاون الدولي في مجال مكافحة هذا النوع من الجرائم وكذا إشكالاته هذا من جهة، ومن جهة أخرى تناولنا مسار الاتفاقية العالمية لمكافحة الجريمة السيبرانية برعاية الأمم المتحدة بحدود2023.

البـــاب الأول

الجريمة المعلوماتية و مكافحتها في القانون الجزائري

الباب الأول

الجريمة المعلوماتية ومكافحتها في القانون الجزائري

الجريمة المعلوماتية واحدة من الظواهر الإجرامية المستحدثة، والمجرم يحاول دائما الاستفادة من أية وسيلة لارتكاب جرائمه، والتقدم التكنولوجي قدم له وسائل مستحدثة للوصول إلى غايته، والمشرع لا يقف مكتوف الأيدي عندما يجد تهديدا للمصالح الأساسية التي يقوم عليها المجتمع، والحقيقة أن التقدم التكنولوجي خاصة في مجال الاتصالات تسبب إلى جانب خلق وسائل جديدة في ارتكاب الجريمة التقليدية إلى خلق جرائم مستحدثة تتعلق بهذا الكيان التكنولوجي الجديد.[1]

وعليه سوف نحاول التطرق تحت هذا الباب للإطار المفاهيمي للجريمة المعلوماتية وذلك بتبيان التعاريف المتعلقة بهذه الظاهرة وكذا أهم الخصائص التي تمتاز بها مع تبيان الأركان التي تقوم عليها هذه الجريمة وكذا تقسيماتها، وكذا التطرق لنظم الحاسب الآلي والمجرم المعلوماتي كل هذا تحت الفصل الأول، أما الفصل الثاني فخصص لمكافحة هذه الجريمة في القانون الجزائري وذلك بموجب القوانين العامة من جهة وكذا بموجب قوانين وهيئات خاصة من جهة أخرى دون أن ننسى تبيان واقع هذه الجريمة في الجزائر بإبراز تطورها وأهم الإحصائيات التي شهدتها في الآونة الأخيرة.

[1] - ياسر سيد فهمي، المواجهة الموضوعية للجرائم الالكترونية، دار النهضة العربية، القاهرة ، جمهورية مصر العربية 2023، ص7.

الفصل الأول

الإطار المفاهيمي للجريمة المعلوماتية

الفصل الأول

الإطار المفاهيمي للجريمة المعلوماتية

مر العالم بعدة ثورات، كان لها تأثير كبير على جميع مجالات الحياة الاقتصادية والسياسية والاجتماعية والعلمية والتربوية، فكانت الثورة الصناعية في القرن الثامن عشر و القرن التاسع عشر، ثم جاءت الثورة الإلكترونية في الثمانينيات من القرن العشرين، التي أدت إلى تطور صناعة الحاسبات الآلية و البرمجيات والأقمار الصناعية، وظهر ما يسمى بتكنولوجيا المعلومات، والتي تعني الحصول على المعلومات بصورها المختلفة، ومعالجاتها وتخزينها واستعادتها، وتوظيفها عند اتخاذ القرارات، و توزيعها بواسطة أجهزة تعمل إلكترونيا، وتوجد عدة أشكال لتكنولوجيا المعلومات، منها الاتصال بالأقمار الصناعية، وشبكات الهاتف الرقمية، وأجهزة الحاسوب متعددة الوسائط، و مؤتمرات الفيديو التفاعلية والأقراص المدمجة، وشبكة الحاسوب المحلية والعالمية، ويعد ذلك تحولا من العصر الصناعي إلى العصر المعلوماتي، أو عصر المعرفة، ثم كانت الثورة اللاسلكية في نهاية القرن العشرين وبداية القرن الحادي والعشرين، حيث كان الهاتف الجوال المتحرك والأجهزة اللاسلكية التي انتشرت بسرعة فائقة وبإعداد كبيرة في العالم أجمع ،أكبر مؤشر على أهمية الثورة اللاسلكية ودورها في الحياة.[1]

[1]–محمود محمد محمود جاب، الجرائم الناشئة عن استخدام الهواتف النقالة، المكتب الجامعي الحديث، الإسكندرية، جمهورية مصر العربية، الكتاب الأول، 2018، ص 7 .

المبحث الأول

ماهية الجريمة المعلوماتية

مما لا شك فيه أن الجريمة عموما تطورت بتطور نمط الإنسان، وقد بلغ هذا التطور قمته مع ظهور وسائل وتقنيات الاتصالات الحديثة والشبكات الإنترنت، التي شملت مختلف نشاطات الإنسان حتى في ارتكاب الجريمة، لاسيما مع تزايد مستخدمي هذه الشبكة بشكل مذهل، و لما راج الإنترنت كوسيلة اتصال وتم استعماله في شتى مناحي المعاملات اليومية للناس، ظهرت سلبيات استعماله بعد استغلاله من المجرمين، مما أدي إلى ظهور جرائم لم تكن موجودة من قبل، وأضحت شبكة الإنترنت وما يتصل بها من أجهزة الكمبيوتر، وأجهزة الاتصالات الحديثة مسرحا لارتكاب الجرائم، التي تمثل عدوانا على حرمة الحياة الخاصة وإزعاجا لمن تقع عليهم تلك الجرائم، أو سبا أو قذفا في حقهم، أو الإبلاغ كذبا عن أمور منسوبة لهم، أو بالأحرى وسيلة سهلة لارتكاب هذه الجرائم.

الأمر الذي يتعين معه بيان ماهية الجريمة المرتكبة عبر الإنترنت عن طريق الاتصال بشبكة المعلومات الدولية، سواء أكان الاتصال بواسطة حاسب آلي أو كمبيوتر لوحي، أو كمبيوتر محمول، أو من خلال أي من أجهزة الاتصالات الحديثة كالتليفونات الذكية أو سواء كانت هذه الأجهزة متصلة بهذه الشبكة بواسطة هاتف سلكي أو لا سلكي، أم عن طريق شريحة خط تليفوني عبر شبكات الهواتف النقالة.[1]

[1]– بهاء المرى، شرح قانون مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات، العربية للنشر والتوزيع، أفنان للطباعة، جمهورية مصر العربية 2019، ص13.

المطلب الأول

تعريف الجريمة المعلوماتية وخصائصها

تعددت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع ذلك إلى الخلاف الذي أثير بشأن تعريف هذه الجريمة، ومن قبلها تعريف المعلومة ذاتها، فالجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها، لأن الجريمة المعلوماتية هي من الظواهر الحديثة، وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات، وقد أحاط بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها، ولكن الفقه لم يجتمع على وضع تعريف محدد لها بل أن البعض ذهب إلى ترجيح عدم وضع هذا التعريف بحجة أن هذا النوع من الإجرام ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني.[1]

بداية سنتطرق إلى إشكالية المصطلح، ثم نتطرق للمحاولات الفقهية والقانونية لتعريف هذه الجريمة

الفرع الأول

تعريف الجريمة المعلوماتية

أولا- في التشريع

عرفت المادة الأولى من القانون الكويتي رقم 63 سنة 2015 في شأن مكافحة لجرائم تقنية المعلومات، الجريمة المعلوماتية، بأنها " كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية، أو غير ذلك من وسائل تقنية المعلوماتية بالمخالفة لأحكام هذا القانون".

[1] – عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، جمهورية مصر العربية، الطبعة الأولى، 2012، ص40 .

وعرفت المادة الأولى من القانون القطري رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الالكترونية، بأنه "أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو شبكة معلوماتية بطريقة غير مشروعة، بما يخالف أحكام القانون".

وعرفت المادة الأولى من المرسوم السلطاني العماني رقم 69 لسنة 2008، بإصدار قانون معلومات الإلكترونية، برنامج الحاسب الآلي بأنه مجموعة معلومات إلكترونية أو تعليمات تستعمل بطريقة مباشرة أو غير مباشرة في النظام لمعالجة المعلومات الإلكترونية بغرض الوصول إلى نتائج محددة .[1]

وعرفت منظمة التعاون الاقتصادي والتنمية(OECD) الجريمة المعلوماتية بأنها " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".[2]

ثانيا-إشكالية المصطلح

نلاحظ عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، وتكشف النماذج المعروفة لتعريفات هذه الجريمة، على تعدد المصطلحات المستخدمة للدلالة عليها وتحديد مفهومها، هناك ما يطلق عليها اسم جرائم الحاسبات أو إساءة استخدام الحاسب، أو الجرائم المرتبطة أو المتعلقة بالحاسبات، أو جرائم المعالجة الآلية للبيانات أو جرائم التكنولوجيا الحديثة، أو جرائم المعلوماتية.[3]

ومن الجدير بالذكر أن أغلب التعبيرات تداولا في هذا المجال هي " الجريمة الالكترونية " و "الجريمة المعلوماتية "، واستخدام التعبير الأخير يعتبر الأكثر اتساقا مع اللغة العربية التي لا تعد مفردة "الالكترونية " من مفرداتها، بل هي كلمة أجنبية معربة، فضلا عن كون مصطلح "المعلوماتية"

[1]-محمد علي سويلم، مكافحة الجرائم الالكترونية، دراسة مقارنة بالتشريعات العربية والأجنبية، دار المطبوعات الجامعية، الإسكندرية، مصر، الطبعة الأولى 2019، ص 17، 18.

[2] – محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الالكترونية –دراسة مقارنة– دار الفكر والقانون للنشر والتوزيع، المنصورة، مصر، 2015، ص15.

[3] – محمد علي سويلم، المرجع نفسه، ص 18.

هو الأكثر تداولا في الأدبيات القانونية المعاصرة، كما أن العديد من التشريعات العربية استعملت هذا المصطلح، منها نظام مكافحة الجرائم المعلوماتية السعودي، قانون جرائم المعلوماتية السوداني وغيرها.[1]

اصطلاح الجريمة المعلوماتية عام، ويشمل التقنيات الحالية والمستقبلية كلها المستخدمة في التعامل مع المعلومات بما في ذلك الحاسوب وشبكة الانترنت.[2]

ثالثا- التعريفات الفقهية والقانونية للجريمة المعلوماتية

تعريفات الجريمة المعلوماتية تختلف فيما بينها ضيقا وأتساعا، ويمكن تصنيفها في أربع فئات هي:

- تعريفات مرتبطة بالحاسب (معيار وسيلة ارتكاب الجريمة).
- التعريفات مرتبطة بموضوع الجريمة (معيار موضوع الجريمة).
- التعريفات مرتبطة بمعيار مدى توفر للمهارة بالتقنية المعلوماتية.
- المعيار المزدوج (المختلط).

1- معيار وسيلة ارتكاب الجريمة

يعتمد هذا المعيار على وسيلة ارتكاب الجريمة، فقد نصت الفقرة رقم ثمانية من المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي عام 2007، على أن الجريمة المعلوماتية هي أي فعل يرتكب متضمنا استخدام الحاسب الآلي، أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام، وكذلك المادة الأولى من القانون القطري رقم(14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، و المادة الأولى من القانون الكويتي رقم 63 لسنة2015في شأن مكافحة جرائم تقنية المعلومات.

[1] – عمار عباس الحسني، جرائم الحاسوب والانترنت، الجرائم المعلوماتية، منشورات زين الحقوقية، بيروت، لبنان، الطبعة الأولى ،2017، ص36 .

[2] – نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى 2008، ص47 .

وفي الفقه: عرفها الفقيه الألماني تيدمان Tiedemann بأنها كل أشكال السلوك غير مشروع "أو الضار بالمجتمع" الذي يرتكب باستخدام الحاسب ،[1] وعرفها الفقيه Merew بأنها الفعل غير المشروع الذي يتورط في إرتكابه الحاسب الآلي.[2]

وعرفها **الفقيه الإنجليزي "ليزي بول"** بأنها كل فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية[3]، وعرفها الفقيه" **ميتو**" بأنها الفعل غير المشروع الذي يستخدم فيه الحاسب الآلي كأداة رئيسة، أو هي تلك التي الجرائم يكون فيها دور الحاسب الآلي إيجابيا أكثر من سلبي، أو هي كل نشاط إجرامي يؤدي فيه النظام دورا لإتمامه، أو يقع على النظام نفسه، أو أنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود .[4]

وعرفها البعض الآخر بأنها هي نشاط إجرامي تستخدم فيه التقنية الالكترونية (الحاسوب الآلي الرقمي وشبكة الإنترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف .[5]

في حين عرفها مكتب تقييم التقنية في الولايات المتحدة الأميركية من خلال تعريف جريمة الحاسب بأنها " الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا".[6]

أما مشروع القانون العربي النموذجي في شأن مكافحة جرائم الكمبيوتر والانترنت، الذي صيغ في جامعة الدول العربية بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب في 2003/5/22،

---

[1] - Klaus Tiedman , Fraude et autres délits d'affaire commis a l'aide de l'ordinateur électronique, revue D.P.C 1984.No7.P.612.

[2] - Merwe Vander, Computer crimes and other crimes against information technology in south africa R.I.D.P,1993,P554.

[3] - Toty and Hardcastle , Computer related crime in information technology andthelawU.K.1986,P26.

[4] – محمد علي سويلم، المرجع السابق، ص20.

[5] – محمد ممدوح بذير، مكافحة الجريمة المعلوماتية عبر شبكات الإنترنت، مركز الدراسات العربية للنشر والتوزيع، الطبعة الأولى 2019، ص20 .

[6] – محمد علي سويلم ، المرجع نفسه، ص 18، 19.

والذي تم إقراره قد عرف الجريمة الالكترونية في المادة الأولى منه بأنها " كل فعل مؤثم يتم ارتكابه عبر أي وسيط اليكتروني " .[1]

ولم يسلم هذا المعيار من النقد، باعتبار أن تعريف الجريمة يقوم على العمل الأساسي فيها، وليس على مجرد الأداة المستعملة في ارتكابها، كما أن الوسيلة ليست معتبرة لدى الشارع الجنائي عند التجريم لكون كافة الوسائل متساوية، والبنيان القانوني للجريمة بتوافر أركانها هو محل الاعتبار عند تطبيق نصوص التجريم، فضلا عن أن الأخذ بهذا المعيار يؤدي إلى التوسع في نطاق الجرائم المعلوماتية.[2]

2- معيار موضوع الجريمة

يرى أنصار هذا الاتجاه وجوب أن يكون الحاسب أو أنظمته هي محل " موضوع " هذه الجريمة ومنهم الفقيه روزنبلات Rosenblatt والذي عرف هذه الجريمة بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه .[3]

وفي هذا المعنى أيضا عرفها البعض على أنها " السلوك السيئ المتعمد الذي يستخدم نظم المعلومات لإتلاف المعلومات، أو إساءة استخدامها، مما يتسبب أو يحاول التسبب إما بإلحاق الضرر بالضحية، أو حصول الجاني على فوائد لا يستحقها أو هي كل سلوك غير شرعي أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات .

وعرفها خبراء منظمة التعاون والتنمية الاقتصادية خلال مؤتمر عقد في باريس عام 1983 حول الجرائم المرتبطة بالمعلوماتية "على أنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح فيه يتعلق بالمعالجة الآلية للبيانات أو نقلها".

ويؤخذ على هذا المعيار أنه يضيق من نطاق الجرائم المعلوماتية، و يقصرها على الجرائم الواقعة على الحاسب الآلي دون الجرائم المرتكبة بواسطته أو عن طريقه.[1]

---

[1] – بهاء المرى، المرجع السابق، ص16.

[2]– محمد علي سويلم، المرجع السابق، ص20 .

[3] – عمار عباس الحسني، المرجع السابق، ص 39 .

3- المعيار المستند إلى المعرفة التقنية لدى مرتكب الجريمة

يوجد تعريف لوزارة العدل الأمريكية، معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979، حيث عرفتها بأنها " أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها "، وعرفها الفقيه الفرنسي "**فيفانت**" بأنها " مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب " .[2]

يعرف مكتب تقييم التقنية في الولايات المتحدة الأميركية من خلال تعريف جرائم الحاسوب، بأنها " الجرائم التي تلعب فيها البيانات الكمبيوترية، والبرامج المعلوماتية دورا رئيسيا" وكذلك تعريف " David thompson" بأنها " آية جريمة يكون متطلبا اقترافها أن تتوفر لدى فاعلها معرفة تقنية للحاسب".

وقد عرفتها منظمة التعاون الاقتصادي للتنمية OCDE بأنها " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".

وعرفها الفقيه ستين سكيولبريك " steinschiollerg" بأنها "جريمة يكون متطلبا أن تتوافر لدى فاعلها بمعرفة بتقنية الحاسوب".

ومع ذلك فقد انتقد البعض هذا الاتجاه الأخير في تعريف الجريمة المعلوماتية بالقول " إن هذا الاتجاه يضيق على نحو كبير من الجريمة المعلوماتية ...وإن الجريمة المعلوماتية من وجهة نظر هزا الاتجاه سوف تصبح أشبه بالخرافة، فهذا الاتجاه يحصر الجريمة المعلوماتية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها، وهو إن تحقق في بعض الأحوال، فإنه لا يتحقق في كثير منها، ففي كثير من الحالات يرتكب الجناة الفعل الإجرامي دون الحاجة إلى هذا القدر من المعرفة والخبرة .."[3].

---

[1]- محمد علي سويلم، المرجع السابق، ص 21 .

[2]- محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية، المكتبة العصرية للنشر والتوزيع، المنصورة، مصر، 2010، ص30 .

[3] - عمار عباس الحسني، المرجع السابق، ص39.

4- المعيار المختلط

يعتمد هذا المعيار على الدمج بين معيار أداة الجريمة ومعيار موضوع الجريمة، والمعياران يمثلان ذات الشيء وهو الحاسب الآلي أو الكمبيوتر، ومن ذلك التعريف الذي اعتمده خبراء من بلجيكا، في معرض ردهم على الاستبيان الذي أجرته منظمة التعاون والتنمية الاقتصادية حول الغش المعلوماتي، بأن كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة، أو غير مباشرة عن تدخل التقنية المعلوماتية.

وعرفها البعض بأنه جريمة استخدم الحاسب كوسيلة أو أداة لارتكابها، أو يمثل إغراء بذلك أو جريمة يكون الحاسب ذاته ضحيتها.

وقد تبنت هذا المعيار منظمة الأمم المتحدة في مؤتمرها العاشر لمنع الجريمة ومعاقبة المجرمين، الذي عقد في فينا في الفترة من 07 إلى10افريل2000، وعرفت الجريمة الإلكترونية بأنها " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".

ويرجح التعريف المختلط، فتشمل الجريمة الإلكترونية كل نشاط إجرامي يمكن ارتكابه في بيئة إلكترونية،[1] وعليه فالاتجاه المختلط فجمع بين عدة معايير في تعريفه.

رابعا- تعريف الجريمة المعلوماتية في التشريع الجزائري

عرف المشرع الجزائري الجريمة المعلوماتية في المادة الثانية من القانون 09-04 والتي سماها " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال " بأنها " جرائم المساس بأنظمة المعالجة الآلية

[1]- محمد علي سويلم، المرجع السابق، ص 23 .

للمعطيات المحددة في قانون العقوبات، وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية ".[1]

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

1- 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 .

2- التعريف على أساس معيار وسيلة ارتكاب الجريمة :

بالإضافة إلى الاستناد في تحديد الجريمة المعلوماتية على موضوع الجريمة، أضاف المشرع الجزائري معيار آخر لتحديد الجريمة المعلوماتية، وهو وسيلة ارتكاب الجريمة وهي المنظومة المعلوماتية، أو نظام الاتصالات الالكترونية بالقول " ...وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية، فوسيلة ارتكاب الجريمة أو تسهيل ارتكابها في هذا التعريف هي محل اعتبار في تكييف الجريمة ، وهذا ما نص عليه الأمر رقم 21-11 المؤرخ في 25 غشت 2021 المتمم للأمر رقم 66-155 والمتضمن قانون الإجراءات الجزائية، وذلك في المادة 211 مكرر 22 فقرة3 .[2]

وهنا يمكن القول أن الجريمة المعلوماتية حسب المشرع الجزائري تنقسم إلى طائفتين، تضم الطائفة الأولى، الجرائم التي ترتكب ضد نظام المعالجة الآلية للمعطيات، وتستهدف المساس الكلي أو الجزئي

---

[1]- المادة الثانية من القانون 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ح.ر.ج.ح، العدد 47.

[2]- أمر رقم 21-11المؤرخ في 25غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 18صفر 1386الموافق8 يونيو 1966، والمتضمن قانون الإجراءات الجزائية، ج ر ج ج، العدد65.

بهذه المنظومة، وهي الجرائم المنصوص عليها في الفصل السابع مكرر من قانون العقوبات تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات "، فيما تتضمن الطائفة الثانية كل الجرائم الأخرى المنصوص عليها في قانون العقوبات، أو في القوانين الخاصة التي يتم ارتكابها، أو يتم تسهيل ارتكابها باستخدام منظومة معلوماتية، أو أي نظام للاتصالات .[1]

الفرع الثاني

خصائص الجريمة المعلوماتية

للجريمة المعلوماتية خصائص عدة أهمها :

أولا- الجريمة المعلوماتية جريمة عابرة للحدود

الجريمة المعلوماتية جريمة عابرة الحدود، لا تحدها حدود الدول فهي متمردة على عنصر المكان والنطاق الجغرافي، حيث تدخل في طائفة الجرائم عبر الوطنية، ويرجع ذلك إلى البيئة الإلكترونية التي تقع فيها تلك الجرائم، والتي تقوم على الرابط الإلكتروني بين الحواسيب سواء داخل الدولة الواحدة، أو بين عدة دول بواسطة شبكات إلكترونية مثل الإنترنت، والتي صممت في الأصل لتسهيل عملية النقل المعلومات والاتصالات، فأضحت تستخدم كوسيلة لارتكاب الجرائم، فقد ترتكب جريمة بواسطة الحاسب الآلي عن طريق الشبكات الدولية (الإنترنت)، وتتحقق نتائجها الإجرامية في دولة أخرى من العالم مرورا بمزود خدمة أو قنوات اتصال في إقليم دولة ثالثة، و يترتب على البعد عبر الوطني للجريمة المعلوماتية عدة إشكاليات مشابهة لتلك المرتبطة بالجرائم ذات الطابع عبر الوطنية أهمها، اصطدام إجراءات التحقيق وضبط المتهمين وملاحقتهم بمبدأ السيادة الوطنية للدولة، وخاصة في الجرائم التي تتطلب اتخاذ إجراء من إجراءات التحقيق في إقليم دولة أجنبية، وكذلك

[1] – عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان، الجزائر 2021، ص18،20،19.

إشكالية الاختصاص القضائي وإشكالية تحديد القانون واجب التطبيق، كما أنه من جهة أخرى تشكل الإجراءات الرسمية المعقدة والتي تستغرق وقتا ليس بالقصير في حالات المساعدة القانونية أو القضائية بين الدول، والتي تتعارض مع طبيعة الجرائم المعلوماتية التي تتطلب سرعة في التحقيقات، حيث أن جزء كبير من الأدلة في الجرائم المعلوماتية غير ملموس ويزول بسرعة، وهو ما يتطلب أن تكون إجراءات التحقيق، وجمع الأدلة بصورة. سريعة وآنية.[1]

ثانيا– صعوبة اكتشاف الجرائم المعلوماتية وإثباتها

تتصف الجريمة المعلوماتية بأنها صعبة الإثبات، ولكن ليست مستحيلة الإثبات، و أساس ذلك أن الجاني والمجني عليه في كثير من الأحيان مجهولين خاصة في تلك النوعية من الجرائم التي تتعلق بوسائل الاتصال، وليس بالحاسب الآلي بصورة مجردة من اتصاله بتلك الشبكات، إذ أن الجاني يستخدم الوسائل الفنية والتقنية في الكثير من الأحيان، كما أن الفعل المكون للركن المادي للجريمة والذي يمثل السلوك الإجرامي لا يستغرق وقتا طويلا بل في مجرد ثوان (cyber crime)، ويتم في الخفاء، ومؤدى ذلك أن الجرائم المعلوماتية في أكثر صورها خفية.

وهناك صعوبات أخرى أيضا تكمن في صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، إذ يستطيع المجرم المعلوماتي في أقل من ثانية أن يمحو أو يحرف، أو يغير البيانات و المعلومات الموجودة في الكمبيوتر، لذا فإن للمصادفة و سواء الحظ دورا في اكتشافها، يفوق دور أساليب التدقيق والرقابة، ومعظم مرتكبيها الذين تم ضبطهم وفقا لما لاحظه أحد الخبراء في الجريمة المعلوماتية ، إما أنهم تصرفوا بغباء، أو لم يستخدموا الأنظمة المعلوماتية بمهارة.[2]

هذا النوع من الجرائم يتم في بيئة افتراضية، ناهيك على أن الجاني يمكنه ارتكاب الجريمة في دولة أو قارة أخرى، كما توفر التقنية المعلوماتية للمجرم إخفاء آثار الجريمة عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية وبالتالي محو آثاره، مما يخلق صعوبات بالغة لسلطات البحث والتحري في ملاحقته وضمان عدم إفلاته من العقاب، خاصة أن تنفيذها لا يتطلب وجود

[1]– محمد كمال محمد الدسوقي، الحماية الجنائية لسرعة المعلومات الالكترونية، دراسة مقارنة، دار الفكر والقانون للنشر والتوزيع، المنصورة، جمهورية مصر العربية 2015، ص 20، 21.

[2] – محمد علي سويلم، المرجع السابق، ص30.

الفاعل في مكان الجريمة، بل يمكنه تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل سواء كان من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة...[1]

ويوجد صعوبة في إثبات الجريمة المعلوماتية، تكمن في الجناة مرتكبي تلك الجرائم الذين يتسمون بالذكاء والدهاء والخبرة التقنية أثناء ارتكابها، إضافة إلى عدم ملائمة الأدلة والتقنية في القانون الجنائي.

فصعوبة إثبات هذه الجريمة يرجع إلى عدة أسباب، من بينها وسيلة تنفيذها، والتي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد، بالإضافة إلى الإحجام عن الإبلاغ عنها في حال اكتشافها لخشية المجني من فقد ثقة عملائها، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة، ولذلك يقترح ضرورة عقد دورات تدريبية مشتركة بين رجال القضاء والنيابة العامة ورجال الشرطة، والخبراء الفنيين مجتمعين معا، وذلك بغرض معرفة كل جهة بطبيعة عمل كل جهة أخرى، مما يحقق التعاون بين هذه الجهات وصولا إلى أنسب الطرق القانونية لمكافحة الجرائم المعلوماتية، لذلك أن الإجرام المعلوماتي هو إجرام الأذكياء مقارنة بالإجرام التقليدي الذي يميل إلى العنف، كما أن المجرم المعلوماتي ذو مهارات تقنية عالية وإلمام بتكنولوجيا النظام المعلوماتية.[2]

ثالثا- سهلة الارتكاب (أسلوب ارتكاب الجريمة المعلوماتية)

ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي، الذي قد يكون في صورة ممارسة العنف والإيذاء، كما هو في حال جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر، و تقليد المفاتيح كما هو الحال في جريمة السرقة، فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها لا تحتاج إلى العنف، بل

[1]- يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة الإسكندرية، مصر 2019، ص82.

[2]- محمد علي سويلم، المرجع السابق، ص30إلى 32.

كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقديم يوظف في ارتكاب الأفعال غير المشروعة.

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت) مع وجود مجرم يوظف خبرته أو قدراته على التعامل مع الشبكة للقيام بجرائم مختلفة، كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين، كل ذلك دون حاجة لسفك الدماء.[1]

رابعا- صعوبة إثبات الجريمة المعلوماتية

يترتب على الخصائص المتقدمة المتعلقة بدولية هذه الجريمة، وصعوبة اكتشافها وهدوئها، إن هذه الجريمة يصعب إثباتها، وهذه الصعوبة راجعة إلى عدد من الأسباب، منها أنها جريمة لا تترك أثرا ماديا ملموسا، فضلا عن وقوعها في الغالب من قبل مجرمين محترفين، ولعل ما يزيد في صعوبة إثبات هذه الجرائم نقص الخبرة الفنية والتقنية لدى الشرطة، وجهات الادعاء العام والقضاء، إذ أن هذا النوع من الجرائم يتطلب تدريبا وتأهيلا لأفراد هذه الجهات في مجال التقنية الحديثة، من حيث كيفية جمع الأدلة وإجراء التفتيش والملاحقة في بيئة النظام المعلوماتي، مما يجعل من الجهود المبذولة في هذا المجال غير مناسبة وحجم وخطورة هذه الجرائم.

و الجاني في هذه الجرائم في الغالب يقوم بإخفاء أو تدمير دليل إدانته في ثانية واحدة، مما يضيع معه دليل أو أدلة الجريمة، إضافة إلى أن هذا الجاني لا يقوم بمهاجمة ماديات جهاز الحاسب كما الجريمة التقليدية حتى يمكن القبض عليه، بل أنه يرتكب جريمته من خلال هذا الجهاز متخفيا، وربما يكون في دولة أخرى أو قارة أخرى.[2]

خامسا- الجريمة المعلوماتية تتم عادة بتواطؤ أكثر من شخص

تتميز الجريمة المعلوماتية أنها تتم عادة بتعاون أكثر من شخص على ارتكابها إضرار بالجهة المجني عليها، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات

[1]- نهلا عبد القادر المومني، المرجع السابق، ص57،58.

[2]- عمار عباس الحسني، المرجع السابق، ص54.

الحاسوب والإنترنت، يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب، وتحويل مكاسب إليه.

والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود، قد يكون اشتراكا سلبيا، وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكا إيجابيا، وهو غالبا كذلك يتمثل في مساعدة فنية أو مادية.[1]

المطلب الثاني

أركان وتقسيمات الجريمة المعلوماتية

لكل جريمة ترتكب على الساحة الداخلية أو الدولية أركان لوجودها وتوافر عناصر لقيامها، إن المشرع يتطلب دائما وجود أركان لتحمل مسئولية الجريمة ووقوعها، فبتمثل دائما الركن المادي والمعنوي لضرورة المسائلة عن وقوع الجريمة فبدونها لا يمكن المسائلة عن جريمة ما، ويتمثل الركن المادي لأي جريمة هو النشاط أو السلوك الذي جعل الجريمة تنشأ، والركن المعنوي متمثل في القصد الجنائي لإحداث الجريمة ونتيجتها وذلك حتى تتحقق وقوع الجريمة، ولكن أحيانا لم يتطلب المشرع علاقة السببية بين الركن المادي والمعنوي وإنما قد يكتفي بالسلوك فقط أي الركن المادي.[2]

كما أن للجريمة المعلوماتية صور متعددة لا يمكن حصرها، ولكن مع ذلك فقد حاول بعض الفقهاء والبعض من المؤسسات الدولية تحديد هذه الصور خلال تصنيف هذه الجرائم.

[1]– نهلا عبد القادر المومني، المرجع السابق، ص 58.

[2]– هناء مصطفى الخبيري، الجرائم المعلوماتية وتقنين العملات الرقمية، دار النهضة العربية، القاهرة، جمهورية مصر العربية 2023، ص63.

الفرع الأول

أركان الجريمة المعلوماتية

تقوم الجريمة على ركنين رئيسيين هم الركن المادي والركن المعنوي، فلا بد للجريمة المعلوماتية هي إذن من ركن مادي يمثل كيانها الملموس ويعبر عن إرادة الفاعل بصورة يمكن إثباتها، ولا بد أيضا من ركن معنوي يعبر عن إرادة المجرم المعلوماتي.[1]

أولا- الركن المادي:

ينطلق مبدأ تحديد الفعل غير المشروع وإعطائه صفة الجريمة، بتحديد الركن المادي فيه، فلا جريمة دون ركن مادي، الذي يمثل في السلوك الذي يقوم به الجاني من أجل تحقيق غاية ما ويحدد له القانون العقاب اللازم، وهو يتباين بتباين الجرائم المرتكبة من قبل الجاني، شريطة أن يكون له مظهر خارجي ملموس، غير أن تحديد الركن المادي في الجرائم الواقعة عبر الشبكة العالمية للإنترنت تكتنفه العديد من الصعوبات خاصة فيما يتعلق بتحديد النتيجة الإجرامية والرابطة السببية.

1- القواعد العامة في الركن المادي للجريمة

أ- **السلوك الإجرامي:** يعد السلوك الإجرامي أهم عناصر الركن المادي لأي جريمة، لأنه يكشف عن سلوك مخالف لإرادة المشرع، ويبدو بمظاهر مادية ملموسة في العالم الخارجي، ويعني ذلك أن الأفكار داخل النفس لا عقاب عليها، يعرف السلوك الإجرامي في الجرائم التقليدية على أنه فعل الجاني الذي يحدث أثر في العالم الخارجي، وبغير هذا السلوك لا يمكن محاسبة الشخص مهما بلغت خطورة أفكاره وهواجسه الداخلية، والسلوك هو الذي يخرج النية والتفكير في الإجرام إلى حيز الوجود، واعتبار القانون ولا يكاد يفرق بين السلوك الإيجابي (الفعل)والسلوك السلبي (الامتناع عن الفعل) مادام أن لهما نفس النتيجة.

[1]- بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، سبتمبر2018، ص 353.

- **السلوك الإيجابي:** يكون في صورة فعل أو قول يجرمه القانون يصدر عن الجاني ويؤدي إحداث نتيجة في الجرائم ذات النتيجة، وكذلك يعتبر سلوكا إجراميا في ذاته في الجرائم الشكلية، ولا يهتم القانون بالوسيلة سواء كانت مادية أو معنوية فإذا كان السلوك محظور قانونا فهو يشكل جريمة، وكذلك إذا أدى إلى نتيجة منعها القانون، ويدخل ضمن السلوك الايجابي فعل السرقة والقتل والضرب والنصب وشهادة الزور والبلاغ الكاذب، والتحريض على الجريمة والغش والتدليس وغيرها من السلوكيات.[1]

- **السلوك السلبي:** يتمثل هذا الفعل بسلوك أو موقف يتخذه المكلف بقاعدة قانونية تفرض عليه أن يعمل فلا يعمل، ففي هذه الحالة، يقوم المكلف بالحيلولة دون جسمه كله أو بعضه وبين الحركة التي يتطلبها القانون، أو قد يتحرك باتجاه مضاد لما أمره به.

يقوم الفعل السلبي على الامتناع أو إحجام شخص عن القيام بعمل يوجبه عليه القانون إذا كان باستطاعته القيام به، وعليه فلا يجوز للقاضي أن يمتنع عن الحكم بالدعوى، ولا للشاهد أن يمتنع عن الإدلاء بشهادته أمام المحكمة بواقعه يعلمها ولا للموظف أن يمتنع عن أداء مهام وظيفته.

ب- النتيجة الإجرامية: يقصد بالنتيجة الإجرامية الأثر المادي الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي، فالسلوك قد أحدث تغييرا حسيا ملموسا في الواقع الخارجي، ومفهوم النتيجة كعنصر في الركن المادي للجريمة يقوم على أساس ما يعتد به المشرع ويرتب عليه نتائج بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى.

ج- الرابطة السببية: هي الصلة التي تربط بين الفعل والنتيجة، وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة، و أهمية رابطة السببية ترجع إلى أن إسناد النتيجة إلى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتحقق رابطة السببية تلازما ماديا بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حد الشروع، إذ لا يعد مسئولا عن النتيجة التي تحققت، أما إذا كانت

[1]- محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الإنترنت، والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت، دراسة مقارنة، مركز الدراسات العربية للنشر والتوزيع، الجيزة، جمهورية مصر العربية، الطبعة الأولى 2019، ص 95.

الجريمة غير عمدية فإن نفي رابطة السببية يؤدي إلى انتفاء المسؤولية كلية عنها، ذلك أنه لا شروع في الجرائم غير العمدية.[1]

2- الركن المادي للجريمة المعلوماتية.

حسب النصوص القانونية المنظمة للجريمة المعلوماتية في قانون العقوبات الجزائري وبعض القوانين المقارنة، المشرع الجزائري لم يشترط ضرورة أن تترتب نتيجة معينة بل اكتفى بتوفر السلوك المادي لقيام الجريمة المعلوماتية بغض النظر عن الضرر الذي تسبب فيه هذا السلوك للضحية، والدليل على ذلك أن القانون يعاقب على مجرد الدخول للمنظومة المعلوماتية دون أن يشترط حصول ضرر عن هذا الدخول، بل جعل تحقق النتيجة في الدخول والبقاء عن طريق الغش في المنظومة المعلوماتية كظرف مشدد وليس شرط للعقوبة.

زيادة على ذلك، فإن القانون يعاقب على مجرد الشروع في هذه الأفعال بنفس العقوبة المقررة للجريمة التامة، ولا يعدو أن يكون الضرر مجرد ظرف مشدد للعقوبة، أو أن يكون محلا لدعوى مدنية للمطالبة بالتعويض، وهذا يعني أن الجريمة المعلوماتية هي من الجرائم الشكلية التي لا يتعدى الركن المادي فيها توفر السلوك المادي دون أن يتعداه إلى النتيجة والعلاقة السببية، ويتخذ السلوك في هذه الجريمة صورة السلوك الإيجابي المتمثل في الدخول أو البقاء، إلا أن النشاط أو السلوك المادي في الجريمة المعلوماتية يتطلب توفر بعض الشروط والظروف التي تتلائم مع خصوصية هذا النوع من الجرائم التي ترتكب في بيئة رقمية ومن طرف شخص يفترض فيه قدر من المعرفة بجهاز الحاسوب وطريقة استخدامه، فالنشاط أو السلوك غير المشروع الذي يقوم به المجرم المعلوماتي والذي يعد أساسيا لقيام الجريمة المعلوماتية يدور في نطاق هذه البيئة ويستمد منها خصوصياتها لكونها جريمة تقوم على فعل يستخدم تقنية المعلومات عن طريق المنظومة المعلوماتية كوسيلة لارتكابها أو للاعتداء على هذه المنظومة، وبالتالي يختلف النشاط أو السلوك غير المشروع في الجريمة المعلوماتية

[1] - محمد ممدوح بدير، المرجع السابق، ص96.

باختلاف نوع الجريمة المرتكبة، بحيث تتنوع الجرائم المعلوماتية من جرائم ترتكب بواسطة المنظومة المعلوماتية، وأخرى ترتكب ضد هذه المنظومة.[1]

ثانيا– الركن المعنوي

لم يعرف المشرع الجزائري القصد الجنائي على غرار غالبية التشريعات، واكتفى بالنص في الجرائم على العمد، كما لا يكفي لقيام الجريمة ارتكاب عمل مادي فقط، بل لابد من أن يصدر أيضا عن إرادة الجاني، هذه العلاقة التي تربط العمل المادي بالفاعل تسمى بالركن المعنوي، الذي يتمثل في نية داخلية يضمرها الجاني في نفسه، ومن ثم يتخذ الركن المعنوي صورتين أساسيتين هما،صورة الخطأ العمد أي القصد الجنائي، وصورة الخطأ غير العمد أي الإهمال وعدم الاحتياط، إن الركن المعنوي في مختلف الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات تتخذ صورة القصد الجنائي إضافة إلى نية الغش، فالجرائم الإلكترونية هي من جرائم التقنية العالية تتطلب من المجرم الإلكتروني قدرا من المعرفة والتخصص، فكان من المتصور غالبا وقوعها في صورة واحدة هي صورة العمد، على اعتبار أن الجاني خطط ودبر لارتكاب جريمته من أجل الحصول على المعلومات أو لاختراق شبكة الحاسوب، أو الاعتداء على أنظمة المعالجة الآلية للمعطيات، سواء بالإدخال أو المحو أو التعديل.

فمثلا جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، هي جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصرية العلم والإرادة، فيلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء بهدف الإدخال أو المحو أو التعديل، وأن يعلم بأن سلوكه هذا يؤدي للتلاعب في المعطيات، كما يجب أن يعلم إنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاءه داخل النظام مشروعا، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع، سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء، أو كان يجهل بوجود حظر للدخول أو البقاء.[2]

[1]– عميمر عبد القادر، المرجع السابق، ص89،90.

[2]– يزيد بوحليط، المرجع السابق، ص134،135.

الفرع الثاني

تقسيمات الجرائم المعلوماتية

للجرائم المعلوماتية صور متعددة لا يمكن حصرها، كونها متجددة ومتزايدة باستمرار وبصورة مطردة مع التطور التكنولوجي من جهة، ومع تزايد استعمال الكمبيوتر و الإنترنت وغيرها من الأجهزة التقنية في مجالات الحياة المختلفة من جهة أخرى، بالإضافة إلى أن هذه الصور تختلف من بلد لآخر ومن مجتمع لآخر، ولكن مع ذلك فقد حاول بعض الفقهاء والبعض من المؤسسات الدولية تحديد هذه الصور خلال تصنيف هذه الجرائم.

أولا- تصنيف الفقيه مارتن واسك "Martin wasik"

صنف مارتن واسك الجرائم المعلوماتية إلى ثلاث أصناف، الصنف الأول يتضمن جرائم الاحتيال المعلوماتي وسرقة المعلومات، أما الصنف الثاني يتضمن جرائم الدخول والاستعمال غير الصرح بهما للنظام المعلوماتي أما التصنيف الثالث هو الجرائم الواقعة من خلال الكمبيوتر والأفعال المساعدة على ارتكاب الجرائم المعلوماتية[1]، وهي كما يلي:

1- الطائفة الأولى" الاحتيال المعلوماتي وسرقة المعلومات".

و تتضمن "جرائم التلاعب بالمعلومات المعالجة آليا بهدف الحصول من ورائه على ربح مادي غير مشروع، تزوير المعلومات المعالجة آليا بنية استخدامها فيما بعد في أغراض غير مشروعة، الحصول على المعلومات المعالجة آليا بطريقة غير مشروعة، القرصنة الواقعة على البرامج المعلوماتية".

2- الطائفة الثانية " الدخول والاستعمال غير المصرح بهما للنظام المعلوماتي".

لعل ابرز الجرائم التي تندرج تحت هذا القسم هي : جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي والجريمة هذه هي ذاتها متى ارتكبت بنية ارتكاب جريمة معلوماتية أخرى وجريمة

[1] – wasik martin , Crime and the Computer(Oxford Monographs on Criminal Law and Justice) , Oxford Universitypress , 1991,p41.

الاعتراض غير المشروع لنظام الحاسب الآلي وجريمة الاستعمال غير المصرح به لنظام الحاسب والأفعال غير المشروعة المتصلة بالبيانات الشخصية المعالجة آليا .[1]

3-الطائفة الثالثة " الجرائم الواقعة من خلال الكمبيوتر والأفعال المساعدة على ارتكاب الجرائم المعلوماتية".

وتشمل جرائم " أفعال التخريب والإتلاف الواقعة على مكونات المادية أو المعنوية للحاسب الآلي، الابتزاز والتهديد بتدمير المكونات المادية أو المعنوية للحاسب الآلي، صناعة وبيع المعدات والأدوات المساعدة على ارتكاب جرائم الكمبيوتر من مثل إعداد البرامج الخبيثة، أي الفيروسات التي تساعد على ارتكاب جرائم إتلاف المكونات المادية أو المعنوية للحاسب الآلي، الإفشاء غير المشروع للمعلومات التي يؤتمن الجاني عليها بحكم وظيفته، استعمال أنظمة الكمبيوتر في جرائم الاعتداء على أمن وسلامة الأفراد " .

ويؤخذ على هذا التصنيف أنه يعتبر جرائم الواقعة على المكونات المادية للكمبيوتر جرائم معلوماتية، في حين أن مثل هذه الجرائم هي جرائم تقليدية وليست معلوماتية، كما ويعاب على هذا التصنيف محاولته حصر وتحديد الأفعال المساعدة على ارتكاب الجرائم المعلوماتية، في حين أن حصر وتحديد مثل هذه الأفعال من الصعوبة بمكان في ظل التطورات السريعة والمستمرة للتكنولوجيا واستخداماتها المتشعبة.[2]

ثانيا- التقسيم الثلاثي للأستاذ سايبر

قسم الفقيه " UltrichSaeber" الأستاذ في جامعة "Wurzburg" في ألمانيا، وأحد أبرز المتخصصين بجرائم الكمبيوتر، الجرائم المعلوماتية إلى ثلاثة أقسام، الأول هو تلك الجرائم التي تهدد

[1] - عمار عباس الحسيني، المرجع السابق، ص 97.

[2]- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الإسكندرية، جمهورية مصر العربية 2018، ص32إلى34.

المصالح القومية للدولة وسلامة الأفراد، والثاني الجرائم المعلوماتية الاقتصادية، والثالث جرائم المعلوماتية التي تمس الحياة الخاصة.[1]

1- الجرائم التي تهدد المصالح القومية وسلامة الأفراد:

لم تعد الجريمة المعلوماتية قاصرة على الصورة البسيطة التي تمس أموال الأفراد و حقوقهم، بل باتت تهدد مصالح الأمن القومي والمصالح العليا للدولة، ومن أمثلتها التلاعب إلكترونيا بنتائج الانتخابات، كما حصل في الفلبين عام 1986، حيث تم اكتشاف مجموعة من الأوامر غير الصحيحة التي من شأنها تغيير نتيجة الانتخابات "**التزوير**"، ومنها مثلا جرائم تتعلق بالأمن القومي وسلامة البلاد، وكذلك جرائم عرقلة حسن سير العدالة كما حصل في ألمانيا، حيث حوكم بعض الأشخاص بتهمة الشروع في التلاعب بسجلات الشرطة لحذف أسماء بعض الأشخاص المطلوب القبض عليهم .

أما الجرائم المعلوماتية التي تمس السلامة الشخصية للأفراد، فمنها مثلا الجرائم الواقعة على أنظمة الحاسب المستخدمة في المؤسسات والمستشفيات ومعامل البحوث والتحاليل وما شابه، ولعل أبرزها اليوم ما يتعلق بحركة وسلامة الطيران، ومنها مثلا ما حدث في مطار كيندي في نيويورك عام 1979 حينما تعرضت إحدى الطائرات كانت تروم الهبوط في هذا المطار، والتي كان على متنها السفير الروسي آنذاك إلى تلاعب من قبل أحد المراقبين الجويين بنظام الحساب الآلي، وكذلك ما حدث عام 1984 حينما أخطأت إحدى الطائرات التابعة لشركة الطيران الكورية طريقها بسبب خطأ في برمجة الحسابات مما أدي إلى قصفها من قبل الطائرات الروسية.[2]

2- الجرائم المعلوماتية الاقتصادية:

وتشمل جرائم الاحتيال المعلوماتي بقصد الحصول وبغير حق على أموال أو أصول أو خدمات، التجسس المعلوماتي في نطاق قطاع الأعمال، القرصنة على برامج الحاسب الآلي، الإتلاف المعلوماتي من خلال الاعتداء على مكونات الكمبيوتر المادية أو غير المادية، أفعال الدخول غير

[1]- ulrichsieber , Legal Aspects of Computer-Related Crime in the Information Society-COMCRIME-Study- prepared for the European Commission ,version 1.0 of 1st January 1998 ,p24 ,26,27,38,39.

[2] - عمار عباس الحسني، المرجع السابق، ص98.

المصرح به للنظام المعلوماتي، سرقة الخدمات أو الاستعمال غير المصرح به للنظام المعلوماتي، الجرائم التقليدية الواقعة في نطاق قطاع الأعمال بمساعدة النظام المعلوماتي .[1]

3- الجرائم المعلوماتية التي تمس الحياة الخاصة.

الجرائم في هذا القسم تتعلق في ما يعرف بـ " البيانات الشخصية " أو المعلومات الشخصية، ولعل أبرز الجرائم التي تنطوي تحت هذا القسم هي الإفشاء غير المشروع للبيانات الشخصية وإساءة استخدامها، ومخالفة القواعد الشكلية التي يجب مراعاتها في مجال معالجة البيانات الشخصية، والجمع والتخزين غير المشروع لبيانات صحيحة واستخدام بيانات شخصية غير صحيحة.

أ- الإفشاء غير المشروع للبيانات الشخصية وإساءة استخدامها

لعل أكثر البيانات عرضة لجريمة الإفشاء المعلوماتي هي تلك الموجودة في ما يعرف بـ "بنوك المعلومات "، وكذلك الأسرار المتعلقة بالقطاع الأمني الذي تبدو فيه سمة الاحتفاظ بالمعلومات إلكترونيا واضحة.

ب- مخالفة القواعد الشكلية التي يجب مراعاتها في مجال معالجة البيانات الشخصية

تطلبت التشريعات المتخصصة عددا من القواعد والضوابط الشكلية التي لا بد من مراعاتها بغية معالجة البيانات الشخصية، ومنها مثلا ضرورة الحصول على ترخيص من جهة معينة، ولعل معالجة البيانات الشخصية بغير مراعاة هذه القواعد يعد جريمة معلوماتية معاقب عليها.[2]

ج- جمع وتخزين "بيانات شخصية صحيحة "بشكل غير مشروع

يتمثل فعل الانتهاك للحق في الحياة الخاصة للأفراد في عملية جمع وتخزين بيانات صحيحة عنهم لكن على نحو غير مشروع وغير قانوني، ويستمد هذا الجمع أو التخزين صفته غير المشروعة أما من الأساليب غير المشروعة المستخدمة للحصول على هذه البيانات والمعلومات، أو من طبيعة مضمونها، فمن حيث الأساليب غير المشروعة فقد يتم الاعتماد على وسائل تشكل انتهاكا واضحا

[1] - رشاد خالد عمر، المرجع السابق، ص34.

[2] - عمار عباس الحسني، المرجع السابق، ص99.

للخصوصية وذلك من أجل جمع المعلومات والبيانات عن الأفراد، ومن ضمن هذه الأساليب القيام بالتقاط الارتجاجات التي تحدثها الأصوات في الجدران الإسمنتية للحجرات وترجمتها إلى عبارات وكلمات بواسطة حاسوب مزود ببرنامج خاص، وكذلك قد يتم مراقبة الرسائل المتبادلة واعتراضها والتقاطها عن طريق البريد الالكتروني أو توصيل أسلاك بطريقة خفية إلى الحاسوب الذي تختزن بداخله البيانات أو التوصل بطريق غير مشروع إلى ملفات بيانات تخص آخرين، أو بأي وسيلة أخرى غير مشروعة كالتدليس والغش أو التصنت على المكالمات التي تتم عن طريق شبكة الانترنت، أما الجانب الآخر الذي يضفي صفة عدم المشروعية على جمع وتخزين البيانات هو أن تكون هذه البيانات غير صالحة للجمع والتخزين بسبب مضمونها .[1]

د- استخدام بيانات شخصية غير صحيحة

يقع هذا الاستخدام المجرم قانونا بإحدى الصورتين، الأولى جمع أو معالجة أو نشر بيانات شخصية غير صحيحة بواسطة الأشخاص الذين رخص لهم القانون ذلك، وهذه الصورة كما تقع بشكل عمدي فإنها تقع إهمالا أو عدم احتياط، أما الصورة الثانية فتتم عن طريق تغيير البيانات الشخصية أو ومحوها عن طريق أشخاص غير مصرح لهم بهذا التغيير أو المحو، وتنطوي هذه الصورة على المساس بالحقوق المالية للمرخص له بتخزين هذه البيانات.[2]

ثالثا- التقسيم الخاص بمنظمة التعاون الاقتصادي والتنمية:

قامت المنظمة بمسح لجريمة الحاسب الآلي بالدول الأعضاء بالمنظمة، وقد أسفر عمل اللجنة عن صدور تقرير في 1986 بعنوان "جرائم الحاسب الآلي"، وخلصت اللجنة في تقريرها إلى أن الأفعال الإجرامية المتعلقة بالجريمة المعلوماتية هي:

1- إدخال معلومات إلى نظام الحاسب الآلي، أو تعديل، أو محو معلومات موجودة على نحو غير مشروع، وذلك بنية تحويل الأموال أو الممتلكات التي تمثلها المعلومات.

[1] - نهلا عبد القادر المومني، المرجع السابق، ص174.

[2]-عمار عباس الحسني، المرجع السابق، ص101.

2- إدخال معلومات إلى نظام الحاسب الآلي، أو تعديل، أو محو معلومات موجودة بالفعل، واعتراض نظام الحاسب الآلي، وذلك بنية إعاقاته عن أداء وظيفته.

3- استغلال برامج الحاسب الآلي تجاريا، وطرحها بالأسواق، وذلك انتهاكا لحقوق المالك، أو الحصول غير المشروع على المعلومات .

4- الدخول أو الاعتراض غير المصرح به لنظام الحاسب الآلي متى تم ذلك عمدا سواء كان الدخول أو الاعتراض بنية ارتكاب جريمة أولا.

5- الاستعمال غير المصرح به لنظام الحاسب الآلي.[1]

رابعا- التقسيم الخاص بالمجلس الأوروبي:

تم الاهتمام بالجريمة المعلوماتية من خلال المؤتمر الثاني عشر لرؤساء معاهد العلوم الجنائية 1976 م، وأسفر المؤتمر عن صدور التوصية رقم 81(12).

والتي أقرتها لجنة الوزراء في المجلس الأوروبي في 25يونيو1981، قامت التوصية بتعريف جرائم الحاسب ضمن إطار الجرائم الاقتصادية كما يلي:

1- جرائم سرقة المعلومات.

2- التجسس المعلوماتي.

3- التلاعب بالبيانات المعالجة إلكترونيا.

واشترطت اللجنة لقيام تلك الجرائم، أن يتوافر بشأنها الشروط التالية:

أ- أن يترتب على الفعل ضرر جسيم، أو أن يخشى مثل هذا الضرر.

ب- أن يتوافر لدى الفاعل معرفة خاصة بتكنولوجيا المعلومات.

[1] - محمد محمود المكاوي، المرجع السابق، ص93.

ج- أن يكون هناك صلة وظيفية تربط بين الفاعل وبين محل السلوك الإجرامي المتمثل في البيانات المعالجة إلكترونيا.[1]

خامسا- تقسيم اتفاقية بودابست :[2]

حرص مجلس أوروبا على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات، وتجلى ذلك في اتفاقية بودابست في 23نوفمبر2001 المتعلقة بالإجرام الكوني، بمعنى الإجرام المعلوماتي أو الجرائم المعلوماتية، إيمانا من الدول الأعضاء في هذا المجلس والدول الأخرى الموقعة على هذه الاتفاقية بالتغيرات العميقة التي حدثت بسبب الرقمية والتقارب والعولمة المستمرة للشبكات المعلوماتية.

وقسمت هذه الاتفاقية الجرائم المعلوماتية إلى أربعة أقسام هامة وهي:

1- الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية، كالولوج غير القانوني " المادة الثانية "، والاعتراض غير القانوني " المادة الثالثة"، والاعتداء على سلامة البيانات "المادة الرابعة"، والاعتداء على سلامة النظام "المادة الخامسة"، وإساءة استخدام أجهزة الحاسب "المادة السادسة ".

2- الجرائم المعلوماتية الجرائم المتصلة بالحاسب، كالتزوير المعلوماتي "المادة السابعة"، و الغش المعلوماتي "المادة الثامنة".

3- الجرائم المتصلة بالمحتوى "المادة التاسعة "، و الجرائم المتصلة بالمواد الإباحية للأطفال "المادة التاسعة".

4- الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة "المادة العاشرة ".

---

[1]- محمد محمود المكاوي، المرجع السابق، ص92.

[2]- هلالي عبد الله أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، دار النهضة العربية، القاهرة، جمهورية مصر العربية، الطبعة الثامنة 2011، ص8،9 .

المبحث الثاني

نظم الحاسب الآلي والمجرم المعلوماتي

سوف نتطرق تحت هذا المبحث لنظم الحاسب الآلي وذلك من خلال التطرق لتعريفه وكذا تبيان أنواعه ومكوناته هذا من جهة، ومن جهة أخرى التطرق لماهية الانترنت وذلك بتعريفها وتبيان تطورها التاريخي وكذا خدماتها كل هذا تحت المطلب الأول، أما المطلب الثاني فخصصناه للمجرم المعلوماتي وذلك بتعريفه وتبيان أهم سماته وكذا دوافعه للإجرام بتبيان بعضها مثل تحقيق الكسب المالي أو دوافع سياسية مثلا أو رغبة منه في التعلم وغيرها .

المطلب الأول

ماهية الحاسوب والإنترنت

إن الجريمة المعلوماتية مرتبطة سواء بالحاسوب، أو الإنترنت، أو كلاهما، فكان علينا التطرق إليهما، ولو بشكل موجز قبل التطرق لهذا النوع من الجرائم.

الفرع الأول

ماهية الحاسوب

نعالج تحت هذا المطلب كل من تعريف الحاسوب، وأنواعه، ومكوناته.

أولا- التعريف بالحاسوب

لا بد من الإشارة ابتداء إلى أن العديد من الكتاب يذهب إلى تسمية الحاسوب "بالكمبيوتر" وهي تسميات تدل على معنى واحد، ويبدو أن سبب هذا الخلط والتداخل بين المصطلحين يعود إلى الترجمة من اللغة الأجنبية إلى اللغة العربية، فهذا الجهاز يطلق عليه بحسب الاصطلاح الأجنبي تسمية

« computer »التي تعني العقل إلكتروني والتي ترجمت إلى العربية تحت اصطلاح "الحاسب الآلي" ، أو "الحاسوب الآلي" .[1]

1- التعريف اللغوي للحاسوب

على وزن فاعول، هو مشتق من الجذر اللغوي "حسب"، وحسبه أي عده، والحساب هو العد وحاسبه محاسبة، أي ناقشه الحساب، والحسبان بمعنى العد و التدبير والتدقيق.

ويشير البعض بهذا الصدد إلى أن تسمية هذا الجهاز ابتداء كانت التسمية الإنجليزية ذاتها "computer " ، حيث شاع استخدام هذا المصطلح في بداية عهده، أو كما سماه البعض "qunicailler" باعتبار أن هذا المصطلح هو الترجمة الحرفية للمصطلح الإنجليزي الشائع"hardware"، غير أنه سمي فيما بعد بـ"الحاسوب"، أو "الحاسب الآلي"، وهي التسمية الشائعة التي صارت عنوانا لكثير من المؤلفات المتخصصة، وغير المتخصصة، ومما تجدر إليه الإشارة أن مصطلح "الحاسوب"، هو المصطلح الذي لجأت إلى استعماله بعض المؤسسات العربية، كمجمع اللغة العربية الأردني، الذي عرب كلمة computer المشتقة من الفعل comput إلى الحاسوب، بوصفها الترجمة المقبولة، على أساس أن الفعل comput يعني باللغة العربية الفعل "يحسب" كما استخدمت هذا المصطلح أيضا "المنظمة العربية للمواصفات والمقاييس" في إطار إشارتها إلى النظام الآلي.

وعلى العموم فقد عرف جهاز الحاسوب " الكمبيوتر" بالعديد من التعريفات الفقهية والتشريعية، وفي نهاية الأمر يبقى تعريف هذا الجهاز تعريفا له طابع فني.

2- التعريف الفقهي

يذهب البعض إلى تعريف بأنه "مجموعة من الآلات الالكترونية تقوم بمجموعة مترابطة ومتتالية من العمليات على مجموعة من المعطيات الداخلة تتناولها بالمعالجة وفقا لمجموعة من التعليمات

[1]- عمار عباس الحسني، المرجع السابق، ص11.

المنسقة بشكل منطقي وتسلسلي حسب خطة موضوعة مسبقا لحل مسألة معينة معروفة بغرض الحصول على نتائج ومعلومات تفيد في تحقيق أغراض معينة".[1]

ومن هذه **التعريفات** مثلا أنه " جهاز إلكتروني يعمل طبقا لتعليمات محددة سلفا، ويمكنه استقبال البيانات وتخزينها، والقيام بمعالجتها بدون تدخل من الإنسان ثم استخراج النتائج المطلوبة، وعرف أيضا بأنه "الآلة المتفاعلة مع الأوامر الإنسانية ذات التقنية المتطورة في معالجة البيانات"، وعرف بأنه " آلة مبرمجة مكونة من عدة وحدات متناسقة في عملها، مهمتها معالجة البيانات والمعطيات"، كما عرف بأنه " جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية، طبقا للتعليمات المعطاة له بسرعة تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة، وبدرجة عالية من الدقة، وله القدرة على التعامل مع كم هائل من البيانات، وتشغيلها واسترجاعها عند الحاجة إليها".

3- التعريف من الناحية الفنية الصرفة

ذهبت الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني إلى تعريفه بأنه "جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال البيانات أو إخراج معلومات وإجراء عمليات حسابية، أو منطقية، وهو يقوم بالكتابة على أجهزة الإخراج أو التخزين، والبيانات يتم إدخالها بواسطة مشغل الحاسب عن طريق وحدات الإدخال مثل لوحة المفاتيح، أو استرجاعها من خلال وحدة المعالجة المركزية التي تقوم بإجراء العمليات الحسابية، وكذلك العمليات المنطقية، ثم تتم كتابة البيانات على أجهزة الإخراج مثل الطابعات، أو وسائط التخزين المختلفة.

4-التعريف من الناحية التشريعية

فقد عرفه القانون الأمريكي بأنه " جهاز إلكتروني بصري كيميائي كهربائي، أو جهاز إعداد معلومات ذو سرعة عالية، يؤدي وظائف منطقية حسابية أو تخزينية، و يشتمل على أي تسهيل لتخزين المعلومات، أو تسهيل اتصالات مباشرة مقترنة، أو تعمل بالاقتران مع هذا الجهاز، كما عرفه نظام مكافحة جرائم المعلوماتية السعودي لسنة 1428هـ الحاسب الآلي بأنه " أي جهاز إلكتروني

[1] – عصام عبد الفتاح مطر، الحكومة الالكترونية بين النظرية والتطبيق، دار الجامعة الجديدة، الإسكندرية، مصر 2018، ص 16.

ثابت، أو منقول سلكيا و لاسلكي، يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها أو استقبالها أو تصفحها، يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له".[1]

ثانيا- أنواع أجهزة الحاسوب

تتعدد تقسيمات أجهزة الحاسوب وأبرزها تقسم من حيث وظيفتها وتركيبها من جهة ومن جهة أخرى من حيث أحجامها.

1- أقسام الحاسبات الإلكترونية من حيث وظيفتها وتركيبها

تتنوع الحاسبات الإلكترونية حيث يمكن تقسيمها من حيث وظيفتها وتركيبها إلى:

أ- **الحاسوب القياسي:** يستخدم هذا الحاسوب في القياسات الكمية التي لا يمكن التعبير عنها بالعدد مباشرة، و مجالات استخدام هذا الحاسوب، تكون في التطبيقات التي تحتاج إلى عمليات تفاضلية، وفي تطبيقات التغذية العكسية، إذ يستخدم في السيطرة على حركة القذائف الصاروخية، والعمليات الكيمياوية المسيرة بصورة أوتوماتيكية، وفي التطبيقات التي تحتاج إلى سيطرة أنية ومباشرة، وتستخدم أيضا في محطات توزيع الشبكات الكهربائية على المدن، وفي شبكات الري الخارجية وفي سدور المياه.

ب- **الحاسوب الرقمي** : الحاسوب الرقمي يتعامل مع الأرقام في عمليات الإدخال والإخراج والمعالجة في البيانات تخزن في ذاكرته في شكل أرقام وإذا طلب منه استرجاعها فسيعطيها في الشكل المقروء وليس كما هو مسجل في ذاكرته، وهذا النوع هو المستخدم والمنتشر عالميا في بنوك المعلومات.

ج- **الحاسوب الهجين أو المختلط** : وهو الحاسوب الذي يجمع بين الأسلوبين السابقين ويمكن الحصول عليه بالتوصيل المباشر بين حاسوب رقمي وآخر قياسي بواسطة جهاز تخزين خاص.

[1]- عمار عباس الحسني، المرجع السابق، ص11 الى14.

2- أقسام الحاسبات الإلكترونية من حيث أحجامها:

تتنوع الحاسبات الالكترونية من حيث أحجامها، حيث يمكن تصنيفها إلى:

أ- **الحاسوب الكبير** : ويتميز هذا الحاسوب بكبر حجمه وسعة ذاكرته والقدرة الفائقة على معالجة البيانات بسرعة عالية، وينفذ هذا الحاسوب ملايين التعليمات في الثانية الواحدة، وهذا النوع يستخدم في الغالب الأعم من قبل البنوك، والمنظمات الكبيرة لمعالجة كميات كبيرة من البيانات كتحضير الشيكات المدفوعة والفواتير والطلبيات.

ب- الحاسب المتوسط : وهو حاسوب صغير نسبيا إذا قورن بالحاسوب الكبير، وهو ينجز عملياته بصورة متكاملة، و وقت أطول من الوقت الذي ينجز فيه الحاسوب الكبير هذه العمليات، ويستخدم هذا النوع في الأعمال التجارية الكبيرة والمعقدة نوعا ما، وتستخدم في الأماكن التي يكون فيها استخدام الحواسيب الشخصية غير مناسب.

ج- الحواسيب الصغيرة: وهو أصغر أنواع الحواسيب وأكثرها شيوعا، ويفضل الملايين من الأشخاص استخدامها نظرا لحجمها الصغير وتكلفتها المتدنية.

وعليه فالحواسيب الكبيرة والمتوسطة والصغيرة، هي أشهر أنواع الحواسيب من حيث الحجم وهناك أنواع أخرى منها:- **الكمبيوتر المحمول:** وهو جهاز كمبيوتر يسهل التنقل به من مكان إلى مكان ويؤدي مهام الكمبيوتر العادي، ولا يقل خطورة من حيث ارتكاب الجرائم عن الهواتف الذكية أو الكمبيوترات اللوحية " تابلت".[1]

- **حواسيب الجيب** :وهي حواسيب صغيرة تمسك باليد وتقوم بالوظائف نفسها التي يمكن أن تقوم بها الحواسيب المحمولة، ولكن بشكل بسيط.

- **شبكات الحواسيب:** وهي إما مجموعة حواسيب شخصية تتصل معا بأسلاك حيث يسهل نقل المعلومات بين الأجهزة، ولكن هذا لا يلغي استقلالية كل حاسوب عن الآخر بمعداته وبرمجياته، وإما

[1] - بهاء المرى، جرائم المحمول والانترنت، منشأة المعارف، الإسكندرية، مصر 2018، ص 20.

حاسوب يسمى الخادم ، يتصل مع مجموعة محطات، أو طرفيات مثل الحواسيب الشخصية تسمى العملاء[1].

ثالثا- مكونات الحاسب الآلي(الحاسوب)

الحاسب الآلي من حيث تكوينه يمكن رده إلى قسمين المادي والمعنوي.

1- القسم المادي:

والذي يشتمل على الأجزاء المحسوسة المادية التي يمكن رؤيتها، ولمسها في الحاسب الآلي، ويمكن رد هذه المكونات إلى:

أ- **جهاز الإدخال:** هي أدوات يمكن بواسطتها إدخال البيانات إلى الحاسوب مثل لوحة المفاتيح والفأرة والماسح الضوئي وقلم الإدخال والميكروفون وقارئ الباركود (الشيفرة العمودية) [2].

ب- وحدات المعالجة: وتنطلق من وحدة المعالجة المركزية، وهي بمثابة العقل المدير المسيطر، والمتحكم بكافة مهام الحاسب الآلي، ويندرج ضمن هذه الوحدة الرئيسية وحدات إضافية أولى مساعدة ومتخصصة منها:وحدة التحكم ، وحدة الحساب والمنطق، وحدة التخزين.

ج- وحدات الإخراج : وتستخدم لإخراج البيانات والمعلومات المعالجة أليا داخل الحاسب الآلي والحيز الواقعي الملموس بأشكال وطلبات معينة، وهي الشاشة screen، و الطابعة printer ، والسماعة القادرة على إخراج الأصوات بشكل مسموع.

2- القسم المعنوي

وهي عموما برامج الحاسب الآلي، والتي تعتبر القسم غير المرئي وغير الملموس من الحاسب الآلي، وهي عبارة عن إشارات كهربائية مغناطيسية قادرة على معالجة البيانات والمعلومات المدخلة

[1]- نهلا عبد القادر المومني، المرجع السابق، ص21، ص22.

[2] - ar.m.wikipedia.org/wil
الدخول يوم 10-03-2023 على الساعة 02:31

للحاسب الآلي، والخروج بها بصورة مختلفة بناء على الطلب المتوفر أصلا ضمن آليات محددة، وتنقسم البرامج وفقا لذلك إلى أنواع مختلفة هي:

أ- **برامج التشغيل:** هي إحدى أنواع البرامج وأكثرها أهمية، إذ تعتمد عليها سائر برامج الحاسب الآلي الأخرى لاحتوائها على آليات العمل والتشغيل كما يعتمد عليها الحاسب الآلي ذاته، وهي بمثابة الروح للجسد، وهي وسيلة المستخدم للحصول على مزايا وخدمات الحاسب الآلي المتوقعة، إذ يحتوي برنامج التشغيل في كل تطبيق على الأوامر اللازمة لتفعيل هذا التطبيق أو ذاك.

وعادة ما تعتمد برامج التشغيل على نواح ابتكارية خلاقة، فهي تعتمد على لغة البرمجية كما يسميها أصحابها، والتي تمكن البرامج من العمل، ومن لغات البرمجة المعتمدة لغة الآلة، ولغة التجميع ، ومن تطبيقاتها عمليا لغة **بيسك**، و لغة **فورتزان**، ولغة **باسكال**، ولغة **كوبول** وغيرها.

ب- برامج التطبيق: تأتي هذه البرامج تلبية لرغبات متلقي خدمات الحاسب الآلي، وهي تأتي بمهام و وظائف فائقة وعظيمة ذات صلة بعمل الإنسان، وفي شتى مجالات الحياة، طبيا وقانونيا، اجتماعيا واقتصاديا وترفيهيا ونحو ذلك، فإذا كان ذلك كله معا بشكل مناسب كان لدينا جهاز حاسب اليد و جزأين معنوي ومادي، يملك برامج تشغيلية كافية لأداء عمله الأصلي، وبرامج تطبيقية قادرة على تلبية مهام خاصة تطلب منه في مجال ما،وكان هذا الجهاز بهذه الصفة أحد أمرين:- جهاز شخصي.

- شبكة متكاملة، سواء كانت محدودة داخلية أم خاصة أم غير محدودة بما يعرف بشبكة الإنترنت.[1]

الفرع الثاني

ماهية الانترنت

حدث نمو نوعي في غضون القرن العشرين لحجم ومقاييس المعلومات والمعارف المتداولة وسمي ذلك بالانفجار المعلوماتي أو الثورة المعلوماتية، وباتت صناعة المعلوماتية في العقود الأخيرة الموجه الرئيسي لتسريع التقدم العلمي، وكان لظهور الانترنت أثر كبير في انتقال المعلومات وتداولها

[1]- أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، 2014 ص29إلى31.

والاستفادة منها في وقت قياسي في أي مكان في العالم، فالانترنت ساهم بشكل لا نظير له في صناعة المعلومات وثورتها فهو أحد العناصر الرئيسية التي ترتكز عليها تكنولوجيا المعلومات .[1]

وللوقوف على تقنية الانترنت لابد علينا أن نتعرض إلى تعريفها، وكذلك تطورها التاريخي، وكذا استخداماتها .

أولا- تعريف الانترنت :

وهو عبارة عن مجموعة من الحاسبات المنتشرة جغرافيا عبر العالم والمرتبطة من خلال شبكات منطقة محلية (LAN) [2]، وشبكات منطقة واسعة (WAN) [3]موزعة في أنحاء العالم بهدف نقل وتبادل المعلومات والبيانات، وهذه الحاسبات قد تكون متصلة بخطوط تليفون أو كابلات أو أقمار صناعية أو وصلات لا سلكية .[4]

عرفت تقنية الانترنت بالعديد من التسميات، فقد سميت مثلا بـ (الشبكة العنكبوتية الإلكترونية) أو (شبكة الشبكات) أو (الفضاء السيبراني الالكتروني Cyberspace)، جدير بالذكر أن مفرد " الإنترنت Internet" هي مختصر لتعبير " Interconnected network" التي تعني " الشبكة البينية" وهو اسم يدل على بنية شبكة الانترنت باعتبارها شبكة مابين الشبكات، ولهذا فمن الخطأ القول الشائع أن كلمة الانترنت مكونة من المقطع "Inter" وهو مختصر "International" والتي تعني " دولي " وكلمة " Network " والتي تعني " شبكة " وبذلك يصبح ترجمة عبارة الانترنت (الشبكة الدولية للمعلومات)، وهو قول غير صحيح .[5]

---

[1]- نهلا عبد القادر المومني، المرجع السابق، ص 34.

[2]- شبكة العمل المحلية هي شبكة تسمح للمستخدمين بالمشاركة في استخدام الأجهزة والمعدات والبرمجيات عن طريق حاسب يسمى خادم الشبكة، ويمكن استخدام هذه الشبكة في شركة أو وزارة أو هيئة .

[3]- وتكون هذه الشبكة على مستوى المنظمات الكبرى والشركات والبنوك والدول.

[4]- عصام عبد الفتاح مطر، المرجع السابق، ص 24.

[5] - عمار عباس الحسني، المرجع السابق، ص20.

ثانيا– التطور التاريخي لشبكة الانترنت:

لم تكن الانترنت كفكرة في حسبان من بدئها، وكانت البداية عندما أطلق الاتحاد السوفيتي القمر الصناعي " سبوتنك " (sputnik) في عام 1957 وحينها شعرت الولايات المتحدة الأمريكية بالخطر لهذا التقدم العلمي وأنها تحتاج إلى التفوق على هذا التطور، فتم إنشاء وكالة لمشروعات الأبحاث المتقدمة سميت "أرب" (ARPA) تتبع وزارة الدفاع الأمريكية وعهد إليها بمهمة التفوق العلمي والتكنولوجي للقوات المسلحة في مواجهة الاتحاد السوفيتي، وفي عام 1962 عهدت القوات الجوية الأمريكية لمؤسسة حكومية متخصصة في أنشطة البحوث والتطوير تسمى "راند" (Rand) بتنفيذ دراسة لتحقيق ضمان السيطرة على الصواريخ في حال حدوث كوارث واتصال المسئولين في وزارة الدفاع الأمريكية فيما بينهم، فقدم الباحث " بول باران" (Paul Baran) الباحث في مجال الاتصالات مقترحا لإنشاء شبكة اتصالات وربط الحاسبات بشبكة واحدة تعمل على تجزئة الرسالة messagالمراد إرسالها إلى موقع معين في الشبكة إلى حزم متساوية بحيث يتم نقل كل جزء من الرسالة من خلال طريق يختلف عن الآخر وعند وصل كل الأجزاء تتجمع مرة أخرى في نقطة الاستقبال لتشكل الرسالة كما كانت مرسلة وذلك لتفادي عملية الاختراق وسميت هذه الطريقة PacketSwitched Network وكانت هذه الفكرة هي بداية فكرة الانترنت .[1]

فعهدت وزارة الدفاع الأمريكية لوكالة مشاريع الأبحاث المتطورة بهذه المهمة في عام 1964.[2]

كانت النشأة سنة 1969 في الولايات المتحدة الأمريكية، عندما قرر مجموعة من العلماء إقامة نظام حاسوبي داخل وزارة الدفاع الأمريكية لتمكين العسكريين من متابعة عمل الحكومة ومن تطوير خدماتهم ونشاطاتهم العسكرية، ومن تحسب نشوب الحرب النووية، ولاسيما عند ظهور التهديدات النووية، والحرب الباردة بين أمريكا والاتحاد السوفيتي، الإشراف على المشروع وكالة (ARPA) [3]في

[1] – بهاء المرى، شرح قانون مكافحة جرائم تقنية المعلومات، المرجع السابق، ص 9 .

[2]– بهاء المرى، جرائم المحمول والانترنت، منشأة المعارف، الإسكندرية ، مصر، 2018، ص15.

[3] – وكالة مشاريع الأبحاث المتقدمة (Advanced Research Projects Agency) .

قسم الدفاع في الولايات المتحدة الأمريكية بالتعاون مع بعض المتعاقدين والجامعات وأطلق عليها في البداية اسم (ARPANET).[1]

ثم تطور المشروع بعد ذلك إلى الاستعمال السلمي بجانب الاستعمال العسكري، حيث انقسم عام 1983 إلى شبكتين احتفظت الشبكة الأولى باسمها الأساسي (ARPANE) وبالغرض الأساسي الذي نشأت من أجله وهو خدمة جهاز المخابرات المركزية الأمريكية ويرمز إليها بـ(CIA) وسميت الشبكة الأخرى باسم (MAIL NET) وتلك الشبكة تم تخصيصها للاستخدامات المدنية التي خصصت للاستخدام السلمي المدني ومن ثم ظهر اسم (ENTER NET)، وفي عام 1986 أمكن ربط خمس مراكز للكومبيوترات العملاقة وأطلق عليها اسم (NSF NET) والتي أصبحت فيما بعد العمود الفقري والأساسي لنمو و ازدهار شبكة الانترنت في الولايات المتحدة الأمريكية ثم دول العالم أجمع بعد ذلك .[2]

في مارس 1989 ظهرت الشبكة العالمية للمعلومات (WWW) عندما اقترح تيم بيرزلى (الذي يعمل في المركز الأوروبي للأبحاث النووية الذي يضم مجموعة من الباحثين الأوروبيين في مجال الفيزياء والطاقة) مشروعا لنقل الأبحاث والأفكار فعليا ضمن مركزهم، حيث كان الاتصال الفعلي من أحد أهداف المركز لأن العاملين فيه كانوا موزعين في عدد مختلف من البلدان، وتسهم هذه الشبكة في الحصول على المعلومات اللازمة في كافة المجالات من خلال التصفح في المواقع الموجودة بهذه الشبكة، وبالتالي يمكن للمنظمات عمل صفحات لها تشير لنشاطها والمنتجات التي تقدمها للجمهور سواء سلع أو خدمات حكومية أو خاصة، أي توفير كافة المعلومات بحيث يكون العملاء على معرفة تامة بالخدمات التي تهمهم داخل الموقع والاستفادة منها بأقل جهد ووقت من خلال تسهيل الإجراءات للمستخدمين .[3]

مع حلول عام 1990 عانت شبكة (ARPANET) من البطء وظهر فيها الكثير من العيوب، كما أن ظهور حواسيب أصغر حجما وأكثر قوة من الحواسيب المتوسطة أدى إلى ضعف شبكة (NSFNET) .

[1] – هارون منصر، تكنولوجيا الاتصال الحديثة، المسائل النظرية والتطبيقية، دار الألمعية للنشر والتوزيع، قسنطينة، الجزائر، الطبعة الأولى 2012، ص 115.

[2] – منير محمد الجنبيهى، ممدوح محمد الجنبيهى، دار الفكر الجامعي، الإسكندرية، مصر 2006، ص8.

[3] – عصام عبد الفتاح مطر، المرجع السابق، ص25.

إن الحاجة الماسة إلى استخدام الشبكات نفسها لأغراض تجارية يستفيد منها الأفراد والشركات والمؤسسات أدى إلى تطور الشبكة من الجانب التجاري حيث ابتدع عدد من الشركات الكبرى شبكاتهم العالمية، أضف إلى ذلك أن الإصدار الأول من موزاييك(MOSAIC) مستعرض الشبكة العالمية عام 1993 وما تبعه من إصدار (نت سكيب) و(مايكروسوفت)، كل هذه الأمور أدت إلى تطور شبكة الانترنت بالصورة التي نراها الآن، حيث تربط هذه الشبكة في الوقت الحاضر بين ملايين الحواسيب الممتدة عبر قارات العالم، وهناك ملايين المشتركين والمستخدمين الذين يستعملون هذه الشبكة لأغراض مختلفة لتحقيق أهداف تتنوع حسب مراكز هؤلاء الأشخاص وطبيعة أعمالهم .[1]

أما الجزائر سعت إلى الاستفادة من خدمات شبكة الانترنت والتقنيات المرتبطة بها، من خلال ارتباطها بشبكة الانترنت في شهر مارس من عام 1994عن طريق مركز البحث والإعلام العلمي والتقني (CERIST)، الذي أنشئ في شهر مارس سنة 1986 من قبل وزارة التعليم العالي والبحث العلمي، وكان من مهامه الأساسية أنذاك هو العمل على إقامة شبكة وطنية وربطها بشبكات إقليمية ودولية، وعرفت الجزائر منذ سنة 1994 تقدما ملحوظا في مجال الاهتمام والاشتراك والتعامل مع الانترنت، ففي نفس السنة كانت الجزائر مرتبطة بالانترنت عن طريق إيطاليا، تقدر سرعة الارتباط بـ9600حرف ثنائي في الثانية 9.6 Ko، وهي سرعة جد ضعيفة، وقد تم ذلك في إطار مشروع تعاون مع منظمة اليونسكو بهدف إقامة شبكة معلوماتية في إفريقيا تسمى بـ (RINAF)، وتكون الجزائر هي النقطة المحورية للشبكة في شمال إفريقيا، وفي مارس 1999 أصبحت قدرة الانترنت في الجزائر بقوة 2 ميغابات في الثانية، وبعد إصدار المرسوم التنفيذي رقم 98-257 والمعدل بمرسوم تنفيذي آخر 2000-307 الذي يحدد شروط وكيفيات وضع واستغلال خدمة الانترنت، ظهر مزودون جدد خواص وعموميين مما زاد في عدد مستخدمي الشبكة .[2]

ونقدم بعض الإحصائيات للوقوف على حجم المترددين على خدمات الانترنت في إفريقيا والجزائر وبعض الدول العربية الإفريقية حسب أحدث الأرقام[3]:

[1] – نهلا عبد القادر المومني، المرجع السابق، ص38.

[2] – هارون منصر، المرجع السابق، ص141.

[3] – www.internetworldstats.com الدخول للموقع يوم 2022/09/22 على الساعة 10:35

AFRICA 2022 POPULATION AND INTERNET USERS STATISTICS						
AFRICA	Population (2022 Est.)	Internet Users 31-DEC-2000	Internet Users 31-DEC-21	Internet Penetration	Internet Growth % 2000 - 2021	Facebook subscribers 30-APRIL-22
Algeria	45,150,879	50,000	37,836,425	83.8 %	50,756 %	26,291,400
Angola	34,592,611	30,000	8,980,670	26.0 %	29,835 %	2,875,600
Benin	12,653,644	15,000	3,801,758	30.0 %	25,245 %	1,686,800
Burkina Faso	21,863,344	10,000	4,594,265	21.0 %	45,842 %	2,539,900
Cameroon	27,646,656	20,000	9,158,422	33.1 %	39,292 %	4,723,600
Central AfricanRep.	4,967,426	1,500	557,085	11.2 %	37,039 %	150,000
Chad	17,217,597	1,000	2,237,932	13.0 %	223,693 %	644,200
Comoros	900,222	1,500	228,800	25.4%	12,813 %	223,000
Congo	5,744,245	500	930,800	16.2 %	166,540 %	904,700
Congo, Dem. Rep.	94,152,930	500	16,355,917	17.4 %	3,271,083 %	5,117,700
Djibouti	1,011,573	1,400	548,832	54.3 %	39,102 %	151,000
Egypt	105,530,371	450,000	54,741,493	51.9 %	12,064 %	51,286,200
Equatorial Guinea	1,481,822	500	362,891	24.5 %	72,478 %	125,700
Eritrea	3,626,986	5,000	248,199	6.8 %	4,864 %	6,200
Eswatini	1,179,737	10,000	665,245	56.4 %	6,552 %	421,500
Ethiopia	119,748,379	10,000	21,147,255	17.7 %	211,372 %	7,535,700
Gabon	2,313,754	15,000	1,367,641	60.0 %	9,017 %	872,600
Gambia	2,531,578	4,000	442,050	19.0 %	11,713 %	478,000
Ghana	32,154,245	30,000	14,767,818	45.9 %	49,126 %	9,163,200
Guinea	13,734,762	8,000	2,551,672	18.6 %	31,795 %	2,446,700
Guinea-Bissau	2,046,008	1,500	900,000	44.0 %	16,566 %	900,000
Kenya	55,752,020	200,000	46,870,422	85.2 %	23,335 %	12,445,700
Libya	7,024,811	10,000	6,658,900	94.8 %	58,470 %	6,658,900
Madagascar	28,427,328	30,000	2,864,000	10.1 %	9,446 %	2,864,000

Mali	20,855,735	18,800	12,480,176	59.8 %	66,284 %	2,033,300
Mauritania	4,775,119	5,000	969,519	20.3 %	19,290 %	927,300
Morocco	37,344,795	100,000	25,589,581	68.5 %	25,489 %	21,730,000
TOTAL AFRICA	1,373,486,514	4,514,400	590,296,163	43.0 %	12,975 %	255,412,900
Rest of World	6,502,279,070	356,471,092	4,463,594,959	68.6 %	88.3 %	2,475,026,941
WORLD TOTAL	7,875,765,584	360,985,492	5,053,891,122	64.2 %	100.0 %	2,730,439,841

ثالثا- خدمات الانترنت :

توجد خدمات كثيرة للشبكة العالمية للمعلومات "الانترنت"، سوف نتطرق للبعض منها

1-البريد الالكتروني :

خدمة البريد الالكتروني تسمح بتبادل المعلومات بين ملايين المستخدمين في مختلف أرجاء المعمورة، ويمكن لرسائل البريد الالكتروني أن تكون نصوصا عادية أو نصوصا محررة، أو معطيات أو بيانات، أو حتى صوت أو صورة، ويتم تبادل هذه الرسائل بشكل يكاد يكون فوريا اعتمادا على حجم الرسائل وسرعات خطوط النقل والمسافة التخيلية بين المرسل والمستقبل، وهناك مميزات أخرى لهذه الخدمة منها إمكانية المشاركة في مجموعة مناقشة عبر لوائح البريد الالكتروني والتعرف على أناس جدد، ويوجد في الوقت الراهن العديد من الهيئات التي تعتمد تماما على البريد الالكتروني في أعمالها وتبادل وثائقها حيث ألغت التعامل بالوثائق الورقية واعتمدت الوثائق الالكترونية [1]، وغير ذلك من الخدمات التي يقوم بها البريد الالكتروني .

2- المجموعات الإخبارية (News groups): وهي عبارة عن أماكن وساحات افتراضية للقاء والتحادث بين مستخدمي شبكة الانترنت من ذوي الاهتمامات المشتركة الذين يؤلفون فيما بينهم مجموعات نقاش وتبادل للبيانات والمعلومات والأفكار حول موضوع معين من المواضيع .[2]

[1] - عصام عبد الفتاح مطر، المرجع السابق، ص 26.

[2] - نهلا عبد القادر المومني، المرجع السابق، ص41.

3- الشبكة العنكبوتية العملاقة (world.wide.web) :

وهي ما يرمز لها اختصارا بالرمز (w.w.w)، أو ما تسمى أيضا ب"خدمة الويب" وهذا الأخير نظام فرعي من أنظمة الانترنت إلا انه مع ذلك يعد نظاما معلوماتيا عالميا مؤلفا من كم هائل من النصوص والصور والعينات الصوتية ولقطات الفيديو وغيرها، ومن ثم فخدمة الويب هذه تعد النظام الأعظم والأكثر شهرة على شبكة الانترنت اليوم، بحيث يستطيع المستخدم من خلال برنامج يسمى متصفح أو مستعرض تصفح محتويات هذا النظام، عن طريق تتبع الوصلات التشعبية أو اختيار المواقع التي يرغب في زيارتها والقيام بنشاطات أكاديمية كالبحث العلمي أو نشاطات اجتماعية كالتعارف والتخاطب والتراسل أو نشاطات ترفيهية كالألعاب، أو اقتصادية كالتسوق وغيرها...[1]

4- التجارة الالكترونية :

تعتبر الانترنت وسيلة من وسائل التجارة الالكترونية، إذ أتاحت الانترنت لطرفي العقد التقابل وجها لوجه بالصوت والصورة رغم تباعدهما ألاف الأميال، والاتفاق على التفصيلات الدقيقة، بعد إبداء الإيجاب ثم القبول بطريق الانترنت، ثم إبرام العقد، والتوقيع عليه بطريق – التوقيع الالكتروني – دون حاجة لاجتماع المتعاقدين في مكان واحد، ويتم إبرام العقد بالطبع بعد أن يكون البائع أو المورد أو مقدم الخدمة قد أعلن عنها بطريقة واضحة وكافية على شبكة الانترنت، وأن يكون الطرف الآخر قد اطلع على هذا الإعلان وحصل على الإيضاحات والتفسيرات المطلوبة بشأن السلعة أو الخدمة المعروضة، وكل هذه مراحل سابقة لإبرام العقد، ويمكن للمشتري أو المستورد أن يسدد قيمة بضاعته عن طريق الدفع – بواسطة شبكة الانترنت – ويكفيه في ذلك رقم حسابه البنكي ورقم بطاقة الائتمان الخاصة به .[2]

5- خدمة الدخول عن بعد:

[1] – عمار عباس الحسني، المرجع السابق، ص28.

[2] – عبد الفتاح بيومي حجازي، الأحداث والانترنت دراسة متعمقة عن أثر الانترنت في انحراف الأحداث، دار الكتب القانونية، المحلة الكبرى، مصر 2007 ، ص30.

(TEL NET) وهي خدمة تتيح استخدام أي برامج أو تطبيقات في حاسب إلى آخر .[1]

وعليه فإن استخدام تقنيات الحاسب الآلي والانترنت، لم يعد قاصرا على ميادين علمية أو صناعية محدودة، بل أصبح الحاسب الآلي وتقنياته الحديثة عنصرا أساسيا في جميع المعاملات والأنشطة التي يقوم بها الإنسان وتمس حياة كل فرد، فالفاكس، الهاتف المحمول، أجهزة التصوير المقطعية، أجهزة التحاليل الطبية، معدات العمليات الجراحية، التجارة الالكترونية، وسائل النقل والاتصالات الفضائية، بطاقات الصرف الآلي ...، أصبحت منظمة بالتقنيات العالية للحاسب الآلي، ولاشك أن اتساع نطاق استخدام هذه التقنيات العالية في بيئة المعلومات العالمية ومن خلال البنيات التحتية لنظام المعلومات الكونية سوف يؤدي إلى تزايد الجرائم والأنشطة غير المشروعة في هذا المجال،[2] فيما يعرف بجرائم الحاسب الآلي والانترنت أو الجرائم الالكترونية.[3]

المطلب الثاني

التعريف بالمجرم المعلوماتي وسماته وأهم دوافعه

قبل وجود شبكة تربط بين الحسابات ومستخدميها، فقد كانت هناك فئات مستقلة ومتوازية من الهاكرز، وفي الغالب لم تكن هذه الفئات يعرف بعضها البعض، ومع ذلك كانت تجمعها صفات مشتركة، منها ابتداع البرمجيات ومشاركة بعضهم بعضا، إضفاء قيمة عالية من حرية التساؤل، اختراق السرية، التشارك في المعلومات بوصفها إستراتيجية مثالية وعملية، وضع الحق مع القوة، التركيز على الحدس أو التعقل، مقت أو كراهية السلطة، الذكاء الخبيث أو اللعوب، وقد نشأت المجموعات الأولى لهذه الفئات في البيئات الأكاديمية كالحرم الجامعي.

كلمة هاكر Haker تصف في – الأصل– المختص المتمكن الذي لديه قدرات ومهارات خاصة في مجال الحساب وأمن المعلومات، وهذه الكلمة وليدة ثقافة تفرعت من الأوساط الأكاديمية في الستينات عبر السجال الذي كان مستعرا بين نادي تك موديل ريلرود، ومختبر معهد ماساتشوستس

[1] – منير محمد الجنبيهى، ممدوح محمد الجنبيهى، المرجع السابق، ص12

[2] – مصطفى يوسف كافي، جرائم (الفساد –غسل الأموال–السياحة – الإرهاب الالكتروني– المعلوماتية)، مكتبة المجتمع العربي للنشر والتوزيع، عمان 2013، ص151.

[3] - Jan Walden in Chris Reed and John Angle, Computer law Oxford University Press, Fifth edition,2003,p295.

للتكنولوجيا للذكاء الصناعي في معهد ماساتشوسس للتكنولوجيا وهكذا كانت كلمة Hacker تطلق على المبرمج programmer الذكي الذي كان يتحدى الأنظمة المختلفة، و يحاول اقتحامها لاختبار قدراته ومهاراته دون أن تكون في نيته ارتكاب أي جريمة .

ويوضح ريتشارد ستولمان، أحد خبراء المعلوماتية ذلك بقوله، إن القاسم المشترك الأعظم بين الهاكرز هو حبهم الجم للتميز والبرمجة، أنهم يريدون أن يصنعوا برامجهم التي يستخدمونها في أفضل مكانة ممكنة تفوق تصور أي شخص آخر، بحيث تجعلك مندهشا دائما، ومستخدما افعل تفضيل قائلا " انظر ما أروع هذا، إنك لم تكن تعتقد أن هذا يمكن فعله" .

ومن هذا المنظور، ساهم هؤلاء الهاكرز Hackers أو المبرمجون الماهرون في تصميم بنية وتقنيات الشبكات المختلفة.

أصبحت كلمة هاكرHacker تعرف مبرمجا ذا قدرات خاصة يمكن أن يستخدمها في الصواب، كما يمكن أن يستخدمها في الخطأ، بل لقد بالغ بعض من يكتبون في هذا المجال وخاصة عبر وسائل الإعلام المختلفة في الدور السلبي للهاكر، إلى أن أصبحت كلمة هاكر لا تقترن إلا بالشخص المفسد.

ثم ظهرت كلمة الكراكرCracker لتكون بمثابة طوق نجاة للمعنى الحقيقي لكلمة الهاكر، والتي بمقتضاها عادت التفرقة بين الهاكر الصالح والهاكر المفسد، وأصبحت كلمة كراكر تعني من يقوم بأعمال التخريب والاقتحام لأسباب غير إيجابية، وهذا الشخص هو الذي يسمي كراكر أو قرصان، أي هاكر مفسد، وهكذا احتدم الخلاف من جديد بين من يدافعون عن مفهوم كلمة الهاكر ونطاقها، والمعارضين لذلك، إلى أن توافق الرأي على أن المقصود بمصطلح الهاكرhacker الشخص الذي يقوم بعمليات الاختراق والتخريب والتجسس عبر شبكة الإنترنت، وأن يطلق مصطلح كراكرز على المتخصصين في فك أو كسر شفرات البرامج أو كلمات السر، وليس تخريب الشبكات، فهم نوع من الهاكرز المتخصص.[1]

[1]– هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، القاهرة ، جمهورية مصر العربية 2015، ص169الى 175 .

الفرع الأول

التعريف بالمجرم المعلوماتي وسماته

أولا- تعريف المجرم المعلوماتي

من الناحية الجنائية تعني تسمية "المجرم المعلوماتي" ذلك الشخص الذي يمتلك مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسوب الإلكتروني، والقادر على استخدام هذا التكتيك لاختراق الرقم السري لتغيير المعلومات، أو تقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه، أما خبراء الحاسوب والإنترنت، بل وحتى العديد من كتاب القانون في هذا المجال، ذهبوا إلى أن المجرم المعلوماتي يظهر بأحد الصورتين، الأولى هي الـ " Hackers"، وهم من يتحدون إجراءات أمن النظم والشبكات دون أن تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، إنما ينطلقون من دوافع التحدي وإثبات المقدرة، أما الثانية فهي الـ " Crackers"، وهم ممن تعكس اعتداءاتهم ميولا إجرامية خطرة، وهذا المعيار تعتمد عليه التشريعات الأمريكية في التمييز بين النوعين من المجرمين، فيما يميل البعض إلى تسمية المجرم المعلوماتي بـ"المجرم الإلكتروني الرقمي"، ويعرف بأنه "من لديه القدرة على تحويل لغته إلى لغة رقمية، وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني أو الرقمي وملحقاته ووسائل الاتصال الرقمية، وذلك بأداء فعل أو امتناع عنه، مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة مخالفة قواعد الضبط الاجتماعي محليا أو دوليا".

ويمكن القول أن صورة " الإجرام المعلوماتي" أو "المجرم المعلوماتي" باتت غير واضحة بين من يرى أن المجرم المعلوماتي ينتمي إلى "طائفة المجرمين بطبيعتهم" أو ما يسمون ب "المجرمين ذوي الياقات الزرقاء"، وبين من يرى أنهم ينتمون إلى طائفة "الإجرام المكتسب"، أو ما يسمون بـ "المجرمين ذوي الياقات البيضاء " .[1]

[1]- مصطلح المجرمون ذو الياقات البيضاء مصطلح متداول في ميدان علم الاجتماع أول من استخدمه الأستاذ "سندرلاند"، دلالة على أولئك المجرمين الذين لا تظهر عليهم عوامل الإجرام لتمتعهم بمناصب إدارية أو مكانة اجتماعية، حيث يرتكبون هذه الجرائم وهم جالسون في أماكنهم ومكاتبهم الراقية دون أن تتلوث أيديهم فعليا بها، ومن أشهر جرائم ذوي الياقات البيضاء، جريمة غسيل الأموال وجرائم التزوير والاحتيال وتجارة الرقيق الأبيض.

على العموم فإن تسمية "الهاكرز" تعود إلى ستينيات القرن الماضي، حيث أطلقت على الشخص الذي لديه قدرات متميزة في مجال الحاسوب، مستغلا برامجه أقصى استغلال، وفي بداية السبعينيات تمكن شخصان من ولاية كاليفورنيا من فك رموز الشفرة الخاصة بالاتصالات الهاتفية، متمكنا من اختراق نظام الهواتف من دون دفع رسوم "فواتير" المكالمات، وفي مطلع الثمانينات تمت أول عملية اعتقال للهاكرز، حيث قامت الشرطة الفدرالية في مدينة "ملوكي" بضبط مجموعة كبيرة من الهاكرز، قاموا باختراق ستين موقعا في مختلف أنحاء الولايات المتحدة، ثم صدر بعد ذلك قانون "السيطرة على الجريمة المتكاملة"، والذي أتاح للشرطة الأمريكية القبض على منفذي عمليات الاحتيال المتعلقة بالبطاقات الائتمانية و الكمبيوتر، أما في أواخر الثمانيات فقد صدر قانون جديد في الولايات المتحدة عرف ب"قانون الاحتيال بالكمبيوتر وسوء الاستخدام"، والذي زاد من سلطات الشرطة الفيدرالية قياسا بالقانون الأول، غير أنها هجمات الهاكرز باتت تتزايد مع تزايد المواقع الإلكترونية. ففي عام 1999 شهدت الولايات المتحدة خمسة ألاف حالة اختراق، وفي عام 2000 بلغت هذه الحالات سبعة عشر ألف، علما أن هذه الحالات هي المسجلة فقط، أما حصيلة الأضرار الناجمة عن هذه الجرائم والتي أعلنت عنها الولايات المتحدة عام 2000 بلغت (**1.5** تريليون دولار)، جديرا بالذكر أن صورة "الهاكرز" لم تظهر بشكل واضح في مطلع ستينيات القرن الماضي، وذلك بسبب كبر حجم الحاسبات الآلية آنذاك، فضلا، و وجود الحراسات عليها، إضافة إلى وجودها في غرف ذات درجات حرارة معينة، مما يحول بين هؤلاء المجرمين وبين الوصول إليها، ومع ذلك فإن "**درينيسريتشي**" و"**كيننومبسون** " يعدان من أوائل وأشهر الهاكرز آنذاك لتصميمهما عام **1969** برنامج سمي الـ"**يونكس**"، والذي يعد الأسرع في ذلك الوقت، غير أن المدة الزمنية المنحصرة بين **1980 و1989** تعد الفترة الذهبية للهاكرز بسبب تصميم الحاسب الإلكتروني **IBM**، وأصبح الحاسب صغير الحجم وسهل النقل، ويمكن استخدامه في أي مكان أو زمان، ولهذا بدأ الهاكرز في هذه الحقبة بالعمل الحقيقي على الاختراق والتخريب، ولهذا ظهرت مجموعات الهاكرز التي كانت تقوم بتخريب أجهزة المؤسسات التجارية، أما الفترة الممتدة بين الأعوام **1990 و1994** فقد كانت البدايات الأولى لحرب الهاكرز، حيث أنشأ شخص يدعى" **ليكس لوثر**" مجموعة أطلق عليها اسم **LOD** وهي عبارة عن مجموعة من الهاكرز الهواة يقومون باختراق أجهزة الآخرين والقرصنة، وكانت تلك المجموعة هي الأذكى بين مجموعات **الهاكرز**، حتى ظهرت مجموعة أخرى تسمى **MOD** بقيادة شخص يدعى

"**فيبر**"، وهي مجموعة منافسة للمجموعة الأولى، ومع بداية عام **1990** بدأت المجموعتان بحرب كبيرة أطلق عليها "**حرب الهاكرز**"، استمرت ما يقارب الأربع سنوات، وكان كل طرف في هذه الحرب يحاول اختراق أجهزة وأنظمة الطرف الآخر، حتى انتهت بالقبض على"**فيبر**" رئيس مجموعة **MOD** ، ولكن حرب الهاكرز ومجموعاته لم تنته اليوم، بل هي في تزايد مستمر ومن غير اليسير القول بإمكان القضاء عليها وتطويقها.[1]

ثانيا- سمات المجرم المعلوماتي "صفات"

إذ كان المجرم المعلوماتي يرتكب جرائمه وهو يمارس وظيفته في مجال الحاسوب، فلابد وأن يكون إنسانا اجتماعيا، ويقوم بواجباته ويمارس حقوقه الاجتماعية والسياسية دون وجود أي عائق في حياته العملية، وأيضا لا بد أن يكون الشخص الذي يرتكب جريمته المعلوماتية إنسانا محترفا يتمتع بقدر كبير من الذكاء.[2]

1- المجرم المعلوماتي هو إنسان ذكي

يختلف الإجرام معلومات عن الإجرام التقليدي الذي يميل عادة إلى العنف، مع ذلك إذا كانت الجرائم المتصور وقوعها في بيئة النظام المعلوماتي تتفق أحيانا مع الإجرام التقليدي من حيث تطلب العنف في سبيل ارتكابها، إلا أن الإجرام المعلوماتي يتميز بأنه ينشأ من تقنيات التدمير الناعمة، و بمعنى آخر يكفي أن يقوم المجرم المعلوماتي بالتلاعب في بيانات وبرامج الحاسب الآلي لكي يمحو هذه البيانات أو يعطل استخدام البرامج، وليس عليه سوى أن يلجأ إلى زرع الفيروسات في هذه البرامج، أو باستخدام القنابل المنطقية أو الزمنية أو برامج الدودة لكي يشل حركة النظام المعلوماتي، ويجعله غير قادر على القيام بوظائفه الطبيعية، وقد يصل الأمر إلى حد احتراف الإجرام، مما يشكل

[1] – عمار عباس الحسني، المرجع السابق، ص 58 الى 60.

[2]– محمود مدين، الجريمة الالكترونية وتحديات الأمن القومي، المصرية للنشر والتوزيع، القاهرة، جمهورية مصر العربية، الطبعة الثانية 2019، ص60 .

خطرا كبيرا على المجتمع سواء كان فردا أو جماعة منظمة وغير ذلك، وهو ما يعني في النهاية أن المجرم المعلوماتي من النوابغ، أي أنه إنسان ذكي ومحترف.[1]

2- المجرم المعلوماتي مجرم متخصص

ثبتت من عديد القضايا أن عددا من المجرمين لا يرتكبون إلا جرائم الكمبيوتر، أي أنهم يتخصصون في هذا النوع من الجرائم.

3- المجرم المعلوماتي مجرم عائد إلى الإجرام أحيانا

يعود كثيرا من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات، التي أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة في المرة السابقة، ويؤدي ذلك إلى العود إلى الإجرام، وقد ينتهي بهم الأمر في المرة التالية إلى تقديمهم إلى المحاكمة.

4- المجرم المعلوماتي مجرم هاوي في حالات كثيرة

لا يسهل على الشخص الهاوي إلا في حالات قليلة أن يرتكب جرائم بطريق الكومبيوتر، فالأمر يقتضي كثيرا من الدقة والتخصص في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر، كما يحدث في البنوك مثلا، ولا يحول ذلك دون ظهور مجرمين هواة في مجال هذا النوع من الجرائم في حالات عديدة، وهذا ما أثبتته أحداث كثيرة في بلاد متعددة وخاصة في الولايات المتحدة الأمريكية.

5- المجرم المعلوماتي مجرم غير عنيف

ينتمي الإجرام المعلوماتي إلى إجرام الحيلة، فلا يلجأ المجرم المعلوماتي إلى العنف في ارتكاب جرائمه، هذا النوع من الجرائم لا يستلزم مقدار من العنف القيام به.

6- المجرم معلوماتي متكيف اجتماعيا

[1] - محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، جمهورية مصر العربية، 2011، ص78.

لا يضع المجرم المعلوماتي نفسه في حالة عداء سافر مع المجتمع الذي يحيط به، بل إنه إنسان متكيف معه، ذلك أنه أصلا إنسان مرتفع الذكاء، ويساعده ذلك على عملية التكيف، وما الذكاء في رأي كثيرين سوى القدرة على التكيف، ولا يعني ذلك التقليل من شأن المجرم المعلوماتي، بل إن خطورته الإجرامية قد تتزايد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه.[1]

الفرع الثاني

دوافع الإجرام المعلوماتي

تتعدد البواعث والدوافع التي تعطي للمجرم المعلوماتي دافع لارتكاب جرائمه، ولعل أهمها كالآتي:

أولا- تحقيق الكسب المالي "المادي"

تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لارتكاب الجريمة المعلوماتية، وهو من أهم الدوافع وأكثرها تحريكا للمجرم نظرا للربح الكبير الذي يمكن أن يحققه هذا النوع من الأنشطة الإجرامية، وغالبا ما يكون الدافع لارتكاب هذه الجرائم وقوع الجاني بمشاكل مادية تعجزه عن سداد ديونه المستحقة، أو لوجود مشاكل عائلية تعود إلى عدم توفر الأموال، أو الحاجة لها للعب القمار، أو شراء المخدرات، إلى غير ذلك، حيث يسعى الجاني للخروج من هذا المأزق إلى عمليات التلاعب بالأنظمة المعلوماتية للبنوك والمؤسسات المالية، وذلك بواسطة اختراق الأنظمة المعلوماتية لها و اكتشافه لفجواتها الأمنية.

يقوم مرتكبو الجريمة عبر الإنترنت دوي الكفاءة الفنية العالية، بما لديهم من خبرة ومهارة في المجال التكنولوجي، بتوجيه هذه الإمكانيات نحو المؤسسات المالية لمحاولة تحقيق المكاسب المادية، إما بسرقة تلك الأموال أو بتحويلها لحسابه الشخصي داخل البنك، يستطيع المجرمون بمجرد دخولهم إلى أنظمة البنوك معرفة أرقام الحاسب وسرقتها أو تحويلها،[2] حيث أنه في فرنسا سنة 1986 كانت

[1]- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، جمهورية مصر العربية، طبعة 2013، ص15،14.

[2]- محمد ممدوح بذير، المرجع السابق، ص58.57.

مداخيل مرتكبي جريمة الاحتيال في مجال المعالجة الآلية للمعطيات أضعاف المضاعفة من ارتكاب الجرائم التقليدية .[1]

ثانيا– المتعة والتحدي والرغبة في قهر النظام المعلوماتي وإثبات الذات

اختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة، قد يشكل متعة كبيرة لمرتكبها وتسلية تغطي أوقات فراغه، ويوضح هذا الأمر من خلال ما ذكره أحد قراصنة الحاسوب:" كانت القرصنة هي النداء الأخير الذي يبعثه دماغي، فقد كنت أعود إلى البيت بعد يوم آخر في المدرسة، وأدير تشغيل جهاز الحاسوب، وأصبح عضوا في نخبة قراصنة الأنظمة، كان الأمر مختلفا برمته حيث لا وجود لعطف الكبار، وحيث الحكم هو موهبتك فقط، في البدء كنت أسجل اسمي في لوحة النشرات الخاصة، حيث يقوم الأشخاص الآخرون الذين يفعلون مثلي بالتردد على هذا الموقع، ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد، وبعد ذلك أبدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدأ عقلي بقطع مليون ميل في الساعة، وأنسى جسدي تماما بينما أتنقل من جهاز حاسوب إلى آخر محاولا العثور على سبيل للوصول إلى هدفي، لقد كان الأمر يشبه سرعة العمل في متاهة، إلى جانب الاكتشاف الكبير لأعداد ضخمة من المعلومات، وكان يرافق تزايد سرعة الأدرينالين الإثارة المحظورة بفعل شيء غير قانوني، وكل خطوة أخطوها كان يمكن أن تسقطني بيد السلطات، كنت على حافة التكنولوجيا واكتشاف ما وراءها، واكتشاف الكهوف الإلكترونية التي لم يكن من المفترض وجودي بها".

على صعيد آخر، قد يكون الدافع وراء ارتكاب جرائم المعلوماتية، هو الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها، إذ يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم على وسائل التكنولوجيا الحديثة.

فمجرمو المعلوماتية يتملكهم شعور بالبحث عن القوة، ويؤدي ارتكابهم للجرائم بواسطة الوسائل التقنية الحديثة إلى تعويضهم عن الإحساس بالدونية، ففي بعض الأحيان وجد أن مجرد إظهار شعور

[1] - Philippe Rose- La Criminalité informatique Edite par Presses Universitaires de France Paris- 1988 p490.

جنون العظمة هو الدافع لارتكاب فعل الغش المعلوماتي، وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي هو مفتاح لسر كل نظام قد ينتابه إحساس بالإهمال أو بالنقص داخل المنشأة التي يعمل بها، وقد يندفع تحت تأثير رغبة قوية من أجل تأكيد قدراته التقنية لإدارة المنشأة إلى ارتكاب الجريمة المعلوماتية.[1]

ثالثا-الدوافع السياسية

شهدت السنوات المنصرمة وجود حرب سياسية إلكترونية بين العديد من الدول، لاسيما في حالات الحرب، والاختلافات السياسية كاختراق المواقع الإلكترونية للدولة الأخرى، والتجسس عبر الإنترنت الذي بات من أبرز الوسائل المخابراتية، أو تدمير بعض المواقع الرسمية أو إيقافها عن العمل، ناهيك عن بعض المجرمين المعلوماتيين غير المنتمين إلى جهات سياسية أو حكومية، قد يقومون بدوافع سياسية ووطنية باختراق مواقع إلكترونية لبلدان معادية لبلدانهم.[2]

رابعا-الرغبة في التعلم

هناك من يرتكب هذه الجرائم بغية الحصول على الجديد من المعلومات، وسبر أغوار هذه التقنية المتسارعة في النمو والتطور، وهؤلاء الأشخاص يقومون بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم، ويفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت ممكن، حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة، ويكرس البعض منهم كل وقته في تعليم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوبية.[3]

[1]- نهلا عبد القادر المومني، المرجع السابق، ص91،92 .

[2]- عمار عباس الحسني، المرجع السابق، ص 66.

[3]- محمد ممدوح بدير، المرجع السابق، ص 58،ص59.

الفصل الثانـي

مكافحة الجرائم المعلوماتية

في القانون الجزائري

الفصل الثاني

مكافحة الجرائم المعلوماتية في القانون الجزائري

رغبة من المشرع الجزائري تقليص الهوة مابين التشريعات القائمة والموجهة لصد هذه الجريمة المستحدثة من جهة، ومن جهة أخرى محاولة المشرع الجزائري تدارك الفراغ التشريعي القائم في هذا المجال في ظل جريمة حديثة مع قوانين غير مواكبة لهذا النوع من الجرائم وبتزايد تسارعي بوقوع أضرار للأفراد ولمؤسسات الدولة، سهر المشرع متجاوبا مع كل المعطيات المذكورة أنفا على تعديل ترسانته القانونية من جهة، و استحداث قوانين أخرى خاصة في هذا المجال من جهة أخرى .

وعليه سوف نحاول أن نعرج في دراستنا على القوانين العامة التي تخص هذا المجال في المبحث الأول، أما المبحث الثاني سوف نخصصه للقوانين الخاصة التي واجهة هذا النوع من الجرائم .

المبحث الأول

مكافحة الجريمة المعلوماتية بموجب القوانين العامة

لمجابهة الجريمة المعلوماتية حاول المشرع الجزائري إصدار قوانين عامة وخاصة في هذا المجال مستفيدا من تجربته البسيطة السابقة من جهة، ومن إيجابيات انضمامه لاتفاقيات دولية وإقليمية تخص هذا المجال من جهة أخرى .

وعليه قبل تبيان القوانين العامة التي جاء بها المشرع الجزائري سوف نعرج ولو بشكل بسيط على واقع الجريمة المعلوماتية في الجزائر.

المطلب الأول

واقع الجريمة المعلوماتية في الجزائر وسبل مواجهتها بموجب الدستور والقانون المدني الجزائري

قبل التطرق لسبل مجابهة الجريمة المعلوماتية بموجب الدستور الجزائري والقانون المدني الجزائري يتوجب علينا القيام ولو بعجالة لتبيان من جهة بعض الإحصائيات لعالم الهاتف والانترنت في الجزائر لسنة 2022 لكي تكون لنا نظرة ولو تقنية للتطور وللحجم الهائل للجانب التعاملي مع هذه الهالة التكنولوجية، ومن جهة أخرى إيضاح للقارئ الكريم واقع الجريمة المعلوماتية وتطورها في الجزائر.

الفرع الأول

إحصائيات وواقع الجريمة المعلوماتية في الجزائر

سوف نتطرق تحت هذا الفرع لإحصائيات الهاتف والانترنت في الجزائر خلال عام 2022 من جهة، ومن جهة أخرى نتطرق بشكل مبسط لواقع الجريمة المعلوماتية في الجزائر.

أولا–إحصاءات الهاتف والإنترنت في الجزائر خلال عام 2022

أكد مختصون بمكافحة الجريمة السيبرانية، أنه وفقا لآخر تقرير للموقع الإلكتروني "داتاريبورتال" Datareportal"، المختص في الإحصائيات المتعلقة بالإنترنت الهاتف الثابت والنقال في العالم، فإن عدد مستخدمي الإنترنت في الجزائر ارتفع بـ3.6مليون في ظرف سنة منتقلا بذلك إلى 26.35 مليون مستخدم.

وأبرز التقارير أن الجزائر أحصت إلى غاية 31 جانفي2021، حوالي 26.35 مليون مستخدم، ما يمثل زيادة تقدر بـ3.6 مليون مستخدم منذ جانفي 2020.[1]

كما عرف عدد مستخدمي مواقع التواصل الاجتماعي" فيسبوك وتويتر و اليوتيوب انستغرام " ارتفاعاً في الجزائر إلى غاية 31جانفي 2021، حيث تم تسجيل نحو 3 ملايين مستخدم جديد لمواقع التواصل الاجتماعي، أي بزيادة 13.6 بالمائة خلال سنة واحدة، وهو ما جعل العدد الإجمالي لمستخدمي هذه التطبيقات يقفز إلى25مليون أي بنسبة 56.5% من عدد السكان الإجمالي، حيث تستعمل أغلبية مستخدمي مواقع التواصل الاجتماعي، الهاتف الذكي واللوحات الإلكترونية للاتصال بهذه الشبكات.[2]

---

[1] – جريدة الشروق الجزائرية، "2021/11/23" ، نوارة باشوش " الإجرام الالكتروني...أرقام مرعبة "، الموقع www.echoroukonline.com

[2]– جريدة الشروق الجزائرية، "2021/11/23"، نوارة باشوش "الاجرام الالكتروني...أرقام مرعبة "، الموقع www.echoroukonline.com

كشفت سلطة ضبط البريد والاتصال الإلكترونية، عن تسجيل قرابة 47 مليون مشترك في الإنترنت الثابت (خط الاشتراك الرقميADSL– الألياف البصرية FTTH– الجيل الرابعLTE/WIMAX) والنقال (الجيل الثالث والرابع)، خلال الثلاثي الأول من سنة 2022 مقابل 43.5 مليون خلال الفترة نفسها من سنة 2021.

وأوضح هذا التقرير أن عدد المشتركين في الانترنت بلغ 46.9مليون مشترك في الثلاثي الأول من 2022 مقابل 43.5 مليون مشترك خلال نفس الفترة من العام الماضي، بزيادة قدرها 7.93بالمائة.[1]

وبلغ عدد المشتركين في الإنترنت الثابت 4.2 مليون مشترك إلى غاية 31 مارس 2022(3.8 مليون مشترك خلال الفترة ذاتها من 2021)، وسجل الإنترنت النقال أزيد من 42.6 مليون مشترك خلال الثلاثي الأول من العام الجاري(39.6 مليون خلال نفس الفترة من سنة 2021).

وأضاف المصدر ذاته إنه من بين 4.2 مليون مشترك في الإنترنت الثابت فان 2.5 مليون هم مشتركون في الإنترنت عالي التدفق(ADSL)، و1.3 مليون في الشبكة الثابتة(LTE FIXE) و216.900 في الألياف البصرية حتى المنزل(FTTH) ، و443 في تكنولوجية ويماكس.

من العدد الإجمالي لمشتركي الانترنت الثابت (4.2 مليون)، هناك 97.5 % مشتركون مقيمون، مقابل 2.4 بالمائة فقط من المشتركين المهنيين.[2]

[1] – www.entv.dz ، المؤسسة العمومية للتلفزيون الجزائري، إنترنت ثابت ونقال، قرابة 47 مليون مشترك في الثلاثي الأولى من سنة 2022 بالجزائر(سلطة)، نور الدين بن حراث، يوم 12/08/ 2022 تم الدخول يوم 2022/08/15 على الساعة 11:38.

[2] – www.entv.dz ،المؤسسة العمومية للتلفزيون الجزائري، إنترنت ثابت ونقال، قرابة 47 مليون مشترك في الثلاثي الأولى من سنة 2022 بالجزائر(سلطة)، نور الدين بن حراث، يوم 12/08/ 2022 تم الدخول يوم 2022/08/15 على الساعة 11:38.

وفيما يخص المشتركين في مختلف عروض الإنترنت الثابت، فإن 1.3 بالمائة منهم يتوفرون على تدفقات بين 8 ميغا و10 ميغا و82.6 بالمائة بين 10 ميغا و20 ميغا، و15.98 بالمائة بين 20 ميغا و100 ميغا و 0.05 بالمائة أكثر من 100 ميغا.

وفيما يتعلق بحركة البيانات المستهلكة، فقد تضاعف حجمها حيث انتقل من 706 مليون جيغا أوكتي خلال الثلاثي الأول من السنة الماضية إلى 1486 مليون جيغا أوكتي خلال الثلاثي الأول من السنة الجارية، منها 1314 مليون جيغا أوكتي لمشتركيADSL، و76 مليون جيغا أوكتي لمشتركي الجيل الرابع الثابت، و96مليون جيغا أوكتي لمشتركي FTTH.

وقدر النطاق الترددي المستهلك خلال الثلاثي الأول من سنة 2022 بـ 2240جيغابايت/ الثانية أو تيرابايت /الثانية.

وبخصوص سوق الإنترنت النقال، فقد تم تسجيل أكثر من 42.6 مليون مشترك نشط خلال الثلاثي الأول من سنة2022 مقابل 39.6 مليون خلال نفس الفترة من سنة 2021. ومن مجموع 42.6 مليون مشترك في الإنترنت النقال،تم تسجيل 35.7 مليون مشترك في شبكة الجيل الرابع و6.8 مليون في شبكة الجيل الثالث، حسبما أشارت إليه سلطة الضبط، مضيفة أن 97.25 بالمائة من المستعملين سجلوا في اشراكات من نوعDATA و VOIX مقابل سوى 2.75 بالمائة من مجموع المشتركين المسجلين في عروض DATA فقط.

ومن جهة أخرى تم تسجيل حجم إجمالي لاستهلاك داتا يفوق 612.5 مليون جيغا أوكتي خلال الثلاثي الأول من السنة الجارية، مقابل 445.6 مليون جيغا أوكتي السنة الماضية.

ويقدر معدل الحجم الشهري لاستهلاك داتا لكل مشترك به 5 جيغا أوكتي خلال الثلاثي الأول من سنة2022، وقد تم إعداد هذا التقرير على مجموع 44.08 مليون نسمة و7.34 مليون أسرة إلى غاية 31مارس 2022. [1]

[1]– www.entv.dz، المؤسسة العمومية للتلفزيون الجزائري، إنترنت ثابت ونقال، قرابة 47 مليون مشترك في الثلاثي الأولى من سنة 2022 بالجزائر(سلطة)، نور الدين بن حراث، يوم 12/08/ 2022 تم الدخول يوم 2022/08/15 على الساعة 11:38.

ثانيا- واقع الجريمة المعلوماتية في الجزائر (تطور)

من أحد مساوئ تطبيق تكنولوجيا المعلومات والاتصال جرائم الانترنت، وأولى بدايات استعمال الإنترنت في الجزائر التي تعود سنة 1993 عن طريق مركز الأبحاثCERIST، وبعد أن تم تحرير القطاع سنة 1998 ازداد عدد مقدمي خدمة الانترنت ومستعمليها ليشهد تزايد غير مسبوق، وعليه فإن ظاهرة الجريمة المعلوماتية بدأت تظهر في الجزائر سنة 2005 أين سجلت ظاهرة واحدة فقط، ومع تزايد انتشار الانترنت في الجزائر، ارتفع حجم الظاهرة حيث سجل سنة 2009 حوالي 88 حالة شخص متهما تتعلق بالجريمة المعلوماتية.[1]

تمكنت الفرق المتخصصة في مكافحة الجرائم المعلوماتية للأمن الوطني سنة 2014 وبناء على شكاوي، من معالجة**211 قضية** تتعلق بجرائم الإنترنت، قدم من خلالها الدليل المادي عن تورط **205 مشتبها** فيه منهم **28 امرأة** ومن بين هاته القضايا مايلي:

- 75 قضية تمس بأنظمة المعالجة الآلية للمعطيات.
- 59 قضية لها علاقة بالقذف والمساس بحرمة الحياة الخاصة.
- 28 قضية متعلقة بالتهديد بالتشهير.
- 26 قضية انتحال هوية الغير
- 09 قضايا لها علاقة بنشر الصور المخلة بالحياء.
- 03 قضايا متعلقة بالنصب والاحتيال عن طريق الإنترنت.
- 06 قضايا متعلقة بالاهانة والسب عن طريق الإنترنت.

[1]- حنان مسكين، واقع مكافحة الجرائم المعلوماتية واتجاهاتها التشريعية في الجزائر، مقال منشور في المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الرابع، العدد الأول، سنة 2020، ص 618.

– قضيتان متعلقتان بالاستعمال غير الشرعي للبطاقات الإلكترونية.[1]

وسجلت مصالح المديرية العامة للأمن الوطني، المختصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خلال ال08 أشهر الأولى من سنة 2016، 567 قضية تتعلق بجرائم الانترنت، تورط فيها 543شخصا . [2]

نوع الجريمة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	النسبة المئوية للقضايا المسجلة
جرائم المساس بالأشخاص عبر الانترنت	430	289	365	68%
جرائم الاعتداء على سلامة الأنظمة المعلوماتية	57	31	39	55%
جرائم الاحتيال عبر الانترنت	25	17	32	68%
جرائم التحريض والتطرف عبر الانترنت	14	14	31	100%
الجرائم المخلة بالحياء	12	08	22	67%
جرائم بيع السلع المحظورة عبر الانترنت	06	05	15	84%
جرائم مختلفة(نسخ، البرامج دون حق، القرصنة)	23	21	39	92%
المجموع	567	385	543	68%

[1]– www.algriepolice.dz ، المديرية العامة للأمن الوطني، الأمن الوطني يعالج 211 جريمة إلكترونية، الزيارة يوم 02. 08. 2022 على الساعة 21:07.

[2] – www.algeriepolice.dz ،المديرية العامة للأمن الوطني، الزيارة يوم 2022/08/02 على الساعة 20:45 .

وبمناسبة الاحتفال باليوم العالمي للإنترنت الآمن، المصادف لـ 7 فبراير من كل سنة، والذي تحتفل به أكثر من 100 دولة عبر العالم، أعلنت المديرية العامة للأمن الوطني عن تسجيل أكثر من 1055 جريمة إلكترونية خلال سنة 2016 تتعلق بالمساس بالأشخاص عبر الإنترنت، الاعتداء على سلامة الأنظمة المعلوماتية، الاحتيال عبر الإنترنت، وغيرها من أنواع الجرائم الإلكترونية والتي تورط فيها أكثر من 946 شخص.[1]

تورط 1514 شخصا في2026 جريمة سيبريانية على مستوى منطقة وسط البلاد خلال سنة 2020، حسب حصيلة كشف عنها المفتش الجهوي لشرطة منطقة الوسط بن الشيخ فريد زين الدين، وأوضح ذات المسئول خلال عرضه لحصيلة النشاط السنوي لشرطة منطقة الوسط سنة 2020، والتي تضم11 ولاية، أنه تم إحصاء 2026 قضية تخص المساس بأنظمة المعالجة الآلية للمعطيات، تورط فيها 1514 شخص حيث عولج منها 1264 قضية.

وأشار نفس المسئول، إلى تسجيل "**ارتفاع**" في عدد الجرائم السيبرانية في 2020 مقارنة بسنة 2019، وذلك جراء تدابير الحجر الصحي التي فرضتها جائحة كورونا، حيث استغل المتورطون هذه الفترة للقيام بأعمالهم الإجرامية.[2]

حذرت المصالح الأمنية من ارتفاع الجرائم الإلكترونية في الجزائر، حيث أكدت أن الجريمة فعلا انتقلت من العالم الحقيقي إلى الافتراضي العابر للحدود، نظراً لسرعة تنفيذها، إذ سجلت مصالح الدرك والشرطة قرابة 8 ألاف جريمة إلكترونية خلال سنة 2020، حيث سجلت المديرية العامة للأمن الوطني ارتفاع قياسيا، أي من 500 جريمة سنة 2015 إلى5200 قضية خاصة بالجرائم الإلكترونية سنة 2020، في حين سجلت قيادة الدرك الوطني 1362 جريمة سيبرانية تورط فيها 1028 شخص خلال 2020.

---

[1]– المديرية العامة للأمن الوطني تشارك الحملة التوعوية العالمية "كن أنت التغيير"، موقع المديرية العامة للأمن الوطني www.algriepolice.dz ، الزيارة يوم 02. 08. 2022. على الساعة19:44.

[2]– جريدة أخبار اليوم، يومية إخبارية جزائرية " الأربعاء 13يناير2021 "، أرقام مرعبة على تفاقم الإجرام الإلكتروني في الجزائر.

وبينت عملية تحليل المعطيات للجرائم المسجلة، أن القذف والسب عبر الفضاء الافتراضي احتل الصادرة بنسبة تفوق 55 بالمائة، تليها الجرائم ضد الأمن العمومي، ثم الأفعال الماسة بالحياة الخاصة وإفشاء الأسرار، وأخيراً الابتزاز والنصب والاحتيال والاستغلال الجنسي والأفعال المخالفة للآداب العامة وقضايا مشابهة.

ومن جهتها فإن شركة "كاسبرسكي" المختصة في محاربة الجريمة السيبرانية أحبطت 95الف هجمة إلكترونية ضد الجزائر خلال سنة 2020، حيث صنفت سنة 2018 الأولى عربيا والـ14 عالميا من حيث البلدان أكثر تعرضا للهجمات الإلكترونية.[1]

أحصت المديرية العامة للأمن الوطني 5163 قضية في سنة 2020، تمت معالجة منها 4135 قضية، أي بارتفاع معدله 22.63% مقارنة بنسبة 2019.[2]

الفرع الثاني

مواجهة الجريمة المعلوماتية بموجب الدستور والقانون المدني الجزائري

سوف نتناول تحت هذا الفرع مجابهة الجريمة المعلوماتية بموجب الدستور الجزائري من جهة والقانون المدني من جهة ثانية .

أولا– الدستور الجزائري والجريمة المعلوماتية:

حرص التعديل الدستوري لسنة 2008 على حماية الحياة الخاصة للمواطنين، حيث حسب المادة 39 نص بصريح العبارة على أنه لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها

[1] – جريدة الشروق الجزائرية، "2021/11/23"، نوارة باشوش " الاجرام الالكتروني...أرقام مرعبة "، الموقع www.echoroukonline.com

[2]– المديرية العامة للأمن الوطني، منتدى الأمن الوطني، مدير الشرطة القضائية يعرض الحصيلة السنوية لنشاطات مصالح الشرطة القضائية لسنة 2020.
الموقع www.algeriepolice.dz ، الزيارة يوم 2022/08/02 على الساعة 20:23.

القانون، و أكد على أن سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، وهذا حسب القانون رقم08-19 المتضمن تعديل الدستور الجزائري.[1]

وقد كفل التعديل الدستوري لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016 حماية الحقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق، ومن أهم المبادئ الدستورية الهامة :

المادة 38" الحريات الأساسية وحقوق الإنسان والمواطن مضمونة ".

المادة 44" حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن، حقوق المؤلف يحميها القانون.

لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي، الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون .

تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة".

إذ لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، كما أن القانون يحمي سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، أن القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا أمر قضائي.[2]

وكذلك التعديل الدستوري لـ 2016 قام بإثراء الحقوق والحريات، من بينها تقوية حماية الحياة الخاصة، وكتم أسرار الاتصالات في المراسلات، وذلك من خلال المادة 46 بحيث أكد على أنه، لا

---

[1]- القانون رقم 08-19 المؤرخ في 15 نوفمبر 2008، يتضمن التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية، العدد63 .

[2]- بوضياف اسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، سبتمبر 2018، ص361.

- المواد 39،44 من القانون رقم 16-01 المؤرخ في 06 مارس 2016، يتضمن التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية، العدد 14 .

يجوز بأي شكل المساس بهذه الحقوق، دون أمر معلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم .[1]

وأكد على حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، واعتبره حق أساسي يضمنه القانون، ويعاقب على انتهاكه، وهذا ما أكدته وحرصت عليه المادة 47 من تعديل 2020 " لكل شخص الحق في حماية حياته الخاصة وشرفه. لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت .

لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي، يعاقب القانون على انتهاك لهذه الحقوق".[2]

ثانيا – القانون المدني والجريمة المعلوماتية:

نظرا للأهمية الدستورية لحرمة الحياة الخاصة، قد سارع المشرع الجزائري ونص على أنه لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته، أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر في المادة 124 من القانون المدني الجزائري" كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض"، وقد جاء هذا النص عاما وشاملا لأي اعتداء يقع على أي حق من الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة، وقد أورد هذا النص مبدأ مهما هو حق من وقع اعتداء على حياته الخاصة في التعويض عما لحقه من ضرر، فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض، " فالفعل الضار هو أساس المسؤولية "، وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية على الاعتداءات الإلكترونية التي تمس بالحياة الخاصة على شبكة الإنترنت، وهو عنصر متحول وصعب

[1]– القانون رقم 16–01 المؤرخ في 06 مارس 2016، يتضمن التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية، العدد 14 .

[2]– المادة 47 من المرسوم الرئاسي رقم 20–442 المؤرخ في 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية، العدد 82 .

التحديد في الجرائم التي تمس الخصوصية على المواقع الإلكترونية لما تشكله من صعوبات في الإثبات، وفي تحديد هوية المعتدي، وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الإلكتروني الشخصي على أساس الخطأ الواجب الإثبات ، فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة، بل يجب أن يكون ذلك الفعل الإلكتروني قد وصل إلى درجة الخطأ الذي يشكل اعتداء قابل لإثبات وإن وقع على الشبكة.[1]

المطلب الثاني

مكافحة جرائم المعلوماتية بموجب قانون العقوبات وقانون الإجراءات الجزائية الجزائري

سوف نحاول من خلال هذا العنوان تبيان مسايرة المشرع الجزائري للجريمة المعلوماتية من خلال مكافحته لها باستحداث قوانين رادعة وإجراءات مواكبة لهذا النوع من الجرائم من خلال تبيان قانون عقوبات وقانون للإجراءات الجزائية محين كل مرة لمسايرة هذه الظاهرة.

الفرع الأول

مكافحة جرائم المعلوماتية بموجب قانون العقوبات الجزائري

دراستنا لمكافحة جرائم المعلوماتية بموجب قانون العقوبات الجزائري، تكون حسب التطور التاريخي لهذا القانون ومسايرته لهذه الجريمة.

[1]–حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر العاصمة يوم 29–3–2017م، ص 107.
– بوضياف اسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، سبتمبر 2018، ص 361.

أولا- جريمة الإساءة بالوسائل الإلكترونية حسب القانون رقم 01 - 09 المؤرخ في 26 يونيو 2001:[1]

تحت القسم الأول المعنون بالاهانة والتعدي على الموظفين ومؤسسات الدولة، نجد أنه نظرا للتطور في مجال المعلوماتية في الجزائر، وانعكاساتها الإيجابية والسلبية، حاول المشرع الجزائري بأن يساير هذا التطور من خلال بعض التعديلات أهمها، ما جاء في المواد 144 مكرر، و144 مكرر1، 144 مكرر2، 146، وذلك بتبيان بعض الجرائم التي تمس موظفي ومؤسسات الدولة، والعقوبات المسلطة عليها .

1- جريمة الإساءة إلى رئيس الجمهورية[2] :

إن جريمة الإساءة إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سب أو قذف، سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح، أو بأي آلية لبث الصوت أو الصورة، أو بأي وسيلة إلكترونية أو معلوماتية أو إعلامية.

وهنا العقوبة تكون بالحبس من ثلاثة أشهر إلى اثني عشر شهرا، وبغرامة من 50.000دج إلى 250.000دج أو بإحدى هاتين العقوبتين فقط .[3]

2- جرائم الإساءة إلى الرسول "صلى الله عليه وسلم "[4]:

جرائم الإساءة إلى الرسول " صلى الله عليه وسلم"، أو بقية الأنبياء، أو الاستهزاء بالمعلوم من الدين بالضرورة أو بأي شعيرة من شعائر الإسلام، سواء عن طريق الكتابة أو الرسم أو التصريح أو آية وسيلة أخرى.

---

[1] - القانون رقم 01-09 المِؤرخ في 26 يونيو سنة 2001، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر ج ج، العدد 34.

[2] - المادة 144مكرر من القانون رقم 01-09، المصدر نفسه.

[3] - تم مضاعفة العقوبة من 100.000دج إلى 500.000دج حسب القانون رقم 11-14المؤرخ في 2 غشت 2011.

[4] - المادة 144 مكرر2 من القانون 01-09، المصدر نفسه .

وهنا العقوبة تكون بالحبس من ثلاث سنوات إلى خمس سنوات، وبغرامة من 50.000دج إلى 100.000دج، أو بإحدى هاتين العقوبتين فقط .[1]

3- جريمة الإساءة إلى مؤسسات الدولة الأخرى[2]:

كذلك تطبق على الإهانة أو السب أو القذف، الموجه بواسطة الوسائل التي حددتها المادتان 144 مكرر، و144مكرر1 ضد البرلمان أو إحدى غرفتيه، أو ضد المجالس القضائية، أو المحاكم أو ضد الجيش الوطني الشعبي، أو أية هيئة نظامية أو عمومية أخرى، والذي يهمنا هنا هي الوسيلة الإلكترونية أو المعلوماتية.

وهنا تطبق العقوبة المنصوص عليها في المادة 144مكرر .[3]

ثانيا- جريمة المساس بأنظمة المعالجة الآلية للمعطيات حسب "القانون رقم 04-15" المؤرخ في 10نوفمبر2004:[4]

القانون رقم 04-15المؤرخ في 27 رمضان عام 1425، الموافق ل10 نوفمبر سنة 2004 يعدل ويتمم الأمر رقم 66 - 156 المؤرخ في 18 صفر عام 1386هـ الموافق 8 يونيو1966م، والمتضمن قانون العقوبات .

[1] - حسب القانون 06-23 إلى جانب إبقاء عقوبة الحبس كما هي، تم مضاعفة الغرامة من 50.000دج إلى 200.000دج.

[2] - تضاعف العقوبة حسب القانون رقم 11-14 الغرامة من 100.000دج إلى 500.000دج.

[3] - المادة 146 من القانون رقم 01-09، المصدر السابق.

[4] - القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات، ج ر ج ج، العدد 71 .

أضاف المشرع الجزائري قسم سابع مكرر، المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات، من المواد 394 مكرر إلى 394 مكرر7، وكانت هذه قفزة نوعية في مجال مجابهة الجريمة المعلوماتية، بحيث نص على مجموعة من الجرائم والعقوبات المقررة لها فنص على:

1 – جريمة الدخول أو البقاء عن طريق الغش، في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وهنا العقوبة تكون بالحبس من ثلاثة أشهر إلى سنة، وبغرامة من 50.000دج إلى 100.000دج .[1]

2 – جريمة إدخال بطريق الغش معطيات في نظام المعالجة الآلية، أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها .

العقوبة هنا الحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000دج إلى 2.000.000دج . [2]

3– يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج ، كل من يقوم عمدا وعن طريف الغش ب :أ– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية .

ب – حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات.[3]

4– جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضد الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، وهنا تضاعف العقوبات المنصوص عليها في هذا القسم " قسم المساس بأنظمة المعالجة الآلية للمعطيات " .[4]

---

[1] – المادة 394 مكرر من القانون رقم 04–15، المصدر السابق .

[2] – المادة 394 مكرر1 من القانون 04–15، المصدر نفسه .

[3] – المادة 394مكرر2 من القانون 04–15، المصدر نفسه.

[4] – المادة 394مكرر3 من القانون 04–15، المصدر نفسه .

5 – الجرائم المرتكبة من طرف شخص معنوي، والتي تمس أنظمة المعالجة الآلية للمعطيات، والعقوبة هنا تكون بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي .[1]

ثالثا– الجرائم التي نص عليها القانون رقم 06–23 المؤرخ في 20 ديسمبر2006 :[2]

نص هذا القانون على جريمة المساس بحرمة الحياة الخاصة، وكذا جريمة المساس بالمعالجة الآلية للمعطيات.

1–جريمة المساس بحرمة الحياة الخاصة:

تحت "**القسم الخامس**" المعنون بـ"**الاعتداءات على الشرف والاعتداء على الأشخاص وعلى حياتهم الخاصة وإفشاء الأسرار**"، كان للمشرع الجزائري بصمة جديدة وإضافة في المجال تجريم الأفعال الماسة بحرمة الحياة الخاصة بأية تقنية كانت،"**المادة 303 مكرر و303 مكرر1 و303 مكرر 2 و303 مكرر 3** " .

أ – عاقب المشرع الجزائري كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت، سواء بـ:

– التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

–التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات بغرامة من50.000دج إلى 300.000دج.

و يعاقب على الشروع في ارتكاب الجنحة منصوص عليها هنا بالعقوبات ذاتها المقررة للجريمة التامة ، ويضع صفح الضحية حدا للمتابعة الجزائية.[3]

[1] – المادة 394 مكرر4 من القانون 04–15، المصدر السابق .

[2] – القانون رقم 06–23 المؤرخ في 20–12–2006 ، يعدل ويتمم الأمر رقم 66–156 المؤرخ في 8 يونيو 1966، والمتضمن قانون العقوبات، ج ر ج ج، العدد84 .

[3] – المادة 303مكرر من القانون رقم 06–23، المصدر نفسه.

ب– كما أن المشرع الجزائري :

– عاقب كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدام بأية وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بغير إذن صاحبها أو رضاه بنفس العقوبة المنصوص عليها في المادة 303مكرر.

– وأعتبر أن عندما ترتكب الجنحة المنصوص عليها في الفقرة السابقة عن طريق الصحافة، تطبق الأحكام الخاصة المنصوص عليها في القوانين ذات العلاقة لتحديد الأشخاص المسئولين.

وعاقب كذلك على الشروع في ارتكاب هذه الجنحة المتطرق إليها في الفقرة الأولى أي الفقرة قبل السابقة بالعقوبات المقررة للجريمة التامة .

كما بين أن صفح الضحية يضع حد للمتابعة الجزائية.[1]

ج– يجوز للمحكمة أن:

– تحظر على المحكوم عليه من أجل جرائم المنصوص عليها في المادتين 303 مكرر و303 مكرر 1 ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 9مكرر1 " **الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية** "، مدة لا تتجاوز خمس سنوات .

– كما يجوز لها أن تأمر بنشر حكم الإدانة طبقا للكيفيات المبينة في المادة 18 من هذا القانون، " للمحكمة عند الحكم بالإدانة أن تأمر في الحالات التي يحددها القانون بنشر الحكم بأكمله أو مستخرج منه في جريدة أو أكثر يعينها، أو بتعليقه في الأماكن التي يبينها، وذلك كله على نفقة المحكوم عليه، على ألا تتجاوز مصاريف النشر المبلغ الذي يحدده الحكم بالإدانة لهذا الغرض، وألا تتجاوز مدة التغليق شهر واحد ".

ويتعين دائما الحكم بمصادرة الأشياء التي استعملت لارتكاب جريمة.[2]

[1] – المادة 303 مكرر1 من القانون رقم 06–23، المصدر السابق .

[2] – المادة 303 مكرر2 من القانون رقم 06–23، المصدر نفسه.

وبالتالي نستشف من المواد السابقة الذكر خاصة بذكر بأي تقنية كانت، بأن المشرع الجزائري حاول مسايرة التطور التكنولوجي المتسارع، الذي لم يصبح يقتصر فقط على الجرائم المرتبطة بالكمبيوتر، بل امتد إلى وسائل اتصالات أخرى، أهمها وأخطرها استعمال الهواتف الذكية في ظل تزايد التدفق في الإنترنت، وكذا تقنيات أخرى التي أصبحت تشكل خطرا على حرمة الحياة الخاصة.

2- جريمة المساس بالمعالجة الآلية للمعطيات:

بالعودة إلى القسم السابع مكرر المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات من المواد 394 مكرر إلى 394مكرر 7 وفي ظل التعديل الذي جاء به القانون رقم 06-23، وبرجوعنا للمادة

394 مكرر لاحظنا الزيادة في مجال العقوبة بالغرامة من50.000دج إلى 200.000دج بدلا من 50.000دج إلى 100.000دج لمرتكب جريمة الدخول أو البقاء عن طريق الغش، في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك .[1]

نفس الشئ عند رجوعنا للمادة 394مكرر1 لاحظنا كذلك الزيادة في مجال العقوبة بالغرامة من 500.000دج إلى 4.000.000دج بدلا من 500.000دج إلى 2.000.000دج لكل من ارتكب جريمة إدخال بطريق الغش معطيات في نظام المعالجة الآلية، أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها .[2]

كذلك العقوبة التي جاءت بها المادة 394مكرر2، وهنا خاصة الغرامة تغيرت من 1.000.000دج إلى 10.000.000دج بدلا من 1.000.000دج إلى 5.000.000دج [3]، عدا ذلك لم يمس القانون رقم 06-23 المواد الأخرى وهي 394مكرر3، 394مكرر4.

[1] – المادة 394 مكرر من القانون رقم 06-23 ، المصدر السابق .

[2] – المادة 394 مكرر1 من القانون 06-23 ، المصدر نفسه .

[3] – المادة 394 مكرر2 من القانون 06-23 ، المصدر نفسه .

رابعا – جريمة سرقة المال المعلوماتي حسب القانون رقم 09 -01 المؤرخ في 25-02-2009:[1]

نصت المادة 350 مكرر 1 من هذا القانون، على أنه يعاقب بالحبس من سنتين إلى عشر سنوات وبغرامة من 200.000دج إلى 1.000.000دج كل من سرق أو حاول سرقة ممتلك ثقافي منقول محمي أو معرف.[2]

وهنا المشرع الجزائري اعتبر المعلوماتية، مالا يمكن سرقته، وذلك بموجب هذا القانون، وهنا المشرع أحسن ما فعل، نظرا لما يشكله المال المعلوماتي من قيمة مالية مستحدثة.[3]

خامسا- الجرائم الموصوفة بأفعال إرهابية أو تخريبية وجرائم المساس بأنظمة المعالجة الآلية للمعطيات حسب القانون رقم 16 – 02 المؤرخ في 19يونيو2016:[4]

1- الجرائم الموصوفة بأفعال إرهابية أو تخريبية:

تحت القسم الرابع مكرر المعنون "**بالجرائم الموصوفة بأفعال إرهابية أو تخريبية**":

أ – حسب **المادة 87 مكرر 11** من القانون رقم **16-02** المؤرخ في **19-6-2016** يعاقب كل من يستخدم " **تكنولوجيات الإعلام والاتصال** " بالسجن المؤقت من خمس سنوات إلى عشر سنوات وبغرامة من 100.000دج إلى 500,000دج :

---

[1] – القانون رقم 09-01 المؤرخ في 25- 02 - 2009 يعدل ويتمم الأمر رقم 66 - 156 المؤرخ في. 08-06-1966 والمتضمن قانون العقوبات، ج ر ج ج رقم 15، المؤرخة 08- 03- 2009.

[2] – المادة 350 مكرر 1 من القانون رقم 09-01 ،المصدر نفسه .

[3]- يزيد بوحليط، المرجع السابق، ص146.

[4] – القانون رقم 16-02 المؤرخ في 19يونيو2016 المتمم للأمر رقم 66-156، والمتضمن قانون العقوبات، ج ر ج ج رقم 37 المؤرخة في 22 يونيو2016 .

– كل جزائري أو أجنبي مقيم بالجزائر، بطريقة شرعية أو غير شرعية، يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي التدريب عليها.

– كل من يوفر أو يجمع عمدا أموالا بأي وسيلة وبصورة مباشرة أو غير مباشرة، بقصد استخدامها أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو تلقي التدريب عليها.

– كل من قام عمدا بتمويل أو تنظيم سفر أشخاص إلى دولة أخرى، بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تسهيل ذلك السفر.[1]

ب – كما أنه وتحت طائلة هذا القسم، الذي هو القسم الرابع مكرر، قسم الجرائم الموصوفة بأفعال إرهابية أو تخريبية، يعاقب القانون رقم 16– 02 بالسجن المؤقت من خمس سنوات إلى عشر سنوات وبغرامة من 100,000دج إلى 500.000دج، كل من يستخدم " **تكنولوجيات الإعلام والاتصال** " لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها، أو ينشر أفكارها بصورة مباشرة أو غير مباشرة.[2]

2– جرائم المساس بأنظمة المعالجة الآلية للمعطيات :

يعاقب مقدم خدمات [3]"الانترنت" دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 2,000,000دج إلى

[1]– القانون رقم 16–02 ، المصدر السابق.

[2]– المادة 87 مكرر 12 من القانون رقم 16–02 ،المصدر نفسه.

[3] – مقدمو الخدمات :هم أ– أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات، ب– وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال ولمستعمليها.

10,000,000دج، أو بإحدى هاتين العقوبتين، الذي لا يقوم رغم اعذاره من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته [1]، أو صدور أمر أو حكم قضائي يلزمه بذلك :

أ- بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها، أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا.

ب- بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة السابقة، أو لجعل الدخول إليها غير ممكن.[2]

[1]- "نص القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لمكافحتها في الفصل الخامس منه، على إنشاء هيئة وطنية للوقاية من الجرائم المعلوماتية، ويعتبر هذا التشريع نقلة نوعية في النصوص الإجرائية الجزائية، بالنظر إلى نوعية الإجراءات، التي نص عليها كمراقبة الاتصالات السلكية واللاسلكية والمراسلات الالكترونية والاتصالات الهاتفية، وكذا مراقبة كل المعطيات الشخصية على الإنترنت، وهو ما قد يتخذ أحيانا بقصد أو دون قصد كطريق للمساس بحرمة حياة الأشخاص وأمن اتصالاتهم وبياناتهم الشخصية المالية والصحية والاجتماعية، لذلك تم إنشاء الهيئة الوطنية للوقاية من جرائم تكنولوجيا المعلومات ومكافحتها، لتكون هذه الهيئة هي الجهة الرقابية الخاصة بهذا النوع من الجرائم حتى تضمن الحق الدستوري لكل مواطن في حرمة حياته ومراسلاته من المساس بها بداعي مكافحة الجرائم، وبقصد تفعيل نصف المادة 13 من القانون 09-04، فقد صدر في البداية المرسوم الرئاسي15-261 المحدد لتشكيلة وتنظيم وكيفية سير الهيئات الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، غير أنه في 2019 صدور مرسوم رئاسي 19-172 المعدل بالإلغاء لأحكام المرسوم الرئاسي 15- 261 وذلك نتيجة الظروف السياسية والأمنية التي عرفتها البلاد في تلك الفترة مما أفضى إلى ظهور مخاطر فعلية لتعرض الأمن العمومي وكذا المؤسسات الدستورية للخطر، فجاء هذا المرسوم ليغير من الطبيعة القانونية للهيئة، حيث نقل الإشراف عليها من وزارة العدل إلى وزارة الدفاع، مما حول إلى هيئة ذات طابع أمني". مأخود عن بوكحيل حكيمة، سامية بن عديد، الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الاتصال ودورها في تفتيش نظم المعلوماتية، مجلة الدراسات القانونية المقارنة، المجلد 07/العدد01،2021،ص1544.

[2] – المادة 394مكرر8 من القانون رقم 16-02، المصدر السابق .

سادسا- جرائم الغش في الامتحانات الرسمية حسب القانون رقم 20 -06 المؤرخ في 28 -04- 2020:[1]

في إطار تنامي ظاهرة الغش في الامتحانات الرسمية، خاصة في الامتحانات النهائية للتعليم الابتدائي والمتوسط والثانوي، وخاصة باستعمال التقنيات الحديثة، عمد الفصل التاسع، تحت عنوان المساس بنزاهة الامتحانات والمسابقات، المدرج تحت الباب الأول، الجنايات والجنح ضد الشيء العمومي، من الكتاب الثالث الجنايات والجنح وعقوباتها، من الجزء الثاني التجريم، على مجابهة هذه الظاهرة من المواد 253 مكرر 06 إلى المادة 253 مكرر 12.

1 - تكون العقوبة الحبس من خمس سنوات إلى عشر سنوات، والغرامة من 500.000دج إلى 1.000.000دج. إذا ارتكبت الأفعال المنصوص عليها في المادة 253 مكرر 6، وهي " كل من قام قبل أو أثناء الامتحانات أو المسابقات بنشر أو تسريب مواضيع و/ أو أجوبة الامتحانات النهائية للتعليم الابتدائي أو المتوسط أو الثانوي أو مسابقات التعليم العالي أو التعليم والتكوين المهنيين، والمسابقات المهنية الوطنية"، وذلك من قبل الأشخاص المكلفين بتحضير أو تنظيم أو تأطير الامتحانات و المسابقات أو الإشراف عليها، وكذا من قبل مجموعة أشخاص، وذلك باستعمال منظومة للمعالجة الآلية المعطيات، وكذا باستعمال وسائل الاتصال عن بعد.[2]

2- يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجرائم المنصوص عليها في هذا الفصل " المساس بنزاهة الامتحانات والمسابقات "، والأموال المتحصلة منها، وإغلاق الموقع الإلكتروني أو الحساب الإلكتروني الذي ارتكبت بواسطتة الجريمة، أو جعل الدخول إليه غير ممكن،

[1] - القانون رقم 20-06 المؤرخ في 28-04-2020 يعدل ويتمم الأمر رقم 66- 156 المؤرخ في 8 يونيو1966 والمتضمن قانون العقوبات، ج ر ج ج العدد 25 الصادر في 29 أبريل 2020 .

[2]- المادة 253 مكرر7 من القانون رقم 20-06 المؤرخ في 28-04-2020 يعدل ويتمم الأمر رقم 66- 156 المؤرخ في 8 يونيو1966 والمتضمن قانون العقوبات، ج ر ج ج العدد 25 الصادر في 29 أبريل 2020 .

وإغلاق محل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه دون الإخلال بحقوق الغير حسن النية.[1]

سابعا- جرائم الإهانة والتعدي على المؤسسات الصحية ومستخدميها حسب الأمر رقم 20-01:[2]

في إطار تنامي ظاهرة الإهانة والتعدي على المؤسسات الصحية ومستخدميها، هذا في الحقيقة هو من واقعنا المرير، كان لا بد من وضع قوانين رادعة لهذه الظاهرة المشينة، التي أثرت على مردود هذه المؤسسات ومستخدميها، خاصة من أطباء وممرضين فجاء هذا الأمر رقم 20-01 الذي فعلا وضع الدواء على الداء نظريا نوعا ما، لأن الواقع عكس ذلك، لازلنا نشاهد هذا النوع من الجرائم .

الإهانة والتعدي على المؤسسات الصحية ومستخدميها جاء ضمن القسم الأول مكرر من الفصل الخامس، الجنايات والجنح الذي يرتكبها الأشخاص ضد النظام العمومي، تحت الباب الأول، الجنايات والجناح ضد الشيء العمومي، تحت الكتاب الثالث، الجنايات والجنح وعقوباتها، من الجزاء الثاني، التجريم، حيث تصدت لهذه الظاهرة عدة مواد، خاصة المواد من 149إلى 149مكرر 14 .

1- عاقبت المادة 149 مكرر3 بالحبس من سنتين إلى خمس سنوات، وبغرامة من 200.000دج إلى 500.000دج كل من يقوم بتسجيل مكالمات أو أحاديث أو التقاط أو نشر صور أو فيديوهات أو أخبار أو معلومات على موقع أو شبكة إلكترونية، أو في مواقع التواصل الاجتماعي، أو بأي وسيلة أخرى، قصد الإضرار أو المساس بالمهنية أو بالسلامة المعنوية لأحد مهنيي الصحة، أو أحد موظفي أو مستخدمي الهياكل والمؤسسات الصحية أثناء تأدية مهامهم أو بمناسبتها .

كما أن هذه المادة طبقت نفس العقوبة، إذا ارتكبت الأفعال السابقة، وذلك إضرارا بالمرضى وأسرهم، أو بالهياكل والمؤسسات الصحية، ولم تنسى حتى حرمة الموتى.

---

[1]- المادة 253 مكرر11، المصدر السابق .

[2]- الأمر رقم 20-01 مؤرخ في 30-7-2020، يعدل ويتمم الأمر رقم 66 - 156 والمتضمن قانون العقوبات، ج ر ج ج، العدد 44، الصادر في 30-7-2020.

وتحت سياق نفس المادة، تمت مضاعفة العقوبات المنصوص عليها في نفس المادة، إذا تم تحوير الصور أو الفيديوهات أو الأخبار أو المعلومات بشكل مغرض، أو تم التقاطها خلسة، أو في الأماكن غير المفتوحة للجمهور بالهيكل أو المؤسسة الصحية، أو إذا تم إخراجها عن سياقها.[1]

2– الأمر 20–01 شدد من العقوبة من خلال المادة 149 مكرر 5 بالحبس 5 سنوات إلى 15 سنة ، والغرامة من 500.000دج إلى 1.500.000دج، إذا ارتكبت الأفعال المنصوص عليها، خاصة في المادة 149 مكرر 3 خلال فترات الحجر الصحي، أو خلال وقوع كارثة طبيعية أو بيولوجية أو تكنولوجية أو غيرها من الكوارث، وكذا قصد النيل من مصداقية الهياكل و المؤسسات الصحية ومهنيتها.[2]

3 – يمكن حرمان المحكوم عليه بسبب ارتكاب جريمة من الجرائم المنصوص عليها في هذا القسم، أي القسم الأول مكرر "الإهانة والتعدي على المؤسسات الصحية ومستخدميها "، من استخدام أي شبكة إلكترونية أو منظومة معلوماتية، أو أي وسيلة من وسائل تكنولوجيات الإعلام والاتصال، لمدة أقصاها ثلاث سنوات، تسري ابتداء من يوم انقضاء العقوبة الأصلية أو الإفراج عن المحكوم عليه، أو من تاريخ صيرورة الحكم نهائيا بالنسبة للمحكوم عليه غير المحبوس.[3]

كما يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وبإغلاق الموقع الإلكتروني أو الحساب الإلكتروني الذي ارتكبت بواسطته الجريمة أو جعل الدخول إليه غير ممكن، وإغلاق محل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه.[4]

---

[1]– المادة 149 مكرر3، من الأمر رقم 20–01 مؤرخ في 30–7–2020، يعدل ويتمم الأمر رقم 66 – 156 والمتضمن قانون العقوبات، ج ر ج ج، العدد 44، الصادر في 30–7–2020.

[2]– المادة 149 مكرر 5 من الأمر رقم 20–01، المصدر نفسه.

[3]– المادة 149 مكرر8 من الأمر رقم 20–01، المصدر نفسه .

[4]– المادة 149 مكرر 9 من الأمر رقم 20–01، المصدر نفسه .

الفرع الثاني

مكافحة الجريمة المعلوماتية بموجب قانون الإجراءات الجزائية

دراستنا لمكافحة جرائم المعلوماتية بموجب قانون الإجراءات الجزائية، تكون حسب التطور التاريخي لهذا القانون ومسايرته لهذه الجريمة.

أولا- الاختصاص القضائي في الجرائم المعلوماتية حسب القانون رقم 04-14المؤرخ في 10 نوفمبر 2004:[1]

1- الاختصاص المحلي لقاضي التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

حسب الفصل الثالث المعنون بـ " في قاضي التحقيق"، نجد أن المادة 40 من القانون رقم 04 -14 المؤرخ في 10-11-2004، حددت الاختصاص المحلي لقاضي التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهذا يعد تطورا يحاول فيه المشرع الجزائري أن يتماشى مع الواقع الإلكتروني.

وهذا التعديل حسب المادة 40 من قانون الإجراءات الجزائية جاء كما يلي:

يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة، أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها، أو بمحل القبض على أحد هؤلاء الأشخاص، حتى ولو كان هذا القبض قد حصل لسبب آخر.

[1]- القانون رقم 04-14 مؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966، والمتضمن قانون الإجراءات الجزائية، ج ر ج ج العدد71 .

يجوز تمديد الاختصاص المحلي لقاضي التحقيق، إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم في **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.**[1]

2- الاختصاص المحلي لوكيل الجمهورية في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات :

نص المشرع الجزائري على **تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم المعلوماتية** في المادة 37 من قانون الإجراءات الجزائية، التي نصت على أنه "يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، و بمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها، أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص، حتى و لو حصل هذا القبض لسبب آخر.

يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى ، عن طريق التنظيم في **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.**[2]

3- الاختصاص المحلي للمحكمة في الجرائم المعلوماتية:

المشرع الجزائري نص في هذا التعديل، إلى **تمديد الاختصاص المحلي للمحكمة في الجرائم المعلوماتية،** وهذه حسب الفقرة الخامسة من المادة 329 حيث نص على أنه "يجوز تمديد الاختصاص المحلي للمحكمة، إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.**[3]

4 - كما نصت المادة 40 مكرر على أنه تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية، التي تم توسيع اختصاصها المحلي طبقا للمواد 37 و40 و329 من هذا القانون، مع مراعاة أحكام المواد من 40 مكرر 1 إلى 40 مكرر 5 .

[1]- المادة 40 من القانون رقم 04-14، المصدر السابق .

[2]- المادة 37 من القانون رقم 04-14، المصدر نفسه .

[3]- المادة 329 من القانون رقم 04-14، المصدر نفسه.

فحسب المادة 40 مكرر 1، يخبر ضباط الشرطة القضائية فورا وكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة، ويبلغونه بأصل وبنسختين من إجراءات التحقيق، ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة.

وحسب المادة 40 مكرر 2 يطالب النائب العام بالإجراءات فورا، إذا اعتبر أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة 40 مكرر من القانون.

وحسب المادة 40 مكرر 3، يجوز للنائب العام لدى المجلس القضائي التابعة له الجهة القضائية المختصة، أن يطالب بالإجراءات في جميع مراحل الدعوى.

و في حالة فتح تحقيق قضائي، يصدر قاضي التحقيق أمرا بالتخلي عن الإجراءات لفائدة قاضي التحقيق لدى المحكمة المختصة المذكورة في المادة 40 مكرر من هذا القانون.

كما يحتفظ الأمر بالقبض، أو الأمر بالحبس المؤقت، الذي صدر ضد المتهم حسب المادة 40 مكرر 4 بقوته التنفيذية، إلى أن تفصل فيه المحكمة المختصة المذكورة في المادة 40 مكرر، مع مراعاة أحكام المواد 123 وما يليها من هذا القانون.

كما يجوز لقاضي التحقيق تلقائيا، أو بناء على طلب النيابة العامة، و طوال مدة الإجراءات حسب المادة 40 مكرر 5 أن يأمر باتخاذ كل إجراء تحفظي، أو تدبير أمن زيادة على حجز الأموال المتحصل عليها من الجريمة، أو التي استعملت في ارتكابها.[1]

ثانيا- تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق حسب المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر2006:[2]

تطبيقا لأحكام المواد 37 و40 و329 من الأمر رقم 66- 155 المؤرخ في 18صفر عام 1386هـ، الموافق ل8 يونيو سنة 1966، والمتضمن قانون الإجراءات الجزائية، يهدف هذا المرسوم

[1] - المادة 40 مكرر 5 من القانون 04-14، المصدر السابق .

[2] - المرسوم التنفيذي رقم 06- 348 المؤرخ في 12 رمضان1427هـ، الموافق ل 5أكتوبر2006م، يتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية وقضاة التحقيق، ج ر ج ج العدد63 .

إلى تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دوائر اختصاص محاكم أخرى، كما هو محدد في المواد 2 و 3 و4 و 5 من هذا المرسوم، في الجرائم المتعلقة بالمتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية، **والجرائم الماسة بأنظمة المعالجة الآليات للمعطيات**، و جرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.[1]

1 – يمتد الاختصاص المحلي لمحكمة سيدي أمحمد ووكيل الجمهورية و قاضي التحقيق بها إلى محاكم المجالس القضائية لـ : الجزائر و الشلف و الاغواط والبليدة و البويرة و تيزي وزو والجلفة والمدية والمسيلة و بومرداس و تيبازة وعين الدفلى.[2]

2 – يمتد الاختصاص المحلي لمحكمة قسنطينة و وكيل الجمهورية وقاضي التحقيق بها، إلى محاكم المجالس القضائية لـ : قسنطينة وأم البواقي وباتنة وبجاية وبسكرة وتبسة وجيجل وسطيف وسكيكدة وعنابة وقالمة وبرج بوعريريج والطارف والوادي وخنشلة وسوق أهراس وميلة.[3]

3 – يمتد الاختصاص المحلي لمحكمة ورقلة ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية لـ : ورقلة و أدرار و تامنغاست و إيليزي و تندوف و غرداية.[4]

4 – يمتد الاختصاص المحلي لمحكمة وهران و وكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية لـ :

وهران وبشار وتلمسان وتيارت وسعيدة وسيدي بلعباس ومستغانم ومعسكر والبيض وتيسمسيلت والنعامة وعين تموشنت و غليزان.[5]

[1] – المادة الأولى من المرسوم التنفيذي رقم 06– 348، المصدر السابق.

[2] – المادة الثانية من المرسوم التنفيذي رقم 06–348، المصدر نفسه .

[3] – المادة الثالثة من المرسوم التنفيذي رقم 06–348، المصدر نفسه .

[4] – المادة الرابعة من المرسوم التنفيذي رقم 06–348، المصدر نفسه .

[5] – المادة الخامسة من المرسوم التنفيذي رقم 06–348، المصدر نفسه .

ومن الملاحظ أن تمديد الاختصاص المحلي لقاضي التحقيق مشمولا، كما هو الشأن بالنسبة للنيابة بأحكام المرسوم التنفيذي رقم 06-348 المؤرخ في نص 05-10- 2006 وقد حددت المادة الأولى من المرسوم المشار له، مجال الاختصاص المحلي الممدد في نطاق الأقطاب القضائية والمحددة في المواد 2،3،4،5 من نفس المرسوم في الجرائم المتعلقة بالمتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف ، وما يهمنا في الموضوع ما هو متعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

ثالثا-التدابير الإجرائية المستحدثة التي تتعلق بالتحقيق في الجرائم الإلكترونية حسب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006:[2]

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الإلكتروني، لا تكون فقط بإرسال قواعد قانونية موضوعية ذات طبيعية ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها أن تفادي وقوع الجريمة الإلكترونية، أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما استدراكه المشرع بتضمين القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية، تدابير إجرائية مستحدثة، تتعلق بالتحقيق في الجرائم الإلكترونية، تتمثل في مراقبة الاتصالات الإلكترونية، تسجيلها والتسرب .[3]

وقبل التطرق لتلك الإجراءات نتطرق لبعض الإجراءات كالتفتيش الذي أحاطه المشرع بقواعد صارمة، وكذا التوقيف للنظر.

---

[1]- زيبحة زيدان، المرجع السابق، ص 115.

[2]- القانون رقم 06 - 22 المؤرخ في 20 ديسمبر2006 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386هـ الموافق في 8 يونيو1966م، يتضمن قانون الإجراءات الجزائية المعدل والمتمم، ج ر ج ج رقم 84 مؤرخة في 24 - 12 - 2006، ص 14.

[3]- بوضياف إسمهان، المرجع السابق، ص364.

1-التفتيش:

نظرا لخطورة التفتيش باعتباره إجراء يمس بالدرجة الأولى بحقوق الأفراد وحرياتهم، وجب على المشرع إحاطته بضوابط تشكل في حقيقتها ضمانات لتكريس التوازن بين حماية المجتمع من جهة وعدم المساس بحقوق الأفراد وحرياتهم من جهة أخرى، من بينها ضرورة الحصول على إذن مكتوب بالتفتيش استنادا لنصوص المواد 44،64،68 من قانون الإجراءات الجزائية، وضرورة حضور صاحب المسكن عملية التفتيش، وإلزامية حصول التفتيش في التوقيت المحدد قانونا، إلا أن خصوصية الجريمة المعلوماتية فرضت على المشرع أن يورد استثناءات على هذه الضوابط، من بينها التعديل الذي ألحقه على قانون الإجراءات الجزائية بالقانون 06-22 والذي استثنى بموجبه حضور المشتبه فيه أو الشاهدين عملية التفتيش، بالإضافة إلى الاستثناء الوارد بالفقرة الثالثة من المادة 47 من قانون الإجراءات الجزائية والمتعلق بجواز إجراء التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل إذا تعلق الأمر بنوع معين من الجرائم من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1]، ويجوز لقاضي التحقيق القيام بعملية التفتيش أو ضبط الأشياء ليلا ونهارا وفي أي مكان على مستوى التراب الوطني، إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[2]

2-التوقيف للنظر:

يعرف التوقيف للنظر بأنه إجراء بوليسي، يأمر به ضباط الشرطة القضائية بوضع شخص يريد التحفظ عليه فيوقفه في مركز الشرطة أو الدرك الوطني لمدة 48 ساعة كلما دعته مقتضيات التحقيق ذلك.[3]

---

[1] – حليم رامي، إجراءات استخلاص الدليل في الجرائم المعلوماتية، دفاتر البحوث العلمية، المركز الجامعي مرسلي عبد الله، تيبازة، الجزائر، المجاد 9، العدد1، السنة2021، ص232،231.

[2]– علي شملال، المستحدث في قانون الإجراءات الجزائي الجزائري، الكتاب الثاني التحقيق والمحاكمة، طباعات المسارات العلمية، الدويرة، الجزائر، الطبعة 2022، ص68.

[3]– عبد الله اوهايبية، شرح قانون الإجراءات الجزائية الجزائري " التحري والتحقيق"، دار هومه، الجزائر2005، ص239.

إذا رأى ضباط الشرطة القضائية لمقتضيات التحقيق، أن يوقف للنظر شخصا أو أكثر مما أشير إليهم في المادة 50[1]، فعليه أن يطلع فورا وكيل الجمهورية بذلك ويقدم له تقريرا عن دواعي التوقف للنظر، ولا يجوز أن تتجاوز مدة التوقيف للنظر ثمان وأربعين ساعة، ويمكن تمديد أجال التوقيف للنظر بإذن مكتوب من وكيل الجمهورية المختص، مرة واحدة عندما يتعلق الأمر بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات .[2]

3- اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

يقصد باعتراض المراسلات التتبع السري والمتواصل للمشتبه به قبل وبعد ارتكابه للجريمة ثم القبض عليه متلبسا بها، ويعرف على أنه إجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة، ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث، وهي تعتبر أيضا وسيلة هامة من الوسائل الحديثة للبحث والتحري تستخدمها الضبطية القضائية واجهة الإجرام الخطير وتتم عبر وسائل الاتصال السلكية واللاسلكية.[3]

ونظرا للتطور الذي عرفه مجال الاتصال فان نص المادة 65 مكرر5 جاء موسعا، أي لم يقتصر الاعتراض على المكالمات الهاتفية بل وسعه لمختلف أنواع الاتصال السلكية واللاسلكية.[4]

وإلى جانب المشرع الجزائري نجد كذلك المشرع الفرنسي قد كرس هذه التقنية في المادة 100 من قانون الإجراءات الجزائية التي تنص على أنه" في المواد الجنائية والمواد الجنحية إذا كانت العقوبة

---

[1] – يجوز لضباط الشرطة منع أي شخص من مبارحة مكان الجريمة ريثما ينتهي من إجراء تحرياته، وعلى كل شخص يبدو له ضروريا في مجرى استدلالاته القضائية التعرف على هويته أو التحقق من شخصيته أن يمتثل له في كل ما يطلبه من إجراءات في هذا الخصوص .

[2] – المادة 51 فقرة 6 من القانون رقم 06-22، المصدر السابق.

[3] – محمد علي سويلم، المرجع السابق، ص735.

[4] – فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، العدد 33، جوان 2010، ص237.

تفوق سنتين يمكن لقاضي التحقيق إذا دعت مقتضيات البحث والتحري أن يأمر باعتراض وتسجيل ونقل المراسلات التي تتمعن طريق وسائل الاتصال".[1]

ولقد أشار المشرع الجزائري إلى ظروف و كيفية اللجوء إلى هذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية على النحو:" إذا اقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... يجوز لوكيل الجمهورية المختص أن يأذن:

– باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

– وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث و تسجيل الكلام المتفوه به ، بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص، أو عدة أشخاص يتواجدون في مكان خاص."

فبموجب هذه المادة فإن المشرع الجزائري يسمح لسلطات التحقيق والاستدلال إذا استدعت ضرورة التحري في الجريمة المتلبس بها، أو التحقيق في الجريمة الإلكترونية، اللجوء إلى إجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والأصوات والتقاط الصور، و الاستعانة بكل الترتيبات التقنية اللازمة لذلك، من أجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها، دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة.

ومع هذا فإن المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء ، بل أحاطه بمجموعة من الضمانات القانونية، التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد.[2]

[1] – سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر باتنة، 2012–2013، ص178.

[2]– بوضياف إسمهان، المرجع السابق، ص363،364.

4- التسرب :

التسرب هو قيام ضباط 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، ومن أجل تحقيق هذا الغرض يسمح لضابط أو عون الشرطة القضائية أن يستعمل هوية مستعارة .[1]

إذا اقتضت ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب.[2]

رابعا- ضمان زيارة المحامي بعد انقضاء نصف المدة القصوى للشخص الموقوف للنظر حسب الأمر رقم 15-02 المؤرخ في 23يوليو سنة2015:[3]

حسب المادة 51 من هذا الأمر، إذا رأى ضابط الشرطة القضائية لمقتضيات التحقيق، أن يوقف للنظر شخصا أو أكثر، توجد ضدهم دلائل تحمل على الاشتباه في ارتكابهم جناية أو جنحة يقرر لها القانون عقوبة سالبة للحرية، فعليه أن يبلغ الشخص المعني بهذا القرار، ويطلع فورا وكيل الجمهورية بذلك، ويقدم له تقريرا عند دواعي التوقيف للنظر، ولا يجوز أن تتجاوز مدة التوقيف للنظر 48 ساعة، ويمكن تمديد أجال التوقيف للنظر، بإذن مكتوب من وكيل الجمهورية المختص مرة واحدة، عندما يتعلق الأمر بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات.[4]

[1] - علي شملال، المرجع السابق، ص 81.

[2] - المادة 65 مكرر 11 من القانون 06-22، المصدر السابق.

[3] - الأمر رقم 15-02 المؤرخ في 23 يوليو سنة2015، يعدل ويتمم الأمر رقم 66-15المؤرخ في 18 صفر عام 1368 الموافق في 8 يونيو سنة 1966، والمتضمن قانون الإجراءات الجزائية، ج ر ج ج، العدد 40.

[4] - المادة 51 من الأمر رقم 15-02، المصدر نفسه.

ويمكن للشخص الموقوف أن يتلقى زيارة محاميه، بعد **انقضاء نصف المدة القصوى**، أي بعد 48 ساعة من توقيفه.[1]

ويجوز لوكيل الجمهورية إذا اقتضى الأمر، سواء من تلقاء نفسه أو بناء على طلب أفراد عائلته الشخص الموقف للنظر أو محاميه، أن يندب طبيبا لفحصه في أي لحظة في آجال التوقيف.[2]

خامسا- الأمر رقم 20-04 المؤرخ في 30غشت سنة 2020:[3]

سوف نتطرق لإجراءات التحقيق بالنسبة للجرائم المعلوماتية حسب الأمر رقم 20-04 من جهة، ومن جهة أخرى نتطرق باختصار للقطب الجزائي الوطني المتخصص لمكافحة الجريمة الاقتصادية والمالية .

1- إجراءات التحقيق بالنسبة للجرائم المعلوماتية حسب الأمر رقم 20-04 :

تحت الفصل الثالث " في قاضي التحقيق " من الباب الأول "في البحث والتحري عن الجرائم " من الكتاب الأول " في مباشرة الدعوى العمومية وإجراء التحقيق"، نجد أن المادة 40 مكرر1 من الأمر رقم 20-04 اعتبرت أنه عندما يتعلق الأمر بإحدى الجرائم المنصوص عليها في الفقرة 2 من المادة 37، والمقصود بها جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف، والتي تهمنا هنا خاصة **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**، يخبر ضباط الشرطة القضائية فورا، وكيل الجمهورية لدى المحكمة المختصة إقليميا، ويرسلون له الأصل ونسختين من إجراءات التحقيق، ويحيل هذا الأخير فورا النسخة الثانية إلى وكيل الجمهورية لدى الجهة القضائية ذات الاختصاص الإقليمي الموسع .[4]

---

[1] – المادة 51مكرر 1 فقرة 4 من الأمر رقم 15-02 ، المصدر السابق .

[2] – المادة 52 من الأمر رقم 15-02 ، المصدر نفسه .

[3] – الأمر رقم 20-04 مؤرخ في 30 غشت سنة 2020 يعدل ويتمم الأمر رقم 66- 155 المؤرخ في 18 صفر عام 1386 الموافق 8يونيو سنة 1966م ، والمتضمن قانون الإجراءات الجزائية، ج ر ج ج العدد 51 سنة 2020.

[4]– المادة 40 مكرر1 من الأمر رقم 20-04 ، المصدر نفسه.

كما يطالب وكيل الجمهورية لدى الجهة القضائية ذات الاختصاص الإقليمي الموسع، بعد أخذ رأي النائب العام بالإجراءات فورا، إذا اعتبر أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة 40 مكرر من هذا القانون، وهنا يقصد ما تطرق له القانون رقم 04-14 بتطبيق قواعد هذا القانون المتعلقة بالدعوة العمومية والتحقيق والمحاكمة أمام الجهات التي تم توسيع اختصاصها المحلي طبقا للمواد 37 و40 و329 المذكورين سابقا من هذا القانون، وما جاء به المرسوم التنفيذي رقم 06-348 المذكور سابقا .

وفي هذه الحالة يتلقى ضباط الشرطة القضائية العاملون بدائرة اختصاص هذه المحكمة، التعليمات مباشرة من وكيل الجمهورية لدى هذه الجهة القضائية.[1]

يمكن وكيل الجمهورية لدى المحكمة ذات الاختصاص الإقليمي الموسع، بعد أخذ رأي النائب العام، أن يطالب بملف الإجراءات خلال جميع مراحل الدعوى .

وفي حالة فتح تحقيق قضائي، يصدر قاضي التحقيق أمرا بالتخلي عن الإجراءات لفائدة قاضي التحقيق لدى المحكمة المختصة المذكورة في المادة 40 مكرر من هذا القانون، وفي هذه الحالة يتلقى ضابط الشرطة القضائية العاملون بدائرة اختصاص هذه المحكمة، التعليمات مباشرة من قاضي التحقيق بهذه الجهات القضائية.[2]

2- القطب الجزائي الوطني المتخصص لمكافحة الجريمة الاقتصادية والمالية:

من خلال الباب الرابع" القطب الجزائي الاقتصادي والمالي"، حسب المادة 211 مكرر التي نصت على أنه ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر قطب جزائي وطني متخصص لمكافحة الجريمة الاقتصادية والمالية.[3]

---

[1]- المادة 40 مكرر2 من الأمر رقم 20-04 ، المصدر السابق.

[2]- المادة 40 مكرر 3 من الأمر رقم 20-04، المصدر نفسه .

[3] - المادة 211مكرر من الأمر رقم 20-04، المصدر تفسه.

ويمارس وكيل الجمهورية لدى القطب الجزائي الاقتصادي والمالي، وكذا قاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل الإقليم الوطني.[1]

القطب الجزائي الاقتصادي والمالي، يتولى البحث والتحري والمتابعة والتحقيق والحكم في الجرائم الاقتصادية والمالية الأكثر تعقيدا، وفي الجرائم مرتبطة بها .

ويقصد بالجريمة الاقتصادية والمالية الأكثر تعقيدا، الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين، أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة، أو جسامة الأضرار المترتبة عليها، أو لصبغتها المنظمة أو العابرة للحدود الوطنية، أو لاستعمال تكنولوجيات الإعلام والاتصال في ارتكابها، تتطلب اللجوء إلى وسائل تحر خاصة، أو خبرة فنية متخصصة أو تعاون قضائي دولي.[2]

وهنا بالإضافة إلى خطورة وضخامة هذا الجرائم، وخاصة ما نصت عليه المادة 211 مكرر 2، وخاصة منها جرائم الفساد، وجرائم الصرف وحركة رؤوس الأموال من وإلى الخارج، جرائم التهريب وغيرها، والذي يهمنا هو استعمال تكنولوجيات الإعلام والاتصال في ارتكابها، مما تطلب لمواجهتها اللجوء إلى وسائل خاصة في التحري، أو خبرة فنية متخصصة، أو تعاون قضائي دولي.

سادسا- استحداث قطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب الأمر 21-11:

جاء الأمر رقم 21-11[3] المتمم والمعدل لقانون الإجراءات الجزائية الجزائري والقاضي باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال .

[1] – المادة 211 مكرر1 من الأمر رقم 20-04، المصدر السابق .

[2] – المادة 211 مكرر3 من الأمر رقم 20-04 ، المصدر نفسه .

[3] – أمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق 25غشت سنة2021، يتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج ر ج ج العدد65.

القطب المستحدث أنشأ على مستوى محكمة مقر مجلس قضاء الجزائر، كقطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها.[1]

استحداث قطب جزائي متخصص في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال يندرج ضمن إستراتيجية شاملة للدولة إزاء هذا النوع من الجرائم، إذ يمثل هذا القطب خطوة إضافية في مسار التصدي للجرائم الالكترونية، بعدما أنشأ المشرع في السياق ذاته هيئة وطنية مكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وأدرجها ضمن زمرة " السلطات الإدارية المستقلة "، على خلاف القطب الجزائي الذي يكتسي الطبيعة القضائية، وأن السير في اتجاه التخصص القضائي ضرورة فرضتها العولمة التي أفرزت العديد من المعطيات ليس بإمكان القضاء بصورته العادية أن يتصدى لها، سيما بخصوص جرائم التكنولوجيا الفائقة بسبب الاحتراف والذكاء الذي يتميز به مرتكبي هذه الجرائم وبسبب سهولة إخفاء آثار الجريمة، يضاف إلى ذلك العبء الثقيل الذي يقع على القضاء عموما والذي يجعل من السير نحو التخصص ضرورة لا مفر منها، وإذا كانت الأقطاب الجزائية عموما لا تشكل تخصصا قضائيا بالمعنى الدقيق للمصطلح، إلا أنها تعد خطوة هامة للسير نحو الاتجاه.[2]

1- اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال:

إن الاختصاص النوعي للمحاكم يتحدد على أساس نوع الجريمة، ويتحدد نوع الجريمة على أساس العقوبة المقررة لها في قانون العقوبات، أو القوانين المكملة له، أي أن الاختصاص النوعي يفترض تحديد الواقعة وتطابقها مع نموذج قانوني خاص بجريمة بعينها، ثم تحديد نوعها على أساس

[1] – المادة 211مكرر22 من الأمر رقم 21-11، المصدر السابق.

[2] بن عمیور أمینة – بوحلایس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 07/العدد:01(2022)، ص72.

مقدار العقوبة، فالمادة 211 مكرر22 اعتبرت أن القطب المستحدث يختص بمعالجة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها .[1]

وحسب المادة 211 مكرر 24 منح المشرع الجزائري حصريا هذا القطب الفصل في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا الجرائم المرتبطة بها، حيث نصت على أنه " مع مراعاة أحكام الفقرة 2 من المادة 211مكرر22 [2]، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، و قاضي التحقيق ورئيس ذات القطب حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أذناه وكذا الجرائم المرتبطة بها :

– الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني.

– جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع .

– جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية.

– جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية .

– جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين.

– جرائم التمييز وخطاب الكراهية ."[3]

- بوقرة جمال الدين، عنان جمال الدين، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، المجلد 7، العدد1، جوان 2022، ص1684.[1]

[2] – " كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحا . "

[3] – المادة 211 مكرر 24 من الأمر رقم 21–11، المصدر السابق.

وكذا حسب المادة 211مكرر25 يختص وكيل الجمهورية لهذا القطب المستحدث، وكذا قاضي التحقيق ورئيس ذات القطب، حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا والجرائم المرتبطة بها .

حيث شرحت الفقرة الثانية من نفس المادة المقصود بالجريمة المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا، هي الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة أثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين، تتطلب استعمال وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي .[1]

2- بعض الإجراءات المتبعة أمام القطب المستحدث :

إذا كانت الجريمة المرتكبة من الجرائم التي ينعقد فيها **الاختصاص الحصري للقطب المستحدث،** فإنه يتعين تحويل ملف القضية وجوبا للقطب المستحدث وفق الحالات التالية:[2]

- إذا كانت القضية في طور البحث والتحري، فإنه يجب إرسال التقارير الإخبارية وإجراءات التحقيق من قبل مصالح الضبطية القضائية، مباشرة إلى وكيل الجمهورية لدى القطب المستحدث، ويتلقى ضباط الشرطة القضائية التعليمات منه مباشرة، وفي حالة فتح تحقيق قضائي فإنهم يتلقون الانابات القضائية من طرف قاضي التحقيق لدى القطب .

- إذا تم إيداع محاضر التحقيق المتعلقة بهذه القضايا على مستوى نيابات الجمهورية المختصة محليا، فإن الاختصاص الحصري ينعقد لوكيل الجمهورية لدى القطب المستحدث لذا يتعين على وكيل الجمهورية المبلغ بالملف أن يصدر مقررا بالتخلي، ويحول الملف إلى وكيل الجمهورية لدى القطب المستحدث.

[1] - المادة 211 مكرر 25 من الأمر رقم 21-11، المصدر السابق .

[2] - بوقرة جمال الدين، عنان جمال الدين، المرجع السابق، ص 1687،1688.

– إذا كانت القضية معروضة أمام قضاة التحقيق على مستوى المحاكم الوطنية، فإن قاضي التحقيق يصدر أمرا بعدم الاختصاص، وبعد صيرورة هذا الأمر نهائيا يحول ملف القضية بسعي من وكيل الجمهورية وجوبا إلى قاضي التحقيق على مستوى القطب المستحدث، مع بقاء الأوامر بالإيداع والقبض الصادرة عن قاضي التحقيق سارية المفعول إلى غاية صدور أمر مخالف من الجهة المختصة .

– إذا كانت القضية مطروحة أمام قضاة الحكم عبر المحاكم الوطنية، ولكون أحكام قانون الإجراءات الجزائية تطبق بأثر فوري حتى على القضايا التي ارتكبت قبل صدوره طالما لم يصدر بشأنها حكم، فإنه يتعين على قاضي الحكم أن يصدر حكمه بعدم الاختصاص، وبعد صيرورة هذا الحكم نهائيا يحول ملف القضية بسعي من وكيل الجمهورية وجوبا إلى القطب المستحدث.

3– إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع اختصاص القطب الاقتصادي والمالي، يؤول الاختصاص وجوبا لهذا الأخير.[1]

4– إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع اختصاص محكمة مقر مجلس قضاء الجزائر، يؤول الاختصاص وجوبا لهذه الأخيرة.[2]

[1] – المادة 211 مكرر28 من الأمر رقم 21–11، المصدر السابق .

[2] – المادة 211 مكرر29 من الأمر رقم 21–11، المصدر نفسه .

المبحث الثاني

مكافحة الجرائم المعلوماتية بموجب القوانين والهيئات الخاصة

نحاول التطرق تحت هذا المبحث لمطلبين، نتطرق من خلاله لمكافحة الجريمة المعلوماتية بموجب بعض القوانين الخاصة تحت مظلة المطلب الأول، أما المطلب الثاني سنتطرق تحته لمكافحة هذا النوع من الجرائم في ظل بعض الهيئات.

المطلب الأول

مكافحة الجرائم المعلوماتية بموجب القوانين الخاصة

سنتطرق لبعض القوانين التي شهدتها الجزائر في هذا المجال:

الفرع الأول

القواعد العامة المتعلقة بالبريد والاتصالات

نعالج في البداية القانون رقم 2000-03 الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ثم نتطرق لـ القانون رقم 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية.

أولا - القانون رقم 2000-03 يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية:[1]

إن الأزمة المالية التي شهدتها الجزائر نهاية ثمانينيات القرن الماضي دفعت بالسلطات العمومية إلى إقرار جملة من الإصلاحات الاقتصادية مست العديد من القطاعات، ومنها قطاع البريد والمواصلات المحتكر من طرف الدولة، بموجب المادة 17 من دستور 1989، وكذلك دستور

[1] - القانون رقم 2000-03 مؤرخ في 5 جمادى الأولى عام1421الموافق 5 غشت سنة 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، ج ر ج ج، العدد 48.

1996، و الأمر 75 /89 المتضمن قانون البريد والاتصالات، حيث صدر القانون 2000 /03 المؤرخ في 3 غشت 2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، والذي كرس من خلاله المشرع الجزائري، تحويل نشاطات استغلال البريد والمواصلات السلكية واللاسلكية، التي تمارسها وزارة البريد والمواصلات السلكية واللاسلكية إلى مؤسسة عمومية ذات طابع صناعي وتجاري للبريد، وإلى متعامل للمواصلات السلكية واللاسلكية ينشأ وفقا للتشريع المعمول به، وبالتالي بداية فتح هذا النشاط أمام استثمارات القطاع الخاص، ومن أجل ضبط قطاع البريد والمواصلات السلكية واللاسلكية، نصت المادة 10 من القانون 2000/ 03 على إنشاء سلطة ضبط مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، مهمتها ضمان السهر على وجود منافسة فعلية ومشروعة في سوقي البريد والمواصلات السلكية واللاسلكية بعد تحريره من احتكار الدولة، وإقامة التوازن بين حقوق والتزامات كل المتعاملين الاقتصاديين في سوقي البريد والمواصلات السلكية واللاسلكية.[1]

حاول المشرع الجزائري بموجب هذا القانون، مواكبة التشريعات الأخرى، وذلك في مجال التحويلات المالية، بإدخال التطور التكنولوجي في هذا الإطار، عن طريق تحويل الأموال إلكترونيا، حيث أنه حسب المادة 87 من هذا القانون تحت القسم الرابع المعنون بالحوالات، أعطى إمكانية إرسال الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق الإلكتروني.[2]

كما اعتبرت المادة 84 فقرة ثانية، والتي بدورها أشارت إلى تطبيق أحكام المادة 89 من هذا القانون، أن المتعامل مسئولا عن المبالغ المحولة إلى حوالات إلى حين دفعها، وهنا يقصد بتطبيق هذه المادة، عن استعمال حوالات دفع عادية أو إلكترونية أو برقية، والتي تهمنا هنا هي الإلكترونية.

وبالتالي هنا نص هذا القانون في جزء منه، على الاستغلال الأمثل لتكنولوجيا تحويل الأموال بواسطة الطريق الإلكتروني، وهذا بموجب نص المادة 87، كما اعتبر المشرع المسؤولية قائمة على

[1]– سعيود محمد الطاهر، استقلالية سلطة ضبط البريد والاتصالات الإلكترونية في ظل أحكام القانون 18 /04، مجلة الدراسات حول فعلية القاعدة القانونية، المجلد 04 العدد 01 –2020، ص 33،34.

[2]– المادة 87 من القانون رقم 2000–03، المصدر السابق.

عاتق المتعامل، فيما يخص المبالغ المحولة بموجب نص المادة 84/ 02، ويمثل هذا المجال بيئة خصبة للمجرم الإلكتروني، لارتكاب جرائم سرقة وتحويل الأموال، لذا أضفى المشرع حماية جزائية على استغلال هذه التكنولوجيا، نظرا لما ينجر عنها من أضرار تمس مصالح الدولة والأفراد على حد سواء، فأحاط سرية المراسلات التي هي حق دستوري[1]، مكفول بحماية خاصة بموجب نص المادتان 105 و 137 من القانون نفسه[2].

المادة 105 اعتبرت أنه "لا يمكن بأي حال من الأحوال انتهاك سرية المراسلات"، بل أنها رتبت جزاء على ذلك، بالنص على معاقبة كل من تسول له نفسه وبحكم مهنته، أن يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات، إذ أحالت المادة 127 منه ذلك إلى المادة 137 من قانون العقوبات، والتي تنص على ما يلي " كل موظف أو عون من أعوان الدولة، أو مستخدم أو مندوب عن مصلحة البريد، يقوم بفض أو اختلاس أو إتلاف رسائل مسلمة إلى البريد، أو يسهل فضها أو اختلاسها أو إتلافها، يعاقب بالحبس من ثلاثة أشهر إلى خمس سنوات وبغرامة من 30.000دج إلى 500.000دج، ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق، يختلس أو يتلف برقيه أو يديع محتواها.

ويعاقب الجاني فضلا عن ذلك، بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات.

مؤكدة على أن هذا النص يطبق على كل شخص مرخص له بتقديم خدمة البريد السريع أو الدولي أو كل عون يعمل لديه، والذي يتولى في إطار ممارسته لمهامه فتح أو تحويل أو تخريب أو انتهاك سرية المراسلات.[3]

---

[1]– هذا ما أكده التعديل الدستوري الأخير لسنة 2020 في مادته 47 وفي فقراتها الثانية والثالثة، بقولها لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت، ولا مساس بهذا الحق إلا بأمر معلل من السلطة القضائية.

[2]– يزيد بوحليط، المرجع السابق، ص147 .

[3]–زيبحة زيدان، المرجع السابق، ص77.

ثانيا- القانون رقم 18-04 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية:[1]

في ظل التغيرات العالمية المتسارعة التي يشهدها قطاع البريد والمواصلات السلكية واللاسلكية نتيجة التطور التكنولوجي، وكذا تطور السوق التنافسية لنشاط البريد والاتصالات، تدخل المشرع الجزائري سنة 2018 لسد الثغرات القانونية التي كشف عنها تطبيق أحكام القانون 2000/ 03 من خلال إصدار القانون 18- 04 المؤرخ في 10-5-2018م، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الذي نص في المادة 11 على إنشاء سلطة ضبط مستقلة تحت تسمية سلطة ضبط البريد والاتصالات الإلكترونية، تتمتع بالشخصية المعنوية والاستقلال المالي، تكلف بضمان ضبط أسواق البريد والاتصالات الإلكترونية لحساب الدولة، من خلال السهر على وجود منافسة فعلية ومشروعة في هذين السوقين، باتخاذ كل التدابير الضروري لترقية المنافسة .[2]

تحت القسم الثاني من هذا القانون " الاتصالات الإلكترونية"، نجد المادة 10 قد وضعت بعض المفاهيم من بينها، المقصود بالاتصالات الإلكترونية والأمن السيبراني، فاعتبرت الاتصالات الإلكترونية في فقرتها الأولى، بأنها كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات، مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية، أو بطريقة كهرومغناطيسية، أما في فقرتها الثالثة، فقصدت الأمن السيبراني، مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية، وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث، من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة، وفي نفس المادة تطرق لمفهوم الانترنت في فقرتها الخامسة، واعتبرها شبكة معلوماتية عالمية، تتشكل من

[1] - القانون رقم 18- 04 مؤرخ في 24شعبان1439هـ، الموافق ل10مايو2018م، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر.ج.ج، العدد 27 في 13 مايو 2018 .

[2]- سعيود محمد الطاهر، المرجع السابق، ص 34.

مجموعة شبكات وطنية وإقليمية وخاصة موصولة فيما بينها عن طريق بروتوكول الاتصال IP وتعمل معا بهدف تقديم واجهة موحدة لمستعمليها.[1]

واعتبرت المادة 97 الموجودة تحت الفصل الأول "**القواعد العامة**"، من الباب الثالث "**النظام القانوني للاتصالات الإلكترونية**"، أنه يخضع إنشاء واستغلال شبكات الاتصالات الإلكترونية المفتوحة للجمهور، وتقديم خدمات الاتصالات الإلكترونية للجمهور، إلى احترام شروط المداومة ونوعية الخدمات والوفرة وأمن وسلامة الشبكات والخدمات، واحترام شروط خصوصية البيانات والمعلومات، التي تم إيصالها بواسطة شبكات الاتصالات الإلكترونية، واحترام شروط حماية الحياة الخاصة للمشتركين والبيانات ذات الطابع الشخصي.[2]

وأكدت المادة 117 من نفس القانون، على أن لا يمس استعمال شبكات وخدمات الاتصالات الإلكترونية، النظام العام والدفاع الوطني والأمن العمومي من جهة، وكرامة وحفظ الحياة الخاصة للآخرين من جهة ثانية، ومن جهة أخرى حماية الأطفال، خصوصا فيما يتعلق باستعمال خدمات الإنترنت.[3]

كما ألزموا متعاملوا الاتصالات الإلكترونية، باتخاذ التدابير التي من شأنها أن تضمن سرية المكالمات والمعلومات التي يحوزونها على مشتركيهم، وألا يسمحوا بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية، والوصلات والمحادثات والمبادلات الإلكترونية، دون إذن مسبق من السلطة القضائية، ويجب عليهم أن يطلعوا أعوانهم على الالتزامات التي يخضعون لها، وعلى العقوبات التي يتعرضون لها في حالة عدم احترامهم لهذه الأحكام.[4]

[1]– المادة 10 من القانون رقم 18–04، المصدر السابق.

[2]– المادة 97 من القانون رقم 18–04، المصدر نفسه.

[3]– المادة 117 من القانون رقم 18–04، المصدر نفسه .

[4]– المادة 119من القانون رقم 18–04، المصدر نفسه.

وألزم هذا القانون المتعاملون وكذا مستخدموهم، باحترام سرية المراسلات الصادرة عن طريق الاتصالات الإلكترونية، وشروط حماية الحياة الخاصة والمعلومات الاسمية للمشتركين.[1]

وتحت الباب الرابع "**الأحكام الجزائية**"، تسلط عقوبة الحبس من سنة إلى خمس سنوات وبغرامة من 500,000دج إلى 1,000,000دج كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه، أو يخبر بوجودها.[2]

ويعاقب بالحبس من سنة إلى ثلاث سنوات، وبغرامة من 1,000,000دج إلى 5,000,000دج أو بإحدى هاتين العقوبتين، كل متعامل للبريد يفتح أو يحول أو يخرب البريد أو يساعد في ارتكاب هذه الأفعال، وتسري نفس العقوبات على كل متعامل للاتصالات الإلكترونية، يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية، أو أمر أو ساعد في ارتكاب هذه الأفعال، ويمكن الجهة القضائية أيضا النطق بواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 9 من قانون العقوبات.[3]

كما يعاقب بالحبس من ستة أشهر إلى سنتين، وبغرامة من 500.000دج إلى 1,000,000دج أو بإحدى هاتين العقوبتين، كل شخص مستخدم لدى متعامل للاتصالات الإلكترونية، يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية، أو أمر أو ساعد في ارتكاب هذه الأفعال.[4]

---

[1]–المادة160 من القانون رقم 18–04، المصدر السابق.

[2]–المادة 164من القانون رقم 18–04، المصدر نفسه .

[3]–المادة 165 من القانون رقم 18– 04، المصدر نفسه .

ونصت المادة 9 من قانون العقوبات على أن العقوبات التكميلية هي:1–الحجر القانوني، 2– الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية، 3– تحديد الإقامة، 4– المنع من الإقامة، 5– المصادرة الجزئية للأموال، 6– المنع المؤقت من ممارسة مهنة أو نشاط،7– إغلاق المؤسسة، 8– الإقصاء من الصفقات العمومية، 9– الحظر إصدار الشيكات و/أو استعمال بطاقات الدفع، 10– تعليق أو سحب رخصة السياقة أو إلغاؤها مع المنع من استصدار رخصة جديدة ، 11–سحب جواز السفر، 12– نشر أو تعليق حكم أو قرار الإدانة .

[4]– المادة 166 من القانون رقم 18– 04، المصدر نفسه .

وحسب المادة 171 يعاقب بالحبس من سنة إلى ثلاث سنوات، وبغرامة من 1,000,000دج إلى 5,000,000دج أو بإحدى هاتين العقوبتين، كل من ينشئ أو يستغل شبكة اتصالات إلكترونية مفتوحة للجمهور دون الرخصة المنصوص عليها في المادة 123 من هذا القانون، أو ممارسة النشاط خرقا لقرار التعليق أو سحب هذه الرخصة.[1]

الفرع الثاني

قانون التأمينات الاجتماعية والقانون المتعلق بالتوقيع والتصديق الالكترونيين

سوف نتطرق تحت هذا الفرع لقانونين مهمين وهما القانون رقم 08 -01 المؤرخ في 23 يناير2008 يتعلق بالتأمينات الاجتماعية، والقانون رقم15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

أولا-القانون رقم 08 -01 المؤرخ في 23 يناير2008 يتعلق بالتأمينات الاجتماعية:[2]

المشرع الجزائري استبق بهذا القانون الأحداث، ويمكن اعتبار ذلك اتجاها إيجابيا تحسبا للتطور المذهل لاستعمال التكنولوجية وتعميم الشبكة المعلوماتية في مختلف المجالات، إذ نص على أن صفة المؤمن له اجتماعيا تثبت ببطاقة إلكترونية، وحددت المادة 06 مكرر1 منه على أن البطاقة الإلكترونية تسلم للمؤمن له اجتماعيا مجانا من طرف هيئات الضمان الاجتماعي، وهي صالحة في كل التراب الوطني، وهي تقدم لكل مقدم علاج أو مقدم خدمات مرتبطة بالعلاج، وهذا الأخير يزود بمفتاح إلكتروني يسمى "المفتاح الإلكتروني لهيكل العلاج " حسب نص المادة 65 مكرر من هذا القانون.[3]

---

[1]- المادة 171 من القانون رقم 18 04. المصدر السابق.

[2] - القانون رقم 08-01 المؤرخ في 23 يناير سنة 2008، يتمم القانون رقم 83-11 المؤرخ في 2 يوليو سنة 1983 والمتعلق بالتأمينات الاجتماعية، ج ر ج ج / العدد 04 في 2008/01/27، ص4.

[3]- زيبحة زيدان، المرجع السابق، ص 78.

وبطبيعة الحال نظرا لاحتواء هذه البطاقة على معلومات سرية تتعلق بالحياة الخاصة للأفراد، أحاطها بالحماية الجزائية اللازمة، فنص في **المادة 93 مكرر2** على " دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين إلى خمس سنوات، وبغرامة من 100.000دج إلى 200.000دج كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة، كما تضاعف العقوبة على كل من يقوم عن طريق الغش بتعديل أو حذف للمعطيات حسب نص المادة 93مكرر3.[1]

كذلك المشرع الجزائري لم يفوت الفرصة وهو بصدد قانون خاص، أن يشدد العقوبة على كل من تلاعب في المعطيات أو البيانات المدرجة والمتضمنة في البطاقة الإلكترونية، سواء كانت تلك المعطيات تقنية معالجة آليا، أو إدارية محضة، كما أضفى حماية على البرمجيات، وذلك بتشديد العقوبة على كل من قام بنسخ أو تعديل فيها بطريقة غير مشروعة حسب هذا القانون.[2]

ثانيا- القانون رقم15-04 المتعلق بالتوقيع والتصديق الالكترونيين:[3]

نظرا لمتطلبات المعاملات الإلكترونية، لاسيما في ظل التوجه نحو الحكومة الإلكترونية ومقتضيات التجارة الإلكترونية، وبعد أن أدرج المشرع الجزائري نظام الإثبات بالكتابة في الشكل الإلكتروني ضمن قواعد الإثبات، أقر بنظام التوقيع والتصديق الإلكترونيين والاعتراف بحجيتهما في الإثبات قصد توفير الحماية اللازمة لوسائل الدفع الإلكتروني بالنسبة لمعاملات التجارة الإلكترونية، وزرع الثقة لدى المتعاملين لما يمتاز به من مستوى عال من الخصوصية والسرية.[4]

وجرم القانون رقم 15-04 بعض الأفعال المرتبطة بالبيانات والمعلومات ذات الطابع الشخصي التي تشكل الاعتداء عليها جريمة يعاقب مرتكبيها بأحكام جزائية، وهي:

---

[1]- يزيد بوحليط، المرجع السابق، ص 148.

[2]- زيبحة زيدان، المرجع السابق، ص 79.

[3]- القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين المؤرخ بتاريخ 1 فبراير2015م، ج.ر.ج.ج/ العدد 06/ 2015/02/10، ص06.

[4]- يزيد بوحليط ، المرجع نفسه، ص 148.

1- جريمة إفشاء البيانات الشخصية أو إساءة استعمالها:

حسب نص المادة 68 من هذا القانون يعاقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات، وبغرامة من مليون دينار إلى خمسة ملايين دينار، أو بإحدى هاتين العقوبتين فقط، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير.

2- جريمة الإخلال بسرية البيانات :

وفقا لنص المادة 42 من القانون 15-04 يجب على مؤدي خدمات التصديق الإلكتروني أن يحافظوا على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكترونية الممنوحة، فإذا أخلوا بهذا الواجب يعاقب بالحبس من ثلاثة أشهر إلى سنتين، وبغرامة من 200,000دج إلى مليون دينار أو بإحدى هاتين العقوبتين.

المشرع الجزائري أراد أن يضفي حمايته على المعلومات الشخصية التي تؤخذ من الأفراد، وأسبغ عليها صفة السرية لما لها من خصوصية معينة، وحسنا فعل عندما جرم الإخلال بسرية هذه البيانات، فتخزين المعلومات لا يعني أن هذه المعلومات قد انتقلت من الخصوصية إلى العلانية، كما أن الرضا بالتجميع والتخزين لا يعني حرية تداول ونقل المعلومات إلى جميع الناس،[1]وهذا ما نصت عليه الاتفاقيات الدولية .

3- جريمة جمع البيانات الشخصية للمعني دون موافقة :

المادة 43 من هذا القانون نصت على أنه لا يمكن لمؤدي خدمات التصديق الإلكتروني، أن يجمع البيانات الشخصية للمعني إلا بموافقته الصريحة، ومتى أخل بهذا الواجب، يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات وبغرامة مالية من 200.000دج إلى مليون دينار، أو بإحدى هاتين العقوبتين فقط.[2]

[1]- سي حمدي عبد المومن – قيرة سعاد، الجريمة الالكترونية وآليات التصدي لها في القانون الجزائري، مجلة البيان للدراسات القانونية والسياسية، المجلد 07، العدد01، جوان 2022، ص66.

[2]- سي حمدي عبد المومن – قيرة سعاد، المرجع نفسه، ص66.

وحسب المادة 42 الموجودة تحت الفصل الثاني معالجة المعطيات ذات الطابع الشخصي المرتبطة بخدمات التصديق والتوقيع الإلكترونيين، من الباب الخامس التزامات المسئول عن المعالجة من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، أنه ما عادا في حالة موافقتهم الصريحة يجب الحصول على المعطيات ذات الطابع الشخصي التي يتم جمعها من قبل مؤدي خدمات التصديق الإلكتروني لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني من الأشخاص المعنيين بها مباشرة، ولا يجوز معالجتها لأغراض غير تلك التي جمعت من أجلها.[1]

الفرع الثالث

القانون رقم 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:[2]

نظرا لخطورة هذا النوع من الجرائم، تطلب على المشرع الجزائري سن العديد من القوانين، وهنا نقصد القوانين الخاصة فجاء المشرع بالقانون 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أولا- أحكام عامة:

هدف هذا القانون وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذا حسب المادة الأولى منه.

---

[1]- المادة 42 من القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439هـ الموافق ل10يونيو سنة 2018م، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر ج ج، العدد 34.

[2]- القانون رقم 09- 04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،ح.ر.ج.ح، العدد 47.

كما وضح هذا القانون بعض المفاهيم المتعلقة بهذا النوع من الجرائم ، كمفهوم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والمنظومة المعلوماتية، ومعطيات معلوماتية، ومقدمو الخدمات، و الاتصالات الإلكترونية.[1]

ثانيا- مجال التطبيق:

يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية، وفي القانون 09-04 وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية، وذلك مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات.[2]

ثالثا- الحالات التي تسمح باللجوء إلى المراقبة الالكترونية

أما الفصل الثاني "**مراقبة الاتصالات الإلكترونية**" تطرق للحالات التي تسمح باللجوء إلى المراقبة الإلكترونية وهي كالآتي:[3]

1- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

2- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية، على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني.

3- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية .

4- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة .

---

[1]- المادة 2 من القانون 09-04، المصدر السابق.

[2]- المادة 3 من القانون رقم 09- 04، المصدر نفسه.

[3]- المادة 04 من القانون رقم 09-04، المصدر نفسه .

رابعا- القواعد الإجرائية التي تساعد على كشف ملابسات الجريمة المعلوماتية:

ونص الفصل الثالث على **القواعد الإجرائية التي تساعد على كشف ملابسات هذا النوع من الجرائم**، وذلك من حيث تفتيش للمنظومة المعلوماتية وحجز المعطيات المعلوماتية .

1-تفتيش المنظومة المعلوماتية:

أجاز هذا القانون للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي إطار هذا القانون الدخول بغرض التفتيش ولو عن بعد إلى :

أ- منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها .

ب- منظومة تخزين معلوماتية .

كما انه إذا كان هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها، بعد إعلام السلطة القضائية المختصة مسبقا بذلك، أما إذا كان تبين بأنها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة، طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبادئ المعاملة بالمثل .[1]

التفتيش يأخذ مجالين في الوضعيات المشار إليها، إما أن يكون في مجال أعمال التحقيق تقوم به السلطات القضائية المختصة، وإما أن يكون في مجال أعمال الاستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطات المختصة، وفي كلتا الحالتين يكون جهاز الحاسوب هو المستهدف بمختلف ما يتكون منه .[2]

[1] – المادة 5 من القانون رقم 09-04، المصدر السابق .

[2] – سي حمدي عبد المومن – قيرة سعاد، المرجع السابق، ص65.

كما أنه يمكن للسلطات المكلفة بالتفتيش، تسخير كل شخص لديه دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها ، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها .[1]

2-حجز المعطيات المعلوماتية: عندما يتم اكتشاف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، ويتبين للسلطة التي تباشر التفتيش ، أنه ليس من الضروري حجز كل المنظومة، يتم في هذه الحالة نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز.

وعلى هذه السلطات السهر على المحافظة على هذه المعطيات في كل الأحوال، حتى ولو جاز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق.[2]

ويتعين على السلطة التي تقوم بالتفتيش، استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة إذا استحالة إجراء الحجز لأسباب تقنية تبعا لما جاءت به المادة 06 من هذا القانون.[3]

أما فيما يتعلق "**بالمعطيات المحجوزة ذات المحتوى المجرم**"، يمكن للسلطة التي تباشر التفتيش أن تآمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة.[4]

---

[1] – الفقرة الأخيرة من المادة 5 من القانون رقم 09-04 ، المصدر السابق .

[2]– المادة 06 من القانون رقم 09 -04، المصدر نفسه .

[3]– المادة 07 من القانون رقم 09- 04، المصدر نفسه .

[4]–المادة 08 من القانون رقم 09- 04، المصدر نفسه .

خامسا- التزامات مقدمي الخدمات:

أما الفصل الرابع من هذا القانون 09- 04 تطرق ل "التزامات مقدمي الخدمات" ، وقبل التطرق لهذه الالتزامات لابد علينا معرفة من هم مقدمي الخدمات.

1- مقدمي الخدمة: حسب المادة 02 من القانون 09-04 هم أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

وهذا ما نصت عليه اتفاقية بودابست الموقعة في 23 نوفمبر 2001 المتعلقة بالإجرام الكوني في المادة الأولى، معتبرة مقدم الخدمة fournisseur de service كل جهة عامة أو خاصة تقدم لمستخدمي خدماتها إمكانية الاتصال عن طريق النظام المعلوماتي، وكل جهة أخرى تعالج أو تخزن البيانات المعلوماتية بدلا من خدمة الاتصال أو نيابة عن مستخدمي هذه الخدمة.[1]

في إطار هذا القانون، يتعين على مقدمي الخدمات، تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف هذه السلطات، كما يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.[2]

2- التزامات مقدمي الخدمة:

أ- **حفظ المعطيات المتعلقة بحركة السير:** وذلك بحفظ :

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

---

[1]-نصوص اتفاقية بودابست 2001، الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي منشورة على الموقع الرسمي للمجلس الأوروبي على الرابط التالي:

https://rm.coe.int/budapest-convention-in- arabic/1680739173

[2]- المادة 10 من القانون رقم 09- 04، المصدر السابق .

– المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

– الخصائص التقنية وكذا تاريخ و وقت ومدة كل اتصال.

– المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

– المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال، وكذا عناوين المواقع المطلع عليها.

أما بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

ب– و بالنسبة للالتزامات الخاصة بمقدمي خدمة الإنترنت: يتعين عليهم التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، كما يتعين عليهم وضع ترتيبات تقنية تسمح بحصر إمكانيات الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وأخبار المشتركين لديهم بوجودها.[1]

سادسا– الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته:

أما الفصل الخامس فتطرق " للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته".

وعليه حسب المادة 13 من القانون 09 – 04 نصت على أنه تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ومكافحته ومن مهامها:

[1]– المادة 12 من القانون رقم 09– 04، المصدر السابق .

1-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

2- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

3- تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.[1]

سابعا- التعاون والمساعدة القضائية الدولية:

هنا أشار القانون 09-04 إلى نقطتين مهمتين وهما، التعاون القضائي الدولي من جهة والقيود الواردة على طلب المساعدة القضائية الدولية من جهة أخرى.

1-التعاون القضائي الدولي : تطرق هذا القانون إلى الاختصاص القضائي، وكذا المساعدة القضائية الدولية المتبادلة.

أ-**الاختصاص القضائي:** تختص المحاكم الجزائية زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.[2]

ب-**المساعدة القضائية الدولية المتبادلة:** يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني، وذلك في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بالقانون 09-04 وكشف مرتكبيها،ويمكن في حالة الاستعجال مع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية إذا وردت عن طريق

[1]- المادة 13 و14 من القانون 09 – 04، المصدر السابق .

[2] - المادة 15 من القانون 09-04، المصدر نفسه.

وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.[1]

ج- تبادل المعلومات واتخاذ الإجراءات التحفظية: تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل .[2]

2- القيود الواردة على طلب المساعدة القضائية الدولية: من بين القيود الواردة المساس بالنظام العام والسيادة الوطنية وهنا يرفض تنفيذ طلب المساعدة، كذلك يمكن أن تكون الاستجابة لطلبات المساعدة القضائية مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب .[3]

المطلب الثاني

مكافحة الجريمة المعلوماتية بواسطة هيئات وسلطات خاصة

سنتطرق تحت هذا الفرع للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من جهة، وكذا للسلطة الوطنية لحماية المعطيات ذات الطابع الخاص من جهة ثانية .

الفرع الأول

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

سوف نتحدث عن نشأة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ومراحل تطورها وكذا مهامها بموجب المراسيم المتتالية هذا من جهة ومن جهة أخرى نتطرق لما جاء به المرسوم الرئاسي الجديد رقم 21-439 الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

[1] – المادة 16 من القانون 09-04، المصدر السابق .

[2] – المادة 17 من القانون 09-04، المصدر نفسه .

[3] – المادة 18 من القانون 09-04، المصدر نفسه.

أولا- نشأة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ومراحل تطورها وكذا مهامها بموجب المراسيم المتتالية:

1- نشأة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ومراحل تطورها بموجب المراسيم المتتالية:

في 2009 أنشأ المشرع الجزائري هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها [1]، وقد أعطى لها في **المرسوم الرئاسي رقم 15- 261** [2]صفة السلطة الإدارية المستقلة، وذلك في المادة 2، وتظهر هذه السلطة المستقلة من خلال تمتعها بالشخصية المعنوية والاستقلال المالي، وإعدادها لنظامها الداخلي وتمثيلها لنفسها أمام المؤسسات الوطنية والدولية وعلى مستوى القضاء، إلا أنها أخضعها للرقابة، ففي **المادة 32** مثلا من **المرسوم الرئاسي رقم 15 -261** " يرفع رئيس اللجنة المديرة للهيئة إلى رئيس الجمهورية تقارير فصلية عن نشاطات الهيئة"، وهذا ما يتنافى والاستقلالية، إلى جانب تشكيلته ففي **المواد 6 و7** مثلا من **المرسوم الرئاسي رقم 15- 261** بحيث تضم الهيئة لجنة مديرة يرأسها وزير العدل ويتشكل أعضاؤها من وزيري الداخلية والبريد وتكنولوجيات الإعلام والاتصال، وقائد الدرك الوطني والمدير العام للأمن الوطني، وممثل عن رئاسة الجمهورية وممثل عن وزارة الدفاع (يعينان بمرسوم رئاسي)، و قاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء، ضف إلى ذلك عدم تمتعها بسلطة العقاب كما هو معهود لمؤسسات الضبط المستقلة، لكن صفة السلطة الإدارية المستقلة تراجع عنها المشرع الجزائري لاحقا بموجب **المرسوم الرئاسي 19- 172** [3]، واعتبرها مؤسسة عمومية ذات طابع إداري توضع تحت سلطة وزارة الدفاع.[1]

---

[1] - القانون رقم 09- 04، المصدر السابق .

[2] - المرسوم الرئاسي رقم 15-261 مؤرخ في 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج، العدد 53 – 08 أكتوبر 2015، ص16.

[3]- المرسوم الرئاسي رقم **19-172** مؤرخ في 3 شوال عام 1440هـ، الموافق ل6 يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها و كيفيات سيرها، ج.ر.ج.ج، العدد 37.

وأصبحت الهيئة بعد صدور **المرسوم الرئاسي رقم 19- 172** مكونة من جهازين اثنين هما، **مجلس التوجيه ومديرية عامة** طبقا لنص **المادة الرابعة** .

فمجلس التوجيه حسب **المادة 5** تشكيلته من ممثلي الوزارات الآتية، وزارة الدفاع الوطني، الوزارة المكلفة بالداخلية، وزارة العدل، الوزارة المكلفة بالمواصلات السلكية واللاسلكية، برئاسة وزير الدفاع الوطني أو ممثليه.

الملاحظ أن هذا المرسوم حصر تشكيلة الهيئة في أربع وزارات وأسقط عدة قطاعات أخرى كالأمن والدرك الوطني والقضاة، وهو ما يعاب على المشرع عند إسقاطه عضوية القضاة ذوي الخبرة في مجال مكافحة الجرائم السيبيرانية.

أما **المديرية العامة**، اكتفى المرسوم الرئاسي بوضعها تحت إدارة مدير عام، وتضم مديرية تقنية، مديرية الإدارة والوسائل، مجموعة من المصالح من دون تحديد تشكيلها بدقة.

فالمرسوم الرئاسي الجديد قد لجأ إلى التقليص من الهياكل الرئيسية المكونة للهيئة على خلاف سابقة، وعوضها بهياكل جديدة فرعية تعمل تحت سلطة المديرية العامة وتتمثل في مديرية تقنية، مديرية للإدارة والوسائل، مصالح من دون تحديد تشكيلتها التي ترجع من دون شك للمدير العام بتفويض من وزير الدفاع بالنظر للمهام التي تقوم بها.

وعليه، هذا المرسوم الرئاسي الذي تم تعديله اتجه إلى تركيز هياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من خلال إحلال نظام تدرج لصالح المديرية العامة، بعد أن كان لصالح اللجنة المديرة في ظل المرسوم السابق،[2] حيث كلا المرسومان تم تعديلهما.

---

[1]– حابت آمال، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، المجلد 05، العدد 03، ديسمبر 2021 ص 466.

[2]– خرشي إلهام، النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة الأبحاث القانونية والسياسية، المجلد 04، العدد 01، 2022 ص 63، 64.

2- مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

هنا علينا الرجوع إلى نص **المادة 14** من **القانون رقم 09- 04**، التي ذكرت لنا مهام الهيئة، من تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، إلى مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

وأخيرا إلى تبادل المعلومات مع نظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.[1]

المرسوم الرئاسي رقم 19- 172 حسب **مادته 24** قام بإلغاء جميع الأحكام المخالفة لهذا المرسوم، لاسيما أحكام **المرسوم الرئاسي رقم 15- 261** الذي يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

فبالرجوع إلى هذا **القانون 19-172 فمجلس التوجيه** الذي تطرقنا له سابقا يكلف على الخصوص، بما يأتي:

- التداول حول الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بـ الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

- التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

- القيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها، والأهداف المنشودة بدقة.

[1]- المادة 14 من القانون 09- 04، المصدر السابق .

– اقتراح كل نشاط يتصل بالبحث، وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[1]

أما **المديرية العامة** فمن بين صلاحياتها:

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– تبادل المعلومات مع مثيلاتها الأجنبية بغض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم.[2]

فالمديرية التقنية التي تضمنها المديرية العامة، **تكلف** حسب المادة 11 بمهمة المراقبة الوقائية للاتصالات الإلكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة،[3]**وتتولى كذلك على الخصوص:**

– مساعدة السلطات القضائية و مصالح الشرطة القضائية بناء على طلبها، بما في ذلك في مجال الخبرات القضائية في إطار مكافحة الجريمة المتصلة بتكنولوجيات الإعلام والاتصال والجرائم التي تتطلب اللجوء إلى أساليب التحري الخاصة للهيئة.

– جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية.[4]

كذلك حسب المادة 14 من المرسوم الرئاسي رقم 19–172 تضع المديرية التقنية التجهيزات والوسائل والأجهزة التقنية الضرورية لتنفيذ مهامها على مستوى المنشآت القاعدية للمتعاملين ومقدمي الخدمات، وهم ملزمون بتقديم المساعدة الضرورية للمديرية التقنية من أجل تنفيذ مهامها.[5]

كانت الهيئة في ظل المرسوم الرئاسي رقم 15–261 تتمتع بمهام استشارية ومساعدة في تكوين المحققين إلا أن المرسوم الرئاسي 19–172 سحب منها هذا الاختصاص وأبقى اختصاصها المتمثل

---

[1]– المادة 06 من المرسوم الرئاسي رقم **19–172**، المصدر السابق.

[2]– المادة 09 من المرسوم الرئاسي رقم 19–172، المصدر نفسه .

[3]– المادة 11من المرسوم الرئاسي رقم 19–172، المصدر نفسه.

[4]– المادة 12 من المرسوم الرئاسي رقم 19–172، المصدر نفسه.

[5] – المادة14 من المرسوم الرئاسي رقم 19–172، المصدر نفسه.

في التحري، كذلك ألغى الرقابة التي كانت تخضع لها هذه الهيئة سواء رقابة السلطة التنفيذية المتمثلة في رئيس الجمهورية من خلال التقارير الفصلية التي ترفع له من قبل الهيئة، وكذا الرقابة القضائية حيث تمارس الهيئة اختصاصاتها تحت رقابة السلطة القضائية دون أن تحددها، أما المرسوم الرئاسي رقم 19-172 الذي ألغى الرقابتين، جرد كذلك الهيئة من صفة السلطة المستقلة وأخضعها لوزارة الدفاع الوطني، كما أغفل الحديث عن دور الهيئة في الحالات الإستعجالية والطارئة، وأغفل كذلك ضبط المواعيد القانونية الخاصة بالاحتفاظ بالمعلومات المستقاة من ممارسة الهيئة لمهامها، وهو من ضمانات حماية الحريات الخاصة.[1]

ثانيا : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في ظل المرسوم الرئاسي 21-439 :

ان المرسوم الرئاسي 19-172 تم إلغائه بموجب المرسوم الرئاسي 20-183 والمتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، لكن هذا لم يدم طويلا وذلك بمجئ مرسوم رئاسي جديد رقم 21-439 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

1- تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها :

تحت سلطة رئيس الجمهورية تتكون الهيئة من مجلس توجيه ومديرية عامة.[2]

أ- مجلس توجيه الهيئة :

الأمين العام لرئاسة الجمهورية حسب المادة السادسة من هذا المرسوم هو الذي يتولى رئاسة هذا المجلس، أما تشكيلته فتتكون مما يلي:

[1]- حابت آمال، المرجع السابق، ص 478.

[2]- المادة 5 من المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر سنة 2021 ، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ج ر ج ج، العدد 86.

الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج، الأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية، الأمين العام لوزارة العدل، الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية، قائد الدرك الوطني، المدير العام للأمن الداخلي، المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي، المدير العام للأمن الوطني، رئيس مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي، ممثل عن رئاسة الجمهورية يعين من طرف رئيس الجمهورية.

الملاحظ أن هذا المرسوم تدارك بإدراجه في هذه التشكيلة عدة قطاعات كالأمن والدرك الوطني، لكن ما يعاب عليه عدم إدراجه مثلا أهل الاختصاص من باحثين في هذا المجال كأعضاء في هذا المجلس.

ب- المديرية العامة للهيئة:

للمديرية العامة للهيئة مدير عام يعين بموجب مرسوم رئاسي، وبدوره عليه السهر على حسن سير هذه الهيئة كضمان التسيير الإداري والمالي للهيئة، وكذا كتمثيل الهيئة لدى القضاء وفي جميع أعمال الحياة المدنية، إخطار رئيس الجمهورية فورا عن كل حادثة من شأنها المساس بأمن الدولة أو تلك المرتبطة بالأعمال الإرهابية أو التخريبية، كما يخطر أيضا رئيس أركان الجيش الوطني الشعبي عندما يتعلق الأمر بمسائل تخص الدفاع الوطني، وله مهام كثيرة وذلك حسب المادة 10 من هذا المرسوم .

وتضم هذه المديرية عدة مديريات وهي مديرية المراقبة الوقائية واليقظة الالكترونية، مديرية الإدارة والوسائل، مصلحة للدراسة والتلخيص، مصلحة للتعاون واليقظة التكنولوجية، ملحقات جهوية .

2- سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها :

سوف نبين أهم النقاط التي نص عليها هذا المرسوم لسير الهيئة وهي:

أ- حسب المادة 20 من هذا المرسوم لسير هذه الهيئة يلحق بها قضاة وكذا ضباط وأعوان للشرطة القضائية مؤهلون من المصالح العسكرية للأمن والدرك الوطني والأمن الوطني، وكذا مستخدمو الدعم

التقني والإداري للمصالح العسكرية للأمن المختصة والدرك الوطني والأمن الوطني،[1] كما يمكن أن توظف فئات أخرى من المستخدمين حسب الحاجة التي تراها الهيئة.[2]

ب- يمكن للهيئة وفي إطار علاقات التعاون أن تطلب حسب هذا المرسوم من أي جهاز أو مؤسسة أو مصلحة أي وثيقة أو معلومة ضرورية لإنجاز الدور المناط لها.[3]

ج- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو التي تمس بأمن الدولة ومكافحتها، تكلف الهيئة حصريا في مجال اختصاصها بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها داخل منظومة معلوماتية تحت سلطة قاض لدى الهيئة .[4]

د- كذلك لتنفيذ عملية مراقبة الاتصالات الالكترونية يمكن الهيئة أن تضع وحدة مراقبة واحدة أو أكثر تزود بالوسائل والتجهيزات التقنية الضرورية التي تسمح لها بأداء مهامها.[5]

هـ- المعلومات المستقاة أثناء عمليات المراقبة تحفظ خلال حيازتها من طرف الهيئة وفقا للقواعد المطبقة على حماية المعلومات المصنفة .[6]

و- كذلك يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعون للهيئة أثناء ممارستهم لوظائفهم أو بمناسبتها بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم أنه يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الالكترونية .[7]

ز- الهيئة يمكن أن تطلب مساعدة موظفين مختصين من الوزارات المعنية في مجال تكنولوجيات الإعلام والاتصال ، كما يمكنها أن تستعين بأي خبير أو أي شخص يمكن أن يساعدها في أعمالها.[1]

---

[1] – المادة 20 من المرسوم الرئاسي 21-439، المصدر السابق.

[2] – المادة 21 من المرسوم الرئاسي 21-439، المصدر نفسه.

[3] – المادة 24 من المرسوم الرئاسي 21-439، المصدر ننسه.

[4]– المادة 25 من المرسوم الرئاسي 21-439، المصدر نفسه.

[5]– المادة 26 من المرسوم الرئاسي 21-439، المصدر نفسه.

[6]– المادة 27 من المرسوم الرئاسي 21-439، المصدر نفسه .

[7] – المادة 30 من المرسوم الرئاسي 21-439، المصدر نفسه .

3- المهام المنوطة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

حسب المرسوم الرئاسي 21-439 فإن أهم المهام المنوطة للهيئة هي كالتالي:

أ- تحديد الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ووضعها حيز التنفيذ.

ب- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ج- ضمان المراقبة الوقائية للاتصالات الإلكترونية تحت سلطة القاضي المختص ، قصد الكشف عن الجرائم المتصلة بالأعمال الإرهابية أو التخريبية أو التي تمس بأمن الدولة.

د- تضمن الهيئة بالتنسيق مع المصالح المختصة لوزارة الدفاع الوطني المراقبة الالكترونية عندما يتعلق الأمر بأمن الجيش .

هـ- تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجعل استعمالها في الإجراءات القضائية .

و- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال .

ز- المساهمة في تحيين المعايير القانونية في مجال اختصاصها.

ح- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال عن طريق جمع المعلومات والتزويد بها وإنجاز الخبرات القضائية.

ط- تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

[1] - المادة 32 من المرسوم الرئاسي 21-439، المصدر السابق .

ي- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.[1]

تعتبر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها من الهيئات التي لقت استحسانا في أواسط خبراء مجال مكافحة الجريمة المعلوماتية وهذا لما لها من إضافة إيجابية في هذا المجال رغم خبرتها القصيرة وكثرة التعديلات التي مستها، ولكن غالبيتها كانت تصب في الاتجاه الايجابي بوضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

الفرع الثاني

السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي حسب القانون رقم18-07 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:[2]

مواكبة للمشرع الجزائري للجرائم الماسة بخصوصيته الأفراد، أصدر قانون يهدف إلى تحديد قواعد **حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،** وهذه المعالجة مهما كان مصدرها أو شكلها، يجب أن يكون في إطار احترام الكرامة الإنسانية والحياة الخاصة و الحريات العامة، وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم، وهو القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

أولا- إنشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

هي سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي، تنشأ لدى رئيس الجمهورية يحدد مقرها في الجزائر العاصمة، تتمتع بالشخصية المعنوية والاستقلال المالي والإداري، وتعد السلطة الوطنية نظامها الداخلي الذي يحدد لاسيما كيفية تنظيمها وسيرها وتصادق عليه.[1]

[1] - المادة 4 من المرسوم الرئاسي 21-439، المصدر السابق.

[2] - القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439هـ الموافق لـ10يونيو سنة 2018م، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،ج ر ج ج، العدد 34.

ثانيا- تشكيلة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:[2]

السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي تتشكل من:

1-ثلاث شخصيات من بينهم الرئيس يختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال عمل السلطة الوطنية.

2- ثلاث قضاة يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة.

3- عضو عن كل غرفة من البرلمان، يتم اختياره من قبل رئيس كل غرفة بعد التشاور مع رؤساء المجموعات البرلمانية.

4- ممثل عن المجلس الوطني لحقوق الإنسان.

5- ممثل عن وزير الدفاع الوطن.

6- ممثل عن وزير الشؤون الخارجية.

7- ممثل عن الوزير المكلف بالداخلية.

8- ممثل عن وزير العدل حافظ الأختام.

9- ممثل عن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيات و الرقمنة .

10- ممثل عن الوزير المكلف بالصحة.

11- ممثل عن وزير العمل والتشغيل والضمان الاجتماعي.

ويتم اختيار أعضاء السلطة الوطنية حسب اختصاصهم، القانوني أو التقني في مجال معالجة المعطيات ذات الطابع الشخصي.

ويمكن للسلطة الوطنية أن تستعين بأي شخص مؤهل من شأنه مساعدتها في أشغالها.

---

[1]- المادة 22 من القانون رقم 18-07، المصدر السابق .

[2] - المادة 23 من القانون رقم 18-07، المصدر نفسه.

ثالثا-عهدة السلطة الوطنية : خمس سنوات قابلة للتجديد، ويعين رئيسها وأعضاؤها بموجب مرسوم رئاسي.[1]

رابعا- مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

تكلف بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة.

وتتمثل مهامها في هذا الصدد فيما يلي:

1- منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.

2- إعلام الأشخاص المعنيين والمسئولين عن المعالجة بحقوقهم وواجباتهم.

3- تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي، أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة.

4- تلقى الاحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي، وإعلام أصحابها بمآلها.

5- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون.

6- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة .

7- الأمر بإغلاق معطيات أو سحبها أو إتلافها.

[1]- المادة 23 من القانون رقم 18-07، المصدر السابق.

8 – تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.

9– تطوير علاقات التعاون مع السلطات الأجنبية الممثلة مع مراعاة المعاملة بالمثل.

10– إصدار عقوبات إدارية.

11– وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي.

12 – وضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي.

كما في إطار ممارسة مهامها تعلم السلطة الوطنية النائب العام المختص فورا في حالة معاينة وقائع تحتمل الوصف الجزائي.[1]

كما يجب على رئيس وأعضاء السلطة الوطنية، المحافظة على الطابع السري للمعطيات ذات الطابع الشخصي والمعلومات التي اطلعوا عليها بهذه الصفة ولو بعد انتهاء مهامهم، ما لم يوجد نص قانون يقضي بخلاف ذلك، ولا يجوز لرئيس السلطة الوطنية وأعضائها، أن يمتلكوا بصفة مباشرة أو غير مباشرة مصالح في أي مؤسسة تمارس نشاطاتها في مجال معالجة المعطيات ذات الطابع الشخصي.[2]

خامسا– شرح بعض المفاهيم:

1– المقصود بالمعطيات ذات الطابع الشخصي:

يقصد بالمعطيات ذات الطابع الشخصي كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو

[1]– المادة 25 من القانون رقم 18 –07، المصدر السابق .

[2]– المادة 26 من القانون رقم 18– 07، المصدر نفسه .

عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية .[1]

2-الشخص المعني : هو كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة.[2]

3- معالجة المعطيات ذات الطابع الشخصي:

هو كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية، أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال، عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني، وكذا الإغلاق أو التشفير أو المسح أو الإتلاف.[3]

سادسا- الجزاءات المترتبة لحماية المعطيات ذات الطابع الشخصي حسب القانون 18-07:

هنا نتطرق للجرائم التي جاء بها هذا القانون والجزاءات المترتبة عليها:

1-جريمة المساس بالكرامة الإنسانية والحياة الخاصة عند معالجة المعطيات :

بناءا على ما جاء به التعديل الدستوري لسنة 2016 في المادة 46 بأنه لا يجوز انتهاك حرمة حياة المواطن الخاصة، حرمة شرفه، ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، كما أنه لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم، كما أن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه . [4]

[1]- المادة 03 من القانون رقم18-07 ، المصدر السابق.

[2]- المادة 03 من القانون رقم18-07، المصدر نفسه .

[3]- المادة 03 من القانون رقم18-07، المصدر نفسه.

[4]- المادة 46 من التعديل الدستوري 2016، المصدر السابق .

وهذا ما أكد عليه التعديل الدستوري لسنة 2020 في مادته 47.[1]

عدم احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وحقوق الأشخاص وشرفهم وسمعتهم، عند معالجة المعطيات، هذا الخرق يؤدي إلى المعاقبة بالحبس من سنتين إلى خمس سنوات وبغرامة من 200,000دج إلى 500,000دج.[2]

2-جريمة معالجة المعطيات ذات الطابع الشخصي دون الموافقة الصريحة للشخص المعني: خرق نص المادة 07 من القانون 18 -07 التي تنص على أنه لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني، هذا الخرق يؤدي إلى المعاقبة بالحبس من سنة إلى ثلاث سنوات وبغرامة من 100,000دج إلى 300,000دج

ويعاقب بنفس العقوبة، كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني، عندما تستهدف هذه المعالجة لاسيما الإشهار التجاري، أو عندما يكون الاعتراض مبنيا على أسباب شرعية.[3]

3- جريمة معالجة المعطيات ذات الطابع الشخصي دون تصريح مسبق لدى السلطة الوطنية أو دون ترخيص منها:

طبقا لنص المادة 12 تخضع كل عملية معالجة معطيات ذات طابع شخصي لتصريح مسبق لدى السلطة الوطنية أو لترخيص منها و خرقا لهذه المادة يؤدي إلى المعاقبة بالحبس من سنتين إلى خمس سنوات و بغرامة من 200,000دج إلى 500,000دج كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام هذه المادة .[4]

---

[1]- المادة 47:"لكل شخص الحق في حماية حياته الخاصة وشرفه. لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت. لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية .حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. يعاقب القانون على كل انتهاك لهذه الحقوق."

[2]- المادة 54 من القانون رقم 18- 07، المصدر السابق.

[3]- المادة 55 من القانون رقم 18 -07، المصدر نفسه.

[4]- المادة 56 من القانون رقم 18- 07، المصدر نفسه .

4- جريمة معالجة معطيات لأغراض غير مصرح به أو مرخص لها:

كل من قام بإنجاز أو باستعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها أو المرخص لها، هنا يعاقب بالحبس من ستة أشهر إلى سنة وبغرامة من 60,000دج إلى 100,000دج أو بإحدى هاتين العقوبتين .[1]

5- جريمة جمع معطيات ذات طابع شخصي بطريقة تدليسية:

جمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة، يعاقب هنا بالحبس من سنة إلى ثلاث سنوات وبغرامة من 100,000دج إلى 300,000دج.[2]

6- جريمة السماح لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي:

كل من سمح لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي،هنا العقوبة بالحبس من سنتين إلى خمس سنوات وبغرامة من 200.000دج إلى 500,000دج .[3]

7- جريمة عرقلة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

كل من عرقل عمل السلطة الوطنية، وذلك بـ:الاعتراض على إجراء عملية التحقيق في عين المكان – عن طريق رفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية أو إخفاء أو إزالة الوثائق أو المعلومات – عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم

[1]- المادة 58 من القانون رقم 18- 07، المصدر السابق.

[2]- المادة 59 من القانون رقم 18- 07، المصدر نفسه.

[3]- المادة 60 من القانون رقم 18 -07، المصدر نفسه.

تقديمها بشكل مباشر وواضح، هذه العرقلة تؤدي إلى العقوبة بالحبس من ستة أشهر إلى سنتين، وبغرامة من 60,000دج إلى 200,000دج أو بإحدى هاتين العقوبتين .[1]

8- جريمة إفشاء المعلومات المحمية بموجب القانون 18- 07 :

إفشاء المعلومات المحمية بموجب القانون 18- 07 : يعاقب كل من يشكل السلطة الوطنية والأمانة التنفيذية للسلطة الوطنية بعقوبة الحبس من شهر إلى ستة أشهر وبغرامة من 20,000 إلى 100,000دج[2]، وهي عقوبة المادة 301 من قانون العقوبات الموجودة تحت القسم الخامس المعنون بـ **الاعتداءات على شرف واعتبار الأشخاص وعلى حياتهم الخاصة وإفشاء الأسرار**، التي كانت تخص الأطباء والجراحون والصيادلة والقابلات، وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة، على أسرار أدلى بها إليهم و أفشو ها في غير الحالات التي يوجب عليهم فيها القانون إفشائها ويصرح لهم بذلك.

9- جريمة خرق التزامات سلامة التدابير التقنية والتنظيمية:

خرق التزامات سلامة التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من المسئول عن هذه المعالجة، هذا يؤدي إلى التعرض للعقوبة من 200,000دج إلى 500,000دج، كما يعاقب بنفس العقوبة كل من قام بالاحتفاظ بـ المعطيات ذات الطابع الشخصي بعد المدة المطلوبة أو المصرح أو المرخص بها .[3]

10- جريمة نقل المعطيات ذات الطابع الشخصي نحو دولة أجنبية:

نقل المعطيات ذات الطابع الشخصي نحو دولة أجنبية خرقا للمادة 44 من القانون 18- 07 " لا يجوز لمسئول عن معالجة نقل المعطيات ذات طابع شخصي إلى دولة أجنبية إلا بترخيص للسلطة الوطنية، وفقا لأحكام هذا القانون، وإذا كانت هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة و

[1]- المادة 61 من القانون رقم 18 -07، المصدر السابق.

[2]- المادة 62 من القانون 18 – 07، المصدر نفسه .

[3]- المادة 65 من القانون 18 – 07، المصدر نفسه .

الحريات والحقوق الأساسية للأشخاص إزاء المعالجة التي تخضع لها هذه المعطيات أو التي قد تخضع لها.

تقدر السلطة الوطنية المستوى الكافي من الحماية الذي تضمنه دولة معينة، لاسيما وفقا للمقتضيات القانونية المعمول بها في هذه الدولة و لإجراءات الأمن المطبقة فيها، وللخصائص المتعلقة بالمعالجة مثل غاياتها ومدتها وكذا طبيعة وأصل ووجهة المعطيات المعالجة.

وفي جميع الأحوال ، يمنع إرسال وتحويل معطيات ذات الطابع الشخصي إلى دولة أجنبية عندما قد يؤدي ذلك إلى المساس بالأمن العمومي أو المصالح الحيوية للدولة"، هنا يتعرض كل من يقوم بذلك بعقوبة الحبس من سنة إلى خمس سنوات وبغرامة من 500,000دج إلى 1,000,000دج.[1] .

[1]– المادة 67 من القانون 18–07، المصدر السابق .

الباب الثاني

مكافحة جرائم المعلوماتية دوليا

الباب الثاني

مكافحة جرائم المعلوماتية دوليا

من نتائج التطور التكنولوجي الحاصل على المستوى الدولي والوطني، أن أصبحت المعلومات أو بتعبير أكثر دقة "تقنية المعلومات" من أساسيات الحياة في المجتمعات الحديثة وخصوصا في مطلع الألفية الجديدة، وكما هي العادة دائما تبرز الجوانب الإيجابية للتكنولوجيا المعلوماتية الهادفة إلى مزيد من الرفاهية للبشرية وفي ذات الوقت تظهر الآثار السلبية لهذه التكنولوجيا بدليل لجوء البعض من مستخدمي هذه التقنية الحديثة في تحقيق أهداف شخصية بحسب المصالح الخاصة التي يهتموا بها سواء فيما يتعلق باستخدامات الحاسب الآلي بصفة عامة أو شبكة الانترنت بصفة خاصة من خلال احتراف اقتراف الجرائم المعلوماتية بواسطة هذه الوسائل التقنية المستحدثة، وغني عن البيان أن هذه الجرائم تؤدي غالبا إلى أضرار مادية ومعنوية تلحق بالأشخاص والمشروعات العاملة في مجال تقنية المعلومات، وهو الأمر الذي يثير التساؤل حول الوسائل الوقائية والعلاجية لمكافحة مثل هذه الجرائم المعلوماتية.[1]

وللتأكيد على أهمية وخطورة الجرائم المعلوماتية فقد أفرد مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين إحدى حلقات عمله الأربع التي وردت على جدول أعماله لدراسة الجرائم المتعلقة بشبكات الحاسوب والانترنت، وقد أشير خلال المناقشات إلى أن الجرائم المعلوماتية تمثل أحد تحديات القرن الحادي والعشرين، وقد صارت هناك ضرورة ملحة ومبررات قوية للتعاون الدولي لمكافحة الجرائم

[1] - محمد علي العريان، المرجع السابق، ص23.

المعلوماتية، مع ضرورة النظر إلى التعاون بمفهومه الشامل، بحيث يتسع لاستيعاب الصور المختلفة لمجالات التعاون .[1]

و بعدما تطرقنا في الباب الأول من موضوعنا هذا لمكافحة الجريمة المعلوماتية في القانون الجزائري مبرزين في البداية الإطار المفاهيمي لهذا النوع من الجرائم ثم عالجنا هذا النوع من الجرائم في التشريع الجزائري موضحين سبل مكافحته من خلال القوانين الجزائرية سواء العامة أو الخاصة، سوف نتطرق في الباب الثاني لمكافحة هذا النوع من الجرائم دوليا بتقسيمنا له لفصلين، مبرزين في الفصل الأول القوانين والاتفاقيات الدولية في مجال مكافح الجريمة المعلوماتية، حيث قسمنا هذا الفصل إلى مبحثين، متناولين تحت المبحث الأول المعاهدات والقوانين الخاصة بحماية حق الملكية الفكرية، أما المبحث الثاني فعالجناه تحت عنوان الاتفاقيات الدولية في مجال مكافحة الجريمة السيبرانية، متطرقين خاصة إلى معاهدة بودابست وبروتوكولاتها من جهة، ومبرزين الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من جهة ثانية، أما الفصل الثاني فجاء مكملا للفصل الأول بعنوان الاتجاهات الدولية في مجال مكافحة الجرائم المعلوماتية، وبدوره قسم إلى مبحثين، أوله تطرقنا فيه للتعاون الدولي في مجال مكافحة جرائم المعلوماتية وإشكالاته، أما المبحث الثاني أبرزنا فيه الطريق نحو اتفاقية عالمية لمكافحة الجريمة السيبرانية برعاية الأمم المتحدة بحدود 2023 .

[1] - عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، جمهورية مصر العربية، 2015، ص11.

الفصل الأول

القوانين والاتفاقيات الدولية في مجال مكافحة الجريمة المعلوماتية

الفصل الأول

القوانين والاتفاقيات الدولية في مجال مكافحة الجريمة المعلوماتية

لمعالجة هذا الفصل عمدنا تقسيمه إلى مبحثين، حيث جاء عنوان المبحث الأول تحت مسمى المعاهدات والقوانين الخاصة بحماية حق الملكية الفكرية متطرقين تحته للمعاهدات الدولية التي إبرامها في مجال حماية حقوق الملكية الفكرية كاتفاقية برن لحماية المصنفات الفنية والأدبية وكذا معاهدة تربس ومعاهدة الويبو هذا من جهة، ومن جهة أخرى وتحت نفس المبحث تم التطرق للقوانين التي أصدرتها الجزائر وبعض الدول العربية في مجال حماية حقوق الملكية الفكرية، أما المبحث الثاني فجاء تحت عنوان الاتفاقيات الدولية في مجال مكافحة الجريمة السيبرانية حاولنا الولوج من خلاله لمعاهدة بودابست لمكافحة جرائم الانترنت وذلك من خلال التطرق لها قبل البروتوكول الإضافي الثاني لها من جهة، وكذا إبراز البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية 2022 من جهة أخرى، كما أنه وتحت نفس المبحث تطرقنا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات مبرزين بعض الأحكام العامة الخاصة بها مرورا بمحطة التجريم والأحكام الإجرائية وصولا للتعاون القانوني والقضائي وبعض الأحكام الختامية الخاصة بها .

المبحث الأول

المعاهدات والقوانين الخاصة بحماية حق الملكية الفكرية

تعتبر حماية الملكية الفكرية هي من أكثر الحقوق التي يتم انتهاكها يوميا على شبكة الإنترنت وعلى كافة شبكات الاتصالات والمعلومات على مستوى العالم، وعليه فوجود معاهدات دولية تمنع تلك الانتهاكات، وإصدار كل دولة قوانين خاصة بها تعمل على حماية حقوق الملكية الفكرية، كل ذلك يؤدي إلى الحفاظ على تلك الحقوق من الانتهاك الذي يتم يوميا دون أي رادع يحمي أصحاب تلك الحقوق.

وسوف نتعرض أولا للمعاهدات التي تم إبرامها في هذا المجال، وسوف نعرض ثانيا لما تم إصداره من قوانين في هذا المجال خاصة في الدول العربية.[1]

المطلب الأول

المعاهدات الدولية التي تم إبرامها في مجال حماية حقوق الملكية الفكرية

سوف نتطرق لعدة معاهدات تخص هذا المجال ومنها:

[1]– منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع السابق، ص 199،200.

الفرع الأول

اتفاقية برن لحماية المصنفات الفنية والأدبية

تم اعتمادها من قبل الدول المتعاقدة في 9 سبتمبر 1886، وقد تجمعت الدول المتعاقدة على شكل إتحاد من أجل حماية حقوق مؤلف المصنفات المحمية بموجب الاتفاق، وسمي هذا الاتحاد بـ"**اتحاد برن**".

وينظر إلى "**اتفاقية برن**"، على أنها الأب الشرعي لتنظيم حقوق المؤلف والحقوق المجاورة على المستوى الدولي، خصوصا وأنها من أوائل الاتفاقيات التي تم التوصل لها لمعالجة سائل حقوق المؤلف.

وقد تمت مراجعة نصوص الاتفاقية عدة مرات، وتعرضت للتعديل أكثر من مرة في ضوء التطورات السريعة في مجال التكنولوجيا المتصلة بالمصنفات الأدبية والفنية، وقد كانت آخر ثلاث مراجعات خضعت لها الاتفاقية في بروكسل عام 1948، و ستوكهولم عام 1967، وفي باريس عام 1971.[1]

وقد انضمت إليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 341/97 في 13-09-1997، الذي يتضمن انضمام الجمهورية الجزائرية الديمقراطية الشعبية مع التحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية، التي كان لها عدة تعديلات أهمها تعديل باريس 1971 وآخرها في 28-9-1979.[2]

[1]- طلعت زايد، حق المؤلف وتشريعاته في الوطن العربي، مطابع مركز الدعم الإعلامي، الإسماعيلية، مصر، ديسمبر 2006، ص 30

[2]-المرسوم الرئاسي رقم 341/97، المؤرخ في 13-09-1997، ج ر ج ج، العدد 61 السنة 34 الموافق لـ14-9-1997م.

ولأهمية هذه الاتفاقية ودورها في توفير الحماية للمؤلفين وأعمالهم ولدت في أحكامها عدة نصوص ومبادئ.

أولا – المبادئ الأساسية للاتفاقية:[1]

تقوم هذه الاتفاقية على ثلاثة مبادئ رئيسية وهي:

1– مبدأ المعاملة الوطنية: ويعني هذا المبدأ بأن تتمتع المصنفات التي تم إعدادها في دولة من دول الاتحاد بالحماية في بقية دول الاتحاد، وبنفس مستوى الحماية الممنوح من تلك الدول لمصنفات مواطنيها.

2 – مبدأ الحماية التلقائية: وتعني أن المصنفات تحمي بشكل تلقائي للمصنفات وبمجرد تأليفها، ولا تتوقف على أي تسجيل أو إيداع أو أي إجراء شكلي آخر.

3– مبدأ استقلالية الحماية: وتعني أن التمتع بالحقوق الممنوحة للمصنف أو ممارستها لا يجوز أن تتوقف على وجود حماية في بلد المنشأ.

ثانيا– المصنفات المحمية بموجب اتفاقية برن:

تشمل عبارة المصنفات الأدبية والفنية كل إنتاج في المجال الأدبي والعلمي والفني أيا كانت طريقة أو شكل التعبير عنه مثل الكتب والكتيبات وغيرها من المحررات والمحاضرات والخطب والأعمال الأخرى وتعتبر هذه المصنفات المحمية على سبيل المثال لا الحصر، وقد تركت الاتفاقية حرية مد نطاق الحماية إلى بعض المصنفات الأخرى للدول الأعضاء، مثل حماية النصوص الرسمية ذات الطابع التشريعي أو الإداري أو القضائي، أو مصنفات الفنون التطبيقية والمحاضرات والخطب، إلا أن الاتفاقية قد اشترطت تثبيت بعض المصنفات على دعامة مادية كشرط للحماية.[2]

[1] - ar.m.wikipedia.org/wiki/...
الدخول يوم 01-03-2023 على الساعة 15:29
[2] - docdroid.net/UHT3G7I/sfh-khbraaa-almlky...
اتفاقية برن لحماية المصنفات الأدبية والفنية، وثيقة باريس 1971والمعدلة في سبتمبر 1979، الزيارة يوم 01–03–2023 على الساعة 18:00

الفرع الثاني

إتفاقية تربس ومعاهدة الويبو

أولا : إتفاقية تربس "اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية"

إن الكساد الاقتصادي العالمي الذي أصاب العالم بعد الحرب العالمية الثانية، قد حدا بالحلفاء آنذاك، بضرورة إنشاء نظام جديد للتجارة يهدف إلى إزالة العوائق التي تواجه التجارة، وبناءا على ذلك فقد تم في 30-10-1947م إقرار الاتفاقية العامة للتعريفات الجمركية والتجارة، أو ما عرفت لفترة طويلة باتفاقية "**الجات Gatt**"، إلا أنه وبعد مرور 47 عاما، وبعد إدراك الحاجة إلى إيجاد اتفاقية أخرى أكثر شمولا لتحل محل الاتفاقية الأولى، فقد تم في 15-4-1994 التوقيع على الوثيقة الختامية لنتائج جولة الأوروغواي للمفاوضات متعددة الأطراف، والتي انتهت بإنشاء منظمة التجارة العالمية "**wto**"، وقد تضمنت الاتفاقية العامة "**wto**"مجموعة من الاتفاقيات المتعددة الأخرى، والاتفاقية التي تهمنا في هذا المجال هي " اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية "، وتعرف "**باتفاقية تربس**"، والتي تقع في **73 مادة**، وتهدف إلى المساعدة في تحرير التجارة العالمية، عن طريق تشجيع وتحفيز حقوق الملكية الفكرية، وأن تضمن بأن لا تكون التدابير المتخذة لإنفاذ حقوق الملكية الفكرية بحد ذاتها عائقا أمام التجارة الدولية.[1]

1- المبادئ الأساسية لاتفاق تربس:

أ- مبدأ المعاملة الوطنية:

هذا المبدأ يعني معاملة الدولة للأجنبي نفس المعاملة التي يتلقاها أحد رعاياها في إقليم دولة الأجنبي، ولهذا فإن الدولة تحرص على زيادة الحقوق التي يمنحها للأجنبي حتى يتسنى لرعاياها المقيمين في دولة ذلك الأجنبي الحصول على نفس هذه الحقوق، ويعد هذا المبدأ من أهم المبادئ التي تؤدي إلى رفع مستوى الحماية المقررة لعناصر الملكية الفكرية ولقد نصت عليه المادة الثالثة من الاتفاقية .

[1] – طلعت زايد، المرجع السابق، ص34.

ب- مبدأ الدولة الأولى بالرعاية:

هذا المبدأ يلزم البلدان الأعضاء بألا تميز في المعاملة فيما يتعلق بعناصر حقوق الملكية الفكرية بين مواطني الدول الأعضاء وبالتالي يجب على الدول الأعضاء المساواة بين مواطني جميع الدول الأعضاء في الحقوق والالتزامات، وعليه وطبقا لهذا المبدأ فإن أية ميزة أو تفضيل أو امتياز أو حصانة يمنحها بلد عضو لمواطني أي بلد آخر، يجب أن يمنح على الفور دون أي شرط لمواطني البلدان الأعضاء الأخرى وهذا ما نصت عليه المادة الرابعة من هذا المبدأ .[1]

اتفاقية تربس تلزم البلدان الأعضاء بمراعاة الأحكام التي تنص عليها **المواد** من **1 وحتى 21** من معاهدة برن (1971) وملحقها، مع عدم إلزام الدول الأعضـــاء في الاتفاقية بالحقوق المنصوص عليها في **المادة 6 مكرر** من معاهدة برن أو الحقوق النابعة عنها.[2]

2- حقوق التأليف والحقوق المجاورة المحمية بموجب اتفاقية التريبس:

اتفاقية تربس تضمنت أحكام مجموعة من القواعد لحماية بعض المصنفات والمواضيع المتعلقة بحقوق التأليف والحقوق المجاورة، والتي تميزت في بعض الأحيان بالحداثة عما سبقها من اتفاقيات مماثلة، ومن ضمن تلك الأمور على سبيل المثال النص على **حماية برامج الحاسب الآلي وقواعد البيانات،** فقد تضمنت الاتفاقية **حماية برامج الحاسب الآلي** سواء كانت بلغة المصدر أو بلغة الآلة باعتبارها من الأعمال الأدبية وفق مفهوم أحكام اتفاقية برن لحماية المصنفات الأدبية والفنية لعام 1971 .[3]

كما نصت الاتفاقية كذلك على حماية البيانات المجمعة أو المواد الأخرى ، سواء كانت في شكل مقروء آليا أو أي شكل آخر، أو ما يسمى بقواعد البيانات إذا كانت تشكل عملا مبتكرا نتيجة انتقاء أو

[1]- زواني نادية، اتفاقية تربس وتأثيرها على البلدان النامية، مجلة البحوث، جامعة الجزائر، العدد09-الجزء الاول2016، ص14.

[2] - المادة 9-2/1 من اتفاقية تربس " اتفاقية جوانب حقوق الملكية الفكرية المتصلة بالتجارة ".

[3] - المادة 10-1 من اتفاقية تربس " اتفاقية جوانب حقوق الملكية الفكرية المتصلة بالتجارة ".

ترتيب محتوياتها، وأن الحماية لا تشمل البيانات أو المواد في حد ذاتها، مع عدم الإخلال بحقوق المؤلفين المتعلقة بتلك البيانات أو المواد ذاتها.[1]

وحسب المادة 11 من نفس الاتفاقية نصت وبشكل إلزامي للبلدان الأعضاء في" wto"بمنح المؤلفين وخلفائهم حق إجازة أو حظر تأجير أعمالهم الأصلية المحمية تأجيرا تجاريا للجمهور ، وقد قيدت الاتفاقية أيضا حق الإجازة أو الحظر على التأجير فيما يتعلق ببرامج الحاسب الآلي حينما لا يكون البرنامج نفسه الموضوع الأساسي للتأجير.[2]

ثانيا– معاهد الويبو(WIPO) المنظمة العالمية للملكية الفكرية

هي منظمة متخصصة للأمم المتحدة مسئولة عن تعزيز وحماية الملكية الفكرية على أساس دولي، ويتسم عملها بكونه تكميليا لمنظمة التجارة العالمية، وهي تبحث في إنشاء الآليات التعاونية التي تحد من المشكلات التي تواجه الملكية الفكرية، وهذه المنظمة هي التي عقدت مؤتمرها الدولي الذي تمخض عام 1996 عن اتفاقية حق النشر للمنظمة العالمية للملكية الفكرية، المتضمنة لحق النشر للمنظمة العالمية للملكية الفكرية المتضمنة لحق النشر المرتبط **بالتكنولوجيا الرقمية،** وخاصة **الإنترنت،** كما أن هذه المنظمة هي المسئولة عن الاتفاقيات المتعددة الأطراف، مثل اتفاقية برن المتعلقة بالملكية الفكرية لعام 1997.[3]

معاهدة الويبو تنقسم إلى عدة معاهدات أهمها، معاهدة الويبو بشأن حق المؤلف.

معاهدة الويبو بشأن حق المؤلف:[4]

تم اعتمادها في جنيف في 20ديسمبر/كانون الأول 1996، وتتكون المعاهدة من 25 مادة، وتبدأ بالديباجة إذ تقر فيها بما لتطور تكنولوجيا المعلومات والاتصالات وتقاربها من أثر عميق في ابتكار المصنفات الأدبية والفنية والانتفاع بها، وإذ تشدد على ما للحماية الممنوحة بموجب حق

[1] – المادة 10–2 من اتفاقية تربس، المصدر السابق.

[2] – المادة 11 من اتفاقية تربس، المصدر نفسه.

[3] – محمد محمود المكاوي، المرجع السابق، ص 408.

[4] – معاهدة الويبو بشأن حق المؤلف (لسنة 1996)

Wipolex.wipo.int/ar/text/295156

المؤلف من أهمية بارزة في حق الابتكار الأدبي والفني[1]، ثم تناولت علاقة هذه المعاهدة باتفاقية برن في المادة الأولى، ثم تعرضت لنطاق حماية حق المؤلف في المادة الثانية بقولها تشمل الحماية الممنوحة بموجب حق المؤلف أوجه التعبير وليس الأفكار أو الإجراءات أو أساليب العمل أو مفاهيم الرياضيات في حد ذاتها[2]، وتطرقت في المادة الرابعة لبرامج الحاسوب معبرة على أنها تتمتع بالحماية باعتبارها مصنفات أدبية بمعنى المادة 2 من اتفاقية برن ، وتطبق تلك الحماية على برامج الحاسوب أيا كانت طريقة التعبير عنها أو شكلها . [3]

كما تطرقت لحق التوزيع وحق التأجير، وحق نقل المصنف إلى الجمهور، كما تطرقت للالتزامات المتعلقة بالتدابير التكنولوجية في مادتها الحادية عشر باعتبارها أنه على الأطراف المتعاقدة أن تنص في قوانينها على حماية مناسبة وعلى جزاءات فعالة ضد التحايل على التدابير التكنولوجية الفعالة التي يستعملها المؤلفون لدى ممارسة حقوقهم بناء على هذه المعاهدة أو اتفاقية برن والتي تمنع من مباشرة أعمال لم يصرح بها المؤلفون المعنيون أو لم يسمح بها القانون، فيما يتعلق بمصنفاتهم[4]، والالتزامات المتعلقة بالمعلومات الضرورية لإدارة الحقوق، وكذلك الحقوق والالتزامات المترتبة على المعاهدة ودخول المعاهدة حيز التنفيذ، وتطرقت لنقطة التحفظ على المعاهدة وكذا نقضها وكذا لغات المعاهدة.[5]

و نصت المادة 20 من اتفاقية برن، على أن تحتفظ حكومات دول الاتحاد بالحق في عقد اتفاقيات خاصة فيما بينها مادامت هذه الاتفاقيات تخول حقوقا تفوق تلك التي تمنحها هذه الاتفاقية، أو تتضمن نصوصا لا تتعارض مع هذه الاتفاقية .

وكانت للنص السالف الذكر من المادة الأولى من المعاهدة الأولى بالتالي أهمية خاصة في تفسير المعاهدة، إذ أنه يبين أن تفسير المعاهدة الذي قد يؤدي إلى الحد من الحماية التي تمنحها اتفاقية برن يعتبر مرفوضا.

---

[1] – ديباجة معاهدة الويبو بشأن حق المؤلف (لسنة 1996)، المصدر السابق.

[2] – المادة الثانية من معاهدة الويبو بشأن حق المؤلف (لسنة 1996)، المصدر نفسه.

[3] – المادة الرابعة من معاهدة الويبو بشأن حق المؤلف (لسنة 1996)، المصدر نفسه.

بيان متفق عليه بشأن المادة 4: يتمشى نطاق الحماية الممنوحة لبرامج الحاسوب بناء على المادة 4 من هذه المعاهدة، بالاقتران بالمادة2، مع المادة 2 من اتفاقية برن، ويتساوى والأحكام المعنية من اتفاق تربس.

[4] – المادة 11 معاهدة الويبو بشأن حق المؤلف (لسنة 1996)، المصدر نفسه.

[5] – معاهدة الويبو بشأن حق المؤلف (لسنة 1996)، المصدر نفسه.

وتعطي المادة الرابعة من المعاهدة الأولى ضمانا إضافيا للالتزام باتفاقية برن بأكبر قدر ممكن، إذ أنها تضم جميع الأحكام الجوهرية لاتفاقية برن بالإحالة إليها، و تنص على أن (على الأطراف المتعاقدة أن تراعي المواد من 1 إلى 21 والملحق من اتفاقية برن).[1]

وتوضح المادة الثالثة أن اتفاقية برن تشير في ذلك السياق إلى وثيقة باريس لاتفاقية برن سنة 1971.

وينبغي قراءة تلك النصوص على ضوء أحكام المادة 17 من المعاهدة، وبناء على تلك المادة، لا تكون المعاهدة متاحة للبلدان الأطراف في وثيقة باريس لسنة 1971 والبلدان الأطراف في آية وثيقة من وثائق اتفاقية برن فحسب، بل بالنسبة أيضا إلى كل دولة عضو في الويبو، سواء كانت طرفا في الاتفاقية أو لم تكن طرفا فيها، ويجوز لبعض المنظمات الدولية الحكومية أيضا أن تصبح أطرافا في المعاهدة.

وتحتوي المادة الثانية من المعاهدة الأولى بند ضمان مشابها للبند الوارد في المادة 2-2 من اتفاق تربس، ونصت على أنه ليس في هذه المعاهدة ما يحد من الالتزامات المترتبة على الأطراف المتعاقدة بعضها تجاه البعض الآخر بناء على اتفاقية برن لحماية المصنفات الأدبية والفنية، غير أن نطاق ذلك البند يختلف عن نطاق البند الوارد في اتفاق تربس وينطوي الأخير على أهمية من وجهة نظر مادة واحدة على الأقل من اتفاقية برن تضم أحكاما جوهرية، أي المادة السادسة المتعلقة بالحقوق المعنوية، إذ لا ينص اتفاق تربس على أية حقوق أو التزامات فيما يتعلق بتلك المادة.[2]

المطلب الثاني

القوانين التي أصدرتها الجزائر و بعض الدول العربية في مجال حماية حقوق الملكية الفكرية

سوف نتعرض في هذه الدراسة لبعض القوانين في دول معينة في مجال حماية حقوق الملكية الفكرية.

[1]– منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع السابق، ص 202 ،203.

[2]– منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع نفسه، ص 204.

الفرع الأول

الحماية من الجرائم المعلوماتية من خلال قانون الملكية الأدبية والفنية في الجزائر

في الجزائر قبل الاستقلال كانت الحماية المقررة لحقوق المؤلف هو ما كان مطبقا في القانون الفرنسي، والتي ظلت سارية المفعول إلى غداة الاستقلال.

وبتاريخ25 فيفري صدر أمر رقم 66-48 يقضي بانضمام الجزائر إلى اتفاقية باريس لحماية الملكية الصناعية.

وفي 3-4-1973 صدر تشريع رقم 73- 14 المتعلق بحق المؤلف، وفي 05 جوان 1973 انضمت الجزائر إلى الاتفاقية العالمية لحماية حقوق المؤلفين المبرمة سنة1952 وذلك بمقتضى الأمر 73- 26 .

بتاريخ 29 جويلية بمقتضى تشريع 73- 46 أنشأت الجزائر الديوان الوطني لحق المؤلف.

و بمقتضى تشريع رقم 97-10 المؤرخ في 6-3-1997م صدر القانون المتعلق بحقوق المؤلف والحقوق المجاورة، والذي تم تعديله بمقتضى أمر 03-05 المؤرخ في19-7-2003م.[1]

إن المتضرر الأول من إساءة استخدام شبكة المعلوماتية حقوق الملكية الفكرية سواء ما يتعلق منها بحقوق المؤلف أو الحقوق المجاورة أو المتعلقة بالبرامج والإصدارات الخاصة بنظم المعلومات أو المصنفات الفكرية أو الأدبية أو الأبحاث العلمية التي باتت متاحة على شبكة المعلوماتية، ويتم نسخها وتداولها دون أن تنسب إلى صاحبها الأصلي، وهو ما يلحق ضررا بليغا بهذه الطائفة من الحقوق التي تعرف بالذهنية أو الفكرية، و مما لا شك فيه أنه يجب التشدد في مواجهة منتهكي حقوق الملكية الفكرية، خاصة وأن القوانين ذات العلاقة لم تجرم الأفعال التي تتم بإساءة استخدام تقنية المعلوماتية هذا من ناحية، ومن ناحية أخرى أي قانون حماية المؤلف والحقوق المجاورة الوطني لا زال قاصرا في مواجهة هذه الانتهاكات.[2]

---

[1]- فاضلي إدريس، حقوق المؤلف والحقوق المجاورة، ديوان المطبوعات الجامعية، الجزائر 2015 ص 19 ،20.

[2]-فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان يومي 24 -25 /03/ 2017، ص 115.

جاء الأمر 03-05 المعدل لأمر 97-10 منسجما مع التطور العلمي المتسارع والمتعاقب، وما اقتضاه ذلك من وجوب بسط الحماية على برنامج الكمبيوتر أو الحاسوب نظرا لما تطلبه تكوينه من عمل ذهني، وقد جاء التنصيص على ذلك بوضوح في المادة الرابعة فقرة(أ) بعبارة "برنامج الحاسوب"كمصنف من المصنفات الأدبية الأصلية المحمية وهو مصنف من نوع خاص، فالحماية المقررة قانونا لا تشمل إلا برنامج الحاسوب وليس سنده المادي الذي يستفيد هو الآخر من الحماية المقررة على ضوء براءة الاختراع متى توفرت شروطها، أما شكل البرنامج الذي يظهر على الشاشة فحمايته كقاعدة عامة تخضع لنظام الرسوم والنماذج الصناعية، في حين وظائفه غير محمية، وكذلك الأفكار التي كانت مصدر هذا العمل الإبداعي، فحقوق المؤلف لا تسري حمايتها على الأفكار ولا مصدر وظائف "اللوجسيال"، إن الحماية المقررة للمصنفات الفكرية بما فيها " اللوجسيال" لا تتطلب إجراءات إيداع ، فالحماية تمنح على أسس الابتكار، إن صاحب اللوجسيال يتمتع بحقوق معنوية ومادية على مصنفة شأنه في ذلك شأن أي مالك لمصنف أدبي كحقه في ذكر اسمه على دعائم المصنف، وتقرير الكشف على مصنفة و وضعه في التداول بواسطة التأجير التجاري طبقا لنص المادة 27-2 من أمر 03-05.[1]

المشرع الجزائري حول التصدي الجريمة المعلوماتية من خلال قانون الملكية الأدبية والفنية المتعلق بحق المؤلف والحقوق المجاورة الصادر بموجب الأمر رقم 03-05 المؤرخ في 23-07- 2003 المتعلق بحقوق المؤلف والحقوق المجاورة حيث وسع قائمة المؤلفات المحمية، وذلك بإدماج برامج المعلوماتية ضمن المصنفات الأصلية والتي عبر عنها بمنصفات قواعد بيانات برامج المعلوماتية، كما شدد العقوبات على المساس بحقوق المؤلفين خاصة المصنفات الرقمية التي تشملها الحماية المذكورة.[2]

---

[1]- فاضلي إدريس، المرجع السابق، ص 84،85.

[2]-حنان مسكين، واقع مكافحة الجرائم المعلوماتية واتجاهاتها التشريعية في الجزائر، مقال منشور بالمجلة الأكاديمية للبحوث القانونية السياسية، المجلد الرابع، العدد الأول، سنة 2020، ص 620.

وقواعد البيانات هي مجموعة معطيات أو أعمال في شكل ممنهج، يتم الدخول إليها بوسائل إلكترونية أو بأي وسائل أخرى.[1]

أكد المشرع الجزائري في القانون 03-05 على أن المصنف الفكري يعتبر من معطيات الحاسب الآلي التي تحتاج إلى حماية وعقوبة على من يتعدى على الحق المالي أو الأدبي لمؤلف البرنامج و البيانات،[2]ويشكل فعل من أفعال التقليد المنصوص عليها في المادة 151 من الأمر رقم 03-05، التي تقرر العقوبات الجزائية المكرسة في المواد 153، 156، 157، 158 من الأمر نفسه، و تحدد المادة 151 فقرة واحد من الأمر رقم 03-05 الجنح المرتبطة بالحق المعنوي للمؤلف، وهي تتمثل في الكشف غير المشروع عن المصنف الأدبي والفني، كأن يتم الكشف عن برنامج في الوقت أو بطريقة يرى المؤلف أنها غير مناسبة، والمساس بسلامة المصنف الأدبي أو الفني، كأن يقوم شخص بتعديل أو تغيير أو حذف أو إضافة أو تحويل على البرنامج أو بيانات الحاسب دون إذن من المؤلف.[3]

أما الجنح المرتبطة بالحق الأدبي للمؤلف فتتمثل في الاستنساخ غير الشرعي للمصنف، يعتمد على قيام الشخص باستنساخ برامج أو بيانات الحاسب بأي أسلوب كان وجعله في شكل نسخ مقلدة دون إذن المؤلف، كذلك الإبلاغ غير الشرعي للمصنف كأن يقوم شخص بإبلاغ وإعلام عموم الجمهور

[1] - David Forest et Gautier Kaufman, Droit de L'informatique, Gualino éditeur , Extenso édition, France,2010, p29.

[2]– يعرف برنامج الكمبيوتر كونه هو جميع العناصر غير المادية وغير الملموسة اللازمة لتشغيل أجهزة الكمبيوتر، فهو بمثابة مجموعة أوامر وتعليمات قابلة للتنفيذ، ولا يتعدى هذا التعريف عما عرفته المنظمة العالمية للملكية الفكرية " ويبو" بقولها بأن البرنامج هو مجموعة من تعليمات يمكنها أن تساعد في الوصول إلى خاصية أو نتيجة ما في حال إذا نقلت على ركيزة أو دعامة تستوعبها وبواسطة آلة بإمكانها التعامل مع المعلومة، وتختلف في كونها برامج تشغيل وبرامج تطبيق، وتختلف برنامج الحاسوب على قاعدة البيانات والتي هي بمثابة بنك معلومات، وهي مجموعة البيانات التي تخزن و تسترجع وتعطي المعرفة أو ما يسمى بالمعلومة، وبقدر ما هي ناتج فكري مرتبط بصاحبه فهي بمثابة مصف يحميه القانون بما في ذلك مواقع الويب، من المعلوم أن حق المؤلف يعد الوسيلة الأقرب لحماية حقوق المبدعين، وهو حق ذو طبيعة مزدوجة معنوي ومادي أو مالي وفي مجمعها تسند إلى أحكام اتفاقية يرن لحماية المصنفات الإدارية والفنية والمبرمة سنة 1886، وتعد الاتفاقية الأولى في المجال الدولي لحماية حق المؤلف عدلت في باريس بتاريخ 24 جويلية 1971 ...–هذا عن الأستاذة زيبحة زيدان، المرجع السابق، ص 87.

[3]– بدر الدين خلاف، التنظيم القانوني للجريمة المعلوماتية في الجزائر، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة ،الجزائر، المجلد السادس، العدد الثاني، جوان 2021 ص 343، 344.

بمصنف برنامج وبيانات الحاسب دون علم وترخيص من المؤلف سواء كان الإبلاغ مباشر أو غير مباشر.

أما الجنح المرتبطة بالمصنف المقلد فهي تتعلق بالتصرفات والتعاملات التي ترد على المصنف المقلد، الذي يمكن أن يكون برنامج أو بيانات الحاسب الآلي، وفيما يتعلق بالعقوبات المقررة لهذه الجناح، حددت المادة 153 من الأمر رقم 03-05 عقوبات أصلية تتمثل في عقوبة الحبس من 06 أشهر إلى 03 سنوات على كل من ارتكب جنحة تقليد مصنف بما فيها المصنفات المعلوماتية، وبغرامة مالية تتراوح بين 500,000دج و1000,000دج، إضافة إلى عقوبات تكميلية تتمثل في:

- مصادرة المبالغ المساوية لإقساط الإيرادات المحصلة من الاستغلال غير المشروع للمصنف.
- مصادرة وإتلاف كل عتاد انشأ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة.
- الأمر بطلب من المتضرر بتعليق ونشر أحكام الإدانة على نفقة المحكوم عليه.[1]

الفرع الثاني

القوانين التي أصدرتها بعض الدول العربية في مجال حماية حقوق الملكية الفكرية

سوف نتطرق لمجال حماية حقوق الملكية الفكرية في كل من جمهورية مصر العربية و سوريا، وكذلك الإمارات العربية المتحدة والكويت.

أولا – حماية الملكية الفكرية في جمهورية مصر العربية:

يرى بعض من الفقه المصري أن برامج الحاسب الآلي كانت تدخل ضمن المصنفات المحمية في ظل القانون رقم 354 لسنة 1954، وذلك استنادا لنص المادة الأولى والثانية منه[2]الخاص بحماية حق المؤلف، والذي يعد أول التشريعات العربية بعد الاستقلال العربي، والذي عدل بالقانون رقم 38 لسنة 1992، وعدل أيضا بالقانون رقم 29 لسنة 1994، وفي يونيو سنة 2002 صدر القانون رقم 82

[1]– بدر الدين خلاف، المرجع السابق ،ص 343، 344.

[2] – هناء مصطفى الخبيري، المرجع السابق، ص108.

الخاص بحماية حقوق الملكية الفكرية ليلغي القانون السابق، وقد نص في المادة 140 منه على أنه " تتمتع بحماية هذا القانون حقوق المؤلفين على مصنفاتهم الأدبية والفنية وبوجه خاص المصنفات الآتية:-.....،2-برامج الحاسب الآلي،3- قواعد البيانات سواء كانت مقروءة من الحاسب الآلي أو من غيره....."، وقد تم تشديد عقوبة الاعتداء على حقوق المؤلفين، حيث نصت المادة 181 من القانون رقم 82 لسنة 2002 على أن " مع عدم الإخلال بأية عقوبة أشد في قانون آخر، يعاقب بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن 5.000 جنيه. ولا تتجاوز 10,000 جنيه، أو بإحدى هاتين العقوبتين كل من ارتكب الأفعال الآتية:..... سابعا- نشر مصنف أو تسجيل صوتي أو برنامج إذاعي أو أداء محمى طبقا لأحكام هذا القانون عبر أجهزة الحاسب الآلي أو شبكات الإنترنت أو شبكات المعلومات أو شبكات الاتصالات، أو غيرها من الوسائل بدون إذن كتابي مسبق من المؤلف أو صاحب الحق المجاورة" .[1]

ثانيا - حماية الملكية الفكرية في التشريع السوري:

حدد المشرع السوري في المادة الثالثة من قانون حقوق المؤلف رقم 12 لسنة 2001 نطاق الحماية القانونية التي كفلها المشرع، والتي تشمل البيانات المعالجة الآلية، لنصها على أن " تتمتع جميع المصنفات بالحماية وفق أحكام هذا القانون وتشمل الحماية بصفة خاصة ما يلي:.....

هـ- مصنفات البرمجيات الحاسوبية بما في ذلك وثائق تصميمها ومجموعات البيانات، وتشمل الحماية عنوان المصنف ، إلا إذا كان العنوان لفظا جاريا للدلالة على موضوع المصنف".

كما نصت المادة 40 من الأفعال المجرمة والعقوبة المستحقة لمرتكبيها لنصها على أن " يعاقب بالحبس من ثلاثة أشهر إلى سنتين وبغرامة لا تقل عن 100,000 ليرة سورية أو بإحدى هاتين العقوبتين.

1- كل من اعتدى على أي حق من الحقوق المشمولة بالحماية في المواد 7،6.5. من هذا القانون.

2- كل من نسب لنفسه مصنفا ليس من تأليفه....

[1]- مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي "دراسة مقارنة"، دار النهضة العربية ،القاهرة، مصر، الطبعة الأولى 2015 ص55 ،56.

3- كل من تصرف أو حاز أو عرض للبيع أو أذاع على الجمهور بأية وسيلة كانت أو أدخل إلى أراضي الجمهورية العربية السورية مصنفا مخالفا بذلك، أحكام الحماية المقررة بموجب هذا القانون بقصد الاستغلال التجاري.

4- كل من أعاد في الجمهورية العربية السورية إنتاج مصنفات محمية مخالفا أحكام هذا القانون، وكذلك كل من باع هذه المصنفات أو أصدرها أو تولى نقلها أو نشرها أو تأجيرها، وهو يعلم بالمخالفة، وتعدد العقوبات بتعدد المصنفات موضوع الاعتداء".

وقد شدد المشرع العقوبة في حالة العود وذلك بمضاعفة العقوبة (المادة 41 من القانون)، كما نصت على أن تضاعف العقوبة المنصوص عليها في المادة السابقة في حالة التكرار.[1]

ثالثا- حماية الملكية الفكرية في التشريع الإماراتي:

إن القانون الاتحادي رقم (40) لسنة 1992 في شأن حماية المصنفات الفكرية وحقوق المؤلف حسب المادة الثانية منه، بأن يتمتع بالحماية المقررة في هذا القانون مؤلفو المصنفات الفكرية المبتكرة في الآداب والفنون والعلوم ، أيا كانت قيمة هذه المصنفات أو نوعيتها أو الغرض من تأليفها أو طريقة التعبير عنها، وتشمل الحماية المصنفات الفكرية الآتية:.....

ز- المصنفات السينمائية والتلفزيونية والإذاعية والأعمال الإبتكارية السمعية والبصرية وبرامج الحاسوب.[2]

وبالتالي، يصبح نسخ المواد المحمية بموجب قانون حماية الملكية الفكرية من غير إذن أو توزيع نسخها عملا غير قانوني فلا يجوز صنع أية نسخ من غير إذن صريح من صاحب حق الملكية الفكرية، يمنع قانون دولة الإمارات العربية المتحدة نسخ برامج الكمبيوتر بدون إذن، وكل من يقبض عليه متلبسا بقرصنة البرامج سيخضع هو وشركته للمحاكمة بموجب القانون المدني أو الجنائي،

[1]- محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت "دراسة مقارنة"، دار الفكر والقانون، المنصورة، مصر، الطبعة الأولى 2013 ص 83 ، 84.

[2]- القانون الاتحادي رقم 40 لسنة 1992 في شأن حماية المصنفات الفكرية وحقوق المؤلف .

وتشمل العقوبات حسب القانون غرامة مالية قدرها 50000 درهم أو أكثر، بالإضافة إلى مصادرة المنتجات والحبس لمدة تصل إلى ثلاث سنوات.[1]

رابعا – حماية الملكية الفكرية في التشريع الكويتي:

حسب القانون رقم 64 لسنة 1999 في شأن حقوق الملكية الفكرية، يتمتع بحماية هذا القانون حسب المادة الأولى منه مؤلفو المصنفات المبتكرة في الآداب والفنون والعلوم أيا كانت قيمة هذه المصنفات أو نوعها أو الغرض من تأليفها أو طريقة التعبير عنها، ويعتبر مؤلفا الشخص الذي يبتكر المصنف أو ينسب إليه عند نشره، سواء أكان ذلك بذكر اسمه على المصنف أو بأي طريقة أخرى، إلا إذا قام الدليل على خلاف ذلك، وتشمل الحماية بصفة خاصة حسب **المادة الثانية الفقرة كمصنفات الحاسب الآلي من برامج وقواعد بيانات وما يماثلها.**

أما بالنسبة للجزاءات المترتبة عن هذا القانون، فحسب **المادة 42 فقرة ج** يعاقب بالحبس مدة لا تزيد عن سنة واحدة وبغرامة لا تزيد عن 500 دينار أو بإحدى هاتين العقوبتين كل من كشف أو سهل كشف برامج الحاسب الآلي قبل نشرها، ويجوز للمحكمة أن تقضي بمصادرة جميع الأدوات المخصصة للنشر غير المشروع، إذا كانت لا تصلح إلا لهذا النشر، وكذلك بمصادرة جميع النسخ، كما يجوز لها أن تأمر بنشر الحكم في جريدة واحدة أو أكثر على نفقة المحكوم عليه.

وإذا سبق الحكم على المتهم بعقوبة لارتكابه هذه الجريمة، جاز للمحكمة أن تقضي فيه في هذه الجريمة بعقوبة تزيد على الحد الأقصى المقرر قانونا، بشرط ألا تتجاوز الزيادة نصف هذا الحد، و بغلق المنشأة التي استغلت في ارتكاب الجريمة لمدة لا تزيد ستة أشهر.[2]

ثم جاء القانون رقم 22 لسنة 2016 في شأن حقوق المؤلف والحقوق المجاورة.

لكن تم إلغاء هذا القانون والقانون 64 لسنة 1999 في شأن حقوق الملكية الفكرية بمجيء القانون رقم 75 لسنة 2019 في شأن حقوق المؤلف والحقوق المجاورة، وهذا حسب المادة 49 منه.[3]

---

[1]– منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع السابق، ص 206.

[2]– القانون الكويتي رقم 64 لسنة 1999 في شأن حقوق الملكية الفكرية.

[3]– المادة 49 "يلغي القانون رقم 22 لسنة 2016 في شأن حقوق المؤلف والحقوق المجاورة والقانون رقم 64 لسنة 1999 في شأن حقوق الملكية الفكرية، كما يلغي كل نص يخالف أحكام هذا القانون".

فالمادة 43 منه عاقبت بالحبس مدة لا تقل عن ستة أشهر ولا تزيد عن سنتين وغرامة لا تقل عن 500 دينار ولا تزيد عن 50,000 دينار أو إحدى هاتين العقوبتين، كل من قام بغير إذن كتابي من المؤلف أو صاحب الحق المجاور، أو من يخلفهما بالاعتداء من جهة على حق من الحقوق الأدبية أو المالية للمؤلف أو صاحب الحقوق المجاورة المنصوص عليها في هذا القانون، بما في ذلك إتاحة أي مصنف للجمهور أو عرض أي مصنف أو أداء أو تسجيل صوتي أو برنامج البث مما تشمله الحماية المقررة في هذا القانون عبر **أجهزة الحاسب الآلي أو شبكات المعلومات أو شبكات الاتصالات أو غيرها من الطرق أو المسائل الأخرى.**

ومن جهة أخرى ببيع أو تأجير مصنف أو تسجيل صوتي أو برنامج بيت محمي طبقا لأحكام هذا القانون أو طرحه للتداول بأي صورة من الصور.[1]

أما حسب المادة 44 من نفس هذا القانون يعاقب بالحبس لمدة لا تقل عن ستة أشهر ولا تزيد على سنتين وبغرامة لا تقل عن 1000 دينار ولا تزيد عن 100,000 دينار أو بإحدى هاتين العقوبتين، كل من ارتكب أيا من الأفعال الآتية:

– تصنيع أو تجميع أو استيراد أو تصدير بغرض البيع أو التأجير أو الاتجار أو توزيع أي جهاز أو وسيلة أو أداة مصممة أو معدة خصيصا للتحايل على الحماية التكنولوجية التي يستخدمها المؤلف أو صاحب الحق المجاور.

– اختراق تدابير الحماية التكنولوجية التي يستخدمها المؤلف أو صاحب الحق المجاور لحماية الحقوق المنصوص عليها في هذا القانون أو للمحافظة على جودة ونقاء نسخ المصنفات دون وجه حق.

– إزالة أو تعطيل أو تعيب لأي حماية تقنية أو معلومات إلكترونية تستهدف تنظيم وإدارة المعلومات الضرورية لإدارة الحقوق المقررة في هذا القانون دون وجه حق.

– حذف أو تغيير أي معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق المقررة في هذا القانون دون وجه حق.

[1]– المادة 43 من القانون رقم 75 لسنة 2019 في شأن حقوق المؤلف الكويتي والحقوق المجاورة.

– توزيع أو استيراد لأغراض التوزيع أو بث أو نقل إلى الجمهور أو الإتاحة له مصنفات أو موضوعات الحقوق المجاورة أو نسخ منها مع علمه أنه قد حذفت منها أو غيرت فيها معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق المقررة في هذا القانون دون وجه حق.

– تخزين أو تحميل أي نسخة من برامج الحاسب الآلي أو تطبيقاته أو قواعد البيانات على الحاسب الآلي دون إجازة من المؤلف أو صاحب الحق المجاور أو خلفهما.[1]

كما حسب المادة 45 من نفس هذا القانون للمحكمة الحكم بمصادرة النسخ محل الجريمة أو المتحصلة منها، وكذلك المعدات والأدوات التي استخدمت في ارتكابها، وللمحكمة أن تأمر بإتلافها فيما عاد الأعمال المعمارية المشيدة وفق الاشتراطات البيئية.

كما يجوز للمحكمة عند الحكم بالإدانة أن تحكم بإغلاق النشأة التي ارتكبت فيها الجريمة مدة لا تتجاوز ستة أشهر، كما يجوز لها الحكم بسحب الترخيص و بغلق المنشأة نهائيا في حالة العود.

وللمحكمة أن تأمر بنشر ملخص الحكم النهائي الصادر بالإدانة في جريدتين يوميتين على نفقة المحكوم عليه .

وحسب المادة 46 في حالة العود إلى ارتكاب إحدى الجرائم المشار إليها في المادة 43، 44 من هذا القانون خلال خمس سنوات من تاريخ الحكم النهائي يزاد الحد الأقصى للعقوبة المقررة قانونا بمقدار النصف.[2]

المبحث الثاني

الاتفاقيات الدولية في مجال مكافحة الجريمة السيبرانية

تعد الاتفاقيات والمعاهدات الدولية من أهم صور التعاون الدولي بصفة عامة، وفي مجال مكافحة الجرائم الناتجة عن الإجرام المعلوماتي بصفة خاصة[3]، ومن بين المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، معاهدة بودابست لمكافحة جرائم الانترنت، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وسوف نتطرق إليهما فيما يلي :

[1]– المادة 44 من القانون رقم 75 لسنة 2019 في شأن حقوق المؤلف والحقوق المجاورة الكويتي.

[2]– المادة 45، 46 من القانون رقم 75 لسنة 2019 في شأن حقوق المؤلف والحقوق المجاورة الكويتي.

[3] - Robert O, Keohan, After Hegmony , Cooperation And Discord In The World Political Economy, Princeton University Press1984,p51.

المطلب الأول

معاهدة بودابست لمكافحة جرائم الإنترنت "اتفاقية بشأن الفضاء الإلكتروني"

حرص مجلس أوروبا على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات، وتجلي ذلك في اتفاقية بودابست الموقعة في 23 نوفمبر 2001 المتعلقة بالإجرام الكوني، بمعنى الإجرام المعلوماتي أو الجرائم المعلوماتية، إيمانا من الدول الأعضاء في هذا المجلس والدول الأخرى الموقعة على هذه الاتفاقية بالتغيرات العميقة التي حدثت بسبب الرقمية، والتقارب، والعولمة المستمرة للشبكات المعلوماتية.[1]

وقد تم صياغة هذه الاتفاقية من جانب عدد كبير من الخبراء القانونين في مجلس أوروبا وبمساعدة دول أخرى، لاسيما الولايات المتحدة الأمريكية، وبعد مشاورات عديدة بين الحكومات وأجهزة الشرطة وقطاع الكمبيوتر على مستوى العالم.[2]

وبعد التوقيع على تلك المعاهدة الدولية التي تهدف إلى توحيد الجهود الدولية في مجال مكافحة جرائم المعلوماتية، والتي انتقلت من مرحلة ابتدائية كانت تتمثل في محاولات التسلل البريئة، التي كان يقوم بها هواة في الأغلب الأعم من الحالات، ودون أي غرض إجرامي إلى مرحلة جديدة يقوم بها محترفون على أعلى درجة من التخصص، وتتمثل في الاحتيال والاختلاس وجرائم تهديد الحياة، وهي قضايا تعرض حياة وممتلكات الكثير من رواد شبكة الإنترنت للخطر، هي الخطوة الأولى في مجال تكوين تضامن دولي مناهض لتلك الجرائم التي تتم على شبكة الإنترنت، واستخدامها الاستخدام الأسوأ، وبعد التوقيع على تلك الاتفاقية من المسئولين في الدول الأوروبية إضافة إلى أمريكا واليابان وكندا وجنوب إفريقيا، هو نتاج مباحثات ومفاوضات استغرقت أكثر من أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لتلك الاتفاقية، حتى يتم التوقيع عليها من جميع الأطراف دون أن تجد

---

[1]- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص5.

[2] – محمد علي العريان، المرجع السابق، ص 25.

حيث تم التوقيع عليها في النهاية من قبل ثلاثون دولة بتاريخ 23 نوفمبر 2001.

أي اعتراض من أي منهم، بل على العكس لتجد القبول من أطراف جدد ليتم توسيع دائرة الدول التي توافق على الانضمام في تلك الاتفاقية، ويتم توسيع الاتحاد الدولي والتضامن الدولي.[1]

الفرع الأول

معاهدة بودابست لمكافحة جرائم الانترنت قبل البروتوكول الإضافي الثاني لها

أولا–الجرائم التي قسمتها الاتفاقية

ذهبت هذه الاتفاقية إلى تقسيم هذه الجرائم إلى أربعة أقسام رئيسية.

1– الجرائم ضد سرية وسلامة وإتاحة البيانات ونظم المعلوماتية، كالولوج غير القانوني والاعتداء على سلامة البيانات وسلامة النظام، وإساءة استخدام الحاسب وجرائم تدمير البيانات.

2– الجرائم المعلوماتية المرتبطة بالحاسب كالتزوير المعلوماتي والاحتيال المعلوماتي.

3– الجرائم المعلوماتية المتعلقة بالمواد الإباحية و الغير أخلاقية.

4– فتتعلق بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة وقرصنة البرمجيات.[2]

ثانيا– مكونات الاتفاقية

تتكون الاتفاقية من ديباجة و عدد ثماني وأربعون مادة موزعة على **أربعة أبواب**.

الأول: يعالج استخدام المصطلحات، و**الثاني** يبين الإجراءات الواجب اتخاذها على المستوى المحلي والقانون الموضوعي والقانون الإجرائي، و**الثالث** مخصص للتعاون الدولي، **والباب الرابع** يحدد الأحكام الختامية.[1]

[1]– محمود مدين، المرجع السابق، ص 157.

[2]– عمار عباس الحسني، المرجع السابق، ص104.

1- استخدام المصطلحات: حيث تطرق **الباب الأول** إلى تعبير:

أ- نظام معلوماتي Systéme informatique .

ب- البيانات المعلوماتية Données informatiques .

ج- مقدم الخدمة fournisseur de service.

د- البيانات المتعلقة بالمرور Données relatives au traffic .....[2]

2-الإجراءات الواجب اتخاذها على المستوى المحلي والقانون الموضوعي والقانون الإجرائي: هنا الباب الثاني قسم لعدة فصول:

أ- الفصل **الأول** تطرق للجوانب الموضوعية للجرائم المعلوماتية الذي قسم إلى عدة مباحث، حيث المبحث **الأول** للجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية مقسما إلى:الولوج غير القانوني، الاعتراض غير القانوني،الاعتداء على سلامة البيانات، الاعتداء على سلامة النظام، إساءة استخدام أجهزة الحاسب.

أما المبحث الثاني فتطرق للجرائم المتصلة بالحاسب وقسمت إلى: التزوير المعلوماتي، الغش المعلوماتي، وصولا للمبحث الثالث المتطرق للجرائم المتصلة بالمحتوى، معالجا فيه الجرائم المتصلة بالمواد الإباحية للأطفال.

وبدوره **المبحث الرابع** عالج الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة.

وأخيراً **المبحث الخامس** تطرق لأشكال الأخرى للمسؤولية والجزاءات

- الشروع والاشتراك.
- مسئولية الأشخاص المعنوية
- الجزاءات والإجراءات.[3]

---

[1]- محمد علي العريان، المرجع السابق، ص25.

[2]- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقة عليها، المرجع السابق، ص 16 ، 29.

[3]- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع نفسه، ص 442، 444.

ب- أما **الفصل الثاني** فتطرق للجوانب الإجرائية لجرائم المعلوماتية (المواد14 - 21)، وعولج فيها في المبحث الأول لنطاق تطبيق قانون الإجراءات الجنائية والشروط والضمانات.

أما المبحث الثاني فتطرق فيه، للتحفظ العاجل على البيانات المعلوماتية المخزنة، وكذلك التحفظ والإفشاء العاجلان لبيانات المرور، أما المبحث الثاني فعالج الأمر بإنتاج بيانات معلوماتية، أما المبحث الرابع لتفتيش وضبط البيانات المعلوماتية المخزنة.

وأخيرا المبحث الأخير فعالج نقطة التجميع في الوقت الفعلي لبيانات المرور، واعتراض بيانات المحتوى .

3- التعاون الدولي :هنا **الباب الثالث** تطرق للأحكام المتعلقة بجرائم المعلوماتية عابرة الحدود (المواد 23-35) مقسماً إلى فصلين:

أ- الفصل **الأول** مبني على الأحكام العامة لجرائم المعلوماتية عابرة الحدود بما فيها التعاون الدولي، تسليم المجرمين، المساعدة القضائية المتبادلة، إجراءات طلب المساعدة القضائية المتبادلة.

ب-الفصل الثاني عالج مجالات المساعدة المتبادلة بشأن جرائم المعلوماتية عابرة الحدود، بما فيها المساعدة المتبادلة في مجال، الإجراءات الوقتية العاجلة، المساعدة المتبادلة في مجال سلطات التحقيق، إنشاء شبكة طوارئ دائمة لتفعيل المساعدة المتبادلة.[1]

4- الباب الرابع عالج الأحكام الختامية.

لقد قام وضعوا الاتفاقية بتحديد الإطار العام لهذه الجرائم والمتمثل في الدخول غير المشروع أو الاعتراض غير المشروع أو الاعتداء على سلامة البيانات أو النظام المعلوماتي، وكذلك إساءة استخدام الأجهزة الحاسوبية أو التزوير المعلوماتي أو الغش المعلوماتي، وقد أوجبت اتفاقية بودابست بعض الشروط حتى تأخذ الأفعال السابقة وصف الجريمة.

وتتمثل هذه الشروط فيما يلي.

- أن ترتكب الجرائم المذكورة في الاتفاقية دون وجه حق.
- أن ترتكب الجرائم المذكورة بطريقة عمدية من أجل إقرار المسؤولية الجنائية.

[1]- هيلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص 445، 448.

ثالثا- التزامات الدول الأطراف تجاه اتفاقية بودابست وأهم أهدافها

1- التزامات الدول الأطراف تجاه اتفاقية بودابست

اتفاقية بودابست فرصت على الدول الأطراف عند سن تشريعاتها الداخلية المتعلقة بالجرائم المعلوماتية، أن تراعي الاتفاقيات الدولية لحقوق الإنسان مثل: الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية لعام 1950، والميثاق الدولي حول الحقوق المدنية والسياسية لعام 1966، ويجب أيضا على الدول الأطراف الاعتماد على معايير لتقرير الاختصاص القضائي حول الجرائم المقررة في هذه الاتفاقية المتمثلة في مبدأ الإقليمية ومبدأ نسبية الاختصاص المكاني ومبدأ الجنسية وغير ذلك.[1]

2- أهداف اتفاقية بودابست

وأخيرا، ومن خلال استعراض ملامح الاتفاقية، يمكن تخليص أهدافها في:

أ-السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنظمة للاتفاقية من غير الدول الأوروبية.

ب- التأكيد على أهمية التعاون الإقليمي والدولي في ميدان مكافحة الجرائم الإلكترونية، وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة الإجرام الإلكتروني.

ج- ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة الكومبيوتر وشبكاته وأنشطة إساءة استخدامها، بما في ذلك تحديد الإطار الموضوعي لهذه الأنشطة والإطار الإجرائي لها.

[1] - بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم ،تخصص قانون عام، جامعة الجزائر 01 بن يوسف بن خدة، كلية الحقوق، السنة الجامعية 2017،2018، ص31،32 .

د- تحقيق التوازن بين حماية حقوق الإنسان الأساسية المعترف بها بموجب اتفاقية مجلس أوروبا لحماية حقوق الإنسان وحرياته الأساسية لعام 1950، والعهد الدولي للحقوق المدنية والسياسية لعام 1966والاتفاقيات العالمية الأخرى في ميدان حقوق الإنسان، وتحديدا الحقوق المتصلة بالرأي وحرية الوصول إلى المعلومات وحرية البحث، والتلقي والنقل للمعلومات والأفكار، وبين الحق في الخصوصية وفي حيازة المعلومات.[1]

رابعا- البروتوكول الإضافي الأول لاتفاقية الجريمة الالكترونية المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة بواسطة النظم الحاسوبية.

هذا البروتوكول تم النص عليه بتاريخ 28 يناير 2003م وبدأ النفاد في 01 مارس2006، ويلزم الدول التي صادقت عليه لتجريم نشر العنصرية وكراهية الأجانب المواد من خلال أنظمة الكمبيوتر، فضلا على التهديدات والشتائم بدافع العنصرية أو كراهية الأجانب.[2]

وعلى الرغم من أن هذه الاتفاقية لا تعالج الإرهاب المعلوماتي على وجه الخصوص، إلا أنها صيغت بطريقة قادرة على تتبع نطاق تهديدات الإرهابيين لتشمل جريمة الإرهاب المعلوماتي.

أصدرت لجنة اتفاقية الجرائم المعلوماتية سنة 2016 مذكرة توجيهية تتعلق بجوانب الإرهاب المعلوماتي بموجب اتفاقية بودابست، تعلن فيها أن " الجرائم الموضوعية في الاتفاقية قد تكون أيضا أعمالا إرهابية على النحو المحدد في القانون المعمول به"، وجاءت هذه المذكرة الإضافية بموجب الاتفاقية في الوقت المناسب، لتسلط المذكرة الضوء على أن هذه الاتفاقية ليست معاهدة بالإرهاب، إلا أنه يمكن القول: أن الجرائم الموضوعية في الاتفاقية يمكن أن تنفذ على أنها أعمال إرهابية لتسهيل الإرهاب ولدعم الإرهاب، ومن ذلك الأعمال التحريضية أو الجانب التمويلي.[3]

---

[1] – بدري فيصل، المرجع السابق، ص32 .

[2]– mimirbook.com/ar/07a712c41b6

اتفاقية الجريمة السيبيرانية، الزيارة للموقع يوم 07-08-2022 على الساعة 12:46

[3]– وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبيراني :التجربة الماليزية نموذجا، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المقالة 5، المجلد 23، العدد 1- الرقم المسلسل للعدد90،يناير2022، ص 151-178.

صادقت 65 دولة على الاتفاقية وذلك اعتبارا من ديسمبر 2020 ، بينما وقعت أربع دول أخرى على الاتفاقية لكنها لم تقم بالتصديق عليها.[1]

وكذا انطلاقا من 28 /04/ 2021صادقت عليها السويد وبالتالي ارتقت إلى الدولة 66 المصادقة عليها.[2]

منذ دخولها حيز النفاذ، الدول المهمة مثل البرازيل والهند، وقد انخفضت على اعتماد الاتفاقية على أساس أنهم لم يشاركوا في صياغتها.

تعارض روسيا الاتفاقية مشيرة إلى أن التبني ينتهك السيادة الروسية، وعادة ما ترفض التعاون في تحقيقات إنفاذ القانون المتعلقة بالجرائم الإلكترونية، أنه أول صك متعدد الأطراف ملزم قانوناً لتنظيم جرائم الانترنيت.

الفرع الثاني

البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية 2022.

إن دول الأعضاء في مجلس أوروبا والدول الأخرى الأطراف في الاتفاقية المتعلقة بالجريمة الإلكترونية (سلسلة المعاهدات الأوروبية رقم 185 المشار إليها فيما بعد بـ " الاتفاقية")، التي فتح باب التوقيع عليها في بودابست بتاريخ 23 نوفمبر 2001 و الموقعة على هذه الوثيقة، وإذ تضع في اعتبارها مدى انتشار الاتفاقية وتأثيرها في جميع مناطق العالم، وإذ تشير إلى أن الاتفاقية استكملت بالفعل البروتوكول الإضافي بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب على طريقة أنظمة الكومبيوتر،(سلسلة المعاهدات الأوروبية رقم 189)، الذي فتح باب التوقيع

[1]Stringfiscer.com/ar/convention ou cybercrime

اتفاقية الجرائم الالكترونية يوم 2022/08/07 على الساعة 12:56

[2] – wipolex.wipo.int/ar//reaties/952

موقع المنظمة العالمية للملكية الفكرية wipo يوم 2022/08/07 على الساعة 12:26

عليه في ستراسبورغ بتاريخ 28يناير2003 (يشار إليه باسم بروتوكول الأول) بالنسبة للدول الأطراف في البروتوكول المذكور.[1]

وإذا تأخذ بعين الاعتبار معاهدات مجلس أوروبا القائمة بشأن التعاون في المسائل الجنائية، وكذلك الاتفاقيات والترتيبات الأخرى بشأن التعاون في المسائل الجنائية بين الأطراف في الاتفاقية، وإذا تأخذ في الحسبان أيضا اتفاق حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (سلسلة المعاهدات الأوروبية رقم 108) ،كما تم تعديلها بموجب بروتوكولها التعديلي (سلسلة المعاهدات الأوروبية رقم 223)، الذي فتح باب التوقيع عليه في ستراسبورغ بتاريخ 10أكتوبر 2018 وجواز دعوة أي دولة للانضمام إليه.

وإذا تقر بالاستخدام المتزايد لتكنولوجيا المعلومات والاتصالات، بما في ذلك خدمات الإنترنت، وزيادة الجريمة السيبرانية، التي تشكل تهديدا للديمقراطية وسيادة القانون، والتي تعتبرها دول كثيرة أيضا تهديدا لحقوق الإنسان، و إذ تدرك أيضا تزايد عدد ضحايا الجرائم الإلكترونية وأهمية تحقيق العدالة لهؤلاء الضحايا .

وإذ تشير إلى أن الحكومات تتحمل مسؤولية حماية المجتمع والأفراد من الجريمة ليس فقط خارج الإنترنت، ولكن أيضا عبر الإنترنت، بما في ذلك من خلال التحقيقات الجنائية والملاحقات القضائية الفعالة.

وإذ تدرك أن الأدلة المتعلقة بأي جريمة جنائية يتم تخزينها بشكل متزايد في شكل إلكتروني على أنظمة الكمبيوتر في ولايات قضائية أجنبية أو معتمدة، أو غير معروفة واقتناعا منها بالحاجة إلى اتخاذ تدابير إضافية للحصـــول على مثل هذه الأدلــة بشكل قانوني، ضمانا لاستجابة جنائية فعالة وتعزيزاً سيادة القانون.[2]

---

[1] – amended–2021/1680a54ed1rm.coe.int/ara–2nd–add–prot

المجلس الأوروبي، سلسلة معاهدات مجلس أوروبا، البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن تعزيز التعاون والكشف عن الأدلة الالكترونية.

[2] –amended–2021/1680a54ed1rm.coe.int/ara–2nd–add–prot

المجلس الأوروبي، سلسلة معاهدات مجلس أوروبا، البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن تعزيز التعاون والكشف عن الأدلة الالكترونية 2022، المصدر نفسه.

وإذ تقر بالحاجة إلى تعاون متزايد و أكثر كفاءة بين الدول والقطاع الخاص، وأنه في هذا السياق تمت حاجة إلى مزيد من الوضوح أو اليقين القانوني بالنسبة لمقدمي الخدمات والكيانات الأخرى، فيما يتعلق بالظروف التي قد يستجيبون فيها للطلبات المباشرة من سلطات العدالة الجنائية لدى الدول الأطراف الأخرى للكشف عن البيانات الإلكترونية.

وإذ تسعى بالتالي إلى زيادة تعزيز التعاون بشأن الجرائم الإلكترونية، وجمع الأدلة في شكل إلكتروني عن أي جريمة جنائية لغرض تحقيقات أو إجراءات جنائية محددة، من خلال أدوات إضافية تتعلق بالمساعدة المتبادلة الأكثر كفاءة، وأشكال التعاون الأخرى بين السلطات المتخصصة، وإلى تعزيز التعاون في حالات الطوارئ والتعاون المباشر بين السلطات المختصة ومقدم الخدمات والكيانات الأخرى التي تمتلك أو تتحكم في المعلومات ذات الصلة.

واقتناعا منها بأن الظروف والضمانات الفعالة لحماية حقوق الإنسان والحريات الأساسية، مفيدة للتعاون العابر للحدود الفعال لأغراض العدالة الجنائية، بما في ذلك بين القطاعين العام والخاص.

واعترافا منها بأن جميع الأدلة الإلكترونية في إطار التحقيقات الجنائية، غالبا ما يتعلق بالبيانات الشخصية، وبأنه يتعين على العديد من الأطراف حماية الخصوصية والبيانات الشخصية من أجل الوفاء بالتزاماتها الدستورية والدولية.

وإذ تضع في اعتبارها الحاجة إلى ضمان خضوع تدابير العدالة الجنائية الفعالة، بشأن الجرائم الإلكترونية وجمع الأدلة في شكل إلكتروني، لشروط وضمانات توفر الحماية الكافية لحقوق الإنسان والحريات الأساسية، بما في ذلك الحقوق المنبثقة عن الالتزامات التي تعهدت بها الدول بموجب صكوك حقوق الإنسان الدولية المعمول بها، على غرار اتفاقية عام 1950 لحماية حقوق الإنسان و الحريات الأساسية لمجلس أوروبا (سلسلة المعاهدات الأوروبية رقم 5)، و عهد الأمم المتحدة الدولي الخاص بالحقوق المدنية والسياسية لعام 1966، والميثاق الإفريقي لحقوق الإنسان والشعوب لسنة 1981، والاتفاقية الأمريكية لحقوق الإنسان لعام 1969 وغيرها من المعاهدات الدولية المتعلقة بحقوق الإنسان.[1]

[1] – amended-2021/1680a54ed1rm.coe.int/ara-2nd-add-prot

المجلس الأوروبي، سلسلة معاهدات مجلس أوروبا، البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن تعزيز التعاون والكشف عن الأدلة الالكترونية 2022، المصدر السابق.

اتفقت على هذا البروتوكول المكون من:

أربعة أبواب، الباب الأول تطرق للأحكام العامة، والباب الثاني لتدابير تعزيز التعاون، أما الباب الثالث للشروط والضمانات، والباب الأخير للأحكام الختامية.

أولا-الأحكام العامة التي جاء بها هذا البروتوكول

تطرق هذا البروتوكول تحت الباب الأول إلى الغرض من البروتوكول ونطاق تطبيقه، وكذلك التعريفات، وفي الأخير إلى اللغة المطلوبة.

1- الغرض من البروتوكول:

الغرض من هذا البروتوكول هو استكمال الاتفاقية بين الدول الأطراف في هذا البروتوكول، وكذا استكمال البروتوكول الأول بين الدول أطراف هذا البروتوكول التي هي أيضا طرفا في البروتوكول الأول.[1]

2- نطاق التطبيق:

يتم تطبيق التدابير الواردة في هذا البروتوكول، من التحقيقات أو الإجراءات الجنائية الخاصة المتعلقة بالجرائم الجنائية ذات الصلة بأنظمة الكمبيوتر والبيانات، وجميع الأدلة ذات الشكل الإلكتروني عن الجريمة الجنائية بالنسبة للدول الأطراف في الاتفاقية التي هي أيضا أطراف في هذا البروتوكول.

كما يتم تطبيق التدابير الواردة في هذا البروتوكول، بالنسبة للدول الأطراف في البروتوكول الأول، التي هي أيضا أطراف في هذا البروتوكول على التحقيقات أو الإجراءات الجنائية الخاصة المتعلقة بالجرائم الجنائية المنصوص عليها في البروتوكول الأول.

كما يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتنفيذ الالتزامات المنصوص عليها في هذا البروتوكول.[1]

[1]-المادة الأولى من البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن التعاون والكشف عن الأدلة الالكترونية 2022، المصدر السابق.

3-التعريفات:

أ – **سريان التعريفات السابقة:** تسري التعاريف الواردة في المادتين 01 و18 فقرة 03 من الاتفاقية على هذا البروتوكول.

بالرجوع إلى المادة 01 من الاتفاقية[2]، نجد أنها تتطرق لتعريفات للأغراض هذه الاتفاقية، وذلك مثل:

-**النظام المعلوماتي:** الذي يعني كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة، والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى، تنفيذا لبرنامج معين بأداء معالجة آلية للبيانات.

– **البيانات المعلوماتية** :التي تعني كل تمثيل للوقائع، أو المعلومات أو المفاهيم تحت أي شكل، وتكون مهيأة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة، يجعل الحاسوب يؤدي المهمة.

– **مقدم الخدمة**[3]: وهو كل جهة عامة أو خاصة تقدم لمستخدمي خدماتها إمكانية الاتصال عن طريق النظام المعلوماتي، وكل جهة أخرى تعالج أو تخزن البيانات المعلوماتية بدلا من خدمة الاتصال أو نيابة عن مستخدمي هذه الخدمة.

– **البيانات المتعلقة بالمرور**: والتي تعني كل البيانات التي تتعامل مع الاتصال، والتي تمر من خلال النظام المعلوماتي، أو يتم إعدادها بواسطة هذا الأخير، والذي يعد عنصرا في سلسلة الاتصال،

---

[1]– المادة الثانية من البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن التعاون والكشف عن الأدلة الالكترونية 2022 ، المصدر السابق.

[2] – المادة الأولى من اتفاقية بودابست لمكافحة جرائم المعلوماتية، المصدر السابق.

[3]–حرصت المذكرة التفسيرية على أن توضح أن تعريف "مقدم الخدمة" الوارد في الفترة ج من المادة الأولى من الاتفاقية ينطبق على كل من يقوم بخدمات الاتصال، أو خدمات معالجة البيانات أو خدمات تخزين البيانات، يستوي في ذلك أن تكون الجهة التي تقدم الخدمة جهة عامة أو خاصة ،كما يستوي أن تكون الخدمة مقدمة لمجموعة من المستخدمين يشكلون جماعة مغلقة، أو أنها مقدمة للجمهور، كذلك يستوي أن تكون الخدمة مقابل رسوم أو بالمجان، كما يشمل هذا التعريف الأشخاص الذين يعرضون خدمة الاستضافة ، أو التخزين المؤقت بمعنى الإخفاء، أو الربط بالشبكة، كل أولئك يمتد نطاق التعريف ليشملهم، لكن لا ينطبق هذا التعريف على مجرد مقدم المحتوى، كأن يتعاقد شخص مع هذا المقدم على إنشاء موقع له على الشبكة العالمية دون أن يقوم هذا الأخير بأي خدمات أخرى كخدمات الاتصال أو المعالجة أو التخزين ." هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص25،26 .

بالإشارة إلى مصدر الاتصال، مكان الوصول، خط السير، الساعة التاريخ، الحجم، مدة الاتصال، أو نوع الخدمة المؤداة.

وبرجوعنا كذلك إلى المادة 18 المعنونة ب **الأمر بإنتاج بيانات معلوماتية** (الأمر بتقديم بيانات معلوماتية)، الفقرة الثالثة منها[1]، تطرقت لتعبير "**البيانات المتعلقة بالمشتركين**"، والمقصود منها كل المعلومات تحتوي على شكل بيانات معلوماتية أو أي شكل آخر في حوزة مقدم الخدمة وترتبط بالمشتركين وخدماتهم، غير بيانات المرور أو المحتوى والتي من خلالها يمكن تحديد:

- نوع خدمة الاتصال المستخدمة، والأوضاع الفنية المنصوص عليها بالنسبة لفترة الخدمة.

- الهوية، العنوان البريدي أو الجغرافي، ورقم تليفون المشترك، ورقم الولوج، والبيانات المتعلقة بدفع الفاتورة، والمبلغ المدفوع، و المتوافرة على أساس عقد أو اتفاق تقديم الخدمة.

- أية معلومات أخرى تتعلق بموقع تجهيزات الاتصال، المتوافرة على أساس عقد أو اتفاق تقديم الخدمة.

وعليه كقاعدة عامة، تعبير المعلومات المتعلقة بالمشتركين، فهو يعني كل معلومات تم حيازتها بواسطة إدارة مقدم الخدمات تتصل بالمشترك وخدماته، والبيانات المتعلقة بالمشتركين التي يتم حيازتها، كما يمكن أن تأخذ شكل بيانات معلوماتية، فإن أيضا يمكن أن تأخذ شكلا آخر كأن تكون مستندات ورقية، وفي هذه الحالة الأخيرة فإن الأمر يتطلب نصا خاصا في هذه المادة لمعالجة هذا النوع من المعلومات.

أما المصطلح "مشترك" فإنه يشير إلى العديد من طوائف زبائن مقدمي الخدمات، الشخص الذي يدفع مقابل الخدمة، العميل الذي يدفع مقدما نظير الخدمات التي يستعملها الشخص الذي يستفيد من الخدمات مجانا، وتشمل أيضا كل المعلومات المتعلقة بالأشخاص المخول لهم استخدام حساب المشترك.[2]

ب- التعريفات التي جاء بها البروتوكول:

- **السلطة المركزية:** يقصد بها السلطة أو السلطات المعينة بموجب معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريعات موحدة أو متبادلة سارية بين الأطراف المعنية، أو في حالة عدم

[1]- المادة 18. فقرة 03 من اتفاقية بودابست لمكافحة جرائم المعلوماتية، المصدر السابق.

[2]- الهلال عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقة عليها، المرجع السابق، ص 230.

وجودها، السلطة أو السلطات المعينة من قبل إحدى الدول الأطراف بموجب المادة 27 الفقرة 2- أ من الاتفاقية.[1]

المادة 27 تطرقت للإجراءات المتعلقة بطلبات المساعدة القضائية المتبادلة بين الأطراف في ظل غياب اتفاقية دولية مطبقة، وبالعودة إلى **الفقرة 2**- أ من هذه المادة اعتبرت، أنه يجب على كل طرف أن يعين هيئة مركزية أو هيئات تكون مسئولة عن إرسال أو الرد على طلبات المساعدة المتبادلة، أو تنفيذ هذه الطلبات أو إرسالها إلى السلطات المختصة.[2]

-**السلطة المختصة** : هي سلطة قضائية أو إدارية أو غيرها من سلطات إنفاذ القانون المخولة بموجب القانون المحلي بإصدار الأمر بتنفيذ التدابير الواردة في هذا البروتوكول، أو الترخيص بها، أو تتولى تنفيذها لغرض جمع أو تقديم أدلة فيما يتعلق بتحقيقات أو إجراءات جنائية خاصة.

- **حالة الطوارئ** :هي الوضعية التي يوجد فيها خطر كبير ووشيك على حياة أو سلامة أي شخص طبيعي.

- **البيان الشخصية:** معلومات متعلقة بشخص طبيعي محدد أو يمكن التعريف عليه.

- **الطرف المحول:** الطرف الذي يقوم بنقل البيانات استجابة لطلب، أو كجزء من فريق تحقيق مشترك، أو لأغراض القسم الثاني من الباب الثاني، أي (إجراءات تعزيز التعاون المباشر مع مقدمي الخدمات وغيرهم من الكيانات في الأطراف الأخرى، وذلك من حيث طلب معلومات حول تسجيل اسم نطاق وإفشاء المعلومات المتعلقة بالمشاركين)، طرف يوجد فوق ترابه مقدم خدمات قادر على نقل البيانات أو كيان يوفر خدمات تسجيل أسماء النطاقات.[3]

4 -**اللغة** : الطلبات والأوامر والمعلومات المصاحبة المقدمة إلى أحد الأطراف ، يجب أن تكون بلغة مقبولة لدى الطرف متلقي الطلب، أو الطرف المخطر، أو تكون مصحوبة بترجمة إلى هذه اللغة.

---

[1]- المادة 03 فقرة2-أ من البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن تعزيز التعاون و الكشف من الأدلة الالكترونية 2022، المصدر السابق.

[2]-المادة 27 فقرة 2-أ من اتفاقية بودابست لمكافحة الجرائم المعلوماتية، المصدر السابق.

[3]-المادة 03 فقرة 2- ب-ج-د-هـ، من البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن تعزيز التعاون والكشف عن الأدلة الالكترونية 2022، المصدر نفسه.

وكذلك يجب أن تكون الأوامر المنصوص عليها في **المادة 7** أي " **إفشاء المعلومات المتعلقة بالمشتركين**"، والطلبات المنصوص عليها في **المادة 6** أي "**طلبات معلومات حول تسجيل اسم نطاق** "، وأي معلومات مصاحبة:

- محررة بلغة الطرف الآخر التي يقبل بها مقدم الخدمة أو الكيان.
- محررة بلغة أخرى مقبولة لدى مقدم الخدمة أو الكيان.
- مصحوبة بترجمة إلى إحدى اللغات الواردة في الفقرة السابقتين.[1]

ثانيا- تدابير تعزيز التعاون

هذا العنوان جاء كعنوان للباب الثاني من هذا البروتوكول، والذي بدوره قسم إلى خمسة أقسام، القسم الأول تطرق للمبادئ العامة المطبقة على الباب الثاني، أما القسم الثاني فتطرق لإجراءات تعزيز التعاون المباشر مع مقدمي الخدمات وغيرهم من الكيانات في الأطراف الأخرى، والقسم الثالث عالج إجراءات تعزيز التعاون الدولي بين السلطات للكشف عن بيانات الكمبيوتر المخزنة.

أما القسم الرابع فتطرق للإجراءات المتعلقة بالمساعدة المتبادلة في حالات الطوارئ.

والقسم الأخير للإجراءات المتعلقة بالتعاون الدولي في حالة عدم وجود اتفاقيات دولية سارية المفعول.

1- المبادئ العامة المطبقة على تدابير تعزيز التعاون:

تحت القسم 1 من الباب الثاني الذي تطرق للمبادئ العامة المطبقة على تدابير تعزيز التعاون، نجد أهمها:

أ-الدول الأطراف تتعاون بشكل متبادل إلى أقصى حد ممكن.

ب-فيما يخص طلب معلومات حول تسجيل hسم نطاق، وإفشاء المعلومات المتعلقة بالمشتركين، فهنا نص على إجراءات لتعزيز التعاون الدولي بين السلطات للكشف عن بيانات الكمبيوتر المخزنة، كما تسري مقتضيات القسم 2"إجراءات تعزيز التعاون المباشر مع مقدمي الخدمات وغيرهم من الكيانات

[1]- المادة 04 من البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن تعزيز التعاون والكشف عن الأدلة الالكترونية 2022، المصدر السابق.

في الأطراف الأخرى"، سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة أملا على أساس تشريع موحد أو متبادل ساري المفعول بين الأطراف المعنية.

ج- إجراءات تعزيز التعاون الدولي بين السلطات للكشف عن بيانات الكمبيوتر المخزنة، بما فيها تفعيل الأوامر الصادرة عن دولة طرف أخرى بشأن الإنتاج المعجل لمعلومات المشترك وبيانات المرور حسب المادة 08، وكذا الكشف السريع عن بيانات الكمبيوتر المخزنة في حالة الطوارئ حالة المادة 09.

وتسري إجراءات تعزيز التعاون الدولي بين السلطات للكشف عن بيانات الكمبيوتر المخزنة سواء كانت هناك معاهدة، أو ترتيب للمساعدة المتبادلة أم لا، على أساس تشريع موحد أو متبادل ساري المفعول بين الطرف مقدم الطلب والطرف الذي يتلقاه.

د- كذلك نص على الإجراءات المتعلقة بالمساعدة المتبادلة في حالات الطوارئ، وهذا حسب المادة العاشرة من هذا القانون، سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة أم لا على أساس تشريع موحد أو متبادل ساري المفعول بين الطرف مقدم الطلب والطرف الذي يتلقاه.

هـ-نصت كذلك على الإجراءات المتعلقة بالتعاون الدولي في حالة عدم وجود اتفاقيات دولية سارية المفعول، كالتداول بالفيديو وفوق التحقيق المشتركة والتحقيقات المشتركة.

2- كذلك تحت القسم 2 من الباب الثاني، الذي تطرق للمبادئ العامة المطبقة على تدابير تعزيز التعاون، نص القسم الثاني على إجراءات تعزيز التعاون المباشر مع مقدمي الخدمات وغيرهم من الكيانات في الأطراف الأخرى، بما فيها طلب معلومات حول تسجيل اسم نطاق، وإفشاء المعلومات المتعلقة بالمشتركين.[1]

3- أما القسم الثالث من نفس الباب، فتطرق لإجراءات تعزيز التعاون الدولي بين السلطات للكشف عن بيانات الكمبيوتر المخزنة، بما فيها تفعيل الأوامر الصادرة عن دولة طرف أخرى بشأن الإنتاج

[1]- المادة 06 و 07 من البروتوكول الإضافي الثاني، المصدر السابق.

المعجل لمعلومات المشترك وبيانات المرور، وكذا الكشف السريع عن بيانات الكمبيوتر المخزنة في حالة الطوارئ.[1]

4- أما القسم الرابع من نفس الباب الثاني، فتطرق للإجراءات المتعلقة بالمساعدة المتبادلة في حالات الطوارئ وذلك مثل: جواز لكل دولة طرف طلب المساعدة المتبادلة على وجه السرعة عندما يرى أن هناك حالة طوارئ، وهذا الطلب يجب أن يتضمن وصفا للوقائع التي تثبت وجود حالة طارئة وكيفية ارتباط المساعدة المتبادلة المطلوبة بها.

ونص على إجراءات الطرف المتلقي في الجهة المقابلة كقبول المتلقي الطلبات في شكل إلكتروني، وغير ذلك.[2]

5- أما القسم الخامس من نفس الباب، فنص على الإجراءات المتعلقة بالتعاون الدولي في حالة عدم وجود اتفاقيات دولية سارية المفعول كالتداول بالفيديو، كجواز للطرف الطالب أن يلتمس أخذ أقوال شاهد أو خبير عبر التداول بالفيديو، ويجوز للطرف المتلقي أن يسمح بذلك.

كذلك هذا القسم تطرق لفرق التحقيق المشتركة والتحقيقات المشتركة.[3]

ثالثا- الشروط والضمانات وكذا حماية المعطيات الشخصية

الباب الثالث من هذا البروتوكول تطرق لنقطتين مهمتين وهما الشروط والضمانات وكذا حماية المعطيات الشخصية.

1- الشروط والضمانات:

توفير للحماية الكافية لحقوق الإنسان والحريات يجب على كل طرف وضع وتنفيذ وتطبيق الصلاحيات والإجراءات المنصوص عليها في هذا البروتوكول للشروط والضمانات المنصوص عليها

[1]-المادة 08 و09 من البروتوكول الإضافي الثاني، المصدر السابق.

[2] - المادة 10من البروتوكول الإضافي الثاني، المصدر نفسه.

[3]-المادة 11 و 12 من البروتوكول الإضافي الثاني، المصدر نفسه.

في قانونه المحلي[1]، وعلى الأخص الحقوق الناشئة عن الالتزامات التي تعهد بها في ظل اتفاقية المجلس الأوروبي عام 1950 لحماية حقوق الإنسان وحرياته الأساسية، والاتفاقية الدولية للحقوق المدنية والسياسية للأمم المتحدة لعام 1966، والاتفاقيات العالمية الأخرى المطبقة والخاصة بحقوق الإنسان[2].

2- حماية المعطيات الشخصية:

حماية للمعطيات الشخصية تطرق هذا البروتوكول الإضافي إلى نطاق التطبيق فيما يتعلق معالجة البيانات الشخصية، وكذا الغرض والاستخدام لمعالجة هذه البيانات، وكذا من جهة أخرى أوجب على كل طرف اتخاذ خطوات معقولة لضمان الحفاظ على البيانات الشخصية بطريقة دقيقة وكاملة، والحرص على أنها محدثة بالقدر الضروري والمناسب لتتم معالجتها طبقا للقانون، مع مراعاة الأغراض التي تتم معالجتها من أجلها وهذا يدخل ضمن الجودة والسلامة.

كذلك تطرق للبيانات الحساسة حيث أنه حرص على عدم جوازية قيام أحد الأطراف بمعالجة بيانات شخصية تكشف عن الأصل العرقي أو الاثني أو الآراء السياسية أو المعتقدات الدينية أو غيرها من المعتقدات أو العضوية النقابية، وكذا البيانات الجينية والبيانات البيومترية الحساسة في ضوء المخاطر التي تنطوي عليها، أو البيانات الشخصية المتعلقة بالصحة أو الحياة الجنسية، إلا في ظل ضمانات مناسبة للوقاية من مخاطر التأثير الضار غير المبرر الناجم عن استخدام هذه البيانات، ولاسيما ضد التمييز غير القانوني.

كذلك نص على آجال الاحتفاظ بالبيانات ذات الطابع الشخصي، والتي تكون حسب المدة الضرورية والمناسبة بالنسبة لكل دولة طرف.

ومن جهة أخرى تطرق لنقطة مهمة، وهي القرارات الآلية حيث اعتبر أن القرارات التي ينتج عنها تأثير سلبي كبير على المصالح ذات الصلة للفرد الذي تتعلق به البيانات الشخصية، لا تستند فقط على المعالجة الآلية للبيانات الشخصية، ما لم يسمح بذلك بموجب القانون المحلي وبضمانات مناسبة تتضمن إمكانية الحصول على تدخل بشري.

---

[1]- المادة 13 من البروتوكول الإضافي الثاني، المصدر السابق.

[2]- المادة 15 من اتفاقية بودابست لمكافحة جرائم المعلوماتية، المصدر السابق.

كما حرص هذا البروتوكول على توفير كل دولة طرف، التدابير التكنولوجية والمادية والتنظيمية المناسبة لحماية البيانات ذات الطابع الشخصي، ولاسيما ضد الضياع أو الوصول العرضي أو غير المصرح به، أو الكشف أو التغيير أو التدمير "الحادث الأمني"، وهذا يدخل ضمن أمن البيانات والحوادث الأمنية.

كما تطرق لحفظ السجلات، وكذا التبادل اللاحق بين هيئات طرف معين، وكذا النقل اللاحق للمعطيات إلى دولة أخرى أو منظمة دولية أخرى.

كذلك يجب أن يكون لكل طرف سلطة عامة واحدة أو أكثر، تمارس مجتمعة أو منفصلة وظائف وصلاحيات الرقابة المستقلة والفعالة، ويجب أن تشمل وظائف و اختصاصات هذه السلطات مجتمعة أو منفصلة صلاحية التحقيق والتعامل مع الشكاوى والقدرة على اتخاذ الإجراءات الصحيحة.

وفي الأخير يجوز لأي دولة طرف تعليق نقل البيانات الشخصية إلى دولة طرف أخرى إذا كان لديها دليل قوي على أن الطرف الآخر ينتهك بشكل منهجي أو مادي شروط هذه المادة، أو على احتمال وقوع خرق مادي وشيك، ولا يجوز تعليق نقل البيانات قبل نهاية مهلة معقولة لا يتم التوصل خلالها إلى حل، ومع ذلك يجوز لأي طرف أن يعلق مؤقتا عمليات النقل في حالة حدوث خرق منهجي أو مادي يشكل خطرا كبيرا ووشيكا على حياة أو سلامة شخص ذاتي أومن شأنه التسبب في ضرر كبير على سمعته أو وضعيته المالية، و يجب عليه في هذه الحالة إخطار الطرف الآخر وبدء المشاورات معه على الفور، إذا لم تؤدي المشاورات إلى حل يجوز للطرف الآخر التصرف بالمثل وتعليق عمليات النقل إذا كان لديه دليل قوي على أن التعليق من قبل الطرف الأول مخالف للشروط، ويجب على الطرف المعلق رفع التعليق بمجرد معالجة الخرق الذي كان يبرره، ويجب حينها رفع أي تعليق متبادل لنقل المعطيات، ويجب الاستمرار في معالجة أي بيانات ذات طابع شخصي تم نقلها قبل التعليق وفق هذا البروتوكول.[1]

رابعا-الأحكام الختامية

تطرق الباب الأخير لعدة أحكام أهمها، الآثار المترتبة عن البروتوكول، وكذا طريقة التوقيع ودخول حيز التنفيذ لهذا البروتوكول، كذلك من بين الأحكام الختامية تطرق للبند الاتحادي، التطبيق الإقليمي

[1]-المادة 14 من البروتوكول الإضافي الثاني، المصدر السابق.

لهذا البروتوكول،التحفظات والإعلانات، تسوية النزاعات، مشاورات الأطراف وتقييم التنفيذ، الانسحاب، الإبلاغ .[1]

وفي الأخير حسب بيانات 08 ماي 2022 لوزارة العدل الجزائرية اعتبرت أنه وفي إطار التعاون مع البرنامج الأوروبي لمكافحة الجريمة السيبرانية، يشارك إطاران من الإدارة المركزية لوزارة العدل في تظاهرة " افتتاح التوقيع على البروتوكول الإضافي الثاني لاتفاقية الجريمة المعلوماتية" وكذا ندوة دولية حول " تعزيز التعاون والكشف عن الأدلة الإلكترونية" يومي 12و13 ماي 2022، بستراسبورغ بفرنسا.

وللعلم تم التفاوض على البروتوكول المذكور لمدة أربع سنوات (سبتمبر 2017 إلى غاية ماي 2021) وتم المصادقة على صيغته في17نوفمبر 2021، وتم افتتاحه للتوقيع عليه بمجلس أوروبا بستراسبورغ فرنسا يوم 12 ماي 2020 في إطار الندوة الدولية المذكورة، كما يتم من خلال هذه التظاهرة مناقشة أدوات البروتوكول الإضافي الثاني والتعاون بين القطاعين العام والخاص، والتعاون في الحالات الطارئة، ودور نقاط الاتصال وبناء القدرات.[2]

وفي بيانات وزارة العدل الجزائرية في 12 جوان 2022، معتبرتا أنه وفي إطار التعاون مع البرنامج الأوروبي لمكافحة الجريمة السيبرانية cybersud يشارك قاضيان 02 و إطار 01 في الاجتماع الثامن للجنة المديرة للبرنامج الأوروبي لمكافحة الجريمة السيبرانية يوم 16و17 جوان 2022ببوخارست، رومانيا ويهدف الاجتماع إلى جمع الفاعلين من البلدان الشريكة في هذا البرنامج لتقييم نشاطات البرنامج وتقديم اقتراحات بشأنها، وكذا الأولويات والمشاريع الوطنية في المجال مكافحة الجريمة المعلوماتية والمساهمة في تحضير برنامج النشاطات من شهر جويلية إلى ديسمبر 2022، وهو فرصة لتبادل وجهات النظر حول مسعى دعم بناء القدرات وفقا للسياسات والاستراتيجيات الوطنية بما يتماشى مع التطورات الحديثة على المستوى الذي يشهدها العالم.[3]

---

[1]–من المادة 15إلى المادة 25 من البروتوكول الإضافي الثاني، المصدر السابق

[2]–موقع وزارة العدل(/ العمليات– التكوينية–المبرمجة–لفائدة 1–4/ar/www.mjustice.dz –)الزيارة يوم 2022/08/07 على الساعة 16:40.

[3]–موقع وزارة العدل www.mjustice.dz بيانات 12 جوان 2022.الدخول يوم 2022/08/07 على الساعة 16:30 .

وفي بيانات وزارة العدل ليوم 19 جوان 2022 ،وفي إطار التعاون كذلك مع المجلس الأوروبي لمكافحة الجريمة السريانية cybersud يشارك 30 مستفيدا منهم 21 قاضيا وإطار من وزارة العدل و09اطارات من وزارة الشؤون الخارجية والجالية الوطنية بالخارج في ورشة عبر الإنترنت حول "البروتوكول الإضافي الثاني الملحق باتفاقية بودابست للجريمة المعلوماتية في إطار التشريع الجزائري" يوم 21 جوان 2022 هدف هذه الورشة التي تضم هيئات العدالة الجزائرية، ممثلي الدول الشريكة في هذا البرنامج وخبراء من مجلس أوروبا إلى التقييم المشترك للتشريعات الوطنية على ضوء أحكام البروتوكول الإضافي الثاني الملحق باتفاقية بودابست للجريمة المعلوماتية في إطار التشريع الوطني الجزائري وكذا تحديد الثغرات المحتمل وجودها في التشريع الوطني و وسائل سد مثل هذه الثغرات.[1]

المطلب الثاني

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[2]

إن الدول العربية الموقعة رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات، التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعا منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وأخذا بالمبادئ الدينية والأخلاقية السامية، ولاسيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة والتزاما بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان.[3]

---

[1]– موقع وزارة العدل www.mjustice.dz بيانات 19 جوان 2022.الدخول يوم 2022/08/07 على الساعة 17:00 .

[2]– الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة في 21-12-2010، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم :14-252المؤرخ في 08-09-2014، ج ر ج ج، العدد57 المؤرخة في 28-09-2014.

[3]– ديباجة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المصدر السابق.

وجاءت مضامين الاتفاقية العربية مطابقة لأحكام اتفاقية بودابست خاصة على مستوى القواعد الإجرائية، سواء من حيث نطاق التطبيق أو طبيعة هذه القواعد، حيث نصت على مجموعة من القواعد الإجرائية أوجبت على الدول الأطراف ملائمتها مع قوانينها الوطنية فيما يتعلق بالأبحاث الجنائية، كتدابير التحفظ على بيانات الكمبيوتر المخزنة وكشفها وإصدار الأوامر بتسليمها وإجراء التفتيش على المعلومات المخزنة وضبطها والجمع الفوري لها واعتراض محتواها، أو ما يرتبط بالتعاون الدولي القانوني والقضائي، لاسيما على مستوى تحديد الاختصاص القضائي، وتسليم المجرمين والمساعدة المتبادلة وضوابطها بين الدول الأطراف، ونوع المعلومات القابلة للتعاون والأجهزة المتخصصة المشرفة عليها.[1]

هذه الاتفاقية شهدت خمس فصول، فصلها الأول تطرق للأحكام العامة، أما الفصل الثاني فتطرق للتجريم، والفصل الثالث للأحكام الإجرائية، أما الفصل الرابع للتعاون القانوني والقضائي، أما الفصل الأخير للأحكام الختامية.

الفرع الأول

أحكام عامة للاتفاقية العربية

أولا- الهدف من الاتفاقية:

هدف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذا النوع من الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.[2]

---

[1]- إدريس بالمحجوب، تأثير الجريمة الالكترونية على الائتمان المالي، مطبعة الأمنية، الرباط، المغرب، العدد السابع 2014، ص 83.

وافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21 .-مرسوم رئاسي رقم 14-252، المؤرخ في 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، الجريدة الرسمية الجمهورية الجزائرية، العدد 57، الصادرة في 28 سبتمبر سنة 2014.

[2]- المادة 01 من الاتفاقية العربية لمكافحة جرائم المعلوماتية، المصدر السابق .

ثانيا- المصطلحات:

تعرضت هذه الاتفاقية لمفهوم عديد المصطلحات أهمها : تقنية المعلومات، مزود الخدمة، البيانات، البرنامج المعلوماتي، النظام المعلوماتي، الشبكة المعلوماتية، الموقع، الالتقاط، معلومات المشترك.

فمثلا :

1- **الالتقاط** : يقصد بها مشاهدة البيانات أو المعلومات أو الحصول عليها.

2- **معلومات المشترك** : أية معلومات موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات، عدا المعلومات التي يمكن بواسطتها معرفة:

أ- نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة.

ب- هوية المشترك وعنوانه البريدي أو الجغرافي أو هاتفه، و معلومات الدفع المتوفرة بناء على اتفاق أو ترتيب الخدمة.

ج - أية معلومات أخرى عن موقع تركيب معدات الاتصال بناء على اتفاق الخدمة.[1]

ثالثا- مجالات تطبيق الاتفاقية:

جاءت هذه الاتفاقية لتطبق على هذا النوع من الجرائم، وهذه لغاية منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك إذا ارتكبت في أكثر من دولة وإذا ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى، كذلك إذا ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة، وكذا إذا ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى.[2]

[1]- المادة 02 من الاتفاقية العربية لمكافحة جرائم المعلوماتية، المصدر السابق.

[2]- المادة 03 من الاتفاقية العربية لمكافحة جرائم المعلوماتية، المصدر نفسه .

الفرع الثاني

التجريم والأحكام الإجرائية

سوف نتطرق تحت هذا الفرع للتجريم والأحكام الإجرائية:

أولا: التجريم:

حسب المادة الخامسة من هذه الاتفاقية، تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، أي الفصل الثاني المعنون ب"التجريم"، وذلك وفقا لتشريعاتها وأنظمتها الداخلية، وحسب هذا الفصل نلاحظ أنه تطرق لعدة جرائم منها، جريمة الدخول غير المشروع ،وجريمة الاعتراض غير المشروع، والاعتداء على سلامة البيانات، كما تطرق إلى جريمة إساءة استخدام وسائل تقنية المعلومات، كما تطرق لجريمة التزوير و جريمة الاحتيال، وجريمة الإباحة والجرائم الأخرى المرتبطة بها كالمقامرة والاستغلال الجنسي.

كما تطرق في المادة الرابعة عشر من هذه الاتفاقية إلى جريمة الاعتداء على حرمة الحياة الخاصة.

و تطرق للجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، كذلك تطرق لجرائم عديدة أخرى كانتهاك لحق المؤلف والحقوق المجاورة، الاستخدام غير المشروع لأدوات الدفع الإلكتروني وغيرها....

1-جريمة الدخول غير المشروع:

حسب الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، يدخل ضمن هذه الجريمة:

أ- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

ب- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: - محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال، وإلحاق الضرر بالمستخدمين والمستفيدين.

- الحصول على معلومات حكومية سرية.

فبرجوعنا للتشريع الجزائري يعتبر قانون العقوبات الجزائري من القوانين العربية السباقة في هذا الموضوع، بل أنه من التشريعات المواكبة للتشريعات الغربية على هدى التشريع الأمريكي والإنجليزي والفرنسي، خطى المشرع الجزائري هذه الخطوة بالمبادرة إلى تعديل قانون العقوبات بمقتضى القانون رقم 04-15، بإدراج القسم السابع مكرر بمحتوى المادة 394 مكرر إلى 394 مكرر7، ويبدو أن المشرع لم يكتفي بذلك بل قطع أشواطا أخرى في اتجاه فرض حماية جنائية على الحياة الخاصة للأفراد، حين بادر بتعديل جديد لقانون العقوبات، وهو الذي جاء به القانون رقم 06 - 23 والذي مس المادة 303 وإقراره المادة 303 مكرر إلى 303 مكرر 3، وهو بذلك يضع سياجا لحماية خصوصية الأفراد تحسبا للاستخدام السيئ للوسائل التكنولوجية الحديثة عن طريق الكمبيوتر أو الهاتف النقال، وما يرتبط بها من تقنيات مثل ما يسمى بـ البلوتوت وغيره.

وقد نصت المادة 394 مكرر من قانون العقوبات على أنه " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50,000دج إلى 100,000دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

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 دج إلى 150,000 دج".

يلاحظ أن المشرع الجزائري جرم **فعل الدخول بطريقة غير شرعية إلى المنظومة المعلوماتية،** واعتبر هذا التصرف في حد ذاته يشكل جريمة، إذ يستخلص لأول وهلة أن مجرد اختراق جهاز الكمبيوتر، سواء كان ذلك بقصد الوصول إلى البيانات أو لمجرد التسلية، يعد انتهاكا للنظام المعلوماتي بطريقة غير مشروعة.

ويمكن حسب مفهوم النص أن الجريمة تتحقق بالصور التالية:

– بمجرد الوصول إلى نظام معلوماتي، لكن بطريق الغش أي أن الجريمة عمدية هنا تقوم بتوافر القصد الجنائي العام.

– أن يكون الجاني عالما بدخوله إلى منظومة معلومات لا تخصه، وواضح من نص المادة 394 مكرر من قانون العقوبات أن جريمة الدخول غير المشروع تصبح قائمة حتى لو لم يترتب عن ذلك أي أضرار بالمعلومات، ودون تحديد للزمن ذلك أن جريمة الدخول غير المشروع هي جريمة وقتية، على عكس جريمة البقاء في المنظومة التي تعد من الجرائم المستمرة.[1]

أما **جريمة البقاء غير المشروع داخل النظام المعلوماتي**، فيقصد به التواجد داخل هذا النظام بالمخالفة لإرادة الشخص صاحب النظام أو من له السيطرة عليه، وتتحقق في الحالة التي يجد الشخص فيها نفسه داخل النظام عن طريق الخطأ أو الصدفة، إلا أنه يقرر البقاء داخل النظام وعدم قطع الاتصال به، ويمكن تصور ذلك في الحالة التي يكون فيها الشخص في سبيله للدخول إلى نظام معلوماتي له الحق في الدخول إليه، إلا أنه يجد نفسه بسبب استخدام شفرة خاطئة داخل نظام آخر.[2]

المشرع الجزائري لم يكتف بتجريم الدخول أو البقاء غير المشروعين في النظام المعلوماتي، بل تجاوز ذلك إلى تجريم مجرد **المحاولة**، وذلك حسب العبارة الواردة في نص المادة 394 مكرر بالقول "**أو يحاول ذلك**"، غير أن ما هو مثار هنا، وهو من الصعوبة بمكان، وهو ما يتعلق بفكرة الإثبات وما من شأنه إعطاء تصور يفيد بأن هناك شروع أو محاولة طالما أن الجريمة في حد ذاتها تطرح إشكالا في الإثبات.[3]

وشدد المشرع الجزائري العقوبة في حالة ترتب عن جريمة الدخول أو البقاء غير المشروع:

---

[1]– زيبحة زيدان، المرجع السابق، ص 48– 49.

[2]– سي حمدي عبد المومن، قيرة سعاد، الجريمة الالكترونية وآليات التصدي لها في القانون الجزائري، مجلة البيان للدراسات القانونية والسياسية، المجلد 07، العدد 01، جوان 2022، ص 64

[3] – زيجة زيدان، المرجع نفسه، ص 51.

– حذف أو تغيير لمعطيات المنظومة، هنا حسب المادة 394 مكرر من قانون العقوبات، الفقرة 2 " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة" .

ويقصد بالحذف كل فعل من شأنه أن يجعل المعطيات غير موجودة أو غير متاحة لمستعملي النظام الشرعيين، أما عن التغيير فهو تعديل للمعطيات الموجودة، ويرى الفقه أن من الصعب التمييز بين فعلي الحذف والتغيير، ذلك أنه لإجراء التغيير فلا مفر من الإلغاء أي الحذف.

وجاء الهدف من هذا التشديد هو حماية سلامة المعطيات التي يحويها النظام المعلوماتي، هذه المعطيات التي أصبحت تمثل قيما مستحدثة يتعين حمايتها إلى جانب ما تتمتع به الأشياء المادية من حماية، ولم يحدد المشرع الجزائري نوع المعطيات المعنية بالحماية، مما يعني أن كافة أنواع المعطيات تشملها الحماية دون تخصيص، في حين أن المشرع الفرنسي قد خص المعطيات ذات الطابع الشخصي بالحماية واعتبرها ظرفا مشددا، من خلال إضافة فقرة ثالثة في المادة 323– 1 من قانون العقوبات الفرنسي، وهو عندما تكون جريمة الدخول أو البقاء داخل النظام قد كانت ضد نظام معالجة للمعطيات ذات الطابع الشخصي التي تقوم به الدولة في هذا المجال.[1]

– تخريب نظام اشتغال المنظومة : هنا تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50,000دج إلى 150,000دج.

– المساس بهيئات ومؤسسات الدولة : حسب المادة 394 مكرر 3 تضاعف العقوبات المنصوص عليها في هذا القسم، أي قسم المساس بأنظمة المعالجة الآلية للمعطيات إذا استهدفت هذه الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاصة للقانون العام.[2]

2– جريمة الاعتراض غير المشروع :عرفت المادة السابعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بأنه الاعتراض المتعمد دون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات .[1]

[1]– بطيحي نسمة، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، مجلة الفقه القانوني والسياسي، المجلد 01، العدد 01، 1– 06– 2019، ص 82–83.

[2]– المادة 394 مكرر 3، من قانون العقوبات الجزائري، المصدر السابق.

وكذلك يقصد بالاعتراض المعلوماتي غير المصرح به، معرفة محتوى الاتصال داخل حاسب واحد أو بين نظامين مختلفين، أو عدة أنظمة ترتبط فيما بينها من خلال التقاط المعلومات التي يتضمنها هذا الاتصال، وبصيغة بسيطة يمكن أن تشبه " أفعال الاعتراض غير المصرح به " بأنها أشبه بأفعال التصنت غير المشروع على محادثة تليفونية، ومن هنا يشكل الاعتراض سلوكا تجسسيا مجرما .

والوسيلة الأبرز لاعتراض النظام المعلوماتي تتمثل في استخدام الموجات الكهربائية الصادرة عن الحاسب الآلي، ويتم اعتراض الحاسب في الولايات المتحدة بـ التقاط الموجات الكهربائية وجمع المعلومات عن بعد، ولهذا فقد عرفت بعض التشريعات أفعال " الالتقاط " ومنها القانون السعودي بأنه " مشاهدة البيانات أو الحصول عليها دون مسوغ نظامي صحيح"، والقانون السوداني بالقول " الالتقاط، مشاهدة البيانات أو المعلومات الواردة في أي رسالة إلكترونية أو سماعها أو الحصول عليها "، أما القانون العماني فقد عرفها بالقول " مشاهدة البيانات الإلكترونية أو الحصول عليها "، أما القانون البرتغالي فقد عرفه "بالقول " الاعتراض، كل عمل يهدف إلى الوصول إلى المعلومات التي تتضمنها أنظمة المعالجة الآلية للمعلومات باستخدام أجهزة كهرومغناطيسية أو سمعية أو ميكانيكية أو غير ذلك".[2]

وموقف بعض التشريعات العربية من جريمة الاعتراض غير المشروع للمعلومات والبيانات، فحسب المادة 16 من قانون مكافحة جرائم تقنية المعلومات المصري، يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه أو بإحدى هاتين العقوبتين كل من اعترض بدون وجه حق أية معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها ".[3]

[1] – المادة السابعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، المصدر السابق.

[2] – عمار عباس الحسيني، المرجع السابق، ص 335.

[3] – المادة 16 من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات المصري، الجريدة الرسمية العدد32 مكرر (ج)، السنة الحادية والستون، 3ذي الحجة سنة 1439 الموافق 14 أغسطس سنة 2018 .

3- الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات

هذا ما نصت عليه المادة الخامسة عشر من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، واعتبرت أنه ما يدخل ضمن هذا النوع من الجرائم.

- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.

- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.

- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.[1]

هناك العديد من التشريعات تناولت في نصوصها جريمة الإرهاب في صورته التقليدية مع ما قد يثار في ظلها من مشكلات قانونية، فإن عددا من التشريعات العربية المتخصصة بجرائم المعلوماتية قد نصت على تجريم أفعال الإرهاب المعلوماتي والعقاب عليها، ومنها دولة الإمارات العربية المتحدة وصدور المرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.

حسب المادة 21 التي تنص على التحبيذ والترويج للجماعات الإرهابية، حيث تعاقب بالسجن مدة لا تقل عن 10 سنوات ولا تزيد عن 25 سنة، والغرامة لا تقل عن 2,000,000 درهم ولا تزيد على 4,000,000 درهم، كل من أنشأ أو أدار موقعا إلكترونيا أو أشرف عليه أو نشر معلومات أو بيانات على الشبكة المعلوماتية أو وسيلة تقنية معلومات لجماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة ، بقصد تسهيل الاتصال بقيادتها أو أعضائها، أو لاستقطاب عضوية لها أو ترويج أو تحبيذ أفكارها أو تمويل أنشطتها، أو توفير المساعدة الفعلية لها، أو بقصد نشر أساليب تصنيع الأجهزة الحارقة أو الأسلحة أو الذخائر أو المتفجرات أو المواد الخطيرة، أو أي أدوات أخرى تستخدم في الأعمال الإرهابية.

وتكون بالعقوبة الحبس لمدة لا تزيد على خمس سنوات والغرامة التي لا تقل عن 500,000 درهم، ولا تزيد على 1,000,000 درهم لمن حمل محتوى أيا من المواقع المشار إليها في الفقرة الأولى

[1]- المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المصدر السابق.

من هذه المادة أو أعاد بثها أو نشرها بأي وسيلة كانت أو تكرر دخوله إليها لمشاهدتها، أو نشر أي محتوي يتضمن التحريض على الكراهية.

وللمحكمة في غير حالات العود بدلا من الحكم بالعقوبة المشار إليها في الفقرة السابقة أن تحكم بإيداع المتهم إحدى دور المناصحة أو الحكم بوضعه تحت المراقبة الإلكترونية، ومنعه من استخدام أيا من وسائل تقنية المعلومات خلال فترة تقدرها المحكمة على ألا تزيد عن الحد الأقصى للعقوبة المقررة.[1]

وعاقب المشرع السعودي بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على 5,000,000 ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

– إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحذ أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات الأجهزة الحارقة أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.

– الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.[2]

ثانيا – الأحكام الإجرائية :

تطرق الفصل الثالث لنطاق تطبيق الأحكام الإجرائية، وكذا التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين، كما تطرق كذلك لأمر تسليم المعلومات، وتفتيش المعلومات المخزنة، وضبط المعلومات المخزنة، من جهة أخرى، تطرق لنقطة الجمع الفوري لمعلومات تتبع المستخدمين واعتراض معلومات المحتوى، وهنا نتطرق لبعض النقاط التي شملها هذا الفصل من بينها:

[1]– المادة 21 من مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الالكترونية، صدر بتاريخ 20 سبتمبر 2021، والعمل به اعتبارا من 02 يناير 2022.

[2]– المادة السابعة من نظام مكافحة جرائم المعلوماتية السعودي لسنة 1428هـ.

1- نطاق تطبيق الأحكام الإجرائية:

حسب الفقرة الأولى من المادة الثانية والعشرون من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، تلتزم كل دولة طرف بأن تتبنى في قانونها الداخلي التشريعات والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في هذا الفصل، أي الفصل الثالث من الاتفاقية.

كذلك مع مراعاة أحكام المادة التاسعة والعشرون " اعتراض معلومات المحتوى "

(أ- تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يختص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من:

- الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة في الطرف.

- التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

ب- إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني إجراءات الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة الطرف فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري لمعلومات المحتوى المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

ج- تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود خدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ هذه الصلاحيات).

على كل دولة طرف بأن تتبنى في قانونها الداخلي التشريعات والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في الفصل الثالث (الأحكام الإجرائية) من هذه الاتفاقية وتطبيقها على:

- الجرائم المنصوص عليها في المواد السادسة إلى التاسعة عشر من هذه الاتفاقية، أي جريمة الدخول غير المشروع، جريمة الاعتراض غير المشروع، الاعتداء على سلامة البيانات،جريمة إساءة استخدام وسائل تقنية المعلومات، جريمة التزوير، جريمة الاحتيال، جريمة الإباحة، المقامرة،

الاستغلال الجنسي، جريمة الاعتداء على حرمة الحياة الخاصة، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة ، الاستخدام الغير مشروع لأدوات الدفع الإلكترونية،...

- أية جرائم أخرى ترتكب بواسطة تقنية المعلومات.

- جمع الأدلة عن الجرائم بشكل إلكتروني.

كما يجوز للدولة الطرف أن تحتفظ بحقها في عدم تطبيق تلك الإجراءات كلما كانت غير قادرة بسبب محدودية التشريع على تطبيقها على الاتصالات التي تبث بواسطة تقنية معلومات لمزود خدمة، وذلك إذا كانت التقنية : - يتم تشغيلها لصالح مجموعة مغلقة من المستخدمين.

- لا تستخدم شبكات اتصال عامة وليست مرتبطة بتقنية: معلومات أخرى سواء كانت عامة أو خاصة.

كذلك على كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة في المادتين 29و30 المتعلقتان باعتراض معلومات المحتوى،وكذلك الاختصاص.[1]

2- التحفظ العاجل على البيانات المخزنة في تقنية المعلومات

حسب المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

أ- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة، بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات، وخصوصا إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل.

ب - تلتزم كل دولة طرف بتبني الإجراءات الضرورية بواسطة استصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته، ومن أجل إلزامه بحفظ وصيانة

[1]- المادة 21 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المصدر السابق.

سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي.

ج- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسئول عن حفظ تقنية المعلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي.[1]

الفرع الثالث

التعاون القانوني والقضائي والأحكام الختامية

سوف نتطرق تحت هذا الفرع بداية للتعاون القانوني والقضائي الذي تطرقت له الاتفاقي، ثم في الأخير لـ الأحكام الختامية التي خرجت بها هذه الأخيرة.

أولا-التعاون القانوني والقضائي: تطرق الفصل الرابع من الاتفاقية للتعاون القانوني والقضائي مسلطا الضوء على عدة نقاط أهمها :

الاختصاص، تسليم المجرمين، المساعدة المتبادلة، المعلومات العرضية المتلقاة، الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة،رفض المساعدة، السرية وحدود الاستخدام، الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات، الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة، التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة، الوصول إلى معلومات تقنية المعلومات عبر الحدود، التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين، التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى.

كذلك تكفل كل دولة طرف وفقا للمبادئ الأساسية لنظامها القانوني، وجود جهاز متخصص ومتفرغ على مدار الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية

[1]- المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المصدر السابق.

المعلومات أو لجمع الأدلة بشكلها الإلكتروني في جريمة معينة،[1]مثلا إجراء الحفظ العاجل للمعلومات المخزنة في أنظمة المعلومات.

1- مفهوم الإجراء: إن الفقرة الأولى من هذه المادة تسمح لكل طرف أن يطلب، والفقرة الثالثة تقرر أن على كل طرف أن يكون لديه الطرق القانونية للحصول على، التحفظ العاجل على بيانات مخزنة لدى نظام معلوماتي في إقليم الطرف المقدم إليه الطلب، حتى لا يتم تغيير هذه البيانات، أو نقلها أو حذفها خلال الفترة الزمنية اللازمة لإعداد ونقل وتنفيذ طلب المساعدة المتبادلة بخصوص الحصول على هذه البيانات.

إن عملية التحفظ عبارة عن إجراء محدود أي طبيعة وقتية معينة للتدخل بطريقة أكثر سريعة من مجرد تنفيذ التماس أو طلب المساعدة المتبادلة التقليدي، إذ أن البيانات المعلوماتية تتسم بأنها سريعة الزوال، إذ يكفي بعض نقرات عادة على مفاتيح الحاسب، أو استخدام بعض البرامج الآلية، حتى يتم حذف هذه البيانات أو تغييرها أو نقلها، مما يؤدي إلى استحالة تتبع مرتكب الجريمة، أو تدمير الأدلة القاطعة على إجرامه، كذلك هناك بضعة أشكال للبيانات المعلوماتية لا يتم تخزينها إلا لفترات قصيرة من الزمن قبل محوها، لهذه الأسباب مجتمعة تم الاتفاق على وجود آلية تضمن توافر هذه البيانات أثناء الفترة الطويلة والمعقدة لتنفيذ الالتماس الرسمي للمساعدة والذي قد يمتد لعدة أسابيع أو شهور.

وإذا كان هذا الإجراء يعد أكثر سرعة من إجراء المساعدة المتبادلة التقليدي، فإنه يمكن أن يعد أقل تدخلا، فهو لا يتطلب من مسئولي المساعدة المتبادلة للشخص المقدم إليه الطلب للاستحواذ على بيانات من الجهة القائمة عليها، إنما كل ما هنالك هو أن الطرف المقدم إليه الطلب يضمن أن هذه الجهة ،وغالبا ما تكون مورد خدمات أو شخص ثالث أن يتحفظ على البيانات ولا يقوم بمحوها انتظارا لصدور أمر بتحويلها إلى السلطات المكلفة بتطبيق القانون في مرحلة لاحقة.

كذلك فإن هذا الإجراء يتسم بكونه عاجلا ويحترم حق الإنسان المعني بهذه البيانات في الخصوصية، لأن تلك البيانات لا يتم كشف سريتها أو فحصها من قبل أي أحد من الموظفين الحكوميين إلا بعد استيفاء المعايير المطبقة بالنسبة لكشف السرية، وفقا لمعاهدات المساعدة المتبادلة

[1]- المواد من 30 الى 43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المصدر السابق.

متعددة الأطراف، ومن ناحية أخرى فإن الطرف المقدم إليه الطلب يكون مسموحا له باستخدام إجراءات أخرى لضمان التحفظ العاجل على البيانات، بما فيها التنفيذ العاجل لأمر تفتيش هذه البيانات، فالشرط الأساسي في كل هذا هو تسريع الإجراءات إلى أقصى حد ممكن لمنع البيانات من الضياع بشكل يتعذر معه استردادها.[1]

2- أحكام إجراء الحفظ العاجل للمعلومات المخزنة عن أنظمة المعلومات:

هذا ما نصت عليه المادة السابعة والثلاثون من الاتفاقية العربية، حيث اعتبرت:

أ- لأي دولة طرف أن تطلب من دولة طرف أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات تقع ضمن إقليمها بخصوص ما تود الدولة الطرف الطالبة للمساعدة أن تقدم طلبا بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات.

ب- يجب أن يحدد طلب الحفظ حسب الفقرة واحد ما يلي :

- السلطة التي تتطلب الحفظ

- الجريمة موضوع التحقيق وملخصا للوقائع

-معلومات تقنية المعلومات التي يجب حفظها وعلاقتها بالجريمة.

- أية معلومات متوفرة لتحديد المسئول عن المعلومات المخزنة أو موقع تقنية المعلومات.

- موجبات طلب الحفظ

-رغبة الدولة الطرف بتسليم طلب المساعدة الثنائية للبحث أو الوصول أو الضبط أو تأمين أو كشف معلومات تقنية المعلومات المخزنة.

[1]-هلالي عبد الله احمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليه، المرجع السابق، ص366،367.

ج- عند استلام إحدى الدول الأطراف الطلب من دولة طرف أخرى، فعليها أن تتخذ جميع الإجراءات المناسبة لحفظ المعلومات المحددة بشكل عاجل بحسب قانونها الداخلي، ولغايات الاستجابة إلى الطلب فلا يشترط وجود ازدواجية التجريم القيام بالحفظ.

د-أي دولة طرف تشترط وجود ازدواجية التجريم للاستجابة لطلب المساعدة، يجوز لها في حالات الجرائم عادا المنصوص عليها في الفصل الثاني من هذه الاتفاقية، أن تحتفظ بحقها برفض طلب الحفظ حسب هذه المادة إذا كان هناك سبب للاعتقاد بأنه لن يتم تلبية شرط ازدواجية التجريم في وقت الكشف.

هـ- بالإضافة لذلك، يمكن رفض طالب الحفظ إذا : أ- تعلق الطلب بجريمة تعتبرها الدول الطرف المطلوب منها جريمة سياسي، ب- اعتبار الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سيادتها أو أمنها أو نظامها أو مصالحها.

و- حيثما تعتقد الدولة الطرف المطلوب منها المساعدة بأن الحفظ لن يضمن التوفر المستقبلي للمعلومات أو سيهدد سرية تحقيقات الدولة الطرف الطالبة لها أو سلامتها، فيجب عليها إعلام الدولة الطرف الطالبة لها لتحدد بعدها مدى إمكانية تنفيذ الطالب.

ز- أي حفظ ناجم عن الاستجابة للطلب المذكور في (الفقرة واحد) يجب أن يكون لفترة لا تقل عن 60 يوما من أجل تمكين الدولة الطرف الطالبة من تسليم طلب البحث أو الوصول أو الضبط أو التأمين أو الكشف للمعلومات، وبعد استلام مثل هذه الطلب يجب الاستمرار في حفظ المعلومات حسب القرار الخاص بالطلب.[1]

ثانيا- الأحكام الختامية :

تضمن الفصل الخامس من الاتفاقية الأحكام الختامية أهمها:

1- العمل على اتخاذ الإجراءات الداخلية اللازمة لوضع هذه الاتفاقية موضع التنفيذ من طرف الجهات المختصة لدى الدول الأطراف.

2- الانضمام لهذه الاتفاقية مفتوح للدول غير الموقعة بالنسبة لدول الجامعة العربية.

[1]- المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المصدر السابق.

3- عدم جوازية الدول الأطراف أن تبدي أي تحفظ ينطوي على مخالفة لنصوص هذه الاتفاقية أو الخروج عن أهدافها.

4- يجوز الاقتراح أي تعديل للدولة الطرف وفق إجراءات.

5-جواز الانسحاب من هذه الاتفاقية وفق إجراءات.

الجزائر بناء على تقرير وزير الشؤون الخارجية وبناء على الدستور، لاسيما المادة 77-11 منه، وبعد الاطلاع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21-12-2010، بموجب مرسوم رئاسي رقم 14-252 مؤرخ في 13 ذي القعدة عام 1435 الموافق ل8-9-2014م، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ21-12-2010م.

الفصل الثاني

الاتجاهات الدولية في مجال مكافحة الجرائم المعلوماتية

الفصل الثاني

الاتجاهات الدولية في مجال مكافحة الجرائم المعلوماتية

إن مكافحة الجرائم المعلوماتية لن يكون له أي تأثير يذكر إلا إذا كان هناك تعاونا دوليا مع ضرورة التنسيق والتعاون الدولي في مجال مكافحة الجرائم المعلوماتية بما يضمن نجاح جهود المكافحة في هذا المجال مع استمرار التعاون بين الأجهزة المعنية بمكافحة هذه الجرائم داخل كل دولة وتعزيز جهود الأمم المتحدة لاستخدام شبكة المعلومات الدولية (الانترنت) في الأعمال الايجابية.

أن أي مجهود أو إجراءات قد تقوم بها أي من الدول على مستوى العالم لن يأتي بأي نتائج ملموسة تحد من ارتكاب تلك النوعية من الجرائم، فتلك الجرائم لها طابع خاص تتسم به هو أنها جرائم عابرة الحدود، فهي لا تتم من داخل دولة ويكون تأثيرها منحصر في تلك الدولة وإنما تلك الجرائم ترتكب عبر عدد من الدول لتتم في دول أخرى وتكون آثارها ممتدة إلى عدد غير محدود من الدول، وعليه فإن الأساس الذي يرتكز عليه مجال مكافحة الجرائم المعلوماتية هو التعاون الدولي وتنسيق الجهود المبذولة بين كافة دول العالم، وبدون هذا التعاون لن يكون هناك أي أثر لأي مجهود تقوم به أي من الدول بمفردها.[1]

طبقا للمعطيات السابقة تحت هذا الفصل قسمنا هذا الأخير إلى مبحثين، المبحث الأول تم التطرق فيه للتعاون الدولي في مجال مكافحة جرائم المعلوماتية وإشكالاته أما المبحث الثاني فتم معالجته تحت عنوان الطريق نحو اتفاقية عالمية لمكافحة الجريمة السيبرانية برعاية الأمم المتحدة بحدود 2023 في ظل تجاذبات القوى الكبرى.

[1] – محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية، المكتبة العصرية للنشر والتوزيع، المنصورة ، جمهورية مصر العربية، الطبعة الأولى 2010، ص411.

المبحث الأول

التعاون الدولي في مجال مكافحة جرائم المعلوماتية وإشكالاته

تعد الجرائم المعلوماتية إحدى أهم صور الجرائم ذات البعد الدولي العابر للحدود، حيث لم تعد تلك الحدود بعد تشكل حاجزا أمام مرتكبي هذه الجرائم، كما أن نشاط هؤلاء الجناة لم يعد قاصرا على إقليم معين بل امتد إلى أكثر من إقليم، بحيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في بلدن معين، ويقبل على التنفيذ في بلد آخر، ويهرب إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة، فالجريمة أصبح لها طابع دولي، والمجرم أصبح مجرما دوليا.[1]

إن التعاون والتضامن الدولي أمر هام جدا في مجال مكافحة جرائم المعلوماتية، وبدون هذا التعاون الدولي لن يكون هناك أي أثر لأي مجهود تقوم به أي من الدول بمفردها، نظرا لأنه سيكون عديم الفائدة وبلا أثر تقريبا، ولن يؤدي إلى الحد من ارتكاب تلك الجرائم التي تكون في الأغلب الأعم من الجرائم عابرة للحدود.[2]

وعليه تطرقنا تحت هذا المبحث لمطلبين ، المطلب الأول عالجنا فيه موضوع التعاون الدولي في مجال مكافحة الجريمة المعلوماتية ، وفي المطلب الثاني تطرقنا لإشكالات هذا التعاون .

[1]– عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 11.

[2] – محمد محمود المكاوي، المرجع السابق، ص419.

المطلب الأول

التعاون الدولي في مكافحة الجريمة المعلوماتية

لم تعد جرائم المعلوماتية حبيسة النطاق الإقليمي لكل دولة، وكأن دول العالم مربعات منعزلة عن رقعة شطرنج، إذ أن نطاقها لا يقتصر على المستوى المحلي أو القومي، بل يمتد ليشمل المستوى الإقليمي والدولي، فهي بمثابة وباء حقيقي يحتاج إلى تحرك عالمي.

ومن هذا المنظور، كانت فكرة التعاون الدولي وضرورة تفعيله من أجل مواجهة هذه النوعية من الجرائم العابرة للحدود والقارات، والجزائر جزء لا يتجزأ من نسيج هذا العالم الذي نعيش فيه.[1]

ومن أجل استجلاء فكرة الالتزام بالتعاون الدولي لمواجهة جرائم المعلوماتية، فإننا سنتحدث عن أوجه التعاون الدولي في مكافحة الجرائم المعلوماتية.

- التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى الأمني.
- التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى القضائي.
- التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى تسليم المجرمين

الفرع الأول

التعاون الدولي في مواجهة الجريمة المعلوماتية على المستوى الأمني:

أولا- مفهوم التعاون الأمني الدولي:

بالنظر إلى التعاون الأمني الدولي بمفهومه الواسع، نجد أنه يشمل مجالات مختلفة، كالمجال الشرطي، والمجال القانوني، والمجال القضائي، ومرد ذلك أن تحقيق الأمن يتطلب تنفيذ إجراءات

[1]- هلالي عبد اللاه أحمد، الموجهة الجنائية لجرائم المعلوماتية في النظام المصري والبحريني على ضوء اتفاقية بودابست، المرجع السابق، ص243.

تتعلق بتلك المجالات مجتمعة، والتعاون الأمني الدولي لا يقتصر على إجراءات ملاحقة الأشخاص المطلوبين للعدالة وحسب، بل يتعدى الأمر ذلك ليشمل مكافحة الجريمة بشقيها الوقائي والقمعي، بل يشمل العناية بحقوق المتهمين والضحايا، ومراعاة حقوق الدول وسيادتها، ويعرف التعاون الأمني الدولي بأنه " تبادل العون والمساعدة وتضافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشاركة في مجال التصدي لمخاطر الإجرام، وما يرتبط به من مجالات أخرى، مثل مجال العدالة الجنائية، ومجال الأمن، أو لتخطي مشكلات الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين وتعقب مصادر التهديد، سواء أكانت المساعدة المتبادلة قانونية أو قضائية أو شرطية، وسواء اقتصرت على دولتين فقط أو امتدت إقليميا أو عالميا"، ويعد التعاون الأمني الدولي ثمرة تطور العلاقات الدولية، ونتيجة حتمية لما تشهده الجريمة من تطور متلاحق يكاد يقفز في أرقامه من عام إلى آخر حتى أصبح تطور الجريمة في حد ذاته ظاهرة دولية.[1]

ثانيا– ضرورة التعاون الأمني الدولي:

حتى يسهل لكل دولة الاستمرار والعيش من غيرها من الدول، فإنها تحتاج إلى قدر من الأمن والنظام، وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، فنتيجة التطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات، وظهور الإنترنت والانتشار الواسع والسريع لها، أدى إلى ظهور أشكال وأنماط جديدة من الجرائم، منها الجرائم المعلوماتية التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها، بل تعدت ذلك، ومع تمييزها بالعالمية وبكونها عابرة للحدود، فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدولة المختلفة، وذلك إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي هذا النوع من الجرائم وتعميمها، فمثلا في جرائم البث والنشر الفيروسي، قد يكون مرتكب الهجوم يحمل جنسية دولة ما ويشن هجوما فيروسي من حواسب موجودة في دولة

[1]– عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 19، 20.

أخرى، وتقع الآثار المدمرة لها الهجوم في دولة ثالثة، فمن البديهي أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها[1].

لذلك لابد من أن يكون هناك تعاون دولي يتفق مع طبيعة هذه الجرائم، والتي تتميز بطابع خاص يقتضي أن تكون هناك إجراءات تحقيقية سريعة، ويسمح هذا التعاون الدولي بسهولة الاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك عن طريق إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالحاسوب والإنترنت وتعميمها، والدولة بمفردها لا تستطيع القضاء على هذه الجرائم لأنها عابرة للحدود، لذلك فإن الحاجة ملحة إلى تعاون أجهزة الشرطة بين الدول وتنسيق العمل فيما بينها لضبط المجرمين ومكافحة هذه الجرائم.[2]

وأصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة، وتتعاون من خلال أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة، بالإضافة إلى تعقب المجرمين الفارين من وجه العدالة، و من أساليب هذا التعاون الدولي: التعاون الشرطي، والإداري، اللذان يمكنهما أن يحققا أهدافا لا قبل للأجهزة الشرطية والإدارية الإقليمية أن يحققاها في مجال مكافحة هذه الجريمة.

فقد ظهرت العديد من الأجهزة في هذا المجال منها: المنظمة الدولية للشرطة الجنائية "الأنتربول"، مركز الشرطة الأوروبية أو "الأوروبول"، الأورجست، شنجن، المكتب العربي للشرطة الجنائية، أما التعاون الإداري فيكون من خلال التعاون على صعيد الإجراءات والأوامر والقرارات التي تتم من أجل المحافظة على النظام العام في المجتمعات الأطراف في المعاهدات والاتفاقيات.[3]

[1] – يوسف حسن يوسف، المرجع السابق، ص 144.

[2]–أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، دراسة تحليلية تأصيلية مقارنة، المركز القومي للإصدارات القانونية، القاهرة، مصر، الطبعة الأولى 2017، ص 128، 129.

[3]– عبد الله سيف المكتوب، المرجع السابق، ص 220 ،223.

ثالثا- التعاون الأمني وجهود الإنتربول" المنظمة الدولية للشرطة الجنائية" في مكافحة الجريمة المعلوماتية":

الإنتربول "بالإنجليزية Interpol " هي اختصار لكلمة الشرطة الدولية "بالإنجليزية international police"، والاسم الكامل لها هو منظمة الشرطة الجنائية الدولية "بالإنجليزية international **criminal police organization**"، وهي أكبر منظمة شرطة دولية أنشئت في عام 1923 ومقرها الرئيسي في مدينة ليون بفرنسا.[1]

هي منظمة حكومية دولية فيها 195 بلدا عضوا، انضمت إليها الجزائر في 1963، مهمتها أن تساعد أجهزة الشرطة في جميع هذه الدول، على العمل معا لجعل العالم مكانا أكثر أمنا، فهي تمكن البلدان من تبادل البيانات المتعلقة بالجرائم والمجرمين والوصول إليها، وتقدم الدعم الفني والميداني بمختلف أشكاله.[2]

1-هياكل الإنتربول: تتوالى الأمانة العامة للانتربول تنسيق الأنشطة اليومية لمكافحة مجموعة من الجرائم، ويديرها الأمين العام[3]، يعمل في الأمانة العامة ضباط الشرطة والمدنيين، وهي تتخذ من **ليون** مقرا لها، ولها مجمع عالمي للابتكار في سنغافورة والعديد من المكاتب الفرعية في مناطق مختلفة من العالم، وفي كل بلد يشكل المكتب المركزي الوطني للانتربول[4] نقطة الاتصال الأساسية للأمانة العامة

---

[1]- ويكيبيديا.

[2]-www.interpol.int/ar/3/3

الزيارة للموقع يوم 2022/08/17، على الساعة 09:59

[3]- الأمين العام الحالي، الألماني السيد يورغن شتوك، وقد عين في الدورة الـ 83 للجمعية العامة في موناكو في نوفمبر 2014، وأعيد تعيينه في الدورة الـ88 للجمعية في شيلي في عام 2019 لتفويض ثان مدته خمس سنوات.

[4] - المكتب المركزي الوطني هو جهة الاتصال في البلد لجميع أنشطة الانتربول، كل من البلدان الأعضاء تستضيف مكتبا مركزيا وطنيا للانتربول(NCB)، وهذا ما يربط أجهزة إنفاذ القانون الوطنية لديها بالبلدان الأخرى وبالأمانة العامة عبر شبكة اتصالات الشرطة العالمية الآمنة المسماة I-24/7(المنظومة العالمية للاتصالات الشرطية)، العديد من الجرائم اليوم لها جانب دولي، كالجرائم السيبرية والفارين أو السلع المسروقة أو غير المشروعة التي تقودها جماعات الجريمة المنظمة، عندما تتجاوز الجريمة ولايته القضائية الوطنية، يحتاج البلد دعم دولي لحلها.

و المكاتب المركزية الوطنية الأخرى، يتولى ضباط الشرطة الوطنية إدارة المكتب المركزي الوطني، ويكون الأخير عادة تابعا للوزارة الحكومية المسئولة عن العمل الشرطي.

أما الجمعية العامة فهي الهيئة الإدارية العليا التي تجمع كافة البلدان مرة في السنة لإتخاذ القرارات.[1]

2- الوصل بين أجهزة الشرطة: يتم تأمين الرابط بين جميع البلدان عبر ما يعرف بـ المنظومة العالمية للاتصالات الشرطية I-24/7 ، وتستخدم الدول هذه الشبكة الآمنة لتتصل بغيرها من الدول وبالأمانة العامة للانتربول، كذلك تتيح هذه المنظومة للبلدان الوصول إلى قواعد البيانات وإلى الخدمات بشكل آني، سواء من مواقع مركزية أو نائية، وتتولى أيضا تنسيق شبكات ضباط الشرطة والخبراء في مختلف مجالات الجريمة، الذين يجتمعون في الفرق العاملة وفي المؤتمرات لتبادل الخبرات والأفكار.[2]

3- مهمة الانتربول: توفر الأمانة العامة للبلدان الأعضاء مجموعة من الخبرات و الخدمات، فالانتربول تتدبر 19 قاعدة بيانات شرطية، تحتوي على معلومات عن الجرائم و المجرمين (كالأسماء وبصمات الأصابع وجوازات السفر المسروقة)، والتي يمكن للبلدان الاستفادة منها بشكل آني.

وتقدم أيضا الدعم في التحقيقات عن طريق تحليل الأدلة الجنائية، والمساعدة في تحديد مكان الفارين من العدالة في جميع أنحاء العالم.

ويعيد التدريب جزءا بارزا من العمل في الكثير من المجالات حتى يصبح الموظفين ملمين بكيفية الاستفادة من خدمات الانتربول بشكل فعال.

وتخصص خبرات هذا الجهاز لدعم الجهود الوطنية في مكافحة الجرائم في ثلاثة مجالات عالمية والتي تعتبر أكثر إلحاحا اليوم، وهي الإرهاب، والجريمة السيبرية، والجريمة المنظمة.

---

[1] -www.interpol.int/ar/3/3

[2]- www.imterpol.int/ar/3/3 الزيارة يوم 17-08-2022 على الساعة10:58

يتولى الموظفون العاملون في كل من مجالات الجريمة المتخصصة هذه، إدارة مجموعة غنية من مختلف الأنشطة مع البلدان الأعضاء، منها إسناد التحقيقات، والعمليات الميدانية والتدريب...، والأهم من ذلك استشراف المستقبل من خلال البحث في الجرائم الدولية و اتجاهاتها ومتابعة آخر المستجدات المتصلة بها.[1]

أنشأت المنظمة الدولية الجنائية "الإنتربول" في مجال الجرائم المعلوماتية خلال عام 2004 **وحدة خاصة لمكافحة جرائم التكنولوجيا**، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى (G8) بوضع استراتيجيات لمواجهة هذا النوع من الجرائم، من خلال إنشاء مركز اتصالات أمني عبر الشبكة يعمل على مدار 24 ساعة و7 أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف، واستخدام وسائل حديثة في تلك المكافحة، كاستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الأطراف، من خلال استخدام برنامج للتحليل والمقارنة لتلك الصور، وتزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق فيها وغير ذلك .[2]

عرض الإنتربول في تقريره السنوي بعضا من أبرز الأنشطة التي نفذها في **عام 2021، منها التطرق لأمن الفضاء السيبيري**، ومن أبرز الأنشطة في هذا المجال:

أسفر تحقيق وعملية نفذا على مدى 30 شهرا في عدة قارات عن اعتقال أشخاص وإصدار نشرات حمراء بشأن مشبوهين يعتقد أنهم يقفون وراء شبكة عالمية ترتكب جرائم سيبرية باستخدام برمجيات خبيثة، وعممت نشرتان حمراوان (النشرة الحمراء هي تنبيه يتعلق بالأشخاص المطلوبين على مستوى الدولي) على البلدان 194 الأعضاء في الإنتربول بناء على طلب قدمته الشعبة الكورية للتحقيقات في الجريمة السيبرية عبر المكتب المركزي الوطني للإنتربول في سيئول.

ويأتي إصدار النشرتين بعد أن اعتقلت أوكرانيا ستة أعضاء في عصابة مشهورة مختصة ببرمجيات انتزاع الفدية، وذلك في سياق عملية نسقها الإنتربول على الصعيد العالمي بالتعاون مع أجهزة إنفاذ

[1]–www.imterpol.int/ar/3/3 الزيارة يوم 17–08–2022 على الساعة 11:22

[2]– فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الالكترونية، مجلة البحوث في الحقوق والعلوم السياسية، 03–06–2022، المجلد 08، العدد 01، ص 438.

القانون في أوكرانيا وكوريا والولايات المتحدة في **يونيو 2021**، وتأتي هذه المداهمة العالمية التي تحمل الاسم الرمزي "عمليةcyclone " في أعقاب تحقيقات أجرتها الشرطة على المستوى العالمي في اعتداءات على شركات كورية، ومؤسسات أكاديمية أمريكية شنتها هذه العصابة عن طريق بث برمجية انتزاع الفدية CIOP، وأفيد بأن القراصنة مستخدمي برمجيةCIOP في أوكرانيا قد استهدفوا في اعتداءاتهم، كيانات خاصة ومؤسسات تجارية في كوريا، والولايات المتحدة فمنعوها من الوصول إلى ملفاتها وشبكاتها الحاسوبية ، ثم طلبوا فدى باهظة لمنعها هذا الوصول مجددا، ويعتقد أن المشتبه فيهم قد سهلوا نقل وقبض أصول مالية لحساب العصابة الأنفة الذكر، مهددين في الوقت نفسه أيضا بتعميم بيانات حساسة إذا لم يدفع لهم المزيد من الأموال، ونسق عملية cyclon مركز الإنتربول المتعدد الاختصاصات **لمكافحة الجريمة السيبرية** في سنغافورة، حيث تبادلت الجهات المعنية بيانات الاستخبارات في إطار تفاعلي ومأمون عبر شبكة الإنتربول وأدواته العالمية، وتمكنت الشرطة الأوكرانية بفضل البيانات الإستخباراتية التي جمعت من إجراء أكثر من 20 عملية تفتيش في منازل وشركات ومركبات، ومن مصادرة ممتلكات وحواسيب وضبط مبلغ 185000 دولار أمريكي نقدا، فضلا عن اعتقال ستة أشخاص.

وقال مدير مكافحة الجريمة السيبرية لدى الإنتربول كريغ جونز: " بالرغم من اشتداد وطأة الاعتداءات المرتكبة باستخدام برمجيات انتزاع الفدية على الصعيد الدولي، أسفر هذا التحالف بين الشرطة والقطاع الخاص على أولى الاعتقالات في أوساط عصابات الجريمة السيبرية، من قبل أجهزة إنفاذ القانون، ما يوجه رسالة قوية إلى مرتكبي هذه الاعتداءات مفادها أننا سنلاحقهم دون هوادة أينما اختبئوا في الفضاء السيبري".[1]

ونفذت المنظمة عملية cyclone ، بفضل المعلومات التي قدمها شركاؤها من القطاع الخاص، أي trend microومعهد الدفاع السيبريkasperskylabو fortinetو palo alto networksو group-ib من خلال مشروع الإنتربولgateway، ويرمي هذا المشروع إلى تعزيز الشراكات بين

[1] -www.interpol.int/ar/1/1/2021/57 الزيارة يوم 17-08-2022 على الساعة15:30

أجهزة إنفاذ القانون والقطاع الخاص من أجل جمع بيانات عن التهديدات من شتى المصادر، وتمكين أجهزة الشرطة من منع الاعتداءات.[1]

هذه المنظمة إنما تهدف إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة، مع تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة إليها وتبادلها فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف ومدها بالمعلومات المتوفرة لديها على إقليمها، وخاصة بالنسبة للجرائم المتشعبة على عدة دول ومنها جرائم الإنترنت.[2]

باتت الجرائم اليوم تتخذ طابعا دوليا أكثر فأكثر، ومن بالغ الأهمية بمكان أن يجري التنسيق بين كافة الجهات الفاعلة في الحفاظ على بنية أمنية عالمية، وبما أن الأنتربول منظمة عالمية، فإنه قادر على أن يشكل منبرا للتعاون، وذلك لأنه يمكن أجهزة الشرطة من العمل مباشرة مع بعضها البعض حتى بين الدول التي لا تربطها علاقات دبلوماسية. كما أنها بمثابة لسان ناطق باسم الشرطة على الساحة العالمية، فتعمل مع الحكومات على أعلى المستويات لحتها على التعاون والاستفادة من خدماتها.[3]

الفرع الثاني

التعاون الدولي في مواجهة الجريمة المعلوماتية على المستوى القضائي

بما أن الجرائم المعلوماتية ذات طابع عالمي، وبالتالي يمكن أن تتعدى آثارها عدة دول، فإن ملاحقة مرتكبي هذه الجرائم وتقديمهم للمحاكمة وتوقيع العقاب عليهم، يستلزم القيام بأعمال إجرائية خارج حدود الدولة، حيث ارتكبت الجريمة أو جزء منها، مثل معاينة موقع الإنترنت في الخارج، أو ضبط الأقراص الصلبة التي توجد عليها معلومات غير مشروعة أو صور إباحية، أو القبض على

---

[1]– www.interpol.int/ar/1/1/2021/57 الزيارة يوم 17-08-2022 على الساعة15:30

[2]– عبد الله سيف المكتوب، المرجع السابق، ص229.

[3] – www.interpol.int/ar/3/3 الزيارة يوم17-08-2022 على الساعة 16:00

المتهمين أو سماع الشهود، أو اللجوء إلى الإنابة القضائية، أو تقديم المعلومات التي يمكن أن تساعدهم في تحقيق هذه الجرائم، كل ذلك لا يمكن تحقيقه بدون تعاون قضائي بين الدول، ويتخذ التعاون القضائي الدولي في هذا المجال عدة صور أهمها : المساعدة القضائية بما فيها من نقل الإجراءات، الإنابة القضائية الدولية،[1] وتبادل المعلومات، وغيرها.

أولا- تعريف المساعدة القضائية الدولية:

هي" كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم".[2]

لكن هذه الإجراءات تتطلب إجراء تحديثات في الاتفاقيات الدولية، لكي تواكب التطورات و الإشكالات المستحدثة من الجرائم التي تمتاز بالسرعة، وبالتالي فإن ملاحقة مرتكبي هذه الجرائم وتقديمهم للعدالة من أجل توقيع العقاب عليهم يستلزم القيام بإجراءات إجرائية خارج حدود الدولة، حيث ارتكبت الجريمة أو جزء منها.

ومن هذه الإجراءات معاينة مواقع الإنترنت في الخارج أو ضبط الأقراص الصلبة، أو تفتيش نظام الحاسوب الآلي، وهذا كله قد يصطدم بمشاكل الحدود و الولايات القضائية.[3]

وقد تعرضت اتفاقية الأمم المتحدة لمكافحة الجريمة إلى ضرورة تفعيل المساعدة القضائية المتبادلة بين الدول في مرحلة التحقيق أو المحاكمة، والمتعلقة بالجرائم المنصوص عليها في هذه الاتفاقية، حيث نصت المادة 18 منه على أن تقدم الدول الأطراف لبعضها البعض، أكبر قد ممكن من المساعدة القانونية المتبادلة في التحقيقات والملاحقات والإجراءات القضائية، فيما يتصل بالجرائم المشمولة بهذه الاتفاقية، وترتبط المساعدة القضائية بما تقدمه دولة ما من إجراءات من شأنها تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم، وتعتبر الاتفاقية الدولية منبع الالتزامات بين

[1]- عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 30.

[2]- عبد الله سيف المكتوب، المرجع السابق، ص 201.

[3]- خالد حازم إبراهيم، المرجع السابق، ص382.

الدول، على أن يظل ما ليس ملزما ممكنا، وفقا لما ينص عليه القانون الداخلي في كل من الدولتين، وقد أدرجه المشروع الجزائري ونص عليه في القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مادته 16، معتبرا أنه في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية، يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.[1]

ثانيا- صور المساعدة القضائية الدولية:

1- تبادل المعلومات:

توفر هذه الآلية للدول المتعاونة كافة المعلومات الصحيحة والموثقة المتاحة من خلال متابعة نشاط المنظمات الإجرامية ومصادر وحركة أموالها، لذلك فقد أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين بتطوير التبادل المنهجي للمعلومات، وأن تقوم منظمة الأمم المتحدة بإنشاء قاعدة معلوماتية لإعلام الدول الأطراف بالاتجاهات العالمية في مجال الجريمة، وهو ما يصدق على الجريمة المعلوماتية، وهو ما أكده اتفاق شنغان للاتحاد الأوروبي، من خلال صياغتة نظاما متكاملا لتبادل المعلومات، لذلك تعتبر الوقاية من خلال المعلومات عنصرا جوهريا، والقاعدة الأساسية للكفاح ضد الجريمة المعلوماتية، وضمان خلق نظام فعال للمواجهة وعلى هذا الأساس، تبتت مسودات الاتفاقية الخاصة بمكافحة الجريمة المنظمة تبادل المعلومات بوصفة آلية وقائية للكفاح ضد هذه الجريمة، نصت (المادة 2/12) من مشروع الاتفاقية الإطارية على أنه على الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي للأشخاص المتورطين في الجرائم المنظمة.[2]

ولهذه الصورة من صور المساعدة القضائية الدولية، صدى كبير في كثير من الاتفاقيات كالبند (و) والبند (ز) من الفقرة الثانية من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة

[1]- فريد ناشف، المرجع السابق، ص 440

[2]- طارق عفيفي صادق أحمد، المرجع السابق، ص 202.

في المسائل الجنائية، والبند أولا من المادة الرابعة من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي.[1]

وذات الصورة نجدها في المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي، و المادة الأولى والثانية من النموذج الاستراتيجي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي، ويوجد لها تطبيق كذلك في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000 في البنود الثالث والرابع والخامس من المادة الثامنة منها.[2]

وفي الجزائر نص المشرع الجزائري في المادة 17 من القانون رقم 04/09 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،على أنه تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة، والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل.[3]

2-نقل الإجراءات:

يقصد بنقل الإجراءات قيام دولة بناءا على اتفاقية باتخاذ إجراءات جنائية بصدد جريمة ارتكاب في إقليم دولة أخرى، ولمصلحة هذه الدولة، وذلك ضمن شروط معينة وهي:

- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوبة إليها.
- أن تكون الإجراءات المطلوبة اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة.
- أن يكون الإجراء المطلوب اتخاذه يؤدي إلى الوصول إلى الحقيقة، كأن تكون أدلة الجريمة موجودة بالدولة المطلوب إليها.[4]

---

[1]- خالد حازم إبراهيم، المرجع السابق، ص 383.

[2]- يوسف حسن يوسف، الجرائم الدولية الإنترنت، المركز القومي لإصدارات القانونية، القاهرة، مصر،الطبعة الأولى 2011 ص 151.

[3]- المادة 17 من القانون رقم 09-04، المصدر السابق.

[4]- أحمد عبد اللاه المراغي، المرجع السابق، ص 130 ،131.

وهذا ما أكدت عليه **المادة 21** تحت عنوان نقل الإجراءات الجنائية من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (نوفمبر 2000)، حيث نصت على أنه : تنظر الدول الأطراف في إمكانية أن تنقل إحداها إلى الأخرى إجراءات الملاحقة المتعلقة بجرم مشمول بهذه الاتفاقية، في الحالات التي يعتبر فيها ذلك النقل في صالح سلامة إقامة العدل، وخصوصا عندما يتعلق الأمر بعدة ولايات قضائية، وذلك بهدف تركيز الملاحقة، وإلى مثل هذا أيضا نصت المادة التاسعة من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999 في المادة التاسعة حيث نصت على "لكل دولة طرف أن تطلب إلى أية دولة أخرى متعاقدة القيام في إقليمها نيابة عنها بأي إجراء قضائي متعلق بدعوى ناشئة عن جريمة إرهابية وبصفة خاصة.

- سماع شهادة الشهود، والأقوال التي تؤخذ على سبيل الاستدلال.

- تبليغ الوثائق القضائية.

- تنفيذ عمليات التفتيش والحجز.

- إجراء المعاينة وفحص الأشياء.

- الحصول على المستندات أو الوثائق أو السجلات اللازمة أو نسخ مصدقة منها.[1]

وحسنا فعل المشرع الجزائري في سياسته الجنائية، حينما قام بالتصديق على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، خاصة في مجال مكافحة الجرائم الإلكترونية على اعتبار أنه لا يمكن لدولة بمفردها القيام بذلك نظرا للطبيعة الخاصة لهذه الجرائم المستحدثة، من جهة أخرى اتجاه المشرع إلى إبرام الاتفاقيات الثنائية في هذا المجال قصد التعاون على مكافحة هذا النوع المستحدث من الجرائم، مثل إبرام اتفاقيتين ثنائيتين مع فرنسا الأولى سنة 2007 في مجال التعاون في مكافحة الجرائم المنظمة، والثانية بتاريخ 10/15/ 2016 بخصوص التعاون القضائي في المجال

[1]- عبد الله سيف المكتوب، المرجع السابق، ص 204.

الجنائي و المتعلقة بمكافحة الجريمة المنظمة العابرة للأوطان، ومنها الجرائم الإلكترونية بكافة أشكالها.[1]

3- الإنابة القضائية الدولية:

يقصد بالإنابة القضائية طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة المنيبة إلى الدولة المنابة، لضرورة ذلك في الفصل في مسألة معروضة على السلطات القضائية في الدولة المنيبة ويتعذر عليها القيام به بنفسها، فالإنابة القضائية على هذا النحو، تسهيل الإجراءات الجنائية وتكفي لإحداث تعاون إجرائي دولي بما يكفل إجراء التحقيقات اللازمة لكشف الحقيقة، و يتضمن سماع الشهود وإجراء المعاينات وكافة إجراءات التحقيق، وترسل للدولة المنابة ملف بالدعوى الجنائية بمحاضر الاستدلالات والتحقيقات والمستندات، ويبين في طلب الإنابة الإجراء المراد اتخاذه تحديدا، أو يرسل الطلب من الجهات القضائية و بالطريق الدبلوماسي، وفي هذا الصدد الإنابة القضائية مع هذا النحو تستلزم وقتا أكثر مما يحتمل الأمر في العالم الافتراضي، وهو ما يستلزم ضرورة التعاون القضائي بصور أكثر وبما يحقق عنصر الزمن و أهمية في مجال مواجهة الجريمة الإلكترونية لكون سلوك الطريق الدبلوماسي يستغرق وقت لا تتحمله سمة الجريمة الإلكترونية وأدواتها ووسائل ارتكابها.[2]

أ- مراحل الإنابة القضائية

وتتحقق الإنابة القضائية الدولية في إحدى المرحلتين:

- المرحلة الأولى- مرحلة التحقيق الابتدائي:

في هذه المرحلة، قد تشمل الإنابة مباشرة إجراء معين من إجراءات التحقيق، كسؤال متهم أو شاهد يقيم خارج حدود إقليم الدولة على سبيل المثال، وقد تشمل جميع أعمال التحقيق كسماع الشهود،

[1]- يزيد بوحليط، المرجع السابق، ص 510.

[2]- محمود عبد العزيز أبا زيد، المرجع السابق، ص 317 ،318.

والمواجهات وندب الخبراء، وضبط الأشياء، والتفتيش، واستجواب المتهمين، بيد أنه لا يجوز أن يطلب في الإنابة القضائية حبس المتهم المراد استجوابه، لأن هذا الإجراء لا يتخذ إلا عند التسليم.

- المرحلة الثانية – مرحلة التحقيق النهائي أو المحاكمة:

يجوز للمحكمة أثناء نظر الدعوى أن تنيب إحدى السلطات الأجنبية في اتخاذ إجراء أو أكثر من إجراءات المحاكمة، كإجراء المعاينة مثلا أو سماع شاهد أو أكثر موجود في الخارج.

ب- أساس الإنابة القضائية:

تجد الإنابة القضائية أساسها في القوانين الوطنية وفي الاتفاقيات الدولية، وفي مبدأ المعاملة بالمثل، وتطبيقا لذلك نصت المادة 21 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية عام 2000 على أنه " يتعين على الدول الأطراف أن تنظر في إمكانية أن تنقل إحداها إلى الأخرى إجراءات الملاحقة المتعلقة بجم مشمول بهذه الاتفاقية، في الحالات التي يعتبر فيها ذلك النقل في صالح السير السليم للعدالة و خصوصا عندما يتعلق الأمر بعدة ولايات قضائية، وذلك بهدف تركيز الملاحقة".[1]

ثالثا- القيود الواردة على طلب المساعدة القضائية الدولية:

في الجزائر حسب المادة 18 من القانون رقم 09-04 المؤرخ في 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فإنه يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.

[1]- محمد علي سويلم، المرجع السابق، ص 782 ،783.

كما أنه يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة، أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.[1]

وحسب المادة 31 من القانون القطري رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، لا يجوز رفض طلب المساعدة القانونية المتبادلة إلا في الحالات التالية:

1- إذا لم يكن الطلب صادرا عن جهة مختصة طبقا لقانون الدولة التي تطلب المساعدة، أو إذا لم يرسل الطلب وفقا للقوانين المعمول بها، أو إذا كانت محتوياته تتضمن مخالفة جوهرية لأحكام هذا القانون أو أي قانون آخر.

2- إذا كان تنفيذ الطلب يحتمل أن يمس بأمن الدولة أو سيادتها أو نظامها العام أو مصالحها الأساسية.

3- إذا كانت الجريمة التي يتعلق بها الطلب تمثل موضوع دعوى جنائية منظورة أو فصل فيها بحكم قضائي في الدولة.

4- إذا كانت هناك أسباب جوهرية تدعو للاعتقاد بأن التدبير أو الأمر المطلوب إصداره لا يستهدف الشخص المعني إلا بسبب عنصره أو ديانته أو جنسيته أو عرقه أو آرائه السياسية أو جنسه أو حالته.

5- إذا كانت الجريمة المذكورة في الطلب غير منصوص عليها في قوانين الدولة أو ليست لها جريمة مماثلة منصوص عليها في قوانين الدولة، ومع ذلك إنه يتعين خلافا لذلك تقديم المساعدة إذا كانت لا تنطوي على تدابير جبرية.

6- إذا كان من غير الممكن إصدار أمر باتخاذ التدابير المطلوبة أو تنفيذها بسبب قواعد التقادم المنطبقة على الجرائم المنصوص عليها في هذا القانون بمقتضى قوانين الدولة أو الدولة التي تطلب المساعدة.

7- إذا كان الأمر المطلوب تنفيذه غير قابل للنفاذ بمقتضى القانون.

[1]- المادة 18 من القانون رقم 09-04، المصدر السابق.

8- إذا كان إصدار القرار في الدولة الطالبة قد جرى في ظروف لم تتوفر فيها الضمانات الكافية فيما يتعلق بحقوق المتهم.[1]

وعليه، فإنه يجوز رفض طلب المساعدة قضائية في الحالات التالية:

1- إذا ارتأت الدولة المطلوب إليها أن من شأن تنفيذ الطالب المساس بسيادتها أو أمنها القومي أو نظامها العام أو غير ذلك من مصالحها الأساسية، أو أي سبب ينص عليه قانونها، بما في ذلك نظامها المتعلق بحقوق الإنسان الأساسية، وهذا حسب (الفقرة ب) من المادة 21 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، والفقرة 21 من المادة 46 من اتفاقية مكافحة الفساد.
2- إذا كان الطلب يتعلق بجريمة لا تعتبر الأفعال والأركان المكونة لها جرما إذا كانت قد وقعت في نطاق الاختصاص القضائي للدولة المطلوب إليها.
3- إذا لم يكن في وسع الدولة الطالبة تقديم مساعدة مماثلة للدولة المطلوب إليها.
4- إذا كانت أحكام المساعدة المطلوبة قد تضر بتحقيق أو إجراء في الدولة المطلوب إليها، أو تضر بسلامة أي شخص أو تفرض عبئا ثقيلا على موارد تلك الدولة.
5- إذا لم يقدم الطلب وفقا لأحكام الاتفاقيات الدولية.
6- إذا كانت ثمة أسباب جدية للاعتقاد بأن طلب المساعدة قد قدم لغرض محاكمة شخص على أساس عنصري، جنسية، ديانته، جنسه، أصله العرقي أو أرائه السياسية، أو أن وضع ذلك الشخص قد يتضرر لأي من تلك الأسباب.
7- إذا كان الفعل يعد جريمة وفقا للقانون العسكري، دون أن يكون كذلك وفقا للقانون الجنائي العادي.

8-إذا كان القانون الداخلي للدولة الطرف متلقية الطلب يحضر على سلطاتها تنفيذ الإجراء المطلوب بشأن أي جرم مماثل، لو كان ذلك الجرم خاضعا لتحقيق أو ملاحقة أو إجراءات قضائية في إطار ولايتها القضائية.

[1]- المادة 31 من القانون القطري رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، الجريدة الرسمية العدد 15، تاريخ النشر 02-10-2014 الموافق لـ 1435/12/8.

8- إذا كانت تلبية الطلب تتعارض مع النظام القانوني للدولة الطرف متلقية الطلب فيما يتعلق بالمساعدة القانونية المتبادلة، وهذا حسب اتفاقية مكافحة الفساد.[1]

الفرع الثالث

التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى تسليم المجرمين

من الطبيعي بمكان أن الأحكام الجنائية إذا لم يتم تنفيذها فلا يكون هناك جدوى لأي إجراء أو مواجهة لمرتكبي الجرائم وينهار معه أي سبيل للردع الخاص أو العام، بل وتنهار أي قيمة للإجراءات التي تتخذ حتى الوصول للحكم الصادر في الدعوى الجنائية، ولما كان ذلك كان مرتكب جريمة الكمبيوتر وفي العديد من الأحوال قد يكون في دول أجنبية غير التي وقعت فيها الجريمة ومما يؤدي للإفلات من العقاب في كثير من الأحيان فكان من الأهمية اللجوء لتسليم المجرمين وتفعيل ذلك.[2]

ويقوم مبدأ تسليم المجرمين على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب إحدى الجرائم العابرة للحدود مثل جرائم الإنترنت، عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلا عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة.

والغرض من التسليم هو عدم إفلات المتهم من العقاب في حالة ما إذا كان القانون الداخلي للدولة المتواجد على إقليمها المتهم لا يسمح لتلك الدولة بمحاكمته عن جريمته، وبالتالي فإن تسليم المجرمين هو أحد مظاهر التعاون الدولي في مكافحة الجريمة.

وقد تناولت العديد من الاتفاقيات والمؤتمرات الدولية موضوع تسليم المجرمين، تدعو فيها إلى إبرام معاهدة عالمية لتسليم المجرمين، من بينها المؤتمر الأول للشرطة القضائية في موناكو عام 1924، والمؤتمر الدولي للعقاب في لندن عام 1945، ويرتكن نظام تسليم المجرمين أو المحكوم عليهم إلى

[1]- محمد علي سويلم، المرجع السابق، ص 775، ص 776.

[2]- محمود عبد العزيز أبازيد، المرجع السابق، ص 320.

الاتفاقيات المنعقدة بين الدول في هذا الشأن، والتي قد تكون ثنائية، أي تتم بين دولتين وفقا لما تقرانه من شروط وضوابط، أو تكون متعددة الأطراف أي يتم توقيعها بين عدة دول، أو تكون اتفاقيات التسليم دولية.[1]

والجدير بالذكر أن منظمة الأمم المتحدة وضعت عام 1990 معاهدة نموذجية لتسليم المجرمين لتكون إطارا يساعد الدول التي بصدد التفاوض على اتفاقيات التسليم الثنائية، ولذلك فقد حرصت معظم الدول على سن التشريعات الخاصة بتسليم المجرمين، ومنها المشرع الجزائري الذي أخذ هذا الإجراء كمظهر من مظاهر التعاون الدولي بين السلطات القضائية الأجنبية في قانون الإجراءات الجزائية، و المادة 31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 21-12-2010م،[2] وغيرها.

أولا – شروط تسليم المجرمين:

في الواقع أن تسليم المجرمين لا يتم هكذا دون وجود ضوابط وشروط تحكمه، بل أن هناك عددا من الشروط التي ينبغي توافرها، من بين هذه الشروط.

1-التجريم المزدوج:

ويقصد به أن يكون الفعل المطلوب للتسليم من أجله مجرما في تشريع الدولة طالبة التسليم، وذلك في تشريع الدولة المطلوب إليها التسليم، و شرط التجريم المزدوج يجد أساسه في أن الدولة طالبة التسليم تبتغي من وراء طلبها محاكمة من نسب إليه ارتكاب السلوك الإجرامي أو تنفيذ العقوبة المحكوم بها عليه، وهذا يفترض بداهة أن السلوك مجرم في تشريعها، حيث أنه إذا لم يكن مجرما فلا يتصور وجود دعوى عمومية أو ملاحقة جزائية ضد الشخص المتهم، كما لا يتصور قيام حكم جزائي يقضي

[1]- عادل عبد العال، إبراهيم خراشي، المرجع السابق، ص 42،43.

[2]- أمال فكري، إشكاليات الإثبات والاختصاص في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود، مجلة العلوم القانونية والسياسية، منشورات جامعة الشهيد حمة لخضر الوادي- الجزائر، العدد السابع عشر، الجزء الثاني، جانفي 2018 ص 646- 647.

بعقوبة عليه هذا من ناحية، ومن ناحية أخرى لا يجوز مطالبة الدولة المطلوب إليها التسليم بإيقاع عقوبة على ارتكاب سلوك ما غير مجرم وفقا لقانونها.[1]

لقد أشار المشرع الجزائري إلى هذا الشرط في المادة 697 قانون الإجراءات الجزائية، حين عدد الأفعال التي تجيز التسليم سواء كان الشخص مطلوبا أو مقبولا بعد استيفائه الشروط الواردة في المادة 696 من نفس القانون، ثم اتبعها بشرط ازدواج التجريم، يلاحظ أن المشرع تناول فقط الحالة التي تكون فيها الجزائر مطلوب منها التسليم، وذلك أمر طبيعي لما للتسليم من علاقة بالسيادة مما يلزم كل دولة بتنظيم أحكامها وفقا لما يتناسب مع تشريعها، فقد أجاز المشرع التسليم في جميع الأفعال المعاقب عليها بجناية حسب قانون الدولة الطالبة، أما بالنسبة للأفعال المعاقب عليها بجنحة، فقد خصها بشرط أن يكون الحد الأقصى للعقوبة سنتين أو أقل، أو إذا قضي على المتهم بعقوبة تساوي أو تجاوز الحبس لمدة شهرين كحد أدنى، كل ذلك مع ضرورة أن يكون الفعل معاقبا عليه طبقا للقانون الجزائري، طبعا وفقا للمادة 697 " لا يجوز قبول التسليم في أية حالة إذا كان الفعل غير معاقب عليه طبقا للقانون الجزائري بعقوبة جناية أو جنحة " إعمالا لشرط ازدواج التجريم.[2]

معظم الاتفاقيات التي أبرمتها الجزائر تضمنت بدورها شرط ازدواج التجريم، منها اتفاقية تسليم المجرمين بين حكومة الجمهورية الجزائرية وحكومة الجمهورية الفرنسية المصادق عليه بموجب مرسوم رئاسي رقم 21- 166 المؤرخ في 25 أبريل سنة 2021 فيما يتعلق بالجرائم الواجب التسليم، حسب المادة 2 فترة 1 التي نصت على أنه " لأغراض هذه الاتفاقية، الجرائم التي توجب التسليم هي الجرائم المعاقب عليها بمقتضى قوانين كل من الطرفين بعقوبة سالبة للحرية لا تقل عن سنة أو بعقوبة حبس أشد ".[3]

---

[1]- خالد حازم إبراهيم ، المرجع السابق، ص388.

[2]- فايزة بلال، الشروط الأساسية المتعلقة بالجريمة في نظام تسليم المجرمين، المجلة الجزائرية للقانون والعدالة، مركز البحوث القانونية والقضائية، دار هومه، الجزائر، العدد الأول 2017، ص130.

[3]- المادة 1/2 من المرسوم الرئاسي رقم 21- 166 مؤرخ في 13 رمضان عام 1442 الموافق ل 25 أبريل سنة 2021، يتضمن التصديق على اتفاقية تسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية، وحكومة الجمهورية الفرنسية الموقعة بالجزائر في 27 -01-2019،ج ر ج ج العدد34، ص5.

وعليه، إنه لا بد من توافر بعض الاعتبارات في الجرائم موضوع التسليم، حيث تستمد هذه الاعتبارات من القانون الجزائري وكذلك الاتفاقيات التي أبرمتها الجزائر فيما يتعلق بالتعاون القضائي وتسليم المجرمين، إذ إن اختلاف الدول في شروط تطبيق مبدأ التسليم واختلاف تفسير ذلك، خصوصا فيما يتعلق بتكييف بعض الجرائم أدى إلى عدم الاستجابة لطلب التسليم من قبل الدولة المطلوب منها التسليم،لذلك لا يكفي أن يكون الفعل المنسوب إلى الشخص المطلوب جريمة معاقب عليها في كلتا الدولتين الطالبة والمطلوب منها التسليم، وإنما يجب أن تكون هذه الجريمة على قدر من الأهمية والخطورة الإجرامية، حيث أنه لا يجوز أن تشغل أجهزة الدولة في قضايا تافهة ليس لها من الخطورة ما يبرر الإجراءات العميقة والنفقات التي تتطلبها عملية التسليم عادة.[1]

ولذلك فإن حكما لمحكمة تمييز دبي(الطعن بالتمييز رقم 21 لسنة 2008، تسليم مجرمين في الجلسة العلنية المنعقدة يوم الاثنين الموافق 18-2-2008م ينص على أنه " لما كان ذلك وكانت الجريمة المطلوب تسليم الطاعن من أجلها معاقب عليها بمقتضى قانون الدولة طالبة التسليم بالسجن من سنة إلى سبع سنوات، كما أنه معاقب عليها بمقتضى قانون دولة الإمارات المطلوب إليها التسليم بالحبس حتى ثلاث سنوات مما تكون معه شروط التسليم قد تحققت في الطلب المعروض".

هذا وفيما يتعلق بتسليم المجرمين فقد أكدت العديد من الاتفاقيات والمعاهدات على هذا الشرط من خلال نصوصها المتضمنة، فهناك على سبيل المثال المادة 40 من اتفاقية الرياض العربية للتعاون القضائي، وهناك كذلك المادة 08 من الاتفاقية العربية لمكافحة الإرهاب الصادرة عن مجلسي وزارة الداخلية والعدل العرب والموقعة في مدينة القاهرة بتاريخ 22-4-1998م.[2]

2- الشروط المتعلقة بالأشخاص المطلوب تسليمهم:

من المبادئ المستقر عليها في المجتمع الدولي، أنه لا يجوز تسليم الرعايا، وقد نصت على ذلك معظم التشريعات الوطنية والاتفاقيات الدولية، فإذا ما قام شخص من رعايا الدولة بارتكاب جريمة فلا

[1]- العيند محمد زيد، ليلى عصماني، شروط تسليم المجرمين في النظام القانوني الجزائري، مجلة الاجتهاد القضائي، المجلد 13، العدد01، مارس 2021، ص 629.

[2]- عبد الله سيف الكيتوب، المرجع السابق، ص212،213.

يجوز تسليمه، كذلك لا يجوز تسليم من تم منحهم حق اللجوء السياسي، إذ أن هناك إجماعا دوليا على استبعاد الجرائم السياسية من نطاق التسليم سواء أكان على الاتفاقيات الدولية أم التشريعات الوطنية، فهو إجماع بلغ حد تكريسه كمبدأ.

كذلك فإنه متى كان الشخص المطلوب تسليمه قد سبقت محاكمته عن الجريمة المطلوب تسليمه من أجلها، فبرئ منها أو عوقب عنها، فإنه لا يجوز تسليمه، ليس هذا فحسب، بل أيضا لا يجوز التسليم متى ما كان قيد التحقيق والمحاكمة عن ارتكابه، فعلا ما هو ذاته المطلوب تسليمه من أجله، ويعد هذا الشرط من الضمانات الأساسية عند محاكمة الشخص المطلوب تسليمه، ويهدف إلى توفير أكبر قدر ممكن من الحماية القضائية للشخص المطلوب تسليمه إلى الدولة الطالبة، وذلك حتى لا يتعرض هذا الشخص لعقوبة مزدوجة، وأكدت على هذا الشرط العديد من التشريعات الوطنية والمعاهدات والاتفاقيات الخاصة بتسليم المتهمين، مثل اتفاقية جامعة الدول العربية لتسليم المجرمين رقم 35 لسنة 1956 والتي تنص المادة خمسة منها على أنه " لا يجري التسليم إذا كان الشخص المطلوب تسليمه قد سبقت محاكمته عن الجريمة التي طلب تسليمه من أجلها فبرئ منها أو عوقب أو كان قيد التحقيق أو المحاكمة عن ذات الجريمة المطلوب تسليمه من أجلها في الدولة المطلوب منها التسليم".[1]

وحسب المادة 698 من قانون الإجراءات الجزائية الجزائري لا يقبل التسليم في:

أ- إذا كان الشخص المطلوب تسليمه جزائري الجنسية، والعبرة في تقدير هذه الصفة بوقت وقوع الجريمة المطلوب التسليم من أجلها.

ب- إذا كانت للجناية أو الجنحة صبغة سياسية أو إذا تبين من الظروف أن التسليم مطلوب لغرض سياسي.

ج- إذا ارتكبت الجناية أو الجنحة في الأراضي الجزائرية.

[1] – شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة، مجلة علمية محكمة للعلوم القانونية، المجلد17، العدد1، شوال1441هـ/ يونيو2020م، ص757، 758.

د- إذا تمت متابعة الجناية أو الجنحة والحكم فيها نهائيا في الأراضي الجزائرية ولو كانت قد ارتكبت خارجها.

هـ- إذا كانت الدعوى العمومية قد سقطت بالتقادم قبل تقديم الطلب، أو كانت العقوبة قد انقضت بالتقادم قبل القبض على الشخص المطلوب تسليمه، وعلى العموم كلما انقضت الدعوى العمومية في الدولة الطالبة وذلك طبقا لقوانين الدولة الطالبة أو الدولة المطلوب إليها التسليم.

و- إذا صدر عفو في الدولة الطالبة أو الدولة المطلوب إليها التسليم، ويشترط في الحالة الأخيرة أن تكون الجريمة من عداد تلك التي كان من الجائز أن تكون موضوع متابعة في هذه الدولة إذا ارتكبت خارج إقليمها من شخص أجنبي عنها.[1]

ويظهر مبدأ عدم جواز تسليم المواطنين في جميع الاتفاقيات الثنائية الموقعة من قبل الجزائر،[2]وحتى مع الدول التي تجيز تسليم مواطنيها كالولايات المتحدة الأميركية وبريطانيا، إلا أن نص المادة الثالثة من اتفاقية الجزائر وبريطانيا بخصوص تسليم المجرمين تنص على أنه يمكن لأي طرف أن يسلم مواطنيه للطرف الآخر شريطة أن يسمح تشريعه بذلك، وبكون التشريع الجزائري لا يسمح بذلك، فإنه لا يمكن تسليم المواطنين الجزائريين، إلا أن مبدأ عدم جواز تسليم المواطنين لا يعني إفلات الجاني من العقاب، فرفض الجزائر تسليم مواطنيها لا يحول دون متابعتهم ومحاكمتهم إعمالا لمبدأ "التسليم أو المحاكمة".[3]

3- الشروط المتعلقة بالجريمة المطلوب التسليم لأجلها

هناك ثلاثة أساليب تتخذها العديد من الدول لتحديد طبيعة الجرائم التي يجوز فيها التسليم وذلك على النحو التالي:

[1] – المادة 698 من قانون الإجراءات الجزائية الجزائري، المصدر السابق.

[2]– المادة 03 من اتفاقية تسليم المجرمين بين الجزائر وفرنسا، حسب المرسوم الرئاسي رقم 21 – 166 المؤرخ في 25-4-2021م الذي يتضمن التصديق على هذه الاتفاقية، ج.ر.ج.ج، العدد 34 ص 5.

[3]– العنيد محمد زيد، ليلى عصماني، المرجع السابق، ص 628.

أ-الأسلوب الأول: أسلوب الحصر أو نهج القائمة:

ويعتمد هذا الأسلوب على إدراج مجموعة من الجرائم على سبيل الحصر، على سبيل المثال(القتل، النصب، السرقة، غسيل الأموال،...)، وتدرج هذه الجرائم في قائمة تلحق بالقانون أو الاتفاقية لتكون هذه الجرائم دون غيرها من الجرائم الأخرى هي التي يتم التسليم من أجلها، ويعد هذا الأسلوب من أقل الأساليب شيوعا وانتشارا بين دول العالم، إذ أنه يؤدي إلى إفلات بعض المجرمين من العقاب متى كانت الجريمة المرتكبة من قبلهم غير واردة في القائمة.[1]

ب-الأسلوب الثاني : أسلوب جسامة الجريمة أو الحد الأدنى للعقوبة:

يعتبر هذا الأسلوب الأكثر شيوعا في تحديد الجرائم التي يجوز التسليم فيها، وهو يعني أن تحدد الدول في تشريعاتها الداخلية أو في المعاهدات الثنائية أو متعددة الأطراف الحد الأدنى للعقوبة المقررة للجرائم التي يمكن أن يتم التسليم لأجلها، ويعد التشريع العماني من التشريعات التي اعتنقت هادا الأسلوب، حيث اشترط أن تكون الجريمة المطلوب من أجلها التسليم جناية أو جنحة معاقب عليها بالسجن مدة لا تقل عن سنة وفقا للقوانين العمانية، وفي حالة كون المطلوب تسليمه محكوما عليه فإنه يشترط أن لا تقل العقوبة المحكوم بها عن الحبس لمدة ستة أشهر.[2]

وهذا ما نص عليه قانون الإجراءات الجزائية الجزائري في مادته 697، حيث اشترط أن تكون الجريمة المطلوب من أجلها التسليم هي:

- جميع الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جناية.

- الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جنحة، إذا كان الحد الأقصى للعقوبة المطبقة طبقا لنصوص ذلك القانون سنتين أو أقل أو إذا تعلق الأمر بمتهم قضي عليه بالعقوبة إذا كانت العقوبة التي قضي بها من الجهة القضائية للدولة الطالبة تساوي أو تتجاوز الحبس لمدة شهرين.

[1]- شيخة حسين الزهراني، المرجع السابق، ص 758.

[2]- يوسف حسن يوسف، المرجع السابق، ص 166، 167.

ولا يجوز قبول التسليم في أية حالة إذا كان الفعل غير معاقب عليه طبقا للقانون الجزائري بعقوبة جناية أو جنحة.[1]

وحسب الاتفاقية الثنائية بين الجزائر وفرنسا لتسليم المجرمين، فإنه حسب المادة الثانية فإن الجرائم التي يتوجب التسليم هي الجرائم المعاقب عليها بمقتضى قوانين كل من الطرفين بعقوبة سالبة للحرية لا تقل عن سنة أو بعقوبة حبس أشد، وإذا تم تقديم طلب التسليم بغرض تنفيذ عقوبة سالبة للحرية يجب أن لا تقل المدة المتبقية من العقوبة عن ستة أشهر.[2]

ج- الأسلوب الثالث : النظام المختلط:

يحقق هذا النظام فائدتين، فمن جهة يضمن درجة معينة من جسامة الجريمة المعاقب عليها في البلدين ليتم التسليم وفقا لها، ومن جهة أخرى يضمن خضوع جرائم محددة تمثل خطرا على الدول الأطراف للتسليم دون النظر لدرجة جسامتها أو العقوبة المقررة لها.[3]

ثانيا - إجراءات طلب التسليم:

طالما أن تسليم المجرمين إنما يتم بين الدولة طالبة التسليم، وبين الدولة المطلوب منها تسليم المجرمين، فإن هذا يستتبع بالضرورة أن تكون هناك إجراءات من قبل كلتا الدولتين، إذن فهي القواعد والأسس التي تنتهجها الدول الأطراف فيما يتعلق بعملية التسليم وفقا لقوانينها الوطنية وتعهداتها الدولية، وذلك بهدف إحداث نوع من التوازن بين حرية الأشخاص وحقوقهم من جانب، وبين الحفاظ على أمنها واستقرارها من جانب آخر.[4]

وتتم إجراءات التسليم في جمهورية مصر العربية بتقديم طلب من حكومة الدولة الطالبة إلى الحكومة المصرية عن طريق وزارة الخارجية المصرية بالطرق الدبلوماسية، والتي تحيله بعد فحصه

---

[1]- المادة 697 من قانون الإجراءات الجزائية الجزائري، المصدر السابق.

[2]- المادة الثانية من المرسوم الرئاسي رقم 21- 166 المؤرخ في 25-4-2021م يتضمن التصديق على اتفاقية تسليم المجرمين بين الجزائر وفرنسا.

[3]-خالد حازم إبراهيم، المرجع السابق، ص 379.

[4]- عبد الله سيف المكتوب، المرجع السابق، ص 216.

سياسيا لوزارة العدل للنظر في مدى أحقيته، ويرفق بطلب التسليم بيان بالأفعال المطلوب التسليم من أجلها وزمان ومكان ارتكابها والتكييف القانوني والنصوص الواجبة التطبيق .

وإذا كان الغرض من التسليم تنفيذ عقوبة، يرفق صورة رسمية من الحكم القضائي البات بالإدانة حتى يتم التحقق من شروط التسليم طبقا للاتفاقيات.

ويمكن تقديم طلب التسليم من الدولة الطالبة كتابة للنائب العام الذي يكون له سلطة الفصل في هذا الطلب بالموافقة أو الرفض، وفي حالة طلب مصر تسليم الشخص من دولة أجنبية، فالنائب العام يطلب من وزير العدل توجيه الطلب إلى السلطات المختصة في الدول الأجنبية بالطرق الدبلوماسية.[1]

أما في الجزائر حسب قانون الإجراءات الجزائية الجزائري، نجد أن أغلب الأحكام الخاصة بتسليم المجرمين نظمت في حالة كون الجزائر هي الدولة المطلوب منها التسليم.

حسب الفصل الثاني المعنون في إجراءات التسليم في مواده من 702 إلى 713 تطرق لإجراءات التسليم.

يوجه طلب التسليم إلى الحكومة الجزائرية بالطريق الدبلوماسي ويرفق به إما الحكم الصادر بالعقوبة حتى ولو كان غيابيا وإما أوراق الإجراءات الجزائية التي صدر بها الأمر رسميا بإحالة المتهم إلى جهة القضاء الجزائي، أو التي تؤدي إلى ذلك بقوة القانون وإما أمر القبض أو أية ورقة صادرة من السلطة القضائية ولها ذات القوة على أن تتضمن هذه الأوراق الأخيرة بيانا دقيقا للفعل الذي صدرت من أجله وتاريخ هذا الفعل، ويجب أن تقدم أصول الأوراق المبنية عاليه أو نسخ رسمية فيها، ويجب على الحكومة الطالبة أن تقدم في الوقت ذاته نسخة من النصوص المطبقة على الفعل المكون للجريمة، وأن ترفق بيانا بوقائع الدعوى.[2]

[1]– عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 48، 49.

[2]– المادة 702 من قانون الإجراءات الجزائية الجزائري، المصدر السابق.

يتولى وزير الخارجية تحويل طلب التسليم بعد فحص المستندات ومعه الملف إلى وزير العدل الذي يتحقق من سلامة الطلب ويعطيه خط السير الذي يتطلبه القانون.[1]

يقوم النائب العام باستجواب الأجنبي للتحقق من شخصيته ويبلغه المستند الذي قبض عليه بموجبه وذلك خلال ال24 ساعة التالية للقبض عليه، ويحرر محضر بهذا الإجراءات.[2]

وثم ينقل الأجنبي في أقصر أجل ويحبس في سجن العاصمة،[3] وتحول في الوقت ذاته المستندات المقدمة تأييدا لطلب التسليم إلى النائب العام لدى المحكمة العليا الذي يقوم باستجواب الأجنبي، ويحرر بذلك محضرا خلال 24 ساعة.[4]

ترفع المحاضر وكافة المستندات إلى الغرفة الجنائية بالمحكمة العليا، ويمثل الأجنبي أمامها في ميعاد أقصاه ثمانية أيام تبدأ من تاريخ تبليغ المستندات ،ويجوز أن يمنح مدة ثمانية أيام قبل المرافعات، وذلك بناء على طلب النيابة العامة أو الأجنبي، ثم يجري بعد ذلك استجوابه ويحرر محضر بهذا الاستجواب، وتكون الجلسة علنية ما لم يتقرر خلاف ذلك بناء على طلب النيابة أو الحاضر.[5]

إذا قرر صاحب الشأن عند مثوله أنه يتنازل عن التمسك بالنصوص السابقة وأنه يقبل رسميا تسليمه إلى سلطات الدولة الطالبة فتثبت المحكمة هذا الإقرار، وتحول نسخة من هذا الإقرار بغير تأخير بواسطة النائب العام إلى وزير العدل لاتخاذ ما يلزم بشأنها.[6]

حسب المادة 709 تقوم المحكمة العليا في الحالة العكسية بإبداء رأيها المعلل في طلب التسليم، ويكون هذا الرأي في غير صالح الطلب إذا تراءى للمحكمة وجود خطأ وأن الشروط القانونية غير مستوفاة ويجب إعادة الملف إلى وزير العدل.

---

[1]– المادة 703 من قانون الإجراءات الجزائية الجزائري، المصدر السابق.

[2]– المادة 704من قانون الإجراءات الجزائية الجزائري، المصدر نفسه.

[3]– المادة 705 من قانون الإجراءات الجزائية الجزائري، المصدر نفسه.

[4]– المادة 706 من قانون الإجراءات الجزائية الجزائري، المصدر نفسه.

[5]– المادة 707 من قانون الإجراءات الجزائية الجزائري، المصدر نفسه.

[6]– المادة 708من قانون الإجراءات الجزائية الجزائري، المصدر نفسه.

إذا أصدرت المحكمة العليا رأيا مسببا برفض طلب التسليم، فإن هذا الرأي يكون نهائيا ولا يجوز قبول التسليم.[1]

أما في الحالة العكسية، يعرض وزير العدل لتوقيع إذا كان هناك محل لذلك مرسوما بالإذن بالتسليم، وإذا انقضى ميعاد شهر من تاريخ تبليغ هذا المرسوم إلى حكومة الدولة الطالبة دون أن يقوم ممثلو تلك الدولة باستلام الشخص المقرر تسليمه فيفرج عنه، ولا يجوز المطالبة به بعد ذلك لنفس السبب.[2]

أما في حالة الاستعجال:

يجوز لوكيل الجمهورية لدى المجلس القضائي و بناء على طلب مباشر من السلطات القضائية للدولة الطالبة أن يأمر بالقبض المؤقت على الأجنبي، وذلك إذا أرسل إليه مجرد إخطار سواء بالبريد أو بأي طريق من طرق الإرسال الأكثر سرعة التي يكون لها أثر مكتوب مادي يدل على وجود أحد المستندات المبينة في المادة 702، ويجب أن يرسل إلى وزارة الخارجية في الوقت ذاته إخطار قانوني عن الطلب بالطريق الدبلوماسي أو البريد أو البرق أو بأي طريق من طرق الإرسال التي يكون لها أثر مكتوب، ويجب على النائب العام أن يحيط وزير العدل والنائب العام لدى المحكمة العليا علما بهذا القبض. [3]

وقد تناولت اتفاقية بودابست الإجراءات الواجب إتباعها في حالة تسليم المجرمين من دولة إلى أخرى في المادة 42فقرة 7، حيث نصت على:

7-أ- يقدم كل طرف وقت التوقيع أو عند إيداع وثيقة التصديق أو القبول أو الموافقة أو الانضمام بإخطار السكرتير العام لمجلس أوروبا باسم وعنوان كل سلطة مسئولة عن إصدار أو تلقي طلبات التسليم أو أوامر الضبط التحفظي في حالة عدم وجود اتفاقية.

---

[1]- المادة 710من قانون الإجراءات الجزائية الجزائري، المصدر السابق

[2]- المادة 711من قانون الإجراءات الجزائية الجزائري، المصدر نفسه.

[3]- المادة 712 من قانون الإجراءات الجزائية الجزائري، المصدر نفسه.

ب- يقوم السكرتير العام لمجلس أوروبا بإنشاء وتحديث سجل خاص بالسلطات المسئولة التي يعينها الأطراف، ويلتزم كل طرف بالتأكد من صحة البيانات التي يتم حفظها في هذا السجل طوال الوقت .

والملاحظ أن المادة السابعة قد حددت المسئول عن استلام طلبات التسليم، حيث ألزمت الأطراف في حالة غياب اتفاق إبلاغ السكرتير العام لمجلس أوروبا باسم وعنوان سلطاته المسئولة عن إرسال، أو استقبال طلبات التسليم أو القبض المؤقت، وتطبيق هذه الفقرة محدودة بالحالة التي لا يكون فيها اتفاق مبرم بين الأطراف ذوي الشأن.[1]

المطلب الثاني

إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية

يشكل التعاون العالمي الطريقة الحقيقية الوحيدة لأجل محاربة وجود مضامين مجرمة على الإنترنت، بواسطة نصوص عالمية كالاتفاقية حول جرائم الفضاء السيبراني، إلا أن الإنترنت تمتاز بغياب الحدود، وبلا مادية الاتصالات، هذه الميزة العالمية تجعل تنظيم شبكات معقدا.

طرح الطابع العلمي مشاكل متعددة في أي مجال كان وبصورة أخص في مجال الإنترنت، فالحلول المنصوص عليها في التشريعات الداخلية، لا يمكن أن تكون نافعة إلا إذا أظهرت البلدان إرادة للتعاون، يبدو من الصعوبة بمكان تنظيم الشبكة بواسطة القوانين الداخلية كون الحدود ليست محصورة.

يصطدم التعاون القضائي بالخلاف التشريعي، وبالأصول الصعبة والمعقدة، أنها سيادة الدول الوطنية التي تفرض حقيقة المشكلة، لأن كل بلد يريد أن يحافظ على جزء من الرقابة على شبكة الإنترنت، إلا أن من البديهي أن تحتاج إلى الإنترنت لتنظيم عالمي بعد أخذ خصائصها بعين

[1]- عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 49، 50.

الاعتبار، إذا فرض كل بلد على جاره قانونه الوطني، لا تتحقق المكافحة ضد وجود مضامين غير مشروعة بسرعة.

صعب تحقيق التعاون العالمي إذ يجب تجميع عدة نقاط من أجل إيجاد نقاط مشتركة للتوصل إلى تناغم بين القواعد القانونية على الشبكة، معظم الدول تبحث عن حلول عالمية من أجل تأمين الاعتراف بالأحكام الأجنبية، وإعطائها الصيغة التنفيذية.

لذلك اتجهت نحو القانون الدولي الذي يشكل الوسيلة الوحيدة الموجودة في غياب الحدود، وفي ظل البث السريع للمعلومات حاولوا وضع جزء من السيادة جانبا، وتوضيح مبادئ عامة من أجل مكافحة جرائم التكنولوجيا بصورة فعالة.[1]

ومع ضرورة هذا التعاون والمناداة به، ظهرت صعوبات ومعوقات تقف دون تحققه، وتجعله صعب الحصول وأهمها:

الفرع الأول

الإشكالات المتعلقة بملائمة وتطبيق القوانين

من أهم هذه الإشكالات:

أولا- عدم كفاية وملائمة القوانين القائمة:

إن التطور في المجال التكنولوجي سواء من ناحية الحياة العامة أوالخاصة واعتماد الجميع عليه في سائر شؤونهم، واستغلال الجناة لتلك التقنية في ارتكاب جرائمهم، هذا التطور في الحقيقة لا يقابل وللأسف تطور بذات الدرجة في النصوص القانونية.

[1]- أودين سلوم الحايك، مسؤولية مزودي خدمات الإنترنت التقنية، المؤسسة الحديثة للكتاب، طرابلس، لبنان 2009 ص342،343.

وبالتالي فإن الكثير من نصوص القوانين الجنائية الداخلية لبعض الدول لا يكفي بوضعها الحالي لمواجهة تلك الصور المستحدثة من الجرائم لتطلب غالبية النصوص الصفة المادية في الشيء محل ارتكاب الجريمة، وهو ما يتنافى مع الطبيعة المعلوماتية، وبالتالي تخرج تلك الصور من طائلة التجريم والعقاب.

وعلى الرغم من إصدار العديد من الدول للتشريعات المتعلقة بالجرائم المعلوماتية و انضمامهما للعديد من الاتفاقيات الدولية التي تجرم الأفعال المخالفة للمعاهدات المنظمة لهذه الجرائم، إلا أن هذه النصوص غير كافية لمعالجة سائر الجرائم المرتكبة في مجال الكمبيوتر والإنترنت، الأمر الذي يؤدي لتقليل جهود رجال الشرطة عند ضبط الجرائم والكشف عن مرتكبيها، كما أن الكثير من التشريعات الداخلية للدول وإن كانت تحتوي على قواعد عامة يمكن تطبيقها على الجرائم التقليدية، إلا أنه نظرا لاختلاف أركان وشروط الجرائم المعلوماتية عن أركان وشروط الجرائم التقليدية، فإنه يترتب على ذلك عدم إمكان تطبيق هذه النصوص على هذه الجرائم، مما يصعب مهمة الأجهزة الشرطية والقضائية في ضبط هذه الجرائم وملاحقة مرتكبيها قضائيا.[1]

ثانيا– النظم القانونية الإجرائية المختلفة بين الدول وعدم وجود تنسيق فيما بينها:

عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة المتعلقة بالجريمة المعلوماتية بين الدول المختلفة، خاصة فيما يتعلق بالتحقيق والحصول على الأدلة، لاسيما وأن الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة عن طريق الضبط أو التفتيش في نظام معلوماتي معين أمر في غاية الصعوبة، فضلا عن صعوبة الحصول على الدليل ذاته.[2]

تعتبر قضية الدودة الحاسوبية(لوف باغ) التي أعدت في الفلبين عام 2000، وقيل أنها عطلت ملايين الحواسيب في جميع أنحاء العالم، أحسن مثال على اختلاف النهج القانونية بين الدول، حيث

[1]– عادل عبد العال إبراهيم خراشي، المرجع السابق، ص52،53.

[2]– قطاف سليمان، بوقرين عبد الحليم، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد 05، العدد 02، 2022، ص 83.

أعاقت هذه القضية التحقيقات بسبب أن ذلك العمل المؤدي والضار لم يكن آنذاك مجرما بشكل كاف في الفلبين.[1]

ثالثا– إشكالية القانون الواجب التطبيق في الجريمة المعلوماتية:

تختلف من دولة لأخرى مسألة التكييف القانوني للجريمة المعلوماتية من حيث النشاط الإجرامي والإجرائي ، كما أن خصوصيتها المتميزة بالتعدي من دولة لأخرى يثير العديد من الصعوبات في التصدي لمرتكبيها، الأمر الذي يفرض ضرورة وضع أسس ومبادئ دولية موحدة تفرض على التشريعات الوطنية احترامها والعمل بها من أجل مكافحة هذه الجريمة، لأن التعارض بشأن القانون الواجب التطبيق لا يحقق فكرة التعاون الدولي، مما يؤدي إلى إفلات المجرمين من العقاب.[2]

رابعا– عدم وجود اتفاقيات دولية موحدة بخصوص جرائم المعلوماتية:

لم تجتمع الدول على التوقيع على اتفاقية واحدة لمكافحة جرائم المعلوماتية، والأمر متروك في غالبية الأحوال إلى الاتفاقيات الثنائية التي تبرم بين الدول والتي تتناول جرائم مختلفة ينتمي إليها البعض عن الجرائم المعلوماتية ولا ينتمي إليها البعض الآخر.

ويبرهن ذلك على الحاجة إلى اتفاقيات ثنائية واتفاقية جماعية لمكافحة الجرائم التقليدية التي تقع بطريق الكمبيوتر والإنترنت، وكذلك مكافحة الجرائم الخاصة التي لا تقع إلا بطريق الكمبيوتر والإنترنت.[3]

---

[1]– محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الانترنت و الاستدلال كوسيلة لإثبات الجريمة المرتبكة عبر الانترنت "دراسة مقارنة" ،مركز الدراسات العربية للنشر و التوزيع، الجيزة، جمهورية مصر العربية، الطبعة الأولى، 2019، ص191.

[2]– خليفي محمد، إشكالية الاختصاص القضائي الدولي في مكافحة الجريمة المعلوماتية، مجلة الميزان، العدد الأول، ديسمبر2016، ص 256.

[3]– غنام محمد غنام، المرجع السابق، ص225،224.

الفرع الثاني

الصعوبات المتعلقة بالتعاون الدولي

من بين هذه الصعوبات مايلي:

أولا- إشكالية التجريم المزدوج:

التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، فهو منصوص عليه في أغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين، وبالرغم من أهمية ذلك، نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية، سيما وأن معظم الدول لا تجرم هذه الجرائم، بالإضافة إلى أنه من الصعوبة أن نحدد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الإنترنت أو لا، الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المتعلقة بالإنترنت.[1]

ثانيا- الصعوبات الخاصة بالمساعدات القضائية الدولية:

الأصل بالنسبة لطلبات الإنابة القضائية الدولية والتي تعد من أهم صور المساعدات القضائية الدولية في المجال الجنائي أن تسلم بالطرق الدبلوماسية، وهذا بالطبع يجعلها تتسم بالبطء والتعقيد، والذي يتعارض مع طبيعة الإنترنت وما تتميز به من سرعة، وهو الأمر الذي انعكس على الجرائم المتعلقة بالإنترنت، كذلك من الصعوبات الكبيرة في مجال المساعدات القضائية الدولية المتبادلة التباطؤ في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد

[1]- محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14 / العدد 02 -2016 ، ص61.

الاستجابة وغيرها من الأسباب، فكم هو محبط شطب قضية لعدم تلبية طلب بسيط في الوقت المناسب.[1]

ثالثا- الصعوبات الخاصة بالتعاون الدولي في مجال التدريب:

تتمثل في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل، من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات ومن الصعوبات أيضا، والتي قد تهدد التعاون في مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الأفراد المتدربين، سيما في مجال تكنولوجيا المعلومات وشبكات الاتصال، حيث إنه يوجد بعض الأشخاص ممن لا يعي في هذا المجال شيئا، وعلى النظير يوجد أناس على درجة كبيرة من المعرفة والثقافة في هذا المجال، بالإضافة إلى نظرة المتدرب إلى الدورة التدريبية على أنها مرحلة تدريبية أو عبء لا طائل منه، تهدد العملية التدريبية برمتها وبالطبع نسف التعاون الدولي في هذا المجال أيضا من الصعوبات التي قد تؤثر على العملية التدريبية وعلى التعاون الدولي فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية وعدم قدرتها على تمثيل الواقع العملي لبيئة العمل الطبيعية تمثيلا تاما و متقنا، من حيث ما يدور بها من وقائع وملابسات وإجراءات، وما يتم فيها من نشاطات لا تبلغ حد التطابق من طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية.[2]

[1]- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، مكتبة الوفاء القانونية، الإسكندرية، جمهورية مصر العربية، الطبعة الأولى 2011، ص437،438.

[2]- أمير فرج يوسف، المرجع السابق، ص 438.

الفرع الثالث

إشكالات أخرى

أولا- عدم وجود نموذج موحد للنشاط الإجرامي:

نظرا لعدم وجود مفهوم عام مشترك بين الدول حول نماذج النشاط المتعلق بالجرائم المعلوماتية، ونظرا لاختلاف المفاهيم الخاصة بها لاختلاف التقاليد والأعراف القانونية الدولية، فإن هذا يضعف من منظومة القانون الدولي في مجال ضبط تلك الجرائم، وبالتالي يسهل على الجناة الإفلات من المسائل الجنائية.

يضفي عدم توفر تعريف موحد للجريمة المعلوماتية إلى بقاء أفعالا جريمة دون تجريم، حيث تكون أفعال في تشريع ما معتبرة جرما، وتكون في تشريع آخر مباحة لاختلاف تحديد عناصر الجرم المعلوماتي.

تثير الطبيعة الدولية للجريمة المعلوماتية مشاكل فيما يتعلق تحيدي القانون الواجب التطبيق، هل هو قانون الدولة التي ارتكب فيها الفعل أم قانون الدولة التي ظهرت فيها الآثار الضارة، إضافة إلى تعارض القوانين من ناحية موضوعية وإجرائية، الأمر الذي يستلزم ضرورة العمل على توحيد التشريعات فيما يتعلق بمكافحة الجرائم المعلوماتية، إضافة إلى إبرام اتفاقيات في هذا المجال.[1]

ثانيا- عدم وجود قنوات الاتصال:

لتحقيق هذا الهدف، كان لازما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم

[1]- محمد ممدوح بدير، المرجع السابق، ص189،199.

القدرة على جمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي لجرائم معنية و لمجرمين معينين، وبالتالي تنعدم الفائدة من هذا التعاون.[1]

ثالثا- إشكالية الاختصاص في الجرائم المتعلقة بالإنترنت:

كونها تعد من المشكلات التي تعرقل الحصول على الدليل فيها خاصة وأنها من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي والدولي، بسبب التداخل والترابط بين شبكات المعلومات، لأن الجريمة قد تقع في مكان معين وتنتج آثارها في المكان آخر.[2]

هذه الجرائم تعد من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي أو الدولي، ولا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلي، حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك، ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي حيث اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول، بالنسبة للجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة الحدود، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبادئ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى، فتتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية، كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الاطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة.[3]

يلاحظ أن اختصاص القضاء بنظر الجرائم التي تتم عبر شبكة الإنترنت والقانون الواجب تطبيقه على الفعل، لا يحضى بالوضوح أو القبول أمام حقيقة أن غالبية هذه الأفعال من قبل أشخاص من خارج حدود الدولة أو أنه تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود حتى عندما

[1]- محمد أحمد سليمان عيسى، المرجع السابق، ص 70.

[2]- قطاف سليمان، بوقرين عبد الحليم، المرجع السابق، ص83.

[3]- يوسف حسن يوسف، المرجع السابق، ص188،187.

يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، وهو ما يبرز أهمية اختبار مدى ملائمة قواعد الاختصاص والقانون الواجب التطبيق، وما إذا كانت النظريات والقواعد القائمة في هذا الحقل تطال هذه الجرائم أم يتعين إفراد قواعد خاصة بها في ضوء خصوصيته، وما تثيره من مشكلات في حق الاختصاص القضائي، ويرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات امتداد أنشطة الملاحقة والتحري، والضبط والتفتيش خارج الحدود.

أدى هذا البعد عبر الوطني للجريمة المرتكبة عبر الإنترنت إلى تشتت الجهود وإعاقة التعاون الدولي في مجال التصدي لهذا النوع من الإجرام، وذلك لاختلاف الإجراءات الجنائية أو النزاع حول القانون الواجب التطبيق.[1]

المبحث الثاني

الطريق نحو اتفاقية عالمية لمكافحة الجريمة السيبرانية برعاية الأمم المتحدة بحدود2023 في ظل تجاذبات القوى الكبرى

في طريقنا إلى اتفاقية عالمية لمكافحة الجريمة السيبرانية في غضون سنة 2023 حاولنا وباختصار شديد المرور عبر بعض المحطات للأمم المتحدة من قرارات للأمين العام والجمعية العامة التي نعتبرها كبوادر أولية لميلاد هذه الاتفاقية، لكن ومن خلال دراستنا المبدئية لهذه المحطات لاحظنا أن ميلاد هذه الاتفاقية سيكون بشكل عسير في أحسن أحوالها لأنه في ظل المستجدات الدولية الراهنة من تجاذبات للقوى الكبرى، خاصة في ظل الحرب الروسية الأوكرانية، **وفي** ظل الصراع الروسي الصيني من جهة والأمريكي من جهة أخرى حول مشروع هذه الاتفاقية بترحيب روسي صيني لها و

[1]– محمد ممدوح بدير، المرجع السابق، ص 192، 193.

بتململ أمريكي لهذا المشروع وتشجيعه للاتفاقيات الثنائية واتفاقية المجلس الأوروبي لمكافحة الجريمة السيبرانية.

المطلب الأول

قرارات الجمعية العامة والأمين العام للأمم المتحدة في الدورة الثالثة والسبعون والرابعة والسبعون في مجال مكافحة الجريمة المعلوماتية

سوف نحاول تحت هذا المطلب الرجوع لقرارات الجمعية العامة والأمين العام للأمم المتحدة المتعلقة بمجال الجريمة المعلوماتية في الدورتين الثالثة والسبعون والرابعة والسبعون.

الفرع الأول

قرار الجمعية العامة للأمم المتحدة في الدورة الثالثة والسبعون في مجال مكافحة الجريمة المعلوماتية

ارتأيت في هذا الفرع قبل التطرق لقرار الجمعية العامة للأمم المتحدة 187/73 أن أعرج على محطة من أهم المحطات التي شهدها العالم وكان لها تأثير كبير على الأزمة الاقتصادية والأمنية التي شهدها ويشهدها العالم إلى يومنا هذا ألا وهي باختصار أزمة كوفيد-19 وما للتهديدات السيبرانيية المرتبطة بهذا الوباء.

أولا- الجريمة المعلوماتية وكوفيد19:

لم يكن أحد في العالم يعلم بأن شهر نوفمبر لسنة 2019 يعتبر كبداية لأزمة عالمية انعكست تداعياتها إلى يومنا هذا، وربما إلى أمد غير قريب في المستقبل، حيث أنه يعتبر يوم 17 نوفمبر 2019 بداية لطريق طويل لما هو معروف الآن باسم وباء COVID-19، لم يكن من الممكن توقع

وصول الأمر لأزمة عالمية تتحدى كافة الطبقات الاجتماعية وجميع القطاعات الصناعية والتجارية والسكنية بالعالم، وقد نتج عن هذا الوباء الحديث تحديات جديدة أصبحت من غير الممكن توقع نتائجها، وعليه كلما ظهرت أزمة جديدة يكون المجرمون أول من ينتهزون الفرصة لاستغلال الضحايا حسني النية في أوقات الخوف، وعدم اليقين والشك، حيث يتخذ ذلك الاستغلال أشكالاً متعددة من النطاق المادي إلى الرقمي، وقد أثبت التاريخ أن الطريقة الأكثر فاعلية لمواجهة تلك التهديدات هي الوقاية ورفع الوعي على جميع المستويات الشخصية والعملية.

كوفيد 19 وباء أسفر عن تحدي كبير نادراً ما أثير من قبل، فهو وباء عالمي ويؤثر على الجميع بغض النظر عن الموقع الجغرافي، العِرق، الدين، الأصل الاجتماعي، الجنس، الإعاقة، الدخل أو أي وضع آخر، وفي هذا السياق يسعى المجرمون للاستفادة من تلك المخاوف والتهديدات والهلع الذي أصاب الناس. [1]

ولعل أهم التهديدات الالكترونية التي كانت تستهدف أي مستخدم لتكنولوجيا الانترنت في ظل الأزمة الصحية :الحملات الخبيثة وذلك مثل رسائل البريد الالكترونية المخادعة كنشر فيروسات باستخدام صور من تقرير حول الوباء أو من خلال نصائح صحية من مصادر حكومية رسمية، وكذلك مثل انتحال هوية موقع رسمي[2]، نشر البرامج الخبيثة[3]، حملات وهمية، التضليل.

1– www.unodc.org

01 ماي 2020، مكتب الأمم المتحدة المعني بالمخدرات والجريمة –كوفيد–19، تحليل التهديدات الالكترونية . COVID19_MENA_Cyber_Reportt_AR2(2).PDF

2– لقد أعلن المركز الوطني للأمن الالكتروني (NCSC) بالمملكة المتحدة تمكن مجرمو شبكات الانترنت من انتحال صفة موقع المركز الأمريكي لمكافحة الأمراض (CDC) بخلق نطاق الكتروني بأسماء مماثلة للعنوان الإلكتروني لمركز ولقرصنة كلمات المرور بالإضافة إلى قيامهم بطلب تبرعات "بيتكوين" لتمويل لقاح مزور.

3– العديد من تلك العناوين الالكترونية تخلق صفحات يتم تحميلها عن طريق برامج خبيثة تم تصميمها لاستغلال نقاط الضعف بأنظمة تشغيل معينة .

يمكن لتلك البرامج الخبيثة سرقة بيانات من أي نوع، بيانات بطاقات الائتمان، بيانات بنكية، بيانات حساسة للمتصفح واستخدامها لأغراض إجرامية.

علما أنه نظرا لاعتماد الكثير من الأشخاص على مواقع التواصل الاجتماعي للحصول على معلومات وللتواصل مع أصدقائهم وعائلاتهم، للعمل، والتسوق عبر الإنترنت والمزيد، فقد تضاعف استخدام تلك المواقع كنتيجة لأزمة وباء كوفيد-19 حيث أظهرت الإحصائيات تلك الزيادة، مما يساعد على فهم تأثير الحملات الخبيثة المشار إليها على الوضع، ذلك يتيح لمجرمي الانترنت الوصول لعدد كبير من الضحايا المحتملين من خلال محاولاتهم المستمرة في التحايل على الأشخاص والكيانات في مثل هذه الظروف.

إن البيانات المذكورة بالإحصائيات المشار إليها أدناه جمعت عن طريق استطلاع رأي لأكثر من 25000 مستخدم في 30 سوق خلال الفترة من 14إلى 24 مارس 2020.

يعتبر تطبيق واتساب (WhatsApp) من بين التطبيقات التي شهدت زيادة في نسبة الاستخدام قدرها 40% في بداية الأزمة زادت نسبة الاستخدام بمقدار 27%، ووصلت تلك الزيادة إلى 41% في منتصف المرحلة من الوباء، ووصلت نسبة استخدام تطبيق واتساب في الدول التي تعاني من مراحل متقدمة من الوباء إلى 51%، أما في إسبانيا مثلا فتعدت ذلك ووصلت لدرجة أكبر من ذلك إلى76% أو أكثر، ولا تعد تلك الزيادة في نسبة الاستخدام على ذلك التطبيق فقط، فقد أثبتت دراسة أن تطبيقات أخرى مثل "فيسبوك" (Facebook)، "إنستاجرام" (Instagram)، "وي شات" (WeChat) و"ويبو" (Weibo) قد شهدت زيادة في استخدامهم بنسبة 40% في مثل هذه التطبيقات.[1]

1- الانتربول :

إن مجرمو الانترنت الواسعوا الحيلة والانتهازيون استغلوا وباء كوفيد- 19 لشن مختلف أنواع الاعتداءات السيبرانية، حيث أنه منذ تفشي الوباء عادت إلى الظهور برمجيات خبيثة معروفة كانت مختفية نسبيا، و اتخذت أشكالا جديدة، واستفادت من هذه الجائحة لتعزيز أساليبها القائمة على الهندسة الاجتماعية، والتطور المستمر في هذا المجال في مثل هذه الظروف .

[1] – www.unodc.org

01 ماي2020 ، مكتب الأمم المتحدة المعني بالمخدرات والجريمة – كوفيد -19، تحليل التهديدات الالكترونية.

أ- أبرز التهديدات في ظل وباء كورونا:

النطاقات الخبيثة، عمليات الاحتيال الالكترونية ومواقع التصيد الاحتيالي، البرمجيات الخبيثة لجمع البيانــات، البرمجيات التخريبية الخبيثة(برمجيــات انتزاع الفدية وهجمات تعطيل الخدمة ddos).[1]

ب- العمل عن بعد في ظل الوباء:

إن مجرمو الانترنت يستغلون أبرز مواطن الضعف في المنظومات المعلوماتية والتطبيقات التي تستخدمها الشركات والحكومات والمدارس لتمكين موظفيها من العمل عن بعد، حيث أنه تزايد عدد الأفراد الذين يعتمدون في عملهم على الوسائل المعلوماتية، الأمر الذي يلقي بثقله على التدابير الأمنية المتخذة تجاه تفشي الوباء، حيث أن المجرمون يبحثون عن المزيد من الفرص لسرقة المعلومات أو تحقيق الأرباح أو تعطيل المنظومات الالكترونية، وغير ذلك .

ج- الإنتربول وأهم الإجراءات التي قام بها:

إن الانتربول قام بإعداد برنامج عالمي لمكافحة جريمة الانترنت، وقاد الإجراءات العالمية التي تتخذها أجهزة تنفيذ القانون لمكافحة التهديدات السيبرية التي تستغل تفشي وباء كوفيد19، وعمم نشرات بنفسجية من أجل تنبيه البلدان الأعضاء إلى التهديدات السيبرانية الجديدة والشديدة الخطورة، وأعطى إرشادات تقنية للمنظمات التي تقع ضحية هذه الاعتداءات لمساعدتها في جهود التعافي التي تبذلها، وأجرى استقصاء عالمي في مجال الجريمة السيبرية لإدراك الوضع العالمي السريع التغيّر على نحو أفضل، وتعاون أيضا مع مجموعات خبراء في مجال الأمن السيبراني عبر الإنترنت وعقد اجتماعات افتراضية في حالات الطوارئ مع جهات معنية شتى، منها رؤساء الوحدات الوطنية والإقليمية لمكافحة الجريمة السيبرية وفريق خبراء الانتربول العالمي لمكافحة جريمة الانترنت والشركاء من القطاع الخاص

[1] – يبث مرتكبو الجرائم السيبرية برمجيات تخريبية خبيثة مثل برمجة انتزاع الفدية لتعطيل بنى تحتية ومؤسسات حيوية مثل المستشفيات والمراكز الطبية التي تجاوزت الأزمة الصحية طاقاتها أصلا، والاعتداءات التي تشنها هذه البرمجيات لا تستهدف سرقة المعلومات عادة ، بل منع هذه البنى التحتية من الوصول إلى البيانات الحساسة أو تعطيل منظوماتها الكمبيوترية، ما يؤدي إلى تفاقم وضع مأسوي أساسا في العالم الواقعي.

من أجل تزويد البلدان الأعضاء بخدمات متكيفة مع احتياجاتها لمنع الجريمة السيبرانية وكشفها والتحقيق فيها وغير ذلك.[1]

2- اليوروبول "الوكالة الشرطية الأوروبية" :

اعتبرت "يوروبول" أن جائحة كورونا كان لها دور كبير في زيادة الجرائم المعلوماتية في العالم الأوروبي، كالجرائم الجنسية المتعلقة بالأطفال، وجرائم الاحتيال عبر عالم الإنترنت، وكان لليوروبول في بيان لها بأن "المجرمين عمدوا على استغلال الوباء لتصيد ضحاياهم، حيث كان الحجر كوسط خصب دفع المستخدمين للجوء إلى الإنترنت على مستوى لم يسبق له مثيل من قبل".

واعتبرت الوكالة في تقريره السنوي حول الجرائم، أن **عمليات الاحتيال عبر الإنترنت**" أصبحت إستراتيجية مثالية للمجرمين المعلوماتيين الساعين إلى بيع منتجات يدعون أنها تقي من فيروس كورونا الجديد أو تشفي منه"، وأوضحت الوكالة بأن " التصيد" بواسطة الرسائل الإلكترونية يشكل "تهديدا فاعلا" إذ بات المجرمون يستخدمون أساليب أكثر تطورا في هذا المجال عما كان عليه من قبل.

كما أن المواد التي تنطوي على استغلال جنسي للأطفال عبر الإنترنت كان في تزايد كبير إبان الأزمة الصحية أي أزمة الوباء، وأشارت إلى أن نشر مواد من هذا النوع أصبح أكثر قبول في الأوساط الشعبية في ظل الأزمة عليه من قبل، وذلك بسبب القيود المفروضة خاصة القيد على السفر وقيود أخرى .

وتم نقل البيان عن المفوضية الأوروبية للشؤون الداخلية "**إيلفايو هانسن**" قولها إن " الجائحة أدت إلى تباطؤ جوانب عدة في الحياة المعتادة للناس، لكنها يا للأسف زادت وتيرة النشاط الإجرامي عبر الإنترنت"، وأضافت أن مجموعات " الجريمة المنظمة تستغل الأشخاص الأكثر عرضة كالعاطلين من

[1]-www.interpol.int

التهديدات السيبرية المرتبطة بكوفيد – 19 في العالم الدخول يوم 2022/08/05 على الساعة 11:44
20COM0312-CyberCampain_ProjectSheet-AR-2020-05.pdf

العمل الجدد، أو الشركات المفلسة أو الأسوأ من كل ذلك الأطفال" وشددت على ضرورة أن يكثف الاتحاد الأوروبي جهوده "بصورة ملحة " لمكافحة الجريمة المعلوماتية.[1]

3- مكتب الأمم المتحدة المعني بالمخدرات و الجريمة وتحليله للتهديدات الالكترونية على مستوى منطقة الشرق الأوسط وشمال إفريقيا :

إن منطقة الشرق الأوسط وشمال إفريقيا لم يكن لها مهرب من الهجمات الالكترونية، وكان لها رصيد هي الأخرى حيث استغل مجرمو شبكات الانترنت انشغال السلطات بتداعيات هذا الوباء من أجل القيام بهجماتهم ومن أهم ما أستهدف في هذه المنطقة بواسطة هذه الهجمات الالكترونية:

أ- **البنى التحتية الحكومية والمصرفية:** إن البنية التحتية المصرفية والحكومية كان لها نصيب الأسد من الهجمات الالكترونية، وكان ذلك ناجما عن تلك الخدمات المقيدة وذلك لفرض حظر التجوال في العديد من تلك المناطق، وكان لتلك الهجمات ضحايا كثر خاصة ضحايا المصارف.

ب- **مواقع التواصل الاجتماعي:** إن الحجر الصحي ساهم بشكل أو بأخر في انتشار الجريمة الالكترونية حيث حتم على الأشخاص البقاء في منازلهم، الأمر الذي أدى بهؤلاء البحث عن متنفس، الشئ الذي أدى بالأفراد التوجه إلى مواقع التواصل الاجتماعي، الأمر الذي أدى بمجرمي شبكات الانترنت تحويل انتباههم لعدة تطبيقات مستخدمة على نطاق واسع بالمنطقة لشن هجمات مختلفة، مثلا يوم 15 ابريل 2020 شهد تطبيق " **تيك توك** " (Tiktok)، والذي ارتفعت نسبة استخدامه بالمنطقة بصورة استثنائية العديد من نقاط الضعف التي استغلها مجرمو شبكات الانترنت، حيث تم إضافة مقاطع فيديو غير معتمدة وغير مصرح بها لحسابات الضحايا دون علمهم، والجدير بالذكر أن العديد من المنظمات الإقليمية تستخدم ذلك التطبيق مما قد يترتب عليه انتشار معلومات خاطئة حول كوفيد- 19 وما ينجم عنه من نتائج وخيمة .

[1] -arabic.euronews.com

"يوروبول" ، جائحة كورونا ساهمت في زيادة الجرائم الالكترونية في أنحاء أروبا ، بقلم يورونيوز 2020/10/06.

ج- عقد الاجتماعات والمؤتمرات عبر الانترنت: نظرا لحظر التجوال المفروض في معظم دول المنطقة، وإتباع معايير السلامة وخاصة معايير التباعد الاجتماعي، الأمر الذي حتم استخدام بعض التطبيقات الشائعة لعقد الاجتماعات والمؤتمرات وغير ذلك، حيث استغل مجرمي الانترنت نقاط ضعف تلك التطبيقات لشن هجماتهم مما سمح لهم بالتحكم بالجلسات وكذا اعتراض الصوت والصورة ، وعرض مضمون غير مرغوب فيه أثناء انعقاد المؤتمر أو الدورة التدريبية من جهة، وكذا عرض أسرار تلك الاجتماعات من جهة أخرى، وغير ذلك من الاختراقات.[1]

ثانيا- قرار الجمعية العامة للأمم المتحدة 73/ 187 المعنون بـــ "مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية "

في الدورة الثالثة والسبعون وتحت البند 109 من جدول أعمال الجمعية العامة للأمم المتحدة، اتخذت قرارا في 17 كانون الأول / ديسمبر 2018 وهو قراره 73/ 187 المعنون بمكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية.

إن الجمعية العامة للأمم المتحدة اتضح لها أن التكنولوجية الحديثة هي سلاح دو حدين، من جهة تساهم في تنمية الدول ، إلا أنه من جهة أخرى تعتبر كسلاح في يد المجرمين الأمر الذي يؤدي إلى ارتفاع مستويات الجريمة، لكنه وفي المقابل لاحظت الجمعية العامة أن لهذه التكنولوجية الجديدة إمكانات هائلة، بما في ذلك الذكاء الاصطناعي لمنع ومكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية ، كما لاحظت كذلك ارتفاع معدلات الجرائم المرتكبة في العالم الرقمي، وازدياد تنوعها وتأثيرها على استقرار البنى التحتية الحيوية للدول والمؤسسات والأفراد، واعتبرت أن مختلف المجرمين بمن فيهم المتاجرون بالأشخاص، يستفيدون من تكنولوجيات المعلومات والاتصالات للقيام بأنشطة إجرامية خطيرة.

إن الجمعية العامة للأمم المتحدة شددت اللهجة على ضرورة تعزيز التنسيق والتعاون بين الدول في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، بما فيها تقديم المساعدة

---

[1] – www.unodc.org

مكتب الأمم المتحدة المعني بالمخدرات والجريمة –كوفيد – 19 : تحليل التهديدات الالكترونية، 01 ماي 2020.

التقنية للبلدان النامية، بناء على طلبها من أجل تحسين التشريعات الوطنية وبناء قدرات السلطات الوطنية بغية التصدي لذلك الاستخدام بكل أشكاله، بما يشمل منعه والكشف عنه والتحقيق فيه وملاحقة مرتكبيه قضائيا، كما أكدت على أنه في استخدام تكنولوجيات المعلومات والاتصال أخذ العناية اللازمة في احترام حقوق الإنسان والحريات الأساسية لما لها من الأهمية بما كان .

وفي الأخير جاءت الجمعية العامة للأمم المتحدة بقرار مهم وهو طلب إلى الأمين العام أن يلتمس من الدول الأعضاء رأيهم بشأن العقبات والتحديات التي تعترضها في مجال مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وأن يقدم تقريرا استنادا إلى تلك الآراء إلى الجمعية العامة لكي تنظر فيه في دورتها الرابعة والسبعين .[1]

الفرع الثاني

قرارات الأمين العام والجمعية العامة للأمم المتحدة في الدورة الرابعة والسبعون في مجال مكافحة الجريمة المعلوماتية

سوف نتطرق تحت هذا الفرع لقرارات الأمين العام والجمعية العامة للأمم المتحدة في مجال مكافحة الجريمة المعلوماتية في الدورة الرابعة والسبعون.

أولا – تقرير الأمين العام للأمم المتحدة في الدورة 74 عملا بقرار الجمعية 73/ 187 المعنون "مكافحة استخدام تكنولوجيا المعلومات والاتصال للأغراض الإجرامية "

في الدورة الرابعة والسبعون، وتحت البند 109 من جدول الأعمال المؤقت "مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية"، أعد الأمين العام تقريرا في 30 جويلية 2019 عملا بقرار الجمعية العامة 73/ 187 المعنون "مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية"، ويحتوي هذا التقرير على معلومات عن آراء الدول الأعضاء المقدمة عملا بالقرار 187/73.

---

[1]–www.un.org/ar/ga/73/resolutions.shtml

قرار الجمعية العامة للأمم المتحدة، رقم القرار A/RES/73/187

حيث أنه تطبيقا لهذا الطلب تم دعوة الدول الأعضاء في المذكرتين الشفويتين CU2019/90/DTA/OCB/CSS و CU2019/55/DTA/OCB/CMLS والمؤرختين في13 فبراير 2019 و19مارس2019 على التوالي، والصادرتين عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة، إلى تقديم معلومات عن التحديات التي تعترضها في مجال مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وأبلغت الأمانة الدول الأعضاء بأن هذه المعلومات سوف تستخدم لإعداد تقرير عن تنفيذ القرار 187/73 لتقديمه إلى الجمعية العامة للنظر فيه في دورتها الرابعة والسبعين.

كانت هناك استجابة من عدة دول بناءا على ذلك الطلب مبرزة أرائها، ومن بين هذه الدول، روسيا، الصين، الولايات المتحدة الأمريكية، العربية السعودية، الأردن، ألمانيا، وغير ذلك من الدول.[1]

حيث أن هذه الدول عرضت تجاربها وخبراتها في هذا المجال مقدمة معلومات عن التحديات المرتبطة بالمجال التقني و المعلوماتي، كما أبرزت أهمية التعـــاون الدولي في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية وهذا لما لها من أهمية بين الدول.[2]

ومن بين هذه الدول، اقترحنا آراء كل من الصين، وروسيا، والمملكة العربية السعودية، والولايات المتحدة الأمريكية.

1- جمهورية الصين الشعبية

من بين المقترحات التي جاءت بها الصين في هذا الإطار أنها رأت خاصة فيما يتعلق بالتشريعات الدولية، أن اتفاقية الجريمة المنظمة لا يمكن أن تستجيب بفعالية للمتطلبات الجديدة للتعاون الدولي للتصدي لجريمة الانترنت، وتوجد بعض الاتفاقيات الإقليمية في هذا المجال، مثل ما جاءت به منظمة شنغهاي للتعاون، وكذا مجلس أوروبا، وجامعة الدول العربية، غير أن التشريعات الدولية لمكافحة جريمة الانترنت مجزأة بسبب الاختلافات بين دول الأعضاء، فالصين رأت أن

[1]–www.unodc.org/doucuments/cybercrime/S G report /V1908180_APDF.A/74/130

[2] – www.unodc.org/doucuments/cybercrime/S G report /V1908180_APDF. A/74/130

المجتمع الدولي بحاجة ملحة إلى وضع إطار قانوني عالمي لمكافحة الجريمة السيبرانية، وإلى العمل سويا لمواجهة وضع الجريمة الذي تتزايد خطورته بمرور الوقت، ولاسيما مواجهة التحديات الجديدة الناشئة عن التكنولوجيات الجديدة، مثل الحوسبة السحابية[1] ، وتؤيد الصين الرأي القائل بأن تتفاوض جميع الدول بشأن **اتفاقية عالمية لمكافحة الجريمة السيبرانية**، مفتوحة العضوية أمام جميع البلدان، وأن تقر تلك الاتفاقية، وذلك تحت رعاية الأمم المتحدة مستفيدة من التجارب السابقة.[2]

كما رأت الصين أن الاتفاقية العالمية ينبغي أن تنسق بفعالية بين القوانين والممارسات الوطنية الخاصة بمكافحة الجريمة السيبرانية، وأن تتصدى في الوقت المناسب للمشكلات الجديدة الناشئة مع التطور التكنولوجي، وأن توفر حلولا مقبولة عالميا للحوكمة العالمية للجريمة السيبرانية، وفيما يتعلق بنطاق التطبيق، وبالإضافة إلى الجرائم المرتكبة ضد النظم الحاسوبية، ينبغي أن تنطبق الاتفاقية أيضا على الجرائم المرتكبة أساسا من خلال استخدام الإنترنت وتكنولوجيا المعلومات، فضلا عن الأنشطة التي تساعد على ارتكاب هذه الجرائم والتدبير لارتكابها، وعلى صعيد إنفاذ القانون والتحقيق ينبغي أن تنص الاتفاقية على تدابير محددة الأهداف لإنفاذ القانون والتحقيق، وأن تضع ترتيبات لمسائل الشراكة بين القطاعين العام والخاص، مع توضيح التزامات مقدمي خدمات الشبكات ومشغليها المتعلقة بالتعاون على منع الجريمة السيبرانية والمساعدة على إنفاذ القانون والتحقيق، ومن حيث التعاون الدولي، ينبغي أن تنظم الاتفاقية الممارسة المتمثلة في الحصول على الأدلة الإلكترونية عبر الحدود، وأن تصمم آلية أكثر كفاءة لجمع الأدلة، استنادا إلى احترام سيادة الدول وحماية حقوق الشركات والأفراد، وأن تضع أحكاما للجهاز القضائي تتسق مع خصائص الجريمة السيبرانية، وبالإضافة إلى ذلك، ينبغي أن تنص الاتفاقية على أحكام بشأن بناء القدرات والمساعدة التقنية وآليات منع الجريمة.[3]

---

[1]–عن موقع : aws.mazon.com/ar/what-is-cloud-computing

الحوسبة السحابية تعني توفير موارد تقنية المعلومات حسب الطلب عبر الإنترنت مع تسعير التكلفة حسب الاستخدام، فبدلا من شراء مراكز البيانات والخوادم المادية وامتلاكها والاحتفاظ بها، يمكنك الوصول والاستفادة من الخدمات التكنولوجية، مثل إمكانات الحوسبة ،والتخزين، وقواعد البيانات، بأسلوب يعتمد على احتياجات، وذلك من خلال جهة موفرة للخدمات السحابية مثل Servies (AWS) Amazon Web

[2] –www.unodc.org/doucuments/cybercrime/S G report /V1908180_APDF

[3] – www.unodc.org/doucuments/cybercrime/S G report /V1908180_APDF

الصين كذلك لمحت فيما يخص التعاون الدولي، على أنه قبل استحداث اتفاقية عالمية ينبغي تشجيع الدول على الاضطلاع بالتعاون العملي على مكافحة جريمة الانترنت على أساس الاحترام المتبادل والمساواة والمنفعة المتبادلة، وفقا لاتفاقية الجريمة المنظمة و الاتفاقيات الإقليمية والمعاهدات الثنائية، كما نبهت الصين على أن بعض الدول مشيرة هنا خاصة للولايات المتحدة الأمريكية ضمنيا، أنها أقرت تشريعات وطنية لتجاوز قنوات المساعدة القضائية وقنوات التعاون في مجال إنفاذ القانون، وقامت من جانب واحد بالحصول على بيانات إلكترونية موجودة في الخارج، وهو ما أثار بدوره سلبا على المبادئ الأساسية للقانون الدولي، مثل السيادة وحماية حقوق الأفراد والشركات بين الدول.[1]

أما على الصعيد الوطني، رأت الصين من خلال تجربتها في هذا المجال أنه ينبغي للدول أن تتخذ على المستوى المحلي إجراءات في هذا المجال للتصدي لهذا النوع من الجرائم منها:

أ- العمل على تقوية جهات تنفيذ القانون والجهات القضائية للتحقيق في جرائم الانترنت، وذلك لمواكبة التحديات الناشئة عن التكنولوجيات الجديدة و المتطورة.

ب- إعطاء العناية لمجال الأدلة الالكترونية من خلال تبيان القواعد الخاصة للحصول على الأدلة الإلكترونية وقبولها، وكذا مراعاة طبيعة هذا النوع من الأدلة من جهة أخرى، ومن جهة ثالثة العمل على بناء قدرات أجهزة البحث عن الأدلة الإلكترونية قانونيا وتقنيا.[2]

2- روسيا:

روسيا أشارت إلى أن الجريمة المعلوماتية أصبحت رقما صعبا من حيث تداعياتها وذلك منذ فترة طويلة من حيث أنها تشكل تهديدا عالميا يؤثر على جميع بلدان المعمورة، وذلك لعدم وجود نهج موحد تجاه هذه المسألة، وكذا في ظل غياب إطار قانوني دولي شامل للتعاون، كما أن الاتفاقيات الإقليمية لم تثبت نجاعتها تجاه هذه الظاهرة ، كما اعتبرت روسيا أن اتفاقية مجلس أوروبا المتعلقة بالجريمة المعلوماتية أنها صك غير كاف لمواجهة التهديدات الراهنة، كما أن روسيا شجعت على وضع مبادئ وقواعد عالمية تتشارك فيها جميع الأطراف المهتمة ،وتضع الأسس للتعاون الدولي الفعال على

[1] –www.unodc.org/doucuments/cybercrime/S G report /V1908180_APDF A/74/130

[2] – www.unodc.org/doucuments/cybercrime/S G report /V1908180_APDF

مكافحة الجريمة المعلوماتية، ويمكن أن يكون هذا الصك هو اتفاقية لمكافحة الجرائم المتعلقة باستخدام تكنولوجيات المعلومات والاتصالات، تبرم تحت رعاية الأمم المتحدة وتراعي الواقع الراهن ومبدأ المساواة في السيادة ومبدأ عدم التدخل في الشؤون الداخلية للدول، وفي هذا السياق يعتبر البحث عن حل سياسي وبناء من خلال التوافق في الآراء هو المهمة الأساسية لمواجهة هذه الظاهرة .[1]

3- المملكة العربية السعودية:

العربية السعودية أشارت إلى عدة أسباب كانت ضمن العقبات أمام مكافحة الجريمة المعلوملتية منها:

أ- إشكالية التعاون بين الشركات الخاصة بالمنصات الرقمية مع الجهات القانونية وجهات تنفيذ القانون في جميع أنحاء المعمورة.

ب - انتحال هوية أشخاص آخرين على الإنترنت، وغياب الهوية الرقمية في العالم الافتراضي.

ج- يوجد تباين في تشريعات الدول الأعضاء من جهة، ومن جهة أخرى نقص التعاون بين الدول لمجابهة هذه الظاهرة.

د- يوجد افتقار في بلدان كثيرة إلى نظم المعلومات المتطورة التي تتيح رصد العمليات المشبوهة وتحديد مصادرها ومن يقف ورائها هذا من جهة، ومن جهة أخرى ضعف مجال الأمن المعلوماتي تقنيا وبشريا الأمر الذي يتطلب تأهيل القائمين عليه.

هـ- استبدال العملات التقليدية بعملات رقمية يسهل على الجماعات الإجرامية إخفاء الكثير من معاملاتها المالية على الإنترنت.

و- عدم وجود الوعي الكافي لاستخدام هذه التكنولوجيا، الأمر الذي ساهم في تطور هذا النوع من الجرائم، وعليه لابد من زيادة الوعي في هذا المجال.[2]

[1] -www.unodc.org/doucuments/cybercrime/S G report /V1908180_APDF

[2]- www.unodc.org/doucuments/cybercrime/S G report /V1908180_APDF

4- الولايات المتحدة الأمريكية :

إن الو م أ صرحت بأنها تواجه أربعة تحديات رئيسية، وعليه سوف نذكر بعض من هذه التحديات :[1]

أ- الضغط الذي يمارس من أجل الحد من مساهمات الخبراء في السياسات الدولية، أما الضغط الذي يمارسه بعض الحكومات لإطلاق نقاشات سياسية بشأن معاهدات عالمية جديدة، على الرغم من عدم وجود تأييد بتوافق الآراء لإتباع هذا النهج، فهو يستهلك الموارد القيمة ويضعف مقدرة الخبراء على إسداء مشورة مجدية بشأن كيفية التغلب على التحديات الأساسية التي تواجهها الدول الأعضاء عند التحقيق في قضايا الجريمة المعلوماتية وملاحقة مرتكبيها قضائيا، والمداخلات التي يسهم بها الخبراء ضرورية لفهم مسائل معقدة مثل حماية حرية التعبير،القيود المناسبة على سلطة الدولة،التنفيذ الفعال للأطر والآليات القائمة،توفير التدريب والمساعدة التقنية للبلدان النامية في الوقت الضروري.

ب- تطور الجريمة المعلوماتية من جهة، و اتساع نطاق تهديدات الجماعات الإجرامية العابرة للحدود المحلية، من خلال ما تسببه هذا النوع من الجرائم باعتمادها على تكنولوجيات المعلومات والاتصالات، ولعل أبرزها الشبكة الخفية[2]، التي تعتبر من بين الشبكات الأكثر خطورة.

ج- المؤهلات الجد محدودة للأطر الوطنية سواء من الجانب البشري أو التقني، التكوين القانوني، وكذا من جانب القدرات في مجال التحقيق ، وهذا التحدي جعل الولايات المتحدة الأمريكية في مواجهة الجريمة المعلوماتية مكبلة اليدين في العمل مع الشركاء .

د- الصعوبات التي تواجه الولايات المتحدة الأمريكية في الحصول على الأدلة الإلكترونية في التحقيقات من الولايات القضائية الأجنبية في مجال إنفاذ القانون من أجل مكافحة الجريمة المعلوماتية،

---

[1] - www.unodc.org/doucuments/cybercrime/S G report /V1908180_APDF

[2] – عن موقع: www.safespace.qa/topic/ شبكة الانترنت الخفية.

شبكة الانترنت الخفية، يشير هذا المصطلح إلى المعلومات ومواقع الانترنت غير المفهرسة في محركات البحث العادية، أو المحمية بكلمة مرور ،ما يعني أنه لا يمكن الوصول إليها عبر البحث في محركات البحث العادية، وبالتالي تسمى هذه المعلومات بالخفية، تعتبر المنشورات والصفحات على الفيسبوك مثلا، والتفاصيل المصرفية والحسابات على (أمازون) أو صندوق البريد الخاص بنا، معلومات خفية، بسبب عدم قدرة عموم الناس على الوصول إليها بالبحث البسيط، إضافة إلى ذلك هناك معلومات أو مواقع إنترنت أخرى غير مسجلة أو متوفرة عل محركات البحث، أو ظلت متاحة لمؤسسيها فقط، وتعد جزءا من محتوى شبكة الانترنت الخفية أيضا.

وفي المقابل كذلك في تنفيذ طلبات الولايات القضائية للدول الأخرى للحصول على الأدلة الالكترونية من الولايات المتحدة الأمريكية يعتبر هذا تحد داخلي لها لقصور طلبات الحصول على تلك المساعدة التي تحتاج مزيد من المعلومات والتوضيحات من الشركاء الدوليين، وبالتالي الولايات المتحدة الأمريكية أوصت هنا بمزيد من بناء القدرات في هذا المجال.

وفي الأخير فمن أجل الحصول على الأدلة الإلكترونية، تستخدم الدول الأعضاء المعاهدات الثنائية للمساعدة القانونية المتبادلة، وكذلك الاتفاقيات المتعددة الأطراف، مثل اتفاقية مجلس أوروبا المتعلقة بالجريمة المعلوماتية واتفاقية الجريمة المنظمة، كأساس قانوني للتعاون، ويشارك أيضا أكثر من 80 بلدا بنشاط في شبكة نقاط الاتصال "7/24" المعنية بجرائم التكنولوجيا العالية، التابعة لمجموعة البلدان السبعة، من أجل تسهيل تلبية طلبات الحفاظ على البيانات وغيرها من الطلبات، وتوصي الولايات المتحدة بأن تنظر الدول الأعضاء في الانضمام إلى هذه المعاهدات والشبكات واستخدامها في مكافحة الجريمة المعلوماتية.[1]

ثانيا – قرار الجمعية العامة في 12ديسمبر 2019 حول تطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

في الدورة الرابعة والسبعون وفي الجلسة العامة 46 وتحت البند 93 من جدول الأعمال " **التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي**" قرار اتخذته الجمعية العامة في 12ديسمبر2019 حول التطورات في ميدان المعلومات والاتصالات السلكية و اللاسلكية في سياق الأمن الدولي .

إذ أن الجمعية العامة:[2]

[1]–www.unodc.org/doucuments/cybercrime/S G report /V1908180_APDF.

[2] – Documents–dds–ny.un.org/doc/undoc/gen/n19/410/05/pdf/n1941005.pdf

تؤكد ما يترقبه المجتمع الدولي من استخدام تكنولوجيا المعلومات والاتصالات في الأغراض السلمية في سبيل تحقيق الصالح العام للبشرية والنهوض بالتنمية المستدامة في جميع البلدان بصرف النظر عن تطورها التكنولوجي.

وتؤكد على أنه من فوائد الدول تشجيع استخدام تكنولوجيا المعلومات والاتصالات في الأغراض السلمية وليس لأغراض عسكرية، وهناك قلق لإمكانية استخدام هذا النوع من التكنولوجية في الصراعات المستقبلية بين الدول.[1]

وإذ تؤكد أن من الضروري منع استخدام موارد أو تكنولوجيا المعلومات لأغراض إجرامية أو إرهابية، وضرورة احترام حقوق الإنسان والحريات الأساسية عند استخدام تكنولوجيا المعلومات والاتصالات، أما بناء القدرات فاعتبرته أمر لا بد منه لتعاون الدول وبناء الثقة في مجال أمن تكنولوجيا المعلومات والاتصالات، كما اعتبرت أن بعض الدول قد تحتاج إلى المساعدة في جهودها الرامية إلى سد الفجوة في مجال أمن تكنولوجيا المعلومات والاتصالات واستخدامها، وتلح على أن تدابير بناء القدرات ينبغي أن تتوخى تشجيع استخدام تكنولوجيا المعلومات والاتصالات في الأغراض السلمية فقط .

واعتبرت أن الأمم المتحدة لعبت دورا طلائعي في تشجيع الحوار بين الدول الأعضاء من أجل التوصل إلى تفاهمات مشتركة بشأن أمن تكنولوجيا المعلومات والاتصالات واستخدامها، وكذلك في بلورة تفاهمات مشتركة بشأن التنظيم القانوني الدولي لأنشطة الدول في ميدان تكنولوجيا المعلومات والاتصالات ومعايير وقواعد ومبادئ السلوك المسئول للدول في هذا الميدان، وبضرورة أن تشجع الأمم المتحدة الجهود الإقليمية وتعزز تدابير بناء الثقة والشفافية، وتدعم بناء القدرات ونشر أفضل الممارسات الفعالة.

وأكدت على أنه وتحت رعاية الأمم المتحدة ضرورة استمرارية عملية التفاوض بشأن الأمن في استخدام تكنولوجيا المعلومات والاتصالات،[2] كما ترحب ببدء عملية التفاوض في شكل فريق الأمم

[1] – وهذا ما هو حاصل في الوقت الراهن في النزاع الروسي الأوكراني .

[2] – Documents-dds-ny.un.org/doc/undoc/gen/n19/410/05/pdf/n1941005.pdf

المتحدة العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وترحب أيضا بفريق الخبراء الحكوميين المعني في نفس الاختصاص.[1]

ثالثا- قرار الجمعية العامة في 12ديسمبر 2019 حول الارتقاء بسلوك الدول المسئول في الفضاء الإلكتروني في سياق الأمن الدولي.

في الدورة الرابعة والسبعون وفي الجلسة العامة 46 وتحت البند 93 من جدول الأعمال "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي".

قرار اتخذته الجمعية العامة في 12 ديسمبر 2019 في ضرورة الارتقاء بسلوك الدول المسئول في الفضاء الإلكتروني في سياق الأمن الدولي.

إذ الجمعية العامة:

ترى و تلاحظ أن هناك تقدما كبيرا قد أحرز في تطوير وتطبيق أحدث ما وصلت إليه تكنولوجيا المعلومات ووسائل الاتصال السلكية واللاسلكية في الوقت الراهن، وأن هذه التكنولوجيا سلاح دو حدين.

كما اعتبرت أن من فائدة ومصلحة جميع الدول تعزيز استخدام تكنولوجيا المعلومات والاتصالات في الأغراض السلمية ومنع نشوب النزاعات نتيجة استخدامها، وإذ تعرب عن القلق لاحتمال استخدام هذه التكنولوجيا والوسائل في أغراض لا تتفق مع أهداف صون الاستقرار والأمن الدوليين، ويمكن أن تؤثر تأثيرا سلبيا في سلامة الهياكل الأساسية للدول، مما يضر بأمنها في الميدانين المدني و العسكري على السواء، وإذ تؤكد ضرورة تعزيز التنسيق والتعاون بين الدول في مجال مجابهة إساءة استخدام هذه التكنولوجيا.[2]

---

[1] – www.un.org/ar/ga/74/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n19/410/05/pdf/n1941005.pdfA/RES/74/29

[2]–www.un.org/ar/ga/74/resolution.shtml

Document-dds-ny.un.org/doc/undoc/gen/n19/409/98/pdf/n1940998.pdfA/RES/74/28

1- تهيب بالدول الأعضاء إلى القيام بما يلي:

أ- أن تسترشد في استخدامها لتكنولوجيا المعلومات والاتصالات بتقارير الأعوام 2010و2013 و2015 الصادرة عن فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

ب- أن تدعم تنفيذ التدابير التعاونية، على النحو المحدد في تقارير فريق الخبراء الحكوميين للتصدي للأخطار الناشئة في هذا الميدان وضمان تهيئة بيئة لتكنولوجيا المعلومات والاتصالات منفتحة وقابلة للتشغيل البيني و موثوقة ومأمونة، بما يتفق وضرورة صون التدفق الحر للمعلومات.

2- تدعو جميع الدول الأعضاء إلى أن تواصل، آخذة في اعتبارها التقييمات والتوصيات الواردة في تقارير فريق الخبراء الحكوميين، موافاة الأمين العام بآرائها وتقييماتها بشأن المسألتين التاليتين:

أ- الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان.

ب- مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين.

3- ترحب ببدء أعمال الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.[1]

رابعا - قرار الجمعية العامة في 18 ديسمبر 2019 بتعزيز المساعدة التقنية وبناء القدرات لتدعيم التدابير الوطنية والتعاون الدولي في مجال مكافحة الجريمة السيبرانية، بما يشمل تبادل المعلومات:

في الدورة الرابعة والسبعون وفي الجلسة العامة 50، وتحت البند 106 من جدول الأعمال "منع الجريمة والعدالة الجنائية " قرار اتخذه الجمعية العامة في 18ديسمبر 2019 بتعزيز المساعدة التقنية وبناء القدرات لتدعيم التدابير الوطنية والتعاون الدولي في مجال مكافحة الجريمة السيبرانية، بما يشتمل تبادل المعلومات.

[1] - www.un.org/ar/ga/74/resolution.shtml

Document-dds-ny.un.org/doc/undoc/gen/n19/409/98/pdf/n1940998.pdfA/RES/74/28

إذ الجمعية العامة :

اعتبرت أنه يمكن للدول الأطراف أن تستخدم اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لتوفير التعاون الدولي من أجل منع ومكافحة الجريمة المنظمة عبر الوطنية ، وكذلك أن تستخدمها في بعض قضايا الجريمة المعلوماتية، وإذا تدرك التحديات التي تواجهها جميع الدول في مكافحة الجريمة المعلوماتية، وإذ تشدد على ضرورة تعزيز المساعدة التقنية وأنشطة بناء القدرات، بناء على الطلب، واستنادا إلى الاحتياجات الوطنية مع مراعاة التحديات الخاصة التي تواجهها البلدان النامية في هذا المجال.

أ- الجمعية العامة ترحب بنتائج الاجتماع الخامس لفريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة المعلوماتية، المعقود في فيينا في الفترة من 27الى29 مارس 2019، وتعتبر أن فريق الخبراء سيضع وفقا لخطة عمله للفترة 2018-2021، استنتاجات وتوصيات يمكن تقديمها إلى لجنة منع الجريمة والعدالة الجنائية.

ب- تسلم بأن فريق الخبراء هو منبر مهم لتبادل المعلومات عن التشريعات الوطنية، والممارسات الفضلى والمساعدة التقنية والتعاون الدولي بغية دراسة الخيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجريمة المعلوماتية واقتراح تدابير جديدة في هذا الشأن،[1]و تشجع الدول الأعضاء على وضع وتنفيذ تدابير تكفل فعالية التحقيق والملاحقة القضائية على الصعيد الوطني في الجرائم المعلوماتية والجرائم التي تكون فيها الأدلة الإلكترونية مهمة، وتضمن إمكانية الحصول على تعاون دولي فعال في هذا المجال، تماشيا مع القانون الوطني وبما يتوافق مع أحكام القانون الدولي المنطبقة ذات الصلة، بما في ذلك الصكوك الدولية لحقوق الإنسان الواجب التطبيق، كما تحث الدول الأعضاء على تشجيع تدريب موظفي أجهزة إنفاذ القانون وسلطات التحقيق والنيابة العامة والقضاة على التعامل مع الجريمة المعلوماتية، بما يشمل التدريب على المهارات المناسبة في جمع الأدلة وتكنولوجيا المعلومات، وتجهيزهم ليضطلعوا بأدوارهم بفعالية في التحقيق في الجرائم المعلوماتية وملاحقة مرتكبيها وتقديمهم إلى العدالة، و تشجيع الدول

[1] – www.un.org/ar/ga/74/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n19/429/90/pdf/n1942990.pdfARES/74/173

الأعضاء على السعي إلى توفير المساعدة التقنية المناسبة وبناء القدرات المستدامة عند الطلب، واستنادا إلى الاحتياجات الوطنية، ابتغاء تعزيز قدرة السلطات الوطنية على التصدي للجريمة المعلوماتية، ومواصلة تبادل الآراء بشأن الخبرات العملية والجوانب التقنية الأخرى في هذا الصدد.

ج- تطلب إلى مكتب الأمم المتحدة و المعني بالمخدرات والجريمة أن يواصل جمع المعلومات دوريا عن التطورات الجديدة والتقدم المحرز والممارسات الفضلى المستبانة، وأن يواصل إبلاغ هذه المعلومات إلى فريق الخبراء وإلى لجنة منع الجريمة والعدالة الجنائية، وتدعو فريق الخبراء إلى أن يقوم، استنادا إلى ما ينهض به من أعمال ودون المساس بالمسائل الأخرى المندرجة في إطار ولايته، بتزويد مكتب الأمم المتحدة المعني بالمخدرات والجريمة بالمشورة اللازمة، بما يشمل الجوانب المتعلقة بالبرنامج العالمي المعني بالجريمة المعلوماتية، من أجل المساعدة في استبانة الاحتياجات ذات الأولوية القصوى في مجال بناء القدرات وتدابير التصدي الفعالة، وذلك دون المساس بوضع اللجنة بصفتها الهيئة الإدارية لبرنامج الجريمة التابعة للمكتب.

د- تطلب إلى مكتب الأمم المتحدة المعني بالمخدرات والجريمة أن يواصل تزويد الدول الأعضاء، بناء على طلبها، ووفقا لاحتياجاتها الوطنية، بمساعدات تقنية وبرامج لبناء القدرات المستدامة على التصدي للجريمة المعلوماتية، من خلال البرنامج العالمي المعني بالجريمة المعلوماتية وعن طريق مكاتبه الإقليمية وغيرها، ابتغاء منع الجرائم السريانية بكل أشكالها والكشف عنها، والتحقيق فيما وملاحقة مرتكبيها، مع التسليم بأن التعاون مع الدول الأعضاء والمنظمات الدولية والإقليمية ذات الصلة والقطاع الخاص والمجتمع المدني والجهات المعنية الأخرى من شأنه أن يسير هذا النشاط، كما تدعو الدول الأعضاء إلى النظر في مواصلة التعاون، حسب الاقتضاء وبطريقة شفافة وخاضعة للمساءلة، مع القطاع الخاص والمجتمع المدني، في وضع التدابير الرامية إلى مكافحة الجريمة المعلوماتية.[1]

[1] – www.un.org/ar/ga/74/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n19/429/90/pdf/n1942990.pdfARES/74/173

خامسا – قرار اتخذته الجمعية العامة في 18ديسمبر 2019 حول مكافحة الاستغلال الجنسي للأطفال وانتهاكهم جنسيا على الإنترنت.

في الدورة الرابعة والسبعون وفي الجلسة العامة 50 وتحت البند 106 من جدول الأعمال "من الجريمة والعدالة الجنائية" قرار اتخذته الجمعية في 18ديسمبر2019م بمكافحة الاستغلال الجنسي للأطفال وانتهاكهم جنسيا على الإنترنت.

إذ الجمعية العامة :

تعطي أهمية و تسلم بضرورة المبادرات والشركات سواء دولية وإقليمية وثنائية تدعيما للجهود المبذولة لحماية الأطفال من الاستغلال الجنسي عبر عالم الإنترنت، وذلك من خلال دراسات تهدف لإنشاء أرضية استدلالية دقيقة بشأن استعمال الأطفال للإنترنت، وإذ الجمعية العامة كذلك تنوه في هذا الصدد ماتبدله منظمات مثل التحالف العالمي للحماية (WeProtect) و المنظمة العالمية لحماية الطفل على الإنترنت من جهود.

إذ كذلك الجمعية العامة:

1- تحث الدول الأعضاء على تجريم الاستغلال الجنسي للأطفال وانتهاكهم جنسيا، بما في ذلك الاستغلال الجنسي للأطفال وانتهاكهم جنسيا على الإنترنت، وتحتهم كذلك على بذل مزيد من الجهود في مجابهة هذا النوع من الجرائم المرتكبة عبر الانترنت .

2- تهيب بالدول الأعضاء التي هي أطراف في البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية أن تنفذ التزاماتها القانونية.[1]

3- على الدول الأعضاء نشر الوعي الكافي لخطر للمواد المتعلقة بالاستغلال الجنسي للأطفال وانتهاكهم جنسيا، وبأن هذه المواد تشكل جرائم جنسية ضد الأطفال، وكيف أن إنتاجها وتوزيعها

[1] –www.un.org/ar/ga/74/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n19/431/25/pdf/n1943125.pdfA/RES/74/174

واستخداماتها، يعرض المزيد من الأطفال لخطر الاستغلال والانتهاك الجنسيين، خاصة التصرفات المصورة في هذه المواد وتأجيج الطلب عليها، وذلك لما لها من خطر.

4- كذلك تحث أيضا دول الأعضاء على اتخاذ ما يتوافق مع قوانينها الوطنية من تشريعات أو التدابير أخرى تيسر على مقدمي خدمات الإنترنت وخدمات الوصول إليها وسائر الكيانات المعنية الكشف عن المواد المتعلقة بالاستغلال الجنسي للأطفال وانتهاكهم جنسيا، وأن تكفل بالتماشي مع القوانين الوطنية، قيام مقدمي خدمات الإنترنت وخدمات الوصول إليها وسائر الكيانات المعنية بإبلاغ السلطات المعنية عن تلك المواد وإزالتها، بما يشمل القيام بذلك التعاون مع أجهزة إنفاذ القانون، وتشجع أيضا الدول الأعضاء على تبادل المعلومات بشأن أفضل الممارسات على نحو استباقي واتخاذ الإجراءات اللازمة لمكافحة الاستغلال الجنسي للأطفال وانتهاكهم جنسيا، بما في ذلك مصادرة أو حذف المواد المتعلقة بالانتهاك الجنسي للأطفال من الانترنت وتقليل المساحة الزمنية التي يستغرقها القيام بذلك، بما يتسق مع القوانين الداخلية للدول، وكذلك توفير الموارد اللازمة للتحري والمتابعة القضائية.

5- تشجع كذلك الدول الأعضاء على إشراك المؤسسات الحكومية المسئولة عن الاتصالات وسياسات حماية البيانات وممثلي صناعة تكنولوجيا المعلومات والاتصالات في تعزيز التنسيق الوطني لمكافحة الاستغلال الجنسي للأطفال وانتهاكهم جنسيا، وكذا الإبلاغ عن المعاملات المالية المشبوهة وتعقبها، ونشر ثقافة الإبلاغ عن مثل هذه الجرائم في أوساط العوام .

6- كذلك تشجع أيضا الدول الأعضاء الحفاظ على توازن مناسب بين وضع وتنفيذ سياسات حماية الخصوصية والجهود الرامية إلى استبانة المواد التي تنطوي على اعتداء جنسي على الأطفال وجرائم الاستغلال الجنسي للأطفال وانتهاكهم جنسيا على الانترنت والإبلاغ عنها ، ومن جهة أخرى وتوفير الدعم اللازم لهم من خلال تيسير وصولهم إلى برامج مناسبة وخدمات للرعاية والمشورة جيدة النوعية وقائمة على الأدلة من أجل مساعدتهم على التعافي بدنيا ونفسيا واجتماعيا، إلى جانب توفير الرعاية النفسية والمشورة اللازمة للتعافي من الصدمات وإعادة التأهيل والإدماج في المجتمع مع كفالة وصون

حقوق الأطفال المتضررين، وحماية خصوصية الضحايا وسرية المعلومات التي أبلغوا عنها، وذلك بمساعدة الجهات المعنية .[1]

7- تعزيز سياسة التعاون الدولي على مكافحة الاستغلال الجنسي للأطفال وانتهاكهم جنسيا على الانترنت مع إعطاء عناية لخصوصية الأطفال في هذا الإطار.

المطلب الثاني

قرارات الجمعية العامة للأمم المتحدة في الدورة الخامسة والسبعون والسادسة والسبعون في مجال مكافحة الجريمة المعلوماتية

سوف نتطرق تحت هذا المطلب لقرارات الجمعية العامة للأمم المتحدة حول مجال مكافحة الجريمة السيبيرانية في دورتي الأمم المتحدة الخامسة والسبعون والسادسة والسبعون .

الفرع الأول

قرارات الجمعية العامة للأمم المتحدة في الدورة الخامسة والسبعون في مجال مكافحة الجريمة المعلوماتية

وفي هذا المجال نتطرق لعدة قرارات أهمها :

أولا- قرار اتخذته الجمعية العامة في 23 نوفمبر 2020 حول التعاون بين الأمم المتحدة والمنظمة الدولية للشرطة الجنائية "الإنتربول".

في الدورة الخامسة والسبعون وفي الجلسة العامة 30 وتحت البند 130 (ذ) من جدول الأعمال "التعاون بين الأمم المتحدة والمنظمات الإقليمية والمنظمات الأخرى، التعاون بين الأمم المتحدة والمنظمة الدولية للشرطة الجنائية الانتربول".

[1]-www.un.org/ar/ga/74/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n19/431/25/pdf/n1943125.pdf

A/RES/74/174

قرار اتخذته الجمعية العامة في 23أكتوبر 2020م حول التعاون بين الأمم المتحدة والانتربول.

إذ الجمعية العامة:

تدعو إلى تعزيز التعاون بين الأمم المتحدة والمنظمة الدولية للشرطة الجنائية "الانتربول"، ضمن إطار ولاية كل منها على ما يلي:[1]

1- منع ومكافحة الجريمة العابرة للحدود الوطنية، ولاسيما الجريمة المنظمة عبر الوطنية، بما يشمل إساءة استخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية، بما في ذلك الانترنت و وسائل التواصل الاجتماعي.

2- القضاء على الإرهاب ومكافحته بوسائل منها مكافحة استخدام تكنولوجيات المعلومات والاتصالات في الأغراض الإجرامية، بما في ذلك الإنترنت و وسائل التواصل الاجتماعي لخدمة أغراض إرهابية، مع احترام حقوق الإنسان والحريات الأساسية، ومكافحته تمويل الإرهاب، بما في ذلك التمويل بواسطة استخدام التكنولوجيات والأساليب الناشئة التي يعرفها العالم.

وكذلك تقوم بالتشجيع على مواصلة التعاون مكتب الأمم المتحدة المعني بالمخدرات والجريمة، والانتربول لمواجهة التحديات التي تتعرض لها الدول الأعضاء في مكافحة الجريمة المعلوماتية، عن طريق المساعدة التقنية وأنشطة بناء القدرات التي تتيحها الانتربول وكيانات الأمم المتحدة المعنية، بناء على طلبها واستنادا إلى الاحتياجات الوطنية، مع مراعاة التحديات المحددة التي تواجهها البلدان النامية ، وذلك باعتبارها من البلدات الأكثر تضررا.

[1] - www.un.org/ar/ga/75/resolutions.shtml
Documents-dds-ny.un.org/doc/undoc/gen/n20/330/14/pdf/n2033014.pdf
A/RES/75/10

ثانيا – قرار اتخذته الجمعية العامة في 16ديسمبر2020 حول الحق في الخصوصية في العصر الرقمي.

في الدورة الخامسة والسبعون وفي الجلسة العامة 46 تحت البند 72(ب) من جدول الأعمال " تعزيز حقوق الإنسان وحمايتها : مسائل حقوق الإنسان، بما في ذلك النهج البديلة لتحسين التمتع الفعلي بحقوق الإنسان والحريات الأساسية"، قرار اتخذته الجمعية العامة في 16ديسمبر2020 حول الحق في الخصوصية في العصر الرقمي.

إذ الجمعية العامة:

1- تدعو جميع الدول:

أ – احترام وحماية الحق في الخصوصية، وخاصة في ظل الاتصالات الرقمية، وباتخاذ التدابير اللازمة للحد من انتهاك هذا الحق.

ب- إعادة النظر بانتظام في إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة الاتصالات واعتراضها وبجميع البيانات الشخصية، بما في ذلك مراقبة الاتصالات واعتراضها وجميع البيانات على نطاق واسع، وكذلك فيما يتعلق باستخدام تكنولوجيات التنميط واتخاذ القرارات آليا والتعلم الآلي والتكنولوجيات البيومترية، وذلك بهدف صون الحق في الخصوصية عن طريق ضمان التنفيذ الكامل والفعلي لجميع الالتزامات الملقاة على عاتقها بموجب القانون الدولي لحقوق الإنسان، وأن تضع لذلك آليات محلية للرقابة البرلمانية والإدارية و القضائية.

ج- التشاور مع جميع أصحاب المصلحة المعنيين، بما في ذلك مع المؤسسات التجارية والمنظمات الدولية والمجتمع المدني، بسن وتنفيذ التشريعات الملائمة تتضمن جزاءات فعالة وسبل انتصاف مناسبة، وتحمي الأفراد من الانتهاكات والتجاوزات الماسة بالحق في الخصوصية، ولاسيما ما كان من هذه الانتهاكات والتجاوزات عن طريق جمع البيانات الشخصية أو تجهيزها أو الاحتفاظ بها

أو تداولها أو استخدامها، بطرق تعسفية وغير قانونية، من قبل الأفراد والحكومات والمؤسسات التجارية ومنظمات القطاع الخاص، أو أنها تنظر في مواصلة إعمال القائم من تلك القوانين.[1]

د- النظر في سن وتنفيذ تشريعات ولوائح تنظيمية وسياسات لضمان احترام جميع المؤسسات التجارية، بما في ذلك مؤسسات وسائل التواصل الاجتماعي وغيرها من المنصات الإلكترونية، احتراما كاملا للحق في الخصوصية وغيرها من حقوق الإنسان ذات الصلة في تصميم التكنولوجيات وتطويرها ونشرها وتقييمها، بما في ذلك الذكاء الاصطناعي، أو أن تنظر في مواصلة إعمال القائم من تلك التشريعات واللوائح التنظيمية والسياسات، وأن تتيح للأفراد الذين قد تكون حقوقهم قد تعرضت للانتهاك أو التجاوز إمكانية الوصول إلى سبل انتصاف فعالة، بما في ذلك الحصول على التعويضات وضمانات بعدم تكرار ما وقع، وأن تنظر في إعادة وتنفيذ تشريعات ولوائح تنظيمية وسياسات لحماية البيانات، وأن تنظر في وضع ومراجعة وتنفيذ وتعزيز سياسات مراعية للاعتبارات الجنسانية تعزز وتحمي حق جميع الأفراد في الخصوصية في عصر الرقمنة.

هـ- إعطاء عناية للتعليم الجيد لتمكين الجميع من حماية خصوصياتهم بفعالية، وذلك باكتساب المعارف الرقمية والمهارات التقنية اللازمة للقيام بذلك.

و- اتخاذ الخطوات اللازمة لتمكين المؤسسات التجارية من اعتماد تدابير طوعية كافية لتحقيق الشفافية فيما يتعلق بالطلبات التي تصدر عن سلطات الدولة للحصول على بيانات المستخدمين والمعلومات الخاصة بهم.

ز - اتخاذ التدابير المناسبة لضمان تصميم برامج الهوية الرقمية أو البيومترية وتنفيذها وتشغيلها في إطار الضمانات القانونية والتقنية المناسبة وبالامتثال التام للالتزامات الواقعة على الدول بموجب القانون الدولي لحقوق الإنسان.

[1] - www.un.org/ar/ga/75/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n20/371/73/pdf/n2037173.pdfA/RES/75/176

2- تدعو جميع المؤسسات التجارية التي تقوم بجمع البيانات وتخزينها واستخدامها وتداولها وتجهيزها بـ :[1]

أ- الوفاء بالتزامها عن احترام حقوق الإنسان، بما في ذلك الحق في الخصوصية في العصر الرقمي، وكذا إبلاغ المستخدمين بطريقة واضحة بكل ما يمكن أن يمس بحقهم في الخصوصية من جراء جمع بياناتهم واستخدامها وتداولها و الاحتفاظ بها، وأن تضع سياسات لتحقيق الشفافية تتيح للمستخدمين أن يعبروا بحرية وعن بينة عن موافقتهم المعقولة ، حسب الاقتضاء.

ب - التكفل بإدماج احترام الحق في الخصوصية وغيره من حقوق الإنسان الدولية في تصميم تكنولوجيات اتخاذ القرارات آليا والتعلم الآلي وتشغيلها وتقييمها، وأن تنص على دفع تعويضات عن انتهاكات حقوق الإنسان التي تكون قد تسببت أو أسهمت فيها.

ج - أن تكفل للأفراد إمكانية الوصول إلى بياناتهم الشخصية واعتماد التدابير المناسبة التي تتيح إمكانية تعديل الموافقة المتعلقة بالبيانات وتصحيحها وتحديثها وحذفها وسحبها، لاسيما إن كانت البيانات غير صحيحة أو غير دقيقة، أو إذا تم الحصول على البيانات بصورة غير قانونية.

د - أن تضع الضمانات المناسبة بهدف منع الآثار الضارة بحقوق الإنسان التي ترتبط ارتباطا مباشرا بعملياتها أو منتجاتها أو خدماتها، أو إلى التخفف من تلك الآثار، بما في ذلك باستخدام الشروط التعاقدية عند الضرورة، أو أن تخطر الكيانات المعنية بالتجاوزات أو الانتهاكات عند اكتشاف إساءة لاستخدام منتجاتها وخدماتها.

3- أن تقوم بتشجيع المؤسسات التجارية على العمل لإيجاد الحلول التقنية اللازمة لتأمين وحماية سرية الاتصالات الرقمية، بحيث يمكن أن تشمل هذه الحلول تدابير التشفير وإخفاء الهوية وإغفال الهوية ، وتدعو الدول إلى عدم التدخل في استخدام تلك الحلول التقنية، على أن تكون أي قيود

[1] - www.un.org/ar/ga/75/resolutions.shtml
Documents-dds-ny.un.org/doc/undoc/gen/n20/371/73/pdf/n2037173.pdf
A/RES/75/176

تفرضها على تلك الحلول ممتثلة للالتزامات الملقاة على الدول بموجب القانون الدولي لحقوق الإنسان، وأن تضع سياسات تعترف للأفراد بخصوصيات الاتصالات الرقمية وكذا تقوم بحمايتها.[1]

ثالثا – قرار اتخذته الجمعية العامة في 3 مارس2021 حول التعاون بين الأمم المتحدة ومجلس أوروبا:

في الدورة الخامسة والسبعون، وفي الجلسة العامة 56، وتحت البند 130 (ل) من جدول الأعمال التعاون بين الأمم المتحدة والمنظمات الإقليمية والمنظمات الأخرى "التعاون بين الأمم المتحدة ومجلس أوروبا"، قرار اتخذته الجمعية العامة في 3مارس2021 حول التعاون بين الأمم المتحدة ومجلس أوروبا.

إذ الجمعية العامة:

تنوه على استمرار تطوير اتفاقية مجلس أوروبا لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية، المفتوحة أمام جميع الدول لتنضم إليها وتحديثها، وتؤكد على أنه يجب حماية واحترام الحق في الخصوصية وحرية التعبير في ظل تطور مجتمع المعلومات والإنترنت، ، مثلما جاء في المادة 17و19 من العهد الدولي الخاص بالحقوق المدنية والسياسية، بما في ذلك من حيث صلته بحماية البيانات، وتشير إلى أن فرض أي قيود على هذه الحقوق يجب أن يتم في امتثال تام للقانون الدولي لحقوق الإنسان، وتنوه بأهمية عمل مجلس أوروبا في حماية حقوق الإنسان على شبكة الإنترنت وخارجها، بما في ذلك في مكافحة خطاب الكراهية، وترحب بالتعاون بين وكالات الأمم المتحدة ذات الصلة و الإجراءات الخاصة لمجلس حقوق الإنسان، بما فيها المقرر الخاص المعني بالحق في الخصوصية، والمقررة الخاصة المعنية بتعزيز وحماية الحق في حرية الرأي.

كما ترحب بالتعاون الوثيق بين المنظمتين في مكافحة الجريمة المنظمة العابرة للحدود الوطنية والجرائم الحاسوبية والإرهاب وغسل الأموال والجرائم البيئية وتواصل التشجيع عليه، فضلا عن التعاون

[1] – www.un.org/ar/ga/75/resolutions.shtml
Documents-dds-ny.un.org/doc/undoc/gen/n20/371/73/pdf/n2037173.pdf
A/RES/75/176

فيما يتعلق بحماية حقوق ضحايا تلك الجرائم، وتذكر مرة أخرى بأن اتفاقية مجلس أوروبا المتعلقة بالجرائم الحاسوبية وبروتوكولها الإضافي المتعلق بتجريم الأفعال المتسمة بطابع العنصرية وكراهية الأجانب التي تتركب عبر النظم الحاسوبية، مفتوحة للانضمام إليها أمام جميع دول العالم.[1]

رابعا- قرار اتخذته الجمعية العامة في 26ماي2021م حول مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية:

في الدورة الخامسة والسبعون وفي الجلسة العامة 71 تحت البند 112 من جدول الأعمال "مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية"، قرار اتخذته الجمعية العامة في 26ماي2020م حول مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

إذ الجمعية العامة :

تلاحظ أن تكنولوجيات المعلومات والاتصالات، بالرغم من أنها تتيح إمكانيات هائلة لتنمية الدول، فإنها تخلق فرصا جديدة للجناة وقد تؤدي إلى استفحال مستويات الجريمة ودرجات تعقيدها، وإذ تشير إلى قرارها 74/ 247 المؤرخ 27 ديسمبر 2019 الذي قررت فيه أن اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية ينبغي أن تتفق على الخطوط العريضة لأنشطتها المستقبلية وطرائق القيام بتلك الأنشطة قصد عرضها على الجمعية العامة في دورتها الخامسة والسبعين للنظر فيها والموافقة عليها.

1- ترحب بانتخاب أعضاء مكتب اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية في دورتها التنظيمية المعقودة في 10 مايو 2021.[1]

[1] - www.un.org/ar/ga/75/resolutions.shtml
Documents-dds-ny.un.org/doc/undoc/gen/n21/075/94/pdf/n2105794.pdf
A/RES/75/265

2- تقرر أن يواصل مكتب الأمم المتحدة المعني بالمخدرات والجريمة العمل باعتباره أمانة اللجنة المختصة.

3- تشير مع التقدير إلى الدورة التنظيمية للجنة المخصصة، التي عقدت في نيويورك في الفترة من 10الى 12مايو 2021.

4- تقرر أن تعقد اللجنة المخصصة ما لا يقل عن ست دورات، مدة كل دورة منها 10 أيام، اعتبارا من كانون الثاني /يناير2022، وأن تختم عملها من أجل تقديم مشروع اتفاقية إلى الجمعية العامة في دورتها الثامنة والسبعين.

5- تقرر أيضا أن تعقد اللجنة المخصصة الدورات التفاوضية الأولى والثالثة والسادسة في نيويورك والثانية والرابعة والخامسة في فينا، و أن تسترشد بالنظام الداخلي للجمعية العامة، بينما يجري اتخاذ جميع قرارات اللجنة بشأن المسائل الموضوعية التي لم يحصل بشأنها توافق في الآراء بأغلبية ثلثي الممثلين الحاضرين المشاركين في التصويت، على أن تقوم الرئيسة قبل ذلك، بناء على قرار يتخذه المكتب، بإبلاغ اللجنة بأن كل جهد للتوصل إلى اتفاق بتوافق الآراء قد استنفذ.

6- تقرر كذلك أن تعقد اللجنة المخصصة الدورة الختامية في نيويورك لأغراض اعتماد مشروع الاتفاقية.

7- تقرر أن تدعو إلى الدورات الموضوعية للجنة المخصصة، حسب الاقتضاء، ممثلي المنظمات الحكومية الدولية العالمية والإقليمية المهتمة، بمن فيهم ممثلو هيئة الأمم المتحدة ووكالاتها المتخصصة وصناديقها، وكذلك ممثلو اللجنة الفنية التابعة للمجلس الاقتصادي والاجتماعي بصفة مراقبين.

---

[1]- السيدة فوزية بومعيزة مباركي (الجزائر) رئيسة، والسيد أرسي دوينوغرا فردوسي (إندونيسيا) مقررا ،والسيد إميل ستويانوفسكي (أستراليا)، والسيد ووهايوين (الصين)، والسيدكلاوديوبيغيروكاستيلو(الجمهورية الدومينيكية)، والسيد محمد حمدي الملا(مصر)، والسيد ماركو كونابو (إستونيا)، والسيد تشيتاروشيميزو(اليابان)، والسيدة صبرا أماري موريلوسنتينو(نيكاراغوا)، والسيد تيرلومون جورج- ماريا تينديزوا(نيجيريا)، والسيدة دومينيكا كرويس (بولندا)، والسيد أنطونيو دي أليمدارييرو(البرتغال)، والسيد دميتري بوكين (الاتحاد الروسي)، والسيدة كيتي سويب (سورينام) ، والسيد جيمس والش(الولايات المتحدة الأمريكية)، نوابا للرئيسة.

8- تؤكد من جديد أن ممثلي المنظمات غير الحكومية التي تتمتع بمركز استشاري لدى المجلس الاقتصادي والاجتماعي، وفقا لقرار المجلس 1996/ 31المؤرخ 25 تموز يوليه 1996، يجوز لهم أن يسجلوا أنفسهم لدى الأمانة للمشاركة في دورات اللجنة المخصصة.[1]

9- تطلب إلى رئيسة اللجنة المخصصة أن تقوم بالتشاور مع مكتب الأمم المتحدة المعني بالمخدرات والجريمة، بإعداد قائمة بأسماء ممثلي المنظمات الأخرى غير الحكومية المعنية ومنظمات المجتمع المدني والأوساط الأكاديمية والقطاع الخاص، بمن فيهم من لديهم الخبرة في ميدان الجريمة السيبرانية، الذين يمكنهم أن يشاركوا في عمل اللجنة المخصصة، مع مراعاة مبدأي الشفافية و التمثيل الجغرافي العادل، وإيلاء ما يجب من اعتبار للتكافؤ بين الجنسين، وأن تقدم القائمة المقترحة إلى الدول الأعضاء لتنظر فيها على أساس عدم الاعتراض [2]، وأن تعرض القائمة على نظر اللجنة المخصصة كي تتخذ اللجنة قرارا نهائيا بشأن المشاركة.

10- تشجع رئيسة اللجنة المخصصة على استضافة مشاورات في الفترات الفاصلة بين الدورات لاستقاء الأفكار من طائفة متنوعة من الجهات صاحبة المصلحة بشأن إعداد مشروع الاتفاقية.

11- تؤكد من جديد أن تراعي اللجنة المخصصة مراعاة كاملة الصكوك الدولية القائمة والجهود المبذولة على كل من الصعيد الوطني والإقليمي والدولي لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، ولاسيما ما قام به فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية من أعمال وما توصل إليه من نتائج.[3]

---

[1]- www.un.org/ar/ga/75/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n21/133/49/pdf/n2113349.pdf

A/RES/75/282

[2] - تتضمن القائمة الأسماء المقترحة والأسماء النهائية ، ويجري إعلام رئيسة اللجنة المخصصة ومكتب الأمم المتحدة المعني بالمخدرات والجريمة ومقدم الطلب بالأساس العام لأي اعتراضات ، إذا طلبتها واحدة أو أكثر من الدول الأعضاء في الأمم المتحدة أو الدول الأعضاء في الوكالات المتخصصة

[3] - www.un.org/ar/ga/75/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n21/133/49/pdf/n2113349.pdf

A/RES/75/282

الفرع الثاني

قرار اتخذته الجمعية العامة في6 ديسمبر 2021 بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي ، وتعزيز السلوك المسئول من جانب الدول في استخدام تكنولوجيات المعلومات والاتصال

في الدورة السادسة والسبعون وفي الجلسة العامة 45 وتحت البند 95 من جدول الأعمال "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، قرار اتخذته الجمعية العامة في 6 ديسمبر 2021 في هذا المجال .

حيث أن الجمعية العامة أشارت إلى قراراتها السابقة من بينها القرار 75/ 32 في 7ديسمبر 2020م، و75/ 240 في 31 ديسمبر 2020، و72/ 512 في 4ديسمبر 2017 و 564/75 في 28 أبريل 2021.[1]

حيث شددت على أن من مصلحة جميع الدول تشجيع استخدام تكنولوجيات المعلومات والاتصالات في الأغراض السلمية ومنع نشوب النزاعات الناشئة عن استخدام تكنولوجيات المعلومات والاتصالات.

وإذ أشارت إلى أن عددا من الدول يطور قدرات في مجال تكنولوجيا المعلومات والاتصالات للأغراض العسكرية، وأن احتمال استخدام تكنولوجيات المعلومات والاتصالات في النزاعات المقبلة بين الدول آخذ في التزايد.

وإذ لاحظت تحقيق تقدم كبير في تطوير وتطبيق أحدث تكنولوجيات المعلومات و وسائل الاتصالات السلكية واللاسلكية، وإذ أعربت عن القلق من احتمال استخدام هذه التكنولوجيا و الوسائل في أغراض لا تتفق مع أهداف صون الاستقرار والأمن الدوليين، ويمكن أن تؤثر تأثيرا سلبيا على سلامة الهياكل الأساسية للدول، مما يضر بأمنها في الميادين **المدني والعسكري** على السواء.

---

[1] – www.un.org/ar/ga/76/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n21/377/46/pdf/n2137746.pdf

A/RES/76/19

وإذ أعربت عن القلق أيضا من الأنشطة الخبيثة في مجال تكنولوجيا المعلومات الاتصال التي تستهدف الهياكل الأساسية الحيوية ومرافق الهياكل الأساسية الحيوية للمعلومات التي تدعم الخدمات الأساسية المقدمة للجمهور، وإذا رأت أن من الضروري منع استخدام موارد أو تكنولوجيات المعلومات لأغراض إجرامية أو إرهابية.

وقد شددت على أهمية احترام حقوق الإنسان والحريات الأساسية في استخدام تكنولوجيات المعلومات والاتصالات، وإذ أشارت إلى أن بناء القدرات أمر ضروري لتعاون الدول وبناء الثقة في مجال أمن تكنولوجيا المعلومات والاتصالات .

وإذ أكدت من جديد أن المعايير الطوعية وغير الملزمة للسلوك المسئول من جانب الدول يمكن أن تحد من المخاطر التي تهدد السلام والأمن والاستقرار على الصعيد الدولي، بل تسعي إلى تحديد مقاييس للسلوك المسئول من جانب الدول، وتؤكد من جديد أيضا في الوقت نفسه أنه، بالنظر إلى السمات الفريدة لتكنولوجيات المعلومات والاتصالات، يمكن وضع قواعد إضافية بمرور الوقت، وبشكل منفصل، وإذ تشير إلى إمكانية وضع التزامات ملزمة إضافية في المستقبل، حسب الاقتضاء.

وإذ أكدت من جديد أيضا أن الأمم المتحدة ينبغي لها أن تواصل القيام بدور رائد في تعزيز الحوار بشأن استخدام تكنولوجيات المعلومات والاتصالات من جانب الدول.

وقد سلمت بأهمية الجهود التي يبذلها في هذا الاتجاه فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية المعنيان بالتطورات في ميدان المعلومـات والاتصالات

السلكية واللاسلكية في سياق الأمن الدولي.[1]

وإذ تسترشد بتقارير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي لأعوام 2010. 2013، 2015.

[1]–www.un.org/ar/ga/76/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n21/377/46/pdf/n2137746.pdfA/RES/76/19

1 – تسلم بإقرار التقرير النهائي المعتمد بتوافق الآراء للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

2– ترحب بالتقرير النهائي المعتمد بتوافق الآراء لفريق الأمم المتحدة للخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسئولة في سياق الأمن الدولي.

3– تهيب بالدول الأعضاء أن تسترشد في استخدامها لتكنولوجيات المعلومات والاتصالات بتقرير الفريق العامل المفتوح العضوية لعام 2021 وتقرير فريق الخبراء الحكوميين لعام 2021.

4– تؤيد الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021– 2025، وتعترف بولايته وفقا لقرار الجمعية العامة 75/ 240.

5 – تؤكد كذلك أن الفريق العامل المفتوح العضوية للفترة 2021– 2025 ينبغي أن يأخذ في اعتباره النتائج التي توصل إليها الفريق العامل المفتوح العضوية السابق وفرق الخبراء الحكوميين السابقة وأن يعزز ما بذلته تلك الفرق من جهود، وأن يكون قائما على توافق الآراء وأن يركز على تحقيق النتائج.[1]

6– تدعو جميع الدول الأعضاء إلى أن تواصل، آخذة في اعتبارها التقييمات والتوصيات الواردة في تقرير الفريق العامل المفتوح العضوية وتقارير فريق الخبراء الحكوميين، موافاة الأمين العام بآرائها وتقييماتها بشأن المسألتين التاليتين:

ا– الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان.

ب– مضمون المفاهيم مشار إليها في تقرير الفريق العامل المفتوح العضوية وتقارير فريق الخبراء الحكوميين.

[1] –www.un.org/ar/ga/76/resolutions.shtml

Documents–dds–ny.un.org/doc/undoc/gen/n21/377/46/pdf/n2137746.pdf A/RES/76/19

7 – تقرر أن تدرج في جدول الأعمال المؤقت لدورتها السابعة والسبعون البند المعنون "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي".[1]

في انتظار اختتام عمل اللجنة المخصصة لوضع مشروع اتفاقية دولية شاملة، بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وتقديمه إلى الجمعية العامة في دورتها الثامنة والسبعون التي تفتح يوم الثلاثاء 5سبتمبر 2023م.

نأمل أن ترى هذه الاتفاقية النور وأن تكون لها أرضية حقيقية لمجابهة هذا النوع من الجرائم خاصة في ظل التنامي المتسارع لها من جهة، وكذا في ظل سلوك بعض الدول الغير مسئول في الفضاء الإلكتروني في سياق الأمن الدولي، الذي قد يؤثر على مخرجات هذه الاتفاقية.

[1]– www.un.org/ar/ga/76/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n21/377/46/pdf/n2137746.pdfA/RES/76/19

الخاتمـــة

إن التطور العلمي الذي يشهده العالم خاصة في المجال التكنولوجي الرقمي بما في ذلك عالم الاتصالات، تطور ظاهره وعلنه كله يحمل مظاهر السرعة والدقة والعصرنة والتطور والقوة والريادة والتحكم، ولكن باطنه لا يخلوا من مخاوف التدخل والتحكم والتدمر والاختراق ، وذلك لما يحمل في طياته من بدور لإجرام وجريمة لم يألفها المجتمع من قبل ألا وهي الجريمة المعلوماتية، هذه الجريمة المستحدثة التي تعتبر من الجرائم التي وجدت ضالتها في ظل هذا التطور اللا متناهي في المجال التكنولوجي المتسارع، ومما لا شك فيه أن لهذا التطور انعكاس سلبي بانتشار لهذه الظاهرة بمختلف أشكالها وصورها.

وقد تناول الباحث موضوع الدراسة مكافحة الجريمة المعلوماتية في القانون الجزائري والدولي في بابين على النحو التالي :

أولا : خصص الباب الأول لدراسة الجريمة المعلوماتية ومكافحتها في القانون الجزائري، وذلك من خلال التطرق للإطار المفاهيمي للجريمة المعلوماتية في الفصل الأول، أما الفصل الثاني فتم التطرق فيه لمكافحة هذه الظاهرة بموجب القانون الجزائري وذلك من خلال القوانين العامة والقوانين والهيئات الخاصة .

ثانيا : أما الباب الثاني فخصصناه لمكافحة الجريمة المعلوماتية دوليا، وذلك من خلال تبيان القوانين والاتفاقيات الدولية في مجال مكافحة الجريمة المعلوماتية في الفصل الأول بتبيان المعاهدات والقوانين الخاصة بحماية حق الملكية الفكرية من جهة، وكذا الاتفاقيات الدولية في مجال مكافحة الجريمة السيبرانية من جهة أخرى، أما الفصل الثاني فتم التطرق فيه للاتجاهات الدولية في مجال مكافحة الجرائم المعلوماتية، وذلك من خلال التطرق للتعاون الدولي في مجال مكافحة جرائم المعلوماتية وإشكالاته من جهة، وكذا التطرق لما هو قادم من خلال اتفاقية عالمية لمكافحة الجريمة السيبرانية برعاية الأمم المتحدة في غضون سنة 2023 من جهة أخرى .

وقد انتهت الدراسة إلى مجموعة من النتائج والتوصيات على النحو الآتي :

النتائج:

1- نلاحظ عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، وتكشف النماذج المعروفة لتعريفات هذه الجريمة على تعدد المصطلحات المستخدمة للدلالة عليها وتحديد مفهومها، هناك ما يطلق عليها اسم جرائم الحاسبات أو إساءة استخدام الحاسب، أو الجرائم المرتبطة أو المتعلقة بالحاسبات، أو جرائم المعالجة الآلية للبيانات أو جرائم التكنولوجيا الحديثة، أو جرائم المعلوماتية.

2- أصبح للمشرع الجنائي مسؤولية كبيرة في مواجهة الجريمة المعلوماتية خاصة في ظل التطور التكنولوجي المعلوماتي الهائل والمتسارع.

3- سارع المشرع الجزائري في تعديل منظومته القانونية لتتماشى مع الطبيعة الخاصة لهذا النوع من الجرائم، وخاصة منذ سنة 2004 وذلك سواء من الناحية الموضوعية والإجرائية دون أن ننسى التعديلات التي سبقتها .

4- لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الإلكتروني، لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعية ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها أن تتفادى وقوع الجريمة الإلكترونية، أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما استدراكه المشرع بتضمين القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة، تتعلق بالتحقيق في الجرائم الإلكترونية، تتمثل في مراقبة الاتصالات الإلكترونية، تسجيلها والتسرب.

5- نظرا لخطورة هذا النوع من الجرائم، تطلب على المشرع الجزائري سن العديد من القوانين، ومنها القوانين الخاصة فجاء المشرع بالقانون 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث هدف هذا القانون وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذا حسب المادة الأولى منه، كما وضح هذا القانون بعض المفاهيم المتعلقة بهذا النوع من الجرائم، كمفهوم الجرائم المتصلة

بتكنولوجيات الإعلام والاتصال، والمنظومة المعلوماتية، ومعطيات معلوماتية، ومقدمو الخدمات، و الاتصالات الإلكترونية.

6- المرسوم الرئاسي 21-439 الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حرص على أن هذه الهيئة يجب أن تنظم وتشارك في عمليات التوعية حول استعمال تكنولوجيات الإعلام والاتصال وحول المخاطر المتصلة بها، كما أن هذا المرسوم جاء بعدة إضافات مهمة في هذا المجال .

7- أمام التغيرات العالمية المتسارعة التي يشهدها قطاع البريد والمواصلات السلكية واللاسلكية نتيجة التطور التكنولوجي، وكذا تطور السوق التنافسية لنشاط البريد والاتصالات، تدخل المشرع الجزائري سنة 2018 لسد الثغرات القانونية التي كشف عنها تطبيق أحكام القانون 2000/ 03 من خلال إصدار القانون 18/ 04 المؤرخ في 10-5-2018م، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الذي نص في المادة 11 على إنشاء سلطة ضبط مستقلة تحت تسمية سلطة ضبط البريد والاتصالات الإلكترونية، تتمتع بالشخصية المعنوية والاستقلال المالي، تكلف بضمان ضبط أسواق البريد والاتصالات الإلكترونية لحساب الدولة، من خلال السهر على وجود منافسة فعلية ومشروعة في هذين السوقين، باتخاذ كل التدابير الضرورية لترقية المنافسة.

8- لمتطلبات المعاملات الإلكترونية، لاسيما في ظل التوجه نحو الحكومة الإلكترونية ومقتضيات التجارة الإلكترونية، وبعد أن أدرج المشرع الجزائري نظام الإثبات بالكتابة في الشكل الإلكتروني ضمن قواعد الإثبات، أقر بنظام التوقيع والتصديق الإلكترونيين والاعتراف بحجيتهما في الإثبات قصد توفير الحماية اللازمة لوسائل الدفع الإلكتروني بالنسبة لمعاملات التجارة الإلكترونية، وزرع الثقة لدى المتعاملين لما يمتاز به من مستوى عال للسرية والخصوصية، وجرم القانون رقم 15-04 بعض الأفعال المرتبطة بالبيانات والمعلومات ذات الطابع الشخصي التي تشكل الاعتداء عليها جريمة يعاقب مرتكبيها بأحكام جزائية.

9- مواكبة المشرع الجزائري للجرائم الماسة بخصوصية الأفراد، أصدر قانون يهدف إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وهذه المعالجة

مهما كان مصدرها أو شكلها، يجب أن يكون في إطار احترام الكرامة الإنسانية والحياة الخاصة و الحريات العامة، وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم، وهو القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

10- حاول المشرع الجزائري مواجهة الجريمة الإلكترونية من خلال قانون الملكية الأدبية والفنية المتعلق بحق المؤلف والحقوق المجاورة الصادر بموجب الأمر رقم 03-05 المؤرخ في 23-07-2003 المتعلق بحقوق المؤلف والحقوق المجاورة حيث وسع قائمة المؤلفات المحمية، وذلك بإدماج برامج المعلوماتية ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد بيانات برامج المعلوماتية، كما شدد العقوبات على المساس بحقوق المؤلفين خاصة المنصفات الرقمية التي تشملها الحماية.

11- استحداث قطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب الأمر رقم 21-11 المتمم والمعدل لقانون الإجراءات الجزائية الجزائري، القطب المستحدث أنشأ على مستوى محكمة مقر مجلس قضاء الجزائر، كقطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، استحداث هذا القطب يندرج ضمن إستراتيجية شاملة للدولة إزاء هذا النوع من الجرائم، إذ يمثل هذا القطب خطوة إضافية في مسار التصدي للجرائم الالكترونية.

12- ينظر إلى "**اتفاقية برن**"، على أنها الأب الشرعي لتنظيم حقوق المؤلف والحقوق المجاورة على المستوى الدولي، خصوصا وأنها من أوائل الاتفاقيات التي تم التوصل لها لمعالجة مسائل حقوق المؤلف.

13- معاهدة الويبو بشأن حق المؤلف تطرقت في المادة الرابعة لبرامج الحاسوب معبرة على أنها تتمتع بالحماية باعتبارها مصنفات أدبية بمعنى المادة 2 من اتفاقية برن، وتطبق تلك الحماية على برامج الحاسوب أيا كانت طريقة التعبير عنها أو شكلها.

14- بمجيء القانون رقم 75 لسنة 2019 الكويتي في شأن حقوق المؤلف والحقوق المجاورة، فالمادة 43 منه عاقبت بالحبس مدة لا تقل عن ستة أشهر ولا تزيد عن سنتين وغرامة لا تقل عن 500 دينار ولا تزيد عن 50,000 دينار أو إحدى هاتين العقوبتين، كل من قام بغير إذن كتابي من

المؤلف أو صاحب الحق المجاور، أو من يخلفهما بالاعتداء من جهة على حق من الحقوق الأدبية أو المالية للمؤلف أو صاحب الحقوق المجاورة المنصوص عليها في هذا القانون، بما في ذلك إتاحة أي مصنف للجمهور أو عرض أي مصنف أو أداء أو تسجيل صوتي أو برنامج البث مما تشمله الحماية المقررة في هذا القانون عبر أجهزة الحاسب الآلي أو شبكات المعلومات أو شبكات الاتصالات أو غيرها من الطرق أو المسائل الأخرى.

15- حرص مجلس أوروبا على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات، وتجلى ذلك في اتفاقية بودابست الموقعة في 23 نوفمبر 2001 المتعلقة بالإجرام الكوني، بمعنى الإجرام المعلوماتي أو الجرائم المعلوماتية، إيمانا من الدول الأعضاء في هذا المجلس والدول الأخرى الموقعة على هذه الاتفاقية بالتغيرات العميقة التي حدثت بسبب الرقمية، والتقارب، والعولمة المستمرة للشبكات المعلوماتية.

16- البروتوكول الإضافي الأول لاتفاقية الجريمة الالكترونية المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة بواسطة نظم الحاسوب، هذا البروتوكول تم النص عليه بتاريخ 28 يناير 2003م وبدأ النفاد في 01 مارس2006، ويلزم الدول التي صادقت عليه لتجريم نشر العنصرية وكراهية الأجانب المواد من خلال أنظمة الكمبيوتر، فضلا على التهديدات والشتائم بدافع العنصرية أو كراهية الأجانب.

17- هدف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذا النوع من الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

18- يشكل التعاون العالمي الطريقة الحقيقية الوحيدة لأجل محاربة وجود مضامين مجرمة على الإنترنت، بواسطة نصوص عالمية كالاتفاقية حول جرائم الفضاء السيبراني، إلا أن الإنترنت تمتاز بغياب الحدود، وبلا مادية الاتصالات، هذه الميزة العالمية تجعل تنظيم الشبكات معقدا، و طرح الطابع العالمي مشاكل متعددة في أي مجال كان وبصورة أخص في مجال الإنترنت، فالحلول المنصوص عليها في التشريعات الداخلية، لا يمكن أن تكون نافعة إلا إذا أظهرت البلدان إرادة للتعاون، يبدو من الصعوبة بمكان تنظيم الشبكة بواسطة القوانين الداخلية كون الحدود ليست محصورة، لذلك اتجهت نحو القانون الدولي الذي يشكل الوسيلة الوحيدة الموجودة في غياب الحدود،

وفي ظل البث السريع للمعلومات حاولوا وضع جزء من السيادة جانبا، وتوضيح مبادئ عامة من أجل مكافحة جرائم التكنولوجيا بصورة فعالة.

19 – انتظار اختتام عمل اللجنة المخصصة لوضع مشروع اتفاقية دولية شاملة، بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وتقديمه إلى الجمعية العامة في دورتها الثامنة والسبعون التي تفتح يوم الثلاثاء 5سبتمبر2023م، نأمل أن ترى هذه الاتفاقية النور وأن تكون لها أرضية حقيقية لمجابهة هذا النوع من الجرائم خاصة في ظل التنامي المتسارع لها من جهة، وكذا في ظل سلوك بعض الدول الغير مسئول في الفضاء الإلكتروني في سياق الأمن الدولي، الذي قد يؤثر على مخرجات هذه الاتفاقية.

التوصيات:

1– النظر في مواصلة التعاون، حسب الاقتضاء وبطريقة شفافة وخاضعة للمسائلة، مع القطاع الخاص والمجتمع المدني، في وضع التدابير الرامية إلى مكافحة الجريمة المعلوماتية.

2– ضرورة تعزيز التنسيق والتعاون بين الدول في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، بما فيها تقديم المساعدة التقنية للبلدان النامية، بناء على طلبها من أجل تحسين التشريعات الوطنية وبناء قدرات السلطات الوطنية بغية التصدي لذلك الاستخدام بكل أشكاله، بما يشمل منعه والكشف عنه والتحقيق فيه وملاحقة مرتكبيه قضائيا.

3– المجتمع الدولي بحاجة ملحة إلى وضع إطار قانوني عالمي لمكافحة الجريمة المعلوماتية، وإلى العمل سويا لمواجهة وضع الجريمة الذي تتزايد خطورته بمرور الوقت، ولاسيما مواجهة التحديات الجديدة الناشئة عن التكنولوجيات الجديدة، مثل الحوسبة السحابية والذكاء الاصطناعي وانترنت الأشياء والعملات الرقمية المشفرة، وغير ذلك .

4– الحاجة إلى تكثيف الوقاية من خلال زيادة الوعي في المجتمعات بشأن الأساليب التي تستخدمها العصابات الإجرامية الناشطة على الإنترنت.

5- هناك حاجة عاجلة إلى توفير التدريب المتخصص في مجال الأدلة الإلكترونية .

6- ينبغي للدول أن تعطي الأولوية لتقديم المساعدة بشأن الإصلاح التشريعي وبناء القدرات، بغية كفالة ترجمة القوانين الجديدة إلى إجراءات عملية.

7- تشجيع تدريب موظفي أجهزة إنفاذ القانون وسلطات التحقيق والنيابة العامة والقضاة على التعامل مع الجريمة المعلوماتية، بما يشمل التدريب على المهارات المناسبة في جمع الأدلة وتكنولوجيا المعلومات، وتجهيزهم ليضطلعوا بأدوارهم بفعالية في التحقيق في الجرائم المعلوماتية وملاحقة مرتكبيها وتقديمهم إلى العدالة.

8- أهمية الشراكات والمبادرات الدولية والإقليمية والثنائية بين أصحاب المصلحة المتعددين، التي تزيد من فعالية الجهود المبذولة وتعزيز حقوق الطفل والقضاء على الاستغلال الجنسي للأطفال وانتهاكهم جنسيا على الإنترنت، والتي تجري من خلالها بحوث رامية لإنشاء قاعدة استدلالية دقيقة بشأن استخدام الأطفال للإنترنت.

9- أن تتخذ التدابير اللازمة لوضع حد لانتهاكات الحق في الخصوصية، وأن تهيئ الظروف الكفيلة بالحيلولة دون حدوث الانتهاكات، بطرق منها ضمان توافق التشريعات الوطنية ذات الصلة مع الالتزامات الملقاة على عاتقها بموجب القانون الدولي لحقوق الإنسان.

10- ضرورة الانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة الجرائم المعلوماتية .

11- توفير موارد مناسبة من أجل التحري عن الجرائم المتعلقة بالاستغلال الجنسي للأطفال أو انتهاكهم جنسيا على الإنترنت والملاحقة القضائية لمرتكبيها، وفقا لما تقتضيه التشريعات الوطنية .

12- على الدول تبادل المعلومات بشأن أفضل الممارسات على نحو استباقي واتخاذ الإجراءات اللازمة لمكافحة الاستغلال الجنسي للأطفال وانتهاكهم جنسيا، بما في ذلك مصادرة أو حذف المواد المتعلقة بالانتهاك الجنسي للأطفال من الانترنت وتقليل المساحة الزمنية التي يستغرقها القيام بذلك، بما يتسق مع القوانين الوطنية.

الملاحق

الملحق رقم01 :" أمر رقم 21-11المؤرخ في 25غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 18صفر 1386الموافق8 يونيو 1966، والمتضمن قانون الإجراءات الجزائية، المتعلق بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال."

الملحق رقم 01

★

أمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق 25 غشت سنة 2021، يتمّم الأمر رقم 66-155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.

إنّ رئيس الجمهورية،

– بناء على الدستور، لاسيما المواد 139-7 و142 و198 و224 منه،

– وبمقتضى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمدة من قبل الجمعية العامة لمنظمة الأمم المتحدة بتاريخ 15 نوفمبر سنة 2000، المصادق عليها، بتحفظ، بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 22 ذي القعدة عام 1422 الموافق 5 فبراير سنة 2002،

– وبمقتضى الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بموجب المرسوم الرئاسي رقم 14-251 المؤرّخ في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014،

– وبمقتضى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بموجب المرسوم الرئاسي رقم 14-252 المؤرّخ في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014،

– وبمقتضى القانون العضوي رقم 04-11 المؤرخ في 21 رجب عام 1425 الموافق 6 سبتمبر سنة 2004 والمتضمن القانون الأساسي للقضاء،

– وبمقتضى القانون العضوي رقم 05-11 المؤرخ في 10 جمادى الثانية عام 1426 الموافق 17 يوليو سنة 2005 والمتعلق بالتنظيم القضائي، المعدل،

– وبمقتضى القانون العضوي رقم 12-05 المؤرخ في 18 صفر عام 1433 الموافق 12 يناير سنة 2012 والمتعلق بالإعلام،

– وبمقتضى الأمر رقم 66-155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 66-156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 96-22 المؤرّخ في 23 صفر عام 1417 الموافق 9 يوليو سنة 1996 والمتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج، المعدّل والمتمّم،

– وبمقتضى القانون رقم 09-04 المؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– وبمقتضى القانون رقم 14-04 المؤرّخ في 24 ربيع الثاني عام 1435 الموافق 24 فبراير سنة 2014 والمتعلق بالنشاط السمعي البصري،

– وبمقتضى القانون رقم 15-03 المؤرّخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015 والمتعلق بعصرنة العدالة،

– وبمقتضى القانون رقم 15-04 المؤرّخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين،

– وبمقتضى القانون رقم 15–12 المؤرخ في 28 رمضان عام 1436 الموافق 15 يوليو سنة 2015 والمتعلق بحماية الطفل،

– وبمقتضى القانون رقم 18–04 المؤرّخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية،

– وبمقتضى القانون رقم 18–07 المؤرّخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،

– وبمقتضى القانون رقم 20–05 المؤرّخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020 والمتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما،

– وبعد رأي مجلس الدولة،

– وبعد الاستماع إلى مجلس الوزراء،

– وبعد الأخذ بقرار المجلس الدستوري،

يصدر الأمر الآتي نصه :

المادّة الأولى : يهدف هذا الأمر إلى تتميم أحكام الأمر رقم 66–155 المؤرّخ في18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.

المادّة 2 : يتمّم الكتاب الأول من الأمر رقم 66–155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه، بباب سادس عنوانه "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" يتضمن المواد 211 مكرر 22 و211 مكرر23 و211 مكرر 24 و211 مكرر 25 و211 مكرر 26 و211 مكرر 27 و211 مكرر 28 و211 مكرر29، ويحرر كما يأتي :

الباب السادس

القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

"المادة 211 مكرر 22 : ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها.

كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحا.

يقصد، بمفهوم هذا القانون، بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال".

"المادة 211 مكرر 23 : يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل الإقليم الوطني".

"المادة 211 مكرر 24 : مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر 22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقاضي التحقيق ورئيس ذات القطب، حصريًا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أدناه وكذا الجرائم المرتبطة بها :

– الجرائم التي تمسّ بأمن الدولة أو بالدفاع الوطني،

– جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع،

– جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية،

– جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية،

– جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين،

– جرائم التمييز وخطاب الكراهية."

"المادة 211 مكرر 25 : مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر 22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب، حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا والجرائم المرتبطة بها.

يقصد بالجريمة المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا، بمفهوم هذا القانون، الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب

اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة آثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين، تتطلب استعمال وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي".

"*المادة 211 مكرر 26* : تطبق على الاختصاص الحصري للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المنصوص عليه في المادتين 211 مكرر 24 و211 مكرر 25 أعلاه، الإجراءات المنصوص في المواد 211 مكرر 19 إلى 211 مكرر 21 من هذا القانون ".

"*المادة 211 مكرر 27* : دون الإخلال بأحكام المادتين 211 مكرر 24 و211 مكرر25 أعلاه، يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب اختصاصا مشتركا مع الاختصاص الناتج عن تطبيق المواد 37 و40 و329 من هذا القانون بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها.

تطبق، في هذه الحالة، الإجراءات المنصوص عليها في المواد 211 مكرر 4 إلى 211 مكرر 15 من هذا القانون، أمام القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ".

"*المادة 211 مكرر 28* : إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع اختصاص القطب الاقتصادي والمالي، يؤول الاختصاص وجوبا لهذا الأخير".

"*المادة 211 مكرر 29* : إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع اختصاص محكمة مقر مجلس قضاء الجزائر طبقا لأحكام المواد 211 مكرر 16 إلى 211 مكرر 21 من هذا القانون، يؤول الاختصاص وجوبا لهذه الأخيرة".

المادّة 3 : ينشر هذا الأمر في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة .

حرر بالجزائر في 16 محرم عام 1443 الموافق 25 غشت سنة 2021.

عبد المجيد تبون

الملحق رقم02 : " أمر رقم 21-09 مؤرخ في 27 شوال عام 1442 الموافق 8 يونيو سنة 2021، يتعلق بحماية المعلومات والوثائق الإدارية. "

ملحق رقم02

– إدراج القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ضمن تأشيرات الأمر موضوع الإخطار.

ثانيًا : تعد أحكام الأمر المتعلق بحماية المعلومات والوثائق الإدارية، دستورية.

ثالثًا : يبلّغ هذا القرار إلى رئيس الجمهورية.

رابعًا : ينشر هذا القرار في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

بهذا تداول المجلس الدستوري في جلساته المنعقدة بتاريخ 24 و25 و26 شوال عام 1442 الموافق 5 و6 و7 يونيو سنة 2021.

رئيس المجلس الدستوري

كمال فنيش

محمد حبشي، نائبا للرئيس،

سليمة مسراتي، عضوة،

شادية رحاب، عضوة،

إبراهيم بوتخيل، عضوا،

محمد رضا أوسهلة، عضوا،

عبد النور قراوي، عضوا،

خديجة عباد، عضوة،

سماعيل بليط، عضوا،

الهاشمي براهمي، عضوا،

أمحمد عدة جلول، عضوا،

عمر بوراوي، عضوا.

★

أمر رقم 21-09 مؤرّخ في 27 شوّال عام 1442 الموافق 8 يونيو سنة 2021، يتعلق بحماية المعلومات والوثائق الإدارية.

إنّ رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 34 و47 و54 و55 و139 و141 (الفقرة 2) و142 و198 و224 منه،

– وبمقتضى القانون العضوي رقم 12-05 المؤرخ في 18 صفر عام 1433 الموافق 12 يناير سنة 2012 والمتعلق بالإعلام،

– وبمقتضى الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدل والمتمم،

– وبمقتضى الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم،

– وبمقتضى الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدل والمتمم،

– وبمقتضى القانون رقم 88-09 المؤرخ في 7 جمادى الثانية عام 1408 الموافق 26 يناير سنة 1988 والمتعلق بالأرشيف الوطني،

– وبمقتضى القانون رقم 90-11 المؤرخ في 26 رمضان عام 1410 الموافق 21 أبريل سنة 1990 والمتعلق بعلاقات العمل، المعدل والمتمم،

– وبمقتضى الأمر رقم 06-03 المؤرّخ في 19 جمادى الثانية عام 1427 الموافق 15 يوليو سنة 2006 والمتضمن القانون الأساسي العام للوظيفة العمومية،

– وبمقتضى القانون رقم 08-09 المؤرخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبمقتضى القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– وبمقتضى القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية،

– وبمقتضى القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،

– بعد رأي مجلس الدولة،

– وبعد الاستماع إلى مجلس الوزراء،

– وبعد الأخذ بقرار المجلس الدستوري،

يصدر الأمر الآتي نصه :

الفصل الأول
أحكام عامة

المادّة الأولى : يهدف هذا الأمر إلى حماية المعلومات والوثائق الإدارية للسلطات العمومية.

المادّة 2 : تخضع لأحكام هذا الأمر المعلومات والوثائق المصنفة المتعلقة بالدولة ومؤسساتها وهيئاتها التشريعية والقضائية والتنفيذية والإدارات العمومية والجماعات المحلية وكل مؤسسة تملك الدولة كل أو بعض رأسمالها وكل مؤسسة تقدم خدمة عمومية والتي تدعى في النص "السلطات المعنية".

المادّة 3 : يقصد، في مفهوم هذا الأمر، بما يأتي :

1- الموظف العمومي :

– كل شخص يشغل منصبا تشريعيا أو تنفيذيا أو إداريا أو قضائيا أو في أحد المجالس الشعبية المحلية المنتخبة، سواء أكان معيّنا أو منتخبا، دائما أو مؤقتا، مدفوع الأجر أو غير مدفوع الأجر، بصرف النظر عن رتبته أو أقدميته،

– كل شخص آخر يتولى، ولو مؤقتا، وظيفة أو وكالة بأجر أو بدون أجر، ويساهم بهذه الصفة في خدمة هيئة عمومية أو مؤسسة عمومية أو أي مؤسسة أخرى تملك الدولة كل أو بعض رأسمالها، أو أي مؤسسة أخرى تقدم خدمة عمومية،

– كل شخص آخر معرّف بأنه موظف عمومي أو من في حكمه طبقا للتشريع والتنظيم المعمول بهما،

2- الوثيقة : المراسلات والمحررات والمستندات التي أنشأتها أو حصلت عليها أي من السلطات المعنية أثناء ممارسة نشاطها،

3- الوثائق المصنفة : أي مكتوب ورقي أو إلكتروني أو رسم أو مخطط أو خريطة أو صورة أو شريط صوتي أو سمعي بصري أو أي سند مادي أو إلكتروني آخر كانت محل تدابير ترمي إلى منع نشرها أو تقييد الاطلاع عليها،

4- المعلومات : أي حدث أو خبر مهما كان مصدره، وثيقة أو صورة أو شريط صوتي أو مرئي أو سمعي بصري أو محادثة أو مكالمة هاتفية، يؤدي الكشف عنها إلى المساس بالسلطات المعنية.

المادّة 4 : تعد الوثائق المنصوص عليها في هذا الأمر ملكية عمومية، وهي غير قابلة للتصرف فيها أو لاكتسابها بأي طريقة كانت.

المادّة 5 : لا تمس الأحكام الواردة في هذا الأمر بحق المواطن في الوصول إلى المعلومة.

الفصل الثاني
قواعد حماية المعلومات والوثائق المصنفة

المادّة 6 : تصنف الوثائق، حسب درجة حساسيتها، إلى الأصناف الآتية :

– **"سرّي جدا"**، ويتضمن الوثائق التي يلحق إفشاؤها خطرا بالأمن الوطني الداخلي والخارجي،

– **"سرّي"**، ويتضمن الوثائق التي يلحق إفشاؤها ضررا خطيرا بمصالح الدولة،

– **"واجب الكتمان"**، ويتضمن الوثائق التي يلحق إفشاؤها ضررا أكيدا بمصالح الحكومة أو الوزارات أو الإدارات أو إحدى الهيئات العمومية،

– **"توزيع محدود"**، ويتضمن الوثائق التي يؤدي إفشاؤها إلى المساس بمصالح الدولة ولا يجوز الاطلاع عليها إلاّ من قبل الأشخاص المؤهلين بحكم الوظيفة أو المهمة.

تحدد شروط وكيفيات تطبيق هذه المادة عن طريق التنظيم.

المادّة 7 : تلزم السلطات المعنية بتأمين وثائقها ومعلوماتها وحمايتها، وتتخذ التدابير اللازمة لتصنيفها وتنظيم تداولها وحفظها وفقا للأحكام المنصوص عليها في التشريع والتنظيم المعمول بهما، ولا سيما ما يتعلق منها بالأرشيف الوطني.

يجب أن يخضع موظفو السلطات المعنية إلى تكوين خاص في استعمال المعلومات والوثائق المصنفة.

تحدد شروط وكيفيات تطبيق هذه المادة عن طريق التنظيم.

المادّة 8 : لا يمكن أن تكون مراسلات السلطات المعنية مع وإلى الغير، محل نشر أو تداول أو توزيع إلاّ بموافقتها، ما لم ينص القانون على خلاف ذلك.

المادّة 9 : يجب على السلطات المعنية، في حال تسريب معلومات أو وثائق مصنفة، إخطار الجهات المختصة فورا قصد فتح تحقيق.

المادّة 10 : يحظر على أيّ كان نشر أو إفشاء محاضر وأوراق التحريات والتحقيق القضائي أو تمكين من لا صفة له من حيازتها، مع مراعاة الاستثناءات المنصوص عليها في قانون الإجراءات الجزائية.

المادّة 11 : يمنع على أيّ كان اطلع، بحكم عمله أو مسؤوليته، على وثيقة مصنفة أو حصل عليها بأي صورة كانت، أخذ نسخ أو صور منها أو نشر محتواها كله أو بعضه، أو إعلام الغير بوجودها، إلاّ بموافقة السلطة المعنية.

المادّة 12 : يجب على كل شخص يحوز وثيقة مصنفة دون أن يكون مؤهلا لذلك، تسليمها إلى السلطات المعنية ويمنع عليه إفشاء مضمونها، تحت طائلة العقوبات المنصوص عليها في هذا الأمر.

المادّة 13 : يجب على السلطات المعنية، في إطار محاربة المعلومات الكاذبة والمحرّفة، تفعيل الاتصال المؤسساتي والإعلام الفوري للرأي العام.

الفصل الثالث

التزامات الموظف العمومي

المادّة 14 : يلزم الموظف العمومي، تحت طائلة العقوبات المنصوص عليها في هذا الأمر، بالسرّ المهني وعدم إفشاء محتوى أي وثيقة أو أي معلومة اطلع عليها أثناء أو بمناسبة ممارسة مهامه، ما لم ينص القانون على خلاف ذلك.

ويبقى هذا المنع ساريا لمدة عشر (10) سنوات من توقف أو انتهاء العلاقة المهنية للموظف العمومي بالاستقالة أو التسريح أو العزل أو الإحالة على التقاعد أو لأي سبب آخر، مع مراعاة أحكام المادة 50 من هذا الأمر.

المادّة 15 : يمنع على الموظف العمومي إخراج الوثائق المصنفة أو نسخ منها أو صور عنها من مكان العمل، أو طبعها أو نسخها خارج المؤسسات الرسمية، ما لم تقتض ضرورة المصلحة أو طبيعة العمل ذلك.

المادّة 16 : يمنع الموظف العمومي من الإدلاء لوسائل الإعلام أو في وسائل التواصل الاجتماعي بأي معلومة أو تعليق أو تصريح أو مداخلة حول المعلومات و/أو الوثائق التي اطلع عليها، بحكم مهامه، أو حول مسائل ما زالت قيد الدراسة لدى الجهة التي يعمل فيها، ما لم يكن مرخصا له بذلك.

الفصل الرابع

المسؤولية المدنية والتأديبية

المادّة 17 : يجوز للسلطات المعنية طلب تعويض عما أصابها من ضرر نتيجة نشر وثيقة مصنفة أو إفشاء معلومات تخصها، طبقا للقواعد المنصوص عليها في التشريع المعمول به، دون الإخلال بالمتابعات الجزائية المحتملة.

المادّة 18 : يمكن الجهة القضائية المختصة، بناء على طلب إحدى السلطات المعنية، أن توقف، تحت طائلة غرامة تهديدية يومية، نشر أي وثيقة مصنفة.

المادّة 19 : بغضّ النظر عن الأحكام المخالفة المنصوص عليها في التشريع الساري المفعول، يتعرض الموظف العمومي الذي يفشي عمدا وثائق مصنفة إلى التسريح من العمل.

المادّة 20 : يتعرض الموظف العمومي الذي يتسبب، بإهماله، في إفشاء وثائق مصنفة أو يقوم بإخراجها أو بإخراج نسخ منها أو صور عنها خارج مكان العمل أو يقوم بطبعها خارج المصلحة في غير الحالات التي تقتضيها المصلحة، إلى المساءلة التأديبية طبقا للتشريع الساري المفعول.

الفصل الخامس

قواعد إجرائية

المادّة 21 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص الجهات القضائية الجزائرية بالنظر في الجرائم المنصوص عليها في هذا الأمر التي ترتكب خارج التراب الوطني إضرارا بالدولة الجزائرية أو بمؤسساتها.

المادّة 22 : في إطار تطبيق أحكام هذا الأمر، يتعيّن على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها ووضع تحت تصرفها المعطيات التي يتعيّن عليهم حفظها تطبيقا لأحكام هذا الأمر.

ويتعيّن على مقدمي الخدمات كتمان سرّية العمليات التي ينجزونها وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء سرّ التحقيق.

المادّة 23 : يمكن الجهة القضائية المختصة إصدار أمر إلى مقدمي الخدمات، من أجل :

– التحفظ الفوري على المعطيات المتعلقة بالمحتوى و/أو بحركة السير المرتبطة بالجرائم المنصوص عليها في هذا الأمر، وفقا للكيفيات المحددة في التشريع الساري المفعول،

– التدخل الفوري، تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول، لسحب أو تخزين المحتويات التي يتيحون الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تشكل جريمة من الجرائم المنصوص عليها في هذا الأمر، أو بوضع ترتيبات تقنية تسمح بسحب أو تخزين هذه المحتويات أو لجعل الدخول إليها غير ممكن.

المادّة 24 : يجوز للجهة القضائية المختصة، بمناسبة التحقيق في إحدى الجرائم المنصوص عليها في هذا الأمر، أن تأمر أي شخص بتسليمها أي معلومات أو معطيات تكون مخزنة بواسطة استعمال وسائل تكنولوجيات الإعلام والاتصال، تحت طائلة العقوبات المنصوص عليها في هذا الأمر.

المادّة 25 : يمكن لضابط الشرطة القضائية المختص أن يضع، عبر الشبكات الإلكترونية، آليات تقنية للتبليغ عن الجرائم المنصوص عليها في هذا الأمر، ويعلم بذلك فورا وكيل الجمهورية، المختص الذي يأمر بالاستمرار في العملية أو بإيقافها.

المادّة 26 : تباشر النيابة العامة تحريك الدعوى العمومية تلقائيا في الجرائم المنصوص عليها في هذا الأمر.

المادّة 27 : يمكن اللجوء إلى أساليب التحري الخاصة المنصوص عليها في التشريع الساري المفعول، من أجل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا الأمر.

الفصل السادس
الأحكام الجزائية

المادّة 28 : يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 60.000 دج إلى 300.000 دج أو بإحدى هاتين العقوبتين، الموظف العمومي الذي ينشر أو يفشي أو يطلع الغير أو يسمح له بأخذ صور من المعلومات أو الوثائق المصنفة "توزيع محدود".

وتكون العقوبة بالحبس من سنة (1) إلى خمس(5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج إذا أدى ذلك إلى المساس بالاعتبار الواجب للسلطات المعنية.

المادّة 29 : دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج، الموظف العمومي الذي يفشي أو ينشر معلومة أو وثيقة مصنفة " واجب الكتمان" إلى علم الجمهور أو إلى علم شخص لا صفة له في الاطلاع عليها أو يسمح له بأخذ صور منها أو يترك الغير يقوم بذلك.

وتكون العقوبة الحبس من خمس (5) سنوات إلى عشر (10) سنوات والغرامة من 500.000 دج إلى 1.000.000 دج، إذا كانت الوثائق مصنفة "سرّي جدا" أو "سرّي ".

المادّة 30 : تكون العقوبة الحبس من ثلاثة (3) أشهر إلى سنة (1) والغرامة من 30.000 دج إلى 100.000 دج أو إحدى هاتين العقوبتين، إذا ارتكبت الجريمة المنصوص عليها في المادة 28 أعلاه، نتيجة عدم مراعاة الموظف العمومي الأحكام التشريعية و/ أو التنظيمية أو القواعد الاحترازية المرتبطة بطبيعة مهامه أو وظائفه.

تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 60.000 دج إلى 200.000 دج أو إحدى هاتين العقوبتين، إذا ارتكبت الجريمة المنصوص عليها في المادة 29 أعلاه، نتيجة عدم مراعاة الموظف العمومي للأحكام التشريعية و/ أو التنظيمية أو القواعد الاحترازية المرتبطة بطبيعة مهامه أو وظائفه.

المادّة 31 : يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات وبغرامة من 300.000 دج إلى 500.000 دج كل شخص مؤتمن بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلي بها إليه وأفشاها في غير الحالات التي يوجب أو يرخص القانون بالتبليغ عنها.

المادّة 32 : يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات وبغرامة من 300.000 دج إلى 500.000 دج، كل من ينشر محاضر و/ أو أوراق التحريات والتحقيق القضائي أو يفشي محتواها أو يمكّن من لا صفة له من حيازتها.

المادّة 33 : يعاقب بالحبس من خمس (5) سنوات إلى خمس عشرة (15) سنة وبغرامة من 500.000 دج إلى 1.500.000 دج، كل من أطلع الغير بمقابل، أيًا كانت طبيعته، على معلومة أو وثيقة مصنفة أو يسّر لغيره ذلك.

المادّة 34 : دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يعاقب بالحبس من سبع (7) سنوات إلى خمس عشرة (15) سنة وبغرامة من 700.000 دج إلى 1.500.000 دج، كل من يقوم بالأفعال المذكورة في المادّة 33 أعلاه، تنفيذا لخطة مدبرة داخل الوطن أو خارجه.

المادّة 35 : يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج أو باحدى هاتين العقوبتين، كل من يحوز وثيقة مصنفة، دون أن يكون مؤهلا لذلك، ولم يقم بتسليمها إلى السلطات المعنية.

وتطبق العقوبات المنصوص عليها في المادتين 28 و29 من هذا الأمر، حسب الحالة، إذا قام بإفشاء مضمونها.

المادّة 36 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل من يرتكب من غير الفاعلين أو الشركاء، الأفعال الآتية :

1 – إخفاء الوثيقة المصنفة أو الأشياء أو الأدوات التي استعملت أو كانت ستستعمل في ارتكاب الجرائم المنصوص عليها في هذا الأمر والأشياء أو المواد أو الأموال المتحصلة منها مع علمه بذلك.

2 – إتلاف أو اختلاس أو إخفاء أو تزييف عمدا وثيقة عمومية أو خاصة من شأنها تسهيل البحث عن الجرائم المنصوص عليها في هذا الأمر ومعاقبة مرتكبيها.

المادّة 37 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج كل من يدخل دون ترخيص إلى منظومة معلوماتية أو موقع إلكتروني أو شبكة إلكترونية أو

أي وسيلة أخرى من وسائل تكنولوجيات الإعلام والاتصال للسلطات المعنية، بقصد الحصول بغير وجه حق على معلومات أو وثائق مصنفة.

وتضاعف العقوبة في حال نشر هذه المعلومات أو الوثائق المصنفة قصد الإضرار بالسلطات المعنية أو الحصول على منافع مباشرة أو غير مباشرة.

المادّة 38 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، كل من ينشئ أو يدير أو يشرف على موقع إلكتروني أو حساب إلكتروني أو برنامج معلوماتي يستعمل لنشر المعلومات أو الوثائق المصنفة أو محتواها كليا أو جزئيا.

ويعاقب بنفس العقوبة كل من ينشر المعلومات والوثائق المصنفة أو محتواها كليا أو جزئيا على شبكة إلكترونية أو بإحدى وسائل تكنولوجيات الإعلام.

المادّة 39 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من عشر (10) سنوات إلى خمس عشرة (15) سنة وبغرامة من 1.000.000 دج إلى 1.500.000 دج، كل من يقوم عمدا بنشر أو بث، عن طريق الاتصالات الإلكترونية أو منظومة معلوماتية، معلومة أو وثيقة مصنفة، بغرض المساس بالنظام العام والسكينة العمومية.

المادّة 40 : يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات وبغرامة من 300.000 دج إلى 500.000 دج، كل من يمتنع عن تقديم الوثائق المنصوص عليها في المادة 24 من هذا الأمر.

المادّة 41 : يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 30.000 دج إلى 100.000 دج، أو بإحدى هاتين العقوبتين، كل من يقوم بنشر أو تداول أو توزيع المراسلات الإدارية التي لا تندرج ضمن الوثائق المصنفة الصادرة من أو إلى السلطات المعنية دون موافقتها أو في غير الحالات التي يسمح فيها القانون بذلك.

وتكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 60.000 دج إلى 200.000 دج في حالة العود.

المادّة 42 : يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا الأمر، بالعقوبات المنصوص عليها في قانون العقوبات.

المادّة 43 : كل من أنشأ أو شارك في جمعية أو اتفاق تشكل أو تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا الأمر، يعاقب بالعقوبات المقررة للجريمة التامة، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل.

المادّة 44 : دون المساس بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة أو أكثر من الجرائم المنصوص عليها في هذا الأمر، وكذا الأموال المتحصلة منها، وإغلاق الموقع الإلكتروني أو الحساب الإلكتروني الذي ارتكبت بواسطته الجريمة أو جعل الدخول إليه غير ممكن وإغلاق محل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه.

المادّة 45 : يمكن الجهة القضائية المختصة الحكم على مرتكبي الجرائم المنصوص عليها في هذا الأمر، بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات.

كما يمكنها الحكم على الموظف العمومي بالمنع من ممارسة وظيفة عليا نهائيا أو لمدة لا تقل عن خمس (5) سنوات ولا تزيد عن عشر (10) سنوات.

المادّة 46 : يعاقب بالعقوبات المقررة للفاعل، كل من يحرّض بأي وسيلة كانت، على ارتكاب الجرائم المنصوص عليها في هذا الأمر.

المادّة 47 : يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا الأمر، بالعقوبات المقررة للجريمة التامة.

المادّة 48 : مع مراعاة أحكام المادة 41 من هذا الأمر، تضاعف العقوبات المنصوص عليها في هذا الأمر في حالة العود.

الفصل السابع

أحكام ختامية

المادّة 49 : تطبق على إفشاء سرّ الدفاع الوطني وإفشاء السرّ الطبي العقوبات المنصوص عليها في قانون العقوبات.

المادّة 50 : تبقى المعلومات والوثائق المصنفة خاضعة لأحكام هذا الأمر إلى حين رفع السرّية عنها من قبل السلطات العمومية.

المادّة 51 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 27 شوّال عام 1442 الموافق 8 يونيو سنة 2021.

عبد المجيد تبون

الملحق رقم 03 :" مرسوم رئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ."

ملحق رقم03

6 ربيع الثاني عام 1443 هـ
11 نوفمبر سنة 2021 م

الجريدة الرسميّة للجمهوريّة الجزائريّة / العدد 86

5

مراسيم تنظيميّة

مرسوم رئاسي رقم 21-439 مؤرّخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إنّ رئيس الجمهورية،

– بناء على الدستور لا سيما المادتان 91-7 و141 (الفقرة الأولى) منه،

– وبمقتضى القانون العضوي رقم 04-11 المؤرخ في 21 رجب عام 1425 الموافق 6 سبتمبر سنة 2004 والمتضمن القانون الأساسي للقضاء،

– وبمقتضى الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدل والمتمم،

– وبمقتضى الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم،

– وبمقتضى الأمر رقم 71-28 المؤرخ في 26 صفر عام 1391 الموافق 22 أبريل سنة 1971 والمتضمن قانون القضاء العسكري، المعدل والمتمم،

– وبمقتضى القانون رقم 90-21 المؤرخ في 18 صفر عام 1411 الموافق 15 غشت سنة 1990 والمتعلق بالمحاسبة العمومية، المعدل والمتمم،

– وبمقتضى الأمر رقم 06-02 المؤرخ في 29 محرم عام 1427 الموافق 28 فبراير سنة 2006 والمتضمن القانون الأساسي العام للمستخدمين العسكريين، المعدل والمتمم،

– وبمقتضى الأمر رقم 06-03 المؤرخ في 19 جمادى الثانية عام 1427 الموافق 15 يوليو سنة 2006 والمتضمن القانون الأساسي العام للوظيفة العمومية،

– وبمقتضى القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– وبمقتضى القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية،

– وبمقتضى الأمر رقم 21-09 المؤرخ في 27 شوال عام 1442 الموافق 8 يونيو سنة 2021 والمتعلق بحماية المعلومات والوثائق الإدارية،

– وبمقتضى المرسوم رقم 74-60 المؤرخ في 27 محرم عام 1394 الموافق 20 فبراير سنة 1974 والمتضمن إنشاء إطار من الموظفين المدنيين الشبيهين بالموظفين العسكريين في وزارة الدفاع الوطني وتحديد قواعد القانون الأساسي المطبق على الشبيهين الدائمين بالعسكريين، المتمم،

– وبمقتضى المرسوم الرئاسي رقم 20-39 المؤرخ في 8 جمادى الثانية عام 1441 الموافق 2 فبراير سنة 2020 والمتعلق بالتعيين في الوظائف المدنية والعسكرية للدولة، المتمم،

– وبمقتضى المرسوم الرئاسي رقم 20-183 المؤرّخ في 21 ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020 والمتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

يرسم ما يأتي :

الفصل الأول
أحكام عامة

المادّة الأولى : يهدف هذا المرسوم إلى إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تدعى في صلب النص "الهيئة".

المادّة 2 : الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى رئيس الجمهورية.

المادّة 3 : يحدد مقر الهيئة بمدينة الجزائر.

ويمكن نقله إلى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي.

المادّة 4 : تمارس الهيئة المهام المنوطة بها، تحت رقابة السلطة القضائية، طبقا لأحكام قانون الإجراءات الجزائية، والقانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وبهذه الصفة، تكلف الهيئة، على الخصوص، ما يأتي :

– تحديد الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ووضعها حيز التنفيذ،

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– ضمان المراقبة الوقائية للاتصالات الإلكترونية، تحت سلطة القاضي المختص، قصد الكشف عن الجرائم المتصلة بالأعمال الإرهابية أو التخريبية أو التي تمس بأمن الدولة.

كما تضمن الهيئة بالتنسيق مع المصالح المختصة لوزارة الدفاع الوطني، المراقبة الإلكترونية عندما يتعلق الأمر بأمن الجيش، وفقا لنفس الشروط المنصوص عليها في التشريع الساري المفعول.

– تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية،

– المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال،

– المساهمة في تحيين المعايير القانونية في مجال اختصاصها،

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، عن طريق جمع المعلومات والتزويد بها وإنجاز الخبرات القضائية،

– تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، وفقا لأحكام المادتين 17 و18 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه.

الفصل الثاني

تشكيلة الهيئة وتنظيمها

المادّة 5 : تتكون الهيئة من مجلس توجيه ومديرية عامة، يُوضَعان تحت سلطة رئيس الجمهورية، ويُقدمان له عرضًا عن نشاطاتهما.

القسم الأول

مجلس التوجيه

المادّة 6 : يتولى الأمين العام لرئاسة الجمهورية رئاسة مجلس التوجيه الذي يتشكل من الأعضاء الآتي ذكرهم :

– الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج،

– الأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية،

– الأمين العام لوزارة العدل،

– الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية،

– قائد الدرك الوطني،

– المدير العام للأمن الداخلي،

– المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي،

– المدير العام للأمن الوطني،

– رئيس مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي،

– ممثل عن رئاسة الجمهورية، يعينه رئيس الجمهورية.

يتولى المدير العام للهيئة أمانة مجلس التوجيه.

المادّة 7 : يكلف مجلس التوجيه على الخصوص، بما يأتي :

– توجيه عمل الهيئة والإشراف عليه ومراقبته،

– دراسة كل مسألة تخضع لمجال اختصاص الهيئة، والبتّ فيها، لا سيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية المنصوص عليها في المادة 4 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه،

– المداولة حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– دراسة مخطط عمل الهيئة والموافقة عليه،

– القيام بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين العمليات الواجب القيام بها والأهداف المنشودة، بدقة،

– اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– دراسة مشروع ميزانية الهيئة والموافقة عليه،

– المداولة حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية والأجنبية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

– دراسة مشروع النظام الداخلي للهيئة والموافقة عليه،

– تقديم كل اقتراح مفيد يتصل بمجال اختصاص الهيئة وإبداء رأيه في كل مسألة تتصل بمهامها،

– دراسة التقرير السنوي لنشاطات الهيئة والموافقة عليه.

المادّة 8 : يجتمع مجلس التوجيه في دورة عادية مرة واحدة في السنة، بناء على استدعاء من رئيسه.

ويمكنه أن يجتمع في دورة غير عادية، كلّما كان ذلك ضروريا، بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

يعد مجلس التوجيه تقريرا بعد كل دورة.

القسم الثاني
المديرية العامة

المادّة 9 : يدير المديرية العامة مدير عام يعيّن بموجب مرسوم رئاسي، وتنهى مهامه حسب الأشكال نفسها.

تعد وظيفة المدير العام وظيفة عليا في الدولة.

المادّة 10 : يسهر المدير العام على حسن سير الهيئة، ويتولى في هذا المجال :

– اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والسهر على تنفيذها،

– إعداد مشروع ميزانية الهيئة،

– اقتراح مخطط عمل الهيئة والسهر على تنفيذه،

– تنشيط أعمال هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها،

– تحضير اجتماعات مجلس توجيه الهيئة،

– تمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية،

– تمثيل الهيئة لدى القضاء وفي جميع أعمال الحياة المدنية،

– ممارسة السلطة السلّمية على مستخدمي الهيئة،

– السهر على احترام قواعد حماية السرّ المهني في الهيئة،

– السهر على القيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين المعنيين في الهيئة،

– إعداد التقرير السنوي لنشاطات الهيئة، ورفعه إلى رئيس الجمهورية،

– إعداد التقارير الدورية لنشاطات الهيئة ورفعها إلى رئيس مجلس التوجيه،

– ضمان التسيير الإداري والمالي للهيئة،

– إعداد مشروع النظام الداخلي للهيئة،

– المساهمة في تحيين المعايير القانونية في مجال اختصاصه،

– التوظيف على مستوى هياكل المديرية العامة،

– تعيين المستخدمين الذين لم تتحدد كيفيات أخرى لتعيينهم.

يخطر المدير العام للهيئة رئيس الجمهورية، فورا، عن كل حادثة من شأنها المساس بأمن الدولة أو تلك المرتبطة بالأعمال الإرهابية أو التخريبية، كما يخطر أيضا رئيس أركان الجيش الوطني الشعبي عندما يتعلق الأمر بمسائل تخص الدفاع الوطني.

المادّة 11 : تضم المديرية العامة :

– مديرية المراقبة الوقائية واليقظة الإلكترونية،

– مديرية الإدارة والوسائل،

– مصلحة للدراسات والتلخيص،

– مصلحة للتعاون واليقظة التكنولوجية،

– ملحقات جهوية،

المادّة 12 : تعدّ كل من وظائف مدير المراقبة الوقائية واليقظة الإلكترونية، ومدير الإدارة والوسائل، ونواب المديرين، ورئيس مصلحة الدراسات والتلخيص، ورئيس مصلحة التعاون واليقظة التكنولوجية، ورؤساء الملحقات الجهوية، وظائف عليا في الدولة.

يتم التعيين في هذه الوظائف بموجب مرسوم رئاسي بناء على اقتراح من المدير العام للهيئة، وتنهى المهام فيها حسب الأشكال نفسها.

المادّة 13 : يحدد التنظيم الداخلي لهياكل الهيئة بموجب قرار من الأمين العام لرئاسة الجمهورية، بناء على اقتراح من المدير العام للهيئة.

الفرع الأول
مديرية المراقبة الوقائية واليقظة الإلكترونية

المادّة 14 : تكلف مديرية المراقبة الوقائية واليقظة الإلكترونية بما يأتي :

– تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول،

– تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم،

– جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وحفظها،

– تزويد السلطات القضائية ومصالح الشرطة القضائية، تلقائيا أو بناء على طلبها، بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

– القيام بالتدقيق والتفتيش في أي مكان أو هيكل أو جهاز يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية، باستثناء تلك التابعة لوزارة الدفاع الوطني،

– تنشيط عمل الملحقات الجهوية تحت إشراف المدير العام،

– تنظيم و/أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والاتصال، وحول المخاطر المتصلة بها،

– تطبيق قواعد الحفاظ على السرّ المهني في نشاطاتها،

– السهر على إنجاز مهام اليقظة الإلكترونية.

المادّة 15 : تضع مديرية المراقبة الوقائية واليقظة الإلكترونية، على مستوى المنشآت القاعدية لمتعاملي ومقدمي خدمات الاتصالات الالكترونية، التجهيزات والوسائل والأجهزة التقنية الضرورية لتنفيذ مهامها طبقا للتشريع الساري المفعول.

يلزم المتعاملون ومقدمو الخدمات بتقديم المساعدة الضرورية لهذه المديرية من أجل ممارسة مهامها.

تمارس هذه المديرية مهامها المرتبطة بالشرطة القضائية طبقا لأحكام قانون الإجراءات الجزائية.

تنظم مديرية المراقبة الوقائية واليقظة الإلكترونية في مديريات فرعية.

الفرع الثاني

مديرية الإدارة والوسائل

المادّة 16 : تكلف مديرية الإدارة والوسائل، على الخصوص، بما يأتي :

– تسيير الموارد البشرية والوسائل المادية والمالية للهيئة،

– الإسناد التمويني والإسناد التقني للهيئة،

– صيانة العتاد والوسائل والمنشآت،

– إعداد احتياجات الهيئة في إطار تحضير تقديرات الميزانية.

تنظم مديرية الإدارة والوسائل في مديريات فرعية.

الفرع الثالث

مصلحة الدراسات والتلخيص

المادّة 17 : تكلف مصلحة الدراسات والتلخيص، على الخصوص، بما يأتي :

– إعداد مشروع مخطط عمل الهيئة بالتشاور مع الهياكل الأخرى للهيئة،

– القيام بتلخيص الوثائق المتعلقة بنشاطات الهيئة،

– القيام بكل دراسة وبحث تتعلق بنشاطات الهيئة،

– إعداد التقارير والحصائل السنوية لنشاطات الهيئة،

– مركزة ومراقبة الإجراءات المتعلقة بالطلبات القضائية، طبقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية،

– حفظ الوثائق والأرشيف.

الفرع الرابع

مصلحة التعاون واليقظة التكنولوجية

المادّة 18 : تكلف مصلحة التعاون واليقظة التكنولوجية، على الخصوص، بما يأتي :

– التعاون مع الشركاء فيما يخص تنفيذ عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– اليقظة الدائمة في متابعة تكنولوجيات الإعلام والاتصال المتعلقة بنشاطات الهيئة.

الفرع الخامس

الملحقات الجهوية

المادّة 19 : تكلف الملحقة الجهوية بتنفيذ عمليات المراقبة الوقائية للاتصالات الالكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول.

يتم وضع الملحقات الجهوية قيد الخدمة والتشغيل من طرف مديرية المراقبة الوقائية واليقظة الإلكترونية.

الفصل الثالث

سير الهيئة

المادّة 20 : لسير الهيئة، يلحق بها :

– قضاة وفقا للشروط والكيفيات المنصوص عليها بموجب التشريع الساري المفعول،

– ضباط وأعوان للشرطة القضائية مؤهلون من المصالح العسكرية للأمن والدرك الوطني والأمن الوطني، الذين يحدد

عددهم بموجب قرارات مشتركة بين وزير الدفاع الوطني والوزير المكلف بالداخلية والأمين العام لرئاسة الجمهورية،

– مستخدمو الدعم التقني والإداري للمصالح العسكرية للأمن المختصة والدرك الوطني والأمن الوطني.

المادّة 21 : يمكن للهيئة أن توظف فئات أخرى من المستخدمين، حسب الحاجة.

المادّة 22 : يؤدي مستخدمو الهيئة الذين يدعون إلى الاطلاع على المعلومات السرّية، اليمين الآتي نصها أمام المجلس القضائي المختص إقليميا، قبل تنصيبهم :

"أقسم بالله العلي العظيم أن أقوم بعملي أحسن قيام، وأن أخلص في تأدية مهنتي، وأن أكتم الأسرار والمعلومات أيّا كانت التي اطلع عليها أثناء قيامي بعملي أو بمناسبته، وأن أسلك في كل الظروف سلوكا شريفا".

المادّة 23 : يلزم مستخدمو الهيئة بالسرّ المهني وبواجب التحفظ.

ويلزم مستخدمو مقدمي الخدمات في علاقاتهم مع الهيئة، أيضا، بواجب التحفظ.

ويخضع المستخدمون المدعوون إلى الاطلاع على معلومات سرّية، إلى إجراءات التأهيل.

المادّة 24 : في إطار التعاون، يمكن للهيئة أن تطلب من أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة ضروريتين لإنجاز المهام المسندة إليها.

المادّة 25 : قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو التي تمس بأمن الدولة ومكافحتها، تكلف الهيئة حصريا، في مجال اختصاصها، بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها داخل منظومة معلوماتية تحت سلطة قاضٍ لدى الهيئة، وفقا للأحكام المنصوص عليها في المادة 4 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه، على أن تخضع إجراءات التفتيش والحجز لأحكام قانون الإجراءات الجزائية.

المادّة 26 : يمكن الهيئة، لتنفيذ عملية مراقبة الاتصالات الإلكترونية، أن تضع وحدة مراقبة واحدة أو أكثر، تزود بالوسائل والتجهيزات التقنية الضرورية.

يتولى الأعوان المؤهلون في الهيئة ووحداتها المكلفة بالمراقبة، لصالح ضباط الشرطة القضائية، الجوانب التقنية للعمليات المنصوص عليها في قانون الإجراءات الجزائية تحت إدارة ومراقبة قاضٍ لدى الهيئة، وبمساعدة ضابط من الشرطة القضائية أو أكثر ينتمي للهيئة.

تمتثل الوحدة في عملها إلى أحكام التشريع الساري المفعول وشروط الرخصة المسلّمة من السلطة القضائية.

وتدوّن أشغالها في محاضر تعد طبقا لأحكام قانون الإجراءات الجزائية.

المادّة 27 : تحفظ المعلومات المستقاة أثناء عمليات المراقبة، خلال حيازتها من طرف الهيئة، وفقا للقواعد المطبقة على حماية المعلومات المصنفة.

المادّة 28 : تسجل الاتصالات الإلكترونية التي تكون موضوع مراقبة، وتحرر وفقا للشروط والأشكال المنصوص عليها في قانون الإجراءات الجزائية.

وفي هذه الحالة، تسلّم التسجيلات والمحررات محل الطلب، إلى السلطات القضائية وإلى مصالح الشرطة القضائية المختصة وتحتفظ السلطات القضائية، دون سواها بهذه المعطيات أثناء المدة القانونية المنصوص عليها في التشريع الساري المفعول.

المادّة 29 : يجب، تحت طائلة العقوبات الجزائية المنصوص عليها في التشريع الساري المفعول، ألاّ تستخدم الاتصالات الإلكترونية والمعلومات والمعطيات التي تستلمها أو تجمعها الهيئة، لأغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وذلك وفقا للأحكام المنصوص عليها في القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه.

المادّة 30 : يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعون للهيئة، أثناء ممارستهم لوظائفهم أو بمناسبتها، طبقا للشروط والكيفيات المنصوص عليها في التشريع الساري المفعول، ولا سيما قانون الإجراءات الجزائية، بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم أنه يحوز و/أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية.

وفي حالة معاينة أفعال يمكن وصفها جزائيا، تخطر الهيئة وكيل الجمهورية المختص للقيام بالمتابعات المحتملة.

لا تشمل أحكام هذه المادة المنشآت التابعة لوزارة الدفاع الوطني.

المادّة 31 : تضمن المديرية العامة للاستعلام التقني الإسناد المتعدد الأشكال للهيئة.

المادّة 32 : يمكن أن تطلب الهيئة مساعدة موظفين مختصين من الوزارات المعنية في مجال تكنولوجيات الإعلام والاتصال، طبقا للشروط والكيفيات المحددة في التنظيم الساري المفعول.

كما يمكنها أن تستعين بأي خبير أو أي شخص يمكن أن يساعدها في أعمالها.

المادّة 33 : لا يمكن أن تستورد أو تقتني أو تحوز أو تستعمل الوسائل والتجهيزات التقنية لمراقبة الاتصالات الإلكترونية إلاّ الهيئة في إطار اختصاصها.

الفصل الرابع

أحكام مالية

المادّة 34 : تسجل ميزانية الهيئة في الميزانية العامة للدولة، وتلحق ضمن ميزانية رئاسة الجمهورية، طبقا للتشريع والتنظيم الساريي المفعول.

ويكون المدير العام هو الآمر بصرف ميزانية الهيئة.

المادّة 35 : تشتمل ميزانية الهيئة على باب للإيرادات وباب للنفقات.

في باب الإيرادات :

– إعانات الدولة،

– المساهمات المتعلقة بالنشاطات المرتبطة بموضوعها.

في باب النفقات :

– نفقات التسيير،

– نفقات التجهيز،

– كل النفقات الأخرى الضرورية لإنجاز هدفها.

المادّة 36 : تمسك محاسبة الهيئة وفق قواعد المحاسبة العمومية.

يتولى مسك المحاسبة عون محاسب يعيّنه أو يعتمده الوزير المكلف بالمالية.

المادّة 37 : يمارس المراقبة المالية للهيئة مراقب مالي يعيّنه الوزير المكلف بالمالية.

الفصل الخامس

أحكام قانونية أساسية

المادّة 38 : يبقى القضاة وضباط وأعوان الشرطة القضائية وكذا المستخدمون التابعون للوزارات المعنية والممارسون وظائفهم في الهيئة، خاضعين للأحكام التشريعية والتنظيمية والقانونية الأساسية المطبقة عليهم.

المادّة 39 : يستفيد مستخدمو الهيئة، طبقا للتشريع الساري المفعول، من حماية الدولة من التهديدات أو الضغوطات أو الإهانات، مهما تكن طبيعتها، التي قد يتعرضون لها بسبب أو بمناسبة قيامهم بمهامهم.

المادّة 40 : تحدد طريقة صرف النظام التعويضي المطبق على مستخدمي الهيئة بموجب نص خاص.

الفصل السادس

أحكام خاصة وختامية

المادّة 41 : تلغى جميع الأحكام المخالفة لهذا المرسوم لا سيما المرسوم الرئاسي رقم 20-183 المؤرّخ في 21 ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020 والمتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المادّة 42 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021.

عبد المجيد تبون

———★———

مرسوم رئاسي رقم 21-440 مؤرّخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يعدّل ويتمّم المرسوم الرئاسي رقم 02-479 المؤرّخ في 27 شوّال عام 1423 الموافق 31 ديسمبر سنة 2002 والمتضمن إنشاء المجلس الوطني للسياحة وتحديد صلاحياته وتنظيمه وعمله.

———

إنّ رئيس الجمهورية،

– بناء على تقرير وزير السياحة والصناعة التقليدية،

– وبناء على الدستور، لا سيما المادتان 91-7 و141 (الفقرة الأولى) منه،

– وبمقتضى المرسوم الرئاسي رقم 02-479 المؤرخ في 27 شوّال عام 1423 الموافق 31 ديسمبر سنة 2002 والمتضمن إنشاء المجلس الوطني للسياحة ويحدد صلاحياته وتنظيمه وعمله،

– وبمقتضى المرسوم الرئاسي رقم 21-275 المؤرخ في 19 ذي القعدة عام 1442 الموافق 30 يونيو سنة 2021 والمتضمن تعيين الوزير الأول،

– وبمقتضى المرسوم الرئاسي رقم 21-281 المؤرخ في 26 ذي القعدة عام 1442 الموافق 7 يوليو سنة 2021 والمتضمن تعيين أعضاء الحكومة،

يرسم ما يأتي :

المادّة الأولى : يعدّل هذا المرسوم ويتمّم بعض أحكام المرسوم الرئاسي رقم 02-479 المؤرخ في 27 شوّال عام 1423 الموافق 31 ديسمبر سنة 2002 والمتضمن إنشاء المجلس الوطني للسياحة، وتحديد صلاحياته وتنظيمه وعمله.

المادّة 2 : تعدل وتتمم أحكام المواد 2 و3 و5 من المرسوم الرئاسي رقم 02-479 المؤرخ في 27 شوّال عام 1423 الموافق 31 ديسمبر سنة 2002 والمذكور أعلاه، وتحرر كما يأتي :

الملحق رقم 04: " أحكام قضائية صادرة عن القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال."

22/05 2022 15:37 FAX 0001/0004

نسخة عادية

الجمهورية الجزائرية الديمقراطية الشعبية

باسم الشعب الجزائري

حكم

مجلس قضاء: الجزائر
القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال
قسم الجنح

رقم الجدول: 22/00003
رقم الفهرس: 22/00009
تاريخ الحكم: 22/03/23

تحقيق

النيابة ضد /

طبيعة الجرم /
جنحة نشر و ترويج عمدا أخبار كاذبة أو مغرضة بين الجمهور من شأنها المساس بالأمن العمومي أو النظام العام، جنحة الإساءة لرئيس الجمهورية، جنحة إهانة هيئة نظامية، جنحة التحريض على التجمهر غير المسلح.

بالجلسة العلنية المنعقدة بمقر القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

بتاريخ: الثالث و العشرون من شهر مارس سنة
النظر في قضايا الجنح

برئاسة السيد (ة): رئيسا
وبمساعدة السيد(ة): أمين ضبط
وبحضور السيد(ة): وكيل الجمهورية

صدر الحكم الجزائي الآتي بيانه بين الأطراف التالية

السيد وكيل الجمهورية مدعيا باسم الحق العام.

من جهة

ضد /

1): ه
من مواليد: ب: الشريعة
إبن: و (ة)
الساكن :

متهم
معتبر حاضر
غير موقوف

من جهة اخرى.

بيان وقائع الدعوى

- حيث أن المتهم متابع من طرف نيابة الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال لارتكابه بتاريخ 2020/11/01 أي منذ زمن لم يمض عليه أمد التقادم بعد بدائرة اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مجلسه القضائي بجنحة إهانة هيئة نظامية و جنحة الإساءة إلى رئيس الجمهورية و جنحة نشر و ترويج عمدا أخبار كاذبة و مغرضة بين الجمهور من شأنها المساس بالأمن العمومي أو النظام العام و جنحة التحريض على التجمهر غير المسلح الأفعال المنصوص والمعاقب عليها بالمواد 100 و 144 مكرر و 146 و 196 مكرر من قانون العقوبات.

- و حيث أن المتهم المذكور أعلاه أحيل على القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال بموجب أمر إحالة صادر عن قاضي التحقيق بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال بتاريخ 2022/02/16 تحت رقم22/0003.

من حيث الوقائع

يستخلص من الملف الوقائع الآتية:
انه بتاريخ 2020/11/01 رصدت مصالح فرقة مكافحة الجريمة المعلوماتية بأمن ولاية تبسة

رقم الجدول: 22/00003
رقم الفهرس: 22/00009

22/05 2022 15:13 FAX

0001/0009

تطوير مسيرته الفنية ، غير انه رفض طلبه رفضا قاطعا كونه محل شكوك من قبل اغلب ناشطين الحراك الشعبي بولاية تبسة .

عن التفتيش الالكتروني:

ـ بناء على التفتيش الالكتروني للهاتف النقال من نوع Condor Plume H1 ازرق اللون، يحمل رقمي IMEI الأول 352635091382363 ، والثاني 352635091413275 ، مثبت به شريحتين هاتفيتين الأولى جيزي تحمل الرقم ، والثانية اوريدو ، ملك المشتبه به ، وكذا جميع الأنظمة المعلوماتية المثبتة به، ثانيا الصفحة الالكترونية الحاملة للاسم المستعار ، التي تعود ملكيتها المشتبه به ، ثالثا الصفحة الالكترونية الثانية الحاملة للاسم المستعار/ التي تعود ملكيتها المشتبه به (الصفحة الاحتياطية) رابعا الحساب الالكتروني الحامل للاسم المستعار/ لمسيره المشتبه به ، خامسا وحدة مركزية خاصة بجهاز الإعلام الآلي من نوع NGC رمادية اللون ، ملك المشتبه به سادسا جهاز كمبيوتر محمول من نوع Thomson ابيض اللون يحمل الرقم التسلسلي QR0905493803056 ، عثر عليه بغرفة نوم والد المشتبه به ، تعود ملكيته ملك المشتبه به من اجل استرجاع كل ما يفيد التحقيق في القضية ، بنفس التاريخ تم إخضاع الأجهزة المعلوماتية الحاملة للمواصفات السالفة الذكر وكذا الأنظمة المعلوماتية المثبتة أين كانت نتائج التفتيش ايجابية تفاصيلها كانت كما يلي :

- الحساب الالكتروني الحامل للاسم المستعار/ كما يلي:
- استرجاع محادثة بين المدعو من الحساب الالكتروني محل التفتيش والحامل للاسم المستعار و المدعو مسير وصاحب الصفحة الالكترونية المسماة المعروفة بنشاطها التحريضي ومنشوراتها المناوئة للسلطة والنظام في البلاد و المسيئة لمؤسسات الدولة ، كذلك الإساءة للمؤسسة العسكرية و جهاز الشرطة يدعي من خلالها انه تم استدعائهم للمثول أمام الجهة الأمنية دون تحديد نوعها ،طالبا من المدعو وضع منشورات مسيئة للأجهزة الامنية في حال توقيفه من خلال العبارة التالية "

- استرجاع محادثة بين المدعو والمسمى تضمنت قيام هذا الأخير بإرسال فيديو مفبرك بعنوان بمناسبة ال 12/12 نقدم له هذه الأغنية ، كل عام و أنت منتن يسيء من خلاله للسيد رئيس الجمهورية بعبارات على شكل أغنية راب طالبا منه نشرها عبر صفحته الالكترونية المسماة / ، من خلال العبارة التالية // حطها عندك مع عنوان مليح خويا مثلا المغني الوحيد لي قصف النظام اي حاجة قوية خويا.
- رصد محادثة الكترونية المدعو و المدعو تضمنت إرسال هذا الأخير لصور شخصية له بها كتابة تضمنت كلمة
- استرجاع محادثة الكترونية بين السالفي الذكر تضمنت عبارات// خويا لست وحدك كلنا معك واصل يا بطل ، تعيين سفيرا لإحباط معنويات
- رصد محادثات بين المدعو و صاحب الصفحة الالكترونية المجرمة ، تضمن طلب المدعو من صاحب الصفحة المجرمة نشر صور لأفراد الشرطة بالزي الرسمي برتبة عميد اول لا تظهر ملامحه مرفقة بقسيمة استدعاء تابعة لأحد مراكز الشرطة ، مكتوب عليها عبارة يبتزو فيها.
- معاينة و جود محادثة بين صاحب الحساب المجرم المسمى تضمنت صورا مركبة لعدد من إطارات الجيش مدمجة مع صور المسمى تضمنت عبارات // بقايا القايد ما بين السجن و المقبرة ، //تبينيلة // ، // - يهين المخابرات بحبلة.
- استرجاع محادثة بين من الحساب الالكتروني محل التفتيش والحامل للاسم المستعار/ ، و المدعو مسير وصاحب الصفحتين

رقم الجدول: 22/00003
رقم الفهرس: 22/00009

22/05 2022 15:15 FAX

0005/0009

ذلك.
و حيث أن المتهم صرح بالجلسة أنه يعترف بنشر بعض التعاليق فقط و أكد أن الصفحة التي كان ينشر فيها بها عدة مسيرين لها و كان كل واحد منهم باستطاعته نشر الصور و التعاليق مؤكدا أنه غير مسؤول عنها، مضيفا أنه كان يترك صفحته على موقع التواصل الاجتماعي "فيسبوك" مفتوحة و يحتمل بأنها استعملت من طرف أشخاص لنشر الصور و التعاليق التي لا يتذكر بأنه قام بنشرها، كما أكد بأنه فعلا كان يطلع على صفحات كل من الملقب " . " و " " و أنه فعلا اتصل بهما لأجل التعارف و تبادل الأفكار و لم يشاركهما في نشر الأخبار، مضيفا أنه ليست له أي نية في المساس بالنظام العام أو الاهانة.
أحيلت الكلمة للسيد وكيل الجمهورية الذي التمس ضد المتهم عقوبة ثلاثة (03) سنوات حبس نافذ و 200 ألف دينار غرامة نافذة مع مصادرة المحجوزات.
و حيث أن الكلمة الأخيرة كانت للمتهم عملا بأحكام المادة 353 من قانون الإجراءات الجزائية.
وحيث أن القضية تم وضعها في المداولة بجلسة 2022/03/23 ليتم النطق فيها بالحكم الآتي بيانه:

وعليه فإن المحكمة

- بعد الإطلاع على قانون الإجراءات الجزائية المعدل و المتمم.
- بعد الإطلاع على المواد 100 و146 و 144 مكرر و 196 من قانون العقوبات.
- بعد الإطلاع على الملف و الوثائق المرفقة به.
- بعد استجواب المتهم.
- بعد الاستماع إلى التماسات النيابة.
- بعد إعطاء الكلمة الأخيرة للمتهم.
- بعد النظر طبقا للقانون .

من حيث الاختصاص
- حيث أن القطب الجزائي الوطني المتخصص في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال يختص في الجرائم التي ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام و الاتصال كما نصت عليه المادة 211 مكرر 22 من قانون الإجراءات الجزائية المعدل و المتمم، كما يختص حصريا إذا تعلق الأمر بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال الماسة بأمن الدولة و الدفاع الوطني و جرائم ترويج أخبار كاذبة بين الجمهور من شأنها المساس بالسكينة العامة أو استقرار المجتمع و جرائم نشر و ترويج أنباء مغرضة تمس بالنظام و الأمن العموميين ذات الطابع المنظم و العابر للحدود الوطنية و جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات و المؤسسات العمومية و جرائم الاتجار بالأشخاص و بالأعضاء البشرية أو تهريب المهاجرين و جرائم التمييز و خطاب الكراهية حسب المادة 211 مكرر 24 من نفس القانون.
- حيث أن الوقائع المعروضة في قضية الحال، تم ارتكابها بواسطة هاتف ذكي يعالج المعطيات آليا من نوع "كوندور' تم الولوج به إلى الحساب الأكتروني على موقعي التواصل الاجتماعي (face book) و (you tube) و تطبيق (Messenger) تحت الاسم المستعار " "، مما يجعلها من اختصاص محكمة الحال و عليه وجب الفصل فيها طبقا للقانون.
من حيث الدعوى العمومية.
بخصوص جنحة إهانة هيئة نظامية:
- حيث أنه تبين للمحكمة بعد الإطلاع على الوثائق المرفقة بالملف و المناقشات التي دارت بالجلسة بأن جنحة إهانة هيئة نظامية الفعل المنصوص و المعاقب عليه بالمادتين 144 و 146 من قانون العقوبات ثابتة في حق المتهم و أن تقدير المحكمة في ذلك أساسه ما يلي:
من حيث الركن المادي:
1- نشره لمنشورات على شبكة التواصل الاجتماعي " Facebook " على الصفحة التابعة لحسابه المفتوح لدى الشبكة تحت الاسم المستعار " " يحمل عبارات تمس

رقم الجدول: 22/00003
رقم الفهرس: 22/00009

22/05 2022 15:41 FAX 0001

نسخة عادية

الجمهورية الجزائرية الديمقراطية الشعبية

باسم الشعب الجزائري

حكم

مجلس قضاء: الجزائر
القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال
قسم الجنح

رقم الجدول: 21/00004
رقم الفهرس: 22/00007
تاريخ الحكم: 22/03/16

تحقيق

بالجلسة العلنية المنعقدة بمقر القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال
بتاريخ: السادس عشر من شهر مارس سنة
النظر في قضايا الجنح
برئاسة السيد (ة): رئيسا
وبمساعدة السيد(ة): أمين ضبط
وبحضور السيد(ة): وكيل الجمهورية

النيابة ضد /

صدر الحكم الجزائي الآتي بياته بين الأطراف التالية
السيد وكيل الجمهورية_ مدعيا باسم الحق العام.
من جهة

طبيعة الجرم /

جنحة إهانة هيئة نظامية، جنحة الإساءة لرئيس الجمهورية، جنحة النشر و الترويج العمد لأخبار كاذبة و مغرضة بين الجمهور من شأنها المساس بالأمن و النظام العمومي، جنحة التحريض على التجمهر غير المسلح.

ضد /

1):. متهم معتبر حاضر
من مواليد: / / بـ: وهران
إبن: و متزوج (ة)
الساكن :
بمساعدة الأستاذ(ة):

من جهة اخرى

بيان وقائع الدعوى

- حيث أن المتهمة متابعة من طرف نيابة الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال لارتكابها بتاريخ 11 أوت 2021 أي منذ زمن لم يمض عليه أمد التقادم بعد بدائرة اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مجلسه القضائي جنحة إهانة هيئة نظامية و جنحة الإساءة لرئيس الجمهورية و جنحة النشر و الترويج العمد لأخبار كاذبة و مغرضة بين الجمهور من شأنها المساس بالنظام و الأمن العمومي و جنحة التحريض المباشر على التجمهر غير المسلح و الأفعال المنصوص و المعاقب عليها بالمواد 100 فقرة 01 و 144 مكرر و 146 و 196 مكرر من قانون العقوبات.
- و حيث أن المتهمة المذكور أعلاه أحيلت على القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال بموجب أمر إحالة صادر عن قاضي التحقيق بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال بتاريخ 2021/11/21 تحت رقم21/0001.
من حيث الوقائع

يستخلص من الملف الوقائع الآتية:

22/05 2022 15:41 FAX 0002

في إطار مهام اليقظة و الترصد للناشرين للأخبار المغرضة و المسيئة لمؤسسات الدولة و للوحدة الوطنية و النظام العام على مستوى مواقع التواصل الاجتماعي، رصدت المصلحة المركزية لمكافحة الجرائم المعلوماتية للأمن الوطني بتاريخ 11 أوت 2021 صفحة تحمل اسم " " يقوم مسيرها بنشر منشورات تحريضية وإهانة لرئيس الجمهورية وهيئات نظامية.

التحريات الأولية مكنت من تحديد أحد مسيري هذه الصفحة وهو صاحب الحساب المعرف بـ(والرقم الهاتفي يتعلق الأمر بالمشتبه فيها المقيمة بمدينة سطيف، وبعد معاينة المناشير التي تم نشرها عبر صفحة الفايسبوك للمسماة وكذا المناشير التي قامت المشتبه فيها ببثها تبين وجود مناشير تسيء لرئيس الجمهورية و مسيئة لهيئات نظامية (الأمن الوطني و المؤسسة العسكرية) و نشر مناشير تحرض على التجمهر غير المسلح.

ـ مواصلة للتحريات التي باشرها عناصر الضبطية القضائية، تم سماع المشتبه فيها التي صرحت أمامهم أنها صاحبة الحسابين على موقع التواصل الاجتماعي فيسبوك عن طريق الاسمين المستعارين " " و" " التي قامت بإنشائهما عن طريق هاتفها النقال باستعمال الرقم الهاتفي للمتعامل "جيزي"، و أنها تستغلهما عن طريق شبكة الإنترنيت الخاصة بالبيت العائلي، مؤكدة أنها قامت بمشاركة المنشورات عبر حسابها الإلكتروني بسبب الأوضاع الاجتماعية التي يعيشها الشعب الجزائري وبهدف تحسينها للأفضل دون المساس بمؤسسات الدولة.

عن التفتيش الالكتروني:

بموجب إذن بالتفتيش الالكتروني صادر عن وكيل الجمهورية لدى محكمة سطيف بتاريخ 2021/09/21 تحت رقم 21/028724 تم ضبط و حجز الهاتف النقال الخاص بالمشتبه فيها من نوع "Samsung Galaxie J2 Pro"، مزود بشريحة هاتفية للمتعامل جيزي الحاملة للرقم الهاتفي:

كما باشر عناصر الضبطية القضائية عملية تفتيش الكتروني للمنظومة و الحسابات الإلكترونية الخاصة بالمسماة ، أين كانت النتائج على النحو التالي:

1ـ بالنسبة لحساب الفايسبوك تحت تسمية " " :

ـ وجود تطبيقة فايسبوك ومفتوح به حساب باسم " " أين تم نشر عديد من مناشير مغلوطة من شأنها المساس بالنظام والأمن العموميين و إهانة لهيئات نظامية على الصفحة التي تسيرها المشتبه بها تحت تسمية " " .

2- بالنسبة لحساب الفايسبوك تحت تسمية " ":

1- حساب الثاني على نفس الموقع تحت الاسم المستعار " " أين تمت معاينة مناشير تسيء لرئيس الجمهورية.

ـ بعد الانتهاء من عملية التفتيش الإلكتروني تم توثيقها بواسطة محضر معاينة مرفق بملف الإجراءات.

عن التحقيق القضائي

بموجب طلب افتتاحي لإجراء التحقيق صادر عن وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال بتاريخ 2021/10/18 تم متابعة المتهمة بجنحة إهانة هيئة نظامية و جنحة الإساءة لرئيس الجمهورية و جنحة النشر و الترويج العمد لأخبار كاذبة و مغرضة بين الجمهور من شأنها المساس بالنظام و الأمن العمومي و جنحة التحريض المباشر على التجمهر غير المسلح و الأفعال المنصوص و المعاقب عليها بالمواد 100 فقرة 01 و 144 مكرر و 146 و 196 مكرر من قانون العقوبات.

ـ بتاريخ 2021/10/20 حرر قاضي التحقيق محضر ضبط أدلة الإقناع المتمثلة في جهاز هاتف نقال من نوع "Samsung Galaxie J2 Pro"، خاص بالمتهمة.

- بتاريخ 2021/10/20 أصدر قاضي التحقيق أمر بحجز أدلة الإقناع المكورة بمحضر الضبط تحت رقم 21/0001.

ـ بتاريخ 2021/11/09 تم سماع المتهمة عند الحضور الأول أين أنكرت الوقائع

رقم الجدول: 21/00004
رقم الفهرس: 22/00007

صفحة 2 من7

22/05 2022 15:41 FAX 0003

المنسوبة إليها مؤكدة أن كل المنشورات التي قامت بنشرها عبر حسابها في شبكة الإنترنت بموقع التواصل الاجتماعي الفايسبوك كانت بدون أية نية إجرامية، مضيفة أن سبب قيامها بنشر تلك المنشورات هو الوصول إلى اكبر عدد ممكن من المشاركين بصفحتها، لتصبح بذلك معروفة كي تتمكن من مزاولة نشاطها المتمثل في الخياطة، كما أكدت أنها تملك حسابين الأول باسم والثاني باسم مرتبطين برقمها الهاتفي رقم

المركب بهاتفها النقال من نوع قلاكسي سامسونغ، و في الأخير أكدت أنه في بعض الأحيان يستعمله أولادها للاتصال بشبكة الانترنت و بعد غلق المحضر أمر قاضي التحقيق بوضع المتهمة تحت نظام الرقابة القضائية قصد ضمان مثولها أمام العدالة بالتوقيع أسبوعيا لدى المصلحة الولائية للشرطة القضائية بأمن ولاية

- بتاريخ / / تم استجواب المتهمة في الموضوع فصرحت أمام قاضي التحقيق بأنها تقرت بنشرها كل المناشير المبينة في محضر المعاينة المعد من قبل عناصر الضبطية القضائية عبر صفحتها في شبكة فايسبوك وكذا عبر صفحتها الثانية بنفس الشبكة المسماة مؤكدة أنها كانت تجهل بأن كل ما قامت به من نشر مناشير تحتوي على أخبار كاذبة و تسيء لرئيس الجمهورية و تهين هيئات نظامية و تحرض على التجمهر غير المسلح يعاقب عليها القانون.

بعد انتهاء التحقيق أصدر قاضي التحقيق بتاريخ / / أمر بإحالة المتهمة على المحكمة لتتم محاكمتها على الأفعال المنسوبة إليها وفقا للقانون.

من حيث المحاكمة

قد جدولت النيابة القضية لجلسة / / أين تمت مناقشتها بجلسة / / كما يلي:

- صرحت المتهمة عند استجوابها بالجلسة أنها تعترف بنشرها المنشورات على حساب موقع التواصل الاجتماعي "فيسبوك" تحت الاسمين المستعارين " و " محل محضر المعاينة إلا أنها لم تقصد إهانة الهيئات النظامية أو المساس بالنظام العام و لا برئيس الجمهورية و إنما الهدف كان للحصول على العدد الكبير من المشاركين في الصفحة.

- أحيلت الكلمة للسيد وكيل الجمهورية الذي التمس ضد المتهمة عقوبة سنة حبس نافذ و 100 ألف دينار غرامة نافذة مع مصادرة المحجوزات.

- أحيلت الكلمة لدفاع المتهمة ممثلا من طرف الأستاذة

اللتان ترفعتا أمام المحكمة و جاء في مسرح مرافعتهما أن موكلتهما لم تقصد الإهانة و لا المساس برئيس الجمهورية و لا التحريض على التجمهر غير المسلح، كما أضافت الأستاذة بأن موكلتها ارتكبت الوقائع خلال سنة أي قبل صدور القانون رقم 06/20 المستحدث لجنحة النشر و الترويج العمد لأخبار كاذبة و مغرضة بين الجمهور من شأنها المساس بالنظام و الأمن العمومي و التمستا إفادة موكلتهما بالبراءة لانعدام القصد الجنائي.

حيث أن الكلمة الأخيرة كانت للمتهمة عملا بأحكام المادة 353 من قانون الإجراءات الجزائية التي تمسكت بما التمسه الدفاع.

وحيث أن القضية تم وضعها في المداولة بجلسة / / ليتم النطق فيها بالحكم الآتي بيانه:

وعليه فإن المحكمة

- بعد الإطلاع على قانون الإجراءات الجزائية المعدل و المتمم.
- بعد الإطلاع على المواد 100 و 144 مكرر 1 و 196 146من قانون العقوبات.
- بعد الإطلاع على الملف و الوثائق المرفقة به.
- بعد الاستماع إلى التماسات السيد وكيل الجمهورية.
- - بعد الاستماع إلى دفاع المتهمة.
- بعد إعطاء الكلمة الأخيرة للمتهمة و دفاعها.

رقم الجدول: 21/00004
رقم الفهرس: 22/00007

صفحة 3 من 7

- بعد النظر طبقا للقانون .
من حيث الاختصاص
- حيث أن القطب الجزائي الوطني المتخصص في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال يختص في الجرائم التي ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام و الاتصال كما نصت عليه المادة 211 مكرر 22 من قانون الإجراءات الجزائية المعدل و المتمم، كما يختص حصريا إذا تعلق الأمر بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال الماسة بأمن الدولة و الدفاع الوطني و جرائم ترويج أخبار كاذبة بين الجمهور من شأنها المساس بالسكينة العامة أو استقرار المجتمع و جرائم نشر و ترويج أنباء مغرضة تمس بالنظام و الأمن العموميين ذات الطابع المنظم و العابر للحدود الوطنية و جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات و المؤسسات العمومية و جرائم الاتجار بالأشخاص و بالأعضاء البشرية أو تهريب المهاجرين و جرائم التمييز و خطاب الكراهية حسب المادة 211 مكرر 24 من نفس القانون.
- حيث أن الوقائع المعروضة في قضية الحال، تم ارتكابها بواسطة هاتف نقال ذكي ملك المتهمة من نـوع Samsung Galaxie J2 Pro"، مزود بشريحة هاتفية للمتعامل جيزي الحاملة للرقم الهاتفي: و تم إنشاء حسابات الكترونية على مواقع التواصل الاجتماعي (face book) تحت الاسم المستعار " و " " مما يجعلها من اختصاص محكمة الحال و عليه وجب الفصل فيها طبقا للقانون.
من حيث الدعوى العمومية.
بخصوص جنحة إهانة هيئة نظامية:
- حيث أنه تبين للمحكمة بعد الإطلاع على الوثائق المرفقة بالملف و المناقشات التي دارت بالجلسة بأن جنحة إهانة هيئة نظامية الفعل المنصوص و المعاقب عليه بالمادة 144 مكرر و 146 من قانون العقوبات ثابتة في حق المتهمة و أن تقدير المحكمة في ذلك أساسا ما يلي:
من حيث الركن المادي:
1- وضعها منشورات على شبكة التواصل الاجتماعي " Facebook " على الصفحة التابعة لحسابها المفتوح لدى الشبكة تحت الاسم المستعار " " و " " بتاريخ كتابات تمس بمؤسسات الدولة منها عبارة "الوزير الأول الجديد كان في مناصب حساسة في بنك الجزائر لما كانت العصابة تنهب المال العام إلى الخارج و لم يحرك ساكنا و عبارات "هؤلاء البلطجيين اقتحموا اليوم منازل النشطاء و لما ما لقاوهمش روحوا أمهاتهم" مرفقة بصور لأفراد جهاز الأمن الوطني و صور لأفراد الأمن الوطني تحمل عبارة "الجزائر ؟؟؟" و مقارنتها بصورة لأفراد الجيش الصهيوني تحمل عبارة "فلسطين المحتلة" و صورة لفرد من أفراد الجيش الوطني الشعبي بها عبارة "لا أمن و لا جيش و لا جاهزية عسكرية" و صور بإطارات في الجيش الوطني الشعبي تنعتهم بالفاسدين.
من حيث الركن المعنوي:
1- أن المنشورات المرفقة بالعبارات التي قامت المتهمة بنشرها على حساباتها في شبكة التواصل الاجتماعي تحمل شعارات و عبارات مهينة لرئيس الحكومة و لمؤسسة الجيش الوطني الشعبي و لجهاز الأمن الوطني.
2- أن إرادة المتمة ذهبت إلى إهانة هيئات نظامية و رموز الدولة، بما يشكل إهانة لهيئات نظامية.
3- أن المتهمة ارتكبت الأفعال المنسوبة إليها بإرادتها الحرة بدون تدخل أي عامل خارج عنها أرغمها على ذلك مع علمها بأنها أفعال مجرمة و يعاقب عليها القانون.
من حيث الركن الشرعي:
- أن الأفعال التي ارتكبتها المتهمة تشكل العناصر المادية و المعنوية لجنحة اهانة هيئة الأفعال المنصوص و المعاقب عليها وفقا لأحكام المادتين 144 مكرر و 146 من قانون

قائمة المصادر والمراجع

قائمة المصادر و المراجع

أولا- المصادر الشرعية

أ- القرآن الكريم

ب- السنة النبوية

ثانيا – المصادر القانونية

أ-الدساتير الجزائرية

1- دستور 1963

2- دستور 1976

3- دستور 1989

4- التعديل الدستوري لسنة 2002

5- القانون رقم 08-19 المؤرخ في 15 نوفمبر 2008، يتضمن التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية العدد63 .

7- القانون رقم 16-01 المؤرخ في 06 مارس 2016، يتضمن التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية، العدد 14 .

8- المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية، العدد 82 .

ب- المعاهدات الدولية

1- نصوص اتفاقية بودابست 2001، الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي منشورة على الموقع الرسمي للمجلس الأوروبي على الرابط التالي:

https://rm.coe.int/budapest-convention-in- arabic/1680739173

2- معاهدة الويبو بشأن حق المؤلف (لسنة 1996)، منشورة على موقع المنظمة العالمية للملكية الفكرية

Wipolex.wipo.int/ar/text/295156

3- البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن التعاون والكشف عن الأدلة الالكترونية 2022

4- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة في 21-12-2010، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم :14-252المؤرخ في 08-09-2014 ، ج ر ج ج، العدد57 المؤرخة في 28-09-2014.

5- اتفاقية تسليم المجرمين بين الجزائر وفرنسا، حسب المرسوم الرئاسي رقم 21 - 166 المؤرخ في 25-4-2021م الذي يتضمن التصديق على هذه الاتفاقية ، ج.ر.ج.ج، العدد 34 ص 5.

ج-القوانين

1- القانون 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،ح.ر.ج.ح، العدد 47.

2- القانون رقم 01-09 المِؤرخ في 26 يونيو سنة 2001، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر ج ج، العدد 34.

3- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات، ج ر ج ج، العدد 71.

4- القانون رقم 06-23 المؤرخ في 20-12-2006، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، والمتضمن قانون العقوبات، ج ر ج ج، العدد84.

5- القانون رقم 09-01 المؤرخ في 25- 02 - 2009 يعدل ويتمم الأمر رقم 66 - 156 المؤرخ في. 08-06-1966 و المتضمن قانون العقوبات ، ج ر ج ج رقم 15، المؤرخة في 08-03- 2009.

6- القانون رقم 16-02 المؤرخ في 19يونيو2016 المتمم للأمر رقم 66-156، والمتضمن قانون العقوبات، ج ر ج ج رقم 37 المؤرخة في 22يونيو2016 .

7- القانون رقم 20-06 المؤرخ في 28-04-2020 يعدل ويتمم الأمر رقم 66- 156 المؤرخ في 8 يونيو1966 والمتضمن قانون العقوبات، ج ر ج ج العدد 25 الصادر في 29 أبريل 2020 .

8- القانون رقم 04-14 مؤرخ في 27 رمضان1425ه الموافق 10 نوفمبر2004م، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8يونيو1966م، والمتضمن قانون الإجراءات الجزائية ج ر ج ج عدد 71.

9- القانون رقم 06 - 22 المؤرخ في 20 ديسمبر2006 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386ه الموافق في 8 يونيو1966م ، يتضمن قانون الإجراءات الجزائية المعدل والمتمم . الجريدة الرسمية رقم 84 مؤرخة في 24 /12 2006

10- القانون رقم 2000-03 مؤرخ في 5 جمادى الأولى عام1421الموافق 5 غشت سنة 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، **ج ر ج ج العدد 48.**

11- القانون رقم 18- 04 مؤرخ في 24شعبان1439ه، الموافق ل10مايو2018م، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية ،ج.ر.ج.ج،العدد 27 في 13 مايو 2018 .

12- القانون رقم 08-01 المؤرخ في 23 يناير سنة 2008، يتمم القانون رقم 83-11 المؤرخ في 2 يوليو سنة 1983 والمتعلق بالتأمينات الاجتماعية،ج ر ج ج / العدد 04 في 2008/01/27.

13- القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين المؤرخ بتاريخ 1 فبراير2015م، ج.ر.ج.ج/ العدد 06/ 2015/02/10.

14- القانون رقم 18-07 المؤرخ في 25رمضان عام 1439ه الموافق ل10يونيو سنة 2018م، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر ج ج، العدد 34.

15- القانون الاتحادي للإمارات العربية المتحدة رقم 40 لسنة 1992 في شأن حماية المصنفات الفكرية وحقوق المؤلف .

16- القانون الكويتي رقم 64 لسنة 1999 في شأن حقوق الملكية الفكرية.

17- القانون الكويتي رقم 22 لسنة 2016 في شأن حقوق المؤلف والحقوق المجاورة والقانون.

18- القانون رقم 75 لسنة 2019 في شأن حقوق المؤلف الكويتي والحقوق المجاورة.

19- القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات المصري، الجريدة الرسمية العدد32 مكرر (ج) ، السنة الحادية والستون، 3ذي الحجة سنة 1439 الموافق 14 أغسطس سنة 2018 .

20- قانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الالكترونية، صدر بتاريخ 20 سبتمبر 2021، والعمل به اعتبارا من 02 يناير 2022.

21- نظام مكافحة جرائم المعلوماتية السعودي لسنة 1428هـ

22- القانون القطري رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، الجريدة الرسمية العدد 15، تاريخ النشر 02-10-2014 الموافق لـ 1435/12/8

د-الأوامر

1- الأمر رقم 20-01 مؤرخ في 30-7-2020، يعدل ويتمم الأمر رقم 66 - 156 والمتضمن قانون العقوبات، ج ر ج ج، العدد 44، الصادر في 30-7-2020.

2- الأمر رقم 15-02 المؤرخ في 23 يوليو سنة2015 م ، يعدل ويتمم الأمر رقم 66-15المؤرخ في 18 صفر عام 1368 الموافق في 8 يونيو سنة 1966 ، والمتضمن قانون الإجراءات الجزائية، ج ر ج ج العدد 40.

3- أمر رقم 20-04 مؤرخ في 30 غشت سنة 2020 يعدل ويتمم الأمر رقم 66- 155 المؤرخ في 18 صفر عام 1386 الموافق 8يونيو سنة 1966م ، والمتضمن قانون الإجراءات الجزائية. ج ر ج ج العدد 51 سنة 2020.

4- أمر رقم 21-11المؤرخ في 25غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 18صفر 1386الموافق8 يونيو 1966، والمتضمن قانون الإجراءات الجزائية، ج ر ج ج العدد65.

هـ- مراسيم رئاسية

1- المرسوم الرئاسي رقم 341/97، المؤرخ في 13-09-1997، ج ر ج ج، العدد 61 السنة 34 الموافق لـ 14-9-1997م.

2- المرسوم الرئاسي رقم 15-261 مؤرخ في 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج، العدد 53 – 08 أكتوبر 2015.

3- المرسوم الرئاسي رقم **19-172** مؤرخ في 3 شوال عام 1440هـ، الموافق ل6 يونيو سنة 2019 ، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها و كيفيات سيرها، ج.ر.ج.ج، العدد 37.

4- المرسوم الرئاسي رقم20-183 المؤرخ في 13يوليو سنة 2020 ، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

5- المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر سنة 2021 ، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ج ر ج ج، العدد 86.

6- المرسوم الرئاسي رقم 21- 166 مؤرخ في 13 رمضان عام 1442 الموافق ل 25 أبريل سنة 2021 ، يتضمن التصديق على اتفاقية تسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية، وحكومة الجمهورية الفرنسية الموقعة بالجزائر في 27 -01-2019، ج ر ج ج العدد34.

7- المرسوم الرئاسي رقم 21- 166 المؤرخ في 25-4-2021م يتضمن التصديق على اتفاقية تسليم المجرمين بين الجزائر وفرنسا.

و- مراسيم تنفيذية

- المرسوم التنفيذي رقم 06- 348 المؤرخ في 12رمضان1427هـ، الموافق ل 5أكتوبر2006م، يتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية وقضاة التحقيق، ج ر ج ج العدد63 .

قائمة المراجع

أولا- المراجع باللغة العربية

أ-الكتب

1)الكتب العامة

1. إلهام ساعد، التأصيل القانوني لظاهرة الإجرام المنظم في التشريع الدولي والوطني، دار بلقيس، دار البيضاء، الجزائر 2017.
2. بن حيدة محمد، الحق في الحياة الخاصة في إصدار القانون الجزائري، دار هومه، الجزائر، 2018.
3. حسام الدين كمال الاهواني، الحق في احترام الحياة الخاصة الحق في الخصوصية "دراسة مقارنة "، دار النهضة العربية، القاهرة، جمهورية مصر العربية، 1978.
4. طلعت زايد، حق المؤلف وتشريعاته في الوطن العربي، الاتحاد العربي للملكية الفكرية، القاهرة، جمهورية مصر العربية 2006.
5. عبد الرحمن خليفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، دار بلقيس، دار البيضاء ،الجزائر الطبعة الثانية 2016.
6. عبد الله اوهايبية، شرح قانون الإجراءات الجزائية الجزائري " التحري والتحقيق "، دارهومه، الجزالئر2005.
7. علي شملال، المستحدث في قانون الإجراءات الجزائي الجزائري، الكتاب الثاني التحقيق والمحاكمة ،طباعات المسارات العلمية، الدويرة، الجزائر، الطبعة 2022.
8. فاضلي إدريس، حقوق المؤلف والحقوق المجاورة، ديوان المطبوعات الجامعية، الجزائر،2015.
9. فاطمة الزهراء رمضاني، دراسة حول جديد التعديلات الدستورية في الجزائر 2016، النشر الجامعي الجديد، تلمسان، الجزائر 2017.

10.محمد سعيد بوسعدية، الثابت والمتغير في الدساتير الجزائرية، دار البلاغة، الجزائر، الطبعة الأولى 2021.

11.نويري عبد العزيز، الحماية الجزائية للحياة الخاصة في القانونين الجزائري والفرنسي "دراسة مقارنة"، دار هومه، الجزائر الطبعة الثانية 2016.

12.هارون منصر، تكنولوجيا الاتصال الحديثة، المسائل النظرية والتطبيقية، دار الألمعية للنشر والتوزيع، قسنطينة، الجزائر، الطبعة الأولى 2012.

2) الكتب المتخصصة

1. أحمد حسام طه تمام، الجوانب الإجرائية في الجريمة الإرهابية "دراسة مقارنة بالتشريع الفرنسي"، دار النهضة العربية، القاهرة، جمهورية مصر العربية.

2. أحمد عبد الله المراغي ،الجريمة الإلكترونية ودور القانون الجنائي في الحد منها،"دراسة تحليلية تأصيلية مقارنة"، المركز القومي للإصدارات القانونية ،القاهرة ،جمهورية مصر العربية، الطبعة الأولى 2017.

3. إدريس بلمحجوب، تأثير الجريمة الإلكترونية على الائتمان المالي، مطبعة الأمنية ،الرباط، المغرب ، 2012.

4. أسامة أحمد المناعسة ، جلال محمد الزعبي ، جرائم تقنية نظم المعلومات الالكترونية ، دراسة مقارنة ، دار الثقافة للنشر والتوزيع البلد، 2014.

5. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، مكتبة الوفاء القانونية، الإسكندرية، جمهورية مصر العربية، الطبعة الأولى، 2011.

6. أودين سلوم الحايك، مسؤولية مزودي خدمات الإنترنت التقنية، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2009.

7. بهاء المرى، جرائم المحمول والإنترنت، منشأة المعارف ،الإسكندرية، جمهورية مصر العربية 2018.

8. بهاء المرى، شرح قانون مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات، العربية للنشر والتوزيع ،أفنان للطباعة 2019.

9. جمال صالح عبد الحليم، الحماية الجنائية للحق في الخصوصية في مواجهة نظم المعلومات، دار النهضة العربية، القاهرة، جمهورية مصر العربية، الطبعة الأولى، 2018.

10.حازم حسن الجمل، الحماية الجنائية للأمن الإلكتروني، دار الفكر والقانون، المنصورة، جمهورية مصر العربية، 2015.

11.حسام الدين كمال الأهواني، الحق في احترام الحياة الخاصة، الحق في الخصوصية "دراسة مقارنة"، دار النهضة العربية ،القاهرة، جمهورية مصر العربية، 1978.

12.خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية "الإنترنت"،" دراسة مقارنة"، الصفوة، نوفمبر 2014.

13.خالد حسن أحمد لطفي، جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني، "دراسة مقارنة"، دار الفكر الجامعي ،الإسكندرية ،جمهورية مصر العربية ،الطبعة الأولى، 2018.

14.دنيا عبد العزيز فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي، دار النهضة العربية، القاهرة، جمهورية مصر العربية، 2018.

15.راشد محمد المرى، الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر، دار النهضة العربية، القاهرة، جمهورية مصر العربية، الطبعة الأولى 2018.

16.رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية "دراسة تحليلية مقارنة"، المكتب الجامعي الحديث، الإسكندرية، جمهورية مصر العربية،2018.

17.زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى عين مليلة، الجزائر، 2011.

18.ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المطبعة والوراقة الوطنية، مراكش ،المغرب، 2011.

19.طارق عفيفي صادق أحمد، الجرائم الإلكترونية، جرائم الهاتف النقال "دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي"، المركز القومي للإصدارات القانونية، القاهرة جمهورية مصر العربية ،الطبعة الأولى، 2015.

20. عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، جمهورية مصر العربية، 2015.

21. عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية "دراسة قانونية قضائية مقارنة مع أحداث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت"، المركز القومي للإصدارات القانونية، القاهرة، جمهورية مصر العربية، الطبعة الأولى 2012.

22. عبد الفتاح بيومي حجازي، الأحداث والأنترنت، دراسة متعمقة عن أثر الإنترنت في انحراف الأحداث، دار الكتب القانونية، القاهرة، جمهورية مصر العربية 2007.

23. عبد الله سيف الكيتوب، الأحكام الإجرائية لجريمة الاحتيال المعلوماتي، دار النهضة العربية، القاهرة ، جمهورية مصر العربية، 2013.

24. العربي جنان، معالجة المعطيات ذات الطابع الشخصي "الحماية القانونية في التشريع المغربي والمقارن "القانون رقم 08-09" ، المطبعة والوراقة الوطنية، مراكش المغرب، الطبعة الأولى 2010.

25. عصام عبد الفتاح مطر، الحكومة الإلكترونية بين النظرية والتطبيق، دار الجامعة الجديدة، الإسكندرية ،جمهورية مصر العربية2018.

26. عمار عباس الحسني، جرائم الحاسوب والإنترنت (الجرائم المعلوماتية)، منشورات زين الحقوقية ،بيروت، لبنان، الطبعة الأولى 2017.

27. عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية ،النشر الجامعي الجديد، تلمسان، الجزائر، 2021.

28. غسان رباح، حماية الملكية الفكرية والفنية الجديد مع دراسة مقارنة حول جرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الثالثة 2016.

29. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، المنصورة ،جمهورية مصر العربية، 2013.

30. فاضلي إدريس، حقوق المؤلف والحقوق المجاورة، ديوان المطبوعات الجامعية، الجزائر، الطبعة الأولى 2015.

31. محمد الطيب بوطيبي، الجرائم المعلوماتية وفق التشريع المغربي، مطبعة وراقة المقدم، الناظور، المغرب، الطبعة الأولى 2011.

32.محمد حماد مرهج الهيتي، الجريمة المعلوماتية نماذج من تطبيقها، دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونية، القاهرة، جمهورية مصر العربية، 2014.

33.محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، جمهورية مصر العربية، 2011.

34.محمد علي سويلم، مكافحة الجرائم الإلكترونية "دراسة مقارنة بالتشريعات العربية والأجنبية"، دار المطبوعات الجامعية، الإسكندرية، جمهورية مصر العربية، الطبعة الأولى 2019.

35.محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية "دراسة مقارنة"، دار الفكر والقانون للنشر والتوزيع، المنصورة، جمهورية مصر العربية، 2015.

36.محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية " جرائم الكمبيوتر والإنترنت"، المكتبة العصرية للنشر والتوزيع ،المنصورة، جمهورية مصر العربية، الطبعة الأولى، 2010

37.محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الإنترنت، والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت "دراسة مقارنة"، مركز الدراسات العربية للنشر والتوزيع، الجيزة، جمهورية مصر العربية، الطبعة الأولى 2019.

38.محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، " دراسة مقارنة"، دار الفكر والقانون، المنصورة، جمهورية مصر العربية، الطبعة الأولى، 2013.

39.محمود محمد محمود جابر، الجرائم الناشئة عن استخدام الهواتف النقالة (جرائم نظم الاتصالات والمعلومات)، دراسة مقارنة في التشريع المصري والفرنسي والأميركي والاتفاقيات الدولية والإقليمية، المكتب الجامعي الحديث، الإسكندرية، جمهورية مصر العربية، 2018.

40.محمود مدين، الجريمة الإلكترونية وتحديات الأمن القومي، المصرية للنشر والتوزيع، القاهرة، جمهورية مصر العربية، الطبعة الثانية 2019.

41.مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، جمهورية مصر العربية 2000.

42.مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي "دراسة مقارنة"، دار النهضة العربية ،القاهرة، جمهورية مصر العربية، الطبعة الأولى 2015.

43.مصطفى يوسف كافي، جرائم (الفساد –غسل الأموال–السياحة – الإرهاب الالكتروني– المعلوماتية)، مكتبة المجتمع العربي للنشر والتوزيع، عمان، الاردن ،2013.

44.منير محمد الجنبيهي، ممدوح محمد الجنيهي، جرائم الإنترنت والحاسب الآلي و وسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، جمهورية مصر العربية 2006.

45.نائلة عادل، محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية ، بيروت، لبنان، الطبعة الأولى 2005.

46.نهلا عبد القادر المؤمني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008.

47.هلالي عبد اللاه أحمد، جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة ،دار النهضة العربية، القاهرة، جمهورية مصر العربية، 2015.

48.هلالي عبد الله أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، دار النهضة العربية، القاهرة، جمهورية مصر العربية، الطبعة الأولى 2011.

49.هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة، جمهورية مصر العربية، الطبعة الثانية، 2013.

50.هناء مصطفى الخبيري ، الجرائم المعلوماتية وتقنين العملات الرقمية، دار النهضة العربية، القاهرة ، جمهورية مصر العربية 2023.

51.يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، الإسكندرية، جمهورية مصر العربية، 2019.

52.يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، جمهورية مصر العربية، الطبعة الأولى 2011.

53.ياسر سيد فهمي، المواجهة الموضوعية للجرائم الالكترونية، دار النهضة العربية القاهرة، جمهورية مصر العربية2023.

ب–الرسائل والمذكرات.

1) رسائل الدكتوراه

1– آيت بن اعمر غنية، آليات مكافحة جريمة تبييض الأموال على الصعيد الدولي والوطني، مذكرة مقدمة لنيل شهادة الدكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة وهران 2 محمد بن أحمد، وهران، الجزائر، السنة الجامعية 2017– 2018.

2– بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون عام، كلية الحقوق، جامعة الجزائر 01 ، بن يوسف بن خدة ،الجزائر، السنة الجامعية 2017– 2018.

3– بكرار شوش محمد، دور أساليب التحري الخاصة في كشف الجريمة وآثارها على الحقوق والحريات، رسالة لنيل درجة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة وهران–2– محمد بن أحمد، وهران، الجزائر، السنة الجامعية 2017– 2018.

4– بن سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا "الإعلام والاتصال" ،أطروحة مقدمة لنيل شهادة دكتوراه العلوم في العلوم القانونية، تخصص قانون دستوري، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة ،الجزائر، السنة الجامعية 2014– 2015.

5– سمغوني زكرياء، الإجراءات القانونية لإثبات المسؤولية الجنائية عن ارتكاب الجرائم الدولية (نظام روما نموذجا) رسالة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2015 – 2016.

6– عبد الكريم خالد الردايدة، نحو استراتيجية أمنية متقدمة لمواجهة الجرائم المستحدثة "دراسة تطبيقية ميدانية مقارنة على بطاقات الائتمان في الأردن" ،رسالة لنيل درجة الدكتوراه في القانون، جامعة الدول العربية، القاهرة، جمهورية مصر العربية، سنة 2009.

7– محمود أحمد عبد القادر قشطة، التعاون الدولي في مكافحة الجريمة المعلوماتية، رسالة دكتوراه، جامعة الدول العربية، القاهرة ،جمهورية مصر العربية 2015.

8– محمود عبد العزيز أبا زيد، الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، جمهورية مصر العربية 2016.

2) المذكرات:

- سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر باتنة،2012-2013.

ج-المجلات:

1- ادريس بالمحجوب، تأثير الجريمة الالكترونية على الائتمان المالي، مطبعة الأمنية، الرباط، المغرب، العدد السابع،2014.

2- أمال فكري، إشكاليات الإثبات والاختصاص في جرائم تكنلوجيا الإعلام والاتصال العابرة للحدود، مجلة العلوم القانونية والسياسية، منشورات جامعة الشهيد حمة لخضر الوادي- الجزائر، العدد السابع عشر، الجزء الثاني، جانفي 2018.

3- بدر الدين خلاف، التنظيم القانوني للجريمة المعلوماتية في الجزائر، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة ،الجزائر، المجلد السادس، العدد الثاني ، جوان 2021.

4- بطيحي نسمة، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، مجلة الفقه القانوني والسياسي، المجلد 01، العدد 01، 1- 06- 2019.

5- بوضياف اسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، سبتمبر 2018.

6- بوقرة جمال الدين، عنان جمال الدين، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، المجلد 7، العدد1، جوان 2022.

7- بن عمير أمينة - بوحليس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 07/العدد:01(2022)

8- حابت آمال، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال،المجلة الدولية للبحوث القانونية والسياسية، المجلد 05، العدد 03 ، ديسمبر 2021.

9- حليم رامي، إجراءات استخلاص الدليل في الجرائم المعلوماتية، دفاتر البحوث العلمية، المركز الجامعي مرسلي عبد الله، تيبازة، الجزائر، المجاد 9، العدد1، السنة2021.

10- حنان مسكين، واقع مكافحة الجرائم المعلوماتية واتجاهاتها التشريعية في الجزائر، مقال منشور في المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الرابع، العدد الأول، سنة 2020.

11- خرشي إلهام، النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة الأبحاث القانونية والسياسية، المجلد 04، العدد 01، 2022.

12- خليفي محمد، إشكالية الاختصاص القضائي الدولي في مكافحة الجريمة المعلوماتية، مجلة الميزان، العدد الأول، ديسمبر2016.

13- سعيود محمد الطاهر، استقلالية سلطة ضبط البريد والاتصالات الالكترونية في ظل أحكام القانون 04/18، مقال منشور بمجلة الدراسات حول فعلية القاعدة القانونية، المجلد 04، العدد 01: 2020.

14- سي حمدي عبد المؤمن، قيرة سعاد، الجريمة الإلكترونية وآليات التصدي لها في القانون الجزائري ،مجلة البيان للدراسات القانونية والسياسية، المجلد 07/ العدد 01 جوان 2022.

15- شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني ، مجلة جامعة الشارقة، مجلة علمية محكمة للعلوم القانونية ، المجلد17، العدد1، شوال1441هـ/ يونيو2020م.

16- العيند محمد زيد، ليلى عصماني، شروط تسليم المجرمين في النظام القانوني الجزائري، مجلة الاجتهاد القضائي، المجلد 13، العدد01، مارس 2021.

17- فايزة بلال، الشروط الأساسية المتعلقة بالجريمة في نظام تسليم المجرمين، المجلة الجزائرية للقانون والعدالة، مركز البحوث القانونية والقضائية، دار هومه، الجزائر، العدد الأول 2017.

18- فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الالكترونية، مجلة البحوث في الحقوق والعلوم السياسية، 03-06-2022، المجلد 08 ، العدد 01.

19- فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، العدد 33، جوان 2010.

20- قطاف سليمان، بوقرين عبد الحليم، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد 05، العدد 02، 2022.

21- محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكتروني، المجلة الأكاديمية للبحث القانوني، المجلد 14 / العدد 02 -2016

22- وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبيراني :التجربة الماليزية نموذجا، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المقالة 5، المجلد 23، العدد 1- الرقم المسلسل للعدد90، يناير2022.

23- زواني نادية، اتفاقية تربس وتأثيرها على البلدان النامية، مجلة البحوث، جامعة الجزائر، العدد09-الجزء الاول2016.

د- الملتقيات والمؤتمرات

1- حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر العاصمة يوم 29-3-2017م .

2- فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان يومي 24 -25 /03/ 2017

و- الجرائد والصحف

1- جريدة أخبار اليوم، يومية إخبارية جزائرية " الأربعاء 13يناير2021 "، أرقام مرعبة على تفاقم الإجرام الإلكتروني في الجزائر.

2- جريدة الشروق الجزائرية ، "2021/11/23" ، نوارة باشوش " الاجرام الالكتروني...أرقام مرعبة " ، الموقع www.echoroukonline.com

3- arabic.euronews.com

ثانيا –المراجع باللغة الأجنبية

1–David Forest et Gautier Kaufman, Droit de L'informatique, Gualino éditeur , Extenso édition, France,2010.

2–Jan Walden in Chris Reed and John Angle, Computer law Oxford University Press, Fifth edition,2003.

3–Klaus Tiedman , Fraude et autres délits d'affaire commis a l'aide de l'ordinateur électronique, revue D.P.C 1984.

4–Merwe Vander, Computer crimes and other crimes against information technology in south africa R.I.D.P,1993.

5– Philippe Rose- La Criminalité informatique Edite par Presses Universitaires de France Paris- 1988.

6–Robert O, Keohan, After Hegmony , Cooperation And Discord In The World Political Economy, Princeton University Press1984.

7–Toty and Hardcastle , Computer related crime in information technology andthelawU.K.1986.

8– ulrichsieber , Legal Aspects of Computer–Related Crime in the Information Society–COMCRIME–Study– prepared for the European Commission ,version 1.0 of 1st January 1998 .

9– wasik martin , Crime and the Computer(Oxford Monographs on Criminal Law and Justice) , Oxford University press , 1991.

ثالثا– المواقع الالكترونية:

1– www.internetworldstats.com

2– www.echoroukonline.com

3– www.entv.dz

4– www.algriepolice.dz

5- mimirbook.com/ar/07a712c41b6 5-

اتفاقية الجريمة السيبيرانية

6- tringfiscer.com/ar/convention ou cybercrime

اتفاقية الجرائم الالكترونية

7- wipolex.wipo.int/ar//reaties/952

موقع المنظمة العالمية للملكية الفكريةwipo

8- amended-2021/1680a54ed1rm.coe.int/ara-2nd-add-prot

المجلس الأوروبي ، سلسلة معاهدات مجلس أوروبا، البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن تعزيز التعاون والكشف عن الأدلة الالكترونية

9-) موقع وزارة العدل/ لفائدة-المبرمجة-التكوينية- العمليات - www.mjustice.dz/ar/4-1 (

10- -www.mjustice.dz موقع وزارة العدل، بيانات 12 جوان 2022.

11-www.mjustice.dz موقع وزارة العدل، بيانات 19 جوان 2022.

12-www.interpol.int/ar/3/3

13-www.interpol.int/ar/1/1/2021/57

14- www.un.org/ar/ga/73/resolutions.shtml

قرار الجمعية العامة للأمم المتحدة، رقم القرار

A/RES/73/187

15-www.unodc.org/doucuments/cybercrime/S G report /V1908180_APDF.

A/74/130

16- aws.mazon.com/ar/what-is-cloud-computing

17-www.safespace.qa/topic/.شبكة الانترنت الخفية

-18Documents-dds-

ny.un.org/doc/undoc/gen/n19/410/05/pdf/n1941005.pdf

19-www.un.org/ar/ga/74/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n19/410/05/pdf/n1941005.pdf

A/RES/74/29

20- www.un.org/ar/ga/74/resolution.shtml

Document-dds-ny.un.org/doc/undoc/gen/n19/409/98/pdf/n1940998.pdf

A/RES/74/28

21- www.un.org/ar/ga/74/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n19/429/90/pdf/n1942990.pdf

ARES/74/173

22- www.un.org/ar/ga/75/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n20/330/14/pdf/n2033014.pdf

A/RES/75/10

23- www.un.org/ar/ga/75/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n20/371/73/pdf/n2037173.pdf

A/RES/75/176

24-www.un.org/ar/ga/75/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n21/133/49/pdf/n2113349.pdf

A/RES/75/282

25- www.un.org/ar/ga/75/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n21/075/94/pdf/n2105794.pdf

A/RES/75/265

26- www.un.org/ar/ga/76/resolutions.shtml

Documents-dds-ny.un.org/doc/undoc/gen/n21/377/46/pdf/n2137746.pdf

A/RES/76/19

24–www.unodc.org

01ماي2020، مكتب الأمم المتحدة المعني بالمخدرات والجريمة – كوفيد –19، تحليل التهديدات الالكترونية

25– www.interpol.int

التهديدات السيبرية المرتبطة بكوفيد – 19 في العالم

26 - ar.m.wikipedia.org/wil

27- ar.m.wikipedia.org/wiki/...

28 - docdroid.net/UHT3G7I/sfh-khbraaa-almlky...

اتفاقية برن لحماية المصنفات الأدبية والفنية، وثيقة باريس 1971والمعدلة في سبتمبر 1979

الفهرس

المحتوى **الصفحة**

الملخص :

تعتبر الجريمة المعلوماتية من أخطر الجرائم التي شهدها العصر الحديث، و ذلك لمواكبتها حركة التطور في شتى المجالات العلمية و التكنولوجية، وهذه الجريمة هي جريمة عابرة للحدود الوطنية أي أنها جريمة ذات طابع دولي لها انعكاسات سلبية على شتى المستويات.

و قد أدى ظهور هذا النوع من الجرائم إلى خلق تحديات كثيرة في مواجهة النظام القانوني القائم في العديد من الدول و خاصة في مواجهة قانون العقوبات، الأمر الذي أدى إلى البحث فيما إذا كانت النصوص القائمة كافية لمواجهة هذه الجرائم بشتى أنواعها أم أن الأمر يستدعي استحداث قوانين أو نصوص خاصة قادرة على احتوائها و مراعاة طبيعتها و خصوصيتها .

لذلك كان لزاما أن تتصدى الجزائر و معظم دول العالم من خلال القوانين الداخلية و على رأسها قانون العقوبات، و من خلال الاتفاقيات الدولية و الإقليمية و الهيئات الخاصة لمكافحة هذه الظاهرة، وذلك من خلال وضع إستراتيجية شاملة لكبح هذه الجريمة.

الكلمات المفتاحية : الجريمة المعلوماتية، الفضاء الإلكتروني، جرائم عابرة للحدود، الأنظمة المعالجة الآلية للمعطيات، العقوبة ، قانون جزائري .

Résumé :

La cyber criminalité est un des plus dangereux crimes de nos jours . ce genre de crime dépasse les frontières et a beaucoup d'impacts négatifs sur plusieurs domaines . ce genre de crime a poussé le système légal a créer de nouveaux défis , surtout dans le pénal , ce qui a poussé les spécialistes à faire des recherches approfondies sur les textes de loi pour savoir s'ils sont suffisants pour faire face à ce genre de crimes , ou s'il faut créer de novelles lois , ou des textes spécifiques .

C'est pour cela que l'Algérie doit faire face ainsi que les autres pays à travers les lois internes surtout dans le domaine du pénal , et cela en créant une stratégie générale pour freiner ces crimes .

Les mots clés : cyber criminalité, espace internet , crimes transfrontière, systèmes de traitement automatisé de donnés ,punition, loi algérienne ,

Summary:

Cyber crimes Is one of the mostdangerous crimes nowadays . This kind of crimes is beyond frontiérs and has a lot of negative impacts on different fields .

This kind of crime pushed the legal system to create new challenges especially with penal .

Experts made deep researches on law texts to know if they are enough to face this kind of crimes , or if new and more specific law texts are needed to be created .

Therefore, Algeria must face these crimes , also as other countries , with creating a general strategy to brake these crimes .

Key words : cyber crime ,internet network,trans-frontiers crimes ,automated data processing systems , punishment , Algerian law .