الجمهوريّـــة الجزائريّـــة الدّيمقراطيّـــة الشّعبيّـــة

وزارة التعليم العالي و البحث العلمي
جامعـــــة مولاي الطاهـــــر
قســـــم الحقوق

المذكّـــــرة تحت عنوان :

آليات البحث و التحرّي عن الجريمة المعلوماتيّة

مذكّرة مقدّمة لنيل شهادة الماستر في الحقوق
تخصص : قانون جنائي

من إعداد الطالبة :
بغاديـــــد نبيـــة

تحت إشراف الأستاذ
أ.د. عثماني عبد الرّحمن

لجنة المناقشة

أ.د. عثماني عبد الرّحمن .....مشرفا ومقرّرا.
أ.د. مـــــــرزوق محمّد .....رئيســـــــــا.
أ.د. فليـــــح كمـــــــال .....عضوا مناقشا.
أ.د. نابـــــي عبد القـادر .....عضوا مناقشا.

السّنـــــــة الجامعيّـــــة

2016 * 2015

الإهـــــداء

إلـــــى من أوصاني بهما ربي برا وإحسانا

والدي **أمـي وأبـي،**

إلـــــى **إخوتي وأخواتي** و إلى الكتكوتة **رتاج ليندة**

ريحانة قلبي أهدي هذا العمل المتواضـع.

شكـــــر و تقديـــر

يشرفني أن أتقدم بأسمى معاني الشكر

والعرفان

إلى أستاذي الفاضل

الأستاذ الدّكتور عثماني عبد الرّحمـان

الّذي تولـّى مهمة الإشراف على هذه المذكّرة،

كما لا يفوتني أن أخلص بالشكر إلى كل من ساعدني

ولو بالكلمة الطيبة.

قائمة المختصرات

IP : وهو اختصار internet Protocol

IC3 : وهو اختصار Internet Crime complaint center

IFCC : وهو اختصار Internet Froude complaint center

NWC : وهو اختصار National White collar center

ICROS : وهو اختصار Internet Crime Reporting online system

TCP : وهو اختصار Tram mission control protocol

المقدمة

المقدّمة :

لا شك أنّ التطور التكنولوجي الّذي شهده العصر الحديث في مجـال التقنية و المعلومـاتية حقّق للبشر الرقـي و التقدم في شتّى مجالات الحياة لاسيما في مجال الاتصالات حتى أصبح يطلق عليه تسمية عصر المعلوماتية أو عصر ثورة المعلومات وهو ما دعى بالكثير من رجال الاقتصاد و الاجتماع إلى وصف الثورة المعلوماتية بالثورة الصناعية الثانية.

إنّ تدفق التقنية و انتشار التكنولوجيا ساعد على تحقيق الرفاهية و تسهيل ربط الاتصالات وإجراء المعلومات مع اختزال الوقت و التكلفة حتّى أصبح العالم وكأنّه قرية صغيرة وهذا بفضل التطوّر الهائل الّذي عرفته تقنية المعلومات تمّ التوصل إلى فكرة الرّبط بين أجهزة الإعلام الآلي ووسائل الاتصال مما ساعد على ظهور شبكات المعلومات و الّتي كان لها دور فعّال في التطور التكنولوجي و الاتصالات و الحسابات من جهة و البرمجة من جهة اخرى، حيث أصبحت هذه التقنية معتمد عليها بشكل واسع جدّا وهذا في نقل و تبادل المعلومات بالصوت و الصورة عبر أنحاء العالم و الّتي صارت بذلك نظم المعالجة الآلية للمعطيات بفضل التقنيات الّتي تقوم عليها و الّتي تتمثّل في الحواسيب و الشبكات المعلوماتية حيث نجدها في جميع القطاعات سواء قطاع الصناعة ، الصّحة أو التعليم و غيره...

أصبحت من الصعب جدّا الاستغناء على هذه التقنية لأنّها تعتمد عليها في تسيير أعمالها وأصبحت من اللّوازم الأساسية و الضرورية في مواكبة العالم الخارجي و التطور باستخدام نظم المعالجة الآلية لكنّه إلى جانب المزايا التي جلبتها التكنولوجيا و التقنية في شتّى الميادين ترتب عنها جملة من الانعكاسات السلبية وهذا راجع لسوء استخدام التقنية المعلوماتية أو تلك الوسائل فقد أدّى إلى تسهيل ارتكاب الكثير من الجرائم التقليديّة على نطاق واسع على غرار جرائم السرقة و جرائم التجسس وانتهاك حرمة الحياة الخاصّة وحرمة المرسلات و الجرائم المخلّة بالآداب العامّة.

كما أدّى سوء استخدام التقنية المعلوماتية إلى بروز نوع جديد من الجرائم ذو طبيعة خاصّة وتدعى الجريمة المعلوماتية أو الجريمة الإلكترونية، لا تقل في خطورتها و حجم الأضرار الّتي قد تلحقها عن خطورة أهم و أشدّ الجرائم التقليديّة فتكا، لكنّه و رغم أهميّة الجرائم المعلوماتيّة و خطورتها و فداحة الأضرار الّتي قد تلحقها بالدّول الّتي سارعت إلى إدخال التقنية المعلوماتية في أنظمتها الأمنيّة الاجتماعية و الاقتصادية غير أنّ تلك الدّول تخلّفت عن تكريس الإطار القانوني الّذي يحمي تلك المنظومات من الاعتداء عليها أو سوء استغلالها، لاسيما من الأفعال الضّارة و الّتي ترقى إلى وصف الجرائم، و الأخطر من ذلك فإنّ تلك الدّول أهملت وضع إطار قانوني للبحث عن تلك الجرائم و تقديم مرتكبيها أمام العدالة الجنائيّة من خلال وضع آليّات و ترتيبات لازمة لذلك و من خلال تعزيز مبدأ الإثبات بتكريس الدّليل الإلكتروني وتقنينه.

الشّيء الّذي تبعه ظهور أنماط جديدة من الاعتداءات على تلك المعلومات المخزّنة في بيئة افتراضية ليس هذا فحسب بل سهّلت هذه التقنية ارتكاب بعض الجرائم التقليديّة، فازدادت هذه المخاطر تفاقما في ظلّ البيئة الافتراضية الّتي تمثّلها شبكة المعلومات ممّا أفرز نوعا جديدا من الجرائم لم يكن من قبل عرفت بالجرائم المعلوماتيّة أو جرائم تقنيّة المعلومات و الخطورة الّتي تتميّز بها هذه الجرائم أنّها سهلة الارتكاب، و أنّ آثارها ليست محصورة في نطاق الإقليمي للدّولة كما أن مرتكبيها يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الدولية للمعطيات لأن لها طبيعة خاصة وهو عبارة عن اشارات ونبضات إلكترونية تظم المعالجة الالية وشبكات الاتصال العالمية بصورة آلية الأمر الذى بات يثير بعض التحديات القانونية والعملية وبالذات فيما يخص اثبات هذه الجرائم وكيفية مكافحتهم وتقديمهم للعدالة.

فاذا كانت الجهات المكلّفة بالبحث و التحرّي عن الجريمة و الّتي يمكن إدراكها بالحواس لما يخلّفه المجرم من آثار مادّية في مسرح الجريمة من بصمات أو يقع دم أو محرّرات مزوّرة وغير ذلك، فإنّ المشكلات الإجرائيّة الّتي ستواجه هذه الجهات عند تعاملها مع الجريمة المعلوماتية، تبدأ من طبيعة البيئة الافتراضية التقنية الّتي ترتكب فيها، فهي لا تخلّف أي آثار مادّية محسوسة ، فنجد أنّ المجرم المعلوماتي يخفي نشاطه عن طريق التلاعب بالبيانات و الّذي غالبا ما يتحقق في غفلة من المجني عليه وهذا عن سهولة تدمير وإخفاء من مسرح الجريمة ممّا يصعب ويعقّد أمر كشفها وتحديد مرتكبيها.

ولهذا فإنّ هذه الظاهرة الإجرامية التقنيّة أثارت العديد من المجادلات في قانون الإجراءات الجزائيّة الّذي وضعت نصوصه لتحكم الإجراءات المتعلّقة بجرائم تقليديّة لا توجد صعوبة في إثباتها وتحقّق فيها مع خضوعها لمبدأ الاقتناع الشخصي للقاضي الجزائي، وهو الأمر الّذي كان عاملا حاسما لتدخّل المشرّع بنصوصه القانونيّة الجزائيّة، ممّا أدّى إلى ظهور نوع جديد من الأدلّة يمكن الاعتماد عليها في إثبات هذه الجرائم من ذات الطبيعة التقنيّة الّتي تتميّز بها البيئة محلّ الجريمة.

وقد كان ذلك بأن قام المشرّع الجزائري بتعديل قانون الإجراءات الجزائيّة بموجب القانون 22/06 المؤرّخ في 20 ديسمبر 2006، بالإضافة إلى إصداره للقانون 04/03 المتضمّن للقواعد الخاصّة للوقاية من الجرائم المتّصلة بالتكنولوجيا الإعلام و الاتّصال و على هذا الأساس نجد أنّ المشرّع أوجد طرقا إجرائيّة تتّفق و الطبيعة التقنيّة للجريمة المعلوماتية.

حيث يعد موضوع البحث من الموضوعات الجديدة في اطار القسم الاجرائي الّذي اقتصر على البحث في الجوانب الموضوعية دون محاولة الغوص في مسالة إثباتها ومعرفة مدى تأثير خصائصها على الإجراءات المناسبة في ذلك، لأن الجرائم المعلوماتية من المستجدات لم تكن معروفة للقانون الجزائي سواء الموضوعي او الإجرائي لأن الجرائم المعلوماتية تختلف من حيث إجراءات التحقيق وجمع الأدلّة كما هو الحال عليه بالنسبة للجرائم التقليدية لهذا تعد من الجرائم التي يصعب الكشف عنها وإثباتها نظرا للسّرعة والدّقة العالية في تنفيذها وكذا امكانية محوها واخفاء الأدلّة المتحصلة منها عقد تنفيذها.

فمن خلال بحثنا هذا نتطرّق إلى العديد من التساؤلات و الّتي تعتبر جوهر موضوع الدّراسة فمن بين هذه التساؤلات ما يلي :

- ماهي طبيعة الدّليل المناسب لإثبات الجريمة المعلوماتيّة ؟.
- كيف يمكن استخلاص الدّليل الرّقمي من الشبكة الإلكترونيّة ؟.
- كيف تكون طريقة البحث و التحرّي في استخلاص الدّليل الرّقمي ؟.
- ما موقف المشرّع الجزائري من ذلك ؟.

وعلى هذا الأساس يمكن أن نحصر نطاق هذه الدّراسة ضمن خطّة تتكوّن من فصلين:

* فالفصل الأوّل: هو المفهوم القانوني للجريمة المعلوماتيّة.

* أمّا الفصل الثّاني : فنتطرّق إلى الجوانب القانونيّة للتحقيق في الجريمة المعلوماتيّة.

الأنترنت : هي كلمة إنجليزية الأصل تتكوّن من مقطعين هي: Inter و تعني الاتصال أمّا الثانية Net و تعني الشبكة و إذا جمعنا الكلمتين معا فإنّ المعنى الكامل هو : الشبكة المتّصلة.

الفصـــل الأوّل

الفصل الأوّل: المفهوم القانوني للجريمة المعلوماتيّة.

بالرّغم من المزايا الهائلة الّتي تحقّقت كلّ يوم بفضل تقنيّة المعلومات على جميع الأصعدة وفي شتّى الميادين، فإنّ هذه الثورة التكنولوجيّة المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبيّة الخطيرة جرّاء سوء استخدام هذه التقنيّة المتطوّرة و الانحراف عن الأغراض المتوخّاة منها، فالجرائم المعلوماتيّة تعدّ صنفا مستحدثا من الجرائم التي تتعدّى القواعد التقليديّة للتجريم و العقاب الّتي تقتضي ضرورة تحقق أركان الجريمة طبقا لمبدأ شرعيّة الجرائم و العقوبات.

المبحث الأوّل: الجريمة المعلوماتيّة.

تعتبر الجريمة المرتكبة عبر الأنترنت من الآثار السلبية الّتي خلّفتها التقنيّة العاليّة حيث أخذت هذه الظّاهرة الإجراميّة حيّزا كبيرا من الدّراسات من أجل تحديد مفهوم الجريمة المعلوماتيّة، ممّا إنجرّ عنه وضع عدّة مصطلحات للدلالة عليها، من بينها جرائم الحاسب، جرائم التقنيّة العاليّة، جرائم المعلوماتيّة، جرائم الغش المعلوماتي، وصولا إلى الجرائم ويعتبر عدم الاستقرار على مصطلح واحد للدّلالة على الجريمة المرتكبة عبر الأنترنت.

أدّى تطوّر العلوم الجنائيّة إلى ظهور عدّة نظريّات في علم الإجرام و من بين أهمّها تلك المتعلّقة بطبيعة المجرم، فعلى سبيل المثال التطوّر الّذي عرفته الجريمة الاقتصادية نتج عنها ظهور نظريّات جديدة تختلف عن الفئات الإجراميّة التقليديّة و المتمثّلة في فئة مجرمي الأنترنت.

وعلى هذا الأساس فالجريمة بصفة عامّة على أنّها فعل غير مشروع صادر عن إرادة آثمة يقرّر له القانون عقوبة تدبيرا احترازيّا، وتعتمد الجرائم النّاشئة عن استخدام غير المشروع لشبكة الأنترنت على المعلومة بشكل رئيسي وهذا الّذي أدّى إلى إطلاق مصطلح الجريمة المعلوماتيّة على هذا النوع من الجرائم [1] و الّتي كانت هناك اتّجاهات مختلفة في تعريفها.

المطلب الأوّل : مفهوم الجريمة المعلوماتيّة.

تعدّ الجريمة المعلوماتيّة من الظّواهر الإجراميّة الحديثة كما ذكرنا بالإضافة إلى ذلك مفهومها يعدّ من الخطوة الأولى للتعرّف على هذه الظّاهرة الجرميّة من جميع جوانبها القانونيّة، خاصّة إذا علمنا أنّه لا يوجد مصطلح قانوني موحّد للدلالة على هذه الظّاهرة الناشئة في بيئة الكمبيوتر بسبب ذاتها وتميّزها عن غيرهـا من الجرائم التقليديّة، سواء في محلّها أو خصائصها، وممّا لا شك فيه فإنّ أي محاولة من أجل اختيار و تحديد المصطلح الملائم لهذه الظاهرة ينبغي أن يكون مبنيا ومؤسّسا على عدّة ضوابط تقنيّة و قانونيّة أوّلها إدماج البعدين التقني و القانوني، ذلك أنّ تقنيّة المعلومات في أصلها هي نتاج اندماج الحواسب و الاتصال، فأمّا الحوسبة فتقوم على أساس وسائل التقنيّة للإدارة وتنظيم و معالجة المعطيات في إطار تنفيذ مهام محدّد تتّصل بعملي الحساب و المنطق، أمّا الاتصال فهو قائم على وسائل تقنيّة لنقل المعلومات.

و الضابط الثاني يقوم على أساس البحث بشأن الحدود الّتي ينتمي عندها العبث وتلك الّتي تبدأ عندها المسؤوليّة عن أفعال تعدّ مجرمة، و الضابط الثالث أن يكون اختيار المصطلح شاملا لما يعبّر عنه مُلمًا بحدود محلّه، فلا ينبغي أن يقتصر على الجزء ليعني الكل ولا ينصرف إلّا ما لا يجب أن ينطوي تحت نطاقه.

(1) محمّد عبيد الكعبي : الجرائم الناتجة عن استخدام غير مشروع لشبكة الأنترنت دار النّهضة العربيّة القاهرة ص 32.

فالجرائم النّاشئة في البيئة الرّقمية جرائم حديثة، ارتبط مفهومها ولا يزال يرتبط بتكنولوجيا الحسابات وتطوّراتها المستخدمة في تشغيل و تخزين و نقل المعلومات في شكل إلكتروني، وكذا بتكنولوجيا ووسائل الاتصال وشبكات الرّبط، لذلك فإنّه من الضّروري أن يكون أي تعريف لهذا النّمط من الجرائم متّسما بالمرونة و بما يسمح باستيعابه و تواكب مع سائر التقنيّات المبتكرة الرّاهنة و المستقبليّة في مجال تكنولوجيا التعامل مع المعلومات.

لكن التطوّر المستمر و اللامتناهي لتكنولوجيا المعلومـات و الاتّصالات حـال دون وضع تعريف فقهي جـامع و شامل لمفهوم الجريمة المعلوماتية [1] خشية من حصر نطاقها داخل إطار تجريبي محدّد قد يضر بها خاصة في فصل التطوّر المستمر للتقنيّة المعلوماتية، فما يتم تجريبه اليوم قد يصبح غير ذي أهمّيّة بالنسبة لصور مستحدثة أخرى تظهر نتيجة استخدام تقنيات جديدة.

ولقد ذهب الفقهاء في تعريف الجريمة المعلوماتية مذاهب شتّى ووصف تعريفات مختلفة تتمايز وتتباين تبعا لموضوع العلم المنتمية إليه و تبعا لمعيار التعريف ذاته، فاختلفت بين أولئك الباحثين في الظاهرة الإجراميّة النّاشئة عن التقنيّة المعلوماتيّة من الوجهة التقنيّة، وأولئك الباحثين في ذات الظاهرة من الوجهة القانونيّة، و حتّى من الوجهة القانونيّة تعدّدت التعريفات وفي سبيل ذلك فإنّ الفقه الجنائي قد بذل محاولات عديدة لتعريف الجريمة المعلوماتية لعلّ جميع المحاولات الّتي بذلت من أجل تعريف الجريمة المعلوماتية لا تخرج من أحد الاتجاهين أولها يضيف مفهوم الجريمة المعلوماتية أما الاتجاه الثاني يوسع تعريفها .

(1) خالد ممدوح إبراهيم : الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية ، الطبعة الأولى 2009 – .أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، الطبعة 2008.

فأنصار الاتجاه الأوّل حصروا الجريمة المعلوماتية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابهـــا، و أن الجرائم التي تفتقر إلى هذه الدرجة من المعرفة تعد جرائم عادية تتكفل بها النصوص التقليديــة للقوانين العقابيــة، و ذلك على خلاف الجرائم التي تتوفر لها هذه المعرفة فهي فقط التي تكون بحاجة إلى نصوص خاصة تتلاءم مع طبيعتها التي تختلف عن غيرها من الجرائم التقليدية [1] و من التعريفات الّتي وضعها أنصار هذا الاتّجاه أنّ الجريمة المعلوماتية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحسابات الآليّة بقدر كبير[2] وفي هذا الاتّجاه أيضا عرّفه الفقيه (دافيد تومسون DAVID Thomson) [3]، إنّها أية جريمة يكون متطلّبا لاقترافها أن تتوفّر لدى فاعلها معرفة بتقنيّة الحاسب و حسب هذا التعريف فإنّه يشترط أن يكون مرتكب الجريمة المعلوماتية على درجة كبيرة من العلم بتكنولوجيا الحاسب.

و في هذا الاتّجاه أيضا عرفها جانب الفقه بالنظر إلى معيار نتيجة الاعتداء ، إذ يرى الأستاذ (ماس MASS) أنّ المقصود بالجريمة المعلوماتيّة هي تلك الاعتداءات الّتي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح، كما عرفه أيضا الأستاذ (باركر PARKER) أنّ الجريمة المعلوماتيّة بأنّها كل فعل إجرامي متعمّد أيّا كانت صلته بالمعلوماتيّة ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحقّقه الفاعل أمّا بالنسبة للاتجاه الثاني و بالمفهوم الواسع للجريمة المعلوماتيّة حاولوا تعريفها على نحو واسع لتفادي أوجه القصور الّتي شابت تعريفات الاتجاه الأوّل .

(1) نائلة محمد فريد قورة : جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، الطبعة الأولى، ص 30.

(2) نائلة محمد فريد قورة : المرجع السابق، ص 28.

(3) رشيدة بوبكر : جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية ، الطبعة الأولى2012، ص 40.

فإنّ أنصار هذا الاتجاه يرو أنّ مفهوم الجريمة المعلوماتية مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يصيغ عليه وصف الجريمة المعلوماتية، فيذهب فريق من الفقهاء إلى تعريف الجريمة المعلوماتية بأنّها كلّ سلوك إجرامي يتمّ بمساعدة الحاسب الآلي و فريق آخر يعتبرها أنّها كلّ جريمة تتمّ في محيط الحاسبات الآليّة و من هذا التعريف ما جاء به الفقيه (مارو MERWE) الّذي يرى أنّ الجريمة المعلوماتيّة تتمثّل في الفعل غير المشروع الّذي يتورّط في ارتكابه الحاسب الآلي[1].

كما عرّفها الفقيهين (ريتشارد توتي Richard totty) و(أنتوني Anthony hardcastle) على أنّها الجرائم التي يكون للحاسب فيها دورا إيجابيا أكثر منه سلبا [2] ولا شكّ أنّ الاتجاه المتقدّم ينطوي على توسيع كبير لمفهوم الجريمة المعلوماتية، إذ يأخذ عليه هذا التوسع الّذي من شأنه أن يصيغ وصف الجريمة المعلوماتية على أفعال قد لا تكون كذلك لمجرّد مشاركة الحاسب الآلي في النشاط الإجرامي.

ولا يمكن القبول بهذا التوجه فقد لا يعدو أن يكون الحاسب الآلي محلا تقليديا في بعض الجرائم كسرقة الحاسب ذاته أو الأقراص أو الأسطوانات الممغنطة مثلا، فلا يمكن اعطاء وصف الجريمة المعلوماتية على سلوك الفاعل لمجرّد أنّ الحاسب أو احدى مكوّناته المادّيـة كانت محلا لفعل الاختلاس [3].

حتّى هذا الاتجاه انتقد حين وسع من نطـــاق هذه الجريمة إلى درجة التسويـة بين السلوك غير المشروع قانونـا و السلوك الّذي يستحقّ اللّوم أخلاقيا و استهجان الكافة له، كما في التعريف الّذي اورد خبراء منظمة التعاون الاقتصادي و التنمية OECD ذلك أنّه ليس بالضرورة أن يكون الانحراف عن الأخلاق و السّلوك المؤثم معاقب عليه [4].

(1) محمّد أمين الشوابكة : جرائم الحاسوب و الأنترنت، دار الثّقافة للنشر و التوزيع الطبعة الأولى 2009، ص 8.

(2) محمّد سامي الشوا : ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية 1994، ص 6.

(3) نائلة محمد فريد قورة : المرجع السابق، ص 31.

(4) عادل يوسف عبد النبي الشكري : الجريمة المعلوماتية و أزمة الشرعيّة ، دراسات الكوفة العدد السابع، ص 112.

المطلب الثاني : خصائص الجريمة المرتكبة على الأنترنت.

تعتبر الجريمة المرتكبة عبر الأنترنت من بين الجرائم المستحدثة الّتي أتى بها التطوّر في مجال الاتصالات، فهي تختلف عن الجريمة التقليديّة و الّتي ترتكب في العالم المادّي، و لذلك فهي تتميّز بخصائص وسمات جعلت منها ظاهرة اجراميّة جديدة لم يعرفها العالم من قبل و هي على النّحو التالي:

أ) خفاء الجريمة و سرعة التطوّر في ارتكابها : تتّسم الجرائم النّاشئة عن استخدام الأنترنت بأنّها خفية مستترة في أغلبها، لأنّ الضحيّة لا يلاحظها رغم أنّها قد تقع أثناء وجوده على الشبكة، لأنّ الجاني يتمتّع بقدرات فنيّة تمكّنه من جريمته بدقّة، مثلا عند ارسال الفيروس المدمّر و سرقة الأموال والبيانات الخاصّة أو اتلافها، و التجسس وسرقة المكالمات و غيرها من الجرائم [1].

فجرائم الأنترنت في أكثر صورها خفيّة لا يلاحظها المجني عليه أو يدري حتّى بوقوعها و الإمعان في حجب السلوك المكوّن لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونيّة الّتي تسجّل البيانات عن طريقها أمر ليس في كثير من الأحوال بحكم توافر المعرفة و الخبرة في مجال الحاسبات غالبا لدى مرتكبها.

(1) محمّد عبيد الكعبي : المرجع السابق ص 32.

ب) اعتبارها أقل عنفا في التنفيذ : لا تتطلّب هذا النّوع من الجرائم في تنفيذها إلى مجهود كبير أو للعنف فهي أقل جهد ممكن مقارنته بالجرائم التقليديّة الّتي تتطلّب نوعا من الجهد العضلي الّذي قد يكون في صورة ممارسته العنف و الإيذاء و لهذا نجد هذا النّوع من الجرائم يتميّز بطبعه للهدوء بل كلّ ما يحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني فمن هذا المنطق تعدّ الجريمة المرتكبة من الجرائم النظيفة فلا آثار فيها لأيّة عنف وإنّما مجرّد أرقام و بيانات يتمّ تغييرها من السجلاّت في ذاكرة الحاسبات الآليّة و ليس لها أثر خارجي مادّي [1].

ج) جريمة عابرة للحدود : بعد ظهور شبكات المعلوماتيّة لم يعد هناك حدود مرئيّة أو ملموسة تقف أمام نقل المعلومات عبر الدّول المختلفة، فالقدرة الّتي تتمتّع بها الحواسيب وشبكاتها في نقل كميّات كبيرة من المعلومات و تبادلها بين أنظمة يفصل بينهما آلاف الأميال قد أدّت إلى نتيجة مؤدّاها أن أماكن متعدّدة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد [2] فالسهولة في حركة المعلومات عبر أنظمة التقنيّة الحديثة جعل بالإمكان ارتكاب عن طريق حاسوب موجود في دولة معيّنة بينما يتحقّق القول الإجرامي في دولة أخرى.

د) امتناع المجني عليهم عن التبليغ : لا يتم في الغالب الأعم الإبلاغ عن جرائم الأنترنت إمّا لعدم اكتشاف الضحيّة لها وإمّا خشية من التشهير، لذلك نجد أنّ معظم الجرائم تمّ اكتشافها بالصدفة بل وبعد وقت طويل من ارتكابها.

(1) سيناء عبد الله محسن : المواجهة التشريعيّة للجرائم المتّصلة بالكمبيوتر في ضوء التشريعات الدوليّة و الوطنيّة.

(2) نهلة عبد القادر المؤمني : "الجرائم المعلوماتية" دار الثقافة للنشر و التوزيع عمّن 2008، ص 51.

هـ) سرعة محو الدّليل وتوفّر وسائل تقنيّة تعرقل الوصول إليه : تكون البيانات و المعلومات المتداولة عبر شبكة الأنترنت على هيئة رموز مخزّنة على وسائل تخزين ممغنطة لا تقرأ إلاّ بواسطة الحاسب الآلي، و الوقوف على الدّليل الّذي يمكن فهمه بالقراءة و التواصل عن طريقه إلى الجاني يبدو أمر صعب لاسيما وأنّ الجاني يتعمّد إلى عدم ترك أثر لجريمته يسهّل محو الدّليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصّصة لذلك، إذ يتمّ عادة في لمح البصر وبمجرّد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسوب.

و) نقص الخبرة لدى الأجهزة الأمنيّة و القضائيّة وعدم كفاية القوانين الساريّة : تتميّز جرائم المعلوماتيّة بالكثير من السمات الّتي تختلف عن غيرها من الجرائم، الأمر الدي أدّى إلى تغيير شامل في آليّة التحقيق و طرق جمع الأدلّة المتّبعة من الجهات الّتي تقوم بعمليّة التحقيق، و إضافة أعباء تتعلّق بكيفيّة الكشف عن هذه الجريمة وأدلّتها، ونظرا لما تتطلب هذه الجرائم من تقنيّة لارتكابها فهي تتطلب لاكتشافها و البحث عنها، وتستلزم اسلوب خاص في التحقيق و التعامل، الأمر الّذي لم يتحقّق في الجهات الأمنيّة و القضائيّة لدينا، نظرا لنقص المعارف التقنيّة و هو ما يتطلّب تخصص في التقنيّة لتحصين الجهاز الأمني و القضائي ضدّ هذه الظاهرة.

المطلب الثالث : موقف المشرّع الجزائري من الجريمة المعلوماتيّة

لم يجد المشرّع الجزائري حلا الا تعديل قانون العقوبات لسد ما كان من فراغ قانوني في هذا المجال وكان ذلك بموجب القانــون رقم 15/04 المؤرّخ في 2004/11/10 المتمّـم و المعدّل للأمر 156/66 المتضمّن قانـون العقوبـات[1] و الّذي أقرّ له القسم السابع مكرّر تحت عنوان : المساس بأنظمة المعالجة الآليّة ولقد جاء في عرض أسباب هذا التعديل أنّ التقدّم التكنولوجي وانتشار وسائل الاتصال الحديثة أدّى إلى بروز أشكال جديدة للإجرام، ممّا دفع بالكثير من الدول إلى النّص على معاقبتها وأنّ الجزائر على غرار هذه الدّول تسعى من خلال هذا المشروع إلى توفير حماية جزائيّة للأنظمة المعلوماتيّة و أساليب المعالجة الإليّة للمعطيات وأنّ هذه التعديلات من شأنها سدّ الفراغ القانوني.

وقد قدّر المشرّع في تدخّله هذا أنّ جوهر المعلوماتيّة هو المعطيات الّتي تدخل إلى الحاسب الآلي فتحوّل إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدّة لذلك فقد آثر المشرّع الجزائري استخدامه لمصطلح المساس بنظم المعالجة للمعطيات، وينصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات و النظام الّذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج بذلك من نطاق تجريم تلك الجرائم الّتي يكون النظام المعلوماتي وسيلة لارتكابها، وحصرها فقط في صور الأفعال الّتي تشكّل اعتداء على النّظام المعلوماتي، أي الجرائم الّتي يكون النظام المعلوماتي محلاّ لها ثمّ في مرحلة لاحقة اختار المشرّع الجزائري للتعبير عن الجريمة المعلوماتيّة مصطلح الجرائم المتّصلة بتكنولوجيا الإعلام و الاتصال بموجب القانون رقم 04/09 [2] المتضمّن الوقاية من هذه الجرائم و مكافحتها.

(1) قانـون العقوبات الجزائري.

(2) القانون رقم 04/09 المتضمّن الوقاية من هذه الجرائم و مكافحتها

أ) مفهوم نظام المعالجة الآليّة للمعطيات : تبنّى المشرّع الجزائري للدلالة على الجريمة المعلوماتية مصطلح المساس بأنظمة الآليّة للمعطيات معتبرا أنّ النظام المعلوماتي في حدّ ذاته أي المحتوى وما يحتويه من مكونات غبر مادية محلا للجريمة المعلوماتيّة، فالمقصود بنظام المعالجة الآليّة للمعطيات هي عمليّة معالجة المعطيات تحتاج إلى آلية منظمة تتولّى عمليات جمع و توفير المعلومات اللازمة ومعالجتها، وهو الأمر الّذي ولّد الحاجة إلى إجراءات ووسائل تساعد على القيام بذلك فظهر بالنتيجة مصطلح نظم المعلومات المبنيّة على الحسابات الآليّة أو ما يسمّى بنظام المعلومات المحسوبة وهو نظام يعتمد على المكوّنات و الأجهزة البرمجيّة للحاسوب في معالجة المعطيات واسترجاع المعلومات.

فالمشرّع الجزائري عند تعديله لقانون العقوبات وإضافته للقسم السابع مكرّر بعنوان المساس بأنظمة المعالجة الآليّة للمعطيات عارضا من خلاله صور هذه الاعتداءات لم يعرض نظام المعالجة الآليّة للمعطيات، ذلك أنّ العناصر الّتي يتكوّن منها هذا النظام في حالة تطوّر تكنولوجي مستمر يخضع للتطوّرات السريعة و المتلاحقة الّتي تطرأ على البيئة التقنيّة الّتي يمثّلها و الّتي تتسع لإمكانية شمول وسائل تقنيّة جديدة، لا سيما وأنّ العالم الافتراضي لا يزال في بدايته ولن يكون من السهولة احتواؤه، و من جهة أخرى فإنّ نظام المعالجة الآليّة للمعطيات يعدّ تعبيرا فنيّا يصعب على المشتغل بالقانون ادراك طبيعته.

وبالرّغم من ذلك فقد ذهب بعض الدّول إلى وضع تعريف للنظام المعلوماتي في قوانينها الدخيلة ذات صلة، كالقانون الأمريكي الموحّد للمعاملات الإلكترونيّة لسنة 1999، قانون مكافحة جرائم المعلوماتيّة السعودي الصادر بتاريخ 2007/03/26 [1]، قانون سلطنة عمان رقم 2006/69 [2] الخاص بالمعاملات الإلكترونيّة الصادر بتاريخ 2008/05/17.

(1) عرف نظام مكافحة الجرائم المعلوماتيّة للمملكة العربية السعوديّة الصادر بتاريخ 2007/03/26 بأنّه مجموعة برامج و أدوات معدّة لمعالجة البيانات و إدارتها و تشمل الحاسبات الآليّة.

(2) المادّة الأولى من هذا القانون عرفت النظام المعلوماتي بأنّه نظام إلكتروني للتعامل مع المعلومات و البيانات.

أمّا على المستوى الدّولي فإنّ الاتفاقية الدّوليّة لإجرام تقنيّة المعلومات وقفت عند حد هذا المفهوم عندما عرفت نظام المعالجة الآليّة للمعطيات بموجب الفقرة "أ" من المادّة الأولى من الفصل الأوّل بعنوان المصطلحات على أنّه كل آلة بمفردها أو غيرها من الآلات المتّصلة أو المرتبطة والّتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معيّن بأداة معالجة آليّة للبيانات.

فمن خلال التعريفات نستنتج أنّ مصطلح نظام المعالجة الآليّة يستخدم في الحقل القانوني للدلالة على المعنى المقصود نفسه بهذا المصطلح وفقا لمفهومه العلمي، فهو إذن مصطلح ينطبق على أي نظام مهما كان مسمّاه يتوفّر له عدّة عناصر مرتبطة ببعضها بعدد معيّن من الرّوابط لتحقيق المعالجة الآليّة للمعلومات من تجميعها و تخزينها ومعالجتها ونقلها وتبادلها وذلك من خلال برنامج معلوماتي.

ب) المقصود بالجرائم المتّصلة بتكنولوجيا الإعلام و الاتصال[1] : إنّه وقبل صدور القانون رقم 04/09 المؤرّخ في 2009/08/05 المتضمّن القواعد الخاصّة للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها كانت الجريمة المعلوماتيّة في النّظام العقابي الجزائري تقتصر فقط على تلك الأفعال الماسّة بأنظمة المعالجة الآليّة للمعطيات وهي وفقا لدلالة الكلمة تنصرف إلى المعلومات و النّظام الّذي يحتوي عليها بما في ذلك شبكة المعلومات و هذه الأفعال في الحقيقة ماهي إلا جزء من الظاهرة الإجراميّة لأجل هذا فقد تبنّى المشرّع الجزائري حديثا بموجب القانون 04/09 تعريفا موسّعا للجرائم المعلوماتيّة واعتبر أنّها تشمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآليّة للمعطيات المحدّدة في قانون العقوبات من 394 مكرّر إلى المادّة 394 مكرّر 07 أي جريمة اخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتيّة أو نظام للاتصالات الإلكترونيّ، وبذلك لم يعد مفهوم الجريمة المعلوماتيّة في التشريع الجزائري يقتصر على الأفعال الّتي تكون فيها المنظومة المعلوماتيّة محلا للاعتداء بل توسّع نطاقها لتشمل إضافة إلى ذلك تلك الأفعال الّتي تكوّن المنظومة المعلوماتيّة وسيلة لارتكابها.

(1) القانون رقم 04/09 المتضمّن القواعد الخاصّة بالوقاية من الجرائم المتّصلة بتكنولوجيا الإتصال و الإعلام.

المبحث الثاني : الطبيعة القانونيّة للجريمة المعلوماتيّة.

تعتبر أركان الجريمة المعلوماتيّة جزء لا يتجزّأ عن طبيعتها و تخلّف أحدها يؤدّي إلى انتفاء الجريمة، حيث يتطلّب القانون كأصل عام وجود ركن مادّي و ركن معنوي وركن شرعي بموجبه يتمّ التجريم و العقاب و هو الأمر المعمول به في كلّ الجرائم التقليديّة كانت أو مستحدثة، فبرغم من أنّ في الجرائم التقليديّة هناك رأي يلغي الرّكن الشّرعي و اكتفائه بالركن المادي و المعنوي بحجة ان الركن الشرعي هو الّذي يحدّد هذه الأركان غير أنّ في الجريمة المرتكبة عبر الأنترنت يجب أن تتوفّر فيها و الاعتماد على الأركان الثلاثة لتحديد الجريمة.

المطلب الأوّل : أركان الجريمة المعلوماتيّة.

تتخذ الجريمة المعلوماتيّة عبر الأنترنت من الفضاء الافتراضي مسرحا لها، ممّا يجعلها تتميّز بخصوصيات تنفرد بها، إلاّ أنّ ذلك لا يعني عدم وجود تشابه له مع الجريمة المرتكبة في العالم التقليدي أو المادّي فهي تشترك بوجود الفعل غير المشروع [1]، ومجرم يقوم بهذا الفعل، ومن خلال هذا التشابه سوف نتطرّق إلى تبيان الأركان الّتي تقوم عليها هذه الجريمة حيث نبيّن المقارنة بينهما و بين الجريمة التقليديّة، وبالتالي نعمد إلى تبيان مدى انطباق مبدأ المشروعيّة على الجريمة المرتكبة ثمّ نوضّح الرّكن المادّي وننتهي إلى تحديد الركن المعنوي.

(1) فايز بن عبد الله الشهري : "التحدّيات الأمنية المصاحبة لوسائل الاتصال الحديثة " دراسته وصفيّة تأصيليّة للظاهرة الإجراميّة على شبكة الأنترنت دار الفكر الجامعي / الطبعة الثانيّة 2011، ص 10.

أ) الرّكن الشرعي : يقصد بالركن الشرعي للجريمة وجود نص يجرّم الفعل و يوضّح العقاب المترتّب عليه وقت وقوع هذا الفعل، فمبدأ الشرعيّة الجنائيّة يمنع المساءلة الجنائيّة ما لم يتوفّر النّص القانوني، فلا جريمة ولا عقوبة إلاّ بنص، ومتى ما انتفى النّص عل التجريم مثل هذه الأفعال الّتي تطالها النصوص القائمة امتنعت المسؤوليّة وتحقيق القصور في مكافحة كهده الجرائم [1].

أوّلاً – مدى انطباق النّصوص القائمة على الجرائم المعلوماتيّة : تشعّب الإشكالات النّاجمة عن استخدام الحواسيب الآليّة وشبكاتها جعل مهمّة القضاء صعبة نظرا لعدم وجود نصوص كفيلة بمعالجة هذه الإشكاليّة و الّتي من بينها الاستخدام غير المشروع.

حاولت قوانين العقوبات مواجهة تحدّيات الجرائم المرتكبة عبر الأنترنت بطرق تقليديّة كتلك المقرّرة في جرائم الأموال، إلاّ أنّه تبيّن قصور هذه الوسائل التقليديّة عن مواجهة العديد من الأفعال الّتي تهدّد مصالح اجتماعية والّتي ارتبطت بظهور وانتشار أجهزة الكمبيوتر.

تبيّن في بعض الأحوال أنّ ثمّة أفعال جديدة ترتبط باستعمال الكمبيوتر لا تكفي النصوص القائمة لمكافحتها، من ذلك الاعتداء على حرمة الحياة الخاصّة، هذا النّوع من الاعتداء لا يعاقب عليه قانون العقوبات إلاّ إذا كان مرتبطا بمكان خاص، أمّا تجميع معلومات عن الأفراد وتسجيلها في الكمبيوتر، فإنّه لا يخضع للتجريم وفقا للقواعد العامّة، كما أنّ التداخل في النظام نظام الحاسب الآلي.

(1) يونس عرب : قراءة في الاتجاهات التشريعيّة للجرائم الإلكترونيّة مع بيان موقف الدّول العربيّة وتجربة سلطنة عمان، عالم الكب الحديثة، ص 98.

وتغيّر البيانات، فهي صورة جديدة لا يعرفها قانون العقوبات قبل ظهور الكمبيوتر وشبكة الأنترنت، كلّ ذلك يأكد قصور القواعد التقليديّة في القانون الجنائي على مكافحة هذا النّوع الجديد من الجرائم[1].

لا يتطوّر القانون الجنائي بنفس السّرعة التي تتطوّر بها التكنولوجيا ولا بنفس المهارة الّتي يأتي بها الذّهن البشري لتسخير هذه المبتكرات لاستخدامه السّيء، لذلك وكاستنتاج أوّلي ومنطقي نعتقد أنّ القانون الجنائي لا يكتفي من حيث المبدأ في مواجهة هذا النّمط من الإجرام خاصّة أنّ النصوص قد وضعت للتطبيق وفق معايير معيّنة كانت سائدة أيّام وضعها[2].

ثانيا– الحاجة لتدخّل المشرّع لمواجهة جرائم الأنترنت : تعتبر الجريمة الواقعة من نتاج التطوّر التكنولوجي أنّها من المستحدثات الّتي عجزت مواد القوانين العقابية التقليدية مواجهتها، لذلك سعت معظم دول العالم و لا سيما المتقدمة قانونا الى سن التشريعات و القوانين لمواجهة هذه الجرائم.

تعتبر الولايات المتحدة الأمريكية من الدول السّباقة التي جسدت تشريع مستقل بشأن الجرائم الكمبيوتر بصفة عامة و جرائم الأنترنيت بصفة خاصة، كما تتميز الولايات المتحدة الأمريكية بوجود أكبر قدر من التشريعات تغطي جرائم الكمبيوتر و الأنترنيت و الاتصالات[3].

(1) يونس عرب :قراءة في الاتجاهات التشريعيّة للجرائم الإلكترونيّة مع بيان موقف الدّول العربيّة وتجربة سلطنة عمان.

(2) محمّد عبيد الكعبي : المرجع السّابق ص 58.

(3) يونس عرب :قراءة في الاتجاهات التشريعيّة للجرائم الإلكترونيّة.

وضعت الولايات المتحدة الأمريكية قانونـا خاصا بحماية الحاسوب و الشبكات المحوسبة، و ذلك عام 1976، و في عام 1985 حدد معهد العدالة القومي فيها خمسة أنواع رئيسية من الجرائم و هي:

1- جرائم الحاسوب الداخلية.

2- جرائم الاستخدام غير المشروع عن بعد، شبكات المعلومات المحوسبة.

3- جرائم التلاعب بالحاسوب، أي التلاعب غير المخول و غير المشروع.

4- دعم التعاملات الإجرامية للنظم و الشبكات المحوسبة، و إسنادها من قبل الأخرين.

5- سرقة البرامج الجاهزة و المكونات المادية.

صدر في عام 1986 قانون آخر يعرف فيه جميـــع المصطلحات الضروريـة لتطبيق جرائم النظـم المعلوماتيـة و الشبكات المحوسبة، و على أثر ذلك قامت الولايات المتحدة الأمريكية الدّاخلية بدورها بإصدار تشريعاتها الخاصّة بها للتعامل مع هذه الجرائم، و التي تتماشى مع التشريعات الاتحادية[1].

قام المشرع الفرنسي كذلك بسن تشريع خاص فيها يخص الإجرام المعلوماتي و ذلك في أوت سنة 1986، حيث تقدّم النّائب "جاك جود فران" باقتراح قانون تمّ اعتماده من البرلمان الفرنسي وصدر في 5 يناير 1988 برقم 19 تحت عنوان "الجرائم في المواد المعلوماتيّة" وتمّ ادماجه في الفصل الثاني من قانون العقوبات وخصّصت له المواد من 2/432 إلى 9/462.

(1) أحمد بن محمّد اليماني : الحماية الجنائيّة للبريد الإلكترونيّ.

الجدير بالذّكر أنّ الفصل المخصّص لهذه الجرائم ألحق بالباب المخصّص بالجنايات و الجنح ضدّ الأشخاص، أي بعد الفصل الثاني من الجرائم المخصّصة بالجنايات و الجنح ضدّ الملكيّة، وقد ركّزت اللّجنة التشريعيّة على الهدف الّذي توخاه اقتراح "جود فران" حماية النّظام المعلوماتي ضدّ أي اعتداء خارجي، فأقرت أنّ الهدف من النّصوص الجديدة تجريم و ردع الدّخول غير المشروع على البرامج المعلوماتيّة [1].

ثالثا– التوسّع في تفسير النصوص القائمة لتطبيقها على الجرائم : ليس أمام الدّول الّتي لم تسن بعد قوانين خاصّة لتجريم مختلف الجرائم النّاشئة عن الاستخدام غير المشروع لشبكة الأنترنت سوى تطبيق القوانين الجنائيّة القائمة بموادها التقليديّة على هذه الوقائع خوفا من إفلات الجناة من قبضة العدالة، وذلك مع بعض التفسير الموسّع لهذه النّصوص[2].

فعلى الرّغم من القصور التشريعي قد أصبح واقعا ملموسا، إلاّ أنّ هذا لا يحول دون الاجتهاد في تفسير النصوص العقابيّة التقليديّة الّتي تعاقب على صور الاعتداءات المختلفة على الأموال، بحيث يمكن تطبيقها على الجرائم المستحدثة الّتي أوجدتها ثورة الاتصالات عن بعد, فلا محالة أنّ التطور قد يوسع من دائرة المجالات الّتي تحميها نصوص التجريم و العقاب بحيث يمكن أن ندخل في إطارها عناصر أخرى لطالما أمكن اعتبارها من جنسها و أن المشرع يحميها بذات هذه النصوص، و يكون اتخاذ سبيل التفسير الموسع للنصوص التقليدية من أجل تطبيقها على الجرائم المرتكبة عبر الأنترنت، بمنع السلطات القضائية حرية تفسير هذه النصوص حيث أن القاضي يمكنه أن يعطي تفسيرا أكثر مرونة للنصوص القانونية يسمح من وضع هذه الجرائم تحت طائلة التجريم و المتابعة و ذلك في ظل السلطة التقديرية الّتي يتمتع بها القاضي.

(1) أحمد خليفة الملط : الجرائم المعلوماتيّة، دار الفكر الجامعي الإسكندرية، الطبعة الثانيّة، 2006.

(2) محمّد عبيد الكعبي : المرجع السابق، ص 32.

ب) الرّكن المادي : ينطبق مبدأ تحديد الفعل غير المشروع و إعطائه ضدّ الجريمة بتحديد الرّكن المادّي فيه، فلا جريمة دون الركن المادّي، الّذي يتمثل في السلوك الّذي يقوم به الجاني، من أجل تحقيق غاية ما يحدّد له القانون العقاب اللاّزم، وهو تبيان الجرائم المرتكبة من قبل الجاني، شريطة أن يكون له مظهر خارجي ملموس، غير أنّ تحديد الرّكن المادّي في الجرائم الواقعة عبر الشبكة العالميّة للأنترنت تواجهه العديد من الصعوبات خاصّة فيما يتعلّق بتحديد النتيجة الإجراميّة والرّبطة السببية وهي كالتالي :

أوّلاً – القواعد العامّة في الرّكن المادّي للجريمة :

1 – السلوك الإجرامي : يعدّ السلوك الإجرامي أهمّ عناصر الرّكن المادّي لأي جريمة، لأنّه يكشف عن سلوك مخالف لإرادة المشرّع، ويبدو بمظاهر مادّية ملموسة في العالم الخارجي ويعني ذلك أنّ الأفكار داخل النّفس لا عقاب عليه، ويعرف السلوك الإجرامي في الجرائم التقليديّة على أنّه فعل الجاني الّذي يحدث آثر في العالم الخارجي، وبغيّر هذا السلوك لا يمكن محاسبة الشخص مهما بلغت خطورة أفكاره، و السلوك هو الّذي يخرج النّيّة و التفكير في الإجرام إلى حيّز الوجود واعتبار القانون ولا يكاد يفرّق بين السلوك الإيجابي (الفعل) و السلوك السلبي (الامتناع عن الفعل) مادام أنّ لهما نفس النتيجة.

أ – السلوك الإيجابي : يكون في صورة فعل أو قول يجرّمه القانون يصدر عن الجاني ويؤدّي إلى إحداث نتيجة في الجرائم ذات النتيجة وكذلك يعتبر سلوك إجرامي في ذاته في الجرائم الشكليّة

ب – السلوك السلبي : يتمثّل هذا الفعل بسلوك أو موقف يتّخذه المكلّف بقاعدة قانونيّة تفرض عليه أن يعمل فلا يعمل، ففي هذه الحالة يقوم المكلّف بالحيلولة دون جسمه كلّه أو بعضه أو يتحرّك باتّجاه مضاد لما أمره به و عليه فلا يجوز للقاضي أن يمتنع عن الحكم بالدّعوى ولا للشاهد أن يمتنع عن الإدلاء بشهادة أمام المحكمة بواقعة يعلمها ولا للموظف أن يمتنع عن أداء مهام وظيفته [1].

ثانياً – النتيجة الإجراميّة :

يقصد بالنتيجة الإجراميّة الأثر المادّي الّذي يحدث في العالم الخارجي، كأثر للسلوك الإجرامي، فالسلوك قد أحدث تغييرًا حسّيا ملموسا ومفهوم النتيجة كعنصر في الرّكن المادّي يقوم على أساس ما يعتد به المشرّع وتترتّب عليه النتائج.

ثالثاً – الرّبطة السببيّة :

يقصد بالرّابطة السببيّة هي الصّلة الّتي تربط بين الفعل و النتيجة وتثبت أنّ ارتكاب الفعل هو الّذي أدّى إلى حدوث النتيجة وأهمّيّة رابطة السببيّة ترجع إلى أنّ إسناد النتيجة إلى الفعل هو شرط أساسي لتقرير مسؤوليّة الفعل عن النتيجة، وتحقيق رابطة سببيّة تلازما مادّيا بين الفعل و النتيجة يؤدّي إلى وقوف مسؤوليّة الجاني عند حدّ الشروع، إذ لا يعدّ مسؤولا عن النتيجة الّتي تحقّقت، أمّا إذا كانت الجريمة غير عمديّة فإنّ نفي الرّابطة السببيّة يؤدّي إلى اختفاء المسؤوليّة كلّيا عنها.

رابعاً – تحديد الرّكن المادّي في الجريمة المرتكبة عبر الأنترنت :

تحديد الرّكن المادّي في هذه الجرائم يثير جملة من الصعوبات الّتي تفرضها طبيعة الوسط الّذي تمّ فيه الجريمة مثل الجانب التقني، وهذا ما يميّز ركنها المادّي، الّذي يجب أن يتمّ باستخدام أجهزة الحاسوب أو الشبكة العالميّة للأنترنت.

(1) عبد الله سليمان : شرح قانون العقوبات الجزائري، القسم العام، ديوان المطبوعات الجامعية الجزائر: 1995 ص148.

ج) الرّكن المعنوي : يعتبر الرّكن المعنوي هو الحالة النفسيّة للجاني و العلاقة الّتي ترتبط بين مادّيات الجريمة وشخصية الجاني و يطلق عليه الرّكن الأدبي أو الشّخصي وهو يعني في الحقيقة الجاني أو المجرم تحديدا، فالرّكن المعنوي هو المسلك الذّهني أو النّفسي للجانب باعتباره محور القانون الجنائي، فهل المقوّمات الّتي تحكم الرّكن المعنوي في الجرائم التقليديّة هي نفسها في الجرائم المرتكبة عبر الأنترنت؟.

أوّلاً – الرّكن المعنوي في نطاق الجريمة التقليديّة : ويتمثّل الرّكن المعنوي في ظلّ التقليديّة في :

1 – عناصر القصد الجنائي :

أ – العلم : لا يتحقّق القصد الجنائي إلاّ إذا كان الجاني يعلم بالعناصر الأساسيّة لقيام الجريمة سواء تعلّق بسلوكه الإجرامي أم بمضوع الاعتداء، فإذا كان الجاني جاهلا بشيء من ذلك فلا يتحقّق القصد الجنائي.

ب – الإرادة : الإرادة هي كلّ نشاط نفسي يهدف إلى تحقيق غرض معيّن فإذا كان غرض الجاني تحقيق نتيجة إجراميّة كانت الإرادة المتّجهة إلى الفعل المنطوي على إحداث النتيجة هي "القصد الجنائي" و الغرض هو الهدف القريب الّذي تتجه إليه الإرادة، أمّا الباعث فهو عبارة عن الدّافع إلى إشباع حاجة معيّنة وهذا الدّافع له طبيعة نفسيّة بخلاف الغاية الّتي لها طبيعة موضوعيّة.

2 – صور القصد الجنائي :

أ – القصد الجنائي العام : يهدف الجاني عند ارتكابه الواقعة الإجراميّة مع العلم بعناصرها إلى تحقيق غرض معيّن، بتحقيقه قد تتمّ الجريمة ويتوفّر لها القصد الجنائي العام، ففي جريمة القتل يكون غرض الجاني إزهاق روح المجني عليه، فالقصد العام أمرا ضروري.

ب – القصد الجنائي الخاص : يلتقي القصد الخاص مع القصد العام في جميع عناصره، ويزيد عنه في تحديد الإرادة الإجراميّة لدى الجاني.

ثانيا – تحديد الرّكن المعنوي في الجريمة المرتكبة عبر الأنترنت :

يكتسي تحديد الرّكن المعنوي بالغ الأهمّية في الجريمة المرتكبة في العالم المادّي، حيث بموجبه يمكن تحديد مناط مسائلة الجاني، وذلك بتحديد القصد الجنائي لديه، الّذي بدونه لا يمكن أن يعاقب الشّخص المرتكب للفعل.

يتلاقى القصد الجنائي بصورتيه العام و الخاص في الجرائم المرتكبة عبر الأنترنت مع مثيله في الجرائم التقليديّة في عدّة نقاط منها، العلم و الإرادة، فالمجرم يجب أن يكون عالما بأنّ الفعل الّذي يقوم به يعتبر غير مشروع وذلك بإرادة صريحة من أجل إحداث الضرر للمجني عليه أمّا القصد الخاص فيلتقي مع القصد العام في الكثير من عناصره ويزيد عنه في تحديد الإرادة الإجراميّة لدى الجاني.

يقوم الرّكن المعنوي للجريمة عبر الأنترنت على أساس مجسّد في توافر الإرادة الآثمة لدى الفاعل وتتوجّه هذه الإرادة إلى القيام بعمل غير مشروع، كانتحال شخصيّة أو سرقة البطاقات الائتمانية، كما يجب أن تتوفّر نتيجة الجريمة المترتبة عل الأفعال السّابقة لكي تكتسّب صفة الجاني الصّفة الجرميّة.

المطلب الثاني : أطراف الجريمة المعلوماتيّة.

لقد أضافت المعلوماتيّة الكثير من الجوانب الإيجابيّة إلى حياتنا، إلاّ أنّها في المقابل جلبت معها شكلا جديدا من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتيّة، فلم يكن لارتباط الجريمة المعلوماتيّة بالحاسب الآلي أثره على تميّز هذه الجريمة عن غيرها من الجرائم التقليديّة فحسب، بل كان له أثره أيضا على تميّز المجرم المعلوماتي عن غيره من المجرمين التقليديين.

فمظاهر الخطورة الّتي تتجلّى بها الجريمة المعلوماتيّة أنّ مرتكبيها يتّسمون بالذّكاء و الدّراية في التعامل في مجال المعالجة الآليّة للمعطيات و الإلمام بالمهارات و المعارف التقنيّة، وإذا كان الشّخص الّذي يرتكب الفعل غير المشروع ويتعدّى فيه على حقّ من حقوق الغير بالمعنى الواسع يعدّ في نظم القانون مجرم ويتعرّض للعقاب، وعلى هذا الأساس يجب أن نتطرّق إلى صفت وسمات المجرم المعلوماتي وكذا أصنافه وأنماطه.

*** خصائص المجرم المعلوماتي :**

يتميّز المجرم المعلوماتي عن غيره من المجرمين بصفات وسمات معيّنة جعلت منه محل العديد من الأبحاث و الدراسات حيث اختلف الباحثون في تحديد هذه الخصائص كما اختلفوا في كيفيّة وصف جرائم ذوي الباقات البيضاء [1] على مجرمي المعلوماتيّة ذلك أنّ كلاّ من هؤلاء المجرمين قد يكون من ذوي الكفاءات فالسّمات الّتي يتميّز بها المجرم المعلوماتي هي كالتالي :

أ – الذكاء : يعتبر الذّكاء من أهمّ صفات مرتكب الجريمة المعلوماتيّة لأنّه يتطلّب المعرفة التقنيّة وكيفيّة الدّخول إلى أنظمة الحاسب الآلي و القدرة على التعديل وتغيير في البرامج وهذا ما يميزه عن المجرم التقليدي الّذي يميل إلى العنف [2]، فتجلّى أهمّية صفة الذّكاء بالنّسبة لمرتكب الجريمة المعلوماتيّة في عدم استخدام العنف، فالسّلوك الإجرامي ينشأ من تقنيّات التدمير النّاعمة.

ب – المهارة : تعدّ المهارة من أبرز خصائص المجرم المعلوماتي و الّتي قد يكتسبها عن طريق الخبرة المكتسبة في مجال التكنولوجيا المعلومات، كما أنّ المهارة الّتي يتميّز بها المجرم المعلوماتي تمكّنه من تكوين تصوّر كامل للجريمة، إذ يستطيع أن يطبّق جريمته على أنظمة مماثلة كتلك الّتي يستهدفها وذلك قبل تنفيذ جريمته فعادة ما يلجأ المجرم المعلوماتي الى التمهيد لارتكاب جريمته بالتّعرّف على المحيط الّذي تدور فيه وكذا الظروف الّتي تحيط بالجريمة المراد تنفيذها.

ج – التنظيم و التخطيط : تتميّز الجريمة المعلوماتيّة عادة بوجود أكثر من فاعل للنشاط الإجرامي الواحد، إذ ترتكب أغلب الجرائم المعلوماتيّة من عدّة أشخاص يحدّد لكلّ شخص منهم دور معيّن ويتمّ العمل بينهم وفقا لتخطيط و تنظيم مسبق قبل الشروع في ارتكاب الجريمة لأنّ الجريمة تحتاج إلى نسخ برامج الحاسب الآلي مثلا إلى من يقوم بنسخ تلك البرامج وإلى من يقوم بعمليّة بيعها.

---

(1) مصطلح المجرمين ذوي الباقات البيضاء مصطلح أطلقه علم الاجتماع "SUTHER Lanc" أين وضع أنّ هذه الجريمة ترتكب من قبل الطبقة الرّاقية.

2) غنّام محمد غنّام:الحماية الجنائيّة لبطاقات الائتمان مؤتمر الجوانب القانونيّة والأمنيّة للعمليّات الإلكترونيّة دبي2003 ص5

د – المجرم المعلوماتي يبرّر أركان جريمته : أثبتت بعض الدّراسات أنّه لا يوجد شعور لدى المجرم المعلوماتي بعدم أخلاقيّة ما يقوم به أو لمساسه بمصالح أو لقيم يحرص المجتمع على حمايتها بل لا يعتبر ما يقوم به يدخل في عداد الجرائم، خاصّة في الحالات الّتي يقف فيها السّلوك عند حدّ قهر نظام الحاسوب وتخطّي الحماية المفروضة حوله لذلك فإنّ كثيرا من العاملين في مجال المعلوماتيّة لا يجدون أيّ خطأ في استعمال الشفرات السّريّة الخاصّة بالدّخول إلى أنظمة الحسابات الآليّة بطريقة غير مشروعة.

* **أصناف المجرم المعلوماتي** : من خلال الخصائص التي تطرّقنا إليها يمكن أن نضع تصنيف لمجرمي المعلوماتيّة وهكذا يمكن تصنيف مرتكبي الجرائم المعلوماتيّة إلى مجموعة الطوائف أي أنّه كلّ مجرم يمكن إدراجه ضمن طائفة محدّدة دون غيرها :

أ – فئة صغار مجرمي المعلوماتيّة : أو كما يسمّهم البعض بنوابغ المعلوماتيّة لكن نلاحظ في هذه الفئة من الأشخاص الّذين يرتكبون جرائم المعلوماتيّة بغرض التّسلية دون أن تكون لهم نيّة إحداث الضرر بالمجني عليهم، وهم غالبا ما يكون في مرحلة المراهقة و على الرّغم من صغر سنّهم إلاّ أنّهم قادرون على اقتحام كافة أنواع الأنظمة المعلوماتيّة.

ب – فئة القراصنة أو المحترفون : والّتي يمكن تقسيمهم إلى قسمين :

1 – الهاكر (les Hackers) [1] : وهم متطفّلـون الّذين يتحدّون أمن النّظم المعلوماتيّـــة و الشبكات من خلال الدّخول إلى أنظمة الحسابات الآليّة غير المصرّح لهم بالدّخول إليها، وفي الغالب لا تكون لهم دوافع تخريبيّة لكن من باب اكتساب الخبرة أو بدافع الفضول.

2 – الكراكر(les Crackers) : وهم الأشخاص الّذين يقومون بالتسلّل إلى أنظمة المعالجة الآليّة للاطلاع على المعلومات المخزّنة بها لإلحاق الضّرر أو سرقتها وذلك بهدف التّحدّي الإبداعي [2] حيث تتميّز هذه الفئة بحدّة الإدراك و المهارة التّقنيّة.

3 – فئة المحترفين : وتعتبر هذه الفئة هي الأخطر، لأنّها تهدف بالأساس إلى تحقيق الكسب المادّي، حيث تعتبر الأضرار الّتي تترتّب عن هذه الأفعال تكون بالغة الضرر بعكس الفئات الأخرى، كما يتمتّعون بكفاءات عاليّة في مجال المعلوماتيّة

4 – فئة الحاذقين : الهدف من هذه الفئة هو الانتقام كأثر لتصرّف صاحب العمل معهم أو تعبيرا منهم على غضبهم من هيئة معيّنة.

(1) عرفت اتفاقية الأمم المتّحدة لمكافحة إساءة استعمال تكنولوجيا المعلوماتيّة لغرض إجرامي رقم (55/63) المؤرّخة في 2000/04/12.

(2) مصطفى محمّد موسى : التحقيق في الجرائم الإلكترونيّة مطابع الشّرطة ط1 ص 15.

المطلب الثالث : أساليب ودوافع ارتكاب الجريمة المعلوماتيّة.

إنّه على خلاف الجرائم التقليديّة الّتي تتطلّب بطبيعتها نوعا من المجهود العضلي و العنف و الّذي يتّخذ شكل الإيذاء كما هو مثلا في جريمة القتل فإنّ الجريمة المعلوماتيّة على خلاف ذلك فإنّها من الجرائم الهادئة التي لا تتطلّب سوى عدد من لمسات على أجهزة الحاسوب حتّى تؤدّي إلى اختراق أكبر نظم المعالجة الآليّة وهتك سرّيتها أو محو ما تحتويه من معلومات إذ يجب أن تتوفّر على مرتكبها إلى القدرة و الدّراية في التعامل مع نظم المعالجة و الإلمام بالمهارات و المعارف التقنيّة ولهذا نجد أنّ المجرم المعلوماتي له أساليب و دوافع في ارتكاب الجريمة المعلوماتيّة.

* **أساليب ارتكاب الجريمة المعلوماتيّة** : تتشابه جرائم المعلوماتيّة مع الجرائم التقليديّة من حيث استخدام المجرم لوسائل وأساليب غير مشروعة و غير قانونيّة في سبيل ارتكابه للجريمة، غير أنّ الجرائم المعلوماتيّة تتميّز في ارتكابها من طرف مجرمين يستعملون كلّ ما من شأنه خداع الحاسب الآلي و التحايل على أنظمته المعلوماتيّة وتقنياته لتنفيذ جرائمهم وتمثل فيما يلي :

أ – الاختراق "Hacking" : تقوم معظم جرائم المعلوماتيّة على تقنيّة الاختراق وذلك بغرض الدّخول غير المشروع لأنظمة المعالجة الآليّة للمعطيات، فالاختراق بشكل عام هو القدرة على الوصول لهدف معيّن بطريقة غير مشروعة عن طريق ثغرات ويكون قد تم التسلّل إلى جهاز الضّحيّة دون علمه إلى مجموعة من الأدوات و الوسائل، فيقوم المخترق بالبحث عن الضّحيّة من خلال معرفة رقم (IP) [1] الخاص به، ويتمّ البحث عن هذا الرّقم بمجموعة من الخطوات يقوم بها المخترق على جهازه الّذي يشترط أن يكون متّصلا بجهاز الضّحيّة عبر شبكة الأنترنت.

(1) (IP) يتطلّب تشغيل نظم الاتّصالات الكمبيوترية هو أن تكون هناك آليّة من أجل عنونة الأجهزة سواء المرسلة أو المستقبلة.

كما يوجد أسلوب آخر للاختراق وهو انتحال شخصيّة الموقع ويعتبر هذا الأسلوب حديثا نسبيا في مجال الجرائم المعلوماتيّة ويقوم هذا الأسلوب على قيام المخترق بوضع نفسه في موقع بيني بين برامج المستعرض للحاسب الخاص بأحد مستخدمي الأنترنت وبين الموقع (WEB) ومن هذا البيني يستطيع المجرم المعلوماتي من خلال جهاز حاسوبه مراقبة أي معلومة متبادلة بين الضّحيّة الّذي يزور الموقع وبين الموقع نفسه.

ب – البرامج الخبيثة "Les Virus" : تعدّ الفيروسات بمثابة المرض الّذي يصيب المعطيات وتتمتّع الفيروسات بقدرة فائقة على مهاجمة أجهزة الحاسوب والشبكات المعلوماتيّة وتعطّل الاتصالات وتشويه البيانات ويستخدم الفيروس بشكل عام لتحقيق أحد الغرضين سواء الغرض الحمائي أو الغرض التخريبي.

فالغرض الحمائي يكون من أجل حماية النسخ الأصليّة من خطر النسخ غير المرخّص به فينشط الفيروس بمجرّد النسخ ويدمّر نظام الحاسوب.

أمّا الغرض التخريبي ويتم اعداد هذه الفيروسات من طرف خبراء البرامج بهدف التخريب بحدّ ذاته أو بهدف الحصول على منافع شخصيّة.

* **دوافع ارتكاب الجريمة المعلوماتيّة** : يعتبر الدّافع هو العامل المحرّك للإرادة الّتي توجّه السلوك الإجرامي، فيمكن حصر هذه الدّوافع إلى نوعين دوافع شخصيّة وأخرى خارجيّة :

أ – الدوافع الشخصيّة : يمكن رد الدوافع الشخصيّة لدى المجرم المعلوماتي إلى دوافع مادّية وأخرى ذهنيّة ، فالدوافع المـادّية من أكثر الدّوافع الّتي تحرّك الجـاني لاقتراف الجريمـة المعلومـاتيّة، فيعمد الجـاني رغبة منه في تحقيق الثـراء و الكسب المادّي إلى التلاعب بأنظمة المعالجة الآليّة للبنوك و المؤسّسات الماليّة أو اختراق نظم المعالجة الآليّة لها من خلال اكتشافه لفجواتها الأمنيّة، أمّا الدّافع الذّهني هو مجرّد شغف بالإلكترونيات والرّغبة في تحدّي وقهر النّظام.

ب – الدوافع الخارجيّة : قد يتأثّر المجرم المعلوماتي ببعض المواقف قد تكون دافعة له على اقتراف الإجرام المعلوماتي ولا يسعى في ذلك حينها لا للمتعة ولا لكسب المال و الّتي نحصرها في ما يلي :

– دوافع الانتقام وهي من أخطر الدوافع فمثلا إذا كان هناك مشاكل بين موظّف ورب العمل لأسباب تتعلّق بالحياة المهنيّة يولّد لدى المجرم المعلوماتي الانتقام من رب العمل.

– أمّا دّافع التعاون و التواطىء فهو نوع كثير التكرار في الجرائم المعلوماتيّة وغالبا ما يقوم متخصّص في الأنظمة المعلوماتيّة بالجانب الفنّي من المشروع الإجرامي والآخر من المحيط أو خارج المؤسّسة المجني عليها فيقوم بتغطية عمليات التلاعب وتحويل المكاسب المادّية وعادة ما يمارسون التلصص على الأنظمة.

الفصل الثّانـــي

الفصل الثّاني : الجوانب القانونيّة للتحقيق في الجريمة المعلوماتيّة.

إنّ طبيعة الجرائم المعلوماتيّة بعناصرها ووسائل ارتكابها قد تدفع المشرّع الجزائي إلى أن يعيد النّظر في كثير من المسائل الإجرائيّة، خاصّة فيما يتعلّق بمسألة الإثبات باعتبارها أهمّ موضوعات هذا القانون، ذلك أنّ الدّليل الّذي يقوّي على إثبات هذا النّوع من الجرائم لابدّ أن يكون من ذات طبيعتها التقنيّة، وهو الأمر الّذي لا تكون فيه القواعد الإجرائيّة التقليديّة لاستخلاص الدّليل قادرة على القيام به، مما يستوجب تدخّل المشرّع لتكريس قواعد إجرائيّة يمكن للجهات المكلّفة بالبحث والتحرّي عن الجريمة المعلوماتيّة و الاعتماد عليها للوصول إلى الدّليل المناسب في إثبات الجريمة المعلوماتيّة.

ولاشكّ أنّ هذا الدّليل سيتمّ استخلاصه من البيئة الرّقميّة والّتي تعتبر مسرح الجريمة المعلوماتيّة ممّا يجعله يتميّز بخصائصها وهو الأمر الّذي يقودنا إلى الحديث عن مسألة قبول هذا الدّليل أمام القضاء ومدى تعبيره عن الحقيقة نظرا لما يمكن أن يخضع له من التنزيف و التحريف والأخطاء بل وحتّى مع ضمان مصداقية هذا الدّليل وكذا مشروعيته، فإنّ الأمر لا يتوقّف عند هذا الحد، بل يتجاوزه إلى مسألة أكبر أهمّية تتعلّق بمدى خضوع هذا الدّليل ذو الأصالة العلميّة للسلطة التقديريّة للقاضي الجزائي الّذي يشكل جوهر أي حكم.

المبحث الأوّل : التحقيق في الجريمة المعلوماتيّة.

إنّ التحقيق هو إجراء من أهم الإجراءات الّتي تتخذ بعد وقوع الجريمة، لما له من أهميّة في التثبيت من حقيقة وقوعها وإقامة الإسناد المادّي على مرتكبها بأدلّة الإثبات على اختلاف أنواعها، وهو كما يدلّ اسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتّهم من عدمه بعد جمع الأدلّة القائمة على الجريمة.

والثابت أنّ الدّعوى الجزائيّة تمرّ بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة، وتمرّ عمليّة التحقيق بمرحلتين أيضا : مرحلة التحقيق الأوّلي ومرحلة التحقيق الابتدائي، فالمرحلة الأولى هي مرحلة جمع الاستدلالات الّتي يباشرها أعضاء الضبط القضائي[1] و المرحلة الثانية تدخل في اختصاص قاضي التحقيق. وإنّنا نؤيّد الرّأي أو الاتجاه الّذي يقسّم التحقيق إلى :

- تحقيق أوّلي والّذي يناط به رجال الضبطيّة القضائيّة.
- تحقيق قضائي ويناط به رجال القضاء وهذا الأخير ينقسم إلى تحقيق ابتدائي من اختصاص قاضي التحقيق وتحقيق نهائي يكون في مرحلة المحاكمة من طرف قضاة المحاكم وفي جميع أنواع التحقيق هذه يكون للقائمين عليه من ضبطيّة قضائيّة وقضاة صلاحيّة ممارسة إجراءات البحث و التحرّي المحدّدة وفقا لقانون الإجراءات الجزائيّة، وهو الأمر الّذي يفهم صراحة من خلال استقراء نص المادّة 12 و 38 من قانون الإجراءات الجزائيّة الواردتين في الباب الأوّل من هذا القانون تحت عنوان "في البحث و التحرّي عن الجرائم" حيث تنصّ المادّة 12 من الفقرة الثّالثة أنّه "يناط بالضبط القضائي مهمّة البحث و التحرّي عن الجرائم المقرّرة في قانون العقوبات".

(1) حسب المادّة 15 من قانون الإجراءات الجزائيّة "يتمتّع بصفة ضابط الشرطة".

وتنصّ في نفس الوقت المادّة 38 من نفس القانون أنّه "يناط بقاضي التحقيق إجراءات البحث والتّحرّي" وعليه فإنّه يمكن القول أنّ إجراءات البحث و التّحرّي عن الجرائم هي من صلاحيات جهات التحقيق سواء كان أوّليا أم ابتدائيا، وبهذا المفهوم فإنّ إجراءات البحث و التّحرّي الّتي يباشرها رجال الضبط القضائي تصبّ في إطار التحقيق الأوّلي، بينما هذه الإجراءات عندما يباشرها قاضي التحقيق تعتبر تحقيقا ابتدائيا.

وإذا كان التّحقيق عموما يعتمد على ذكاء المحقّق وفطنته وقوّة ملاحظته وأن يحاول بكل الجهد أن يقوم بالتحقيق في الجريمة ومتابعتها و البحث عن الأدلّة وصولا لإظهار الحقيقة، فإنّ التحقيق في البيئة الإلكترونيّة يستوجب بالإضافة إلى كلّ هذا تطويرا لأساليبه وتكليف جهات مختصّة لممارسته من أجل مواكبة حركة الجريمة وتطوّر أساليب ارتكابها في هذه البيئة.

المطلب الأوّل : الأجهزة المكلّفة بالبحث والتحرّي عن الجريمة المعلوماتيّة

لقد كان للتزايد المستمر للجرائم المعلوماتيّة الأثر البالغ في ضرورة تطوير أجهزة الضبط القضائي لتواكب التّطور الحاصل في مجال الجريمة، ونتيجة لهذا التحدّي قامت معظم الدول بإحداث أجهزة متخصّصة بمكافحة هذا النّوع من الإجرام المستحدث تتولّى مهمّة التحرّي عن جرائم العالم الافتراضي وكشف النقاب عنها، وقد حملت هذه الأجهزة تسميات مختلفة مثلا شرطة الأنترنت أو فرقة التّحري عن الجرائم المعلوماتيّة ولا يقتصر دور هذه الأجهزة على المستوى الوطني فقط بل هناك أجهزة مختصّة على المستوى الدّولي أيضا.

* الأجهزة المختصّة بالبحث والتحرّي عن الجريمة المعلوماتيّة على المستوى الدّاخلي :

لقد ظهرت العديد من الأجهزة و الهيئات المتخصّصة في مجال الجريمة المعلوماتيّة في إطار مكافحتها والبحث والتحرّي عنها وعن مرتكبها سواء على المستوى الوطني أم على الصّعيد الدّولي. إنّه بالنّظر إلى الطبيعة التقنيّة الّتي تتميّز بها الجريمة المعلوماتيّة ذهبت أغلب الأنظمة القانونيّة الإجرائيّة في التشريعات المقارنة إلى أن تعهد بمسألة البحث و التحرّي عن هذا النّوع من الجرائم لأجهزة متخصّصة، لها من الكفاءة والتدريب والوسائل البشريّة و المادّية ما يؤهّلها للتعامل مع هذا النّوع المستحدث من الإجرام.

* **الأجهزة المختصّة في الدّول الأجنبيّة** : كانت الدّول المتقدّمة سبّاقة بإحداث هذه الأجهزة إذ أنّ مكافحة الجرائم المعلوماتيّة مرتبط بمدى تقدّم الدّول من النّاحية التقنيّة وبمدى توفّر الإمكانيات المادّية اللاّزمة لإنشاء هذه الأجهـزة ونذكر على سبيل المثـال في هذا الصّدد الدول التاليّة :

1 – الولايات المتّحدة الأمريكيّة : قامت الولايات المتّحدة الأمريكيّة بإنشاء عدّة أجهزة لمكافحة الجريمة المعلوماتيّة ومنها :

– شرطة الواب Web Police : وتعتبر نقطة مراقبة على الأنترنت إضافة إلى أنّها تتلقّى الشكاوي وتسعى إلى البحث عن الأدلّة ضدّهم وتقديمهم إلى المحاكمة [1].

– مركز تلقي شكاوي جرائم الأنترنت IC3 : والّذي تمّ إنشاؤه من طرف مكتب التحقيقات الفدرالي FBA في سنة 2000 ثمّ في عام 2003 تمّ دمج مركز شكاوي الاحتيال عبر الأنترنت المعروف ب IFCC مع هذا المركز ويعمل مركز IC3 بصورة تشاركيّة مع مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الباقات البيضاء NWC ويقوم هذا المركز بتلقي الشكاوي عبر موقعه على الأنترنت أين يقوم الشّاكي بمليء استمارة إلكترونيّة ثمّ يقوم المختصّون في هذا المركز بتحليل الشكاوي وربطها بالشكاوي الأخرى المستلمة من قبل.

(1) جميل عبد الباقي الصغير، الجوانب الإجرائيّة للجرائم المتعلّقة بالأنترنت، بحث منشور على الأنترنت .www.arablawinfo.com

– **قسم جرائم الحاسوب والعدوان على حقوق الملكيّة الفكريّة** : ويختصّ هذا القسم بالتعريف بهذه الجرائم و الكشف عنها وملاحقة مرتكبها.

– **نيابة جرائم الحاسوب والاتصالات CTC** : وتتألّف من مجموعة من قضاة النيابة العامّة ممّن تلقّوا تدريبات مكثّفة على نظم المعالجة الآليّة للبيانات.

– **المركز الوطني لحماية البنية التحتيّة** : التّابع للمباحث الفدراليّة الأمريكيّة وقد حدّد هذا المركز البنى التحتيّة الّتي تعتبر هدفا للهجومات و الاعتداءات عبر الأنترنت وعلى رأسها شبكات الاتصالات.

وإضافة إلى هذه الأجهزة يوجد أيضا في الولايات المتّحدة الأمريكيّة كوحدة متخصّصة بمكافحة الإجرام المعلوماتي التابعة لقسم العدالة الأمريكي تتكوّن من خبراء في نظام الحوسبة.

2 – في بريطانيا : قامت السلطات البريطانيّة بتخصيص وحدة تضمّ نخبة من رجال الشّرطة المتخصّصين في البحث و التحرّي عن الجرائم المعلوماتيّة وتضمّ هذه الوحدة نحو ثمانين عنصرا على درجة عاليّة من الكفاءة في المجال التقني وقد بدأت هذه الوحدة نشاطها عام 2001.

3 – في فرنسا : قامت الحكومة الفرنسيّة بإنشاء عدّة أجهزة لمكافحة الجرائم المعلوماتيّة ونذكر من هذه الأجهزة :

– القسم الوطني لقمع جرائم المساس بالأموال و الأشخاص : ويتكوّن هذا القسم من محقّقين بجرائم العالم الافتراضي وقد بدأ هذا القسم مهامه عام 1997.

– المكتب المركزي لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات و الاتصالات : ويعدّ هذا المكتب سلاح الدّولة الفرنسيّة في مكافحة الجرائم المعلوماتيّة، وقد تمّ إنشاؤه في 2001/05/15.

4 – في الصّين : قامت السلطات في هذا البلد بإنشاء وحدة متخصّصة على مستوى جهاز الشّرطة تعرف باسم "القوّة المضادّة للهكرة" وهي تختصّ برقابة المعلومات الّتي يسمح لمواطنيها الدّخول إليها عبر الأنترنت.

*** الأجهزة المختصّة بالبحث والتحرّي عن الجريمة المعلوماتيّة على المستوى الوطني :**

أمّا الوضع في بلادنا فإنّه وبالنّظر إلى الخصوصيّة الّتي تتميّز بها الجريمة المعلوماتيّة كان الأمر محتّما لتوفير أجهزة مختصّة تعنى بعمليّة البحث و التّحرّي عن الجريمة المعلوماتيّة وكان ذلك إمّا على مستوى جهاز الشّرطة أو الدّرك الوطني.

*** الأجهزة المختصّة بالبحث والتحرّي عن الجريمة المعلوماتيّة على المستوى الدولي و الإقليمي** : إنّ الجرائم المعلوماتيّة تتميّز بأنّها عابرة للحدود الوطنيّة يمكن أن يتعدّى أثرها عدّة دول، لذلك كان لابدّ من وجود تعاون دولي من أجل مكافحة هذا النّوع من الإجرام ومن أساليب التعاون الدولي التعاون الأمني الّذي يمكن أن يحقّق أهدافه ومن أبرز هذه الأجهزة في مجال مكافحة الجرائم المعلوماتيّة على هذا الصّعيد نذكر ما يلي :

– على المستوى الدّولي : تعدّ المنظّمة الدّولية للشرطة الجنائيّة (الإنتربول) [1] من أهمّ الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامّة ومنها الجرائم المعلوماتيّة، وتهدف هذه المنظّمة الدوليّة إلى تشجيع التعاون بين أجهزة الشّرطة في الدول الأطراف على نحو فعال من أجل مكافحة الجريمة ذات الطابع العالمي بما في ذلك الإجرام المرتبط بالمعلوماتيّة، وتستخدم هذه المنظّمة لتحقيق أهدافها وسيلتين :

– تجميع البيانات و المعلومات المتعلّقة بالجريمة عن طريق المكاتب الوطنيّة الموجودة في أقاليم الدولة الأطراف.

– التعاون في ملاحقة المجرمين الفارّين وإلقاء القبض عليهم وتسليمهم للدولة الّتي تطالب بتسليمهم لها.

وتعمل المنظمة الدوليّة للشرطة الجنائيّة في مجال الجرائم المعلوماتيّة بوضع قائمة إسميّة لضباط مختصين يمكن الاستعانة بهم في مجال البحث و التّحرّي في قضايا الجرائم المعلوماتيّة كما توفّر هذه المنظّمة للدّولة الأطراف المعلومات اللاّزمة عن طريق العمليّة في مجال الجريمة المعلوماتيّة من خلال خلق فرق عمل وورشات تكوين. ولقد أنشأت هذه المنظّمة وحدة متخصّصة في مكافحة الجرائم المعلوماتيّة تقوم بتزويد أجهزة الشّرطة التابعة للدّولة الأعضاء بإرشادات حول التحقيق في هذا النّوع من الإجرام وكيفية التدريب على مكافحته.

(1) بعد انتهاء الحرب العالمية الثانيّة عقد في بروكسل (بلجيكا) مؤتمر دولي في الفترة من 9-6/9عام 1964 انتهى إلى إيجاد اللّجنة الدوليّة للشرطة الجنائيّة، ونقل مقرّها إلى باريس وغيّر اسمها ليصبح المنظمة الدوليّة للشرطة الجنائيّة "الإنتربول".

* **الشرطة الأوروبيّة أو الأجهزة على المستوى الإقليمي "الأوروبول"** : وهو جهاز على المستوى الاتحاد الأوروبي تمّ إنشاؤه في لكسمبورغ عام 1992 ومقرّه مدينة لاهاي هولندا ليكون حلقة وصل بين أجهزة الشّرطة الوطنيّة للدّول الأعضاء في مجال الجرائم الإرهابيّة و المخدّرات والجريمة المنظّمة وكذا الإجرام المعلوماتي، ويهدف هذا الجهاز إلى تسهيل تبادل المعلومات بين أجهزة الشّرطة لمختلف الدّول الأعضاء وكذا تجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص أي جريمة من جرائم المذكورة ومنها الجريمة المعلوماتيّة، وبمبادرة من الشّرطة القضائيّة الفرنسيّة تمّ إنشاء جهاز على مستوى الأوروبول أطلق عليه اسم "ICROS" Internet Crime Reporting online system

* **الأوروجيست"Euro gust"** : وهو جهاز يعمل على المستوى الأوروبي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم تمّ إنشاؤه عام 2002 وينعقد اختصاصه عندما تمسّ الجريمة دولتين على الأقل بين الدول الأعضاء في الاتحاد الأوروبي أو دولة عضو مع دولة أخرى من غير الاتحاد الأوروبي.

ويعدّ الأوروجيست وحدة للتعاون القضائي، مهمّتها الأساسيّة هي التنسيق بين السلطات القضائيّة المكلّفة بالتحقيقات ولها من الصلاحيات ما يؤهّلها لفتح تحقيقات ومباشرة متابعات جزائيّة [1].

(1) - Myriam QUEMENER. YES CHARPENEL Cybercriminalité droit pénal applique économique septembre 2010، p. 209.

المطلب الثاني : خصائص التحقيق والمحقق في الجريمة المعلوماتيّة

تعدّ مرحلة التحقيـــق الابتدائي أو ما يطلق عليها مرحلـــة جمع الاستدلالات، مرحلـة هامّـــة في سبيل البحث و التّحرّي عن الجرائم، وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلّق الأمر بالجريمة المعلوماتيّة، لأنّها تعدّ حجر الزاوية الّذي سيتمّ على أساسه بناء الدّعوى برمّتها.

فما يتمّ جمعه من معلومات وأدلّة رقميّة في المرحلة الّتي تعقب ارتكاب الجريمة مباشرة قد لا يبقى متاحا بعد مرور وقت قصير على ارتكابها والسبب في ذلك يعود إلى الطبيعة التقنيّة لهذه الجرائم، ففي كثير من الجرائم المعلوماتيّة لم يترك الجاني وراءه سوى ذلك التعبير الّذي يعتري وجوه القائمين على تعقبه و الممزوج بالإحباط و الإعجاب معا.

* **خصائص التحقيق في الجريمة المعلوماتيّة** : التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة و راسخة بدونها ما كان ليتمتّع التحقيق بتلك الصّفة.

وهذه القواعد إمّا قانونيّة وإمّا فنيّة، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع والامتثال، أمّا الثّانية فتتميّز بالمرونة الّتي يضفي عليها المحقّق من خبرته وفطنته ومهارته الكثير [1].

ذلك أنّ الفكر البشري المتعلّق بالمجرم المعلوماتي يجب أن يقابله فكر بشري من قبل المحقق الجنائي، وبالتالي فإنّ أسلوب التحقيق وفكر المحقق الجنائي يجب أن يتغيّر ويتطوّر أيضا، وذلك كنتيجة طبيعيّة لمواجهة فكر المجرم المعلوماتي.

(1) خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونيّة، دار الفكر الجامعي، الطبعة الأولى 2009، ص 56.

أولا : منهج أو أسلوب التحقيق الابتدائي للجريمة المعلوماتيّة : التحقيق عموما هو مجموعة الإجراءات الّتي يقوم بها المحقق وتؤّدي إلى اكتشاف الجريمة ومعرفة مرتكبيها تمهيدا لتقديمهم إلى المحاكمة، وقد تكون هذه الإجراءات عمليّة كالتفتيش أو فنّية كمضاهات البصمات أو برمجيّة كتحديد كيفية الدخول إلى المعطيات المخزّنة في النظام المعلوماتي.

والهدف من التحقيق الابتدائي هو التأكد أولا من وقوع جريمة يعاقب عليها القانون، ومن ثمّة معرفة نوع هذه الجريمة ومن هو الجاني ومن هو المجني عليه، وكذا معرفة وقوعها وماهي الوسائل الّتي استعملت في ارتكابها ويكون ذلك في الجريمة المعلوماتيّة وفقا لمنهج تحقيقي يختلف عن غيره بالنّسبة للجرائم الأخرى.

1 / وضع خطة عمل التحقيق : يبدأ المحقق عمله عند تجميع الاستدلالات المتعلّقة بالجريمة المعلوماتيّة بوضع خطّة العمل اللاّزمة على ضوء المعلومات المتوافرة لديه، وتحديد الفريق الفنّي اللاّزم للقيام بمساعدته في أعمال التحقيق وذلك على النّحو الآتي :

– وضع الخطّة المناسبة الّتي لا تبدأ إلاّ بعد معاينة مسرح الجريمة و التّعرّف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصوّرات الكفيلة للتصدّي للجريمة.

– التخطيط الفنّي للتحقيق وذلك من أجل الوصول إلى أفضل الطرق و الأساليب للتعامل مع هذه الجرائم بالتفصيل و الوضوح.

– عمل دراسة وافية وجادّة لكافة إجراءات التحقيق ضمن الخطّة المسبقة الّتي تمّ وضعها وناقشها العاملون في فريق التّحقيق.

– تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمّتهم وعملهم و تقليل الاثار السلبية و الاسراع في انجاز العمل و هو ما يؤدي إلى ضمان مستوى جيد من الاداء.

– تحديد الإجراءات المسبقة و التي من شأنها التقليل من الأخطاء الفرديّة الّتي قد تنتج عن قلّة الخبرة أو نقص المعرفة وبالتّالي تساعد على إيجاد درجة جيّدة من التقيّد بالمستوى المطلوب مع ضمان أن الخطوات الّتي يقوم بها المحقّق خلال جميع مراحل التحقيق تسيير ضمن الضوابط التشريعيّة وتقلّل من الأخطاء الّتي قد تضر بالقضيّـة في مرحلة المحاكمة [1].

ويجب أن ترتكز خطة العمل على مجموعة من البنود الأساسيّة يتم الارتكاز عليها أثناء تنفيد الخطّة وهي أن يتمّ تعيين الأشخاص الّذين سيتمّ التحقيق معهم وتحديد النقاط الّتي يجب استضاحها معهم وتقدير مدى الحاجة للاستعانة ببعض الفنيين اللّازم توافرهم لاستكمال التحقيق [2].

بالإضافة إلى مراعاة الظروف والملابسات المحيطة بالواقعة ذلك أنّ من هذه الظروف تشمل عوامل مهمّة يجب مراعاتها عند وضع خطّة العمل ومنها :

– مدى أهمّية الأجهزة و الشبكات المتضرّرة لعمل المنظّمة.
– مدى حساسيّة البيانات الّتي يحتمل سرقتها أو إتلافها.
– مستوى الاختراق الأمني الّذي تسبب فيه الجاني.

ثمّ بعد ذلك وضع الأسلوب الأمثل لعمليّة التفتيش وذلك من خلال تحديد نوع الأدلّة الّتي يريد فريق التحقيق البحث عنها.

(1) محمد نصير السرحاني، مهارات التحقيق الجنائي التقني في جرائم الحاسوب و الأنترنت، رسالة الماجستير جامعة نايف العربيّة للعلوم الأمنيّة الرّياض 2004، ص 72.

(2) هشام رستم، الجوانب الإجرائيّة للجرائم المعلوماتيّة، مكتبة الآلات الحديثة، أسيوط 2000، ص 59.

2 / تشكيل فريق التحقيق :

إنّ التحقيق الابتدائي في الجرائم المعلوماتيّة يكون غالبا أكبر من أن يتولاه شخص واحد بمفرده، حتّى ولو كانت المضبوطات هي مجرّد حاسب شخصي واحد، ولذلك فإنّه يفضّل أن يتعاون عدّة محققين في إنجاز مهمّة التحقيق و العثور على الأدلّة.

ويجب أن يتشكّل فريق التحقيق من فنيين وأخصائيين ذوي خبرة في مجال الحاسوب والأنترنت، ويمتازون بمهارات في التحقيق الجنائي بشكل عام و التحقيق الجنائي الإلكتروني بشكل خاص. ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والأنترنت ليتمكّنوا من فك التعقيدات الّتي تفرضها ظروف وملابسات كل جريمة [1].

وإن كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلاّ أنّه يأخذ أهمّية خاصّة في الجرائم المعلوماتيّة لما تتطلّبه من مهارات فنّية وخبرات متنوّعة قد لا تتوافر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النّوع من الجرائم أمرا ضروريا. ومن النّاحية العمليّة غالبا ما يتكوّن فريق التحقيق في الجرائم المعلوماتيّة من :

- المحقق الرّئيسي ويكون ممّن لهم خبرة في التحقيق الجنائي.
- خبراء الحاسوب وشبكات الأنترنت الّذين يعرفون ظروف الحادث وكيفيّة التعامل مع هذه الجرائم.
- خبراء ضبط وتحرير الأدلّة الرقميّة العارفين بأمور تفتيش الحاسوب.
- خبراء أنظمة الحاسوب الّذين يتعاملون مع الأنظمة البرمجيّة.
- خبراء التصوير والبصمات والرّسم التخطيطي [2].

(1) عبد اللّه حسين محمود، إجراءات جمع الأدلّة في الجريمة المعلوماتيّة، مؤتمر الجوانب القانونيّة والأمنيّة للعمليات الإلكترونيّة، دبي 2003، ص 612.

(2) عبد اللّه محمود، المرجع السابق، ص 613.

وفي هذا الإطار نجد أنّ المشرع الجزائري قد أشار إلى مسألة إمكانيّة استعانة الجهات المكلّفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب و النظم المعلوماتيّة، أو ممّن لهم دراية بالتدابير المتّخذة لحماية المعطيات المعلوماتيّة، وذلك بغرض مساعدة جهات التحقيق في إنجاز مهمّتها وتزويدها بالمعلومات الضروريّة لذلك [1].

ثانيا : العناصر الأساسية للتحقيق الابتدائي في مجال الجريمة المعلوماتيّة : ونقصد بها تلك الإجراءات الّتي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحدّدة الّتي تثبت وقوع الجريمة وتحدّد شخصية مرتكبها، وهناك إجراءات واحتياطات يتعيّن على الضبطيّة القضائيّة مراعاتها أثناء التحقيق الابتدائي [2].

1 / الإجراءات الّتي يجب مراعاتها قبل البدء في التحقيق : ويمكن أن نسرد الأهم منها كما يأتي :

– تحديد نوع نظام المعالجة الآليّة للمعطيات فهل هو كمبيوتر معزول أم متّصل بشبكة معلومات.

– وضع مخطط تفصيلي للمنشأة الّتي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.

– إذا وقعت الجريمة على شبكة فإنّه يجب حصر طرفيات الاتصال بها أو منها لمعرفة الطرق الّتي تمّت بها عمليّة الاختراق من عدمه، وهل هناك حواسيب آليّة خارج هذه المشكلة ولها إمكانيّة الاتصال بها أم لا ؟.

(1) أنظر المادّة 05 الفقرة الأخيرة من القانون 04/09 المتضمّن القواعد الخاصّة للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

(2) جميل عبد الباقي الصغير، المرجع السابق، ص 119، عبد الفتاح بيومي حجازي، الدّليل الجنائي و التزوير المعلوماتي، دار الكتب القانونيّة المجلّة الكبرى، ط1، ص84، محمد الأمين الشبري، المرجع السابق، ص50.

– مراعاة صعوبة بقاء الدّليل فترة طويلة في الجريمة المعلوماتيّة.

– مراعاة أنّ الجاني قد يتدخّل من خلال الشبكة لإتلاف كل المعلومات المخزّنة.

– يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فاعليّة الجاني في أن يقوم بطريقة ما يمحو آثار جريمته.

– فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها، والتحفظ على الهواتف المحمولة من قبل الآخرين الّذين لا علاقة لهم بعمليّة التحقيق لأنّهم قد يسيئون استخدامها لطمس البيانات.

– التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنّها من الخدع الّتي يستعملها الجاني عند الاختراق، أن يتمّ ذلك بخط هاتفي مسروق عن طريق الدخول إلى شبكة الهاتف و التلاعب فيها وتضليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك.

– إبعاد الموظفين عن أجهزة الحاسب الآلي بعد الحصول منهم على كلمة السّر وكذا الشفرات في حالة وجودها.

– تصوير الأجهزة المستهدفة (الّتي وقعت بها أو عليها الجريمة) من الأمام و الخلف وذلك لإثبات أنّها كانت تعمل وكذلك للمساعدة في إعادة تركيبه من أجل البدء في إجراءات التحقيق.

2 / الإجراءات الّتي يجب مراعاتها أثناء التحقيق : عند البدء في عمليّة التحقيق الابتدائي لا سيما عند القيام بعمليّة تفتيش جهاز الحاسوب فإنّه على رجال الضبطيّة القضائيّة وبرفقتهم الخبراء الّذين يستعينون بهم مراعاة ما يلي :

– عمل نسخة احتياطية من الأقراص الصّلبة أو الأسطوانة المرنة قبل استخدامها و التأكد فنيا من دقّة النسخ عن طريق الأمر (Disk Comp).

– نزع غطاء الحاسب الآلي المستهدف و التّأكد من عدم وجود أقراص صلبة إضافيّة.

– أن يكون الهدف من نسخ محتوى الأسطوانة و الأقراص تحليل المعلومات الموجودة بها بغرض التوصّل إلى معرفة الملفات الممسوحة، ويمكن استعادتها من سلة المهملات مع ملاحظة أنّ هناك بعض الملفات الّتي إن مسحت وضغط على أزرار معينة مثل (Shift delete) في وقت واحد لا يمكن استعادتها وكذا من أجل معرفة الملفات الخفية المخزّنة في ذاكرة الحاسوب.

– العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابيّة الّتي تكون قد استخدمت في جريمة اختلاس معلوماتي.

– العمل على فحص العلاقة بين برامج التطبيقات و الملفات خاصة تلك الّتي تتعلّق بدخول المعلومات وخروجها.

– حفظ المعدات و الأجهزة الّتي تضبط بطريقة فنيّة و سليمة.

* **خصائص المحقق المعلوماتي** : أمام التطور التقني و التكنولوجي الّذي صاحب الجريمة المعلوماتيّة فإنّ المتخصصين بالتحقيق في هذا النّوع من الإجرام المستحدث يختلفون عن أولئك المختصين بضبط الجرائم التقليديّة من حيث الخصائص وطريقة التكوين، ذلك أنّ التحقيق في هذه الجرائم لا يعتمد على التدريبات الجسديّة الّتي يتلقاها عادة رجال الضبطيّة القضائيّة وإنّما يعتمد على البناء العلمي والتكنولوجي وهم يتولون مهمّة البحث و التحرّي عن الجرائم المعلوماتيّة وكشف النقاب عنها.

وإذا كان قد سبق وأن طرحنا خصائص الجريمة المعلوماتيّة وكذا خصائص المجرم المعلوماتي فإنّه في اعتقادنا يلزم الأمر معرفة الخصائص التي يجب أن يتوفّر عليها من يتصدّى لمهمة البحث و التّحري عن هذا النـّوع من الجرائم و المجرمين.

* **الخصائص الفنّية للمحقق في الجريمة المعلوماتيّة** : تلعب الأجهزة الأمنيّة دورا أساسيا في صيانة أمن المجتمع وذلك إمّا بالقيام بدور وقائي إلى منع ارتكاب الجرائم و الحيلولة دون وقوعها وتقليل فرص اقترافها، وإمّا القيام بدور قضائي في ضبط الجرائم ومرتكبيها بعد حدوثها.

ولقد أضاف ظهور الجرائم المعلوماتيّة النّابعة من التطوّر الإلكتروني أعباء جديدة على أجهزة التحقيق لما يتطلّبه التصدّي لهذه الجرائم من قدرات فنّية لم يألفها رجال الضبطيّة القضائيّة ولم يتعوّدوا عليها، ما يستلزم ضرورة توفير الإمكانات و المهارات المطلوبة في هذا المجال.

والمشكلة الأساسية الّتي تواجه المحققين في جرائم نظم المعلومات هي خلفيّة المحقق نفسه فمتخصصو الحاسب الآلي قد تكون لديهم المعرفة التقنيّة اللّازمة ولكنّهم ليسوا مدرّبين على تفهم دوافع الجريمة وجمع الأدلّة لتقديم المتّهم للمحاكمة.

وفي كثير من الحالات نجد أنّ متخصص الحاسب يعتقد أنّ لديه الدّليل الحاسم حول جريمة معلوماتيّة ما، ولكن من النّاحية القانونيّة يتبيّن فيما بعد أنّ الدّليل لا يصلح لإقامة الدّعوى، بينما المحقّقون ذوي الخلفيّة القانونيّة قد تكون لديهم خبرة واسعة في التحقيق ولكنّهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي الّتي يستخدمها المجرمون في هذا النّوع من الجرائم [1].

وإذا كانت مهارات التعامل مع مسرح الجريمة و التحفظ على الأدلّة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق الّتي لا يتوقّع أحد عدم توافرها لدى المحقق، إلاّ أنّه يلزمه عند مباشرته التحقيق في الجريمة المعلوماتيّة معرفة العديد من الجوانب الفنّية ليقوم بعمله على أحسن وجه ونذكر منها :

– معرفة الجوانب الفنّية والتقنيّة لأجهزة الحاسوب و الأنترنت و الّتي تتعلّق بالجريمة المرتكبة ذلك أنّ افتقار ضابط الشرطة القضائيّة للتأهيل الكافي في الميدان التقني قد يفضي إلى إتلاف وتدمير الدّليل، على اعتبار أن جهله بأساليب ارتكاب الجريمة المعلوماتيّة يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدّي إلى محو الأدلّة الرّقميّة أو تدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات الّتي تخزّن بها البيانات [2].

(1) في حادثة طلب أحد المحققين من المشتبه فيه أن يريه الملف الّذي قام بتزويره وذلك انطلاقا من الحاسب الشخصي له فما كان للمشتبه فيه إلاّ أن قام عمدا بحذف هذا الملف وبذلك أضاع الدليل الرّئيسي في الجريمة وفي حادثة أخرى ثمّ القبض على بعض المتّهمين وضبط الحاسوب ثمّ قامت جهات التحقيق بتفكيك الحاسوب باعتباره دليل الجريمة.

(2) جميل عبد الباقي الصغير، أدلّة الإثبات الجنائي والتكنولوجيّة الحديثة، دار النّهضة العربيّة، القاهرة 2002، ص 115.

وبالتالي فإنّ الكشف عن هذه الجرائم يقتضي أن تكون الأجهزة المعنيّة على دراية كافية بأساسيات التعامل مع هذه الجرائم وكيفيّة تقصيها وضبطها وصولا إلى مرتكبيها.

- إتباع الإجراءات الصحيحة و المشروعة من أجل سرعة المحافظة على الأدلّة الإلكترونيّة الّتي تدلّ على وقوع الجريمة، وتخزينها في الأقراص المعدّة لذلك ومنع حذفها و الحرص على عدم تعريض وسائط التخزين كالأقراص المرنة أو المدمجة لأيّة مؤثرات خارجيّة كالقوى الكهرومغناطيسيّة أو الميكروويف حتّى لا تتلف محتوياتها.

- كما يتوجّب على المحقق معرفة آليّة عمل تشكيلات الحاسوب والأنترنت، وتبرز أهمّية فهم المحقق لهذه المبادئ في كونها ضروريّة لتصوّر كيفيّة ارتكاب الفعل الإجرامي في العالم الافتراضي من اختراق للشبكات واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويلها عن مسارها، كما أنّها تعطي للمحقق تصوّرا جيّدا عن مدى إمكانيّة متابعة مصدر الاعتداء على الشبكة و المعوقات الّتي تحول دون ذلك [1].

- يتوجّب على المحقق أن يستطيع التمييز بين الأنظمة المختلفة لتشغيل الحاسوب وأن يلمّ بجميع الأنظمة التشغيليّة لأجهزة الحاسوب وما تتسم به من خصائص ومميّزات كل نظام على حدة لأنّه ملزم بالتعامل معها، وكذلك أنظمة الملفات الّتي يعتمدها كلّ نظام حتّى يتمكّن من إجراء التحقيق في الجرائم المعلوماتيّة وفي كشف المجرمين ومعاينة مسرح الجريمة.

وقامت بنقله إلى مركز الشرطة ثمّ بعدها تبيّن أنّ تشغيل الجهاز لفحص مكوّناته يحتاج إلى إعادة توصيل الكابلات الّتي تمّ نقلها دون أن يتمّ ترقيمها وكان الأمر يبدو شبه مستحيل وضاع حتّى الدليل أيضا.

(1) حسين الغافري، المرجع السابق، ص 02.

– و إذا كان التعامل المباشر مع هذه الأنظمة و القيام بفحصها ورفع الأدلّة الجنائيّة الرّقميّة الموجودة فيها يعتبر مهمّة الخبير "إلاّ أنّ معرفة المحقق الجنائي الأوّليّة بهذه الأنظمة ضروريّة لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة المعلوماتية".

– كما يتعيّن على المحقق كذلك التعرّف على معطيات الحاسوب المختلفة ليصبح قادرا على معرفة صيغ الملفات وما يمكن أن تحتويه من معطيات، ومعرفته لأهم التطبيقات الّتي يمكنه من خلالها قراءة أو مشاهدة محتوى هذه الملفات [1] الّتي تعدّ في غاية الأهمّية، لأنّها تعتبر الوعاء الحقيقي لأدلّة الإدانة في كثير من القضايا ذات الصّلة بالحاسوب و الأنترنت بما تحتويه من معلومات.

– ومن الأمور الفنّية الّتي يتوجّب على المحقق معرفتها أيضا أن يكون ملما بالأساليب المستخدمة في ارتكاب الجرائم المعلوماتيّة وتقنيات الأمن المعلوماتي، ذلك أنّ معرفة رجال التحقيق لهذه الأساليب يعدّ من الأمور المهمّة الّتي تساعدهم في معرفة الجناة ومواقع ارتكاب الجريمة ومن أي طرفيّة إلكترونيّة صدر السلوك الإجرامي وكذلك في مناقشة الشهود وسماع المشتبه فيهم ومحاصرتهم بالأسئلة الّتي تتعلّق بكيفيّة ارتكاب الجريمة وطرق تنفيذها.

كما أنّ الإلمام بتقنيات الأمن المعلوماتيّة و الحاسوبيّة من الأمور المهمّة و الّتي لابدّ للمحقق المعلوماتي من معرفتها واستيعابها، لأنّها تساعده في معرفة مجريات التحقيق، فالمحقق عندما يباشر التحقيق في جريمة اختراق شبكة الحاسوب التابعة لمؤسسة ما يسأل القائمين على الشبكة عن نوع برامج الحماية المستخدمة وكيفية إعدادها و الكيفيّة الّتي تفاعلت بها مع الحدث محلّ التحقيق.

(1) يتمّ حفظ البيانات الرّقميّة داخل الحاسوب على شكل مجموعات أو كتل من البيانات تمثّل وحدة واحدة تسمّى الملفات ويتميّز كلّ ملف ببينة وصيغة خاصّة تميّزه عن غيره، وغالبا ما ترتبط صيغة بنوع محدّد من المحتوى كأن يحتوي الملف على بيانات تمثل صورا أو أصاتا أو مستندا خطيا منسق أو غير منسّق.

وهناك الكثير من التقنيات الّتي تستخدم في أمن الحاسوب و الشبكات والّتي تكون وثيقة الصّلة بالتحقيق ويكون فهم المحقق لوظائفها وأسلوب عملها وطرق استخدامها عاملا مساعدا له عند قراءته للتقارير الجنائيّة الّتي يعدّها خبير الحاسوب و الّتي تعدّ من أهمّ الوثائق الّتي يرجع إليها المحقق ويعتمد عليها في تحقيقه وترفق بعد ذلك بمحاضر التحقيق ويرتكز عليها توجيه الاتهام عند اللّزوم.

* **تأهيل وتدريب المحقق المعلوماتي** : في مكافحة الجرائم المعلوماتيّة بصفة عامّة لابدّ من وضع سياسة جنائيّة رشيدة تستند على تدريب أجهزة العدالة الجنائيّة لمكافحة هذه الجريمة، ويمتدّ هذا التدريب و التأهيل إلى العاملين بأجهزة الضبطيّة القضائيّة.

وقد تنبّهت الدول إلى هذا الأمر وظهر هذا الاهتمام في توصيات العديد من المؤتمرات الدّوليّة الخاصّة بمنع الجريمة ومعاملة المجرمين، ومنها ما جاء في القاعدة 1/22 من قواعد بيكين الّتي أكدت على الحاجة إلى التخصص المهني و التدريب.

ولهذا فإنّه من الضروري إعداد المحققين في الجرائم المعلوماتيّة باعتبارهم يواجهون أنشطة إجراميّة معقّدة وتنفّذ بطرق دقيقة وذكيّة، ويأتي ذلك من خلال الإسراع في أنّ يطور رجال البحث الجنائي وسائلهم البحثيّة وقدراتهم العلميّة وليس بالضرورة أن يكون المحقق في الجريمة المعلوماتيّة خبيرا في الحاسوب و النظم المعلوماتيّة ولكن لابدّ من الإلمام ببعض المسائل الأوّليّة الّتي تمكّنه من التفاهم مع خبراء الحاسب الآلي وحسن استغلالهم في كشف الجرائم وجمع الأدلّة.

كما أنّه من الضروري أن يكون المحقق ملما بالإجراءات الاحتياطية الّتي ينبغي اتخاذها على مسرح الجريمـــة و التدابير اللاّزمة لتأمين الأدلّة ومعلوماتها الممغنطة بصورة علميّة وسليمة [1].

وإذا كانت الشركات الخاصّة تستعين بمحققين هم خبراء في الحواسيب، فالجهات الحكوميّة أولى بإعداد كوادرها للضبط و التحقيق في الجرائم المعلوماتيّة، فالتقدّم المتواصل في تكنولوجيا الحاسب الآلي والأنترنت يفرض على جهات تطبيق القانون أن تسير في خطوات متناسقة مع التطوّرات السريعة الّتي تشهدها هذه التقنيات وهذا الأمر يتطلّب الإلمام بالتقنيات الجديدة حتّى يمكن مواجهة مجرمي المعلوماتيّة.

(1) محمّد الأمين البشري، التحقيق في جرائم الحاسب الآلي بحث مقدّم إلى مؤتمر القانون و الكمبيوتر و الأنترنت بكلّية الشريعة و القانون، جامعة الإمارات العربيّة المتّحدة الفترة من 01 إلى 03 ماي 2000.

المبحث الثاني: وسائل الإثبات للجريمة المعلوماتيّة.

يختلف الوسط الّذي ترتكب فيه الجريمة المعلوماتية من وسط مادّي إلى وسط معنوي إمّا يعرف بالوسط الافتراضي، وعلى ضوء دلك فإنّ أدلّة الإثبات في إطار مدى اتّفاقها مع الطبيعة التقنيّة لهذه الجرائم ووسائل ارتكابها أصبح غير ذي معني إذا لم يكن مدعّما بتوفيق من قبل التقنيّة ذاتها، ممّا أدّى إلى ظهور طائفة خاصّة من الأدلّة الإجراميّة يمكن الاعتماد عليها في اثبات هذه الجرائم ومن ثمّة نسبها إلى فاعلها بحيث يكون من ذات الطبيعة التقنيّة النّاجمة عن النظم المعلوماتيّة الّتي تنتج عنها في حالة الاعتداء عليها مع طبيعة الوسط الّذي ارتكبت فيه الجريمة و هي الأدلّة الرّقميّة أو الأدلّة الإلكترونيّة حسب ما عبّرت عنها الاتفاقية الأوروبيّة لمكافحة الجرائم المعلوماتيّة.

فالدّليل أثر يولد أو حقيقة تنبعث من الجريمة المرتكبة، ولذلك فإنّ طبيعة الدّليل يتشكّل من طبيعة الجريمة الّتي يولد منها، فدّليل التزوير يأتي من اثبات تغيّر الحقيقة في المحرّر الّذي يقع عليه، و دليل جريمة القتل قد يولد من فحص الأداة الّتي استخدمت في القتل وطلقات الذّخيرة الّتي استعملت فيها، وتطبيق ذلك على الجريمة المعلوماتيّة فإنّه يمكن أن تثبت بأدلّة تقنيّة ناتجة عن الوسائل التقنيّة الّتي ارتكبت بواسطتها.

المطلب الأوّل : الدّليل الرّقمي.

إنّ الدليل الرّقمي مأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطسية أو كهربائيّة يمكن تجمّعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصّة ويتمّ تقديمها في شكل دليل يمكن اعتماده أمام القضاء، وهناك من يعرفه بأنّه معلومات يقبلها المنطق و العقل ويعتمدها العلم، يتمّ الحصول عليها بإجراءات قانونيّة وعلميّة بترجمة البيانات الحسابيّة المخزّنة في أجهزة النظم المعلوماتيّة وملحقاتها وشبكات الاتّصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أوجاني أو مجني عليه، وأنّه الدّليل الّذي يوجد له أساسا في العالم الافتراضي.

كما عرف الدّليل الرّقمي أيضا أنّه مجموعة المجالات أو النبضات المغناطيسيّة أو الكهربائيّة الّتي يمكن تجميعها و تحليلها باستخدام برامج وتطبيقات خاصّة لتظهر في شكل صور أو تسجيلات صوتيّة أو مرئيّة.

فالدّليل الرّقمي هو أي معلومات سواء كانت من صنع الإنسان أو تمّ استخلاصها من الحاسوب يتقبّلها العقل و المنطق.

كما ذهبت بعض التعريفات الى أنّ الأدلّة الجنائيّة الرّقميّة ماهي إلاّ مرحلة متقدّمة من الأدلّة المادّية الملموسة الّتي يمكن إدراكها بإحدى الحواس الطبيعيّة للإنسان إلى الاستعانة بجميع ما يبتكره العلم من وسائل تقنيّة عالية ومنها الحاسوب، ولكن الحقيقة أنّ الأدلّة الرّقميّة هي نوع متميّز من وسائل الإثبات ولها من الخصائص العلميّة والمواصفات القانونيّة.

* **خصائص الدّليل الرّقمي** : تقوم خصائص الدّليل الرّقمي على مدى ارتباطه بالبيئة الافتراضية و الّذي يتميّز بعدّة خصائص تميّزه عن الدّليل الجنائي التقليدي.

1 – الدليل الرّقمي هو دليل علمي : أي أنّه يحتاج إلى بيئته التقنيّة الّتي يتكوّن فيها لكونه من طبيعة تقنيّة المعلومات ذات المبنى العلمي ومن ثمّة فإنّ ما ينطبق عل الدّليل العلمي ينطبق على الدّليل الرّقمي.

2 – **الدّليل الرّقمي من طبيعة تقنيّة** : الدّليل الرّقمي يجب أن يكون مستنبطا من البيئة الرّقميّة أو التقنيّة وهي في إطار جرائم المعلوماتيّة ممثّلة في العالم الرّقمي أو العالم الافتراضي.

3 – الدّليل الرّقمي دليل متنوّع ومتطوّر : يشتمل الدّليل الرّقمي كافة أشكال وأنواع البيانات الرّقميّة الممكن تداولها رقميّا بحيث يكون بينها وبين الجريمة رابطة من نوع خاص وتتّصل بالضّحيّة على النّحو الّذي يحقّق هذه الرّابطة بينها وبين الجاني وتعني هذه الخاصيّة أنّه على الرّغم من أنّ الدليل الرّقمي في أساسه متحد التكوين بلغة الحوسبة و الرّقميّة إلاّ أنّه مع ذلك يتّخذ أشكالا مختلفة يمكن أن يظهر عليها، كأن يكون بيانات غير مقروءة من خلال ضبط مصدر الدّليل كما هو الشّأن حال المراقبة عبر الشبكات، وقد يكون بيانات مفهومة كما لو كان وثيقة معدّة بنظام المعالجة الآليّة كما من الممكن أن يكون صورة ثابتة أو متحرّكة (أفلام رقميّة) أمّا عن كون الدّليل الرّقمي دليلا متطوّر فهي خاصّية تكاد تكون تلقائيّة، نظرا لارتباطه بالطّبيعة الّتي تتمتّع بها حركة الاتصال عبر الأنترنت و العالم الافتراضي.

4 – الدّليل الرّقمي صعب التخلّص منه : إنّ القاعدة الّتي تسري على كافّة ما يتعلّق بهيكلة تكنولوجيا المعلومات، هي أنّه كلّما حدث اتّصال بتكنولوجيا المعلومات في معنى ادخال بيانات إلى ذلك العالم فإنّه يصعب التّخلّص منها، ويمكن اعتبار هذه الخاصيّة ميزة يتمتّع بها الدّليل الرّقمي عن غيره من الأدلّة التقليديّة.

5 – الدّليل الرّقمي ذو طبيعة رقميّة ثنائيّة (1–0) : إنّ الآثار الّتي يتركها مستخدم النّظام المعلوماتي و الّتي تشمل الرّسائل المرسلة منه أو الّتي استقبلها وكافّة الاتصالات الّتي تمت من خلال الحاسب الآلي وشبكة الاتصالات تكون على شكل الرّقمي، فالبيانات الموجودة داخل الحاسب الآلي سواء كانت في شّكل نصوص أو حروف أو أرقام أو فيديو تحوّل إلى صيغة رقميّة حيث ترتكز تكنولوجيا المعلوماتيّة الحديثة على تقنيّة التّرقيم الّتي تعني ترجمة أو تحويل أي مستند إلى نظام ثنائي في تمثيل الأعداد يفهمه الحاسب الآلي قوامه الرقمان (0) و (1) فأيّ شيء في العالم الرّقمي يتكوّن من الصفر و الواحد.

كما يأخذ الدّليل الرّقمي في تحديد أنواعه إلى نوعين رئيسيين هما :

أ – السجلات الّتي تمّ إنشاؤها بواسطة الجهاز التلقائي وتعتبر هذه السجلات من مخرجات الجهاز ولم يساهم الإنسان في إنشائها.

ب – السجلات الّتي جزء منها تمّ حفظه بإدخال وجزء تمّ انشاءه بواسطة الجهاز ومن أمثلة ذلك البيانات الّتي تمّ ادخالها إلى الأدلّة و تتمّ معالجتها من خلال برامج خاصّة، و أمّا النّوع الثّاني أي الأدلّة الرّقميّة الّتي تعدّ لتكون وسيلة اثبات فهي تلك الأدلّة الّتي تنشأ دون إرادة الشّخص بمعنى أي أثر يتركه دون أن يكون راغبا في وجوده ويسمّى هذا النّوع من الأدلّة بالبصمة الرّقميّة أو الآثار المعلوماتيّة للرّقميّة، وهي تتجسّد في الآثار الّتي يتركها مستخدم النظام المعلوماتي بسبب تسجيل الرّسائل المرسلة منه أو الّتي يستقبلها وكافّة الاتصالات الّتي تمّت من خلال النّظام المعلوماتي وشبكة الاتصالات.

* **مصادر الحصول عل الدّليل الرّقمي** : إنّ مصادر الحصول على الدّليل الرّقمي تكمن في البيئة الرّقميّة الّتي ارتكبت فيها الجريمة المعلوماتيّة، وتتمثّل في أجهزة الحواسيب الخاصّة بالجاني أو المجني عليه وكذا أجهزة مقدّم الخدمة.

وهذه المصادر قد تكون على سبيل المثال لا الحصر إذ أنّ التطوّر العلمي و التقني قد يسفر عن أنواع جديدة من المصادر التقنيّة، إذ المقصود هنا من أين يمكن لجهات التحقيق و التّحرّي عن الجريمة المعلوماتيّة استخلاص الدّليل الرّقمي.

* **فحص جهاز الحاسوب الخاص بالجاني و المجني عليه** : إنّ فحص جهاز الحاسوب الخاص بالجاني يمكن من التحقيق وبيان الطريقة الّتي قام بها هذا الأخير في ارتكاب جرائمه، وممّا لا شكّ فيه أنّ المجني عليه هو المصدر الكاشف و النتيجة الّتي يترتّب عليها ما قام به الجاني من جرائم، وبالتالي فإنّ فحص جهاز الحاسوب الخاص به يمكن المحقّق من معرفة الدّخول وتتبع مصدره.

ويمكن الوصول إلى الدّليل الرّقمي المتعلّق بالجرائم المعلوماتيّة من خلال أجهزة الحاسوب سواء الخاصّة بالجاني أو المجني عليه عن طريق البحث في المصدرين التاليين :

أولا : أنظمة الحاسوب وملحقاتها : تعدّ الحواسيب مصدرا غنيّا بالأدلّة الرّقميّة خاصّة تلك الحواسيب الشخصيّة الّتي تعدّ بمثابة أرشفة سلوكيّة للأفراد، فهذه الحواسيب تحتوي على الكثير من المعلومات المتعلّقة بنشاطات الأفراد ورغباتهم، وعمليّة حجز الحاسوب بقصد تفحّصه تعدّ نقطة البداية في الكشف عن خفايا الجريمة المعلوماتيّة باعتبار أنّ هذا الجهاز هو وسيلة تنفيذها، و الحاسب الآلي في ذاته يقوم في تركيبته على أمرين هما : القطع الصّلبة (Hardware) والقطع المرنة أو البرمجيات (Soft ware) وهناك عنصر ثالث يتوزّع بين البرمجيات و القطع الصّلبة وهو عنصر المعلوماتية [1] لذلك فإنّ الأمر يستلزم أن يكون الفحص مادّيا ومعنويا للارتباط القائم بشكل طبيعي بين مكوّنات الحاسوب ككل.

(1) حسين بن سعيد بن سيف الفاغري، المرجع السابق، ص 425.

وقد تعتمد عمليّة الفحص على الحاسوب ذاته أي ما يسمّى بالفحص الذّاتي من خلال قيام الحاسوب ذاته بفحص مكوّناته وتقديم تقرير كامل بذلك إلى طالب الفحص، ومثل هذه العمليّة تتطلّب من القائم بها مهارة عاليّة أو قد يتمّ الفحص عن طريق الاستعانة بجهاز آخر أو أجهزة تقنيّة للبحث في جزئيات عبر جهاز الحاسوب، ويجب أن تشمل عمليّة الفحص على ما يلي :

1 – فحص القرص الصلب : يحتوي القرص الصلب بداخله على مجموع البيانات الرّقميّة ذات الطابع الثنائي و الّتي تتميّز بعدم تشابهها فيما بينها على الرّغم من وحدة الرّقم الثنائي (0.1) وتتمّ عمليّة فحص القرص الصّلب إمّا كلّيا أو جزئيّا، فالفحص الجزئي يؤدّي إلى التعرّف على محتوى البيانات و الّتي يؤدّي التعامل معها إلى الكشف عن القيمة الإستردادية للبيانات المخزونة فيه سواء كانت محتويات مكتوبة، صور أو أصوات ....إلخ.

بالإضافة إلى إمكانيّة معرفة ما تمّ حذفه من بيانات وبرامج بالاستعانة ببرمجيات خاصّة للقيام بذلك [1] والمثال المستخدم هنا هو حالة البحث في ملفات النسخ و هذه الأخيرة هي عبارة عن ملفات تأخذ نسخة احتياطية عن كلّ صفحة يتمّ الولوج إليها عبر الأنترنت كما توجد ملفّات خاصّة بالتنزيل (Download file) مهمّتها استقبال الملفّات الّتي يتمّ تحميلها على جهاز الحاسب الآلي من خارجه و عبر الأنترنت فهذه الملفّات مركزها القرص الصّلب.

(1) عمر أبو بكر بن يونس، المرجع السابق، ص 10 – 11.

وللتعرّف على محتويات القرص الصّلب فإنّ ذلك يتوقّف على مسائل عديدة منها الكيفية الّتي يتمّ بها ضبط الحاسوب ومهارة الشخص القائم باستخلاص البيانات دون العبث بمحتوياتها لذلك فإنّه عند ضبط جهاز الحاسب الآلي، على المحقق أن ينتزع القرص من الجهاز الخاص به ويحافظ عليه من الارتجاج أو الاصطدام بأي شيء، وعدم محاولة تفريغ اي بيانات متواجدة عليه و ذلك تفاديا لفقد أي بيانات، و تسليمه إلى الفنّي الخبير المختص الذي يقوم بتحليل النسخ التي تصدر من القرص و بعرض ما توصل إليه على المحقق.

و هنا لابد من مراعاة شرط سلامة جهاز الحاسب الآلي، الذي يعني صحة حركة القطع الصلبة فيه و ذلك لتجنب الوقوع في مأزق رفض المحكمة الاعتداد بالدّليل المنبثق عنه، فشرط سلامة الحاسوب مطعن رئيسي على كل دليل تمّ الحصول عليه بحيث يجب الكشف على حركة الحاسوب بداية و الإقرار بسلامته [1].

وإنّ من الأشياء الّتي تظهر بعد عمليّة فحص أي قرص صلب لأي جهاز تلك البيانات الّتي كان يستخدمها الجاني، وكذا الصّور المخزّنة فيه ومخابئ صفحات الأنترنت، ومن خلالها يمكن التوصّل لصفحات وعناوين مواقع الأنترنت وكذا رسائل البريد الإلكتروني بالإضافة إلى رؤوس الصفحات المرسلة والمتلقات ومجموعة البرامج الجاهزة المتخصّصة الّتي استخدمها (المشتبه فيه) ومنها يمكن تحديد أصدقاء (المشتبه فيه) وكذا تحديد ما يتحاورون فيه.

(1) خالد ممدوح إبراهيم، الجرائم المعلوماتيّة، المرجع السابق، ص 215.

2 – فحص البرمجيات : يتطلّب الأمر في مثل هذه الحالة أن نميّز بين الفحص الداخلي للبرمجيات و الفحص الخارجي لها، فالفحص الداخلي يتمّ من خلال البحث في البناء المنطقي للبرمجة بما يوحي بأنّ هناك مجهودا تجديديا في إعداده للعمل حين إنزاله على جهاز الحاسب الآلي Installation من خلال تتبع خطوات منطقيّة تعبّر عن هذا الجهد، وأكثر ما يتمّ البحث عنه في إطار الفحص الدّاخلي هو البحث عن مصدر الملفّات الموجودة في هذا الإطار، ذلك أنّ النسخ عبر الأنترنت لا يشبه النسخ باستخدام برمجيات المعالجة فالأوّل نسخ عبر العالم الافتراضي و الثّاني يتمّ باستخدام مصنف متداول في العالم المادّي، وتفيد وسيلة النسخ في ترتيب كيفية حدوث الجريمة.

أمّا في حالة الفحص الخارجي والّذي يتمّ اللّجوء فيه إلى النسخة الأصليّة للمقارنة بينها وبين النسخة محلّ الاشتباه وذلك للدلالة على ثبوت ارتكاب الجريمة بدرجة مقنعة.

وفي كلتا الحالتين ينبغي التنبيه إلى خطورة البرمجيات المعيبة الّتي يمكن أن تؤثّر في الحاسوب وتجعله محلّ شك تهتزّ معه قيمة الدّليل، يكون لهذا القصور أثره في عمليّة تقييم الدّليل المستمد من البرمجيات ذاتها[1].

(1) خالد ممدوح إبراهيم ، المرجع السابق، ص 219.

3 – فحص النظام المعلوماتي : إنّ المهمّة الأساسيّة لكلّ نظام معلوماتي هو تحقيق فرضيّة تنفيذ الأوامر الّتي يمكن أن يقوم بها مستخدم الحاسوب، وتعني عمليّة فحص النظام المعلوماتي ضبط كافة ما يحتويه جهاز الحاسب الآلي من معلومات [1] يمكن استرجاعها عبره تكون مخزّنة في ملفات على أي شكل يمكن أن تكون عليها الحركة الإستردادية مادام موضوعها يشكّل جريمة.

والحقيقة أنّه على حسب كثرة التعامل بالحاسب الآلي يتكاثر محتوى النظام المعلوماتي مما يزيد من صعوبة فحصه بالنظر إلى الحجم الضخم و الكم الهائل من المعلومات المخزّنة فيه.

بالإضافة إلى أنّ عمليّة تخزين البيانات لا تتخذ شكلا محدّدا وإنّما تتنوّع أساليبها، و الّتي يصل مداها إلى حد إمكانية تخزين البيانات بشكل آمن في الحاسوب بنظام التشغيل أو بنظام إخفاء البيانات المعلوماتيّة بحيث لا يظهر الملف حتّى في حالة البحث الآلي للحاسب عنه و الّذي قد يحتوي على مواد إجراميّة، وتفوّت الفرصة بسبب هذه التقنيّة على المحقّقين من الوصول إليه [2].

(1) إنّ النّظام المعلوماتي للحاسب الآلي لا يحتوي على معلومات مكتوبة كما هو المعتقد السّئد، وإنّما المحتوى المعلوماتي عادة ما يتكوّن من بيانات ثنائيّة الهيئة الرّقميّة يتمّ إيداعها في الحاسب الآلي في شكل تخزين (Stockage) ويقوم الحاسوب بمعالجة هذه البيانات ويبرزها على هيئة معلومة محدّدة حين يتمّ استدعاؤها من قبل مستخدم الحاسوب ومادام لم يتم استدعاء معلومات محدّدة فإن بياناتها تضلّ في حالة تخزين في الحاسوب فلا يقوم الحاسوب باستدعاء كافّة المعلومات مرّة واحدة.

(2) خالد ممدوح إبراهيم، المرجع السّابق، ص 222.

ثانيا : فحص أنظمة الاتصال بالأنترنت : يقصد بنظام الاتصال بالأنترنت بالمفهوم الإجرائي هو تلك الإجراءات أو المراحل المتّبعة حال استخدام الاتصال بالأنترنت، ومن أهمّ المسائل المثارة في صدد فحص أنظمة الاتصال بالأنترنت سعيا وراء البحث عن الدّليل هي مسألة تحديد مكان الجريمة أو جهاز الحاسب الآلي الّذي انطلق منه النشاط الإجرامي، وذلك من خلال تتبع الحركة العكسيّة لمسار الأنترنت أي تتبع الحركة التراسليّة للنشاط الممارس من خلال الأنترنت، فالحاسوب بمجرّد أن يتعرّف على المسار يقوم تلقائيا باختيار البروتوكول التراسلي الّذي من خلاله يقوم باستدعاء البيانات [1].

و يستخدم في عملية تتبع حركة مسار الأنترنت نظام فحص إلكتروني يطلق عليه علم البصمات المعاصر [2] و ما يتم التوصل إليه بعد ذلك هو عنوان رقمي يسمى adresse IP Protocol internet و هو عبارة عن بروتوكول لعنونة البيانات و المواقع في شبكة الأنترنت، و بمقتضى هذا البروتوكول (IP) يتم التعرف على الكومبيوتر الموصول بشبكة الأنترنت من خلال عناوين عديدة، حيث لكل كومبيوتر عنوانه الوحيد و الخاص به تماما [3] يسمّى IP Adresse و كل عنوان IP مكون من جزئين.

1) عمر بن يونس ، الجرائم النّاشئة عن استخدام الأنترنت، المرجع السّابق، ص998.

(2) وقد تمّ استخدام هذا المنهج في الكشف عن العديد من الجرائم مثل تتبع مبتكر فيروس ميليسا وكذا التوصّل إلى الشخص الّذي ابتكر موقع خدمات بولمي روج لأخبار المال الاحتياطي لكن يرفع الأسهم بطريق الخداع .

(3) عبد الحميد عبد المطلب استخدم بروتوكول TCP /IP في بحث وتحقيق الجرائم مع الكمبيوتر، المرجع السابق، ص 5.

الأول يشمل أرقام الشبكة و الثاني يشمل أرقام مقدم الخدمة [1] و يعمل بروتوكول IP بشكل متزامن مع هذا بروتوكول آخر وهو بروتوكول التحكّم بالنّقل (Tram mission control protocol) TCP وهذان البروتوكولان (TCP/IP) هما من عائلة بروتوكولات الاتصال بين عدّة أجهزة من الحواسيب طوّرت أساسا لنقل البيانات بين أنظمة (UNIX) [2] ثمّ أصبحت المقياس المستخدم لنقل البيانات الرّقميّة عبر شبكة الأنترنت، ويرتكز البروتوكولان معا (TCP/IP) على تقنيّة التبديل المعلوماتي بواسطة الحزم المعلوماتيّة (Packet) بين مختلف الوصلات السّلكيّة واللاّسلكيّة المتخصّصة الّتي تربط الشبكات المختلفة الموصولة فيما بينها.

وحزمة المعلومات جزء أو قسم من ملف معلوماتي ذات حجم مصغّر ثابت تحمل كلّ منها رقما خاصا ومعلومات تعريفيّة بكل من المرسل و المرسل إليه، وعند كلّ وصلة تتمّ قراءة جهة المقصد أو المرسل إليه ثمّ تتمّ إعادة إرسال الحزمة المارة عبرهما نحو الوصلات التالية الأقرب إلى جهة المقصد النّهائيّة. ويعتبر نظام TCP/IP من أكثر البروتوكولات المستخدمة في شبكة الأنترنت فهو جزء أساسي منه، لذلك تبرز أهمّية الاستعانة بالمعلومات والمصادر والعناوين الّتي يمكن أن يحتويها هذا البروتوكول في تحقيق الجرائم المعلوماتيّة، حيث تدلّ بصفة جازمة عن مصدر الجهاز المستخدم في الجريمة وتحديد الأجهزة الّتي أصابها الضّرر من الفعل الإجرامي وتحديد نوعيّة النشاط الإجرامي من خلال الفترة الزّمنيّة لاقتراف الجريمة [3].

(1) يعبّر عن عناوين الأنترنت الرّقميّة الوحيد سلسلة مؤلّفة من أربع مجموعات من الأرقام مفصولة عن بعضها بنقاط أو حروف أبجديّة رمزيّة دالّة عليها، يجري صفّها ضمن تسلسل هرمي ويتولّى نسخ هذه الأرقام أو استبدالها بحروف مؤسّسة الأنترنت لمنح الأسماء و الأرقام وهي لجنة دوليّة خاصّة تعمل بالتنسيق مع المنظّمة الدوليّة للملكيّة الفكريّة مهمّتها ابتكار آليّة لمنح عناوين المواقع وتأخذ في الحسبان البعد الدولي لشبكة الأنترنت وكيفيّة حل المنازعات بشأنها، وكان يقوم بهذه المهمّة قبل إنشاء المؤسّسة عام 198 لجنة منح الأرقام في الأنترنت وهي هيئة أناطت مؤسّسة الأنترنت بها مهمّة إدارة نظام منح عناوين الأنترنت حسب بروتوكول IP قبل أن تنتقل هذه المهمّة إلى مؤسّسة الأنترنت لمنح الأرقام و الأسماء.

(2) UNIX هو نظام تشغيل متعدّد المهام ومتعدد المستخدمين مصمّم لاستخدامه في الكومبيوتر المنزلي أو المكتبي باعتبار أنّ هذا النظام مكتوب بلغة (C) لذلك فهو أكثر قابليّة للنقل المعلوماتي من الأنظمة الأخرى، واللّغة (C) لغة برمجة عالية المستوى صمّمت أصلا لتعمل تحت النظام UNIX وهي مستخدمة في كتابة كافّة التطبيقات بعد أن يرى وضع مقاييسها من قبل المعهد القومي الأمريكي للمقاييس.

(3) ممدوح عبد الحميد عبد المطلب ، المرجع السابق، ص 1.

ويتنازع إمكانيّة تحديد مسار الأنترنت من عدمه رأيان، إذ يذهب رأي إلى أنّه لا يمكن تحديد مسار ارتكاب الجريمة وتكمن واجهة هذا الرّأي في أنّ شبكة الأنترنت ذات طبيعة مرنة بحيث أنّه حتّى وإن أمكن مستقبلا تحديد مسار الأنترنت، فإن ما يتمّ الحصول عليه في هذا الإطار إنّما هو دليل رقمي يحتاج إلى تكملته بأدلّة إثبات أخرى، فيما لو اقتصر الأمر على هذا الدّليل فإن الأمر يظلّ في حومة الشّك [1] ذلك أنّ ما يتمّ التوصّل إليه في الحقيقة من خلال الدّليل الرّقمي إنّما هو عنوان رقمي فقط (Adresse TP) وهذا لا يكفي في نسبة العمل الإجرامي إلى صاحب الحاسوب أو العنوان المذكور، إذ من الممكن ألاّ يكون هو مرتكب الجريمة كما لو كان جهاز الحاسوب مسروقا أو يكون أحد يستخدمه احتيالا أو يتمّ استخدام جهاز الحاسوب في مقهى الأنترنت، فمثل هذه الأمور تجعل من الصّعوبة بمكان الاعتماد على مسار حركة الأنترنت للتوصّل إلى تحديد شخص الجاني وإنّما قد يحتاج الأمر إلى دليل مادّي مكمّل للدليل الرّقمي، ويمكن التّأكيد على أنّه حتّى في الحالات الّتي تمّت فيها إدانة أشخاص أمام القضاء المقارن كان هناك دائما دليل مادّي يتمّ الاستناد إليه إلى جوار الدّليل الرّقمي، في حين يذهب الرّأي الآخر إلى القول بإمكانيّة تتبّع مسار الأنترنت ويمكن من خلال هذا التتبّع التّوصل إلى تحديد مسار العمل الإجرامي.

وتجدر الإشارة إلى أنّه في إطار فحص نظام الاتصال بالأنترنت كمصدر يمكن من خلاله البحث عن الدّليل الرّقمي، يتضمّن أيضا لزوم فحص الخادم أو الملقم "Serveur" وهو حاسوب ضخم مهمّته تحقيق حركة الاتصال بالمواقع و الصّفحات الّتي تتمّ استضافتها على هيئة رقميّة فيه، لذلك فإنّه يطلق على الخادم Lieu de stockage numérisées des données.

(1) خالد ممدوح إبراهيم، المرجع السّابق، ص 207 – 208.

* **تعاون مزودي الخدمة مع جهات التحقيق** : لما كان الدّليل الرّقمي قابع في البيئة التقنيّة ويتّسم بخصائصها، وهي خصائص تبنى على أساس الطبيعة المرنة الّتي عليها العالم الافتراضي، فإنّ للفاعل إمكانيّة إزالة الدّليل من على بعد باستخدام التقنيّة ذاتها، من أجل ذلك استلزم الأمر وضع إطار قانوني وهو نظام إلزام مزودي الخدمة[1] بحفظ المعطيات.

وهذا ما تضمنه قرار الجمعيّة العامّة للأمم المتّحدة رقم (63/55) المؤرّخ في 2001/01/22 و المتعلّق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجراميّة وذلك في الفقرة "و" من المادّة الأولى منه و الّتي ألزمت الدّول أن تسمح بحفظ المعطيات الإلكترونيّة المتعلّقة بالتحقيقات الجنائيّة الخاصّة وسرعة الوصول إليها وهو ما أكّده المشرّع الجزائري بموجب المادّة 10 من الفصل الرّابع في القانون 04/09 المتضمّن القواعد الخاصّة بالوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها تحت عنوان "التزامات مقدّمي الخدمات".

أوّلا : المقصود بمزوّدي الخدمات : حسب المادّة الأولى فقرة "ج" من اتفاقية بودابست فإنّ مزوّد الخدمة هو كلّ من يقوم بخدمات الإيصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات، وقد يكون جهة عامّة أو جهة خاصّة وقد يقدّم خدماته للجمهور أو لمجموعة من المستخدمين الّذين يشكّلون مجموعة مغلقة.

(1) أورد المشرّع الجزائري في المادّة 10 أنّه في إطار تطبيق أحكام هذا القانون (04/09) يتعيّن على مزوّدي الخدمة تقديم المساعدات للسلطات المكلّفة بالتحرّيات القضائيّة...بوضع المعطيات الّتي يتعيّن عليهم حفظه وفقا لأحكام المادّة 11 أدناه تحت تصرّف هذه السلطات.

ويعرف قانون حماية الحياة الخاصّة في مجال الاتصالات الإلكترونية في الولايات المتّحدة الأمريكيّة نوعين من مزوّدي الخدمة :

– **النّوع الأوّل** : مزوّد خدمة الاتصالات الإلكترونيّة ويقصد به كلّ من يقدّم خدمة إلى مستخدمي الشبكة و الّتي تتمثّل في تسهيل إرسال واستقبال الاتصالات الإلكترونيّة.

– **النّوع الثاني** : وهو مزوّد خدمة الحوسبة عن بعد ويقصد به كلّ من يقدّم للجمهور خدمة معالجة البيانات عن بعد بوسيلة من وسائل الاتصالات الإلكترونيّة.

وقد عرف المشرّع الجزائري مزوّد الخدمة (مقدّم الخدمة) بموجب الفقرة 06 من المادّة الثانيّة في القانون 04/09 بأنّه :

1 / كلّ كيان عام أو خاص يقدّم لمستعملي خدماته ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات.

2 / أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتيّة لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

وعلى هدي ذلك فإنّ المراسلة بالبريد الإلكتروني والّتي يتمّ استقبالها بواسطة مزود الخدمة الخاص بالمرسل إليه والّتي لم يطّلع عليها بعد، فإنّها تستقرّ في حالة تخزين إلكتروني وتكون في هذه المرحلة نسخة من الاتصال المخزّنة تتواجد فقط كإجراء أو وسيط مؤقّت في انتظار استقبال المرسل إليه لها من مزود الخدمة، وبمجرّد استلام المرسل إليه المراسلة بالبريد الإلكتروني فإنّ الاتصال يكون قد وصل إلى وجهته الأخيرة، وهنا يكون موقف مزوّد الخدمة يتراوح بين أمرين : إمّا أن يقوم بمسح تلك الرّسالة أو يقوم بالاحتفاظ بها [1].

---

(1) تجدر الإشارة إلى أنّه من الأهميّة بمكان التفرقة بين مصطلحي التحفّظ عل المعطيات La conservation des données و الاحتفاظ أو أرشفة المعطيات L archivage des données فرغم أنّ للكلمتين معنيين متجاورين في اللغة الشائعة لكن لهما معنى مختلف في اللغة المعلوماتيّة إذ أنّ عبارة يتحفّظ على المعطيات تعني حفظ معطيات سبق وجودها في شكل مخزّن وحمايتها من كلّ شيء يمكن أن يؤدّي إلى إتلافها أو تجريدها من صفتها أو حالتها الرّاهنة، في حين أنّ عبارة الاحتفاظ تعني حفظ المعطيات لدى حائزها بالنّسبة لمستقبل المعطيات الّتي في طور الإنتاج و التوالد ومعنى ذلك أنّ أرشفة المعطيات عبارة عن عمليّة تخزين للمعطيات على عكس التحفّظ عليها الّذي يعني النشاط الّذي يضمن للمعطيات سلامتها وسرّيتها.

ثانيا : التزامات مقدّمي الخدمة : ألزم المشرّع الجزائري مقدّمي الخدمات بحفظ المعطيات [1]، وذلك بتجميع المعطيات المعلوماتيّة وحفظها وحيازتها في أرشيف ووضعها في ترتيب معيّن في انتظار اتخاذ إجراءات قانونيّة محتملة أخرى كالتفتيش وغيره.

وما تجدر الإشارة إليه في هذا الإطار أنّه ليست أي معطيات معلوماتيّة محلّ اعتبار من المشرّع، بل حصر المشرّع الجزائري المعطيات المعلوماتيّة الواجب حفظها من طرف مزوّدي الخدمة في المعطيات المتعلّقة بحركة السّير (معطيات المرور)، وهي كلمة عرفها في المادّة الثانية من القانون 04/09 تلك المعطيات المتعلّقة بالاتصال عن طريق منظومة معلوماتيّة تنتجها هذه الأخيرة.

باعتبارها جزءا من حلقة الاتصالات، توضح مصدر الاتصال، الوجهة المرسل إليها والطريق الّذي يسلكه ووقت وتاريخ وحجم ومدّة الاتّصال، ونوع الخدمة، وقد حصر المشرّع معطيات المرور الّتي ألزم في المادّة 11 مزوّدي الخدمة بحفظها في :

1 – المعطيات الّتي تسمح بالتّعرّف على مستعملي الخدمة.

2 – المعطيات المتعلّقة بالتجهيزات الطرفية المستعملة للاتّصال.

3 – الخصائص التقنيّة وكذا تاريخ ووقت ومدّة كلّ اتّصال.

4 – المعطيات المتعلّقة بالخدمات التكميليّة المطلوبة أو المستعملة ومقدّميها.

5 – المعطيات الّتي تسمح بالتّعرّف على المرسل إليه الاتّصال وكذا عناوين المواقع المطلع عليها.

(1) آثر المشرّع الجزائري استعمال عبارة حفظ المعطيات في المادّة 11 بدل التحفظ على المعطيات وذلك عكس ما فعلت اتفاقية بودابست في المادّة 16 منها وهو بذلك إمّا أنّه لا يفرّق بين المصطلحين أو أنّه لا يقيم أهمّية لمسألة ضمان أمن المعطيات من خطر التغير أو التجريد من صفتها أو حالتها الرّاهنة.

وقد عرفت اتفاقية بودابست في مادّتها الأولى الفقرة "د" هذا النّوع من المعطيات بأنّها صنف من بيانات الحاسوب الّتي تشكّل محلاّ لنظام قانوني محدّد، حيث يتمّ توالد هذه المعطيات من الحواسيب عبر تسلسل حركة الاتصالات لتحديد سلك الاتصالات من مصدرها إلى الجهة المقصودة، وهي بذلك تشمل طائفة من المعطيات تتمثّل في مصدر الاتصال، ووجهته المقصودة خط السّير، وقت أو زمن الاتصال، حجم الاتصال، ومدّته ونوع الخدمة المؤدّاة.

وبما أنّ حفظ المعطيات إجراء وقتي واحترام للحق في الخصوصيّة فإن المشرّع الجزائري وضع التزاما على مزودي الخدمات بإزالة المعطيات الّتي يقومون بتخزينها بعد سنة من تاريخ التسجيل [1]، وعلى غرار المشرّع الجزائري نجد المشرّع الفرنسي حرص بدوره في نطاق التخزين التلقائي للمعطيات المتعلّقة بالاتصالات الإلكترونيّة.

وذلك بموجب المادّة 32 قانون البريد و الاتصالات الإلكترونيّة المضافة بموجب المادّة 29 من القانون رقم 1062/2001 والمعدّلة بالمادّة 20 من القانون 239/2003 المؤرّخ في 2003/03/18 المتعلّق بالأمن الداخلي على ضرورة مسح المعطيات المخزّنة بعد الاحتفاظ بها لمدّة أقصاها سنة إذا دعت مقتضيات البحث و التحقيق والمتابعة القضائيّة ذلك.

وقد رتّب المشرّع الجزائري مسؤوليّة إداريّة وأخرى جزائيّة على تقاعس مزوّدي الخدمة عن حفظ المعطيات المذكورة، [2] لإمكانيّة أن يشكّل هذا التقصير عرقلة للسير العادي للتحرّيات القضائيّة.

واسترشادا بما ذكر فإنّ مزوّدي لخدمة الأنترنت يعتبرون مصدرا لجهات البحث و التحقيق للحصول على الدّليل الرّقمي من خلال المعطيات الّتي يكونون ملزمين بحفظها وملزمين في نفس الوقت بوضعها تحت تصرّف هذه الجهات إذا ما تمّ طلبها.

(1) المادّة 11 من القانون (04/09) "...تحدّد مدّة حفظ المعطيات المذكورة في هذه المادّة بسنة واحدة ابتداء من تاريخ التسجيل"

(2) المادّة 11 الفقرة الأخيرة "...يعاقب الشخص الطبيعي بالحبس من 06 أشهر إلى 05 سنوات وبغرامة من 50.000 دج ويعاقب الشخص المعنوي وفقا للقواعد المقرّرة في قانون العقوبات".

المطلب الثاني : مشروعيّة الدّليل الرّقمي.

تعرف المشروعيّة بأنّها التوافق والتقيّد بأحكام القانون في إطاره ومضمونه العام، فهي تهدف إلى تقرير ضمانة أساسية وجديرة للأفراد لحماية حرّيتهم وحقوقهم الشّخصية ضدّ تعسّف السلطة، ومن تطاول عليها في غير الحالات الّتي رخّص فيها القانون بذلك، من أجل حماية النظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته، لذلك فإنّه لصحّة الإجراءات الّتي تقوم بها جهة التحقيق أن يكون مبدأ المشروعيّة من أجل أن تثمر على دليل صحيح وسليم يعوّل عليه القضاء في أحكامه، فلا شكّ أنّ مبدأ شرعيّة الجرائم والعقوبات الّتي يستقيم عليها بنيان القانون الجنائي الموضوعي ينعكس على قواعد الإثبات الجنائي ويفرض خضوعها هي الأخرى لمبدأ المشروعيّة، والّتي تستلزم عدم قبول أي دليل يكون البحث عنه أو الحصول عليه قد تمّ بطريقة غير مشروعة، وتعدّ مسألة قبول الدّليل الجنائي بصفة عامّة الخطوة الأولى الّتي يتخذها القاضي الجزائي اتجاهه وذلك بعد التنقيب عنه وقبل اخضاعه لتقديره، وقبول الدّليل على هذا النّحو يتّسع ويضيق تبعا للمبادئ الّتي تقوم عليها أنظمة الإثبات السائدة و الحقيقة أنّ مشروعيّة الدّليل الرّقمي هي مشروعية وجود ومشروعيّة حصول.

* **مشروعيّة وجود الدليل الرّقمي** : ويقصد بمشروعية وجود الدّليل الرّقمي أن يعترف المشرّع بهذا الدّليل من خلال تصنيفه في قائمة الأدلّة القانونيّة الّتي يجيز القانون فيها للقاضي الاستناد إليه في تكوين عقيدته، ولعلّ المعيار الّذي يتحدّد على أساسه موقف القوانين فيما يتعلّق بسلطة القاضي الجزائي في قبول الدّليل الرّقمي يتمثّل في طبيعة نظام الإثبات السّائد في الدّولة إذ تختلف النّظم القانونيّة في موقفها من حيث الأدلّة الّتي يمكن قبولها في الإثبات.

*** موقف المشرّع الجزائري من الدّليل الرّقمي :**

لقد عرفت التشريعات الإجرائيّة الجزائيّة نظامين رئيسيين للإثبات هما :

* نظام الإثبات المقيّد وفيه يقوم المشرّع بتحديد أدلّة الإثبات وكذا قوّة الإثباتيّة لكل دليل من الأدلّة بناءا على قناعة المشرّع بها وهو ما يعرف بنظام الأدلّة القانونيّة.

* نظام الإثبات الحر والّذي يقوم على أساس حرّية الإثبات فلا يقوم المشرّع بتحديد الأدلّة بل يكون للقاضي دور إيجابي في البحث عن الأدلّة وتقدير قوّتها الثبوتيّة حسب قناعته بها، فلا يلزمه القانون بأدلّة للاستناد إليها في تكوين قناعته فله أن يبني هذه القناعة على أي دليل.

وفي هذا الصّدد فإنّ المشرّع الجزائري وكغيره من التشريعات المنتميّة إلى النظام الحر لا نجده قد أفرد نصوص خاصّة تحظر على القاضي مقدّما قبول أو عدم قبول أي دليل بما في ذلك الدّليل الرّقمي وهو أمر منطقي طالما أنّ المشرّع الجزائري يستند لمبدأ حريّة الإثبات. حيث يتضمّن القانون 04/09 المتضمّن القواعد الخاصّة بالوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام و الاتصال، ومنها أنّ الأصل في الأدلّة مشروعيّة وجودها ومن تمّ فإنّ الدّليل الرّقمي سيكون مشروعا من حيث الوجود ومن جهة أخرى فإنّه وطبقا لمبدأ الشّرعيّة الإجرائيّة فلا يكون الدّليل مقبولا في عمليّة الإثبات إلاّ إذا كان مشروعا لأنّ القاضي لا يقدر إلاّ الدّليل المقبول ولا يكون كذلك إلاّ إذا كان مشروعا.

* **مشروعيّة الحصول على الدليل الرّقمي** : لأنه من الضّروري أن يتم رسم ضوابط وأطر معيّنة يتعيّن أن تمارس في نطاقها عمليّة البحث عن الأدلّة وتحصيلها والتحقّق فيها بحيث لا تنحرف عن الغرض الّذي يبتغيه المشرّع من وراءها وهو الوصول إلى الحقيقة الفعليّة في الدّعوى فهي الهدف الإسمي لقانون الإجراءات الجزائيّة.

فإنّه من المقرّر أنّ الإدانة في أي جريمة لا بدّ من أن تكون مبنيّة على أدلّة مشروعة تمّ الحصول عليها وفق قواعد الأخلاق واحترام القانون من طرف الجهة المختصّة بجمع الدّليل الجزائي بما يتضمّنه من أدلّة مستخرجة من وسائل إلكترونيّة، ولا يكون مشروعا إلاّ إذا أجرى التنقيب عنه أو الحصول عليه أو كانت عمليّة تقديمه إلى القضاء أو إقامته أمامه بالطرق الّتي رسمها القانون، فمتى ما تمّ الحصول على الدليل خارج هذه القواعد القانونيّة فلا يعتدّ بقيمته مهما كانت دلالته الحقيقيّة وذلك لعدم مشروعيّة وعلى هذا الأساس فإنّ إجراءات جمع الأدلّة الرّقميّة المتحصلة من الوسائل الإلكترونيّة إذا خالفت القواعد الإجرائيّة الّتي تنظّم كيفيّة الحصول عليها فإنّها تكون باطلة وبالتّالي بطلان الدّليل المستمد منها ولا تصلح لأنّ تكون أدلّة تبنى عليها الإدانة في المواد الجنائيّة.

وفي إطار مشروعيّة الأدلّة الرّقميّة نجد أن قانون الإجراءات الجنائيّة الفرنسي رغم أنّه يتضمّن نصوص تتعلّق بمبدأ الأمانة و النزاهة في البحث عن الحقيقة إلاّ أنّ الفقه و القضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليديّة أم في مجال التنقيب في الجرائم المعلوماتيّة، ويشير الرأي الفقهي الفرنسي إلى أنّ القضاء قبل استخدام الوسائل العلميّة الحديثة في عمليّة البحث و التحرّي عن الجرائم تحت تحفّظ أن يتمّ الحصول على الأدلّة الجنائيّة ومن بينها الأدلّة الرّقميّة بطريقة شرعيّة ونزيهة [1]. وقد قضي في هولندا أنّه إذا كانت بيانات الحاسوب المسجّلة في ملفات الشّرطة غير قانونية فذلك يؤدّي إلى نتيجة مؤدّاها ضرورة محو هذه البيانات وعدم إمكانيّة استخدامها كدليل جنائي بسبب مبدأ استبعاد الأدلّة القانونيّة.

(1) علي محمّد حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت، عالم الكتب الحديثة، الأردن، ص186.

ومن قبيل الأدلّة غير المشروعة الحصول على دليل رقمي من خلال إجراء مراقبة الاتصالات دون أن يكون محلا لإذن من السلطة القضائيّة المختصّة، أو اتخاذ ترتيبات تقنيّة من أجل تفتيش منظومة معلوماتيّة تؤدّي إلى المساس بالحياة الخاصّة للغير أو ممارسة الإكراه المادّي أو المعنوي في مواجهة المشتبه فيه من أجل فك شيفرة نظام من النظم المعلوماتيّة أو التحريض على ارتكاب الجريمة غير الطرق الضبطية [1] وبعض الطرق غير المشروعة أيضا كاستخدام التدليس أو الغش أو الخداع للحصول على أدلّة إلكترونيّة. ولقد صادقت لجنة الوزراء التابعة للمجلس العربي في 1981/01/28 على اتفاقية خاصّة بحماية الأشخاص في مواجهة مخاطر المعالجة الآليّة للبيانات ذات الطبيعة الشّخصيّة، ومن المحاور المهمّة الّتي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة ومستمدّة بطرق مشروعة وعدم إفشاءها أو استعمالها في غير الأغراض المخصّصة لها، كما أنّ للشخص المعني الحق في التعرّف و الاطلاع على البيانات المسجّلة المتعلّقة به وتصحيحها وتعديلها ومناقضتها ومحوها إذا كانت باطلة [2].

ولقد وضعت الدساتير و القوانين الإجرائيّة نصوص تضمّن ضوابط لشرعيّة الإجراءات الماسّة بالحرّية، ومن تمّ مخالفة هذه النصوص في استخلاص الدّليل يصبح دّليلا بالمشروعيّة والقول و بذلك يهدر قيمته، فمشروعيّة الدّليل تتطلّب صفة في مضمونه وأن يكون هذا المضمون قد تمّ الحصول عليه بطرق مشروعة تدلّ على الأمانة و النّزاهة من حيث طرق الحصول عليه، والحقيقة أنّ مشروعيّة الدّليل تعدّ قيدا وخطا فاصلا بين حق الدّولة في توقيع العقاب لضمان أمن واستقرار المجتمع من جهة، وبين ضمان حقوق الأفراد وحرّياتهم من جهة أخرى.

(1) علي محمّد حسن الطوالبة، المرجع السابق، ص189.

(2) مشار إليه لدى رشيدة بوكر.

المطلب الثالث : موقف المشرّع الجزائري من الدّليل الرّقمي في مجال الإثبات الجزائي.

إنّ الإثبات في المواد الجنائيّة هو النتيجة الّتي تتحقّق باستعمال وسائله وطرقه المختلفة للوصول إلى الدليل الّذي يستعين به القاضي لاستخلاص حقيقة الوقائع المعروضة عليه وإعمال حكم القانون عليها، ويعني ذلك أنّ موضوع الإثبات هو الوقائع وليس القانون[1].

وبالتالي فإنّ الإثبات الجزائي هو كلّ ما يؤدّي إلى كشف غموض الجريمة وإقامة الدّليل على وقوعها والتّأكد من أنّ المتّهم هو مرتكب الجريمة بالفعل ووجود الدّليل على ذلك، ويعتبر الدّليل الوسيلة القانونيّة الّتي يستعين بها القاضي للوصول إلى الحقيقة وكشف غموض الجريمة ونسبتها إلى المتّهم. ولقد ذهب الفقه الإجرائي إلى وضع نظامين إجرائيين في مجال الإثبات الجزائي يختلفان فيما بينهما من حيث الأسس الّتي يقوم عليها كلّ واحد منهما وهذه الأنظمة هي :

نظام الإثبات القانوني أو المقيّد وفيه يحدّد القانون الأدلّة الّتي يجوز الأخذ بها و الاستناد عليها و الثّاني هو نظام الإثبات الحر أو المطلق وفيه لا يقيّد القانون القاضي بأدلّة معيّنة في إثبات الواقعة وله أن يقتنع بأي دليل يعرض عليه.

فأي من هذين النظامين أخذ به الشرع الجزائري وما أثّر ذلك على مسألة الإثبات بالدّليل الرّقمي في الجريمة المعلوماتيّة.

(1) أشرف عبد القادر قنديل، النظريّة العامّة للبحث الجنائي وأثرها في عقيدة القاضي، المرجع السابق، ص212.

*** أنظمة الإثبات الجزائي :**

يوجد في مجال الإثبات الجزائي نظامان :

1 / نظام الإثبات المقيّد أو نظام الأدلّة القانونيّة : Système de la preuve légale مفاد هذا النّظام هو أن يتقيّد القاضي في حكمه سواء بالإدانة أو البراءة بأنواع معيّنة من الأدلّة طبقا لما يرسمه التشريع، فالفكرة الأساسيّة لهذا النظام تقوم على أنّ المشرّع هو الّذي يكون له الدّور الأساسي في الإثبات، وذلك من خلال التحديد المسبق للأدلّة المقدّمة في الدّعوى و الّتي يستند إليها القاضي الجزائي في حكمه ولا سبيل له إلى الاستناد إلى أي دليل لم ينص عليه القانون صراحة ضمن أدلّة الإثبات.

وفي هذا النظام لا يكون للقاضي الجزائي دور في القيمة الاقناعيّة للدليل فيتقيّد القاضي وفق هذا النظام بالأدلّة الّتي رسمها الشرع سلفا دون أن يعمل فيها ميوله أو اقتناعه الشخصي بشأنها، إذ يقوم اقتناع الشّرع مقام اقتناع القاضي وعليه فإنّ اليقين القانوني يقوم اساسا على افتراض صحّة الدّليل بغض النظر عن حقيقة الواقع واختلاف ظروف الدّعوى، ويتجلّى دور القاضي في هذا النّظام كمطبق فحسب من حيث مراعاة توافر الدّليل وشروطه، بحيث إذا لم تتوافر هذه الشروط وتلك الآليات الّتي يتطلبها القانون في الدّليل فإنّ القاضي لا يستطيع أن يحكم بالإدانة حتّى ولو كان اقتناعه يقينا بارتكاب المتّهم للجريمة المسندة إليه.

ويقوم هذا النّظام على مجموعة من الخصائص أهمّها أنّ دور القاضي الجزائي سلبي، ذلك أنّ الإثبات الجنائي في هذا النّظام يخضع لقواعد شكلية تتضح في سلطة القاضي المقيّدة في تقدير عناصر الإثبات الّتي يستمدّ منها اقتناعه وتقدير قيمة الأدلّة المعروضة عليه، كما يتميّز أيضا هذا النّظام بالدّور الإيجابي للمشرّع في عمليّة الإثبات من حيث أنّه هو الّذي ينظم قبول الأدلّة سواء عن طريق تعيين الأدلّة المقبولة للحكم بالإدانة، أو باستبعاد أدلّة أخرى أو بإخضاع كلّ دليل لشروط معيّنة، وأنّه هو الّذي يحدّد القيمة الإقناعيّة لكلّ دليل بأن يعطي لبعض الأدلّة الحجية الأقوى دون الأدلّة الأخرى.

وقد أعاب الفقه الجنائي على هذا النّظام أنّه أخرج القاضي من وظيفته الطبيعيّة الّتي تتمثل في فحصه للدليل وتقديره، ومن تمّ تكوين اقتناعه الشخصي وأقحم المشرّع في وظيفة القاضي وإملاء أدلّة الإدانة عليه على سبيل الحصر.

و من العيوب الّتي واجهها هذا النظام أيضا أنّه قام بتقنين اليقين في نصوص قانونيّة محدّدة سلفا رغم أنّ اليقين مسألة يطرحها الواقع ويقدّرها القاضي.

2 / نظام الإثبات الحر أو نظام الاقتناع الشخصي للقاضي الجزائي

وفقا لهذا النظام لا يرسم القانون طرقا محدّدة للإثبات، إذ يتمتّع القاضي الجزائي في هذا النظام بحرّية مطلقة في تكوين اعتقاده من أي دليل يطرح أمامه [1] ومن ثمّة فإنّ هذا النظام يقوم على خاصتين أساسيتين :

– الخاصية الأوّلى تتمثل في إطلاق حرّية الإثبات للقاضي الجزائي انطلاقا من موضوع الإثبات في المسائل الجزائيّة الدي يتعلّق بوقائع مادّية ونفسيّة لا يصلح لإثباتها تحديد مجموعة من القواعد الإثباتيّة مسبقا، بل إنّ الإثبات في هذه المسائل يكون بكافّة طرق الإثبات.

– والخاصّية الثانيّة تتمثل في حرّية القاضي الجزائي في الاقتناع بالدّليل المطروح عليه في جلسة المحاكمة دون أن يكون عليه أي رقيب سوى ضميره ودون أن يكون مطالبا ببيان سبب اقتناعه بدليل آخر.

وعلى هذا الأساس يكون للقاضي الجزائي دور فعال حيال الدّليل الّذي يوضع أمامه، وله في مقابل ذلك كافّة الصلاحيات الّتي تمكّنه من اتخاذ الإجراء الّذي يراه مناسبا ويخدم لإظهار الحقيقة.

وعقيدة القاضي هي نتاج وزن الأدلّة المطروحة بالدّعوى الجزائيّة أمامه والّذي يقوم بقبول الأدلّة الّتي قدّمها أطراف الدّعوى، فلا يوجد حظر على الأدلّة إلاّ إذا كانت غير مشروعة، وقد ذهب البعض [2] إلى القول أنّ الاقتناع الشخصي للقاضي الجزائي هو الضمانة الحقيقيّة لضبط ميزان العدالة.

---

(1) محمّد عبد الغريب، حرّية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام، المرجع السابق، ص 8.
(2) أشرف عبد القادر قنديل، المرجع السابق، ص 213.

*** موقف الشرع الجزائي الجزائري من أنظمة الإثبات وأثر ذلك في إثبات الجريمة المعلوماتيّة.**

نصّت المادّة 212 من قانون الإجراءات الجزائية على أنّه يجوز إثبات الجرائم بأي طريق من طرق الإثبات وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ..." كما نصّت المادّة 307 من قانون الإجراءات الجزائيّة أيضا أنّ القانون لا يطلب من القضاة أن يقدّموا حسابا عن الوسائل الّتي قد وصلوا بها إلى تكوين اقتناعهم وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلّة المسندة للمتّهم....."

ومن خلال هذين النّصين القانونيين يتضح جليا أنّ المشرّع الجزائري قد تبنّى كقاعدة عامّة نظام الاقتناع الشخصي للقاضي الجزائي، إلاّ واستثناء نجده أخذ أيضا بنظام الأدلّة القانونيّة في إثبات بعض الجرائم أين اشترط لإثباتها أدلّة قانونيّة محدّدة مسبقا وعلى سبيل الحصر [1].

وبتحليل المادّة 212 من قانون الإجراءات الجزائيّة نجدها تكرس قاعدتين تكمل إحداهما الأخرى، قاعدة الاقتناع الحر للقاضي الجزائي من جهة وقاعدة حرّية اختيار وسائل الإثبات الجزائي من جهة أخرى.

وإذا كان الدّليل الرّقمي ذو الأصالة العلميّة هو الأوفر و الأنسب في إثبات الجريمة المعلوماتيّة فما مدى إمكانيّة إعمال القاضي الجزائي لمبدأ الاقتناع الشخصي حيال هذا الدّليل طبقا لأحكام المادّة 212 من قانون الإجراءات الجزائيّة.

(1) أنظر المادّتين 341، 339 من قانون العقوبات الجزائري.

*** مفهوم الاقتناع الشخصي للقاضي الجنائي :**

إن الاقتناع الشخصي للقاضي الجزائي هو عبارة عن نشاط عقلي لا يتدخّل فيه المشرّع ليبيّن للقاضي كيفيّة ممارسته وترجمته إلى واقع منتج ولا يرسم له كيف يشكل معادلاته الذّهنيّة في مجال تقدير الأدلّة ليصل من خلالها إلى الحقيقة.

1 / تعريف مبدأ الاقتناع الشخصي : يعرّف فقهاء القانون الجزائي الاقتناع بأنّه حالة ذهنيّة ذاتيّة تستنتج من الوقائع المعروضة على بساط البحث، أو بمعنى آخر هو حالة ذهنيّة ذو خاصّيّة ذاتيّة نتيجة تفاعل ضمير القاضي وأدلّة الإثبات المطروحة والّتي يثيرها الخصوم إمّا لإثبات أو إنكار إتّهام [1]، كما عرّف الاقتناع الشخصي أيضا بأنّه حالة تطرد الشّك و الاحتمال، ويجد هذا المبدأ مناخه الطبيعي الملائم في ظل مذهب الإثبات الحر الّذي لا يضع تقديرا مسبقا لأدلّة معيّنة لا يمكن الوصول بغيرها إلى اليقين [2]، ومن خلال هذا التعريف فإنّ الاقتناع الشخصي للقاضي الجزائي يتميّز بخاصّيتين هما :

-الخاصية الأولى تتمثل في أنّه حالة ذهنيّة مبنيّة على الاحتمال وأنّ العبرة ليست بكثر الأدلّة وإنّما بما تتركه من أثر في نفسيّة القاضي، لأنّ هذا التأثير سيلعب دورا في تحديد مصير الدّعوى الجزائيّة بالإدانة أو البراءة.

- والخاصّية الثانيّة تتمثّل في أنّ القاضي حر في أن يأخذ عقيدته أو اقتناعه من أي دليل لكن يجب التأكد هنا أنّ حريّة الإثبات في المسائل الجزائيّة ليست خاصّيّة يتميّز بها القاضي الجزائي لتتسع سلطته في الإدانة أو البراءة.

(1) نصر الدّين ماروك، النظريّة العامّة للإثبات الجنائي، الجزء الأوّل، ص 620.

(2) زبدة مسعود، الاقتناع الشخصي للقاضي الجزائي، المؤسّسة الوطنيّة للكتاب، الطبعة الأول، ص 08.

ولكنّها ترجع إلى الإثبات في المسائل الجزائيّة والوصول إلى الدّليل مسألة جد صعبة وذلك لاختلاف أساليب ارتكاب الجريمة وأنّ المجرم عادة ما يسعى إلى إخفاء جريمته، لذلك فالبحث عن الحقيقة من خلال الأدلّة الجزائيّة لا يكون إلاّ عن طريق منح القاضي الجزائي هامشا عن الحريّة لمناقشة الدّليل الّذي يراه مناسبا في إثبات الجريمة.

2 / وسائل تكوين الاقتناع الشخصي للقاضي الجزائي :

إنّ الجهد الاستنباطي الّذي يبذله القاضي من خلال نشاطه العقلي المكوّن لقناعته والّذي ينصرف إلى فرز الحقيقة من الدّليل محلّ تقديره يرتكز فيه القاضي على :

– قبوله جميع الأدلّة المطروحة أمامه في الجلسة ولا يحظر على القاضي أو يفرض عليه دليل محدّد ولا يتقيّد إلاّ بقيد مشروعيّة الدّليل وأنّه قد تمّ طرحه للمناقشة بالجلسة.

– أن يقوم القاضي بوزن كلّ دليل على حدى عن باقي الأدلّة المطروحة أمامه وله أن يهدر أي دليل مهما كانت قيمته طالما أنّه لم يطمئنّ إليه.

– سلطة القاضي في تنسيق الأدلّة المطروحة أمامه ومساندة الأدلّة لبعضها أو ما يعرف بتساند الأدلّة.

*** سلطة القاضي الجزائي في تقدير الدليل الرّقمي :**

إنّ الأصالة العلميّة للدليل الرّقمي جعلت من سلطة القاضي في تقدير هذا الدّليل محل خلاف فقهي، إذ أنّ هناك من يرى أنّ الدّليل العلمي ومنه الدّليل الرّقمي له قوّته الثبوتيّة الملزمة حتّى للقاضي، مستندين في رأيهم إلى أنّ هذا الدّليل يتّسم بالدّقة العلميّة الّتي يبلغ معها إلى درجة اليقين، وهناك من يرى أنّ مبدأ حرّية القاضي في الاقتناع يجب أن يبسط سلطاته على كلّ الأدلّة دون استثناء حتّى على الدّليل الرّقمي، معتبرين أنّ إعطاء الدّليل الرّقمي قوّة ثبوتيّة لا يستطيع القاضي مناقشتها أو تقديرها يعدّ بمثابة رجوع إلى مذهب الإثبات القانوني (المقيّد).

والمشرّع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الجرائم الّتي قد يتطلّب إثباتها دليلا معيّنا، ومنح القاضي الجزائي سلطة تقدير الدّليل والحريّة في تكوين اقتناعه من أي دليل يطمئنّ إليه، فهل تنصرف هذه السّلطة التقديريّة الّتي يتمتّع بها القاضي الجزائي إلى الدليل الرّقمي المستخرج من الوسائل الإلكترونيّة ؟

لقد سبق الذّكر أنّ الجريمة المعلوماتيّة في القانون الجزائري تشمل الأفعال الماسّة بأنظمة المعالجة الآليّة للمعطيات وكذا كل جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتيّة أو نظام للاتصالات الإلكترونيّة، وهذه الأخيرة قد تنصرف إلى جرائم تقليديّة منصوص عليها في قانون العقوبات يمكن حسب طبيعتها أن ترتكب بواسطة منظومة معلوماتيّة.

وهذا يعني أنّ الإجرام المعلوماتي قد يأخذ وصف الجناية أو الجنحة أو المخالفة حسب وصف الجرم المرتكب بواسطة المنظومة المعلوماتيّة، وإن كان مبدأ الاقتناع القضائي عام النطاق لدى كافة أنواع المحاكم الجزائيّة سواء كانت محاكم الجنايات أم الجنح أم المخالفات [1] فإنّ قواعد بيان عناصر تقدير الدليل تختلف حسب اختلاف وصف الفعل المجرم، فإذا كان الفعل من طبيعة جنائيّة فإنّ محكمة الجنايات تتمتّع بسلطة تقديريّة مطلقة في مواجهة الأدلّة المعروضة أمامها وتصدر أحكامها دون أن يكون قضاتها مطالبين بتسبيب أحكامهم ولا رقابة لجهات الطعن عليهم، أمّا إذا أخذ الفعل المجرم وصف الجنحة فإنّ قاضي الجنح مطالب بعرض وبيان تقديره للدليل المعروض عليه من خلال تسبيب حكمه، والّذي يكون محلّ رقابة من جهات الطعن [2]، لهذا فهو مطالب باحترام القواعد العامّة المنظّمة للقوّة الثبوتيّة لكلّ وسيلة من وسائل الإثبات والّتي قد تأخذ شكل محاضر معدّة بمناسبة تفتيش أو اعتراض مراسلات أو شكل تقرير خبرة محرّر بمناسبة معاينة وفحص الأدلّة المضبوطة من جهاز الإعلام الآلي أو دعامات إلكترونيّة.

فأمّا ما يتعلّق بالمحاضر فإنّ الشرع اعتبر أنّها كقاعدة عامّة مجرّد استدلالات ما لم ينصّ القانون على خلاف ذلك، ولا يكون للمحضر أي قوّة إثبات إلاّ إذا كان صحيحا من حيث الشّكل، وأنّه قد تمّ إعداده من طرف واضعه أثناء مباشرة أعمال وظيفته، ويكون مضمونه ما يدخل في اختصاصه [3]، إلاّ أنّ المحاضر الّتي يخول القانون لضباط الشرطة القضائيّة إعدادها بنص خاص لإثبات جنح معيّنة فإنّ هذه المحاضر تكون لها حجتها ما لم يدحضها دليل عكسي[4].

(1) وإن كان المشرّع الجزائري لم يحدد ذلك صراحة في المواد المقرّرة لهذا المبدأ راجع المواد 212.307 من قانون الإجراءات الجزائيّة بخلاف المشرّع الفرنسي فقد صرّح ذلك صراحة حيث خصّص المادّة (353-1) من قانون الإجراءات الجزائيّة لتطبيق المبدأ أمام محكمة الجنايات كما نصّت المادّة (427) من ذات القانون على تطبيق هذا المبدأ بالنسبة لمحاكم الجنح.

(2) أنظر المادّة 379 من قانون الإجراءات الجزائيّة الجزائري والّتي تقابلها المادّتين 485-593 من قانون الإجراءات الجزائيّة الفرنسي.

(3) أنظر المادّة 214 من قانون الإجراءات الجزائيّة.

(4) أنظر المادّة 216 من قانون الإجراءات الجزائيّة.

أمّا بالنسبة لتقارير الخبرة فإنّ المحكمة العليا ذهبت للقول أنّ الخبرة شأنها شأن باقي أدلّة الإثبات تخضع للسلطة التقديريّة لقاضي الموضوع [1]، وهذا المعنى تؤكّده المادّة 215 من قانون الإجراءات الجزائيّة الّتي تنصّ على أنّه : "لا تعتبر التقارير المثبتة للجنايات أو الجنح إلاّ مجرّد استدلالات...".

لكن الطبيعة العلميّة و التقنيّة للجريمة المعلوماتيّة غالبا ما تفرض على القاضي الاستناد في تكوين اقتناعه على الخبرة الفنيّة و التقيّد بالنتيجة المتوصّل إليها الخبير في تقرير خبرته ولا يمكنه طرحها واستبعادها إلاّ إذا قدّر أن ما تحمله من أدلّة لا يتوافق مع ظروف وملابسات الواقعة أو تتناقض مع الحقيقة العلميّة، فحسب الاجتهاد القضائي أنّه أحيانا ما تكون الخبرة وحدها كافيّة بالنسبة للقاضي عندما يكون مطالبا للفصل في وقائع ذات طابع تقني دون أن يحتاج إلى مناقشتها [2].

وفي الأخير يمكن القول أنّ إساءة استخدام التقنيّة المعلوماتيّة تعدّ من الموضوعات الّتي فرضت نفسها على المستوى الوطني و الدولي على حد سواء، وأجبرت التشريع الجزائي على التدخّل من أجل مواجهتها بتشريعات حاسمة لمكافحتها ومعاقبة مرتكبيها، إلاّ أنّ ذلك يبدو غير كاف لتحقيق هذا الهدف، فعلى المستوى الإجرائي تثير الجريمة المعلوماتيّة مشكلات عدّة بدءا من مرحلة الاستدلال حتّى صدور الحكم الجزائي لا سيما فيما يتعلّق بإثبات الجريمة المعلوماتيّة ومدى صلاحيّة الدّليل الرّقمي للإثبات ومدى شرعيّة الأدلّة المتحصّل عليها عبر التقنيّة المعلوماتيّة وحجيّتها أمام القاضي الجزائي، لذلك خصّص هذا الفصل لتناول هذه المسائل من خلال تحديد الأجهزة المكلّفة بالبحث و التحرّي عن الجريمة المعلوماتيّة، ثمّ التعريف بالخصائص الّتي يتميّز بها التحقيق و المحققون فيها.

ثمّ بعد ذلك تمّ البحث في الدّليل المناسب لإثبات هذا النوع من الجرائم وهو ما يعرف بالدليل الرّقمي أين تمّ توضيح مفهومه وتحديد أشكاله ومصادر الحصول عليه، كما تمّ معالجة القواعد الإجرائيّة المستعملة في التحقيق من أجل استخلاصه وماهي الصعوبات والمعوقات الّتي تواجه القائمين على ذلك، كما تمّ التناول في هذا الفصل مسألة ضمانات المشتبه فيه أثناء ممارسة إجراءات الحصول على الدّليل الرّقمي وأثرها على الحق في الخصوصيّة، وأخيرا تمّ بحث القيمة القانونيّة للدليل الرّقمي في مجال الإثبات الجزائي و ما هو موقف المشرّع الجزائري من هذا الدّليل.

---

(1) ورد في مضمون قرار المحكمة العليا المؤرّخ في 1995/07/11 المنشور في نشرة القضاء رقم 58 لسنة 2006، ص 170.

(2) قرار المحكمة العليا الغرفة الجنائيّة مؤرّخ في 2002/06/04 نشرة القضاة رقم 58 لسنة 2006، ص 255.

الخاتمة

إن مفهوم الجرائم المعلوماتية ينصرف إلى الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات، والتي تستهدف بشكل خاص المعلومات المختلفة في البيئة الرقمية، بالإضافة إلى كل جريمة ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية، وهذه الأخيرة في الغالب ما تكون جرائم تقليدية.

و من أهم مميزات جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، أنّها تنصب على محل من نوع خاص يختلف تماما على محل الجرائم التقليدية، فهذه الجرائم تستهدف المساس بالمعلومات الإلكترونية المتواجدة في البيئة الرقمية على هيئة إشارات ونبضات غير مرئية تنساب عبر أجزاء النظام المعلوماتي وشبكات الاتصال العالمية.

وقد تبين لي أنه ونظرا لكون النصوص الجزائية العقابية إنما وضعت للتعامل مع جرائم تنصب على محل مادي ملموس، فإن الأمر قد تبعه قصور أو عجز هذه النصوص القانونية عن توفير الحماية الجزائية لمثل محل الجرائم المعلوماتية فكان ذلك من دواعي تدخل المشرع إلى إصدار نصوص جزائية تجرم بحق الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات وهو ما يقتضيه مبدأ الشرعية الموضوعية القائم على التفسير الضيق للنصوص القانونية العقابية وعدم جواز القياس.

وقد توصلت أيضا إلى أن هذا القصور لم يعتر النصوص الموضوعية فقط ولم يقف عند الشق الموضوعي للقانون الجزائي، بل امتد تأثير التقنية المعلوماتية إلى الشق الإجرائي للقانون الجزائي، فقد أثارت هذه التقنية الحديثة العديد من الإشكالات في نطاقها، ذلك أن نصوص قانون الإجراءات الجزائية إنما وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجزائي في الاقتناع.

لذلك فإن الطبيعة الخاصة للجريمة المعلوماتية دعت المشرع إلى إعادة تقييم بعض القواعد الإجرائية المتاحة في استخلاص الدليل كالتفتيش والضبط وجعلها صائغة الاستعمال في مجال البيئة الرقمية، وهو ما كان فعلا بموجب القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فضلا عن استحداث نوع من قواعد إجرائية أخرى تتلاءم مع الطبيعة الرقمية التي يكون عليها الدليل المناسب في إثبات هذا النوع من الجرائم كاعتراض المراسلات والمراقبة الإلكترونية .

وقد تبين معنا كذلك أن الدليل المناسب والأوفر في إثبات الجريمة المعلوماتية هو الدليل الرقمي والذي هو عبارة عن معلومات مخزنة في النظم المعلوماتية في شكل نبضات مغناطيسية أو كهربائية من الممكن من الناحية التقنية استخلاصه من البيئة الرقمية التي يتواجد بها، وتجميعه باستخدام برامج وتطبيقات تقنية، ليظهر بعد ذلك في شكل مخرجات إلكترونية أو حتى ورقية بعد طبعه.

كما أظهر البحث أيضا أن عملية استخلاص الدليل الرقمي سواء بالطرق الإجرائية التقليدية أو المستحدثة ليس من السهولة بما كان، إذ تعوقها في غالب الأحيان صعوبات تتعلق إما بالطبيعة التكوينية للدليل الرقمي أو بالعامل البشري.

إن الدليل الرقمي على ضوء ما أسفرت عليه التطورات التقنية في مجال المعلوماتية لا يغني عنه أن يكون مشروعا، وذلك بأن يتم الحصول عليه بالطرق القانونية وأن يقدم للمحكمة على نفس الهيئة التي تم جمعه عليها، لأن لا يطرأ عليه أي تغيير أو تحريف خلال فترة حفظه.

إن الأدلة الرقمية وإن كانت تتمتع بقيمة علمية قاطعة في الدلالة على الحقائق التي تتضمنها، إلا أن الكشف عن الهوية الحقيقية للفاعل ليس بالأمر السهل، فقد يمكن التعرف على هوية الحاسوب المستعمل في ارتكاب الجريمة والمرتبط بشبكة الإنترنت من خلال عنوان IP إلا أنه من الصعب تحديد هوية الفاعل ما لم يتم تدعيم هذا الدليل الرقمي بالأدلة التقليدية الأخرى فيما بعد.

وقد لاحظت من خلال البحث حول مسألة تقدير القيمة القانونية للدليل الرقمي أنه يجب التمييز بين أمرين الأول : القيمة العلمية القاطعة للدليل الرقمي والثاني : الظروف والملابسات التي تحيط بهذا الدليل، فالقاضي ليس له أن ينازع فيما أسفرت عليه تكنولوجيا المعلوماتية والعلوم التقنية من الناحية العلمية وإنما له أن يقدر الظروف والملابسات التي أحاطت بهذا الدليل، ويمكن له في سبيل ذلك الاستعانة بطرق الإثبات التقليدية التي توجد عادة إلى جانب الدليل الرقمي، وله في ذلك أن يرفض هذا الدليل إذا لم يقتنع بظروف القضية وملابساتها.

وهذا ما قادني إلى الوصول إلى نتيجة أخرى مؤداها تمتع القاضي الجزائي بدور إيجابي من حيث تقدير القيمة القانونية للدليل الرقمي وخضوعه للسلطة التقديرية، شأنه في ذلك شأن باقي الأدلة.

كما تبين أن الاتصالات الإلكترونية والنظم المعلوماتية تعتبر أحد أوجه الحياة الخاصة للإنسان ومظهرا من مظاهر خصوصياته، وبالتالي فإن إجراءات استخلاص الدليل في البيئة الرقمية قد تؤدي إلى المساس بهذه الخصوصية وإمكانية إطلاع المحققين على أسرار خاصة بأشخاص قد لا يكون لهم أصلا يد في الجريمة، مما جعل المشرع يحرص كل الحرص على هذه المسألة بأن اشترط اللجوء إلى هذه الإجراءات إذا دعت إلى ذلك ضرورة التحري والتحقيق والتي يجب أن تقدر بقدرها.

وفي الأخير فإنه وعلى ما توصلت إليه في هذا البحث فإنه قد بدا لي أن أقدم جملة من المقترحات آمل أن أكون موفقة في طرحها.

إن الجزائر وهي تخطوا الخطوات الأولى في تطبيق مشروع الحكومة الإلكترونية والذي من خلاله يتم السعي إلى استخدام تقنية المعلومات والاتصالات الإلكترونية في توفير وتقديم معلومات وخدمات الحكومة للمواطنين وجعلها متاحة للجمهور، فهذا المشروع لابد أن تتبعه خطوة تشريعية هامة يكون الهدف منها توفير الحماية القانونية الشاملة لهذا المفهوم بصورة منسجمة ومتزامنة مع هذا التحول من أجل تخطي الثغرات القانونية التي قد يستفيد منها العابثون بأمن المعلومات، لا سيما وأن الأمر يتعلق بأنظمة معلوماتية تخص إدارات الدولة.

وحسب مفهوم المادة 44 من قانون الإجراءات الجزائية الفقرة الثانية المدرجة بموجب القانون 06/22 المؤرخ في 2006/12/20 فإنه لا يجوز لضباط الشرطة القضائية في إطار التحري والتحقيق عن الجرائم الماسة بأنظمة المعالجة للمعطيات الانتقال إلى مساكن الأشخاص الذين يظهرون أنهم ساهموا في ارتكاب هذه الجريمة لإجراء التفتيش هناك إلا بإذن مكتوب من الجهة المختصة، مع وجوب استظهار هذا الإذن قبل الدخول إلى المسكن والشروع في عملية التفتيش، وعليه فالإذن في هذه المادة يتعلق حصرا بتفتيش المساكن، لكن المشرع في القانون04/09 أجاز في إطار التحري والتحقيق في الجريمة المعلوماتية تفتيش محل آخر غير السكن وهو المنظومة المعلوماتية دون أن يشترط للدخول إليها ضرورة الحصول على إذن من الجهة القضائية المختصة، فحصول ضابط الشرطة القضائية على إذن يسمح له بالدخول إلى الأماكن التي تتواجد بها الحواسيب لا ينصرف في رأيي إلى الإذن بدخول المنظومة المعلوماتية لهذه الحواسيب وتفتيشها لاختلاف محل التفتيش أصلا، لذلك أقترح على المشرع إضافة فقرة أخرى للمادة 05 من القانون 04/09 كما يلي "لا يجوز إجراء عمليات التفتيش في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة".

سبق وأن مر بنا أن من بين الصعوبات في تحديد هوية المجرم المعلوماتي هو استعمال هذا الأخير لحواسيب غير شخصية في تنفيذ جريمته وغالبا ما تكون في مقاهي الإنترنت، هذه الأخيرة التي يرتادها عدد كبير من الزبائن لا يمكن معرفة هوياتهم، لذلك أقترح على المشرع إعادة النظر في تسير هذه المقاهي وعدم اعتبارها مجرد نشاط تجاري كغيره من الأنشطة التجارية الأخرى، بل لابد من فرض أعباء والتزامات على مقدمي هذه الخدمة ومسيري مقاهي الإنترنت، كأن يطلب من أي زبون قبل شروعه في استعمال الإنترنت ملء استمارة تحدد فيها كامل هويته والتوقيت الذي استعمل فيه شبكة الإنترنت ورقم جهاز الحاسوب الذي استعمله، كما يلتزم مسير المقهى بالاحتفاظ بعناوين المواقع التي تم زيارتها في ذاكرة كل حاسوب لمدة معينة، ونفس الشيء بالنسبة لاستعمال شبكات الإنترنت الموجودة في المؤسسات العامة كالجامعات وغيرها.

ليس بالخفي أن هناك من الشركات الخاصة التي تحوي منظوماتها المعلوماتية على المعلومات الشخصية أو الاسمية للعديد من المتعاملين معها، فالشركات المتخصصة في مجال الاتصالات مثلا، كمتعاملي الهاتف النقال تعتبر من خلال عدد المشتركين لديها بمثابة بنك للمعلومات الإسمية والتي يمكن التلاعب واستعمالها في أغراض غير مشروعة، لذلك اقترح على المشرع أن يتدخل لوضع القواعد القانونية الخاصة بالضمانات الوقائية للحياة الشخصية في إطار قانون متكامل يكون بمثابة مبادئ يقوم عليها نشاط نظم المعلومات الشخصية أو الإسمية.

أرجوا أن أكون قد وفقت في معالجة هذا الموضوع، وإن لم أوفق فعذري أنني اجتهدت ولكل مجتهد نصيب.

قائمة المراجع

قائمة المراجع

أولا : القوانين

- الدستور الجزائري سنة 1996.
- قانون العقوبات المعدل و المتمم.
- قانون الإجراءات الجزائية المعدل و المتمم.
- قانون 04/09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- قانون 2000/03 المؤرخ في 5 جمادى الأولى 1421 الموافق لـ 5 أوت 2000 محدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية
- مرسوم رئاسي 183/04 مؤرخ في 8 جمادى الأولى 1425 الموافق لـ 26 يونيو 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد القانوني الأساسي.

– ثانيا: الكتب باللغة العربية

1 / الكتب العامة

1 – أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، دار هومة، طبعة 2003.
2 – أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، 1996.
3 – أشرف عبد القادر قنديل، النظرية العامة للبحث الجنائي وأثرها في عقيدة القاضي، دار الجامعة الجديدة، طبعة 2011.
4 – حاتم حسن موسى بكار، سلطة القاضي الجنائي في تقدير العقوبة والتدابير الاحترازية، الدار الجماهيرية للنشر والتوزيع والإعلان، ط1 2005.
5 – فايز الإيعالي، قواعد الإجراءات الجزائية أو أصول المحاكمات الجزائية على ضوء القانون والفقه والاجتهاد ، المؤسسة الحديثة للكتاب، ط 1 1994.
6 – عبد الله سليمان، شرح قانون العقوبات الجزائري القسم العام الجزء الأول (الجريمة)، ديوان المطبوعات الجامعية.
7 – علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، 2006.
8 – عبد الله أوهيبية، شرح قانون الإجراءات الجزائية الجزائري التحري والتحقيق، دار هومة، الطبعة 2003.
9 – محمد محدة، ضمانات المتهم أثناء التحقيق دار الهدى، الطبعة الأولى 1992-1991.
10 – محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثانية 2010.
11 – محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة القاهرة، طبعة 2008

2 / الكتب المتخصصة

1 – أمير فرج يوسف، – الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية الإسكندرية 2009.
– الجريمة الإلكترونية والمعلوماتية، والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر الأنترنت، مكتبة الوفاء القانونية الإسكندرية، الطبعة الأولى 2011
2 – عبد الله حسين علي محمود ، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات
3 – عمر محمد بن يونس، الدليل الرقمي، بحث منشور على موقع .www.arablawinfo.com

4 – ممدوح عبد الحميد عبد المطلب،
– استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكمبيوتر، بحث منشور على موقع www.arablawinfo.com
– استخدم بروتوكولTCP/IP في بحث وتحقيق الجرائم مع الكمبيوتر، المرجع السابق، ص .5
5 – محمّد عبيد الكعبي، الجرائم الناتجة عن استخدام غير مشروع لشبكة الأنترنت، دار النّهضة العربيّة القاهرة ص .32
6 – نائلة محمد فريد قروة، المرجع السابق ص .30
7 – رشيدة بوبكر، المرجع السابق ص .40
8 – محمّد أمين الشوابكة، جرائم الحاسوب و الأنترنت، دار الثّقافة للنشر و التوزيع الطبعة الأولى 2009 ص .8
9 – محمّد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية 1994 ص 6.
10 – عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية و أزمة الشرعيّة ، دراسات الكوفة العدد السابع ص .112
11 – سيناء عبد الله محسن، المواجهة التشريعيّة للجرائم المتّصلة بالكمبيوتر في ضوء التشريعات الدوليّة و الوطنيّة.
12 – نهلا عبد القادر المؤمني، "الجرائم المعلوماتية" دار الثقافة للنشر و التوزيع عمّن 2008 ص .51
13 – فايز بن عبد الله الشهري، "التحدّيات الأمنية المصاحبة لوسائل الاتصال الحديثة" دراسة وصفية للظاهرة الإجراميّة على شبكة الأنترنت ص .10
14 – يونس عرب، قراءة في الاتجاهات التشريعيّة للجرائم الإلكترونيّة مع بيان موقف الدّول العربيّة وتجربة سلطنة عمان.
15 – أحمد بن محمّد اليمانى، الحماية الجنائيّة للبريد الإلكترونيّ.
16 – أحمد خليفة الملط، المرجع السّابق ص .126
17 – عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، ديوان المطبوعات الجامعية الجزائر: 1995 ص.148
18 – غنّام محمد غنّام، الحماية الجنائيّة لبطاقات الائتمان مؤتمر الجوانب القانونيّة و الأمنيّة للعمليّات الإلكترونيّة دبي 2003 ص .05
19 – مصطفى محمّد موسى، التحقيق في الجرائم الإلكترونيّة مطابع الشّرطة ط1 ص .15
20 – جميل عبد الباقي الصغير، الجوانب الإجرائيّة للجرائم المتعلّقة بالأنترنت.
21 – محمد طارق عبد الرّؤوف الحن، المرجع السّبق، ص .230
22 – خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونيّة، دار الفكر الجامعي، الطبعة الأولى 2009، ص .56
23 – محمد نصير السرحاني، مهارات التحقيق الجنائي التقني في جرائم الحاسوب و الأنترنت، رسالة الماجستير جامعة نايف العربيّة للعلوم الأمنيّة الرّياض 2004. ص .72
24 – هشام رستم، الجوانب الإجرائيّة للجرائم المعلوماتيّة، مكتبة الآلات الحديثة، أسيوط 2000، ص .59
25 – عبد اللّه حسين محمود، إجراءات جمع الأدلّة في الجريمة المعلوماتيّة، مؤتمر الجوانب القانونيّة والأمنيّة للعمليات الإلكترونيّة، دبي 2003، ص .612
26 – حسين الغفاري، المرجع السابق، ص .02
27 – محمّد الأمين البشري، التحقيق في جرائم الحاسب الآلي بحث مقدّم إلى مؤتمر القانون و الكمبيوتر و الأنترنت بكلّية الشريعة و القانون، جامعة الإمارات العربيّة المتّحدة الفترة من 01 إلى 03 ماي 2000.

28 – علي محمّد حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت، عالم الكتب الحديثة، الأردن، ص186.
29 – أشرف عبد القادر قنديل، النظريّة العامّة للبحث الجنائي وأثرها في عقيدة القاضي، المرجع السابق، ص.212
30 – محمّد عبد الغريب، حرّية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام، المرجع السابق، ص .8
31 – نصر الدّين ماروك، النظريّة العامّة للإثبات الجنائي، الجزء الأوّل، ص .620
32 – زبدة مسعود، الاقتناع الشخصي للقاضي الجزائي، المؤسّسة الوطنيّة للكتاب، الطبعة الأول، ص 08.

ثالثا: المراجع باللغة الأجنبية

1 / الكتب باللغة الفرنسية

1 - Myriam QUEMENER : YES CHARPENEL .cybercriminalité Droit pénal appliqué .Normandie Roto impression 2010.

الفهرس