وزارة التعليم العالي والبحث العلمي
جامعة المسيلة

كلية/معهد: الحقوق والعلوم السياسية

قسم: الحقوق

الرقم التسلسلي: .....

رقم التسجيل: 171735088097

مكافحة الجريمة الإلكترونية على مستوى التشريعات الوطنية والدولية

مقدمة لنيل شهادة: الماستر LMD في تخصص: قانون جنائي

اعداد الطالب(ة):

سعادة نور الإيمان

تحت إشراف الأستاذ:

مقروف محمد

اما م لجنة المناقشة

الرقم	الاسم واللقب	الرتبة العلمية	الجامعة	الصفة
1	عبدلي حمزة	أستاذ محاضر	المسيلة	رئيسا
2	محمد مقروف	أستاذ محاضر أ	المسيلة	مشرفا ومقررا
3	والي عبد اللطيف	أستاذ محاضر	المسيلة	ممتحنا

السنة الجامعية: 2022/2021

استمارة معلومات

الصورة

المعلومات الشخصية:

الاسم: نور الايمان اللقب: السعادة

اسم الأب: العنصري اسم ولقب الأم: سعادة صليحة

تاريخ الازدياد: 1998/02/07 مكان الازدياد: تيسلمان

رقم الهاتف: 06.75.96.07.69

البريد الالكتروني:

العنوان الشخصي:

الباكالوريا:

معدل: 11.11 شعبة التخصص: ادبي وفلسفة سنة الحصول على شهادة الباكالوريا: 2017

الليسانس:

التخصص: قانون خاص السنة سنة التخرج: 2020/2019

الماستر:

التخصص: قانون جنائي السنة سنة التخرج: 2022/2021

التخصص الثاني في الماستر (إن وجد):

وضعية المهنية:

موظف: ☐ عاطل عن العمل: ☒

في حالة موظف:

الوضع الحالي:

القطاع: عمومي

المؤسسة المستخدمة:

اسم المؤسسة / الشركة:

الرتبة في العمل:

الصفة:

الموظف رقم: الموظف في صفة: النوع العقد:

امضاء الطالب

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة محمد بوضياف بالمسيلة

كلية الحقوق والعلوم السياسية
قسم : قانون جنائي

المرجع: القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 المحدد للقواعد المتعلقة بالوقاية من السرقات العلمية ومكافحتها

تصريح شرفي

خاص بالالتزام بقواعد النزاهة العلمية لانجاز البحث

أنا الممضي أدناه،

السيد(ة) لسعادة نورالايمان

الصفة: طالب، أستاذ باحث، باحث دائم طالبة

الحامل لبطاقة التعريف الوطنية رقم: 119981001000/000/760005

الصادرة بتاريخ 2016/04/24 عن دائرة/ بلدية أولاد دراج

المسجل(ة) بكلية الحقوق والعلوم السياسية قسم : قانون جنائي

والمكلف بانجاز أعمال بحث (مذكرة ماستر، مذكرة ماجيستير، أطروحة دكتوراه) الموسومة بـ :

مكافحة الجريمة الالكترونية عن مضمون التشريعات الوطنية والدولية

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ 09/05/2022

إمضاء المعني

إهداء :

الى من علمتني كيف يكون الصبر طريقا للنجاح، السند والقدوة

الى من رضاها غايتي وطموحي، أعطتني الكثير ولم تنتظر الشكر،

الى باعثة العزم والتصميم والإرادة صاحبة البصمة الصادقة في

حياتي والدتي الغالية أطال الله عمرها.

كلمة شكر وعرفان:

بسم الله الرحمان الرحيم

ربي أوزعني أن أشكر نعمتك التي أنعمت على رعي والدي وأن أعمل صالحا ترضاه وأدخلني برحمتك في عبادك الصالحين. سورة النمل الآية19

كما أتقدم بالشكر والتقدير الى أستاذ المشرف الدكتور مقروف محمد على ما بذله من جهد مخلص فقد كان لتوجيهاته ونصائحه الأثر في أن تكون هذه المذكرة بعمده الصورة.

مقدمة

مقدمة:

إن التقدم العلمي والتكنولوجي الهائل الذي تشهده البشرية في عصر الحديث يلقى بضلاله ونتائجه على كافة جرائمي الحياة، والعلاقات بين الأفراد والدول فقد أصبحت تكنولوجيا المعلومات اليوم سمة من سمات العصر الراهن فالتقدم العلمي والتكنولوجي فتح أفاقا ضخمة أمام تقدم البشرية وتحقيق مستوى أفضل من الحياة، إلا أنه يحمل في نفس الوقت بين طياته مخاطر ضخمة تهدد قيم وحقوق وأمن الأفراد والجماعة فقد أدى الإستعمال الغير المشروع إلى ظهور نوع جديد من الجرائم سميت بالجرائم الإلكترونية أو الجرائم المعلوماتية أو جرائم الأنترنت وهذه المصطلحات كلها تعبر عن مجموعة من الجرائم المرتبطة بالأنظمة الإلكترونية والشبكة المعلوماتية وخصوصا على شبكة الأنترنت.

تعد جرائم الكمبيوتر والأنترنت أو ما يطلق عليه بالجرائم الإلكترونية من الجرائم المعاصرة والعابرة للحدود التي ظهرت مع الإنتشار التكنولوجي كما عرفها البعض بـ: "كل عمل أو إمتناع عن العمل يأتيه الإنسان إضرار بمكونات الحاسوب المادية والمعنوية، وشبكات الإتصال الدولية للمعلومات بإعتبارها من المصالح الوطنية التي توجب الحماية الجنائية لهما.

إن شبكة المعلومات الدولية عبارة عن أداة لربط بين مختلف شعوب العالم وأما الطابع العالمي والمخاطر الإلكترونية، باتت التشريعات الوطنية بمفردها عاجزة عن التصدي لها بحلول منعزلة حيث يطفوا تنازع الإختصاص التشريعي والقضائي ومحاولة التعرف على القانون الواجب تطبيق والقضاء المختص، لذلك ظهرت الحاجة إلى ميلاد قواعد قانونية ذات طابع دولي، ذلك أن دولية العلاقات القانونية تقتضي دولية القواعد القانونية التي تحكمها، ولا يأتي ذلك إلا بوجود إتفاقيات دولية لإقامة نظام قانوني تلتزم به الدول المتعاقدة عند وضع تشريعاتها الوطنية، حتى لا تختلف في أسسها وحلولها بحيث يصعب التقرب إليها.

فبتنامي معدلات الجريمة الإلكترونية وتطور أشكالها وتهديدها المباشر قد دق ناقوس الخطر مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن هذه الجرائم التي إستهدفت الإعتداء على معطيات بدلالتها التقنية الواسعة.

ولعل تلك الإرهاصات والمتناقضات كانت الدافع وراء إجراء تلك الدراسة التي حاولنا من خلالها جمع شتات الموضوع لتنسيق بينهما وتحديد إطارها القانوني والمشكلات القانونية والموضوعية التي تثيرها.

كما أن عملية البحث عن الآليات القانونية لمكافحة الجرائم الإلكترونية تعد مسألة بالغة الأهمية العلمية والعملية منها خاصة مع تنامي دور التعاملات الإلكترونية في حياتنا اليومية مع بروز الحاجة إلى زرع الثقة والطمأنينة في قلوب المتعاملين بالأجهزة الإلكترونية على خلاف أنواعها وما هذه الدراسة المعنونة بـ:

مكافحة الجريمة الإلكترونية على مستوى التشريعات الوطنية والدولية، دراسة مقارنة إلا عينة من تلك البحوث التي تهدف إلى المساهمة ولو بالقليل وإيجاد آليات القانونية فعالة في مكافحة الجرائم الإلكترونية بإختلاف أنواعها وفي سبيل تحقيق ذلك سنحاول الإجابة عن الإشكالية جوهرية تتمثل فيما يلي:

ماهي الآليات القانونية لمكافحة الجريمة الإلكترونية على مستوى التشريعات الوطنية والدولية؟

أسباب إختيار الموضوع:

سهولة إرتكاب الجريمة الإلكترونية التزايد المستمر لجرائم الحاسوب حب الإطلاع والإستكشاف والفهم والبحث في كل ما هو جديد على أساس أن هذه الجريمة مستحدثة ولا تزال خفية المعالم.

- التزايد المستمر لجرائم الإلكترونية.
- الإستغلال المتعسف للحاسوب.
- ديمومة التعامل مع جهاز الكمبيوتر وشبكاته.

الرغبة في معالجة هذا الموضوع الذي تعتبر الشبكة العنكبوتية من أهم وسائل إرتكاب هذه الجريمة.

المنهج المتبع:

إستعملنا في دراستنا هذه عن بعض المناهج الملائمة وطبيعة الموضوع منها المنهج الوصفي بهدف بيان الإطار القانوني للجريمة الإلكترونية والآليات القانونية لمكافحتها على مستوى التشريعات الوطنية والدولية.

ثم إعتمدنا في ذلك على منهج تحليل المحتوى (التحليلي) بقصد تحليل مضمون النصوص القانونية المتضمنة الجرائم الإلكترونية محل الدراسة وإستنباط الأحكام المتعلقة بها.

ثم المنهج المقارن، لمعرفة موقف المشرع الجزائري مقارنة مع تشريعات الأخرى، وذلك لإستفادة من تجارب الدول وفهم النصوص القانونية وتطبيقاتها.

متبعة في ذلك خطة منهجية ثنائية الفصول، حيث خصص الفصل الأول إلى الإطار القانوني للجريمة الإلكترونية؛ أما الفصل الثاني فقد عالج (تطرق) إلى الآليات القانونية لمكافحة الجريمة الإلكترونية على مستوى التشريعات الوطنية والدولية.

المبحث الأول تضمن السياسة الدولية لمكافحة الجريمة الإلكترونية، أما المبحث الثاني تضمن مكافحة الجريمة الإلكترونية على مستوى التشريعات الوطنية.

الفصل

الأول

الفصل الأول: الإطار القانوني للجريمة الإلكترونية

تمهيد:

إذا كانت الثورة المعلوماتية التي شهدها العالم في الألفية الأخيرة قد ساهمت في تسهيل الحياة البشرية وتطورها في جميع المجالات نظرا لما تقدمه من خدمات عديدة، فهي لا تعترف بالحدود الجغرافية والسياسية، إلا أنه لسوء الحظ لم تنج من يد المجرمين خاصة من هؤلاء الذين يمتلكون أداة معرفة إذ أصبح تشكل أداة لإرتكاب جرائمهم أو محلا لها ونظارا لجسامة أخطارها وفداحة خسائرها وسهولة إرتكابها وسرعة إنتشارها، أصبح التعامل مع صور هذه الجرائم موضع إهتمام بالغ.

وبناءا على ما سبق سنقسم الدراسة في هذا الفصل إلى مبحثين، نتناول في المبحث الأول: مفهوم الجريمة الإلكترونية، أما المبحث الثاني: طبيعة القانونية الجريمة الإلكترونية.

المبحث الأول: مفهوم الجريمة الإلكترونية:

إهتم فقهاء القانون الجنائي مع مطلع السبعينات بدراسة جرائم تقنية المعلومات الأولى بإعتبارها ظاهرة فرضت نفسها على المجتمع، لما تنطوي عليه هذه الجرائم من مجموعة من السمات الخاصة حيث كان إرتباطها بالحاسب الآلي مميزا لها عن غيرها من الجرائم الأخرى، ومنذ ذلك التاريخ ونظرا لحداثة الظاهرة نسبينا لكن ناحية والتطور المتلاحق الذي يطرأ عليها من ناحية أخرى، فقد تعددت التعريفات التي أستخدمت للدلالة عليها وسنحاول في هذا المبدأ التعرف على الجريمة الإلكترونية وبيان خصائصها مع ذكر سمات ومميزات مرتكبيها (المجرم الإلكتروني).

المطلب الأول: تعريف الجريمة الإلكترونية:

لقد إختلف الفقهاء حول وضع تعريف موحد للجريمة الإلكترونية، ويعود ذلك للإختلاف حول تعدي نطاق هذه الجريمة، فالبعض من هؤلاء الفقهاء ينظر إليها بمفهوم ضيق، والبعض الآخر ينظر إليها بمفهوم موسع وسنحاول التعرض لهذه التعاريف من خلال الفروع التالية:

الفرع الأول: الإتجاه الضيق في تعريف الجريمة الإلكترونية:

من التعريفات المضيقة لجريمة تكنولوجيا المعلومات الحديثة ما جاء به الفقيه (Merwe) حيث يرى أن هذه الجريمة تتمثل في الفعل غير المشرع الذي يتورط في إرتكابه الحساب الآلي".

يرى الفقيه (tredeman) أن جريمة تكنولوجيا المعلومات الحديثة تشمل "أي جريمة ضد المال مرتبطة بإستخدام المعالجة الآلية للمعلومات".

ويعرف مكتب المحاسبة العامة للولايات المتحدة الأمريكية (GOA) جريمة تكنولوجيا المعلومات بأنها "هي جريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة إستخدام المخرجات، إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدًا من الناحية التقنية مثل تعديل الكمبيوتر"[1]

ويرى الأستاذ "Rosemblatt" بأن الجريمة الإلكترونية هي "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغيير أو حذفها أو التي تحول عن طريقه".[2]

ومن جهة أخرى قد عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا 2000 الجريمة المعلوماتية بأنها: "جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي إرتكابها في بيئة إلكترونية".[3]

وحسب الدكتورة هدى فشفوش هي: كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات، أو هي "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كانت مرتبطة بتقنية المعلومات".

وقد عرفها آخرون بأنها: "الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا هاما، أو هي كل فعل إجرامي يستخدم الحاسب الآلي في إرتكابه كأداة رئيسية".[1]

---

[1] على جعفر، جرائم تكنولوجية المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، مكتبة زين الحقوقية والأدبية، الطبعة الأولى، 2013، ص78-79.

[2] عائشة تايري، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة درارية، أدرار، 2016، ص07.

[3] حليمة حوالف، معالم الجريمة المعلوماتية في القانون الجزائري، مجلة البحوث القانونية والسياسية، مجلد 03، عدد16، 2012، ص143.

ما يؤخذ بعد إستعراضنا للتعريفات التي قيلت في جرائم الإنترنت، فأنه كما بين ذكره في البداية لا يوجد أي من تلك التعاريف التي حددت المقصود من هذه الجريمة بصورة جامعة مانعة كونها متقاربة من بعضها البعض، فبعض من فقها هذا الإتجاه ركز عن معيار موضوع الجريمة، والبعض الآخر ركز عن وسيلة إرتكابها، والبعض الآخر ركز على معيار النتيجة.

الفرع الثاني: الإتجاه الموسع في تعريف الجريمة الإلكترونية:

عرفها أصحاب الإتجاه الموسع بأنها: «كل سلوك إجرامي يتم مساعدة الحاسوب» أو هي كل جريمة تتم في محيط أجهزة الحاسوب وفي ذالك الإتجاه يرى الفقيهان (Michel & Credo) أن سوء إستخدام الحاسوب أو جريمة الحاسوب تسهل إستخدام الحاسوب كأداة لإرتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته كما تمتد لتشمل الإعتداءات المادية سواء على الجهاز الحاسوب ذاته أو المعدات المتصلة به.[2]

وقد إتجه جانب كبير من الفقهاء إلى إعتماد التعريف الذي تبنته منظمة التعاون الإقتصادي والتنمية (OCDE) للجريمة المعلوماتية في إجتماع باريس عام 1983 على أنها «كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها».[3]

هناك مفهوم واسعا للجرائم المعلوماتية بحيث يحيط بكل شكل من الأشكال التعسف في مجال إستخدام المعلوماتية معتبرا أن هذا التعسف "ما هو إلا فعل إجرامي يتصل بتقنية المعلومات يؤدي إلى تكبد المجني عليه خسارة ويحقق الفاعل ربحا متعمدًا".[4]

وهناك من يعرفها على أنها الجرائم ذات طابع المادي التي تتمثل في كل سلوك غير قانوني من خلال إستخدام الأجهزة الإلكترونية ينتج منها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة

---

[1] يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة لنيل ماستر أكاديمي، فرع حقوق، جامعة المسيلة، كلية الحقوق، 2016، ص10، مذكرة ماستر.

[2] شاهين خضر ورضوان سعادة، الجريمة الإلكترونية وإجراءات مواجهتها، قسم حقوق، جامعة المسيلة، كلية الحقوق، 2021، مذكرة الماستر، ص10.

[3] أسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، العدد 11، سبتمبر 2018، ص351-352.

[4] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة02، 2006، ص85.

مقابلة، وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل السرقة أو إتلاف المعلومات الموجودة في الأجهزة، ومن ثم إبتزاز الأشخاص بإستخدام تلك المعلومات.[1]

وقد عرفت كذلك كونها "كل فعل غير مشروع إقترن بالتواصل مع منظومات معلوماتية وشبكات الإتصال الخاصة به، والتي يحميها قانون العقوبات ويفرض عقابا لها".[2]

الفرع الثالث: التعريف القانوني للجريمة الإلكترونية:

عرفها المشرع الجزائري من خلال المادة02 من القانون 04/09 المؤرخ في 14 شعبان 05/1430 أوت 2009؛ والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال: «جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية، أو نظام للإتصالات الإلكترونية».[3]

وبهذا فقد وفق المشرع برأينا في تعريفه لأنه جمع الحالات التي تكون فيها نظم المعلوماتية وشبكات الإتصال إما موضوعا للجريمة أو وسيلة أو دعامة للجرائم التقليدية، ولولا هذه النظم المعلوماتية وشبكات الإتصال ما كان أن نصيغ صفة المعلوماتية على هذه الجرائم[4]، ومن أمثلة الجريمة الإلكترونية المرتكبة في الجزائر، تسريب أسئلة البكالوريا 2016، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي ألقي عليه القبض من طرف الشرطة الفدرالية الأمريكية.[5]

ويلاحظ على هذا العريف ما يلي:

أولا: أن المشرع الجزائري قد إعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة وهو نظام الإتصالات الإلكترونية وثانهما معيار موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات وثالثهما معيار القانون الواجب التطبيق، أو الركن الشرعي للجريمة المنصوص عليه في قانون العقوبات.

---

[1] أسمهان بوضياف، مرجع سابق، ص353.

[2] حليمة حوالف، المرجع السابق، ص143.

[3] عبد المالك صوالي، تشريعات الجريمة الإلكترونية في البيئة الإعلامية العالمية، جامعة محمد بوضياف المسيلة، جوان2018، العدد10، ص460.

[4] محمد بوعمرة وسيد علي بنينال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة الماستر، قسم قانون خاص، جامعة البويرة، كلية الحقوق والعلوم السياسية، 2020، ص06.

[5] عائشة تايري، الجريمة الإلكترونية في التشريع الجزائري، المرجع السابق، ص09.

ثانيا: حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقرار بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل إرتكابها عليه. وهذا ما وسع من نطاق المجال الجرائم الإلكترونية في التشريع الجزائري.[1]

المطلب الثاني: خصائص الجريمة الإلكترونية

تتميز الجرائم الإلكترونية المرتكبة بواسطة الكمبيوتر سواء كأداة الجريمة أو هدف لها بخصائص منفردة عن باقي الجرائم، نظرا لطبيعتها الخاصة فهي تتم في وسط إفتراضي يخلق صعوبات بالغة سواء في مجال إكتشافها أو في مجال ملاحقة مرتكبيها، بما يترك فرصا لإفلات المجرم من العقاب.

وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات والحقائق والتي إنعكست بدورها على مرتكب هذه الجريمة، والذي إصطلح على تسميته بالمجرم المعلوماتي أو مجرم التقنية الحديثة لتميزه أيضا عن المجرم التقليدي، وسوف نحاول من خلال المطلب أن نتعرف عن أهم خصائص جريمة تكنولوجيا المعلومات الحديثة وذلك من خلال فرعين إثنين:

فرع01: خصائص الجريمة الإلكترونية.

فرع02: سمات المجرم في تقنية المعلومات الحديثة.

الفرع الأول: خصائص جريمة تقنية المعلومات الحديثة:

أضفى إرتباط الجريمة الإلكترونية بجهاز الحاسوب وشبكة الأنترنت مجموعة من الخصائص تنفرد بها عن غيرها من الجرائم التقليدي وهذا ما كسبها لونا وطابعا قانونيا خاص.

أولا: جريمة تكنولوجيا المعلومات الحديثة متعددة الحدود أو جريمة عابرة للحدود الدولية:

يكمن القول إن أهم الخصائص التي تميز جريمة تكنولوجي المعلومات الحديثة هي تخطيها للحدود الجغرافية، ومن ثم إكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعددة الحدود. فالمجتمع التقنية الحديثة لا يعترف بالحدود الجغرافية، فهو مجتمع متفتح عبرة شبكات تخترق الزمان والمكان

[1] أسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، المرجع السابق، ص 353.

دون أن يخضع لحرس الحدود، فهي تربط بين دول لا تتحدها حدود الطبيعة أو حدود السياسة وتسمح لمستخدميها بالتنقل المعنوي و الإفتراضي بين الدول والقارات بدون تعقيدات أو صعوبات أو عوائق، فهي عالم ضخم متنوع متجدد خالي من الحدود والعوائق حيث أن أماكن متعددة في دول مختلفة قد تتأثر بجريمة تكنولوجيا المعلومات الحديثة الواحدة في آن واحد، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان إرتكاب جريمة عن طريق نظام معلومات إلكتروني موجود في دولة معينة، بينما يتحقق الفعل الإجرامي في دولة أخرى.

هذه الطبيعة التي تتميز بها جريمة تكنولوجيا المعلومات الحديثة كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الإختصاص القضائي بهذه الجريمة، كذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وبالتالي فإن الوصول للحقيقة بشأنها يستوجب الإستعانة بخبرة فنية عالية المستوى.[1]

ثانيا: الجرائم ترتكب عبر شبكة الإنترنت أو عليها:

تعد شبكة الأنترنت الحقل الذي تقع فيه جرائم الإنترنت، وذلك لأنها تمثل حلقة الوصول بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك والشركات الصناعية وغيرها من الأهداف التي تكون غالبا الضحية لها، إلا أنه بالرغم من كونها الوسيلة لإرتكاب جرائم الإنترنت إلى جانب الحاسب الآلي، فإنها كذلك لم تنجوا من يد المجرمين لأنها هي الأخرى قد تكون محلاً للإعتداءات.[2]

ثالثا: الحاسب الآلي هو أداة إرتكاب جرائم المعلومات:

خاصية أن الحاسب الآلي computer هو دائما أداة الجريمة في الجرائم التي ترتكب على شبكة الإنترنت، هي خاصية منفردة عن أي جريمة أخرى ذلك أن الحاسب الآلي هو الأداة الوحيدة التي تمكن

---

[1] علي جعفر، المرجع السابق، ص98-99.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006، ص37.

الشخص من الدخول على شبكة الإنترنت internet وقيامه بتنفيذ جريمته أيًا كان نوعها، وعليه فالحاسب الآلي هو الأداة الوحيدة لإرتكاب أي جريمة من جرائم التي ترتكب على شبكة الإنترنت.[1]

رابعا: مرتكب جرائم الإنترنت هو شخص ذو خبرة فائقة في مجال الحواسيب:

تتطلب جرائم الأنترنت على غرار الجرائم التقليدية حرفية فنية عالية سواء عند إرتكابها أو عند العمل على عدم إكتشافها من الشخص الذي يرتكبها، أي يجب أن يكون ذلك الشخص خبيرًا بالقدر اللازم والكافي بأمور الحوسبة والإنترنت، ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي، وأن الشرطة أول ما تبحث عن خبراء الكمبيوتر عند إرتكاب هذا النوع من الجرائم.[2]

خامسا: جرائم يصعب إكتشافها:

يمكن رد الأسباب التي تقف وراء صعوبة إكتشاف الجرائم المعلوماتية إلى عدم تركها لأثار خارجية كما في جرائم التقليدية، فهي تتم في بيئة إفتراضية (Virtual Environnement) ناهيك على أن الجاني يمكنه إرتكاب الجريمة في دولة أو قارة أخرى كما توفر التقنية المعلوماتية للمجرم إخفاء أثار الجريمة عن طريق التلاعب غير المرئي في نبضات أو ذبذبات الإلكترونية وبالتالي محو اثاره مما يخلق صعوبات بالغة لسلطات البحث والتحري في ملاحقته وضمان عدم إفلاته من العقاب، خاصة أن تنفيذها لا يتطلب وجود الفاعل في مكان الجريمة بل يمكنه تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل سواء كان من خلال الدخول لشبكة المعنية أو إعتراض عملية تحويل مالية أو سرقة معلومات هامة.

للأسف يلعب المجني عليه في الجرائم الإلكترونية دورا سلبيا في الكشف عنها فمن جهة يمنع في الغالب عن التبليغ عنها لسببين، الأول صعوبة تحديد هوية المجرم الإلكتروني وثانيا التحديات التقنية لإستخلاص الدليل الإلكتروني.

ناهيك عن إعتبارات أخرى قد تكون شخصية أو مالية أو متعلقة بالسمعة؛ وعموما هناك عدة أسباب تخول دون إستكشاف الجرائم الإلكترونية منها:

---

[1] عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، الطبعة الأولى، 1430/2009، عمان، دار المستقبل للنشر والتوزيع، ص140.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، المرجع السابق، ص37.

1. التكنولوجيا المعقدة وقدرة التخزين الهائلة والسرعة البالغة التي يعمل بها الحاسوب.
2. عدم وجود خطط بديلة لدى ضحايا الجرائم الإلكترونية للرد عليها وتفادي أضرارها.[1]

الفرع الثاني: سمات المجرم في جرائم تقنية المعلومات الحديثة:

ما من شك أن المدى الزمني لنشأة وتطور العلوم الجنائية وما نتج في نطاقتها من دراسات وتحديدا في ميدان عالم الإجرام أمكن في ظلها بلورة سمات عامة للمجرمين تبعا للجرائم التي يرتكبونها، فعلى سبيل المثال الجريمة الإلكترونية بالرجوع إلى تعريف الجريمة الإلكترونية بدلالة مرتكبيها فهي "قيام شخص ما مكنته معرفته وإستخدامه لأجهزة الحاسوب والأنترنت، أو لمعرفته لأحدهما من إرتكاب الجريمة المختارة"، وإنطلاقا من تفرد الجرائم الإلكترونية بخصائص عديدة، ينسحب ذلك أيضا على المجرم المعلوماتي الذي تتوفر فيه مميزات كالتخصص والإحترافية، إضافة إلى الذكاء وعدم إستعمال العنف.

أولا: التخصص والإحترافية:

1. **التخصص:** رأينا سلفا أن إرتباط الجرائم المعلوماتية بتكنولوجيا المعلومات ميزتها عن غيرها من الجرائم التقليدية، وهذا الإرتباط هو نفسه من أسباب تميز المجرم المعلوماتي عن غيره من المجرمين التقليدين، لقد إتضح من مختلف الدراسات التي أجريت في هذا المجال في كل من أوروبا والولايات المتحدة الأمريكية، أن أغلب مرتكبي هذه الجرائم هم من الشباب الذين تتراوح أعمارهم بين 25-45 سنة معظمهم من ذوي الإختصاص العالي، مما جعل البعض يشبههم بالمجرمين ذوي "الياقات البيضاء" وأنهم لتسمون بالحرص الشديد خشية ضبطهم وإفتضاح أمرهم.

تجدر الإشارة إلى أن توافر البراعة والمهارة في إستعمال الحاسوب ليس حكرا على أصحاب التخصص في هذا المجال، وبإعتبار أن المعلوماتية صارت متاحة للجميع نتيجة إنتشار الحواسيب وشبكة الأنترنت وثقافة إستعمالها، إذ يمكن لكل من يمتلك القدرة على التعامل مع الحواسيب ويتبع التقنيات الجديدة في مجال المعلوماتية، أن يكتسب مهارة كبيرة، وبالتالي إرتكاب جرائم في هذا المجال.

---

[1] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتفاقية العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات، قانون الإجراءات الجزائية، قوانين خاصة 2019، دار الجامعة الجديدة 40 سوتنير، الإسكندرية، ص82-83.

2. **الإحترافية:** يتمتع المجرم المعلوماتي بإحترافية كبيرة في تنفيذ جرائمه، حيث يرتكبها بواسطة الكمبيوتر الأمر الذي يقتضي الخبرة والإدراك الواسعين والمهارة التقنية اللازمة لتحقيق أهدافه الإجرامية. إن المقصود بالمهارة في هذا المجال أن يكون المجرم على درجة من العلم والدراية في التعامل في مجال المعالجة الآلية للمعطيات، والتي قد يكتسبها من خلال الدراسة المتخصصة أو عن طريق الخبرة المكتسبة في المجال تكنولوجيا المعلومات كإختراق نظم الكمبيوتر العائدة لشركات الصناعية والتجارية والقيام بعمليات الإحتيال والتزوير عن طريق شبكة الإنترنت بقصد تحقيق مكاسب مادية أو غيرها. كما تمكنهم إحترافيتهم من التغلب على العقبات التي أوجدها المختصون في مجال البرمجيات لتوفير أنظمة لحماية الكمبيوتر من كافة أشكال القرصنة، كما في حالة البنوك والشركات والمؤسسات الصناعية والعسكرية...إلخ.

ثانيا: الذكاء وعدم إستعمال العنف:

1. **الذكاء:** المجرم المعلوماتي ليس شخصية عادية، فهو يتصف بالذكاء، وهو على قدر كبير سرعة الفهم وسعة الإطلاع والنشاط الذهني المتقدم الذي يسعى إلى خداع الكمبيوتر، إضافة إلى القدرة على التعامل مع كل ما يصدر في مجال إستعمال الكمبيوتر وبرامجه، وإستغلال شبكة الإنترنت فيستطيع التلاعب بالمعلومات أو الكيانات المنطقية للحاسوب كزرع فيروسات لنسخ البيانات أو تدميرها.

2. **عدم إستعمال العنف:** بمعنى أن المجرم لا يلجأ للمجهود العضلي كما في الجرائم التقليدية فالجرائم المعلوماتية هي جرائم هادئة بطبيعتها (Soft Crines) لا تحتاج للعنف فهذه الجرائم تنتمي إلى إجرام الحيلة، أو ما يعرف بجرائم "الياقة البيضاء" كما يتمتع فيها المجرم بالتكيف الإجتماعي، أي لا يناص أحد العداء كما أنه على درجة عالية من الثقافة.[1]

ثالثا: التكيف الإجتماعي: فالمجرم يقوم بواجباته ويمارس حقوقه الإجتماعية والسياسية دون أي عائق في حياته اليومية، إذ تعتبر هذه الخاصية إمتداد السمة التخطيط والتنظيم حيث أن التكيف الإجتماعي ينشأ بين مجموعة لها صفات مشتركة.[2]

ويمكن إجمال القواسم المشتركة بين هؤلاء المجرمين في عدة صفات وهي:

---

[1] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتفاقية العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات، قانون الإجراءات الجزائية، مرجع سابق، ص 85-86-87-88.

[2] عائشة تايري، مرجع سابق، ص20

- عادة ما تتراوح أعمارهم ما بين 18 و45 سنة.
- المهارة والإلهام الكامل والقدرة الهائلة في مجال نظم المعلوماتية.
- الثقة الزائدة بالنفس.
- الإلهام بمسرح الجريمة بما يجنيه فجائية المواقف التي قد تؤدي إلى إفشال مخططه وإفتضاح أمره.

أسباب الإجرام الإلكتروني:

تبين مما سبق أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الأفعال الإجرامية التقليدية لذى من الطبيعي أن تجد نفس الإختلاف في الأسباب والعوامل التي تدفع لإرتكاب الفعل الغير مشروع ويأتي في مقدمة هذه الأسباب غاية التعليم التي تتمثل في إستخدام الكمبيوتر والإمكانيات المستخدمة في نظام المعلومات وغاية الربح التي كثيرا ما تدفع إلى التعدي على نظام المعلومات بالإضافة إلى الدوافع الشخصية والمؤثرات الخارجية تكون سببا لإرتكاب هذه الجرائم.

1 غاية التعليم:

يشير الأستاذ ليفي مؤلف كتاب "قراصنة الأنظمة" إلى أخلاقيات هؤلاء القراصنة التي ترتكز على مبدأين أساسين هما:

- إن الدخول إلى جميع أنظمة الكمبيوتر يمكن أن يعلمك كيف يسير العالم.
- إن جميع المعلومات يجب أن تكون غير خاضعة للقيود.

وبناءا على هذين المبدأين فإن أجهزة الكمبيوتر المعنية ما هي إلا آلات البحث والمعلومات بدورها ماهي إلا لبرامج وأنظمة معلومات وأن جميع المعلومات لابد أن تكون غير خاضعة لأية قيود أي تتاح حرية نسخها وجعلها تتناسب مع إستخدامات الأشخاص.[1]

مثال: عامل طلاء يدعى Romald تمكن بفضل الألة المسروقة من التواصل لأسلوب مطالعة وقام بالسطو على صانع الموزعات الآلية ولكن ألقي القبض عليه قبل أن يستفيد من نزعته المستخدمة ونسب إليه جريمة سرقة الألة.

[1] سليمة سعيدي وبلال حجاز، جرائم المعلوماتية والشبكات في العصر الرقمي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2017، ص36.

ومن الملاحظ على وجه الدقة أن بعض مرتكبين أفعال الغش المعلوماتي ليسوا على جانب كبير من الخطورة الإجرامية وكل ما يهمهم هو تحقيق إنتصارات تقنية دون أن تكون لهم نواية أثمة، وإن كان هذا لا يمنع من أن تكون هناك بواعث أخرى أثمة وغير شريفة تحَض على إرتكاب أفعال الغش المعلوماتي.[1]

2 تحقيق مكاسب مالية:

أحيانا يكون هدف الهاكر من التسلل وإختراق المواقع للحصول على ربح مالي عن طريق المساومة على البرامج أو المعلومات المتحصل عليها بطريقة الإختلاس من جهاز الكمبيوتر أو عن طريق إستعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية وقد أشارت مجلة Sécurité Informatique إلى الرغبة في تحقيق الثراء من بين العوامل الأساسية لإرتكاب الجريمة المعلوماتية حيث أشارت إلى:

- 43% من حالات الغش المعلن عنها من أجل إختلاس الأموال.
- 23% من أجل سرقة المعلومات.
- 19% أعمال إتلاف.
- 10% سرقة وقت الآلة أي إستعمال الغير مشروع للآلة لتحقيق أعراض شخصية.

لذلك نجد أن الدافع لإرتكاب الجريمة المعلوماتية يمكن أن يكون سببه مجرد سداد ديون أو مشاكل مالية عائلية أو إدمان ألعاب الأقمار أو المخدرات ويمكن أن نبين في هذا المجال الواقعة إستلاء مبرمج يعمل لدى إحدى الشركات الألمانية على 22 شريط ممغنط يحتوي على المعلومات هامة بخصوص عملاء وإنتاج هذه الشركة حيث هدد السارق ببيعها لشركات منافسة إذا لم تدفع فدية مقدرها 200000 دولار وبعد تحليل الخسائر الناتجة عن بيع هذه المعلومات وجدت بأنها تفوق بكثير المبلغ المطلوب ففضلت الشركة الدفع مقابل إسترجاع الأشرطة المسروقة.

3 الإنبهار بالتقنية:

مع ظهور التقنية المعلوماتية الحديثة وإنتشارها في المجتمعات الحديثة سواء تعلق الأمر بالمعلومات أو تعلق بالحاسبات الآلية فإن الأمر في النهاية يؤدي إلى الإنبهار بالتقنية ولذلك فإن هؤلاء الدخلاء ليسوا على

[1] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص56.

قدر كبير من الخطورة الإجرامية وإنما هو في الغالب يفضلون تحقيق إنتصارات تقنية دون أن تتوفر لديهم أية نوايا سيئة ونضرب مثلا لذلك، نشر في مجلة "Experéses" الفرنسية وتدور أحداث القصة حول عامل طلاء مباني توجه إلى أحد البنوك لإداع شيك خاص به تعاصر ذلك مع لحظة عطل الموزع الآلي للنقود حيث شاهد مستخدم صيانة الأجهزة الآلية يستخرج النقود من الالة عند الطلب عن طريق إستخدام بطاقة خاصة وقد أحدث هذا الإبتكار للآلة تصدعا في الحياة العادية لعامل الطلاء الذي عكف على تعليم تقنية الحاسب لمدة عامين ثم قام بالسطو على الموزع الالي للبنك وقد تمكن هذا العامل بفضل الآلة المسروقة من التوصل إلى أسلوب مطالعة السحب وقد ألقي عليه القبض قبل أن يستفيد من براعته المستحدثة وقد تنسب إليه جريمة السرقة.

4 الدافع الشخصي والمؤثرات الخارجية:

طبيعة الإنسان كمخلوق ضعيف سيكولوجي من الممكن في بعض المواقف ان يستسلم للمؤثرات الخارجية، فمجرد إظهار جنون العظمة قد يكون هو الدافع لإرتكاب فعل الغش المعلوماتي، فترى المحلل أو المبرمج المعلوماتي وهو مفتاح سر كل نظام قد يندفع تحت تأثير رغبة قوية من أجل تأكيد قدراته التقنية لإدارة المنشأة إلى إرتكاب فعل الغش المعلوماتي وقد يعترف به.[1]

وفي نطاق المنافسة والتجسس الخاصة ومجالات الأعمال التجارية عامة نوى أعمال الغش المعلوماتي تمارس تحت تهديد أو ضغط من الغير فهذا ما يدفع بعض المنشآت بل بعض الدول إلى الإتصال بالأفراد الذين يشغلون مراكز مرموقة كي يعلموا لصالح المنشآت منافسة بهدف الإطلاع على بعض المعلومات الأساسية مثل الرشوة، الإغراء، الخداع عند اللزوم، الإكراه والتهديد وقد يفضلون زرع جواسيس خاصة بهم.[2]

5 واقع خاصة بالمنشأة:

من العناصر المؤثرة التي تؤدي إلى زيادة الجرائم المعلوماتية لدى المنشأة بعض الدوافع التي تكون خاصة بها...والمتمثلة لدى الشخص المسؤول عن المراكز المعلوماتي بالمنشأة حيث يمكنه وضعه الوظيفي من إستغلال منصبه إذا شاء لمصلحته ويعتمد بعض المتخصصين في تقنية الأنظمة المعلومات أن من مزايا

---

[1] سليمة سعيدي، بلال حجاز، المرجع السابق، ص37-38-39.

[2] سامي علي حامد عباد، المرجع السابق، ص57-58.

مراكزهم الوظيفية ومهارتهم الفنية إستخدام الأنظمة وبرامجها لإغراض شخصية أو للتباري الفكري فيما بينهم أو ممارسة بعض الهوايات الدائرة في فلك التقنية، ومن شأن ذلك تمادي بعضهم إلى إستخدام الأنظمة بصورة غير مشروعة تصل إلى حد إرتكاب جرائم خطيرة بالمنشأة لمصلحته الخاصة.

وهناك مثال على ذلك الإستخدام الغير مشروع للنظم المعلوماتي تتلخص وقائعه وتتمثل في أن مستشارا لدى إحدى البنوك الكبرى يدعى Rifkin Stanly كان يتمتع بتقنية مطلقة من جانب البنك وسمحت له إختصاصته بالولوج إلى مفاتيحين إلكترونية من ثلاثة أساسية للتحكم في التحويلات الإلكترونية للنقود من بنك إلى آخر وقد تمكن بفضل معالجته الآلية للمعلومات وتألقه الشديد مع النظام المعلوماتي من الوصول إلى المفتاح الثالث من خلاله إستطاع تحويل 10 مليون دولار إلى حساب بنكي مفتوح بإسمه في سويسرا وألقي القبض عليه وصدر ضده حكم بالسجن لمدة 6 سنوات.[1]

المبحث الثاني: الطبعة القانونية للجريمة الإلكترونية:

إن التطور الهائل في مجال المعلوماتية أدى إلى ظهور أنواع عديدة من الجرائم الإلكترونية التي أصبحت تشكل خطرا يهدد حياة المجتمعات بأكملها، والتي لها طبيعة خاصة تمييزها عن غيرها من الجرائم.

تكمن الطبيعة القانونية للجريمة الإلكترونية في؛ تمييزها بصفة فنية ومفردات ومصطلحات جديدة كالبرامج والبيانات التي تشكل محلا للإعتداء أو تستخدم كوسيلة بالإعتداء، فمعضم مستندات الجريمة الإلكترونية عبارة عن التسجيلات إلكترونية تتم عبر شبكات الإتصال المعلوماتي ذات طبيعة خاصة متميزة، ذلك راجع إلى طبيعة المال المعلوماتي وحداثه ظهور الحاسب الآلي وتقنية تشغيله.

موضوع الجريمة الإلكترونية:

ترتكب هذه الجرائم على الحاسب نفسه سواء على مكوناته المادية أو معلوماته وقد يستخدم الحاسب كأداة لإرتكاب إحدى هذه الجرائم وبالتالي هناك حالات للمواضيع التي تدور حولها الجريمة المعلوماتية أو الإلكترونية وهي:

01 وقوع الجريمة على مكونات الحاسب المادية:

[1] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، المرجع السابق، ص91.

وتتحق هذه الحاجة إذا كانت مكونات الحاسب المادية من أجهزة والكابلات والمعدات وشبكات الربط وآلات الطباعة والشرائط الخام التي سجلت عليها البرامج والمعطيات هي محل أو موضوع لهذه الجريمة وبالتالي فإن هذه الحالات لا تثير مشكلة بإعتبار هذه المكونات المادية محل الإعتداء تتمتع بالحماية الجنائية للنصوص التقليدية بإعتبارها من المواد المنقولة التي تخضع سرقتها وإتلافها للنصوص الجنائية ومنه فإن الأمر الراهن لا يثير أي إشكال حيال تطبيق النصوص التقليدية على هذه الأموال.

2 وقوع الجريمة على مكونات المعلوماتية أو غير المادية للحاسب:

وتتحقق هذه الحالة عندما تكون مكونات الحاسب المعلوماتية غير المادية مثل البرامج المستخدمة، البيانات والمعطيات المخزنة في الذاكرة محلا أو موضوعا للجريمة حيث من الممكن أن يقوم أحد الأشخاص بالإعتداء على برامج الحاسب أو أن يدعي ملكيته أو يقوم بسرقة أو تقليد أو نقل أو تعطيل برنامج ما أو يقوم بإنشاء محتوياته أمام البيانات وبنوك المعطيات فإنه يستطيع العبث بها أو تحريفها وتزويرها ونسخها.

ونظرا لطابع الخاص الذي يميز هذه المكونات أن النصوص التقليدية الحالية لقانون العقوبات تكون عاجزة عن مواجهة ما قد يقع عليها من الجرائم نظرا لحداثتها النسبية ولأن النصوص الحالية تعجز عن شمول الحالات الجديدة الطارئة ولأن القانون الجنائي نفسه يعاني من فراغ تشريعي في المجال المعلوماتي.

3 حالة إستخدام الحاسب الآلي كأداة للجريمة:

في هذه الحالة لا يكون الحاسب محل أو موضوع الجريمة وبالتالي لا يكون محلا للحماية الجنائية ولكن تقع الجريمة بواسطته أي أنه يستخدم كأداة لإرتكابها فمن الممكن أن تقع بعض الجرائم بواسطة الحاسب مثل الجرائم التي تقع على الذمة المالية من سرقة ونصب وخيانة للأمانة والتزوير في عمليات السحب، وإنتهاك حرمة الحياة الخاصة بل ويستعمل للقتل كذلك عن طريق برمجة جهاز التفجير يتم التحكم فيه عن بعد.[1]

كما أن المال المعلوماتي ينقسم إلى نوعين: إما مال معلوماتي ذو طبيعة معنوية ويتمثل في الرامج والمعلومات أيا كان نوعها؛ وإما أن يكون المال المعلوماتي ذو طبيعة مادية ويتمثل في الأدوات وآلات الحاسب الآلي الملموسة، إذ قد يترتب على إختلاف هذه الطبيعة القانونية للمال المعلوماتي إختلاف في النتائج المترتبة على تطبيق بعض النصوص القانون الجنائي التقليدي.

[1] سليمة سعيدي، بلال حجاز، جرائم المعلومات والشبكات في العصر الرقمي، المرجع السابق، ص68-69.

بحيث إن قواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة، وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها الإثبات ومتابعة مرتكبيها ومن هنا يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.

تختلف الجرائم الإلكترونية عن الجرائم التقليدية من حيث الطبيعة القانونية؛ فالجرائم الإلكترونية من الجرائم المستحدثة تكون فيها شبكة الأنترنت أما وسيلة لإرتكابها أو محلا لها ويستخدم الحاسوب فيها كأداة لتسهيل إرتكابها.[1]

أركان الجريمة الإلكترونية:

هما لا شك فيه أن الجريمة الإلكترونية لا تختلف عن أي جريمة تقليدية أخرى إذ أنها تتطلب لتحقيقها الأركان المتفق على ضرورة توفيرها في أي جريمة لكي تتواجد على أرض الواقع، فبالإضافة إلى ضرورة تواجد الشرط المبدئي في كل جريمة أي النص الشرعي المجرم أو الصفة الغير مشروعة، فإنه لابد من وجود الركنين اللذين تتألف منها كل جريمة وهما: الركن المادي والركن المعنوي.

أولا: النص الشرعي المجرم أو الصفة غير المشروعة في جرائم الأنترنت:

قال تعالى:﴿ قُلْ أَيُّ شَيْءٍ أَكْبَرُ شَهَادَةً ۖ قُلِ اللَّهُ ۖ شَهِيدٌ بَيْنِي وَبَيْنَكُمْ ۚ وَأُوحِيَ إِلَيَّ هَٰذَا الْقُرْآنُ لِأُنذِرَكُم بِهِ وَمَن بَلَغَ ۚ أَئِنَّكُمْ لَتَشْهَدُونَ أَنَّ مَعَ اللَّهِ آلِهَةً أُخْرَىٰ ۚ قُل لَّا أَشْهَدُ ۚ قُلْ إِنَّمَا هُوَ إِلَٰهٌ وَاحِدٌ وَإِنَّنِي بَرِيءٌ مِّمَّا تُشْرِكُونَ ﴾.

قال تعالى: وَمَا كَانَ رَبُّكَ مُهْلِكَ الْقُرَىٰ حَتَّىٰ يَبْعَثَ فِي أُمِّهَا رَسُولًا يَتْلُو عَلَيْهِمْ آيَاتِنَا ۚ وَمَا كُنَّا مُهْلِكِي الْقُرَىٰ إِلَّا وَأَهْلُهَا ظَالِمُونَ ﴿٥٩﴾

النص الشرعي هو نص التجريم الذي يضفي على الفعل أو الإمتناع الصفة غير المشروعة، وقد إختلف الفقه ولا يزال حول طبيعته، فهناك من يعتبره ركنا في الجريمة الى جانب الركن المادي والمعنوي، وهناك من

[1] حسيبة جلود وزينب عماري، الجريمة الإلكترونية في الفقه الإسلامي وقانون العقوبات الجزائري، دراسة مقارنة، جامعة المسيلة، كلية العلوم الإنسانية والإجتماعية، قسم العلوم الإسلامية، 2019، ص25-26.

يعتبره صفة غير مشروعة تقترن بالسلوك فتجعله مجرما ومعاقب عليه؛ ويتجسد هذا النص من خلال مبدأ شهير هو "لا جريمة ولا عقوبة ولا تدبير آمن إلا بقانون" أي ما يعرف بمبدأ شرعية الجرائم والعقوبات.

وهو مبدأ ذو طابع عالمي، إلا أن الدول إعتادت على الإعتراف به في النطاق المحلي لا غير والإشكال المطروح هنا: ما محل جريمة الأنترنت من مبدأ شرعية الجرائم والعقوبات؟ وما مدى إلتقاء هذا المبدأ مع ظاهرة جرائم الأنترنت العابرة للحدود؟ وهل تنتمي جرائم الأنترنت إلى قانون الأنترنت أم أنها مشتقة من التجديد الذي يخترق بالضرورة أحد فروع القانون المتعددة وهو فرع القانون الجنائي؟

لقد أثار الفقه المعاصر موضوعا على جانب كبير من الأهمية يتعلق بتفاعل نظم التقنية الحديثة مع القانون الجنائي وتأثير ذلك على مبدأ الشرعية لاسيما حال إنعدام وجود نصوص قانونية تحكم مظاهر التعامل مع تلك التقنية.

وتعتبر جرائم الأنترنت التي أفرزتها الأنترنت، أحد التحديات الكبرى التي تقف أمام تطبيقات القانون الجنائي، والذي يكون في الكثير من الأحيان محلا لقصور بيَّن في تنظيم تلك الجرائم المستحدثة وهذا ما يسهل الكثير من المجرمين إرتكابها والإفلات من العقاب.[1]

ثانيا: الركن المادي:

لا يعاقب القانون الجنائي على الأفكار والنوايا السيئة مالم تخرج إلى الوجود الخارجي بفعل أو عمل، وهذا الفعل أو العمل الخارجي الذي يعبر عن النية الجنائية أو الخطأ الجزائي يسمى بالركن المادي للجريمة[2]، فيعرف بأنه يتمثل في سلوك إجرامي معين يتطلبه القانون كمناط للعقاب حتى هذه الجريمة على أن يحقق نتيجة ضارة لهذا السلوك الإجرامي كشرط بذاته يتعين قيامه حتى يعاقب على الجريمة، وفضلا عن ذلك يجب أن يرتبط النشاط أو السلوك الإجرامي ونتيجته الضارة بعلاقة سلبية، وهو ما يطلق عليه "الإستناد المادي" وعليه فالركن المادي في الجريمة التامة يقوم على ثلاثة عناصر وهي السلوك الإجرامي الذي يقع

[1] نبيلة هبة هروال، المرجع السابق، ص 41و 44.

[2] يزيد بوحليط، المرجع السابق، ص130.

من الجاني والنتيجة الضارة أو الخطر المترتب على هذا السلوك سواءا كان مقصودا أم لا، وأخيرا علاقة السببية بين سلوك الجاني والنتيجة التي تحققت[1].

وبالتالي يتمثل السلوك الإجرامي في النشاط الخارجي للجريمة أو هو حركة الجاني الإختيارية والتي يترتب عليها تغيير في العالم الخارجي كما يتخذ السلوك الإجرامي إحدى الصورتين:

أ سلوك إيجابي: يتمثل في حركة عضوية إرادية تقوم على الإدراك والتميز وحرية الإختيار في القيام بعمل ينهي القانون عن إرتكابه.

ب سلوك سلبي (الإمتناع): خلافا للقاعدة العامة فقد يأمر المشرع بالإقدام على أمر معين ويقرر عقوبة لمن يمتنع عن إتيانه، متخذا بذلك موقفا سلبيا كما أمر به القانون. أما بخصوص الجرائم الإلكترونية، ونظرا لما توفره تكنولوجيا الحوسبة والإتصال من تقنيات مذهلة تتميز بالسرعة والدقة وإمكانية الإفلات من الملاحقة في هذه البيئة الرقمية، فالركن المادي فيها عادة ما يبدأ بضغطة زر على لوحة مفاتيح أو بلمسة على شاشة الحاسوب أو الهاتف النقال، مثال: قيام المجرم الإلكتروني بالدخول للشبكة والتعارف على أشخاص كمستثمر أو تاجر قصد الحصول على أموالهم عبر شبكة الأنترنت. أو عند قيام المجرم ببرمجة فيروس وإرساله سواء لتحميل بيانات أو تدميرها، أو إرسال ملف فيديوا أو رسالة نصية تمس بشخص متلقى عبر البريد الإلكتروني أو الهاتف النقال.

إن السلوك الأجرامي في الجريمة الإلكترونية يرتبط عموما بالمعلومات المخزنة على الحاسوب[2] أو تلك التي يتم إدخالها فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى النظام أرصدة العملاء في البنوك أو إساءة إستخدام بطاقة الإنتمان.

ب النتيجة الإجرامية:

يعد هذا العنصر أحد عناصر الركن المادي في جريمة إلى جواز السلوك الإجرامي والعلاقة السببية، وتثير مسألة النتيجة الإجرامية في جرائم الأنترنت مشاكل عدة من أهمها: تحديد هل جريمة الأنترنت هي جريمة مرتكبة سلوكا ونتيجة في العالم الإفتراضي أم هناك إمتداد للنتيجة لتحقيق منتهاها في العالم المادي.

---

[1] علي لجلط، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، ط01، 2013، مكتبة زين الحقوقية والأدبية، ص121.

[2] يزيد بوحليط، المرجع السابق، ص31-32.

ج علاقة السببية :

هي العنصر الثاني من العناصر التي يتكون منها الركن المادي في الجريمة ويجب لقيام جريمة الأنترنت، أن تكون هناك رابطة مادية بين السلوك المادي والنتيجة الإجرامية المتحققة، فمثلا يجب لتحقق جريمة إنتهاك الحق في الخصوصية عبر الأنترنت، أن يكون هناك دخول على الأنترنت بإستخدام حاسوب عامل والقيام بإختراق الخوادم المختلفة في مسارها، ثم بعد ذلك التعدي على خصوصية موقع. وكذلك يمكن إعتبار علاقة السببية قائمة بمجرد ثبوت الضرر في مجرد البث.[1]

ثالثا: الركن المعنوي:

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، فالركن المعنوي هو المسلك الذهني أو النفس للجاني بإعتباره محور القانون الجاني لذلك، أنه في إطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية، من علم وإرادة آثمة وقصد جرمي مع إقرار حق الدولة في العقاب الذي يبني على هذه المقومات، لذلك يمكن تعريف الركن المعنوي بأنه العلاقة التي تربط بين مادية الجريمة وشخصيات الجاني مرتكبيها وهذه العلاقة هي محل الإذناب بمعنى إستحقاق العقاب، ومن ثم يوجه إليها لوم القانون وعقابه.[2]

يتكون الركن المعنوي للجريمة الإلكترونية من عنصريها أي العلم والإرادة.

1 العلم: هو إدراك الفاعل للأمور.

2 الإرادة: وهي إتجاه السلوك الإجرامي لتحقيق النتيجة.

طبقا للمبادئ العامة المعروفة في القانون العقوبات قد يكون القصد الجنائي عاما أو خاصا، فالقصد الجنائي العام هو الهدف المباشر للسلوك الإجرامي وينحصر في حدود إرتكاب الفعل؛ أما القصد الجنائي

[1] نبيلة هبة هروال، الجوانب الإجرامية لجرائم الأنترنت، المرجع السابق ص 47 و48

[2] عبد الله دعش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة إستكمالا للحصول على درجة الماجيستر في القانون العام، جامعة الشرق الأوسط سنة 2014، ص29

الخاص فهو ما يتطلب توافره في بعض الجرائم دون أخرى فلا يكتفي الفاعل بإرتكاب الجريمة بل يذهب إلى التأكد من تحقيق نتيجة.[1]

خطورة الجرائم المعلوماتية:

إن ظاهرة الجرائم الإلكترونية ظاهرة إجرامية مستجدة نسبيا تقرع في جانبيها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر، وهول الخسائر الناجمة عنها بإعتبارها تستهدف الإعتداء على المعطيات بدلالتها التقنية الواسعة، بيانات، معلومات وبرامج بكافة أنواعها فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء، يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات وتطال إعتداءاتها معطيات الكمبيوتر المخزنة والمعلومة المنقولة ، عبر نظم وشبكات المعلومات؛ وفي مقدمتها الأنترنت.

الخطورة على الصعيد الأقتصادي والمالي:

وحسب تقرير 2011 THE NORTON CYBEROCRIME REPORT الصادر عن شركة سيمانتك العالمية المتخصصة في آمن المعلومات حول أوضاع جرائم المعلومات في عام 2011 والذي حمل عنوان "صورة إجمالية لأوضاع آمن المعلومات حول العالم" نقلا عن مراكز الجزيرة للدراسات فقد بلغت عدد الشكاوى التي تتلقاها مركز شكاوى إحتيال الأنترنت الأمريكي(IFFG) منذ بداية أعماله في أيار 2000 م وحتى شهر تشريف ثاني من العام نفسه(أي خلال ستة أشهر فقط(6087) شكوى من ضمنها 5273 حالة تتعلق بإختراق الكمبيوتر عبر الأنترنت، وقد بلغت الخسائر المتصلة بهذه الشكاوي ما يقارب(4,6) مليون دولار.

وأعلن مركز بلاغات جرائم الأنترنت Internet crime complain center (IG^3) في تقريره السنوي لعام(2007)م أن مقدار ما تم خسارته في تكاليف الإستقبال(الإستقبال فقط) للبلاغات الناجمة من سوء إستخدام الأنترنت هو 198,4مليون دولار وذلك بزيادة قدرها 15,3مليون دولار عن السنة التي قبلها.

[1] حسيبة جلود، عماري زينب، الجريمة الإلكترونية في الفئة الإسلامي وقانون العقوبات الجزائري، دراسة مقارنة ص24 جامعة محمد بوضياف 1442/2020،1441/2019

ثم إن الفاتورة الإجمالية لجرائم آمن المعلومات عالميا وعربيا في(2011) وحدها تقدر بحوالي 388مليار دولار آمريكي، أما التكلفة النقدية المباشرة لهذه الجرائم المتمثلة في الأموال المسروقة ونفقات إزالة آثار الهجومات فتقدر بحوالي(114) مليار دولار. ومعنى ذلك أن القيمة المالية لجرائم المعلومات أكبر من السوق السوداء لمخدرات الماريجوانا والكوكايين والهيروين مجتمعين التي تقدر بحوالي(288) مليار دولار. وتزيد عن قيمة السوق العالمية للمخدرات عموما التي تصل الى411مليار دولار، وأعلى من الأنفاق السنوي كمنظمة الأمم المتحدة للأمومة والطفولة (اليونسيف) بحوالي100ضعف. حيث تصل ميزانيتها الى (3,65) مليار دولار. كما تعادل هذه الخسائر ما تم إنفاقه خلال 90عاما من مكافحة الملاريا وضعف ما تم إنفاقه على التعليم في 38عاما.

*وقد بلغ المعدل السنوي لوقوع جرائم المعلوماتية حول العالم 50ألف جريمة وإعتداء في الساعة تأثر بها(589) مليون شخص وهو رقم أكبر من عدد سكان الولايات المتحدة وكندا وغرب أوروبا مجتمعين، ويعادل 09% من إجمالي سكان العالم. وقد توزعت هذه الجرائم ما بين جرائم الفيروسات والبريد الإلكتروني الملوث والضار وجرائم الإحتيال والنصب والإصطياد (للحصول على معلومات بنكية سرية) والجرائم المتعلقة بإختراق الهواتف المحمولة.[1]

[1] سليمة سعدي وحجاز بلال. جرائم المعلومات والشبكات في العصر الرقمي، المرجع السابق، ص64 و65.

الفصل الثاني

الفصل الثاني: الآليات القانونية لمكافحة الجريمة الإلكترونية على المستوى التشريعات الدولية والوطنية.

إن أنشطة مكافحة جرائم الكمبيوتر أبرزت تحديات ومشكلات جمة، فهي جرائم عابرة للحدود نتيجة إستعمال شبكة الأنترنت كما أنها ل تترك أثر مادي في مصرح الجريمة كغيرها من الجرائم ذات طبيعة مادية ولتظافر العديد من الصعوبات تناوعت الجهود الدولية والوطنية في مكافحة الجريمة الإلكترونية حيث تم إتخاذ العديد من الآليات والإجراءات لحد والتقليل منها.

المبحث الأول: السياسة الدولية لمكافحة الجريمة الإلكترونية:

إن الجريمة الإلكترونية بإعتبارها من الجرائم المعلوماتية المعاصرة التي واكبت عصر التقدم التكنولوجي خصوصا بعد ظهور شبكة المعلومات الدولية "الأنترنت" بسبب التقدم العلمي الحاصل ساعد على إنتشار وتنوع السلوك الإجرامي الذي أصبح يهدد الإنسان في مختلف المجالات وبالنظر لخطورة هذه الجريمة وصعوبة الكشف عنها وغياب الدليل المادي الذي يدين مرتكبيها فإنها أصبحت تطغى على ساحة الإجرام وبشكل كبير نتيجة لغياب إستراتيجية فعالة لمحاربتها والتقليل منها خاصة على مستوى الدولي في ظل صعوبة التعاون الدولي للحد منها وقلة الإتفاقيات الدولية وهذا بالنظر إلى طبيعتها الخاصة.

المطلب الأول: التعاون الدولي ودوره في مكافحة الجريمة الإلكترونية:

لما كانت جرائم الأنترنت ذات صفة عالمية، يمكن أن تتعدى أثارها عدة دول، فإن ملاحقة مرتكبيها وتقديمهم للمحكمة، وتوقيع العقاب عليهم يتطلب ضرورة التعاون فيما بين الدول للقبض على المتهمين أو لجمع الأدلة أو سماع الشهود، أو اللجوء إلى الإنابة القضائية. وتجدر الإشارة إلى أنه لم يعد ينظر إلى ذلك التعاون بإعتباره أنه يخلق "سيادة فوق الدول"، بقدر ما أصبح يعني التعاون بين "سيادة دول مختلفة" ترمي جميعا إلى تسديد وتفعيل حلقات المكافحة بوجه عام، والجريمة عبر الوطنية بوجه خاص.[1]

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت "مرحلة جمع الإستدلالات"، دراسة مقارنة، المرجع السابق، ص147.

الفرع الأول: التعاون ودوره في مكافحة الجريمة:

يعرف التعاون الأمني بين الدول على أنه: "مجموعة الإجراءات التي تتخذها سلطة دولة ما أو جهاز منظمة دولية حكومية بناء على طلب دولة أو منظمة دولية أخرى سواء كانت إجراءات في المجال القضائي أو القانوني الشرطي إستنادا إلى المصادر القانونية الدولية المختلفة بهدف المساعدة في مكافحة الجريمة بصفة عامة والجرائم ذات الطابع الدولي بصفة خاصة.

ومن جهة ثانية حث قرار الأمم المتحدة رقم: 88/52 بتاريخ: 1988/02/04 تحت عنوان: "التعاون الدولي في المسائل الجنائية" على أن المعاهدات للأمم المتحدة بشأن التعاون الدولي في المسائل الجنائية توفر أدوات مهمة لأجل تطوير التعاون بما يسهم في زيادة الكفاءة في مكافحة الإجرام.

كما تبرز أهمية التعاون القضائي في مجال مكافحة الجرائم عبر الوطنية ومنها الجرائم الإلكترونية، في تميز هذه الأخيرة بخاصية عدم الإعتراف بالحدود الجغرافية، فهي تتحرك في فضاء شبكي يصعب معه ملاحقة المجرمين، مما فرض حتمية التعاون الدولي لأنه شبه مستحيل مكافحة هذا النوع من الجرائم دون تعاون دولي حقيقي وفعال على جميع الأصعدة، سواء على مستوى التجريم والعقاب أو على مستوى الإجراءات ناهيك عن تطوير الآليات الملاحقة القضائية الوطنية والدولية من خلال إحداث مؤسسات متخصصة في هذا المجال مثل: الأنتربول والمحكمة الجنائية الدولية...[1].

كما أبلغت الولايات المتحدة بأنها تواجه أربع تحديات رئيسية، أولهما الضغط الذي يمارس من أجل الحد من مساهمات الخبراء في السياسة الدولية، ففي حين أن أساليب إنقاذ القانون التقليدية قابلة لتكييفها لمكافحة الجريمة السيبرانية، فإن التحديات المواجهة معقدة وماضية مع التطور، ومن ثم فإن أي نقاشات عن السياسات في إطار الأمم المتحدة بشأن الجريمة السيبرانية ينبغي أن تفيد من المداخلات والمنشورات المباشرة عن الخبراء التقنيين، أما الضغط الذي تمارسه بعض الحكومات لإطلاق نقاشات سياسية بشأن معاهدات عالمية جديدة، على الرغم من عدم وجود تأييد يتوافق الأراء لإتباع هذا المنهج، فهو يستهلك الموارد القيمة وضعف مقدرة الخبراء على سداد مشوارة مجدية بشأن كيفية التغلب على التحديات الأساسية التي تواجهها الدول الأعضاء عند التحقيق في قضايا الجريمة السيبرانية وملاحقة مرتكبيها قضائيا، والمداخلات التي يسهم بها الخبراء ضرورية لفهم مسائل معقدة مثل مايلي:

[1] يزيد بوحليط، المرجع السابق، ص496-497.

- حماية حرية التعبير.
- القيود المناسبة على سلطة الدولة.
- التنفيذ الفعال للأطر القائمة.
- توفير التدريب والمساعدة التقنية للبلدان النامية في الوقت المناسب.[1]

صورة التعاون الدولي في مجال مكافحة جرائم الكمبيوتر والأنترنت؛ سنتطرق إلى أبرز هذه الصور فيما يلي:

1- **تبادل المعلومات:** تتمثل هذه الإجرام في تقديم المعلومات والبيانات والوثائق التي لها علاقة بالإستدلال أو التحقيق للسلطة القضائية الأجنبية أثناء نظرها في جريمة ما، حيث تعطي الدول أهمية قصوى لتبادل المعلومات بوصفها وسيلة فعالة لمكافحة الإجرام عموما، والجريمة المعلوماتية خصوصا، لما توفره المعلومات الصحيحة والموثوقة من مساندة لأجهزة تنفيذ القوانين في كافة المجالات، بما في ذلك متابعة النشاط المنظمات الإجرامية لذلك أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين، وبتطوير التبادل المنهجي للمعلومات بوصفه عنصرا رئيسيا من عناصر خطة العمل الدولية لمنع الجريمة ومكافحتها وأوصى بأنه على منظمة الأمم المتحدة أن ينشئ قاعدة معلوماتية لإعلام الدول الأطراف بالإتجاهات العالمية في مجال الجريمة.

2- **الإنابة القضائية:** ويقصد بها "طلب إتخاذ إجراء قضائي من الإجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوبة إليها، بهدف الفصل في مسألة معروضة على السلطة القضائية للدولة الطالبة ويتعذر عليها القيام به بنفسها". كما تنتج الإنابة القضائية عن الواجبات أو الإلتزامات التي يفرضها القانون الدولي العام على الدول، وبموجبها يعهد للسلطات القضائية المطلوب منها إتخاذ إجراء القيام بالتحقيق أو بالعديد من التحقيقات لمصلحة السلطة القضائية المختصة في الدول الطالبة، مع مراعاة إحترام حقوق وحريات الإنسان المعترف بها عالميا، ومقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة كالمثل وإحترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القانونية. وتهدف الإنابة القضائية إلى نقل الإجراءات في المسائل الجنائية لمواجهة ما تشهده الظواهر الإجرامية من تطور ناهيك عن طابع السرعة الذي تتطلبه الإجراءات المتعلقة بملاحقة الجريمة الإلكترونية سواء كان ذلك بواسطة الولوج عن بعد

[1] الأمم المتحدة (الجمعية العامة، الدورة الرابعة والسبعون، البند 109 من جدول الأعمال المؤقت، مكافحة إستخدام تكنولوجيا المعلومات والإتصال للأغراض إجرامية، تقرير الأهمية العامة، ص105.

في المنظومة المعلوماتية أو تقفي أثار المجرم الإلكتروني لضبط المعلومات محل الجريمة، كما أن الإنابة القضائية تجد أساسها في القوانين الوطنية وفي الإتفاقيات الدولية وفي مبدأ المعاملة بالمثل.

3- **تنفيذ الحكم الأجنبي:** من المفاهيم التي يجب تجاوزها لدعم أوامر التعاون الدولي، عدم قابلية الحكم الأجنبي للتنفيذ بحجة أن الحكم الجنائي في حقيقته مظهر لسيادة الدولة ويلحقها في توقيع العقاب، إلا أنه لا ينبغي أن يقتصر الأمر على ما يترتبه الحكم الجنائي الأجنبي من أثار سلبية مثل: عدم جواز محاكمة الشخص على الفعل الواحد مرتين. نتيجة تلك الجهود تم إبرام العديد من الإتفاقيات الدولية، لتنفيذ الأحكام القضائية بما فيها الأحكام الجنائية لوضع قواعد خاصة لتنفيذ الأحكام الأجنبية كعرض الحكم الأجنبي أمام جهة قضائية وطنية لمنحه الصيغة التنفيذية عندما يستنفذ كافة طرق الطعن ويكون غير مخالف للنظام العام حسب قانون القاضي الأمر بالتنفيذ.[1]

البند01: الصعوبات التي تعيق التعاون الدولي في مكافحة الجريمة الإلكترونية:

أثبت الواقع العلمي أن الدولة لا تستطيع وحدها وبمجهودها الخاص القضاء على الجرائم العابرة للحدود وبالأخص الجريمة الإلكترونية، لذا يعد التوافق بين السياسة الجنائية الداخلية والسياسة الجنائية الدولية مقدمة طبيعية لتحقيق نتائج إيجابية في مكافحة الجريمة العابرة لحدود والتي مثلت شبكة الأنترنت إحدى صورها المستحدثة مما يوجب تعاونا دوليا في مكافحتها نظرا لطابعها المتخطي للحدود دولية الواحدة والمتسمية بالبعد عبر الوطن، كما تواجه عملية مكافحة هاته الجريمة عدة صعوبات نذكر منها على سبيل المثال لا الحصر مايلي:

01. **عدم وجود نموذج موحد لنشاط الإجرامي:** فالأنظمة القانونية التي وضعت من أجل مكافحة الجرائم الإلكترونية يختلف وصفها للأفعال الإجرامية التي تتم بها هذه الجرائم، نظرا لإختلاف العادات والتقاليد والديانات والثقافات وغيرها من مجتمع لأخر، مما أنتج إختلافا في السياسة التشريعية وخاصة الجنائية منها، فقد نجد أنواعا من الجرائم الإلكترونية مباحة في نظم قانونية ومجرم في أخرى.

02. **تنوع وإختلاف النظم القانونية الإجرائية:** والمتمثلة خاصة في طرق التحري والتحقيق والمحاكمة كما هو الحال بالنسبة لطرق جمع الأدلة الإلكترونية فهذه الإجراءات قد تكون لها قيمتها القانونية في دولة وعدميتها في دولة أخرى.

[1] يزيد بوحلط، المرجع السابق، ص552-553-554.

03. **عدم وجود قنوات الإتصال:** من أهم الأهداف الموجودة في التعاون الدولي الحصول على معلومات وبيانات متعلقة بالجريمة الإلكترونية، ولتحقيق هذه الهدف كان لزاما أن يكون هناك نظام إتصال يسمح للجهات القائمة على التحقيق بالإتصال بالجهات الأخرى خاصة الأجنبية منها لتسهيل عملية جمع الأدلة والمعلومات المهمة والمطلوبة بخصوص المجرم المرتكب، ولكن غياب مثل هذا النظام يعني عدم قدرة على جمع الأدلة الإلكترونية والمعلومات التي تساعد على مكافحة الجريمة الإلكترونية والمجرم الإلكتروني.[1]

صعوبات متعلقة بالمساعدة القضائية الدولية: تتميز الجرائم الإلكترونية بأنها جرائم عابرة للحدود نتيجة إستعمال شبكة الأنترنت فإذا إرتكبت الجريمة عبر الأنترنت تزداد العقبات القانونية صعوبة، فلا نكون أمام مشكلات إجرائية تخص ضبط الجريمة وإثباتها فحسب، بل نجد أنفسنا أمام مشكلة أكثر تعقيدا تتمثل في تحديد الإختصاص القضائي المرتبط بتحديد القانون الواجب التطبيق على هذه الجريمة، على إعتبار أن قواعد الإختصاص القضائي التقليدية صيغت لكي تحدد الإختصاص المتعلق بجرائم قابلة للتحديد المكاني للجريمة، وهي قواعد ترتكز على مبدأ الإقليمية و هوما يرتبط بسيادة الدولة، فلا يكون الخروج عليه بقبول الإختصاص قضائي الأجنبي إلا في حالات إستثنائية يجب النص عليها صراحة. وعليه تعتبر المساعدات القضائية الدولية بمختلف صورها كالإبانة القضائية وتبادل المعلومات وتسليم المجرمين...إلخ. من أهم صور التعاون الدولي في مجال الجنائي، غير أنها تتم بالطرق الدبلوماسية مما يجعلها تتسم بالبطء والتعقيد، لذلك تتعارض مع طبيعة الجرائم الإلكترونية التي تتميز بالسرعة العالية في التنفيذ، إضافة إلى مشكل التماطل في الرد على طلبات المساعدة القضائية وتنفيذها بشروط معنية، أو بسبب نقص المواطنين المدربين أو نتيجة الصعوبات اللغوية والفوارق في طبيعية الإجراءات بين الدول التي تعقد الإستجابة في الوقت المناسب مما يتيح الفرصة لإفلات المجرم المعلوماتي وفقدان أثره في هذه البيئة الإفتراضية.[2]

4. صعوبات متعلقة بالتعاون الدولي في مجال التدريب:

رغم أهمية تدريب أعضاء الأجهزة القضائية في مجال البحث والتحري عن الجرائم الإلكترونية للكشف عنها وملاحقة مرتكبيها، إلا أن هناك بعض الصعوبات المتعرضة نوجزها فيما يلي:

---

[1] خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه، قانون جنائي، جامعة أحمد دراية، كلية الحقوق والعلوم السياسية، أدرار،2021/2020، ص 215-217.

[2] يزيد بوحليط، المرجع السابق، 2019، ص526.

- عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لإعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون.

- وجود فوارق فردية بين المتدربين وتأثيرها على عملية إكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الأفراد المتدربين، لاسيما في مجال تقنية المعلومات وشبكات الإتصال.

- النظرة السلبية للمتدرب إتجاه العملية التدريبية على أنها عبئ لا طائل منه، مما ينتج عنه عدم تحديد المعارف والخبرات خاصة في مجال مكافحة الجرائم الإلكترونية.

- عدم القدرة البيئة التدريبية على تمثيل الواقع العلمي لبيئة العمل الطبيعية تمثيلا تاما ومتقنا، من حيث ما يدور بها من وقائع وملابسات وإجراءات لا تبلغ حد التطابق مع طبيعة المهام التي سيقوم بها المدربون، خاصة أنها تتم في وسط إفتراضي.

- إرتفاع كلفة الدورات التدريبية مما لا يتيح لكثير من الدول تمكين أفراد أجهزتها القضائية لإستفادة منها.[1]

البند02: الحلول العلمية فيما يتعلق ببعض الإجراءات المتطلبة لمكافحة الجريمة الإلكترونية:

يطرح بعض الفقه "حلول عملية المواجهة تحديات ومشكلات الجرائم وتتمثل بالآتي:

1- لابد من إتخاذ وسائل الحيطة والحذر في تعامل البنوك مع الأنشطة المصرفية التي تتم عبر الأنترنت نظرا لأن تركيز غاسلي الأموال يتم على هذه البنوك، وبهذه الأساليب بإعتبارها مرتعا خصبا لتجارتهم خصوصا إذا كانت الدول التي ترعى هذه البنوك أو التي في ضيافتها تعاني من عجز في النظام الرقابي العام للدولة.

2- إصدار قوانين واضحة وصارمة تلزم جميع المصارف بوضع الخطوات العملية الضرورية لمنع غسل الأموال فيها خاصة تلك الأموال التي يتم التعامل بها عبر الأنترنت.

3- ضرورة قيام المصاريف بتدابير عملية من شأنها تكشف محاولات غسل الأموال فيها ومراقبة جميع التعاملات الإلكترونية.

[1] يزيد بوحليط، المرجع السابق، ص527.

4- ضرورة قيام المصاريف بإنشاء أجهزة أو إدارات تتولى مراقبة ومتابعة البلاغات في الدول التي تصلها عن أي عملية أو نشاط مشبوه، وبالتالي الإبلاغ عنها للجهات المختصة في الدولة خاصة إن كانت تلك العمليات المصرفية تتعلق بأنشطة تتم عبر الأنترنت.

5- ضرورة تدريب المحققين على القيام بالكشف عما تحتويه أجهزة الكمبيوتر من البرامج مخزنة عند الضرورة مما ييسر عمليات التفتيش التي تتم على الكمبيوتر المتهم.

6- ضرورة الإستعانة بخبراء في الكمبيوتر والشبكات أثناء عمليات التقصي والتحقيق في جرائم المعلوماتية والأنترنت.[1]

الفرع الثاني: المنظمة الدولية لشرطة الجنائية (الأنتربول):

تعد المنظمة الدولية لشرطة الجنائية (الأنتربول) من أقدم صور التعاون الشرطي في مكافحة الجريمة، ففي نهاية سنة 1923 نجح الدكتور "جوهانو سوبرا" مدير الشرطة فينا في عقد مؤتمر دولي ثاني على مستوى الدولي لشرطة الجنائية، وذلك في الفترة من الثالث إلى السابع من شهر سبتمبر عام 1923، ضم مندوبي تسع عشرة 19 دولة، وتمحض عنه ولادة لجنة دولية لشرطة الجنائية Internationnal criminal police commission ICPO حدد مقرها بفيانا، تعمل على التنسيق بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة، والتي أطلق عليها إسم المنظمة الدولية للشرطة الجنائية (الأنتربول) سنة 1956، حدد مقرها في مدينة ليون الفرنسية.

حيث تنقسم شبكة إتصالات الأنتربل إلى ثلاث مستويات هرمية: المكاتب المركزية الوطنية، المحطات الإقليمية والمحطة المركزية الموجودة في الأمانة العامة للأنتربول وتضم المنظمة الدولية للشرطة الجنائية (الأنتربول) حاليا حولي 194 بلدا عضوا. تستضيف كل دولة مكتبا مركزيا وطنيا للأنتربول NCB، يربط الشرطة الوطنية بشبكة الأنتربول العالمية.

البند الأول: مهام المنظمة الدولية لشرطة الجنائية الأنتربول:

للمنظمة الدولية للشرطة الجنائية الأنتربول عدة مهام كونها من أبرز المنظمات في مكافحة الجرائم الدولية العابرة للحدود في العالم، فقد وجدت الأنتربول لتحقيق عدة أمور منها:

[1] عبد الله دعش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، المرجع السابق، ص111.

أولا: التعاون الدولي لمواجهة الإجرام الدولي المتزايد بإستمرار

ثانيا: تأمين الإتصال الرسمي بين الرجال الشرطة في مختلف أرجاء العالم، بغية تبادل الخبرات والأفكار والمناهج وأساليب العمل في مجالات الأمن المختلفة منذ وجدت الدولة القومية (الوطنية) التي تفصل بينها الحدود الجغرافية والصناعية، وإرتباط الظهارة الإجرامية برغبة المجرم للإنتقال من كان إلى آخر إبتعاد عن مسرح جريمته وإختفائه عن نظر السلطات الأمنية، ولأجل تحقيق أهدافه تقوم الأنتربول بتجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم، من مختلف المكاتب المركزية الوطنية للشرطة الجنائية في دول الأعضاء، حيث تقوم المنظمة بعد تجميعها للبيانات والمعلومات بتنظيمها لتكون بها أرشيفا متكاملا يمكن الرجوع إليه عن الحاجة.

ومن المهام التي يقوم بها الأنتربول فيما يخص الجريمة الإلكترونية تعقب مجرمي المعلوماتية عامة وشبكة الأنترنت خاصة، وتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابرة للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الإتصال بحثا عن ما قد يحتويه من أدلة وبراهين على إرتكاب الجريمة المعلوماتية، إذ يتم تبادل المعلومات من خلال منصة الإتصالات الأمنية التي تعمل على مدار الساعة وطول أيام الأسبوع من أجل تسهيل التحقيقات المتعلقة بالجرائم الإلكترونية التي تجريها وكالات وزارة العدل ووزارة الأمن الوطني.

ومن المهام المهمة جدا والتي تقوم بها المنظمة الدولية للشرطة الجنائية (الأنتربول) عملية ضبط المجرمين أو توقيفهم مؤقتا إلى حين تسليمهم، وهذا إلى جانب قيامها بتنظيم دورات تكوينية لتبادل الخبرات وتقديم الدعم الفني لأجهزة الشرطة ومصالح الأمنية الدولية حتى يتسنى إعطاء بعد دولي لعمالها، وإقامة تبادل منظم للبيانات المتعلقة بالتهديدات الإلكترونية من أجل تعزيز أنشطة الأمن السيبراني الذي يطلع به الأنتربول ودوله الأعضاء، حيث قال "وانغ بينغ" الباحث في معهد شارهار بشنغهاي في إطار إختتام أعمال إجتماع الجمعية العامة 86 للشرطة الجنائية الدولية "الأنتربول" التي تمت بمشاركة نحو ألف شخصية من كبار قادة الشرطة والسياسيين من 156 دولة في العاصمة الصينية بكين: "إن الجرائم السيبرانية ذات طبيعة عابرة للحدود، وذلك يحتم على كافة الدول التعاون مع المنظمة الأنتربول الدولية، لوضع حد لهذه الظاهرة وهو ما تقوم به الصين الآن، حيث تمكنت في السنوات الأخيرة من إستعادة أكثر من 2000 متهم في إطار الحملة التي أطلقها الرئيس الصيني عام 2013، وعرفت باسم "مطاردة النمور" ومنوها بأن ذلك بفضل تعاون وتنسيق الصين مع الشرطة الجنائية الدولية.

البند الثاني: دور الإنتربول في مكافحة الجريمة الإلكترونية:

تمثل المنظمة الدولية للشرطة الجنائية (الأنتربول) همزة وصل بين مختلف أجهزة الشرطة عبر العالم، ومع المنظمات الإقليمية والدولية الأخرى من خلال موقعها الهام الذي يسمح لها بتعزيز قدرتها على منع الجريمة وتحديد هوية المجرمين وإعتقالهم، ولأن الجريمة الإلكترونية تعد إحدى أكبر التحديات التي تواجه مختلف دول العالم، فإن منظمة الأنتربول قامت ومازالت تقوم ببذل مجهودات من أجل مكافحتها، والأمثل على ذلك نذكر على سبيل المثال: ما حصل في الجمهورية اللبنانية، حين تلقت النيابة العامة اللبنانية برقية من الأنتربول في ألمانيا، تم على أثرها توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صورة إباحية لقاصر دون أعوام من موقعه على شبكة الأنترنت.

وفي إطار عملية نسقها الأنتربول في منظمة أسيا والمحيط الهادي سميت بـ: First Light 2015 شاركت فيها 23 بلدا، تم من خلالها إعتقال أكثر من 500 شخص وإغلاق 15 مركز للإتصال، إستهدفت هذه العملية أشخاص قاموا بعمليات إحتيال إرتكبت بواسطة الهاتف والبريد الإلكتروني قدرت قيمتها بملايين الدولارات.

وفي سنة 2016 قام الأنتربول والهيئة النيجيرية للجرائم الإقتصادية والمالية في إطار عملية مشتركة بالقبض على زعيم شبكة الإجرام دولية، في نيجيريا إسمه "مايك" إشترك معه مالا يقل عن أربعين 40 شخصا من ماليزيا وجنوب إفريقيا قاموا بآلاف عمليات الإحتيال عبر الأنترنت والتي تستهدف مئات الضحايا في جميع أنحاء العالم مستعملين مختلف مخططات الإحتيال التجاري عبر البريد الإلكتروني.[1]

المطلب الثاني: الإتفاقيات الدولية المتعلقة بمكافحة الجريمة الإلكترونية:

تعد المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، فقد بات من المؤكد أن جرائم تكنولوجيا المعلومات هي جرائم عابرة للحدود أي أنها لا تتم وتنتهي في أراضي دولة بعينها فالتعاون الدولي هو أهم سبل مكافحة جرائم الأنترنت وملاحقة مرتكبيها وبالتالي فالمعاهدات الدولية التي تنظم إليها العديد من الدول هي النموذج الذي يكون هذا التعاون الدولي.

[1] شنتيرة خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)،المرجع السابق، ص208 إلى 213.

الفرع الأول: أهم الإتفاقيات والصكوك الخاصة بالجريمة المعلوماتية:

مع تطور تقنية المعلومات، وإهتمام الأنظمة الدولية بموضوع الجرائم المعلوماتية وقعت العديد من الصكوك المواثيق الدولية من طرف دولة أدركت فعلا مدى الخطورة التي تشكلها هذه الجريمة، بوصفها من الجرائم العابرة للحدود، فقد يكون الجاني في بلد والمضرور في بلد آخر.

بند01: القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء هافانا 1990 بشأن الجرائم ذات الصلة بالكمبيوتر.

يعد هذا القرار من الجهود الذي بذلتها الأمم المتحدة حيث عقد هذا المؤتمر في هافانا سنة 1990 حيث حث في قراراه المتعلق بالجرائم ذات الصلة بالكمبيوتر الدول الأعضاء وأن تكثف جهودها لمكافحة إساءة إستعمال هذا الجهاز وبتجريم تلك الأفعال جنائيا، وإتخاذ الإجراءات التالية متى دعت الضرورة لذلك:

- ضمان أن الجزاءات والقوانين الراهنة بشأن سلطات التحقيق والإدانة في الإجراءات القضائية تنطبق على نحو ملائم، وإدخال تغيرات مناسبة عليها إذ دعت الضرورة لذلك.
- النص على الجرائم والجزاءات والإجراءات تتعلق بالتحقيق والأدلة حيث تدعوا الضرورة للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو ملائم.

كما حث أيضا الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على صعيد الدولي من أجل مكافحة الجرائم المتصلة بالكمبيوتر بما في ذلك دخولها كأطراف في المعاهدة المتعلقة بتسليم المجرمين وتبادل المساعدات في المسائل الخاصة المرتبطة بهذه الجريمة، ونصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات صلة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية تنطبق بكل ما هو تام على الأشكال الجديدة للإجرام مثال الجرائم الإلكترونية، وأن تتخذ خطوات محددة نحو تحقيق الهدف.

كما تكمل الأمم المتحدة رؤيتها بشأن الجريمة المعلوماتية بصفة عامة بضرورة وضع أو تطوير:

1. معايير دولية لأمن المعالجة الآلية للبيانات.
2. إتخاذ تدابير ملائمة لحل الإشكالية الإختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود أو ذات الطبيعة الدولية.

3. إبرام إتفاقية دولية تنطوي على النصوص تنظيم وإجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت ذاته لحقوق الأفراد وحرياتهم وسيادة الدول.[1]

بند 02: معاهدة بودابست لمكافحة الجرائم الأنترنتBudapest :

لما كانت شبكة الأنترنت لا تخضع لأية حدود ولا سيادة الدولة وبالتالي للسيادة القانونية لدولة معينة ظهرت الجرائم الإلكترونية على الصعيد الدولي فمرتكبي الجريمة يكون في دولة مختلفة عن الدولة التي تقع فيها جريمته وأصبحت الجرائم منظمة Organised crime الأمر الذي حدا بالمشرع الدولي للبحث عن إطار قانوني دولي يكون فيه التعاون بين الدول أمريكا يكون ليس إختياريا لإيجاد حل لهذه الجرائم الحديثة.[2]

فقد شهدت العاصمة المجرية بودايست في أواخر عام 2001، أول المعاهدات الدولية التي تكافح الجرائم الأنترنت وتبلور التعاون الدولي في محاربتها ومحاولة الحد منها خاصة بعد أن واصلت تلك الجرائم إلى حد خطير حيث أصبحت تهدد الأشخاص والممتلكات وبعد توقيع على تلك الإتفاقية من مسؤولين في الدول الأوروبية إضافة إلى أمريكا واليابان وكندا وجنوب إفريقيا هو نتائج مباحثات ومفاوضات إستغرقت ما يزيد عن أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لتلك الإتفاقيات حتى يتم التوقيع عليها من طرف جميع الأطراف دون إعتراض.[3]

البند 03: إتفاقية برن الدولية لحماية المصنفات الأدبية والفنية:

يهدف حماية حقوق المؤلفين على مصنفاتهم الأدبية بأكثر الطرق فعالية تم إبرام إتفاقية برن الدولية في 09 سبتمبر 1886، والمكملة بباريس في ماي 1896، والمعدلة في برلين في 13 سبتمبر 1908، والمكملة في 20 مارس 1914، والمعدلة بروما في جوان 1928، وبروكسل سنة 1948، وإستوكهم لهم في جويلية 1967، وباريس في جويلية 1971، حيث تشكل الدول الأطراف في هذه الإتفاقية إتحاد لحماية حقوق المؤلفين على مصنفاتهم الأدبية والفنية.

---

[1] ليندة شربشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية الإتجاهات الدولية في مكافحة الجريمة الدولية، المركز الجامعي سوق أهراس، ص244-245.

[2] وليد طه، التنظيم التشريعي للجرائم الإلكترونية في إتفاقية بودايست، عضو قطاع التشريع بوزارة العدل جمهورية مصر العربية، ص15.

[3] سليمة سعيدي وبلال حجاز، جرائم المعلومات وشبكات في العصر الرقمي، المرجع السابق، ص146.

وبموجب إتفاقية برن الدولية تتمتع برامج الحاسب الآلي "الكمبيوتر" سواء كانت بلغة المصدر أو بلغة الآلة بالحماية بإعتبارها أعمالا أدبية وفقا لما جاء فيها المتعلقة بالجوانب المتصلة بالتجارة الدولية حيث تسعى الدول "TRIPIS" إضافة إلى إتفاقية الأطراف في الإتفاقية إلى تشجيع الحماية الفعالة وملائمة لحقوق الملكية الفكرية من أجل التخفيف العراقيل التي تعوق التجارة الدولية.[1]

الفرع الثاني: نماذج عن الجريمة الإلكترونية على مستوى الدولي:

تتنوع الجريمة الإلكترونية وتأخذ أشكالا مختلفة نجدول التطرق إليها على سبيل المثال مع تدعيمها ببعض الأمثلة من دول العالم:

بند01: جرائم التجسس الإلكتروني وجرائم القرصنة:

جرائم التجسس الإلكتروني: يعتمد هذا النوع من الجرائم على التقنيات عالية التقدم حيث لم يعد يقتصر التجسس على ما يتعلق بالمعلومات العسكرية والسياسية بل يتعداه إلى المجال الإقتصادي والتجاري والثقافي ولقد ظهر هذا النوع من الجرائم خصوصا بعد أحداث الحادي عشر من سبتمبر التي شهدتها الولايات المتحدة الأمريكية، ومن الأساليب المعتمدة أسلوب إخفاء المعلومات داخل المعلومات بحيث يتم إخفاء تلك المعلومات المهمة والمستهدفة داخل معلومات عادية في جهاز الحاسب الآلي ومن ثم يتم تهريبها بإستعمال أساليب متطورة لا يتم إكتشافها ولو ضبط الشخص متلبسا ومثال ذلك قيام شبكة دولية ضخمة للتجسس الإلكتروني التي تعمل تحت إشراف وكالة الأمن القومي الأمريكية بالتعاون مع أجهزة الإستخبارات في كندا وبريطانيا لرصد على المحطات الموجهة إلى الأقمار الصناعية والشبكات الدولية بل يشمل الاتصالات التي تجري عبر أنظمة الإتصالات الأرضية.

جرائم القرصنة: إتسعت وتطورت صور القرصنة من خلال العثور على مواقع الإنترنت لترويج البرامج المقرصنة مجانا أو بمقابل مبلغ رمزي مما ألحق العديد من الخسائر المادية الباهظة مما أدى بالشركات

[1] ليندة شربشة، المرجع السابق، ص 246.

المتخصصة في صناعة البرامج إلى إنشاء منظمة خاصة لمراقبة وتحليل ما يعرف بسوابق البرمجيات، ومنها منظمة إتحاد برمجيا الأعمال التي أجريت دراسة حول ذلك وتبنت الحلول المناسبة.

ومثال ذلك تعرض أنظمة تشغيل مايكروسوفت لبرامج الكمبيوتر لعملية قرصنة مستعملين في ذلك عامل ذكي لبرامج الكمبيوتر يمكن التجول بحرية عبر الشبكات لإلتقاط المعلومات ونقلها دون قيام المتسلل بإختراق الكمبيوتر نفسه، حيث تم فتح تحقيق في هذا المجال.

كما تم أيضا إرسال فيروسات لتخريب الجهاز ومحتوياته حيث بمجرد كتابة كلمة أو فتح البرنامج الحامل للفيروس، والرسالة البريدية المرسل معها الفيروس تتم إصابة الجهاز ومن ثم يقوم بمسح محتوياته أو العبث بالملفات الموجودة فيه.[1]

البند 02: جرائم الإرهاب الإلكتروني والجرائم المنظمة:

جريمة الإرهاب الإلكتروني:

مفهوم الإرهاب الإلكتروني: المقصود بالإرهاب هو إستخدام التقنيات الرقمية لإخافة وإخضاع الأخرين، أو هو القيام بمهاجمة نظم المعلوماتية على خلفية دوافع سياسية أو عرقية أو دينية.

مفهوم الجريمة الإرهابية الإلكترونية: هي نوع من الإرهاب الحديث الذي وظف وإستثمر تقنيات المعلومات والإتصالات بشكل يلائم متطلباته، وأهدافه وذلك بغرض إثارة الخوف وزعزعة إستقرار المجتمعات في تنفيذ التخطيط للعمليات الإجرامية الإرهابية على وسائل الإتصال الإلكتروني.

لقد أصبحت التنظيمات الإرهابية في السنوات الأخيرة تمتلك قدرة كبيرة في توظيف المسائل التكنولوجية حيث أصبح إستخدام مصطلح "الإرهاب التكنولوجي" موضوعيا إلى أبعد الحدود، كما تم توضيح الدراسات التي نشرها مركز الأبحاث لدراسات الصراع والإرهاب في لندن بعنوان: التكنولوجيا والإرهاب؛ التهديد الجديد للألفية الجديدة والتي كتبها كل من ستيفن أرباورز–وكمبرلي أركيز، حيث أكدت هذه الدراسة أن التنظيمات الإرهابية أصبح بإمكانها حاليا الحصول على كل ما تريد من المعلومات عبر إستخدام المتقن للكمبيوتر، من خلال إستغلال ثغرات شبكات المعلومات أو اللجوء إلى عمليات القرصنة المعلوماتية والدخول إلى بنوك

[1] ليندة شربشة، المرجع السابق، ص242،243.

المعلوماتية العسكرية والأمنية للدول، وإستغلالها في تخطيط للعمليات الإرهابية، كما يمكنها أيضا الدخول إلى الشبكات البورصية والأسواق المالية وتدميرها بقصد المساس بالقوة الإقتصادية لدول المستهدفة.[1]

كما دعت منظمة الأمم المتحدة للدول الأعضاء في مؤتمرها الثامن المتعلق بمنع الجريمة إلى ضرورة إتخاذ إجراءات فعالة لمحاربة الجريمة الإرهابية الإلكترونية، وذلك من خلال العمل على تحديث القوانين والتشريعات من جهة، وتفعيل التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة من جهة ثانية، وذلك في ظل مراعاة حريات وحقوق الإنسان الأساسية وإشتراك المجتمع المدني في محاربة مثل هذه الجرائم، وتدعم هذا المؤتمر بإتفاقية أخرى عقدتها هيئة الأمم المتحدة سنة 2000، والتي حملت عنوان " مكافحة إساءة إستعمال التكنولوجيا لأغراض إجرامية".

الجرائم المنظمة:

يتبادر إلى الذهن فور التحدث عن الجريمة المنظمة عصابات المافيا كون تلك العصابات من أشهر المؤسسات الإجرامية المنظمة والتي بادرت بالأخذ بوسائل التقنية الحديثة سواء من حيث تنظيم أو تنفيذ أعمالها، ومن ذلك إنشاء مواقع خاصة بها على شبكة الأنترنت لمساعدتها في إدارة العمليات وتلقي المراسلات وإصطياد الضحايا وتوسيع أعمال وغسيل الأموال كما تستخدم تلك المواقع في إنشاء مواقع إفتراضية تساعد المنظمة في تجاوز قوانين بلد محدد بحيث تعمل في بلد آخر يسمح بتلك الأنشطة.

ويوجد على الشبكة (210) مواقع تحتوي على إسم نطاقها على كلمة مافيا، في حين يوجد (24) موقعا يحتوي على كلمة مافيا، كما وجد (04) مواقع مافيا يهودية، وقد خصص بعض هذه المواقع للأعضاء فقط ولم يسمح لغيرهم بتصفح تلك المواقع في حين سمحت بعض المواقع للعامة بتصفح المواقع وقامت أخرى بوضع إستمارة تسجيل لمن يرغب في الإنظمام إلى العصابة من أعضاء جدد، والجريمة المنظمة ليست وليدة التقدم وإن كانت قد إستفادت منه.[2]

[1] نصير لعرباوي وفاتح النور رحموني، الجريمة الإرهابية الإلكترونية، المعيار 43، جانفي 2018، ص 379-380-383-384.

[2] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الأنترنت، المرجع السابق، ص82-83.

ولما كانت الجريمة المنظمة هي إحدى الظواهر الاجتماعية التي تهدد الأمن العام في الدولة، فإن الجريمة الإرهابية ظاهرة سياسية تهدد النظام الاجتماعي بمفهومه العريض ويهدف الإرهاب إلى تحقيق أهداف سياسية بينما الجريمة المنظمة هي عنف منظم بقصد الحصول على مكاسب مالية بطرق وأساليب غير مشروعة.[1]

المبحث الثاني: مكافحة الجريمة الإلكترونية على مستوى التشريعات الوطنية:

إن المعلوماتية وبرامج الحاسب الآلي أصبحت تهيمن على الكثير من جوانب حياتنا المعاصرة في أبعادها الإقتصادية والثقافية والإجتماعية، وباتت تشكيل ثروة تقنية وصناعية وفكرية عالية مما يستدعي التدخل لحمايتها على الصعيد الوطني، فالواقع العلمي يكشف عن بيئة ضخمة ومعقدة يصعب إحكام قبضة الأمن والمراقبة والتحكم بشأنها، حيث تزدهر عمليات القرصنة الفكرية وسرقة المعلومات المعالجة إلكترونيا والأموال والإعتداء على حقوق ومصالح وقيم مشروعة للغير، وتخريب البرامج وتدمير المواقع وبث الأمور التي تهدد الأمن وتخدش الحياء العام بما يسيء إلى قواعد النظام العام وحسن الأدب لكل ذلك كان التدخل التشريعي لتجريم تلك الأفعال مما يثير المسؤولية الجنائية.[2]

المطلب الأول: الأجهزة المكلفة بالبحث والتحري في الجريمة الإلكترونية:

نظرا لتفاقم الظاهرة الإجرامية المعلوماتية من يوم لأخر ونظرا إلى الطبيعة الخاصة التي تتميز بها هذه الجرائم، كان من الضروري تطوير أجهزة الشرطة القضائية لتواكب التطور الحاصل في مجال الجريمة الإلكترونية (المعلوماتية)، لهذا عمدت معظم الدول إلى إستحداث وحدات خاصة لمكافحة هذا النوع من الجرائم.

ففي الجزائر تم تسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال إضافة إلى وحدات قضائية تابعة لسلك الأمن والدرك الوطني.

---

[1] شيماء حليفة، الإستراتيجية الأوروبية في مكافحة الجريمة المنظمة 2018/2001، مذكرة الماستر تخصص إستراتيجية وعلاقات دولية، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2019/2018، ص15.

[2] محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، 2007، ص29-30.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها:

في إطار الإصلاحات التي تنتهجها الجزائر مؤخرا ذات طابع القانوني والأمني والسياسي وإصلاح العدالة لتعزيز دولة القانون ومكافحة الجريمة الإلكترونية، أصدرت عدة قوانين والتي تم من خلالها إنشاء مصالح والهيئات تضم مجموعة من الموارد البشرية والإمكانيات المادية والتقنية والتي تسهل عملية البحث عن مرتكبي الجرائم الإلكترونية، وتمكن من القبض عليهم وتسليمهم للجهات القضائية المختصة الوطنية منها أو الدولية، ومن بينها: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

فبموجب المادة 13 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، نص المشرع على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.[1] والتي كانت محط أنظار العديد من وسائل الإعلام التي تحدثت عنها، ولكن بعدها إختفت أخبارها، حتى إعتقد الجميع أنها ستبقى حبرا على ورق كغيرها من الكيانات القانونية والتي مصيرها البقاء حبيسة المواد والنصوص القانونية، إلا أنه وفي 08 من شهر أكتوبر 2015 تم إصدار مرسوم رئاسي 15-261.[2]

وعلى غير العادة قام المشرع الجزائري بعدها بأربعة سنوات تقريبا بإصدار مرسوم رئاسي آخر تحت رقم 19-172 والخاص بتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها وتنظيمها وكيفية سيرها، والذي يتكون من خمس وعشرين 25 مادة نصت المادة الرابعة والعشرون 24 منه على إلغاء المرسوم الرئاسي 15-261 الصادر في 2015 السالف الذكر.[3]

---

[1] جاء في المادة 13 من قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، السالف الذكر أنه: "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بالإعلام والإتصال ومكافحتها، تحديد تشكيلتها وتنظيمها وكيفية سيرها عن طريق التنظيم".

[2] المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 24/2015 ذوالحجة 1436؛ الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المنشور بالجريدة الرسمية، عدد53، بتاريخ 08أكتوبر 2015، ص16 (الملغى).

[3] نصت المادة 24 من المرسوم الرئاسي 19-172 الذي يحدد تشكيلة الهيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها، السالف الذكر على إلغاء جميع أحكام مخالفة لهذا المرسوم لاسيما أحكام المرسوم الرئاسي 15-261 المؤرخ في 2015/10/08 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

تم بعد حوالي 13 شهرا قام المشرع بإصدار مرسوم رئاسي تحت رقم 20-183 والمتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وكافحتها، متكون من 38 مادة، ألغت المادة 37 من المرسوم الرئاسي رقم 19-172 السالف الذكر.[1]

أولا: تعريف الهيئة المخصصة في البحث والتحري عن الجرائم الإلكترونية:

الهيئة المتخصصة في مجال مكافحة الجريمة المعلوماتية هي وحدات تستند مهامها الوقاية ومكافحة الجرائم الإلكترونية بالنظر إلى تشكيلتها البشرية الخاصة التي تضم محققين من نوع خاص تجمع لديهم صفة الشرطة القضائية إضافة إلى المعرفة الواسعة بالنظم المعلوماتية والمجرم الإلكتروني.[2]

الهيئة الوطنية تعد السلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرية يترأسها وزير العدل، وتظم أساسا أعضاء من الحكومة معنيين بالموضوع، ومسؤولي مصالح الأمن وقضائيين إثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

أما فيما يخص تشكيلها قد نص عليه المادة الثالثة[3] من المرسوم 19-127 "تنظم الهيئة من مجلس التوجيه ومديرية عامة" حيث يترأس مجلس التوجيه وزير الدفاع الوطني أو ممثله ويتشكل من ممثلي الوزرات الآتية: وزارة الدفاع الوطني، وزارة المكلفة بالداخلية وزارة العدل، الوزارة المكلفة بالمواصلات السلكية واللاسلكية وتتولى المديرية العامة أمانة المجلس فحين تضم المديرية العامة: مديرية للإدارة والوسائل والمصالح.[4]

بعدما كانت تضم هذه الهيئة حسب المادة 06 من المرسوم 15-261[5] الذي يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، لجنة مديرية

---

[1] تنص المادة37 من مرسوم رئاسي 20-183 مؤرخ في 13يوليو2020 المتضمن إعادة تنظيم الهيئة الوطنية لوقاية من جرائم المتصلة بتكنولوجيا الإعلام والإتصال وكافحتها، الصادر جريدة الرسمية رقم40 مؤرخ في18يوليو2020، أنه "تلغى جميع أحكام مخالفة لهذا المرسوم، لاسيما أحكام مرسوم رئاسي 19-172 مؤرخ في06يونيو2019 الذي حدد تشكيلة الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام وافتصال وكافحتها وتنظيمها وطرق سيرها.

[2] محمد بوعمرة سيد علي ينينال، المرجع السابق، ص31.

[3] المادة 03 من المرسوم 19-127.

[4] المادة 05 و10 من المرسوم 19-127.

[5] المادة 06من المرسوم15-261 المؤرخ في08أكتوبر2015، الذي يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات الإعلام وافتصال ومكافحتها، جريدة رسمية عدد 53.

ومديرية عامة ومديرية للمراقبة الوقائية واليقظة الإلكترونية ومديرية التنسيق الإلكتروني ومركز للعمليات التقنية وملحقات جهوية حيث يترأس اللجنة المديرية الوزير المكلف بالعدل[1].تعرف أحكام المواد من 01 إلى04 من القانون 09-04 بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والإستغلال المالي توضع لدى وزير المكلف بالعدل ويقع مقرها بالجزائر العاصمة.

ثانيا: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال:

من مهام الهيئة الوطنية تفعيل التعاون القضائي والأمن الدولي وإدارة وتنسيق عمليات الوقاية ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية.

هناك الحالات التي تسمح بمراقبة الاتصالات الإلكترونية لأغراض وقائية كالوقاية من جرائم الإرهاب والجرائم الماسة بأمن الدولة بإذن النائب العام لدى مجلس قضاء الجزائر لمدة ستة أشهر قابلة لتجديد والوقاية من الإعتداءات على المنظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية كالإقتصاد الوطني بإذن السلطة القضائية.[2]

- تنص المادة 14 من نفس القانون على أنه: "تتولى الهيئة المذكورة في المادة 13 خصوصا المهام التالية:

- تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعطيات المقيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وتحديد مكان تواجدهم.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

[1] حليمة حوالف، معالم الجريمة المعلوماتية في القانون الجزائري، مجلة البحوث القانونية السياسية، العدد16، ص 152،146.

[2] عدلية مراد وروان عبدلي، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، قانون جنائي، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، 2021/2020، ص79.

ثالثا: إختصارات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال:

بينت الفقرة 02 من المادة 04 من المرسوم الرئاسي 15-261[1] المهام الأساسية التي تكلف بها الهيئة وهي على سبيل الحصر، الهدف منها هو الوقاية من الجرائم الإلكترونية ومكافحة هذه الأخيرة من خلال الإسهام في الأعمال البحث والتحقيق ومد يد العون لمصالح الشرطة القضائية ومن أبرز مهام هذه الهيئة:

- إقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.
- تنشيط وتنسيق عمليات الوقاية عن الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.
- مساعدة السلطة القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدتها بالمعلومات والخبرات القضائية.
- ضمان المراقبة الوقائية للإتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والماسة بأمن الدولة وذلك تحت سلطة القاضي المختص بإستثناء أي هيئات وطنية أخرى.
- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل إستعمالها في إجراءات القضائية.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال إختصاصها.
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال.
- المساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والإتصال.
- المساهمة في تحديث المعايير القانونية في مجال إختصاصها.[2]

---

[1] المرسوم الرئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية عدد53، بتاريخ 08 أكتوبر 2015.

[2] يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر أكاديمي، قانون جنائي، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، 2017/2016، ص 19-20.

الفرع الثاني: وحدات الأمن الوطني المتخصصة في مكافحة الجريمة الإلكترونية:

إن مكافحة الجريمة الإلكترونية أضحت من بين أولويات الدولة الجزائرية إذ لابد من الإستجابة للإنشغالات الأمنية المتزايدة والمحافظة على الطمأنينة والأمن العمومي في الفضاء الإلكتروني، أو كما يسمى الفضاء الأزرق، لأجل ذلك فقد خصصت الدولة الجزائرية عدة وحدات مختصصة لمكافحة هذه الجريمة، فمنها المتواجدة في مؤسسة الشرطة (البند01) وأخرى في مؤسسة الدرك الوطني (البند02) وتفصيلهما كما يلي:

البند01: الشرطة الجزائرية ودورها في مكافحة الجريمة الإلكترونية:

إن من بين الأهداف الإستراتيجية التي تهدف مؤسسة الشرطة القيام بها هي كشف الجريمة والقبض على مرتكبيها والوقاية والحد منها، وحماية الحريات وصون الحقوق، والإستعداد لمواجهة الأزمات والكوارث بفعالية من أجل الضبط الجيد للأمن وحفظ النظام العام، وأداء جميع المهام المسندة للأمن الوطني كما حددها التشريع والتنظيم المعمول بهما[1]، ففي سبيل المكافحة الفعالة للجريمة الإلكترونية خصص الأمن الوطني موارد بشرية متخصصة[2]، من خلال تعزيز صفوفه بضباط ذوي خلفيات جامعية عالية المستوى في ميادين العلوم الإنسانية والإجتماعية على الخصوص تستفيد من تدريبات عالية المستوى في العلاقات العامة وإدراة عمل الفرق الشرطية والتعامل مع الحالات الخاصة في صفوف المنحرفين والمجرمين، كما خصص الأمن الوطني موارد هيكلية وتنظيمية لمحاربة الجريمة الإلكترونية كمديرية الشرطة القضائية[3] والمصالح المركزية لمكافحة الجريمة الإلكترونية التابعة لمديرية الأمن الوطني، والتي تم إنشاءها بقرار من المدير العام للأمن الوطني سنة 2015، حيث كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني على مستوى المديرية العامة للأمن الوطني تم إنشاءها سنة 2011، لأن الجريمة الإلكترونية في تطور مستمر تم الإنتقال إلى المرحلة الثانية، حيث تم توسيع التشكيل الأمني بتكوين فصائل على مستوى 48 ولاية تابعة للمصالح الولائية القضائية بأمن الولايات.

---

[1] المادة02 من المرسوم التنفيذي 10-322 المؤرخ في 22 ديسمبر 2010، المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني الصادرة بالجريدة الرسمية، عدد78 بتاريخ 26 ديسمبر 2010، ص04.

[2] حسب المادة 109 من المرسوم التنفيذي 10-322 المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني، المرسوم نفسه، فإنه من بين المناصب العليا في الأسلاك الخاصة التبعة للأمن الوطني، أشخاص تابعين للشرطة التقنية والعلمية والمكلفون بتقديم خبرة في مجال الجرائم إلكترونية، كما يوجد مدربين ومكونين لضمان التكوين الجيد وتجديد المعلومات وتحسين مستوى التقنيين والبيداغوجي للمتدربين.

[3] تتمثل مهام مدرية الشرطة القضائية في تنشيط وتنسيق وتوجيه المصالح المكلفة بمعاينة مخالفات ق ع وكذا جمع ادلة والبحث عن المجرمين طالما لم يتم فتح تحقيق من قبل جهات قضائية "معلومات متاحة على موقع إلكتروني لمديرية الأمن الوطني الجزائري: www.algeriepolice.dz .

ومن الأمثلة على ما قامت به هذه الفصائل لأجل مكافحة الجريمة الإلكترونية، القضية التي عالجتها فرقة مكافحة الجرائم الإلكترونية بالمصالحة الولائية للشرطة القضائية لأمن ولاية عين الدفلى، والمتعلقة بالغش في إمتحانات شهادة التعليم المتوسط دورة جوان 2019 بواسطة الوسائط الاجتماعية، حيث أسفرت التحريات التقنية التي باشرتها عناصر الفرقة، وبالتنسيق مع المصالحة المركزية لمكافح الجرائم الإلكترونية بمديرية الشرطة القضائية وبإشراف الهيئات القضائية على توقيف ثلاثة أشخاص وتقديمهم للعدالة.

ومن أجل مواكبة التطور التكنولوجي والرفع من مستوى المعرفي والمهاري والأدائي للمحققين تم إستحداث صنفين من التكوين المتخصص:

الصنف الأول: محقق في الجريمة المعلوماتية "ICC" خاص بإطارات ومفتشي المصالح المحققة في مجال الجريمة المعلوماتية.

الصنف الثاني: متدخل أول في الجريمة المعلوماتية "PICC"، خاص بأعوان الشرطة العاملين في مجال مكافحة الجريمة المعلوماتية، كما يقوم الأمن الوطني بتأهيل وإعداد الكفاءات العلمية المؤهلة لمواجهة هذا النوع من الإجرام وذلك بتطوير العملية التدريبية لرفع مستوى الأداء لتلبية الإحتياجات الأمنية الحالية والمستقبلية، لذا قامت المنظمات الحكومية ومنظمات الشرطة في بعض بتدريب رجالها وتكوينهم.

وفي سنة 2017، تم إستحداث معهد الدراسات العليا في الأمن الوطني بموجب المرسوم الرئاسي 17-145 والذي تم إلغاءه سنة2019 بموجب المرسوم الرئاسي 19-278، حيث نصت بعض مواده على المهام المسندة لهذا المعهد ومنها أنه يضمن تكوينات جامعية في الدرجتين الثانية والثالثة في الأمن الوطني وفي الدراسات الإستراتيجية والعلاقات الدولية، كما يمكنه أن يقدم تكوينات متواصلة مؤهلة، الأكاديمية منها والمتخصصة، والتي تخصصت لفائدة المستخدمين العسكريين والمدنيين، والوطنيين والأجانب، ويعمل المعهد على القيام بدراسات وبحوث في اليقضة الإستراتيجية والإستشرافية في مجالات الأمن والدراسات الإستراتيجية والعلاقات الدولية والتكنولوجيات العسكرية والأمن السيبراني ووسائل الإعلام والإتصال والتنمية الإقتصادية والإجتماعية الثقافية[1]، إضافة إلى تنظيمه دورات تكوين حسب الطلب وملتقيات ومحاضرات وأيام دراسية وطنية وأجنبية في مواضيع ذات علاقة بمجال إختصاصه لفائدة إطارات وطنية وأجنبية[2]، حيث نجد مساهمة

[1] المادة 08 من نفس المرسوم الرئاسي.

[2] المادة 09 من نفس المرسوم الرئاسي.

هذه المعاهد على أرض الواقع جلية فالمعهد الوطني للشرطة الجنائية منذ 2014 إلى يومنا هذا ساهم في تكوين 152 إطار شرطة من الدول الشقيقة، لاسيما تونس، فلسطين، ليبيا، أوغندا، السودان، النيجر، البنين، وكينيا.

ولأن النتائج التي توصلت إليها الشرطة الجزائرية في مكافحة الجريمة الإلكترونية لا بأس بها، فقد كان ذلك محطة إشادة من بعض الشخصيات، ومنها ما ورد في تصريح السيد "مانغ هانغواي Meng Hongwei" رئيس منظمة الأنتربول خلال زيارة العمل التي قام بها للجزائر في شهر ماي سنة 2018، حيث أشاد بالتقدم الذي أحرزه الجهاز الشرطي الجزائري، وما وصلت إليه الشرطة الجزائرية من تطور وإحترافية ودعا إلى تعزيز التعاون وتفعيل الآليات تبادل الخبرات المعلوماتية من أجل ضمان فعالية أكثر في مواجهة جميع أشكال الجرائم المستحدثة وبالأخص الجريمة الإلكترونية.

البند02: الدرك الوطني ودوره في مكافحة الجريمة الإلكترونية:

يعد الدرك الوطني من بين قوات الأمن الفاعلة في مكافحة الإجرام عموما والجريمة الإلكترونية خصوصا، وذلك من خلال ماله من إمكانيات بشرية ومادية مخصصة لهذا الغرض، فمكافحة الجريمة الإلكترونية أضحت من بين أولويات الدولة الجزائرية، وذلك في إطار الإستجابة للإنشغالات الأمنية المتزايدة والمحافظة على الطمأنينة والأمن العمومي في الفضاء السيبراني الوطني، فالبداية الفعلية لمحاربة قيادة الدرك الوطني للجريمة الإلكترونية، كانت في سنة 2004، ليتم بعدها إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها والذي يعد اليوم العصب الذي يسير مهام المكافحة واليقظة وفرض إحترام القوانين في الوقت الذي يبحر فيه الملايين من المستخدمين عبر صفحات الأنترنت سواء في الخواص أو المؤسسات في الفضاء الإلكترونية.

لقد عمل المركز سالف الذكر منذ إنشاءه سنة 2008 على تأمين منظومة المعلومات لخدمة الأمن العمومي، حيث يهدف ضباط وأعوان الشرطة القضائية المؤهلين في الدرك الوطني إلى تطبيق القوانين وجمع الأدلة وتحليل معطيات وبيانات الجرائم الإلكترونية المرتكبة والبحث عن مرتكبي الجرائم عموما، وتحديد هوية أصحابها سواء أكانوا أشخاص فرادى أو عصابات ويعمل المراكز على المساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها في هذا الخصوص، كما إستطاع المراكز معالجة أزيد من 100 جريمة إلكترونية سنة 2014، وما يفوق 500 قضية رقمية خلال سنة 2015، منها 300 جريمة تتعلق بمواقع التواصل الاجتماعي "فايسبوك" و 20 جريمة رقمية تعلقت بإختراق مواقع رسمية لمؤسسات خاصة وعامة إستهدف

مجرموها أنظمة المعالجة الآلية للمعطيات، وفي الخمسة أشهر الأولى من سنة 2019، تم معالجة 1188 قضية بنجاح مجموع 1515 قضية مسجلة مع توقيف 1512 متورط، ولأن الأطفال هم أكثر الفئات العمرية تضررا من الجريمة الإلكترونية فقد قامت قيادة الدرك الوطني بمجموعة من البرامج التوعوية بالتنسيق مع وزارة التربية الوطنية من خلال دروس التوعية في المدارس التي جربت فيها تلك البرامج لخطوة الأولى نحو زيادة وعي الطلاب بمخاطر الجريمة الإلكترونية وحمايتهم منها.

ولأن عملية مواكبة التطورات والمستجدات الحاصلة في مجال التكنولوجيات الحديثة، أمر لابد من السعي لتحقيقه في سبيل تقديم خدمات أمنية ترقى إلى تطلعات المواطنين، عمل جهاز الدرك الوطني على تكوين الإطارات وأعوان الدرك الوطني بشكل متواصل، وذلك من خلال إنشاء مدارس ومعاهد لهذا الغرض كمدرسة الشرطة القضائية التابعة للدرك، والمعهد الوطني للشرطة القضائية بالمحاولة، والذي تم إنشاؤه سنة 1999 ليقوم بتكوين متخصصين في الشرطة القضائية، وإجراء بحوث متعلقة بالظواهر الإجتماعية ذات صلة بالجريمة.

ويعد المعهد مؤسسة فعالة في تحديد السياسة الجنائية المثلى لمكافحة الإجرام بشتى أنواعه من خلال البحوث المتعلقة بالجرائم والعمل على ترقية البحث التطبيقي وأساليب التحريات التي تثبت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي والتي يستعان فيها بالتكنولوجيات الدقيقة، والإستفادة من النتائج المتوصل إليها في كل من الملتقيات والمحاضرات أو الندوات التي يشارك فيها على الصعيدين الوطني والدولي والتي يهدف من خلالها إلى تطوير مستوى مستخدمي المعهد، الذين يخضعون لدورات تحسين المستوى والتكوين ما بعد التدرج في تخصصات العلوم الجنائية التي تنظم من طرف المعهد، إضافة إلى مهام أخرى قد يطلع بها.[1]

المطلب الثاني: حماية المعلومات الإلكترونية:

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الإلكتروني وما يصاحبها من أضرار على الأفراد وعلى المؤسسات الدولة من جهة، ومحاولة منه للتدارك الفراغ التشريعي عمد منذ الألفية الثانية إلى تعديلات لعديد من القوانين الوطنية، بما فيها التشريعات العقابية وعلى رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال التكنولوجيا الإعلام والإتصال.

[1] خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص191 و203.

الفرع الأول: صور الإعتداءات الماسة بأنظمة المعالجة الالية للمعطيات:

لقد إستحذث المشرع الجزائري في تعديله لقانون العقوبات بمقتضى القانون15/04 المؤرخ في 10 نوفمبر 2004، بإدراج القسم السابع مكرر وخصصه للإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات حيث جرم بعض الأفعال وحدد لها عقوبات[1]، وسنورد فيما يلي أهم المواد في القانون الجزائري والتي عدلت لتتماشى مع التوجيهات الحديثة في معالجة المعلومات بطريقة إلكترونية ويمكن تلخيص أهم الإعتداءات المشمولة بالمعالجة القانونية في:

1. الدخول والبقاء غير المشروع في المعالجة الآلية للمعطيات.
2. الإعتداءات العمدية على نظام المعالجة الآلية للمعطيات.

هذه الإعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات كشرط مسبق بخلاف الإعتداءات على منتوجات النظام وسنتعرض إليها بالتفصيل فيما يلي:

1. الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

نصت المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50.000 إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك[2] تضاعف العقوبة إذ ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذ ترتب عن الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة «تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة المالية من 50.000 إلى 150.000 دج»، كما نصت عليه المادة 02 من الإتفاقية الدولية للإجرام المعلوماتي".

الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع فيما الصورة المشددة، تتحقق بتوافر الظروف المشددة لها، ويكون في الحالة التي تنتج في نظام أو تخريب النظام إشغال المنظومة.[3]

---

[1] حليمة حوالف، معالم الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص146.

[2] المادة 394 مكرر من القانون 06-23 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر 66-156 المتضمن قانون العقوبات، الجريدة الرسمية، عدد84.

[3] سليمة سعيدي وبلال حجاز، جرائم المعلومات والشبكات في العصر الرقمي، المرجع السابق، ص149-148.

ويقصد بالدخول هو ذلك النشاط المتمثل في الإتصال بنظام الكمبيوتر، يهدف الفاعل من خلاله إلى الإطلاع على المعلومات التي يحتويها النظام وحسب نص المادة المذكورة أعلاه لكي يكون الدخول مجرما لا يشترط أن يقع على كامل النظام، بل يكفي أن يقع الدخول على جزء منه، وإشتراط كذلك أن يكون الدخول عن الغش غير أنه لم يحدد وسائل وطرق الغش.

وفضلا عن الدخول في نظام فإن المشرع أضاف ما يعرف بالبقاء Le Maintien في نظام المعالجة الآلية للمعطيات ويتمثل هذا النشاط في مكوث الفاعل وإستمراره داخل نظام الكمبيوتر بعد دخوله ولو عرض أو يجاور الوقت المسموح به للبقاء[1].

الصورة المشددة: وقد نصت الفقرة (3/2) من المادة 394 مكرر على "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة".

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إستغلال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة مالية من 50.000 إلى 150.000دج.

نصت المادة 394 مكرر3/2 من قانون العقوبات على ظرفين تشديد هما عقوبة جريمة الدخول والبقاء داخل النظام، ويحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائفه، ويكفي لتوفير هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع وتلك النتيجة الضارة ولا يشترط أن تكون تلك النتيجة الضارة مقصودة لأن تطلب مثل هذا الشرط يكون غير معقول حيث أن المشرع نص على تجريم الإعتداء المقصود على نظام عن طريق محو أو تعديل المعطيات التي يحتويها بإعتباره جريمة مستقلة.[2]

تعد أنشطة الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات من أكثر الجرائم شيوعا آخرها قضية إختراق موقع جامعة باجي مختار بعنابة برسم الدخول الجامعي لسنة 2016/2015 من أجل التلاعب

[1] حليمة حوالف، معالم الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص147.

[2] سليمة سعيدي وبلال حجاز، مرجع السابق، ص150.

بالتسجيلات الجامعية وتوجيه العشرات من الطلبة والطالبات إلى تخصصات جامعية دون توافر الشروط المطلوبة.[1]

2. الإعتداء العمدي على سير نظام المعالجة الآلية للمعطيات:

النشاط الإجرامي في هذه الجريمة يتمثل في أفعال الإدخال والمحو والتعديل، ويكفي إدخال أحدهما لقيام الجريمة، فلا يشترط إجتماعهما معا حتى يتوافر النشاط الإجرامي فيها، ومن ثم يقام الركن المادي في الجريمة.

لكن القاسم المشترك في هذه الأفعال جميعا هو إنطوائها على تلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل أخرى قائمة.

وعلى ذلك فإن موضوع السلوك الإجرامي في هذه الجريمة محدد، وهو الإعتداء على معطيات في نظم المعالجة، أي البيانات التي أدخلت لمعالجتها وتحولت إلى معطيات عابرة عن رموز أو إشارات تمثل تلك المعلومة، أي البيانات التي تمت معالجتها.

ومن صور الركن المادي في هذه الجريمة كما يلي: فعل الإدخال، فعل المحو وفعل التعديل.

أ. **فعل الإدخال:** يتحقق فعل الإدخال بإضافة معطيات جديدة على الدعامة–الشيء المادي–الخاصة به، سواء كانت خيالية أم يوجد عليها معطيات من قبل، وهذه الجريمة تقع غالبا بمعرفة المسؤول عن القسم المعلوماتي والذي يسند إليه وظائف المحاسبة والمعاملات المالية، لأنه يكون أفضل وضع يؤهله لإرتكاب هذا النمط من التلاعب غير المشروع.

ومن الصور العملية لإدخال معلومات مصطنعة، قيام المسؤول المعلوماتي في المنشأة يضم مستخدمين غير موجودين بالفعل، أو قيامه بالإبقاء على مستخدمين تركوا الوظيفة بالفعل.

ب. **فعل المحو:** المحو سلوك إجرامي في جريمة إختراق النظم المعلوماتية يقصد به إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

---

[1] يزيد بوحليط، المرجع السابق، ص177.

ويمكن للمسؤولين عن حفظ البيانات وبصورة مبسطة أن يدمروا أو يتلفوا المعلومات التي كلفوا بحفظها داخل الحاسب الآلي، وذلك عن طريق إتلاف المعلومات أو محوها.

ج. **فعل التعديل:** ويقصد بالسلوك الإجرامي، وصورة التعديل تغيير المعطيات الموجودة داخل النظام وإستبدالها بمعطيات أخرى، وقد يتم التلاعب في المعطيات عن طريق إستبدالها، أو عن طريق التلاعب في البرنامج وذلك بإمدادها بمعطيات مغايرة تؤدي لنتائج مغايرة عن تلك التي صمم البرنامج لأجلها.

وكقاعدة عامة فإن المحو أو التعديل للمعطيات الموجودة في النظام، كصورتين للركن المادي في جريمة الإعتداء على نظام المعالجة الآلية للمعطيات، يتم عن طريق برامج عربية تتلاعب في هذه المعطيات وذلك لمحوها كليا أو جزئيا أو تعديلها، وذلك بإستخدام القنبلة المعلوماتية الخاصة بمعطيات.[1]

الفرع الثاني: الإجراءات الردعية والعقابية:

إن القانون الجنائي التقليدي لا يتطور دائما، بنفس السرعة التي تتطور بها التكنولوجيا الجديدة لاسيما أن نصوصه وضعت في عصر لم يكن الأنترنت قد ظهر فيه ولم تظهر المشاكل القانونية الناتجة عن إستخدامه، لكن نجد أن المشرع الجزائري تدارك الفراغ القانوني في مجال الإجرام المعلوماتي ولو نسبيا، خصوصا بموجب القانون 04-15 المتضمن تعديل قانون العقوبات إذ بموجبه جرم بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات، وقد سبق ذكرها في الفرع الأول أما العقوبات سأطرق لها خلال هذا الفرع:

البند01: العقوبات المقررة على شخص طبيعي:

إن من خلال إستقرار النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات، إذ نجد سلم خطورة يتضمن ثلاثة درجات، جريمة الدخول أو البقاء بالغش في الدرجة الأولى وبعدها في الدرجة الثانية جريمة الدخول والبقاء المشددة أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس العمدي بالمعطيات.

[1] عبد الفتاح بيومي حجازي، كافة مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، دراسة قانونية متعمقة في القانون المعلوماتي، دار الفكر الجامعي، الإسكندرية، الطبعة 01، سنة 2006، ص 376 إلى387.

1. الدخول والبقاء بالغش (الجريمة البسيطة):

العقوبة المقررة هي ثلاثة أشهر إلى سنة حبس مع غرامة مالية من 50.000إلى 100.000دج (المادة 394 مكرر).

2. الدخول والبقاء بالغش (الجريمة المشددة):

تضاعف العقوبة إذ ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة، وتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة مالية من 50.000دج إلى 150.000دج إذ ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام إشتغال المنظومة (المادة 394 مكرر02-03).

3. الإعتداء العمدي على المعطيات:

طبقا لنص المادة 394 مكرر2 فالعقوبة المقررة للإعتداء العمدي على المعطيات الموجودة داخل النظام هي الحبس من 6 أشهر إلى 3 سنوات وغرامة من 500.000إلى 2.000.000دج أما العقوبة المقررة لإستخدام المعطيات في إرتكاب الجرائم الماسة بالأنظمة المعلوماتية العقوبة المقررة هي الحبس من شهرين إلى 3 سنوات وغرامة من 1.000.000دج إلى5.000.000دج.1

العقوبات التكميلية:

نصت المادة 394 مكرر06 من نفس القانون على مجموعة من العقوبات التكميلية يحكم بها إلى جانب العقوبات الأصلية وهي كالتالي:

- ✓ **المصادرة**: وتعني مصادرة الأجهزة والبرامج والوسائل المستخدمة لإرتكاب الجرائم الماسة بالنظام وذلك ببيعها، أو حجزها مع مراعاة حقوق الغير حسن النية.
- ✓ **إغلاق المواقع**: إغلاق المواقع الأنترنت أو المواقع الإلكترونية بصفة عامة، والتي كانت وسيلة لإرتكاب هذه الجرائم أو ساهمت في إرتكابها.

[1] سليمة سعيدي، المرجع السابق، ص152.

إغلاق المحل (المقهى الإلكتروني): يكون في الحالة التي يكون صاحب المحل مشاركا في الجريمة، وذلك تمت الجريمة وهو عالم بها ولم يتصدى لها بالإخبار عنها، أو بمنع مرتكبيها من إرتياد محله لإرتكاب مثل هذه الجرائم.

والملاحظ أن هذه العقوبات جاءت رادعة حيث تضاعف عند الضرورة كما إشتملت على عقوبات تكميلية، وحتى عقوبات الشخص المعنوي.[1]

البند02: العقوبات المطبقة على الشخص المعنوي:

مبدأ مسألة الشخص المعنوي وارد في المادة 12 من الإتفاقية الدولية للإجرام المعلوماتي، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة، والشروع فيها، كل ذلك بشرط أن تكون الجريمة قد إرتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه.

كما تجدر الإشارة إلى أن المشرع الجزائري قد أقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي وذلك في نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات الذي ينص على أن: "العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح هي:

الغرامة التي تساوي من مرة إلى 5 مرات الحد الأقصى للغرامة المقدرة لشخص الطبيعي في القانون الذي يعاقب على الجريمة.

واحدة أو أكثر من العقوبات الآتية:

حل الشخص المعنوي.

غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات.

الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات.

[1] عائشة تايري، الجريمة الإلكترونية في التشريع الجزائري، مرجع سابق، ص39.

المنع من مزاولة نشاط أو عدة أنشطة مهنية أو إجتماعية بشكل مباشرا أو غير مباشر نهائيا أو لمدة تتجاوز 5 سنوات.

مصادرة الشيء الذي إستعمل فيها إرتكاب أو نتج عنها.

نشر أو تعليق حكم الإدانة.

الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي إرتكب الجريمة بمناسبة.

بالنسبة لعقوبات الغرامة المالية المطبقة على الشخص المعنوي عند إرتكابه أحد الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة 394 مكرر 4 قانون عقوبات 5 مرات الحد الأقصى للغرامة المالية المقررة لشخص الطبيعي[1].

كما نص المشرع الجزائري في المادة 51 مكرر من القانون 15/04 على مسألة الشخص المعنوي وذلك وفق شروط:

أن ترتكب إحدى الجرائم المنصوص عليها قانونا.

أن تكون بواسطة أحد أعضاء أو ممثلي الشخص المعنوي.

أن ترتكب الجريمة لحساب الشخص المعنوي.

البند 03: عقوبة الإشتراك والشروع في الجريمة:

نصت عليها المادة 11 من الإتفاقية الدولية للإجرام المعلوماتي وقد تبنى المشرع الجزائري مبدأ معاقبته الإتفاق الجنائي بنص المادة 394 مكرر بعرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ولم يخضعها لأحكام المادة 176 من قانون العقوبات المتعلق بجمعية الأشرار.[2]

[1] سليمة سعيدي وبلال حجاز، جرائم المعلوماتية والشبكات في العصر الرقمي، المرجع السابق، ص154-155.

[2] سليمة سعيدي، المرجع السابق، ص155.

عقوبة الإشتراك:

عقوبة الاشتراك نص عليها المادة 394 مكرر05 من القانون رقم 15/04 بقولها "كل من شارك في مجموعة أو إتفاق تألف بغرض الإعتداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

عقوبة الشروع:

نصت المادة 394 مكرر07 من نفس القانون "بقولها يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".1

الفرع الثالث: تطور المنظومة القانونية لمكافحة الجرائم الإلكترونية في الجزائر.

إنطلقت عملية إستغلال شبكة الأنترنت في الجزائر منذ سنة 1995 مع إساءة إستخدام هذه التقنية الحديثة، ظهرت جرائم مستحدثة تختلف تماما في مفهومها عن الجرائم التقليدية، مما دفع بالمشرع الجزائري إلى تعديل منظومته الجزائية للحد من إنتشارها، وكان ذلك بداية سنة 2004 وستتناول في هذا الفرع جملة القوانين المتعلقة بمواجهة الجريمة الإلكترونية.

1 بخصوص تعديل قانون العقوبات

القانون رقم01-09 المؤرخ في2001/06/26

القانون رقم04-15 المؤرخ في2004/11/10

قانون رقم 06-23 المؤرخ في2006/12/20

قانون رقم 09-01 المؤرخ في2009/12/25

2 بخصوص تعديل قانون الإجراءات الجزائية:

3 بخصوص القوانين الخاصة:

[1] عائشة تايري، الجريمة الإلكترونية في التشريع الجزائري، مرجع سابق، ص38.

قانون رقم 2000-03 المؤرخ في 2000/08/05: يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية

الأمر رقم 03-05 المؤرخ في 2003/06/19 يتعلق بحقوق المؤلف والحقوق المجاورة.

القانون رقم 08-01 المؤرخ في 2008/01/23 يتعلق بالتأمينات الإجتماعية.

القانون رقم 09-04 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنلوجيا الإعلام والإتصال ومكافحتها.

القانون رقم 15-04 المؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتصديق الإلكتروني.

4 بعض الإتفاقيات الدولية.

البند01: القوانين المتعلقة بمواجهة الجرائم الإلكترونية:

مع التطور المذهل الحاصل في مجال الحوسبة والإتصال، سارعت الجزائر على غرار دول العالم لإستغلال هذه التقنية في شتى المجالات، عن طريق تسطير برامج طموحة مثل ربط الجزائر بشبكة الأنترنت عالية التدفق عن طريق الأقمار الصناعية أو كوابل وتمكين مؤسسات الدولة من التعامل بهذه التقنية للوصول لحكومة إلكترونية رائدة ناهيك عن إتصال الأنترنت لكل بيت بتدفقها عالي، إضافة إلى تمكين كل أسرة جزائرية من شراء حاسوب مثل برنامج (أسرتيك)، كما فتح مجال إستغلال الهاتف النقال للخواص....إلخ. فمن خلال هذه المعطيات لاشك أن هناك جرائم إلكترونية عديدة ترتكب سواء كان الحاسوب هدفا أو وسيلة لها، أو الجرائم التي ترتكب بواسطة شبكة الأنترنت، أو التي ترتكب بإستعمال شبكة الإتصال لذلك سارع المشرع الجزائري إلى حماية هذا الفضاء السبراني و مستعمليه من خلال إصدار جملة من القوانين سواءا ما تعلق الأمر بالقانون العام أو بموجب نصوص خاصة، أو بما تعلق بالتصديق على الإتفاقيات العربية والدولية وهي تمثل بداية لمنظومة قانونية فعالة ومتكاملة لمكافحة هذه الجرائم.

أولا: بخصوص تعديل قانون العقوبات:

في إطار مكافحة الجرائم الإلكترونية التي تعتبر ذات طبيعة خاصة، قام المشرع الجزائري بتعديل قانون العقوبات على مراحل نوجزها كما يلي:

1 القانون رقم 01-09 المؤرخ في 2001/06/26:

نظرا لإنتشار الوسائل الإلكترونية والمعلوماتية وتوسيع شبكة الأنترنت، قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم 01-09 المعدل والمتهم لقانون العقوبات في القسم الأول تحت عنوان: "الإهانة والتعدي عن الموظفين ومؤسسات الدولة فنص في المواد من(144 مكرر-144 مكرر2) والمادة 146 على الجرائم الإهانة والسبب ضد رئيس الجمهورية ومؤسسات الدولة بإستعمال الوسائل الإلكترونية أو المعلوماتية حيث كان هدف المشرع منع المجرم الإلكتروني من إساءة إستخدام هذا الفضاء الإفتراضي، وتمهيد الطريق نحو توسيع مكافحة هذا النوع من الجرائم المستحدثة الى مجالات أخرى كما سنرى.

2 القانون رقم04-15 المؤرخ في 2004/11/10:

مع تقدم الجزائر في إستغلال مجال تكنلوجيا الإعلام والإتصال قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم (15/04) سالف الذكر بإضافة قسم سابع مكرر تحت عنوان: "المساس بأنظمة المعالجة الألية للمعطيات" من المادة (394 مكرر-394مكرر7) بهدف مكافحة الجرائم المستحدثة الناشئة عن إساءة إستعمال هذه التقنية، حيث نص على جملة من الجرائم كجريمة الدخول عن طريق الغش في كل جزء من منظومة معلوماتية، وجريمة تخريب نظام إستغلال المنظومة المعلوماتية.

و بالتالي نستطيع القول أن المشرع الجزائري تدارك ولو نسبيا الفراغ القانوني في مجال مواجهة الإجرام الإلكتروني وهي تمثل قفزة نوعية برغم أن الدول مجاورة سبقتها في وضع قوانين في ذات الشأن مثل تونس(قانون العقد الإلكتروني لسنة2001) والمغرب(القانون رقم03-07 المتعلق بالإخلال بسير نظام المعالجة الآلية للمعطيات) كما تجدر الإشارة إلى أن المشرع الجزائري قد ركز في هذا القانون على الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات. وأغفل الإعتداءات الماسة بمنتوجات الإعلام الآلي والمتمثلة في التزوير المعلوماتي.

3 القانون رقم06-23 المؤرخ في 2006/12/20:

مع تزايد كبير في إستعمال تقنية المعلومات، ونظرا لخطورة الأفعال الواقعة على الحياة الخاصة للأفراد، وسع المشرع الجزائري تدريجيا من سياسته الجنائية الخاصة بتجريم والعقاب الى جرائم المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت، كإستعمال الحاسب وشبكة الأنترنت، والهاتف النقال...إلخ، وهذا بموجب القانون رقم 06-23 المعدل والمتمم لقانون العقوبات، أين نصت المواد من (303مكرر،

303مكرر3) على: إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه، أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

4 القانون رقم09-01 المؤرخ في 2009/02/25:

نظرا للإشكالية الفقهية التي أثيرت حول مدى إعتبار المعلوماتية مالا سارع المشرع الجزائري إلى إعتبار المعلوماتية مالا يمكن سرقته وذلك بموجب القانون رقم09-01 المعدل و المتمم لقانون العقوبات. أين نصت المادة 350 مكرر(1) من ق ع ج على:

"يعاقب بالحبس من سنتين الى 10 سنوات وبغرامة من 200.000 دج الى 1.000.000 دج كل من سرق أو حاول سرقة ممتلك ثقافي منقول محمي أو معرف"، وحسنا فعل المشروع نظرا لما يشكله المال المعلوماتي من قيمة مالية مستحدثة.

ثانيا: بخصوص تعديل قانون الإجراءات الجزائية:

في إطار إستعمال سياسة الجنائية الخاصة بمكافحة الجرائم الإلكترونية في شقيها الإجرائي، كان لزاما على المشرع الجزائري تعديل قانون الإجراءات الجزائية بهدف إستحداث إجراءات جديدة تتوافق وطبيعة الخاصة للجرائم الإلكترونية فنص القانون رقم 06-22 المؤرخ في 2006/12/20 يعدل ويتمم قانون الإجراءات الجزائية على جملة من الإجراءات الجديدة في الفصل الرابع تحت عنوان: في إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور «من المادة(65 مكرر5، 56 مكرر10)، كما نص أيضا في الفصل الخامس تحت عنوان:" في التسرب" بموجب المادة(56 مكرر11-56مكرر18) وهي إجراءات تمكن سلطات البحث والتحري من الكشف عن المجرم الإلكتروني في هذه البيئة الإفتراضية التي يصعب التحقيق فيها بسبب طبيعتها الخاصة.

ثالثا: بخصوص القوانين الخاصة:

1) قانون رقم:2000-03 المؤرخ في 2000/8/5 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية:

نص هذا القانون في جزء منه بموجب نص المادة(87)، كما إعتبر المشرع المسؤولة قائمة على عائق المتعامل يخص المبالغ المحمولة بموجب نص المادة (2/84)، ويمثل هذا المجال بيئة خصبة للمجرم الإلكتروني لإرتكاب جرائم سرقة وتحويل الأموال....إلخ، لذا أضفى المشرع حماية جزائية على إستغلال هذه التكنولوجيا نظرا لما ينجز عنها من أضرار تمس مصالح الدولة والأفراد على حد سواء، فأحاط سرية المراسلات التي هي على حق دستوري مكفول بحماية خاصة بموجب نص المادتين(105)و(137) من القانون نفسه.

2) الأمر رقم03-05 المؤرخ في 2003/05/19 يتعلق بحقوق المؤلف والحقوق المجاورة:

إن أهم ما جاء به الأمر بخصوص مكافحة الجرائم الإلكترونية، هو تصنيف برامج الحاسوب بموجب المادة(04/أ) وقواعد البيانات بموجب المادة(1/05).

كما أحاطهما بحماية جزائية تمثلت في جرائم التقليد، وهذا بموجب نصوص المواد من(143)وما بعدها و(151)وما بعدها.

3) القانون رقم 08-01 المؤرخ في 2008/01/23 يتعلق بالتأمينات الإجتماعية:

يمكن القول أن المشرع الجزائري في هذا القانون، قد إستبق الأحداث تحسبا للتطور الهائل في مجال إستعمال التكنولوجيا الحديثة وتعميم إستعمال الشبكة المعلوماتية في شتى المجالات، إذ نص في المادة(06) مكرر من هذا القانون على:" تثبيت صفة المؤمن له إجتماعيا ببطاقة إلكترونية...". ونظرا لإحتواء هذه البطاقة على معلومات سرية تتعلق بالحياة الخاصة للأفراد، أحاطها للحماية الجزائية اللازمة، فنص في المادة(93 مكرر2) على:" دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين الى خمس سنوات وبغرامة من 100.000دج الى 200.000دج كل من يسلم أو يستلم بهدف الإستعمال غير المشروع البطاقة الإلكترونية للمؤمن له إجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمنهجي الصحة" كما تضاعف العقوبة حسب نص المادة(93 مكرر3) على كل من يقوم عن طريق الغش بتعديل أو حذف للمعطيات.

4) القانون رقم 09-04 المؤرخ في 2009/08/05 يتضمن القواع الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الأعلام والإتصال ومكافحتها: إن تفاقم الإعتدادات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، تطلب تدخل تشريعيا صريحا سوى على المستوى الدولي أو الداخلي، حيث عرفت

المادة (2/02) من قانون سالف الذكر، المنظومة المعلوماتية،" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المترابطة، يقوم واحد منها أو أكثر لمعالجة آلية للمعطيات تنفيذا لبرامج معين". بدأت نصوص هذا القانون بتحديد مصطلحات ثم نص على جملة من القواعد الإجرائية الجديدة الخاصة بحالات مراقبة الإتصالات الإلكترونية وبتفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية وإلتزامات مقدمي الخدمات، والتعاون والمساعدة القضائية الدولية إضافة إلى إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

5) القانون رقم 15-04 المؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين:

تبعا لمتطلبات المعاملات الإلكترونية لاسيما في ضل التواجه نحو الحكومة الإلكترونية ومقتضيات التجارة الإلكترونية، وبعد أن أدرج المشرع الجزائري نظام الإثبات بالكتابة في الشكل الإلكتروني ضمن قواعد الإثبات. أقر بنظام التوقيع والتصديق الإلكترونين والإعتراف بحجيتهما في الإثبات، قصد توفير الحماية اللازمة لوسائل الدفع الإلكتروني بالنسبة لمعاملات التجارة الإلكترونية وزرع الثقة لدى المتعاملين لما يمتاز به مستوى عال للسرية والخصوصية.

رابعا: بعض الإتفاقيات الدولية: نذكر منها:

1- إتفاقية حماية حقوق المؤلف بباريس بتاريخ1971/07/24 إنضمت إليها الجزائر بموجب المرسوم الرئاسي رقم 71-741 المؤرخ في 1971/09/18.

2- إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من طرف الجمعية العامة بتاريخ 2001/05/31 صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم04-165 المؤرخ في 2004/06/08.

3- إتفاق الشراكة الأورو متوسطي بين الإتحاد الأوربي والجزائر بتاريخ2002/04/22 صادقت عليه الجزائر بموجب قانون رقم 1144/2003 بتاريخ2003/12/02.

4- إبرام إتفاقية دولية ثنائية مع الحكومة الفرنسية والمتعلقة بـ: التعاون في مجال الأمن ومكافحة الإجرام المنظم" حيث تنص المادة(10/01) من الإتفاقية على"...مكافحة الإحتيالات المرتبطة بتكنولوجيا الإعلام والإتصال الجديدة...".

الخاتمة:

بتوفيق من الله وتسديده ثم جمع معلومة هذه الدراسة التي لا شك أنه يعتريها النقص والخلل، لكن حسبنا أنها عمل بشري والنقص فيها وارد مهما يدل الإنسان من جهد ومسعى، وقد حاولنا في هذه الدراسة تبيان الأليات القانونية لمكافحة الجريمة الإلكترونية على مستوى التشريعات الوطنية والدولية وملامح إطارها القانوني.

فقد أضفى التطور المماثل لتقنية المعلومات وإندماجها بتقنية الإتصالات فيها الى ظهور جريمة الإلكترونية بإعتبارها من الجرائم الإلكترونية المعاصرة التي والبحث عصر التقدم التكنولوجي فهي ترتكب في مسرح غير قابل لتحديد الجغرافي إلا أنه يضم الجد تجمع إنساني يتميز بالإرتباط وتشابك؛ فهي نوعا مستحدثا من الجرائم تشعدي القواعد التقليدية لتجريم و العقاب فلا هروب من الواقع الذي يشهد تنامي ظاهرة الجرائم والتي أصبحت تأخذ أنماط جديدة كلما زاد الذكاء الإجرامي غير وسائل الإلكترونية ولهذا لابد من معرفة دور بعض التشريعات المقارنة من الحماية الجزائية من الجريمة الإلكترونية ودورها والحد من مشكلاتها القانونية ولمواجهة مثل هذا الجريمة العابرة مواجهة نعالة يحي تجريم صورها في القانون الوطني للمعاقبة عليها وأن يكون هناك تضامن وتعاون دولي لمواجهة مشاكلها

النتائج:

1)أنه وبالرغم ما حققته الأنترنت من ايجابيات وما قدمته من تسهيلات للبشرية، إلا أنها لم تسلم من أيدي المجريمين وأنها أصبحت أداة لإرتكاب جرائمهم وهذا ما أدى الى بروز طاقة جديدة من الجرائم تختلف عن جرائم التقليدية و تميزها عنها بحداثتها من حيث الأساليب والأدوات المستعملة في تنفيذها.

2)نظرا للطبيعة الخاصة للجريمة الإلكترونية لا يوجد إتفاق على وضع تعريف موحد لها، او إستعمال مصطلح معين للدلالة على هذه الظاهرة الجرمية الناشئة في بيئة الكمبيوتر والأنترنت وهو إختلاف رافق ظاهرة الإجرام المرتبطة بتكنولوجيات الإعلام والإتصال، فهي تتم في فضاء أفتراضي يتسم بالتغيير والإنتشار الجغرافي في العابر للحدود

3)تتسبب الجرائم الإلكترونية في أضرار نفسية وإقتصادية بالغة يصعب حصرها وبالتالي كان لزاما على المشرع عند رضعه لسياسته الجنائية الإحاطة الشاملة والمعرفة الدقيقة بما هيبتها وبكفاية صورها وتحديد أركانها واوجه النشاط الإجرامي فيها قصد تحقيق الفعالية في مكافتها وضمان عدم إفلات المجرم.

4)تصنف جرائم الأنترنت ضمن جرائم التقنية العالية،وهي عبارة عن جرائم عابرة للحدود تفع غلى شبكة الأنترنت أو بواسطتها من قبل شخص على دراية فائقة بها.

5)إستعمال المشرع مصطلح "منظومة"يدلا"من مصطلح"نظام" لترك الباب مفتوح في حال ظهور منظومات معلوماتية جديدة مع تعدد إستعمالها.

6)تطرا لظهور شبكة الأنترنت أصبح العالم عبارة عن قرية صغيرة وبالتالي فإن جرائم الحاسوب والأنترنت ترتكب في موقع ما وتحقق النتيجة في الموقع آخر يبعد عنها الألف الأميال وبالتالي فأنها تكون جرائم وطنية أو دولية ومن هنا يجب تكثيف الجهود والتعاون الدولي لمكافحتها وتطوير جهود البوليس الدولي(الأنتربول)من أجل ذلك.

التوصيات:

1)تطوير التشريعات العقابية،وإصدار تشريعات جديدة لمواجهة الجرائم المستحدثة، والتي ترتكب عبر الحتسوب والشبكة الدولية للمعلومات (الأنترنت) بست نصوص تشريعية في قانون العقوبات تجرم هذه الأفعال ببيان كل جريمة ووضع العقوبات المقررة بها.

2)عقد الندوات العلمية والقانونية والأمنية من أجل التعريف بالجرائم الإلكترونية و معالجة أسبابها وبيان سبل مواجهة هذه الجرائم

3)وجوب وضع الحماية الجنائية للمعلومات والبيانات المهمة لمنع المجرمين من إختراقها وإتلافها.

4)إنشاء شرطة متخصصة لمكافحة جرائم الحاسوب والأنترنت.

5)وجوب التعاون الوطني والدولي في المجالين الأمني والقضائي لملاحقة المجرمين وسرعة كشفهم وإلقاء القبض عليهم وتبادل المعلومات المتوفرة عن المجرمين، وتبادل الخيرات المتعلقة بمكافحة هذه الجرائم.

المصادر والمراجع:

القرآن الكريم:

1. الآية 19 من سورة الأنعام.
2. الآية 59 من سورة القصاص.

الكتب:

1- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة02، 2006.

2- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2007.

3- سليمة سعدي وحجاز بلال. جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي الإسكندرية. الطبعة الأولى2017.

4- عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، الطبعة الأولى، 1430/2009، عمان، دار المستقبل للنشر والتوزيع.

5- عبد الفتاح بيومي حجازي، كافة مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، دراسة قانونية متعمقة في القانون المعلوماتي، دار الفكر الجامعي، الإسكندرية، الطبعة 01، سنة 2006.

6- على جعفر، جرائم تكنلوجية المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، مكتبة زين الحقوقية والأدبية، الطبعة الأولى، 2013.

7- علي لجلط، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، ط01، 2013، مكتبة زين الحقوقية والأدبية.

8- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، 2007.

9- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006.

10- يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتفاقية العربية لمكافحة جرائم التقنية المعلومات قانون العقوبات، قانون الإجراءات الجزائية، قوانين خاصة 2019، دار الجامعة الجديدة 40 سوتنير، الإسكندرية.

القوانين والمراسيم:

1- تنص المادة37 من مرسوم رئاسي 20-183 مؤرخ في 13يوليو2020 المتضمن إعادة تنظيم الهيئة الوطنية لوقاية من جرائم المتصلة بتكنولوجيا الإعلام والإتصال وكافحتها، الصادر جريدة الرسمية رقم40 مؤرخ في18يوليو2020، أنه "تلغى جميع أحكام مخالفة لهذا المرسوم، لاسيما أحكام مرسوم رئاسي 19-172 مؤرخ في06يونيو2019 الذي حدد تشكيلة الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام وافتصال وكافحتها وتنظيمها وطرق سيرها.

2- جاء في المادة 13 من قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، السالف الذكر أنه: "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بالإعلام والإتصال ومكافحتها، تحديد تشكيلتها وتنظيمها وكيفية سيرها عن طريق التنظيم".

3- حسب المادة 109 من المرسوم التنفيذي 10-322 المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني، المرسوم نفسه، فإنه من بين المناصب العليا في الأسلاك الخاصة التبعة للأمن الوطني، أشخاص تابعين للشرطة التقنية والعلمية والمكلفون بتقديم خبرة في مجال الجرائم إلكترونية، كما يوجد مدربين ومكونين لضمان التكوين الجيد وتجديد المعلومات وتحسين مستوى التقنيين والبيداغوجي للمتدربين.

4- المادة 03 من المرسوم 19-127.

5- المادة 05 و10 من المرسوم 19-127.

6- المادة 06من المرسوم15-261 المؤرخ في08أكتوبر 2015، الذي يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات الإعلام وافتصال ومكافحتها، جريدة رسمية عدد 53.

7- المادة 08 من نفس المرسوم الرئاسي.

8- المادة 09 من نفس المرسوم الرئاسي.

9- المادة 394 مكرر من القانون 06-23 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر 66-156 المتضمن قانون العقوبات، الجريدة الرسمية، عدد84.

10- المادة02 من المرسوم التنفيذي 10-322 المؤرخ في 22 ديسمبر 2010، المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني الصادرة بالجريدة الرسمية، عدد78 بتاريخ 26 ديسمبر 2010، ص04.

11- المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 24/2015 ذوالحجة 1436؛ الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، االجريدة الرسمية، عدد53، بتاريخ 08أكتوبر 2015، ص16 (الملغى).

12- نصت المادة 24 من المرسوم الرئاسي 19-172 الذي يحدد تشكيلة الهيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها، السالف الذكر على إلغاء

جميع أحكام مخالفة لهذا المرسوم لاسيما أحكام المرسوم الرئاسي 15-261 المؤرخ في 2015/10/08 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

المجلات والملتقيات:

1- أسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، العدد 11، سبتمبر 2018.

2- الأمم المتحدة (الجمعية العامة، الدورة الرابعة والسبعون، البند 109 من جدول الأعمال المؤقت، مكافحة إستخدام تكنولوجيا المعلومات والإتصال للأغراض إجرامية، تقرير الأهمية العامة.

3- حليمة حوالف، معالم الجريمة المعلوماتية في القانون الجزائري، مجلة البحوث القانونية والسياسية، مجلد 03، عدد16، 2012.

4- عبد المالك صوالي، تشريعات الجريمة الإلكترونية في البيئة الإعلامية العالمية، جامعة محمد بوضياف المسيلة، جوان2018، العدد10.

5- ليندة شربشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية الإتجاهات الدولية في مكافحة الجريمة الدولية، المركز الجامعي سوق أهراس.

6- نصير لعرباوي وفاتح النور رحموني، الجريمة الإرهابية الإلكترونية، المعيار 43، جانفي 2018.

7- وليد طه، التنظيم التشريعي للجرائم الإلكترونية في إتفاقية بودابست، عضو قطاع التشريع بوزارة العدل جمهورية مصر العربية.

الرسائل العلمية:

الدكتوراه والماجيستر:

1- خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه، قانون جنائي، جامعة أحمد دراية، كلية الحقوق والعلوم السياسية، أدرار،2021/2020.

2- عبد الله دعش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة إستكمالات للحصول على درجة الماجيستر في القانون العام، جامعة الشرق الأوسط سنة 2014.

الماستر:

1- حسيبة جلود وزينب عماري، الجريمة الإلكترونية في الفقه الإسلامي وقانون العقوبات الجزائري، دراسة مقارنة، جامعة المسيلة، كلية العلوم الإنسانية والإجتماعية، قسم العلوم الإسلامية، 2020/2019.

2- شاهين خضر ورضوان سعادة، الجريمة الإلكترونية وإجراءات مواجهتها، قسم حقوق، جامعة المسيلة، كلية الحقوق، 2021، مذكرة الماستر.

3- شيماء حليفة، الإستراتيجية الأوروبية في مكافحة الجريمة المنظمة 2018/2001، مذكرة الماستر تخصص إستراتيجية وعلاقات دولية، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2019/2018.

4- عائشة تايري، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة درارية، أدرار، 2016.

5- عدلية مراد وروان عبدلي، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، قانون جنائي، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، 2021/2020.

6- محمد بوعمرة وسيد علي بنينال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة الماستر، قسم قانون خاص، جامعة البويرة، كلية الحقوق والعلوم السياسية، 2020.

7- يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة لنيل ماستر أكاديمي، فرع حقوق، جامعة المسيلة، كلية الحقوق، 2016، مذكرة ماستر.

المواقع الإلكترونية:

1. تتمثل مهام مدرية الشرطة القضائية في تنشيط وتنسيق وتوجيه المصالح المكلفة بمعاينة مخالفات ق ع وكذا جمع ادلة والبحث عن المجرمين طالما لم يتم فتح تحقيق من قبل جهات قضائية "معلومات متاحة على موقع إلكتروني لمديرية الأمن الوطني الجزائري: www.algeriepolice.dz .

الملخص:

الجرائم الإلكترونية هي واحدة من أعظم ويلات هذا القرن إذا أصبحت واقعا مفزعا للدول و الأفراد، ويعود ذلك أساسا الى إمكانيات المتاحة للمجرم الإلكتروني وذلك بتقدم وسائل الإتصال وذيوع إستعمال الحاسوب وسهولة إستخدام الأنترنت فبالتخفي خلق شاشتهم يستطيع صناعة ونشر الفيروسات، الإختراقات وتعطيل الأجهزة.

ومن جهة أخرى فإن مكافحة الجريمة الإلكترونية تواجهها عدة عقبات بالنظر الى طبيعتها الإفتراضية أفرزت تحديات واضحة للقوانين التي وضعت لمكافحتها فقد تغيرت الجريمة من صورتها المادية التقليدية الى أخرى معتوبة وتنتج عن ذلك مشكلة تفسر النصوص ومبدأ الشرعية(قمت أبرز المشاكل التي تواجه سياسة مكافحة جرائم الحاسوب لا على الصعيد الدولي بل وفي نطاق التشريعات الوطنية عدم التعامل معها كوحدة واحدة في إطار الحماية الجنائية للمعلومة)

الكلمات المفتاحية:

الجريمة الإلكترونية–إجراءات مواجهة الجريمة الإلكترونية –الجرم الإلكتروني

Abstract

Cybercrime is one of the greatest scourges of this century if it becomes a shocking reality for countries and individuals, mainly because of the possibilities available to cybercriminals by advancing the means of communication, the widespread use of the computer and the ease of use of the Internet.

On the other hand, the fight against cybercrime faces several obstacles, given its hypothetical nature, which has created clear challenges to the laws designed to combat it. The crime has changed from its traditional physical image to its flawed image, resulting in a problem that interprets the texts and the principle of legality. (I have highlighted the problems facing the policy of combating computer crime not at the international level but within the scope of national legislation, not being treated as a single unit within the framework of criminal protection of information)

Keywords:

الملخص

Cybercrime – Cyber crime countermeasures – Cyber crime

الفهرس:

Table des matières