وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

قسم: القانون العام

المرجع:.....

مذكرة نهاية الدراسة لنيل شهادة الماستر

إثبات الجريمة المعلوماتية في التشريع الجزائري

ميدان الحقوق والعلوم السياسية

الشعبة: الحقوق

التخصص: القانون الجنائي والعلوم الجنائية

من إعداد الطالب(ة):

بن زرت اسيا

تحت إشراف الأستاذ(ة):

بن عبو عفيف

أعضاء لجنة المناقشة

الأستاذ(ة).....وافي حاجة.....رئيسا

الأستاذ(ة).....بن عبو عفيف.....مشرفا مقررا

الأستاذ(ة).....رحوي فؤاد.....مناقشا

السنة الجامعية: 2019/2018

نوقشت يوم: 2019/07/10


بسم الله الرحمن الرحيم

اهداء

الى الوالدين فلولاهما لما وصلت لما أنا عليه اليوم فمنهما تعلمت الصمود مهما كانت الصعوبات. أمي، أطال الله في عمرها وأبي رحمه الله، والى إخوتي وعائلتي الكبيرة وأسرتي الصغيرة ولا سيما زوجي الذي طالما ساعدني وشجعني على إكمال دراستي، والى أهل زوجي الذين دعموني ووقفوا الى جانبي حتى وصلت الى هذه المرحلة وكذلك الى ابني العزيز حفظه الله والى أساتذتي الكرام فمنهم استقيت الحروف وتعلمت كيف أنطق الكلمات وأصوغ العبارات ولا سيما الأستاذ المشرف بن عبو عفيف وإلى الزملاء والزميلات أهدي لكم رسالة الماستر راجية من المولى سبحانه وتعالى أن يجد القبول.

الشكر والعرفان

أستاذي بن عبو عفيف

لولا ما قدمته لي من توجيه رشيد ورأي سديد، فلا أملك عرفانا بما تفضلت به علي إلا أن أسدي لك وافر الشكر وأتقدم لك بعمق الإمتنان، وخالص التقدير.

ويسرني كذلك أن أتقدم بجزيل الشكر والعرفان إلى اللجنة الموقرة التي قبلت مناقشة هذا البحث المتواضع.

الى أساتذتي الذين جمعتني معهم مقاعد دراستي واستقبلوني وكانوا معي منذ السنوات الأولى.

مقدمة:

لقد شهدت الوسائل التقنية الحديثة انتشارا واسعا في العصر الحالي فعلى سبيل المثال فقد تغلغلت الحاسبات الآلية وشبكة الانترنت في جميع جوانب الحياة، بحيث أصبحت العديد من الدول تعتمد عليها في تسيير مرافقها الحيوية كالدفاع والامن والاقتصاد، كما ان هذه الأخيرة عرفت انتشارا واسعا على المستوى الاجتماعي بحيث اصبح معظم الافراد يلجؤون الى استخدام مجموعة من التقنيات الالكترونية في تسيير شؤون حياتهم اليومية، كالتواصل وتبادل المعارف عبر شبكة الانترنت في شكل ارقام ورموز الكترونية ويتم ذلك بمجرد كبسة زر على الحاسب الآلي.

ونظرا لما تتميز به النظم المعلوماتية من دقة وسرعة في تجميع المعلومات وتخزينها ومعالجتها، فإنها خلفت إنجازات وتطورات كبيرة في المجال التقني، وهذا راجع للاستخدامات الكثيرة لها في مختلف قطاعات الحياة إلا ان هذه التكنولوجيا أدت الى ظهور نوع جديد من الاعتداءات على الحياة الخاصة للأفراد، كما انها أحدثت خسائر كبيرة لاقتصاد الدول.

بالإضافة الى ذلك فإن الوسائل العلمية الحديثة ساعدت المجرم المعلوماتي على القيام بمختلف الجرائم المعلوماتية كإختراق شبكات الانترنت وتزييف النقود الالكترونية وتزوير المستندات الالكترونية...الخ، بسرعة وبدقة عالية دون ترك أي اثر للكشف عنها او معرفة مصدرها، كما ان هذا الاعتداء يمكن ان يكون على مجموعة من المجني عليهم في نفس الوقت وفي مختلف انحاء العالم عن طريق ما يسمى بشبكة الانترنت.

كما ان الطبيعة الخاصة لمحل ارتكاب الجرائم المعلوماتية والذي يتمثل في المعلومات صعبت على السلطات المختصة بالبحث والتحري مباشرة مهامها والمتمثلة في القيام بإجراءات الاستدلال والتحقيق عبر البيئة الرقمية وهذا راجع لتعودهم على التعامل مع الجرائم التقليدية والتي تخلف آثارا مادية في مسرح الجريمة كالبصمات مما يسهل عليهم هذه

المهمة على عكس الجرائم المعلوماتية، فإنها لا تخلف آثارا مادية وهذا لانعدام الدليل المرئي لها، وبفضل هذه الخاصية فإن الجاني في هذه الجرائم يمكنه إخفاء وطمس الدليل من مسرح الجريمة، مما يزيد الامر تعقيدا على هذه السلطات، ولذلك فإن عملية البحث والتحري لهذه الجرائم تحتاج الى طرف الكترونية فنية وتقنية تتناسب مع طبيعتها بشكل يمكنها من ترجمة الأرقام والرموز الى بيانات مقروءة تصلح بأن تكون ادلة للإثبات لهذه الجرائم ونسبتها لفاعليها ويطلق عليها اسم الأدلة المعلوماتية.

ولقد تعاظم دور الاثبات خاصة في ظل ما افرزته ثورة المعلومات والاتصالات من سلوكيات منحرفة اجتماعيا لم تكن موجودة في الماضي، حيث ومع التطور التقني في أساليب ارتكاب الجرائم اصبح مطلوبا من سلطات انفاذ القانون ان تتعامل مع نوع مستحدث من الأدلة في مجال الاثبات الجنائي سواء من حيث كم البيانات المدونة في جهاز الحاسوب الآلي وكيفية اثباتها، او سواء من حيث وسيلة اثباتها، لا سيما وان هذه السلطات في الوقت الحالي غير مؤهلة للقيام بهذا الدور، وهي ثغرة يعتمد عليها المجرم المعلوماتي الذي يعكس اعلى درجات المهارة في فنون التعامل مع الحاسوب الآلي، الامر الذي اصبح يستدعي وبشدة إعادة النظر في وسائل الاثبات التقليدية وتطويها بما يواكب التطور في أساليب ارتكاب هذه الجرائم، فضلا عن ضرورة وضع الخطط والبرامج الاستراتيجية لتحديث أجهزة العدالة الجنائية وتطويرها من حيث كوادرها البشرية لتصبح قادرة من الناحية التقنية على التصدي لهذا النوع من الجرائم.

السبب الرئيسي الذي دفعنا لاختيار هذا الموضوع كونه من الموضوعات المستحدثة التي تعاني من نقص الدراسات كما ان التطرق لهذا الموضوع يتسنى لنا معرفة مدى مواكبة التطور القانوني للتقدم التكنولوجي الذي شهده العالم في منتصف القرن العشرين لأن هذا التطور لم يخلف اثار إيجابية فحسب، بل تعدى الى أبعد من ذلك، فقد استغل ذلك معظم الأشخاص للقيام بمختلف الجرائم وذلك بالاستعانة بالتقنيات التكنولوجية الحديثة.

أهمية الموضوع:

فقد كان محور دراستنا في هذه المذكرة انها تكمن هذه الأهمية في كون أن الجريمة المعلوماتية من الجرائم المستحدثة والتي في تطور مستمر كما أن أساليب ارتكابها دائمة العمل على مواكبة التطور التكنولوجي الحاصل في ميدان المعلوماتية فان أهمية هذا الموضوع تتضح في كونه تناول أحدث الوسائل العلمية وأكثرها انتشار

أما بالنسبة لإشكالية هذا الموضوع:

إذا كانت نصوص قانون الإجراءات الجزائية وجدت لتحكم الإجراءات المتعلقة بجرائم تقليدية، التي لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجميع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع من أجل الوصول إلى الحقيقة الموضوعية بشأن الجريمة والمجرم، فإن الأمر مختلف تماما في الجريمة المعلوماتية التي ثارت بشأنها مشكلات إجرائية كبيرة فرضتها طبيعة ولهذا الغرض، البيئة الافتراضية التي ترتكب فيها الجرائم، من هنا نطرح الاشكال التالي:

- كيف يمكن اثبات الجريمة المعلوماتية؟
- ما طبيعة الإجراءات التي تخضع لها؟

في الفصل الأول سلطنا الضوء على **خصوصية اثبات الجرائم المعلوماتية** ;ذلك من خلال تقسيمه الى مبحثين تناولنا في المبحث الأول **مفهوم الجرائم المعلوماتية** وخصصنا في المبحث الثاني للحديث عن **مراحل اثبات الجريمة المعلوماتية.**

اما في الفصل الثاني فعالجنا من خلاله **إجراءات المحاكمة في الجريمة المعلوماتية** من خلال تقسيمه الى مبحثين، في المبحث الأول **مرحلة المحاكمة** والمبحث الثاني **شروط قبول الأدلة وحجيتها في الاثبات.**

نبيل صقر، جرائم الكمبيوتر والانترنت في التشريع الجزائري، دار الهلال للخدمات الإعلامية، الجزائر، 2005.

تمهيد:

أدى التقدم العلمي الحاصل في مجال تقنية المعلومات وتدفقها في السنوات الأخيرة وكذا الانتشار المطرد لأجهزة الحاسوب الآلي الى ظهور نوع جديد من الجرائم لم تكن موجودة من قبل، ارتبطت ارتباطا وثيقا بتكنولوجيا المعلومات والاتصالات، عرفت بالعديد من التسميات من بينها تسمية الجرائم المعلوماتية، بحيث لم يتفق الفقهاء الى حد اليوم على مسمى موحد لهذا النوع من الجرائم، والتي تعد أحد اهم ثمار التقدم السريع في المجالات العلمية سواء اقتصرت على الحاسوب او تعدته الى الانترنت. اتسمت هذه الجرائم بطبيعة خاصة ميزتها عن غيرها من الجرائم التقليدية، فهي تتم في بيئة رقمية لا علاقة لها بالأوراق او الاجسام او الأشياء او غيرها من ماديات الطبيعة، كما انها تشكل نوعا جديدا من الجرائم التي لا تعترف لا بالمكان ولا بالزمان، ضاربة عرض الحائط جميع الحواجز والحدود، ومرتكبوها لهم من الذكاء والمهارة التقنية العالية والمعرفة الفنية في مجال المعلوماتية، ما يمكنهم من اقتراف جرائمهم دون ترك سبيل الاهتداء إليهم، وذلك لاستخدام طرق وأساليب تقنية عالية الكفاءة يصعب اكتشافها.

إن ما يميز هذه الجرائم من طبيعة خاصة ترك آثار واضحة على إثباتها، حيث انتقل الإثبات فيها من نطاق ما هو ملموس ومحسوس الى نطاق ما هو افتراضي ورقمي، فلم تعد هناك آثار تقليدية يمكن اعتمادها في إثبات ما يقع من جرائم معلوماتية، وإنما أصبح الإثبات فيها يعتمد على ارقام وبيانات ومعلومات قد تتغير وتمحى من السجلات المخزنة في الحواسب الآلية، والتي ليس لها أي اثر خارجي ملموس (1) ، و على ذلك تم الانتقال من مرحلة التعامل مع ادلة مادية الى مرحلة التعامل مع نوع جديد من الأدلة ذات الطبيعة غير المرئية، السهلة المحو وكذا التدمير، وتحول بذلك مسرح الجريمة المعلوماتية من مسرح تقليدي يمكن العثور

---

(1): محمد علي العريان ،الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر، الأزاريطة، 2004.

فيه على العديد من الأدلة التي تثبت ما يقع عليه من جرائم، الى مسرح افتراضي يصعب الحصول فيه على مثل هذه الادلة، ليس هذا فحسب، وإنما اتسع هذا المسرح ليتخطى إقليم الدولة الواحدة الى دول أخرى لا يمكن تمديد إجراءات الضبط والتفتيش اليها، الا بوجود اتفاقيات او معاهدات تسمح بذاك، كما ان السرعة التي ترتكب بها الجريمة بحيث قد لا تستغرق أكثر من عدد من الثواني، قد تعقد من عملية اثباتها. فضلا عن هذا فإن ما تلم به أجهزة العدالة الجنائية من معرفة بالقواعد القانونية الواجب اتباعها في اثبات الجرائم بصفة عامة، أصبح لا يكفي لوحده لإثبات الجرائم المعلوماتية.

إن كل ما يدعو الى القول ان إثبات هذا النوع من الجرائم يكتسي خصوصية تميزه عن إثبات غيره من الجرائم التقليدية، وتتجسد هذه الخصوصية بصفة أساسية في ما يكتنف هذا الإثبات من صعوبات في مجال هذه الجرائم. وهذا ما سنحاول التطرق اليه من خلال هذا الفصل، وحتى نكون منطقيين ومنهجيين في عرض افكارنا، ارتأينا تقسيمه الى مبحثين نتطرق في المبحث الأول الى مفهوم الجرائم المعلوماتية، ومن ثم نتناول في المبحث الثاني مراحل اثبات الجرائم المعلوماتية.

المبحث الأول: مفهوم الجريمة المعلوماتية

تعد الجرائم المعلوماتية من الجرائم الحديثة نسبيا، والتي ظهرت بظهور تكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات، وهي بلا جدال جرائم ضربت بقوة، وتنامت بسرعة فائقة في ظل الانفتاح العالمي وارتباط الأسواق الدولية بعضها ببعض، فأصبحت تشكل خطرا يهدد الافراد في ممتلكاتهم وخصوصياتهم، والمؤسسات في كيانها المادي والاقتصادي، وحتى المعلومات في امنها وسيادتها. ونظرا لجسامة اخطار هذه الجرائم وفداحة خسائرها وسرعة انتشارها من جهة، وحداثتها النسبية من جهة أخرى، أصبحت

موضوع اهتمام بالغ من قبل العديد من الفقهاء ورجال القانون، سعيا منهم لفهم هذه الظاهرة وإبراز موضوعها وتحديد انواعها، مما يتيح المجال لرفع الغموض عنها والالتباس حولها، وذلك من اجل توعية أفضل بمخاطرها. فسلامة التعامل مع أي ظاهرة مستحدثة يقتضي أولا وقبل كل شيء إيضاح معالمها وتحديد ماهيتها، وهذا ما سنحاول التطرق اليه في هذا المبحث من خلال تقسيمه الى مطلبين، نتناول في المطلب الأول تعريف الجريمة المعلوماتية، ثم نتطرق في المطلب الثاني على أهم أنواعها ودوافع ارتكابها.

المطلب الأول: تعــريف الجــريمة المعلوماتية.

تعتبر الجرائم المعلوماتية من الأنماط المستحدثة التي رافقت التطور التكنولوجي الحديث، فهي لم تحظ بعد بالاستقرار على النحو الذي حظيت به نظيرتها من الجرائم التقليدية، الامر الذي أدى الى وجود اختلافات جوهرية بين شرائح القانون بصفة عامة والقانون الجنائي بصفة خاصة، سواء من حيث المصطلحات المستخدمة للتعبير عنها، او من حيث التعريفات التي وضعت لها. (1)

تعدد المصطلحات الدالة على الجرائم المعلوماتية

ان اول ما يلفت انتباه الباحث في ظاهرة الجرائم المعلوماتية هو تنوع المصطلحات الدالة عليها، فقد تناولت الدراسات هذه الظاهرة بعدد ليس بقليل من المصطلحات، وهذا راجح للتطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات، التي تعد بيئة هذه الظاهرة المستحدثة.

فهنالك من استعمل مصطلح "الاحتيال المعلوماتي"، وهناك من أطلق عليها تسمية "الجرائم التي يساعد على ارتكابها الحاسوب الآلي"، ويفضل البعض استعمال عبارة التعسف

في استعمال الحاسوب الآلي او إساءة استعمال الحاسوب الآلي للدلالة على هذه الظاهرة، على أساس ان هذه المصطلحات اشمل وأوسع، لأنها تشمل الى جانب الجرائم كافة الصور التي تنطوي على إساءة استخدام الحاسوب الآلي دون ان تصل الى درجة السلوك الإجرامي (1) وهناك من فضل استعمال مصطلح جرائم نظم المعلومات (2) وذلك لسببين اساسيين، الأول كون ان هذا المصطلح يعبر عن محل الأنشطة الاجرامية ويمكنه ان يتواكب مع التطورات المستحدثة في مجال المعلوماتية ووظيفتها في الحياة الاجتماعية دون ان يتم حصرها في نطاق وسيلة معنية، والثاني كون المصطلحات الأخرى تربط نفسها بأداة ووسيلة ارتكاب الأنشطة الاجرامية او تحصرها في نطاق نوع معين، مما يؤدي الى تجدد ظهور المشاكل القانونية في تطبيق النصوص على الواقع. وليس بعيدا عن هذا المصطلح أطلق عليها البعض مصطلح جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

وفي ظل التقدم التكنولوجي يفضل البعض استخدام مصطلح "جرائم التكنولوجيا الحديثة" على أساس انها جرائم تكنولوجيا باعتبارها مرتبطة ارتباطا وثيقا بالتكنولوجيا التي تعتمد أساسا على الحواسب وغيرها من أجهزة تقنية قد تظهر في المستقبل، وهي حديثة نظرا لحداثتها النسبية من ناحية وارتباطها الوثيق بما قد يظهر من أجهزة حديثة قد تكون ذات طاقة تخزينية وسرعة فائقة ومرونة في التشغيل.

ومن جانبنا، فإننا نميل مع البعض الى استخدام مصطلح الجرائم المعلوماتية للدلالة على الجرائم المتعلقة بالحاسوب الآلي والانترنت، وذلك كون هذا المصطلح يشمل جميع جوانب المعلوماتية سواء من الناحية الاجتماعية او الاقتصادية او القانونية، فضلا على اشتماله جميع التقنيات المستعملة في التعامل مع المعلومات، الحالية منها والمستقبلية.

ويمكن القول انه مهما تعددت المصطلحات المستخدمة للدلالة على الجرائم

---

(1): نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2005.

(2): أيمن عبد الله فكري، جرائم نظم المعلومات، دار الجامعة الجديدة للمنشورات، الإسكندرية، 2007.

المعلوماتية، الا انه لابد من مراعاة اعتبارات هامة عند اختيار المصطلح الدال عليها، وتتمثل هذه الاعتبارات فيما يلي: (1)

– اختيار المصطلح يتعين ان يزاوج بين البعدين التقني والقانوني.

– دقة اختيار المصطلح، حيث يتعين ان ينطلق من أهمية التمييز بين المصطلحات المنتمية لما يعرف بأخلاقيات التقنية او اخلاقيات الحاسوب والانترنت، وبين ما يعرف بإجرام التقنية او جرائم الحاسوب.

– أن يكون المصطلح قادرا على ان يعبر بقدر الإمكان عن حدود محله، فيكون شاملا لما يعبر عنه.

تعدد التعريفات الدالة على الجرائم المعلوماتية

تعددت الجهود المبذولة من قبل المهتمين بدراسة هذا النمط المستحدث من الجرائم لوضع تعريف للجرائم المعلوماتية، الا ان محاولاتهم في وضع تعريف جامع مانع لها، باءت بالفشل، حتى قيل ان هذه الجرائم تقاوم التعريف (2)، كما ذهب البعض الى التشكيك في إمكانية وضع تعريف يحدد مفهوم الجريمة المعلوماتية، وارجعوا صعوبة ذلك الى امرين هما: (3)

– الخشية من حصر نطاق الجريمة داخل إطار يضر بها، وذلك لان الطبيعة الفنية للجريمة المعلوماتية تفرض صعوبة في حصرها داخل إطار قانوني تجريمي محدد وواضح.

– وجود بعد دولي للجريمة المعلوماتية، يستوجب ان يكون التعريف متفق عليه على نطاق واسع حتى يمكن العمل من خلاله، وتنسيق التعاون فيما بين الدول في المجالات

---

(1): أيمن عبد الله فكري، المرجع السابق.
(2): نائلة عادل محمد فريد قورة، المرجع السابق.
(3): أيمن عبد الله فكري، نفس المرجع.

المتعلقة بالإجرام المعلوماتي.

وقد تناولت العديد من الدراسات ما جاء من تعريفات مختلفة للجرائم المعلوماتية، واختلفت في طرق تناوها. وسنتطرق من خلال ما يلي الي سرد بعض من تلك التعاريف بغية الوصول الى التعريف المناسب

التعاريف التي اعتمدت على موضوع الجريمة

من ذلك، التعريف الذي اقترحه خبراء منظمة التعاون الاقتصادي والتنمية في عام 1983 م حيث عرفوا الجريمة المعلوماتية بأنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/أو بنقلها)" (1). إن هذا التعريف يخلط بين السلوك الإجرامي الذي يصلح لأن يشكل الركن المادي للجريمة المعلوماتية وبين السلوك غير الأخلاقي والذي قد لا يشكل الركن المادي للجريمة باعتبار أنه ليس كل سلوك غير أخلاقي يعتبر سلوكا إجراميا.

وقد عرف مجموعة من الخبراء المختصين من بلجيكا جرائم الحاسوب في معرض رد بلادهم على الاستبيان الذي أجرته منظمة التعاون الاقتصادي والتنمية OECDحول الغش المعلوماتي في عام 1982م بأن: «كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجًا، بطريقة مباشرة أو غير مباشرة، عن الاستخدام غير المشروع لتقنية المعلومات». (2)

كما أورد الدكتور الشوا محمد، في مؤلف له تحت عنوان الغش المعلوماتي كظاهرة إجرامية مستحدثة تعريفا مشابها للتعريف السابق، حيث عرف الغش المعلوماتي بأنه: « كل

Legal Aspects Of Computer-related Crime in the Information (1998),): SIEBER ULRICH1(Society. http://europa.eu.int/ISPO/legal/en/comcrime/sieber موقع انترنت ---

(2): د/ رستم هشام، قانون العقوبات ومخاطر التقنية، مكتبة الآلات الحديثة، أسيوط، 1992، ص10.

فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويهدف إلى الاعتداء على الأموال المادية والمعنوية » (1).

وعرفتها هدى قشقوش بأنها: « كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات » (2).

التعاريف التي اعتمدت على وسيلة ارتكاب الجريمة

التعريف الذي قال به الأستاذ توم فورستر TOM FORESTER بأنها «فعل إجرامي يستخدم الكومبيوتر في ارتكابه كأداة رئيسية» (3) .

والتعريف الذي وضعه تاديمان TIEDEMANN بأنها: « كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب» (4).

كما عرفها الفقيهان TOTTY و ARDCASTLE بأنها: « تلك الجرائم التي يكون قد وقع في مراح ارتكابها بعض العمليات الفعلية داخل نظام الحاسوب، وبعبارة أخرى هي تلك الجرائم التي يكون دور الحاسوب فيها إيجابيا أكثر منه سلبيا » (5).

و يعرفها الأستاذان JACK BOLOGNA و ROBERT J.LINDQUIST بأنها « جريمة يستخدم فيها الحاسوب كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها» (6) .

---

(1): د/ الشوا محمد، الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحوث المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، جمهورية مصر العربية، سنة 1993، ص8.

(2): د/هدي قشقوش، جرائم الحاسوب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، سنة 1999، ص 20.

(3): TOM FORESTER, Essential Proplems to Hig-Tech Society First Mit Pres Edition, Cambridge, Massachusetts, 1989, P :104.

(4): TIEDEMANN, Fraude Et Autres Delits D'affaires Commis A L'aide D'ordinateurs Electroniques. R.D.P.C 1984. N°7; P :61 .

(5): TOTY Technology AND HARDCASTLE: Computer Related Crime in Information .K.1986. andthelawu

(6): TOTY AND HARDCASTLE, Ouvrage Precedent, P26.

التعاريف التي اعتمدت على محل الجريمة

ذهب البعض الى تعريف الجريمة المعلوماتية تبعا للمحل الذي ترد عليه، حيث يعرفها الفقيه (Rosblat) على انها "نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسوب الآلي، او التي تحول عن طريقه" (1)، ويعرفها الفقيه (Parker)بأنها" كل فعل اجرامي متعدد أيا كانت صلته بالمعلومات، تنشأ عنه خسارة تلحق بالمجني عليه او كسب يحققه الفاعل" .كما حاول كلا من الأستاذين (Vivant) و (Le Stains) وضع تعريف يراعى فيه موضوع الجريمة وذلك بوصفها بأنها "مجموعة الأفعال غير المشروعة والمرتبطة بالمعلوماتية والتي يمكن ان تكون جديرة بالعقاب (2)، وذهب مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية عام 1983 الى تعريف الجريمة المعلوماتية على انها "كل سلوك غير مشروع او غير أخلاقي او غير مصرح به يتعلق بالمعالجة الآلية للبيانات" (3)، كما اشارت الدكتورة هدى حامد قشقوش بأن الجرائم المعلوماتية هي "مجموع الجرائم التي تتصل بالمعلوماتية." (4)

التعريفات القائمة على مرتكب الجريمة

استندت هذه التعريفات على مدى إلمام الجاني مرتكب الجريمة المعلوماتية بالتقنية المعلوماتية، ومن بين هذه التعريفات، التعريف الذي جاء به الفقيه (Thompson David) الذي

---

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

(2): محمد علي العريان، نفس المرجع.

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

(4): هدى حامد قشقو جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، من 25 الى 28 أكتوبر 1993.

عرف الجرمة المعلوماتية على انها "أية جريمة يكون متطلبا لافتراقها، أن يتوفر لدى فاعلها معرفة بتقنية الحاسوب (1)، كما عرفها الفقيه (Stein Schjolberg) على أنها "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبة، والتحقيق فيه وملاحقته قضائيا" وفي ذات السياق فقد تبنت وزارة العدل الامريكية في دليلها لعام 1989 الدراسة التي قام بها معهد ستانفورد للأبحاث، فعرفت الجريمة المعلوماتية على أنها "أية جرمة لفاعلها معرفة فنية بالحواسب تمكنه من ارتكابها" (2) ، كما عرفها الدكتور اليوسف عبد العزيز على انها "جرائم يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسوب في عمل غير قانوني." (3)

المطلب الثـــاني: أنواع الجـــرائم المعلوماتية ودوافـــع ارتكابها

لم يتوقف الاختلاف بين الفقهاء والدارسين لظاهرة الجرائم المعلوماتية عند تعريفها فحسب، وإنما امتد هذا الاختلاف ليشمل أيضا تصنيفها، فوجدت العديد من التصنيفات، فيصنفها الاستاذ (Vasik Martin) الى جرائم الدخول والاستعمال غير المصرح بهما الى نظام الحاسوب الآلي، وجرائم الاحتيال المعلوماتي وسرقة المعلومات، وكذا الجرائم التي يساعد الحاسوب الآلي على ارتكابها والافعال التي تساعد على ارتكاب جرائم الحواسب الآلية (4) وذهب الفقيه (Sieber Ulrich) الى تقسيم الجرائم المعلوماتية الى ثلاثة اقسام، يتعلق القسم الأول بجرائم الحاسوب الآلي الاقتصادية والثاني بجرائم الحاسوب الآلي التي تعتدي على

---

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

(2): أيمن عبد الله فكري، المرجع السابق.

(3): اليوسف عبد العزيز، التقنية في الجرائم المستحدثة، بحث منشور ضمن كتاب الظواهرالاجرامية المستحدثة وسبل مواجهتها، منشورات أكاديمية نايف للعلوم الامنية، الرياض، 1999.

(4): محمد أبو بكر سلامة، جرائم الكمبيوتر والانترنت، منشأة المعارف، الإسكندرية،2006.

الحياة الخاصة، والقسم الثالث يتعلق بتلك الجرائم التي تهدد المصالح القومية والسلامة الشخصية للأفراد (1) وقد حاول بعض الفقهاء العرب وضع تصنيف للجرائم المعلوماتية، من بينهم الدكتور أحمد حسام طه حيث صنفها الى فئتين رئيسيتين، الجرائم الموجهة ضد النظم المعلوماتية، والجرائم المرتكبة عن طريق الاستعانة بنظم المعلوماتية. كما صنفها الدكتور عبد الفتاح بيومي حجازي الى جرائم العبث بالحاسوب الآلي، جرائم الإخلال بأمن الحاسوب الآلي، وجرائم غش الحاسوب الآلي (2).

بالإضافة الى التصنيفات التي جاء بها الفقهاء للجرائم المعلوماتية، لم تتوان بعض الهيئات الدولية في وضع تصنيف لها من بينها المجلس الاوروبي، الذي صنف أنواع الإعتداءات التي يتعرض لها الحاسوب الآلي الى طائفتين، الطائفة الأولى تضم قائمة إلزامية كجرائم التزوير والاحتيال المعلوماتي وتخريب الحاسوب الآلي...الخ، وهي طائفة الجرائم التي ألزم المجلس على الدول الأعضاء فيه النص عليها في تشريعاتها الجنائية، اما الطائفة الثانية فتضم قائمة اختيارية كالتجسس المعلوماتي، الاستعمال غير المصرح به لنظام الحاسوب الآلي...الخ.

وبعيدا عن الاختلافات الفقهية التي جاءت بشأن تصنيف الجرائم المعلوماتية والتي يمكن إرجاعها بشكل أساسي الى الاختلافات الجوهرية في تعريفها، أثرنا التطرق الى اهم أنواع الجرائم المعلوماتية وذلك من خلال تصنيفها الى طائفتين أساسيتين تناسقا مع موضوعها: طائفة الجرائم التي يكون فيها النظام المعلوماتي هدفا للاعتداء وطائفة الجرائم التي يكون فيها النظام المعلوماتي وسيلة للاعتداء. ولاستيعاب أفضل لهذه الجرائم، ارتأينا الحديث عن كل نوع من أنواع هذه الجرائم مع بيان دوافع ارتكابها.

---

(1): أيمن عبد الله فكري، المرجع السابق.

(2): عبد الفتاح بيومي حجازي الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر.2005

وتقسم الجرائم المعلوماتية الى:

أولا: جريمة التخريب ونقل الأموال: وهي بدورها تنقسم الى:

1- جريمة اتلاف معطيات الحاسوب او تخريبها: المقصود بهذه الجريمة، هو الاتلاف او التخريب الذي يقع على بيانات ومعلومات وبرامج الحاسوب لا على الكيان المادي له، فهذا الجانب لا يثير صعوبة في تحديد الجريمة ووسائل حمايتها. فمن خلال هذا التعريف لهذه الجريمة، فانه لا بد من عرض صور ووسائل ارتكاب هذه الجريمة، فانه لا بد من عرض صور ووسائل ارتكاب هذه الجريمة، فجانب من الفقه يرى انها تتخذ صورتين هما:

أ): محو المعلومات كليا وتدميرها الكترونيا.

ب): تشويه المعلومة او البرنامج على نحو يجعلها غير صالحة للاستعمال.

2- الجرائم المصرفية "نقل الأموال": ان جريمة التعدي -بواسطة الكمبيوتر- تتم عن طريق افراد، يتمتعون بخبرة ودراية طويلة في التعامل مع هذه الأجهزة المتطورة. ان ارتكاب هذه الجريمة (التعدي) بتم في الغالب لأسباب شخصية او سياسية او اقتصادية، حيث يعمد المجرم الى الدخول الى المصارف وتحويل الأموال من حسابات الى حسابات اخرى، وهي اصعب الجرائم التي ترتكب في الوقت الحالي لكونها لا تعرف الحدود، او المكان او الزمان. وقد امتدت هذه الجرائم لتشمل التلاعب في بطاقات الائتمان التي تمت سرقتها، واستخدامها للشراء بواسطة الانترت، وتعد عمليات السطو على بطاقات الائتمان احدث أنماط السلوك الإجرامي التي ارتبطت بشبكة الانترنت، من بنوك او مؤسسات مالية او افراد. وقد زاد خطر انتشار هذا النوع من الجرائم صعوبة التوصل الى مرتكبيها، ففي كثير من الأحيان يكشف حامل بطاقة الفيزا في دولة ما ان بطاقته قد استخدمت في شراء سلعة من احد المحلات في دولة ثانية، ويكون الفاعل في دولة ثالثة وقد تمت الواقعة من خلال موقع المحل البائع على شبكة الانترنت.

ثانيا: جرائم أخرى متعلقة بالحاسوب والانترنت: تنقسم الى:

1. جريمة التزييف والتزوير: ان تزييف العملة وما يصاحبها من جرائم أخرى يعاقب عليها القانون لما تسببه من أضرار للمواطنين في معاملاتهم اليومية المستمرة، ولآثارها المدمرة في الاستقرار والاطمئنان الاقتصادي. وباعتبارها تشكل عدوانا مباشرا على سيادة الدولة في حق من صميم حقوقها، يستوجب مقاومتها بشدة وتوعية المواطنين وتنبيه المسؤولين لهذه الظاهرة التي غزت المجتمعات الإنسانية منذ أن عرف الانسان العملة كوسيلة للمبادلات. وقد انتشر تزييف العملة انتشارا خطيرا في العصر الحديث، لسهولة وسرعة المواصلات وتداخل الحدود بين الدول. كما تطورت هذه الجريمة واخذت في طابعها الشكل الدولي.

2. التشهير: توجد بعض الظواهر السلبية التي برزت على شبكة الانترنت، مثل تسهيل الدعارة وبث الإباحية وخدش الحياء، ونشر بعض القيم السلبية وغير ذلك، وبالرغم من الإيجابيات الهائلة لشبكة الانترنت، فإن المخاطرة الناجمة عن هذه الشبكة بالغة الحد والعمق خاصة بالنسبة للأحداث صغار السن، حيث ان الاحداث يميلون الى التقليد والمحاكاة واثبات الذات، والحدث المهيأ للانحراف يكون مستعدا للاستجابة لأي مؤثر خارجي يؤجج استعداده الداخلي وميله الذاتي للانحراف. وشبكة الانترنت توفر لهؤلاء المادة الخصبة من المواد الاباحية، والتراسل مع الأقران سيئي الخلق محرفي الميول. كما تعد شبكة الانترنت الفضاء الرحب لنشر أي فضائح على اختلاف أنواعها او التشهير بأي شخص دون أي ضابط قانوني.

3- النسخ غير المرخص للمصنفات الرقمية: المصنفات الرقمية عبارة عن برمجيات، وقواعد البيانات وطبوغرافيا الدوائر المتكاملة، وهي مصنفات جاءت وليدة علوم الحوسبة مستقلة عن علوم الاتصال وتبادل المعطيات وشبكات المعلومات.

ومع ظهور شبكات المعلومات، والتي ارتبطت في الذهنية العامة بشبكة الانترنت، كمعبر عنها وعن التفاعل والدمج بين وسائل الحوسبة والاتصال، ظهرت أنماط جديدة من

المصنفات الممكن الحصول عليها خاصة مع وجود شبكات الانترنت. الا انه في واقع الامر تعتبر هذه المصنفات مؤلفات خاصة، كل نشر او نسخ او استفادة منها يعتبر تعدي على حقوق الملكية الفكرية للمؤلف. تعتبر هذه الجريمة من الجرائم المنتشرة بصفة واسعة خاصة في دول العالم الثالث، اين يجد الفرد صعوبة في اقتناء المصنف الأصلي فيلجأ الى الحصول عليه بطرق غير مشروعة. وقد تقدر خسائر شركة "ميكروسوفت" حوالي 16.000.000 دولار سنويا من جراء القرصنة والتداول غير المشروع لمنتجاتها.

ثالثا: جرائم الكترونية أخرى: تتعدد وتتنوع الجرائم المعلوماتية مما لا يسعنا لذكرها بالتفصيل، لذا سنورد بعض منها بإيجاز:

1: إنشاء المواقع السياسية والدينية المعادية.

2: إنشاء المواقع المعادية للأشخاص او الجهات السياسية او الفكرية.

3: جرائم القرصنة.

4: جرائم التجسس المعلوماتي.

5: الإرهاب المعلوماتي: يقوم الارهابيون بإنشاء وتصميم مواقع لهم على شبكة الانترنت لنشر أفكارهم والدعوة الى مبادئهم.

8: الجرائم المنظمة عبر الانترنت: تتمثل في: تجارة المخدرات وغسيل الأموال، السطو على أموال البنوك وقيادة الجماعات الإرهابية عن بعد.

جريمة سرقة البرامج والمعلومات

يطلق على هذه الجريمة جريمة قرصنة البرامج والمعلومات او القرصنة المعلوماتية ويقصد بها "نسخ البرامج على نحو غير مشروع او الحصول دون وجه حق على معلومات مخزنة في ذاكرة الحاسوب بطريقة مباشرة او غير مباشرة."(1)

---

(1): نهلا عبد القادر المومني، الجرائم المعلوماتية ، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان ،2008.

جريمة التلاعب بالبرامج والمعلومات

ان التلاعب بالبرامج والمعلومات يعتبر من الجرائم الشائعة التي استفحلت في الآونة الأخيرة خاصة في بلداننا العربية.

نظرا للانتشار الرهيب الذي عرفه هذا النوع من الجرائم، سارعت مختلف التشريعات الى تجريمه، ومن بين هذه التشريعات المشرع الجزائري، حيث نص على هذه الجريمة في المادة 394 مكرر 1 من قانون العقوبات "يعاقب بالحبس من ستة (6) اشهر الى ثلاث (3) سنوات وبغرامة من 500.000 دج الى 2.000.000 دج، كل من ادخل بطريق الغش معطيات في نظام او أزال او عدل بطريقة الغش المعطيات التي يتضمنها."

جريمة الدخول والبقاء الغير المشروع في النظام المعلوماتي

تعد هذه الجريمة من الأنشطة الجرمية الأكثر انتشارا، وهي تتطلب عادة تجاوز إجراءات الحماية التقنية للنظام كتجاوز كلمة السر والجدران النارية وغيرها، ويستخدم النظام المعلوماتي في هذه الحالة كوسيلة لتحقيق الولوج أو البقاء.

نص المشرع الجزائري على جريمة الدخول أو البقاء في النظام المعلوماتي في الفقرة الأولى من المادة 394 مكرر من قانون العقوبات "يعاقب بالحبس من ثلاثة (3) أشهر الى سنة (1) وبغرامة من 50.000دج الى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"

يتخذ السلوك الاجرامي في هذه الجريمة صورة الدخول أو البقاء غير المشروع في النظام المعلوماتي.

جريمة التجسس المعلوماتي

تعتبر جريمة التجسس المعلوماتي من الجرائم التي أصبحت تشكل خطرا كبيرا على الافراد وكذا المؤسسات وحتى الدول، حيث اصبح التجسس يشمل مختلف الجوانب، بدءا بالأفراد، وذلك من خلال التعدي على خصوصياتهم واسرارهم وبياناتهم الشخصية، انتقالا

الى المؤسسات التجارية والصناعية وذلك من خلال كشف الاسرار التسويقية والتجارية وكذا كشف نتائج الأبحاث الصناعية والتجارية، وصولا الى المؤسسات الأمنية والعسكرية للدول من خلال الحصول على الخطط العسكرية واسرار الدولة الحربية وحجم العتاد الحربي وغير ذلك من المعلومات التي قد يشكل الحصول عليها تهديدا حقيقيا للدول.

نص المشرع الجزائري على جريمة التجسس في المادة 64 من قانون العقوبات، واشتمل هذا النص بصفة أساسية على التجسس الذي يستهدف امن الدولة، والملاحظ ان المشرع قد راعى اخطار التجسس المعلوماتي الذي يتم بوسائل التقنية المعلوماتية، وهذا ما يستشف من الفقرة الثانية من المادة 63 من قانون العقوبات التي تقضي "..الاستحواذ بأية وسيلة كانت على مثل هذه المعلومات او الأشياء او المستندات او التصميمات بقصد تسليمها الى دولة اجنبية او احد عملائها."

جريمة الاعتداء على الحياة الخاصة على الافراد

ان الانتشار الواسع للحاسوب الآلي على مستوى الافراد أصبح يمثل تهديدا كبيرا لخصوصياتهم واسرارهم، ذلك ان الحواسب تتميز بسرعة فائقة في العمل وسعة غير محدودة في استيعاب البيانات، التي لا تنحصر فحسب في حالة تخزين هذه البيانات، بل تتعداها لاستخراج هذه البيانات من ذاكرة الحاسوب الآلي، الامر الذي يمكن القول معه بإمكانية الإطلاع على قدر لا يستهان به من هذه البيانات التي قد تكون متكاملة الى حد بعيد ومتصلة بجوانب الحياة الخاصة للفرد، وذلك بمجرد جولة سريعة قد لا تستغرق اكثر من ثوان معدودة.

مراعاة للخطورة التي قد تمثلها التقنية المعلوماتية من خطر على خصوصيات الافراد واسرارهم، قضى المشرع الجزائري في المادة 303 مكرر من قانون العقوبات "يعاقب بالحبس من ستة (6) اشهر الى ثلاث (3) سنوات وبغرامة من 50.000 دج الى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص باي تقنية كانت وذلك:

– بإلتقاط او تسجيل او نقل مكالمات او احاديث خاصة او سرية بغير إذن صاحبها او رضاه.

– بإلتقاط او تسجيل او نقل صورة لشخص في مكان خاص بغير إذن صاحبها او رضاه...."

كما يعاقب المشرع الجزائري في المادة 394 مكرر 2 كل من يقوم بحيازة او إفشاء او نشر او استعمال لاي غرض كان المعطيات التي تم الحصول عليها نتيجة الدخول او البقاء في النظام المعلوماتي وكذا نتيجة التلاعب في معطياته ومن بينها المعطيات المتعلقة بالحياة الخاصة للأفراد.

يتخذ السلوك الإجرامي في جريمة الاعتداء على الحياة الخاصة للأفراد عدة صور، ولعل من أهمها:

– الإطلاع غير المشروع على البيانات الشخصية.

– الإفشاء غير المشروع للبيانات وإساءة استخدامها.

– الإعتداء على سرية الاتصالات والمراسلات.

دوافع إرتكاب الجرائم المعلوماتية

إن الدافع هو قوة نفسية تدفع الإرادة الى الإتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو بذلك يختلف من جريمة الى اخرى، تبعا لاختلاف الناس من حيث السن والجنس ودرجة التعليم وغير ذلك من المؤثرات، كما يختلف بالنسبة للجريمة الواحدة (1). ورغم ان الدافع لا يعتبر من عناصر الجريمة الا انه يلعب دورا كبيرا في الكشف عن مجرميها. ولعل من اهم الدوافع التي تدفع المجرم المعلوماتي لارتكاب جريمته ما يلي:

---

(1): فوزية عبد الستار، شرح قانون العقوبات، الطبعة الخامسة، دار النهضة العربية، القاهرة، 1991.

البحث عن الربح المادي

البحث عن الربح المادي يعتبر من اهم دوافع المجرمين المعلوماتيين (1) ، حيث يقوم هؤلاء بتوجيه امكانياتهم ومهاراتهم وخبراتهم في مجال المعلوماتية من اجل الحصول على الأموال سواء بطريقة مباشرة، كالدخول الى أنظمة المؤسسات المالية وتحويل الأموال الى حسابات خاصة بهم، واما بطريقة غير مباشرة بإتاحة الاطلاع على معلومات معينة مقابل مبالغ مالية ضخمة، خاصة اذا كانت هذه المعلومات ذات أهمية كبيرة لطالبيها.

فقد اشارت مجلة (Informatique Sècuritè) على لسان الأستاذ (Parker) وهي مجلة متخصصة في الامن المعلوماتي ان 43 % من حالات الغش المعلن عنها قد بوشرت من اجل اختلاس اموال، و23 % من أجل سرقة معلومات، 19 % أفعال اتلاف و15 %سرقة وقت الآلة أي استعمال غير مشروع للحاسوب لأجل تحقيق منافع شخصية.

وفي الواقع فإن المحرك لاقتراف الجرائم المعلوماتية، يمكن ان ينطلق من مجرد النجاة من غرق الديون المستحقة، او من المشاكل العائلية الراجعة الى النقود او من الخسائر الضخمة لألعاب القمار او من ادمان المخدرات. (2)

إثبات التفوق العلمي

قد يكون الدافع الى ارتكاب الجريمة المعلوماتية بعيدا عن النية الاجرامية، وانما يكون مجرد رغبة في اثبات الذات من خلال تحدي تقنية الأنظمة المعلوماتية واثبات تفوقهم عليها وقدرتهم على اختراقها والدخول اليها، لدرجة أنهم وإزاء ظهور أي تقنية مستحدثة يسعون بكل الطرق الى إيجاد وسائل التفوق عليها. وقد يتولد لدى البعض منهم صفة الغرور والمتعة بحيث يقدم المجرم على ارتكاب الجريمة تعاليا وتفاخرا بقدرته على احداث الاثار المترتبة عنها.

---

(1) : Philippe Rosè, La criminalité informatique, deuxième édition, Edition Dahleb, 1995

(2): محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدثة،المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ،من 25 الى 28 أكتوبر 1993.

الانتقام

يعد دافع الانتقام من أخطر الدوافع التي يمكن أن تدفع الشخص الى ارتكاب جريمة، لأن هذا الدافع غالبا ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، لأنه غالبا ما يكون أحد موظفيها، و يكون له هذا الدافع – الانتقام – نتيجة اما لفصله من العمل أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته (1). فعلى سبيل المثال، دفع الانتقام بمسؤول عن النظام، تم طرده من المؤسسة التي يعمل بها سنة 1999، الى زرع قنبلة منطقية في برنامج موجود في آلات العمل لمستخدمه السابق، مما أدى إلى تعطيل المؤسسة عن العمل لمدة شهر كامل.

التجسس

قد يكون الدافع الى ارتكاب الجريمة المعلوماتية هو جمع معلومات لمصلحة جهات معينة قد تكون اشخاص او مؤسسات او دول، حيث أصبحت المعلومات في الوقت الحاضر تشكل سلاحا فتاكا في يد من يمتلكه. ولهذا تسعى العديد من الجهات الى تجنيد افراد تكون مهمتهم الأساسية هي القيام بعمليات التجسس لصالحها، فالتنافس الاقتصادي أدى بالمؤسسات الى السعي جاهدة للحصول على الاسرار التسويقية وخطوات الإنتاج وكذا عناوين العملاء، وغير ذلك من المعلومات التي تخص نظيراتها من المؤسسات. كما ان التسابق الفضائي والعسكري والنووي أدى بالدول الى تكثيف عمليات التجسس من خلال اختراق النظم الأمنية والعسكرية والنووية من اجل الحصول على المعلومات التي تجعلها قادرة على مواجهة أي خطر يهددها.

---

(1): أيمن عبد الحفيظ ،الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية، (دون دا نشر)، 2005.

المبحث الثـاني: مراحل إثبات الجريمة المعلوماتية

تمهيد:

إن الجريمة المعلوماتية تعتبر كأي جريمة من الجرائم المنصوص عليها في قوانين العقوبات والقوانين الأخرى، فلذلك تتسع الجريمة المعلوماتية بدعوى عمومية وهذه الدعوة تتم بمراحل وهي عمل دراستنا، مرحلة البحث والتحري ومرحلة التحقيق.

المطلب الأول: مـرحلـة البحث والتحري في الجريمة المعلوماتية

إن هذه المرحلة من اختصاص ضباط الشرطة القضائية وهم نوعان، النوع الأول هم الذين يتمتعون باختصاص عام ويختصون بإجراءات الاستدلال بشأن الجرائم المنصوص عليها في قانون العقوبات ، أما النوع الثاني : فهم ذو الاختصاص النوعي المحدود بخصوص نوع معين من الجرائم حددها القانون على سبيل الحصر هؤلاء المشار اليهم في المادة 21 من قانون الإجراءات الجزائية وسلطتهم كذلك محددة لا تمتد إلى مرحلة التفتيش ودخول المنازل والمعامل والمباني أو الأماكن المحاطة بأساور إلا بحضور أحد ضباط الشرطة القضائية ومن بين هؤلاء رؤساء الأقسام المهندسون وأعوان الغابات وحماية الأراضي وتعد محاصرتهم ذات حجية وقوة إثبات كما استقر عليه القضاء الوطني.

وما يهمنا في هذه الدراسة هو دور الضبطية القضائية ومجال اختصاصها فيما يتعلق بالجريمة المعلوماتية.

الفـرع الأول: الإجـراءات التقليدية لـجمع الـدليل.

سنتطرق في هذا الفرع إلى إجرائيين الإجراءات المادية والإجراءات الشخصية.

أولا: الإجـراءات المـاديـة: تتمثل هذه الإجراءات في المعاينة والتفتيش والضبط.

1/ **المعـاينة:** هي رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة.

وتعتبر المعاينة إجراءا من إجراءات التحقيق التي تقوم بها سلطة التحقيق بنفسها أو تندب ضباط الشرطة القضائية للقيام بها. كما يمكن للمحكمة أن تقوم بإجراءات معاينة إذا رأت. (1)

ذلك يستدعي لكشف الحقيقة سواء كان ذلك من تلقاء نفسها أو بناءا على طلب من الشخص المعني بعد موافقة القاضي المختص بناءا على طلب عريضة. (2)

كيفية إجـراء المعـاينة التقنية لمسرح الجـريمة المعلوماتية.

عند العلم بوقوع الجريمة فإن أول خطوة يقوم بها مأمور الضبط القضائي هو الانتقال إلى مسرح الجريمة، لأن هذا الأخير حجز الزاوية في التحقيق الجنائي ومكمن الآثار والأدلة المادية، وينبغي التعامل في الإطار مع مسرح الجريمة المعلوماتية على أنه مسرحان هما:

المسرح تقليدي: يقع خارج البيئة المعلوماتية لأنه يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة، وهو أقرب إلى مسرح الجريمة التقليدية ويترك فيها الجاني عدة أثار كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.

المسرح افتراضي: يقع داخل البيئة المعلوماتية، لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الأنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله. (3)

ونظرا لاختلاف مسرح الجريمة عن غيره من الجرائم الأخرى فينبغي التعامل الخاص مع هذه

---

(1): عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، كلية الحقوق جامعة الإسكندرية، 2006.

(2): نفس المرجع، ص 84.

(3): نفس المرجع، ص 85، 86.

الجريمة وذلك بإتباع عدة قواعد فنية قبل الانتقال المسرح الجريمة المعلوماتية والمتمثل في:

– ضرورة وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكاتها.

– وجود خريطة توضح الموقع الذي سيتم معاينته وتفاصيل المبنى أو الطابق موضوع البلاغ، وعدد الأجهزة والخزائن والملفات ويحدد ذلك من خلال مصادر سرية لجهات الأمن.

– تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية حتى يتم تحديد كيفية التعاون معها فنيا قبل المعاينة.

– تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج.

– إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن.

– تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة على حده، وذلك حتى لا تتداخل الاختصاصات.

– إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل.

– أن تتم هذه المعاينة وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية.

– تأمين عدم انقطاع التيار الكهربائي لأن معاينة الأجهزة وما بها من برامج وشبكات وأنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي. (1)

2– تفتيش في البيئة المعلوماتية:

أ– تعـريف التفتيش:

ان التفتيش المنصب على منظومة المعلوماتية يختلف عن التفتيش المتعارف

---

(1): عائشة بن قارة مصطفى، المرجع السابق، ص 87.

عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية والوضعية وموضوع التفتيش.

على رغم من إن المشرع الجزائري اعتبر التفتيش إجراء من الإجراءات التحقيق وإحاطته بقواعد صارمة إلا أنه لم يورد تعريفا خاصا ودقيقا وقد اهتم الدستور الجزائري بعدم مساس بحرية الأشخاص وكرامتهم وأكد ذلك في المادة 40 منه بالقول: " فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة."

وفي الأخير أن التشريعات العربية تتفق على تعريف التفتيش بأنه إجراء من إجراءات التحقيق غايته ضبط الأدلة الجريمة موضوع التحقيق وكل ما يفيد الحقيقة في شأنها. (1)

ب- شـــروط التفتيش:

ان شروط التفتيش تنقسم إلى نوعين: شروط شكلية وموضوعية.

/1الشــروط الشكليــة للتفتيش:

حددت المادة 44 من قانون الإجراءات الجزئية الجزائري سيما بعد التعديل الذي حصل بموجب القانون 06-22 في 20 سبتمبر 2006 وهي: (2)

1- وجود إذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق.

2- الاستظهار بالإذن قبل دخول المنزل المراد تفتيشه.

---

(1): زيبخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، د ط، 2011، ص 130، 131.

(2): نفس المرجع، ص 20، 21.

3- أن يتضمن الإذن بيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش.

4- حضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه.

5- في حالة رفض الحضور يستدعي ضابط الشرطة القضائية شاهدين من غير الموظفين الخاضعين لسلطته. (1)

6- الميقات الزمني لإجراء التفتيش في الجرائم المعلوماتية: يقصد الفترة في القانون الإجراءات الجزائية الجزائري في المادة 47 منه على أنه من الساعة الخامسة صباحا ألى الساعة الثامنة مساءا أما إذا طلب صاحب المنزل ذلك وجهت نداءات من الداخل أو في الأحوال أما الإستثنائية المقررة قانونا .وهناك حالات إستثنائية كحالة الطوارىء وغيرها يجوز التفتيش في كل ساعة من ساعات الليل أو النهار.

أما في قانون العقوبات الفرنسي فنجده مهدد من الساعة السادسة صباحا إلى الساعة التاسعة مساءا طبقا لنص المادة 55 قانون الإجراءات الجزائية الفرنسي إلا أن هناك حالات إستثنائية يصح فيها إجراء التفتيش ليلا أو نهارا تتمثل في حالة رضا صاحب المنزل وحالة الضرورة كحالة الإستغاثة من داخل المنزل وخالتي الحريق والغرق أو ماشابه ذلك.

7- محضر التفتيش في الجرائم المعلوماتية: يتم تحرير محضر لكي يثبت فيه ماتم من إجراءات وما أسفر عنه التفتيش من أدلة ولم يتطلب القانون شكل خاص للمحضر التفتيش وبالتالي لايشترط لصحته سوء ما تستوجبه القواعد العامة في المحاضر عموما. (2)

---

(1): مولود ديدان، قانون الإجراءات الجزائية، دار بلقيس الجزائر، د ط، ديسمبر 2014، ص 121.

(2): عائشة بن قارة مصطفى، المرجع السابق، ص 111 ،103، 104

2/ الشــروط الموضـوعيـة للتفتيش:

يقصد بهذه الشروط بصفة عامة الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، ويمكن حصرها في ثلاث شروط: أساسية هي: السبب، المحل، السلطة المختصة بالقيام به، وسنفصل كل شرط على حدا:

- **سبب التفتيش:** الهدف من هذا السبب هو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث ويتمثل في وقوع الجريمة ما جناية أو جنحة واتهام شخص أو أشخاص معينين في كشف الحقيقة لدى المتهم أو في مسكنه أو بشخص غيره أو مسكنه. (1)

- **محــل التفتيش:** محل التفتيش في الجريمة المعلوماتية هو الحاسب والشبكة التي تتمثل في مكوناتها الخادم والمزود الالى والمضيف والملحقات التقنية.

- **السلطـة المختصة بالتفتيش:** الأصل أن التشريع المصري يمنح لنيابة العامة سلطة الإختصاص بالتفتيش على خلاف التشريع الفرنسي والجزائري اللتا أخذتا بنظام الفصل بين سلطتي الإتهام والتحقيق أما الإستثناء يمنح لضباط الشرطة القضائية هذا الإختصاص في الحالات التالية:

- **بـطلان إذن التفتيش:**

إن مراقبة المحادثات الهاتفية (سلكية أو اللاسلكية) وتسجيلها هو إجراء من إجراءات التفتيش إلا أنه نظرا لخطورة هذا الإجراء باعتباره يتعرض لمستودع سر الفرد ويزيل الحظر على بقاء سريته مقصورة على نفسه ومن أراد ائتمانه عليه فيباح لغيره الإطلاع على مكنون سره فقد حرص الدستور وقانون إجراءات الجنائية على تأكيد ذلك واشتراط لمراقبة المحادثات الهاتفية (سلكية أو اللاسلكية) صدور أمر قضائي مسبب.

---

(1) : المواد 34 و 60 و 70 ، قانون الإجراءات الجنائية المصري مع اخر تعديلاته لقانون رقم 153 لسنة 2007 والمؤرخ في 2007/6/16 ، المنشورات الجريدة الرسمية ، العدد 24 مكرر.

3/ الضبط:

إن الضبط في قانون الإجراءات الجزائية هو وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها. (1)

ان الضبط في الجريمة المعلوماتية يختلف عن ضبط في الجرائم الأخرى من حيث المحل لأن الجريمة المعلوماتية يردالضبط على الأشياء ذات طبيعة معنوية وهي البيانات والمراسلات والإتصالات المعلوماتية من جعة ولها طبيعة مادية كالورق والكمبيوتر وملحقاته والأقراص الصلبة الخارجية والمرنة وأقراص الليزر البطاقات الممغنطة.

ثـانيـا ــ الإجـراءات الشخصيـة:

سنتطرق في هذه المجموعة التي ذات طبيعة شخصية لأنه غالبا ما يتوسط فيها الشخص بين القيام بالاجراء والحصول على الدليل وتتمثل هذه الإجراءات في: عملية التسرب، الشهادة، والخبرة التقنية، استجواب المتهم.

1/ التســـرب:

جاءت المادة 65 مكرر 12 قانون الإجراءات الجزائية الجزائري تعرف التسرب بأنه "يقصد بالتسرب ضباط أعوان الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإتهامهم أنه فاعل معهم أو شريك لهم خاف. (2)

يسمح لضباط الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وإن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 أدناه ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريض على إرتكاب الجرائم. (3)

---

(1): عائشة بن قارة مصطفى ، المرجع السابق ، ص 201 ، 114.

(2): زبيحة زيدان، المرجع السابق، ص 169.

(3): زبيحة زيدان ، نفس المرجع ، ص 169.

أما بالنسبة لمواصفـات الأذن بالتسـرب وطبيعته حددتها المادة 65 مكرر15 من قانون الإجراءات الجزائية وهي:

1. أن يسلم فقط لضرورة التحري أو التحقيق القضائي.
2. أن يكون مكتوبا.
3. أن يكون مسببا.
4. أن يذكر في الإذن طبيعة الجريمة التي ينص عليها الإذن.
5. يذكر فيه هوية ضابط الشرطة القضائية المعني أو الذي تتم العملية تحت مسؤوليته.
6. يحدد فيه المدة المقررة للعملية والمحددة بأربعة (4 (أشهر وهي قابلة للتجديد لمدة 4 أشهر أخرى كل ما دعت الضرورة لذلك.
7. أن تودع الرخصة أي الإذن في ملف الإجراءات بعد الإنتهاء من عملية التسرب.

وملاحظة على ذلك أنه إذا أغفل شرط من هذه الشروط يؤدي إلى بطلان الإذن. (1)

خرج المشرع الجزائي عن الأصل العام في التحقيق القائم بالفصل بين سلطتي الإتهام والتحقيق وأو كل لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية مهمة إصدار الإذن بالتسرب.

2/ الشهـادة في الجـريمة المعلوماتية:

أ- **تعـريف الشـاهد في الجـريمة المعلوماتية:** يطلق عليه إسم الشاهد المعلوماتي لأنه هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الالي والذي يكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الالية للبيانات فلذلك نجد أن الشاهد المعلوماتي

(1): مولود ديدان، قانون الإجراءات الجزائية، المرجع السابق، ص 35.

ينحصر في عدة طوائف تتمثل في: مشغلة الحاسب الالي، خبراء البرمجة، المحللون، مهندسوا الصيانة والإتصالات، مديرو النظم.

ولشاهد إلتزامات لابد التقيد بها مثل: طبع ملفات البيانات المخزنة في ذاكرة الحاسوب الآلي أو الدعامة الأخرى على أن يقوم بطبعها وتسليمها إلى سلطات التحقيق والإفصاح عن كلمات المرور السرية والكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة.

3- الخبـرة في الجـريمة المعلوماتية:

لابد أن يكون الخبير صاحب مقدرة وإمكانيات العلمية والفنية في مسألة موضوع الخبرة ويستطيع القيام بدوره وللقيام بهذا الأخير عليه أن يبين المكان المحتمل لأدلة الإثبات وشكلها وهيئتها والأثار إقتصادية والمالية المترتبة على التحقيق في الجريمة المعلوماتية وكيفية عزل النظام المعلوماتي عند الحاجة دون إتلاف الأدلة أو الأجهزة أو تدميرها.

4- إستجـواب المتهم فـي الجـريمة المعلوماتية:

أحالت التشريعات إستجواب المتهم بضمانات خاصة وذلك في القسم الخامس من الباب الثالث الكتاب الأول من قانون الإجراءات الجزائية وتتمثل في حق الإستعانة بمحام أثناء الإستجواب وتمكينه من الإطلاع على ملف والإتصال به.

والإستجواب ماهو إلا مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق ومطالبته بإبداء رأيه في الأدلة القائمة ضده إما تنفيذا أو تسليما، وذلك قصد محاولة كشف الحقيقة وإستظهارها بالطرق القانونية .أحالت التشريعات إستجواب المتهم بضمانات خاصة وذلك في القسم الخامس من الباب الثالث الكتاب الأول من قانون الإجراءات الجزائية وتتمثل في حق الإستعانة بمحام أثناء الإستجواب.

الفـــرع الثـــاني: الإجـــراءات الحـــديثة لجمع الـدليـل المعلوماتي

أولا: الإجـراءات المتعلقة بالبيـانـات السـاكنة:

1- التحفظ المعجـل على البيـانـات المخـزنـة:

في مادة مادة 16 من إتفاقية بودابيست نصت على ضرورة كل طرف السماح لسلطاته المختصة أن تأمر أو تفرض بطريقة أخرى مزود الخدمة التحفظ العاجل على البيانات المعلوماتية المخزنة بما في ذلك البيانات المتعلقة بالأمور المخزنة بواسطة نظام المعلوماتي، وذلك ما تكون هناك أسباب تدعو للإعتقاد بأن هذه البيانات على وجه الخصوص معرفة للفقد أو التغيير، وذلك من خلال مدة 90 يوم كحد أقصى وهذه المدة قابلة للتمديد.

2- مقصـود بمـزودي الخـدمـات: مزود الخدمات هو من يقدم خدمته إلى الجمهور بوجه عام في مجال الاتصالات المعلوماتية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود.

3- مفهـوم التحفظ المعجـل على البيـانـات المخـزنـة:

يقصد به توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته، في أنتظار اتخاذ أجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية ". (1)

ثانيـا: الإجـراءات المتعلقة بالبيـانـات المتحـركـة (اعتـراض الاتصالات الإلكتـرونية):

1- حـرمـة الإتصـالات الإلكتـرونية الخـاصة:

نتيجة لتطور التكنولوجي الذي أدى إلى إفراز أجهزة المراقبة ذات تقنية إلى مراقبة الأحاديث تمس بحق الإنسان في الخصوصية ومايتفرغ عنه من سرية الأحاديث الخاصة،

(1): عائشة بن قارة مصطفى ، المرجع السابق ، ص 155 ،159.

وهو لصرف الصلة بالإنسان.

فلذلك أقرت معظم التشريعات على توفير قدر كبير من الحماية الجنائية على سرية الاتصالات الخاصة للأفراد، حيث عاقب المشرع الجزائري لأول مرة اعتراض الاتصالات السلكية واللاسلكية دون إذن بذلك " بموجب القانون رقم (06-23) المؤرخ في 20 ديسمبر 2006 المعدل لقانون العقوبات الجزائري، حيث تنص المادة 303 مكرر من قانون العقوبات على أنه " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 000.50 دج إلى 000.300 دج كل من تعمد الماس بحرمة الحياة الخاصة للأشخاص، بأي تقنية كانت وذلك:

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

2- بالتقاط أو تسجيل أو نقل صورة لشخص من مكان خاص ، بغير إذن صاحبها أو رضاه"

3- ويعاقب على شروع في هذه الجرائم بنفس عقوبات الجريمة التامة.

ولم تقتصر الحماية عند التجريم الأطفال الخاصة بالاعتراض، بل شملتها أيضا إلى عقاب كل من احتفظ أو دفع أو سمح بأية وسيلة كانت التسجيلات المتحصل عليها بأحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون.

أما بالنسبة للمشرع المصري فقد عاقب بالحبس مدة لا تقل من سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن. (1)

ب/ إعتـراض الاتصـالات الإلكتـرونية بنـاء على إذن:

مما لا شك فيه أن الحماية التي يكفلها المشرع للإتصالات العادية لا تقتصر نطاقها على هذا النوع من الإتصالات فحسب ، بل تمتد هذه الحماية إلى الاتصالات الإلكترونية عبر

---

(1): عائشة بن قارة مصطفى ، المرجع السابق ، ص 169.

الانترنت من باب أولى بحسبان أن الغاية من وراء هذه الحماية هي حماية الحياة الخاصة للإنسان بحماية مستودع أسراره الشخصية، هذه الأسرار تكون أكثر انتهاكا إذا ما استخدمت الوسائل المعلوماتية في الوصول إليها ، ومن ثم فإنها تكون في حاجة إلى حماية أكثر من تلك الحماية التي تحتاجها الاتصالات العادية ، وإذا اقتضت ضرورة التحقيق اعتراض هذه الاتصالات وتسجيلها ، فستتبع حينها نفس الضمانات المقررة للمحادثات التلفونية ، مع مراعاة خصوصية هذه الاتصالات الحديثة ، وتتمثل أهم الضمانات القانونية فيما يلي:

السلطة المختصة بإصدار إذن الإعتراض:

إصدار إذن من طرف سلطة القضائية تعد ضمانة لازمة لمشروعية الإعتراض على الإتصالات السلكية واللاسلكية في القانون الفرنسي.

المطلب الثاني: مرحلة التحقيق في الجريمة المعلوماتية

تعتبر هذه المرحلة هي المرحلة الثانية بعد مرحلة جمع إستدلالات وستختص في هذا المطلب على دراسة هذه المرحلة.

الفرع الأول: تعيين قاضي التحقيق

في الجزائر يتعين قاضي التحقيق بمقتضى قرار من وزارة العدل ، ثم عدل المشرع عن ذلك بموجب القانون 01 ــ 08 المؤرخ في 26 جوان 2001 .وأصبح التعيين بموجب مرسوم رئاسي ، وفقا لنص المادة 39 قانون الإجراءات الجزائية ، إلا أنه حت هذه الأخيرة تم الغائها بموجب القانون رقم 06ـ22 المؤرخ في 20 ديسمبر 2006 ليرجع من جديد للتعيين (1) بموجب قرار من وزير العدل بعد إستشارة الأعلى للقضاء من بين قضاة الجمهورية ، وهذا رجوعا إلى نص المادة 50 من قانون الأساسي للقضاة ، وتكون مدة التعيين ثلاث سنوات ، وتنتهي مهام قاضي التحقيق بنفس الأشكال التي يتعين فيها ، أي بقرار من وزير العدل. (2)

---

(1): عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، دار بلقيس لنشر، د ط ، 2015 ، ص 224.

(2): نفس المرجع، ص 223، 224.

أما في مصر يكون ذلك بناء على طلب النيابة العامة أو طلب من المتهم أو المدعي بالحقوق المدنية إلى رئيس المحكمة الإبتدائية التي يكون الجريمة قد وقعت في دائرة إختصاصها أو التي يقيم فيها أو التي ضبط فيها طبقا لنص المادة 217 قانون الإجراءات الجزائية فيجوز لرئيس المحكمة الإبتدائية رفض الطلب المقدم من طرف المتهم أو المدعي بالحقوق المدنية بقرار لايقبل الطعن فيه.

الفـرع الثـاني: إختصـاص قـاضي التحـقيـق

سنتناول في هذا العنصر قواعد الإختصاص الشخصي ثم النوعي وأخيرا المحلي لقاضي التحقيق.

أولا: الإخـتصـاص الشخصـي

لأصل أن قاضي التحقيق يحقق مع جميع الأشخاص دون تمييز ، إلا أن المشرع الجزائري إستثنى بعض الفئات كالأحداث العسكريين ضباط الشرطة القضائية قضاة الحكم والتحقيق ومساعدي وكيل الجمهورية قضاة المجالس القضائية ورؤساء المحاكم ووكلاء الجمهورية قضاة المحكمة العليا ورؤساء المجالس القضائية والنواب العامون وأعضاء الحكومة والولاة.

ويختص كذلك بالتحقيق مع جميع الجرائم القانون العام سواء كانت جناية أو جنحة أو مخالفة التي من خلالها تقدم النيابة العامة طلب إفتتاحي أو الجنايات أو جنح التي من خلالها يقدم الطرف المدني إدعاء مدنيا. (1)

ثـانيا: الإختصـاص النـوعـي

يختص قاضي التحقيق بالتحقيق في جميع الجرائم ويكون ذلك وجوبي في الجنايات وجوازي في الجنح إذا كان هناك نص وإختياري في المخالفات طبقا لنص المادة 66 من قانون _____

(1): عبد الرحمان خلفي ، المرجع السابق ، ص 226 ، 227 ، 228.

الإجراءات الجزائية التحقيق الإبتدائي وجوبي في مواد الجنايات أما في مواد الجنح فيكون إختياري مالم يكن ثمة نصوص خاصة، كما يجوز إجراءه في مواد المخالفات إذا طلبه وكيل الجمهورية.

إن قاضي التحقيق يختص في المحاكم الجهوية في الجرائم التي إختصها المشرع بالنظر في الجرائم المخذرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الالية للمعطيات وجرائم تبييض الأموال والإرهاب وجرائم الصرف طبقا للمرسوم التنفيذي رقم06 ـ 348 المؤرخ في 2006/10/5. (1)

ثـالثا: الإختصـاص المحـلي

تنص المادة 40 من قانون الإجراءات الجزائية " يتحدد إختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في إقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر..." يمتد إختصاص قاضي التحقيق إلى أكثر من محكمة طبقا لنص المادة 2/40 مكرر من قانون الإجراءات الجزائية.

الفـرع الثـالث: سلطـات قـاضي التحقيق وحـدود الدعوى الجنائية أمامه

القيام بإتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة وبالتحري عن أدلة الإتهام وأدلة النفي المادة 68 قانون الإجراءات الجزائية.

يجوز لقاضي التحقيق أن يأمر بإجراء فحص الطبي كما له أن يعهد إلى الطبيب بإجراء فحص نفساني أو يأمر بإتخاذ أي إجراء يراه مفيدا المادة 68 قانون الإجراءات

(1): عبد الرحمان خلفي ، المرجع السابق ، ص ، ص 228.

الجزائية .ينسق القاضي المكلف بالتحقيق سير إجراءات التحقيق وله وحده الصفة في مسائل الرقابة القضائية والحبس المؤقت إتخاذ أوامر التصرف في القضية طبقا لنص المادة 70 قانون الإجراءات الجزائية. (1)

– يستطيع القاضي سماع أقوال كل من يشير إليهم في الشكوى بإعتبارهم شهودا طبقا لنص المادة 73 قانون الإجراءات الجزائية.

– يستطيع القاضي التحقيق الإنتقال إلى أماكن وقوع الجرائم لإجراء جمع المعاينات اللازمة أو القيام بتفتيشها طبقا لنص المادة 79 قانون الإجراءات الجزائية.

– إستدعاء كل شخص يرى فائدة من سماع شهادته بواسطة أحد أعوان القوة العمومية طبقا لنص المادة 88 قانون الإجراءات الجزائية.

– يجوز للقاضي إستدعاء مترجم طبقا لنص المادة 91 قانون الإجراءات الجزائية.

– إصدار أمر بإحضار المتهم أو بإيداعه السجن أو بإلقاء القبض عليه حسب نص المادة 109 قانون الإجراءات الجزئية. (2)

– تفتيش المتهم، وتفتيش المسكن غير مسكن المتهم، ومراقبة المحادثات السلكية واللاسلكية، وضبط الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات لدى مكاتب البريد والبرق حسب نص المادة 91 و94 و95 قانون الإجراءات الجزائية المصري. (3)

الفـرع الـرابـع: سمـات التـي يتميـز بهـا قـاضي التحقيق بالنسبة للجريمة المعلوماتية

إن الجريمة المعلوماتية تختلف عن الجريمة التقليدية فلذلك لايمكن أن يحقق فيها أي قاضي تحقيق وإنما لابد أن يكون له صفات خاصة وهذه الصفات هي:

---

(1): مولود ديدان ، قانون الإجراءات الجزائية ، المرجع السابق ، ص 18، 39، 40.

(2): نفس المرجع، ص 40، 42، 45، 50.

(3): المادة 91 و94 و95 قانون الإجراءات الجزائية المصري رقم 153 المرجع السابق.

كأن يكون لديه معرفة بلغات البرمجة وأنظمة التشغيل الجديدة وأن يميل إلى تصميم البرامج أكثر من تشغيلها ويحب معرفة الجديد عن هذه البرامج وأن يستطيع تصميم ونحليل البرامج أو أنظمة التشغيل بسرعة وأن يؤمن بوجود أشخاص اخرين مثله لديهم القدرة على إختراق والشبكة وكل هذه الأمور لا تتوافر إلا لمن كان لديه إمكانات عقلية تزيد على متوسط العام المألوف.

الفـرع الخـامس: كيفية إتصـال قـاضي التحقيـق بملف الـدعوى خـاص بالجـريمة المعلوماتية

يتصل القاضي التحقيق بملف الدعوى إما عن طريق وكيل الجمهورية بموجب إجراء تحقيق رسمي لطلب الإفتتاحي لإجراء تحقيق، وإما عن طريق شكوى جزائية مقدم من المضرور وهذا ماأكدته 3/38 من قانون الإجراءات الجزائية الجزائري على "... يختص بالتحقيق في الحادث بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في المادتين 67 و73." (1)

أولا: الطلب الإفتتـاحي لإجـراء التحقيـق

يتصل وكيل الجمهورية بملف ضباط الشرطة القضائية فيمكن لوكيل الجمهورية أن يطلب فتح التحقيق ما لم ينص القانون على وجوب التحقيق في بعض الجنح، ويمكن لوكيل الجمهورية أن يقدم طلبا إضافيا لقاضي التحقيق إذا أظهرت وقائع جديدة طبقا للمادة 67/3 قانون الإجراءات الجزائية الجزائري على أنه " لايجوز لقاضي التحقيق أن يجري تحقيقا إلا بموجب طلب من وكيل الجمهورية لإجراء التحقيق حتى ولو كان ذلك بصدد جناية أو جنحة متلبس بها. (2)

ويتقيد القاضي التحقيق بالوقائع دون الأشخاص طبقا المادة 3/67 و4 من قانون

(1): مولود ديدان ، قانون الإجراءات الجزائية ، المرجع السابق ، ص 17.
(2): عبد الرحمان الخلفي ، المرجع السابق ، ص 330.

الإجراءات الجزائية " ...ولقاضي التحقيق سلطة الإتهام كل شخص ساهم بصفته فاعلا أو شريكا في الوقائع المجال تحقيقها إليه.

فإذا وصلت لعلم قاضي التحقيق وقائع لم يشير إليها في طلب إجراء التحقيق تعين عليه أن يحيل فورا إلى وكيل الجمهورية الشكاوى أو المحاضر المثبتة لتلك الوقائع. (1)

ثـانيا /الشكـوى المصحـوبـة بـإدعـاء المـدني:

تنص المادة 72 من قانون الإجراءات الجزائية " يجوز لكل شخص تضرر من جناية أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص". (2)

ان إحدى طرق تحريك الدعوى من طرف الأفراد ، وهي في نفس الوقت إحدى طرق إتصال قاضي التحقيق بملف الدعوى.

ويلجأ عادة المتضرر من الجريمة إلى هذه الطريقة تجنبا لطول الإجراءات وتقليصا للوقت، وحرصا منه على أن يكون الإشراف على على ملف من طرف قاضي التحقيق لا أن يكون من طرف الضبطية القضائية التي عادة يكون لها تأثير على مجرى التحقيق، كما أنه يستفيد من تتبع مجريات الدعوى العمومية بنفسه طالما كان هو من حركها.

إلا أن أخطر سلبيات الإدعاء المدني يتمثل في سوء إستعمال هذا الطريق لأن من شأنه أن يعرض الطرف المدني إلى متابعة جزائية بتهمة الوشاية كاذبة إذا ما خسر دعواه، ولهذا عليه أن يتأكد من أن إتهامه كان مبنيا على دليل قوي في الدعوى. (3)

---

(1): مولود ديدان ، قانون الإجراءات الجزائية ، المرجع السابق ، ص 37

(2): عبد الرحمان الخلفي ، المرجع السابق ، ص 231

(3): نفس المرجع، ص 231 ، 233.

الفـرع السـادس: إستئنـاف أوامـر قـاضـي التحـقيق

الجهات التي تستأنف أوامر قاضي التحقيق هي:

أولا ـــ النيـابـة العـامة:

لوكيل الجمهورية أو أحد مساعديه إستئناف جميع أوامر قاضي التحقيق دون إستثناء وذلك طبقا لنص المادة 170 من قانون الإجراءات الجزائية الجزائري " الوكيل الجمهورية في أن يستأنف أمام غرفة الإتهام جميع أوامر قاضي التحقيق.

ويكون هذا اللإستئناف تقرير لدى قلم كتب المحكمة ويجب أن يرفع في ثلاثة أيام من تاريخ صدور الأمر..." (1)

يجوز للنائب العام الطعن في أوامر قاضي التحقيق في ظرف 20 يوما على ألا يكون لهذا الطعن أثر موقف في حالة إستئناف أمر الإفراج ظرف 20 يوما على ألا يكون لهذا الطعن أثر موقف في حالة إستئناف أمر الإفراج ويفرج على المتهم رغم ستئناف النائب العام مالم يكن وكيل الجمهورية قد إستأنفه بالطبع ويجب أن يبلغ النائب العام عند إستئنافه الخصوم في الدعوى، وذلك خلال العشرين يوما التالية لصدور الأمر حتى يكونوا على بينة من أمرهم ولايفاجؤا بقرار من غرفة الإتهام في غير صالحهم. (2)

طبقا لنص المادة 171 من قانون الإجراءات الجزائية الجزائري " يحق الإستئناف أيضا للنائب العام في جميع الأحوال ويجب أن يبلغ إستئنافه للخصوم خلال العشرين يوما التالية لصدور أمر قاضي التحقيق ولايوقف هذا الميعاد ولا رفع الإستئناف بتنفيذ الأمر بالإفراج المؤقت". (3)

---

(1): عبد الرحمان خلفي ، المرجع السابق ، ص231 ، 233

(2): مولود ديدان ، قانون الإجراءات الجزائية ، المرجع السابق ، ص 78.

(3): عبد الرحمان خلفي ، نفس المرجع، ص 296.

ثـــانيا ـــــ إستئنـــاف المتهم:

إن المتهم لايجوز له إستئناف جميع أوامر قاضي التحقيق و يرفع الإستئناف بعريضة تودع لدى قلم مكتب المحكمة في ظرف ثلاثة (3) أيام من تبليغ الأمر إلى المتهم طبقا للمادة 168 قانون الإجراءات الجزائية.

ثـــالثـا ـــــ إستئنـــاف المـــدعـــي المـــدنـــي:

كما أجاز المشرع الجزائري للمدعي المدني الحق في إستئناف أوامر قاضي التحقيق التي لها علاقة بحقوقه المدنية، وبمفهوم المخالفة لايجوز له إستئناف الأوامر المتعلقة بالجانب الجزائي مثل الحبس المؤقت والإفراج والرقابة القضائية. (1)

ويرفع الإستئناف خلال (03) يام من تاريخ تبليغ الأمر المراد إستئنافه إلى المدعي المدني، وذلك بتقديم عريضة لدى قلم كاتب ضبط قاضي التحقيق طبقا لنص المادة 3/173 قانون الإجراءات الجزائية. (2)

---

(1): عبد الرحمان خلفي ، المرجع السابق ، ص 298

(2): مولود ديدان ، قانون الإجراءات الجزائية ، المرجع السابق ، ص 79

المبحث الأول: مرحلة المحاكمة

المطلب الأول: جهة الحكم في الجريمة المعلوماتية

الفرع الأول: الإختصـاص المحـلي فـي الجـريمة المعلوماتية

طبقا نص المادة 37 من قانون الإجراءات يتحدد الإختصاص المحلي للجريمة في ثلاث ضوابط في أو المكان إقامة المتهم أو مكان ضبط

كما نصت أحكام المرسوم التنفيذي رقم 06 ــ 348 المؤرخ في 5 أكتوبر 2006 على تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دائرة إختصاص محاكم أخرى، ويتعلق الأمر بكل من محكمة سيدي محمد بالجزائر العاصمة وكذا محكمة قسنطينة ومحكمة ورقلة وقسم محكمة وهران.

وفي نطاق الجرائم المعلوماتية فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس وتتحقق النتيجة بتدمير المعلومات في مكان اخر، فإن الإختصاص ينعقد إما في مكان السلوك أو مكان تحقق النتيجة، وتعد الجريمة المعلوماتية إذا تمت عن طريق شبكة الأنترنت جريمة مستمرة حيث تعتبر أنها إرتكبت في جميع الأماكن التي إمتدت الجريمة فيها.

ومتى كانت الجريمة المعلوماتية، أيا كان نوعها، فقد وسع المشرع الجزائري من إختصاص المحاكم الجزائية بالنظر في الجرائم المعلوماتية أو المتصلة بتكنولوجيات الإعلام والإتصال إذا إرتكبت خارج الإقليم الوطني، أو إذا كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإقتصادية الإستراتيجية للدولة وذلك في إطار التعاون الدولي.

ثـانيـا/: الإختـصـاص النـوعـي في الجـريمة المعلوماتية:

يتحدد الإختصاص النوعي للمحكمة الفصل في القضية معروضة عليها تبعا لنوع الجريمة التي ينظر فيها، حيث تختص محكمة الجنايات في الفصل في الجنايات والجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الإتهام حسب نص المادة 248 من قانون الإجراءات الجزائية الجزائري، كما تختص المحاكم في النظر في الجنح والمخالفات فيما عدا الإستثناءات المنصوص عليها في قوانين خاصة حسب المادة 328 قانون الإجراءات الجزائية.

ولأن الطبيعة التقنية المعقدة للجرائم المعلوماتية تفرض على رجال القضاء لتكوين يمكنهم من متابعة هذه الجرائم فقد خصها المشرع مع بعض أنواع الجرائم المتعلقة بالمتاجرة بالمخذرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبيض الأموال والإرهاب ، والجرائم المتعلقة بالتشريع الخاص بالصرف بإجراءات خاصة إذا جعل الإختصاص ينعقد إلى دائرة إختصاص أخرى وهذا مانصت عليه المواد 37 ، 40 ، والمادة 329 من قانون الإجراءات الجزائية أثر التعديل الذي جاء به القانون رقم 04 ـ 14 المؤرخ في 10 نوفمبر 2004 والذي حددت أحكامه في المرسوم التنفيذي رقم 06 ــ 348 والمتعلق بالتنظيم القضائي حيث نص على إنشاء أقطاب قضائية متخصصة ذات إختصاص إقليمي موسع لدى المحاكم بكل من الجزائر العاصمة ، قسنطينة ، وهران ، ورقلة. (1)

الفرع الثاني: تشكيلة المحكمـة

تختلف تشكيلة المحكمة الجزائية بحسب قسم ونوع قسم الجنح خاصة بالجريمة المعلوماتية على مستوى المحكمة يتشكل من فرد ويساعده كاتب ضبط وبحضور وكيل الجمهورية أو مساعديه.

أما الغرفة الجزائية على مستوى المجلس قضائي فالتشكيلة فيها ثلاثية، أي تتشكل

---

(1): القانون رقم 04 ـ14 المرجع السابق ، ص 4.

من رئيس غرفة ومستشارين إثنين بالإضافة إلى كاتب ضبط وبحضور النائب العام أو أحد مساعديه.

أما محكمة الجنايات فتتشكل من رئيس المحكمة ومستشارين ومحلفين وكاتب الضبط والنيابة العامة أو من يمثلها.

تستهل المحكمة جلستها بالإعلان أولا عن إفتتاحها بالقول بإسم الشعب الجزائري الجلسة مفتوحة، ثم المناداة على أطراف الخصومة بداية بالمتهم والضحية والشهود والمسؤول المدني والتأكد من حضورهم أو غيابهم، ثم يتم التحقيق من هوية المتهم وتبليغه بالتهمة المنسوبة إليه والمادة القانونية المتابع بها، وإذا كانت الدعوى غير مهيأة للحكم أمرت المحكمة بتأجيلها إلى أقرب جلسة ، وفي هذه الحالة وطبقا لأحكام المادة 339 مكرر 6 المستحدثة بموجب الأمر 15 ــ 02 المؤرخ في 23 جويلية 2015 من قانون الإجراءات الجزائية تتخذ المجكمة إحدى الإجراءات التالية:

- ترك المتهم حرا.
- إخضاع المتهم لتدابير أو أكثر من تدابير الرقابة القضائية المنصوص عليها في المادة 125 مكرر 1 قانون الإجراءات الجزائية.
- وضع المتهم في الحبس المؤقت.
- مع الإشارة وأن هذه التدابير لا تقبل الإستئناف. (1)

وإذا كان المتهم قد سبق حبسه من طرف قاضي التحقيق عن طريق الحبس المؤقت أو بموجب إجراءات المثول الفردي فإنه يساق بواسطة القوة العمومية لحضور الجلسة ويخطره رئيس الجلسة بأن له الحق في إختيار محام الدفاع عنه فإن طلب ذلك أمهاه

(1): عبد الرحمان خلفي ، المرجع السابق ، ص 321.

القاضي مهلة لاتقل عن ثلاثة أيام لتحضي دفاعه.

ثم يواجه القاضي المتهم بكل الأدلة القائمة ضده ويتم مناقشتها بالتفصيل من طرف القاضي وبعدها يقوم القاضي بسماع الشهود.

وبعد الإنتهاء من تحقيق تعطى الكلمة للطرف المدني فقط دون المطالبة بالعقوبات الجزائية، لتقوم بعد ذلك النيابة العامة بالمرافعة وتقديم إلتماساتها في الشق الجزائي فقط وفي الأخير يقوم دفاع المتهم بتقديم مرافعته وتقديم إلتماساتها ، ويكون بعدها لنيابة العامة والمدعى حق الرد على مرافقة محامي المتهم ، وتعطى الكلمة الأخيرة بعدها للمتهم ومحاميه.

. ثم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكمه في نفس الجلسة أو يحدد تاريخ لاحق منطق بالحكم.

الفـرع الثـالث: القـواعـد العـامة للمحـاكمة

تنفيذ المحاكمة بمجموعة من المبادئ تنطبق على محكمة الجزائية لقسم الجنح على مستوى المحكمة أو الغرفة الجزائية سنحاول شرحها على توضيح الآتي بيانه: (2)

أولا: عـلانـية الجلسة

جل التشريعات تقر بمبدأ علانية الجلسة ، وذلك أن العلانية تسمح للجمهور بمراقبة عمل المحكمة ومنه الإطمئنان والشعور بالعدالة وهذا على التحقيق الأولي الذي تقوم به ضباط الشرطة القضائية وكذا التحقيق الإبتدائي الذي تقوم به الجهات التحقيق ، فكلاهم يتم في سرية ، إلا أن العلانية ليست في جميع الجلسات بل القاضي سلطة تقديرية في إخراج القصر من الجلسة ، كما يمكن أن تكون الجلسة سرية إذا كان في علانيتها خطر على نظام العام والأداب العامة ، إلا أن هذا الحكم يجب أن يصدر في جلسة علنية ، ويحكم هذا المبدأ نص المادة 285 من قانون الإجراءات الجزائية الجزائري.

---

(1): عبد الرحمان خلفي ، المرجع السابق ، ص 322.

ثـانـيا: شفـوية المـرافـعات

فأطراف الخصومة الحق في مناقشة كل دليل يعرض بالجلسة حتى يتمكن الجميع من الدفاع عن نفسه ولايتم الإكتفاء بالتحقيقات الأولية والإبتدائية التي سبقت المحاكمة.

ثـالثـا: حـضور أطـراف الخـصومـة

لايجوز إجراء المحاكمة دون أطراف الخصومة لذلك أوجب المشرع حضور كل من الضحية والمتهم أما بالنسبة لنيابة فهي جزء من التشكيلة. (1)

رابـعـا: تـدويـن التحـقيـق النهائـي

لا يمكن للمحكمة أن تنعقد في حالة غياب أمين الضبط لأن دوره يتجسد في تدوين كل ما يدور بالجلسة. (2)

المطلب الثاني: إجراءات سير المحاكمة في الجريمة المعلوماتية

لا تختلف إجراءات سير المحاكمة في الجرائم المعلوماتية عن الإجراءات المتبعة في غيرها من الجرائم، غير أن ارتباط الجرائم المعلوماتية بتقنيات ومصطلحات فنية وعلمية قد تشكل صعوبة في وجه القضاة أثناء نظرهم في الدعاوى المتعلقة بهذا النوع من الجرائم، وهذا ما أدى بالبعض إلى الدعوة إلى ضرورة أن تسبق مرحلة المحاكمة مرحلة تحضيرية يتم من خلالها توضيح ما قد يكتنف هذه الجرائم من غموض.

تحضير إجراءات المحاكمة في الجرائم المعلوماتية

يرى البعض أن التحضير للمحاكمة في الجرائم المعلوماتية يكتسي أهمية بالغة،

---

(1): عبد الرحمان خلفي ، المرجع السابق ، ص 324.

(2): أسامة عبد الله قايد ، شرح قانون الإجراءات الجنائية ، د ط ، دار النهضة العربية ، القاهرة ، 2007 ، ص 608.

فتقديم المعلومات العلمية ومصطلحات التقنية العالية أمام المحاكم شرحها للقضاة تشكل صعوبة بالغة لدى المحققين وأعضاء النيابة، وترك مهمة الشرح والتقديم لخبراء الحاسوب الآلي كلية، تفقد القضية الجنائية عناصرها القانونية، ولذلك يرون أنه من الضروري أن تتبع في تحضير إجراءات المحاكمة في الجرائم المعلوماتية الخطوات التالي:

- **الخطوة الأولى:** ويقوم بها المحقق وهي إجراءات تلخيص القضية وتعبئة النماذج والاستمارات الخاصة بملف القضية وإعداد ورقة حصر التهم وصياغة سيناريو الجريمة كما كشفتها التحريات والأدلة المتوفرة.

- **الخطوة الثانية:** وهي اللقاء بين المحقق وخبراء الحاسوب الآلي الذين أسهموا مع المحقق في إجراءات الضبط والتفتيش أو فحص البرامج وجمع الأدلة الجنائية، في هذا اللقاء يتم حصر الأدلة المتوفرة وترتيبها وفقا لأهمية كل دليل أو بينة أو قرينة، كما يقوم المحقق في هذه المرحلة بشرح الجوانب القانونية للخبراء والتأكيد على ربط الأدلة والخبرة العلمية بعناصر وأركان الجريمة التي ينوي محاكمة المتهم بموجبها.

- **الخطوة الثالثة:** في هذه الخطوة يلتقي المحقق بممثل الاتهام أو وكيل النيابة الذي يتولى مهمة الادعاء أمام القضاء، وذلك لشرح أبعاد الفصل الإجرامي وتمكين ممثل الادعاء من صياغة التهمة المناسبة والاتفاق حول عناصر وأركان الجريمة وترتيب الأدلة لإثبات كل ركن أو عنصر من الجريمة موضوع الاتهام، ومن الضروري في هذه المرحلة التيقن من مدى إلمام ممثل الاتهام بالتقنيات والبرامج ذات العلاقة بالحاسوب الآلي موضوع القضية.

- **الخطوة الرابعة:** في هذه المرحلة يتم اللقاء بين المحقق وممثل النيابة وخبراء الحاسوب الآلي لترتيب المصطلحات الفنية المستخدمة أثناء إجراءات المحاكمة، مع ضرورة الاتفاق حول تلك المصطلحات وكيفية استخدامها والمرافعات التي قد ترد أثناء

الاستجواب، حتى تطمئن الأطراف على أن هناك لغة موحدة بينهم لا تقبل الشك أو الخطأ، علما أن المتهم في مثل هذه القضايا على دراية بمصطلحات الحاسوب الآلي ومن حقه أن يجادل بما لديه من علم ومعرفة للدفاع عن نفسه، كما انه من الضروري مراعاة أي خلاف ينشب بين ممثل النيابة العامة وخبراء الحاسوب الآلي أمام المحكمة، لأن ذلك قد يطيح بجميع الأدلة الفنية التي تقوم عليها التهمة، إذ أن الشك يفسر لصالح المتهم ومن السهل إثارة الشكوك في مجال تقنيات الحاسوب الآلي المفتوحة على جميع أبواب المعرفة.

- **الخطوة الخامسة:** وهي مرحلة وضع سيناريو المحاكمة ويقصد بالسيناريو ترتيب الأحداث والوقائع والعمليات الفنية التي تشكل الجريمة مع توفر عناصر القصد الجنائي وإظهار مبررات علاقة المتهم الذي سيمثل أمام المحكمة بالفعل الإجرامي موضوع الاتهام، ويشمل والسيناريو أسلوب الإخراج القانوني بالكيفية التي تنساب بها الحقائق المؤكدة إلى عقل القاضي.

ومن جانبنا نرى انه وان كانت مثل هذه الخطوات تكتسي أهمية كبيرة في الجرائم المعلوماتية نظرا لتعقديها والغموض الذي يكتنفها، فإن أهميتها لا تقل عن غيرها من الجرائم، فالتحضير للمحاكمة من شأنه أن يكفل التنسيق الجيد بين جهات التحقيق والحكم من اجل الوقوف على حقيقة أي واقعة وكشف خباياها.

سير إجراءات المحاكمة في الجرائم المعلوماتية

إن سير إجراءات المحاكمة في الجرائم المعلوماتية كغيرها من الجرائم، تختلف تبعا للمحكمة المنظورة أمامها الدعوى المتعلقة بها.فقد تكون الجريمة المعلوماتية جنحة فتنظرالدعوى بشأنها أمام محكمة الجنح والمخالفات وقد تكون الجريمة المعلوماتية جناية فتنظر الدعوى بشأنها أمام محكمة الجنايات، وقد يكون المتهم بالجريمة المعلوماتية حدثا فتنظر الدعوى أمام محكمة الأحداث. وسنقتصر على بيان إجراءات سير المحاكمة في الجريمة المعلوماتية وفقا للتشريع الجزائري الذي قد تنظر الدعاوى المتعلقة بجرائم

معلوماتية في ظله، إما أمام محكمة الجنح والمخالفات إذا كان المتهم بالجريمة شخصا بالغا أو إما أمام محكمة الأحداث إذا كان المتهم بها حدثا.

إجراءات سير المحاكمة في الجرائم المعلوماتية أمام محكمة الجنح

تسري إجراءات المحاكمة في الجرائم المعلوماتية أمام محكمة الجنح و المخالفات وفقا للقواعد العامة المقررة لسير الإجراءات أمامها]105[، و التي يمكن اختصارها فيما يلي:

-الإعلان عن بدء الجلسة

تبدأ المحكمة جلستها بالإعلان عن افتتاحها ثم المناداة على أطراف الدعوى من متهمين وضحايا وكذا شهود ومسؤولين مدنيين إن وجدوا، ليتم التأكد من حضورهم أو غيابهم ويتحقق الرئيس من هوية المتهم ويعرفه بالإجراء الذي تمت من خلاله إحالته على المحكمة حيث تقضي المادة 343 من قانون الإجراءات الجزائية "يتحقق الرئيس من هوية المتهم ويعرف بالإجراء الذي رفعت بموجبه الدعوى للمحكمة، كما يتحقق عند الاقتضاء من حضور أو غياب المسؤول بالحقوق المدنية أو المدعي المدني والشهود..."

- بدء إجراءات التحقيق

تبدأ إجراءات التحقيق باستجواب المتهم ومناقشته تفصيلا في التهمة المنسوبة إليه و مواجهته بالأدلة القائمة ضده ، و ذلك إما لتنفيذها أو الاعتراف بها، و لرئيس المحكمة توجيه ما يراه ضروريا من أسئلة للمتهم، كما يجوز ذلك للنيابة العامة، وكذا للمدعي المدني و للدفاع، وفي هذه الحالة توجه الأسئلة من خلال الرئيس، حيث تنص المادة 224 من قانون الإجراءات الجزائية الجزائري "يقوم الرئيس باستجواب المتهم قبل سماع الشهود ويتلقى أقواله ويجوز للنيابة العامة توجيه أسئلة إلى المتهم كما يجوز ذلك للمدعي المدني وللدفاع عن طريق الرئيس". وبعد استجواب المتهم يتم سماع المدعي المدني و يتلقى الرئيس تصريحاته بشأن ظروف الجريمة المرتكبة و الضرر اللاحق به،

و بعدها تسمع شهادة الشهود حيث يلتزم كل منهم بالإدلاء بما لديه من معلومات حول الواقعة المرتكبة و ذلك بعد تأديتهم اليمين القانونية، يتم الاستماع أولا لشهود الإثبات ثم يتم الاستماع لشهود النفي.

بعد الانتهاء من سماع الشهود، يعرض الخبراء الموجه لهم استدعاء للحضور للجلسة، نتائج ما قاموا به من أعمال فنية ككيفية قيامهم بعملية استخلاص الدليل المعلوماتي ونقله الي دعامة مادية وغير ذلك من الأعمال، وذلك بعد أدائهم اليمين القانونية المقررة. ويجوز للرئيس إما من تلقاء نفسه أو بناء على طلب النيابة العامة أو الخصوم أو محاميهم توجيه أسئلة للخبراء وذلك في حدود مهمتهم المنجزة.

- المرافعات

تبدأ المرافعات بسماع المدعي المدني أو محاميه حيث يقدم هذا الأخير طلباته المتمثلة في التعويض عن الضرر اللاحق به، بعد ذلك تتقدم النيابة العامة بطلباتها سواء الكتابية أو الشفوية والتي ترمي إلى تحقيق العدالة، ثم يقدم محامي المتهم مرافعته دفاعا عن المتهم سواء بالسعي إلى تفنيد التهمة عن موكله ومن ثم طلب البراءة، أو طلب تخفيف الحكم، وللمدعي المدني والنيابة العامة دائما حق الرد، ثم تترك للمتهم ومحاميه الكلمة الأخيرة.

- الإعلان عن تاريخ الحكم

يعلن الرئيس عن انتهاء المرافعات فيقرر إما إصدار الحكم في الحال، أو يحدد تاريخا للنطق بالحكم.

إجراءات سير المحاكمة في الجرائم المعلوماتية أمام محكمة الأحداث

تتم محاكمة المتهم الحدث في جريمة معلوماتية وفقا للإجراءات المقررة لمحاكمة هذه الفئة والتي خصها المشرع بإجراءات يطغى عليها طابع من البساطة والمرونة في التطبيق، مكن تلخيصها فيما يلي:

- سرية الجلسة

تتم محاكمة الحدث في جلسة سرية سواء بمكتب أو في غرفة المشورة، وذلك حفاظا على سمعته حيث تنص المادة 461 من قانون الإجراءات الجزائية الجزائر «تحصل مرافعات في سرية و يسمع أطراف الدعوى و يتعين حضور الحدث بشخصه حضر معه نائبه القانوني و محاميه، و تسمع شهادة الشهود إن لزم الأمر بالأوضاع المعتادة».

- بدء التحقيق

بعد أن يتأكد القاضي من هوية الحدث، يخبره بالتهمة المنسوبة إليه ويستفسره فيها في الظروف التي أدت به إلى ارتكابها، وسماع الحدث لا يكون إلا بحضور نائبه القانوني الذي هو إما احد والديه أو وصيه أو متولي حضانته، كما يقوم القاضي بسماع هذا الأخير ويستفسره عن ظروف الحدث وطبعه ونفسيته وعن كل ما قد يؤدي إلى الوقوف عن الأسباب التي أدت إلى جنوحه، ثم بعد ذلك يقوم القاضي بسماع الطرف المدني وكذا الشهود وذلك بالأوضاع العادية لسماعهم.

- المرافعات

إن تعيين محام للحدث وجوبي سواء تم تعيينه من قبل الحدث أو نائبه القانوني، أو تم تعيينه تلقائيا من قبل المحكمة، فحضور المحامي مع الحدث ضروري، و تسري المرافعات بالأحوال العادية لسيرها حيث يتم سماع المدعي المدني أو محاميه، و من ثم تقدم النيابة العامة طلباتها، فيقدم الدفاع مرافعاته و للمدعي المدني و النيابة حق الرد على دفاع المتهم الحدث، تبقى الكلمة الأخيرة للمتهم الحدث و محاميه، غير انه لا يسمح بحضور المرافعات إلا لشهود القضية و الأقارب القريبين للحدث ووصيه أو نائبه القانوني و أعضاء النقابة الوطنية للمحامين ممثلي الجمعيات أو الرابطات أو المصالح أو الأنظمة

المهتمة بشؤون الأحداث و المندوبين المكلفين بالرقابة على الأحداث المراقبين و رجال القضاء.

- الإعلان عن الحكم

رغم أن المشرع قرر سرية جلسة محاكمة الحدث، إلا أن هذه السرية لم تشتمل صدور الحكم. حيث يصدر الحكم في جلسة علنية وبحضور الحدث.

المبحث الثاني: شروط قبول الأدلة المعلوماتية وحجيتها في الاثبات

المطلب الأول: شروط قبول الأدلة المعلوماتية

يشترط لقبول الأدلة المعلوماتية أن تكون مشروعة، و يقصد بذلك ضرورة اتفاق الإجراء الذي تم الحصول من خلاله على الدليل المعلوماتي مع القواعد القانونية و الأنظمة الثابتة في وجدان المجتمع المتحضر أي أن قاعدة مشروعية الدليل الجنائي لا تقتصر و فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع، بل يجب أيضا مراعاة إعلانات حقوق الإنسان و المواثيق و الاتفاقيات الدولية، قواعد النظام العام و حسن الآداب في المجتمع، بالإضافة إلى المبادئ التي استقرت عليها المحكمة العليا (1)، و قد أشار المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في البرازيل في الفترة من 4 إلى 9 سبتمبر 1994 في قراره الصادر حول القواعد الإجرائية في بيئة جرائم الحاسوب، على أن الانتهاكات غير المشروعة لحقوق الإنسان التي يرتكبها رجال السلطة

(1): أحمد فتحي سرور، شرعية والإجراءات الجنائية، دار النهضة العربية، القاهرة، 1997.

العامة، يمكن أن تبطل الدليل المتحصل عليه، بالإضافة إلى تقرير المسؤولية الجنائية لرجل السلطة العامة الذي انتهك القانون (1)، ولقد صادقت لجنة الوزراء التابعة للمجلس الأوربي في 28/01/1981 على اتفاقية خاصة بحماية الاشخاص في مواجهة مخاطرالمعالجة الآلية للبيانات ذات الطبيعة الشخصية، ومن المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة، ومستمدة بطرق مشروعة.

وعلى ذلك فإن القاضي ليس له أن يستند في حكمه على دليل معلوماتي تم الحصول عليه بطرق غير مشروعة. و من أمثلة الطرق غير المشروعة أو غير النزيهة التي يمكن أن تستخدم في الحصول على الأدلة المعلوماتية، إكراه المتهم (ماديا أو معنويا) من أجل فك شفرة الدخول إلى النظم المعلوماتية أو كلمة السر اللازمة للدخول إلى ملف البيانات المختزنة، أو الاستجوابات المنهكة لقوى المتهم المعلوماتي، كأن يستدعى للتحقيق معه لمدد طويلة بغية معرفة معلومات معينة حول قاعدة بيانات أو نظام إدارة قواعد البيانات أو قنوات إرسال البيانات (2)، كما تعتبر من الطرق غير المشروعة في الحصول على الأدلة المعلوماتية قيام ضباط الشرطة القضائية بعمليات مراقبة الكترونية دون الحصول على إذن مسبق من السلطات المختصة.

إن كل دليل معلوماتي تم الحصول عليه بطرق غير مشروعة يجب على القاضي استبعاده، حتى و لو كان هذا الدليل، دليلا صارخا على إدانة المتهم المعلوماتي، وفي هذا الشأن ذهب المشرع الانجليزي إلى توسيع قاعدة استبعاد الدليل الجنائي الذي تم الحصول عليه بطريقة غير مشروعة. فوفقا له فإن كل دليل قد تم التوصل إليه مباشرة أو بطريقة غير مباشرة و كان متضمنا اعتداء على الحقوق الأساسية للمواطن يتعين استبعاده من جلسة

---

(1): أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2008.

(2): جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002.

المرافعات، حتى و لو كان دليلا ملائما أو موضوعيا يتصل بموضوع النزاع مباشرة يثبته أو يساهم في إثباته. (1)

أن تكون الأدلة المعلوماتية يقينية

يشترط لقبول الأدلة المعلوماتية أن تكون هذه الأدلة مبنية على الجزم واليقين بعيدة عن الظن التخمين، ذلك انه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين، وهذا الجزم واليقين ليس مطلقا بل نسبيا فقط، فالمطلوب أن يبني القاضي عقيدته على أساس احتمالات ذات درجة عالية من الثقة لا يهزها أو يناقضها احتمال أخر. (2)

ويمكن للقاضي أن يصل إلى اليقين والجزم من خلال ما يعرض عليه من أدلة مستخرجة من الحاسوب والانترنت، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها، فيحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه، فكأن القاضي يصل إلى هذا اليقين من خلال نوعين من المعرفة: أولهما المعرفة الحسية التي تدركها الحواس من خلال معاينة هذه الأدلة وتفحصها، وثانيهما المعرفة العقلية التي يقوم بها القاضيعن طريق التحليل والاستنتاج من خلال الربط بين هذه الأدلة والملابسات التي أحاطت بها، فإذا لم ينته القاضي إلى الجزم بنسبة الفعل أو الجريمة المعلوماتية إلى المتهم المعلوماتي تعين عليه أن يقضي بالبراءة، فالشك يجب أن يستفيد منه المتهم المعلوماتي. (3)

---

(1): هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997، ص 128، 129.

(2): نفس المرجع، ص 85.

(3): نفس المرجع، ص 90، 91.

هذا وتشترط بعض التشريعات شروطا معينة ليقينية الأدلة المستمدة من الحواسب والانترنت، كقانون البوليس والإثبات في بريطانيا لسنة 1984، حيث يشترط ليقينية الأدلة المعلوماتية أن تكون البيانات دقيقة وناتجة عن الحاسوب بصورة سليمة، أما في كندا فإن الرأي السائد في الفقه هو اعتبار مخرجات الحاسوب من أفضل الأدلة، وهو ذات ما ذهبت إليه بعض قوانين الولايات في أمريكا، حيث قضت أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تعد أفضل الأدلة المتاحة لإثبات هذه البيانات، وبالتالي يتحقق مبدأ يقينية الأدلة المعلوماتية، بيد أن هذا لم يمنع القضاء الأمريكي من استبعاد هذه المخرجات إذا كانت ناتجة عن حاسوب لا يؤدي وظائفه بصورة سليمة أو كان القائم عليه لا تتوافر فيه الثقة والطمأنينة.

ويقرر الفقه الياباني قبول الأدلة المستخرجة من الحاسوب والتي تم تحويلها إلى صورة مرئية سواء كانت هي الأصل أم كانت نسخا مستخرجة عن هذا الأصل، ففي هذه الحالة يتحقق اليقين الذي ينبني عليه الحكم الجنائي، كما يمكن أن يتحقق اليقين لهذه المخرجات أيضا من خلال التقاريرالتي يقدمها الخبراء.

أما على مستوى تشريعاتنا العربية فنجد المشرع الأردني يعتبر من خلال المادة 21 من قانون المعاملات الالكترونية المؤقت رقم 85 لسنة 2001 نظام المعالجة الالكتروني مؤهلا لإثبات تحويل الحق في السند بشرط أن تكون النسخة المعتمدة من السند محددة بصورة غير قابلة للتغيير وأن تدل النسخة المعتمدة من السند على اسم الشخص الذي تم سحب السند لمصلحته.

أن يتم مناقشة الأدلة المعلوماتية في الجلسة

إن اقتناع القاضي لا يجوز أن يبنى إلا على الأدلة التي عرضت في الجلسة وتمت مناقشتها، فمناقشة هذه الأخيرة في الجلسة توضح حقيقتها وتجلى غموضها

وتكشف للمحكمة العناصر التي تكون منها قناعتها، كما أن استناد القا ضي على دليل لم يطرح بالجلسة وليس له أصل ثابت بأوراق الدعوى يعني أن عمله يعتبر ابتداعا وانتزاعا للخيال (1). وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات، يجب أن يعرض في الجلسة، ليس من خلال ملف الدعوى في التحقيق الابتدائي، لكن بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحواسب الآلية وأيضا بالنسبة لشهود الجرائم المعلوماتية الذين قد سبق وأن سمعت أقوالهم في التحقيق الابتدائي، فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة، كذلك فإن خبراء الأنظمة المعلوماتية على اختلاف تخصصاتهم ينبغي أن يمثلوا أمام المحاكم لمناقشتهم أو مناقشة تقاريرهم التي خلصوا إليها إظهارا للحقيقة وكشفا للحق. (2)

وقد اشترطت جل التشريعات وجوب مناقشة الأدلة في الجلسة، ومن بينها المشرع الجزائري وذلك من خلال الفقرة الثانية من المادة 212 من قانون الإجراءات الجزائية السالفة الذكر، كما نص عليه المشرع المصري من خلال المادة 302 من قانون الإجراءات الجزائية ومع ذلك لا يجوز له أن يبني حكمه على دليل لم يطرح أمامه بالجلسة..."

وتجدر الإشارة إلى أن مناقشة الأدلة المعلوماتية تحتاج إلى خبرة فنية ومعرفة بتقنيات الحاسوب الآلي، وهنا تظهر أهمية تدريب القضاة الذي نوهنا عنه فيما سبق، فمن شأن هذا التدريب أن يساعد القضاة على المناقشة الجيدة والبناءة للأدلة المعلوماتية على اختلاف أنواعها مفرداتها.

---

(1): رمزي رياض، سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2004.

(2): هلالي عبد الإله أحمد، المرجع السابق، ص 104.

المطلب الثاني: حجية الأدلة المعلوماتية في الاثبات

حجية الأدلة المعلوماتية في الإثبات

إن حجية الأدلة المعلوماتية هي قيمة ما تتمتع به بأنواعها المختلفة الورقية أو الالكترونية والمصغرات الفيلمية من قوة استدلالية على صدق نسبة الفعل الإجرامي لشخص معين أو كذبه (1). وتختلف حجية الأدلة المعلوماتية من دولة إلى أخرى تبعا لنظام الإثبات المعتمد في كل منها. وتكشف الدراسات على وجود ثلاث أنظمة رئيسية للإثبات نظام الأدلة القانونية، نظام حرية الإثبات أو الاقتناع الذاتي للقاضي، ونظام الإثبات المختلط.

حجية الأدلة المعلوماتية في ظل نظام الأدلة القانونية

تكون الأدلة في نظام الأدلة القانونية محصورة ومحددة مسبقا من المشرع ولا يجوز للقاضي أن يخرج عليها أو يبني حكمه على خلافها، وبالتالي تكون قوتها الإثباتية محددة، فإذا ما توفرت شروط الدليل بالشكل الذي حدده المشرع وجب على القاضي أن يبني اقتناعه ويؤسس حكمه على أساس هذا الدليل، حتى إن لم يكن مقتنعا به شخصيا، وعند عدم توافر الشروط المطلوبة قانونا يكون كذلك القاضي ملزما ببناء اقتناعه وتأسيس حكمه على أساس عدم قيام الدليل على الادعاء وإن كان القاضي مقتنعا تماما بثبوت الادعاء، و في ذلك بلا شك تقييد لسلطته التقديرية.

إن نظام الأدلة القانونية من شأنه في الكثير من الأحيان التقليل من أهمية الدليل المستمد من الحاسوب، خاصة وأن هذا النظام يعمل بقاعدة "الدليل الأفضل" أو "قاعدة المحر الأصلي"، والتي مؤداها انه لا يجوز قبول صورة للمستند أو المحرر إذا كان من الممكن
الحصول على الأصل، وهو ما يقتضي إلغاء الدليل الثانوي لمحتوى المستند وتأسيسا على

---

(1): هلالي عبد الإله أحمد، المرجع السابق، ص 22.

ذلك شترط في الدليل الذي يقدم إلى ساحة القضاء أن يكون دليلا أصليا، فالأصل يفضل على الصورة أو النسخة المطابقة. (1)

على ذلك فإن قبول الأدلة المعلوماتية كأدلة صالحة للإثبات أمام القضاء، قد يثير الكثير من الشكوك عندما تكون في صورة مخرجات للحاسوب، ذلك باعتبار أن الإشارات الالكترونية و النبضات الممغنطة التي تعتمد عليها الحواسب الآلية في تشغيلها ليست مرئية للعين البشرية، الأمر الذي لا يتأتى معه للقاضي مناظرتها أو وضع يده على الدليل الأصلى، وما يقدم إليه من وثائق أخرجها الحاسوب –رغم أهميتها لنجاح الملاحقة الجنائية– يمكن الاعتراض على قبولها بدعوى أنها نسخ لأصول، مما يجعلها دليلا ثانويا ليس أصليا.

ومن الدول التي تتبنى هذا النظام المملكة المتحدة، والتي أصدرت قانونا للشرطة الإثبات الجنائي سنة 1984 حوى تنظيما محددا لمسألة قبول مخرجات الحاسوب كأدلة إثبات في المواد الجنائية، حيث قضى بأن المستند الناتج عن الحاسوب الآلي لا يقبل كدليل، إذا لم يستكمل باختبارات الثقة المنصوص عليها في القسم 69 من هذا القانون، والتي يمكن بلورتها في ضرورة عدم وجود سبب معقول يدعو إلى الاعتقاد بأن مخرج الحاسوب غير دقيق أو أن بياناته غير سليمة. كما أوجبت أن يكون الحاسوب الناتج عنه هذا المخرج يعمل بكفاءة وبصورة سليمة (2). بمعنى أن قبول المستند الناتج عن الحاسوب في ظل هذا القانون يتوقف على مدى تطابقه مع المعلومات التي يتضمنها الحاسوب الآلي.

حجية الأدلة المعلوماتية في ظل نظام الإثبات الحر

نظام الإثبات الحر أو ما يسمى بنظام الاقتناع الذاتي للقاضي يقوم على أساس حرية الإثبات حيث يكون للقاضي سلطة تقديرية واسعة في تقدير الأدلة و قبولها، و لا

---

(1): هلالي عبد الإله أحمد، المرجع السابق، ص 94.

(2) : نفس المرجع، ص 53.

سلطان عليه في ذلك إلا ضميره، و بذلك فله أن يبني قناعته على أي دليل طرح أمامه بالجلسة بشرط أن يكون هذا الدليل مشروعا. غير أن الملاحظ أن التعامل بالأنظمة المعلوماتية أصبح يفرض منطقا يتماشى وحرية القاضي أمام الدليل في الدعاوى العامة، فللأنظمة المعلوماتية دقة رقمية مخارج، لا يمكن دحضها إلا بالمعطيات التي تناقضها.

ويمكن القول أنه وفي ظل هذا النظام فإن حجية الأدلة المعلوماتية لا تثير أية صعوبات، فالدول التي تتبنى هذا النظام لا تتردد عموما في طرح الأدلة المعلوماتية أمام المحاكم وتجد صعوبة في قبولها. ومن بين هذه الدول الجزائر حيث تنص الفقرة الأولى من المادة 212 من قانون الإجراءات الجزائية "يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لإقناعه الشخصي"، فالقانون الجزائري يعتمد مبدأ الإثبات الحر كأصل ونظام الأدلة القانونية كاستثناء، فلا يوجد ما يحول دون قبول الأدلة المعلوماتية في ظله طالما أنها لا ترد ضمن الاستثناءات المقررة.

وفي فرنسا كذلك فإن حجية الأدلة المتحصلة من الحاسوب، على المستوى الجنائي لا تبدو مسألة ملحة أو عاجلة في نظر الفقهاء هناك، فالأساس هو حرية الأدلة وحرية القاضي في تقدير هذه الأدلة، و يدرس الفقه الفرنسي هذه الحجية تحت طائلة نطاق قبول الأدلة الناشئة عن الآلة آو الأدلة العلمية مثل أجهزة التصوير وأشرطة التسجيل وأجهزة التصنت. (1)

حجية الأدلة المعلوماتية في ظل النظام المختلط

يقوم النظام المختلط على تحديد المشرع سلفا لأدلة الإثبات التي يجوز للقاضي الاستناد إليها عند إصداره لحكمه في الدعوى التي ينظرها، مع منحه الحق في تقييم كل

---

(1): هلالي عبد الإله أحمد، المرجع السابق، ص 196.

دليل على حد تقرير كفايته للحكم بالإدانة، حيث أن المشرع لا يقوم بتحديد قيمة كل دليل في الإثبات أو إنما يترك هذا الأمر للقاضي يقدره بكامل سلطته التقديرية. ومن التطبيقات التشريعية الآخذة بهذا النظام نجد المشرع الياباني الذي حصر طرق الإثبات المقبولة في أقوال المتهم، أقوال الشهود القرائن والخبرة. أما بالنسبة لأدلة الحاسوب والانترنت، فيقرر الفقه الياباني أن السجلات الالكترونية غير مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة، إلا إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق محتويات الطباعة لمثل هذه السجلات، وفي مثل هذه الحالة يتم قبول هذه الأدلة الناتجة عن الحاسوب والانترنت سواء كانت هي الأصل أم كانت نسخة من هذا الأصل. (1)

هذا ويلجأ البعض في الفقه الياباني وسايره البعض في الفقه المصري إلى حيلة يتم من خلالها التوصل إلى إمكانية قبول الأدلة المستمدة من الحاسوب الآلي في إثبات وقائع الدعاوى التي تتناول الجرائم المعلوماتية، والمتمثلة في التفرقة بين وسائل الإثبات وطرق الإثبات المترتبة، فمن حيث وسائل الإثبات يرون أنها محددة على سبيل الحصر، أما طرق الإثبات فهي متنوعة وتتزايد يوما بعد يوم مع التقدم العلمي والتكنولوجي.

وعلى الرغم ما قد تثيره حجية الأدلة المعلوماتية في بعض الأنظمة القانونية من صعوبات، إلا أن هناك من ذهب إلى القول أن هذه الأدلة (خاصة الرقمية منها)، لا تثير أية صعوبات أمام المحاكم، وأرجع ذلك للأسباب التالية:

- الثقة التي اكتسبها الحاسوب والكفاءة التي حققتها النظم الحديثة للمعلوماتية ف مختلف المجالات.
- ارتباط الأدلة الجنائية المعلوماتية (الرقمية) وآثارها، بالجريمة موضوع المحاكمة.

---

(1): هلالي عبد الإله أحمد، المرجع السابق، ص 62.

– وضوح الأدلة المعلوماتية ودقتها في إثبات العلاقة بين الجاني والمجني عليه أو بين الجاني والسلوك الإجرامي.

– إمكانية تعقب آثار الأدلة المعلوماتية والوصول إلى مصادرها بدقة.

– قيام الأدلة المعلوماتية على نظريات حسابية مؤكدة لا يتطرق إليها الشك، مما يقوي من يقينية الأدلة المعلوماتية.

– الأدلة المعلوماتية يدعمها – عادة – رأي خبير، وللخبرة في المواد الجنائية دورها في الكشف عن الأدلة وفحصها وتقييمها وعرضها أمام المحاكم وفق شروط وقواعد نظمها القانون واقرها القضاء.

من جانبنا نرى أن هذا الرأي صائب نوعا ما، فطبيعة الأدلة المعلوماتية وكونها تطبيق من تطبيقات الأدلة العلمية يجعلها تكتسي نوعا من الموضوعية والمصداقية، ولكن على الرغم من ذلك فإن الأمر لا خلو من الصعوبات، وذلك راجع لحداثة هذا النوع من الأدلة التي أصبح القضاة ولعدم معرفتهم الجيدة بها يخشون التعامل معها، مما يجعل أمر قبولها يعتمد على مدى تفهم القاضي لها مدى قدرته على الربط بينها وبين موضوع الجريمة المعلوماتية المرتكبة.

خاتمة:

باتت الثورة المعلوماتية السمة التي تميز العصر، فالعالم اليوم يمر بلحظة انبهار محاولا استيعاب فوائد هذه الثورة الهائلة، التي أثرت في الفكر الإنساني. فقد أصبح استخدام الأنظمة المعلوماتية المقياس الذي يحدد مدى تطور الشعوب و تقدمها، حيث أحدثت هذه الثورة نقلة فريدة من نوعها، انتقلت بالشعوب من طور الركود و البطء في ممارسة الأنشطة المختلفة إلى طور المرونة والسرعة والديناميكية والحركة، نحو أداء الخدمات المرفقية و الوظيفية المؤسساتية و تبادل المعلومات بشكل سهل و بسيط، وكذا الربط بين الأفراد و الجماعات والشركات داخل المجتمع الدولي و كأنهم ينتمون إلى بلد واحد، فضلا عن تقريب المسافات ولغة الحوار و ممارسة المعاملات بكافة أنواعها عن طريق الشبكات المعلوماتية الدولية الداخلية.

هذه الثورة المعلوماتية و رغم فوائدها التي لا تعد لاو تحصى، ألقت بمسؤولية كبيرة على عاتق أجهزة العدالة الجنائية التي باتت عاجزة عن استيعاب ما أفرزته هذه الثورة من جرائم لم تألف التعامل معها من قبل نظرا للطبيعة الخاصة التي تميزها و ارتباطها بشكل أساسي بالتقنيات المعلوماتية، التي ما فتئت أن ظهرت حتى أصبحت بعض الجهات و الأفراد تتسابق في التفنن في استخدامها من أجل تحقيق أهداف إجرامية، حيث أصبحت هذه التقنيات وسيلة جديدة في أيدي مجرمي المعلوماتية، المعروفين بمهارتهم و ذكائهم و إلمامهم بتقنيات الحاسوب الآلي و برمجياته و لغاته من أجل ارتكاب أخطر جرائمهم.

أمام هذا كله أصبحنا أمام معادلة غير متكافئة، طرفاها، أجهزة عدالة جنائية غير مؤهلة كما يجب للقيام بدورها في ظل التطورات المتلاحقة والمتسارعة للتقنيات المعلوماتية وفي ظل غياب المعرفة التقنية لديها، ومجرمون معلوماتيون لهم من الخبرة والمهارة و المعرفة الفنية ما يؤهلهم لارتكاب جرائمهم دون إمكانية الاستدلال عليهم وبالتالي نشهد حاليا قفزة غير معقولة في ارتكاب الجرائم المعلوماتية، يقابلها ركود غير معهود في أجهزة العدالة الجنائية التي لا زالت في ثبات و غفلة.

و عليه و بناء على ما سبق، تطلب الأمر أن نتقدم بنتائج ما وصلنا إليه من خلال هذا الجهد المتواضع الذي قمنا به في سبيل التصدي لموضوع شديد الحساسية و في حاجة دائمة للدراسة و التحليل بفعل ارتباطه بالتطور المستمر لتكنولوجيا المعلومات، و يمكن بلورة هذه النتائج فيما يلي:

– بالنظر لحداثة هذا السلوك الإجرامي والذي يتجسد في الجريمة المعلوماتية، فإنه لا يوجد لحد الآن إجماع فقهي موحد على تعريف لها مما أدى بالقول أن جريمة المعلوماتية تقاوم التعريف.

– أن الجرائم المعلوماتية أصبحت تشكل نمطا خطيرا من الجرائم، التي يقوم النشاط الإجرامي فيها على استخدام تقنية الحاسوب الآلي بشكل مباشر أو غير مباشر كوسيلة أو هدف لتنفيذ الفعل المنشود.

– أن ارتباط الجرائم المعلوماتية بالتقنية المعلوماتية، جعل منها جرائم ذات طبيعة خاصة، تتميز عن غيرها من الجرائم التقليدية، سواء من حيث ماهيتها، ومن حيث مرتكبيها وحتى من حيث ضحاياها.

– أن عوائق إثبات الجرائم المعلوماتية متعددة ومتنوعة، منها ما تعلق بالجريمة ذاتها، منها ما تعلق بأدلتها، ومنها ما تعلق بالعامل البشري فيها.

– أن ما تثيره الطبيعة الخاصة بالجرائم المعلوماتية من عوائق في حقل إثباتها أصبح يستدعي التعامل معها وفق ما يتناسب وطبيعتها.

– أن ما تتوفر عليه أجهزة العدالة الجنائية من مهارات قانونية، لم يعد يكفي لوحده لإثبات الجرائم المعلوماتية، و إنما أصبح الأمر يتطلب توفر مجموعة من المهارات الفنية من حيث التعرف على الحواسب الآلية و ملحقاتها، و معرفة أساسيات عمل الشبكات مصطلحاتها، وغير ذلك من المعارف الفنية التي ترتبط ارتباطا وثيقا بالجرائم المعلوماتية.

– أن إثبات الجرائم المعلوماتية، أصبح يستدعي و بشدة إعداد البرامج التدريبية المتخصصة الكفيلة بتلقين الجهات القائمة على إثبات الجرائم المعلوماتية، فنيات البحث والتحر التحقيق و الحكم في هذا النوع المستحدث من الجرائم.

– أن أجهزة العدالة الجنائية لم تعد قادرة لوحدها، على إثبات هذا النوع من الجرائم، إنما أصبح من الضروري أن تساند هذه الأخيرة جهات خاصة تكون عونا لها كأجهزة شرطة

متخصصة للبحث والتحري في الجرائم المعلوماتية، و كذا فريق للتحقيق في هذا النوع من الجرائم.

– أن وسائل التحقيق التقليدية لم تعد كافية لوحدها لإثبات هذا النوع من الجرائم، و إنما أصبح و لابد من تزويد أجهزة العدالة الجنائية بمجموعة من الأجهزة و البرمجيات الفنية التي تساعد في تحديد نوع الجريمة و توقيت ارتكابها و مصدرها و شخصية مرتكبيها، و كذا استرجاع الأدلة المتعلقة بها.

– أن الإجراءات التقليدية أصبحت قاصرة عن إثبات الجرائم المعلوماتية المتميزة بسهولة ارتكابها وسرعة محوها، فأصبح الأمر يتطلب اتخاذ إجراءات تتلاءم و طبيعة هذه الجرائم، خاصة فيما يتعلق بإجراءات الضبط و التفتيش و المعاينة.

– أن الأدلة المعلوماتية ما هي إلا تطبيق من تطبيقات الدليل العلمي بما تتميز به من موضوعية وحياد وكفاءة، ولهذا يجب أن تثير أية صعوبة عند تقديمها كأدلة إثبات في الجرائم المعلوماتية.

– أن الوصول إلى الحكم السديد في الجرائم المعلوماتية، أصبح يتوقف على مدى قدرة القاضي على مناقشة الدليل المعلوماتي، المناقشة العلمية الصحيحة التي تقوم على مدى تفهم القاضي لفحوى التقدم العلمي في مجال التقنية المعلوماتية و مدى قدرته على الربط بين الدليل المعلوماتي و الجريمة المرتكبة.

وعلى ذلك يمكن القول أن مجمل ما تم التوصل إليه من خلال هذه الدراسة، أن نظم قواعد الإثبات التقليدية قاصرة على إثبات ما يقع من جرائم معلوماتية، فضلا على أن الفكر الأمني والقضائي غير ملائم لعملية إثبات الجرائم المعلوماتية، بل أصبح الأمر يحتاج إلى رجل أمن معلوماتي، ومحقق معلوماتي، وقاض معلوماتي. لهذا ارتأينا أن نختم هذه الدراسة بمجموعة من التوصيات، لعلها تساهم ولو بقدر ضئيل في حل بعض المشكلات التي لمحناها في ثنايا هذه الدراسة، وتتمثل هذه التوصيات فيما يلي:

– توعية مستخدمي الانترنت والحاسوب الآلي و موظفي المصارف و المراكز العلمية، حول خطورة الجرائم المعلوماتية و ضرورة الحماية منها من جهة، و أهمية الإبلاغ عنها و الإرشاد إلى مرتكبيها من جهة أخر.

– الحرص على تحقيق التعاون الدولي لمواجهة الاجرام المعلوماتي وذلك عن طريق الدخول في اتفاقيات ومعاهدات لمكافحة هذه الجرائم، وذلك لتضييق الخناق على العابثين بالتعامل من خلال الشبكة المعلوماتية.

– الحرص على تدريب رجال البحث والتحري والخبراء والقضاة على التعامل مع الجرائم المعلوماتية من الناحيتين الفنية والعلمية.

– العمل على تكريس قواعد قانونية جديدة تتناسب مع طبيعة الجرائم المعلوماتية، وانشاء وحدات مختصة للبحث والتحري والتحقيق في الجريمة المعلوماتية.

قائمة المراجع

1. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الأزاريطة، 2004.

2. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2005.

3. أيمن عبد الله فكري، جرائم نظم المعلومات، دار الجامعة الجديدة للمنشورات، الإسكندرية، 2007.

Legal Aspects Of Computer-related Crime in the Information (1998), 4. SIEBER ULRICH Society. http://europa.eu.int/ISPO/legal/en/comcrime/sieber

5. رستم هشام، قانون العقوبات ومخاطر التقنية، مكتبة الآلات الحديثة، أسيوط، 1992.

6. د/ الشوا محمد، الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحوث المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، جمهورية مصر العربية، 1993.

7. د/هدي قشقوش، جرائم الحاسوب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، 1999.

8. TOM FORESTER, Essential Proplems to Hig-Tech Society First Mit Pres Edition, Cambridge, Massachusetts, 1989.

9. TIEDEMANN, Fraude Et Autres Delits D'affaires Commis A L'aide D'ordinateurs Electroniques. R.D.P.C 1984. N°7.

10. Technology AND HARDCASTLE: Computer Related Crime in Information TOTY .K.1986. andthelawu.

11. Ouvrage Precedent TOTY AND HARDCASTLE.

12. أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006.

13. هدى حامد قشقو جرائم الكمبيوتر و الجرائم الأخرى في مجال تكنولوجيا المعلومات بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، من 25 الى 28 أكتوبر، 1993.

14. اليوسف عبد العزيز، التقنية في الجرائم المستحدثة، بحث منشور ضمن كتاب الظواهرالاجرامية المستحدثة وسبل مواجهتها، منشورات أكاديمية نايف للعلوم الامنية، الرياض، 1999.

15. محمد أبو بكر سلامة، جرائم الكمبيوتر والانترنت، منشأة المعارف، الإسكندرية، 2006.

16. عبد الفتاح بيومي حجازي الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2005.

17. نهلا عبد القادر المومني، الجرائم المعلوماتية ، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان ،2008.

18. فوزية عبد الستار، شرح قانون العقوبات، الطبعة الخامسة، دار النهضة العربية، القاهرة، 1991.

19. Philippe Rosè, La criminalité informatique, deuxième édition, Edition Dahleb, 199519.

20. محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدثة،المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، من 25 الى 28 أكتوبر 1993.

21. أيمن عبد الحفيظ ،الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية، (دون دا نشر)، 2005.

22. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، كلية الحقوق جامعة الإسكندرية، 2006.

23. زبيخة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، عين مليلة ، الجزائر ، د ط ، 2011.

24. مولود ديدان، قانون الإجراءات الجزائية، دار بلقيس الجزائر، د ط، ديسمبر 2014.

24. المواد 34 و 60 و 70 ، قانون الإجراءات الجنائية المصري مع اخر تعديلاته لقانون رقم 153 لسنة 2007 والمؤرخ في 2007/6/16 ، المنشورات الجريدة الرسمية ، العدد 24 مكرر.
25. عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، دار بلقيس لنشر، د ط ، 2015.
26. المادة 91 و94 و95 قانون الإجراءات الجزائية المصري رقم 153 المرجع السابق.
27. أسامة عبد الله قايد ، شرح قانون الإجراءات الجنائية ، د ط ، دار النهضة العربية ، القاهرة ، 2007.
28. أحمد فتحي سرور، شرعية والإجراءات الجنائية، دار النهضة العربية، القاهرة، 1997.
29. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2008.
30. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002.
31. هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997.
32. رمزي رياض، سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2004.