وزارة التعليـــم العالـــي والبحث العلمي

جامعة العربي التبسي

كلية الحقوق والعلوم السياسية

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر

تخصص: الجريمة والأمن العمومي

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في التشريع الجزائري

إعداد الطالبة:

- حمزاوي زينة

إشراف الدكتورة:

خالدي شريفة

لجنة المناقشة

الأستاذ	الرتبة	الجامعة	الصفة
شعبان لامية	أستاذ محاضر ب	جامعة العربي التبسي	رئيســـــــا
خالدي شريفة	أستاذ محاضر ب	جامعة العربي التبسي	مشرفا ومقررا
بوجوراف فهيم	أستاذ مساعد أ	جامعة العربي التبسي	ممتحنـــــــا

السنة الجامعية: 2020-2021

جامعة العربي التبسي–تبسة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر

تخصص: الجريمة والأمن العمومي

بعنـــــوان:

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في التشريع الجزائري

إعداد الطالبة:

– حمزاوي زينة

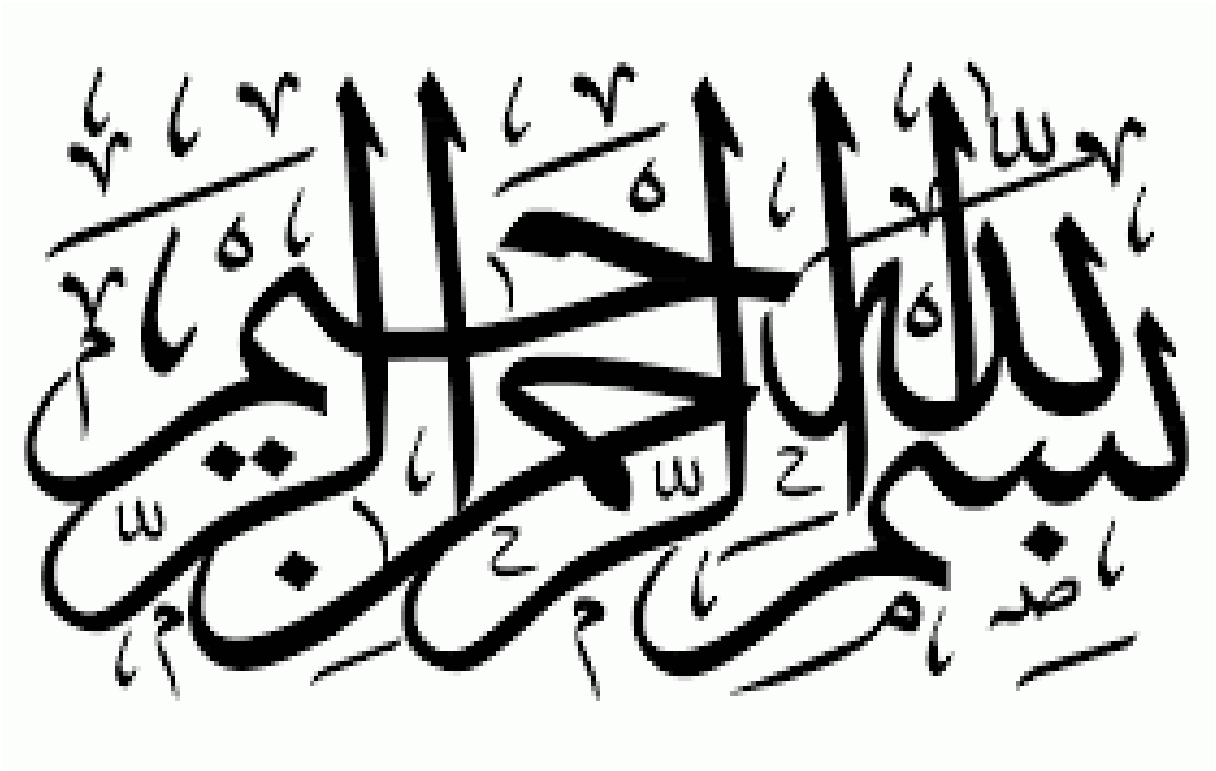
إشراف الدكتورة:

– شريفة خالدي

لجنة المناقشة

الأستاذ	الرتبة	الجامعة	الصفة
شعبان لامية	أستاذ محاضر ب	جامعة العربي التبسي	رئيســـــــا
شريفة خالدي	أستاذ محاضر ب	جامعة العربي التبسي	مشرفا ومقررا
بوجوراف فهيم	أستاذ مساعد أ	جامعة العربي التبسي	ممتحنـــــــا

السنة الجامعية: 2020–2021


بسم الله الرحمن الرحيم

بسم الله الرحمن الرحيم

﴿قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا ۖ إِنَّكَ أَنتَ الْعَلِيمُ الْحَكِيمُ ﴿٣٢﴾﴾

سورة البقرة الآية 32

شكر وعرفان:

الحمد لله حتى يرضى . . . وحين يرضى . . . والحمد لله بعد ما يرضى صاحب الفضل علينا وعلى كل الآنام . . . والصلاة والسلام على المصطفى نور الإسلام

ها قد أوصلتنا الأقدار إلى آخر المشوار، والذي نتمناه خطوة البداية لا نقطة النهاية، هذه الأقدار التي وضعت في طريقنا أناسا وقفوا إلى جانبنا واستحقوا منا الشكر والامتنان .

أتقدم بجزيل الشكر والعرفان إلى مثلي الأعلى وقدوتي في العمل والاجتهاد، وطلب العلم التي ضحت بثمين وقتها بتحفزها وإرشادها المستمر، إلى من لا تفيها كل كلمات الشكر وعبارات الامتنان والتقدير كامل حقها إلى حضرة الأستاذة المشرفة الدكتورة "خالدي شريفة" .

كما أشكر أعضاء اللجنة الموقرة لقبولهم مناقشة هذه المذكرة جزاهم الله منا خير الجزاء .

شكر خاص:

أتوجه بالشكر الخاص للأستاذة الدكتورة "خالدي خديجة" مسؤولة تخصص "الجريمة والأمن العمومي".

بينما نعبر عن عرفاننا علينا ألا ننسى أن أقصى درجات التقدير لا تمثل بنطق الكلام وإنما بتطبيقه.

شكرا لك من أعماق قلبي على عطائك الدائم، العمل ليس مجرد تشريف ولا هو منصب للمفاخرة، بل هو تكليف وأمانة، وأنتم قد أثبتم بالوجه الشرعي أنكم بقدر المسؤولية والأمانة، وأنكم خير من تولى المناصب، فشكرا لكم على جهودكم الرائعة وعلى عملكم وتعاونكم لأجل رفعة هذه الدفعة "جريمة وأمن عمومي" التي لولاكم لما تقدمت.

إن قلت شكرا فشكرا لن يوفيكم، حقا سعيتم فكان السعي مشكورا، إن جف حبري عن التعبير بكيتكم قلب به صفاء الصب.

إلى كل أساتذة معهد العلوم القانونية والإدارية –جامعة العربي التبسي مع حفظ الأسماء والألقاب على رأسهم الأساتذة:

د. عزاز هدى، خماسية حفيظة، د. شعبان لميا، د. بريك عبد الرحمن، د. بوخاتم معمر، د. بوجوراف فهيم، د. شنيخر هاجر.

كما لا ننسى من ساعدني وساهم في إنجاز هذا البحث رئيس مجلس قضاء تبسة، الملازم الأول للشرطة حسين حمانة.

ورئيس خلية الاتصال والعلاقات العامة بأمن ولاية تبسة الملازم الأول للشرطة يوسف بوفنارة

وإلى كل من علمني حرفا ووجهني بكلمة.. وساعدني بدعاء وإلى كل من ساعدني من قريب أو بعيد.

إهداء

باسم كل عمل صادق وعقل واع، وهدف صالح، باسم كل هذا أهدي ثمرة جهدي

إلى أعز ما لدي في الوجود

إلى الشمعة التي أضاءت وأذابت نفسها وما زالت تدمع من أجل أن تكون أمل إلى مشوار حياتي..

إلى أمي الحنونة.

إلى الذي لو استطعت أضع على رأسه تاج الملك وملكته وكان العرض لفعلت ... إلى أبي العزيز

إلى النور الذي أضاء دربي، ورسم لي خطى الإيمان الحقيقي... إلى من جعلتني زهرة بالعطر كاسرة

قيود الوهن، إلى من جعلتني أرسو سفينتي في ميناء الواقع... إلى من جعل الحب رمزا يسكن

فؤادي... إلى الأم الثاني زوجة خالي صحرة.

إلى من أدعو الله أن يكونوا لي عونا في هذه الحياة... عماد البيت وقرة العين إخوتي

إلى إخوتي وأخواتي التي لم تلدهن أمي

إلى كل الأهل والأقارب وأخص بالذكر عائلة حمزاوي، شقروش. أهدي ثمرة جهدي وهذا العمل

المتواضع.

إلى من حفزتني إلى الرجوع إلى مقاعد الدراسة إذ تبقى علما تكن نجوم أهتدي بها اليوم والغد...

إلى اللاتي قاسمتنا لحظات العمر بحلوها ومرها

إلى من وقفنا لمساعدتي دون انتظار رد الجميل... إلى من تقاسمت معي تعب وعناء هذا العمل.

إلى من بعثهن لي القدر مهما قدمت لن أوفي حقهن: زرفاوي كريمة وعكريش لطيفة أطال الله في

عمرهن.

إلى النهر الخالد الذي يقتض محبة وطنية ، إلى القلب المفعم بالحب والعمر وبراءة الأطفال، إلى

نهلة عولمي.

إلى من أقسمت معهن حلو ومر الحياة الجامعية: عباسي شيماء، سلاطنية أميمة، ماجن نبيلة.

إلى أعز الأصدقاء والصديقات: إلى كل دفعة العلوم القانونية والإدارية تخصص: جريمة وأمن

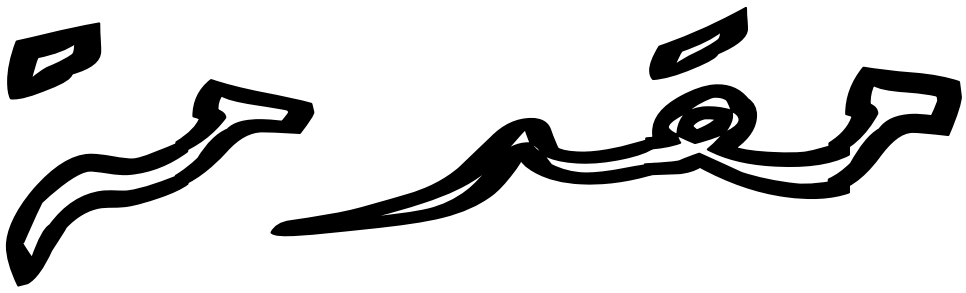
عمومي دفعة 2020-2021

إلى كل من حفظه قلبي ونساهم قلمي

إلى كل زملائي وزميلاتي التي أعرفهم ولم تنطق اللسان بهم

قائمة المختصرات:

ج.ج	جمهورية جزائرية
ج.ر	الجريدة الرسمية
ق.إ.ج.ج	قانون الإجراءات الجزائية الجزائري
ق.ع.ج	قانون العقوبات الجزائري
د.ط	دون طبعة
د.ب.ن	دون بلد نشر
د. س.ن	دون سنة النشر
ص	صفحة
ع	عدد



أدى التطور الهائل في عالم تكنولوجيا المعلوماتية ووسائل الاتصال إلى تعاظم دورها بشكل كبير في شتى مجالات الحياة، وأصبحت الحواسيب وشبكة الانترنت تحتل مساحة هامة في الحياة اليومية للمواطن، وبات يعتمد عليها بشكل شبه كلي في تسيير شؤونه اليومية، وتسير مختلف المرافق الإدارية والعلمية والاقتصادية الأمر الذي تطلب توفير أقصى درجات الحماية لهذه الوسائل الحديث وما يحيط بها، تجنبا لتعطيل سير ذلك المرافق الحيوية أو الاعتداء عليها بما تؤثر على المصالح والخدمات التي باتت تقدمها في العالم اليوم.

لقد أصبحت هذه الجرائم تشكل هاجسا حقيقيا للكثير من الدول باعتبارها من أخطر الجرائم العابرة للحدود، الأمر الي دفعها إلى العمل بشكل جاد على مكافحتها، سواء من خلال إبرام اتفاقيات ثنائية أو وضع تشريعات وطنية للحد منها ومكافحتها.

كما أدى هذا التطور الذي عرفته تكنولوجيا المعلوماتية وتطبيقاتها المتعددة إلى بروز مشاكل قانونية جديدة، تطلب حلها البحث في الأوضاع القانونية القائمة ومدى ملاءمتها لمواجهة هذه المشاكل، خاصة وأن القاضي الجزائي مقيد عند نظره في الدعوى العمومية بمبدأ الشرعية، فهو لا يستطيع أن يجرم أفعالا لم ينص عليها المشرع، وحتى ولو كانت على درجة عالية من الخطورة الإجرامية.

لذلك فقد بات اليوم إفراد قانون خاص للحد ومكافحة الجرائم الإلكترونية أكثر من ضروري، حيث حاول المشرع استحداث آليات قانونية تسمح بالحد من انتشار هذه الجرائم والوقاية منها ومكافحتها بشكل فعال، من خلال وضع منظومة قانونية متكاملة ترتكز أساسا على كل من قانوني العقوبات والإجراءات الجزائرية، وتم تدعيمها بالقانون رقم 09-04 مؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تلاه صدور المرسوم الرئاسي رقم 15-261 مؤرخ في 08 أكتوبر، يحدد شكلية وتنظيم وكيفيات سير الهيئة الوطنية للوقاية

من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث تم إرساء قواعد إجرائية جديدة تتضمن تحكما جيدا في أساليب مكافحة هذا النوع من الجرائم.

وابتغاء الوصول إلى الهدف الذي من أجله أختير هذا الموضوع محل الدراسة فقد تبلور في عدة اعتبارات: تقديم رؤية قانونية، كيف حاول المشرع الجزائري الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها من خلال إبراز أهم الآليات القانونية التي جاء بها القانون رقم 09-04 السالف الذكر في مجال الوقاية، ومناقشة المفاهيم القانونية المتعلقة بالجرائم، وربطها بالمفاهيم القانونية المعلقة، قصد التنبيه واقع تفشي ظاهرة الإجرام المعلوماتي.

وقد سبق التطرق لهذا الموضع في الرسائل ومذكرات التخرج بعنوان الجريمة الإلكترونية أما بصدد هذا الموضوع نذكر منها: أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة مقدمة لنيل شهادة الماجستير، تخصص قانون جنائي جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، 2012-2013 الذي كاتب اشكالية البحث تتمحور حول كيفية تنظيم آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ظل القانون رقم 09-04 وتمحورت حولها أسئلة فرعية، أما بالنسبة للنتائج المتوصل إليها أنه بصدور هذا القانون يعد تحديات فعليا للسلطات القضائية وأعوانها (سلطات الضبط القضائي، المحامين) من أجل تطبيقه نظرا لخصوصية الإجراءات التي جاء بها.

- سمية قبايلي، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في التشريع الجزائري، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي، أم البواقي، كلية الحقوق والعلوم السياسية، قسم الحقوق، كانت اشكالية البحث تتحور حول عن كيفية معالجة المشرع الجزائري لظاهرة الإجرام المتصل

بتكنولوجيا والاتصال سواء من الناحية الموضوعية أو على صعيد القوانين الإجرامية؟ وما مدى خصوصية هذه الجرائم، وماهي آليات مكافحتها؟

أما بالنسبة لنتائج المتوصل إليها كغيرها من الباحثين، وهي الاستعانة بمختصين وخبراء لضبط الجريمة، وتكوين فرق الضبطية والقضاة، مع توفير كافة الوسائل المادية والتقنية اللازمة للقيام بمهامها على أحسن وجه.

أفادتنا الدراسات السابقة بشقيها النظرية والمنهجية من خلال مساعدتنا في تحديد وضبط إشكالية الدراسة الحالية، أو في تحليل المنهج الملائم.

وأن ما يميز دراستنا الحالية عن الدراسات السابقة هو تطرقنا إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات بشيء من التفصيل.

وهذا لا يعني أن البحث لا يخلو من الصعوبات لأن كل عمل ناجح يكون شاقا ومتعبا، ومن الصعوبات التي واجهتها في انجاز هذا العمل هي شساعة الموضوع بالدرجة الأولى وصعوبة التعامل مع المختصين بهذا الموضوع وكذا قلة المراجع الوطنية الخاصة بهذا الموضوع.

ومن خلال الطرح السالف ذكره فأول ما يتبادر إلى الأذهان هو:

ما المقصود بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الذي جاء به المشرع الجزائري؟ وما مدى فعالية السياسة الجنائية المنبعثة من قبل المشرع الجزائري لمواكبة التطور الذي لحق الجريمة في مجال البحث التحري والكشف ومكافحتها من الناحية الإجرائية؟

وقد اعتمدنا على المنهج الوصفي التحليلي في دراسته هذا البحث لأنه الأنسب لطبيعة الموضوع الذي تعتمد على اظهار أهم الآليات التي جاءت في هذا القانون، والوقوف على مفهوم وخصائص الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وإبراز أهم الآليات التي أوجدها المشرع لمكافحتها والوقاية منها.

وعلى هذا ارتأينا أن تكون الخطة مقسمة إلى فصلين، خصصنا الفصل الأول منها لتحديد الإطار العام أو المفاهيمي للجرائم المتصلة بتكنولوجيات الإعلام والاتصـــال، أمـــا الفصل الثاني فقد تم تخصيصه للآليات الإجرائية لمكافحة الجرائم المتصلة بتكنولوجيـــات الإعلام والاتصال.

الفصل الأول

الإطار العام للجرائم المتصلة بتكنولوجيات الإعلام والاتصال

أصبحت المعلومات في عصرنا الحالي تلعب دورا هاما في جوانب الحياة كلها، حتى أصبحت سلعة قابلة للتداول ومع هذا التطور الهائل الذي عرفه مجتمع المعلومات تجاوز إلى أبعد من ذلك وأصبحت ترتكب العديد من الجرائم في مجال المعلوماتية وأطلق عليها بالجريمة المعلوماتية.

وهي صنفا مستحدثا من الجرائم التي اختلفت الاحتمالات في الاتفاق على إعطاء تعريف موحدا هذه الجريمة، وهي العبارة الأكثر تداولا عند الفقهاء القانونيين، لكن في دراستنا هذه نستعمل العبارة التي جاء بها المشرع الجزائري وهي "الجرائم المتصلة بتكنولوجيات الإعلام والاتصالّ، لذلك سنتطرق في الفصل الأول الإطار العام للجرائم المتصلة بتكنولوجيا الإعلام والاتصال وفقا للتقسيم التالي:

المبحث الأول: ماهية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

المبحث الثاني: تصنيفات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

المبحث الأول: ماهية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

إن مسألة وضع تعريف للجريمة كان محل لاجتهادات الفقهاء، حيث لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة، فهناك من يطلق عليها تسمية الجرائم الإلكترونية، وهناك من يطلق عليها تسمية جرائم المعلوماتية، في حين يذهب آخرون إلى تسميتها جرائم إساءة استخدام تكنولوجيات المعلومات والاتصال[1]، ويسمون آخرون جرائم الكمبيوتر والانترنت، وهناك من يطلق عليها الجرائم المستحدثة.

وللوقوف على ماهيتها يستوجب علينا أن نقف عند مدلولها ونبرز الخصائص التي تتمتع بها عن غيرها من الجرائم وهو ما نبينه من خلال (المطلب الأول) وخصوصية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من حيث صفة مرتكبيها في (المطلب الثاني).

المطلب الأول: تعريف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وخصائصها

اختلفت الاتجاهات الفقهية في تعريف هذه الجرائم فهناك من حصرها في تعريفات ضيقة وهناك من أعطاها تعريفات واسعة وهذا ما نبينه في (الفرع الأول).

الفرع الأول: التعريفات الضيقة والموسعة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال

أولا: التعريفات الضيقة: هي مجموعة من العناصر البشرية والآلية التي تعمل معا على تجميع البيانات ومعالجتها وتحليلها وتبويبها طبقا لقواعد وإجراءات مقننة لأغراض

1- المادة (02): من القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ع 47، الصادرة في 16-08-2009، ص 05.

محددة، بغرض إتاحتها للباحثين وصانعي القرارات والمستفيدين الآخرين، على شكل مناسبة ومفيد[1].

في حين اصطلح اتجاه آخر على تسميتها بالجريمة المعلوماتية، إذ نظر إليها من زاوية محددة واعتمدوا على تعريفاتهم على أساس الأداة أو الوسيلة على ارتكاب الجريمة والمتمثلة في أداة الحاسب الآلي.

ومن بين التعريفات التي جاء بها في الفقه إذ اعتبرها على أنها «كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الآلية بقدر كبير لازما لارتكابها من ناحية ولملاحقته وتحقيقه من ناحية أخرى»[2].

فيجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها.

وعرفت أيضا: «أنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقة»[3].

كذلك عرفت على أنها: «الفعل غير المشروع الذي يتورط في ارتكابه الجاني، أو هي الفعل الإجرامي الذي يستخدم في اختراق الحاسوب باعتباره أداة رئيسية»[4].

من خلال التعريفات فقد اعتمد أنصار الاتجاه الضيق في تعريفهم للجريمة المعلوماتية فإنه نظروا إلى الوسيلة كأداة لارتكاب جرائمهم.

1- عامر إبراهيم قندلجي، علاء الدين عبد القادر الجنابي، نظم المعلومات الإدارية وتكنولوجيا المعلومات، ط08، دار المسيرة للنشر والتوزيع والطباعة، جمال أحمد محمد خلف وإخوانه، عمان، الأردن، 2014، ص 28.

2- نائلة عال محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، (د.ط)، منشورات الحلبي الحقوقية، بيروت، 2005، ص 28.

3- فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة ماجستير في القانون العام، قلقاط شكري، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011-2012، ص 32.

4- نهلا عبد القادر المومني، الجرائم المعلوماتية، ط02، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص 48.

ثانيا: التعريفات الموسعة

حاول بعض الفقهاء إعطاء تعريف موسع وذلك لمحاولة وتقادي أوجه القصور التي شابت تعريفات الاتجاه الضيق في التصدي لظاهرة الإجرام المعلوماتي.

إذ رأى واضعو التعريفات الموسعة أنها ليست الجريمة المعلوماتية هي التي يكوّن النظام المعلوماتي[1].

من جانب آخر عرفت: «هي كل سلوك غير مشروع يتم بالتدخل في العمليات الإلكترونية التي تمس أمن النظم المعلوماتية والمعطيات التي تعالجها»[2].

وتم تعريفها كذلك: «كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو هي «جريمة تتم في محيط أجهزة الكمبيوتر»، أو هي «كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها»[3].

وتبنى الخبير الأمريكي (Paker) مفهوما واسعة للجريمة المعلوماتية، حيث عرفها «كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه كسبا يحققه الفاعل»[4].

1- أحمد خليفة الملط، الجرائم المعلوماتية، ط02، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 85-86.

2- تعريفه تبناه المؤتمر العاشر للأمم المتحدة لمنه الجريمة ومعاقبة المجرمين بتاريخ 10-17 أفريل 2000 والمنعقد، ص 08. متاح على الموقع: http//oie.gov/ind تاريخ الاطلاع 20-01-2021 الساعة: 10:30

3- خالد ممدوح إبراهيم: أمن الجريمة الإلكترونية، الدار الجامعية، ط2008، مشار إليه في رصاع فتيحة، مرجع سابق، ص 40.

4- نهلا عبد القادر المومني، المرجع السابق، ص 49.

ثالثا: تعريف المشرع الجزائري للجرائم المتصلة بتكنولوجيا الإعلام والاتصال

أما بخصوص المشرع الجزائري فقد اختار اسم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بدلا من الجرائم المعلوماتية، فإنه عرفها في المادة (02) من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته بقوله: «يقصد في مفهوم هذا القانون: الجرائم المتصلة بتكنولوجيا الإعلام والاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية»[1].

من هذا التعريف يمكن أن تحصي ثلاثة أنواع من الجرائم التي تعد من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال هي:

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات في المواد 394م إلى 394 م7 وهي أفعال الدخول أو البقاء في طريق الغش في منظومة للمعالجة الآلية للمعطيات، وكذلك فعل الإدخال أو الإزالة أو التعديل بطريق الغش لمعطيات في نظام المعالجة الآلية.
- الأشكال التقليدية المجرمة كالغش والنصب عن طريق شبكة الأنترنت.
- الجرائم المعروفة بالمحتوى كجرائم القذف والسب وتحريض القصر على الفسق والدعارة.

ومن خلال هذا التعريف الذي جاء به قانون 09-04 نلاحظ أن المشرع الجزائري لم يقم بتحديد درجة دور المنظومة المعلوماتية أو نظام الاتصالات الإلكترونية في ارتكاب هذه الجرائم فحسب التعريف فإنه يكفي مجرد أن ترتكب الجريمة أو يسهل ارتكابها

1- رشيد بوبكر: جرائم الاعتداء على نظام المعالجة الآلية، ط01، منشورات الحلبي الحقوقية، بيروت، 2012، ص 43.

بالمنظومة المعلوماتية أو نظام الاتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم التي تكون فيها للتقنية المعلوماتية دور ثانوي، كما أن المشرع لم يحدد صور السلوك المجرم الذي يرتكب أو يسهل ارتكابه منظومة معلوماتية أو نظام الاتصالات الإلكترونية.

كما عرفت الاتفاقية العرفية لمكافحة جرائم تقنية المعلومات، وذلك تحت الفصل الأول بعنوان أحكام عامة، وذلك من خلال المادة (02) من الاتفاقية بأن جريمة تقنية المعلومات: «أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترقيتها وتنظمها واسترجاعها ومعالجتها وتحويلها وتبادلها وفقا للأوامر والتعليمات المخزنة المرتبطة سلكيا ولا سلكيا في نظام أو شبكة»[1].

لأن هناك عدة تعريفات للجرائم المتصلة بتكنولوجيات الإعلام والاتصال أوردها الفقه، في أغلبها ضيقة لأنها تقتصر على الأنظمة المعلوماتية وخاصة منها المرتبكة عن طريق جهاز الحاسوب، غير مبرزين الأفعال التي ترتكب بواسطة أو ضد أنظمة الاتصالات، كجرائم القذف، السب باستعمال البريد الإلكتروني أو غرف الدردشة في مواقع الأنترنت.

فالأنظمة المعلوماتية مرتبطة ببعضها البعض بواسطة شبكة الاتصال، هي أيضا منظمة في مجموعة واحدة مع شبكات المعلومات، وفي الوقت الحاضر شبكة الأنترنت

1- مرسوم رئاسي رقم 19-252 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ج.ج.ر ع 57، المؤرخ في 18-09-2014، ص 04.

هي مثال عن نوع الشبكات المعلوماتية، حيث تتصل أجهزة الحاسوب فيما بينها وتتم عملية تبادل المعطيات[1] من خلاله.

الفرع الثاني: خصائص جرائم تكنولوجيات الإعلام والاتصال

تتصف هذه الجرائم بمميزات خاصة مقارنة بالجريمة التقليدية، سواء تعلق الأمر بطبيعة محل الذي يقع عليه الاعتداء أو الشخص الذي يقدم على ارتكابه أو تعلق الأمر بالنطاق المكاني أو بأسلوب ارتكابها التي يتم توضيحها كالآتي: [2]

أولا: جريمة عابرة للحدود الدولية

بعد ظهور شبكات المعلومات المختلفة ومن خلال الأقمار الصناعية والفضائيات والأنترنت جعل الانتشار الثقافي وعولمة الثقافة أمرا ممكنا وشائعا، إلا أنه نتج عنه ما يعرف بالجريمة المعلوماتية باعتبارها لا تعترف بالحدود الإقليمية للدول، ولا بالمكان أو الزمان، ففي مجتمع المعلومات تتلاشى الحدود الجغرافية بين الدول، وذلك يعود لارتباط العالم بشبكة واحدة[3].

ولعل القدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات معتبرة من المعلومات قد ترتكب جرائم في دولة ما، وبتحقيق الفعل الإجرامي في دولة أخرى فهي تتميز بالتباعد الجغرافي بين الفاعل والمجني عليه[4].

1- عرفتها الوكالة الفرنسية للتقنين (Almor) المعطيات (Les donnés) أنها «كل حادث مفهوم أو تعليمية تقدم في شكل متفق عليه قابل للتبادل عن طريق النشر أو بواسطة الحاسوب أو ينتجها الحاسوب»، للمزيد من التفصيل انظر: مفتاح محمد دياب، معجم المصطلحات وتكنولوجيا المعلومات والاتصالات، الدار الدولية، القاهرة، 1995، ص 42.

2- رشيد بوبكر، المرجع السابق، ص 89.

3- عبد العادل الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية (دراسة قانونية قضائية مقارنة)، ط01، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 55.

4- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، (د.ط)، (دار البلدية، عمان)، 2010، ص 141.

كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات، ولعل الأموال المستهدفة والبعد في المسافة قد تفصل الجاني عن هذه المعلومات والأموال، وهذا ما يميز الجريمة المعلوماتية عن الجريمة التقليدية.

ثانيا: صعوبة اكتشافها وإثباتها

إن صعوبة اكتشافها لأنها ترتكب بهدوء، ويكون في كثير من الأحيان بمحض الصدفة، ولأن مستعملي تكنولوجيا الإعلام والاتصال غير مجبرين على الكشف عن هويتهم عند استعمالهم لهذه التكنولوجيات، وخاصة عند تواصلهم بشبكة الأنترنت، وخاصة عند تواصلهم بشبكة الأنترنت يكون من الصعب التوصل إليهم والكثير من مرتكبي الأفعال الصادرة والمجرمة لا ينالون جزاءهم لعدم إمكانية التوصل إليهم وخاصة في الدول التي لا تملك التقنية والمهارات اللازمة في مؤسساتها الأمنية أو من خلال التحقيق في تلك الجرائم من طرف سلطاتها القضائية[1].

إن التحقيق في الجرائم المعلوماتية يتطلب الإلمام بتقنيات تكنولوجيات الإعلام والاتصال وليس فقط تعلمها، بل مواكبة التطور السريع الذي يحدث كل يوم في هذا المجال بالتحقيق يستلزم ذلك أن تقوم السلطات بالتدريب والتأهيل اللازمين والاستعانة بذوي الخبرة الأكفة حتى تكون أعمالهم على قدر من المهنية التي يمكن بها تقديم دليل إلكتروني موثق إلى القضاء.

مع العلم أن الدليل الإلكتروني يترك دائما آثار في حالة محو أو تعديله، والخبير فقط لكشف التلاعبات التي تحدث في النظم المعلوماتية التي يحدثها المجرمون لمحو آثار

1- محمد صالح العادلي، الجرائم المعلوماتية، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط 2-4 أفريل 2006، ص 07.

جرائمهم والآثار التي توصلوا إليها، وهذا ما سنوضحه بالتفصيل في الفصل الثاني من هذه الدراسة[1].

ثالثا: أنها جريمة منظمة

في البداية اعتبرت الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كسلسلة متتابعة من الاعتداءات على الشبكات، ولكنها تعنونت بصبغة المافيا أي الجريمة المنظمة، منشئة بذلك "سوق سوداء" حقيقته للمعلومات المقرصنة، ابتداء من التعدي على الحقوق الملكية الفكرية والفنية، والغش في البطاقات البنكية، فأصبحت هناك صلات قوية في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم التقليدية، وهي في المقابل أصبحوا مجرمي المعلوماتية أكثر تنظيما يوما بعد يوم، لأن هذه الجرام هادئة من نوعها لا تحتاج إلى عنف في ارتكابها، فالتقنية والخبرة في مجال المعلوماتية تكفيان لوحدهما لارتكاب أخطر الجرائم التي قد تهز كيان مؤسسة مالية ما[2].

المطلب الثاني: خصوصية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من حيث صفة مرتكبيها

لقد أضافت المعلوماتية الكثير من الجوانب الإيجابية إلى حياتنا، إلا أنها في المقابل جلبت معها شكلا جديدا من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية، فلم يكن لارتباط الجريمة المعلوماتية بالجانب الآلي أثره على تمييز هذه الجريمة عن غيرها من الجرائم التقليدية فحسب، بل كان له أثره أيضا على تميز المجرم المعلوماتي عن غيره

1- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير، تخصص القانون الدولي للأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 18.

2- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04 تحت إشراف د. قريشي محمد، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، قسم الحقوق، تخصص: ق. جنائي، 2012-2013، مشار إليه: أحمد مسعود مريم: المرجع نفسه، ص 13.

من المجرمين التقليديين وفي هذا الصدد تناول تعريف المجرم المعلوماتي وإبراز سماته (الفرع الأول) ثم أصناف ومرتكبي هذه الجرائم (الفرع الثاني).

الفرع الأول: تعريف المجرم المعلوماتي وخصائصه

إن الاشخاص الذين يقومون بارتكابها عادة يكونون من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه أدنى حد من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الأنترنت، وهذا ما سنوضحه.

أولا: المجرم المعلوماتي[1]

هل كل شخص سواء طفل، رجل، أنثى، يأتي أفعالا إرادية تشكل سلوكا إيجابيا أو سلبيا باستخدام تقنية المعلوماتية لإحداث نموذج إجرامي بالاعتداء على حق أو مصلحة.

وسمات المجرم المعلوماتي تشبه في كثير من الأحيان سمات المجرمين قد يكونوا من ذوي الباقات البيضاء، حيث أن كل من هؤلاء المجرمين قد يكونوا من ذوي المناصب الرفيعة والمستوى العالي، ومن ذوي التخصصات والكفاءات العالية ويتمتعون بالذكاء والقدرة على التكيف الاجتماعي في المحيط الذي يعيشون فيه.

ثانيا: خصائص المجرم المعلوماتي

يتميز المجرم المعلوماتي بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين، ومن أهم هذه الخصائص ما يلي:

1- حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص: علم الإجرام والعقاب، إشراف: د. شادية رحاب، كلية الحقوق والعلوم السياسية، باتنة، السنة الجامعية 2011-2012، ص 27.

أ- الذكاء:

وهي أهم صفات مرتكب الجرائم المعلوماتية لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج، فهو ينشأ من تقنيات التدمير الناعمة (Sabotage soft) فيكفي أن يقوم المجرم المعلوماتي بالتلاعب بالبيانات وبرامج الحاسب الآلي لكي يمحو أو يدمر هذه البيانات أو يعطل استخدام هذه البرامج[1].

ب- المهارة:

وهي المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيات الإعلام، أو بمجرد التفاعل الاجتماعي مع الآخرين، إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال[2].

ج- المعرفة:

تتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، إذ أن المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا بجريمته، كون المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته[3].

1- سعيداني نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص: علوم جنائية، إشراف: زرارة صالحي الواسعة، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، السنة الجامعية 2012-2013، ص 57.

2- نائلة عادل محمد فريدة قورة، مرجع سابق، ص 08.

3- المرجع نفسه، ص 57.

بالإضافة إلى السلطة والوسيلة، وما يميز المجرم المعلوماتي هي الدوافع التي تدفعه لارتكاب جريمته فهي مختلفة ومتعددة قد تكون السعي وراء تحقيق الربح، وقد تكون أيضا الانتقام من المسؤول في العمل أو الوظيفة التي ينتمي إليها، وقد تكون الرغبة أيضا في قهر النظام والتفوق على وسائل التقنية وتعقيدها، وقد يكون الدافع أيضا يجب التعلم والاستكشاف كما أنه قد يرتبط بالسياسة والايديولوجيا وغيرها من البواعث[1].

الفرع الثاني: أصناف وصفة مرتكبي الجرائم المتصلة بتكنولوجيا الاعلام والاتصال:

يمكن تقسيم مجرمي تكنولوجيات الاعلام والاتصال إلى طوائف مختلفة، وضمن أن يكون المجرم لواحد مزيجا من أكثر من طائف وتتمثل هذه الطوائف:

أ- الطائفة الأولى: صغار مجرمي المعلوماتية

ويسميها البعض صغار نوابغ المعلوماتية، ويقصد بهم الشباب البالغ المفتون بالمعلوماتية وأنظمتها[2].

رغم الجدل الذي أثير لهذه الفئة إلا أنه في الواقع يجب عدم التقليل من خطورة هؤلاء الأشخاص، فهذه الفئة قد تتعدى مرحلة الهواية والعبث لتحل مرحلة متقدمة أكثر في مجال ارتكاب الجرائم المعلوماتية، وهي مرحلة الاحتراف، لأن هذه الفئة تكون أكثر تقبلا لأي أفكار تعرض أو تفرض عليها خاصة إذا كانت تحمل المغامرة والإثارة والتحدي في طياتها.

1- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، (د.ط)، دار الجامعة الجديدة، الإسكندرية، 2007، ص 33.

2- الشوا ساسي، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط01، دار النهضة العربية، القاهرة، ص 39.

ب- الطائفة الثانية: القراصنة (Pirat)

قراصنة المعلومات هم عادة مبرمجون من أصحاب الخبرة يهدفون إلى الدخول إلى الأنظمة المعلوماتية غير المسموح لهم بالدخول إليها وكسر الحواجز الأمنية المحيطة بهذه الأنظمة، ويمكن تصنيف القراصنة إلى صنفين:

أ- القراصنة الهواة العابثون أو الهاكرز (Hakers)

يرون في اختراق الأنظمة المعلوماتية تحديا لقدراتهم الذاتية، يقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون على اقتحام المواقع الأمنية أو بمجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع، ولا توجد دوافع تخريبية وراء أعمالهم، وهذه الطائفة غالبا ما تكون من هواة الحاسوب، بل قد يكون الفضول وجب المعرفة والتعمق في عمل الأنظمة المعلوماتية دافعهم الأول[1].

وأن هناك قيمة مميزة لهذه الفئة ألا وهي تبادلهم للمعلومات فيما بينهم تحديدا التشارك في وسائل الاختراق وآليات نجاحها في مواطن الضعف، في نظم الحاسوب والشبكات الخاصة عن طريق النشرات الإعلامية الإلكترونية، ومجموعات الأخبار.

ب- القراصنة المحترفون (Crackers)

هذه الفئة تعكس اعتداءاتهم ميولا إجرامية خطرة تنبئ في رغبتها في إحداث التخريب، ويتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب.

1- عرفت اتفاقية الأمم المتحدة لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم (55/63) المؤرخة في 2000/04/12 الهاكر (المخترق) بأنه: «المبرمج المتوقف جدا ولكنه يستخدم جل طاقته في الاتجاه غير شرعي لمحاولة اختراق أنظمة حاسوبية بهدف إثبات قدراته أو التباهي بها وأحيانا لأهداف إجرامية».

وأثبت الواقع العملي أن الهاكرز يستعين بالكراكر إذا ما صادفه أي نوع من أنواع الحماية، وغالبا ما يكون هدف هذه الفئة هو الحصول على المال أو بغرض الشهرة وأعمارهم تتراوح بين 25-45 عاما[1].

ج- الموظفون العاملون في مجال الأنظمة المعلوماتية:

نظرا لأن النظام المعلوماتي هو مجال عملهم الأساسي، ونظرا لمهارات والمعرفة التقنية التي يتمتعون بها فإنهم يقترفون بعض الجرائم المعلوماتية التي من الممكن أن تحقق أهدافهم الشخصية وأهمها الكسب المادي، لأن العلاقة الوظيفية التي تربط بين الموظف والمجني عليه تجعل عملية ارتكابه للجريمة المعلوماتية أسهل نظار للثقة التي يتمتع بها[2].

وهناك فئة من الموظفين الحاقدين على عملهم أو على مؤسساتهم الذين قد يقومون بأفعال إجرامية لا تهدف إلى الكسب المادي بل هدفهم الانتقام والثأر من أصحاب عملهم، وهذه الفئة يذهب البعض إلى تسميتها بفئة "مجرمي المعلوماتية الحاقدين"[3].

د- مجرمو المعلوماتية أصحاب الآراء المتطرفة:

تتألف هذه الفئة من الجماعات الإرهابية أو المتطرفة التي تتكون من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات، يرتكز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه[4].

1- محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، ط01، دار الحامد للنشر والتوزيع، عمان، 2007، ص 73.

2- أحمد خليفة الملط، المرجع السابق، ص 62.

3- محمد سليمان مصطفى، جرائم الحاسوب وأساليب مواجهتها، مجلة الآنى والحياة، العدد 199، 1999، ص 50.

4- نائلة عادل محمد فريد قورة، مرجع سابق، ص 58.

فهذه الجماعات تدافع عن قضية أو معتقد معين ولا تهدف إلى تحقيق الربح المادي، وهي تختلف عن المنظمات الإجرامية المنظمة، لأن هذه الأخيرة تهدف إلى تحقيق مصالحها الشخصية المباشرة.

هـ- مجرمو المعلوماتية في إطار الجريمة المنظمة:

هذه الجريمة تعد من جرائم ذوي النفوذ والسلطات التي قد يتورط فيها رجال السياسة وأصحاب المناصب الرفيعة فهي تعد بالفعل من جرائم ذوي الباقات البيضاء.

وتسعى هذه المنظمات إلى الاستفادة من أجهزة التقنية المعلوماتية الحديثة المتمثلة في جهاز الحاسوب وشبكة الأنترنت لتسوية أعمالها وتسهيل تنفيذها مثلا: غسيل الأموال، تجارة الرقيق، الأعضاء البشرية[1].

1- عمر أبو الفتوح عبد العظيم (الحماسي)، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دارسة مقارنة، (د.ط)، دار النهضة العربية، القاهرة، 2010، ص 102.

المبحث الثاني: تصنيفات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

لم يكتف القانون الجزائري باستحداث جرائم جديدة تتصدى للعدوان على أنظمة المعالجة الآلية للمعطيات في قانون العقوبات رقم: 04-15 المؤرخ في 10 نوفمبر 2004[1]، ولكنه وضع أيضا القانون رقم 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد خلف هذا القانون فئة جديدة من الجرائم أطلق عليها اسم "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، وتشمل حسبه جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في قانون العقوبات، أي الجرائم محل الدراسة هنا، المحددة في القسم السابع مكرر من الفصل الثالث الباب الثاني من الكتاب الثالث من قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية (المادة02، فقرة أ من القانون رقم 09-04).

وسنتطرق في هذا المبحث لتصنيفات هذه الجرائم حسب التقسيم الذي تبناه المشرع الجزائري، ومنه نقسم هذا المبحث إلى مطلبين نتناول في المطلب الأول: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وفي المطلب الثاني: الجرائم الأخرى المرتكبة عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

1- الأمر رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، الجمهورية الجزائرية، الجريدة الرسمية، عدد 71.

المطلب الأول: جرائم المساس بأنظمة المعالجة الآلية للمعطيات الإلكترونية في إطار قانون العقوبات

الجرائم الماسة بالأنظمة المعلوماتية وإن كانت تختلف في أركانها وعقوباتها إلا أن ما، أي أن القاسم المشترك بينهما هو نظام المعالجة الآلية، وهو ما سنبرزه بشيء من التفصيل على النحو التالي:

الفرع الأول: صور الجرائم الواردة في إطار قانون العقوبات الجزائري

نص المشرع الجزائري من خلال نصوص قانون العقوبات على مجموعة من الأفعال من خلال المواد 394 مكرر إلى 394 مكرر7[1]، التي يمكن تلخيصها فيما يلي:

- الدخول أو البقاء داخل منظومة معلوماتية عن طريق الغش أو جزء منها (المادة 394 مكرر1).
- إتلاف أو حذف أو لمعطيات المنظومة أو تخريب أشغال المنظومة (المادة 394 مكرر2).
- إدخال بطريق الغش معطيات في نظم المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها (المادة 394 مكرر1).
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر 1/2).
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر2/2).

1- القانون 04-15 المتضمن قانون العقوبات المعدل والمتمم، المرجع السابق.

وعليه انطلاقا من هذا التقسيم سوف نستعرض هذه الجرائم بشيء من التفصيل على النحو التالي:

أولا: جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

نص المشرع الجزائري على جريمة الدخول أو البقاء داخل منظومة معلوماتية عن طريق الغش أو في جزء منها في المادة (394 مكرر1)، ويمكن القول وانطلاقا من نص المادة أنه ولقيام هذه الجريمة لابد من اشتمالها هما المادي والمعنوي، إذ لا يتحقق المفهوم القانوني للجريمة إلا بوجود نص تشريعي وارتكاب فعل أو امتناع، إذ لا جريمة ولا عقوبة إلا بنص، كما سنلتزم الإضافة إلى ذلك عدم مساءلة الشخص عن الفعل أو الترك إلا إذا قام به بإرادته واختياره، فهناك:

- الصورة البسيطة لفعل الدخول أو البقاء غير المشروع.
- الصورة المشددة لجريمة الدخول إلى النظام أو البقاء غير المشروع.

1- الركن المادي في الصورة البسيطة لفعل الدخول أو البقاء غير المشروع:

أ- **فعل الدخول:** [1] بما أن المشرع لم يحدد وسيلة الدخول إلى النظام، فإنه يمكن الدخول بأية وسيلة كانت، وذلك عن طريق كلمة السر الحقيقية متى كان الجاني غير مخول باستخدامها أو باستخدام برنامج أو شفرة خاصة أو عن طريق استخدام الرقم الكودي لشخص آخر أو الدخول من خلال شخص مسموح له بالدخول[2].

وتقع هذه الجريمة من أي إنسان أيا كانت صفته سواء كان يعمل في مجال الأنظمة أم لا علاقة له بنظم الكمبيوتر وسواء كان يستطيع الاستفادة من النظام أم لا، إنما يشترط

1- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، (د.ط)، المكتبة القانونية، القاهرة، 1999، ص 121.

2- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، (د.ط)، دار الفكر الجامعي، الإسكندرية، 2002، ص 28-29.

ألا يكون من أولئك الذين لهم حق الدخول إلى النظام، ويتحقق الدخول غير المشروع كذلك متى كان مخالفا لإرادة صاحب النظام أو من له حق السيطرة عليه، كتلك الأنظمة المتعلقة بأسرار الدولة أو دفاعها أو تتضمن بيانات شخصية تتعلق بجريمة الحياة الخاصة بحيث لا يجوز الاطلاع عليها[1].

ويتحقق فعل الدخول غير المشروع إلى النظام، حتى دخل الجاني إلى النظام كله أو جزء منه كالدخول إلى شبكة الاتصال أو البرنامج، وكذلك يتحقق الدخول غير المشروع متى كان مسموحا بالدخول لجزء معين في البرنامج وآخر غير مسموح له بالدخول فيه.

فمثلا لو فرضنا أن الجاني دخل إلى موقع –أمازون دوت كوم– وهو موقع للبيع الإلكتروني معد للجمهور، لكنه تجاوز الموقع إلى البيانات الخاصة بإعداد الموقع وتنظيمه في صفحة (Home Page) وتنطوي على معلومات لا يجوز للجمهور الدخول إليها، وبالتالي يكون فعل الجاني مكونا لجريمة الدخول غير المشروع، رغم أن الموقع في ذاته مفتوحا للجمهور[2]، لذلك يخرج من نطاق الدخول غير المشروع، الدخول إلى برنامج منعزل عن نظام المعلومات الذي يحظر عليه الدخول فيه.

كما لا تتوفر الجريمة إن اقتصر دور الجاني على مجرد قراءة الشاشة دون الولوج إلى داخل النظام، إذ بهذه الأفعال لا تقوم جريمة الدخول غير المشروع للنظام المعلوماتي[3].

1– علي عبد القار القهوجي، المرجع السابق، ص 123.

2– خيثر مسعود، الحماية الجنائية لبرامج الكمبيوتر، (د.ط)، دار الهدى، عين مليلة، الجزائر، 2010، ص 115–116.

3– عبد الفتاح بيومي حجازي، النظام القانوني كحماية التجارة الإلكترونية، المرجع السابق، ص 30.

ب- فعل البقاء: يقصد به «التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام»[1]، ومما لاشك فيه أن البقاء داخل نظام الكمبيوتر بعد دخوله طريق الخطأ لا يختلف عن الدخول غير المصرح به من حيث وجوب التجريم، فاتجاه إرادة الفاعل إلى البقاء داخل هذا النظام على الرغم من معرفته أنه غير مصرح له بالدخول، لا يختلف في جوهره عن الدخول غير المصرح به إلى نظام الكمبيوتر.

فالنتيجة الإجرامية في الحالتين واحدة وهي الوصول إلى نظام غير مصرح للدخول إليه، فالمصلحة التي يحميها القانون هي حماية نظام الكمبيوتر في الحالتين[2]، وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا، والإشكالية التي تثور في هذا الصدد: متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء؟

ذهب رأي من الفقه إلى أن جريمة الدخول تتحقق منذ اللحظة التي يتم فعلا الدخول إلى البرامج، وتبقى مدة من الزمن داخله، وبعد تلك اللحظة تبدأ جريمة البقاء وتنتهي بانتهاء حالة البقاء، ويذهب رأي آخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه أن بقاءه داخل النظام غير المشروع.

بينما يذهب رأي راجع من الفقه إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجوال داخل النظام أو يستمر في التجوال داخله بعد انتهاء الوقت المحدد، أي منذ علم الجاني أنه ليس حق الدخول، فإذا دخل وظل ساكنا تظل الجريمة جريمة دخول إلى النظام، أما إذا بدأ في التجوال حتى مع علمه بأن بقاءه ممنوع في النظام، فإن جريمة البقاء داخل النظام تبدأ من اللحظة لأنه من التجول في النظام يعلم

1- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، المرجع السابق، ص 133.

2- نائلة عادل محمد فريد قورة، جرائم الكمبيوتر الاقتصادية، مرجع سابق، ص 346.

مسبقا أن مبدأ دخوله واستمراره فيه غير مشروع، ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام[1].

2- الركن المادي: تعتبر جريمة الدخول أو البقاء من الجرائم العمدية[2]، بحيث يكفي فيها القصد العام، فيكفي لتوافر هذه الجريمة أن يعلم الجاني أنه قد دخل إلى نظام ليس له حق الدخول فيه أو تعمد البقاء فيه، رغم انتهاء مدة حقه في البقاء ولول كان الدخول مشروعا، أما إذا انتفى علمه فإنها لا تتوافر الجريمة، كأن يجهل وجود حظر الدخول، أو أنه مسوح له الدخول فيه، ولا يتأثر القصد الإجرامي بالباعث على الدخول أو البقاء، فيظل القصد الإجرامي قائما حتى ولو كان الباعث من الدخول أو البقاء للفضول أو التنزه أو إثبات القدرة على الانتصار على النظام.

أما عن القصد الخاص، فلا يبدو من خلال نص المادة 394 مكرر من قانون العقوبات أن المشرع الجزائري يتطلب وجود نية خاصة لدى الجاني حتى تقوم جريمة الدخول أو البقاء، ذلك أن القصد الخاص علم وإرادة تنصرفان إلى وقائع خارجة عن أركان الجريمة إلى وقائع لا تدخل ضمن عناصرها[3].

1- أمحمدي بوزينة آمنة، الحماية الجنائية للمعطيات الإلكترونية في إطار القانون الجزائري (مذكرة تحليلية لقانوني العقوبات وحقوق المؤلف)، أستاذة محاضرة قسم (ب)، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلين الشلف، مجلة سيليوفيليا للدراسات المكتبات والمعلومات، العدد 05/ 7781-2661، issn، تاريخ النشر: 30-03-2020، ص 102.

2- المرجع نفسه، نفس الصفحة.

3- أشرف شمس الدين، الحماية الجنائية للمستند الإلكتروني، (د.ط)، دار النهضة العربية، القاهرة، 2006، ص 45، للمزيد من التفصيل: قسيمة محمد، خضيري حمزة، مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في قانون العقوبات الجزائري، مجلة صوت القانون، المجلد السابع، العدد 02، نوفمبر، 2002، ص 136.

ثانيا: الصورة المشددة لجريمة الدخول إلى النظام أو البقاء غير المشروع

نصت المادة 394 مكرر (2-3) قانون العقوبات على أنه: «تضاعف العقوبة إذ ترتب على ذلك حذف أو تغير لمعطيات المنظومة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من الستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000دج».

باستقراء نص المادة (394) مكرر 2 و3 من قانون العقوبات، نجد أنها قد نصت على ظرفين مشددين تشدد بهما عقوبة الدخول أو البقاء داخل النظام، ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام أو عدم قدرة النظام على تأدية وظيفته ويكفي لتوافر هذا الظرف المشدد أن تكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت، وهي محو النظام أو عدم قدرته على أداء وظيفته أو تعديل البيانات[1]، وبذلك الهدف الأساسي من هذا النص هو التعرض لكل محاولة لإعاقة أو تحريف قد تلحق بهذا النظام، وبذلك فإنه لتحقق هذه الجريمة يستلزم توافر الركن المادي والركن المعنوي.

أولا: الركن المادي

يتمثل الركن المادي إما في فعل توقيف أو تعطيل نظام المعالجة الآلية للمعطيات عن أداء نشاطه ولا يشترط أن تقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام، بل يكفي أن يؤثر على هذه العناصر فقط سواء المادية (جهاز الكمبيوتر نفسه، شبكات الاتصال، أجهزة النقل)، أو المعنوية البرامج والمعطيات[2].

1- خيثر مسعود، مرجع سابق، ص 119.

2- أمال قارة، مذكرة ماجستير بعنوان: الجريمة المعلوماتية، كلية الحقوق، جامعة الجزائر، 2001، ص 115.

1- التعطيل أو التوقيف: تعتبر عملية إعاقة سير عمل نظام المعالجة الآلية للمعطيات بأنها: «فعل يتسبب في تباطؤ أو ارتباك عمل نظام المعالجة، ومن ثم ينتج عن ذلك تغيير في حالة عمل النظام، وهذا الارتباك الناجم عن الإعاقة تتأثر به أجهزة الكمبيوتر والبرامج على السواء»[1]، ومن أمثلة التخريب أو التعطيل الواقع على أنظمة المعالجة قضية روبير موريس (Rober morris)، وهي أحد أول الهجمات الكبرى والخطرة في بيئة الشبكات، ففي مارس عام 1988 تمكن طالب يبلغ من العمر 23 عاما، ويدعى روبير موريس من إطلاق فيروس عرف باسم "دودة مورس" عبر الأنترنت، أدى إلى إصافة 06 آلاف جهاز يرتبط معها حوالي 60.000 نظام عبر الأنترنت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد قدرته الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصانة بحوالي مئة مليون دولار، إضافة إلى مبلغ أكثر من ذلك تمثل في الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة[2].

ويحصل فعل التعطيل أو التوقيف بأي وسيلة كانت، فالمشرع لم يشترط وسيلة معينة، وبالتالي يستوي أن يكون بوسيلة مادية أو معنوية، ومن أمثلة وسائل التعطيل المادية، استعمال العنف لمنع الوصول إلى الأجهزة ككسرها أو تحطيمها، أو تحطيم إسطوانة أو قطع شبكات الاتصال أو سكب كوب شاي أو أي مادة أخرى أو منع العاملين من الوصول إلى النظام، أما الإعاقة أو التعطيل بوسيلة معنوية، فقد تتحقق بإدخال فيروس عن البرنامج أو تعديل كلمة السر أو كيفية أداء النظام لوظيفته بوسيلة تؤدي إلى أن يتباطئ في أدائه لوظيفته المعلوماتية داخل النظام المعلوماتي[3].

1- خيثر مسعود، المرجع السابق، ص 121.

2- يونس عرب: جرائم الكمبيوتر والأنترنت، بحث مقدم إلى مؤتمر الأمن العربي تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 2002.

3- علي عبد القادر قهوجي: الحماية الجنائية لبرامج الكمبيوتر، المرجع السابق، ص 139.

2- الإفساد أو التعييب: يقصد به كل فعل وإن كان لا يعطل نظام معالجة البيانات، لكنه يجعل هذا النظام غير قادر على الاستعمال السليم، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.

وتنوع وسائل التغييب أو الإفساد كاستخدام القنبلة المعلوماتية، بحيث يدخل من خلالها مجموعة من المعطيات تتكاثر داخل النظام بحيث تجعله غير صالح للاستعمال[1]، أو استخدام فيروس يطلق عليه "حصان طراودة"، وغير ذلك من الفيروسات التي توقف أو تفسد أو تعطل النظام[2].

ثانيا: الركن المعنوي

جريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات جريمة عمدية، بحيث يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصرية العلم والإرادة، على اعتبار اتجاه إرادة الجاني إلى فعل الإفساد مع علمه بأن نشاطه الإجرامي من شأنه أن يوصله إلى تلك النتيجة، فإذا قام شخص يتعامل مع النظام بصورة مشروعة بإعاقة أو إفساد النظام نتيجة لخطأ في التشغيل أو التعامل مع البيانات ينتفي القصد الجنائي لديه ولا يسأل عن هذه الجريمة[3].

1- في سنة 1996 قام مصمم ومبرمج شبكات كمبيوتر ورئيس سابق لشركة أوميغا (Omega)، بإطلاق قنبلة إلكترونية بعد 20 يوما من فصله من العمل استطاعت أن تلغى كافة التصاميم وبرامج الانتاج لإحدى كبرى مصانع التقنية العتالي في نيوجرسي والمرتبطة والمؤثرة على نظم التحكم المستحدثة في (Nasa) والتجربة الأمريكية ملحقا خسائر بلغت 10 ملايين دولار، مشار إليه: يونس عرب، جرائم الكمبيوتر والأنترنت، المرجع السابق، دون صفحة.

2- ضياء مصطفى عثمان، السرقة الإلكترونية (دراسة فقهية)، ط01، دار النفائس للنشر والتوزيع، عمان، 2011، ص 73-75.

3- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص 30.

ثالثا: الاعتداءات العمدية على المعطيات الموجودة داخل النظام

النشاط الإجرامي في هذه الجريمة ينحصر في أفعال الإدخال والمحو والتعديل، ويكفي توافر إحداها لقيام الجريمة فلا يشترط اجتماعها معا، ومن ثم يقوم الركن في الجريمة، لكن القاسم المشترك في هذه الأفعال جميعا هو انطوائها على تلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل آخر قائمة[1].

من هنا يمكن القول أن النشاط الإجرامي لهذه الجريمة أنها تنصب على المعطيات أي المعلومات المعالجة آليا التي أصبحت رموزا وإشارات وليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل النشاط الإجرامي يقتصر على المعطيات خارج النظام سواء قبل دخولهما أم خروجها، أما المعلومات غير المعالجة التي لم تدخل إلى النظام، فهي خارج نطاق الحماية المشمولة لهذا النص، وإن كان يجوز حمايتها وفقا لنصوص جنائية أخرى[2].

وتقوم هذه الجريمة على صورتين هما:

أولا: الاعتداءات العمدية على المعطيات الموجودة داخل النظام

النشاط الإجرامي في جريمة الاعتداء العمدي على المعطيات يتجسد في إحدى الصور الثلاث التالية: [3]

1-فعل الإدخال (L'intrusion)

2-فعل المحو (L'effacement)

1- د. محمد نجيب حسني، الموجز في شرح قانون العقوبات، القسم الخاص، (د.ط)، دار النهضة العربية، القاهرة، 2003، ص 253.

2- علي عبد القادر القهوجي، المرجع السابق، ص 58.

3- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص 179،

3-فعل التعديل (Modification)

لا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط: كي يتوافر الركن المادي، وأفعال الإدخال والمحو والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة أو محو أو تعديل معطيات موجودة من قبل، وهذا يعني أن النشاط الإجرامي في هذه الجريمة إنما يرد على محل أو موضوع محدد وهو المعطيات أو المعلومات التي تمت معالجتها آليا التي أصبحت مجرد إشارات أو رموزا تمثل تلك المعلومات، وليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام أي التي يحتويها النظام وتشكل جزء منه[1].

عموما التلاعب في المعطيات الموجودة داخل النظام يتخذ إحدى الأشكال التالية:

1- الإدخال: يقصد بفعل إضافة معطيات جديدة على الدعامة الخاصة بالمعلومات المعالجة آليا سواء كانت خالية أم كان يوجد عليها معطيات من قبل بقصد التشويش على صحة البيانات القائمة، ولعل اصطناع المعلومات هو الأكثر سهولة في التنفيذ ولاسيما في المنشآت ذات الأموال حيث يعد المسؤول في القسم المعلوماتي في أفضل وضع يؤهله لارتكاب هذا النمط غير المشروع من التلاعب[2].

ويتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة، هذه الأخيرة ليسحب بمقتضاها النقود من أجهزة السحب الآلي، وذلك حين يستخدم رقمه الخاص والسري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ

1- فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية المزمع عقده بأكاديمية الدراسات العليا بيلسا في أكتوبر 2009، ص 30.

2- نبيل صقر، جرائم الكمبيوتر والأنترنت، موسوعة الفكر القانوني، (د.ط)، دار الهلال للخدمات الإعلانية، الجزائر، 2005، ص 141.

الموجود في حسابه، وكذلك الحامل الشرعي لبطاقة الائتمان التي يسدد عن طريقها مبلغ أكثر من المبلغ المحدد له.

وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أو من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب (فيروس) يضيف معطيات جديدة.

2- المحو: يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة ومثالها: قيام بعض المسؤولين بالاستيلاء على مبلغ قدره 61 ألف دولار، كانت قد أرسلته إحدى شركات التأمين لصالح أحد المراكز الطبية وقاموا بفتح حسابات وهمية وضعوا المبلغ بها وحتى تتم هذه العملية بنجاح قاموا بمحو حسابات من سجلات الحاسب الآلي للمركز الطبي وهي حسابات الموثقين، وذلك إما جعلها غير قابلة للتحصيل وإما بحذفها من الملفات[1].

3- التعديل: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى، وتتحقق فعل المحور والتعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها، وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة Gomme d'effacement أو برنامج الفيروسات بصفة عامة[2].

1- عبد الفتاح بيومي جهازي، النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص 49.

2- فشار عطاء الله، المرجع السابق، ص 30-31.

ثانيا: المساس العمدي بالمعطيات خارج النظام

وفر المشرع الجزائري الحماية الجزائية للمعطيات في حد ذاتها من خلال تجريمه السلوكات التالية.

فنص المادة 394 م 2 ستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة أم لا كأن تكون مخزنة على أشرطة أو أقراص أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

1- الركن المادي: الواضح من خلال صياغة هذا النص أنه تضمن صورتين للركن المادي لهذه الجريمة، فهناك:

الصورة الأولى: نصت المادة 394 مكرر 1/2[1]، على تجريم تصميم أو بحيث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوصة عليها في هذا القسم، أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من احدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بأهداف المنافسة غير المشروعة، الجوسسة، الارهاب، التحريض على الفسق ....الخ.

الصورة الثانية: جرمت الفقرة الثانية من 394 مكرر 2/2 حيازة أو افشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم.

1- المادة 394 مكرر 1/2 من القانون رقم 66-156 المتضمن قانون العقوبات المعدل والمتمم بموجب القانون 04-15، المرجع السابق.

2- الركن المعنوي: تتحقق هذه الجريمة لمجرد توافر النية بكافة عناصرها، العلم، الإدارة، وبالتالي لا يشترك لقيامها نية الاضرار بالشخص مالك البرنامج أو صاحب النظام، وإن كان الضرر قد يتحقق في الواقع نتيجة النشاط الاجرامي إلا أنه ليس عنصرا في الجريمة.

الفرع الثاني: عقوبة جرائم الاعتداء على نظام المعالجة الآلية للمعطيات:

طبقا للمادة 13 من الاتفاقية الدولية للإجرام المعلوماتي، فإن العقوبات المقررة للإجرام المعلوماتي يجب أن تكون رادعة وتتضمن عقوبات مالية وسالبة للحرية، تتمثل في عقوبات أصلية وعقوبات تكميلية[1]. تطبق على الشخص الطبيعي، كما توجد عقوبات تطبق على الشخص المعنوي بناءا على تبني مبدأ مساءلته الشخص المعنوي الواردة في المادة 12 من الاتفاقية.

كما نص المشرع على مجموعة من العقوبات عن الجرائم الماسة بالنظام والمتمثلة في عقوبات أصلية وأخرى تكميلية بموجب المواد من 394 مكرر إلى 394 مكرر 5، كما نص على عقوبة الأشخاص المعنوية والأشخاص الطبيعية، وأيضا عقوبة المساهمة والشريك في الجريمة.

واعتمد المشرع أثناء وضعه لهاته الجرائم على معيار أساسه الخطورة الإجرامية لكل جريمة على حدا، بحيث اتبع مبدأ الهرمية في التدرج في سلم العقوبات، فنص على جريمة الدخول أو البقاء في الصورة البسيطة والمشددة، تم نص على جريمة الاعتداء العمدي على المعطيات باعتبارها أشد خطورة من سابقها، ذلك أنها تستهدف المعطيات الموجودة داخل النظام بها فيها البيانات، والبرامج، المعطيات، وأي اعتداء عليها سيؤدي لا محال إلى وقف النظام أو تعطيله أو تغيير سير وجهة هذا النظام.

1- الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ: 2001/11/08.

أولا: العقوبات المقررة للشخص الطبيعي

1- العقوبات الأصلية:

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

- الدخول والبقاء بالغش (الجريمة البسيطة): العقوبة المقررة هي 03 أشهر إلى سنة حبس و50.000 ج إلى 100.000 دج غرامة (المادة 394 مكرر).

- الدخول والبقاء بالغش (الجريمة المشددة): تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة، وتكون العقوبة الحبس من 06 أشهر إلى سنتين وغرامة من 50.000 إلى 150.000دج، إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام أشغال المنظومة (المادة 394 مكرر 3/2).

- الاعتداء العمدي على المعطيات طبقا لنص المادة 394 مكرر1، فالعقوبة المقررة للاعتداء العمدي على المعطيات الموجودة داخل النظام الحبس من 06 أشهر إلى 03 سنوات وغرامة من 50.000 دج إلى 2000.000 دج، أما العقوبة المقررة لاستخدام المعطيات وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، العقوبة المقررة هي الحبس من شهرين إلى 03 سنوات وغرامة من 1000.000 دج إلى 5000.000 دج (394 مكرر2) [1].

1- الأمر رقم 66-156 المؤرخ في 18 صفر 1386، الموافق لـــ 08 يونيو سنة 1966 يتضمن قانون العقوبات المعدل والتمم بالقانون 04-15، الجمهورية الجزائرية، الجريدة الرسمية عدد 71 المؤرخ في 10 نوفمبر 2004، المرجع السابق.

2- العقوبات التكميلية:

نصت المادة (394 مكرر3) من قانون العقوبات على العقوبات التكميلية المتمثلة في:

* **المصادرة:** وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية، على مراعاة حقوق الغير حسن النية.

* إعلاق المواقع والأمر يتعلق بالمواقع (Les sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

* **إعلاق المحل أو مكان الاستغلال:** إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق المقهى الإلكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكها[1].

ثانيا: العقوبات المقررة للشخص المعنوي

أقر المشرع الجزائري مبدأ مسائلة الشخص المعنوي في القانون 15/04 المؤرخ في 10-11-2004 المعدل والمتمم للأمر 156/66، وذلك بنص المادة (51 مكرر) من هذا التعديل[2]، كما تجدر الإشارة أن المشرع الجزائري، وقد أقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي، وذلك في نص المادة (18 مكرر)

1- فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، المرجع السابق، ص 33-34.

2- محمد مزاولي، نطاق المسؤولية الجنائية لمسيري المؤسسات الاقتصادية في القانون الجزائري (دراسة مقارنة)، رسالة ماجستير، المركز الجامعي، الجزائر، 2006، ص 310.

من القانون رقم 15/05 المتضمن قانون العقوبات[1].

أما بالنسبة لعقوبات الغرامة المطبقة على الشخص المعنوي عند ارتكابه أحد الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة (394 مكرر4) من قانون العقوبات 05 مرات الحد الأقصى المقررة للشخص الطبيعي.

ثالثا: عقوبة الاشتراك والشروع في الاعتداء على نظام المعالجة الآلية للمعطيات

1- عقوبة الاشتراك: نصت عليه المادة (11) من الاتفاقية الدولية للإجرام المعلوماتي، وقد تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة (394 مكرر 5)، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ولم يخضعها لأحكام المادة (176) من قانون العقوبات المتعلقة بجمعية الأشرار[2].

من خلال استقراء نص المادة أعلاه، نجد أن المشرع الجزائري لم يخرج عن القواعد العامة لعقوبة الشريك، حيث رصد لها نفس عقوبة الجريمة التامة، ذلك أن جرائم الاعتداء على نظام المعالجة الآلية للمعلومات، أغلبها يتم في شكل مجموعات، وإن لم

1- نصت المادة 18 مكرر، على أن العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح هي:
أ- الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.=
ب- وحدة أو أكثر من العقوبات الآتية:
- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 05 سنوات.
- الإقصاء في الصفقات العمومية لمدة لا تتجاوز 05 سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا ولمدة لا يتجاوز 05 سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 05 سنوات.

2- حيث نصت المادة (399) مكرر 05 من قانون العقوبات الجزائري: «كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية يعاقب بالعقوبات المقررة بالجريمة ذاتها»، انظر الأمر 66-156 المتضمن قانون العقوبات، المصدر السابق، ص 158.

يسبق اتفاق بين المجموعة على ارتكاب هذه، ولكن النتيجة الإجرامية بين اتفاق ضمني بين أفراد المجموعة، إذ أن هذه الجرائم لا تتطلب اجتماع حقيقي فيما بين شخصين أو أكثر، وإنما يتصور الاتفاق الجنائي بمجرد انتقال كلمة الرضى شخص إلى آخر، وإن لم يكن بينهما معرفة سابقة ويستوي أن يكون أفراد الاتفاق مجموعة أشخاص طبيعية أو معنوية.

وأن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص، ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها، فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد.

فبالنسبة لمجموعة أو الاتفاق يستوي أن يكون أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي، كما يستوي أن يعرف أشخاص الاتفاق بعضهم بعضها كما في العصابة أم تكون مجرد مجموعة من الأشخاص لا يعرف أحدهم الآخر من قبل، ولكن اتفقوا فيما بينهم على القيام بالنشاط الإجرامي، المهم أن يتم الاتفاق بين شخصين على الأقل.

كما جرمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الشروع والاشتراك في ارتكاب الجرائم في المادة (19): «الاشتراك في ارتكاب أي جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف...»[1].

1- المرسوم الرئاسي 14-252 المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المصدر السابق، ص 07.

2- عقوبة الشروع في الاعتداء على نظام المعالجة الآلية للمعطيات:

الجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص، وقد نصت عليه المادة (11) من الاتفاقية الدولية للإجرام المعلوماتي، كما تبنى المشرع الجزائري فكرة العقوبة على الشروع في ارتكاب الجنح الماسة بنظام المعالجة الآلية للمعطيات بموجب المادة (394 مكرر7) من قانون العقوبات، وذلك رغبة منه في توفير حماية فعالة لهذا النظام[1].

المطلب الثاني: الجرائم التي ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية

فضلا عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات والتي يكون النظام المعلوماتي فيها محلا للجريمة، نتناول في هذا المطلب الجرائم التي ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، وهي جرائم القانون العام التي نص المشرع الجزائري على تدخل المنظومة المعلوماتية كوسيلة لارتكابها وسنقسم هذا المطلب إلى فرعين نتناول في (الفرع الأول) الجرائم المنصوص عليها في قانون العقوبات وفي الفرع الثاني الجرائم المنصوص عليها بموجب نصوص خاصة.

الفرع الأول: الجرائم المنصوص عليها في قانون العقوبات

سنتناول في هذا الفرع الجرائم التي يمكن أن تتدخل الوسيلة الإلكترونية في ارتكابها والتي نص عليها المشرع الجزائري في قانون العقوبات.

1- أمال قارة، مذكرة ماجستير بعنوان الجريمة المعلوماتية، المرجع السابق، ص 133.

أولا: جرائم الاعتبار

عالج المشرع الجزائري جرائم الاعتداء على شرف واعتبار الأشخاص وعلى حياتهم الخاصة في قانون العقوبات في الباب الثالث من الكتاب الثالث القسم الخاص منه في المواد من 296 إلى 300.

1- جريمة القذف عبر مواقع التواصل الاجتماعي في التشريع الجزائري

عرف المشرع الجزائري القذف في المادة (296) من قانون العقوبات بأنه: «كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها به أو إسناد إليهم أو إلى تلك الهيئة»[1]. وعلة تجريم القذف هو مساسه بشرف المجني عليه واعتباره، فهو يجعل الواقعة محل القذف سهلة التصديق وأقرب إلى الاحتمال، فضلا عن أن علانية هذه الواقعة تتيح مجالا سريعا للانتشار مما سبب إساءة لمكانة المجني عليه وهو ما جعل هذه الجريمة أشد جسامة من سائر جرائم الاعتداء وعلى الشرف والاعتبار.

2- أركان جريمة القذف عبر مواقع التواصل الاجتماعي

الركن المادي:

1- فعل الإسناد: «يقصد بالإسناد نسبة أمر أو واقعة إلى شخص معين، بأي وسيلة من وسائل التعبير»[2].

1- الأمر رقم 66-156 المتضمن قانون العقوبات، المعدل والمتمم بموجب القانون 04-15، المرجع السابق، ص 110.

2- فتوح عبد الله الشاذلي، شرح قانون العقوبات –القسم الخاص–، دون طبعة، دار المطبوعات الجامعية، الإسكندرية، 2001، ص 299، مشار إليه، ط.و، لسود موسى، جامعة العربي التبسي–تبسة، التكيف القانوني لجريمة القذف عبر مواقع التواصل الاجتماعي في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، العدد 5، 01-01-2019، ص 282 عبر المواقع:

http://www.aspj.ceist.dz/en1presentation evue/304.

يتحقق فعل الإسناد بأي وسيلة من وسائل التعبير سواء بالقول أو الصياح أو التهديد أو المنشورات أو اللافتات أو الإعلانات أو الكتابة، الإشارة، الرسوم، الصور، أو أية وسيلة تنقل فكرة الجاني إلى فكر شخص أو أشخاص آخرين، ويتحقق الإسناد سواء بنية القذف إلى المجني عليه على سبيل القطع والتأكيد، أو الشك أو الاحتمال...

2- موضوع الإسناد: يشترط في موضوع الإسناد 03 عناصر:

أ- تحديد الواقعة: وهو ما يميزه عن السب، فالقذف لا يكون إلا بإسناد واقعة معينة محددة إلى المجني عليه، ولكن دون أن يكون التحديد تاما وكاملا بذكر كل التفاصيل وهو ما يرجع للسلطة التقديرية للقاضي للتحديد التام والكامل للواقعة.

ب- أن تكون الواقعة موجهة للعقاب أو الاحتقار ممن أسندت إليه: أي أن الواقعة يجب أن يحرمها القانون ويعاقب عليها بعقوبة جنائية مثل واقعة التزوير أو الاختلاس، أو خيانة الأمانة، كما يمكن أن تكون العقوبة المقررة للواقعة تأديبية، وذلك لعمومية النص الجنائي «ويعاقب على نشر هذا الادعاء»[1].

ج- أن يكون إسناد الواقعة علنيا: يقصد بالعلانية: اتصال علم الجمهور بفعل أو قول أو كتاب أو تمثيل، وقد بين المشرع الجزائري في نص المادة 296 قانون العقوبات الجزائري صور للعلانية من عبارات الحديث أو الصياح أو التهديد، وبما أن مواقع التواصل الاجتماعي هي وسائل يستخدمها من يشاء لنشر الأخبار والآراء بشكل مكتوب أو مسموع فإنها تعتبر إعلاما بديلا، وهي من الوسائل الإعلامية الحديثة، والتي يمكن أن تطبق عليها القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

1- المادة 276 من الأمر 66-156، المتضمن قانون العقوبات المعدل والمتمم بموجب القانون رقم 04-15، المرجع السابق.

3- الركن المعنوي: هي جريمة عمدية، ولذلك لابد من توافر القصد الجنائي، وهو القصد العام، وهو علم الجاني بأن الوقائع التي يسندها كانت صادقة، وعلى ذلك اتجهت إرادته إلى إذاعة هذه الوقائع.

وبما أن الشروع في الجنح لا يعاقب عليه المشرع الجزائري إلا إذا نص على ذلك صراحة وجريمة القذف عبر المواقع التواصل، لم تنص ولو أي واحدة منها على فعل الشروع وبالتالي استبعاد تجريم الشروع أو المحاولة من شرعية التجريم والعقاب في التشريع الجزائري.

4- نماذج قانونية لجريمة القذف عبر مواقع التواصل الاجتماعي:

1- قذف الهيئات: نصت المادة 296 من قانون العقوبات الجزائري على أن محل جريمة القذف هما الاشخاص أو الهيئات، بينما نصت المادة 144 من ق.ع على جريمة القذف على شخص رئيس الجمهورية، كما نصت المادة 146 م أيضا على القذف الموجه ضد البرلمان أو إحدى غرفه أو ضد الجهات القضائية أو ضد الجيش الوطني الشعبي، أو هيئة نظامية أو عمومية.

أ- القذف الموجه رئيس الجمهورية عبر مواقع التواصل الاجتماعي:

يقوم الركن المادي في جريمة القذف الموجه لرئيس الجمهورية عبر مواقع التواصل الاجتماعي، يكون حسب صفة وظيفته، أو مركزه السياسي، وليس بوصفه إنسانا فقط، فبالتالي فإن فعل الإسناد هو نية إساءة إلى رئيس الجمهورية عن طريق القذف، أما موضوع الإسناد فهو أن تكون هذه الواقعة تمس وتخدش شرف واعتبار هذا الأخير وهو ما حددته نص المادة 296 ق.ع.ج، وقد عرف الشرف فقها بأنه: «مجموعة الميزات أو المكنات التي تمثل قدرا من القيم الأدبية التي يفترض توافرها بالضرورة لدى كل قرار بحكم كونه شخصا آدميا»[1].

1- نبيل صقر، الوسيط في جرائم الأشخاص (د.ط)، دار الهدى، عين مليلة، الجزائر، 2009، ص 114.

الاعتبار فهو: «تلك الشروط أو الصفات أو القيم المعنوية والأدبية التي يتمتع بها الشخص على النحو الذي تقتضيه إنسانيته ومكانته الاجتماعية ومركزه الاجتماعي»[1].

وبالتالي فإن المشرع الجزائري قد ربط الإساءة الموجهة لشخص رئيس الجمهورية بالقذف، لكي يتحقق السلوك الإجرامي، ولن يتحقق إلا بتوافر أهم شرط في جريمة القذف، وهو العلانية، فالعلانية في هذا السلوك المجرم لا تنطوي على الإساءة عن طريق القذف فقط، بل في إذاعة هذا القذف على النحو الذي يوصل هذه الإساءة إلى علم الجمهور عن طريق مواقف التواصل الاجتماعي.

5- الجزاءات الجنائية لجريمة قذف رئيس الجمهورية عبر التواصل الاجتماعي: [2]

بالرجوع إلى المادة (144) مكرر: يعاقب على القذف الموجه لرئيس الجمهورية والهيئات بالحبس من 03 أشهر إلى (12) شهر وغرامة من (50.000دج) إلى (250.000دج) وتضاعف في حالة العود، ثم عدلت هذه المادة لتصبح العقوبة هي الغرامة من 100.000دج إلى 500.000دج، وتضاعف الغرامة في حالة العود.

1- عبد القادر شيخ، شرح قانون العقوبات –القسم الخاص، ج02، (د.ط)، منشورات جامعة حلب، سوريا، 2006، ص 119، مشار إليهم في: ط.د، لود موسى، جامعة العربي التبسي–تبسة، المرجع السابق، ص 286.

2- لحسن بن شيخ آث ملويا، المنتقى في القضاء العقابي، ط01، دار الخلدونية، الجزائر، 2008، ص 342.

2- القذف الموجه إلى الرسول (صلى الله عليه وسلم) أو بقية الأنبياء عبر مواقع التواصل الاجتماعي:

أ- الركن المادي: جاءت المادة 144 مكرر (02) بتجريم فعل الإساءة إلى الرسول (صلى الله عليه وسلم) أو بقية الأنبياء، إلا أن المشرع لم يحدد طبيعة الإساءة، لأنها يمكن أن تأخذ عدة صور، يمكن أن نقول أن الإساءة تندرج ضمنها عدة سلوكات منها الإهانة أو السب أو القذف.

باعتبار أن طرق الإساءة المذكورة في المادة 144 مكرر (الكتابة، الرسم، التصريح أو بأي وسيلة أخرى).

ب- الجزاءات الجنائية لجريمة قذف الرسول (صلى الله عليه وسلم) أو بقية الأبياء عبر مواقع التواصل الاجتماعي:

عاقبت المادة 144 مكرر02[1] مرتكب جنحة لرسول صلى الله عليه وسلم، أو أحد الأنبياء عبر مواقع التواصل الاجتماعي في صورتها المشددة نوعا ما مقارنة بالإساءة إلى رئيس الجمهورية، باعتبار أن المساس بالمعتقدات والمقدسات يتجاوز كل قيم دنيوية، فحدد القانون عقوبة الحبس من 03 سنوات إلى 05 سنوات وبغرامة من 50.000دج إلى 100.000دج، كما لم يحدد المشرع الجزائري حكم خاص في حالة العود وبالتالي يلجأ إلى الأحكام العامة.

1- راجع المادة 144 مكرر 02 من قانون العقوبات الجزائري المعدل والمتمم.

3- القذف الموجه لسلطات الدولة الثلاث عبر مواقع التواصل الاجتماعي:

إن السلطات الثلاث في الدولة هي نتاج لمبدأ الفصل بين السلطات، والذي تبناه الدستور الجزائري[1]، فالسلطة التنفيذية: «هي مجموع الموظفين المكلفين بتنفيذ القوانين بدءا من رئيس الدولة إلى آخر موظف في السلم الإداري»، ونظمها المشرع في المواد من 84 إلى 111 من الدستور، أما السلطة التشريعية فهي «الهيئة المختصة بإعداد وسن القوانين والمصادقة عليها ومراقبة أعمال الحكومة في حدود القواعد التي يقرها الدستور»، والتي نظمتها المواد من 112 إلى 155.

أما السلطة القضائية: «هي سلطة الفصل بين المنازعات المعروضة أمامها، وهي السلطة المسؤولة بتطبيق القانون»، وتنظمها المواد من 156 إلى 177.

أ- **الركن المادي:** نصت عليه المادة 146 من الأمر 66-156 المتضمن قانون العقوبات الجزائري[2]، أن القذف ضد السلطات الثلاث لا يقع إلا على موظف عام أو من فيه حكمه بسبب الوظيفة أو أثناء تأديتها، أو قد يقع على السلطة في حد ذاتها، كوحدة كاملة ولا يتحقق السلوك المجرم لهذه الجريمة عبر مواقع التواصل الاجتماعي إلا عن طريق تحقق شرط العلانية لدى الجمهور، مع توفر شرط علم القاذف.

1- المرسوم الرئاسي رقم 96-438 المؤرخ في 07 ديسمبر 1996، المتضمن دستور الجزائر، الجمهورية الجزائرية، جريدة رسمية، عدد 76 لسنة 1996، المعدل والمتمم بموجب القانون رقم 16-01 المؤرخ في 16 مارس 2016، الجمهورية الجزائرية، جريدة رسمية، عدد 14، الصادرة في 07 مارس 20016.

2- المادة 146 من الأمر 66-156 المتضمن قانون العقوبات الجزائري المعدل والمتمم بموجب القانون 04-15: «القذف الموجه بواسطة الوسائل المحددة في المادة 144 ضد البرلمان أو إحدى غرفتيه أو ضد الجهات القضائية».

ب- الجزاءات المقررة لقذف سلطات الدولة عبر مواقع التواصل الاجتماعي:

لقد أحالت المادة 146 ق.ع.ج لعقوبة القذف الموجهة ضد سلطات الدولة والهيئات النظامية إلى المادة 144 مكرر والتي تم ذكر العقوبات المقررة فيها، حيث عدلت فأصبحت الغرامة من 100.000 دج إلى 500.000 دج فقط.

3- قذف المؤسسات العسكرية والهيئات العمومية والنظامية:

أ- قذف المؤسسات العسكرية:

نجد أن المشرع الجزائري قد جعل القضاء العسكري قضاء استثنائي بحكم تشريعه بعقوبات خاصة، وذلك نظرا لحساسية هذه المؤسسة السيادية، إلا أن المشرع الجزائري خصص جريمة القذف على هذه المؤسسة بنص قانوني في محتوى نص المادة 146 ق.ع.ج فجريمة القذف الموجهة إلى المؤسسة العسكري تكتسي نفس العناصر السابقة وهي الإسناد وموضوعه، أما بالنسبة للجزاء المذكور في نص المادة 144 بغرامة من 100.00 دج إلى 500.000دج، وتضاعف في حالة العود.

ب- قذف الهيئات العمومية والنظامية:

لم يعرف المشرع الجزائري هذه الهيئات ولكن بالرجوع إلى القضاء الفرنسي تعرف كما يلي: «الهيئات التي لها وجود شرعي دائم والتي خولها الدستور والقوانين قسطا من السلطة أو الإدارة العمومية»[1]، فأدرجها المشرع الجزائري ضمن المادة 146 ق.ع.ج لتدخل ضمن الهيئات المحمية نفس عناصر القذف والجزاء المذكورة سابقا.

1- أحسن بوسقيعة، الوجيز في القانون الخاص، ج01، ط17، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2014، ص 223.

ثانيا: جريمة السب:

1- تعريفه: تنص المادة 297 من ق.ع.ج على أن: «يعد سبا كل تعبير مشين أو عبارة تتضمن تحفيزا أو قدحا لا ينطوي على إسناد أية واقعة».

يقصد بالسبب كل خدش للشرف والاعتبار فهو مدلول من القذف الذي لا يتحقق، إلا بإسناد واقعة معينة، وقد تناول المشرع الجزائري السب في القسم الخاص تحت عنوان الاعتداء على شرف واعتبار الأشخاص ونص عليه في المواد 297، 298 مكرر، 299 من قانون العقوبات[1].

والعنصر الذي يفرق بين السب عن القذف هو أن القذف لا يكون إلا بإسناد أمر معين، أما السبب فيتوافر بكل ما يتضمن خدشا للشرف أو الاعتبار، أي بكل ما يمس قيمة الإنسان عند نفسه أو يحط من كرامته أو شخصيته عند غيره، وعلى ذلك فكل قذف يتضمن نفس الوقت سبا، ولكن قد يخدش الشرف والاعتبار بغير إسناد واقعة معينة، وقد يكون ذلك بإسناد عيب معين دون تعيين واقعة معينة، كم يقول لآخر أنهل أو مزور أو نصاب أو سكير أو فاسق وهنا قد يختلط القذف بالسب وتكون العبرة في التفرقة بينهما بتعيين الوقائع حسب ظروف الأحوال، ويتعين حتى يعتبر السب مكونا لجريمة أن يوجه على شخص أو أشخاص معينين.

فإذا كانت ألفاظ السب عامة أو موجهة إلى الشخص خيالي فلا جريمة، فالسكير الذي يدفعه سكره إلى التفوه في الطريق العام بألفاظ السب غير قاصد بذلك لشخص معين لا يشكل سبّه هذا جريمة، ولكن قد يحتاط الجاني فلا يذكر اسم المجني عليه صراحة بها عباراته، وعندئذ يكون كمحكمة الموضوع أن نتعرف على الشخص من وجه إليه السب من عبارات السب وظروف وحصوله والملابسات التي اكتشفت.

1- أحسن بوسقيعة، المرجع السابق، ص 223.

2- أركان جريمة السب:

من نص المادة 297 من ق.ع.ج تبين لنا أن لجريمة السب 03 أركان هي:

- **الركن المادي:** وهو السلوك الذي يصدر من الجاني ويكون منطويا على خدش الشرف والاعتبار ضد المجني عليه.

- **العلانية:** حيث أن لا عقاب على جريمة السب إلا إذا ارتكبت علانية.

- **القصد الجنائي:** هو قصد عام على عنصري العلم والإرادة، فيتعين على المتهم بمعنى الألفاظ التي صدرت عنه إدراكه ما يتضمنه المعني من خدش لشرف المجني عليه واعتباره وأن يعلم المتهم بعلانية نشاطه وأن تتجه إرداته إلى النطق بعبارات السب أو تسجيله كتابة أو إلى إذاعة عبارات السب وإتاحة العلم بها لجمهور الناس.

3- العقوبات المقررة لجريمة السب:

لقد جرم المشرع الجزائري كل تعبير مشين أو عبارة تحفيز أو قدح تنطوي تحت نص المادة 297 من ق.ع.ج واعتباره سبا، وحدد له عقوبات كونه اعتداء على شرف واعتبار الأشخاص، وجاءت المادة 298 مكرر و299 من ق.ع.ج.

تنص المادة 298 مكرر: يعاقب على السب الموجه إلى شخص أو أكثر بسبب انتمائهم إلى مجموعة عرقية أو منهية أو على دين معين بالحبس من 05 أيام إلى 06 أشهر وبغرامة من 5.000 دج إلى 50.000 دج أو بإحدى هاتين العقوبتين فقط.

وتنص المادة 299: «يعاقب على السب الموجه إلى فرد أو عدة أفراد بالحبس من شهر (01) إلى 03 أشهر وبغرامة مالية من 10.000 دج إلى 25.000 دج، يضح صفح الضحية حدا للمتابعة الجزائية.

وبالرجوع إلى نص المادة (20)[1] من قانون مكافحة جرائم تقنية المعلومات رقم (05) لعالم 2012 جرمت جريمتي السب والقذف، وأن العقوبة التي حددها المشرع لهذه الجريمة هي «الحبس والغرامة التي لا تقل عن مائتين وخمسين ألف درهم»، وتجاوز خمسمائة ألف درهم، أي حدد العقوبة عند رفع حد الغرامة.

ثانيا: الاعتداء على حرمة الحياة الخاصة

1- تعريفها: لم يعرف القضاء والتشريع الحياة الخاصة، نظرا لكونها فكرة مرنة وغير محددة وتختلف باختلاف الزمان والمكان والأشخاص، إلا أن ذلك لا يمنع أن تتمتع بالحماية القانونية الكاملة في العديد من التشريعات، وقد أقر الدستور الجزائري لحماية الحق في الحياة الخاصة، فنص المادة 39 على حماية الحق في الحياة الخاصة فلا يجوز الاعتداء على هذه القاعدة الدستورية الهامة، سواء من المعاهدات والاتفاقيات التي تبرمها الجزائر أو القوانين والعضوية والعادية أو القوانين التنظيمية، كما أنه إلى جانب الحماية الدستورية نجد نوعين من الحماية يتمثلان في الحماية المدنية والجزائية.

حيث أقر المشرع من خلال نص المادة 47 وما يليها من القانون المدني الجزائري[2]، الحماية المدنية للمساس بالحقوق اللازمة لشخصية الأفراد، أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته لن يطلب وفق الاعتداء مع التعويض عما لحقه من ضرر، ويكون لمن وقع عليه الاعتداء الحق في طلب وقفه دون حاجة لإثبات الضرر.

1- عبد الرحيم الشيباني، شيماء إسحاق، المسؤولية الجزائية عن جريمتي السب والقذف بالوسائل الإلكترونية طبقا للمرسوم رقم (05) لسنة 2012 شأن قانون مكافحة جرائم تقنية المعلومات، 2018، ص 48.

2- الأمر رقم: 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني الجزائري، الجمهورية الجزائرية، جريدة رسمية، عدد 78، الصادرة في 30 سبتمبر 1975.

أما الحماية الجزائية فقد أورد المشرع الجزائري قواعد التجريم المساس بالحق في الخصوصية لأول مرة سنة 2006 الذي تضمن الحماية الدستورية للحياة الخاصة من خلال المواد 303 مكرر إلى المادة 303 مكرر 3 من ق.ع[1].

تضمن نص المادة 303 مكرر «على يعاقب بالحبس من 06 أشهر إلى 03 سنوات وبغرامة مالية من 50.000 دج إلى 300.000دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

1-بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

2-بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات المقررة للجريمة التامة، يضع صفح الضحية حد للمتابعة الجزائية».

فقد تصدى المشرع بالتجريم والعقاب بمجرد تحقق صورة من صور الاعتداء على حرمة الحياة الخاصة.

كما تطرق المشرع الجزائري في العديد من القوانين الخاصة إلى حماية الحق في الخصوصية نذكر منها على سبيل المثال قانون المحاماة، القانون الأساسي للوظيفة العامة، القانون العضوي المتعلق بالإعلام.

1- القانون رقم 55-156 المتضمن قانون العقوبات المعدل والمتمم بموجب القانون 06-23 المؤرخ في 20 ديسمبر 2006، الجمهورية الجزائرية، جريدة رسمية، عدد 84، ص 23.

وأجاز المشرع اختراق الحق في الخصوصية حماية للمصلحة العامة في إطار التحقيق في بعض الجرائم الخطيرة[1]، متى اقتضت ضرورات التحري في الجريمة المتلبس أو التحقيق الابتدائي.

كما نصت المادة (04) من القانون رقم: 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2] على أنه: «يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 من الأفعال الموصوفة لجرائم الإرهاب والتخريب، أو الجرائم الماسة بأمن الدولة في حالة توافر معلومات عن احتمال الاعتداء على منظومة معلوماتية... وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات، بالنسبة للمساس بالحياة الخاصة للغير».

2- صور الاعتداء على الحياة الخاصة:

بالرجوع إلى المشرع الجزائري لم يحدد نطاق الاعتداء الإلكتروني على الحق في الحياة الخاصة عبر الوسائل الإلكترونية والرقمية، ولم ينظم مظاهر حماية خصوصية المعلومات أو البيانات الخصية وسائل معالجتها الإلكترونية، بل اكتفى بإقرار المبدأ العام في حماية الخصوصية بشكل عام دون التعرض للوسيلة أو التقنية المعتمدة لارتكاب الجريمة، إلحاق الضرر بالشخص وأهم المخاطر التي تهدد الحياة الخاصة في ظل تطور المعلوماتية.

إساءة جمع البيانات عن الأشخاص واستخدامها في غير الغرض المخصص لها (نتيجة استخدام الحواسب الآلية كبنوك المعلومات على الحياة الخاصة).

1- المادة 65 مكرر05 من القانون رقم 66-156 المعدل والمتمم بموجب القانون رقم 06-22 من قانون الإجراءات الجزائية وهي جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد،

2- القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مرجع سابق.

بموجب القانون رقم 15/04 المتضمن تعديل قانون العقوبات في الفصل الثالث من الباب الثاني من الكتاب الثالث القسم السابع مكرر تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات من المواد 394 مكرر إلى 394 مكرر[1]، تم ذكرها في المطلب الأول من المبحث الأول.

- جرائم السب والقذف وتشويه السمعة.
- التقاط أو تسجيل أو نقل مكالمات بغير إذن صاحبها.
- التقاط أو تسجيل صورة في مكان خاص، بغير إذن صاحبها.
- الاعتداء على سرية المراسلات[2]. باختلالها أو استخدامها أو إذاعتها من خلال التجسس على الاتصالات.

بالإضافة إلى جريمة التهديد والمضايقة والملاحقة وجريمة انتحال الشخصية وهي جريمة الألفية الجديدة كما سماها بعض المختصين في أمن المعلومات، والقيام بعمليات النصب والاحتيال من خلال التقرير والاستدراج وغالبا ضحايا صغار السن، بهذه الإساءة إلى سمعة الضحية أو الاستيلاء على الأرصدة البنكية أو السحب من البطاقات الائتمانية وسرقة الحسابات المصرفية[3].

1- الأمر رقم 66-156 المتضمن قانون العقوبات الجزائري المعدل والمتمم بموجب الأمر 04-15، مرجع سابق.

2- عرفت المادة 09 من القانون رقم 20-03 المؤرخ في 05 أوت 2006 المتضمن القواعد العامة بالبريد والمواصلات السلكية واللاسلكية، ج.ر، عدد 98: «بأنه اتصال مجسد بشكل كتابي عبر مختلف الوسائل المادية التي يتم توصيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، ولا تعير الكتب والمجلات والجرائد واليوميات كمادة مراسلات».

3- ابتسام مناع، تخصص قانون عقاري، جريمة الاعتداء الإلكتروني على الحياة الخاصة في التشريع الجزائري، مجلة الشريعة والاقتصاد، مجلد08، الإصدار الأول، 2019، ص 325.

الفرع الثاني: الجرائم المنصوص عليها بموجب نصوص خاصة

نظرا لتدخل المعلوماتية في جميع المجالات ارتأينا التطرق للنصوص الخاصة التي أقرت الحماية الجزائية.

أولا: الحماية الجنائية في نطاق قانون حق المؤلف

نظرا لنسبة الحماية المقررة من خلال النصوص التقليدية في قانون العقوبات الجزائري، ارتأينا البحث في مدى إمكانية الحماية من خلال نصوص قانون الملكية الفكرية وبالتجديد قانون حقوق المؤلف، باعتبار المشرع الجزائري مثله مثل باقي معظم التشريعات، قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءات الاختراع، وذلك طبقا لنص المادة (07) من الأمر 07/03 المتضمن براءة الاختراع: «ولا تعد من قبل الاختراعات في مفهوم هذا الأمر برامج الحاسوب»[1]. نجد أن المشرع الجزائري عرف هذه الأفعال هي تلك المكونة لجريمة التقليدية والجرائم الملحقة بها، بالإضافة إلى أهم العقوبات التي في الأمر رقم 05/03 الصادر بتاريخ 19-07-2003 المتعلق لحق المؤلف.

- الحماية عن طريق تجريم تقليد برامج الكمبيوتر:

عرفت جريمة التقليد بأنها: «نقل مصنف لم يسقط في الملك العام من غير إذن مؤلفه، وعرفت كذلك بأنها: «القيام بعمل لا يقوم به سوى المؤلف أو يرخص به».

أما قانون حق المؤلف فلم يتعرض لتعريف جريمة التقليد، وإنما اكتفى بتعداد الأفعال المشكلة للجرائم الموصوفة بالتقليد (151) و(152) من الأمر 05/03 بقوله: «ويعد مرتكبا لجنحة التقليد كل من يقوم بالأفعال الآتية:

1- الأمر 07/03 المؤرخ في 19-07-2003 المتعلق ببراءات الاختراع، ج.ج. جريدة رسمية، عدد44.

- الكشف غير المشروع للمصنف أو المساس سلامة مصنف أو أداء لفنان مؤد أو عازف.
- استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة»[1].

من هذا المنطق يمكن القول أنه لقيام جريمة التقليد لابد من توافر ركنين أساسيين الركن المادي والركن المعنوي.

1- الركن المادي: لقيام الركن المادي لابد من توافر سلوك ونتيجة وعلاقة سببية بينهما، والنشاط الإجرامي في جريمة التقليد يأخذ صورة من إحدى الصورتين السابقتين الذكر في المادتين (151) و(152) وذلك على النحو التالي:

أ- الكشف غير المشروع عن البرمجية:

بالرجوع إلى أحكام المادة (22) من الأمر رقم 05/03 قد نصت على أن للمؤلف الحق في الكشف عنه باسمه أو باسمو مستعار، ويمكنه تحويل هذا الحق إلى الغير، كما يعود هذا الحق إلى ورثته بعد وفاته، فلهم الحق في الكشف عن البرمجية[2]، وبالتالي فإن عملية الكشف عن البرمجية وإظهار من قبل الغير الذي لم يحال به هذا الحق يعد اعتداء غير مشروع ويدخل نطاق التجريم، ومن بين طرق الكشف غير المشروع عن البرمجيات كسر حمايتها عن طريق الحصول على الشفرة السرية التي تسمح بالدخول للبرمجة، واستغلالها كمستعمل مرخص له كذلك قرصنة الرقم التسلسلي للنسخة من البرمجة.

1- الأمر رقم 03-05 الصادر بتاريخ 19-07-2003 المتعلق بحق المؤلف والحقوق المحاورة المعدل والمتمم للأمر رقم 14/73، ج.ج.ر، ع44.

2- بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري وفقا لأحكام قانون حقوق المؤلف الجديد، الأمر رقم 05/03، ط01، دار الخلودونية، الجزائر، 2007، ص 78-79.

ب- المساس بسلامة البرمجية:

للمؤلف وحده الحق في تعديل أو تحوير أو تغيير أو حذف أو إضافة في برنامجه، ولا يمكن للغير الاعتراض على ذلك ما لم يكن فيه إخلال أو مساس بمصالحهم وهذا ما يظهر من خلال المادة (90)[1] من الأمر رقم 03-05، إلا أنه يرد استثناء هذه المادة المنصوص عليه بالمادة (25) من هذا الأمر.

بمفهوم المخالفة أنه إذا لم يكن من شأن هذه التعديلات المساس بسمعة المؤلف أو بشرفه أو بمصالحه المشروعة، فإنه لا يمكن الاعتراض عليها من طرف المؤلف.

ج- استنساخ البرنامج بأي أسلوب من الأساليب في شكل نسخ مقلدة:

يعد هذا السلوك الإجرامي من أشهر وأخطر عمليات التقليد والقرصنة المعلوماتية بسهولة القيام بها وقلة تكاليفها وارتفاع مداخيلها، واستنساخ البرمجيات قد يتم في عدة أشكال وصور باختلاف الدعامة والمصدر المتواجد في هذه البرمجيات، ولكن الإشكال المطروح أن الاستنساخ المقصود يتمثل فقط في إجراء نسخة طبق الأصل للبرمجة من مصدرها إلى وسيلة أو دعامة مشابهة (كمثال: نسخ قرص مضغوط CD إلى آخر بواسطة Gravure du cd) أم كل استنساخ يعتبر غير مشروع كيفما كان سواء من دعامة إلى أخرى أو غيرها؟

والمقصود بالاستنساخ هو كل عملية الهدف منها الاعتداء على البرامج محل الحماية بأي طريقة كانت، وتبقى مسألة توسيع نطاق هذه السلوكيات أو تصنيفها من اختصاص المصالح الأساسية للشركات أو الأفراد المعنيين بها.

2- الركن المعنوي: لا يكفي لقيام جريمة التقليد وجود الركن المادي وحده بل لابد من توافر عنصري العلم والإرادة لدى الجاني أثناء قيامه بأي اعتداء في صورة من الصور

1- راجع المادة 90 من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق والمجاورة، مرجع سابق.

السابقة، والقصد المتطلب في هذه الحالة هو القصد العام وليس الخاص، فليس بالضرورة أن يقصد المعتدي الحاق الضرر بمؤلف البرنامج، وبالتالي فيكفي أن يعلم الجاني أنه يعتدي على برنامج لشخص آخر وأن ذلك الفعل يعد جريمة.

3- الجرائم الملحقة بجريمة التقليد:

نصت على هذه الجرائم الفقرات الثالثة والرابعة والخامسة من الأمر رقم 05/03 الصادر بتاريخ 19-07-2003 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر 14/73[1]، وهي كالتالي:

1- الركن المادي: لتوافر الركن المادي للجرائم الملحقة لجريمة التقليد، لابد وأن يتم سلوك من السلوكيات التالية:

أ- استيراد أو تصدير برامج مقلدة من مصنف أو آداء: بسط المشرع الجزائري حمايته على جميع البرامج المحمية سواء بالقانون الجزائري أو لقانون دولة أجنبية بشرط أن يكون متمتعا بالحماية في دولته، فيستوي بذلك أن يكون مؤلف البرنامج جزائري أو أجنبي، كما يشترط لقيام هذه الجريمة عدم موافقة المؤلف، وهي بذلك تشترك مع جرائم التقليد في التداول كون أن الموافقة المطلوبة في هذه الحالة هي موافقة كتابية، بمعنى أن الموافقة الضمنية أو الشفوية أو الموافقة اللاحقة لا تغني عن المتابعة.

ب- المشاركة في تقليد برنامج من مضف أو أداء:

تعد هذه الصورة تطبيقا للقواعد العامة لمعاقبة الشريك وهو الشخص الذي يساهم في هذه الجريمة سواء بعمله لمدة محدودة أو غير محدودة.

1- الأمر 03-05 الصادر بتاريخ 19 جويلية 2003 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر 73-14، مرجع سابق.

جـــ- رفض دفع المكافأة المسحقة عمدا لمؤلف البرنامج:

ما نصت عليه المادة (95) من قانون حماية حق المؤلف، وتكون غالبا من جراء تنازل مؤلف عن حق من حقوقه المادية سواء كلية أو بصفة مؤقتة.

د- بيع برامج أو تأجير أو وضع رهن التداول لبرامج مقيدة من مصنف أو أداء:

يظهر الركن المادي لهذه الجريمة في حالة التعامل في البرامج المقلدة سواء بالبيع أو التداول، ويكون البرنامج مقلدا إذا كان مشابها للبرنامج الأصلي المحمي من طرف القانون، والعبرة في ذلك بأوجه النسبة لا بأوجه الاختلاف، بحيث من شأنه أن ينخدع به الجمهور في المعاملات[1].

2- الركن المعنوي: القصد الجنائي لهذه الجرائم مفترض بحيث يقوم الركن المعنوي بمجرد اتجاه إرادة الجاني إلى القيام بسلوك من السلوكيات السابقة، فهو مرتبط بتوافر الركن المادي، والشروع متصور في أغلب هذه الجرائم، وبالتالي فالقصد المتطلب في هذه الجرائم هو القصد العام فقط، وتجدر الإشارة إلى أن جريمة التصدير والاستيراد للبرامج المقلدة التي تتطلب إلى جانب القصد العام توافر القصد الخاص، إذ لابد من أن تتجه إرادة الجاني إلى فعل من الفعلين المذكورين "الاستيراد والتصدير"[2].

3- العقوبات المقررة لجريمة التقليد:

نصت المادة (153) من الأمر رقم 05/03 على عقوبة التقليد بقولها: «يعاقب مرتكب جنحة تقليد مصنف أو أداء كما هو منصوص عليه في المادتين (151) و(152) أعلاه، بالحبس من 06 أشهر إلى 03 سنوات وبغرامة مالية من خمسمائة ألف دينار جزائري إلى مليون دينار، سواء كان النشر قد حصل في الجزائر أو في الخارج».

1- خيثر مسعود، الحماية الجنائية لبرامج الكمبيوتر، المرجع السابق، ص 34.

2- المرجع نفسه، ص 98.

ويستوجب العقوبة المقررة في المادة (153) أعلاه، كل من شارك بعمله أو بالوسائل التي يجوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة، أي أن هذه العقوبات تسري على جميع صور التقليد السابقة.

- العقوبات التكميلية:

وهي الغلق، المصادرة، ونشر ملخص الحكم الصادر في الدعوى.

الغلق: للمحكمة الحكم بغلق المؤسسة التي يستغلها المقلد سواء كامن مملوكة لهم أم مستأجرة، ويجوز كذلك الحكم بالغلق المؤقت أو النهائي لهذه المؤسسة، وذلك بالموازاة مع حجم الخسائر أو نوع الجريمة القائمة ويرجع الفصل فيها لمحكمة الموضوع[1].

المصادرة: أن المصادرة وجوبيا، فالقاضي ملزم بأن يحكم بمصادرة وإتلاف جميع الوسائل والعتاد المستخدم في النسخ والتقليد، وحددت الجهة التي يمكن أن تؤول إليها هذه الأموال والوسائل محل المصادرة، بحيث قررت تسليها للمؤلف أو مالك الحقوق أو ذويه، وبالتالي يعتبر بمثابة تعويض عن الضرر اللاحق لهم[2].

نشر ملخص الحكم: يقصد بهذه العقوبة التشهير بالمحكوم عليه والتأثير على شخصيته الأدبية والمالية، فهي ماسة بالشرف والاعتبار وهي عقوبة تكميلية وجوبية يجب الحكم بها ذاتها في حال صدور حكم الإدانة حتى ولو وقت تنفيذه[3].

1- المادة 156 من الأمر رقم 05/03، المتعلق بحق المؤلف والحقوق المجاورة، مرجع سابق.

2- المادة 159، المرجع نفسه.

3- خيثر مسعود، المرجع السابق، ص 101-102.

ثانيا: الجرائم المنصوص عليها من خلال قانون التأمينات

1- تعريف البطاقة الإلكترونية: هي تلك البطاقة التي تحتوي على بيانات المعالجة الآلية، تحوي بيانات إسمية ومعلومات عن صاحبها[1].

2- الحماية الجزائية للبطاقات الإلكترونية: [2] نصت المادة (06 مكرر01) من القانون: 08-01 على أن البطاقة الإلكترونية تسلم للمؤمن له اجتماعيا مجانا ومن طرف هيئات الضمان الاجتماعي، وهي صالحة في كل التراب الوطني وهي تقدم لكل مقدم علاج أو مقدم خدمات مرتبطة بالعلاج، وهذا الأخير هي "المفتاح الإلكتروني لهيكل العلاج".

3- العقوبات المقررة: [3] يعاقب كل من يسلم أو يستلم البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج بغرض استعمالها بطريقة غير مشروعة، بالحبس من سنتين إلى 05 سنوات وبغرامة من (100.000دج) دج في (200.000دج) أيضا.

يعاقب كل من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لمهني الصحة، وهي نفس العقوبة التي تطلق كذلك على كل من قام بتعديل أو نسخ وبطريقة غير مشروعة البرمجيات التي تسمح بالوصول إلى استعمال المعطيات المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا.

1- عباوي نجاة، الإشكاليات القانونية في تجريم الاعتداء على أنظمة المعلومات، دفاتر السياسة والقانون، جامعة محمد الطاهري بشار، العدد 15، الجزائر، 2010، ص 288.

2- القانون رقم 08-01 المؤرخ في 23 يناير 2008 المتمم للأمر رقم 1/83 المؤرخ في 02 يوليو 1983 المتعلق بالتأمينات الاجتماعية، ج.ر، ع04 الصادرة في 27 يناير 2008، ص 07.

3- المادة 65 مكرر 03، المرجع نفسه، ص 08.

ثالثا: الحماية الجزائية للتوقيع والتصديق الإلكترونين من خلال القانون رقم 04/15

عرف المشرع الجزائري التوقيع الإلكترونين من خلال المادة02 فقرة 01 من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكتروني، أنه «بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق».

1- حماية التوقيع الإلكتروني عن طريق التشفير:

ظهر التشفير كتقنية التوقيع الإلكتروني والمعاملات الإلكترونية، ذلك أنه إجراء يؤدي إلى الثقة والأمان، فهو يعتمد على أساليب واستخدام أدوات لتحويل المعلومات وإخفاء محتوياتها للحيلولة دون تعديلها أو استخدامها غير المشروع.

التشفير هو تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو تعديلها وتغييرها[1]، وهنا نوعان تشفير مماثل وتشفير اللامماثل.

2- مفهوم التصديق الإلكتروني: يعرف بأنه «وسيلة آمنة للتحقق من صحة التوقيع أو المحرر، حيث يتم نسبه إلى شخص أو كان معين ومن ثم فإنه وسيلة سلامة وتأمين التعامل عبر الأنترنت سواء من حيث مضمونه ومدخله وتاريخه وأطرافه».

فالحماية الجنائية للتوقيع الإلكتروني في إطار قانون العقوبات الجزائري، حيث أن المشرع الجزائري حرم كل أنواع الاعتداءات التي تستهدف الدخول غير المشروع للأنظمة المعلوماتية تغييرا أو إتلاف للمعطيات.

1- صحراوي مصطفى، طالب دكتوراه، الحماية الفنية والجزائية للتوقيع الإلكتروني على ضوء القانون 15-04 المتعلق بالتوقيع والتصديق الإلكتروني، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 004، عدد01، تاريخ النشر: 10-12-2018، ص 96-98.

3- حماية التوقيع الإلكتروني في ظل القانون المتعلق بالتوقيع والتصديق الإلكتروني (04-15)

حرص المشرع الجزائري على تضمين القانون 04/15 مجموعة من العقوبات الإدارية والمالية، والجزائية لكل من يمس بيانات التوقيع الإلكتروني في شكل جريمة في أحكام القانون السالف الذكر:

حيث نصت المواد من 66 إلى 75 من القانون 15-04: [1]

1-يعاقب بالحبس من 03 أشهر إلى 03 سنوات، وبغرامة من 20 ألف (20.000) إلى مائتين ألف دينار جزائري أو بهاتين العقوبتين على جريمة الادعاء بقرارات كاذبة للحصول على شهادة التصديق الإلكتروني المرصوفة...

2-جنحة إصدار شهادة التصديق الإلكتروني دون ترخيص أو سحب.

3-الصنف الثاني يتمثل في الجرائم المرتبطة بطلب الخدمة وتتمثل في:

- جنحة الإدلاء بالقرارات الكاذبة للحصول على شهادات التصديٌ.
- جنحة حيازة أو إنشاء أو استعمال بيانات توقيع موصوفة خاصة بالغير.
- جنحة استعمال شهادة التصديق الإلكتروني الموصوفة بغير الغرض الذي منحت لأجله.

1- المواد من 66 إلى 75 من القانون رقم 15-04، المصدر السابق، ص 15.

خلاصة الفصل الأول:

استخدم المشرع الجزائري مصطلح الجرائم المتصلة لتكنولوجيات الإعلام والاتصال للدلالة على جرائم المساس بأنظمة المعالجة الآلية للمعطيات والجرائم المرتكبة بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وهي تسمية انفرد بها المشرع الجزائري، حيث تبنى أغلب التشريعات المقارنة مصطلح الجريمة المعلوماتية، هذه الجريمة ترتكب في العالم الافتراضي منحها خصوصية كبيرة انعكست على طبيعة السلوك الإجرامي ومحله، كما أثرت على إجراءات متابعتها، هذا وتصنف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تبعا للعديد من المعايير، حيث يذهب البعض إلى تصنيفها تبعا للدور الذي يلعبه الحاسب الآلي إذا ما كان محل الاعتداء أو وسيلة، وبالرجوع للقانون 09-04 نجد أن المشرع قد سن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ضمن التعريف الذي أورده في نص المادة (02) إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات وجرائم ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

الفصل الثاني

الآليات الإجرائية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

سن المشرع الجزائري قواعد إجرائية حديثة، تتوائم مع الطبيعة التقنية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال والأدلة الناتجة عنها والتي تكون في شكل إلكتروني، إيمانا منه بقصور الإجراءات الجزائية القائمة لمواجهة هذه الجرائم المستحدثة.

والواقع أن المشرع الجزائري على غرار باقي التشريعات العربية والغربية وضع عديد القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وتجلى ذلك من خلال ما احتواه التشريع العقابي وكذا القواعد الإجرائية التي تتبع في مجال الكشف عنها، فضلا عن إصداره للقانون 09-04 السالف الذكر، وكذا استحدثه بموجب المرسوم الرئاسي 261/15 المؤرخ في 08-10-2015 للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وباعتبارها في كثير من الأحيان جرائم عابرة للحدود جعل الهيئات الوطنية تعاون على هيئات دولية لمكافحتها.

وسنتناول في هذا الفصل خصوصية إجراءات متابعة الجرائم المتصلة لتكنولوجيا الإعلام والاتصال في (المبحث الأول) وهيئات متابعة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في (المبحث الثاني).

المبحث الأول: خصوصية إجراءات متابعة الجرائم المتصلة لتكنولوجيات الإعلام والاتصال

المبحث الثاني: هيئات متابعة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

المبحث الأول: خصوصية إجراءات متابعة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تخضع متابعة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للأحكام العامة المقررة في قانون الإجراءات الجزائية، بالإضافة لقواعد إجرائية جديدة نص عليها المشرع الجزائري بصدور القانون رقم 09-04، لذلك سنتناول في هذا البحث خصوصية إجراءات المتابعة من خلال التركيز على الإجراءات الواردة في القانون رقم 09-04، كما سنتطرق إلى مسألة إثبات هذه الجرائم، وعليه نقسم هذا المبحث إلى مطلبين نتناول في المطلب الأول ضبط الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وفي المطلب الثاني إثبات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

المطلب الأول: ضبط الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

إن للجريمة المعلوماتية خصوصية من الناحية الإجرائية من خلال اعتمادنا على قانون الإجراءات الجزائية الجزائري، وكذا القانون رقم 04/09[1] المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إذ أن قانون الإجراءات الجزائية ينص فقط على القواعد العامة التي تطبق على الجرائم التقليدية، أما بالنسبة لقانون رقم 04/09 فقد وضع لمتابعة الجريمة المعلوماتية من خلال بعض الجرائم الخاصة المتمثلة في حجز المعطيات ومراقبة الاتصالات الإلكترونية، وحفظ المعطيات وهذا سنتطرق إليه من خلال تقسيم هذا المطلب إلى فرعين: (الفرع الأول) الإجراءات الواردة في قانون الإجراءات الجزائية وفي (الفرع الثاني) الإجراءات الواردة في قانون 09-04.

1- القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع السابق.

الفرع الأول: الإجراءات الواردة في قانون الإجراءات الجزائية

سنتناول في هذ الفرع الإجراءات التي استحدثها المشرع الجزائري في قانون الإجراءات الجزائية[1]، كما سنبرز خصوصية بعض الإجراءات في مجال ضبط جرائم تكنولوجيات الإعلام والاتصال.

أولا: معاينة مسرح الجريمة

مسرح الجريمة هو البيئة الإلكترونية المتكونة من البيانات الرقمية التي تتواجد وتنتقل داخل بيئة الجهاز وشبكاته في ذاكرته وأقراصه الصلبة الموجودة بداخله، والتي يجب أن يكون التعامل مع الأدلة الرقمية.

فمسرح الجريمة الإلكترونية هو المكان الذي ارتكبت فيه الجريمة أو جزء منها ويشمل الأماكن التي اكتشفت فيها الجريمة أو أجزاء منها، وقد يكون مسرح الجريمة في مكان أو عدة أماكن، وفقا للجريمة وعناصرها والمراحل التي مرت بها منذ البدء في التخطيط لها والإعداد، التجهيز والتنفيذ ومرحلة التصرف في عائداتها وإخفاء معالمها[2].

كذلك يمكن دراسة معاينة مسرح الجريمة الإلكترونية من خلال التحليل الجنائي[3] لمعلومات الحاسوب، ومعاينة محل الجرائم الواقعة داخل وخارج النظم المعلوماتية.

1- الأمر رقم 15-02 المؤرخ في 23 يوليو 2015 المعدل والمتمم للأمر 66-155، المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج.ر، ع40 الصادرة في 23 يوليو 2015.

2- ماجد ياقوت، أصول التحقيق -دراسة مقارنة-، ط03، منشأة المعارف، الإسكندرية، (د.س.ن)، ص 69.

3- التحليل الجنائي الرقمي، يتضمن الجهاز أو المنظومة المعلوماتية وتحليل العمليات واسترجاع البيانات والملفات من أجل الحصول على الدليل الرقمي الذي يستخدم في التحقيقات القانونية، للمزيد من التفصيل انظر: جميل حسين طويلة: التحليل الجنائي الرقمي، مكتبة النور، سوريا، (د.ط)، (د.س)، ص01.

أ- مفهوم المعاينة:

تعرف المعاينة بأنه إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص نفسه مكانا أو شخصا أو شيئا له علاقة بالجريمة، لإثبات حالته والتحفظ على كل ما قد يفيد من الآثار في الكشف عن الحقيقة، فهي بذلك تعد من إجراءات التحقيق الابتدائي التي يجوز لسلطات التحقيق اللجوء إليها من تلقاء نفسها كلما رأت في ذلك ضرورة لإجلاء الحقية أو بناء على طلب من الخصوم، والأصل أن يجري المعاينة بحضور أطراف الدعوى الجزائية، غير أنه يجوز للمحقق إجراؤها في غيابهم نظرا لما تقتضيه من سرعة الانتقال إلى محل الجريمة قبل ضياع أو تعديل الأدلة[1].

حيث تتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، غير أن الانتقال هذا يختلف حسب طبيعة الجريمة الإلكترونية المرتكبة، ولمعاينة مسرح هذه الجريمة تتم في حالتين:

1- معاينة الجرائم الواقعة على المكونات المادية للجهاز: تتم المعاينة في جهاز الإعلام الآلي كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الجهاز ذات الطابع المادي المحسوس، فهي لا تثير أية مشكلة بحيث يمكن لضابط الشرط القضائية معاينتها، والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.

2- معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها: المكونات غير المادية هي برامج الجهاز وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينات أو فائدتها وهذه الصعوبات يمكن تلخصيها فيما يلي:

1-نقص وقلة الآثار المادية التي تقع على المكونات غير المادية للجهاز.

1- براهيمي جمال: التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، سنة 2018، ص 56.

2-تردد عدد كبير من الأشخاص على مسرح الجريمة خلال فترة زمنية قصيرة، والتي غالبا ما تكون طويلة، وذلك بين اقتران الجريمة والكشف عنها[1].

ب- القواعد الإجرائية لمعاينة مسرح الجريمة: هي جملة من الإجراءات المطبقة في كافة الجرائم، إلا أن التشريع الجزائري ينص على جملة من القواعد التي تعد وجوبية للقيام بالمعاينة، فأجاز المعاينة في الجنح وجعلها وجوبية في الجنايات وهي قد تتم في مكان عام أو خاص، فإذا كانت في مكان عام فضابط الشرطة القضائية لا يحتاج أي إذن ندب سلطة تحقيق بإجراءاتها، أما إذا كان خاص فلابد من شروط خاصة.

إذ أن الجرائم التي تقع في الوسط الإلكتروني، أو داخل المنظومة المعلوماتية لها أساليب خاصة، نص عليها المشرع الجزائري من خلال نصوص قانون الإجراءات الجزائية المتمثلة في إخطار وكيل الجمهورية أوقات إجراء المعاينة بالإضافة إلى رضا صاحب السكن.

1- إخطار وكيل الجمهورية: لا يمكن معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلا بعد إخطار وكيل الجمهورية بدائرة اختصاص من قبل ضابط الشرطة القضائية[2].

وعملا بنص المواد (18-32-42-63) من ق.إ.ج.ج، بالإضافة إلى نص المادة (42) و(49) من قانون القضاء العسكري، من واجبات ضباط الشرطة القضائية إذا ما علموا بأية جريمة بأن يقوم بإخطار وكيل الجمهورية سواء كان مدنيا أو عسكريا باعتباره

1- ماجد ياقوت، المرجع السابق، ص 70.

2- المادة (42) من الأمر 66-155 المعدل والمتمم بالقانون 07/17 المؤرخ في 27 مارس 2017، ج.ر، ع20 الصادر بتاريخ 29 مارس 2017 المتضمن قانون الإجراءات الجزائية.

المسؤول المباشر عن الشرطة القضائية على أن يكون الإخطار مسبوقا بتأكيد ضباط الشرطة القضائية من وقوع الجريمة فعلا.

كما أن الإخطار يكون باستعمال كافة الوسائل المتداولة عليها، فقد يكون بالكتابة أو باستعمال الهاتف النقال أو عن طريق أجهزة أخرى كالفاكس.

2- أوقات المعاينات: ألزم المشرع ضباط الشرطة أخذ الإذن من وكيل الجمهورية المختص من أجل الدخول إلى منازل الأشخاص للقيام بالتفتيش والمعاينات، فتطبق هذه القواعد عند الانتقال لمعاينة الجرائم الإلكترونية، حيث يجوز إجراء المعاينات في النظم المعلوماتية في كل ساعات النهار والليل، وفي محل سكاني أو غير سكاني بناء على إذن مسبق من وكيل الجمهورية المختص.

وبالرجوع إلى نص المادة (47) من ق.إ.ج نجد أن المشرع الجزائري أجاز إجراء المعاينة والتفتيش والحجز في كل محل سكني أو غير سكني وفي كل ساعة من ساعات النهار أو الليل دون تأخير هذه الإجراءات، عندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كما يجوز لضابط الشرطة القضائية أن يستعين بأشخاص مؤهلين لذلك[1].

3- رضا صاحب السكن: لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المشتبه فيها إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات أو يجب أن يكون هذا الرضا صريحا، وكذلك الشأن بخصوص الجرائم الواقعة على النظم المعلوماتية، وهذا ما نص عليه المشرع الجزائري في نص المادة (64) من ق.إ.ج[2].

1- راجع المادتان (47) و(49) من القانون رقم 66-155 المعدل والمتمم بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المتضمن قانون الإجراءات الجزائية الجزائرية، المرجع السابق، ص 22.

2- راجع المادة (64)، المرجع نفسه، ص 28.

ولنجاح المعاينة في الجرائم المعلوماتية يجب اتباع ومراعاة القواعد الفنية والمتمثلة فيا يلي:

- القيام بتصوير الجهاز، وما قد يتصل به من أجهزة ظرفية ومحتوياته، وأوضاع المكان الذي يوجد به بصفة عامة مع التركيز على تصوير أجزائه الخلفية وملحقاته ومراعاة التاريخ والزمان والمكان الذي التقطت فيه كل صورة.
- يجب ملاحظة وإثبات الحالة التي تكون عليها توصيلات الكابلات (الخيوط الكهربائية للجهاز) اللازمة للتأكد من عدم وجود أي مجالات مغناطسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو للبيانات المسجلة.
- وضع مخطط تفصيلي للمنشأة الواقعة بها الجريمة مع كشف تفصيلي على المسؤولين بهما ودور كل واحد منهم...
- يجب أن تقتصر مباشرة عملية المعاينة على مأسور بالضبط والباحثين ممن تتوفر فيهم الكفاءات العلمية والخبرة الفنية في مجال جهاز الإعلام الآلي، واسترجاع المعلومات وممن تلقون التدريب الكافي لمواجهة هذه النوعية من الجرائم والتعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة[1].

ثانيا: إجراءات التحري الخاصة

يعرف التحري بأنه مجموعة الإجراءات الأولية التي يباشرها أعوان الضبطية القضائية بمجرد علمهم بارتكاب الجريمة، والتي تتمثل في البحث عن الأدلة والقرائن لإثبات الجريمة[2].

1- أمحمدي بوزينة آمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لقانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام...)، 2016، ص 67.

2- محمد مجدة، ضمانات المشتبه فيه أثناء التحريات الأولية، ط02، دار الهدى، الجزائر، 1991-1992، ص 22.

وفي إطار المكافحة الإجرائية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وبموجب قانون 06-22 المعدل لقانون الإجراءات الجزائية، تم توسيع مجال اختصاص النيابة العامة في مجال البحث والتحري عن الجرائم بمنح الإذن بالتفتيش للقيام باعتراض المراسلات وتسجيل الأصوات، والتقاط الصور، التسرب في المواد 65 م05، 11، 12، 15.

1- اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

أ- **تعريف اعتراض المراسلات:** يقصد باعتراض المراسلات التتبع السري والمتواصل للمشتبه قبل وبعد ارتكابه للجريمة ثم القبض عليه متلبسا بها.

ويعرف على أنه إجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة، ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث، وهي تعتبر أيضا وسيلة هامة من الوسائل الحديثة للبحث والتحري تستخدمها الضبطية واجهة الإجرام الخطير، وتتم عبر وسائل الاتصال السلكية واللاسلكية[1].

يقصد بالمراسلات قانونا هي جمع الخطابات المكتوبة سواء أرسلت بطريق البريد أو بواسطة رسول خاص، وكذلك المطبوعات والطرود والبرقيات التي توجد لدى مكاتب البريد أو البرق، وسوي أن تكون داخل مظروف أو مفتوح.

والملاحظ أن المشرع الجزائري عندما تكلم على اعتراض المراسلات طبقا للمادة (65) مكرر 05 من ق.إ.ج.ج فإنه حدد نوع المراسلات وهي تلك التي تتم بواسطة الاتصال السلكي واللاسلكي واستبعد الوسائل البريدية أي الخطابات الخطية التي يتم عن طريق البريد، وذلك حرصا على ضمان حرية وسرية المراسلات بين الأفراد المكفولة

1- أحسن بوسقيعة: التحقيق القضائي، (د.ط)، دار هومة، الجزائر، 2010، ص 113.

دستورية هذا من جهة، ومن جهة أخرى فإن أفراد الشبكات والعصابات المنظمة كثيرا ما ينفذون خططهم الإجرامية باستعمال أدوات وتجهيزات متطورة.

لم يتطرق المشرع الجزائري إلى تحديد مفهوم اعتراض المراسلات فهل يقصد بها التنصت الهاتفي أم مجرد الاطلاع عليها؟ أو يمتد إلى أكثر من ذلك من خلال ضبط كل ما له علاقة بوسائل المواصلات السلكية واللاسلكية كالبرقيات، الفاكس، التلكس، الرسائل القصيرة للجهاز المحمول، المواقع المفتوحة على شبكة الأنترنت؟

وبالرجوع إلى المادة (08) ف11 من قانون 03/2000 المتعلق بالبريد والمواصلات السلكية واللاسلكية فكل مراسل أو إرسال أو استقبال علامات أو إشارات كتابات، صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي، إذا كان الحال كذلك فلكل إشارة أو كتابة أو صورة أو صوت مهما كانت وسيلة الاتصال يصلح أن يكون محلا للاعتراض.

ب- تعريف تسجيل الأصوات: يقصد به النقل المباشر والآلي للمنتوجات الصوتية من مصادرها بنبرانها ومميزاتها الفردية وخواصها الذاتية بما تحمله من عيوب في النطق إلى شريط تسجيل بحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي[1]. والتسجيل الصوتي المتخذ كوسيلة للتحري عن الجرائم يشمل الكلام المتفوه بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية، وبالرجوع إلى نص المادة (65) م 05 ق.إ.ج.ج، نستشف أن المقصود بتسجيل الأصوات هو: «وضع البرقيات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه

1- سليمان بن عبد الله بن سليمان العجلان، حق الإنسان في حرمة مراسلاته واتصالاته الهاتفية الخاصة في النظام الجنائي السعودي، دراسة تطبيقية مقارنة، الرياض، 2005، ص 377.

به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية»[1].

ج- تعريف التقاط الصور: من التقنيات التي استحدثها المشرع الجزائري في البحث والتحري أسلوب التصوير بمختلف أنواعه وعبر عليه في نص المادة (65) مكرر 09 من ق.إ.ج.ج بعبارة التقاط الصور، والتي تتمثل في وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط الصور لشخص أو عدة أشخاص يتواجدون بمكان خاص، فلم يكتف المشرع بالسماح لقاضي التحقيق بتسجيل الأصوات بل مكنه أيضا من إمكانية التقاط الصور، فعدسة الكاميرا التي أصبحت من أفضل الأساليب لإثبات الحالة بما تنقله من صور حية وكاملة لمكان معين أو لحدث معين أو واقعة معينة، وعرف القضاء هذه العملية بأنها وضع أجهزة تصوير صغيرة الحجم وإخفائها في أمكنة خاصة لالتقاط صور تفيد في إجراء الحقيقة وتسجيلها[2].

2- التسرب: أنه تقنية من تقنيات التحري التي تسمح للشخص التوغل داخل جماعة إجرامية، فإن المشرع الجزائري نجده قد أحاط هذه العملية بمجموعة من الشروط، كما أعطى بعض الصفات التي ينبغي أن يسرب بها العون المتمثلة في السرية، الخديعة واستعمال الهوية المستعارة.

كما جعل المتسرب يظهر كفاعل أصلي في العملية أو شريك فيها أو خاف.

أ- تعريف التسرب: لقد عرف المشرع التسرب في نص المادة (65) م12 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية على أنه: «يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطية القضائية المكلف بتنسيق

1- أحسن بوسقيعة، المرجع السابق، ص 113.

2- مصطفاوي عبد القادر، أساليب البحث والتحري الخاصة وإجراءاتها، مجلة المحكمة العليا، العدد الثاني، 2009، ص 70.

العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف».

كما ألزم المشرع الجزائري أن تنفذ العملية في سرية تامة (م65- م01/16 من ق.إ.ج.)، وبهوية مستعارة واستعمال الخديعة والتعامل مباشرة مع الفاعل الأصلي للجريمة، كما نصت عليه المادة (56) من القانون 01/06 تحت تسمية الاختراق[1].

ب- شروط إجراء التسرب: إن المشرع الجزائري قد وضع مجموعة من الشروط الشكلية والموضوعية لإجراء عملية التسرب يستلزم التقيد والالتزام بها.

1- الشروط الشكلية:

- أن يصدر إذنا للقيام به.
- أن يكون قانونيا وحاملا لصفة الوثيقة الرسمية (ذلك الأمر القضائي الصادر عن وكيل الجمهورية المختص إقليميا، أو قاضي التحقيق بعد إخطار وكيل الجمهورية م65 م11 ق.إ.ج.ج).
- أن يكون الإذن مكتوبا ومبينا بذكر المبررات التي استندت إليها النيابة العامة لإصداره، والتي دفعت ضابط الشرطة القضائية لتنفيذ هذه العملية وتحديد الجريمة، هوية وصفة ضابط الشرطة التي تتم تحت مسؤوليته[2]. وذكر مدة التسرب التي لا يمكن أن تتعدى 04 أشهر.

2- الشروط الموضوعية: هي حالة الضرورة، وأن يكون التسرب تحت مسؤولية ضابط الشرطة القضائية.

1- القانون 01/06 المؤرخ في 20 فيفري 2006 المتعلق بالوقاية من الفساد ومكافحته، الجمهورية الجزائرية، جريدة رسمية، عدد 14، الصادر في 08 مارس 2008.

2- انظر المادة (65) م 01/15 من القانون 06/22، مرجع سابق.

أ- وجود حالة الضرورة: نصت المادة (65) م11 من ق 22/06 بعبارة «عندما تقتضي ضرورات التحري أو التحقيق في الجرائم المذكورة على سبيل الحصر في مادة (65) م05 أعلاه...».

ب- إجراء التسرب تحت مسؤولية ضابط الشرطة القضائية المنسق للعملية: هذا الشرط أوصى به المشرع الجزائري من خلال نص المادة (65 م12) من ق.إ.ج.ج: «يقصد بالتسرب قيام ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية....».

الفرع الثاني: الإجراءات الواردة في القانون رقم: 09-04

بالإضافة للإجراءات العامة الواردة في قانون الإجراءات الجزائية نص القانون 09-04 على بعض الإجراءات التي يتمتع بنوع من الخصوصية في مجال ضبط الجرائم المتصلة لتكنولوجيات الإعلام والاتصال.

أولا: تفتيش المنظومة المعلوماتية

تكمن وظيفة نظم المعلومات في معالجة واسترجاع وتخزين ونشر المعلومات سواء داخل منظومة معلوماتية واحدة أو متصلة بأخرى، وسواء داخل الإقليم الوطني أو خارجه.

1- تعريف التفتيش: لم يضع المشرع الجزائري تعريفا للتفتيش، فقد اعتبره إجراء من إجراءات التحقيق الهدف منه الحصول على الأدلة لإثبات الجريمة للوصول إلى الجاني، هناك صعوبات جمة يصادفها رجال الضبطية القضائية والمحققين في ضبط الجرائم المعلوماتية بسبب طمعيتها الخاصة فهي تتم في فضاء إلكترونية يتسم بالتغيير الديناميكية والانتشار الجغرافي العابر للحدود[1].

1- يوسف المصري: "الجرائم المعلوماتية والرقمية للحاسوب والانترنت"، ط01، دار العدالة، القاهرة، 2011، ص 217.

غير أن المشرع الجزائري خرج عن هذا المبدأ واستبق الأحداث، فجعل من إجراء التفتيش مهمة وقائية للغاية منها الحيلولة دون وقوع الجريمة المعلوماتية من خلال القيام بعمليات المراقبة المسبقة وفق نص المادة (03) من القانون 09-04 السالف الذكر: «.... والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية»، كما نصت المادة (02/09) من نفس القانون على أنه: «في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني...» [1]. وعليه تسمح هذه الإجراءات بتسهيل مكافحة الجرائم المعلوماتية.

إن الهدف من التفتيش المنصب على المنظومة المعلوماتية هو منع المجرم المعلوماتي من تدمير أو إخفاء الدليل للإفلات من العقوبة، وذلك بموجب نصوص القانون 09-04 السالف الذكر وتطبيقا لنصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات خاصة المادتين (26) و(27) المتعلقتين بتفتيش المعلومات المخزنة وضبطها[2]. لذا أدرج المشرع الجزائري التفتيش في مجال الجرائم المعلوماتية في قانون الإجراءات الجزائية، فالتفتيش في هذه الحالة يختلف عن التفتيش العادي، فهو يتوقف أساسا على طبيعة المكان الذي يحتوي على أجهزة الكمبيوتر ومكوناته وفيما إذا كان خاصا أو عاما ناهيك عن تحديد الإقليم إذا كان وطنيا أو أجنبيا، فلقد نصت المادة (05) من القانون رقم 09-04 السالف الذكر على أنه: «يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

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

1- المادة (04) من القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع السابق، ص 06.

2- المادتين (26) و(27) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مرجع سابق، ص 08.

ب- منظومة تخزين معلوماتية...».

من خلال هذه المادة أجاز المشرع الجزائري الدخول بغرض التفتيش ولو عن بعد إلى المنظومة المعلوماتية دون إذن صاحبها، وهذا بالرغم اعتبار برامج الحاسوب من بين المصنفات الأدبية المحمية بموجب نصوص خاصة[1]، وعليه يجب الانتقال إلى مكان تواجد الحاسوب أو أحد مكوناته المادية مثل الأقراص الصلبة المرنة فمن السهولة ضبط جهاز الحاسوب ومكوناته وملحقاته وحجزها وتقديمها كدليل لإدانة المتهم، لأن التفتيش إذا تعلق بالمكونات المادية للحاسوب لا مشكلة ويتم وفقا لأحكام المادة (44) من ق.إ.ج.ج.

2- الجهة القضائية المختصة: بالرجوع إلى نص المادة (4/ ف أ) من القانون رقم: 09-04 السالف الذكر التي بين كيفيات المراقبة للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، بين لنا المشرع الجهة القضائية المختصة بهذه الحالة في نفس المادة الفقرة الأخيرة، إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنع ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة لتكنولوجيات الإعلام والاتصال ومكافحته المنصوص عليها بموجب المادة (13) إذنا لمدة 06 أشهر قابل للتجديد.

إذ يتعين الرجوع إلى التدابير التي نص عليها قانون الإجراءات الجزائية في مجال التحري والتفتيش بالنسبة للجرائم الإلكترونية، وبالضرورة في مجال الاختصاص بالنسبة لوكيل الجمهورية وقاضي التحقيق باعتبارهما الجهة المؤهلة بمنح الإذن بالتفتيش وفقا للشروط المنصوص عليها بموجب نص المادة (44) من ق.إ.ج.ج[2]. وفي نفس الصدد

1- عبد الهادي بن زيطة، حماية برامج الحاسوب في التشريع الجزائري، مرجع سابق، ص 34-35.

2- المواد: 44-37-40 من القانون رقم 66-155 المعدل والمتمم بموجب القانون 06-22 المتضمن قانون الإجراءات الجزائية الجزائري، المرجع السابق.

المادة 37 من القانون رقم 66-155، المعدل والمتمم بموجب القانون 04-14، المؤرخ في 10 نوفمبر 2004، ص 14.

أثارت المادتان 37-40 من ق.إ.ج بتمديد الاختصاص لكل من وكيل الجمهورية وقاضي التحقيق في جرائم معينة من بينها الجرائم الماسة بالمعالجة الآلية للمعطيات.

3- تمديد التفتيش إلى منظومة معلوماتية أو جزء منها: نظرا لخطورة هذه الجرائم المستحدثة، ويقصد ملاحقة المجرم المعلوماتي نص المشرع الجزائري على تمديد إجراء التفتيش سواء داخل الإقليم الوطني أو خارجه.

أ- تمديد التفتيش داخل الإقليم الوطني: أدى سوء استخدام القضاء (Cyberspase)[1] إلى بروز جرائم مستحدثة تسمى بالجرائم المعلوماتية (Cybercrimes)، إذ يمكن للمجرم لدخول والانتقال من منظومة معلوماتية لأخرى بما يسمح له بتغيير أو تدمير المعطيات ناهيك عن صعوبة تتبعه وإيجاد دليل ضده، نص عليها المشرع في نص المادة (05) من القانون 09-04 التي سبق ذكرها، كما نؤكد أن هذه الإجراءات تكتسي طابع الرسمية، وبذلك حاول المشرع الجزائري غلق منافذ إفلات المجرم في هذا النوع من الجرائم التي يتسم بالتعقيد والتطور الدائم في استخدام تقنية الحوسبة والاتصال، مما أجاز معه للسلطات المكلفة بالتفتيش تسخير كل شخص مختص في مجال عمل المنظومة المعلوماتية.

ب- تمديد التفتيش خارج الإقليم وشروط المساعدة القضائية: تتصف الجرائم المعلوماتية بأنها جرائم عابرة للحدود يمكن للمجرم المعلوماتي من أي مكان في العالم يملك جهاز حاسوب متصل بشبكة الأنترنت الإضرار بمصالح الوطن، كاستهداف أمن الدولة واستقرار مؤسساتها أو الدفاع الوطني أو سلامة الاقتصاد الوطني، وفي هذا الصدد نصت المادة (15) من القانون 09-04 على أنه: «زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائية بالنظر في الجرائم المتصلة

1- يقصد بالقضاء السيبراني: العوالم الافتراضية التي تخلفها الشبكات المعلوماتية، للمزيد من التفصيل انظر: حسين بن سعيد الغافري: السياسة الجنائية في مواجهة جرائم الأنترنت، (د.ط)، دار النهضة العربية، القاهرة، 2009، ص 14.

بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني».

وبذلك أقر المشرع إجراءات صارمة لملاحقة هذا النوع من الجرائم خارج الإقليم الوطني، وذلك من خلال توسيع نطاق التفتيش، بموجب نص المادة (05) ف04 من القانون 09-04 السالف الذكر[1].

*** شروط المساعدة القضائية الدولية:**

نصت عليها المادة 16 من القانون 09-04[2]. وتعرف المساعدة القضائية الدولية أنها: «كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمته المحاكمة في دولة أخرى بصدد جريمة من الجرائم»[3]. ونظرا لحالة الاستعجال والسرعة التي تتطالها إجراءات التحقيق في مثل هذه الجرائم التي يستعمل التقنيات المتطورة في مجال الحاسوب والأنترنت ونظم الاتصالات ولضمان عدم إفلات المجرم المعلوماتي من العقاب نصت المادة 16/ ف02 على قبول طلبات المساعدة القضائية حتى وإن جاءت عن طريق وسائل الاتصال السريعة كالبريد الإلكترونية أو الفاكس بشرط التأكد من صحتها فقط.

كما سبق للمشرع الجزائري وضع شروطا للمساعدة القضائية تطبيقا لنصوص لاتفاقية العربية لمكافح جرائم تقنية المعلومات م (04) ف01، وهذا ما ترجمته فحوى المادة (17) من القانون 09-04 يتمثل في:

1- المادة 05/ف04، من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مرجع سابق.

2- المادة 16 من القانون 09-04، المرجع نفسه.

3- خالد ممدوح إبراهيم: الجرائم المعلوماتية، مرجع سابق، ص 407.

- تكون وفقا للاتفاقيات الدولية المبرمة في مجال مكافحة الجرائم المعلوماتية، وما يرتبط بها كتبادل المعلومات وتسليم المجرمين والإنابة القضائية...
- خضوعها لمبدأ المعاملة بالمثل الطي يؤكد سيادة الدولة.
- توفر شروط أمن كافية للتأكد من صحة المعلومات الواردة عن طريق وسائل الاتصال الحديثة مثل: البريد الإلكتروني، الفاكس.

*** القيود الواردة عليها:**

حسب نص المادة (18) من القانون 09-04 السالف الذكر[1].

* أنه يمكن رفض تنفيذ طلبات المساعدة القضائية، إذا كانت تمس أولا بالسيادة الوطنية وما تثيره هذه المسألة من حساسية بين الدول، وثانيا بالنظام العام والآداب العامة.

* إن الاستجابة للمساعدة القضائية، مقيدة بشرط المحافظة على سرية المعلومات المبلغة أيضا عدم استعمالها في غير ما هو مقدم في الطلب، بسبب أهمية المعطيات والبيانات التي قد تحتويها منظومة معلوماتية خاصة ما تعلق بأمن الدولة وأفرادها.

ثانيا: حجز المعطيات المعلوماتية

يظل الهدف الأساسي لعملية تفتيش المنظومة المعلوماتية هو وضع اليد على الأدلة المادية التي تساعد على كشف المجرم، وما يتطلب ذلك من تدابير حجز معينة، خاصة وأن التقنية المعلوماتية تتيح له محو أو تعديل الدليل بكبسة زر وفي جزء من الثانية، أما إذا استحال حجز المعطيات المعلوماتية لأسباب تقنية أجاز المشرع للسلطات المختصة القيام بالإجراءات اللازمة لمنع الوصول إليها وكذا حدود استعمالها.

1- راجع المادة 18 من القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مرجع سابق.

أ- **تدابير الحجز:** يمكن تخزين المعطيات في ذاكرة الحاسوب أو في برامجه إذ تعتبر كيانات غير مادي مما شكل اختلافا في التشريعات العالمية حول مدى اعتبارها قابلو للحجز، حيث أضفى المشرع الجزائري حماية قانونية لقواعد البيانات بموجب نص المادة (05)ف02، من الأمر 03-05 المؤرخ في 19-2003/07 المتعلق بحقوق المؤلف والحقوق المجاورة، واعتبرها من المصنفات المحمية سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى، وطبقا لنص المادة (06) ف01 من القانون 09-04 التي تنص: «... يتم نسخ كل المعطيات اللازمة على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية»، حيث استعمل المشرع مصطلح دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز مثل: القرص المرن، والقرص الصلب والقرص المضغوط والذاكرة الوميضة والأشرطة المغناطسية...الخ، كما ترك المجال مفتوحا أمام ظهور تقنيات تخزين جديدة بناء على التطورات التقنية المذهلة في مجال صناعة الحواسيب وملحقاتها، إذ أنه لا يمكن التعامل مع تلك المعطيات في شكلها الأولى المعنوي، وهي عبارة عن نبضات أو ذبذبات إلكترونية أو إثارة ممغنطة[1]. إلا بعد نسخها على هذه الدعامات.

كما تتم عملية الحجز وفقا للقواعد المقررة في نص المادة (84) من ق.إ.ج. كاحترام إجراءات التحقيق وخاصة احترام سر المهنة وحقوق الدفاع بما يكفل أمن وسرية وسلامة المعطيات في المنظومة المعلوماتية[2]. ووفقا لنص المادة (06) ف03 من نفس

1- أمير فرج يوسف المحامي: الجرائم المعلوماتية على شبكة الأنترنت، (د.ط)، دار المطبوعات الجامعية، الإسكندرية، بدون سنة نشر، ص 237.

2- تنص المادة (84) ق.إ.ج. المعدل والمتمم على أنه: «إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات، فإن لقاضي التحقيق أو ضابط الشرطة القضائية أو المنتدب عنه وحدها الحق في الاطلاع عليها... ويجوز على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في إحراز مختومة، ولا يجوز فتح هذه الأحراز أو الوثائق إلا بحضور المتهم مصحوبا بالمحاسبة...».

القانون، وهذا تحت طائلة العقوبات وفقا لنص المادة (85) من ق.إ.ج، وهو نفس ما نصت عليه المادتان 07 و09 من القانون 09-04، إضافة إلى إجراء الحجز، نص قانون العقوبات في المادة (394) مكرر 06 على تدابير أخرى كمصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع الإلكترونية التي تكون محلا للجريمة[1].

ب- الحجز عن طريق منع الوصول إلى المعطيات وحدود استعمالها: يخلق تتبع المجرم المعلوماتي صعوبات تقنية بالغة تحول في كثير من الأحيان دون الكشف عنه، وبالتالي إفلاته من العقاب، لذلك نص المشرع في المادة 07 من القانون 09-04: «إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 06 أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الدخول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة»، هنا عدم تحديد المشرع للأسباب التقنية المانعة للحجز، سواء ما تعلق بالمنظومة المعلوماتية نفسها كاستحالة الدخول لوجود كلمة السر أو نظام حماية يصعب اختراقه، أو ما تعلق بعملية نسخ المعطيات بسبب التطور الدائم في هذه التقنيات وما يتطلبه ذلك من توفير الوسائل التقنية اللازمة، إضافة إلى ضمان تكوين دوري يقصد اكتساب أعضاء الأجهزة القضائية المختصة في مجال التحقيق والكشف عن الجرائم المعلوماتية المهارات المتطلبة لمكافحتها.

ويبقى الهدف عدم تمكين المجرم من الوصول للمعطيات المخزنة في المنظومة المعلوماتية لاستعمالها أو نسخها أو الاطلاع عليها، لأنها تشكل محل الجريمة، إذ تحتوي على أدلة قد يتمكن المجرم من تهريبها أو تدميرها أو تعديلها، كما نص المشرع تحت طائلة العقوبات على حدود استعمال المعلومات المتحصل عليها من عمليات المراقبة إلا

1- تنص المادة 384 مكرر 06 من ق.ع المعدل والمتمم: «مع الاحتفاظ بحقوق الغير حتى السنة، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي يكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم صاحبها».

فيما تتطلبه التحريات والتحقيقات القضائية وهذا بموجب نص المادة (09) من القانون 09-04 السالف الذكر[1].

ثالثا: مراقبة الاتصالات الإلكترونية في التشريع الجزائري

تعتبر المراقبة الإلكترونية استفتاءا لمبدأ الحق في الخصوصية المعلوماتية تتم عن طريق مراقبة المراسلات الإلكترونية وتسجيل الأصوات والتقاط الصور بوسائل جد متطورة، وهذا نتيجة للثورة التكنولوجية الحديثة التي لعبت دورا هاما في ظهورها.

وعمل المشرع الجزائري على إقرار المراقبة الإلكترونية كإجراء استثنائي من خلال استحداث القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما وضع مجموعة من الضمانات القانونية التي تقيد اللجوء لإجراء المراقبة الإلكترونية.

1- إقرار مشروعية مراقبة الاتصالات الإلكترونية كإجراء استثنائي:

تم إقرار مشروعية مراقبة الاتصالات الإلكترونية كإجراء استثنائي لمواجهة الإجرام المستحدث تجسيدا لمضمون الاتفاقيات الدولية[2]. التي نادت بضرورة استخدام مثل هذا الإجراء في ظل التطورات التي يشهدها الإجرام المنظم، وعملا بمبدأ سمو المعاهدات الدولية على القوانين الداخلية بادرت الجزائر على تكريس هذا الإجراء صراحة

1- تنص المادة 09 من القانون 09-04 على أنه: «تحت طائلة العقوبات المنصوص عليها من التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية»، مرجع سابق، ص 07.

2- من بين الاتفاقيات التي نصت على ضرورة استخدام المراقبة الإلكترونية نجد اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من قبل الجمعية العامة بموجب القرار 25/55 الصادر في 15-11-2000، وذلك= =بموجب المادة (20) منها إضافة إلى اتفاقية الأمم المتحدة لمكافحة الفساد التي دخلا حيز التنفيذ بتاريخ 29-09-2003 نصت هي الأخرى على استخدام المراقبة الإلكترونية بموجب المادة (50) منها تحت مصطلح الترصد الإلكتروني.

بموجب القانون رقم 09-04 المؤرخ في 05 أوت 2005 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك وفقا لنص كل من المادتين 03 و04 اللتان عبرتا صراحة عن إجازة اللجوء لإجراء المراقبة الإلكترونية في مواجهة الجرائم المعلوماتية.

وعلى النحو خرج المشرع الجزائري عن القاعدة العامة التي تقتضي تنفيذ إجراءات التحقيق عند ارتكاب الجريمة لجمع الأدلة والقرائن، وجعل مراقبة الاتصالات الإلكترونية مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة، من خلال القيام بعمليات المراقبة المسبقة، وهو ما نصت عليه المادة (03) من القانون أعلاه التي حددت دواعي اللجوء إلى مراقبة الاتصالات الإلكترونية، المتمثلة في مقتضيات حماية النظام العام، ومستلزمات التحريات والتحقيقات القضائية الجارية[1].

وقد أدرج المشرع الجزائري هذه الآلية ضمن التدابير الوقائية من الجرائم التي ترتكب بواسطة المعلوماتية إلى جانب منح إمكانية القيام بإجراء مراقبة الاتصالات الإلكترونية في إطار التحريات والتحقيقات القضائية بهدف الوصول إلى أدلة لا يمكن الوصول إليها دون اللجوء إلى هذه الآلية، يمكن كذلك تطويع هذه الآلية لكي تعمل في بيئة الرقابة لغرض الوقاية من احتمال وقوع جرائم خطيرة من شأنها تهديد كيان الدولة وهو ما قررته المادة (04) من القانون 09-04 السالف الذكر التي منحت إمكانية القيام بعمليات المراقبة الإلكترونية للاتصالات للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وكذا في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نمحو يهدد النظام العام أو الدفاع الوطني.

1- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، (د.ط)، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011، ص 138.

وتهدف هذه الآلية كذلك إلى تعزيز التعاون الدولي في مكافحة الإجرام المستحدث في مجال المعلوماتية، ذلك أن الإجرام أصبح عابرا للحدود الوطنية لا يرتبط في كثير من الأحيان بمكان معين، ويكون ذلك في إطار المساعدة الدولية المتبادلة وفقا لما نص عليه القانون والاتفاقيات في هذا الشأن[1].

وعليه لا يجوز اللجوء إلى إجراء المراقبة الإلكترونية[2] إلا في الحالات المذكورة في المادة 04 من القانون 09-04 كما يلي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الابحاث الجارية دون اللجوء إلى المراقبة الإلكترونية في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

يتضح من خلال استقراء هذه الحالات أن المشرع الجزائري قلص من الحالات التي يمكن اللجوء فيها إلى إجراء المراقبة الإلكترونية وحصرها في الجرائم التي تمس الأمن الوطني، وحالات تنفيذ المساعدة القضائية ومقتضيات التحريات والتحقيقات القضائية[3] إلا

1- ثابت دنيا زاد، مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، العدد السادس، جامعة العربي التبسي-تبسة، 2016، ص 209-210.

2- ربيعي حسين، المراقبة الإلكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد01، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2016، ص 420-422.

3- محمد بوزينة آمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، مرجع سابق، ص 74.

أنه لم يحدد على سبيل الحصر الجرائم المعنية بهذه المراقبة مما يتضح أنه يمكن تطبيقها على جميع الجرائم في حالة توافر ضرورة التحريات ومستلزمات التحقيقات القضائية.

وتتضمن المراقبة الإلكترونية اعتراض الاتصالات والبيانات الهاتفية واستخدام أجهزة التنصب المختلفة والدارة المغلقة، ونظم التعرف على لوحات أرقام السيارات وغيرها من الأجهزة، بهدف المنع والكشف عن الجرائم الخطيرة التي تهدد حياة الأفراد والجماعات.

إن المشرع الجزائري لم يترك هذا الإجراء دون رعاية قانونية بل قيده بمجموعة من الضمانات.

2- تقييد إجراء المراقبة الإلكترونية بمجموعة من الضمانات القانونية: حرص المشرع الجزائري على تحديد الضمانات التي تسمح باللجوء لإجراء المراقبة الإلكترونية للحد من التعسف في استخدامه من طرف السلطة المختصة به، وحفاظا على الحق في الخصوصية المعلوماتية من كل اعتداء عليه، فقد اشترط للجوء إلى مراقبة الاتصالات الإلكترونية الحصول على إذن من طرف السلطة القضائية إضافة إلى الاحتفاظ بالسرية واستعمال المعطيات المتحصل عليها عن طريق المراقبة في حدود ضيقة.

أ- ضرورة الحصول على إذن من طرف السلطة القضائية المختصة: نصت المادة (14/ ف02) من القانون رقم 09-04 على أنه لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب صادر عن السلطات القضائية المختصة دون تحديد فيما تتمثل هذه السلطة، إلا أنه بالرجوع للمادة (03) من نفس القانون نجد أنها نصت على: «... مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات... ووفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية»، وتحديدا المادة (65) م05 في ق.إ.ج تحدثنا عنها سلفا[1].

1- راجع المادة 65 من القانون رقم 55-155، المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون رقم 06-22، مرجع سابق.

ويجب على القضاء قبل إصدار الإذن تقدير مدى توفر حالة من الحالات الواردة على سبيل الحصر في المادة (04) ف(01).

ب- الالتزام بالسرية أثناء مراقبة الاتصالات الإلكترونية: اشترطت المادة (10) من القانون رقم (09-04) السالف الذكر على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وكذا المعلومات المحصلة منها، لذا يعاقب كل من يتجه نحو استغلال هذا الإجراء لأغراض شخصية، أو كل تجاوز لحدود المراقبة الإلكترونية نحو انتهاك حرمة الحياة الخاصة للأفراد، إلى جانب ذلك تلتزم الجهة المختصة بهذا الإجراء أيضا تحرير محضر كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، وأن يذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها.

ج- حدود استعمال المعطيات المتحصل عليها عن طريق مراقبة الاتصالات الإلكترونية: ينتج عن مراقبة الاتصالات الإلكترونية تجميع وتسجيل محتوى هذه الاتصالات سواء تمثلت في محادثات شفوية أو رسائل إلكترونية متبادلة عن طريق البريد الإلكتروني أو التقاط الصور وذلك باستعمال الترتيبات التقنية المناسبة، وحفاظا على مثل هذه المعطيات المتحصل عليها عن طريق المراقبة قيد المشرع استعمالها في الحدود الضرورية للتحريات والتحقيقات القضائية تحت طائلة العقوبات المنصوص عليها في قانون العقوبات وهو ما أكدت عليه المادة 09 من القانون 04/09.

المطلب الثاني: إثبات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

يعد الدليل الجنائي جوهر الإثبات ووسيلة لإسناد الواقعة الإجرامية إلى المتهم أو نفيه عنه، وبهدف الدليل الجنائي إلى الإثبات ويعرف هذا الأخير على أنه: «إقامة الدليل لدى السلطات المختصة بالإجراءات الجنائية على حقيقة واقعة بأشخاصها ذات أهمية قانونية، وذلك بالطرق التي حددها القانون وفق القواعد التي أخضعها لها»[1].

1- خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص 177.

وإثر التقدم العلمي والتكنولوجي ظهر ما يسمى بالنظام المعلوماتي، مع ما يحتويه من قواعد بيانات وبرامج ومعلومات، حيث تعتبر الجرائم المعلوماتية صنفا جديدا من الجرائم، وذلك لارتباطها بتقنية حديثة وهي تكنولوجيا المعلومات والاتصالات، فظهر بذلك نوع جديد من المجرمين ينتقل بالجريمة من صورتها التقليدية إلى أخرى إلكترونية حديثة، مما استوجب تحول الدليل الجنائي من صورته التقليدية إلى الرقمية، وهذا ما سنتناوله في (الفرع الأول) مفهوم الدليل الجنائي الرقمي، ثم حجية الدليل الرقمي أمام القضاء الجزائي (الفرع الثاني).

الفرع الأول: مفهوم الدليل الجنائي الرقمي

تنوعت التعريفات التي قيلت في شأن الدليل الرقمي أو الإلكتروني وتباينت بين التوسع في مفهومه والتضيق فيه، فقد عرفته المنظمة العالمية لدليل الكمبيوتر (IOCE) في أكتوبر في 2011 بأنه: «المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية»[1].

كما عرفه البعض على أنه: «الدليل المأخوذ من أجهزة الحاسب لآلي يكون في شكل مجلات أو نبضات مغناطسية أو كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة ويتم تقديمها في شكل دليل يمكن اعتباره أمام القضاء»[2].

وعليه يمكن القول أن الدليل الرقمي هو ذلك الدليل الذي يشأ في العالم الرقمي، والذي كون على شكل مستخرج مادي يتم قبوله في جلسة المحاكمة، وسوف نتناول في

1- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط01، مطابع الشرطة، القاهرة، 2008، ص 213.

2- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، (د.ط)، دار الكتب القانونية، مصر، 2006، ص 88.

هذا الإطار إلى خصائص الدليل الرقمي، ثم تقسيماته، وأخيرا الإجراءات التقنية في جمع الأدلة.

أولا: خصائص الدليل الجنائي الرقمي

للدليل الجنائي الرقمي عدة مزايا يتصف بها دون غيره من الأدلة الجنائية، فهو دليل علمي غير مرئي، ذو طبيعة تقنية يصعب التخلص منه ويكون قابلا للنسخ وفقا للتفصيل الآتي:

1- دليل غير مرئي أي يتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، بل إدراكها يتم باستخدام أجهزة ومعدات الحاسب الآلي (hardware) ونظم برمجيات الحاسوب (Sojt ware) [1].

2- الدليل الرقمي من طبيعة تقنية: حيث أن التقنية تنتج فيضانات رقمية تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي يتكون منها الحاسب الآلي فهي ذات طبيعة ديناميكية فائقة السرعة، تنتقل من مكان إلى آخر عن طريق شبكات الاتصال[2].

3- الدليل الرقمي دليل علمي، وبالتالي يستعد تعارضه مع القواعد العلمية السلمية وفقا لقاعدة في القضاء المقارن مفادها: «أن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة»[3].

4- قابلية الدليل الرقمي للنسخ: حيث أن هذه الخاصية تقلل أو تعدم مخاطر إتلاف الدليل الأصلي، حيث تتطابق طريقة النسخ مع طريقة الإنشاء، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل من الفقد والتلف، عن طريق نسخ طبق الأصل من الدليل[4].

1- عائشة بن قارة مصطفى، حجية الدليل الإلكترونية في مجال الإثبات الجنائي، (د.ط)، دار الجامعة الجديدة، الإسكندرية، (د.سن.ن)، ص 61.

2- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، ط01، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 23.

3- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، رسالة دكتوراه، جامعة عين شمس، 2004، ص 977.

4- المرجع نفسه، ص 978.

5- صعوبة التخلص من الدليل الرقمي، حتى في حالة إصدار أمر من الجاني بإزالته فيمكن استرجاعه عن طريق برامج الاسترجاع.

ثالثا: تقسيمات الدليل الرقمي

للدليل الرقمي أشكال مختلفة منها:

1- السجلات المحفوظة في الحاسوب: وتشمل الوثائق المكتوبة والمحفوظة مثل (البريد الإلكتروني ووسائل غرف الدردشة وملفات معالجة الكلمات).

2- السجلات التي يتم إنشاؤها بواسطة الحاسوب: وتعد مخرجات أصلية للحاسوب، حيث لم يشارك الأشخاص في إعدادها، مثل: (سجلات الهاتف، وفواتير أجهزة السحب الآلي للنقود).

3- السجلات المختلطة: التي جزء منها تم حفظه بالادخال وجزء آخر تم إنشاؤها عن طريق الحاسب الآلي، منها أوراق العمل المالية التي تم حفظها بالإدخال تم معالجتها عن طريق برنامج (Exel) لإجراء العمليات الحسابية عليها.

في حين ذهب بعض الفقهاء إلى تقسيم الدليل الرقمي إلى:

- **القسم الأول:** الأدلة الرقمية الخاصة بأجهزة الكمبيوتر، وتشمل على جهاز الحاسب الآلي وملحقاته كالطابعات وكذا المواديم والأقراص المدمجة (CD) وذاكرة الفلاش (USB) والأشرطة الممغنطة[1].

- **القسم الثاني:** الأدلة الرقمية الخاصة بالشبكة الدولية للمعلومات (الأنترنت)، كالبريد الإلكتروني وغرف المحادثات.

1- ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 88.

- **القسم الثالث:** الأدلة الخاصة بالبروتوكولات نقل وتبادل المعلومات بين الأجهزة المتصلة شبكة الأنترنت ومن أمثلتها بروتوكول (TPCIR) [1]. الكوكيز (Cookis) [2].

ثالثا: الإجراءات التقنية في جمع الأدلة الرقمية

لغرض جمع الدليل الرقمي الذي يثبت الجريمة المرتكبة ونسبها إلى المتهم، فإن الخبير أو المحقق يحتاج لمجموعة من الوسائل التي تتنوع من مادية إلى إجرائية.

أ- **الأدوات المادية في جمع الأدلة الرقمية:** وهي الأدوات الفنية التي تستخدم في بيئة النظام المعلوماتية ومن هذه الوسائل:

1- عنوان بروتوكول الأنرتنت (Mak.ip)، البريد الإلكتروني، برامج المحادثة: يعتبر عنوان الأنترنت المسؤول عن تراسل حزم البيانات عبر شبكة الأنترنت وتوجيهها إلى أهدافها، وهو بتواجد لكل جهاز مرتبط بالأنترنت، ويتكون من أربعة أجزاء، حيث أن الجزء الرابع يحدد جهاز الحاسوب الذي تم الاتصال منه، وعليه في حالة اقتراف إحدى الجرائم يكون من السهل التعرف على رقم الجهاز الذي تم من خلاله ارتكاب العملية وبالتالي تحديد الجاني.

2- البروكسي (Proxy): يعمل البروكسي كوسيط بين المستخدم والشبكة، وتقوم فكرته على أساس تلقيه طلبا من المستخدم للبحث عن صفقة ما ضمن ذاكرة (Cache= المحلية المتوفرة لديه، فيحقق البروكسي فيها إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فيقوم بإرسالها دون الرجوع إلى الشبكة، أما في حالة عدم تنزيلها من قبل فإنه يعمل

1- بوتوكول: تقوم بالتعاون فيما بينها بنقل المعلومات الخاصة بالمستخدم وفقا لنظام هيكلة تبادل المعلومات مشار إليه في: سيدي محمد لبشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية، دراسة تحليلية تطبيقية، رسالة الماجستير، جامعة نايف العربي للعلوم الأمنية، الرياض، 2010، ص 73.

2- الكوكيز: أداة يتم من خلالها جمع البيانات التعريفية الخاصة بالمستخدم عن طريق الاتصال بين الخادم (Sewer) والقرص الصلب لحاسب المستخدم، للمزيد من التفصيل انظر: خالد ممدوح إبراهيم، المرجع السابق، ص 304.

كمزود زبون ويقوم بإرسال الطلب إلى الشبكة العالمية، حيث يستخدم أحد عناوين (IP)، ومن أهم مزاياه أن ذاكرة (Cache) المتوفرة لديه تحفظ تلك المعلومات التي تم تنزيلها، وفي حالة وجود أي إشكال يتم فحص تلك العمليات المحفوظة والتي تخص المتهم والموجودة عند مزود الخدمة[1].

3- برامج التتبع: تقوم هذه البرامج بالتعرف على محاولات الاختراق وتقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ومثاله برنامج (Hack tacer) وهو مصمم للعمل في الأجهزة المكتبية، وعندما يرصد محاولة الاختراق يسارع بإغلاق منافذ الدخول أمام المخترق ثم يبدأ بعملية المطاردة تستهدف اقتفاء أثر مرتكب عملية الاختراق، من يصل إلى الجهاز الذي حدثت منه العملية[2].

3- نظام كشف الاختراق: يرمز له بـــ IDS وهي برامج تقوم بمراقبة بعض العمليات التي تتم على مستوى الشبكة أو الحاسب، مع تحليلها بحثا عن وجود أي إشارة تدل على وجود تهديد، حيث أنه يسجل الأحداث فور وقوعها ويقارن نتائج التحاليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية، وفي حالة اكتشافه لإحدى هذه الصفات يقوم بإنذار مدير النظام ويسجل البيانات الخاصة بذلك الاعتداء.

ب- الوسائل الإجرائية: ويقصد بها تلك العمليات التي تهدف إلى جمع الدليل الرقمي، وذلك بتحديد وقوع الجريمة، وانتهاء نسبتها لمرتكبيها، ومن هذه الوسائل:

1- خالد ممدوح إبراهيم، المرجع السابق، ص 304.

2- Hack tracer: يتكون من شاشة رئيسية تقدم للمستخدم بيان شامل بعمليات الاختراق الحيوي على اسم وتاريخ الواقعة وعنوان IP، الذي تمت من خلاله عملية الاختراق واسم الدولة التي تمت منها المحاولة، وصولا إلى الحاسوب الذي تمت منع عملية الاختراق، خالد ممدوح، المرجع نفسه، ص 306.

1- اقتفاء الأثر: تتم عملية تتبع المجرم المعلوماتي خصوصا في حالة إذا لم يتم بمحور آثاره، وهذا عن طريق اقتفاء أثره باستخدام مجموعة من البرامج المساعدة وصولا إلى الحاسب الذي تمت منه العملية.

2- الاستعانة بالذكاء الاصطناعي: يمكن الاستعانة به في حصر الحقائق والاحتمالات أو الأسباب والفرضيات، ومن ثم استنتاج النتائج على ضوء عمليات حسابية يتم تحليلها بالكمبيوتر وفق برامج صممت خصيصا لذلك، حيث أنها تعتمد على نظرية الاحتمالات بإعطاء كافة الاحتمالات، ثم أكثر الإحتمالات وصولا إلى الاحتمال الأقوى مع إعطاء الأسباب[1].

3- التوفيق خلال فقرة التحقيق: من العوامل المساعدة في جمع الأدلة الرقمية وسائل التحفظ على المتهم، ولعل من أبرزها التوفيق الذي يعتبر من إجراءات التحقيق وفق ضوابط حددها القانون وهذا للمحافظة على الأدلة من عملية الإتلاف أو الإخفاء[2].

1- خالد ممدوح إبراهيم، المرجع السابق، ص 306.

2- المرجع نفسه، ص 308.

الفرع الثاني: حجية الدليل الرقمي أمام القضاء الجزائي

يتمتع القاضي الجزائي بسلطة واسعة في تقدير الأدلة حتى وإن كانت عملية مثل الدليل الرقمي، فإن لقبوله يجب توافر شروط معينة يتم على أي أساس تتحدد سلطة القاضي الجنائي في قبول الأدلة الرقمية.

أولا: شروط قبول الدليل الرقمي أمام القضاء

الدليل الرقمي مثله مثل باقي الأدلة التقليدية لكي يتم قبوله أمام القاضي الجزائي لابد أن يتوافر على مجموعة من الشروط والاسم (وصفه) وتتمثل هذه الشروط في:

أ- مشروعية الدليل الرقمي: يشترط أن يتم الحصول عليه بطرق مشروعة مرافقة للقانون، وعليه فإن استخدام وسائل غير مشروحة للحصول على الأدلة الرقمية يترتب عليها بطلان الإجراءات وعدم صلاحيتها لأن تكون أدلة إدانة في المواد الجزائية، ومن هذه الإجراءات استخدام الإكراه المادي أو المعنوي أو الغش ضد الجاني مثلا لفك شفرة الدخول إلى النظام[1].

ب- بلوغ اقتناع القاضي درجة اليقين: يعتبر شرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة تقليدية أو حديثة، فالدليل الرقمي يجب أن يكون غير قابل للشك، إذ أن هذا الأخير لمصلحة المتهم طبقا للمادة 45 من الدستور الجزائري[2].

وإذا كان القاضي في الجرائم التقليدية يستطيع الوصول إلى اليقين عن طريق الحس والمعاينة والتحليل والاستنتاج، فإن الجرم بوقوع الجريمة المعلوماتية يحتاج من القاضي نوعا آخر من المعرفة العلمية بالأمور المعلوماتية، إذ أن الجهل بهذه الأمور

1- المادة 307 من الأمر 55-155 المتضمن قانون الإجراءات الجزائية الجزائري.

2- نصت المادة (45) من المرسوم الرئاسي رقم 438/96 المتعلق بإصدار نص تعديل الدستور الجزائري ورد فيها: «كل شخص يعتبر بريئا حتى تثبت جهة قضائية نظامية إدانته، مع كل الضمانات التي يتطلبها القانون».

يؤدي إلى التشكيك في قيمة الدليل، وبالتالي يقضي بالحكم بالبراءة ويستفيد المتهم المعلوماتي من هذا الشك.

ج- شرط مناقشة الدليل الرقمي: من أهم قواعد الإجراءات أن القاضي لا يبني حكمه إلا على أدلة طرحت أمامه في الجلسة، ويترتب عن ذلك أن يكون الدليل أصل ثابت في أوراق الدعوى، وأن تمنح للخصوم فرصة الاطلاع عليه ومناقشته، وهو ما قضت به المادة 2/R12 ق.إ.ج.ج[1]. وهو ما ينطبق أيضا على الدليل الرقمي أيا كان شكل ذلك الدليل، وتقوم مناقشة الدليل على أمرين اثنين: أولهما إتاحة الفرصة للخصوم للاطلاع على الدليل الرقمي والرد عليه حتى يتمكن الخصوم من استيفاء حقوق الدفاع ومواجهة هذه الأدلة، أما الأمر الثاني أن يكون للدليل أصل في أوراق الدعوى، وذلك حتى يكون اقتناع القاضي مبني على أساس[2].

ولقد أدرج المشرع الجزائري مبدأ المواجهة وأحاطته بضمانات قوية في المادتين 100-101 من ق.إ.ج.

ثانيا: سلطة القاضي الجنائي في قبوله الأدلة الرقمية

تتحدد سلطة القاضي الجنائي في قبول الدليل الرقمي حيث طبيعة نظام الإثبات السائد، وتنقسم هذه الأنظمة إلى: النظام اللاتيني، الأنجلو سلوني.

أ- النظام اللاتيني: يطلق عليه بنظام الأدلة الإقناعية (نظام الإثبات الجر) وفيه أن المشرع لا يحدد أدلة الإثبات ووسائله بل يترك الحرية للقاضي في تأسيس حكمه وفقا

1- المادة (02/212) من الأمر 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بموجب الأمر رقم 17-07 المؤرخ في 27 مارس 2017، «ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه».

2- المادة (01/112) ق.إ.ج: «يجوز إثبات الجرائم بأي طريق عن طريق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لإقناعه الخاص...».

لاقتناعه الشخصي وبدون أن يفرض عليه دليل معين، كرسه المشرع الجزائري كمبدأ في نص المادة 1/212 ق.إ.ج.ج ويتطور دور الإثبات العلمي مع ظهور الدليل الرقمي جعل القاضي في هذا النظام يضطر التعامل مع الأدلة المستحدثة بغية اكتشاف الجرائم، ونتيجة لهذا المبدأ فإن القاضي غير مقيد بالأدلة التي يقدمها أطراف الدعوى، لأن من حقه أن يبادر بنفسه لاتخاذ جميع الإجراءات بحثا عن الأدلة اللازمة لتكوين قناعته، وفي سبيل ذلك له أو يوجه أوامر إلى مزود خدمة الأنترنت من أجل جمع الأدلة الرقمية كعناوين المواقع التي اطلع عليها المتهم، والملفات والحوارات التي شارك فيها، والرسائل التي أرسلها واستقبلها، كما له أن يأمر مشغل النظام بتقدير المعلومات اللازمة لاختراق النظام والولوج إلى داخله، كالإفصاح من الكلمات السرية والشفرات الخاصة لتشغيل البرامج المختلفة، وله أن يأمر بتفتيش الحاسب الآلي[1]. كما أن القاضي الجنائي له أن يتأكد أولا من قبول الدليل ومدى صحته ومصداقيته.

ب- النظام الأنجلوسكسوني: يطلق عليه نظام الإثبات المحدد أو نظام الأدلة القانونية، حيث أن المشرع يحدد فيه الأدلة مسبقا، فلا يجوز للقاضي أن يخرج عليها، وعليه فإنه في حالة توافر الدليل على شروط حددها وقيدها المشرع يكون القاضي ملزما بتأسيس حكمه حتى وإن كان القاضي غير مقتنع به ومن الدول التي أخذت به انجلترا وأمريكا، وجنوب افريقيا[2].

ويعلم هذا الدليل في هذا النظام قاعدتان:

1- قاعدة استبعاد شهادة السماع: والمقصود بها تلك المادة التي يكون الشاهد الذي قد أدلى بها سمعها ولم يشارك في وضعها بإحدى حواسه، ويعتبر الدليل الرقمي شهادة سماع

1- عائشة بن قارة مصطفى، المرجع السابق، ص 194.

2- شيماء عبد الغاني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية دار الجامعة الجديدة، الاسكندرية، 2007، ص 387.

كونه تستضيف أقوالا ومواد قام بوصفها الإنسان في الحاسوب فهي في الحقيقة حدثت خارج المحكمة، وبالتالي تم استيعابها ولكن هناك حالات استثنائية يتم فيها القبول أهمها: البيانات والمعلومات التي يتم الحصول عليها من الكمبيوتر.

2- قاعدة الدليل الأفضل: والمقصود بها أنه لأجل إثبات محتويات كتابة أو سجل أو صورة فإن أصل الكتابة أو السجل أو الصورة يكون مطلوبا.

المبحث الثاني: هيئات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

أدى التطور الكبير في عالم تكنولوجيا المعلوماتية وأجهزة الاتصال واتساع استعمال الشبكة الأنترنت إلى احتلالها مساحة واسعة في الحياة اليومية للمواطنين، لكن في المقابل ساهمت في بروز العديد من الجرائم المتصلة بها التي أصبحت هاجسا حقيقيا للكثير من الدول باعتبارها من أخطر الجرائم العابرة للحدود، الأمر الذي دفعها إلى العمل على إيجاد حلول سريعة لمكافحتها والحد من انتشارها، سواء من خلال إبرام اتفاقيات دولية أو سن تشريعات وطنية، ولأن أفراد قانون خاص للحد ومكافحة الجرائم الإلكترونية باتت اليوم أكثر من ضرورة.

حاولت الجزائر استحداث آليات قانونية تسمح بالحد من انتشار هذه الجرائم، من خلال وضع منظومة قانونية متكاملة ترتكز أساسا على كل من قانوني العقوبات والإجراءات الجزائية، وتم تدعيمها بالقانون رقم 09-04 السابق الذكر المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ومكافحتها، فظهرت العديد من الأجهزة والهيئات المتخصصة في هذه الجرائم على المستوى الدولي والوطني، نشير في هذا المبحث للهيئات الوطنية المختصة في (المطلب الأول) والهيئات الدولية في (المطلب الثاني).

المطلب الأول: الهيئات الوطنية

على المستوى الوطني تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بالإضافة إلى توسيع الاختصاص القضائي عندما يتعلق الأمر بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، لتفصل فيها الأقطاب الجزائية المتخصصة ليس هذا فحسب، بل تحديد الولاية والاختصاص القضائي بالنسبة لجرائم تكنولوجيا الإعلام والاتصال العابرة للحدود تقتضي معرفة المبادئ التي يعتمد عليها في تحديد هذا القانون، وهذا ما سنتناوله في هذا المطلب، حيث تناول (الفرع الأول) الاختصاص القضائي، وفي (الفرع الثاني) الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وفي (الفرع الثالث) تنازع الاختصاص في جرائم تكنولوجيات الإعلام والاتصال.

الفرع الأول: الاختصاص القضائي في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

بموجب أحكام المرسوم التنفيذي رقم 06-348 المؤرخ في 08 أكتوبر 2006، أنشأ المشرع أقطابا جزائية، وحدد لها اختصاص محلي موسعا ونوعيا، وهذا على النحو التالي:

أولا: الاختصاص المحلي: نصت عليه المواد من (02) إلى (05) من المرسوم المذكور على تمديد الاختصاص المحلي لمحاكم كل من: سيدي أمحمد، قسنطينة، ورقلة، وهران إلى دوائر اختصاص من محاكم أخرى[1].

1- من ذلك ما تمت عليه المادة 02 من المرسوم 06-348 المؤرخ في 08 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجمهورية الجزائرية، جريدة رسمية، عدد 63، على أنه يمتد الاختصاص المحلي لمحكمة سيدي أمحمد ووكيل الجمهورية وقاضي التحقيق إلى محاكم المجالس القضائية لكل من الجزائر والشلف والأغواط والبليدة والبويرة وتيزي وزو، الجلفة، المدية، المسيلة، بومرداس، تيبازة، وعين الدفلى، وكذلك بالنسبة لباقي المحاكم الأخرى وفقا لما هو محدد في المواد (03) إلى (05) من المرسوم التنفيذي رقم 06-348.

ثانيا: الاختصاص النوعي

حددت المادة الأولى منه على الاختصاص النوعي لهذه الأقطاب الجزائية، في بعض الجرائم منها الجرائم المتعلقة بالمخدرات، جرائم تبييض الأموال وغيرها... وكذلك الجرائم الماسة كأنظمة المعالجة الآلية للمعطيات.

ثالثا: أما بخصوص عمل ضباط الشرطة القضائية، فإنه طبقا لقواعد الاختصاص المحلي لضباط الشرطة القضائية، التي تقضي طبقا للمادة 16 من قانون الإجراءات الجزائية، على أنهم يمارسون اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة، إلا أنه بموجب أحكام المادة 16 مكرر (1) من قانون الإجراءات الجزائية، فإنه بإمكانهم تمديد عملهم عبر كامل الإقليم الوطني، وذلك لمراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول يحمل على الاشتباه فيهم بارتكاب الجرائم المبينة في المادة 16 من قانون الإجراءات الجزائية، ومنها الجرائم الماسة كأنظمة المعالجة الآلية للمعطيات[1].

وإضافة إلى قواعد الاختصاص النوعي المنصوص عليه في قانون الإجراءات الجزائية، نصت المادة (15) من القانون 09-04 على انعقاد للمحاكم الجزائية بالنظر في الجرائم المرتكبة خارج الإقليم الوطني، عندما يكون مرتكب هذه الجرائم أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني، وهذا ما سنتناوله بالتفصيل في النوع الثالث.

الفرع الثاني: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

أصدر رئيس الجمهورية مرسوم رئاسي رقم 15-261. مؤرخ في 08 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة

1- جاءت في التعديل الصادر بالقانون 06-22 المؤرخ في 20-12-2006، المتضمن تعديل ق.إ.ج.ج.

بتكنولوجيا الإعلام والاتصال ومكافحتها، نص في مادته الأولى على أنه تطبيقا لأحكام المادة 13 من القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تدعي في صلب النص الهيئة[1] وحسب نص المادة الثانية تعتبر هذه الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل[2].

أولا: مهام الهيئة

تمارس الهيئة المهام المنصوص عليها في المادة (14) من القانون رقم 04/09 المؤرخ في 05 أوت سنة 2009 تحت رقابة السلطة القضائية طبقا لأحكام التشريع الساري المفعول لاسيما منها قانون الإجراءات الجزائية والقانون المذكور أعلاه تكلف الهيئة في ظل احترام الأحكام التشريعية المبنية أعلاه على الخصوص بما يأتي:

- اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3].
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بها في ذلك من خلال جمع المعلومات والتزويد بها، ومن خلال الخبرات القضائية وهو ما نصت عليه المادة 14 فقرة (ب) من القانون 09-04.

1- المادة (01) من المرسوم الرئاسي رقم 261/15 المؤرخ في 08 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفياي سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجمهورية الجزائرية، جريدة رسمية، عدد 53، ص 16.

2- المادة (02) المرجع نفسه، ص 16.

3- المادة (04) المرجع نفسه، ص 16.

- تقوم الهيئة بإذن من السلطات القضائية بجميع إجراءات التحري والأعمال التقنية الخاصة بالتحقيقات كمساعدة لمصالح الشرطة القضائية المختصة لتحقيقات لجرائم خاصة ارتكبت أو سهل ارتكابها استعمال تكنولوجيات الإعلام والاتصال.
- ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.
- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

ثانيا: تشكيل الهيئة وتنظيمها

تضم الهيئة لجنة مديرة ومديرية عامة ومديرية للمراقبة الوقائية واليقظة الإلكترونية ومديرية للنسق التقني ومركز للعمليات التقنية وملحقات جهرية[1]، حيث يرأس اللجنة المديرة الوزير المكلف بالعدل وتشكل من الوزير المكلف بالداخلية والوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال وقائد الدرس الوطني والمدير العام للأمن الوطني وممثل عن رئاسة الجمهورية وممثل عن وزارة الدفاع الوطنية وقاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء[2].

تكلف اللجنة المديرة على الخصوم بتوجيه عمل الهيئة والإشراف عليه ومراقبته ودراسة كل مسألة تخضع لمجال اختصاص الهيئة لاسيما فيما يتعلق بتوفر شروط اللجوء

1- المادة (06) من المرسوم الرئاسي رقم 15-261، المتضمن تشكيلة وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مرجع سابق، ص 17.

2- المادة (07) المرجع نفسه، ص 17.

للمراقبة الوقائية للاتصالات الإلكترونية المنصوص عليها في المادة (04) من القانون رقم 04-09 السالف الذكر.

بالإضافة إلى ذلك تختص الهيئة بضبط برنامج عمل الهيئة وتحديد شروط وكيفيات تنفيذ والقيام دوريا بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها، والأهداف المنشودة بدقة، واقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة لتكنولوجيات الإعلام والاتصال ومكافحتها ودراسة مشروع النظام الداخلي للهيئة والموافقة عليه.

أما المادة (11) فتنص على أن مديرية المراقبة الوقائية واليقظة الإلكترونية تكلف على الخصوص على تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول، وإرسال المعلومات المحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة وتكلف مديرية التنسيق التقني على الخصوص بإنجاز الخبرات القضائية في مجال اختصاص الهيئة وتكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها وإعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال والقيام بمبادرة منها، وبناء على طلب اللجنة المديرة لكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها[1].

كما تضم الهيئة قضاة وضباطا وأعوانا من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطني، وفقا لأحكام قانون الإجراءات الجزائية تكلف

1- المادة 08-11-12 من المرسوم الرئاسي رقم 261/15، المتضمن تشكيلة وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مرجع سابق، ص 17.

بتجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية وضمان المراقبة والوقاية للاتصالات الإلكترونية قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات أو الجرائم الأخرى، تحت سلطة القاضي المختص.

للإشارة هنا تمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني والأمن الوطني، وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة لتكنولوجيا الإعلام والاتصال من معالجة أكثر من 1000 جريمة الإلكترونية منها 30% على مواقع التواصل الاجتماعي، هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول عام 2016 وجود 11 قضية متعلقة بالإرهاب الإلكتروني، أغلبها خاصة بتهديدات إرهابية باسم تنظيم داعش الإرهابي لتسفر جهود البحث والتحري والسبق بين مختلف القطاعات المختصة توقيف 58 شخص متوسط في قضايا إرهاب إلكتروني تمت إحالتهم على القضاء.

هذا واستطاعت الشرطة الجزائرية المتخصصة من توقيف ما يزيد من 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق وسوريا وليس كما تمكن من فك شفرات الرسائل المتبادلة، وما يزيد عن 30 خلية تسعى لاستقطاب الشباب لتجنيده عبر مواقع الأنترنت ومنصات التواصل الاجتماعي خاصة الفايسبوك والتويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة وتلقيها معلومات تفيد بوجود منشورات إرهابية تدعو للمشركة في منتديات إرهابية إلى جانب اتصالات محلية دولية[1].

1- آمال بن صويلح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني بالجزائر، مداخلة الملتقى الدولي حول "الإجرام السيراني المفاهيم والتحديات"، 11-12 أفريل 2017، ص 11. للمزيد من التفاصيل عبر الموقع: fsecg.univ-guelma.dz

بالإضافة إلى الهيئة الوطنية، الهيئة القضائية، هناك أجهزة تابعة لها مختصة في متابعة الجريمة الإلكترونية وهي:

أ- **الوحدات التابعة لسلك الأمن الوطني:** توجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية وهي كالتالي:

- المخبر المركزي للشرطة العلمية بالجزائر العاصمة.
- المخبر الجهوي للشرطة العلمية بقسنطينة.
- المخبر الجهوي للشرطة العلمية بوهران.

في سبيل تدعيم المصالح الولائية للشرطة القضائية قامت المديرية العامة للأمن الوطني سنة 2010 بغلق ما يقارب 23 خلية لمكافحة الجريمة المعلوماتية على مستوى ولايات الوسط، الشرق، الغرب والجنوب، التقويم فيها بعد بتعميم الخلايا على جميع مصالح أمن ولايات الوطن[1].

ب- الوحدات التابعة للقيادة العامة للدرك الوطني: أهم الوحدات التابعة للدرك الوطني والمكلفة بالبحث والتحقيق في الجرائم المعلوماتية على المستوى المركزي نجد المعهد الوطني للأدلة الجنائية وعلم الإجرام والكائن مقره في بوشاوي، وهو مؤسسة وطنية ذات طابع إداري تم إنشاءه بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26 جوان 2004.

الوظيفة الأساسية للوحدة هي خدمة العدالة ودعم الوحدات التحري في إطار مهام الشرطة القضائية في مجال مكافحة شتى أنواع الجرائم بما فيها الجريمة المعلوماتية، حيث

1- عبد الرحمن حملاوي، دور المديرية العامة للأمن الوطني في مكافحة الجريمة الإلكترونية، ورقة نصية مقدمة لأعمال الملتقى الوطني حول الوقاية والمكافحة، يومي 16-17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر، ص 09-10.

يوجد بها المركز قسم الإعلام الآلي والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية.

كما توجد أجهزة أخرى على مستوى الدرك الوطني نذكر منها:

- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني.
- مديرية الأمن العمومي والاستقلال.
- المصلحة المركزية للتحريات الجنائية.

إضافة إلى كل فصائل الأبحاث التابعة للدرك الوطني والمكلفة بالتحقيق في الجرائم المعلوماتية[1].

الفرع الثالث: تنازع الاختصاص في جرائم تكنولوجيات الإعلام والاتصال

يعتبر مبدأ الإقليمية[2] هو المبدأ المهيمن على تطبيق القانون الجنائي من حيث المكان، غير أن هذا المبدأ يفقد صلاحيته للتطبيق بالنسبة لجرائم تكنولوجيا الإعلام والاتصال، التي تتجاوز حدود المكان، فجرائم الأنترنت عابرة للحدود، والشبكة العنكبوتية لا تتأثر بها، دولة بعينها، لكن عملا بمبدأ الإقليمية فإن كل دولة تمارس سيادتها على إقليمها بتطبيق قوانينها داخل حدودها، بصرف النظر عن جنسية مرتكب الجريمة الذي يحتمل معه تنازع القوانين حيال الواقعة الواحدة، والذي يتتبع بالضرورة تنازع الاختصاص وبالذات فيما يتعلق بالجرائم العابرة للحدود التي ترتكب عبر شبكة الأنترنت.

1- عز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، ورقة بحثية مقدمة لأعمال الملتقى الوطني حول الوقاية والمكافحة يومي 16-17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر.

2- انظر المادة (588) من قانون الإجراءات الجزائية الجزائرية.

إن تحديد القانون الواجب التطبيق في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود يقتضي معرفة المبادئ التي يعتمد عليها في تحديد هذا القانون، وبالتبعية تحديد الولاية أو الاختصاص القضائي.

أولا: مبدأ إقليمية الاختصاص

تقتضي مبدأ الإقليمية أن يخضع كل من يرتكب عمل إجرامي على إقليم الدولة لقانون العقوبات المعمول به لتلك الدولة، ولا فرق في ذلك بين مواطن أو أجنبي، وتطبيقا للمبدأ نص قانون العقوبات الجزائري في المادة (03) [1] على أنه: «يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية...»، ويعين هذا المبدأ أن قانون العقوبات يطبق على أي جريمة تقع داخل الإقليم الوطني بغض النظر عن جنسية مرتكبه أو المجني)عليه، ويتعقد الاختصاص وفقا له يتحقق أحد العناصر المكونة للجريمة سلوكا أو نتيجة ولو كان الفعل غير معاقب عليه في البلد الأصلي، ومن ثم يجب تطبيق قانون العقوبات الوطني.

كما يمكن بناء على هذا المبدأ متابعة الجاني خارج القطر متى كان مساهما أو شريكا في الجريمة التي وقعت داخل الوطن، غير أن هذا المبدأ يجد صعوبة كبيرة في تطبيقه بالنسبة للجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وهذا بالنظر لطبيعتها وخصائصها التي يميزها عن الجريمة التقليدية وخصوصا صعوبة تحديد مكان وقوعها وارتكابها بدقة، وكذا زمان حدوثها، فتطبق المبدأ يصطدم بعقبة مادية تتمثل في صعوبة تحديد مكان وقوع الفعل الأصلي باعتباره شرط أولي لعقد الاختصاص للقاضي الوطني.

1- راجع المادة 03 من قانون العقوبات الجزائري المعدل والمتمم، مرجع سابق.

ثانيا: الاستثناءات الواردة على مبدأ إقليمية النص الجنائي

إن قانون العقوبات يبسط سلطانه في حدود إقليم الدولة على الجرائم التي ترتكب فيه سواء كان الجاني أو المجني عليه مواطنا أو أجنبيا، لكن هذه القاعدة استثناءات في بعض الحالات.

أ- **مبدأ عينية النص الجنائي:** إن مبدأ العينة ينسجم مع حق الدولة في حماية مصالحها الأساسية والجوهرية من الاعتداء عليها، حيث يعطي لها الحق في هذه الحالة بتطبيق قانونها الجنائي بغض النظر عن مكان وقوع هذه الجرائم أو عن جنسية مرتكبيها[1]، وقد تلقى هذا المبدأ عدة اعتراضات بالإضافة إلى وجود صعوبات في تنفيذه، في حين أخذت به بعض الدول مع تحديد لنوع من الجرائم مثل ما فعل المشرع الجزائري في نص المادة (588) من قانون الإجراءات الجزائية[2]، لكن في الواقع يصادف المبدأ العديد من الصعوبات ترجع بالأساس إلى طبيعة وخصائص جرائم تكنولوجيا الإعلام والاتصال العابر للحدود، حيث لا تظهر مادياتها بوضوح، كما أن الفاعل يبقى مجهولا، مما يترتب عليه التعقيد في الإجراءات.

ب- مبدأ شخصية النص الجنائي: وهو احتفاظ الشخص الأجنبي بقانونه الشخصي وهو خارج إقليم دولته، وذلك في مواضيع معينة كحقه في التقاضي، ويأخذ المشرع الجزائري مبدأ الشخصية في نص المادتين (582)، (583) من قانون الإجراءات الجزائية، إلا أن هذا المبدأ وردت عليه قيود بصفة عامة، وبالتالي فإن الاختصاص لا ينعقد في المحاكم الوطنية بشكل تلقائي بالنسبة للجرائم التي تقع في الخارج.

كما أن هذا المبدأ يعتمد بصفة أساسية على الجاني من حيث الكشف على هويته والتعرف عن جنسيته وهي معلومات تعد صعبة المنال في جرائم تكنولوجيا الإعلام

1- محمود نجيب حسني، شرح قانون العقوبات، القسم العام، ط05، دار النهضة العربية، مصر، 1982، ص 121.

2- المادة 588 من الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

والاتصال العابرة للحدود من جهة، ومن جهة ثانية فإن محاكمة المجرم الذي يقيم في دولة أجنبية تحتاج إلى إجراءات خاصة.

ج- تطبيق مبدأ عالمية النص الجنائي على جرائم الأنترنت: يطبق وفقا هذا المبدأ النص الجنائي على كل جريمة يقبض على مرتكبيها في إقليم الدولة أيا كان مكان ارتكابها وجنسية الفاعل أو الجاني، فالدولة التي تضبط المجرم عليها لمعاقبتها ومحاسبته بحسب قانونها الوطني.

لكن الأخذ بمبدأ عالمية النص الجنائي على إطلاقه، أين يطبق قانون العقوبات على كل مجرم يقبض عليه في إقليم الدولة، أيا كانت الدولة التي ارتكب فيها الفعل الإجرامي وأيا كانت جنسية الجاني قد يؤدي إلى تعارض بين قوانين الدول، إذ يجعل لكل دولة اختصاص بالنظر في أية قضية هي بالأصل من اختصاص قانون آخر، ويتعارض مع مبادئ قانون العقوبات نفسه الذي هو بالأصل قانون إقليمي[1]، كل هذا يجعل تطبيق المبدأ أمرا صعبا من الناحية العملية، ولذا فقد درج البعض على تقييد المبدأ بتطبيق على بعض الأنواع من الجرائم، منها جرائم الأنترنت العابر للحدود، فتضافرت الجهود في مكافحة هذا النوع من الإجرام تشريعيا وقضائيا وتنفيذيا.

1- عمر خوري، شرح قانون العقوبات، القسم العام، (د.ط)، ديوان المطبوعات الجامعية، الجزائر، 2007-2008، ص 34.

المطلب الثاني: الهيئات الدولية

من المعروف أن الجرائم المعلوماتية هي جرائم عابرة للحدود أي أنها لا تتم ولا تنتهي في أراضي دولة نعيشها[1].

وعليه فالتعاون الدولي هم من أهم سبل مكافحتها وملاحقة مرتكبيها فيعتبر التعاون الدولي يزداد محل ارتكاب تلك الجرائم، ويطمئن مرتكبيها من عدم امكانية ملاحقتهم اذ يكون من السهل عليهم من دولة إلى أخرى.

ومن أجل مواجهة وتقليص ارتكاب الجريمة وذلك من خلال اتخاذ إجراءات دولية خاصة منصوص عليها في اتفاقيات دولية وكذا القانون 04/09 وتتمثل هذه الإجراءات في اتخاذ حملة من التدابير والأبيات المشتركة ذات الطبيعة الأمنية والفنية التي تضمن منح الجريمة أو الكشف عنها في مرحلة التنفيذ أو ما يسمى بالمساعدة الأمنية والفنية (الفرع الأول))، أما الثاني فيتعلق بإجراءات اتخاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة وهو يدعى بالمساعدة القضائية الدولية (الفرع الثاني).

الفرع الأول: تدعيم المساعدة الأمنية والفنية المتبادلة بين الدول:

أثبت الواقع بأن أية دولة مهما بلغت قوتها ودرجة تطورها لا تستطيع بمفردها القضاء على الجرائم المعلوماتية العابرة للحدود، لأن سلطتها الأمنية عادة ما تصطدم لمبدأ احترام سيادة الدولة واختصاصها القضائي الذي يقع حجر عثرة أمام اكتشاف هذه الجرائم وتعقب المجرمين وكذا متابعتهم خارج إلى حدود الإقليم الوطني لذا فالسبل في ذلك هو خلق فضاءات تعاون وفنوات اتصال أجهزة الشرطة فيما بين الدول وتنسيق العمل الأمني بعضها مع البعض عن طريق إنشاء هيئات أمنية إقليمية ودولية مشتركة، وخلق فضاءات

1- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي الداخلي، أطروحة لنيل شهادة الدكتوراه علوم -قانون عام- كلية الحقوق، جامعة الجزائر01، بن يوسف بن خدة، 2017-2018، ص 111.

أخرى لتبادل الخبرات والمهارات الفنية في هذا المجال عن طريق عقد دورات تدريسية لمواكبة التطور السريع الحاصل في ميدان الجرائم المستحدث ذات البعد الدولي.

أولا: تفعيل التعاون الأمني أو الشرطي الدولي:

يعتبر التعاون الشرطي مظهر من مظاهر التعاون الدولي الذي تسعى من خلاله الدول إلى تجاوز الصعوبات التي تطرحها عملية البحث والتحري وجمع الأدلة خارج الإقليم الوطني بخصوص الجرائم الإلكترونية العابرة للحدود، ويتجسد هذا التعاون في إنشاء هيئات أمنية دولية وإقليمية مشتركة تضمن الاتصال المباشر بين سلطات الأمن في الدول والتبادل السريع للمعلومات بخصوص الجرائم المرتكبة والمجرمين، وتوفر المساعدة والتنسيق فيما بينها من أجل تحقيق أهداف لا قبل للشرطة الإقليمية تحقيقها، ومن أبرز هذه الهيئات على هذا الصعيد نذكر ما يلي:

1- دور المنظمة الدولية للشرطة الجنائية (Interpol) في دعم التعاون الأمني:

تعتبر المنظمة الدولية للشرطة الجنائية أحسن نموذج للتعاون الشرطي[1]. فهي تمثل أكبر شبكة اتصالات لتبادل المعلومات الأمنية على القوى العالمي، الهدف منها تعزيز وتشجيع المساعدة المتبادلة بين أجهزة الشرطة القضائية في الدول الأطراف من أجل التصدي الفعال للجرائم ذات الطابع العالمي بما في ذلك الجرائم المرتبطة للمعلوماتية وتجاوز العقبات التي ينيرها الطابع العالمي والخاص لهذا النوع من الجرائم، بالإضافة

[1]– أنشئت هذه الهيئة عام 1923 تحت اسم البعثة الدولية للشرطة الجنائية لمناسبة المؤتمر الدول للشرطة القضائية المنعقد بمدينة فيينا، ثم تحولت في عام 1956 إلى "المنظمة الدولية لشرطة الجنائية" بعد اصدار الجمعية العامة لمنظمة الأمم المتحدة في دورتها الخامسة والعشرون قرار اعتماد نظامها الأساسي، ومقرها في مدينة ليون (lyon) الفرنسية، وتضم حاليا أكثر من 189 دولة و للمزيد من التفاصيل حول نشأة الأنتربول أنظر الموقع الإلكتروني التالي:
- http://www.interpol.int/public/ipo/default-asp

إلى إنشاء وتطوير كل النظم القادرة على المساهمة بفعالية في الوقاية من هـذه الجـرام ومكافحتها[1]. وتعتمد المنظمة لتحقيق أهدافها على طريقتين:

الطريقة الأولـى: تتمثل في تجميع كافة البيانات والمعلومات المتعلقة بالجريمة والمجرمين عن طريق المكاتب المركزية للمنظمة الموجودة على أقاليم الدول الأطـراف، وتخزينهـا على شكل أرشيف يتم الرجوع إليها وتبادلها بشكل سريع فيما بين هذه المكاتب كما دعت ضرورة التحقيق والبحث إلى ذلك ومن أجل تمثيل هذه المهمة أنشئت المنظمة في جـوان 2006 نظام عالمي للإنذار العاجل متصل مباشرة مع المكاتب المركزية المتواجـدة فـي الدول الأطراف يعمل 24 ساعة على مدار أيام الأسبوع.

الطريقة الثانية: تتجسد في التنسيق والتعاون بين الدول الأعضاء في ملاحقة المجـرمين الفارين والقبض عليهم وتسليمهم للدولة طالبة التسلم عـن طريـق المكاتـب المركزيـة المتواجدة على أقاليم ومن خلال اذاعة مذكرات التوقيف دوليا ومنحها قوة نفاذ عالمية.

ونظرا لتنوع أنظمة الدول الأطراف فقد وضع خيارين للأنشطة الاتصال داخل هذه الشبكة الأول مخصص للدول المركزية، تجري الاتصالات العالمية لشرطة فيها من خلال الجمعية العامة واللجنة التنفيذية بواسطة الأمانة العامـة للمنظمـة، أمـا الثـاني للـدول اللامركزية، وفيه تجري الاتصالات مباشرة بين أجهزة الشرطة في الدول المختلفة عـن طريق المكاتب المركزية الوطنية.

إلى جانب ذلك تلعب الأمانة العامة للإنتربول دورا كبيرا في تعزيز التعاون الدولي الأمني في مجال مكافحة الجريمة من خلال اصدارها تراث اخبارية إعلامه مـن تلقـاء

1- أنظر هذه الأهداف في المادة (02) من ميثاق المنظمة الدولية للشرطة الجنائية على الموقع الإلكتروني التالي:
- http://adamrights.org/001.htm

نفسها[1]. أو بناء على طلب من المكاتب الوطنية المركزية لشرطة الجنائية في الدول الأطراف، أو من أي منظمة دولية تربطها بالأنتربول اتفاقية تعاون ومن أجل توسيع المساعدة الأمنية أو الشرطة في مجال مكافحة الجرمة الإلكترونية إلى أكبر نطاق ممكن، قام الانتربول بإنشاء عدة مراكز اتصالات إقليمية في كل من طوكيو، نيوزيلندا، نيروبي، أذربيجان، ويوفس أيرس (الأرجنتين) ومكتب اقليمي فرعي في بنكوك لتسهيل عملية نقل وتبادل المعلومات فيما بينها، كما قام مؤخرا بغلق ثلاث هياكل خاصة وهي: الندوة الإقليمية الأوروبية، اللجنة التقنية الأوروبية والأمانة الإقليمية الأوروبية.

ومما لا شك فيه أن سلطات الأمن الجزائرية باشرت العديد من الأعمال الإجرائية في إطار المساعدة القضائية الدولية مع الأنتربول، فعلي سبيل المثال فتح تحقيق قضائي في أكثر من (800) قضية متعلقة بالجريمة الإلكترونية منذ دخول القانون رقم (09-04) حيز التنفيذ، وهي القضايا التي تورط فيها فراتريون وأجانب وتم تسوية معظمها بتعاون مع سلطات الأمن الأجنبية، وقد كان أول هذه القضايا، عندما تحركت سلطات الضبط ولاية باتنة في عام 2010 بناء على معلومات كافية قدمت إليها من قبل الشرطة الأمريكية حول تقني سامي في الإعلام الآلي جزائري عمره 21 سنة، يقوم باختراق موقع شركة أمريكية متخصصة في حماية المعلومات والبرامج الإلكترونية للعديد من الشركات الأمريكية، ثم استغلال تلك المعلومات والبرامج لصالح شركات منافسة مقابل مبالغ مالية ضخمة والذي أحيل للقضاء ومحاكمته وفقا للقانون لمحكمة الجنح باتنة[2].

ومن الأمثلة أيضا: توقيف مصالح الأمن الجزائرية لشاب جزائري صاحب مقهى الانترنت ببلدية بومرداس إثر ورود شكوى من المكتب الفيدرالي الأمريكي للتحقيقات عن طريق مكتب الأنتربول بالجزائر، مفادها أنها تلقت رسالة الكترونية باللغة الانجليزية

[1]- تتمثل هذه النشرات في الثرة الخضراء الغرض منها التزايد بتحذيرات ومعلومات جنائية، أشخاص ارتكبوا جرائم، ويرجع ارتكابهم جرائم مماثلة في بلدان أخرى، والثرى البرتغالية تصدر لغرض التحذير والاستخبار الجنائي.

2- زيدان ربيحة، الجريمة المعلوماتية في التشريع الجزائري، مرجع سابق، ص 146.

مجهولة الهوية مصدرها جهاز يقع في هذه المقهى، تهدد بوضع قنبلة لإحدى أحياء مدينة جوهانسبورغ لجنوب إفريقيا ستهدف المناصرين الأمريكيين قبل انطلاق مباراة كرة القدم بين المنتخب الجزائري والأمريكي في كأس العالم[1]. وبالمقابل تعرضت مؤسسات جزائرية عديدة لأعمال قرصنة واختراق من طرف أجانب، أين استلزم قمعها تعاون وتنسيق أمني مع السلطات المختصة في الدول المعنية، ومن أمثلتها اختراق موقع الشروق أونلاين ومحاولة تخزينه من قبل هاكرز مصريين[2].

2- مساهمة شرطة (الأنترنت) الويب الدولية (IWP) في تكريس المساعدة الأجنبية:

هي منظمة دولة أنشأت في الولايات المتحدة الأمريكية عام 1986، لتلقي بلاغات وشكاوى مستخدمي شبكة الأنترنت وملاحقة الجناة إلكترونيا والبحث والتحري عن الأدلة ضدهم وتقديمهم للمحاكمة.

وتضم هذه الهيئة متخصصين من سلطات إنفاذ القانون والمؤسسات الحكومية وضباط شرطة وخبراء فنيين من 61 دولة حول العالم، كما أنها تمارس اختصاصها في تتبع الأنظمة الإجرامية التي ترتكب عبر شبكة الأنترنت على المستوى العالمي، وبالتعاون والمشاركة مع سلطات إنفاذ القانون التابعة للدول الأعضاء، أو أية دولة أخرى معينة بالجريمة، وتعد منظمة شرطة الأنترنت في عملها على قاعدة بيانات مركزية كعلاقة يتم من خلالها تسجيل كافة الحوادث والأنشطة الإجرامية التي استخدم فيها الأنترنت والتي تم الإبلاغ عنها[3].

1- جريدة الخبر اليومية، العدد الصادر في 2010/07/21.

2- جريدة الشروق اليومية، العدد الصادر في: 2010/05/26.

3- أيمن عبد الحفيظ، حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة، عدد01، القاهرة صادر في 25 جانفي 2004، ص 226.

ونظرا للمهارات الفنية العالية والقدرات المعرفية والعلمية الخارقة التي يتمتع بها القائمين على هذه المنظمة في مجال التكنولوجيات الحديثة، أضحت مقصدا لطلبات المساعدة الأمنية والقضائية من مختلف دول العالم.

3- دور الشرطة الأوروبية (Europol) في توفير الشق الأمني في أوروبا: يمثل الأوروبول جهاز للشرطة الجنائية على مستوى الاتحاد الأوروبي، أنشأ في لكسمبورغ بموجب الاتفاقية 26 جويلية 1995، ودخل حيز الخدمة في عام 1999 بعد أن اتخذ مقره في مدينة لاهاي بهولندا، ليكن همزة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال ملاحقة الجرائم العابرة للحدود بما فيها جرائم الإرهاب والمخدرات الجريمة المنظمة، وكذا الجرائم الإلكترونية[1].

ويهدف أساسا هذا الجهاز إلى تسهيل عملية البحث والتحري وتبادل المعلومات بين سلطات الأمن التابعة لدول الاتحاد، وتجميع. تخزين وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أية دولة عضو بخصوص جريمة من الجرائم المذكورة بما في ذلك الجريمة الإلكترونية(2)، كما يتولى الأوروبول إسداء النصيحة وتقديم التوجيهات والإرشادات المقيدة ومختلف أنواع الدعم المادي أو اللوجيستيكي لهيئات التحقيق الوطنية.

استحدث جهاز على مستوى الأوروبول في عام 2010 أطلق عليه اسم (**Internet Crime Reporting online cros**) مهمته توفير أكبر قدر ممكن من التعاون والنسق الأمني السريع في مجال مكافحة الجريمة الإلكترونية بين دول الاتحاد الأوروبي، وهو الجهاز الذي تم تدعيمه مؤخرا في جويلية 2017 بهيئة أخرى متخصصة تدعى المركز الأوروبي للجريمة الإلكترونية **(EC3)**.

1- الموقع الإلكتروني Europolsur :http://www.europol-eu.int

2- انظر مبادئ وأهداف الأوروبول في المادة (K19) من اتفاقية مستريخت منشور في الموقع الإلكتروني: http://fr.wikipidia.org/wikitrait/3/agde maastiricly

4- منظمة الشرطة الجنائية الإفريقية (AFRIPOL): وهي أكبر منظمة شرطة في القارة الإفريقية مكونة من قوات الشرطة لـــ 41 دولة أنشأت بمبادرة من الدولة الجزائرية يوم 13 ديسمبر 2015، ومقرها بالجزائر العاصمة[1]، ومع الإعلان رسميا عن بداية نشاطها يوم الأحد 06-07-2017 في الاتحاد الإفريقي المنعقد بالجزائر، وترتكز مهام الأفريبول كما أعلن عنها المدير العام للأمن الوطني الجزائري في مضاعفة رصيد تعاون الشرطي الإقليمي والدولي، تحديد السياسة العامة للشرطة الجنائية وتوفير التكوين وإعادة تأهيل مختلف أجهزة الشرطة الإفريقية التي تشهد تأثرا أو ضعفا على مستوى الأداء، تعزيز قيم السلم والأمن والاستقرار في القارة الإفريقية، وضع التحديات وإيجاد الحلول الجادة والفعالة للجرائم العديدة التي تواجهها بعض الدول الإفريقية، مثل تنامي الجرائم الإرهابية والمتاجرة بالمخدرات والقرصنة البحرية وتبييض الأموال والجرائم المعلوماتية، السماح بالتحدث بصوت واحد على الصعيد الدولي وتطور الموقف الإفريقي المشترك في سبيل تفضيل الحلول الإفريقية وتفادي الوصفات المفروضة عليها، وكذا السعي إلى تعميق تبادل وجهات النظر حول ترقية العلاقات استثنائية بين المؤسسات الشرطية للبلدان الإفريقية[2].

ثانيا: تكثيف التعاون الفني الدولي

لا تكفي المساعدة الأمنية الدولية وحدها لتجاوز العقبات التي يفرضها التحقيق الجنائي في الجرائم الإلكترونية، بل لابد من مصاحبتها بالمساعدة الفنية وتبادل الخبرات

1- طرحت الجزائر لأول مرة إنشاء منظمة الأفريبول الندوة الجهوية الإفريقية 22 للأنتربول التي احتضنها في شهر سبتمبر 2013، وتم دعم الفكرة على هامش الجمعية العامة لـــ 82 للمنظمة الدولية للشرطة الجنائية "الأنتربول" التي انعقدت في أكتوبر 2013 في كولومبيا، قبل أن يتم اعتماد الفكرة من خلال تبني الوثيقة المبدئية وإعلان الجزائر خلال الندوة الإفريقية للمديرية والمفتشين العامة الأفارقة للشرطة المنعقدة في فبراير 2014 بالجزائر العاصمة، ثم تبنيها رسميا خلال القمة الـــ 23 للاتحاد الإفريقي في غينيا الإستوائية في جوان 2014 سابقا.

2- أنظر: تصريحات المدير العام للأمن الوطني الجزائري عبد الغاني هامل حول مهام الأخر في جريدة الرياض اليومية الصادرة بتاريخ: 7-08-2017، على الموقع التالي:
http://www.alriyath.com/1109557

والمعارف بين الدول، لأن سلطان الأمن وأجهزة العدالة الجنائية ليست بذات الجاهزية والكفاءة لمواجهة الجريمة الإلكترونية في جميع الدول، إنما تختلف من دولة إلى أخرى بحسب درجة تقدمها ورقيها.

ومن هذا المنطلق فقد ناشت معظم الاتفاقيات الدولية والإقليمية ذات الصلة بضرورة وأهمية وجود تعاون متبادل في مجال التدريب ونقل الخبرات والمعارف فيما بين الدول[1].

وتتم عملية تبادل المساعدة الفنية بين أجهزة العدالة الجنائية للدول من طريق ندوات و مؤتمرات أو توصيات عمل جماعية متخصصة تعقد على المستوى الدولي أو الإقليمي، حيث تقدم هذه الفعاليات العلمية من أبحاثها ودراساتها حول المستجدات المتعلقة بالجرائم الإلكترونية المستحدثة من خلال تحليل ومناقشة أبعادها وتحديد أنماطها وأهم الصفات التي يتميز بها المجرم الإلكتروني والدوافع وراء ارتكابه للجريمة، وبيان أساليب ارتكابها، مخاطرها وتهديداتها وما يقابلها من وسائل الوقاية والمكافحة في النهاية بتقارير وتوصيات أو اتفاق مشترك يفيد الجميع.

الفرع الثاني: تشجيع المساعدة القضائية الدولية

يقصد بالمساعدة القضائية الدولية، كل إجراء قضائي تقوم به دولة من شأنها تسهيل عملية للمتابعة والمحاكمة الجزائية في دولة أخرى بخصوص جريمة من الجرائم[2]. انطلاقا من هذا التعريف تظهر الحاجة الملحة إلى المساعدة القضائية الدولية في عملية مكافحة الإجرام العابر للحدود بصفة عامة والجريمة الإلكترونية على وجه الخصوص،

1- نذكر على سبيل المثالث نص المادة (29) من اتفاقية منظمة الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000، المادة 09، من مشروع الاتفاقية العربية لمكافحة المنظمة عبد الحدود

2- يوسف حسين يوسف، الجرائم الدولية للأنترنت، ط01، المركز القومي للإصدارات القانونية، القاهرة، 2011، ص 150.

سبسب ما تثيره هذه الأخيرة من صعوبات في تحديد هوية المجرم الإلكترونية صعوبات انباتها وملاحقة مرتكبيها، في ظل عالميتها وتشتت عناصرها بين الدول، وكذا المشكلات المتعلقة بكيفية استيراد البيانات التي تم تخزينها عن بعد في حالة اعتبارها دليل اثبات، حيث لا توجد قاعدة عامة كل المشكلات دون تعاون أو مساعدة قضائية.

ما بخصوص التعاون القضائي الدولي في مجال التصدي لظاهرة الإجرام الإلكترونية فتعتبر الاتفاقية الأوروبية حول الجريمة الإلكترونية لعام 2001 نموذجا يقتد به، لإقرارها عدة إجراءات تعاون مستحدثة بالإضافة إلى تعزيزها لصور التعاون القضائي الدولي المعاون عليها أو التقليدية، والتي سوف نخصها بالدراسة على هذا المنوال:

أولا: تثمين الإجراءات التقليدية للتعاون الدولي: [1]

وتتضمن مختلف صور التعاون التي تشري على الجرائم الإلكترونية وغيرها من الجرائم التقليدية العابرة للحدود على حد سواء، وقد كرستها الاتفاقية الأوروبية في المادة (2) حينما أوصت الدول الأطراف على تطبيق الاتفاقيات الدولية حول التعاون الدولي في المسائل الجريمة ذات الصلة، ويمكن تلخيص هذه الإجراءات فيما يلي:

أ- **تبادل المعلومات:** يعتبر هذا الإجراء من وسائل التعاون الدولي على المستوى الإجرائي الجنائي، التي تسمح بالاتصال المباشر بين الأجهزة القضائية والأمنية في الدول المختلفة من أجل تبادل المعلومات المتعلقة بالجريمة والمجرمين، وعادة ما يتحقق هذا الإجراء بتقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية، لمناسبة نظريها في جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات المتخذة ضدهم والسوابق القضائية الخاصة بهم.

1- براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 315.

كما قد يتحقق تبادل المعلومات أيضا بشكل عفوي مثلما أكدت المادة (26) من الاتفاقية الأوروبية حول الجريمة الإلكترونية لعام 2001، وذلك بقيام السلطات القضائية في دولة ما من تلقاء نفسها بتقديم معلومات مهمة ومفيدة للتحقيقات أو الدعاوي الجنائية التي تقوم عليها مثيلتها في دولة ثانية، ومن دون أن تطلبها منها هذه الأخيرة أن تدرك حتى بوجودها.

ولأن المساعدة القضائية الدولية بما فيها تبادل المعلومات تتم في الغالب وفق الطرق الرسمية الدبلوماسية التي تتسم بالبطء والتعقيب، فقد أضافت المادة (3/27) من الاتفاقية المذكورة أعلاه، أنه في حالة الطوارئ أو الاستعجال، كما هو الحال عادة بالنسبة لتحقيق في الجرائم الإلكترونية، يمكن ارسال طلبات تبادل المعلومات مباشرة من قبل الهيئات القضائية أو الأمنية في الدولة التي قدمت إلى الهيئات القضائية أو الأمنية التي تحوز على هذه المعلومات في الدولة المطلوب منها، على أن تتولى الهيئات الأولى عقب هذا الإجراء الاسترشادي نسخة عن الطلب إلى السلطات المركزية التابعة لهم ليتم نقله إلى السلطات المركزية التابعة للفريق المطلوب منه[1].

ولقد لقيت هذه الصورة من المساعدة القضائية صدى كبير في العديد من الاتفاقيات الدولية، أهمها ما جاء في المادة الأولى فقرة (02) من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية(2). والمادة (48) فقرتها الأولى البند (د) من اتفاقية الأمم المتحدة لمكافحة الفساد والتعاون الدولي، ثم المادة الرابعة فقرة (01) في معاهدة منظمة المؤتمر الإسلامي لمكافحة الارهاب الدولي(3). وكذا ما جاء الفترات الثالثة

1- أنظر نص المادة (3/27) من الاتفاقية الأوروبية حول الجريمة الإلكترونية لعام 2001، مرجع سابق.

2- صدرت هذه المعاهدة الجنائية اختتام العملية العامة 68 للأمم المتحدة المنعقدة في 990/12/14، وقد أوحيت المادة 2/01 منها على الدول الأطراف التوفير لبعضها البعض أكبر قدر ممكن من المساعدة القضائية وتبادل المعلومات.

3- اعتمدت من قبل مرتمر وزراء خارجية دول منظمة المؤتمر الإسلامي في اختتام اجتماعهم المنعقد في الفترة من 28 جوان إلى 01 جويلية 1999.

والرابعة والخامسة من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية(1). إذ فرضت على الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي.

كذلك ما قضت به المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي شأن ضرورة تبادل المعلومات بين الأطراف والتنسيق بين الأنظمة القضائية العربية، وما ورد في المادتين الأولى والثانية من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي(2).

أما على مستوى التشريع الوطني، فلم يغفل المشرع الجزائري عن النص على هذا الإجرام المهم جدا للمساعدة القضائية الدولية في المادة (17) من القانون (04/09) المتضمن الوقاية من الجرائم المتصلة لتكنولوجيات الاعلام والاتصال ومكافحتها، إذ أجاز للسلطات المهنية الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات ولو باستعمال مختلف وسائل الاتصال السريعة في حالة الاستعجال، وذلك في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل، ليس هذا فحسب بل قام بإنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا المعلومات تشكل من خبراء ومتخصصي في هذا المجال، وجعل نم مهامها الأساسية السهر على تنفيذ طلب المساعدة الصادرة عن الدول الأجنبية

1- يتم التوقيع عليها في مدينة باليرمو عام 2000، متوفرة في الموقع التالي:
http://www.uncjm.org/documentconvartion/dcotac/final.document

2- صدرت الاتفاقية الأولى في 6-4-1993 بمدينة الرياض، أما الثانية في 22-12-2003، الكويت مشار اليهما في: فهد عبد الله العيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق الجامعية القاهرة، 201، ص 534.

وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها في إطـــار الاتفاقيات التي توقعها في الجزائر[1].

2- نقل الإجراءات:

يقصد بهذا الإجراء، قيام دولة ما بناء على اتفاقية أو معاهــدة باتخـــاذ اجـــراءات جنائية على اقليمها بخصوص جريمة ارتكبت في اقليم دولة أخرى ولمصلحة هذه الأخيرة متى توافرت شروط معينة، أهمها التجريم المـــزدوج، وشـــرعية الإجـــراءات المطلوبـــة اتخاذها بمنظور قانون دولة المطلوب منها، وأن تكون هذه الإجراءات ضرورية ومهمـــة لكشف الحقيقة.

ولقد تم النص لأول مرة على نقل الإجراءات كإحدى صور المساعدة القضائية في المادة الثالثة من الاتفاقية الأوروبية للمساعدة المتبادلة في القضايا الجنائية للعام 1959[2]. ثم تناقلتها عديد من الاتفاقيات الدولية والاقليمية، في مقـــدمتها معاهـــدة الأمـــم المتحـــدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية عام 1990، معاهدة منظمة المـــؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999[3]. واتفاقية الأمم المتحدة لمكافحـــة الجريمـــة المنظمة عبر الوطنية لعام 2000[4].

ومع إشاعة الجرائم المرتبطة بتكنولوجية الاعلام والاتصال الحديث، زادت الحاجة إلى المساعدة القضائية الدولية من طريق نقل الإجراءات لكن ليس على الطريقة التقليديـــة

1- أنظر المادة 2/4 البند السادس من المرسوم الرئاسي رقم (15-261) المؤرخ في 8 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة لتكنولوجية الاعلام والاتصال، مرجع سابق.

2- نصت هذه المادة على أنه: «يجب على الدولة المطلوب منها أن تنفذ وفقا للنمط المنصوص عليه في قانونها الداخلي، أية رسائل تتعلق بالقضايا الجنائية، والموجهة إليها من السلطات القضائية للدول الطالبة لأغراض للحصول على شهادة، أو ارساء أشياء أو مواد لتقديمها كدليل، أو محاضر رسمية أو اية وثائق قضائية»

3- أنظر نص المادة (09) من المعاهدة (اعتمدت من قبل وزراء الخارجية دول المنظمة المنعقد في أوغادوغة المنعقد خلال فترة 28 يونيو إلى 1 يوليو 1999 الموقع التالي: hrlibrary.unn.edu.arab -

4- أنظر المادة (25-3) من هذه الاتفاقية، مرجع سابق.

والبطنية القائمة على نقل الوثائق الخطية والمختومة عبر الفترات الدبلوماسية أو أنظمة إرسال البريد القديمة، إنما وفق وسائل جديدة فورية وسريعة، ذات مصداقية ودقيقة بالقدر الكافي الذي يتطلب التعامل مع هذه الجرائم، وهو ما أوصت به الفقرة الثالثة من المادة 25 من الاتفاقية الأوروبية حول جريمة الإلكترونية نصبها على أنه «يمكن لكل طرف في حالة الاستعجال، أن يقدم طلبا للمساعدة المتبادلة أو الاتصالات من طريق وسائل الاتصال السريعة كالفاكس أو البريد الإلكتروني، وذلك لما توفره هذه الوسائل من شروط كافية للأمن والتوثيق بما في ذلك التشفير إن كان ضروريا، مع التأكيد الرسمي اللاحق حينما يكون ذلك مطلوبا من طرف الدولة الموجه إليها الطلب، وعلى هذه الأخيرة الموافقة على طلب المساعدة والرد عن مرافق احدى وسائل الاتصال العاجلة المذكورة»[1].

3- تبادل الانابة القضائية الدولية:

وهو طلب تتقدم به دولة ما إلى أخرى يتضمن اتخاذ إجراء قضائي من إجراءات الدعوى الجزائية في اقليمها نيابة عنها، ويكون هذا الإجراء ضروري للفصل في قضية معروضة على السلطة القضائية في الدول الطالبة[2]. وتهدف هذه الصورة من صور المساعد القضائية إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل اقليم الدول الأخرى، كسماع الشهود إو إجراء التفتيش وغيرها، وفي العادة يتم إرسال طلب الانابة القضائية عبر القنوات الدبلوماسية، ومن ثم ارساله بعد ذلك إلى السلطات القضائية المختصة في الدولة المتلقية

1- حازم العارون، الإنابة القضائية الدولية المجلة الجنائية القومية، العدد الثاني، القاهرة، 1988، ص 20.

2- نذكر منها ما ورد في المادة 2/27 من الثقافة الاتفاقية الأوروبية حول الجرائم الإلكترونية لعام 2001، إذ نصت على أنه:

2- أ: يجب على كل طرف أن يعين هيئة مركزية أو هيئات تكون مسؤولة من ارسال أو الرد على طلبات المساعدة المتبادلة أو تنفيذ هذه الطلبات أو ارسالها إلى السلطات المختصة

2-ب: يجب على الهيئات المركزية أن تتصل بعضها البعض بشكل مباشر ...

الطلب، إلا أنه وسعيا وراء الحد من الروتين والتعقيد والبطاء الذي تتميز بها الإجـــراءات الدبلوماسية، صبحت المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضـــائية الدوليـــة تشترك على الدول الأطراف تعيين سلطة مركزية، عادة ما تكون وزارة العـــدل، ترســـل إليها الطالبات مباشرة لاختصار الوقت وتسريع الإجراءات بدلا من الولوج إلى القنـــوات الدبلوماسية التي قد تأخذ وقتا أطول[1].

وتجدر الإشارة إلى أن التشريع الجزائري جاء خاليا من أي تنظيم لمسألة الإنابـــة القضائية الدولية، مما يعني ترك المجال لأحكام الإنابة القضائية الواردة فـــي الاتفاقيـــات الدولية التي وقعت عليها الجزائر، ويمكن أن هنا باتفاقية تبادل الإنابة القضـــائية الدوليـــة المبرمة بين الجمهورية الجزائرية وفرنسا في 1962/08/28، والتـــي نصـــت علـــى أن البلدين «يتعاونان لتقديم المعونة أو المساعدة القضائية التي تطالبها كل دولة» كما تضمنت شروط تنفيذ الإنابة النضالية، وضوابط المحافظة على النظام العام في الدولة المرسل إليها طلب الإنابة، وكذا الجهة التي تتولى تنفيذ الإنابة، وتحمل نفقاتها.

4- تسليم المجرمين:

يعتبر هذا الإجراء شكل من أشكال التعاون القضائي الدولي لمكافحة الجريمة الذي فرضته التطورات العامل في كافة المجالات ومنها مجال تكنولوجيات الإعلام والاتصال، إذ لم تعد الحدود الجغرافية للدول تشكل حاجزا أما مرتكبي الجـــرائم، كمـــا أن نشـــاطهم الإجرام لم يعد مقتصرا على اقليم معين بل امتد إلى عدة أقاليم، وباعتبـــار لا يمكـــن لأي دولة تجاوز حدودها الإقليمية متابعة المجرمين الفارين جزائيا، كان لا بد من إيجاد آليـــة معينة للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق اقليمها لتفادي إفـــلات هؤلاء المجرمين من العقاب.

1- براهيمي جمال ،التحقيق في الجرائم الالكترونية ، المرجع السابق ،ص323.

ويرتكز أساسا ذا الإجراء، على قيام دولة يتواجد على إقليمها متهم باحدى الجرائم العابرة ومنها الجريمة الالكترونية أو مدان فيها بحكم قضائي، تسليمه إلى الدولة التي وقعت الجرمة على اقليمها، أو التي صدر فيها حكم الإدانة، الهدف محاكمته أو تنفيذ الحكم عليه، وذلك بناء على طلب هذه الدولة وتأسيسا على معاهدة تسليم المجرمين بين الدولتين أو على أسا مبدأ المعاملة بالمثل[1]. ومن هنا تبين أن هذا الإجراء تحقيق مصلحة كلتا الدولتين المعنيتين لعملية التسليم، فهيو يحقق مصلحة الدولة المطلوب منها تسليم كونه يساعد على تطهير اقليمها من شخص مجرم قد شكل بقاءه تهديدا لأمنها واستقرارها، ونظرا للمصلحة المشتركة التي يحققها الإجراء المذكور، لم تتأخر معظم الدول في عقد اتفاقيات دولية واقليمية ثانية[2]. وقد كانت الدول الأوروبية سابقة، إذ أبرمت منذ 13 ديسمبر 1957 أول اتفاقية في هذا المجال، نظمت فيها أحكام التسليم شروطه وإجراءات، وهي الأحكام التي تم تثبيتها وتدعيمها بموجب المادة (24) من اتفاقية الأوروبية حول الجرائم الإلكترونية لعام 2001، من خلال إدراج الجريمة الإلكترونية ضمن الجرائم التي يجوز فيها تسلح المجرمين[3]. وكذا اقتراح بعض الحلول لمشاكل التي تثيرها عملية التسلح[4].

أما عن المشرع الجزائري، فقد اعترف بدوره بإمكانية تسليح المجرمين كإحدى التدابير المساعدة القضائية وجعل منه مبدأ دستوري، وذلك نصه في المادة 82 من

1- لحمر فاقة، إجراءات تسليم المجرمين في الجزائر على ضوء الاتفاقيات الدولية، مذكرة لنيل شهادة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة وهران، 2013، ص 08.

2- اتفاقية الجزائرية البريطانية المؤرخة في 11-06-2006، والتي أثرها استلمت الجزائر المتهم عبد المؤمن خليفة، أنظر: جريدة رسمية، عدد 81، صادر في 2006/12/13.

3- تنص المادة 24 على: 1-أ: «تطبق هذه المادة على تسليم المجرمين فيما بين الأطراف بالنسبة للجرائم المنصوص عليها في المواد من (2-11)من هذه الاتفاقية ...»

4- تعتبر الجرائم الجنائية الواردة في الفقرة (1) من هذه المادة مدرجة كجرائم يجب فيه التسليم في أية اتفاقية بشأن تسليم المجرمين قائمة بين الأطراف، ويتعهد الأطراف بإدراج هذه الجرام على أنها يتم فيها تسليم المجرمين في أي اتفاقية بشأن تسليم المجرمين يتم إبرامها فيها»

الدستور على «مبدأ جواز تسليم شخص بناء على قانون تسليم المجرمين وتطبيقا لـــه»[1]. أما عن الأحكام الموضوعية والإجرامية المتعلقة بعملية تسليم المجرمين فقد فصل فيها في المواد (694) وما يليها من قانون الإجراءات الجزائية.

ثانيا: إقرار إجراءات جديدة للتعاون الدولي القضائي: [2]

لقد بينا كيف أن إجراءات المساعدة القضائية التقليدية، بالرغم من أهميتها، إلا أنها تتم بالطرق الدبلوماسية التي تتم بالبطء والتعقيد، وهو ما يجعلها وغالب الأحســـان غيـــر مجدية في مواجهة الجرائم الإلكترونية التي تتميز بمنتهى؟؟؟؟ نتيجة لهذا الوضع ظهـــرت الحاجة إلى البحث عن سبل بديلة للتعاون القضائي الدولي تتفق مع طبيعـــة هـــذا النـــوع المستحدث من الجرائم، ولعل من ضمن هذه السبل التي وجدها الدول استحداث اجراءات تعاون جديدة معنية بالتحقيق في الجرائم الإلكترونية، وهي الإجراءات ذاتها التي تضـــمنها القسم الثاني من الفصل الثالث من الاتفاقية الأوروبية حول الجريمة الإلكترونيـــة، والتـــي سنذكر على النحو التالي:

1- طلب الحفظ العاجل للمعطيات المخزنة:

يعتبر هذا الإجراء آلية جديدة للتعاون القضائي الدولي في مجال مكافحة الجـــرائم المرتكبة عبر وسائل الإعلام والاتصال الإلكترونية، والتي استحدثت بموجب المادة (29) من الاتفاقية الأوروبية لعام 2001، لتمكين أي دولة طرف في الاتفاقية من المطالبة بحفظ البيانات المخزنة في أجهزة الحاسب الموجودة في أراضي الدولة المطلوب منها على وجه

1- أنظر المادة (24) فقرة 1 ب، والفقرات 3، 4، 5، 6 وغيرها.

2- أنظر المادة (82) من القانون (16-01) المؤرخ في 6 مارس 2016، يتضمن التعديل الدستوري، مرجع سابق.

السرعة، خلال الفترة اللازمة لتقديم طلب المساعدة المتبادلة شأنها بغرض القيام بالتفتيش، أو الدخول بأي طريقة مماثلة، وضبط، أو الحصول أو الكشف عن هذه البيانات[1].

وفي حالة قبول الطلب المذكور تلتزم الدولة المطلوب منها بحفظ تلك البيانات لمدة لا تقل عن ستون (60) يوما، حتى تبين للدولة طالبة الحفظ تقديم طلب القيام بالتفتيش أو الدخول بأي طريقة مماثلة، وضبط أو الحصول أو الكشف عن هذه البيانات، ولكن بعد تلقي هذا الطلب ستمر عملية حفظ البيانات إلى غاية النظر فيه بالرفض أو القبول[2].

ومن مميزات هذا الإجراء أنه بمثابة تدبير تحفظي احترازي سريع تسعى من ورائه الدول إلى حماية بيانات الجريمة من أي تعتبر أو إزالة أو محور قد يسمها من قبل المجرم خاصة بعد علمه بوجود إجراءات التحقيق والمتابعة اتخذت ضده، كما يكفل المحافظة على سرية البيانات التي تهم الشخص المعني.

3-طلب الكشف عن البيانات المحفوظة:

يعتبر هذا الإجراء مكمل للإجراء الأول (الحفظ السريع للبيانات) نصت عليه المادة 34 من الاتفاقية الأوروبية أعلاه تلتزم بموجبه الدولة المطلوب منها حفظ بيانات المرور المتعلقة بأي بث أو اتصال عبر أجهزة الحاسب التابعة لها، والتي تبين لها أن هذا البث أو الاتصال انتقل من مورد خدمات هذا، ومصدر الاتصال، وكذا المسار الذي تم من خلاله الاتصال.

ولاحق للطرق الموجه إليه هذا الطلب رفض الإفصاح أو الكشف عن البيانات المارة للأسباب نفسها المتعلقة برفض طلب حفظ البيانات المخزنة في جهاز الحاسب وهي

1- أنظر المادة (29 ف1) من الاتفاقية الأوروبية حول الجريمة الإلكترونية لعام 2001، مرجع سابق.
2- أنظر المادة (29 ف 7)، من الاتفاقية نفسها.

عندما ينصب الطلب على جريمة سياسية أو من شأنه الإخلال بسيادة الدولة أو تأمينها أو نظامها العام، أو بمصالحها الأساسية[1].

3- طلب الدخول لغرض التفتيش والضبط والكشف من البيانات المخزنة:

تم النص على هذا الإجراء في المادة (31) من الاتفاقية الأوروبية حول الجريمة الإلكترونية، التي أجازت لأية دولة طرف أن تطلب من دولة طرف أخرى السماح لها بإجراء التفتيش أو الدخول بأنه طريقة مماثلة للكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف، بما في ذلك تلك البيانات المحفوظة وفقا لمادة 29) أعلاه[2].

وقد أوجبت هذه المادة على الدول الأطراف الاستجابة لمثل هذا الطلب بأسرع ما يمكن في الحالات الآتية.

أ- إذا كانت هناك أسباب تدعو للاعتقاد بأن البيانات المعنية معرضة لمخاطر الفقد أو التعديل[3].

ب- إذا كانت الوسائل والاتفاقيات والتشريعات الواردة في الفقرة 2 تستلزم تعاونا سريعا.

أكثر من ذلك فإن المادة (32) من الاتفاقية ذاتها تسمح لأي دولة طرف للولوج للبيانات المخزنة داخل إقليم دولة طرف أخرى دون الحصول على اذن مسبق نم هذه الأخيرة، شرط أن يتم ذلك بموافقة صاحب الجهاز المخزن فيها تلك البيانات أو الذي يتمتع سلطة الإفصاح عنها، أو تكون هذه البيانات متاحة للجمهور.

1- المادة (30) من الاتفاقية الأوروبية حول الجريمة الإلكترونية لعام 2001، مرجع سابق.

2- الفقرة الأولى من المادة (31)، المرجع نفسه.

3- أنظر الفقرة الثالثة من المادة (31)، المرجع نفسه.

4- تبادل المساعدة لجمع البيانات في الوقت الحقيقـــي: (entraide dans la collecte en temps réel de données relative au trafic)

تبين فيما سبق أنه عادة ما يستغرق المحققون وقتا كثيرا في تعقب اتصال الكتروني ما قبل الوصول إلى مصدره، وقد يحدث أثناء هذه الفترة اقدام مورد خدمات على محـــور البيانات المرور المتعلقة بهذا الاتصال قبل التمكن من حفظها، الأمر الـــذي يحـــول دون إمكانية الحصول على هذه البيانات في وقتها الحقيقي.

ولعل هذه المشكلة، وصفت المادة 33 من الاتفاقية الأوروبية المنوع عنـــاه أعـــلاه التزاما على الدول الأطراف بالتعاون بعضها البعض في جميع البيانات المرور المرتبطة لاتصالات الجارية عبر احدى وسائل الاتصال المتواجدة على اقليمها في وقتها الحقيقي.

ويما أن جمع البيانات المرور في وقتها الحقيقي يشكل الوسيلة الأولى لتحديد هوية المجرم الالكتروني، ونظرا لطبيعة هذا الإجراء الذي يقل تطفلا على الخصوصـــية عـــن غيره من إجراءات البحث والتحقيق، فقد أصوت الاتفاقية الدول الأطراف بتقـــديم أوســـع مساعدة ممكنة في هذا الشأن ولو في غياب شرط التجريم المزدوج.

ومن أجل إضفاء الفعالية والحيوية على مختلف صور المساعدة القضائية الدوليـــة السالفة الذكر، ألزمت المادة (35) من الاتفاقية المذكورة كل دولة طـــرف إنشـــاء نقطـــة اتصال وطنية تعمل 24 ساعة طول أيام الأسلوب، تكون مهمتها ضمان توفير المســـاعدة المباشرة والفورية في مجال التحقيقات والمتابعات الجزائية المعلقة بالجرائم الإلكترونيـــة للسلطات القضائية التابعة للدول الأطراف الأخرى[1].

وتجدر الإشارة إلى أن المشرع الجزائري لم ينصف بشكل صـــريح علـــى هـــذه الإجراءات الجديدة للتعاون القضائي الدولي، ولكن يمكن أن نجد لها مكان في تفسير نص

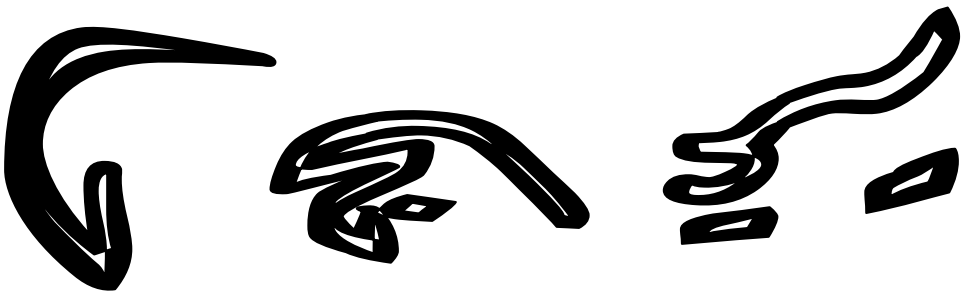
1- نص المادة (39)، من الاتفاقية الأوروبية حول الجريمة الإلكترونية لعام 2001، مرجع سابق.

المادة (16) من القانون (04/09) [1] السالف الذكر، إذ جاءت بصيغة العموم بنصها على أنه «في إطار التحريات أو التحقيقات القضائية لمعاينة الجرائم المشمولة بهـذا القـانون وكشف مرتكبيها، يمكن لسلطات المختصة تبادل المساعدات القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني».

1- المادة 16 من القانون 09-04 المتعلق بالقواعد الخاصة بالوقاية المتصلة بتكنولوجيات الإعلام والاتصال.

ملخص الفصل:

أدى التطور الكبير في عالم تكنولوجيا المعلوماتيـــة وأجهـــزة الاتصـــال واتســـاع استعمال الشبكة الانترنت إلى احتلال مساحة واسعة في الحياة اليومية للمواطنين، لكن في المقابل ساهمت في بروز العديد من الجرائم المتصلة بها، التي أصبحت تشـــكل هاجســـا حقيقيا للكثير من الدول باعتبارها من أخطر الجرائم العابرة للحدود، الأمر الذي يضـــعها إلى العجل على إيجاد حلول سريعة لمكافحتها والحد من انتشارها، سواء من خلال ابـــرام اتفاقيات دولية أو سنن تشريعات وطنية، ولأن افراد قانون خاص للحد ومكافحة الجـــرائم الالكترونية بات اليوم أكثر من ضرورة، حاولت الجزائر استحداث آليات قانونية تســـمح بالحد من انتشار هذه الجرائم، من خلال وضع منظومة قانونية متكاملة ترتكز أساسا على كل من قانوني العقوبات والإجراءات الضرائبية، وتم تـــدعيمها بالقـــانون رقـــم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيـــات الاعـــلام والاتصـــال ومكافحتها.



تبقى الحماية الفنية والتقنية مهما بلغت درجتها عاجزة عن التطور الرهيب الذي تشهده تقنيات اختراق الأجهزة الإلكتروني لاسيما الحواسيب، وهو ما أدى إلى استفحال الجريمة الإلكترونية وتسبب في أضرار مادية ومالية وحتى نفسية للعديد من الضحايا.

تبين لنا من خلال هذه الدارسة مدى خطورة الجرائم الإلكترونية وصعوبة اكتشافها، حيث وقفت مختلف النظم القانونية عاجزة عن مكافحتها، نظرا للعد الهائل من هذه الجرائم المتزايدة بشكل غير مسبوق.

كما أن الجهود الوطنية والدولية لمكافحة الجرائم الإلكترونية لا تزال في بدايتها الأولى، ولا ترق إلى المستوى المطلوب، وأمام هذه الوضعية حاول المشرع الحد من خطورة هذه الجرائم، من خلال ادراجه لتعديلات هامة على قانون العقوبات وقانون الإجراءات الجزائية، وسن القانون رمق 09-04 للوقاية ومكافحة هذه الجريمة.

ومن حيث النتائج المتوصل إليها نجد مايلي:

- تعد الجرائم المتصلة لتكنولوجيات الاعلام والاتصال من الجرائم المستحدثة التي تعتمد التقنية الحديثة والمتطورة لذلك تتطلب مكافحتها الاعتماد على وسائل تقنية لا تقل حداثة عن الرسائل المستعملة في ارتكابها.
- تظهر خطورة الجرائم في كونها جرائم عابرة للحدود وضعية الاكتشاف والآليات، ويصعب فيها تحديد الاخصاص القضائي، نتيجة لكون شبكة الانترنت هي المجال الحيوي لارتكابها.
- ترتكب جرائم تكنولوجيات الإعلام والاتصال في عالم افتراضي غير ملموس ماديا لكن لا وجود حقيقي أهم خصائصه هي أنه غير مقيد بحدود زمنية ومكانية، وهو ما يتطلب ضرورة إعادة النظر في الكثير من القواعد والمسلمات القانونية مثل قواعد الاختصاص القضائي وغيره من المبادئ القانونية.

- رغم المحاولات الجديرة بالاحترام التي قام بها المشرع الجزائري إلا أنها تبقى غير كافية بسبب التطور الكبير في مختلف الأجهزة الالكترونية.

وعلى ضوء هذه المعطيات نطرح ما يراه تحسبا:

- الاسراع في وضع آليات قانونية ردعية للوقاية ومكافحة انتشار الجرائم الالكترونية.
- توفير الامكانات البشرية والمادية والتقنية الحديثة للمراكز والأجهزة المتخصصة في مكافحة الجرائم الإلكترونية.
- باعتبار أن الجرائم الإلكترونية تعد من الجرائم العابرة للحدود يتعين تكثيف التعاون، فهو السبيل الوحيد للحد من امتدادها واستشارها.
- تأهيل عناصر الضبطية القضائية ورجال الأمن المكلفين بعمليات البحث والتحري، حول كيفية التعامل مع الأدلة وضبطها.

نموذج إذن بالتسرب

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة العدل

مجلس قضاء قسنطينة

محكمة قسنطينة

نيابة الجمهورية

رقم:

إذن بالتسرب

- بعد الإطلاع على المواد 65 مكرر 11-12-13-14-15 من قانون الإجراءات الجزائية .
- بعد الإطلاع على التقرير الإخباري الأولي المحرر بتاريخ.....
- بعد الإطلاع على طلب الضبطية القضائية المؤرخ.....
- بعد الإطلاع على طلب إجراءات التحقيق الساري بخصوص قضية.....

لهذه الأسباب

نحن وكيل الجمهورية / قاضي التحقيق لدى محكمة قسنطينة
نأذن بتسرب مفتش أو عون الشرطة
ضمن الشروط المحددة في قانون الإجراءات الجزائية طبقا للمواد المذكورة أعلاه تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية السيد.....
ويبقى هذا الإذن صالح لمدة 04 أشهر قابلة للتجديد عملا بنص المادة 65 مكرر 15 من قانون الإجراءات الجزائية.

حرر بمكتبنا في
وكيل الجمهورية
قاضي التحقيق

بينها قضية استهداف موقع "الشروق أونلاين" وتخريبه من قبل مصريين

فتح تحقيق في 800 اعتداء إلكتروني شنه "هاكرز"

فتحت الجهات القضائية المختصة تحقيقات معمقة في 800 قضية متعلقة بالجريمة الإلكترونية منذ دخول قانون مكافحة الجريمة الإلكترونية حيز التنفيذ السنة المنقضية، حيث تورط في هذه القضايا جزائريون وأجانب استهدفوا شبكات وبنوك المعلومات المركزية لمؤسسات جزائرية ومتعددة الجنسيات.

كشف، أمس، عبد العزيز دردوري رئيس مدير عام مؤسسة الأمن المعلوماتي وأمن شبكات الاتصال على هامش إلقائه محاضرة حول "الأمن المعلوماتي والجريمة الإلكترونية" بمركز الدراسات الإستراتيجية لجريدة "الشعب" بالجزائر العاصمة، عن فتح الجهات القضائية المختصة بالتنسيق مع خبراء المعلوماتية المعتمدين من قبل وزارة العدل تحقيقات معمقة في 800 قضية متعلقة بالهجمات الإلكترونية التي استهدفت شبكات وبنوك معلومات مؤسسات حساسة وكذا تخريب مواقع إلكترونية عن طريق القرصنة الرقمية.

وأوضح صاحب مؤسسة الأمن المعلوماتي وأمن شبكات الاتصال الجزائرية أن العدد الحقيقي للهجمات الإلكترونية التي تتعرض لها المواقع الجزائرية وشبكات وبنوك معلومات المؤسسات الجزائرية غير محدد بدقة لأن الكثير من ضحايا هذه الهجمات لا يصرحون بها أو حتى أنهم لا يتفطنون لعملية القرصنة الإلكترونية واختراق قواعد بياناتهم من قبل الغير، مضيفا أن الحكومة الجزائرية مطالبة بوضع تشريعات وقوانين كافية لحماية مستعملي الأنترنيت وأصحاب المواقع الإلكترونية وبنوك المعلومات وشبكات الاتصال من الاختراق والقرصنة، فضلا عن تكثيف دورات التوعية والتكوين لرفع مستوى الوعي والمعرفة الرقمية.

وذكر المتحدث أن الجريمة الإلكترونية والقرصنة الرقمية كبدت العالم خلال سنة 2008 خسائر مالية تجاوزت 100 مليار دولار، مشيرا إلى أن كل من الولايات المتحدة الأمريكية وروسيا والصين تعتبر الدول الأكثر خطورة في مجال تهديد أمن المعلومات، في حين تمثل كل من نيجريا وغانا وجنوب إفريقيا والكاميرون الدول الأخطر في الجريمة الإلكترونية على مستوى القارة الإفريقية ما يستدعي على الجزائر تعزيز أمنها المعلوماتي من خلال خطة حكومية تؤمن مختلف المؤسسات والهيئات خاصة في ظل تحضير الجزائر لإطلاق مشروع الحكومة والتجارة الإلكترونية .

كما أثارت قضية اختراق موقع "الشروق أونلاين" ومحاولة الاستيلاء عليه وتخريبه من قبل جهات مصرية نقاشا واسعا على هامش الندوة باعتبارها أكبر قضية مست الأمن المعلوماتي لمؤسسة جزائرية، حيث تعرض موقع "الشروق أونلاين" أكبر موقع إلكتروني جزائري من حيث عدد الزيارات والمشاهدة شهر مارس المنقضي إلى هجمة الكترونية مصرية تم فيها الاستيلاء على اسم النطاق ومرر القراصنة المصريون رسائل عبر الموقع قبل أن تسترجعه مؤسسة "الشروق" للإعلام والنشر بعد تكثيف الاتصالات مع المؤسسة الأمريكية المكلفة بإيواء الموقع ورفع شكوى للسلطات الجزائرية قصد التحقيق في حيثيات القضية.

● زين العابدين جبارة

القذف والتشهير عن طريق منظومة معلوماتية (فايسبوك)

تعود الوقائع إلى تعرض المدعو/ س للقذف والتشهير عن طريق منظومة معلوماتية من قبل مجهول فإن الوقائع تعود الى منذ حوالي 15 يوما، أين ورده طلب الصداقة عبر موقع التواصل الاجتماعي فيسبوك من صاحب العلبة الالكترونية الحاملة للاسم المستعار **bbbbbbbbb** مرفقة برسالة نصية تتضمن عبارات مشينة لشخصه غير أنه مسحها، وبعد حوالي يومين تقريبا قام المعني بالأمر بنشر صور الضحية ضمن الإعلانات بعلبة لإلكترونيه فيسبوك لهذا الاخير مع إرفاقها بعبارات القذف لشخصه، مضيفا أن المشتكي منه قام بأخذ الصور التي قام بنشرها من علبته الإلكترونية (الصور الشخصية) ثم نشرها بالموقع (فيسبوك) دون علمه أو رضاه، وكذلك نشر نفس الصور مكتوب عليها عبارات فاضحة بالحي الذي يقيم فيه.

الإجراءات المتبعة: وفق قانون الإجراءات الجزائية قبل صدور القانون 04/09 وإنشاء فرق مكافحة الجرائم المعلوماتية .

- ترسيم شكوى الضحية وإخطار وكيل الجمهورية، مع قيام الشاكي بمعاينة الجريمة وإحضار نسخ من صفحة الإعلانات التي تم فيها نشر الصور وأفعال القذف .
- قيام الشاكي بإحضار الرابط أو رقم هاتف المشتبه فيه، بعدها تم تكليف المتعامل أوريدو في تحديد صاحب الشريحة 0555.....من أجل تحديد هوية المشتبه فيه، أو تسخير وكالات الاتصالات الجزائر من اجل تحديد مستخدم الرابط واسم الجاهز الذي يستخدمه المشتبه فيه.
- رد وكالة أوريدو أو اتصالات الجزائر ايجابي بتحديد الهوية الكاملة للمشتبه فيه ونوعية الجهاز المستعمل.
- طلب الإذن من وكيل الجمهورية من أجل تفتيش مسكن المشتبه فيه للحصول على الجهاز بعد الحصول على الإذن بالتفتيش، تم الانتقال إلى مسكن المشتبه فيه للقيام بالتفتيش.
- حجز الوحدة المركزية لجهاز الإعلام الآلي، وكذلك صور الضحية التي تم ضبطها بمنزل المشتبه فيه، توقيف المشتبه فيه وسماعه على محضر، تقديم الأطراف .

ملف الإجراءات :

- محضر شكوى (01)، محضر سماع (01)، استمارة معلومات (01)، صور فوتوغرافية مأخوذة من الفيسبوك (04)، شهادة ميلاد (01)، تكليف شخصي ورد وكالة أوريدو (01) محضر تفتيش وحجز(01)، تقرير مصور (01).

انتهاك حرمه الحيات الخاصة عن طريق خرق منظومة معلوماتية

تعود الوقائع إلى تعرض المسماة / ح ل إلى اختراق موقعها المعلوماتي فايسبوك وكذلك SKYPE من قبل المدعو/ Zohir باسم مستعار الذي طلب منها الصداقة، وبمجرد قبول صداقته سيطر على علبتها الالكترونية، وفي محاولة منها للدخول عبر السكايب وجدت نفس الشخص يطلب منها الصداقة، وبنفس الفعلة تم السيطرة على SKYPE، حيث قام بالتقاط صور للضحية وهي شبه عارية دون علمها أو رضاها، بعدها قامت الضحية بفتح علبة فايسبوك أخرى لتفاجئ بوجود صورها على موقع التواصل الاجتماعي والتي التقطها الفاعل.

الإجراءات المتبعة بخصوص المعاينات والتفتيش والحجز بموجب قانون الإجراءات الجزائية وكذا القانون 04/09 الخاص للوقاية من الجرائم المتصلة بتكنلوجيات الإعلام والاتصال ومكافحتها

-ترسيم شكوى الضحية وإخطار وكيل الجمهورية.

-البحث عن صاحب الاسم المستعار / Zohir وتحديد الرابط الخاص به من اجل معرفة معلومته الشخصية ومراقبة أماكن اتصاله والوسيلة المستعملة في التواصل عبر موقع التواصل الاجتماعي .

-بعد تكليف مصالح اتصالات الجزائر (قطب جواب) تم موافاتنا بهوية المشترك الذي استعمل من خلاله ذلك العنوان و يتعلق الأمر بالمدعو /----------

-بالوصول إلى المعلومات حول الشخص والجهاز المستعمل.

-طلب الإذن بتمديد الاختصاص.

- طلب الإذن من وكيل الجمهورية بتفتيش مسكن المشتبه فيه للبحث عن الأجهزة المستعملة.
- انتقلنا إلى مقر السكن موضوع الإذن بالتفتيش الكائن ---------- العملية التي كانت إيجابية.
- إجراء عملية معاينة تقليدية حيث تم حجز الوحدة المركزية لجهاز الإعلام الآلي تحمل علامة Emachines، بعد طلب الإذن بإخضاع الوحدة المركزية للتفتيش إلكتروني، تم تفتيش المعطيات ومعاينة داخل الذاكرة المنطقية للوحدة المركزية.
- حجز المعطيات في قرص صلب يحتوي على المجلد الذي يحتوي على جميع المعلومات والصور المذكورة في المحضر.
- طلب مراقبة إلكترونية للإيميلات المشتبه فيه، بعدها تم تقديم الأطراف .
- ملف الإجراءات يتكون من: محضر شكوى (01)، محضر سماع(01)، استمارة معلومات (01)، رد وكالة اتصالات الجزائر (01)، شهادة ميلاد (01)، محضر تفتيش وحجز تقني (01)، محضر مراقبة تقني(01)، محضر تحريات تقني (01)، كما تم حجز الوحدة المركزية من نوع Emachines

نموذج عن محضر تفتيش تقني حول قضية المساس بحرمة الحياة الخاصة عن طريق منظومة معلوماتية

محضر تفتيش وحجز إلكتروني

قضية :

الموضوع:

-/ **انه في يوم**: الإثنين الموافق للثاني عشر من شهر جانفي----------

-/ **من سنة**: ألفين وخمسة عشر(2015).-------/**الساعة**: الثامنة صباحا. ----------

-/ **نحن**: ملازم أول للشرطة ----------، بمديرية الشرطة القضائية. ----------

-/ **ضابط الشرطة القضائية** بدائرة الاختصاص بمساعدة..... بفرقة مكافحة الجرائم المعلوماتية ----------

-/في إطار التحقيق المفتوح في قضية المساس بحرمة الحياة الخاصة التي راحت ضحيتها المدعوة/ .....

-/بناءا على نص المادة 05 من قانون رقم 04/09/ المؤرخ في 2009/08/05 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال، وبناءا على الأمر بتمديد الاختصاص والإذن بالتفتيش المنظومة المعلوماتية الحاملين للرقم 14/000615 بتاريخ 2015/01/05 الصادرين عن السيد/ وكيل الجمهورية لدى محكمة الحراش، الناص على تمديد الاختصاص إلى محكمة عين تموشنت، المؤشر عليه من طرف السيد/ وكيل الجمهورية لدى نفس المحكمة بتاريخ 2015/01/07، و الإذن بالتفتيش الناص على تفتيش مسكن المدعوة/ ف ق، نقول أننا بتاريخ 2015/01/07 انتقلنا إلى مقر السكن موضوع الإذن بالتفتيش الكائن..... العملية التي كانت إيجابية و تم من خلالها حجز الوحدة المركزية لجهاز الإعلام الآلي التي تحمل علامة Emachines، ملك المشتبه فيه المدعو/ ...../----------

-/ أنه بتاريخ اليوم و الساعة المشار إليهما أعلاه إجراء عملية معاينة و تفتيش إلكتروني.

-/ يتبين من خلال فحص الجهاز أن المشتبه به قام بحذف نظام التشغيل السابق وتثبيت نضام WINDOWS 7 جديد بتاريخ 2014/11/18 (صورة01)----------

صورة خاصة بالضحية

صورة01

-/في الوهلة الأولى قمنا بمعاينة متصفح الأنترنات « Google Chrome » المثبت على جهاز الكمبيوتر الخاص بالمشتبه فيه، أين عثرنا على عنوان البريد الإلكتروني «---------- » (صورة02)، المستعمل في إنشاء حساب الفيسبوك « -----Ka » الذي قام من خلاله بالاتصال بالضحية بعد قرصنة جهازها، مع العلم أنه قام بتغيير إسم حسابه من إسم « ----- إلى « o----- »

-/عملية تفتيش الأقراص الصلبة بينت أن عملية الولوج إليها محمية بكلمة سر ----------

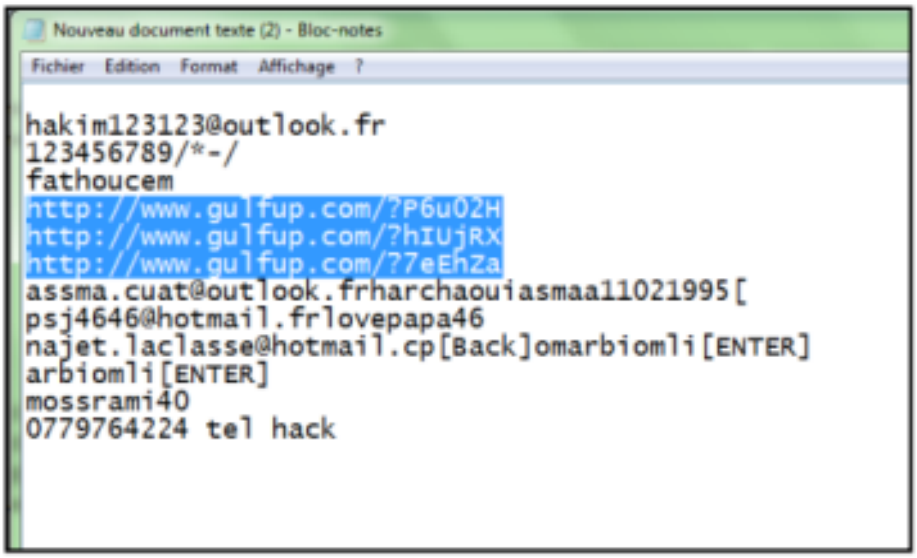
/ تفتيش القرص الصلب C لم يسفر عن أي نتيجة تتعلق بالقضية محل التحقيق، كما أنه لا يوجد أي برنامج يستعمل في القرصنة مثبت على الجهاز بعد تاريخ حذف نظام تشغيل الجهاز المذكور أعلاه----------

-/ تفتيش القرص الصلب D لم يسفر عن أي نتيجة تتعلق بالقضية محل التحقيق مع وجود بعض البرامج التي قد تستعمل في عمليات القرصنة----------

-/تفتيش القرص الصلب الأخير E بين مايلي:----------

-/ وجود ملف باسم Nouveau document texte(2).txt يحوي ثلاثة (3) روابط على موقع www.golfup.com حيث قام المشتبه فيه بوضع الفيروس يقوم الضحايا بتحميله على أساس أنه ملف أخر (صورة03) ----------

صورة 02



صورة 03

جنسي sexy.love.exe (صورة04) ----------

صورة 04

-/الرابط الثاني http://www.gulfup.com/?hIUjRX يقود إلى تحميل الفيروس على أساس أنه برنامج تسلية funny.appll.exe (صورة05) ----------

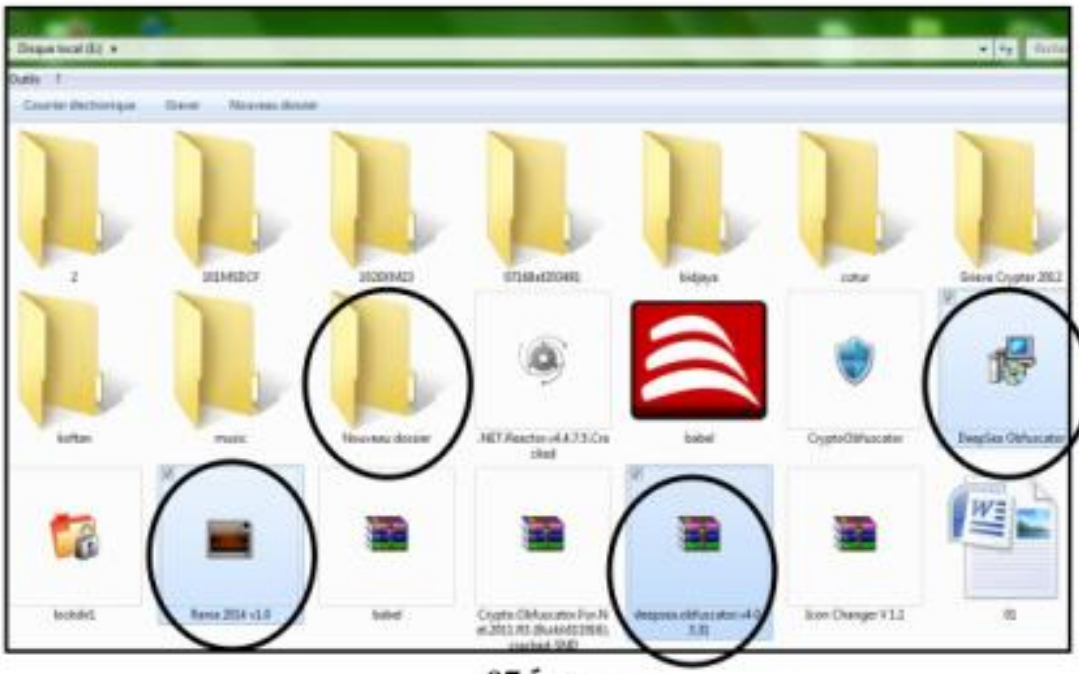
صورة05

صورة06

-/الرابط الثالث http://www.gulfup.com/?7eEhZa يقود إلى تحميل الفيروس على أساس أنه برنامج انترنت nat.exe (صورة06) ----------

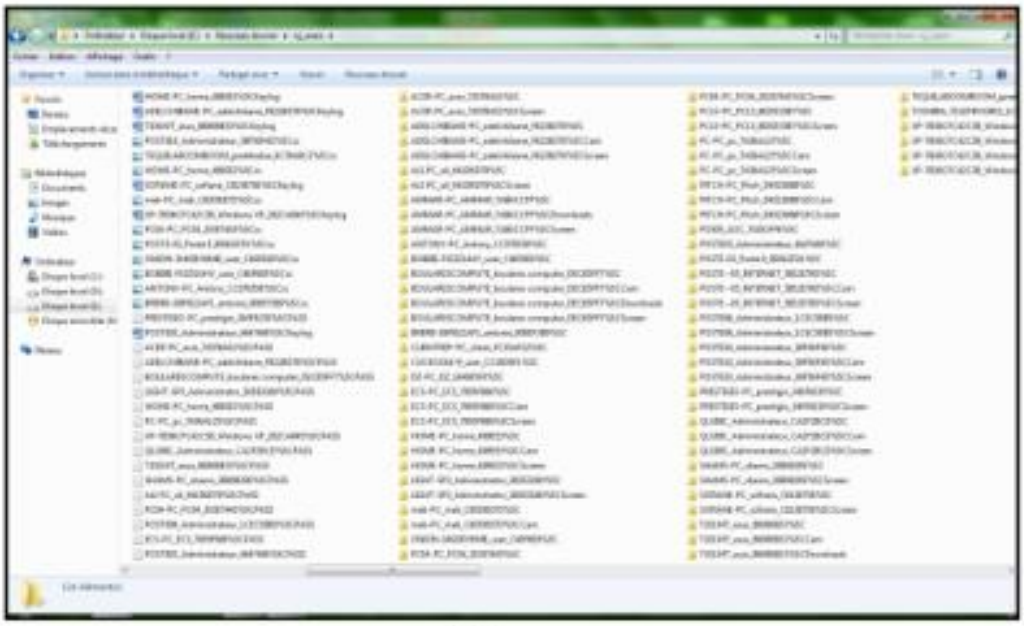
-/ وجود البرنامجين Rania 2014 v1.0 و DeepSea Obfuscator المستعملين في تشفير الفيروس من طرف المشتبه فيه لكي لا تتعرف عليه برامج الحماية (صورة07) ----------

-/وجود ملف مسمى Nouveau dossier يحتوي ملفات (صورة07) خلقها برنامج Nijrat الذي يقوم بتحضير الفيروسات-



صورة 07

-/داخل المجلد nj_users الموجود داخل المجلدNouveau dossier يوجد العديد من الملفات والمجلدات التي قام الفيروس بإرسالها للمشتبه فيه من أجهزة الكمبيوتر الخاصة بالضحايا



صورة 08

-/ من ضمن هذه الملفات توجد ملفات word تنتهي جميعها بكلمة keylog قام برنامج keyloger بإنشائها (برنامج يقوم بإرسال ما يكتب الضحية على لوحة المفاتيح)، من بين هذه الملفات يوجد ملف باسم QLUBIC_Administrateur_CA2FBCD%5Ckeylog خاص بالقضية محل التحقيق يحتوي على ما كتبته الضحية خلال استعمالها للجهاز (صورة09) ----------

-/كما يوجد ملفات بصيغة TXT تنتهي جميعها بكلمة PASS تحتوي على اسم المستخدم وكلمات المرور لمختلف الحسابات الخاصة بالضحايا، من بين هذه الملفات يوجد ملف باسم QLUBIC_Administrateur_CA2FBCD%5CPASS خاص بالقضية محل التحقيق يحتوي على حسابات الشاكية (صورة09)، كما توجد مجلدات كل مجلد خاص بضحية تحتوي على صور قام المشتبه فيه بأخذها أو تصويرها من أجهزة الضحايا، من بين هذه المجلدات يوجد ثلاث (03) مجلدات خاصة بالقضية محل التحقيق (صورة09) ----------

صورة09

-/ المجلد الأول باسم QLUBIC_Administrateur_CA2FBCD%5C لا يحتوي على أي ملف ----

-/ المجلد الثاني باسم QLUBIC_Administrateur_CA2FBCD%5CCam يحتوي على ثمانية عشر(18) صورة قام المشتبه فيه بتصويرها عند تمكنه من فتح كميرا جهاز الكمبيوتر الخاص بالشاكية هذه الصور خاصة بالشاكية المدعوة/ ح ل و ابنة أخيها المدعوة/ ------- وهي كالتالي: الصور الخاصة بالشاكية المدعوة/ --------/الصور الخاصة بالمدعوة/ ----------:

-/ المجلد الثالث باسم QLUBIC_Administrateur_CA2FBCD%5CScreen يحتوي على أربعة عشر (14) صورة قام المشتبه فيه بتصويره لسطح المكتب تظهر فيها الشاكية المدعوة/ ح ل أثناء محادثة شخصية في برنامج SKYPE بينها و بين حساب يسمى « Zohir » خاص برجل كما هو مبين بالصور أسفلها،كما يوجد خمسة (05) مجلدات أخرى تحتوي على صور لأشخاص تم اختراق أجهزة الكمبيوتر الخاصة بهم من طرف المشتبه فيه، هذه المجلدات موجودة بالقرص المضغوط المرفق وتسمى على التوالي:
/المجلد الأول « BOULARESCOMPUTE_boulares computer_DEC85FF7%5CDownloads» ---------
/المجلد الثاني « ECS-PC_ECS_7095F088%5CScreen »----------
-/المجلد الثالث « PITCH-PC_Pitch_D4515688%5CScreen »----------
-/المجلد الرابع « POSTE--05_INTERNET_5852E79D%5CScreen »----------
-/ المجلد الخامس « XP-7B36CFC42C3B_Windows XP_282CA04E%5CDownloads » -------
-/نرفق لكم مع هذا المحضر قرص صلب يحتوي على المجلد الذي يحتوي على جميع المعلومات والصور المذكورة في المحضر. ----------
-/أثناء عملية التفتيش الإلكتروني استعملنا برتوكول الأنترنت التالي.....
-/عاينا بأن المدعو/++++++++ قام بالولوج للإيميل محل التفتيش الإلكتروني بتاريخ 2013/12/23، مستعملا برتوكول الأنترنت 41.103.239.124 و41.109.229.247، أنظر صورة رقم 10-11---/

صورة رقم 10

صورة رقم 11

-/قمنا بتفتيش الحساب الإلكتروني الحامل للاسم المستعار aaaaaa.sec والمربوط بالإيميل aaaaaaaaaaaa@gmail.com (صورة 12)----------

صورة 12

-عاينا بأن الحساب الإلكتروني محل التفتيش مربوط بالإيميل aaaaaaa@gmail.com، أنظر صورة رقم 13.

صورة رقم 13

-/ كما أننا أثناء معاينة الصفحة المجرمة الحاملة للاسم المستعار " أسرار المجلس الشعبي الوطني" عاينا بأن الحساب الإلكتروني الحامل للإسم المستعار " aaaaaa.sec " يعتبر عضو مؤسس ومسير الصفحة (الصورة رقم 14)---- ----------/

صورة رقم 14

-/تمت عملية التفتيش و المراقبة الإلكترونية في ظروف حسنة دون تسجيل أي شيء يستحق الذكر.------

-/ لما سبق ذكره حرر هذا المحضر في يومه و ساعته ووقعناه رفقة المعني بالأمر و مساعدينا.--------

المعني بالأمر **المساعدين** **ضابط الشرطة القضائية**

قائمة المصادر والمراجع

قائمة المصادر:

أولا: القوانين

أ- التشريع الأساسي:

1- الدستور الجزائري 1996 الصادر بموجب المرسوم الرئاسي رقم 96-438 المؤرخ في 07 سبتمبر 1996 المتضمن دستور الجزائري، جمهورية جزائرية جريدة رسمية، عدد 76-08 ديسمبر 1996، المعدل والمتمم بموجب القانون رقم 16-01 المؤرخ في 16- مارس، المتضمن التعديل الدستوري جمهورية جزائرية جريدة رسمية – عدد 14 صادر في 07 مارس 2016.

ب- الاتفاقيات الدولية:

1- اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، رقم (63-55) صادرة عن هيئة الأمم المتحدة بالجمعية العامة 18-19 ديسمبر 2000، المصادق عليها بموجب المرسوم الرئاسي رقم 14-252 الموافق لـ: 08 سبتمبر 2014، المحرر بالقاهرة في 21 ديسمبر 2010، جريدة رسمية، عدد 57. متاحة على الموقع الإلكتروني:

- F.PDFhttp://WWW.UNODC.ORG./PDF/CRIME /ARES 56/121

2- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، متاحة على الموقع الإلكتروني التالي: WWW.ARAB LEGAIMET.ORG

3- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية باليرمو عام 2000، متوفرة في الموقع التالي:

ttp://www.uncjm.org/documentconvartion/dcotac/final.document-2/convontion-french

4- اتفاقية تسليم المجرم بين الجزائر وبريطانيا، مؤرخة في 11 جوان 2006، جمهورية جزائرية، الجريدة الرسمية، عدد 81ن صادر في 13 ديسمبر 2006.

5- اتفاقية مستراخيت على الموقع التالي:

http// :Fr.wikipidia.org/wiki/trait/c31.Agda.mastricht

- المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين بتاريخ 10-17 أفريل 2000 متاح على الموقع:

http://oie.gov/sy/ind

ج- القوانين العادية:

1- القانون رقم 55-156 المتضمن قانون العقوبات المعدل والمتمم بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، جمهورية جزائرية، جريدة رسمية، عدد 84.

2- القانون رقم 03/2000 المؤرخ في 05 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، جمهورية جزائرية، جريدة رسمية، العدد 98، صادر بتاريخ 06 أوت 2000.

3- القانون رقم: 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر 66-155 المتضمن قانون العقوبات، جمهورية جزائرية جريدة رسمية، عدد 71، صادر في 10 نوفمبر 2004.

4- القانون رقم 14-04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66-156 المتضمن قانون الإجراءات الجزائية، جمهورية جزائرية، جريدة رسمية، عدد 71، الصادر في 10- نوفمبر 2004.

5- القانون رقم 06-01 المؤرخ في 20 جوان 2006 المتضمن قانون الوقاية من الفساد ومكافحته، جمهورية جزائرية، جريدة رسمية، عدد 14، صادرة في 08 مارس 2006 المعدل والمتمم.

6- القانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، جمهورية جزائرية جريدة رسمية، عدد 84، صادرة في تاريخ: 24 ديسمبر 2006.

7- القانون رقم 08-02 المؤرخ في 25 يناير 2008، المتم للأمر رقم 83/ المؤرخ في 02 يوليو 1983، المتعلق بالتأمينات الاجتماعية، جمهورية جزائرية، جريدة رسمية، العدد 04، الصادر في 27 يناير 2008.

8- القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ: 05 أوت سنة 2009 والمتضمن القواعد الخاصة بالوقاية المتصلة لتكنولوجيات الإعلام والاتصال ومكافحتها، جمهورية جزائرية جريدة رسمية، العدد 47، صادرة بتاريخ 16 أوت 2009.

9- القانون رقم 11-15 المرخ في 02 أوت 2011، يعدل ويتم القانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته، جمهورية جزائرية جريدة رسمية، عدد 44، الصادرة في 10 أوت 2010.

10- القانون رقم 17-07 المؤرخ في 27 مارس 2017، المعدل والتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، جمهورية جزائرية، جريدة رسمية، عدد 20، صادرة في 29 مارس 2017.

الأوامر:

1- الأمر رقم: 03/07 المؤرخ في 19 جويلية 2003 المتعلق براءة الاختراع، جريدة رسمية، عدد44.

2- الأمر رقم 05/09 الصادر بتاريخ 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، المعدل والمتمم للأمر 14/73، جمهورية جزائرية جريدة رسمية، العدد الرابع.

3- الأمر رقم 75-58 المؤرخ في 1975/09/26 المتضمن القانون المدني الجزائري. جمهورية جزائرية، جريدة رسمية، عدد 78، الصادرة في 30 سبتمبر 1975.

المراسيم:

1- المرسوم 06-348 المؤرخ في 05 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، جمهورية جزائرية، جريدة رسمية، عدد 63.

2- المرسوم الرئاسي رقم 261-15 مؤرخ في 24 ذي الحجة عام 1436 الموافق لـ 8 أكتوبر سنة 2015 تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة لتكنولوجيات الإعلام والاتصال ومكافحتها الجمهورية الجزائرية جريدة رسمية، عدد 53.

المؤلفات:

أ- المؤلفات العامة:

1-أحسن بوسقيعة، التحقيق القضائي، د ط، دار هومة الجزائر، 2010.

2-أحسن بوسقيعة، الوجيز في القانون الخاص، الجزء الأول، الطبعة 17 ، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2004.

3-عبد القادر شيخ، شرح قانون العقوبات، القسم الخاص، الجزء الثاني، د ط، منشورات جامعية حلب، سوريا، 2006.

4-عمر خوري، شرح قانون العقوبات، القيم العام، د ط، ديوان المطبوعات الجامعية، الجزائر، 2007-2008.

5-لحسن بن شيخ آث ملويا، المنتقى في القضاء العقابي، ط 1، دار الخلدونية، الجزائر، 2008.

6-محمد نجيب حسين، الموجز في شرح قانون العقوبات، القسم الخاص، د ط، دار النهضة العربية، القاهرة، 2003.

7-محمد نجيب حسين، شرح قانون العقوبات القسم العام، ط 5، دار النهضة العربية، مصر 1982.

8-نبيل صقر، الوسيط في جرائم الأشخاص، د ط، دار الهدى، عين مليلة، الجزائر، 2009.

المؤلفات الخاصة:

1-أحمد خليفة الملط، الجرائم المعلوماتية، ط 2، دار الفكر الجامعي، الاسكندرية، مصر، 2006.

2-أشرف شمس الدين الحماية الجنائية للمستند الإلكتروني، د ط، دار النهضة العربية، القاهرة، 2006 (للمزيد من التفصيل أنظر قسيمة محمد، خضيري حمزة، مكافحة

الجرائم الماسة بنظام لمعالجة الآلية للمعلومات في قانون العقوبات الجزائري، مجلة صوت القانون، مجلد 7، العدد 2، نوفمبر 2002).

3-بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري وفقا لأحكام قانون حقوق المؤلف الجديد، الأمر رقم 06-05، ط 1، دار الخلدونية الجزائر، 2007.

4-جعفر حسن حاسم الطائي، جرائم تكنولوجيا المعلومات، د ط، دار البلدية، عمان، 2010.

5-جميل حسين طويلة التحليل الجنائي الرقمي، د ط، مكتبة النور، د س ن،سوريا.

6-حسين بن سعيد الغافري، السياسة الجنائية في مواجهة مراسم الانترنت، د ط، دار النهضة العربية، القاهرة، 2009.

7-خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، (د.ط)، دار الثقافة للنشر والتوزيع، عمان، 2011.

8-خالد محمد وإبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية 2008.

9-خيثر مسعود، الحماية الجنائية لبرامج الكمبيوتر، (د.ط)، دار الهدى، عين مليلة، الجزائر، 2010.

10-رشيد بوبكر، جرائم الاعتداء على نظم المعالجة الآلية، ط01، منشورات الحلبي الحقوقية، بيروت، 2012.

11-زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، (د.ط)، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011.

12-سليمان بن عبد الله بن سليمان العجلان، حق الإنسان في جريمة مراسلاته واتصالاته الهاتفية الخاصة في النظام الجنائي السعودي، دراسة تطبيقية مقارنة، (د.ط)، الرياض، 2005.

13-الشواء ساسي، ثورة المعلومات وانعكاساتها قانون العقوبات، ط01، دار النهضة العربية، القاهرة، (د.س.ن).

14-شيماء عبد الغاني، محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، (د.ط)، دار الجامعة الجديدة، الإسكندرية، 2007.

15-ضياء مصطفى عثمان، السرقة الإلكترونية (دراسة فقهية)، ط01، دار النفائس للنشر والتوزيع، عمان، 2011.

16-عادل الديربي، محمد صادق، الجرائم الإلكترونية (دراسة مقارنة)، ط 1، المركز القومي للاصدارات القانونية، القاهرة، 2012.

17-عامر إبراهيم قندلجي، علاء الدين عبد القادر الجنابي، نظم المعلومات الإدارية وتكنولوجيا المعلومات، ط08، دار المسيرة للنشر والتوزيع والطباعة، جمال أحمد محمد خلف وإخوانه، عمان، الأردن، 2014.

18-عائشة بن قارة مصطفى، حجة الدليل الإلكتروني في مجال الإثبات الجنائي، (د.ط)، دار الجامعة الجديدة، الإسكندرية.

19-عبد الرحيم الشيحاني، شيماء إسحاق، المسؤولية الجزائية عن جريمتي السب والقذف بالوسائل الإلكترونية طبقا للمرسوم (05) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، 2018.

20-عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، (د.ط)، دار الفكر الجامعي، الإسكندرية، 2002.

21-على عبد القادر القهوجي الحماية الجنائية لبرامج الكمبيوتر، د ط، المكتبة القانونية، القاهرة، 1999.

22-عمر أبو الفتوح عبد العظيم (الهمامي)، الحماية الجنائية للمعلومات المسجلة الكترونيا -دراسة مقارنة- د ط، دار النهضة العربية، القاهرة، 2010.

23-ماجد ياقوت، أصول التحقيق، دراسة مقارنة، ط03، منشأة المعارف، الإسكندرية، (د.س.ن).

24-محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، (د.ط)، دار الجامعة الجديدة، 2007.

25-محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، ط01، دار الحامد للنشر والتوزيع، عمان، 2007.

26-مفتاح محمد دياب، معجم المصطلحات وتكنولوجيات المعلومات والاتصالات، (د.ط)، الدار الدولية، القاهرة، 1995.

27-ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، (د.ط)، دار الكتاب القانونية، مصر، 2006.

28-نائلة عال محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، (د.ط)، منشورات الحلبي الحقوقية، بيروت، 2005.

29-نبيل صقر، جرائم الكمبيوتر والأنترنت، موسوعة الفكر القانوني، (د.ط)، دار الهلال للخدمات الإعلانية، الجزائر، 2015.

30-نهلا عبد القادر المومني، الجرائم المعلوماتية، ط02، دار الثقافة للنشر والتوزيع، الأردن، 2010.

31-يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والأنترنت، ط01، دار العدالة، القاهرة، 2017.

32-يوسف حسن يوسف، الجرائم الدولية للأنترنت، ط01، المركز القومي للإصدارات القانونية، القاهرة، 2011.

الرسائل والمذكرات الجامعية:

أ- رسائل الدكتوراه:

1-بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي الداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص: قانون عام، كلية الحقوق، جامعة الجزائر01، بن يوسف بن خدة، 2017-2018.

2-براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018.

3-عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، رسالة دكتوراه، جامعة عين شمس، 2004.

ب- رسائل الماجستير:

1-أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم (09-04، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، قسم الحقوق تخصص قانون جنائي، 2013-2014.

2-أمال قارة، الجريمة المعلوماتية، رسالة لنيل درجة ماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، الجزائر، 2001، على الموقع التالي: socio.yoo7.comt2964-topic.

3-حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص: علم الإجرام والعقاب، كلية الحقوق والعلوم السياسية، باتنة، 2011-2012.

4-سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص: علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2013.

5-سيدي محمد البشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية، دراسة تحليلية تطبيقية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010.

6-صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير، تخصص القانون الدولي للأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.

7-فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011-2012.

8-لحمر فافة، إجراءات تسليم المجرمين في الجزائر على ضوء الاتفاقيات الدولية، مذكرة لنيل شهادة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة وهران، 2013.

9-محمد مزوالي، نطاق المسؤولية الجنائية لمسيري المؤسسات الاقتصادية في القانون الجزائري (دراسة مقارنة)، رسالة ماجستير، المركز الجامعي، الجزائر، 2006.

المقالات العلمية:

10-ابتسام مناع، جريمة الاعتداء الإلكتروني على الحياة الخاصة في التشريع الجزائري، مجلة الشريعة والاقتصاد، مجلد 80، إصدار الأول، 2019.

11-أمحمد بوزينة آمنة، الحماية الجنائية للمعطيات الإلكترونية في إطار القانون الجزائري، مذكرة تحليلية لقانوني العقوبات وحقوق المؤلف، مجلة سيليوفيليا للدراسات المكتبات والمعلومات، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، العدد الخامس، 026617781 155 m، مارس 2020.

12-أيمن عبد الحفيظ، حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مركز البحوث الشرطة، القاهرة، العدد الأول، جانفي 2004، على الموقع الإلكتروني: http://www.europol.eu.int : Europol sur.

13-ثابت دنيا زاد، مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، جامعة العربي التبسي-تبسة، العدد السادس، 2016.

14-حازم العارون، الإنابة القضائية الدولية، المجلة الجنائية القومية، القاهرة، العدد الثاني، 1988.

15-ربيعي حسين، المراقبة الإلكترونية وحق الفرد في الخصوصية داخل القضاء الرقمي، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، المجلد 13، العدد الأول، 2016.

16-صحراوي مصطفى، الحماية الفنية والجزائية للتوقيع الإلكتروني على ضوء القانون 15-04 المتعلق بالتوقيع والتصديق الإلكتروني، مجلة البحوث في الحقوق والعلوم السياسية، مجلد 04، عدد01، ديسمبر، 2018.

17-عباوي نجاة، الإشكاليات القانونية في تجريم الاعتداء على أنظمة المعلومات، دفاتر السياسة والقانون، جامعة محمد الطاهري، بشار، الجزائر، العدد 15، 2010.

18-محمد سليمان مصطفى، جرائم الحاسوب وأساليب مواجهتها، مجلة الآنى والحياة، العدد 199، 1999.

19-مصطفاوي عبد القادر، أساليب البحث والتحري الخاصة وإجراءاتها، مجلة المحكمة العليا، العدد الثاني، 2009.

الجرائد:

1-جريدة الخبر اليومية، العدد الصادر في 21-07-2010.

2-جريدة الشروق، العدد الصادر في 26-05-2010.

3-جريدة الرياض اليومية الصادرة بتاريخ: 07-08-2017، على الموقع:

http://www.alriyath.com/mo9557

4-الأنتربول على الموقع:

http://www.interpol.int/pulic/cop/defanlt.asp

المداخلات:

1-أمال بن صويلح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، خطوة هامة نحو مكافحة الإرهاب الإلكتروني بالجزائر، مداخلة الملتقى الدولي

حول الإجرام السيراني المفاهيم والتحـــديات، 11-12 أفريـــل 2017، عبـــر الموقـــع: **Fszcg.univ-guelma.dz**

ورقة بحثية:

1-عبد الرحمن حملاوي، دور المديرية العامة للأمن الـــوطني فـــي مكافحـــة الجريمـــة الإلكترونية، ورقة بحثية مقدمة للأعمال الملتقى الوطني حول الوقاية والمكافحـــة يـــومي: 16-17 نوفمبر 2015، كلية الحقوق وجامعة بسكرة، الجزائر.

2-أيمن عبد الحفيظ، حدود مشروعية دور أجهزة الشرطة في مواجهة جرائم المعلوماتية، مجلة مركز البحوث الشرطة، عدد01،

Europol sur : http://www.europol-eu.int

3-فشار عطا الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقـــدم إلـــى الملتقى المغاربي حول القانون والمعلوماتية المزمع عقده بأكاديمية الدراسات العليا، ليبيا، أكتوبر، 2009.

4-يونس عرب، جرائم الكمبيوتر، بحث مقدم إلى المؤتمر الأمن العربي تنظـــيم المركـــز العربي للدراسات والبحوث الجنائية، أبو ظبي، 2002

فهرس المحتويات

ملخص:

الإجرام الإلكتروني واحد من أخطر الظواهر الإجرامية المستحدثة، في المجتمع الجزائري كما في المجتمعات الأخرى، حيث شهدت الألفية الأخيرة ثورة تكنولوجية استغلها الأشراف كما الأشرار في تحقيق دوافع مشينة أحسنها الشغف بالتقنية وأسوءها الربع المادي، لهذا كان لزاما على المشرع الجزائري التدخل عبر عديد النصوص القانونية الموضوعة والإجرائية لمواجهة الجريمة والمجرم المعلوماتي.

الكلمات المفتاحية: الجريمة والإجرام السيراني – الإلكتروني – المجرم المعلوماتي – الأقطاب – الهيئة المستقلة للرقابة من جرائم تكنولوجيا الإعلام.

Aastract:

Électronicien criminality is one of most serious criminal phenomena created in Algerian society as in other societies. The last millennium Witnessed a technological revolution that was exploited by superviors as the bad guys to achieve deplorable mottives, the best of wich is the passion for technology and the worst of material profit. Thus, the Algerian legislator had to in tervene throngh mamy sulstantive and procedural texts to confront the crime and informationcriminal.

Kev Words :crime- eléctromic - crimimal-police-cyber Crminal-Independent Commission for the prevention of conputer Crime.