جامعة ابن خلدون– تيارت
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر
في الحقوق
التخصص: قانون جنائي
بعنوان:

إجراءات البحث والتحري في جريمة الأنترنت

إعداد الطلبة:
* سافر جهيدة
* زوكل عابد إسماعيل

تحت إشراف:
* أ/د.هروال نبيلة هبة

لجنة المناقشة		
د. جلجال محفوظ	أستاذ محاضر (أ)	رئيسا
أ/د. هروال نبيلة هبة	أستاذة التعليم العالي	مشرفا ومقررا
د. طفياني مخطارية	أستاذة محاضرة (أ)	عضوا مناقشا
أ/د. مبطوش الحاج	أستاذ التعليم العالي	عضوا مدعوا

السّنة الجامعيّة

1441 ـ 1442هـ /2020- 2021م


بسم الله الرحمن الرحيم

كلمة شكر

﴿وَأَمَّا بِنِعْمَةِ رَبِّكَ فَحَدِّثْ﴾

الحمد الله والشكر له أولا، الذي شرح لانا صدرنا ويسر أمرنا ، وخفف عنا وزرنا وأحلل عقدة من لساننا، وأفقه قولنا، ووفقنا في إتمام هذا العمل المتواضع، ملك الملوك به استعنت وعليه توكلت فهو خير المتوكلين .لا يسعني في هذا المقام إلا أن أتقدم بالشكر الجزيل والتقدير لكل من أسهم في إخراج هذه المذكرة إلى النور؛ وأخص بذلك أستاذتنا الفاضلة الأستاذة الدكتورة *نبيلة هبة هروال* على تفضلها قبول الإشراف على هذه المذكرة، وعلى ما قدمته من النصح والتوجيه والإرشاد وعلى صبرها علينا طول هذه المدة رغم كثرة الارتباطات والانشغالات فجزاها الله كل خير.

و إلى كل من ساهم بالمساعدة ومد يد العون لنا، ولو بالكلمة الطيبة من قريب أو من بعيد في سبيل إنجاز هذا العمل

إهداء

أهدي ثمرة عملي هذا إلى...

أحن قلب في الوجود بعد حنان الله، إلى من دعت الله لي بالتوفيق وألحت في الدعاء إلى قرة عيني والدتي الغالية أطال الله في عمرها، وقدرني الله على رد جزء من جميلها، وإلى والدي رحمه الله وأسكنه فسيح جنانه.

وإلى من وقفت بحانبي في كل الأيام وساعدتني ولم تبخل عني في سبيل العلم والمعرفة فكانت سر نجاحي وتوفيقي وسندا لي أختي العزيزة الحاجة فاطمة أرجو من الله أن يمد في عمرها.

إلى من ترعرعت معهم ونما غصني بينهم إخوتي وأحبتي حفظهم الله: عبد اللطيف، عبد المؤمن، منصور، يوسف، مخطار.

إلى رفيقاتي اللواتي التقيت بهم في درب الحياة وقضيت معهم أياما لا تنسى: أميرة، أسماء، سارة، نور الهدى، دنيا.

إلى كل من وسعتهم ذاكرتي ولم تسعهم مذكرتي

جزاهم الله عني خير جزاء.

إهداء

إلى من بلغ الرسالة وأدى الأمانة ونصح الأمة

إلى نبي الرحمة ونور العالمين

إلى من أضاءت شمعة حياتي وعلمتني الصبر وتكبدت العناء لأجلنا

أمي الحبيبة أطال الله في عمرها

إلى قرة عيني وصاحب الدعم المتواصل

إلى من خطى لي المبادئ والأخلاق على صفحة بيضاء

أبي الغالي أطال الله في عمره

إلى سندي المتين

إلى من يعتبرون نجاحي نجاحا لهم

إلى معنى المساندة والاهتمام

إخوتي الأعزاء نوري ومحمد

إلى من أتقاسم معهم دفئ العائلة

إلى كل فرد من عائلة زوكل و خليفة

بالأخص محمد وعائلة كبريت

إلى المواقف والأخوة ومعني الصداقة الحقيقية

أخي وصديقي نور الدين

إلى جميع أصدقائي

وكل من قدم لنا المساعدة في انجاز هذا العمل

إلى كل هؤلاء أهدي ثمرة جهدي

عايد

إسماعيل

قائمة المختصرات

N.W.3.C	Le centre blans nationale du crime de collier
B.D.R.J	Les brigades départementales des renseignements et d'investigations judiciaires.
I.R.C.G.N	Institut de recherche criminelle de la gendarmerie nationale
O.C.L.C.T.I.C	L'office central de lutte contre la criminalité aux technologies de l'information et de la télécommunication
D.N.R.A.P.B	La division nationale de répression des atteintes aux biens et personnes
D.R.P.J.	Les directions régionales de la police judiciaire
S. T.R.J.D	Le département internet du service technique de recherches judiciaires
I.F.C.C	Le centre de plainte de fraude d'internet
F.B.I	Bureau d'instruction fédérale
I.C.3	Internet crime complaint center
I. N .C.C/GN	L'Institut national de criminologie et de criminalistique/Gendarmerie Nationale
CPLCIC-GN	Centre de prévention et de lutte contre la criminalité informatique et cybercriminalité/Gendarmerie Nationale
CIA	Central Intelligence Agency
O.E.C.D	Agency Organisation for Economic Cooperation and Development

تمهيد

تمهيد:

تميز هذا القرن باختراعات هائلة على المستوى التقني لعلى من أهمها وأكثرها فائدة ظهور الحاسب الآلي، وقد أصبح من لوازم الحياة المتطورة، سواء على المستوى العام أو الخاص.

ولا يخفى أن كل تطور تقني تكون له انعكاساته على المستوى القانوني بصفة عامة، وفي إطار القانون الجنائي على وجه الخصوص، فكل المخترعات الحديثة تثير مسألة الحماية الجنائية لها، سواء في إطار النصوص التقليدية أو باستحداث النصوص الملائمة لطبيعتها والدور الذي تؤديه في مختلف مجالات النشاط. كما أن هذه المخترعات الحديثة تؤثر في الإنسان كيانا ونشاطا، ولذلك فإنها تثير موضوع الحماية منها، أي حماية الإنسان وضمان حقوقه وحرياته الأساسية في مواجهة الغزو الذي تفرضه على جوانب من النشاط الإنساني إلى وقت قريب من المحرمات التي لا يجوز الإطلاع عليها.[1]

غير أن كل هذا التطور والتحول في أسلوب حياة الإنسان حمل معه مظاهر سلبية أثرت على أمن الدول والأفراد بالسلب، وذلك من خلال ظهور صور الغير المشروع لتقنية المعلوماتية، وهي التي أصطلح عليها قانونا وصف "جرائم الإنترنت" وهذا النوع الحديث من السلوكات الإجرامية الماسة بأمن وسلامة النظم المعلوماتية وبحقوق الغير تشكل خطرا بالغا وذلك لتعدد أوصافها الإجرامية،كجرائم سرقة المعلومات أو تخريبها، أو جرائم التحويل غير المشروع للأموال، أو جرائم التعدي على الغير عبر الشبكات، من جرائم مستحدثة تتسم بطابعها المعنوي الخالص وتخلو من الطابع المادي المميز لأغلب الجرائم التقليدية.

وامتدت الجريمة المستحدثة عن طريق الحاسب الآلي إلى شبكة الإنترنت، فالأشخاص الذين يستخدمون هذه الشبكة منهم الأسوياء، ومنهم دون ذلك ومجرمي شبكة الإنترنت يختلفون في ميولهم وأغراضهم، هؤلاء يمكنهم التعبير عن أنفسهم عن طريق شبكة الإنترنت ولهم مواقعهم

[1]- فتوح الشاذلي ،**جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية** ، منشورات الحلبي الحقوقية، الإسكندرية، مصر ، 2003، ص07.

الخاصة بهم على الشبكة، والتي من خلالها يروجون فيها لأفكارهم ومبادئهم. وعن طريق هذه المواقع تنتقل هذه الأفكار إلى مستخدمي الشبكة ومتصفحي هذه المواقع التي تكتسب بعض المتعاطفين معها.[1]

وإستقطب مفهوم جريمة الإنترنت مفهوم الفقهاء والقانونيين و المختصين في مجال المعلوماتية ،من أجل وضع تعريف شامل لجريمة الإنترنت، فحاول كل منهم حسب اختصاصه وضع تعريف ملائم فمنهم من عرفها تعريفا ضيقا وقال بأنها "الجرائم المرتبطة بالحاسوب والتي تشكل انتهاكا للقانون الجنائي" ومنهم من قال بأنها "تلك الجريمة التي يستخدم فيها الحاسوب" وهو تعريف واسع جدا."[2]

وقد عرف المشرع الجزائري جريمة الإنترنت في نص المادة 02 فقرة01 من قانون 09-04 الصادر في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بالقول أن هي "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق المنظومة المعلوماتية أو نظام للاتصالات الإلكترونية."[3]

بالنظر إلى التعاريف التي وردت لمفهوم جريمة الإنترنت وبدون شك ستتبادر إلى أذهاننا فكرة التساؤل حول الطبيعة القانونية لجريمة الإنترنت، فهي في ظاهرها جريمة غير مادية أي بدون أثر مادي ملموس فمجالها البيئة الإلكترونية مما يجعلها مختلفة كليا عن الجرائم الأخرى التي يرى التشريع الجنائي أنها تهدد مصلحة الغير العامة والخاصة، فيرى البعض بأن جريمة الإنترنت جريمة من نوع خاص ويرى البعض الآخر بأن جريمة الإنترنت جريمة مستحدثة.

---

[1]- عبد الفتاح بيومي حجازي ،**جرائم الكومبيوتر والإنترنت**، دار الكتب القانونية، مصر ،2007، ص15.

[2]- عمر بن محمد العتبي ، **الأمن المعلوماتي ومدى توافقه مع المعايير المحلية والدولية** ، رسالة مقدمة من أجل نيل شهادة الدكتوراه، جامعة نايف للعلوم الأنفية، السعودية ،2010، ص 21.

[3]- القانون 04/09الصادر بتاريخ 16 أوت 2009، الجريدة الرسمية رقم 47، ص05.

وإن ظهور كل هذه المفاهيم الإجرامية الحديثة، قلب مفاهيم النظرية التقليدية للجريمة فقد أدخلت جريمة الإنترنت على هذه الأخيرة صورا جديدة للجريمة بركنها الشرعي وأساليب وطرق حديثة لم تكن معروفة من قبل مست من خلال ركنها المادي فجرائم الإنترنت جرائم ناعمة، لا تستوجب لتحقيقها وسائلا وجهدا ماديا كبيرا وذلك من خلال اعتماد الجناة على وسائل تكنولوجيا وأساليب إجرامية حديثة ومتطورة تسمح لهم بنيل مبتغاهم بأقل جهد وبأسرع وقت ممكن دون اللجوء إلى العنف المادي، فمجرمو الإنترنت يتميزون بالذكاء والمعرفة الواسعة في مجال المعلوماتية وأدق تفاصيلها وهو ما يسمح بذلك بالتحكم في أثار وأدلة جرائمه من خلال تدميرها ومحوها وهو ما يجعل من أمر أغلب جرائم الإنترنت خفية لا يمكن اكتشافها أو تتبع أثارها، بالنظر إلى الطبيعة الخاصة للأدلة الناتجة عن هذا النوع من الجرائم، والتي أصبحت تشكل التحدي الأكبر الذي يواجه النصوص الجزائية الإجرائية، التي تنظم سير جملة الإجراءات الخاصة بعمليات البحث والتحقيق وملاحقة المجرمين، في إطار شرعي من أجل تقديمهم أمام العدالة.[1]

وأهمية هذا الموضوع تكمن في التزايد المستمر للنشاط الإجرامي عبر النظم المعلوماتية، وتزايد درجة خطورة هذا النشاط وارتفاع مستوى التهديدات التي يشكلها على الأمن العام في ظل الاعتماد المطلق على تكنولوجيا المعلومات في المجتمعات المعاصرة يقابله عجز سلطات البحث والتحقيق عن رسم نموذج موحد لهذه الجرائم والاستقرار على جملة من الإجراءات الخاصة بمتابعتها نظرا لتطورها الدائم والمستمر، مما ينتج عنه أحيانا غياب أو جمود إجرائي و عجزه عن تفعيل الإجراءات بسبب عدم ملائمته للجريمة محل البحث والتحقيق، وجريمة الإنترنت وكغيرها من أنواع الجرائم الأخرى، تمر بذات مرحلتي الاستدلال والتحقيق القضائي، وما يترتب على ذلك من إجراءات قانونية وفنية وشكلية ويعتبر إجراء التحقيق القضائي هو الأساس في مجال البحث والتحقيق المعلوماتي، وذلك لما يكتسبه هذا الأخير من أهمية قصوى في مجال استخلاص الحقائق

[1]- مخلوف عكاشة ، **دور الشرطة القضائية في مكافحة الجريمة الإلكترونية** ، كلية الحقوق، جامعة الدك تور مولاي الطاهر، سعيدة ،2016-2017، ص04.

بشأن الجريمة، لكن تبقى الإجراءات الأخرى الخاصة بمرحلة الاستدلال أو التحري الفنية منها خصوصا ضرورية لأجل استكمال متطلبات التحقيق القضائي في مجال جريمة الإنترنت.[1]

وتصنيف موضوع إجراءات البحث والتحري من بين أهم المواضيع المطروحة للنقاش، فهي تشغل باستمرار حيزا مهما من جهود الباحثين كذلك الفقه والتشريع لأجل وضع إستراتيجيات قانونية وعملية مستقبلية، تضمن عدم فقدان السيطرة على تقنية المعلومات وتحويلها من تقنية تساعد على تطور المجتمعات من خلال تبادل المعارف و المعلومات إلى تقنية هدامة.

فنظرا لكون أن جرائم الإنترنت من الجرائم المستحدثة التي تستعمل فيها التقنية العالية ونظرا لكونها من الجرائم العابرة للحدود، فغن المشرع أصبح يعيد النظر في الكثير من المسائل الإجرائية بان هذا النوع من الجرائم جعل موضوع الإجراءات الجنائية في مأزق حقيقي إذ ظهرت نتيجة عنه جملة من الصعوبات والإشكاليات العملية، التي تعرقل وتقف كحجر عائق أمام أجهزة العدالة في مواجهتهم لهذه الطائفة من الجوانب لا سيما أجهزة الضبط والتحري القائمة على مباشرة البحث والتحري في مرحلة جمع الاستدلالات، إذ أصبحت هذه الفئة تواجه مشاكل إجرائية أثناء ممارستها لواجباتها في الكشف عن هذا النوع من الجرائم وملاحقة مرتكبيها وتقديمهم للمحاكمة نظرا لعدم تخصصها وجهلها لطبيعتها أي نقص الخبرة في هذا المجال. ومن المشاكل التي تواجه تلك الفئة هي أن مسرح الجريمة الذي ترتكب فيه هذا النوع من الجرائم يختلف عن ذلك الذي ترتكب فيه الجرائم التقليدية، كما أن الدليل فيها غير مرئي كما أنها في أغلب الأحيان لا يتم التبليغ عنها وتبقى في طي الكتمان هذا من جهة ومن جهة المشاكل الإجرائية هي كيفية التفتيش والضبط والمعاينة في العالم الإفتراضي وكذلك كيفية التعامل مع البلاغات والشكاوى التي غالبا ما تسجل ضد مجهول من العالم ،لذلك كان من الواجب على رجال الفقه أن يضعو الحلول القانونية اللازمة متا يمكن أن ينشا عن جرائم الإنترنت من مشاكل إجرائية في مرحلة جمع الاستدلالات ليستنير المشرع الإجرائي بها عند سنه للقوانين.

[1]- عبد الفتاح بيومي حجازي، المرجع السابق، ص67.

ومن الأسباب التي دفعتنا إلى اختيار هذا الموضوع هو الوقوف على حقيقة التعامل مع جريمة الإنترنت من الناحية الإجرائية فالكثير من الدراسات التي عينت بهذه الجرائم باتت تركز على الجانب الموضوعي فقط.

الرغبة في التعمق في دراسة وتحليل الدور الذي تلعبه الشرطة القضائية في مكافحة النشاط الإجرامي الالكتروني، والتي أسست لها الجهود والمعاهدات الدولية والإقليمية، والاتفاقيات العربية لمكافحة الجرائم المنتشرة بالتقنية المعلوماتية وكذلك الجهود التشريعية الداخلية، كما هو عليه الحال في الجزائر التي أقرت بتشريع خاص يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك بتاريخ 05 أوت 2009 متوجب القانون 04/09 وهي القوانين التي تحاول تنظيم فضاء المعلوماتية بصفة عامة ومكافحة الجانب الإجرامي المتصل بها، من خلال تحديد قواعد إجرائية خاصة تسمح متتابعة هذا النوع من الجرائم ومرتكبيها بشكل يضمن شرعية الإجراءات المتخذة، بهدف ردع هذه الفئة من المجرمين.[1]

ومن الأسباب الشخصية تكمن في اهتمامنا بمجال جريمة الإنترنت وما يترتب عنها من جرائم وكذا إجراءات البحث والتحري فيها تختلف كل الاختلاف عن الإجراءات المتبعة في الجرائم التقليدية وبالإضافة إلى انه موضوع جديد **وقد حالت بيننا وبين بحثنا المتواضع كما كمن نطمح انجازه صعوبات ومعوقات أهما** قلة الدراسات

السابقة في المجال الإجرائي واتجاه أغلبها إلى معالجة الظاهرة الإجرائية المعلوماتية من ناحية السلوك الإجرامي والعقوبات المقررة لها، دون التركيز على الجانب الإجرائي، وهو ما جعلنا أمام حتمية تجميع المعلومات الخاصة بالموضوع في شكل جزئي وإعادة تجميعها في شكل متناسق وفق خطة عمل.

إن التغير الحاصل على مستوى النشاط الإجرامي بفعل اتصاله بتقنية المعلوماتية، صاحبه تحول كبير على المستوى القانوني وبالخصوص الإجرائي فظهرت آليات وإجراءات قانونية

[1]- مخلوف عكاشة، المرجع السابق، ص06.

مستحدثة في مجال البحث والتحقيق، أساسها النص القانوني، وميدانها جرائم الإنترنت غير أن تطور كلا المجالين لا يسري بنفس الوتيرة، فجرائم الإنترنت تتطور بشكل سريع ومذهل فيما تعرف النصوص والإجراءات القانونية وتيرة بطيئة من حيث مسايرتها لواقع جريمة الإنترنت، مما يخلق دوما فجوة بين الجريمة والإجراءات الموضوعية لمتابعتها قد تسبب في تعطيل أو شل عمل الجهات المختصة بمباشرة هذه الإجراءات.[1]

ومن الصعوبات التي واجهتنا ضيق الوقت بسبب جائحة كورونا "كوفيد 19" والثابت أن الموضوع لم يكن مستهلكا من ذي قبل بتفصيله، ولا يوجد إلا كتابا واحدا في موضوع إجراءات البحث والتحري في جريمة الإنترنت وهو الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات دراسة مقارنة للدكتورة نبيلة هبة هروال.

وقد خلصنا ببحثنا المتواضع إلى بيان ولو بسيط لإجراءات البحث والتحري لجريمة الإنترنت، **ويهدف هذا الموضوع إلى** دراسة جريمة الإنترنت ودور الضبطية القضائية في مرحلة البحث والتحري من حيث تحديد مفهوم الشرطة القضائية، والتعريف بالجهود الدولية والوطنية لمكافحتها وأبرز الاتفاقيات الدولية في هذا الشأن وصولا إلى تبيان موقف التشريعات الأجنبية و العربية من هده الجريمة بحيث ينظر إلى جميع الجوانب الموضوعية الخاصة به، يتبع هذا الهدف من الدراسة من محاولة المساهمة في وضع الخطوط العريضة للتعرف على طرق التحقيق في هذا النوع من الجرائم ذلك أن جدة وحداثة جرائم الإنترنت وما تتسم به من خصائص سوف يجد معه المحقق نفسه في حيرة أمامها وكيفية التعامل معها وأسلوب التحقيق فيها، إذ لا شك أن إجراءات التحقيق وجمع الأدلة بخصوص هذه الجرائم يختلف عما هو الحال عليه في الجرائم التقليدية.[2]

كما يهدف إلى الوقوف على السياسات الجنائية المعاصرة في معالجة التحقيق في هذه الجرائم وتحقيق التوازن الفكري الالكتروني للمتحري والباحث في هذا النوع ما الجرائم، توضيح

[1]- مخلوف عكاشة، المرجع السابق، ص07.

[2]- سعيداني نعيم، آليات **البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري** ،كلية الحقوق، جامعة الحاج لخضر، الجزائر، 2013/2012، ص07.

القواعد والإجراءات اللازمة لتلقي وتحديد محضر جمع الأدلة، معرفة الصفات والمؤهلات الواجب توافرها في التحري الجنائي في جرائم الإنترنت.[1]

ونظرا لأهمية الجريمة حل الدراسة م ا لاعتماد على المنهج التحليلي، الوصفي ، كونه الأنسب لمثل هذه الدراسات من خلال تحليل مختلف المواد القانونية التي تتضمن الإجراءات المتابعة في جريمة الإنترنت واختلافها عن النصوص الإجرائية التقليدية وكذا وصف ظاهرة جريمة وكذا قيامنا بوصف المفاهيم الخاصة بالإجراءات المستعملة في البحث والتحري والصعوبات التي تواجهها، كما اعتمدنا على المنهج المقارن في بعض الأحيان.

أما في منهج التحليل حاولنا في هذا البحث تحليل بعض المفاهيم والغوص في جزيئاتها وطرحها بشكل من التفصيل والتشريع لما بدا لنا من أهميتها، مثلما كان الحال لإجراء تفتيش المنظومة المعلوماتية ، الإشكاليات القانونية التي يطرحها موضوع البحث أفرزت جريمة الإنترنت تحديات واضحة للقوانين التي وضعت لمكافحتها فقد تغيرت الجريمة من صورتها التقليدية المتمثلة في صورتها المادية إلى أخرى معنوية، ويتم ذلك عن مشكلة تفسير النصوص القانونية ويظهر القياس في المواد الجنائية ومبدأ شرعية الجنائي، وهذه العوامل تؤدي إلى إفلات كبير من مجرمي هذه الجرائم من العقوبات كما أفرزت ثورة الاتصالات والمعلومات نوع جديد من الجرائم لم يتصور المشرع الوطني حدوثها أصلا ومن هذا كان من الضروري أن تواكب التشريعات الوطنية المختلفة هذا التطور الملحوظ في جرائم الإنترنت، فالمواجهة التشريعية ضرورية للتعامل من خلال قواعد قانوني غير تقليدية لهذا النوع من الجرائم المستحدثة.

كما أن تطور الجوانب القانونية والتشريعية قد لا تكون دائما بخطى متوازية مع تطور جريمة الإنترنت مما نتج عنه عكس التشريعات القائمة عن مواجهة هذا الخطر.

[1]– فيروز عوض كريم، صالح ميرغني، **إجراءات التحري والضبط في الجريمة الإ لكترونية**، قسم القانون، جامعة الشندي، 2017، ص 03.

ومنه نطرح الإشكالية التالية: **هل هناك هيئة مخصصة لمكافحة هذا النوع من الجرائم؟ وما هي الآليات التي انتهجتها التشريعات في مكافحة جريمة الإنترنت سيما في مرحلة التحقيق الأولي؟**

ولقد تم الإجابة على هذه الإشكالية عن طريق تقسيم بحثنا تقسيما علميا ممنهجا، وذلك من خلال الفصول والمباحث والمطالب كما سيلي إلماما بالموضوع قدر المستطاع كالأتي:

فقسّم البحث إلى فصلين، الفصل الأول تم التطرق فيه إلى الأجهزة المختصة في البحث والتحري في جريمة الإنترنت والذي بدوره قسم إلى مبحثين، المبحث الأول شرطة الإنترنت كضبطية مختصة في البحث والتحري عن جريمة الإنترنت، احتوى هذا المبحث مطلبين، المطلب الأول الدوافع التي أدت إلى إنشائها والمبادئ التي تحكمها، وفي المطلب الثاني دور شرطة الإنترنت كضبطية مختصة في البحث والتحري عن جريمة الإنترنت، أما المبحث الثاني شرطة الإنترنت على المستوى الوطني والدولي، في المطلب الأول على المستوى الوطني، في المبحث الثاني، على المستوى الدولي.

أما الفصل الثاني تم تناول فيه اختصاصات شرطة الإنترنت، تضمن هو الآخر مبحثين، المبحث الأول سلطات شرطة الإنترنت في الظروف العادية به مطلبين، المطلب الأول تلقي البلاغات والشكاوى في جريمة الإنترنت، والمطلب الثاني البحث والتحري عن الجرائم والجناة في جريمة الإنترنت ،ويكمن المبحث الثاني سلطات شرطة الإنترنت في الظروف الاستثنائية، تمحور هذا الأخير في مطلبين، المطلب الأول المعاينة والتفتيش في جريمة الإنترنت، والمطلب الثاني إجراءات البحث والتحري الخاصة .

الفصل الأول

الأجهزة المختصة في البحث والتحري عن جريمة الإنترنت

تمهيد وتقسيم:

نتيجة للتطور التكنولوجي لتقنية المعلومات والتقدم السريع والمتواصل لتطوير الأجهزة والبرامج المعلوماتية واعتماد قطاعات كبيرة من المجتمع على التقنية المعلوماتية على المستوى الدولي والمحلي في شتى المجالات والميادين الحربية والمالية والثقافية والاجتماعية والاقتصادية والسياسية. فقد اتسعت دائرة استخدام الحاسبات الإلكترونية خلال القرنين الماضيين باضطراد وتطور مستمر وبسرعة غير مسبوقة وأصبحت كافة الأجهزة العامة والخاصة تعتمد عليها في تسيير شؤونها وتقلص دور الأوعية الورقية واقتران ذلك بالاعتماد على أوعية أخرى غير ورقية في البيئة المعلوماتية كالملفات والأشرطة والأسطوانات والأقراص الضوئية.

ولمسايرة هذا التقدم التكنولوجي ولعلاج هذه المشكلة شهدت التشريعات الحديثة تطورا كبيرا في إجراءات ضبط هذه الجرائم على غرار نصوص التجريم الحديثة لهذه الجرائم المستحدثة وأمام هذه التحديات كان من الضروري إعداد قوات خاصة لمواجهة هذا العدوان الإلكتروني عبر الإنترنت، أطلق عليها تسميات عديدة منها شرطة الإنترنت أو الشرطة الإلكترونية فما هي هده الشرطة؟ و ما هي دوافع التي أدت إلى إنشائها؟ و ما هي المبادئ التي تحكمها؟

ولقد تم تخصيص هذا الفصل للإجابة عن مجموعة الإشكاليات، و ذلك من خلال تقسيمه إلى المباحث التالية:

المبحث الأول: شرطة الإنترنت كضبطية مختصة في البحث والتحري عن جريمة الإنترنت

المبحث الثاني: شرطة الإنترنت على المستوى الوطني والدولي

المبحث الأول: شرطة الإنترنت كضبطية مختصة في البحث والتحري عن جريمة الإنترنت

الاستخدام المتزايد للأنظمة المعلوماتية رغم ماله من فوائد جمة وعظيمة في مجال الرقي والتقدم التكنولوجي يقابله وجه آخر مظلم حيث توجد أثار سلبية لهذا الاستخدام نتيجة الاستغلال المتعسف والسيئ لهذه التقنية مما أفرز نوعا جديدا من الإجرام يطلق عليه الإجرام المعلوماتي وأصبح حقيقة اجتماعي أو ظاهرة اجتماعية تستوجب النظر إليها ومعالجتها قانونيا حتى نضع الضوابط التي من شأنها أن تحد من التعدي المؤثر على التقنية الحديثة لنظم المعلومات.[1]

ولذلك كان من الضروري إعداد وتجهيز قوات خاصة لمواجهة هذا العدوان الإلكتروني عبر الإنترنت والذي أصبح أحد الهواجس التي تعيشها المجتمعات المتقدمة والنامية.

وعلى هذا فالإشكال المطروح هنا هو: هل توجد هناك ضبطية قضائية متخصصة في البحث على هذا النوع من الجرائم المستحدثة؟ وهل هناك ضبطية متخصصة الحيلولة دون وقوع مثل ذلك من الجرائم؟ وما الفرق بينها وبين الضبطية القضائية العادية؟ وللإجابة على هذه الإشكاليات تم تقسيم هذا المبحث إلى المطالب التالية:

المطلب الأول:الدوافع التي أدت إلى إنشاء شرطة الأنترنت والمبادئ التي تحكمها

تعتبر جريمة الإنترنت من الظواهر الحديثة وذلك لارتباطها بتكنولوجيا حديثة، ومن المواضيع الأكثر انتشارا على المستوى الدولي والإقليمي والمحلي فلقد أخذت هذه الجريمة باعتبارها نتاج الاستخدام السلبي للتكنولوجيا، وما يتصل بها من تقنيات حيزا كبيرا من الاهتمام بهذا الجانب وذلك لجسامة الآثار الناشئة عم هذه الظاهرة الحديثة نوعا ما وفي جميع مجالات الحياة.

إن الدعوة العمومية باعتبارها الوسيلة القانونية لاستفتاء حق الدولة في العقاب تبدأ إجراءاتها بمرحلة البحث والتحري التي تهدف إلى البحث عن الجريمة والكشف عن مرتكبيها وإن الإجراءات الجزائية المتخذة خلال هذه المرحلة تتولاها أجهزة شرطة الإنترنت.

---

[1]- فتوح الشاذلي، **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية**، منشورات الحلبي الحقوقية، الإسكندرية، مصر، 2003، ص350.

الفرع الأول: إنشاء شرطة الأنترنت

أولا:تعريف شرطة الإنترنت

تم وضع شرطة متخصصة لمواجهة هذا الإجرام المستحدث أطلق عليها مصطلحات مختلفة ولكنها متقاربة: "كشرطة الإنترنت (Gyber police) " أو "درك الإنترنت (Gyber gendarme) " أو "دورية شرطة الإنترنت (Cyber – patrouille) " أو "متحري الإنترنت (Cyber détectives)".

يقصد بشرطة الإنترنت: "نوع من الإجراءات والضمانات للمحافظة على أموال الغير وأسرارهم".[1]

تقوم بها ضبطية قضائية مختلفة تماما عن تلك التي تقوم بالكشف عن الجرائم التقليدية، لكونها لا تعتمد على التدريبات المادية أو الفيزيولوجية التي يتلقاها رجال الشرطة للوصول إلى هذه المرتبة وإنما تعتمد على قوة تكوين البناء العلمي والتكنولوجي لأفرادها وهي تتولى في ذلك مهمة مباشرة جميع الاستدلالات والتحري في العالم الافتراضي، كما يمكنها أن تطارد الهكرة ومخترقي الأنظمة على كافة المستويات.

كما يعود الاختصاص في البحث والتحري في جرائم الإنترنت إلى أعضاء الضبطية القضائية مما يضعنا أمام معادلة غير متكافئة، طرفها أجهزة البحث والتحري والتحقيق بنقص خبرتهم في مجال الكمبيوتر والإنترنت والمعاملات الإلكترونية، والطرف الآخر هم قراصنة محتالون يتمتعون بمهارات عالية يواكبون كل جديد في عالم المعلوماتية والاتصال.

يعد جهاز الشرطة الأداة الرئيسية لصيانة أمن المجتمع ووقايته من عوامل تقويضه بالإضافة لدوره القضائي في ضبط الجرائم فله دور وقائي بهدف منع ارتكاب الجرائم والحيلولة دون ارتكابها

[1]- جميل عبد الباقي الصغير، **الجوانب الجزائية للجرائم المتعلقة بالإنترنت**، دار النهضة العربية، القاهرة، مصر، 2002، ص 77.

وتقليل فرص اقترافها وبالتالي تقل أضرارها المباشرة وغير المباشرة فهو يوفر للأفراد الطمأنينة على أرواحهم وأموالهم وذلك بمنع أو اتقاء كل خطر من شأنه أن يسبب ضررا لهم.

وعندما تمارس الشرطة هذه الوظيفة يطلق عليها الضبطية الإدارية أو بوليس المنع وهي سابقة على وظيفة الشرطة القضائية التي لا تباشرها إلا بعد وقوع الجريمة والتي يطلق عليها بوليس العقاب وعملا يصعب التمييز بين سلطتي المنع والعقاب نظرا لوحدة جهاز الشرطة الذي يتحمل في الغالب مهام الوظيفتين وذلك لتحقيق الفاعلية وتبسيط الإجراءات.[1]

ونظرا لطبيعة الجرائم المعلوماتية الخاصة وكيان البيئة المعلوماتية الغير محسوس وصعوبة الدور الشرطي الوقائي لمنع ارتكاب هذه الجرائم خصوصا إذا كان محلها البيانات التي تحويها الملفات أو الاسطوانات أو بنوك المعلومات.

فلا تستطيع الشرطة أن تؤدي دورا ايجابيا في هذا المجال.

ولكن نظرا لأن قلب النظام المعلوماتي أو البيئة المعلوماتية هو البرامج المعلوماتية فقد وضعت القوانين الحديثة بعض النصوص التي توفر الحماية الممكنة لهذه البرامج.

وتقوم أجهزة الشرطة بدور هام في الحفاظ على هذه البرامج من السرقة أو النسخ الغير مشروع لها.[2]

وبرامج الحاسب تعتبر بمثابة العقل المفكر للحاسب ويطلق عليها القيم الفكرية وتحتاج إلى العناية الكافية لحمايتها من العبث بها لزيادة إنتاجها والاستثمار فيها للارتقاء بكفاءتها الاقتصادية والمحافظة على القدرات المادية والبشرية المستخدمة فيها.

ولما كانت صناعة البرمجيات قد غدت من الصناعات الهامة التي تساهم في زيادة الدخل القومي وتساهم في كفاءة إنتاجية الأنظمة المعلوماتية فأصبحت محل عناية و اهتمام الدولة فوفرت لها

[1]- فتوح الشاذلي، **جرائم الكمبيوتر**، المرجع السابق، ص349.

[2]- فتوح الشاذلي، المرجع نفسه، ص 351.

الحماية القانونية كما لو كلت إلى الأجهزة الأمنية باتخاذ الإجراءات الكفيلة للحد من جرائم سرقتها أو نسخها أو التعدي عليها.

فدور الشرطة ينحصر في نطاق ضيق حدده القانون بالتزام المتعاملين في هذه البرامج واستخداماتها والمتعاملين معها بالحصول على ترخيص للتعامل مع هذه الأجهزة وبرامجها ومنوط بالشرطة للتأكد من التزام هذه الجهات بذلك الأمر.[1]

ثانيا: دوافع إنشاء شرطة الانترنت

إن من أهم العوامل الداعية لإنشاء جهاز مختص بالجرائم الانترنت هو الطبيعة المميزة لهذه الجرائم كونها جرائم تقع في بيئة افتراضية، ولا تترك آثار مادية مثلما هو الأمر في الجرائم العادية كون أن جريمة الانترنت جريمة عابرة للحدود وكذلك صعوبة اكتشافها وإثباتها.

ولقد قامت المنظمات الحكومية ومنظمات الشرطة في بعض الدول بتدريب رجالها وذلك بترتيب دورات تخصصية لهم في ذلك المجال، ومن بين تلك الدول: الولايات المتحدة الأمريكية والتي قامت بعقد تلك الدورات المتخصصة مدة كل منها أربعة أسابيع وذلك من أجل تزويد محققي الشرطة والعاملين في إدارات العدالة الجنائية بمعارف ومهارات حول برمجة الحاسوب وتشغيله مع استخدام تطبيق بنكي مصغر وحاسب آلي صغير.[2]

وإلى جانب الولايات المتحدة الأمريكية تقوم كندا بتدريب رجال الضبطية القضائية على تقنيات الحوسبة. وكذلك الحال بالنسبة للملكة المتحدة إذ تنظم فيها إسكوتلانديار دورات متخصصة تشمل التدريب على لغتي البرمجة كوبول (Copol) وباسك (Basic) ودراسة مجموعة حالات مع تحليل الوظائف والاختصاصات المتنوعة في مجال المعالجة الآلية للبيانات والمخاطر التي يكمن أن تكون سببا فيها.[3]

---

[1]- فتوح الشاذلي، المرجع نفسه، ص351.

[2]- نبيلة هبة هروال، **الجوانب الإجرائية لجرائم الانترنت**، دار الفكر الجامعي، مصر،2007، ص100.

[3]- هشام محمد فريد رستم، **الجرائم المعلوماتية أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين** ، مجلة الأمن والقانون، كلية شرطة دبي، العدد الثاني السنة 7 وما بعدها، 1999، ص30.

أما بالنسبة لمصر فقد اتخذت فيها وزارة الداخلية مجموعة من الإجراءات لمكافحة الجرائم المعلوماتية منها: تعديل منهج التدريب والدراسة في كل من كلية الشرطة وكلية تدريب بالتنمية بأكاديمية الشرطة وذلك بإدخال مواد جديدة لدراسة الحاسبات الآلية ونظم المعلومات المرتبطة بها.[1] وشأن والتكوين في البحث والتنقيب وفي ملاحقة مرتكبي جرائم الانترنت إلى جانب وحدات الدرك الفرنسي[2].

الفرع الثاني: المبادئ التي تحكم شرطة الإنترنت والصعوبات التي تواجهها

وجرائم الحاسب بإعتبارها من الجرائم المستحدثة فإنها مزيدا من الأعباء على جهاز الشرطة وذلك بالنظر إلى قلة خبرتها في مواجهتها حيث لم يعهد بجرائم من مثيلتها من قبل، وتوجد ثمة صعوبات تحول دون أداء هذا الجهاز لدوره في مواجهة الجريمة الإلكترونية.

ولما كانت هذه الجرائم لها طبيعة خاصة وأدلتها غير محسوسة وتحتاج لخبرة فنية وتقنية عالية كي تتعامل مع هذه الخواص الجديدة وتواكب التكنولوجيا الحديثة لهذه البيئة والعاملين فيها والمتعاملين معها.

أولا: المبادئ التي تحكم شرطة الإنترنت

يحكم الضبط القضائي في ظل البحث والتنقيب عن جرائم الإنترنت مبادئ معينة ، وإن كانت غير مختلفة عن تلك الموجودة في حالة البحث والتنقيب عن الجرائم التقليدية وهي:

1-من الناحية الأولى: يشترط أن تكون الفئة ممن تتمتع بفن الضبط القضائي، أي يجب أن تكون متخصصة في إدراك كيفية عمل الضبط القضائي وموضوعاته، لكي تكون مستعدة دائما للتعامل مع هذه النوعية من الجرائم، وذلك عن طريق تدريبها وتكوينها في أمور تقنية الحوسبة والإنترنت، وفي كيفية التعامل مع هذا العالم الافتراضي.

[1]- علاء الدين محمد شحاتة، **رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي**، دار النهضة العربية، القاهرة، مصر، 1993، ص587.

[2]- Web Algérie : le premier portail algérien depeuis 1996, des cadres de la gendarmerie algérienne en formation en France, disponible en ligne à l'adresse suivante : http://www.webalgérie.com.

2–من الناحية الثانية: فتجدر الإشارة إلى أن انتشار الإنترنت وإمكانية ارتكاب سلوك سلبي عبرها، يستدعي إعادة النظر في تفسير المشروعية [1] في بعض أعمال الضبط المناط بها مأمورو الضبط القضائي، كما هو الشأن في التخفي عبر الاتصالات وإمكانية انتحاله اسما وهميا ودخوله في حلقات النقاش وممارسته للتراسل الإلكتروني بقصد الكشف عن الجرائم.

3–ومن الناحية الثالثة: فإنه ومن الإجراءات اللازمة والمتطلبة في مرحلة جمع الاستدلالات أن يلتزم مأمور الضبط القضائي بتحرير محضر يثبت فيه كل ما اتخذه من إجراءات للكشف عن الجريمة، من انتقال إلى مسرح الجريمة ومعاينته والضبط وسماع الشهود... الخ والحال لا يختلف في بيئة الإنترنت التي وقعت فيها الجريمة، إذ يمكن لمأمور الضبط القضائي تحرير ذلك المحضر عبر الإنترنت.

4–من الناحية الرابعة: فإنه يستوجب لقيام مأموري الضبط القضائي بالإجراءات التي تمس وتقيد حرية المتهم أو المشتبه فيه، كالتفتيش والضبط والقبض في الحالات الاستثنائية أن يتصدر إذنا من السلطات المختصة للقيام بتلك الإجراءات. و الأمر لا يتغير في بيئة الإنترنت، إذ يمكن لتلك الإجراءات أن تتم في تلك الأخيرة دون أي إشكال، مع مراعاة بعض الاختلافات.

5–من الناحية الخامسة: فإنه يجب على مأمور الضبط القضائي كقاعدة عامة، ولأجل صحة إجراءاته أن يكون مختصا بالقيام بذلك الإجراء سواء من ناحية الاختصاص المكاني أو النوعي أو الزماني[2].

وتجدر الإشارة أن هناك نقطة هامة يجب ذكرها هي أنه في إذا كان رجل الضبط القضائي يملك الصلاحية الضبط القضائي في نطاق الإجرام تخصصه ، وليس له أن يتجاوزه في نطلق

---

[1]– يقصد بالمشروعية: "التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام" لمزيد من التفاصيل ينظر د/ أيمن عبد الحفيظ عبد الحميد سليمان، **إستراتيجية مكافحة الجرائم الحاسب الآلي** ، دراسة مقارنة، رسالة دكتوراه، أكاديمية الشرطة، ص351 وما بعدها.

[2]– نبيلة هبة هروال، المرجع السابق، ص103.

الإجرام العادي فإنه وفي إطار جرائم الإنترنت يحتاج الأمر إلى إعادة تفسير، لكون أن تلك الأخيرة تتميز بأنها عابرة للحدود (Transnationale). أي أن هناك حاجة لوضع نص يسمح بمقتضاه لرجال الضبط القضائي بالانتقال عبر العالم الافتراضي للتعاون مع جهات الضبط الدولية، وخصوصا في الحالات التي تتوفر فيها اتفاقيات دولية بيم الدول، من أجل مكافحة الإجرام عبر ذلك العالم.

ثانيا: الفرق بينها وبين الشرطة العادية:

1) أوجه التشابه:

- **من حيث الهدف:** يهدفان إلى حماية النظام العام والسكينة العامة والصحة العامة، يهدفان إلى محاربة الجريمة مهما كان نوعها فهي وقائية ومكافحة في نفس الوقت.

2) أوجه الإختلاف:

- **من حيث التكوين:** شرطة الإنترنت تعتمد في تكوينها على البناء العلمي والتكنولوجي، أما الشرطة العادية تعتمد على التدريبات المادية والفيزيولوجية.
- **من حيث الإجراءات:** شرطة الإنترنت إجراءاتها مستحدثة (كالتسرب وإعتراض المراسلات والمراقبة الإلكترونية)، أما الشرطة العادية فإجراءاتها تقليدية.
- **من حيث الإختصاص:** شرطة الإنترنت إختصاصها وطني، أما الشرطة العادية إختصاصها إقليمي.
- **من حيث المعاينة:** شرطة الإنترنت تقوم بالمعاينة في المسرح الإفتراضي، أما الشرطة العادية تقوم بالمعاينة في المسرح التقليدي.
- **من حيث التفتيش:** شرطة الإنترنت يكون التفتيش في أي وقت، أما الشرطة العادية يكون التفتيش فيها محدودا من الساعة الخامسة صباحا إلى غاية الساعة الثامنة مساءا إلا في الظروف الإستثنائية.

ثالثا: الصعوبات التي تواجهها في مواجهة جرائم الإنترنت

إن جرائم الإنترنت تعتبر من أكبر التحديات التي تواجه أجهزة العدالة الجنائية بما فيها أجهزة ضبط الجرائم أي رجال الضبطية القضائية، ولقد تناول مؤتمر الأنتربول السادس لجرائم المعلومات الذي شهدته القاهرة في الفترة ما بين 13 إلى 2005/24/15 تلك التحديات التي تواجه أجهزة الضبط القضائي في مكافحتها لجرائم الإنترنت على المستويين المحلي والدولي.

1)**التحديات المحلية**: وهي تتمثل في ثلاث نقاط وهي:

أ-تتمثل في انتشار مقاهي الإنترنت: التي يستطيع أي فرد من خلالها أن يتعامل مع شبكة الشبكات بما فيه المجرم الذي يستخدمها لإرتكاب جرائمه، وهو ما يؤدي إلى صعوبة التوصل لمرتكبيها لعدم التزام تلك المقاهي بشروط التراخيص بالإضافة إلى إمكانية تنقل ذلك المجرم بين أكثر من مقهى خلال اليوم الواحد، ما يؤدي إلى صعوبة التوصل بصورة دورية لأدلة الإثبات لقيام تلك المقاهي بإعادة تشكيل الأجهزة ولاسيما وان تلك الأدلة توصف بغير المرئية وبأنها سهلة المحو والتدمير في زمن قصير جدا. [1]

ب-يتمثل في تكنولوجيا الـ ADSL: أو ما يعرف باسم الإنترنت فائق السرعة والذي لم يسلمك هو الآخر من يد المجرمين، إذ استخدموه لتنفيذ مخططاتهم الإجرامية وذلك عن طريق اشتراكهم إلى جانب أشخاص آخرين في جهاز واحد عن طريق موزع خطوط مما يؤدي إلى صعوبة التوصل إليهم.

ج-ظهور الإنترنت اللاسلكي (WIFI): والذي هو الآخر لم يلفت من أيدي المجرمين إذا سهل لهم التنقل إلى عدة أمكنة في اليوم الواحد.

[1]- لمزيد من التفاصيل ينظر د/ هشام محمد فريد رستم، مرجع سابق، ص 17/16. د/ جميل عبد الباقي الصغير، **الجوانب الإجرائية للجرائم المتعلقة بالإنترنت**، دار النهضة العربية، القاهرة، مصر، 2002، ص4. د/ عبد الله حسين علي محمود، **سرقة المعلومات المخزنة في الحاسب الآلي** ، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 2002، ص344 وما بعدها.

2)**التحديات الدولية:** وهي تتمحور في ثلاث نقاط:

أ-عمليات التخفي (PROXY)[1]: أثناء التجوال في شبكة الإنترنت والتي تؤمنها بعض المواقع فعلى الرغم من أهمية البروكسيات والهدف التي صممت من اجله، لتامين الشبكات والمواقع ضد الاختراقات فإنها استغلت استغلالا سيئا من قبل القراصنة بل غن مصممي الفيروسات المدمرة من خلال تلك المواقع قاموا بإطلاق فيروساتهم المدمرة على العالم، الأمر الذي بات يشكل ظاهرة خطيرة.

ب-غياب المفهوم العام: متفق عليه بين الدول حول نماذج النشاط المكون لجريمة الإنترنت والتعريف القانوني لها جعلها جريمة عابرة للحدود.[2]

ج-أن مسرح جريمة الإنترنت كان من الماضي: في الدول المتقدمة ثم امتد إلى الدول النائية التي أدخلت التكنولوجيا المتقدمة كعامل يدعم التنمية في السنوات الأخيرة.[3]

وإضافة إلى الأسباب السابقة والتي أدت إلى بروز تحديات وصعوبات في عمل جهاز الضبط القضائي هناك أسباب أخرى وهي:

1-أن ما يزيد في صعوبة عمل مأموري الضبط القضائي في العالم الافتراضي خفاء الجريمة إذ تتميز الجرائم التي تقع على الإنترنت أو بواسطتها، في أكثر صورها بأنها مستمرة وخفية لا يلحظها المجني عليه غالبا أو يدري حتى بوقوعها فهي غالبا ما تكتشف بمحض الصدفة فمثلا أن التجسس

---

[1]- المقصود بـ (PROXY): هو تطبيق يتم تركيبه على خوادم تسمى الـ proxy servers وتعتمد عليه الشبكات الداخلية ومزود الخدمة كوسيط بين المستخدمين الإنترنت، وهو يساهم بجزء لا بأس به في الحماية والسرعة والأمان فضلا عن عزله للشبكة عن الشبكة العالمية الخارجية (WWW).

[2]- ناجي الجرجاوي، **الجريمة المعلوماتية تتصاعد....وتحتاج تعاونا دوليا ومعايير قانونية جديدة** ، لغة المصدر، مجلة الأهرام للكمبيوتر والإنترنت والاتصالات، العدد الثالث والخمسون، السنة الخامسة، 2005، ص67.

[3]- نبيلة هبة هروال، **الجوانب الإجرائية لجرائم الانترنت**، المرجع السابق، ص171.

المعلوماتي بنسخ الملفات وسرقة وقت الآلة من النادر اكتشافها من طرف الشركات التي تقع ضحية لهما [1] وبذلك فهي توصف بالجريمة غير المرئية.

2-كما أنها لا تترك أثار مادية تدين مرتكبيها وتوصله إلى المحاكمة وتوقيع العقوبة أي أن أدلتها غير مرئية وسهلة المحو والتدمير في زمن يسير جدا، كما انه يصعب الوصول غليها خاصة في الحالات التي يستعمل فيما كلمة السر أو التشفير أو تلك التي يدس فيها تعليمات خفية بين البيانات المخزنة إلكترونيا أو المنقولة عبر شبكة الاتصال أو ترميزها لإعاقة أو منع إطلاع عليها أو ضبطها.[2]

3-وما يزيد الأمر تعقيدا هو أن جريمة الإنترنت عادة ما تتم عن بعد حيث لا يتواجد الفاعل على مسرح الجريمة ومن ثم تتباعد المسافات بين الفعل والنتيجة.[3]

4-أضف إلى ذلك نقص خبرة الشرطة في وجهات الإدعاء والقضاء فيجب أن يكون الجهاز المختص بالبحث والتحري، عن جرائم الإنترنت بصفة خاصة والجرائم المعلوماتية بصفة عامة ويتمتع بمهارات خاصة تتماشى مع التقنية التي يتعامل بها، وأن يتم تدريبه على استخدام أساليب وتقنيات تحقيق جديدة ومبتكرة تتماشى مع الجرائم المستحدثة تعتمد على التقنية والتكنولوجيا.

5-كما يعني مأمور الضبط القضائي فكثيرا ما يجدون أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية، مع هذه النوعية من الجرائم وكثيرا ما يفشلون في تقدير الأهمية تلك الجريمة لنقص الخبرة بالتدريب ومما يزيد من صعوبة هذا الأمر أنه كثيرا ما يساهمون نظرا لنقص خبرتهم في تدمير دليل الإدانة.

وبذلك فهذه الصعوبات والتحديات كان من الممكن تجنبها إذا درب مأموري الضبط القضائي والمحققين تدريبا كافيا على التعامل، مع مثل هذا النوع من الجرائم وبذلك يمكن

---

[1]- هشام محمد فريد رستم، **الجرائم المعلوماتية أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين** ، المرجع السابق، ص18.

[2]- عبد الله حسين علي محمود ، **سرقة المعلومات المخزنة في الحاسب الآلي**، المرجع السابق، ص364 وما بعدها.

[3]- عبد الله حسين علي محمود ، المرجع نفسه، ص351 وما بعدها.

استخلاص قاعدتين جوهريتين يجب على أجهزة الضبط والتحقيق مراعاتها أثناء بحثهم وتحريهم وتحقيقهم في جرائم الإنترنت [1] وهي:

-ضرورة عدم إدخال أي تعديل على الوضع الذي يوجد عليه الحاسب الآلي.

-عدم السماح للمتهم باستخدام الحاسب موضوع الجريمة أو أي حاسب آخر متصل بالشبكة.

المطلب الثاني: دور شرطة الإنترنت كضبطية مختصة في البحث والتحري عن جريمة الإنترنت

إن الدولة الحديثة تتميز بأنها دولة قانون كونها تخضع سائر سلطاتها إلى مبدأ المشروعية بحيث تكون تصرفات تلك السلطات محكومة داخل إطار قانوني، محدد لها سلفا لا تستطيع الفكاك منه[2] ولما كان الأصل هو التمتع بالحرية والاستثناء هو القيد أو القيود ، وجب أن تخضع هذه القيود إلى ضوابط تمنع أو تحد من التعسف في ممارسته، فالقانون هو من يضمن التكامل بيم مصلحة كل من الفرد في حماية حريته والجماعة في تحقيق أمنها واستقرارها داخل الدولة .

فقد يقتضي هذا التنسيق في بعض الأحوال المساس بالحرية الشخصية للفرد أو بحقوقه وحرماته فيكون هذا المساس متمثلا في صورة القبض، أو التفتيش سواء كان محله الشخص أو المسكن مما يشكل انتهاكا لحقوقه وحرماته ففي مثل هذه الأحوال يصبح الفرد أحوج ما يكون إلى الحماية، ومهمة المشرع في أن يصنع الضمانات ما يكفل أن يكون المساس بحقوق الفرد وحرماته في أقل الحدود وما يلزم لتحقيق الصالح العام في كشف الحقيقة عن الجريمة وتحديد مرتكبيها .[3]

---

[1]- نبيلة هبة هروال، **الجوانب الإجرائية لجرائم الانترنت**، المرجع السابق، ص174.

[2]- جمال جرجس مجلع تاوضروس، **الشرعية الدستورية لأعمال الضبطية القضائية** ، النسر الذهبي للطباعة عابدين، مصر، 2006، ص27.

[3]- عبد الله ماجد العكايلة، **الوجيز في الضبطية القضائية** ، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 35.

ولكي لا يساء استعمال الحقوق والحريات أو التعدي عليها وجب على السلطة العامة إيجاد هيئة تحفظ للنظام صفة الالتزام والتي يعبر عنها بالضبطية، والتي لها نوعان متمثلان في الضبطية الإدارية والضبطية القضائية إلا أن قانون الإجراءات الجزائية لا يحفل إلا بالضبطية القضائية لوحدها.[1]

ويكمن عمل رجال الضبطية القضائية في البحث والتحري عن الجرائم ومرتكبيها، فمهمتهم الأساسية تنحصر في البحث والتحري إذا لم يبدأ التحقيق ن أما إذا بدأ، فيقع عليهم تنفيذ الأوامر الصادرة إليهم سواء كان الأمر صادر من القانون أو مصدره سلطة قضائية، إما قاضي التحقيق عن طريق الإنابة أو عن طريق جهة أخرى ليكون عملهم مشروعا .

وتلعب الشرطة القضائية دورا هاما في البحث عن الجرائم وجمع الأدلة عنها وهذا الدور يشكل الوظيفة الأساسية لها، وبذلك قام المشرع الجزائري بتحديد الدور الذي تلعبه الشرطة القضائية كضبطية مختصة في مواجهة الجرائم سواء كانت هذه الأخيرة تقليدية أو حديثة، وعليه فإننا قسمنا هذا المبحث إلى مطلبين: الأول يتضمن دورها كضبطية إدارية وقائية والثاني دورها كضبطية قضائية.

الفرع الأول :دور شرطة الإنترنت كضبطية إدارية وقائية

نظرا للمرونة التي يتسم بها الضبط الإداري كان من الصعب على الفقه والقضاء الإداري وضع تعريف محدد له، وهذا نظرا لاختلافهما في وضع المعايير التي تميز بينه وبين الأنظمة المشابهة له، كالضبط القضائي على سبيل المثال، غير أنهما أجمعا على تقسيمه إلى ضبط إداري عام وآخر خاص. لذلك سنضمن هذا المطلب إلى وضع تعريف للضبط الإداري وفقا لبعض الفقهاء وذكر خصائصه وتقسيماته، كما سنتطرق لاحقا للضبط الإداري المختص بمكافحة جرائم الإنترنت.

[1]– نصر الدين هنوني ودارين قدح، المرجع السابق، ص15 .

الضبط الإداري المختص بمكافحة جرائم الإنترنت

كما هو الشأن في تعريفه في جرائم الإنترنت بأنه يقوم بدور فعال في مكافحة جرائم الإنترنت إذ وكما سبق ذكره أنفا ولما كانت صلاحياته تتمركز حول الوقاية من الإجرام، وذلك من خلال اتخاذ كافة الإجراءات والوسائل للحيلولة دون وقوع ذلك الأخير عن طريق حفظ النظام بعناصره الثلاث "الأمن العام والسكينة العامة والصحة العامة، ولما كانت هناك إمكانية الجمع بين أعمال الضبط القضائي والإداري معا كتلك الحالة التي يتم فيها تفتيش الحقائب عبر المنافذ الجمركية فيتم اكتشاف جريمة أثناء هذا التفتيش كان من المنطقي أن يكون هناك محل لعمل الضبط الإداري في العالم الافتراضي".[1]

وعليه فان الضبط الإداري المختص بمكافحة جرائم الانترنت يهدف إلى الحد من هذه الجرائم من خلال تحديدها وإقرار العقوبات المحددة لها، من خلال المساعدة على نشر الأمن المعلوماتي، وحفظ الحقوق التي تترتب على استخدام شبكة الانترنت والحاسب الآلي بطرق مشروعة، وحماية المصلحة والآداب العامة.

ومع هذا التطور الحاصل، تم وضع أجهزة للشرطة مسخرة للقيام بدوريات في غرف الدردشة لمراقبة كل ما يجري بداخلها، ولها في ذلك جميع الصلاحيات اللازمة للوقاية من كافة صور الإجرام. ومن بين تلك الصلاحيات، إجراء التفتيش الذي يقوم به مأمور الضبط القضائي على أجهزة الحاسب الآلي في مقاهي الانترنت أو إحدى المؤسسات بقصد التأكد من صلاحية البرمجيات، وإذ به يكتشف عدم صلاحيتها مع وجود برمجيات أو صور إباحية.[2]

أما من ناحية أخرى فان بعض العاملين في بيئة الإنترنت يتمتعون بصفة الضبطية الإدارية، كمزودي الدخول و مقدمي خدمات الإنترنت، إذ أن أعمالهم ووفقا للقانون تمنح لهم الصلاحية في الرقابة عبر المزود عن سير حركة العمل ومدى خضوع العاملين والمتعاملين مع الإنترنت للنظام

[1]- نبيلة هبه هروال، **الجوانب الإجرائية لجرائم الانترنت**، المرجع السابق، ص 86.

[2]- نبيلة هبه هروال،المرجع نفسه، ص86.

والقانون، بحيث أنه إذا حدث ووجدت الجريمة باكتشافها بهذا الأسلوب، فانه ليس لرجال الضبط الإداري سوى التحفظ على أدلة الجريمة لغاية وصول رجال الضبط القضائي[1].

والى جانب الإجراءات المتخذة من قبل رجال الضبط الإداري في التصدي أو منع جرائم الإنترنت مبكرا، هناك إجراءات بها العاملون بالمنشئات الحيوية، والتي تسمى "أمن المعلومات"، والتي هي عبارة عن احتياطات وإجراءات تتخذها الإدارات الحديثة لمنع وقوع الجريمة، وذلك من خلال تحديد المعلومات الهامة، ثم تحليل المخاطر والتهديدات والقابلية للعدوان، ثم تطبيق الإجراءات المضادة لتصل إلى مرحلة التقييم[2].

ويلاحظ أن دور كل موظف في تطبيق هذه الاحتياطات يتم تحديده مسبقا وفقا لنوع الجريمة التي تهدد المنشأة. فأما ما يخص جرائم الانترنت فنجد أن هناك موظفين يقتصر دورهم على مجرد الإبلاغ عن حدوث أي اعتداء على أنظمة الحاسبات الآلية التي يتعاملون معها، وهناك موظفون آخرون، والذين يختصون بالمواجهة الفعلية عند حدوث أي اعتداء كان"[3].

وعليه ومما سبق تناوله في هذا المطلب من مفهوم الضبط الإداري من جانبه الفقهي، وذكر الخصائص التي يتسم بها، وكذا الضبط الإداري المختص بجرائم الانترنت ودوره والعاملين بالمنشئات الحيوية في التصدي أو منع وقوع جرائم الانترنت، فإننا سنوضح فيما يلي دور القضائي في مكافحة هذا النوع من الجرائم التي هي محور دراستنا، وهذا وفق ما يلي:

الفرع الثاني: دور شرطة الإنترنت كضبطية قضائية

لاشك أن التطور المستمر في تكنولوجيا المعلومات جعل مهمة رجال الضبطية القضائية في اكتشاف الجرائم المتعلقة بالانترنت أصعب من ذي قبل، إذ لا يكفي أن يكون رجال الضبطية

---

[1]- نبيلة هبه هروال، المرجع السابق، ص87.

[2]- أيمن عبد الحفيظ عبد الحميد سليمان، **إستراتيجية مكافحة جرائم الحاسب الآلي دراسة مقارنة** ، رسالة دكتوراه، أكاديمية الشرطة، بدون سنة، ص374 وما بعدها.

[3]- نبيلة هبه هروال، **الجوانب الإجرائية لجرائم الانترنت**، المرجع السابق، ص ص87-88.

القضائية ملمين بالجوانب القانونية فحسب، بل يجب أن تكون لديهم الخبرة اللازمة للتعامل مع مثل هذه الجرائم.

وعليه سنتطرق إلى الضبط القضائي بصفة عامة في الفرع الأول، وكذا الضبط القضائي المختص بجرائم الإنترنت في الفرع الثاني.

أولا: الضبط القضائي المختص بمكافحة جرائم الإنترنت

أ-كما سبق ذكره أعلاه لم تسلم الضبطية القضائية من التطور التكنولوجي، وما افرزه من إجرام مستحدث، إذ نتج عن ذلك نوع من التحدي الكبير لأجهزة العدالة الجنائية: أجهزة التحقيق وأجهزة القضاء وأجهزة ضبط الجرائم والمتمثلة في رجال الضبطية القضائية، إذ أصبح هؤلاء عاجزين عن الكشف عن مثل هذه الجرائم، نظرا لما تتميز به من خصائص ترجع إلى طبيعتها الخاصة وما يكتفها من تعقيد، فضلا عن عجزهم عن ملاحقة مرتكبيها.

ولقد أثير في المؤتمر الدولي لجرائم الحاسوب المنعقد في أوسلو/النرويج في الفترة ما بين 29-2000/5/31، موضوع عدم إمكانية البنية التحتية للإنترنت من التوصل إلى تحديد شخصية مرتكب الجريمة، أو المصدر الحقيقي لها، وموقعه على وجه التحديد، وإن كانت توفر إمكانية التعرف على عنوان ورقم الحاسوب فقط المرتبط بالإنترنت والمستعمل كوسيلة لارتكاب الجريمة، أي ما يطلق عليه في النظام التقني (IP) Internet Protocol. وبالتالي تحديد الشخص صاحب ذلك الرقم بسهولة، لتبدأ بعد ذلك سلسلة إثبات ارتكابه للجريمة من عدمه. ولكن في مقابل ذلك، فإن هذا الرقم ليس موحدا على المستوى العالمي، إذ أن هناك أقلية من الدول التي تتبعه دون غيرها وخاصة الدول العربية[1] .

ولذلك كان من الضروري إعداد وتجهيز قوات خاصة (forces spéciales) لمواجهة هذا العدوان الإلكتروني عبر الإنترنت، والذي أصبح أحد الهواجس التي تعيشها المجتمعات المتقدمة

[1]- عمر محمد أبو بكر بن يونس، **الجرائم الناشئة عن استخدام الإنترنت**، دار النهضة العربية، القاهرة، مصر، 2004، ص811.

والنامية. وهذا ما توصلت إليه دول كثيرة، وجاءت به توصية المجلس الأوروبي رقم ر (95) 13 في 1995/09/11 في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، إذ دعت إلى ضرورة تشكيل وحدات خاصة لمكافحة جرائم الحاسب الآلي وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات[1].

وكذلك ما دعا إليه وزير الداخلية الفرنسي السابق Villepin Dominique de.[2]

وأيضا ما وصى عليه المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة ما بين 25-1993 /10/28.[3]

ب-إن المشرع الجزائري يكون قد سارع على تدارك النقص وسد الفراغ القائم بخصوص مجالات التحقيق الابتدائي إثر التطور الذي عرفته الجريمة بأشكالها الحديثة كما هو الحال في جرائم الإنترنت لذلك جاءت تعديلات قانون الإجراءات الجزائية متعاقبة سيما التعديل الذي جاء به القانون 06-22 المؤرخ في 2006/12/20 والذي مدد من صلاحيات الضبطية القضائية ووسع دائرة اختصاصها ودعمه في ذلك القانون رقم 09-04 المؤرخ في 2009/08/05 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كما سوف نرى.

---

[1] - عبد الله حسين على محمود، **سرقة المعلومات المخزنة في الحاسب الآلي**، ط2، دار النهضة العربية، القاهرة، مصر، 2002، ص354.

[2] Le ministre de l'intérieure français a déclaré : « j'entends créer des cyber-patrouilles de la toile en donnant aux services de police et de gendarmerie les moyens de détecter et d'infiltrer les sites qui diffusent des contenus inacceptables, qu'il s'agisse de pédopornographie ou d'appels à la haine raciale » Jed All : une cyber-patrouille de police sur internet, publié le 25 mars 2005, disponible en ligne à l'adresse suivante : http://aliquid.free.fr .

[3] - علاء الدين محمد شحاتة، **رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي** ، المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في الفترة ما بين 25-1993/10/28، **مشكلات المسؤولية الجنائية في مجال الجرائم الواقعة على البيئة، الجرائم الواقعة في مجال التكنولوجيا المعلومات**، دار النهضة العربية، القاهرة، مصر، 1993، ص587.

أناط القانون الجزائري بالضبطية القضائية مهمة البحث والتحري عن الجرائم المحددة في قانون العقوبات تماشيا مع المبدأ الدستوري المتعارف عليه لا جريمة ولا عقوبة إلا بالنص[1] وذلك في مرحلة أولية قبل أن يباشر بشأنها التحقيق القضائي ويتضح من نص المادة 12 من قانون الإجراءات الجزائية أن مناط البحث عن الجرائم بالنسبة للضبطية القضائية ينحصر في جمع الأدلة والبحث عن مرتكبي تلك الجرائم فإذا ما ابتدأ التحقيق القضائي تقلص دورها لينحصر في تنفيذ طلبات جهات التحقيق القضائي وإنجاز ما توجه إليه من طلبات ويدير وكيل الجمهورية إدارة الضبط القضائي بما في ذلك تنقيط ضباط الشرطة القضائية والذي يؤخذ في الحسبان عند الترقية.[2]

كما تنص عليه المادة 18 مكرر من قانون الإجراءات الجزائية في إطار الصلاحيات المحدد في نص المادة 36 من قانون الإجراءات الجزائية وكل ذلك تحت إشراف النائب العام وتحت رقابة غرفة الاتهام بدائرة اختصاص المجلس التابعين له وفقا لأحكام المادة 206 من قانون الإجراءات الجزائية نفسه ما عدا ضباط الشرطة التابعين للأمن العسكري يؤول الاختصاص بشأنهم إلى غرفة الاتهام في جزائر العاصمة وفقا في نص المادة 207 لقانون الإجراءات الجزائية.

ومعلوم أن ضباط الشرطة القضائية نوعان: النوع الأول وهم الذين يتمتعون باختصاص عام ويختصون بإجراءات الاستدلال بشان الجرائم المنصوص عليها في قانون العقوبات، أما النوع الثاني فهم ذو الاختصاص النوعي المحدود بخصوص نوع معين من الجرائم حددها قانون على سبيل الحصر وهؤلاء هم المشار لهم بنص المادة 21 من قانون الإجراءات الجزائية وسلطتهم كذلك محدودة لا تمتد إلى مرحلة التفتيش ودخول منازل والمعامل والمباني أو الأفنية أو الأماكن المحاطة بأسوار إلا بحضور احد ضباط الشرطة القضائية.[3]

لم يشذ المشرع الجزائي عن قواعد العامة المنصوص عليها في قانون الإجراءات الجزائرية لكنه أرسى قواعد جديدة ذات طبيعة خاصة كان من اللازم أن تلد مع التطور الحاصل في حقل جريمة

---

[1]- المادة 46 من الدستور الجزائري.

[2]- زبيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، دار الهدى، عين ميلة، الجزائر، 2011، ص116.

[3]- زبيحة زيدان، المرجع نفسه، ص116.

الإنترنت كظاهرة حديثة وبهذا الصدد جاء القانون رقم 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الأعلام والاتصال ومكافحتها ومن هذا نصت عليه المادة 03 منه مما تتطلبه مستلزمات التحريات أو التحقيقات القضائية وهي وضع ترتيبات تقنية هدفها مي يلي:

- مراقبة الاتصالات الإلكترونية.
- تجميع تلك الاتصالات الإلكترونية.
- وتسجيل الاتصالات الإلكترونية في حينها.
- القيام بإجراءات التفتيش للمنظومة المعلوماتية.
- القيام بإجراءات الحجز داخل المنظومة المعلوماتية.

يضاف إلى ذلك ما نصت عليه المادة 65 مكرر 05 من قانون الإجراءات الجزائية من إجراءات مخولة للنيابة وهي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية التالية ودون موافقة المعنيين للوصول إلى ما يلي:

أ. التقاط الكلام:

- تثبيت وتسجيل الكلام في المواصفات التالية:
- المتفوه به من طرف أي شخص.
- بين عدة أشخاص.
- سواء كان الكلام بصفة خاصة أو سرية.
- في أماكن خاصة أو عمومية.

ب. التقاط الصور في المواصفات التالية:

- لشخص.
- لعدة أشخاص.

– في مكان خاص.[1]

ثم كيف يتم وضع تلك الترتيبات التقنية:

1 –السلطة المخولة بتسليم الإذن:

أ. في مرحلة التحري والتحقيق الابتدائي.

ب. في مرحلة التحقيق القضائي.

2 – تقنيات عمليات التحري والتحقيق بالتسرب:

–تعريف التسرب.

–السلطة المخولة بمنح الإذن بالتسرب.

–خصوصيات الإذن بالتسرب.

–الأعمال الملخص بها للمتسرب.

إن ما يجب التنويه به ونحن بصدد توضيح وتدقيق العناصر المذكورة بات من الصعوبة بمكان التوفيق من مبدئي الحفاظ على النظام العام وعدم المساس بحرمة الحياة الخاصة للأشخاص وشرفهم في إطار تنفيذ مستلزمات التحريات والتحقيقات القضائية كما جاءت بها المادة 03 من قانون رقم 09-04 المشار لها سيما وأن حرية المواطن وحقوقه محمية دستوريا ولا يسمح الدستور بالتجسس أو التنصت عليها.

وإذا كان القانون 09-04 المتعلق بقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال قد عرف في المادة الأولى منه مفهوم الاتصالات الالكترونية بأنها (أي اتصال أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية) فإن القانون نفسه حدد على سبيل الحصر الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الالكترونية وذلك حسب ما أوردته المادة 4 كما يلي:

أ.للوقاية من الفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

[1] – زبيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، المرجع السابق، ص121.

ب.في حالة توفر على احتمال اعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ج.لمقتضيات التحريات و التحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الالكترونية.

د.في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة مما يتعين الإشارة به هناك أنه وبصدد الفقرة ألف (أ) أعلاه.

لا يفوت التذكير بان جرائم الإرهاب أخذت حيزا هاما من اهتمامات المشرع الجزائري إذ بالإضافة إلى ما أوردته المادة 87 مكرر من قانون العقوبات يأتي قانون رقم 06-01 المؤرخ في 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته ليدعم الإجراءات الخاصة بأعمال التحري والبحث عن الجرائم الإنترنت وتقفي آثار المجرمين المحد من نشاطهم والقبض عليهم وبهذا الصدد حددت المادة 56 من هذا القانون بعض التدابير في مجال التحري وجمع الأدلة منها ما يلي:

-اللجوء إلى تسليم المراقب.

-إتباع أساليب التحري الخاصة مثل:

أ. الترصد الإلكتروني.

ب. الإختراق.

المبحث الثاني: شرطة الإنترنت على المستوى الوطني والدولي

لقد تولد عن ظهور الإنترنت إجرام من نوع مميز، أصبح يهدد دول العالم بأكملها دون استثناء، ولقد شهدت السنوات الأخيرة تزايدا كبيرا في كم ذلك الإجرام بشتى أشكاله، سواء تلك المتعلقة بالجرائم الجنسية أو بجرائم السب والقذف أو بجرائم السرقة والاحتيال...

وأمام هذا التزايد المستمر والمتضاعف لهذا الإجرام قررت الدول وضع حد له وذلك عن طريق تجهيز أجهزة لمكافحته ومن بين تلك الأجهزة إعداد شرطة متخصصة لمواجهته (Anti-haking task) سواء على المستوى الوطني أو الدولي وهذا ما دعت إليه الاتفاقية الأوروبية لجرائم الإنترنت وكذلك المؤتمر المنعقد في السوربون/باريس (Sorbonne- paris) في 2005/1/19 والذي كان موضوعه "الشرطة والإنترنت".[1]

وفيما يلي الإشارة إلى الدول التي وضعت فيها وحدات خاصة من الشرطة لمكافحة جرائم الإنترنت مع التركيز بالأخص على فرنسا وذلك على المستويين الوطني والدولي.

المطلب الأول: على المستوى الوطني

لقد أحدثت جرائم الإنترنت طوارئ في أجهزة القضاء وأجهزة الضبط القضائي والتحقيق لذلك هناك ضرورة لإنشاء أجهزة خاصة بهذه الجرائم تختلف تماما عن الأجهزة الضبط العادية وهو ما جعل اتفاقية بوادبيست للإجرام المعلوماتي تنادى بضرورة إنشاء مثل هذه الأجهزة على المستوى الوطني.

وكذلك سن الإجراءات التشريعية اللازمة لذلك يجب على كل طرف أن يتنبنى من الإجراءات التشريعية أو أي إجراءات أخرى، يرى أنها ضرورية من اجل إنشاء السلطات ووضع

[1] Conférence police et internet, 19 janvier2005, sorbonne, paris, disponible en ligne a l'adresse suivante http://www.isos.fr

الإجراءات المنصوص عليها في الإجراءات الخاصة وكذلك السماح لكل طرف بأن يحتفظ بالحق بعدم تطبيق الإجراءات المنصوص عليها إلا على فئة معينة من الجرائم.[1]

الفرع الأول: الدول الأجنبية

ومن بين الدول التي سعت إلى استحداث وإنشاء أجهزة من اجل مكافحة هذا الإجرام المستحدث هي:

1)الولايات المتحدة الأمريكية:

تعتبر الولايات المتحدة الأمريكية من الدول التي تزداد فيها ظاهرة الإجرام عبر الانترنت وتتضاعف فيها الخسائر الناتجة عن تلك الظاهرة، والتي تلحق بالقطاعات العامة أو الخاصة بذلك فهي تعتبر الدول السباقة في مجال إنشاء أجهزة خاصة للبحث والتحري في جرائم الإنترنت.

ومن بين الوحدات التي أنشأة في الولايات المتحدة الأمريكية نجد المكتب المركزي لمكافحة الجريمة المرتبطة بتكنولوجيا المعلومات والاتصالات، وكذلك قسم جرائم الحاسوب وجرائم الحقوق الملكية الفكرية الذي تم إنشاؤه سنة 1991 والذي يختص بالكشف عن الجرائم الحاسب الآلي وحقوق الملكية وعن ملاحقة مرتكبيها[2] وكذلك معهد أمن الحواسيب.

وكذلك نجد وحدة جرائم الإنترنت وهي وحدة تختص بالتحقيق في جرائم حقوق الملكية الفكرية وفي جرائم المرتبطة بالتقنية العالية، ويترأسها مدير مساعد لمكتب التحقيقات الفيدرالي لها ذات مرتبة وحدة التفتيش الجنائي [3]، ومكتب رئيس التكنولوجيا وهو مكتب مفوض مباشرة من

---

[1]- هلالي عبد الله أحمد، اتفاقية **بوادبست لمكافحة جرائم الإنترنت** ، دار النهضة العربية، القاهرة، مصر، 2007، ص184.

[2]- بدأ هذا القسم موحدة تابعة لوزارة العدل الأمريكية، وفي عام 1996أصبح قسما نتيجة لتضخم أعماله فقد بدأ بخمسة وكلاء نيابة ليصبح عام 2000 أكثر من 20 وكيل نيابة لمزيد من تفاصيل أنظر د/ عمر محمد أبو بكر بن يونس، **الجرائم الناشئة عن استخدام الإنترنت**، دار النهضة العربية، القاهرة، 2004، ص812.

[3]-Cyber police contre cyber crimes mcybercriminalité, le fbi se structure, le canada se prépare, le 15/01/2000, disponible en ligne à l'adresse suivante http://stratégique.free.fr.

مكتب مدير التحقيقات الفيدرالية الأمريكي لتسيير مختلف المشروعات التكنولوجية وملاحقة مرتكبي الجرائم الواقعة في ذلك المجال.

كما تم إنشاء المركز الوطني لحماية البيئة التحتية التابعة للمباحث الفيدرالية الأمريكية في 1998/2/28 والذي يتقاسم مهامه مع وزيرة الدفاع، وهو يتكون من فريق سري يصل عدد أعضائه إلى 125 رجل حكومي.

وتجدر الإشارة إلى أن نشأة هذا الفريق تعود إلى تقرير جمعية العمل حول جرائم الإنترنت والمقدم إلى الرئيس الأمريكي السابق (Bill Clinton) بيل كلينتون، والذي حددت من خلاله البنية التحتية التي تعتبر هدفا للهجومات والاعتداءات عبر الإنترنت والمتمثلة في الاتصالات والكهرباء والغاز والبترول، وسائل النقل والبنوك والمؤسسات الاقتصادية والمياه النقية ومصالح الاستعجال والمصالح الإدارية والاجتماعية.[1]

وإلى جانب الوحدات السابقة فقد تم تأسيس مركز تلقي شكاوي الاحتلال عبر الإنترنت من طرف مكتب التحقيقات الفيدرالي بالاشتراك مع المركز الوطني لجرائم الياقات البيضاء[2](NW3C)، وإنشاء وكالة تابعة لمكتب التحقيقات الفيدرالي إلى جانب المركز الوطني لحماية البنيات التحتية مهمتها التنسيق في مكافحة القرصنة المعلوماتية.

وإلى جانب تلك الأقسام والمراكز هناك وحدة متخصصة تابعة لقسم العدالة الأمريكي مكلفة بمكافحة الإجرام المعلوماتي تتكون من خبراء في تقنيات الحوسبة والإنترنت ومن مستشارين قانونيين[3].

[1]- نبيلة هبة هروال، المرجع السابق، ص 110.

[2]- يقصد بالياقات البيضاء: هو مصطلح غربي يطلق على أولئك الناس الذين يقومون بعمل "ذهني" مكتبي مثل المديرين والمتخصصين، وهم بذلك يتميزون عن أصحاب الياقات البيضاء الذين يقومون بعمل يدوي ميداني كالعمال.

[3]- عمر محمد أبو بكر بن يونس، **الجرائم الناشئة عن استخدام الإنترنت**، المرجع السابق، ص812.

ويجب التنويه إلى أن مكتب التحقيقات الفيدرالي يعتبر في حد ذاته الجهاز القيادي لمواجهة الإرهاب عبر الإنترنت[1].

2)فرنسا:

أما بخصوص فرنسا فهي كغيرها من دول العالم لأم تبقى مكتوفة الأيدي بل سخرت كل قواتها، لمواجهة هذا الهاجس الذي يعيشه هذا العالم، سواء على المستوى الوطني أو الأوروبي فقد قرر وزير الداخلية الفرنسي الأسبق دومنيك دي فالبان (Dominique de villepin) ، بعد إطلاعه على التقرير المقدم لم من قبل وزير المالية من قبل وزير المالية والاقتصاد تيري برتون(Thierry Breton) ، والذي أكد فيه تضاعف كم جرائم الإنترنت بمختلف أشكالها.

ووضح حد لهذه الآفة التي تعاني منها دول العالم عامة وفرنسا خاصة وذلك من خلال اقتراح مشروع قانون يهدف إلى دعم الأمن الداخلي، عن طريق مكافحة الإجرام المرتكب عبر تلك الشبكة وتوفير الأمن المعلوماتي [2] عبرها لمستخدميها الفرنسيين بالإضافة إلى جوانب أمنية أخرى وفي هذا يرى انه يجب إتباع مخطط محكم لتحقيق تلك الأهداف والتي يجب أن يتضمن خطوط عريضة كما يلي:

1.دعم قوات الشرطة والدرك المتخصصين في المكافحة وذلك عن طريق زيادة عددهم:

قرر وزير الداخلية الفرنسي السابق في إطار مكافحته للجرائم الإنترنت، زيادة عدد أفراد الشرطة والدرك المتخصصين في البحث والتحري والتحقيق في هذا النوع من الجرائم، ليصل عددهم سنة 2008 إلى 600 شرطي ودركي إلى جانب حسن تنظيم أشغالهم وتقوية قدراتهم القانونية في التحقيق، وفي مراقبة كافة أشغال العدوان الالكتروني التي يمكن أن ترتكب أو تكون تلك الشبكة محلا لها كالإرهاب والقرصنة المعلوماتية والعنصرية والسامية وإرهاب الأجانب.

[1]– عمر محمد أبو بكر بن يونس، المرجع نفسه، ص812.

[2]–يتم توفير الأمن المعلوماتي عن طريق توفير امن تبادل المعلومات ومكافحة الاحتيال عبر تلك الشبكة وكذلك محاربة الاستغلال الجنسي عبرها.

وفي هذا الإطار نجد وزير الداخلية الفرنسي السابق يقترح خلق وسائل خاصة للتحقيق تمكن من اكتشاف الجرائم الخطيرة في الوقت المناسب، فمثلا يمكن للمحققين أن يشاركوا تحت اسم مستعار في المحادثات الإلكترونية بدون أن يكونوا مسئولين جنائيا.[1]

وإلى جانب ذلك نجد وزير الاقتصاد والمالية تيري برتون (Thierry Breton) في تقريره المقدم إلى وزير الداخلية السابق يقترح إضافة مادة من مشروع قانون الرقابة من الانحراف لتسهيل التحقيق وإجراءاته في جرائم الإنترنت.

وذلك كما يلي مكمن لرجال ومأموري الضبط القضائي المختصين في البحث عن الجرائم المشار إليها في المواد 227-18 إلى 277-24 من قانون العقوبات الفرنسي [2] إذ ما ارتكبت بواسطة وسيلة اتصال عامة على المباشر دون أن تترب عليهم مسؤولية جنائية القيام بالأعمال التالية:

-المشاركة تحت اسم مستعار في المحادثات الالكترونية.

-الاتصال باستخدام تلك الوسيلة بالأشخاص المشتبه في ارتكابهم لهذه الجرائم.

-التحفظ عن المحتويات غير المشروعة وفقا لشروط المحدودة في مرسوم.

2.تكوين شبكة خبراء من الشرطة والدرك (Réseau d'experts police-gendarme):

كما قرر كما قرر وزير الداخلية تطوير تكوين رجال الشرطة والدرك المتخصصين في التحقيق في هذا الإجرام تماشيا مع سرعة التطوير التكنولوجي، الذي يشهده العالم وفي هذا يعلن وزير الداخلية الفرنسي السابق أن الشرطة والدرك سيستفيدون من تكوين يتلاءم مع هذا النوع من الإجرام عن طريق عقد مؤتمر للإنترنت (forum d'internet) مشترك ومؤمن يبدأ قبل نهاية يونيو 2005 حتى يتمكنوا من اقتسام المعلومات التقنية والقانونية.

---

[1]-Le portail des sciences sciences : le nombre d'enquêteurs spécialisés en cybercriminalit é va doubler en France, disponible en ligne à l'adresse précédente.

[2]- ينظر مواد من 227-18 إلى 227-24 من قانون العقوبات الفرنسي.

ويهدف ذلك تكوين غلى فهم طريقة تفكير المنحرفين عبر الإنترنت وبالتالي تسهيل عملية الكشف عن جرائمهم والقبض عليهم، ولتجسيد ذلك على ارض الواقع قام وزير الداخلية الفرنسي السابق بالإعلان عن إنشاء شبكة للخبراء تضم رجالا من الشرطة والدرك تتقاسم فيما بينها اختصاص المكافحة، بالإضافة إلى توفير رقابة تكنولوجية خاصة تستخدم فيها طرق حديثة للتنقيب والتحقيق تتماشى مع التطوير الذي يشهده وسائل المعلوماتية.[1]

كما يتم عقد ندوة سنوية مشتركة بالتنسيق بين رجال الشرطة القضائية ورجال الدرك الوطني تضم كل سنة مجموعة من المحققين المختصين، في مكافحة جرائم الإنترنت من اجل مناقشة الإجرام المعلوماتي ووضع حلول له سواء من الناحية النظرية أو التطبيقية وغلى جانب ذلك تنظم أيام دراسة ذات مستوى الآلي لهؤلاء المحققين.

من قبل المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات (OCLTIC) والشرطة القضائية ومعهد البحوث الجنائية التابع للدرك الوطني (I.R.C.G.N) يتم فيها مناقشة مواضيع ذات الأهمية كالمشاكل في الإيصال اللاسلكي والتعريفات القانونية للاتصالات الإلكترونية...الخ.

وإضافة إلى كل ذلك لقد أنشئت عدة وحدات ومراكز متخصصة وغير متخصصة ضمن الشرطة والدرك الوطني في فرنسا، لمكافحة هذا الإجرام المستحدث بجميع صوره وهذا ما أشارت إليه الاتفاقية الأوروبية لمكافحة جرائم الإنترنت والتي وقعت وانضمت غليها فرنسا وصادقت على سريانها في أرضها وكذلك وزير الداخلية الفرنسي من خلال مخططه في مكافحة هذه النوعية من الإجرام ومن ابرز هذه الوحدات هي:

أ.المراكز المتخصصة على مستوى مصالح الشرطة:

ونجد على هذا المستوى حوالي 50 محققا وتحريا متخصصا في البحث والتحري عن الإجرام المعلوماتي وذلك كما يلي:

[1]-Myriam Berbera : le gouvernement français passe à la vitesse supérieure, article publié le 08/09/200 disponible en ligne l'adresse précédente http://www.rfi.fr .

❖ **القسم الوطني لقمع جرائم المساس بالأموال والأشخاص D.N.R.A.P.B :**

ويتكون هذا القسم في مجموعه من ستة محققين ومتحرين متكونين ومتخصصين في التحقيق في بيئة الإنترنت (العالم الإفتراضي)، ولقد بدأ هذا القسم مهامه عام 1997 وهو يشهد منذ ذلك التاريخ إرتفاعا هائلا في عدد البلاغات التي تصل إليه من جراء الجرائم التي تقع في تلك البيئة إذ وصل عام 2004 إلى 3000 بلاغ.

وتجدر الإشارة إلى أن البلاغات التي تصل إلى القسم **D.N.R.A.P.B** تكون نتيجة للحجز على عناوين الـ IP (Adresse)، وأرقام بطاقات الائتمان من قبل السلطات التي تحليها بدورها إلى السلطات الوطني عن طريق قنوات التعاون القضائي الدولي.[1]

❖ **المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات O.C.L.C.T.I.C:**

يعتبر هذا المكتب سلاح الدولة الفرنسية في مكافحة جرائم الإنترنت أساسا إلى جانب وحدات أخرى، ولقد تم إنشاؤه بموجب مرسوم بيوزاري [2] رقم 2000-405 المؤرخ في 2000/05/15 على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية.

يساعده في نشاطه كل من وزارة الدفاع (المديرية العامة للدرك الوطني) ووزارة الاقتصاد والمالية والصناعة (المديرية العامة للجمارك والحقوق غير المباشر، والمديرية للمنافسة والاستهلاك وقمع الاحتيال)، وهو يتمتع كغيره من المكاتب المتخصصة باختصاص وطني يتحدد نطاقه في الجرائم الخاصة والمرتبطة بتكنولوجيا المعلومات والاتصالات سواء أكانت تلك التكنولوجيا محلا للاعتداء أو وسيلة لارتكاب وتسهيل ارتكاب ذلك الاعتداء.

[1] Recommandation du forum des droits sur l'internet : les enfants du net ii, 25/01/2005, disponible en ligne à l'adresse http://www.fouruminternet.org .

[2] – يقصد بالمرسوم البيوزاري: (Décret Interministériel) قرار تشترك في إصداره عدة وزارات.

ب.المراكز الغير متخصصة على مستوى الشرطة والدرك:

وإلى جانب المراكز المتخصصة لمكافحة جرائم الإنترنت لفرنسا توجد وحدات شرطية أخرى وبالرغم من عدم تخصصها في تلك المكافحة إلى أنها تساهم فيها بقدر لا يمكن إنكاره منها:

—الإدارات الإقليمية على مستوى مصالح الشرطة القضائية.

— الإدارات الإقليمية لفريق حماية الأحداث.[1]

الفرع الثاني: الدول العربية

باعتبار جرائم الإنترنت من الجرائم المستحدثة والعابرة للحدود فإن معظم الدول سواء المتقدمة أو النامية، العربية أو الأجنبية أصبحت تخشاها وتعاني منها لذلك كان من الواجب إيجاد جهاز لمكافحتها والحد من خطورتها وبذلك انتهجت معظم الدول العربية بنظام الرقيب (Proxy)، وذلك من اجل الرقابة على تلك الشبكة عن طريق القيام بمراجعة نوعية الخدمات المقدمة عبر تلك الأخيرة لمنع ظهور أي من تلك الخدمات المحظورة.

1)في مصر:

تعتبر جمهورية مصر العربية من الدول التي تعاني من جرائم الإنترنت وأصبحت تخشاها وبذلك قامت بإصدار قانون 63 لسنة 2015 والمتعلق في مكافحة جرائم تقنية المعلومات، من أجل مكافحة تلك الجريمة بتوقيع عقوبات حول مرتكبيها كما أنها قامت بإنشاء بعض أجهزة التي تخص بمكافحة هذا الإجرام المستحدث ومن بين تلك الأجهزة هي:

أ.الإدارة العامة للمباحث الأموال العامة:

والتي تضطلع بمكافحة الجرائم الاقتصادية بصفة عامة والمستحدثة بصفة خاصة باعتبارها إحدى الروافد الرئيسية لقطاع الأمن الاقتصادي، ومن أكثر تلك الجرائم المكافحة جرائم التزوير العملات الورقية التي يكون الحاسب الآلي أداة لارتكابها.[2]

---

[1] نبيلة هبة هروال، المرجع السابق، ص133

[2] أيمن عبد الحفيظ عبد الحميد سليمان، **إستراتيجية مكافحة جرائم الحاسب الآلي دراسة مقارنة**، المرجع السابق، ص452.

ب.الإدارة العامة للتوثيق والمعلومات:

تعتبر هذه الإدارة من أكبر الإدارات بوزارة الداخلية تعاملا مع الجرائم المعلوماتية وهي في ذلك تختص بعمليات المتابعة الفنية لكثير من الجرائم، ويبدأ عملها من خلال المتابعة الفنية والتحري عن الجرائم المبلغ عناه من الإدارات الأخرى وذلك من خلال استخدام شبكة الإنترنت وتحديد شخص المتهم.

هذا من جهة ومن جهة أخرى فهي تقوم بتحديد ذلك المتهم من خلال عملية التتبع ويعتمد أسلوب عمل هذه الإدارة في معرفة شخص مرتكب الجريمة، عن استخدام البرامج الحديثة وذلك عن طريق الاعتماد على رقم (IP) الذي يتعامل من خلاله الشخص مع شبكة الإنترنت.

وتعد جرائم السرقة التي ترتكب باستخدام كارت الفيزا من أكثر الجرائم التي تسعى الإدارة العامة للمعلومات والتوثيق إلى ضبطها.

ج.الإدارة العامة المصنفة الفنية:

وهي تهتم بحماية الملكية الفكرية وحرية الإبداع والتعبير من أي أعمال غير المشروعة كالنسخ والتقليد وهي تقوم بذلك انطلاقا من تلقيها إخطار (بلاغ أو شكوى)، عن وقوع مثل ذلك الجرائم لتبدأ في التحري والتفتيش والتحفظ على ما تحصلت عليه من وسائط منسوخة وكذا الأجهزة المستخدمة في عمليات النسخ وتجدر الإشارة إلى أن الإدارة العامة للمصنفات الفنية تقوم بحملات تفتيشية كبيرة في جميع أنحاء الجمهورية لضبط تلك الجرائم.[1]

2)في الإمارات العربية المتحدة:

شكلت شرطة أبو ظبي فرقا متخصصة لمكافحة الجرائم الإلكترونية تستقبل البلاغات وتضطلع بمهمة البحث عبر المواقع الإلكترونية وحجبها إن كان إباحية، فضلا عن تشكيل الشرطة فرقا ميدانية للبحث والتحري لبعض البلاغات أو ورود أي معلومات لحدوث جريمة تتطلب مزيدا من البحث خارج نطاق مكتب إدارة التحريات والمباحث الجنائية في شرطة أبو ظبي.

[1]- أيمن عبد الحفيظ عبد الحميد سليمان، المرجع نفسه، ص455.

وقال العقيد الدكتور راشد محمد بورشيد رئيس قسم الجريمة المنظمة في الإدارة في تصريح لـ الإتحاد إن الجريمة الإلكترونية، هي التي يتم ارتكابها من خلال الاستخدام أو الاستغلال غير الشرعي لأجهزة الحاسوب أو تقنية المعلومات والتي نص عليها القانون الاتحادي رقم (2) لسنة 2006.[1]

ولوحظ إلى أن الجرائم الإلكترونية تختلف أشكالها ليس كما يعتقد البعض أنها محدودة بل تبدأ من السب والتشهير وانتحال الشخصية، وتزوير البطاقات الائتمانية، مرورا بالابتزاز والنصب والاحتيال، والقرصنة الالكترونية والتصيد عبر الإنترنت.

وأضاف انه يمكن للجمهور من المواطنين والمقيمين التواصل مع الشرطة في حال تعرضهم للجرائم الالكترونية، وذلك من خلال غرفة العمليات المركزية (999) أو عن طريق الدوريات الالكترونية في حالة وجود أي معلومة أو خبر قد يسبب جريمة في حد ذاتها وأيضا هناك المصادر السرية.

وبالنسبة لمواجهة هذه الجرائم وطرق محاربتها قال رئيس قسم الجريمة المنظمة في إدارة التحريات والمباحث الجنائية في شرطة أبو ظبي، إن طرق المواجهة تكون عبر استخدام برامج الحماية والتوعية باستخدام شبكة الإنترنت بطريقة آمنة وتغيير كلمات السر بشكل دوري والتبليغ عند الريبة أو الشك في أي موقع وجهة إلكترونية غير قانونية والإشراف العائلي في حال استخدام الأطفال للإنترنت.

وعن الخطوات التي يجب اتخاذها حين وقوع شخص ضحية للنصب إلكترونيا، أوضح أن هناك العديد من الخطوات التي يجب على أي شخص إتباعها في حال وقوعه ضحية إحدى الجرائم الإلكترونية، سرعة إبلاغ غرفة العمليات المركزية (999)، أو التوجه إلى أقرب مركز شرطة أو إلى إدارة التحريات والمباحث الجنائية (قسم الجريمة المنظمة – فرع الجرائم الإلكترونية) أو

[1]– مقالة احمد عبد العزيز، تاريخ النشر 13 فبراير 2002 على الموقع http://www.alittihad.ae

الاتصال بهاتف رقم (025127777) أو الاتصال على خدمة أمان الإلكترونية (8002626) التابعة لشرطة أبو ظبي.

3)في الجزائر:

إن الجزائر ومدى مسايرتها للتطور التكنولوجي وما تشهده هي الأخرى من أنواع مختلفة من جرائم الإنترنت كانت دائما في الواجهة ومسايرة لما تواجهه الدول التي تضررت مبكرا من هذا النوع من الإجرام فقد قامت بكل ما من شأنه أن يحمي مصالحها ومصالح شعبها ويوفر لهم الاستغلال الآمن للتكنولوجيا، فقد قامت بتشريع القوانين التي تواجه جرائم الإنترنت كما احتلت الميدان سريعا بجميع أجهزتها الأمنية والقضائية وقد خلقت إطارات وأنظمة كفيلة بمواجهة الانتشار المتصارع لهذا النوع من الإجرام على جميع الأصعدة.

وفي الجزائر يبدو أن هناك محاولات لتطوير المنظومة القانونية وإصدار تشريعات تواكب التطور الحاصل في المجال التكنولوجي خاصة ما تعلق منها بتكنولوجيات الإعلام والاتصال تم تغيير حتى اسم الوزارة المعنية لتأخذ اسم وزارة البريد وتكنولوجيات الإعلام والاتصال وفي ذلك مؤشر على النية الحقيقية في خوض غمار الالتحاق بمصاف الدول الآخذة بناصية هذه التقنية.

ولذلك كان لابد من توفير كوادر وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة المعلوماتية وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني، فعلى مستوى جهاز الشرطة فقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الآلي، بالإضافة إلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية تعمل بالتنسيق مع هذه المخابر.

أما على مستوى الدرك الوطني فإنه يوجد بالعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك، الذي يختص بالتحقيق في

الجرائم المعلوماتية بالإضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني.[1]

ومن بين الأجهزة المتخصصة في البحث والتحري عن جرائم الإنترنت[2] هي:

1-المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني INCC/G :

يتكون من إحدى عشر دائرة متخصصة في مجالات مختلفة، فجميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية، ودائرة الإعلام الآلي الالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما تقدم مساعدة تقنية للمحققين في المعايانات.

2-مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني CPLCIC/GN.

يضع الدرك الوطني لتنفيذ مهامهفي مجال الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، او على مستوى القيادات الجهوية والمحلية وهي كالآتي:

- ✓ قيادة الدرك الوطنية.
- ✓الوحدات الإقليمية.
- ✓الوحدات المشكلة.
- ✓وحدات الإسناد.
- ✓هياكل التكوين.
- ✓المعهد الوطني للأدلة الجنائية وعلم الإجرام.
- ✓المصالح المراكز العلمية والتقنية.

---

[1]- حابت أمال، **ورقة مقدمة في محاضرة حول الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في قانون الجزائري**، جامعة مولود معمري، تيزي وزو، ص21.

[2]- عز الدين عز الدين، **الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ورقة مقدمة في ملتقى الوطني لمديرية العامة للأمن الوطني لمكافحة الجرائم** بسكرة في 2015/11/16، ص11.

✓المصلحة المركزية.

✓المفرزة الخاصة للتدخل.

تعمل مؤسسة الدرك الوطني جادة للتطلع بمختلف الجرائم المرتكبة على شبكة الإنترنت وهذا للتسهيل مهمة البحث والمعاينة والتفتيش في أنظمة الحزاسيب والعمل على مراقبة مختلف الشبكات، وبالتالي تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني في خدمة هذه الأهداف، وذلك حسب الإختصاص والصلاحيات وطبيعة الجريمة إلى ثلاث مستويات مركزية، جهوية، محلية.

3-المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

تتصدى هذه المديرية لجريمة الإنترنت من عدة جوانب ومنها الجانب التوعوي بحيث لم تغفل المديرية العامة للامن الوطني عن الوقاية التوعوية وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الاطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة جرائم الإنترنت.

بالإضافة على الدور الفعال التي تلعبه الشرطة في البحث والتحري والتفتيش بحيث توكل لوحدات متخصصة من أجهزة الشرطة بمكافحة جرائم الإنترنت بعد توفير التكوين الكافي والمناسب في هذا المجال مما يسمح لها بالتفتيش والبحث والتحري والتحفظ على الأدلة التي تثبت هذا النوع من الجرائم ورغم عدم اختصاصها ببعض الجرائم مثل جرائم التجارة الإلكترونية إلا أنها تمد يد العون للأجهزة المختصة كونها تملك الكفاءة الفنية فهي تعينها فنيا في مجال البحث وتحليل المعلومات المتحصل عليها وتحضير الوثائق الرسمية والمثول للشهادة أمام المحاكم.[1]

[1] لحاق عيسى، الأدلة الجنائية الالكترونية، مجلة البحوث بالحقوق والعلوم السياسية، العدد 1،المجلد4، تيارت 2018، ص. 33

4-الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تم تحديد تشكيلتها وتنظيمها وسيرها بواسطة المرسوم الرئاسي رقم 261/15 في 2015/10/08.

تعتبر هذه الهيئة قفزة نوعية في إطار مسار الإصلاحات التي تنتهجها الجزائر مؤخرا ذات الطابع القانوني والأمني والسياسي لتعزيز دولة القانون ويتجلى دور هذه الهيئة فيما يلي:

-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

-مساعدة السلطات القضائية والمصالح الشرطة القضائية في التحريات التي تجري بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال، من خلال جمع المعلومات وانجاز الخبرات القضائية.

-تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

كما لعبت المديرية العامة للأمن الوطني دورا مهما في التصدي لهذا النوع من الإجرام المستحدث حيث قامت في سنة 2003 بإرسال إطارين إلى دولة فرنسا للتكوين، في مجال مكافحة جرائم الإنترنت كما أنها لم تفوت أي فرصة لحضور الملتقيات الدولية التي تنظم من الدول الأجنبية التي عانت مبكرا من هذا النوع من الجرائم كما تم فتح تحقيق دعوة من المحققين المختصين في هذا المجال في فرنسا لتكوين دفعة من 22 ضابط شرطة خلال سنة 2003.[1]

كما حرصت المديرية العامة للأمن الوطني على استحداث هياكل جديدة تدعيما للهياكل القديمة المختصة في مكافحة الجرائم على مستوى المديرية العامة للأمن الوطني وعليه قررت القيادة العليا لأمن الوطني استحدث مخابر وفصائل وخلايا مختصة في مكافحة هذا الإجرام وذلك من خلال[2]:

[1]- حملاوي عبد الرحمن، **المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية** ، ورقة مقدمة في الملتقى الوطني للمديرية العامة للأمن، بسكرة، 16-2015/11/17، ص1.

[2]- حملاوي عبد الرحمن، المرجع نفسه، ص8.

أ.استحداث بمخابر الشرطة العلمية سنة 2007 الكائن مقرها بالجزائر العصمة ووهران وقسنطينة أقسام مختصة، في تتبع الأدلة الرقمية من خلال استغلال أجهزة إلكترونية قصد استخراج وتتبع ما من شانه أن يفيد في التحقيق ويساعد العدالة في تقرير الأحكام في القضايا التي تكون من هذا النوع، ومن أهم الأجهزة المستغلة في ذلك هي: أدوات التخزين الرقمية (أجهزة التصوير، بطاقات الذاكرة، الأقراص الصلبة ...إلخ) وأجهزة الكمبيوتر وجميع لواحقها.

ب.تدعيم مصالح الولائية للشرطة القضائية في سنة 2010 ما يقارب 23 خلية لمكافحة جرائم الإنترنت موزعة كما يلي: 08 على مستوى ولايات الشرق، 08 على مستوى ولايات الوسط، 06 على مستوى ولايات الغرب، 01 على مستوى ولاية الجنوب.

لتقوم بعدها المديرية العامة للأمن الوطني بتعميم الخلايا على جميع مصالح امن ولايات الوطن، وبذلك فقد قامت المديرية العامة بتسطير برنامج محكم للحد من الانتشار السريع لجرائم الإنترنت.

ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والامني والدولي وإدارة وتنسيق عمليات الوقاية، ولمساعدة التقنية للجهات القضائية والامنية مع امكانيات تكليفها بخبرات قضائية، في حالة الإعتداءات على المنظومة المعلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

5-الهيئات القضائية الجزائية المتخصصة:

أنشأت بموجب قانون 14/04المؤرخ في 10/11/2004 المعدل والمتمم لقانون الإجراءات الجزائية تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 392، 37، 40، من قانون الإجراءات الجزائية الجزائري تتمتع باختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 342/06 المؤرخ في 05/01/2006.

بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذ كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من قانون رقم 04/09.

المطلب الثاني: على المستوى الدولي

لما كانت جرائم الإنترنت ذات صفة عالمية يمكن أن تتعدى آثارها عدة دول، فإن ملاحقة مرتكبيها وتقديمهم إلى المحاكمة وتوقيع العقاب عليهم يتطلب ضرورة تعاون فيما بين الدول للقبض على المتهمين أو لجمع الأدلة أو سماع الشهود أو اللجوء إلى الإنابة القضائية أو تقديم المعلومات التي يمكن إن تساهم في تحقيق ذلك وهذا ما نصت عليه اتفاقية الأوروبية لجرائم الإنترنت وأكدت عليه لكونه أصبح يمثل إحدى الضرورات اللازمة لمواجهة هذه الأنشطة الإجرامية المستحدثة على نحو يتكامل مع دور القوانين الوطنية.

الفرع الأول: على المستوى الدولي (المنظمة الدولية للشرطة الجنائية)

من أهم أجهزة التعاون الشرطى المكلفة بمكافحة الإجرام بصفة عامة وإجرام الإنترنت بصفة خاصة "المنظمة الدولية للشرطة الجنائية" الإنتربول (OIPC) التي تتخذ من باريس مقرا لها.

أولا: مفهوم المنظمة الدولية للشرطة الجنائية

إن هذه المنظمة الدولية هي من قبيل المنظمات الدواية المتخصصة التي تهتم بالتعاون الدولي بين الدول الأعضاء فيها في مجال مكافحة الجريمة وتعقب المجرمين الذين يستطيعون تجاوز حدود الدولة التي إرتكبو فيها جرائمهم وهربوا إلى دول أخرى.[1]

منظمة تعي بمحاربة الإجرام الدولي المتزايد وتامين الاتصالات الرسمية بين رجال الشرطة في جميع أرجاء العالم لتبادل الخبرات والآراء ومناهج العمل وترسيخ التعاون المتبادل بين سلطات

[1]– منتصر سعيد حمودة، **المنظمة الدواية للشرطة الجنائية "الأنتربول"**، الطبعة الأولى ، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص11.

الشرطة الجنائية لدول الأعضاء فيها ضمن القوانين السارية في هذه الدول مع مراعاة المبادئ العامة لحقوق الإنسان.[1]

ويمكن لنا تعريف المنظمة الدولية للشرطة الجنائية كما تشير تسميتها عبارة عن منظمة دولية حكومية دائمة، تتمتع بالشخصية القانونية الدولية، والأهلية القانونية اللازمة للقيام بمهامها، تم إنشاؤها من قبل مجموعة من الدول بمقتضى وثيقة أطلق عليها اسم الدستور بغرض الإشراف والتنسيق ودعم التعاون الدولي بين أجهزة الشرطة في مجال مكافحة الجريمة.

إذا انطلاقا من تصنيف المنظمة الدولية للشرطة الجنائية ضمن المنظمات الدولية الحكومية جاز لنا اعتبارها شخص من أشخاص القانون الدولي العام، إذ أن هذا الوصف لا يتحقق إلا إذا توفرت العناصر التالية:

1 -عنصر الكيان المتميز الدائم.

2 -عنصر الإرادة الذاتية.

3 -الاستناد إلى اتفاقية دولية تنشأ المنظمة.

4 -إن الاشتراك في عضوية هذه المنظمة لا ينقص من سيادة دول الأعضاء.[2]

ثانيا: اختصاصاتها

وهي في ذلك متخصصة في مكافحة الجرائم ذات الطابع الدولي وخاصة تلك المتعلقة بالعنف ضد الأشخاص والجرائم الواقعة عن الأموال وهي كذلك تختص بمكافحة الإجرام المنظم العابر للحدود بجميع صوره، بما في ذلك المرتبط بجرائم الإنترنت وخاصة ذلك المتعلق بالاستغلال الجنسي للأطفال.[3]

---

[1]- الطيب نوار، **أنتربول منظمة الدولية للشرطة الجنائية**، مجلة بونة، مدرسة الشرطة، العدد 3، عنابة، الجزائر، 2001، ص20.

[2]- محمد منصور الصاوي، **أحكام القانون الدولي في مجال مكافحة الجرائم الدولية للمخدرات** ، دار المطبوعات الجامعية، الإسكندرية، مصر، دون سنة، ص ص651-652.

[3]- نبيلة هبة هروال، المرجع السابق، ص151.

هذا من جهة ومن جهة أخرى فهي تقوم بوضع استراتيجيات محكمة لمواجهة هذا النوع المستحدث من الإجرام بالتعاون مع المجموعة الثمانية G8 وذلك من خلال:

1 إنشاء مركز اتصالات أمني عبر شبكة يعمل 24 ساعة على 24 ساعة وسبعة أيام على سبعة أيام على مستوى البوليس في الدول الأطراف.

2 استخدام وسائل حديثة في تلك المكافحة كاستخدام تلك القاعدة من بيانات المركزية للصور الإباحية الممولة من قبل دول الأطراف.

ومن جهة أخرى تجدر الإشارة على أن نطاق اختصاصه المكاني محدد في دول التي لا تنتمي إلى الاتحاد الأوروبي وذلك لانعقاد الاختصاص فيه لوحدات أخرى كالأوربول وقنوات شنجن.

وهكذا يتول الأنتربول إقامة علاقات بين الدول المنظمة وتبادل معلومات بين سلطات التحقيق فيما يتعلق بالجرائم المتشعبة في عدة دول كتلك المرتبطة بجرائم الإنترنت، ولا سيما تلك المتعلقة بالاستغلال الجنسي للأطفال.

الفرع الثاني: على المستوى الأوروبي

أولا: الأوربول أو مركز الشرطة الأوروبية

الأوربول هو أحد الأجهزة المتواجدة على المستوى الأوروبي والتي تتخذ من لاهاي هولندا مقرا لها وهي مكلفة بمكافحة الإجرام عن طريق:

معالجة المعلومات المرتبطة بالأنشطة الإجرامية على مستو الإتحاد الأوروبي، ودعم وتشجيع سلطات التحقيق وذلك بتكميل وسائلهم وتحديثها من أجل مكافحة جميع الإجرام المنظم الدولي الخطير، وكذا بتسهيل تبادل تلك المعلومات عن طريق تزويد المحققين بتحاليل عملية و إستراتيجية وبدعمهم بخبراته ومدهم بمساعداته التقنية.[1]

وللأوربول دور فعال في مكافحة جرائم الإنترنت إذ نجده يقوم بتسهيل التحقيقات المرتبطة بوقائع بث أو امتلاك محتويات إباحية عبر الإنترنت بين الدول الأوروبية.

[1]- نبيلة هبة هروال، المرجع السابق، ص158.

ولقد تم في ذات السياق عقد اجتماعات لمكافحة هذا النوع من الإجرام في جوان 2001 في لاهاي. إلى جانب اجتماعات أخرى بمشاركة السلطات القمعية الألمانية، تحت عنوان: مكافحة الاستغلال الجنسي للأطفال.[1]

ثانيا: الأورجيست

وإلى جانب الأوربول يتواجد على المستوى الأوروبي الأورجست كجهاز يساعد على التعاون القضائي والشرطي في مواجهة ومكافحة جميع أنواع الجرائم الخطيرة.

وتنعقد اختصاصاته عندما يمس ذلك الإجرام دولتين على الأقل من أعضاء الإتحاد الأوروبي أو دولة عضو مع دولة من دول العالم الثالث أو دولة عضو مع الرابطة الأوروبية وهي في ذلك غير مقتصرة على الأشخاص فقط وإنما تشمل كذلك المؤسسات وتجدر الإشارة إلى الأورجست يمثل دعامة في فعالية التحقيقات والمطاردات المتبعة من قبل السلطات القضائية الوطنية وخصوصا فيما يتعلق بالأنشطة المرتبطة بجرائم الإنترنت.[2]

وهو في ذلك على علاقة وثيقة مع الأوربول إذ يمدها بالتحليلات اللازمة للقيام بالتحقيقات في الجرائم المنظمة وهو يتكون من نواب عامين، ومستشارين ومأموري الضبط القضائي للدول الأعضاء في الإتحاد الأوروبي دور الاختصاص ومندوبي من قبل كل دولة عضو في الإتحاد وفقا لنظامها القانوني.

وتتلخص نشاطاته في:

- تحسين التنسيق والتعاون بين السلطات القضائية المختصة لدول الأطراف.
- تبادل معطيات بين دول الأعضاء الإتحاد الأوروبي وكذا التحفظ عنها.

[1]-Recommandation du forum des droits sur l'internet : les enfants du net 2, disponible à l'adresse précédente

[2]- تعتبر جرائم الإنترنت إحدى الجرائم التي تختص المنظمة بمكافحتها، أنظر في ذلك المادة 04 من قرار اجلس الإتحاد الأوروبي.

كما يمكنه أن يطلب من الوكلاء العامين ذوي الاختصاص الوطني إجراء تحقيقات أو إجراء ملاحقات أو التبليغ عن الجرائم إلى السلطات المختصة لدول الأطراف.[1]

[1]-L'harmonisation des moyens de lutte contre la cybercriminalit é, disponible à l'adresse précédente.

الفصل الثاني

اختصاصات شرطة الأنترنت

تمهيد وتقسيم:

الثابت فقها وقانونا أن مأموري الضبط القضائي بما فيها أجهزة الشرطة، وكذلك سلطات التحقيق القضائي تلعب دورا رئيسيا في عملية تطبيق القانون على الوجه الصحيح حيث يتوقف عليهما هذا الأمر بصفة كلية تأسيسا على أن جهاز الشرطة هو المنوط به منع الجريمة ووقاية المجتمع والحفاظ عليه وعلى قيمه الاجتماعية والاقتصادية والأخلاقية حيث يقوم بدور فعال في ضبط أدلة الجريمة ومرتكبيها وكشف كل ما يتعلق بها حال وقوعها وذلك بهدف مساعدة أجهزة التحقيق القضائي في الوصول إلى أدلة الجريمة.[1]

وجرائم الإنترنت هي من الجرائم المستحدثة التي تلقى المزيد من الأعباء على جهازي الشرطة والقضاء وذلك بالنظر إلى ضعف خبرة كل منهما في مواجهة هذه الجرائم والتي لم يواجها بمثلها من قبل وهذا بوصفها من الجرائم المستحدثة التي ظهرت كأثر مترتب على ثورة المعلومات التي يعيشها عالمنا.

غير انه توجد صعوبات كثيرة تواجه الشرطة أو القضاء في مواجهة جرائم الكمبيوتر والإنترنت.

ومنه تم تقسيم هذا الفصل إلى المباحث التالية:

المبحث الأول: سلطات شرطة الانترنت في الظروف العادية

المبحث الثاني: سلطات شرطة الإنترنت في الظروف الاستثنائية

[1]- عفيفي كامل عفيفي، **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون** ، بدون دار نشر،ص325-236، وكذلك مدحت رمضان، الوجيز في شرح قانون الإجراءات الجزائية الاتحادي لدولة الإمارات العربية المتحدة، دار النهضة العربية، القاهرة 2000 -2001، ص143-144.

المبحث الأول: سلطات شرطة الانترنت في الظروف العادية

قد يصل إلى علم المحققين وقوع الجرائم من جراء الدوريات التي تقوم بها الضبطية القضائية وإلا فإنها تصل إلى علمهم إما بتلقي البلاغات من طرف عامة الناس أو الشكاوي من الأطراف المضرورة.

والمقصود بالظروف العادية هنا: الأحوال التي يمارس فيها عضو الضبط القضائي اختصاصه نتيجة لتلقيه نبأ وقوع الجريمة بأي طريقة من الطرق السابقة ماعدا التلبس. ولما كانت جريمة الإنترنت جريمة تهدد المجتمعات وبالتالي تهدد صالحها العام، كان من الضروري أن تتبع بشأنها الضبطية القضائية عدة إجراءات تهدف إلى التأكد من وقوع الجريمة والتحفظ على مسرحها وتحديد مرتكبها وحصر شهودها، ثم يثبت بعد ذلك ما قام به من إجراءات في محضر جمع الاستدلالات، مع نوع من الخصوصية التي تتماشى مع طبيعتها.[1]

وتجدر الإشارة إلى أن ما يهمنا من تلك الإجراءات في موضوعنا هذا هي: تلقي البلاغات والشكاوى والتي سنتناولها في الفرع الأول، والبحث والتحري عن الجرائم والجناة في الفرع الثاني.

المطلب الأول: تلقي البلاغات والشكاوى:

تظل الجريمة مستترة ما لم يتم التبليغ عنها إلى الجهات المختصة بالتحقيق وبمجرد وصول نبا وقوعها إلى تلك الجهات، فإنها تتخذ عدة إجراءات للتأكد من وقوعها وكشف مرتكبيها، ومعرفة المحققين لوقوع جريمة ما يتم وفق طريقتين سنتطرق لهما بالترتيب خلال الفرعين الأول والثاني.

الفرع الأول: البلاغات في جرائم الانترنت:

أولا: تعريف البلاغ

لغة: أصله الفعل بلغ، وبلغ الشيء، يبلغ بلوغا وبلاغا وصل وانتهى، فالبلاغ فهو ما يتبلغ به ويتوصل إلى الشيء المطلوب والبلاغ ما بلغك.

[1]– نبيلة هبة هروال، المرجع السابق، ص176.

اصطلاحا: حسب الفقهاء المصريين نجد أن البلاغ عن الجرائم هو" إخبار السلطات العامة عن وقوع الجريمة والإرشاد عن مرتكبيها بغية تقديمهم والقبض عليهم تمهيدا لمحاكمتهم".[1]

وكذلك يقصد به :" إخبار السلطات المختصة عن وقوع جريمة أو أنها على وشك الوقوع،أو أن هناك اتفاقا جنائيا أو أدلة أو قرائن أو عزما على ارتكابها أو وجود شك أو خوفا من أنها ارتكبت".[2]

التبليغ هو إخطار السلطات المختصة بوقوع جريمة، وهذا الإخطار واجب أدبي يتقيد به المواطن الصالح سواء وقعت الجريمة عليه او على غيره، إن أهمية التبليغ تعطي للمجني عليه ولغيره من الأفراد في جرائم الإنترنت دور لا يستهان به لأنه قد يكون السبيل الوحيد لكشف هذه الجرائم، وهو دور يعطي الفرصة لأجهزة الضبطية القضائية فرصة التحرك بسرعة من أجل مواجهة جريمة الإنترنت وبعبر عدم الابلاغ سببا رئيسيا في تفاقم جرائم الإنترنت.[3]

فالتبليغ هو المشكلة الحقيقية التي واجهت الجهات المختصة بمواجهة جريمة الإنترنت، فغالبية الهيئات في المؤسسات تخشى الإبلاغ عن جرائم الانترنت خوفا من فقدان عملائها وهو ما ينتج عنه إفلات مرتكب الجريمة بفعلته. والتبليغ هو اخبار السلطات المختصة عن وقوع الجريمة او أنها على وشك الوقوع ، أو كان هناك اتفاقا جنائيا، أو ادلة أو قرائن أو عزما على ارتكابها او وجود شك أو خوف من انها ارتكبت.

وفي هذا الصدد نصت الفقرة الأولى من المادة 17 المعدلة بموجب الأمر 02/15 قانون الإجراءات الجزائري على انه: "يباشر ضابط الشرطة القضائية السلطات الموضحة في المادتين

---

[1]- أمل خلف سفهان الحباشنة، **التبليغ عن الجرائم في التشريع الأردني** ، رسالة مقدمة إلى عمادة الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في قسم القانون العام، جامعة مؤتة، 2008، ص7.

[2]- محمد الأمين البشرى، **التحقيق في جرائم الحاسب الآلي والإنترنت** ، المجلة العربية للدراسات الأمنية والتدريب، العدد الثلاثون، أكاديمية نايف للعلوم الأمنية، 2000، ص349.

[3]- خالد عياد الحلبي، مرجع سايق، ص192.

12و13 ويتلقون الشطاوى والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية" تقابلها تص المادة 17 من قانون الإجراءات الجزائية الجزائري.

ثانيا: أنواعه

ويتم البلاغ بكافة السبل التي توصل المعلومات إلى الجهات المختصة بالتحقيق والبحث والتحري، فقد يتم كتابيا أو شفويا بمعرفة المجني عليه أو غيره ممن شاهدو وقوع الجريمة أو وصل إليهم خبر وقوعها، وقد يتم بمعرفة الجاني نفسه عندما يبلغ عن جريمته. ويصطلح على البلاغ في هاتين الحالتين" بالبلاغ المادي". وقد يقدم بواسطة البريد أو البرق أو التليفون أو الصحف، وهذا ما يصطلح عليه" بالبلاغ المعنوي". أو قد يقدم عن طريق الإنترنت وهذا ما يسمى "بالبلاغ الرقمي"[1].

والجدير بالإشارة أنه وتماشيا مع التطور التكنولوجي الحاصل، قد تم وضع العديد من المواقع المخصصة للتبليغ عن الجرائم التقليدية والمستحدثة وإرساله إلى الجهات المختصة كموقع المباحث الفيدرالية الأمريكية، وكذا منظمة الإنترنت الأهلية وغيرهما من المواقع التي تخص الضبط القضائي المختص بتلقي تلك البلاغات.

وجدير بالذكر أن القانون لم يشترط أن يكون مصدر البلاغ معلوم الهوية، أي وبمفهوم المخالفة يصح أن يكون البلاغ من قبل مجهول، كما يصح أن يكون البلاغ من معلوم الهوية، ويجب على مأمور الضبط القضائي في الحالتين ولا سيما الأولى منهما تناول البلاغ بجدية كاملة، وحتى يكون البلاغ وافيا لابد من توافر العناصر التالية: نوع الحادثة، تحديد المجني عليه، زمن وقوع الجريمة ومكانها، بيان الإصابات ومعرفة السبب والدوافع التي حملت الجاني على الجريمة وأخيرا معرفة المتهم[2].

[1]- نبيلة هبة هروال، المرجع السابق، ص180.

[2]- نبيلة هبة هروال، المرجع السابق، ص 181.

ويثبت البلاغ بالخطوات التالية: فتح محضر تحقيق للقضية، إضافة إلى وضع رقم تسلسلي للبلاغ الذي يعد رقما للقضية.

ثالثا: كيفية التبليغ في جرائم الإنترنت:

قد يكون البلاغ واجب في جميع الجرائم كما هو الحال في قانون الإجراءات الجنائية المصري وقد يكون اختياري في بعض الجرائم وواجب في جرائم أخرى كما هو منصوص عليه في القانون الجزائري في المادة 91 ق ا ج [1]، كما يتم التبليغ بمختلف الوسائل التي توصل المعلومات إلى الجهات المختصة بالتحقيق فقد يكون التبليغ كتابيا، أو شفويا ومن أي شخص سواء كان متضررا أو غير متضرر وهذا ما يطلق عليه بالبلاغ المعنوي، وقد يتم عن طريق الانترنت وهذا ما يسمى بالبلاغ الرقمي.

وذلك إما عن طريق إرسال رسالة الكترونية إلى عنوان البريد الالكتروني للجهات المختصة بالتحقيق كإبلاغها عن وجود صفحات أو مواقع غير مشروعة بإرسال رسالة الكترونية مثلا، تتضمن التبليغ عن وجود موقع منشور فيه صور الاستغلال الجنسي للأطفال[2].

أما المعلومات الواجب على المحقق معرفتها من قبل المبلغ، فينبغي عليه أن يدونها عند تلقي البلاغ، والتي يمكنه الحصول عليها من خلال طرح مجموعة من التساؤلات حول تاريخ ووقت تلقي البلاغ، المعلومات الشخصية للمبلغ، طبيعة ونوع الجريمة الالكترونية، محل البلاغ وغيرها من الأسئلة التي تخدم التحقيق.

رابعا: الجهة المختصة بتلقي البلاغات في جرائم الإنترنت:

من بين العديد من الجهات المختصة بتلقي البلاغات في هذا النوع من الجرائم، أخذنا في هذا السياق فرنسا كنموذج.

[1]- راجع المادة 91 من قانون الاجراءات الجزائية الجزائري.

[2]- نفس المرجع، ص182.

لقد أنشئت عدة وحدات ومراكز لمكافحة جرائم الانترنت في تلك الأخيرة، ومن بين تلك المراكز: "المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات" والذي يعتبر سلاح الدولة في مكافحتها لذلك النوع الجديد من الإجرام، ومن بين اختصاصاته تلقي البلاغات وتحليلها في حالة وجود مواقع تنشر صورا للاستغلال الجنسي للأطفال.[1]

فمع وصول تلك البلاغات إلى ذلك المكتب يتم تحليلها ودراستها، ويتم تسجيلها أوتوماتيكيا أو آليا في قاعدة البيانات التي يقوم بتسييرها ليقوم بعد ذلك بمراجعة أولية لها سواء من الناحيتين التقنية أو القانونية بحيث يتأكد من صحة ما ورد فيها من معلومات حول حدوث تلك الجرائم وجسامتها، ويقيمها، ثم يقوم بعد ذلك بإبلاغ مصالح الدرك والشرطة وذوي الاختصاص الإقليمي[2].

ليتم بعدها تسجيل البلاغ لدى المصالح المختصة، ويتم بعدها إعطاء رقم تسلسلي للمبلغ وهذا من أجل تمكينه من معرفة مستجدات التحقيقات.

ومن جهة أخرى فان معالجة تلك البلاغات تتم بواسطة محققين مختصين في المعلوماتية وكذا في الإجراءات الجنائية، ومن جهة ثالثة، فان الاختصاص الإقليمي للقيام بالإجراءات التي تتبع البلاغ ينعقد للجهة المتواجدة فيها مستخدم الانترنت الذي شاهد أو تلقى فيها صور الاستغلال الجنسي للأطفال.

كما ينعقد الاختصاص الإقليمي في معالجة تلك البلاغات، للجهة المتواجد فيها الخادم إذا ما تبين أنه موجود في فرنسا.[3]

[1]- نبيلة هبة هروال، المرجع السابق، ص 186.

[2]- نفس المرجع ، ص187.

[3]- نفس المرجع، ص 187-188.

الفرع الثاني: الشكوى في جرائم الإنترنت.

في غالب الأحيان يترتب على الجريمة ضرر خاص يصيب أحد الأفراد سواء ماديا أو معنويا، فيكون لديه الحق في تحريك الدعوى العمومية وهذا بتقديم شكوى تكون أمام الجهات المختصة بالتحقيق، وهذا ما نص عليه المشرع الجزائري في المادة 72 من ق ا ج.[1]

أولا: تعريف الشكوى

"ذلك البلاغ أو الإخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة طالبا تحريك الدعوى العمومية بشان جرائم معينة حظر المشرع تحريكها بصدها قبل تقديمه، أي أن هناك بعض الجرائم حددها المشرع على سبيل الحصر، لا يمكن تحريك الدعوى العمومية فيها إلا بعد تقديم شكوى من قبل المجني عليه أو "وكيله الخاص[2]".[3]

ولا يوجب القانون للشكوى شكلا معينا وإنما يقتصر فيها المعني بالأمر على ذكر اسمه وسنه وعنوانه وموجز الوقائع، والمواد القانونية التي تعاقب الفعل المرتكب، وإعطاء كافة المعلومات الخاصة بمرتكب الجريمة إذا كان معلوما.[4]

---

[1]- المادة 72 ق ا ج "يجوز لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بان يتقدم بشكواه أما قاضي التحقيق المختص".

[2]- نبيلة هبه هروال، المرجع السابق، ص189.

[3]- بالنسبة للمشرع الجزائري حدد الجرائم التي تشترط فيها الشكوى وهي:

-جريمة الزنا المنصوص عليها في المادة 339 من قانون العقوبات الجزائري.

- جرائم السرقة التي تقع بين الأقارب والحواشي والأصهار لغاية الدرجة الرابعة وفق المادتين 368 و 369 من قانون العقوبات الجزائري.

-جرائم النصب وفق المادة372 ق ع ج وخيانة الأمانة المادة 377 نفس القانون، وإخفاء الأشياء المسروقة المادة 389 نفس القانون متى وقعت بين الأشخاص المشار إليهم في المادة369 ق ع ج.

-خطف أو إبعاد القاصر وزواجها من خاطفها المادة 326 ق ع ج.

-ترك أحد الوالدين لأسرته أو الزوج الذي يتخلى عن زوجته مع علمه بأنها حامل المادة 261 ق ع ج.

[4]- محمد حزيط، **قاضي التحقيق في النظام القضائي الجزائري**، دار هومة، الجزائر، ط2، 2009، ص28.

وانه من بين هذه الجرائم ما يتم ارتكابها بواسطة شبكة الإنترنت، كالقذف والسب والشتم وكذا جرائم النشر كالتعدي على خصوصيات الأفراد.

وعليه هل يشترط في مثل هذا النوع من الجرائم المرتكبة الشكوى حتى يتم تحريك الدعوى العمومية؟ وإذا ما كانت واجبة، فهل يكون هنالك اختلاف في أحكامها عن ما جرى في العادة؟.

ثانيا: أحكام الشكوى في جرائم الإنترنت:

لا تختلف أحكام الشكوى في الجرائم التقليدية عن تلك التي ترتكب عبر الانترنت، إذ لا يجوز للجهات المختصة تحريك الدعوى العمومية في تلك الجرائم إلا بعد تقديم شكوى من المجني عليه أو المتضرر منها أو من وكيله الخاص ضد المتهم، لكن وكما سبق ذكره فانه كثيرا ما يصعب تحديد الجاني أو المتهم في هذا النوع من الجرائم، هذا ما أدى ببعض الفقه إلى ترتيب مسؤولية مزود الدخول أو خدمات الانترنت عن تلك الجرائم مستندين في ذلك على مبدأ افتراض مسؤولية الغير.[1]

وهذا ما يجعل موضوع الشكوى في هذه الجرائم محل جدل قانوني، وخصوصا إذا علمنا أن تقديم الشكوى من قبل المجني عليه قد يوجه إلى السلطات العامة ضد مزودي الخدمات، دون حاجة إلى متابعة التحريات لمعرفة الجاني الحقيقي.[2]

ومن جهة أخرى فان الإشكال الذي يثار يتعلق بمدى قبول الشكوى إذا كان المجني عليه قد تعرض إلى سب أو قذف من الجاني في الوقت الذي كان يستخدم فيه الاستعارة عبر الإنترنت، فهل تقبل شكواه إلى السلطات العامة في هذا الإطار؟.

يتجه رأي إلى قبول شكوى المجني عليه عندما يكون في حالة تخفي دون أية عوائق في هذا الإطار حتى لو كانت الوقائع التي نسبها إليه الجاني مما يدخل في طائلة الشخصية الوهمية، وهناك

[1]- نبيلة هبه هروال، المرجع السابق، ص191-192.

[2]- عمر محمد أبو بكر بن يونس، **الجرائم الناشئة عن استخدام الإنترنت** ، دار النهضة العربية، القاهرة، 2004، ص 836.

من يرى إجازة ذلك في حالة واحدة هي إذا كان الغرض من الاستعارة مشروعا [1]، ولعل الرأي الراجح في الإجابة على الإشكال السابق هو الرأي الثاني.

ثالثا: المراكز المتخصصة بتلقي تلك الشكاوى:

خصصت العديد من المراكز من بينها مركز تلقي الشكاوى عن جرائم الاحتيال عبر الإنترنت"IFCC" الذي تم تأسيسه في فرجينيا الغربية بالو.م.أ من طرف مكتب التحقيقات الفدرالي"FBI" والمركز الوطني لجرائم الياقات البيضاء " NW3C" من أجل مكافحة ظاهرة الاحتيال عبر الإنترنت المتصاعدة والموقع المخصص لتلقي الشكاوى من الضحايا. [2]

وبمجرد وصول تلك الشكاوى إلى عنوان ذلك المركز، يقوم الفريق المختص في تلك الجرائم بترتيب تلك الأخيرة وتحليلها لتحديد تكييفها القانوني، كما يقوم بالمساعدة على ملاحقة المحتالين والكشف عنهم عبر الإنترنت وعن الاتفاقات الاحتيالية التي تتم عبرها على المستويين الوطني والدولي على السواء.

ويوجد إلى جانب ذلك المركز في الولايات المتحدة الأمريكية، مركز معالجة الشكاوى المرتبطة بجرائم الإنترنت (IC3) والذي من اختصاصاته تلقي تلك الشكاوى التي تصله من خلال العنوان الالكتروني السابق وتحليلها لتحديد نوع ودرجة ذلك الإجرام، أو بمعنى آخر للتأكد من ذلك الإجرام وتقييمه، لإرساله بعد ذلك إلى السلطات القضائية المختصة بالبحث والتحري.[3]

المطلب الثاني: البحث والتحري عن الجرائم والجناة

عندما تتضح معالم وقوع جريمة الإنترنت أو أي جريمة أخرى فان على مأموري الضبط القضائي المبادرة في الحال، ومن دون تباطؤ بالبحث والتحري عنها وبمراقبة المشبوهين، واستيقافهم ومطاردة الفارين وتعقب الجناة والبحث عنهم وجمع الأدلة لإثبات إدانتهم، وتعتبر إجراءات

[1]- عمر محمد أبو بكر بن يونس، المرجع السابق، ص836.

[2]- نبيلة هبة هروال، المرجع السابق، ص193.

[3]- نفس المرجع، ص193.

البحث والتحري عن الجريمة من الإجراءات الاستدلالية التي يقصد بها الكشف عن الجريمة والبحث عن أدلتها وبذلك فهي عبارة عن أول إجراء لاختبار ما حدث.[1]

أي هي عبارة عن مجموعة من الإجراءات التي يقوم بها رجال الضبط القضائي أو من يستعينون بهم من رجال الشرطة أو المرشدين أو المخبرين، من أجل كشف حقيقة الجرم الواقع ومعرفة كيفية حدوثه والظروف والملابسات المحيطة به فهي التي تقود إلى وضوح الرؤية وإعطاء صورة واضحة لما وقع بشكل جيد.[2]

إجراءات التحري والبحث من الإجراءات الضرورية في جرائم الإنترنت كغيرها من الجرائم ويقصد بها مجموعة الإجراءات التي يقوم بها المتحري عبر شبكة الإنترنت، بواسطة التقنية الالكترونية الرقمية تحت تغطية للحصول على البيانات ومعلومات تعريفية أو توضيحية عن الأشخاص أو عن الأماكن أو الأشياء حسب طبيعتها للحد من الجرائم الالكترونية أو ضبطها لتحقيق الأمن الالكتروني أو لأي غرض آخر، وبهذا فهي وسيلة لجمع المعلومات والأدلة عن الجرائم بصفة خاصة، سواء التامة منها أم لا.[3]

ولمأمور الضبط القضائي في هذا الشأن سلطة تقديرية واسعة في اختيار وسائل إجراءات التحري، والتي يراها مناسبة وضرورية لإتمام عمله بصورة ايجابية في جمع المعلومات التي سيستغلها لضبط الجريمة أو للحد منها، وله في هذا العديد من المصادر ولعل أبرزها ما سنتناوله في هذا المطلب والمتمثلة في: الإرشاد الجنائي أولا وكذا المراقبة الالكترونية عبر الإنترنت ثانيا، وفق ما يلي:

الفرع الأول: الإرشاد الجنائي عبر الإنترنت

يعد الإرشاد الجنائي من أهم المصادر التي يعتمد عليها رجل الضبط القضائي في تحرياته وجمع المعلومات. وهو يلعب دورا كبيرا في التقصي والكشف عن جرائم الإنترنت، إذ نجد أن

[1]- محمد علي السالم آل عياد الحلبي، **اختصاص رجال الضبط القضائي في التحري والاستدلال والتحقيق**، الطبعة الأولى، 1982، ص20.

[2]- إبراهيم حامد طنطاوي، المرجع السابق، ص22.

[3]- نبيلة هبة هروال، المرجع السابق، ص194-195.

العديد من المؤسسات الضبطية حول العالم تقوم باستخدامه، وذلك عن طريق تجنيد عناصرها أو الغير للدخول إلى العالم الافتراضي وبالأخص عبر حلقات النقاش وقاعات الدردشة والاتصال المباشر، مستخدمين في ذلك أسماء وصفات هيئات مستعارة ووهمية بقصد البحث عن الجرائم ومرتكبيها وتقديمهم إلى المحاكمة[1].

وتجدر الإشارة إلى أنه وعلى خلاف ما هو متعارف عليه في الإرشاد عندما يتعلق الأمر بالبحث عن الجرائم المرتكبة في العالم المادي،"من أن المرشد يكون من عامة الناس إلا انه في العالم الافتراضي يمكن أن يقوم به مأمور الضبط القضائي بنفسه أو يكلف به غيره ممن هم على اتصال بالإنترنت، ذلك لأنه يحتاج بذل مجهود مادي كبير بل كل ما عليه فعله هو الحصول على إذن رسمي لمباشرة مهامه في البحث والتحري عن الجرائم ومرتكبيها، ويجب أن يتضمن ذلك الأخير رقم الحاسوب وصلاحيته للعمل وخلوه من العوائق التكنولوجية واحتواءه على برمجيات أصلية وليست منسوخة فضلا على ذكر أرقامها المسلسلة ورقم وتاريخ الترخيص بها وجهة إصدارها"[2].

وبمجرد حصوله عليه، فما عليه سوى أن يجلس أمام حاسوب يكون متصلا بشبكة الشبكات للقيام بعمله، وهذا بدخوله في العديد من النقاشات مع الغير مستخدما فيها أسماء مستعارة لأشخاص أو لهيئات مختلفة، عبر قاعات الدردشة وحلقات النقاش.

وبمجرد بروز نية ذلك الأخير في المشروع الإجرامي المراد ارتكابه أو الذي ارتكبه، كأن يذكر انه ينوي الحصول على بطاقات ائتمان بصورة احتيالية، أو أنه يريد استغلال الأطفال جنسيا وبث صورهم عبر هذه الشبكة. فهنا يكون للمرشد الجنائي (سواء أكان مأمور الضبط القضائي أو غيره المكلف بذلك) القيام بتقصي المعلومات، كسؤال الهاكر مثلا عن كيفية حصوله على تلك البطاقات أو عن كيفية مخادعته للقاصرين واستدراجهم للقيام بذلك العمل الإباحي.[3]

[1]- نبيلة هبة هروال، المرجع السابق ، ص195-196.

[2]- نفس المرجع ، ص196.

[3]- نفس المرجع، ص196-197.

وبمجرد حصوله على المعلومات اللازمة في حالة إذا كان المرشد من الغير، فانه يسهر على توصيلها إلى جهات الضبط التي تباشر هي كذلك عملها في ضبط المجرمين وإحضارهم مستخدمة في ذلك برمجيات معينة تقودها إلى مسار مزود الإنترنت الذي ينشط فيه مرتكب الجريمة، أما إذا المرشد من مأموري الضبط القضائي فانه يقوم باستدراج المجرم حتى يتم التعرف عليه وبالتالي إلقاء القبض عليه.

الفرع الثاني: المراقبة الالكترونية للاتصالات عبر الإنترنت

في ظل سعي الدولة لفرض قبضتها على الانترنت وشبكات التواصل الاجتماعي، لم تكتفي بملاحقة النشطاء للتعبير عن رأيهم في المجال العام بل سعت لفرض الرقابة الشاملة على المجال العام والخاص معا عن طريق مراقبة الاتصالات ، وتعتبر هذه الأخيرة من أهم مصادر التحري التي غالبا ما تتم الاستعانة بها في البحث والتحري عن الجرائم سواء التامة أو لا، وسواء كانت تقليدية أو مستحدثة كجرائم الانترنت، والتي تعتبر جزء لا يمكن الاستغناء عنه في إطار أعمال رجال البحث والتحري والتي تعتبر أسرع الطرق لكشف الجرائم.

وكما سبق ذكره فان المراقبة تتم في جميع الجرائم سواء كانت هذه الأخيرة تقليدية أو مستحدثة والتي تسمى "المراقبة الالكترونية (La cyber surveillance) أو (To keep watch)

أولا: تعريفها

ويقصد بها: "مراقبة شبكة الاتصالات" أو "العمل الذي يقوم به المراقب (بكسر القاف) باستخدام التقنية الالكترونية لجمع بيانات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا، أو شيئا حسب طبيعته مرتبط بالزمن (التاريخ والوقت) لتحقيق غرض أمني أو لأي غرض أخر"[1].

[1]- نبيلة هبة هروال، المرجع السابق، ص198.

وعليه يتبين من خلال استقرائنا للتعريفين السابقين، أن المراقبة الالكترونية تعتبر واحدة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، والتي يقوم بها مراقب الكتروني يتمثل في مأمور الضبط القضائي، والذي يتميز بكفاءة تقنية عالية تكون متماشية مع نوع الجريمة التي أمامه، مستخدما التقنية الالكترونية، كمراقبة أحد الهكرة الذين قاموا باختراق الحاسب الآلي الخاص بأحد الأشخاص والذي يعتبر ضحية الاختراق.[1]

ويشترط في كل هذا أن يحصل على إذن من ذلك المجني عليه أو من الجهة القضائية المختصة كالحصول على أمر بتلك المراقبة من المحكمة، كما هو الحال في قانون الاتصالات us code (18sec 2518) المعروف بالباب الثالث(Title III) .[2]

هذا من جهة، ومن جهة أخرى فان المشتبه فيه المراقب من طرف مأمور الضبط القضائي هو شبكة الاتصالات، وذلك عن طريق مراقبة الشخص الذي أساء استخدام مواقع الانترنت أو البريد الالكتروني، إذ يتم من خلالها مراقبة اتصالاته الالكترونية المشتبه فيها أي تلك التي تتم عن طريق الإنترنت بما في ذلك مراسلات البريد الالكتروني.[3]

ومن جهة أخرى كذلك فان التقنية المستخدمة في هذه المراقبة هي التقنية الالكترونية والتي تعنى بمجموعة الأجهزة المتكاملة مع بعضها، بغرض تشغيل مجموعة من البيانات المتعلقة بالمجرمين أو المشتبه فيهم وفق برنامج موضوع مسبقا لتحديدهم من أجل ضبطهم وتفتيشهم وجمع الأدلة قبلهم لإثبات إدانتهم وتقديمهم إلى المحاكمة.[4]

[1]- نبيلة هبة هروال، المرجع السابق، ص 199.

[2]- عمر محمد بن يونس، **الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي** ، الطبعة الأولى، 2005، ص372-373.

[3]- نبيلة هبة هروال، المرجع السابق، ص 199.

[4]- المرجع نفسه، ص200-201.

ثانيا: بعض النماذج عن المراقبة الالكترونية

1 تقنية برنامج كارنيفور:

وهذا طبقا لمكتب التحقيقات الفدرالي فان هذه التقنية تتمثل في كونها نظام كمبيوتري مصمم ليسمح لمكتب التحقيقات الفدرالي، بتطبيق أمر محكمة بجمع معلومات محددة من أجل تعقب وفحص رسائل البريد الالكتروني المرسلة والواردة عبر أي حاسب خادم تستخدمه أي شركة تقوم بخدمة توفير الإنترنت، أو أية اتصالات الكترونية أخرى من والى مستخدم معين يستهدفه تحقيق ما، ويشتبه في أن تيار الوسائل المار عبر خدماتها يحمل معلومات عن جرائم جنائية. ولا يتم تنفيذ هذه العملية إلا بعد الحصول على إذن من المحكمة المختصة بوضع أجهزة تلك الشركة تحت المراقبة.

إلا أن هذه التقنية قد اعتبرت بأنها تخترق حق الخصوصية، ولذلك أصدر القضاء الأمريكي خلال الأسبوع الثاني من شهر أغسطس/أوت 2000، حكما يلزم مكتب التحقيق الفدرالي إلى بإذاعة التسجيلات والمعلومات التي يحصل عليها من عمليات التنصت على رسائل البريد الالكتروني لمستخدمي شبكة الإنترنت، أثناء البحث والتحري عن الجناة في الجرائم المختلفة، وأمهل القاضي المكتب 10 أيام لتنفيذ الحكم، وذات الشأن بالنسبة للكونغرس الأمريكي[1]. ولكن بالرغم من ذلك، فقد حققت هذه التقنية نجاحات كبيرة في تعقب المجرمين، ولقد أصبح يطلق على هذه التقنية بعد سنة 2001 تقنية"DCS1000". أصبحت تختص بمتابعة القضايا المتعلقة بالأمن القومي والتصدي لأي محاولة لتنفيذ هجومات داخل الو م أ، وقد تمكن مكتب التحقيقات الفدرالية بفضل هذه التقنية من تقديم قرائن أدانت قائد ميليشيات كانت تستخدم

[1]– مصطفى محمد موسى، **المراقبة الالكترونية عبر شبكة الإنترنت**، دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية، الكتاب الخامس، الطبعة الأولى، دار الكتب والوثائق القومية المصرية، 2003، ص205.

الإنترنت للتراسل، وللتخطيط للدخول إلى المنشات العسكرية لسرقة متفجرات وتفجير محطات الطاقة الموجودة جنوب شرق الو.م.أ[1].

2 –تقنية كشف وجمع الأدلة والقرائن من رسائل البريد الالكتروني:

تم تأسيس شركة " اكتشاف الأدلة والقرائن الالكترونية" في سنة 1988 من قبل الأمريكي جون جيسين، وهي عبارة عن شركة اختصاصها البحث والتحري عن الوثائق الالكترونية باعتبار أنها وثائق تترك وراءها أثرا لا يمحى، ويمكن استعادتها مهما اجتهد الفاعل في محوها على غرار الوثائق المدونة في الأوراق، ولقد طورت الشركة العديد من برامج البحث في ذاكرة الكمبيوتر في الرسائل الممحاة والمعلومات المصاحبة لها والتي لا يراها متلقوا الرسالة في غالب الأحيان.

وهذه المعلومات تشمل الطريق الذي سلكته الرسالة في البداية من جهاز المرسل مرورا بعدد من الأجهزة، ويتم تجميع المعلومات في أرشيف خاص، ليكون جاهزا للاستخدام ومتاحا للخبراء والمحققين ورجال التحري والمراقبة، ولقد ظهرت أهمية هذه النوعية من الشركات بعد الدعوى التي رفعتها وزارة العدل الأمريكية و19 ولاية ضد شركة مايكروسوفت لبرامج الكمبيوتر[2].

3 – تقنية مراقبة البريد الالكتروني:

هي برنامج صممه الأمريكي ريتشارد أتوني، من أجل سير محتوى البريد الالكتروني موضوع المراقبة وقراءة الرسائل التي قام صاحبها بإتلافها أو تلك التي لم يقم بتخزينها أساسا. ولقد استخدمت أجهزة الاستخبارات الأمريكية هذا البرنامج لكشف مشتبه فيه من الجنسية الروسية حاول اختراق مواقع شبكة الإنترنت[3].

[1]– نبيلة هبة هروال، المرجع السابق، ص 202.

[2]– مصطفى محمد موسى، المرجع السابق، ص215.

[3]– نبيلة هبة هروال،المرجع السابق، ص203.

4 تقنية تعقب المواقع الإباحية:

أو ما يسمى برنامج" نوبد شرطة الإنترنت"، وهو برنامج يبحث عن الصور الجنسية المخلة على أنظمة الكمبيوتر التي تعمل ببرامج تشغيل ويندوز الحديث ويبلغ الهيئات الحكومية عنها، بهدف تطهير الشبكة من المواقع الإباحية والجنسية وهو يصل إلى تلك الأخيرة على شكل دودة الكترونية ملحقة برسالة الكترونية، بعنوان" ساعدونا لإنهاء المواقع الإباحية".[1]

وعليه فانه تجدر الإشارة إلى أن المراقبة الالكترونية هي التحكم في نشر والوصول إلى المعلومات على الإنترنت كحجب بعض المواقع الالكترونية خصوصا الإباحية منها، وبالتالي مكافحة الإجرام عبر الإنترنت على الصعيد الدولي.

ثالثا: مراقبة الاتصالات الالكترونية وفق المشرع الجزائري

1 مراقبة الاتصالات الالكترونية:

لم يشذ المشرع الجزائري عن القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية لكنه أرسى قواعد جديدة ذات طبيعة خاصة كان من اللازم أن تلد مع التطور الحاصل في حقل الجريمة المعلوماتية كظاهرة حديثة وبهذا الصدد جاء القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

ومنه سنتطرق إلى إجراء مراقبة الاتصالات الالكترونية الذي أقره القانون 09-40:

لقد تبنى الدستور الجزائري هذا المبدأ وبكل وضوح في نص المادة 47 من التعديل الدستوري لسنة 2020 منه بالقول " لكل شخص الحق في سرّية مراسلاته واتصالاته الخاصة في أي شكل كانت"[2]، وليس غريبا أن الأديان السماوية حرصت على كرامة الإنسان بشكل خاص، مثلما جاء به الدين الإسلامي في تهجين التصرفات الهادفة إلى المساس بحرمة الإنسان ونهيه عن كل من الغيبة والنميمة والتجسس مصداقا لقوله تعالى: ﴿ **يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِنَ الظَّنِّ إِنَّ**

[1]- نبيلة هبة هروال،المرجع السابق ، ص203.

[2]- راجع المادة 47 من التعديل الدستوري لسنة 2020.

بَعْضَ الظَّنِّ إِثْمٌ وَلا تَجَسَّسُوا وَلا يَغْتَبْ بَعْضُكُمْ بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَحِيمٌ﴾[1]

ويبدو أن المشرع الجزائري لم يستثن المراسلات العادية كذلك والتي تتم عن طريق وسائل الاتصال السلكية واللاسلكية كما ورد في نص المادة 65 مكرر5 من قانون الإجراءات الجزائية، إذ نصت على انه في الجرائم المعلوماتية أي الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وإذا كانت هذه الأخيرة متعارف عليها ومقصود منها جميع المراسلات أو الرسائل والبرقيات والمحادثات السلكية واللاسلكية المرسلة عن طريق البريد فان فقهاء يعتبرونها محمية قانونا ضد كل اطلاع عليها.[2]

وكذلك ما جاء به قانون البريد والمواصلات رقم 2000-03 والذي يحرص بقوة على حماية سرية المراسلات والاتصالات وفق ما أكدته المادة 137 منه على أن كل شخص يفشي أو ينشر أو يستعمل مضمون المراسلات المرسلة عن طريق اللاسلكي الكهربائي أو يخبر بوجودها دون موافقة أو ترخيص المرسل والمرسل إليه يتعرض للعقوبة المنصوص عليها في المادة 137 من قانون العقوبات.[3]

وفيما يتعلق بالبريد الالكتروني يمكن القول أن القانون 09-04 المذكور سابقا أعطى تعريفا للاتصالات الالكترونية في المادة الثانية منه مفهوم الاتصالات الالكترونية بأنها" أي اتصال أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية"، والمستخلص من هذا التعريف أن المراسلات الالكترونية تتشابه إلى حد كبير مع المراسلات التقليدية لكن تختلف عنها في التقنيات والآليات[4].

---

[1] – سورة الحجرات، الآية: 12.

[2] – زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى عين مليلة، الجزائر، 2011، ص124-125.

[3] – راجع المادة 137 من قانون العقوبات الجزائري.

[4] – زيبحة زيدان، المرجع السابق، ص126.

فالبريد الالكتروني يتضمن هو الآخر برامج متخصصة للكتابة والتراسل وتخزين الرسائل الالكترونية، ومن أهمها برامج التشفير الخاصة.

2 -كيف تتم مراقبة الاتصالات الالكترونية:

نص القانون رقم 09-04 السابق ذكره في المادة 03 منه على ما يلي:

"مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

ومن الواضح أن مراقبة الاتصالات حددها القانون على سبيل الاستثناء في حالات محددة حصريا وفق المادة 04 من القانون السابق وهي:

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

ب.في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

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

د.في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة [1]، وما يلاحظ أن المشرع ونظرا لما يترتب عن تطبيق هذا التدابير ميدانيا من مساس بحرية الحياة الخاصة وخصوصيتها وهي مقدسة ومحمية دستوريا.

[1]- راجع المادة 4 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات.

3 -تجميع الاتصالات الالكترونية وتسجيل محتواها:

من المعلوم أن الرسالة الالكترونية ذات طابع خاص، لكنها لا تختلف عن الرسالة الورقية من حيث أن مآلها من حيث حفظها أو الاستغناء عنها وإهمالها، لكن ما يميز الأولى أي الرسالة الالكترونية سواء المهملة أو المحفوظة يمكن الوصول إليها عن طريق صناديق البريد الخاصة أو الملفات المحفوظة أو الرجوع إلى سلة المهملات فالتحقيق الذي يجري بغرض ضبط المراسلات الالكترونية يكون أمام ثلاث خيارات بعد الولوج إلى البريد الالكتروني EMAIL، فيعد تحديد صندوق البريد للمتهم المشكو منه يتمحور العمل حول الثلاث عناصر وهي: الوارد IN، الصادرOUT، الحفظ وسلة المهملاتTRASH [1].

فبذلك يمكن مراجعة قائمة الرسائل التي وصلت إلى المشكو منه في الوارد والعكس بالنسبة للمرسلة منه على قائمة الصادر وكذا الشأن بالنسبة للرسائل المحفوظة أو المهملة.

غير أن ما يجب تأكيده هنا هو أن المشرع ونظرا لحساسية الموضوع والذي يعد مرتبطا بقدر كبير بذاتية الأشخاص فقد جعل تدابير وإجراءات التحقيق تحت طائلة المسؤولية الجزائية، وهذا ما نص عليه في المادة 4 من القانون 09-04 الفقرة "د" والأخيرة على أن الترتيبات التقنية الموضوعة للأعراض المنصوص عليها في الفقرة "أ" من المادة ذاتها موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها وذلك تحت طائلة العقوبات المنصوص عليها قانون العقوبات للمساس بالحياة الخاصة للغير [2].

[1]- زبيحة زيدان، المرجع السابق، ص128.

[2]- نفس المرجع، ص128-129.

المبحث الثاني: سلطات شرطة الإنترنت في الظروف الاستثنائية

زود القانون رجال الضبط القضائي بجانب من سلطة التحقيق بمباشرة على سبيل الاستثناء في الأحوال المعينة، ويقصد بالاختصاصات الاستثنائية، في أن مهمة الأساسية للسلطة الضبطية القضائية هي جمع الاستدلالات لإجراء التحقيق وكان الأصل أن يقتصر نشاط رجالها على عملهم الأساسي، وان يحال بينهم وبين مباشرة أي عمل من أعمال التحقيق لأنهم اختصاص سلطة أخرى.

راع المشرع في اختيار أفرادها شروط معينة تتناسب مع خطورة دورهم وأهمها القدرة الفنية على إدارة التحقيق غير أن المشرع لم يلتزم هذا الأصل على إطلاقه، بل خرج في بعض الحالات نزولا على حكم الضرورة ويستمد رجال الضبط القضائي سلطتهم في مجال التحقيق إما من نص القانون مباشرة أو من قرار يصدره القائم أصلا بالتحقيق وهو ما يعرف بالندب.

غير أنه والذي يتم التطرق إليه في هذا المبحث هو سلطة التحقيق المستمدة من القانون مباشرة إذ يقتصر دور الضبطية القضائية، على مباشرة إجراءات محددة لا يصح لهم تجاوزها وهي: التفتيش، المعاينة والضبط فقط وذلك إذا توفرت حالة التلبس [1] وهو حالة تلازم الجريمة ذاتها دون فاعلها وهو نوعان حقيق والاعتباري.

وعلى هذا يتم تقسيم هذا المبحث وفقا للمطلبين التاليين:

المطلب الأول: المعاينة والتفتيش في جريمة الإنترنت.

المطلب الثاني: إجراءات البحث والتحري الخاصة.

[1]- عوض محمد، المرجع السابق، ص314 -315.

المطلب الأول: المعاينة والتفتيش في جريمة الإنترنت

يعتبر المكان الذي ارتكبت فيه الجريمة الوعاء الأساسي الذي يحتوي على أخطر الأدلة الجنائية التي يخلها الجاني وراءه في أعقاب اقترافه الجريمة، وفي لحظة يكون فيها اضطرابه العصبي والذهني قد بلغ قمة الانفعال بصورة لا تتيح المراجعة الدقيقة لإعماله وإزالة الآثار التي يخلفها في مكان الحادث فمهما كانت دقته سوف يترك وراءه ما قد يشير إلى شخصيته.[1]

الفرع الأول: المعاينة

أولا: تعريف المعاينة

أ.تعريف المعاينة لغة: المعاينة هي المشاهدة بالعين، عاين غيره رآه بعينه، وجاء في الأمثال والعيان لا يحتاج إلى بيان، ويضرب لإظهار مزايا المشاهد للتصديق بالشيء دون برهان.[2]

ب.تعريف المعاينة اصطلاحا: هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها كذلك جميع الأشياء الأخرى التي تفيد في كشف الحقيقة، واتخاذ ما يلزم من إجراءات كضبط بعض الأشياء.

فالهدف من المعاينة هو لغرضين اثنين: الأول جمع الأدلة الناتجة عن الجريمة "الآثار" والثاني إتاحت الفرصة للمحقق لكي يشاهد بنفسه مكان وقوع الجريمة لكي تكون لديه فكرة واضحة لا لبس فيها ولا غموض عن كيفية وقوع الجريمة.

ولقد أشارت قانون الإجراءات الجنائية إلى إجراء المعاينة باعتباره إجراء من إجراءات التي تمتلكها السلطات التحقيقية بمختلف فئاتها وطوائفها[3]، وهذا ما ورد في نص المادة 79 من قانون الإجراءات الجزائية الجزائري "يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها...".

---

[1]- نبيلة هروال، المرجع السابق، ص212.

[2]- علي بن هادية، بلحسن البليش، الجيلالي بن الحاج يحي، القاموس الجديد للطلاب، الشركة الوطنية، الشركة التونسية، الجزائر، تونس،ط1، 1979، ص642.

[3]- نفس المرجع، ص257.

ج.تعريف المعاينة قانونا: المعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة فهي بهذا المعنى تستلزم الانتقال غلى محل الواقعة أو أي محل آخر يوجد به أثار يرى المحقق أن لها صلة بالجريمة والأصل أن إجراء المعاينة متروك لتقدير المحقق لا يقوم بها إلا إذا كان هناك فائدة من ورائها، كما أن هناك حالات يوجد فيها القانون على النيابة الانتقال فورا إلى مسرح الجريمة وهي حالة إخطارها بجناية متلبس بها.[1]

ثانيا: كيفية إجراء المعاينة التقنية لمسرح جريمة الإنترنت

تتم المعاينة في جرائم الإنترنت كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية إلا أن الانتقال هنا لا يكون إلى العالم المادي، وإنما غلى العالم الإفتراضي أو الفضاء الالكتروني (Cyber space).[2]

وينبغي التعامل في هذا الإطار مع مسرح جريمة الإنترنت على انه مسرحان هما:

مسرح تقليدي: ويقع خارج بيئة الحاسوب والإنترنت ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أي جريمة تقليدية قد يترك فيها الجاني آثار عدة كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.

مسرح افتراضي: ويقع داخل البيئة الالكترونية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الإنترنت في ذاكرة الأقراص الصلبة الموجودة في داخله.[3]

فالمعاينة تتم بالانتقال إلى محل الواقعة الإجرامية كقاعدة إجرائية مقررة في هذا الشأن إلا أنه في إطار جرائم الإنترنت، فإن المعاينة تعد من الموضوعات الجديدة وذلك أن مسألة الانتقال هذه لا تكون بالضرورة عبر العالم المادي وإنما يجب أن تكون بالضرورة عبر العالم الافتراضي.

---

[1]- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق، دار النهضة العربية، القاهرة، ط1، 2009، ص100.

[2]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، ط 1، دار الفكر الجامعي، الإسكندرية، 2010، ص156.

[3]- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجنائي والقانون المقارن، دار الجامعة الجديدة، 2010، ص84.

وهناك عدة طرق يستطيع بها عضو سلطة التحقيق أو مأمور الضبط القضائي أن ينتقل إلى عالم الإفتراضي لمعاينته وذلك من خلال:

1-من مكتبه بالمحكمة من خلال بالكمبيوتر الخاص به.

2-كما يمكنه اللجوء إلى مقهى الإنترنت (Internet Cafè).

3-وأيضا يجوز له اللجوء إلى مقر عمل مزود بخدمة الإنترنت الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة.[1]

4-كما يستطيع المحقق أيضا الانتقال إلى عالم الإفتراضي للمعاينة من خلال مقر مكتب الخبير التقني المختص إذ توفر له في القانون ما يبيح ذلك.

ذلك أنه وفي كل الأحوال يلزم أن يقوم عضو التحقيق بالمعاينة من خلال الكومبيوتر أو خادم ومن ثم فإن مشكلة الانتقال المادي، إلى محل ارتكاب الواقعة الإجرامية لا تشكل ذلك العائق أمام عضو التحقيق وإنما المشكلة تكون من خلال الانتقال إلى العالم الافتراضي حيث يلزم أن يكون هذا الانتقال بالسرعة الكافية التي تتم زوال آثار الجريمة [2]، ويجب على المحقق الجنائي أو مأمور الضبط القضائي قبل الانتقال إلى إجراء المعاينة إلى مسرح جريمة الإنترنت إتباع الخطوات التالية:

1-توفير المعلومات مسبقة عن مكان الجريمة ومن مالك هذا المكان ونوع أجهزة الكومبيوتر المتوقع مداهمتها وشبكاتها، وذلك لتحديد إمكانية التعامل معها فنيا من حيث الضبط والتامين وحفظ المعلومات.

2-الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل.

3-قطع التيار الكهربائي عن موقع المعاينة لشل فعالية الجاني في القيام بأي فعل بشأنه التأثير او محو أثار الجريمة.

[1]- عمر محمد أبو بكر بن يونس، المرجع السابق، ص895.

[2]- خالد ممدوح إبراهيم، المرجع السابق، ص157.

4-إعداد فريق تفتيش من المتخصصين والفنين.

5-إعداد الأمر القضائي اللازم للقيام بالتفتيش سواء كان ذلك أمر من النيابة العامة أم الأمر من القاضي الجزائي المختص وذلك في الحالات التي حددها القانون.[1]

ومن الإجراءات التي يتعين إتباعها عند إجراء المعاينة ما يلي:

6-القيام بتصوير جهاز الحاسب الآلي الذي ترتكب عن طريقه الجرائم وما قد يتصل به من أجهزة طرفية ومحتوياته.

7-العينة البالغة بملاحظة الطريقة التي تتم بها إعداد النظام والآثار الالكترونية التي يخلفها الولوج أو التردد على المواقع بشبكة الإنترنت، وبوجه خاص السجلات الالكترونية التي تزود بها شبكات المعلومات لمعرفة وقع الاتصال ونوع الجهاز الذي تتم عن طريقه الولوج إلى النظام أو المواقع أو الدخول معه في حوار.

8-ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل حين عرض الأمر فيما بعد على القضاء.

9-عدم نقل المعلومات من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الكومبيوتر، من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو او إتلاف البيانات المسجلة.

10-التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة.

11-التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات صلة بالجريمة.

12-وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع الكشف التفصيلي بالمسؤولين بها ودور كل واحد منهم.

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص158.

13-قصر مباشرة المعاينة على فئة معينة من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الكومبيوتر وشبكات ونظم المعلومات واسترجاع المعلومات والذين تلقو تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يحويها مسرح جريمة الإنترنت.[1]

الفرع الثاني: التفتيش وضبط الأدلة في جريمة الإنترنت

التفتيش وضبط الأدلة في جريمة الإنترنت يحتاجان إلى تقنيات خاصة تختلف عن حالات الجرائم التقليدية وذلك راجع لطبيعة الوسيلة المستخدمة لارتكاب الجريمة، كذلك يرجع الاختلاف إلى أن مسرح الجريمة في جريمة الإنترنت معلومات وبيانات غير ملموسة مما يصعب هذين الإجراء ويستلزم وسائل خاصة مقارنة بالظروف العادية فهل يكفي التعريف التقليدي لهذا الإجراء للإلمام بكل عناصرهما الواقعة على نظم الحاسب الآلي والإنترنت؟ وما مدى قابلية التقنية العالية لهذا الإجراء؟.

أولا: التفتيش في جريمة الإنترنت

يمكن تعريف التفتيش بأنه السعي للحصول على الأدلة لدى المتهم ذاته أو مسكنه حيثما تكون تحركاته شريطة إتباع إجراءات شكلية تطلبها القانون، وتكمن الفكرة الأساسية للتفتيش في إباحة الحق في الخصوصية طالما أن هناك مبررا في القانون لهذا الانتهاك، ومن ثم يعد التفتيش أحد مظاهر تقييد الحريات الإنسانية التي ساهمت التشريعات الأساسية في دعم المحافظة عليها[2].

والتفتيش ليس غاية في حد ذاته وإنما هو وسيلة لغاية تتمثل في ما يكمن الوصول من خلاله إلى أدلة مادية تسهم في بيان وظهور الحقيقة [3]، ويثور التساؤل حول إمكانية تطبيق القواعد العامة للتفتيش على صورة تفتيش نظم الحاسوب والإنترنت ذلك أن هذا الإجراء يهدف إلى جمع الأدلة

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص174.

[2]- عمر محمد أبو بكر بن يونس، المرجع السابق، ص852.

[3]- صادق المرصفاوي، **أصول الإجراءات الجنائية في القانون المقارن**، منشأة المعارف، الإسكندرية، 1982، ص385.

المادية، في حين أن النظم المعلوماتية عبارة عن كيان معنوي [1] ولا تتوافر له صفة المادة سواء تعلق ذلك ببرامج الحاسوب أم ما يشمل عليه من بيانات لكن من المعروف أن نظم المعالجة الآلية تتكون من مكونات مادية وأخرى غير مادية ترتبط بغيرها عبر شبكات اتصال بعدية على مستوى المحلي أو الدولي[2].

1) محل التفتيش في البيئة الرقمية

يتكون النظام المعلوماتي من مكونات مادية (HARD WARE) ومكونات منطقية (SOFT WARE) كما أن له شبكات اتصالات بعدية سلكية ولا سلكية على المستوى المحلي والدولي فهل تخضع هذه المكونات للتفتيش؟

أ. تفتيش المكونات المادية لنظام المعالجة الآلية:

إن التفتيش الواقع على المكونات المادية للنظام المعالجة الآلية لا توجد فيه أي مشكلة في التنفيذ لإمكانية ذلك وسهولته، مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها وتأتي سهولة هذا التفتيش لأنه يرد على أشياء مادية لا خلاف حول خضوعها للتفتيش طبقا لقواعد قانون الإجراءات الجزائية الخاصة لهذا الإجراء.

إلى أن المشرع الجزائري بمناسبة التعديل الذي ألحقه على قانون الإجراءات الجزائية استثنى بموجب الفقرة الثالثة من المادة 45 وكذا الفقرة الثانية من المادة 47 والفقرة الثالثة من المادة 64 تطبيق هذه الضمانات عند إجراء التفتيش، بمناسبة تحقيق مفتوح بخصوص جرائم الإنترنت ويفهم

[1]- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، عالم الكتب الحديثة، الأردن، 2004، ص07.

[2]- رشيدة بوكر خالد ممدوح إبراهيم، المرجع السابق، ص 174، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، الطبعة الأولى، 2012، ص394.

الاستقراء هذه المواد أن المشرع لا يشترط حضور الشخص الذي يشتبه في أنه ساهم في ارتكاب الجريمة عند تفتيش مسكنه[1].

كما يجوز القيام بإجراء التفتيش في كل ساعة من ساعات النهار أو الليل [2] ودون حاجة إلى رضائه عند قيام هذا الإجراء [3]، والملاحظ أن المشرع الجزائري في هذه الحالة قد غلب المصلحة العامة على حريات الأفراد وذلك اعتبارين:

-ذاتية جريمة الإنترنت المتمثلة في إمكانية اختفائها بشرعة فائقة.

-افتراض كون الدليل الرقمي هو الدليل الوحيد في الدعوة الجزائية ومن ثم ارتكاز كل العملية الإثباتية على وجوده.

ب. تفتيش المكونات المعنوية لنظام المعالجة الآلية:

إذا كان الأمر قد انتهى بنا إلى صلاح المكونات المادية للنظم المعلوماتية كمحل يرد عليه التفتيش فإن امتداد ذلك إلى مكوناته الغير مادية، هو محل جدل كبير حول مدى صلاحيتها لان تكون موضوعا للتفتيش تمهيدا لضبط الأدلة فالخلاف الحاصل في مسالة أن التفتيش التحقيق وسيلة للبحث عن الأدلة المادية إذ هو إجراء يسعى إلى ضبط الأدلة المتعلقة بالجريمة لتقديمها إلى المحكمة المختصة كدليل إدانة.

ويتضح موقف المشرع الجزائري من خلال القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حينما أجاز صراحة تفتيش

[1]- تنص المادة 3/45 من قانون الإجراءات الجزائية المعدل والمتمم على انه « لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بصرف باستثناء الأحكام المتعلقة بالحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات».

[2]- تنص المادة 3/47 من قانون الإجراءات الجزائية المعدل والمتمم على انه«يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص».

[3]- تنص المادة 2/64 من قانون الإجراءات الجزائية المعدل والمتم على انه «وتطبق فضلا على ذلك أحكام المواد من 44 إلى 47 من هذا القانون».

المنظومات المعلوماتية وذلك بموجب المادة 05 منه التي نصت على انه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية التفتيش ولو عن بعد[1].

2) شروط التفتيش في البيئة الرقمية

لقد حرصت القوانين الإجرائية على إحاطة إجراء التفتيش بشروط وضمانات أساسية نظرا لما يمكن أن يحدثه من مساس يحق الإنسان في حريته الشخصية، وهدف ذلك هو تحقيق الموازنة بين مصلحة المجتمع في عقاب المجرم وبين حقوق الأفراد وحرياتهم ومن الشروط والضمانات التي يجب توافرها منها ما هو موضوعي ومنها ماهو شكلي.

1 –الشروط الشكلية للتفتيش في البيئة الرقمية:

إن القواعد الشكلية لا تهدف إلى تحقيق العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب، وإنما تقيم بالإضافة إلى مقتضيات الإجراء سياجا يحمي الحريات الفردية [2] ولعلى أبرز هذه الشروط هي:

أ. إجراء التفتيش بحضور أشخاص معنيين بالقانون:

غنى عن البيان أن التفتيش فيه إطلاع على أسرار الغير التي تحرم أغلب التشريعات الإجرائية الإطلاع عليها لذلك فإنه من مطالعة التشريعات المقارنة، نجد أن بعضها أوجب حضور عملية التفتيش الذي تجريه الضبطية القضائية للمشتبه فيه أو شهود وأوجبت تشريعات أخرى حضور أشخاص معينين قي القانون في حالات معينة، وأجازت في أحوال أخرى إجراء التفتيش دون حضور أحد وهناك تشريعات سكتت تماما عن التعرض لهذا الشرط، وإن كان المشرع الجزائري من التشريعات الإجرائية التي أوجبت ضرورة حصول إجراء التفتيش المتعلق بالمساكن وملحقاتها بحضور

[1]– تنص المادة 2/5 من القانون 04/09 المتعلق بالقواعد المتعلقة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أن «إذا كانت هناك أسباب تدعو إلى الإعتقاد بان المعطيات عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول غلها إنطلاقا من المنظومة الأولي، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد أعلام السلطة القضائية المختصة مسبقا بذلك».

[2]– علي حسن محمد الطوالبة، المرجع السابق، ص47.

المشتبه فيه عندما يتم تفتيش مسكنه من طرف الضبطية القضائية، وأما إن تعذر ذلك بامتناعه عن حضور التفتيش أو كان هاربا يتم هذا الإجراء بحضور شاهدين من غبر الموظفين الخاضعين لسلطة ضابط الشرطة القضائية القائم بالتفتيش[1].

ب. الميعاد الزمني لإجراء التفتيش في البيئة الرقمية:

على القائم بإجراء التفتيش الالتزام بإجرائه من خلال فترة زمنية عادة ما يحددها المشرع وذلك حرصا على تضيق النطاق الاعتداء على الحرية الفردية وحرمة المسكن، في حين لم يحدد البعض الأخر من التشريعات وقتا معينا يتم فيه إجراء التفتيش وإنما ترك للقائم بالتفتيش تحديد الوقت المناسب للقيام به دون النظر إلى أي اعتبار آخر يتعلق بالمحل المراد تفتيشه و من بين تلك التشريعات قانون الإجراءات الجنائية المصرية.

ج. محضر التفتيش في جرائم الإنترنت:

لاعتبار التفتيش عمل من أعمال التحقيق ينبغي تحرير محضر يثبت فيه ما تم من إجراءات وما نتج عن التفتيش من أدلة، ولأن القانون لم يتطلب شكلا خاصا في محضر التفتيش فغنه لا يشترط لصحته سوى ما تستوجب القواعد العامة في الحاضر عموما من وجوب أن يكون مكتوبا باللغة العربية[2].

وأن يحمل تاريخ تحرير وتوقيع محرره [3] وأن يتضمن كافة الإجراءات التي اتخذت بشأن الواقع التي يبثها ونفس الكلام السابق ينطبق على محضر تفتيش الحاسوب، فإنه يستلزم بالإضافة لأي

[1]- تنص المادة 1/45 من قانون الإجراءات الجزائية المعدل أو المتمم على انه «إذا وقع التفتيش في مسكن شخص اشتبه فيه انه ساهم في ارتكاب جناية فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بان يكلفه بتعين ممثل له، وإذا امتنع عن ذلك أو كان هاربا إستدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته».

[2]- طبقا لنص المادة 03 من الدستور الجزائري 2016 «ا اللغة العربية هي اللغة الوطنية والرسمية، تظل العربية اللغة الرسمية للدولة».

[3]- تنص المادة 54 من قانون الإجراءات الجزائية المعدل والمتمم على أن «المحاضر التي يضعها ضباط الشرطة القضائية طبقا للقانون ينبغي تحريرها في الحال وعليه أن يوقع على كل ورقة من أوراقه».

شكليات السابقة ضرورة إحاطة قاضي التحقيق أو عضو النيابة بتقنية المعلومات ثم لا ينبغي بعد ذلك أن يكون هناك شخص متخصص في الحاسوب والإنترنت يرافقه للاستعانة به في مجال الخبرة الفنية الضرورية وفي صياغة مسودة محضر التفتيش.

2 -الشروط الموضوعية للتفتيش في البيئة الرقمية:

أ. وجود سبب للتفتيش:

إن سبب التفتيش في القواعد العامة بوصفة إجراء من إجراءات التحقيق هو وقوع الجريمة واتهام شخص، أو عدة أشخاص بارتكابها أو المساهمة فيها وتوافر أمارات وقرائن قوية على وجود أشياء في كشف الحقيقة لدى المشتبه فيه أو غيره وبناءا عليه وتطبيقا على الجرائم الإنترنت فإن سبب التفتيش المتعلق بهذا النوع من الجرائم.

ب. تحديد محل التفتيش:

يقصد بمحل التفتيش المستودع الذي يحفظ فيه الشخص بالأشياء المادية التي تتضمن سره ومحل التفتيش في الجرائم الإنترنت الحاسوب والشبكة، التي تشمل في مكوناتها الخادم والمزود للآلي والمضيف والملحقات التقنية...إلخ.

وحكم تفتيش هذه المكونات يتوقف عل طبيعة المكان الموجود فيه فيما إذا كان من الأماكن العامة من الأماكن الخاصة، وتكمن أهمية التفرقة هنا في أن هذه الكيانات في الأماكن الخاصة يكون لها حكم تفتيش المساكن بنفس الضمانات المقررة قانونا سيما اشتراط الإذن بالتفتيش من السلطات القضائية المختصة [1] وهذه الضمانة خاصة بجميع الجرائم بما فيها جرائم الإنترنت.

[1] – تنص المادة 44 من قانون الإجراءات الجزائية المعدل والمتمم على انه «لا يجوز لضباط الشرطة القضائية الإنتقال غلى مساكم الذين يظهر انه مساهمو في الجناية او انهم يحوزون أوراقا أو اشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش إلا بإذن صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الإستضهار بهذا الأمر قبل الدخول فقي المنزل والشروع بالتفتيش».

أما التفتيش الواقع على مكونات الحاسوب الموجودة في الأماكن العامة فإن أغلب التشريعات تجيز لرجال الضبطية القضائية، دخول المجال العام المفتوحة للجمهور كمقاهي الإنترنت من أجل مراقبتها والتأكد من إحرامها للأخلاق والآداب العامة بكل سهولة دون الحاجة للإذن بالتفتيش[1].

ج. الإذن بالتفتيش:

يثير التساؤل حول إمكانية تطبيق القواعد العامة في التفتيش على صورة تفتيش نظم الحاسوب علما أن التفتيش التقليدي يهدف إلى جمع الأدلة المادية، في حين أن نظم الحاسوب عبارة عن كيان معنوي ولا تتوافر له صفة المادة ولما كان محل التفتيش بصورتها التقليدية المساكن والأماكن الملحقة بها، فقد أضفى عليها القانون الإجرائي حماية خاصة باعتبارها مكنونا لسر الأفراد ومحلا لخصوصياتهم.

د. تحديد مجال الإذن بالتفتيش:

ويتجه الرأي الغالب في التشريعات المقارنة على غرار المشرع الجزائري إلى تطلب شرط التحديد لصحة الإذن بالتفتيش على أن يجب أن يتعين الإذن بالتفتيش بيان لوصف الجرم وعنوان الأماكن التي يتم زيارتها وتفتيشها وذلك تحت طائلة البطلان [2]، وفي نطاق تفتيش الأنظمة المعلوماتية فمن المعلوم أن التخزين هو البيئة التي تتصف بها الحوسبة أو الرقمية في البيئة الرقمية بهذه الصفة تعد مجالا ضخما يمكن تخزين مليارات المعلومات والملفات.

ومن اجل هذا فإن صياغة الإذن بالتفتيش الخاصة بالبيئة الرقمية وحتى تنفيذه يشكلان تحديات كبيرة إذ أن المادة المطلوبة قد تختلط بكميات هائلة من البيانات الأخرى، التي لا تناسب الموضوع قيد التحقيق لذلك فغنه لا يستقيم الأمر مع مبدأ الخصوصية أن يطلع ضابط الشرطة

[1]- علي حسن محمد الطوالبة، المرجع السابق، ص81.

[2]- تنص المادة 3/44 من قانون الإجراءات الجزائية المعدل والمتمم على أنه «يجب أن يتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي ستتم زيارتها وتفتيشها وإجراء الحجز فيها ذلك تحت طائلة البطلان».

القضائية على جميع البيانات الشخصية الموجودة بالحاسوب كما أن ضبط النظام برمته قد يسبب خسارة غير واجبة للمشتبه فيه[1].

والمشرع الجزائري كأغلب التشريعات لا يقد حلا لهذه المسالة وما نجده على مستوى العمل القضائي في الولايات المتحدة الأمريكية، وجود تضارب بين الأحكام القضائية بخصوص هذه المسالة ففيها اعتبرت بعض الأحكام أن جهاز الحاسوب بما يحتويه من ملفات ومعلومات صندوقا واحدا ولا يستوجب تفتيشه إلا إذنا واحدا فقط، اعتبرت على خلاف ذلك أحكام أخرى أن كل ملف في الحاسوب يتطلب إذنا خاصا لتفتيشه مسببة حكمها على أساس أن الكومبيوتر يحتوي على العديد من الملفات، وإذا كان أجيز لضابط الشرطة والقضائية فتح الملفات الأخرى الموجودة داخل جهاز الحاسوب فغن ذلك سوف يؤدي بالفعل على الاعتداء على الحياة الخاصة التي يتمتع بها الفرد[2].

ومن الدول التي نصت التي نصت تشريعاتها على ضرورة تحديد مجال الإذن بالتفتيش الولايات المتحدة الأمريكية وكندا حيث نصتا على أن يكون إذن التفتيش متضمننا:

- البحث عن أدلة متحصلة من كيان الحاسب المنطقي والتي يدخل فيها برامج التطبيق ونظم التشغيل.
- البيانات المستخدمة بواسطة برنامج الكومبيوتر.
- السجلات التي تثبت استخدام الأنظمة الآلة لمعالجة البيانات.
- السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات.

ثانيا: ضبط الدليل الرقمي في جريمة الإنترنت

1)تعريف الدليل الرقمي

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص221.

[2]- رشيدة بوكر، المرجع السابق، ص412.

يجب الإشارة قبل البدء في التعريفات أنه قد أصطلح على هذا الدليل عدة تسميات منها: الدليل الرقمي الدليل المعلوماتي والدليل التقني إضافة إلى تعدد التعريفات التي قيلت بشأن الدليل الرقمي وتباينت بين التوسع والتضييق ويرجع ذلك لوضع العلم الذي ينتمي إليه الدليل، فاختلفت بين أولئك الباحثين في مجال التقنية والباحثين في مجال القانون ومن بين التعريفات الدول الرقمي هي:

يعرف الدليل الرقمي أو التقني Digital èvidence أو الإلكتروني Electronique èvidence بأنه «كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من انجاز مهمة لها»[1].

أو أنه «أنه الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ، يمكن تجميعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء»[2].

أو أنه «معلومات مخزنة في أجهزة الحاسوب وملحاقاتها من دسكات وأقراص مرنة وغيرها من وسائل تقنية المعلومات، كالطابعات والفاكس أو المتنقلة عبر شبكات الإتصال والتي يتم تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة بهدف إثبات وقوع الجريمة وتسبتها إلى مرتكبيها»[3].

كما أن ليس للدليل الرقمي صورة واحدة بل يوجد له العديد من الصور والأشكال وهي:

1. **الصورة الرقمية:** وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة وفي العادة تقدم الصورة في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية والصورة الرقمية مثل تكنولوجيا بديلة للصورة التقليدية.

---

[1]- عمر محمد أبو بكر بن يونس، المرجع السابق، ص852.

[2]- ممدوح عبد الحميد عبد المطلب، البحث **والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت** ، دار الفكر القانونية ، مصر، 2006، ص 88.

[3]- عائشة بن قارة مصطفى، المرجع السابق، ص61.

2. **التسجيلات الصوتية:** وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية وتشمل المحادثات الصوتية على الإنترنت.

3. **النصوص المكتوبة:** وتشمل النصوص التي تم كتابتها بواسطة الآلة الرقمية ومنها الرسائل عبر البريد الإلكتروني والبيانات المسجلة بأجهزة الحاسب الآلي.

ووفقا لما قررته وزارة العدل الأمريكية سنة 2002 فإن الدليل الرقمي يمكن أن يأخذ الأشكال التالية:

- السجلات المحفوظة في الحاسوب وهي الوثائق المكتوبة والمحفوظة مثل البريد الإلكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الإنترنت.
- السجلات التي تم إنشاؤها بواسطة الحاسوب وتعتبر مخرجات برامج الحاسوب و بالتالي لم يلمسها الإنسان.
- السجلات التي جزء منها تم حفظه بالإدخال، وجزء آخر تم إنشاؤه بواسطة الحاسوب بعد معالجتها من خلال برامج معين.

كما أن هناك من يقسم أشكال الدليل الرقمي تقسيما يتطابق مع تقسيم الجريمة عبر الحاسب الآلي على النحو التالي:

- أدلة رقمية خاصة بأجهزة الحاسب الآلي وشبكاتها.
- أدلة رقمية خاصة بالشبكة العالمية للمعلومات.
- أدلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

2)ضبط الدليل الرقمي:

إن الغاية من التفتيش في ضبط الأدلة المادية التي تفيد في كشف الحقيقة وعلى ذلك فإن الأشياء المتعلقة بجريمة الإنترنت هي الأثر المباشر الذي يسفر عنه الإجراء، فالأساس القانوني

للضبط هو العلاقة التي تربط بينه وبين الأشياء المتعلقة بالجريمة التي يشملها التحقيق والتي تفيد في كشف الحقيقة ما كان منها ضد المشتبه فيه وما كان في مصلحته.[1]

ولقد تعودت جهات التحقيق في الجرائم التقليدية أن يقع الضبط على الأشياء المادية فقط بوصفها أدلة مادية للجريمة التي يجري التفتيش بشأنها، لكن في مجال الجرائم الانترنت الطبيعية العلمية المعقدة للدليل الرقمي الذي يوجب التفتيش عنه وضبطه لإثبات هذا النوع من الجرائم ليس كالدليل التقليدي، فالبيئة الإفتراضية لا تنتج سكينا أو سلاحا ناريا وإنما تنتج نبضات رقمية تشكل قيمة وجوهر الدليل الرقمي فهل يصلح هذا النوع من الدليل لأن يكون محلا للضبط وما هي الإجراءات المتبعة في ذلك ؟.

1 -مدى صلاحية ضبط أدلة الجرائم الإنترنت:

غنى عن البيان أن الضبط هو وضع اليد على شيء يتصل بالجريمة ويفيد في كشف الحقيقة عنها وعن مرتكبها[2] وهو كما سبق القول لا يرد إلا على الأشياء المادية، وعلى هذا الأساس فإن ضبط المكونات المادية للحاسوب لا يثير مشاكل في الفقه المقارن ولا يوجد خلاف بين فقهاء القانون في إمكانية ضبط هذه المكونات[3]، بل حتى إمكانية ضبط الحاسوب بشكل كامل لتأكيد الاحتفاظ بالدليل إذا كان مشغل الجهاز الجهاز غير متعاون مع جهات التحقيق[4].

لقد اختلفت التشريعات الإجرائية والاتجاهات الفقهية حول مسألة ضبط الأشياء المعنوية والكيانات المنطقية، والتي لا تصلح بطبيعتها محلا لوضع اليد وهي مجردة من دعامتها المادية المثبتة عليها وانقسمت في ذلك إلى اتجاهين:

[1]- ممدوح عبد الحميد عبد المطلب، المرجع السابق ، ص15.

[2]-خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2011،ص170.

[3]- هاشم محمد فريد رستم، المرجع السابق، ص93.

[4]- عفيفي كامل عفيفي، المرجع السابق، ص353.

الاتجاه الأول: يري أصحابه أنه لا يمكن تصور إجراء الضبط على الكيانات المنطقية للحاسوب لانتفاء الكيان المادي عنها، وبالتالي عدم صلاحية البيانات المخزنة آليا لأن تكون محلا للضبط بالكيفية المنصوص عليها بموجب النصوص التقليدية لإنتفاء الطابع المادي عن هذه البيانات، في حال تجردها عن الدعامة المادية[1] ومن التشريعات التي أتخذت بهذا الاتجاه قانون الإجراءات الجنائية الألماني.

الإتجاه الثاني: يري أنصار هذا الإتجاه أن المعطيات المخزنة آليا كونها مجردة عن الدعامة المادية التي تحويها لا يوجد ما يمنع من صلاحيتها بهذه الصورة، لأن تكون محلا للضبط المنصوص عليه بمقتضى النصوص التقليدية مستندين إلى أن الغاية من التفتيش هو ضد الأدلة التي تفيد في كشف الحقيقة وبالتالي يمتد هذا المفهوم ليشمل البيانات الإلكترونية بمختلف أشكالها.

وفي الجزائر فقد تدخل المشرع الجزائري بموجب القانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أين إستحدث المادة 06 التي تنص على أنه «عندما تكشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف الجرائم، أو مرتكبها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفق القواعد المقررة في قانون الإجراءات الجزائية ».

2 -أنواع الأدلة محل الضبط في الجرائم الإنترنت:

إن الغاية من التفتيش هو ضبط شيء يتعلق بالجريمة ويفيد التحقيق الجاري بشأنها سواء أكان هذا الشيء أدوات استعملت في إرتكاب الجريمة أو شيئا نتج عنها، أو غير ذلك مما يفيد في كشف الحقيقة والضبط في مجال الجرائم الإنترنت يتصل بضبط المكونات المادية لأنظمة الحاسوب وضبط المكونات المعنوية والبرمجيات وكذا ضبط المعطيات التي تتناقل أو يجري تبادلها، في نطاق

[1]-عفيفي كامل عفيفي، المرجع السابق، ص358.

شبكة المعلومات التي تربط الحواسيب وما يتصل بها [1]، وعلى هذا الأساس فإن من الأشياء التي يتم ضبطها والتحفظ عليها في الجرائم الإنترنت والتي لها قيمة في إثبات تلك الجرائم ونسبتها إلى المتهم:

أ.ضبط جهاز الكومبيوتر وملحقاته: ذلك أن ضبطه أمر مهم جدا للقول بأن الجريمة الواقعة هي جريمة الإنترنت، وأنه مرتبط بالمكان والشخص الحائز على هذا الجهاز والأجهزة الكومبيوتر [2] وملحقاته أنواع مختلفة الأمر الذي يتطلب في ضابط الشرطة القضائية المعرفة الكافية التي تؤهله للتعامل معه والتعرف على مواصفاته بسرعة.

ب.ضبط المعدات المستعملة في شبكة الإنترنت وأهمها المودم (Modem): وهي الوسيلة التي تمكن أجهزة الكومبيوتر من الإتصال ببعضها البعض عبر خطوط الهاتف.

ج.وسائط التخزين المتحركة: كالأقراص المدمجة وأقراص الليزر والأقراص الملونة والأشرطة المغناطيسية.

د.ضبط البرمجيات (Software) : فإذا كان الدليل الرقمي ينشأ بإستخدام برنامج خاص فإن ضبط الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل .

هـ.ضبط البريد الإلكتروني: والذي يحتوي على برامج متخصصة لكتابة وإرسال وإستعراض وتخزين الرسائل الإلكترونية، وهذه الرسائل لا يختلف التعامل معها عن التعامل مع الرسالة الورقية إذ بمقدور المستخدم أن يطرحها جانبا أو يرد عليها أو ينقلها إلى شخص آخر أو يحفظ بها في ملف خاص، لذلك فالمحقق الذي يريد ضبط الرسائل الإلكترونية (boitte Email) الخاص به يشغل برامج البريد الإلكتروني في جهاز حاسوبه ثم مراجعة قائمة الرسائل ليلتقط من بينها الرسالة المطلوبة.

3 -الصعوبات التي تواجه المحقق أثناء عملية الضبط:

[1]- خالد عياد الحلبي، المرجع السابق، ص169.

[2]- نفس المرجع، ص275.

إن عملية ضبط البيانات المعالجة آليا تواجهها عدة صعوبات أهمها:

أ.ضخامة البيانات التي من الواجب فحصها من قبل المحقق وذلك نتيجة حجم الشبكة التي تحتوي على هذه البيانات، الأمر الذي يتطلب من الخبرة الفنية ما يلزم لتحديد البيانات التي تصلح كأدلة جنائية من عدمه[1].

ب.قد يحتوي النظام المعلوماتي أو شبكة الإنترنت على عناصر لا يمكن فصلها ومع ذلك يتعين ضبطها لأنها تتضمن عناصر الإثبات، فيلزم بالضرورة ضبط النظام أو الشبكة كلها وهو الأمر الذي قد يترتب عليه التوقف عن العمل في المشروعات صاحبة النظام[2]، لذلك فإنه يتعين في هذه الحالة مبدأ التناسب والذي يقصد به اقتصار الضبط على الأدلة التي تفيد في كشف الحقيقة ولها علاقة بالجريمة.

ج.كما أنه قد توجد هذه البيانات والمعطيات في شبكات وأجهزة تابعة لدولة أجنبية مما يستدعي تعاونها مع جهات التحقيق الوطنية.

د.وإذا كانت عملية الضبط لهذه الوسائل التقنية تتم في الأنظمة المعلوماتية الكبيرة أو الشبكات الكبيرة فقد يؤدي إجراء الضبط إلى عزل النظام المعلوماتي بالكامل، عن دائرته لمدة زمنية قد تطول أو تقصر مما قد يتسبب في إلحاق أضرار بالجهة المستخدمة بالنظام بالإضافة على عدم إبداء مستخدمي الأنظمة المعلوماتية الإستعداد للتعاون الكامل والفعال مع سلطات التحقيق لما قد يعنيه إجراء الضبط بالنسبة لها مساسا بالسرية.

هـ.كما أن الضبط في مجال الإنترنت قد يمثل أحيانا إعتداء على حقوق الغير أو على حرمة حياته الخاصة مما يستوجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات ومن الصعوبات كذلك التي تعيق الوصول إلى ضبط الدليل الرقمي تلك الأحزمة الأمنية المفروضة من قبل مستخدم النظام حول البيانات التي يحويها هذا النظام، ومما يزيد من صعوبة الأمر على المحقق الجنائي عدم معرفته

[1]- عفيفي كامل عفيفي، المرجع السابق، ص355.

[2]- شيماء عبد الغني، المرجع السابق، ص358.

لكلمة السر أو شفرة المرور أو شفرة ترميز البيانات وقد لا يبدي المشتبه فيه تعاون في الكشف عن هذه الشفرات لجهات التحقيق.

1) إجراءات ضبط الدليل الرقمي:

يصعب إقامة الدليل على الجرائم التي تقع على العمليات الالكترونية المختلفة وذلك بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة، لأن محل تلك الجرائم كما عرفنا سابقا هو جوانب معنوية تتعلق بالمعالجة الآلية للمعطيات والتي تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة لا يمكن للإنسان قرائتها أو إدراكها إلا من خلال هذه الحواسيب التي تحفظها ولأجل ذلك فإن القواعد التقليدية في الإثبات لا تكف لضبط مثل هذه البيانات لذلك فإن طريقة ضبط المعلومات المعالجة آليا تختلف عما هي عليه عند ضبط مكونات المحسوسة كالأقراص المرنة، المودم، والخادم.

ومن خلال دراستنا للقانون 04/09 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، نجد أن المشرع وضع طريقتين لضبط الأدلة الرقمية وهي:

الطريقة الأولى: وتكون عن طريق نسخ المعطيات [1] محل البحث عن دعامة تخزين الكترونية تكون هذه الأخيرة قابلة لحجزها ووضعها في إحراز، حسب ماهو مقرر في قواعد تحريز الدليل المنصوص عليها في قانون الإجراءات الجزائية.

الطريقة الثانية: تكون باستعمال التقنيات المناسبة لمنع الأشخاص المرخص لهم باستعمال المنظومة المعلوماتية[1]، من الوصول إلى المعطيات، التي تحويها هذه المنظومة أو القيام بنسخها ويكون ذلك في حالة ما إذا استحال لأسباب تقنية ضبط هذه المعطيات وفق الطريقة الأولى.

[1] – تنص المادة 06 من قانون 04/09 تتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على انه «عندما تكشف السلطة التي تباشر التفتيش لمنظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف = =عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل منظومة، يتم نسخ المعطيات محل البحث وكذا معطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والموضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية».

وإن كان الدليل الرقمي يخضع في ضبطه إلى قواعد تحرير الأدلة الجنائية عموما إلا أنه ونظرا إلى الطبيعة الخاصة له، فإن عملية ضبطه وتحريره تحتاج إلى بعض الإجراءات الخاصة لحمايته فنيا والحفاظ عليه وصيانته من إمكانية العبث به وهو ما نوه عليه المشرع حينما وجب على السلطات التي تقوم بعملية ضبط الدليل الرقمي أن تسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية [2]، وأن لا يؤدي استعمال الوسائل التقنية في ذلك إلى المساس بمحتوى هذه المعطيات ومن هذه الإجراءات الخاصة في هذا الإطار نذكر على سبيل المثال:

1. أخذ نسخة احتياطية عن المعطيات والعمل عليها لضمان عدم المساس بالدليل الأصلي.ذ
2. عدم تمثيل برامج على الحاسوب مسرح الجريمة خوفا من إتلاف الأدلة الموجودة عليه أو محو الذاكرة أو الملفات أو عدم السماح للمشتبه به بالتعامل مع الحاسوب.
3. ضبط الدعائم الأصلية للمعلومات وعدم الإقتصار على ضبط نسخها.
4. عدم ثني القرص لان ذلك يؤدي إلى تلفه وفقدانه للمعلومات المسجلة عليه.
5. عدم تعريض الأقراص والأشرطة الممغنطة لدرجات حرارة عالية ولا إلى الرطوبة.

المطلب الثاني: إجراءات البحث والتحري الخاصة

لم تسلم طرق الإثبات من تأثيرات ثورة المعلومات وتكنولوجيا الاتصال فالتناغم المطلوب تحقيقه دائما بين طبيعة الدليل وطبيعة الجريمة التي يولد منها ويصلح لإثباتها، أفرز إلى حيز الوجود طرقا إجرائية تتناسب والطبيعة التقنية لجريمة الإنترنت ولدليل الرقمي لكي يمكن عن طريقها الوصول إليه واستخلاصه، ونقصد بذلك تكريس تقنية المعلومات لجمع الدليل الرقمي ومن ضمن

[1] – تنص المادة 7 من قانون 04/09 المتضمن للقواعد الخاصة من الجرائم للوقاية المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على انه «إذا استحال إجراء الحجز وفقا لما هو منصوص في المادة 6 أعلاه لأسباب تقنية يتعين على هذه السلطة التي تقوم بالتفتيش على استعمال التقنيات المناسبة لمنع الوصول لإلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة».

[2] تنص المادة 3/6 من قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على انه «يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية».

المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته في مكافحة الجريمة المعلوماتية، ومن بينها جريمة الإنترنت، هذا ما جاء به في القانون 06/ 22 المؤرخ في 2006/12/20 المعدل والمتمم لإجراءات الجزائية من خلال إجرائي التسرب واعتراض المراسلات ثم من خلال 04/09 استحدث إجرائين آخرين وهما المراقبة الإلكترونية[1] وحفظ المعطيات المتعلقة بحركة السير.

الفرع الأول: التسرب

إن التطرق إلى عملية التسرب أو مباشرة العمل بهذا أسلوب مرتبط بطبيعة الجرائم حيث أن المشرع الجزائري أجاز اللجوء إلى هذا الإجراء في إطار محدد وخصصه للجرائم الحديثة والتي سميت بالجرائم الخطيرة دون غيرها من باقي الجرائم المنصوص عليها في قانون 22/06 هذا القانون الذي جاء معدلا ومتمما لقانون الإجراءات الجزائية الجزائري أجاز اللجوء إلى عملية التسرب كوسيلة تحري خاصة في جرائم محددة.[2]

أولا: الجرائم الماسة بأنظمة المعالجة (جرائم الالكترونية)

لقد سن الفقهاء عدد كبير من التعريفات لهذا النوع من الجرائم المصطلح على تسميتها بجرائم الكومبيوتر منها:

أنها كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه.

ومن التعريفات التي تنطلق من وسيلة ارتكاب الجريمة فإن أصحابها منطلق من أن جريمة الكومبيوتر تتحقق باستخدام الكومبيوتر ووسيلة لارتكاب الجريمة من هذه التعريفات أنها: الجريمة التي تلعب فيها البرامج المعلوماتية دورا رئيسيا حسب تعريف مكتب تقيم التقنية بالولايات المتحدة الأمريكية.

[1]- للمزيد من التفاصيل ينظر إلى المبحث الأول.

[2]- حمزة قريشي، الوسائل الحديثة في البحث والتحري في قانون الجزائري، ط1، الجزائر، 2017، ص143.

لقد تأثر المشرع الجزائري بالجدال العالمي الذي أفرزته التطورات المذهلة لأنظمة المعلوماتية فاعتبر المساس بها جرائم أدرجها في القسم السابع مكرر من قانون العقوبات المعدل بالقانون 22/06 المؤرخ في 2006/12/20 بما سماه بأنظمة المعالجة الآلية للمعطيات بالمواد 394 مكرر إلى 394 مكرر 7.

ومن الأفعال المعاقب عليها ما يلي: (إدخال أو إبقاء عن طريق الغش في كل الأجزاء من أجزاء المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، حذف وتغيير لمعطيات المنظومة، وتخريب أشغال المنظومة، إزالة وتعديل عن طريق الغش معطيات آلية، القيام عن طريق الغش بتصميم أو بحث أو تجميع أو بحث أو نشر أو اتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية عمدا، حيازة أو إفشاء أو نشر أو استعمال عن طريق الغش للمعطيات المتحصل عليها)، أضاف المشرع مقررا نفس العقوبات لمحاولة في هاته الجرائم وكذا قرر العقوبات على الشخص المعنوي المرتكب.[1]

ثانيا: في قانون الإجراءات الجزائية

أجاز قانون الإجراءات الجزائية المعدل والمتمم لضباط الشرطة القضائية القيام بهذه العملية لكنه قيدهم بجملة من الشروط لابد من توافرها لكي يكون هذا الإجراء صحيحا ومنتجا لأثاره وهي:

1) أن يصدر الإذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية المختص وهذا ما أكدت عليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية المعدل والمتمم.[2]

2) أن يوجه هذا الإذن لضباط الشرطة القضائية أو أحد أعوانه تحت مسؤولية الضابط.

[1]- حمزة قريشي، المرجع السابق، ص148.

[2]- تنص المادة 65 مكرر 11 من قانون الإجراءات الجزائية المعدل والمتمم على انه «عندما تقضي ضرورة التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه».

3) أن تكون الجريمة المتسرب فيها تشكل احد الجرائم المنصوص عليها في المادة 65 مكرر 5 من قانون الإجراءات الجزائية.[1]

4) أن يكن الإذن مكتوبا ومتسببا ومحدد المدة وإلا كانت تحت طائلة البطلان وفقا لما ورد في المادة 65 مكرر 15 من قانون الإجراءات الجزائية المعدل والمتمم.

5) يتعين على العضو المتسرب إعداد تقرير يتضمن جميع ما قام به من إجراءات لمعاينة الجريمة شرط أن لا يتعرض هذا العضو والمسخرين لهذه المهنة للخطر.

ثالثا: شروط التسرب

من أجل أن تتم عملية التسرب وانجاح العملية وتسهيل متابعة جريمة الإنترنت و المجرمين ومهام المتسرب[2]، فقد أحاط المشرع جملة من الشروط يعين مراعاتها عندما تقتضي التحريات كون هذا الاجراء من اخطر الاجراءات انتهاكا لحرمة الحياة الخاصة للمشتبه فيه. وتمثل هذه الشروط في: شكلية وأخرى موضوعية سنتناولها:

أ. **الشروط الشكلية:**

- أن يكون صادر بإذن قضائي إما وكيل الجمهورية أو قاضي التحقيق المختص.
- أن يكون إدن مكتوبا وإلا وقع تحت طائلة البطلان.
- ذكر اسم الضابط التي تتم عملية التسرب تحت مسؤوليته او عون الشرطة القضائية باعتباره مساعدا له.[3]
- المدة المطلوبة لعميلة التسرب 4 محددة قانونا قابلة للتجديد ويمكن توقيفها حتى انتهاء المدة المحددة لها.

[1]- تنص المادة 65 مكرر 05 من قانون الإجراءات الجزائية المعدل والمتمم على انه « إذا اقتضت ضرورات في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبيض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد....».

[2]- محمد حزيط، مذكرات في قانون الاجراءات الجزائية الجزائري، الطبعة2، دار هومة، الجزائر، 2010،ص65.

[3]- ينظر المادة 65 مكرر 16 من تعديل 2006 من قانون الاجراءات الجزائية الجزائري.

ب. الشروط الموضوعية:

- تسبيب الإذن بالتسرب خاصة إذا أثبت أن الاعتداء على الوسائط الفعلية العادية غير كافي للتوصل إلى الحقيقة ومن ثم لابد من وكيل الجمهورية او قاضي التحقيق ان يقدم تيريرا على اساس الذي تم الاعتماد عليه من أجل السماح بالقيام بعملية التسرب.
- إن نوع الجريمة هي من الجرائم الماسة يأنظمة المعالجة الآلية للمعطيات.

الفرع الثاني: اعتراض المرسلات وحفظ المعطيات المتعلقة بحركة السير

ولقد كانت اعتراض المراسلات من بين الإجراءات الخاصة في عملية البحث والتحري في جريمة الإنترنت.

أولا: اعتراض المرسلات

نظم المشرع الجزائري اعتراض المرسلات وتسجيل الأصوات والتقاط الصور في المواد من 65 مكرر 5 إلى غاية المادة 65 مكرر 10، والتي تجيز لضباط الشرطة القضائية واعوانهم القيام بهذه الأعمال إذا اقتضت الضرورات التحري في الجرائم المتلبس بها أو بعض الجرائم وذلك بموجب إذن من وكيل الجمهورية المختص او بموجب إذن من قاضي التحقيق الابتدائي تتمثل هذه الأعمال فيما يلي:

-اعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلكية واللاسلكية.

-اجراء ترتيبات تقنية من أجل التقاط تثبيت بث وتسجيل الكلام المتفوه به من طرف الأشخاص في اماكن العامة او الخاصة، والتقاط الصور لشخص دون موافقة المعنيين بالأمرك.

المشرع الجزائري لم يعرف مصطلح الاعتراض وقد عرفه القانون الأمريكي بأن "الاعتراض هو الحصول على محتوى الاتصال السلكي او الالكتروني أو الشفوي وذلك باستعمال أي وسيلة الكترونية أو ميكانيكية أو أي وسيلة أخرى[1]".

تسجيل الاصوات:

[1]- شيماء عبد الغني محمد عطا الله، المرجع السابق، ص 251.

يقصد يه مراقبة الأحداث وتسجيلها وكل الاتصالات التي تتم عن طريق سلكي او لا سلكي، أي ان عملية المراقبة تشمل كل أدوات الاتصال سواء سلكية أو لاسلكية، وتتمثل في وضع تقنية دون موافقة المعنيين من اجل التقاط و تثبيت و بث وتسجيل الكلام المتفوه به بصقة خاصة او سرية من طرف شخص أو عدة أشخاص.

التقاط الصور:

هي تلك العملية التقنية التي يتم بواسطتها التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

والمشرع الجزائري أجاز طبقا للمادة 65 مكرر 5 ضباط الشرطة القضائية القيام بالاعتراض للمراسلات تسجيل الأصوات والتقاط الصور لكنه قيدهم بجملة من الشروط لتكون اجراءاتهم صحيحة ومنتجة لأثارها وهي:

- أن يدر الإذن من وكيل الجمهورية او قاضي التحقيق المختصين.
- أن يوجه هذا الإذن لضباط الشرطة القضائية فلا بجوز أن يوجه لأحد الأعوان لأن مهمتهم تنحصر في مساعدة الضباط.
- أن يقوم الضابط بهده الأعمال سعيا للكشف عن جرائم حددها المشرع في المادة 65 مكرر 5 وهي مذكورة على سبيل الحصر، وقد يرجع ذلك للخطورة الاجرامية لهذه الأعمال وأثرها على السياسة العامة في الدولة واقتصادها اما إذا كانت هذه الاعمال في غير هذه الجرائم فإجراؤه باطل.
- أن بكون هدا الإذن مكتوبا ومحدد المدة إلا إذا كانت تحت طائلة البطلان.
- يتعين على ضباط القائم بهذه المهمة تحرير محضر يتضمن كافة الأعمال والإجراءات التي قام بها كما يتضمن وصفا دقيقا للوقائع المثبتة لصحة ما قام به، كما يتعين عليه تحديد ساعة انطلاقه لمباشرة الأعمال ووقت أعمالها.

-إن تقييد ضابط الشرطة القضائية بجميع الشروط والقيود التي تطلبها قانون الإجراءات الجزائية أثناء قيامهم بهذه الأعمال وهي اعتراض المراسلات وتسجيل الأصوات، والتقاط الصور لا يعني أن الجهات المعنية النيابة العامة وقضاة التحقيق أو الحكم، مجبرة على الأخذ بها فهي كغيرها من الأعمال تحرر في محضر وتودع في الملفات وهذه الأخيرة سلطة تقدير إمكانية الأخذ بها أو استبعادها.

ثانيا: حفظ المعطيات المتعلقة بحركة السير

قررت التشريعات الحديثة ومنها المشرع الجزائري ملزم في تقديم خدمات حفظ المعطيات المتعلقة بحركة السير ضمان للوصول إلى أثار الجريمة مهما كانت.

أ. تعريفها:

ويقصد بمقدمي الخدمات أي كيان عام او خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام اتصالات وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصالات المذكورة أو مستعمليها.[1]

وبقصد بالمعطبات المتعلقة بحركة السير، هي تلك المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها تلك الأخيرة باعتبارها جزء من حلقة اتصال توضح مصدر الاتصال، والوجهة المسلة إليها والطريق الذي يسلكه، ووقت وتاريخ وحجم مدة الاتصال ونوع الخدمة.[2]

ب. المعطيات الواجب حفظها:

وقد حدد المشرع الجزائري المعطيات التي يجب على مقدمي الخدمات حفظها إلى ما يلي:

-المعطيات التي تسمح بالتعرف على مستخدمي الخدمة.

-الخدمة التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم وكذا عناوين المواقع.

[1]- ينظر للمادة 12 فقرة "د" من قانون 04/09.

[2]- ينظر للمادة 2 فقرة "ه" من قانون 04/09

-الخصائص التقنية وكذا تاريخ ووقت ومدة الاتصال وتكون مدة الحفظ لا تتجاوز سنة، وإلا تعرض مقدمي الخدمة للعقوبات المقرر في المادة 11 من قانون 04/09.

الخصائص التقنية و كذا تاريخ و وقت و مدة الاتصال و تكون مدة الحفظ لا تتجاوز سنة، و إلا تعرض مقدمي الخدمة للعقوبات المقررة في المادة 11من قانون 04/09.

خاتمة

خاتمة:

لقد أضحى العالم اليوم يعيش في زمن التطور التكنولوجي أو ما يعرف بالثورة المعلوماتية، حيث أصبحت حياتنا اليومية تستدعي اللجوء إليها فقط مكنت طرق المعالجة الآلية لمعطيات المجتمعات من تجاوز فكرة الحدود الإقليمية نظرا لكون التكنولوجيا أو العزيمة هي عابرة للحدود.

وأمام هذا التطور فقط ارتبطت به ظهور ما يعرف بجرائم الإنترنت وذلك نتيجة لاستخدام السيئ للنظم المعلوماتية أو الحاسوب الذي نتج عن هذا الأخير عدة أضرار لا يمكن حصرها، وذلك لأنها تهدد أمن المعطيات من جهة وتمس بحرية الأفراد والمؤسسات من جهة أخرى.

ولأن الحماية الفنية مهما بلغت درجتها من التعقيد والصعوبة فهي لا تستطيع المقاومة أمام التطور التقني الذي تشهده تقنيات الاختراق وكذا عجز النصوص التقليدية في توفير الحماية خاصة من الناحية الإجرائية، ما دفع العديد من الدول إلى إبرام اتناقيات وسن قوانين داخلية من أجل توفير الحماية الجنائية الإجرائية لها ومن هذه الدول الجزائر.

وقد حاولنا من خلال الفصلين الكاملين الوقوف على حل الأحكام الإجرائية الخاصة بمتابعة مرتكبي جرائم الإنترنت من أجل إقرار الحماية لها فوجدنا أن لجريمة الإنترنت خصوصية من الناحية الإجرائية من خلال اعتمادنا على قانون الإجراءات الجزائية الجزائري وكذا قانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

في هذا المقام وجدنا أن هناك بعض الإجراءات تعتبر قاسما مشتركا بين الجرائم التقليدية وجرائم الإنترنت، كالمعاينة على مسرح الجريمة وكذا التفتيش الالكتروني وضبط الدليل الرقمي والمستحدث إجراءات جديدة جاء بها تعديل قانون الإجراءات الجزائية سنة 2006 التي تعرف بأساليب التحري حيث تعتبر كل هذه الإجراءات سواء كانت جريمة إنترنت أو تقليدية.

الآن وقد فرغنا من هذا البحث نستطيع القول أن النتائج التي توصلنا إليها تتمثل في:

-إن التقنية المعلوماتية أصبحت من أساسيات حياة الدول والشعوب ولا يمكن تصور فكرة التخلي عنها، نظرا لتزايد مجالات استعمالاتها في كافة المجالات، وذلك بالرغم من كافة التهديدات التي تشكلها جريمة الإنترنت على امن وسلامة نظامها ومستعمليها.

-وتعتبر مرحلة إجراءات البحث والتحري من ابرز واهم المراحل التي يستعان بها لمواجهة جرائم الإنترنت ولقد تم تسخير ضبطية قضائية مختصة للقيام بمباشرة إجراءاتها مهمتها تحديد لمستخدمي هذه الشبكة ما يباح وما لا يباح فيها.

-وتختلف هذه الضبطية على الضبطية القائمة على مباشرة إجراءات مرحلة البحث والتحري في الجرائم التقليدية، لكونها لا تعتمد على التدريبات المادية أو الفيزيولوجية التي يتلقاها هؤلاء للوصول إلى هذه المرتبة، وإنما تعتمد على قوة تكوين البناء العلمي والتكنولوجي لأفرادها.

-والى جانب الضبطية القضائية هناك ضبطية إدارية مختصة في الحيلولة دون وقوع جرائم الإنترنت وذلك عن طريق القيام بدوريات في غرف الدردشة لمراقبة ما يحدث فيها.

-وتباشر شرطة الإنترنت اختصاصاتها إما على المستوى الوطني، كالمكتب المركزي بمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات الموجود في فرنسا، أو على المستوى الأوروبي كالأورجيست أو على المستوى الدولي كالانتربول.

-بالرغم من ذلك فإن مأموري الضبط القضائي يتبع بشأن جرائم الإنترنت ذات الإجراءات التي يتبعها بشأن الجرائم التقليدية مع نوع الخصوصية التي تتماشى مع طبيعتها، سواء في ظل ظروف العادية أو في ظل الظروف الاستثنائية، فيلاحظ أن البلاغ عن جرائم الإنترنت يتم بنفس الطريقة التي يتم فيها التبليغ عن الجرائم التقليدية وهي إما عن طريق البلاغ المادي وذلك إما كتابيا أو شفويا، أو عن طريق البلاغ المعنوي وذلك بإرسال بريد أو عن طريق مكالمة هاتفية، وذلك بإرسال رسالة الكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالبحث والتحري، أو عن طريق ملأ استمارات رقمية متواجدة في المواقع المخصصة لتلقي البلاغات والشكاوى.

-أما المعاينة فهي لا تتمتع بنفس الدرجة من الأهمية التي تتمتع بها في مسرح الجرائم التقليدية بسبب قلة الآثار المادية المتخلفة عن جرائم الإنترنت.

-أما التفتيش فنلاحظ أن المشرع الجزائري من خلال قانون 04/09 أجاز في إطار التحري والتحقيق في جريمة الإنترنت تفتيش محل آخر غير السكن، و هو المنظومة المعلوماتية كما اقترح المشرع إضافة

فقرة أخرى للمادة 05من قانون 04/09 كما يلي "لا يجوز إجراء عمليات التفتيش في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة ."

-أما بالنسبة فيما يخص ضبط الدليل الرقمي فيجب على مأمور الضبط القضائي بأن يرد على البيانات الالكترونية إلى جانب الأشياء المادية كضبط المراسلات الالكترونية كالبريد الالكتروني .

-وإن عملية التسرب في نطاق جرائم الاعتداء على أنظمة المعالجة الآلية في ولوج ضباط أو عون الشرطة القضائية إلى العالم الإفتراضي واشتراكه مثلا في محادثات غرف الدردشة أو حلقات النقاش أو الاتصال المباشر في كيفية قيام أحدهم باختراق شبكات أو بث الفيروسات.

-وتكون المراقبة الالكترونية هي الأخرى من أهم مصادر التحري التي يستعان بها في البحث والتقصي عن جرائم الإنترنت، ويقوم بها مراقب الكتروني يتمثل في مأمور ضبط قضائي ذو كفاءة تقنية عالية ومحلها هو شبكة الاتصالات والتقنية المستخدمة فيها هي التقنية الالكترونية.

-تعتمد إجراءات البحث والتحقيق في مجال جرائم الإنترنت على القواعد الفنية العملية أكثر منه على القواعد الإجرائية القانونية، فلا جدوى من النص من توفر المهارة اللازمة للتعامل مع جريمة الإنترنت، كما أن حسن سير الإجراءات ذات الطبيعة الفنية والعملية يعتمد مباشرة على مدى توفر الوسائل المادية الضرورية من حواسيب متطورة وشبكات اتصال مؤمنة، وبرامج خاصة تسمح بتحصيل الدليل الالكتروني، تسهل من مهمة الخبير في مجال البحث والتحري المعلوماتي.

-إن إجراءات البحث والتحري هي إجراءات من نوع خاص يشترط لمباشرتها التقيد بمجموعة من الشروط أهمها التقيد بالنص الإجرائي الملائم، لما قد تنطوي عليه هذه الإجراءات من مساس بالحريات الفردية والإطلاع على مستودع سر الأفراد كالتصنت الالكتروني واعتراض البريد الالكتروني، وحجز المعطيات والبيانات الشخصية وكل ذلك حفاظا على سلامة الإجراءات من طائلة البطلان وكذلك حفاظا على حرية الأفراد وكرامتهم.

بعد استعراض النتائج تم التوصل إلى مجموعة من التوصيات:

-أن يتم تنسيق دولي وسياسات جنائية من أجل وضع قانون لمكافحة جرائم الإنترنت.

-تعزيز عمل الجهات الأمنية والقضائية في مجال مكافحة جرائم الإنترنت، وذلك من خلال تدريب الكفاءات العاملة على طبيعة الإجراءات المتخذة في مجال جرائم الإنترنت ومدى خصوصية هذا النوع من الجرائم والمجرمين في آن واحد.

-ضرورة إنشاء لجان مخصصة في مكافحة جرائم الإنترنت في الدول العربية.

-ضرورة العمل على تحسيس ضحايا جرائم الإنترنت بضرورة تبليغ عن أي جريمة قد يقعون ضحايا لها، إضافة إلى الإطلاع على كافة الأساليب الإجرامية الحديثة المستعملة في مجال جريمة الإنترنت.

-ضرورة تسجيل أسماء الأشخاص الذين يستخدمون الشبكة في مقاهي الإنترنت والمدة التي استغرقوها.

-إبرام اتفاقيات تنظم وقت امتداد إجراءات التفتيش خارج الدولة وكيفية اتخاذ مثل هذا الإجراء.

-نشر الوعي والثقافة المطلوبة لدى مستخدمي شبكة الإنترنت حتى لا يقعو في عملية النصب والاحتيال عن طريق شبكة الإنترنت.

-وضع سجل أمني إلكتروني يتضمن قائمة بمجرمي المعلوماتية يسمح بوضعهم تحت المراقبة الأمنية أي رصد نشاطاتهم المعلوماتية المشبوهة عبر الشبكة.

الإسراع لسن القواعد الإجرائية الخاصة تتلائم مع طبيعة الإنترنت وإعادة النظر في مدى تطبيق قوانين من عدمه.

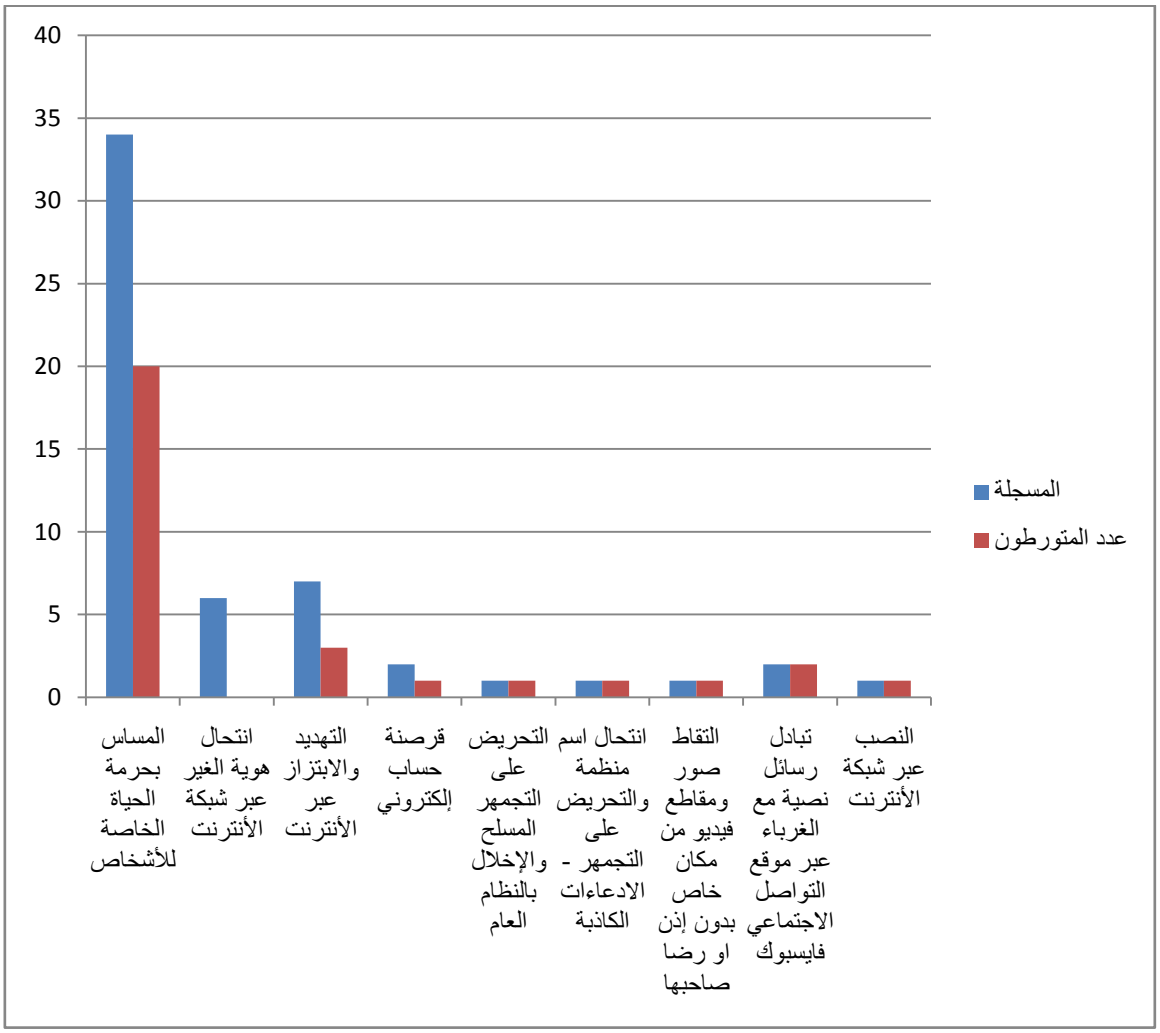
الملاحق

الملحق رقم 01: قضايا الجرائم الإلكترونية المسجلة خلال سنة 2017

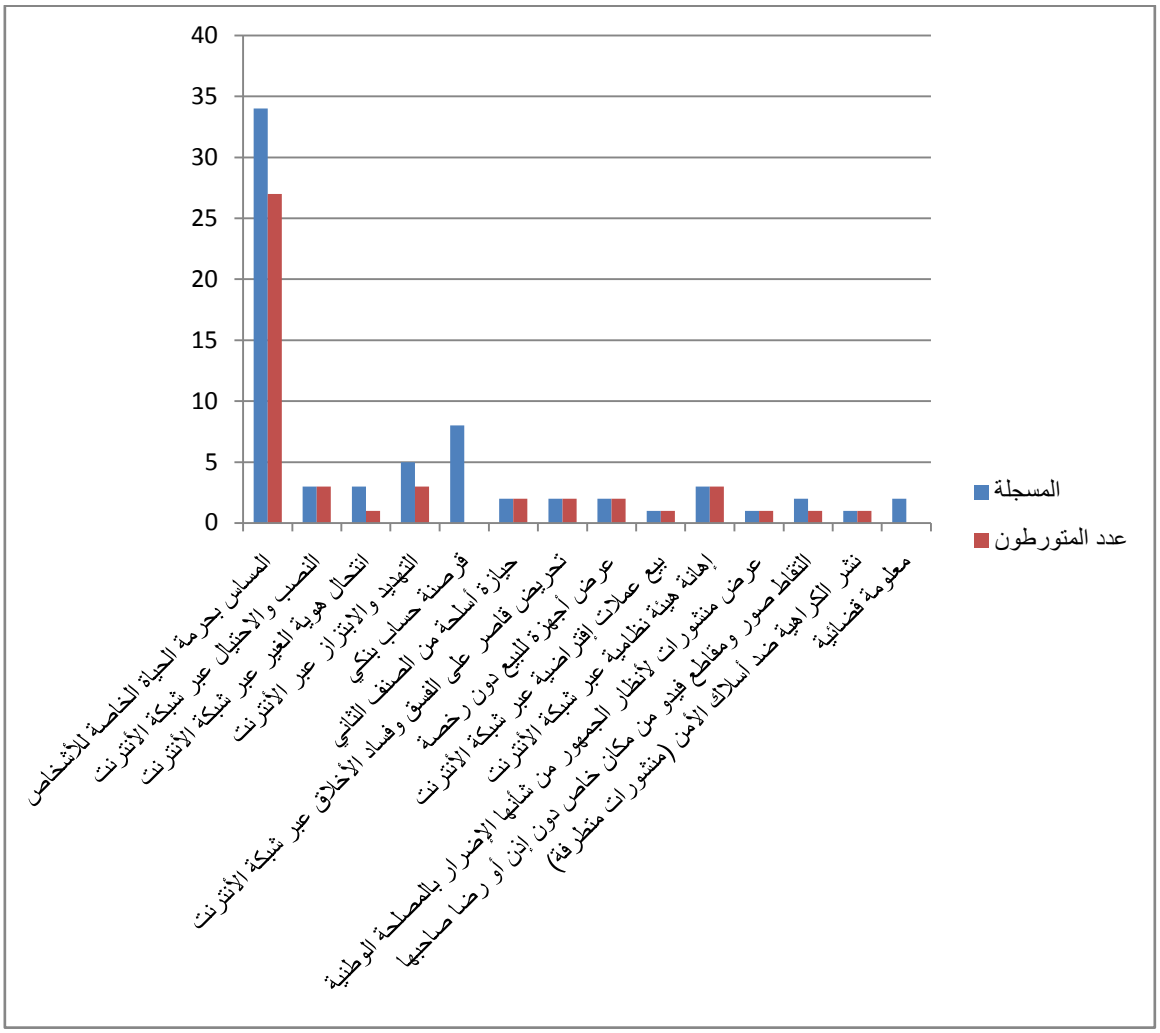
طبيعة الجريمة	المسجلة	عدد المتورطون
المساس بحرمة الحياة الخاصة للأشخاص	34	20
انتحال هوية الغير عبر شبكة الأنترنت	6	
التهديد والابتزاز عبر الأنترنت	7	3
قرصنة حساب إلكتروني	2	1
التحريض على التجمهر المسلح والإخلال بالنظام العام	1	1
انتحال اسم منظمة والتحريض على التجمهر –الادعاءات الكاذبة	1	1
التقاط صور ومقاطع فيديو من مكان خاص بدون إذن او رضا صاحبها	1	1
تبادل رسائل نصية مع الغرباء عبر موقع التواصل الاجتماعي فايسبوك	2	2
النصب عبر شبكة الأنترنت	1	1

من خلال الإحصائيات المذكورة في الجدول أعلاه يتبين لنا أن الجرائم الإلكترونية في سنة 2017 كانت قليلة نوعا ما فقد بلغت على المستوى المحلي –ولاية تيارت– حوالي 55 قضية مسجلة عند مصالح الشرطة القضائية وأغلبها جرائم المساس بحرمة الحياة الخاصة للأشخاص فقد بلغت أكثر من 80 % وهذا ما يوضحه التمثيل البياني أدناه –الملحق رقم 02–.

الملحق رقم 02: قضايا الجرائم الإلكترونية المسجلة خلال سنة 2017



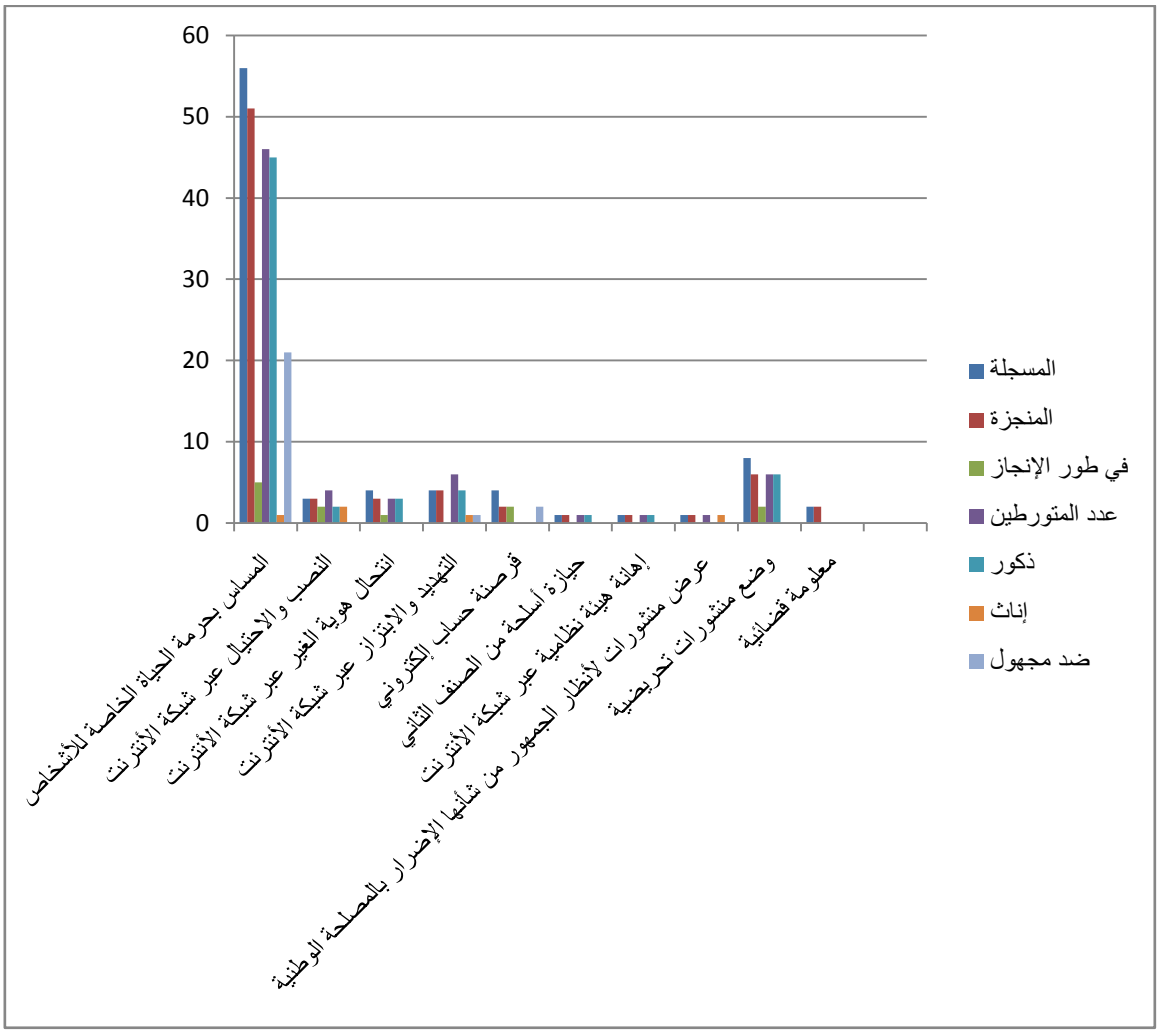
الملحق رقم 03: قضايا الجرائم الإلكترونية المسجلة خلال سنة 2018



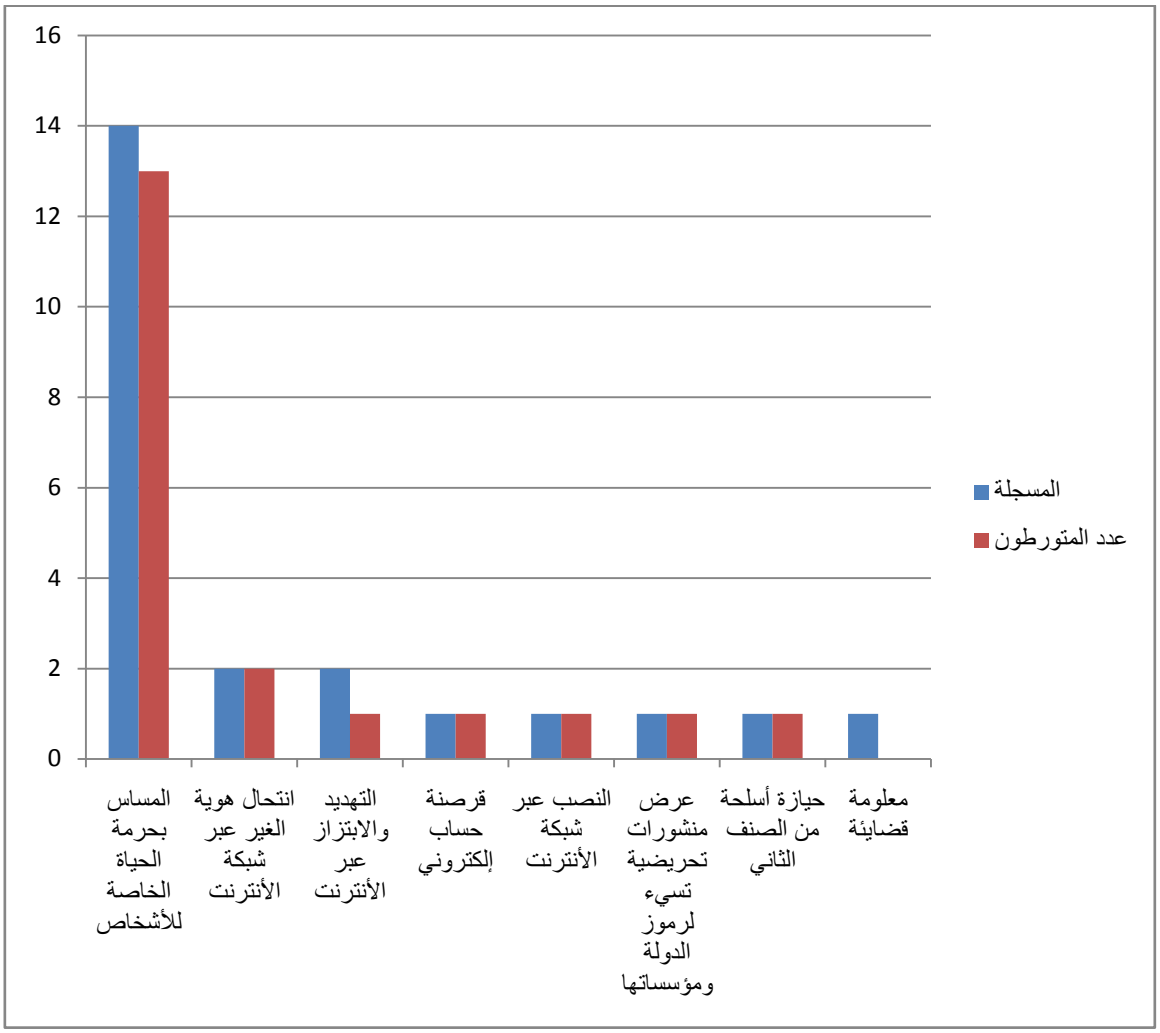
الملحق رقم 04: قضايا الجرائم الإلكترونية المسجلة خلال سنة 2019

طبيعة الجريمة	المسجلة	المنجزة	في طور الإنجاز	عدد المتورطين	ذكور	إناث	ضد مجهول
المساس بحرمة الحياة الخاصة للأشخاص	56	51	5	46	45	1	21
النصب والاحتيال عبر شبكة الأنترنت	3	3		4	2	2	
انتحال هوية الغير عبر شبكة الأنترنت	4	3	1	3	3		
التهديد والابتزاز عبر شبكة الأنترنت	4	4		5	4	1	1
قرصنة حساب إلكتروني	4	2	2				2
حيازة أسلحة من الصنف الثاني	1	1		1	1		
إهانة هيئة نظامية عبر شبكة الأنترنت	1	1		1	1		
عرض منشورات لأنظار الجمهور من شأنها الإضرار بالمصلحة الوطنية	1	1		1		1	
وضع منشورات تحريضية	8	6	2	6	6		
معلومة قضائية	2	2					
المجموع	84	74	10	67	62	5	24

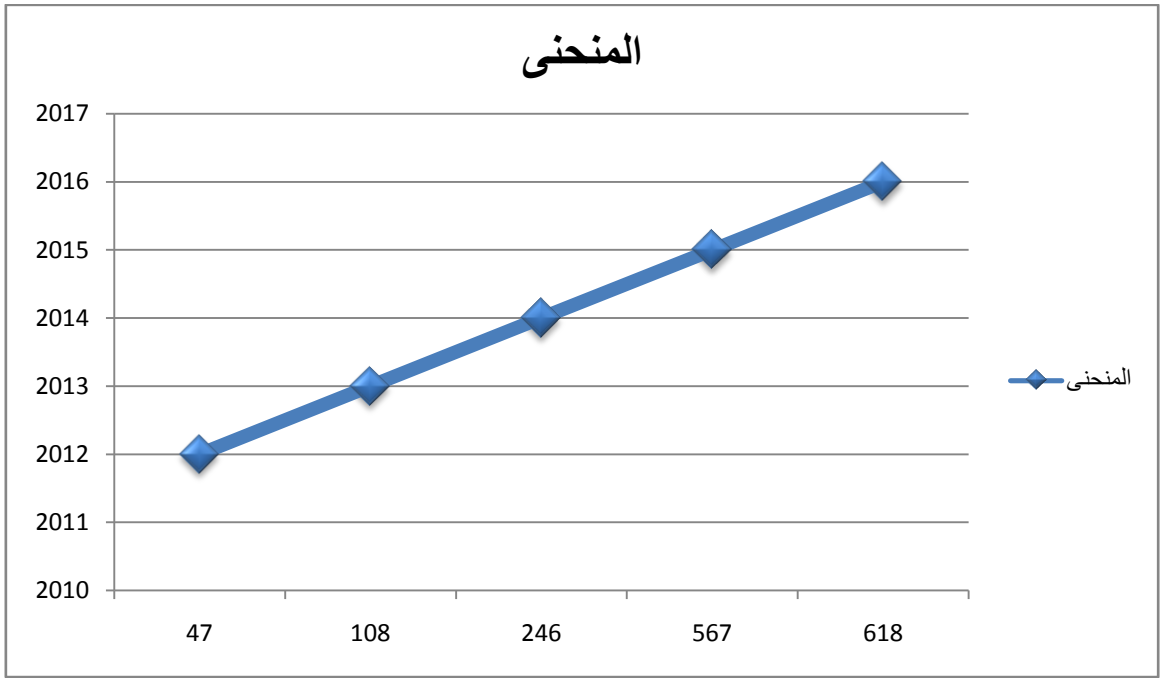
الملحق رقم 05: قضايا الجرائم الإلكترونية المسجلة خلال سنة 2019.



الملحق رقم 06: قضايا الجرائم الإلكترونية المسجلة خلال فترة 2019/01/01 إلى غاية 2019/05/31



الملحق رقم 07: إحصائيات الجريمة الإلكترونية على المستوى الوطني خلال فترة (2012– 2016)



قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: النصوص التشريعية.

أ–الدساتير:

1–الدستور الجزائري المعدل بموجب القانون رقم 20–251 المؤرخ في 27 محرم عام 1442 الموافق لـ 15 سبتمبر 2020 المتضمن التعديل الدستوري، ج ر ج ج، العدد 54، المؤرخة في 16 سبتمبر 2020.

ب–القوانين:

2–الأمر رقم 66–156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، ج.ر ج ج، العدد49، الصادرة في 11 جوان 1966، المعدل والمتمم بموجب الأمر 20–01 المؤرخ في 09 ذي الحجة 1441هـ الموافق لـ 30 يوليو 2020، ج ر ج ج، العدد 44، الصادر في 30 يوليو 2020.

3–القانون 04/09الصادر بتاريخ 16 أوت 2009، الجريدة الرسمية رقم 47، ص05.

ثانيا: الكتب.

4–جمال جرجس مجلع تاوضروس، **الشرعية الدستورية لأعمال الضبطية القضائية** ، النسر الذهبي للطباعة عابدين، مصر، 2006.

5–جميل عبد الباقي الصغير، **الجوانب الإجرائية للجرائم المتعلقة بالإنترنت** ، دار النهضة العربية، القاهرة، مصر، 2002.

6–حمزة قريشي، الوسائل الحديثة في البحث والتحري في قانون الجزائري، ط1، الجزائر، 2017.

7–خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2011.

8–خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2010.

9-ممدوح عبد الحميد عبد المطلب، **البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت** ، دار الفكر القانونية ، مصر، 2006.

10-رشيدة بوكر خالد ممدوح إبراهيم، **جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن**، منشورات الحلبي الحقوقية، الطبعة الأولى، 2012.

11- زبيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي** ، دار الهدى، عين ميلة، الجزائر، 2011.

12-صادق المرصفاوي، **أصول الإجراءات الجنائية في القانون المقارن** ، منشأة المعارف، الإسكندرية، 1982.

13-عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجنائي والقانون المقارن، دار الجامعة الجديدة، 2010.

14-عبد الفتاح بيومي حجازي ،**جرائم الكومبيوتر والإنترنت**، دار الكتب القانونية، مصر ،2007.

15-عبد الفتاح بيومي حجازي، **الجوانب الإجرائية لأعمال التحقيق** ، دار النهضة العربية، القاهرة، ط1، 2009.

16-عبد الله حسين على محمود، **سرقة المعلومات المخزنة في الحاسب الآلي** ، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 2002.

17-عبد الله ماجد العكايلة، **الوجيز في الضبطية القضائية**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

18-عفيفي كامل عفيفي، **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون**، بدون دار نشر.

19-مدحت رمضان، الوجيز في شرح قانون الإجراءات الجزائية الاتحادي لدولة الإمارات العربية المتحدة، دار النهضة العربية، القاهرة 2000 -2001.

20-علي بن هادية، بلحسن البليش، الجيلالي بن الحاج يحي، **القاموس الجديد للطلاب** ، الشركة الوطنية، الشركة التونسية، الجزائر، تونس،ط1، 1979.

21-علي حسن محمد الطوالبة، **التفتيش الجنائي على نظم الحاسوب والإنترنت** ، عالم الكتب الحديثة، الأردن، 2004.

22-عمر محمد أبو بكر بن يونس، **الجرائم الناشئة عن استخدام الإنترنت** ، دار النهضة العربية، القاهرة، مصر، 2004.

23-عمر محمد بن يونس، **الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي** ، الطبعة الأولى، 2005.

24-فتوح الشاذلي ،**جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية** ، منشورات الحلبي الحقوقية، الإسكندرية، مصر ، 2003.

25-فيروز عوض كريم، صالح ميرغني، **إجراءات التحري والضبط في الجريمة الإ لكترونية**، قسم القانون، جامعة الشندي، 2017.

26-محمد حزيط، **قاضي التحقيق في النظام القضائي الجزائري** ، دار هومة، الجزائر، الطبعة الثانية، 2009.

27-محمد حزيط، **مذكرات في قانون الاجراءات الجزائية الجزائري** ، الطبعة الثانية ، دار هومة، الجزائر، 2010.

28-محمد علي السالم آل عياد الحلبي، **اختصاص رجال الضبط القضائي في التحري والاستدلال والتحقيق**، الطبعة الأولى، 1982.

29-محمد منصور الصاوي، **أحكام القانون الدولي في مجال مكافحة الجرائم الدولية للمخدرات** ، دار المطبوعات الجامعية، الإسكندرية، مصر، دون سنة.

30-هلالي عبد الله أحمد، اتفاقية **بوادبست لمكافحة جرائم الإنترنت** ، دار النهضة العربية، القاهرة، مصر، 2007.

31-منتصر سعيد حمودة، **المنظمة الدواية للشرطة الجنائية "الأنتربول"**، الطبعة الأولى ، دار الفكر الجامعي، الإسكندرية، مصر، 2008.

32-نبيلة هبة هروال، **الجوانب الإجرائية لجرائم الانترنت**، دار الفكر الجامعي، مصر،2007.

33-مصطفى محمد موسى، **المراقبة الالكترونية عبر شبكة الإنترنت**، دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية، الكتاب الخامس، الطبعة الأولى، دار الكتب والوثائق القومية المصرية، 2003.

ثالثا: الأطروحات والرسائل الجامعية.

34-أيمن عبد الحفيظ عبد الحميد سليمان، **إستراتيجية مكافحة الجرائم الحاسب الآلي** ، دراسة مقارنة، رسالة دكتوراه، أكاديمية الشرطة.

35-عمر بن محمد العتبي ، **الأمن المعلوماتي ومدى توافقه مع المعايير المحلية والدولية** ، رسالة مقدمة من أجل نيل شهادة الدكتوراه، جامعة نايف للعلوم الأنفية، السعودية ،2010.

36-أمل خلف سفهان الحباشنة، **التبليغ عن الجرائم في التشريع الأردني** ، رسالة مقدمة إلى عمادة الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في قسم القانون العام، جامعة مؤتة، 2008.

37-سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، رسالة ماجستير، كلية الحقوق، جامعة الحاج لخضر، الجزائر، 2013/2012.

رابعا: المقالات والمجلات العلمية.

38-الطيب نوار، **أنتربول منظمة الدولية للشرطة الجنائية** ، مجلة بونة، مدرسة الشرطة، العدد 3، عنابة، الجزائر، 2001.

لحاق عيسى، الأدلة الجنائية الالكترونية، مجلة البحوث بالحقوق والعلوم السياسية، العدد 1،المجلد4، تيارت 2018.

39-محمد الأمين البشرى، **التحقيق في جرائم الحاسب الآلي والإنترنت** ، المجلة العربية للدراسات الأمنية والتدريب، العدد الثلاثون، أكاديمية نايف للعلوم الأمنية، 2000.

40-هشام محمد فريد رستم، **الجرائم المعلوماتية أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين** ، مجلة الأمن والقانون، كلية شرطة دبي، العدد الثاني السنة 7 وما بعدها، 1999.

41-ناجي الجرجاوي، **الجريمة المعلوماتية تتصاعد....وتحتاج تعاونا دوليا ومعايير قانونية جديدة** ، لغة المصدر، مجلة الأهرام للكمبيوتر والإنترنت والاتصالات، العدد الثالث والخمسون، السنة الخامسة، 2005.

خامسا: المؤتمرات والملتقيات العلمية.

42-حابت أمال، **ورقة مقدمة في محاضرة حول الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في قانون الجزائري**، جامعة مولود معمري، تيزي وزو.

43-حملاوي عبد الرحمن، **المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية** ، ورقة مقدمة في الملتقى الوطني للمديرية العامة للأمن، بسكرة، 16-2015/11/17.

44-عز الدين عز الدين، **الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها** ، ورقة مقدمة في ملتقى الوطني لمديرية العامة للأمن الوطني لمكافحة الجرائم، بسكرة في 2015/11/16.

45-علاء الدين محمد شحاتة، **رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي** ، المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في الفترة ما بين 25-1993/10/28، **مشكلات المسؤولية الجنائية في مجال الجرائم الواقعة على البيئة، الجرائم الواقعة في مجال التكنولوجيا المعلومات**، دار النهضة العربية، القاهرة، مصر، 1993.

سابعا: المراجع باللغة الأجنبية.

46-Conférence police et internet, 19 janvier2005, sorbonne, paris, disponible en ligne a l'adresse suivante http://www.isos.fr

47-Cyber police contre cyber crimes mcybercriminalité, le fbi se structure, le canada se prépare, le 15/01/2000, disponible en ligne à l'adresse suivante http://stratégique.free.fr.

48-L'harmonisation des moyens de lutte contre la cybercriminalit é, disponible à l'adresse précédente.

49-Le ministre de l'intérieure français a déclaré : « j'entends créer des cyber-patrouilles de la toile en donnant aux services de police et de gendarmerie les moyens de détecter et d'infiltrer les sites qui diffusent des contenus inacceptables, qu'il s'agisse de pédopornographie ou d'appels à la haine raciale » Jed All : une cyber-patrouille de police sur internet, publié le 25 mars 2005, disponible en ligne à l'adresse suivante : http://aliquid.free.fr .

50-Le portail des sciences sciences : le nombre d'enquêteurs spécialisés en cybercriminalit é va doubler en France, disponible en ligne à l'adresse précédente.

51-Myriam Berbera : le gouvernement français passe à la vitesse supérieure, article publié le 08/09/200 disponible en ligne l'adresse précédente http://www.rfi.fr .

52-Recommandation du forum des droits sur l'internet : les enfants du net ii, 25/01/2005, disponible en ligne à l'adresse http://www.fouruminternet.org .

53-Web Algérie : le premier portail algérien depeuis 1996, des cadres de la gendarmerie algérienne en formation en France, disponible en ligne à l'adresse suivante : http://www.webalgérie.com.

فهرس الموضوعات

فهرس الموضوعات

كلمة شكر .....

الإهداء.....

قائمة المختصرات .....

تمهيد 01

الفصل الأول: الأجهزة المختصة في البحث والتحري عن جريمة الإنترنت

تمهيد وتقسيم 10

المبحث الأول: شرطة الإنترنت كضبطية مختصة في البحث والتحري عن جريمة الإنترنت 11

المطلب الأول:الدوافع التي أدت إلى إنشائها والمبادئ التي تحكمها..... 11

الفرع الأول: إنشاء شرطة الأنترنت..... 12

الفرع الثاني: المبادئ التي تحكم شرطة الإنترنت والصعوبات التي تواجهها..... 15

المطلب الثاني: دور شرطة الإنترنت كضبطية مختصة في البحث والتحري عن جريمة الإنترنت

..... 21

الفرع الأول :دور شرطة الإنترنت كضبطية إدارية وقائية..... 22

الفرع الثاني: دور شرطة الإنترنت كضبطية قضائية..... 24

المبحث الثاني: شرطة الإنترنت على المستوى الوطني والدولي 31

المطلب الأول: على المستوى الوطني 31

الفرع الأول: الدول الأجنبية..... 32

الفرع الثاني: الدول العربية 38

المطلب الثاني: على المستوى الدولي..... 46

الفرع الأول: على المستوى الدولي (المنظمة الدولية للشرطة الجنائية)..... 46

الفرع الثاني: على المستوى الأوروبي..... 48

الفصل الثاني: اختصاصات شرطة الأنترنت

تمهيد وتقسيم 52

المبحث الأول: سلطات شرطة الانترنت في الظروف العادية..... 53

المطلب الأول: تلقي البلاغات والشكاوى 53

الفرع الأول: البلاغات في جرائم الانترنت..... 53

الفرع الثاني: الشكوى في جرائم الإنترنت..... 58

المطلب الثاني: البحث والتحري عن الجرائم والجناة 60

الفرع الأول: الإرشاد الجنائي عبر الإنترنت..... 61

الفرع الثاني: المراقبة الالكترونية للاتصالات عبر الإنترنت 63

المبحث الثاني: سلطات شرطة الإنترنت في الظروف الاستثنائية 71

المطلب الأول: المعاينة والتفتيش في جريمة الإنترنت..... 72

الفرع الأول: المعاينة..... 72

الفرع الثاني: التفتيش وضبط الأدلة في جريمة الإنترنت 76

المطلب الثاني: إجراءات البحث والتحري الخاصة 92

الفرع الأول: التسرب 92

الفرع الثاني: اعتراض المرسلات وحفظ المعطيات المتعلقة بحركة السير..... 95

خاتمة..... 100

الملاحق..... 105

قائمة المصادر والمراجع 113

فهرس الموضوعات..... 120