جامعة أبو بكر بلقايد – تلمسان

كلية الحقوق و العلوم السياسية

قسم القانون الخاص

إشكالية الإثبات في جـــرائم الإنـــترنت في التشريع الجزائري

أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص

من إعداد الطالبة :

مولاي ملياني دلال

تحت إشراف :

أ. د كحلولة محمد

أعضاء اللجنة المناقشة :

أ. بن عمار محمد	**أستـــاذ التعليم العالي**	**جامعة تلمسان**	**رئيسا**
أ. كحلولة محـــمد	**أستـــاذ التعليم العالي**	**جامعة تلمسان**	**مشرفا و مقررا**
أ. هامل هـــــواري	**أستاذ محاضر "أ"**	**جامعة سعـــيدة**	**مناقشا**
أ. بن أحمد حـــاج	**أستاذ محاضر "أ"**	**جامعة سعـــيدة**	**مناقشا**

السنة الجامعية 2017-2018

جامعة أبو بكر بلقايد – تلمسان

كلية الحقوق و العلوم السياسية

قسم القانون الخاص

إشكالية الإثبات في جـــرائم الإنـــترنت في التشريع الجزائري

أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص

من إعداد الطالبة :

مولاي ملياني دلال

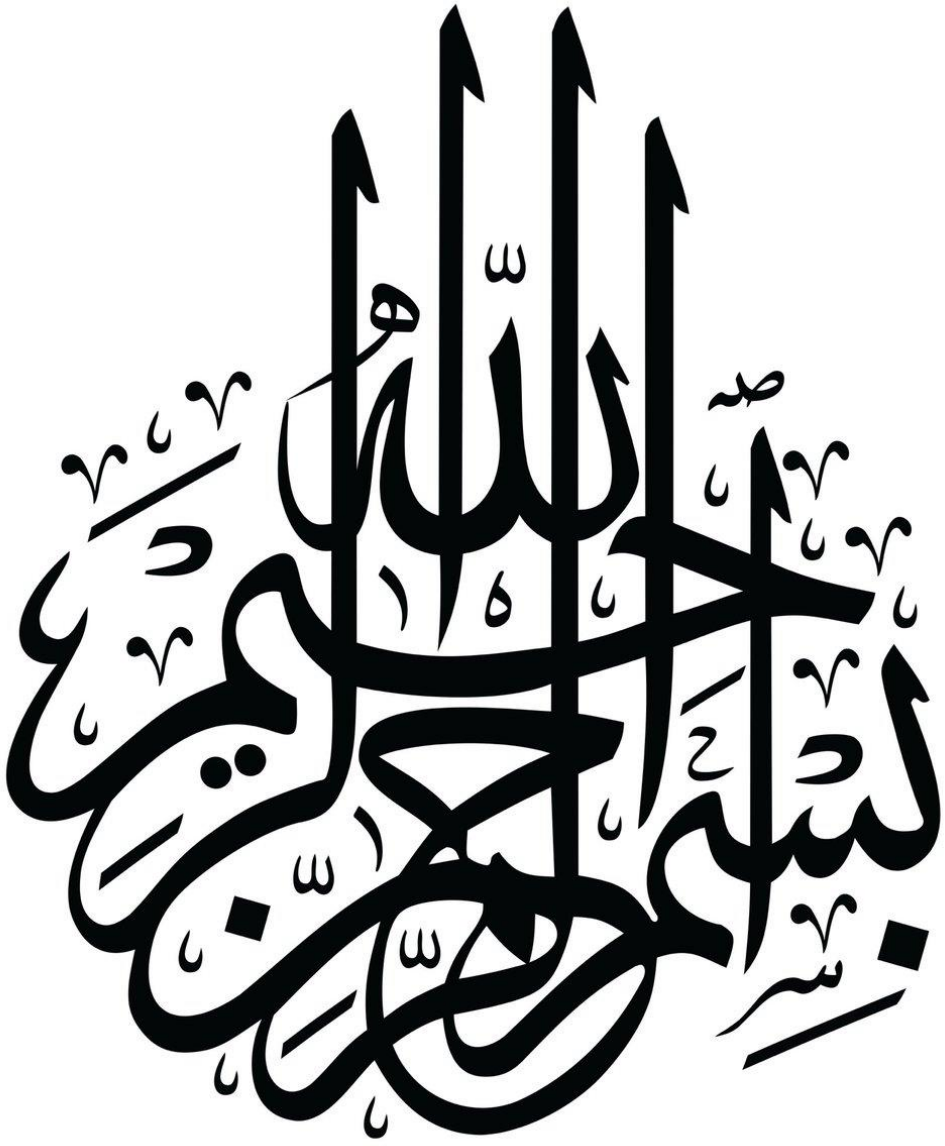
تحت إشراف :

أ. د كحلولة محمد

أعضاء اللجنة المناقشة :

أ. بن عمار محمد	**أستـــــاذ التعليم العالي**	**جامعة تلمسان**	**رئيسا**
أ. كحلولة محـــمد	**أستـــــاذ التعليم العالي**	**جامعة تلمسان**	**مشرفا و مقررا**
أ. هامل هـــــواري	**أستاذ محاضر "أ"**	**جامعة سعـــيدة**	**مناقشا**
أ. بن أحمد حـــاج	**أستاذ محاضر "أ"**	**جامعة سعـــيدة**	**مناقشا**

السنة الجامعية 2017–2018


بسم الله الرحمن الرحيم

شكر وتقدير

الحمد لله والشكر لله أن وفقني بقدرته إلى سبيل العلم ويسر لي إنجاز هذا البحث كما أتقدم بالشكر الجزيل وتقديري الكبير إلى الأستاذ المحترم الدكتور كحلولة محمد على حرصه وسعة صبره في المتابعة والإشراف وتصويب هذه الرسالة،فجزاه الله كل الخير

كما أتقدم بالشكر الجزيل إلى أعضاء لجنة المناقشة الأفاضل على قبولهم مناقشة هذه الرسالة وإبداء ملاحظاتهم عليها.

والشكر موصول لكل من قدم يد العون والمساعدة من أجل إتمام هذه الرسالة

دلال مولاي ملياني

إهداء

أهدي هذا العمل المتواضع إلى:

أمـــي وأبـــي

و إلى زوجـــي

و إلى ابنتي أية فاطمة الزهراء و إلهام بشرى

و إلى إخوتي وأخواتي وأبنائهم

و إلى كل من ساندني وساعدي، وشد من همتي ولو بكلمة طيبة

و إلى المرحوم الدكتور مأمون عبد الكريم

دلال مولاي ملياني

قائمة أهم المختصرات

1-قائمة المختصرات باللغة العربية:

ج. ر..... الجريدة الرسمية

ج..... جزء

دج..... دينار جزائري

ص..... صفحة

ط..... الطبعة

ع..... عدد

ف.....فقرة

ق. ا . ج .ج..... .قانون الإجراءات الجزائية الجزائري

ق. ع .ج..... قانون العقوبات الجزائري

قانون 09-04..... قانون 09-04المتعلق بمكافحة تكنولوجيات الحديثة للإعلام والاتصال

مج..... مجلد

الهيئة الوطنية..... الهيئة الوطنية لمكافحة جرائم تكنولوجيات الإعلام والاتصال

2-Liste des abréviations en langue française

éd……édition

JORA …….. Journal Officiel République Algérienne

n……numéro

Op.cit……option citée

P…….Page

مـــــقدمة

اجتاحت العالم في أواخر القرن العشرين، ثورة معلومات انبثقت عنها ثورة للاتصالات واللتان لم تبرحا مكانهما وظلتا في تطور مستمر و أحدثتا طفرة تقنية يصعب التحكم فيها، حتى أنّه أصبح لا يمكن الاستغناء عن نظم المعلوماتية لعمل شبكات الاتصال و الإعلام[1]، ففي عصر التكنولوجيات الحديثة للإعلام والاتصال، صارت كل مجالات الحياة مرتبطة بلمسة بسيطة، لتحصل على ما تريد من معلومات وخدمات، فأصبحت تكنولوجيات الإعلام والاتصال سمة الحياة المعاصرة بعد أن كانت من الكماليات، والإنترنت هي من تمثل حاليا هذا التطور دون منازع كوسيلة الاتصال المعلوماتية المثلى، ذلك أنّه من خلال شبكة الاتصالات يتم الدخول إلى المنظومة المعلوماتية[2]، ومنها إلى ما كان عالماً واسعًا وقارات شاسعة وأصبح قرية صغيرة ولكن غير مرسومة الحدود، فبعد أنْ دخلت الإنترنت حياتنا، بعالمها الافتراضي غيّرت كثيرًا من المفاهيم.

فما كان بعيداً صعب المنال، أصبح قريباً في متناول اليد، فشأنها شأن كُلَّ تطور تكنولوجي تحمل الإنترنت في طياتها إيجابيات كثيرة تتمثل في الخدمات التي تقدمها، والتي لا يمكن تجاهلها خصوصا في مواجهة من يحاولون إظهار الجانب المظلم منها فقط، على أنّ الطابع العالمي للإنترنت لا يجب أنْ يكون ذريعة لاستبعاد إنفاذ القانون، أو البيانات المعالجة أليا بجميع أشكالها عبر شبكة الإنترنت بمنائ عن الرقابة أياً كانت.

الملاحظ أنّ شبكة الإنترنت في تطور مستمر، وكذا خدماتها باعتبار أنّها قد تم استغلالها في جميع مجالات الحياة الاقتصادية والسياسية والاجتماعية والدبلوماسية، وذلك من خلال الاعتماد عليها للتحكم في تسيير المرافق الحيوية للدول و الحكومات، من بنوك المعلومات المزودة ببيانات مالية وشخصية للأفراد كالإدارة الإالكترونية ومجالات الدفاع والأمن ، وأصبح الأفراد يُسيَّرون يومياتهم من خلال مجموعة من التطبيقات والبرمجيات، حيث تشمل تكنولوجيا الإعلام و الاتصال المعالجة الآلية

[1] أحمد حسام طه تمام، الحماية الجنائية لتكنولوجيا الاتصال، دراسة مقارنة، دار النهضة العربية،القاهرة ،مصر،2002،ص1.

[2] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، دراسة معمقة ومقارنة في الجرائم، المركز القومي للإصدارات القانونية، القاهرة، مصر،2011، ص9.

للمعطيات والتكنولوجيات الحديثة للإتصالات، أمّا المعالجة فتقوم على استخدام وسائل تقنية لتسيير وتنظيم ومعالجة المعطيات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق، أمّا التكنولوجيات الحديثة للإتصالات فهي قائمة على تطور الوسائل التقنية بدلالتها المختلفة كالوثائق والأخبار [1]، لكن وبالمقابل ووفق المعطيات السابقة فالإنترنت قد أوجدت فضاءً لا يستهان به من الحرية، والتي أعطت أعصاب النفوس الضعيفة فرصة لارتكاب أعمال إجرامية، ضد الأموال الأشخاص و المؤسسات وحتى الدول، من دون أن يكون هناك تواجد فعلي للمجرم في مسرح الجريمة، والذي، أدى إلى ظهور أو بروز فئة من الأشخاص لم يعرفهم المجتمع من قبل يتمتعون بالخبرة التي تمكنهم من تسخير التقنية لحسابهم وإشباعا لرغباتهم بمقابل أو بدونه، يُعد خطرا يهدد أمن المجتمع ككل[2].

إنّ عدم امتلاك الانترنت من طرف جهة محددة بذاتها، تسيطر عليها مثّل خطرا حقيقيا افرز سلوكيات إجرامية ، على أنّ خطر هذه الجرائم يكمن في أنّها في طبيعتها تجمع بين الذكاء الاصطناعي والذكاء البشرى، أي أن جرائم الانترنت تجمع بين ما هو إنساني وماهر ألـي تقني، فجمعت بين ذكاء المجرم وذكاء الأجهزة الرقمية [3].

ورغم كل ما تمتلكه الإنترنت من إيجابيات، إلا أنّ الأمر لا يخلو من السلبيات التي تتجسد في ظواهر سلبية مستحدثة تمس بالنظام العام والأمن العام، كجرائم الإرهاب الإلكتروني وتخريب المنظومة المعلوماتية، وعلى إثر السلبيات التي برزت للوجود، نجمت مشاكل قانونية عديدة تفاقمت حتى أصبح يطلق على الإنترنت فضاء خارج القانون، حيث أن الشبكة أضافت بيانات جديدة، لم تكن معروفة من قبل، مما أعجز الدول المتصلة بشبكة الإنترنت من إقامة التوازن المفترض بين العديد من الحريات

[1] فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية ،دكتوراه في الحقوق،كلية الحقوق ،جامعة عين شمس،القاهرة،مصر،2012،ص 35.

[2] عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، دار المستقبل ،الطبعة الأولى، عمان الأردن ،2008، ص74.

[3] عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، دراسة قانونية مقارنة، دار الثقافة، عمان، الأردن، 2015،ص 225.

وفي مقدمتها حرية الحياة الخاصة وبين القيود الموضوعة عليه باسم النظام العام وباسم حماية الفرد والمجتمع والتي تختلف من دولة لأخرى[1].

وقد صاحب تطور التقنيات المعلوماتية في استخدامات، حدوث تغييرين هامين نتج عنهما صعوبة عملية الإثبات، بداية من جمع الأدلة وانتهاءً بتقديرها، وهما تغيير الحامل أو الدعامة التي تحوي المعطيات المعالجة أليا من الدعامة الورقية إلى الإلكترونية أو الرقمية مما ابرز أهمية المعلومات مستقلة عن دعامتها المادية[2]، أمّا الثاني فهو تغّير في حجم وكم البيانات والمعطيات المطلوب فحصها وتمحيصها وفرزها وتصنيفها[3].

إنّ ظهور مفاهيم إجرامية جديدة، مختلفة عن مفاهيم الجرائم السائدة، والتي مست خصوصا الجانب المادي أو الركن المادي الذي حلّ محله النشاط التقني بأقل جهد و أسرع وقت، ودون أدنى عنف مادي ملموس، جعل الفقهاء ورجال القانون بما فيهم سلطات الضبط والتحقيق القضائي، يتفطنون إلى وجود جرائم جديدة مستحدثة كاختـلاف أدلة الإثبات الجنائي عن الأدلـة العادية لباقي الجرائم، مع عجز الطرق العادية أي إجراءات البحث والتحري في مجملها عن فك غموض وأسرار الجريمة لجمع الدليل ومتابعة المتهم، من حيث محل الدليل وشكل الدليل نفسه، وكذا تعاظم حجمه، فوجود دليل لا مادي مختلف عن الأدلة الموجودة، أدى إلى اختلاف نوع الجرائم واختلاف دليلها.

ممـا يجعل إثباتها جنائياً فيه مشقة وصعوبة، فعملية الإثبات تتطلب تقديم الدليل، وبالتالي إثبات الواقعة الإجرامية، مما انعكس أثره على قانون العقوبات، و قانون الإجراءات الجنائية، لذلك فإن لذاتية جرائم الإنترنت أثر علىإثباتها.

[1] حسين بن سعيد ألغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، 2009 ، ص44.

[2] ايمن عبد الله فكري، جرائم نظم المعلومات ،دراسة مقارنة، دار الجامعة الجديدة ،الإسكندرية ،مصر، 2007.ص12.

[3] فهد عبد الله العبيد العازمي، المرجع السابق.ص372.

فالإثبات بمعناه الضيق هو البرهان المبين للحقيقة، أمَّا مفهومه الواسع فهو مجموعة الوسائل المستعملة للوصول إلى إظهـــار الحقيقة[1]، وتوجد قواعد الإثبات مكانة أهمية بالغة في فـــروع القانــون، فالحق دون دليل يسنده هو والعدم سواء، فالدليل هو الذي يدعم الحق ويجعل وجوده قائما، وتزداد أهمية الإثبات في المجال الجنائي لأن حق الدولة في العقاب يتجرد من قيمته ما لم يقم الدليل أمام القضاء على وقوع الجريمة ونسبتها إلى المتهم[2]، ومن المجالات التي تأثرت مباشرة بالتطور التكنولوجي، المجال الأمني الذي كانت السلطات المتخصصة السبّاقة نسبيًا في استعمال الوسائل الحديثة لمكافحة الجريمة أي أنها استعملت التكنولوجيات الحديثة لأغراض وقائية قبل القضائية، ومن بين الميادين التي تأثرت بالتطور التكنولوجي الإثبات الجنائي، وقد تأثر كثيرا بثورة المعلومات والتطور التكنولوجي لوسائل الاتصال والإعلام خاصة الظواهر والسلوكيات التي أفرزتها التكنولوجيات الحديثة، وبالتالي طبيعة الأدلة الناتجة عنه وطرق وأليات اكتشافها والحصول عليها وتحصيلها.

و لما أصبحت الأدلة العادية قاصرة لوحدها في إثبات جرائم الانترنت، ولكن هذا لا يعد سببا لفقدانها قيمتها الثبوتية، في مثل هذه الجرائم، كونها تعد من دعائم الإثبات في جرائم الإنترنت، والتي لا يمكن الاستغناء عنها بأي طريقة، وهذا ما حاولنا تبيانه من خلال هذه الدراسة أي تكاملية الأدلة العادية أو دعائم الإثبات والدليل الجنائي الالكتروني لإثبات جرائم الانترنت، ولمواجهة قصور الأدلة العادية عمد المشرع إلى تعديل وسن قوانين خاصة.

وكما هو معلوم تهدف قواعد الإثبات الجنائي الوصول إلى الحقيقة، سواء تعلق الأمر بالسلوك المرتكب أو الشخص المشتبه فيه، والذي لا يتأتّي إلّا من خلال إجراءات الإثبات المتمثلة في البحث و التحري عن الدليل الجنائي وتقديمه للقضاء ليقول كلمته على أساسه إما بالإدانة أو البراءة[3].

[1] محمد مروان،نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري،الجزء الأول،ديوان المطبوعات الجامعية بن عكنون الجزائر،1999،ص105

[2] سامح احمد البلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الانترنت،رسالة دكتوراه، جامعة الإسكندرية، مصر 2010.،ص317.

[3] موسى مسعود ارحومة، قبول الدليل العلمي أمام القضاء الجنائي، دراسة مقارنة، منشورات جامعة قاريونس، بنغازي، ليبيا، 1999.ص420.

غالباً ما يقع السلوك الإجرامي في جرائم الإنترنت دون علم الضحية، مما يضيف عبئا إضافياً على السلطات المختصة في التحري والتحقيق، ويمكن استشعار واقع الحال الصراع غير المعلن بين مجرم الانترنت والسلطات المختصة بالتحري والتحقيق ، ذلك أنّ مجرم الانترنت في تطوير مستمر لمهاراته لضمان عدم الكشف أو محو آثار الدليل الجنائي الالكتروني وهو أحد طرفي عملية الإثبات الجنائي في جرائم الانترنت، بحيث لا يترك آثار مادية ملموسة، ويرافق هذا السلوك مشكلة تتعلق بالسبيل الموصل إلى الجاني.

لذلك حاول المشرع الجزائري من خلال تدخلاته التشريعية المتباعدة، التنصيص على إجراءات خاصة، رافقتها إمكانيات لم تحدد مدى فاعليتها على أرض الواقع لحد الآن في ظل غياب إعلام قانوني واضح وإحصائيات دقيقة في مجال جرائم الاستخدام غير المشروع للإنترنت.

بادرت الجزائر في سن تشريعات منذ سنة 2004، ومع التطور الحاصل في تقنية المعلومات، واجه المشرع الجزائري السلوكيات غيرالمشروعة الدائرة في مجالها بالقانون رقم(04-15)[1] ثم قانون للوقاية رقم(09-04)[2]، بإدراج جرائم المعالجة الآلية للمعطيات ضمن جرائم الإنترنت، هي "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية"[3]. فقد جعل المنظومة المعلوماتية وسيلة لارتكاب الجريمة أو محلا يقع عليه السلوك الإجرامي، وبذلك غدا للتطور التكنولوجي والعلمي على القانون الجزائي أثار لا يمكن إنكارها، وعلى وجه الخصوص عندما يتعلق الأمر بنظرية الإثبات الجزائي، يجب التنويه أنّ جرائم الإنترنت يدخل في نطاقها العديد من

[1] القانون(04-15)المؤرخ في 10نوفمبر 2004 ،يعدل ويتمم الأمر رقم(66-156)المؤرخ في 8 جويلية 1966،المتضمن قانون العقوبات،ج ر 71ليوم 10 نوفمبر 2004.

[2] القانون(09-04)يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 14 غشت عام 1430 الموافق 05غشت سنة 2009 ج.ر عدد 47 ل 16غشت 2009 ص 05.

[3] المادة الثانية من القانون القانون (09-04) يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ص05.

السلوكيات الإجرامية، سواء في تلك التي يتم استخدام الإنترنت في القيام بها، وتلك التي يكون الانترنت محلا لها.

الأصل في التحقيق والتحري إخضاع جميع الجرائم إلى إجراءات جزائية متماثلة، دون أي استثناء يرد على نوع خاص بالجرائم، أو حتى دليل خاص للإثبات، ولكن شيئًا فشيئاً ابتعد عن الأصل وورد الاستثناء بنص، بعدما اختلفت طريقة ارتكاب الجريمة ،بعد التطور التكنولوجي الكبير ،كما وأنّ الجزائر صادقت على اتفاقيات دولية، فرض عليها تكييف قوانينها الداخلية مع عدة اتفاقيات[1]، أو استنباط مختلف الأحكام الإجرائية من اتفاقيات إقليمية بصبغة عالمية[2].وكان هذا على حساب الحرية الشخصية للأفراد في مقابل صلاحيات أوسع للسلطات المختصة بالتحري والتحقيق، وهذا نتيجة تفشي الجريمة مما تسبب في الإخلال بالنظام العام، مما أدى إلى استقلال جرائم كجرائم الانترنت بإجراءات استثنائية وبدليل منفرد مهم لا يجوز، ومن غير الممكن أن يكون غائبا كأساس لإثبات جرائم الانترنت. ذلك لأنّ مصلحة المجتمع هي في مكافحة الجرائم الخطيرة و المعقدة تعلو على حرمة المراسلات و ذلك في ظل احترام الضوابط المحددة قانونا، "فالتطور التكنولوجي، ساهم في انتهاك الحريات عن طريق أجهزة التصنت والتسجيل الالكتروني"[3].

وقد أثارت الإجراءات الجزائية الخاصة في مجال إثبات جرائم الإنترنت العديد من الاستفسارات حول مدى مشروعيتها، وإمكانية الاستناد عليها كدليل إثبات في المواد الجزائية الخاصة و بجرائم تكنولوجيات الإعلام والاتصال هل هناك ضوابط وضمانات تجعل هذه الإجراءات الخاصة في أضيق الحدود لاستخدامها. وكما يتفق فقهاء القانون الجنائي على أن قانون الإجراءات الجزائية يُعتبر من القوانين المنظمة للحرية الشخصية للمشتبه فيه وللمتهم، و ضمانات المشتبه فيه أثناء إجراءات الحصول على الدليل الجنائي، والحق في الحياة الخاصة كان ومازال يثير جدلا، خصوصا أنّه أول حق

[1] اتفاقية الأمم المتحدة لمكافحة الفساد، المعتمدة من قيل الجمعية العامة للأمم المتحدة بنيويورك يوم 31 أكتوبر سنة2003، والتي صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي(04-128)مؤرخ في 29 صفر 1425 الموافق 19 أبريل2004، ج.ررقم26ليوم 25 ابريل 2004،ص12.

[2] اتفاقية بودابست الاجرام السيبيري متوفرة على الموقع التالي https://rm.coe.int/16802fa3ff تاريخ الاطلاع.26-02-2016.

[3] مبذر الويس، أثر التطور التكنولوجي على الحريات العامة،منشاة المعارف الإسكندرية، مصر،1998،ص1.

يتم انتهاكه، عند تغليب مصلحة الدولة في العقاب، والانتهاكات التي يواجهها في ظل التطور المستمر والسريع لتكنولوجيات الإعلام والاتصال،و قد كفل الدستور الجزائري حمايـة هـذا الحـق[1]، فحماية الحياة الخاصة للأفراد واحتـرام خصوصياتهم، دليل على رقي الأنظمة القانونية لأي دولة ولو نظريا.

ومن مشاكل البحث والتحري في جرائم الإنترنت، شساعة مسرح الجريمة الافتراضي، ليشمل أكثر من إقليم دولة في العالم الافتراضي، مما يعد إنتهاكا للسيادة الوطنية، والتي تصدى لها المشرع الجزائري من خلال القانون(09-04)في ما يخص البحث والتحري الخاص بجرائم الانترنت، ولو من ناحية قانونية نظرية تجعل هذا الحل سليماً، عن طريق التعاون الدولي في مجال هذه الجرائم وجعل أساس المعاملة وجود اتفاقيات ثنائية، والمعاملة بإعمال (قاعدة المعاملة بالمثل)بحيث يسمح بالاتصال المباشر بين أجهزة الأمنية لفعالية التحقيق.

مع تحديد وحصر عناصر الجريمة والمشتبه فيهم، فإنّه يمكن أن يكون بريئاً وإثبات صحة هذه الاحتمالات هو بالإثبات الجنائي لذلك فالهدف من التحقيق هو الإثبات الجنائي.

كما أن تكنولوجيات الإعلام والاتصال قد أثّرت في المفاهيم التقليدية الثابتة لمحل السلوك الإجرامي[2]، وأنّ التغيرات التي أحدثتها تكنولوجيات الإعلام والاتصال قد أثارت العديد من المشاكل القانونية عندما صعب التعامل مع نماذج إجرامية حديثة.

[1] المادة (46) من الدستور المعدل، القانون (16-01)يتضمن التعديل الدستوري المؤرخ في 26 جمادى الأولى عام 1437الموافق6 مارس2016،ج ر رقم 14 المؤرخة في 07 مارس2016.ص11.

التي تنص مايلي" لا يجوز انتهاك حُرمة حياة المواطن الخاصّة، وحرمة شرفه، ويحميهما القانون.سرّية المراسلات والاتّصالات الخاصّة بكلّ أشكالها مضمونة لايجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية.ويعاقب القانون على انتهاك هذا الحكم.حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه "

[2] ايمن عبد الله فكري، المرجع السابق، ص10.

ولعل الدافع والباعث للبحث في هذا الموضوع، الشغف بكل ماهو جديد في عالم التقنية وتكنولوجيات الإعلام والاتصال، وخصوصا ما تعلق بذلك الدمج أو التزاوج بين الإعلام والاتصال والقانون.

فمحاولة دراسة موضوع مستحدث، يثير العديد من التساؤلات القانونية والتي حاولنا مناقشتها، وتجلت صعوبات هذه الدراسة في المتابعة في موضوع الإثبات الذي سبق لنا التطرق إليه في دراسة سابقة، وذلك قبل صدور النصوص التشريعية في القانون الجزائري، وأن مسألة التطرق لجرائم الإنترنت يقودنا مباشرة إلى ضرورة الإلمام بالنواحي التقنية التي حاولنا حصرها في حدود ضيقة.

ويعد موضوع البحث من الموضوعات الجديدة التي أصبحت تأخذ شيئا فشيئا حيزا كبيراً من البحث العلمي، وقد تم التركيز على الجوانب الموضوعية والإجرائية للإثبات، ومحاولة الخوض في مسألة الإثبات توضيح أثر التطور الحديث لتكنولوجيات الإعلام والاتصال نظرية للإثبات حديثة، ومدى تأثير خصائصها على الإجراءات وتلك الإجراءات على الحقوق والحريات.

ويأتي العمل الحالي، كمحاولة متواضعة لتسليط الضوء على الاشكالات الموضوعية والإجرائية لجرائم الإنترنت في التشريع الجزائري، وخصوصا الجانب الإجرائي وبالضبط الإثبات الجنائي حيث تهدف الدراسةإلى البحث عن النقائص ومحاولة إيجاد حلول مناسبة.

للموضوع أهمية بالغة من خلال ارتباطه الوثيق بالانترنت، وتعدد المتدخلين في هذه الخدمة وبالتالي قيام المسؤولية، التي لابد من إثباتها، وفي اعتقادنا أنَّ الحجم الحقيقي للإعتداءات عبر الانترنت كهدف ووسيلة هي أكبر بكثير مما هو معلن عنه، فهي في تزايد مستمر، لا لشيء إلا للكم الهائل للبيانات والإحجام عن الإبلاغ من طرف الضحية وعدم القدرة على اكتشاف وإثبات السلوك الإجرامي.

إنّ التهديدات الأمنية للحاسبات الآلية، ذات طابع دولي ممّا يجعل الدول بمفردها عاجزة عن مكـافحتها، والــتي لا يمكن أن تحصل إلا بوجـود تعـاون دولي وهذا مانص عليه المشرع الجــزائــري ، باعتماد مزودي الخدمات، ويكمن خطر جرائم الإنترنت- وخصوصا جرائم التقنية منها- في اجتماع الذكاء الصناعي والبشري في نفس الوقت[1].

وبالتالي لإثبات هذه الجرائم نكون أمام نوعين من الأدلة، دليل غير مرئي لا محسوس قوامه كم هائل من البيانات وطرق تقليدية أو دعائم إثبات تحاول أن تنسب الفعل إلى المشتبه فيه الحقيقي، ولما كانت الدراسة خاصة بالتشريع الجزائري و في ظلّ وجود العديد من الثغرات القانونية، حاولنا أن نبحث عن حل ضمن القوانين الوطنية الأخرى والتي لها نفس الطابع الجزائي. لذلك اعتمدنا على المنهج المقارن، التحليلي، الوصفي والذي تتوافر فيه مجموعة من الإجراءات البحثية، التي تتكامل لعرض الموضوع من خلال معرفة مواصفات الموضوع التقنية التي جعلته يتميز عن الإثبات في جرائم مغايرة من الناحية القانونية الإجرائية وتحليل الحقائق بغرض استخلاص النتائج بغية للوصول إلى تقرير مدى حجية الأدلة لإثبات جرائم الإنترنت.

كما أنّ استخدام التكنولوجيات الحديثة اثّر على حقٍّ مهمٍّ جدّا وهو الحق في الحياة الخاصة في مجالات الحياة العادية والتي يمكن متابعة المعتدي فيها جزائيا، وكذا استعمالها كوسائل مساعدة للإثبات وبالضبط في الإجراءات الخاصة التي تعد أي الإجراءات الخاصة استثناء من الحياة الخاصة.

ولما كان القانون الجزائي محكوم بقاعدة الشرعية وعدم القياس، فكان الهدف تسليط الضوء على مشاكــل الإثبات الجنائي وأهم النقــائص الــتي تخللت النصوص القــانونية فــي التشريــع الجزائري وبالمقابــــل معرفة نوع الأدلة التي يمكن اعتمادها في الإثبات الجنـائي، بما فيهـــــا الأدلـة العـاديـــة

[1] فهد عبد الله العبيد العازمي ، المرجع السابق، ص07.

أو دعائم الإثبات الجنائي في جرائم الإنترنت، وكيف للقانون أن يواكب التطور التقني من خلال تطور نظرية الإثبات الجنائي، هذا التطور الذي يسير بوتيرة متسارعة، قد يفقد الحكومات والأفراد على حد سواء السيطرة والتحكم في تكنولوجيات الإعلام والاتصال.

على ضوء كل ما ذكر سابقا يمكن طرح الإشكالية التالية: هل تختلف إجراءات الاثبات الجنائي في جرائم الانترنت عن باقي الجرائم في التشريع الجزائري؟

لمناقشة هذه الإشكالية تّم اعتماد خطة ثنائية من بابين ، الباب الأول عن ذاتية جرائم الإنترنت في التشريع الجزائري، الخصوصية التي تكتسيها مع العلم أنّ مصطلح جرائم الانترنت هو مرادف "لجرائم تكنولوجيات الإعلام والاتصال" وهو نفسه "الجرائم المعلوماتية" و"الجرائم الالكترونية"، التي لم يستطع الفقهاء مع اجتهاداتهم من التفريق بينها، لأن ذاتية جرائم الانترنت أدى إلى وجود خصوصية في الدليل الناتج عنها.

أمّا الباب الثاني عن إجراءات الإثبات الجنائي في جرائم الانترنت في التشريع الجزائري ،محاولين أن يقدم هذا الموضوع اسهاماً بسيطاً لقواعد جديدة في نظرية الإثبات الجنائي في جرائم الانترنت، قد تكون بدايتها التعرف على أهم الصعوبات والعقبات التي تقف في الواجهة لإثبات هذه الجرائم، ولكن الأهم نسبة هذا السلوك الإجرامي لشخص بذاته أو عدة أشخاص، لأن الدليل الجنائي في هذه الجرائم من نوع خاص يتميز بخصوصية محله ومسرحه الافتراضي .

البـــــــاب الأول

ذاتية جرائم الإنترنت في التشريع الجزائري

مما لاشك فيه انّ التطور التقني في مجال التكنولوجيات الحديثة للإعلام و الاتصال ،لم يؤثر فقط في أصناف المجرمين بل اثر في الإثبات الجنائي نفسه للجريمة، وبالتحديد سبل إثباتها.

فكل تقنية مستحدثة ينشأ عنها في كل لحظة، وفي كل مرحلة من مراحل تطورها ظاهرة تشكل سلوكًا إجراميًا؛ خاصة بها يهدد المجتمع بخطر حقيقي[1]، حيث يعمل الانترنت على نشر أو إذاعة طرق تحقيق السلوك الإجرامي[2]، فرافق تطور تكنولوجيات الإعلام والاتصال، تغير واضح في طبيعة المعلومات، فتغيرت الدعامة التي تحتوي المعلومات من الشكل الورقي إلى الشكل الالكتروني أي على أقراص الليزر وحتى الشبكات الافتراضية، وهو ما يعرف باستقلالية المعلومة عن دعامتها المادية أعطى لها خصائص جديدة[3]، وبتغير الدعامة الخاصة بحفظ البيانات التي أصبحت أسهل وأكثر سعة، ازدادت كمية المعلومات لحد يصعب التحكم في تدفقه.

وبعد أن أقــرّت الجزائر رقمنة كل شيء، ونقصد بذلك الإدارة الالكترونية، حينها قام المشرع الجزائري بخطوات ملفتة للانتباه، باتّجاه مكافحة الجرائم ومن بينها جرائم الانترنت، وهي جرائم مرتبطة بتكنولوجية الإعلام والاتصال، والتّي نلاحظ أنّ كل التطور الحــالي في تكنولوجية الإعلام والاتصال من ألياف بصرية وأقمار صناعية وأجيال متعاقبة للهواتف النقالة والأرضية ما هي إلا دعائم للتدفق السريع للانترنت في كل مكان وزمان. من هنا كان علينا التطرق إلى ما تتميز به جرائم الانترنت (الفصل الأول) من خصائص تجعلها جرائم ذات طابع خاص، والدليل الخاص بإثباتها (الفصل الثاني) من دليل جنائي الكتروني ودعائم إثبات و ما يميزه من خصائص ومصادر.

[1] محمد سامي الشوا، ثورة المعلومات وانعكاسها على قانون العقوبات، دار النهضة العربية، القاهرة،مصر، 2003.ص51.

[2] *Solange Ghernaouti-Hélie, Internet et Sécurité,* Paris, *PUF*, « Que sais-je ? »,2002.p14.

[3] ايمن عبد الله فكري ، المرجع السابق، ص34.

الفصل الأول:الإطار القانوني لجرائم الانترنت في التشريع الجزائري.

تعد جرائم الإنترنت من الجرائم المستحدثة، التي ظهرت حديثا بظهور الانترنت، والتي تتمتع بخصائص متميزة عن الجرائم الباقية، كونها جرائم ذات سلوك تقني، فقد اختلف في تسميتها مند ظهورها وكل مرة تظهر مصطلحات تواكب التطور التقني لتكنولوجيات الإعلام والاتصال، جرائم معلوماتية، جرائم الكترونية، ولكن شيئا فشيئًا أصبح مصطلح جرائم الانترنت الأكثر شيوعا واستعمالا وهو ما تبنيناه في هذه الرسالة .

قد حاول المشرع الجزائري وضع كل أنواع الجرائم المستحدثة المتعلقة بالتكنولوجيات الحديثة و الجرائم العادية المرتكبة بمناسبتها في خانة واحدة و هي الجرائم المتعلقة بتكنولوجيات الحديثة للإعلام و الاتصال،فبعد أن تم إدراج سنة (2004) في تعديل قانون العقوبات أول نص يجرم المساس بالمعالجة الآلية للمعطيات قام المشرع بإضافة نص قانوني خاص مستقل عن قانون العقوبات، دمج الجرائم سالفة الذكر في إطار تكنولوجيات الإعلام والاتصال سنة (2009)ثم سنة (2016) قام بإدراج تكنولوجيات الإعلام والاتصال ضمن الوسائل التي يعتد بها في الجرائم الإرهابية.

ومن ثَمَّ فانّه من المفيد لدراسة هذا النوع من الجرائم بيان مفهوم جرائم الانترنت في حد ذاتها(المبحث الأول) ثم الاطلاع على صورها في التشريع الجزائري(المبحث الثاني)

المبحث الأول:مفهوم جرائم الانترنت في التشريع الجزائري.

إنّ جرائم الانترنت أو جرائم الاستخدام غير المشروع للانترنت، هي الجرائم المتصلة بالإعلام[1]والاتّصال[2]، أو الجرائم المعلوماتية، أو جرائم تكنولوجيات الإعلام والاتصال التي يطلق عليها جرائم المعالجة الآلية للمعطيات، كذلك تعرف جرائم الانترنت على انّها كل فعل غير مشروع اقترن بالتواصل مع المنظومة المعلوماتية وشبكات الاتصال،و حين غياب هذا الرابط- الاتصال و الإعلام- لا يمكن الحديث عن الفعل غير المشروع [3]، وما يلحقها من جرائم ، وقد نصّ المشرع الجزائري في المادة الأولى من القانون (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على مايلي:"يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها" أما المادة الثانية فقد أعطت تقسيما لهابقولها"...أ- الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية..."[4] ،إذا ما هو تعريف جرائم الانترنت؟(المطلب الأول) وما هي سمات أو خصائص جرائم الانترنت؟(المطلب الثاني).

---

[1] **الإعلام**:تلك العملية التي ترتب عنها نشر الأخبار والمعلومات الدقيقة التي ترتكز على الصدق والصراحة ومخاطبة عقول الجماهير وعواطفهم السامية، والارتقاء بمستوى الرأي ، ويقوم الإعلام على التنوير والتثقيف،مستخدما أسلوب الشرح والجدل المنطقي والتفسير. محمد جمال الفار ، المعجم الإعلامي ، دار أسامة والمشرق الثقافي، عمان الأردن، 2010،ص27.كما عرف القانون العضوي رقم(12-05) في المادة (3) منه أنشطة الإعلام بقولها:"يقصد بأنشطة الإعلام، في مفهوم هذا القانون العضوي، كل نشر أو بث لوقائع أحداث أو رسائل أو أراء أو أفكار أو معارف،عبر أية وسيلة مكتوبة أو مسموعة أو متلفزة أو الكترونية،و تكون موجهة للجمهور او لفئة منه."المادة الثالثة من القانون العضوي رقم (12-05) المؤرخ في 18صفر عام 1433 الموافق12يناير سنة2012 يتعلق بالإعلام ،ج.ر رقم 02 المؤرخة في 15 يناير2012،ص21.

[2] **الاتصال**: هو العملية التي يتم عن طريقها انتقال المعرفة من شخص إلى اخر حتى تصبح مشاعا بينهما وتؤدي الى التفاهم بين هذين الشخصين ، وبذلك يصبح لهذه العملية عناصر ومكونات واتجاه تسير فيه واتجاه تسعى الى تحقيقه و مجال تعمل فيه ويؤثر فيها. محمد جمال الفار، المرجع السابق،ص87.

[3] Mohamed Chawki, Combattre la cybercriminalité, Edition de Saint Amans France, 2008, p 41.

[4] Art. 2. « - Au sens de la présente loi, on entend par :

المطلب الأول:تعريف جرائم الانترنت.

حاول جانب من الفقه تعريف جرائم الانترنت ضمن عبارات بسيطة من اجل أن يتم استيعابها،وتضييق نطاقها[1]، باعتبارها جرائم مستقلة لم تظهر إلا بظهور الانترنت كجرائم الاختراق والنشر الفيروسي، في حين أن هناك اتجاه أخر حاول التوسيع في تعريف جرائم الانترنت، وسواء تم تبني التعريف الضيق (الفرع الأول) أو الموسع لجرائم الانترنت(الفرع الثاني). فانّ الأهم في الأمر هو تعريف أهم العناصر المتصلة بالتعريف والمتمثل في المعلوماتية والانترنت، وهما الركيزتين اللتين يبنى عليها تعرف الجرائم محل الدراسة.

الفرع الأول:التعريف الضيق لجرائم الانترنت.

تعرف جرائم الانترنت بأنّها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بمعنى المنظومة المعلوماتية بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود[2]، حيث يعتبر سلوكا غير مشروع يؤثر في سلامة وأمن الأجهزة والمعلومات(أولا) الموجودة بها، فالتعريف الضيق يأخذ بعين الاعتبار الوسيلة المستخدمة وهي الحاسب الآلي أو–المنظومة المعلوماتية–(ثانيا)، الذي كان لوقت قريب الوسيلة الوحيدة للولوج إلى الإنترنت، لكن بعد ظهور الجيل الثالث والرابع له واستغلال الألياف البصرية والأقمار الصناعية أدرك معظم المشرعين(وعلى رأسهم المشرع الجزائري) أن الحاسب الآلي أو المنظومة المعلوماتية، ليست الوسيلة الوحيدة على الإطلاق لارتكاب هذه الجرائم، وقد دعا الكثير إلى تفادي مثل هذا التعريف بحجة أن الجريمة المعلوماتية او

---

a -Infractions liées aux technologies de l'information et de la communication : les infractions portant atteinte aux systèmes de traitement automatisé de données telles que définies par le code pénal ainsi que toute autre infraction commise ou dont la commission est facilitée par un système informatique ou un système de communication électronique. » Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication , JOR A , N° 47,p4

[1] Parker(DonnB) ,Nycum(S) and Aura (s),Computer Abus,:Stanford research institute,1973;Taber(J.k), On Computer Crime ,C.L.J,1979,vol1,p.517هامش مشار اليه لدى نائلة عادل محمد فريد قورة ، المرجع السابق، ص28.

[2] عبد الفتاح بيومي حجازي ،الدليل الجنائي و التزوير في جرائم الكمبيوتر والإنترنت ،المحلة كبرى ،مصر،2001،ص1.

جريمة الانترنت ما هي إلا جريمة تقليدية ارتكبت بأسلوب جديد[1]، وعلى اثر الانتقاد الموجه لهذا التعريف حاول هؤلاء المهتمون التوسيع من المفهوم بإدراج وسائل الاتصالات والبرمجيات .

أولا: المعلوماتية أو علم المعلومات .

كانت المعلوماتية أول خطوة نحو الثورة التقنية التي وجدت منذ أكثر من ربع قرن ولازالت في تقدم مستمـر، يقصد بها :"ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات تجميعها وتنظيمها؛ واختزالها واسترجاعها وتفسيرها وبثّها وتحويلها واستخدامها"[2]؛ لذلك فإنّ المعلوماتية هي عملية معالجة للمعلومات[3]، لذلك وحماية للمعلومة انقسم الفقه في تحديد طبيعتها القانونية باعتبارها محل الجرائم محل الدراسة، وأنّها بمعزل عن الوسيط المادي الذي يمكن ان تندمج فيه[4].

امّا عن **الاتجاه الأول** فهو يرى أنّ المعلومات هي من القيم المالية، باعتبارها قابلة للتملك ويمكن تقويمها اقتصاديا، لذلك يمكن انّ تكون محل للحقوق المالية، ذلك لإمكانية استغلالها كخدمات ومنافع[5].

في حين أن **الاتجاه الثاني**، يرفض أن يُدرج المعلومات ضمن القيم المالية لأنّها لابد أن تكون قابلة للتملك، وهو مالا يمكن في اعتقاده لطبيعتها المعنوية، ويترتب على ذلك أنّ الأشياء التي يمكن الاستئثار بها هي وحدها التي تدخل في عداد القيم[6].

---

[1] نائلة عادل محمد فريد قورة ،جرائم الحاسب الآلي الاقتصادية.دراسة نظرية وتطبيقية،منشورات الحلبي الحقوقية، لبنان،2005،ص28.

[2] أحمد خليفة الملط ،الجرائم المعلوماتية،دراسة مقارنة،ط2،دار الفكر الجامعي،الاسكندرية،مصر،2006 ،ص 78.

[3] عرّفت الاتفاقية الأوروبية المعلومات بأنها كل إبراز للحقائق والمعلومات أو المعاني في هيئة تقبل المعالجة في نظام الحاسوب بما في ذلك البرنامج الذي يجعل الحاسوب مؤهلا للعمل (المادة الأولى الفقرة أ من الاتفاقية الأوروبية للإجرام السيبيري ؛https://rm.coe.int/16802fa3ff.

[4] نائلة عادل محمد فريد قورة، المرجع السابق، ص111.

[5] نائلة عادل محمد فريد قورة، المرجع السابق، ص116

[6] نائلة عادل محمد فريد قورة، المرجع السابق، ص119

أ- تعريف المعلومة.

المعلومة هي كل البيانات والمعطيات التي يمكن أن تأخذ أشكال مختلفة، نصوص أو فيديو، أو صور أو تسجيلات صوتية، والتي يمكن أن تتمتع بالحماية الفنية القانونية عبر أي وسيلة تخزين أو عرض؛ "فالواقع أنّ المعلومات الوفيرة لا تعني شيئا ذا قيمة في مجتمع لا يحسن ما تحتويه هذه المعلومة من مفاهيم وعلاقات"[1]، وما يشابه المعلومة في المعنى البيانات[2]،وهي المعطيات المتصلة بجهة معينة، في حين انّ المعلومة هي المعنى المستخلص منها بعد معالجتها[3]، فهي عبارة عن كلمات وأرقام ورموز وحقائق خام لا يوجد صلة بينها صالحة لتكوين فكرة أو معرفة[4].

أمّا المعطيات فقد عرّفها المشرع الجزائري في الفقرة (ج) من المادة(2) من الفصل الأول من القانون(09-04) لسنة2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنّها"أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شانها جعل منظومة معلوماتية تؤدي وظيفتها"[5].

غير أنّ ما يهمنا هو الحماية التي تتصف بها المعلومات، لذلك وبعد اطلاعنا على بعض المراجع فإنها، وفي النهاية لا تميز بين المعطيات والمعلومات والبيانات خصوصا في ظل تطور

[1] فهد عبد الله العبيد العازمي، المرجع السابق ،ص 37.

[2] "البيانات هي معلومات في حالة كمون اما المعلومات فهي بيانات في حالة حركة ونشاط، لذلك البيانات تمثل حقائق رقمية او غير رقمية او مشاهدات واقعية لا تصورية او قياسات تتم بطريقة منهجية يمكن لاحد الناس قراءتها وفهم دلالتها"،ايمن عبد الله فكري،المرجع السابق.ص39.

[3] هشام فريد رستم ،قانون العقوبات ومخاطر التقنية،مكتبة الآلات الكاتبة،1995،ص26.

[4] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة،منشاة المعارف الإسكندرية،مصر ،بدون سنة.ص12. "فالمعرفة هي العلم بموضوع خارجي لا تدركه الحواس أصلا إلا انه يمكن إدراكه بواسطة فكرة،فهناك المعرفة ثم المعلومة ثم المعطيات او البيان الذي يعالج المعلومة"،ايمن عبد الله فكري، المرجع السابق، ص40.

[5] Art2 « c -Données informatiques : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction. » Loi n° 09-04

تكنولوجيات الإعلام والاتصال،لان هناك ترابطاً بينهم[1]، ولكن لابد من التمييز بين المعلومات ومصطلح المعلوماتية، فقد استعمل مصطلح المعلوماتية لأول مرة من طرف ميخالوف (Mekhlov) مدير المعهد الاتحادي للمعلومات العلمية والتقنية بالاتحاد السوفياتي سابقا؛ وسماه بعلم " المعلومات العلمية " ثم انتشر استخدامه بعد ذلك على مستوى جغرافي واسع، إذن فالمعلوماتية هي المعلومة المعالجة أليا ولكي تكون محل حماية قانونية لا بد أن تتوافر على الشروط التالية[2]:

ب– الشروط الواجب توافرها في المعلومة.

المعلومة هي رموز نستخلص منها معنى معين في مجال محدد وتتمتع بالتحديد والابتكار والسرية والاستئثار[3]، والشروط الواجب توافرها في المعلومة تتمثل فيما يلي:

1– التكاملية وسلامة المحتوى بمعنى التأكد من أن المحتوى المعلوماتي سليم لم يتم تعديله أو تغييره بداية من معالجتها وصولا إلى إخراجها بطريقة غير مشروعة[4]، لذلك فان أي معلومة قابلة للعبث فيها بهذا المفهوم هي غير قابلة للحماية القانونية.

2– التحديد والابتكار،أن تكون المعلومة محددة يعني أن توصل معنى محدد للمتلقي، أمّا الابتكار أيْ أن تكون مميزة عن المعلومات المتاحة ،لأنّها نتاج فكري إنساني.

3– استمرارية توفر المعلومة، بمعنى بإمكان المستخدم أن يستغلها ويعمل بها دون أن يكون هناك أي مانع من ذلك.

[1] نائلة عادل محمد فريد قورة، المرجع السابق ، ص.57

[2] منير محمد الجنبيهي،ممدوح محمد الجنبيهي، جرائم الانترنت، دار الفكر الجامعي، الإسكندرية، مصر ، 2004.ص30.

[3] أحمد خليفة الملط ،المرجع السابق، ص 74.

[4] علي عبد القادر القهوجي،الحماية الجنائية للبيانات المعالجة الكترونيا، مؤتمر القانون والكمبيوتر والانترنت،كلية الشريعة والقانون،العين ،جامعة الإمارات العربية المتحدة،من 1الى3 ماي 2000، المجلد الثاني، الطبعة الثالثة،2004، ص600.

4-عدم إنكار التصرف المرتبط بالمعلومات ممن قام به،وهو ضمان المستخدم الذي قام بتحين مثلا للمعلومة أن لا ينكره، فيمكن إثبات أي تصرف غير مشروع إذا تعلق الأمر بالعبث بالمعلومة أثناء إخراجها مثلا.

5-السرية والاستئثار،لا يمكن حماية أي معلومة دون أن تكون سرية، فهو ما يميزها عن المعلومات المباحة التي يمكن للجميع حيازتها، فلا تلحق الحماية القانونية إلا المعلومة المحمية بأي طريق إما عن طريق التشفير أو الكلمة السرية أو غيرها من أصناف الحماية المتجددة كل مرة، وبهذا فان لم تتوافر هذه العناصر فلا مجال لان تكون المعلومة محمية[1].

ولكن ما يجدر التنويه له أن هذه العناصر قد تتلاءم مع معلومات معينة كالمعلومات العسكرية والأمنية والسيادية والاقتصادية الحساسة للدول، أما إذا تعلق الأمر بالأفراد فإذا حاولنا لم شتات كل هذه العناصر من اجل أن تصبح المعلومة قابلة للحماية، فانّه يصعب بمكان تطبيق ذلك، خصوصا مع انتشار شبكات التواصل الاجتماعي، وانتشار الواسع لأساليب الاختراق المبسط وبالتالي العبث بالمعلومات .

ج -أنواع المعلومات.

بعد أن تطرقنا إلى الشروط الواجب توافرها في المعلومات على أساسها، يمكن تصنيف المعلومات إمّا على أساس نوعيتها أو على أساس طبيعتها[2]برغم انّ هناك معلومات لا تدخل تحت آي تصنيف.

1-الفئة الأولى:المعلومات من حيث نوعيتها

[1] فهد عبد الله العبيد العازمي،المرجع السابق،ص 42و43.

[2] محمد سامي الشوا، المرجع السابق، ص94و95و ايمن عبد الله فكري، المرجع السابق، ص29-33.

– **المعلومات الشخصية**: المعلومات المرتبطة بالشخص المخاطب بها كاسمه وحالته الاجتماعية وموطنه وصحيفة السوابق القضائية الخاصة به[1]، والمعلومات التي تطلب من الشخص في حالة استخراجه لبطاقة التعريف الوطنية البيومترية أو جواز السفر، والتي يتم معالجتها، فتصبح معلومات او معطيات معالجة اليا، فتجب لها الحماية القانونية، وهي المعلومات التي لم تكن محميتا من قِبل المشرع الجزائري إلاّ بعد التعديل الأخير للدستور في المادة 46منه التي جاء فيها مايلي:"لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه ويحميها القانون.سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

لا يجوز بأي شكل المساس بالحقوق دون أمر معلل من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم.

حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه"[2].

كما انّه أدرج حماية المعلومات المتحصل عليها عند اللجوء إلى إجراءات التحري الخاصة، والمذكورة في قانون (09-04)باعتبارها معلومات مصنفة التي تعد المعلومات الشخصية من فئاتها،باعتبارها معلومات مستقاة من إجراءات، التي يعتبر موضوعها معلومات شخصية من أصنافها.

– **المعلومات المالية والاقتصادية**:وهي المعلومات التي تتعلق بعناصر الذمة المالية للأفراد، أو ما يطلق عليه بالنقوذ الالكترونية أو ما يتعلق بالأسرار التجارية وسر الصنعة[3].

[1] عبد الله حسين على محمود،سرقة المعلومات المخزنة في الحاسب الآلي،دار النهضة العربية،القاهرة مصر، 2002 ،ص 159

[2] القانون (16-01)يتضمن التعديل الدستوري المؤرخ في 26 جمادى الأولى عام 1437الموافق6 مارس2016 ،ج ر رقم 14 المؤرخة في 07 مارس2016 ص 11.

[3] نائلة عادل محمد قورة، المرجع السابق، ص100.

-المعلومات التجارية والصناعية:والتي تتعلق بدراسة السوق والتصنيع والإنتاج

-المعلومات العسكرية:والمتمثلة في أسرار الدولة، المشروعات النووية والتصنيع والتحديث للأسلحة والمعدات إلى غير ذلك من المعلومات المتعلقة بالنشاط العسكري[1].

2-الفئة الثانية:المعلومات من حيث طبيعتها .

-المعلومات السرية:وهي المعلومات غير المصرح بها وخصوصا ما تعلق بالأسرار العسكرية، والأمن الوطني وهي من المعلومات التي دأب المشرع على حمايتها وخصوصا من تطور التقنية، في القانون (09-04) ، التي يكون الاطلاع عليها والحصول عليها مقصورا على أشخاص معينين فقط، وتكون المعلومات الخاصة بالمصنفات الفكرية، والأدبية وهي المعلومات التي تكّون بنات أفكار الشخص، أي إنتاجه الفكري، وتظهر في شكل مصنفات محمية، قد اقر لها القانون ذلك، والتي تعد من المعلومات السرية[2].

-المعلومات غير السرية: وهي المعلومات المتاحة للجمهور دون وجود أي حماية أمنية لها،كالمعلومات المتداولة في المنتديات ومواقع تواصل الاجتماعي دون أن تتحقق لها أي حماية فنية أو قانونية. الواقع ان هناك تقسيمات أخرى ومختلفة[3].

[1] محمد سامي الشوا ،المرجع السابق، ص59.

[2] محمد سامي الشوا، المرجع السابق،ص174 وما يليها،ايمن عبد الله فكري،المرجع السابق،ص31-32.

[3]هناك من يقسم المعلومات إلى ثلاث أقسام، المعلومات الاسمية والتي تنقسم بدورها إلى معلومات شخصية لا يمكن الاطلاع عليها إلا بموافقة الشخص،والمعلومات الموضوعية كالمقالات والمعلومات الخاصة بالمصنفات الفكرية وأخيرا المعلومات المتاحة ،وهي المعلومات التي يمكن تداولها من طرف الجميع،للمزيد راجع ،عفيفي كامل عفيفي،المرجع السابق،ص وفهد عبد الله العازمي، المرجع السابق،ص40.

ثانيا: نظام المعلومات[1].

إنّ نظم المعلومات أو المنظومة المعلوماتية عماد التقنية، يشمل هذا النظام كل وسيلة مخصصة لصناعة المعلومات أو معالجتها أو لتخزينها أو لعرضها أو لإتلافها، يتطلب تشغيله الاستعانة بشكل أو بأخر بالوسائل الالكترونية[2].

أ–تعريف نظم المعلومات.

عرّفت معاهدة بودابست نظم المعلومات بأنّها:"كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة التي يمكن أن تقوم بمفردها، أو مع مجموعة عناصر أخرى تنفيذا لبرامج معينة ،بأداء معالجة آلية للمعلومات"[3] ،وعرفها المشرع الجزائري في المادة الثانية من القانون (09-04) كالاتي:"ب– المنظومة المعلوماتية:أي نظام منفصل او مجموعة من الأنظمة المتصلة يبعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرامج معينة "، ورغم الارتباط الوثيق بين الإنترنت و الحاسوب إلا أن الفرق واضح بينهما حيث أنّ الحاسب الآلي أو المنظومة المعلوماتية جزء من شبكة الانترنت، ويمكن تعريف الحاسوب كذلك بأنه "آلة حاسبة إلكترونية تستقبل البيانات ثم تقوم عن طريق الاستعانة ببرامج معينة بعملية تشغيل هذه البيانات للوصول إلى النتائج المطلوبة"[4].أي "هو الآلة المتفاعلة مع الأوامر الإنسانية ذات التقنية المتطورة في معالجة البيانات"[5].

---

[1] Art2 « b -Système informatique : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données. » Loi n° 09-04

[2] ممدوح عبد الحميد عبد المطلب ،زبيدة محمد حاسم،عبد الله عبد العزيز،أنموذج مقترح لقواعد اعتماد الدليل الرقمي لإثبات في الجرائم عبر الكمبيوتر،بحث مقدم لمؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس ، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي،9-11ربيع الأول 1424هـ،الموافق 10-13مايو 2003، ص 2236 .

[3] هلالي عبد الإله احمد، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001 ، دار النهضة العربية ، القاهرة ، مصر، 2006،ص40.

[4] أحمد خليفة الملط، المرجع السابق، ص 25.

[5] عمر محمد بن يونس أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب،دار النهضة العربية،2004،ص55.

فهذه الآلـة هي عبارة عن جهاز إلكتروني تعمل بنظام الحوسبة الذي أصبح يدخل أية آلة رقمية حديثة في نطاقه، و لكننا رأينا سابقا أن هناك اختلاف بين الحاسب الآلي و الهـواتف النقالة، لأن الحاسب هو جهاز معلوماتي لمعالجة المعطيات أمّـا الهاتف النقـال هو وسيـلة اتصـال، ولكن بالتطور التقني حصل هناك تزاوج بين تقنية الحاسب و الاتصال أو ما يسمى التكنولوجيات الحديثة للاتصال و الإعلام.

و من خلال التعريفات السابقة يمكننا أن نعرف الحاسب بأنه عبارة عن جهاز إلكتروني يتكون من مجموعة متداخلة من الأجزاء تعمل فيما بينها بهدف مشترك هو إخراج العمليات الحسابية و المنطقية طبقا لبرامج يتم وضعه مسبقا من خلال عدة عمليات هي الإدخال و المعالجة، و الاسترجاع و الإخراج.[1]

ب–مكونات نظم المعلومات.

تتكون المنظومة المعلوماتية من مكونات مادية ومعنوية، أي مكونات أساسية و المتمثلة في أنظمة التشغيل و أنظمة البرمجة.و الكيانات التطبيقية، و تضم هذه الفئة البرامج التي تمكن مستخدم الجهاز من أن ينفذ بواسطته عملا محددا بدقة و متصلا باحتياجات هذا المستخدم الخاصة و الذي يسعى لمواجهة مشكلة ما.[2](معالجة النصوص، جداول البيانات الإلكترونية و برامج قواعد البيانات، برامج التحليل الإحصائي و برامج التطبيقات من الرسم و التصميم الهندسي...)، مع العلم أنّ هذه البرمجيات و التطبيقات هي التي تساهم في فعالية الخدمات الجديدة للحكومة الإلكترونية و التجارة الإلكترونية، لذلك كان يجب حمايتها قانونيا ثم حماية البيانات و المعطيات التي تحتويها و التي تكون عادة سرية و تتعلق بالحياة الخاصة، و هذا ما تفطن

[1] أحمد خليفة الملط، المرجع السابق، ص27.

[2] علي جبار الحسيناوي، جرائم الحاسوب و الأنترنت، دار اليازوري العلمية للنشر و التوزيع ، عمان، الأردن، 2009، ص 28.

له جزئيا المشرع الجزائري بسنه للقانون (03-05)[1]، رغم أنّه لم يورد أي تعريف لبرامج الكمبيوتر و الواقع أن هذه الكيانات المنطقية أو المعنوية، لا تتعلق فقط بالحاسب الآلي بمفهومه الضيق، بل تتعداه إلى البرمجيات التي تستخدمها الهواتف النقالة و الذكية و مختلف الآلات التي يمكن أن تتصل شبكة الأنترنت و لكن، ما تجدر الإشارة إليه أن الشركات المنتجة لهذه البرمجيات قد تفطنت إلى ضرورة إيجاد نمط معين لهذه البرمجيات عند تحملها بحسب كل وعاء رقمي، أي هناك برمجية خاصة بالحاسب الشخصي و أخرى بالهاتف الذكي و أخرى باللوح الرقمي و حتى الخاصة بساعة اليد.

أمّا البرامج أو المكونات المنطقية، هي مجموعة من التعليمات والأوامر المكتوبة بإحدى لغات الحاسب الآلي التي يتم تحويلها لاحقا من قبل المؤلف أو المجمع أو المترجم إلى لغة الآلة التي يفهمه المعالج الرئيسي في الحاسب[2]، ولكن كما ذكرنا مع التطور التقني وظهور الهواتف النقالة التي يمكن بها الولوج للإنترنت،حتى هذه البرامج كيفت على حسب الآلة ، فمثلا هناك شركات عالمية لبرامج مكافحة الفيروسات طرحت منتوجا لها من أجل مسح الهواتف النقالة وكشف الفيروسات ،فلم تعد البرامج والتطبيقات خاصة فقط بالحماية الأمنية لوسائل الولوج إلى الانترنت فقط بل حتى شبكاته ، تنقسم البرامج إلى برامج تشغيل هي البرامج التي تهيأ لأداء الوظائف المطلوبة منها والمحددة بنمط البرنامج[3] ،أما برامج التطبيق فهي برامج معالجة المعلومات.

ج- مفهوم نظام المعالجة الآلية للمعطيات:

للدلالة على جرائم الانترنت استعمل المشرع للوهلة الأولى، نظام المعالجة الآلية أو النظام المعلوماتي وهو سلسلة من المعلومات التي تتم أليا باستخدام نظام معلوماتي،يقوم بتجميع

[1] الأمر (03-05)المؤرخ في 19 جمادى الأول عام 1424 الموافق 23 يوليو لسنة 2003، يتعلق بحقوق المؤلف والحقوق المجاورة ج.ر 44 ليوم 23 يونيو لسنة2003 ،ص3

[2] محمد الربيعي،احمد احمد شعبان الدسوقي،عبد العزيز إبراهيم الجبري ،على بن صالح الغامدي، المعجم الشامل لمصطلحات الحاسب الآلي والإنترنت. الطبعة الأولى ،مكتبة العبيكان ،الرياض 2002،ص341.

[3] محمد حماد مرهج الهيتي،التكنولوجيا الحديثة والقانون الجنائي.دار الثقافة ، الأردن ،2004،ص147.

وتسجيل، والتعديل والاسترجاع للمعطيات بهدف الحصول على نتائج صالحة للاستعمال[1]، والذي يمثل النشاط التقني في جرائم الانترنت، وهو مايميزها عن باقي الجرائم، لأنه أي النشاط التقني عنصر لازم في مثل هذا النوع من الجرائم، ولكن اعتماد النظام المعلوماتي والمعتمد أساس على معالجة المعلومة أي المعلوماتية ، كمحل للجريمة سوف يؤدي إلى عجز النصوص القانونية التي تحمي هذا النظام–المعلوماتي– لحماية باقي الحقوق التي وجبت لها الحماية القانونية.

لذلك ونتيجة التطور التقني الحاصل في تكنولوجيات الإعلام والاتصال، وما يتطلبه من ضرورة القيام بتوفير المعلومة —والذي يعد احد خصائصها الاصيلة– والمتمثل بالانترنت لحد الآن ومن هذا المنطلق قام المشرع بتبني موضوع تكنولوجيات الإعلام والاتصال كمحل لجرائم الانترنت، حيث انه هناك العديد من الجرائم العادية التي يتم ارتكابها بواسطة هذه التكنولوجيات، مما أضفى– أي على هذه السلوكيات العادية المستحدثة –خصوصية في محل الجريمة، وبالتالي خصوصية في اثباتها وهذا ما ينعكس على إجراءات الإثبات، رغم أنّ الأصل هو تصنيفها من الجرائم العادية بالنسبة إلى التطور التكنولوجي والوسائل الحديثة المستعملة في ارتكابها.

الفرع الثاني:التعريف الواسع لجرائم الإنترنت[2].

على اثر التعريف الضيق لجرائم الانترنت والذي حصرها في الجرائم التقنية فقط، او جرائم المساس بالمعالجة الآلية للمعطيات، تم إعطاء تعريف أوسع بغية إدراج شبكات الاتصال في تعريف جرائم الانترنت وهي عمل غير قانوني يستخدم فيه الحاسب الآلي كأداة أو موضوع[3]للجريمة بمفهومه الواسع الذي يشمل شبكات الاتصال، لذلك من أجل تعريف جرائم الإنترنت أو جرائم تكنولوجيات الإعلام والاتصال لا بد من تعريف بعض المصطلحات، التي يتم تداولها كالحاسب

[1] ايمن فكري، المرجع السابق، ص55.

[2] Roden(Adrian) ,computer crime and the law,C.L.J,1991,vol.15,p.399، هامش مشار اليه لدى نائلة عادل محمد قورة فريد قورة، المرجع السابق، ص30.

[3] محمد عبد الله المنشاوي ،جرائم الانترنت من منظور شرعي وقانوني،انظر الموقع
http://www.ba-menoufia.com/books-pdf/1304065160509f5b748.pdf تاريخ الاطلاع:26-11-2014

الآلي أو المنظومة المعلوماتية والبرامج والتطبيقات الخاصة بها والخدمات التي تقدمها ، وباعتبار هذه المصطلحات نقاط مشتركة بين العديد من مواضيع الأطروحة سوف يتم التطرق لها في حينها.

تعرف تكنولوجيا المعلومات بوصفها الأداة التي ترتكب عبرها أو من خلالها هذا النوع من الجرائم، فعرفتها منظمة اليونسكو[1] بأنّها "مجالات أو فروع المعرفة العلمية والتكنولوجية والهندسية والأساليب الإدارية المستخدمة في تناول ومعالجة المعلومات وتطبيقاتها والمرتبطة بالحاسبات أو الحواسيب الآلية وتفاعلها مع الإنسان وما يرتبط بذلك من أمور اجتماعية واقتصادية وثقافية.[2] كما تعرف تكنولوجيات الإعلام والاتصال بأنّها :" مجموعة من التقنيات والأدوات أو الوسائل أو النظم المختلفة التي يتم توظيفها لمعالجة المضمون أو المحتوى الإعلامي والاتصالي"[3].

من هنا لابد من تعريف الانترنت، باعتباره الوسيلة التي بعد أن كانت جزءاً من الاتصال أصبحت تجمع بينه وبين الإعلام،مكونة بذلك محل الجريمة كوسيلة أو موضوع.

أولا: تعريف الانترنت.

الانترنت"هي تلك الوسيلة أو الأداة التواصلّية بين الشبكات المعلوماتية دون اعتبار للحدود الدولية"[4]،كما يطلق عليها عدة تسميات بحسب الخدمات التي تقدمها أو الخصائص التي تلحقها ،فالواقع أنّ معظم الأفراد حتى لا نقول كل فرد في المجتمع الجزائري أصبح يعرف مصطلح الانترنت

[1] اليونسكو منظمة الأمم المتحدة للتربية والعلم والثقافة هي وكالة متخصصة تتبع منظمة الأمم المتحدة تأسست عام1945، هدف المنظمة الرئيسي هو المساهمة بإحلال السلام والأمن عن طريق رفع مستوى التعاون بين دول العالم في مجالات التربية والتعليم والثقافة لإحلال الاحترام العالمي للعدالة ولسيادة القانون ولحقوق الإنسان ومبادئ الحرية الأساسية ،يرجى الاطلاع على الروابط https://ar.wikipedia.org/wiki/%D9%8A%D9%88%D9%86%D8%B3%D9%83%D9%88 و http://ar.unesco.org/about-us/introducing-unesco

[2] عبد الحكيم رشيد توبة،المرجع السابق،ص109.

[3] محمد الفاتح حمدي، مسعود بوسعدية، ياسين قرناني،تكنولوجيا الاتصال والإعلام الحديثة، كنوز الحكمة، الابيار ،الجزائر،2010.ص3.

[4] عمر محمد أبو بكر بن يونس ،الجرائم الناشئة عن استخدام الإنترنت،الأحكام الموضوعية والجوانب الإجرائية،المرجع السابق،ص31.

أو النت، ومن ذلك كيفية استخدامه خصوصا مع سهولة الولوج إلى الشبكة عبر الهواتف الذكية واللوحات الرقمية .

أ- خصائص الإنترنت.

انّ تميز الانترنت بخصائص معينة ناتج عن وجود تعاريف مختلفة له، اذ ليست للتقنية قيمة في ذاتها وإنما هي وسيلة لتنظيم العمل بموضوع ما والاستفادة منه ...فإذا أضفت المعلومات كموضوع للتقنية فإننا بصدد الانترنت[1]، هذا ما يدفعنا للقول أنّ الانترنت عالم افتراضي لكل شيء، وهي بجانبها المظلم تجسد تهديدا حقيقيا ضد المجتمع[2]، فهو عالم موازي لعالمنا الحقيقي بداية من الحياة الاجتماعية إلى الاقتصادية وصولا إلى السياسية، وكل وسائل الإعلام والاتصال التي ظهرت بعد الانترنت لحد الآن هي عبارة عن وسائل داعمة ومساعدة لانتشارها، ولكن هذا لا يمنعنا من تقديم وإعطاء تعريف للانترنت فهي شبكة تسمح بانضمام شبكات معلوماتية مختلفة عن طريق استخدام بروتوكول (IP-TCP) والبريد الالكتروني(Email) ومجموعة الأخبار (news group)وصفحات(FTP) وبنوك المعلومات[3]، حيث أن (IP-TCP) هما بروتوكولات التي ميزت الانترنت عن باقي وسائل الاتصال في البداية، وهما عبارة عن"بروتوكول تقني حول الاتصالات مشتق من بروتوكولين مستقلين هما :بروتوكول التحكم في النقل TCP(Transfert Control Protocol)؛ و بروتوكول انترنت (IP Internet Protocol) ونظرا لاشتراكهما جرى العمل عادة إلى الإشارة إليهما مجتمعين[4]، كما عرفت الانترنت بأنها"شبكة تتألف من عدد من الحاسبات الآلية التي ترتبط فيما بينها، أما عن طريق الخطوط التليفونية أو الأقمار الصناعية،لتكون شبكة

[1] عمر محمد أبو بكر بن يونس ،المرجع السابق،ص.40 ويقول العالمان الأمريكيان جلي هاري كادليل (Glee Hara Cadly) ، وزميله بان ماكروجل(Pat Mc Regal)، انّه لا توجد إجابة محددة للإجابة على ماهية الانترنت، عبد الفتاح بيومي حجازي ،الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة،المرجع السابق،ص21.

[2] *Solange Ghernaouti-Hélie, , Internet et Sécurité* op.cit . p27.

[3] انظرj .huit.op.cit.p02 مرجع مشار اليه لدى رشدي محمد على محمد عيد،المرجع السابق،ص39.

[4] حسين بن سعيد ألغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق ،ص18.

كبيرة تتيح لمستخدميها الدخول في أي وقت متى كان الحاسب الآلي الخاص به مزود بجهاز مودم"[1].

يلاحظ أنّ تعريف شبكة الانترنت، مفهوم متطور بحسب تطور الوسيلة المستخدمة للولوج إلى الانترنت، فالتعاريف كانت في أول الأمر تنحصر في الحاسب الآلي بنوعيه الشخصي والمحمول، ثم بعد ذلك الهواتف النقالة إلى ساعات اليد وغيرها؛ مما ظهر وسوف يظهر مستقبلا، مما يبرز جليا أنّ العامل المشترك في تطور تكنولوجيات الإعلام والاتصال هو وجود شبكة الانترنت المتصل بها؛ عبر الحاسب أو الهاتف أو غيرها من الوسائل، فعدم وجود شبكة الانترنت لا يدعو للبحث أصلا.

إنّ تمتع الانترنت بمجموعة من المزايا جعلتها الأصل في الاتصال والإعلام؛ بعد أن كانت وسيلة اتصال فقط.والتطور المستمر للانترنت لا يجعلها محصورة في الخصائص الآتية أنها ليست مملوكة للغير (لأحد)،تتميز بالنمو السريع والتغيير المستمر وهذا لافتراضية المجتمع المندمج تحت لوائها، من خلال مواقع التواصل الاجتماعي، وهذا لقلة تكلفتها نسبيا، مما أدى إلى عبورها الحدود الدولية وأصبحت ظاهرة دولية بامتياز.

ب–الخدمات التي يقدمها الإنترنت.

تتعددالخدمات التي يقدمها الانترنت وهي في تطور مستمر مادام أنّ هناك تطور في التقنية، كالبريد الإلكتروني، المنتديـات و المجموعات الإخبارية، تحويل أو نقل الملفـات(F.T.P)[2]، خدمة الويب، خدمات التحدث (chat)، (net phone)، الفايبر، الواتس أب، وغيرها من الخدمات التي تظهر بين الفينة والأخرى، نذكر أهم الخدمات على سبيل المثال والمتمثلة في:

[1] جميل عبد الباقي الصغير ،الانترنت والقانون الجنائي للأحكام الموضوعية للجرائم المتعلقة بالانترنت،دار النهضة العربية،القاهرة ،مصر ،ص04,

[2] المادة (2) من المرسوم التنفيذي (98- 257) يضبط شروط وكيفيات إقامة خدمات الانترنت واستغلالها المؤرخ في 3 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998، ،ج ر عدد 63 لسنة 1998،ص5 تنص على مايلي" بروتوكول نقل الملفات (FTP) File Transfer Protocol :خدمة تعبئة الملفات عن بعد بصيغة نقطة الى نقطة".

1-خدمة التجارة الإلكترونية: بما فيها التسويق والشراء الإلكتروني، وهي عملية ترويج وتبادل السلع والخدمات وإتمام صفقاتها باستخدام وسائل الاتصال و تكنولوجيا تبادل المعلومات الحديثة عن بعد، لاسيما شبكة المعلومات الدولية (الانترنت) دون حاجة لانتقال الأطراف والتقائهم في مكان معين[1].وهي استخدام المنظومة المعلوماتية عن طريق الانترنت، بقصد التوصل إلى اتفاقيات تجارية[2]، ولا يزال لحد الآن الخلط بين التجارة الالكترونية، والإعلانات التجارية فكل من يحاول تعريفها يضيف فقط مصطلح عبر الانترنت في حين تمثل عِلماً من التبادل التجاري مستقلا بذاته، وهذا ما تفطنت له بعض الدول التي حاولت تقنين هذه التجارة.حيث بعدما كانت المعلومة مجردة من أي قيمة تجارية عند المستهلك أصبحت سلعة يطلق عليها المنتجات أو عالم المنتجات الالكترونية[3]، ورغم أنّ الجزائر ما زالت تلحظ إقبالاً محتشماً على هذا النوع من التجارة كون الفرد الجزائري لا يثق كثيرا بما هو غير ملموس، خصوصا ماتعلق بالدفع الالكتروني، رغم هذا هناك من المواقع الإلكترونية سجلت حضورها بإسهامها في إدخال ثقافة التجارة الإلكترونية مثل موقع (موقع الكتروني للتجارة الالكترونية).

2-الشبكة المعلوماتية الدولية (World Wide Web): وهي تعد بمثابة بوابة الإنترنت وهذا ما يطلق على الخدمات مثلا بوابة وزارة العدل على الإنترنت: www.mjustice.dz، فهي ضمن خدمات الشبكة بعد أن ظهرت بصورة أوضح قبل انتشار شبكة الإنترنت؛ حيث عرفها المشرع الجزائري من خلال المرسوم التنفيذي (98-275)[4] في المادة الثانية تعرفا كالآتي:" خدمة تفاعلية للإطلاع أو احتواء الصفحات متعددة الوسائط (Multimedia)، نصوص رسوم بيانية صوت أو صورة، موصولة بينها عن طريق صلات تسمى نصوص متعددة (Hypertexte).

[1] احمد عبد الكريم سلامة، الانترنت والقانون الدولي الخاص،فراق أ م خلاف؟مؤتمر القانون والكمبيوتر والانترنت، مج 1،ط3كلية الشريعة والقانون ،الشارقة، الامارات العربية المتحدة ، 2004،ص28.

[2] عمر محمد بن يونس أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق.ص140.

[3] عمر محمد بن يونس أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق،ص140.

[4] المرسوم التنفيذي (98-275) ، سابق الذكر، ص30.

3-البريد الإلكتروني[1]: يرجع ظهور البريد الإلكتروني إلى العالم الأمريكي راي توملنسون (RayToMlinson[2])؛ أصبح للبريد الإلكتروني أهمية كبيرة في ظل التطور الحاصل في التجارة الإلكترونية والحكومة الإلكترونية، وبات مؤخرا من أهم وسائل المعاملات الإلكترونية خصوصا مع صدور بعض القوانين، التي جسدت ذلك كقانون عصرنة العدالة[3].

4-المراجعة الطبية عن طريق الإنترنت والتدخلات الجراحية: ويكون عن طريق مواقع الكترونية وتطبيقات للهواتف الذكية ، لتشخيص الأمراض وصرف الدواء المناسب، على أنّ هناك العديد من التحفظات خصوصا إذا تعلق الأمر بإبداء تشخيص خاطئ، وقد أطلق طبيب جزائري تطبيقًا خاص أُطلق عليه اسم "رأي ثاني" وهو تطبيق جديد يمكن تحميله على الهواتف الذكية من اجل الحصول على رأي طبي ثان من أطباء جزائريين مقيمين في الخارج[4].

5-المجالات العسكرية: وهي التي نشأت أصلا لأجلها لأنها وسيلة فعالة للاتصالات والمعلومات على حد سواء، ولكن هي أيضا وسيلة للتجسس.

6-التعلم عن بعد: ربما هي أهم الخدمات الإيجابية للإنترنت، حيث باتت تساهم بقوة في تغيير العالم، بعد أن أصبح الوصول للمعلومة يسيرا، زيادة على وفرة المعلومات وسرعتها إلا أنها بدأت تساهم في تغير طرق التعلم، فعلى سبيل المثال موقع كاليوتيوب (Youtube)[5] يوفر كما ضخما

---

[1] سوف نعود للحديث عن البريد الالكتروني وكيفية ضبط محتواه في حينه الذي يعرف من خـلال المـرسوم (98-257) في المـــــادة2"...البريد الالكتروني e-mail خدمة تبادل رسائل الكترونية بين المستعملين" .

[2] أول من قام بتصميم برنامج للبريد الالكتروني عام 1971 في الولايات المتحدة الأمريكية.

[3] قانون رقم(15-03)مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، يتعلق بعصرنة العدالة،ج.ر رقم 06 ليوم 10 فبراير سنة 2015 ، ص.4.

[4] يرجى الاطلاع على الموقع التالي:http://www.radioalgerie.dz/news/ar/reportage/75905.html

[5] هو أشهر موقع ويب إلكتروني لعرض الأفلام بأنواعها المختلفة العلمية، والثقافية، والاجتماعية، والثورية، والفنية .. إلخ، وقد تأسس سنة 2005م، على يد مجموعة موظفين سابقين في شركة باي بال، حيث يقوم على السماح لمستخدميه برفع الفيديوهات والتسجيلات المصورة، ويتيح لهم أيضاً مشاهدة فورية دون الحاجة إلى تحميل لأي فيديو مرفوع على الموقع بشكل مجاني. إقرأ المزيد على موضوع.كوم

من المحاضرات والدروس في جميع المجالات والشُعب وبكل اللُّغات، والتي يمكن الاستعانة بها في أي وقت مما يسهل طريقة الاستيعاب من حيث الزمان والمكان.

7-الادارة الالكترونية:ولعل من أهم إيجابيات الإنترنت الحكومة الإلكترونية، التي رغم تأخر الجزائر والعمل بها؛ إلّا أنه خلال السنوات الأخيرة تم تفعيلها، وقد كانت السبّاقة لذلك وبشكل مهني وزارة العدل، وهذا من خلال الخدمات التي تقدمها؛ كطلب الجنسية وصحيفة السوابق العدلية، بالإضافة إلى إطلاع المحامي والدفاع إلى ما آلت إليه قضيتهم إلى غيرها من الخدمات عبر الخط.

كما أنّ وزارة الداخلية والجماعات المحلية الجزائرية، أدرجت خدمة تتبع سير إجراءات الحصول على جواز السفر وبطاقة التعريف البيومتريتين[1]، بل أبعد من ذلك وهو إيداع الملف كاملا عبر شبكة الإنترنت، هي خطوة إيجابية لصالح الإدارة الإلكترونية في الجزائر؛ إذا ما تم تأمين شبكة الإنترنت باحترافية وهذا بالتركيز على ضرورة صياغة القوانين التي تنظم مثل هذه المعاملات الإدارية الإلكترونية من الاستخدام غير المشروع، بدأ بالجانب الوقائي الذي يعتمد على الأمن المعلوماتي مع ضرورة أن تكون التطبيقات أصلية أو حتى من إنتاج وطني يضمن خلوها من برمجيات التجسس كما هو الحال بالنسبة لوندوز 10؛ ولو أننا نعتقد أن أي برمجية مغلقة قد تحتوي، وأكيد أنها تحتوي على برمجيات تجسس، بالإضافة إلى توعية مستخدمي هذه الخدمات بإتباع الطرق السلمية، كمحو البيانات بعد ملئها في مكانها المخصص، تفاديا لاستعمالها بطرق غير شرعية.

http://mawdoo3.com/%D8%A8%D8%AD%D8%AB_%D8%B9%D9%86_%D8%A7%D9%84%D9%8A%D9%88%D8%AA%D9%8A%D9%88%D8%A8

[1] يرجى الاطلاع على الموقع: https://passeport.interieur.gov.dz/Ar/Suivi/Suivi_Demande

ثانيا:محل جرائم الانترنت.

كما هو معلوم أنّ المشرع الجزائري حاول جمع كل بعض أنواع الجرائم تحت مفهوم جرائم الانترنت منها الجرائم التقنية البحتة والجرائم التي تكون فيها الانترنت وسيلة لارتكاب الجريمة ،أو وسيلة مسهلة ومساعدة لارتكاب السلوك الإجرامي.وعلى هذا الأساس فان تحديد محل الجريمة ياخد ثلاث صور وهي:

أ–أن يكون محل الجريمة واقعا على شبكة الانترنت بمكوناتها المادية.

أي أنّ الاعتداء على المكونات المادية لشبكة الانترنت وكابلات التوصيل والمنظومة المعلوماتية بمكوناتها المادية من أجهزة حاسوب وطابعات وغيرها لا يعدوان يكون هذا الاعتداء داخل في إطار الجرائم العادية، بحسب نوع الاعتداء ومحل الاعتداء المشمول بالحماية الجنائية كالإتلاف والسرقة، والذي يخرج هذا النوع من الجرائم من الصنف الذي نحن بصدد دراسته.

ب–أن يكون محل الجريمة استعمال الانترنت كوسيلة.

وهي الحالة التي تكون فيها شبكة الانترنت بكل مكوناتها وسيلة لارتكاب الجريمة،حيث يختلف محل الجريمة بحسب الشيئ الذي ينصب عليه السلوك الإجرامي للفاعل والذي يشكل محلا للحق او المصلحة المحمية، فتطبق عليها النصوص العادية ولكن التي تحتوي على ما يثبث ويجيز استخدام الأساليب الخاصة للتحري والتحقيق المتعلقة بتكنولوجيات الإعلام والاتصال،كمصطلح التقنية، أو باستخدام تكنولوجيات الإعلام والاتصال وهو الأمر الحاصل في الجرائم الإرهابية وجرائم امن الدولة والجرائم المتعلقة بالاقتصاد الوطني والجرائم المتعلقة بالاعتداء على الحق في الحياة الخاصة وجريمة اهانة رئيس الجمهورية[1].

[1] هي الجرائم التي أفردنا لبعضها فقط دراسة في المبحث الثاني من هذا الفصل،ص51.

ج–وقوع الجريمة على شبكة الانترنت.

أي أنّ الانترنت هي محل الاعتداء، حيث يتحقق السلوك الإجرامي هنا عندما تكون الانترنت بمكوناتها أي المكونات المعنوية محل اعتداء، من تطبيقات، وبرمجيات، كالعبث فيها وتخريبها وهي الحالة التي تكون في النصوص العادية قاصرة على مساءلة المجرم فيها، لدى قام المشرع بتدارك ذلك سنة 2004[1].

[1] قد اخد المشرع الجزائري بتحيين النصوص والقوانين في مجال الانترنت والمعلوماتية منذ سنة 2004 إثر تعديله لقانون العقوبات، بعد تأثره بما افرزته التكنولوجيات الحديثة للإعلام والاتصال، من أشكال جديدة للإجرام، وهذا بموجب ،القانون (04-15) المؤرخ في 10 نوفمبر 2004 المتتم للأمر (66-156) المتضمن قانون العقوبات، حيث أضاف قسما سابعا مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، فتضمن ثمانية مواد؛ من المادة (394 مكرر) إلى المادة (394 مكرر7)، ونصت فيها على الجرائم التالية:

1–الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات، أو محاولة ذلك (المادة 394 مكرر/1)، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير المعطيات المنظومة (المادة 394 مكرر/2)

2–الدخول أو البقاء المؤدي إلى تخريب نظام تشغيل المنظومة (المادة 394 مكرر/3)

3–إدخال أو إزالة أو تعديل بطريق الغش معطيات نظام المعالجة الآلية (المادة 394 مكرر/1)

4–تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات المخزنة أو المعالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر/2)

5–حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر/2)

مع العلم أنه في حالة استهداف السلوك الإجرامي الدفاع الوطني أو الهيئات والمؤسسات العمومية تضاعف العقوبة (المادة 394 مكرر3)

كما شددت المادة (394 مكرر4) عقوبة الغرامة على الشخص المعنوي، بالإضافة إلى مواد الاشتراك والاتفاق الجنائي وفق المادة 394 مكرر5.

ومن العقوبات التي أقر بها المشرع في تعديل 2004 لقانون العقوبات ما جاءت به المادة (394 مكرر7) بنصها على عقوبة المصادرة التي تنصب على أشياء استعملت أو كانت معدة لاستعمال في ارتكاب الجريمة والأشياء المحصلة منها(1)، والتي تتمثل في مثل هذه الجرائم كما نصت عليه المادة (394 مكرر7) في مصادرة وسائل ارتكاب الجريمة الأجهزة والبرامج بالإضافة إلى إغلاق المواقع محل الجريمة، وهنا المقصود الموقع الإلكتروني (Web site)، أي الموقع الافتراضي زيادة على إغلاق الموقع أو المحل الذي تمت فيه الجريمة.

وبعد فترة ليست بالطويلة، عاد وعدّل المشروع الجزائري في قانون العقوبات، ومن مجمل ما عدّل القسم السابع مكرر الخاص بجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، حيث تم تشديد كل من عقوبة الحبس والغرامة، وهذا بموجب القانون (06-23) المؤرخ في 20 سبتمبر 2006، ربما للانتشار الذي عرفته الإنترنت وبداية استخدامها من كل فئات المجتمع وبالرجوع إلى المصطلح الذي استعمله المشرع الجزائري عند تجريمة السلوكيات المرتبطة بالتكنولوجيا الحديثة للإعلام والاتصال، في البدء استخدم مصطلح المساس بأنظمة المعالجة الآلية للمعطيات ثم في متن النصوص استخدم مصطلح المعطيات والمنظومة المعلوماتية .

على أنّ الذي يجمع هذه الحالات هو الاعتداء على الانترنت ومايتصل بها من معلوماتية او المعلومات المعالجة، وبالتالي،نلاحظ ومن خلال التشريع الجزائري انه قد جمع في محل الاعتداء بين الحق في المعلومات[1] والحق على المعلومات[2] .

المطلب الثاني:سمات جرائم الانترنت.

لم يكن لارتباط جرائم الانترنت بتكنولوجيات الإعلام والاتصال اثر على تمييزها عن باقي الجرائم العادية الأخرى فحسب، بل كان له الأثر الواضح على تمييز المجرم عن غيره من المجرمين الآخرين في جرائم كالفساد أو المخدرات أو السرقة، وغيرها من الجرائم ضد الأموال وضد الأشخاص.أما ضحاياهم فهم من كل الفئات سواء الأطفال أو البالغين وحتى المرضى بالمستشفيات، فهي بكل بساطة جرائم تتم بكل برودة أعصاب وفي الكثير من الأحيان دون أدنى مجهود عضلي لأنها تعتمد على الدراية والمعرفة العلمية، فأي خصائص تميز جرائم الانترنت؟ (الفرع الأول)ومن هم مستخدموها ؟(الفرع الثاني)

الفرع الأول:خصائص جرائم الانترنت

تتميز جرائم الإنترنت بخصائص تجعلها مختلفة عن الجرائم العادية، فهي جرائم تختلف وسيلتها عن الوسائل العادية كالسلاح الأبيض في جريمة القتل ،حتى مرتكبوها يختلفون عن المجرمين الآخرين، واذ سوف يقتصر هذا الفرع على الوسيلة المستخدمة وعالمية الجريمة وصعوبة الإثبات.

أولا:الوسيلة المستخدمة في ارتكابها.

يقرر القانون في كثير من الجرائم وسائل معينة يستخدمها المجرم من أجل ارتكاب الجريمة ،كالسم في جريمة القتل بالسم ،أو السلاح الأبيض وغيرها من الجرائم،ففي جرائم الإنترنت لابد من وجود وسائل معينة للقول أننا أمام جريمة إنترنت ،أو جريمة استخدام غير مشروع للإنترنت .

[1] **الحق في المعلومة**:"حماية المعلومات العامة التي يستفيذ بها الجميع من خلال حماية إتاحتها وتوفيرها للكافة وضمان سلامتها وصحتها حتى يمكن الاستفادة بها وتجرم الأفعال التي من شانها التأثير في هذا الحق" ايمن عبد الله فكري، المرجع السابق، ص13.

[2] **الحق على المعلومات** "حماية تلك المعلومات التي يكون للشخص سواء كان شخصا طبيعيا أو معنويا سلطة أو قدرة أو سيطرة وتحكم عليها لأنها تمثل حق الملكية أو المعلومات خاصة يكون لصاحبها حق عليها ويكون الاعتداء عليها من قبل الغير مجرما ويعاقب عليه، الأمر الذي يهدف إلى حماية تلك المعلومات الخاصة" ايمن عبد الله فكري، المرجع السابق، ص13 .

فعند الحديث عن الوسيلة التي ترتكب بها هذه الجرائم نجد أن الإنترنت عبارة عن استغلال متقدم للحاسب الآلي[1]،فهي بحد ذاتها وسيلة مشروعة ولكن الاستخدام السيئ حرفها عن وظيفتها كوسيلة للاتصال والمعلوماتية، وكذا الحاسبات وأجهزة الربط المودم وحتى البرمجيات المتخصصة للاتصال بالإنترنت أو الشبكة الافتراضية[2]، فهي مشروعة بحد ذاتها ،فأي نشاط إجرامي يحتاج إلى وسيلة هذه الأخيرة التي تكون في معظم الأحيان مشروعة ،فالسلاح الأبيض ليس وسيلة غير مشروعة ولكن حيازتها بدون ترخيص يعد تجريما لحيازة وسيلة، فالنشاط المادي ليس وسيلة وإنما الحيازة غير المشروعة لها[3].

فالوسيلة هي جزء من النشاط التقني والعكس غير صحيح، ولكن هذا لا يعني أن هذه الجرائم جرائم وسيلة، لأن هذه الوسيلة في حد ذاتها تكون عرضة للسلوك الإجرامي، ومن هنا لابد لنا من التفرقة بين النشاط التقني الذي يعني العلم والإدراك باستخدام الإنترنت، والوسيلة التي تعتبر مكونات هذا النشاط التقني، فالبرمجيات مثلا تعد من الوسائل لمباشرة النشاط التقني[4].

إن الوسائل التي تعتمدها جرائم الانترنت قد تكون نفسها محل الاعتداء وبالتالي مسرح الجريمة لا ينحصر في حيز معين، لذلك كلما انتشرت الحواسيب النقالة والهواتف الخلوية كلما أصبحنا وسط عالم لا متناهي يسمى الشبكة الافتراضية،يصعب فيها البحث عن اثر أو أي دليل لتتبع المشتبه فيه لتعدد مسارح الجريمة، لذلك الانترنت تكون في جرائم محل اعتداء وهي الجرائم الحديثة نسبيا، امّا عن باقي الجرائم العادية فإضافة الانترنت كأداة أو و سلية يدخلها في عداد جرائم الانترنت[5].

---

[1] نائلة عادل محمد فريد قورة ،المرجع السابق،ص60.

[2] هي شبكة توفر للمستخدمين الاتصال المحلي والخارجي مع الشبكات الأخرى المتوافقة وغير المتوافقة مع شبكة المستخدم من خلال واجهة تطبيق واحدة سهلة الاستخدام أنظر محمد الربيعي وآخرون ، المرجع السابق، ص341.

[3] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص250.

[4] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص 251.

[5] Solange Ghernaouti-Hélie , La cybercriminalité: le visible et l'invisible, Collection le savoir suisse, 2009,p14

ثانيا:جريمة عابرة للحدود.

إنّ طبيعة الإنترنت وكونها شبكة عالمية جعل من الجرائم التي ترتكب عبرها هي الأخرى ذات طبيعة عالمية عابرة للحدود، ويعنى هذا أن عبورها ليس من قبيل العبور المادي...وإنما الإنترنت عابرة بطبيعتها للحدود الدولية بل أنّ هذا يعدُّ من أهم خصائصها الثابتة[1]،لذلك أصبحت شكلا مستحدثا للجريمة العابرة للحدود، وعليه تعتبر جرائم الإنترنت شكلا جديدا من الجرائم العابرة للحدود الوطنية، والتي لا تعتبر للحدود الجغرافية، مع وجود الحاسب الآلي وشبكات الاتصال أمكن ربط عدد هائل من الحواسب، تمَّ ذلك بأنظمة لا سلكية وأقمار صناعية وألياف بصرية، حيث أصبح أمر الإعلام والاتصال هين .

لذلك تعتبر جرائم الانترنت نمط جديد من الجرائم العابرة للحدود الوطنية، لذلك تقوم أجهزة كالانتربول عن طريق موظفيها عبر العالم بتوفير قاعدة بيانات يمكن من خلالها التصدي لهذه الجرائم ومكافحتها[2].

قد اكتسبت هذه الجرائم طابعا دوليا، حيث أصبحت متعدية الحدود،فمثلا جريمة اختراق المواقع يكون مرتكبها عادة في دولة معينة ،فيقوم باختراق موقع معين أو أي نظام معلوماتي، وقد يكون هذا الاختراق في دولة واحدة أو ضمن عدة دول دون أن يعبر الحدود المادية الواقعية،كما هو عليه الحال في جرائم تبييض الأموال والمخدرات .

كذلك هو الحال بالنسبة لجرائم نشر الفيروسات ،فمن يعمل على تصميم البرامج الخبيثة،فإن سلوكه الإجرامي يصيب كل الأجهزة الموصولة بشبكة الإنترنت سواء الأجهزة الموجودة داخل الدولة التي يقيم بها أو خارجها،حيث تجتمع الصفتين في جرائم الإنترنت باعتبارها وطنية عابرة للحدود ،مما يؤدي بالضرورة إلى خضوعها لأكثر من قانون جنائي.

ثالثا:صعوبة اكتشاف والإثبات الجنائي.

إنّ الكثير من جرائم الانترنت لا يعلم بوقوعها أصلا، وحتى وان تم اكتشافها يصعب إثباتها وذلك في ظل غياب الحدود الجغرافية، وسهولة استخدام الانترنت مقابل تكلفة بسيطة بالمقارنة مع وسائل اتصال أخرى.

[1] عمر محمد أبو بكر بن يونس،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص250.

[2] عبد الله حسين محمود، المرجع السابق،361-362.

أ–صعوبة اكتشاف جرائم الانترنت

عادة ما تكتشف هذه الجرائم عن طريق الصدفة البحتة، ذلك لأنّها لا تترك أثارا حيث يعود السبب إلى عدم ترك اثر مادي ملموس، بالإضافة إلى قدرة المجرم على محو دليلا لإدانة بشكل سريع مما يشكل عائقا إضافيا لصعوبة الاكتشاف[1].

حيث انّ الجريمة الالكترونية في أكثر صورها لا يلحظها المجني عليه وهذا راجع إلى الخبرة والمعرفة التي يتمتع بها المجرم المعلوماتي[2]، ومن ناحية أخرى يلعب المجني عليها و الضحية دورا مهما في صعوبة اكتشافا لجريمة أو حتى وقوعها، وهذا بعد تحفظ الجهات التي تم الاعتداء عليها، عن الإبلاغ وذلك بان تتخذ ماهو مناسب من إجراءات أمنية داخل منظومتها دون أن تبلغ السلطات المختصة وهذا خوفا على سمعتها، وخصوصا المؤسسات المالية[3]،وبالضرورة فان صعوبة الاكتشاف تؤدي إلى صعوبة الإثبات.

ب–صعوبة الإثبات في جرائم الانترنت.

حتى وان تم اكتشاف وقوع الجريمة من جرائم الانترنت، والإبلاغ عنها فانّ إثباتها ليس بالأمر الهين، والذي يحيطه الكثير من الصعاب وهذا لوجود مسرح لامادي، مما يزيد من تعقيد عملية البحث والتحري، ذلك أنّ المعطيات هي عبارة عن نبضات غير مرئية مما يجعل أمر محو الدليل أمر كليا أمر غير مستحيل[4] .

ولما كان مسرح الجريمة الالكترونية مسرحاً غير مادي، لا يمكن استنباط الأدلة منه لعدم وجود أثار مادية فان دوره في إثبات الجريمة يتضاءل شيئا فشيئا وهذا لكون جرائم الانترنت لا تترك أثار مادية بالإضافة إلى أنّ مسرح الالكتروني يدخل الآلاف بل لا نبالغ إذا قلنا الملايين خلال نفس الوقت وقوع الجريمة وعدة جرائم[5].ومن حين وقوعها إلى اكتشافها إلى الإبلاغ عنها والتحري عنها فترة من الزمن كفيلة بتغير معالم الدليل بعد أنْ يعبث بها المجرم نفسه.

---

[1] جميل عبد الباقي الصغير، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، مصر، ص17.

[2] هشام محمد فريد رستم، الجوانب الإجرامية للجوانب المعلوماتية،مجلة الأمن والقانون، العدد الثاني،كلية شرطة دبي، الامارات العربية المتحدة،ص16.

[3] هشام محمد فريد رستم، الجوانب الإجرامية للجوانب المعلوماتية ،المرجع السابق، ص25و26.

[4] هشام محمد فريد رستم، الجوانب الإجرامية للجوانب المعلوماتية،المرجع السابق،ص23.

[5] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت،المرجع السابق،ص95.

الفرع الثاني: مستخدم الانترنت.

يلج الانترنت يوميا ملايين الأشخاص، الصالح منه و غيره، و باختلاف هؤلاء تختلف الأدوار و تتنوع بين مجرم و ضحية، فمستخدم الانترنت هو شخص يتصل بالمواقع الالكترونية، إما للحصول على معلومات إخبارية أو صحية أو ثقافية، أوسياسية أو اجتماعية أو غيرها، سواء كان شخص مهني أو متمرس،فالمستخدم قد يكون الضحية أو مجرم الانترنت –التقني- ومزود خدمة الانترنت ؛وبين هذا و ذاك فسنعتمد على مصلح مستخدم الانترنت مرادفا لضحية جرائم الانترنت، ولكن السؤال التي يتبادر للدهن من هم ضحايا جرائم الانترنت؟.

الجواب بسيط كل شخص دون استثناء، سواء كان مستخدما عادي للانترنت، أو مزود لخدمات الانترنت، أو أي شخص طبيعي أو معنوي كالشركات والمؤسسات، وحتى الدول والحكومات ،دون أن ننسى غير المستخدم للانترنت ،لأّن بياناته الشخصية تم رقمنتها، فهو معرض لأي سلوك إجرامي حتى دون علمه.

على أنْ يُقتصر في الدراسة على الضحية(أولا) ومجرم الانترنت(ثانيا) في هذا الفصل

أولا:الضحية أو المجني عليه.

بتعدد أصنـــاف المجرم قد يتعدد أصناف الضحايا، ولكن ليس بقدر تعدد المجـرم المعلومـــاتي، فالضحية قد يكون شخص طبيعي أو معنوي.

فيمكن أن يكون الضحية فرد عادي في المجتمع أو مؤسسة اقتصادية كشركات التامين، أما الأخطر فهو أن تكون بالدولة أو الواقعة في المجال العسكري من خلال عملية التجسس[1]، والتي لم يغفل عنها المشرع الجزائري، وشملها بإجراءات خاصة للوقاية من جرائم تكنولوجيات الإعلام والاتصال، أي إجراء مراقبة الاتصالات الالكترونية باعتبارها إجراءا وقائيا في إطار الضبط الإداري

[1] جلال محمد الزعبي و اسامة احمد مناعسة ،جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة، دار الثقافة،عمان الاردن،2010،1431،ص77.

وهذا بموجب المادة (04) من القانون(09-04) والتي سوف نتطرق لها في سياق الفصل الأول من الباب الثاني.

بالعودة إلى المجني عليه أو الضحية، لابد لنا من توضيح مصطلح مستخدم الانترنت، بالإضافة إلى توضيح أنّ المجني عليه كما قلنا سابقا قد يكون شخص عادي أو معنوي، وحتى مقدم خدمات الانترنت نفسه بمختلف أنواعه بحسب الخدمات التي يقدمها.

الضحية أو المجني عليه، يكون غالبا دوره سلبي جدا أمام تكتم العديد وخوفهم على سمعتهم، لذلك فهم يحجمون عن الإبلاغ، أما إذا كان المجني عليه و الضحية مؤسسة اقتصادية تجارية استثمارية ،فالأكيد أنها لن تفضح نفسها ،في حالة اختراق موقعها الالكتروني، لوجود ثغرة أمنية أو سرقة كلمات السر أو فك التشفير وغيرها من أساليب ارتكاب الجريمة، ولن يقوم بذلك حتى مقدم الخدمات، إلاّ في حالات معينة لكي تعفيه من المسؤولية القانونية، وبالتالي فان الخوف على السمعة وثقة العملاء ،يؤدي حتما إلى العزوف عن الإبلاغ حيث أنّ الصدفة تلعب دورا في كشف الجرائم خصوصا في البلدان النامية[1].

وقد حدد الإعلان العالمي الخاص بالمبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة الذي اعتمدته الجمعية العامة للأمم المتحدة بقرارها رقم 401434 الصـادر بتاريخ 29-11-1985 تعريف الضحية "ويقصد به الأشخاص الذين أصيبوا بضرر فردي أو جماعي بما في ذلك الضرر البدني أو العقلي أو المعاناة النفسية أو الخسارة الاقتصادية أو الحرمان بدرجة كبيرة من التمتع بحقوق أساسية، عن طريق أفعال أو حالات إهمال تشكل انتهاكا لقوانين جنائية نافذة في الدول بما فيها القوانين التي تحرم الإساءة لاستعمال السلطة كما يشمل المصطلح

[1] جلال محمد الزعبي المرجع السابق،ص78.

أيضا حسب الاقتضاء العائلة المباشرة للضحية الأصلية أو فاعليها المباشرين والأشخاص الذين أصيبوا بضرر جراء التدخل لمساعدة الضحايا في محنتهم أو لمنع الإيذاء"[1].

وعليه فان الضحية في جرائم الانترنت وفي الجريمة بصفة عامة قد يكون شخصاً طبيعيً، أو شخصاً معنوياً أُنتهِك حق من حقوقه المحمية قانونا ، فلحقه جراء ذلك ضرر معنوي أو مادي، مع الملاحظ أنّ هذه الضحية أو المجني عليه قد يكون سبباً في ارتكاب السلوك الإجرامي، إمّا لجهله بالجريمة وارتكابها، أولعدم احتياطه في أخد تدابير الحماية الأمنية اللّازمة لمنظومته المعلوماتية،او حتى بسبب عدم القيام او التخاذل في واجب الرقابة والتوجيه لأطفاله حين استخدام الشبكة وباقي الأجهزة المتصل بها،في حين يشترك الضحية كشخص طبيعي أو معنوي في أنّ العديد منهم يحجمون عن الإبلاغ عند وقوع جريمة من جرائم الانترنت وهذا خوفا على السمعة والشرف والاعتبار،إذا كانت الضحية شخص طبيعي ، أمّا الشخص المعنوي فيحرص على أنْ لا تمّس سمعته المالية والاقتصادية أي شيء، حتى ولو أخفى أضرار مالية بالغة عن اختراق نظامه الأمني أو التلاعب ببيانات عملائه.

ثانيا:مجرم الانترنت.

يعد مجرم الانترنت أهم الفاعلين في جريمة الانترنت، باعتباره يجمع بين جرائم الانترنت التي قد تكون فيها هذه الأخيرة، إمّا وسيلة أو محل للجريمة، ولن نستعمل مصطلح مجرم تقني-يستخدم هذا المصطلح عندما يتعلق الأمر بالجرائم التقنية التي تعتبر نوعاً من جرائم الانترنت- لان المجرم التقني متعلق بجميع المجرمين في اختصاص التقنية حتى وان كانت غير متعلقة بتكنولوجيات الإعلام

[1] يرجى الاطلاع على مرفق الاعلان العالمي الخاص بالمبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة ، اعتمد ونشر بموجب قرار الجمعية العامة للامم المتحدة رقم 40 /34 المؤرخ بتاريخ 29-11-1985 (وثيقة الامم المتحدة رقم 34 /40 /A /RES)،ص320.

https://documents-dds- ny.un.org/doc/RESOLUTION/GEN/NR0/472/21/IMG/NR047221.pdf?OpenElement

والاتصال ، على أنّ مصطلح مجرم الانترنت في المؤلفات هو مرادف لمصطلح مجرم المعلوماتي، ولهما نفس المعنى.

إنّ ظهور مجرم الانترنت كما يطلق عليه البعض المجرم المعلوماتي، هو ظاهرة جديدة وبالتالي فكرة جديدة في الفقه الجنائي وعلم الإجرام[1] وحتى علم النفس الجنائي[2]، حيث انّه يختلف عن الجاني في جرائم القتل، والموظف المرتشي في جرائم الفساد، و لكن مجرم ذو مهارات تقنية عالية ملم بالتقنية، المستخدمة في المنظومة المعلوماتية، و قادرا على استخدام العديد من الطرق أبرزها الاختراق[3].

إنّ شخصية مجرم الانترنت وتقنية ارتكابه للجرائم، من أهم الخصائص التي اتصفت بها جرائم الانترنت، التي أضحت يوما بعد يوم تضيف إلى قائمة المجرمين أصنافاً جديدة ،بعدما كانت مقتصرة فقط على ذوي الكفاءات العلمية والتقنيةالعارفين بالتكنولوجيات الحديثة، هذه التكنولوجيا التي دللت الصعاب وأبرزت للوجود فئة جديدة من الجانحين الصغار،ضف إلى ذلك أنّ معظم مجرمي الانترنت لا يأبهون –ليس الكل– للمردود المادي في مقابل استمتاعهم والاحتفال بانتصاراتهم جراء كسر أو تجاوز الحماية الأمنية أو ما يعرف بأمن المعلومات[4]، عن طريق تجاوز

[1] علم الإجرام:العلم الذي يدرس الجريمة باعتبارها ظاهرة اجتماعية، بما يستهدف وصفها وتحليلها وتقصي اسبابها، أو الفرع من العلوم الجنائية الذي يدرس الجاني ومشاكله ويدرس الموقف الإجرامي بعناصره المختلفة دراسة واقعية تجريبية محاولا الوصول إلى تحليل ظاهرة الجريمة التي تدور حولها أحكام القانون الجنائي تحليلا علميا.عمار عباس الحسيني،مبادئ علمي الاجرام والعقاب،ط1،منشورات الحليبي الحقوقية،بيروت ،لبنان،2013،ص18.

[2] علم النفس الجنائي:علم يدرس العوامل النفسية من خلال نظريات المذهب النفسي وعلم الاجتماع الجنائي،أكرم نشأت إبراهيم،علم النفس الجنائي،مكتبة دار الثقافة للنشر والتوزيع،عمان الاردن،1996،ص5.

[3] الاختراق:هو طريق لارتكاب جرائم الانترنت والخاصة بالجرائم التقنية ،سوف يتم تعريفه في المبحث الموالي في إطار الركن المادي لجريمة الدخول والبقاء إلى المنظومة المعلوماتية.

[4] امن المعلومات:علم امن المعلومات "هو علم يعنى بدراسته تدابير حماية وسلامة وتوافر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها سامح احمدالبلتاجي موسى،المرجع السابق،ص383.

الثغرات الأمنية، وهو ما يدعو إلى دراسته ومعرفة فئاته من خلال تعريف مجرم الانترنت، و أصناف مجرمي الانترنت .

أ-تعريف مجرم الانترنت.

نتعرف من خلال هذا الفرع على مفهوم مجرم الانترنت و الخصائص التي ينفرد بها عن المجرم في غير جرائم الانترنت و ذلك كما يلي:

1- مجرم الانترنت.

الأصل أنّ المصطلح الذي أُطلق على مجرم تكنولوجيات الإعلام والاتصال، في تطور مستمر فهناك مجرم الانترنت و مجرم الحاسوب، واللذان يشكلان معا المجرم التقني، هذا المجرم الذي يستعمل التقنية من اجل ارتكاب جرائمه، أي تقنية المعلومات، وهو يختلف عن مجرم الانترنت هذا الأخير الذي لا يتمتع بمدارك علمية وتخصصية، في معظم الأحيان بل مداركه بسيطة وهذا راجع إلى السهولة في استخدام التقنية التي أتاحتها الانترنت[1]، أطلق مصطلح "هاكر" في أول الستينيات من القرن الماضي على المبرمج الماهر القادر على التعامل مع الحاسب الآلي و مشاكله بخبرة و دراية و يطلق خبراء امن المعلوماتية الالكترونية مصطلح "هاكر"[2] على من يخترق الحاسب الآلي و مصطلح "كراكرز" على الفئة التي لديها قدرة على الاختراق[1].

---

[1] عمر محمد بن يونس أبو بكر،المرجع السابق،ص 233-234.

[2] يعود الفضل في الكشف عن مصطلح الهاكر الى كاتب الخيال العلمي وليام جيبسون في مؤلفه the neu-romancer الذي أصدره 1984، Cybercriminalité et contrefaçonEric Przysw,a FYP editions, 2010,p17، حيث انه كان يقدم حلولا لمشاكل البرمجة بشكل تطوعي في زمن لم يكن برامج (Windows) قد ظهرت، هاكر ، و تعني الملم بالبرمجة و مقدم الخدمة للآخرين ، و في زمن عددهم لا يتجاوز بضع ألوف على مستوى العالم . كما تستخدم وسائل الإعلام مصطلح "هاكرز" على إطلاقها دون تمييز بين الصالح و الطالح. يعتبر "هاكرز" في تلك الفترة من الزمان عباقرة في البرمجة فهو المبرمج الذي يقوم بتصميم أسرع البرامج الخالية من المشاكل و العيوب التي تعيق البرنامج عن القيام بدورة المطلوب منه ، و من أشهر الهاكرز في تلك الفترة من الزمان ، "دينيس ريتش" و "كين طومسون" اللذان نجحا في أواخر الستينات في إخراج برنامج ليونيكس ، لذلك فمن الأفضل عدم إطلاق مصطلح الهاكرز على الأشخاص الذين يدخلون عنوة إلى الأنظمة بقصد التخريب أو التطفل.، و من أشهر مجرمين التقنية ،روبرت موريس (أمريكي الجنسية)، و فلاديمير لوفين (روسي الجنسية)، و كيفين ميتينيك (أمريكي الجنسية)

إلاّ انّه وبالنظر إلى أنّ الانترنت وسيلة جمعت بين تقنيتي الإعلام والاتصال، فانّه لا يمكن بأي حال من الأحوال أن نسلم أنّ مجرم الانترنت، هو فقط المجرم البسيط الذي لا يتمتع بأي مدارك، فمجرد استعمال للمنظومة المعلوماتية أو الهاتف النقال بأبسط التطبيقات هو شيئ تقني مكتسب، لا يرقى طبعا لتقنيات الاختراق وزرع القنابل المنطقية، لذلك فان اعتمدنا مفهوم مجرم الانترنت البسيط فإننا سوف نسقط من إجمالي هذا المصطلح مجرمي الجرائم التقنية البحتة،فمجرم الانترنت هو المجرم الذي يتمتع بمدارك تدرج من البسيطة إلى اعلي الدرجات في التحكم بالتقنية المعلوماتية ،يتمتع بمجموعة من الخصائص، وبالتالي ترجع الصعوبة في تحديد خصائص معينة للمجرم المعلوماتي أو مجرم الانترنت،او المجرم التقني إلى تعدد جرائم الانترنت وتنوعها، حيث أصبحت بلا منازع تغطي كل مجالات الحياة دون استثناء[2]، الأمنية والعسكرية والاقتصادية والاجتماعية وغيرها.

2-خصائص مجرم الانترنت:

إنّ جرائم الانترنت بصفة خاصة ، و إن كان يتميز ببعض السمات الخاصة إلا انّه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه [3]، وشانها شان باقي المجرمين قد يمارس سلوكه الإجرامي، منفردا أو داخل الجماعة، ومع التطور التكنولوجي والتقني أفرزت كما ذكرنا عدة أصناف من مجرمي الانترنت،تجمع بينهم صفات مشتركة[4].

، و ديفيد سميث (أمريكي الجنسية).لمزيد من التفاصيل انظر:ايمن عبد الله فكري ،المرجع السابق،ص109.و مصطفى محمد موسى،التحقيق الجنائي في الجرائم الالكترونية،مطابع الشرطة –شارع المرور-الدراسة-القاهرة،مصر،2009،ص154،سامي محمد الشوا،المرجع السابق،ص48،51 و عبد الحكيم رشيد توبه، المرجع السابق.ص156.

[1] مصطفى محمد موسى،التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق،ص143.

[2] غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة ، مصر 2010، ص13.

[3] نائلة عادل محمد فريد قورة، المرجع السابق ،ص57

[4] يتميز المجرم التقني بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين، و يرمز إليها الأستاذ Parker بكلمة SKRAMوهي تعني المهارة Skills، المعرفة Knowledge، الوسيلة Resources، السلطة Authority، و أخيرا الباعث، Motivies هامش Parker (DonnB.) Op.cit .p.136-138مشار اليه ادى نائلة عادل محمد فريد قورة، المرجع السابق.ص57.

-السمات المشتركة بين جميع فئات مرتكبي جرائم الانترنت:

تتوافر لدى هؤلاء أو معظمهم مجموعة من الخصائص و السمات تميزهم عن غيرهم من المتورطين في أشكال الانحراف و الإجرام الأخرى، تتمثل تلك السمات المشتركة بين جميع فئات مرتكبي تلك الجرائم فيما يلي:

-السن:

الواقع إنّ سن الرشد الجنائي الذي حدده المشرع الجزائري، والمقدر بثمانية عشر سنة، قد لا يكون سنا مرجعيا في جرائم الانترنت، فقد صادفنا في الواقع أطفال لم يتجاوز سنهم ثمانية سنوات مهويسين بالتقنية، يملكون من المهارات ما لا يملكها أباؤهم، لدى فمن المنطقي أن يعيد المشرع الجزائري النظر في الأهلية الجنائية خصوصا ما تعلق منها بجرائم الانترنت، ذلك حتى أن العقوبات المخففة أو التوبيخ، في اعتقادنا لا يفي بالغرض في مثل هذه الحالات لانّ الهدف من العقوبة هو الردع، وما يردع مجرم التقنية هو ابعاده وحرمانه منها.

-الذكاء :

يعتبر الذكاء من أهم صفات مرتكبي جرائم الانترنت سابقا(ليس الذكاء من اهم سمات مجرمي الانترنت الان بل هو خاص ببعض أنواع هذه الجرائم على رأسها الجرائم التقنية)، لانّ ذلك يتطلب منه المعرفة العلمية لكيفية الدخول إلى المنظومة المعلوماتية والعبث فيها التعديل و التغيير في البرمجيات والتطبيقات، فجرائم الانترنت أو جرائم تكنولوجيات الإعلام والاتصال، بالمقارنة بالجرائم التقليدية أو العادية التي تكون عنيفة في الكثير من الأحيان[1].

[1] محمد سامي الشوا،المرجع السابق.ص49.

-متكيف اجتماعيا:

إنّ السلوكيات الإجرامية التي يرتكبها مجرم الانترنت مسرحها العالم الافتراضي، وما يميزه من صفات كونه افتراضي لا مادي لا محسوس، ويتميز مجرم الانترنت بتكيفه مع المجتمع، بمعنى انّه أصلا عضو في المجتمع وليس منبوذا أبدا من طرفه،لانّ مجرم الانترنت، مجرم غير عنيف، ذلك انه ينتمي إلى إجرام الحيلة للقيام به، شخص ذو مهارات ، ولكن اذا كان الإجرام إذا كان في شكل جماعات، يكون أكثر تنظيما وتخطيطا، وتطور في السلوك الإجرامي وهذا لوجود المجرم في جماعة.

على عكس تاجر المخدرات أو الموظف المرتشي أو السارق والذي عادة –ليس في كل الأحيان– تظهر عليه بعض الصفات التي تدل على ميوله الإجرامية، فقد يكون السارق من أهل المنزل ولكن لا يتفطن إليه احد[1].

-المعرفة:

ينتمي مرتكب هذه الجرائم عادة إلى دوي المعرفة العلمية العالية، وأول ظهور له كان في الشركات والمؤسسات، وعادة ما يكون هؤلاء محل ثقة مدرائهم الذين لا يفقهون شيئا،في خبايا المنظومة المعلوماتية والشبكات،ولكن وكما ذكرنا سابقا المعرفة العلمية المعتبرة هي معرفة الحد الأدنى من تشغيل أي وسيلة للوصول إلى الانترنت، لان تكنولوجيات الإعلام والاتصال هي التي سهلت الاستخدام وجعلت الحد الأدنى من المعرفة يكفي لظهور الجريمة وإمكانية ارتكابها[2].

[1] على عكس المجرم الانترنت ، ولو أننا نسجل فرق بين مجرم الانترنت في الجرائم التقنية ومجرم الانترنت في باقي جرائم الانترنت، فمجرم الانترنت في الجرائم التقنية يتطلب منه تفرغ ووقت طويل في دراسة الثغرات الأمنية والاختراق ونشر الفيروسات ، مما يجعله منعزلا عن محيطه امّا في غير الجرائم التقنية فالمجرم يكون اجتماعيا جدا، حتى انه يستخدم المعلومات التي يعرفها عن الأشخاص ثم ينشرها في العالم الافتراضي، أو يستخدم كلمات السر التي يبوح بها الضحية عن حسن نية مما يستخدمها المجرم في استفزاز الضحية،كما تنشا علاقات مع المجرم علا قات حتى على المستوى الدولي ، فيقوم باستثمار المعرفة والتقدم العلمي هشام محمد فريد رستم، قانون العقوبات ومخاطر التقنية ، المرجع السابق، ص42و.43

[2] جلال محمد الزعبي و اسامة احمد المناعسة، المرجع السابق،ص.70

انّ مجرم الانترنت مجرم متخصص[1]، فقد ثبت في العديد من القضايا انّ عددا من المجرمين لا يرتكبون سوى جرائم الانترنت، أي أنهم متخصصون في هذا النوع[2]،لذلك هو مجرم عائد إلى الإجرام، أي انّه دائما في حالة عود، وهذا لسهولة إتيان السلوك الإجرامي، وصعوبة اكتشافها، حيث يعود الكثير من مجرمي الانترنت إلى ارتكاب جرائم على الانترنت، وهذا لسد الثغرات التي أدت إلى التعرف عليهم، فمجرم الانترنت، مجرم محترف، ذلك انّه لا يسهل على الشخص المبتدى سوى في حالات قليلة، أن يرتكب جرائمه عن طريق الانترنت، أيا كانت وسيلة الولوج. فالأمر يقتضى الكثير من الدقة و التخصيص في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية الأنظمة المعلوماتية[3].

-التخفي:

معظم مرتكبي جرائم الانترنت ، يختفون تحت أسماء وهمية أو مستعارة خشية ملاحقتهم عند تسجيل بياناتهم الشخصية للحصول على بريد الكتروني أو الدخول إلى مواقع على الشبكة، لذلك لابد من اتجاه القوانين الدولية والإقليمية لضرورة التعاون الدولي، والتوقيع بروتوكولات ثنائية لتسليم المجرمين والتعاون القضائي في إطار المعاملة بالمثل[4].

ب-تصنيف مجرمي الانترنت.

إن دراسات علم الإجرام الحديثة في مواد جرائم الانترنت أو الإجرام المتصل بتكنولوجيات الإعلام والاتصال، تسعى إلى إيجاد تصنيف لمجرمي الانترنت لكنها تجد صعوبة في تحقيق ذلك، ومرجعه إلى التطور السريع في المنظومة المعلوماتية والشبكات وكذا الوسائل المستخدمة في الوصول

[1] عبد الفتاح بيومي حجازي ، مبادئ الاجراءات الجنائية ،المرجع السابق ،ص45.

[2] غنام محمد غنام، المرجع السابق، ص14.

[3] عبد الفتاح بيومي حجازي ، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، المرجع السابق،ص 46.

[4] وهذا ماجسده القانون الجزائري و بالضبط القانون(09-04) في الفصل السادس

إليها، فاختلاف الوسائل أدى إلى اختلاف الجرائم، واختلاف أصناف المجرمين[1] ، لدلك فان هناك شبه إجماع على جمع جميع أصناف المجرمين تحت تسمية واحدة المجرم التقني[2]، ذلك أنّ الانترنت لم تعد مجرد شبكة، بل تطورت وأصبحت تجمع بين الحوسبة والتقنية ، وأصبحت وجهين لعملة واحد الأول هو الاتصال والثاني الإعلام.

هناك عدة محاولات قام به الفقه لتصنيف مجرمي الانترنت سنذكر أهمها كما يلي وقبلها هناك من المحاولات الفقهية التي صنفت على أساس السن أو الخطورة الإجرامية أو حتى تبني تصنيفات المؤلفين الأجانب وأعطوها عنوان أفضل التصنيفات لمجرمي الانترنت[3]، ولكن بالرغم من كل التصنيفات والمعايير المعتمدة عليها فالمجرم يبقى مجرما يستوجب المساءلة الجنائية.

يمكن تقسيم مجرمي التقنية الى ثلاثة فئات: المخترقون ، و المحترفون ، و الحاقدون ، كما ان من التصنيفات الهامة، التمييز بين صغار السن من مجرمي الانترنت و بين البالغين الذين يتجهون للعمل معا لتكوين المنظمات الإجرامية الخطرة .

1-المخترقون أو المتطفلون :

هذا النوع لا تختلف عن طائفة هاكرز، فالهاكرز متطفلون يتحّدون إجراءات امن النظم و الشبكات، لكن لا تتوافر لديهم في الغالب دوافع إجرامية، و إنّما دوافع التحدي و إثبات المقدرة أمّا الكراكرز، فانّ اعتداءاتهم تعكس ميولهم الإجرامي ورغبتهم في ارتكاب الجريمة[4].

[1] يونس عرب ،جرائم الكمبيوتر والانترنت، منشورعلى الموقع التالي:
http://www.arablaw.org/Download/CyberCrimes_WorkPaper.doc تاريخ الاطلاع 03-03-2015.

[2] سامي محمد الشوا،المرجع السابق،ص 51 ونائلة قورة،المرجع السابق،ص56-61.

[3] ايمن عبد الله فكري، المرجع السابق، ص 107.

[4] ايمن عبد الله فكري، المرجع السابق،109.

2-مجرمو الكمبيوتر المحترفون

تتميز هذه الطائفة بالخبرة الواسعة، والمهارات التقنية، كما تتميز بالتنظيم و التخطيط لدى، فانّ هذه الطائفة تعد الأخطر من بين مجرمي التقنية؛ حيث تهدف لتحقيق الربح المادي لحسابها أو لغيرها،و يتم تصنيف أفراد هذه الطائفة إلى مجموعات متعددة إما تبعا لتخصصهم بنوع معين من الجرائم او تبعا للوسيلة المتبعة من قبلهم في ارتكاب الجرائم[1].

3-الحاقدون:

هذه الفئة لا تسعى إلى أي هدف مما ترجوه باقي الطائفتين، ولكن ما يحكم إرادتها الحرة الانتقام، والذي لا يعدو أن يكون دافعاً إجرامياً. و لهذا فإنهم ينقسمون إمَّا إلى مستخدمي للنظام بوصفهم موظفين أو مشتركين أو على علاقة ما بالنظام المعلوماتي محل الجريمة،وإلى أشخاص خارج النظام تتوفر لديهم أسباب الانتقام من الشخص المعنوي المستهدف .

كما يمكن تصنيف أولئك المجرمين بحسب السن الى:

4-طائفة صغار السن:

من الملفت للانتباه أن جرائم الانترنت، لم تعد قاصرة على الفئات المتخصصة ممن لهم دراية واسعة بالتقنية، بل برز للوجود طائفة جديدة وهم صغار النوابغ يوصفون بالشباب البالغ المفتونون بالمعلوماتية والحاسبات الآلية[2].وهي الفئة التي تشكل وسوف تشكل إشكال قانوني فيما يخص المسؤولية الجزائية،و يثير صغار النوابغ جدلا واسعا، حول إسباغ الصفة التجريمة عليهم وبالتالي مساءلتهم جزائيا[3].

---

[1] حاتم عبد الرحمان منصور ، الإجرام المعلوماتي، ط1،دار النهضة العربية،مصر ،2002،ص96-98 مرجع مشار اليه لدى ايمن عبد الله فكري، المرجع السابق،ص110.

[2] محمد سامي الشوا، المرجع السابق،ص52.

[3] يمكن رد الاتجاهات الفقهية التي تعرضت لذلك الى ثلاث اتجاهات:

5-المجرمون البالغون أومحترفو الإجرام:

إنّ مرتكبي جرائم الانترنت عموما ، ينتمون وفق الدراسات إلى فئة عمرية تتراوح بين (25-35) عاما[1]، و بالتالي يمتاز مرتكبو هذه الجرائم بصفات الشباب العمرية و الاجتماعية ، و إذا استثنينا صغار السن من بينهم ، الذين تكون أعمارهم دون الحد الأدنى المشار إليه[2].

-الاتجاه الأول: لا يرى إسباغ أي صفة تجريميه على هذه الفئة ، أو على الأفعال التي تقوم بها ، و لا يرى وجوب تصنيفهم ضمن الطوائف الإجرامية لمجرمي الانترنت، استنادا إلى أن صغار السن " لديهم ببساطة ميل للمغامرة و التحدي ، و الرغبة في الاكتشاف".لا توجب معاقبتهم.

-الاتجاه الثاني: الذي يحتفي بهذه الفئة و يناصرها و يعتبرها ممن يقدم الخدمة لأمن المعلومات و وسائل الحماية و يصفهم أحيانا بالأبطال الشعبيين

-الاتجاه الثالث: يرى أن مرتكبي الجرائم الانترنت من هذه الطائفة ، يصنفون ضمن مجرمي الانترنت كغيرهم دون تمييز استنادا إلى أن تحديد الحد الفاصل بين العبث في المنظومة المعلوماتية والشبكات و بين الجريمة أمر عسير من جهة ، و دون اثر على وصف الفعل – قانونا- من جهة أخرى ، و استنادا إلى أن خطورة أفعالهم التي تتميز بانتهاك الأنظمة و اختراق الحواسب و الانترنت و تجاوز إجراءات الأمن ، و التي تعد بحق من أكثر جرائم الانترنت تعقيدا من الوجهة التقنية ، عوضا عن نتائجها الخطيرة،وهي الظاهرة التي تفشت ولكن ومع تحديد سن الرشد الجنائي فانه لا يمكن اعتبار هؤلاء مجرمين مما يدعو إلى تدخل المشرع الجزائري إلى إعادة النظر في سن الجنائي من جهة ونوع العقوبات المقررة لمثل هذه الجرائم. محمد سامي الشوا، المرجع السابق، ص8 وهشام فريد رستم، قانون العقوبات....،المرجع السابق،ص43، يونس عرب، http://www.arablaw.org/Download/CyberCrimes_General.doc

[1] يرجى الاطلاع على الملحق1،ص335.

[2] محمد سامي الشوا، المرجع السابق،ص54.

المبحث الثاني:صور جرائم الانترنت في التشريع الجزائري

يهدف الإثبات الجنائي -كما ذكر سلفا- إلى إثبات وقوع الجريمة، وتحديدا إثبات قيام أركانها، -الركن الشرعي والمادي والمعنوي -وكل ما يلحقها من ظروف وأعذار في جميع مراحل السلوك الإجرامي على نحو يقود حتما إلى التعرف على المجرم، وتوجيه الاتهام إلى المشتبه فيه، والحقيقة أنّ التطرق بشيء من التفصيل في هذه الجرائم يسعى إلى بيان، أهم ركنين المادي والمعنوي واختلافها عن الجرائم الأخرى، مما يصعب عملية الإثبات ويجعله إشكالية مطروحة.

ولقد أشار القانون(09- 04)[1]لجرائم تكنولوجيات الإعلام والاتصال في عدة صور تندرج ضمن جرائم المساس بالأنظمة المعالجة الآلية للمعطيات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

ويلاحظ أن جرائم الانترنت يمكن تقسيمها إلى صنفان، يتمثل الصنف الأول في الجرائم التقنية، والتي عبر عنها المشرع بجرائم المساس بالأنظمة المعالجة الآلية للمعطيات أو ما يعرف بالإجرام المعلوماتي عبر الشبكة. أمّا الصنف الثاني فيشمل باقي الجرائم التي ترتكب بواسطة الانترنت، أو ما يعرف بالإجرام غير المعلوماتي، وهي كل الجرائم العادية التي ترتكب عبر شبكة الانترنت أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

وعلى هذا النحو سيتم التطرق في إطار هذا المبحث فقط إلى صور جرائم الانترنت التي أوردها المشرع الجزائري والمتمثلة في الجرائم التقنية (المطلب الأول)، ثم الجرائم التي ذكر فيها المشرع صراحة مصطلح "المعلوماتية أوتكنولوجيات الإعلام والاتصال" أي ما تعلق بالأنترنت، وتحديدا جريمة الإرهاب الالكتروني وجريمة إهانة رئيس الجمهورية (المطلب الثاني).

[1] طبقا لنص المادة(02) من القانون(09-04).

المطلب الأول: الجرائم التقنية في التشريع الجزائري.

عبر المشرع الجزائري عن الجرائم التقنية بجرائم المساس بالأنظمة المعالجة الآلية للمعطيات، وهي جرائم تتحد مع بعضها في العديد من الأحكام المشتركة (الفرع الأول)، وتجد صورها كما أوردها المشرع الجزائري في جريمتي الدخول والبقاء (الفرع الثاني).

الفرع الأول: الأحكام المشتركة للجرائم التقنية.

الجرائم التقنية هي أول ما استهل به المشرع الجزائري تجريمه للظواهر غير المشروعة المرتبطة بالانترنت، والتي يطلق عليها جرائم الغش المعلوماتي، وهي بدورها تأخذ صورتين، الأولى الدخول في منظومة معلوماتية والصورة الثانية المساس بمنظومة معلوماتية، وتعتمد الأحكام المشتركة للجرائم التقنية بالأساس، على تجريم الشروع والاتفاق الجنائي بالإضافة للظروف المشددة، والتي استهدفت بالدرجة الأولى الجرائم التي تمس بالأمن الوطني والسيادة الوطنية، زيادة على تجريم السلوكيات المرتبطة بالشخص المعنوي .

أولا: الاتفاق الجنائي في الجرائم التقنية.

لم يكتف المشرع الجزائري بتجريم الاتفاق في الجرائم المساس بالمعالجة الآلية للمعطيات أو الجرائم التقنية بالنصوص المتعلقة بتكوين جمعية أشرار[1]، وهي القيام بأفعال تحضيرية لارتكاب جناية أو جنحة ضد الأشخاص أو الأموال حيث أن لهذه الجريمة ما يميزها عن باقي الجرائم ، فمن الصعب تصنيفها، من جهة يعاقب على مجرد الأعمال التحضيرية التي في الأصل هي غير معاقب عليها، ولكن من ناحية أخرى لها علاقة بالعديد من الجرائم الأمر الذي يعقد من تصنيفها[2].

[1] لم يخضع المشرع الجزائري الاتفاق الجنائي في هذه الجرائم للمواد (176-177) من قانون العقوبات والمتعلقة بتكوين جمعية أشرار.

[2] أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ، ط 15، دار هومه الجزائر 2013، ص523.

أ–الركن الشرعي

الواقع إن المشرع الجزائري تبنى المساءلة الجنائية في الاتفاق الجنائي باعتبارها جريمة مستقلة، وهذا بنص المادة (394مكرر5) من ق.ع.ج ربما لأن هناك العديد من الجرائم التقنية ترتكب في شكل جمعيات إجرامية، مما يشكل خطورة اكبر عند قيام المجرم بتنفيذ الجريمة بمفرده.

ويعتبر الاتفاق الجنائي مرحلة سابقة لارتكاب الجريمة، والأصل أن مرحلة التفكير والتحضير غير معاقب عليها، ولكن هذا لا يمنع المشرع من إدخالها في دائرة العقاب لخطورة الفعل الإجرامي. ولعل مبادرة المشرع في تجريم الاتفاق بغرض الإعداد لجريمة تقنية، هي أنّ هذا النوع من الجرائم يتم في إطار مجموعات خصوصا، إذن بمفهوم المخالفة، إذا حضّر المجرم لارتكاب جريمة تقنية، لا يمكن بأي حال الأحوال تطبيق النص طبعا إذا تعلق الأمر بمجرم واحد .

كما أن المشرع الجزائري لم يقم بتجريم مجرد العزم والتصميم على الإعداد لجرائم تقنية، بل أصّر على أن يكون مجسدا بفعل أو عدة أفعال مادية، وهو ما نصت عليه المادة (394مكرر)من قانون العقوبات التي جاء نصها كالأتي ".... وكان هذا التحضير مجسد بفعل أو عدة أفعال مادية." والتي عادة ما تكّون أعمال تحضرية، كالحصول على برمجيات الفيروسات، أو محاولات الدخول مرارا وتكرارا من اجل اكتشاف الثغرات الأمنية. وتتمثل عقوبة الاتفاق الجنائي وفق المادة (394مكرر5) نفس العقوبة لجريمة من الجرائم التقنية أو جرائم المساس بالأنظمة للمعالجة الآلية للمعطيات.

ب–الركن المادي للاتفاق الجنائي في الجرائم التقنية.

يتحقق هذا الركن بفعل المشاركة في الاتفاق وهذا بتحقيق الاتفاق إرادتين أو أكثر واجتماعهما على أمر معين. والاتفاق له مظهر مادي ملموس من خلال تعبير كل شخص عن

إرادته، فالتعبير عن الإرادة يعتبر فعلا ماديا كالقول الشفوي[1]، والذي يمكن تصوره في نطاق هذه الجرائم بالمحادثات على مواقع التواصل الاجتماعي والرسائل الصوتية، ورسائل البريد الالكتروني.

ويترتب على ذلك، أنّه لا يمكن الحديث عن الاتفاق الجنائي إلا في حالة وجود أكثر من شخصين يتفقان بأي طريقة كانت " ففي حال تعدد المتَفقون دون أن تجمعهم إرادة واحدة لتحضير الجريمة، وكان غرض باقي المجموعة الاستهزاء فقط بإرادة المجرم فلا قيام للاتفاق الجنائي في هذه الحالة"[2]، لذلك لابد أن يتفق الجميع على تحضير جريمة من الجرائم التقنية، وهذا عن طريق التحضير المادي متمثل في النشاط التقني لارتكابها، لذلك وجب أن تكون الإرادة موحدة ، لارتكاب الجريمة، وإلاّ لا مجال للحديث عن الاتفاق الجنائي المعاقب عليه بموجب المادة (394مكرر5).

ج–الركن المعنوي للاتفاق الجنائي في الجرائم التقنية.

إنّ الاتفاق الجنائي في جرائم التقنية هي جريمة عمدية، لابد من توافر القصد العام بعنصرية العلم والإرادة.

ويُراد بعنصر العلم أن يعلم المجرم بالعناصر اللازمة للجريمة، والأهم منه أن يقع الاتفاق الذي يستوي أن يكون عن سابق المعرفة بين الأشخاص الطبيعية والمعنوية أو بمناسبة الاتفاق الآني بينهم، بحيث لا يمكن أن يترتب العقاب إلا إذا اتفق شخصين على الأقل.

ويمكن ملاحظة أن الجرائم التقنية أو جرائم المساس بالمعالجة الآلية للمعطيات في الكثير من الأحيان تتم بنشر فيروس أو اختراق المواقع الالكترونية دون سابق اتفاق فيما بينهم على انه

[1] الغوتي بن ملحة، الجريمة المنظمة في القانون العقوبات الجزائري ، مجلة كلية أصول الدين للبحوث و الدراسات الإسلامية ، العدد 03 ، سبتمبر 2000، ص 259 ، مرجع مشار إليه لدى فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني ، رسالة دكتوراه ، قسم الحقوق،بن عكنون، جامعة الجزائر، 2009 – 2010 ،ص 146.

[2] رشيدة بوكر،جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارنة، الطبعة الأولى ، منشورات حلبي الحقوقية، لبنان 2012، ص345.

بالمقاربة مع دول تنتج برامج الحماية من الفيروسات والاختراق يشكل فيها المجرمون مجموعات تنطبق عليهم حكم الاتفاق، حيث يشكلون مجموعات لتبادل الخبرات حول نشر الفيروسات وتصميمها، لذلك بانتفاء العلم ينتفي الاتفاق، وبالتالي تنتفي المسؤولية الجزائية ، امّا العنصر الثاني للقصد الجنائي العلم لابد من توافر الإرادة وهو اتجاهها لتحقيق السلوك الإجرامي والمتمثل في التحضير لجريمة التقنية.

ثانيا:الشروع في الجرائم التقنية.

الشروع يعد ثاني عنصر من الأركان المشتركة للجرائم التقنية أو جرائم المساس بالأنظمة للمعالجة الآلية للمعطيات، وهي البدء في التنفيذ أو الشروع، أو كما يُطلق عليه المشرع الجزائري المحاولة، وهو الفعل المعاقب عليه بموجب المادة (30) ق.ع.ج،[1] فالشروع هو الفعل الذي لا تتحقق نتيجته الإجرامية لسبب خارج عن إرادة المجرم، بمعنى ليس بعدول منه بل لأسباب خارج عن نطاقه تؤدي إلى وقف تنفيذ جريمة من الجرائم التقنية وفق لنص المادة(394 مكرر7).

أ–الركن الشرعي للشروع في الجرائم التقنية.

وسع المشرع الجزائري من نطاق التجريم في هذه الجرائم، بحيث حتى الشروع في الاتفاق معاقب عليه، رغم انّه قد يكون من الصعب إثبات الجريمة التامة نفسها لا لشيء إلا لخصائص التي اتصفت بها، سواء تعلق الأمر بالجريمة نفسها أو بمرتكبها، فما بال إثبات الاتفاق والشروع فيه.

ويترتب على ذلك، أنّ أي تجاوز لأساليب الوقاية والتحري سوف يعرض الحق في الحياة الخاصة للخطر، ولا نقصد بذلك المجرم، بل أي مشترك أو مستخدم للانترنت، لذلك ربما كان من

[1] المادة 30 من ق.ع.ج"كل المحاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى و لو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها" .

الأنسب والأسلم توعية المستخدم لاستعمال وتفعيل الحماية الأمنية، وتوعيته بالطرق البسيطة كحفظ كلمة السر ومسح البيانات الخاصة عند نهاية كل استعمال للشبكة.

ب –الركن المادي للشروع في الجرائم التقنية.

يقوم الركن المادي في الشروع في الجرائم التقنية على نفس الأفعال التي تقوم عليها الجريمة، ففي جريمة الدخول يقوم الشروع على فعل الدخول، ولكن لا يتحقق لسبب خارج عن إرادة المجرم، وبذلك تدخل المشرع الجزائري تدخل لقمع هذا السلوك والمتعلق بالأعمال التحضيرية لكونها تشكل جريمة مستقلة باعتبارها تمس مصلحة محمية، وعلى سبيل المثال، فقد يقوم الجاني في الجرائم التقنية ببث البرامج التي يستطيع من خلالها الدخول إلى النظام أو معلومات، والبدء بالأفعال التي تؤدي إلى الاختراق، النظام المعلوماتي أو البدء في الاتصال بالنظام المستهدف في شبكة الاتصالات.

غير أنّ تدخل أسباب وعوامل أخرى أحيانا، يحول دون تحقيق ذلك كانقطاع التيار الكهربائي[1] ،وقد يصلح هذا الطرح في جرائم أخرى غير الجرائم التقنية، ربما الجرائم العادية التي ترتكب عبر الانترنت.

وبهذا فإنّه في الكثير من الأحيان، لا تأخذ الجريمة وقت طويلا في التنفيذ مما يصعب عملية المتابعة على فعل الشروع، إلا إذا كانت هناك مساعدة في إثبات الشروع عن طريق الأدلة العادية كالشهود مثلا،والواقع أن الإجراءات الوقائية التي أدرجها المشرع الجزائري في إطار القانون(09-04)قد تلعب دورا فعالا في إثبات الشروع في مثل هذه الجرائم، بالتالي متابعة مجرم الانترنت جزائيا وتسليط العقاب عليه.

[1] فايز محمد راجح غلاب ، المرجع السابق، ص 153.

ج–الركن المعنوي.

إنّ الركن المعنوي مهم في الشروع، فيتعين على المجرم أن يكون عالما بالوقائع ذات الأهمية في تكوين الجريمة، فكل ما يتطلب القانون من وقائع لبناء أركان الجريمة واستكمال عناصرها يتعين أن يكون الجاني عالما بها[1]، وبالتالي،فإنه لا يرتب على مجرد الدخول إلى نظام المعالجة الآلية، أنّ المتهم شرع في ارتكاب جريمة التلاعب بالمعلومات مثلا ما لم يتوجه قصده إلى إتمام هذه الجريمة، وإنّما قد يسال عن دخول غير مصرح به متى توافرت أركانه[2].

ثالثا:الجرائم التقنية المرتكبة ضد المؤسسات و الهيئات العامة.

إنّ أي فعل يستهدف الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، إذا تحققت به إحدى الجرائم المنصوص عليها في القسم السابع مكرر من ق.ع.ج، سواء كانت جريمة الدخول أو البقاء إلى أنظمة المعالجة الآلية لنظم تلك المؤسسات أو الهيئات، أو جريمة إتلاف الأنظمة، فإنّه يقع تحت طائلة المساءلة وفقا لنص المادة (394مكرر3) من ق.ع. ج.

أ–الركن الشرعي.

نصت المادة (394مكرر3) من ق.ع.ج على تجريم الدخول إلى الأنظمة الخاصة بالدفاع الوطني[3] ، أو المؤسسات والهيئات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات اشد ، حيث ورد النص كالتالي: " تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات اشد".

[1] نائلة عادل محمد قورة، مرجع سابق، ص 365.

[2] رشيدة بوبكر، مرجع سابق ، ص 360.

[3] حيث أن المشرع الجزائري قد عقد الاختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني ،عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني وهذا ما نصت عليه المادة(15)من القانون (09-04.) حفاظا على سيادة الدولة ومصالحها الخارجية.

ب–الركن المادي.

الركن المادي للجرائم التقنية التي يستهدف من خلالها الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، يتمثل بالأفعال والنتائج الخاصة، بالركن المادي لجريمة الدخول والبقاء إلى نظام المعالجة الآلية للمعطيات، وجريمة التلاعب بالمعطيات وجريمة التعامل مع معطيات غير شرعية متحصلة من جريمة، أو يمكن أن ترتكب بها جريمة انترنت.

ج–الركن المعنوي

الركن المعنوي للجرائم التقنية التي يستهدف من خلالها الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام لا يختلف عن الركن المعنوي الخاص بكل جريمة على حدا، والمتمثل بالقصد الجنائي العام بعنصرية العلم والإرادة والمتطلب تحققه في اغلب الجرائم باستثناء جريمة الدخول أو البقاء في صورتيهما المشددة، التي تطلب المشرع فيهما القصد الجنائي الخاص إلى جانب القصد الجنائي العام. إذ لابد أن يكون الجاني عالما بأنه يرتكب جريمة تقنية، وبالتالي جريمة انترنت ضد مؤسسة أو جهة عامة، بإرادته الحرة قاصدا إحداث النتيجة.

د–العقوبات.

ذكرنا سلفا أن جرائم الانترنت تشترك في العديد من الأحكام المتعلقة بالتجريم، وهي كذلك تشترك في بعض الأحكام المتعلقة بالعقوبة، ومن ذلك تشديد عقوبة الاعتداء على الأنظمة والمعطيات المتعلقة بالدفاع والهيئات والمؤسسات الخاضعة للقانون العام عن غيرها من الجهات والأشخاص، وهذا راجع للحماية الموجه إلى المصلحة العامة ومؤسسات دون غيرها من المصالح.

ففي حالة ارتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات واستهدفت تلك الجريمة مؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، فإنّه يتم مضاعفة العقوبة مقارنة بالجرائم التي تستهدف الأفراد وأشخاص القانون الخاص.

وعلى هذا النحو، يتم التمييز في مقدار العقاب بين جريمة الدخول والبقاء في أنظمة مؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، وعقوبة جريمة التلاعب بالمعطيات، وعقوبة جريمة التعامل في المعطيات غير مشروعة وهذا ما سنتناوله فيما يلي:

1- عقوبة جريمة الدخول و البقاء في أنظمة مؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام

تتضاعف العقوبة في هذه الحالة لتصبح الحبس من (6) أشهر إلى سنتين والغرامة من مائة ألف 100.000دج إلى 200.000دج، بعد أن كانت عقوبة الجريمة حينما تستهدف أنظمة الأشخاص أو الأفراد العاديين هي الحبس من (3) أشهر إلى (1)سنة والغرامة من 50.000دج إلى 100.000دج [1].

إذا تَّم ارتكابها ضد المؤسسات والجهات الخاضعة للقانون العام، وفقا لنص المادة(394مكرر3) حيث نصت على أنّ (تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة لدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام ، دون الإخلال بتطبيق عقوبات اشد[2].

وإذا تترتب على جريمة الدخول أو البقاء تخريب نظام الاشتغال المنظومة: فتصبح عقوبة الحبس من (1) إلى (4) سنوات، والغرامة من (100.000دج) إلى (300.000دج) بعد أن كانت الحبس من (6) أشهر إلى سنتين والغرامة من (50.000دج) إلى (150.000دج)[3].

2 – عقوبة جريمة التلاعب بالمعطيات

[1] يرجى الاطلاع على نص المادة (394 مكرر) ونص المادة(394 مكرر3) من ق.ع.ج.

[2] المادة (394 مكرر) و المادة (394 مكرر 3) من ق.ع.ج.

[3] المادة (394 مكرر) و المادة (394 مكرر 3) من ق.ع.ج

تضاعف العقوبة لكل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية، أو ازال أو عدل بطريق الغش المعطيات التي يتضمنها نظام المعالجة الآلية التابع لمؤسسة الدفاع الوطني، أو الهيئات الخاضعة للقانون العام، حيث تصبح عقوبة الحبس من سنة (1) إلى (6) سنوات، والغرامة من (1000.000دج) إلى (4000.000دج)، وذلك بعد أن كانت العقوبة لمرتكبي الجريمة في حالة اقترافها في مواجهة أشخاص القانون الخاص هي الحبس من (6) اشهر إلى (3) سنوات، و بغرامة من (500.000دج) إلى (2000.000دج) [1].

3- عقوبة جريمة التعامل في المعطيات غير مشروعة

بموجب المادة (394مكرر3) من قانون العقوبات، فإن العقوبة تصبح الحبس من (4) أشهر إلى (6) سنوات، والغرامة من (2000.000دج) إلى (10.000.000دج)، بعد أن كانت وفق نص المادة (394 مكرر) هي الحبس من شهرين إلى (3) سنوات والغرامة من (1000.000دج) إلى (5000.000دج)[2] .

رابعا:الجريمة التقنية المرتكبة من الشخص المعنوي .

يمكن للشخص المعنوي أن يرتكب إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو الجرائم التقنية عن طريق ممثليها، أي من لهم الصفة في تمثيل الشخص المعنوي أمام الغير.

وقد نص قانون العقوبات الجزائري على عقوبة الشخص المعنوي في حالة ارتكاب إحدى الجرائم التقنية المنصوص عليها في القانون، حيث شدد العقوبة ليجعلها تساوي خمس مرات عقوبة الشخص الطبيعي للجريمة ذاتها.

أ-أركان الجريمة التقنية المرتكبة من الشخص المعنوي. نصت المادة (394مكرر4) من ق.ع.ج على عقوبة الجرائم التقنية المرتكبة من قبل الشخص المعنوي بقولها : " يعاقب الشخص

[1] المادة (394 مكرر) و المادة (394 مكرر 3) من ق.ع.ج.

[2] المواد (394 مكرر 2) و (394 مكرر 3) من ق.ع.ح

المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس 5 مرات الحد الأقصى الغرامة المقررة للشخص الطبيعي"،و قد سار المشرع الجزائري بذلك على ضوء ما جاءت به اتفاقية بودابست في نص مادتها 12[1]، رغم أنّ الجزائر لم تصادق عليها[2]،وصادقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[3].

1- الركن المادي:

تقع الجرائم التي يرتكبها الشخص المعنوي بإتيان السلوك الإجرامي الذي يترتب عليه قيام المسؤولية والمتمثل في الدخول والبقاء، وهما الفعلان الرئيسان في جرائم التقنية وباقي الأفعال التي سوف يأتي على شرحها في الفروع اللاحقة.

[1] نصت المادة (12) من اتفاقية بودابست على مسؤولية الأشخاص المعنوية و حثت الدول الأعضاء على العمل بما ورد بالنص حيث ورد النص على النحو التالي :

- يجب على كل طرف أن يتخذ الإجراءات التشريعية ، أو أي إجراءات يرى أنها ضرورية من اجل اعتبار الأشخاص المعنوية مسئولة عن الجرائم المشار إليها في الاتفاقية الحالية إذا ارتكبت لمصلحتها عن طريق شخص طبيعي أخر ، يترف بشكل فردي، أو بوصفة عضوا في مؤسسة الشخص المعنوي ، و يمارس سلطة القيادة في داخلها بناء على القواعد التالية ، سلطة تمثيل الشخص المعنوي ، أو سلطة اتخاذ القرار باسم الشخص المعنوي ، أو سلطة ممارسة الضبط داخل الشخص المعنوي .
- بالإضافة إلى الحالات التي سبق النص عليها في الفقرة لأولى فانه يجب على كل طرف أن يتخذ الإجراءات الضرورية من اجل التأكد من أن الشخص المعنوي يمكن الن يكون مسؤولا إذا تخلفت المراقبة و الضبط من قبل شخص طبيعي مشار إليه في الفقرة 1 قد جعل من الممكن ارتكاب الجرائم المشار إليها في الفقرة السابقة لحساب الشخص المعنوي عن طريق شخص طبيعي يتصرف تحت سلطته.
- تكون نطق مسؤولية الشخصية المعنوية في نطاق المسؤولية الإدارية و الجنائية و المدنية ، حسب الجريمة المقترفة .
- كما أن مسؤولية الشخص المعنوي لا تعفي الشخص الطبيعي من المسؤولية.

[2]الجريدة الرسمية للمناقشات، المجلس الشعبي الوطني والخاصة بالمناقشة العامة لمشروع القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها http://www.apn.dz/ar/images/journal_officiel_debats/6_legislature/jod_6leg_122.pdf ، تاريخ الاطلاع8-8-2013

[3] مرسوم الرئاسي رقم(14-252) مؤرخ في 13ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014،يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ21 ديسمبر سنة2010، ج.ررقم57ليوم28 سبتمبر2014،ص4

2- الركن المعنوي:

يتحقق الركن المعنوي في الجرائم التقنية المرتكبة من طرف الشخص المعنوي إذا توافر القصد الجنائي العام بعنصرية العلم والإرادة.

وبهذا، يشترط لقيام الجريمة التقنية المرتكبة من الشخص المعنوي، أن يكون من ارتكب الجريمة باسم الشخص المعنوي، أو لحسابه، عالما بأنّه يرتكب جريمة من الجرائم التي تضمنها القسم السابع مكرر من قانون العقوبات الجزائري،كما يجب أن تتوافر الإرادة لاقتراف إحدى جرائم من قبل ممثل الشخص المعنوي، أو يمارس سلطة اتخاذ القرار باسمه[1].

ب- عقوبة الجريمة التقنية المرتكبة من الشخص المعنوي

تطبق على الشخص المعنوي نوعان من العقوبات، منها عقوبات وردت في نصوص قانون العقوبات بشكل عام[2]، وعقوبات وردت في نصوص خاصة بالجرائم التقنية أو جرائم المساس

[1] احسن بوسقيعة، الوجيز في القانون الجزائي الخاص، المرجع السابق،80.

[2] **عقوبات الجرائم المرتكبة من طرف الشخص المعنوي بشكل عام**

تضمن قانون العقوبات الجزائري عدداً من العقوبات في حال سئل الشخص المعنوي لجناية أو جنحة منصوص عليها في القانون، منها عقوبة الغرامة كعقوبة أصلية إضافة إلى عدد من العقوبات التكميلية.

– **العقوبة الأصلية:** و تتمثل في الغرامة التي تساوي من مرة إلى خمس مرات للعقوبة المقررة على الشخص الطبيعي،الفقرة(1) من المادة(18مكرر) من القانون رقم (04-15) المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات الجزائري.2006.

– **العقوبة التكميلية:** يعاقب الشخص المعنوي بواحدة أو أكثر من العقوبات التكميلية التالية، الفقرة(2) من المادة(18 مكرر) من القانون رقم (06-23) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات،

- حل الشخص المعنوي
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.
- المنع من ممارسة نشاط أو عدة أنشطة مهنية.
- نشر الحكم وتعليقه.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.

والعقوبات السابقة ليست خاصة بالجرائم التقنية فقط، وإنما يمكن أن توقع على كل الجرائم التي يرتكبها الشخص المعنوي.

بأنظمة المعالجة الآلية للمعطيات المرتكبة من الشخص المعنوي،فتكون عقوبات الجرائم التقنية وفقا للقانون الجزائري كما يأتي:

1-عقوبة جريمة الدخول أو البقاء في صورتها العادية،تكون عقوبة جريمة الدخول والبقاء المرتكبة من قبل الشخص المعنوي وهي الغرامة خمس مرات أضعاف عقوبة الجريمة المرتكبة من الشخص الطبيعي، فتكون من 250.000 دج مائتين وخمسين ألف دينار إلى 500.000دج خمسمائة ألف دينار[1].

2- عقوبة جريمة الدخول أو البقاء في صورتها المشددة[2]

تختلف عقوبة جريمة الدخول والبقاء المرتكبة من قبل الشخص المعنوي بحسب النتيجة المترتبة على الدخول والبقاء:

-إذا نتج عن الدخول أو البقاء حذف أو تغيير لمعطيات النظام:

تكون العقوبة من 500.000دج خمسمائة ألف دينار جزائري إلى 1.000.000دج مليون دينار جزائري.

-إذا نتج عن الدخول أو البقاء تخريب تشغيل المنظومة المعلوماتية:

وفي هذه الحالة تكون العقوبة من 250.000 دج مائتان وخمسين ألف دينار إلى750.000 سبعمائة وخمسين ألف دينار جزائري.

-عقوبة جريمة التلاعب بالمعطيات:

تكون عقوبة جريمة التلاعب بالمعطيات سواء بإدخال معطيات عن طرق الغش إلى نظام المعالجة الآلية للمعطيات،أم الحذف، أم التعديل للمعطيات التي يتضمنها النظام من 2.500.000دج مليونين ونصف إلى 10.000.000دج عشرة ملايين دينار جزائري[3].

---

[1] المادتين (394 مكرر، و394 مكرر4) من قانون العقوبات.

2والتي حصرها المشرع الجزائري في أثار أو نتائج الدخول أو البقاء دون الأخذ بعين الاعتبار إلى الركن المعنوي.

[3] المادتين (394 مكرر 1، و394 مكرر4)، من القانون السابق.

-عقوبة التعامل في معطيات غير شرعية.

في هذه الحالة تكون العقوبة من 5.000.000 دج خمسة ملايين دج إلى 25.000.000 دج خمسة و عشرون مليونا[1].

خامسا- العقوبات التكميلية للجرائم التقنية

زيادة على الأحكام المشتركة للجريمة التقنية السالف ذكرها، فإن الجرائم الانترنت تشترك في العقوبات التكميلية – المتعلقة بالجنح- المنصوص عليها في قانون العقوبات الجزائري بشكل عام[2]،

[1] المادتين (394 مكرر 2، و394 مكرر4)، من القانون نفسه.

[2] المواد من (9 إلى 18) من القانون رقم (06-23) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم (66-165) المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات.

العقوبات التكميلية للجرائم المرتكبة من الشخص الطبيعي بشكل عام.

العقوبات التكميلية التي وردت في ق.ع.ج يمكن تطبيقها على جرائم الانترنت بالنسبة للعقوبات التي نص القانون بتطبيقها على الجنح، أو على الجنايات والجنح، وجميع تلك العقوبات جوازية وليست وجوبية كما في بعض عقوبات الجنايات وهي:

-الحجز القانوني، وهي عقوبة وجوبية بالنسبة للجنايات، ومن ثم فهي جوازية بالنسبة للجنح ومنها الجرائم الانترنت.

-تحديد الإقامة، وتتمثل بإلزام المحكوم عليه أن يقيم في نطاق إقليمي يحدده الحكم لمدة لا تتجاوز خمس سنوات. راجع المادة (11) من ق.ع.ج.

-المنع من الإقامة لمدة لا تزيد عن خمس سنوات بالنسبة للجنايات. تضمنت المادة 12 من ق.ع.ج رقم 06-23 المؤرخ في 20ديسمبر 2006 تعريف المنع من الإقامة بأنه: حظر تواجد المحكوم عليه في بعض الأماكن لمدة لا تزيد عن خمس سنوات في مواد الجنح، وعشر سنوات في الجنايات بخلاف قرار المنع من الإقامة بالتراب الوطني، التي تكون مدتها 10 سنوات أو نهائية، وتطبق على كل أجنبي ارتكب جناية أو جنحة، راجع ج.ر رقم 84، ص13.

-الحرمان من ممارسة الحقوق الوطنية، والمدنية، والعائلية لمدة لا تزيد عن خمس سنوات، خولت المادة (14) من ق.ع.ج للمحكمة عند قضائها في جنحة بجواز حظر ممارسة حق أو أكثر من الحقوق الوطنية، والمدنية، والعائلية المنصوص عليها في المادة 9 مكرر وهذه الحقوق وفقا للمادة الأخيرة هي:

-العزل أو الإقصاء من جميع الوظائف والمناصب العمومية التي لها علاقة بالجريمة

-الحرمان من حق الانتخاب والترشيح ومن حمل أي وسام

-عدم الأهلية لآن يكون مساعدا محلفا ، أو خبيرا، أو شاهد على أي عقد، أو شاهد أمام القضاء إلا على سبيل الاستدلال

-الحرمان من الحق في حمل الأسلحة، وفي التدريس، أو في إدارة مدرسة، أو الخدمة في مؤسسة للتعليم بوصفه أستاذا أو مدرسا، أو مراقبا.عدم الأهلية لأن يكون وصيا أو مقدما.

-سقوط حق الولاية كلها أو بعضها، وتطبق تلك العقوبات من تاريخ انقضاء العقوبة السالبة للحرية أو الإفراج عن المحكوم عليه.

بالإضافة إلى عقوبتي المصادرة والإغلاق اللتين تضمنتهما المادة (394مكرر4)كعقوبتين تكميليتين تخص الجرائم التقنية[1].

وكما أن القانون العقوبات الجزائري قد نص على العقوبات التكميلية للجنايات والجنح، قد نص على عقوبتي المصادرة والإغلاق ضمن النصوص المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، وجعل بعضها وجوبية في بعض الجنايات، وبعضها جوازية في الجنايات والجنح، باستثناء مصادرة الأشياء المضبوطة التي يعد صنعها أو حيازتها أو إحرازها أو استعمالها أو بيعها أو عرضها للبيع جريمة في ذاتها، ولو لم تكن مملوكة للمتهم أو لم يحكم بإدانته، مع مراعاة حقوق الغير حسن النية[2].

-المصادرة الجزئية للأموال.

-المنع المؤقت لمدة لا تتجاوز خمس سنوات من ممارسة مهنة أو نشاط إذا ثبت علاقة المهنة أو النشاط بالجريمة المرتكبة، أو ثمة خطرا في استمرار ممارسة المهنة أو النشاط. المادة (16) من القانون رقم (06-23)المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات الجزائري.

-إغلاق المؤسسة لمدة لا تزيد عن خمس سنوات بالنسبة للجنح وهي عقوبة تطبق بالنسبة للجنايات والجنح إلا أنها في الجنايات عشر سنوات وفي الجنح خمس سنوات، راجع المادة (16 مكرر1) من ق.ع.ج.

- الإقصاء من الصفقات العمومية لمدة لا تزيد عن خمس سنوات في الجنح، ومنها جرائم التقنية أو جرائم المعالجة الآلية للمعطيات والإقصاء من الصفقات العمومية تعني منع المحكوم عليه من المشاركة بصفة مباشرة أو غير مباشرة في أي صفقة عمومية وقد تكون بصورة نهائية أو لمدة عشر سنوات بالنسبة للجنايات، وخمس سنوات بالنسبة للجنح، ونحن إذا نشير إلى العقوبة المتعلقة بالجنح في المتن، لأنها هي التي يمكن تطبيقها على الجرائم المعلوماتية. راجع المادة (16 مكرر2)ع.ج..

الخطر من إصدار الشيكات أو بطاقات الدفع، وتكون بالنسبة للجنح خمس سنوات وبالنسبة للجنايات فتكون مدة الحظر من إصدار الشيكات أو استعمال البطاقات هي عشر سنوات. المادة(16مكرر3) من ق.ع.ج.

- تعليق أو سحب رخصة السياقة، أو إلغائها مع المنع من استصدار رخصة جديدة ويكون الحظر لمدة خمس سنوات. وتطبق على الجنايات والجنح، وتكون مدة الحظر متساوية وهي خمس سنوات. راجع المادة(16 مكرر4)من القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 ج.ر. رقم 84، ص13

- سحب جواز السفر، ولمدة خمس سنوات المادة(16 مكرر5)من نفس القانون.

- نشر الحكم أو تعليق حكم أو قرار الإدانة. المادة (18) من نفس القانون

[1] المادة (394 مكرر6) من القانون رقم (04-15) المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات الجزائري.

[2] المادة394 مكرر6:مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة، مع إغلاق المواقع التي تكون محل لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

أ-عقوبة المصادرة:

يقصد بعقوبة المصادرة الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة أو ما يعادل قيمتها عند الاقتضاء[1]. ويبدو أن المصادرة وفقا للمادة(394مكرر6)من ق.ع.ج. سالفة الذكر هي عقوبة وجوبية.

وهذا من ناحية، لأنّها لم تترك خيار للقاضي للحكم بها من دونها كما في العقوبات الأصلية والمشددة للجريمة، ومن ناحية أخرى، لأن الهدف من هذه العقوبة هو الحد من تلك الجرائم[2]، فأصحاب الأجهزة والوسائل عندما يعلمون مسبقا بأنه سوف تتم مصادرة لكل الأجهزة والوسائل التي ترتكب بها الجريمة، والتي تكون عادة باهضة الثمن، بالإضافة إلى العقوبات الأصلية التي ستوقع عليهم، فإن ذلك سيكون مانعا من الإقدام على ارتكاب تلك الجرائم، ولتطبيق عقوبة المصادرة فإنه يتطلب توافر بعض الشروط منها[3]:

- يجب أن تكون عقوبة المصادرة تالية لعقوبة أصلية من العقوبات المنصوص عليها في القانون، وهي الحبس أو الغرامة، وتكون العقوبة وجوبية في الجنايات والجنح وليست جوازية، إلّا أنها تكون وجوبية في الجنايات بشكل عام، أما في الجنح والمخالفات فلا تكون وجوبية، إلا إذا نص القانون على تلك العقوبات[4]. وذلك ما ينطبق على عقوبة المصادرة في جرائم المساس بأنظمة
- أن تتم مصادرة الأجهزة والوسائل التي استخدمت في ارتكاب الجريمة مهما كانت تلك الوسائل عادية أو متطورة، مثلا كاستخدام مؤلَف خاص بكيفيات اختراق إمّا مطبوعة أو على صفحات الواب، وقد يستخدم برنامج، ولا يُشترط أن تكون الوسائل والأجهزة التي يتم مصادرتها

[1] راجع المادة (15)من ق.ع.ج رقم (06-23) المؤرخ في 20 ديسمبر2006 المعدل والمتمم للأمر رقم (66-165) المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات.

[2] عبد القادر عدو،المرجع السابق، ص399-400

[3] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط 12، دار هومه، الجزائر2012-2013.ص345-346.

[4] المادة (15 مكرر1) ق.ع.ج.

كعقوبة تكميلية محددة على سبيل الحصر، وإنما تنطبق العقوبة على أية وسيلة كانت، ويجب أن تكون الأشياء التي يحكم بمصادرتها قد تم ضبطها من قبل الجهات المختصة.

- يجب أن لا تمتد عقوبة المصادرة على حقوق الغير حسن النية[1]، لان الأصل أنّ العقوبة شخصية، وهو الإشكال الذي يصعب حله لان الأشياء المصادرة في الكثير من الأحيان مشتركة. ولا تقصر حقوق الغير حسن النية على حق الملكية فحسب، بل إن الحقوق الأخرى مثل حق الانتفاع والرهن يسري عليها ما يسري على حقوق الملكية ولا تشملها عقوبة المصادرة بحق حسن النية[2].

ب–عقوبة الغلق

نصت المادة(394مكرر6)من قانون العقوبات على عقوبة الغلق إلى جانب عقوبة المصادرة كعقوبتين تكميليتين، يعاقب بهما كل من ارتكب جريمة من جرائم التقنية، أو جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في القانون.

وتشمل غلق المواقع التي استغلت أو استخدمت في ارتكاب أي من جرائم التقنية المنصوص عليها في القسم السابع مكرر من قانون العقوبات وكذا غلق المحلات، أو أماكن الاستغلال التي ارتكبت منها تلك الجرائم إذا ارتكبت بعلم مالكها.

أما فيما يخص العقوبات المحددة للشخص المعنوي في قانون (09-04) فقد أحال المشرع الجزائري القاضي في الحكم بالعقوبة إلى القواعد العامة المقررة في قانون العقوبات وبالتالي فان الغرامة المحددة في جريمة عرقلة حسن سير التحريات القضائية في جرائم تكنولوجيات الإعلام

[1] يعتبر من غير حسن النية الأشخاص الذين لم يكونوا محل المتابعة أو الإدانة من أجل الوقائع التي أدت إلى المصادرة، ولديهم سند ملكية أو حيازة صحيح أو مشروع على الأشياء القابلة للمصادرة. راجع المادة(15 مكرر2)من ق.ع.ج رقم(06-23) المؤرخ في 20ديسمبر 2006.

[2] محمد خليفة مرجع سابق، ص121.

والاتصال تكون حسب المادة 18مكرر من قانون العقوبات من 250.000 دينار جزائري الى 2.500.000 دينار جزائري[1].

وبعد إلمام بمجمل الأحكام المشتركة للجرائم التقنية أو جرائم تكنولوجيات الإعلام والاتصال التي تعتبر جرائم المساس بالأنظمة المعالجة الآلية للمعطيات، ومن خلال النصوص القانونية يأخذ هذا النوع من الجرائم في التشريع الجزائري صورتين وهما إما الدخول أو البقاء في منظومة معلوماتية أو المساس بمنظومة معلوماتية، وهو ما سوف نتطرق له في الفرع الثاني.

الفرع الثاني: جريمتا الدخول والبقاء في نظام المعالجة الآلية.

يطلق على جريمة الدخول والبقاء "الولوج غير القانوني أو غير المشروع"، فالصورة الأولى من هذه الجرائم هي الأهم ضمن أصناف الجرائم التقنية على العموم، رغم أنّ المشرع الجزائري لم يتطرق إلى جميع أنواع الجرائم التقنية، أو ما يعرف بالإجرام المعلوماتي، و جريمة الدخول والبقاء غير المشروع هي من جرائم التي نصت عليها اتفاقية بودابست في مادتها الثانية[2].

وقد جمع المشرع الجزائري بين الحماية الجنائية للمعطيات في حد ذاتها كمحل للجريمة، والحماية الجنائية للمنظومة المعلوماتية باعتبارها مستودع هذه المعطيات، أو طريقة لتسييرها.

ويترتب على ذلك، أنّه لا يمكن إفراد حماية جنائية لشيء دون أن يكون له قالب أو هيكل حتى، وإن كان مترامي الأطراف أو غير محدود، وهو الحال بالنسبة لتكنولوجيات الإعلام والاتصال أو شبكة الانترنت. والواقع أن الأصل في الجرائم التقنية هو الدخول أو البقاء، أما باقي

[1] المادة (11) من القانون(09-04)الفقرة الأخيرة"دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6)إلى خمس(5)سنوات وبغرامة من 50.000دج إلى 500.000دج.يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات

[2] المادة الثانية من اتفاقية بودابست التي استمد منها المشرع الجزائري معظم الأحكام القانونية الموضوعية والإجرائية لجرائم الإنترنت أو تكنولوجيات الإعلام والاتصال.

الجرائم فلا يمكن أن تكون أو ترتكب إلّا بهذين السلوكين، إلاّ أن يكون هذا الاعتداء خارج المنظومة، وهنا يمكن تطبيق نصوص جرائم أخرى كالإتلاف أو السرقة.

أولا:الركن الشرعي لجريمتي البقاء والدخول في منظومة معلوماتية.

جريمة الدخول غير المشروع إلى منظومة المعلوماتية جريمة مستحدثة جرّمها المشرع الجزائري وفق المادة (394مكرر)ق .ع .ج، فالدخول هو فعل سابق للبقاء، بحيث لا يتصور البقاء من غير دخول للمنظومة المعلوماتية، تحتوي هذه المنظومة بشبكاتها على كم هائل من المعطيات من أبسط البيانات الشخصية إلى أسرار الدولة الاقتصادية والسياسية والعسكرية، ولهذه الجريمة في صورتان بسيطة ومشددة.

أما الصورة البسيطة منها تتحقق بمجرد الدخول، والمشددة فيتحقق بالبقاء مع تحقق النتيجة الإجرامية، وهي المتمثلة في الصور المنصوص عليها والمتمثلة في الحذف والتغيير والتخريب.

ثانيا:الركن المادي لجريمة الدخول والبقاء إلى المنظومة المعلوماتية.

تقع جريمة الدخول والبقاء بمجرد إتيان السلوك الإجرامي وهو الدخول إلى النظام أو البقاء بعد الدخول بطريقة عرضية وغير مقصودة[1].

أ–الدخول: هو الولوج إلى منظومة معلوماتية دون تصريح، وبالتالي يكون مخالف لإرادة من له السيطرة على المنظومة "سواء كانت الأنظمة التي تمَّ الدخول إليها متعلقة بأسرار الدولة أو دفاعها، أو تتضمن معطيات شخصية تتعلق بحرمة الحياة الخاصة أو غير ذلك"[2].

لذلك يختلف فعل الدخول عن غيره، كونه في جرائم الانترنت يتعلق بالعالم الافتراضي، أي مسرح لا مادي غير محسوس لا يمكن لمسه وهو ما يدعى بالاختراق أي عملية الدخول غير

[1] ايمن عبد الله فكري، المرجع السابق، ص200.

[2] علي عبد القادر القهواجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، المرجع السابق، ص50.

مصرحة أي اختراق للنظام المعلوماتي والحماية الأمنية التي تم تنصيبها وتفعيلها،ويتم ذلك عن طريق حصان طروادة وهو فيروس يخترق نظم ويستغل الثغرات الأمنية فيها[1].

ب– البقاء: هو "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام"[2].إذن فجريمة الدخول والبقاء تتطلب وجود نظام معلوماتي مؤمن، أي يخضع لحماية أمنية أو ما يعرف بأمن المعلومات، فلو فرضنا أن المنظومة المعلوماتية هي عبارة عن سكن، فمن غير المعقول ألا نوصد الأبواب ضد أي سرقة أو اعتداء، وهذا ما يمثل أمن المعلومات.

ولكن قد لا ينطبق مثال السكن على نظام واحد وهو الخاص بالفرد، ولكن يكف لنا أن نراقب مجموعة الأنظمة المتشعبة والمتشابكة خصوصا أن مالكها ليس شخص طبيعي أو معنوي معروف، وهو خاصية شبكة الانترنت كما أنّه، ليس من حق أي شخص الدخول والبقاء في منظومة غير محمية، فقط لأن أبوابها غير موصدة[3]. خصوصا أننا نعلم أن الأمن المعلوماتي مكلّف جدا في الكثير من الأحيان.

ج – الحماية الأمنية أو أمن المعلومات: تنقسم الأنظمة المعلوماتية إلى أنظمة مفتوحة للجمهور والتي تعامل على أنها أماكن عامة أي متاحة للجمهور، وأماكن خاصة غير محمية، وأخرى خاصة محمية، وهنا الأماكن تمثل المنظومة المعلوماتية. فاختلف الفقه حول ضرورة وجود حماية أمنية، من أجل استحقاق الحماية الجنائية. وانقسم الفقه إلى فريقين بين مؤيد ورافض للحماية الأمنية.

[1] ايمن عبد الله فكري، المرجع السابق، ص201.

[2] علي عبد القادر القهواجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، المرجع السابق، ص52.

[3] وهو ما ذهب إليه المشرع الجزائري حيث أنه لم يشر إلى ضرورة وجود حماية أمنية على النظام المعلوماتي، فكل النظم هي تحت طائلة النصوص المتعلقة بالمعالجة الآلية للمعطيات،والحماية الجنائية لسلوكيات المرتكبة ضد تكنولوجيات الإعلام والاتصال و بمساعدتهما.

1-الرأي الأول: المؤيد لضرورة وجود حماية أمنية.يستند إلى أنّه من "غير المقبول حماية معلومات هامة تركها المسؤولون عنها دون أية إجراءات تكفل لها الحماية"[1]، حيث فعل الاعتداء عن طريق الاختراق، لا يكون واضحا، إلا إذا تم اختراق الحماية الأمنية للنظام، ذلك أن وجود نظام امني يحمي الشبكة من الانتهاكات، و فعل الدخول هو إثبات سوء نية القائم بالمحاولة[2]، إضافة إلى إثبات الركن المادي للجريمة.

على أنّه توجد تقنيات حديثة لتأمين نظام المعلومات من الاختراق، ومنها بصمة العين والإصبع، بحيث تمثلان إجراءات حماية يصعب اختراقه إذا تم الجمع بينهما، بذلك يمكن تأمين الملفات كلها وعدم فتحها إلا باستخدام تلك التقنية.

2-الرأي الثاني: الرافض لضرورة وجود حماية أمنية.

وهو الاتجاه الذي يفرض الحماية الجنائية حتى من غير وجود حماية أمنية، ويستند إلى أن تطبيق هذا الشرط قد يؤدي في الكثير من الأحيان إلى تضييق تطبيق القانون. وبالتالي الاعتداء على المعلوماتية والمعلومات المعالجة آليا، وهذا ما أدى إلى تجاهل الأخطاء البرمجية التي يقع فيها المبرمجون أو المسئولون عن أمن النظام[3].

غير أنّه، ومع التطور التقني فإن الحماية الفنية أصبحت خيار متاحا مع الأجهزة ولشبكات مجانا، لذلك فهي كما ذكرنا إثبات للركن المعنوي لجرائم التقنية- بمحاولة ارتكاب السلوك الإجرامي رغم وجود الحماية الأمنية -، وتتضاءل أهمية الحماية الجنائية ليس أمام سلوكيات المجرم، بل أمام التطور التقني للمنظومة في حد ذاتها وخصوصا بعد انتشار wifi[4] في الأماكن العمومية[1]وظهور الجيل الثالث والرابع للهواتف الذكية والألياف البصرية.

---

[1] نائلة عادل محمد قورة ، مرجع سابق، ص353.

[2] أحمد حسام طه تمام، المرجع السابق، ص02.

[3] نائلة عادل محمد قورة ، المرجع السابق، ص355.

[4] WI-FI. الواي فاي هي اختصار لWireless Fidelity ، أي البث اللاسلكي الفائق الدقة والسرعة، ويستخدم لتعريف أي من تقنيات الاتصال اللاسلكي في المعيار IEEE 802.11 وهي التقنية التي تقوم عليها معظم الشبكات اللاسلكية WLAN اليوم، فهي تستخدم

د-فعل الدخول والبقاء غير المصرح به:

يرتبط فعل الدخول بعدم التصريح أي أنّه إذا كان الدخول إلى النظام المعلوماتي مصرح به فلا مجال للحديث عن جريمة الدخول الغير المصرح به، وهو الحال بالنسبة للإجراءات الجزائية التي أقرها المشرع الجزائري في إطار القانون (09-04) والخاصة بهذه الجرائم.

1-فعل الدخول غير المصرح به:

يشمل الدخول والشروع فيه أي المحاولة فالدخول هنا لا نقصد به الدخول المادي، وإنّما هو الدخول اللامادي غير المحسوس المتناسب مع البيانات المعالجة أليا حيث لم يحدد أي وسيلة يتم الدخول بها، لذلك تقع الجريمة بأي وسيلة أو طريقة ويستوي أن يتم الدخول مباشرة أو عند طريق غير مباشر[2] .

ويتحقق الدخول إلى أي نظام معلوماتي بأي طريقة مباشرة، كالدخول من نظام يعمل عليه موظف أو الدخول الغير المباشر والذي يتم من نظام إلى آخر باعتبار أن المنظومة المعلوماتية هي مجموعة من الأنظمة المنفردة، وهذا طبعا باعتبار الشبكة محور هذا الربط، كما فصّلنا سابقا، فلولا وجودها-المعلوماتية والانترنت- لما برزت إلى الوجود هذه المشاكل القانونية التقنية على حد سواء.

ويقصد بالدخول في المنظومة المعلوماتية الاتصال بنظام الكمبيوتر بأي طريقة كانت حيث يمكن تصور الدخول في النظام، بأن يقوم المستخدم بالدخول في النظام دون أن يكون مسموحا له بذالك، وسواء قام في ذالك المتدخل بعمل توصيلة من النظام أو تدخل إليه عن طريق شبكة

موجات الراديو لتبادل المعلومات بدلاً من الأسلاك والكوابل، كما أنها قادرة على اختراق الجدران والحواجز، وذات سرعة عالية في نقل واستقبال البيانات، انظر الموقع،http://readinfos.blogspot.com/2012/08/wifi.html

[1] بلدية الجزائر تطلق خدمة الانترنت في وسائل النقل.

http://www.elmouwatin.dz/?%D9%85%D8%A4%D8%B3%D8%B3%D8%A9-%D8%A7%D9%84%D9%86%D9%82%D9%84-%D8%A7%D9%84%D8%AD%D8%B6%D8%B1%D9%8A,6467

[2] جميل عبد الباقي الصغير،القانون الجنائي و التكنولوجيات الحديثة،الطبعة الثانية، دار النهضة العربية، القاهرة،2012،ص28.

الإنترنت[1]، لذلك فإن الدخول في الجرائم التقنية هو"الولوج غير المشروع لنظام المعالجة الآلية أو مجموعة نظم عن طريق انتهاك الإجراءات الأمنية"[2] ويتم الدخول غير المصرح به، وبالتالي غير المشروع عن طريق، الاختراق المباشر والاختراق غير المباشر[3].

وتؤكد المادة (394مكرر)من قانون العقوبات أن جريمة تعد قائمة بمجرد الدخول أو البقاء من دون موافقة صاحب النظام ،وحتى وإن لم يجد في الملفات ما يبحث عنه من معلومات أو يحدث ضررا[4] أي أن الجريمة تقوم بمجرد الولوج إلى المنظومة المعلوماتية ،حتى بدون حدوث ضرر أو فائدة ،فالدخول هنا كان بدون وجه حق[5].

كما عاقب المشرع على الشروع في دخول منظومة معلوماتية أي المحاولة، والهدف هو التشديد على حماية الأنظمة المعلوماتية من الانتهاك[6] "فكل استعمال للنظام دون رضا صاحبه

---

[1] شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، المرجع السابق،دار الجامعة الجديدة ،الإسكندرية،مصر،2007،ص99.

[2] زينات طلعت شحادة، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، بدون طبعة، المنشورات الحقوقية ، لبنان، ،ص43.

[3] **– الاختراق المباشر**

الاختراق المباشر يتم على أساس أخطاء برمجية ،ويقع تحت مجموعة من الأساليب منها:

- البحث عن المنافذ المفتوحة عن طريق الشبكات.
- مسح النوافذ.
- استغلال المنافذ المفتوحة.
- كسر كلمات السر الخاصة بالشبكات.
- اقتحام نظم تشغيل الشبكة.
- الهندسة الاجتماعية.

– الاختراق غير المباشر أو المبطن

ويتحقق الاختراق غير المباشر أو المبطن عن طريق حصان طروادة، عن طريقIP (Address ، وعن طريق الكوكي Cookie . سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات رسائل ماجستير في العلوم الشرطية ،جامعة نايف العربية للعلوم المنية، الرياض ،المملكة العربية السعودية ،2003 ،ص73-83.

[4] شيماء عبد الغني محمد عطا الله، المرجع السابق ،ص122.

[5] حسين بن سعيد الغافري ،المرجع السابق ،ص352.

[6] فايز محمد راجح غلاب، الرجع السابق، ص352.

يشكل دخولا والعكس، فإن الدخول لا يعني بالضرورة استعمال النظام.[1]" ولم يحدد المشرع فئة الأشخاص المرتكبين لجريمة الدخول،كما فعل في فرض ركن مفترض لقيام الجريمة كما هو الحال في جرائم الفساد، أي أن يقوم بها موظف وهنا وفي هذه الجرائم محلّ الدراسة، فالركن المفترض فيها هو وجود نشاط تقني.

2-فعل البقاء غير المصرح به: هو "التواجد داخل نظام المعالجة الآلية للمعطيات ضد الإرادة من له الحق في السيطرة على هذا النظام[2]".

ويختلف فعل البقاء عن فعل الدخول،كون فعل الدخول لحظي أمّا البقاء فهو مستمر، فقد يكون فعل الدخول يعد دخول مشروع أو مصرح به وقد يكون مجتمعًا ومعاقب عليه مع الدخول أو مستقلا.

كما انه لفعل للبقاء غير المشروع عدة صور، فقد يكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح بالبقاء بداخل النظام،أو في الحالة التي يطبع فيها نسخة، من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية والإطلاع فقط[3]،ويتحقق هذا أيضا بالنسبة للخدمات المفتوحة للجمهور،والتي يستطيع فيها الجاني الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة[4].

إنّ الفعل ليس مشروط بوقت معين أي لا علاقة له بالزمن، فالمهم هو تحقق البقاء غير المشروع، سواء بعد عملية دخول مشروعة، أو تم بعد تجاوز المدة المسموحة بالبقاء في النظام.

[1] فايز محمد راجح غلاب، المرجع السابق، ص197.

[2] عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الإلكترونية، ص52.

[3] نهلا عبد القادر المومني، الجرائم المعلوماتية،دار الثقافة للنشر والتوزيع،عمان الأردن،2008،ص155.

[4] محمد الحماد الهيتي، التكنولوجيا الحديثة و القانون الجنائي ، دار الثقافة للنشر والتوزيع، الأردن2010، ص182.

ثالثا: الركن المعنوي لجريمة الدخول والبقاء.

شأن كل الجرائم لابد من توافر القصد الجرائم العام بعنصرية العلم والإرادة، حيث اشترط المشرع الجزائري في الدخول البسيط أن يتم عن طريق الغش، وبالتالي فهي جريمة عمدية، فالمهتم يقوم بالدخول أو البقاء إلى نظام المعالجة الآلية، ولم يحدد المشرع هوية النظام الذي تم الدخول أو البقاء فيه، والواقع أنّ هذا الدخول أو البقاء لا يمكن أن يتصور أنه بمحض الصدفة،الاّ إذا كانت المنظومات متشعبة وهو حال شبكة الإنترنت وأنظمتها، لدى فهي جريمة، إذن نحن أمام إشكالية إثبات السلوك في المجمل.

وعلى هذا النحو، فالحال سيزداد صعوبة إذا تطرقنا لجزئيات تلعب التقنية فيها دورا رئيسيا. فدخول أي نظام معالجة ضدّ رغبة مسؤول النظام، أيا كان الدافع سواء على سبيل الفضول أو إثبات قدرة الانتصار على النظام أو اللعب أو اللهو، مع انصراف إرادته إلى ارتكاب السلوك الإجرامي. إذ يكفي أن تكون نية المجرم قد اتجهت إلى الدخول غير المشروع في نظام المعالجة الآلية دون اشتراط أن تتجه هذه النية إلى تحقيق الضرر[1].

وبهذا، فالدخول باستعمال الغش ينفي الخطأ العمدي الجنائي لتحقيق النتيجة و الذي يتحقق في صورة التلاعب لمعلومات نظام المعالجة، النصوص عليه بالمادة (394مكرر1) فمن النادر أن يدخل الفاعل منظومة معلوماتية وهو غير مدرك لذلك[2].

فكما ذكر سابقا، أن ما يميز المجرم التقني مجرم الانترنت، هو الدراية بتكنولوجيات الإعلام والاتصال والتي تحول دون إمكانية التسليم بالخطأ أو البقاء وعلى الرغم من ذلك فإن انتفاء العلم ينتفي به القصد الجنائي[3].

[1] زينات طلعت شحاده ، المرجع السابق ، ص51.

[2] فايز محمد راجح غلاب ، المرجع السابق، ص199.

[3] نائلة عادل محمد قورة، المرجع السابق، ص365.

إذن، يلزم الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء وأن يعلم الجاني بأنّه ليس له الحق في الدخول إلى النظام والبقاء فيه.

رابعا:الصورة المشددة للجريمة.

تنص المادة (394مكرر 2) من ق.ع.ج الفقرة الثانية على مايلي "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج".

كما نصت الفقرة الثالثة (03) من نفس المادة على الظرفين تشدد بهما عقوبة الدخول والبقاء داخل النظام، ويتحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائفه، ويكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع وتلك النتيجة الضارة، ولا يشترط أن تكون تلك النتيجة الضارة مقصودة، لأن تطلب من هذا الشرط يكون غير معقول[1].

الفرع الثالث:جرائم الاعتداءالعمدي والتعامل في البيانات و نظم المعالجة الالية للمعطيات

انّ الأصل أنّ جرائم التقنية في التشريع الجزائري، تنحصر في الدخول إلى المنظومة المعلوماتية، لان الأصل في السلوك الإجرامي هو النشاط التقني أي الدخول غير الصرح به امّا ما يليها من بقاء غير مشروع وتخريب في النظام وما يتبعه من تخريب فهو خاص بالظروف المشددة، إلا أنّ هذا الطرح لم يتبناه المشرع بحسب قراءة النصوص القانونية المتعلقة بالموضوع.

[1] نائلة عادل محمد قورة، المرجع السابق، ص349.

أولا: جريمة الاعتداء العمدي على البيانات المخزنة في النظام.

وهي الجريمة التالية التي نص عليها المشرع الجزائري، وهي نفس المادة الرابعة من الاتفاقية الأوروبية للإجرام السيبيري، والتي عنونتها بالاعتداء على سلامة المعلومات[1].

أ-الركن الشرعي:

نصت المادة(394مكرر1) على مايلي:"يعاقب بالحبس من ستة6أشهر إلى ثلاث3 سنوات وبغرامة من 500.000الى 2000000د ج،كل من ادخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريقة الغش المعطيات التي يتضمنها".

ب-الركن المادي جريمة الاعتداء العمدي على البيانات المخزنة في النظام:

لا يتحقق النشاط الإجرامي لهذه الجريمة إلا بتحقق صورة من الصور الثلاث التي أدرجها المشرع الجزائري و هي الإدخال أو الإزالة أو التعديل.

1- الإدخال:

ويقصد به:"إضافة معلومات جديدة على دعامة سواء كانت خالية من المعطيات أو كان يوجد بها معلومات[2]"،حيث يشمل هذا الفعل إدخال خصائص ممغنطة في الدعامة الموجودة سواء كانت فارغة أو كانت تحتوي على خصائص ممغنطة قبل هذا الإدخال[3]".

ويتم عادة في المنظومة إمّا باستعمال تعسفي لبطاقات الدفع أو عن طريق استعمال برامج يكون الهدف منها في الغالب إتلاف البيانات المخزنة في النظام كليا أو تعديلها بما يخدم المجرم،

[1] المادة الرابعة:الاعتداء على سلامة البيانات"1-يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنّها ضرورية لتجريم، تبعا لقانونه المحلي،إذا حدث ذلك عمدا، ودون حق،أي أضرار، أو محو، أو تعطيل، إتلاف، أو طمس لبيانات الحاسب.
2-يمكن لأي طرف أن يحتفظ بحق اشتراط أن يكون السلوك المنصوص عليه في الفقرة الأولى يؤدي إلى أضرار جسيمة." هلالي عبد الاه احمد،الجوانب الموضوعية والإجرائية لجرائم المعلوماتية،المرجع السابق،ص85.

[2] فايز محمد راجح غلاب ، المرجع السابق ، ص212.

[3] محمد خليفة ، المرجع السابق ، ص179.

وهو ما يمكن أن يجد له فضاء و واسعا مع انتشار خدمة الحكومة أو الإدارة الإلكترونية، وما يمكن أن يقع من إدخال للمعلومات غير صحيحة سواء تعلق الأمر بالبيانات الشخصية أو المالية أو غيرها ،أمّا الصورة الثانية للركن المادي هي:

2-المحو:

وهو الإزالة أي إزالة جزء من المعطيات المسجلة على دعامة أو الموجودة بداخل النظام، أو تحطيم تلك الدعامة، أو نقل أو تخريب جزء من المعطيات الخاصة بالذاكرة[1]. لذلك فإنه لابد من وجود معطيات معالجة، وإلاّ فإنّه لا يمكن بأي حال من الأحوال القيام بالمحو دون أن يكون هناك دخول مصرح-الدخول المصرح الى جزء من النظام المعلوماتي ولكن يتم تجاوز التصريح الممنوح- أو غير مصرح به للمنظومة المعلوماتية والذي يُتطلب للبقاء-عن طريق الاختراق-[2]، لأنّه رغم أن العملية قد تكون في فترة زمنية بسيطة، إلّا أنّ هذا يعتبر بقاء من أجل المحو أو الإدخال أو التعديل.

3-التعديل[3]:

ويقصد به "تغيير المعطيات الموجودة داخل نظام المعالجة الآلية للبيانات أو بمعطيات أخرى.كما يقصد به قيام الغير ممن لا يملك الحق في إحداث تعديل في المعلومات بتعديلها[4] وعلى هذا الأساس جريمة التلاعب بالمعطيات وردت صورها على سبيل الحصر، وبالتالي فإن أي أسلوب يخرج عن الأساليب السابقة الذكر لا يقع تحت طائلة التجريم، ولو شكل اعتداء على المنظومة المعلوماتية.

[1] فايز محمد راجح غلاب ، المرجع السابق ، ص212.

[2] محمد خليفة المرجع السابق،115

[3] من خلال قرائتنا لم تتضمن اتفاقية بودابست في موادها التعديل كصورة من صور التلاعب بالمعلومات وإنما الإضرار بالمعلومات عموما في المادة 04 من الاتفاقية.

[4] عمر أبو بكر يونس ، الجرائم الناشئة عن استخدام الإنترنت ، مرجع سابق ص363.

من كل ما سبق، فإن فعل الإدخال يختلف عن التعديل ذلك أن الإدخال هو إضافة جديدة لما كان موجود أصلا، وهذا ما يمكن كما قلنا أن يكون في إطار بعض البيانات المتعلقة بالوثائق الرسمية المرقمنة، غير أنّ التعديل قد يكون في معطيات موجودة أصلا فالإدخال يزيد من حجم البيانات على عكس الإزالة التي تنقص من حجم المعلومات.

أما **التعديل** فهو يحتفظ بنفس الحجم ولكن بتغيير ويدخل في هذا القيام بهذا السلوك الإجرامي أو النشاط التقني بالتحديد واستعمال العديد من البرامج "كحصان طروادة[1] والدودة[2] والقنبلة الزمنية[3].

وللإشارة، فإن المشرع الجزائري قد حدد معطيات المنظومة المعلوماتية،أو التي هي في طريق المعالجة، دون المعطيات التي هي خارج النظام أو المنظومة، لأنّه من البديهي أن يتم مراجعة البيانات أثناء عملية المراجعة وسهل معرفة إذا تمّ التلاعب بها من عدمه، إنّ جريمة الدخول والبقاء هي جريمة خطر، وليس جريمة ضرر بمعنى أنّه يعاقب المجرم بمجرد إتيان السلوك الإجرامي المتمثلة في الدخول أو البقاء أو كليهما معا ولكن جريمة الاعتداء والتي تتم عن طريق التلاعب فهي جريمة عمدية، حيث أنّ إرادة الجاني تتجه إلى إدخال إزالة أو تعديل، مع علمه أن ليس له الحق في ذلك.

ج- الركن المعنوي: جريمة الاعتداء العمدي على البيانات المخزنة في النظام.

يتعين على المجرم أن يعلم أنّ هذه المعلومات ليست ملكا له، بل لغيره[4] إذ بمفهوم المخالفة، إذا كانت المعلومات كلها له أو اعتقد أنها ملك له، فله أن يتلاعب بها ويستخدمها بمعنى أن

[1] حصان طروادة:برنامج له قدرة كبيرة على الاختباء في البرنامج الأصلي وعند تشغيل البرنامج ينشط ليبدأ نشاطه التدميري والذي يؤدي إلى تعديل أو محو بعض البيانات من الجهاز او تدمير النظام كله.احمد خليفة الملط، المرجع السابق،ص543.

[2] الدودة:عبارة عن برنامج تشغيل أية فجوات في نظم التشغيل كي تنتقل من نظام معلوماتي إلى أخر أو من شبكة إلى أخرى. احمد خليفة الملط، المرجع السابق،ص544.

[3] القنبلة الزمنية:عبارة عن برنامج ينفد في لحظة محددةاو فترة زمنية منتظمة...فهي تثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة. احمد خليفة الملط، المرجع السابق،ص545.

[4] فايز محمد راجح غلاب، المرجع السابق ، ص219.

يعدلها أو يزيلها، وهذا ما لا يمكن تصوره إطلاقا، لأنّه في حالة أنّه تم التأكيد على صحة هذه المعلومات وتمت معالجتها، فلا يمكنه تعديلها إلا إذا صرح أو رخص له المخول قانونا بذلك، وبالتالي إذا فعلها، فهو اعتداء على المعلومات المعالجة فالعبرة هنا في هذه الجريمة بالنظام أولا ثم المعلومة المتواجدة فيه.

وقد لا يكون الباعث في هذه الجريمة إحداث ضرر بل قد يكون الباعث مقصدا اجتماعيا، أو فعل ما يعتقد الجاني أنه صواب أو مساعدة لشخص ما ، بمعنى ألا يقصد المجرم الإضرار.

وبهذا، تقوم الجريمة بمجرد إتيان صورة من صور الركن المادي دون الأخذ بعين الاعتبار بالباعث الذي قد يكون حسن، ويمكن الإعطاء العديد من الأمثلة: كالاستفادة من السكنات الاجتماعية، أو التكفل الطبي أو حتى حذف بيانات إحصاء المواطنين للخدمة الوطنية، أو أي خدمة يراها المجرم خدمة اجتماعية أو إنسانية، وهو ما لا يبرر العبث الذي قام به حتى وان كان بدافع الخير والمساعدة.

ثانيا: جريمة التعامل في البيانات خارج النظام.

هي جريمة التعامل في معلومات غير مشروعة وهي الجريمة المنصوص عليها في المادة(4مكرر2)[1] من ق.ع.ج، وهي النتيجة الحتمية والتي لابد من العقاب عليها، فما مصير المعلومات التي تم مثلا حذفها أو تعديلها بعد الخروج من المنظومة المعلوماتية لذلك كان لابد من تجريم أي سلوك إجرامي يخضع المعلومات المتحصل عليها لأي تعامل غير مشروع.

لذا لم يسع المشرع الجزائري إلى حماية المعطيات المعالجة فقط، بل أقر الحماية إلى المعطيات غير المعالجة، والتي تكون إما مخزنة في النظام المعلوماتي أي ساكنة أو متحركة[2] أي مرسلة عن طريق النظام المعلوماتي، حيث أن الغاية من التجريم هو إمكانية استعمال هذه المعطيات المتحصل عليها. "وتشمل جريمتي الدخول والبقاء، أو الاعتداءات العمدية على المعطيات داخل النظام، أو

[1] تقابلها المادة 06 من اتفاقية بودابست 2001.

[2] لكل نوع من هذه المعطيات، إجراء تحقيق خاص به، سوف نتناوله في الباب الثاني،الفصل الأول،المبحث الثاني،ص204.

تخريب النظام كظرف مشدد على جريمة الدخول أو البقاء ،والتلاعب بالمعطيات المخزنة في نظام المعالجة الآلية للمعطيات[1].

أ-الركن المادي:

و يتمثل النشاط الإجرامي، هو التعامل مع معلومات صالحة لارتكاب جريمة من جرائم بحيث وضع المشرع طرق وأشكال للتعامل مع المعطيات التي سبق استعمالها في ارتكاب الجريمة، وهي على نوعين:

1-معلومات صالحة لارتكاب الجريمة:

وهي الأفعال التي يكفي لتحقق النشاط الإجرامي قيام المجرم بإتيان أحد هذه الأفعال:

-التصميم:

هو الفعل الذي يقوم به المجرم المعلوماتي، وفي هذه الحالة هم المختصون في البرمجة وإعداد التطبيقات، وبعض هواة تصميم البرامج الذين اعتمدوا على أنفسهم في تنمية موهبة التصميم المعلوماتي لديهم، وأشهر البرامج التخريبية هي الفيروسات وبرامج الاختراق.

رغم أنّه هناك من يدافع على هؤلاء باعتبارهم يكشفون الثغرات الأمنية الموجودة في النظام المعلوماتي، وبالفعل فهم يفعلون ذلك ولكن هذا لا يبرر ما يقومون به كونهم يكشفون أمورا تتعلق بالحياة الخاصة لمالك النظام[2]بالإضافة إلى أن الكثير من برمجيات الفيروسات تخرج عن نطاق السيطرة وهو الحال مع دودة موريس[3].

-البحث:

يقصد به التنقيب والتفتيش عن المعطيات، وهو البحث عن هذه المعطيات ولذلك جاءت عبارة البحث بعد عبارة التصميم مباشرة وإن كان النص صياغته عامه[4].

---

[1] أمال قارة ،الحماية الجزائية للمعلوماتيةفي التشريع الجزائري،الطبعة الأولى،دار هومة،بوزريعة، الجزائر،2006، ص123.

[2] فايز محمد راجح غلاب ،المرجع السابق ،ص226.

[3] دودة موريس هو أول ظهور لجرائم الانترنت. احمد خليفة الملط، المرجع السابق،ص544

[4] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية،مصر،2007،ص201.

ويترتب على ذلك، أن البحث هنا يشمل كيفية تصميم البرامج وإعدادها لترتكب الجريمة، ويشمل البحث كل المعطيات المخزنة في المنظومة المعلوماتية التي يتم معالجتها آليا والمرسلة. ومن أمثلة ذلك، بطاقات الدفع والائتمان، أو حتى البحث عن بيانات شخصية لاستعمالها لاحقا لابتزاز الأفراد أو حتى المؤسسات، وهي مرحلة سابقة لارتكاب جريمة المساس بالمعالجة الآلية للمعطيات، وبالتالي جرائم الانترنت باعتبار أن جرائم المعالجة الآلية للمعطيات، هي من صور الإعلام والاتصال وهذا طبقا لنص المادة (02) من قانون(09-04).

-التجميع:

ويقصد به تجميع أكبر قدر ممكن من المعطيات التي يمكن أن ترتكب بها جريمة الدخول أو البقاء إلى نظام المعالجة الآلية للمعطيات، أو جريمة التلاعب في معطيات الحاسوب أو غيرها من الجرائم المعلوماتية المنصوص عليها، قد يكون بموجب برامج ذات كفاءة في التجميع،لا تتأثر بوجود الحماية الأمنية أي يقتضي الحصول على المعلومات من أجل استخدامها ،لذلك فالمجرم يبذل قدراته التقنية في الحصول عليها[1].

-التوفير:

وهو الوضع تحت التصرف المصطلح الذي استخدمته اتفاقية[2] بودابست حيث يعني "التوفير إلى عرض المعلومات وإتاحتها وجعلها في متناول الغير، بل وتحت تصرفه وحيازته"[3].

وعلى عكس من ذلك، التجميع الذي يكون متاحا سرا أو علنا، مثلا كلمات المرور لمجموعة من المواقع الإلكترونية،ومعلومات عن الاختراق والتسلل، والتصنت المتاحة إما مجانا أو بالمقابل ،على أنه يمكن إدراج العديد من المصطلحات التي تفيد معنى التوفير.

[1] بالرجوع إلى اتفاقية بودابست فقد استخدمت مصطلح "الحصول للاستخدام" ولكن ما معنى أن يجمع الشخص معلومات خصوصا باستخدام تقنيات الاختراق فهو دليل على سوء النية والقصد في ارتكاب هذه الجريمة.

[2] المادة 06 من اتفاقية بودابست.

[3] بوكر رشيدة،المرجع السابق ،ص282.

-النشر:

هو التوزيع الإيجابي للمادة المجرمة[1]ويقصد به "إذاعة المعلومات محل الجريمة وتمكين الغير من الإطلاع عليها وذلك مهما كانت طبيعتها"[2].

وبذلك فإن النشر هو إذاعة المعطيات بأي وسيلة كانت،وسينوي أن تكون معلومات صادقة أو كاذبة ،فالعبرة بالتجريم أنّها ،معطيات محمية جزائيا بغض النظر عن مدى مصداقيتها.

-الاتجار:

وهو مصطلح خاص بالمشرع الجزائري[3]، والذي ومن خلال قراءتنا لمواد الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي لم تتضمن هذا المصطلح، حيث أن ما ورد في الاتفاقية مصطلح البيع والاستيراد، كالاتجار بالمخدرات هو مجرم كذلك الاتجار بالمعطيات كذلك، وهو تقديم المعلومات للغير بدون مقابل، أي كان نقدي أو عيني أو عبارة عن خدمة.

فقد تكون المعلومات عبارة عن شفرة دخول، أو بيانات المرور أو أي بيانات تسمح بالولوج إلى كل أو جزء من النظام المعلوماتي بعد ارتكاب جريمة من الجرائم المعلوماتية[4].

2-التعامل بمعلومات متحصل عليها من الجريمة.

إن الاعتماد على البيانات أو التعامل فيها ،كما ذكرنا يأخذ صورتين الأولى هي ما ذكرنا سابقا أما الثاني فيتمثل في معلومات متحصل عليها من جريمة تقنية، وهو الصورة التي ذكرتها المادة (394مكرر)2 من ق.ع.ج في فقرتها الثانية، فيكفي سلوك صورة من الصور الآتية حتى تكون بصدد جريمة الاعتداء على المعطيات.

[1] هلالي عبد الإله،الجوانب الإجرائية الموضوعية والإجرائية لجرائم المعلوماتية ، المرجع السابق،ص124.

[2] محمد خليفة،المرجع السابق،ص203.

المادة(394مكرر2)ق.ع.ج تنص:"...1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق

[3] منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

[4] هلالي عبد الإله ، الجوانب الإجرائية الموضوعية والإجرائية لجرائم المعلوماتية ،المرجع السابق ، ص97.

-الحيازة:

تتحقق بسيطرة المجرم المعلوماتي على البيانات المتحصل عليها من جريمة الدخول أو البقاء في نظام المعالجة الآلية، أو غيرها من جرائم المعالجة الآلية للمعطيات التي نص عليها المشرع الجزائري"، وهي سيطرة واقعية وإدارية للحائز على المنقول تخوله الانتفاع به تعديل كيانه ،تحطيمه أو نقله فهي إذا سيطرة إدارية للشخص على الشيء"[1].

وفي هذا الصدد الأمر يتعلق بالمعطيات المتحصل عليها من جريمة، فأصل السلوك غير مشروع ،فالأولى أن تكون حيازة متحصلاته الإجرامية غير مشروعة حتى وإن لم يتم إفشاؤها.

وقد تكون المعطيات المتحصل عليها من الجريمة تتعلق بالدولة، وبالتالي فهي تمس بأمنها أو تمس بحياة الشخصية للأفراد ،وهو الحق المحمي بموجب الدستور. مع العلم أن المشرع لم يحدد نوع المعطيات المتحصل عليها من الجريمة ،ذلك أن نوع المعلومات التي يتعامل فيها والمتحصل عليها تحدد نوع الجريمة وآليات متابعتها لأنه طبعا إذا تعلق الأمر بالأمن الوطني وأسرار الدولة يختلف الأمر إذا تعلق الأمر بمعلومات تخص البيانات الشخصية.

- الإفشاء:

ربما أهم ما يسوء الضحية في الجرائم التقنية وبالضبط في محصلاتها الإجرامية هو الإفشاء، أي ايذاع كل المعلومات أو جزء منها متحصل عليها من الجريمة عبر الانترنت بحيث تصبح هذه المعلومات في متناول أكثر من شخص غير المجرم، بحسب الغرض منها.وبما أن الانترنت وسيلة إعلام واتصال في نفس الوقت، فيمكن التخيل لأي مدى سوف تنتشر هذه المعلومات[2].

[1] محمد زكي أو عامر، قانون العقوبات القسم الخاص ،الدار الجامعية للطباعة والنشر ،بيروت 1990 ، ص148. هامش مشار إليه لدى رشيدة بوكر ، ص285.

[2] موقع ويكلكس
https://ar.wikipedia.org/wiki/%D9%88%D9%8A%D9%83%D9%8A%D9%84%D9%8A%D9%83%D8%B3

-النشر:

إن تكنولوجيات الإعلام والاتصال هي وسائل للنشر متطورة بسرعة، وهذه الوسيلة هي من أهم وسائل الاعتداء على الحياة الخاصة عبر الانترنت، طبعا للمعطيات التي يتم التحصل عليها بطريقة غير مشروعة، عن طريق الاختراق ويتم فعل النشر عن طريق أية وسيلة كانت.

-الاستعمال:

إنّ الأخطر من جميع الأفعال السابقة هو استعمال البيانات المتحصل عليها وما تحتويه من معلومات وأسرار، والأمثلة في ذلك كثير كالاستعمال للابتزاز أو الحصول على الأموال فهو ينتقل من مجرد احتمال ارتكاب الجريمة بعد تحقق الأفعال السابقة إلى سلوكها فعلا بعد استعمال المعطيات[1].

وهذا وقد وسع المشرع من دائرة التجريم إلى كل استعمال للمعلومات مهما كان الهدف منه ومهما كان نوعه، وهو ما يستفاد من عبارة " أو استعمال لأي غرض كان "[2]. والملاحظ أن المشرع الجزائري وإدراكا منه لخطورة هذه الأفعال لم يأخذ بعين الاعتبار عدد مرات تكرار الأفعال مما يعني انه يكفي أن يرتكب الفعل مرة واحدة ليكون السلوك مجرما.

ج-الركن المعنوي

إن جريمة التعامل مع المعطيات غير المشروعة هي جريمة غير عمدية في صورتها وفقا لنص المادة (394مكرر2) حيث ورد لفظ عمدا وعن طريق الغش وبذلك لابد من توافر القصد العام والقصد الخاص.

وليتحقق القصد العام: لابد من اكتمال عنصريه العلم والإرادة. أما العلم، أن يحيط المجرم علما بكافة العناصر أي يعلم بان المعلومات غير مشروعة وان استعمالها أو نشرها أو فشاءها أو المتاجرة بها، هو سلوك غير مشروع يحمل في طياته اعتداء على مصلحة محمية قانونا، وبالتالي فان انتفاء

[1] فايز محمد راجح غلاب،المرجع السابق، ص237.

[2] المادة(394مكرر2)ق.ع.ج.

العلم ينتفي به القصد الجنائي لذلك فان الصورة الثانية من هذه الجريمة هي التعامل في البيانات المتحصل عليها من جريمة تجعل من المنطقي أن يكون توافر القصد الجنائي العام كافيا لقيام الجريمة ومتابعة المجرم. وان ما يدل على أن المشرع اكتفى بالقصد العام فقط، هو في الصورة الثانية دون الأولى وذلك بقوله" مهما كان الغرض من الأفعال المكونة لها".

أمّا الإرادة، يجب أن تتجه إرادة المجرم الحرة إلى إتيان السلوك الإجرامي، والمتمثل في الأفعال سالفة الذكر.

غير انه، فإنه لا يكفي لقيام الجريمة في صورتيها التعامل في معلومات صالحة لارتكاب جريمة، وأن يتوافر لدى الفاعل القصد الجنائي العام، بل يلزم أن يتوافر القصد الجنائي الخاص، أي اتجاه العلم والإرادة إلى وقائع لا تدخل في تكوين أركان الجريمة.

ويتحقق القصد الجنائي الخاص في التعامل بالمعطيات التي ترتكب بها جريمة ويتحقق ذلك بالتمهيد والإعداد لاستعمالها في ارتكاب الجريمة، وهو ما يتعلق بنفسية المجرم. أما استعمال المعطيات في ارتكاب الجريمة فليس ركنا في هذه الجريمة فقد لا يقوم احد باستعمال هذه المعطيات، ولكن مع ذلك تقوم الجريمة[1].

وبالتالي، فإن جريمة تقوم إذا كانت بنية استخدام الأساليب أو الأفعال المذكورة على سبيل الحصر، لأنه من غير معقول قيام جريمة بأفعال معينة دون أن يكون بسوء نية حيث أن نفس الأفعال قد تستعمل لأغراض مشروعة باعتبارها مزدوجة الاستعمال[2].

ثالثا– جريمة الاعتداءات العمدية على سير نظم المعالجة الآلية للمعطيات:

وهي الجريمة التي مفادها الاعتداء العمدي على نظام المعالجة الآلية للبيانات كافة الأفعال التي من شانها أن تؤدي إلى الإعاقة أو إفساد النظام وتسبب في بطء عمله أو إيقافه عن التشغيل.

[1] محمد خليفة، المرجع السابق، ص213.

[2] رشيدة بوكر، المرجع السابق، ص298.

والواقع أن المشرع الجزائري لم ينص على هذه الجريمة بنص تجريمي مستقل، بل جرم الآثار الناجمة عنها من إفساد وتعطيل وإتلاف والواردة في نص المادة (394مكرر1) و(394 مكرر)ق.ع.ج.

المطلب الثاني:الإجرام غير ألمعلوماتي في التشريع الجزائري.

وهي جرائم الانترنت تعتمد على شبكة الانترنت وتكنولوجيات الإعلام والاتصال كوسيلة لارتكاب الجريمة، والتي ذكر المشرع الجزائري في نصوص القانونية الخاصة بها كلمة تقنية أو انترنت أو تكنولوجيات الإعلام والاتصال والتي أثرنا بدراسة جريمتين فقط، وهي الإرهاب الالكتروني وإهانة رئيس الجمهورية، هناك من الجرائم التي ذكرها المشرع في القانون(09-04) والتي اعتبر فيها بعض الجرائم المتعلقة بالدفاع الوطني وامن الدولة والاقتصاد الوطني من جرائم الانترنت التي تكون فيها تكنولوجيات الإعلام والاتصال وسيلة لارتكابها. .

الفرع الأول: جريمة الإرهاب الالكتروني

يمكن تعريف الإرهاب الإلكتروني بأنه العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، وذلك باستخدام الموارد المعلوماتية والوسائل الإلكترونية[1].فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية من أجل تخويف وترويع الآخرين

وبهذا، تعد جريمة الإرهاب الالكتروني من الجرائم العمدية التي يتوجب توافرها على الأركان العامة المتمثلة في الركن الشرعي(أولا)، الركن المادي(ثانيا)، ثم الركن المعنوي(ثالثا).

[1] عبدالله بن عبدالعزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات،بحث مقدم إلى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت،القاهرة ،جمهورية مصر العربية،في 2-4 جوان 2008 ، ص 16-19.

أولا: الركن الشرعي

خصَ المشرع الجزائري المادة (87 مكرر1) م قانون العقوبات[1]، المضافة بالأمر(95-10)[2] بتعريف الفعل الإرهابي أو التخريبي، فجاء نصُّها على النحو الآتي: " يعتبر فعلا إرهابيا أو تخريبا في مفهوم هذا الأمر كل فعل يستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يأتي:

بث الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء المعنوي أو الجسدي على الأشخاص أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو المس بممتلكاتهم.

- عرقلة حركة المرور أو حرية التنقل في الطرق و التجمهر أو الاعتصام في الساحات العمومية.
- الاعتداء على رموز الأمة والجمهورية ونبش أو تدنيس القبور.
- الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون مسوغ قانوني.
- الاعتداء على المحيط أو إدخال مادة أو تسريبها في الجو أو في باطن الأرض أو إلقائها عليها أو في المياه بما فيها الإقليمية من شأنها جعل صحة الإنسان أو الحيوان أو البيئة الطبيعية في خطر.
- عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام.
- عرقلة سير المؤسسات العمومية أو الاعتداء على حياة أعوانها أو ممتلكاتها أو عرقلة تطبيق القوانين والتنظيمات ".

[1] أمر رقم (66-156)المؤرخ في 18 صفر عام 1386 هـ الموافق ل 08 يونيو سنة 1966 يتضمن قانون العقوبات.

[2] أمر رقم(95-10)المؤرخ في 25 رمضان 1415 هـ الموافق ل 25 فبراير 1995 المعدل والمتمم للأمر رقم 66- 155 المؤرخ في 08 يونيو 1966المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 11ليوم29 رمضان 1415 هـ الموافق ل 25 فبراير 1995.

ذلك بالإضافة إلى أن وصف الجريمة الإرهابية أو التخريبية يكون على إنشاء أو تنظيم جمعية أو تنظيم جماعة أو منظمة، الغرض منها القيام بفعل إرهابي أو تخريبي، ويوصف بنفس الوصف الانخراط أو المشاركة في تلك التنظيمات أو الجمعيات مهما كان شكلها.

كما يضاف إلى الأفعال الموصوفة بالإرهابية أو التخريبية الإشادة أو تشجيع أو تمويل الأفعال الإرهابية أو التخريبية مهما كانت الوسيلة في ذلك.

وتأخذ هذا الوصف إعادة طبع أو نشر الوثائق أو المطبوعات أو التسجيلات التي تشيد بالأفعال الإرهابية أو التخريبية.

وتأخذ أيضا نفس الوصف كل جزائري ينخرط في الخارج في جمعية أو جماعة أو منظمة مهما كان شكلها وتكون إرهابية أو تخريبية، حتى ولو لم تكن أفعالها موجهة ضد الجزائر.

أيضا تأخذ وصف الجريمة الإرهابية أو التخريبية حيازة أسلحة ممنوعة أو ذخائر و الاستيلاء عليها أو حملها أو الاتجار فيها أو استيرادها أو تصديرها أو صنعها أو تصليحها أو استعمالها دون رخصة من السلطة المختصة .

أيضًا يحمل نفس الوصف بيع أسلحة بيضاء أو شراؤها أو توزيعها أو استيرادها أو وضعها عن علم لأغراض مخالفة للقانون[1].

ويحمل نفس الوصف فعلان آخران وردا في المادة (87 مكرر10) أضافها القانون رقم01-09 المؤرخ في 26-06-2001[2]، وهما انتحال صفة إمام مسجد واستعمال المسجد مخالفة لمهمته النبيلة بوجه عام .

وكذا من خلال المادة (394مكرر3) والتي اعتبرت ظرف مشدد حين تستهدف الجرائم التقنية الدفاع الوطني أو الهيئات والمؤسسات المتعلقة بالقانون العام ، وهي أي الانترنت أو

[1] المواد 87 مكرر 2 ،3 ،4، 5،6 ،7 من ق.ع.ج.

[2] قانون رقم(01-09) مؤرخ في 4 ربيع الثاني عام 1422الموافق 26 يونيو سنة 2001،يعدل ويتمم الأمر (66-156) المؤرخ في 18 صفر عام 1386 الموافق8 يونيوسنة1966 والمتضمن قانون العقوبات،ج.ر رقم 34 ليوم 27 يونيو سنة 2001،ص2.

تكنولوجيات الإعلام والاتصال تدخل تحت عبارة " أي وسيلة كانت" التي استخدمت في المادة 87 مكرر من قانون العقوبات سالفة الذكر.

والمادة (87مكرر12):"يعاقب بالسجن المؤقت من خمس(5) سنوات عشر(10) سنوات وبغرامة من 100.000 دج الى500.000 دج،كل من يستخدم تكنولوجيات الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أن تقع أنشطتها تحت طائلة أحكام هذا القسم، أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو بنشر أفكارها بصورة مباشرة أو غير مباشرة."

وهذا بعد التصعيد الذي عرفته الأعمال الإرهابية بمساعدة الانترنت أو تكنولوجيات الإعلام والاتصال، حيث إنّ الإرهاب الالكتروني يتميز عن غيره بالطريقة العصرية والوسائل الالكترونية،كما يشير الإرهاب الالكتروني إلى عنصرين فضاء الانترنت والإرهاب[1]، وهو ما جسده المشرع قبل ذلك في القانون (09-04) السالف الذكر في المادة 4 منه، والذي سمح باللجوء إلى مراقبة الاتصالات الالكترونية وهذا للوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة، وفي حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة، أو الدفاع الوطني أو النظام العام.

وبالتالي قام المشرع الجزائري بالتأكيد على لجوء السلطات المختصة إلى كل أساليب التحري الخاصة، حين يتعلق الأمر باستخدام الانترنت كوسيلة لارتكاب السلوك الإجرامي، لكنه قام بتعديل ما خص الجرائم الإرهابية فقط دون الجرائم الأخرى، وإذا أخذنا بهذا الطرح فان أي مادة في قانون العقوبات والقوانين الخاصة والتي تحتوي نصوصها القانونية، عل مصطلح و"بأي تقنية كانت" هي من الجرائم التي يمكن ارتكابها عبر الانترنت وصالحة لان تكون الإجراءات الخاصة من بين وسائلها في التحقيق ولكن بأي ضمانات.

[1] علي عدنان الفيل، الاجرام الالكتروني،دراسة مقارنة، منشورات زين الحقوقية،الطبعة الأولى، 2011، ص61.

ثانيا: الركن المادي لجريمة الإرهاب الالكتروني.

يتكون الركن المادي من السلوكيات الإجرامية التي تستخدم فيها تكنولوجيات الإعلام والاتصال في ارتكابها، وهذا باستخدام الانترنت بمواقع التواصل الاجتماعي كالفايس بوك.

وقد تم تحديد هذه الأفعال تجسيدا منه لارتكاب الجريمة الإرهابية عبر شبكة الانترنت وهو ما يعرف بالإرهاب الالكتروني، والذي يتجسد في ثلاثة أنواع هي: إرهاب الأفراد، إرهاب المؤسسات، وإرهاب ضد الدول[1] بموجب القانون (16-02) سالف الذكر المواد على التوالي(87مكرر11):"يعاقب بالسجن المؤقت من (5) سنوات إلى عشر(10) سنوات وبغرامة من 100.00الى 500.000، كل جزائري أو أجنبي مقيم بالجزائر، بطريقة شرعية أو غير شرعية يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها.

يعاقب بنفس العقوبة كل من:

-يوفر أو يجمع عمدا أموالا بأي وسيلة وبصورة مباشرة أو غير مباشرة، بقصد استخدامها أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض ارتكاب الأفعال المذكورة في الفقرة الأولى من هذه المادة.

-قيام عمدا بتمويل أو تنظيم سفر أشخاص إلى دولة أخرى، بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تسهيل ذلك السفر.

-يستخدم تكنولوجيات الإعلام والاتصال لارتكاب الأفعال المذكورة في هذه المادة".

جاءت هذه المادة تقنينا لبعض الأفعال التي تستخدمها الجماعات الإرهابية من اجل القيام بأعمالها الإجرامية، فربما كان من المفيد أن يضيف المشرع الوسيلة وهي الانترنت للسلوكيات الإجرامية المكونة للركن المادي لجرائم الإرهاب ويضيف لها باقي السلوكيات أو بالأحرى الظواهر

[1] عبد الحكيم رشيد توبة، المرجع السابق،173 -175.

التي ظهرت حديثا من تجنيد للشباب والقصر والنساء، للالتحاق بالجماعات الإرهابية خصوصا خارج الوطن بالإضافة إلى التمويل والتدريب وحتى صنع الأسلحة والقنابل.

ثالثا: الركن المعنوي لجريمة الإرهاب الالكتروني

استبعد المشرع الجزائري من عناصر المكونة لجريمة الإرهاب الالكتروني، البواعث والدوافع والأغراض[1]، وهذا ما جسدته المادة (87مكرر11) المذكور أعلاه، حيث انّه لابد على من يقدم على استخدام التكنولوجيات الحديثة للإعلام والاتصال أن تتوافر لديه النية لتوفير الأموال وجمعها عبر الانترنت بأي طريقة كانت، من دعوة أو إشهار أو حتى ابتزاز والمساعدة في سفر الأشخاص، لذلك كل هذه السلوكيات لا تكون أبدا ضمن أعمال الإهمال، على انّ المتابعة المستمرة والمتواصلة لمواقع الكترونية وصفحات خاصة بالجماعات المتطرفة والإرهابية، يعد تأييدا لتلك الجماعات لان الأكيد أن الشخص لن يسال أو يتابع قضائيا من ضغط زر الإعجاب لمرة واحدة فقط على الانضمام إلى جماعة إرهابية عبر الانترنت.

أمّا الجريمة الثانية التي ذكرت فيها الوسائل المعلوماتية والتقنية صراحة والتي تدخل في نطاق الدراسة هي جريمة إهانة وسب وقذف رئيس الجمهورية.

الفرع الثاني: جريمة إهانة وسب وقذف رئيس الجمهورية.

إن جريمة الإهانة أو إهانة رئيس الجمهورية[2]الذي يعتبر ركن مفترض في هذه الجريمة تقوم على الادعاء بالواقعة أو إسنادها للغير وتحقق القصد الجنائي، فبعد ظهور المواقع الالكترونية

[1] جلال محمد الزعبي، وأسامة احمد المناعسة، المرجع السابق،276.

[2] بالنسبة لرؤساء الدول الأجنبية، فان المادة (123) من قانون العضوي الإعلام (12-05) سالف الذكر بقولها"يعاقب بغرامة من خمسة وعشرين ألف دينار(25.000دج) إلى مائة ألف دينار(100.000دج) كل من أهان بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي،رؤساء الدول الأجنبية وأعضاء البعثات الدبلوماسية المعتمدين لدى حكومة الجمهورية الجزائرية الديمقراطية الشعبية".

[1]"الواب web".على شبكة الانترنت ،أصبح لها دور فعال في تفشي الإجرام،ووسيلة ترتكب بها الجريمة.

تقوم هذه الجريمة على أركان تفصيلها فيما يلي:

أولا:الركن الشرعي.

يتمثل هذا الركن في المادة(144مكرر) من ق.ع.ج، والتي تم استحداثها بموجب تعديل قانون العقوبات لسنة2001[2]، وهي من النصوص التي كانت امتداداً لحماية الموظف بوجه عام، من موظفين عموميين وقضاة...، لذلك كان لابد من حماية رئيس الجمهورية باعتباره القاضي الأول للبلاد، القائد الأعلى للقوات المسلحة وزير الدفاع غير أنّه هناك اختلاف بين إهانة رئيس الجمهورية وباقي فئات الموظف والتي هي تتمثل في الوسيلة المعلوماتية.

لذلك، يحبذ أن يعيد المشرع الجزائري وخصوصا ما تعلق بالجانب الجزائي إعادة صياغة النصوص القانونية بإضافة العبارة:" أي تقنية أو معلوماتية أو الكترونية أو تكنولوجيات الإعلام الاتصال"، وهذا لكي لا تتخطى السلطات المختصة استعمال الإجراءات الخاصة مبدأ مهما هو مبدأ الشرعية الإجرائية في عمليات التحقيق والتحري.

ثانيا: الركن المادي

ينقسم الركن المادي إلى مضمون التعبيروسند التعبير[3].

أ- مضمون التعبير أو الإهانة:

طبقا لنص المادة(144مكرر) من ق.ع.ج يكون مضمون التعبير والمكون للركن المادي لجريمة الاهانة رئيس الجمهورية هو السب والقذف والإهانة نفسها، وهي المصطلحات التي عرفها المشرع

[1] الموقع:"إمكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد" المادة (2) من الاتفاقية العربية لمكافحة جرائم التقنية، المصادق عليها بالمرسوم الرئاسي رقم(14-252) مؤرخ في 13ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014 .

[2] القانون رقم(01-09) سالف الذكر.

[3] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص،المرجع السابق،257 .

في المواد التي جرم فيها السب والقذف، وتعرف المادة(296) من ق.ع.ج القذف على النحو التالي: " يعد قذفا كل إدعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيآت المدعى عليها بها أو إسنادها إليهم أوالى تلك الهيأة " .

وتضيف نفس المادة في شطرها الثاني:" يعاقب على نشر هذا الإدعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولم تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيأة دون ذكر الاسم ولكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة"

أمّا السب هو ما عرفته المادة (297) من ق.ع.ج" يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة"

أما الاهانة فهي الانتقاص من الاحترام لاعتبار شخص رئيس الجمهورية، ولا يتحقق هذا الركن إلا بتوافر العلانية والتي تتمثل في الجهر والإذاعة السب والقذف أمام الجمهور بوسيلة الكترونية أو معلوماتية أو إعلامية[1]

ب– سند التعبير أو الوسيلة المستعملة: تقضي جريمة الإهانة أن تتم بوسائل معينة، ولكن منذ تعديل(01-09)[2] أصبحت الوسيلة تختلف حسب صفة الشخص أو الهيأة المحمية.

أمّا الإهانة الموجهة لشخص رئيس الجمهورية بالمادة (144مكرر) فيمكن أن تتم بإحدى الوسائل التي تتحقق معها العلنية[3]، رغم أن هذا الشرط لم يشر إليه المشرع الجزائري في هذه الجريمة، حيث نصت المادة (144مكرر) ق.ع.ج "...كل من أساء لرئيس الجمهورية بعبارات

[1] مدحت رمضان، المرجع السابق،ص90-91.

[2] القانون(01-09) سالف الذكر.

[3] تحقق العلانية إذا تم نقل الكلام أو الصوت عن طريق الوسائل الآلية ، وهو ما تتيحه الانترنت من نقل الصوت والصورة الساكنة والمتحركة لمستخدم لآخر وآخر مع العلم أن المشرع لم يحدد زمان ومكان هذا النقل. محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع،عمان الأردن،2009،ص51و52.كما أن الانترنت بجميع تطبيقاتها يمكن أن تصل إلى الأماكن الخاصة وسواء تلقى المستخدم هذه الصور وغيرها في مكان عام أو خاص فالعلانية تتحقق،مدحت رمضان ،جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، مصر، ص93.

تتضمن إهانة ...وكان ذلك عن طريق الكتابة أو الرسم أو التصريح أو أية آلية لبث الصوت والصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى".

وتأسيسا على ذلك، لا تقع جنحة الإهانة إلا بواسطة الوسائل المذكورة والتي وسع فيها المشرع فهي تشمل كل الوسائل العادية والمتطورة. وبالتالي تكنولوجيات الإعلام والاتصال وسواء كانت رسومات أو كتابات أو تصريحات أو صور أو وسائل الكترونية ومعلوماتية وعلى رأسها الانترنت، وأهمها على الإطلاق مواقع التواصل الاجتماعي[1].

ثالثا: الركن المعنوي

تعتبر جنحة الإهانة من الجرائم العمدية التي تقتضي توافر علم الجاني بصفة الضحية أي انه رئيس الجمهورية، واستهدافها اعتبارا لتلك الصفة، قاصدا المساس بشرف أو اعتبار الضحية، وتعد هذه الجريمة من الجرائم العمدية التي يقتضي توافر القصد العام والقصد الخاص لقيامها.

ويتمثل القصد العام في علم الجاني بصفة الضحية واستهدافها اعتبارا لتلك الصفة أما القصد الخاص فيتمثل في نية المساس بالشرف أو الاعتبار أو الاحترام الواجب[2].

أما الجزاء الجنائي،فقبل تعديل المادة(144 مكرر) ق.ع.ج بموجب القانون (11-14)[3] ،كانت العقوبة المقررة عن ارتكاب جريمة الإساءة إلى رئيس الجمهورية، تتمثل في الحبس من 03 أشهر إلى12شهر،وغرامة من 50.000 د.ج إلى 500.000 د.ج أو بإحدى هاتين العقوبتين فقط.

كما نصت نفس المادة على أحد أسباب تشديد العقوبة و هي حالة العود التي تضاعف فيها الغرامة.

---

[1] لا باس في هذه النقطة إدراج بعض القضايا المتعلقة بتهمة إهانة رئيس الجمهورية عبر مواقع التواصل الاجتماعي يرجى الإطلاع على الرابط http://www.elkhabar.com/press/article/101843 ، تاريخ الإطلاع:6 مارس 2016.

[2] أحسن بوسقيعة، المرجع السابق، ص. 226.

[3] (11-14) مؤرخ في 2 رمضان عام 1432 الموافق ل 2 غشت سنة 2011 ،يعدل الأمر رقم(66-156) المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو 1966 والمتضمن قانون العقوبات،ج.ر رقم44 ليوم 10 غشت سنة 2011 ،ص04.

نفس هذه العقوبات توقع في حالة إذا كانت الإهانة قد ارتكبت بواسطة نشرية يومية أسبوعية أو شهرية أو غيرها، على مدير النشرية و رئيس تحريرها و على النشرية نفسها طبقا لنص المادة (144مكرر1) ق.ع.ج،لكن بعد التعديل ألغى المشرع الجزائري المادة (144مكرر1) ق.ع.ج، كما ألغى عقوبة الحبس من نص المادة(144مكرر) ق.ع.ج

و أبقى فقط على الغرامة مع الرفع منها، و بذلك أصبحت توقع على مرتكب جريمة الإساءة إلى رئيس الجمهورية حالياً الغرامة من 100.000 د.ج إلى 500.000 د.ج.

وبعد دراسة جرائم الانترنت واهم الخصائص المرتبطة بها، وكذا أنواعها بما نص عليه المشرع الجزائري، نواصل الدراسة لتسليط الضوء على أدلة الإثبات المناسبة لمثل هذه الجرائم في الفصل التالي.

الفصل الثاني:أدلة إثبات جرائم الإنترنت في التشريع الجزائري.

الإثبات هو العملية المتكاملة التي تهدف إلى البحث عن الأدلة التي تثبت حدوث الواقعة الجرمية[1]، ومن أهم المظاهر التي جعلت الفقهاء ورجال القانون بما فيهم سلطات الضبط والتحقيق القضائي، يتفطنون إلى ظهور جرائم جديدة مستحدثة، اختلاف الأدلة الحاصلة منها عن الأدلة العادية، من حيث محل الدليل وشكل الدليل نفسه، وكذا تعاظم حجمه، فوجود دليل لا مادي مختلف عن الأدلة الموجودة ، أدى إلى إختلاف نوع الجرائم وإختلاف دليلها.

الأصل حرية الإثبات في المواد الجزائية هو الذي سمح بقبول العديد من الأدلة العلمية،كأدلة في المواد الجزائية ، ماعدا ما أستثني بنص وقُيّد بدليل، لا يقبل دليل في جرائم الإنترنت إلاّ ماكان بشكل إلكتروني مدعم بأدلة أخرى، ووفق نص المادة (212) من ق.ا.ج.ج: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص.ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه"، وهي الحالة المتعلقة بإثبات جريمة الزنا[2]، وكما يستبعد الدليل المستنبط من مراسلات المحامي[3] ، كما انّه تقرر قوة ثبوتية لبعض

[1] محمد محمد محمد عنب، استخدام التكنولوجيا الحديثة في الإثبات، القاهرة ،مصر،2007 ،ص09.

[2] لإثبات جريمة الزنا:المادة (341)ق .ع.ج الدليل الذي يقبل عن ارتكاب الجريمة المعاقب عليها بالمادة (339) يقوم إما على محضر قضائي يحرره احد رجال الضبط القضائي عن حالة تلبس وإما وارد في رسائل أو مستندات صادرة من المتهم وإما بإقرار قضائي.والمادة من ق.ا.ج.ج

[3] المادة (217) من ق. ا .ج .ج "لا يستنبط الدليل الكتابي من المراسلة المتبادلة بين المتهم ومحاميه".

المحاضر التي لا تقبل الطعن فيها إلا بالتزوير[1]، والأكيد أن إثبات المسائل غير الجزائية يحترم فيها الإثبات المنصوص عليه في المواد المراد إثباتها طبيعة المعاملة.

يعتبر الدليل الجنائي الإلكتروني أو كما أطلق عليه المشرع الجزائري الدليل في الشكل الإلكتروني (المبحث الأول) بموجب المادة (16)من القانون (09-04) ، من الأدلة العلمية التي لها خصائص معينة ، بالمقابل وجود هذا الدليل مسرحه العالم الإفتراضي ، لدى كان لابدّ من وجود دعائم لاستكمال الإثبات في مواد جرائم الإنترنت فشهادة الشهود والمعاينة وغيرها من طرق الإثبات الجنائي لها دور فعال في إثبات جرائم الإنترنت ، إلا أنّ ذلك يبدو قاصر في ملاحقة مجرم الإنترنت [2] أو دعائم الإثبات الجنائي في جرائم الإنترنت (المبحث الثاني) والذي لا يكتمل الاثبات في هذا النوع من الجرائم إلاّ بها.

المبحث الأول:ماهية الدليل الجنائي الالكتروني.

مما لاشك فيه أنّ الدليل الجنائي الإلكتروني يتمتع بالحداثة النسبية، بإعتباره وليد لتكنولوجيات الإعلام و الإتصال، وبالتحديد المنظومة المعلوماتية وشبكة الإنترنت، لذا فانّ الاهتمام بالأدلة الرقمية أو الإلكترونية في تزايد، وهو علم من العلوم الحديثة حيث يهدف إلى معرفة كيفية حفظ الأدلة وجمعها وتقديمها إلى القضاء حتى تكون مقبولة[3]، ودراسة الدليل الجنائي الإلكتروني من المواضيع التي حضت باهتمام وافر من طرف خبراء الأمن المعلوماتي، قبل أن يكون اهتمام دارسي القانون به كدليل في جرائم الإنترنت، ذلك أنّه يتميز بصبغة تقنية بحتة تجعل القضاء دائما في حاجة إلى خبير لإعطاء رأيه، وهذا كحال الأدلة الحديثة نسبيا والمستحدثة كالبصمة الوراثية ، ومن المعلوم أنّ لكل دليل خصائص تميزه عن باقي الأدلة ، إلا أنّ مصادره –مصادر

[1] المادة (218)من ق. ا. ج .ج"إنّ المواد التي تحرر عنها محاضرها حجيتها إلى أن يطعن فيها بالتزوير تنظمها قوانين خاصة".

[2] عمر عيسى الفقي،الجرائم المعلوماتية، المكتب الجامعي الحديث الإسكندرية، مصر، 2006،ص89.

[3] فهد عبد الله العبيد العازمي، المرجع السابق،ص345.

الحصول عليه- قد جمعت بين مكونات المنظومة المعلوماتية والمتدخلين في شبكة الإنترنت ،لذا و تفاديا للتكرار سوف نتجنب المواضيع السابقة التي تم شرحها في هذه الأطروحة والتي وردت في سياق الفصل الأول وعلى رأسها المجرم، كمصدر للدليل الجنائي الالكتروني.

ومما سبق سوف نخصص(المطلب الأول) الدليل الجنائي الإلكتروني، يليه مصادر الدليل الجنائي الإلكتروني في(المطلب الثاني).

المطلب الأول: الدليل الجنائي الإلكتروني.

حظيت جرائم الإنترنت بالاهتمام من طرف المشرع الجزائري بداية من سنة الفين وأربعة بتعديل قانون العقوبات، وهذا بسبب انتشار تكنولوجيات الإعلام الاتصال، إلا أنّ الدليل الجنائي في شكله الإلكتروني لم يحظ بنفس الاهتمام الّا سنة ألفين وتسعة، بعد أن تعاظم دور الإنترنت في شتى مناحي الحياة، لذا لم يستطع المشرع تجاوز ذلك، فأقر إجراءات خاصة للكشف عنه وتخزينه، حيث انّه من نفس الوسط أي العالم الافتراضي اللامادي.

مع ملاحظة انه قد يكون الدليل الجنائي الإلكتروني متضمنا إثبات الجريمة ومرتكبيها معا، وعادة ما يكون جسم الجريمة عبر الإنترنت عادة هو الدليل الجنائي ذاته[1]، وقد يكون هذا الجسم الدليل الجنائي الإلكتروني متضمن ما يفيد نسبة الجريمة لشخص ما ، كما لو أرسل شخص لأخر رسالة عبر البريد الإلكتروني تتضمن فيروسات تؤدي إلى إتلاف الموقع الإلكتروني الخاص بذلك

[1] مثلا القيام بالجريمة عن طريق القنابل المنطقية هذا النوع من القنابل أي المنطقية هو برنامج خبيث صغير يتم إدخاله، وبمجرد حدوث واقعة تم إدخال بيانات يشتغل البرنامج ، ويمكن أن يخرب المنظومة المعلوماتية، والأصل أن البرنامج هو احد صور القنبلة المعلوماتية والتي تنقسم بدورها إلى القنبلة المنطقية سالفة الذكر، والقنبلة الزمنية التي تنشط في تاريخ معين محدد بالذات أي محدد بالساعة واليوم والوقت اللازم،وتعرف القنبلة المعلوماتية بأنها برنامج خبيث يتم إدخاله بطرق غير مشروعة وخفية مع البرامج وهي عبارة عن مجموعة من الملفات التي يتم تقسيمها حتى لا يمكن التعرف عليها وبمجرد توافر الشروط الزمنية والمكانية كاليوم أو انجاز أمر معين تبدأ عملها في تخريب المنظومة المعلوماتية ، والشبكات وهي عبارة عن شفرة موقوتة يستخدمها في مواجهة المؤسسات التي يعملون بها بغرض حماية أنفسهم ضد الطرد من العمل،عمر ابو بكر بن يونس ،المرجع السابق، ص371و372، محمد أمين شوابكة، المرجع السابق،ص240و241، محمد سامي الشوا ،المرجع السابق، ص50.

الشخص ، فان هذه الرسالة بذاتها تعد دليلا على وقوع الجريمة ، وفي نفس الوقت تعد دليلا على نسبة إرتكابها لشخص معين وهو المرسل إذا تضمنت بيانات تدل على شخصه[1].

الفرع الأول:تعريف الدليل الجنائي الالكتروني.

إن الدليل الجنائي الالكتروني هو من الأدلة الجنائية التي لها من الخصائص ما يميزها عن باقي الأدلة ولكن لابد لنا من تعريف الأصل وهو الدليل الجنائي، ثم تعريف الدليل الجنائي في شكله الالكتروني كما أطلق عليه المشرع الجزائري فيما يلي.

أولا: الدليل الجنائي.

هو " معلومة يقبلها المنطق والعقل يتم الحصول عليها بإجراءات قانونية ووسائل فنية أو مادية ، أو قولية، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص ما، له علاقة بجريمة أو جان أو مجني عليه".[2] أو هو" الأثر المنطبق في نفس أو شيء ناتج عن جريمة وقعت أو على وشك الوقوع، من جهة ومن جهة أخرى الأثر الذي ينطبق على شخص محدد صَدَرَ عنه السلوك الإجرامي"[3].

تقسم الأدلة الجنائية إلى عدة أقسام فهناك الأدلة القانونية وهي الأدلة التي حددها القانون، وحدد حالات استعمالها وحجيتها كبعض المحررات من المحاضر الرسمية التي يحررها أشخاص مختصون كمحاضر الجمارك ومديرية التجارة، و هناك الأدلة الفنية وهو الدليل الذي اقره رأي خبير

[1] طارق الجملي،الدليل الرقمي في مجال الإثبات الجنائي، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا ، طرابلس، ليبيا من 28- 29 / 10 / 2009 ،ص 49.

[2] محمد أمين البشري ،التحقيق في الجرائم المستحدثة ،بدون طبعة ،جامعة نايف العربية للعلوم الأمنية – الرياض – المملكة العربية السعودية ،2004 ،ص 231.

[3] Jean Larguier, Philippe Conte, Procédure pénale 22e, édition ,2010,Dalloz,Paris.p334

وفق معايير قانونية وعلمية معينة، والأدلة القولية وهي الأدلة الصادرة عن أشخاص تؤثر في اقتناع القاضي.

والملاحظ أنّ الكثير من رجال القانون يلتبس عليه الأمر فيما يخص الدليل وبعض المصطلحات أو المفردات التي تعطي المعنى نفسه، كالدليل ووسيلة الإثبات أو الدليل والإثبات نفسه ، فالدليل هو ما عرفناه سابقا أمّا وسائل الحصول عليه فهي " الإجراءات المعرّف بها والتي يتم من خلالها الوصول إلى الدليل فهي ما ينتج عنها الدليل ومثالها التفتيش والمراقبة والمعاينة [1] ، إذاً أن كل الإجراءات السالفة الذكر بالإضافة إلى أخرى كالتسرب والتقاط الصور هي عبارة عن وسائل للوصول إلى الجاني ، طبقا لشروط معينة وفي إطار احترام الحقوق والحريات.

هناك علاقة وطيدة بين الدليل والإثبات، حتى يعتقد أنّهما مفردتان مترادفتان فالدليل " يتكون من حقائق متنوعة تقدم للمحكمة ولكن نتيجتها هي الإثبات "[2]، وبالتالي فإن هذه الحقائق تمثل الأدلة المقدمة أمام جهات الحكم ، لذلك فإن الإثبات هو أعم وأشمل من الدليل نفسه ، فالدليل وجمعه هو مرحلة من مراحل العملية الإثباتية[3].

أمّا الدليل والأثر، الواقع أنّ الأثر المتخلف عن الجاني في مسرح الجريمة ، يمكن أن يتحول إلى دليل، إذا تم الاستفادة منه واستقراء مدلوله واستنباط مكوناته ، يصبح قرينة على أمر ودليلا على شئ[4]، فهو كل شكل أو صورة أو علامة يتركها المشتبه فيه على جسم معين ، هنا تعلق الأمر بالآثار المادية أو غير المادية على المسرح الواقعي للجريمة أو الإفتراضي، وإذا تم التعرف على مدلوله ، فإنه وقت إذاً يصبح دليلا[5].

[1] محمد أمين البشري ،المرجع السابق ، ص232.

[2] محمد أمين البشري ،المرجع السابق ، ص232.

[3] سامح احمد البلتاجي موسى، المرجع السابق، ص372.

[4] محمد أمين البشري ،المرجع السابق ، ص.233

[5] سامح احمد البلتاجي موسى، المرجع السابق، ص373.

ثانيا: الدليل الجنائي في شكله الإلكتروني.

هو "كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقمي ، بحيث يمكن الحاسوب من إنجاز مهمة ما"[1]على أنّ الحاسوب ليس الآلة الوحيدة التي يمكن انجاز المهمات بها ، إذاً هو الدليل الذي يتواجد بالعالم الإفتراضي دالا على وقوع جريمة الإنترنت ، الواقع أن الدليل الإلكتروني يأخذ هذا المصطلح أو مصطلح الدليل الجنائي إلكتروني نسبة إلى النظام الرقمي الثنائي (1-0) [2]، فهو الدليل الذي يجد له أساسا في العالم الإفتراضي ويقود إلى الجريمة"[3]، وبالتالي مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور وتسجيلات صوتية أو مرئية [4]، أو بيانات أو أي مخرج من المخرجات الكمبيوترية ، كالمحررات لأنه لابد من تحول هذا الدليل إلى شيء ملموس ولو بالتقريب كي يفهمه قاضي الموضوع.

مع العلم أن المشرع الجزائري قد استخدم مصطلح " الشكل الإلكتروني"، وذلك في نص المادة (1/16) من القانون (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال التي جاء فيها ما يلي: "... يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني" ، وهو نفس المصطلح المستعمل في القانون المدني الجزائري ، وبالتحديد في المادة (323 مكرر/1):" يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على ورق بشرط إمكانية التأكد من

---

[1] محمدابو بكر بن يونس، المرجع السابق، ص969.

[2] النظام الرقمي الثنائي ،وهي الصيغة التي تسجل بها كل البيانات (أشكال وحروف ورموز وغيرها) داخل الحاسب الآلي ،حيث يمثل الصفر وضع الإغلاق off،والواحد وضع التشغيل on،ويمثل الرقم صفر0 أو الرقم واحد1 ما يعرف بالبيت bitK ويشكل عدد بيت bits ما يعرف بالبايتbyte. هامش مشار إليه لدى عائشة بن قارة مصطفى،حجية الدليل الجنائي الالكتروني في مجال الإثبات الجنائي،في القانون الجزائري والقانون المقارن،دار الجامعة الجديدة،الإسكندرية،مصر،2010،ص13.

[3] منى فتحي أحمد عبد الكريم، الجريمة عبر شبكة الدولية للمعلومات،صورها ومشاكل إثباتها،رسالة دكتوراه،كلية الحقوق،جامعة القاهرة،مصر، ص162.

[4] طارق محمد الجملي،المرجع السابق،ص44.

هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"[1] ، وهي الشروط التي أكد عليها المشرع في نص المادة (2/16) من القانون رقم(09-04):"... وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها".

إذاً فالمشرع الجزائري لم يحصر أدلة الإثبات، وهذا تطبيقا لمبدأ حرية الإثبات في المواد الجزائية، على عكس المعاملات المدنية التي تتميز بأن الإثبات فيها مقيد أو شكلي، وبالتالي فإن الإثبات في المواد الجزائية هو إثبات حر مع مراعاة مشروعية الإجراءات الجزائية المتبعة في كشف الدليل وجمعه وتقديمه، كالمعاينة والتفتيش وندب الخبير.

ومما لا شك فيه أن إختلاف محل الجريمة ومسرحها الإفتراضي، جعل بعض الإجراءات الجزائية عاجزة عن كشف الدليل وجمعه وتقديمه ، مما جعل المشرع الجزائري يثمن بعض الإجراءات الجزائية ويضيف إجراءات جديدة، من خلال تعديله لقانون الإجراءات الجزائية لسنة 2006، والقانون (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما. و هذا بعدما أدرك أن تكنولوجيا الإعلام والإتصال تنفرد بدليل خاص للإثبات، وبالتالي تعجز إجراءات جمعه إذا لم تكيف هذه الأخيرة وخصائصها، أو تثمن الإجراءات التي يمكن عن طريقها جمع الدليل وتقديمه ، وهذا حتى تكون داخل حدود شرعية الحصول على الدليل الجنائي ، حيث أن كل دليل لا تحترم فيه الشروط الموضوعية والشكلية هو باطل بطلان إجراءاته.

مع العلم أن كل المحاولات الفقهية عجزت عن التفرقة بين الدليل الإلكتروني و الدليل الرقمي، ويمكن إعطاء عدة تعريفات للدليل الإلكتروني منها أنّه " معلومات مختزنة في أجهزة الحاسوب وملحقاتها من ديسكات وأقراص مرنة وغيرها من وسائل تقنية المعلومات ، كالطابعات

[1] القانون رقم (05-10) المؤرخ في 20 يونيو 2005 يعدل ويتمم الأمر رقم (75-58) المؤرخ في 20 رمضان عام1395 الموافق 26 سبتمبر 1975و المتضمن القانون المدني المعدل والمتمم ،ج .ر رقم 44 المؤرخ في 26 يونيو 2005،ص17.

والفاكس أو منتقلة عبر شبكة الإتصال، والتي يتم تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة يهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبيها"[1] ، بمعنى أنه الدليل المتواجد في العالم غير المادي الإفتراضي، والذي يمكن أن يتواجد في النظام المعلوماتي بمكنوناته المادية والمعنوية أو عبر شبكات الإتصال، أي "الدليل المأخوذ من أجهزة الكمبيوتر والذي يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الأصوات والأشكال والرسوم.

وذلك من اجل اعتماده أمام أجهزة إنفاذ القانون"[2]فهو الدليل"المشتق من أو بواسطة النظم البرمجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الإتصال من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور وأشكال وأصوات لأداة وقوع الجريمة ولتقرير البراءة أو الإدانة فيها[3] يهدف إلى إثبات وقوع جريمة عبر الإنترنت ونسبة الفعل الإجرامي إلى مستخدم معين، والجدير بالملاحظة أن المستخدم الذي نقصده هنا لن يكون بالضرورة شخص طبيعي أو معنوي، بل هذا الدليل قد يقود فقط إلى النظام المعلوماتي التي ارتكبت عن طريقه واحدة من الجرائم محل الدراسة ، ومن هنا فإنه لابد من وجود تكامل بين الدليل الجنائي الالكتروني والأدلة العادية الأخرى."وتمتاز النصوص الرقمية بسهولة إستنساخها بوقت قصير، وبكلفة هامشية دون المساس بالأصل ولا

[1] عائشة بن قارة مصطفى، المرجع السابق، ص61

[2] ممدوح عبد الحميد عبد المطلب ،البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية،المحلة لكبرى،مصر2006،ص88.

[3] عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي جامعة نايف العربية للعلوم الأمنية،الرياض، المملكة العربية السعودية،12-14 نوفمبر 2007،ص13.

بنوعية النسخ، فالنسخ تكرار للأصل وليس نسخة منه"[1] ،وبالتالي لا يمكن طرح الإشكال في أصالة الدليل الجنائي الالكتروني عندما يتعلق الأمر بالقيمة القانونية للدليل الجنائي الإلكتروني، وقيمته الثبوتية .

الفرع الثاني: خصائص وأشكال الدليل الجنائي الإلكتروني.

إن الدليل الجنائي الإلكتروني هو من الأدلة العلمية التي لابد لها من تعامل وفق معايير تقنية، دون الإخلال بالجانب القانوني للحصول عليها فهو المعلومات التي يقبلها العقل والمنطق ويعتمدها العلم يتحصل عليه عن طريق إجراءات تقنية، بضمانات قانونية[2]، وقد كانت هذه الخصائص(أولا) ناتجة عن تلك الطبيعة المختلفة عن باقي الأدلة الحديثة ، التي أثر ت بدورها على أشكال هذا الدليل(ثانيا).

أولا: خصائص الدليل الجنائي الإلكتروني.

الدليل في العالم المادي الملموس، عبارة عن مجموعة من الآثار التي يتركها المجرم أثناء إقترافه الجريمة، يتم الكشف عنها بمختلف الوسائل كاستخدام التحاليل أو الأشعة من أجل إظهارها و الاستفادة منها للإدانة[3]، في حين أن الدليل الجنائي الإلكتروني غير ذلك تماما، لوجوده ضمن البيئة الرقمية، فمثلا الصورة الموجودة على جهاز الكمبيوتر وشبكة الإنترنت ليس لها وجود في العالم المادي إلا عن طريق طباعتها، فهي عبارة عن مجموعة من الأرقام متمثلة في الصفر ورقم واحد، فالطبيعة الخاصة للدليل الجنائي الإلكتروني تتطلب الإلمام بالتقنية، وحتى اللجوء إلى الخبرة، وبالتالي فإن الدليل الجنائي الإلكتروني له صلة وثيقة بتكنولوجيا المعلومات، وهذا لطبيعته غير

[1] ممدوح عبد الحميد عبد المطلب ،زبيدة محمد حاسم،عبد الله عبد العزيز،أنموذج مقترح لقواعد اعتماد الدليل الرقمي لإثبات في الجرائم عبر الكمبيوتر،بحث مقدم لمؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي،9-11ربيع الأول 1424هـ،الموافق 10-13مايو 2003 م،ص 2237 .

[2] خالد عياد الحلبي،إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت،الطبعة1،دار الثقافة للنشر والتوزيع،عمان الأردن،2011، ص230.

[3] رشيدة بوكر ،المرجع السابق،ص488

الملموسة في العالم الافتراضي. إذاً هو يختلف عن باقي الأدلة كونه دليل علمي لكن ذو طبيعة تقنية ، يتطور بتطور التقنية ولكن في نفس الوقت يصعب طمسه، في ظل اتساع مسرحه الجنائي.

أ–دليل علمي: انّ اي دليل له منطق يجب ألا يخرج عليه، حيث يجب عليه عدم تعارضه مع القواعد العلمية السليمة و الدليل الجنائي الإلكتروني له ذات الطبيعة، إذ لا يجب أن يخرج الدليل العلمي عما توصل إليه العلم الرقمي وإلا فقد معناه[1]، فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القضاء المقارن أن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة[2]، لدى لابد من أن يوافق الدليل الجنائي الإلكتروني التطور التكنولوجي الحاصل، كما أن الدليل العلمي هو عنصر مساعد في تكوين قرار القاضي[3]، حيث أن محله البيئة الافتراضية التي يتكون فيها،لذلك يتكون الدليل الالكتروني من بيانات ومعلومات ذات صفة الكترونية غير ملموسة ولا تدرك بالحواس العادية، بل يتطلب لإدراكها الاستعانة ببرامج ووسائل خاصة[4].

ب–دليل الجنائي الإلكتروني دليل تقني: إنّ الدليل التقني يختلف تماما عن السلاح الأبيض المستخدم في جريمة القتل أو الشيك بدون رصيد ، لذلك فهو يتفق وطبيعة الجريمة ، وتحتوي البيئة الرقمية على كم هائل من المعلومات التي يتم تمثيلها عن طريق أرقام ، ولما كانت توفر خدمات عالية الجودة تتناسب في الكثير من الأحيان وأفكار الشخص، الذي ساعدته البيئة الرقمية في الحصول على الكثير[5]، كالشهادات الجامعية وحضور المحاضرات دون أن يكون هذا الحضور ماديًا ملموسا، مما ساعد على الإقبال عليها، ورغم أن كل ما تقدمه مشروع إلا أن الأمر لا يسلم من العبث والاختلاس والسرقة على مستوى الشبكة، لذلك فالدليل الجنائي الإلكتروني مرتبط بالبيئة الرقمية، فهو ينشأ من رحمها، فإذا وقعت الجريمة ضمن واقع مادي ملموس فلا مجال للحديث عن

[1] عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق،ص977.

[2] عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق ،ص977.

[3] Madjid kali, La preuve dans le procès pénal, revue de la gendarmerie, n° 16 février 2006.p33

[4] خالد عياد الحلبي، المرجع السابق، ص231.

[5] عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص978

الدليل الجنائي الإلكتروني، لذلك هو تقني بامتياز، يقتضي وجود خبرة قضائية متخصصة. وهو ما عمل عليه المشرع الجزائري، بان وضع قوانين خاصة بالجرائم المتعلقة به والأشخاص المنطوين بالجانب الجزائي في إستخلاصه وتقديمه، وهذا عن طريق نسخه، على ان هذه النسخة لها نفس قيمة الدليل الجنائي الإلكتروني، والواقع تعتبر مطابقة النسخة للأصل ضمانة لعدم نفاد المجرم من المسؤولية في نفس الوقت هي حفاظ على الدليل الجنائي الإلكترونية من الفقد[1] .

ج–التطور المستمر للدليل الجنائي الإلكتروني: إن الدليل الجنائي الإلكتروني يتطور بسرعة فائقة ، وهذا بتطور التقنية ، ففي البدا لم يكن في الإمكان الحصول على صور أو الفيديو عن طريق الإنترنت ، حيث كانت الخدمات مقتصرة على الرسائل النصية دون الصور ، في حين أن اليوم يمكن الإتصال بالشبكة ليس عن طريق خطوط الهاتف الثابت بل تعداه للهواتف اللاسلكية والنقالة والأقمار الصناعية والألياف البصرية.

ولكن بتطور الصناعة والتجارة وازدهارها، أصبح للمعلومات أهمية بالغة حيث أنّه على أساسها تم استخدام عملية التشفير وتطويرها، للقيمة البالغة لتلك المعلومات التي تدر على أصحابها أموال طائلة، سواء تعلق الأمر بالأسرار التجارية والصناعية والسياسية، وتعتبر قدرة الموظف على تشفير المعلومات ثغرة أمنية خطيرة حيث يقوم الموظف بتشفير بعض الأسرار التجارية ونقلها مشفرة إلى الشركات المنافسة وهو بذلك يستطيع أن يفلت من العقوبة حيث لا يمكن إثبات أي سلوك إجرامي ضده إذ أن دليل الجريمة لا يستطيع قراءته سواه[2].

د–دليل غير ملموس يصعب طمسه:انّ الدليل الجنائي الإلكتروني ، دليل غير مادي بمعنى أن المخرجات الكمبيوترية ليست هي الدليل نفسه بل هي فقط تجسيد له ، ولكن يتميز بصعوبة محوه أو تحطيمه ، حيث أن المحاولات المتتالية للجاني ، تسجل وهذا باستخدام برمجيات بالغة التعقيد ،

[1] خالد عياد الحلبي، المرجع السابق، ص232.

[2] حسن طاهر داوود،المرجع السابق،ص40.

وبالتالي يستدل في حالة العبث عن قيام المجرم بالسلوك الإجرامي[1] ، ولكن العبث به ، يؤدي لإضعاف حجيته في الإثبات ويشكك فيه وفي مدى مصداقيته ، فتصبح البراءة من نصيب المتهم ، لان الشك يفسر لصالحه ، وان كان لا يعول على هذا الدليل فانه يمكن إدانة مرتكب الجريمة بالنصوص التي تجرم مثل هذه الأفعال[2].

ثانيا: أشكال الدليل الجنائي الإلكتروني.

في الواقع أنّ مصادر الدليل الجنائي الالكتروني، لها صلة وثيقة بأصنافه حيث تقسم الأدلة الجنائية الالكترونية إلى عدة أنواع وهذا حسب أماكن تواجدها؛ وهي نفس الأماكن التي يمكننا الحصول منها على الدليل الجنائي الالكتروني، و على اثر ذلك يمكن تصنيف الدليل الجنائي الالكتروني، التقسيم التقليدي ثم وفق التقسيم الحديث.

أ- التقسيم التقليدي ويمكن تقسيم الدليل الجنائي الإلكتروني[3]، وفق التقسيم التقليدي أي أدلة أعدت لتكون وسيلة إثبات وأدلة لم تعد لتكون وسيلة إثبات.

1-أدلة التي أعدَّت لتكون وسيلة إثبات فهي، السجلات التي تم إنشاؤها بواسطة المنظومة المعلوماتية تلقائيا، السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الآلة ، ومن أمثلة ذلك البيانات التي يتم إدخالها للآلة وتتم معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات[4].

[1] سامح احمد البلتاجي موسى، المرجع السابق، ص381.

[2] عمر محمد ابو بكر بن يونس،الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص983.

[3] محمد طارق الجملي، المرجع السابق،ص44.

[4] محمد طارق الجملي، المرجع السابق،ص46.

2-أدلة لم تعد لتكون وسيلة إثبات، أي نشأت دون إرادة اشخص، أي تركها الجاني دون أن يكون راغبا فيها، وهي البصمة الرقمية والآثار المعلوماتية.الآثار الرقمية يعتمد فيها على (IP) [1].

ويتم استخراج الدليل الجنائي الإلكتروني عن طريق بروتوكولان(IP /TCP) ف(IP) هو المسؤول على إرسال رزم على عنوان وجهة المعطيات، أما بروتوكول(TCP)هو المسؤول عن تدقيق صحة نقل المعطيات من الحاسب إلى الحاسب الخادم ولكن السؤال الذي يمكن طرحه ما هو دور هذه البروتوكولات في الإثبات، أي الحصول على الدليل الجنائي الإلكتروني؟

تكون الإجابة كالتالي الطريق التي تعمل بها هذه البروتوكولات تمكن من معرفة مصادر والعناوين والمعلومات والتي يحتويها هذا البروتوكول، فهو بروتوكول اتصال بين الشبكات ، لذلك وعن طريقها يمكن تحديد المنظومة المعلوماتية المستخدمة في جرائم الإنترنت ، بكل تفاصيلها الزمنية والمكانية ، حيث يمكن تتبع المراسلات ويمكن عن طريقها استعادة البيانات[2]، ومن ناحية عملية المخول بالولوج وتتبع مسار الإتصال هو مقدم خدمات الإنترنت، الذي يعتبر مصدر من المصادر الشخصية للحصول على الدليل الجنائي الإلكترونية وسوف نفرد لهم مطلب خاص.

ب- التقسيم الحديث للدليل الالكتروني.

يمكن تقسيم الأدلة الجنائية الالكترونية كما يلي : الأدلة الالكترونية الخاصة بأجهزة الكمبيوتر وشبكاتها ،الأدلة الالكترونية الخاصة بالإنترنت،الأدلة الرقمية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات،الأدلة الالكترونية الخاصة بالشبكة العالمية للمعلومات[3].

[1] عبد الفتاح بيومي حجازي ،الدليل الجنائي و التزوير في جرائم الكمبيوتر والإنترنت ،المحلة كبرى ،مصر2001،ص50، و عائشة بن قارة،المرجع السابق،ص64.

[2] فهد عبد الله العبيد العازمي، المرجع السابق،ص482 وما بعدها

[3] عبد المطلب عبد الحميد ممدوح، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية ،مصر،2006،ص78.

كما يوجد الدليل الجنائي الإلكتروني في صورة مخرجات التي يمكن بها فهم الدليل باعتبار ان مكان تواجده الاصلي هو البيئة الافتراضية، وهو على ثلاثة أشكال أمّا مخرجات ورقية عن طرق الطابعات أو مخرجات لاورقية أي الكترونية كالدعامات عن طريق شاشات المنظومة المعلوماتية أو غيرها من عارض البيانات[1].وهذه المخرجات الإلكترونية أو الرقمية أو الكمبيوترية- بإعتبار أن هذه المخرجات قد تكون من هاتف نقال أو ساعة يد كما يمكن أن تعرض من الهاتف النقال نفسه إذا كان مسرحا لجريمة الإنترنت – هي عبارة عن أثار معلوماتية وهي"الآثار الرقمية تمثل رؤية لمسرح الجريمة الحقيقي"[2] ، فهي عبارة عن ما يخلفه الجرم المعلوماتي وراءه ، أو مستخدم الإنترنت بصفة عامة ، فتتنوع هذه الآثار بين مراسلات البريد الإلكتروني ، والفيديوهات الرقمية والصور وغيرها من الإتصالات والتسجيلات الصوتية الإلكترونية[3].

كما يمكن أن يكون الدليل الجنائي الإلكتروني على شكل برامج أو تطبيقات ، ذلك انه يستمد صورته وأشكاله من أشكال المعلومات أو من صورة المعلومات ، والتي هي في تطور وتغير مستمر ، مادام ان هناك تطور مستمر في تكنولوجيات الإعلام والإتصال.

1- المخرجات الورقية:وهي الحالة التي تسجل فيها كل البيانات على ورق ، طبعا من غير المحاضر التي تحرر ويرفق بها الدليل الجنائي الإلكتروني المتحصل عليه بالإجراءات الجزائية التي سوف نأتي على عرضها في حينها.

2- المخرجات الإلكترونية:وهي التي تتمثل في الأشرطة المغناطيسية و والأقراص المغناطيسية والقرص المرن والقرص الصلب ، وهي فقط أنواع نذكرها على سبيل المثال ، بإعتبار أنّ التطور

[1] هلالي عبد الاله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية،دراسة مقارنة،ط2، دار النهضة العربية،القاهرة،مصر،2008،ص.16

[2] ممدوح عبد الحميد عبد المطلب و آخرون، المرجع السابق، ص 2238.

[3] التسجيلات الصوتية الرقمية أو الالكترونية وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية وتشمل المحادثات الصوتية على الانترنت والهاتف، والتي يمكن حجزها بواسطة إجراء مراقبة الاتصالات الالكترونية ،المنصوص عليها في المادة 04 من القانون(09-04).

التكنولوجي قد فتح المجال واسعا أمام التخزين على الشبكة دون أن يكون لذلك أي أثر أو نسخة على جهاز الكمبيوتر أو الهاتف النقال كخدمة اي كلود(iclowd) لأجهزة ابل أو ما يعرف بالتخزين الإفتراضي، الأشرطة المغناطيسية ، ويتم فيه تخزين البرامج والملفات وهو لازم لقراءة البيانات فيها قراءة الشريط في ذاته حيث تنظم المعلومات على شكل وحدات ، امّا الأقراص المغناطيسية فهي أفضل الوسائط التي يمكن استخدامها للتخزين العشوائي أو المباشر والتي تتميز بقدرتها الاستيعابية العالية وسرعة تداول المعلومات المخزنة عليها[1].

3-المخرجات المعروضة على وسائل العرض: بالإضافة إلى المخرجات الورقية والإلكترونية هناك مخرجات معروضة والتي يتم فيها الاعتماد على وسائل العرض امّا على الشاشات كالكمبيوتر وساعات الذكية و والهواتف الذكية ، حيث يتم استعراض المعطيات التي تم إدخالها أو المعالجة آليا بواسطة برامج وتطبيقات معينة[2].

الفرع الثالث:مصادر الدليل الجنائي الإلكتروني.

في الواقع أن مصادر الدليل الجنائي الإلكتروني ، لها صلة وثيقة بأنواعه حيث تقسم الأدلة إلى عدة أنواع ، وهذا حسب أماكن تواجدها ، وهي نفس الأماكن التي يمكننا الحصول منها على الدليل الجنائي الإلكتروني، من اجل تعقب مجرم الإنترنت وبالتالي تقديمه للمحاكمة كما ذكرنا سابقا.

فتنوع الدليل الجنائي الإلكتروني يفيد أنّ هناك عدة طرق للحصول عليه ، ذلك أن شبكة الإنترنت هي شبكة معقدة ، ولكن ورغم كل هذا فان الإتصال بها عملية سهلة خصوصا مع وجود نوعين من خدمات الولوج إلى شبكة الإنترنت السلكي والمتمثل في وجود خط هاتفي ومودم، والتي أصبحت طريقة غير فعالة بظهور الإنترنت اللاسلكي، أما الثاني فهو انترنت لا

[1] هلالي عبد الاله احمد، حجية المخرجات الكمبيوتريةفي المواد الجنائية،المرجع السابق،ص19.

[2] هلالي عبد الاله احمد، حجية المخرجات الكمبيوتريةفي المواد الجنائية،المرجع السابق،ص21.

سلكي ، وبالتالي فان الحصول على الدليل الجنائي الإلكتروني يتطلب فحص نظم الإتصال بالإنترنت وفحص مركبات الحاسب وكل جهاز يمكن الولوج به إلى الإنترنت كالهواتف النقالة . غير أنّه وبالمقابل قد يتواجد الدليل الجنائي الإلكتروني بحوزة أشخاص هم إما ضحايا أو ممن لهم دور مهم في كشف جرائم الإنترنت ، سواء كانوا أشخاص طبيعيين أو معنويين ، وتكمن أهميتهم كمصادر للدليل الجنائي الإلكتروني ، ليس بالمصادر –المادية– التي يحوزنها مثلا الهواتف النقالة بل ، نسبة هذا الدليل لشخص معين وهو الأهم في جرائم الإنترنت .ونظرا لاهمية مزود خدمات الإنترنت في الموضوع فقد اردنا له فرع خاص.

أولا:نظم الإتصال بالشبكة.

ويتمثل في نظام فحص مسار الإنترنت ، أي الحركة التَرَاسُلِية للنشاط الممارس من خلال شبكة الإنترنت ، فالمنظومة المعلوماتية بمجرد أن تتعرف على المسار تقوم تلقائيا باختيار البروتوكول التراسل والذي عن طريقه يقوم الجهاز باستدعاء البيانات[1]، وفحص بروتوكولات الإنترنت IP Address ان فحص بروتوكول الإنترنت يمكن من التعرف على المنظومة المعلوماتية التي ارتكب السلوك الإجرامي دون الشخص[2] ، وفحص الخادم الذي يعمل على الربط بين أعضاء الإنترنت، مما يمكنهم من التحاور عن طريق مختلف الوسائط الاجتماعية والبريد الإلكتروني[3]، إن منطق التعرف على النظام المعلوماتي الذي تمت مباشرة ارتكاب الجريمة عبره من السهولة بمكان، وهذا الأمر يطلق عليه عملية التعرف على بروتوكول الإنترنت IP[4] ، وهذا الأمر طبيعي خصوصا إذا تم الإبلاغ عن الجريمة أو كانت هناك عمليات مراقبة تقوم مديرية المراقبة

[1] عمر محمد بن يونس أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص998.

[2] Eoghan Casey, computer evidence and computer crime forensic science, computers and the internet,Cambridge university press,2000.p.7.

[3] سامح احمد البلتاجي موسى، المرجع السابق، ص387

[4] عمر محمد بن يونس أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص1006.

الوقائية واليقظة الإلكترونية ، كما انّه يمكن الحصول علىIPعن طريق برمجيات معينة ، وهنا في حال تم إكتشاف الجريمة حيث يكون الأمر سهلا لو كانت الجريمة قد تمت عبر حاسوب شخصي ، هنا يمكن لأجهزة الضبط أن تلاحق الجاني كما يمكن فحص الخادم أو الملقم ، وفحص النظام الأمني البرمجي وهذا للحصول على مزيد من الأدلة الجنائية الإلكترونية المتواجدة على مستواها.

ثانيا:فحص مركبات المنظومة المعلوماتية.

إنّ أهم مصادر الدليل الجنائي الإلكتروني، هو الحاسوب وكل مكوناته سواء المادية أو المعنوية بالإضافة إلى مجموع الوسائل التي يمكن الولوج بها إلى شبكة الإنترنت كالهواتف النقالة ، وشاشات التلفزيون وساعات اليد إن النظام المعلومات يحتوى على بيانات في هيئة رقمية متبادلة،كما يمكن، فحص نظام ذاكرة التخزين، والذي يمكن تعريفه بأنه قدرة الحاسوب الآلية على الإحتفاظ بنسخة كاملة مما اطلع عيه عضو الإنترنت أثناء إبحاره في العالم الإفتراضي[1].

أ- فحص القرص الصلب.

يعد القرص الصلب المحتوى الذي يضم في داخله مجموعة من البيانات الرقمية ذات الطابع الثنائي[2]، ويتم فحص القرص الصلب إما كليا أو جزئيا وهذا حسب نوع الجريمة والآثار المترتبة عليها أي الأضرار الناجمة عنها.

ب-الفحص الجزئي للقرص الصلب.

ويتم ذلك عن طريق استرداد المعلومات الموجودة على مستواه الموجود في ساعة التفتيش أو المعاينة أو التي تم حذفها ، والمثال التقليدي المستخدم هنا هو حالة البحث في الملفات النسخ

[1] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص1017.

[2] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق ،ص1011.

الإضافية التي تحتويها نظم التشغيل مثل النوافذ[1] ، والملفات المؤقتة ، حيث انّه بمجرد الولوج إلى شبكة الإنترنت فان هذه الملفات تحتفظ بنسخ كما يمكن كذلك فحص ملفات الخاصة بالتحميل.

ج–فحص البرمجيات.

وهي المكون المعنوي للحاسوب ، ويثار هنا ما إذا كانت البرمجيات معطوبة أي بها خلل في حد ذاتها ، ولعل من اللازم التطرق إلى موضوع أهمية فحص البرمجيات عبر الحاسوب وذلك أن برمجية الحاسوب ليست ذات نظرة مثالية حسبما عرضنا[2] ، إن برمجية الحاسوب يمكن أن تؤثر في الحاسوب فتجعله محل شك يمكن أن يهز قيمتها كدليل هذا لقصور له أثر هـ في عملية تقييم الدليل المستمد من البرمجية ذاتها ، فمثلا إن استمداد أدلة حين فحص برمجية معينة كبرمجية البريد الإلكتروني أو برمجية اتصال بمواقع الدعارة أو برمجية تحصيل أموال المخدرات أو لبرمجية العاب القمار....الخ مركبة على الحاسوب، فان مجرد كون هذه البرمجية معطوبة ليست من الأسباب ليجعلها قاصرة عن استمداد دليل يحمل الإدانة ، حتى وان أمكن استخدام برمجيات عالية الكفاءة لتنقيتها من الشوائب ، إذ يظل حالها محل شك ، لذلك تعد البرمجيات المعطوبة في مستوى عناصر الاستدلال وليست دليلا كاملا[3].

د–الملحقات.

من بينها فحص الطابعة، فالتطور يطال كل الأجزاء والأجهزة الموصولة بالحاسب الآلي ومنها الطابعة التي أصبحت تتميز بميزة تخزين منطقية لمجموع الصفحات التي تم استخراجها من الحاسوب ، حتى في الحالة التي يكون هذا الملف قد تم إلغاؤه[4] ، وفي الواقع هناك برمجيات متطورة

[1] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت المرجع السابق ،ص1012.
[2] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت نفسه،ص1013.
[3] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت نفسه،ص1013.
[4] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت المرجع نفسه،ص1018.

تقوم باسترجاع مخرجات الطابعة ، فمثل هذه البرمجيات تساعد في معرفة ما إذا كان الشخص قد قام بطباعة صفحات تتضمن صور داعرة وخليعة من الإنترنت وتاريخ قيامه بذلك وساعته بدقة غريبة [1] ، ويراعي أن تقدير ما إذا كان مالك الحاسوب أو الهوية عبر الإنترنت هو مرتكب الجريمة عبر الإنترنت، وإنما تم تخريجه بالطباعة منسوب إليه يظل خاضعا لتقدير محكمة الموضوع في كل الأحوال[2]كما يمكن فحص لوح المفاتيح، حيث أن عمل مجرم الإنترنت قد يصل إلى أن يتحكم في لوحة المفاتيح ومن تم يمكن الاعتماد عليها في استمداد الدليل.

المطلب الثاني: المتدخلون في شبكة الإنترنت .

إنّ خدمة الإنترنت تمر بأكثر من وسيط، حيث انّه لا يمكن أن يتّم ذلك دون الاستعانة بالقائمين عليها من مزودي خدمات و الذي أطلق عليهم المشرع الجزائري في إطار القانون (09-04)مقدمو الخدمات فالمادة الثانية منه تعرفهم بما يلي"...د- مقدمو الخدمات:1- أي كيان عام أو خاص يقدم لمستعملي خدماته ، القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام اتصالات ، 2-وأي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها ، ".. مهمتهم الأساسية إيصال خدمة الإنترنت لمستعمليها ، و لكن يختلف كل متدخل من هؤلاء في الخدمة المقدمة للمستخدم ، و بالتالي مسؤوليته الجزائية اتجاه المستخدم ، و بعد الإلتزامات التي اقرها القانون سالف الذكر ، يعد مزود خدمة الإنترنت من بين مصادر الدليل الجنائي الإلكتروني و أماكن تواجده ، على غرار باقي المتدخلين و المتمثلين في مستخدم الإنترنت (الضحية) في إطار هذه الجرائم سواء تعلق الأمر بشخص طبيعي أو معنوي ، أو مجرم الإنترنت نفسه

الجدير بالذكر أن المتدخلون في الشبكة هم المستخدمون ، لكن لكل دوره فالمستخدم العادي الذي يقوم بتلقي المعلومات فقط ، هو مستخدم سلبي ، و لو أنه يدخل في هذا النطاق

[1] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت، نفسه،ص1019.

[2] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت، نفسه،ص1019.

إبداء الآراء و الرد على التعليقات، و لكن إذا تجاوز ذلك توريد للمعلومات و تخزينها و إنتاجها يصبح هذا الأخير مستخدما ايجابيا ، كأن يكون مورداً للمعلومات ، و يستوي كذلك أن يكون هذا المستخدم الذي من دونه لا مكان لوجود الشبكة بعالمها الإفتراضي في عالمنا الواقعي فما فائدة شبكة دون رواد أو مستخدمين – شخص طبيعي أو معنوي ، على انه من مصادر الدليل الجنائي الإلكتروني المستخدم والذي سوف نقتصر في دراسته على مزود خدمة الإنترنت بإعتباره متحكما في خدماتها المقدمة وله دور كبير في تحصيل الدليل عن طريق الإلتزامات التي ألقاها على عاتقه المشرع الجزائري في نص قانون(09-04) مبينين تعريفه(الفرع الأول) والإلتزامات الخاصة به (الفرع الثاني)، وسنؤجل مسؤوليته عن بعض السلوكيات التي جرمها المشرع بمناسبة تأديته لبعض الإلتزامات إلى الفصل الثاني من الباب الثاني بإعتبارها ضمانات لحماية الحق في الحياة الخاصة ، وحماية الحصول على الدليل ، والتي وردت في القانون الخاص أمّا ماتعلق بقيام مسؤوليته في قانون العقوبات فسوف ناتي على ذكرها (الفرع الثالث).

الفرع الأول: مقدم خدمة الإنترنت [1].

كما ذكرنا سابقا أن عملية إيصال خدمة الإنترنت[1] بمفهومها الواسع، تمر بعدة وسطاء من اجل وصول الخدمة للمستخدم، فمقدم خدمة الإنترنت[2]هو من يضع تحت تصرف المستخدم

[1] **مقدمو خدمات الانترنت في الجزائر:**

– شبكة الاتصال PAC-DZ وهي شبكة تشرف عليها ادارة البريد والمواصلات السلكية واللاسلكية،تربك شبكة المعلومات الدولية وبنوك وقواعد ومعطيات .

– مركز البحث والإعلام العلمي والتقني CERIST الذي انشأ من قبل وزارة التعليم العالي والبحث العلمي سنة 1986 . وبعد صدور المرسوم التنفيذي (98-257) المؤرخ 25 اوت1998 والمعدل بالمرسوم التنفيذي (2000-307) بتاريخ 17 أكتوبر 2000 الذي يحدد شروط و كيفيات وضع واستغلال خدمة الانترنت برز للوجود مقدمو خدمة الانترنت خواص وعموميون .

–شركة فوب الجزائر.شركة تقوم بتوفير خدمات الانترنت وتشمل استضافة المواقع وتصميمها

–ايه س ايه الجزائر:شركة متخصصة في تقديم الخدمات المتنوعة وتصميم الجرافيكس،والاتصال عن طريق الأقمار الصناعية.

– الجيري كوم الجزائر :شركة جزائرية متخصصة في تقديم خدمات الانترنت والبريد الالكتروني، وغيرها كشركة الو لاين الجزائر و وصال الجزائر للمزيد من التفاصيل يرجى الاطلاع على ،محمد الفاتح حمدي، مسعود بوسعدية، ياسين قرناني،تكنولوجيا الاتصال والإعلام الحديثة، كنوز الحكمة، الابيار ،الجزائر،2010،ص64-65-66.

الوسائل التقنية من اجل الولوج إلى شبكة الإنترنت [3]، و من الملاحظ وفق تعريف المادة الثانية من القانون(09-04) الفقرة "د" المذكورة سابقا أن المشرع الجزائري لم يفرق بين هؤلاء المتدخلين ، في عملية إيصال خدمة الإنترنت والأصل أنّه لا يمكن الحصول على خدمة الإنترنت ، والدخول واستغلال هذه الشبكة، دون أن يتم ذلك عن طريق مقدميها أو ما يعرف بالوسطاء، ورغم تعدد طرق الوصول إلى الإنترنت مثلا (ISDN/ADSL)[4] ، لكن العامل المشترك لكل هذا هو وجود مزود خدمات كل حسب الدور الذي يلعبه ، لإيصال الخدمة.

أولا: تعريف مقدم خدمات الإنترنت .

يعرف مقدم خدمات الإنترنت بأنه الهيئة أو جهة في بلد معين تمنح حق اشتراك الراغبين في شبكة الإنترنت [5]وهو من يقوم بخدمة الإتصال أو خدمة معالجة البيانات أو خدمة تخزين البيانات أو خدمة الاستضافة أو التخزين المؤقت... أو الربط بالشبكات[6]، وهي بالتقريب نفس التعاريف

---

[1] **لإقامة خدمة الانترنت لابد من شروط معينة**: نص المشرع الجزائري في المادة 04 من المرسوم التنفيذي(2000-307) الذي يضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها ،على أنه لا يرخص بإقامة خدمات انترنت واستغلالها لأغراض تجارية إلا ضمن الشروط **للأشخاص المعنويين الخاضعين للقانون الجزائري** وعليه يتضح لممارسة نشاط خدمات الانترنت يشترط أن يمارسها مقدم خدمات الانترنت بناء على **ترخيص**، يجب على الطالب أن يقدم عرض مفصل عن الخدمات التي يقترح تقديمها، وشروط وكيفية الولوج إلى هذه الخدمات كذلك يشترط دراسة تقنية حول الشبكة المقترحة وحول التجهيزات والبرامج المعلوماتية التابعة لها،وهذا بنص المادة 05 من المرسوم التنفيذي(98-257)،يرجى الاطلاع على المرسوم التنفيذي. المرسوم التنفيذي(2000 -307)المؤرخ في 14 أكتوبر سنة 2000 المعدل والمتمم للمرسوم التنفيذي (98 -257)المؤرخ في 25 أوت 1998،ج.ر63 ليوم 26غشت 1998ص6 و ج.ر60 ليوم 15اكتوبر 2000ص 15على التوالي.

[2] Art2 « d -Fournisseurs de services :1 - toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique et/ou d.un système de télécommunication ;

2 - et toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs » Loi n° 09-04.

[3] Myriam Quéméner, Yves Charpenel, op. cit.p38.

[4] (ISDN) الشبكة الرقمية للخدمات المتكاملة، وهي شبكة اتصالات رقمية عالمية واسعة ناشئة عن خدمات الهاتف الموجودة.

[5] محمد الربيعي، احمد شعبان الدسوقي و آخرون، المرجع السابق، ص105.

[6] هلالي عبد الإله احمد، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، المرجع السابق، ص48.

الواردة في نص المادة الثانية من القانون (09-04) بإعتبار أن المشرع الجزائري اخذ معظم أحكام هذا القانون من الاتفاقية الأوروبية لمكافحة الإجرام السيبيري .

و لعل الملاحظ من خلال هذه التعاريف أن المشرع الجزائري قد شمل كل مقدمي خدمة الإنترنت ، مما أدى إلى عدم التميز بينهم، لأنّه من الناحية العملية- أي تعاون المزود مع السلطات المختصة- ، فان المهم فيها هو الحصول على هوية المشتبه فيه ومكانه و جميع اتصالاته ، وهذا الذي لا يكون أو لا يتحقق إلاّ بتضافر جهود الجميع أي متعهد الوصول ومتعهد إيواء و مقدمي خدمات الإنترنت ، لكن هذا ما لا يعكسه الواقع ، لوجود إختلاف في نوعية الخدمات المقدمة ، فمن يقوم بالتوصيل لا يمكن أن تقع على عاتقه التزام كمراقبة معطيات المحتوى لأنه هو عمليا ناقل مادي للمعلومات.فهل هناك فعلا إختلاف في أصناف وسطاء الإنترنت ؟

ثانيا:الخدمات التي يقدمها مزود خدمات الإنترنت .

قبل تحديد أصناف مزودي خدمات الإنترنت، لابد من تحديد مجموعة الخدمات التي يقدمها هؤلاء، وعلى أثر ها يمكن تصنيفهم بحسب الخدمة المقدمة قبل التطرق إلى إلتزامات مقدمي خدمات الإنترنت، لابد أولا من التعريف بالخدمات التي تقدم من طرفهم لمستخدم الإنترنت كأصل عام ، و المتمثل في الخدمات الفنية و الخدمات المعلوماتية ، حيث تحدد طبيعة الخدمة نوع مقدم الخدمة في ظل عدم تصنيفهم في القانون الجزائري ، ويمكن تقسيم الخدمات إلى صنفين خدمات تقنية أو تكنولوجية وأخرى غير تقنية أي معلوماتية.

أ-الخدمات الفنية ، تختلف الخدمات الفنية التي يقدمها بعض مقدمي خدمة الإنترنت و التي تتمثل إمّا في خدمات النقل المادي للمعلومات أو في خدمات توصيل الخدمة.

1-خدمات النقل المادي للمعلومات[1]:

يتولى النقل المادي للمعلومات، لوجود توصيلات أسلاك و كابلات مؤسسات عمومية كاتصالات الجزائر مثلا، حيث يقع على عاتقها التوصيل المادي للمعلومات فالوسيط أو مزود الوصول هو مجرد ساعي بين المستخدم و النظام المعلوماتي، و هذا بموجب عقد بينه و بين المشترك ، فإذا نظرنا إلى طبيعة هذه الخدمة نجدها تختلف عن خدمة الإيواء أو التخزين التي و بشروط مفروضة من مقدم الخدمة يمكن الاطلاع على محتواها، كأن يتم الاتفاق على ذلك، وبإذن من وكيل الجمهورية ، كان يكون محتوى مخل بالآداب العامة، لذلك قد يكون لمقدم خدمة أن يراقب المحتوى وبالتالي يكون مسؤول عن الاستخدام غير الشرعي للانترنت، ما عدا ذلك هو مجرد ساعي البريد ، تنحصر مهمته في تامين النقل المادي للمعلومات بين الأطراف المختلفة من مرسلين إلى مرسل إليهم ، و حماية الشبكة من مختلف الاعطاب الفنية و تصليحها و صيانتها الدورية، و تعويض المستخدمين عن مده انقطاع الخدمة ، التي تتم عادة عن طريق تمديد فترة الاشتراك.

2-خدمات الوصول: و هي الخدمة التي من خلالها يستطيع المستخدم الدخول إلى مواقع الإنترنت و هذا ما يوفره عن طريق البريد الإلكتروني أو حتى كلمات السر و يمكن أن يقترح كذلك خدمات أخرى. كاقتراح " مضمون معلوماتي معين يتم بثه عبر الشبكة"[1].

لكن مع ملاحظة أنّ مقدم وصول خدمات الإنترنت الذي يمكن أن يعرض خدمات كالإيواء أو الاستضافة و بالتالي يمكن أن يجمع متعهد الوصول أو مقدم نقل الخدمات للمعلومات لا يمكنه ذلك (أي من الناحية النظرية) و قد تكون الخدمات المقدمة هي من قبيل الخدمات المعلوماتية التي تتنوع بين الإيواء أو الاستضافة أو الجمع أو التأليف .

[1] احمد قاسم فرج ، النظام المعلوماتي القانوني لمقدمي خدمات الانترنت – دراسة تحليلية مقارنة – مجلة المنار ، المجلد 13 ، العدد 09، 2007 ، ص 329 .

[1] احمد فرج ، المرجع السابق ، ص 329.

ب-الخدمات المعلوماتية:

وهي الخدمات التي يقدمها نوع من مقدمي خدمات الإنترنت، والتي قد ترتب مسؤولية جنائية في حالة عدم التزامهم بما هو مقرر قانونا، لأنهم مؤهلين بحسب ما يمتلكونه من وسائل معلوماتية من مراقبة المشتركين وتقفي أثر هم في حالة الاختراق مثلا أو بث محتوى غير مشروع.

1-خدمات الإيواء أو الاستضافة: و تكون هذه الخدمة بموجب عقد مع المستخدم حيث يلعب دورا جوهريا في التعرف على شخصية طالب الخدمة و بإحاطته علما بشروط استعمالها، و بإعلامه بوجوب عدم تجاوز الإطار الصحيح و المشروع لاستخدام الوسائل التقنية و المعلومات المخصصة له [1]، و هو ما يختلف عن خدمة توريد المعلومات، لذلك فطبيعة الخدمة التي يقدمها متعهد الإيواء تجعل الأنسب والأقدر على تحديد هوية مرتكبي جريمة الإنترنت، ومعرفة مضمون أي نشاط تقني إجرامي عبر شبكة الإنترنت[2] .

2-خدمة توريد المعلومات: يقوم الشخص الطبيعي أو المعنوي بتحميل النظام بالمعلومات التي قام بتأليفها أو جمعها حول موضوع معين ، بأنّه يتولى الإختيار و التجميع و التوريد للمادة المعلوماتية حتى تصل إلى الجمهور.[3]

و عليه من كل ما سبق أردنا وضع تعريفات لخدمات التي يقدمها مزودي خدمة الإنترنت ، من اجل توضيح الفرق بينهم، وما يهمنا في هذه الدراسة هو دور مقدم خدمات الإنترنت بأصنافه، في إثبات الجنائي لجرائم الإنترنت، والملاحظ انّه كلما كانت الخدمات التي يقدمها مزود الخدمات خارج العالم الافتراضي فان مسؤوليته تتضاءل ، ولكنه دوره ليس منعدم لانه أساس الولوج إلى الإنترنت عن طريق الخدمات التقنية لها علاقة بالجانب الفني والتقني البحت، و دوره في

[1] احمد فرج ، المرجع السابق ، ص 329.

[2] فهد عبد الله العبيد العازمي،المرجع السابق،ص484.

[3] محمد حسين منصور ، المرجع السابق ، ص 199.

الإثبات الجنائي لمثل هذه الجرائم، معرفة صاحب عقد الاشتراك على الأقل، في حين أن مزود الخدمات المعلوماتية بكل أصنافه فهم مصدر مهم في استرجاع الدليل الجنائي الإلكتروني، وهذا عن طريق مساعدة السلطات المختصة[1] ، كما أن لهم دور متميز في منع الوصول إلى المحتوى غير المشروع.

[1] ملخص القضية : في سنة 2017 و في إطار التحقيق القضائي المفتوح من طرف فصيلة الأبحاث للدرك الوطني بالجزائر والمتعلقة بالشكوى المقدمة من طرف إطار سامي بإحدى الوزارات ضد مجهول من أجل قرصنة علبة البريد الإلكتروني "a.personne@ministère.dz" ومحاولة إختراق خادم البريد الإلكتروني للوزارة، قام مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية بالبحث والتحري حول هذه القضية.

بعد الاطلاع على فحوى المراسلة، تم التنقل إلى مجمع اتصالات الجزائر ببن عكنون بصفته مورد خدمة البريد الإلكتروني الخاصة بالوزارة المعنية للقيام بالمعاينات اللازمة ورفع الآثار وكل المعلومات التقنية المتعلقة بالقضية. نتائج العملية كانت كالتالي :

بتاريخ : 2016/07/29، ابتداءا من الساعة : 14:00، قام المشتبه فيه بإرسال ملف (Word) يحتوي على برنامج خبيث (Code malicieux) إلى بعض مستعملي البريد الإلكتروني للوزارة، وذلك باستخدام علبة البريد الإلكتروني : "a.personne@ministère.dz "، والتي قام بقرصنتها في وقت سابق.

يقوم البرنامج الخبيث بتحميل برنامج آخر بإسم : "VIP.exe" من الرابط :

(https://www.dropbox.com/s/29fllwj64be4htu/vip.exe?dl=1)، هذا الأخير وبعد تحميله يقوم بتثبيت أربعة (04) برامج للتجسس وجمع البيانات الخاصة بأجهزة الضحايا، ويتعلق الامر بالبرامج التالية :

Uac-manager.exe : عبارة عن برنامج (keylogger) يقوم بتسجيل وحفظ البيانات المدخلة عن طريق لوحة المفاتيح.

Xvim.exe : برنامج يقوم بالتحكم عن بعد في تشغيل كاميرا الأجهزة المخترقة.

Lame.exe : برنامج يقوم بالتحكم في تسجيل الأصوات من الأجهزة المخترقة.

Chromeupdt.exe : برنامج يقوم باسترجاع جميع كلمات المرور المخزنة في قاعدة بيانات المستكشف (Chrome).

لغياب المعلومات التقنية الكافية والتي تسمح بتحديد هوية المشتبه فيه، تم اللجوء إلى تشغيل هذه البرامج الخبيثة في وسط افتراضي معزول (Machine Virtuelle) بهدف تحديد مكان الخادم الذي يقوم باسترجاع وتخزين المعلومات المقرصنة من أجهزة الضحايا، أين تم التوصل إلى عنوان الموقع الإلكتروني

خادم الموقع الإلكتروني : "msdnsservice.sytes.net"، متواجد في الجزائر ويستعمل خدمة الاستضافة المجانية "sytes.net" الموجهة للأفراد والتي تسمح بتحديث العنوان IP الذي يستعمله الخادم بصفة مستمرة.

تم تحديد العنوان IP : 105.101.228.232 المستعمل من طرف المشتبه فيه لاسترجاع وتخزين المعلومات المقرصنة بتاريخ : 2016/07/27 على الساعة : 10:02.

ثالثا:أصناف مزودي خدمات الإنترنت .

على أثر الخدمات التي يقدمها مزود خدمات الإنترنت، يمكن تصنيف مزودي خدمة الإنترنت إلى:

أ–مورد الوصول أو متعهد الوصول: أو مقدم خدمة الوصول ، مهمته توصيل المستخدم للشبكة ، حيث أن الخدمات التي يقوم بها ذات طبيعة فنية ، و ذلك عن طريق وضع الحاسب الخادم الخاص به الذي يرتبط بصفة دائمة بالإنترنت تحت تصرف المشتركين ، لذلك دورة تقني بحث ، فمتعهد الوصول " هو كل شخص طبيعي أو معنوي يقدم للعملاء الراغبين من الجمهور خدمة الوصول إلى الإنترنت حيث يقوم بتزويد العميل ، بمقتضى عقد اشتراك بالوسائل الفنية التي تمكنه من الالتحاق بالشبكة و الوصول إلى المواقع التي يرغب فيها و ذلك من خلال توصيله بمقدمي الخدمات [1]، و من ذلك انّه يمكن تزويد المشتركين ببرامج أو تطبيقات، كما يحدث مع اتصالات الجزائر في تزويد برنامج لحماية الأطفال من المواقع الإباحية[2].

ب –متعهد الإيواء: أي أّن وظيفته إيواء كل ما هو معلوماتي ، بداية من المعطيات و البيانات التي تأخذ إما شكل صور أو رسوم أو فيديوهات و غيرها و يقوم بهذه العملية إما شخص طبيعي أو معنوي، فهو بمثابة المؤجر لمساحة معينة من العالم الإفتراضي، و من ذلك يمكن للمستأجر أن يحوي مكانه المؤجر كل ما يرغب به دون أي رقابة ويستخدم في ذلك الحاسب المضيف ،

تعريف العنوان IP : 105.101.228.232 لدى اتصالات الجزائر مكن من الوصول إلى مستعمل لإشتراك في خدمة الأنترنت ADSL لشخص المسمى: ت. أ، الساكن بـ حي براهيم رايس – الجزائر.

بعد التنقل الى مسكن المشتبه به تم حجز جميع الوسائل المستعملة في الجريمة و تقديمه للعدالة.

–المعلومات مقدمة من طرف مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للجزائر العاصمة.بعد الزيارة الميدانية يوم 4 يناير 2018 .

[1] محمد حسين منصور،المسؤولية الالكترونية،دار الجامعة الجديدة، الإسكندرية، مصر،2009،ص 209.

[2] أطلقت اتصالات الجزائر لزبائنها الخواص خدمة المراقبة الأبوية "في أمان" التي تسمح للأولياء بحماية أطفالهم من أخطار الإبحار على الشبكة العنكبوتية.

فالحاسب المركزي الرئيسي يقوم باستضافة أجهزة أخرى من خلال الإتصال به مباشرة و يسمى المضيف لأنّه يستضيف أجهزة أخرى من خلال الإتصال به مباشرة و يسمى المضيف لأنه يستضيف البيانات و بثها و استرجاعها و الاستفادة من الخدمات الأخرى من خلال البرامج المتعددة الموجودة على الجهاز المضيف[1].

ج –ناقل المعلومات: هو الذي يتولى النقل المادي لها بوسائله الفنية، يقوم بالربط بين الشبكات ، تنفيذ لعقد نقل المعلومات ، بين الحاسبات المرتبطة بمواقع الإنترنت أو بمستخدمي الشبكة[2] ، حيث ينحصر دوره من خلال هذا التعريف في الربط بين مختلف الشبكات أي "كقاعدة عامة عدم مراقبته أو علمه بالمعلومات التي تعبر الشبكة بواسطته"[3].

د–منتج المعلومة أو مؤلفها: قد يكون شخص طبيعي أو معنوي ، وعادة يتمثل في مواقع الأخبار و المواقع الثقافية و الفنية ، و هي عادة مواقع الكترونية ضخمة محمولة من جهات معينة تعرف نفسها عن طريق طرح سؤال من نحن؟ أي عبارة عن شخص طبيعي أو معنوي يعمل من خلال وسائل تقنية وفق أحكام وشروط وضوابط على بث معلومات معينة حول موضوع معين على إحدى مواقع الشبكة المعلوماتية[4].

هـ–ناشر خدمة الشبكة المعلوماتية: هو من يقوم بإنشاء موقع على شبكة وتحريرها[5] ، ويسمح فيه بإضافة أشخاص وتلقي برامج ومعلومات وتطبيقات من قبلهم وهو من يقوم بتدوين

[1] محمد الربيعي، احمد احمد شعبان الدسوقي ، المرجع السابق، ص 206

[2] عايد رجا الخلايلة، المسؤولية التقصيرية الالكترونية، المسؤولية الناشئة عن اساءة استخدام اجهزة الحاسوب والانترنت،دراسة مقارنة ،الطبعة الاولى،دار الثقافة،عمان ، الاردن، ص56.

[3] محمد حسين منصور، المرجع السابق، ص 197

[4] إبراهيم سليمان القطاونه ومحمد أمين الخرشه المسؤولية الجزائية لمقدمي خدمة الشبكة المعلوماتية ومورديها ومتعهديها وناشريها دراسة مقارنة – الأردن الإمارات العربية المتحدة –مجلة الشريعة والقانون كلية القانون جامعة الإمارات العربية المتحدة،العدد 66،رجب 1437هـ،أبريل2016.ص239.

[5] Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p .44.

المحتوى وتحريره وصياغة وإرساله إلى موقع إلكتروني وجعله متاح أمام مستخدمي الشبكة بشروط وأحكام وضوابط[1].

و عادة ما يمكن إنشاء هذه المواقع التي توفر لها قوالب مجانية للمدونات الشخصية التي تتضمن أمور غير مشروعة بدعوة حرية التعبير.

بناء على ما سبق ذكره فانه كلّما كانت الخدمات المقدمة تُعني بتوصيل المعلومة، و إمداد التوصيلات اللازمة و تسهيل خدمة الدخول إلى شبكة الإنترنت هو مقدم لخدمة الوصول، أمّا إذا تعدى الأمر مجرد الأعمال المادية للوصول إلى الشبكة فهو بصدد تقديم خدمة الإنترنت بما تشمله من محتوى و إيواء و تخزين و إنتاج، فكل ما كانت الخدمة المقدمة من المقدم خارج العالم الإفتراضي فهو غير مسؤول عن المحتوى، و على اعتبار مقدم خدمة الإنترنت هو " المسؤول الرئيسي عن المعلومات التي تتداول على شبكة الإنترنت بإعتبار انه الوحيد الذي يملك سلطة حقيقية في رقابة محتوى هذه المعلومات[2]. إذاً مسؤولية مزود خدمة الإنترنت تتوقف بالدرجة الأولى ، على الخدمة التي يؤديها ، فدوره الأصيل هو ربط مستخدمي الإنترنت بالشبكة، فكل من تجاوز هذا الدور مسؤول بقدر اطلاعه على المحتوى غير المشروع[3].

الفرع الثاني: المسؤولية الجزائية لمزودي خدمات الإنترنت .

في هذا الفرع لا بد من الإشارة إلى الالتزامات التي اقرها المشرع على عاتق مزودي خدمات الانترنت، والتي بإهمالها يسال مزود خدمة الإنترنت جزائيا.

أولا: التزامات مقدمي خدمات الإنترنت .

[1] إبراهيم سليمان القطاونه ومحمد أمين الخرشه، المرجع السابق،ص264.

[2] عايد رجا الخلايلة ، المرجع السابق، ص59.

[3] Sedallian Valerie,Droit de l`Internet. réglementation responsabilités, contrats, collection AUI, Paris1997.p 13

يمكن تقسيم هذه الالتزامات بحسب ما اقره المشرع الجزائري و هذا بالاعتماد على نوع الخدمة المقدمة من قبلهم ، والواقع أن الإلتزامات الملقاة على عاتق مزودو خدمات الإنترنت هي التي جعلته يلعب دوراً فعالاً في أن يكون من مصادر الدليل الجنائي الإلكتروني وبالتالي الإثبات الجنائي لجرائم الإنترنت .

أ-إلتزامات متعهد الوصول :

إنّ من أهمّ مقدمي خدمة الإنترنت هو متعهد الوصول فالنشاط الرئيسي يتمحور في تزويد مستخدمي الإنترنت بالآليات التقنية لاستغلال المواقع الإلكترونية و ما تحتويه، و هذا بموجب عقد تقديم الخدمات لذا يفترض بمتعهد الوصول المسؤول احترام إلتزاماته الجوهرية الإعلامية منها و التقنية[1].فإلتزامات ذات طبيعة إعلامية، هي جوهر الاستعمال السليم لشبكة الإنترنت و التي تعني بإعلام المستخدم بمخاطر الإنترنت من جهة وضرورة احترام اللوائح و الأنظمة و خصوصا ما تعلق بحق الغير ، حيث تكمن أهمية متعهد الوصول في كونه المخول في طلب كل المعلومات عن المستخدم من هويته و أهليته و بريده الإلكتروني ، بذلك تقع عليه التزام و هو وضع حفظ هذه البيانات خلال سنة كما ذكرت ذلك المادة (11)من القانون(09-04) و هذه البيانات سواء كانت حقيقية أو وهمية مستعاره لا يمكن التأكد منها كل مرة ، ذلك مع إمكانية استخدام أسامي وهمية.أماّ التزامات ذات طبيعة تقنية فقد ذكرنا انّ دور متعهد الوصول هو الربط المستخدم بالمحتوى المعلوماتي و تسهيل العملية لذلك ، فالأصل في هذا هو عدم تدخل متعهد الوصول في المحتوى المعلوماتي، فهو يقوم بدور الوسيط بينهما فقط-أي المستخدم والمحتوى المعلوماتي-، لكن هذا لا يمنع من اخذ الحيطة اذا تعلق الأمر بالمحتوى.

[1] احمد قاسم فرج ، المرجع السابق، ص229-300.

ب –إلتزامات مقدمي الخدمة المعلوماتية:

تختلف إلتزامات مقدمي خدمة الإيواء التي تعتبر من الخدمات المعلوماتية عن خدمات النقل المادي للمضمون المعلوماتي،كما تختلف إلتزامات مورد المعلومات أو مؤلف و جامع المعلومات و إذ ننوه هنا أنّ المعلومات التي نقصدها هي المعلومات المحمية قانونا ، مع ملاحظة وانه وعند قراءتنا للمرسوم التنفيذي(98-257) والقانون (09-04) انّه لم يضع إلتزامات خاصة بكل صنف من مزودي خدمات الإنترنت ، كما لم يحدد مسؤولية كل مقدم خدمة بحسب الإمكانيات المتاحة في تقديم الخدمة فوضع الكل في مسار واحد سواء تعلق الأمر بالإلتزامات أو حتى المسؤولية، وهي النقطة التي يجب التفات إليها ، بوضع نظام قانوني خاص بمقدمي خدمات الإنترنت بما يتمتعون به من حقوق وما يلتزمون به من واجبات.

1–فإلتزامات متعهد الإيواء ، والاتجاه العام أنّ إلزام مقدمي خدمة الإيواء هو الالتزام بالإعلام[1]، أي إعلام أصحاب المواقع على الشبكة بضرورة احترام القوانين واللوائح والأنظمة واحترام حقوق الملكية الفكرية وبذل العناية اللازمة لمنع تداول المضمون أو المعلومات غير المشروعة، وذلك من خلال جهود اليقظة ، أي ممارسة الرقابة الدقيقة و العميقة و الهدف هو تصحيح وضعه أو قطع الخدمة عنه التي تتناسب وإمكانياتهم[2] .

[1] ورد تعريف الالتزام بالاعلام والذي يقصد منه إحاطة المستهلك بكافة المعلومات ذات الصلة بالمنتوج، و هذا طبقا لنص المادة (17) من قانون (09 -03) المتعلق بحماية المستهلك و قمع الغش المؤرخ في 25 فبراير2009،ج.ر رقم15 ليوم 8 مارس2009،ص12. التي تنص على أنه " يجب على كل متدخل أن يعلم المستهلك بكافة المعلومات المتعلقة بالمنتوج الذي يضعه للاستهلاك..."، و عليه يشمل الالتزام بالإعلام، التزام المتدخل بـ :

– **الإدلاء أو الإفضاء** بالمعلومات اللازمة المتعلقة بالمنتوجات أو الخدمات، و التي تشمل التعريف بها (مكوناتها، خصائصها، كميتها، تاريخ إنتاجها، نهاية صلاحيتها...)، و كذلك كيفية استعمالها.

– **التحذير** من خطورة هذه المنتوجات، ذلك أن الانتفاع بالمنتوج على أكمل وجه يقتضي من المتدخل تحذير المستهلك من مخاطر المنتوج ذاته، و كذا المخاطر الناجمة عن استعماله أو حيازته.

[2] محمد حسين منصور، المرجع السابق، ص203.

2-إلتزامات مورد المعلومات، و هو صاحب السلطة الحقيقية في مراقبة المعلومات التي تبث على الإنترنت كموقع (youtube) ، لذلك يجب أن يورد المعلومات بكل شفافية[1]، اي يتوجب على مورد المعلومات و الذي له أن يدير المعلومات و يؤلفها انّ يقوم باطلاع مستخدمي الإنترنت و متعهديّ الوصول و الإيواء على البيانات و المعلومات التي تعرف به و بالنشاط الإلكتروني الذي يديره[2]و من قبيل ذلك ما تقوم به من تعريف بنفسها و مقرها و عنوانها و مركزها، كما يجب عليه إعمال وكفالة حق الرد ، فتوريد المعلومات هو نشرها[3]، والتي تتمثل في وضع المعلومات المعالجة أليا تحت تصرف مستخدمي الشبكة بأي شكل كانت صورة أو فيديو أو رسوم أو بيانات أو غيرها.

فتوريد المعلومات عبر شبكة الإنترنت، عن طريق مورد المعلومات يتخذ صورتين إماّ أن يكون مؤلف المعلومة والناشر لها في نفس الوقت ، وهي الخدمة الأصيلة لهذا المورد أو مقدم الخدمة ، أو أن تكون في صورة نشر لهذه المعلومات وهي الخدمة الاستثنائية من مجموع ما يقدمه مورد المعلومات من خدمات عبر الشبكة، إذاً هو صاحب السلطة الحقيقة في مراقبة المضمون المعلوماتي في المشروع لذلك شبه هذا الأخير برئيس التحرير.

تطبيقا لذلك يختلف مزود المعلومات عن متعهد الإيواء ، أنّ متعهد الإيواء ليس له أن يُؤلف محتوى معلوماتي ، هو يقوم فقط بالاستضافة، ولكن يلتقيان في تقديم الخدمة المعلوماتية عبر الإنترنت [4]، لكن من كل ما تقدم نرى انّه لا يمكن إهمال أي خدمة يقدمها مزودو خدمات الإنترنت، بداية من النقل المادي للمعلومات إلى إيوائها ثمّ توريد ونشرها وتأليفها فهذه الخدمات هي التي تنتج خدمة متكاملة، لا يمكن الاستغناء عن أي مرحلة من مراحلها التقنية والمعلوماتية.

ثانيا:مسؤولية المترتبة عن الإخلال بالتزامات مقدمي خدمات الإنترنت.

[1] عمر محمد ابوبكر بن يونس، المرجع السابق، ص777.

[2] احمد قاسم فرج ، المرجع السابق، ص339.

[3] فهد عبد الله العبيد العازمي، المرجع السابق،ص485.

[4] فهد عبد الله العبيد العازمي، المرجع السابق،ص486 و487.

إنّ الاطّلاع الواسع لمزودي خدمات الإنترنت، على بيانات الإتصال والاشتراك عبر الشبكة ،واستعماله للتقنيات والبرمجيات ومزودات البروكسي وبرامج تحسس (IP)، تمكنه الحصول على كل المعلومات عن المستخدم وبالتالي تتبعه عند اقترافه أي سلوك إجرامي، وهذا مالا يعتقده المجرم المعلوماتي[1]، وخصوصا المتطفلين منهم، بعد استعمال أسماء وهمية، لكن ليس هو الأمر أو كما يظنون، فمزودي خدمات الإنترنت يملكون من التجهيزات والتطبيقات والبرامج ما يسمح لهم بتعقب الإتصالات الإلكترونية ومعرفة هوية المتصلين وبالتالي مرتكبي السلوك الإجرامي، لذلك ألقى المشرع الجزائري في إطار القانون(09-04)التزامات، أداؤها يمكن في مساعدة السلطات القضائية المختصة في تحديد هوية الجاني وتتبعه، لذلك يلعب مزود الخدمات دورا مهما في إثبات جرائم الإنترنت، على ان تقوم المسؤولية الجزائية تجاهه في حال الإخلال بها.

أ-الآراء الفقهية حول مسؤولية مزود خدمات الإنترنت :

اختلفت الآراء حول اساس المسؤولية الجنائية لمزود خدمات الإنترنت، فسنعرض أولا من أنكر هذه المسؤولية ثم بعد ذلك من قال بوجوب أن يتحمل مقدم الخدمات مسؤولية جرائم الاستخدام غير المشروع للانترنت.

1- الرأي الأول:يؤسس عدم مسؤولية مزود خدمات الانترنت على أساس أن العمل الذي يقوم به هو تقني بحث، يتمثل في عملية التوصيل، وبالتالي عمله لا يمنحه القدرة على تتبع مستخدم الإنترنت [2].وهو ما يعطل الحق في حرية الكلمة والصحافة، فهم ليسوا ناشرين للمضمون المعلوماتي[3].

[1] فهد عبد الله العبيد العازي،المرجع السابق،ص482.

[2] جميل عبد الباقي الصغير ،الانترنت والقانون الجنائي،المرجع السابق،ص119.

[3] منى فتحي أحمد عبد الكريم، المرجع السابق،ص148.

مع وجود الملايين على شبكة الإنترنت، فإنّه من غير المعقول مساءلة مزود خدمة على قذف أو سب على موقع بالإضافة إلى ذلك ظهور عدة مصطلحات، أو حتى لغة مختلف عن متمثلة في لهجات محلية مدعمة بأرقام مقلوبة، واختصارات لفظية من المستحيل مراقبتها ، ومن هنا نستنتج أنه لا يمكن مساءلة مزود خدمات الإنترنت .في حين يرى جانب من الفقه غير ذلك.

2- الرأي الثاني: يذهب إلى انّ المساءلة الجنائية لمزود خدمات الانترنت تكون على أساس المسؤولية التوجيهية[1]، فمادام أنّ مزود الخدمة هو المسؤول عن خدمة الإنترنت، فهو بصفة أو بأخرى مسؤول على الأقل ما تحويه صفحات الشبكة من بيانات مخالفة للنظام العام والآداب العامة ، كما يمكنه أن يفرض قيود لتحكم المستخدمين عن إساءتهم أو استخدامهم غير المشروع للانترنت ، حيث انّه وبالإمكانيات التقنية التي يملكها، عليه واجب الإشراف[2].

وبالرجوع إلى المشرع الجزائري فقد حسم الموضوع ، وكما ذكرنا لم يفرق بين مقدمي خدمة الإنترنت، فالكل مسؤول والكل يخضع للالتزامات، وانّ المشرع الجزائري ومن خلال مواد مساعدة السلطات والالتزامات التي تقع على عاتق مزود الخدمات والمسؤولية المترتبة عنها من خلال القانون (09-04) ، لكن هذه الالتزامات والمسؤولية الجنائية المترتبة عنها تتعلق بدور في التحري والإثبات ومساعدة السلطات في ذلك.

ب- جريمة الإخلال بالالتزامات الخاصة بمزودي خدمة" الإنترنت ".

اوجد التطور التقني للإعلام والاتصال تداخلا في خدمات مزودي خدمة الإنترنت، مما صعب من عملية التفريق بينهم من ناحية المسؤولية، وفي النقطة الموالية سندرس المسؤولية المترتبة خصوصا عند الإخلال بالالتزامات الخاصة الملقاة على عاتقه فقط[3].

[1] جميل عبد الباقي الصغير، القانون الجنائي، المرجع السابق، ص118.

[2] منى فتحي أحمد عبد الكريم، المرجع السابق،149.

[3] أمّا اذا تعلق الأمر بإفشاء أسرار التحري-هي من بين الجرائم التي أحالها المشرع الجزائري على القواعد العامة-وجريمة عرقلة حسن سير التحريات سوف نتعرضلها بالتفصيل في المبحث الأخير من الفصل الثاني من الباب الثاني.

1-الركن الشرعي لجريمة الإخلال بالالتزامات الخاصة بمزودي خدمة" الإنترنت ".

نصت المادة12:زيادة على الالتزامات المنصوص عليها في المادة11أعلاه ، يتعين على مقدمي خدمات "الإنترنت " مايلي:

أ-التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين أو جعل الدخول إليها غير ممكن ،

ب -وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها."

ويتضح لنا من كل ما سبق أنّ المشرع الجزائري وبموجب القانون (09-04)فرض إلتزامات عامة[1] وخاصة[2] على مقدمي خدمة الإنترنت .

[1] التزام بمساعد السلطات عن طريق حفظ المعطيات المتعلقة بحركة السير هذه الأخيرة تساعد السلطات المختصة، وهي الهيئة ذات الاختصاص الوحيد في البحث والتحري في جرائم الإنترنت، بأن تسمح بحفظ معطيات مستعمل خدمة الإنترنت،هذه المعطيات هي بمثابة هوية الإتصال، والتي عن طريقه يمكن تحديد مصدر الإتصال هل هو وطني أو دولي، وكذا تحديد المكان مما يسهل المتابعة ، وفي الواقع قلنا هو تحديد لوسيلة الإتصال وليس للمشتبه فيه نفسه،ومما لا شك فيه أنّ قيام مقدم الخدمات بهذه العملية هو من قبيل الاعتداء على الحق في الحياة الخاصة ، ولكن مادام القانون أمر بذلك ، فهي تدخل في نطاق الأفعال المبررة طبعا غير ما تعلق منها بكتمان السر المهني، وقد حدد المشرع الجزائري مدة الاحتفاظ بهذه البيانات بسنة واحدة، من هنا نلاحظ أنّ مقدمو خدمات الإنترنت هم من أهم مصادر الدليل الجنائي الإلكتروني في جرائم الإنترنت، بكل ما يملكون من وسائل تقنية وتراخيص قانونية لحفظ والتعرف على المعطيات الخاصة بمستعملي الخدمة ، أينما كانوا وحيثما تواجدوا.

[2] وقبل القانون (09-04)وضع المشرع التزامات في مواجهة مقدمي خدمات الانترنت . في المرسوم التنفيذي(98-257)المؤرخ في 25 أوت 1998 في المادة 14 من المرسوم التنفيذي رقم(98-257) منها التقنية ، والأخلاقية ، كما اقر مسؤوليته ، كالآتي : **الالتزامات التقنية** :فرض المشرع الجزائري على مقدمي خدمات الانترنت التزامات تقنية تتمثل في تسهيل النفاذ إلى خدمات الانترنت حسب الإمكانيات المتوفرة إلى كل الراغبين في ذلك باستعمال أنجع الوسائل التقنية ، وكذا إعطاء مشتركيه معلومات واضحة ودقيقة حول موضوع النفاذ إلى خدمات الانترنت وصيغة مساعدتهم كلما طلبوا ذلك ، وكذلك عرض أي مشروع خاص باستعمال منظومات الترميز على اللجنة . كما ألزمهم باتخاذ كل الإجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات المفتوحة لمشتركيه قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الاداب العامة اما **الالتزامات غير التقنية** :وحفاظا على الحق في الحياة الخاصة لمشتركيه ألزم المشرع مقدمي خدمات الانترنت المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه الخاصة وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون، إذ يلتزم بالحفاظ على معطيات مشتركيه وإلا سئل عن جريمة إفشاء الأسرار المنصوص عليها في المادة من قانون العقوبات (301) ، كما فرض عليهم التزام أخلاقي متمثل في احترام قواعد حسن السيرة بالامتناع خاصة عن استعمال أي طريقة غير مشروعة سواء اتجاه المستعملين أو تجاه مقدمي خدمات الانترنت الآخرين ، إضافة إلى

2-الركن المادي لجريمة الإخلال بالالتزامات الخاصة بمزودي خدمة" الإنترنت ".

انّ الركن المادي يتمثل في تنفيذ الالتزامات الملقاة على مزود الخدمات بموجب المادة (12)من القانون (09-04) سالف الذكر، ولكن الأهم إثبات هذه التزامات التي حدد طرقها المشرع الجزائري.

-التزامات مقدمي خدمة الإنترنت خاصة:

الزم المشرع الجزائر مزود خدمات الانترنت التدخل الفوري لسحب المحتويات غير المشروعة أو إعاقة الدخول إليها، ووضع الترتيبات اللازمة لحصر وليس منع الدخول إلى مواقع مخالفة للنظام العام[1]والآداب العامة[2]، وإخبار المشتركين بها، دون أن يرتب أي عقوبات في حالة إخلاله بهذا الالتزام أو تعديه ومنعه محتوى معلوماتي قد لا يروق له، وهو تعدي على الحق في المعلومة، مع العلم أنّ التزامات الخاصة أو العامة التي اقرها المشرع الجزائري في إطار القانون(09-04) ماهي إلا تذكير بالالتزامات المقررة بموجب المرسوم التنفيذي (98-256) سالف الذكر[3].

حيث أنّ هذه الالتزام يدخل في إطار الضبط الإداري، ولكن هذا الالتزام وجد من غير مقابل، كما سبق ذكره لذلك لا يمكن للسلطات المختصة أن تتابع مزود الخدمات عن أي سلوك إذا لم ينص صراحة على أنّ إتيانه أو الامتناع عنه يعد جريمة ، - وهذا ما تفطن إليه المشرع

هذه الالتزامات فرض المشرع على مقدمي خدمات الانترنت التزامات متمثلة في تحمل مسؤولية محتوى الصفحات وموزعات المعطيات التي يستخرجها يتعلق بمحتوى الصفحات التي يستخرجونها وفقا للأحكام التشريعية المعمول .

[1] النظام العام مجموعة المصالح الأساسية التي يقوم عليها كيان مجتمع سواء كانت سياسية او اجتماعية او اقتصادية فقواعد النظام العام هي تلك التي يقصد بها تحقيق مصلحة عامة التي هي كل أمر يتعلق بالنظام الأساسي للمجتمع بحيث يرجح على كل مصلحة فردية، ابتسام القرام، المصطلحات القانونية في التشريع الجزائري،قصر الكتاب، البليدة،الجزائر1998.ص41.

[2] الآداب العامة فهي مجموعة المبادئ الأخلاقية السائدة في المجتمع و التي تمثل الحد الأدنى للقيم و الأخلاق العامة الضرورية لحماية المجتمع من الانحلال .

[3] Hadjira Bouder,fournisseures de services I nternet , Prevention et lutte contre la cybercriminalite ,actes du seminaire international alger le 5-6 mai 2010 ,CRJJ ,2011.P209

الجزائري واستدركه في تعديل قانون العقوبات لسنة 2016 بان على ذلك في المادة (394مكرر8)[1].

في حين وانه من ناحية ثانية، أعطيت لمقدم الخدمات الحق في التدخل ومنع بعض المحتويات قد تكون بعيدة كل البعد عما نصت عليه المادة (12) من القانون(09-04) ، أو العكس يتنصل من المسؤولية بوضع رسائل وبنود عند التسجيل، ترفع عنه أي مسؤولية تخص الأفراد وسلوكياتهم أو أرائهم مهما كانت متطرفة ، لأنه قد لا يكفي أن تكون مثلا الرسائل غير المشروعة في مواقع لمجموعات الأخبار أو التواصل الاجتماعي دليل على أنّ المحتوى غير مشروع[2].

-**إثبات الاخلال بالتزامات الخاصة** :يتمثل السلوك الاجرامي في جريمة الإخلال بإلتزامات الخاصة في عدم الالتزام بسحب المحتوى غير المشروع وهو المحتوى الذي يمس النظام العام والآداب العامة، أو حتى الإخلال بوضع ترتيبات تقنية، يمنع الولوج للمعلومات غير المشروعة،كما ذكرنا سابقاً لذلك فان الامتناع عن سحب المحتوى ، بعد التدخل يمكن إثباته عن طريق:

– اعذاره من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ، وهذا بما تملكه من صلاحيات في مراقبة الوقائية للاتصالات الإلكترونية.

[1] المادة(394مكرر8) ق.ع.ج "دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول ، يعاقب بالحبس من سنة إلى ثلاث(3) سنوات وبغرامة من 2.000.000دج إلى 10.000.000 دج ، أو بإحدى هاتين العقوبتين فقط ، مقدم خدمات "الإنترنت " بمفهوم المادة (2)من القانون رقم (09-04) المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ، الذي لا يقوم رغم اعذاره من الهيئة الوطنية المنصوص عليها في القانون المذكور أو صدور أمر أو حكم قضائي يلزمه بذلك:

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

ب-بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة(أ) من هذه المادة أو لجعل الدخول إليها غير ممكن."

[2] Sedallian Valerie, droit de l`internet, op.cit 139 .

–صدور أمر أو حكم قضائي يلزمه بذلك[1] ، وهنا يمكن تصور الإعذار عن طريق شكوى من الضحية ولكن المشرع لم يذكرها في سياق ، المادة السابقة والتي قد تكون من بين الإجراءات المهمة التي تمنع الوصول إلى المحتوى غير المشروع من طرف مزودي خدمات الإنترنت ، ولكن طبعا بشروط وقد تكون الشكوى تخص جرائم معينة تتعلق بحماية الحق في الحقوق الشخصية ، كالحق في حرمة الجسد والصورة.

وفي غير هذه الحالات المذكورة على سبيل الحصر، لا يمكن إثبات تجاوز مزود خدمات الإنترنت لالتزامه وبالتالي قيام المسؤولية الجزائية في هذه الجريمة، لذلك قد يلعب البلاغ أو الشكوى من المتضرر دورا في سحب أو منع الولوج إلى المحتوى غير المشروع،فتنتفي عن المزود المسؤولية الجزائية.

3–الركن المعنوي:أن هذه الجريمة هي جريمة عمديه تتطلب توافر القصد الجنائي العام والخاص، أي العلم والإرادة، العلم بالمحتوى غير المشروع ولم يتم وضع التقنيات اللازمة، للتصدي له ومنع الوصول إليه، أو حتى وضع التقنيات المناسبة ، رغم أعذاره من الهيئة أو وجود حكم أو قرار قضائي.

"مما دفع شركات الخدمة الكبيرة، مثل(Hotmail)و(Yahoo) و غيرهما إلى التشدد في مراقبة المشتركين وتقديم معلومات عنهم وعن عناوينهم وعن (IP) أي أجهزة الكمبيوتر المستخدمة للدخول إلى الإنترنت إلى الجهات القانونية حتى لا تتعرض هذه الشركات إلى الملاحقة القضائية[2]. فبعيدا عن أي ضمانات اقرها المشرع الجزائري لحماية الحياة الخاصة في مواجهة مقدم خدمة الإنترنت ، ومن خلال كل ماسبق ذكره ، فقد أكدنا أنّ مقدم خدمات الإنترنت هو من

[1] يمكن تصور ذلك مثلا في طلب متضرر من الجهة القضائية المختصة اتخاذ تدابير تحول دون المساس بحقوق معينة كحقوق المؤلف والحقوق المجاورة ، بإجراءات تحفظية والتي تمس مثلا منع الوصول إلى محتوى غير مشروع والذي يتمثل هنا في الاعتداء على حقوق المؤلف عن طريق الانترنت، ويخطر مزود الخدمات بهذا القرار عن طريق الجهة القضائية المصدرة له ، المادة 144 و147 من الأمر 03-05 مؤرخ في 19 جمادى الاولى عام 1424 الموافق 19 يوليوسنة 2003،يتعلق بحقوق المؤلف والحقوق المجاورة،ج ر عدد 44 ليوم23 يوليو سنة 2003، ص20.

[2] فهد عبد الله العبيد العازمي، المرجع السابق،ص481.

المصادر المهمة التي يمكن لسلطات البحث والتحري، أن تجد ضالتها في البحث عن الدليل الجنائي الإلكتروني ، بمساعدة مقدم خدمة الإنترنت، الذي يعتبر شريكا مهما وطرفا أهم لجمع الدليل الجنائي المتعلق بجرائم الإنترنت .

من كل ما سبق تفصيله بمجمل ما يقدمه مقدم خدمات الإنترنت الذي ، لم يفصل المشرع الجزائري في أنواعه وحتى الخدمات المقدمة من طرفه ، كان لابد على المشرع الجزائري أن يفرق بين مختلف أصنافهم ، هذا التصنيف الذي سوف يحدد بدقة مسؤولية كل مقدم خدمات على حدٍ ، فمقدم خدمة الوصول يختلف عن مقدم خدمة الولوج[1] ، ورغم ذلك فقد أقر مسؤولية مقدم الخدمات وهذا بحسب الالتزامات الملقاة على عاتقه، إضافة إلى ما تعلق بالاعتداء على الحق في الحياة الخاصة وإفشاء السر المهني باعتباره من أصحاب المهن، وأن تقيده أي مزود الخدمات بالالتزامات الملقاة على عاتقه تجعله في منأى عن المساءلة الجزائية.

[1] Hadjira Bouder.fournisseures de services Internet , Prevention et lutte contre la cybercriminalité,actes du seminaire international alger le 5-6 mai 2010 , Centre de Recherche Juridique et Judiciaire CRJJ ,2011.P209

المبحث الثاني:دعائم الإثبات الجنائي في جرائم الانترنت.

إنّ الهدف من الإثبات هو تبيان التطابق بين النموذج القانوني للجريمة وبين الواقعة المعروضة، لأجل هذا نلجأ إلى وسائل معينة هي وسائل الإثبات، ووسيلة الإثبات هي كل ما يستخدم في إثبات الحقيقة، فهي نشاط يبدل في سبيل اكتشاف حالة أو مسالة أو شيء ونقلها إلى المجال الواقعي الملموس[1]، وان الاعتماد على دليل الجنائي الالكتروني فقط لإثبات جرائم الانترنت يجعل هذه العملية مشوبة بنقصان، لأنّه لا يمكن أن يكون الدليل الجنائي الالكتروني وحده دليلٌ قائمٌ بذاته ليس لنقص في الدليل ذاته، بل في الصورة التي يتواجد عليها أي الصورة غير الملموسة، والتي لها حيز مادي يشملها، وهنا تأتي الأدلة ووسائل الإثبات الأخرى لتكميل العملية الاثباتية من دعائم قولية واستدلالية (المطلب الأول) ودعائم الإثبات المادية (المطلب الثاني) ، إن الدليل الجنائي الالكتروني تقف حدوده عند التعرف على عنوان بروتوكول الانترنت، وفى أفضل الفروض الوصول إلى المنظومة المعلوماتية الذي ارتكبت منها الجريمة، فهى لا توصلنا إلى معرفة الفاعل الحقيقي.

المطلب الأول:الدعائم القولية والاستدلالية(شهادة الشهود والقرائن)

إنّ إدراج طرق إثبات معينة كدعائم للإثبات الجنائي في جرائم الانترنت، لما لمسنا فيها من إمكانية أن تكون مفيدة ومنتجه في عملية الإثبات، ولتأقلمها الواضح مع تكنولوجيات الإعلام

[1] فهد عبد الله العبيد العازمي،المرجع السابق،ص 358.

والاتصال دون غيرها من طرق الإثبات الأخرى في مجال التحقيق والتحري، خصوصا انّ تكون معدة مسبقا للإثبات، لذلك نستثني من الدعائم القولية والاستدلالية استجواب المتهم واعترافه، ونبقي على شهادة الشهود (الفرع الأول) والقرائن (الفرع الثاني)

الفرع الأول: شهادة الشهود في جرائم الانترنت.

لشهادة الشهود في مجال الإثبات الجنائي كدليل أهمية بالغة، وهي لازالت تحتفظ بدورها الهام وقيمتها الكبيرة، باعتبار الجريمة عمل غير مشروع يجتهد الجاني في التكتم عند ارتكابها، ويعمل على إخفائها، من هنا كان وجود شاهد على الجريمة مكسبا للعدالة وحسن سيرها[1] ،في ظل تراجع بعض الأدلة الأخرى كالاعتراف في مجال الجرائم العادية، وقد احتفظت بنفس القيمة الثبوتية إن لم نقل قد تضاعفت في مواد جنائية كجرائم تكنولوجيات الإعلام والاتصال.بان حددت لها شروط معينة وأشخاص محددين للإدلاء بها، بطرق تتناسب و عصرنه العدالة.

تعتبر الشهادة من دعائم الإثبات الجنائي في جرائم الانترنت أو جرائم تكنولوجيات الإعلام والاتصال، وهي لازالت تحتفظ بقيمتها في الجرائم العادية، فهي الطريق العادي للإثبات الجنائي لأنها تنصب في المعتاد على حوادث عابرة تقع فجأة لا يسبقها تراض أو اتفاق[2]، كما هو الحال في جرائم النصب وخيانة الأمانة والتزوير التي تعتمد في إثباتها المحررات،

فالشهادة هي ما يدركه الشخص بحواسه الخمس الرؤية والسمع والشم واللمس والذوق، إذ الشهادة "ما أدركه الشخص التي تقبل شهادته بأحد حواسه مطابق لحقيقة الواقعة فهي إقرار للشخص عن واقعة أو وقائع متعلقة بالدعوى، أدركها مباشرة بحاسة من حواسه، يؤديها بشكل شفوي أمام الجهات القضائية، بعد حلفه اليمين القانونية"[3]، لذلك هي التعبير الصادق الذي

[1] إحمود فالح الخرابشة، الإشكالات الإجرائية للشهادة في المسائل الجزائية، دراسة مقارنة، ط 1، دار الثقافة ، عمان، الأردن، ص23.

[2] مصطفى محمد الدغيدي ،التحريات والإثبات الجنائي.شركة ناس للطباعة ،2004، ص117.

[3] إحمود فالح الخرابشة،المرجع السابق، ص35.

يصدر في مجلس القضاء من شخص يقبل قوله بعد أداء اليمين في شأن واقعة عاينها بحاسة من حواسه.[1]

وإذا كانت شهادة الشهود تقبل بشروط منصوص عليها في قانون الإجراءات الجزائية من أي شخص بأي مستوى علمي أو اجتماعي، فهي ليست كذلك في جرائم الانترنت،- وهذاراجع طبعا إلى اختلاف مسرح الجريمة الافتراضي والدليل الناتج عنها ،الدليل الجنائي الالكتروني-لدى يجب أن تكون من قِبل أشخاص متخصصين في التكنولوجيات الاعلام والاتصال، وعادة ما يملكون معلومات مهمة تخص المنظومة المعلوماتية، ولما كان هناك اختلاف بين الشهادة العادية والشهادة في جرائم الانترنت،هذا لا محال يؤدي إلى اختلاف فئات الشهود فيها وكذا اختلاف طرق أدائها.

كيف يمكن الاخد بشهادة الشهود في جرائم الانترنت كدليل للإثبات؟ من المخول للإدلاء بها اي الشاهد المعلوماتي(أولا)، وماهية الالتزامات الملقاة على عاتقه في جرائم الانترنت (ثانيا).

أولا:الشاهد ألمعلوماتي.

يختلف الشاهد في جرائم الانترنت باختلاف طريقة الإثبات، وهذا باختلاف محلها، فالشاهد في مثل هذه الجرائم "هو الفني صاحب الخبرة والتخصص وتقنية وعلوم الحاسب، والذي تكون لديه معلومات جوهرية لازمة لولوج نظام المعالجة الآلية... وإذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله"[2].

الجريمة محل الشهادة تشمل النظام ألمعلوماتي[3]، بمفهومه الواسع والذي يتضمن حتى الشبكات المحلية والدولية.إذ يطلق على الشاهد في جرائم الانترنت مصطلح الشاهد ألمعلوماتي تمييزا له عن

[1] هلالي عبد الله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، ط 2، دار النهضة العربية، القاهرة، مصر، 2008، ص35.

[2] هلالي عبد الله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية ،المرجع السابق،ص23.

[3] النظام ألمعلوماتي المنظومة المعلوماتية:أي نظام منفصل أو مجموعة من الأنظمة المتصلة يبعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرامج معينة

الشاهد التقليدي، إن صح القول في الجريمة بصورتها التقليدية كما نص عليها في قانون العقوبات[1].

مواكبة للتطور التشريعي، أدرج المشرع الجزائري بعض النصوص تتضمن تعديلات في شهادة الشهود وبالضبط في شخص الشاهد والمتمثل في حماية الشهود[2]،من مختلف الاعتداءات التي قد تطالهم أو دويهم في جرائم معينة، لدى سوف نناقش أولا فئات الشاهد ألمعلوماتي ،تم الحماية التي اقرها المشرع للشهود من خلال التعديل الأخير للإجراءات الجزائية.

أ- فئات الشاهد ألمعلوماتي[3].

إن ظهور فئات تكون مؤهلة دون غيرها للإدلاء بالشهادة في جرائم تكنولوجيات الإعلام والاتصال، من المظاهر التي ميزت جرائم تكنولوجيات الإعلام والاتصال عن باقي الجرائم.لدى لابد أن يكون الشاهد ألمعلوماتي إما من الأشخاص الذين لهم صلة بالمنظومة المعلوماتية أو من أشخاص لهم صلة بالانترنت.

1- أشخاص لهم صلة بالمنظومة المعلوماتية[4].

يكون قائم تشغيل الحاسوب أو خبير برمجة ، أو مخطط برامج النظم أو مخطط برامج تطبيقات أو محلل أو مهندس صيانة واتصالات.

---

[1] عبد الفتاح بيومي حجازي،مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت،دار الكتب القانونية،المحلة الكبرى ،مصر ،2007،ص157.

[2] الأمر رقم (15-02)المؤرخ في 7 شوال عام 1436 الموافق 23 يوليو 2015 يعدل ويتمم الأمر رقم(66-155)المؤرخ في 18 صفر عام1386 الموافق 8يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية ،ج.ر رقم 40 ليوم 23 يوليو 2015،حيث أضاف فصل سادس من الباب الثاني للكتاب الأول بعنوان "حماية الشهود والخبراء والضحايا" من المواد 65مكرر19 إلى 65مكرر 28.

[3] هلالي عبد الله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، المرجع السابق،ص33 وما بعدها

[4] على محمود على حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي،المرجع السابق،ص49، عبد الفتاح بيومي حجازي،مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت ، المرجع السابق،158-160.

–مشغلو الحاسب الآلي:هو ذلك الشخص المسئول عن تشغيل الجهاز والمعدات والملحقات والأدوات المتصلة به،حيث يتمتع مشغلو الحاسب الآلي والانترنت بخبرة كبيرة جدا في استخدامهما ولواحقهما.

-خبراء البرمجة:هم الأشخاص المتخصصين في كتابة أوامر البرامج الخاصة بالحاسب الآلي،ويتم تقسيم الخبراء إلى مخططي برامج التطبيقات ومخططي برامج النظم ،حيث يقوم مخططو برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم،ومن ثم تحويلها إلى برامج دقيقة وموثقة لتحقيق يجمع هذه المواصفات،أما الفئة الثانية فهي مخططي برامج النظم ،فان دورهم يلخص في اختيار وتعديل وتصحيح برامج نظام الحاسب الداخلي المعقدة.

–المحللون:المحلل هو ذلك الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام المعاينة ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة، واستنتاج العلاقات الوظيفية بين هذه الوحدات.

–مهندسو الصيانة والاتصالات:هم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

–مديرو النظم.وهم الذين يوكل إليهم أعمال الإدارة في النظم المعلوماتية.

وبالنظر إلى اختلاف الشاهد ألمعلوماتي عن الشاهد العادي، هنا يلاحظ أنّ الشاهد العادي قد يلعب دور مهم في إكمال العملية الاثباتية في جرائم الانترنت،عندما يتعلق الأمر بالنشاط المادي في العالم الواقعي لمجرم الانترنت، مثلا كأن يحدد من طرف السلطات المختصة مصدرالسلوك الاجرامي عبر الانترنت عن طريق[1] (IP) هو عنوان الكمبيوتر المتصل، الذي قد يكون في مقهى

[1] " احد أهم البروتوكولات الأساسية وهو عبارة عن رقم مكون من أربعة أجزاء في كل جزء اقل من 256 يعرف الجزء الأول من الرقم بدءا من اليسار المنطقة الجغرافية والجزء الثاني يحدد المنظمة أو الحاسوب المزود والجزء الثالث يحدد مجموعة الحاسبات التي ينتمي إليها الجهاز أما الجزء الرابع

الانترنت (cyber café) أما الشاهد أو الشهود فهم صاحب أو مساعد صاحب المحل أو غيرهما، من الذين يشهدون على ما وقع، كالتردد المنتظم للمشتبه فيه على مقهى الانترنت.وعلى نفس الكمبيوتر، مما قد يساعد في متابعته.

2-أشخاص لهم صلة بالإنترنت.

إن التطور الحاصل في شبكة الانترنت قد ابرز للوجود مقدمين لخدماتها، سواء بالتوصيل أو النشر أو غيرها من الخدمات، بحيث أصبح إضافة فئة جديدة للشاهد ألمعلوماتي ،على الفئات السابقة أمر ملح،تتمثل في أشخاص على صلة وثيقة بالإنترنت، ودراية عالية في تسيرها وتتمثل في مقدمي خدمة الانترنت بأصنافهم من متعهدي وصول وإيواء بالإضافة إلى مستخدم الانترنت ومهندسو الصيانة للشبكات والتخزين والنشر[1].

إذا سلمنا أن هذا الطرح صحيح بناءا على الالتزامات التي وضعها المشرع الجزائري لمقدمي خدمة الانترنت من خلال نصوص القانون (09-04)،والتي تتطابق والالتزامات في الآراء الفقهية،إلا أنّه لا جدوى من هذا التقسيم لسبب أن الشاهد في كلا الفئتين يتمتع بمهارات تقنية ،لا يمكن إلغاؤها كشرط من شروط الشهادة في مجال جرائم المرتبطة بتكنولوجيات الإعلام والاتصال،كما أن هذا التصنيف أي تقسيم الشهود في مثل هذه الجرائم على أساس الفصل بين الحاسب الآلي أو المنظومة المعلوماتية وشبكة الانترنت لا فائدة قانونية مرجو منه في ظل الاندماج الوثيق بين الإعلام والاتصال، فالمراكز القانونية تبقى نفسها في ظل توافر الشروط القانونية،كما أن من حقوق الشهود في جرائم المرتبطة بتكنولوجيات الإعلام والاتصال الحماية ضد أي اعتداء.

والأخير فهو يحدد الجهاز المستخدم ويمكن اعتبار هذا الرقم نوعا من الخرائط الخاصة بالانترنت حيث يمكن الاتصال بأي حاسوب أو أي موقع من خلال نقطة معينة على هذه الخريطة".حسين بن سعيد الغافري ،المرجع السابق،ص19.

[1] عبد الفتاح بيومي حجازي،مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت ،المرجع السابق،ص159

ب–حماية الشهود.

بعد صدور تعديل قانون الإجراءات الجزائية الذي جاء بتغيرات مهمة على مستوى الحريات العامة، خصص المشرع الجزائري فصلا كاملا من أجل حماية الشهود والخبراء والضحايا في المادة (10) الباب الثاني من الكتاب الأول من الأمر رقم (66-155) المؤرخ في 18 صفر 1386 بفصل سادس عنوانه "في حماية الشهود والخبراء والضحايا" .

1–تعريف حماية الشهود.

من بين التعديلات في قانون الإجراءات الجزائية لسنة 2015 ،عشرة مواد قانونية من المادة (65مكرر19) إلى المادة (65 مكرر 28)، هي إضافة موفقة للمنظومة الإجرائية، و يتعلق الأمر بحماية الشهود الذين بسبب الخوف من إلحاق الأذى بشخصيتهم أو بدويهم يحجمون في الكثير من الأحيان عن الإدلاء بشهادتهم على أكمل وجه، فجاء المشرع لفرض ضمانات لحمايتهم قبل مباشرة المتابعة الجزائية أو في أي مرحلة من مراحل الإجراءات القضائية، تتم هذه الحماية إما بطلب الشخص المعني أو بطلب ضابط الشرطة القضائية، و يتم هذا من قبل السلطة القضائية المختصة وهذا وفق ما جاءت به المادة (65 مكرر21)من القانون (15-02)الذي يعدل ويتمم الأمر رقم (66-155) المتضمن قانون الإجراءات الجزائية.

الجدير بالذكر أن هذا الإجراء أو البرنامج المتعلق بحماية الشهود، هو ما ذكرته المادة(32) من اتفاقية الأمم المتحدة لمكافحة الفساد، المعتمدة من قبل الجمعية العامة للأمم المتحدة بنيويورك يوم 31 أكتوبر 2003، والتي صادقت عليها الجزائر بتحفظ بالمرسوم الرئاسي رقم(04-128) مؤرخ في 29 صفر 1425 الموافق 19 أبريل 2004[1] .

يتمثل هذا الإجراء في الحماية الإجرائية وغير الإجرائية كما ذكرنا سابقا، عن طريق العديد من الوسائل كإخفاء المعلومات المتعلقة بهوية الشاهد، رقم هاتفه، مقر سكناه، والعديد من

[1] الجريدة الرسمية للجمهورية الجزائرية، العدد 26 ليوم 25 أبريل 2004، ص12.

الإجراءات والهدف منها الحفاظ على الشاهد وعائلته ضد المتهم في جرائم حددت بموجب المادة (65 مكرر19) من قانون الإجراءات الجزائية وهي الجريمة المنظمة[1] أو الإرهاب أو الفساد.

2-حماية الشهود في جرائم الانترنت.

من خلال نصوص حماية الشهود نجد أن المشرع هذه المرة قد خرج عن قاعدة الجرائم الخاصة التي حددها بموجب المادة (65 مكرر) قانون الإجراءات الجزائية، حيث كانت الإجراءات الخاصة[2] ينصص عليها بالتوازي مع الجرائم الخاصة-أي أنّ المشرع الجزائري خص إجراء حماية الشهود فقط لشهود الجريمة المنظمة والإرهاب والفساد وبالتالي استثنى باقي الجرائم منها جرائم الانترنت أو الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال- ، ويرجع السبب في أن المشرع الجزائري أفرغ محتوى الاتفاقية في القانون فقط دون أن يرجع إلى تحديد كل الجرائم الخاصة ومنها جرائم المرتبطة بتكنولوجيات الإعلام والاتصال،فكان لابد من إيجاد نوع من التوازن بين الإجراءات الخاصة التي فيها اعتداء على الحياة الخاص بمقابل لابد من حماية الضحية والشاهد والخبير .

خصوصا أنها إجراءات سوف تساعد في كشف وملاحقة المتهمين في العديد من الجرائم الخاصة كما هو الحال في جرائم المخدرات، وجريمة عبر الوطنية وجرائم الصرف وجريمة المعالجة الآلية للمعطيات التي يعتبر فيها شهادة الشهود من أبرز طرق الإثبات الأكثر فاعلية في القضاء بالبراءة أو الإدانة.

والعمل على أن تكون حماية الشهود وسيلة فعالة لأداء الشهود كما يجب لذلك "يجب البعد عن أساليب الاستجواب التي تنطوي على التحرش والترهيب بالنسبة للشهود لأن ذلك سيؤدي

[1] يتعين عن كل دولة طرف أن تتخذ تدابير ملائمة في حدود إمكاناتها لتوفير حماية فعالة من أي انتقام أو ترهيب محتمل للشهود في الإجراءات الجنائية الذين يلبون شهادة بخصوص الجرائم المشمولة بهذه الاتفاقية، وكذلك لأقاربهم وسائر الأشخاص ألوثيقي الصلة بهم حسب الاقتضاء، المادة 24 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة فقرة 01.

[2] تتمثل الإجراءات الخاصة في إجراءات يتم تقليص ضمانات المشتبه فيه إلى أضيق الحدود لتمس بذلك حياته الخاصة كالتسرب واعتراض المراسلات ومراقبة الاتصالات الالكترونية.

إلى إصرار الشاهد على تغيير الحقائق"[1]فبدل أن نحمي الشاهد تدفعه إلى تغيير الحقيقة التي أدركها بإحدى حواسه و"يتشجع الشاهد ويقدم على الإدلاء بشهادته عندما يشعر بالأمان على نفسه وعلى عائلته وأقاربه من بعده، أما إذا كان هناك خطر يهدده بسبب إدلائه شهادته فإنه سوف يحجم عنها، وربما يصل الأمر إلى الامتناع عن الحضور أو قلب الموازين إذا حضر لصالح المجرم خوفا من بطشه على نفسه أو على أقاربه.[2]

ثانيا:التزامات الشاهد ألمعلوماتي.

تجدر الملاحظة والإشارة أن هناك اختلافاً واضحاً بين الشاهد العادي أو التقليدي والشاهد المعلوماتي، ففي الجرائم العادية كل شخص تنطبق عليه شروط أداء الشهادة هو أهل لها، في حين أن الشاهد في جرائم الانترنت لابد أن يكون منتميا إلى الفئات التالية ليعتد بشهادته، يقع على الشاهد واجب التعاون مع القضاء ،فهناك التزام عام بموجبه يلتزم كل مواطن باتخاذ المبادرة في إعلام القضاء الجنائي بما وصل إلى علمه حول ارتكاب الجريمة الجنائية[3].

فالشاهد في الجرائم العادية ملزم بالحضور متى ما تم استدعاؤه وإلا تعرض للعقاب أو إجباره للحضور مالم يكن تمت عذر مقبول وفق نص المادة (2/97) من ق.ا.ج.ج، حيث يجب أن يحلف اليمين قبل أداءه الشهادة، لكي تكون لها قيمة قانونية وفق المادة (2/93) من نفس القانون السالف الذكر،والذي يترتب على عدم أدائها البطلان،ويترتب على الشاهد التزام بأداء الشهادة أي الإدلاء بما وقع تحت حواسه إلا إذا تعلق الأمر بالسر المهني،فلا يجوز له أن يطلب إعفاءه من أدائها حيث يتحرى قول الحقيقة وهذا بنص المادة(2/97) من قانون الإجراءات الجزائية. وقد نتج عن اختلاف الشهادة المعلوماتية عن شهادة الشهود في الجرائم الأخرى،ما يعرف بالالتزام الشاهد ألمعلوماتي الذي يختلف عن التزام الشاهد العادي.

[1] إحمود فالح الخرابشة، المرجع السابق، ص272

[2] إحمود فالح الخرابشة، المرجع السابق، ص278.

[3] محمد مروان ،نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الثاني.ديوان المطبوعات الجامعية ، الجزائر ،1999،ص308.

أ-ماهية الالتزام بالإعلام.

إن الإعلام في جرائم تكنولوجيات الإعلام والاتصال أو جرائم الانترنت: "جوهرها متى كان الشاهد ألمعلوماتي حائزا لمعلومات جوهرية لازمة لاختراق نظام المعالجة الآلية للبيانات بحثا عن أدلة للجريمة داخلة تتطلبها مصلحة التحقيق فإنه يكون مطالب بأن يعلم بها سلطات التحقيق والتحري على سبيل الإلزام"[1]،على أنه في حالة عدم تأدية هذا الالتزام سوف يعرض الشاهد إلى عقوبة جزائية متى ما نص القانون على ذلك، إذن هناك اختلاف بين الالتزام بأداء الشهادة في الجرائم العادية وجرائم تكنولوجيات الإعلام والاتصال ولكن إلى أي مدى يلتزم الشاهد ألمعلوماتي بالإعلام والذي يختلف عن البلاغ هو كل مايرد إلى علم ضابط الشرطة القضائية من أخبار عن الجريمة شفاهة أو كتابه أو بأي وسيله[2].حيث أن هناك اتجاهين فقهين في هذا الصدد.

1-الاتجاه الأول:يرى هذا الاتجاه أن إفشاء كلمات السر هي ليست من التزامات الشاهد ألمعلوماتي وبالتالي من واجبه الحفاظ عليها وعدم الإدلاء بها، لان شهادته تنصب على معرفة قائمة لديه بالفعل ،ولا تشمل تقديم معلومات جديدة[3]،بيد انه على الشاهد ألمعلوماتي أن يعاون في العمليات المنجزة لصالح التحقيق وذلك تحت طائلة قانون العقوبات وتحديدا جريمة عرقلة حسن سير التحريات القضائية وهذا ما جاء في نص المادة (11)من قانون(09-04).

فجوهر الشهادة المعلوماتية هو الالتزام بالإعلام، وذلك على أساس أن الإدلاء بمعلومات لازمة لاختراق نظام معلوماتي معين بحثا عن أدلة الجريمة داخله يخرج عن نطاق الوقائع محل الشهادة"[4].

[1] هلالي عبد الله أحمد ،التزام الشاهد بالاعلام في الجرائم المعلوماتية، المرجع السابق، ص25.

[2] محمد حزيط ،مذكرات في قانون الإجراءات الجزائية،الطبعة الرابعة،دار هومة ،2009،ص59.

[3] عبد الله حسين على محمود،المرج السابق،ص381.

[4] هلالي عبد الله أحمد، التزام الشاهد بالاعلام في الجرائم المعلوماتية، المرجع السابق، ص70.

2-الاتجاه الثاني:إن إفشاء كلمات السر والإفصاح عنها لسلطات التحقيق هو التزام قانوني طالما وجد نص قانوني، فليس ثمة أي مسؤولية قانونية تقع على الشاهد المعلوماتي بفئاته إذا رفض تقديم المعلومات المطلوبة إلا في حالة إذا وقع ذلك في مرحلتي التحقيق الابتدائي والمحاكمة[1].

وهي ضمن قانون الإجراءات الجزائية، أما إذا تعلق الأمر بالالتزام بإعلام من طرف الشاهد فهو يتخطى الشهادة بمعنى أنه لكون الشاهد المعلوماتي يختلف عن العادي فليس للمشرع أن يجبره على كشف كلمات السر، ولو أن المشرع الجزائري وبالطرح السالف الذكر قد جعل مزود خدمات[2] الانترنت من فئة الشهود الذين يقع على عاتقهم الالتزام بالإعلام، وذلك من خلال القانون (09-04) وبالضبط ضمن المادة (10)[3]، والذي قابل عدم الالتزام بعقوبات جزائية مترتبة عن جريمة عرقلة حسن سير التحريات القضائية، وبالتالي أصبح الالتزام بالإعلام بعد صدور القانون (09-04)مقننا، لذلك يجب أن "يراعي الشاهد المعلوماتي في إعلامه أن يكون مفهوما، بسيطا محددا، دقيقا، صادقا، وأمينا".[4]

فالشاهد عليه أن يدلي بما وقع على حواسه وليس مجبرا على التعاون مع سلطات التحقيق والتحري فيما خرج عن ذلك، لذلك كان التزام الشاهد المعلوماتي بالإعلام يتطلب الشرعية والمتمثلة في نص الإلزام وهو ما أورده المشرع الجزائري في قانون (09-04)والذي يدخل ضمن الأفعال المبررة.

---

[1] فهد عبد الله العازمي،المرجع السابق،ص455.

[2] أو مقدمو الخدمة حيث عرفه المشرع الجزائري في إطار القانون (09-04) المادة(02) فقرة د (مقدمو الخدمات :1- أي كيان عام أو خاص يقدم لمستعملي خدماته،القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات2-وأي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها).

[3] المادة (10)من القانون (09-04)في إطار تطبيق أحكام هذا القانون،يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة (11) أدناه،تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.)

[4] هلالي عبد الله أحمد، التزام الشاهد بالاعلام في الجرائم المعلوماتية ، المرجع السابق، ص59.

أمّا إذا تعلق الأمر بالتزام بأداء الشهادة ،فهو الأمر الذي ينطبق على الشاهد العادي والشاهد ألمعلوماتي بنفس القدر المنصوص، في قانون الإجراءات الجزائية وفق المادة (97) حيث على الشاهد الحضور الشخصي سواء الواقعي أو باستعمال وسائل المرئية عن بعد،حلف اليمين القانونية[1]،وأداء الشهادة مع مراعاة الأحكام القانونية للسر المهني.

وبعد الاطلاع على التزامات الشاهد العادية والمستقاة من نصوص قانون الإجراءات الجزائية والاجتهادات الفقهية، فإننا نرى أنه ورغم اختلاف الشهادة العادية عن المعلوماتية وبالتالي من يقوم عليها، ليس مبرر لطبع ملفات البيانات أو الإفصاح عن كلمات السر دون إذن، ففي الأصل ليست من التزامات الشاهد العادي "أن يتعاون مع سلطات البحث والتحري تعاونا فعالا"[2]،إلا ما تعلق منها بمرحلة التحقيق النهائي ومع السلطات المخولة .

ب– شروط الالتزام بالإعلام في جرائم الانترنت.

لالتزام الشاهد بالإعلام لابد من توافر شروط معينة،الإخلال بها يعرضه للمسائلة الجزائية

1–أن تكون بصدد جناية أو جنحة من جرائم تكنولوجيات الإعلام والاتصال واقعة بالفعل، وليست متوقع الحدوث ،لان الإعلام يأتي مباشرة بعد العلم بوقوع السلوك الإجرامي.

2–أن يكون الشاهد ألمعلوماتي على علم ودراية بالمعلومات، والتي تكون تحت سيطرته بالنظر إلى طبيعة نشاطه، والمتمثل في مزود خدمة الانترنت، وأعضاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،باعتبارهم يمارسون مهام وفق المادة (14) من القانون (09-04)والمادة 04 من المرسوم الرئاسي رقم (15–261)[3]،من شانها أن تجعلهم من فئات

[1] حلف اليمين القانونية لأداء الشهادة وفق المادة(93)يستثنى من ذلك القصر اقل من ستة عشر سنة والمحكوم عليهم بالحرمان من الحقوق الوطنية،وأصول المتهم وفروعه وزوجه وأخوته وأصهاره على درجته من عمود النسب وفق المادة (228) ق.ا.ج.ج.

[2] سامح أحمد البلتاجي موسى، المرجع السابق، ص296.

[3] مرسوم الرئاسي رقم (15–261) مؤرخ في 24ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج ر 53 ص 21.

الشاهد ألمعلوماتي السالفة الذكر،وهو ما جسدته المادة (11) من نفس المرسوم،والتي تنص على مهام مديرية المراقبة الوقائية واليقظة الالكترونية[1].

الواقع أن اعتبار أفراد الهيئة من أصناف الشاهد ألمعلوماتي لم يذكر صراحة، ولكن هو من أصناف الشهود باعتبار ان عملية المراقبة الالكترونية للاتصالات، وعملية التسرب إجراءات خاصة بالإنترنت، فالضابط القائم بعملية التسرب يجوز سماعه باعتباره شاهد عن العملية[2]، اي عملية التسرب وهو الحال بالنسبة لأعضاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال،والذين يستفيدون من حماية الدولة من التهديدات والضغوطات او الاهانات ،بمناسبة قيامهم بمهامهم[3].

3- أن تصب كل هذه الأمور في مصلحة التحقيق وملاحقة الجاني وتوقيع العقاب باعتبار أن هذا التكليف الذي حدده القانون سوف يأتي في سياق البحث عن الدليل الجنائي الرقمي،ومع التطور الحاصل في تكنولوجيات الإعلام والاتصال عمد المشرع الجزائري إلى تطويروعصرنة العدالة،وهذا ما جاء به القانون (15-03) المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015 يتعلق بعصرنة العدالة [4].

ثالثا:شهادة الشهود الالكترونية.

قد جاءت المادة(15)من القانون السالف الذكر اعلاه على انّه يمكن سماع الشهود عن طريق المحادثة المرئية عن بعد لسماع الشهود أثناء الحكم ،وهو ما يعبر عنه بالشهادة الالكترونية، وهي الشهادة التي وذلك لتعلقها بوسائل معينة في أدائها،أي الوسائل التقنية [5]مع العلم أنها شهادة

[1] المادة (11) من المرسوم (15-261)"...-تزويد السلطات القضائية ومصالح الشرطة القضائية،تلقائيا او بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال... "

[2] المادة (65مكرر 18)من ق.ا.ج.ج

[3] المادة 40 من المرسوم الرئاسي رقم(15-261) سالف الذكر

[4] الجريدة الرسمية رقم06 ليوم 10 فبراير 2015.

[5]هلالي عبد اله، التزام الشاهد بالاعلام في الجرائم المعلوماتية، المرجع السابق،ص33

صالحة في جميع الجرائم فهي متعلقة بطريق أداء الشهادة، ومن ذلك ولحسن سير العادلة فانه لابد من تطبيق شروط معينة للاخد بها كما أنها على صنفين

أ–شروط الشهادة الالكترونية(الوسيلة)[1].

تكون الشهادة عن طريق محادثة مرئية وليست سماعية أي شاهد يظهر صورة ويسمع إلى شهادته في نفس الوقت مع احترام القواعد المنصوص عليها في قانون الإجراءات الجزائية المتعلقة بالشاهد نفسه ،كالأهلية للشهادة.لأنه وفي حالة صغر السن أي اقل من ستة عشر سنة وإذا كان الشخص محكوم عليه بعقوبة سالبة للحرية ،لا يمكن الاستماع إلى الشاهد إلا على سبيل الاستئناس ودون حلف اليمين،على أن تضمن الوسيلة المستعملة سرية الإرسال وأمانته، فلابد على السلطات أن تضمن عدم اختراق شبكة الإرسال من طرف مجرمين أو متطفلين ،ذلك انه سوف يؤدي إلى عرقلة حسن سير المحاكمة[2]، هذا من ناحية من ناحية أخرى ،وفي نفس السياق فإنه لابد من تأمين الوسائل المستعملة التي تضمن السرية والأمانة أو ما يعرف بالأمن ألمعلوماتي ، مما يفرض على السلطات المختصة الجزائرية أن تتحرى استعمال كل ما هو أصلي في البرمجيات من أجل ضمان السرية و الموثوقية لهذا النوع من الإجراء.

وأخيرًا إفراغ الشهادة الالكترونية (هنا وسيلة الإدلاء بالشهادة وليس موضوع الشهادة) على دعامة ضمانا لسلامة الشهادة، وترفق الدعامة بملف الإجراءات على أنّه يجب أن تكون في عدة نسخ، بمعنى أكثر من دعامة معلوماتية[3].

[1] سن المشرع الجزائري قانون عصرنة العدالة ، من أهم أهدافه استخدام تقنية المحادثة المرئية عن بعد في الإجراءات القضائية، حسب نص المادة الأولى من قانون رقم(15-03) مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، يتعلق بعصرنة العدالة،ج.ر. رقم 6 ليوم 10 فبراير سنة2015 م.ص.4.

[2] كأن يخترق رابط البث المرئي فيمكن لمتهم هارب أن يغير وقائع وملابسات معينة تخدم مصلحته،نتيجة اختراقه البث المرئي،وبالتالي عرقلة السير الحسن للعدالة،مع العلم أن اختراق البث هو من جرائم الانترنت أو تكنولوجيات الإعلام والاتصال التي لم ينص عليها المشرع الجزائري، لذلك لابد من إعادة النظر في تقسيم جرائم تكنولوجيات الإعلام والاتصال

[3] المادة(14فقرة2) من القانون من قانون رقم(15-03) ، يتعلق بعصرنة العدالة،ص5.

ثم تحرير محضر تدون فيه التصريحات كاملة وحرفيا للشاهد عن بعد كما لو أن الشاهد حضر الجلسة واقعيا وليس افتراضيا، فيوقع قاض الحكم وأمين ضبط الجلسة على المحضر[1].

تتم الشهادة عن بعد بالمحادثة المرئية بمقر المحكمة الأقرب من مكان إقامة الشاهد، حيث أنّه لابد من التأكد من هويته وشروط أدائه الشهادة[2].

ب–أقسام شهادة الشهود الالكترونية:

الواقع أنها تنقسم لقسمين الشهادة المرئية ذات الاتجاه الواحدو الشهادة المرئية ذات الاتجاهين،وهي شهادة لتسهيل الإجراءات القضائية دون أن تكون مخصصة للشاهد العادي أو الشاهد المعلوماتي ويدخل هذا في إطار مواكبة التطورات التقنية والتسريع من وتيرة الإجراءات القضائية.

1–الشهادة المرئية ذات الاتجاه الواحد[3].

حيث أن الشاهد يدلي بشهادة حية ،فمن مصطلحها هي شهادة مرئية أي أن المحكمة وهيئة المحلفين هم الوحيدين الذين يستطيعون رؤية الشاهد دون أن يراهم هو، هذا النوع من الشهادة رغم وجوده إلا انه ينقص من القيمة القانونية للشهادة والتي تعتمد على أسلوب المواجهة .

2–الشهادة المرئية ذات الاتجاهين.

وفيها يرى الشاهد قاعة المحكمة ويراه من بالمحكمة من قاض ومحلفين وأفراد...وتقدير اختيار أي من الشهادتين بالأسلوب الالكتروني يخضع لتقدير المحكمة [4]،وتعتمد الشهادة الرقمية في جرائم العادية كما في جرائم الانترنت ،خصوصا أن هذه الجرائم عابرة للحدود ،لذلك فان إتاحة هذا

[1] المادة (14 فقرة3)من القانون من قانون رقم(15–03) يتعلق بعصرنة العدالة ،ص5

[2] المادة (16)من القانون من قانون رقم(05–03) يتعلق بعصرنة العدالة،ص6.

[3] عمر محمد بن يونس أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب،دار النهضة العربية،2004.،ص957.

[4] المرجع نفسه،ص958.

النوع من الشهادة ووجود التعاون الدولي قد يحقق ما تصبو إليه الدول لمكافحة هذا النوع من الجرائم،وهو ماجسده المشرع الجزائري في إطار قانون عصرنة العدالة[1]،وهذا في المادة(15)منه التي جاء فيها مايلي:"يمكن قاضي التحقيق أن يستعمل المحادثة المرئية عن بعد في استجواب أو سماع شخص وفي إجراء مواجهات بين عدة أشخاص.يمكن أيضا أن تستعمل المحادثات المرئية عن بعد لسماع الشهود ..."

شهادة الشهود في جرائم الانترنت، موضوع أخد نصيبه في اعتماد التقنيات الحديثة للإدلاء بها، دون التفصيل في الفئات المعنية بالإعلام في جرائم تكنولوجيات الإعلام والاتصال أو بالأحرى الالتزام بالإعلام،طبعا بعيدا عن الشاهد العادي أو ألمعلوماتي الذي يلعب دورا مهما في عملية الإثبات الجنائي في مثل هذه الجرائم،التي تعد خطيرو خصوصا ما تعلق منها بالاعتداء على المنظومة المعلوماتية التي تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، ومن اجل صون حرية الشاهد مما يؤثر على إرادته للإدلاء والإعلام، فان هناك من طرق الإثبات التي قد تلعب دور مميز في إثبات جرائم الانترنت وهي القرائن في الفرع الموالي.

الفرع الثاني: القرائن في جرائم الانترنت.

تعتبر القرائن من الأدلة غير المباشرة التي تخضع للسلطة التقديرية للقاضي،وهي في الكثير من الأحيان تلعب دورا مكملا لاقتناع القاضي حيث كثيرا ما يستعين بها في العملية الإثباتية.

القرينة عموما هي استنباط الشارع أو القاضي لأمر مجهول من الأمر المعلوم و هو دليل غير مباشر لأنها لا تؤدي إلى ما يراد أثباته مباشرة بل تؤدي إليه بواسطة الأمر المعلوم 2،والقرينة هي دليل إثبات غير مباشر ،ويفترض الإثبات بالقرائن تغيير محل الإثبات فبدلا من أن يرد الإثبات على الواقعة ذات الأهمية في الدعوى الجزائية أي واقعة ارتكاب الجريمة ونسبتها إلى المتهم ،يرد

[1] قانون رقم (15-03) سالف الذكر .

[2] عبد الحميد الشواربي،الإثبات الجنائي في ضوء القضاء والفقه،منشاة المعارف ،مصر ،1996.ص335.

الإثبات على واقعة أخرى مختلفة ولكن بين الواقعتين صلة سببية منطقية يمكن لقواعد الاستنباط المنطقي أن تستخلص وقوع الجريمة ونسبتها إلى المتهم[1]،وتجد القرائن لها نصيبا في إثبات جرائم الإنترنت، ولكن تثير هي الأخرى مشاكل معينة تجعلها أقل أهمية ،وذلك نتيجة غموضها وإمكانية مساس بحريات الأشخاص عن طريق استنباطات ملفقة من مجرمي الانترنت.

تلعب القرائن دورا في إثبات جرائم الانترنت ولكنها تظل قاصرة عن القيام بدور هام في عملية إثبات هذه الجرائم رغم أهميتها.

أولا :أهمية القرائن في جرائم الانترنت.

يمكن القول إجمالا أن الدليل الجنائي الالكتروني، اقرب إلى القرائن منه إلى أنواع الأدلة الأخرى[2]،ويمكن اعتماد القرائن في إثبات جرائم الانترنت باعتبار أنها جرائم صعبة الإثبات، وهناك بعض الوقائع يستحيل إقامة الدليل المباشر عليها حيث إذا اقتصر الأمر على نظام الإثبات المباشر لا يمكن الفصل في الدعوى الجزائية ،مما استدعى ويستدعي اعتماد الدليل غير المباشر عن طريق القرائن للتوصل إلى إقامة الدليل على الوقائع[3]،فإذا كانت القرائن تحتل مركزا في ميدان الإثبات الجزائي فان القناعة التي تعتمد عليها يجب أن ترتكز على أسس مبدئية منها الصلة بين الواقعة الثابتة والواقعة المراد إثباتها ،وان تكون الصلة قوية وقاطعة لا تترك مجالا للشك وذلك على اعتبار أن الشك يفسر لمصلحة المتهم ،ومن هذه المنطلقات ،ينهض الارتباط الوثيق بين قوة القرينة والثبوت اليقيني للواقعة[4]،وقد زاد من أهمية الإثبات بالقرائن مع ظهور جرائم الانترنت يعلو شأن الإثبات بالقرائن كنتيجة لاتساع مجال الإثبات بها نتيجة تطور العلوم[5].

[1] محمد احمد محمود، الوجيز في أدلة الإثبات، دار الفكر الجامعي،مصر،ص20.

[2] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص936.

[3] الياس ابوعيد ،نظرية الإثبات في أصول المحاكمات المدنية والجزائية،الجزء الثالث،منشورات زين الحقوقية،لبنان،2005،ص394.

[4] الياس ابوعيد،المرجع السابق،ص399و400.

[5] على محمود على حمودة، البحث السابق، منشور على موقع السابق،ص68.

ثانيا:أثر القرائن في جرائم الانترنت.

يمكن تقسيم القرائن في مجال جرائم الانترنت إلى قرائن قاطعة وأخرى بسيطة وهذا ما يساعد كثيرا في إثبات جرائم الانترنت ،إذ تظل المفارقة في إطار الدليل الجنائي الالكتروني، كونه لا يزال في حاجة إلى دليل مادي لكي يمكننا التوصل بمقتضاه إلى الإدانة ، ومن ثم يمكن في هذا المنحى مساواته من حيث هيكلته كدليل بالقرائن دون غيرها1،ولكن في نفس السياق فان خطورة جرائم الانترنت؛ وذكاء مرتكبي هذا النوع من الجرائم واتصافهم بأنهم النخبة المميزة في مجال المعلوماتية والاتصالات قد يحدث ضرر كبير بأبرياء ليس لهم أي علاقة حتى باستخدام الانترنت. فقط لان هذا المجرم وبسوء نية منه استخدم البيانات الشخصية لفرد يعرف عنه أدق تفاصيل حياته أو أخر لا يمت له بأي صلة،بل بمحض الصدفة عثر على بياناته،فيمكن لهذا المجرم أن يترك الآثار والعلامات التي تدين الأبرياء لكي ينجو بفعلته، وإزاء نقطة الشك التي تدور حول القرائن، فإنه من الضروري الاعتراف بأن القرائن كدليل كامل في العالم الرقمي إنما يجعل حقوق الإنسان عرضة للانتهاك ،حيث أنها تؤدي بالضرورة إلى قيام الإدانة أو حتى البراءة على أساس الافتراض[2].

المطلب الثاني:دعائم الإثبات المادية.(المعاينة والخبرة).

تعتبر المعاينة من دعائم الإثبات المادية في جرائم الانترنت، ولذلك فان المحكمة تلجا إليها أحيانا من تلقاء نفسها ،فتساهم في تكوين عقيدة المحكمة إذ تمنحها أفكار وانطباعات مادية ناجمة عن الاطلاع أو الفحص المباشر لمحل المعاينة دون وساطة شهود أو خبراء،كما أنها تجسد لديها ما حوته الدعوى من عناصر إثبات،فتُوقن بصحتها أو بفسادها[3]، فالمعاينة في جوهرها ملاحظة وفحص حي مباشرة لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة[4]،ومن اجل أن تؤدي المعاينة دورها

[1] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص937.

[2] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق ،ص937.

[3] أحمد شوقي الشلقاني ،مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني ،ديوان المطبوعات الجامعية ،2003،ص459.

[4] جميل عبد الباقي الصغير، ،الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص26.

في الإثبات،فانه يستحسن أن يستعان بخبير فني متخصص في شبكة الانترنت، بصحبة المحضر ،وذلك حتى نمنع أي تشكيك في صحة الدليل المستمد منه[1]،فيدخل الخبير إلى شبكة الانترنت حيث يوجد الموقع الذي توجد عليه المعلومات المجرمة من خلال الحاسب الخاص بجهة عمله،وذلك حتى لا يعطي الفرصة للمتهم في المنازعة في قيمة الدليل المستمد من المعاينة التي أجراها[2]، لذلك ترتبط المعاينة(الفرع الأول) بالخبرة(الفرع الثاني) الفنية في مجال جرائم الانترنت.

الفرع الأول:المعاينة

إن المعاينة إجراء يهدف إلى أمرين، الأول جمع الأدلة التي تخلفت عن الجريمة كرفع البصمات، وكل ما يفيد في كشف الحقيقة سواء لأنّه استخدم في إحداث الجريمة أو تخلف عنها، والثاني إعطاء المحقق فرصة ليشاهد بنفسه على الطبيعة مسرح الجريمة[3] حيث يتمكن من تمحيص الأقوال التي أبديت حول كيفية وقوع الجريمة وتقدير المسافات ومدى الرؤية وغيرها [4]، لذلك وجود نظام أو برمجية تسجيل الدخول إلى شبكة الانترنت وبالتالي تحديد الأشخاص أو حتى ضبط المجرم المعلوماتي في حالة تلبس، او عن طريق المراقبة الوقائية من طرف احد أفراد الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال،يعتبر قرينة قاطعة على وجود القصد الجنائي وسوء نيته في ارتكاب جريمة من جرائم الانترنت[5] .

أولا:تعريف المعاينة.

يعتبر المكان الذي ارتكبت فيه الجريمة الوعاء الأساسي الذي يحتوى على اخطر الأدلة الجنائية التي يخلفها الجاني ورائه في أعقاب اقترافه الجريمة، فالمعاينة هي مشاهدة وإثبات الحالة القائمة في مكان الجريمة و الأشياء التي يتعلق بها وتنفيذ في كشف الحقيقة واثبات حالة الأشخاص

[1] Sedallian Valerie,Droit de l`Internet. réglementation responsabilités, op.cit.p254.

[2] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص29.

[3] مصطفى مجدي هرجة،المرجع السابق،ص83.

[4] مصطفى محمد الدغيدي، المرجع السابق، ص141-142.

[5]فهد عبد الله العازمي،المرجع السابق،ص268.

الذي لهم صلة بها [1]،والملاحظ انه ليس كل انتقال للسلطات المختصة هو بغرض المعاينة فقد يكون انتقال قاض التحقيق لأجل التفتيش أو إجراء التحقيق في مكان الواقعة أو حتى سماع الشهود،وفي الجرائم المتلبس بها ،أو أي جريمة تقبل المعاينة بطبيعتها[2]،هو ليس الأمر بالنسبة لجرائم الفساد مثلا أو جرائم التزوير أو السب والشتم وهي الجرائم التي لا يتصور فيها ان تكون للمعاينة فيها الأهمية الكبيرة إذا تمت عبر الانترنت.هي ليست إجراء تلقائي في مباشرتها ،بل إجراء هادف، لكشف كل عناصر الجريمة.

فالمعاينة هي إجراء قد يقوم به قاض التحقيق وذلك بالانتقال إلى مكان وقوع الجريمة وهذا ما نصت عليه المادة(79)من قانون الإجراءات الجزائية الجزائري ،أما فيما يخص مرحلة المحاكمة فيجوز للجهة القضائية إما من تلقاء نفسها أو بناء على طلب احد أطراف الدعوى أن تأمر بالمعاينة وهذا وفق المادة(235) من قانون الإجراءات الجزائري .

إنّ استعانة سلطات جمع الاستدلالات والتحقيق والحكم بالخبراء هو أمر ضروري حين نتعامل مع الجرائم المتعلقة بالانترنت نظرا للطابع الفني لأساليب ارتكابها والطبيعة غير المادية لمحل الاعتداء[3]وهي خصائص سبق أن فصلنا فيها قبلا.

أ– المعاينة الفنية.

هو إجراء يتخذ بواسطة الفنيين في محل الحادث سواء عن طريق رسمه ورفع الآثار المادية منه ،كآثار البصمات وأثار الدم ويتم وفق الخطوات التالية،وهنا المعاينة الفنية هي المكمل للمعاينة الافتراضية،ذلك أن الكثير من مجرمي الانترنت –المجرم ألمعلوماتي– يتركون بصماتهم على مكونات النظام ألمعلوماتي،كالتوصيلات التي قد يقوم بها المخترقون من جهاز إلى أخر أو بعض أجهزة

[1] مصطفى مجدي هرجه، المرجع السابق، ص83.

[2] سامح احمد البلتاجي موسى، المرجع السابق،ص233.

[3] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص28.

المراقبة الالكترونية الحساسة،والواقع ان المعاينة الفنية تكون فعالة في الكشف عن الأدلة فيما يتعلق بالكيان المادي للمنظومة المعلوماتية،وتكمل بنتائجها ما سوف تسفر عنه المعاينة الافتراضية.

1-وصف الجريمة بالكتابة.

يعتمد فيها الفنيون على وصف أدق التفاصيل ،فكلها مهم مهما كانت صغيرة ،كأن يقوم المعاين بوصف الجثة وصفا تفصيليا يبرز،موضعها وحالتها والملابس الموجودة عليها وحالة الجروح بها ونوع الآثار الموجودة فيها ومدى بعدها أو قربها من الأثاث[1]،وغيرها من التفاصيل التي تعطي وصفا حقيقيا ،رغم أنّ هذه المعاينة لاتنجح في المسرح الافتراضي لانعدام وجود اثر مادي،فمثلا القتل عبر استخدام الانترنت يختلف مثلا يمكن أن يقوم المجرم بذلك عن طريق تغير التقرير الطبي أو وصفة الدواء أو التحاليل ،فيكون هذا التغيير السبب المباشر في إزهاق روح الضحية.

2-تصوير مكان الحوادث.

تظهر فائدة التصوير في الحالات الآتية،إظهار الحادث بالحالة التي تركها عليه المجرم دون زيادة أو نقصان من مساحة الفعل مهما مر عليه من زمن،سهولة إعادة تكوين محل الجريمة وهذا لتمثيل طريقة ارتكاب الجريمة على النحو الذي قام به المجرم إذا استلزم التحقيق ذلك،الصورة الفوتوغرافية تظهر جميع مشتملات مسرح الجريمة ولا تغفل منه شيئا خصوصا مع تطور تقنية التصوير الرقمي[2].

3-رفع الآثار المادية.

هي مجموع من الآثار المادية المتخلفة عن الجريمة كالزجاج أو الشعر أو بصمات الأصابع ،وهي أثار تختلف من نوع إلى أخر من الجرائم،فمثلا يمكن رفع أثار بصمات الأصابع عن جهاز

[1] عبد الحميد الشواربي،المرجع السابق،ص225.

[2] عبد الحميد الشواربي، المرجع السابق،ص226 و228.

الكمبيوتر الشخصي للمتهم ،في حالة قيامه بعملية الاختراق من عليه،ضنا منه انه قد اتخذ كل تدابير الحماية اللازمة لعدم كشفه.

إذن للمعاينة الفنية أهمية إذا تعلق الأمر بالمسرح المادي للجريمة ،او كلما كانت الوقائع اكثر اتصالا بالمسرح المادي لجريمة الانترنت،ولكن هذا يبدو قاصرا إذا لم يكتمل إطار المعاينة في المسرح الافتراضي أو اللامادي .

ب- المعاينة في جرائم الانترنت.

في إطار دراسة مدى اعتبار المعاينة من الدعائم الإثبات المادية في إثبات جرائم الانترنت،لابد أن نعرف المعاينة عبر الانترنت أهميتها وشروطهافالمعاينة في جرائم الانترنت هي معاينة الاثار التي يتركها مجرم الانترنت والتي عادة ما تتمثل في المراسلات الالكترونية البريد الالكترونية ،والمحادثات الهاتفية والفيديوهات وحتى البرامج المستخدمة على المسرح الافتراضي اللامادي.

1-أهمية المعاينة في جرائم الانترنت.

تلعب المعاينة دورا مهما في الجرائم العادية عكس جرائم الانترنت، وتعود عدم فاعلية المعاينة في مجال الجرائم المتعلقة بالانترنت هو إمكانية الجاني التلاعب بالبيانات عن بعد لان ارتكاب الجريمة عادة يكون عن طريق اختراق الاتصالات الالكترونية [1]،كما ذكرنا فيما سبق أن الأدلة والآثار التي تخلفها جرائم الانترنت أثار رقمية اي غير ملموسة، بالإضافة إلى أن مسرح الجريمة الافتراضية مسرح يتردد عليه العديد من الأشخاص وغالبا ما تكون هناك فترة زمنية معتبرة بين اقتراف الجريمة والكشف عنها إما مصادفة أو عن طريق البلاغ ،وهذا ما يؤدي في الكثير من الأحيان إلى إتلاف الأدلة وبالتالي عدم إمكانية معاينتها [2]،ولكن إذا تمت المعاينة فهي تشكل عاملا هاما لكشف أثار الجريمة وكيفية وقوعها ،فمعاينة مسرح الجريمة يسفر عن اكتشاف الجريمة

[1] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص29.

[2] منى فتحي احمد عبد الكريم،المرجع السابق،ص179،و عبد الله حسين على محمود، المرجع السابق،ص357.

،فمثلا وجود بعض البرامج المزروعة كالفيروسات تشير في حد ذاتها إلى أن الدوافع من وراء هذه الجريمة هو الانتقام أو العدوانية[1].

2-أشكال المعاينة في العالم الافتراضي.

تختلف أشكال المعاينة من جريمة إلى أخرى في جرائم الانترنت ،حيث ما ينطبق على جريمة لا يمكن تطبيقه على أخرى ،على أن هناك طرق عامة تتوافق مع طبيعة الاتصال بالانترنت أو الوسيلة التي يتم بها ذلك الاتصال مثلا هناك وسيلة تصوير شاشة الحاسوب[2] ،لتظهر المعلومات أو الصور المطلوب معاينتها ،كما أن هناك برمجيات متخصصة في أخد صور،بالإضافة أن نظام التشغيل يوفر خاصية الحفظ باسم التي يمكن استخدامها من اجل حفظ الأدلة أثناء المعاينة،وكما ذكرنا فان لكل جريمة خصوصية معينة فلو أخدنا على سبيل المثال الجرائم الاستغلال الجنسي للأطفال يمكن التحفظ على الصور والفيديو الموجودة على جهاز المتهم ،سواء كان هذا الجهاز حاسوب أو هاتف نقال أو لوح رقمي عن طريق حفظها ولكن من الأصل، وهذا شرط أساسي ونقصد من الأصل أي المصدر والذي عادة يكون من خلال معاينة مزودي خدمات الانترنت، وخصوصا مقدم خدمة الإيواء لا التوصيل،كذلك البريد الالكتروني الذي يحتوي على عبارات القذف لابد من التحفظ عليه والى ذلك من جرائم كل حسب سلوكها الاجرامي.

ثانيا:إجراءات المعاينة.

إن المعاينة في جرائم الانترنت تجمع بين المعاينة العادية والرقمية أي التي تتم داخل مسرح الجريمة الافتراضي،لذلك يتم معاينة المسرحين على حد سواء العادي والالكتروني،ثم بعد ذلك هناك كيفيات للمعاينة لابد من إتباعها.

[1] سليمان مهجع العنزي،المرجع السابق،ص110.

[2] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص29.

أ-معاينة مسرح الجريمة.

الجمع في المعاينة بين المسرح التقليدي والمسرح الافتراضي له أهمية كبيرة للتوصل إلى أدلة الإدانة،ففي الكثير من الأحيان يترك المجرم التقني أثارا مادية في المسرح التقليدي أو العادي أو المادي تكون مكملة لما سوف يتوصل إليه من معاينة المسرح الافتراضي.

1-المسرح التقليدي.

يقصد به مسرح الجريمة الذي يقع خارج المنظومة المعلوماتية أو شبكة الانترنت ،والتي يكون الجاني وصلها عند ارتكاب جريمة بهدف الحصول على أدلة مادية ،حيث يتوجب على المحقق بالمكان الذي حدثت فيه الجريمة شاملا كل ما يمكن أن تصل إليه الأدلة والتي توجد به كالآثار المادية المتخلفة من المجرم بمقهى الانترنت مثلا او الحاسب الشخصي أو الهاتف واللوح الرقمي وأثار استخدامه الأجهزة[1].

2-المسرح الرقمي.

يقصد به مسرح الجريمة الذي يقع داخل المنظومة المعلوماتية والتي يكون المجرم المعلوماتي وصلها عند ارتكاب جريمة سواء باستخدام الجهاز بالوصول مباشرة أو الوصول غير المباشر عن طريق شبكة بهدف الحصول على دليل الكتروني[2]، فالمحقق في المسرح التقليدي يبحث عن بصمات المجرم وما تبقى من أثاره ،وعندما يترك المجرم التقني بصمات رقمية قد تستطيع السلطات المختصة في الضبط وحجز المعطيات الحصول على معلومات عن هذا المجرم وذلك عن طريق المواقع التي تفتح سجلات تتضمن بعض المعلومات عن المجرم باستخدام بعض البرمجيات يمكن معرفة البريد الالكتروني ،وعلى الرغم من أن هذا العمل غير قانوني إلا إذا كان بتصريح خاص من

[1] سليمان مهجع العنزي،المرجع السابق،ص124.

[2] سليمان مهجع العنزي ،لمرجع السابق،ص124.

النيابة أو القاضي المختص أو كان للبحث عن أدلة في نطاق عمل الضبطية القضائية ،وأسهل طريقة لمعرفة ما تسجله المواقع التي يزورها مستخدم الانترنت،عادة التوجه إلى موقع www.consumer.net/analyze. والانتظار قليلا قبل أن يكشف هذا الموقع المعلومات، ويعرضها أمام رجل الضبط القضائي على الشاشة[1].

ب- كيفية المعاينة[2].

تتم المعاينة عن طريق الانتقال إلى العالم الافتراضي وهذا إما عن طريق الوسائل المتاحة للولوج إلى الانترنت،كالمنظومة المعلوماتية والهاتف النقال في أي مكان[3]،وأيضا يجوز له اللجوء إلى مقر مزود الانترنت الذي يعتبر أفضل مكان يمكن من خلاله إجراء معاينة[4]،ولما كانت معاينة المسرح الافتراضي تختلف عن المعاينة في المسرح التقليدي، لابد من مراعاة شروط معينة من اجل الوصول إلى الأدلة وهي:

-تصوير المنظومة المعلوماتية والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة،العناية بملاحظة الطريقة التي تم بها إعداد النظام،او تجميد مخرجات الشاشة.

-ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة.

-عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

[1] عبد المطلب عبد الحميد ممدوح، المرجع السابق، ص69.

[2] عمر ابو بكر يونس،الجرائم الناشئة عن استخدام الانترنت،المرجع السابق،859.

[3] نعتقد أن الولوج إلى العالم الافتراضي للقيام بعملية المعاينة يكون أكثر مهنية عن طريق الحاسوب المتصل بالانترنت لدى المحقق أو المحكمة.

[4] عمر محمد بن يونس أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص859.

-التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة وفحصها، ويرفع من عليها البصمات ذات الصلة بالجريمة،التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات،قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات[1]،كما أن هناك إجراء يضاف إلى كل هذا وهو عملية الحجز ،وهو حجز الأقراص الصلبة الخاصة بالخصم[2]،أوعن طريق الإرشاد أو الأسلوب الإرشادي لجرائم العالم الافتراضي، والذي يحدد هوية المتسلل انطلاقا من النقطة الأولى وهي اقتفاء الأثر[3]

على أن المعاينة في جرائم الانترنت تعترضها العديد من الصعوبات، ذلك انّ جرائم الانترنت لا تترك أثار مادية كباقي الجرائم ولكن أثار غير ملموسة ، أو ما يطلق عليها بالآثار المعلوماتية ،هذه الآثار تتواجد بمسرح افتراضي يتعاقب عليه العديد من المستخدمين ، فيصعب تحديد هوية صاحب الآثار الجنائية المعلوماتية،كما انه يمكن العبث وتغيير وحذف هذه الآثار، قلة كفاءة المحققين في استخدام الشبكة مما يعطي للمجرم الفرصة في تعديل الآثار المعلوماتية وبالتالي الدليل الجنائي الالكتروني[4].

[1] محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية. المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنظم من طرف أكاديمية شرطة دبي – مركز البحوث والدراسات –من 26 /4/ 2003الى28 /2003/4 دبي – الإمارات العربية المتحدة ،ص07.

[2] Sedallian Valerie, droit de l`internet, op.cit.p 254.

[3] ايمن عبد الحفيظ ،حدود مشروعية دور اجهزة الشرطة في مواجهة الجرائم المعلوماتية ،مجلة بحوث الشرطة العدد25 ،يناير 2004، القاهرة ،مصر،ص 367،منى فتحي احمد عبد الكريم،المرجع السابق،ص178،

[4] سليمان احمد محمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت،دكتوراه،في العلوم الشرطية ،اكاديمية الشرطة،القاهرة مصر 2007،ص289.

الفرع الثاني:الخبرة التقنية.

"قد يكون من بين العناصر التي يستعين بها القاضي لتكوين عقيدته في الدعوى الجنائية مسائل فنية لا يتسع علمه لتعرفها ولاوقته لفحصها كتحليل الدماء او تحقيق خطوط او اجراء محاسبة"[1].

إن الخبرة التقنية هي أهم طرق الإثبات في جرائم الانترنت، والدليل أن المشرع أولى لها أهمية بالغة وأسندها كاختصاص أصيل للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب نص المادة(12) من المرسوم الرئاسي رقم (15-261)"تكلف مديرية التنسيق التقني على الخصوص، بما يلي:-انجاز الخبرات القضائية في مجال اختصاص الهيئة...." وتعتبر من أهم دعائم الإثبات في جرائم الانترنت ،رغم ماتطرحه من أشكال ليس في قيمتها كطريق للإثبات وإنما لمكانتها في الإثبات الجنائي، التي قد تجعل دور القاضي سلبيا في مثل هذه الجرائم.

أولا:تعريف الخبرة.

الخبرة هي" الاستشارة الفنية التي يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى فنية أو دراية علمية لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته"[2]، وقد يحتاج الأمر إلى عمليات فنية دقيقة لإمكان الدخول إلى أنظمة الوسائل الإلكترونية نتيجة استخدام الشيفرات والأكواد السرية، وإذا كان الهدف من الخبرة الوصول إلى الحقيقة في مسائل علمية وفنية ومادية فإنها لا تكون حكرا على سلطة التحقيق

[1] حسن صادق المرصفاوي،أصول الإجراءات الجنائية ،منشاة المعارف الإسكندرية،مصر،1996.ص120

[2] عبد الحميد الشواربي،المرجع السابق،ص206.

وإنما يحق للمحكمة أن تأمر بها[1]،ولكن ومن جهة أخرى رأي الخبير يعطى دائما بصفة استشارية؛ ولا تتقيد به المحكمة.

فهو ليس حكم قضائي، وليس له قيمة أكثر من شهادة الشهود، ولا يمنع القاضي من حقه التام في تقدير الوقائع التي تعرض عليه حق قدرها ،والمحكمة ليست مقيدة برأي الخبير في معرفة التلازم بين الفعل والنتيجة وفي نوع الأدلة المستخدمة حتى ولو تعلق الأمر بهذا النوع الخطير من جرائم الانترنت ،فللمحكمة أن تختار ما ترى الأخذ به كما أن لها تفضيل تقرير على تقرير أخر ولها أن تبحث في مسالة وتفصل فيها بدون اخذ رأي الخبراء،"فلا شك أن الأخذ بأي دليل فني ماهو إلا انعكاس لثقة أجهزة التحقيق والقضاء في أعمال الخبرة"[2].

ثانيا–أنواع الخبرة[3].

تقسم الخبرة القضائية إلى عدة أصناف بحسب الجهة التي قامت بها، على أنّ الاختصاص الأصيل يعود إلى الهيئة الوطنية لمكافحة جرائم تكنولوجيات الإعلام و الاتصال كما سيأتي.

أ–الخبرة الخاصة.

وهذا النوع من الخبرة تلجا فيها الجهات القضائية إلى المكاتب الخاصة،حيث أن هؤلاء الخبراء خارج سلطات هذه الجهات المختصة هم اقدر على إعطاء خبرة مناسبة لهذا النوع من الجرائم ،وهي عبارة عن جمعيات تعمل على رصد حركة الجريمة عبر الانترنت ومعرفة تطوراتها في كافة مظاهرها وإشكالها[4]،وبالتالي فهذا النوع من الخبرة عندما تستفيد منه الجهات القضائية لما يملكه

[1] على محمود على حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي،- المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنظم من طرف أكاديمية شرطة دبي – مركز البحوث والدراسات -من 26 /4/ 2003الى28 /2003/4 دبي – الإمارات العربية المتحدة،ص52.

[2] برهامي ابو بكر عزمي،الشرعية الإجرائية للأدلة العلمية"دراسة تحليلية لأعمال الخبرة"،دار النهضة العربية،القاهرة مصر،2006،ص.2

[3] عمر أبو بكر بن يونس،الجرائم الناشئة عن استخدام الانترنت،المرجع السابق،ص1034.

[4] المرجع نفسه،ص1036.

هؤلاء من خبرة عالية وهذا ناتج ليس عن الدراسة فقط بل عن الإبحار اليومي داخل الشبكة الذي اكسبهم خبرات عالية،وهو مالا يجد له مكان في إطار جرائم الانترنت في التشريع الجزائري،بعد أن أصبحت الخبرة في مجال جرائم الانترنت اختصاص أصيل لأعضاء الهيئة الوطنية للوقاية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ب–المؤسسات التعليمية.

إن الانترنت هي نتاج التطور العلمي الذي عملت عليه مختلف المؤسسات التعليمية سواء كانت عسكرية أو مدنية، تعتمد على منهج تعليمي وليس تجاري ،لأنها تعتمد على تدعيم الدول لها ماديا،والواقع أن الدولة الجزائرية قد أنفقت الكثير على الجامعات والمؤسسات التعليمية ،ولكن من ناحية عملية فالبحوث الجادة تبقى حبيسة الأدراج فلا يستفاد في الكثير من الأحيان من هؤلاء الباحثين في مجال تكنولوجيات الإعلام والاتصال ،في ظل غياب مشروع وطني واضح المعالم،فليس هناك أحسن من صاحب اختصاص يفك سر جريمة عبر الانترنت .

ج–الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

شهدت الجزائر تطورا ملحوظا في مجال مكافحة جرائم الانترنت او جرائم تكنولوجيات الإعلام والاتصال ،وتعد الهيئة الوطنية صاحبة الاختصاص الأصيل في كل الإجراءات الخاصة بمثل هذه الجرائم؛ وكذا ما تعلق بالإجراءات الخاصة بالجرائم الخاصة بالمادة(65 مكرر) من ق.ا.ج.ج.

نصت المادة04 من المرسوم الرئاسي رقم (15-216)فقرة 5 "....مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال المعلومات والتزويد بها ومن خلال الخبرات القضائية..."،وهذا بغرض مكافحة التصعيد الخطير في جرائم الانترنت،وتبرز أهمية هذه الهيئة في تنوع مديرياتها والتي لها اختصاص

وطني ودولي ،يمكنها من الإلمام بجميع أركان الجريمة وبالتالي تحقيق الفائدة المرجوة من إنشائها وهي مكافحة جرائم تكنولوجيات الإعلام والاتصال.

على ذلك ووفقا للمادة (12) من المرسوم المذكور اعلاه "تكلف مديرية التنسيق التقني على الخصوص،بما يأتي:-إنجاز الخبرات القضائية في مجال اختصاص الهيئة...."، كما يلعب المعهد الوطني للأدلة الجنائية وعلم الإجرام دورا مهما فيما يخص الخبرة التقنية، من الناحية العملية.

ثالثا:الخبير التقني.

إن الخبير التقني يختلف عن الخبراء الاقتصاديين والماليين،كما أن لأهل الخبرة شروط معينة لابد من توافرها. وبناءا عليه فاذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة أمر واجب على جهة التحقيق والقاضي،فهي اوجب في مجال الجرائم الالكترونية،حيث تتعلق بمسائل فنية بالغةالتعقيد وحل الجريمة فيها غير مادي، والتطور في أساليب ارتكابها سريع ومتلاحق،ولا يكشف غموضها الّا متخصص وعلى درجة من التميز في مجال تخصصه[1].

ا-تعريف الخبير التقني.

الخبير هو كل شخص له دراية خاصة بمسألة من المسائل، فيلجأ إلى الخبرة كلما قامت في الدعوى مسألة تتطلب حلها معلومات خاصة لا يتمكن القاضي من نفسه الدراية العلمية و الفنية لها[2]،فللمحاكم الاستعانة بأهل الخبرة وهي كثيرا ما تلجأ إلى هذه الطريقة التي يبررها أنها طريقة ضرورية يتحتم اتخاذها كلما ظهر أنه يمكن الوصول بواسطتها إلى اكتشاف الحقيقة،للمحكمة تعيين الخبراء من تلقاء نفسها أو بناء على طلب الخصوم[3]،وهذا في المسائل الفنية العلمية التي تواجه القضاء،ومتى قدم الطلب من احد الخصوم فلا يسوغ للمحكمة أن ترفضه إلا إذا رأت أن الوجه المطلوب تحقيقه غير متعلق بالموضوع ولا جائز القبول أو أن الواقعة

[1] فهد عبد الله العازمي،المرجع السابق،ص645

[2] مصطفى مجدي هرجه، الإثبات في المواد الجنائية، دار المطبوعات الجامعية، مصر، 2000،ص100.

[3] مصطفى مجدي هرجه، المرجع السابق،ص102.

المبحوث فيها واضحة وضوحا كافيا ولكن يتعين على المحكمة تبرير حكمها بالرفض بأسباب مقبولة[1]، لم يحدد القانون الخبراء الذين يجوز للمحكمة الاستعانة بهم فيجوز لها أن تختار لهذا الغرض أي شخص ترى فيه الكفاية اللازمة،حيث يختلف الخبير التقني عن الخبير المعتمد حاليا وذلك أن هذا الخبير قد يعين دون أن يكون ضمن قائمة الخبراء المعتمدين ،وقد يعين أكثر من خبير في نفس الجريمة المتعلقة بالانترنت فمثلا الأمر ليس متعلق بجريمة سرقة عبر الانترنت أو قرصنة على حقوق الملكية الفكرية أو تخريب معلوماتي أو تعديل في نظم معلومات... وإنما ابعد من ذلك فهو يتفاعل مع بيئة متعددة الاستخدامات هي الانترنت[2]،مع الإشارة إلى أن المشرع الجزائري لم ينظم كيفية ندب الخبير أمام المحكمة، لدى تسري عليه أحكام المعمول بها في هذا الشأن القواعد المعمول بها في مرحلة التحقيق الابتدائي أي المواد (143)الى(156) ق. ا .ج.ج والمادة (219) من نفس القانون.

ب–شروط أهل الخبرة.

الشروط المتطلبة في الخبرة في مجال الجرائم الناشئة عن الاستخدام غير المشروع للانترنت،إذا كانت الوسائل الإلكترونية متعددة وأن شبكات الاتصال بينها متنوعة، كما وأن طبيعتها الفنية تجعلها موزعة على تخصصات فنية وعلمية دقيقة، فإن ذلك يستوجب من جهات التحقيق والمحاكمة أن تراعى ذلك عند اختيارها للخبير، فيجب أن تتيقن أنّه تتوافر لديه الإمكانات والقدرات العلمية والفنية في مجال التخصص الدقيق للحقل الذي يطلب منه بحثه، ولا يكفي في ذلك حصول الخبير على درجة علمية معينة وإنما يجب أن تتوافر لديه أيضا الخبرة العلمية التي تمكنه

[1] محمد حسين منصور،المرجع السابق،ص214.

[2] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص988.

من اكتساب كفاءة فنية عالية ،وبالنظر إلى الطبيعة الفنية والعلمية للخبرة في مجال الجرائم الإلكترونية فإنه يمكن تحديد هذه الخبرة في الموضوعات الآتية[1]:

1-الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسة والفرعية، والأجهزة الطرفية الملحقة به، وكلمات المرور أو السر وأكواد التشفير.

2-طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية، وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

3-قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك إعطاب أو تدمير الأدلة المتحصلة من الوسائل الإلكترونية.

4-التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة[2].

بالمقابل فالجزائر قد خطت خطوات ايجابية في تقنين العديد من المسائل وعلى راسها الخبرة، وتجدر الإشارة إلى أنه وإن كان من المقرر أن المحكمة تملك سلطة تقديرية بالنسبة لتقدير الخبير الذي يرد إليها، إلا أن ذلك لا يمتد إلى المسائل الفنية فلا يجوز لها تفنيدها إلا بأسانيد فنية، تخضع للتقدير المطلق لمحكمة الموضوع، ومن ثم فلا تستطيع المحكمة أن تفندها وترد عليها إلا بأسانيد فنية قد يصعب عليها أن تشق طريقها فيها إلا عن طريق خبرة فنية أخرى[3].

[1] على محمود علي حمودة،المرجع السابق،ص53،هشام فريد رستم،الجوانب الاجرائية للجرائم المعلوماتية،المرجع السابق،ص140-141

[2] على محمود علي حمودة،المرجع السابق،ص 53.

[3] على محمود علي حمودة،المرجع السابق،ص .53

ج–عمل الخبير التقني[1].

لما أوضحنا أن الخبير في جرائم الانترنت هو خبير من نوع خاص كما انه يمكن أن يكون هناك فريق من الخبراء في نفس قضية تتعلق بجرائم الانترنت، لذلك كان لزاما أن نشرح أكثر عمل هذا الخبير،الذي يمكن الاستعانة به في أي مرحلة من مراحل الاستدلال والتحقيق والمحاكمة،وكذا القيود الواردة على عمله،على أن هذا الخبير عليه أن يلتزم بالمشروعية في أدائه لمهامه دون يخل بحق من حقوق الإنسان؛على رأسها الحق في الحياة الخاصة ،كما يلتزم بالسر المهني وواجب التحفظ.

1–تحري الحقيقة.

إن الخبرة في مواد جرائم الانترنت عنصر أساسي، بحيث يتطلب الأمر ليس مجرد التعرف على الجزئيات التي تسمح بالإدانة، وبالتالي تحديد كيفية ارتكاب الجريمة من زاوية التقنية، إنما يكون قصد الخبير التقني أيضا التعرف على ما يمكن أن يكون فكرة تقنية جديدة تفيد القضاء ومدى إمكانية قبولها في القانون[2]،وفي هذا فان الخبير يعتمد عدة أساليب في ذلك ،أن يقوم بتجميع وتحصيل لمجموعة من المواقع التي تشكل جريمة في ذاتها، كما هو الشأن في التهديد أو النصب أو السب أو جرائم النسخ وبث صور فاضحة بقصد الدعاية للتحريض على ارتكاب جرائم الدعارة والرقيق الأبيض ودعارة الأطفال وغيرها[3]،وهذا من اجل القيام بعملية تحديد المسار والتوصل الى معرفة بروتوكول الانترنت IP،أما الأسلوب الثاني الذي يعتمده عمل الخبير التقني ،هو قيامه بتجميع المواقع ولكن هذه الأخيرة خارج نطاق الجريمة،وهذه المواقع عبارة عن مواقع تحتوي على إرشادات لمواضيع كصناعة القنابل والحصول على المخدرات وكيفية زراعتها هذه المواقع يتم متابعتها باعتبارها مواقع لها روابط تؤدي إلى كشف عن جرائم انترنت، بطريقة غير مباشرة،ويتم

[1] سليمان احمد ابو الفضل، المرجع السابق،ص338 وما بعدها، فهد عبد الله العازمي،المرجع السابق،ص649-651.

[2] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص1041.

[3] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق ،ص1043.

ذلك باستخدام برمجيات متطورة مهمتها الكشف عن مثل هذه المواقع باستمرار ومعرفة الجديد فيها[1]،رغم انه وفي نفس السياق يمكن منع هذه المواقع من المنع بواسطة البروكسي.

2-التحفظ على الأدلة.

إن عمل الخبير التقني في مجال جرائم الانترنت يبدو أكثر إرهاقا لان عمله يكون في العالم الافتراضي ،يتعامل مع أدلة ليست ملموسة بل رقمية، تتطلب كل العناية في الحفاظ عليها من اجل تقديمها إلى المحكمة ،مرورا بمرحلتي الاستدلال والتحقيق،مع العلم أن لابد له من التأكد من سلامة البرمجيات التي يستخدمها للحصول على الأدلة وفحصها وإلا كان خبرته مشوبة بعيب وبالتالي يمكن ردها.

3-القيود الواردة على عمل الخبير.

إنّ أهم القيود الواردة على عمل الخبير هو ضرورة التحلي بالسرية التامة خصوصا ما تعلق بكيفيات الاختراق والثغرات الأمنية الموجودة في الأنظمة المعلوماتية،لان الخبير هنا من أعضاء الهيئة الوطنية للوقاية،رغم أن شرح الثغرات الأمنية الموجودة هو بمثابة اكتشاف وانتصار للخبير ودليل على علمه وكفاءته بالإضافة إلى أن الأساليب التي يستخدمها في تحليل هذه الجرائم تكون مشروعة،وهو باعتماد الخبرة الصادرة من أعضاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وهذا حسب المادة (12)من المرسوم(15-261) سالف الذكر،ولكن المشكل في جرائم الانترنت انه وفي بعض الأحيان يستعان بمجرمين سابقين أي الهاكر للوصول إلى حل بعض القضايا العالقة ،مما يهدد هذه الخبرة بعدم قبولها،ولكن هناك رأي يقول "أن استعانة خبير قضائي بمجرم معلوماتي للتعرف على أسلوب ارتكاب جريمة معلوماتية لا يجعل من الهاكر خبيرا في الدعوى ،إذ أن التقييم المعلوماتي يظل هنا للخبير القضائي ثم

[1] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق ،ص1044.

لقاضي،الموضوع في نهاية المطاف"[1]،ولكن ورغم هذه الاستعانة فهي على درجة من الخطورة ،كما أنها تدعو إلى دراسة هذه الظاهرة بكل موضوعية و إيجاد الحلول التشريعية المناسبة لها.

[1] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص1048.

البـــــــاب الثاني:

إجراءات الإثبات الجنائي في جرائم الانترنت في التشريع الجزائري

إنّ الدليل المستمد من اعتراض المراسلات والتقاط الصور وتسجيل الأصوات،ومراقبة الاتصالات الالكترونية يعد ثمرة من ثمرات التطور العلمي التي تساعد على كشف الحقيقة، فهو دليل علمي يجوز اللجوء إليه في الإثبات الجنائي، طالما توخي فيه المشروعية، ولم يشكل اعتداء على حريات الأفراد وحقوقهم، من خلال التقيد بالضمانات القانونية والفنية، ويخضع في النهاية للاقتناع الوجداني للقاضي[1]وقد برزت الصوت والصورة والاتصالات الالكترونية في الآونة الأخيرة،كوسائل فعالة في كشف العديد من الجرائم وإقامة الدليل على مقترفيها[2].

في هذا الإطار وضعت عدة آليات إجرائية خاصة، بداية من تعديل قانون الإجراءات الجزائية سنة 2006[3]. و استحدث إجراءات جديدة في مواجهة هذه الجريمة و لعل أهمها إجراءي التسرب و إجراء اعتراض المراسلات السلكية و اللاسلكية وتسجيل الأصوات والتقاط الصور.

كما آنه بعد ثلاث سنوات قام المشرع بسن قانون خاص رقم (09-04) المتعلق بمكافحة تكنولوجيات الإعلام و الاتصال السالف الذكر، حيث انه كان لزاما على المشرع مواكبة التطور ووضع إجراءات خاصة أكثر فاعلية؛تتوافق وتكنولوجيات الإعلام و الاتصال .

الأصل أن إجراء التحقيق في جرائم الانترنت، يمكن تقسيمه إلى قسمين الأول، هو إجراء جمع الأدلة وتحصيلها، والتي يهدف منها أساسا البحث عن الأدلة الجنائية وتتمثل أساسا في إجرائي التسرب والتقاط الصور والمراقبة الالكترونية والتفتيش. أما الإجراءات التحفظية ضد المتهم، لا تشمل التحقيق بالمعنى المباشر لانّ التحقيق هو التنقيب، ولكن الهدف من الإجراءات التحفظية منع العبث بالأدلة، كالتأثير على الشاهد ليغير شهادته، وهو ما يخرج من نطاق بحثنا كالأمر بالقبض والإحضار وجميع الأوامر القسرية.

[1] محمد أمين الخرشة، مشروعه الصوت والصورة في الإثبات الجنائي، دراسة مقارنة، دار الثقافة، عمان، الأردن،2015، ص57.

[2] موسى مسعود ارحومة، قبول الدليل العلمي أمام القضاء الجنائي، دراسة مقارنة،منشورات جامعة قاريونس، بنغازي،ليبيا، 1999،448 .

[3] القانون (06-22) المؤرخ في 20 ديسمبر 2006 يعدل و يتمم الأمر رقم (66-155) المؤرخ في 15 جويلية 1966 المتضمن قانون الإجراءات الجزائية ج.ر العدد 84 الصادرة بتاريخ 24 ديسمبر 2006.

و الواقع أن مجمل الإجراءات التي سنها المشرع الجزائري هي إجراءات تتناسب و نوع الجرائم ، و جديرة بالدراسة من ناحية كونها خاصة فقط بجرائم خاصة جرائم الانترنت وهي جرائم تكنولوجيات الإعلام والاتصال من بينها جرائم المعالجة الآلية للمعطيات؛والجرائم المتصلة بها وكذا المسهلة لها باعتبار تكنولوجيات الإعلام والاتصال وسيلة لها، و من ناحية أخرى معرفة مدى مشروعيتها وبالتالي مشروعية الدليل المتحصلة منها والضمانات المحيطة به لأنها إجراءات تقضي على الحق في الحياة الخاصة بأتّم معنى الكلمة .

لكن القانون يتجاوز بعض الضمانات في مقابل الوصول إلى الحقيقة، هذه الإجراءات التي لم تأتي من فراغ بل هو نتيجة المصادقة على العديد من الاتفاقيات التي تلزم الدولة بتحديث أساليب البحث والتحري و التعاون من اجل ضبط الدليل و ملاحقة المجرمين، كل هذا في إطار هيئة الأمم المتحدة[1].

حيث و بعد المصادقة على هذه الاتفاقيات بادر المشرع الجزائري إلى إدراج الأساليب الخاصة بالتحري و المتعلق بالجرائم الخاصة[2]، و التي من بينها جرائم تكنولوجيات الإعلام و الاتصال. ضمن قانون (06-22) السالف الذكر و القانون (09-04)و المتمثلة في أساليب ؛ تنتهك الحقوق و الحريات على رأسها الحق في الحياة الخاصة، وهذا بعد ان رجّحت المصلحة العامة لحماية المجتمع في مواجهة حماية الحق في الحياة الخاصة.

بعدما وقفت عاجزة كل أساليب التحري و التحقيق في مواجهة هذه الجرائم المستحدثة على اثباتها وتحصيل أدلتها، في حين أنّ حسن إدارة التحقيق قد يوجد للأساليب العادية، حتى لا نقول

[1] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية الصادرة 15 نوفمبر 2000 و التي صادقت عليها الجزائر بموجب المرسوم الرئاسي (02-55) المؤرخ في 2002/02/05 ج.ر09 ليوم 10 فبراير2002،ص61و اتفاقية مكافحة الفساد بتاريخ 31 أكتوبر 2003 و صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم(04-28) الصادر في 19-04-2004 ج.ر رقم 26 ليوم 25 ابريل2004 .

[2] الجرائم الخاصة هي الجرائم التي ذكرتها المادة (16) من قانون الإجراءات الجزائية التي أوردها المشرع الجزائري على سبيل الحصر في الفقرة السادسة "...غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بتشريع الخاص بالصرف...".

التقليدية مكان في مواجهة هذه الجرائم من اجل تكامل العملية الاثباتية وإعطاء نتائج مفيدة، وهذا مايدعم الدليل الجنائي للإثبات أو مايعرف بدعائم الإثبات السالفة الذكر في نهاية الباب الأول.

و بعد الحصول على هذا الدليل يتم تقييمه عن طريق خبراء قد يكونون من نفس الهيئة سالفة الذكر أو ممن تنطبق عليهم الشروط، و بين تحقيق مصلحة المجتمع في عقاب الجاني و حماية الحق في الحياة الخاصة للفرد و إعمال مبدأ قرينة البراءة الذي من نتائجه أن عبء الإثبات يقع على النيابة كجهة اتهام والمدعي، وبالتالي يعفى المتهم من إثبات براءته وهو الإثبات التي يمتد إلى أركان الجريمة الشرعي والمادي والمعنوي[1] عن طريق الضمانات الحصول على الدليل يلعب القاضي دور مهما و حاسما، تمحور حريته في الاقتناع و قبول الدليل الجنائي في إثبات جرائم الانترنت، كل ذلك يتم دراسته من خلال التحقيق الجنائي في جريمة الانترنت (الفصل الأول)، و القيمة القانونية للدليل الجنائي الالكتروني (الفصل الثاني) .

الفصل الأول:التحري و التحقيق في جرائم الانترنت في التشريع الجزائري.

لقاضي التحقيق[2] أن يباشر التحقيق و هو صاحب الاختصاص الأصيل في ذلك و لكن لكل قاعدة استثناء، و هو الحال بالنسبة لجرائم الانترنت، حيث خوّل القانون بعض السلطات لفئات مختصة، و الواقع أن التحقيق لا ينشأ تبعا لشخص معيّن و إنّما تبعا لأدلة إذا اجتمعت كونت عناصر القناعة لدى المحقق بان الجريمة قد ارتكبت فعلا بالشكل المدعى به[3]،وفي سبيل إظهار الحقيقة خول المشرع للسلطات المختصة إجراءات تمس بالحق في الحياة الخاصة وهذا كما سبق ذكره بموجب تعديل قانون الإجراءات الجزائية لسنة (2006)بعد أن صادقت الجزائر على

[1] بالنسبة للركن المادي على النيابة أن تثبت الأفعال المرتكبة من طرف الجاني قائمة، والبحث عن عناصر هو إسناده إلى شخص معلوم، أي معين، بالإضافة إلى إثبات الركن المعنوي، لذلك على النيابة إثبات القصد الجنائي، مروان محمد المرجع السابق، ج2، ص166 وما بعدها.

[2] "آن البحث عن الأدلة هو سبب وجود قضاء التحقيق"،محمد مروان، المرجع السابق،ج1،ص268.

[3] مليكه درياد ، نطاق سلطات قاضي التحقيق و الرقابة عليها ، ديوان المطبوعات الجامعية،بن عكنون، الجزائر،2012 ص 23.

العديد من اتفاقيات الأمم المتحدة،وهي اعتراض المراسلات وتسجيل الأصوات والالتقاط الصور والتسرب، الإجراءات الواردة في قانون الإجراءات الجزائية(المبحث الأول) ، الإجراءات المتعلقة بمراقبة الاتصالات الالكترونية والتفتيش والحجز الخاص بالمعطيات في إطار القانون(09-04)(المبحث الثاني).

لذلك فلقاضي التحقيق أن يقوم بمهامه بحسب ما نصت عليه المادة(38) من قانون الإجراءات الجزائية [1]، بطرق الاتصال به و ذلك إما بطلب من وكيل الجمهورية أو عن طريق الشكوى المصحوبة بادعاء مدني و هذا بحسب نص المادة(67) من قانون الإجراءات الجزائية، أي التحقيق الابتدائي.

المبحث الأول:التحري والتحقيق في جرائم الانترنت في إطار قانون الإجراءات الجزائية.

مادام أن المشرع الجزائري قد افرد للإجراءات الخاصة بتكنولوجيات الإعلام و الاتصال أي الجرائم المتصلة بالانترنت قانونا خاصا، جوهرها الأساسي المراقبة وهي الإجراءات "التي لا تخرج عن كونها رقابة مشروعة لشخص أو مكان أو أحاديث أو مراسلات مكتوبة أو مسموعة أو مرئية ،نتيجة الاشتباه في تصرفات غير قانونية وذلك بصورة لا يحس معها الغير بمباشرتها لطابع السرية التي يكتنفها"[2].

[1] المادة 38 :" تناط بقاضي التحقيق إجراءات البحث و التحري و لا يجوز له أن يشترك في الحكم في قضايا نظرها بصفته قاضيا للتحقيق و إلا كان ذلك الحكم باطلا"

و له في سبيل مباشرة مهام وظيفته أن يستعين مباشرة بالقوة العمومية .

و يختص بالتحقيق في الحادث بناءا على طلب من وكيل الجمهورية أو شكوى مصحوبة بادعاء مدني ضمن الشروط النصوص عليها في المادتين67 و 73.

في حالة الجناية أو الجنحة المتلبس بها يباشر قاضي التحقيق السلطات المخولة له بمقتضى المادة 57 و مايليها".

[2] فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية،مجلة العلوم الإنسانية، عدد 33،جوان 2010،جامعة الإخوة المنتوري قسنطينة ، الجزائر،ص236.

فقد ارتأينا أن نخصص للإجراءات الواردة في قانون الإجراءات الجزائية مبحثا ذلك أنها إجراءات لجرائم الانترنت، منها جرائم المساس بالمعالجة الآلية للمعطيات، كما أنها إجراءات خاصة لجرائم خاصة التي تم التنصيص عليها في إطار المادة (16)من قانون الإجراءات الجزائية السالفة الذكر[1]، وهي على نوعين اعتراض المراسلات و تسجيل الأصوات و التقاط الصور (المطلب الأول)، التسرب (المطلب الثاني).

[1]–**جرائم المخدرات** المنصوص عليها في القانون (04-18) مؤرخ في 25 ديسمبر 2004 يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها،ج.ر رقم 83 ليوم 26 ديسمبر2004.و هذا ضمن المادة 17 منه و التي تشمل كل من المخدرات و المؤثرات العقلية ، مع ملاحظة أن المشرع في نص المادة(16)من ق.ا,ج,ج قد نص على المخدرات دون المؤثرات العقلية، زيادة على أن ما تعلق بالمخدرات فقد اقتصر على المتاجرة فقط دون الاستهلاك .

–**الجريمة المنظمة عابرة الحدود الوطنية**،(176) من قانون العقوبات المادة المعدلة بموجب القانون(04-15) مؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات ج.ر.رقم 71 بتاريخ 10 نوفمبر 2004،إن التعريف الشائع للجريمة المنظمة هو أنها مؤسسة إجرامية ذات تنظيم هيكلي متدرج تمارس أنشطة غير مشروعة بهدف الحصول على المال مستخدمةكافة الطرق الناتجة لتحقيق هذا الهدف لتمويل مشروعها لإجرامي و ذلك في سرية تامة لتأمين و حماية أعضائها ،

–**الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**، يرجى الرجوع إلى المبحث الثاني من الفصل الأول من الباب الأول لهذه الرسالة،ص51.

–**جرائم تبييض الأموال** قانون (05-01) ليوم 06 فبراير 2005 يتعلق بالوقاية من تبييض الأموال و تمويل الإرهاب و مكافحتها. ج.ر رقم 11 ليوم 9 فبراير2005، المادة 389 مكرر و تشمل تحويل الممتلكات أو نقلها مع علم الفاعل أنها عائدات إجرامية بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات .

إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها ،اكتساب الممتلكات أو حيازتها أو استخدامها مع علم القائد بذلك أنها عائدات إجرامية ،و كل أعمال المشاركة – التواطؤ- التحريض على ارتكابها و تسهيلها و إبداء المشورة بشأنها تبيض الأموال .

–**الجرائم الإرهابية**،و هي الجرائم التي نص عليها قانون العقوبات ضمن القسم الرابع مكرر تحت عنوان الجرائم الموصوفة بأفعال إرهابية و تخريبية من الفصل الأول ضمن الباب الأول من الكتاب الثاني الجزء الثاني و ذلك من المادة 87 مكرر إلى 87 مكرر 9 من ق.ع و التي جاءت ضمن الأمر رقم (95-11) المؤرخ في 1995/02/25،حيث صنفتها من بين الأفعال التي تعد أعمالا إرهابية و هو كل فعل يستهدف أمن الدولة الوحدة الوطنية اللازمة الترابية ، استقرار المؤسسات ،يرجى الرجوع الى المبحث الثاني من الفصل الأول من الباب الأول من هذه الرسالة،ص51.

–**جرائم الصرف**: الجرائم المتعلقة بالتشريع الخاص بالصرف،جاءت هذه الجرائم ضمن الأمر رقم (96-22)المؤرخ في 1996/07/09 المتعلق بقمع مخالفات التشريع و التنظيم الخاصين بالصرف و حركة رؤوس الأموال من وإلى الخارج ج.ر رقم43 ليوم 10 يوليو1996.

المطلب الأول:اعتراض المراسلات والتقاط الصور وتسجيل الأصوات[1].

إنّ من أثر استخدام تكنولوجيات الإعلام والاتصّال، ظهور أنواع جديدة من الإجرام المستحدث والذي بدوره يؤثّر على نوعية الدليل الجنائي، الذي بدوره يحتاج إلى وسائل خاصة لجمعه وتقديمه[2]، ومن بين هذه الأساليب التي أقرتها الاتفاقيات الدولية والإقليمية، والتي جسدتها التشريعات الوطنية ومن بينها التشريع الجزائري؛ بموجب القانون رقم (06-22)المؤرخ في 20-12-2006 المعدل والمتمم لقانون الإجراءات الجزائية من خلال الفصل الرابع من الباب الثاني من الكتاب الأول تحت عنوان في اعتراض المراسلات وتسجيل الأصوات والتقـــــاط الصور(الفرع الأول)ـ المواد من (65 مكرر5) إلى المادة (65 مكرر10) ماهو تعريف هذه الإجراءات وماهي شروط اللجوء إليها(الفرع الثاني).

–جرائم الفساد: و هي كل فعل من الأفعال الواردة في القانون (06-01) المؤرخ في 20 فبراير2006يتعلق بالوقاية من الفساد ومكافحته ج.ررقم 14 بتاريخ 8مارس2006.و التي تشمل كل أفعال الرشوة اختلاس المال العام و الخاص ، اخذ فوائد من الصفقات العمومية تلقى الهدايا للعجز عن تبرير الزيادة غير المبررة في الأموال إبرام صفقات بصورة مخالفة للقانون ، عدم التصريح بالممتلكات أو عدم صحة التصريح.

[1] نستثني المراقبة من الإجراءات الخاصة بجرائم الانترنت الواردة في قانون الإجراءات الجزائية، كونها متعلقة بتمديد الاختصاص،أدخلت المادة (7)من القانون (06-22) تعديلا على المادة (16) قانون إجراءات جزائية و أكملته بإدراج المادة (16 مكرر) التي تضمنت المراقبة فنصت على " يمكن لضباط الشرطة القضائية و تحت سلطتهم أعوان الشرطة القضائية ما لم يعترض على ذلك وكيل الجمهورية المختص بعد إخباره يمددوا عبر كامل الإقليم الوطني عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحتمل الاشتباه فيهم بارتكاب الجرائم المبينة أعلاه في المادة 16، أو مراقبة وجهة أو نقل الأشياء أو الأموال أو متحصلات من ارتكاب هذه الجرائم أو قد تستعمل في ارتكابها " و الملاحظة أن المراقبة هنا جاءت في إطار تمديد الاختصاص و ليس ضمن أساليب الخاصة كالتسرب و اعتراض المراسلات، و كما اشرنا سابق كل أساليب التحري الخاصة هي ضمن اتفاقيات الأمم المتحدة التي صادقت عليها الجزائر.و هو الحال بالنسبة لنص المادة 20 من الاتفاقية المتعلقة بمكافحة الجريمة عبر الوطنية، لذلك عند بحثنا في الموضوع وجدنا أن معظم المؤلفين يستثنون المراقبة من أعمال البحث و التحري و التحقيق الخاصة؛ ذلك أنها وردت كما قلنا كامتداد لاختصاص و ليس أسلوب التحري، لأنها لم ترد في المواد 65 مكرر5 إلى 65 مكرر 18 ذلك أن امتداد الاختصاص مرتبط أصلا بالمراقبة المادية للشخص أو الشيء أو الأموال أو المتحصلات الإجرامية لأنّ بدونها لن تكون للتحرّي أي فائدة، و لكن سوف نتطرق لها باعتبار هذا المصطلح قد جاء به القانون 09-04، بخصوص مراقبة الاتصالات الالكترونية ، لذلك سوف نعمل على التفريق بين المراقبة المنصوص عليها في المادة (16 مكرر) من ق.ا.ج.ج و المراقبة المنصوص عليها في المادة (04) من قانون (09-04)كل هذا في إطار آليات الكشف عن الدليل في جرائم الانترنت في المبحث الموالي.

[2] Aurélie Bergeaud-Wetterwald, Jean-Christophe Saint-Pau , La preuve pénale, Problèmes contemporains en droit comparé , Editions L'Harmattan, 2013,p14

الفرع الأول:تعريف اعتراض المراسلات وتسجيل الأصوات والتقـــــاط الصور.

ظهرت ملامح اللجوء إلى التقنية واضحة في التطور التشريعي الجزائي لدى المشرع الجزائري، منذ سنة 2006، بتعديله لقانون الإجراءات الجزائية،حيث تكمن أهمية هذه المواكبة في صورة تتلائم في الإجراءات الجزائية و جرائم الانترنت وكذا بيان دور الأجهزة الإجرائية المختصة لمواجهة هذه النوعية من الجرائم وضبطها بما يتوافق مع بيئتها .

يترافـق التطـور التكنولـوجي بتطـور في التشـريع سـواء في قواعـده الموضـوعية أو الإجرائيـة، خصوصا ما يتعلق بالإثبات الجنائي خصوصا، وهو الحال بالنسبة لاعتراض المراسلات(أولا) والتي يقصد بها التصنت التلفوني[1]، التقاط الصور(ثانيا)وتسجيل الأصوات (ثالثا) .

أولا:اعتراض المراسلات.

إن اعـتراض المراسـلات خصوصـا المكتوبـة هـي مـن الأسـاليب القديمـة في التحقيـق[2]، أمـّا اذا كانت عن الطريق السلكي أو اللاسلكي، نعنى بها السكون أو استماع الحديث مع ترك الكلام، وهو الاستماع سرا بوسيلة أيا كان نوعها تقليدية او متطورة لكلام له صفة الخصوصية متبادلة بين شخصين أو أكثر[3]. يقصد بالحق في المراسلات عدم جواز الكشـف عـن محتوياتها لاعتبـاره مجالاها هاما لإيداع الأسرار تعلقت بالمرسل أو المرسل إليه أو حتى الغير، والتي جاءت في شكل مراسلة[4].

[1]أحسن بوسقيعة، التحقيق القضائي، دار هومه، الجزائر،2012، ص113. ويتم التصنت بطريقتين أو أسلوبين **الأول** عن طريق الربط السلكي مباشرة بالخط الهاتفي المتجه من المركز إلى منزل الشخص المراقب حيث توصيل السلك بسماعة تليفون وجهاز تسجيل، يتم من خلالها التصنت والتسجيل، يمكن للشخص المراقب اكتشافها نظرا لما يطرأ على الاتصال من تشويش بسبب تدخل المتصنت، أما الأسلوب **الثاني** مادام ان الاعتراض خاص بالاتصالات السلكية واللاسلكية فالأسلوب الثاني هو التصنت اللاسلكي حيث انه يتم عن طريق الالتقاط المغناطيسي ، والتقاط الاحاديث عن طريق المجال المغناطيسي، والواقع ان التكنولوجيات الحديثة قد احدثت نقلة نوعية في مجال التنصت حتى على الهواتف النقالة ،عن طريق استخدام مايكروفون الهاتف الخليوي لنقل وتسجيل الاحاديث،محمد امين الخرشة ،المرجع السابق،ص50-51.

[2] Sylvain Métille , Mesures techniques de surveillance et respect des droits fondamentaux en particulier dans le cadre de l'instruction pénale et du renseignement;collection neuchateloise,2011 ,p36

[3] عبد الحميد الشواربي، المرجع السابق، ص9.

[4] علي احمد عبد الزعبي، حق الخصوصية في القانون الجنائي"دراسة مقارنة"،المؤسسة الحديثة للكتاب، طرابلس،لبنان،2006،ص182و183.

وفقاً لنص المادة (65 مكرر 5) حدد المشرع إجراء اعتراض المراسلات التي تتم بطريقة سلكي ولاسلكي[1]، حيث استثنى المراسلات الإلكترونية، لأنّه يمكن أن تتم خارج النطاق السلكي أو اللاسلكي، و قد أفرد لها مواد قانونية خاصة في إطار القانون (09-04) لمراقبة الاتصالات الإلكترونية، مما لا يدعو للشك أن المراسلات المقصودة هنا هي المتعلقة بالهاتف الثابت والنقال ولكن بعد رقمنة كل وسائل الاتصال والإعلام يصعب التفرقة بين ما هو رقمي وما هو غير ذلك، لذلك وعلى هذا الأساس جمع المشرع كل الاتصالات في خندق واحد بموجب المادة (05) من المرسوم رقم(15-261)[2].

أ-مـــراقبة الهـــاتف:

مراقبة المحادثات التلفونية تعني من ناحية التصنت على المحادثات، ومن ناحية أخرى تسجيلها بأجهزة التسجيل.ويكفي مباشرة هاتين العمليتين (التصنت أو التسجيل) لقيام المراقبة، فقد تتم بمجرد التصنت، وقد يكتفي بالتسجيل الذي يسمع بعد ذلك ثم يفرغ مضمونه في المحضر المعد لذلك[3]. لذلك لايعدّ؛ من مراقبة الهاتف تركيب جهاز كاشف من قبل السلطات المختصة على هاتف المجني عليه في جريمة القذف بناءا على طلبه من اجل معرفة الأرقام المتصلة، فالهدف هنا هو الكشف دون التصنت[4]. كما يقصد باعتراض المراسلات "اعتراض أو تسجيل أو نسخ للمراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهي عبارة عن بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض "[5] واعتراض أي شيء في

[1] المادة (65 مكرر1) "... اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية".

[2] مرسوم رئاسي رقم (15-261) يحدد تشكيلة وتنظيم كيفيات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج ر 53 ليوم 08 أكتوبر 2015 ،ص17.

[3] محمد ابو العلا عقيدة ،مراقبة المحادثات التليفونية،دراسة مقارنة،2008،دار النهضة العربية،القاهرة ،مصر،ص15.

[4] محمد ابو العلا عقيدة، مراقبة المحادثات التليفونية ،المرجع السابق،ص17.

[5] رشيدة بوكر، المرجع السابق، ص441.

مسار المراسلات وتمنع مرورها ووصولها لمستقبليها حتى تفحصها؛ وربما يؤدي ذلك إلى تسجيلها أو نسخها بحسب حالتها المرسلة.

والأصل أن هذا الإجراءات يدخل ضمن الاعتداء على الحق في الحياة الخاصة، باعتبار ان الحق في سرية المراسلات يعد جوهر الحق في الخصوصية، لذلك كان لممارسة هذا الإجراء شروط تضمن حقوق وحريات الأفراد من طرف السلطات المختصة.

وبالعودة إلى مفهوم المراسلات بالوسائل السلكية واللاسلكية، نجد أن القانون (2000-03) ، المحدد للقواعد المتعلقة بالبريد والمواصلات السلكية واللاسلكية[1] فإنه عرفها في المادة(08الفقرة11) "كل تراسل أو إرسال أو استقبال علامات أو إشارات كتابات صور أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية"[2]،فهنا المشرع كان قصد المراسلات العادية أي دون أن تكون مرقمنة، أي المراسلات التي يخرج من نطاقها المراسلات الالكترونية، المقصودة في القانون(09-04).

وبالرجوع إلى المادة الثامنة من قانون (2000-03)فإن المراسلات محل الاعتراض قد تكون المكالمات الهاتفية أو المراسلات المكتوبة بأي طريقة عدا الاتصالات الإلكترونية لأنها منظمة بموجب قانون خاص، ويتجسد هذا الاعتراض في مراقبة الهاتف فلأي مدى هذا الاعتراض مشروع؟.

أو اعتراض المكالمات الهاتفية سواء الهاتف الثابت أو النقال الإجراء الذي ينتهك الحياة الخاصة، خصوصا أن الوسيلة المستخدمة في المراسلات هي الهاتف الذي يسترسل الفرد في الحديث عن كل أموره من المعلنة إلى المسترة، والذي خصها المشرع بضمانات بداية من نوع

[1] بعد ان تّم إيداع أطروحة الدكتوراه من أجل المناقشة، قام المشرع الجزائري بالغاء القانون (2000-03) بالقانون (18-04) مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية ،ج ر 27 ليوم 13 مايو 2018،ص.3.

[2] القانون (2000-03) مؤرخ في 5جمادى الاولى عام 1421 الموافق5غشت سنة 2000ج.ر عدد 48 ليوم 06 غشت2000ص03.

الجرائم التي تلجأ فيها السلطات المختصة لهذا الإجراء وصولا للإذن والمراقبة المستمرة مِنْ مَنْ اصدر الإذن، والتي تعتبر اي اعتراض المراسلات اشد انتهاك لحرمة الحياة الخاصة من المراقبة عبر نظام التعقب البعدي GPS[1].

ونقصد بمراقبة الهاتف[2]، هي اعتداء على حرية الحديث الذي هو حق من الحقوق اللصيقة بالشخصية الإنسانية ، اعتراض المكالمات الهاتفية، والتوقف في مسارها الاتصالي بين المرسل والمرسل إليه، وهذا ما ذكرت المادة (65 مكرر5)عن طريق وضع الترتيبات التقنية، دون موافقة الأشخاص المتصلين والأصل أن الاتصالات السلكية تكون بين طرفين فقط، بعكس الاتصالات الهاتفية الإلكترونية قد تكون ضمن مجموعة من الأفراد كما هو الحال في(skype)، ولكن تجدر الإشارة إليه وبالنظر إلى التطور التقني، وعملية رقمنة وسائل الاتصال والإعلام أصبح الأمر أكثر بساطة من ذي قبل طبعا بتوافر شروط للإجراء نفسه، أو الترتيبات التقنية، لدى نرى بان الإجراءات التي جاء بها قانون الإجراءات الجزائية كانت ملائمة لفترة ما قبل رقمنة الاتصالات التي بموجبها يمكن مراقبة الهاتف بكل شبكاته أي الثابت والمنقول وما يدعم ذلك هو نص المشرع في المادة (05) من المرسوم (15-261) التي أضافت إلى الاتصالات الإلكترونية، الهاتف الثابت والنقال.وأصل مراقبة الهاتف أو المراسلات (السمعية وتسجيلها) أو" أصل القاعدة يوجد في الطبيعة السرية للخطابات الخاصة ... ومضمونها عدم جواز مصادرة أو اغتيال سرية المراسلات بين الأفراد لما يتضمنه من اعتداء على حق ملكية الخطابات المتضمن لهذه المراسلات"[3].

ومما لا شك فيه أنّ هذه المراسلات لم تعد حقا مطلقا، فكل شيء نسبي لأن لكل قاعدة استثناء ولذلك كان للسلطة المختصة حق اللجوء إلى الإجراءات الخاصة في جرائم محددة قانونا

[1] Aurélie Bergeaud-Wetterwald, Jean-Christophe Saint-Pau ,Op ;Cit ;P ;19

[2] محمد أمين الخرشة، المرجع السابق، ص46.

[3] منذر الويس،المرجع السابق،ص252.

بشروط معينة لولاها لخرج الفعل الذي يقوم به الضابط المختص من دائرة الإباحة إلى دائرة التجريم.

ب–مدى مشروعية مراقبة الاتصالات الهاتفية:

ويرى الفقه أنّ مراقبة الهاتف الإجراء في حد ذاته وليس الدليل الناتج عنه، تتأرجح بين قائل بعدم مشروعيته ، وأخر بمشروعيته.

1–عدم مشروعية مراقبة للاتصالات الهاتفية:

الأصل فيها أنها تنافي الأخلاق لما تشمله من استراق للسمع فالأصل أن المراقبة تنجر عنها تسجيل للمحادثات وهو ما يتعارض وحق الإنسان في الحياة الخاصة التي عادة ما تكون موضوعا للمحادثات الهاتفية، إذ لا يجوز الحصول على أدلة تكشف غموض الجريمة وتدين المتهم؛ بإتباع أسلوب غير نزيه في البحث والتحري، وهو المبدأ الذي يتفق مع احترام حقوق الإنسان، ومن بينها حقوق الدفاع التي تعد شرطا لازما لنزاهة البحث عن الأدلة وبالتالي صحة الإجراء[1].

2–مشروعية مراقبة الاتصالات الهاتفية:

إن الزيادة المطردة للجرائم هو الذي دعي العديد من الفقهاء وخاصة للافراد، لضرورة الأخذ بإجراء التصنت الهاتفي، وإخراجه إلى دائرة الأفعال المبررة في مواجهة جرائم خطيرة كالمخدرات والرشوة والجرائم المتعلقة بأمن الدولة والإرهاب[2]، وجسدته بعد ذلك اتفاقيات الأمم المتحدة التي صادقت الجزائر عليها.

إذن فانّ الأصل في إجراء مراقبة الهاتف هو الحظر، وهو ما كرسه الدستور الجزائري، وهذا حفاظا على الحرية الشخصية، فلولا أن علم الشخص انّه مراقب لما تحدث بكل حرية عن كل ما

[1] محمد ابو العلا عقيدة، مراقبة المحادثات التليفونية المرجع السابق،ص22 –27

[2] محمد ابو العلا عقيدة، مراقبة المحادثات التليفونية ،المرجع السابق،ص 32

هو سر أو شخصي، بالمقابل فانّه ولمواجهة بعض الجرائم كان لابد من إقرار هذا الإجراء ولكن بشروط تضمن عدم التعسف في استعماله،والتأكد من الشخص مصدر الحديث والتأكد كذلك من عدم تعديل بالإضافة أو الحذف في التسجيلات، وبالتالي يكون الدليل الناتج عنه دليل مشروع يمكن الاعتداد به في الحكم على المتهم بالإدانة أو البراءة.

ثانيا:التسجيل الصوتي.

ثاني إجراء من الإجراءات الخاصة التي سنها المشرع الجزائري، إجراء التسجيل الصوتي الذي يتم اللجوء إليه بالإضافة إلى شرط الجرائم الخاصة لابد لممن شروط معينة.

أ-تعريف السجيل الصوتي

التسجيل الصوتي يشمل تسجيل الأحاديث الشخصية وتسجيل الأصوات،فالحديث عبارة عن كل صوت له دلالة التعبير عن مجموعة من المعاني والأفكار[1]، كما يشمل التحدث بصوت مرتفع، لذلك يخرج عن نطاق تسجيل الأصوات الأحاديث التي لا تتضمن اعتداء على الحق في حماية الحديث وتسجيله كما هو الحال في تسجيل الأحاديث الإذاعية والتلفزيونية أو الصحفية بعد موافقة المعني[2]، أمّا تسجيل الصوت فهو إفراغ الأحاديث الخاصة في وعاء يحفظها مخصص لإعادة سماعها في وقت لاحق ونقله من مكان إلى أخر[3]. وهو التعريف المرتبط باعتراض المراسلات باعتبار انّه لا يمكن اعتراض هذه الأخير دون تسجيل[4]، والذي لم يعرفه المشرع الجزائري بل وضح الجانب الفني منه في المادة (65مكرر 5)الفقرة 3 ق.ا.ج.ج بقولها "هو وضع الترتيبات التقنية

[1] علي احمد عبد الزعبي،المرجع السابق،264 .

[2] نقادي عبد الحفيظ، التسجيل الصوتي،المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية،جامعة بن عكنون، الجزائر، ع2009،1، ص311.

[3] عاقلي فضيلة، الحماية القانونية للحق في الحياة الخاصة ،دراسة مقارنة،دكتوراه علوم في القانون الخاص جامعة الإخوة منتوري قسنطينة،كلية الحقوق،2011-2012، ص242.

[4] أمينة ركاب،أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري،مذكرة ماجستير،كلية الحقوق والعلوم السياسية،جامعة ابو بكر بلقايد تلمسان،الجزائر،2014-2015، ص60.

دون موافقة المعنيين، من أجل التقاط أو تثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية".

ثار خلاف حول مشروعية التسجيل الصوتي، حيث أنّ المقصود من التسجيل الأصوات المحادثات الخاصة أو تسجيل المحادثات الخاصة دون أن يرتبط ذلك بالمكان المتواجد فيه[1]، فالأصل أن المشرع قد اوجد الحماية الجنائية للحديث الخاص دون نوع المكان، وهذا بموجب المادة (303مكرر) من قانون العقوبات.

ب–معيار تسجيل الأحاديث.

على اثر ما يخلفه تسجيل الأحاديث الخاصة من انتهاك للحق في الحياة الخاصة، في مقابل أن يكون الدليل الأكثر نجاعة لإثبات العديد من الجرائم الخطيرة والمنتشرة كجرائم الانترنت، حاول الفقه وضع معيار فاصل بين ماهو حديث خاص وما يخرج من نطاقه، إنّ الأصل أنّ ايّ حديث يدور بواسطة وسيلة أيـّا كانت تقليدية أو متطورة هو حديث خاص يجرم الاعتداء على خصوصيته، ولكن كيف نميز بين الحديث الخاص والعام إذا كان الأشخاص في مواجهة بعض أي في نطاق مكاني متقارب،اعتمد اتجاه من الفقه على المعيار الشخصي أي معيار الشخصي أو موضوع الحديث وآخرون اعتمدوا المعيار الموضوعي[2].

1–الاتجاه الأول:المعيار الشخصي

إن الأصل في التميز بين ما هو خاص وعام، موضوع الحديث نفسه فكلما كان الحديث فحواه أمور خاصة، يتحدث بها الفرد بتحفظ بغية أن لا يسمعه الغير حتى وان كان في مكان عام، فهو حديث خاص[3]. ولكن هذا لا يمنع من جواز تسجيله – الحديث الخاص –وفق شروط

[1] محمد امين الخرشة،المرجع السابق،ص143

[2] ياسر الأمير فاروق،مراقبة الأحاديث الخاصة في الإجراءات الجنائية،دار المطبوعات الجامعية ، مصر،2009 ص521 و523.

[3] ركاب امينة ،المرجع السابق،ص63.

وضمانات قانونية متى ثبت أنّ تسجيل هذه الأصوات تحمل في طياتها دليل للجريمة كان للإثبات[1]. مع ملاحظة ان المشرع الجزائري وبموجب المادة (65 مكرر 5) الفقرة 3 من قانون الإجراءات الجزائية قد أخذ بالمعيار أعلاه أي المعيار الشخصي، وعلى اثر ذلك ظهر اتجاه ثاني وهذا بعد وجود صعوبة في تحديد مفهوم الحديث الخاص.

2-الاتجاه الثاني المعيار الموضوعي.

بغض النظر على طبيعة الحديث الخاص أو العام لان هناك الكثير من الأشخاص،لا يمكن الجزم بنوع الحديث الذي تفوه به، يرى أنصار هذا الاتجاه انه لابد من الاخذ بطبيعة المكان الذي يدور فيه الحديث كمعيار للتفرقة بين الحديث العام والحديث الخاص ،وذلك بحسب طبيعة المكان المتواجد فيه،أي المكان العام فالحديث الدائر هو حديث عام أما في المكان الخاص فالحديث خاص،كل حديث في مكان خاص الأصل فيه انّه واجب الحماية، على عكس الحديث الخاص في المكان العام، فلا يمكن طلب الحماية من المشرع بعد الإفراط بالحديث في أسرار خاصة في مكان عام، في حين أنّ معيار المكان الخاص لا يكفل الحماية للحديث الخاص ، لذلك برز معيار مفاده أنّ خصوصية الحديث تتحدد على أساس طبيعة المكان من جهة ومن جهة طبيعة الحديث ذاته[2]،أي أنّ الحديث أصلا خاص في مكان خاص وإذا تعلق بالحياة الخاص فهو خاص في المكان العام، حيث انه ومن الواقع يمكن أن تشكل الأماكن العامة فضاء جيدا لتبادل الأحاديث السرية والمتعلقة بالحياة الخاصة للأطراف، دون وجودهم في أماكن خاصة كالمنزل مثلا.

عادة لا يكتمل الدليل دون صورة، أي تسجيل الأصوات والتقاط الصور، رغم أنّ كل دليل هو مستقل بحد ذاته.

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائكم الكمبيوتر والانترنت، المرجع السابق،ص،375.

[2] علي احمد عبد الزعبي،المرجع السابق،264 و265.

ومما لا شك فيه أن الاعتداء على الأحاديث الخاصة التي تعني النطق والتفوه لشخص أو عدة أشخاص أو لذات الإنسان نفسه سرا أو في مكان خاص، لا يقتصر فقط على المحادثات بل قد يشمل الاعتداء على النطاق السمعي للحياة الخاصة للفرد، إذا فالأصل أن تسجيل الصوت محظور ولكن إذا تعلق الأمر بجرائم خاصة فهو من الأفعال المبررة.

ثالثا: التقاط الصور.

إنّ الحق في الصورة هو من مظاهر الحياة الخاصة للفرد والتي يمكن الاعتراض عليها أي في أخد صورة له و لولم يرغب، ولكن نعيد ونكرر انّه اذا كان التقاط الصور دون غيره هو الدليل الوحيد لإظهار الحقيقة في جرائم الخاصة ومنها جرائم الانترنت ،رخص المشرع الجزائري التقاطها خفية عن صاحبها وبالتالي رضاه لم يعد في الاعتبار ،وذلك تغليبا للمصلحة العامة على الخاصة أو ما يعرف بالرقابة المرئية.

أ-تعريف التقاط الصور

التقاط الصور عن طريق وضع الترتيبات والمعدات التقنية اللازمة دون أخذ موافقة المعنيين في مكان خاص، فإذا تعلقّ الأمر بجريمة خاصة يمكن اللجوء إلى التقاط الصور في مكان خاص و هو المكان الواضح المعالم والذي لا يمكن الدخول إليه إلا بإذن[1]، ورغم أن هذه الأساليب قد تساعد كثيرا في إثبات أو نفي الجريمة عن المتهم ،إلا أن التطور التكنولوجي يقف حائلا دون اعتبارها دليلا سيدًا، لدى على القاضي التعامل معه كدليل عادي مثل باقي الأدلة[2]؛ خصوصا في ظل نقص الضمانات الإجرائية من جهة، والتطور التقني والاستعمال الرقمي في معالجة الصورة والصوت،التي لا نفرق فيها بين الأصلي والمفبرك .

[1] علي أحمد عبد الزعبي، المرجع السابق،ص174.

[2] فوزي عمارة، ،المرجع السابق،ص238.

إنّ للشخص الحق في الصورة، حيث يخول له حق الاعتراض على التقاط صورة له باعتبارها من مظاهر الحق في الحياة الخاصة،ويدخل في هذا النطاق إنتاج ونشر الصورة دون رضاه، والتقاط الصور هو تثبيت الصورة على أي دعامة كانت إمّا الدعامة الورقية أو المادية، أو دعامة رقمية ،ونقل وإرسال وتحويل الصورة يقصد به تمكين شخص يوجد في مكان مختلف عن المكان الذي التقطت له الصورة من الاطلاع عليها ،سواء كان المكان عام واو خاص[1].كما وانه بالتطور التكنولوجي تعددت وسائل تسجيل الصورة ،إمّا عن طريق آلات التصوير أو أي آلة متطور تستعمل ألان تلتقط الصور الساكنة أو المتحركة، أوسوف تظهر مستقبلا إن شاء الله،ومنه الهاتف الخليوي الذي أصبح يحتوي على تقنيات عالية لتسجيل الصور والفيديوهات بأعلى تقنية وجودة في الصورة، وبإمكان أي كان استخدامه، حيث لم يعد استخدام التقنيات المتطور حكرا على السلطات الأمنية، فكما للأجهزة المتطورة إسهاما في التحري والتحقيق هي كذلك مصدر لخطر يهدد الأفراد[2].

ب–معيار التقاط الصور. وكحال التسجيل الصوتي اختلف الفقه في تحديد طبيعة المكان الخاص، الذي يدخل التقاط الصور ضمن التجريم أو الإباحة، فمنهم من تبنى المعيار الشخصي أي الاعتداد بحالة الخصوصية لتحديد المكان الخاص،في حين اعتبر آخرون أنّ العبرة بالمكان دون حالة الأشخاص.

1–المعيار الموضوعي: والذي يضع لطبيعة المكان وزنا في تحديد مدلول المكان الخاص، الذي يخرج من نطاقه التعريف التالي للمكان العام ،هوكل مكان يمكن ارتياده من قبل الجمهور سواء بمقابل أو بغير مقابل وسواء كان الدخول بشرط أو من غيره وينقسم المكان العام إلى ثلاثة أنواع:

[1] عاقلي فضيلة، المرجع السابق، ص72.

[2] محمد امين الخرشة، المرجع السابق،ص 173و174.

-الأماكن العامة بطبيعتها :ويقصد بها الأماكن التي تكون معدة منذ إنشائها لدخول الجمهور،وتردد عليها في حرية(الميادين والشوارع والأزقة والمنتزهات و الحدائق المفتوحة) .

-الأماكن العامة بالتخصيص:وهي الأماكن التي يسمح بارتيادها في أوقات معينة، ويكون الدخول إليها ممنوعا في غير هذه الأوقات (المرافق العامة التي تتصل أعمالها بالجمهور ودور السينما، ودور العبادة)

-الأماكن العامة بالمصادفة، وهي بحسب الأصل تكون أماكن خاصة، ويكون أمر ارتيادها مقصورا على أفراد وطوائف معينة ، إلا انّه يباح للجمهور بصفة عارضة ارتيادها والدخول فيها(المدارس ، السجون ، النوادي ،المخازن، والمحال التجارية) [1].

وبالعودة إلى نص المادة(65مكرر5) ومن خلال قراءتها نستنتج أن المشرع الجزائري قد أعطى وزنا للمكان العام، بمعنى انّ تحديد المكان الخاص أو طبيعة المكان هو بما يأنس له الأشخاص ويرتاحون فيه في التقاط الصور أي المعيار الموضوعي أي طبيعة المكان، على عكس تسجيل الأصوات فالعبرة فيه بالحديث الخاص، أي معيار الشخصي حسب نص المادة"...التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.."، وفي هذا انتهاك لخصوصية الأشخاص خصوصا ما تعلق بالعلاقات الأسرية، والرابطة الزوجية، حتى لو تعلق الأمر بضرورات التحقيق وبجرائم الخاصة ،ذلك أنّ التقاط الصور والفيديوهات في أماكن خاصة لا يشمل معه فقط المشتبه فيه بل يتعداه إلى الأسرة والأزواج وحتى الغير.

2-المعيار الشخصي. ياخد أنصار من يعتمدون هذا المعيار بحالة الأشخاص، دون أماكن تواجدهم،بمعنى وجودهم في مكان خاص مكان مغلق يتعذر بلوغه بنظرات من الخارج، ولا يكون دخوله إلا بإذن صاحبه، مهما كانت وضعية هذا الأخير، سواء أكان مالكه أم مستغله أم المنتفع

[1] هامش محمد عبد العظيم محمد، حرمة الحياة الخاصة في ظل التطور العلمي الحديث،رسالة دكتوراه،جامعة القاهرة،1988،مشار إليه لدي محمد أمين خرشة، المرجع السابق، ص180.

به، المهم أنه ساكنه، وهو بهذا يعتبر بمثابة دائرة خاصة و محددة به[1]، وهو المكان الذي يشمل أي نطاق لا يمكن للغير دخوله،حتى ولو كان في مكان عام-مثلا السكن الوظيفي داخل مؤسسة عمومية- أخد شخص على جنب في مكان عمومي والتحدث معه،فحيز وجودهما رغم انه مكان عام إلا انّ الشخص أضفى عليه طابع الخصوصية[2].

مما لاشك فيه أنّ جميع الإجراءات السالفة الذكر هي اعتداء على الحق في الحياة الخاصة حتى وان كان لجمع الدليل الجنائي لأخطر الجرائم في نظر المشرع والذي اعتمدها أي الإجراءات بناء على اتفاقيات دولية، إلا أن ذلك لا يمنع من وجود شروط موضوعية وإجرائية للجوء إلى مثل هذه الإجراءات.

الفرع الثاني:شروط الأخذ بإجراء اعتراض المراسلات والتقاط الصور وتسجيل الأصوات.

لكل إجراء شروط خاصة به، ويمكن استخلاصها من المادة(65 مكرر 5) ق.ا.ج.ج والمتمثلة في مجموع من القيود والضوابط لتضيق مجال التعدي على الخصوصية من خلال تعسف السلطة القضائية في اللجوء إلى هذه الأساليب الخاصة عبر إقراره مجموعة من الشروط التي تتمثل في شروط موضوعية(اولا)وأخرى شكلية(الفرع الثاني).

أولا:الشروط الموضوعية لإجراء اعتراض المراسلات والتقاط الصور وتسجيل الأصوات.

حتى يلجا قاضي التحقيق إلى مثل هذه الإجراءات لابد من وجود دلائل؛ وقرائن قوية لارتكاب السلوك الإجرامي المتعلقة بجرائم الانترنت، بمعنى وجود ضرورة للجوء إلى مثل هذا الإجراء، تتم في زمان ومكان محدد، من طرف سلطات مختصة بموجب القانون لكي تتم بمنائ عن أي مسؤولية قانونية، انّ اعتراض المراسلات مسألة خطيرة ولكنها في غاية الأهمية، فتقدير ضرورة اللجوء إليها أمرا صعبا لذلك وضع المشرع شروط ذلك،جريمة متلبس بها أو التحقيق الابتدائي

[1] jacques Ravanas, la protection contre la réalisation et la publication de leur image, Librairie générale de droit et jurisprudence, paris, 1978, p 202

[2] ياسر الأمير فاوروق،المرجع السابق،ص 527.

جرائم الانترنت، الجناية أو الجنحة لا يمكن لأي حال من الأحوال لوكيل الجمهورية أو قاضي التحقيق اللجوء إلى الأساليب الخاصة للتحري إلا في الجرائم التي حددها المشرع على سبيل الحصر والتي تم ذكرها سابقا.

أ–إذن من وكيل الجمهورية أو قاضي التحقيق: لا بد من إذن صادر من وكيل الجمهورية وتحت مراقبته المباشرة، اوإذن من قاضي التحقيق في حالة فتح تحقيق قضائي، وكذلك يكون تحت مراقبته المباشرة لقاض التحقيق.

ب–وجود دلائل قوية على ارتكاب الجنحة أو الجناية: لابد أن هذه الأساليب الخاصة ستكشف غموض الجريمة من الجرائم الخاصة وهو كشف الحقيقة[1]، والمهم أن الأساليب العادية لم تتمكن من كشف غموض الجريمة وجمع أدلتها الجزائية، اما عن مدة الإجراء الخاص، إن مدة أي إجراء من الإجراءات السالفة الذكر حدده المشرع الجزائري بأربعة أشهر وفق المادة(65 مكرر 7) من ق. إ. ج.ج وهي مدة قابلة للتجديد، دون ان يحدد المشرع عدد مرات التجديد

ج- مباشرة هذا الأسلوب من طرف ضابط الشرطة القضائية دون غيره :

لا يباشر هذا الأسلوب- أجراء اعتراض المراسلات والتقاط الصور وتسجيل الأصوات -إلاّ من طرف ضابط الشرطة القضائية دون غيره من رجال الضبطية القضائية و هذا الشرط يفهم من نص المادة (65 مكرر 08)ق.ا.ج.ج ".....أو ضابط الشرطة القضائية الذي أذن له ".

و كذا من نص المادة (65مكرر09) ق.ا.ج.جالتي تنصص على:" يحرر ضابط الشرطة القضائية المأذون له أو المناب محضرا عن كل عملية اعتراض ".

د–أن لا يتم اللجوء إليه إلّا في الجرائم المحددة حصراً:

في نص المادة (65مكرر05) دون غيرها من الجرائم مهما كانت خطورتها و يتعلق الأمر بجرائم المخدرات – الجريمة المنظمة العابرة للحدود الوطنية – الجرائم ، الماسة بأنظمة المعالجة الآلية

[1] درياد مليكة، المرجع السابق، ص149.

للمعطيات أي جرائم تكنولوجيات الإعلام والاتصال لان الجرائم الماسة بالمعالجة الآلية للمعطيات هي جزء من الجرائم تكنولوجيات الإعلام والاتصال، تبيض الأموال، الإرهاب، جرائم الصرف، وقد سبق التفصيل في ذلك[1].

أن ما يتحصل عليه بأسلوب التصنت من أدله صوتية أو يتم تسجيله بأي أسلوب آخر لا يعول عليه قانونا في إدانة الأشخاص والهيئات، و السبب يرجع في ذلك أن حكم الإدانة مبني على يقين الذي لا يقبل الشك؛ و ما يقلل من أهمية الأخذ بالتسجيل الصوتي أو التسجيل السمعي البصري الكثير من العقبات على راسها التطور التقني الكبير الذي أصبح يقلب الحقائق، من تقليد للأصوات وبرامج وتطبيقات تسهل عملية الحذف والتزييف والإخراج، هو ما انتشر في الهواتف الذكية، للأفراد، فما بال استعمالها من طرف السلطات المختصة خصوصا ممن تعسفوا في استعمال السلطة .

بالتالي ومن ناحية نظرية محضة، لا يعتد بالتسجيل سواء كان صوتي أو سمعي بصري في مسائل الإثبات و يبقى قرينة بسيطة أثناء مرحلة جمع الاستدلالات أو التحقيق لابد لها من دعائم للإثبات ، وبالتالي ومن ناحية نظرية كما سبق وذكرنا هي لاترقى إلى أدلة كاملة في جرائم الانترنت.

ثانيا:الشروط الشكلية لإجراء اعتراض المراسلات والتقاط الصور وتسجيل الأصوات.

يعتمد اللجوء لإجراء اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، على شروط شكلية منها الإذن المكتوب وضع الترتيبات اللازمة أي الترتيبات التقنية وفي الأخير تحرير المحضر.

أ-الحصول على إذن مكتوب :

قبل الحصول على الإذن في مثل اللجوء إلى هذه الإجراءات لابد أن يكون مصدره مختصا نوعيا وإقليميا ، في البحث والتحقيق في جرائم الانترنت، وفقا ما يحدد الاختصاص النوعي أي

[1] انظر هامش1 للمبحث الأول من الفصل الأول من الباب الثاني،ص176.

نوع الجريمة و الاختصاص الإقليمي والمتعلق بالضوابط الثلاث أي محل وقوع الجريمة أو القبض على المتهم أو محل إقامته[1].

قيدت المادة (65 مكرر5) في فقرتيها 5 و4 ق.ا.ج.ج ضباط الشرطة القضائية، قبل اللجوء إلى اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، الحصول على إذن مكتوب من وكيل الجمهورية المختص أو قاضي التحقيق تحت مراقبتهما المباشرة، و يجب أن يتضمن الإذن البيانات التالية:

1-ذكر العناصر التي تسمح بالتعرف على الأماكن المطلوب التقاط الصور فيها او تسجيل الأحاديث سكنية أو غيرها .

2-ذكر نوع الجريمة التي تبرر اللجوء إلى هذا الأسلوب الخاص في التحقيق.

3-تحديد المدة الزمنية في الإذن، التي لا يمكن أن تتجاوز (4)أشهر قابلة للتجديد ضمن نفس الشروط الشكلية و والموضوعية و ذلك بتحديد تاريخ بداية العملية و نهايتها، و الملاحظ أن المشرع الجزائري لم يتطرق إلى مسالة ضرورة إيداع نسخة من الإذن في ملف الإجراءات و لم يشترط أن تكون الإذن مسببا رغم أنّ التسبيب ضمانة لحماية الحياة الخاصة، والتي يجب على المشرع الجزائري تداركها بالتنصيص على أن يكون الإذن مسبب وهذا بتوضيح الأسباب والدوافع في إصدار الإذن، فذكر نوع الجريمة الخاصة لا يعد تسبيبا.

4- الجرائم التي تكشف عرضا: لم يلحق المشرع الجزائري الإجراء بالبطلان جراء الاكتشاف العرضي لأدلة جديدة، خلال اللجوء إلى الإجراء في الأعلى[2]،وفي الأخير فانه لابد من التنويه أنّ المشرع الجزائري، لم يستثني أي فرد من هذه الإجراءات ،حتى أولئك الذين يتمتعون بحصانة دبلوماسية أو نيابية أو غيرهم.

[1] عبد الله اوهايبة،قانون الاجراءات الجزائية الجزائري،التحري والتحقيق،دار هومة،2015، ص213-217.

[2] المادة(65مكرر2/6) من ق.ا.ج.ج"اذا اكتشفت جرائم أخرى غير تلك التي ورد في إذن القاضي، فان ذلك لا يكون سببا لبطلان الإجراءات العارضة"

ب- وضع الترتيبات التقنية[1] :

إنَّ عملية التسخير هذه تندرج في إطار وضع الترتيبات التقنية لكل إجراء بحسب ما يقتضيه من ترتيبات من الجانب الفني، وهي من الإجراءات التي تتطلب أهل للخبرة للقيام بها من تركيب للأجهزة[2]، ووضعها في أماكن مناسبة ومراقبة بثها، إلى غير ذلك من الإجراءات الفنية، دام أن هذا وأوكلت إلى أشخاص مختصين من غير ضباط الشرطة القضائية المكلفين بالإجراء وهذا لعدم تخصصهم التقني، هؤلاء الأشخاص-الخبراء التقنيين- هم من الأعوان المؤهلين في الهيئة، وهذا بنص المادة (41)من المرسوم سالف الذكر[3]، و توجب وضع الترتيبات التقنية الدخول إلى المحلات السكنية أو غيرها دون علم أو رضا أو أصحاب تلك الأماكن، إلا أن الملاحظ أن المشرع عندما تطرق إلى الدخول الأماكن الخاصة أو العمومية نص على أن القيام بالترتيبات التقنية تكون دون رضا و دون علم الأشخاص الذين لهم حق على تلك الأماكن وهو ما جاءت به المادة(65مكرر5) من قانون الإجراءات الجزائية[4].وعلى الضابط المكلف بهذه المهمة، الالتزام بكتمان

---

[1]أوكل المشرع الجزائري وضع الترتيبات التقنية بصفة حصرية للجرائم الخاصة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب نص المادة (41) الفقرة الأخيرة من المرسوم الرئاسي(15-261):" يتولى الأعوان المؤهلون في الهيئة ووحداتها المكلفة بالمراقبة، لصالح ضباط الشرطة القضائية، الجوانب التقنية للعمليات المنصوص عليها في قانون الإجراءات الجزائية".

[2] قنن المشرع الجزائري في المرسوم الجهات التي تستورد أو تقتني أو تحوز أو تستعمل الأجهزة الحساسة لمراقبة الاتصالات الالكترونية ، وهذا في محاولة منه للحد من استعمال هذه التقنيات الحديثة لمراقبة الأشخاص والتجسس عليهم وجعلها في يد الهيئة فقط مع إمكانية وعند الاقتضاء أن تقوم بذلك سلطة ضبط الاتصالات السلكية واللاسلكية والمؤسسة العمومية المكلفة بشبكات الاتصال .

[3] **المادة** (41)من المرسوم الرئاسي(15-261): "تمارس الهيئة الحصرية في مجال مراقبة الاتصالات الالكترونية تحت مراقبة قاض مختص، باستثناء الحالات المنصوص عليها في قانون الإجراءات الجزائية.

وزيادة على ذلك، وما عدا الحالات المبينة ي الفقرة السابقة، لا يمكن أن تستورد أو تقتني أو تحوز أو تستعمل الوسائل والتجهيزات التقنية لمراقبة الاتصالات الالكترونية إلا الهيئة، أو عند الاقتضاء، سلطة ضبط الاتصالات السلكية واللاسلكية وكذا المؤسسة العمومية المكلفة بشبكات الاتصالات، وذلك باستثناء أي هيئة أو مؤسسة أو شخص.يتولى الأعوان المؤهلون في الهيئة ووحداتها المكلفة بالمراقبة، لصالح ضباط الشرطة القضائية، الجوانب التقنية للعمليات المنصوص عليها في قانون الإجراءات الجزائية."

[4] المادة (65مكرر5) من ق.ا.ج.ج

السر المهني بنص المادة(1/11) من ق.ا.ج."والتي نصت" تكون إجراءات التحري والتحقيق سري، ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع".

ج- تحرير محاضر عن العملية ونسخ ووصف وترجمة التسجيلات:

إنّ تحرير المحاضر من المراحل المهمة التي لابد ان تحظى بالعناية اللازمة من طرف الضابط المكلف، وفق المادة (18) من ق.ا.ج. تحرير المحضر هو من المهام المنوطة بضابط الشرطة القضائية، يتضمن كل كبيرة وصغيرة فيما يخص المهام التي كلف بها وكذا الإجراءات التي قام بها والأدلة التي جمعها أو الاستنتاجات التي توصل إليها بعد تحليله للوقائع والقرائن ،لذلك يتضمن المحضر الإجراء الذي تم اللجوء إليه من طرف ضابط الشرطة القضائية المأذون له أو المناب و الجوانب التقنية من خلال تحديد الوسائل المستعملة والذي لا ينتظر نهاية مدة الإجراء لتحريره المحضر[1].

كما انه ينبغي على ضابط الشرطة القضائية وبموجب المادة(65مكرر)من ق.ا.ج. ان يرفق المحضر المرفق بملف الدعوى بترجمة للمراسلات والأصوات الأجنبية،خصوصا ان هذه الجرائم في الكثير من الأحيان أطرافها أشخاص أجنبية. و كذا وصف للصور،للحفاظ على الأدلة المتحصل عليها والرجوع إليها عند الضرورة. ولما لم يتطرق المشرع الجزائري يتطرق إلى القوة الثبوتية لهذه المحاضر المحررة عن طريق اللجوء إلى أساليب التحري الخاصة إذ جعلها خاضعة للقواعد العامة طبقا للمادة(212) ق.ا.ج .ج.

المطلب الثاني: التسرب.

من الإجراءات المثيرة للنقاش و الخاصة ببعض الجرائم هو إجراء التسرب؛ الذي أضافه المشرع الجزائري بموجب تعديل قانون الإجراءات الجزائية لسنة 2006. و الذي أحاطه بالعديد من الشروط الخاصة بالإجراء نفسه و بالشخص القائم به، هذا الإجراء هو ردّة فعل من المشرع على

[1] ركاب أمينة، المرجع السابق،ص83.

قصور و عجز الأساليب البحث و التحري العادية أن لم نقل التقليدية[1] ،باعتبار أنّ الأصل في إجراء التسرب[2] إجراء تقليدي أي سبق اللجوء إليه كما انه يختلف عن الإجراءات السابقة كونها إجراءات مادية أما التسرب فهو إجراء شخصي يتطلب أن يكون الضابط المتخفي حاضرا في مسرح الجريمة[3].

أدرجت عملية التسرب في المادة (65مكرر11)حتى(65 مكرر 18)من قانون الإجراءات الجزائية و يقصد به "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انّه فاعل معهم أو شريك أو خاف" [4] و يلاحظ أن المشرع الجزائري قد عرف التسرب، على غير العادة، والتي اصبحت-أي تعريف المصطلحات في نص قانوني- قواعد أرساها المشرع في ظل تطور التقنية، حيث يلجا إلى عملية التسرب في جرائم خاصة دون سواها و المتضمنة جرائم الانترنت[5]،ما يلاحظ أن المشرع الجزائري قد استعمل مصطلح التسرب في قانون الإجراءات الجزائية، ومصطلح الاختراق في قانون مكافحة الفساد[6].

---

[1] رشيدة بوكر،المرجع السابق،ص433.

[2] يختلف اجراء التسرب عن الارشاد الجنائي ويكون الإرشاد الجنائي صالحا وذو فائدة في عمليات الاختراق، حيث يتدخل المرشد بصفته احد المخترقين المبتدئين،الذين يجمعون المعلومات عن كيفيات الاختراق ومكان تواجد الثغرات الأمنية في النظام المعلوماتي،وحال الحصول على المعلومات،يتم المرشد من غير مأموري الضبط بتوصيلها إلى جهات الضبط المختصة ،أما إذا كان المرشد من مأموري الضبط القضائي فإنه يقوم باستدراجه حتى يتم التعرف عليه وبالتالي القبض عليه. انظر عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص838.

[3] Sylvain Métille ,Op ;Cit ,p152

[4] المادة(65 مكرر12) الفقرة 02 من قانون الإجراءات الجزائية .

[5] المادة 65 مكررمن ق.ا.ج.ج

[6] و ما يثبت أن المشرع الجزائري قصد نفس الإجراء بمصطلحين منفردين هو استخدام نفس المصطلح باللغة الفرنسية في النص باللغة الفرنسية (Infiltration)

و قد يوجه سؤال لماذا ندرس التسرب و هو من خلال تعريفه لا يتلاءم و طبيعة الدليل الجنائي الالكتروني الذي سبق وأن فصلنا فيه. و الواقع أن دراسة نظام التسرب لا بد منه لانه من إجراءات التحري الخاصة في جرائم تكنولوجيات الإعلام و الاتصال-باعتبار جرائم المعالجة الآلية للمعطيات هي من جرائم تكنولوجيات الإعلام والاتصال أي جرائم الانترنت-التي نص عليها المشرع صراحة في المادة(16)من قانون الإجراءات الجزائية الجزائري، كما انّه إجراء لا يخص العالم المادي فقط بل يمكن تفعيله في العالم الرقمي أو البيئة الافتراضية، كأن يقوم الضابط بالدخول إلى مواقع التواصل الاجتماعي والتي توفر خدمة الإبحار بأسماء وصفات وهمية أو مستعارة ومن خلال الاتصال بالمشتبه فيهم والاستفادة من كيفيات عملهم للاختراق وغيره من أساليب ارتكاب الجريمة. مما يدعم رأينا الداعي" إلى تفعيل وجود تكامل بين طرق و آليات جمع الدليل الالكتروني الجنائي (التحري و التحقيق الرقمي) و دعائم الإثبات الجنائي المتمثلة في طرق الإثبات العادية، التي تساهم بدورها في إسناد الفعل الإجرامي إلى المشتبه فيه و بالتالي إكمال إطار العملية الاثباتية في حلقة الخصومة الجنائية".

الأصل في إجراء التسرب، انّه إجراء منصوص عليه في المادة(56)من الاتفاقية التي صادقت عليها الجزائر و المتعلقة بمكافحة الفساد[1] ولكن هو إجراء خاص كذلك بجرائم الانترنت، ولأجل اللجوء إلى مثل هذا الإجراء لابد من توافر شروط شكلية وموضوعية نذكرها فيما يلي:

الفرع الأول: الشروط الموضوعية لإجراء التسرب.

للجوء لإجراء التسرب و نظرا لمساسه بحرية الأفراد، وهذا بعد اطمئنانهم لشخص المتسرب، فان المشرع الجزائري قد أحاطه بجملة من الشروط التي يجب توافرها لإضفاء طابع الشرعية على العملية. كما أحاطه كذلك بضمانات قانونية لتسهيل مهام القائمين به لبلوغ أهدافهم و هذا يظهر من خلال احترام الشروط المنصوص عليها في المادة(65مكرر15)من ق.ا.ج .ج.

[1] انظر المطلب الأول من هذا المبحث،ص177.

أولا : مباشرة التسرب من طرف أعوان الشرطة القضائية في إطار قانون الإجراءات الجزائية.

يناط ضباط الشرطة القضائية القيام بمجمل الإجراءات الجزائية المتعلقة بالبحث والتحري والتحقيق في جرائم الانترنت، وفق ما يقره القانون في مواده سواء تعلق الأمر بقانون الإجراءات الجزائية أو القوانين المكملة، هؤلاء هم ضباط الشرطة القضائية والموظفين و المكلفين ببعض مهام الضبط القضائي[1] .

أ-ضباط الشرطة القضائية: حددت المادة(15) من قانون الإجراءات الجزائية[2]،حيث يتمتع بصفة ضباط الشرطة القضائية الفئات التالية:

1-رؤساء المجالس الشعبية البلدية، وضباط الدرك الوطني والموظفون التابعون للأسلاك الخاصة للمراقبين ومحافظي وضباط الشرطة للأمن الوطني.

2-ضباط شرطة القضائية المعينين بقرار مشترك وتضم ضباط وضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك صادر عن وزير الدفاع الوطني وزير العدل على أنّ هؤلاء تنحصر مهامهم في الجرائم المتعلقة أو الماسة بأمن الدولة[3].

---

[1] ويختلف الضبط القضائي عن الضبط الإداري الذي هو مجموعة من القواعد التي يتم فرضها من الإدارة على الأفراد، من اجل تنظيم الحياة العامة للمواطنين، وهذا بمناسبة ممارستهم لأنشطتهم اليومية، من اجل الحفاظ على النظام العام والآداب العامة، بهدف الوقاية،الضبط الإداري هو ولاية السلطة التنفيذية لبسط النظام والمحافظة على السكينة العامة والصحة العامة والأمن العام، داود عبد الرزاق الباز، تدابير حماية الأمن العام بين الشريعة والقانون، المجلة العربية للدراسات الأمنية والتدريب، المجلد 18، العدد 35، 1424هـ، أكاديمية نايف للعلوم الأمنية، الرياض، المملكة العربية السعودية،ص66-69. في حين أن الضبط القضائي هو مجموعة العمليات والاختصاصات والإجراءات التي يقوم بها رجال الضبط القضائي بأجهزته الدرك الوطني والأمن الوطني او أي عون مخول له الضبط القضائي، للبحث والتحري عن الجريمة ومرتكبيها وجمع التحريات الخاصة بها، عبد الله اوهايبية ، المرجع السابق،ص77.

[2] المادة (15) من الأمر(15-02) المعدل والمتمم لقانون المتضمن قانون الإجراءات الجزائية.

[3] لقد تمّ حصر مهمة ضباط وضباط الصف التابعين للمصالح العسكرية في إطار مهمة الشرطة القضائية التي يمارسونها في نوع واحد من الجرائم وهي الجرائم الماسة بأمن الدولة، وفق نص المادة (15مكرر) ومضمونها:"تنحصر مهمة الشرطة القضائية لضباط وضباط الصف التابعين للمصالح العسكرية للأمن في الجرائم الماسة بأمن الدولة المنصوص والمعاقب عليها في قانون العقوبات.

3-الفئة التي تترشح للتمتع بصفة ضابط الشرطة القضائية، حيث تمنح لها صفة الضبطية بعد الموافقة من طرف لجنة خاصة، ويتم تعيينهم بناء على قرار مشترك من وزير العدل ووزير الدفاع بالنسبة لذوي الرتب في الدرك والدركيين الذين امضوا في سلك الدرك الوطني ثلاث سنوات على الأقل، إما من وزير العدل ووزير الداخلية والجماعات المحلية بالنسبة للموظيفين التابعين للأسلاك الخاصة للمفتشين وحفاظ وأعوان الشرطة التي تثبت لهم الاقدمية ثلاث سنوات على الأقل بهذه الصفة.

ب-أعوان الضبط القضائي:

حددت المادة أعوان الضبط القضائي في المادة (19)ق.ا.ج والذين يقتصر دورهم في معاونة ضباط الشرطة القضائية في مباشرة مهامهم ،و يثبتون الجرائم المقررة في قانون العقوبات ممتثلين في ذلك لأوامر رؤسائهم وخاضعين لنظام الهيئة التي ينتمون إليها ويقومون بجمع كافة المعلومات الكاشفة عن مرتكبي تلك الجرائم.

ثانيا:وقوع جريمة انترنت جناية أو جنحة.

حتى يؤسس وكيل الجمهورية أو قاضي التحقيق الإذن بالتسرب لابد من أن نكون بصدد جريمة من جرائم الانترنت التي حددناها سابقا، سواء كانت الانترنت في هي الوسيلة أو الهدف، وهذا استنادا إلى نص المادة(65مكرر11)ق.ا.ج.ج و المادة الثاني من القانون (09-04).

وهذا لحصر إجراء ينتهك الحق في الحياة الخاصة في أضيق الحدود فوقع جريمة انترنت أمر وارد وقد تكون من الجرائم المستمرة كالدخول والبقاء غير المشروع للمواقع أو الاعتداء على الحق في الحياة

تمارس هذه المهام تحت إدارة وكيل الجمهورية و إشراف النائب العام و رقابة غرفة الَتهام المختصة وفقا لاحكام المادة 207 من هذا القانون،قانون رقم (17-07) مؤرخ في 28 جمادى الثانية عام 1438 الموافق 27 مارس 2017، يعدل ويتمم قانون الاجراءات الجزائية،ج.ررقم20 ليوم29مارس2017،ص6." وهذه الجرائم من جرائم الانترنت التي نص عليها المشرع أنها مما يشرع فيها اللجوء إلى الإجراءات الخاصة بالمراقبة الالكترونية للاتصالات بموجب نص المادة 4من القانون (09-04)بقولها...أ-للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو المساسة بأمن الدولة".

الخاصة، والتي يتطلب بعض الوقت لتنفيدها، ومن هنا يأذن لضابط الشرطة القضائية المختص أن يتسرب إلى المواقع الالكترونية ومواقع التوصل الاجتماعي للقيام بهذه المهمة ومع تحقق باقي الشروط؛ ذلك أنّ هذا الإجراء لا يكون إلا بعد وجود دلائل قوية على ارتكاب جريمة الانترنت، والتي تؤيده ظروف معقولة لدى أعضاء الهيئة المختصة[1]، التي تؤدي إلى اتخاذ إجراءات ماسة بالحرية الفردية وهذا لضمان السير الحسن للعدالة [2].

ثالثا:ضرورة إجراء التسرب في إطار التحري أو التحقيق لجريمة من جرائم الانترنت.

إنّ اللجوء إلى إجراء التسرب في جرائم الانترنت، لابد أن يكون فقط في حالة التلبس والتحقيق الابتدائي أي بموجب المادة (65 مكرر11) من ق.ا.ج.ج، آي في التلبس[3] آو التحقيق الابتدائي[4]،والمشرع الجزائري حتى لا ينزع عن عملية التسرب الصيغة القانونية كإجراء من إجراءات التحقيق كلف قاضي التحقيق الإذن بها ومراقبتها، أما تنفيذها فيتم بمعرفة ضابط الشرطة القضائية في إطار الإنابة القضائية، الذي هو حق مكفول لقاضي التحقيق لتنفيذ مثل هذه العمليات[5].

لذلك فان اللجوء إلى التسرب غير مرتبط بالإجراءات والسير في الدعوى العمومية بقدر ارتباطه بجريمة الانترنت نفسها، باعتباره ضرورة يجب اللجوء إليه في ظل عجز الإجراءات العادية أو غير المثمنة كالتفتيش عن بعد ،في كشف خبايا وإسرار جريمة من جرائم الانترنت.

---

[1] لأعضاء الهيئة الوطنية مهام من بينها ماذكرته المادة (11)من المرسوم الرئاسي رقم(15-261)يقولها"...تزويد السلطات القضائية وصالح الشرطة القضائية، تلقائيا أو بناء على طلبها، بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال"

[2] خالد ممدوح ابراهيم،فن التحقيق الجنائي في جرائم الالكترونية،ط1، دار الفكر الجامعي،مصر، 2009، ص219.

[3] المادة (41) ق.اج.ج :"توصف الجناية او الجنحة بانها في حالة تلبس اذا كانت مرتكبة في الحال او عقب ارتكابها.

كما تعتبر الجناية او الجنحة متلبسا بها اذا كان الشخص المشتبه في ارتكابه إياها في وقت قريب جدا من وقت وقوع الجريمة قد تبعه العامة بالصياح أو وجدت في حيازته أشياء أو وجدت أثار أو دلائل تدعو إلى افتراض مساهمته في الجناية او الجنحة.

وتتسم بصفة التلبس كل جناية او جنحة وقعت ولو في غير الظروف المنصوص عليها في الفقرتين السابقتين اذا كانت قد ارتكبت في منزل وكشف صاحب المنزل عنها عقب وقوعها وبادر في الحال باستدعاء احد ضباط الشرطة القضائية لاثباتها"

[4] المادة (63)من ق.اج.ج" يقوم ضباط الشرطة القضائية ، وتحت رقابتهم أعوان الشرطة القضائية، بالتحقيقات الابتدائية بمجرد علمهم بوقوع الجريمة إما بناءا على تعليمات وكيل الجمهورية و إما من تلقاء أنفسهم

[5] فوزي عمارة،المرجع السابق،ص247.

فضرورة التحقيق في معناها الضيق تعد من الشروط الأساسية للجوء إلى هذا الإجراء، لان التسرب أجيز لعلة معينة ولغرض خاص وبصفة استثنائية فتخلف تلك العلة يمنع قاضي التحقيق من الإذن به وإلا عد متعسفا، أو معنى أخر أن التسرب الذي لا يلتمس من حصوله فائدة لإظهار الحقيقة يعد تسربا تحكميا[1]،كباقي الإجراءات لابد لإجراء التسرب أن يتوافر على شروط شكلية، لضمان مشروعية اللجوء اليه.

الفرع الثاني: الشروط الشكلية لإجراء التسرب في جرائم الانترنت.

يلاحظ انه ومن خلال نص المادة (65مكرر5) من قانون الإجراءات الجزائية أن المشرع الجزائري، لم يأمر قاضي التحقيق بل أذن له باللجوء إلى إجراء من الإجراءات الخاصة؛ وربما حتى لا يتمكن وكيل الجمهورية من أن يستأنف الأمر، لأنّه لا يمكن أن يستأنف الإذن، وهذا بموجب المادة(170) من قانون الإجراءات الجزائية[2]، لان الأمر يتعلق هنا بالسرية التي يجب أن تحيط بهذا النوع من الإجراءات كي لا نكشف حين اللجوء إليها، الإجراء والشخص المكلف للقيام به[3].

أولا:الحصول على إذن .

الاذن هو محرر رسمي صادر من جهة مختصة متمثلة إما في وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، حسب الأحوال، مُسلم إلى جهة مختصة متمثلة في ضباط الشرطة القضائية، فلا يمكن بأي حال من الأحوال مباشرة عملية التسرب و الكشف عن الجرائم المنصوص عليها قانونا و المذكورة في المادة(65مكرر05)، إلا بعد الحصول على إذن من وكيل الجمهورية المختص إقليما أو قاضي التحقيق بعد إخطار و كيل الجمهورية و يجب أن يتضمن الإذن بإجراء التسرب تحت طائلة جزاء البطلان الشروط والأوضاع القانونية وعليه يجب أن يكون الإذن مسبب ومكتوب حيث يتعين أن يكون الإذن الصادر من طرف و كيل الجمهورية أو قاضي

[1] فوزي عمارة،المرجع السابق،ص 247.

[2] المادة(1/170) من ق.ا.ج.ج"لوكيل الجمهورية الحق في أن يستأنف امام غرفة الاتهام جميع أوامر قاضي التحقيق"

[3] فوزي عمارة،المرجع السابق،ص242.

التحقيق متضمنا للأسباب الداعية لاتخاذه كأن تفشل الإجراءات العادية من تتبع الجناة وجمع الأدلة فلا تكون ذات جدوى.على أن تكون هذه الأسباب مبنية على استدلالات جدية يتخذ منها أسباب لإجراء عملية التسرب ويخضع تقدير جدية التحريات إلى وكيل الجمهورية أو القاضي التحقيق وهذا لتحقيق القيمة المرجوة من الإجراء وهي الوصول إلى الحقيقة[1] .

إذ أن كتابة او التدويـــــن في إطار الإجراءات الجزائية خيـر وسيلة لإثبات حصول الإجـراء و الظروف الذي أدت إلى اتخاذه و الآثار المترتبة عليه عليه[2] فالأصل في العمل الإجرائي الكتابة [3].

بالإضافة أن يذكر في الإذن الجريمة-جريمة الانترنت- التـــي تبرر اللجوء إلى هذا الأسلوب،وهي الجرائم المحددة على سبيل الحصر في المادة(65مكرر 5) من ق.ا.ج.ج و التي سبق ذكرها[4] ، مع ذكر الضابط الذي تتم عملية التسرب تحت مسؤوليته و يشرف على تنفيذها (الاسم - اللقب –الرتبة – المصلحة) اي ذكر هويته كاملة للضابط أو العون المكلف،

ثانيا : تحديد المدة المطلوبة لعملية التسرب في جرائم الانترنت.

طبقا لنص المادة(65 مكرر 15) يجب أن لا تتجاوز هذه المدة 04 أشهر، و يتم تمديدها طبقا لمقتضيات التحري أو التحقيق و بنفس الشروط الشكلية و الموضوعية، و ذلك بتحديد دقيق لتاريخ بداية التسرب و نهايته نظرا لما يقتضيه هذين التاريخين من أهمية بالنظر إلى صحة لإجراءات و ينتهي التسرب بنفس الأوضاع و الشكليات المقررة لمباشرته و ذلك بموجب أمر صادر من وكيل الجمهورية أو قاضي التحقيق حتى قبل انتهاء المدة المحددة في الإذن بالتسرب مع مراعاة الاستثناء

[1] مليكة درياد،المرجع السابق،ص155.

[2] رتبت المشرع الجزائري على تخلف الكتابة في الإذن البطلان على عكس الإخطار الذي يكون عادة شفويا .

[3] بوكر رشيدة ، المرجع السابق، ص435.

[4] مليكة درياد،المرجع السابق،ص.156

الذي أو ردته المادة(65 مكرر17) الذي يقتضي إمكانية تجديد الإذن بالتسرب لمدة 04 أشهر أخرى إذا لم يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه [1].

وحرصا من المشرع على حماية الأعوان المختصين والمأذون لهم في عملية التسرب، فان المشرع اوجب عدم إظهار هوية العون المتسرب، في كل مراحل الإجراء لأي سبب كان،لما في ذلك لكشف في عملية التسرب وتفويت الفرصة في القبض على المتهم وبالتالي تعريض العضو إلى الخطر،حيث يترتب على ذلك عقوبات تتراوح بين الحبس من سنتين(2) إلى خمس (5)سنوات وبغرامة من(50.000) دج إلى (200.000)دج[2].

إذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب أو جرح على الأشخاص المتسربين أو أبناءهم أو أصولهم المباشرين فتكون العقوبة الحبس من 5سنوات إلى عشر سنوات وبغرامة من(200.000) دج إلى (1.000.000)دج[3].وتمتد الحماية إلى فترة المحاكمةكذلك، والذي يسمع كشاهد[4] وتمتد هذه الحماية حتى أثناء فترة المحاكمة .

ثالثا: تحرير المحضر الخاص بإجراء التسرب.

إن نص المادتين(65 مكرر 9 ومكرر10) يشيران إلى أن ضابط الشرطة القضائية يقوم بوصف أو نسخ التسجيلات على محضر،حيث يتولى ضابط الشرطة القضائية فضلا عن حفظ الدليل أو الدعامة المتعلقة بالتسجيل و ختمها مع وضع شريط التسجيل ضمن حرز مغلق لوضعها بين يدي القضاء، هذا فيما يخص اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، وبالقياس عليها اذ لم يورد المشرع تحرير المحضر في المواد المتعلقة بالتسرب الا انه من البديهي ان يقوم ضابط الشرطة القضائية بتحرير محضر عن مهمته ، وقد ذكر المشرع ذلك ان يتم هذا في شكل تقرير ، وهو ما نصت عليه المادة (65مكرر13) من ق.أ.ج.ج"يحرر ضابط الشرطة

[1] رشيدة بوكر، المرجع السابق، ص436.

[2] المادة(ة65مكرر2/16).ق.ا.ج.ج.

[3] المادة(65مكرر4/16).ق.ا.ج.ج.

[4] المادة65(مكرر18).ق.ا.ج.ج.

القضائية المكلف بتنسيق عملية التسرب تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر امن الضابط أو العون المتسرب وكذا الأشخاص المسخرين طبقا للمادة (65مكرر14) ادناه."

على انّه وبعد أنْ تعرفنا على إجراءات الإثبات في قانون الإجراءات الجزائية، نمر إلى دراسة الإجراءات الخاصة بجرائم الانترنت فقط وهي الإجراءات الواردة في إطار القانون (09-04)، مع التذكير أنّ بعض الجرائم الخاصة كالجرائم الإرهابية هي من جرائم الانترنت، لان المشرع أورد في التعديل الأخير استعمال وسائل تكنولوجيات الإعلام والاتصال في مثل هذه الجرائم، واللجوء إلى المراقبة الالكترونية للاتصال كإجراء وقائي منها .

المبحث الثاني:التحقيق في إطار القانون (09-04)

لم تعد إجراءات التحري والتحقيق العادي في مجال الإثبات الجنائي قادرة على فك لغز السلوكيات الإجرامية، وهذا بعد أن تفوق المجرمون على العديد من الأساليب الوقائية في مواجهة مكافحة الجريمة، لذلك استدعى واقع الحال أن تعتمد السلطات المختصة أساليب جديدة تواكب التغيرات الحاصلة ، خصوصا ما تعلق بتكنولوجيات الحديثة للإعلام والاتصال،فجرائم الانترنت هي جرائم ذات طابع دولي كما سبق لنا أن أوضحنا، وإذ قرر المجتمع الدولي أن يكافح هذه الجرائم وبالتحديد الاتحاد الأوربي عن طريق اتفاقية بودابست2001،هذه الاتفاقية التي صادقت عليها دول خارج الاتحاد الأوربي- الولايات المتحدة الأمريكية واليابان وإفريقيا الجنوبية-، أصبحت نموذجا يقتدى به لسن القوانين الوطنية في مجال مكافحة جرائم الانترنت وان لم يُصادق عليها.

المطلب الأول: المراقبة الالكترونية للاتصالات في التشريع الجزائري.

الاتصالات سمة عصر السرعة فلا يكاد يخلوا بيت من وسيلة لهذه الاتصالات سواء ثابتة أو محمولة، ولكن لكل تقدم إيجابيات وسلبيات فكما توفر هذه الأخيرة الوصول إلى مصدر المعلومة بسرعة فائقة ودون أي جهد يذكر وبأقل التكاليف، فهي لم تسلم من استغلالها لأغراض إجرامية، خصوصا لسرعة توفرها وحجبها عن الرقابة كونها إشارات (لغة 1-0) ، يصعب على الشخص العادي أن يفهم فحواها، على غرار المحادثات الهاتفية، مما دعى المشرع إلى مراقبة هذه الأخيرة أي الاتصالات ،حيث تلعب مراقبة الاتصالات دورا لا يستهان به في كشف جرائم الانترنت ليس ذلك فحسب بل حتى في مكافحة الجريمة ، فبعد أن اتجه المشرع إلى اتخاذ التطور التكنولوجي وسيلة للمساعدة في كشف وتحري الجرائم، دعت لها الضرورة الملحة إلى اعتراض المراسلات المتعلقة بالمحتوى أما يصطلح عليه بمراقبة الاتصالات الالكترونية في القانون(09-04)[1].

[1] القانون(09-04) المؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد 47 الصادرة في 16 أوت 2009.

على الرغم من أن الإجراء هذا في أصله إجراء استثنائي إلا أنه من أخطر الإجراءات التي سنها المشرع الجزائري لحد الآن، لارتباطها بحق أصيل يحميه الدستور الحق في الحياة الخاصة، الذي يعد أحد الحقوق الأساسية التي أثارت جدلا واسعا على مر الزمان، ولعله الذي ينظر فيه وفي حمايتة كل مره في ظل التطور التقني الرهيب الذي عرى الحق من مضمونه.

والأصل أن المشرع الجزائري كغيره من المشرعين أفرد للحق في الحياة الخاصة، أو الحق في الخصوصية حماية دستورية جسدتها مختلف المواد الواردة فيه على غرار قانون العقوبات ، إلا أنه قد يكون إجراء مراقبة الاتصالات الالكترونية الحل الفعال لمثل الجرائم الخاصة، نظرا لخطوتها وسهولة ارتكابها، وتهديدها الصارخ للمجتمع، وفي المقابل جعل إجراء المراقبة استثناء للإجراءات الجزائية وضمن نطاق ضيق في إجراء التحري والتحقيق، وأمام معادلة حق الدولة في ملاحقة المجرم ومعاقبته وحق الفرد في حياة خاصة وضع المشرع الجزائري ضمانات لحماية هذا الحق كدرع واقي لحماية الحقوق والحريات الفردية.

من كل مما سبق ما هو أساس مراقبة الاتصالات الالكترونية(الفرع الأول)وما هي شروط اللجوء اليها(الفرع الثاني).

الفرع الأول: الأساس مراقبة الاتصالات الالكترونية

إن تطور أساليب ارتكاب الجريمة وسرعة انتشارها عرض الحق في الخصوصية للانتهاك تدريجيا، إن لم يكن من طرف المجرم فهو من السلطات المختصة ولكن ما يشفع في هذه الحالة أنها تدخل ضمن الأفعال المبررة التي وجدت من أجل إحداث توازن بين مصلحة المجتمع والفرد، فأساس مراقبة الاتصالات عبر الانترنت هو سلوك إجرامي يعري الحق في الخصوصية من كل معاينة، لكن بالمقابل كإجراء كان لا بد منه من أجل مواجهة جرائم محددة وردت في التشريع الجزائري تتسم ببعدها الدولي وفي أحيان كثيرة بخسائرها الكبيرة وتنظيمها المحكم.

أولا:حظر مراقبة الاتصالات الالكترونية

حمى المشرع الجزائري الحق في الحياة الخاصة باعتبارها من الحقوق اللصيقة بالشخصية، والأكثر عرضة للانتهاك، في الدستور وكذا القوانين الأخرى سواء تعلق الأمر بالقوانين الموضوعية أو الإجرائية.

أ–في الدستور الجزائري.

شأنه شأن معظم الحقوق حظي الحق في الخصوصية بحماية دستورية، وهذا راجع لأهميته، وقد يكون الحق في حرية الاتصال جزء من هذا الحق، والحق في الخصوصية هو أحد الحقوق اللصيقة التي تثبت للإنسان، والتي عادة يصعب حصر الجوانب المختلفة لها فاعتنى الدستور الجزائري بذلك في مختلف مواده كالمادة (46) منه، التي تنص مايلي" لا يجوز انتهاك حُرمة حياة المواطن الخاصّة، وحرمة شرفه، ويحميهما القانون.سرّية المراسلات والاتّصالات الخاصّة بكلّ أشكالها مضمونة لايجوز ياي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية.ويعاقب القانون على انتهاك هذا الحكم.حماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق اساسي يضمنه القانون ويعاقب على انتهاكه[1]."

وغيرها من المواد الدستورية [2].فالملاحظ ان الدستور وضع حماية شاملة لجميع المراسلات والاتصالات بأي شكل سواء كانت تقليدية أو تقنية،وكما جرت عليه العادة ترك للفقه أمر

[1] المادة (46)من القانون(16-01) يتضمن التعديل الدستوري المؤرخ في 26 جمادى الأولى عام 1437الموافق6 مارس2016،ج ر رقم 14 المؤرخة في 07 مارس2016.ص

[2] المادة 40 : تضمن الدولة عدم انتهاك حُرمة الإنسان.
ويُحظَر أي عنف بدني أو معنوي أو أي مساس بالكرامة.
المعاملة القاسية واللاانسانية أو المهينة يقمعها القانون.
المادة 41 : يعاقب القانون على المخالفات المرتكَبة ضد الحقوق والحريات، وعلى كل ما يمس سلامة الإنسان البدنية والمعنوية.
المادة 42 : لا مساس بحُرمة حرية المعتقد، وحُرمة حرية الرأي.
حرية ممارسة العبادة مضمونة في ظل احترام القانون.

تعريف الحق محل الحماية،حيث يمكن تعريف الحق في الحياة الخاصة بأنه حق احترام سرية وخصوصية الأشخاص من أي تدخل مادي أو معنوي [1].

ب–في القانون الجزائي الجزائري

مند صدور قانون العقوبات سنة 1966، جسد القانون حماية غير مباشرة من خلال حماية الحقوق اللصيقة بالشخصية كضمان عدم إفشاء السر المهني المادة (301) والحق في سرية المراسلات المادة (303) ثم عمل على تجريم سلوكيات إجرامية، كجنحة انتهاك المعطيات المعالجة أليا،وللذكر فان أول جنحة إفشاء معلومات المتعلقة بالحياة الخاصة، نصت عليها المادة (27)[2]من القانون رقم(04-19)المتعلق بتنصيب العمال ومراقبة التشغيل[3]،تم المواد 303 مكرر[4] تحت عنوان الاعتداء على شرف واعتبار الأشخاص من القانون(06-23) المتضمن تعديل قانون العقوبات[5].

المادة 44 : حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن.

حقوق المؤلف يحميها القانون.

لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي.

الحريات الاكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون.

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

المادة 47 : تضمن الدولة عدم انتهاك حُرمة المسكن.

فلا تفتيش إلا بمقتضى القانون، وفي إطار احترامه.

ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة.

المادة48:حريات التعبير ،وإنشاء الجمعيات ،والاجتماع،مضمونة للمواطن.

المادة 157 : تحمي السلطة القضائية المجتمع والحريات، وتضمن للجميع ولكل واحد المحافظة على حقوقهم الأساسية.

[1] عبد الله فكري،المرجع السابق،ص613.

[2] المادة 27 "يعرض افشاء المعلومات الشخصية التي تمس بالحياة الخاصة لطالب التشغيل مرتكبه لغرامة من 50000 دج الى 100000 دج"

[3] قانون رقم 04-19 المؤرخ في 13 دو القعدة عام 1425 الموافق 25 ديسمبر 2004 يتعلق بتنصيب العمال و مراقبة التشغيل الجريدة الرسمية 26 ديسمبر 2004.

[4] نصت المادة 303 مكرر على انه " يعاقب بالحبس من 6 أشهر إلى ثلاث سنوات وبغرامة من 50,000 إلى 300,000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأي تقنية كانت وذلك :

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

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

[5] القانون رقم (06-23)المؤرخ في 29ذو القعدة عام 1427 الموافق ل 20 ديسمبر سنة 2006 المعدل و المتمم للأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 المتضمن قانون العقوبات

لدى فالمشرع الجزائري من قراءتنا لمختلف النصوص القانونية قد أقر حماية للحياة الخاصة من مختلف الاعتداءات على الحقوق اللصيقة بالشخصية من بينها حرية الاتصال ،وما يترتب عنها من اطلاع على معلومات لم يُرد الفرد أن يطلع عليها الآخرون ايا كانت مكانتهم،فما بال اعتراضها وتسجيلها واستخدام محتواها وهو الهدف الذي تقوم على أساسه مراقبة الاتصالات الالكترونية.

ثانيا:تعريف مراقبة الاتصالات الالكترونية

تتمثل المراقبة في كشف الجرائم قبل وقوعها وتلعب دورا لا يستهان به في الكشف عن جرائم الانترنت وليس ذلك وحسب بل في عملية مكافحة الجريمة،المراقبة هي وسيلة هامة من وسائل الإرشاد الجنائي والتي يقوم بها المرشد أو مأمور الضبط القضائي سواء بنفسه أو من يفوضه في ذلك من مرشدين سريين لا يكشفون عن هويتهم أو المهام الموكلة إليهم بقصد البحث عن الجرائم ومرتكبيها[1] .

أ-إجراء مراقبة الاتصالات الالكترونية

يقصد به المراقبة الأمنية التي محلها الاتصالات الالكترونية التي عرفها المشرع الجزائري في إطار القانون (09-04) وهي أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية[2]،وإدراكا منه أي المشرع الجزائري لاختلاف مسرح الجريمة العادي عن مسرح الجريمة الافتراضي واللامتناهي، أفرد إجراء خاص بالاتصالات الالكترونية لمراقبتها سواء وقاية من الجرائم أو كإجراء قضائي يدخل ضمن

[1] بن يونس عمر محمد ، الجرائم الناشئة عن إستخدام الأنترنت ،المرجع السابق،ص840

[2] المادة (02) من القانون (09-04)يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 14 غشت عام 1430 الموافق 05غشت سنة 2009- الجريدة الرسمية عدد 47 ل 16غشت 2009 ص 05.

Art2 « f -Communications électroniques : toute transmission, émission ou réception de signes, de signaux, d'.écrits, d'images, de sons ou de renseignements de toute nature, par tout moyen électronique.» Loi n° 09-04

اختصاصات ضابط الشرطة القضائية ،فعملية المراقبة الأمنية الالكترونية، هي عمل أمني أساسي لنظام معلومات إلكتروني، يقوم فيه المراقب بكسر القاف بمراقبة المراقب(بفتح القاف)بواسطة الأجهزة الالكترونية وعبر شبكة الانترنت لتحقيق غرض محدد[1].

وقد استعمل المشرع الجزائري مصطلح مراقبة الاتصالات الالكترونية، بالرغم أن معظم أحكام قانون(09-04) هي مستمدة من اتفاقية بوداست والتي استخدمت مصطلح اعتراض[2] معطيات المحتوى، والأصل أن مصطلح الاعتراض نظمه المشرع الجزائري بنص المادة (65 مكرر) من قانون الإجراءات الجزائري الذي يخص الاتصالات السلكية واللاسلكية والمراقبة الاتصالات الالكترونية خاص بالجرائم التي ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية أي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

ب- محل مراقبة الاتصالات الالكترونية.

إن محل المراقبة هو ذلك الهدف الذي تتم مراقبته وتتبع تحركاته وتصرفاته ،في نطاق المراقبة الالكترونية محل المراقبة هو الحاسوب الرقمي أو الموقع عبر شبكة الانترنت أو البريد الالكتروني بما يحويه من مراسلات الكترونية وحلقات نقاش وغرفة دردشة وقد يكون محلها الهاتف النقال المتصل بشبكة الانترنت[3] وحتى ساعة اليد الذكية او اللوح الرقمي،اذن محل المراقبة يشمل الاتصالات الالكترونية الخاصة والتي عرفتها المادة الثانية من القانون(09-04) [4]، قد ميز المشرع بين نوعين من المعطيات المعالجة المراقبة ،النوع الأول ،المراقبة المتعلقة بحركة السير معطيات المرور[5] ،اما النوع

---

[1] مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت- دراسة مقارنة- دار الكتب القانونية – المجلة الكبرى مصر، ص192

[2] ورد مصطلح الاعتراض أو Interception في المادة 21 من اتفاقية بودابست http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm

[3] سامح احمد البلتاجي موسى،المرجع السابق،ص 111.

[4] المادة الثانية من القانون (09-04)

[5] Art2 « e -Données relatives au trafic : toute donnée ayant trait à une communication passant par un système informatique, produite par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ainsi que le type de service. » Loi n° 09-04

الثاني ،المعطيات المتعلقة بمحتوى الاتصال،فبالنسبة للنوع الأول عرفت المادة (02) من القانون (09-04)،أما النوع الثاني،والمتعلق بالمحتوى فلم يرد تعريف لذلك، ولو انه بمفهوم المخالفة هي كل المعطيات المعالجة باستثناء ما تعلق بمعطيات المرور،فمعطيات المحتوى هي محل المراقبة الالكترونية ذلك بان أدرجها المشرع في المادة الرابعة من القانون(09-04)، أما معطيات المرور فقد خصها المشرع بإجراء حفظ المعطيات المتعلقة بحركة السير المادة (11) من القانون (09-04).

مع الإشارة إلى أنّ المحل المراقب في هذا النوع من الجرائم لا يدل على المستخدم العادي والذي لا يعتبر بأي حال من الأحوال شخص الجاني، حيث لا يمكن حصر الجريمة في شخص معين لكون الجريمة بدأت من الحاسوب تحديدا، أو الهاتف الذكي أو اللوح الرقمي أو أي جهاز متصل بالإنترنت، بما يعني أنّ مرتكب الجريمة يظل في إطار الاحتمالات التي يحتاج إلى دعم مادي لتأييد نسبة الجريمة إليه، فقد جعل هذا الأمر فكرة مصطلح المستخدم ترجع إلى الحاسوب، وليس للفرد العامل عليه[1].

[1] سامح احمد البلتاجي موسى،المرجع السابق ،ص 112

الفرع الثاني:ضمانات مراقبة الاتصالات الالكترونية في التشريع الجزائري.

اتخاذ إجراء المراقبة كنوع من الوقاية أو حتى كإجراء قضائي فيه الكثير من الجرأة التي جعلت مراقبة الاتصالات تحت المجهر بحثا عن مدى كفاية شروطها كضمان لحفظ الحقوق والحريات ،وأمام التوجه نحو رقمنة الاتصالات تصبح المراقبة الالكترونية أهم إجراء وقائي وقضائي باعتبارها شاملة لجميع أنواع الاتصالات.

أولا: شــروط مـراقبة الاتصالات الالكترونية في التشريع الجزائري .

لكي يتم مراقبة الاتصالات الالكترونية على الوجه الصحيح لابد أن يلتزم ضابط الشرطة القضائية المختص والمكلف بهذا الإجراء ،الذي لابد أن يكون من ذوي الكفاءة والخبرة في استخدام التكنولوجيات الحديثة للاتصال وهذا بعد تأهيله لأعلى مستوى من الدراية التقنية، بشروط المراقبة التي تعتبر ضمانات في مقابل كفالة حماية الحق في الحياة الخاصة، لذلك فالمادة تجيز التدخل في نطاق الحياة الخاصة للأفراد ولكن بشروط معينة.

أ–الشروط العامة.

تتمثل في جدية الأسباب أي الجدية الكافية وهذا بغض النظر عن النتيجة التي التوصل إليها أي نتيجة سلبية والايجابية ،التقيد بالكشف عن النشاط الإجرامي وهذا بتحديد الهدف من مراقبة الاتصالات والمتمثل في الوقاية من الجرائم أو الكشف عنها، وهذا ما جسدته المادة الثالثة من القانون السالف الذكر، بالإضافة الى التقيد بالغرض المرجو من المراقبة، حيث انه قبل اللجوء إلى المراقبة لابد من وجود دلائل على إمكانية وجود الجريمة أو وجودها بالفعل على أن تكون هناك وقائع فعلا منسوبة إلى مشتبه فيه و أخيرا،مشروعية الوسيلة،فاستخدام البرمجيات[1] اللازمة لعملية

[1]–برمجيات تعقب المجرمين وهي برمجيات تعتمد على البيانات المخزنة والتي يتم الرجوع إليها عند الحاجة من اجل مقارنة معطيات المرسلة،

المراقبة لابد أن تكون أصيلة أي ليست مستنسخة عن البرامج الأصلية لكي يكون للدليل قيمة أصيلة في الإثبات الجنائي،والجدير بالذكر ان مراقبة الاتصالات الالكترونية كانت في الأصل إجراء وقائي لحماية الشبكات ،وبالتالي أساسها برمجيات المراقبة المستعملة من طرف مجرمي الشبكة العالمية ،والتي تستخدمها المصالح المختصة في الضبط من اجل مراقبة الاتصالات على الشبكة.

ب–الشروط الخاصة.

تتمثل هذه الشروط الخاصة فيما يلي:

1– الإذن المكتوب، اذ لا يجوز إجراء المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة وهو الشرط المشترك بين جميع الجرائم التي يمكن اللجوء فيها لإجراء المراقبة كأسلوب وقائي إذا تعلق الأمر بالوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة ،أو كإجراء قضائي إذا تعلق الأمر الاعتداء على منظومة معلوماتية تهدد النظام او الدفاع الوطني ،أو مؤسسات الدولة أو الاقتصاد الوطني، أو لمقتضيات التحريات والتحقيقات القضائية التي لا يمكن

ا_طريقة ماندريك لمراقبة المجرمين:عبارة عن دائرة تلفونية مغلقة مكونة من عدة كاميرات خفية تقوم بارسال الصور الى جهاز الحاسوب الرقمي الذي يقوم بمقارنتها مع البيانات التي تحوي صور المجرمين المسجلين واصحاب السوابق العدلية.

ب_ برنامج كارنيفور ا و 1000dsc وهي التسمية التي أطلقت على هذه البرمجية بعد إحداث الحادي عشر من سبتمبر بالولايات المتحدة الامريكية ،تسمح برصد المعلومات الواردة الى والصادرة عن البريد الالكتروني و او رصد حركة البيانات من والى عنوان معين على الشبكة ،حيث انه لا يقوم بتغيير البيانات بل التصنت عليها وتسجيل نسخة منها .

مع العلم آن هناك برامج أخرى التي تعمل على تجميع اكبر عدد من المعلومات والبيانات الشخصية على شبكة الانترنت ،حيث تقوم برامج المراقبة الالكترونية بكسر الحواجز على شبكات الكمبيوتر والدخول إلى الوثائق الحكومية والتجارية في جميع أنحاء المعمورة.

ج_ برمجيات مراقبة البريد الكتروني:تتمثل في التجسس على البريد الالكتروني ،برنامج email spy monitorيقوم بمراقبة كل ما يتم طباعته على لوحة المفاتيح ويعمل البرنامج خفية دون علم من يستخدم الحاسوب او اللوح الرقمي او حتى الهاتف النقال خصوصا مع وجود خدمة الجيل الثالث للاتصالات و العديد من البرامج شم الرزم networks pachet sniffersو برنامج blaster-e وهو برنامج لمراقبة ضربات لوحة المفاتيح والعديد العديد من البرمجيات.لمزيد من التوضيح انظر ، سامح احمد البلتاجي موسى، المرجع السابق ،ص117و118.

المتابعة فيها إلا عبر اللجوء إلى المراقبة الالكترونية أو في إطار تنفيذ طلبات المساعدة القضائية الدولية[1].

2–مدة الاجراء، الشرط الثاني هو تحديد المدة المتعلقة بالجرائم المتعلقة بالإرهاب والتخريب والماسة بأمن الدولة بستة أشهر قابلة للتجديد وهو الشرط الذي استثنى باقي حالات مراقبة الاتصالات الالكترونية،كما جعل المشرع النائب العام لدى مجلس قضاء الجزائر مختصا بمنح ضباط الشرطة القضائية المنتمون للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته ،الإذن لإجراء مراقبة الاتصالات[2].

المطلب الثاني:التفتيش و الحجز في جرائم الانترنت في التشريع الجزائري.

يهدف التفتيش إلى البحث عن الأدلة التي تفيد في كشف الحقيقة، وهو من بين الإجراءات التي ثمنها المشرع الجزائري من خلال القانون (09-04)(الفرع الأول)، أما الضبط أو الحجز كما أطلق عليه المشرع في إطار القانون (09-04) إجراء جديد خاص بالمعطيات والذي يتناسب مع طبيعة اللامادية واللامحسوسة لجرائم الانترنت (الفرع الثاني).

الفرع الأول:التفتيش في جرائم الانترنت في التشريع الجزائري.

التفتيش هو البحث في مستودع السر عن أشياء تفيد في الكشف عن جريمة وقعت ونسبتها إلى مرتكبيها [3]،وهو " إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص ، وذلك بهدف إثبات إرتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة " وعرفه البعض الآخر بأنه " البحث

[1] حالات اللجوء الى مراقبة الاتصالات الالكترونية الواردة في المادة (04) من القانون (09-04)

[2] انظر المادة(04)و المادة(13) من القانون(09-04).

[3] مأمون سلامة ،قانون الإجراءات الجنائية معلقا عليه بالفقه وإحكام القضاء ،مكتبة رجال القضاء ،1980،ص 244.

عن الأشياء المتعلقة بالجريمة لضبطها وضبط كل ما يفيد في كشف حقيقتها ويجب أن يكون للتفتيش سند من القانون " [1] .

من خلال هذه التعريفات يتضح بأن التفتيش ينطبق على الجرائم التي تترك آثار مادية وبالتالي فلا توجد مشكلات تعيق إجراؤه لأن من خلاله سيتم البحث عن الأدلة المادية الملموسة ، من هنا ذهب جانب من الفقه إلى القول بأنه إذا كانت الجريمة واقعة على المكونات المادية للنظام المعلوماتي، فلا عائق يحول دون تطبيق القواعد التقليدية للتفتيش، أما إذا كانت الجريمة واقعة على البرمجيات والتطبيقات وبيانات النظام المعلوماتي وشبكاته ، فإن الصعوبات تبرز، والتي تستلزم أن يقع التفتيش على المكونات المادية والمعنوية للنظام المعلوماتي والشبكات، لضبط أدلتها وبالتالي إدانة مرتكبها، فإن المشرع الجزائري قد ساير تطور هذه الجريمة المستحدثة وذلك عندما نص على إجراءات التفتيش التي تتناسب وطبيعتها وذلك في القانون رقم (09-04) السالف الذكر [2] ،من كل ما سبق ما هو نطاق التفتيش في جرائم الانترنت،(اولا) والشروط الواجب توافرها(ثانيا).

أولا: نطاق تفتيش مكونات النظام ألمعلوماتي في جرائم الانترنت.

يتكون النظام ألمعلوماتي من مكونات مادية وغير مادية أي معنوية، بالإضافة إلى الشبكات المحلية والإقليمية والدولية التي تكون محل للتفتيش من اجل الحصول عل الدليل الجنائي الالكتروني[3] وهو المعلومات المخزنة في الأجهزة الحاسوب ولواحقها وغيرها من الوسائل التقنية الأخرى وكذا

[1] خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، الطبعة الأولى ، دار الفكر الجامعي ، الإسكندرية ،مصر، 2009 ، ص. 182 .

[2] فايز محمد راجح غلاب ، المرجع السابق، ص307 .

[3] المادة من(16) القانون (09-04)

شبكات الاتصال والتي يتم تجميعها باستخدام برامج وتطبيقات وتكنولوجيات خاصة بهدف إثبات وقوع الجريمة ونسبتها الى مرتكبيها[1].

أ – تفتيش مكونات النظام المعلوماتي المادية والمعنوية

يتكون النظام المعلوماتي من مكونات مادية وغير مادية أي معنوية ، فبالنسبة للنوع الأول من هذه المكونات يمكن القول بأنها جميع المكونات المادية الملموسة ، اللازمة لعمله وإشتغاله بوجه يحقق وظيفته ويؤدي الغرض المطلوب منه ، ومن حيث الأصل يؤدي نظام المعالجة الآلية ثلاثة عمليات رئيسية هي الإدخال ، المعالجة والتخزين ، والإخراج ، وتبعا لهذه العمليات تنقسم أجزاء نظام المعالجة الآلية إلى ثلاث أقسام رئيسية[2]، أما بالنسبة للنوع الثاني من مكونات النظام المعلوماتي أو نظام المعالجة الآلية ، فهي تلك المكونات الغير المادية أو كما يصطلح على تسميتها بالبرامج أو البرمجيات أو الكيان المنطقي والتي تعرف على أنها مجموعة البرامج والأساليب والقواعد وعند الإقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات وبهذا يشمل الكيان المنطقي على جميع العناصر الغير المادية اللازمة لتشغيل الكيان المادي[3]،والواقع ان تفتيش النوع الأول من المكونات المادية لنظام المعلوماتي لا يثير أي مشكلات تعيق القيام به ، مثلها مثل أي مكونات

[1] عائشة بن قارة مصطفى، المرجع السابق، ص61

[2] لقد تم تعريف هذه المكونات في الفصل الاول من الباب الاول ولكن لاباس باعادة التذكير بها وهي وحدات الإدخال : وهي مجموعة الوحدات المسؤولة عن إيصال البيانات للحاسوب فتقوم بإستقبال البيانات المدخلة إلى الحاسوب وتمريرها داخل الجهاز إلى وحدة الذاكرة للتخزين ، ومن أجهزة الإدخال لوحة المفاتيح ، الفأرة ، مشغل الأقراص .

وحدة المعالجة المركزية : وتعتبر بمثابة العقل المفكر والمسيطر على باقي الوحدات المكونة لنظام المعالجة الآلية بحيث تعمل هذه الوحدة على تنفيذ جميع العمليات الخاصة بالتشغيل وعمليات المقارنة المنطقية والعمليات الحسابية الموجودة في البرنامج تنفيذه من وإلى الوحدات المساعدة مع ضمان تحرك المعلومات من وإلى الذاكرة الرئيسية ، ومن أهم مكونات هذه الوحدة الذاكرة ووحدة الحساب والمنطق ووحدة التحكم .

وحدة الإخراج : وهي الوسائط المستخدمة لإظهار نتائج التشغيل ومعالجة البيانات ومن أهم هذه الوسائل الشاشة والطابعة.انظر رشيدة بوكر ،المرجع السابق، ص. 58

[3] جبار الحسناوي ، المرجع السابق، ص. 25 .

مادية أخرى يتم تفتيشها بالطرق العادية وبموجب النصوص الإجرائية العادية ، بخلاف النوع الثاني الذي يثير تفتيشه مشكلات نظرا لطبيعتها المنطقية وكذلك طبيعة إجراءات التفتيش التي هي من نفس الطبيعة المعنوية [1] ، لكن هذا لا يمنع أن أسباب ومتطلبات التفتيش ودوافعه هي واحدة سواء تعلق الامر بالمكونات المادية او المعنوية ، وهي كشف الحقيقة وضبط الأدلة[2]

1 – تفتيش مكونات النظام المعلوماتي المادية .

ليس هناك خلاف حول تفتيش المكونات المادية للنظام المعلوماتي بحثا عن شيء يتصل بجريمة وقعت ، يفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش،بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات ، هل هو من الأماكن العامة أو من الأماكن الخاصة ؟ حيث أن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش ، فإذا كانت موجودة في مكان خاص كمسكن المتهم وأحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات والإجراءات المقررة قانونا،أما لو وجد شخص يحمل مكونات الكمبيوتر المادية أو كان مسيطرا عليها أو حائز لها في مكان ما من الأماكن العامة سواء كانت بطبيعتها أو كانت عامة بالتخصيص فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال [3].

فالتشريع الإجرائي الجزائري ، يتضمن نصوص قانونية تنطبق من حيث الأصل على تفتيش المكونات المادية للنظام المعلوماتي بهدف كشف الجريمة وتجميع الأدلة ، وبناءً على ما سبق فإن تفتيش المكونات المادية للمنظومة المعلوماتية مثل لوحة المفاتيح أو الفأرة أو الشاشة وغيرها من

[1] فايز محمد راجح غلاب ، المرجع السابق ، ص. 307 .

[2] -Myriam QUEMENER et Joel FERRY, Cybercriminalité, Défi mondial et réponses, Ed ECONOMICA, PARIS, 2007, P 238.

[3] خالد ممدوح إبراهيم ، فت التحقيق الجنائي، المرجع السابق ، ص. 195 و 196 .

الأشياء المادية الملموسة وكذلك البصمات الموجودة عليها لا تدخل ضمن المشاكل الإجرائية التي تعيق إجراء التفتيش إذ بالإمكان تطبيق النصوص العادية وبهذا فإن أجهزة الكمبيوتر التي يراد تفتيشها تخضع للقواعد التي تخضع لها الأدوات المادية الأخرى ، فإن كانت في مسكن فإنه ينطبق عليها ما ينطبق على تفتيش المساكن والتي من بينها مراعاة وقت التفتيش والإذن بالتفتيش والأشخاص القائمين على التفتيش والأشخاص المطلوب حضورهم ومراعاة الاختصاص المكاني[1]،ومن النصوص القانونية التي يمكن تطبيقها في هذا المجال نص المادة (64) ق إ ج ج والمواد (37)و (40) و(42)ومن المواد (44) إلى(47)ق إ ج ج[2] .

2 – تفتيش مكونات النظام ألمعلوماتي المعنوية .

قد يرد التفتيش على المكونات النظام ألمعلوماتي المتمثل في المعلومات المعالجة أليا ، ولعل الصورة المعتادة والمثال العملي الذي يمكن تقريره هو فحص البرمجيات الذي يعد من الوسائل الرئيسية في الكشف عن أكثر جرائم الاعتداء على نظم المعالجة الآلية [3]، مثل الدخول الغير المشروع إلى نظم الغير ، فوجود برمجيات غير مصنفة تعمل في بيئة الاختراق أو تساعد عليه كما هو الشأن في برمجيات المسح للكشف عن الأبواب المفتوحة يمكن أن يشكل منطقة إستفهام ودلالة كافية أيضا على إرتكاب الشخص لجريمة الدخول الغير المشروع لنظام المعالجة الآلية إذا إستتبع ذلك إعترافا[4] شفويا بإرتكاب الجريمة ،ومن هنا فإن التفتيش في مكونات النظام المعلوماتي المعنوية ، يشكل إحدى أهم المشاكل التي تعيق إجراءات التحقيق ، حيث أثارت هذه الصورة

[1] فايز محمد راجح غلاب ، المرجع السابق ، ص. 309 .

[2] المـادة(64) والمواد من 44 إلى 47 من القانون رقم(06 –22) المؤرخ في 20 ديسمبر 2006 ، يعـدل ويتمم الأمـر رقم 66 – 155 ج ر،العدد 84 ، الصادرة في 24 ديسمبر 2006 ، ص. 16.

[3] رشيدة بوكر ، المرجع السابق ، ص. 397

[4] الاعتراف وشهادة الشهود والخبرة هي من دعائم الإثبات الجنائي في جرائم تكنولوجيات الإعلام والاتصال.

خلافا كبيرا في الفقه المقارن لأن هذا النوع من التفتيش ينصب على بيانات وبرامج النظام المعلوماتي التي تغيب فيها الطبيعة المادية فليس لها أي أثر مادي محسوس في العالم الخارجي [1] .

فذهب رأي إلى جواز ضبط البيانات الإلكترونية بمختلف أشكالها ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط " أي شيء "، فإن ذلك يجب تفسيره بحيث يشمل بيانات المعالجة اليا [2].

بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير ملموسة ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أحكام خاصة تكون أكثر ملائمة لهذه المعلومات اللامحسوسة [3] .

وهذا ما تبناه المشرع الجزائري حيث أنه واستجابة لهذه التغيرات أجاز تفتيش المعطيات المعلوماتية وذلك بموجب المادة(05) من القانون رقم(09-04) السالف الذكر ، حيث أجازت هذه المادة للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة (4) من نفس القانون، التي من بينها توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الاقتصاد الوطني وللوقاية من الجرائم الماسة بأمن الدولة، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلوماتية [4].

ب – تفتيش المنظومة المعلوماتية عن بعد في جرائم الانترنت.

[1] فايز محمد راجح غلاب ، المرجع السابق نفسه ، ص. 311 .

[2] انظر في ذلك عائشة بن قارة مصطفى،المرجع السابق،ص91.

[3] خالد ممدوح إبراهيم ، فن التحقيق في الجرائم الإلكترونية ، المرجع السابق ، ص. 197 .

[4] رشيدة بوكر ، المرجع السابق ، ص. 348 ، 349

بالإضافة إلى كون تفتيش النظام المعلوماتي تعد من الإشكاليات التي تعيق سير التحقيق فإن تفتيش شبكات النظام المعلوماتي تثير مشكلة قد تكون أشد خطورة من تفتيش النظام المعلوماتي ذاته حينما يكون مرتبط بشبكة إتصال،وتثار هذه المشكلة عندما يتعلق الأمربنهاية طرفية موجودة في منزل المتهم ومتصلة بجهاز يقع خارج منزل المتهم في نفس الدولة ومملوك لغير المتهم ، كما تثار الإشكالية بصورة أكبر عندما يكون النظام المراد تفتيشه واقعا خارج الدولة وتعد شبكة الإنترنت هي الشبكة الأهم التي تشكل عائقا في مجال التفتيش الجنائي من بين الشبكات المختلفة بسبب الانتشار الواسع لها والعدد الهائل من البشر الذين يستخدمونها والخدمات التي تقدمها في مجال الحياة المختلفة والكم الهائل من البيانات والمواقع التي تتضمنها [1] ، لذلك فان التفتيش في نطاق جرائم الانترنت لا يخرج عن احدى الفرضيتن

1- حالة جهاز متصل بجهاز المتهم داخل الدولة.

تتمثل المشكلة في هذه الحالة عندما تقوم سلطة التحقيق بتفتيش جهاز متصل بجهاز المتهم ويقع داخل الدولة وكذا تجاوز الإختصاص المكاني لسلطة التحقيق من ناحية والإعتداء على خصوصيات الغير من ناحية أخرى .

ونظرا لوجود قصور في نصوص قانون الإجراءات الجزائية بعد تعديل الأخير لسنة 2006، حيث لم يتضمن التفتيش عن بعد للكيانات المنطقية في نظام المعالجة الآلية للبيانات[2]، تم مواجهة ذلك القصور بأن سُمح للسلطات القضائية المختصة لمقتضيات التحريات والتحقيقات القضائية تمديد التفتيش عن المعطيات المبحوث عنها بسرعة إلى أي منظومة معلوماتية أو جزء منها تقع داخل الإقليم الوطني ،وهذا ما نصت عليه الفقرة الثانية من المادة (05)من القـانون رقم (09-04)السالف الذكر، وما يدخل ضمن نطاق حالة الاستعجال في تمديد الاختصاص خوفا من

[1] فايز محمد راجح غلاب ، المرجع السابق ، ص. 312 .

[2] فايز محمد راجح غلاب ، المرجع السابق ، ص. 314 .

العبث بالأدلة الرقمية، والمنصوص عليه في المادة (19) من الاتفاقية الأوروبية للإجرام السيبيري المستقى منها القانون (09-04) .

2 – حالة جهاز متصل بجهاز المتهم خارج الدولة.

في هذه الحالة فإن الإشكالية تثار بصورة أكبر، في حالة أن يكون الجهاز المطلوب تفتيشه والمتصل بجهاز المتهم بنهاية طرفية يقع خارج الدولة، ففي الغالب يعّمد مرتكبي جرائم الانترنت إلى تخزين البيانات الخاصة بهم والتي تعد أدلة لإدانتهم في جرائم تم ارتكابها من قبلهم خارج الدولة اي قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة ،عن طريق شبكة الاتصالات البعدية بهدف عرقلة التحقيقات[1].

التفتيش عن بعد أصبح مشكلة تواجه النظام الإجرائي ككل، حيث يتم إجراؤه من خلال الحاسوب ذاته وتزداد خطورة الأمر حينما يتم استخدام برامج تمتلكها دول معينة متقدمة في مجال التكنولوجيا الرقمية، للتفتيش على أنظمة دول أخرى، لكونه لا يستند إلى مبرر قانوني ويشكل اعتداء على الخصوصية، فضلا عن كونه يجعل الدولة عرضة للاعتداء في إطار جريمة التجسس عليها أي المساس بأمن الدولة.

بالنسبة للقانون الجزائري فقد تلافى مشكلة التفتيش عن بعد خارج الإقليم الوطني بموجب الفقرة الثالثة من المادة (5) من القانون رقم(09– 04) السالف الذكر التي نصت على أنه " إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى ، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل "، فبخصوص هذه الفقرة قيل بأنّه لا يمكن تفتيش تلك المنظومة وإنما يجب الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل ، فبالرغم من

[1] فايز محمد راجح غلاب ، المرجع السابق ، ص. 314 .

إمكانية تفتيشها من الناحية التقنية داخل النطاق الإقليمي؛ إلا أن ذلك لا يتم إلا بعد موافقة الطرف الأجنبي لأنّه أمر متعلق بسيادة الدول على أراضيها وهذا يؤكد على أهمية التعاون الدولي في نطاق مكافحة جرائم الانترنت والذي جسده المشرع الجزائري من خلال المادة (21) من القانون (09-04)،وبالعودة إلى الاتفاقية الأوربية الموقعة في بودابست وبالضبط في المادة (32) منها أجازت الولوج بغرض التفتيش والضبط في أجهزة موجودة خارج الحدود الإقليمية لدولة أخرى بدون إذن في حالة ان تكون البيانات متاحة للجمهور، او حالة الرضا بالتفتيش من حائز البيانات ايّا كان سواء المستخدم العادي أو مقدمي الخدمة.[1]وهو أمر فيه نظر ونسجل في صدده تحفظ شديد لما فيه من اعتداء على سيادة الدولة قبل الاعتداء على خصوصيات الأفراد.

وحتى لا يصبح إجراء التفتيش تحت طائلة البطلان،لابد من أن يستوفي مجموعة من الشروط الموضوعية والشكلية التي تعتبر ضمانات حماية الحق في الحياة الخاصة[2] .

ثانيا : شروط التفتيش في جرائم الانترنت.

يتضح مما سبق ان جرائم الانترنت يمكن أن تخضع لإجراء التفتيش طبقا للقواعد العادية أو المستحدثة، هذا الإجراء الذي وجد أثناء مباشرته أنه يتضمن تقييد للحرية الفردية واعتداء على حرمة الحياة الخاصة[3]، لهذا نجد أن القوانين الإجرائية قد حرصت على إحاطة إجراء التفتيش بشروط وضمانات أساسية وهدف ذلك تحقيق الموازنة بين مصلحة المجتمع في عقاب المتهم[4]، وبين

[1] يرجى الرجوع الى المبحث الثاني من الفصل الثاني من الباب الأول،ص118.

[2] حيث يمكن تعريف الحق في الحياة الخاصة بأنه حق احترام سرية وخصوصية الأشخاص من أي تدخل مادي أو معنوي ،انظر في ذلك عبد الله فكري،المرجع السابق،ص613

[3] رشيدة بوكر ، المرجع السابق ، ص. 405 .

[4] المتهم فهو الشخص الذي حركت ضده الدعوى العمومية قصد معاقبته عن الجريمة المرتكبة المنسوبة اليه، وذلك بوصفه اما فاعلا او شريكا او متدخلا او محرضا في اي مرحلة من مراحل الدعوى مادام لم يصبح الحكم عليه نهائيا ،محمد محدة، ضمانات المتهم اثناء التحقيق، الجزء الثالث،ص18، اما المشتبه به هو الشخص الذي بدأت ضده التحريات لقيام قرائن تدل على ارتكابه الجريمة او مشاركته فيها ولم تحرك الدعوى العمومية ضده بعد. محمد محدة، ضمانات المشتبه فيه، دار الهدى،عين مليلة، الجزائر،الجزء الثاني،1992،ص52.

حقوق الأفراد وحرياتهم ، ومن الشروط والضمانات التي يجب توافرها منها ما هو موضوعي ومنها ما هو شكلي .

أ – الشروط الموضوعية للتفتيش في جرائم الانترنت.

تتمثل الشروط الموضوعية التي يلزم تحققها لإجراء التفتيش في سبب التفتيش الذي يتمثل في وقوع الجريمة ، ونسبة إرتكابها إلى متهم إضافة إلى ضرورة أن ينصب التفتيش على محل يحتمل العثور فيه على أدلة الجريمة وأخيرا يفترض لكي يكون التفتيش صحيحا أن يكون له غاية تتمثل في أن يكون التفتيش بغرض العثور على الآثار والأشياء التي يمكن أن تفيد في كشف الجريمة .

1 – وجود سبب لتفتيش النظام المعلوماتي .

الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة واقعة بالفعل ، وترجحت نسبتها إلى متهم معين ، وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية[1]، وذلك عملا بقاعدة المشروعية " لا جريمة إلا بنص " وبالتالي لا يجوز التفتيش من أجل فعل لا يشكل جريمة وفي حالة عدم توافر الدلائل الكافية بإقترافها ونسبتها إلى شخص أو أشخاص ، فسبب التفتيش بحثا عن أدلة الجريمة يعد ضمانة بالنسبة للجرائم المنصوص عليها في القوانين إذ بدون السّبب المتمثل في الجريمة،سواء كانت جناية او جنحة دون المخالفة، وبدون توجيه الإتهام لشخص أو أشخاص محددين فإن القيام بالتفتيش يعد إجراءً باطلا ، ولا يكفي لقيام سبب التفتيش ، وقوع جريمة منصوص عليها في القانون كجرائم الانترنت التي تناولها المشرع الجزائري بنصوص قانونية تضفي وصف التجريم على الأفعال المكونة لها ، بل لا بد من توافر أمارات قوية على وجود أشياء تفيد في كشف هذه الجريمة ، عند وجود اجهزة ومعدات معلوماتية ويمكن ان تعد قرائن وإمارات قوية تدل على أنها استعملت في

[1] خالد ممدوح إبراهيم ،المرجع السابق ، ص. 209 .

ارتكاب الجريمة المعلوماتية[1]، وبالتالي توجيه الاتهام الى شخص معين أو عدة أشخاص بارتكاب جريمة من جرائم الانترنت أو الاشتراك فيها.

2- المحل و الغاية من التفتيش .

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سّره والسّر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة [2] ، ومحل التفتيش قد يكون منزلا وقد يكون شخصا وقد يكون محله رسائل[3].

هذا ومحل التفتيش في إطار جرائم الانترنت هو نظام المعالجة بكل مكوناته المادية والمعنوية ،وشبكات الإتصال كما سبق بيانه وفي هذا المجال لا داعي لتكرار مدى قابلية هذه المكونات المادية والمعنوية فضلا عن شبكات الاتصال للتفتيش،كما انه ونظرا لخطورة إجراء التفتيش على الحياة الخاصة للأفراد بإعتباره إجراء من إجراءات التحقيق فلا بد أن يكون له غاية إذ بدونها ، وكذلك في حالة تجاوزها فإن الإجراء سيكون باطلا وبهذا الخصوص نصت المادة (81)ق.إ.ج.ج على أن يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة ، وفي تكنولوجيات الإعلام والاتصال بصفة عامة نجد أن المشرع الجزائري وبخصوص الغرض من التفتيش قد أحال تفصيل ذلك إلى قواعد قانون الإجراءات الجزائية حيث نص على أنه : " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة الرابعة أعلاه ، الدخول بغرض التفتيش ولو عن بعد إلى :

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

[1] فهد عبد الله عبيد العازمي، المرجع السابق ،ص321

[2] رشيدة بوكر ، المرجع السابق ، ص. 408 .

[3] فايز محمد راجح غلاب ، المرجع السابق نفسه ، ص. 321 .

– منظومة تخزين معلوماتية. " [1] .

وبالتالي فإنه إذا تحققت الغاية من التفتيش وفقا لنصوص قانون الإجراءات الجزائية فيحق للسلطات المختصة بالتحقيق الدخول إلى النظام المعلوماتي أو جزء منه سواء تعلق الأمر بالمستخدم أو مزود خدمة الانترنت سواء لتوصيل الخدمة او تقديم خدمة الايواء، بغرض التفتيش على ذلك النظام أو المعطيات المخزنة به، كما يجوز الدخول إلى نظام معلوماتي آخر داخل الإقليم الوطني أيضا بغرض التفتيش إذا ما تحققت الغاية منه وذلك في حالة وجود أسباب تدعو للاعتقاد بأنّ المعطيات محل البحث مخزنة في ذلك النظام [2] .

3– السلطات المختصة في التفتيش في جرائم الانترنت.

هذا وقد كلفت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حصريا بالقيام بإجراءات التفتيش داخل منظومة معلوماتية تحت سلطة قاضي مختص وهذا وفق المادة(21)من المرسوم الرئاسي رقم (15-261)[3]، على أن هذا الإجراء أي التفتيش وإجراء مراقبة الاتصالات الالكترونية هي مهام منوطة بهذه الهيئة لاغير، وهذا في إطار الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة، تحت طائلة العقوبات بالنسبة للمساس بالحياة الخاصة للغير، وهو مانصت عليه المادة 04 من القانون(09-04) سالف الذكر،كما يمكن القضاة وضباط الشرطة القضائية التابعون للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم انه يحوز واو يستعمل وسائل وتجهيزات موجة لمراقبة الاتصالات الالكترونية وهذا وفق المادة 30 من المرسوم السالف الذكر.

[1] المادة(05) من القانون (09– 04) السالف الذكر

[2] فايز محمد راجح غلاب ، المرجع السابق ، ص. 327 .

[3] مرسوم الرئاسي رقم (15-261) مؤرخ في 24ذي الحجة عام 1436 الموافق 8 اكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ج ر 53 ص 21.

ب – الشروط الشكلية للتفتيش في جرائم الانترنت.

بالإضافة إلى الشروط الموضوعية للتفتيش، توجد شروط أخرى ذات طابع شكلي يجب مراعاتها عند ممارسة هذا الإجراء وذلك صونا للحريات الفردية من التعسف أو الإنحراف في إستخدام السلطة[1].

1 – وقت التفتيش.

تذهب أغلب التشريعات الجزائية إلى تحديد وقت معين يتم فيه إجراء التفتيش ، وذلك حرصا منها على تضيق نطاق الإعتداء على الحرية الفردية وحرمة المسكن، حيث ذهب المشرع الجزائري ، إلى حظر تفتيش المنازل وما في حكمها في وقت معين فنجد ميقات التفتيش في التشريع الجزائري قد حدد من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا وذلك من خلال المادة (47) ق .إ .ج .ج، وبذلك نجد أن هذه النصوص قد هدفت إلى حماية حرمة الأفراد ليلا، حيث يعد المسكن ملجأ حصين لهم، لا يجوز انتهاكه ليلا حفاظا على خصوصياتهم .

ومع أن إشتراط تفتيش المنازل بوقت معين يعد ضمانة للمحافظة على خصوصيات الآخرين ، فإن ذلك الشرط لا يؤخذ به على إطلاقه ، حيث ورد العديد من الاستثناءات على تلك القاعدة تضمنت الخروج على الميقات الزمني في التفتيش بالنسبة لبعض الجرائم وكذلك في بعض الحالات مثل حالة الضرورة ، من ذلك وفي نطاق التفتيش المتعلق بجرائم الانترنت، فإن الإستثناء الوارد بالمادة (3/47) ق إ ج والمتعلق بجواز إجراء ضابط الشرطة القضائية التفتيش في كل ساعة من ساعات الليل أو النهار عندما يتعلق التحقيق بنوع معين من الجرائم ، والتي شملت الجرائم المعلوماتية، ذلك أن تطبيق القيد السابق على هذا النوع من الجرائم ، قد يكون سببا في

[1] خالد ممدوح إبراهيم ، فن التحقيق في الجرائم الالكترونية، المرجع السابق ، ص. 220 .

إخفاء الأدلة ومن ثمت عرقلة سير التحقيق لكون أدلة هذه الجرائم هي عبارة عن كيانات غير مادية يمكن إخفاء أدلتها بسرعة غير متوقعة،إذا علم الجاني مسبقا بالوقت الذي سيتم تفتيش أنظمته فيه [1] .

2- الأشخاص المطلوب حضورهم للتفتيش .

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم العادية وذلك لضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط [2]، حيث يعتبر-حضور أشخاص للتفتيش- من القواعد الأساسية التي يترتب على مخالفتها البطلان وقد نص المشرع الجزائري على هذا الضمان في المادة (45) و (83)ق. إ. ج.ج

وبالرغم من أهمية مثل هذه الضمانات التي تهدف إلى عدم التعسف في استخدامها،إلا أنها قد تتحول إلى مشكلات تحول دون الوصول إلى النتائج المتوقعة من إجراء التفتيش في حالة أن يكون التفتيش يخص إحدى جرائم الانترنت، بسبب أن إشعار الأشخاص المطلوب حضورهم قد يتيح لهم التلاعب بالمعطيات والبرامج والتطبيقات المراد تفتيشها ، وبالتالي إخفاء أدلة الجرائم أو التلاعب بها ومن ثم صعوبة التوصل إلى مرتكبها ، فقد يتم التلاعب بالأدلة وإخفاءها عن بعد في الوقت ما بين إجراءات إصدار الإذن بالتفتيش وموافقة المتهم بأن يتم التفتيش بحضوره ، وعليه فقد تنبه المشرع الجزائري لمثل هذا الإجراء فلم يشترط في تفتيش عدد من الجرائم حضور المتهم أو صاحب المنزل المراد تفتيشه أو الشهود ومن تلك الجرائم ، الجرائم الماسة بأنظمة المعالجة الآلية،وجرائم المرتبطة بتكنولوجيات الإعلام والاتصال [3] .

[1] فايز محمد راجح غلاب، المرجع السابق ، ص. 329 – 330 .
[2] رشيدة بوكر ، المرجع السابق، ص. 413
[3] فايز محمد راجح غلاب ، المرجع السابق ،ص. 337 .

3- محضر التفتيش.

باعتبار التفتيش عملا من أعمال التحقيق فإنه ينبغي تحرير محضر به يثبت فيه كل ما تم من إجراءات، وما أسفر عنه التفتيش من أدلة، ولم يتطلب القانون شكلا خاصا لهذا المحضر ، مما ينبغي أنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر وفق قانون الإجراءات الجزائية، كأن يكون مكتوبا باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره ، وأن يحوي في طياته كافة الإجراءات التي أتخذها بشأن الوقائع التي بينها ، حيث نصت المادة (68/ 2)ق.إ.ج .ج " وتحرر نسخة من هذه الإجراءات وكذلك جميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل " ، كما نصت المادة(79)ق.إ.ج.ج على أنّه " ... ويستعين قاضي التحقيق دائما بكاتب ويحرر محضرا بما يقوم به من إجراءات "

بالإضافة إلى ما سبق ذكره من إحاطة قاضي التحقيق أو عضو النيابة العامة بتقنية المعلومات ، ومن جهة أخرى لا بد أن يرافقه شخصا متخصصا في المعلوماتية للاستعانة به في المسائل الفنية الضرورية ، فوجود خبير سوف يساعد في صياغة مسوّدة محضر التحقيق بحيث يتم تغطية كل الجوانب الفنية في عملية التفتيش [1].

إن الحديث عن التفتيش في جرائم الانترنت، لا يكتمل إلا بالتعرض لإجراء الضبط أو حجز المعطيات المعلوماتية أي اثر التفتيش، باعتباره الوسيلة التي من خلالها يتم الوصول إلى الأدلة التي تثبت الحقيقة التي تبحث عنها الدعوى الجزائية، رغم انّه يؤخذ على مثل هذا الإجراء انه ومن ناحية مالية يخلق عبئا اقتصاديا بالنسبة للشركات الناشطة في مجال التجارة الالكترونية ،وعملائها عندما يجدون أنفسهم ممنوعين من الولوج إلى قواعد البيانات التي تجمع بين المعطيات المباحة والمجرمة[2].

[1] خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق ، ص. 225 .

[2] هلالي عبد الاه احمد،الجوانب الموضوعية والإجرائية لجرائم المعلوماتية،المرجع السابق، ص242.

مما لاشك فيه أن النتيجة التي ينتهي إليها التفتيش هي الضبط أو حجز المعطيات المعلوماتية كما نص عليه المشرع الجزائري في المادة(06) من القانون(09-04)[1]، ويختلف الضبط أو الحجز في جرائم الانترنت عن باقي الجرائم الأخرى كون أن محله المنظومة المعلوماتية والشبكات، أي أشياء ذات طبيعة لامحسوسة أي معنوية لامادية .

الفرع الثاني:الضبط في جرائم الانترنت في إطار القانون (09-04).

لمّاً اقر المشرع الجزائري تفتيش المنظومة المعلوماتية كما سبق و أن فصلنا؛ فبالضرورة كان لابد له أن يقر ضبط الأشياء المستخلصة من تفتيش البيئة الافتراضية، بما يناسبها وهو الحجز بأنواعه، وهذا بحسب ما يتناسب والبيئة التي يتواجد فيها الدليل الجنائي الالكتروني، أي إما عن طريق النسخ على دعامة تخزين أو عن طريق منع الوصول إلى المعطيات[2]، وضبط أو حجز المعلومات هنا هو كل ما تعلق بإجراءات التحقيق المذكورة سابقا أي المراقبة الالكترونية للاتصالات والتفتيش عن بعد أي أن الضبط هنا يعد من إجراءات التحقيق، حيث أن الضبط يعد في الأصل من إجراءات الاستدلال؛ إلا إذا تم بناءا على تفتيش فيعد من إجراءات التحقيق كما هو الحال عليه في هذه الحال[3].و"هو الحصول على أشياء ذات صلة بجريمة وقعت ويفيد في كشف حقيقتها

[1] المادة 06 الفقرة الأولى من القانون 09-04 "عندما تكتشف السلطة تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وانه ليس من الضروري حجز كل المنظومة ،يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في احراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

المادة06 الفقرة الثانية والثالثة من القانون 09-04"يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية""غير انه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق ،شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات"

[2] المادة (07)من القانون(09-04)"إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6اعلاه،لأسباب تقنية ،يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية ،أو إلى نسخها ،الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة"

[3] عفيفي كامل عفيفي،المرجع السابق، ،ص480.

وحقيقة نسبتها إلى المتهمين"[1] أو هو استخدام البرامج الهامة من أجل الولوج للبيانات المراد ضبطها الى جانب وضع اليد على تلك الدعائم المادية"[2].

والواقع انه لا يمكننا المرور مباشرة إلى أنواع الحجز المعلوماتي وشروط القيام به؛ دون أن نذكر الصعوبات التي تواجه المحقق أثناء عملية الضبط فهذه العملية تواجهها الكثير من الصعوبات تتعلق بالدليل نفسه او المعلومات المعالجة المحجوزة أو مكان الحجز وكيفية الحجز.

أولا :مشاكل الضبط في جرائم الانترنت.

الواقع هذه الصعوبات هي متعلقة بالتحقيق نفسه في جرائم الانترنت باعتبار الضبط هو الأثر الذي يتركه التحقيق، ثم بعد دلك نذكر اهو الوسائل المادية والإجرائية المساعدة في الضبط والتحقيق.

أ–صعوبات الضبط في جرائم الانترنت.

انّ المشاكل و الصعوبات التي تكتسي التحري و التحقيق في جرائم الانترنت وبالتالي الضبط عديدة، حيث أن التحري و التحقيق الالكتروني أو الرقمي تختلف عنه في الجرائم العادية و ذلك بتعامل المتحري مع أدلة غير مادية.

فإذا ربطنا التحري و التحقيق بالضحية، فإنّ أول مشكل يواجه سلطات البحث و التحري، هو إحجام العديد من مستخدمي الانترنت عن الإبلاغ أو تقديم شكوى التي تعتبر من أهم مهام ضباط الشرطة القضائية في جميع الجرائم و هذا بحسب نص المادة(17-1)من قانون الإجراءات الجزائية.ومن معوقات التحقيق :

[1] سامح احمد البلتاجي موسى ، المرجع السابق،ص274.

[2] سليمان احمد فضل،المرجع السابق،ص312.

1-الكم الهائل للبيانات والاستخدام الكبير لها ،واستخدام طرق كالتشفير[1] لإعاقة الوصل إليها، ولكن في مواجهة ذلك، أعطى المشرع الجزائري بعض المهام التي تساعد في حفظ البيانات يقوم بها مزود خدمات الانترنت و هو نفس الأمر المنصوص عليه في المادة(16)من اتفاقية الأوروبية لمكافحة جرائم الانترنت

و لما كانت جرائم الانترنت من الجرائم الخاصة، فانه من قراءتنا لنصوص (09-04)و المرسوم الرئاسي سالف الذكر، لم يشر إلى تقديم البلاغ أو الشكوى عبر الانترنت، رغم ان جرائم تكنولوجيات الإعلام و الاتصال قد يكون الأنسب لها، أن تقدم البلاغ[2] أو الشكوى[3] في حال تقدم به المبلغ أن يكون عبر الانترنت، وربما هو الأنسب إذا ما قام مثلا بنسخ رابط الموقع الالكتروني الذي يعتقد انّه اخترق جهازه أو أرسل له رسائل تهديد و ما إلى ذلك، و لكن نص المادة (17) جاء عاما و لم يحدد الوسيلة لتقديم البلاغ، الذي يكون من أي شخص دون الشكوى التي يجب أن تقدم من الشخص المضرور ، و فرضا انّه تمّ إنشاء موقع للهيئة سالفة الذكر عبر الانترنت و وضع بريد للاتصال و تقديم البلاغات فانّ العائق الأكبر يبقى لدى الضحية لاعتبارات تمّ ذكرها سابقا.

[1] التشفير :هي طريقة يتم بواسطتها جعل قراءة وفهم وثيقة ما امرا مستحيلا بالنسبة لاي شخص لا يملك مفتاح التشفير،انظر المغيث ،معجم قانون تكنولوجيات الإعلام والاتصال، عربي ،فرنسي،انجليزي،الطبعة الأولى،مركز البحث في الإعلام العلمي والتقني،الجزائر،2008،ص54.

[2] بإمكانك إرسال معلومات أو التبليغ عن أية جريمة مهما كان نوعها بغرض المساهمة في حفظ النظام والأمن العمومي، في كل حالات الاستعجالات، إتصل بالرقم الأخضر 1055

[3] بإمكانك إيداع شكوى مسبقة عن طريق الأنترنت وتأكيدها لدى الوحدة المعنية،هذه الخدمة تمكنك من ربح الوقت بفضل حجز موعد مسبق عبر الأنترنت مع فرقة الدرك المختصة إقليميا،يحدد لك موعد ويرسل إليك عن طريق بريدك لإلكتروني، في حالة عدم التقدم لتأكيد الشكوى خلال مدة 30 يوما بعد الموعد المحدد، تلغى الشكوى تلقائيا، في كل حالات الإستعجالات، إتصل بالرقم الأخضر 1055 انظر لموقع الالكتروني التالي https://ppgn.mdn.dz/prep.php ا

2-صعوبات تتعلق بالمعلومات.

– ضخامة المعلومات التي من يجب فحصها من قبل المحقق عن طريق الشخص المكلف بهذه المهمة المنتمي إلى الهيئة الوطنية، الموجودة على شبكة الانترنت خصوصا أنّ النشر الالكتروني لم يعد مقتصر على فئات معينة في ظل تزايد سهولة النشر على مواقع التواصل الاجتماعي.

– ومن الصعوبات كذلك التي تعيق الوصول إلى ضبط الدليل الجنائي الالكتروني، وجود حماية أمنية المفروضة من قبل مستخدم النظام حول البيانات التي يحويها هذا النظام. وهذا باستخدام مختلف طرق الحماية ككلمات السر أو شفرات المرور أو شفرات ترميز البيانات مما تصعب من عملية الضبط.

– إنّ تعطيل النظام المعلوماتي بما فيها الشبكات، لضبط المعلومات هو إشكال يعترض الكثير من أصحاب المؤسسات التي تعتمد في نشاطها على شبكة الانترنت وبالتالي إلى، خسارة أموال طائلة لأنها تتضمن عناصر الإثبات، لذلك لابد من إعمال "مبدأ التناسب"[1].

3-.من ناحية مكان الحجز وكيفيته:لا محدودية شبكة الانترنت وسّع من حدود مسرح الجريمة، والتي في الكثير من الأحيان تتجاوز الحدود الوطنية، أي الإقليم الوطني الأمر الذي يتطلب وجود تعاون دولي في إطار التحقيقات ،دون المساس بسيادة الدولة[2]، اتساع مسرح الدليل الجنائي الالكتروني حيث انّ أهم خاصية لجرائم الإنترنت هو صعوبة اكتشافها وبالتالي اثباتها ، ذلك انها جريمة ليس لها اي علاقة بالواقع المادي الملموس، فيمكن للمجرم أن يعبث بالبيانات دون ان يلحظ الضحية لذلك يواجه الضابط المختص والخبير على حد سواء مجموعة من المشاكل والصعوبات في سبيل جمع الأدلة ، ففي حالة إغلاق المنظومة المعلومتية تُفقد العديد من المعطيات .

[1] مبدأ التناسب في ضبط الدليل هو الاقتصار على الأدلة التي تؤدي إلى كشف الحقيقة كي لا يؤدي إلى تعطيل النظام المعلوماتي، شيماء عبد الغني محمد عطا الله، المرجع السابق، ص358.

[2] المادة (15) والمادة (16) من القانون(09-04)

خصوصا إذا كان الإغلاق بصفة عشوائية مما يؤدي إلى محو المعطيات، كما أنّ ذكاء الجاني و قيامه بزرع قنابل زمنية قد يصعب على سلطات الضبط تحصيل الدليل الجنائي الإلكتروني ، بالإضافة إلى طبيعة مسرح الجريمة والمتمثل في العالم الإفتراضي وخصوصا إذا امتد هذا المسرح على أكثر من إقليم دولة ، هذا و من جهة أخرى عملية إخفاء هوية المستخدم التي تقوم بها العديد من المواقع وإخفاء البيانات الشخصية يشكل عائقا أمام الخبير والمحقق على حد سواء في استعادة وإعادة بناء الدليل الجنائي الإلكتروني.هي أهم المشاكل التي لابد من مجابهتها تشريعيا وفنيا عن طريق ما يعرف بالتدريب الأمني التخصصي للهيئات المختصة[1].

ب- الوسائل المساعدة في الضبط والتحقيق.

تنقسم الوسائل المساعدة في الضبط والتحري في جرائم الانترنت، الى وسائل مادية واخرى اجرائية

1- الوسائل المادية المساعدة في الضبط والتحقيق.

وهي الأدوات الفنية التي غالبا ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها [2]:

- عناوين،IP والبريد الإلكتروني، وبرامج المحادثة.

فعنوان الإنترنت هو المسئول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها، وهو يشبه إلى حد كبير عنوان البريد العادي، حيث يتيح للموجهات والشبكات المعنية نقل الرسالة، وهو يوجد بكل جهاز مرتبط بالإنترنت، ويتكون من أربعة أجزاء، كل جزء يتكون من

[1] سامح احمد البلتاجي موسى، المرجع السابق، ص393.

[2] سليمان مهجع العنزي،المرجع السابق،ص98.

أربع خانات، فيكون المجموع اثنا عشر خانة كحد أقصى، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد الحاسب الآلي الذي تم الاتصال منه[1].

ويمكن لمزود خدمة الإنترنت أن يراقب المشترك، كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضا إذا ما توافرت لديها أجهزة وبرامج خاصة لذلك، طبعا بطلب من السلطات المختصة، لتحديد رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية[2].

---

[1] سليمان مهجع العنزي،المرجع السابق،ص98.

[2]ومن الحالات الملموسة التي تحصلنا على معلومات عليها من طرف مركز مكافحة الجرائم المعلوماتية التابع لقيادة الدرك الوطني على مستوى الجزائر العاصمة، بعد الزيارة الميدانية يوم 4 يناير 2018 وتتلخص وقائع القضية كالاتي: أواخر سنة (2013)أين تقدمت المسماة "ق.ي" بشكوى ضد شخص يحمل اسم مستعار"B.M" هذا الأخير قام باختراق حاسوب الشاكية وتحكم فيه عن بعد ملتقطا لها صورا عن طريق كاميرا الواب الخاصة بها ،ليقوم بنشر صورها على موقع التواصل الاجتماعي فايس بوك بهدف ابتزازها .

التحريات على شبكة الانترنت أفضت إلى مايلي:تبقى طريقة اختراق حاسوب الضحية مجهولة في ظل تكتمها عن الأنشطة الحقيقية التي قامت بها على الانترنت و التي مكنت المشتبه فيه من التحكم في حاسوبها الشخصي، ربما لشعورها بالإحراج و خصوصا بحضور والديها اثناء التحقيق معها.

الضحية قامت بطمس الأدلة المتروكة أثناء اختراق حاسوبها و هذا بتفويض شخص ثالث بإصلاحه و نزع البرامج الخبيثة منه،تم التأكد من عملية الابتزاز و تصوير الضحية بدون علمها من خلال الاطلاع على المحادثة التي جرت بين الضحية و المشتبه فيه على الفايس بوك.

نتائج التحقيق : بعد التدقيق في المعطيات المنشورة في حساب المشتبه فيه على الفايس بوك تحت الاسم B. M توصلنا الى مايلي:

المشتبه به هاكر ينسب نفسه إلى مجموعة الهاكر المشهورة باسم Anonymous ،البحث في الانترنت بالتوقيع B. M لتعقب أنشطة هذا الأخير بهذا الاسم لم تأتي بأي جديد يذكر. المشتبه فيه انشأ حسابه لأول مرة سنة **2011** باسم **كريم**. المشتبه فيه وضع صورة لحاسبه لشاب يضع قناع Anonymous و كتابة تم تمويهها، قد تكون هذه الصورة له كون بعض أصدقائه في الفايس بوك يضعون نفس الأقنعة مع تواقيع مختلفة،باستعمال طرق بحث متقدمة على الانترنت لمحاولة معرفة الصورة الأصلية بدون تمويه و كذا المواقع التي وضعت فيها و هذا لجمع معلومات من شانها تعريف الشخص المقنع، تم التوصل إلى أن الصورة لشخص وضع إعلان لبيع قناع Anonymous على الموقع المتخصص في إعلانات البيع على الانترنت ouedkniss.com مع معلومات للاتصال به من أجل شرائه.تم تعريف رقم الهاتف المتروك على الإعلان في موقع ouedkniss.com،تم تسخير مالك الموقع ouedkniss.comالمتواجد بالقبة و هذا من أجل الحصول على جميع المعلومات الممكنة عن صاحب الحساب المشتبه فيه (رقم هاتف تفعيل الحساب، جميع عناوين IP التي اتصل بها المشتبه فيه إلى حسابه، المحادثات التي جرت مع المشتبه فيه من خلال الموقع ، إعلانات أخرى للمشتبه به،...).تعريف أرقام الهاتف و عناوين IP المتحصل عليها من تسخير مالك الموقع. مع معلومات ميدانية عن المشتبه فيه تضم بالخصوص معارفه التقنية. بعد إجراء مقاربات شاملة تم توقيف المتورطين و تقديمهم للعدالة.

هذا وتوجد أكثر من طريقة يمكن من خلالها معرفة هذا العنوان الخاص بجهاز الحاسب الآلي في حالة الاتصال المباشر، منها على سبيل المثال ما يستخدم في حالة العمل على نظام تشغيل (WINDOWS) حيث يتم كتابة (WINPCFG) في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان(IP) ، مع ملاحظة أن عنوان الإنترنت قد يتغير مع كل اتصال بشبكة الإنترنت،أمّا في حالة استخدام أحد البرامج التحادثية كأداة للجريمة فإنه يتطلب تحديد هوية المتصل، كما تحدد رسالة البريد الإلكتروني عنوان شخصية مرسلها حتى ولو لم يدون معلوماته في خانة المرسل شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعدادات البريد الإلكتروني معلومات صحيحة [1].

– البروكسيPROXY .

يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة Cache Memoryوتقوم فكرة البروكسي على تلقى مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن ذاكرة Cache المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فيقوم بإعادة إرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، أما انه لم يتم تنزيلها من قبل فيتم إرسال الطلب إلى الشبكة العالمية، وفي هذه الأخيرة يعمل البروكسي كمزود زبون ويستخدم أحد عناوين IP ومن أهم مزايا مزود البروكسي أن ذاكرة Cache المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوى في الإثبات عن طريق فحص تلك العلميات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة [2].

[1] سليمان مهجع العنزي، البحث السابق،ص99.

[2] سليمان مهجع العنزي، البحث السابق،ص99.

–برامج التتبع، تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم وتقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوى هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IPالتي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى [1]،حيث تلعب هذه البرامج دور هام في التحقيق.

– نظام كشف الاختراق، ويرمز له اختصارا بالأحرف IDS وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسب الآلي أو الشبكة مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسوب أو الشبكة[2]، والتي يمكن أن تقدم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها[3].

– نظام جرة العسل.Honey Pot ،وهو نظام حاسوبي مصمم خصيصا لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أية بيانات ذات أهمية، ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعا خاطئ بسهولة الاعتداء على هذا النظام بهدف إغرائه بمهاجمته ليتم منعه من الاعتداء على أي جهاز آخر في الشبكة، في الوقت الذي يتم جمع أكبر قدر ممكن

---

[1] سليمان مهجع العنزي،البحث السابق،ص100.

[2] Bace Rebecca ،هامش رقم 49 مشار إليه لدى حسن بن سعيد الغافري،البحث السابق ،المنشور على الموقع السابق.

[3] ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاصة بتسجيل الأحداث فور وقوعها في جهاز الحاسب الآلي أو الشبكة،ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية والتي يطلق عليها أهل الاختصاص مصطلح التوقيع،وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عده ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة ، محمد بن نصير محمد السرحاني،مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت ،رسالة ماجستير ،أكاديمية نايف للعلوم الأمنية،الرياض،2004،ص84.

من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء، وتحليلها وبالتالي اتخاذ إجراء وقائي فعال[1].

-أدوات تدقيق ومراجعة العمليات الحاسوبية:Auditing Tools ،وهي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجري على ملفات ونظام تشغيل حاسوب معين وتسجيلها في ملفات خاصة يطلق عليها Logs والكثير من هذه الأدوات تأتي مضمنة في أنظمة التشغيل المختلفة، وبعضها يأتي كبرامج مستقلة يتم تركيبها على أنظمة التشغيل بعد إعدادها للعمل[2]، وكل ما يحتاجه الأمر هو قيام مدير الشبكة أو النظام بتفعيلها وإعدادها للعمل في وقت مبكر وسابق لارتكاب الجريمة حتى يمكن أن تقوم بتسجيل المعلومات التي قد يكون لها علاقة بالحادثة وربما ساعدت في كشف أسلوب الجريمة وشخصية مرتكبها[3]،ومن الأمثلة على هذه الأدوات أداة Event Viewerلبيئة النوافذ، وأداة Syslogd لبيئة يونيكس [4].

-أدوات الضبط.هي أدوات تعتبر من الوسائل المادية التي تساعد في ضبط الجرائم الناشئة عن استخدام غير المشروع للانترنت،منها على سبيل المثال برامج الحماية وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، وبرامج التصنت على الشبكة، والتقارير التي تنتجها نظم أمن البيانات، ومراجعة قاعدة البيانات، وبرامج النسخ الاحتياطي،تستخدم لعمل نسخة مطابقة تماما للأقراص الصلبة الموجودة في الحواسيب محل التحقيق وعلى مستوى البتBitstream Backup، بغرض عمل الفحوصات الجنائية عليها دون تعريض الأقراص الأصلية لأي تغير في البيانات الموجود[5].

[1] محمد بن نصير محمد السرحاني،المرجع السابق ،ص84.

[2] محمد بن نصير محمد السرحاني،المرجع السابق ،ص84.

[3] Camplian ، مرجع مشار إليه لدى ، محمد بن نصير محمد السرحاني،المرجع السابق،ص84.

[4] محمد بن نصير محمد السرحاني،البحث السابق،نفس الموضع.

[5] Vacca، مرجع مشار إليه لدى ، محمد بن نصير محمد السرحاني،المرجع السابق،ص85.

– الوسائل المساعدة للتحقيق.

من هذه الوسائل الأدوات المستخدمة في استرجاع المعلومات من الأقراص التالفة، وبرامج كسر كلمات المرور، وبرامج الضغط وفك الضغط، وبرامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسب، وبرامج نسخ البيانات، كذلك من الأدوات المهمة والتي تساعد في عملية التحقيق في برامج منع الكتابة على القرص الصلب، وذلك بعد ارتكاب الجريمة مما يساعد في المحافظة على مسرح الجريمة، وهناك البرامج التي تساعد على استرجاع الملفات والمعلومات التي قد يلجأ الجاني إلى حذفها نهائيا من الحاسب الآلي ومن أشهرها على سبيل المثال، برنامج Get Free لبيئة النوافذ، وبرنامج Extractor لبيئة يونيكس[1].والعديد من البرمجيات التي تستعملها السلطات المختصة والمخولة قانونا ، وخصوصا في مجال الخبرة واسترداد الدليل الجنائي الالكتروني[2].

– أدوات فحص ومراقبة الشبكات[3].

هذه الأدوات تستخدم في فحص بروتوكول(TCP/IP) وذلك لمعرفة ما قد يصيب الشبكة من مشاكل، ومعرفة العمليات التي تتعرض لها[4].

---

[1] سليمان بن مهجع العنزي، المرجع السابق ص 101-102 و محمد بن نصير محمد السرحاني، المرجع السابق ص85.

[2] وهي برامج تمكن المحقق من الإطلاع على محتوى كل ملف حاسوبي Hexadecimal Editors كبرمجيات تحرير الملفات الست عشرية بشكله الثنائي، متيحة له المزيد من القدرة على تحليل الملف والتعرف على طبيعة البيانات التي يحتويها، خاصة وأن بعض الأنظمة قد لا تستطيع تحديد إلى أية فئة من الملفات ينتمي هذا الملف، وقد يتطلب الأمر استخدام هذا النوع من برامج التحرير التي تعتمد على أن الكثير من الملفات تحتوى على مجموعة من الرموز ذات الدلالة تتواجد في بداية الملف، ويستطيع الخبير الحاسوبي من خلالها تحديد نوع الملف بدقة ومن أشهر هذه البرنامج. Hex Ganderو winمحمد بن نصير محمد السرحاني،المرجع السابق ،ص85.

[3] سليمان بن مهجع العنزي، المرجع السابق، ص 104.

[4] ومن هذه الأدوات، أداةRP، ووظيفتها تحديد مكان الحاسب الآلي فيزيائيا على الشبكة، برنامج Visual Route 5.2a وهو عبارة عن برنامج يلتقط أي عملية فحص عملت ضد الشبكة، فيقوم بتقديم أجوبة تبين المعلومات التي حدث فيها مسح، والمناطق التي مر فيها الهجوم، وبعد معرفة عنوان IP أو اسم الجهة يرسم البرنامج خط يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم، أداة TRACER،تقوم هذه الأداة برسم مسار بين جهازين تظهر فيه كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني وتوجه من خلالها والوقت والفترات التي قضاها، وهي تسمح برؤية المسار الذي اتخذه IP من مضيف إلى آخر، وتستخدم هذه الأداة الخيار Time To

2- الوسائل الإجرائية.

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها:

- اقتفاء الأثر.

من أخطر ما يخشاه مجرم الانترنت أو المجرم التقني تقصي أثره أثناء ارتكابه للجريمة، فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل بين جنباتها العديد من النصائح أولاها نصيحة هي قم بمسح آثارك Cover Your Tracks ، فلولم يقم المخترق بمسح آثاره فمؤكد أنه سوف يتم القبض عليه حتى وإن كانت عملية الاختراق قد تمت بشكل سليم، ويمكن تقصي الأثر بطرق عدة سواء عن طريق بريد إلكتروني تم استقباله أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق[1].

-الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته.

ينبغي على المحقق وهو بصدد التحقيق في إحدى الجرائم المتعلقة بشبكة الإنترنت أن يطلع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء، كما ينبغي عليه الإطلاع على عمليات النظام المعلوماتي كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة مواد النظام والمستفيدين والملفات والإجراءات وتصنيف الموارد العامة، ومدى مزامنة الأجهزة، ومدى تخصيص

Live TTLالتي تكون ضمن IP لكي تستقبل من كل موجه رسالة وبذلك يكون هو العدد الحقيقي للوثبات،ويتم بذلك تحديد وبشكل دقيق المسار التي تسلكه الرزمة،وهذه الأداة تستخدم في الأساس للمسح الميداني للشبكات المراد التخطيط للهجوم عليها، إذ أنه يبين الشبكة وتخطيطها والجدران النارية المستخدمة ونظام الترشيح ونقاط الضعف، ولكن يمكن أيضا يمكن من خلالها معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والاختراقات التي وقعت عليها،أداة، NET STAT هي أداة لفحص حالة الاتصال الحالي للبرتوكول(TCP/IP)، ولها عدد من المهام من أهمها عرض جميع الاتصالات الحالية، ومنافذ التصنت، وعرض المنافذ والعناوين بصورة رقمية وعرض كامل لجدول التوجيه سليمان بن مهجع العنزي، المرجع السابق، ص 105.

[1] سليمان بن مهجع العنزي، المرجع السابق، ص105.

وقت معين في اليوم يسمح باستخدام كلمات المرور، ومدى توزيع الصلاحيات للمستفيدين،وإجراءات أمن العاملين، وأسلوب النسخ الاحتياطي، والاستعانة ببرامج الحماية، كمراقبة المستفيدين والموارد والبرامج التي تعالج البيانات وتسجيل الوقائع وحالات فشل الدخول إلى النظام، بالإضافة إلى معرفة نوعية برامج الحماية وأسلوب عملها، والاستفادة من التقارير التي تنتجها نظم أمن البيانات وتقارير جدران الحماية [1].

– الاستعانة بالذكاء الصناعي[2].

أثبتت تقنيات الحاسب الآلي نجاحها في جمع الأدلة الجنائية وتحليلها واستنتاج الحقائق منها، كما يمكن الاستعانة بالذكاء الصناعي في حصر الحقائق والاحتمالات والأسباب والفرضيات ومن ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي، وفق برامج صممت خصيصا لهذا الغرض.

ثانيا: ضبط الدليل الجنائي في جرائم الانترنت:

إنّ الضبط في جرائم الانترنت، يكون حسب الشيئ المضبوط أو بمعنى اصح شكل الدليل الجنائي الالكتروني، فقد يكون عبارة عن صور أو مراسلات أو محررات كالصور التي تكون في البريد الالكتروني أو اتصالات الكترونية مكتوبة،، حيث اختلفت الآراء الفقهية في مدى إمكانية ضبط او الدليل الجنائي الالكتروني وماهي سبل حجز الدليل الجنائي الالكتروني ثم أدرجنا الشائع في ضبط الدليل الجنائي ضبط البريد الالكتروني، وهذا ما سنتناوله بالتفصيل فيما يلي:

أ– مدى صلاحية ضبط أدلة الجرائم الانترنت[1]:إنّ الأصل أنّ الضبط يرد على الأدلة المادية، لوجود كيان يحويها كالمخدر أو السلاح الناري في مختلف الجرائم، ولكن وبعد ظهور جرائم الانترنت وأدلتها غير المادية؛ شكل هذا خلافا حول مدى صلاحية هذه الأدلة للضبط.

[1] محمد نصير بن محمد السرحاني، المرجع السابق ،ص 79.

[2] سليمان بن مهجع العنزي، المرجع السابق، ص106.

1-الاتّجاه الأول: يرى أنصاره أنه لا يمكن تصور إجراء الضبط على المكونات المعنوية أو الكيانات المنطقية للنظام المعلوماتي، لعدم وجود كيان مادي، لذلك لا تصلح المعلومات المعالجة أليا والاتصالات الالكترونية أن تكون محلا للضبط، بنفس إجراءات الضبط الخاصة بالجرائم الأخرى حتى ماتعلق منه بالجرائم الخاصة[2].

2-الاتجاه الثاني: هذا الاتجاه هو عكس الاتجاه الاول، المعلومات المعالجة أليا أو الاتصالات الالكترونية يمكن أن تكون محلا للضبط، لانّ الضبط يكون لكل دليل ناتج عن التفتيش، أي يمكن استخدام النصوص المتعلقة بالضبط في قانون الإجراءات الجزائية، ومادامت هذه البيانات هي عبارة عن نبضات مغناطيسية ،وتقبل أن تخزن وتسجل وتنقل إذن لها وجود مادي وبالتالي تعامل كالأدلة المادية[3].

وبين هذا وذاك فصَل المشرع الجزائري في هذا الإشكال، بان تدخل تشريعيا و اقرّ الضبط للدليل الجنائي الالكتروني، والذي أعطاه أي الضبط مصطلح الحجز لكي يتلاءم وطبيعة الدليل ،كما بين أنواعه وفق ما يتوافق وخصائصه.وحيث انه لا يمكن حجز المعطيات بطريقة واحدة اقر المشرع الجزائري أساليب تصلح للحجز بمقتضاها وهذا حال وجود عراقيل تمنع ذلك كوجود الدليل خارج المنظومة المعلوماتية بمعنى أن لا يُتمكن من حجزه من خلال المكونات المادية للحاسب أو الهاتف النقال أو أية تقنية أخرى،لذلك كان لابد من وضع أساليب أخرى للحجز كالحجز عن طريق النسخ او المنع من الوصول .

[1] هشام محمد فريد رستم،الجوانب الاجرائية للجريمة المعلوماتية،المرجع السابق،ص98 وما يليها.

[2] هشام محمد فريد رستم،الجوانب الاجرائية للجريمة المعلوماتية،المرجع السابق،ص93-94 وهلالي عبد اله احمد،تفتيش نظم الحاسب الالي وضمانات المتهم المعلوماتي،دراسات مقارنة، المرجع السابق، ص85.

[3] فهد عبد الله العبيد العازمي،المرجع السابق،ص307.

ب–حجز المنظومة المعلوماتية.

كما ذكرنا سابقا فان إجراء التفتيش قد يطال المنظومة المعلوماتية بمكوناتها المادية[1] والمعنوية والشبكات؛ ومثلها الحجز والذي يتعلق بالمعطيات المعلوماتية، التي تحمل في طياتها الدليل الجنائي الالكتروني.

بالتالي تسحب جميع الشروط الموضوعية والشكلية للتفتيش عن بعد على حجز المعطيات، باعتبار الحجز هو اثر التفتيش لاستخلاص الدليل الجنائي في شكله الالكتروني، وبالعودة إلى محل الحجز فهو المنظومة المعلوماتية بمكوناتها المادية والمعنوية، وفي هذا الصدد فانه لا مجال للحديث عن حجز المكونات المادية، والتي قد يكون انسب مصطلح يتلاءم وطبيعتها هو الضبط والتي تنطبق عليها شروط ضبط الأدلة المادية[2]،وهي جزء مكمل لضبط الأدلة في جرائم الانترنت، حيث أنّ لها قيمة في الإثبات، الأوراق أو المحررات التي عادة ما يطبعها الأشخاص كدليل على قيامهم مثلا بمعاملات مصرفية عبر الانترنت، بالإضافة إلى كل المكونات المادية للمنظومة المعلوماتية من أجهزة حاسوب وأقراص والدعائم المعلوماتية، بالإضافة إلى المودم والطابعة وبطاقة الذاكرة، أي كل ما يتعلق بالمكونات المادية للمنظومة المعلوماتية، كما يمكن اضافة اي وسيلة حديثة مادية يمكن الولوج اليها للإنترنت ، كالهاتف النقال وساعة اليد وغيرهما.

بيد أنّ الإشكال يثور حين يتعلق الأمر بالمكونات المعنوية وارتباطها بالشبكات، هذا الأمر الذي فصل فيه المشرع بتنظيمه في المادة (06) من القانون (09-04)،وبالتالي فقد فصل في الخلاف الفقهي حول مدى قابلية المعطيات المعلوماتية للحجز، باعتبار أن الضبط وهو "وضع

[1] والمتمثلة في المخرجات والمستندات الورقية التي تم طباعتها،الحاسب الآلي وملحقاته الأقراص وغيرها من المكونات المادية التي تم التطرق اليها في الفصل الأول من الباب الأول من هذه الأطروحة،كما تطبق على هذه المكونات المواد 81 من قانون الاجراءات الجزائية و84 و85 و45 و 139 منه بالاضافة الى المادة 25 من قانون العقوبات.للمزيد من المعلومات انظر خالد ممدوح ابراهيم،فن التحقيق في الجرائم الالكترونية،المرجع السابق،ص275.

[2] مصطفى محمد الدغيدي،المرجع السابق،ص362.

اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها"[1]، بإدراجه المعطيات المعلوماتية محل للضبط أو الحجز، كون أنّ الضبط يرد في الأصل على الأشياء المادية والتي يندرج تحتها المكونات المادية للمنظومة المعلوماتية من شاشة عرض،الفارة،وكل المكونات المادية التي تم التطرق لها في الباب الأول من هذه الأطروحة ،كلوحة المفاتيح أو الطابعة أو الماسح الضوئي، أو حتى الهاتف النقال أو أي جهاز يستخدم تقنية المعلومات.

أمّا فيما يخص المكونات المنطقية والتي تشمل المعلومات والبيانات المعالجة أليا، وهي المعنية هنا ،فيتم حجزها وهذا بموجب نص المادة (6) [2]من القانون(09-04) سالفة الذكر وتتم عن طريق الحجز والذي فصّل به المشرع الجزائري بحسب مقدرة السلطات المختصة على القيام بالحجز وحسنا قد فعل المشرع الجزائري بتوضيح طرق الحجز قانون، ذلك انّ اي إخلال بجمع الأدلة وحجزها فيد يعرض الإجراء إلى بطلانه[3].

1-أنواع الحجز المعلوماتي.

تجدر الإشارة إلى أنّ المشرع الجزائري قد فصل في أقسام الحجز ألمعلوماتي، انطلاق من تنوع مصادر الحصول على البيانات التي تشكل الدليل الجنائي الالكتروني، باعتبار أنّ الطريقة المستعملة في حجز منظومة معلوماتية معينة، قد لا يكون الحال بالنسبة لمنظومة أخرى ،وعليه يتم حجز المعطيات المعلوماتية إما عن طريق نسخ المعطيات على دعامة تخزين الكترونية، أو الحجز عن طريق منع الوصول،على أنّ أنواع الحجز هذه التي تحرم الأشخاص غير المشتبه فيهم ومزودي الخدمة من

[1] مأمون سلامة، المرجع السابق،ص358.

[2] يقابل نص المادة(6) من قانون(09-04) نص المادة(19) من القسم الرابع للاتفاقية الأوربية للإجرام السيبيري.

[3] -Myriam QUÉMÉNER, Yves CHARPENEL Cybercriminalité, Droit pénal appliqué, 2010, ECONOMICA ,Paris France

الو لولوج إليها أي إلى المعلومات ، يمكن إعادتها أي رفع الحظر عليها بعد انتهاء عملية التحقيق وكل الإجراءات الجزائية الخاصة بالجريمة[1].

-الحجز عن طريق نسخ المعطيات.

على دعامة تخزين الكترونية والتي تكون بدورها قابلة للحجز والوضع في احراز كما نصت علية المادة (06) في فقرتها الأولى من القانون (09-04)،ويكون هذا بالنسبة للمعطيات القابلة للنسخ، وبالتالي القابلة للحجز ولو انه من وجهة نظر الباحثة "أن المعطيات المجرمة قد لا يتوانى المجرمون عن تشفيرها وتأمينها معلوماتيا من النسخ والنقل"، وهذه الطريقة التي عادة ما تكون فيها المعطيات مشفرة، فيتم نسخها من اجل فك التشفير لاحقا ،أو أي برمجية تحتوي على قنابل زمنية او وقتية [2]لدى وضع المشرع طريقة ثانية للحجز.

-الحجز عن طريق منع الوصول .

الحجز عن طريق منع الوصول هو تجميد التعامل من المنظومة المعلوماتية تحتوي على أدلة جنائية، وهو الإجراء الذي يمكن أن يؤخد به إذا تعذر نسخ البيانات الرقمية، ومثال ذلك منع الوصول إلى المواقع الإباحية[3]، أو المواقع الإرهابية التي تدعو إلى الأفكار المضللة وتوضح كيفيات صنع القنابل وما إلى ذلك، وهي طريقة نصت عليها المادة (07) من القانون (09-04)،وهي الحالة التي تلجا إليها السلطات المختصة في التفتيش والضبط أي حجز المعطيات المعلوماتية عن طريق استعمال تقنيات مناسبة لمنع الوصول إلى المنظومة المعلوماتية التي تحوي الدليل الجنائي الالكتروني؛ والتي عادة ما تكون تحت تصرف مزودي خدمات الانترنت وخصوصا متعهدي الإيواء أو الاستضافة ومتعهدي التخزين،بعد الخوض في إجراءات جمع الدليل الجنائي الالكتروني،

[1] هلالي عبد اله احمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، المرجع السابق، ص241.

[2] عمر ابو بكر بن يونس، المرجع السابق،ص871.

[3] عمر ابو بكر بن يونس، المرجع السابق،ص871.

الذي نؤكد أن جمعه لا يعتمد فقط على إجراءات الواردة في القانون (09-04) بل الإجراءات الخاصة الواردة في قانون الإجراءات الجزائية ،إضافة إلى طرق الإثبات العادية.

لابد من التعريج على شروط قبوله باعتباره نوع جديد مستقل عن باقي الأدلة الجنائية، والخاص بنوع معين من الجرائم، صنفها المشرع في إطار الجرائم الخاصة، وأي جزاء رتبه المشرع الجزائري في حال الإخلال بالشروط المتطلبة للإجراءات، في مواجهة حماية الحق في الحياة الخاصة وحقوق الدفاع.

ج –ضبط البريد الالكتروني:

إنّ أهم بيانات يمكن ضبطها في جرائم الانترنت هي الاتصالات الالكترونية، والتي تختلف فقد تكون عبارة عن صور أو فيديوهات أو معلومات معالجة او غير معالجة أليا، وبأي صورة كانت عادة ما يتم تخزينها أماّ على الشبكة أو تحميلها على مواقع التحميل أو وضعها على صفحات التواصل الاجتماعي، ولكن كل هذا مرتبط بالضرورة بالبريد الالكتروني للشخص الذي ترد كل شاردة وواردة في بريده الالكتروني، وحاليا دخل الهاتف الذكي بقوة واصبحت الرسائل القصيرة لها نفس المهام في تلقي كل شاردة وواردة، وكل تصرف قام به حيث أنّ هذه المواقع تتطلب ضرورة حصول المشترك على بريد الكتروني، ويعتبر البريد الالكتروني انسب محل لضبط الاتصالات الالكترونية، حتى انه يعتقد انه اسهل للاعتراض من البريد العادي او التقليدي[1].

لذلك فالبريد الالكتروني للمشتبه فيه هو الفضاء الأكثر ملائمة للبحث عن الأدلة وضبطها بعد عملية التفتيش أو المعاينة [2]، لان للضبط أو حجز المعطيات في البيئة الافتراضية وظيفتان، جمع الأدلة أي نسخ المعطيات، و مصادرة المعطيات وذلك بجعلها في نسخة أصلية غير قابل

[1] Sylvain Métille.op .cit ,p37

[2] محمد فتحي محمد أنور عزت، تفتيش شبكة الانترنت،لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبارات التي تقع بواسطتها،دراسة مقارنة،ط1،2012،المركز القومي للإصدارات القانونية،القاهرة،مصر، 451.

للوصول إليها،وبالتالي الضبط لا يعني المحو النهائي للبيانات المحجوزة[1]، إن الأصل آن مكونات شبكة الانترنت المادية والمعنوية،بما فيها المنظمومة المعلوماتية ، محل بعض الجرائم فيها هو المال المعلوماتي بمعنى يوصف المكونات المعنوية من برامج وتطبيقات بأنها شيئ منقول، يمكن نقل المكونات هذه المكونات المتمثلة في المعطيات المعالجة أليا و المعلومات من منظومة إلى أخرى ومن شبكة إلى أخرى[2].

على انّه يجب توخي روح المسؤولية في عدم الاطلاع على محتويات الرسائل الالكترونية التي لا تعني التحقيق ،عند ضبط هذه المراسلات من طرف الضابط المختص، فمثلا إذا كان العون المختص والمخول بهذه العملية يريد ضبط الرسائل الالكترونية التي وصلت إلى المتهم لابد عليه من مراجعة الرسائل الجديدة الواردة فقط ويمكن طباعتها أو نسخها على دعامة[3]، إلا انّه ومن ناحية عملية يتعذر أن يفصل العون بين ضبط هذه الرسائل الواردة وعدم الاطلاع عليها، لذلك فلا يمكن مراقبته لصعوبة ذلك ،كون المعلومات المضبوطة هي معلومات لا محسوسة معنوية ،وبالتالي فلا يكون إلا تحت طائلة إفشاء السر المهني فقط ،وضميره المهني الواعي في عدم التعسف في استعمال السلطة. يُنظر للنظام المعلوماتي على أنه فضاء افتراضي قد يرتبط بأكثر من جهاز ضمن منظومة واحدة، فيعد كل جهاز متضمنًا لنهاية طرفية للنظام المعلوماتي، وللتوضيح نضرب المثال التالي: فإذا كانت هناك منظومة لمجموعة فروع لمصرف واحد مرتبطة بعدة أجهزة، فإن كل جهاز بفرع من هذه الفروع سوف يمثل نهاية طرفية للنظام المعلوماتي المتمثل في المنظومة[4].

و إذا كانت فكرة السيادة الدولية ترتبط بالمفهوم التقليدي للإقليم، ف إننا لا نجد ما يمنع من تطبيق هذا الحكم في شأن تفتيش طرف لنظام معلوماتي من خلال الولوج من نهاية طرفية في

[1] هلالي عبد اله احمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، المرجع السابق، ص241.

[2] محمد فتحي محمد انور عزت، تفتيش شبكة الانترنت، المرجع السابق، ص452.

[3] هلالي عبد الاله احمد،تفتيش نظم الحاسب الالي وضمانات المتهم المعلوماتي،دراسة مقارنة، المرجع السابق، 216.

[4] طارق محمد الجملي ،المرجع السابق ،ص63

دولة أخرى، إذ ذلك لا ينتهك سيادة الدولة، فالنظام المعلوماتي لا يعرف الحدود، والوحدة التي يتمييز بها والتي أ شرنا إليها سابقًا، هي التي تعطي للجهة القائمة بالتفتيش سلطة الولوج وتتبع المعلومات ولو امتد ناشطها لطرف نظام معلوماتي في دولة أخرى، ولا يحد من سلطتها هذه- حسب ر أينا- إلا وجود نظام شفرة للدخول للمعلومات، فذلك يخرج هذا الجزء من نطاق الوحدة المعنوية، وهو ما تفقد معه تلك الجهة لاصحياتها في ذلك الجزء[1].

[1]طارق محمد الجملي ،المرجع السابق ،ص64

الفصل الثاني: الاختصاص والتعاون القضائي الدولي و القيمة القانونية للدليل الجنائي في جرائم الانترنت

لم تتضمن النصوص التشريعية، نصاً خاصاً يحدد مدى مشروعية اعتراض المراسلات أو التقاط الصور أو تسجيل الأصوات، ماعدا بعض المواد الدستورية التي أكدت على احترام حرمة الإنسان، ثم إقرار المسؤولية القانونية على من يمس بسلامة الإنسان البدنية والمعنوية، بالإضافة إلى حماية معالجة البيانات ذات الطابع الشخصي، وهذا بعد ضخ الكم الهائل من البيانات المعالجة أليا، لاستخدامها في جوازات السفر وبطاقات التعريف البيومترية، وغيرها من الاستخدامات، لذلك فالدليل الجنائي في جرائم الانترنت وليد إجراء مرخص به، متى كان الإجراء المستمد منه غير مشروع كان الدليل الجنائي الالكتروني منطقيا غير مشروع[1].

الأساس المتين الذي تستند عليه التشريعات، في حماية الحقوق والحريات وعلى رأسها الحق في الحياة الخاصة، وجود ضمانات إجرائية وقبلها دستورية، لأي إجراء من الإجراءات الخاصة المتعلقة بجرائم الانترنت،والتي سوف نقتصر فيها على إجراءات المستحدثة الخاصة بجرائم الانترنت أي مانصت عليه المواد(65مكرر5) ومايليها، وما نصت عليه المواد في القانون(09-04)، لان البيانات المخزنة داخل النظم ليست جميعا تتصل بجريمة الانترنت –سواء كان الاعتداء على الانترنت او باستعمال الانترنت–، منها بيانات خاصة وأخرى ذات قيمة اقتصادية او سياسية او غيرها، لهذا اهتم القانونيون بمخاطر الاعتداء على الخصوصية أو الحياة الخاصة في معرض البحث والكشف و الحصول عن الدليل أو في معرض قبول الدليل ذي طبيعة الكترونية سواء من حيث تنظيم أعمال جمع وتخزين ومعالجة ونقل البيانات أو من حيث حقوق الدخول إليها وحق أصحابها بسلامتها وصحتها وتعديلها، أو من حيث إقرار الحماية الجزائية لهذه البيانات[2].

[1] مصطفى يوسف، مشروعية الدليل في المسائل الجنائية،في ضوء الفقه والقضاء، بدون دار نشر،بدون ذكر البلد،2010 ،ص20.

[2] فهد عبد الله العبيد العازمي، المرجع السابق،ص440

واستكمالا لإجراءات الإثبات الجنائي لجرائم الانترنت لابد من الوقوف على الاختصاص القضائي في مثل هذه الجرائم ، والتعاون الدولي(المبحث الأول) كونها جرائم ذات طبيعة دولية لا يمكن فك رموزها ومتابعة المشتبه فيهم إلا بوجوده ،ثم تحديد القيمة القانونية للدليل الجنائي في جرائم الانترنت(المبحث الثاني) وخصوصا الدليل الجنائي الالكتروني.

المبحث الأول:الاختصاص القضائي والتعاون الدولي في جرائم الانترنت.

بعد أن تطرقنا لمحل إجراءات التحقيق في إطار قانوني الإجراءات الجزائية الجزائري وقانون تكنولوجيات الإعلام والاتصال، يجب علينا قبل تقدير هذا الدليل الناتج عنها، من حيث الضمانات المحيطة به للحصول عليه وقيمته الثبوتية، تحديد الاختصاص القضائي(المطلب الأول) سواء الداخلي أو الدولي في مثل هذه الجرائم ثم تكملة باقي الإجراءات والتي تخص التعاون الدولي باعتبار جرائم الانترنت هي جرائم عابرة للحدود الوطنية يلعب فيها التعاون الدولي(المطلب الثاني) دورا هاما في جمع الدليل، وملاحقة المجرمين حتى تسليمهم، وهذا لعدم وجود نظام قانوني للإثبات موحد بين الدول هنا يلعب التعاون الدولي دورا مهما في جمع الدليل الجنـائي في جرائم الانترنت و تحديدًا الدليل الجنائي الالكتروني[1] .

المطلب الأول:الاختصاص القضائي في جرائم الانترنت في التشريع الجزائري.

إنَّ من أهم المشاكل التي تعترض أي تقدم في سير العملية الاثباتية وإجراءاتها هو مشكل الاختصاص القضائي في الجرائم العادية، والذي يبدو أكثر تعقيدا حينما يتعلق الأمر بجرائم ذات بعد دولي ومنها جرائم الانترنت، فمسالة الاختصاص القضائي على كل المستويات المحلي والدولي ، هو تنازع أكثر من جهة قضائية سواء وطنية أو دولية للنظر في جرائم الانترنت.

إذن كيف عالج المشرع الجزائري هذه المسالة وما هي الحلول التي تبناها من اجل إنجاح عملية جمع الدليل الجنائي في جرائم الانترنت؟ من خلال تحديد قواعد الاختصاص القضائي الداخلي

[1]Solange Ghernaouti –Hélie, Sécurité Informatique et réseaux, dunod, paris, 2006,P.31.

(الفرع الأول) والقواعد الإجرائية المستحدثة في إطار الاختصاص القضائي الدولي طبعا في إطار القانون (09-04)(الفرع الثاني)، وماهي الهيئات الوطنية المختصة في جرائم الانترنت(الفرع الثالث).

الفرع الأول:الاختصاص القضائي الداخلي.

الاختصاص القضائي الداخلي أو الاختصاص القضائي المحلي أو الإقليمي، تمديد القضاء المختص في الفصل في الدعوى الجزائية دون وجود نزاع في الاختصاص، حيث يقوم ذلك وفق معايير عددها المشرع الجزائري، في المادة(1/37) من قانون ا.ج.ج.ج كمايلي:"يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة احد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على احد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب أخر".أي يتحدد الاختصاص القضائي بمكان وقوع الجريمة، أو المكان الذي يقيم فيه المتهم أو المكان الذي يقبض فيه المتهم حتى ولو كان القبض قد وقع لسبب أخر[1].

وفي الفقرة الثانية من المادة سالفة الذكر:"يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم والجريمة المنظمة عبر الحدود الوطنية

[1] المادة(329)ق. ا. ج .ج:" تختص محليا بالنظر في الجنحة محكمة محل الجريمة أو محل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر.

ولا تكون محكمة محل حبس المحكوم عليه مختصة إلا وفق الأوضاع المنصوص عليها في المادتين 552 و553.

كما تختص المحكمة كذلك بالنظر في الجنح والمخالفات غير القابلة للتجزئة أو المرتبطة.

وتختص المحكمة التي ارتكبت في نطاق دائرتها المخالفة أو المحكمة الموجودة في بلد إقامة مرتكب المخالفة بالنظر في تلك المخالفة.

يجوز تمديد الاختصاص المحلّي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التّنظيم، في جرائم المخدّرات والجريمة المنظّمة عبر الحدود الوطنيّة، والجرائم الماسّة بأنظمة المعالجة الآليّة للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلّقة بالتّشريع الخاصّ بالصّرف ."

والجرائم الماسة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف"[1].

ولما كانت جرائم الانترنت جرائم لا تعترف بالحدود المادية الواقعية، والجرائم الماسة بالمعالجة الآلية للمعطيات من صورها، فانّه عندما ترتكب الجريمة في إقليم الدولة الجزائرية، هنا الاختصاص القضائي جزائري. وبسبب طبيعة هذه الجرائم التي أوضحنا أهم خصائصها في الباب الأول من هذه الأطروحة، قد مُدِد الاختصاص القضائي ليشمل كل إقليم الدولة، حيث مدد الاختصاص لجرائم الانترنت أو جرائم تكنولوجيات الإعلام والاتصال ومن بينها جرائم المعالجة الآلية للمعطيات بموجب نص المادة (37) و (47)و (80)و (329) ق.ا.ج.ج.على أنّ هذا التمديد يشمل السلطات المختصة، وكيل الجمهورية وفق المادة (37) من قانون الإجراءات الجزائية وضباط الشرطة القضائية المادة(40مكرر1)،واختصاص قاضي التحقيق طبقا للمادة (40)من ق.ا.ج.ج، واختصاص المحاكم وفق المادة (329) من نفس القانون حيث أجاز تمديد الاختصاص إلى دائرة محاكم أخرى عن طريق التنظيم ،بموجب المرسوم التنفيذي رقـــم (06-348)[2].

[1] المادة(37) القانون رقم (04-14) المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 الموافق 10 نوفمبر سنة 2004،ج.ر رقم 71 ليوم 10 نوفمبر2004 ،ص4، المعدل والمتمم للأمر رقم (66-155) المتضمن قانون الإجراءات الجزائية .

[2] المرسوم التنفيذي رقم (06-348)المؤرخ في 12 رمضان عام 1427 الموافق 5 أكتوبر سنة 2006 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ،المعدل بالمرسوم التنفيذي رقم(16-267)مؤرخ في 15 محّرم عام 1438 الموافق 17 أكتوبر سنة 2016،ج ر رقم 62 ليوم 23 أكتوبر 2016.ص10،وبالتالي قد أجاز المشرع الجزائري تمديد الاختصاص المحلي لبعض وكلاء الجمهورية ، وقضاة التحقيق ودوائر اختصاص المحاكم كالاتي:

-يمتد الاختصاص المحلي لمحكمة سيدي امحمد ووكيل الجمهورية وقاضي التحقيق بها الى محاكم المجالس القضائية للجزائر والشلف والاغواط والبليدةوالبويرة وتيزي وزو والجلفة والمدية والمسيلة وبومرداس وتيبازة وعين الدفلى.

- يمتد الاختصاص المحلي لمحكمة قسنطينة وام البواقي وباتنة و بجاية وتبسة وجيجل وسطيف وسكيكدة وعنابة وقالمة وبرج بوعريريج والطارف وخنشلة وسوق اهراس وميلة.

-يمتد الاختصاص لمحكمة ورقلة ووكيل الجمهورية وقاضي التحقيق بها الى محاكم المجالس القضائية لورقلة وادرار وتامنغست وايليزي وبسكرة والوادي وغرداية.

- يمتد الاختصاص المحلي لمحكمة وهران ووكيل الجمهورية وقاضي التحقيق بها الى محاكم المجالس القضائية لوهران وبشار وتلمسان وتيارت وتندوف وسعيدة وسيدي بلعباس ومستغانم ومعسكر والبيض وتيسمسيلت والنعامة وعين تموشنت وغليزان.

وعليه فان الاختصاص القضائي في الجرائم يتحدد حسب:[1]

أ– ضرورة التحقيق:ان وجود دلائل قوية لارتكاب جريمة الانترنت يجيز للقاضي التحقيق تمديد الاختصاص حيث يدخل في نطاق محاكم أخرى مجاورة.

-أن يكون هناك ضرورة للانتقال خارج نطاق اختصاصه المكاني .

- أن يخطر وكيل الجمهورية في نطاق الاختصاص الذي يعمل في نفس دائرة اختصاصه.

- إخطار وكيل الجمهورية في نطاق الاختصاص الذي تم التمديد إليه.

- توضيح الأسباب التي أدّت إلى تمديد الاختصاص .

لذلك فان قواعد الاختصاص من النظام العام وهذا لارتباطها بحسن سير العدالة، فهي تحدد الأهلية الإجرائية لجهات القضاء لنظر الخصومة[2].

ب-التمديدلا يتم إلا في جرائم معينة: وهي جرائم تشمل تمديد وكيل الجمهورية واختصاصات في التحقيق والمحكمة، ويدعم هذا التمديد ما جاءت به المادة(5) من القانون (09-04)والتي شملت بتمديد الاختصاص حين يتعلق الأمر بمسرح الجريمة الافتراضي بمعنى انّ المشرع قد حاول الجمع بين المسرحين العادي أو التقليدي والمسرح الافتراضي؛ فقد نصت المادة(5) من القانون السالف الذكرعلى مايلي: "...إذا كانت هناك أسباب تدعو للاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وان هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك".

[1] فايز محمد راجح غلاب، المرجع السابق، ص377-378، درياد مليكة،المرجع السابق،ص154 وما بعدها.

[2] سامح احمد البلتاجي موسى، المرجع السابق، ص395.

إنَّ هذه المادة إضافة جيدة خصوصاً، أنَّ هذه المادة والمواد السابقة الذكر تجمع بين تمديد الاختصاص في المسرحين الإجراميين العادي أي المادي واللامادي الافتراضي، وبذلك يتسنى للجهات المختصة التوصل إلى أفضل النتائج عندما يتعلق الأمر بالتحقيق في جرائم الانترنت، ذلك انّه لابد من أن لا نهمل أي من المسرحين؛ وهو ما يجدر بالسلطات المختصة الانتباه له في عملية جمع الدليل الجنائي الالكتروني، دون إهمال دعائم الإثبات الجنائي الأخرى كشهادة الشهود مثلا.هذا حتى تكون الأدلة الناجمة تتحلى بالمصداقية ويقينية بقدر ما كانت الإجراءات شاملة لكلى المسرحين.

بذلك فالأدلة الناتجة هي أدلة قوية بعيدة عن الانتقادات الموجهة إليها، في حال كان الدليل الناتج عن احد المسرحين الإجراميين فقط، وذلك بعد أن تتكامل جميع أدلة الإثبات أي جمع الدليل الالكتروني، وكذا فاعلية دعائم الإثبات في المسرح العادي.

الفرع الثاني:الاختصاص القضائي الدولي.

إنّ ما يثير الإشكال في تمديد الاختصاص في جرائم الانترنت هو امتداد مسرحها إلى أكثر من إقليم دولة، فان كان بإمكان التصدي إلى اتساع نطاق الجريمة داخل الدولة؛ باعتبارها وحدة واحدة، هو ما لا يمكن تصوره إذا تعلق الأمر بامتداد مسرح الجريمة إلى أكثر من إقليم دولة، ذلك أّن أهم خصائص جرائم الانترنت أنّها عابرة للحدود، وهو ما يصطدم بمبدأ أصيل في تطبيق القانون الجزائي مبدأ الإقليمية (أولا)، طبعا دون انتهاك سيادة الدولة في تحصيل الدليل الجنائي الالكتروني، والمبادئ الاحتياطية (ثانيا)،فالطبيعة التقنية للمنظومة المعلوماتية المرتبطة بتكنولوجيات الإعلام والاتصال تؤدي لا محال إلى أن يصبح إقليم أكثر من دولة مسرحا لجريمة من جرائم الانترنت[1].

[1] عادل عزام سقف الحيط، المرجع السابق، ص349.

ومما يزيد من إشكالية تطبيق قواعد الاختصاص هو اختلاف التشريعات والنظم القانونية لكل دولة.

أولا: مبدأ الإقليمية في جرائم الانترنت.

تعتبر المحاكم الجزائرية صاحبة الاختصاص الأصيل بالنظر في الجرائم المتعلقة بالانترنت والتي تقع على إقليمها،كل السلوك الإجرامي أو جزء منه دون الأخذ بعين الاعتبار شخص المتهم وهو المبدأ المجسد في المادة (3 فقرة1) من ق.ع.ج[1]، هذا المبدأ الذي يعد مظهرا من مظاهر السيادة أي دولة.

الأصل أنّ يطبق القانون الجزائي بشقّيه الموضوعي والإجرائي، ما كان السلوك الإجرامي قد وقع على إقليم الدولة، وهذا بنص المادة (3) من قانون العقوبات والمادة (586)من قانون الإجراءات الجزائية منه، فلكل دولة الحق في تحديد نطاق تطبيق قانونها الجزائي، وبالتالي تحديد الاختصاص القضائي وفق ما تمليه ضرورة حماية مصالحها العليا السيادية[2].

إنّ كل دولة تملك أن تحدد تطبيق القانون الجزائي استنادا إلى مكان وجود تواجد احد أركان الجريمة أو انطوى الفعل الإجرامي على سلوك يمس بالمصالح الأساسية للدولة من امن وطني واقتصادي أو حتى ما أملته ضرورة التعاون الدولي في المجال الجزائي[3].

الأصل أنّ عناصر الركن المادي لأي جريمة يكون في نطاق جغرافي واحد أي إقليم دولة واحدة، بداية من وقوع السلوك الإجرامي إلى تحقيق النتيجة الإجرامية غير أنّ جرائم الانترنت قد يتجزأ فيها الركن المادي، والذي اشرنا إليه –بالنشاط التقني – قد يتوزع على أكثر من منظومة

[1] المادة (03) من ق.ع.ج تنص على مايلي"يطبق قانون العقوبات على كافة الجرائم التي ترتكب في اراضي الجمهورية .
كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجزائية"

[2] عمر عبيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان وفقا للمعطيات التكنولوجية المعاصرة ، رسالة دكتوراه في القانون الجنائي ،كلية الحقوق ،جامعة القاهرة ،2006، ص1.

[3] عمر عبيد محمد الغول،المرجع السابق،ص 7.

معلوماتية التي تكون ضمن إقليم دولة غير دولة ارتكاب السلوك الإجرامي، كالتلاعب بالبيانات أو المتاجرة بها أو تخريبها الذي يتم في نطاق إقليم دولة ولكن النتائج لا تتحقق إلا بإقليم دولة أخرى وهنا نكون أمام ما يعرف بتنازع القوانين، والتي انقسم الفقه بشأنها إلى ثلاثة اتجاهات رئيسية، أي أنّ الأصل أنّ الاختصاص القضائي الدولي قد تنازعه ثلاث اتجاهات، قد عني الاتّجاه الأول بوقوع السلوك الإجرامي كمعيار لتحديد الاختصاص في المقابل ذهب اتّجاه أخر الاخد بمعيار مغاير للاتجاه الأول بان اقر انّ مكان تحقق النتيجة الإجرامية هو الذي يحدد اختصاص القضائي للدولة ، وبين هذا وذاك رأي ثالث أخد بالمعيارين معا ولكن بشروط معينة.

أ–الاتجاه الأول:معيار السلوك الإجرامي لتحديد مكان وقوع الجريمة.

حيث ينعقد الاختصاص للمحكمة التي يقع في دائرة اختصاصها النشاط الإجرامي.لان الاخد بمعيار حصول النشاط الإجرامي هو أيسر في عملية الإثبات وجمع أدلة الجريمة، حيث أن السلطات المختصة في نظرها هي اقرب من مسرح الجريمة[1].

ب–الاتجاه الثاني:مكان تحقق النتيجة كمعيار لتحديد الاختصاص.

إنّ تعرض الاتجاه الأول لمجموعة من الانتقادات انصبت على انّه لا يعير أي اهتمام أو وزن لمكان تحقق النتيجة الإجرامية، وهي الهدف الأساسي من السلوك الإجرامي، في حين أن مكان إتيان السلوك الإجرامي لا يعدو أن يكون مصدر الضرر فقط[2].هذا من جهة، من جهة أخرى فان تقادم الجريمة يحسب من يوم وقوع الضرر أي النتيجة الإجرامية، ناهيك عن التعويض وعلى وقع انتقادات الاتجاه القائل باختصاص القضائي لمكان وقوع السلوك الإجرامي، بنى هذا الاتجاه مبرراته، التي تقول أن الجريمة لابد انّ وحدة واحدة وعدم الفصل بين عناصرها، لتجتمع أركانها

[1] موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا ، طرابلس من 28 . 29 / 10 / 2009،ص14.

[2] موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المرجع السابق ،ص15.

وخصوصا الركن المادي وهو ماتجسده النتيجة الإجرامية، ولكن كالاتجاه الأول لقي هذا الاتجاه النقذ، خصوصا ما تعلق منه بالشروع أو الجريمة الخائبة، وعدم معاقبة على جرائم التي لا يعتد فيها بتحقق النتيجة الإجرامية. وكدأب الآراء والاتجاهات برز اتجاه ثالث.

ج–الاتجاه الثالث. تحقق عناصر الركن المادي معيار تحديد الاختصاص.

قام على أنقاض انتقادات الموجه للاتجاهين ومفاده أنّ الجريمة تقع في كل مكان تتحقق فيه عناصر الركن المادي[1]، أي النشاط والسلوك الإجرامي معا وهنا"يتم تغليب قانون محل تحقق النتيجة إذا كانت الجريمة تامة، ومن قبيل ذلك الجرائم السلوك والنتيجة (الجرائم المادية) في حين يفضل مكان النشاط أو السلوك إذا كانت الجريمة قد توقفت عند الشروع أو كانت من قبيل جرائم السلوك المجرد"[2].

ونـــرى أنّ الاتجاه الثالث هو الاتّجاه الموفق للاخذ به انسجاما مع ذاتية جرائم الانترنـــت، انّ الأصل في هذه الجرائم هو الامتداد الجغرافي العادي واللامادي، أي تتصف بأنّها جرائم عابرة للحدود الوطنية المتعارف عليها، وبذلك هي جامعة للعديد من المسارح الإجرامية، فإذا تعلق الأمر بالسلوك الإجرامي الواقع على إقليم الدولة بكل عناصر الركن المادي فالأصل هو تطبيق القانون الجزائري، وفق مبدأ الإقليمية(والتي وفي نطاقه يمكن تمديد الاختصاص إلى خارج دائرة اختصاص السلطات المختصة بالتحري والتحقيق بالشروط سالفة الذكر)؛ والذي يعد من بين مظاهر ممارسة الدولة لسيادتها، ولكن ليس هو الحال بالنسبة لكل جرائم الانترنت، لانّ طبيعة الانترنت وجرائمه يجعل من هذه الجرائم خاضعة للعديد من القوانين، كأن يقع السلوك في بلد معين والأثر في بلد أخر وغيرها من الحالات والتي تجعل كل هذه الدول تتمسك باختصاصها، بكونها البلد المنوط بتطبيق القانون على هذه السلوكيات الإجرامية.

[1] موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المرجع السابق ،ص16.

[2] موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المرجع السابق،ص17.

ثانيا:المبادئ الاحتياطية في جرائم الانترنت.

تعمد الدولة إلى حماية مصالحها على إقليمها الوطني، وهذا الأصل؛ ولكن حين تشكل الاعتداءات تهديدا لمصالحها،وخارج حدود إقليمها لابد عليها من إعمال مبادئ استثنائية حماية لمصالحها ومواطنيها وبالمقابل دون الاعتداء على سيادة الدولة الأخرى.

أ-مبـــدأ العينية.

إنّ المشرع الجزائي في كل نص من نصوص القسم الخاص يفصح عادة على ثلاثة أمور،ماهية المصلحة المحمية أو الحق الجدير بالحماية والذي يستهدف بالاعتداء الفعل الضار المكون للجريمة،صور السلوك المضّر بهذه المصلحة أو بهذا الحق المحمي، والذي يتكون منه الجريمة،الجزاء المحدد خصيصا لهذه الجريمة.[1]

وللدولة كشخصية اعتبارية، مصالح وحقوق عامة تعتد إلى حمايتها عن طريق تجريم الأفعال التي تضر بها أو تعرضها للخطر بوضع الجزاء الرادع لها، والمصالح والحقوق العامة التي تهم أي دولة هي:

التي تنبثق عن كيان الدولة ذاته كشخص من أشخاص القانون الدولي، أو عن استقلالها وسيادتها وسلامتها أو عن علاقتها الدولية؛ أوهي التي تنبثق عن القانون الأساسي ونظام الحكم للدولة وسلطاتها العامة، وعن وحدة الشعب وأمنه واستقراره وعدم النيل منه[2].

ولما لم يكن بإمكان مبدأ الإقليمية حماية كل المصالح المتعلقة بالدولة وحماية كامل سيادتها اوجبت الضرورة الملحة لمجابهة العجز الذي يكتنف مبدأ الإقليمية[3]، خصوصا في جرائم الانترنت

[1] سمير عالية، الوجيز في شرح الجرائم الواقعة على دراسة أمن الدولة، دراسة مقارنة، المؤسسة الجامعية للدراسات والنشر والتوزيع، الطبعة الأولى، 1999، ص18.

[2] سمير عالية، المرجع السابق، ص45.

[3] ناصر عيسى بن صليهم، مبدأ العينية وأثره في مكافحة الجرائم العابرة للحدود الدولية دراسة مقارنة،رسالة ماجستير في العدالة الجنائية ،جامعة نايف للعلوم الأمنية، الرياض ،المملكة العربية السعودية، 1430هـ-2009م. المرجع السابق ،ص.39

التي تتحقق أركانها على أكثر من إقليم افتراضي، حيث أن مبدأ العينية له ما يبرره إذا تعلق الأمر بحماية المصالح الوطنية خارج إقليم الدولة حتى وان كان افتراضي، غير ملموس وهو حال مسرح الجريمة في جرائم الانترنت، وهو ما جعل المشرع إضافة إلى المادة (588) من قانون الإجراءات الجزائية العمل بمبدأ العينية يضيف المادة (15)من القانون (09-04)والتي تنص على أن المحاكم الجزائرية وحدها تختص بالنظر في جرائم تكنولوجيات الإعلام والاتصال أي جرائم الانترنت ولكن بشروط:

1-أن يتعلق الأمر بجرائم تكنولوجيات الإعلام والاتصال.

2-أن ترتكب الجريمة خارج الإقليم الوطني[1] .

3-أن يكون المرتكب للجريمة أجنبيا.

4-أن يستهدف مؤسسات الدولة الجزائرية الدفاع الوطني المصالح الإستراتيجية للاقتصاد الوطني.

ورغم أنه ومن الناحية النظرية هو حل سليم لتطبيق القانون الجزائري، وبالتالي مجمل الإجراءات الخاصة بالإثبات الجزائي وإجراءات الحصول على الأدلة الجنائية الإلكترونية أو العادية لمحاكمة المتهم؛ إلا أنّه يصطدم بالعديد من حالات الواقعية ومن بينها اختلاف النظم الإجرائية والعقابية مثلا: ما هو مجرم في الجزائر هو مباح في فرنسا، بالإضافة إلى عرف عدم تسليم المواطنين لدولة أخرى، وهي من بين صعوبات التي تواجه التعاون الدولي[2]، لهذا تم تجاوز هذه العمليات عن طريق التعاون الدولي وبالأخص المساعدة القضائية والإنابة القضائية، لذلك فمن الملاحظ وبصورة جلية أن جرائم الانترنت لا تستجيب إلى العديد من معايير الاختصاص التقليدية، إن صح التعبير

[1] الإقليم"هو المجال الذي تمارس فيه الدولة سيادتها ويمتنع عليها أن تتعداه" ومن مشتملات الإقليم، الأرض أو البر، الإقليم المائي أو البحري، والإقليم الجوي. فوزي أو صديق، الوافي في شرح القانون الدستوري الجزائري ،ديوان المطبوعات الجامعية، الجزء الأول،نظرية الدولة، بن عكنون ، الجزائر، 2003، ص77.

[2] حسين بن سعيدالغافري، السياسة الجنائية في مواجهة جرائم الانترنت،المرجع السابق،ص291.

لذلك لابد من حُلولٍ تتجاوز هذه المعايير، طبعا ليس حلولا وليدة الصدفة بل مبنية على دراسات نظرية وعملية في نفس الوقت، تتناسب والجانب التقني لهذه الجرائم لذلك كان من المناسب ما أورده المشرع في القانون(09-04)وبالضبط في مادته (15)منه وان يجسد ذلك عن طريق الاتفاقيات الثنائية والجماعية.

إلاّ انّه وبالنظر إلى تطبيق مبدأ العينية نجد انّه ينتهك سيادة الدولة التي وقعت عليها الجريمة باعتبار المسرح الافتراضي هو إقليم الدولة غير المعلن، من ناحية ومن ناحية أخرى قد يبدو صعب التطبيق خصوصا اذا تعلق الأمر بالجاني الحامل لجنسية الدولة التي تم فيها الاعتداء على مصالح الدولة المعتدى عليها، فالأكيد أنّ الدولة لن تسلم رعاياها لدولة أجنبية من هنا كان لابد من إعمال مبدأ المعاملة بالمثل، وإبرام الاتفاقيات الثنائية والجماعية، لكي يعطي هذا المبدأ النتائج المرجو لراب النقص الذي يشوب مبدأ الإقليمية وما يترتب عليه من عدم حماية لمصالح الدولة في جرائم الانترنت خصوصا[1].

ب–مبدأ الشخصية.

وهو من المبادئ الاحتياطية للاختصاص القضائي، **ويعني** أن يطبق على كل من يحمل جنسية الدولة بصرف النظر عن مكان وقوع الجريمة والمصالح المحمية التي انتهكت نتيجة وقوع الجريمة[2]،وهذا مانص عليه المشرع الجزائري في المادة (582) من ق.ا.ج.ج كالأتي:"كل واقعة موصوفة بأنها جناية معاقب عليها من القانون الجزائري ارتكبها جزائري في خارج إقليم الجمهورية يجوز أن تتابع ويحكم فيها في الجزائر.

[1] عمر عبيد محمد الغول، المرجع السابق،ص187-188.

[2] سامح احمد البلتاجي موسى،المرجع السابق،ص409.

غير انّه لا يجوز أن تجري المتابعة أو المحاكمة إلاّ إذا عاد الجاني إلى الجزائر ولم يثبت انه حكم عليه نهائيا في الخارج وان يثبت في حالة الحكم بالإدانة انّه قضى العقوبة أو سقطت عنه بالتقادم أو حصل على العفو"

ومن كل ماسبق فان مبدأ الشخصية في حال أن طبق كما هو من الناحية النظرية فسيكون مبدأ فعَّال في جرائم الانترنت،حيث يرتكز في الأصل على تجنب فرار من يحملون جنسية الدولة من الملاحقة الجزائية عند ارتكابهم السلوك الإجرامي خارج إقليم الدولة أواكثر، ويمكن تجسيد ذلك على المسرح الافتراضي، لكن ورغم إمكانية تطبيقه نظريا، فالأكيد انّه يصطدم بالكثير من العقبات وأولها سيادة الدولة،وتنوع النظم القانونية.

ولتطبيق مبدأ الشخصية لا بد من توافر شروط معينة ،أن يكون المتهم جزائري الجنسية عند ارتكابه الجريمة ،التي يجب ان تكون إماّ جناية او جنحة ،معاقبا عليها في القانون الجزائري والأجنبي، أن يعود المتهم إلى ارض الوطن، وما دامت هذه الجرائم جرائم عابرة للحدود الوطنية، كان لابد من وجود تعاون دولي سواء قضائي أو امني لمتابعة المجرمين، وبالتالي إثبات الجريمة.

الفرع الثالث:الهيئات الوطنية المختصة في الوقاية جرائم الانترنت.

عملت السلطات المختصة و على رأسها وزارة العدل على تكوين قضاة و كذا ضباط شرطة قضائية في الخارج، من اجل مواجهة النقص الحاصل في الخبرة. كما نصت المادة (14) من القانون (09-04)على المهام المنوطة بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحته[1]والتي فصلت فيها المادة (4) من المرسوم الرئاسي رقم(15-261) مؤرخ

[1] المادة 14 من القانون 09- 04 "تتولى الهيئة المذكورة في المادة 13 أعلاه خصوصا المهام الآتية :

أ- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته.

ب- مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشان الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال بما في ذلك تجميع المعلومات و انجاز الخبرات القضائية

ج -تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعريف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و تحديد مكان تواجدهم".

في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015[1]، يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها .

إنّ ملازمة جرائم الانترنت لخصائص معينة، أدى إلى إفراد المشرع الجزائري أجهزة خاصة بهذه الجريمة لجمع الأدلة الخاصة بها، على رأسها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته-ذات الاختصاص الأصيل والوحيد والتي يقع مقرها ببلدية حيدرة الجزائر العاصمة-، ولكن هذا لم يمنع المشرع الجزائري استحداث معاهد وطنية ومراكز ومصالح متخصصة قبل تنصيب الهيئة، لعبت دورا مميزا في كشف هذا النوع من الجرائم وملاحقة المجرمين لهذا كان لابد من معرفة أهم المهـام المناطة بالهيئة الوطنية (أولا)ومهام باقي المعاهد والمراكز والمصالح في مجال جمع الدليل لاثبات جرائم الانترنت(ثانيا)

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

للوقايـة من جرائم الانترنت ومكافحتهاأنشأ المشرع الجزائري بموجب القانـون(09-04)وبالتحديد المادة (13) بقولها" تنشا هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم".

ونظرا لحداثة الدراسات في مجال الهيئات المتخصصة في مكافحة جرائم تكنولوجيا الإعلام والاتصال في القانون الجزائري، لم نجد دراسات أو أبحاث سابقة لذالك حاولنا التركيز في هذا البحث على تحليل القوانين والمراسيم المنظمة لهذا الموضوع، ليظهر مـن خـلال القانون(09-04) والمرسوم الرئاسي رقم (15-261) السالف الذكر والذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي وضعها المشرع الجزائري لتجسيد دور الهيئة الوطنية لمكافحة جرائم الانترنت في تولي الجانب الرقابي والقضائي في

[1] ج.ر رقم 53 ليوم 8 اكتوبر 2015ص16.

ما يخص جرائم الانترنت، ومهام التعاون الدولي المناط بها من اجل الحصول على الدليل الجنائي الالكتروني في المرتبة الأولى.

تختص الهيئة الوطنية بمكافحة جرائم الانترنت والوقاية، بما يجعلها متميزة عن غيرها من المراكز المختصة أو المعاهد، والتي انشات في فترات وجيزة من اجل مواكبة وقمع الجريمة التي اتسمت بالسرعة والانتشار، وذالك في إطار قانوني يعد الأساس في القيام بمهامها ، في إطار هيئة[1] متكونة

من لجنة مديرة[2] التي تكلف بما جاء في المادة (8) من المرسوم الرئاسي(15-261) سالف الذكر وخصوصا"... توجيه عمل الهيئة والإشراف عليه ومراقبته،..دراسة كل مسألة تخضع لمجال اختصاص الهيئة، لاسيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الالكترونية النصوص عليها في المادة 4 من القانون رقم (09-04) المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت سنة 2009 والمذكور أعلاه،...القيام دوريا بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة، للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة".

ومديرية عامة[3] ومديرية للمراقبة الوقائية واليقظة الالكترونية والتي تكلف وفق المادة (11)من المرسوم الرئاسي(15-261) سالف الذكر كما يلي" : تكلف مديرية المراقبة الوقائية واليقظة الإلكترونية على الخصوص، بما يأتي:

---

[1] المادة (6)من المرسوم الرئاسي رقم (15-261) تضم الهيئة:

-لجنة مديرة.-مديرية عامة.-مديرية للمراقبة الوقائية واليقظة الإلكترونية.-مديرية للتنسيق التقني.مركز للعمليات التقنية.-ملحقات جهوية.

[2] المادة(7): يرأس اللجنة المديرة الوزير المكلف بالعدل، وتتشكل الأعضاء الآتي ذكرهم:

-الوزير المكلف بالداخلية.-الوزير المكلف بالبريد وتكنولوجيات الاعلام والاتصال.-قائد الدرك الوطني.المدير العام للأمن الوطني.-ممثل عن رئاسة الجمهورية.-ممثل عن وزارة الدفاع الوطني.-قاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

يعين ممثلا رئاسة الجمهورية ووزارة الدفاع الوطني بموجب مرسوم رئاسي.

[3] المادة 10: يتولى المدير العام الصلاحيات الآتية على الخصوص:

- تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول.
- إرسال المعلومات المحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية المختصة.
- تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم.
- جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- تنظيم و/أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والاتصال، وحول المخاطر المتصلة بها.
- تنفيذ توجيهات اللجنة المديرة.
- تزويد السلطات القضائية ومصالح الشرطة القضائية، تلقائيا أو بناء على طلبها، بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

- السهر على حسن سير الهيئة.
- السهر على تنفيد برنامج عمل الهيئة.
- تنشيط نشاطات هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها.
- تحضير اجتماعات اللجنة المديرة.
- تمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية.
- تمثيل الهيئة لدى القضاء وفي جميع أعمال الحياة المدنية.
- ممارسة السلطة السلمية على مستخدمي الهيئة.
- السهر على احترام قواعد حماية السر في الهيئة.
- السهر على القيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين المعنيين في الهيئة.
- إعداد التقرير السنوي لنشاطات الهيئة وعرضه على اللجنة المديرة للمصادقة عليه.
- ضمان التسيير الإداري والمالي للهيئة.

- وضع مراكز العمليات التقنية والملحقات الجهوية قيد الخدمة والسهر على حسن سيرها وكذا الحفاظ على الحالة الجيدة لمنشأتها وتجهيزاتها ووسائلها التقنية.
- تطبيق قواعد الحفاظ على السر في نشاطاتها.

و مديرية للتنسيق التقني[1] و مركز للعمليات التقنية[2] وملحقات جهوية.

ثانيا:مراكز وأقسام والمعاهد المختصة بجرائم الانترنت[3].

من قراءتنا لنص المادة(21)[4]من المرسوم الرئاسي(15-261)، أصبح للهيئة الاختصاص الأصيل في جرائم الانترنت وخصوصا إذا تعلق الأمر بإجراء المراقبة الالكترونية للاتصالات الوقائية، وقبل إنشاء الهيئة انعقد الاختصاص لسلطات الضبطية المختصة والتي تم

---

[1] **المادة** (12) المرسوم الرئاسي(15-261): تكلف مديرية التنسيق التقني على الخصوص بما يأتي:

- إنجاز الخبرات القضائية في مجال اختصاص الهيئة.
- تكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها.
- إعداد الاحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- القيام بمبادرة منها أو بناء على طلب اللجنة المديرة، بكل دراسة أو تحليل أو تقييم يتعلق بصلاحيتها.

تسيير منظومة الإعلام للهيئة وإدارتها.

[2] المادة (13): يزود مركز العمليات التقنية بالمنشآت والتجهيزات والوسائل المادية وكذا بالمستخدمين التقنيين الضروريين لتنفيذ العمليات التقنية لمراقبة الاتصالات الالكترونية.ويتبع هذا المركز مديرية المراقبة الوقائية واليقظة الالكترونية ويتم تشغيله من طرفه.

[3] الرائد منير جلاب، دور الدرك الوطني في ميدان محاربة جرائم المعلوماتية،الملتقى الوطني، الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري،المركز الجامعية احمد زبانة، غليزان7و8 فبراير2017 وعبد الرحمان حملاوي، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية،بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة16و17 نوفمبر2015،كلية الحقوق،جامعة بسكرة.و عز الدين عز الدين،الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة16و17 نوفمبر2015،كلية الحقوق،جامعة بسكرة.

[4] **المادة**(21)من المرسوم الرئاسي(15-261):" قصد الوقاية من الأعمال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة، تكلف الهيئة حصريا بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية تحت سلطة قاضي مختص، ووفقا للأحكام المنصوص عليها في المادة 4 من القانون رقم (09-04)المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت سنة 2009 والمذكور أعلاه".

ذكرهاسابقا[1]،لكن وبعد انتشار الجريمة وتعدد صورها وحتى أدلة إثباتها وخصوصية الإجراءات حاولت الجزائر مسايرة التطور والاقتداء ببعض الدول الأجنبية، فأوجدت مراكز وكذا أقسام خاصة بجرائم الإعلام الآلي والمعلوماتية تابعة للأمن الوطني أو الدرك الوطني.

أ–مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها[2]:

هو الهيكل متخصص تابع لقيادة الدرك الوطني، يقع مقره بالجزائر العاصمة بالدائرة الإدارية لبئر مراد رايس،ولممارسة صلاحياته،ينقسم قسم اليقظة المعلوماتية،قسم التحقيقات المعلوماتية،قسم الأمن الرقمي،مصلحة التقنية والاستغلال، مصلحة الإدارة والوسائل.

ومن صلاحيات المركز انه يكلف بمايلي:

– ضمان يقظة عامة ومستمرة على شبكة الانترنيت؛

–الوقاية من كل أنواع الجرائم المرتبطة بتكنولوجيات الإعلام والإتصال و مكافحتها؛

–مساعدة السلطات القضائية وإجراء الخبرة التقنية المتعلقة بالجرائم المرتبطة بتكنولوجيات الإعلام والإتصال؛

–تقديم المساعدة للتنظيمات العمومية الوطنية، في ما يتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والإتصال ومكافحتها؛

–تقديم المساعدة لوحدات الدرك الوطني المكلفة بالشرطة القضائية لمعاينة الجرائم التي سهل إرتكابها أو المرتبطة باستعمال أنظمة الإعلام الآلي وتكنولوجيات الإعلام والإتصال، جمع أدلتها والبحث عن مرتكبيها؛

[1] تم التعرض إلى إجراء المراقبة الالكترونية في المبحث الثاني من الفصل الأول من الباب الثاني،ص204

[2] المعلومات مقدمة من طرف الرائد المكلف بالاتصال في المركز، الزيارة الميدانية ليوم 4 يناير2018، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها.

-إعداد و تفعيل الاستراتيجية الرقمية للدرك الوطني؛

-المشاركة في إعداد وتفعيل الاستراتيجية الرقمية الوطنية؛

-التمكن والتحكم في قواعد أمن التكنولوجيات وأنظمة الإعلام؛

-المشاركة في تقوية أمن أنظمة الإعلام الوطنية وحماية فضاء المعلومات الوطني؛

-المشاركة في إعداد القوانين والنظم المسيرة لمجال تكنولوجيات الاعلام والاتصال؛

-إنشاء علاقات تنسيق وتعاون مع مختلف المتدخلين في مجال تكنولوجيات الإعلام والاتصال.

ب-المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

أحدث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وأخذ تسميته وحدد قانونه الأساسي بموجب المرسوم الرئاسي رقم (04 -183)[1].

1-نُظِّم المعهد حسب ما جاء في المادة (06) من المرسوم الرئاسي الذي أحدث بموجبه على النحو التالي:

-مديرية الأدلة الجنائية وتظم أربعة (04) مديريات:

-المديرية الفرعية للتحقيقات العلمية والتقنية؛

-المديرية الفرعية للتحاليل الفيزيوكيميائية، الإعلام الآلي والإلكترونيك (دائرة الإلكترونيك والإعلام الآلي تتكفل بكل ما يخص برامج الإعلام الآلي (سرقة، تحطيم...إلخ)، مراقبة الشرائح الالكترونية؛ التزييف في ميدان الإعلام الآلي وكل ما يتعلق بالهاتف النقال)؛

-مديرية الدراسات والبحث في علم الإجرام.

[1] المرسوم الرئاسي رقم(04-183) المؤرخ في 8 جمادى الأولى عام 1425هـ الموافق 26 يونيو سنة 2004 ، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر رقم 41 ليوم 27 يونيو 2004،ص18.

-مصلحة التنظيم والمناهج.

-مصلحة الإدارة و الوسائل.

2- المهـــام:

-إجراء، بناء على طلب من القضاة والمحققين أو السلطات المؤهلة، الخبرات و الفحوص العلمية التي تخضع لإختصاص كل طرف في إطار التحريات الأولية والتحقيقات القضائية، بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح؛

-تقديم مساعدة علمية أثناء القيام بالتحريات المعقدة بإستخدام مناهج الشرطة العلمية والتقنية الرامية إلى تجميع و تحليل الأشياء والآثار والوثائق المأخوذة من مسرح الجريمة؛

-المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام؛

-تصميم بنوك معطيات وانجازها طبقا للقانون، بما في ذلك تلك الخاصة بالبصمات الجينية التي ستكون في متناول المحققين والقضاة بغرض وضع المقاربات واستخلاص الروابط المحتملة بين المجرمين وأساليب النشاط الإجرامي؛

-المشاركة بصفته هيئة تضمن الفحوص والخبرات في مجال عالم الإجرام، في تحديد سياسة جنائية مثلى لمكافحة الإجرام؛

-المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيات الدقيقة؛

-العمل على ترقية البحث التطبيقي وأساليب التحريات التي ثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي؛

-المشاركة في تنظيم دورات تحسين المستوى والتكوين ما بعد التدرج في تخصصات العلوم الجنائية؛

-تصور الأبحاث الموكلة إلى الغير و ضمان متابعتها و تقديرها[1].

ج-المصلحة المركزية للتحريات الجنائية:

المصلحة المركزية للتحريات الجنائية على مستوى قيادة الدرك الوطني تشارك وتدعم الوحدات الإقليمية في التحقيقات،التي من طبيعتها، تتطلب كفاءة مهنية ووسائل تقنية للتحري القضائي المتخصص خاصة في مجال الجرائم الكبرى، الجريمة المنظمة، الإرهاب والتخريب الجنوح المالي والاقتصادي والمتعلق بتكنولوجيات الإعلام والاتصال، وتكلف من جهة أخرى، بربط علاقات تعاون مع مختلف الأجهزة الوطنية والدولية المتخصصة، بما فيها المكتب الوطني المركزي الانتربول في إطار مكافحة الجريمة المنظمة، في حالة ما إذا الموارد البشرية و "INTERPOL"[2]

[1] الرائد منير جلاب، دور الدرك الوطني في ميدان محاربة جرائم المعلوماتية،الملتقى الوطني، الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري،المركز الجامعية احمد زبانة، غليزان7و8 فبراير2017

[2]الانتربول، يتمثل دور الإنتربول في تمكين أجهزة الشرطة في العالم أجمع من العمل معا لجعل العالم أكثر أمانا. والبنية التحتية المتطورة للدعم الفني والميداني التي تملكها المنظمة تساعد على مواجهة التحديات الإجرامية المتنامية التي يشهدها القرن الحادي والعشرون.

في1914 انعقاد المؤتمر الأول للشرطة الجنائية الدولية في موناكو. ضباط شرطة ورجال قانون وقضاة من 24 بلدا يجتمعون للتباحث بشأن إجراءات التوقيف، وأساليب التبيّن، والسجلات المركزية للمجرمين الدوليين، وإجراءات التسليم.

1923إنشاء اللجنة الدولية للشرطة الجنائية واختيار فيينا (النمسا) مقرا لها، بمبادرة من الدكتور يوهانس شوبر، رئيس شرطة فيينا.

1956إثر اعتماد قانون أساسي معاصر، تغيير اسم اللجنة الدولية للشرطة الجنائية ليصبح المنظمة الدولية للشرطة الجنائية (الإنتربول)، واستخدام الاسم المختصر م د ش ج – إنتربول أو الإنتربول فقط. المنظمة تصبح مستقلة عن طريق جمع المساهمات من البلدان الأعضاء والتعويل على الاستثمارات باعتبارها وسيلة التمويل الأساسية.

https://www.interpol.int/ar/%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D8%B9%D9%86-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D8%A8%D9%88%D9%84/%D9%84%D9%85%D8%AD%D8%A9-%D8%AA%D8%A7%D8%B1%D9%8A%D8%AE%D9%8A%D8%A9

،إنضمت الجزائر إلى المنظمة الدولية للشرطة الجنائية – أنتربول، أثناء إنعقاد الجمعية العامة للأنتربول بهلسنكي/فنلندا، خلال شهر أوت 1963، بمشاركة 53 بلدا، ممثلة بالمكتب المركزي الوطني، حيث يعمل المكتب المركزي الوطني تحت الوصاية المباشرة لمديرية الشرطة القضائية/المديرية العامة للأمن الوطني، و يباشر مهامه وفقا لنصوص التشريعات الوطنية، ملتزما بالأطر القانونية المسيرة للمنظمة الدولية للشرطة الجنائية – أنتربول.

http://www.algeriepolice.dz/?-%D8%A7%D9%84%D8%AF%D9%88%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D8%A7%D8%A8%D9%82%D8%A9

الوسائل المادية المقحمة في بداية التحقيق تستلزم تدعيم تكميلي، فان لمدير التحقيق إمكانية طلب يد المساعدة عن طريق السلم القيادي للاستفادة من إمكانيات هذه الهيئة.

د–مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن :

هي مصلحة أوكلت لها مهام معينة مشار إليها في المادة(5) و(6) من المرسوم الرئـــــــاسي رقم (14-183)[1]، حيث أنّ من بين هذه المهام، المساهمة في الوقاية من الإجرام المتصل بالتكنولوجيات الجديدة للإعلام والاتصال وفي قمعه.والتي تم الإشارة إليهم باعتبارهم من أعوان الشرطة القضائية، المكلفين بمهام في إطار جرائم الانترنت والذين يتم تحديد عددهم بموجب قرار مشترك بين وزارة العدل والدفاع الوطني[2].

لذلك فان الضباط المؤهلين بالقيام بالمهام وبمعالجة الآثار القضائية وكذا تنفيذ الانابات القضائية والطلبات وجمع المعطيات وكذا معالجة ملفات التعاون القضائي المتبادل دون الخروج عن هذه المهام والصلاحيات هم فقط أعوان مصلحة التحقيق القضائي لمديرية الأمن الداخلي المحددين بموجي القرار المشترك بين وزارة العدل والدفاع الوطني دون غيرهم؛ كأعوان مختصين داخل الهيئة الوطنية لمكافحة تكنولوجيات الإعلام والاتصال في ظل احترام الإجراءات الجزائية وقانون العقوبات.

حيث تمارس هذه المصلحة مهامها بتسير من ضابط سام من وزارة الدفاع الوطني وفق المادة (2) من المرسوم الرئاسي رقم(14-183) سالف الذكر،على أن تمارس هذه المهام تحت مراقبة

[1] المرسوم الرئاسي رقم (14-183) مؤرخ في 13 شعبان عام 1435 الموافق 11 يونيو سنة 2014، يتضمن إنشاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن ،ومهامها وتنظيمها،ج ر رقم 32 ليوم 12 يونيو سنة 2014،ص4.

[2] المادة 20 من المرسوم الرئاسي رقم(15-262) السالف الذكر" ... كما تزود بضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني يحدد عددهم بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل ، والدفاع الوطني و الأمن الوطني والداخلية.

وتزود أيضا بمستخدمي الدعم التقني والإداري ويجلب هؤلاء المستخدمون من ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني و الأمن الوطني."

النائب العام وكذا رقابة غرفة الاتهام وهذا بإقليم الاختصاص وهو ماجاءت به المادة (3) من المرسوم سالف الذكر؛بموجب تراخيص تسلمها السلطات القضائية المختصة[1].

المطلب الثاني: التعاون الدولي في جرائم الانترنت.

إنّ الأكيد أنّ الجريمة عبر الانترنت ذات بعد دولي عابر للحدود الوطنية، وأنّ من بين الإجراءات المهمة التي تساعد في إثبات الجريمة والحد من الإشكالات المطروحة من هذه الناحية هي وجود تعاون دولي[2]، حقيقي بين الدول، بعدما أصبحت الحدود الواقعية تختلف عن تلك الافتراضية، والتي بدورها لم تعد، تشكل حاجز لارتكاب السلوك الإجرامي، بحيث امتدت لأكثر من إقليم ولا مجال أن التعاون الجنائي الدولي في مجاله الإجرائي، أضحى ضرورة لقمع هذه الجريمة عن طريق تسهيل طرق جمع أدلتها الجنائية الإلكترونية، فأي دولة مهما بلغ تطورها في مجال التكنولوجيات الحديثة لا تستطيع بمفردها القضاء على جرائم الانترنت، فالأهم من وجود ترسانة تشريعية، هو قابلية هذه القوانين للتطبيق فعليا، والذي يتم عن طريق التعاون بين سلطات في التحري والتحقيق وتبادل المعلومات مع الدول .

يعتبر التعاون الدولي من أهم الوسائل في جرائم الانترنت، فهو يهدف إلى تحقيق العدالة على المستوى الدولي، وبما انّ خصائص جرائم الانترنت أنها ظاهرة جمعت بين الوطني والدولي، كان لابد من وجود هذا النوع من التعاون في إطار المبادئ الدستورية والقانونية للدولة الجزائرية.

[1] المادة 9 من المرسوم الرئاسي رقم(14-183) "يخضع تنفيذ الدعوى الشرطة القضائية بعنوان صلاحيات مصلحة التحقيق القضائي المنصوص عليها في المواد 4و5 و6و8 أعلاه، إلى التراخيص الضرورية التي تسلمها السلطات القضائية المختصة .

[2] تعاون الدولي "هو اشتراك ثنائي بين دولتين أو جماعي بين عدة دول في توحيد إجراءاتها القضائية كذلك المتعلقة بالأدلة الجنائية أو الإدلاء بالشهادات تبادل المعلومات والمساعدة القانونية المتبادلة ... وغيرها من الإجراءات المشابهة، بما في ذلك الترتيبات التعاونية الأخرى المتفق عليها بين الأطراف المعينة والتي تهدف إلى تنفيذ الأحكام الجنائية . متعب بن عبد الله السند، التعاون الدولي في تنفيذ الأحكام الجنائية وأثره في تحقيق العدالة، رسالة ماجستير، كلية الدراسات العليا،جامعة نايف العربية للعلوم الامنية، الرياض، المملكة العربية السعودية، 1432هـ-2011م،ص10.

وترتبط فكرة التعاون الدولي بفكرة الجريمة عبر الوطنية[1] أو الجريمة العابرة للحدود الدولية، وهما جريمتين غير إقليميتين في أغلب الأحيان مما يؤدي إلى توزع أركانها على عدة أقاليم دولية من جهة ومن جهة أخرى يسهل طمس وإتلاف أدلة الإثبات، مما يشكل صعوبة في مواجهة القوانين الداخلية لهذا النوع من الجرائم[2]، ومن مظاهره الاتفاقيات والمؤتمرات.

الفرع الأول: التعاون القضائي الدولي.

يعد التعاون القضائي الدولي من ابرز مظاهر التعاون الدولي في مجال مكافحة جرائم الانترنت وملاحقة المجرمين بعد إثبات ونسبة الجريمة إلى أولائك عابري الحدود، وهو ماجسده المشرع الجزائري في إطار القانون (09-04)، كما أنّ هناك تعاون امني دولي تقوم به هيئات دولية كالانتربول أو الشرطة الجنائية الدولية والذي من أهم أدواره تفعيل التعاون بين أجهزة الشرطة التابعة للدول الأعضاء.

أولا:تعريف التعاون القضائي الدولي.

ويعني تبادل العون والمساعدة لتحقيق هدف معين[3]،والأصل أن يتم التعاون الدولي في صورة مساعدة قضائية تتم عن طريق المساعدة القضائية اللازمة في التحري والتحقيق وتبادل المعلومات مع السلطات المختصة والأجهزة بمختلف الدول عن طريق الحصول على مختلف التسجيلات للاتصالات الالكترونية وغيرها، حيث أن المشرع الجزائري قد أوجد استثناء، فالأصل أن هذه المساعدة تتم عن طريق التمثيل الدبلوماسي أو ما يعرف بالقنوات الدبلوماسية كما هو منصوص

[1] الجريمة عبر الوطنية"الجريمة التي ترتكب خارج إقليم الدولة ويكون احد عناصرها أجنبيا عن الدولة وتضر بالمصالح الدولة الأساسية والجوهرية"فهد ناصر عيسى بن صليهم، مبدأ العينية وأثره في مكافحة الجرائم العابرة للحدود الدولية دراسة مقارنة،رسالة ماجستير في العدالة الجنائية ،جامعة نايف للعلوم الأمنية، الرياض ،المملكة العربية السعودية، 1430هـ-2009م.

[2] سامح احمد البلتاجي موسى، المرجع السابق، ص498.

[3] فهد عبد الله العازمي،المرجع السابق،ص504.

عليه في المادة (721)ق.ا.ج.ج[1]، لكن ومواكبة للتطور السريع والمستمر وفي حالة الاستعجال، (وهذا في محاولة إلى إزاحة عوائق التعاون الدولي ومن بينها المساعدة القضائية، بتيسير الاتصال وتنسيق العمل على أساس احترام السيادة والمعاملة بالمثل)،يتم جمع الأدلة ومن بينها الأدلة الجنائية الالكترونية بالطرق السريعة والتي تتجسد في الفاكس، والبريد الالكتروني ولكن بشروط معينة[2]. إنّ الأكيد أنّ جرائم الانترنت،جريمة ترتكب عبر العديد من الدول مما توجب تدليل معوقات الحصول على دليل إثباتها وهذا عن طريق التعاون الدولي وتحديد عن طريق المساعدة والإنابة القضائية، كل هذه الإجراءات تحكمها قاعدة المعاملة بالمثل وإلا عد ذلك انتهاك للسيادة الوطنية.

لكن بالمقابل يصطدم هذا الإجراء أي التعاون الدولي بمشكلة تبرز للوجود وهي السيادة الوطنية،كون أنّ التعاون الدولي بكل صوره من مساعدة وإنابة قضائية، تتطلب الدخول إلى الإقليم الدَّولي ليس الواقعي بل الافتراضي عن طريق تتبع المجرمين إلى أنظمة معلوماتية غير وطنية .

إنّ جرائم الانترنت والتي حددنا أنّها يمكن أن تكون الجرائم العادية المرتكبة عبر الانترنت أو جرائم الاعتداء على الانترنت هي جرائم ذات بعد دولي كما ذكرنا سابقا،مما يؤهل الإجراءات الدولية وبالتحديد المساعدة القضائية والإنابة أن تلعب دورا فعالا في الجانب الإجرائي للحصول على الدليل الجنائي الالكتروني وهذا ماعكسه القانون(09-04)[3].

مما سبق الإشارة إليه أن جريمة الانترنت ذات طابع دولي،مما قد يسبب مخاطر تجاوز إقليم الدولة التي انطلق منها السلوك الإجرامي، أو حتى تحققت النتيجة الإجرامية .

[1] المادة (721) ق.ا.ج.ج."في حالة المتابعات الجزائية غير السياسية في بلد أجنبي تسلم الانابات القضائية الصادرة من السلطة الأجنبية بالطريق الدبلوماسي وترسل الى وزارة العدل بالأوضاع المنصوص عليها في المادة 703 وتنفذ الانابات إذا كان لها محل وفقا للقانون الجزائري وكل ذلك بشرط المعاملة بالمثل."

[2] المادة (16) من القانون (09-04).

[3] فايز محمد راجح غلاب،المرجع السابق ،ص259.

وحتى ينجح أي عمل قضائي في مجال جرائم الانترنت، لابد له من تدليل الصعاب أمام أي من العقبات التي يواجهها وهو الحال حين أقر المشرع الجزائري بتمديد الاختصاص في جرائم تكنولوجيات الإعلام والاتصال في حال كان وطني ولكن ليس هو الحال بالنسبة للدولي، فلابد من وجود تعاون دولي جنائي في مجال جرائم الانترنت وبالتحديد التعاون القضائي حيث أنه وبتتبع الاتصالات الالكترونية يؤدي بالضرورة وفي الكثير من الأحيان إلى تجاوز إقليم الدولة الأخرى وهو ما لا يجوز لأنه ينتهك سيادة الدولة لذلك التعاون القضائي بين السلطات كان عليها إيجاد تعاون قضائي بينهما من أجل سهولة هذه الإجراءات الجزائية وإجراء العمل القضائي على أراضي الدولة الأجنبية ولكن بشروط معينة وفي هذا الصدد حدد القانون (09-04) في مادته (13) منه "..." على أن مهام هذه الهيئة أي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته في المادة (14) فقرة ج "... تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم" وما أكدته المادة (4)من المرسوم الرئاسي رقم (15-261) الذي تحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها" ... السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير وتبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

والمادة (11) من نفس المرسوم والخاصة بالمساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم".

ثانيا:التعاون الأمني الدولي.

يمكن تعريفه أي التعاون الدولي الأمني، "تبادل العون والمساعدة وتضافر الجهود المشتركة في مجال التصدي لمخاطر الإجرام وما يرتبط به من مجالات أخرى، مثل مجال العدالة الجنائية ومجال

الأمن أو لتخطي مشكلات الحدود والسيادة التي قد تعترض الجهود الدولية لملاحقة المجرمين وتعقب مصادر التهديد سواء كانت المساعدة المتبادلة قانونية أو قضائية أو شرطية، وسواء اقتصرت على دولتين فقط أو امتدت إقليميا أو عالميا"[1].

لقد وجد التعاون الدولي الأمني مكانا له، في إطار جرائم الانترنت حيث عملت الجزائر على تكييف قوانين خاصة بهذا المجال وفق البيئة الافتراضية، ذلك أن هذا التعاون الأمني هو مطلب أساسي في قمع جريمة الانترنت والحفاظ على النظام العام، إلا أننا نرى وجود فجوة واسعة بين النصوص القانونية، وبين التوعية بمخاطر الانترنت، لذلك هناك عدم تنسيق بين مصالح الأمنية والسلطات المختصة وبين الأفراد وخصوصا في الجانب التوعوي وقد يرجع هذا إلى أسباب عديدة قد نذكر منها.

-عدم التنسيق بين السلطات الأمنية والأفراد بشكل دائم ومستمر حول مخاطر الانترنت بكل القنوات المتاحة كالإعلامية والأيام التحسيسية.

-عدم التنسيق بين السلطات الأمنية والجمعيات في هذا المجال رغم انعدامها على حد ما نعلم

- عدم وجود ممثلين للمجتمع المدني مختصين في التوعية من مخاطر الانترنت بالدرجة الأولى- لأن العمل الأمني أو التعاون الأمني في هذه الجرائم بذّات لا يقتصر فقط على هيئة معنية تقوم بالتنسيق بين الأجهزة، بل أكثر من ذلك التنسيق مع الجمعيات والفرد في حد ذاته.

والأصل في التعاون الأمني الدولي له دور استباقي أي وقائي، قبل أن يكون قمعي، ذلك عن طريق كشف الجريمة من الأعمال التحضيرية إن وجدت[2]، والذي لا يكون إلا بمواكبة إجراءات التحري

[1] خالد بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتواره في الفلسفة في العلوم الأمنية كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية، الرياض. المملكة العربية السعودية . 2006، 1427، ص38.

[2] سامح احمد البلتاجي موسى،المرجع السابق، ص524.

والتحقيق الخاصة بجرائم الانترنت والتي دأب المشرع للاعتراف بها وتقنينها مند سنة(2006) بتعديله قانون الإجراءات الجزائية وكذا باقي القوانين.

يتجسد هذا التعاون في أجهزة على رأسها الأنتربول وكذا المكتب العربي وهي أجهزة لها مكاتب على المستوى الدول الأعضاء ومنها الجزائر.

الفرع الثاني: صور التعاون القضائي الدولي:

الواقع أنه بعد قراءة نص المرسوم الرئاسي(15-261)يبين، أنّه هناك أسس قد وضعت تهدف إلى إيجاد تعاون دولي حقيقي بأن تكون للجزائر جهود واضحة للتعاون الدولي في مجال الجرائم الخاصة ومن بينها جرائم الانترنت وقبل في إطار الدستور وقانون الإجراءات الجزائية وقانون تكنولوجيات الإعلام والاتصال.

كما يعتمد التعاون الأمني على المساعدة التكنولوجية وتبادل الخبرات بين الدول، ذلك أن كل الاتفاقيات الدولية والإقليمية ذات الصلة دعت إلى ضرورة وجود تعاون دولي في مجال التدريب ونقل الخبرات فيما بينها وهذا ما جسدته المادة(29)من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية .

لذلك كان أن أقرت الجزائر العديد من البرامج الخاصة بتكوين القضاة ورجال الضبطية القضائية، والتي لا يمكن الوصول إلى إكسابهم الخبرة الفنية في هذا المجال عن طريق التدريب، وهي إحدى الإجراءات تحد من إفلات المجرمين وهذا عن طريق ملاحقتهم وإقامة الدليل وإحالتهم إلى المحاكمة ولا يتم إلا وفق مناهج تدريب معينة[1]، ذلك أنه لا يمكن بأي حال من الأحوال قمع جرائم الانترنت داخليا دون أن يكون هناك تعاون دولي إمّا قضائي أو أمني ولكن تواجه هذا

[1] مناهج التدريب،هي جزء من عملية التنمية الإدارية للسلطات المختصة والتي تعتمد على الاستثمار في العنصر البشري، وتشمل بيان المخاطر والتهديدات ونقاط الضعف لشبكة المعلومات وبيان أهم صفات مجرم الانترنت وهي عبارة عن دورات متخصصة لمواجهة جرائم الانترنت،فهد عبد الله العزمي،المرجع السابق، ص653-657.

التعاون العديد من الصعوبات، رغم أنه أي التعاون هو ضرورة وأولوية في مواجهة جرائم الانترنت ونقصد به هنا إجراءات التحري والتحقيق وبالتالي إقامة الدليل لكي لا يفلت المجرم من العقاب ولكن رغم ذلك هناك معوقات تتجسد في عدم وجود نموذج موحد للنشاط الإجرامي، اختلاف النظم القانونية الإجرائية،التجريم المزدوج الذي يعتبر هذا الشرط من شروط تسليم المجرمين.

أولا– المساعدة القضائية:

لما كانت جرائم الانترنت ذات طابع عالمي كما ذكرنا، أي تتجاوز الحدود الإقليمية الطبيعية للدول يستلزم ذلك القيام بمجموعة من الأعمال القضائية خارج الحدود الوطنية أو العكس كمعاينة أو تفتيش أو حجز المعطيات في حال الاتصال عن بعد أو حتى سماع الشاهد المعلوماتي أو اللجوء إلى الإنابة القضائية وتقديم المعلومات اللازمة لتنفيذ التحقيق في جرائم الانترنت[1].

وقد نص المشرع الجزائري على المساعد القضائية المتبادلة في المادة (16) من القانون (09-04)سالف الذكر.حيث انه وفي إطار التحريات والتحقيقات القضائية الجارية لمعاينة جرائم الانترنت يمكن للسلطات المخولة تبادل المساعدة القضائية الدولية في إطار جمع الأدلة الجنائية الالكترونية .

ثانيا: تبادل المعلومات ونقل الإجراءات في جرائم الانترنت.

وهي صورة من صور المساعدة القضائية على المستوى الدولي[2].والتي تسمح بالاتصال المباشر بين الجهات القضائية المختصة، من اجل تبادل المعلومات حول الجريمة والمجرمين على حدّ سواء،وقيام دولة معينة باتخاد الإجراءات جزائية بحيث تكون الجريمة قد ارتكبت على إقليم دولة أخرى ولكن لمصلحة هذه الدولة ،وذلك بتوافر شروط معينة، والمتمثلة في التجريم المزدوج ، على

[1] جميل عبد الباقي الصغير، الجوانب الإجرائية، المرجع السابق،ص79.

[2]وقد أقرت ذلك الاتفاقية الأوروبية حول الجريمة الافتراضية سالفة الذكر،وان الجزائر احدت بما جاء في هذه الاتفاقية رغم عدم المصادقة عليها، والتي جاء في المادة (23) منها تقرر صراحة وجوب توافر التعاون الدولي بين الأطراف وتعميقه وتقليل العوائق بما يوفر اكبر قدر من السهولة والسرعة لتبادل المعلومات والأدلة بين الدول الأطراف.

أن تكون هذه الإجراءات مهمة للوصول إلى الحقيقة، وكل هذه الصور من التعاون الدولي قد وردت في نصوص اتفاقيات الأمم المتحدة لمكافحة الفساد والجريمة المنظمة عبر الوطنية، والاتفاقية العربية للتعاون القضائي الموقعة بين الحكومات (اتفاقية الرياض للتعاون القضائي)[1].

ثالثا: الإنابة القضائية[2].

تتميز الإنابة القضائية في جرائم الانترنت عن باقي الجرائم بأهمية بالغة تتعلق خصوصا بالحفاظ على السيادة الوطنية، والمعاملة بالمثل، حيث يساعد تنفيذ هذا التعاون في الوقت

[1] مرسوم رئاسي رقم (01-47) مؤرخ في 17 ذي القعدة عام1421 الموافق 11 فبراير سنة 2011،يتضمن التصديق على اتفاقية الرياض العربية للتعاون القضائي الموقعةفي الرياض بتاريخ 23 جمادى الثانيةعام 1403 الموافق 6 افريل سنة 1983 وكذا تعديل المادة 69 من الاتفاقية الموافقة عليه في 26 نوفمبر1997 من طرف مجلس وزراء العدل العرب في دور انعقاده العادي الثالث عشر،ج.ر،رقم11 ليوم12فبراير2001،ص3

[2] على الرغم من تزايد جرائم الانترنت بشكل ملحوظ في السنوات الأخيرة، إلا انّ التعاون الدولى وخصوصا الإنابة القضائية الخاصة بمثل هذه الجرائم قليل جدا وهذا راجع بالدرجة الأولى لعدم وجود اتفاقيات ثنائية للتعاون والدليل على ضعف التعاون الدولي هو العدد القليل لحالاته التي تحصلنا عليها رغم أنّ القانون (09-04) صدر منذ اكثر من ثماني سنوات، وهذه معلومات تم الحصول عليها من المركز،بالتاريخ السابق،تبين حالة تنفيذ إنابة قضائية الدولية،الوحدة : فصيلة الأبحاث للدرك الوطني بالجزائر

ملخص القضية :في يوم 13 أكتوبر 2011 بين الساعة 18:30و19:10 تعرض الموقع الحكومي الفرنسي www.ardennes.pref.gouv.fr التابع لمنطقة la Préfecture des Ardennes على شبكة الانترنت، للولوج غير مرخص به من طرف شخص أو عدة أشخاص قاموا من خلال هذا الولوج بالتحكم في الموقع مع تغيير محتواه وهذا باستعمال تقنية حقن SQL ، حيث ترك مخترق هذا الموقع توقيع باسم مستعار nOm_dz على صفحة استقبال الموقع.

بعد الاطلاع على الملفات المرفقة (وعددها 08) مع الإنابة القضائية و التي تتضمن معلومات حول تتبع أنشطة الشخص المشتبه به على الانترنت، صاحب التوقيع nOm_dz مع عناوين IP التي استعملها لذلك، نستخلص ما يلي:

رئيس مصلحة الإعلام الآلي لـ la Préfecture des Ardennes قام بتزويد المحققين الفرنسيين بعناوين IP من بينها عناوين لاتصالات بالموقع تمت من الجزائر خلال الثلاثة أيام التي سبقت اختراق الموقع ، يمكن للمشتبه به أن يكون قد استعملها، هاته العناوين ملك لمزود خدمة الانترنت الجزائري (س).

-لدى تعريف منشئ المدونة باسم nOm_dz لدى الموقع skyrock.com ، تم تعريف عنوان IP الذي استخدمه هذا الشخص لإنشاء هذه المدونة مع تحديد عنوان البريد الالكتروني الذي قام من خلاله بانشائها وهو dzhacker.dz@hotmail.fr مع تعريف عناوين ip لاتصاله بهذا البريد ، لدى microsoft ، من بينها عناوين IP من الجزائر ملك لمزود خدمة الانترنت الجزائري (س).

-بعد التركيز على العناوين الخاصة بالولوج للبريد الالكتروني nOm_dz @hotmail.com ، و إجراء مقاربة شاملة تمكن المحققون من تعريف هوية الهاكر nOm_dz ، و الذي تم توقيفه و تقديمه للعدالة.

المناسب، وهذا ما يتناسب مع طبيعة الدليل الجنائي الالكتروني، وبالتالي عدم ضياع الأدلة والآثار المتعلقة بالجريمة ومن ثم انجاز التحقيقات في الدولة الطالبة للمساعدة القضائية، ويحفظ حقوق المتهمين في الإسراع بمحاكمتهم[1] .

يقصد بالإنابة القضائية طلب اتّخاذ إجراء قضائي من السلطة القضائية المنيبة إلى السلطة المنابة، بأي طريق سواء قضائي أو دبلوماسي –لان الأصل في التعاون الدولي هو الطريق الدبلوماسي–تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها للقيام في إقليمها ونيابة عنها بآي إجراء قضائي،كالتحقيق أو جمع الأدلة متعلق بجريمة دولية من جرائم الانترنت للفصل في مسالة مثارة لدى الدولة الطالبة وخارج نطاق اختصاصها مما يتعذر عليها القيام بالإجراء بذاتها[2]،وتهدف إلى تسهيل الإجراءات الجزائية بين الدول بما يكفل إجراءات التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى ،كسماع شهادة الشهود، والأقوال التي تؤخد على سبيل الاستدلال، وتبليغ السندات القضائية وتنفيذ عمليات التفتيش والحجز، وإجراء المعاينة ...[3]

ومن خلال النصوص القانونية الواردة في التشريع الجزائري تقسم الإنابة القضائية إلى قسمين بحسب ما جاء في نص المادة (721)و(722) ق.ا.ج.ج.

أ–الانابات القضائية المرسلة إلى الخارج:

تنص المادة (721) ق.ا.ج.ج على مايلي:"في حالة المتابعات الجزائية غير السياسية في بلد أجنبي تسلم الانابات القضائية الصادرة من السلطة الأجنبية بالطريق الدبلوماسي وترسل إلى وزارة العدل

[1] خالد بن مبارك القريوي القحطاني، المرجع السابق، ص63.

[2] حازم الحارون،الانابة القضائية الدولية ،المجلة الجنائية القومية، القاهرة،العدد 2،يوليو1988،ص20.

[3] نص المادة 46 الفقرة 13 من اتفاقية الأمم المتحدة لمكافحة الفساد.

بالأوضاع المنصوص عليها في المادة(703)وتنفذ الانابات القضائية إذا كان لها محل وفقا للقانون الجزائري وكل ذلك بشرط المعاملة بالمثل."

ب- الانابات القضائية الواردة من الخارج:

(722)ق.ا.ج.ج"في حالة المتابعات الجزائية الواقعة في الخارج إذا رأت حكومة أجنبية من الضروري تبليغ ورقة من أوراق الإجراءات أو حكم إلى شخص مقيم في الأراضي الجزائرية فيرسل المستند وفقا للأوضاع المنصوص عليها في المادتين (702)و(703) مصحوبا بترجمة عند الاقتضاء ويحصل التبليغ إلى الشخص بناء على طلب النيابة العامة وذلك بواسطة المندوب المختص ويعاد الأصل المثبت للتبليغ إلى الحكومة الطالبة بنفس الطريق وكل ذلك بشرط المعاملة بالمثل."

اذ ا الإنابة القضائية تجد أساسا لها في القانون الوطني والاتفاقيات الدولية ومبدأ المعاملة بالمثل،حيث يتم إرسال الطلب أي طلب الإنابة عن طريق السبل الدبلوماسية، مع العلم أنّ هذا الطريق فيه من التعقيد والبطء مافيه نتيجة احترامه لقواعد معينة وواجبات وهو الحقيقة ما يتعارض مع سرعة هذا العصر وبالتحديد جرائم الانترنت[1]، وهو ما تفطن إليه المشرع الجزائري كما ذكرنا سابقا انه يمكن في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثـل،قبول طلبات المساعدة القضائية المذكورة عن طريق وسائل الاتصال السريعة بما في ذلك الفاكس أو البريد الالكتروني وذلك بقدر ما توفره هذه الوسائط من شروط امن كافية للتأكد من صحتها[2].

وفي الأخير يمكن إجمال مجموع إجراءات التعاون الدولي التي اقرها المشرع الجزائري في المواد (16)و(17)و(18)من القانون (09-04) انّه وبما يتطلب من كشف سريع لجرائم الانترنت وملاحقة مجرميها فانه:

[1] فهد عبد الله العبيد العازمي، المرجع السابق، ص539.

[2] المادة (16) من القانون (09-04).

-يُخول للجهات المختصة الحق في تبادل المساعدة القضائية الدولية بأي صورة من صورها لجمع الدليل الجنائي الإلكتروني.

- لما كان طبيعة الدليل الجنائي الالكتروني، الأصل الثابت فيه سهولة اخفائه وتعديله لمن هم مختصون في شانه أصبح قبول المساعدة ممكناً في حالة الاستعجال بعيدا عن الطرق الدبلوماسية ،بشرط المعاملة بالمثل، وأعمال الاتفاقيات الدولية في هذا المجال.

- إتخاذ الإجراءات التحفظية اللازمة من طرف السلطات المختصة، والواقع أنّ اتخاذ مثل هذا الإجراء لا يكون الاّ إذا كانت هناك معاملة بالمثل أو اتفاقية دولية ذلك أن إجراء التحفظ وخصوصا على الدليل الجنائي الالكتروني، قد يحمل عند تحليله العديد من المعلومات والبيانات التي تتعلق بالدول وسيادتها، خصوصا أنّ المشرع قصد من كل هذه الإجراءات الجرائم الخـاصة، أو الأفعال الموصوفة بجرائم الإرهاب والتخريب أو جرائم المساس بأمن الدولة، أو الدفاع الوطـني أو الاقتصاد الوطني.

على انّــه ورغم وجود اتفاقيات دولية عديدة فيما يخص التعاون الدولي إلا أنّ اختلاف جرائم الإنترنت، عن باقي الجرائم والصعوبات التي تتعلق بإقامة الدليل وكل الإجراءات الخاصة به،كل ذلك يؤدي إلى تعثر الإثبات وإقامة الدليل وبالتالي ملاحقة الجاني، لذلك لابد أن تكون الاتفاقيات الدولية شاملة عند إعدادها على خصوصية جرائم الانترنت والأدلة المتعلقة بها،كما يجب أن تنطوي على الإشارة لمسألة سيادة الدولة في العالم الافتراضي، والمعاملة بالمثل وهو ما جسدته المشرع الجزائري في القانون (09-04) .

وبعد أن تطرقنا إلى هذه النقاط الأساسية، المتمثلة في تحديد الاختصاص وتمديده على المستوى الوطني والدولي، والتعاون الدولي والأجهزة المختصة في اثبات جرائم الانترنت، لابد من تقييم هذا الدليل في نهاية الإجراءات موضوع المبحث الأخيرمن هذا الفصل.

المبحث الثاني:القيمة القانونية للدليل الجنائي في جرائم الانترنت في التشريع الجزائري.

إنّ الأصل، انّه لا يمكن إنكار الدور الايجابي الذي تلعبه تكنولوجيات الإعلام لاتصال وبالضبط الانترنت، في تطوير البحث والتحري وبالتالي الحد من انتشار الجريمة، وتسهيل عمليات التحري لتجنب الأخطاء،وإذا كانت الطرق التقليدية تكفي لإثبات الجرائم العادية، فإنّها تعجز عن إثبات جرائم الانترنت، فالدليل أثر يولد أو حقيقة تنبعث من الجريمة المرتكبة، ويجب لمنطقية هذا الدليل ومصداقيته أن يكون الوصول إليه بطريقة صحيحة بحيث أن الحقيقة التي يعبّر عنها تصل إلى القاضي ميسرة دون تعجل هذا الأخير للوصول إليها[1]، وانّه إن فعل فإن الحقيقة التي تنبعث منه – وهذا حاله – تكون زائفة وغير معبرة عن واقع الدعوى[2]، إذا فان اعتماد أدلة غير الأدلة العادية وطرق لإثبات تختلف عن الطرق العادية أو تكييفها وفق لتطور التقني الحاصل الذي يسير بسرعة هائلة، دون أن يتوقف لبرهة،يفرض على المشرع الأخذ بطرق جديدة من أجل أن تكون عملية الإثبات مبنية على أسس قانونية وعلمية لا تنقص من حجيتها باعتبارها وسائل علمية وتقنية وفي نفس الوقت لا تمثل اعتداء على حرية المتهم وحرماته[3].

لتحقق قيمة ثبوتية للدليل الجنائي في جرائم الانترنت، لابد من وجود ضمانات تحمي الحق في الخصوصية، هذه الضمانات–هذه الضمانات في حالة الإخلال بها يقابلها جزاء جنائي– هي التي تتطلبها مشروعية الحصول عليه، وإذا اكتملا طرفا المعادلة؛ أي وجود ضمانات أساسها النصوص القانونية المطبقة، يكون للدليل في جرائم الانترنت وزناً في عملية الإثبات، لذلك لايبقى للقاضي إلاّ أنْ يقدِّر مدى صلاحية الظروف والملابسات التي قد تمّ فيها الحصول على الدليل، من أجل الحكم وفقه، بإدانة ألمتهم أو نفي التهمة عنه، على أنّ ثبوت قيمة قانونية للإثبات

---

[1] عبد الفتاح بيومي حجازي ،الدليل الجنائي و التزوير في جرائم الكمبيوتر والإنترنت، ص109.

[2] على محمود على حمودة، المرجع السابق،ص37.

[3] احمد ايو القاسم،طبيعة نظرية الإثبات الجنائي العلمي وما تثيره من قضايا فقهية ومشاكل تطبيقية، مجلة كلية الدراسات العليا العدد16 يناير 2007، ص41.

بالدليل الجنائي يرتكز على حماية الحقوق والحريات، بترتيب المسؤولية الجزائية على كل معتد على الحياة الخاصة في مواجهة الفرد أثناء عملية الإثبات أو أي عرقلة أو عدم التزام بما يفرضه القانون للوصول إلى الدليل والتي تعني مشروعية الدليل الجنائي في جرائم الانترنت (المطلب الأول)وتحقيق القيمة الثبوتية لا يكتمل إلاّ باقتناع القاضي بالدليل(المطلب الثاني).

المطلب الأول:مشروعية الدليل الجنائي في جرائم الانترنت.

قلنا أنّ مشروعية الدليل تتمثل في اللجوء إلى الإجراء وفق مانص عليه القانون وفي إطار من النزاهة والشفافية وبعيداً عن الخداع والتدليس من غير المنصوص عليه قانونا ولضرورات التحقيق القضائي-ربما عدم اللجوء النيابة أو قضاء التحقيق لهذه الأساليب في الكثير من الحالات، راجع للنقائض التي سجلت في النصوص القانونية التي تمس بضمانات اللجوء إلى الإجراءات الخاصة خصوصا أنها تمس مباشرة الحياة الخاصة للفرد قبْلَ المتهم-، ولمّا كانت سياسة الإثبات في المواد الجزائية تنتهج المذهب الحر، أي حرية الإثبات[1]، الذي يسمح بصفة عامة بإمكان أن يلجا القاضي بكل حرية لوسيلة الإثبات التي يراها ملائمة، بموجب نص المادة (212) من ق.ا.ج.ج، ولكن وبالمقابل هناك مبدأ أخر يكمل مبدأ الحرية ويقيد القاضي، هو مبدأ الشرعية في الحصول وتقدير الدليل[2] في ذلك هو مشروعية الدليل الجنائي ومنه الدليل الجنائي الالكتروني، وهو الحمل الملقى على عاتق قاضي التحقيق، باعتباره مسؤولا عن إظهار الحقيقة عن طريق جمع كل الأدلة التي تساعد في إظهارها، طبعا هذا في ظل الشروط والضمانات التي اقرها المشرع الجزائري، والتي وبعد دراستها وجدنا أنّها تنقصها العديد من التفاصيل، في الشروط و الضمانات من اجل حماية

[1] من المفروض أن نميز بين حرية الإثبات وحرية القاضي في الاقتناع ،فيقصد بحرية الإثبات، انّ لكل أطراف الدعوى من ضمنهم القاضي اختيار وسائل الإثبات المناسبة للواقعة محل الإثبات، بينكما حرية القاضي في الاقتناع هو نطاق سلطة القاضي في قبول وتقدير الدليل ، حيث يمثل الأساس الذي يقود المرحلة النهائية في تقدير الدليل الجنائي ،احمد ضياء الدين محمد خليل، مشروعية الدليل الجنائي في المواد الجنائية،دراسة مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجنائية، رسالة، كلية الحقوق، جامعة عين شمس القاهرة،مصر،1982، ص248 هامش مشار إليه لدى عائشة بن قارة مصطفى، المرجع السابق، ص184.

[2] مروان محمد، المرجع السابق، ج2،ص338.

الحياة الخاصة للفرد عموما، خصوصا أنّ جرائم الانترنت وفي جانب سلوكها الإجرامي، تشرك العديد من الأطراف في الاتصالات الالكترونية المستخدمين ، ومزودي خدمات الانترنت بما فيهم الغير حسن النية والمتمثل في أيّ شخص منا.

الفرع الأول:مشروعية الحصول على الدليل الجنائي في جرائم الانترنت.

تقتضي فاعلية مبدأ شرعية الإجراءات، ضرورة الرقابة القضائية على كافة الإجراءات التي يتخدها قاضي التحقيق قبل المتهم، وذلك لبيان مدى توافقها مع القيود القانونية الموضوعية والشكلية المقررة لشرعية الإجراءات الجزائية وضمان سلامة التزام سلطة قاض التحقيق حدودها القانونية والدستورية[1].

لا يجوز للضابط المختص أن يقوم بإجراء التحريات عن واقعة لا تشكل جناية أو جنحة، مالم يطلب منه إجرائها مما له الحق في ذلك سواء منْ مَنْ خول لهم القانون ذلك، وإلّا عرّض نفسه للمسؤولية، حيث لا يجوز أن تترك سمعة الناس عرضة للبحث والتحري عنها دون مقتضى.كذلك لا يجوز للضابط المختص إجراء تحريات عن شخص معين أو واقعة معينة بناء على طلب شخص أخر[2].

بهذا يكون جمع الأدلة الصحيحة من مصادرها الشرعية هو الهدف الأساسي لكافة النشاطات التي تتعامل مع الجريمة منذ وقوعها أو وصولها إلى علم السلطات بأي كيفية[3]، وانّ حجية الدليل تكمن في الشرعية الإجرائية، تعني انّه لا إجراء بغير سند قانوني، ويتمثل مضمون الشرعية الإجرائية في أن يحدد القانون كل إجراء جنائي، أي ما يتعلق بجميع الأساليب الخاصة

[1] درياد مليكة ،المرجع السابق، ص178

[2] سعد سلامة، تفعيل دور التحريات في الإثبات الجنائي في ظل التقنيات الحديثة لمكافحة الجريمة،مجلة كلية الدراسات العليا، متخصصة في علوم الشرطة،القاهرة العدد الخامس عشر يوليو 2006جماد آخر 1427،ص92.

[3] برهامي أبو بكر عزمي،المرجع السابق،ص.1

بالتحري المنظمة لسير الإجراءات الجنائية، والإشراف القضائي على الإجراءات الجنائية لضمان الحريات[1].

على ذلك يجب أن يكون الدليل الجنائي في جرائم الانترنت، بمافي ذلك الدليل الجنائي الالكتروني ذا قوة قانونية؛ يستمد منها وجودة من التشريع عموما ومن نصوص قانون الإجراءات الجزائية، والقوانين المكملة خصوصاً. بان يحدد القانون كل إجراء جنائي وهو ما قام به المشرع الجزائري في قانون الإجراءات الجزائية وقانون(09-04)و كذا المرسوم الرئاسي، ولكن لم ينأى بهذا التنصيص عن وجود بعض النقائص، والتي أوردناها من اجل لفت انتباه المشرع إلى ضرورة إعادة النظر فيها، وفي النقائص التي تشوبها.

أولا:الضمانات القانونية في إطار قانون الإجراءات الجزائية.

شروط الحصول على الدليل الجنائي الالكتروني ودعائم الإثبات الجنائي لجرائم الانترنت، معا تعطي دليلا متكامل واضح المعالم يطرح أمام قضاء الموضوع لمناقشته، وهو الدليل الذي تم الكشف عنه وجمعه وتقديمه وفق الشروط القانونية المنصوص عليها.

إنّ الهدف من إدراج هذه النقطة؛ معرفة مدى الوجود الحقيقي لضمانات الحصول على الدليل في جرائم الانترنت وليس دراسة حالات واقعية، وهذا في إطار مشروعية الحصول على الدليل.

من خلال مراجعتنا لمجمل المواد المنظمة لهذه الإجراءات، لا حظنا وفي إطار الإجراءات الواردة في قانون الإجراءات الجزائية أنّ الضمانات المتعلقة ب:

[1] برهامي ابو بكر عزمي،المرجع السابق،ص19.

أ- اعتراض المراسلات والتقاط الصور وتسجيل المراسلات:

1- الإذن : وهو جوهر الإجراء من الشروط الشكلية التي يجب توافرها والذي أهمله المشرع الجزائري في إجراء التقاط الصور وتسجيل الصوت والأصل أن النص الدستوري في المادة (46) بقولها:"لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه ويحميها القانون.سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

لا يجوز بأي شكل المساس بالحقوق دون أمر معلل من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم.

حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه"[1].

وبالرجوع إلى نص المواد وما تطرقنا إليه في الفصل السابق نلاحظ أن المشرع الجزائري قصر شرط الإذن على تدبير اعتراض المراسلات دون التسجيل الصوتي، وهو ما أكد عليه النص الدستوري في المادة أعلاه.لذلك فانّ الإذن هو الأصل ثم بعد ذلك التعليل، فلا يمكن أن يسبب اللجوء إلى الإجراء دون وجود إذن أصلا، ومن هنا يعد ذلك نقصا شاب شرط إجراء التسجيل الصوتي الذي يعد في ذاته إجراء استثنائي، وهو ما يستوجب تداركه في التعديلات اللاحقة لقانون الإجراءات الجزائية.

2- مدة الإجراء وتجديده: لم يراع المشرع الجزائري مدة الإجراء وتجديده فيما تعلق بالتقاط الصور والتسجيل الصوتي، والذي يعتبر من الضمانات التي لا تدع مجالا للتعسف في استعمال السلطة من طرف أفراد السلطة المختصة، غير النزيهين فهم بشر غير معصومين من الخطأ، إذا كان من الأجدى تحديد عدد مرات قابلية التجديد،كما انّه ومن ناحية أخرى لم ينص صراحة على ما

[1] القانون(16-01) يتضمن التعديل الدستوري المؤرخ في 26 جمادى الأولى عام 1437الموافق6 مارس2016،ج ر رقم 14 المؤرخة في 07 مارس2016 ص 11.

إذا كان يجوز لقاضي التحقيق، الذي أذن بهذه العمليات توقيفها قبل الموعد المحدد في الإذن، لان الإذن لم ينص عليه أصلا في اللجوء إلى هذا الإجراء، والذي نلاحظ بدورنا وقد سبقنا آخرون إلى ذلك، انّه لم يعطى الأهمية البالغة كما هو الحال بالنسبة لإجراء التسرب مقارنة بباقي الإجراءات.

3-التسبيب:أو الأمر المعلل من السلطة القضائية كما نصت عليها المادة (46) من الدستور الجزائري، الذي لم يشترطه المشرع الجزائري -الإذن من قاضي التحقيق- في التقاط الصور والتسجيل الصوتي ، مما يمس بشكل واضح في الحياة الخاصة وحقوق الدفاع، حتى أنه أي المشرع الجزائري لم يتدارك هذا خلال تعديله الأخير لقانون الإجراءات الجزائية لسنة 2015و2017 .

لم يرتب المشرع أي جزاء على مخالفة أحكام هذه المادة، رغم أنّ هذا الأخير قد بدأها ب "يجب" التي تفيد الإلزام، والأصل في الإلزام أن يرتب مسؤولية على مخالفته، وما يدعو للتنويه و الانتباه انّ المشرع في كل مرة يستعمل مصطلح الأمر عندما يتعلق الأمر باتخاذ إجراء من إجراءات التحقيق ،إلا انّه في إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وحتى التسرب ،استخدم مصطلح الإذن، والذي عند استخدام مصطلح الأمر فانّه من حق وكيل الجمهورية استئناف أوامر قاضي التحقيق، أمّا إذا كان المصطلح المستخدم (إذن) فانّه ليس لوكيل الجمهورية الاستئناف[1]، هذا قد يرجع لسرية التي تحيط بهذه الإجراءات حتى لا تكون هناك فرصة لكشفها، ولكنها بالمقابل سوف تقتصر على أشخاص معينين مكلفين بهذه الإجراءات، والتي يجعل الطعن فيها غير ممكن، مما يضع الحق في الحياة الخاصة والحق في الدفاع على المحك، وبالتالي لا يمكن تطبيق أي جزاء وتحمل أي مسؤولية لانعدام وجود الأساس القانوني للمساءلة أصلاً، في ظل غياب شروط الجوهرية للجوء إلى أساليب خاصة لتحقيق نتائج مماثلة.

من هنا نلاحظ أنّه وفي نفس القانون أي الإجراءات الجزائية، أورد المشرع ضمانات لحماية الحياة الخاصة عن طريق وضع شروط في إجراء معين دون أخر، مع العلم انّه و في الإجراءات

[1] فوزي عمارة ،المرجع السابق،ص241.

المادية أي التقاط الصور والتسجيل الصوتي لم يذكر السبب والإذن، أما التسرب فقد نص على هذين الشرطين، فقد أولى اهتمام اكبر للإجراءات الشخصية-التسرب-والتي يكون المكلف بالإجراء، محدد الهوية مما اوجب حمايته جنائيا، وعدم ترتيب أي مسؤولية قانونية عليه، رغم انّه يستخدم أساليب الخداع والتدليس.

4-مصير التسجيلات:

من نتائج اعتراض المراسلات تسجيلات تحتوي الدليل الخاص بجرائم الانترنت، والسؤال الذي يمكن طرحه ما هو مصير هذه التسجيلات؟ أي الصور والمراسلات والأحاديث التي تم تسجيلها، إجابة على ذلك استوجب المشرع في المادة (65مكرر9)ق.ا.ج.ج على ضابط الشرطة القضائية المأذون له أو المناب من طرف قاض مختص أن يقوم بتحرير محضر عن العملية التي قام بها، وكل ما تعلق بالتقنيات والترتيبات طبعا مع ذكر تاريخ وساعة بداية والانتهاء من العملية.

و انتهى المشرع الجزائري، في المادة (65مكرر10) من ق.ا.ج.ج إلى وصف أو نسخ المراسلات والصور والمحادثات والمفيدة في إظهار الحقيقة في محضر يودع بالملف.

تنسخ وتترجم المكالمات التي تتم باللغة الأجنبية، عند الاقتضاء، بمساعدة مترجم يسخر لهذا الغرض اذا جميع التسجيلات من أحاديث وصور، تحرر ضمن محضر هذا المحضر تطبق عليه شروط المحاضر العادية والمنصوص عليها في قانون الإجراءات الجزائية، والتي لا تكون صحيحة إلا طبقا لنص المادة (214) ق.ا.ج.ج[1].

وعن التسجيلات والصور التي في المحاضر لم يحدد المشرع الجزائري مصيرها، ومدة الاحتفاظ بها عكس ماقرره في قانون كقانون حماية الطفل[2] في المادة (46)منه.

[1] المادة (214)من ق.إ.ج.ج." لا يكون للمحضر أو التقرير قوة الإثبات إلا إذا كان صحيحا في الشكل ويكون قد حرره واضعه أثناء مباشرة أعمال وظيفته وأورد فيه عن موضوع داخل نطاق اختصاصه ما قد رآه أو سمعه أو عاينه بنفسه"

[2] قانون رقم (15-12)مؤرخ في 28 رمضان عام 1436 الموافق 15 يوليو سنة2015، يتعلق بحماية الطفل،ج.ررقم39 بتاريخ 19 يوليو سنة2015ص4.

ب- إجراء التسرب.

إن إجراء التسرب هو من الإجراءات الشخصية، من الإجراءات الخاصة المهمة التي أتت أكلها، فيما يتعلق بجرائم كجرائم الفساد[1]، والتي يمكن اللجوء إليها في جرائم الانترنت،وقد سبق وتطرقنا إلى الشروط الواجبة لكي يتم اللجوء إلى هذا الإجراء الاستثنائي.

وهو الإجراء الذي اقره المشرع من خلال تعديله لقانون الإجراءات الجزائية، فالجهة المختصة بإصداره، إما وكيل الجمهورية أو قاضي التحقيق وهذا بموجب إذن[2]، وتحديد نوع الجريمة التي يجب أن تكون في سياق الجرائم الخاصة(65مكرر5)بالإضافة طبعا إلى التسبيب .

الواقع أن إجراء التسرب يختلف عن اعتراض المراسلات الالكترونية، لانّ التسرب هو إجراء شخصي من الفرد المختص، ويمكن تصوره في العالم الافتراض،كأن يقوم بالدخول إلى مواقع التواصل الاجتماعي بهوية مستعارة، دون استخدام الوسائل التقنية على عكس المراقبة الالكترونية التي تستخدم التقنية في الحصول على دليل الإثبات، أمّا التسرب فأسلوبه استعمال الغش والخداع طبعا في إطار القانون. وانّه تدعيما لسياسة المشرع طبعا في إطار الجرائم الخاصة، رجح فيها كل مرة المصلحة العامة على المصلحة الخاصة، ذلك انّه وحتى إذا تّم اكتشاف جريمة أخرى في إطار إجراء اعتراض المراسلات و تسجيل الصور أو التقاط الصور، فانّ الإجراء صحيح؛ أي لا يكون سببا للبطلان[3].

---

[1] قرار المحكمة العليا ، ملف رقم 517405، بتاريخ 04 فبراير 2009 ، مجلة المحكمة العليا، 2009،عدد 2.ص396.، ولقد جاء في حيثيات القضية، في صدد تحليل المحكمة العليا للوجه الثاني المثار من قبل الدفاع:"حيث انه بعد الاطلاع على القرار المطعون فيه يتبين أنّ قضاة المجلس سببوا قرارهم بما فيه الكفاية ولم يقصروا في ذلك، اذ انه ورد في حيثيات القرار انّ المتهم (م.ف) الذي كان يعمل كمحافظ للشرطة بميناء سكيكدة ضبط في حالة تلبس عن طريق إجراء تسرب وهو يحاول قبض مبلغ مالي مقابل تمكين الشخص المتسرب من الإبحار غير الشرعي، لذلك راى المجلس ان المتهم اساء استغلال وظيفته وقبل مزية غير مستحقة....الخ" مع العلم ان المتهم في قضية الحال توبع بجريمتي رشوة الموظف العمومي وإساءة استغلال الوظيفة وساعده شخص على الإبحار غير الشرعي بموجب م545 من قانون البحري، والمادة 25 /2 والمادة 33 من قانون مكافحة الفساد. هامش مشار اليه لدى، ركاب أمينة ، المرجع السابق، ص94.

[2] المادة(65 مكرر)ق.ا.ج.ج.

[3] المادة(65مكرر 6) ق.ا.ج.ج.

اذن هي النقائص التي شابت ضمانات اللجوء إلى الإجراءات الخاصة في إطار قانون الإجراءات الجزائية، فماذا عن الإجراءات في القانون (09-04).

ثانيا:الضمانات القانونية في إطار قانون (09-04).

يشتمل القانون (09-04) على إجراءات خاصة، وهي امّا إجراءات تم تثمينها كالتفتيش عن بعد وحجز المعطيات او جديدة كمراقبة الاتصالات الالكترونية.

أ-التفتيش وضبط الأدلة الجنائية في جرائم الانترنت :بداية بهذين الإجراءين باعتبارهما إجراءين أصيلين في قانون الإجراءات الجزائية، وتم تثمينهما في إطار القانون(09-04)، أي تكيفهما وفق محل الضبط وهي الآثار المعلوماتية، التي تخلفها جرائم الانترنت، وهي خطوة موفقة من المشرع الجزائري،فاهم الضمانات في

1-التفتيش عن بعد:

لا يصدر الإذن بالتفتيش إلا بعد وقوع الجريمة وفق المادة(44)من ق.إ.ج.ج[1]والمادة(05) من قانون(09-04)، على أن تكون جناية أو جنحة، لذلك فلا يجوز إصدار إذن التفتيش بشان جريمة يحتمل وقوعها مستقبلا، وهذا عكس ما اقره المشرع الجزائري في مراقبة الاتصالات الالكترونية، حين يتعلق الأمر بالجرائم الإرهابية التي يمكن فيها اللجوء إلى المراقبة الالكترونية الوقائية.

كما يجب أن تتحقق فائدة من هذا التفتيش وهو إظهار الحقيقة وفق المادة (81) من ق. ا.ج.ج.

[1] (44)من ق.إ.ج.ج تنص على مايلي:" لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء متعلقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش .
ويكون الأمر كذلك في حالة التحري في الجنحة المتلبس بهااو التحقيق في احدى الجرائم المذكورة في المادتين37 و40 من هذا القانون..."

على أنّ المشرع لم يذكر شرط ميعاد التفتيش، فقد تنازل عنه صراحة، وهذا تماشيا مع ما اقره في عدم الالتزام بساعات أو ميقات التفتيش في الجرائم الخاصة ومنها جرائم الإرهاب بما فيها جرائم الإرهاب الالكتروني.

– لا يشترط حضور المشتبه فيه المادة(65مكرر6)رغم أننا ننوه أن هذا التفتيش خصوصا ما تعلق بالمنظومة المعلوماتية أي ما تعلق بالكيان المتحرك، من الصعب حضور المشتبه فيه وخصوصا أنّ المسرح أو مكان التفتيش افتراضي لا محسوس.

– المحافظة على الأسرار هي ضمانة أقرتها المادة (8) و(9) من القانون(09-04) والمادة (46) ق ا ج ج ، والتي بانتهاكها تترتب المسؤولية الجزائية على الضابط المكلف أو الضباط المكلفين بهذا الإجراء ، والتي سوف نتطرق لها لا حقا.

2- **الضبط** أو الحجز يتم عن طريق النسخ على دعامة تخزين وهذا للحفاظ على الأدلة، أو كل ما توصل إليه من عملية التفتيش، ويتم المحافظة عليه عن طريق وضعها في احراز حيث تسري على كيفية التعامل مع الأدلة الجنائية بحسب المادة (6) من قانون (09-04)قواعد الوضع في احراز المنصوص عليها في قانون الإجراءات الجزائية.

ب–مراقبة الاتصالات الالكترونية:

لم يحدد المشرع الجزائري مدة المراقبة كما فعل بشان اعتراض المراسلات في قانون الإجراءات الجزائرية، ونص على المدة الخاصة بمراقبة الاتصالات في الجرائم الإرهابية فقط[1].

كما أنّ المشرع وضع ضمانه هامة، ربما كانت مفروضة عليه، لأنّه وبكل بساطة لا يستطيع القيام بهذا الإجراء أي مراقبة الاتصالات الالكترونية، بكل مايلزمها من دراية علمية وتقنية وتجهيزات ،إلا أن يقوم بها ضباط مختصون لذلك فقد جاءت المادة (23) من المرسوم الرئاسي بان أكدت

[1] المادة 4 من القانون (09-04)تنص على مايلي:"...عندما يتعلق الامر بالحالة المنصوص عليها في الفقرة"أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 ادناه،أدنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبينطبيعة الترتيبات التقنية المستعملة والاغراض الموجهة لها ...."

انّه لا يمكن أن يشارك في عملية لمراقبة الاتصالات الالكترونية إلا أعضاء الوحدة أو الوحدات التي أوكلت لها السلطة القضائية هذه المهمة[1].

يتخذ مسؤول الوحدة أثناء سير العملية كل التدابير اللازمة، بالاتصال مع المسؤولين المعنيين في الهيئة، من أجل ضمان سرية العملية وحماية المعلومات المستقاة من المراقبة "وهم أعضاء مديرية المراقبة الوقائية واليقظة القانونية وهذا بحسب نص المادة (11) من المرسوم "تكلف مديرية المراقبة الوقائية واليقظة الالكترونية على الخصوص بما يلي:- تنفيذ عمليات المراقبة الوقائية للاتصالات الالكترونية، من اجل الكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول."

على ان تحرر الاتصالات في محضر وفق مانص عليه قانون الإجراءات الجزائية، وهو قيد يضمن احترام الحياة الخاصة من التلاعب بالاتصالات، بالتعديل او بالإضافة أو التعديل بالتغيير او الحذف، على أنّ الاطلاع على هذا المحضر لا يكون إلا بمعرفة القائمين على الإجراء فقط.

-إن المعلومات الناتجة عن مراقبة الاتصالات الالكترونية هي معلومات سرية كفل لها المشرع الحماية، هذه الحماية تأتي بعد انتهاك الحياة الخاصة للأفراد طبعا بترخيص لضرورات التحقيق، فالضمانات لحماية الحقوق جاءت بعد أن اقر المشرع إجراءات خطيرة لكشف جرائم الانترنت.

لكن الخطوة المميزة التي جاء بها المشرع الجزائري في إطار المرسوم (15-261) المؤرخ في 8 أكتوبر 2015 وفي المادة (24) منه:"تحفظ المعلومات المستقاة أثناء عمليات المراقبة، خلال حيازتها من الهيئة، وفقا للقواعد المطبقة على حماية المعلومات المصنفة و التي لاحظنا من خلال بحثنا أن مصطلح المعلومات المصنفة مرتبط بمصطلح الوثائق المصنفة[2]، والتي عرفها المشرع الجزائري

[1] المادة(23)من المرسوم الرئاسي(15-261) تنص على مايلي:"لا يمكن أن يشارك في عملية لمراقبة الاتصالات الالكترونية إلا أعضاء الوحدة أو الوحدات التي أوكلت لها السلطة القضائية هذه المهمة...."

[2] وهذا ما نلاحظه من خلال نص المادة الأولى من المرسوم رقم(84-388) مؤرخ في 29 ربيع الأول عام 1405 الموافق 22 ديسمبر سنة 1984 يحدد كيفيات تأهيل الموظفين الذين يدعون إلى الاطلاع على المعلومات أو الوثائق المصنف، ج.ر 69 مؤرخة في 26 ديسمبر

الوثيقة المصنفة أي مكتوب، أو رسم، أو مخطط، أو خريطة، أو صورة، أو شريط صوتي، أو فيلمي، أو أية وثيقة، أو سند مادي يتضمن معلومات تجب حمايتها[1].

الواقع أنّ هذه الحماية هي للمعلومات المتعلقة بالأسرار العسكرية والاقتصادية وامن الدولة، دون أن تكون لها علاقة بحماية الحياة الخاصة للأفراد، باعتبار أن المشرع الجزائري قد خص المصالح المحمية أي المتعلقة بالدفاع وامن واقتصاد الدولة بحماية واسعة وهو الحال والصحيح، ولكن في المقابل نلاحظ انّ ماتعلق بباقي الجرائم المرتكبة لم يتناولها بذلك التفصيل.

-تسليم التسجيلات والمحررات:الأصل أن تسلم التسجيلات إلى السلطات القضائية المختصة، ولكن ما هي المدة الزمنية لهذه التسجيلات وكيف يمكن التخلص منها، الواقع أن المشرع الجزائري ومن خلال قراءتنا للنصوص فقد اورد مدة حفظ المعطيات والتي حددت بسنة واحدة من تاريخ التسجيل بالنسبة لمقدم خدمة الانترنت[2]. في إطار الالتزامات الملقاة على عاتقه لتقديم المساعدة للسلطات المختصة تحت طائلة قانون العقوبات[3] على انه لم توضح كيفيات التخلص من هذه التسجيلات و لم يُتطرق لذلك في قانون الإجراءات الجزائية بعد أن أحالنا عليه.ولكن وبعد اطلاعنا على قانون حماية الطفل وبالتحديد في المادة (46)من القانون[4]، وبغض النظر عن نوع الجريمة التي يتم التحقيق فيها تقر المادة على انه"يتم إتلاف التسجيل ونسخته في اجل سنة واحدة(1) ابتداءا من تاريخ انقضاء الدعوى العمومية ويعد محضر بذلك"، ونحن نؤيدها وندعو المشرع إلى إدراج مثل هذه الأحكام التي تصون الحياة الخاصة وتمنع أي تلاعب بالأدلة المتحصل

1984،ص2380."يجب على الموظفين من جميع الرتب في المؤسسات التابعة للدولة أن يحصلو على تأهيل خاص يسمح لهم بمعالجة الوثائق المصنفةوالاطلاع على المعلومات المصنفةو/او الدخول الى النقاط الحساسة او البالغة الحساسية".

[1] المادة 2 من المرسوم رقم (84-387)مؤرخ في 29 ربيع الأول عام 1405 الموافق 22 ديسمبر سنة 1984 يحدد التدابير المخصصة لحماية الوثائق المصنف،ج.ر 69 مؤرخة في 26 ديسمبر 1984،ص2378.

[2] المادة(11) من القانون(09-04).

[3] المادة(10)من القانون (09-04).

[4] قانون رقم (15-12)مؤرخ في 28 رمضان عام 1436 الموافق 15 يوليو سنة2015، يتعلق بحماية الطفل،ج ر رقم39 بتاريخ 19 يوليو سنة2015 ص11.

عليها من تسجيلات الكترونية، وهذا بان تتلف جميع الاتصالات المنسوخة من طرف نفس الهيئة بعد انقضاء الدعوى العمومية، كل حسب إذا كان السلوك الإجرامي يشكل جنحة أو جناية إلا ما تعلق بالجرائم التي لا تتقادم فيها الدعوى وهي المستهدفة بإجراء مراقبة الاتصالات الالكترونية بالدرجة الأولى[1].

– ولعل أهم إجراء يضمن عدم انتهاك الحياة الخاصة للفرد، لان هذه الإجراءات لا تخص فقط المتهم بل حتى الغير، هو ما نصت عليه المادة(41) من المرسوم الرئاسي (15-261) الذي حدد تنظيم الهيئة،نصت على مايلي" تمارس الهيئة الحصرية في مجال مراقبة الاتصالات الالكترونية تحت مراقبة قاض مختص"، ثم استدرك الحالات المنصوص عليها في قانون الإجراءات الجزائية، والمتعلق اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، على الرغم أنّ التجهيزات الحساسة تستوردها وتحوزها الهيئة فقط، او سلطة الضبط أو مؤسسة عمومية لشبكات الاتصال وهنا فتح المجال رغم أنّ الهيئات التي لها الحق في الاستيراد هي ثلاثة ولكنها بموظفيها، فتحت المجال لسوء الاستعمال وانتهاك الخصوصية دون قيد أو شرط.

من كل ماسبق ماذا يترتب عن الإخلال بهذه الضمانات في إطار قانون الإجراءات الجزائية والقوانين المكملة.

الفرع الثاني: جزاء الإخلال بمشروعية الدليل الجنائي في جرائم الانترنت.

ثبوت قيمة قانونية للدليل وطرحه للمحكمة لابد أن يكون هذا الدليل مشروعا بمعنى لا يلحقه البطلان أي لابد من استبعاد الأدلة غير المشروعة، فالأدلة لابد من أن تتطابق شروط جمعا والكشف عنها مع ما ورد في النصوص الإجرائية، لأنّه في حال لم يتم ذلك فانّه يلحق الإجراء البطلان(أولا) والذي يلحق الدليل بدوره، ومن جهة أخرى يمكن أن تترتب مسؤولية قانونية على

[1] تتقادم الدعوى العمومية في مواد الجنايات بعد مرور (10) سنوات من يوم اقتراف الجريمة او تاريخ أخر إجراء اتخذ للمتابعة المادة(7) ق.ا.ج.ج،أمآ الجنح فتتقادم الدعوى العمومية بعد مرور (3) سنوات من يوم اقتراف الجريمة أو من تاريخ أخر إجراء صحيح للمتابعة المادة (8) ق.ا.ج.ج، وتتقادم الدعوى العمومية في مواد المخالفات بعد مرور سنتين كاملتين من يوم اقتراف الجريمة أو تاريخ أخر إجراء اتخذ للمتابعة المادة(9) ق.ا.ج.ج، ولكن في الجنايات والجنح التي توصف بأفعال إرهابية وتخريبية المتعلقة بالجريمة المنظمة العابر للحدود الوطنية أو الرشوة أو اختلاس الأموال العمومية فهي لا تنقضي الدعوى العمومية بالتقادم المادة (8مكرر) ق.أ.ج.ج.

الضابط المختص أو من خول لهم مساعدة السلطات(ثانيا)،وبتوافر هدين العنصرين نضمن مشروعية الدليل وعدم التعسف في الحق أو استعمال السلطة، لدى يجب أن يُراعى أثناء البحث عن الأدلة إتباع الإجراءات المشروعة الصحيحة[1]. لذلك فانّ أيّ إجراء في اعتداء على الحق في الحياة الخاصة والحريات العامة هو إجراء باطل.

اذن فالقضاء هو المخول بمراقبة هذه الأعمال الإجرائية، وموضوعنا هو موضوع إجرائي وهو إثبات جرائم الانترنت، لذلك فان شرعية الإثبات تتطلب عدم قبول أي أدلة تم الحصول عليها أو البحث عنها بطريقة غير مشروعة، وهذا ما نوّه إليه المشرع الجزائري في تعديل قانون الإجراءات الجزائية في المادة (68 مكرر) منه"... مع مراعاة حقوق الدفاع واحترام قرينة البراءة..."[2].

فبذلك أكد المشرع على وجود جزاءات لكل سلطة مختصة يقوم احد أفرادها بانتهاك حقوق الدفاع، أو قرينة البراءة أو الحق في الحياة الخاصة إلا ما تقرر بنص.والاعتداء على القاعدة الإجرائية غالبا ما يكون، ضمن دائرة الإهمال وعدم احترام التعليمات، وإغفال الإجراءات القواعد التي تحقق مصلحة المتهم، وبالتالي تغلب مصلحة التحقيق والأهداف المرجوة منه على حقوق وحريات المتهم نفسه[3]، على أن جرائم الانترنت لها من الخصوصية ما يجعلها من الجرائم التي تشمل المتهم والغير، هذا الغير عادة يكون طرف في العلاقة سواء بإرادته أو دونها،كما نوهنا إليه في مواضع عدة ،لان أصلا الانترنت بجهود مجرميها جعلت الحياة الخاصة عارية من كل خصوصية. فأصبح اهتمامنا أن نحمي الغير الذي وجد نفسه في دائرة التحقيقات والمراقبة مصلحته أولى بالحماية من حقوق المتهم نفس.

[1] درياد مليكة ،المرجع السابق، ص178.

[2] المادة (68مكرر) من قانون الإجراءات الجزائية المعدلة بموجب أمر رقم(15-02)مؤرخ في 7 شوال عام 1436 الموافق 23 يوليو سنة2015،يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية،ج ر40 ليوم نفس اليوم ،ص28.

[3] محمد امين خرشة ،المرجع السابق،215

وبناءا على كل ماسبق يعتبر البطلان جزاء ا لضمان الشرعية الإجرائية، وهذا بعدم تحقق الأثر المتوخى من الدليل المتحصل عليه وهو الإثبات.

أولا– البطلان الجزائي.

اقرَّ قانون الإجراءات الجزائية جزاءا إجرائيا يتمثل في بطلان العمل الذي يخالف قاعدة إجرائية، البطلان هو الجزاء الذي يلحق إجراء نتيجة مخالفته أو إغفاله لقاعدة جوهرية في الإجراءات يترتب عنه عدم إنتاجه لأي أثر قانوني[1]، هذا الإجراء الذي يدخل في نطاق استبعاد الإجراء المتحصل عليه بطريقة غير مشروعة، حيث اشترط المشرع الجزائري في كل عمل إجرائي ضرورة توافر شروط معينة لا يصح إلاّ بها، وبالتالي فانّ الإجراء يجب أن يتم بالطريقة التي حددها التشريع، ومن قبل السلطات المختصة التي أناط بها القانون اللجوء إلى الإجراء الخاص في الجرائم الخاصة[2].

الأصل في الإجراءات الجزائية أنّها تهدف إلى حسن سير العدالة، لذلك وكما وضحنا سابقا أنّ المشرع الجزائري وعلى غرار الكثير من التشريعات، غلب في مجموع من السلوكيات الإجرامية المصلحة العامة على الخاصة فيما يتعلق بالحقوق والحريات، وهذا في الجرائم الخطيرة، ففرضت عليه الاتفاقيات الدولية المصادق عليها إضافة بعض الإجراءات الخاصة التي تتماشى وطبيعتها، وهذا تماشيا مع تكييف ما جاء في الاتفاقية مع القانون الوطني، فقيمة الدليل غير المشروع مثلا –الرقابة بغير إذن في الجرائم التي تتطلب الإذن– أو الإكراه على فك الشفرة للحصول على كلمة السر والولوج في المنظومة المعلوماتية، فالأصل أن مصير هذا الدليل هو البطلان وفق نص المادة(191) من ق.ا.ج.ج[3]، وبالرجوع إلى مواد الذي نصت على البطلان وهي متفرقة–مواد من (157)الى

[1] أحمد الشافعي، البطلان في قانون الإجراءات الجزائية، دراسة مقارنة، الطبعة الثانية، دار هومة، الجزائر، 2005، ص 11.

[2] محمد امين خرشة ،المرجع السابق،214.

[3] المادة (191) من ق.ا.ج.ج:"تنظر غرفة الاتهام في صحة الإجراءات المرفوعة إليها وإذا تكشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به، وعند الاقتضاء ببطلان الإجراءات التالية له كلها أو بعضها.ولها بعد الإبطال، أن تتصدى لموضوع الإجراء أو تحيل الملف إلى قاضي التحقيق نفسه أو لقاض غيره لمواصلة إجراءات التحقيق".

(161)من ق.ا.ج.ج والمادتين (100)وق.ا.ج.ج(105)البطلان القانوني و المادة (159) من ق.ا.ج.ج البطلان الذاتي.

أ-البطلان القانوني أو بطلان المقرر بنص صريح، ومن تسميته فأساسه النص القانوني أي أنّ الإخلال بشرط معين يؤدي إلى بطلان الإجراء، فالبطلان هو جزاء يلحق إجراء تم مخالفا للشكليات التي يشترطها القانون[1]، وهي الحالات التي وردت في المواد(38)[2] و(48)[3]و(44)و(65 مكرر)و(157)و(198)و(260)من ق.ا.ج.ج، واشترط قانون الإجراءات الجزائية شكليات معينة في إجراءات التحقيق الابتدائي يقوم بها قاضي التحقيق، غير أنه لا يكفي أن ينص القانون على إتباع إجراء معين ليترتب على مخالفته أو إغفاله البطلان، بل يجب أن ينص القانون على أن هذه المخالفة ترتب البطلان لذلك يسمى هذا البطلان بالبطلان النصي[4].

وقد رتب المشرع البطلان القانوني بصدد إجراءات التحقيق في عدة حالات،فنصت المادة (38) من ق.ا.ج.ج على أنّه " تناط بقاضي التحقيق إجراءات البحث والتحري، ولا يجوز له أن يشترك في الحكم في قضايا نظرها بصفته قاضيا للتحقيق وإلا كان ذلك الحكم باطلا "، وذهبت المادة (48)من نفس القانون إلى أنه يجب مراعاة الإجراءات التي استوجبتها المادتان(45)و(47) ويترتب على مخالفتها البطلان[5].

---

[1] أحمد الشافعي، المرجع السابق، ص29.

[2]المادة (1/38)ق.ا.ج.ج:" تناط بقاضي التحقيق إجراءات البحث والتحري ولا يجوز له أن يشترك في الحكم في قضايا نظرها بصفته قاضيا للتحقيق وإلا كان ذلك الحكم باطلا".

[3] المادة(48)ق.ا.ج.ج:"يجب مراعاة الإجراءات التي استوجبتها المادتان 45و47 ويترتب على مخالفتها البطلان"

[4]أحسن بوسقيعة، التحقيق القضائي، المرجع السابق، ص187.

[5] كما نصت المادة 1/157 من قانون الإجراءات الجزائية على أنه " تراعى الأحكام المقررة في المادة 100 المتعلقة باستجواب المتهمين والمادة 105 المتعلقة بسماع المدعي المدني وإلا ترتب على مخالفتها بطلان الإجراء نفسه وما يتلوه من إجراءات".وتنص المادة (198)من نفس القانون على أن قرار الإحالة يتضمن بيان الوقائع موضوع الاتهام ووصفها القانوني وإلا كان باطلا.

ويتضح من ذلك أن المشرع عندما يريد أن يرتب جزاء البطلان على مخالفة إجراء معين للقانون فإنه ينص عليه بعبارات صريحة وواضحة لا تقبل أي تأويل، وبالتالي فإنه لا يمكن للقاضي أن يحكم بإبطال إجراء ما لم ينص عليه القانون صراحة، مما يجعل القاضي لا يتمتع بأي سلطة تقديرية فهو مقيد بالنص ولا يحكم بالبطلان حتى ولو كان الإجراء يمس حقوق الدفاع ويضر بمصالح الأطراف[1].وبالنسبة لجرائم الانترنت وما يلحق الإخلال بالحصول على الدليل الجنائي إذا تعلق الآمر بإجراء خاص هو المادة(65مكرر15)ق.ا.ج.ج، والمتعلق بالجزاء المترتب عن عدم وجود الإذن المكتوب لإجراء عملية التسرب في جرائم الانترنت، وعدم بيان الأسباب التي دعت إلى اللجوء إلى هذا الإجراء.

ب–البطلان الذاتي أو الجوهري:

هو البطلان الذي يترتب على مخالفة الأحكام الجوهرية الخاصة بالتحقيق، إذا أخلّت بحقوق الدفاع أو بأي خصم أخر ما لم يتنازل الطرف المعني عن التمسك بالبطلان المقرر لمصلحته[2].

وهنا تكمن السلطة التقديرية للقاضي في إبداء حالة البطلان الجوهري المنصوص عليها بموجب المادة (159) ق.ا.ج.ج[3]، ولكن هنا عليه أن يتبع النصوص التي تحمل الالتزام مثلا أو التي تلزم السلطات المختصة أو من خول لها بموجب القانون التدخل في إجراء من إجراءات التحقيق، وجود الإجراء الذي يخل بحقوق الدفاع أو حسن سير العدالة وهذه المعايير أصلا هي عبارة عن سلوكيات إجرامية عاقب عليها المشرع عنها.

[1] أحمد الشافعي، المرجع السابق، ص32 وما يليها.

[2] محمد حزيط، المرجع السابق، ص167.

[3]المادة 159 من ق.ا.ج.ج:" يترتب البطلان أيضا على مخالفة الأحكام الجوهرية المقررة في هذا الباب خلاف الأحكام المقررة في المادتين 100 و105 إذا ترتب على مخالفتها إخلال بحقوق الدفاع أو حقوق أي خصم في الدعوى.وتقرر غرفة الاتهام ما اذا كان البطلان يتعين قصره على الإجراء المطعون فيه أو امتداد جزئيا أو كليا على الإجراءات اللاحقة له.ويجوز دائما للخصم التنازل عن التمسك بالبطلان المقرر لمصلحته وحده .ويتعين ان يكون هذا التنازل صريحا.ويرفع الامر لغرفة الاتهام طبقا للمادة السابقة وتفصل فيه طبقا لما هو مقرر في المادة 191."

1- مفهوم البطلان الجوهري[1]:

ونظرا لكون هذا البطلان من وضع الفقه والقضاء فإن القاضي يتمتع بسلطة تقديرية في تقرير البطلان والحكم به حتى ولو لم ينص عليه القانون وذلك إذا تعلق الأمر بمخالفة أو إغفال قاعدة جوهرية في الإجراءات، ومع هذه المرونة والسلطة التي يتمتع بها القاضي في الحكم ببطلان الإجراء حسب جسامة المخالفة وأهميتها ومدى مساسها بحقوق الدفاع، فإنه من الصعب تحديد وتعريف القواعد الجوهرية والقواعد غير الجوهرية[2].

نص قانون الإجراءات الجزائية على إجراءات شكلية عديدة، غير أنّها ليست جميعا بنفس الأهمية والقيمة القانونية ولا ترتب نفس النتائج والآثار، فهناك إجراءات جوهرية وضعت من أجل التنظيم والإرشاد والتوجيه بحيث لا يترتب على مخالفتها البطلان.

كما أن المشرع لم يعط تعريفا للقواعد الجوهرية ولا القواعد غير الجوهرية بل ترك هذه المهمة لاجتهاد القضاء والفقه، وبالتالي بقي الأمر غامضا يحتاج إلى توضيح طبقا لمقتضيات الشرعية الإجرائية.

2- الإجراءات الجوهرية والإجراءات غير الجوهرية.

- الإجراءات الجوهرية: تنص المادة (1/159) من قانون الإجراءات الجزائية على أنه يترتب البطلان أيضا على مخالفة الأحكام الجوهرية الواردة في الباب الثالث الخاص بالتحقيق بالإضافة إلى تلك المنصوص عليها في المادتين(100) و(105) إذا ترتب على مخالفتها إخلال بحقوق الدفاع أو حقوق أي خصم في الدعوى.

[1] بارش سليمان،شرح قانون الإجراءات الجزائية الجزائري، الجزء الأول، دار الهدى، عين مليلة، الجزائر، 2007، ص35.
[2] أحمد الشافعي، المرجع السابق، ص35.

اعتمد المشرع على حقوق الدفاع كمعيار لتحديد الإجراء الجوهري، وقد اعتبرت المحكمة العليا أن الشكلية تعبر جوهرية عندما تمس بحقوق من يتمسك بها[1].

ومع ذلك فإن المشرع لم يحدد مضمون حقوق الدفاع طبقا لمبدأ الشرعية الذي يقتضي توضيح وتبيين النصوص الجنائية تفاديا للتفسير القضائي الذي طالما ترتب عليه إخلال بحقوق ومصلحة المتهم.

وبذلك يعتبر الإجراء جوهريا يرمي إلى حسن سير العدالة وجوب التوقيع على الطلب الافتتاحي لإجراء تحقيق وتدعيم هذا الطلب بالوثائق اللازمة لمباشرة التحقيق، ويعتبر إجراءا جوهريا يترتب على مخالفته أو إغفاله مساس بحقوق الدفاع استجواب المتهم بعد تحليفه اليمين وكذا استنباط اعتراف المتهم من وسائل غير مشروعة.

وقد استقرت المحكمة العليا على أن الإجراء يكون جوهريا إذا كان يهدف إلى حماية حقوق الدفاع أو حقوق أطراف الدعوى الجزائية أو يرمي إلى حسن سير العدالة فيعتبر إجراءا جوهريا استجواب المتهم قبل إصدار أمر إيداع ضده[2]،والمعيار في تحديد الإجراء الجوهري من غيره مرتبط بالمصلحة التي يحميها سواء كانت المصلحة عامة أو مصلحة خاصة، ويترتب على عدم مراعاة الإجراء الجوهري البطلان[3].

والإجراءات الجوهرية لا يمكن تعدادها ولا حصرها لأن عددها يمكن أن يتغير تبعا لتعديلات قانون الإجراءات الجزائية التي قد تنشئ أشكالا جوهرية جديدة.

[1] قرار جنائي صادر في 1989/11/28 ملف رقم 58430، المجلة القضائية، العدد الثاني لسنة 1994، ص 262 وما يليها.

[2] قرار غرفة الجنح والمخالفات الصادر في: 1983/11/29 ملف رقم 34094، المجلة القضائية العدد الرابع لسنة 1989، ص278 وما يليها.

[3] قرار غرفة الجنح والمخالفات الصادر في: 1990/01/23 ملف رقم 59484، المجلة القضائية العدد الأول لسنة 1992، ص 200 وما يليها.

– **الإجراءات غير الجوهرية:** هي إجراءات إرشادية تنظيمية نص عليها المشرع لمجرد إرشاد وتوجيه رجال القضاء والأطراف إلى الطريقة المناسبة لإجراء التحقيق والفصل في الدعوى الجزائية[1].

ومثال الإجراءات غير الجوهرية كذلك عدم تبليغ المتهم بجلسة غرفة الاتهام إذا ما ثبت أنه تم تبليغ محاميه بتاريخ الجلسة وحضر إليها، وقدم أمام غرفة الاتهام ملاحظات شفوية طبقا للمادة (182) من ق.ا.ج.ج، وكذا عدم تبليغ المتهم بأمر الإيداع الصادر ضده طبقا للمادة(2/117)من نفس القانون.

وفي سبيل الوصول إلى كشف الحقيقة وتحقيقا للتوازن بين مصلحة المتهم ومصلحة المجتمع تعد إجراءات جوهرية[2] ، تلك الإجراءات التي تحدد ضمانات الحرية الشخصية للمتهم وتكفل الإشراف القضائي على الإجراء والتي تتمثل في ضمانات الحرية الشخصية، وأهمها قرينة البراءة، إنّ هذه القاعدة المقررة هي أنّ الأصل في الإنسان البراءة حتى تثبت إدانته، فهي الفطرة الطبيعية التي وجد عليها، فحرية الشخص مكفولة في نطاق هذه القاعدة، غير أن مصلحة المجتمع قد تبرز لتمس تلك الحرية الشخصية[3].وقرينة البراءة تعني أنّ الأصل في المتهم براءته مما اتهم به من أفعال، ويبقى الأصل ثابت حتى يثبت بالحكم القضائي حكم الإدانة[4]، والتي يحاول الفرد بكل ما أوتي من قوة أن يحافظ عليها ويدافع عنها وهي القاعدة التي اقرها المشرع الجزائري في أكثر من مناسبة وسياق. بالإضافة إلى ضمانات حقوق الدفاع، والضمانات المتعلقة بالحياة الخاصة التي تحمي الحق في كتمان الأسرار والتي تواجه الإجراءات الماسة بها مثل التفتيش والتصنت على المكالمات

[1] قضت المحكمة العليا في القرار الصادر في 1998/07/14 من الغرفة الجنائية الأولى في الطعن رقم 195447 أن ذكر رقم قاعة الجلسة في الاستدعاء لا يشكل إجراءا جوهريا ولا يعتبر مخالفة لقاعدة جوهرية في الإجراءات يترتب عنه البطلان، وفي قرار أخر قرار صادر بتاريخ 1985/07/02 من الغرفة الجنائية الثانية في الطعن رقم 43509 قضت أن ترتيب القضايا وجدولتها في دورة عادية أو غير عادية هو إجراء تنظيمي وإداري لا جوهري لذلك لا ينجر عنه البطلان، جيلالي بغدادي، الاجتهاد القضائي في المواد الجزائية ، الجزء الأول، الطبعة الأولى، الديوان الوطني للأشغال التربوية، الجزائر 1999، ص 113

[2] احسن بوسقيعة، التحقيق القضائي،المرجع السابق، ص 193،و أحمد الشافعي، المرجع السابق، ص 45 وما يليها.

[3] منذر الويس، المرجع السابق،ص.437. جميل عبد الباقي الصغير، ادلة الاثبات الجنائي وتكنولوجيا الحديثة، المرجع السابق، ص،111.

[4] سامح احمد البلتاجي موسى ، المرجع السابق،ص329.

الهاتفية ومراقبة الاتصالات الالكترونية وكذا حجز المعطيات المعلوماتية الناتجة عن التفتيش عن بعد.

- **القواعد التي تكفل الإشراف القضائي:** تعد القواعد المتعلقة بالتنظيم القضائي قواعد جوهرية كتلك المتعلقة باختصاص قاضي التحقيق وكيفية مباشرته إجراءات التحقيق الابتدائي.

وقد كان الهدف من إدراج هذه النقطة هو تبيان أنّ المشرع الجزائري، قد نصّ على البطلان كنتيجة تلحق الإجراء المعيب، ونخص بذكر بعض الإجراءات دون الأخرى، ولو أن البطلان يلحق كل إجراء دون استثناء لم يعمل في الشروط الخاصة للجوء إلى الإجراء من شروط موضوعية أو شكلية، هذه الأخيرة هي ضمانات لحماية الحقوق والحريات للأفراد، فكان من الأحسن أن يتوسع المشرع في هذه النقطة لان اتساع رقعة جرائم الانترنت والمسرح الافتراضي أو العالم الافتراضي، يجعل مثلا من إجراء معيب –كعدم الحصول على إذن –لا يضر فقط بالمشتبه فيه ولكن بالغير، فعند التفتيش أو المراقبة، كل مستخدم لشبكة والتابع لمزود انترنت معين هو تحت الرقابة ،– طبعا بحكم الوسائل التقنية التي تمكنه من ذلك التي تدخل في إطار الأداء الحسن لوظيفته– في حين انّه كان يظن انّه ينعم بالخصوصية، وقبلها اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، فهي لا تخص المشتبه فيه نفسه بل تتعداه لكل من يحيط به من أفراد عاديين طبيعيين ومعنويين، أماّ الجزاء الذي يلحق الإخلال بالضمانات فهو قيام المسؤولية و نقصد بها هنا المسؤولية الجزائية.

ثانيا:المسؤولية المتعلقة بالإخلال بقواعد الحصول على الدليل الجنائي في جرائم الانترنت.

الضمانات التي تحاط بإجراءات الحصول على الدليل يترتب عن مخالفتها جزاءات جنائية وهو ما يهمنا، ومخالفتها رتب عليها المشرع الجزائري اثر قانوني يلحق الشخص المخالف وهم الأشخاص المكلفون بالتحقيق والتحري في إطار هذا النوع من الجرائم، والأشخاص المناط بهم التعاون وتقديم المساعدة في مواجهة جرائم الانترنت.

كما ذكرنا ضمانات مصدرها قانون العقوبات وأخرى مصدرها قانون الإجراءات الجزائية وأخيرة مصدرها القوانين الخاصة والمراسيم التنظيمية الخاصة بها.

أ-الاعتداء على الحق في الحياة الخاصة .

من بين أهمّ صور التجسس على حرمة الحياة الخاصة، التجسس عن طريق حاستي النظـر و السمع، فالتجسس على حرمة الحياة الخاصة قد يكون باختلاس النظر أو التصوير أو نقل الصور الخاصة بمشهد من مشاهد حرمة الحياة الخاصة[1].وتختلف الوسائل التي تساعد في ذلك من اتصالات تماثلية عادية إلى اتصالات باستخدام التقنية الحديثة متمثلة في الاتصالات الالكترونية.

ولا شك أنَّ هناك ارتباط وثيق بين التقدم التقني بشكل عام واتساع مجال الرقابة الاجتماعية على الأفراد، وهذا بظهور وسائل تنصت على جميع الأجهزة المحمولة، وهي أدوات رقابة واستراق غير مسبوقة في يد الأفراد من غير مسؤولية[2].

لكن هذا لا يعني أن يسمح القانون بانتهاك الحياة الخاصة، للإفراد المشتبه فيهم والغير حسن النية ،فوضع المشرع الجزائري لذلك ضمانات في القانون الأساسي، والتي فعلها في إطار قانون العقوبات،وهي تعبير عن حماية حقيقية وفعالة في مواجهة آليات كشف جرائم الانترنت وإثباتها.

1-الاعتداء على الحق في الصورة والصوت.

نلاحظ أنّ المشرع الجزائري كلما اقّر إجراءات للتحقيق والتحري تمس حريات الفرد على رأسها الحق في الحياة الخاصة، وما يتفرع منها من حقوق أخرى كالحق في الصورة والحديث الخاص، أصبح شيئا فشيئا يقلص من ضمانات اللجوء لمثل هذه الإجراءات.وإذ نحن لسنا مع

[1] عاقلي فضيلة، الحماية القانونية للحق في الحياة الخاصة ،دراسة مقارنة ،دكتوراه علوم في القانون الخاص جامعة الإخوة منتوري قسنطينة،كلية الحقوق،2011-2012،ص 155و مرنيز فاطمة.

[2] عبد الرحمان محمد خلف،نظرة حول المشكلات القانونية والعلمية لمواجهة الجريمة المعلوماتية، مجلة كلية الدراسات العليا، القاهرة،جمهورية مصر العربية، العدد 21 يوليو2009،شعبان1430 هـ، ص20.

التقليص من ضمانات اللجوء لمثل هذه الإجراءات، ولكن قد يرجع ذلك إلى مجمل العراقيل والصعوبات التي تواجه كشف جرائم الانترنت في حدّ ذاتها، وإذا كان الأمر كذلك فلا يجب على المشرع الجزائري، أن يغض الطرف على أن هذه الإجراءات لا تخص فقط المتهم و المشتبه فيه، وإنّما لها علاقة وثيقة بالغير، باعتباره طرفا إمّا في محادثة أو صورة أو تسجيل صوتي أو حتى كصديق على مواقع التواصل الاجتماعي أو مرسل أو مرسل إليه عبر البريد الالكتروني أو الفايبر أو غيرها، من هنا جرم بعض أفعال الاعتداء على الصورة والصوت.

-الركن الشرعي:

الجدير بالذكر أن المراسلات الإلكترونية قد تتضمن صورا أو تسجيلات لمكالمات أو أحاديث، فنجد أن المشرع الجزائري قام بتجريم الالتقاط أو التسجيل أو النقل لصور أو تسجيلات بدون رضا صاحبها عندما يتم بأية تقنية كانت، و التي تصدق حتى على المراسلة الإلكترونية عن طريق الانترنت، إذ تنص المواد(303مكرر) و(303مكرر1) على التوالي[1] على هذه السلوكيات المجرمة.

فالملاحظ أنّ المشرع أولى حماية خاصة للصور والتسجيلات والمكالمات و الأحاديث و ذلك بتجريمه للأفعال السالفة الذكر في المواد (303 مكرر) و(303مكرر1) والتي تمس بالحياة الخاصة للأشخاص بأية تقنية كانت.

[1] " يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات و بغرامة من خمسين ألف50.000 إلى 300.000ثلاثمائة ألف دينار جزائري كل من تعمد المساس بحرمة الحياة الخاصة بأية تقنية كانت و ذلك :

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

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

أما المادة (303 مكرر 1) فتنص " يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بوضع في متناول الجمهور أو الغير أو استخدم بأية وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون"

-الركن المادي: يتحقق الركن المادي لهذه الجريمة بإحدى الصور النشاط الإجرامي، وبأي تقنية عن طريق التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة، التقاط أو تسجيل أو نقل الصورة، الاحتفاظ نشر واستخدام التسجيل أو الصور أو الوثائق.

-التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة.أي الاستماع سرا إلى كلام له صفة الخصوصية[1]،بين شخصين دون رضا الشخص،عن طريق التنصت،أو التسجيل الذي يقصد به حفظ الحديث بآي طريقة أو تقنية أو وسيلة، كما تقوم الجريمة عن طريق النقل أي أقل الحديث.

- التقاط أو تسجيل أو نقل الصورة.وتقوم هذه الجريمة في شكل التقاط أو التسجيل أونقل الصورة،فالتقاط الصورة يعني أخذها لشخص أو لعدة أشخاص، أمّا تسجيل الصورة، هو تثبيت الصورة، وهذه العملية تحدث في الأجهزة الأكثر تطورًا، وهنا تزداد خطورة هذه التقنيات من حيث الاعتداء على حرمة الحياة الخاصة للأشخاص.

ونقل الصورة فهو تحويلها وإرسالها من موضع لآخر بغرض تمكين شخص موجود في مكان مختلف عن المكان الذي يوجد فيه المعتدي على حرمة حياته الخاصة بواسطة الصورة وتوزيعها[2]

- الاحتفاظ، نشر واستخدام التسجيل أو الصور أو الوثائق.

يقصد بالاحتفاظ، إمساك الجاني لتسجيل أو صورة أو مستند خاص بشخص أو أشخاص آخرين عن قصد، مع علمه بمحتوى التسجيل أو المستند، مع ضرورة أن يكون قد تم الحصول على التسجيل أو الصورة أو الوثيقة عن طريق الالتقاط أو التسجيل أو النقل للمكالمات أو الأحاديث الخاصة أو السرية أو لصورة المجني عليه في مكان خاص[3].

أمّا الوضع في متناول الجمهور أو الغير :فيقصد به إعلان الغير عن محتوى التسجيل أو الصورة أو الوثيقة، بأي وسيلة كانت و عرضها بصورة واضحة.[4]

[1] إنّ المحادثات المقصودة هنا هي المحادثات السرية، يرجى الرجوع إلى المبحث الأول من الفصل الأول من الباب الثاني لهذه الرسالة،ص.184

[2] مدحت رمضان، المرجع السابق،95.

[3] مدحت رمضان، المرجع السابق،117.

[4] مدحت رمضان، المرجع السابق،96.

السماح بالوضع في متناول الجمهور أو الغير :يتخذ هذا السلوك مظهرا سلبيا بعدم الاعتراض على النشر والإذاعة للصور أو المكالمات والمحادثات الخاصة، كما يتخذ أيضا مظهرا إيجابيا من خلال تسليم وتقديم جسم الجريمة لغرض الإعلان عنه أو تسهيل ذلك

امّا الصورة الأخيرة في فعل الاستعمال، ويتمثل في استخدام التسجيل أو الوثيقة لتحقيق غرض ما، أي النشاط الذي يسعى الجاني من خلاله إلى تحقيق الغاية التي يرغب فيها.

-الركن المعنوي:

تعتبرسلوكيات التقاط أو تسجيل أو نقل مكالمات أو أحاديث أو الصور خاصة من الجرائم العمدية التي لا تقوم عن طريق الخطأ وهذا ماورد بصريح العبارة في المادة (303)مكرر ق.ع.ج،كما تعتبر السلوكيات المنصوص والمعاقب عليها بالمادة (303مكرر1) من قانون العقوبات سلوكيات عمدية،يتطلب لقيامها توافر القصد الجنائي بتوافر عنصري العلم والإرادة،فيجب أن يعلم الجاني بمصدر الحصول على التسجيل أو الصورة أو الوثيقة، وأنّه يقوم بالاحتفاظ به أو وضعه أو السماح بوضعه في متناول الجمهور أو الغير أو استخدامه، كما ينبغي أن تتجه إرادته إلى إتيان الأفعال المادية بالاحتفاظ أو الوضع أو السماع بالوضع في متناول الجمهور أو الغير أو الاستخدام للتسجيل أو الصورة أو المستند موضوع الجريمة.

2- الاعتداء على المراسلات:

لقد ذكرنا أن الإجراءات الجزائية عامة والإجراءات الخاصة للجرائم الخاصة لابد من أن يلجا إليها، في إطار من الأخلاق والنزاهة وبعيدا عن المحسوبية والمتاجرة بالوظيفة والتعسف في استعمال الحق، ورتب المشرع الجزائري مسؤولية جنائية عن تجاوز شروط اللجوء إلى مثل هذه الإجراءات المخولة قانونا باستعمالها من طرف السلطات المختصة بالتحري والتحقيق، حيث يصل هؤلاء إلى ارتكابهم سلوك إجرامية يرتب المسؤولية الجنائية .

نصت المادة (137) من ق.ع.ج لجزائري على ان"كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد، يقوم بفض أو اختلاس ،أو إتلاف رسائل مسلمة إلى

البريد أو يسهّل فضها أو اختلاسها أو إتلافها، يعاقب بالحبس من ثلاثة أشهر إلي خمس سنوات، وبغرامة من 30.000 دح إلي 50.000 دج.

يعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق يختلس أو يتلف برقية أو يذيع محتواها، ويعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشرة سنوات".

ونصت المادة (303) من ق.ع.ج على مايلي " كل من يفض أو يتلف رسائل أو مراسلات موجهة إلي الغير،وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة (137)، يعاقب بالحبس من شهر واحد إلى سنة و بغرامة من 25.000 إلى 100.000دج أو بإحدى هاتين العقوبتين"

– الركن المادي:

يشترط لقيام جريمة الاعتداء على سرية المراسلات[1]قيام الشخص موظف كان أو غيره بالأفعال المنصوص عليها والمتمثلة في :

– **الفتح أو الفض،** وهو كل فعل مادي من شانه فض الحرز أو المظروف الذي يغلف او يحوي الرسالة فمجرد فض الحرز المغلف بأي صورة يعد فتحا للمكاتيب[2]،ويمكن أن تكون باستخدام التقنية الحديثة وبالتالي لا يمكن اكتشافها من طرف الأفراد[3]،ولو انّه عمليا أصبحت مواقع التي تقدم خدمة البريد الالكتروني أي تقدم خدمة الإيواء تبعث برسائل تنبه فيها المشترك بأنه تم فتح بريده الالكتروني في بلد أخر مثلا، وتطلب منه تأكيد هويته حفاظا على سرية المراسلات.

[1] لتعريف المراسلات يرجى الاطلاع على المبحث الأول ،من الفصل الأول من الباب الثاني لهذه الرسالة،ص180.

[2] عصام احمد البهجي،المرجع السابق،ص291

[3] منذر لويس،المرجع السابق،ص262.

–الاختلاس، عاقب المشرع الجزائري، على اختلاس المراسلات الخاصة بصورة مباشرة، في المادة (137) من ق.ع.ج التي تحمي المراسلات الخاصة من الاعتداء عليها، قد يختلس الموظف أو غيره رسالة أو برقية معينة،و تتجه نيته إلى اعتبارها مملوكة له ويضيفها إلى ملكه[1]، يختلف الاختلاس عن الإخفاء كون هذا الأخير يستلزم تعمد الاحتفاظ بالخطاب و لو لفترة قصيرة قبل وصوله إلى المرسل إليه.

–الإتلاف،يقصد بالإتلاف تغييب الرسالة و جعلها غير صالحة وهو ما يتصوره في الرسائل الالكترونية الواردة إلى البريد الالكتروني خصوصا أنّ محلها افتراضي بحث[2]، والشخص العادي لا يمكن له أن يكتشف الإتلاف آو العبث هذا إذا ما أضفنا في الحسبان أن الأشخاص المختصون لهم من الإمكانيات ما يمكنهم من فعل ذلك بعيدا عن النزاهة.

لأن ينتفع بها على النحو المعدة له أصلا، و لذلك فإنه يعد من قبيل الإتلاف، إعدام الرسالة جزئيا أو كليا، كأن يتم ذلك بحرقها أو تمزيقها أو مسح المادة المكتوبة بصورة كلية أو جزئية ، بحيث يتعذر على المرسل إليه لانتفاع بها و بحسب ما هو مقرر، و قد نص المشرع الجزائري على اعتبار الإتلاف صورة من صور التعدي على سرية المراسلات في المواد (137)و(303)من قانون العقوبات الجزائري.

فبعد أن اعترف الدستور بحرمة الحياة الخاصة، ووضع ضمانات في قانون العقوبات والإجراءات الجزائية بما فيها القوانين المكملة، هو صون للحقوق الدستورية،كما أن استخدام التقنيات الحديثة في البحث والتحري والتحقيق، فيه من المجازفة بالحق في الحياة الخاصة وقيمة الدليل في نفس الوقت، مثلا قد لا تكون التسجيلات الكترونية واقعية، بل محرفة بها حذف أو تغير أو ما إلى ذلك، أو عدم فعالية للأجهزة سواء في التسجيلات الصوتية في تسجيل الصوت في

[1] عصام احمد البهجي،المرجع السابق،ص291

[2] علي احمد عبد الزعبي،المرجع السابق،ص232.

الأماكن العامة بسبب اكتظاظ الناس مثلا، أو ضخامة البيانات والاتصالات المرسلة على مستوى شبكة الانترنت، مما يؤدي إلى اختلاط المراسلات وبالتالي يصعب التمييز بين المشتبه فيه والغير[1].

ذكرنا أنّ مشروعية الدليل تتمثل في اللجوء إلى الإجراء وفق مانص عليه القانون وفي إطار من النزاهة والشفافية وبعيد عن الخداع والتدليس من غير المنصوص عليه قانونا ولضرورات التحقيق القضائي،"وتأكيدا على الأهمية القصوى لحماية حرمة الحياة الخاصة، تبرز ضرورة تدخل المجتمع بما في ذلك نظامه الدستوري، من اجل حماية الحريات والحياة الخاصة من أخطار ذيوع أسرار الأشخاص عبر وسائل الاتصالات والتكنولوجية الحديثة والمنتشرة"[2].

ب- إفشاء السر المهني:

الجزاء الجنائي التالي جراء الإخلال بضمانات الحصول على الدليل في جرائم الانترنت،هو قيام المسؤولية على إفشاء الأسرار المهنية ومن بينها اسرار التحقيق، فإفشاء سر من أسرار التحري والتحقيق قد يعطي الفرصة للجاني الحقيق للهرب وان يتهم الغير حسن النية لمجرد انّه كان من مجموعة الأصدقاء على مواقع التواصل الاجتماعي، لمشتبه فيه يحرض على الإرهاب بجهل منه، نص المشرع على الطابع السري لهذه الإجراءات وهذا بموجب نص المادة (11) من ق.ا.ج.ج.[3]

[1] موسى مسعود ارحومة، قبول الدليل العلمي أمام القضاء الجنائي، المرجع السابق ،ص 420.

[2] طارق صديق رشيد كه ردى، حماية الحرية الشخصية في القانون الجنائي، منشورات الحلبي الحقوقية، بيروت ، لبنان،2011. ص.210

[3]نص المادة (11)من ق.ا.ج.ج " تكون إجراءات التحري والتحقيق سرية، ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع.
كل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها.
غير انه تفاديا لانتشار معلومات غير كاملة أو غير صحيحة أو لوضع حد للإخلال بالنظام العام،يجوز لممثل النيابة العامة أو لضابط الشرطة القضائية بعد الحصول على إذن مكتوب من وكيل الجمهورية أن يُطلع الرأي العام بعناصر موضوعية مستخلصة من الإجراءات على أن لا تتضمن أي تقييم للأعباء المتمسك بها ضد الأشخاص المتورطين.تراعى في كل الأحوال قرينة البراءة وحرمة الحياة الخاصة" من أمر رقم (15-02)مؤرخ في 7 شوال عام 1436 الموافق 23 يوليو سنة2015،يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية،ج ر40 ليوم نفس اليوم ،ص28.

وكذا المادة(301) من ق.ع.ج والتي تعاقب كل من أفشى سر المهنة بالحبس من شهر إلى ستة أشهر،وبغرامة من 20000 دج إلى 100000 دج على إفشاء السر المهني[1].

أماّ القانون(09-04)،أضاف عنصر جديد مكلف بالكتمان، ونقصد بذلك مقدمي خدمات الانترنت وهذا بموجب المادة(10)من القانون السالف الذكر[2]،باعتبار أنّ مقدم خدمات الانترنت هو من الأشخاص المؤتمنين بحكم المهنة على أسرار المشتركين وعمليات التحقيق على حد سواء، وهذا حسب ما جاء في الالتزامات الملقاة على عاتقهم كما شرحنا سابقا[3].

لذلك فانّ الإخلال بمبدأ سرية التحقيق والتحقيقات القضائية، يعرض الشخص المكلف بالإجراءات الخاصة في جرائم الانترنت، والذي خوله القانون ذلك تحت طائلة قانون العقوبات وتحديدا نص المادة(301)، حيث على الضابط المكلف بالإجراء، ومقدم خدمات الانترنت معني بكتمان سر التحري والتحقيقات القضائية.

نص عليها المشرع الجزائري في المادة(10الفقرة2) من قانون (09-04) والتي تنص على أنه : "يتعين على مقدمي خدمات الانترنت كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق ". ولقيام هذه الجريمة لابد من توافر ركنين مادي و معنوي.

1-الركن المادي:

[1] المادة (1/301) من ق.ع.ج تنص على ما يلي"يعاقب بالحبس من شهر إلى ستة أشهر وبغرامة من 20000 إلى 100000دج الأطباء والجراحون والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلى بها إليهم وافشوها في غير الحالات التي يوجب عليهم فيها القانون إفشاءها ويصرح لهم بذلك."

[2]المادة10 من القانون (09-04)في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق."

[3] يرجى الاطلاع على المبحث الأول من الفصل الثاني من الباب الأول من هذه الرسالة ،ص118.

يتمثل الركن المادي لهذه الجريمة في إفشاء أسرار التحري والتحقيق، أي إذاعتها ونقلها واطلاع الغير عليها بعد أن كان العلم بها قاصرا على أصحابها أو الذين ائتمنوا عليها بحكم وظيفتهم [1]،حيث يعد سراً كل ما يعرفه الأمين أثناء أو بمناسبة ممارسة وظيفته او مهنته وكان في افشائه حرج لغيره[2]. ومادام مزود الخدمات مؤتمن على أسرار البحث والتحقيق ، فيتعين عليه كتمان سرية العمليات وبالتالي يشمل محل هذه الجريمة إفشاء العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، والمتعلقة بالتحري والتحقيق كالتعرف على مشترك الانترنت وبروتوكول الانترنت المعرف للمشترك والاتصالات التي أجراها.

2- الركن المعنوي:

جريمة إفشاء أسرار التحري والتحقيق هي جريمة عمدية لابد فيها من توافر القصد الجنائي العام ، فيجب أن يعلم الجاني بأنه يرتكب جريمة إفشاء أسرار التحري والتحقيق، وأن تتجه إرادته إلى ارتكاب هذه الجريمة[3]،حيث تقوم الجريمة بتوافر القصد الجنائي العام دون الخاص إلى جانب الركن المادي للجريمة المتمثل في إفشاء أسرار التحري والتحقيق من قبل مزودي خدمات الانترنت لذلك رتب المشرع المسؤولية الجزائية على الأفراد المختصين في اللجوء لهذه الإجراءات وهي وجوب احترام سرية البحث والتحري والتحقيق ،وهنا ليس فقط لصون احترام الحياة الخاصة، فالمتهم بريء حتى تثبت ادانته، ولكن لتحقيق السير الحسن للعدالة.

ج–جريمة عدم حفظ المعطيات المتعلقة بحركة السير:

نظمها المشرع في المادة (11فقرة 4و5)من قانون قم (09-04)والتي تنص على أنه دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات

[1] شيماء عبد الغني عطا الله، مرجع سابق، ص214

[2] احسن بوسقيعة، الوجيز في القانون الجزائي الخاص،الجزء الأول،المرجع السابق،ص279.

[3] احسن بوسقيعة، الوجيز في القانون الجزائي الخاص،الجزء الأول،المرجع السابق،ص280-281.

القضائية ، ويعاقب الشخص الطبيعي بالحبس من ستة(6)أشهر إلى خمس(5)سنوات وبغرامة من 50.000د ج إلى 500.000 د ج، أمّا الشخص المعنوي فيعاقب بالغرامة المقررة في المادة (18مكرر) من ق.ع.ج.

وتقوم هذه الجريمة على ركنين مادي ومعنوي على التفصيل الآتي:

1-**الركن المادي** :من قانون (09-04) وهي عدم حفظ مزودي الخدمات للمعطيات المنصوص عليها في المادة(11)يتمثل الركن المادي لهذه الجريمة في عدم احترام الالتزامات المنصوص عليها في المادة (3/11)و عدم حفظها للمدة المحددة قانونا وهي سنة ابتداء من تاريخ التسجيل وفقا المادة (11)[1] من القانون اعلاه.

وبالتالي يتمثل النشاط الإجرامي لهذه الجريمة في عدم حفظ المعطيات المتعلقة بحركة السير أصلا، أو عدم حفظها في المدة القانونية، أما محل الجريمة فيتمثل في المعطيات المتعلقة بحركة السير المنصوص عليها في المادة (11)من هذا القانون ولا تقوم هذه الجريمة بمجرد توافر المشاط الإجرامـــي، بل يتطلب المشرع لقيامها نتيجة معينة، وهي أن يؤدي عدم حفظ تلك المعطيات إلى عرقلة وتعطيل حسن سير التحريات القضائية بسبب عدم حفظ مزودي الخدمات للمعطيات أو عدم حفظها للمدة المحددة قانونا.

ويعاقب الشخص الطبيعي بالحبس من ستة أشهر إلى خمس سنوات وبغرامة من 50000إلى500.000دج،أما الشخص المعنوي فيعاقب بالغرامة المقررة في المادة (18مكرر)ق.ع.ج[2].

[1] المادة(7/11) من القانون(09-04)"...تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل"

[2]المادة(18 مكرر/1) ق.ع.ج "العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي:

1-الغرامة التي تساوي مرة الى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة...."

2-**الركن المعنوي** :فيجب أن يعلم الجاني بأنه هذه الجريمة عمدية لابد فيها من توافر القصد الجنائي العام نشاطه مجرم، وأنّه يتسبب في عرقلة حسن سير التحريات القضائية بسب عدم حفظه المعطيات المتعلقة بحركة السير .كما يجب أن تتجه إرادته إلى ارتكاب هذه الجريمة، وتحقيق النتيجة الإجرامية المتمثلة في عرقلة حين سير التحريات القضائية.

المطلب الثاني:حجية الدليل الجنائي في جرائم الانترنت في التشريع الجزائري.

يلعب القضاء دورا مهما في انفاذ القانون، بوضعه ضمانات حماية حقوق الإنسان حيّز التنفيذ، والدليل الجنائي في جرائم الانترنت شانه شان الأدلة الأخرى، لابد أن يخضع على قدم المساواة مع باقي الأدلة لقواعد القبول أمام القضاء، خاضع بذلك للسلطة التقديرية للقاضي ،وأول هذه القواعد هي المشروعية، لكن في مقابل ذلك وبعدكل الذي درسناه من خصائص للدليل الجنائي الالكتروني والمستمدة من ذاتية جرائم الانترنت نفسها، فان قبول الإثبات به يثير العديد من الإشكالات، بداية من وعاء هذا الدليل نفسه أي المنظومة المعلوماتية بمفهومها الواسع وصولا إلى الإجراءات الحصول عليه، ثم تقديمه وهذه الإشكالات لها علاقة وثيقة بقيمته في الإثبات وتقديره من طرف القاضي[1].

إذن فالإشكال ليست في تكوين الدليل الجنائي الالكتروني وصلاحيته أن يكون من أدلة الإثبات جرائم الانترنت، خصوصا أنّ هناك واقعة افتراضية تركت أثار لا محسوسة، ثم الحصول عليها وجمعها وتقييمها، وبالنتيجة شكلت أثار رقمية تم تحليلها وفق برامج معينة أعطت دليل معيّن[2]. لكن الإشكال الذي يثور، هل هذا الدليل يملك من المصداقية التي تعبر عن الحقيقة، اقتراف السلوك الإجرامي والذي، يمكن للقاضي الحكم به دون سواه؟لان الدليل الجنائي

[1] سعيد عبد اللطيف حسن،اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت،دار النهضة العربية،القاهرة،مصر،1999،ص149.

[2] فهد عبد الله العزمي،المرجع السابق،ص354،محمد فتحي محمد انور عزت، المرجع السابق،406.

الالكتروني قد يوجس في نفس القاضي الشك في قيمته الثبوتية[1]، فكل شك يفسر لصالح المتهم[2]، وهذا راجع بالدرجة الأولى إلى ذاتية الجرائم المرتبطة به، وطرق الحصول عليه التي قد يعتريها التزييف والتحريف، صعب الإثبات.لذلك كان لابد من توافر شروط تفضي إلى مصداقية وبالتالي قبولها كأدلة إثبات في المواد الجزائية وتحديدا جرائم الانترنت[3].

لقد أثار قبول الدليل الجنائي الالكتروني والدليل الجنائي في جرائم الانترنت عدة مشاكل؛ وشكل تحديا كبيرا أمام القضاء، خصوصا انّه دليل يعتمد على الخبرة في كل مراحل الحصول عليه وآليات الكشف والتحري والمحاكمة . والتي توجب أن لا يكون القاضي، كالقضاة الذين يحكمون في جرائم اقتصادية أو جرائم ضد الأشخاص العادية، بل يجب أن يكون ملما بمختلف التطورات الحاصلة في عالم الرقمية،وكأي دليل ورغم كونه حديثا فلا بد له من شروط لقبوله (الفرع الأول) ،وتبيان القيود الواردة على قبوله(الفرع الثاني).

الفرع الأول:شروط قبول الدليل الجنائي في جرائم الانترنت.

أهمية الدليل في المواد الجنائية أهمية عظيمة لأنه هو الذي يناصر الحقيقة ويبين مرتكب الجريمة، وهو الذي يحول الشك إلى يقين[4]،إنّ قبول الدليل من طرف القاضي عمليه هي مُقدمة على عملية تقدير الدليل، ذلك انّه لا يمكن الدخول في عملية التقدير دون أن يقبل هذا الدليل أصلا.كما أن أساس القبول أي قبول الدليل الجنائي الالكتروني، أن يكون مشروعا وهو أساس

[1] عبد الصبور عبد القوي على المصري، المحكمة الرقمية والجريمة المعلوماتية، دراسة مقارنة،مكتبة القانون والاقتصاد،الرياض، المملكة العربية السعودية،2012،ص353.

[2] المادة 56 من الدستور:"كل شخص يعتبر بريئا حتى تثبت جهة قضائية نظامية ادانته، في اطار محاكمة عادلة تؤمن له الضمانات اللازمة للدفاع عن نفسه"

[3] مدحت رمضان، المرجع السابق، ص72.

[1] Thierry Care Catherine Ginestet, Droit Penal – Procedure – Penale, Dalloz ed, 2000, P. 235.

قبوله في الإثبات الجنائي، والواقع أنّ المشرع الجزائري قد تبنى مبدأ حرية الإثبات[1]، في الإثبات الجنائي في المواد الجزائية وهذا بنص المادة (212) ق.ا.ج.ج.

اعتمد المشرع الجزائري حرية الإثبات في المواد الجنائية، ما عدا ما استثني بنص القانون، وعلى هذا الأساس فان حرية الإثبات هي التي سمحت بقبول الدليل الجنائي الالكتروني، ودعائم الإثبات الجنائي بعد تكييفها وفق التكنولوجيات الحديثة من جهة، معنى ذلك أن الشخص حر في تقديم الأدلة التي تثبت براءته بكافة الوسائل، فكل الأدلة العادية والعلمية متساوية في القيمة الثبوتية في المواد الجزائية، إلاّ بالقدر الذي تحدثه من اثر في نفس القاضي من ارتياح واطمئنان[2]، للحكم على أساسها.

وتجدر الإشارة أنّ المقصود بالقاضي، ليس هو قضاء الحكم فحسب، وإنما يشمل أيضا قضاء التحقيق باعتبار أنّ مشكلة الإثبات قد تثور في أي مرحلة تمر بها الدعوى العمومية، بل يمكن أن تثور قبل ذلك أي في مرحلة جمع الاستدلالات أيضا[3].

نظم المشرع دعائم الإثبات بموجب القانون[4]،كما اعتراف المشرع بوجود الدليل الجنائي الالكتروني، وهذا ما اقره بموجب المادة (6) من قانون (09-04)،إن الشرعية في التحصِّل على الدليل عموما والدليل الجنائي الالكتروني خصوصا، له أهمية كبرى لما في تحصيل الدليل من انتهاك لحقوق الأفراد، فقد تتأثر هذه الأدلة الأخيرة بالتقدم العلمي، وذلك إذا ما استخدمت الأجهزة

[1] تتقاسم عملية الإثبات الجنائي نظامين أساسين، نظام الإثبات الحر أو المعنوي الاقتناع الشخصي للقاضي هو الذي يتحكم في قرار القاضي، لذلك هو يكرس مبداحرية القاضي في الاقتناع، محمد مروان، المرجع السابق،ج1،ص39. ونظام الإثبات المقيد أو الإثبات القانوني، المشرع هو الذي يحدد وسائل الإثبات فيقر قواعد قانونية ثابتة.،فالقاض يقتصر دوره على فحص مدى توفر الأحكام القانونية المتعلقة بالإثبات، محمد مروان ، المرجع السابق،ج1، ص35.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص184.

[3] عائشة بن قارة مصطفى، المرجع السابق، ص192.

[4] يرجى الرجوع إلى المبحث الثاني من الفصل الثاني من الباب الأول لهذه الرسالة،ص136.

الحديثة وتكنولوجيات الإعلام والاتصال في الحصول على الدليل،وهي السمة الغالبة على إجراءات التحقيق والتحري الخاصة بجرائم الانترنت، وهنا نكون أمام إجراءات باطلة تمس نزاهة الدليل ووجوب ابتعاده عن الغش والخداع. ، وبالتالي استبعاده من الدعوى لعدم مشروعيته.[1]

إنّ مبدأ مشروعية الدليل الجنائي بما يتضمنه من مخرجات كمبيوترية، وضرورة اتفاق الإجراء مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع[2]، أي أن قاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع، بل يجب أيضا مراعاة إعلانات حقوق الإنسان والمواثيق والاتفاقيات الدولية[3]، وكما يمكن أن يتحصل على دعائم الإثبات بطرق غير مشروعة، فانّه كذلك الحال بالنسبة للدليل الجنائي الالكتروني، فيمكن في الكثير من الأحيان الحصول عليه بطرق تعتبر غير مشروعة، كاستخدام الهاكر المسبوق قضائيا، من اجل الوصول إلى الدليل طبعا عن طريق استعمال الخبرة التقنية، حيث تعتبر من الأعمال غير المشروعة للحصول على الدليل الجنائي الالكتروني، هي عملية التحريض على ارتكاب الجريمة عبر الانترنت، من قبل رجال الضبطية القضائية كالتحريض على الغش أو التزوير المعلوماتي والتجسس المعلوماتي، الاستخدام غير المصرح به للحاسب..الخ التنصت والمراقبة الالكترونية عن بعد لشبكات الحاسب الآلي دون إذن[4].

أولا:يقينية الدليل الجنائي في جرائم الانترنت.

هي الحالة الذهنية والعقلانية التي تؤكد وجود الحقيقة عن طريق ما تستنتجه وسائل الإدراك عند القاضي، وهذا من خلال ما يُعرض عليه، وما ينطبق في ذهنه من تصورات على قدر عالي من التأكيد[5]. لذلك يجب أن تصل قيمة الدليل إلى درجة القطعية من الناحية العلمية البحثة من

[1] Thierry Care – Catherine, Op. Cit, P. 245.

[2] جميل عبد الباقي الصغير ،أدلة الإثبات في التكنولوجيا الحديثة، المرجع السابق،ص110.

[2] هلالي عبد الاه احمد،حجية المخرجات الكمبيوترية في المواد الجنائية،المرجع السابق،ص118.

[4] هلالي عبد الاه احمد، حجية المخرجات الكمبيوترية في المواد الجنائية ، المرجع السابق، ص124.

[5] على محمود حمود، المرجع السابق، ص23.

ناحية، ومن ناحية أخرى ألاّ يكون في الأخذ بهذا الدليل العلمي المساس بحريات الأفراد إلا قبول كل ما يتمخض عن المنظومة المعلوماتية وشبكاتها من أدلة إثبات أو نفي.

معنى اليقين أن تكون الأدلة الجنائية الالكترونية غير قابلة للشك[1]، وان سلامة الحكم القضائي له علاقة وثيقة بمدى سلامة الدليل الجنائي الالكتروني وتقديره[2]،يمكن الوصول إلى اليقين بالنسبة للدليل الجنائي الكتروني عن طريق نوعين من المعرفة أولها المعرفة الحسية التي تدركها الحواس والأخر المعرفة العقلية التي يقوم بها العقل عن طريق التحليل والاستنتاج، وهكذا يمكن أن نلخص إلى أن المحقق أو القاضي الذي يعاين جسم الجريمة سواء كانت عادية أو جريمة انترنت عن طريق حواسه لا يمكنه معاينة الفعل الجنائي لحظة وقوعه وإنما يعاين فقط النتائج التي تترتب عليه[3]،وعن طريق التحليل والاستنتاج يمكنه التوصل إلى الكيفية التي تمت بها الجريمة والأدلة التي استخدمت والآثار التي تدل على شخصية مرتكبها ومراحل تنفيذها من قبل فاعليتها كما حدث على ارض الواقع[4]، فاليقين والاقتناع والحقيقة عبارة عن حلقات ثلاث في سلسلة واحدة بدايتها اليقين وهذا اليقين يتدرج من الضعف إلى القوة مع تدرج السير في إجراءات الدعوى الجنائية، ويواكب هذا التدرج أخر في الاقتناع، وعندما يكتمل اليقين ينشا ما يسمى بالاقتناع اليقيني، وهو أساس الحقيقة القضائية التي ينشدها القاضي في حكمه[5].

ثانيا:مناقشة الدليل الجنائي في جرائم الانترنت.

إن من تطبيقات مبدأ شفوية المحاكمة، مناقشة الأدلة المطروحة أمامها ومن بينها الدليل الجنائي الالكتروني ودعائم الإثبات، وهو اطلاع أطراف الدعوى عليها-اي الاطلاع على الأدلة-

[1] فهد عبد الله العبيد العازمي، المرجع السابق، ص388.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص179.

[3] سليمان احمد محمد ابو الفضل،المرجع السابق،ص287.

[4] هلالي عبد الاه احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق،ص79-80.

[5] هلالي عبد الاه احمد حجية المخرجات الكمبيوترية في المواد الجنائية المرجع السابق،ص83.

وهذا احتراما لحقوق الدفاع[1]، و الهدف منه مواجهة كل طرف بالأدلة التي تكون في الدليل الجنائي في الانترنت، عن طريق بيانات معروضة على الشاشة أو غيرها من حاملات البيانات، والمستخرجات وهذا بالفعل ما جسدته المادة2/212من قانون الإجراءات الجزائية الجزائري. فالقناعة التي تولدت لدى القاضي هو جزء من مناقشة تلك الأدلة التي عن طريقها تتضح قوة الأدلة من ضعفها، وبالتالي فستبنى لدى القاضي قناعة بتلك الأدلة أو بتركها[2].

فيترتب عن ذلك، انّه يجب مناقشة كل أشكال الدليل الجنائي في جرائم الانترنت بما فيها الدليل الجنائي الالكتروني، أي صورته التي يمكن انْ يفهمها القاضي وأطراف الدعوى من شهود وضحايا، والتي تتجسد في أشرطة وأقراص ممغنطة،كما انّه ولدعم مناقشة سليمة لهذه الأدلة لابد من وجود خبير إثناء الجلسة لشرح هذا الدليل، لأنّه من الناحية التطبيقة هو دليل معقد جدا[3].

إن المرافعات تكون شفوية وحضورية، وهذا لمناقشة جميع الأدلة المطروحة في الجلسة، وعلى ذلك فانّ كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات، يجب أن يعرض في الجلسة، ليس من خلال ملف الدعوى في التحقيق الابتدائي، لكن بصفة مباشرة أمام القاضي، أي في الجلسة، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسبات الآلية والهواتف النقالة ومختلف أجهزة الولوج إلى الإنترنت، وأيضا بالنسبة لشهود الجرائم الانترنت، الذين يكون قد سبق أن سمعت أقوالهم في التحقيق الابتدائي، فانّه يجب أن يُعيدوا الإدلاء بأقوالهم مرة أخرى من جديد أمام المحكمة [4].

---

[1] محمد حسين الحمداني و نوفل على الصفو، مبدا الاقتناع القضائي، مجلة الرافدين للحقوق، مجلد 1 السنة العشرة، عدد24 سنة 2005،ص.250.

[2] راغب محمد غلاب،المرجع السابق، ص413.

[3] ويتم ذلك عن طريق تقييم الدليل للتاكد من مصداقيته عن طريق التحقق من سلامته من كل عبث عن طريق فكرة التحليل التناظري الرقمي، ويستعاد في هذا بعلم الكمبيوتر، للكشف عن وجود تلاعب من عدمه واستخدام الخوارزميات، وهي عمليات حسابية خاصة، او عن طريق استعمال الدليل المحايد وهو نوع من الادلة الرقمية المخزنة في البيئة الافتراضية لا علاقة له بموضوع الجريمة يساعد في التاكد من سلامة الدليل الرقمي وعدم الحصول أي تعديل عليه،خالد عياد الحلبي، المرجع السابق،ص249.

[4] هلالي عبد الاه احمد، حجية المخرجات الكمبيوترية في المواد الجنائية ،المرجع السابق ،ص104.

وهو الحال كذلك لخبراء الأنظمة المعلوماتية على اختلاف تخصصاتهم، ينبغي أن يمثلوا أمام المحاكم لمناقشتهم أو مناقشة تقاريرهم التي خلصوا إليها إظهارا للحقيقة وكشفا للحق، وأخيرًا فان متحصلات جريمة الانترنت، التي يتم ضبطها يجب أن تعرض على القاضي شخصيا بكافة عناصرها، ذلك لان حياد القاضي يوجب عليه أن لا يُقيم قضاءه إلّا على ما طرح أمامه وكان موضوع الفحص والتحقيق والمناقشة[1].

وفي مناقشة الدليل الجنائي الالكتروني لابد من أن يكون أعضاء الهيئة المكلفين بهذه الإجراءات ماثلين أمام هيئة المحكمة، باعتبار أنّ لهم الاختصاص الأصيل في تحري والبحث واثبات جرائم الانترنت، إما كخبراء أو كشهود بحسب وضعهم القانوني، وسبق أن وضحنا ذلك في فصول سابقة[2].

الفرع الثاني:مدى حرية القاضي في تقدير الدليل الجنائي في جرائم الانترنت.

إن أهمية الدليل في المواد الجنائية أهمية عظيمة لأنه هو الذي يناصر الحقيقة ويبين مرتكب الجريمة، وهو الذي يحول الشك إلى يقين[3]، ولا يغيب عن الذهن أن البحث عن الدليل يجب أن يتم في إطار الشرعية الإجرائية[4]، وفي إطار مبدأ أن الأصل في المتهم البراءة، فالحق في الدليل يجب أن يتركز على حماية كرامة وشرف الإنساني، وحتى يكون للقاضي السيطرة الكاملة في الدعوى الجزائية ، لا بد له أن يكون على دراية واسعة بالأدلة العلمية الحديث ،لأنها تكون محل مناقشة من قبل الأطراف، فيكون أي ألقاض قادرا على استيعاب هذه المناقشة؛ ممـــا ينجح المهمة الكـلف بها [5]، لدلك فنحن ندعو أن يكون قضاة الموضوع والذين يكلفون بهذا النوع من القضايا أي المتعلقة بجرائم الانترنت أن يكونوا مما سبق لهم الدراسة والتكوين في مجال تكنولوجيات الإعلام

[1] هلالي عبد الاه احمد، حجية المخرجات الكمبيوترية في المواد الجنائية ،المرجع السابق ،ص105.

[2] يرجى الرجوع الى المبحث الثاني من الفصل الثاني من الباب الأول من هذه الرسالة،260.

[3] Thiery Care- Catherine Ginestet , Op. Cit,P. 235

[4] جمال الحيدري، ضوابط اعتبار المخرجات الالكترونية أدلة إثبات في القضايا الجزائية، مجلة العلوم القانونية، العدد1 المجلد، 21، 2006،ص75.

[5] منى فتحي احمد عبد الكريم، المرجع السابق،ص125.

والاتصال، فالأمر لا يتعلق بفهم واستيعاب قوانين تكنولوجيات الإعلام والاتصال، الذي يكون على شكل دورات تكوينية لمدة أيام فقط، بل هو ابعد من ذلك لفهم خبايا العالم الافتراضي وبالتالي فهم السلوك التقني الإجرامي مما يسهل على القاضي استيعاب الدليل الجنائي الالكتروني[1].

يقصد بحرية القاضي في تكوين اقتناعه الذاتي أن تكون له كامل الحرية في أن يستمد اقتناعه من أي دليل يطمئن اليه، من الأدلة التي تقدم في سياق الدعوى، دون أن يتقيد بدليل معين بذاته، طبعا إلا ما نص عليه القانون[2]، بحثا عن الأدلة اللازمة لتكوين اقتناعه[3].

فالقاعدة إذاً أن تقدير الدليل الجنائي الالكتروني، هو مما تستقل به محكمة الموضوع، التي لها سلطان مطلق في استخلاص ما تقتنع به، ويطمئن لها ضميرها[4]، إنّ القاعدة في الدليل الجنائي الالكتروني، أن تكون الأدلة مما يقبلها القانون وبالتالي تخضع هذه الأدلة لمبدأ حرية القاضي الجزائي في الاقتناع بها وصولا للحقيقة[5].

أولا:الاقتناع الحر للقاضي.

حتى يبنى الحكم على يقين ينبغي أنْ يُمنح القاضي من السبل والوسائل ما يمكنه من الوصول إلى الحقيقة في الواقعة المطروحة عليه[6]، ومن المقرر قانوناً أنّ عبء الإثبات في المواد الجنائية يقع على النيابة العامة، بحيث أن الجاني معفى من هذه المسألة، والسبب في ذلك يرجع إلى كونه يستفيد من مبدأ أساسي وهو مبدأ افتراض براءة المتهم، وان عبء الإثبات حسب قاعدة

[1] ولما يتعلق الأمر بالجنايات ووجود المحلفين الذي أصبح عددهم أربعة بموجب تعديل قانون الإجراءات الجزائية، هنا ننوه إلى ضرورة أن ينتقى المحلفين بعناية وممن تتوافر لديهم دراية بالانترنت ومجالات استعمالها.

[2] منى فتحي احمد عبد الكريم ، المرجع السابق،ض124.

[3] بن فردية محمد،الدليل الجنائي الرقمي وحجيته امام القضاء الجزائي(دراسة مقارنة)، المجلة الاكاديمية للبحث القانوني ، جامعة عبد الرحمان ميرة، بجاية كلية الحقوق والعلوم السياسة، سنة5 المجلد9 عدد2014،1.ص282.

[4] مصطفى يوسف، المرجع السابق،46.

[5] فهد عبد الله العبيد العازمي، المرجع السابق، ص356.

[6] حسن صادق المرصفاوي،أصول الإجراءات الجنائية ،منشاة المعارف الإسكندرية،مصر،1996،ص625.

البراءة المفترضة دوما في المتهم على من يدعيها، وسلطة الاتهام تتحمل عبء الاتهام كأصل عام[1].

مبدأ حرية القاضي الجنائي في تكوين عقيدته، وصول القاضي بعقله ووجدانه إلى درجة اليقين التام دونما أي شك بحقيقة الواقعة محل الادعاء والتي تكون إدانة المتهم أو براءته[2]، وان كان القاضي غير مكلف بتبيان أسباب اقتناعه الشخصي إلا انّه مكلف بتبيان أسباب الحكم الذي انتهى إليه[3]،هذا وان قضاة التحقيق لا يقدرون أدلة الإثبات إلا من ناحية مدى كفايتها للاتهام[4]، للاتهام[4]، أي يكفي لتبرير الاتهام، بمعنى تواجد دلائل تقرب من أنّ المتهم هو الفاعل في هذه الجريمة، فالشك يفسر ضد المتهم في مرحلة الاتهام ويفسر لصالحه في المرحلة اللاحقة وهي الحكم[5]،"الاقتناع أن يتوفر لدى القاضي من الأدلة الوضعية ما يكفي لتسبيب ادعائه بالتسليم بثبوت الوقائع كما أثبتها في حكمه ونسبتها إلى المتهم"[6].

واقع أن الدليل الجنائي في جرائم الانترنت، والدليل الجنائي الالكتروني، يطرح صعوبات التحصل عليه ثم الاحتفاظ به، ولكن هناك صعوبة أخرى وهي مدى إمكانية اقتناع قاض الموضوع بهذا الدليل، خصوصا أنّ له الحرية التامة في النظر بتقديم أي دليل يراه لازما لإظهار الحقيقة[7]، حتى وان وصف ان هذا الدليل هو دليل علمي، والأصل أن الدليل الذي يتم مناقشته في المحكمة هو الدليل الأصل أي ليس النسخة طبق الأصل، وهذا ما لا يمكن حدوثه في الدليل الجنائي الالكتروني، ولكن ما يقف إلى جانب الدليل الجنائي الالكتروني ومدى اقتناع قاض الجنائي به هو دخول عدة أدلة علمية حديثة دائرة الإثبات الجنائي، مما يفتح الطريق أمامه لان يتفحصه القاضي

[1] سامح احمد البلتاجي موسى،المرجع السابق،ص314.
[2] سامح احمد البلتاجي موسى،المرجع السابق ،ص334.
[3] منى فتحي احمد عبد الكريم ،المرجع السابق، ص124.
[4] جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، المرجع السابق، ص15.
[5] منى فتحي احمد عبد الكريم ،المرجع السابق، ص125.
[6] عبد الحكيم فوده ،المرجع السابق، ص24.
[7] محمد مروان،المرجع السابق،ج2، ص471.

الجنائي، ولا يُطرح جانبا بحجة انّه نسخة[1]، وليس أصلا، فمثلا إن الأدلة يمكن أن تحتويها ملفات، حيث يتم تخزينها في الحاسوب والطابعة....بل ويمكن أن يكون الدليل متضمنا النظام ألاسترادادي للملفات التي تحتويه،كما هو الشأن في حالة حذف الملفات باستخدام خاصية الإلغاء، فيقوم الخبراء باستخدام خاصية الاسترداد، حتى وان شمل إلغاء ملف الانترنت المؤقت الذي يأخذ نسخة من كل صفحة يتم الولوج إليها عبر الانترنت، وفي هذه الحالة تثار مسالة مدى جدوى الدليل المسترد واثر الحذف عليه[2].

فلو قلنا أنّ القاضي الجنائي لا يأخذ بالدليل الجنائي الالكتروني لأنه ليس الأصل، هنا لكونه بالضرورة أمام دليل نفي للمتهم وبالتالي براءة المتهم مما نسب إليه وبالتالي رفض الدليل الجنائي الالكتروني كدليل للإثبات في جرائم الانترنت، وبقي لدينا فقط أدلة عادية ،تحمل من نقاط الضعف الكثير لإثبات جرائم الانترنت لذلك كان لابد من حل تشريعي يفصل في ذلك وهذا ماقام به المشرع الجزائري في القانون (09-04) تم تطويرها لكي تشمل الدليل الجنائي في شكله الالكتروني، وبالتالي للدليل الجنائي الالكتروني، نفس درجة ومكانة الأدلة الأخرى إن لم نقل أعلى درجة، بالمقارنة مع فكه لغموض السلوك الإجرامي، في جرائم الانترنت، والجرائم الملحقة بها.

رغم أن القاضي له الحرية في تكوين عقيدته في كل الأدلة المطروحة أمامه الشرعية وغير الشرعية، فليس له اعتماد الدليل الذي تم الحصول عليه بطريقة غير شرعية، على انّه في اسناد البراءة لا تتطلب مشروعية الدليل الجنائي في جرائم الانترنت[3]، بما في ذلك الدليل الجنائي الالكتروني، فحرية اقتناع القاضي مرتبطة بمشروعية الدليل الجنائي الالكتروني، إذن فالإشكال ليس

[1] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص987.

[2] عمر محمد بن يونس أبو بكر ،الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص.988

[3] احمد عوض بلال،المرجع السابق،ص22.

في قيمة الدليل الجنائي الالكتروني بل في طريقة الحصول عليه[1]، التي قد تشكل انتقاصا من الحريات في سبيل الحصول عليه، وهو ما لا حظنا في آليات الحصول على الدليل الجنائي الالكتروني، ولكن في المقابل لن يطرح القاضي جانباً مجمل الضمانات التي وضعها المشرع للحصول عليه حتى انّه انشأ هيئة بمكافحة والوقاية جرائم الانترنت ومنها إجراءات الإثبات.

ثانيا:القيود الوارد على حرية القاضي.

لقد ذكرنا سابقا أنّ الدليل الجنائي الالكتروني ينتمي إلى الأدلة العلمية، التي أقرها المشرع الجنائي بأن لها حجية في الإثبات كما هو الحال بالنسبة للبصمة الوراثية[2]، ومادام قد نص عليه المشرع في القانون ما على القاضي إلاّ الاخد به، فهناك أدلة إلكترونية قد ساعد في الحصول عليها استخدام الوسائل الإلكترونية مثال ذلك، استخدام أجهزة الرادار وكاميرات التصوير، وكاميرات الفيديو[3] والوسائل الحديثة في التصنت، والتسجيلات بمساعدة مسجلات الصوت، والتي تستخدم في ضبط الكثير من الجرائم[4]، تلك الأدلة التي أخد بها المشرع وقبلها القضاء في إطار مجموعة من الشروط من أهمها أن يتم الحصول عليها بطريقة شرعية ونزيهة، وان يتم مناقشتها حضوريا عن طريق الأطراف، وهذا ما قام بإدراجه المشرع الجزائري في تعديله لقانون الإجراءات الجزائية السابق الذكر في المادة (65 مكرر5) إلى المادة (65 مكرر10) تحت عنوان في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

[1] منى فتحي احمد عبد الكريم ،المرجع السابق، ص126و127.

[2] قانون (16-03)مؤرخ في 14 رمضان عام 1437 الموافق 19 يونيو سنة 2016، يتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص.ج ر رقم 37 ليوم 17 رمضان عام 1437 الموافق 22 يونيو سنة 2016 م ،ص5.

[3] مرسوم رئاسي رقم(15-228)مؤرخ في 7 ذي القعدة عام 1436 الموافق 22 غشت سنة2015، يحدد القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو وسيره. ص3

[4] Gaston Stefani et Georges Levasseur et Bernard Bouloc, procédure pénale, 17 édition , Dalloz 2000 .P.35.

ولكن انتشار الأدلة العلمية، يدفع بالبعض إلى الاعتقاد بأنّه باتساع مساحة الأدلة العلمية ومنها الدليل الجنائي الالكتروني، بمقدار ما يكون انكماش وتضاؤل دور القاضي الجنائي في التقدير[1]، فان كان الأصل كما ذكرنا سابق هو حرية القاصي في تكوين عقيدته واقتناعه الشخصي، هي قاعدة لها استثناء ولكل حرية قيد، وينبغي استبعاد هذا التصور، وذلك لان الدليل العلمي يخضع لأمرين الأمر الأول القيمة العلمية القاطعة للدليل[2]، الأمر الثاني الظروف والملابسات التي وجد فيها هذا الدليل[3]، بمعنى أن القاضي ليس له أن يناقش القيمة العلمية لهذا الدليل، فقد تّم عن طريق خبرة من طرف خبير مختص وهذا خارج مجال اختصاص القاضي، فللقاضي أن يكون ملما بالتطور الحاصل في مجال تكنولوجيا الإعلام والاتصال، ولكن ليس له أن يقدر القيمة العلمية للدليل الجنائي الالكتروني الإثباتية، بمعنى مدى ثبوت إدانة الشخص من عدمه، أما الظرف الثاني وهي الملابسات التي وجد فيها الدليل فإنها تدخل في نطاق تقديره الذاتي، فهذا من طبيعة عمله[4] ، حيث أن له السلطة التقديرية والاقتناع الذاتي الذي يجعله متحررا من كل القيود من اجل إحقاق الحق، فالدليل الجنائي الالكتروني قوة من الناحية العلمية، ولكن تقدير الظروف والملابسات التي أحاطت بالسلوك الإجرامي هي من تقدير القاضي الجنائي ومن هذا المنطلق، فان هذه السلطة التي أعطيت للقاضي يوما جسدتها المادة (307) من قانون الإجراءات الجزائرية، قد تحول دون وقوع الكثير من الإخفاقات وإدانة المتهم بمجرد أن الدليل العلمي ومنه الدليل الجنائي الالكتروني قد اثبت تقرير الخبرة أن المتهم هو الفاعل خصوصا أن جرائم الانترنت فيها من التعقيدات، ما سهل اتهام اشخاص أبرياء.

[1] عائشة بن قارة مصطفى، المرجع السابق،ص248.

[2] جميل عبد الباقي الصغير، أدلة الإثبات والتكنولوجيا الحديثة،المرجع السابق،ص22و هلالي عبد إلاه احمد ، حجية المخرجات، المرجع السابق،ص47.

[3] هلالي عبد إلاه احمد ، حجية المخرجات، المرجع السابق ،ص46.

[4] هلالي عبد إلاه احمد ، حجية المخرجات، المرجع السابق المرجع نفسه،ص46.

اذا حالات أو الاستثناءات على حرية القاضي، هي الحالة المتعلقة بإثبات جريمة الزنا[1] ، وكما يستبعد الدليل المستنبط من مراسلات المحامي[2] ، كما انه تقرر قوة ثبوتية لبعض المحاضر التي لا تقبل الطعن فيها إلا بالتزوير[3] ، والأكيد أن إثبات المسائل غير الجزائية يحترم فيها الإثبات المنصوص عليه في المواد المراد إثباتها، ولقد نص المشرع الجزائري على مبدأ حرية الإثبات الجنائي بالنسبة لمرحلة المحاكمة في المادة (1/235) من ق.إ.ج.ج بقولها: " يجوز للجهة القضائية إما من تلقاء نفسها أو بناءًا على طلب النيابة العامة أو المدعي المدني أو المتهم أن تأمر بإجراء الانتقالات اللازمة لإظهار الحقيقة ." غير انه ترد استثناءات وهي من القيود الواردة على حرية اقتناعه.

أ–جريمة الزنا في التشريع الجزائري.

فهذه الجريمة نصت عليها المادة (341) ق.ع.ج، حيث أوردت على سبيل الحصر أدلة إثبات هذه الجريمة في:

– محضر إثبات التلبس بالجنحة الذي يحرره ضابط الشرطة القضائية،

– الاعتراف الصادر من المتهم ضمن رسائل أو مذكرات يصف فيها فعل الزنا بصراحة ووضوح,

– الإقرار القضائي, أي اعتراف المتهم أمام القضاء بكل أو بعض ما هو منسوب إليه.

و من هنا فنجد أن هذه الأدلة الثلاثة قد وجدت على سبيل الحصر ،لا يجوز التوسع فيها، و لا القياس عليها.

[1] لإثبات جريمة الزنا:المادة(341)ق .ع.ج الدليل الذي يقبل عن ارتكاب الجريمة المعاقب عليها بالمادة (339) يقوم اما على محضر قضائي يحرره احد رجال الضبط القضائي عن حالة تلبس وأما وارد في رسائل او مستندات صادرة من المتهم وإما باقرار قضائي.والمادة من ق.ا.ج.ج

[2] المادة (217) من ق. ا. ج .ج "لا يستنبط الدليل الكتابي من المراسلة المتبادلة بين المتهم ومحاميه".

[3]المادة (218) من ق. ا .ج .ج"إنّ المواد التي تحرر عنها محاضر لها حجيتها إلى أن يطعن فيها بالتزوير تنظمها قوانين خاصة".

و عليه فان المحكمة إذا ما اعتمدت في تكوين قناعتها و إدانة المتهم على محضر لم يحرر من ذوي الاختصاص عن حالة أو على حالة شهادة شهود، أو غير ذلك من وسائل الإثبات غير المحددة في نص المادة (341) ق.ع.ج،فان حكمها سيكون مخالفا للقانون تحت طائلة البطلان.[1]

ب- إثبات المسائل غير الجزائية.

إن إثبات المسائل غير الجزائية التي يتعلق الجرم بها يجب أن يكون بإتباع قواعد الإثبات الخاصة بها، وهذا يعني أن يتطلب من القاضي عندما تثار أمامه مسألة غير جزائية –مدنية–تابعة للدعوى العمومية، وكانت هذه المسألة تحتاج إلى إثبات أن يتبع طرق الإثبات الخاصة التي تطبق على هذه المسائل فيما لو كان النزاع غير منظور أمام المحكمة الجزائية، ويشترط الفقه توافر شرطين لتقيد القاضي الجنائي بطرق للإثبات غير جزائية في مواد غير جزائية في الدعوى العمومية،ان لا تكون الواقعة محل التجريم هي نفسها محل الإثبات، أي الواقعة غير الجزائية سابقة على الجريمة، وان تكون القوانين المنظمة للواقعة غير جزائية لازمة للفصل في الدعوى العمومية[2].

ج-استبعاد بعض وسائل الإثبات.

هناك بعض الأدلة لا يجوز الأخذ بها في الإثبات في المواد الجزائية، وهذا لأن الأخذ بها يخل بحق الدفاع، لهذا قام المشرع الجزائري باستبعادها وعدم الأخذ بها كوسيلة من وسائل الإثبات، حيث نصت في هذا الصدد المادة (217) من ق.إ.ج.ج المعدل والمتمم على ما يلي: "لا يستنبط الدليل الكتابي من المراسلة المتبادلة بين المتهم ومحاميه."، بالتالي يمكن القول بأنه لا يمكن الاستعانة برسالة قام بإرسالها المتهم إلى محاميه يعترف فيها أنّه قام بارتكاب الجريمة كدليل ضده لإثبات الجريمة بحقه .

[1] قرار صادر بتاريخ 02-07-1989 ملف رقم59100 المجلة القضائية عدد ثالث1991،ص112.

[2] محمد حسين الحمداني و نوفل على الصفو، المرجع السابق،ص285.

د- القوة الثبوتية لبعض المحاضر: لا يوجد دليل له قوة ثبوتية أكثر من دليل آخر، فجميع الأدلة تحمل نفس القوة الثبوتية إذا اقر المشرع حرية الإثبات في المواد الجزائية، إلا أنه قد وجد في القانون الجزائري استثناءات لبعض المحاضر طبقا لنص المادة (218) من ق.إ.ج.ج التي نصت على أنّه: " إن المواد التي تحرر عنها محاضر لها حجيتها إلى أن يطعن فيها بالتزوير تنظمها قوانين خاصة ."ومن الأمثلة على هذه المحاضر نجد: محاضر الجمركية، محاضر مفتشي مديرية التجارة، محاضر الجلسات في المحاكمة، محاضر التحقيق الصادرة عن قاضي التحقيق، وغيرها.

فالقاعدة العامة كما ذكرنا هي حرية القاضي في تقدير الأدلة، ومنها الدليل الجنائي الالكتروني، ولكن هناك محررات وبالضبط محاضر لها حجية، والواقع يثبت انّ القاضي يتقيد بها، رغم أنّ حجية هذه المحاضر ليست مطلقة بل قابلة لإثبات العكس، وهنا قد يكون القاضي مقيد بمحاضر الضبطية التي تحرر في إطار جرائم الانترنت فمعظم الجرائم المعروضة على قضاة الموضوع يتم الحكم بالإدانة باعتبار انّها جرائم تتطلب دراية بالمعلوماتية، وبالتالي لا مجال لوجود حسن النية.

وفي الأخير فان إجراءات الإثبات الجنائي في جرائم الانترنت، إجراءات مهمة وخطيرة في نفس الوقت، فبدونها لا يمكن الحصول على الدليل في جرائم الانترنت سواء تعلق الأمر بالدليل الجنائي الالكتروني أو دعائم الإثبات، بالمقابل تنتهك الحق في الحياة الخاصة بالدرجة الأولى وباقي الحقوق، ومن كل ماسبق قد يصبح في المستقبل الاعتماد الكلي على (TCP/IP) كدليل جنائي دو حجية، ويصبح قيد يرد على حرية الاقتناع الشخصي للقاضي، رغم انّه دليل كامل في البيئة الافتراضية لابد له من دعائم إثبات في البيئة الواقعية كي تكتمل العملية الاثباتية.

الخـــاتمـــة

من خلال ما سبق وبعد استعراضنا بالبحث والدراسة، لموضوع إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، تبين جليا مدى تأثر كل مجالات الحياة بتطور تكنولوجيات الإعلام والاتصال، وبالأخص السلوك الإجرامي ودليل إثباته.فقد حاولنا قدر الإمكان تبسيط الجانب الفني في هذا النوع من الجرائم المستحدثة دون إهمال الجانب القانوني والذي هو محور البحث،فالدمج الحاصل بين القانون والتكنولوجيات الإعلام والاتصال هو صبغة الموضوع .

فلا أحد يمكنه الإنكار أنّ الإنترنت قد أثرت في سلوكيات الأفراد، وفي إجراءات التحري والتحقيق وفي دليل الإثبات الجنائي نفسه، وبالتالي ظهرت أو استحدثت مصطلحات ومفردات جديدة كليا في المعنى والمبنى، ويمكن أن نلخص أهم النتائج المتوصل إليها من خلال هذه الدراسة، والتي كانت إجابة عن التساؤلات التي طرحناها سابقا،والنقائص التي سجلت عليها في النقاط التالية:

-إنّ تكنولوجيات الإعلام والاتصال و الإنترنت بالتحديد هي سمة العصر، وهي في تطور مستمر، وما دامت كذلك فانّ البحث في موضوعها متجدد دائما، وتشغل حيزا واسعا في المجال القانوني لا يمكن تجاهله، زيادةً على حجم الجريمة، وتعدد صورها بحيث أصبحت الانترنت وسيلة لمساعدة للإخفاء أو التمويه وحتى لتبيض الأموال والمتاجرة بالمخدرات ، وإرهاب دول وشعوب على حد سواء، والقتل والتشجيع على الانتحار.

- لم يدرج المشرع الجزائري العديد من جرائم الإنترنت وعلى رأسها الجرائم التقنية و غيرها من جرائم الانترنت، ولما كان يحظر القياس في المواد الجنائية وهو المبدأ المقرر في المادة الأولى من قانون العقوبات لذلك ننوه إلى ضرورة إعادة النظر في جرائم الإنترنت في التشريع الجزائري وخصوصا الجرائم التي تستخدم فيها الانترنت كوسيلة.

-واستخدام مصطلحات موحدة في الإجراءات الجزائية كلما أمكن، باعتماد الترجمة السليمة للمصطلحات، فقد استعمل مصطلح الاختراق في قانون الوقاية من الفساد ثم مصطلح

التسرب في باقي الجرائم الخاصة من بينها جرائم الانترنت،كما استخدم مصطلح التسليم المراقب في قانون الفساد ثم مصطلح المراقبة في جرائم الانترنت أي لابد من توحيد المصطلحات الإجرائية في الجرائم الخاصة وكل الإجراءات، وذلك بدراسة وإعادة صياغة وتوحيد المصطلحات بين القوانين الخاصة وقانون الإجراءات الجزائية.

– أثرت الإنترنت في السلوك الإجرامي، وأبرزت للوجود مجرمين لم يتم التعرف عليهم إلاّ بعد انتشارها، ومع التطور الرهيب لم يصبح من متطلبات جرائم الانترنت، أن يكون مجرم الانترنت، ذو معرفة وقدرات عالية ماعدا الجرائم التقنية أما باقي الجرائم التي تكون فيها الانترنت وسيلة، فالمعرفة البسيطة لأبجديات الدخول والولوج إلى المواقع الالكترونية سهلت من ارتكاب جرائم الانترنت، بعدما بسَّطت التكنولوجيا التعامل مع وسائل الإعلام و الإتصال من هواتف ذكية بالإضافة إلى التطبيقات التي تحمل مجانا.

–إنَّ أهم عمل قضائي تأثر بالانترنت هو الإجراءات القضائية والجزائية بالأخص، حتى أنّه يطلق عليها الإجراءات الخاصة أو الاستثنائية، لأنّها تمس بحق أصيل هو الحق في الحياة الخاصة بالدرجة الأولى، الحق واجب الحماية بموجب مواثيق دولية وقوانين وطنية، كالمراقبة الاتصالات الالكترونية، والتفتيش عن بعد، والذي كانت فيه أي هذا الإجراء تغليب المصلحة العامة عن الخاصة ، وتمت ملاحظة أنَّ هناك العديد من النقائص التي لحقت هذه الإجراءات، أما في يخص قانون الإجراءات الجزائية فان غياب بعض الشروط للجوء إلى إجراء، حيث لم يذكر المشرع الإذن والتسبيب في التسجيل الصوتي، ما يعد مخالفا للمادة (46) بقولها:"لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه ويحميها القانون.سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

لا يجوز بأي شكل المساس بالحقوق دون أمر معلل من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم.

-حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه"[1]، من الدستور، أمّا عن التسجيلات والصور التي في محاضر الاستدلال، لم يحدد المشرع الجزائري مصيرها، ومدة الاحتفاظ، في قانون الإجراءات الجزائية وكذا قانون (09-04) في إطار قانون الإجراءات مما يثير المخاوف من استعمالها خارج إطار الشرعية الإجرائية.

-إنّ الحصول على خدمة الانترنت يتطلب تضافر جهود عدة وسطاء لتقديم الخدمة ، وقدلاحظنا أنّ المشـــرع الجزائري لـم يعمل على الفصل بيـــن مختلف مقدمـــي خدمـــات الانتـرنت، وجعلهم في خندق واحد، وهذا حتى لا يبذل جهداً ربما في تحديد مسؤولية كل مقدم لخدمة الإنترنت على حدى ، لذى ننوه وندعو إلى ضرورة سن تشريع خاص لمزودي خدمات الانترنت، ووضع أسس لمساءلته بتوضيح ما له وما عليه من التزامات، وبشكل دقيق ومفصل محترمين في ذلك حرمة الحياة الخاصة وقرينة البراءة، لأن لديهم دوراً هاماً جدا في الإثبات في جرائم الانترنت، بالالتزامات الملقاة على عاتقهم .

- وإجراءات البحث والتحري، الواردة في القانون(09-04) فقد جاءت في اعتقادنا خاصة بجرائم الإنترنت فقط، بمعنى إذا كانت الجرائم تقع على الانترنت أو بالإنترنت، فهي إجراءات خاصة فقط بها، لأنها أكثر ملائمة من الإجراءات الخاصة الباقية، وهي تنطوي على مساس واضح بالحريات الفردية ، حيث خصّ المشرع الإذن بالتفتيش وتحديد المدة الزمنية للرقابة الالكترونية الاتصالات لجرائم الإرهابية فقط دون غيرها من الجرائم. وإذ ننوه على ضرورة التفرقة بين ماهو إجراءات خاصة ببعض الجرائم الخاصة والإجراءات الخاصة بجرائم الانترنت في التشريع الجزائري، إذ أنّه لابد من إقرار إجراءات بنفس الشروط الضمانات والإجراءات العادية لكشف واثبات الجرائم العادية، ولكن هذه المرة لجرائم ترتكب عبر الانترنت وبمساعدته وبين الإجراءات

[1] القانون(16-01) يتضمن التعديل الدستوري، المرجع السابق، ص8.

التي تتضاءل فيها الضمانات وتتقلص فيها الشروط إلى ادني مستوى من اجل قمع جرائم خطيرة سواء تعلق الأمر بجرائم عادية أو جرائم الانترنت.لذلك لابد من وضع حد فاصل بين الإجراءات الخاصة المرتبطة بخطورة الجريمة والإجراءات الخاصة باختلاف مسرح وكيفيات ارتكاب الجريمة.

وبالتالي فانّه يؤخذ على الضمانات التي أوجدها المشرع الجزائري للإثبات جرائم الانترنت انّه فيما يخص الإذن؛ لم يشترطه في التقاط الصور والتسجيل الصوتي. أمّا فيما يخص التجديد وذكر السبب فلم يورد أياً منها في نصوصه ولا حتى بعد تعديل قانون الإجراءات الجزائية.

كما لاحضنا أنّ المشرع الجزائري لم يحدد ما تؤول إليه التسجيلات والنسخ والصور التي ترفق بالمحاضر ،وهنا نحن بصدد قانون الإجراءات الجزائية والأصل أن تحال له كل الإجراءات.

لذلك كان على المشرع الجزائري"على الأقل تفاديا للتعسف في استعمال السلطة أن يرتب بعض الجزاءات عند مخالفة بعض أحكام المواد المنظمة لهذه العمليات فالواقع أثبت أن قاضي التحقيق ماهو إلا إنسان يتصرف بمفردة وهو دوما معرض للخطأ ينبغي على المشرع أن يضع نصوصا تكون ضابطا لتصرفاته، ولا يترك له مطلق الحرية في التصرف دون رقيب أو حسيب"[1].

-إنّ الإشكال في وسائل جمع الدليل الجنائي في جرائم الانترنت ومنه الدليل الجنائي الالكتروني ، خصوصا ما تعلق منها بمراقبة الإتصالات في قانون الإجراءات الجزائية أو في إطار القانون (09-04)هو أنّ هذه المراقبة والتسجيل لن تكون فقط لطرفي الحديث وهو ما ينتهك خصوصية الطرف المتصل بالمشتبه فيه، بل هي أوسع في إطار جرائم الانترنت، مما يجسد انتهاك الحياة الخاصة للمجتمع المعلوماتي برمته،كما أن الضبط في مجال جرائم الانترنت يمثل اعتداء على حقوق الغير و على حرمة حياته الخاصة مما يستوجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق

-ضرورة تحديد الأساليب الإجرائية واستكمالها على نحو يكفل استجابتها بشكل كاف وبغير تعريض حقوق وحريات الأفراد للخطر، لمتطلبات العملية الاثباتية في مجال تقنية المعلومات

[1] فوزي عمارة،المرجع السابق،243.

والاتصالات التي لا تعترف من حيث أثارها بالمكان في مفهومه التقليدي وتعوق بعض مبتكراتها وتسهيلاتها ،تنفيذ الأساليب التقليدية للقسر في قانون الإجراءات الجزائية.[1]

-وفي الأخير فان كل هذه الإجراءات الخاصة بعملية الإثبات ينتج عنها مجموعة من الأدلة تتوزع بين أدلة عادية وأدلة جنائية الكترونية،- وقد استنتجنا أنّ الدليل الجنائي الالكتروني دليل صالح لإثبات الجرائم التي تكون فيها الإنترنت موضوعا أو وسيلة لارتكاب الجريمة، ذلك أنّ معظم الجرائم العادية أصبحت تكنولوجيا ت الإعلام والاتصال تلعب فيها الدور الأهم-، لكل دورها في عملية الإثبات في جرائم الانترنت، وللقاضي دور مهم في تقدير هذه الأدلة فلا بد لها أنْ تكون يقينية غير دائرة في مجال الشك، وأن يناقشها القاضي، فقد خص المشرع الجزائري الجمع و البحث في إطار جرائم الانترنت هيئة وطنية لذلك ومن خلال المرسوم الرئاسي فقد خول الهيئة مهام جد حساسة ،حيث خول في المادة(11)منه "جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" مما يعني بنك للمعلومات المعالجة أليا، لدى لا بد على المشرع الجزائري استدراك الأمر ووضع قانون خاص بالدليل الجنائي الالكتروني وطرق الحصول عليه والتخلص منه ، وكذا حماية جنائية لبنك المعلومات على غرار ما فعل مع بنك المعلومات الخاصة بالبصمة الوراثية.

فقد لاحضنا انّه يغيب أي نص يتعلق بكيفية الاحتفاظ بالدليل الجنائي الالكتروني؛ هنا طبعا باعتباره يختلف في طبيعته عن الأدلة الأخرى، أي كيفية الاحتفاظ بالدعامة وتحريزها ومدتها والتخلص منها، والمسؤولية القانونية المترتبة على ذلك على غرار الاتصالات الالكترونية، لسلامته من العبث.

[1] هشام فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني والية التدريب التخصصي للمحققين،مجلة الأمن والقانون ،كلية شرطة دبي ،الإمارات العربية المتحدة،العدد الثاني،السنة السابعة ،ربيع الاول1420 هـ-يوليو 1999 م،ص82.

-إعـــادة صياغة المادة (212) من قـانون الإجراءات الجزائري بإدراج الدليـل الجنائـــــي

الالكتروني كدليل إثبات، بالإضافة إلى إدراج مصطلح التقنية أو الانترنت أو التكنولوجيات الحديثة للاتصال والإعلام، في جميع طرق الإثبات بعدما بينا أنّ جميعها صالحة لإثبات جرائم الانترنت ولكن بحجية متفاوتة .

-إدراج مصطلح الآثار الرقمية أو المعلوماتية، ضمن المواد المتعلقة بالإجراءات الخاصة في قانون الإجراءات الجزائية والقانون (09-04) لتميز بين جرائم الانترنت والجرائم الخاصة الأخرى، التي يمكن أن يكون الدليل الجنائي في الشكل الالكتروني جزءاً من الأدلة التي تشكل إثبات جرائم عادية، فكما ذكرنا سابقا أنّ الدليل الجزائي الالكتروني له محل في إثبات الجرائم العادية، مما يدعو إلى إعادة النظر في القوانين وخصوصا القانون (09-04) الذي جاء بخطوط عريضة لسياسية جنائية لمكافحة جرائم الانترنت، المستقاة من معاهدة بودابست، إذن لابد من التفصيل أكثر خصوصا إذا ما تعلق الامر بالأمن ألمعلوماتي وهو أسلوب وقائي، الذي يعد جزاء من الأمن القومي، وذلك بتحديد الإطار القانوني للإثبات الجنائي في جرائم الانترنت، .

-كما نحب أن نلفت انتباه المشرع لضرورة إضافة جرائم الانترنت ضمن الجرائم التي تعنى بحماية الشهود مثل جرائم الفساد[1]، لتعتبر ضماناً هاماً تدفع الشاهد للقيام بواجبه ،بعيدا عن التزوير ومطمئنا للحماية الإجرائية من أجل الحصول على دليل إثبات يمكن الإستناد إليه للوصول إلى الحقيقة،كما ننوه إلى ضرورة تعريف مصطلح الالتزام بالإعلام في مثل هذه الجرائم حتى يرفع اللبس عن ما هو واجب و ما هو جائز.

- كما نرى أن يتم إتلاف هذه التسجيلات بعد مرور مدة تقادم الجريمة المستعان فيها بالإجراءات الخاصة للحصول على الدليل الجنائي، وتحريزها ووضع الأختام اللازمة بعد فحصها

[1] المادة(65مكرر19)الأمر رقم(15-02)المؤرخ في 7 شوال عام 1436 الموافق 23 يوليو 2015 يعدل ويتمم الأمر رقم(66-155) المؤرخ في 18 صفر عام1386 الموافق 8يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية ،ج.ر، رقم 40 ليوم 23 يوليو 2015 .

ومناقشتها من طرق قاضي الموضوع. بوضع نظام قانوني خاص بمقدمي خدمات الانترنت بما يتمتعون به من حقوق وما يلتزمون به من واجبات.

- وإذ نلفت انتباه المشرع إلى ضرورة التوسع وإعطاء مفهوم أوضح للمعلومات المصنفة، وإدخال التكنولوجيات الحديثة للإعلام والاتصال في سياق المرسوم رقم(84-387)مؤرخ في 29 ربيع الأول عام 1405 الموافق 22 ديسمبر سنة 1984 يحدد التدابير المخصصة لحماية الوثائق المصنف السالف الذكر وهذا بعد التطور الكبير في التقنية .

-وحتى تتمكن أجهزة إنفاذ القانون من تأدية مهامها، لابد لها من تطوير مهارتها عن طريق التدريب وتجديد المعلومات دوريا، عن طريق تبادل البعتاث في إطار اتفاقيات ثنائية، وتفعيل دورها، وإدراج شُعب وتخصصات في تكنولوجيات الإعلام والاتصال بجانبها القانوني خصوصا.

ونعود ونقول أنّ الوقاية خير من العلاج فوجود التوعية بأمن المعلومات، على مستوى الأفراد و المؤسسات، وإعلام هادف، لنشر الوعي المعلوماتي وميثاق لأخلاقيات التعامل مع الانترنت، هي أكثر الطرق التي تحارب جرائم الإنترنت وتغني عن المشكلات التي تتركها هذه الجرائم ،خصوصا ما تعلق بالتكاليف العالية، للتدريب والحصول على البرمجيات وكذا تحليل الدليل الجنائي الإلكتروني، والآثار السلبية لانتهاك الحقوق والحريات.

تم بحمد الله

الملاحق

الملحق رقم 1

Bilan d’activité du Centre de Prévention et de lutte Contre la Criminalité Informatique Et la Cybercriminalité de la Gendarmerie Nationale

Au titre de l’année 2017

حوصلة نشاط مركز الوقاية من جرائم الاعلام الآلي و جرائم المعلوماتية و مكافحتها للدرك الوطني

لحساب سنة 2017

VOLET ENQUETE :

1. Vue d'ensemble :

N°	Désignation	Point de situation
01	**Assistance technico-opérationnelle des unités territoriales de la GN**	Une action permanente au niveau du CPLCIC visant l'assistance et le soutiens des unités territoriales de la GN dans la résolution des Cyberenquêtes. Le CPLCIC a réalisé en **2017**, **905** Cyberenquêtes jusqu'à fin Novembre, soit une augmentation d'environ **68,21 %** par rapport à la même période de l'année **2016**, qui a vu le traitement de **538** affaires. L'activité du CPLCIC durant l'année **2017** et à l'instar des années précédentes, a considérablement évoluée par rapport à l'année précédente. En témoigne le nombre d'affaires traitées, la diversité des infractions constatées et l'étendue des unités requérantes concernées. Cette évolution est caractérisée par une augmentation significative des affaires traitées, de la diversité des infractions constatées et également de l'étendue des unités requérantes concernées.

2. Tableau synthèse détaillée :

N°	Désignation	Nombre	Répartition par type	Observations
01	**Enquêtes Cybernétiques relatives aux TIC**	**905**	**10,16 % fraudes aux BAC et BEM** **89,83 % ordre et sécurité publique, criminalité sur Internet**	**augmentation de + 68,21 % par rapport à 2016.**
02	**Assistance aux unités territoriales de la GN**	**390**	**-Sections de recherche** **-Brigades de Recherche** **-Brigades Territoriales**	**Ces unités relèvent de (47) groupements territoriaux**

Ce nombre constitue une augmentation d'environ **68,21 %** par rapport à la même période de l'année **2016**, qui a vu le traitement de **538** affaires.

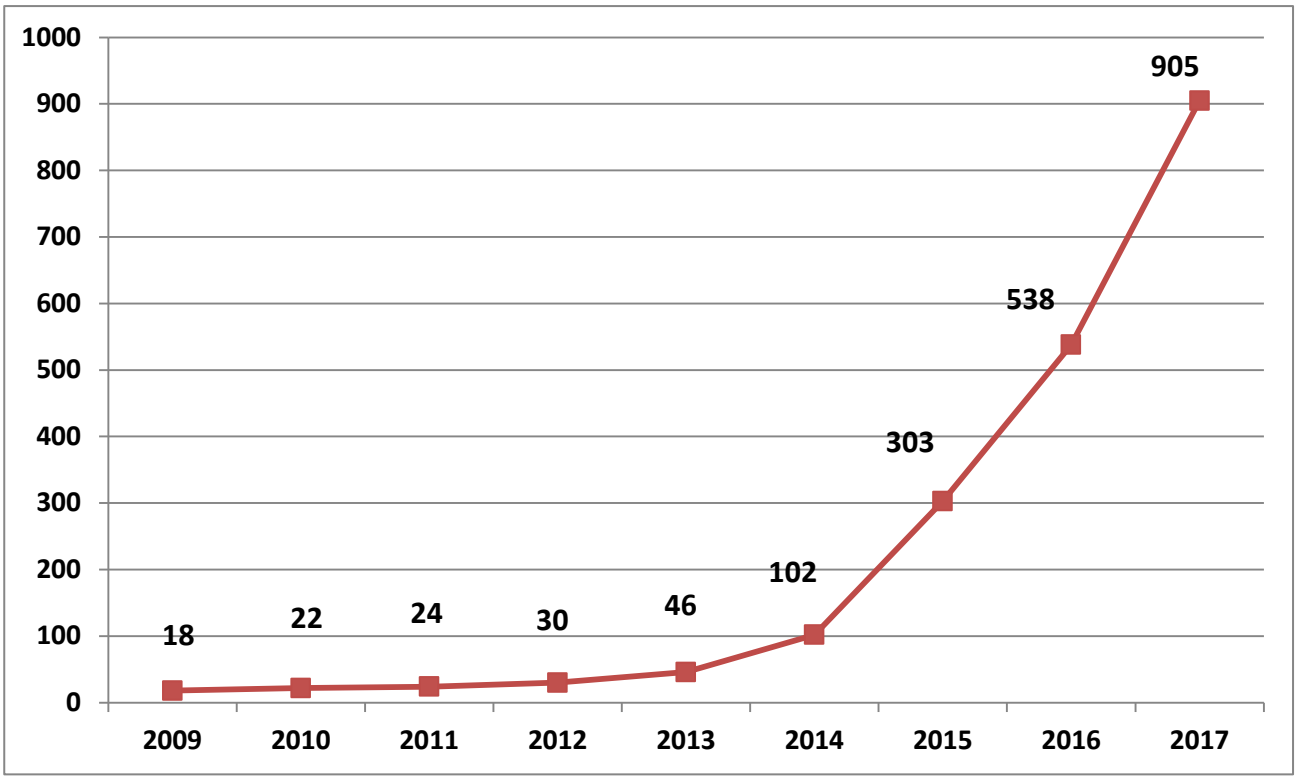
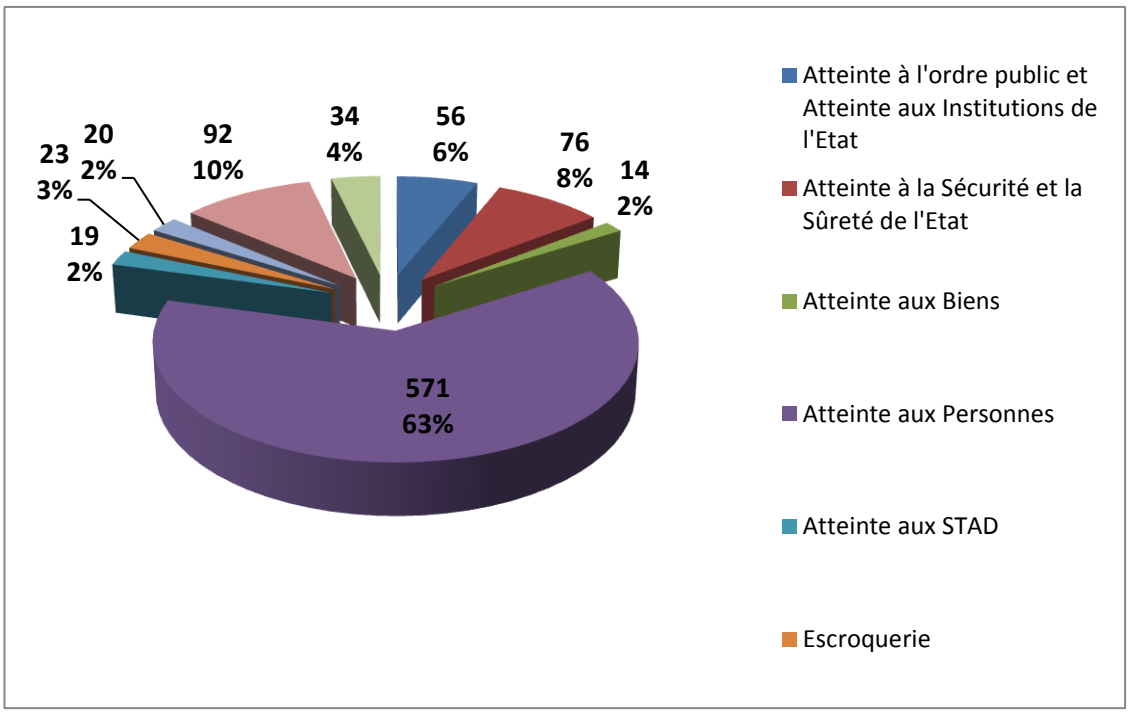


Figure 01 : Evolution de l'activité cyber enquête 2009-2017.

2.1.Types d'infractions :

Les affaires traitées en 2017 sont réparties selon leur nature comme suit :



N°	Répartition par type	Nombre	Pourcentage
01	Atteinte à l'ordre public et Atteinte aux Institutions de l'Etat	56	6,19%
02	Atteinte à la Sécurité et la Sûreté de l'Etat	76	8,40%
03	Atteinte aux Biens	14	1,55%
04	Atteinte aux Personnes	571	63,09%
05	Atteinte aux STAD	19	2,10%
06	Escroquerie	23	2,54%
07	Exploitation des Mineurs	20	2,21%
08	Fraude BAC	92	10,17%
09	Terrorisme	34	3,76%
TOTAL		905	100 %

2.2.Types de victimes :

N°	Type de victime	Nombre d'affaires	Sexe de la victime	Nombre	Observations
01	Physique	619	Masculin	301	Dont 18 mineurs
			Féminin	318	Dont 67 mineurs
02	Morale	286	/		
TOTAL		905			

3. Volet formation de Cyber enquêteurs BMP1-ETIC :

N°	Désignation	Point de situation
01	**Formation d'enquêteurs en Technologie de l'information et de la communication (E-TIC)**	Cette formation vise la formation de personnels spécialisés dans la lutte contre la Cybercriminalité dans chaque groupement territorial de la GN Deux sessions de cette formation **E-TIC** (enquêteurs technologies de l'information et de la communication) ont été réalisées en **2016** et **2017**. La dernière phase de formation de cette formation est programmée au premier trimestre de **2018**. **59** sous officiers ont pris part à cette formation.

4. Volet communication/sensibilisation :

N°	Désignation	Point de situation
01	**Formations assurées par les cadres du CPLCIC**	Ces formations sont destinées pour les militaires de l'arme en cours de formations dans les différentes écoles de la Gendarmerie Nationale pour le transfert de connaissance sur les techniques de veille et d'investigations des enquêtes cybercriminelles. Au total, sept (**07**) cours de formation avec un volume horaire global de trois cent trente quatre heures et **30** minutes (**334,5H**) ont été concrétisées au cours de l'année **2017**.
02	**Animation de conférences**	Les cadres du CPLCIC ont animés au titre de l'année **2017** trente trois (**33**) conférences avec un volume horaire de **132** heures au profit des stagiaires des écoles de la Gendarmerie Nationale de **Zéralda**, **Sétif**, **Isser** et **Sidi Bel Abbes**, ainsi que les différents Commandements Régionaux de la Gendarmerie Nationale et Commandement de forces de l'ANP.

03	**Participation des cadres du CPLCIC aux évènements nationaux**	Les personnels du CPLCIC ont participés au titre de l'année **2017** à treize (**13**) conférences au niveau national, pour la mise à jour des connaissances acquises à l'occasion de l'exercice de leurs missions.
04	**Reportages réalisés par les différents supports de média publics**	Ce volet entre dans le plan d'action du CPLCIC pour la sensibilisation de la société civile Algérienne sur les risques liés à la mauvaise utilisation des nouvelles technologies d'information et de communication, principalement les réseaux sociaux. Au total cinq (**05**) reportages et/ou émissions ont été réalisés.
05	**Sécurité numérique**	Au cours de l'année **2017**, le bureau sécurité numérique a procédé à la réalisation de 97 dossiers relatifs à : • L'analyse cybernétique des applications "TIC" ; • L'élaboration d'études en sécurité numérique ; • L'analyse de dossiers spécifiques, • Prendre en charge les demandes des structures et unités de la GN concernant l'évaluation des TIC.

الملحق رقم 2

Exécution des commissions rogatoires internationales

"Exemples d'affaires traitées par les unités de la Gendarmerie Nationale et la Sûreté Nationale, se rapportant aux infractions liées aux TIC."

1- Affaire traitée par la Sûreté Nationale en collaboration avec le FBI, pour atteinte aux systèmes de traitement automatisé de donnés, détention et commercialisation de donnés numériques obtenues frauduleusement.

Les faits de cette affaire remontent au **17 décembre 2009** lorsque le Ministère de la Justice avait été rendu destinataire d'un courrier adressé par l'attaché juridique du **FBI** en Algérie, portant sur une demande d'entraide judiciaire dans le cadre d'une enquête ouverte par la division du FBI de Detroit, pour piratage informatique de cartes de crédits Visa.

Historique Le 23 juin 2009, la compagnie **Visa** a communiqué des informations au FBI, au sujet de plusieurs tentatives réussites d'acheminement de donnés piratées de cartes de visa à un serveur localisé en **Allemagne**.

En collaboration avec d'autres services étrangers, le FBI a pu récupérer un ensemble de donnés compromises à partir de ce système localisé en Allemagne.

L'analyse de ce système ainsi que des donnés récupérées a révélé qu'un hacker utilisant le pseudonyme **WALLACEZ** avait installé un programme informatique malveillant pour récupérer toutes les donnés saisies par des victimes concernant leurs cartes de visa.

Ces donnés de cartes de visa, une fois saisies sur les systèmes compromis, le programme malveillant les interceptaient et les envoyaient sur un autre serveur localisé en Allemagne. Au total, plus de **10.000 cartes** de crédits ont été piratées.

Les investigations menées par la suite par les éléments du FBI ont conduit à l'identification de deux personnes, présumées responsables de ces faits: l'un d'entre eux est un Algérien demeurant à Annaba.

Le dossier de cette affaire a été communiqué au Ministère de la Justice, lequel l'a transmis aux **éléments de la DGSN** qui ont procédé à l'interpellation du présumé suspect.

Le mis en cause a été présenté devant le Procureur de République près le tribunal d'Annaba **le 07 Mars 2010**, qui a ordonner de le placé sous mandant de dépôt, en attendant son jugement.

2- Affaire traitée par la section de recherche d'Alger dans le cadre d'une commission rogatoire internationale, relative à la tentative d'escroquerie via Internet (Phishing).

Le 11 mars 2010, dans le cadre d'une commission rogatoire internationale délivré par la cour des **grandes instances de Paris,** la **Section de Recherche de la Gendarmerie Nationale d'Alger** a été saisi par le procureur général près la cours d'Alger pour la prise en charge de l'affaire objet de la demande.

Cette commission rogatoire concernait une demande pour ouverture d'enquête au sujet d'une tentative d'escroquerie contre des **citoyens français** via Internet (**Phishing**) notamment sur le site web de la société des cartes bleues.

Sur la base des informations contenues dans la commission rogatoire, ainsi que le rapport technique joint élaboré par l'OCLCTIC Français (l'**O**ffice **C**entral de **L**utte contre la **C**riminalité liée aux **TIC**), les investigations complémentaires menées par les éléments de la section de recherche d'Alger, assistés par deux techniciens cyber-enquêteurs, spécialistes en analyse et détection sur Internet, ont conduit à l'identification et l'arrestation de deux personnes présumées suspects, ainsi que la saisie de leurs équipements informatiques.

L'analyse de l'historique de l'activité Internet de ces équipements, ainsi que tous les supports de stockages numérique ont permis d'extraire et de récupérer d'importants fichiers et données numériques, qui constituerons les preuves matérielles contre les suspects.

قائمة المراجع

I. المراجع باللغة العربية:

أولا–المؤلفات:

أ–المؤلفات العامة:

1- أحسن بوسقيعة، التحقيق القضائي، دار هومه، الجزائر، 2012.

2- أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، ج2، ط.15، دار هومه، الجزائر، 2013.

3- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط 12، دار هومه، الجزائر2013.

4- أحمد الشافعي، البطلان في قانون الإجراءات الجزائية، دراسة مقارنة، الطبعة الثانية، دار هومة، الجزائر، 2005.

5- أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، 2003.

6- إحمود فالح الخرابشة، الإشكالات الإجرائية للشهادة في المسائل الجزائية، دراسة مقارنة، ط 1، دار الثقافة، عمان، الأردن، 2010.

7- أكرم نشأت إبراهيم، علم النفس الجنائي، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن، 1996.

8- بارش سليمان، شرح قانون الإجراءات الجزائية الجزائري، الجزء الأول، دار الهدى، عين مليلة، الجزائر، 2007.

9- برهامي أبو بكر عزمي، الشرعية الإجرائية للأدلة العلمية"دراسة تحليلية لأعمال الخبرة"، دار النهضة العربية، القاهرة، مصر، 2006.

10- جواد الهنداوي، القانون الدستوري والنظم السياسية، العارف للمطبوعات، بيروت، لبنان، 2010.

11- جيلالي بغدادي، الاجتهاد القضائي في المواد الجزائية، الجزء الأول، الطبعة الأولى، الديوان الوطني للأشغال التربوية، الجزائر، 1999.

12- حسن صادق المرصفاوي، أصول الإجراءات الجنائية، منشاة المعارف الإسكندرية، مصر، 1996.

13- سامر محمد سعيد، الانترنت المنافع والمحاذير، دار سعاد الصباح، الطبعة الأولى، الكويت.

14- سمير عالية، الوجيز في شرح الجرائم الواقعة على دراسة أمن الدولة، دراسة مقارنة، المؤسسة الجامعية للدراسات والنشر والتوزيع، الطبعة الأولى، 1999.

15- طارق صديق رشيد كه ردى، حماية الحرية الشخصية في القانون الجنائي، منشورات الحلبي الحقوقية، بيروت ، لبنان،2011.

16- عبد الحميد الشواربي، الإثبات الجنائي في ضوء القضاء والفقه، منشاة المعارف، مصر، 1996 .

17- عبد الله اوهابية، قانون الإجراءات الجزائية الجزائري،التحري والتحقيق،دار هومة،2015

18- علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي، دراسة مقارنة، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2006.

19- عمار عباس الحسيني، مبادئ علمي الإجرام والعقاب، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2013.

20- فوزي او صديق، الوافي في شرح القانون الدستوري الجزائري ،ديوان المطبوعات الجامعية، الجزء الأول، نظرية الدولة، بن عكنون، الجزائر، 2003.

21- محمد أحمد محمود، الوجيز في أدلة الإثبات،دار الفكر الجامعي، مصر، 2002.

22- محمد الحماد الهيتي، التكنولوجيا الحديثة و القانون الجنائي، دار الثقافة للنشر والتوزيع، الأردن، 2010.

23- محمد حزيط، مذكرات في قانون الإجراءات الجزائية، الطبعة الرابعة، دار هومة، 2009.

24 -محمد زكي أو عامر، قانون العقوبات القسم الخاص، الدار الجامعية للطباعة والنشر، بيروت 1990.

25- محمد سامي الشوا، ثورة المعلومات وانعكاسها على قانون العقوبات، دار النهضة العربية، القاهرة،مصر، 2003.

26- محمد محمد محمد عنب، استخدام التكنولوجيا الحديثة في الإثبات، القاهرة، مصر،2007.

27- محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري،الجزء الأول،ديوان المطبوعات الجامعية بن عكنون الجزائر،1999.

28- محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري،الجزء الثاني،ديوان المطبوعات الجامعية بن عكنون الجزائر،1999.

29- مصطفى مجدي هرجه، الإثبات في المواد الجنائية، دار المطبوعات الجامعية، مصر، 2000.

30- مصطفى محمد الدغيدي ،التحريات والإثبات الجنائي.شركة ناس للطباعة ،2004.

31- مليكه درياد، نطاق سلطات قاضي التحقيق و الرقابة عليها ، ديوان المطبوعات الجامعية،بن عكنون، الجزائر،2012

32- منذر الويس، أثر التطور التكنولوجي على الحريات العامة،منشاة المعارف، الإسكندرية، مصر ،1998.

33 - موسى مسعود ارحومة، قبول الدليل العلمي أمام القضاء الجنائي، دراسة مقارنة، منشورات جامعة قاريونس، بنغازي، ليبيا، 1999.

34- هشام فريد رستم، قانون العقوبات ومخاطر التقنية، مكتبة الآلات الكاتبة، 1995.

35-مأمون سلامة، قانون الإجراءات الجنائية معلقا عليه بالفقه وإحكام القضاء، مكتبة رجال القضاء، 1980.

36-محمد جمال الفار، المعجم الإعلامي، دار أسامة و المشرق الثقافي، عمان، الأردن، 2010.

ب-المؤلفات الخاصة:

1- أحمد حسام طه تمام، الحماية الجنائية لتكنولوجيا الاتصال، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2002.

2- أحمد خليفة الملط، الجرائم المعلوماتية، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية ،مصر، 2006.

3- المغيث، معجم قانون تكنولوجيات الإعلام والاتصال، عربي،فرنسي،انجليزي،الطبعة الأولى، مركز البحث في الإعلام العلمي والتقني، الجزائر، 2008.

4 - أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة، بوزريعة، الجزائر، 2006.

5 - أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

6- جلال محمد الزعبي و أسامة احمد مناعسة، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة، دار الثقافة،عمان الأردن،2010.

7- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيات الحديثة(أجهزة الرادار – الحاسبات الآلية –البصمة الوراثية) دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2001.

8- جميل عبد الباقي الصغير، الانترنت والقانون الجنائي للإحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، مصر، 2002.

9- جميل عبد الباقي الصغير، لجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، مصر، 2002.

10- حسين بن سعيد ألغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، 2009.

11- خالد عياد الحلبي،إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت،الطبعة1،دار الثقافة للنشر والتوزيع،عمان، الأردن،2011.

12- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي ، الإسكندرية ، مصر، 2009.

13- رشيدة بوكر ،جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارنة، الطبعة الأولى ، منشورات حلبي الحقوقية، لبنان، 2012.

14- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، المرجع السابق،دار الجامعة الجديدة ،الإسكندرية، مصر،2007

15- عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية،دراسة قانونية مقارنة،دار الثقافة، عمان، الأردن، 2015.

16- عايد رجا الخلايلة، المسؤولية التقصيرية الالكترونية، المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والانترنت،دراسة مقارنة، الطبعة الأولى، دار الثقافة،عمان ، الأردن، 2008.

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

18- عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، دار المستقبل، الطبعة الأولى، عمان الأردن، 2008.

19- عبد الصبور عبد القوي على المصري، المحكمة الرقمية والجريمة المعلوماتية، دراسة مقارنة،مكتبة القانون والاقتصاد،الرياض، المملكة العربية السعودية،2012.

20- عبد الفتاح بيومي حجازي ،الدليل الجنائي و التزوير في جرائم الكمبيوتر والإنترنت ،المحلة كبرى ،مصر، 2001.

21- عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، دراسة معمقة ومقارنة في الجرائم، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2011.

22- عبد الفتاح بيومي حجازي،مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، مصر ،2007.

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

24- عبد المطلب عبد الحميد ممدوح، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006.

25- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشاة المعارف الإسكندرية، مصر، بدون سنة.

26- على جبار الحسناوي، جرائم الحاسوب علي والإنترنت، الطبعة العربية، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009.

27- علي عدنان الفيل، الإجرام الالكتروني، دراسة مقارنة، منشورات زين الحقوقية، الطبعة الأولى، 2011.

28- عمر عيسى الفقي، الجرائم المعلوماتية، المكتب الجامعي الحديث الإسكندرية، مصر، 2006.

29- عمر محمد بن يونس أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب، دار النهضة العربية، 2004.

30- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة ، مصر، 2010.

31- محمد أبو العلا عقيدة، مراقبة المحادثات التليفونية، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2008.

32- محمد الربيعي، أحمد شعبان الدسوقي و آخرون، المعجم الشامل لمصطلحات الحاسب الآلي و الانترنت، الطبعة الأولى، مكتبة العبيكان، الرياض، 2002.

33- محمد الفاتح حمدي، مسعود بوسعدية، ياسين قرناني،تكنولوجيا الاتصال والإعلام الحديثة، كنوز الحكمة، الأبيار، الجزائر، 2010.

34- محمد أمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2004.

35- محمد أمين الخرشة، مشروعه الصوت والصورة في الإثبات الجنائي، دراسة مقارنة، ط2 دار الثقافة، عمان، الأردن، 2015.

36- محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع،عمان الأردن،2009.

37- محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2009.

38- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، الأردن، 2004.

39- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، مصر، 2006.

40- محمد فتحي محمد أنور عزت، تفتيش شبكة الانترنت،لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبارات التي تقع بواسطتها،دراسة مقارنة،ط1،المركز القومي للإصدارات القانونية،القاهرة،مصر، 2012.

41- محمد محمد محمد عنب، استخدام التكنولوجيا الحديثة في الإثبات،القاهرة ،مصر،2007.

42- مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، مصر.

43- مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت ، دراسة مقارنة ، دار الكتب القانونية : المجلة الكبرى مصر،2005.

44- مصطفى يوسف، مشروعية الدليل في المسائل الجنائية،في ضوء الفقه والقضاء، بدون دار نشر،بدون ذكر البلد،2010.

45- مليكه درياد، نطاق سلطات قاضي التحقيق و الرقابة عليها ، ديوان المطبوعات الجامعية،بن عكنون، الجزائر،2012 .

46- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت،دار الكتب القانونية،المحلة الكبرى،مصر ،2006.

47- منير محمد الجنبيهي،ممدوح محمد الجنيبهي، جرائم الانترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2004.

48- موسى مسعود ارحومة، قبول الدليل العلمي أمام القضاء الجنائي، دراسة مقارنة، منشورات جامعة قاريونس، بنغازي، ليبيا، 1999.

49- نائلة عادل محمد فريد قورة ،جرائم الحاسب الآلي الاقتصادية.دراسة نظرية وتطبيقية،منشورات الحلبي الحقوقية، لبنان،2005

50- هلالي عبد الإله احمد، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001 ، دار النهضة العربية ، القاهرة ، مصر، 2006.

51- هلالي عبد الاله احمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، الطبعة الثانية ،دار النهضة العربية،القاهرة ،مصر،2008 .

52- هلالي عبد الاله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية،دراسة مقارنة،ط2، دار النهضة العربية،القاهرة،مصر، 2008.

53- هلالي عبد الله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، ط 2، دار النهضة العربية، القاهرة، مصر، 2008.

54- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، مصر، 2009.

55-مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة القاهرة، مصر، 2009.

ثانيا–الرسائل و المذكرات الجامعية :

أ–الرسائل الجامعية :

1- خالد بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتواره في الفلسفة في العلوم الأمنية كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية، الرياض. المملكة العربية السعودية . 2006، 1427.

2- سامح أحمد البلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الانترنت، رسالة دكتوراه ،جامعة الإسكندرية، مصر 2010.

3- سليمان احمد محمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت،دكتوراه في العلوم الشرطية ،أكاديمية الشرطة، القاهرة، مصر، 2007.

4- عاقلي فضيلة، الحماية القانونية للحق في الحياة الخاصة ،دراسة مقارنة،دكتوراه علوم في القانون الخاص جامعة الإخوة منتوري قسنطينة،كلية الحقوق،2011-2012.

5- عمر عبيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان وفقا للمعطيات التكنولوجية المعاصرة، رسالة دكتوراه في القانون الجنائي، كلية الحقوق، جامعة القاهرة، 2006.

6- فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني اطروحة من اجل الحصول على شهادة دكتوراه في الحقوق فرع القانون الجنائي والعلوم الجنائية ،كلية الحقوق جامعة الجزائر 1، 2010/2009.

7- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية ،دكتوراه في الحقوق،كلية الحقوق ،جامعة عين شمس،القاهرة،2012.

8- منى فتحي أحمد عبد الكريم، الجريمة عبر شبكة الدولية للمعلومات، صورها ومشاكل إثباتها،رسالة دكتوراه،كلية الحقوق،جامعة القاهرة،مصر.2008.

ب- المذكرات الجامعية:

1- أمينة ركاب، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري،مذكرة ماجستير،كلية الحقوق والعلوم السياسية،جامعة ابو بكر بلقايد تلمسان،الجزائر،2014-2015.

2- سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات رسائل ماجستير في العلوم الشرطية ،جامعة نايف العربية للعلوم المنية، الرياض ،المملكة العربية السعودية ،2003.

3- فهد ناصر عيسى بن صليهم، مبدأ العينية وأثره في مكافحة الجرائم العابرة للحدود الدولية دراسة مقارنة،رسالة ماجستير في العدالة الجنائية ،جامعة نايف للعلوم الأمنية، الرياض ،المملكة العربية السعودية، 1430هـ-2009م.

4- متعب بن عبد الله السند، التعاون الدولي في تنفيذ الأحكام الجنائية وأثره في تحقيق العدالة، رسالة ماجستير، كلية الدراسات العليا،جامعة نايف العربية للعلوم الامنية، الرياض، المملكة العربية السعودية، 1432هـ-2011م.

5- محمد بن نصير محمد السرحاني،مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت ،رسالة ماجستير ،أكاديمية نايف للعلوم الأمنية، 2004.

6- ناصر عيسى بن صليهم، مبدأ العينية وأثره في مكافحة الجرائم العابرة للحدود الدولية دراسة مقارنة، رسالة ماجستير في العدالة الجنائية، جامعة نايف للعلوم الأمنية، الرياض، المملكة العربية السعودية، 1430هـ-2009م.

ثالثا– المقالات والأوراق البحثية:

أ–المقالات :

1- إبراهيم سليمان القطاونه ومحمد أمين الخرشه، المسؤولية الجزائية لمقدمي خدمة الشبكة المعلوماتية ومورديها ومتعهديها وناشريها دراسة مقارنة –الأردن الإمارات العربية المتحدة –مجلة الشريعة والقانون كلية القانون جامعة الإمارات العربية المتحدة،العدد 66،رجب 1437هـ،أبريل2016.

2- احمد ايو القاسم،طبيعة نظرية الإثبات الجنائي العلمي وما تثيره من قضايا فقهية ومشاكل تطبيقية، مجلة كلية الدراسات العليا العدد16 يناير 2007.

3- أحمد قاسم فرج ، النظام المعلوماتي القانوني لمقدمي خدمات الانترنت – دراسة تحليلية مقارنة – مجلة المنار،الاردن ، المجلد 13، العدد 09، 2007.

4- أيمن عبد الحفيظ، حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة بحوث الشرطة العدد25، يناير، القاهرة، مصر 2004.

5- بن فردية محمد،الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي(دراسة مقارنة)، المجلة الأكاديمية للبحث القانوني ، جامعة عبد الرحمان ميرة بجاية كلية الحقوق والعلوم السياسة، سنة5 المجلد9، عدد 1، 2014.

6- جمال الحيدري، ضوابط اعتبار المخرجات الالكترونية أدلة إثبات في القضايا الجزائية، مجلة العلوم القانونية،كلية القانون،جامعة بغداد،العراق، العدد1 المجلد، 21، 2006

7- حازم الحارون،الإنابة القضائية الدولية ،المجلة الجنائية القومية، القاهرة،مصر،العدد 2،يوليو1988

8- داود عبد الرزاق الباز، تدابير حماية الأمن العام بين الشريعة والقانون، المجلة العربية للدراسات الأمنية والتدريب، المجلد 18، العدد 35.

9- سعد سلامة، تفعيل دور التحريات في الإثبات الجنائي في ظل التقنيات الحديثة لمكافحة الجريمة،مجلة كلية الدراسات العليا، متخصصة في علوم الشرطة،القاهرة العدد الخامس عشر يوليو 2006جماد آخر 1427.

10- عبد الرحمان محمد خلف، نظرة حول المشكلات القانونية والعلمية لمواجهة الجريمة المعلوماتية، مجلة كلية الدراسات العليا، القاهرة، جمهورية مصر العربية، العدد 21 يوليو2009،شعبان1430 هـ

11- فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية،مجلة العلوم الإنسانية، عدد 33،جوان 2010،جامعة الإخوة المنتوري قسنطينة.

12- محمد حسين الحمداني و نوفل على الصفو، مبدأ الاقتناع القضائي، مجلة الرافدين للحقوق، مجلد 1 السنة العشرة، عدد24، سنة 2005.

13- نقادي عبد الحفيظ، التسجيل الصوتي، المجلة الجزائرية للعلوم القانونية و الاقتصادية والسياسية، جامعة بن عكنون، الجزائر، ع1، 2009.

14- هشام فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني والية التدريب التخصصي للمحققين، مجلة الأمن والقانون، كلية شرطة دبي، الإمارات العربية المتحدة، العدد الثاني، السنة السابعة، ربيع الأول 1420 هـ-يوليو 1999 م.

ب-المداخلات العلمية:

1- احمد عبد الكريم سلامة، الانترنت والقانون الدولي الخاص،فراق أ م خلاف؟مؤتمر القانون والكمبيوتر والانترنت، مجلد1،ط3، كلية الشريعة والقانون ،الشارقة، الإمارات العربية المتحدة، 2004.

2- طارق الجملي،الدليل الرقمي في مجال الإثبات الجنائي، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا ، طرابلس، ليبيا من 28- 29 / 10 / 2009.

3- عبد الرحمان حملاوي، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية،بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة16و17 نوفمبر2015،كلية الحقوق، جامعة بسكرة، الجزائر.

4- عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي جامعة نايف العربية للعلوم الأمنية،الرياض، المملكة العربية السعودية،12-14 نوفمبر 2007.

5- عبدالله بن عبدالعزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات،بحث مقدم إلى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت،القاهرة ،جمهورية مصر العربية،في 2-4 جوان 2008 .

6- عز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة16و17نوفمبر2015، كلية الحقوق، جامعة بسكرة.

7- على محمود على حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي،- المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنظم من طرف أكاديمية شرطة دبي – مركز البحوث والدراسات -من 26 /4/ 2003الى28 /2003/4 دبي – الإمارات العربية المتحدة.

8- علي عبد القادر القهوجي،الحماية الجنائية للبيانات المعالجة الكترونيا، مؤتمر القانون والكمبيوتر والانترنت،كلية الشريعة والقانون،العين ،جامعة الإمارات العربية المتحدة،من 1الى3 ماي 2000.

9- محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية. المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنظم من طرف أكاديمية شرطة دبي – مركز البحوث والدراسات -من 26 /4/ 2003الى28 /2003/4 دبي – الإمارات العربية المتحدة

10- ممدوح عبد الحميد عبد المطلب ،زبيدة محمد حاسم،عبد الله عبد العزيز،أنموذج مقترح لقواعد اعتماد الدليل الرقمي لإثبات في الجرائم عبر الكمبيوتر،بحث مقدم لمؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس ، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي،9-11ربيع الأول 1424هـ،الموافق 10-13مايو 2003 .

11- منير جلاب، دور الدرك الوطني في ميدان محاربة جرائم المعلوماتية،الملتقى الوطني، الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري،المركز الجامعية احمد زبانة،غليزان7و8 فبراير2017 .

12- موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا ، طرابلس من 28 . 29 / 10 / 2009.

رابعا– الدستور و الاتفاقيات الدولية و النصوص القانونية و التنظيمية:

أ– الدستور:

1-القانون (16-01) يتضمن التعديل الدستوري المؤرخ في 26 جمادى الأولى عام 1437الموافق6 مارس2016،ج.ر. رقم 14 المؤرخة في 07 مارس2016.

ب– الاتفاقيات الدولية المصادق عليها:

1–اتفاقية الرياض العربية للتعاون القضائي الموقعة في الرياض بتاريخ 23 جمادى الثانيةعام 1403 الموافق 6 أفريل سنة 1983 وكذا تعديل المادة 69 من الاتفاقية الموافقة عليه في 26 نوفمبر1997 من طرف مجلس وزراء العدل العرب في دور انعقاده العادي الثالث عشر المصادق عليها بالمرسوم الرئاسي رقم (01-47) مؤرخ في 17 ذي القعدة عام1421 الموافق 11 فبراير سنة 2011،ج.ر،رقم11 ليوم12فبراير2001.

2- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية الصادرة 15 نوفمبر 2000 و التي صادقت عليها الجزائر بموجب المرسوم الرئاسي (02-55) المؤرخ في 2002/02/05 ج.ر09 ليوم 10 فبراير2002.

3- اتفاقية الأمم المتحدة لمكافحة الفساد، المعتمدة من قيل الجمعية العامة للأمم المتحدة بنيويورك يوم 31 أكتوبر سنة 2003 والتي صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي(04-128) مؤرخ في 29 صفر 1425 الموافق 19 أبريل2004، ج.ررقم26ليوم 25 ابريل 2004.

4- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ21 ديسمبر سنة2010 المصادق عليها بموجب المرسوم الرئاسي رقم(14-252) مؤرخ في 13ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014،ج.ررقم57ليوم28 سبتمبر2014.

ج- القوانين العضوية:

1- القانون العضوي(12-05) المؤرخ في 18صفر عام 1433 الموافق12يناير سنة2012 يتعلق بالإعلام ،ج.ر رقم 02 المؤرخة في 15 يناير 2012.

د- القوانين :

1- أمر(66-155) المؤرخ في 8جوان 1966 المؤرخ في 18 صفر عام1386 الموافق 8يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية المتضمن قانون الإجراءات الجزائية الجزائري، المعدل و المتمم بالأمر(15-02) المؤرخ في 7 شوال عام 1436 الموافق 23 يوليو 2015.

2-أمر رقم (95-10)المؤرخ في 25 رمضان 1415 هـ الموافق ل 25 فبراير 1995 المعدل والمتمم للأمر رقم 66- 155 المؤرخ في 08 يونيو 1966المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 11يوم29 رمضان 1415 هـ الموافق ل 25 فبراير 1995.

3-الأمر رقم (96-22)المؤرخ في 1996/07/09 المتعلق بقمع مخالفات التشريع و التنظيم الخاصين بالصرف و حركة رؤوس الأموال من وإلى الخارج ج.ر رقم43 ليوم 10 يوليو1996.
4- الأمر(03-05) المؤرخ في 19يوليو2003 المتعلق بحقوق المؤلف و الحقوق المجاورة،ج،ر رقم44 ليوم 23 يوليو2003.

5- قانون (04-14) المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 الموافق 10 نوفمبر سنة 2004،ج.ر رقم 71 ليوم 10 نوفمبر2004 ،ص4، المعدل والمتمم للأمر رقم (66-155) المتضمن قانون الإجراءات الجزائية .
6- قانون رقم (04-19) المؤرخ في 13 دو القعدة عام 1425 الموافق 25 ديسمبر 2004 يتعلق بتنصيب العمال و مراقبة التشغيل الجريدة الرسمية 26 ديسمبر 2004.

7-(04-18) مؤرخ في 25 ديسمبر 2004 يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها،ج.ر رقم 83 ليوم 26 ديسمبر2004.
8- قانون (05-01) ليوم 06 فبراير 2005 يتعلق بالوقاية من تبييض الأموال و تمويل الإرهاب و مكافحتها. ج.ر رقم 11 ليوم 9 فبراير2005.
9- القانون رقم (05-10) المؤرخ في 20 يونيو 2005 يعدل ويتمم الأمر رقم (75-58) المؤرخ في 20 رمضان عام1395 الموافق 26 سبتمبر 1975و المتضمن القانون المدني المعدل والمتمم ،ج .ر رقم 44 المؤرخ في 26 يونيو 2005،ص17.
10- القانون (06-01) المؤرخ في 20 فبراير2006يتعلق بالوقاية من الفساد ومكافحته ج.ر رقم 14 بتاريخ 8مارس2006.
11-قانون (09 -03) المتعلق بحماية المستهلك و قمع الغش المؤرخ في 25 فبراير2009،ج.ر رقم15 ليوم 8 مارس2009.

12- القانون (09-04)المؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

13 - قانون رقم(15-03)مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، يتعلق بعصرنة العدالة،ج.ر رقم 06 ليوم 10 فبراير سنة 2015.

14- قانون رقم (15-12)مؤرخ في 28 رمضان عام 1436 الموافق 15 يوليو سنة2015، يتعلق بحماية الطفل،ج ر رقم39 بتاريخ 19 يوليو سنة2015.

15- قانون (16-02)مؤرخ في 14 رمضان عام 1437 الموافق 19 يونيو سنة 2016، ج ر رقم 37 ليوم 17 رمضان عام 1437 هـ 22 يونيو سنة 2016 م ص4، يتمم الأمر رقم 66-156 المؤرخ في 18عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

16- قانون (16-03)مؤرخ في 14 رمضان عام 1437 الموافق 19 يونيو سنة 2016، يتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص.ج ر رقم 37 ليوم 17 رمضان عام 1437 الموافق 22 يونيو سنة 2016 م.

17- قانون رقم (17-07) مؤرخ في 28 جمادى الثانية عام 1438 الموافق 27 مارس 2017، يعدل ويتمم قانون الإجراءات الجزائية،ج.ررقم20 ليوم29مارس2017.

هـ- المراسيم:

1- المرسوم رقم (84-387)مؤرخ في 29 ربيع الأول عام 1405 الموافق 22 ديسمبر سنة 1984 يحدد التدابير المخصصة لحماية الوثائق المصنف،ج.ر69 مؤرخة في 26 ديسمبر1984.

2- المرسوم رقم(84-388) مؤرخ في 29 ربيع الأول عام 1405 الموافق 22 ديسمبر سنة 1984 يحدد كيفيات تأهيل الموظفين الذين يدعون إلى الاطلاع على المعلومات أو الوثائق المصنف، ج.ر 69 مؤرخة في 26 ديسمبر1984.

3- المرسوم الرئاسي رقم(04-183) المؤرخ في 8 جمادى الأولى عام 1425هـ الموافق 26 يونيو سنة 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر رقم 41 ليوم 27 يونيو 2004،ص18.

4- المرسوم التنفيذي رقم (06-348)المؤرخ في 12 رمضان عام 1427 الموافق 5 أكتوبر سنة 2006 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ،المعدل بالمرسوم التنفيذي رقم(16-267)مؤرخ في 15 محّرم عام 1438 الموافق 17 أكتوبر سنة 2016،ج.ر، رقم 62 ليوم 23 أكتوبر 2016.

5- مرسوم رئاسي رقم(15-228)مؤرخ في 7 ذي القعدة عام 1436 الموافق 22 غشت سنة2015، يحدد القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو وسيره.

6- المرسوم الرئاسي(15-261) مؤرخ في 24ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج. ر. 53 .

خامسا– القرارات القضائية:

1- قرار غرفة الجنح والمخالفات الصادر في: 1983/11/29 ملف رقم 34094، المجلة القضائية العدد الرابع لسنة 1989.

2- قرار جنائي صادر في 1989/11/28 ملف رقم 58430، المجلة القضائية، العدد الثاني لسنة 1994.

3- قرار غرفة الجنح والمخالفات الصادر في: 1990/01/23 ملف رقم 59484، المجلة القضائية العدد الأول لسنة 1992.

سادسا– مواقع الانترنت:

1– الاتفاقية الأوروبية للإجرام السيبيري ؛https://rm.coe.int/16802fa3ff

2– اليونسكو منظمة الأمم المتحدة للتربية والعلم والثقافة
https://ar.wikipedia.org/wiki/%D9%8A%D9%88%D9%86%D8%B3%D9%83%D9%88
http://ar.unesco.org/about-us/introducing-unesco

3– الاعلان العالمي الخاص بالمبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة https://documents-dds-
ny.un.org/doc/RESOLUTION/GEN/NR0/472/21/IMG/NR047221.pdf?OpenElement

4– يونس عرب ،جرائم الكمبيوتر والانترنت، منشورعلى الموقع التالي:
http://www.arablaw.org/Download/CyberCrimes_WorkPaper.doc

5–محمد عبد الله المنشاوي ،جرائم الانترنت من منظور شرعي وقانوني،انظر الموقع
http://www.ba-menoufia.com/books-pdf/1304065160509f5b748.pdf

6–الجريدة الرسمية للمناقشات، المجلس الشعبي الوطني والخاصة بالمناقشة العامة لمشروع القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها
http://www.apn.dz/ar/images/journal_officiel_debats/6_legislature/jod_6leg_122.pdf

7–الانتربول:

https://www.interpol.int/ar/%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D8%B9%D9%86-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D8%A8%D9%88%D9%84/%D9%84%D9%85%D8%AD%D8%A9-%D8%AA%D8%A7%D8%B1%D9%8A%D8%AE%D9%8A%D8%A9

8– تعريف اليوتيوب

http://mawdoo3.com/%D8%A8%D8%AD%D8%AB_%D8%B9%D9%86_%D8%A7%D9%84%D9%8A%D9%88%D8%AA%D9%8A%D9%88%D8%A8

9- جواز السفر

البيومتريhttps://passeport.interieur.gov.dz/Ar/Suivi/Suivi_Demande

II. La bibliographie en langue française :

1- les ouvrages Généraux:

1-Aurélie Bergeaud-Wetterwald, Jean-Christophe Saint-Pau , La preuve pénale, Problèmes contemporains en droit comparé , Editions L'Harmattan, 2013.

2-Eric Przyswa, Cybercriminalité et contrefaçon, FYP editions, 2010 .

3-Gaston Stefani et Georges Levasseur et Bernard Bouloc, procédure pénale, 17 édition, Dalloz 2000.

4-Jean Larguier, Philippe Conte, Procédure pénale 22e édition, 2010, Dalloz, Paris.

5-Solange Ghernaouti-Helie , Sécurité Informatique et réseaux , dunod, paris, 2006.

6- Sylvain Métille , Mesures techniques de surveillance et respect des droits fondamentaux en particulier dans le cadre de l'instruction pénale et du renseignement, collection neuchâteloise, 2011.

7-Thierry Care Catherine Ginestet, Droit Penal – Procedure – Penale, Dalloz ed, 2000.

2- Les ouvrage spéciaux :

1-Christiane Féral-Schuhl , Cyberdroit: le droit à l'épreuve de l'Internet,6e edition , Dalloz, 2010.

2- Jacques Ravanas, la protection contre la réalisation et la publication de leur image, Librairie générale de droit et jurisprudence, paris, 1978.

3-Mohamed Chawki, Combattre la cybercriminalité, Edition de Saint Amans France, 2008

4-Myriam QUEMENER et Joël FERRY, Cybercriminalité, Défi mondial et réponses, Ed ECONOMICA, PARIS, 2007

5-Myriam QUÉMÉNER, Yves CHARPENEL Cybercriminalité, Droit pénal appliqué, 2010, ECONOMICA ,Paris France.

6- Sedallian Valerie, Droit de l`Internet, réglementation responsabilités, contrats, collection AUI, Paris1997.

7- Solange Ghernaouti-Hélie, Internet et Sécurité, *Paris*, PUF, *« Que sais-je ? » ,2002.*

8-Solange Ghernaouti-Hélie , La cybercriminalité: le visible et l'invisible, Collection le savoir suisse, 2009.

9-Solange Ghernaouti –Hélie, Sécurité Informatique et réseaux, dunod, paris, 2006.

3- Les articles:

1- Hadjira Bouder, fournisseurs de services Internet, Prévention et lutte contre la cybercriminalité :actes du séminaire international Alger le 5-6 mai 2010, CRJJ, 2011.

2- Madjid kali, La preuve dans le procès pénal, revue de la gendarmerie, n° 16 février 2006.

الفـــهرس

الشكر	أ
إهداء	ب
قائمة المختصرات	ج
مقدمة	1
البـــــاب الأول ذاتية جرائم الانترنت في التشريع الجزائري	12
الفصل الأول:الإطار القانوني لجرائم الانترنت في التشريع الجزائري.	14
المبحث الأول:مفهوم جرائم الانترنت في التشريع الجزائري.	15
المطلب الأول:تعريف جرائم الانترنت.	16
الفرع الأول:التعريف الضيق لجرائم الانترنت.	16
أولا: المعلوماتية أو علم المعلومات .	17
ثانيا: نظام المعلومات	23
الفرع الثاني:التعريف الواسع لجرائم الإنترنت.	26
أولا: تعريف الانترنت	27
ثانيا:محل جرائم الانترنت	33
المطلب الثاني:سمات جرائم الانترنت.	35
الفرع الأول:خصائص جرائم الانترنت	35
أولا:الوسيلة المستخدمة في ارتكابها.	35
ثانيا:جريمة عابرة للحدود.	37
ثالثا:صعوبة اكتشاف والإثبات الجنائي.	37
الفرع الثاني: مستخدم الانترنت.	39
أولا:الضحية أو المجني عليه.	39
ثانيا:مجرم الانترنت.	41
المبحث الثاني:صور جرائم الانترنت في التشريع الجزائري	51
المطلب الأول: الجرائم التقنية في التشريع الجزائري	52
الفرع الأول: الأحكام المشتركة للجرائم التقنية.	52

أولا: الاتفاق الجنائي في الجرائم التقنية:	52
ثانيا:الشروع في الجرائم التقنية.	55
ثالثا:الجرائم التقنية المرتكبة ضد المؤسسات و الهيئات العامة.	57
رابعا:الجريمة التقنية المرتكبة من الشخص المعنوي .	60
خامسا: العقوبات التكميلية للجرائم التقنية	64
الفرع الثاني: جريمتا الدخول والبقاء في نظام المعالجة الآلية.	68
أولا:الركن الشرعي لجريمتي البقاء والدخول في منظومة معلوماتية.	69
ثانيا:الركن المادي لجريمة الدخول والبقاء إلى المنظومة المعلوماتية	69
ثالثا: الركن المعنوي لجريمة الدخول والبقاء.	75
رابعا: الصورة المشددة للجريمة	76
الفرع الثالث: جرائم الاعتداء العمدي والتعامل في البيانات و نظم المعالجة الالية للمعطيات	76
أولا:جريمة الاعتداء العمدي على البيانات المخزنة في النظام	77
ثانيا:جريمة التعامل في البيانات خارج النظام	80
ثالثا:جريمة الاعتداءات العمدية على سير نظم المعالجة الآلية للمعطيات	86
المطلب الثاني:الإجرام غير ألمعلوماتي في التشريع الجزائري	87
الفرع الأول: جريمة الإرهاب الالكتروني	87
أولا: الركن الشرعي	88
ثانيا: الركن المادي لجريمة الإرهاب الالكتروني.	91
ثالثا: الركن المعنوي لجريمة الإرهاب الالكتروني	92
الفرع الثاني: جريمة إهانة وسب وقذف رئيس الجمهورية.	92
أولا:الركن الشرعي.	93
ثانيا: الركن المادي	93
ثالثا: الركن المعنوي	95
الفصل الثاني:أدلة إثبات جرائم الإنترنت في التشريع الجزائري.	97
المبحث الأول:ماهية الدليل الجنائي الالكتروني.	98

المطلب الأول: الدليل الجنائي الإلكتروني.	99
الفرع الأول:تعريف الدليل الجنائي الالكتروني.	100
أولا: الدليل الجنائي	100
ثانيا:الدليل الجنائي في شكله الالكتروني	102
الفرع الثاني: خصائص وأشكال الدليل الجنائي الإلكتروني.	105
أولا: خصائص الدليل الجنائي الإلكتروني	105
ثانيا:أشكال الدليل الجنائي الإلكتروني	108
الفرع الثالث:مصادر الدليل الجنائي الإلكتروني	111
أولا:نظم الإتصال بالشبكة	112
ثانيا:فحص مركبات المنظومة المعلوماتية.	113
المطلب الثاني: المتدخلون في شبكة الإنترنت .	115
الفرع الاول: مقدم خدمة الإنترنت .	116
أولا: تعريف مقدم خدمات الإنترنت .	117
ثانيا:الخدمات التي يقدمها مزود خدمات الإنترنت .	118
ثالثا:أصناف مزودي خدمات الإنترنت .	122
الفرع الثاني: المسؤولية الجزائية لمزودي خدمات الإنترنت .	124
اولا: التزامات مقدمي خدمات الانترنت	124
ثانيا:المسؤولية المترتبة على الإخلال بالتزامات مقدمي خدمات الانترنت	127
المبحث الثاني:دعائم الإثبات الجنائي في جرائم الانترنت.	135
المطلب الأول:الدعائم القولية والاستدلالية(شهادة الشهود والقرائن)	135
الفرع الأول: شهادة الشهود في جرائم الانترنت.	136
أولا:الشاهد ألمعلوماتي.	137
ثانيا:التزامات الشاهد المعلوماتي	143
ثالثا:شهادة الشهود الإلكترونية	147
الفرع الثاني: القرائن في جرائم الانترنت.	150

أولا :أهمية القرائن في جرائم الانترنت.	151
ثانيا:أثر القرائن في جرائم الانترنت.	152
المطلب الثاني:دعائم الإثبات المادية(المعاينة والخبرة)	152
الفرع الأول:المعاينة	153
أولا:تعريف المعاينة.	153
ثانيا: اجراءات المعاينة	157
الفرع الثاني:الخبرة التقنية.	161
أولا:تعريف الخبرة.	161
ثانيا:أنواع الخبرة	162
ثالثا:الخبير التقني.	164
البـــــاب الثاني: إجراءات الإثبات الجنائي في جرائم الانترنت في التشريع الجزائري	171
الفصل الأول:التحري و التحقيق في جرائم الانترنت في التشريع الجزائري.	174
المبحث الأول:التحري والتحقيق في جرائم الانترنت في إطار قانون الإجراءات الجزائية.	175
المطلب الأول: اعتراض المراسلات والتقاط الصور وتسجيل الأصوات.	177
الفرع الأول:تعريف اعتراض المراسلات وتسجيل الأصوات والتقـــــاط الصور.	178
أولا:اعتراض المراسلات.	178
ثانيا:التسجيل الصوتي.	183
ثالثا: التقاط الصور.	186
الفرع الثاني:شروط الأخذ بإجراء اعتراض المراسلات والتقاط الصور وتسجيل الأصوات.	189
أولا:الشروط الموضوعية لإجراء اعتراض المراسلات والتقاط الصور وتسجيل الأصوات.	189
ثانيا:الشروط الشكلية لإجراء اعتراض المراسلات والتقاط الصور وتسجيل الأصوات.	191
المطلب الثاني: التسرب.	194
الفرع الأول: الشروط الموضوعية لإجراء التسرب.	196

أولا: مباشرة التسرب من طرف أعوان الشرطة القضائية في إطار قانون الإجراءات الجزائية	197
ثانيا:وقوع جريمة انترنت جناية أو جنحة.	198
ثالثا:ضرورة إجراء التسرب في إطار التحري أو التحقيق لجريمة من جرائم الانترنت.	199
الفرع الثاني:الشروط الشكلية لإجراء التسرب في جرائم الانترنت.	200
أولا:الحصول على إذن .	200
ثانيا : تحديد المدة المطلوبة لعملية التسرب في جرائم الانترنت.	201
ثالثا: تحرير المحضر الخاص بإجراء التسرب.	202
المبحث الثاني:التحقيق في إطار القانون (09-04)	204
المطلب الأول: المراقبة الإلكترونية للاتصالات في التشريع الجزائري	204
الفرع الأول: الأساس مراقبة الاتصالات الإلكترونية	205
أولا:حظر مراقبة الاتصالات الإلكترونية	206
ثانيا:تعريف مراقبة الاتصالات الإلكترونية	208
الفرع الثاني:ضمانات مراقبة الاتصالات الإلكترونية في التشريع الجزائري	211
أولا :شروط مراقبة الاتصالات الإلكترونية في التشريع الجزائري	211
المطلب الثاني:التفتيش و الحجز في جرائم الانترنت في التشريع الجزائري.	213
الفرع الأول:التفتيش في جرائم الانترنت في التشريع الجزائري.	213
أولا: نطاق تفتيش مكونات النظام ألمعلوماتي في جرائم الانترنت.	214
ثانيا : شروط التفتيش في جرائم الانترنت.	221
الفرع الثاني:الضبط في جرائم الانترنت في إطار القانون (09-04).	228
أولا :مشاكل الضبط في جرائم الانترنت.	229
ثانيا: ضبط الدليل الجنائي في جرائم الانترنت.	239
الفصل الثاني:الاختصاص والتعاون القضائي الدولي والقيمة القانونية للدليل الجنائي في جرائم الانترنت	247
المبحث الأول:الاختصاص القضائي والتعاون الدولي في جرائم الانترنت	248
المطلب الأول:الاختصاص القضائي في جرائم الانترنت في التشريع الجزائري.	248

الفرع الأول:الاختصاص القضائي الداخلي.	249
الفرع الثاني:الاختصاص القضائي الدولي.	252
أولا:مبدأ الإقليمية في جرائم الانترنت	253
ثانيا:المبادئ الاحتياطية في جرائم الانترنت	256
الفرع الثالث:الهيئات الوطنية المختصة في جرائم الانترنت.	259
أولا:الهيئة الوطنية للوقاية من الجرائم المتصلة تكنولوجيات الإعلام والاتصال ومكافحته	260
ثانيا:مراكز وأقسام والمعاهد المختصة بجرائم الانترنت	263
المطلب الثاني: التعاون الدولي في جرائم الانترنت.	269
الفرع الأول: التعاون القضائي الدولي.	270
أولا:تعريف التعاون القضائي الدولي.	270
ثانيا: التعاون الأمني الدولي	272
الفرع الثاني:صور التعاون القضائي الدولي	274
أولا: المساعدة القضائية.	275
ثانيا: تبادل المعلومات ونقل الإجراءات في جرائم الانترنت.	275
ثالثا: الإنابة القضائية.	276
المبحث الثاني:القيمة القانونية للدليل الجنائي في جرائم الانترنت في التشريع الجزائري.	280
المطلب الأول:مشروعية الدليل الجنائي في جرائم الانترنت.	281
الفرع الأول:مشروعية الحصول على الدليل الجنائي في جرائم الانترنت.	282
أولا: الضمانات القانونية قي إطار قانون الإجراءات الجزائية	283
ثانيا:الضمانات القانونية في إطار قانون (09-04)	288
الفرع الثاني:جزاء الإخلال بمشروعية الدليل الجنائي في جرائم الانترنت.	292
أولا- البطلان الجزائي.	294
ثانيا:المسؤولية المتعلقة بالإخلال بقواعد الحصول على الدليل الجنائي في جرائم لانترنت.	300
المطلب الثاني:حجية الدليل الجنائي في جرائم الانترنت في التشريع الجزائري.	311
الفرع الأول:شروط قبول الدليل الجنائي في جرائم الانترنت.	312

أولا:يقينية الدليل الجنائي في جرائم الانترنت.	314
ثانيا: مناقشة الدليل الجنائي في جرائم الانترنت.	315
الفرع الثاني:مدى حرية القاضي في تقدير الدليل الجنائي في جرائم الانترنت.	317
أولا:الاقتناع الحر للقاضي.	318
ثانيا:القيود الوارد على حرية القاضي.	321
الخاتمة	326
الملاحق	334
قائمة المراجع	344
الفهرس	366

ملخص:

تمثل جرائم الانترنت نمط جديد من أنماط السلوك الإجرامي التي تتميز بخصائص منفردة دفعت المشرع الجزائري إلى سن قوانين خاصة للوقاية منها ومكافحتها، واهم خاصية أثرت في التشريع هو كيفية إثبات هذه الجرائم، وماهي إجراءات الجزائية لإثباتها، لدى قام المشرع بتثمين إجراءات كالتفتيش عن بعد وحجز المعطيات، وإضافة إجراءات جديدة لإثبات جرائم الانترنت كمراقبة الاتصالات الالكترونية. كما قام بتعزيز إجراءات التعاون الدولي للحصول على الدليل في شكله الالكتروني .ولكن ورغم كل الجهود المبذولة فلا يزال يتخلل عملية الإثبات –دعائم الإثبات والدليل الجنائي الالكتروني– نقص يتعلق بضمانات الحصول على الدليل .

كلمات مفتاحية :جرائم الانترنت، تكنولوجيات الإعلام والاتصال، الدليل الجنائي الإلكتروني ،دعائم الإثبات ،المراقبة الالكترونية ،التفتيش عن بعد ،حجز المعطيات.

Résumé:

La cybercriminalité présente une nouvelle forme de délinquance a des caractéristiques uniques qui ont incité le législateur algérien à promulguer des lois spéciales pour les prévenir et les combattre.

La caractéristique la plus importante affectée par la législation est comment prouver ces crimes, et quelles procédures criminelles prouver.

Lorsque le législateur peser des mesures telles que, (Perquisition a distance -Saisie de données informatiques) , et ajouter de nouvelles mesures pour prouver cyber crimes tels que la surveillance des communications électronique, Il a également renforcé les procédures de coopération internationale pour obtenir les preuves sous format électronique , Malgré tous les efforts déployés, le processus de preuve continue(la preuve pénale électronique)Manque de garanties d'obtention de preuve .

Mots-clés: cybercriminalité , technologies de l'information et de la communication, preuves sous forme électronique, la surveillance électronique, Perquisition des systèmes informatiques ,Saisie de données informatiques

Abstract:

Cybercrime presents a new form of delinquency with unique characteristics that prompted the Algerian legislator to promulgate special laws to prevent and combat them. The most important feature affected by the legislation is how to prove these crimes, and what criminal procedures prove. When the legislature weigh measures such as, (Remote search -Data entry computer), and add new measures to prove cyber crimes such as electronic communications monitoring, It also strengthened the international cooperation procedures to obtain the evidence under electronic format, Despite all the efforts made, the process of continuous evidence (electronic criminal evidence) Lack of guarantees of obtaining evidence.

Key-words: Cybercrime, information and communication technologies, digital evidence .cyber surveillance. search and seizure of stored computer data