جامعة جيلالي ليابس – سيدي بلعباس –

كلية الحقوق والعلوم السياسية

أطروحة دكتوراه في العلوم – تخصص علوم قانونية فرع علوم جنائية –

مشروعية الدليل الإلكتروني في مجال الإثبات الجنائي

تحت إشراف:

الأستاذ الدكتور: بوسندة عباس

من إعداد الطالبة:

بوعناد فاطمة زهرة

أعضاء لجنة المناقشة

أ.د. معوان مصطفى	أستاذ التعليم العالي	جامعة سيدي بلعباس	رئيسا
أ.د. بوسندة عباس	أستاذ التعليم العالي	جامعة سيدي بلعباس	مشرفا ومقررا
أ.د. مروان محمد	أستاذ التعليم العالي	جامعة وهران	عضوا
أ.د. نقادي عبد الحفيظ	أستاذ التعليم العالي	جامعة سعيدة	عضوا

السنة الجامعية : 2013–2014

إهداء

إلى من زرعا فيّ حب العلم والسعي نحو إثبات الذات ...

إلى والديّ، أطال الله عمرهما وسدد خطاهما.

إلى زوجي الذي كان لي في الدرب معينا وفي الصبر مثيلا.

إلى قرة عيني، إبنتي الحبيبة "أريج".

إلى أختي "حدهوم" التي كانت تشد من عزيمتي.

إلى كل هؤلاء أهدي هذا الجهد العلمي، داعية الله عز وجل أن يجعل ثوابها لهم حفظا وسعادة وإحسانا في دينهم ودنياهم.

شكر و تقديــر

الحمد لله الذي خلق من العدم وأعز القلم، فأبشر به التنزيل الكريم، وجعله قسما للعلي العظيم، والصلاة والسلام على خير المرسلين ذي الخلق العظيم محمد رسول النهج القويم وداعية الصراط المستقيم، سبحانك لا علم لنا إلا ما علمتنا إنك أنت العليم الحكيم.

وبعد، أتقدم بأسمى كلمات الشكر والتقدير والإعتراف بالفضل والإحترام لأستاذي الجليل الأستاذ الدكتور " عباس بوسندة" لتفضل سيادته عليّ بقبول الإشراف على هذه الرسالة، فشملني بعلمه الغزير وخلقه الرفيع وفضله الوفير، فكان طوال سنوات البحث يعطيني من وقته النفيس الكثير، ويوليني فائق عنايته وتشجيعه وسعة صدره في معالجة موضوع الرسالة، وكان لتوجيهاته السديدة الأثر البالغ في إثراء هذه الرسالة، كونه أمدني بالكثير من الملاحظات القيمة مما كان له أكبر الأثر في إنجازها على الصورة التي وصلت إليها، فهو الأب الروحي وخير معلم و نعم الأستاذ، فشكرا لسيادته على أعظم ما يمنحه الأستاذ لطلبته، وأن يهبنا الله الكثير من أمثاله ويمتعه بموفور الصحة والعافية، فله مني جزيل الشكر ووافر التقدير والإحترام .

كما لا يفوتني أن أتقدم بأسمى آيات الشكر والتقدير والإمتنان والإحترام للأساتذة الأفاضل أعضاء لجنة المناقشة، وفي مقدمتهم الأستاذ الدكتور" مصطفى معوان " كرئيس لها، فمني لأستاذي الكريم كل الشكر والتقدير على تفضله قبول رئاسة لجنة المناقشة، و هذا ما يزيدها قيمة علمية وجزاه الله خير الجزاء.

كما يشرفني أن يكون من بين أعضاء لجنة المناقشة الأستاذ الدكتور "محمد مروان" والأستاذ الدكتور "عبد الحفيظ نقادي"، فشكرا على قبولهما الإشتراك في لجنة المناقشة بالرغم من كثرة التزاماتهما العلمية والمهنية.

كما أريد أن أشكر أعضاء لجنة المناقشة كباحثين حيث استفدت من إصداراتهم القيمة، أين تناولوا موضوع الإثبات من جميع زواياه العلمية والقانونية والقضائية، شرحا وتعليلا ونقدا.

فلجميع هؤلاء كل الشكر والتقدير والعرفان وأن يمتعهم الله بالصحة والعافية.

قائمة المختصرات.

أولا: باللغة العربية.

- أ: أستاذ.
- ت: تاريخ.
- ج : جزء.
- ج ر ج ج : الجريدة الرسمية للجمهورية الجزائرية.
- د : دكتور.
- د.ج : دينار جزائري.
- ص : صفحة.
- ط : طبعة.
- ف : فقرة.
- ق : قانون.
- ق أ : القانون الأردني.
- ق إ ج : قانون الإجراءات الجزائية.
- ق ع ج : قانون العقوبات الجزائري.
- ق ع ف : قانون العقوبات الفرنسي.
- ق م : القانون المدني.
- م : مادة .
- مج : مجموعة.
- ن : نقض.
- هـ : هجري.

ثانيا: باللغة الفرنسية.

- Art : Article.
- B : Bulletin.
- C.C .F: Code civil français.
- C.C.C : Conseil de l'Europe - Convention sur la cybercriminalité.
- C.P.C.E : Code des postes et des communications électroniques.
- C.P.F : Code pénal français.
- C.P.P.F : Code de procédure pénale français.
- Cass .Crim : Cour de cassation, chambre criminelle.
- Ch : Chambre .
- D : Recueil Dalloz .
- Doct : Doctrine.
- éd : édition.
- Gaz . pal : Gazette du palais.
- Ibid : Ibidem (au même endroit).
- IEHEI : Institut européen des hautes études internationales.
- J.C.P : Juris-classeur périodique (semaine juridique).
- N : Numéro.
- Obs : Observation.
- Op.Cit : Opere Citato (ouvrage cité).
- P : Page.
- PUF : Presses Universitaires de France.
- R.I.C.P.T : Revue internationale de criminologie et de police technique.
- R.I.P.C : Revue internationale de police criminelle.
- R.S.C.P : Revue de science criminelle et de droit pénal .
- T : Tome.
- TGI : Tribunal de grande instance.

ثالثا: باللغة الإنجليزية.

- E-Mail : Electronic Mail.
- I O C E : International Organisation Of Computer Evidence.
- IP : Internet Protocol.
- MMS : Multimedia Messaging Service.
- PC : Personal Computer.
- S W G D E : Scientfic Working Group On Digital Evidence.
- SMS : Short Message Service.
- TCP : Transmission Control Protocol .
- www : World Wide Web .

مقدمة:

يشهد العالم اليوم تزايدا ملحوظا في استخدام وسائل الإتصالات الحديثة لنقل وتبادل المعلومات وذلك بعد ما انتشرت أجهزة الإتصال السلكية واللاسلكية وتطورت من الناحية التقنية، إضافة إلى ما رسخ في أذهان أفراد المجتمع من قناعة تامة بأن المحصلة النهائية عن ممارسة مختلف أوجه الأنشطة الإجتماعية والإقتصادية والسياسية تعتمد بشكل كبير على مدى توافر المعلومات بشأنها.

وقد ترتب عن الصلة الوثيقة التي تربط بين وسائل الإتصال والمعلومات، ظهور ما يسمى بعلم تكنولوجيا المعلومات، ذلك العلم الذي يسعى إلى توظيف أجهزة الإتصال في تخزين واسترجاع أو في نقل وتبادل البيانات والمعلومات بين الأفراد دعما للنشاط الفكري الإنساني[1].

كما أبرزت ثورة المعلومات نظاما جديدا أطلق عليه النظام المعلوماتي الذي أوجد بدوره المجتمع المعلوماتي الذي يعتمد على تقنية الإتصال بأنواعها كافة و المعالجة الآلية للمعلومات خاصة، وأصبح المتلقي يتعامل مع كم هائل من البيانات والمعلومات التي تجاوزت حدود المكان واختزلت عنصر الزمان[2].

ويأتي مجتمع المعلومات بعد مراحل متعددة مرّ بها تاريخ البشرية، وتميزت كل مرحلة بخصائص ومميزات، حيث شهدت الإنسانية من قبل تكنولوجيا الصيد ثم تكنولوجيا الزراعة وبعدها تكنولوجيا المعلومات التي رسمت الملامح الأولى لمجتمع المعلومات، هذا الأخير تميز بالتركيز على العمليات التي تعالج فيها المعلومات، والمادة الخام الأساسية به هي المعلومة التي يتم استثمارها بحيث تولد المعرفة معرفة جديدة.

ويقصد أيضا بمجتمع المعلومات جميع الأنشطة والتدابير والممارسات المرتبطة بالمعلومات والإتصالات وخدماتها إنتاجا ونشرا وتنظيما واستغلالا واستثمارا، ويشمل إنتاج المعلومات أنشطة البحث والجهود الإبداعية والتأليف الفكري الموجه لخدمة الأهداف التعليمية والتثقيفية، ورغم تعدد المفاهيم حول مجتمع المعلومات، إلاّ أنه يمكن القول أنّ مجتمع المعلومات يتركز أساسا على إنتاج المعلومة والحصول عليها واستغلالها واستثمارها في خدمة أهداف التنمية الإقتصادية والتطور التكنولوجي في المجتمع المعلوماتي من خلال وضع آليات وإدارة استغلالها بواسطة بنية تحتية للمعلومات وشبكات الإتصال[3].

---

[1]- أنظر في ذلك: د. محمد سامي عبد الصادق، خدمة المعلومات الصوتية و الإلتزامات الناشئة عنها، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2005، ص05.

[2]- د. ناصر بن محمد البقمي ، أهمية الأدلة الرقمية في الإثبات الجنائي، مجلة الفكر الشرطي، المجلد الحادي و العشرون، الإمارات العربية المتحدة، العدد رقم 80، يناير 2012، ص 16.

[3]- لمزيد من التفاصيل حول تعريف مجتمع المعلومات أنظر في ذلك: د. معوان مصطفى، التجارة الإلكترونية ومكافحة الجريمة المعلوماتية، دار الكتاب الحديث، القاهرة، مصر،ط1، سنة 2008، ص14.

وقد كثرت النعوت والأوصاف التي أضفاها العلماء والمفكرون على المرحلة التي يمر بها المجتمع الإنساني، وكلها تعبر عن ضخامة القفزات العلمية الهائلة التي تحققت في شتى مجالات الحياة، والواقع أن العصر الذي نعيشه يمتد ليشمل كل هذه التطورات والإنجازات، ومن هذا المنظور يرى الكثير من المفكرين الغربيين أن التعبير الذي يمكن أن تندرج تحته كل هذه الإنجازات والتطورات بمسمياتها المختلفة هو مصطلح ما بعد الحداثة، وهو الذي تنصهر في بوتقته سائر مظاهر الإنجاز و الإعجاز.[1]

لكن هذا التطور غير المحدود وضع الشعوب الفقيرة والمتخلفة وعالمنا كلّه أمام مشكلات جديدة تقيد الشعوب الفقيرة بأكثر ممّا تطلق يدها، وتزيد تخلفها أمام التطور العالمي بأكثر مما تساعد على تطوّرها، وتوسع الفجوة بينها وبين البلدان المتقدمة، ومع أنّ البلدان المتخلفة تسير إلى الأمام إلاّ أنّ الفجوة تتسع يوما وراء يوم، حتى غدت مشكلة شديدة التعقيد متعددة الأبعاد ذات تأثير على مختلف نواحي الحياة[2].

وقد نتج أيضا عن التطور العلمي والتقدم التقني ظهور الحاسب الآلي، مما أدّى إلى دخول نظام المعالجة الآلية للمعطيات في كافة مجالات الحياة، لأن هذا الحاسب يتمتع بقدرة فائقة في تخزين أكبر قدر من المعلومات والبيانات ويقوم بتصنيفها وترتيبها، بحيث يمكن البحث عنها والحصول عليها بسهولة وبسرعة، كما أصبح أهم وسيلة إتصال[3]، كما ساعدت تلك الحاسبات الإنسان خلال مراحل تطورها المختلفة على حلّ كثير من المشاكل التي كان يصعب على الإنسان حلّها بإمكانياته الذاتية دون بذل الكثير من الجهد والوقت ودون التأكد في نفس الوقت من صحة ودقة النتائج التي توصل إليها، كما أصبح استخدامها عنصرا أساسيا وفعالا لتحقق تقدم الأمم و الشعوب وكذلك معيارا لقياس مدى تحضر تلك الأمم[4].

فمن حيث الشؤون الخاصة للإنسان، فقد استخدم الحاسب الآلي في أداء كثير من الخدمات الأساسية التي يعتمد عليها في حياته اليومية، وتخزين الكثير من المعلومات والأسرار والإحتفاظ بها لحين الحاجة إلى استرجاعها، أمّا بالنسبة للحياة العامة، فلا يوجد مجال إلاّ وقد استحوذت عليه ونظمته الحاسبات الآلية ابتداءا من كبريات الشركات والمؤسسات العالمية والهيئات الحكومية والدولية المختلفة[5]،

---

[1]- د. هلالي عبد اللاه أحمد، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2006، ص12.

[2]- د. معوان مصطفى، التجارة الإلكترونية ومكافحة الجريمة المعلوماتية، المرجع السابق، ص19.

[3] -د. هلال بن محمد بن حارب البوسعيدي، الحماية القانونية و الفنية لقواعد المعلومات المحوسبة، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2009، ص 04.

[4]-د. أيمن عبد الحفيظ ، إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، أكاديمية الشرطة، مصر، بدون طبعة، سنة 2003، ص 48.

[5]- د. عفيفي كامل عفيفي و د. فتوح الشاذلي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية، منشورات الحلبي الحقوقية، لبنان، ط2، سنة 2007، ص 13.

وقد سهلت الحاسبات الآلية من عملية الإتصال السريع والمباشر بين الحكومات والشركات والأفراد، ممّا يدل على التغلب على النظام اليدوي للتخزين أو التعامل أو تبادل المعلومات وهذا بعد التطور الذي شهدته الحاسبات الآلية[1].

هذا إضافة إلى الخصائص الفريدة التي يتمتع بها من حيث أنه قابل للبرمجة فيمكن تصميمه ليؤدي وظائف معينة وذلك عن طريق البرمجيات التي يمكن تطويرها وتحديثها لتؤدي وظائف لا حدود لها[2]، كما لعبت برامجه دورا كبيرا في قطاع الخدمات من حيث احتوائها لكافة القطاعات، فقد دخلت في الإقتصاد والسياسية والقضاء، إذ ساعدت على كشف الجرائم سواء استخدامها كدليل أم كوسيلة لإظهار الأدلة، غير أنّ هذه البرامج تتنوع تبعا لعدة معايير وإن كانت هذه البرامج التي يتم إعدادها تنقسم إلى قسمين، تتمثل في البرامج من الناحية الفنية وحسب الغرض من تشغيلها والتي تشمل البرامج الخاصة بتشغيل جهاز الحاسب والبرامج التطبيقية لها، أمّا القسم الثاني فهي البرامج العملية التي تشتمل على البرامج النمطية إذ يتم استخدامها من كافة المستخدمين والبرامج الخاصة بالمستخدم لوحده دون غيره[3].

وليس من قبيل المبالغة القول بأن مجال تكنولوجيا الإتصالات والمعلومات يعدّ من أكثر المجالات تطورا وامتلاكا للتقنيات الحديثة التي تتيح لعدد لا بأس به من الأفراد الإستفادة من كلّ ما يتوصل إليه العالم في أصناف العلوم، وذلك عن طريق الرابط المباشر بين المعلومات والإتصالات بمختلف أشكالها، ولاشك أنّ الإنترنت هي الثورة الكبرى في عالم الإتصالات[4].

---

[1]- في القرن السابع عشر تمّ اختراع ماكينة الجمع التجارية المعروفة وتطورت الماكينة على مرّ الأيام، وفي عام 1818 بذلت عدة محاولات في تطوير ماكينة الجمع لكي تقوم بحلّ المعادلات الرياضية، وفي عام 1887 إستطاع أحد العلماء أن يبتدع وسيلة ميكانيكية لتسجيل البيانات ومعالجتها، وكان ذلك بتسجيلها في صورة ثقوب على شريحة مستطيلة من الورق، بحيث يكون موقع كلّ ثقب معبرا عن معنى محدد. وفي عام 1930 كانت صناعة الآلات الحاسبة وأجهزة معالجة البيانات لازالت وليدة تحبو إلى أن جاءت الحرب العالمية الثانية تفرض احتياجاتها وأصبحت حينها الطريقة الميكانيكية المتبعة في معالجة البيانات غير قادرة على القيام بالعمليات المطلوبة.

وقد تطورت الحاسبات الإلكترونية فبعدما كانت تعمل بالصمامات الإلكترونية وحجمها كبير ومن أشهرها الحاسب الإلكترو- ميكانيكي **مارك**، الحاسب الإلكتروني **إديساك**، كما أصبحت الحاسبات تعمل بالترانزيستور وقادرة على تخزين كمّ هائل من البيانات، وشهدت تطوّر إلى أن وصلت صناعتها إلى آفاق بعيدة في التقدم التكنولوجي. أنظر في ذلك: د.أحمد خليفة الملط ، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر ، بدون طبعة، سنة 2006، ص24.

[2]- د.عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، شركة البهاء للبرمجيات والكمبيوتر والنشر الإلكتروني، الإسكندرية، مصر، بدون طبعة، بدون سنة، ص21.

[3]- د. محمد فواز المطالقة، النظام القانوني لعقود إعداد برامج الحاسب الآلي، دار الثقافة، عمان، الأردن، سنة 2004، ص 39.

[4]- د. محمد سامي عبد الصادق، المرجع السابق، ص 13.

فالإنترنت كنظام للإتصالات، تعتبر الإمتداد الطبيعي لتكنولوجيا الإتصالات المعتمدة على الحاسبات، وهذه الأخيرة تجد جذورها التاريخية في ظهور و تطور تكنولوجيا الإتصالات الإلكترونية بوجه عام[1]، ولقد أدّى التطور المتسارع لشبكة الإنترنت إلى إحداث تحوّلات في مختلف جوانب الحياة، فهي من أكثر التقنيات أهمية وهي وليدة التزاوج بين نظم الحوسبة ونظم الإتصالات.

وكان ألبرت جو نائب الرئيس الأمريكي هو أوّل من فكّر في استخدام إمكانيات هذه الشبكة على نطاق عالمي وإنشاء ما يعرف بطريق المعلومات الرقمية أو طريق البيانات السريع، أو الطريق السريع الرقمي أو طريق المعلومات السريع أو فائق السرعة[2]، وهذا على غرار الشبكة العنكبوتية أو ما يعرف بشبكة المعلومات العالمية، فهي جزء من شبكة الإنترنت وتعد الجزء الأساسي والمهم منها، ذلك لأنها تشتمل على كافة المعلومات المنقولة عبر الشبكة، وتستخدم الشبكة العنكبوتية لنقل المعلومات التقنية خاصة وتعرف بلغة النص المتشعب، والتي تعمل على توصيل مختلف أنواع المعلومات عن طريق التنقل بين الصفحات والملفات المخزونة في مواقع مختلفة وفق نظام يسهل من التشعب من خلال عدد من العبارات المفتاحية المرتبطة مع بعضها بشكل عنكبوتي تعرف بالوصلات[3].

ومن أكثر الأمور المثيرة للإهتمام في عالم الإنترنت هو أن ليس هناك جهة معينة تتحكم في هذا العالم، وحتى نستطيع إقامة إتصال بين الحواسيب، فإنّ الأمر يتطلب وجود مجموعة من القواعد المتفق عليها والمعروفة باسم "البروتوكولات" والتي هي مجموعة من القوانين التي تحدد وتفصل كيف لحاسبين آليين أن يتصلا ببعضهما البعض عبر شبكة ما، والتي من خصائصها أنّها قادرة للعمل على عدّة محاور كما أنّها مطبقة، فكل طبقة تبدأ عملها بعد أن تنتهي الطبقة التي تحتها أو من فوقها من الإنتهاء من عملها، وتعدّ بسيطة على إعتبار أن كل طبقة في البناء مسؤولة عن بعض من العمليات والمهام[4].

---

[1]- إنّ بدايات فكرة هذه الشبكة لمحت إبان الحرب الباردة بين الإتحاد السوفياتي والولايات المتحدة الأمريكية، عندما أطلق السوفيات المركبة الفضائية **سبوتنك** عام1957، مما دفع الحكومة الأمريكية للتفكير بعمق في عملية تطوير أبحاث الدفاع. وتعود جذور هذه الشبكة العملاقة إلى عام 1969 عندما أسست وزارة الدفاع الأمريكية مشروع يهدف إلى تبادل المعلومات بينها وبين عدد من مراكز البحوث العلمية الهامة.

وفي عام 1971تبنت جامعة كاليفورنيا مشروعا مماثلا، حيث نجحت في إقامة شبكة معلومات ضخمة تضم خمسة عشر مركزا بحثيا كبيرا، أطلق عليها شبكة أربانت Arpanet حيث تمكن الباحثين والعلماء من تبادل المعلومات عن طريق البريد الإلكتروني، وفي سنة 1983إنقسمت شبكة الأربانت الى قسمين: شبكة الأربانت للإستخدامات العسكرية وشبكة مايلنتMilnet للإستخدامات المدنية أي تبادل المعلومات وتوصيل البريد الإلكتروني، ونظرا لأنّه كان من الممكن تبادل المعلومات بين هاتين الشبكتين، فقد ظهر إلى الوجود لأول مرة إصطلاح الإنترنت Internet، لكي يعبّر عن الإتصالات المتبادلة التي تتم بين هتين الشبكتين. أنظر في ذلك: د.محمد إبراهيم أبو الهيجاء، التعاقد بالبيع بواسطة الإنترنت (دراسة مقارنة)، دار الثقافة، عمان، الأردن، بدون طبعة، سنة 2002، ص44.

[2]- د.عمرو عيسى الفقي، وسائل الإتصال الحديثة وحجيتها في الإثبات، المكتب الجامعي الحديث، الإسكندرية، مصر، بدون طبعة، سنة 2006، ص87.

[3]- د. معوان مصطفى، التجارة الإلكترونية و مكافحة الجريمة المعلوماتية، المرجع السابق، ص22.

[4]- أ. منير محمد الجنبيهي و أ. ممدوح محمد الجنبيهي، بروتوكولات و قوانين الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2006، ص23.

وعلى الجانب المقابل، فقد أدى الإستخدام المتزايد للأنظمة المعلوماتية للحاسب إلى كثير من المخاطر رغم ما حققه من فوائد جمة وعظيمة في مجال التقدم التكنولوجي، وتتمثل هذه المخاطر في إمكانية تدمير برامجه وبياناته أو معرفة أسرارها، أو الإحتيال عليها وسرقتها وإتلافها، فقد واكب هذا التقدم التقني تقدما مناظر له وإن كان يفوقه في العقلية البشرية الإجرامية بأغراضها المختلفة، مما أفرز نوعا جديدا من الإجرام يطلق عليه الإجرام الإلكتروني[1].

فالحاسب الآلي من حيث الوجه السلبي لاستخدامه، لعب أدوارا ثلاثة في حقل الجريمة، فهو إمّا وسيلة تقنية لارتكاب الجرائم التقليدية بفعالية وبسرعة أكبر من الطرق التقليدية ، أو هو الهدف الذي تتوجه إليه الأنماط الحديثة من السلوك الإجرامي التي تستهدف المعلومات ذاتها، كما في اختراق النظم المعلوماتية والدخول إليها دون وجه حق، أو هو البيئة لما تتضمنه من محتوى غير قانوني كالمواقع المعلوماتية المروجة للأنشطة الغير مشروعة[2].

فالإعتداء على الحاسب الآلي بصورة عامة أو على أي جزء من أجزائه، يكبّد صاحبه خسائر مادية أو معنوية كحقوق المؤلّف مثلا، فقد فرضت هذه التقنيات نفسها على حقوق المؤلف سواء من حيث محلّها أو مضمونها، بما توفره من أشكال جديدة للتعبير الفني وبما تتيحه من وسائط إلكترونية ينبغي أن تؤدي بحسب الأصل إلى تدعيم الحماية القانونية لحقوق المؤلف في جانبيها الأدبي والمالي، غير أنّ ما حدث هو تنامي احتمالات الإعتداء على هذه الحقوق[3]، ولا ريب أنّ من عوامل الإزدهار والنمو الإقتصادي للدولة وجود نظام قانوني قوي ومتكامل يكفل الحماية للمبتكرين على اختراعاتهم وللمؤلفين على مصنفاتهم[4].

ولاشك أن تطور التقنيات الحديثة و ما تتميز به من خصائص جعلا من الإنترنت جهازا يقدم تسهيلات كبرى للأنشطة الإجرامية، وساعدت المجرمين على زيادة عدد وحجم جرائمهم دون زيادة في الجهد المبذول مع إنخفاض إحتمالات إكتشاف أمرهم ، وخطورة هذه الظاهرة الإجرامية المستجدة أنّ الجريمة يسهل ارتكابها على هذه الأجهزة أو بواسطتها، وأنّ تنفيذها لا يستغرق غالبا إلا دقائق معدودة، فضلا عن أنّ مرتكبي هذه الجرائم، وبالذات في مجال الجريمة المنظمة يلجأون إلى تخزين البيانات مع استخدام شفرات أو رموز

---

[1]- د. عفيفي كامل عفيفي و د. فتوح الشاذلي، المرجع السابق، ص 15.

[2]- د. رامي متولي القاضي، الجرائم المعلوماتية و طرق مواجهتها، بحث مقدّم لمؤتمر الجرائم المستحدثة (كيفية إثباتها و مواجهتها)، المركز القومي للبحوث الاجتماعية والجنائية، مصر، سنة 2010، ص01.

[3]- د.أسامة أحمد بدر، تداول المصنفات عبر الإنترنت، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2004، ص 02.

[4]- د. جلال وفاء محمدين، الحماية القانونية للملكية الصناعية وفقا لإتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تريبس)، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2000، ص09.

سرية لإخفائها عن أجهزة العدالة[1]، وقد أصبحت هذه الجرائم تهدد أمن وسلامة الأفراد والمؤسسات، فالمعلومات تتزايد يوما بعد يوم، ولا تتناقص بالإستخدام أو تستهلك، ومع تزايد المعلومات سوف تتزايد صور الإعتداءات والتهديدات، وظهور العديد من أنماط القضايا المختلفة[2] ، وفي الغالب فإن خطأ صغير في تشغيل هذه النظم يمكن أن يضع حياة الإنسان في خطر.

كما يتطلب الكشف عن الجرائم الإلكترونية ضرورة إستحداث طرق و أساليب جديدة للتحقيق الجنائي، و ذلك لتعقب و اقتفاء أثر هذه الجرائم ذات الطابع الخطير من خلال إجراءات ملائمة و فعالة شريطة مراعاة الإعتبارات المتعلقة بحقوق الإنسان، و في هذا الإطار تظهر أهمية التخصص و الكفاءة المهنية العالية، و دعم القدرات القانونية و الفنية، و مدى إمكان قيام إتجاه عام قادر على أخذ المبادرة و التغلب على الصعوبات القائمة في هذا المجال ، وبدون شك هذا لن يتأتى إلاّ إذا أخذت مختلف الدول على عاتقها إجراء إصلاحات تشريعية تنطلق من فلسفة جديدة ومنظور شامل يعتبر هذه النوعية من الجرائم تستهدف النيل من الأمن الإجتماعي والإقتصادي للدول وتعرضها لمخاطر شتى وعديدة[3].

وإن كان حجم التهديد المعلوماتي يتحدد على ضوء الأهمية التي تمتلكها الملفات و الأدلة الموجودة على الشبكة[4]، فطبيعة هذه الجرائم قد عقّدت من إجراءات جمع الأدلة التي قد تتطلب الرجوع إلى الموقع الأصلي لوقوع الجريمة والذي من الممكن أن يكون داخل دولة أخرى، فإجراءات البحث عن الأدلة في الجرائم الإلكترونية تتميز ببعض الخصوصية بالمقارنة مع الجرائم التقليدية فيما يتعلق بالإجراءات المتبعة في التحقيق مع ضرورة المحافظة على الأدلة و حمايتها من العبث.

إلا أنّ التزايد المستمر في الجرائم الإلكترونية يتطلب من جهات التحقيق والمسؤولين عن تنفيذ القانون إدراك كيفية الحصول على دليل إلكتروني مخزن في الحواسيب[5]، وأن تكون على دراية كافية بهذه المسائل التقنية على اعتبار أن الكشف عن هذا النوع من الجرائم يحتاج إلى أساليب خاصة من أجل الوصول إلى نتائج موثوق فيها، حيث يمكن إعتمادها في إثبات هذه الجرائم.

---

[1]- د. محمد أبو العلا عقيدة، التحقيق و جمع الأدلة في مجال الجرائم الإلكترونية، بدون تاريخ، ص 02. على الموقع: www.flaw.net

[2]- د. رامي متولي القاضي، الجرائم المعلوماتية و طرق مواجهتها، المرجع السابق، ص01.

[3]- د. أحمد وهدان ، المؤتمر العالمي الأول في الإتجاهات الحديثة في التحقيق الجنائي و الإثبات، المجلة الجنائية القومية، المركز القومي للبحوث الإجتماعية والجنائية، مصر، العدد الثاني، يوليو سنة 1996، ص 299– ص 302.

[4]– أ.حسن مظفر الرزو ، الأمن المعلوماتي (معالجة قانونية أولية)، مجلة الأمن و القانون، أكاديمية شرطة دبي، الإمارات العربية المتحدة، العدد الأول، سنة 2008، ص68.

[5]- د. عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، مؤسسة أدم للنشر و التوزيع ، مالطا، بدون طبعة، سنة 2008، ص40.

فالإثبات الجنائي هو تأكيد الحق بالبيّنة، والبيّنة هي الدليل أو الحجة، ومعنى ذلك أن الإثبات في اللغة هو تأكيد حقيقة أيّ شيء بأيّ دليل، أما في القانون، فهو تأكيد لحق متنازع فيه أو مسألة غير مؤكدة بحيث ترتب أثرا قانونيا بالدليل الذي أباحه القانون على ذلك الحق أو تلك المسألة.

وفي المواد الجنائية بصفة خاصة، يقصد بالإثبات إقامة الدليل على وقوع الجريمة أو عدم وقوعها وعلى إسنادها للمتهم أو براءته منها، فالإثبات في المواد الجنائية هو كافة الأدلة الكفيلة إمّا بتحقيق حالة اليقين لدى القاضي أو ترجيح موقف الشك لديه[1] ، والهدف منه هو بيان مدى التطابق بين النموذج القانوني للجريمة وبين الواقعة المعروضة.

وقد عرفه الدكتور "محمد مروان" بأنه : "تلك النتيجة التي تحققت باستعمال وسائل كالمعاينة أو الخبرة أو الشهادة أو القرائن أي إنتاج الدليل، وهو ما يعبر عنه بصيغة أخرى بأن الإثبات هو عملية تسمح بتكوين إقتناع حول مسألة محل شك أو نزاع"، ولهذا يتم الحديث عن نظام الإثبات بدل الإثبات والنظام عبارة تنطوي على جملة من المسائل التي تتعلق بطبيعة الوسائل المقدمة، قوتها الثبوتية، الدور الذي يقوم به أطراف الدعوى و كذا دور القاضي في إدارة هذه الوسائل.

وقد عرفت الأنظمة القانونية نظامين من نظم الإثبات الجنائي هما: نظام الإثبات القانوني[2] ونظام الإثبات المعنوي[3]، ويمكن أن يضاف إليهما نظام ثالث وهو نظام وسط بين النظامين السابقين يسمى بنظام الإثبات المختلط[4].

---

[1]- د.حسنين المحمدي بوادي، الوسائل العلمية الحديثة في الإثبات الجنائي، منشأة المعارف، الإسكندرية، مصر، بدون طبعة، سنة2005، ص05.

[2]- نظام الإثبات القانوني: في هذا النظام الحقيقة القضائية محددة مسبقا بقواعد قانونية، فالمشرع هو الذي يضبط وسائل الإثبات فيقر قواعد قانونية تبين للقاضي وسائل الإثبات المقبولة كما تبين موقع هذه الوسائل في السلم التدريجي وقوتها الثبوتية، فدور القاضي يقتصر على مراعاة تطبيق القانون من حيث توفر دليل الإثبات، فإذا لم يتوفر فإنه يجوز له أن يحكم بالبراءة المقررة حتى ولو كان لديه إقتناع شخصي بأن المتهم الماثل أمامه هو الشخص الذي ارتكب الجريمة. أنظر في ذلك : د. محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ج 1، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، بدون طبعة، سنة 1999، ص 35.

[3]- نظام الإثبات المعنوي أو الحر: يتمثل في أن الإقتناع الشخصي هو وحده الذي يتحكم في قرار القاضي الجنائي، وهذا الإقتناع لابد أن يصدر بكل حرية من ضمير القاضي، فهذا الأخير يجب أن يكون حرا من جهة في اختيار الدليل من بين الأدلة المتعددة، ومن جهة أخرى حر في تقييمها أو تقديرها، فهو يكرس مبدأ حرية القاضي في الإقتناع ولا سلطان عليه في ذلك إلا ضميره . أنظر نفس المرجع ، ص 39.

[4]- نظام الإثبات المختلط : يسعى هذا النظام إلى الجمع بين المفهومين السابقين، فلكي يتسنى للقاضي إصدار حكمه ينبغي عليه أن يكون مقتنعا اقتناعا شخصيا، وفي نفس الوقت يحوز القناعة القانونية كما أقرها المشرع، غير أنه لا يعاب على هذا النظام أنه يربط قناعة القاضي بالقناعة القانونية بمعنى أن الواحدة منهما قد تشكل عائقا حقيقيا على الأخرى، مما يجبر القاضي على عدم الحكم بالإدانة أو البراءة ضد قناعته الشخصية لأن شروط القناعة القانونية غير موجودة، كما أنه من الناحية العملية يؤدي ذلك إلى تطبيق أحدهما إما الأول أو الثاني .أنظر نفس المرجع، ص 42.

وهذا الكلام يدعو إلى الحديث عن تطور نظم الإثبات التي مرت بعدة مراحل:

أولا: المرحلة البدائية: وهي مرحلة ما قبل وجود التنظيم الإجتماعي ووجود الدولة، فكان الفرد يحاول أخد حقه بنفسه إن استطاع، أو ينتقم من المعتدي بحسب قوته الجسدية أو قوة المجموعة البشرية التي ينتمي إليها، وميزة هذه المرحلة أن الضعيف لا حق له[1].

ثانيا: المرحلة الدينية: وقد اتجه تفكير الجماعات في هذه المرحلة إلى الإحتكام إلى الآلهة التي تتمتع بقوة خفية لحسم المنازعات، بحيث كانت الجماعات مثقلة بهموم البحث عن العقيدة، مما أدى إلى إلتصاق الطابع الديني بمفردات الجريمة والمجرم والعقوبة، واندمجت فكرة الجريمة بفكرة الخطيئة الدينية، واعتبر مرتكبها عاصيا، ولعل أهم وسائل الإثبات في هذه المرحلة هي اليمين الحاسمة[2] ، الإبتلاء[3] والمبارزة القضائية.[4]

ثالثا: مرحلة الإثبات المقيد: ظهرت هذه المرحلة مع ظهور الدولة ويعرف بنظام الأدلة القانونية، فبدأت مع تطوّر النظام الإجتماعي وبروز جهة الحكم التي وضعت قواعد بموجبها حددت أنواع الأدلة ومدى قوتها في الإثبات، وبالتالي يكون على الحاكم أو القاضي أن يتأكد فقط من توفر الدليل المطلوب لينطق بالنتيجة[5].

رابعا: مرحلة الإقتناع الذاتي : وفي هذه المرحلة تمّ الإنتقال إلى طريقة مختلفة تماما، بحيث ترك الأمر لحرية القاضي في تقدير الأدلة ومدى اقتناعه بها، مع وضع أسس وقواعد تحدد كيفية الوصول إلى الأدلة ، وهذا هو النظام السائد حاليا في كافة الأنظمة، فدور القاضي هو تمحيص الأدلة التي لها دور في كشف الحقيقة[6].

خامسا: مرحلة الدليل العلمي والإلكتروني: لقد أصبحت هذه المرحلة تلعب دورا كبيرا في الإثبات على حساب الوسائل التقليدية الأخرى حيث ساعدت في ذلك العلوم الحديثة، ولا يمكن لأحد أن يتجاهل ما قدمه العلم الحديث من خدمات في هذا المجال، وما جاء به من إسهامات عظيمة مكنت البشرية من فتح

---

[1]- أ. نجيمي جمال ، إثبات الجريمة على ضوء الإجتهاد القضائي، دار هومه، الجزائر، بدون طبعة، سنة 2012،ص 27.

[2] – اليمين الحاسمة: وهي أن يحلف المتهم يمينا أو المدافع عنه، بأنه غير مذنب حتى يتطهر أو يتخلص من الإتهام المنسوب إليه فهي عملية فردية يؤديها الشخص المتهم أو المدعى عليه علانية.

[3] – الإبتلاء: إتخذت هذه الوسيلة صورا متعددة، كأن يبلى المتهم باجتياز إختبار قاس مثل إلقائه في نهر، أو تجريعه شرابا مسموما، أو أن يغمس المتهم إحدى يديه في إناء معدني مملوء بالماء المغلي، أو المرور خلال نار مشتعلة فإذا نجى فهو برئ لأن عدالة السماء أنقذته.

[4] – المبارزة القضائية: تأخذ صور الإقتتال الفردي بين المتهم والمدعي بحيث يتقاتلان في مكان خاص يسيطر عليه جو تسوده طقوس دينية فإذا انتصر المتهم كان ذلك دليل براءته. أنظر في ذلك: د.محمد أمين الخرشة، مشروعية الصوت و الصورة في الإثبات الجنائي (دراسة مقارنة)، دار الثقافة، عمان، الأردن، ط 1، سنة 2011 ،ص26.

[5]- أ. نجيمي جمال ، المرجع السابق، ص 29.

[6]- نفس المرجع، ص 29، وكذلك :د.محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، مطبعة جامعة القاهرة، مصر، بدون طبعة، سنة1977، ص 04.

آفاق في تذليل الكثير من الصعوبات والعراقيل، وذلك عن طريق الإستعانة بأجهزة التنصت والتسجيل الدقيقة، أو باستخدام آلات التصوير عن بعد، واستخدام العقول الإلكترونية ذات الحساسية العالية والبرامج الإلكترونية الدقيقة، وغير ذلك من التقنيات العديدة والمتطورة التي يصعب حصرها[1].

كما تطورت نظم الإجراءات الرامية إلى تحقيق والمحاكمة وفق نمطين يتمثلان في النظام الإتهامي[2] والنظام التنقيبي[3]، أما قانون الإجراءات الجزائية الجزائري فقد اعتمد النظام التنقيبي في مراحل التحقيق طبقا للمادة (11)[4] منه، كما اعتمد النظام الإتهامي في مرحلة المحاكمة بالنسبة لمختلف جهات الحكم[5] .

وترجع الأهمية العلمية لهذا الموضوع والدافع إلى اختياره إلى التطور المذهل في ميادين العلوم وتكنولوجيات الإتصالات مما يقتضي بالضرورة أن يكون البحث العلمي هو الآخر متماشيا معه.

فقد زادت نسبة الجرائم الإلكترونية بصورة متناسبة مع هذا التقدم، فكان لابدّ من تحديث وسائل الإثبات بما يتناسب و التقدم في أدوات الجريمة الإلكترونية، إذ يتعين على جهات التحقيق أن تستعين بأساليب حديثة في الإثبات الجنائي.

ومن تمّ فإنه حين يثار موضوع الإثبات فإن الأمر يرتبط بنقطتين: الأولى، هي موضوع الدليل التي تسعى إليه العدالة الجنائية بقصد التوصل إلى إثباته، أمّا الثانية، فهي متعلقة بالحقيقة الواقعية، وهي الواقعة بأشخاصها، أي الواقعة الإجرامية التي حدثت ومرتكبيها، والتي يرتب عليها القانون آثارا جنائية سواء من حيث القاعدة الموضوعية أو من حيث القاعدة الإجرائية[6].

---

[1]- د. معوان مصطفى ، التجارة الإلكترونية و مكافحة الجريمة المعلوماتية، المرجع السابق، ص 08.

[2]- النظام الإتهامي يتمثل في قيام المتضرر بتوجيه الإتهام لمن يعتقد أنه هو الجاني، وعندئذ يكون على كل طرف أن يثبت صحة موقفه، ويقتصر دور القاضي على التحكيم لا على التحقيق، كما يتميز بالعلنية والشفوية و الوجاهية.

[3]- النظام التنقيبي يعتمد على التحريات السرية ، وهو يهدف من حيث المبدأ إلى تضييق المجال على المتهمين كي لا يفلتوا من العقاب، وأول ميزات هذا النظام غياب العلنية كما أن الإجراءات تتم كتابيا لتسجيل مواقف الأطراف وتصريحات الشهود، إضافة إلى ذلك تغير دور القاضي من حكم حيادي إلى عضو فاعل يبحث عن الحقيقة. أنظر في ذلك : أ. نجيمي جمال ، المرجع السابق،ص 32.

[4]- تنص المادة 11 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري) على ما يلي:" تكون إجراءات التحري والتحقيق سرية، ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع...".

[5]- بالنسبة لمحكمة الجنايات تنص المادة 285 من قانون الإجراءات الجزائية على ما يلي:" المرافعات علنية ما لم يكن في علانيتها خطر على النظام العام أو الآداب..".

ونفس الأمر بالنسبة لمحكمة الجنح بموجب المادة 342 ومحكمة المخالفات بموجب المادة 398 وكذا غرفة الجنح والمخالفات بالمجلس طبقا لما ورد في المادة 430 من نفس القانون .

[6]- د. محمد فتحي، تفتيش شبكة الإنترنت لضبط جرائم الإعتداء على الآداب العامة، المركز القومي للإصدارات القانونية، القاهرة، مصر، ط1، سنة 2012، 2012، ص12.

وبالرغم من وجود صلة وثيقة بين الإثبات والدليل، فإنه لا يمكن تصوّر تطابق بينهما باعتبار أن الدليل هو الواقعة التي يستخدمها القاضي للبرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه، فهو المحصلة النهائية لكل مراحل الإثبات المختلفة، ومن تمّ فإن كلمة "إثبات" أعمّ وأشمل من كلمة "دليل"[1]، غير أنه نظرا للتقدم العلمي الكبير الذي تحقق في وسائل الإثبات وما نتج عنه من وسائل علمية حديثة، نستطيع أن نتغلب على كل محاولات المتهم لتضليل العدالة، فالمجرم لا يترك وسيلة إلا ويستعين بها من أجل مشروعه الإجرامي، فهو يستعين بجميع معطيات العلوم الحديثة، لذلك فالأمر يتطلب من رجال الأمن و القضاء أن يتصدوا للجريمة بالبحث العلمي و الوسائل العلمية الحديثة التي توصل إليها العقل البشري من أجل مقاومة التيّار الإجرامي[2].

ونظرا لحداثة الوسائل المذكورة، فإن أغلب التشريعات العربية والدولية، لم تكن لها موقف محدد وواضح فيما يتعلق بأمر قبولها في الإثبات وحجيتها القانونية، الأمر الذي ترك الباب مفتوحا أمام الإجتهادات الفقهية بين مؤيد ومعارض، وبالنظر إلى ما بات يشكل استخدام الوسائل المذكورة من خطورة على حقوق الإنسان والحريات العامة، إذ أضحت محورا لمداولات عدد من المؤتمرات العلمية، بقصد إرساء مبادئ عامة تحميها وتضبط استخدامها، لاسيما في ظل قصور التشريعات الوطنية وعدم مواكبتها للتطور العلمي والتكنولوجي[3].

ولاشك أن هذا التطور وصل إلى درجة من التقدم أصبحت تثير المخاوف لأنها تجاوزت حدود حرمة الحياة الخاصة وحرمة الجسد، وأصبحت تكشف كل شيء عن أسرار الإنسان حتى تلك التي لا يرغب هو في معرفتها، وإذا استمر التطور على هذا الحال، فإن أفراد المجتمع سيصبحون عبارة عن أرقام وبيانات داخل الحاسوب، ويكون من يجلس أمام هذه الآلة هو المتحكم في مصيرهم بنقرة على زر الفأرة، أو بالضغط على لوحة المفاتيح[4]، ومع ذلك فقد أصبحت الحياة الخاصة للأفراد[5] والقوانين التي تنظم جمع

---

[1]- د. محمود محمود مصطفى، المرجع السابق، ص 42. نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص 22.

[2]- د. محمد أمين الخرشة، المرجع السابق، ص 31.

[3]- د. معوان مصطفى، التجارة الإلكترونية و مكافحة الجريمة المعلوماتية، المرجع السابق، ص 09.

[4]- أ. نجيمي جمال، المرجع السابق، ص 11.

[5]- نظرا لصعوبة وضع تعريف محدد للحق في الحياة الخاصة، فقد ترك المشرع هذه المسألة للفقه والقضاء، فقد إتجه رأي في الفقه الفرنسي إلى تعريف الحق في الحياة الخاصة، بأنه الحق في الحياة الأسرية و الشخصية و الداخلية والروحية للشخص عندما يعيش وراء بابه المغلق، وقد قيل أن الحق في الحياة الخاصة هو حق الفرد في إستبعاد الآخرين من نطاق حياته الخاصة، والحق في إحترام ذاتيته الشخصية الخاصة، أي الحق في أن يترك وشأنه.كما وسع البعض في مضمون الحياة الخاصة، حيث أخلط بينها وبين فكرة الحرية، و اتجه آخرون إلى تضييق مفهومها، وفضلوا ربطها بأفكار معينة حيث عرّفها أحد الفقهاء بأنها لا تعني فقط الحق في أن يظل المرء بعيدا عن تطفل الآخرين، ولكنها تتسع لأكثر من ذلك، لأنها تعني أن يعيش الشخص كما يحلو له مستمتعا بممارسة أنشطة

المعلومات عن الأشخاص وبرمجتها بواسطة الكمبيوتر لا ترمي فقط إلى حماية المعتدى عليه في حياته الخاصة فقط وإنما كل ما يتعلق به إحتراما لحريته الشخصية[1]، نظرا لتأثر هذا الحق بالتطور التكنولوجي، وإن كان هناك ما يميز بين ما يدخل في نطاق الحياة العامة، وما يتصل بالحياة الخاصة للأفراد.

لذلك كان لابد من التدخل لحماية البيانات المتعلقة بالشخص، على اعتبار أن التقنيات الحديثة أصبحت تشكل خطرا على خصوصيات الأفراد، وإن كان هناك مبدأ مفاده أن الحرية في الحصول على المعلومة حق لكل شخص، إلا أن هناك بعض الشروط تتعلق بمضمون وطبيعة المعلومات المتعلقة بالشخص[2]، لذلك فقد صاحب الإعتماد المتنامي على نظم وخدمات المعلومات الرقمية بزوغ الحاجة الملحة لتوفير الثقة والشفافية لهذه النظم[3].

فلا شك أنّ الأساليب والوسائل العلمية الحديثة تثير مشكلتين أساسيتين في الإثبات تتعلق بمدى مشروعيتها، ومدى حجيتها في الإثبات، فيمكن القول أنّ مسألة قبول الدليل المستمدّ من الوسائل العلمية الحديثة مرتبطة أساسا بفكرة المشروعية وهي ذات المضمون الهام، مما يتعذر في كثير من الأحيان التعبير عنها في قوالب قانونية جامدة وتقليدية، أو إخضاعها لمعايير ثابتة ومحددة، باعتبارها لصيقة على الدوام بالقيم السائدة في مجتمع ما وفي حقبة زمنية معينة، تتباين تبعا لتباين الثقافة في المجتمعات المختلفة ومدى حظ كل منها من التطور و التقدم من ناحية، وإلى أي حد بلغ نضج النظام القانوني فيها وما يوليه من اهتمام بحقوق الإنسان من ناحية أخرى[4].

أما فيما يتعلق بتأثير الأدلّة العلمية في استقلالية القاضي وحريته في تقدير أدلة الإثبات وتكوين اقتناعه، فلأوّل وهلة يبدو أن الخبير التقني هو القاضي الفعلي، بحيث إذا وضع يده على قضية ما، فإنه سيحدد مراكز الأطراف ويشخص المذنب من غيره، ولا يبقي للقاضي إلا تقدير العقوبة، ولكن خلال مراحل البحث سيتم إثبات أن مهام كل من القاضي والخبير ستبقى متكاملة من خلال إستعانة الأول بعمل الثاني.

خاصة معينة، حتى ولو كان سلوكه على مرآى من الناس، كما اتجه رأي إلى بيان ماهية الحياة الخاصة بأنها الحق في الخلوة. أنظر في ذلك: د.محمد محمد الدسوقي الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، سنة 2005، ص 105 وما بعدها.

[1]- د. غنام محمد غنام، الحماية الإدارية و الجنائية للأفراد عند تجميع بياناتهم الشخصية في أجهزة الكمبيوتر، مجلة الأمن و القانون، أكاديمية شرطة دبي، الإمارات العربية المتحدة، العدد الثاني، سنة 2011، ص84.

[2] - Jean Boyer, L'internet et la protection des données personnelles et de la vie privée, Cahiers français, édition de la documentation française, France, 2004, P 69.

[3]- د. كمال السيد غراب، نظم المعلومات الإدارية، دار المعارف، القاهرة، مصر، بدون طبعة، سنة 1997، ص 50.

[4]- د. معوان مصطفى، الإثبات في المعاملات الإلكترونية في التشريعات الدولية ، دار الكتاب الحديث، القاهرة، مصر، ط1، سنة 2009، ص 27.

فالقاضي لا يستطيع أن يكون خبيرا علميا،وفي المقابل رجل العلم يتعامل مع الجوانب المادية والعلمية فقط،فالإستعانة بالخبراء لا يعني تفويض الصلاحيات والتنازل عنها لصالح الخبير التقني، ولذلك كان من المقرّر أنّ القاضي ليس له اللجوء إلى الخبير إلاّ فيما يخص المسائل الفنية فقط[1]، فذكاء المجرم الإلكتروني لا يمكن الكشف عنه، ما لم يكن القائمين على كشف تلك الجرائم يتمتعون بخبرة تكنولوجية تفوق ما يتمتع به الجناة في هذا المجال[2].

وبالرجوع إلى قانون العقوبات، فهو الذي يتولى تحديد الأفعال التي يعتبرها المجتمع عن طريق سلطته التشريعية ماسّة بأمنه وكيانه فيحدّد أركانها كما يحدد العقوبة المناسبة لها، أما قانون الإجراءات الجزائية، فنلاحظ أن الجانب الأوفر منه يتناول مباشرة الدعوى العمومية وإجراءات التحقيق وعمل جهات الحكم، فمعظم أحكامه تدور حول أدلة الإثبات إبتداءا من كيفية الحصول عليها إلى كيفية تقديمها أمام القضاء إلى مناقشتها للوصول إمّا إلى الإقتناع أو الحكم بالإدانة، أو استبعادها ومن تمّ الحكم بالبراءة.

فلا شك أن الشق الموضوعي والإجرائي هما أساس الشرعية الجنائية، إلاّ أنّ الأمر ليس بهذه السهولة في نطاق الجرائم الإلكترونية، لذلك فالقانون الجنائي التقليدي لا يكفي من حيث المبدأ لمواجهة هذا الشكل الجديد من الإجرام، خاصة وأن النصوص التقليدية قد وضعت لتطبّق وفقا لمعايير معينة، يضاف إلى ذلك ما تتميز به الأساليب الفنية التي تستخدم في ارتكاب هذا النوع الجديد من الجرائم من ذاتية خاصة.

وهنا تظهر التحديات لقانون الإجراءات الجزائية، لأن تطبيق هذا القانون يستلزم وجود نص التجريم والعقاب من ناحية، كما أن تطبيق القواعد التقليدية تثير مشاكل معقدة تتعلق بالتكييف القانوني من ناحية أخرى، بالإضافة إلى الصعوبات التي تقف حائلا دون ضبط المجرم مرتكب هذه الجرائم إمّا بسبب عدم جواز تطبيق قانون الدولة عليه أو وجوده خارج دائرة إختصاصها[3].

و إن كان هناك إعتباران لابد من العمل في إطارهما، أولهما دفع الضرر وثانيهما هو الحفاظ على المنافع المرجوة من هذا النظام، و إن تحققت الموازنة بينهما فذلك أفضل الحلول[4].

وحتى وإن وجدت تعديلات في بعض التشريعات، إلا أن تطوّر العلوم المختلفة بشكل سريع جعل من الصعوبة بمكان ملاحقة ذلك التطور ومواكبته على صعيد التنظيم والتقنين في مجال حقوق الإنسان، فقد

---

[1] - أ. نجيمي جمال، المرجع السابق، ص 12.

[2]- د. أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة2012، ص05.

[3]-د. محمد فتحي، المرجع السابق، ص 14.

[4]- د. عمر الفاروق الحسيني، المشكلات العامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دار النهضة العربية، القاهرة، مصر، ط2، سنة1995، ص148.

ظلّت الفجوة ولا تزال كبيرة و الهوة شاسعة وعميقة بين الإثنين مما يشكل عقبة أمام المشرّع في محاولة سدّ الفراغ التشريعي في هذا الميدان، إذ لم يعد ممكنا اللحاق بركب التطور المذهل، باعتبار أن السباق غير متكافئ ولن يكن يوما كذلك[1].

– إشكالية البحث:

إن التحقيق في الجرائم الإلكترونية تواجهه صعوبات وعوائق كبيرة ، وذلك راجع لطبيعة هذه الجرائم التي تتم في بيئة إفتراضية مفتوحة على كل الإحتمالات، الأمر الذي يصعب من اكتشافها، و تمثل هذه المسألة تحديا جديدا لسلطات التحقيق، خاصة في ظل عدم فاعلية القوانين الموجودة في بعض الدول.

وبفعل الطبيعة الخاصة لهذه الجرائم فهي تسهل من مهمة إرتكابها، و في المقابل هناك صعوبة في جمع الأدلة المتعلقة بها، على اعتبار أن الدليل الإلكتروني يثير عدة مشكلات إجرائية، ناهيك عن إمكانية تعديله أو محوه بعد تنفيذ الجريمة من أجل طمس معالمها.

والإشكالية التي يطرحها موضوع البحث تتعلق بالقيمة العلمية لمثل هذه التقنيات الحديثة، و كيف نثق في الدليل المترتب عنها، كما أن الأمر يحتاج إلى ضرورة إحترام مجموعة من الضمانات الفنية و القانونية تكفل مصداقيته و مدى مشروعيته و النتائج المترتبة عنه و مدى قبوله في مجال الإثبات الجنائي.

أضف إلى ذلك، ما قد يلجأ إلية الجناة في هذه الجرائم من تخزين البيانات في أنظمة معلوماتية متواجدة في دول أخرى، الأمر الذي يطرح مشكلة سيادة الدولة، لذلك كان لابد من إعطاء جهات البحث و التحري و التحقيق وسائل تقنية متطورة للكشف عنها، غير أنه لابد من الموازنة بين مطلب الوصول إلى الحقيقة بفضل استخدام هذه التقنيات الحديثة وبين مبدأ احترام حقوق الإنسان، على اعتبار أن حماية الحرية الفردية مطلب مهم لتحقيق مبدأ سيادة القانون، أو ما يعبر عنه بمبدأ المشروعية الذي تقوم عليه الدولة القانونية.

فإذا كانت حماية الحقوق والحريات الفردية من المبادئ الدستورية التي لا يمكن التفريط فيها ، فإن حماية المجتمع و تحقيق الإستقرار و الوصول إلى الحقيقة من أسمى الغايات من أجل إقامة العدالة، فهل يجوز في سبيل الكشف عن الحقيقة التضحية بمصلحة الأفراد من أجل حماية مصلحة المجتمع؟ وهل يمكن في إطار الإثبات الإستعانة بجميع التقنيات الحديثة حتى ولو كان فيها مساس بحقوق وحريات الأفراد؟ وهل

[1] - د. معوان مصطفى، الإثبات في المعاملات الإلكترونية في التشريعات الدولية، المرجع السابق، ص 27.

من ضوابط و ضمانات يمكن اعتمادها عند استخدام هذه الأساليب الحديثة حتى تنتج عن دليل مشروع لإثبات هذه النوعية من الجرائم؟

كما يمكن طرح إشكالية أخرى تتعلق بمدى حرية القاضي الجزائي في تقديره للدليل الإلكتروني، وهل ذلك يتعارض مع مبدأ إقتناعه الشخصي؟

وانطلاقا مما تقدم، سأحاول كذلك معرفة موقف الفقه والقانون والقضاء من مسألة الدليل المستمد من الوسائل الإلكترونية، وما هي الآثار المترتبة في حالة انتهاك الحياة الخاصة للأفراد في ظل إستخدام وسائل وتقنيات حديثة ؟

– الصعوبات التي يطرحها الموضوع:

إنّ ما يمكن ملاحظته خلال مراحل البحث هو عزوف غالبية الباحثين عن التطرق لهذا الموضوع من الناحية القانونية، رغم ما يثيره الدليل الإلكتروني فيما يتعلق بمسألة قبوله و حجيته في الإثبات، خاصة وأن موضوع الإثبات الإلكتروني يعتبر من بين المواضيع الحديثة نسبيا لحداثة الجرائم الإلكترونية.

هذا إضافة إلى أن هذا الموضوع يتعلق بالناحية الفنية و التقنية، إذ يتعين التعرف على الجوانب التقنية للحاسب الآلي وشبكة الإنترنت بالنسبة للباحث، حتى يتسنى له الفهم الجيّد للبحث، خاصة وأنه يحتوي على العديد من المصطلحات التقنية التي تحتاج إلى شخص متخصص في هذا المجال.

كما أنّ أغلب المراجع التي تم الحصول عليها، تناولت الجانب التقني على حساب الجانب القانوني، ومما يزيد الأمر تعقيدا أنّ هذه التقنيات الحديثة هي في تطور مستمر، بينما النصوص القانونية بقيت بدون تعديل وحتى وإن عدلت فإنّ ذلك لم يكن موازيا، حيث أنّ هذه النصوص التقليدية أصبحت عاجزة عن توفير الحماية الكافية.

ناهيك عن وجود قصور في الأحكام القضائية بصفة خاصة، والمتعلقة بقبول الأدلّة الإلكترونية وحجيتها في الإثبات مع وجود صعوبة كبيرة في الحصول عليها، هذا فضلا عن غياب الإتفاقيات المتعلقة بتسليم المجرمين و تنفيذ الأحكام الأجنبية في هذه النوعية من الجرائم.

– منهج البحث:

بالنظر إلى أهمية البحث، وبغية الوصول إلى الأهداف المسطرة ، إرتأيت الإعتماد على المنهج التحليلي المقارن من جهة، والمنهج التأصيلي من جهة أخرى، وذلك من خلال تحليل كافة جوانبه، وأهمّ النقاط المثيرة للجدل وكذا تحليل النصوص القانونية المتعلقة به ، وذلك من أجل معرفة موقف هذه

التشريعات من مسألة مشروعية و مدى قبول الدليل الإلكتروني في مجال الإثبات الجنائي، وذلك لعدم وجود سوابق كثيرة تتعلق بهذا الموضوع في الجزائر.

ومن أجل إثراء هذا الموضوع وحتى تكون الفائدة أكبر سأحاول التطرق إلى موقف التشريع والفقه والقضاء المقارن، وذلك بغية الإستفادة من تجارب بعض الدول التي كانت سبّاقة في هذا الموضوع .

– خطة البحث:

من أجل الإجابة على الإشكاليات التي تم طرحها، تم تقسيم خطة البحث إلى بابين وخاتمة، حيث تطرقت في الباب الأول إلى ماهية الدليل في الجريمة الإلكترونية ومدى مشروعيته والذي قسم بدوره إلى فصلين، حيث تناول الفصل الأول الجريمة الإلكترونية والدليل المترتب عنها، أما الفصل الثاني فيبحث في مشروعية إجراءات جمع الدليل الإلكتروني.

أمّا الباب الثاني فتم تخصيصه لنطاق الدليل الإلكتروني والآثار المترتبة على عدم مشروعيته، حيث قسم إلى فصلين، خصّص الفصل الأول منه لاختصاص القاضي الجزائي وسلطته في قبول الدليل الإلكتروني وتقديره ، أمّا الفصل الثاني فقد تناول الآثار المترتبة على عدم مشروعية الدليل الإلكتروني.

أمّا الخاتمة فقد تضمّنت أهمّ النتائج التي تمّ التوصل إليها، مع إدراج بعض المقترحات والتوصيات التي رأيتها لازمة والتي أرجو أن تلقى قبولا.

الباب الأول: ماهية الدليل في الجريمة الإلكترونية ومدى مشروعيته.

نتيجة للتطور التقني للمعلومات والتقدم السريع والمتواصل لتطوير الأجهزة والبرامج المعلوماتية، واعتماد قطاعات كبيرة من المجتمع على التقنية المعلوماتية في شتى المجالات والميادين الإجتماعية والإقتصادية والسياسية والثقافية، فقد اتسعت دائرة استخدام الحاسبات الإلكترونية باضطراد وتطور مستمر وبسرعة غير مسبوقة، وأصبحت كافة الأجهزة العامة والخاصة تعتمد عليها في تسيير شؤونها، وإزاء هذا التغيير الذي صاحب هذا التقدم التقني الهائل، ظهر نوع جديد من الجرائم تسمى الجرائم الإلكترونية والتي هي إفراز لتقنية المعلومات[1]، كما أنها تتأثر بشكل خاص بالتطورات التكنولوجية والممارسات الجديدة وهذا ما يجعلها تتطور باستمرار[2].

ومما لاشك فيه أن الثورة العلمية في مجال نظم المعلومات الإلكترونية لم تؤثر فقط في نوعية الجرائم التي ترتبت عليها وفي نوعية الجناة الذين يرتكبون هذه الجرائم،وإنما أثرت تأثيرا كبيرا على الإثبات الجنائي، خاصة على طرق الإثبات حيث يمكن القول أن الطرق التقليدية أصبحت عقيمة بالنسبة لإثبات هذا النوع من الجرائم المستحدثة، لذا ظهر نوع خاص من الأدلة يمكن الإعتماد عليه في إثبات الجريمة الإلكترونية ومن تم نسبتها إلى فاعليها، وهو ما يعرف بالدليل الإلكتروني [3].

والدليل الإلكتروني من الأدلة الجنائية التي ظهرت مع ظهور الجرائم الإلكترونية وأصبحت ضرورة ملحة، فرضتها الحاجة إلى أدلة تنتمي إلى البيئة نفسها التي ترتكب فيها أو من خلالها هذه الجرائم، وأصبح هناك إعتراف قانوني بهذه الأدلة، وممارسة فعلية للإستفادة منها، إلاّ أن هناك بعض التخوف والتردد عند إثبات هذه الجرائم الإلكترونية ولأخذ بالدليل الإلكتروني، إضافة إلى وجود بعض الضوابط الإجرائية والتقنية التي تحكم عملية استنتاج الدليل وتقديمه للجهات المعنية، هذه الضوابط التي قد تؤخر الإثبات والإستفادة من الدليل الإلكتروني[4].

وبفعل الطبيعة الخاصة لأنماط الجريمة ، والقدرة على ارتكابها عبر الحدود والقدرة على إتلاف أدلة الجريمة، فإن القواعد الإجرائية الجنائية في ميدان التفتيش والضبط والتحقيق والإختصاص القضائي، يتعين أن تواكب هذا التغير وتضمن تحقيق التوازن بين حماية الحق في الحريات وبين متطلبات فعالية نظام العدالة الجنائي

---

[1]– د. هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص 238.

[2]- Eric Freyssinet, La cybercriminalité en mouvement, Novembre 2010, disponible à l'adresse suivante : www.cairn.info/revue-realites-industrielles-2010-4-page-28.htm.

3– أ. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة الأزاريطة، الإسكندرية، مصر، بدون طبعة، سنة 2010، ص 23.

[4]– د. ناصر بن محمد البقمي، المرجع السابق، ص 17.

في الملاحقة والمساءلة، من هنا كان تأثير التقنية العالية أو تقنية المعلومات على قواعد القانون الجنائي الموضوعية والإجرائية الأميز والأبرز من بين تأثيراتها على بقية فروع القانون[1].

ويعتبر مبدأ شرعية الجرائم والعقوبات صمّام الإستقرار القانوني الذي يجب أن يراعيه المشرع الجزائي عند حماية الحرية الشخصية للفرد، فهذا المبدأ يؤمنه ضد خطر القياس في مجال التجريم والعقاب في قانون العقوبات، وضد خطر التحكم والمساس بالحرية، كما يعتبر مبدأ الأصل في المتهم البراءة صمام الأمان القانوني الذي يجب أن يراعيه المشرع الإجرائي عند تحديد الإجراءات الجنائية حتى لا تكون أداة انتهاك للحقوق والحريات، إذا ما أريد المساس بها تحقيقا لمصلحة عامة.

وإذا كانت الحماية الجنائية للحقوق والحريات وحماية النظام تتم من خلال التجريم والعقاب،وكانت الإجراءات الجزائية تتخذ لتمكين الدولة من اقتضاء سلطتها في العقاب، فإن ذلك لا يعني التضحية بحقوق وحريات الأفراد الذي يتم التجريم والعقاب في مواجهتهم،ومن ناحية أخرى إذا كانت الحماية الجزائية للمصلحة العامة تتقرّر بقانون العقوبات وقانون الإجراءات الجزائية، فإن حماية الحقوق والحريات الأساسية تتقرّر بالدستور،ومن هنا كانت الشرعية الدستورية هي الضمان الأعلى لهذه الحقوق والحريات.

ولكن يبدو أنه لا يمكن أن يتصور العدل بغير حق يرد عليه، ولا حق إلا إذا تأسس على حقيقة وهي دوما في حاجة إلى البحث والتقصي، غير أن سهولة محو الدليل في زمن قصير تعد من أهم الصعوبات التي تعترض الإثبات في مجال الجرائم الإلكترونية، ذلك أنّه يمكن للجاني محو أدلة الإدانة أو تدميرها في وقت قصير وخاصة في حال تفتيش الشبكات أو عمليات الإتصال.

وأيضا تثير الجرائم الإلكترونية بعض المشاكل في جمع الأدلة، حيث يوجد بعض الصعوبات التي تتعلق بالتفتيش وقد تكون البيانات التي يجري البحث عنها مشفرة ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة، فيثور التساؤل عن مدى مشروعية إجباره على فك الشفرة، فسلطات التحقيق إعتادت أن يكون الإثبات ماديا ملموسا، ولكن في محيط الإنترنت لا يستطيع المتحري تطبيق إجراءات الإثبات التقليدية[2].

---

[1]– أ.هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص 07.

[2]– د. محمد فتحي، المرجع السابق، ص 08.

وقد برزت مع ظهور الجرائم الإلكترونية تحديات جديدة للقانون الجنائي،على اعتبار أن النصوص الجنائية التقليدية لا تكفي لمواجهة خطر الإعتداء على النظم المعلوماتية، فكان لابد من إجراء تعديلات قانونية لمواكبة هذا التطور التكنولوجي[1].

وسيتم التطرق للجريمة الإلكترونية والدليل المترتب عنها وذلك في الفصل الأول من خلال مبحثين خصص المبحث الأول منه لماهية الجريمة الإلكترونية، أمّا المبحث الثاني فيبحث في ماهية الدليل الإلكتروني.

أمّا الفصل الثاني فخصص لمشروعية إجراءات جمع الدليل الإلكتروني وذلك في ثلاثة مباحث تم التطرق في المبحث الأول للإجراءات العامة لجمع الدليل الإلكتروني، أمّا المبحث الثاني فقد عني بدراسة الإجراءات الخاصة لجمع الدليل الإلكتروني، وقد خصّص المبحث الثالث للتعاون الدولي في مجال إجراءات جمع الدليل الإلكتروني.

[1]- Lova Emmanuel, Loi contre la cybercriminalité – Retouche et amendement possibles, le 31/07/2014, disponible à l'adresse suivante : www.lexpressmada.com.

الفصل الأول:الجريمة الإلكترونية والدليل المترتب عنها.

يولد الدليل الجنائي بصفة عامة بمولد الجريمة ذاتها، سواء كان ذلك سابق على ارتكابها في مراحل الترتيب والإعداد أو مرحلة الشروع أو معاصرا لها عند اقتراف الأفعال التنفيذية، فالأدلة بطبيعتها تتواجد بتواجد الجريمة التي تقع[1]، لذلك كان من الطبيعي أن أتطرق أوّلا لموضوع الدليل الإلكتروني وهو الجريمة الإلكترونية، لأنه لا يستقيم الحديث عنه إلا بعد دراسة هذه الجريمة التي تعتبر حديثة نسبيا ، وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات، فهي جريمة تقنية يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية توجه للنيل من الحق في المعلومات، وتطال إعتداءاتها معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت، فهي تطال الحق في المعلومات وتمس الحياة الخاصة للأفراد وتهدد الأمن القومي وإبداع العقل البشري.

ونتيجة لحداثة هذه الجريمة، فقد كانت هناك إتجاهات مختلفة في تعريفها، كما أنّها تميزت بمجموعة من الخصائص والصفات عن غيرها من الجرائم الأخرى، كما أنّ هذه الجريمة الإلكترونية جلبت معها طائفة جديدة من المجرمين إصطلح على تسميتهم بمجرمي المعلوماتية، والحقيقة أنّه حتى الآن لم تتضح الصورة جليا بخصوص تحديد أصناف مرتكبي الجرائم الإلكترونية، واستظهار صفاتهم وضبط دوافعهم، وذلك لقلة الدراسات الخاصة بالظاهرة برمّتها من جهة، ونظرا لصعوبة الإلمام بمداها الحقيقي من جهة أخرى بفعل الحجم الكبير من جرائمها الصعبة الإثبات[2].

ومما لاشك فيه أن نشطاء الإنترنت يتمتعون بصفات وخصائص تميزهم عن غيرهم وذلك كانعكاس حتمي لما تتطلبه عمليات استخدام هذه الشبكة من قدرات تقنية وفنية هائلة، كما تختلف دوافعهم في إرتكاب هذه النوعية من الجرائم والأساليب المتبعة في ذلك[3].

لذلك فإن التطرق لمفهوم الجريمة الإلكترونية، والطبيعة الخاصة لهذه الجرائم وبيان موضوعها وخصائصها وسمات مرتكبيها ودوافعهم، يتخذ أهمية قبل التطرق للدليل الالكتروني، وعلى هذا الأساس ارتأيت تناول ماهية الجريمة الإلكترونية في المبحث الأول، أمّا المبحث الثاني فيخصص لماهية الدليل الإلكتروني.

---

[1]–أ. عائشة بن قارة ، المرجع السابق ، ص 25.

[2]– د. يونس عرب، جرائم الكمبيوتر و الإنترنت، بتاريخ 2002/02/01، ص 02، على الموقع www.arablaw.net

[3]– د. حسين الغافري، أ. محمد الألفي ، جرائم الإنترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة ، مصر، بدون طبعة، بدون سنة، ص38.

المبحث الأول: ماهية الجريمة الإلكترونية.

لابدّ أن نشير إلى أنّه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي والبعض الآخر يطلق عليها جريمة الإختلاس المعلوماتي أو الإحتيال المعلوماتي،وآخرون يفضلون تسميتها بالجريمة المعلوماتية.

فهذه الجريمة ناشئة أساسا من التقدم التكنولوجي ، ومدى التطور الذي يطرأ عليه، وهو متجدد بصفة دائمة ومستمرة وخاصة في مجال المعلوماتية[1] فمن الأجدر أن يطلق عليه اصطلاح"جرائم التكنولوجيا الحديثة"، فهي جرائم تكنولوجيا باعتبارها مرتبطة إرتباطا وثيقا بالتكنولوجيا التي تعتمد أساسا على الحواسيب وغيرها من أجهزة تقنية قد تظهر في المستقبل، وهي كذلك جرائم جديدة نظرا لحداثتها النسبية من ناحية، وارتباطها الوثيق بما قد يظهر من أجهزة حديثة تكون ذات طاقة تخزينية وسرعة فائقة ومرونة في التشغيل[2].

ولاختيار المصطلح يتعين أن يتم الدمج بين البعدين التقني والقانوني، فإذا عدنا للحقيقة الأولى المتصلة بنشأة وتطور تقنية المعلومات، نجد أن تقنية المعلومات، تشمل فرعين جرى بحكم التطور تقاربهما واندماجهما الحوسبة والإتصال، أمّا الحوسبة فتقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق، أمّا الإتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها الدارجة[3].

وقد أضافت المعلوماتية الكثير من الجوانب الإيجابية، إلا أنها في المقابل جلبت معها صنفا جديدا من المجرمين إصطلح على تسميتهم بمجرمي المعلوماتية، والمعلوماتية ينظر إليها دائما بوصفها أداة محايدة، وأن مصدر ضعفها وانتهاكها هو الإنسان ذاته، والذي غالبا ما يهيئ فرصة إستغلال الوسيلة المعلوماتية عن حسن أو سوء نية، فجوهر المشكلة يرتبط بالإنسان وشخصيته ودوافعه، وكما هو معروف فإنه لا يمكـــن

---

[1]– المعلوماتية: يشير مصطلح المعلوماتية (Informatique) إلى تكنولوجيا علم المعلومات وهو مصطلح مشتق من اللغتين العربية والفرنسية، من الأحرف الأولى من كلمتي (Information) أي معلومات وأوتوماتيك أو آلي (Automatique)، ويقابل هذان المصطلحان، المصطلح الإنجليزي (Informatic) وقد وضع لهذا المصطلح عدة تعريفات أبرزها ما جاء بقرار وزير التعليم الفرنسي بتاريخ **1981/12/12** من أنّ المعلومات هي علم المعالجة العقلانية بصفة خاصة بواسطة الآلات الأوتوماتيكية للمعلومات التي تعتبر مرتكزا للمعارف الإنسانية والإتصالات في المجال التقني والإقتصادي والإجتماعي. وكذلك ما جاء في القاموس الفرنسي لاروس في معنى المعلوماتية بأنّها: علم المعالجة الآلية والعقلانية للمعلومة باعتبارها مرتكزا للمعارف، كما أنها تكنولوجيا تجميع ومعالجة وإرسال المعلومات بواسطة الكمبيوتر، أو علم المعالجة العقلية للمعلومات باستخدام آلات تعمل ذاتيا. أنظر في ذلك: د. محمد حسن قاسم، مراحل التفاوض في عقد المكينة المعلوماتية (دراسة مقارنة)، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، بدون سنة، ص**04**.

[2]– د. فتوح الشاذلي و د. عفيفي كامل عفيفي، المرجع السابق، ص**33**.

[3]– د.خالد ممدوح إبراهيم، الجرائم المعلوماتية ، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة **2009**، ص **89**.

لأي عقوبة أن تحقق هدفها سواء في مجال الردع العام أو الردع الخاص ما لم تضع في الإعتبار شخصية المجرم[1].

وعلى هذا الأساس سيقسم هذا المبحث إلى مطلبين أتطرق في المطلب الأول لمفهوم الجريمة الإلكترونية، أمّا المطلب الثاني سيخصص لمفهوم الجاني في الجريمة الإلكترونية.

المطلب الأول: مفهوم الجريمة الإلكترونية.

هناك تعبيرات شاعت مع بدايات ظاهرة الجريمة الإلكترونية، واتسع استخدامها كالغش المعلوماتي والإحتيال المعلوماتي، أو إحتيال الحاسوب ونصب الحاسوب، ومن بين الإصطلاحات التي شاعت في العديد من الدراسات وتعود الآن بقوة إصطلاح الجرائم الإقتصادية المرتبطة بالكمبيوتر، وهو تعبير يتعلق بالجرائم التي تستهدف معلومات قطاعات الأعمال أو تلك التي تستهدف السرية وسلامة المحتوى وتوفر المعلومات، وبالتالي يخرج من نطاقها الجرائم التي تستهدف البيانات الشخصية أو الحقوق المعنوية على المصنفات الرقمية وكذلك جرائم المحتوى الضار أو غير المشروع، ولذلك لا يعبر عن كافة أنماط جرائم الكمبيوتر والإنترنت.

أمّا عن إصطلاحي جرائم الكمبيوتر والجرائم المرتبطة بالكمبيوتر فإنّ التمييز بينهما لم يكن منتشرا في بداية الظاهرة، أمّا في ظل تطور الظاهرة ومحاولة الفقهاء تحديد أنماط جرائم الكمبيوتر والإنترنت أصبحوا يستخدمون إصطلاح جرائم الكمبيوتر للدلالة على الأفعال التي يكون الكمبيوتر فيها هدفا للجريمة كالدخول غير المصرح به، وإتلاف البيانات المخزنة في النظم، أمّا إصطلاح الجرائم المرتبطة بالكمبيوتر فهي تلك الجرائم التي يكون الكمبيوتر فيها وسيلة لارتكاب الجريمة كالإحتيال بواسطة الكمبيوتر والتزوير ونحوها.

غير أنّ هذا الإستخدام ليس قاعدة ولا هو إستخدام شائع، لكن مع ذلك بقي هذين الإصطلاحين الأكثر دقة للدلالة على هذه الظاهرة، بالرغم من أنهما وجدا قبل تواجد الشبكات على نطاق واسع وقبل الإنترنت تحديدا، وحتى بعد الإنترنت بقي الكثير يستخدم نفس الإصطلاحين ليس لسبب إلاّ لكون الإنترنت بالنسبة للمفهوم الشامل لنظام المعلومات مكوّن من مكوّنات هذا النظام، ولأنّ النظام من جديد أصبح يعبر عنه باصطلاح نظام الكمبيوتر أو النظام المعلوماتي[2].

---

[1]- أ. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، الأردن، ط 1، سنة 2008، ص76.

[2]- د.خالد ممدوح إبراهيم، الجرائم المعلوماتية ، المرجع السابق، ص 90.

وثمة استخدام إصطلاح يغلب عليه الطابع الإعلامي أكثر من الأكاديمي، وهو إصطلاح جرائم الياقات البيضاء، ولأنّ الدقة العلمية تقتضي انطباق الوصف على الموصوف، فإن جرائم الياقات البيضاء تتسع لتشمل أكثر من جرائم الكمبيوتر والإنترنت وتتصل بمختلف الأشكال الجرمية[1].

أما المشرع الجزائري، فقد استخدم مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، وذلك من خلال تعديل قانون العقوبات بموجب القانون رقم (04-15)[2]، بقسم سابع مكرر عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات"، ويشمل المواد من (394 مكرر) إلى (394 مكرر 7)، وسيتم التطرق إليها بالتفصيل في الباب الثاني.

غير أنه بالنظر لمصطلح المعالجة الآلية للمعطيات، ألاحظ أن المشرع الجزائري استخدم مصطلحا غير دقيق لأنه يقتصر فقط على جرائم الكمبيوتر دون أن يضم أيضا جرائم الإنترنت، ولكن مع تزايد حجم الجرائم الإلكترونية، إستدعى ذلك تدخلا تشريعيا،حيث أصدر المشرع قانون رقم (09-04)[3] تم بموجبه إستعمال مصطلح آخر هو الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

غير أنه يفضل استخدام مصطلح الجريمة الإلكترونية كونه أكثر دقة ووضوحا، كما أنه يشمل كل من جرائم الكمبيوتر والإنترنت وغيرها من الجرائم الناتجة عن استخدام شبكات الإتصال.

وبناء على ذلك فإن مصطلح الجريمة الإلكترونية هو الأمثل حسب رأي العديد من الفقه ، باعتبار أنها تتم عن طريق جهازي كمبيوتر أو أكثر متصلين فيما بينهم عبر شبكة الإنترنت.

ونظرا لوقوع هذه الجريمة في غالب الأحيان في بيئة المعالجة الآلية للبيانات، حيث تكون المعلومات محل الإعتداء عبارة عن نبضات إلكترونية، و تم الإعتراف بأننا أمام ظاهرة إجرامية ذات طبيعة خاصة لها صلة بما يعرف بالقانون الجنائي المعلوماتي.

ووقوع هذه الجرائم في هذه البيئة الخاصة يستلزم بيان مفهوم هذه الجرائم و تحديد أركانها وخصائصها، لأننا نتعامل مع مفردات جديدة كالبرامج و البيانات التي تشكل محلا للإعتداء أو تستخدم وسيلة للإعتداء[4].

---

[1]- أ.نبيل صقر، جرائم الكمبيوتر والإنترنت في التشريع الجزائري، دار الهلال للخدمات الإعلامية،الجزائر، بدون طبعة، سنة 2005، ص38.

[2]- الأمر رقم 66-156 المؤرخ في 08 يونيو 1966 المعدل والمتمم بالقانون رقم 04-15 المؤرخ في 2004/11/10 والمتضمن قانون العقوبات الجزائري، ج ر رقم 71.

[3]- قانون رقم 09-04 المؤرخ في 14 شعبان 1430هـ الموافق ل 5 غشت سنة 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47.

[4]- د. فتوح الشاذلي و عفيفي كامل عفيفي، المرجع السابق، ص 34.

وسأتطرق فيما يلي لتعريف الجريمة الإلكترونية (الفرع الأول) مرورا بتحديد خصائصها (الفرع الثاني)، أمّا(الفرع الثالث) فخصص لمحل الجريمة الإلكترونية.

الفرع الأول: تعريف الجريمة الإلكترونية.

ساهم الحاسب الآلي في تعديل وتطوير النمط السلوكي التقليدي المعتمد على الجهد العضلي في تحقيق النتيجة، هذا التطور فتح المجال أمام سلوكيات جديدة، وأساليب مختلفة لارتكاب أفعال سلبية تمثل جرائم مختلفة تتم باستخدام الحاسب الآلي، أو يكون الحاسب الآلي نفسه محلا لها.

هذه الجرائم كانت محل اهتمام الفقه والقانون الغربي على وجه الخصوص، على اعتبار أن الفقه العربي كان متأخرا، وبالتالي لم يبحثها بعد بصورة جدية، فالجريمة الإلكترونية تقاوم التعريف ولا أدل على ذلك من عدم إتفاق الفقه على تعريف جامع ومانع لها، فبعض هذه التعاريف يرتبط بوسيلة ارتكابها فقط، أو تعريفها حسب الضابط الشخصي أو المعرفة التقنية لدى المجرم[1]،وإن كان البعض الآخر يربطها بالمعلومات، أو الأجهزة وبالأشخاص والأموال.

ولذلك تعد مسألة تعريف الجريمة الإلكترونية من المسائل الصعبة، لأنه في الواقع يصعب حصر صورها، ولهذا تعددت تعريفاتها وفيما يلي سأتناول أبرز التعريفات.

البند الأول: التعريفات الفقهية للجريمة الإلكترونية.

في الواقع يصعب وضع تعريف عام وشامل للجريمة الإلكترونية، إذ لا يوجد تعريف محدد ومتفق عليه بين جميع الفقهاء، حيث ذهب جانب إلى تناولها بالتعريف على نحو ضيق، وجانب آخر عرفها على نحو متسع.

أولا: التعريفات المضيقة للجريمة الإلكترونية.

ما ذهب إليه الفقيه (Van Der Merwe) ، حيث يرى بأن الجريمة الإلكترونية هي: "ذلك الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي، أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسب

[1]– د. هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص 14.

الآلي كأداة رئيسية،أو هي مختلف صور السلوك الإجرامي الذي يرتكب باستخدام المعالجة الآلية للبيانات"[1].

أما الأستاذ (Klaus Tiedmann)، يرى أن "الجريمة الإلكترونية تشمل أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات"[2].

كما أنّ المقصود بالجريمة الإلكترونية: "الإعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح"، أو هي :"نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها، أو حذفها والتي تحوّل عن طريقه"[3].

وإن كان هذا التعريف يتسم بقدر من التكامل غير المتوافر للتعريفات السابقة، إلا أنه يلاحظ عليه أنه بدأ صائبا وانتهى معيبا، فحقق بذلك أساس فكرة المشروعية –أنه لا جريمة ولا عقوبة إلا بنص– ولكنه انتهى إلى توسع غير مبرر في التعريف، حيث ذكر أن جريمة الحاسب يمكن أن تنتج من أي نشاط غير مشروع يتعلق بالمعلومات التي يمكن أن تحوّل عن طريقه، فلم يبيّن طبيعة هذا التحويل، ففتح الباب واسعا أمام التفسيرات التي يمكن أن تعصف بمبدأ المشروعية. كذلك ما يلاحظ على هذا التعريف أنه لم يبيّن محل الإعتداء، بالرغم من أنه يدرج ضمن التعريفات المتركزة حول موضوع الجريمة[4].

كما أنّ ربط الجريمة بتحقيق الربح معناه ربط القاعدة الجزائية بالغاية من الفعل، والواقع أن الغاية لا علاقة لها بالتجريم، فهي ليست عنصرا فيه، بغض النظر عن طبيعتها إن كانت مشروعة أم لا، ولذا فقصر الجرائم الإلكترونية على الحالات التي يقصد فيها المجرم تحقيق الربح أمر غير منطقي وغير مقبول، إذ قد ترتكب جرائم الحاسب الآلي لغير تحقيق الربح، كالتجسس والإطلاع على المعلومات، أو إكتشاف أسرار تجارية أو الإساءة لسمعة الآخرين وكلها باستخدام الحاسب الآلي[5].

---

1 - Van Der Merwe, computer crimes and other crimes against information technologie in South Africa, RIDP, 1993.

نقلا عن: د.طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة، الإسكندرية ، مصر، بدون طبعة، سنة 2009، ص 153.

2- Klaus Tiedmann, Fraude et autres délits d'affaires à commis à l'aide d'ordinateurs électroniques, RDPC, 1984, P612.

نقلا عن : أ. نهلا عبد القادر المومني، المرجع السابق، ص 48.

3– د. يونس عرب، دليل أمن المعلومات والخصوصية، إتحاد المصارف العربية، القاهرة ، مصر، ط 1 ، سنة 2002، ص 213.نقلا عن : أ. نهلا عبد القادر المومني، المرجع السابق، ص48.

4– د. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2001، ص74. نقلا عن : د. طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 156.

5– د. هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص 16.

وقد جاء في تعريف (David Tompson) أنها: "جرائم يكون متطلبا لاقترافها أن يتوافر لدى الفاعل معرفة تقنية الحاسب"[1]، كذلك وحسب هذا التعريف، فإنه يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة، بل كذلك لملاحقتها والتحقيق فيها.

والحقيقة أن التعريفات السابقة للجريمة الإلكترونية كانت قاصرة على الإحاطة بأوجه ظاهرة الإجرام المعلوماتي، وقد عرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها :"الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا".[2]

وعرّفLeslie B. Ball الجريمة الإلكترونية بأنها : "فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية"[3]،غير أن هذا التعريف هو الآخر تعرض للنقد، حيث أن التعريفات التي ترتكز على وسيلة ارتكاب الجريمة ليست جامعة ولا مانعة، كما أنها تتسم بقصور كبير في إعطاء تصور علمي للجرائم الإلكترونية، ومنها الجرائم التي تقع على برامج الحاسب الآلي، كما أن الإعتماد في تعريف الجريمة الالكترونية على الوسيلة المستخدمة في ارتكابها يواجهه عدة إنتقادات لأنه في الجريمة يجب الرجوع إلى العامل الأساسي المكوّن لها، وليس فقط إلى الوسائل المستخدمة لتحقيقها، فليس لمجرد أن الحاسب قد استخدم في جريمة ما، فإنه يجب اعتبارها من الجرائم الإلكترونية[4].

كما يعرفها البعض[5] بأنها: " كل سلوك غير قانوني وغير مشروع مترتب عن الربط بين نظام الكمبيوتر الكمبيوتر وشبكة الإنترنت"،وتعرّف كذلك بأنها: "مجموعة الجرائم المرتكبة عبر شبكة الإنترنت"[6].

كما أنها تعني أيضا:" شبكة عالمية للحواسيب مرتبطة خارجيا"[7].

وإزاء هذه الإنتقادات، حاول جانب من الفقه تعريف الجريمة الإلكترونية على نحو واسع في محاولة لتفادي أوجه القصور التي شابت تعريفات الإتجاه المضيق.

---

[1] - David Tompson, Curent trends in computer crime, control computer quarterly, 1991, P2.
نقلا عن: د. طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 154.

[2]– نقلا عن : نفس المرجع، ص 155.

[3]- Lesli B. Ball, computer crime in the information technologie revolution, RIDP , 1985, P 543.
نقلا عن : نفس المرجع، ص 155.

[4]– د. هلال بن محمد البوسعيدي، المرجع السابق، ص 16.

[5] –Mohamed Chawki, Essai sur la notion de cybercriminalité, IEHEI, France, 2006, P 20.

[6]- La cybercriminalité, disponible à l'adresse suivante : www.interieur.gouv.fr.

[7]– د. شافع بلعيد عاشور، العولمة التجارية و القانونية للتجارة الإلكترونية، دار هومه، الجزائر، بدون طبعة، سنة 2006، ص 16.

ثانيا: التعريفات الموسعة للجريمة الإلكترونية.

يرى أصحاب هذه التعريفات أنّ سوء استخدام الحاسب أو جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة، هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته،كما تمتد جريمة الحاسب لتشمل الإعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به، وكذلك الإستخدام غير المشروع لبطاقات الإئتمان، أو إنتهاك ماكينات الحاسبات الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية، وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة جهاز الحاسب في حد ذاته وأي مكوّن من مكوناته[1].

وتناول الدكتور "هلالي عبد اللاه أحمد" تعريف الجريمة الإلكترونية بأنها: "عمل أو إمتناع يأتيه الإنسان إضرارا بمكونات الحاسب وشبكات الإتصال الخاصة به، التي يحميها قانون العقوبات، ويفرض لها عقابا.

ويمتاز هذا التعريف بالسمات التالية:

1. أنّه يحتوي على كل صور الإعتداء الإيجابية أو السلبية التي تقع إضرارا بمكونات الحاسب المادية والمعنوية وشبكات الإتصال الخاصة به، باعتبارها من المصالح التي يحميها قانون العقوبات.
2. أنّه يتضمن الأثر الجنائي المترتب على العمل أو الإمتناع غير المشروعين، ويتمثل في الجزاء الجنائي بكافة صوره وأنواعه، وهو أشد أشكال التعبير عن معنى الإلزام في القاعدة القانونية.
3. أنّه يحافظ على الشرعية الجنائية إذ لا يمكن أن يوجه أي اتهام ضد شخص لارتكابه فعلا معينا، ما لم يكن منصوصا على تجريم هذا الفعل في القانون، كما لا يمكن تطبيق عقوبة ما لم تكن محددة سلفا.

وتبنى الخبير الأمريكي (Donn Parker) مفهوما واسعا للجريمة الإلكترونية، حيث يشير إلى أنها:"كل فعل إجرامي متعمدا أيّا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل"[2].

---

[1]– د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، ط2، سنة 2008، ص 106.

[2]- Donn Parker, Computer crime, computer security refrence book, 1992, P 121.

نقلا عن : أ.نهلا عبد القادر المومني، المرجع السابق، ص 49.

كذلك يعرف الأستاذ (Michel Vivant) الجريمة الإلكترونية أنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب"[1].

ونظرا لخطورة هذه الجريمة وآثارها الممتدة التي قد تصل من دولة إلى أخرى، فإن بعض الهيئات الدولية المعنية بجرائم الكمبيوتر، قد أرست قواعد لتعريف هذا النوع من الجرائم ومن هذه الهيئات، هيئة التعاون الإقتصادي والتنمية التي اتخذت التعريف التالي:

"أي سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالنقل أو المعالجة الآلية للبيانات "[2]، كما أنّ مفهوم الجريمة الإلكترونية يغطي جميع الجرائم التي ارتكبت عن طريق الأنظمة و الشبكات المعلوماتية، وتكون هذه الأخيرة إما وسيلة أو هدفا من قبل المجرمين[3]، وقد تعرف بأنها:" كل سلوك غير مشروع يرتكب عن طريق شبكة الإنترنت"[4].

وهناك من يعرّفها[5] :"تلك الجرائم التي لا تعرف الحدود الجغرافية، والتي يتم ارتكابها بأداة هي الحاسب الآلي[6]، عن طريق شبكة الإنترنت[7]، وبواسطة شخص على دراية فائقة بها"، كما تعرف بأنها:

1- Michel Vivant, Droit de l'informatique et de réseaux, Lamy, 2001, P183.

نقلا عن : أ. نهلا عبد القادر المومني ، المرجع السابق، ص 49.

2- أ. نهلا عبد القادر المومني، المرجع السابق، ص49.

3 -Internet, comment prévenir et réprimer la cybercriminalité, le 10/07/2014, disponible à l'adresse suivante : www.vie-publique.fr.

4 - La cybercriminalité, disponible à l'adresse suivante : www.interieur.gouv.fr.

5- د. عادل عبد الجواد محمد،إجرام الإنترنت، مجلة الأمن والحياة ، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، العدد 221، ديسمبر سنة 2000، ص70.

6- يعرّف الحاسب لغة بأنّ مصدره الفعل (حسب) أو نحوه، وعلم الحاسب هو علم الأعداد وهي من العدد والتدبير الدقيق، وتعني كلمة الحاسب بالإنجليزية (Computer) ، وقد تعددت الترجمات العربية لهذه الكلمة فأطلق عليها الحاسوب، كما أطلق عليها العقل الإلكتروني، ثم أخيرا أطلق عليها الحاسب، وكلمة (Computer) يقابلها في اللغة الفرنسية (Ordinateur) أي ناظمة آلية، انظر في ذلك :د.أحمد خليفة الملط، المرجع السابق، ص 15، عن المعجم الوجيز، معجم اللغة العربية، وزارة التربية والتعليم، سنة 1995، ص17.

- أمّا التعريف الإصطلاحي فهو جهاز آلي أو آلة تتولى معالجة المعطيات المخزونة في الذاكرة الرئيسية في صيغة معلومات تحت إشراف برنامج مخزون سلفا في الجهاز- ويمكن إعتبار الكمبيوتر آلة حاسبة إلكترونية تستقبل البيانات ثم تقوم عن طريق الإستعانة ببرنامج معين بعملية تشغيل هذه البيانات للوصول إلى النتائج المطلوبة. أنظر في ذلك: د. عبد الفتاح مراد، المرجع السابق، ص18.

7- يجب عدم الخلط بين الإنترنت Internet ونظام الإنترانت Intranetالتي تعني إستخدام التكنولوجيا وبروتوكولات الإنترنت في وسط مغلق، مثال ذلك: المنشأة التي تقيم شبكة للربط بين فروعها المختلفة، باستخدام تقنية تصميم صفحات الإنترنت، حيث يتم وضع لوائح العمل بالشركة أو أسعار بيع منتجاتها أو التطبيقات الخاصة بها، لكي يستفيد منها موظفو البيع أو أي بيانات أخرى تريد المنشأة إطلاع موظّفيها عليها، ولا يمكن لأي شخص خارجها الإطلاع على تلك الصفحات. أنظر في ذلك: د.جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2013، ص3.

ولقد إختلفت التسميات التي أطلقت على الإنترنت، مابين "الشبكة العالمية" أو "الشبكة العنكبوتية" أو "الطريق السريع الرقمي"، والإنترنت لغة، هي كلمة جديدة ، وهي كلمة إنجليزية ومختصرة من مقطعين (Inter) وهي اختصار كلمة (International) وتعني دولي، و (Net) وهي اختصار لكلمة (Network)والتي تعني الشبكة. وبجمع الكلمتين أي (Inter Network) ، فإن المعنى المتحصل عليه هو الشبكة الدولية. ويمكن تعريف الإنترنت بأنها: "عبارة عن وسيط ناقل للمعلومات بين أجهزة الكمبيوتر المتصلة به، بواسطة أنظمة تحكم في البيانات و بروتوكولات و عناوين خاصة، حيث يتصل مستخدموها عن طريق جهاز الحاسب الآلي الشخصي بواسطة الخط الهاتفي، ومحول الإشارات، الذي يقوم بتحويل الإشارات الرقمية ونقل الرسالة بين المرسل والمستقبل مرورا

"نشاط غير قانوني وغير لائق يتم من خلال الفضاء الإلكتروني عن طريق استخدام أجهزة الكمبيوتر و شبكة الإتصالات"[1]،كما تعرف بأنها: "جميع الجرائم التي قد ترتكب في أو من خلال نظام كمبيوتر متصل بشبكة الإنترنت"[2]،ويقصد بها كذلك : "مجموعة من الجرائم المرتكبة من قبل مجرمين يستخدمون أنظمة الكمبيوتر والشبكات في جرائمهم وذلك إمّا لتطوير أو تسهيل الجرائم التي كانت موجودة قبل ظهور الإنترنت"[3]، أو هي:" مجموعة من الأنشطة المخالفة للقانون والمرتبطة بتكنولوجيا الإتصال الحديثة"[4]، إلا أن هذه الخاصية الأخيرة للجرائم الإلكترونية التي تنطوي على استخدام الوسائط الرقمية والتكنولوجيا الحديثة، استدعت الإستعانة بمجرمي المعلوماتية في الكثير من الأحيان[5].

غير أن بعض الفقهاء يرون أن هذه التعريفات تتسم في بعض الحالات بنوع من الشمولية المطلوبة، فليس بمجرد اشتراك الحاسب الآلي أو الإنترنت في الجريمة نصبغ عليها وصف الجريمة الإلكترونية لأنه يوجد بعض الجرائم التي تستهدف الكيانات المادية والأجهزة التقنية أي يمكن أن تشتمل على أنشطة إجرامية تقليدية مثل: السرقة والغش والتزوير، وتلك الجرائم تخضع للنصوص التقليدية لأن الإعتداء فيها يقع على مال مادي منقول، وليس على كيانات منطقية من برامج ومعطيات، كما أنّ هناك من التعريفات من وضعت حدودا فاصلة بين جرائم الكمبيوتر والإنترنت، إلاّ أنّ هذا التمييز غير دقيق، بل مخالف للمفاهيم التقنية،وللمراحل التي توصّل إليها تطوّر وسائل تقنية المعلومات في الدمج بين وسائل الحوسبة والإتصال، فهناك مفهوم عام لنظام الكمبيوتر حيث يستوعب كافة المكونات المادية والمعنوية المتصلة بعمليات الإدخال والمعالجة والتخزين والتبادل، ممّا يجعل الشبكات وارتباط الكمبيوتر بالإنترنت ينطلق من فكرة واحدة وهي تكاملية النظام[6].

إلاّ أنّ البعض[7] يراعي عند تعريف الجريمة الإلكترونية إعتبارات هامة وهي:

1. أن يكون هذا التعريف مقبول ومفهوم على المستوى العالمي.

بالخادم". أنظر في ذلك: د. علي بن عبد الله العسيري، الآثار الأمنية لاستخدام الشباب للإنترنت، بحث مقدم لجامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، سنة 2004، ص 14.

[1]- Solange Ghernaouti – Hélie, Comment lutter contre la cybercriminalité ? Mai 2010, disponible à l'adresse suivante : www.pourlascience.fr

[2] -Erwan Coatnoan De Kerdu, la cybercriminalité pour les entreprises, le 07/03/2014, disponible à l'adresse suivante : www.dynamique-mag.com.

[3]- Nathalie Bismuth, les perspectives pénales de la loppsi 2 en matiére de cybercriminalité, le 10/02/2010, disponible à l'adresse suivante : www.e-juristes.org.

[4]- Daguet Julie et Foubert Charlotte, qu'est-ce que la cybercriminalité ?, le 18/03/2014, disponible à l'adresse suivante :www.causes-cybercriminalité-over-blog.com

[5]- Voir : Gilbert Kallenborn, La cybercriminalité, main dans la main avec le crime organisé, le 16/01/2014, disponible à l'adresse suivante : www.01net.com.

[6] – أ. عائشة بن قارة، المرجع السابق، ص 33.

7– د. نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، لبنان، بدون طبعة، سنة 2005، ص32.

2. أن يراعى في وضع التعريف التطور السريع والمتلاحق لتكنولوجيا المعلومات والإتصالات.

3. أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر لإتمام النشاط الإجرامي[1].

البند الثاني: التعريفات التشريعية للجريمة الإلكترونية.

بداية لابد من الإشارة إلى أن مدونة الأمم المتحدة بشأن الجرائم الإلكترونية، تطرقت إلى الخلاف الواقع بين الخبراء حول ماهية تعريف الجرائم الإلكترونية، و حتى العناصر المكونة لها، و لعل ذلك يفسر عدم التوصل حتى الآن لتعريف متفق عليه دوليا لهذه المصطلحات، و إن اتفقوا ضمنا على وجود ظاهرة تتزايد بمعدلات عالمية لتلك الجرائم[2].

وقد تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفا للجرائم الإلكترونية[3]حيث عرفها بأنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".

ويبدو أن هذا التعريف هو الأقرب للصواب، لأنه حاول الإحاطة بجميع الأشكال الإجرامية للجريمة الإلكترونية، سواء تلك التي قد تقع بواسطة النظام المعلوماتي أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما شمل التعريف جميع الجرائم التي من الممكن أن تقع في بيئة إلكترونية، فهذا التعريف لم يركز على فاعل الجريمة، ولا على مقدرته التقنية، ولا على وسيلة إرتكاب الجريمة، أو على الغاية أو النتيجة التي تسعى لها الجريمة الإلكترونية، كما أنّه يعبّر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، كما أنه يتيح إمكانية التعامل مع التطورات التقنية المستقبلية[4].

كما يتبين أنّ الإتفاقية الأوروبية بشأن الجرائم الإلكترونية التي عقدت في بودابست سنة2001[5] تعتبر تعتبر أنّ مصطلح الجرائم الإلكترونية يتناول النشاطات غير القانونية أو غير المشروعة المرتبطة بأجهزة

---

[1]– د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 75.

[2]– د. هلال بن محمد بن حارب البوسعيدي ، المرجع السابق، ص 20.

3– مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد في فينا في الفترة الممتدة من 10-17 أفريل سنة 2000، انظر في ذلك: أ.نهلا عبد القادر المومني، المرجع السابق، ص50.

[4]– نفس المرجع، ص 50.

[5]– تم التوقيع على اتفاقية بودابست بشأن الجرائم الإلكترونية في 2001/11/23 في بودابست (المجر)، من قبل 30 دولة أوروبية، بالإضافة إلى الدول الأربعة من غير الأعضاء في المجلس الأوروبي وهي كندا، اليابان، جنوب إفريقيا والولايات المتحدة الأمريكية.

Voir : le droit d'internet, le 03/11/2011, disponible à l'adresse suivante : www.ladocumentationfrancaise.fr.

الكمبيوتر باستخدام شبكة الإنترنت، وقد صنفت هذه الجرائم إلى أربعة أنواع : الجرائم ضد سلامة المعلومات وخصوصيتها، الجرائم ذات الصلة بالكمبيوتر، الجرائم المتعلقة بمحتوى الكمبيوتر، الجرائم التي تتعلق بالعلامات التجارية والملكية الفكرية.

إلاّ أنّ هناك جانبا من التشريعات التي أشارت إلى تعريف الجريمة الإلكترونية، رغم أن الأصل كما هو متعارف عليه أنّ المشرع لا يعرف الجريمة لأنّ ذلك ليس من اختصاصه بل من اختصاص الفقه والقضاء، غير أنه قد يجد نفسه مضطرا لذلك إمّا لتحديد أركان الجريمة أو تحديد السلوك الإجرامي المستحدث للجريمة[1]، ومن بين هذه القوانين نذكر: القانون الجزائري، القانون السعودي، القانون الأمريكي.

أولا: القانون الجزائري.

بالرجوع إلى القانون رقم (09-04) السالف ذكره الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، فقد عرّفها بأنها:"جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية"[2].

ثانيا: تعريف القانون السعودي.

تضمّن نظام مكافحة الجرائم الإلكترونية السعودي الصادر بمقتضى المرسوم الملكي رقم(17)[3]تعريف الجريمة الإلكترونية بأنها:"أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".

ثالثا: تعريف القانون الأمريكي.

نص القانون الأمريكي رقم (1213) لسنة 1986 الخاص بمواجهة جرائم الكمبيوتر على تعريف الجريمة الإلكترونية بأنها:" الإستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات،وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة"[4].

---

[1]- د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الإتفاقيات والمواثيق الدولية، دار النهضة العربية، القاهرة، مصر، ط1، سنة 2011، ص 25.

[2]- المادة (02 فقرة أ) من القانون رقم 09-04 السالف الذكر.

3- المادة (01) من نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم 17 المؤرخ في 1428/03/07 هـ .

4- نقلا عن :د. رامي متولي القاضي، المرجع السابق، ص 26.

ومن الملاحظ من خلال هذه التعريفات المعطاة للجريمة الإلكترونية، أن المعيار المناسب في تعريف الجرائم الإلكترونية هو معيار دور نظام الحاسب الآلي في ارتكابها، وبالرغم من ذلك فإن هذا المعيار ليس مطلقا في انضباطه، لكنه الأكثر قبولا، فالأدوار التي يقوم بها الحاسب الآلي تتمثل في كونه إما وسيلة لارتكاب الجريمة أو هدفا لها أو بيئة رقمية لهذه الجرائم، و بإمكان نظام الحاسب لعب الأدوار الثلاثة معا[1].

البند الثالث: التمييز بين جرائم الحاسب الآلي وجرائم الإنترنت.

بالرغم من أن التمييز بين جريمة الإنترنت وجريمة الحاسب الآلي غير دقيق نتيجة الدمج بين وسائل الحوسبة والإتصال، إلا أن هناك من يميز بين هاتين الجريمتين وذلك على النحو التالي:

أولا: أوجه التشابه.

- تعد جريمة الإنترنت وجريمة الحاسب الآلي من الجرائم الخطيرة ذات الآثار الوخيمة، فهما من ذات صنف الجرائم التقنية الحديثة، وقد تتعدى نتائج أي منهما المستوى الشخصي لفرد إلى مستوى منظمة أو هيئة أو كيان إقتصادي أو سياسي[2]، فهذه الهجمات الإلكترونية لها عواقب وخيمة حيث تكلف في المتوسط 2.2 مليون أورو للشركات وفقا لمعهد Ponemon المتخصص في مجال البحوث حول أمن الكمبيوتر[3].
- المجرم المعلوماتي في كلا منهما يتمتع بصفات وسمات عالية وهو يختلف بذلك عن المجرم التقليدي وهو ذو دراية وعلم ومعرفة متقدمة بالأنظمة المشغلة لكليهما، سواء الإنترنت أو الحاسوب.
- كما تشترك جرائم الإنترنت وجرائم الحاسب الآلي في صعوبة الإكتشاف واتباع ذات طرق الإثبات الجزائي لضبط الفاعل.
- كلا من الجريمتين تعتمدان على الحاسب الآلي في ارتكابهما[4].

---

[1]– أ. سمير بردال، جرائم نظام الحاسب الآلي، مذكرة ماجستير، معهد الحقوق،المركز الجامعي مصطفى اسطمبولي، معسكر، سنة 2008، ص 21.

[2]– د. طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 163.

[3]- Christine Lejoux, la cybercriminalité, un business à 1000 milliards, le 01/07/2011, disponible à l'adresse suivante : www.latribune.fr.

[4]– د.طارق إبراهيم الدسوقي عطية، المرجع السابق، ص163.

ثانيا : أوجه الإختلاف.

- تاريخيا أرجع الفقه الجنائي ظهور جرائم الحاسب الآلي إلى عام 1960[1]، أمّا جرائم الإنترنت فيرجعها إلى العام الذي أفاق فيه العالم على دودة موريس سنة 1988[2]، والتي كانت سببا في تعديل التشريع الفيدرالي الأمريكي، كما أنّ جريمة الحاسب يمكن أن تتم دون الحاجة إلى الإرتباط بشبكة الإنترنت، مثل توظيف الحاسبات وملحقاتها في جرائم التزوير والتزييف أو سرقة المعلومات وتدميرها، أمّا جريمة الإنترنت فشرطها الأساسي وجود حاسب آلي متصل بالإنترنت لإتمام أركانها.
- يختلف مجرم الإنترنت عن مجرم الحاسب الآلي في كونه مجرما لا يتمتع بمؤهلات علمية أو تخصصية ذات طابع أكاديمي، وإنما هو يملك تقنية الإنترنت دون حاجة لأن يكون دارسا لها، كما أنّ الإنترنت يحكمه قانون الإنترنت الذي يعتبر فرع جديد من فروع القانون وهو يجمع في علاقة واحدة مباشرة بين معالجة البيانات والمعلوماتية وبين خدمات الإتصال[3].

---

[1]– منذ شيوع إستخدام الكمبيوتر في سنة 1960 إلى غاية 1970، ظهرت أوّل معالجات لما يسمى جرائم الكمبيوتر، واقتصرت المعالجة على مقالات ومواد صحفية وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي والإستخدام الغير المشروع للبيانات المخزنة في نظم الكمبيوتر، ومع تزايد استخدام الحواسيب الشخصية في منتصف السبعينات ظهرت العديد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر، وبدأ الحديث عنها بوصفها ظاهرة إجرامية.

وفي عام 1980 طفا على السطح مفهوم جديد لجرائم الكمبيوتر إرتبط بعمليات اقتحام نظم الكمبيوتر عن بعد وأنشطة نشر و زراعة الفيروسات الإلكترونية، التي تقوم بعمليات لتدمير الملفات أو البرامج، وشاع إصطلاح (الهاكرز) المعبر عن مقتحمي النظم، فجرائم الإنترنت ظهرت في حقل جرائم التقنية العالية في نهاية الثمانينات، و كان ذلك من خلال جريمة (دودة موريس)، وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض جرمية خطيرة.

كما شهدت سنة 1990 تناميا هائلا في حقل الجرائم التقنية وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات، ففي عام 1996 ظهرت هجمات ومن بينها: قضية الجحيم العالمي التي تعامل معها مكتب التحقيقات الفيدرالي، حيث تمكنت هذه المجموعة من اختراق موقع البيت الأبيض و الجيش الأمريكي، وكذلك فيروس ميلسا، وهو فيروس شرس أطلق من قبل مبرمج كمبيوتر اتهم باختراق إتصالات عامة، وحادثة شركة "أوميغا" حيث تمكن مصمم ومبرمج من إطلاق قنبلة إلكترونية بعد 20 يوما من فصله من ذات الشركة، ناهيك عن جرائم أخرى شهدتها هذه المرحلة.

أنظر في ذلك: عبد الفتاح مراد، المرجع السابق، ص38، أ. عبد الله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني، بدون تاريخ، ص8 على الموقع: www.minchaui.com ، د.محمود صالح العادلي، الفراغ التشريعي في مجال مكافحة الجرائم الإلكترونية، بدون تاريخ، ص3 على الموقع: online.comwww.echourouk

[2]–أطلق في عام 1988 عبر شبكة الإنترنت في الولايات المتحدة الأمريكية برنامج يعرف بالدودة (Worm)، والذي سبب لأجهزة الحاسب الآلي إنهيار في قيادة وتوجيه الجامعات والمعدات العسكرية ومنشآت الأبحاث الطبية، وتهدف هذه البرامج إلى العمل على تقليل خفض كفاءة الشبكة أو إلى التخريب الفعلي للملفات والبرامج ونظم التشغيل، وذلك بإشغال أي حيز ممكن من سعة الشبكة.

وقد أطلقت دودة الإنترنت عن طريق طالب أمريكي يدعى (Robert Morris) وهو طالب في قسم علوم الكمبيوتر بجامعة كورنيل بولاية نيويورك، تعمد بث برامج دورة الإنترنت، لكي يثبت عدم ملاءمة وسائل الأمان في شبكات الكمبيوتر، ولكنه تسبب في تدمير الآلاف من شبكات الحاسب الآلي المنتشرة في الولايات المتحدة، بالإضافة إلى إعاقة طريق ومسلك الشبكات وخسائر مالية كبيرة في مواجهة دودة الإنترنت. وقد أدين (موريس) بانتهاك قانون الإحتيال وإساءة إستخدام الكمبيوتر، وحكم عليه بالحبس لمدة ثلاث سنوات، وبالعمل (400) ساعة في الخدمة الاجتماعية، وغرامة قدرها (10.500) دولار، بالإضافة إلى تكاليف المراقبة.أنظر في ذلكأ. محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، عمان، الأردن، بدون طبعة، سنة 2004، ص 239، ص240.

[3]–د. طارق إبراهيم الدسوقي ، المرجع السابق، ص 164. للإشارة هناك بعض الفقه يقرون بوجود فرع جديد من فروع القانون يسمى قانون الإنترنت، أنظر :
Vincent Fauchoux et Pierre Deprez, Le droit de l’internet : Lois, contrats et usages, Litec,, France, 2009, P4.

الفرع الثاني: خصائص الجريمة الإلكترونية.

إنّ إرتباط الجريمة الإلكترونية بجهاز الحاسب الآلي وشبكة الإنترنت، أضفى عليها مجموعة من الخصائص والسمات، فهي جرائم ذات خصائص متفردة خاصة بها لا تتوافر في أي من الجرائم التقليدية في أسلوبها وطريقة ارتكابها[1]، فهذا النوع من الجرائم نتيجة حتمية لكل تطور علمي أو تقني، و يستمد نشاطه من القدرات الهائلة للحاسب الآلي[2]. ولعل من أبرز خصائصها ما يلي:

أولا: طابع التقنية.

تتسم الجريمة الإلكترونية بخاصية مميزة، تتمثل في ارتكاب هذه الجريمة بواسطة أجهزة الحاسب الآلي، غير أن هناك من الجرائم التي ترتكب عبر شبكة الإنترنت، وإن كان هناك إرتباط بين الحاسب الآلي وشبكة الإنترنت أثناء ارتكاب الجريمة،وهذا ما يجعلها تتميز بخصائص معينة بالمقارنة مع الجرائم العادية، وهذا الإرتباط الوثيق بين جرائم الحاسب الآلي وجرائم الإنترنت جعل من هذه الجرائم تتخذ شكلا جديدا ولعل أهم ما يميزها هو صعوبة اكتشافها وضخامة الخسائر المترتبة عنها، حيث أنّ ما كشف عنه "إدوارد سنودن"[3] قد أضرّ بسمعة الشركات العملاقة مثل: غوغل، ميكروسوفت التي أحرجت من قبل مستخدمي الإنترنت الذين شعروا بعدم الثقة[4].

ثانيا: إزدواجية محل الجريمة.

نظرا لأنّ النظام المعلوماتي ذاته ليس من طبيعة واحدة، فهو يتكون من عناصر مادية وأخرى غير مادية، بما يسمح بإمكانية أن يكون موضوع الجريمة ذو طبيعتين مختلفتين أحدهما يتمثل في الجانب المادي، والآخر في الجانب غير المادي، وذلك ليس على مكونات النظام ذاته، بل يشمل ظهور المحل الواحد بمظهرين أحدهما مادي والآخر غير مادي كما هو الحال بالنسبة للمعلومات، فقد تكون في حالة انتقال أو موجودة في ذاكرة النظام المعلوماتي، أي أنها في حالة غير مادية أو تكون تلك المعلومات مجسدة في صورة مادية بتخزينها على دعامة إلكترونية[5].

---

[1]– أ. منير محمد الجنبيهي و أ. ممدوح محمد الجنبيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2006، ص 48.

[2]– أ. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، بدون طبعة، سنة 2005، ص 05.

[3]– إدوارد جوزيف سنودن هو أمريكي، وكان متعاقد تقني وعميل موظف لدى وكالة المخابرات المركزية، وقد قام بتسريب مواد مصنفة على أنها سرية للغاية من وكالة الأمن القومي منها برنامج التجسس بريسم إلى صحيفة الغارديان وصحيفة الواشنطن بوست، حيث وجه له القضاء الأمريكي رسميا تهمة التجسس وسرقة ممتلكات حكومية ونقل معلومات تتعلق بالدفاع الوطني دون إذن.أنظر الموقع الإلكتروني:www.wikipedia.org

[4]- Camille Studer, Les géants du Web et la cybercriminalité, le 30/06/2014, disponible à l'adresse suivante : www.infoguerre.fr.

[5]– د. طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 167.

كما أنّ المعلومات بطبيعتها غير المادية، يمكن أن تخضع لأكثر من نص قانوني، وفقا لما إذا كانت في شكل مادي أو غير مادي، وفي الشكل الأخير يوجد لها أكثر من نص قانوني يمكن أن تخضع له، مثال ذلك إعتبارها مصنّف أدبي مما يثير مشكلة تعدد الأوصاف القانونية على ذات المحل[1].

ثالثا: موضوع الجريمة الإلكترونية بالنسبة لمراحل تشغيل نظام المعالجة الآلية للمعطيات.

بالرغم من إمكانية ارتكاب الجريمة الإلكترونية أثناء أية مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للمعطيات (الإدخال-المعالجة-الإخراج)، فإن لكل مرحلة منها نوعية خاصة من الجرائم لا يمكن –بالنظر إلى طبيعتها- إرتكابها إلاّ في وقت محدد يعتبر بالنسبة لمراحل التشغيل الأمثل لذلك[2]، إلاّ أنّ اتفاقية بودابست جمعتها في مراحل محددة تشمل الجريمة الإلكترونية بشكل يجمع مختلف صور الإعتداء على المعلومات وهي متعلقة بالبيانات الموجودة على الحاسب الآلي، فهي تحدد أن الجريمة الإلكترونية تبدأ بالولوج غير القانوني سواء كان على الحاسب الآلي أو على جزء منه وبأي غرض كان ، وتقرر المذكرة التفسيرية أن الهدف من تحديد أركان الجريمة الإلكترونية هو حماية أمن وسرية وسلامة البيانات المخزنة على الحاسب الآلي للحدّ من تكاليف إصلاح هذا الإعتداء ومشاكله.

وقد قررت إتفاقية بودابست أنّ الإعتراض الغير قانوني لبرامج الحاسب الآلي بنيّة إرسال معلومات أو تخريبها هو مضمون حماية للحرية في نقل البيانات،وحماية حرية التواصل بين مختلف أجهزة الحاسب الآلي، وقد حددت المذكرة أنّ الإعتراض غير القانوني يتم بالحصول على بيانات بطريقة غير قانونية،وحددت فكرة نقل البيانات الغير معلنة موضحة أن فكرة عدم العلانية تعود على الأسلوب المتبع في نقل البيانات وليس البيانات نفسها، كما تعرضت إلى الإعتداء على سلامة البيانات المخزنة على الحاسب الآلي بالمحو والطمس والإتلاف، سواء بإدخال بيانات خاطئة أو برامج مضادة للبرامج الموجودة على الحاسب الآلي كالفيروسات مثلا[3].

رابعا: الجريمة الإلكترونية جريمة عابرة للحدود.

المجتمع المعلوماتي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان، فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات

---

[1]– د.طارق إبراهيم الدسوقي عطية، المرجع السابق، ص167.

[2]– نفس المرجع، ص 167.

[3]– أ. ناير نبيل عمر ، الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2012، ص25.

عبر الدول المختلفة، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة، بينما يتحقق الفعل الإجرامي في دولة أخرى[1]، فهي جريمة وطنية عندما تقع كاملة في نطاق إقليم دولة معينة، وتكون جريمة دولية [2] عندما تتعلق بالقانون الدولي، أي عندما يكون أحد أطرافها شخصا دوليا، وقد تكون جريمة ذات بعد دولي، إذا اتفق المجتمع الدولي بمقتضى إتفاقية دولية بأن جريمة معينة تشكل عدوانا على كل دولة، أو عندما ترتكب الجريمة داخل دولة معينة، إلا أنها تمتد خارج إقليم تلك الدولة مثل جريمة ترويج المخدرات عبر الإنترنت[3].

كما أن عالمية الجريمة الإلكترونية تظهر بصفة خاصة في مجال البنوك، حيث أدى التوسّع الكبير في إجراء المعاملات البنكية عبر شبكات المعلومات الدولية إلى إعطاء بعد دولي لجرائم الإحتيال المعلوماتي بصفة خاصة، حيث أدّى ربط وسائل الإتصالات بالحاسبات الآلية إلى مضاعفة المعاملات المالية الدولية التي تتم بوسائل إلكترونية، وبصفة خاصة من خلال التحويل الإلكتروني للأموال والتبادل الإلكتروني للمعلومات، أمّا فيما يتعلق بالإتلاف المعلوماتي، فإعداد أحد البرامج الخبيثة (الفيروسات) [4] يمكن أن يتمّ في دولة ما، ثم يتم

1- د. محمد علي محمد عبيد المحوث الحمودي، دور مأمور الضبط القضائي في مواجهة جرائم المعلومات، مذكرة ماجستير، كلية الحقوق، جامعة القاهرة، مصر، سنة 2009، ص 243.

2- الجريمة الدولية هي تلك الجريمة التي يكون أحد أطرافها شخصا دوليا كالدولة والمؤسسات ذات الطابع الدولي وترتكب أفعالا غير مشروعة تصنف على أنها جرائم .أنظر في ذلك: د.عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن إستخدام الإنترنت، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2004، ص190. كما تعرّف بأنها: "كل سلوك يصدر عن فرد باسم الدولة أو برضاء منها عن طريق إرادة إجرامية يترتب عليه المساس بمصلحة دولية، تكون هذه الأخيرة مشمولة بحماية القانون الدولي ". انظر في ذلك: د. محمود صالح العادلي، الجريمة الدولية (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2003، ص69.

3- د. محمد طارق عبد الرؤوف الخن، جريمة الإحتيال عبر الإنترنت (الأحكام الموضوعية والأحكام الإجرائية)، منشورات الحلبي الحقوقية، سوريا، ط1، سنة 2011، ص 34.

4- الفيروسات هي برنامج كمبيوتر صمّم لإصابة برامج أخرى، ينسخ من نفسه، ويعتقد خبراء أوروبيون إنتشار فيروسات أكثر عدوانية مما يؤدي إلى زيادة الجماعات الإجرامية وتطوير أساليبها. أنظر في ذلك:

Jean pierre Stroobants, cybercriminalité : la commission européenne multiplie les actions , le 10/02/2014, disponible à l'adresse suivante : www.lemonde.fr.

وقد عرّفها أحد خبراء الفيروسات بأنها نوع من البرامج التي تؤثر في البرامج الأخرى، بحيث تعدل في تلك البرامج لتصبح نسخة منها، وهذا يعني ببساطة أن الفيروس ينسخ نفسه من حاسب آلي إلى آخر بحيث يتكاثر بأعداد كبيرة. أنظر في ذلك: أ. محمد عبد الله منشاوي ، جرائم الإنترنت في المجتمع السعودي ، بدون تاريخ، بحث منشور على الموقع التالي :http :// Minchaoui.com

ويتميز فيروس الحاسب بعدة خصائص أهمها :

أ. العدوى: فهو برنامج يتم تسجيله أو زرعه على الأقراص أو الأسطوانات الخاصة بالحاسب وعند تحميل البرنامج ينتقل الفيروس من جهاز إلى آخر بسرعة فائقة، وينتشر داخل الذاكرة وينسخ نفسه بسرعة غير عادية.

ب. الإختفاء: فيروس الحاسب هو برنامج يتميز بقدرة الإرتباط بالبرامج الأخرى والتخفي من مستخدم الجهاز والتمويه عليه كالدخول في ملفات مخفية أو موضع الذاكرة، ويظل في هذا المكان حتى توقيت أو إشارة معينة، فيقوم بتشغيل نفسه ونشاطه التدميري.

ت. هي مكلفة ماديا: بحيث تكبّد الشركات التجارية في الولايات المتحدة الأمريكية على سبيل المثال ما قيمته بليون دولار سنويا بسبب الأضرار التي تسببها.

نسخ هذا البرنامج مرّات عديدة ويرسل إلى دول متفرقة من العالم[1]، خاصة مع تميز المجرمين في هذه النوعية من الجرائم بأنهم أكثر تنظيما وأكثر وعيا ومهارة بتكنولوجيا المعلومات والإتصالات[2]، كما أصبحوا مصدر قلق كبير للشركات وعملائها في ظل انتشار الإعتداءات على المواقع التجارية[3].

فالجريمة الإلكترونية هي نوع من الجرائم التي يتم ارتكابها عن بعد عبر المسافات، حيث لا يتواجد الفاعل على مسرح الجريمة، بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة، ومن تمّ تتباعد المسافات بين الفعل الذي يتمّ من خلال جهاز حاسوب الفاعل، وبين النتيجة أي المعطيات محل الإعتداء وبالتالي لا تقف الجريمة الإلكترونية عند الحدود الإقليمية لدولة معينة، بل تمتد إلى الحدود الإقليمية لدولة أخرى مما يزيد من صعوبة اكتشافها[4].

خامسا: عدم وجود جهة مسيطرة على مدخلاتها ولا على مخرجاتها.

بمعنى لا توجد جهة مركزية موحدة،أو حتى مجموعة من الجهات المترابطة تتحكم فيما يعرض على شبكة الإنترنت، بل يمكن لأي شخص وضع ما يريده على الشبكة،وكل ما تملكه الجهات التي تحاول فرض رقابة على الإنترنت، أن تقوم بمنع الوصول إلى موقعه، أو إذا كان لها قوة فربما تقوم بإغلاقه أو تدميره بعد أن يكون قد نشر ما يريد، ويمكنه بأقل جهد أن ينتقل إلى موقع آخر[5]، حيث أصبح قراصنة الإنترنت يعتبرون

ث. التدمير: أهم أعراض الإصابة بالفيروس بطء تشغيل النظام الإلكتروني، ثم يقوم بمسح البيانات المخزنة على وسائط التخزين، ويؤدي إلى شغل ذاكرة الجهاز على نحو يتعذر معه التعامل مع البيانات المخزنة على وسائل التخزين، ويؤدي إلى شغل ذاكرة الجهاز على نحو يتعذر معه التعامل مع البيانات أو المعلومات وتتوقف الإستجابة لنظام التشغيل ويؤدي الفيروس إلى التشويش على المعلومات وإدخال أخرى خاطئة.

ج. الإختراق: يتمتع الفيروس بقدرة فائقة على دخول النظام والتسلل إليه واختراق كل سبل الحماية التي يضعها المستخدم. أنظر في ذلك: د.محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2007، ص 243 وما بعدها. وكذلك : د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، كتاب 2، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2004، ص 90.

[1]– كانت القضية المعروفة باسم مرض نقص المناعة المكتسبة (الإيدز) من القضايا التي لفتت النظر إلى البعد الدولي للجرائم الإلكترونية، وتتلخص وقائع هذه القضية التي حدثت عام 1989 في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي هدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة) إذ كان يترتب على تشغيله تعطيل الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل إلى عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس، وفي الثالث من فبراير 1990 تم إلقاء القبض على المتهم (جوزيف بوب) في أوهايو بالولايات المتحدة الأمريكية، وتقدمت المملكة المتحدة بطلب للقضاء الأمريكي لتسليم المتهم ومحاكمته أمام القضاء الإنجليزي، حيث أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة، ووافق القضاء الأمريكي على تسليم المتهم وتم توجيه إحدى عشر تهمة إبتزاز معظمها في دول مختلفة. أنظر في ذلك: د. نهلا عبد القادر المومني، المرجع السابق، ص 51.

[2]- Frédéric Gaudreau, Comité technique : Cybercriminalité, disponible à l’adresse suivante : www.francopol.org.

[3]- Damien Licata Caruso, Cybercriminalité : 72 % des sites français mal protégés contre le piratage, disponible à l’adresse suivante : www.leparisien.fr.

[4]– د. خالد ممدوح ابراهيم ، الجرائم المعلوماتية، المرجع السابق، ص77.

[5]– د. علي بن عبد الله العسيري، المرجع السابق، ص 69.

الإرهابيين الحقيقيين نتيجة للخسائر التي أصبح يكبدها هؤلاء للشركات والمؤسسات الكبرى في جميع أنحاء العالم، مع زيادة في معدلها بنحو 50% مقارنة بالعام الماضي[1].

لكن ينبغي الإشارة إلى أنه يوجد جهات ومنظمات فنية لتنظيم شؤون الشبكة، غير أن معظمها ذو طابع تطوعي، كمنظمة تسجيل أسماء وأرقام الإنترنت، منظمة تسجيل عناوين الإنترنت في أوربا، جمعية الإنترنت(ISCO) وفريق عمل هندسة الإنترنت، هذه الأخيرة التي تساهم في وضع مواصفات معايير الإنترنت وتقديم حلول للمشاكل التقنية في الإنترنت[2].

سادسا: صعوبة إكتشاف وإثبات الجريمة الإلكترونية.

تتصف الجريمة الإلكترونية بأنها صعبة الإثبات، لأن الهاكرز من الممكن أن يستعمل إسما غير حقيقيا، أو أن يرتكب جريمته من خلال إحدى مقاهي الإنترنت، وإن تم اكتشافها فإن ذلك يكون من قبيل الصدفة في غالب الأحيان[3]، ولذلك فإنه في كثير من الحالات يذهب مرتكب الجريمة الإلكترونية بدون عقاب[4].

ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة الإلكترونية ، إلى عدم ترك هذه الجريمة لأي أثر خارجي ، كما أنها جريمة عابرة للحدود كما سبقت الإشارة إلى ذلك، كما أن القدرة على تدمير أدلة الإدانة في ثوان معدودة يشكل عاملا إضافيا في صعوبة إكتشاف هذا النوع من الجرائم، إضافة إلى ارتكابها في بيئة افتراضية[5].

فالجرائم الإلكترونية في أكثر صورها خفية لا يلحظها المجني عليه، أو لا يدري حتى بوقوعها والإمعان في حجم السلوك المكون لها،وإخفائه عن طرق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها،أمرا ليس عسيرا في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبيها[6].

كما أنّ المجني عليه يلعب دورا رئيسيا وهاما في صعوبة إكتشاف وقوع الجريمة الإلكترونية، بحيث تحرص أكبر الجهات التي تتعرض أنظمتها المعلوماتية للإنتهاك أو تمنى بخسائر فادحة من جراء ذلك على عــدم

---

[1]- Combien coûte la cybercriminalité ?, le 16/06/2014, disponible à l'adresse suivante : www.lemondenumerique.com.

[2]–د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة ، مصر، ط 1، سنة 2009، ص27.

[3]– د.جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، مصر، ط1، سنة 1992، ص 17.

[4] - La cybercriminalité plus répandue en France qu'ailleurs, le 19/02/2014,disponible à l'adresse suivante : www.challenges.fr.

[5]– أ. نهلا عبد القادر المومني، المرجع السابق، ص 54.

[6]– د. هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، مصر، ط1، سنة 1974، ص 16. نقلا عن: أ.نهلا عبد القادر المومني، المرجع السابق، ص 54.

الكشف حتى بين موظفيها عما تعرضت له، وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها[1]، خاصة وأن المؤسسات والشركات وكافة الإدارات قامت بإنشاء مواقع تتعامل من خلالها عبر هذه الوسيلة التكنولوجية، على اعتبار أن الإنترنت علاوة على أنها وسيلة للإتصال و مصدر للمعلومات تستعمل أيضا كوسيلة لممارسة التجارة، فهي إختصار للمسافات وربح للوقت[2].

الفرع الثالث: محل الجريمة الإلكترونية.

إن الفضاء المفتوح المتمثل في الإنترنت ينطوي على مخاطر عديدة لأنه يسمح بممارسة الأنشطة غير المشروعة، والإنتشار السريع للفيروس وتدفق المعلومات عبر قنوات مشكوك فيها كالمواقع الإباحية، وبنفس الطريقة سمحت الإنترنت بتطوير الأنشطة التجارية، وتعددت العمليات الإلكترونية كأثر مترتب على الثورة المعلوماتية، بين تلك التي تتصل بعمليات التجارة الإلكترونية[3]وتلك التي تتعلق بعمليات التحويلات المالية

---

[1]– نهلا عبد القادر المومني، المرجع السابق، ص 54.

[2]- Nathalie Moreau, La formation du contrat électronique : Dispositif de protection du cyberconsommateur et modes alternatifs de règlement des conflits(M.A.R.C), mémoire DEA Droit des contrats, Faculté des Sciences Juridiques, Politiques et Sociales, Université de Lille 2,France, Année universitaire 2002/2003, p05.

[3]– ليس هناك تعريف محدد للتجارة الإلكترونية وذلك بسبب تعدد الجهات التي أوردت هذه التعريفات ومشروع الأمم المتحدة رغم تعلقه بالتجارة الإلكترونية إلا أنه لم يتضمن تعريفا لها، واكتفى المشروع بتعريف تبادل المعلومات الإلكترونية "والتي تشمل التجارة الإلكترونية وورد فيه أنها : " النقل الإلكتروني بين جهازين للكمبيوتر للبيانات باستخدام نظام متفق عليه لإعداد المعلومات." أنظر في ذلك: د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2001، ص 10.

وعرفها د . معوان مصطفى بأنها نظام يتيح عبر الإنترنت حركات بيع وشراء السلع والخدمات والمعلومات، كما يتيح دعم توليد العوائد مثل عمليات تعزيز الطلب على تلك السلع والخدمات والمعلومات، حيث إن التجارة الإلكترونية تتيح عبر الإنترنت عمليات دعم المبيعات وخدمة العملاء .

أنظر في ذلك : د . معوان مصطفى، الإثبات في المعاملات الإلكترونية في التشريعات الدولية، دار الكتاب الحديث، القاهرة، مصر، ط 1، سنة 2008، ص 23. كما تعرف على أنها : " كل معاملة تجارية تتم عن بعد، باستعمال وسيلة إلكترونية وذلك حتى إتمام العقد ".أنظر في ذلك : د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، ط1، سنة 2006، ص 57.

وللإشارة فإنه في 1998/11/18 قدمت اللجنة الأوروبية إقتراحا حول الجوانب القانونية للتجارة الإلكترونية في السوق الداخلية، وقد عرفها بعض الفقه الفرنسي بأنها : مجموعة من المعاملات التجارية التي يتم الشراء فيها عن طريق وسائل الإتصال، فهي صورة مستحدثة لطلب السلع والخدمات. أنظر في ذلك :
Santiago Cavanillas, Vincent Gautrais et autres, Commerce électronique, Delta, Bruxelles, 2001, p 37.

وتتميز التجارة الإلكترونية بعدد من الخصائص التي تميزها عن التجارة التقليدية منها:

أ. غياب العلاقة المباشرة بين الأطراف : بحيث لا يكون هناك مجلس العقد بالمعنى التقليدي.

ب. وجود الوسيط الإلكتروني: وهو جهاز الحاسب الآلي لدى كل من الطرفين المتعاقدين والمتصل بشبكة الإتصالات الدولية التي تقوم بنقل التعبير عن الإرادة لكل من الطرفين المتعاقدين في ذات اللحظة رغم تباعد المكان والمواطن.

ت. السرعة في إنجاز الأعمال: ذلك لأنه تنتفي العديد من الأوراق التي كانت تصاحب أوامر البيع والشراء أو شحن البضاعة.أنظر في ذلك: أ. منير محمد الجنبيهي، أ. ممدوح محمد الجنبيهي، الشركات الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة ، سنة 2005، ص11.

الإلكترونية [1]، وما يطلق عليه بالحكومة الإلكترونية[2] وأهم ما يميز هذه العمليات الإلكترونية أنها تتم في شبكة الإنترنت وبذلك فإنها تستفيد من تقنياتها التكنولوجية العالية ومع ذلك فقد بدأت تظهر الآثار السلبية للثورة التكنولوجية، متمثلة في الجريمة الإلكترونية[3] والتي تتميز بطبيعة خاصة، فمعظم حالات إرتكاب الجريمة تتم في مجال المعالجة الإلكترونية للبيانات وذلك بتجميع وتجهيز البيانات لإدخالها إلى الحاسب بغرض الحصول على معلومات مع توفير إمكانيات التصحيح والتعديل والمحو والتخزين والإسترجاع والطباعة، وهي عمليات وثيقة الصلة بارتكاب الجرائم كالتزوير أو النسخ مثلا.

غير أنه لابدّ من التمييز بين الإعتداء الذي يقع على الدعامة ويكون في هذه الحالة قد وقع على شيء مادي، مما يصلح تكييفه حسب النشاط الإجرامي بإحدى جرائم الأموال التي يتطابق نموذجها مع هذا النشاط وبين الإعتداء على المعلومات مستقلة عن الدعامة، حيث يكون قد وقع على شيء معنوي، هذا الشيء المعنوي لابدّ وأن تثبت له صفة المال أوّلا حتى يمكن البحث بعد ذلك في مدى إمكانية وقوع جرائم الأموال عليه[4]،وأصبح من المألوف استخدام شبكات المعلومات المحلية والإقليمية والعالمية بغرض الوصول للإستخدام الأمثل للمعلومات المتوفرة في تخصصات ومجالات معينة، وصار التحاور مع قواعد البيانات والتعامل مع نظم متقدمة الخبرة والذكاء الإصطناعي حقيقة واقعة، وأصبح العالم بذلك تترابط فيه النظم المعلوماتية[5] ومختلف شبكات الإتصالات، وتتلاشى فيه الحواجز الجغرافية والمسافات، وعبر هذه المنظومة تسري

---

[1]– تعرف التحويلات المالية الإلكترونية بأنها عبارة عن عملية منح الإختصاص والصلاحية لبنك معين للقيام بعمليات التحويلات المالية إلكترونيا من حساب بنكي إلى حساب بنكي آخر. أنظر في ذلك : د. سعد غالب التكريتي، د. بشير عباس العلاق، الأعمال الإلكترونية ، دار المناهج للنشر والتوزيع، عمان، الأردن، ط1، سنة 2002، ص 15.

[2]– لا يوجد تعريف محدد لمصطلح الحكومة الإلكترونية نظرا للأبعاد التقنية والإدارية والتجارية التي تؤثر عليها الحكومة الإلكترونية، فالأمم المتحدة عام 2002 عرّفت الحكومة الإلكترونية بأنها: "إستخدام الإنترنت والشبكة العالمية العريضة لإرسال معلومات وخدمات الحكومة للمواطنين، كما أنّ منظمة التعاون والتنمية في المجال الاقتصادي سنة 2003 عرفتها بأنها:"إستخدام تكنولوجيا المعلومات والإتصالات وخصوصا الإنترنت للوصول إلى حكومات أفضل". ويمكن القول أن هناك ثلاثة أبعاد لنشاطات الحكومة الإلكترونية في علاقاتها مع الغير، فهي علاقة الحكومة بالمواطن أي إتصال بين الحكومة والمواطن لتقديم معلومة أو خدمة عن طريق تكنولوجيا المعلومات من جهة ، وعلاقة الحكومة بالشركة أي إتصال بين الحكومة وشركة ما لتقديم معلومة أو خدمة عن طريق تكنولوجيا المعلومات من جهة ثانية، وكذلك علاقة الحكومة بالحكومة ذاتها أو بأخرى للإتصال بين موظف ودائرته الحكومية واتصال بين دائرة حكومية وأخرى للحصول على معلومة أو لتقديم معلومة أو خدمة عن طريق تكنولوجيا المعلومات. أنظر في ذلك: د. معوان مصطفى، الإثبات في المعاملات الإلكترونية في التشريعات الدولية، المرجع السابق، ص 25.

[3]– د.هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص 27.

[4]– أ. أمال قارة، المرجع السابق، ص 16.

5– تعرف النظم المعلوماتية بأنها: مجموعة من العناصر المتداخلة والمتفاعلة مع بعضها، والتي تعمل على جمع البيانات والمعلومات، ومعالجتها ، وتخزينها،وبثها وتوزيعها وذلك بغرض دعم صناعة القرارات، ويشتمل هذا النظام على بيانات عن الأشخاص الأساسيين والأماكن، وعموما فإن نظام المعلومات هو عبارة عن آلية وإجراءات منظمة، تسمح بتجميع وتصنيف وفرز البيانات ومعالجتها، ومن تم تحويلها إلى معلومات يسترجعها الإنسان عند الحاجة، ليتمكن من إنجاز عمل أو اتخاذ قرار أو القيـام بأية وظيفة تفـيد حركة المجتـمع، عن طريق المعرفة التي سيحصل عليها من المعـــلومات المسترجعة من النظام، وقد يتم

المعلومات، ويتم التعامل معها بصور مختلفة من إدخال معلومات،تخزينها،معالجتها، استرجاعها وتعديلها[1]،وبهذا تنعكس البيئة الرقمية على شكل ونوعية وأسلوب الجريمة المستحدثة[2]حتى أن البعض أصبح يخشى الإنتقال إلى العصر الرقمي وإن كان هذا التطور نتيجة حتمية.

أمّا بالنسبة لمحل الجريمة الإلكترونية فإنها تستهدف المعلومات، والتي هي في الحقيقة موضوع الجريمة ومحل الإعتداء، فهي أنماط السلوك الإجرامي التي تطال المعلومات وهي إمّا أن تجسد أو تمثل أصولا أو أموالا أو أسرارا أو بيانات شخصية أو لها قيمة بذاتها كالبرامج[3]، وهذه الطبيعة الخاصة جعلت من الضرورة البحث في مدى انطباق وصف المال على الكيان المعنوي للحاسب الآلي.

البند الأول: الرأي المؤيد لإضفاء وصف المال العام على الكيان المعنوي للحاسب.

مما لاشك فيه أن المكونات المادية للأنظمة المعلوماتية، والتي تتمثل في المعدات والأجهزة هي محل للحماية الجنائية، لأنها تكون موضوعا لجريمة مكتملة الأركان والعناصر، ومن أمثلة ذلك السرقة التي تقع على الكمبيوتر ذاته، أو الأسطوانات المخزن عليها البيانات،كما يمكن أن يكون هذا الجهاز محلا لجريمة النصب أو جريمة خيانة الأمانة، كما قد يكون محلا للإتلاف العمدي.

استرجاع المعلومات، في نظام المعلومات يدويا أو ميكانيكيا، أو إلكترونيا، وهذا الأخير هو الغالب في نظم المعلومات المعاصرة.أنظر في ذلك: د. سعود وصل الله سعد الثبيتي، الجريمة المعاصرة والإستخدامات السلبية للتقنية (جرائم الكمبيوتر والإنترنت)، بدون تاريخ ، ص 29، على الموقع التالي:www.aljareh.com.

كما يعرفها القانون رقم 09-04 السالف الذكر المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها في مادته الثانية (2) فقرة ب بأنها : "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

1- أ. خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر(أساليب وثغرات)، دار الهدى، عين مليلة، الجزائر، ط1، سنة 2010 ، ص 35.

2-الجريمة المستحدثة: يقصد بها أنواع من الجرائم لم تكن معروفة سابقا، وهي بذلك تختلف عن الجرائم التقليدية من حيث كيفية ارتكابها،وخصائص الجناة فيها، وتتم الإستعانة فيها بمعطيات العلم الحديث، أو التقنيات الحديثة من أجل طمس معالمها وعدم كشف مرتكبيها ، أنظر في ذلك، د. محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، بحث مقدّم لجامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، سنة 2004، ص11.

3- أنظر على التوالي : أ.نبيل صقر، جرائم الكمبيوتر والإنترنت في التشريع الجزائري، المرجع السابق، ص95. وكذلك : أ. عبد القادر درقاوي، جريمة السرقة في عصر المعلوماتية، مذكرة ماجستير، كلية الحقوق، جامعة أبي بكر بلقايد، تلمسان، الجزائر، سنة 2005، ص 58.

كما أنه تقع جريمة الأموال على مثل هذه الأجهزة، إما للاستيلاء على الجهاز أو الشيء نفسه محل الجريمة باعتبار أنّ له قيمة مادية[1]، لكن الأمر يطرح إشكال عندما يكون محل الجريمة ليس هو الكيان المادي[2]وإنّما الكيان المعنوي.[3]

ينطلق هذا الفريق من الفقهاء من فكرة مؤدّاها، أنّ البرنامج عبارة عن مجموعة من المعلومات تمت معالجتها وأصبحت رموزا وشفرات لا يمكن العلم بها إلا من خلال الآلة أو أثناء تشغيلها، وبالتالي فإن هذا الرأي يستبعد في مجمله الأفكار والمعارف التي لا يتم تجسيدها في شكل أو قالب معين، ذلك أنّ الفكرة في ذهن صاحبها ليس لها نظام قانوني ما لم يفصح عنها بإخراجها على أرض الواقع في أي شكل من الأشكال القابلة للحماية من طرف القانون وهي بالتالي تأخذ حكم النية فهي مستبعدة من نطاق التجريم ما لم يتم تجسيدها [4].

ويرجع الفضل في إضفاء وصف المال على المعلومة إلى كل من الأستاذين Michel Vivantو Pierre Catala ، فتعد المعلومة طبقا للأستاذ Catalaواستقلالا عن دعامتها المادية من قبيل المال للحيازة ولتدعيم هذا الوصف فقد أشار بأن المعلومة قابلة للحيازة، وهي قيمة تقوم وفقا لسعر السوق، وأنها منتج بصرف النظر عن دعامتها المادية وعن عمل من قدمها، وأنّ المعلومة ترتبط بصاحبها عن طريق علاقة قانونية، وهي علاقة المالك بالشيء الذي يملكه وأنها تنتمي إلى مؤلفها بسبب علاقة التبني التي تربط بينهما، وهي من شأنها أن تؤسس الحيازة اللازمة لإضفاء وصف المال[5]، وعلاوة على ذلك فإن المفاهيم الحديثة أظهرت أنّ مفهوم حق الملكية هو حق عيني غالبا ما يتوارى خلف الشخص صاحب الحق[6].

ويؤكد الأستاذ Michel Vivant هذا الإتجاه، وأسس رأيه على حجتين: الأولى: وهي أن فكرة الشيء أو القيمة لها صورة معنوية، وأن أي نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع إقتصادي وتكون جديرة بالحماية القانونية.

1- د. بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي ، الإسكندرية، مصر، ط1، سنة 2011، ص 22.

2- الكيان المادي: يشمل الأجهزة المادية المختلفة، وهي جهاز الإدخال، ووحدات التشغيل المركزية التي يتم من خلالها معالجة المعلومات وتخزينها وإخراجها، أنظر في ذلك: أ. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، ط 1، سنة 2006، ص 14.

3- الكيان المعنوي: يشمل البرامج المختلفة التي يتحقق من خلالها قيام الحاسب بوظائفه المختلفة، بالإضافة إلى المعلومات المطلوب معالجتها بالفعل، انظر في ذلك: نفس المرجع، ص 15.

4- خثير مسعود، المرجع السابق، ص39.

5- Pierre Catala, le droit à l'épreuve numérique, PUF, 1998, P170.

نقلا عن: د. أحمد خليفة الملط ، المرجع السابق، ص 100.

6- د. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، مصر، ط2، سنة 2002، ص170.

أمّا الثانية: فيرى أن كل الأشياء المملوكة ملكية معنوية والتي يعترف بها القانون، وترتكز على الإعتراف بأن المعلومة قيمة عندما تكون من قبيل البراءات والرسومات والنماذج والتحصيلات الضرورية وحق المؤلف، وأن الذي يقدم ويكشف ويطلع الجماعة على شيء ما بصرف النظر عن الشكل أو الفكرة، فلا توجد ملكية معنوية بدون الإقرار بالقيمة المعلوماتية.[1]

وفي نفس الإتجاه يرى الأستاذ Jacques Larrieu أن للمعلومة قيمة إقتصادية، ولذلك فمن الضروري إضفاء الحماية القانونية على برامج الحاسب الآلي وذلك عندما نكون بصدد براءات الإختراع، كما ينبغي اعتبارها من المصنفات الأدبية وتكون محمية عن طريق حقوق المؤلف[2]، وضمن حقوق الملكية الصناعية، الحقوق التي ترد على علامات مميزة كحق الصانع أو مقدم الخدمة أو التاجر في وضع علامة تجارية يميز بها منتجاته وخدماته[3]، وترمز حقوق الملكية الصناعية إلى المبتكرات الجديدة كالإختراعات وقد نظمها المشرع الجزائري بقانون شهادات المخترعين وبراءات الإختراع[4]، ويذهب هذا الاتجاه كذلك إلى تأييد وصف السرقة على المعلومات، وهذا ما أكده القضاء الفرنسي في حكم لمحكمة Clermont-Ferrand، حيث قامت موظفة بسرقة معلومات شخصية تتعلق بمديرها، وقد حكم عليها بالحبس ثلاثة (03) أشهر مع وقف التنفيذ عن جريمة السرقة[5].

البند الثاني: الرأي المعارض لإضفاء وصف المال العام على الكيان المعنوي للحاسب.

يرى جانب آخر من الفقه[6]، عدم صلاحية المعلومات لأن تكون محلا للإعتداء عليها، مستندا في ذلك على أن المعلومة في حالتها المجردة والفكرة في حد ذاتها لا تقبل التملك والإستثمار، وأن تداولها والإنتفاع بها من حق الكافة دون تمييز، ومن تم لا يمكن أن تكون محلا للملكية الفكرية[7]، وينبغي التمييز بين المعلومات[8] التي لم تتم معالجتها إلكترونيا، والتي تمت معالجتها، وإبراز أهم الفوارق الموجودة بين هذه الأخيرة من

---

[1]– د .أحمد خليفة الملط، المرجع السابق، ص108.

[2]- Jacques Larrieu, Droit de l'internet, Ellipses Edition Marketing, Paris , France, 2010, p 97.

[3]– د . عبد الفتاح بيومي حجازي، مقدمة في حقوق الملكية الفكرية وحماية المستهلك في عقود التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر ، ط1، سنة 2005، ص 14.

[4]– د. سمير جميل حسين الفتلاوي، الملكية الصناعية وفق القوانين الجزائرية، ديوان المطبوعات الجامعية، الجزائر، بدون طبعة، سنة 2002، ص 01.

[5]- TGI de Clermont-Ferrand, Chambre correctionnelle, jugement du 26 Septembre 2011, disponible à l'adresse suivante : www.legalis.net.

[6]– د . معتز سيد محمد أحمد عفيفي، قواعد الإختصاص القضائي بالمسؤولية الإلكترونية عبر شبكة الإنترنت، دار الجامعة الجديدة، الإسكندرية، ط 1، سنة 2013، ص 22.

[7]–أ. أمال قارة، المرجع السابق ، ص19.

[8]– لقد وجدت المعلومات منذ أن خلق الله سبحانه وتعالى الإنسان عندما خلق آدم عليه السلام وعلمه الأسماء كلها قال الله تعالى "وعلّم آدم الأسماء كلها ثم عرضهم على الملائكة فقال أنبئوني بأسماء هؤلاء إن كنتم صادقين " الآية رقم 31 من سورة البقرة.

من جهة والبيانات[1] من جهة أخرى،فيرى أن الأولى باعتبار أن عنصرها الأساسي هو الدلالة لا الدعامة التي تجسدها فإنه لا يمكن إختلاسها، لعدم توافر المادية فيها، بخلاف البيانات التي تمت معالجتها إلكترونيا فتتحدد في كيان مادي يتمثل في نبضات أو إشارات إلكترونية ممغنطة يمكن تخزينها على وسائط معينة، ونقلها واستغلالها وإعادة إنتاجها، فضلا عن إمكانية تقديرها كما وقياسا، فهي ليست شيئا معنويا كالحقوق والأفكار، بل هي شيء له في العالم الخارجي موجود مادي.[2]

وفقا لهذا الرأي فإن المعلومات إذا لم تعالج آليا عن طريق الحاسوب، لا تعتبر من قبيل الأموال الخاضع للحماية الجنائية باعتبار أن هذه المعالجة تتم في صورة نبضات إلكترونية ، مما يمكن القول بأنه بعملية المعالجة تلك تتحول من أموال معنوية إلى أموال مادية، الأمر الذي يخضعها للنصوص التقليدية لجرائم الأموال، ويأخذ نفس حكمها البيانات المخزونة سواء في برامج الحاسب أو في ذاكرته ، وبالتالي تأخذ برامج وبيانات الحاسب حكم الأموال عليه وبالتالي تتمتع بالحماية الجنائية المقررة لها[3].

وبالتالي فإنّ استبعاد المعلومات من نطاق مجموعة الأموال، لا ينطوي على الرفض لكل حماية قانونية، حيث يعتبر كل من الفقه والقضاء في فرنسا بوجود خطأ عند حيازة معلومة الغير على نحو غير مشروع، ومع ذلك يفرض منطق التحليل أن يندرج هذا الخطأ في مجال دعوى المنافسة غير المشروعة، لأنه إذا ما أقر بالخطأ باعتباره كذلك وبناءا على مفهوم الحيازة غير المشروعة للمعلومة، فلا يمكن الوصول إلى ذلك عن طريق تجاهل الحق الإستئثاري والذي سبق رفضه من قبل وتأسيس العقاب على فكرة الحيازة غير المشروعة، فإنّ الخطأ يجد سببه لا في فكرة الحيازة ذاتها للمعلومة، ولكن من خلال الظروف التي اقترنت بهذه الحيازة، وعلى نحو يمكن معه تجنب الإعتراف بفكرة الحق الإستئثاري[4].

فالمعلومات هي أغلى ما يملكه الإنسان لهذا سعى إلى جمعها وتسجيلها على وسائط حفظ مختلفة بدءا من جدران المقابر والمعابد في عصر الفراعنة إلى أن تم اختراع الورق في الصين، وهذا هو السبب في الإبقاء على حضارتهم محفورة في ذاكرة التاريخ، فإذا فقد الإنسان معلوماته فانه يفقد ذاكرته ومن ثمّ تضيع حضارته. وتعرف المعلومات لغويا بأنها مشتقة من كلمة علم ودلالتها فيها، وتدور بوجه عام حول المعرفة التي يمكن نقلها واكتسابها، أما اصطلاحا فهناك من يعرفها بأنها: مجموعة رموز يستخلص منها معنى معين في مجال محدد. أنظر في ذلك: د.أحمد خليفة الملط، المرجع السابق، ص 71.

[1]– البيانات: تعرف لغويا أنها مشتقة من الفعل بين أي أظهر وإتضح وأفصح، أما إصطلاحا : فهي مجموعة الحقائق أو المشاهدات أو القياسات التي تكون عادة على هيئة حروف أو أرقام أو أشكال خاصة تمثل فكرة أو موضوع أو هدف أو شرط أو أية عوامل أخرى، فالبيانات هي المادة الخام التي تشتق منها المعلومات. أنظر في ذلك : نفس المرجع ، ص77.

[2]– أ. خثير مسعود، المرجع السابق، ص42.

[3]– أ. أمال قارة، المرجع السابق، ص20.

[4]– د. عبد الله حسين علي محمود، المرجع السابق، ص165.

وقد حاول الأستاذ Lucas André أن يبرر الخطأ المعترف به على أساس نظرية الإثراء بلا سبب بوصفه تطبيقا خاصا لها وبعيد عن المنافسة غير المشروعة، كما رأت محكمة النقض الفرنسية الإستعانة بفكرة الخطأ لكي تعترف بالحق على المعلومات في احترام الحياة الخاصة[1].

ومن خلال ما تقدم، فإن كلا الرأيين إعترفا لبرامج الكمبيوتر بالحماية المقررة لجرائم الأموال عليها، وإن كانا يختلفان في كيفية إسباغ هذه الحماية عليها، ما يعكس واقعية الرأي الأول، ذلك أن هذه البرامج هي معلومات تنشأ عنها علاقات وتصرفات قانونية عديدة، إضافة إلى ذلك بدأت المعلومات تفرض نفسها في الأسواق كسلعة تباع وتشترى، ولها قيمة أصبحت تفوق مثيلاتها من السلع، و بالرجوع إلى نصوص القانون الجنائي يتبين أنها جاءت عامة، ولم تشترط أن يقع الإعتداء على منقول مادي[2]، كما أن برامج الحاسب الآلي يمكن أن تتم حمايتها كأسرار تجارية أو معلومات غير مفصوح عنها[3].

ولأن المعلومات ذات طبيعة معنوية، وبالرغم من اعتراف النظم القانونية منذ فترة طويلة بالحقوق المعنوية لمؤلفي المصنفات ذات المحتوى الفكري، فإن ما أنتجته التقنية من إبداعات لا تنتهي في حقل البرمجيات المستخدمة للتشغيل وتنفيذ التطبيقات والمهام، كل ذلك أدى إلى إيجاد اهتمام في ميدان حماية مبدعي عصر التقنية[4]، غير أنه لا حق دون أن يثبت من ادعى أنه المالك الحقيقي لحقوق المؤلف على المصنف[5]، كما أن الإعتراف بحق خاص على الإبتكار حافز على الإختراع وزيادة التقدم الصناعي[6].

المطلب الثاني: مفهوم الجاني في الجريمة الإلكترونية.

إنّ المجرم المعلوماتي[7]هو الذي استغل هذه التقنية بما لديه من قدرة على التعامل معها وتحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسب الآلي وملحقاته ووسائل الإتصال الرقمية، والجاني في الجريمة

---

[1] -André Lucas, Droit de l'informatique et de l'internet, Thémis, Paris, France, 2001, P681.

نقلا عن: د. أحمد خليفة الملط، المرجع السابق، ص 126.

[2]– د. علي عبد القادر قهوجي، الحماية الجنائية لبرامج الكمبيوتر، دار الجامعة الجديدة، الإسكندرية، ط1، سنة 1997، ص 54. نقلا عن: أ. مسعود خثير، المرجع السابق، ص 42.

[3]– د.أحمد عبد الخالق، حقوق الملكية الفكرية، دار المريخ للنشر، المملكة العربية السعودية، بدون طبعة، سنة 2002، ص 145.

[4]– د. هلال بن محمد البوسعيدي، المرجع السابق، ص 78.

[5]– د.صلاح الدين جمال الدين، حماية حق المؤلف في ضوء استخدام البث الفضائي للبرامج بالأقمار الصناعية، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2004، ص 72.

[6]– د. فاضلي إدريس، المدخل إلى الملكية الفكرية، دار هومه، الجزائر، بدون طبعة، سنة 2004، ص 197.

7– يقصد بالمجرم المعلوماتي الشخص الذي لديه مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسوب الإلكتروني والقادر على استخدام هذا التكتيك لاختراق الكود السري لتغيير المعلومات، أو لتقليد البرامج أو التعديل أو التحويل من الحسابات عند استخدام الحاسوب نفسه، هذا التعريف وفقا للإصطلاح القانوني. أمّا في الإصطلاح الإلكتروني فيطلق عليه خبراء أمن المعلومات الإلكترونية مصطلح "هاكرز" (Hackers) وهي جمع " هاكر"وهو

الإلكترونية قد يكون شخصا طبيعيا، أو شخصا معنويا يتوافر لديه –كشرط أساسي– معرفة كافية بآلية عمل وتشغيل الحاسب الآلي.

ويمكن القول بأنّ المجرم المعلوماتي تعبير ينطوي على قدر من التجاوز في القول، فالصحيح أنه لا يوجد نموذج محدد للمجرم المعلوماتي، بل هناك عدة نماذج للمجرمين قد يستخدمون الكمبيوتر في جرائمهم، وقد يقومون بأفعال إجرامية ضد الكمبيوتر نفسه، وبالتالي ترجع الصعوبة في تحديد سمات معينة للمجرم المعلوماتي إلى تعدّد جرائم الكمبيوتر وتنوّعها لكي تغطي صورا عديدة من الأنشطة[1].

ورغم ذلك فإنّه يمكن القول بوجود سمات مشتركة بين هؤلاء المجرمين وطائفة المجرمين ذوي الياقات البيضاء[2]، حيث كلا من هؤلاء المجرمين قد يكونوا من ذوي المناصب الرفيعة المستوى ومن ذوي الشخصيات والكفاءات العالية ويتمتعون بالذكاء وبالقدرة على التكيف الإجتماعي، بل إنّ بعضهم يتمتع باحترام وثقة عالية من الأشخاص المحيطين بهم في مجال العمل أو في المحيط الإجتماعي.

وبالتالي يمكن استخلاص مجموعة من السمات التي يتميز بها المجرم المعلوماتي والتي يساعد التعرّف عليها مواجهة هذا النمط الجديد من المجرمين، ويعدّ الأستاذ Donn Parker واحدا من أهم الباحثين الذين اهتموا بالجريمة المعلوماتية بصفة عامة وبالمجرم المعلوماتي بصفة خاصة ، إذ يرى أن المجرم المعلوماتي وإن كان يتميز ببعض السمات الخاصة إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه[3]، خاصة وأنّ الجرائم الإلكترونية أصبحت تحتل مرتبة متقدمة من حيث التأثير على مصالح الدول الكبرى نتيجة الخسائر المترتبة عنها.

الإنسان الذي يقوم بعمليات الإختراق والتخريب عبر شبكة الإنترنت، كما يطلقون مصطلح "كراكرز" (Crakers) على المتخصصين بفك شفرات البرامج وليس تخريب الشبكات فهم نوع من الهاكرز المتخصص. أمّا في اللغة العربية فنظرا لعدم وجود ترجمة لكلمة الهاكر باللغة العربية حتى الآن فنستخدم الكلمة كما هي وإن كان مصطلح "مخترقو أمن الشبكات" هو أقرب تفسير لهذا المعنى. أنظر في ذلك : د. هلال بن محمد بن حارب البوسعيدي، المرجع السابق،ص 38.

[1]– د.عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، بهجت للطباعة والنشر، مصر، ط1، سنة 2009، ص 95.

[2]– مصطلح المجرمين ذوي الياقات البيضاء مصطلح حديث نسبيا وأول من أطلقه عالم الإجتماع (Suther Land)،حيث وضح أنّ هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع ذوي المناصب الإدارية الكبيرة وتشمل أنواع مختلفة من الجرائم كغسيل الأموال وتجارة الرقيق وتزوير العلامات التجارية وغير ذلك من الجرائم التي يقدمون على ارتكابها وهم جالسون في مكاتبهم الفخمة. أنظر في ذلك: د. نهلا عبد القادر المومني، المرجع السابق، ص76.

[3]- Donn Parker, OP.Cit, P123.

نقلا عن : أ. نهلا عبد القادر المومني ، المرجع السابق، ص 79.

وإلى جانب دراسة سمات المجرم المعلوماتي من المهم التطرق إلى أصناف هؤلاء المجرمين ودوافعهم، على اعتبار أن الجرائم الإلكترونية تتدرج من الجرائم البسيطة إلى الجرائم الإرهابية، وذلك تبعا لشخصية المجرم المعلوماتي، وبما لديه من خبرة في مجال استخدام الحاسب الآلي والغرض من ارتكاب الجريمة، فالإجرام المعاصر يتميز بظهور أنماط حديثة تتنوع فيها الظاهرة الإجرامية[1]،وانطلاقا من ذلك سأتطرق في الفرع الأول لفئات الجناة في الجرائم الإلكترونية، أمّا الفرع الثاني فأتناول فيه خصائص هؤلاء الجناة، أمّا الفرع الثالث فخصص لدوافع ارتكاب الجريمة الإلكترونية.

الفرع الأول: فئات الجناة في الجريمة الإلكترونية.

إنّ كل تقنية مستحدثة ينشأ عنها وفي أيّ مرحلة من مراحل تطوّر هذه الظاهرة الإجرامية الخاصة طائفة جديدة من المجرمين، وينطبق ذلك بوجه خاص على المعلوماتية، لأنّ الإمكانيات المستحدثة التي تقدمها الآلة الإلكترونية، من حيث سهولة وسرعة تنفيذ الأعمال الإجرامية، وكذلك إخفاء الأدلة تساعد على نشوء هذه الظاهرة[2].

وتسعى هذه الدراسات إلى إيجاد تقسيم لمجرمي المعلوماتية، لكنها تجد صعوبة في تحقيق ذلك بسبب التغيّر السريع الحاصل في نطاق هذه الظاهرة، ولهذا يتجه الباحثون إلى الإقرار بأنّ أفضل تقسيم لمجرمي المعلوماتية هو التصنيف القائم على أساس أغراض الإعتداء وليس على أساس التكنيك الفني المرتكب في الإعتداء، وعلى أساس الوسائط محل الإعتداء أو المستخدمة لتنفيذه.

ويعدّ من أفضل التصنيفات لمجرمي المعلوماتية تقسيمهم إلى الفئات التالية:

أولا: المخترقون أو المتطفلون: Crakers, Hakers.

طائفة الكركرز لا تختلف عن طائفة الهاكرز من الناحية التجريمية، مع العلم أنّه بين الإصطلاحين تباينا جوهريا قد تم الإشارة إليه، وأفراد هذه الطائفة يرتكبون جرائم التقنية بدافع التحدي الإبداعي،ويجدون أنفسهم أوصياء على أمن نظم المعلومات في المؤسسات المختلفة، والسمة الغالبة على أعضاء هذه الطائفة صغر السن وقلة الخبرة وعدم التمييز بين الأنظمة محل الإختراق[3].

---

[1]– د. أيمن عبد الحفيظ، المرجع السابق، ص 252.

[2]– د. عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة و المجرم المعلوماتي، منشأة المعارف، الإسكندرية، مصر، ط1، سنة 2009، ص102.

[3]– د. أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، ط1، سنة 2010، ص20.

كما يتسم أفراد هذه الطائفة بتبادلهم المعلومات فيما بينهم، وتحديدا التشارك في وسائل الإختراق وآليات نجاحها، وإطلاعهم بعضهم البعض على مواطن الضعف في نظم المعلومات والشبكات[1].

ثانيا : المحترفون.

تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها، ولذلك فإن هذه الطائفة تعدّ الأخطر من بين مجرمي التقنية حيث تهدف اعتداءاتهم إلى تحقيق الكسب المادي لهم، أو للجهات التي كلّفتهم وسخرتهم لارتكاب جرائم الكمبيوتر، كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية أو التعبير عن موقف فكري أو فلسفي، ويمكن تقسيم هذه الطائفة إلى مجموعات متعددة تبعا لتخصصهم بنوع معين من الجرائم، أو تبعا للوسيلة المتبعة من قبلهم لارتكاب الجرائم، مثل طائفة محترفي التجسس الصناعي أو طائفة مجرمي الإحتيال والتزوير[2].

ثالثا: الحاقدون.

هذه الطائفة تحرك أنشطتهم الرغبة في الإنتقام والثأر، كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معه عندما لا يكونون موظفين فيها، ولهذا فإنهم ينقسمون إمّا إلى مستخدمين للنظام بوصفهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الإنتقام من المنشأة المستهدفة في نشاطهم.

ولا يتسم أعضاء هذه الطائفة بالمعرفة التقنية الإحترافية ويغلب على أنشطتهم من الناحية التقنية استخدام تقنيات زراعة الفيروسات وتخريب النظام، ومن حيث الخطورة فهم أقل خطورة من غيرهم من مجرمي التقنية، ولكن ذلك لا يمنع أن تكون الأضرار التي نجمت عن أنشطة بعضهم جسيمة، وألحقت خسائر فادحة بالمؤسسات المستهدفة.[3]

رابعا: صغار نوابغ المعلوماتية.

يطلق لفظ نوابغ المعلوماتية على المجموعات التي تميل للتحدي الفكري، وهم غالبا ما يكونون في مرحلة المراهقة وعلى الرغم من صغر سنهم إلاّ أنهم قادرون على اقتحام كافة أنواع النظم والشركات والمؤسسات المالية، ويتميز هؤلاء المراهقون عن غيرهم من مرتكبي الجرائم التقليدية في أنهم لا يعتبرون أنّ ما

---

[1]- د. أحمد محمود مصطفى، المرجع السابق، ص **21**.

[2]- د. محمد طارق عبد الرؤوف الخن، المرجع السابق، ص **186**.

[3]- د. أحمد محمود مصطفى، المرجع السابق، ص**22**.

يقومون به يعد جريمة لأنّهم يعتقدون أنّ النظام الغير قادر على حماية نفسه ليس من الخطأ اقتحامه،ولذلك فإنهم يعتبرون أنفسهم أبطالا لمساعدة المجتمع في تحديد نقاط الضعف الخاصة بالبرنامج الذي تم اقتحامه.

ويمكن لجماعات صغار نوابغ المعلوماتية أن تتحول إلى فئة القراصنة لأنه عندما يصبحون على درجة عالية وكبيرة من الخبرة والمهارة يتم استئجارهم واستغلالهم في أعمال ذات أهداف إجرامية[1].

وقد ظهرت ثلاثة إتجاهات تتعلق بطبيعة هذه الفئة ومدى خطورة أفرادها، تمثلت فيما يلي[2]:

الإتجاه الأول:

يرى عدم إسباغ أية صفة جرمية على هذه الفئة، ولا يرى ضرورة تصنيفهم ضمن الطوائف الإجرامية لمجرمي التقنية، إستنادا إلى أنّ هؤلاء لديهم ببساطة ميل للمغامرة والتحدي ورغبة في الإكتشاف، إضافة إلى أنهم لا يدركون ولا يقدّرون مطلقا نتائج أفعالهم التي يقومون بها.

الإتجاه الثاني:

يؤيد هذا الإتجاه هذه الفئة، ويعتبرها ممن تقدم خدمة لأمن المعلومات ووسائل الحماية، وينسب أصحاب هذا الإتجاه إلى هذه الفئة الفضل في إكتشاف الثغرات الأمنية في تكنولوجيا المعلومات.

الإتجاه الثالث:

ويرى أصحابه أنّ مرتكبي جرائم الحاسوب من هذه الطائفة، يصنّفون ضمن مجرمي الحاسوب كغيرهم دون تمييز إستنادا إلى أنّ الحد الفاصل بين العبث بالحواسيب وبين الجريمة أمر عسير.

ولا شك أنني أميل إلى الإتجاه الثالث الذي يضفي الصفة الإجرامية على هذه الفئة، لأنه يجب عدم التقليل من خطورة هؤلاء الأشخاص، فهذه الفئة قد تتعدى مرحلة الهواية والعبث لتدخل مرحلة متقدمة أكثر في مجال ارتكاب الجرائم الإلكترونية وهي مرحلة الإحتراف لهذه الجرائم.

كما أن هناك عدة مخاوف تتمثل في احتضان منظمات الجريمة المنظمة لهذه الفئة للإستفادة من مهاراتهم وتطويرها من أجل تحقيق غاياتهم الإجرامية، فهم يقبلون المغامرة و الإثارة والتحدي[3].

خامسا: مجرمو المعلوماتية في إطار الجريمة المنظمة.

في عالم الشبكات الإلكترونية كما هو الحال في العالم الحقيقي، يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة، إلا أنّ مجموعات الجريمة المنظمة بدأت بشكل متزايد باستغلال الفرص الجديدة التي

---

[1]– د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 143.

[2]– د. يونس عرب،المرجع السابق، ص 30. نقلا عن : د. محمد طارق عبد الرؤوف الخن، المرجع السابق، ص188.

[3]– د. نهلا عبد القادر المومني، المرجع السابق، ص 82.

يوفرها العالم الرقمي، فمنظمات الجريمة المنظمة تطوّر أساليب عملها باستمرار بما يحقق أهدافها وغاياتها،وتسعى دوما إلى استغلال الوسائل التقنية الحديثة في القيام بنشاطاتها، فقد وجدت في شبكة الإنترنت وسيلة لا تضاهى للقيام بعمليات تبييض الأموال وكذلك تدعيم تجارة الرقيق الأبيض وتجارة الأعضاء البشرية عبر إنشاء مواقع خاصة بهذه الأعمال[1]، ويسمى المجرم في هذه الحالة بالمجرم المنظم[2].

وتقوم هذه الجماعات بتبنّي أصحاب الكفاءات وأصحاب الخبرة والموهوبين في مجال تقنية المعلومات، وذلك بإغرائهم بالمال لينضموا إليها، ويمارس مجرمو المعلوماتية في نطاق هذه المنظمات نشاطات تدر على المنظمة أرباحا هائلة فيقوموا بتزوير البرامج وتقليدها واختراق شبكات المعلومات الخاصة بالدول والمؤسسات المالية الكبرى العالمية[3].

الفرع الثاني: خصائص الجناة في الجريمة الإلكترونية.

تتميز شخصية المجرم مرتكب الجريمة الإلكترونية بخصائص وصفات تختلف عن مرتكب الجرائم التقليدية الأخرى، وهذا مرجعه تميز شخصية مرتكبي الجرائم الإلكترونية بالتقدم في مجال استخدام الحاسب الآلي، وهم غالبا على درجة علمية وثقافية عالية لكي يتمكنوا من استخدام أجهزة الحاسب الآلي في ارتكاب جرائمهم، وهذا بعكس المجرم العادي الذي غالبا ما يتميز بالقوة العضلية ونادرا ما يتميز بعضهم بعنصر الذكاء[4]، وأهم هذه الخصائص يمكن إجمالها فيما يلي:

أولا: الذكاء المعلوماتي.

يعتبر الذكاء من أهم صفات مرتكب الجريمة الإلكترونية لأنّ ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي، والقدرة على التعديل والتغيير في البرامج وارتكاب جرائم السرقة والنصب وغيرها من الجرائم التي تتطلب أن يكون مرتكب الجريمة على درجة كبيرة من المعرفة لكي يتمكن من ارتكاب تلك الجرائم.[5]

---

[1]– أ. نهلا عبد القادر المومني، المرجع السابق، ص 88.

[2]- Margaret Beare, Les femmes et le crime organisé, disponible à l'adresse suivante : www.publications.gc.ca.

3– أ. نهلا عبد القادر المومني، المرجع السابق، ص 88.

[4]– د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 133.

5– د. أيمن عبد الحفيظ، المرجع السابق، ص 243.

ومثل هذا الذكاء يكتسبه الجاني إمّا من خلال الدراسة المتخصصة لعلوم الكمبيوتر والأنظمة المعلوماتية أو من خلال التطبيق أو الخبرة العملية، أومن خلال اختلاطه إجتماعيا بالمتخصصين في علوم الكمبيوتر والإنترنت والأنظمة المعلوماتية[1]، غير أنّ هناك جرائم معلوماتية يستلزم لارتكابها أن تتوافر لدى الجاني معرفة واسعة جدا بكيفية استخدام أصعب الأجهزة والبرامج، في حين أنّ هناك جرائم معلوماتية أخرى لا يتطلب ارتكابها معرفة تقنية واسعة[2]، كما أنّ أكثر الأشخاص معرفة بهذه المعلومات هم العاملون لدى المؤسسة المجني عليها.

ثانيا: الخبرة والمهارة.

يتصف المجرم المعلوماتي بأنّه على درجة عالية من الخبرة والمهارة في استخدام التقنية، وذلك لأن مستوى الخبرة والمهارة التي يكون عليها هي التي تحدد الأسلوب الذي يرتكب به تلك الجرائم، بحيث إذا كان الشخص مرتكب الجريمة على قدر ضئيل من مستوى الخبرة نجد أن الجرائم التي قد يرتكبها لا تتعدى الإتلاف المعلوماتي إما بالمحو أو الإتلاف، وكذلك نسخ البيانات والبرامج.

أمّا إذا كان الشخص على درجة أعلى من المهارة، فإنّ أسلوب ارتكابه الجرائم يختلف، حيث يقوم عن طريق استخدام الشبكات بالدخول إلى أنظمة الحاسب الآلي وسرقة الأموال وارتكاب جرائم النصب وجرائم التجسس وزرع الفيروسات وغيرها من الجرائم التي تتطلب مستوى معين من المهارة وخبرة كبيرة في ارتكابها[3].

1- تأكد في دراسة أجرتها وزارة الداخلية البريطانية أنّ الأطفال الذين يحبون قضاء وقت أطول أمام ألعاب الكمبيوتر يكونون أذكياء مقارنة بغيرهم ممن لا يمارسون الألعاب ويتوقع لهم اقتحام مجالات عمل ناجحة أكثر من الأطفال المنطوين على أنفسهم، وقد أجريت الدراسة على مائة وسبعة وعشرون شخصا من بينهم ثلاثة وستون طفلا، إلا أنّه بمقارنتهم مع صغار آخرين وجد أنّ هواة الكمبيوتر يعتبرون أشخاصا أذكياء للغاية ومتحمسين وساعين للإنجاز،كما أفادت نتيجة المتابعة لمدة خمسة أعوام على هؤلاء الأطفال أنهم تفوقوا دراسيا والتحقوا بالجامعة ثم التحقوا بوظائف مرموقة.أنظر في ذلك: د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 34.

2- أ. رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة مقارنة)، المكتب الجامعي الحديث، الإسكندرية، مصر، بدون طبعة، سنة 2013، ص 49.

3- د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 134.

ثالثا: السلطة المعلوماتية.

لا يقصد بالسلطة هنا أنّ الجاني يمتلك سلطة سياسية أو عسكرية، بل يقصد بها أنّ المجرم المعلوماتي يتمتع في الغالب بحقوق ومزايا اتجاه النظام المعلوماتي المستهدف[1]، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو أو تعديل المعلومات التي تحتوي عليها. وقد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي، أو مجرد الدخول إلى الأماكن التي تحتوي على أنظمة الحاسبات الآلية، وقد تكون السلطة التي يتمتع بها الجاني غير شرعية، كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر[2].

رابعا: المجرم المعلوماتي يبرّر ارتكاب جريمته.

يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي أنّ ما يقوم به لا يدخل في عداد الجرائم أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية، وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، فهؤلاء الأشخاص لا يدركون أنّ سلوكهم يستحق العقاب، ويبدو أن الإستخدام المتزايد للأنظمة المعلوماتية قد أنشأ حالة نفسية موائمة لتصور استبعاد فكرة الخير والشر وقد ساعد على ذلك عدم وجود احتكاك مباشر بالأشخاص، ومما لاشك فيه أن هذا التباعد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل.[3]

خامسا: الميل إلى التقليد.

يبلغ الميل إلى التقليد منتهاه حين يوجد الفرد وسط آخرين متجمعين، إذ يكون عندئذ أسهل وأسرع انسياقا لتأثير سواه عليه، ويظهر ذلك في مجال الجريمة الإلكترونية لأنّ أغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية التي لديه مما يؤدي به الأمر إلى ارتكاب الجرائم.

1- د. رشاد خالد عمر، المرجع السابق، ص 49.

2-د. طارق إبراهيم الدسوقي عطية، المرجع السابق،ص 177.

3- أ. نهلا عبد القادر المومني، المرجع السابق،ص 78.

ولاشك أنّ هذا يكون نتيجة لعدم الإستواء في شخصية الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصّلها الفرد في ذاته، مما يحجم لديه غريزة التفاعل مع الوسط المحيط مما ينتهي به الأمر إلى التقليد وارتكاب الجريمة.[1]

أما السمات التي تتميز بها المجموعات عن الفرد المستقل في ارتكاب الجرائم المعلوماتية تتمثل فيما يلي:

1. التنظيم والتخطيط:

ترتكب أغلب الجرائم من مجموعة متكونة من عدة أشخاص يحدد لكل شخص دور معين ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة، فمثلا تحتاج جريمة مثل نسخ برامج الحاسب الآلي إلى شخص يقوم بنسخ تلك البرامج وقد يكونون مجموعة أشخاص، ويحتاج أيضا إلى مجموعة تقوم بعملية البيع، وينتج عن هذا التنظيم صعوبة عملية كشف الجريمة وإمكانية تنفيذها بدقة نتيجة للتخصص داخل تلك الجماعة في كل جزء من أجزاء الجريمة[2].

2. التكيف الاجتماعي:

لا يضع مجرم الحاسب الآلي نفسه في حالة عداء سافر مع المجتمع الذي يحيط به، بل إنّه إنسان متكيف معه، ذلك أنّه أصلا إنسان مرتفع الذكاء ويساعده ذلك على عملية التكيف، حيث أنّ التكيف الإجتماعي ينشأ بين مجموعة لها صفات مشتركة، فمثلا جماعة صغار نوابغ المعلوماتية لاشك أنهم يتكيفون في أفكارهم فيما بينهم، وتنشأ بالتالي بينهم صلات وروابط تساعدهم على ارتكاب جرائمهم، وتتعدى تلك الروابط والصلات النطاق المحلي إلى المجال الدولي بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم في استثمار تلك المعرفة والتقدم العلمي[3].

ففكرة المجرم المعلوماتي فكرة جديدة على الفقه الجنائي، ففي الجرائم المتعلقة بالحاسب الآلي لسنا بصدد مجرم عادي، ولكن مجرم ذو مهارات تقنية، وذو دراية بالتكنيك المستخدم في نطاق الحاسب الآلي[4].

1- د.أيمن عبد الحفيظ، المرجع السابق، ص 245.

2- نفس المرجع، ص 246.

3- د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 137.

4-أ. رشاد خالد عمر، المرجع السابق، ص 49.

3. التطور في السلوك الإجرامي:

يؤدي وجود الفرد في جماعة إجرامية مهما بلغت قدرتها العلمية إلى التأثير في قدرته العقلية وسرعة اكتسابه المهارة التقنية، التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة إلى محاولة الوصول على أعلى معدّلات المهارة التقنية المتمثلة في إثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة، فالمجرم المعلوماتي يتميز بالحصول على ما يحتاج إليه أو ابتكار الأساليب التي تقلل من الوسائل اللازمة لإتمام النشاط الإجرامي، والحقيقة أنه كلما كان نظام الحاسب الآلي الذي يحتوي على المعلومات المستهدفة غير مألوف، كانت الوسائل المتطلبة أكثر صعوبة في الحصول عليها، لاقتصارها على عدد قليل من الأفراد هم عادة القائمون على تشغيل النظام[1].

الفرع الثالث: دوافع إرتكاب الجريمة الإلكترونية.

إنّ الدافع أو الباعث أو الغرض أو الغاية تعبيرات لكل منها دلالته الإصطلاحية في القانون الجنائي تتصل بما يعرف بالقصد الجنائي في الجريمة، وهي مسألة تثير جدلا فكريا وقضائيا واسعا ذلك أن القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجنائي فالباعث هو العامل المحرك للإرادة التي توجه السلوك الإجرامي، فهو قوة نفسية تدفع الإرادة إلى الإتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة وهو يختلف من جريمة لأخرى تبعا لاختلاف الناس من حيث السن والجنس، درجة التعليم، وغير ذلك من المؤثرات كما يختلف بالنسبة للجريمة الواحدة من شخص لآخر[2].

أما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي ويتمثل بتحقيق النتيجة التي انصرف إليها القصد الجنائي أو الإعتداء على الحق الذي يحميه قانون العقوبات،أمّا الغاية فهي الهدف البعيد الذي يرمي إليه الجاني لارتكاب الجريمة كإشباع شهوة الإنتقام أو سلب مال المجني عليه في جريمة القتل.

والأصل أنّ الباعث والغاية ليس لهما أثر قانوني في وجود القصد الجنائي الذي يقوم على عنصرين: علم الجاني بعناصر الجريمة واتجاه إرادته إلى تحقيق هذه العناصر أو إلى قبولها ولا تأثير للباعث أو الغاية على قيام الجريمة أو العقاب عليها، فالجريمة تقوم بتحقق عناصرها سواء كان الباعث نبيلا أو رذيلا وسواء كانت

---

[1]- د. أيمن عبد الحفيظ، المرجع السابق، ص 247.

[2]- د. أحمد محمود مصطفى،المرجع السابق، ص23.

الغاية شريفة أو دنيئة، وإذا كانت القاعدة أنّ الباعث أو الغاية لا أثر لهما على قيام الجريمة، فإن القانون يسبغ عليهما في بعض الأحيان أهمية قانونية خاصة[1].

ولاشك أنّ الدوافع على ارتكاب الجرائم الإلكترونية تتباين تبعا لطبيعة المجرم ومدى ثقافته وخبرته في مجال الحاسب الآلي، لأن المتهم يرتكب جريمته بناءا على ما لديه من مهارة وخبرة، فالمتهم ذو الخبرة في مجال البرمجة واستخدام شبكات الحاسب الآلي قد يكون هدفه مختلفا عن هدف المتهم الذي لا تتعدى خبرته مجرد تشغيل جهاز الحاسب الآلي[2]، والبواعث أو الدوافع التي قد تدفع المجرم المعلوماتي إلى ارتكاب جريمته تتنوع، وأهم هذه الدوافع:

أولا: تحقيق المكسب المادي.

يعد هذا الدافع من بين أكثر الدوافع تحريكا للجناة لاقتراف جرائم الحاسوب، ذلك أن خصائص هذه الجرائم وحجم الربح الكبير الممكن تحقيقه من بعضها يتيح تعزيز هذه الدوافع[3]، ويقوم مرتكب الجرائم الإلكترونية ذو الكفاءة الفنية العالية بما لديه من خبرة ومهارة في المجال التكنولوجي بتوجيه هذه الإمكانيات نحو المؤسسات المالية لمحاولة تحقيق المكاسب المادية، إما بسرقة الأموال أو بتحويلها لحسابه الشخصي داخل البنك،ويستطيع المتهم بمجرد دخوله على أنظمة البنوك معرفة أرقام الحاسب وسرقتها أو تحويلها.

ويتم كذلك عن طريق استخدام فيزا كارت أو الماستر كارت البيع والشراء عبر شبكة الإتصالات الدولية من خلال سرقة تلك الأرقام باستخدام شبكة المعلومات،ويكون المكسب أيضا هدفا لمن هم أقل في المعرفة التقنية، غير أن أسلوب ارتكابهم للجريمة يكون محدودا في مجال معين لا يحتاج إلى خبرة أو مهارة[4]، وإن كان من الصعب تقدير الخسائر المالية المرتبطة بهذا النشاط الإجرامي نتيجة عدم الإبلاغ عن هذه الجرائم من طرف كبريات الشركات خوفا من زعزعة ثقة عملائها[5].

---

[1]– أ. نبيل صقر،جرائم الكمبيوتر والإنترنت في التشريع الجزائري، المرجع السابق، ص 117.

[2]– أ. نهلا عبد القادر المومني، المرجع السابق، ص 92.

[3]– د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 138.

[4]– د. أيمن عبد الحفيظ، المرجع السابق، ص 248.

[5]- Clement Bohic, Le poids économique de la cybercriminalité, le 10/06/2014,disponible à l'adresse suivante : www.itespresso.fr.

ثانيا : إثبات التفوّق العلمي والرغبة في قهر النظام المعلوماتي.

يقوم المجرم المعلوماتي بمحاولة إثبات التفوق العلمي من خلال التحدي الفكري أثناء استخدامه للحاسب الآلي وإثبات قدرته على اختراق أنظمة الحاسب الآلي والدخول عليها، وهو أحد الدوافع التي تجعل الكثير يلجأون إلى ارتكاب مثل تلك الأفعال على الرغم من عدم توافر نية ارتكاب الجريمة[1].

فمجرمو المعلوماتية يتملّكهم شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الوسائل التقنية الحديثة إلى تعويضهم عن الإحساس بالدونية، وفي هذا الشأن نجد المبرمج المعلوماتي وهو مفتاح شر كل نظام قد ينتابه إحساس بالإهمال أو بالنقص داخل المنشأة التي يعمل بها، وقد يندفع تحت تأثير رغبة قوية من أجل تأكيد قدراته التقنية لإدارة المنشأة إلى ارتكاب الجريمة الإلكترونية.

ويتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي جرائم الحاسوب في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات[2]، كما أن العديد منهم يتمكنون من الدخول إلى شبكات الإنترنت نتيجة ضعف الحماية الفنية.

ثالثا: الإنتقام.

نشأ عن استخدام التقنية آثار سلبية في سوق العمل من جهة وفي البناء الوظيفي من جهة أخرى، وقد لوحظ أنّ العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل في حالات معينة، هذه الأمور قد تعتبر قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب باعثها الإنتقام من رب العمل[3]، مثلا كالموظف الذي يقوم بتدمير برامج النظام المعلوماتي للمؤسسة التي كان يعمل فيها سابقا وفصل منها انتقاما على فصله، أو التي ما زال يعمل فيها إنتقاما على حرمانه من مكافآت مالية معنية أو من الترقية أو من حقوق ومزايا معينة، وذلك من خلال زرع الفيروسات بداخل النظام أو من خلال زرع القنابل المنطقية الإلكترونية التي تنفجر فيما بعد حسب التوقيت التي وضعه الجاني والذي قد يمتد إلى سنوات وتؤدي بانفجارها إلى تدمير النظام المعلوماتي المستهدف كاملا أو جزئيا[4].

---

[1]– د. أيمن عبد الحفيظ، المرجع السابق، ص 249.

[2]– أ. نهلا عبد القادر المومني، المرجع السابق، ص 92.

[3]– أ. نبيل صقر، جرائم الكمبيوتر و الإنترنت، المرجع السابق، ص 118.

4– أ. رشاد خالد عمر، المرجع السابق، ص 53.

وقد يصدر التصرف بغرض الإنتقام من دولة معادية لدولة أخرى وذلك عن طريق إمّا التجسس على المعلومات أو ارتكاب جرائم السرقة لأصول الأموال أو لمحاولة تشويه صورة هذه الدولة باستخدام الشبكة الدولية للإتصالات[1].

رابعا: الدوافع السياسية والإيديولوجية والعسكرية.

إنّ الكثير من الجرائم الإلكترونية يرتكبها الجناة بدوافع سياسية تهدف إمّا الإساءة للدول وحكوماتها ورؤسائها وقاداتها ومسؤوليها، مثلا كمن يشهّر بأحد مسؤولي الدولة عبر شبكة الإنترنت بأقوال كاذبة أو بصور مزيفة بغية تشويه سمعته أمام مواطنيه أو أمام الدول الأخرى، أو تهدف على الأقل إلى معارضة الدولة سياسيا أو التأثير على سياستها.

ومن جهة أخرى فإنّ الدوافع الإيديولوجية قد تكون وراء العديد من الجرائم الإلكترونية التي يرتكبها مجرمو المعلوماتية،وهذه الدوافع تحددها ثقافة وتفكير الجاني وما يؤمن به من أفكار في مجال معين أو اتجاه موضوع معين من المواضيع الدينية أو السياسية أو العرقية[2]، كأنشطة التنظيمات الإرهابية ضد المواقع الإلكترونية العائدة لجهات لا تتفق مع إيديولوجياتهم أو تحريض على الكراهية العنصرية[3]،كما يعدّ التسابق الفضائي والعسكري بين الدول دافعا لهذه الجريمة، فقد قام القراصنة بالإعتداء على شبكات معلوماتية تابعة لوكالة الفضاء "ناسا" ومواقع أسلحة ذرية تابعة لحكومة الولايات المتحدة الأمريكية[4].

خامسا: إرتكاب الجريمة كوسيلة للتسلية والدعابة والمغامرة.

يعتبر دافع المزاح أو الدعابة من الدوافع التي تجعل الشخص يقوم بتصرفات، وإن كان لا يقصد من ورائها إحداث جرائم وإنما بغرض المزاح فقط، ولكن هذه التصرفات قد ينتج عنها نتائج ترقى إلى درجة الجريمة[5]، هذا إلى جانب التحدي والمغامرة فكثير ما يسمع الفرد أن مصرف ما أو شركة أعلنت أنّ لا أحد يستطيع اختراق نظم الحاسب لديها بسبب الحماية التي فرضتها هذا يدفع المجرمين إلى تحدي ومنافسة مثل هذه الإعلانات[6]، وبما أنّ الجزائر معرضة كبقية دول العالم لهذه النوعية من الجرائم التي أصبحت تشكل خطرا كبيرا على الأشخاص والمؤسسات، فقد كانت هناك عدة مقترحات من قبل المتخصصين في مجال الجرائم

---

[1]–د. أيمن عبد الحفيظ، المرجع السابق، ص 250.

[2]–أ.رشاد خالد عمر، المرجع السابق، ص 54.

[3]- Marc Rees, Les principales mesures du plan anti-cybercriminalité français police, en concert sur le net, le 15/02/2008,disponible à l'adresse suivante : www.poinpact.com.

4– أ. نهلا عبد القادر المومني، المرجع السابق،ص 93.

[5]–د. أيمن عبد الحفيظ، المرجع السابق، ص 250.

6– د. تركي محمد العطيان، جرائم الحاسب الآلي، بدون تاريخ،ص 13، على الموقع :www.aljareh.com

المتصلة بالتكنولوجيات الحديثة، منها وضع كاميرات أمنية لمراقبة نشاط نوادي الإنترنت وضرورة وجود إطار قانوني لمكافحة هذه الجرائم ذات الصلة بالمعلوماتية[1].

المبحث الثاني: ماهية الدليل الإلكتروني.

برزت الظاهرة الرقمية ذات الطبيعة التقنية التي ارتبطت بالحاسب الآلي وشبكة الإنترنت كمفهوم جديد لتنظم بجدارة إلى المفاهيم التقليدية للدليل، لينشأ ما يسمى"الدليل الرقمي" أو "الدليل الإلكتروني" حسب ما أطلق عليه المشرع الأوروبي، والذي أخذت المحاكم في النظم القانونية المقارنة في الإعتداد به والإعتراف له بقيمة قانونية تكاد تتساوى مع الأدلة التقليدية، ومبعث هذا الإعتراف هو النظرة إلى الواقع الجدي للتقنية الرقمية بحسبانها ذات مدلول مؤثر وحقيقي في حياة البشرية في الحاضر والمستقبل [2].

والجريمة الإلكترونية تثير مسألتين أساسيتين: تحديد موقع الجاني و الحفاظ على الأدلة لإثبات الجريمة، إلا أن عملية الإثبات تعترضها قيود تتمثل في عدم كشف الجاني عن هويته، قدرته على حذف وإتلاف الأدلة والطابع الدولي لهذه الجريمة[3]، كما أنّ مرتكبو الجرائم الإلكترونية يستخدمون تكنولوجيا جديدة وأدوات متطورة تجعل من الصعب على السلطات المسؤولة عن التحقيقات متابعتها، فتكنولوجيا المعلومات في تطور مستمر وكل تطور جديد تتبعه خطوات معينة يجب القيام بها لكي يمكن الحد من الإختراقات والهجمات الإجرامية.

كما أنّ استخلاص الدليل الإلكتروني صار جزءا لا يتجزأ من تطبيق القانون، كما أنّ الحصول عليه أصبح أمر صعب الوصول إليه لما يتطلبه من خبرة ومهارة كبيرتين في مجال الحاسوب والإنترنت،وللدليل الإلكتروني أهمية كبيرة ودور أساسي في معرفة كيفية حدوث الجريمة لذلك لابد أن يحتوي التحقيق الجنائي الرقمي على هذا الدليل، ويجب أن يكون لدى الأشخاص المسؤولين عن التعامل مع هذه الجرائم إطلاع على الأمور التقنية وكيفية التعامل معها ومعرفة المبادئ الأساسية للتعامل مع الأدلة الإلكترونية[4]، فبعض الجرائم التي التي ترتكب بالوسائل الإلكترونية تقتضي البحث في ذاكرة الأقراص الصلبة وغيرها من مستخرجات هذه

---

[1]- Algérie vulnérable face à la cybercriminalité, le 02/08/2008,disponible à l'adresse suivante : www.bladi-dz.com.

[2]- د. أحمد شحاتة بيومي، الجرائم الماسة بالحياء عبر وسائل الإتصال المستحدثة، رسالة دكتوراه، كلية الدراسات العليا بأكاديمية الشرطة، مصر، سنة 2009، 2009، ص 254.

[3]- Eric Caprioli, Traçabilité et droit de la preuve électronique, Mai 2001, disponible à l'adresse suivante : www.caprioli-avocats.com.

[4]- د. سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الإنترنت، رسالة دكتوراه، كلية الحقوق ، جامعة الإسكندرية، مصر، سنة 2008، ص338.

الوسائل، كما قد يستخدم المجرم المعلوماتي الوسائل الإلكترونية ذاتها في ارتكاب بعض الجرائم كالتزوير مثلا، الأمر الذي يتطلب حرص وعناية فائقة أثناء البحث عن الدليل حتى لا يصيبه التلف أو التشويه أو التحريف.

ولا شك أنّ التطور الذي وصلت إليه ثورة الإتصالات سيترتب عليه نشوء أدلة تتمتع بحقيقة علمية،وممّا يؤكد ذلك أنّ وسائل الإتصال الحديثة التي تمخض عنها التقدم العلمي تم تزويدها بأنظمة مراقبة يمكن من خلالها اكتشاف أي خلل أو تلاعب في البرنامج أو في عمل الجهاز ذاته، وهذه التقنية لا تقبل المحو أو التعديل[1].

ويفتقر الدليل الإلكتروني إلى تلك الطبيعة التي تميز الأدلة المعروفة في العالم المادي، فهو يقبع في عالم افتراضي وجوده كله مبني على مفاهيم معنوية غير ملموسة، كما أنّه يحتاج إلى مجال تقني يتعامل معه، وإذا كان الدليل العلمي له منطقه الذي يجب ألاّ يخرج عليه من حيث ضرورة عدم تعارضه مع القواعد العلمية الثابتة، فإنّ للدليل الإلكتروني ذات الطبيعة إذ يجب ألاّ يخرج الدليل عمّا توصل إليه العلم الرقمي وإلا فقد معناه[2].

فالتطور التقني صاحبه تطور في طرق إثبات الجريمة الإلكترونية والتعامل معها، فالجرائم العادية يسهل غالبا تحديد مكان ارتكابها، بل أن ذلك يعتبر خطوة أولى وأساسية لكشف ملابسات الجريمة، في حين أنه من الصعوبة بمكان تحديد مكان وقوع الجريمة عند التعامل مع الجرائم الإلكترونية، وذلك لكون الرسائل وملفات الكمبيوتر تنتقل من نظام إلى آخر في ثوان قليلة، كما أنه لا يقف أمام تنقل الملفات والرسائل أية حدود دولية أو جغرافية.

وبناءا على ذلك، ينبغي على الأجهزة الأمنية إتباع معايير محددة وليس الإعتماد فقط على خبرات سابقة من قضايا مختلفة، لأن استخلاص الأدلة الشرعية و القانونية يتطلب إتباع أساليب محددة لا تسمح بأي انحراف أو تعديل يؤدي في النهاية إلى القبض على الجناة وتقديمهم للمحاكمة، خاصة وأن الكثير منهم لديهم معرفة محدودة بالمهارات الفنية التكنولوجية[3].

والدليل الإلكتروني يعدّ دليلا متطورا لأنه نتاج وسائل إلكترونية متطورة، وليس المقصود بتطور الدليل إكتشاف أدلة جديدة، وإنما المقصود بذلك تطور مصادر الحصول عليه بما يتفق مع طبيعة الجريمة والتي

1-أ. محمد حسين علي محمود، التزوير باستخدام الوسائل الإلكترونية،مذكرة ماجستير، كلية الحقوق، جامعة القاهرة، مصر، سنة 2011،ص207.

2- د. أحمد شحاتة بيومي،المرجع السابق،ص 255.

3- د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 13-ص 156.

يكون هذا الدليل أداة لإثباتها وإسنادها إلى مرتكبيها، ولذلك نجد أن الدليل لا يأتي على صورة واحدة بل يوجد له العديد من الصور والأشكال[1].

وبناء على ذلك، يتطلب البحث في ماهية الدليل الإلكتروني، التعرض إلى مفهوم الدليل الإلكتروني في المطلب الأول، أمّا المطلب الثاني فخصص لمصادر الحصول على الدليل الإلكتروني.

المطلب الأول: مفهوم الدليل الإلكتروني.

إنّ الطبيعة الفنية والتقنية لهذه النوعية من الجرائم نتج عنها نوع خاص من الأدلة، إذ أنّ الدليل هو الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها، أي كل ما يتعلق بالوقائع المطروحة عليه لإعمال حكم القانون عليها، فبدون الدليل لن تثبت الجريمة ولن تسند إلى متهم وبالتالي لن يطبق قانون العقوبات.

وإذا كانت الأدلة التقليدية تقوى بسهولة على إثبات الجرائم عامة، إلا أنها قد لا تقوى على إثبات الجرائم التي ترتكب بالوسائل الإلكترونية، فهذه الوسائل سواء كانت أداة في ارتكاب الجريمة، أم كانت محلا لها تساعد على إخفاء الآثار التي تترتب عليها، ممّا يعوق الحصول على الدليل الإلكتروني[2]، إلا أنه لمتابعة التطور المستمر للتكنولوجيا لابد من وضع استراتيجية محكمة عند تخزين البيانات الإلكترونية حتى لا تنتهك الحياة الخاصة للأفراد[3]، وعليه فلابد من التطرق إلى مفهومه وذلك من خلال تعريف الدليل الإلكتروني، وبيان طبيعته وخصائصه ليتم التطرق بعد ذلك لتقسيمات الدليل الإلكتروني على النحو التالي:

الفرع الأول: تعريف الدليل الإلكتروني.

سوف يتم توضيح مفهوم الدليل الجنائي بصفة عامة، وذلك بهدف التعرف على الدليل الإلكتروني، إذ يتعذّر علينا فهمه دون التطرق للدليل الجنائي التقليدي.

---

[1]– د. علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات العربية المتحدة، سنة 2003، ص 39.

[2]– نفس المرجع ، ص 33.

[3]- Peter Vakof, Administration de la preuve électronique, disponible à l'adresse suivante : www.pwc.com/ca/fr/risk/forinsic-technologie/e-discovery.html.

البند الأول: الدليل الجنائي التقليدي.

أولا: الدليل لغة: هو المرشد وما يتم به الإرشاد، وما يستدل به، والدليل هو الدال أيضا،والجمع أدلة ودلالات[1]، وورد في مختار الصحاح أنّ الدليل ما يستدل به، وقد دله على الطريق أي أرشده، يدله بالضم، دلالة بفتح الدال وكسرها، ودلولة بالضم والفتح أعلى، ويقال أدل، والإسم الدال بتشديد اللاّم ، فلان يدل فلانا أي يثق به، قال أبو عبيد: الدال قريب المعنى من المعنى الهدى وهما في السكينة والوقار والهيئة والمنظر وغير ذلك[2] .

ثانيا: الدليل اصطلاحا: هو ما يلزم من العلم به العلم بشيء آخر، وإسم الدليل يقع على كل ما يعرف به المدلول حسيا كان أو شرعيا، قطعيا كان أو غير قطعي،حتى سمي الحس والعقل والنص والقياس وخبر الواحد وظواهر النصوص كلها أدلة[3] .

أما الدليل في الإصطلاح القانوني، فقد تعددت المحاولات الفقهية في وضع تعريف له، فقد عرفه بعض الفقهاء[4] بأنه: "الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها، والمقصود بالحقيقة في هذا السياق، هو كل ما يتعلق بالوقائع المعروضة أمام القاضي لإعمال حكم القانون عليها".

ويعرف كذلك على أنّه الحجية التي تستخلص من واقعة، أو ظاهرة مادية أو معنوية متعلقة بالجريمة، بحيث يولد ظهورها الإقتناع الكافي بوقوع الجريمة، أو واقعة من وقائعها وإسنادها إلى المتهم،أو نفي ذلك، وهو الوسيلة الإثباتية المشروعة التي تسهم في تحقيق حالة اليقين لدى القاضي بطريقة سائغة يطمئن إليها، وأن يؤدي عقلا إلى ما رتبه عليها من أحكام[5].

وذهب الفقيه الإيطالي "جولياني" إلى أنّ الدليل هو المجادلة والنقاش الذي كانت البلاغة تلعب دورا كبيرا لبيان صحة أو عدم صحة أمر ما في منازعة أو خصومة، وأنه الحقائق أو العناصر التي تشكل بداية

1- د. جميل صليبا، المعجم الفلسفي،دار الكتاب اللبناني، بيروت، ط1، سنة 1970، ص23. نقلا عن: د.طارق فوزي الفقي، الجوانب الإجرائية في الجرائم المعلوماتية (دراسة مقارنة)، رسالة دكتوراه ،كلية الحقوق، جامعة المنوفية، مصر، سنة 2011، ص 79.

2- د. محمد بن أبي بن عبد القادر الرازي، مختار الصحاح، المطبعة الأميرية، القاهرة، مصر، 1338 هـ، ص 209. نقلا عن : د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق،ص 161.

3- د. ناصر بن محمد البقمي، المرجع السابق، ص 23.

4- د. طارق فوزي الفقي، المرجع السابق، ص 79.

5- د. ناصر بن محمد البقمي، المرجع السابق، ص 23.

البحث عن الحقيقة في أي بحث جنائي وتؤدي إلى الإقتناع الفعلي إلى جانب قنوات أخرى من الملاحظة والتجربة"[1].

ويعرف الدليل بأنه:" أي شيء يفيد في إثبات أو نفي مسألة معينة في القضية،أو كل ما يتصل إتصالا مباشرا بإدانة المتهم أو تبرئته، إستنادا إلى المنطق، ويجب التركيز على كلمة أي شيء لأنّ أي شيء بالمفهوم الواسع يمكن أن يكون دليلا"[2] .

وبالإستناد إلى تعريف بعض الفقهاء يمكن استخلاص أن الدليل الجنائي هو الحجة أو البينة المبنية على الإقتناع الذاتي المنبثق من واقعة مادية أو معنوية متعلقة بالجريمة أي لها علاقة بالواقعة المراد كشف حقيقتها، بحيث تترك هذه الوقائع إقتناع لدى القاضي بحقيقتها وما يتصل بها، وبالتالي إسناد الجريمة إلى متهم معين بذاته أو نفي ذلك، سواء كان ذلك بطريق مباشر أو غير مباشر[3].

ثالثا: تمييز الدليل الجنائي.

سيتم التفرقة بين الدليل الجنائي كوسيلة إثبات وبين ما قد يختلط به من وسائل إثبات الأخرى، وذلك على النحو التالي:

1. الدليل وإجراءات الحصول عليه:

يشمل الدليل كل واقعة مادية أو معنوية تؤدي إلى إثبات وقوع الجريمة أو تحديد شخصية مرتكبها، أو إثبات إرتكابه لها، سواء تم ذلك مباشرة أو عن طريق غير مباشر، وهو الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة بالإعتماد على الدليل الذي يمثل أثرا منطبعا في نفس أو في شيء أو متجسما في شيء ينمّ عن ارتكاب جريمة وقعت في الماضي أو تقع في الحاضر وعلى شخص معين تنتمي هذه الجريمة إلى سلوكه.

أمّا إجراءات الحصول على الدليل فلا تعد أدلة،وإنما هي المصدر الذي يتم عن طريقه الحصول على الدليل، مثل المعاينة، التفتيش، الخبرة، والإستجواب وما إلى ذلك من إجراءات، وهي بالمعنى القانوني لا تعد أدلة، ولكنها قد تسفر عن أدلة تسهم في الإثبات وتتفق مع الأدلة في عدم تحديدها على سبيل الحصر ولكنها تخضع للضوابط القانونية لكيفية تطبيقها وحدود سلطات القائمين على تنفيذها.[4]

---

[1]- د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 161.

[2]-د. سامح أحمد بلتاجي موسى، المرجع السابق،ص67.

[3]- مشار إليه عند:د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 162.

[4]- د ناصر بن محمد البقمي، المرجع السابق، ص 29.

2. الدليل والإثبات:

يخلط البعض أحيانا بين الدليل الجنائي وبين عملية الإثبات ذاتها لما بينهما من علاقة في نطاق الإجراءات القضائية، ولكن في الواقع يمكن الفصل بين الدليل وبين الإثبات، فالدليل يتكون من حقائق متنوعة تقدّم للمحكمة ولكن نتيجتها هي الإثبات، والإثبات هو مجموعة الأدلة المقدمة في الدعوى سواء لإدانة أو لتبرئة المتهم، فالإثبات أكثر عمومية ويشمل مجموعة الإجراءات الشكلية والموضوعية والقواعد اللازمة لكشف الحقائق وتحقيق العدالة الجنائية[1].

3. الدليل والدلائل أو الأمارات:

يفضي الدليل الجنائي وما ينجم عنه من استنتاجات بثبوت الواقعة ونسبتها إلى المتهم، كما يساعد القاضي في تحديد الحقيقة على وجه الجزم واليقين، ويستعين به للوصول إلى اليقين القضائي، أمّا الدلائل فلا ترقى إلى مستوى الدليل لأنّ الإستنتاج المبني عليها لا يصل إلى حد الجزم واليقين وإنّما يبنى على الإحتمالات ووجود أكثر من تفسير للواقعة[2]، فالأمارة أو الدلالة هي استنتاج واقعة من واقعة أخرى على سبيل الإحتمال أو الإمكان، وبالتالي لا يمكن الإستناد عليها وحدها في الإثبات، وهي تعد أضعف من القرائن في صلتها بالواقعة المراد إثباتها، فهي وإن صلحت لأن يقام عليها اتهام، إلاّ أنّها لا تصلح لأن يبنى عليها حكم قضائي بالإدانة، لأنها لا تصلح لأن تؤدي إلى اليقين القضائي الذي يجب أن يبنى عليه حكم الإدانة.

4. الدليل والأثر:

الأثر هو كل شكل أو صورة أو مادة أو علامة يتركها الجاني على جسم آخر، من شأنها أن تدل عليه أو ترشد عن بعض خواصه أو مميزاته أو على الدور الذي قام به، فالأثر هو كل ما يتركه الجاني في محل الجريمة أو في الأماكن المحيطة أو المجاورة أو في الأماكن المتصلة به، وقد لا يشير الأثر إلى شيء فمجرد وجود بصمات أصابع أو آثار أقدام أو بقعة دم في محل الجريمة هو أثر، وحتى يتم فحصه والتعرف على مدلوله فإنه يصبح حينها دليلا ، فالأثر مرحلة سابقة يمكن أن يتحول إلى دليل[3].

1- د. محمد الأمين البشرى، المرجع السابق، ص 232. نقلا عن: د. سامح أحمد بلتاجي موسى، المرجع السابق،ص 373.

2- د . ناصر بن محمد البقمي، المرجع السابق، ص 29.

3- د. محمد الأمين البشرى، المرجع السابق، ص 233. نقلا عن: د. سامح أحمد بلتاجي موسى ، المرجع السابق،ص 373.

رابعا: أقسام الدليل الجنائي.

ما يهم في هذا المقام هو تقسيم الدليل من حيث مصدره، فهو الأساس الذي تقام عليه المقارنة بين الدليل الجنائي والدليل الإلكتروني.

1. الأدلة المباشرة:هي التي تنصب على الواقعة مباشرة، مثل: شهادة الشهود واعتراف المتهم، وتنقسم الأدلة المباشرة من حيث مصدرها إلى ثلاثة أقسام: مادية وقولية وفنية.

أ– الأدلة المادية: هي التي تنبعث من عناصر مادية ناطقة بنفسها وتؤثر في اقتناع القاضي بطريق مباشر، فهي أقوى أثرا في الإقناع ومصدر هذه الأدلة غالبا هو المعاينة والتفتيش.

ب– الأدلة القولية: هي التي تنبعث من عناصر شخصية تتمثل فيما يصدر من الغير من أقوال، ويتوقف إقتناع القاضي بها على اقتناعه بصدق هذا الغير فيما يصدر عنه من أقوال مثل الشهادة والإستجواب والإعتراف.

ج– الأدلة الفنية:هي التي تنبعث من رأي خبير فني بناء على معايير علمية، يدور حول تقدير مادي أو قولي قائم في الدعوى، فالخبرة بخلاف الشهادة ليس نقلا لصورة معينة في ذهن الشاهد بأحد حواسه،وإنما هي تقدير فني لواقعة معينة بناء على معايير علمية[1].

2. الأدلة غير المباشرة: تنقسم إلى نوعين: القرائن والدلائل.

أ. القرائن : تتحقق باستنتاج مجهول من معلوم وذلك باستنباط الواقعة المجهولة المراد إثباتها من واقعة أخرى ثابتة، وهذا الإستنباط يقوم إمّا على افتراض قانوني أو على صلة منطقية بين الواقعتين، وفي الحالة الأولى تعتبر القرينة قانونية وفي الحالة الثانية تعتبر القرينة قضائية[2].

ب. الدلائل: فهي وإن اتفقت مع القرائن القضائية فهي استنتاج للواقعة المجهولة المراد إثباتها من واقعة أخرى ثابتة، إلا أنّها تختلف عنها في قوة الصلة بين الواقعتين، ففي القرائن القضائية يجب أن تكون الصلة متينة لازمة في حكم العقل والمنطق، بحيث يتولد الإستنتاج من هذه الصلة بحكم الضرورة المنطقية ولا تحتمل تأويلا مقبولا غيره[3]، أمّا الدلائل فإنّ الصلة بين الواقعتين ليست قوية ولا حتمية، ولهذا فإنها وإن كانت تصلح أساسا

---

[1]– د.جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مصر، العدد الأول، يناير 2007،ص 15.

[2]– د.محمد فتحي، المرجع السابق، ص 329.

[3]–د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، بدون طبعة ، سنة 1981، ص 495.نقلا عن : د. محمد فتحي ، المرجع السابق، ص 330.

للإتهام، إلاّ أنّها لا يمكن أن تكون وحدها أساسا للحكم بالإدانة بل يجب أن تتأكد بأدلة أخرى مباشرة أو غير مباشرة[1].

البند الثاني: الدليل الإلكتروني.

بعد التطرق لتعريف الدليل الجنائي بصفة عامة سيتم تعريف الدليل الإلكتروني بصفة خاصة،ولقد تعددت التعاريف التي قيلت بشأن الدليل الإلكتروني، ومن بين هذه التعاريف ما يلي:

يعرفه البعض[2]بأنه:" الدليل المأخوذ من أجهزة الحاسب الآلي، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء.

ويعرّف كذلك بأنه:" معلومات ذات قيمة برهانية أو استدلالية تم تخزينها أو نقلها بشكل رقمي".

وهو أيضا: "المعلومات والبيانات ذات القيمة الإستقصائية والمخزنة أو المنقولة عبر جهاز إلكتروني"[3].

وبتعريف آخر هو معلومات يقبلها العقل والمنطق ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الإتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة وجان أو مجني عليه".[4]

كما يعرّف على أنه:"أي معلومة محررة أو مخزنة في شكل معالج رموز أو أرقام، حيث يستخدمها الحاسوب في إنجاز مهمة ما".

1- د. محمد فتحي، المرجع السابق، ص 330.كما أنّ الأدلة الجنائية تقسم من حيث وجه الإلزام إلى أدلة قضائية وأدلة قانونية، ومن حيث الكفاية لتقرير الإدانة إلى دليل كامل ودليل ناقص، ومن حيث إثبات أو نفي التهمة إلى أدلة إثبات وأدلة نفي التهمة، ومن حيث وعاءها ومصدرها إلى أدلة مادية وأدلة معنوية. ولمزيد من التفاصيل راجع: د. رمسيس بهنام، الإجراءات الجنائية (تأصيلا وتحليلا)، منشأة المعارف، الإسكندرية، مصر، بدون طبعة، سنة 1984، ص226.

2- د. عبد الناصر محمد محمود فرغلي، الإثبات العلمي لجرائم تزييف وتزوير المحررات التقليدية والإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، سنة 2010، ص 120.

3- د. محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 341.

4- د. محمد الأمين البشرى، المرجع السابق، ص 234. نقلا عن : أ. عائشة بن قارة ، المرجع السابق،ص 53.

أمّا الأستاذ "Eogahan Casey" فقال أنّ:" الدليل الجنائي يشمل جميع البيانات الرقمية التي يمكن أن تثبت أنّ جريمة قد ارتكبت أو يمكن أن توجد صلة بين جريمة ومرتكبيها، وبين الجريمة والمتضرر منها"[1].

ويعرف أيضا الدليل الإلكتروني بأنه:" كل ما يستمد من النظم الحاسوبية والوسائل التقنية بطريقة فنية من صور ورسومات أو نصوص مكتوبة أو أصوات أو مواد فيلمية وغيرها، ويتم الوصول إليه والحصول عليه بطريقة قانونية، وعن طريقه يمكن إثبات أو نفي العلاقة بين المتهم وبين الجريمة الواقعة، أو إثبات ونفي العلاقة بينه وبين المجني عليه بما يعين القاضي للوصول إلى حقيقة الواقعة فيقضي إمّا ببراءة المتهم أو بإدانته[2].

في حين عرفه البعض الآخر[3] أنه: "الدليل الذي يجد له أساسا في العالم الإفتراضي ويقود إلى الجريمة".

كما عرفت المنظمة الدولية لأدلة الحاسب (I O C E) هذا الدليل بأنه:"معلومات مخزنة أو منقولة بشكل يمكن قبوله في المحكمة"[4].

أما مجموعة العمل الدولية حول الدليل الرقمي S W G D E فقد عرفته بأنه: "أية معلومات ذات قيمة مخزنة أو منقولة بشكل رقمي"[5].

كما يعرف بأنه:" برامج الحاسوب وبياناته التي تستخدم للإجابة عن الأسئلة الهامة حول الحادثة الأمنية"[6].

---

[1]- Eogahan Casey, Computer & internet crime, available on line in february 2001, at : www.forensic-science.com.

نقلا عن :د. عائشة بن قارة، المرجع السابق، ص 54.

[2]– د. سامح أحمد بلتاجي موسى، المرجع السابق،ص 376.

[3]– د. عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق،ص 590.

[4]– المنظمة الدولية لأدلة الحاسوب (I O C E) International Organisation Of Computer Evidence: هي منظمة تزود الجهات الدولية القانونية بكيفية تبادل المعلومات المتصلة بتحقيقات جرائم الحاسوب ومسائل ذات صلة بالجانب المعلوماتي، أنظر الموقع الإلكتروني:www.ioci.org.

[5]– مجموعة العمل الدولية حول الدليل الرقمي (S W G D E) Scientfic Working Group On Digital Evidence ومقرها الولايات المتحدة الأمريكية، مهمتها توحيد المقاييس الدولية للدليل الرقمي فبراير سنة 1998 من خلال التعاون مع مدراء مختبرات الجريمة الفيدرالية وتطوير معايير حفظ وفحص الدليل الرقمي. أنظر الموقع:www.swegde.org. نقلا عن: د. طارق عبد الرؤوف الخن، المرجع السابق، ص 341.

[6]–نقلا عن: نفس المرجع، ص 341.

بعد استعراض التعريفات التي قيلت بشأن الدليل الإلكتروني، فهي قد تباينت بين التوسيع والتضييق مع اختلاف وجهات النظر بين الباحثين في مجال التقنية،والباحثين في المجال القانوني، فالتعاريف كانت متقاربة من بعضها البعض، إلا أنه تم تسجيل بعض الملاحظات من قبل بعض الفقهاء:

1.هناك خلط في تعريف الدليل الإلكتروني بمفهوم برامج الحاسب الآلي، حيث تم اعتبار هذا الدليل كبيانات يتم إدخالها إلى جهاز الحاسوب وذلك لإنجاز مهمة ما.

2.قد يتفق المصطلحان في أن كليهما يعدا آثارا معلوماتية أو رقمية، حيث يتركهما كل مستخدم للنظام المعلوماتي، ويتخذ شكلا واحدا هو الشكل الرقمي لأن البيانات داخل الكمبيوتر سواء كانت في شكل نصوص أو أحرف أو أرقام أو صور تتحول إلى طبيعة رقمية.

غير أن الفرق بين الدليل الإلكتروني وبرامج الحاسوب يكمن في الوظيفة التي يؤديها كل واحد منهما، فهذا الأخير له دور في تشغيل الحاسوب وتوجيهه إلى حل المشاكل، وبدونها لا يمكن أن يكون إلا آلة صماء كباقي الآلات.

أمّا الدليل الإلكتروني فله أهمية كبيرة في إثبات الجرائم الإلكترونية ونسبتها إلى مرتكبيها غير أن هذا الدليل يمكن استخدامه في إثبات أو نفي الجرائم التقليدية أيضا، كالإتجار بالمخدرات، جرائم القتل والإختطاف التي تستخدم فيها التكنولوجيا الرقمية كأداة لتسهيل تنفيذ الجرائم بسرعة وكفاءة قد تفوق قدرات جهات التحقيق.

3.إن جل التعريفات حصرت مصادر الأدلة الإلكترونية في أجهزة الحاسب الآلي وملحقاته فقط، إلا أن هناك نظم أخرى مدمجة بالحواسيب قد تحتوي على العديد من الأدلة الإلكترونية كالهواتف المحمولة على سبيل المثال، فقد أصبحت هذه الأخيرة مصدر التهديد الأكبر والهدف المفضل لدى العديد من مجرمي المعلوماتية نتيجة لسهولة استعمالها في انتهاك حرمة الحياة الخاصة[1]، وإن كان البعض[2] يرى أن التهديد الأكبر يأتي من الأجهزة النقالة فهذه الأخيرة زادت من تعقيد الوضع.

وبناءا على ذلك حاولت إعطاء تعريف للدليل الإلكتروني بأنه:" أي معلومات مخزنة في الحاسب الآلي أو وسائل إلكترونية أخرى يتم الحصول عليها من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد ترجمتها من أشخاص متخصصين في هذا المجال، وذلك لإثبات وقوع الجريمة الإلكترونية" .

---

[1]– نقلا عن: أ. عائشة بن قارة، المرجع السابق، ص 55 وما بعدها وكذلك: د. طارق فوزي الفقي، المرجع السابق، ص 82 وما بعدها.

[2]–Mathieu Olivier, Cybercriminalité : pourquoi l’Afrique doit faire face ?, le 21/02/2014, disponible à l’adresse suivante :www.jeuneafrique.com.

الفرع الثاني: طبيعة الدليل الإلكتروني.

لاشك أن التطور الحالي لثورة الإتصالات سينعكس أثره على الأدلة المتحصلة من الوسائل الإلكترونية، بحيث يجعل الحقيقة التي ستتولد منها تقترب إلى الحقيقة العلمية،وهذا يفرض عند تقدير قيمة هذه الأدلة في الإثبات الجنائي تقريب هذه الحقيقة العلمية مع الحقيقة القضائية، بحيث أنّ الأولى تساعد الثانية في إثبات حقيقة وقائع محددة ومدى نسبتها إلى متهم معين[1].

ومن هنا تبدو أهمية طبيعة الدليل الإلكتروني الذي يتطلب وسائل علمية للتعامل معه واستنتاجه، كما يتطلب تطوير قدرات من يتعامل مع هذا الدليل من محققين وخبراء، ومن خلال ذلك تتطور الحقيقة القضائية وتستطيع أن تجعل الحقيقة العلمية حقيقة عادلة تقوم على أسس علمية ذات نتائج محددة ودقيقة وواضحة[2].

ونظرا لطبيعة الجرائم الإلكترونية والأدلة المتعلقة بها، الأمر الذي يدعو للتساؤل عن أي نوع من أنواع الأدلة ينتمي الدليل الإلكتروني؟ فهل يعتبر دليل مادي ناتج عن عناصر مادية ملموسة، أم أنه ينتمي إلى الأدلة الفنية نتيجة لاستنتاجه من رأي خبير فني؟أو له طبيعة من نوع خاص؟

للإجابة عن هذه التساؤلات ، فقد ظهرت عدة إتجاهات:

الإتجاه الأول:

يرى أنصاره أنّ الأدلة الإلكترونية ما هي إلاّ مرحلة متقدمة من الأدلة المادية الملموسة التي يمكن إدراكها بإحدى الحواس الطبيعية إذا ما كانت على شكل مطبوعات مستخرجة من الحاسوب، فالأدلة الإلكترونية في منظور هذا الإتجاه لا تختلف من حيث المفهوم والقيمة عن آثار الأسلحة وبصمات الأصابع والبصمة الوراثية وغيرها من الأدلة العلمية[3].

---

[1]–د. علي محمود علي حمودة، المرجع السابق،ص 34.

[2]–د. ناصر بن محمد البقمي، المرجع السابق،ص 40.

[3]– د. طارق فوزي الفقي، المرجع السابق، ص 90.

الإتجاه الثاني:

إنّ بعض الفقهاء[1] حدّدوا حالات من الأدلة لا تعتبر دليلا ماديا وهي الأدلة المستمدة من:

1. الوسائل التي تمس سلاسة جسم الإنسان وصحته النفسية وتكشف أسراره الوجدانية مثل: جهاز كشف الكذب والتنويم المغناطيسي واستخدام جهاز رسم المخ الكهربائي.

2. الوسائل السمعية البصرية التي قد يترتب على استخدامها تعدي على الحياة الخاصة للإنسان كمراقبة المحادثات الهاتفية وأجهزة التنصت، واستبعاد هذه الأدلة يقوم على أساس أنها لا تعتبر أثرا ماديا ملموسا وإن استندت على وسائل علمية بغض النظر عن موقف الفقه القانوني من مشروعيتها، وبالتالي الدليل الإلكتروني ينطبق عليه نفس الأساس بحيث يعتبر مجرد نبضات كهرومغناطيسية غير ملموسة لا تدرك بالحواس العادية بل يتطلب إدراكها الاستعانة ببرامج وتطبيقات خاصة[2].

الإتجاه الثالث:

يرى هذا الإتجاه أنّ الدليل الإلكتروني هو دليل علمي فني يتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة لا تدرك بالحواس العادية، بل يتطلب إدراكها الإستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية، فهو يحتاج إلى مجال تقني يتعامل معه ولأجل ذلك فإنّ ما ينطبق على الدليل العلمي ينطبق على الدليل الإلكتروني[3].

الإتجاه الرابع:

يرى هذا الإتجاه أنّ الأدلة الإلكترونية تنتمي بطبيعتها إلى القرائن التي تعد من أهم الأدلة المؤثرة في الدعوى الجنائية، ومادام أنّ القرائن تتحقق باستنتاج مجهول من معلوم، وبتطبيق ذلك على الدليل الإلكتروني فنجد أنّ دليل الإدانة يتجه بالضرورة إلى حائز أو مالك الحاسب الذي يحتوي قرصه الصلب على دلالة القيام بجريمة انتهاك أو اختراق شبكات الغير، هذه الإشارة هي ما تسمى بالقرينة إذ يستدل على ارتكاب الحائز للجريمة (العلة المجهولة) من خلال وجود جهات إلكترونية له، وهي (العلة المعلومة)[4].

1- د.أحمد أبو القاسم أحمد، الدليل المادي وأهميته في الإثبات الجنائي،دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 1991،ص 17.نقلا عن: أ. عائشة بن قارة ، المرجع السابق، ص68.

2- عائشة بن قارة، المرجع السابق،ص 69.

3- د.طارق فوزي الفقي، المرجع السابق،ص85.

4- د. منى فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات (صورها ومشاكل إثباتها) ، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، سنة 2009، ص 137.

ويرى الفقهاء[1] حول طبيعة الدليل الإلكتروني أنه نظرا للتغير الذي طرأ على طبيعة الدليل الجنائي، وظهور الدليل الإلكتروني الذي يرتبط بالبيئة التقنية،أصبح للأدلة الإلكترونية خاصية تختلف عن الأدلة الجنائية التقليدية المتعارف عليها من حيث مكان وجود الدليل والبيئة التي تحكمه، كل هذه الأسباب تؤدي إلى القول أن الدليل الإلكتروني له طبيعة خاصة لأنّ له من الخصائص ما يجعله دليل مستقل يضاف إلى أدلة الإثبات المادية، القولية والعلمية أو الفنية.

الفرع الثالث: خصائص الدليل الإلكتروني.

إنّ خصوصية الجريمة الإلكترونية فرضت ظهور نوع جديد من الأدلة يتماشى مع طبيعتها، ويتميز هذا الدليل الإلكتروني بما يلي:

أولا: الدليل الإلكتروني من طبيعة تقنية.

ينبغي أن يكون هناك توافق بين الدليل المرصود وبين البيئة التي يستمد منها، ولا وجود للدليل الإلكتروني خارج بيئته التقنية التي تتطور بطبيعتها، هذا التطور الذي يكاد يكون تلقائيا يتمتع بإمكانية ظهور أدلة جديدة ومتطورة ومتجددة، وهذا يؤدي بدوره إلى صعوبة اكتشافها والوصول إليها، فهو ليس بدليل مرئي يمكن فهمه لمجرد القراءة ويتمثل في بيانات غير مرئية لا تفصح عن شخصية معينة[2].

ونتيجة للطبيعة التقنية للدليل الإلكتروني، فإنه يتميز عن الدليل الجنائي التقليدي بما يلي:

1. **إمكانية النسخ:** بحيث يمكن نسخ الدليل الإلكتروني نسخة مطابقة للأصل تماما، بحيث يمكن إجراء الفحص المعلوماتي على هذه النسخة لتفادي خطر إتلاف النسخة الأصلية أثناء عملية الفحص، وهذه الميزة لا توجد في الأدلة التقليدية.
2. **إمكانية كشف التعديل:** فقد يتعرض الدليل الإلكتروني للتعديل المقصود من قبل الجاني، أو التعديل غير المقصود من قبل المحقق أو الخبير المعلوماتي أثناء عملية جمع الدليل، ويمكن كشف ذلك عن طريق استخدام برمجيات تقنية معينة، إضافة إلى إمكانية إجراء المقارنة مع النسخة الأصلية إن وجدت، مما يعني صعوبة إخفاء الجاني لجريمته أو التخفي منها[3].

---

[1]– د. ناصر البقمي، المرجع السابق، ص 37. وكذلك: د. طارق فوزي الفقي، المرجع السابق، ص 91.

[2]– د. ناصر بن محمد البقمي، المرجع السابق، ص 32. وفي نفس المعنى: د.أحمد وهدان ، تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت، مجلة الفكر الشرطي، مركز بحوث الشرطة، الشارقة، الإمارات العربية المتحدة، العدد 1، أبريل 2004، ص 99.

[3]– د. طارق عبد الرؤوف الحن ، المرجع السابق،ص 343.

3. **إمتيازه بالسعة التخزينية العالية:** فآلة الفيديو الرقمية يمكنها تخزين مئات الصور، وقرص صغير يمكنه تخزين مكتبة صغيرة[1].

ثانيا: الدليل الإلكتروني دليل علمي.

الدليل الإلكتروني يحتاج إلى مجال تقني يتعامل معه، فهو كدليل يحتاج إلى بيئته التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات، ولأجل ذلك فإنّ ما ينطبق على الدليل العلمي ينطبق على الدليل الإلكتروني، فالدليل العلمي يخضع لقاعدة لزوم تجاربه مع الحقيقة كاملة وفقا لقاعدة في القضاء المقارن هي قاعدة أنّ القانون مسعاه العدالة أمّا العلم فمسعاه الحقيقة، وإذا كان الدليل العلمي له منطقه الذي يجب ألاّ يخرج عليه من حيث أنّه يجب عدم تعارضه مع القواعد العلمية السليمة، فإنّ الدليل الإلكتروني له ذات الطبيعة وعدم الخروج عن متطلبات العلم الرقمي لا يعني أن هناك قواعد جامدة يرتبط بها الدليل الإلكتروني من حيث طبيعته العلمية، وإنما يجب الأخذ في الاعتبار أنّ العلم الرقمي هو علم متطور جدا، بل إنّه يجد ذاته في قدرته الكبيرة على التطور الذاتي المستمر[2].

ثالثا: تنوّع وتطوّر الدليل الإلكتروني.

وتعني هذه الخاصية أنه على الرغم من أن الدليل الرقمي في أساسه متحد التكوين بلغة الحوسبة والرقمية، فإنه مع ذلك يتخذ أشكالا مختلفة، فمصطلح الدليل الرقمي يشمل كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا، وبحيث يكون بينها وبين الجريمة رابط من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني[3]، حتى أنّ البعض[4] يرى أنّ هناك مرونة في التعامل مع الدليل الإلكتروني مقارنة بالدليل التقليدي، كما أن الإعتراف وقبول الأدلة الإلكترونية من شأنه أن يؤدي إلى ازدهار التجارة الإلكترونية.

وإذا كانت العلاقة أساسية بين البيانات الرقمية والدليل الإلكتروني لكون الأخير إنما هو القالب الذي يحتوي في داخله مجموعة البيانات الرقمية، فإن ذلك يعد تعبيرا عن اتساع قاعدة الدليل الإلكتروني، بحيث يمكنه أن يشمل أنواعا متعددة من البيانات الرقمية تصلح منفردة أو مجتمعة لكي تكون دليلا للإدانة أو للبراءة

1- د. هلال بن محمد بن حارب البوسعيدي، المرجع السابق،ص 253.

2-د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2009،ص 533.

3- د. عمر أبو بكر بن يونس، الدليل الرقمي، الجمعية العربية لقانون الإنترنت، مصر، ط1، سنة 2007، ص 45.

4- Peihao Yuan, l'admission de la preuve électronique dans le droit français et le droit chinois, le 30/03/2011, disponible à l'adresse suivante : www.m2bde.u-paris10.fr.

إذ يشمل هذا التنوع في البيانات الرقمية مظاهر عدة،كأن يكون هذا المحتوى معلومات متنوعة تتضمن نصوصا وصور ومرئيات[1].

رابعا: إعادة بناء المسرح الرقمي للجريمة.

الآثار الرقمية تشمل رؤية لمسرح الجريمة الحقيقي، ومسرح الجريمة الرقمي نفسه،فإذا كانت هناك جريمة حدثت فعليا في العالم الحقيقي واستخدم الكمبيوتر بطريقة ما في أحد أفعالها، فجهات التحقيق عليها أن تبحث في كلا المسرحين، المسرح الحقيقي والمسرح المعلوماتي الرقمي وتوجد ثلاثة أنواع من إعادة بناء الأدلة الإلكترونية وهي الأدلة الإلكترونية التي تم العبث فيها أو محوها والأدلة الإلكترونية الصحيحة وهناك نوع ثالث يطلق عليه الأدلة الإلكترونية الهامشية، ويلاحظ أنه من الضروري لإعادة بناء الدليل الإلكتروني أن يتم الإستعانة بهذه الأنواع الثلاثة فالأدلة الإلكترونية الصحيحة يتم من خلالها استخلاص المعلومات المتعلقة بالجريمة والمجرم من خلال البحث فيها، كما أنّ الأدلة الإلكترونية التي تم محوها أو العبث فيها يتم إعادة بنائها باستخدام برامج خاصة، أمّا الأدلة الإلكترونية الهامشية فهي أدلة تلعب دورا حاسما في إعادة ترميم الأدلة الممحوة أو التي تم العبث فيها.

وإعادة بناء المسرح الرقمي يعتمد على نوع الدليل الإلكتروني، ونوع الكمبيوتر ونظام التشغيل وإعدادات الكمبيوتر وبإصلاح الأدلة التالفة أو الممحوة وربطها بالأدلة الإلكترونية الصحيحة، وسد ثغراتها بالأدلة الإلكترونية الهامشية ويؤدي ذلك إلى ما يسمى بإعادة بناء مسرح الجريمة الرقمي[2].

خامسا: صعوبة التخلص من الدليل الإلكتروني.

هذه الميزة من أهم مزايا الدليل الإلكتروني على الإطلاق، بل يمكن القول بأنها الميزة التي يتمتع بها الدليل الإلكتروني دون غيره من الأدلة التقليدية، وهو بذلك يشبه الدليل العلمي المتعلق بالحمض النووي (A D N) إذ أن كليهما يصعب التخلص منهما[3].

فالأدلة الإلكترونية يمكن إظهارها بعد إخفائها، وإصلاحها بعد إتلافها، واسترجاعها بعد حذفها، حيث يوجد العديد من برامج الحاسوب التي يمكن من خلالها استعادة البيانات التي تم حذفها،ومما يزيد من صعوبة التخلص منها أنه يمكن استخراج نسخ مطابقة للأصل ولها ذات القيمة والحجية في الإثبات، كما أنّ

1- د. حسين بن سعيد الغافري، المرجع السابق،ص 534.

2- د. ناصر بن محمد البقمي، المرجع السابق، ص 33.

3- أ. عائشة بن قارة ،المرجع السابق، ص 63.

نشاط الجاني لمحو الدليل يشكل كدليل أيضا، فنسخة من هذا الفعل أي فعل الجاني لمحو الدليل يتم تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقا كدليل إدانة ضده[1].

الفرع الرابع: تقسيمات الدليل الإلكتروني.

لقد أصبح المجتمع المعلوماتي حقيقة واقعة وتعتمد المجتمعات المعاصرة في تسيير شؤونها على تقنيات الحاسب الآلي، ومن تمّ يتعين على جهات التحقيق مع تقلص الدور التقليدي للوثائق في الإثبات وازدياد كبير في كم المعلومات والتي تتكون في شكل أوعية غير ورقية، أن تتعامل في ممارستها لحق المجتمع في الدفاع عن كيانه ضد الإجرام مع أشكال مستحدثة من الأدلة غير المادية[2]، ولاشك أنه يوجد لها العديد من الصور والأشكال يمكن استعراضها كما يلي:

ينبغي الإشارة إلى أن هناك بعض الأدلة المادية التي لها قيمتها الخاصة في إثبات الجريمة الإلكترونية ونسبها لمتهم معين، ومن هذه الأدلة:

أولا: الأوراق.

قد يكون للأوراق دور حاسم في إثبات العلاقة بين صاحب الشأن والبرنامج الذي يمكن أن يثور نزاع بشأنه، فهذا الأخير يمر بعدة مراحل أثناء إعداده ويظهر في نسخة ورقية[3]، إذ نجد أنّ الكثيرين ممن يقوموا بطبع المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات[4]، وهذه النسخة الورقية يمكن اعتبارها الوجهة النظرية للبرنامج وهي مرحلة لا غنى عنها وذكاء صاحب الشأن وحرصه يظهران في احتفاظه بهذه النسخة الورقية، بحيث يمكن الرجوع إليها والإحتجاج بها على من ينازعه حقا يدعي أنّه صاحبه.

لذا يفضل أن تكون المطالبة بحماية ما مستندة إلى ما يدعمها أي إلى دليل يثبت الحق واللجوء إليها عند حدوث إعتداء ما أيا كان نوع تلك الإعتداءات التي قد تلحق بالبرنامج، فهذا الدليل يشترط فيه أن

1- أ. عائشة بن قارة ، المرجع السابق، ص 63.

2- د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار بهجة، الزقازيق، مصر، بدون طبعة، سنة 2009،ص10.

3-أ. عبير فؤاد عبد العزيز، الحماية الجنائية لبرامج الحاسب الآلي، مذكرة ماجستير، كلية الحقوق، جامعة القاهرة، مصر، سنة 2007، ص235.

4- أ. علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، المكتب الجامعي الحديث، القاهرة، مصر، بدون طبعة، سنة 2012، ص 36.

يكون مقروءا وقابلا للتوصيل للغير بقدر الإمكان، وهو ما يتحقق في النسخة الورقية التي تعتبر الركيزة الأكثر أمنا[1]، وبالتالي فهي تعتبر من الأدلة التي ينبغي الإهتمام بها في البحث عن الحقيقة، ومن هذه الأوراق:

1. أوراق تحضيرية يتم إعدادها بخط اليد كمسودة تصوير العملية التي يتم برمجتها.
2. أوراق تالفة تم طباعتها للتأكد من تمام الجريمة تلقى في سلة المهملات.
3. أوراق أصلية تطبع ويتم الإحتفاظ بها كمرجع أو لأغراض الجريمة.
4. أوراق أساسية وقانونية محفوظة في الملفات العادية أو دفتر الحسابات، ولها علاقة بالجريمة خاصة عند تقليد وتزوير هذه الأوراق بواسطة الحاسب الآلي[2].

ثانيا: جهاز الكمبيوتر وملحقاته.

وجود جهاز الحاسب الآلي هام جدا للقول بأنّ الجريمة الواقعة هي جريمة إلكترونية، وأنها مرتبطة بالمكان أو الشخص الحائز على الجهاز، ولأجهزة الحاسب الآلي أشكال وأحجام مختلفة وخبير الحاسبات الآلية وحده الذي يستطيع أن يتعرف على مواصفاتها بسرعة فائقة.

ثالثا: البرمجيات.

إذا كان الدليل الإلكتروني ينشأ باستخدام برنامج خاص ليس واسع الإنتشار، فإن أخذ الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل.

رابعا: المودم (Modem).

وهو الوسيلة التي تمكن أجهزة الحاسبات الآلية من الإتصال ببعضها البعض عبر خطوط الهاتف، وفي الوقت الحالي تطورت المودم لتكون أجهزة إرسال واستقبال فاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها.[3]

1- أ.عبير فؤاد عبد العزيز، المرجع السابق،ص 37.

2- د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت،المرجع السابق، ص17.

3- أ. علي عدنان الفيل، المرجع السابق،ص 37.

خامسا: وسائط التخزين المتحركة.

كالأقراص المدمجة (أقراص الليزر)[1]، أو الأقراص المرنة[2] والأشرطة المغناطيسية[3].

وتعد هذه الوسائط جزءا من الجريمة الإلكترونية حتى كانت محتوياتها عنصر من عناصر الجريمة، إضافة إلى الأقراص الصلبة التي تعد هي الأخرى وسيلة لتخزين المعلومات[4].

سادسا: المراشد (Manuals): والخاصة بالمكونات المادية والمنطقية للكمبيوتر والتي تفيد في معرفة التفاصيل الدقيقة لكيفية عملها.

سابعا: الطابعات: والتي قد تحتوي على ذاكرة تحتفظ ببعض الصفحات التي سبق طباعتها[5].

ثامنا: المصغرات الفيلمية: وتعرف أيضا بالميكروفيلم وهي عبارة عن أفلام فوتوغرافية يتم تصوير صفحات البيانات عليها مع تصغيرها إلى درجات متناهية في الصغر ويتم ذلك بسرعة هائلة.

تاسعا:مخرجات الشاشة أو وحدة العرض المرئي: وهي الوسيلة الطبيعية لعرض المعلومات بصفة مستمرة على مستخدم الحاسب وتظهر عليها المعلومات لحظيا، ولا يمكن حفظها من خلال هذا المصدر[6].

1- أقراص الليزر: هي أقراص تمتاز بسعة التخزين العالية، ولكن لم تصل بعد لسعة التخزين للقرص الصلب أو سرعته، وتبدو أهمية هذه الأقراص في الجريمة الإلكترونية في أنه يوجد مع جهاز الحاسب الآلي الشخصي (P.C) قدرا كبيرا من هذه الأقراص، ويدون على غلاف القرص بيانات توضح محتوياته، وهذه الأقراص لدى البنوك والشركات تعد بالآلاف لكن في التحقيق لن يعتدّ بالطبع بما دوّن على غلاف القرص من بيانات، بل سيتم إفراغ هذه الأقراص بمعرفة خبير ليقدم بيانات دقيقة أمام جهات التحقيق، ولا يشترط أن تضبط أقراص الليزر مع جهاز الحاسب الآلي، لكنها قد تضبط في مكان آخر ومع ذلك فهي جزء من ماديات الجريمة أو الدليل اللازم لإثباتها لما كانت محتوياتها عنصرا من عناصر الجريمة.أنظر في ذلك: د. عبد الفتاح بيومي حجازي،الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 22.

2- الأقراص المرنة: هي أقراص تستخدم لتخزين الملفات التي لا تحتاج حجم تخزين عالي، لأن حجمها التخزيني قليل. أنظر في ذلك: نفس المرجع،ص21.

3- الشريط المغناطيسي: عبارة عن شريط بلاستيك مغطى بمادة معدنية قابلة للمغنطة، وقد يكون ملفوفا على بكرة كبيرة مثل التي تستخدم في أجهزة التسجيل الصوتي، وقد يكون داخل علبة على هيئة شريط الفيديو أو شريط الكاسيت والفكرة التي تبنى عليها تسجيل البيانات على الشريط المغناطيسي مماثلة لتلك التي يبنى عليها تسجيل الأحاديث على شريط التسجيل الصوتي، فجميع الأشرطة الممغنطة بما رأس للقراءة والكتابة يسجل البيانات على شكل نقطة مغناطيسية على الشريط بشفرة خاصة تدل على البيانات المستخرجة من داخل الحاسب، كما يستطيع هذا الرأس الإحساس بوجود هذه النقطة ويقوم بإرسال النبضات الكهربائية المقابلة لشفرة البيانات من داخل الحاسب، كما يستطيع هذا الرأس الإحساس بوجود هذه النقطة ويقوم بإرسال النبضات الكهربائية المقابلة لشفرة البيانات داخل الحاسب.ويستخدم الشريط المغناطيسي في تخزين البرامج والملفات المتتالية، وتنظم المعلومات على الشريط على شكل وحدات خاصة تشكل كل وحدة منها حزمة، وحجم الحزمة يحدده مستخدم الجهاز، وقد جرى العمل على تخصيص الحزمة الأولى والأخيرة من الملف لتسجيل معلومات تعريفية عن الملف، أنظر في ذلك: د.هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة)،دار النهضة العربية، القاهرة، مصر، ط2،سنة 2008،ص 18.

4- الأقراص الصلبة: هي من أكثر وحدات التخزين إستخداما لسرعتها وكفاءتها العالية وحجم التخزين الكبير الذي توفره وتكون عادة مركبة داخل حافظة الجهاز. أنظر في ذلك: د. عبد الفتاح بيومي حجازي،الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص21.

5- أ.علي عدنان الفيل، المرجع السابق، ص 37.

6- د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص 20.

غير أنه يمكن تقسيم الدليل الإلكتروني إلى أربعة أقسام:

- الأدلة الإلكترونية الخاصة بأجهزة الكمبيوتر وشبكاتها.
- الأدلة الإلكترونية الخاصة بالإنترنت.
- الأدلة الإلكترونية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.
- الأدلة الإلكترونية الخاصة بالشبكة العالمية للمعلومات.

إلا أن هذا التقسيم للدليل الإلكتروني، وإن كان يتناسب مع تقسيم الفقه للجرائم عبر الكمبيوتر،إلا أنه لا يتناسب مع مفهوم التقنية الحديثة، فهذه التقسيمات تدور حول موضوع واحد ألا وهو الدليل الإلكتروني الخاص بجهاز الكمبيوتر وشبكاته، فاختلاف المصطلحات لا يعني إختلاف في المعنى[1].

كما يمكن تقسيم الدليل الإلكتروني إلى ثلاث مجموعات وهي كالتالي:

أولا: السجلات المحفوظة في الحاسوب: وهي الوثائق المكتوبة والمحفوظة مثل البريد الإلكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الإنترنت.

ثانيا: السجلات التي تم إنشاؤها بواسطة الحاسوب:تعتبر مخرجات برامج الحاسوب وبالتالي لم يلمسها الإنسان مثل Log fils وسجلات الهاتف وفواتير أجهزة السحب الآلي ATM.

ثالثا: السجلات التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه بواسطة الحاسوب: ومن الأمثلة عليها أوراق العمل المالية التي تحتوي على مدخلات تم تلقيها إلى برامج أوراق العمل مثل Excel، ومن تم تمت معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها[2].

ويلاحظ أن التنوع في الدليل الإلكتروني يفيد بالضرورة أنه ليس هناك وسيلة واحدة للحصول عليه بل وسائل متعددة، وفي كل الأحوال يظل الدليل المستمد منه رقميا حتى وإن اتخذ هيئة أخرى،كما يلاحظ على هذا التقسيم أنه ليس شامل للدليل الإلكتروني بل اقتصر على نوع محدد منه، وهي سجلات الحاسوب[3].

---

[1]– د. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ط1، سنة 2006، ص88. نقلا عن: أ. عائشة بن قارة مصطفى، المرجع السابق، ص 71.

[2]– د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 179.

[3]– أ. عائشة بن قارة، المرجع السابق، ص 76. وكذلك : د. طارق فوزي الفقي، المرجع السابق، ص 97.

لقد تم استخلاص أن أية محاولة لتقسيم الدليل الإلكتروني، لابد أن يتم فيها مراعاة التطور اللامتناهي الذي تتميز به البيئة الرقمية والتي يستمد منها الدليل الإلكتروني.

المطلب الثاني: مصادر الحصول على الدليل الإلكتروني.

تتسم الجرائم الناشئة عن إساءة استخدام الحاسب الآلي بالطابع التقني، الأمر الذي يقتضي أن يستخدم في تحقيقها إلى جانب قواعد وأساليب التحقيق الجنائي الفني المعروفة وسائل تقنية خاصة وفريدة، كما يتطلب الأمر أن يكون من يتولى تحقيقها متخصصا في معالجة البيانات، والمراجعة والمحاسبة، ويوصي الخبراء باتباع قواعد فنية استرشادية لبلوغ أقصى قدر من النجاح من وراء التحقيقات، يبدو أبرزها في ضرورة إجراء تحريات أولية من خلال وسائل ومواصفات تتلاءم مع خصائص وطبيعة بيئة تقنية المعلومات، وذلك بغرض الحصول على أكبر قدر من المعلومات عن السلوك المكوّن للجريمة أو أسلوب وظروف ارتكابها، مع مراعاة الطبيعة الخاصة للدليل الإلكتروني التي لا تجعله متاحا إلا لفترة قصيرة من الوقت[1].

وهذا لا يتم إلاّ باستخدام الأجهزة الحديثة، ويبرز دور المعمل الجنائي الذي يستخدم كافة النظريات العلمية الحديثة في مجال مكافحة الجريمة والعلوم المساعدة الأخرى التي تهدف جميعها إلى المساهمة قي تقديم الدليل العلمي الذي يساعد في كشف الحقيقة بالطرق القانونية الصحيحة، مع التطوير في أساليب التحقيق ونقله من الإطار التقليدي إلى إطار يتناسب مع طبيعة هذه الجرائم[2]، لأنّ استخلاص الأدلة الدقيقة الشرعية يتطلب اتباع أساليب محددة لا تسمح بأي انحراف أو تعديل تؤدي في النهاية إلى القبض على الجناة وتقديمهم للمحاكمة، وفي هذا الإطار صار للأدلة الجنائية الرقمية ولأمن المعلومات عِلمين خاصين بهما.

كما تتطلب الأدلة الإلكترونية ضرورة الإلمام بعلوم الحاسب الآلي والإنترنت والإتصالات، وما يتعلق بالتقنية من جوانب فنية بحتة، ولا يمكن تفسير الحقيقة العلمية للدليل الإلكتروني إلاّ من خلال الإلمام بالعلوم المرتبطة بالنظام المعلوماتي، غير أنّ الدكتور "عمر محمد بن يونس" يرى أنّ منطق التمييز بين مصادر وعملية الضبط ذاتها للدليل الإلكتروني سببها في الحقيقة أنّ الحيز الإفتراضي والزمان الإفتراضي لا يمكن قياسه بما هو مقرر في العالم المادي.

---

[1]- د.أحمد شحاتة بيومي، المرجع السابق، ص 265.

[2]- د.ناصر بن محمد البقمي،المرجع السابق،ص 34.

ولعل أهم نتيجة ترتبت في الواقع على هذا التقرير أنّ الجريمة عبر الإنترنت تتميز بحيز مختلف عن الحيز الذي يتسع له ارتكاب الجريمة في العالم المادي، فمن الممكن أن يكون مصدر الجريمة في دولة وتتحقق النتيجة في دولة أو دول أخرى، لذلك كان لنظرية الحيز الافتراضي وجودها الرئيسي والجوهري في نظرية الدليل الإلكتروني التي يحاول الفقه إرسائها،ومن تمّ يجب الإهتمام في إطار الدليل الإلكتروني التمييز بين المصدر وضبط الدليل ذاته، وإذا كانت فكرة ضبط المصدر جديدة نوعا ما على فقه الإجراءات عموما، فإن هذا لا يعفي من مسؤولية النظر فيها[1].

وسوف أتطرق للمصادر الأساسية للدليل الإلكتروني المتفق عليها لدى الفقه والقضاء.

الفرع الأول: علم الأدلة الجنائية الرقمية وعلم أمن المعلومات.

إنّ الأدلة الإلكترونية ليست جميعها في صورة واحدة، وإنّما تتنوع وتتباين صورها تبعا لتنوع الوسائل الإلكترونية والأجهزة التي تعتمد على نظم الحواسيب الآلية وكذلك تنوع شبكات الإتصال بينها، لذا فإنّ عملية استخلاص الدليل الإلكتروني صعبة ومعقدة إذا لم يقم بها أصحاب الخبرة في مجال التقنية، بل أنه قد صار للأدلة الجنائية الرقمية ولأمن المعلومات عِلمين خاصين بهما.

وللوصول إلى الأدلة الإلكترونية واكتشافها، فإنّ ذلك الأمر يتحقق عن طريق المعرفة الشاملة بعلوم الأدلة التقنية وأمن المعلومات[2]، وعلى هذا الأساس سأتطرق إلى علم الأدلة الجنائية الرقمية في البند الأول، أمّا البند الثاني فسيخصص لعلم أمن المعلومات.

البند الأول: علم الأدلة الجنائية الرقمية.

هناك بعض العلوم التي ينبغي الإلمام بها في إطار الدليل الإلكتروني، أولها هو مدى الحاجة إلى الحاسب الآلي وعلوم الأدلة الجنائية وعلوم التحليل السلوكي للأدلة الإلكترونية، حيث أنّ علوم الحاسب الآلي تقدم المعلومات التقنية الدقيقة وهي مطلوبة لفهم المظهر أو الطبيعة الخاصة و التقنية للدليل الإلكتروني، بينما علوم الأدلة الجنائية من شأنها أن تقدم منظورا علميا لتحليل أي شكل من أشكال الأدلة الإلكترونية،وتساهم علوم

---

[1]- د. عمر بن يونس، المرجع السابق، ص 60.

[2]-د.سامح أحمد بلتاجي موسى، المرجع السابق، ص 382.

التحليل السلوكي للأدلة الإلكترونية في الربط المحدد بين المعارف التقنية وبين الطرق العلمية لاستخلاص الدليل الالكتروني لفهم أفضل للسلوك الإجرامي التقني[1].

ويمكن أن يعرف هذا العلم بأنه هو العلم الذي يضم خليطا من تخصصي القانون وعلوم تقنيات الحاسوب، ودوره هو جمع وتحليل البيانات من أنظمة الحاسوب والشبكات والإتصالات وأجهزة ووسائط التخزين الرقمية بمختلف أنواعها، وتقديم هذه البيانات كدليل يعتد به قانونا أمام الجهات والسلطات القضائية، ويشمل هذا العلم كل الأجهزة الرقمية كالحواسيب الآلية، أجهزة الهواتف النقّالة والكاميرات الرقمية، بل ويتعدى ذلك إلى بطاقات الإئتمان والبطاقات الذكية، فهو يشمل كل جهاز باستطاعته تخزين البيانات أو نقل المعلومات.

والهدف الرئيسي للعلوم الجنائية الرقمية هو شرح تطبيقي علمي مفصل للوضع الذي عثر عليه الجهاز الرقمي من الناحية القانونية في حالة وقوع جريمة من الجرائم، والمقصود بمصطلح الأجهزة الرقمية كل نظم الحاسوب ووسائل التخزين مثل: القرص الصلب أو الأقراص المدمجة، وثائق إلكترونية مثل: رسالة بريد إلكترونية(E-Mail) أو حتى سلسلة من المعلومات الرقمية في إطار الشبكة الحاسوبية[2].

وهذه العلوم مجتمعة تساهم فيما يلي:

1. الكشف عن الدليل الإلكتروني.
2. إجراء الإختبارات التقنية والعلمية عليه لاختباره والتحقق من أصالته ومصدره كدليل يمكن تقديمه لأجهزة إنفاذ وتطبيق القانون.
3. تحديد الخصائص المميزة للدليل الالكتروني.
4. إصلاح الدليل وإعادة تجميعه من المكونات المادية للحاسب الآلي.
5. عمل نسخة أصلية من الدليل الالكتروني للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.
6. جمع الآثار المعلوماتية الرقمية التي قد تكون تبدلت خلال الشبكة المعلوماتية.

---

[1]– د. هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص 254.

[2]– د. سامح بلتاجي موسى، المرجع السابق، ص 383.

7. إستخدام الخوارزميات التي تعد مجموعة من التعليمات التي يمكن أن تتبع لإنجاز عمل ما بعدد محدد من الخطوات، وذلك عبر تجزئة المسألة البرمجية المراد حلها إلى أجزاء صغيرة بسيطة، وبتجميع هذه الأجهزة يمكن التوصل إلى حل صحيح، وذلك من أجل التأكد من أنّ الدليل لم يتم العبث به أو تعديله.

8. تحريز الدليل الإلكتروني لإثبات أنه أصيل وموثوق به ويقع ضمن سلسلة الأدلة المقدمة في الدعوى[1].

ولاشك أنه من أجل تحقيق حماية أضمن، ينبغي استخدام الخصائص البيولوجية، حيث لا يمكن الدخول إلى الحاسب الآلي إلا من خلال بصمة الأصبع أو حدقة العين أو صورة الوجه الفيزيولوجية[2]، كما أن خبراء أمن المعلومات إبتكروا ميزة العلامة المائية لتلافي تزوير بطاقات الإئتمان مثلا، ويتم ذلك عن طريق شفرة خوارزمية يتم تشفيرها على الشريط بشكل متداخل.[3]

البند الثاني: علم أمن المعلومات.

علم أمن المعلومات هو علم يعني بالنظر إليه من زاوية أكاديمية، أنّه ذلك العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، بينما يعني بالنظر إليه من زاوية تقنية، أنه هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، ومن زاوية قانونية، علم أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الإعتداء عليها أو استغلال نظمها في ارتكاب الجريمة[4].

وفي معرض السباق الدائر بلا توقف بين خبراء أمن المعلومات من جهة، ومخترقي شبكات المعلومات من جانب آخر تبرز أهمية وضع سياسات وإجراءات تأمين علمية وفنية لتأمين أنظمة عمل تلك الشبكات، والمظهر الأول لهذه السياسات هو الجانب الوقائي الذي يقوم على محورين:

الأول: هو تأمين شبكة النظام الداخلية والخارجية والذي يتم بصفة عامة من خلال تقسيم حزم المعلومات المارة في شبكة النظام إلى طبقات متعددة، يتم حماية كل منها من الإختراق باستخدام النظم والآليات الخاصة بذلك مثل تشفير البيانات[5].

---

[1]– د. هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص 254.

[2]– د. أحمد خالد العجلوني، التعاقد عن طريق الإنترنت (دراسة مقارنة)، دار الثقافة، عمان، الأردن، بدون طبعة، سنة 2002، ص 09.

[3]– د. أنس العلبي، النظام القانوني لبطاقات الإعتماد، منشورات الحلبي الحقوقية ، بيروت ، لبنان، ط1، سنة 2005، ص 148.

4– د.سامح أحمد بلتاجي موسى، المرجع السابق، ص383.

5–التشفير هو إجراء يدخل ضمن الحماية الفنية للأنظمة المعلوماتية، ويتم بأدوات أو وسائل أو أساليب لتحويل المعلومات بهدف إخفاء محتوياتها والحيلولة دون تعديلها أو استخدامها غير المشروع، بحيث يتأكد المرسل أن المعلومات لم يتسلمها شخص سوى المرسل إليه الذي يعتبر الوحيد المخول له الإطلاع على محتوى

والثاني: هو تأمين حاسبات الخوادم الرئيسية (Servers) عن طريق تحديد المعلومات التي تتيحها تطبيقات النظام لكل مستوى من مستويات مستخدميه، ومراجعة خدمات الشبكة التي تقدمها نظم التشغيل المختلفة لهم[1]، ووضع السياسات التأمينية الخاصة بالدخول على النظام واستخدام موارده، والإحتفاظ بنسخ احتياطية بصفة دورية في أماكن آمنة، وعدم السماح لتنفيذ أي مسح لمنافذ النظام من خارج الشبكة ووضع قيود صارمة على خروج أجهزة الحاسب المحمولة عن مواقعها بأنظمة المعلومات.

أمّا المظهر الثاني من سياسات الحماية فيعنى بإيجاد النظم القادرة على رصد واكتشاف أي محاولة لاختراق النظام المعلوماتي والتنبيه إلى أي فشل يطرأ على أنظمة التأمين لحظيا، ويشمل ذلك السيطرة على عمليات إدارة الدخول إلى النظام وكشف ما قد يحدث من محاولات للعبث بملفات معلومات نظم التشغيل، كما يستلزم الأمر اتخاذ إجراءات تأمينية فورية في شأن تحديد الثغرة التي تم من خلالها اختراق نظم الحماية وتحديد أسلوب ووقت الاختراق وكلمة السر التي تم استخدامها في ذلك.

ويلاحظ أنّ الحاسب الآلي المنفرد غير المتصل بأي شبكات لا يكون عرضة للإختراق المعلوماتي إطلاقا،وإن كان يمكن أن يتعرض للإختراق المادي من خلال الإتصال به مباشرة، وهنا يكون عملية الحصول على الدليل الإلكتروني سريعة وبسيطة، أمّا إذا كان الجهاز متصلا بشبكة تفاعلية متشابكة فهو عرضة لأن يكون محلا لأدلة إلكترونية ناجمة عن ارتكاب جرائم نتيجة لطبيعة الشبكات وقابليتها للإختراق[2].

وهنا تبرز أهمية الأساليب الفنية لحماية الشبكات كمصدر للدليل الإلكتروني كالبروكسي مثلا الذي عمل كوسيط بين الشبكة ومستخدميها، بحيث تضمن الشركات الكبرى المقدمة لخدمة الإتصال بالشبكات

تلك المعلومات المشفرة. أنظر في ذلك: د. مدحت رمضان، جرائم الإعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2001، ص 25.

وإن كان تشفير المعلومات هو أفضل و أقوى أساليب أمن المعلومات على الإطلاق، ولكن للأسف في مقدور أي شخص أن يسيء استخدامه، وتعتبر قدرة الموظف على تشفير المعلومات ثغرة أمنية خطيرة، حيث قد يقوم الموظف بتشفير بعض الأسرار التجارية ونقلها مشفرة إلى الشركات المنافسة، وهو بذلك يستطيع أن يفلت من العقوبة حيث لا يمكن إثبات أي جرم ضده، إذ أن دليل الجريمة لا يستطيع قراءته سواه. أنظر في ذلك:د. حسن طاهر داوود، جرائم نظم المعلومات، بحث مقدم لأكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، سنة 2000، ص 38.

ونتيجة لهذه الأسباب تمّ إعداد مشروع قانون في هولندا يخضع عملية التشفير لضرورة الحصول على ترخيص، ويلزم مستخدميها بإيداع مفاتيح الشفرات لدى مكتب متخصص يحافظ على سريتها، ويلتزم مع ذلك بتقديم هذه المفاتيح لجهات التحقيق متى حصلوا على أمر بالتفتيش، وإن كان احتمال إفشاء مثل هذه المفاتيح ينال من مصداقية وسائل الحماية.أنظر في ذلك: د. أحمد شحاتة بيومي، المرجع السابق، ص 266.

[1]- يتكون نظام التشغيل من مجموعة البرامج التي تتظافر مع بعضها لتسهل تعامل المستخدم النهائي للنظام، وبرامج التشغيل تشتمل على عدة أنظمة منها: نظام التشغيل (OS_2) إختصارا لعبارة (Operating Système) ومن ميزاته القدرة على تشغيل أكثر من برنامج في نفس اللحظة، وكذلك نظام التشغيل (unix): هو مصمم من أجل المتخصصين والمبرمجين ومن ميزاته قدرته على التعامل مع أكثر من برنامج في نفس اللحظة، وأنه يوفر سرية تمنع غير المتخصصين من الاطلاع على الملفات والبرامج التي لا تخصهم. أنظر في ذلك: د. أحمد خليفة الملط، المرجع السابق،ص 49.

[2]- د.أحمد شحاتة بيومي، المرجع السابق،ص 267.

قدرتها لإدارة الشبكة وضمان الأمن وتوفير خدمات الذاكرة الجاهزة (Cashe Memory)، وتقوم فكرة البروكسي على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن الذاكرة (Cashe) المحلية المتوفرة، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل فيقوم بإعادة إنزالها إلى المستخدم دون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، أمّا أنه لم يتم تنزيلها من قبل فيتم إرسال الطلب إلى الشبكة العالمية وفي هذه الحالة يعمل البروكسي كمزود زبون، ومن أهم مزايا مزود البروكسي أنّ الذاكرة (Cashe) المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوي في الإثبات[1].

وما ينبغي الإشارة إليه أنّ أغراض وأبحاث واستراتيجيات ووسائل أمن المعلومات هي ضمان العناصر التالية لأية معلومات يراد حمايتها:

1. **السرية:** وتعني التأكد من أنّ المعلومات لا تكشف ولا يطلع عليها من قبل الأشخاص الغير مخولين بذلك.
2. **التكاملية وسلامة المحتوى:** وتعني التأكد من أنّ محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص أن يتم تدمير المحتوى أو تغيّره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.
3. **إستمرارية توافر المعلومات أو الخدمة:** وتعني التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وأنّ مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو إعاقة دخوله إليها[2].

وبما أن الأنظمة الإلكترونية دخلت عمل المصارف، لذلك على المصرف أن يلتزم بحسن اختيار الموظفين ومراقبتهم المستمرة، كما تقع المسؤولية على المصرف الذي يقع على عاتقه ضرورة تزويد أنظمته بأنظمة أمن محكمة[3]، وتختلف إجراءات أمن المعلومات من جهة إلى أخرى فقد تكون الجهة القائمة على التنفيذ منشأة حيوية أو مجرد شخص عادي، لأنّ أمن المعلومات يتخذ كافة الصور ويتدرج على حسب أهمية المنشأة وقدرتها على تنفيذ إجراءاته وتطويرها في حالة تطلب ذلك، وتتضمن إجراءات أمن المعلومات مجموعة من الخطوات المطلوبة لتطبيقه في المنشآت الحيوية ويمكن إجمال هذه الإجراءات على النحو التالي[4]:

1- أ. علي عدنان الفيل، المرجع السابق، ص 70.

2- د. سامح أحمد بلتاجي موسى، المرجع السابق، ص 384.

3- د. عزة حمد الحاج سليمان، النظام القانوني للمصارف الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، سنة 2005، ص 106.

4- د. أيمن عبد الحفيظ، المرجع السابق، ص 434.

أولا: تحديد أشخاص لتولي المسؤولية.

يقع تحديد خطوات السياسية الأمنية وإقرارها على عاتق رئيس الجهة فهو يعتبر المسؤول الأول عن تطبيق هذه السياسة،وقد تتولى الجهة ذاتها تنفيذ هذه السياسة الأمنية تجنبا للتكاليف الباهظة التي تنفقها المنشأة في حالة ما إذا كانت هذه السياسة يتولى تنفيذها شركة أمن متخصصة.

ثانيا: مشاركة الموظفين العاملين في المنشأة.

لا تقف السياسة الأمنية الناجحة عند حد إقرارها من قبل مدير ناجح، ولكن الأمر يتطلب أيضا مشاركة الموظفين في المنشأة في تنفيذ هذه السياسة الأمنية في مختلف القطاعات سواء كانوا عناصر أساسية أم كانوا مشاركين في العمل فقط، لأنهم يقع عليهم توخي الحذر لعدم حدوث مشكلة يترتب عليها أضرار مادية تلحق بالمنشأة، مع ربط هؤلاء الموظفين بالتكنولوجيا الأمنية كأساس لكفاءة الأداء الأمني، ويتم مسبقا تحديد دور كل موظف في تطبيق هذه السياسة، ومتابعة نشر الوعي لديهم.

غير أنه لا بد من الإشارة إلى أن أمن المعلومات يمثل تحديا كبيرا، لأنه ينطوي على ميزانية ضخمة قد لا تتناسب مع الدول التي تكون مواردها محدودة، خاصة مع تضاعف الأفعال الإجرامية على شبكة الإنترنت[1]، فأمن المعلومات يعتبر رهانا كبيرا بالنسبة للدول التي تتعرض للإعتداءات المتكررة و التي تمس بصورة فاضحة حياة الأفراد و خصوصياتهم، ولهذا يمكن تصور الخطورة الكبيرة التي يتعرض لها مستخدم الإنترنت[2].

يستخلص مما سبق، أنّه عن طريق هذه العلوم يمكن تحريز الدليل الإلكتروني لإثبات أنه أصيل وموثوق به، فقد أصبحت الإستعانة بالوسائل العلمية التي أفرزها التطور العلمي السريع أمرا حيويا لنجاح التحقيق الجنائي في كشف الجرائم، فلاشك أنّ هذه العلوم ضرورية من أجل فهم الطبيعة الخاصة للدليل الإلكتروني واستخلاصه بشكل صحيح وإعادة إصلاحه عند إتلافه[3].

الفرع الثاني: الأنظمة الواجب فحصها للحصول على الدليل الإلكتروني.

هناك العديد من الأنظمة التي يتعين فحصها من أجل الحصول على الدليل الإلكتروني، فهذا الأخير يمكن الحصول عليه عن طريق فحص النظام المعلوماتي، خاصة و أن الحواسيب تحمل في ذاكرتها العديد من

---

[1] – د. أيمن عبد الحفيظ ، المرجع السابق، ص 434.

[2]- Daniel Ventre, Cyberguerre et guerre de l'information, Lavoisier, Paris France, 2010, p 24.

[3]– د. ناصر بن محمد البقمي، المرجع السابق، ص 33.

الأسرار المتعلقة بالأفراد، والتي لا يرغبون حتما في الكشف عنها لأنها تتعلق بحياتهم الخاصة، و أي مساس بها يعد إنتهاكا،كما قد تكون الأدلة الإلكترونية مبعثرة في البريد الإلكتروني أو الأشرطة الممغنطة[1]،وسيتم تفصيل ذلك على النحو التالي:

البند الأول : فحص أنظمة الإتصال بالإنترنت.

يقصد بنظام الإتصال بالإنترنت بالمفهوم الإجرائي مدى إمكانية اقتناع محكمة الموضوع بالإجراءات المتبعة حال استخدام وسيلة الإتصال بالإنترنت، وفي هذا الإطار تثار مسائل شتى ذلك أنّ الإنترنت من طبيعة مرنة فلا يوجد لها مالك،كما أنّه ليس هناك من يمكنه التسلط عليها.

بالإضافة إلى مسألة أخرى تبرز أثناء فحص نظام الإتصال بالإنترنت سعيا وراء إقامة الدليل على الإدانة هي تحديد المكان الذي انطلق منه النشاط المادي للجريمة.

ومثل هذا الأمر وإن كان لا يقود تحديدا إلى الشخص مرتكب الجريمة إستنادا إلى الدليل الإلكتروني فقط، إلاّ أنّه يمكن أن يساعد حتما في التوصل إليه عبر إقامة الدليل التقليدي فيما بعد على أنّ الأمر لا يقف عند هذا الحد، وإنّما يمتدّ إلى ضرورة التطرق إلى تقصي الحقيقة في أماكن أخرى كفحص كل ما يتعلق بنظام الإتصال بالإنترنت كالشبكات المحلية والعالمية والبيانات وحركة الإسترداد والنظام الأمني المحاط بالإنترنت ونظام الإتصالات القائم وحركته وامتداداته وبرمجيات الإنترنت وحركة الإنزال والتحميل والنظام المعلوماتي المحمل على الإنترنت ودرجة استيعابه[2].

فالدليل الإلكتروني على الرغم من اتساع قاعدته وخصوصيته، إلاّ أنه يمكن أن يكون متواجدا في صيغة ما لا يمكن توقعها، فمثلا نجد أنّ التفتيش في الحاسوب الشخصي سعيا وراء البحث عن ملف ما يرتبط بارتكاب جريمة موضوع هذا التقصي والبحث من قبل الخبير قد لا يؤدي إلى نتيجة تذكر، إلاّ أنّ البحث في نظام البريد الإلكتروني قد يؤدي إلى وجود ما يفيد إثبات الجريمة كما لو كان مرتكب الجريمة قد قام بوضع

[1]-Services d'administration de la preuve électronique, disponible à l'adresse suivante : www.kpmg.com/ca/fr/topics/ediscovery-services/pages/defaul.aspx.

[2]- د. عمر بن محمد بن يونس، الدليل الرقمي، المرجع السابق، ص 61.

نسخة من هذا الملف في خادم البريد الإلكتروني عبر الإنترنت والخاص بهذا الشخص، بحيث يمكن أن يطاله من أي مكان وفي أي وقت، ويتم فحص هذا النظام على النحو التالي:

أولا: فحص مسار الإنترنت.

يقصد بمسار الإنترنت الحركة التراسلية للنشاط الممارس من خلال شبكة الإنترنت، فجهاز الحاسوب بمجرد أن يتعرف على المسار يقوم تلقائيا باختيار البروتوكول التراسلي والذي عن طريقه يقوم الحاسوب باستدعاء البيانات، ويستخدم في تتبع مسار الإنترنت نظام الفحص الإلكتروني الذي يطلق عليه علم البصمات المعاصرة أو علم بصمات القرن الواحد والعشرين، وهو منهج متبع في تتبع الحركة العكسية لمسار الإنترنت ولقد تم على أكثر من جريمة إلكترونية[1].

ثانيا : فحص النظام الأمني للشبكات.

إنّ جهاز الحاسب الآلي المنفرد غير المتصل بأي نوع من الشبكات لا يكون عرضة للإختراق المعلوماتي إطلاقا، وإنما ما يمكن أن يتوافر له هو إختراق مادي، بحيث يتصل مرتكب الجريمة هنا بالحاسوب المنفرد إتصالا مباشرا، وهذا يجعل عملية الحصول على الدليل الإلكتروني سريعة وبسيطة، بحيث تتجه الشبهات إلى حائز الجهاز وكذلك كل من قام باستخدامه على نحو آخر.

أمّا أجهزة الحاسب الآلي المرتبطة بنظام تواصلي عبر شبكات فإنها تكون أكثر عرضة لاستخدامها في ارتكاب الجرائم واحتوائها على الأدلة الإلكترونية خاصة الشبكات غير المحصنة بالتشفير، بحيث تكون أكثر عرضة للإختراق، وبالتالي فإنّ فحصها يتطلب وقتا أكثر للحصول على دليل إلكتروني،في حين تكون الشبكات المحصنة بالتشفير ذات صعوبة أقل في تحصيل الدليل لكون الإختراق يبدو واضحا من خلال الكشف الدوري عليها[2].

ثالثا: فحص بروتوكول الإنترنت.

يتم فحص نظام الإتصال بالإنترنت عن طريق فحص بروتوكول الإنترنت(IP) الذي سجله الحاسوب، ويعدّ البروتوكول طابع مميز لاستخدام الإنترنت فأي شخص يحصل على بروتوكول الإنترنت يمكنه الولوج إليها ليكون عضوا كاملا فيها يباشر الحركة خلالها ويستفيد من خدماتها، وعن طريق فحص

---

[1]– د.فتحي أنور عزت،الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، المركز القومي للإصدارات القانونية، القاهرة، ط2، سنة 2012، ص 618.

[2] – د. حسين بن سعيد الغافري، المرجع السابق،ص 541.

هذا البروتوكول يمكن التعرف على الحاسوب الذي تم ارتكاب الجريمة عن طريقه والبحث لدى مسجلي بروتوكول الإنترنت[1] في قواعد البيانات ليست مهمة صعبة، إذ يمكن لأي شخص القيام بتحديد حائز هذا أو ذلك البروتوكول عن طريق البحث في قاعدة البيانات الخاصة بالمسجلين عن طريق برامج خاصة تقوم برصد هذا البروتوكول[2].

رابعا: فحص الخادم أو الملقم (Server).

الخادم هو عبارة عن هيكلية لوصل أنظمة الحاسوب على الشبكة وهو نظام كبير يمكنه تخزين كميات ضخمة من البيانات ويستطيع تنفيذ التطبيقات الرئيسية، ويحقق حركة الإتصال بالمواقع والصفحات التي تم استضافتها على صورة رقمية لتزويد المستخدمين بخدمات الإنترنت، ومن أجهزة الخوادم أو الملقمات ما يكون متخصص في موضوع معين كالخوادم الخاصة بحلقات النقاش أو تلك المتخصصة في مجموعات الأخبار، ومنها ما تكون مهمته تحقيق الوصول إلى الموقع فقط ويسمى ملقم وصول ، ويعمل الخادم على الربط بين أعضاء الإنترنت مما يمكنهم من التحاور والمناقشة[3].

وتحتاج عملية فحص الخادم إلى ضرورة اتخاذ الإجراءات القانونية اللازمة وفق القانون النافذ في النطاق الإقليمي الذي يوجد فيه، بالإضافة إلى لزوم الأخذ في الاعتبار الغاية من التفتيش، غير أن تقنية الإنترنت تجعل من الممكن القيام بفحص خوادم عن بعد، وذلك باستخدام تقنية حديثة في هذا الإطار تجعل التوصل إلى محتوى حركة الإتصال بالخادم ذات مغزى وربما أفضل من مجرد القيام بفحص الخادم ماديا[4].

البند الثاني: فحص مكونات الحاسب الآلي.

إنّ الحاسب الآلي في حد ذاته يقوم في تركيبته على ثلاثة أمور هي: القطع الصلبة، القطع المرنة أو البرمجيات وأخيرا البيانات ذات القدرة الإستردادية في هيئة معلومات التي تتوزع ما بين تركيبة البرمجيات والقطع الصلبة، وتعتمد عملية فحص الحاسوب على الحاسوب ذاته أيضا سواء بالفحص الذاتي للحاسوب وهو قيام الحاسوب ذاته بفحص مكوناته وتقديم تقرير كامل بذلك إلى طالب الفحص،ومثل هذه الحالة يجب ألاّ يقوم

---

[1] – في عام 1972 تم ربط حوالي 50 جامعة ببعضها عن طريق نظام Arpanet، وفي عام 1973 تم الربط مع جامعة لندن، وهي شبكة إتصالات طورتها وزارة الدفاع الأمريكية. أنظر في ذلك:

Yannis Delmas, Histoire de l'informatique, d'Internet et du Web, disponible à l'adresse suivante : www.delmas-rigoutsos.nom.fr.

[2]– د. حسين بن سعيد الغافري، المرجع السابق، ص 542.

[3]– د. سامح بلتاجي موسى، المرجع السابق،ص 386.

[4] –د. حسين بن سعيد الغافري، المرجع السابق،ص 544.

بها الهواة أو المستخدمون العاديون، حيث تتطلب مثل هذه الحالة قدرات تقنية عالية، وقد يتم الفحص بطريقة الإستعانة بحاسوب آخر وأجهزة تقنية عالية متخصصة في بحث جزئيات عبر الحاسوب[1].

أولا: فحص القرص الصلب.

يعد القرص الصلب المحتوى الذي يضم في داخله مجموعة البيانات الرقمية ذات الطابع الثنائي،ويشير العلماء إلى إمكانية القيام بفحص كلي أو جزئي للقرص الصلب، فالفحص الجزئي يؤدي إلى التعرف على محتوى البيانات ثنائية الرقم والتي يؤدي التعامل معها إلى الكشف على القيمة الإستردادية للبيانات المخزنة فيه سواء كانت محتويات مكتوبة أو صور أو أصوات، وكذلك ما تم حذفه من بيانات وبرمجيات وبرامج، وعملية الإلغاء أو الحذف تحتاج إلى برمجية خاصة للقيام بها، فليس الأمر مرتبطا بقطعة صلبة وإنما ببرمجيات أيضا، والمثال التقليدي المستخدم هنا هو حالة البحث في ملفات النسخ الإضافية التي تحتويها نظم التشغيل وهي ملفات تأخذ نسخا احتياطية من كل صفحة يتم الولوج إليها عبر الإنترنت.

كذلك توجد في نظام التشغيل ملفات خاصة بالإنزال مهمتها استقبال الملفات التي يتم تحميلها على جهاز الحاسب الآلي من خارجه وعبر الإنترنت[2]، ولا بد كذلك من مراعاة شرط سلامة الجهاز والذي يعني صحة حركة القطع الصلبة بحيث يجب أن يعمل بطريقة عادية لتجنب رفض المحكمة الإعتداد بالدليل المنبثق عنه.

ثانيا: فحص البرمجيات.

وهنا يمكن التمييز بين الفحص الداخلي للبرمجيات وحالة الفحص الخارجي لها،ففي حالة الفحص الداخلي والذي يتم من خلال بحث البناء المنطقي للبرمجية بما يوحي بأن هناك مجهودا في إعداده للعمل حين إنزاله في جهاز الحاسب الآلي، وذلك من الأمور التي يدركها الخبراء من حيث استلزام الربط الصحيح في البرمجية ذاتها بحيث يلزم المبرمج تتبع الخطوات المنطقية التي تعبر عن جهده سيما وأنّ الخبراء على دراية بكيفية البرمجة والخيارات المتعددة.

وأكثر ما يتم العمل في إطار الفحص الداخلي هو البحث عن مصدر الملفات الموجودة في هذا الإطار، وعلى أية حال فإنّ الوسيلة التي تم بها النسخ ليست ذات قيمة في هذا الإطار إلاّ أنها تفيد في ترتيب كيفية حدوث هذه الجريمة، وقد يقود مثل هذا الأمر إلى التوصل إلى جرائم أخرى كما لو كان هناك تزييف

---

[1]– د.حسين بن سعيد الغافري، المرجع السابق، ص 544.

[2] – د.عمر محمد بن يونس، الدليل الرقمي، المرجع السابق،ص 74.

للصور، فإن الكشف عما إذا كانت جذورها عبر الإنترنت أم في الواقع المادي من خلال مسح صور فوتوغرافية يمكن أن يقود إلى ترويجها في العالم المادي أو القبض على مرتكبها أو التعرف على كيفية إعداد مثل هذه الصور[1] .

أمّا في حالة الفحص الخارجي فإن ذلك يتم بطريقة مادية عن طريق المقارنة مثلا، كما يحدث في حالة مقارنة أحد البرمجيات المنسوخة بالنسخة الأصلية وذلك حماية لحق المؤلف والملكية الفكرية وبراءة الإختراع.

ويساهم فحص البرمجيات في الكشف عن جرائم الحاسوب في ظل تقنين فكرة العدوان على حقوق الملكية الفكرية،على أنّ فحص البرمجيات يعد أيضا من الوسائل الرئيسية في الكشف عن أكثر جرائم الإنترنت ضراوة مثل جرائم الإختراق والولوج غير المشروع إلى نظم الغير، فمثلا وجود برمجيات غير مصنفة تعمل في بيئة الإختراق أو تساعد عليه، كما هو الشأن في برمجيات المسح للكشف عن الأبواب المفتوحة (Scan ports prog) ، يمكن أن يشكل منطقة استفهام ودلالة كافية أيضا على ارتكاب الشخص لجريمة دخول غير مشروع أو انتهاك نظام حاسوب عامل إذا استتبع ذلك اعترافا شفويا بارتكابه للجريمة، وهو غير الحال إذا كان هناك اعترافا من الشخص في الوقت الذي لا يوجد في حاسوبه برمجيات مثل هذه، إذ لا يمكن الجزم بأنّ هذا الشخص بالرغم من وجود إعتراف بذلك قد قام بارتكاب الجريمة[2].

غير أنه ينبغي الإشارة أنّ مسألة العطب البرمجي تعد من المسائل الخطرة في إطار فحص البرمجيات، كون الإتصال بالإنترنت عبر الحاسوب يستلزم وجود برمجيات محملة فيه، إذ أنّ الحاسوب دون برمجيات يظل دائما مجرد قطع صلبة، إلا أنّ تحديد درجة العطب يمكن القول باختلافها من مكان إلى آخر ومن دولة إلى أخرى، فمن الصعوبة بمكان القول بعدم إمكانية التعويل على الدليل الإلكتروني بمجرد أن الحاسوب يحتوي على برمجيات معطوبة، وإنما وفقا للحالة العادية التي يعمل بها جهاز الحاسب الآلي بحيث لا يمكن التعويل على الدليل المستمد من حاسوب محاصر تماما بالعطب البرمجي، أمّا إذا كان العطب البرمجي يجعل الحاسوب مع ذلك مؤهلا للعمل فإنّ مثل هذا العطب البرمجي لايؤثر في قيمة الدليل[3].

---

[1] – د.حسين الغافري، المرجع السابق،ص 547.

[2] – د. سامح بلتاجي موسى ، المرجع السابق،ص 189.

[3] – د. حسين الغافري، المرجع السابق، ص 550.

ثالثا: فحص النظام المعلوماتي.

يعني فحص النظام المعلوماتي ضبط كافة ما يحتويه جهاز الحاسب الآلي من معلومات يمكن استردادها عبره تكون مخزنة في ملفات على أية شاكلة يمكن أن تكون عليها الحركة الإستردادية، ما دام موضوعها يشكل جريمة بالنظام المعلوماتي للحاسب الآلي لا يحتوي على معلومات كما هو معتقد، وإنّما المحتوى المعلوماتي عادة ما يتكون من بيانات ثنائية الهيئة الرقمية التي يتم إيداعها في الحاسب الآلي، وهذا الإيداع يأخذ شكل تخزين وهذه البيانات يقوم الحاسوب بمعالجتها ويبرزها على هيئة معلومة محددة، حيث يتم استدعاؤها من قبل الغير أو أي مستخدم للحاسوب وما دام لم يتم استدعاء معلومة محددة فإن بياناتها تظل في حالة تخزين في الحاسوب[1].

رابعا: فحص نظام ذاكرة التخزين.

يعد نظام ذاكرة التخزين من مزايا نظم تشغيل الحاسوب تحديدا وكلما كان نظام التشغيل متطورا كان نظام ذاكرة التخزين أكثر دقة، ويمكن تعريفه بأنه: "قدرة الحاسب الآلي على الإحتفاظ في ذاكرته بنسخة كاملة مما اطلع عليه عضو الإنترنت أثناء إبحاره عبر العالم الإفتراضي".

وفحص نظام التخزين في الذاكرة يعد من الأماكن الهامة عند القيام بفحص نظام الحاسب الآلي لمعرفة ما تم زيارته عبر الإنترنت، وتسمح الأنظمة الجديدة بمتابعة ما تمت زيارته لفترة زمنية طويلة حتى وإن كان عضو الإنترنت قد قام بحذف كافة نظام التشغيل بتخزينه، كذلك يمكن استخدام برمجيات للكشف عن مستخدمي الحاسوب أثناء التصفح لفترات طويلة من الزمن قد تصل إلى ستة أشهر كاملة، كما يوجد برمجيات تسمح باستطلاع القرص الصلب حتى في حالات التخلص من محتوياته باستخدام خاصية الإزالة الكلية.

خامسا: فحص الطابعة.

يمكن رصد الجريمة الخارجية سعيا وراء الدليل الإلكتروني بفحص الطابعات سيما الحديثة منها، إذ تتضمن الطابعات الحديثة ميزة تخزين منطقية لمجموع الصفحات التي تم استخراجها من الحاسوب حتى في الحالة التي يكون فيها هذا الملف قد تم إلغاؤه، ففي هذه الحالة الأخيرة يتم استخدام برمجيات متطورة لاسترجاع ما تم اتخاذه من أوامر عبر جهاز الحاسب الآلي منها أمر الطباعة، حيث تقوم الطابعة بطباعة ما

---

[1]- د.حسين بن سعيد الغافري ، المرجع السابق،ص 552.

قامت في فترة زمنية سابقة بطباعته وهو أمر بالضرورة يؤدي إلى الحصول على مخرجات الطابعة التي تفيد في كشف الحقيقة[1].

سادسا: فحص لوحة المفاتيح.

يمكن أن تكون لوحة المفاتيح محلا لفحص خبراء تكنولوجيا المعلومات في المعامل الجنائية، حيث أنّ لوحة المفاتيح الحديثة كثيرا ما يتم استخدامها كخادم وهمي من قبل الهكرة، وفي هذه الحالة يكون التعامل معها كأداة أو وسيلة مساعدة في ارتكاب الجريمة، ومن تم يمكن اعتبار الدليل المستمد منها دليلا يساعد في إبراز حقيقة الواقعية الإجرامية.

سابعا: فحص النظام الأمني البرمجي لأنظمة الحاسوب.

تعد الأنظمة الأمنية في جهاز الحاسب الآلي المنفرد غير المتصل بشبكة ما من أفضل السبل التي تجعله في مأمن من إمكانية ارتكاب جرائم فيه، على أنّ مثل هذه النظم الأمنية المنفردة قد توحي بنوع من الخصوصية التي تستلزم الكشف عن مقومات هذا الجهاز المنفرد، إذ أن الخصوصية المطلقة هنا يمكن أن تكون عاملا سلبيا في رفض تمكين الغير من الإطلاع على محتوى هذه الأجهزة[2].

الفرع الثالث: البرامج والأدوات المستخدمة في جمع الدليل الإلكتروني.

تمت الإشارة فيما سبق إلى خصوصية الجرائم الإلكترونية، خاصة فيما يتعلق بالأدلة غير المرئية والتي تتواجد في بيئة تقنية، ولذلك فهي تحتاج إلى دراية ومعرفة تامة بالطابع الخصوصي لهذه الجرائم والوسائل المستخدمة فيها، مما يقتضي بالضرورة الإعتماد على وسائل علمية وفنية تتناسب مع هذه النوعية من الجرائم للكشف عن الحقيقة،وتتمثل هذه الوسائل في الإستعانة ببعض البرامج والأدوات التي تساهم في جمع الأدلة الإلكترونية والتي من شأنها المساعدة في إثبات هذه الجرائم ذات الطبيعة الخاصة وتحديد هوية مرتكبيها، وسيتم التطرق إلى أهم هذه البرامج والأدوات وذلك على النحو التالي:

---

[1] – د. عمر محمد بن يونس، الدليل الرقمي، المرجع السابق،ص 85.

[2] –د.حسين بن سعيد الغافري، المرجع السابق، ص 556.

البند الأول: برامج جمع الدليل الإلكتروني.

لاشك أنه سيتم التطرق إلى أهم هذه البرامج، وترجع أهميتها في جمع الدليل كون عن طريقها يتم تسهيل الوصول إلى الدليل الإلكتروني، غير أنّه لابد أن يقوم بها خبراء في هذا المجال وذلك نظرا لعملية ودقة هذه الأدلة، ومن هذه البرامج ما يلي:

أولا: برنامج إذن التفتيش.

هو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها، ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل.

ثانيا: قرص بدء تشغيل الحاسب الآلي.

وهو قرص يمكّن المحقق من تشغيل الحاسب الآلي إذا كان نظام التشغيل فيه محميا بكلمة مرور، ويجب أن يكون القرص مزودا ببرنامج مضاعفة المساحة، فربما كان أحدهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.

ثالثا: برنامج معالجة البيانات.

وهو برنامج يمكّن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقسيم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة، أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يمكّن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها.

رابعا: برنامج النسخ.

هو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الحاسب الآلي الخاص بالمتهم ونقلها إلى قرص آخر، وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم.

خامسا: برامج كشف القرص: ويمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن، مهما كانت أساليب تهيئة القرص، هذا البرنامج له نسختان نسخة عادية خاصة بالأفراد ونسخة خاصة بالشرطة[1].

---

[1]-أنظر على التوالي: د. حسن طاهر داوود، المرجع السابق، ص 228 و د. ممدوح عبد الحميد عبد المطلب ، إستخدام بروتوكول TCP IP في بحث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات في الفترة من 26-28 أبريل 2003، الإمارات العربية المتحدة، ص 652.نقلا عن: د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق،ص204.

سادسا: برامج الإتصالات.

وهو يستطيع ربط جهاز حاسب المحقق بجهاز حاسب المتهم لنقل ما به من معلومات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب.

سابعا: برامج التتبع.

تقوم هذه البرامج بالتعرف على محاولات الإختراق التي تتم مع تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على إسم الحدث وتاريخ حدوثه وعنوان بروتوكول الإنترنت التي تمت من خلاله عملية الإختراق وإسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى.

ثامنا: نظام كشف الإختراق.

هذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسبات الآلية أو الشبكة مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن هذه الحاسبات، ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاصة بتسجيل الأحداث فور وقوعها، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للإعتداءات على الأنظمة الحاسوبية، وفي حالة تحقق هذا الأمر يقوم بإنذار مدير النظام بشكل فوري ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة، والتي يمكن أن تقدم معلومات لجهات التحقيق تساعدهم في معرفة طريقة ارتكاب الجريمة وأسلوبها ومصدرها[1].

البند الثاني: أدوات جمع الدليل الإلكتروني.

بالإضافة إلى الأنظمة الواجب فحصها لجمع الدليل الإلكتروني وكذا البرامج، هناك أدوات تستخدم هي الأخرى لهذا الغرض في بنية نظم المعلومات، فعادة ما يكون هذا الدليل في مخرجات الطابعة وفي أجهزة الكمبيوتر وملحقاتها[2]، وفي الأقراص المرنة والصلبة وأشرطة تخزين المعلومات وغيرها من الأجهزة التي تم التطرق إليها بالتفصيل، ولذلك تستخدم عدة أدوات تساهم في جمع هذا الدليل منها:

---

[1] –أ.علي عدنان الفيل، المرجع السابق، ص 71.

[2] – لاشك أنّ أجهزة الكمبيوتر نقصد بها الكمبيوتر الخاص بالمتهم المشتبه فيه، وخاصة وحدة التخزين الدائمة كالقرص الصلب والوحدات الفرعية الملحقة تشتمل على القرص المرن وأقراص الليزر أو أي وحدة تخزين أخرى، بالإضافة إلى جهاز كمبيوتر المجني عليه فلا شك أنه المصدر الكاشف، فقد يكون شخص طبيعي أو مؤسسة خاصة أو عامة أو مؤسسة مالية أو هيئة حكومية وغير ذلك، ناهيك عن جهات أخرى يمكن الإستعانة بها كمقدم خدمة الإنترنت مثل:

أولا: أدوات تدقيق ومراجعة العمليات الحاسوبية.

وهي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجري على ملفات ونظام تشغيل حاسب إلكتروني معين وتسجيلها في ملفات خاصة يطلق عليها (Logs)، والكثير من هذه الأدوات تأتي في أنظمة التشغيل المختلفة وبعضها يأتي كبرامج مستقلة يتم تركيبها على أنظمة التشغيل بعد إعدادها للعمل في وقت مبكر وسابق لارتكاب الجريمة، حتى يمكن أن يقوم بتسجيل المعلومات التي قد يكون لها علاقة بالحادثة ربما ساعدت في كشف أسلوب الجريمة وشخصية مرتكبها.

ثانيا:أدوات الضبط.

هي أدوات تعتبر من الوسائل المادية التي تساعد في ضبط الجريمة الإلكترونية، منها على سبيل المثال: برامج الحماية وأدوات المراجعة وأدوات مراقبة المستخدمين للشبكة وبرامج التنصت على الشبكة والتقارير التي تنتجها نظم أمن البيانات ومراجعة قاعدة البيانات وبرامج النسخ الاحتياطي التي تستخدم لعمل نسخة مطابقة تماما للأقراص الصلبة الموجودة في الحاسبات الإلكترونية محل التحقيق، بغرض عمل فحص عليها دون تعريض الأقراص الأصلية لأي تغير في البيانات الموجودة، ومن أشهر هذه البرمجيات برنامج (**Safe back**)وبرنامج (**Encase**).

ثالثا: الأدوات المساعدة للتحقيق.

من هذه الوسائل الأدوات المستخدمة في استرجاع المعلومات من الأقراص التالفة وبرامج الضغط وفك الضغط وبرامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسبات، وأيضا من الأدوات المهمة والتي تساعد في عملية التحقيق برامج منع الكتابة على القرص الصلب وذلك بعد ارتكاب الجريمة مما يساعد في المحافظة على مسرح الجريمة ، وكذلك توجد برمجيات استعراض الصور والتي تستخدم في عرض الصور الرقمية على شاشة الجهاز، وبالتالي فهي تقدم خدمة لجهات التحقيق من خلال تمكينها من مشاهدة واستعراض الصور الرقمية المخزنة داخل أجهزة الحاسبات الآلية[1].

شركة Yahoo أو Googleأو MSN،فمثل هذه الشركات يتم تسجيل البيانات الخاصة بمنتفعيها، ومن ثمّ يمكن اللجوء إليها للتعرف على هوية المجرم المشتبه فيه. أنظر في ذلك: د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق،ص 202.

[1] – أ. علي عدنان الفيل، المرجع السابق،ص 75.

رابعا: أدوات فحص ومراقبة الشبكات.

هذه الأدوات تستخدم في فحص بروتوكول الإنترنت، وذلك لمعرفة ما قد يصيب الشبكة من مشاكل، ومعرفة العمليات التي تتعرض لها ومن هذه الأدوات:

1- أداة A R P : وظيفتها تحديد مكان الحاسبات الإلكترونية فيزيائيا على الشبكة.

2- برنامج (Visual Route S.2a): هو عبارة عن برنامج يلتقط أية عملية فحص عملت ضد الشبكة، فيقوم بتقديم أجوبة تبين المعلومات التي حدث فيها مسح والمناطق التي مر فيها الهجوم، وبعد معرفة عنوان (IP) أو اسم الجهة يرسم البرنامج خط يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم.

3- أداة Tracer: تقوم هذه الأداة برسم مسار بين جهازين تظهر فيه كل التفاصيل عن المسار والعناوين التي زارها المجني وتوجه من خلالها الوقت والفترات التي قضاها، وهي تسمح برؤية المسار الذي اتخذه (IP) من مضيف إلى آخر، وهذه الأداة تستخدم في الأساس للمسح الميداني للشبكات المراد التخطيط للهجوم عليها، كما يمكن من خلالها معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والإختراقات التي وقعت عليها[1].

4- أداة (Net Stat): هي أداة لفحص حالة الإتصال الحالي للبروتوكول TCP/ IP[2] ولها عدد من المهام من أهمها:عرض جميع الإتصالات الحالية ومنافذ التنصت وعرض المنافذ والعناوين بصورة رقمية وعرض كامل لجدول التوجيه.

---

[1]-أ. علي عدنان الفيل، المرجع السابق، ص 76.

[2] - بروتوكول TCP/IP يضم في الواقع بروتوكولين مستقلين في شبكة الإنترنت هما بروتوكول (TCP) وهو اختصار لكلمة: Transmissioncontrol protocol وبروتوكول الإنترنت (IP) وهو اختصار لكلمة :InternetProtocolحيث يعملان وبشكل متزامن، ويركز البروتوكولين معا على تقنية التبادل المعلوماتي بواسطة الحزم المعلوماتية بين مختلف الوصلات السلكية واللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصولة فيما بينها،وحزمة المعلومات جزء من ملف معلوماتي ذات حجم مصغر ثابت تحمل كل منها رقما خاصا ومعلومات تعريفية بكل من المرسل والمرسل إليه، بحيث تعتبر كل حزمة عبر شبكة الإنترنت بشكل مستقل وعند كل وصلة تتم قراءة جهة المرسل إليه ثم تتم إعادة إرسال الحزمة المارة عبرهما نحو الوصلات التالية الأقرب إلى جهة المقصد النهائية. وبمقتضى بروتوكول (IP)، يتم التعرف على الكمبيوتر الموصول بشبكة الإنترنت من خلال العناوين، حيث كل كمبيوتر موصول بها عنوانه الوحيد الخاص به تماما، وما ينبغي الإشارة إليه أنّ جمع الأدلة الإلكترونية من بروتوكولات النقل وشبكات الإتصالات يمكن أن تشكل صعوبة نسبية من وجهة نظر أجهزة إنفاذ القانون، وبالرغم من أنّ ملفات الولوج تبدو مشابهة للملفات العادية وممكن جمعها مثل أي ملف آخر وهي تحتوي على كميات هائلة من المعلومات التي قد تفيد في التحقيق، إلاّ أنّ الصعوبة في جمع هذه المعلومات أنها عادة ما تكون مختلطة بغيرها من معلومات مستخدمي الكمبيوتر الذين لا دخل لهم، مما قد يشكل تهديدا لخصوصية هؤلاء، لذلك تعمد بعض منظمات تشغيل الكمبيوتر والشبكة إلى عدم إفشاء أسرار جميع ملفات الولوج إلا الخاصة بالمتورطين،كما توجد صعوبة أخرى في جمع الأدلة الإلكترونية من جداول الحالة التشغيلية في البروتوكولات والإتصالات وتتمثل هذه الصعوبة في أنّ

يستخلص أنّ مصادر الأدلة الإلكترونية المذكورة جاءت على سبيل المثال وليس الحصر، إذ أنّ التطور العلمي والتقني قد يسفر عن أنواع جديدة من هذه الأدلة، غير أنّ هذه المصادر في الحقيقة لا يمكن أن ترتبط بدولة واحدة فهي ذات المصادر في كل مكان ، لذلك فإنه من الناحية التقنية يمكن القول بإتحاد المصادر التي يوجد فيها الدليل الإلكتروني وهذا الإتفاق ليس مصدره معاهدة دولية أو اتفاق دولي وإنما فرضته تقنية الحوسبة والرقمية[1].

الجداول تكون متاحة لفترات قصيرة وقد تزول بمجرد انقطاع التيار الكهربائي. أنظر في ذلك:د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 652. نقلا عن: د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 227.

[1]– أ. عمر بن يونس، الدليل الرقمي، المرجع السابق، ص 90.

الفصل الثاني: مشروعية إجراءات جمع الدليل الإلكتروني.

تعد الدعوى الجزائية هي الوسيلة القانونية التي يتم من خلالها اقتضاء حق الدولة في العقاب[1]، ويعد التحقيق الإبتدائي هو أولى مراحل هذه الدعوى إذ تبدأ بمباشرة أيّ من إجراءات التحقيق فيها، أمّا المرحلة الثانية هي مرحلة المحاكمة، ويعبر عنها بالتحقيق النهائي وتشمل الإجراءات التي تتم أمام المحكمة وتنتهي بتقرير الإدانة أو البراءة.

ويسبق إجراءات التحقيق في الدعوى مرحلة تمهيدية تسمى مرحلة الإستدلال يكون الغرض منها التمهيد لها عن طريق جمع الأدلة المثبتة لوقوع الجريمة والبحث عن مرتكبيها وجمع كافة العناصر التي تفيد في تحقيق الدعوى، وبالتالي لا يمكن اعتبارها من إجراءات الدعوى.

والسؤال المطروح فيما يتعلق بكيفية الحصول على هذه الأدلة ومدى نزاهتها وشرعيتها يتنازعه تياران: أحدهما يرى أنه من أجل الوصول وكشف الحقيقة فإنّ كل الطرق المـؤدية للحـصول على أدلة الإدانة أو البراءة مقبولة مهما كان مصدرها وكيفية الحصول عليها على أساس أنّ الغاية تبرر الوسيلة، والتيار الثاني يرى عكس

---

[1] – من أهم وسائل تحريك الدعوى الجزائية البلاغات والشكاوى، أمّا البلاغ يقصد به: إخبار السلطات المختصة عن وقوع الجريمة أو أنها على وشك الوقوع أو أنّ هناك اتفاقا جنائيا أو أدلة أو قرائن أو عزما على ارتكابها أو وجود شك أو خوف من أنها ارتكبت، وبالنسبة للبلاغ في الجرائم الإلكترونية فلا نجد اختلافا كبيرا عمّا هو الحال في الجرائم التقليدية وإن كان يتمتع بنوع من الخصوصية تتماشى مع طبيعة هذه الجرائم، فالبلاغ هنا قد يتم عن طريق الإنترنت أي ما يسمى بالبلاغ الرقمي وذلك إمّا عن طريق إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحقيق لإبلاغها عن وجود صفحا أو مواقع غير مشروعة، كإرسال رسالة إلكترونية مثلا تتضمن التبليغ عن وجود موقع منشور فيه صور للاستغلال الجنسي للأطفال إلى عنوان البريد الإلكتروني الخاص بالدرك الوطني الفرنسي:

Judiciaire@gendarmerie.gov.fr، باعتباره الجهة المختصة بالتحقيق والتحري عن تلك الجرائم بفرنسا، أو إلى موقع شرطة إدارة مكافحة جرائم الحاسبات وشبكات المعلومات المخصص لتلقي البلاغات والشكاوي في جمهورية مصر العربية، أو عن طرق ملء استمارات رقمية متواجدة في المواقع المخصصة لتلقي تلك البلاغات والشكاوي كالموقع الرسمي المركزي للإنترنت الأحداث:

http://www.internet.mineurs.gov.frوالذي يوفر إستمارة بيانات رقمية، وتجدر الإشارة إلى أنه لملء الإستمارة التوضيح والتدقيق في المعلومات لتسهيل العملية من جانب جهات التحقيق، وإلى جانب البلاغ عبر الإنترنت فإنه يمكن التبليغ عن جرائم الإنترنت بنفس الطريقة التي تتم عن طريق البريد أو مكالمة هاتفية. أنظر في ذلك:نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، مصر، ط1، سنة 2007، ص182. أيضا يمكن الإستعانة بـ (SCOCI) أي الخدمة الوطنية لتنسيق مكافحة الجريمة على الإنترنت، والذي يعتبر نقطة اتصال مركزية في الإبلاغ عن مواقع الإنترنت المشبوهة. أنظر في ذلك :

Cybercriminalité : service national de coordination de la lutte contre la cybercriminalité sur internet (SCOCI), le 07/05/2012, disponible à l'adresse suivante :
www.fedpol.admin.ch/fedpol/home/themem/kriminalitaet/cybercrime.htm.

أمّا الشكوى يقصد بها:البلاغ أو الإخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة طالبا تحريك الدعوى العمومية بشأن جرائم معينة حظر المشرع تحريكها قبل تقديمه، غير أنه كثيرا ما يصعب تحديد الجاني أو المتهم شخصيا في هذا النوع من الجرائم، وهذا ما أدى ببعض الفقه إلى ترتيب مسؤولية مزود خدمات الإنترنت عن تلك الجرائم مستندين في ذلك على مبدأ افتراض مسؤولية الغير، وهذا ما يجعل موضوع الشكوى في هذه الجرائم محل جدل قانوني في الوقت الذي كان يستخدم فيه الإستعارة عبر الإنترنت، فقد تضاربت الآراء حول الإجابة على هذا الإشكال، إذ يتجه رأي إلى قبول شكوى المجني عليه عندما يكون في حالة تخفي دون أية عوائق في هذا الإطار، أما د. عمر محمد أبو بكر بن يونس يرى إجازة ذلك إلا في حالة واحدة هي إذا كان الغرض من الإستعارة مشروعا.أنظر في ذلك: أ. نبيلة هبة هروال، المرجع السابق،ص 192.

ذلك بأن المحاكمة العادلة يجب أن تعتمد على الأدلة المحصل عليها بصفة نزيهة وشرعية، لأنه لا يجوز أن نؤسس حكما قانونيا على أدلة محصل عليها بطرق غير قانونية، فمبدأ الشرعية لا يقتصر على القواعد الموضوعية فحسب بل يشمل أيضا القواعد الإجرائية Le principe de la légalité de la preuve، وهو ما يعرف بالشرعية الإجرائية ، فكما أنه لا جريمة ولا عقوبة أو تدبير أمن إلاّ وفقا لما ينص عليه القانون، كذلك يجب أن يتم الحصول على أدلة الإثبات من طرف جهة المتابعة بطرق مشروعة ونزيهة أي دون مخالفة نصوص القانون ودون اللجوء إلى حيل ومناورات وخدع تحرّض وتدفع إلى ارتكاب الجريمة ودون المساس بحقوق الدفاع[1].

وفي نطاق المشروعية يتعين على المشرع سرعة التدخل بسن تشريعات وحصر نماذج الإجرام الإلكتروني والنص على أسس وقواعد العقاب عليها وكذا الإجراءات المتخذة بشأنها، ولا تثريب على المشرع إن هو تحرّر في هذه الإجراءات من القيود التقليدية شريطة عدم الإخلال بالمشروعية الموضوعية أو الإجرائية، وأيضا عدم الإخلال بحقوق المواطن الدستورية باعتبار أنّ الجريمة الإلكترونية هي جريمة غير تقليدية.

فشرعية الإثبات الجنائي تستلزم عدم قبول أي دليل يكون البحث عنه أو الحصول عليه قد تمّ بطريق غير مشروع، هذا البحث مقيد باحترام حقوق الدفاع من جهة وقيم العدالة وأخلاقياتها من جهة أخرى ومقتضيات الحفاظ على كرامة الإنسان من جهة ثالثة، وهو لا يتأتى إلا إذا كان البحث عن الدليل قد تم باستخدام إجراءات مشروعة[2].

والمشروعية يقصد بها: التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام ،وتهدف بصفة عامة إلى تقرير ضمانة أساسية وجدّية للأفراد لحماية حرياتهم وحقوقهم الشخصية من تعسف السلطة، وذلك بالتطاول عليها في غير الحالات التي رخص فيها القانون بذلك من أجل حماية النظام الإجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته[3].

---

[1]– أ. نجيمي جمال، المرجع السابق، ص 79.

[2]– د.طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 348.

[3]– د.أحمد ضياء الدين، مشروعية الدليل في المواد الجنائية، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2010، ص102.

لذلك فمن الأهمية لصحة الإجراءات أن تتسم بمبدأ المشروعية مما يثمر عن دليل صحيح يعوّل عليه القاضي في أحكامه، لأنّ الإجراءات القانونية إذا كانت باطلة وأثمرت عن دليل صحيح، فإنّ القاضي لا يلتفت إليه، لأنّ الهدف الذي يسعى إليه القانون هو حماية حقوق وحريات الأفراد من تعسف السلطة، وما حاجة العدالة إلى دليل صحيح في الإدانة باطل في الأساس فما بني على باطل يكون باطلا.

كما يقصد بمبدأ المشروعية ضرورة احترام القواعد القانونية القائمة بأن تكون كل السلطات العامة والأفراد في إطار القانون، وهذا يعتبر في الدولة المعاصرة حدّا أعلى لسلطان الحاكم وتصرفات الهيئات العامة والمحكومين، ويتطلب الإلتزام بالقانون الطبيعي وما يختزنه من مبادئ قانونية عامة يحتويها ضمير الجماعة ويستقر على مبدأ سيادة الدستور والتشريع[1].

وتستلزم المشروعية وفقا لهذا المعنى ضرورة ارتكاز الدليل على إجراءات مشروعة، سواء كانت تلك الإجراءات بوشرت من قبل القاضي بصورة مباشرة أو غير مباشرة أو قِبل المتهم عند استجوابه واعترافه أم قِبل الغير، ذلك أنّ إهدار المشروعية ومباشرة الإجراء بصورة مخالفة لها سيؤدي بالتأكيد إلى عدم مشروعية الدليل الناجم عنها، الأمر الذي يحتم ضرورة مراعاة كافة أحكامها باعتبارها شرطا أوليا لصحة الحصول على الدليل[2].

وبالرجوع إلى إجراءات الحصول على الأدلة الإلكترونية، فلاشك أنّها من المسائل التي تطرح مجموعة من المشاكل الموضوعية و الإجرائية في مجال التحقيق في الجرائم الإلكترونية نظرا للصعوبات العملية التي تواجه جهات التحقيق[3]،وكذا امتداد الإجراءات في بعض الأحيان إلى دول أخرى، وهذه الإجراءات بعضها إجراءات

---

[1]– د. طارق إبراهيم الدسوقي، المرجع السابق، ص 350.

[2]– أ. خليل هيكل، موقف الفقه الدستوري التقليدي والفقه الإسلامي من بناء وتنظيم الدولة، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 1989، ص 166. نقلا عن :د. طارق إبراهيم الدسوقي، المرجع السابق، ص 350.

[3]– من بين صعوبات التحقيق ما يلي:

أ– خفاء الجريمة: تتسم الجرائم الإلكترونية بطابع الخفاء، فهي تقع مستترة خفية لا يلحظها المجني عليه غالبا أو يدري حتى بوقوعها، والإمعان في حجب وإخفاء السلوك المكون لها ونتائجها عن طريق التلاعب غير المرئي في التقنيات والذبذبات الإلكترونية التي تسجل البيانات عن طريقها،كما أنّ التخريب المنطقي للأنظمة يمكن تمويهه ليبدو كما لو كان خطأ مصدره البرامج أو أجهزة نظام التشغيل.

ب– غياب الدليل المرئي الممكن فهمه بالقراءة: يتمثل أكثر مما تتيحه النظم المعلوماتية من أدلة على الجرائم التي تقع عليها أو بواسطتها في بيانات غير مرئية مسجلة إلكترونيا على دعائم أو وسائط تخزين ممغنطة، ولا يترك التعديل فيها أي أثر يمكن قراءته وإن كانت قابلة للقراءة من قبل الآلة نفسها.

ج– إفتقاد أكثر الآثار التقليدية: قد يتم في بعض العمليات إدخال البيانات مباشرة في نظام الحاسب دون تطلب وجود وثائق مساندة، كما هو الحال في بعض نظم العمليات المباشرة التي تقوم على إبدال الإذن الكتابي لإدخال البيانات بإجراءات أخرى تعتمد على ضوابط للإذن متضمنة برنامج الحاسب، فيكون من السهل ارتكاب بعض الأنواع من الجرائم بإدخال بيانات غير معتمدة في نظام الحاسب أو تعديل برامجه أو البيانات المخزنة داخله دون أن يتخلف ما يشير إلى حدوث هذا الإدخال أو التعديل.

عامة تستخدم لجمع الأدلة بكافة أشكالها ونجدها حتى في الجرائم التقليدية،وبعضها الآخر إجراءات خاصة بالجريمة الإلكترونية تتلاءم وطبيعة هذه البيئة، ولذلك كان من الضروري استحداث أجهزة عدالة متطورة تتماشى مع الجريمة الإلكترونية تتمثل في شرطة الإنترنت[1].

وعلى ذلك سيتم التطرق في المبحث الأول للإجراءات العامة لجمع الدليل الإلكتروني، أمّا المبحث الثاني فخصص للإجراءات الخاصة لجمع الدليل الإلكتروني، وقد عني المبحث الثالث بدراسة التعاون الدولي في مجال إجراءات جمع الدليل الإلكتروني.

المبحث الأول: الإجراءات العامة لجمع الدليل الإلكتروني.

سميت هذه الإجراءات بالعامة لأنها إجراءات هامة وضرورية وهامة في نطاق كشف الجرائم التقليدية والوصول إلى أدلة فيها، كما أنّها إجراءات لها الأهمية ذاتها في نطاق الجرائم الإلكترونية، وكان المشرع الجزائري قد نظم كيفية استنباطها وصولا لهذه الغاية، وأهم هذه الإجراءات كما بينها القانون هي المعاينة، التفتيش والضبط وسماع الشهود وندب الخبراء[2]، غير أن بعض الفقه يرى بأن هذه الإجراءات لها في بيئة تكنولوجيا المعلومات دور ضئيل كما سيتبين لاحقا، فالشهادة على سبيل المثال لا يبدو متصورا ورودها على السلوك المكون للجريمة الإلكترونية بحكم كونها تلاعبا في البيانات والأنظمة والبرامج غير القابلة من حيث المبدأ لأن تشاهد أو تدرك من جانب الغير حتى يمكن أن يشهد بها أمام القضاء شهادة مباشرة، ومجرد الإعتراف الذي يتم الحصول عليه عن طريق الإستجواب لايعد كافيا خاصة في مثل هذه الجرائم التقنية ما لم يدعم بأدلة أخرى، ناهيك عن الخبرة التي تتطلب بالضرورة أن يكون الخبير على مستوى عال من المعرفة والمهارة التقنية.

د- إعاقة الوصول إلى الدليل بوسائل الحماية الفنية: بحيث يشكل استخدام تقنيات التشفير خاصة لهذا الغرض أحد أكبر العقبات التي تعوق الرقابة على البيانات المنقولة عبر حدود الدولة والتي تجعل حماية سرقة البيانات الشخصية المخزنة في مراكز الحاسب أمر بالغ الصعوبة.

هـ- سهولة محو الدليل أو تدميره في وقت قصير بحيث يتمكن الجاني من محو وتدمير أدلة الإدانة في زمن قصير ، فضلا عن سهولة تنصّله من مسؤولية هذا العمل.

و- الضخامة البالغة لكم البيانات المتعين فحصها: فيشكل الكم الهائل للبيانات التي يجري في الأنظمة المعلوماتية تداولها أحد مصادر الصعوبات التي تعيق تحقيق الجرائم التي تقع عليها أو بواسطتها.

ز- الإحجام عن الإبلاغ في مجتمع الأعمال: فقد تحررت أكثر الجهات التي تتعرض أنظمتها المعلوماتية للإنتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له، وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها.أنظر في ذلك: د.رامي متولي القاضي، مكافحة الجرائم المعلوماتية، المرجع السابق، ص 101.

[1]- Eric Freyssinet, 160 Personnes luttent quotidiennement contre la cybercriminalité ,disponible à l'adresse suivante : www.journaldunet.com.

[2]- أ. عائشة بن قارة ، المرجع السابق، ص 78.

وفيما يلي بيان ذلك:

المطلب الأول: المعاينة.

إنّ التحقيق الجنائي في الجرائم الإلكترونية لم يعد ميسور لكافة المحققين وبوسائل وإجراءات التحقيق التقليدية، لأنه يواجه تقنيات حديثة في أسلوب وطريقة ارتكاب الجريمة، الأمر الذي يقتضي إحداث تطوير في قانون الإجراءات الجزائية يستوعب الإجراءات والوسائل الحديثة في كشف الجريمة وضبط فاعليها، بما يواكب استخدام وسائل التقنية والإتصالات الحديثة في ارتكاب الجرائم[1].

ويثير اتخاذ الإجراءات التقليدية في جمع الأدلة ومنها المعاينة[2]بعض الإشكاليات في التطبيق وهو ما سيتم الإشارة إليه على النحو التالي:

الفرع الأول: تعريف المعاينة في البيئة الإلكترونية.

المعاينة هي عبارة عن إجراء ينتقل بمقتضاه القائم بالتحقيق إلى مسرح الجريمة وذلك ليشاهد بنفسه ويجمع الآثار المترتبة عن الجريمة وكيفية وقوعها، وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة بغرض إثبات الجريمة[3].

وتكمن أهمية المعاينة وفاعليتها في التحقيق إلى أنّ المعاينة تتم لمسرح الجريمة، أي أنّ مكان وقوعها بما يحتويه من آثار مادية، وتهدف المعاينة كإجراء إلى التحفظ على الأدلة تمهيدا لفحصها من قبل جهات التحقيق، وتهدف إلى التحفظ على هذه الأدلة تمهيدا لفحصها من قبل جهات التحقيق لاستخلاص الدلائل والقرائن لإثبات ارتكاب الجاني لجريمته.[4]

---

[1]– د.رامي متولي قاضي، المرجع السابق، ص 106.

[2]– هناك فرق بين الإنتقال والمعاينة، فالانتقال يقصد به ذهاب جهات التحقيق إلى المكان الذي ارتكبت فيه الجريمة ، أما المعاينة فيقصد بها قيام جهات التحقيق بإثبات حالة الأشخاص والأشياء ذات الصلة بالجريمة وذلك بهدف جمع الآثار المادية التي تفيد في كشف الحقيقة قبل أن تضيع الأدلة أو يتم إتلافها عمدا. أنظر في ذلك: أ.محمد عبد اللطيف فرج، شرح قانون الإجراءات الجنائية في جمع الإستدلالات والتحقيق الابتدائي، دار النهضة العربية، القاهرة، مصر، ط2، سنة 2010، ص 03.

[3]– د. مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2003،ص 639.

[4]– د. سامح بلتاجي موسى، المرجع السابق، ص 234.

ويقصد بمعاينة مسرح الجريمة الإلكترونية معاينة الآثار التي يتركها مستخدم الإنترنت، وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الإتصالات التي تمت من خلال الحاسوب وعبر شبكة الإنترنت، كما يلاحظ أنّ الآثار الرقمية المستخلصة من أجهزة الحاسوب من الممكن أن تكون مفيدة للغاية بما تحتويه من معلومات.

وبالتالي فإن صفحات المواقع (Web Page)، البريد الإلكتروني (E-mail)، الفيديو الرقمي (Digital Vidéo)، غرف الدردشة والمحادثة والملفات المخزنة في الحاسوب الشخصي، كل هذه الوسائل والأدوات والوسائط يمكن أن تحتوي على أدلة تفيد كثيرا في كشف الحقيقة بشأن الجريمة محل التحقيق.

فمسرح الجريمة هو المكان الذي وقعت فيه الجريمة كلها أو بعضها، بحيث يتخلّف فيه آثار ارتكابها، ويرجع عدم الإهتمام بتعريف مسرح الجريمة وتحديد معالمه على وجه مفصل لاعتبارين:

الأول: أنّ معظم القوانين لا ترتب عادة آثار قانونية بالبطلان على تجاوز الحدود المكانية لمسرح الجريمة عند إجراء المعاينة، تاركة لجهات التحقيق تقدير دائرة النشاط الإجرائي في المعاينة داخل محيط اختصاصه الوظيفي حسب ما يراه ووفقا لما تقتضيه مصلحة التحقيق، طالما أنّ التوسع الميداني في هذا الإجراء ليس فيه مساس بحريات الأفراد وليس فيه خروج على قواعد الإختصاص.

الثاني: أنه لا تثور عادة بشأن تحديد المجال الميداني لمسرح الجريمة منازعة أو جدل بين الخصوم في الدعوى الجزائية أو طلب بطلان الإجراء تأسيسا على تجاوز هذا النطاق المكاني، فالمعاينة إجراء واجب من إجراءات التحقيق تفرضه القوانين على رجال الضبط والتحقيق بمجرد وصول خبر وقوعها إليهم.

وبالتالي لا يجوز لأي خصم أو طرف الإعتراض على إجراء المعاينة أو على طريقة أو أسلوب تنفيذها، فهي ليست إجراء موجه ضد شخص معين حتى ينشأ له حق الطعن فيه بالبطلان[1].

وينبغي الإشارة إلى أن المعاينة في مجال كشف غموض الجريمة الإلكترونية لا تتمتع بنفس الدرجة من الأهمية في الجريمة التقليدية، ومرد ذلك إلى ما يلي:

أولا: أنّ الجرائم التي تقع على نظم المعلومات والشبكات قلّما يترتب على ارتكابها آثارا مادية.

[1]– د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، القاهرة ، مصر، بدون طبعة، سنة 2009، ص 72.

ثانيا: أنّ عددا كبيرا من الأشخاص قد يتردد على مكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة ارتكاب الجريمة واكتشافها، مما يفسح المجال لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها وهو ما يثير الشك في الدليل المستمد من المعاينة[1]، مما يؤدي إلى طرح هذا الدليل جانبا، حيث أنّ الأحكام الجزائية تقوم على الجزم واليقين لا على مجرد الظن والتخمين.

ثالثا: إمكانية التلاعب في البيانات عن بعد أو محوها عن طريق التدخل من خلال وحدة طرفية من قبل الجاني أو معاونيه أو شركائه[2] .

وتتخذ المعاينة في الجرائم الإلكترونية عدة أشكال وذلك حسب نوعية الجرائم المرتكبة، ففي جرائم العدوان على الملكية الفكرية يتم إنزال نسخة من المصنف المعتدى عليه أو التحفظ على نسخة منه وذلك بطباعتها واستخراجها في هيئة ورقية أو صلبة، إلاّ أنّ هناك طرقا عامة تتوافق مع طبيعة النظام المعلوماتي مثل وسيلة تصوير شاشة الحاسوب وذلك بواسطة آلة تصوير تقليدية أو عن طريق استخدام برمجية حاسوب متخصصة في أخذ صورة لما يظهر عل الشاشة،وهو ما يعرف بطريقة تجميد مخرجات الشاشة، أو أن يكون ذلك عن طريق حفظ الموقع باستخدام خاصية الحفظ المتوافرة في نظام التشغيل وبها يمكن حفظ صفحة الموقع على الحاسوب[3].

الفرع الثاني: كيفية إجراء المعاينة في البيئة الإلكترونية.

في إطار الجريمة الإلكترونية فإن عملية الإنتقال والمعاينة تتم بصورة مغايرة تماما لما يحدث في الجرائم التقليدية، حيث يكون الإنتقال عبر عالم ومجتمع إفتراضيين، إلاّ أنّه ينبغي التعامل في هذا الإطار مع مسرح الجريمة الإلكترونية على أنه مسرحان:**مسرح تقليدي**:ويقع خارج بيئة الحاسوب والإنترنت ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية قد يترك فيها الجاني آثار عدة كالبصمات أو وسائط تخزين رقمية.

مسرح إفتراضي: ويقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي توجد داخل الحاسب الآلي وشبكة الإنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله[4]، ويستطيع ضابط الشرطة القضائية أو عضو

---

[1]– د.خالد ممدوح إبراهيم، فن التحقيق الجنائي، المرجع السابق،ص 154.

[2]– د. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 1997،ص 29. نقلا عن: د. خالد ممدوح إبراهيم، فن التحقيق الجنائي، المرجع السابق، ص 154.

[3]–أ. عائشة بن قارة ،المرجع السابق، ص83.

[4]– نفس المرجع ، ص 83.

سلطة التحقيق معاينة المسرح الإفتراضي وهو في مكتبه كما يمكنه أن يلجأ إلى مقهى الإنترنت أو مقر مزود بالإنترنت الذي يعد أفضل مكان يمكن من خلاله إجراء المعاينة وتتلخص هذه العوامل فيما يلي:

1- ضرورة وجود معلومات مسبقة عن مكان وقوع الجريمة وعن إعداد الأجهزة المطلوب معاينتها وأنواعها وشبكاتها وتحديد كيفية التعامل معها فنيا قبل المعاينة، من حيث الضبط أو التأمين أو حفظ المستندات والأوراق المتداولة.

2- وجود خريطة تبين الموقع الذي ستتم معاينته، ووضع خطة أمنية محكمة لعمليات المعاينة والضبط.

3- تجهيز المعدات والأجهزة والبرامج التي سيتم الإستعانة بها في عملة المعاينة.

4- إعداد فريق المتخصصين الذي سيستعان به في إجراء المعاينة وإخطاره قبل موعد إجراء المعاينة بوقت كاف للإستعداد الفني والعملي لإتمام المعاينة بدون أخطاء.

5- تحديد الأدوار وتوزيع الإختصاصات والمهام على كل عضو في فريق المعاينة.

6- مراعاة أن تتم إجراءات المعاينة في إطار المشروعية ووفقا لما تقضي به القوانين في هذا الشأن.

7- تأمين عدم انقطاع التيار الكهربائي حتى لا يحدث ثمة تلاعب في برامج شبكات وأنظمة التشغيل[1].

الفرع الثالث: ضوابط معاينة مسرح الجريمة الإلكترونية.

يشير الفقه الجنائي إلى ضرورة مراعاة مجموعة من الإجراءات أثناء المعاينة حتى تتحقق الفائدة المرجوة منها، ومن بين هذه الضوابط ما يلي:

1- تصوير الحاسوب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة على أن يتم تسجيل مكان وزمان التقاط كل صورة.

2- تسجيل كل ما يمكن ملاحظته بشأن نظام إعداد الحاسوب.

3- إتخاذ الوسائل الكفيلة بإثبات حالة التوصيلات والكابلات المتصلة بنظام الحاسب حتى يمكن المقارنة بين حالة الحاسب وقت المعاينة وحالته بعد ذلك.

4- إجراء الإختبارات اللازمة قبل نقل أي مادة معلوماتية من مكان وقوع الجريمة حتى لا يحدث أي إتلاف للبيانات المخزنة.

[1]- د. سامح بلتاجي موسى، المرجع السابق،ص 236.

5- التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة والشرائط والأقراص المغنطة التي فقدت صلاحيتها للإستعمال ورفع البصمات حيث يمكن الوقوف على الصلة بين أصحاب هذه البصمات والجريمة التي وقعت.

6- التحفظ على المستندات الخاصة بالإدخال وكذلك مخرجات الحاسب الورقية حيث يمكن الوقوف على صلتها بالجريمة.

7- ربط الأقراص الكمبيوترية التي ربما تحصل أدلة مع جهاز يمنع الكتابة أو التسجيل عليها، ممّا يتيح للمحققين قراءة بياناتها من دون تغييرها.

8- إنّ الإسراع في الإنتقال وإجراء المعاينة شرط أساسي في عملية المعاينة،كما يجب المحافظة على حالة الأمكنة قدر المستطاع وتسعى لاستغلالها على الوجه الكامل وفقا للطرق العلمية الحديثة، وهو ما حرص عليه قانون الإجراءات الجزائية فوضع نصوصا تكفل أحسن الضمانات للتحري خلال هذه المرحلة[1] وذلك عن طريق توقيع عقوبات تصل إلى حد السجن في حالة عرقلة سير العدالة،ونفس الموقف يتم إيجاده لدى المشرع الفرنسي[2].

المطلب الثاني: التفتيش.

إنّ التفتيش بصفة عامة هو إجراء من إجراءات التحقيق، بمعنى أنه يهدف إلى السعي للكشف عن الحقيقة عن طريق البحث عن الأدلة بمناسبة جريمة وقعت فعلا ويجري التحقيق بشأنها، وليس من إجراءات البحث والتحري عن الجرائم التي لم يتم التأكد من وقوعها، فالمقصود به هو دخول المساكن والأمكنة التابعة

---

[1]-أ. محمد حسين علي محمود، المرجع السابق، ص 213.

[2]- بينما في القانون الفرنسي نجد هذه الحماية منصوص عليها في المادة 55 من قانون الإجراءات الجزائية الفرنسي بالنسبة لإحداث تغييرات في مسرح الجريمة دون قصد خاص، أمّا إذا كان الفاعل يهدف إلى عرقلة عمل العدالة فإن فعله يخضع حينئذ إلى نص المادة 434-4 من قانون العقوبات الفرنسي كما يلي:

Article 434-4 (C.P.F Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002) : Est Puni de Trois ans d'emprisonnement et de 45000 euros d'amende le fait, en vue de faire obstacle à la manifestation de la vérité :

1- De modifier l'état des lieux d'un crime ou d'un délit soit par l'altération, la falsification ou l'effacement des traces ou indices, soit par l'apport, le déplacement ou la suppression d'objets quelconques.

2- De détruire soustraire receler ou altérer un document public ou privé ou un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables.

Lorsque les faits prévus au présent article sont commis par une personne qui, par ses fonctions, est appelée à concourir à la manifestation de la vérité, la peine est portée à cinq ans d'emprisonnement et à 75000 euros d'amende.

لأشخاص يظهر أنهم ساهموا في الجرم أو أنهم يحوزون أوراق أو أشياء لها علاقة بالأفعال المجرمة من طرف الضبطية القضائية أو القضاة وتفتيشها برضاء أصحابها أو جبرا عنهم، وهذا التعريف مأخوذ من نص المادة(44) من قانون الإجراءات الجزائية الجزائري.

والتفتيش كما يدل عليه المعنى اللغوي هو البحث في مسكن شخص ما أو في أي مكان آخر عن أشياء أو دلائل ذات علاقة بالجريمة، وهناك من يعرّفه بأنه إجراء للتحقيق يسمح بالبحث عن أدلة تتعلق بالجريمة في مسكن شخص أو في أي مكان توجد فيه أشياء يفيد اكتشافها في ظهور الحقيقة[1]، ويتضح من خلالها استقرائنا للتعريف السابق، أنّ التفتيش يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة وهذا تنافر مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي فهي مجرد برامج وبيانات إلكترونية ليس لها أي مظهر مادي محسوس، لذلك من الأجدر إخضاعها لأحكام مستقلة لطبيعتها الخاصة[2].

ويعد التفتيش من إجراءات التحقيق ذات الخطورة الخاصة، لكونه من الإجراءات التي تمس حق الإنسان في الخصوصية، وكونه من الإجراءات الخطيرة فإن المشرع أحاطه بمجموعة من الضمانات لصالح المتهم، يترتب على عدم إحترامها البطلان[3].

وفيما يلي سأتطرق لمفهوم التفتيش في البيئة الإلكترونية وضماناته القانونية، وذلك على النحو التالي:

الفرع الأول: مفهوم التفتيش في البيئة الإلكترونية.

لقد عرّف المجلس الأوروبي إجراء التفتيش في الجرائم الإلكترونية بأنّه الإجراء الذي يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني، فهو الإجراء الذي يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات والأدلة المطلوبة.

وفي الجرائم الإلكترونية، يتضح أنّ الدخول غير المشروع للأنظمة المعلوماتية للبحث والتنقيب في البرامج المستخدمة أو في ملفات البيانات المخزنة عما قد يتصل بجريمة وقعت، إجراء يفيد في كشف الحقيقة

[1]– أ. بحيمي جمال، المرجع السابق ، ص 387.

[2]– أ.نبيلة هبة هروال، المرجع السابق،ص 223.

[3]– د. محمد فتحي، المرجع السابق، ص 396.

عنها وعن مرتكبيها وتقتضيه مصلحة وظروف التحقيق في الجرائم الإلكترونية وهو إجراء جائز قانونا ولو لم ينص عليه صراحة باعتباره يدخل في نطاق التفتيش بمعناه القانوني ويندرج تحت مفهومه[1].

ويستلزم التفتيش عن البيانات المخزنة آليا القيام بعملية ولوج للأنظمة المعلوماتية التي يتم تحديدها لضبط ما يفيد في الكشف عن الجريمة وإيجاد أدلة الإدانة، وهذا يستدعي من جهات التحقيق أن تكون على دراية كاملة حول كيفية التعامل مع برامج وملفات البيانات المخزنة بالحاسب وكذا كلمة السر اللازمة للدخول للنظام[2].

كما يجب التنويه إلى أنّ جانب من الفقه يرى بأن الإصطلاح الواجب إطلاقه على عملية البحث عن أدلة الجريمة المرتكبة في العالم الإفتراضي هو "الولوج أو النفاذ" باعتباره المصطلح الدقيق بالنسبة للمصطلحات المعلوماتية، بينما مصطلح التفتيش يعني البحث، التفحص والتدقيق في البيانات وهو مصطلح تقليدي أكثر، كما أنّ هناك من يستخدم المصطلحين معا بغرض التنظيم والتنسيق بين المفاهيم التقليدية والحديثة[3].

وحيث أنّ تفتيش النظم المعلوماتية بصفة عامة يعدّ من أخطر المراحل مساسا بالحياة الخاصة للأفراد، على اعتبار أن التفتيش يشمل الحاسب الآلي وشبكات الإتصال، لذلك فهو يتميز بنوع من الخصوصية،وعليه سيتم البحث بشيء من التفصيل مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش، وذلك على النحو التالي:

أولا: مدى خضوع المكونات المادية للحاسب الآلي للتفتيش.

إنّ الولوج إلى المكونات المادية للحاسب الآلي بحثا عن شيء ما يتصل بجريمة إلكترونية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبيها يخضع للإجراءات القانونية الخاصة بالتفتيش،بمعنى أنّ حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات، وهل هو من الأماكن العامة أو الأماكن الخاصة، حيث أنّ لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش،فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه، وبنفس الإجراءات والضمانات المقررة قانونا في التشريعات المختلفة، مع مراعاة التمييز ما إذا كانت مكونات الحاسب الآلي المراد تفتيشها منعزلة ومستقلة عن غيرها من الحاسبات الأخرى أم أنها

---

[1]– أ.علي عدنان الفيل، المرجع السابق، ص 38.

[2]– د.عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشأة المعارف، الإسكندرية، مصر، بدون طبعة، سنة 2000، ص338.

[3]– أ. نبيلة هبة هروال، المرجع السابق، ص 294.

متصلة بحاسب آلي آخر أو بنهاية طرفية في مكان آخر كمسكن غير المتهم مثلا، فإذا كانت كذلك وكانت هناك بيانات مخزنة في هذا النظام الأخير من شأنها كشف الحقيقية، تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن.

أمّا لو وجد شخص يحمل مكونات الحاسب الآلي المادية أو كان مسيطرا عليها أو حائزا لها في مكان ما من الأماكن العامة، سواء كانت عامة بطبيعتها كالطرقات العامة والميادين والشوارع أو كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فإن تفتيشها لا يكون إلاّ في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال[1].

ثانيا: مدى خضوع المكونات المعنوية للحاسب الآلي للتفتيش.

تفتيش المكونات المعنوية للحاسب الآلي أثار خلافا كبيرا في الفقه بشأن مدى صلاحية هذه المكونات أن تكون محلا للتفتيش وانطباق مفهومه التقليدي على البحث والولوج إلى نظم الحاسوب بحثا عن أدلة تفيد في كشف الحقيقة،وإزاء ذلك إنقسم الفقه إلى اتجاهين رئيسيين:

الإتجاه الأول:

ذهب إلى جواز تفتيش البيانات الإلكترونية بمختلف أشكالها، ويستند هذا الرأي الفقهي إلى أنّ القوانين الإجرائية عندما تنص على إصدار الإذن بضبط "أي شيء" فإنّ ذلك يجب تفسيره بحيث يشمل بيانات الحاسوب المحسوسة وغير المحسوسة، لأن الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها[2].

وبالرجوع إلى نص المادة (350) من قانون العقوبات الجزائري التي تنصّ على أنّه كل من اختلس شيئا غير مملوك له يعد سارقا، فقد ذكر المشرع كلمة شيء مطلقة دون قيد ودون أن يصف هذا الشيء سواء كان مادي أو معنوي.

وعليه فبرامج الحاسب الآلي يتضمنها هذا المعنى، وبالتالي فهي تقبل التملك والحيازة وذلك باعتبارها كيانا معنويا.

---

[1]– د.هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 73.

[2]–أ. علي عدنان الفيل، المرجع السابق، ص 52

وأضم رأيي إلى رأي الأستاذة "أمال قارة" حينما قالت أنّ هذا الإعتراف لا يعد خروجا عن مبدأ الشرعية فنصوص السرقة تقبل هذا التفسير لأنّها:

1. لا تحدد صفة الشيء محل الجريمة، مادي أو معنوي.

2. هي أشياء معنوية يصدق عليها وصف المال.

3. الظروف والوقت الذي وضعت فيه نصوص السرقة، حيث كانت الأموال المعنوية قليلة العدد والقيمة، وأنّ الحماية الجزائية آنذاك كانت مركزة على حماية الأموال المنقولة المادية، فلم تكن هذه الأشياء المعنوية في ذهن المشرع وقت وضع النصوص السابقة[1].

الإتجاه الثاني:

يرى أنه لا ينطبق المفهوم المادي على بيانات الحاسوب غير المرئية أو غير الملموسة، ولذلك فإنّهم يقترحون مواجهة هذا القصور التشريعي بالنص صراحة على أنّ تفتيش الحاسوب لابد أن يشمل المواد المعالجة عن طريق الحاسب الآلي أو بياناته، بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الإتصالات عن بعد تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسوب[2]، فهذه المكونات المعنوية غير الملموسة لا تصلح بطبيعتها للتفتيش إلا بوجود أحكام خاصة تكون مناسبة أكثر للطبيعة الفنية والتقنية لهذه المعلومات[3].

وبخصوص المشرع الجزائري فقد عاقب على الإعتداءات الماسة بسلامة المعالجة الآلية للمعطيات، إذ جرّم العديد من الأفعال التي تشكل بمختلف صورها الجريمة الإلكترونية، وكان ذلك بموجب القانون رقم (15/04 المؤرخ في 10 نوفمبر 2004)، وقد سبق الإشارة إليه الذي استحدث القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

ومسايرة من المشرع الجزائري للتطورات المعاصرة فقد أصدر القانون رقم (09-04 الصادر في 08 غشت 2009) السابق ذكره أيضا والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام

---

[1]- أ. أمال قارة، المرجع السابق، ص 29.

[2]- د.علي عدنان الفيل، المرجع السابق، ص 43.

[3]- د.موسى مسعود، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون من 28-10/29 /2009، أكاديمية الدراسات العليا، طرابلس، ليبيا، ص 05.

والإتصال ومكافحتها، ونص في المادة الخامسة (05)[1]منه على جواز تفتيش منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها.

وإلى جانب المشرع الجزائري يوجد كذلك المشرع الفرنسي الذي قام بتعديل نصوص التفتيش، حيث أضاف عبارة المعطيات المعلوماتية في المادة (94)[2] من قانون الإجراءات الجزائية الفرنسي.

وبالرجوع إلى إتفاقية بودابست بشأن الجرائم الإلكترونية، فقد نصت على أنّ لكل دولة طرف من حقها أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة بالتفتيش أو الولوج إلى نظام كمبيوتر أو جزء منه أو المعلومات المخزنة فيه، وكذا الوسائط التي يتم تخزين معلومات الكمبيوتر بها مادامت مخزنة في إقليمها طبقا لنص المادة (1/19)[3] من هذه الإتفاقية.

غير أن مكونات الحاسب المعنوية أثارت مشكلة لا مادية بيانات الحاسب الآلي، فيذهب رأي فقهي إلى أنّه في تحديد مدلول الشيء بالنسبة لمكونات الحاسب الآلي، يجب عدم الخلط بين الحق الذهني للشخص على البرامج والكيانات المنطقية، وبين طبيعة هذه البرامج والكيانات، وإنّما يتعين الرجوع في ذلك إلى تحديد مدلول كلمة المادة في العلوم الطبيعية، فإذا كانت المادة تعرّف بأنّها كل ما شغل حيزا ماديا في فراغ معين وأنّ الحيز يمكن قياسه والتحكم فيه، وكانت الكيانات المنطقية أو البرامج تشتغل حيزا ماديا في ذاكرة الحاسب الآلي ويمكن قياسها بمقياس معين هو البايت (Byte) والكلوبايت (Kilo Byte) والميجابيت(Mega Byte)، وهكذا تقاس سعة أو حجم الذاكرة الداخلية للحاسب بعدد الحروف التي يمكن تخزينها بها، كما أنها تأخذ شكل نبضات إلكترونية فإنها تعد طبقا لذلك ذات كيان مادي وتتشابهه مع التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبيل الأشياء المادية[4].

---

[1]– تنص المادة (05) من القانون رقم 09-04 السالف الذكر على ما يلي: " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه، الدخول بغرض التفتيش، ولو عن بعد، إلى :

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

ب– منظومة تخزين معلوماتية ...".

[2]-Article 94 (C.P.P.F Modifié par LOI n°2010-768 du 9 juillet 2010 - art. 1) : Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets ou des données informatiques dont la découverte serait utile à la manifestation de la vérité, ou des biens dont la confiscation est prévue à l'article 131-21 du code pénal.

[3]- Article 19/1 du C.C.C : Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a. à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b. à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.

[4]– د.هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق،ص 88.وكذلك: أ. علي عدنان الفيل، المرجع السابق،ص 42.

ويخلص هذا الرأي الفقهي، إلى أن برامج الحاسب الآلي ينطبق عليها خصائص المادة، وبالتالي تدخل في نطاق الأشياء المادية، ويستوي في ذلك أن تكون برامج نظام أو برامج تطبيقات، إذ لا يوجد أي إختلاف فيما يتعلق بطبيعتهما[1].

ويرى الدكتور "سامح بلتاجي موسى" أن المكونات المعنوية للحاسب الآلي لها وجود مادي فعلي، وتعد المكونات المعنوية للحاسوب و شبكاته كذلك منقولا لإمكان نقلها من مكان لآخر، فضلا عن إمكانية تملكها وحيازتها.

كما أن إنكار إضفاء هذه الصفة على اعتبار أنها ليست جسما متحيزا قابلا للوزن طبقا للنظريات الطبيعية قول خاطئ تماما، راجع إلى عدم الفهم الصحيح لطبيعة وماهية المنقول، وطبيعة وماهية المكونات المعنوية للحاسوب وشبكاته، وهي مال لأنها ذات قيمة مالية، وهي كذلك منقول وذلك لإمكانية حيازتها وملكيتها ونقلها من مكان لآخر[2].

ثالثا : مدى خضوع شبكات الحاسب الآلي للتفتيش (التفتيش عن بعد).

أجهزة الحاسوب ترتبط بعضها ببعض أحيانا عن طريق شبكات، وتلك الشبكات قد تكون داخل الشركة أو المؤسسة وفروعها داخل الحدود الإقليمية لنفس الدولة، وقد يستتبع تفتيش جهاز حاسوب معين الدخول إلى جهاز حاسوب آخر ينتمي إلى شخص آخر في مكان آخر.

كما أنه قد تظهر التحقيقات ضرورة تفتيش جهاز حاسوب متواجد خارج حدود تلك الدولة، كما لو تعلق الأمر بشركة رئيسية وفروعها في الخارج حينما ترتبط أجهزة تلك الشركة بعضها ببعض عن طريق شبكة الإنترنت، وأحيانا ترتبط بعض أجهزة الحاسوب بقاعدة بيانات متواجدة في خارج الدولة التي تجري سلطاتها التحقيق في شأن إحدى الجرائم الإلكترونية[3]، وهو ما يطلق عليه الفقه الفرنسي مصطلح التفتيش على المباشر[4].

---

[1]– د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 89.

[2]–د. سامح بلتاجي موسى، المرجع السابق، ص 255.

[3]– نفس المرجع، ص 255.

[4]- Yann Padova, un aperçu de lutte contre la cybercriminalité en France, RSCP, N°04, Dalloz, 2002, P650.
نقلا عن: أ. عائشة بن قارة، المرجع السابق، ص 109.

ويمكن التمييز في هذه الصورة بين احتمالين:

الإحتمال الأول:إتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة.

تسمح الإتفاقية الأوروبية لجرائم الإنترنت لعام 2001 للدول الأعضاء أن تمدّ نطاق التفتيش الذي كان محله جهاز كمبيوتر معين إلى غيره من الأجهزة المرتبطة به في حالة الإستعجال إذا كان يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش[1]، وذلك طبقا لنص المادة (2/19)[2].

أمّا المشرع الجزائري، فمن خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها فقد أجاز لجهات التحقيق إمتداد التفتيش إلى منظومة معلوماتية أخرى، إذا كان هناك إعتقاد بأنّ المعطيات المبحوث عنها مخزنة لديها بشرط أن تكون هذه المعطيات يمكن الدخول إليها بدءا من المنظومة الأولى، كما أضاف المشرع ضرورة إخطار السلطة القضائية المختصة مسبقا بذلك[3]،وقبله بذلك كان المشرع قد منح ضباط الشرطة القضائية إختصاصات أوسع في حالة ما إذا كانت التحريات الأولية التي يجريها تخص إحدى الجرائم المتعلقة بالمخدرات أو تبييض الأموال أو المتعلقة بالتشريع الخاص بالصرف أو الماسة بأنظمة المعالجة الآلية للمعطيات والجريمة المنظمة عبر الحدود الوطنية وكذا جرائم الفساد، فقد أصبح بموجب تعديل قانون الإجراءات الجزائية يتمتع بصلاحيات واسعة وذلك من أجل تيسير عملية البحث والتحري عن تلك الجرائم نظرا لطبيعتها الخاصة، كما مكّن ضباط الشرطة القضائية من اختصاصات جديدة سيتم التطرق لها في حينها.

---

[1]– د. طارق فوزي الفقي، المرجع السابق، ص 104.

[2]- Article 19/2 du C.C.C : Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 (a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou un d'un accès d'une façon similaire à l'autre système.

[3]– تنص المادة 5 فقرة 02 من القانون رقم 09-04 السالف الذكر:" ...في الحالة المنصوص عليها في الفقرة أ من هذه المادة، إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها ، انطلاقا من المنظومة الأولى ، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك ...".

وإلى جانب المشرع الجزائري، نجد المشرع الفرنسي قام هو الآخر بتعديل قانون الإجراءات الجزائية فقد نصت المادة (57-1/1)[1] على أنه يجوز لضباط الشرطة القضائية أو تحت مسؤولياتهم أعوان الشرطة القضائية، الدخول عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي تم فيها التفتيش على المعطيات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر، بما أنّ هذه المعطيات يتم الدخول إليها أو تكون متاحة إنطلاقا من النظام الرئيسي.

وبخصوص امتداد إذن التفتيش داخل إقليم الدولة، فإن بعض الفقه يعارض امتداد إذن التفتيش إلى الأجهزة المرتبطة لأنّ هذا الأمر سوف يعطي لجهات التحقيق سلطة واسعة، خاصة وأنّ العديد من أجهزة الحاسبات الآلية تكون مرتبطة ببعضها البعض، وبالتالي تمتد هذه السلطة إلى تفتيش أجهزة كثيرة خاصة إذا تم التفتيش دون إخطار الشخص غير المتهم أو حضور من ينوب عنه ولا شك أنّ ذلك يثير شكوك حول مدى مشروعية إجراءات التفتيش في هذه الحالة.

الإحتمال الثاني: أن يكون الحاسب المراد تفتيشه متصلا بنهاية طرفية أو جهاز حاسب آخر خارج حدود الدولة.

قد يلجأ بعض مرتكبي الجرائم تهربا من إمكانية الخضوع للتفتيش إلى تخزين بياناتهم في أنظمة تقنية المعلومات خارج إقليم الدولة عن طريق إدراجها في شبكة الإتصالات البعدية Télécommunication Network الأمر الذي يثير صعوبات أمام جهات التحقيق فيما يتعلق بإجراء التفتيش وجمع الأدلة، وفي هذه الحالة فإن امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من قبلها الإذن ودخوله في المجال الجغرافي لدولة أخرى، وقد يسميه البعض التفتيش عبر الحدود قد يتعذر القيام به بسبب تمسك الدولة بسيادتها[2].

ومن أجل القضاء على صعوبات إجراءات التحقيق، لابد من تعاون دولي في هذا الإطار، لأنه في حالة تجاوز التفتيش إقليم دولة إلى دولة أخرى، فإنه لا يجوز القيام بهذا التفتيش في حالة عدم وجود إتفاقيات

---

[1]- Article 57-1/1 (C.P.P.F Créé par Loi 2003-239 2003-03-18 art. 17 1° JORF 19 mars 2003, Créé par Loi n°2003-239 du 18 mars 2003 - art. 17) : Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

[2]– أ. علي عدنان الفيل، المرجع السابق، ص 46.

ثنائية أو دولية تسمح للدولة القيام بهذا التفتيش العابر للحدود[1]، لأنه في حالة عدم السماح للدول بالتحقيق سيفسح المجال أمام المجرمين للإفلات من العقاب، وهذا ما يؤكد على أهمية التعاون الدولي في مجال إجراءات جمع الأدلة الذي وسنخصص له المبحث الثالث من هذا الفصل.

وقد أكد المجلس الأوروبي في التوصية رقم (17) 1995، على أنّه يمكن أن يمتد نطاق تفتيش الحاسوب إلى النظام المتواجد في الخارج إذا كانت هناك ضرورة لاتخاذ إجراءات عاجلة في هذا الأمر ويتوجب أن يتمّ الحصول على موافقة الدولة التي يمتد التفتيش إلى الأجهزة أو النظام المتواجد في إقليمها، وذلك حتى يكون هذا التفتيش ذو أساس قانوني وكي لا يمثل إنتهاك لسياسة تلك الدولة.

كما أجازت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية من خلال المادة (32)[2] إمكانية الولوج بغرض التفتيش والضبط في أجهزة أو شبكات متعددة متواجدة داخل الحدود الإقليمية لدول أخرى بدون إذن من تلك الدول وذلك في حالتين:

1. عندما تكون البيانات متاحة للجمهور ويمكن لأي أحد الدخول إليها.
2. عندما يكون لدى الطرف الذي دخل أو تسلم البيانات خارج الإقليم عبر نظام حاسوبي في إقليمه الحصول على رضاء قانوني وإرادي ممن يملك سلطة قانونية للكشف عن تلك البيانات عبر النظام الذي تمّ الولوج داخله، فعلى سبيل المثال فإنّ البريد الإلكتروني للشخص يمكن أن يكون مخزنا في دولة أخرى من قِبل مزود الخدمة بهذه الدولة أو يمكن أن يقوم الشخص بتخزين البيانات في دولة أخرى، إذن بافتراض أنّ لهؤلاء سلطة قانونية فإنّه يمكن له استرداد البيانات أو القيام بالكشف عنها بإرادتهم إلى السلطات المسؤولة أو السماح لهم بالدخول إلى البيانات وفقا لما هو مقرر في هذه المادة[3].

أمّا المشرع الجزائري فقد أجاز تمديد التفتيش عن معطيات مبحوث عنها، والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى، بحيث أنها تكون مخزنة في منظومة معلوماتية تقع خارج إقليم الدولة ويكون ذلك

---

[1]– د. محمد أبو العلاء عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، من 26-28 أفريل 2003، دبي، الإمارات العربية المتحدة، ص 34.

2- Article 32 C.C.C :Une Partie peut, sans l'autorisation d'une autre Partie, :
a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou
b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

[3]– د. سامح بلتاجي موسى، المرجع السابق، ص259.

بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية، ووفقا لمبدأ المعاملة بالمثل المعمول به في العلاقات الدولية [1].

وكذلك المشرع الفرنسي فإنه أجاز بموجب المادة (57-2/1)[2] من قانون الإجراءات الجزائية الفرنسي لضابط الشرطة القضائية أن يقوم بتفتيش الأنظمة المتصلة حتى ولو كانت خارج الإقليم.

وفيما يتعلق بامتداد التفتيش خارج إقليم الدولة، وإن كانت بعض التشريعات قد أجازته بما في ذلك التشريع الجزائري، إلاّ أنّ البعض يتحفظ على القيام بهذا الإجراء في حالة عدم علم الدولة التي سوف يمتد إذن التفتيش داخل إقليمها، لأنّ ذلك يعد انتهاكا لسيادة الدولة، فالقاعدة تقضي بعدم جواز تطبيق قانون العقوبات الأجنبي على إقليم الدولة، وعدم نفاذ إذن التفتيش أو القبض وغيرها من الإجراءات من السلطات الأجنبية على إقليم دولة أخرى، إلا إذا استثنينا المعلومات التي تكون متاحة للجمهور كما يحدث في حالة الندوات أو الرسائل التي تجرى عبر الإنترنت والتي يمكن لكافة الناس الإشتراك فيها، فهي لا تعد من أعمال التفتيش ولا تحتاج لموافقة من دولة أخرى[3].

وعليه يتعين على الدول الدخول في اتفاقيات دولية وثنائية تنظم هذه المسألة من أجل إعطاء ضمانات لهذا التفتيش، تتمثل في عدم خرق سيادة الدول الأخرى وعدم إتاحة الفرصة من جهة أمام المجرمين للإفلات من العقاب من خلال تعمدهم تخزين البيانات التي تشكل دليل إدانة ضدهم في منظومة معلوماتية متواجدة في إقليم دولة أخرى، الأمر الذي يشكل تحديا إجرائيا واضحا لدى جهات التحقيق، مع ضرورة الإشارة إلى أنّ الإجراءات على المستوى الدولي نلتمس فيها البطء وعدم الفاعلية مما قد يترتب عليه ضياع الأدلة وطمس معالمها[4].

---

[1]- تنص المادة 05 فقرة 03 من القانون من القانون رقم 09-04 السالف الذكر: " ...إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإنّ الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل ...".

[2]- Article 57-1/2 (C.P.P.F Créé par Loi 2003-239 2003-03-18 art. 17 1° JORF 19 mars 2003, Créé par Loi n°2003-239 du 18 mars 2003 - art. 17) :S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

[3]- د. شيماء عبد الغني، المرجع السابق، ص 303.

[4]- أ.رشاد خالد عمر، المرجع السابق، ص 138

الفرع الثاني: الضمانات القانونية لتفتيش نظم الحاسب الآلي.

إذا كان الوصول إلى الحقيقة يمثل الغاية من الإجراءات الجزائية، ففي كل الحالات فإنّ الغاية لا تبرر الوسيلة،كما أنّ البحث عن الحقيقة لا ينبغي أن يكون طليقا من أي قيد، بل يخضع لضوابط معينة حتى لا يتعسف من يسعى للحصول عليها، فلابد أن تكون هناك مواءمة بين البحث عن الحقيقة مع مراعاة واحترام الحقوق والحريات، باعتبار أنّ التفتيش إجراء يمس صميم الحرية الشخصية، لذا حرصت أغلبية القوانين على إحاطته بشروط وضمانات أساسية من أجل تحقيق الموازنة الضرورية بين مصلحة المجتمع في القصاص من المجرم وردعه وبين حريات الأفراد[1]، وتنقسم الشروط العامة للتفتيش إلى نوعين من الشروط، شروط موضوعية وأخرى شكلية، وذلك على النحو التالي:

أولا: الشروط الموضوعية لتفتيش نظم الحاسب الآلي.

يقصد بالشروط الموضوعية للتفتيش بصفة عامة في الجرائم التقليدية، وعلى وجه الخصوص في الجرائم الإلكترونية هي الشروط اللازمة لإجراء تفتيش صحيح، وهي في المعتاد تكون سابقة له[2]، ويمكن حصر هذه الشروط في: السبب، المحل، والسلطة المختصة بإجرائه، وسيتم التفصيل في كل شرط من هذه الشروط.

1- سبب التفتيش في البيئة الإلكترونية:

سبب التفتيش في الجرائم التقليدية بوصفه إجراء من إجراءات التحقيق هو وقوع جناية أو جنحة واتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها، وتوافر إمارات قوية أو قرائن على وجود أشياء تفيد في كشف الحقيقة لدى المتهم أو غيره[3]، وحتى تبرز خصائص التفتيش المقصود في قانون الإجراءات الجزائية، يجب أن يتم استبعاد أنواع أخرى من التفتيش التي تقوم به جهات إدارية أخرى، وذلك في إطار تنظيم وتسيير المرافق المكلفة بالإشراف عليها، مثل التفتيش الذي تقوم به مصالح الجمارك للأشخاص والبضائع وفقا لأحكام قانون الجمارك[4]، وكذلك التفتيش الذي تقوم به مصالح السجون من تفتيش وقائي

---

[1]- د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي ، المرجع السابق، ص 93.

[2]- أ.عائشة بن قارة، المرجع السابق، ص 99.

[3]- د.هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي ، المرجع السابق، ص 104.

[4]- قانون رقم 07/79 مؤرخ في 21 يوليو 1979 المتضمن قانون الجمارك المعدل و المتمم.

للأشخاص والأمكنة[1]،أو ما تقوم به مختلف أسلاك الأمن بعد إعلان حالات الطوارئ أو الحصار أو الحالة الإستثنائية[2]، وبالتطبيق في مجال الحاسب الآلي لابد أن نكون أولا بصدد جريمة إلكترونية واقعة بالفعل سواء كانت جناية أو جنحة، ولابد ثانيا اتهام شخص أو أشخاص معينين بارتكاب هذه الجريمة الإلكترونية أو المشاركة فيها، ولابد ثالثا من الإعتقاد بوجود معلومات أو أجهزة معلوماتية تتعلق بالجريمة وتفيد في كشف الحقيقة لدى المتهم أو غيره[3]، وفيما يلي تفصيل ذلك:

1.1- أن نكون بصدد جريمة إلكترونية واقعة بالفعل:

بادئ ذي بدء لابد أن يكون التفتيش على إثر وقوع جناية أو جنحة بالضرورة، والمشرع الجزائري لم ينص على المخالفة طبقا لنص المادة (44) من قانون الإجراءات الجزائية، وفي الواقع لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة الإلكترونية، وهذه المسألة سبق التطرق إليها بالتفصيل في الفصل الأول من هذا الباب، فلابد لصحة إجراء التفتيش أن تكون الجريمة محلها هو المعلومات وتكون من أجل الإضرار بمكونات الحاسب وشبكات الإتصال الخاصة به التي يحميها القانون ويفرض لها عقابا، وبمفهوم المخالفة إذا لم تكن جريمة إلكترونية، فإنّه لا يصح التفتيش عن المعلومات أو عن الأجهزة المعلوماتية أو جهاز الحاسب الآلي الخاص بالشخص، طالما أنّ الدلائل لم تدل على وجود معلومات تتعلق بالجريمة في هذه الوسائل[4].

فالجريمة الإلكترونية تقتضي وجود نشاط إجرامي يتمثل في عمل غير مشروع يقع على وسيلة من وسائل التقنية التي تستخدم فيها المعلومات بطريقة مباشرة أو غير مباشرة، على أن تكون هذه الأفعال معاقب عليها، لأنه لا جريمة ولا عقوبة إلا بنص، فلا يمكن تطبيق عقوبة ما لم تكن محددة سلفا، ومؤدى هذه السمة الأخيرة أن يحدد قانون العقوبات مقدما الأفعال التي تعتبر جرائم إلكترونية والعقوبات المقررة لها، وهذا ما فعله المشرع الجزائري حين تصدى لتجريم مجموعة من الأفعال الماسة بسلامة المعالجة الآلية للمعطيات بما في ذلك الدخول أو البقاء عن طريق الغش في منظومة للمعالجة الآلية للمعطيات وهيما يعرف باللغة الفرنسية (STAD)[5]، حذف أو تغيير المعطيات داخل منظومة للمعالجة الآلية للمعطيات تم

---

[1]- قانون رقم 04/05 مؤرخ في 06 فبراير 2005 المتضمن قانون تنظيم السجون وإعادة الإدماج الإجتماعي للمحبوسين، ج ر رقم 12.

[2]- المواد 91 و92 و 93 من دستور 1996 المعدل بالقانون رقم 08-19 المؤرخ في 15 نوفمبر 2008، ج ر رقم 63.نقلا عن : أ. نجيمي جمال ، المرجع السابق، ص 400.

[3]- د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي ، المرجع السابق، ص 104.

[4]- د. بكري يوسف بكري، المرجع السابق، ص 87.

[5]-STAD : تعني: Système de traitement automatisé de donnée (Automated information) وتعني: AIS ، أما بالإنجليزية

الدخول إليها عن طريق الغش، تخريب نظام اشتغال منظومة للمعالجة الآلية للمعطيات، أو إزالة أو تعديل البيانات التي تتضمنها بنفس الطريقة، التعامل مع المعطيات التي تسمح بارتكاب الجرائم الإلكترونية، حيازة أو استعمال المعطيات المحصل عليها عن طريق إحدى الجرائم المعلوماتية، المشاركة في جمعية أشرار تعد للقيام بالجرائم الإلكترونية[1]، ومن خلال استقراء هذه النصوص من المادة (394 مكرر) إلى المادة (394 مكرر 7)من قانون العقوبات الجزائري يتبين وجود تدرج في النظام العقابي، وهذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات.

أمّا المشرع المصري، فقد أضفى حمايته الجنائية لمجالين من مجالات الحاسوب وهما:

الأول: البرامج وقواعد البيانات، وهذه اعتبرها ضمن المصنفات المشمولة بحماية حق المؤلف المنصوص عليها في قانون حماية الملكية الفكرية المصري سنة 2002.

الثاني: البيانات الفردية التي تقتضي إجراء إحصاء للسكان، وكذلك البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين، وفي القانون رقم (143) لسنة 1994 في شأن الأحوال المدنية، أما باقي جرائم الإنترنت سواء أكان الحاسب الآلي محلا للجريمة أو أداة لارتكابها فلا تشملها الحماية الجنائية[2].

وجاء ضمن توصيات المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات، والذي عقد في البرازيل من 4 إلى 9 سبتمبر سنة 1994 قائمة من الأفعال غير المشروعة التي تقع على الحاسبات الآلية، وهذه الأفعال هي كما يلي[3]:

أ- الغش المرتبط بالحاسوب: ويتضمن الإدخال والإتلاف والمحو وطمس البيانات أو برامج الحاسوب أو أي عوائق تؤثر في مجرى البيانات.

ب- التزوير المعلوماتي: ويتضمن الإدخال والإتلاف والمحو، ويكون منصوص عليها في التشريع الوطني بوصفها جريمة تزوير للإضرار ببرامج وبيانات الحاسوب و يشمل: المحو والإتلاف، التعطيل غير المشروع للبيانات والبرامج المعلوماتية.

وقد سبق شرح هذا المصطلح.System

[1]- أ. نجيمي جمال، المرجع السابق، ص 263.

[2]-د. سامح بلتاجي موسى، المرجع السابق، ص 264.

[3]- نقلا عن : نفس المرجع، ص 265.

ج–تخريب الحواسيب: ويحتوي على الإدخال والإتلاف لبيانات وبرامج الحاسوب أو أي عائق آخر للنظم المعلوماتية بنية تعطيل وظيفة الحاسوب.

د– الدخول غير المصرح به: وهو الولوج غير المشروع لنظام معلوماتي أو مجموعة نظم معلوماتية عن طريق انتهاك الإجراءات الأمنية.

هـ–الإعتراض غير المصرح به: وهو إعتراض بدون وجه حق، يتم عن طريق وسائل فنية للإتصال تتجه نحو نظام معلوماتي أو عدة نظم أو شبكة اتصالات، حيث تعمل من خلال تواجدها داخل هذا النظام المعلوماتي أو مجموعة النظم الشبكية.

وما ينبغي الإشارة إليه إلى أنّه لا يكفي مجرد وقوع جريمة من الجرائم الإلكترونية كي يجوز إجراء التفتيش بشأنها، وإنما يتعين أن تكون هذه الجريمة جناية أو جنحة.

ويخلص القول أنّ الشرط الأول من شروط سبب تفتيش نظم الحاسب الآلي، وهو أن نكون بصدد جريمة إلكترونية واقعة بالفعل، سواء كانت جناية أو جنحة، بمعنى أنه يهدف إلى السعي لكشف الحقيقة عن طريق البحث عن الأدلة بمناسبة جريمة واقعة بالفعل، أي لا يصح القيام به لضبط جريمة ستقع في المستقبل، ولو قامت التحريات والدلائل الكافية على أنها ستقع بالفعل.

2.1– إتهام شخص أو أشخاص معينين بارتكاب الجريمة الإلكترونية أو المشاركة فيها:

ينبغي أن تتوافر في الشخص المراد تفتيشه–أي تفتيش شخصه أو تفتيش مسكنه– دلائل كافية تدعو للإعتقاد بأنه قد ساهم في ارتكاب الجريمة الإلكترونية سواء بصفته فاعلا أو شريكا مما يستوجب اتهامه بها، بحيث إذا لم تتوافر هذه الدلائل، كان على قاضي التحقيق بأن يصدر أمرا بأن لا وجه لإقامة الدعوى[1] وهذا ما تؤكده المادة (163)[2] من قانون الإجراءات الجزائية الجزائري، ونفس الفكرة يمكن تأكيدها في المادة (177)[3] من قانون الإجراءات الجزائية الفرنسي.

والحال ذاته بالنسبة للتفتيش في البيئة الإلكترونية، إذ لا يكفي وقوع جريمة إلكترونية فقط، بل يجب أن يكون ذلك الوقوع مقترنا بنسبها إلى شخص أو أشخاص معينين إما بصفتهم فاعلين أصليين

---

[1]– د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 115.

[2]– تنص المادة 163 فقرة 1 من قانون الإجراءات الجزائية الجزائري:"إذا رأى قاضي التحقيق أن الوقائع لا تكون جناية أو جنحة أو مخالفة، أو أنّه لا توجد دلائل كافية ضد المتهم، أو كان مقترف الجريمة ما يزال مجهولا، أصدر أمرا بأن لا وجه لمتابعة المتهم".

[3]-Article 177 / 1 (C.P.P.F Modifié par Loi n°2004-575 du 21 juin 2004 - art. 2 JORF 22 juin 2004) : Si le juge d'instruction estime que les faits ne constituent ni crime, ni délit, ni contravention, ou si l'auteur est resté inconnu, ou s'il n'existe pas de charges suffisantes contre la personne mise en examen, il déclare, par une ordonnance, qu'il n'y a lieu à suivre.

أو شركاء أو بصيغة أخرى يجب توفر دلائل كافية تدعو للإعتقاد بأنّ ذلك المشتبه فيه قد ساهم في ارتكاب تلك الجريمة سواء كفاعل أصلي أو شريك[1]، إلاّ أنّ السؤال الذي يطرح نفسه في هذا المجال يدور حول المقصود بهذه الدلائل الكافية.

الواقع لم تتعرض قوانين الإجراءات الجزائية سواء في الجزائر، في مصر أو فرنسا لتعريف الدلائل الكافية، وإنما اكتفى بالنص على تطلب الدلائل القوية والمتوافقة على الإتهام، إلاّ أنّ الفقه لم يترك الأمر دون أن يتصدى لتحديد مفهوم الدلائل الكافية فعرفها الفقه المصري بأنها:« مجموعة من الوقائع الظاهرة الملموسة التي يستنتج منها أنّ شخصا معينا هو مرتكب الجريمة » [2].

وهناك من عرفها بأنها:« إمارات معينة تستند إلى العقل، وتبدأ من ظروف أو وقائع يستنتج منها الفعل توحي للوهلة الأولى بأنّ جريمة ما وقعت وأنّ شخصا معينا هو مرتكبها، وهذه الأمارات لا يكفي في تقديرها مجرد المنطق، بل لابد في شأنها تدخل الخبرة والتعقل»[3].

وفي الولايات المتحدة الأمريكية، عبر قانون الإجراءات الجنائية الأمريكي عن الدلائل الكافية باصطلاح السبب المعقول أو المحتمل، كما استخدم التعديل الرابع للدستور الأمريكي نفس هدا التعبير، حين نص على حق المواطنين في تأمينهم في أشخاصهم ومنازلهم وأرواحهم ومستنداتهم ضد أي تفتيش غير قانوني ما لم تكن بناء على سبب معقول، كذلك فقد درج القضاء الأمريكي على استخدام هذا المصطلح في أحكامه المختلفة[4].

ويفرق الفقه[5] في مفهوم الدلائل الكافية بين الدلائل الكافية لاكتساب الشخص صفة المتهم والتي تكفي فيها مجرد الشكوك المعقولة، وبين الدلائل الكافية لإحالة الشخص إلى سلطات التحقيق والتي يلزم فيها أن تكون من القوة بحيث ترجح فيها الإدانة على البراءة.

---

[1]– د. بكري يوسف بكري، المرجع السابق، ص 92.

[2]–د. محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، مصر، ط7، سنة 2005، ص226.نقلا عن: عائشة بن قارة، المرجع السابق، ص 102.

[3] – د. بكري يوسف بكري، المرجع السابق، ص94.

[4] – ومن ذلك ما قضت به المحكمة العليا في الولايات المتحدة الأمريكية أنّ السبب المعقول لا يعني أكثر من الشك البسيط، واستطردت تقول أنّ السبب المعقول يوجد في حالة الوقائع والظروف التي تكفي بذاتها للدلالة في تقدير الشخص الحريص على وقوع جريمة من الشخص الذي يراد القبض عليه. د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص117

[5]– د.أحمد فتحي سرور، المرجع السابق، ص640.

وفي مجال الحاسب الآلي يمكن القول بأنّ تعبير الدلائل الكافية يقصد به مجموعة من المظاهر أو الأمارات المعينة القائمة على العقل والمنطق والخبرة الفنية والحرفية للقائم بالتفتيش، والتي تؤيد نسبة الجريمة الإلكترونية إلى شخص معين بوصفه فاعلا أو شريكا[1].

3.1- الإعتقاد بوجود معلومات أو أجهزة معلوماتية عند المتهم أو غيره:

يلزم لصحة إجراء التفتيش أن يكون هناك اعتقاد بوجود معلومات وفقا لما انتهينا إليه من كون التفتيش يشمل بالإضافة إلى المكونات المادية لوسائل التقنية الحديثة المكونات المعنوية والتي تتمثل في المعلومات ولو تمثلت في شكل غير ملموس، أو الإعتقاد بوجود أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة عن الجريمة الإلكترونية التي يجري التفتيش بشأنها لدى المتهم أو لدى غيره، فيلزم أولا أن تتوافر لدى جهات التحقيق الإعتقاد المبني على الدلائل الكافية بالكيفية المذكورة في العنصر السابق، ويلزم أيضا أن يتعلق هذا الإعتقاد بوجود معلومات أو أجهزة أو معدات أو أي أشياء أو مستندات إلكترونية أو أشياء متحصلة من الجريمة تفيد في كشف حقيقة الجريمة الإلكترونية التي يجري التفتيش بشأنها[2]، وبالتالي فإنّ مجرد وقوع جريمة سواء جناية أو جنحة واتهام شخص معين بارتكابها أو المشاركة فيها لا يكفي لجهات التحقيق إصدار إذنها بالتفتيش ومباشرتها، إذ أنّ المعيار لإصدار هذا الإذن أن تكون الدلائل التي تجمعت حول الجريمة تدعو للإعتقاد المعقول بوقوعها، سواء أكان من تجمعت حوله هذه الدلائل فاعلا أصليا لها أم يقف دوره الإجرامي عند حدود الشريك[3].

2- محل التفتيش في البيئة الإلكترونية.

المحل الذي يقع عليه التفتيش للحصول على أدلة في الجرائم الإلكترونية هو جهاز الحاسب الآلي بمكوناته المادية والمعنوية وشبكات الإتصال الخاصة به، وهذه الأخيرة تشتمل على الخادم والمزود الآلي والملحقات التقنية والتي قد تكون في حوزة شخص أو تكون موضوعة في مكان له حرمة المسكن[4].

وبالرجوع لما تم التطرق إليه حول مدى جواز تفتيش نظم الحاسوب فيما يتعلق بمكوناته المادية والمعنوية، فقد تم تناول تفاصيل ذلك فيما سبق، وكذلك فيما يخص مدى إمكانية تفتيش شبكات

---

[1]- د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، 121.

[2]-د. بكري يوسف بكري، المرجع السابق، ص95.

[3]-د.خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص213.

[4]- د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 126.

الحاسوب على النحو السابق عرضه، ولذلك سوف تخصص الدراسة للشخص كمحل للتفتيش في الجرائم الإلكترونية، وكذا المسكن وما في حكمه كمحل للتفتيش في نظم وشبكات الحاسوب والإنترنت.

1.2- المقصود بالشخص كمحل لتفتيش نظم الحاسب الآلي.

عندما يكون الشخص محلا للتفتيش في الجرائم الإلكترونية، فإنه قد يكون من مستغلي أو مستخدمي شبكة الإنترنت أو من الخبراء في مجال البرمجيات، سواء أكانت برامج نظام أو برامج تطبيقات، وقد يكون من المحللين أو من مهندسي الصيانة والإتصالات أو مديري النظم المعلوماتية أو من مزودي خدمات الإنترنت أو من المسؤولين عنها، أو من أشخاص آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية أو أجهزة حاسوب محمولة أو هواتف متصلة بجهاز المودم أو مخرجات أو مستندات أو أكواد، أو غير ذلك مما يتعلق بالجريمة محل البحث، وفي كل الحالات يقصد بالشخص كمحل قابل للتفتيش كل ما يتعلق بكيانه المادي وما يتصل به ويشمل جسم الإنسان وملابسه وأمتعته التي في حوزته متنقلا بها باعتبارها من توابع الشخص[1].

لكن السؤال المطروح، هل يدخل في مضمون هذه الأمتعة السيارة التي قد يستخدمها الشخص في نقل وإخفاء الأجهزة المعلوماتية، وبالتالي تعتبر إمتدادا لشخصه، فتخضع للقواعد المتعلقة بتفتيش الأشخاص؟

في الواقع المشرع الجزائري لم يتناول في قانون الإجراءات الجزائية هذا الموضوع، مما ترك المجال مفتوحا أمام كل الإجتهادات، كما أن مسألة صلاحيات الضبطية القضائية في شأن تفتيش الأشخاص أو بطلان الأدلة المحصل عليها من خلاله لم تطرح بكيفية واضحة وصريحة على القضاء، وربما يعود الأمر إلى عدة عوامل منها جهل المواطن بحقوقه المدنية في مواجهة السلطة العامة، واختلاط المسائل الأمنية بمسائل القانون العام مما يولد شعورا بالخشية لدى المواطن من تفسير اعتراضه تفسيرا بعيدا عن القانون، ولهذا يجب الرجوع إلى أحكام القانون الفرنسي في هذا الشأن للإسترشاد بها باعتبار أن التشريع الجزائري تابع للمدرسة الفرنسية[2].

---

[1]- د. سامح أحمد بلتاجي موسى، المرجع السابق، ص267.

[2]- أ. نجيمي جمال، المرجع السابق، ص 433.

وبناءا على ذلك يعتبر تفتيش الأشخاص في التشريع الفرنسي مماثلا لتفتيش المساكن ويحظى بنفس الحماية القانونية خلافا للتفتيش الوقائي[1]، فهو يعتبر باطلا وكذا الإجراءات التالية له إذا قام به ضابط الشرطة القضائية في حين ليس هناك أي تحقيق مفتوح، وأنّه لا توجد أي علامات ظاهرة تدل على وجود جنحة تنسب للشخص الموقوف، ومن جهة أخرى يعتبر باطلا كل تفتيش أو حجز يقوم بهما عون الشرطة القضائية دون الموافقة الصريحة للشخص الذي تقع عنده العملية، في حين ليس هناك تحقيق موجود أو تصرف مشبوه[2].

وبالرجوع إلى السؤال الذي طرح المتعلق بتفتيش السيارات، فهو ملحق بالتفتيش المعمق للأشخاص باعتبار أن صاحب السيارة يضع فيها غالبا أشياء من خصوصياته وهو مطمئن أنّ لا أحد يطلع عليها بدون إذنه، خصوصا إذا وضعها في الصندوق الداخلي أو الخلفي للسيارة، ولذلك فتفتيشها لا يكون إلاّ من طرف الضبطية القضائية، وقد تناولت أحكامه نصوص المواد (78-2-2) إلى (78-2-4) من قانون الإجراءات الجزائية الفرنسي، وهذا التفتيش يشمل ثلاث حالات هي[3]:

1. يمكن تفتيش السيارات التي تسير في الطريق العمومي أو تتوقف فيه أو تتوقف في أماكن عمومية، وذلك بأمر من وكيل الجمهورية وفي أي وقت من نهار أو ليل، من أجل البحث أو متابعة جرائم محددة، ويتم بحضور السيارة أو سائقها أو بحضور شاهد ليس تابعا لمصالح الضبطية القضائية[4].

2. كما يمكن تفتيش السيارات في الأماكن المذكورة أعلاه في حالة وجود أسباب معقولة تفيد أن السائق أو أحد الركاب يوجد في حالة تلبس بجناية أو جنحة أو الشروع في ذلك[5].

---

[1]– التفتيش السطحي الوقائي هو ما يمكن تسميته بالتلمس الأمني palpation de sécurité، وهو التفتيش الذي يقتصر على التلمس الخارجي من خلال تمرير اليدين على أنحاء مختلفة من الجسم فوق الملابس، إلى جانب استعمال أجهزة مسح يمر عبرها الشخص كما تمر أمتعته في أجهزة مماثلة، فهو يدخل في إطار الضبط الإداري الهادف إلى تفادي وقوع جريمة ولا يتطلب أي إذن أو ترخيص من السلطة القضائية. أنظر في ذلك أ. نجيمي جمال، المرجع السابق، ص431.

[2]– نفس المرجع ، ص 434 .

[3]– نفس المرجع، ص 441.

[4] - Article 78-2-2 (C.P.P.F Modifié par Ordonnance n°2012-351 du 12 mars 2012 - art. 9) :Pour l'application des dispositions du présent article, les véhicules en circulation ne peuvent être immobilisés que le temps strictement nécessaire au déroulement de la visite qui doit avoir lieu en présence du conducteur. Lorsqu'elle porte sur un véhicule à l'arrêt ou en stationnement, la visite se déroule en présence du conducteur ou du propriétaire du véhicule ou, à défaut, d'une personne requise à cet effet par l'officier ou l'agent de police judiciaire et qui ne relève pas de son autorité administrative. La présence d'une personne extérieure n'est toutefois pas requise si la visite comporte des risques graves pour la sécurité des personnes et des biens.

[5] - Article 78-2-3 (C.P.P.F Créé par Loi n°2003-239 du 18 mars 2003 - art. 12, Créé par Loi n°2003-239 du 18 mars 2003 - art. 12 JORF 19 mars 2003) **:** Les officiers de police judiciaire, assistés, le cas échéant, des agents de police judiciaire et des agents de police judiciaire adjoints mentionnés aux 1°, 1° bis et 1° ter de l'article 21, peuvent procéder à la visite des véhicules circulant ou arrêtés sur la voie publique ou dans des lieux accessibles au public lorsqu'il existe à l'égard du conducteur ou d'un passager une ou plusieurs raisons

plausibles de soupçonner qu'il a commis, comme auteur ou comme complice, un crime ou un délit flagrant ; ces dispositions s'appliquent également à la tentative.

3. وأخيرا يمكن تفتيش السيارات في الأماكن المذكورة أعلاه في حالة وجود خطر يهدد أمن الأشخاص أو ممتلكاتهم ويكون بموافقة المعني بالأمر أو بإذن من وكيل الجمهورية[1].

أمّا إذا كانت السيارة مركونة في مستودع صاحبها أو في مستودع خاص فيتم تفتيشها وفق أحكام تفتيش المساكن، وهكذا فالقاعدة أن تفتيش السيارات لا يكون إلا بإذن من وكيل الجمهورية أو حالة علامات الجرم المشهود أو بموافقة سائق السيارة، وبالتالي لا يجوز التفتيش تلقائيا من طرف الضبطية القضائية في حالة التحريات العادية، أمّا في مجال الضبط الإداري فتطبق القواعد العامة وهي جواز التفتيش بشرط موافقة صاحبها، وإن رفض فيمكنه عدم دخول الأمكنة المحروسة (مطارات، فنادق مؤسسات...).

ولمحكمة النقض المصرية نفس الموقف إذ تعتبر أنّ تفتيش السيارات هو بمثابة تفتيش المساكن والأشخاص، فتحيطه بنفس الضمانات إلاّ إذا كانت السيارة مهملة في مكان عام[2].

2.2- المقصود بالمسكن وما في حكمه كمحل لتفتيش نظم الحاسب الآلي.

المقصود بالمسكن في قانون الإجراءات الجزائية وقانون العقوبات الجزائري هو كل مكان معد للسكن سواء كان بناية أو خيمة أو كشكا ثابتا أو متنقلا، فالعبرة بالإستعمال ونيته اتخاذه مأوى ومكانا خاصا للإقامة وحفظ السر عن الآخرين ومكانا لخصوصيات المرء وأسراره، وكذلك كافة توابعه مهما كان استعمالها كالأفنية وسطوح المنازل وحواضر الدواجن والمخازن والإسطبلات...حتى ولو كانت مفصولة بسياج داخل المحيط العام لذلك السكن[3].

Les dispositions des deuxième, troisième et quatrième alinéas de l'article 78-2-2 sont applicables aux dispositions du présent article.

[1] - Article 78-2-4 (C.P.P.F Créé par Loi n°2003-239 du 18 mars 2003 - art. 13, Créé par Loi n°2003-239 du 18 mars 2003 - art. 13 JORF 19 mars 2003) :Pour prévenir une atteinte grave à la sécurité des personnes et des biens, les officiers de police judiciaire et, sur l'ordre et sous la responsabilité de ceux-ci, les agents de police judiciaire et les agents de police judiciaire adjoints mentionnés aux 1°, 1° bis et 1° ter de l'article 21 peuvent procéder non seulement aux contrôles d'identité prévus au septième alinéa de l'article 78-2 mais aussi, avec l'accord du conducteur ou, à défaut, sur instructions du procureur de la République communiquées par tous moyens, à la visite des véhicules circulant, arrêtés ou stationnant sur la voiepublique ou dans des lieux accessibles au public.

Dans l'attente des instructions du procureur de la République, le véhicule peut être immobilisé pour une durée qui ne peut excéder trente minutes.

Les deuxième, troisième et quatrième alinéas de l'article 78-2-2 sont applicables aux dispositions du présent article.

[2]- ومن قضائها في هذا الشأن، لا يجوز تفتيش السيارات الخاصة بالطرق العامة بغير إذن من سلطة التحقيق وفي غير أحوال التلبس، إلا إذا كانت خالية وكان ظاهر الحال يشير إلى تخلي صاحبها عنها. الطعن رقم 1747 لسنة 29 بتاريخ 04-04-1960، نقلا عن: أ.نجيمي جمال، المرجع السابق، ص443.

[3]- أ. نجيمي جمال، المرجع السابق، ص 398.

أمّا قانون الإجراءات الجزائية الجزائري فقد ذكر "تفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني"[1]، وبالتالي فقد توسعت أحكام التفتيش لتشمل محلات مهنية كمكاتب أصحاب المهن الحرة كالأطباء والمحامين والموثقين والمحضرين، وكان لابد من إيجاد معيار تفرقة لتحديد الأماكن المحمية بأحكام التفتيش من غيرها من الأماكن المباحة، وعليه فالأماكن المحمية هي تلك التي لا يجوز الدخول إليها عادة إلاّ بإذن صاحبها، أما باقي الأماكن المفتوحة للجمهور فلا تشملها الحماية ويمكن تفتيشها بصفة عادية، كما أنّ الأماكن التي لا يتخذها المرء سكنا بالمعنى العام لا تشملها الحماية المذكورة[2].

وعلى ذلك يرى الدكتور هلالي عبد اللاه أحمد أنه إذا وجدت مكونات نظم وشبكات الحاسوب سواء كانت مكونات مادية أو معنوية أو شبكات اتصال مرتبطة بها في أي مكان من الأمكنة المذكورة، فإنّ تفتيش هذه المكونات يخضع لذات قواعد تفتيش المساكن أو المحل المتواجدة به.

3- السلطة المختصة بالتفتيش.

لقد خولت المواد (79 إلى 81) من قانون الإجراءات الجزائية الجزائري لقاضي التحقيق الإختصاص بالإنتقال إلى منازل المتهمين أو المشتبه فيهم، أو الذين بحوزتهم أشياء لها علاقة بالجريمة لتفتيشها والحصول على الأدوات المستعملة في الجريمة والمسروقات، وغير ذلك مما يفيد في اكتشاف الجريمة، كما يجوز له أيضا الإنتقال إلى أي مكان يمكن العثور فيه على أشياء من شأن كشفها أن يكون مفيدا للتحقيق أو مكان ارتكاب الجريمة ليقوم بإجراء عملية التفتيش به، غير أنّه يجوز لقاضي التحقيق إذا تعذر عليه القيام بهذه العملية بنفسه أن ينيب ضابط الشرطة القضائية للقيام بعملية التفتيش.وبالنسبة للأحكام المتعلقة بقاضي التحقيق، فالتفتيش أمر جوازي بالنسبة له، وإذا أراد أن يقوم بذلك فعليه إخطار وكيل الجمهورية الذي يحق له أن يرافقه، وإذا حصل التفتيش في مسكن المتهم فعلى قاضي التحقيق أن يلتزم بأحكام المواد من (45 إلى 47) من قانون الإجراءات الجزائية[3]، غير أنه بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات لا تطبق هذه الشروط، باستثناء الأحكام المتعلقة بالحفاظ على السر المهني، وكذا جرد الأشياء وحجز المستندات[4].

---

[1]- تنص المادة 45 فقرة 3 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري) على ما يلي : " ...غير أنه يجب عند تفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر ...".

[2]-أ.بحيمي جمال، المرجع السابق، ص398.

[3]- نفس المرجع، ص 419.

[4]- تنص المادة 45 فقرة أخيرة من قانون الإجراءات الجزائية الجزائري على ما يلي:" ...لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، باستثناء الأحكام المتعلقة بالحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات المذكورة أعلاه ."

وإذا كان الأصل أن يقوم قاضي التحقيق أو النيابة العامة بإجراء التفتيش بنفسه، إلا أنه عمليا غالبا ما تسند هذه المهمة لضابط الشرطة القضائية الذي يتصرف في حالة الجرم المشهود، وقد يتصرف في حالة التحريات العادية، ونظرا للحماية الدستورية والقانونية لحرمة المسكن فإنّ قانون الإجراءات الجزائية قد نص على الإجراءات الواجب احترامها حتى تكون عملية التفتيش صحيحة[1].

1.3- تفتيش نظم الحاسب الآلي بناءا على إذن قضائي بإجرائه:

إنّ سلطة التحقيق الأصلية غير مطالبة بإجراء التفتيش بنفسها في كل الحالات، بل لها أن تلجأ إلى الإنابة في بعض الحالات، فتقوم بندب أحد ضباط الشرطة القضائية لإجرائه، فهو عبارة عن تفويض يصدر من سلطة التحقيق المختصة إلى أحد ضباط الشرطة القضائية مخولا إياه إجراء التفتيش الذي تختص به أصلا تلك السلطة[2]، لذلك ينبغي أن يراعي في إصداره وتحريره جميع القيود الخاصة بالإنابة القضائية.

وينبغي أن تكون هذه الإنابة القضائية متضمنة الإذن بالتفتيش، ساعة وتاريخ صدورها واسم من أصدرها، إسم المأذون له بالتفتيش وإسم المأذون بتفتيش مسكنه وعنوان المسكن والمهمة المقصودة من وراء التفتيش والمهلة المحددة لإجرائه، وقد أوجبت المادة (3/44) من قانون الإجراءات الجزائية الجزائري أن يتضمن الإذن المذكور بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي سيتم زيارتها وتفتيشها وإجراء الحجز فيها وذلك تحت طائلة البطلان، كما أنّ عمليات التفتيش والحجز تنجز تحت الإشراف المباشر للقاضي الذي أذن بها، ويصبح حينها ضابط الشرطة القضائية مقيدا بالقيود التي تقيد قاضي التحقيق[3]، وعليه سوف يتم التطرق إلى ضمانات الإذن بتفتيش نظم الحاسب الآلي، والنتائج المترتبة على هذا الإذن بالتفتيش.

أ. ضمانات الإذن بتفتيش نظم الحاسب الآلي:

من المستقر عليه أنّ من حق رجال الضبط القضائي دخول الأماكن العامة دون الحصول على إذن مسبق، وذلك بهدف الإشراف على تنفيذ القوانين واللوائح، وهذا الحق لا يجيز لضباط الشرطة القضائية أن يقوموا بفتح الأشياء المغلقة الموجودة في المحال العامة، وهذا ما قضت به محكمة النقض المصرية[4]، لأنّه إجراء إداري مقيد بالغرض السابق لا ينبغي أن يتجاوز التعرض إلى حرية الأشخاص واستكشاف الأماكن المغلقة.

---

[1]- أ. نجيمي جمال، المرجع السابق، ص 405.

[2]- د. سامح بلتاجي موسى، المرجع السابق، ص 268.

[3]- أ. محمد حزيط ، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، ط3، سنة 2008، ص 120.

[4]- "لرجال السلطة العامة في دوائر اختصاصهم دخول المحال العامة المفتوحة للجمهور لمراقبة تنفيذ القوانين والقرارات وهذا إجراء إداري مقيد بالغرض سالف البيان ولا يجاوزه إلا التعرض إلى حرية الأشخاص أو استكشاف الأشياء المختلفة غير الظاهرة" نقض أول نوفمبر سنة 1987، مجموعة أحكام النقض المصرية 38 ص 917 رقم 169. نقلا عن: أ. نبيلة هبة هروال، المرجع السابق، ص 248.

وبتطبيق ذلك في المجال الإلكتروني فإنه ليس من حق رجال الضبط القضائي عند دخولهم إلى مقاهي الإنترنت أن يقوموا بفتح الكمبيوتر المغلق لأنهم دخلوا كأشخاص عاديين فهم يتمتعون بنفس الحقوق التي يتمتع بها غيرهم من الأفراد وهي استعمال أجهزة الكمبيوتر بالمقابل المادي المعتاد، كما لا يجوز لهم فتح الأجهزة لمعرفة المواقع التي استعملها شخص جالس على الجهاز لكي يميز من بينها ما يعتبر منافيا للآداب وما لا يعتبر،فهذا العمل لا يدخل ضمن التحريات بل يحتاج إلى إذن للتفتيش.

فالجريمة الإلكترونية كغيرها من الجرائم يمكن أن تتوافر فيها شروط الجريمة المتلبس بها، كأن يكون ضابط الشرطة القضائية في أحد مقاهي الإنترنت ويلاحظ وجود شخص آخر عبر تلك الشبكة في المواقع الإباحية، يقوم بطباعة الصور المتواجدة فيها بواسطة الطابعة، ففي هذه الحالة تحققت شروط التلبس، وبالتالي من الجائز في هذه الحالة القبض على هذا الشخص وتفتيشه[1]، غير أنّ رجل الضبط القضائي ليس من حقه أن يقوم بإجراءات تفتيش تلك الأماكن إلاّ بعد الحصول على إذن بذلك، ويعد ذلك من قبيل إجراءات التفتيش التي ينبغي أن تتوافر على شروط معينة حتى يكون التفتيش صحيحا ويمكن الإعتماد على النتائج التي يسفر عنها، وبالرجوع إلى المادة (44)[2] من قانون الإجراءات الجزائية فقد حددت شروطا لصحة التفتيش في حالة الجرم المشهود، وسأحاول تطبيق هذه الشروط في مجال الحاسب الآلي كما يلي:

- أن تتوافر العلامات الدالة على حالة التلبس.
- أن يكون المسكن أو مكان إجراء التفتيش تابعا لشخص ساهم في الجريمة أو يحوز أوراقا أو أشياء لها علاقة بها، فإذا انتفت رابطة السببية فلا يجوز تفتيش محله.
- الحصول على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق.
- الإستظهار بذلك الإذن قبل الدخول إلى المسكن أو المكان.

---

[1]– أ.نبيلة هبة هروال، المرجع السابق، ص248.

[2]– تنص المادة 44 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري) على ما يلي: " لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلاّ بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الإستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش.

ويكون الأمر كذلك في حالة التحري في الجنحة المتلبس بها أو التحقيق في إحدى الجرائم المذكورة في المادتين 37 و 40 من هذا القانون.

يجب أن يتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي ستتم زيارتها وتفتيشها وإجراء الحجز فيها، وذلك تحت طائلة البطلان.

تنجز هذه العمليات تحت الإشراف المباشر للقاضي الذي أذن بها والذي يمكنه عند الإقتضاء أن ينتقل إلى عين المكان للسهر على احترام أحكام القانون...".

- أن يتضمن ذلك الإذن وصف الجرم وعنوان المكان، ومن المفيد عمليا أن تحدد في الإذن ساعة إصداره إلى جانب التاريخ لأنّ ذلك يفيد في التأكد من صدوره قبل القيام بعملية التفتيش التي يجب أن يذكر توقيتها في محضر التفتيش[1]، غير أنه أبرز ما يتم التأكيد عليه في هذا الصدد هو أن يكون إذن التفتيش محددا خصوصا في محله والأشياء المراد البحث عنها لضبطها، أو بمعنى آخر واصفا بشكل خاص ودقيق الشيء المراد ضبطه، كما لو تضمن ذلك الإذن القيام بتحديد القطع الصلبة المكوّن منها الحاسوب، فالواقع في التشريعات، كما هو الحال في القضاء الأمريكي يطلب التحديد كشرط لازم لصحة الإذن والتفتيش[2].

فإذا ما كان الإذن الصادر بضبط المعلومات في حين قام رجل الضبط القضائي بضبط الجهاز فقد أضحى تنفيذ الإذن مخلا بشرط التحديد، في حين لا يعد الإذن مخلا بشرط التحديد إذا ما تضمن النص على ضبط وتفتيش الجهاز والأقراص المضبوطة وكل البرامج التي تحتوي على أدلة تفيد في كشف الحقيقة، وإذا ما صدر الإذن بضبط الجهاز فليس هناك ما يمنع من ضبط الأقراص الممغنطة التي تكون على مقربة منه، وهذا يتماثل مع القواعد العامة التي تقر أنّ الإذن الصادر بتفتيش المسكن يمتد إلى ملحقاته، كما قد يصدر إذن بتفتيش شخص المتهم ويكون يحمل معه جهاز كمبيوتر محمول أو يقود سيارة بها جهاز كمبيوتر، فإذن التفتيش يشمل الكمبيوتر على اعتبار أنّ الكمبيوتر في كلا الحالتين من ملحقات الشخص[3].

أمّا بالنسبة للملفات، فالأصل هو ضرورة تحديد تلك الملفات محل التفتيش في الإذن، ولكن ذلك يرد عليه استثناء إذا ما وجدت دلائل كافية على وجود ملفات مشبوهة في نفس الجهاز مع جواز أن تكون الصياغة شاملة لتحديد الأشياء محل التفتيش، غير أنّ شرط التحديد صعب نظرا للطبيعة الخاصة للكمبيوتر لاحتوائه على عدد كبير من الملفات والتي لا تدل أسماءها على ما تحتويه بالضرورة، وذلك بوضع المتهم إسم مستعار في حين أن الملف يحتوي على ما يشكل جريمة، وبالتالي هل يعتبر كل ملف صندوقا مغلقا يحتاج كل منها إلى إذن قضائي مستقل عن الآخر؟

---

[1]- أ. نجيمي جمال، المرجع السابق، ص 406.

[2]- United States V.Hay, 231F.3d630, 634 (9th cir, 2000), United States V.Campres, 221F.3d1143, 1147 (10th cir 2000) available online : www.cybercrime.gov/s&smanual2002.hmt.

نقلا عن : د. شيماء عبد الغني، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الأزاريطة، مصر، بدون طبعة، سنة 2007، ص289.

[3]- كما قضت محكمة النقض المصرية بأنّ: حرمة السيارة الخاصة مستمدة من اتصالها بشخص صاحبها أو حائزها نقض 30 يونيو سنة 1969 س30 ص976، رقم 193، 26 نوفمبر سنة 1984 س35 ص 829 رقم 187. نقلا عن:د. شيماء عبد الغني، المرجع السابق، ص289.

في إجابته عن هذا السؤال صدرت للقضاء الأمريكي أحكاما اعتبرت القرص بما فيه من ملفات وجهاز الكمبيوتر بما يحتويه من ملفات صندوقا مغلقا مستقلا، وبالتالي فإنّ هذه الأحكام لا تستوجب صدور إذن قضائي مستقل لكل ملف على حدى[1].

وعلى خلاف ذلك، إتجهت أحكام أخرى للقضاء الأمريكي إلى أنّ كل ملف في الكمبيوتر يتطلب إذنا لتفتيشه، وبناءا على ذلك اعتبرت أن الملف الواحد صندوقا مغلقا، ويرجع السبب في اعتبار الملف الواحد صندوقا مغلقا هو أنّ الكمبيوتر يحتوي على الكثير من المعلومات التي تتعلق بالحياة الخاصة لصاحب هذا الجهاز وإذا أخذنا في الإعتبار أنّه يجوز لرجال الضبط القضائي فتح الملفات الأخرى الموجودة في داخل جهاز الكمبيوتر، فإن ذلك سوف يؤدي بالفعل إلى الإعتداء على الحياة الخاصة التي يتمتع بها الأفراد[2].

كما أنّ القانون الجزائري لم ينص على تحديد مدة زمنية لتنفيذ هذا الإذن، إلاّ أنّه ما دمنا أمام جريمة إلكترونية وما تتطلبه من سرعة لضبط الأدلة قبل تلاشيها أو ضياعها أو العبث بها، فإنه من المفروض أن يتم التنفيذ فورا.

أمّا الأحكام المتعلقة بدعوة صاحب المكان للحضور أو دعوة شاهدين لمرافقة الضابط لا تطبق إذا تعلق الأمر بالجرائم الإلكترونية، أمّا إذا كان التفتيش في أماكن يشغلها شخص ملزم بكتمان السر المهني (كالموثقين والمحامين والأطباء)، فيجب اتخاذ التدابير اللازمة لضمان احترام ذلك السر، غير أن السر المهني لا يمنع مبدئيا من حجز أي وثيقة تفيد في الوصول إلى الحقيقة ما عدا إذا كانت تضر بحقوق الدفاع، غير أنّ قانون الإجراءات الجزائية لم يحدد المقصود بهذه التدابير غير أن قانون المحاماة[3] من خلال نص المادة (22)[4] اشترط حضور النقيب أو ممثليه تحت طائلة البطلان المطلق[5].

---

[1]- United States V.Runyan, 275F.3d449, 464-65 (5th cir, 2001), available online : www.cybercrime.gov/s&smanual2002.hmt.

نقلا عن : د.شيماء عبد الغني، المرجع السابق، ص 290.

[2] -SAV.Walser 275.F.3d,918,986 (10thCir.2001), available online : www.cybercrime.gov/s&smanual2002.hmt.

نقلا عن : نفس المرجع، ص 290.

[3]- قانون رقم 13-07 مؤرخ في 29أكتوبر 2013 يتضمن تنظيم مهنة المحاماة، ج ر رقم 55.

[4]- تنص المادّة 22من قانون تنظيم مهنة المحاماة على ما يلي:"لا يمكن إنتهاك حرمة مكتب المحامي.
لايتم أي تفتيش أو حجز في مكتب المحامي إلا من قبل القاضي المختص بحضور ا لنقيب أو مندوبه أو بعد إ خطارهما قانونا.
تعد باطلة الإجراءات المخالفة للأحكام المنصوص عليها في هذه المادة."

[5]- أ. نجيمي جمال، المرجع السابق، ص 407.

كما أنّ المادة (07) من قانون تنظيم مهنة المحضر القضائي[1] لا تجيز التفتيش إلاّ بناءا على أمر قضائي مكتوب ويكون بحضور رئيس الغرفة الوطنية للمحضرين القضائيين، وكل إجراء يخالف هذه المادة يقع تحت طائلة البطلان، وفي نفس السياق نصت المادة (04) من قانون تنظيم مهنة الموثق[2] على أن مكتب التوثيق لا يجوز تفتيشه إلا بناءا على أمر قضائي مكتوب، ويكون بحضور رئيس الغرفة الجهوية للموثقين أو من يمثله.

غير أنّ هذه النصوص لم تبين دور ممثل التنظيم المهني، كما أنّها لم تشمل بحمايتها مساكن أصحاب هذه المهن واقتصرت على مكان العمل فقط، أمّا بالرجوع إلى قانون الإجراءات الجزائية الفرنسي فنجده قد نص على هذه التفاصيل في نص المادة (56-1)[3]، فشملت الحماية مكتب ومسكن المحامي، كما بيّن النص

---

[1]– قانون رقم 06-03 المؤرخ في 21 محرم 1427 الموافق لـ 20-02-2006 المتضمن قانون تنظيم مهنة المحضر القضائي، ج ر رقم 14.

[2]قانون رقم 06-02 المؤرخ في 21 محرم 1427 الموافق لـ 20-02-2006 المتضمن قانون تنظيم مهنة الموثق، ج ر رقم 14.

[3]-Article 56-1 (C.P.P.F Modifié par LOI n°2010-1 du 4 janvier 2010 - art. 3 (V)) **:** Les perquisitions dans le cabinet d'un avocat ou à son domicile ne peuvent être effectuées que par un magistrat et en présence du bâtonnier ou de son délégué, à la suite d'une décision écrite et motivée prise par ce magistrat, qui indique la nature de l'infraction ou des infractions sur lesquelles portent les investigations, les raisons justifiant la perquisition et l'objet de celle-ci. Le contenu de cette décision est porté dès le début de la perquisition à la connaissance du bâtonnier ou de son délégué par le magistrat. Celui-ci et le bâtonnier ou son délégué ont seuls le droit de consulter ou de prendre connaissance des documents ou des objets se trouvant sur les lieux préalablement à leur éventuelle saisie. Aucune saisie ne peut concerner des documents ou des objets relatifs à d'autres infractions que celles mentionnées dans la décision précitée. Les dispositions du présent alinéa sont édictées à peine de nullité.
Le magistrat qui effectue la perquisition veille à ce que les investigations conduites ne portent pas atteinte au libre exercice de la profession d'avocat.
Le bâtonnier ou son délégué peut s'opposer à la saisie d'un document ou d'un objet s'il estime que cette saisie serait irrégulière. Le document ou l'objet doit alors être placé sous scellé fermé. Ces opérations font l'objet d'un procès-verbal mentionnant les objections du bâtonnier ou de son délégué, qui n'est pas joint au dossier de la procédure. Si d'autres documents ou d'autres objets ont été saisis au cours de la perquisition sans soulever de contestation, ce procès-verbal est distinct de celui prévu par l'article 57. Ce procès-verbal ainsi que le document ou l'objet placé sous scellé fermé sont transmis sans délai au juge des libertés et de la détention, avec l'original ou une copie du dossier de la procédure.
Dans les cinq jours de la réception de ces pièces, le juge des libertés et de la détention statue sur la contestation par ordonnance motivée non susceptible de recours.
A cette fin, il entend le magistrat qui a procédé à la perquisition et, le cas échéant, le procureur de la République, ainsi que l'avocat au cabinet ou au domicile duquel elle a été effectuée et le bâtonnier ou son délégué. Il peut ouvrir le scellé en présence de ces personnes.
S'il estime qu'il n'y a pas lieu à saisir le document ou l'objet, le juge des libertés et de la détention ordonne sa restitution immédiate, ainsi que la destruction du procès-verbal des opérations et, le cas échéant, la cancellation de toute référence à ce document, à son contenu ou à cet objet qui figurerait dans le dossier de la procédure.
Dans le cas contraire, il ordonne le versement du scellé et du procès-verbal au dossier de la procédure. Cette décision n'exclut pas la possibilité ultérieure pour les parties de demander la nullité de la saisie devant, selon les cas, la juridiction de jugement ou la chambre de l'instruction.
Les dispositions du présent article sont également applicables aux perquisitions effectuées dans les locaux de l'ordre des avocats ou des caisses de règlement pécuniaire des avocats. Dans ce cas, les attributions confiées au juge des libertés et de la détention sont exercées par le président du tribunal de grande instance qui doit

حالة اعتراض النقيب أو ممثله عن حجز بعض الوثائق وكيفية حل هذه المسألة من قبل قاضي الحريات، فقد أجاز اعتراض النقيب أو ممثليه على حجز وثيقة ينوي القاضي حجزها إذا رأى أنّ ذلك الحجز غير شرعي، وعندئذ توضع الوثيقة في حرز مغلق ومختوم ويحرر بهذه العمليات محضر يشير إلى اعتراض النقيب أو ممثله ولا يرفق ملف الإجراءات، وإذا كانت هناك وثائق أخرى تم حجزها أثناء التفتيش دون وقوع اعتراضات بشأنها فإن المحضر الخاص بها المنصوص عليه بالمادة (57) يكون منفصلا عن محضر الإعتراض، وهذا المحضر مع الوثيقة الموضوعة في حرز مختوم تحال فورا إلى قاضي الحريات مع أصل ملف الإجراءات أو نسخة منه، وفي الأيام الخمسة من استلام هذه الوثائق يفصل قاضي الحريات والحبس في هذه المنازعة بموجب أمر غير قابل للطعن.

ومن أجل ذلك، فإنّه يقوم بسماع القاضي الذي قام بالتفتيش،وعند الإقتضاء لوكيل الجمهورية وكذا المحامي الذي وقع في مكتبه أو في مسكنه التفتيش والنقيب أو ممثله، ويمكنه فتح الحرز بحضور هؤلاء الأشخاص، فإن تراءى له أنّه لا داعي لحجز الوثيقة فإنّ قاضي الحريات والحبس يأمر بإرجاعها فورا أو إتلاف المحضر المتعلق بالعملية، وفي الحالة العكسية فإنّه يأمر بإدراج الحرز والمحضر في ملف الإجراءات، وهذا القرار لا يمنع الأطراف لاحقا من طلب بطلان الحجز سواء أمام جهة الحكم أو أمام غرفة التحقيق.

أمّا اختصاصات ضباط الشرطة القضائية في حالة التحريات العادية، فالقانون في هذه الحالة لا يجيز تفتيش المساكن إلاّ برضا صريح من صاحب المسكن، فضلا عن احترام أحكام المواد (44 إلى 47) من قانون الإجراءات الجزائية الجزائري المتعلقة بوجوب الحصول على إذن من وكيل الجمهورية، فما يمكن ملاحظته أنّ اشتراط المشرع للإذن القضائي في الحالتين يعني أنّ موافقة أو عدم موافقة صاحب المسكن في حالة التحريات الأولية لا معنى لها[1].

وبالرجوع إلى النصوص التقليدية المنظمة للتفتيش، فإن حدث عرضا وأن تم اكتشاف جريمة أخرى أثناء التفتيش جاز مباشرة التحري والتحقيق بشأنها دون أي مانع قانوني حسبما نصت عليه المادة(44 فقرة 5)[2] من قانون الإجراءات الجزائية الجزائري، وهذا بخلاف ما قضت وتوصلت إليه المحكمة الفيدرالية للولايات المتحدة الأمريكية حيث قضت بأنه إذا قام رجل الضبط بتفتيش الكمبيوتر في خصوص جريمة اتجار بالمخدرات

être préalablement avisé de la perquisition. Il en est de même en cas de perquisition au cabinet ou au domicile du bâtonnier.

[1]– لمزيد من التفاصيل راجع أ.بجيمي جمال، المرجع السابق، ص410.

[2]– تنص المادة 44 فقرة 5من قانون الإجراءات الجزائية على ما يلي:"إذا اكتشفت أثناء هذه العمليات جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة".

وبدلا من ذلك وجد صورا فاضحة للأطفال، فتوقف عن البحث عن الأدلة بخصوص الجريمة الأولى وقام بالبحث عن معلومات بجهاز الكمبيوتر بخصوص الجريمة الثانية، فإنّ ما قام به يجعل الدليل باطلا لأنّه لابد له أن يتوقف عن البحث عن الجريمة الثانية ويعود إلى طلب إذن بالتفتيش خاص بهذه الجريمة على عكس التشريعات ذات الأصل اللاتيني[1].

ب. النتائج القانونية المترتبة على الإذن بتفتيش نظم الحاسب الآلي:

من أهم النتائج المترتبة على الإذن بتفتيش نظم الحاسب الآلي أن يصبح لضابط الشرطة القضائية الصادر له الإذن بالتفتيش نفس السلطات التي تملكها جهة التحقيق الأصلية، كما أنّه يلتزم بنفس الإلتزامات ويخضع لنفس القيود.

وبناءا على ذلك يمكن لضابط الشرطة القضائية اختراق نظم المعالجة الآلية للمعطيات، والبحث عن كل ما يفيد في كشف الحقيقة، فله أن يشاهد مثلا البيانات المخزنة في الحاسب سواء كانت في الذاكرة الرئيسية أو في وحدات التخزين الثانوية وذلك بإحضارها على شاشة العرض، أو استنساخ صورة منها مفهومة ومقروءة، أو ضبطها مع الدعامة المادية التي تحتويها مهما كان شكل هذه الدعامة، أي يستوي أن تكون من قبل الشرائط المغناطيسية أو الأقراص، وبالنسبة لهذه الأخيرة يستوي أن تكون مرنة أو صلبة،وكذلك ضبط أي برامج أو كيانات منطقية، أو كتب تشغيل وإرشادات خاصة بالجهاز، أو أجهزة طباعة المخرجات، أو الأجهزة الطرفية أو المودم بما يكون له اتصال بالجريمة الإلكترونية بل، وحتى ضبط الحاسب الآلي ذاته بكل مكوناته وشبكاته باعتباره دليلا، كذلك يمكن له استخدام إمكانات الحاسب الآلي بما في ذلك كلمات السر ومفتاح الدخول ومفاتيح فك الشفرة[2].

غير أنّ السؤال الذي يمكن طرحه في هذا المقام، ما مدى مشروعيته إجبار المتهم أو غيره على مساعدة سلطة التحقيق في الولوج إلى النظام المعلوماتي؟

-بالنسبة للمتهم:

يتمتع المتهم عبر مراحل الدعوى الجنائية بالحماية المقررة له بموجب مبدأ وجوب افتراض براءته، إلى أن يثبت العكس بالحكم الجنائي البات، و يترتب على ذلك أنه لا يجوز إجباره على تقديم دليل يدين به نفسه، بل له الحق في الصمت، و يجب ألا يفسر صمته بأنه إقرار منه بصحة الإتهام المنسوب إليه، وتجدر الإشارة إلى أن

---

[1] -United States V.Carey, 172 F. 3d1268 (10th Cir. 1999).

نقلا عن :د.عمر محمد بن يونس، الدليل الرقمي، المرجع السابق، ص142.

[2]- د.هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص152.

الحق في الصمت ينص عليه قانون الإجراءات الجزائية الجزائري في المادة 100 منه، والتي تقضي بأنه على قاضي التحقيق أن ينبه المتهم بأنه حر في عدم الإدلاء بأي قرار، و يترتب على ذلك أنه لا يجوز إجبار المتهم على كشف مفاتيح الدخول إلى نظم الوسائل الإلكترونية أو طباعة ملفات بيانات مخزنة داخل هذه النظم[1]، كما لا يجوز إجباره على البوح لسلطات التحقيق بالرقم الكودي السري للمرور إلى ملفات البيانات أو أن يكشف عن كلمة السر وغير ذلك من الأمور التي من شأنها أن تؤدي إلى إدانته[2].

ومن جانبي أميل إلى الرأي الذي يقضي بضرورة الإستعانة بخبراء المعلوماتية من أجل فك الشفرات،وهذا ما أخذ به المشرع الفرنسي[3] ونص على ضرورة تعيين شخص طبيعي ومعنوي يكون مؤهلا للقيام بعملية التشفير إذا كان ذلك ضروريا.

وتجدر الإشارة إلى أنّ هناك طرق علمية لفك رموز الرقم السري إذ أنّ هناك برامج متخصصة في هذا الشأن، كما يمكن من الناحية الفنية فك هذه الشفرات من خلال عدة طرق فنية، وذلك حتى لا يتم إجبار المتهم على تقديم معلومات للولوج إلى النظام المعلوماتي.

-أما بالنسبة لغير المتهم:

إن هؤلاء الأشخاص الذين يتعاملون مع الوسائل الإلكترونية بحكم طبيعة عملهم لا يعتبرون شهودا وفقا لمدلول الشهادة كدليل إثبات في المواد الجنائية، والتي يقصد بها المعلومات الصادرة من شهود يكونوا قد شاهدو بأبصارهم الجريمة لحظة وقوعها أو تجمعت لديهم أدلة تفيد في إثبات وقوعها، أمّا الشاهد في الجرائم الإلكترونية فيقصد به صاحب الخبرة والتخصص في تقنية وعلوم الحاسب والذي تكون لديه معلومات جوهرية لإمكان الدخول إلى نظام المعالجة الآلية للمعطيات[4].

---

[1]- د. علي محمود حمودة، المرجع السابق، ص 49.

[2]- د.فتوح الشاذلي و أ. عفيفي كامل عفيفي، المرجع السابق، ص 365.

[3] - Article 230-1 (C.P.P.F Modifié par Loi n°2004-575 du 21 juin 2004 - art. 38 JORF 22 juin 2004) : Sans préjudice des dispositions des articles 60,77-1 et 156, lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire.

[4]- د. علي محمود حمودة، المرجع السابق، ص 49.

وعليه تفرض بعض التشريعات المقارنة إلتزاما قانونيا بالإفصاح على الشفرات وكلمات السر التي تلزم للدخول إلى نظم الحاسبات الآلية، فالمشرع الفرنسي يلزم الشهود الذين يقع عليهم إلتزام قانوني بأداء الشهادة بالكشف عن المفاتيح وكلمات السر بالنسبة للحاسبات الآلية،[1]، وعليه يمكن إلزام غير المتهم كالشاهد والشخص القائم بتشغيل الحاسب الآلي بتقديم كافة المعلومات والبيانات اللازمة لولوج نظام الحاسب والتعاون مع سلطات التحقيق[2]، وللحديث بقية عند التطرق للشاهد المعلوماتي.

إلاّ أنّه ونظرا للتطورات التكنولوجية الحديثة في مجال المعلوماتية، فقد ظهر نوعا جديدا من الكمبيوترات المحمولة والتي يمكن تشفير الولوج إليها من خلال بصمة الأصابع، أي أنها لا تفتح إلا من خلال بصمة إصبع صاحبها، ولذلك يثور السؤال في هذه الحالة، هل يمكن إجبار صاحبها على أخذ بصمة إصبعه بغية الولوج إلى هذا الكمبيوتر؟

يرى الفقه العراقي أنه بإمكان سلطات التحقيق إرغام المتهم على تقديم بصمة إصبعه لفك التشفير، وهذا في ظل وجود المادة (70)[3] من قانون أصول المحاكمات الجزائية العراقي التي يجيز فيها إرغام المتهم أو المجني عليه في الجناية أو الجنحة على التمكين من أخذ بصمة أصابعه، غير أنّ الإرغام هنا لا يقصد به تقديم بصمة إصبعه من خلال تقييد حركته أو استعمال القوة البدنية، وإنما قصد فقط إمكانية تنبيهه من قبل جهات التحقيق بأنه في حالة عدم امتثاله فإنه سيعرض نفسه للمساءلة الجنائية.

غير أنّ حق الفرد في سلامة جسده وخصوصياته هو حق مضمون بموجب المواثيق الدولية والدساتير والقوانين الوطنية، غير أنّه في حالة امتناع المتهم عن تقديم بصمة أصبعه التي تفتح من خلالها شفرة الكمبيوتر، فيتعين حينها إجبار المتهم على الخضوع قسرا لذلك وهذا قياسا على عمليات التفتيش الجسدي التي تتم جبرا ودون مراعاة رضا الشخص محل التفتيش، وعليه فإنه لا يكفي في هذه الحالة تجريم فعل الرفض أو اعتبار الرفض قرينة على الإذناب الذي يسمح للقاضي بتأسيس حكمه عليها، فالأمر لا يتوقف في هذه لحالة على مجرد استعمال الطرق العلمية أو البرامج المتخصصة، وإنما استعمال وسيلة تعد أكثر أمانا بالنسبة لمجرمي المعلوماتية هي بصمة الأصبع والتي لا يمكن استبدالها بأي حل آخر، سوى إجبار المتهم[4].

---

[1]– د.هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص88. نقلا عن: د. علي محمود حمودة، المرجع السابق، ص 49.

[2]– د.فتوح الشاذلي و أ. عفيفي كامل عفيفي، المرجع السابق، ص 369.

[3]– تنص المادة 70 من قانون أصول المحاكمات الجزائية العراقي على ما يلي: "لقاضي التحقيق أو المحقق أن يرغم المتهم أو المجني عليه في الجناية والجنحة على التمكين من بصمة أصابعه أو غير ذلك مما يفيد في التحقيق".نقلا عن: أ. رشاد خالد عمر، المرجع السابق، ص143.

[4]– أ.رشاد خالد عمر، المرجع السابق، ص144.

2.3- تفتيش نظم الحاسب الآلي بدون إذن قضائي.

الأصل أنه لا يجوز تفتيش الجهاز إلاّ بعد الحصول على إذن قضائي من الجهة المختصة بذلك، ولكن الأصل يرد عليه استثناء وهذا الأمر نجد له تطبيق في القانون الأمريكي والفرنسي لأنه سبق وأوردنا موقف المشرع الجزائري في هذه المسألة، غير أنّه سيتم التركيز على موقف القانون الأمريكي نظرا لما يتضمنه من سوابق في هذا الموضوع.

فتقضي القواعد العامة في التفتيش بأنّه إذا توفرت حالة من الحالات التي يجوز فيها التفتيش بدون إذن فإنّ التفتيش يكون رغم ذلك صحيحا، ومن هذه الإستثناءات في مجال المعلومات ما يلي:

الحالة الأولى:عدم مخالفة التفتيش للتوقع المعقول للحياة الخاصة.

يعتبر التفتيش بدون إذن صحيحا إذا توافر فرض من الفرضين التاليين اللذين قررتهما المحكمة العليا في الولايات المتحدة الأمريكية، وهما:

أ. حالات يتوافر فيها للشخص الحق في التوقع المعقول للحياة الخاصة:

إنّ الفرد إذا كان لديه توقعا معقولا على المعلومات والبيانات المخزنة في الحاسب، فإنّ ذلك يقتضي معاملة الحاسب كالصناديق المغلقة، فالتعديل الرابع للدستور الأمريكي لا يجيز لرجال الضبط القضائي الدخول والإطلاع على المعلومات والبيانات المخزنة في الحاسب بدون إذن، الأمر الذي يطرح تساؤل، هل للفرد توقع معقول للخصوصية على محتويات الحاسب المحمول والأقراص المغنطة التي يحملها؟

لقد أجابت على هذا التساؤل المحاكم الأمريكية وأعملت القياس إذ اعتبرت أجهزة التخزين الإلكترونية بالصناديق المغلقة، ومن تم فإنّ الحصول على المعلومات المخزنة إلكترونيا يتشابه مع فتح الصناديق المغلقة، لأنّ الفرد لديه توقعا معقولا للخصوصية في محتويات الصناديق المغلقة، كما أنّ له ذات الحق بالنسبة للمعلومات والبيانات المخزنة إلكترونيا[1]، وسار القضاء الأمريكي على ذات النهج فيما يتعلق بتوافر التوقع المعقول للحياة الخاصة بالنسبة للملفات المخزنة في الحاسب الشخصي للمتهم[2]،وكذلك البيانات المخزنة في أجهزة الإستدعاء (جهاز النداء الآلي)[3].

---

[1]- United States V.Barth, 26F…Supp-2d 929, 936-37,(W.DTex.1998), available online : www.cybercrime.gov/s&smanual2002.htm.نقلا عن : د. طارق فوزي الفقي، المرجع السابق، ص 123.

[2] -United States department of justice, available online : www.cybercrime.gov/s&smanual2002.htm.

[3]- United States V.Reyes, 922F.Supp.818,832-33, (S.D.N.Y 1996), available online : www.cybercrime.gov/s&smanual2002.htm.

وبالتالي فإنّه لا يجوز الدخول إلى الملفات أو فتح الهواتف المحمولة والحصول على المعلومات المخزنة إلاّ بعد الحصول على إذن من الجهة المختصة[1].

ب. حالات لا يتوافر فيها للشخص الحق في التوقع المعقول للحياة الخاصة:

إذا كان التعديل الرابع للدستور الأمريكي يلزم الحصول على إذن التفتيش إذا كان ذلك يخل بالتوقع المعقول للحياة الخاصة، إلاّ أنّ هذا الإلتزام يتحلل منه رجل الضبط القضائي في إجراء التفتيش ويقع صحيحا دون الحصول على إذن مسبق بذلك، ومن تم يفقد الفرد حقه في الخصوصية إذا كان الحاسب متاحا للجميع، كذلك مشاهدة رجل الضبط كلمة المرور على شاشة لحاسب حال إدخال المتهم لها في الحاسب الخاص به، لأنّ المتهم لا يتوقع أية خصوصية معقولة في العرض الذي يظهر على الشاشة[2]، وأيضا لا يتمتع الأفراد بالتوقع المعقول للخصوصية بالنسبة لمحتويات الحاسب الذي قاموا بسرقته[3].

الحالة الثانية: الرضاء بالتفتيش.

تقضي القواعد العامة بأنّ رجل الضبط القضائي لا يحتاج إلى إذن بالتفتيش إذا كان صاحب المنقول أو العقار محل التفتيش راضيا به، وإذا صدرت الموافقة صحيحة من صاحب الحق، فإنّ هذه الموافقة تحدد النطاق الذي يصح في إطاره التفتيش، فإذا تجاوز هذا النطاق أصبح إجراء غير صحيح[4]، فإذا كان الشخص صاحب الجهاز قد وافق على الإطلاع على الجهاز من الخارج فقط، معنى ذلك لا يجوز لرجل الضبط القضائي تفتيش الجهاز واسترداد الأرقام المسجلة به، لأنّ الموافقة اقتصرت على النظر إلى الجهاز من الخارج لمعرفة نوعه وحجمه دون فتحه، وإن كان هناك أحكاما للقضاء الأمريكي وسعت من تفسيرها للرضا بالتفتيش، فقضى بأنّ الرضا بتفتيش سيارة يتضمن الموافقة على فتح هاتف محمول كان موجودا بالسيارة[5].

---

[1]- United States V.Lynch, 908F.Supp.284,287, (D.V.L 1995), available online : www.cybercrime.gov/s&smanual2002.htm.

[2] -United States V.David, 756F.Supp.1385, (D.Nev. 1991), available online : www.cybercrime.gov/s&smanual2002.htm.

[3] -United States V.Wasler, 275F.3d981k986, (10th cir 2001), available online : www.cybercrime.gov/s&smanual2002.htm. نقلا عن :د.طارق فوزي الفقي، المرجع السابق، ص125.

[4]- ما حدث في الولايات المتحدة الأمريكية من أنّ متهما في جريمة إعتداء جنسي على جارة من جيرانه، فوافق على تفتيش منزله، ولما دخل رجل الشرطة إلى منزله قام بفتح جهاز الكمبيوتر الخاص بالمتهم، وعثر على صور جنسية خاصة بالأطفال، ولما قدمت كدليل على هذا الإتهام استبعدتها المحكمة، وذلك لبطلان الدليل نتيجة لتجاوزه نطاق الرضا المصرح به للتفتيش. أنظر في ذلك: د.شيماء عبد الغني، المرجع السابق، ص318.

[5]- United States V.Galante, 1995WL, 507249, at 3 (S.D.N.Y aug, 25, 1995), available online : www.cybercrime.gov/s&smanual2002.htm.

لذلك قضي في الولايات المتحدة بأنّ المستخدم لدى شركة معينة والذي يرسل معلومات خاصة بتلك الشركة إلى شركة منافسة يفقد حقه في حرمة الحياة الخاصة فيما يتعلق بتلك المعلومات متى وصلت إلى جهاز تلك الشركة الأخيرة[1].

أ- الرضاء الصادر من الزوجة أو الشركاء المنزليين:

إنّ القضاء الأمريكي يعتدّ بالرضا الصادر من أحد المستعملين لجهاز الكمبيوتر عند تعددهم، فالعبرة لديه هي بالإعتياد على الإستعمال وليس بملكية الجهاز، وتطبيقا لذلك قضي بأنّ الصديقة من حقها أن ترضى بتفتيش جهاز الكمبيوتر المتواجد في منزل مشترك مع صديقها على اعتبار أنّ الصديق لم يكن قد وضع كلمة المرور ليخص به ملفاته الشخصية، فكأنه رضي ضمنيا بالإستعمال المشترك مع صديقته لما يتواجد في داخل الجهاز من ملفات، لأنّعدم وجود "كلمة مرور" التي تحمي بعض الملفات تشير إلى رغبة صاحب تلك الملفات بأن يشاركه غيره في استعمال الجهاز[2].

ب- الرضاء الصادر من الوالدين:

بالنسبة للرضا الصادر عن الوالدين بخصوص أجهزة الكمبيوتر التي يستعملها أولادهم، تبنى القضاء الأمريكي تفرقة بين ما إذا كان الأولاد يقل عمرهم عن 18 سنة أو أنه يزيد على ذلك.

فقضت المحاكم الأمريكية بالإعتداد بالرضاء الصادر من الوالدين بالنسبة لتفتيش الكمبيوتر الخاص بابنه القاصر والمتواجد في غرفته[3]، أمّا بالنسبة للإبن البالغ فإنّ المحاكم تعتد برضاء والديهم ما دام الأبناء يعيشون مع والديهم، ويختلف الأمر عندما ينكر الأبناء على والديهم حقهم في دخول حجراتهم الخاصة، في هذه الحالة لا تحق للآباء أن يرضوا بالتفتيش[4].

---

[1]- United States V.Horowitz, 806F. 2d1222 (4th Cir. 1986), available online : www.cybercrime.gov/s&smanual2002.htm.

نقلا عن : د. شيماء عبد الغني، المرجع السابق، ص 320.

[2]- United States V.Smith, 27F. supp 2d1111, 1115-16 (C.D.III. 1998), 29.12.2003, available online : www.lex-electronica.org/articles/v6-2/pepin.htm.

نقلا عن : د. طارق فوزي الفقي، المرجع السابق، ص 130.

[3]- United States V.Lavin, 1992 WL 373486, at 6 (S.D.N.Y, Nov.30.1992), available online : www.cybercrime.gov/s&smanual2002.htm.

نقلا عن :د.شيماء عبد الغني، المرجع السابق، ص328.

[4]- United States V.Rith, 164F. 3d1323,1331 (10th Cir. 1999), available online : www.cybercrime.gov/s&smanual2002.htm.

ج- الرضاء الصادر من مديري النظام:

إنّ شبكة الحاسب تدار بمعرفة ما يسمى بمدير النظام، وهو المنوط به تأمين الشبكة وإصلاحها في حال ظهور أي مشكلات بها، وقد اشترط القضاء الأمريكي أنّ الحصول على موافقة مدير النظام لتفتيش أي حاسب يجب أن يكون متوافقا مع قانون خصوصية الإتصالات الإلكترونية[1]، والذي وضع القواعد المنظمة لحصول السلطات على موافقة مدير النظام بتفتيش حاسب أحد الأفراد.

د- الرضا الضمني بالتفتيش:

ومن صور الرضا الضمني ما يتم تدوينه في تنبيهات تظهر على شاشة الكمبيوتر عند استخدام شبكة الإنترنت، بأنّ المراسلات يمكن أن تخضع للمراقبة، في هذه الحالة يعتبر استمرار مستخدم الكمبيوتر في استعماله دالا على توافر الرضا المفترض من جانبه، وتصح المراقبة عندئذ، وقد طبق القضاء الأمريكي تلك الفكرة في مجال مراقبة هواتف السجن في أثناء محادثات السجناء مع خارج السجن، فقضي بأنّ وضع إدارة السجن لافتة بأنّ المكالمات الهاتفية من أجهزة السجن يمكن أن تخضع للمراقبة، يصح الإستناد إليه كدليل على توافر الرضا الضمني بذلك من جانب مستخدم هذا الهاتف[2].

الحالة الثالثة: تفتيش مقر العمل.

اتجهت أحكام القضاء في بعض التشريعات كالقانون الأمريكي إلى التفرقة إذا ما كان مكان العمل من أماكن العمل الخاصة أو العامة.

أ- تفتيش مقر العمل الخاص:

الأصل أنّ العاملين في القطاع الخاص يتمتعون بالحق في الخصوصية بالنسبة لأماكن عملهم، وبناءا عليه يلزم الحصول على إذن لتفتيش تلك الأماكن إلاّ إذا تم هذا التفتيش برضا من رب العمل أو من مستخدم له سلطة على تلك الأماكن،لذا قضي ببطلان تفتيش ملفات أحد العاملين في تلك الجهات دون إذن بذلك[3].

---

[1]- The electronic communication privacy act (E.C.P.A), 18V.S.C.

نقلا عن : د. طارق فوزي الفقي، المرجع السابق، ص132.

[2]- د.غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر والقانون، المنصورة، مصر، بدون طبعة، سنة 2013، ص198.

[3]- Mancusie V.Deforte, 392J.S.364 (1968),available online : www.cybercrime.gov/s&smanual2002.htm.

نقلا عن: د. شيماء عبد الغني، المرجع السابق، ص 342.

ب– تفتيش أماكن العمل العامة:

تتجه أحكام القضاء في التشريعات المقارنة وخاصة أحكام القضاء الأمريكي بأنّ الأصل أن موظف الحكومة يتمتع بتوقع معقول للخصوصية في مقر عمله، في حين أن هذا التوقع يزول إذا كانت هناك ممارسات فعلية وإجراءات أو لوائح تسمح للمشرف على الموظف والموظفين المساعدين بالدخول إلى مكان عمل الموظف، كما أنّ للرئيس الإداري الرضاء بالتفتيش[1].

هذا إضافة إلى التفتيش بناءا على حالة التلبس، والتفتيش بناءا على القبض على الأشخاص وقد تم الإشارة لهاتين الحالتين فيما سبق وتم شرحها بالتفصيل.

ثانيا: الشروط الشكلية لتفتيش نظم الحاسب الآلي.

بالإضافة إلى الضمانات الموضوعية لتفتيش نظم الحاسب الآلي، والتي سبق التفصيل فيها، توجد ضمانات أخرى ذات طابع شكلي يجب مراعاتها عند ممارسة هذا الإجراء صونا للحريات الفردية من التعسف أو الإنحراف في استخدام السلطة.

والشروط الشكلية لتفتيش نظم الحاسب الآلي منها ما يعتبر عنصرا من عناصر العمل الإجرائي كالحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش وتحرير محضر التفتيش وأسلوب تنفيذه، ومنها ما يعتبر ظرفا له كالوقت الزمني لإجراء التفتيش، وذلك على النحو التالي:

1- الحضور الضروري لبعض الأشخاص أثناء إجراء تفتيش نظم الحاسب الآلي:

من أهم الضمانات الشكلية ما يتطلبه القانون في الجرائم التقليدية من حضور شخص أو أشخاص أثناء التفتيش، والهدف من ذلك ضمان الإطمئنان إلى سلامة الإجراء وصحة الضبط، وبالرجوع إلى التشريعات الإجرائية المختلفة نجد أن غالبيتها لا يسوي بين تفتيش الشخص وتفتيش المساكن وما في حكمها فيما يتعلق باستلزام هذا الإجراء، ومن هذه التشريعات التشريع المصري الذي وإن كان قد عني بمسألة حضور المتهم أو من ينيبه أثناء تفتيش المنزل، فإنّه لم يشترط لصحة تفتيش الأشخاص حضور شهود، وبالنسبة للمساكن وما في حكمها فالمشرع المصري غيّر في الضمانات المقررة وفقا لشخص القائم به، حيث اشترط

---

[1]– طبق هذا المبدأ في واقعة تتلخص وقائعها في أنّ المتخصصون في الحاسب التابع لوكالة الإستخبارات المركزية علموا أنّ أحد موظفي الوكالة يستخدم حاسب العمل للحصول على صور دعارة، فتم الدخول عن بعد إلى الحاسب فتم العثور على العديد من الملفات التي تحتوي على صور دعارة خزنها على القرص الصلب، فدفع ببطلان الدليل الذي أسفر عنه التفتيش عن بعد للقرص الصلب، فقضت المحكمة أنّ سياسة الاستخدام الرسمي للإنترنت تزيل أي توقع للخصوصية بالنسبة للملفات المنسوخة، لأنّ لوائح العمل بالوكالة تقرر أنّ المتخصصين يمكنهم القيام بفحص دوري ومراقبة كل استخدام للإنترنت يقوم به المستخدمين في الوقت الذي يرونه مناسبا لذلك. أنظر في ذلك: د.طارق فوزي الفقي، المرجع السابق، ص143.

حضور شاهدين في حالة ما إذا كان التفتيش يباشر من قِبل رجل الضبط القضائي، وعلى أن يكون هذان الشاهدان بقدر الإمكان من أقارب المتهم البالغين أو من القاطنين معه في المنزل أو من الجيران وهذا حسب المادة (51) من قانون الإجراءات الجنائية المصرية[1].

وعلى العكس من ذلك، ينص القانون الفرنسي والجزائري على واجب حضور شاهدين في كلا الحالتين سواء كان القائم بالتفتيش قاضي التحقيق أو ضابط الشرطة القضائية، ويعد حضور شاهدين إحدى الأشخاص الواجب حضورهم أثناء إجراء تفتيش مسكن المتهم، لأنّه يجب أن يحصل التفتيش بحضور المتهم أو ممثل عنه يقوم هو بتعيينه وإلاّ بحضور شاهدين من غير الموظفين التابعين لسلطة القضاء أو الشرطة[2]، وكما تبين فإنه لا مانع أن يكونا من المقيمين بالمكان أو أقارب المعني أو جيرانه قياسا على ما نصت عليه التشريعات العربية بشرط أن يكونا بالغين[3].

إلاّ أنّ المشرع الجزائري ومن خلال التعديل الذي أجراه على قانون الإجراءات الجزائية بموجب القانون رقم (06-22) في المادة (45 فقرة 7)[4] استثنى مجموعة من الجرائم الخطيرة ومن ضمنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات من الخضوع لقاعدة الحضور هذه، وهذا راجع للطبيعة الخاصة للدليل الإلكتروني من حيث سرعة إتلافه ومحوه.

2- الفترة الزمنية لإجراء تفتيش نظم الحاسب الآلي:

تحرص بعض التشريعات على حضر القيام بتفتيش المساكن وما في حكمها في وقت معين، وذلك حرصا منها على تضييق نطاق الإعتداء على الحرية الفردية وحرمة المساكن، في حين لم تحدد بعض التشريعات وقتا معينا يتم فيه إجراء التفتيش، وإنّما ترك للقائم بالتفتيش تحديد الوقت المناسب للقيام به دون النظر إلى أي

---

[1]- نقلا عن: د.هلالي عبد اللاه أحمد. تفتيش نظم الحاسب الآلي، المرجع السابق، ص164.

[2]- تنص المادة 45 فقرة 1 من قانون الإجراءات الجزائية الجزائري على ما يلي : " ...إذا وقع التفتيش في مسكن شخص يشتبه في أنه ساهم في ارتكاب الجناية فإنه يجب أن يحصل التفتيش بحضوره، إذا تعذر عليه الحضور وقت إجراء التفتيش فعن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له. وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته...".

[3]-أ. نجيمي جمال، المرجع السابق، ص408.

[4]- تنص المادة 45 فقرة 6 من قانون الإجراءات الجزائية الجزائري على ما يلي : " ... لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف، باستثناء الأحكام المتعلقة بالحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات المذكورة أعلاه".

اعتبار آخر يتعلق بالمحل المراد تفتيشه[1]، وهذا هو حال القانون المصري الذي يجيز التفتيش في كل أوقات الليل والنهار، وقد تواترت أحكام محكمة النقض المصرية على هذا المعنى[2].

غير أن القانونين الجزائري والفرنسي يحظران تفتيش المنازل وما في حكمها في وقت معين، وهو محدد في القانون الجزائري من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا إلاّ إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا، وهذا طبقا لنص المادة (43) من قانون الإجراءات الجزائية الجزائرية، ففي هذه الحالات لا يكون هناك مجال للحديث عن وقت التفتيش الذي يتطلبه القانون وتكون تصرفات ضابط الشرطة القضائية الذي يدخل المحل في غير الأوقات المحددة سليمة من الناحية القانونية وتنتج آثارها.

فهذا القيد لا يطبق في حالة التحري حول الجرائم المنصوص عليها بالمواد (342 إلى 348) من قانون العقوبات وتشمل جرائم ضد الأخلاق (تحريض القصر على الفسق، حماية الدعارة والعيش من متحصلاتها، فتح محل الدعارة، الإغراء العلني على الفسق).

وكذلك لا يطبق هذا القيد على فئة الجرائم الخمسة المذكورة في المادة (47فقرة 3)[3]من قانون الإجراءات الجزائية الجزائري وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الإلكترونية، جرائم تبييض الأموال والإرهاب وجرائم الصرف، حيث أنّ التفتيش يكون في كل مكان ودون التقيد بزمان.

أمّا في القانون الفرنسي فنجد وقت التفتيش محددا من الساعة السادسة صباحا إلى الساعة التاسعة مساءا وذلك من خلال المادة (59)[4] من قانون الإجراءات الجزائية الفرنسي، فوفقا لهذا النص فإن تفتيش

---

[1]– د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 175.

[2]– قضت بأنه: من المقرر قانونا أنّ لمأموري الضبط القضائي إذا ما صدر إليهم إذن من النيابة بإجراء التفتيش أن يتخذوا ما يرونه كفيلا بتحقيق الغرض من دون أن يلتزموا في ذلك طريقة بعينها، ما داموا لا يخرجون في إجراءاتهم على القانون، ويكون لهم تخير الظرف المناسب لإجرائه بطريقة مثمرة وفي الوقت الذي يرونه ملائما مادام ذلك يتم خلال الفترة المحددة في الإذن. أنظر في ذلك د.سامح بلتاجي موسى، المرجع السابق، ص 272.

[3]– تنص المادة 47 فقرة 3 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري) على ما يلي : " ... عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف، فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص".

[4]-Article 59 (C.P.P.F Modifié par Loi 93-1013 1993-08-24 art. 20 JORF 25 août 1993 en vigueur le 2 septembre 1993): Sauf réclamation faite de l'intérieur de la maison ou exceptions prévues par la loi, les perquisitions et les visites domiciliaires ne peuvent être commencées avant 6 heures et après 21 heures.
Les formalités mentionnées aux articles 56, 56-1, 57 et au présent article sont prescrites à peine de nullité.

المساكن أو الدخول إليها فيما عدا حالة المطالبة من الداخل (كما في حالة الإستغاثة أو الحريق أو الغرق) أو في الأحوال المنصوص عليها قانونا[1].

وبتطبيق ما تقدم على الجرائم الإلكترونية، فلا توجد نصوص تشريعية في بعض القوانين تحدد وقتا معينا تتم فيه إجراء تفتيش الحواسب المتصلة بالإنترنت والتي تمت عن طريقها تلك الجريمة الكائنة في المنازل وما في حكمها، وبالتالي يسري عليها القواعد العامة التي تحدد الوقت الزمني لإجراء التفتيش في الجرائم التقليدية.

كما قد يكون في تحديد الوقت عائقا كبيرا أمام إجراء التفتيش في الجريمة الإلكترونية، كون هذه الأخيرة يمكن اقترافها في أي وقت، بحيث أنه يمكن ارتكابها من قبل مجرم معلوماتي متواجد في دولة يكون الوقت فيها منتصف الليل على ضحية معلوماتية متواجدة في دولة أخرى يكون الوقت فيها منتصف النهار، فمثل هذا الإختلاف في التوقيت الدولي قد يؤدي في الكثير من الأحيان إلى جعل الجريمة الإلكترونية الواقعة في بلد أو التي بدأت في الوقوع في بلد من هذه الدول خارجة عن الساعات المسموح بالتفتيش فيها قانونا في دولة أخرى.

كما نؤيد موقف المشرع الجزائري كونه أقرب إلى المنطق والصواب باعتباره سلك طريقا وسطا بغية إيجاد نوع من التوازن، حيث استثنى الجرائم الإلكترونية من خطر التفتيش ليلا خاصة وأنّ الأدلة التي تتخلف عنها تكون معرضة لخطر الإتلاف أو المحو أو التعديل، ولذلك يكون من الضروري إجراء التفتيش فيها على وجه السرعة من أجل منع المجرم المعلوماتي من الإفلات من العقاب[2].

3- أسلوب تنفيذ التفتيش في نظم الحاسب الآلي:

قررت محكمة النقض المصرية بأنّ طريقة تنفيذ إذن التفتيش موكولة إلى رجل الضبط المأذون له أن يجريها تحت إشراف سلطة التحقيق ورقابة محكمة الموضوع، فله أن يتخذ من وسائل التحوّط ما يمكنه من تحقيق الغرض من التفتيش المأذون له به، وأن يستعين في ذلك بأعوانه من رجال الضبط القضائي أو بغيرهم من رجال السلطة العامة حيث يكونوا على مرأى منه وتحت بصره[3].

---

[1]- أ. نجيمي جمال، المرجع السابق ، ص 414. وكذلك:
Bernard Bouloc . Gaston stéfani et Georges Levasseur, procédure pénale, Dalloz, Paris, France, 2001, p 370.

[2]- أ.رشاد خالد عمر، المرجع السابق، ص 132.

[3]- نقض 23 يناير 1978م، مجموعة أحكام النقض، س29ق، ص83، نقلا عن"د.سامح أحمد بلتاجي موسى، المرجع السابق، ص270.

كما قضت تلك المحكمة أيضا بأنه:"من المقرر أنّ لمأموري الضبط القضائي إذا ما صدر إليهم إذن من النيابة العامة بإجراء تفتيش، أن يتخذوا ما يرونه كفيلا بتحقيق الغرض منه دون أن يلتزموا في ذلك طريقة بعينها ماداموا لا يخرجون في إجراءاتهم على القانون، ويكون لهم تخير الوقت المناسب لإجرائه بطريقة متميزة وفي الوقت الذي يرونه ملائما مادام أنّ ذلك يتم في خلال الفترة المحددة بالإذن"[1].

وفقا لما جاء في المرشد الأمريكي لتفتيش وضبط جهاز الحاسب الآلي، فإنّه يمكن لرجال الضبط القضائي والمدعين العموميين تفتيش وضبط الحاسبات الآلية بإتباع الخطوات التالية:

أ- تجميع فريق عمل يتكون من رجل الضبط القضائي المكلف بالمهمة والمدعي العام وخبير فني قبل القيام بالتفتيش.

ب- التعرف قدر الإمكان على نظم الحاسب المراد تفتيشها قبل وضح خطة التفتيش أو طلب الإذن، فيمكن لرجال الضبط القضائي حيال ذلك اتباع مناهج مختلفة للحصول على هذه المعلومات منها على سبيل المثال، مقابلة مدير النظام والتي تتم في الغالب بشكل سري من أجل الحصول على جميع المعلومات التي يحتاجها المتخصص الفني ليخطط وينفذ التفتيش، كما يمكن زيارة الموقع الموجود فيها الجهاز والتي تتم أحيانا بشكل سري لكشف بعض عناصر القطع الصلبة، كذلك من الممكن الإستعانة بشبكة الإنترنت التي تعد في ذاتها مصدرا مفيدا للمعلومات.

ج- وضع خطة لتنفيذ التفتيش مع خطة بديلة تكون مبنية على المعلومات التي عرفت عن النظام المراد تفتيشه، ومن بين الموضوعات التي يجب التفكير فيها عند وضع خطط التفتيش ما يلي:

- مدى حاجة الخطة التي يتم وضعها إلى تعديل أو تقليل إمكانية انتهاك قانون حماية الخصوصية أو قانون حماية الإتصالات الإلكترونية.
- مدى حاجة خطة التفتيش لأكثر من إذن.
- مدى حاجة رجال الضبط القضائي إلى استصدار إذن خاص للقيام بتفتيش مفاجئ.
- يجب إعطاء مسودة إذن التفتيش عناية خاصة من حيث اشتمالها على وصف لمحل التفتيش والملكية المراد ضبطها بدقة وواقعية مع شرح لاستراتيجية التفتيش الممكنة[2].

---

[1]- نقض 29 أفريل 1979م، مجموعة أحكام النقض، س20ق، ص511. نقلا عن: د. سامح بلتاجي موسى، المرجع السابق، ص271.

[2]- د.سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، مصر، ط 1، سنة 1999، ص145.

وتفتيش نظم الحاسب الآلي يمكن أن يتم بطرق عدة، فمثلا المرشد الفيدرالي الأمريكي جاء بأربعة طرق أساسية للتفتيش هي:

أ– تفتيش الحاسب الآلي وطبع نسخة ورقية من ملفات معينة في ذات الوقت.

ب– تفتيش الحاسب الآلي وعمل نسخة إلكترونية من ملفات معينة في ذات الوقت.

ج– عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع، وبعد ذلك يتم إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة.

د–ضبط الجهاز وإزالة ملحقاته ومراجعة محتوياته خارج الموقع.

ما يتم استخلاصه هو أنّ أي من هذه الطرق أو الأساليب تعد هي الأفضل اعتمادا على عدة عوامل متعددة لأي تفتيش، مع مراعاة الأخذ بالإعتبار دور القطع الصلبة الخاصة بالحاسوب في ارتكاب الجرائم، لذلك فإن نجاح التفتيش غالبا ما يعتمد على دور تلك القطع[1].

4- محضر تفتيش نظم الحاسب الآلي:

باعتبار أنّ التفتيش عمل من أعمال التحقيق فينبغي تحرير محضر يثبت فيه ما تم من إجراءات وما أسفر عنه من أدلة، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما والتي تقضي بأن يكون مكتوبا باللغة الرسمية، وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها[2].

أمّا بالنسبة لمحضر تفتيش نظم الحاسب الآلي، فإنه يلتزم بالإضافة إلى الشكليات السابقة ضرورة إحاطة قاضي التحقيق أو عضو النيابة بتقنية المعلومات، ثم ينبغي بعد ذلك أن يكون هناك شخص متخصص في الحاسب الآلي يرافقه للإستعانة به في مجال الخبرة الفنية الضرورية، فلا شك أنّ وجود خبير معالجة بيانات سوف يساعد في صياغة مسودة محضر التفتيش، بحيث يتم تغطية كل الجوانب الفنية في عملية التفتيش والضبط التي تتم، بالإضافة إلى المحافظة على الأدلة المتحصل عليها من كل تلف أو مسح[3].

---

[1]– د.حسين الغافري، المرجع السابق، ص 170.

[2]–أ. عائشة بن قارة ، المرجع السايق، ص 113.

[3]– د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي ، المرجع السابق، ص170.

المطلب الثالث: الضبط.

إنّ الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، وعلى ذلك فإن ضبط الأشياء المتعلقة بالجريمة هي الأثر المباشر للتفتيش، ولذلك فإن غالبية التشريعات تجمع بين أحكام الضبط والتفتيش في موضوع واحد، لكن ليس معنى ذلك أن الضبط لا يقع إلا نتيجة للتفتيش، إذ من الممكن أن يكون الضبط نتيجة لمعاينة[1].

والضبط في نطاق قانون الإجراءات الجزائية يقصد به:الحصول على أشياء ذات صلة بجريمة وقعت ويفيد في كشف حقيقتها وحقيقة نسبتها إلى المتهمين، غير أنّ الضبط في الجريمة الإلكترونية يختلف عن الضبط في غير ذلك من الجرائم من حيث المحل، وذلك بسبب أنّ الأول يرد على أشياء ذات طبيعة معنوية وهي البيانات، المراسلات والإتصالات الإلكترونية، أمّا الثاني فيرد على أشياء مادية منقولة كانت أم عقارات، وقد أثارت هذه الطبيعة المعنوية للبيانات جدلا فقهيا واختلافا تشريعيا حول مدى إمكانية ضبطها خاصة إذا كانت مجردة من الدعامة المادية المثبتة عليها، ويرجع السبب في ذلك أن الضبط حسب الأصل لا يرد إلا على الأشياء المادية[2].

ومن أجل التوضيح أكثر سيتم التطرق لضبط المكونات المادية والمعنوية للحاسوب، وفيما يلي تفصيل ذلك:

الفرع الأول: ضبط المكونات المادية للحاسب الآلي.

لا يثير ضبط المكونات المادية للحاسب الآلي أية مشاكل، حيث أنّه يوجد إجماع فقهي على صلاحية تلك المكونات لأن تكون محلا للضبط في حالة ما إذا كانت وسيلة في ارتكاب إحدى الجرائم أو متحصلة منها أو كانت دليلا يفيد في كشف الحقيقة عنها وعن مرتكبيها.

فيمكن ضبط الوحدات المعلوماتية الآتية: وحدة المدخلات بما تشمله من مفردات كلوحة المفاتيح، نظام الفأرة، نظام القلم الضوئي، وضبط وحدات المخرجات وما تشمل عليه من وسائل كالشاشة، الطابعة والمصغرات الفيلمية، أيضا وحدات التخزين كالأقراص الصلبة والمرنة وأقراص الليزر[3].

---

[1]– د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي ، المرجع السابق، ص193.

[2]– أ.عائشة بن قارة، المرجع السابق، ص144.

[3]– د.سامح أحمد بلتاجي موسى، المرجع السابق، ص 275.

الفرع الثاني: ضبط المكونات المعنوية للحاسب الآلي.

إن كان هناك إجماع بشأن ضبط المكونات المادية للحاسب، إلاّ أنّ الفقه اختلف حول مدى صلاحية مكونات الحاسوب المعنوية للضبط ليخلص إلى القول أنّه إذا كانت الغاية دائما هي ضبط ما يفيد في كشف الحقيقة فإنّ ذلك ينسحب إلى البيانات والمعلومات الإلكترونية مادامت تشكل موضوع الجريمة الواقعة أو تشكل الأداة التي استخدمت في ارتكابها أو كانت تلك البيانات والمعلومات من متحصلات هذه الجريمة.

كما أكدت المادة (19) من القسم الرابع للإتفاقية الأوروبية بشأن الجرائم الإلكترونية لعام 2001 على جواز ضبط المعلومات المخزنة بالحاسوب أو على أي وسيط تخزين، حيث يكون لكل دولة طرف السلطة أن تتخذ الإجراءات التالية: أن تضبط نظام الحاسوب أو أي جزء منه أو المعلومات المخزنة به وعلى أي وسيط من وسائط التخزين المتعلقة بالحاسوب وأن تحافظ على سلامة هذه المعلومات المخزنة.

وفي إطار الإتفاقية الأوروبية بشأن الجرائم الإلكترونية، فإنّ مصطلح الضبط يشمل الدعامة المادية التي يتم تخزين المعلومات والبيانات عليها أو الوصول أو التحفظ على نسخة منها، ويشمل أيضا استخدام أو ضبط البرامج الفورية اللازمة للولوج إلى هذه البيانات وضبطها، ومن تم فقد استخدم مصطلح الحصول بطريقة مشابهة وذلك بقصد الأخذ في الإعتبار الطرق غير التقليدية لرفع بيانات غير مادية التي لا يسهل الحصول عليها، وأنّ ذلك لا يتم بطريقة مادية في نطاق بيئة المعلومات[1].

وقد تم التطرق سابقا لجميع الإتجاهات المتعلقة بمدى إمكانية خضوع مكونات الحاسب الآلي المعنوية للتفتيش، وانتهى الأمر إلى ضرورة أن يشمل التفتيش المكونات المعنوية، ويرى الفقه بأنه مادام يجوز تفتيشها فيترتب على ذلك إباحة ضبطها، وإن كان هذا الأمر في اعتقادهم يثير العديد من المشاكل القانونية في ظل غياب نصوص خاصة بذلك في بعض التشريعات خاصة منها العربية على سبيل المثال القانون المصري، وهذا بخلاف التشريع الفرنسي حيث تم إدخال تعديلات على قانون الإجراءات الجزائية الفرنسي لسد هذا الفراغ التشريعي، وذلك بموجب المادة (57-3/1)[2].

---

[1]– د. سامح بلتاجي موسى، المرجع السابق، ص 277.

[2]-Article 57 – 1/3 (C.P.P.F Modifié par LOI n°2009-928 du 29 juillet 2009 - art. 11) dispose que : « les données aux quelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code ».

أمّا المشرع الجزائري، فمن خلال القانون الذي استحدثه للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السابق ذكره قانون رقم (09-04) أجاز حجز المعطيات المعلوماتية حيث نص أنه عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها فيجوز في هذه الحالة أن يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز طبقا للقواعد المقررة في قانون الإجراءات الجزائية، كما أنّه يجب في جميع الأحوال السهر على سلامة هذه المعطيات وعدم المساس بمحتواها[1].

وأضاف المشرع الجزائري أنه في حالة ما إذا كانت عملية الحجز مستحيلة لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش إستعمال التقنيات لمنع الوصول إلى المعطيات الموجودة لدى المنظومة المعلوماتية أو القيام بنسخها[2]، كما يمكن لهذه السلطة أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ويكون ذلك عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك[3].

وعليه ليس هناك من الناحية القانونية ما يمنع من القول بإمكانية خضوع المكونات المعنوية للحاسب للضبط، وكل ما في الأمر أنّ ضبطها وإحرازها يتمان بطرق فنية تقنية تختلف عن الطرق التقليدية المتبعة لضبط وإحراز الأدلة المادية، إلاّ أنّه قد يثور إشكال فيما يتعلق بمحل الضبط ونطاقه،وستعالج هاتين المسألتين على النحو التالي:

أولا: محل الضبط.

مثلما ذكر سابقا، أنّ الضبط يرد على جميع الأشياء التي تفيد في كشف الحقيقة، أمّا الأشياء التي لا تفيد في كشف الحقيقة فلا يصح ضبطها، ولكن هذا الأمر مثير للإشكالية في مجال الضبط الإلكتروني، ذلك أنّه في بعض الأحيان قد لا يكون بالإمكان فصل البيانات أو العناصر التي تفيد في كشف الحقيقة عن النظام

---

[1] – تنص المادة 06 من القانون رقم 09-04 السالف الذكر على ما يلي: " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية ...".

[2]– تنص المادة 7 من القانون رقم 09-04السالف الذكر على ما يلي: " إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 06 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة".

[3]– تنص المادة 8 من القانون رقم 09-04السالف الذكر على ما يلي : " يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك".

أو الشبكة التي تحويها، بالرغم من أهمية ضبطها لإثبات الجريمة الإلكترونية الواقعة، مما يجبر معه سلطات التحقيق على ضبط النظام أو الشبكة المعلوماتية بأكملها، وهذا بدوره يؤدي إلى عزل النظام أو الشبكة بالكامل عن محيطه المعلوماتي، ولفترة غير محددة قد تطول أو تقصر حسب كل حالة، ويترتب على ذلك تعطيل عملها وعمل الجهة التي تديرها وإلى إلحاق أضرار مادية فادحة بها مع أنها قد لا تكون بالضرورة هي المتهمة بالجريمة الواقعة.

ولذلك وبغية معالجة هذه الإشكالية وإيجاد نوع من التوازن ما بين حق الدولة وضحايا الجريمة في الوصول إلى الجناة ومعاقبتهم، وبين حق الجهة صاحبة النظام أو الشبكة في عدم تعطيل عملها، فقد لجأ القضاء في معظم الدول الأوروبية إلى تطبيق معيار أو مبدأ "التناسب" الذي يقضي بضرورة اقتصار الضبط المعلوماتي فقط على تلك البيانات والأنظمة التي تفيد في كشف الحقيقة، وبما يحفظ النظام أو الشبكة المعلوماتية من التعطيل الكامل[1].

ثانيا: كيفية إحراز المضبوطات الإلكترونية.

إنّ إحراز المضبوطات المادية كأجهزة الكمبيوتر وملحقاتها من طابعات وماسحات ضوئية وغيرها لا يثير أي إشكال، حيث تنطبق عليه جميع القواعد التقليدية المنصوص عليها في القانون،ولكن المشكلة تثور عندما يتعلق الأمر بالمضبوطات الإلكترونية الموجودة على شبكة الإنترنت أوفي داخل كمبيوتر يتم تفتيشه عن بعد، ففي هذه الحالة يكون بالإمكان إحراز هذه المضبوطات وفق القواعد التقليدية للضبط والإحراز، بل يلزم لإحرازها اللجوء إلى طرق ووسائل تقنية وفنية تتفق مع الطبيعة الإلكترونية لهذه البيانات وبعدها الجغرافي عن متناول أيدي أجهزة الضبط، ومن بين هذه الطرق على سبيل المثال لا الحصر ما يلي[2]:

1- طريقة النسخ (Copy):

وتتم من خلال نسخ المضبوطات الإلكترونية باستخدام برامج معدة خصيصا لهذا الغرض، مثلا (Laplink)، حيث أنه يتم أخذ نسخة من تلك البيانات أو المضبوطات الإلكترونية، ومن تم يتم لصقها

---

[1]- أ. رشاد خالد عمر، المرجع السابق، ص 149.

[2]-أنظر في ذلك: أ. عائشة بن قارة ، المرجع السابق، ص 116 وكذلك: أ. رشاد خالد عمر، المرجع السابق، ص 150.

وتخزينها باسم معين على إحدى وسائط النقل (CD,DVD) الخاصة بالجهة القائمة بالضبط، على أن يتم حفظ نسخة أخرى من تلك المضبوطات كي تكون بديلا للأولى في حالة تلفها أو ضياعها.

2- طريقة التجميد:

وتتم من خلال تجميد التعامل بالكمبيوتر أو النظام المعلوماتي الذي تتواجد بداخله المضبوطات الإلكترونية، وذلك من خلال برامج معدة خصيصا لهذا الغرض، ومن تم يتم ضغط الملفات أو المضبوطات الإلكترونية من خلال برامج الضغط، حيث تقوم هذه الأخيرة بتقليص حجم تلك الملفات والمضبوطات وتضغطها بداخل ملف أو عدة ملفات صغيرة الحجم، ومن دون أن يؤثر ذلك في سلامة تلك الملفات، بحيث تبقى محتفظة بكامل خواصها الأصلية ليتم حفظها على أقراص الليزر لكي يتم فتحها على أي كمبيوتر من خلال برامج خاصة، ويجب اتباع ما يلي:

1- ضبط الدعائم الأصلية للبيانات وعدم الإقتصار على ضبط نسخها.

2- عدم ثني القرص لأنّ ذلك قد يؤدي إلى تلفه وفقدان البيانات المسجلة عليه.

3- عدم تعريض الأقراص والأشرطة الممغنطة لدرجات الحرارة العالية ولا إلى الرطوبة، مع الإشارة إلى أنّ درجة الحرارة المسموح بها تتراوح بين (4-32) درجة مئوية، أما نسبة الرطوبة المسموح بها تتراوح بين 20% إلى 80%، وبذلك يمكن أن تصل مدة تخزين هذه الأقراص والأشرطة إلى ثلاثة سنوات.

4- عدم الضغط عليه بوضع أشياء ثقيلة وعدم كتابة بيانات اللاصقة الورقية المخصصة للمستخدم بعد لصقها على القرص، لأن الضغط بالقلم قد يفسد سطح القرص.

5- عدم تعريض الأقراص للمجالات المغناطيسية بعد وضعها على الأجهزة حتى لا يفقد ما عليها،لأن التسجيل على الأسطوانة أو القرص يتم مغناطيسيا.

6- منع الوصول إلى البيانات التي تم ضبطها أو رفعها من النظام المعلوماتي، وقد نص على هذا الإجراء المادة (19)[1] من اتفاقية بودابست، ويتم اللجوء إلى هذا الإجراء في حالة ما إذا كانت البيانات تتضمن خطرا أو ضررا بالمجتمع مثل البرامج التي تحتوي على فيروسات أو تقدم نموذجا لعمل الفيروسات، ولا يقصد بعبارة

[1]- Article 19/3 du C.C.C :rendre inaccessibles ou enleverces données informatiques du système informatique consulté.

"الرفع" تدمير البيانات بل تستمر في الوجود، إلا أنه يتم حرمان المشتبه فيه من الولوج إليها، لكن يمكن إعادتها بعد التحقيق الجنائي[1].

غير أنّ ضبط البيانات الإلكترونية المتحصل عليها من التفتيش يثير إشكال آخر يتعلق بمدى جواز الإطلاع على الأسرار التي تتضمنها الأوراق المختومة أو المغلقة الموجودة في منزل المتهم أثناء تفتيشه من قِبل ضابط الشرطة القضائية، وما مدى سريان القيود الخاصة بضبط تلك الأوراق على ضبط البيانات الإلكترونية المتحصل عليها من تفتيش نظم الحاسوب؟.

هذا القول يوجد له تطبيق في التشريع المصري وبالخصوص نص المادة (52)[2] من قانون الإجراءات الجنائية المصري، على اعتبار أنّ المشرع الجزائري والفرنسي خالفا نظيرهما المصري، وذلك بإجازة الإطلاع على الأوراق الموجودة بمنزل المتهم أثناء تفتيشه ولو كانت مختومة ومغلقة من طرف ضابط الشرطة القضائية طبقا لنص المادة (84)[3] من قانون الإجراءات الجزائية الجزائري.

أمّا بالنسبة للإجابة عن هذا الإشكال، فيكون بالإيجاب وذلك لسببين[4]:

1- إنّ العلة التي اقتضت حظر الإطلاع على الأوراق المختومة أو المغلقة تتوفر بالنسبة لمحتوى نظام المعالجة الآلية للمعطيات، فالغلق أو التغليف بالنسبة لتلك الأوراق يضيف عليها مزيدا من السرية ويفصح عن رغبة صاحبها في عدم إطلاع الغير على مضمونها بغير إذن، وهو ما يتحقق بالنسبة للبيانات المخزنة في نظام معلوماتي، لأن محتواها لا يكون مكشوفا بل محجوبا عن الغير، حيث لا يمكن الوصول أو الإطلاع عليها بغير معرفة طريقة ومفاتيح تشغيله.

2- أنّ المادة (52) المذكورة، ترسي قاعدة عامة وضمانة بالنسبة للأسرار التي تتضمنها سائر وسائط وأوعية حفظ وتخزين المعلومات، سواء ما كان منها تقليديا كالأوراق، أو مستحدثا كالأقراص المرنة والأشرطة الممغنطة، ومتى توفر الغلق في تلك الأوعية عن طريق التشفير مثلا، فلا يجوز لضابط الشرطة القضائية الإطلاع عليها.

---

[1]- أ.عائشة بن قارة، المرجع السابق، ص 117.

[2] - تنص المادة 52 من قانون الإجراءات الجنائية المصري:"إذا وجدت في منزل المتهم أوراق مختومة أو مغلقة بأي طريقة أخرى، فلا يجوز لمأمور الضبط القضائي أن يفضها".

[3]- تنص المادة 84 من قانون الإجراءات الجزائية الجزائري:"إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات فإنّ لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الاطلاع عليها قبل ضبطها مع مراعاة ما تقتضيه ضرورات التحقيق وما توجبه الفقرة الثالثة من المادة 83".

[4]- د. طارق ابراهيم الدسوقي عطية، المرجع السابق، ص445.

المطلب الرابع: الشهادة.

الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت، سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم أو براءته منها[1].

كما عرفتها محكمة النقض المصرية بأنّها إدلاء شخص بما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه[2].

وللشهادة في مجال الإجراءات أهمية بالغة لأنّ الجريمة ليست تصرفا قانونيا، ولكنها عمل غير مشروع يجتهد الجاني في التكتم عند ارتكابه ويحرص على إخفائه، ويترتب على ذلك أنّ العثور على شاهد يعتبر مكسبا كبيرا للعدالة.

و لا شك أن سماع الشهود يعتبر كسائر إجراءات التحقيق من الأمور التقليدية لسلطة التحقيق فلها أن تسمع الشهود أو تستغني عنهم فالأمر متروك لظروف التحقيق[3].

ومن بين خصائص الشهادة ما يلي[4]:

1. أنها شخصية يؤديها الشاهد بنفسه ولا تجوز الإنابة أو التوكيل فيها، وعلى الشاهد أن يحضر أمام القاضي لأدائها، فإن تعذر ذلك كان على القاضي أن ينتقل إليه، أمّا الإدلاء بها خارج هذا الإطار أو كتابتها في ورقة عرفية، فإنه يفقدها جوهرها.
2. الشهادة تنصب على ما أدركته حواس الشاهد وليس على تفسيره للحوادث أو تعبيره عن أفكاره الخاصة أو معتقداته.
3. الشهادة دليل ذو قوة متعدية، بحيث أنّ إثبات واقعة بواسطة شهادة الشهود يعني ثبوتها في مواجهة كل الأطراف.
4. ألاّ يكون الشاهد خصما في الدعوى أو عضوا في المحكمة التي تنظر الدعوى.
5. أن تؤدى الشهادة كقاعدة عامة بعد أداء اليمين القانونية.

---

[1]- أ. علي عدنان الفيل، المرجع السابق، ص 61.

[2]- نقض 06 أبريل سنة 1979م، س، 2ق، رقم 90، ص426، نقض 15 يونيو سنة 1964م، س 15 ق، رقم 98، ص493 . نقلا عن : د.محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، ط2، سنة 1988، ص 430.

[3]- أ. علي عدنان الفيل، المرجع السابق، ص 61.

[4]- أ. نجيمي جمال، المرجع السابق، ص 289.

وفي إطار حماية الشاهد، يرى البعض[1] أنه من حق الشاهد أن يمتنع وفقا لتصريح صادر من السلطة القضائية المختصة، من إعطاء أي بيانات شخصية عنه حماية له ولأفراد أسرته.

ولا تقلّ الشهادة أهمية في الجريمة الإلكترونية عن باقي الإجراءات في الحصول على الدليل الإلكتروني، فالقاعدة العامة تقضي بأن يلتزم الشاهد بالإفضاء بما يعلمه من معلومات بخصوص واقعة الجريمة والفاعلين فيها والإدلاء بكل ما يفيد في كشف الحقيقة من وقائع أخرى[2]، ومن أجل التوضيح أكثر سيتم التطرق إلى تحديد المقصود من الشاهد في الجريمة الإلكترونية والتزاماته وبيان مفهوم الشهادة الإلكترونية.

الفرع الأول: المقصود بالشاهد في الجريمة الإلكترونية.

إنّ الشاهد في الجريمة الإلكترونية هو الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، والذي يكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للمعطيات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي، وذلك تمييزا له عن الشاهد التقليدي[3]، ويشمل الشاهد المعلوماتي بهذا المفهوم عدة طوائف من أهمها:

---

[1]- Françoise Thomas et Alain Liners, la justice pénale à l'épreuve du crime organisé, revue internationale de droit pénale, N°01, 1999, P429.

نقلا عن : أ. أمين ودرار،مدى شرعية أساليب البحث والتحري الخاصة وحجيتها في الإثبات الجزائي ، مذكرة ماجيستير ،كلية الحقوق، جامعة الجيلالي ليابس ،سيدي بلعباس،الجزائر،سنة 2009،ص 213.

[2]– أ.عائشة بن قارة، المرجع السابق، ص 126.

[3]– د. هلالي عبد اللاه أحمد، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، ط 1، سنة 1997، ص23.

أولا: القائم على تشغيل الحاسب الآلي.

وهو المسؤول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به، ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات، كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج[1].

وهناك بعضا من مشغلي الحاسوب يكون متخصصا في إدخال البيانات إلى الحاسوب، وهو يقوم بنقل البيانات من الوثائق إلى وسط التخزين حتى تتم معالجتها بواسطة الحاسوب، ويجب أن تتوافر لديه خبرة الكتابة السريعة على لوحة المفاتيح بالإضافة إلى الخبرة الفنية والذكاء.

ثانيا: خبراء البرمجية.

مخططو البرامج هم الأشخاص المتخصصون في كتابة أوامر البرامج ويمكن تصنيفهم إلى فئتين:

الفئة الأولى: مخططو برامج التطبيقات.

الفئة الثانية: مخططو برامج النظم.

1- **مخططو برامج التطبيقات:**ويقوم مخططو برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم، ثم يقوم بتحليلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، وقد يقوم بتنفيذ ذلك مخطط برامج واحد أو عدة مخططين للبرامج وذلك حسب حجم النظام ومتطلباته،وعندما يزداد عدد المخططين يعمل أحدهم كرئيس للمجموعة، كما يعمل بعض أفراد المجموعة في تحرير وكتابة وثائق البرنامج.

2- **مخططو برامج النظم:**وهم أولئك الذين يقومون باختبار وتعديل وتصحيح برامج نظام الحاسوب الداخلية المعقدة، أي أنهم يقومون بالوظائف الخاصة بتجهيز الحاسوب والبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين، بالإضافة إلى إدخال أي تعديلات أو إضافة لهذه البرامج أو الأجزاء[2].

---

[1]- أ. عائشة بن قارة، المرجع السابق، ص 127.

[2]- د.هلالي عبد اللاه أحمد، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية (دراسة مقارنة)، المرجع السابق، ص24.

ثالثا: المحللون:

وهم القائمون على تحليل الخطوات وتجميع البيانات الخاصة بنظام معين، ودراسة هذه البيانات،و من تم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية بين هذه الوحدات، واستنتاج الأماكن التي يمكن تحديدها بواسطة الحاسب.

رابعا: مهندسو الصيانة والإتصالات: وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسبات بمكوناتها وشبكة الإتصال المختلفة المربوطة بها.

خامسا: مديرو النظم: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية[1].

ويحصر قانون الدليل الخاص بولاية كاليفورنيا الأمريكية شهود الجريمة الإلكترونية فيما يلي[2]:

1- محلل النظم الذي صمم وحدد برنامج الحاسب الآلي الذي أنتج الدليل.

2- المبرمج الذي قام بتحرير البرنامج واختباره.

3- المشغل الذي يقوم بتشغيل البرنامج.

4- طاقم عمليات البيانات التي يعد البيانات بالصور التي يستطيع الكمبيوتر قراءتها.

5- أمناء مكتبة الأشرطة الذين يتحملون مسؤولية توفير الأشرطة أو الأسطوانات التي تشتمل على البيانات الصحيحة.

6- مهندس الصيانة الإلكترونية الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة صحيحة.

7- موظفو المدخلات والمخرجات والمسؤولون عن معالجة مدخلات المستخدم في تنفيذ برامجه.

8- المستخدم النهائي الذي يمد بالمعلومات المدخلة ويصرح بتنفيذ برامج الكمبيوتر ويستخدم نتائجها.

غير أنّه ثمة أشخاص آخرين يعدون بمثابة الشهود في الجريمة الإلكترونية ويمثل بيان هذه الفئات فيما يلي:

---

[1]- د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2006، ص 340.

[2]- أ. علي عدنان الفيل، المرجع السابق، ص63.

1- **متعهد الوصول:** هو أي شخص طبيعي أو معنوي لا يقوم إلا بدور فني يتمثل في توصيل الجمهور بشبكة الإنترنت،فهو يضمن بموجب عقود الإشتراك توصيل المستخدم بالمواقع التي يرغب في الدخول إليها، وعلى ذلك فإن هذا المتعهد لا يقدم المعلومة محتوى الرسالة.

2- **متعهد الإيواء:** هو الذي يسمح بالوصول إلى الموقع من خلال شبكة الإنترنت، وهو عبارة عن شركة تجارية أو أحد أشخاص القانون العام، يعرض إيواء صفحات الويب على حاسباته الخادمة، ويتم ذلك غالبا في مقابل أجر.

3- **المنتج:** يقصد بالمنتج هو منتج الخدمة المعلوماتية في وسائل الإتصال السمعي والبصري، ومنتج الخدمة يمكن أن يحاكم كفاعل أصلي حتى ولو كانت الرسالة غير مسجلة بصفة مسبقة على توصيلها إلى الجمهور[1].

4- **ناقل المعلومات:** يمكن أن يصنف كذلك كشاهد في الجريمة الإلكترونية، وهو العامل الفني الذي يقوم بالربط بين الشبكات، وذلك بمقتضى عقد نقل المعلومات من جهاز المستخدم إلى الحاسب الخادم لمتعهد الوصول، ثم نقلها من هذا الحاسب الأخير إلى الحاسبات المرتبطة بمواقع الإنترنت أو لمستخدمي الشبكة الآخرين.

5- **متعهد الخدمات:** ويمكن اعتباره من قبيل الشهود في الجريمة الإلكترونية ويعرف بأنه ناشر الموقع وهو المسؤول الأول عن المعلومات التي تعبر الشبكة، لأنه الوحيد صاحب السلطة الحقيقية في مراقبة المعلومات التي يتم بثها.

6- **مورد المعلومات:** هو ذلك الشخص الذي يقوم بتحميل الجهاز أو النظام بالمعلومات التي قام بتأليفها أو جمعها حول موضوع معين، ومن تم تكون له سيطرة كاملة على المادة المعلوماتية التي تبث عبر الشبكة، فهو الذي يقوم بالإختيار ثم التجميع ثم التوريد حتى يصل إلى الجمهور في صورة مادة معلوماتية على الشبكة.

7- **مؤلف الرسالة:** هو المسؤول الأول عن أي معلومات غير مشروعة تتضمنها هذه الرسالة، فإن تضمنت مثلا عبارات القذف أو السب التي ينشرها أو يرسلها على أحد المؤتمرات، فإنّ مؤلف الرسالة يسأل جنائيا عن هذه العبارات، كما أنه يمكن سؤاله كشاهد عن المعلومات التي وصلت إليه من خلال دوره في خدمة العميل على الشبكة المعلوماتية[2].

---

[1]- د.جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، المرجع السابق، ص 134 وما بعدها.

[2]- د.عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 183 .

الفرع الثاني: إلتزامات الشاهد المعلوماتي.

تتمثل هذه الإلتزامات فيما يلي:

أولا: إلزام الشاهد بالإدلاء بالمعلومات.

إذا كان التزام الشاهد بالشهادة في الجرائم التقليدية لا يثير خلافا يذكر بين الفقهاء، فإنهم قد انقسموا إلى اتجاهين حول مدى جواز التزام الشاهد المعلوماتي في الجرائم الإلكترونية على الإدلاء بمعلومات يملكها بخصوص كيفية الولوج إلى النظام المعلوماتي الخاص به، أو على القيام بطبع ملفات معينة أو تحليل ذاكرة نظامه المعلوماتي، من أجل إعانة سلطات الإستدلال والتحقيق في البحث عن أدلة تخص الجريمة الإلكترونية الواقعة، وفيما يلي تفصيل ذلك:

الإتجاه الأول:

يذهب أنصار هذا الإتجاه إلى عدم جواز إلزام الشاهد المعلوماتي على الإدلاء بتلك المعلومات أو القيام بتلك الأعمال، لأنّ ذلك لا يدخل ضمن الواجبات والإلتزامات المفروضة عليه، وقد تأثر المشرع التركي بهذا الإتجاه، فالقانون التركي لا يجيز إلزام الشاهد المعلوماتي بالإفصاح عن كلمات السر أو الشفرات اللازمة لتشغيل البرامج المختلفة أو الولوج إليها[1]، وكذلك المشرع المجري، حيث أنّ القانون المجري يجيز للشاهد المعلوماتي أن يرفض طبع الملفات المسترجعة من ذاكرة نظامه المعلوماتي[2].

الإتجاه الثاني:

يرى أنّه من الممكن إلزام الشاهد المعلوماتي بالإفصاح عن تلك المعلومات، وذلك من خلال النص الصريح في القانون في فرض إلتزام على عاتقه يسمى (إلتزام الشاهد المعلوماتي بالإعلام في الجريمة المعلوماتية)، الذي يفرض عليه واجبا بتقديم أية معلومات ضرورية ولازمة من أجل إعانة سلطات التحقيق في الحصول على أدلة إثبات عن الجريمة الإلكترونية الواقعة.

---

[1]- د.عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 161.نقلا عن: أ.رشاد خالد عمر، المرجع السابق، ص 156.

[2]- نقلا عن: نفس المرجع، ص 156.

ولا شكّ في أنّ فرض مثل هذا الإلتزام من شأنه أن يلعب دورا وقائيا كبيرا في حفظ النظام المعلوماتي من الخضوع بأكمله للتفتيش والضبط، ففرضه يبعد مثل هذا الإحتمال، لأنّه يمكّن الجهات المختصة بالتحقيق من الوصول إلى المواقع المراد تفتيشها ومن دون الحاجة إلى ضبط النظام[1].

ويذهب اتجاه في الفقه الفرنسي[2] إلى أنّ القواعد العامة في مجال الإجراءات المتعلقة بالشهادة هي التي يتم تطبيقها في مجال الإجراءات الإلكترونية، ومن تم فإنه على الشهود الذين يقع على عاتقهم الإلتزام بتقديم شهادتهم المواد (62)،(109)،(438) من قانون الإجراءات الجزائية الفرنسي، وأن يكشفوا على كلمات المرور السرية التي يعلمونها وشفرات تشغيل البرامج فيما عدا حالات المحافظة على السر المهني، فإنه في حل من الإلتزام بالإدلاء بشهادتهم.

كما يلاحظ أنّ المشرع الأمريكي قد نص وفي أكثر من موضع على إلزام شهود المعلوماتية، خصوصا مزودي خدمات الإتصالات الإلكترونية بتقديم ما يلزم من عون فني تقني لسلطات الإستدلال والتحقيق في الجرائم الإلكترونية، ومن يخالف هذا الالتزام يتعرض لجزاءات[3].

وفي هولندا يتيح مشروع قانون الحاسوب لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل النظام لتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة، وإذا وجدت بيانات مشفرة داخل ذاكرة الحاسب وكانت مصلحة التحقيق تستلزم الحصول عليها، يتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات.

كما يمكن في اليونان الحصول من القائم على تشغيل نظام الحاسوب على كلمة المرور السرية للولوج إلى نظام المعلومات والحصول على بعض الإيضاحات الخاصة بنظامه الأمني، لكن ليس على الشاهد أي التزام بالنسبة لطباعة ملفات بيانات مخزنة في ذاكرة الحاسب، وذلك لأنه يجب أن يشهد على معلومات حازها بالفعل، وليس الكشف عن معلومات جديدة[4].

---

[1]– أ.رشاد خالد عمر، المرجع السابق، ص 695/156.

[2] - Jacques Francillon, les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France, R.I.D.P. 1993, p309.

نقلا عن: أ. عائشة بن قارة، المرجع السابق، ص 131.

[3]– أ.رشاد خالد عمر، المرجع السابق، ص 157.

[4]– أ.علي عدنان الفيل، المرجع السابق، ص 65.

وكذلك المادة (29)من قانون الإجراءات الجنائية المصري التي خولت لرجل الضبط القضائي، سماع أقوال من يكون لديهم معلومات عن الوقائع الجنائية ومرتكبيها، وله أن يسمع في حالة التلبس بالجريمة أقوال الأشخاص الحاضرين في محل الواقعة ومن يمكن الحصول منه على إيضاحات في شأن الجريمة طبقا للمادة (31) من نفس القانون، وأن يطلب من الحاضرين عدم مبارحة محل الواقعة أو الإبتعاد عنه وأن يستحضر في الحال من يمكن الحصول منه على إيضاحات في شأن الواقعة وفقا للمادة (32) من قانون الإجراءات الجنائية المصري.

أمّا قانون الإجراءات الجزائية الجزائري وإذا كان لا يلزم الأفراد على التحمل فإنّه يلزمهم على الأداء، إذ يتعين على كل شخص استدعي بواسطة أحد أعوان القوة العمومية لسماع شهادته أن يحضر ويؤدي اليمين عند الإقتضاء ويدلي بشهادته وإلاّ سيعاقب بمقتضى المادة (97)[1]، أي أنّ الشخص الذي يتراءى لقاضي التحقيق أن سماعه كشاهد مفيد لإظهار الحقيقة، فإنه ملزم بالحضور وبأداء اليمين وبأداء الشهادة ما لم يكن هناك مانع قانوني كالسر المهني، وفي حالة مخالفته لأي من هذه الواجبات، فإنّه يتعرض للإحضار بالقوة العمومية وللعقاب، وإذا كان الشخص يعرف مرتكبي الجناية أو الجنحة، ويرفض الإجابة عن الأسئلة الموجهة إليه فالعقوبة تكون أكثر قساوة وتتمثل في الحبس والغرامة طبقا للمادة (98) من قانون الإجراءات الجزائية الجزائري.

وأمّا أمام جهة الحكم، فالمسألة يحكمها نصوص المواد (222،223) من قانون الإجراءات الجزائية، إذ أنّ كل شخص مكلف بالحضور أمام المحكمة لسماع أقواله كشاهد يكون ملزما بالحضور وحلف اليمين وأداء الشهادة[2]، وإذا تخلف عن الحضور أو امتنع عن حلف اليمين أو أداء الشهادة يعاقب كذلك بالعقوبة المنصوص عليها في المادة (97) المذكورة، كما يخول القانون للجهة القضائية عند تخلف شاهد عن الحضور بغير عذر مقبول ومشروع أن تأمر باستحضاره بواسطة القوة العمومية لسماع أقواله أو تأجيل القضية لجلسة قريبة، ويكون على عاتق الشاهد المتخلف مصاريف التكليف بالحضور والإجراءات والانتقال وغيرها[3].

---

[1]- تنص المادة 97 فقرة 2 من قانون الإجراءات الجزائية الجزائري على ما يلي:"...وإذا لم يحضر الشاهد فيجوز لقاضي التحقيق بناءا على طلب وكيل الجمهورية استحضاره جبرا بواسطة القوة العمومية ....".

[2]- تنص المادة 222 من قانون الإجراءات الجزائية الجزائري على ما يلي:" كل شخص مكلف بالحضور أمام المحكمة لسماع أقواله كشاهد ملزم بالحضور وحلف اليمين و أداء الشهادة ."

[3] – تنص المادة 223 من قانون الإجراءات الجزائية الجزائري على ما يلي:" ... ويجوز للجهة القضائية لدى تخلف شاهد عن الحضور بغير عذر تراه مقبولا ومشروعا، أن تأمر بناءا على طلب النيابة العامة أو من تلقاء نفسها باستحضاره إليها على الفور بواسطة القوة العمومية لسماع أقواله أو تأجيل القضية لجلسة قريبة.

وكذلك الأمر أمام محكمة الجنايات، بحيث إذا تخلف شاهد عن الحضور بدون عذر مقبول جاز لمحكمة الجنايات بناءا على طلب النيابة العامة أو من تلقاء نفسها استحضار الشاهد بواسطة القوة العمومية، والعقوبة في هذه الحالة تكون أكثر قساوة[1].

ثانيا: شروط إلزام الشاهد بالإعلام في الجريمة الإلكترونية.

إنّ الشاهد المعلوماتي عندما يكون حائزا لمعلومات واجبة لاختراق نظام المعالجة الآلية للمعطيات،وتتعلق بالبحث عن الأدلة التي يتطلبها التحقيق عندئذ يكون ملزما بإعلام سلطات التحقيق بذلك، وإلاّ يعد حينها ممتنعا عن الشهادة، كما أنه من شأن هذا الإلتزام أن يحقق مبدأ التوازن في المعلومات الجوهرية المتعلقة بالنظم المعلوماتية بين شهود ومستخدمي الحاسب الآلي وسلطات التحقيق، كما يحقق التعاون والتضامن بين المتعاملين في بيئة تكنولوجيا المعلومات ضد كل من يحاول إساءة استخدام الحاسب الآلي،ويمكن في نفس الوقت من تدارك أوجه القصور والعجز الذي تتسم به الوسائل التقليدية مما بات من الضروري الأخذ بفكرة الإلتزام بالإعلام في الجرائم المعلوماتية[2].

ولا ينشأ إلتزام الشاهد بالإعلام في الجريمة الإلكترونية إلا بتوفر ثلاثة شروط وهي:

1- وقوع جريمة إنترنت فعلا سواء كانت جناية أو جنحة، فحتى يلتزم الشاهد المعلوماتي بالإعلام في أي جريمة إلكترونية لابد أن تكون هذه الجريمة قد وقعت فعلا،فلا ينشأ هذا الإلتزام بشأن جريمة محتملة، فلابد أن تكون الجريمة هي جناية أو جنحة،وبالتالي لا ينشأ هذا الإلتزام بالإعلام على عاتق الشاهد المعلوماتي بشأن ما يقع من مخالفات.

2- أن يكون لدى الشاهد المعلوماتي معرفة وعلم بالمعلومات الجوهرية المتعلقة بالنظام المعلوماتي محل الواقعة ويتمثل مضمون هذه المعلومات في ثلاثة عناصر وهي:

أ- طبع ملفات البيانات المخزنة في ذاكرة الحاسوب أو حاملات البيانات الثانوية ويعلم بها جهات التحقيق.

ب- الإفصاح عن كلمات المرور السرية لجهات التحقيق.

وفي الحالة الأخيرة يجعل الحكم على عاتق الشاهد المتخلف مصاريف التكليف بالحضور والإجراءات والإنتقال وغيرها ...".

[1]- تنص المادة 299 من قانون الإجراءات الجزائية الجزائري على ما يلي: " إذا تخلف شاهد عن الحضور بدون عذر مقبول جاز لمحكمة الجنايات أن تأمر بناءا على طلبات النيابة العامة أو من تلقاء نفسها باستحضار الشاهد المتخلف بواسطة القوة العمومية عند الإقتضاء أو تأجيل القضية لتاريخ لاحق. وفي هذه الحالة، يتعين عليها أن تحكم على الشاهد الذي تخلف عن الحضور أو رفض أن يحلف أو يؤدي شهادته بغرامة من خمسة آلاف دينار (5000دج) إلى عشرة آلاف(10.000دج) أو بالحبس من عشرة (10) أيام إلى شهرين...". أحكام الشهادة: نقلا عن أ. نجيمي جمال ، المرجع السابق، ص 297.

[2]- د.هلالي عبد اللاه أحمد، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية، المرجع السابق، ص 59.

ج- الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة، حيث أنّ الأوامر والرسائل المكتوبة بالشفرة (Code) تحتاج إلى ترجمة كل هذه الشفرة حتى يمكن فهمها.

3- أن تستلزم مصلحة التحقيق ضرورة الحصول على هذه المعلومات الجوهرية، فلا يكفي أن يلتزم الشاهد المعلوماتي بالإعلام في الجريمة الإلكترونية أن يكون هناك أحد الجرائم قد وقعت حقيقة وأنها تعد جناية أو جنحة، بل يجب إضافة إلى ذلك أن يكون من مصلحة التحقيق الحصول على تلك المعلومات الجوهرية وكشف المتورطين فيها والتوصل إليهم، فلابد أن تكون هذه المعلومات لازمة وضرورية كما أنها تفيد في كشف الحقيقة[1].

الفرع الثالث: الشهادة الإلكترونية.

يقصد بمصطلح الشهادة الإلكترونية تلك الصورة من أداء الشهادة والتي لا يكون فيها الشاهد حاضرا جلسة التحقيق بذاته، وإنما تتم بواسطة وسائل إلكترونية أو رقمية متطورة وتتخذ الشهادة الإلكترونية إحدى هاتين الحالتين:

أولا: الشهادة الإلكترونية المسجلة:

هي الحالة التي تكون فيها الشهادة قد تم تسجيلها في تاريخ سابق على إحدى وسائط التسجيل (شريط أو أسطوانة) ثم يتم عرضها فيما بعد على محكمة الموضوع أو جهة التحقيق، بواسطة جهاز إلكتروني، وبالتالي يمكن الرجوع إليها أكثر من مرة وفي أي وقت تحتاج فيه إلى ذلك جهة التحقيق، كما أنّ هذا التسجيل يشكل ضمانة أساسية في عدم وجود إكراه من أي نوع يمكن أن يكون واقعا على المتهم.

[1]- د.سامح أحمد بلتاجي موسى، المرجع السابق، ص 299.

ثانيا: الشهادة الإلكترونية المباشرة أو الفورية:

يفترض حدوث الشهادة في هذه الحالة عن طريق حضور الشاهد جلسة التحقيق النهائي أمام المحكمة حضورا إلكترونيا غير مادي أو جسدي، وذلك بواسطة استخدام الدوائر المغلقة عن بعد.

وقد أثير مدى إمكانية قبول الشهادة الفورية عبر الدوائر الإتصالية الإلكترونية المتكاملة وهو الأمر المقبول فقها، سيما أنّ الشاهد يظهر في هيئته الكاملة، فيبدو كما لو كان حاضرا، وتبرز مظاهر مصداقيته في ردة فعله أثناء سير جلسة التحقيق.

ويميز القضاء الأمريكي بين نوعين من الشهادة الإلكترونية المرئية، فالنوع الأول هو الشهادة المرئية ذات الإتجاه الواحد، ففي هذه الحالة فإنّ الشاهد حين يدلي بشهادته لا يرى سوى الكاميرا المسلطة عليه فالرؤيا تكون من طرف واحد وهو هيئة المحلفين والمحكمة، والنوع الثاني هو الشهادة المرئية ذات الإتجاهين، فيها يرى الشاهد من في المحكمة وهم يرونه أيضا، ومدى الأخذ بأي من الشهادتين متروك لتقدير محكمة الموضوع[1].

المطلب الخامس: الخبرة:

إذا كان التحقيق هو محاولة الوصول إلى الحقيقة، فإنّ هذه الحقيقة قد يعترض الوصول إليها مسائل فنية لا يستطيع المحقق بنفسه الفصل فيها أو التغلب عليها، لأنّ ذلك الأمر يتطلب مهارات وقدرات خاصة قد لا تتوافر لديه وهو ما يدعو للإستعانة بخبير أو أكثر لجلاء مسألة معينة أو أكثر قد تواجهه خلال التحقيقات[2]، والخبرة كطريق من طرق الإثبات في المواد الجزائية ما فتئت أهميتها تتعاظم إلى درجة أصبح البعض يرى أنّ الخبير في الوقت الحالي قد أصبح هو القاضي الفعلي بسبب تقدم العلوم في كافة المجالات، كما لم يعد من السهل التهرب من النتائج الحاسمة التي يقدمها العلم لحل أعقد القضايا المطروحة أمام المحاكم.

فالخبير وإن كان عالما في ميدان علمي ما أو متخصصا في فرع من فروع المعرفة، إلاّ أنّه يتميز من حيث أنّه يطبق معلوماته العلمية والفنية على واقعة معينة، فهو لا يكتفي بعرض النظريات والأبحاث العلمية ولا يقتصر دوره على إبراز الجوانب الفنية لمسألة ما، بل عليه أن يصل إلى نتائج وأجوبة محددة للإجابة عن

---

[1]- د.سامح أحمد بلتاجي موسى، المرجع السابق، ص 297.

[2]- نفس المرجع، ص 280.

انشغال الجهة التي كلفته بالمهمة، وأن يتخذ موقفا بناءا على ما توصلت إليه معارفه، ومن أجل ذلك لا يكفي أن يقدم الخبير القضائي تقريرا علميا يسرد فيه مجموعة النظريات التي تتعلق بموضوع الخبرة، ولا يكفي أن يشير إلى كيفية حدوث الظاهرة المعروضة عليه بل يجب إبداء رأيه[1].

فالخبرة عموما هي علم يتطور مع التطور العلمي والتكنولوجي على جميع المستويات، مما يستوجب وجود هؤلاء المتخصصين لإزالة الغموض الذي يحيط بالمسائل التقنية والفنية، كما تعد فنا قوامه المزج بين ما هو تقني وعلمي وما هو قانوني، وهذا العمل ليس بإمكان كل شخص القيام به، وإنما من الضروري أن يكون الخبير على درجة كبيرة من الإلمام بمتطلبات الميدانين حيث تمكنه من المزج بين هذا وذاك حتى يكون التقرير المطالب بإنجازه منسجما ومتكاملا[2].

كما يقصد بها، إبداء رأي فني من شخص مختص في شأن واقعة ذات أهمية في الدعوى الجزائية[3]، وبقدر تنوع مجالات الحياة وتداخلها بقدر تنوع مجالات الخبرة، وبقدر تنوع القضايا المعروضة أمام المحاكم بقدر تنوع المهام التي تسند للخبراء[4].

وتعد الخبرة التقنية من أقوى مظاهر التعامل أو التفاعل القانوني القضائي مع ظاهرة الحوسبة والرقمية، ذلك أنها تؤدي دورا لا يستهان به إزاء نقص المعرفة القضائية الشخصية لظاهرة الإنترنت، وهذا الأمر لا يعني سوى أن القضاء يتعامل مع الواقع في صورته التقليدية كما المتطورة من ناحية، كما أن ذلك يعني من ناحية أخرى أن الظواهر الجديدة حتى وإن تدخل القانون لوضع حلول للمشاكل التي تطرحها، فإن الدور القضائي في تفسير هذه النصوص القانونية يظل دورا أصليا في هذا الإطار، وهو لكي يؤدي دوره يلزمه الإتفاق مع طبيعة التقنية بعيدا عن الإفتراض، وتبقى الخبرة التقنية في مجال الإنترنت أداة رئيسية لتكوين الحكم الجنائي[5].

والواقع أن هذا النوع المتميز من الخبرة بدأ يتخذ لنفسه حيزا في مجال إثبات الجرائم الإلكترونية حتى أصبح يعرف في الفقه المقارن بمصطلح المعلوماتية الشرعية، ويقصد بها استخدام الطرق العلمية لجمع وتعريف وتحليل وتفسير الدليل الرقمي المأخوذ من مصادر رقمية، و الإحتفاظ به وتوثيقه، على نحو يسهل بناء الحوادث

---

[1]– أ.بجيمي جمال، المرجع السابق، ص 223.

[2]– د.سامح أحمد بلتاجي موسى ، المرجع السابق، ص 280.

[3]– أ.إلياس أبو العيد، نظرية الإثبات في أصول المحاكمات المدنية والجزائية، منشورات زين الحقوقية، لبنان، بدون طبعة، سنة 2005، ص 340.

[4]– أ. بجيمي جمال، المرجع السابق، ص223.

[5]– د. عمر بن يونس، الدليل الرقمي، المرجع السابق، ص 110.

التي تؤدي إلى اكتشاف الجريمة، فالمعلوماتية الشرعية هي عملية البحث التي يقوم بها الخبير المعلوماتي من أجل الحصول على الدليل الإلكتروني، بغية إعادة بناء مجريات القضية وتوضيحها للمحكمة[1].

فلاشك أن الخبرة تعد من أهم العوامل المساعدة لسلطات التحقيق في التعامل مع الواقعة الإجرامية حتى لا يتم إتلاف الدليل، ولذلك لا تختلف الخبرة في الجرائم التقليدية عن تلك الخبرة المتطلبة في الجرائم المعلوماتية، من حيث القواعد المنظمة لها وكذا في نوعية الخبير المنتدب والذي ينبغي أن يكون على دراية بنظم الحاسوب[2]،فالقاضي حين يقوم بالإستعانة بالخبرة في مسألة ما تخص القضية المعروضة أمامه، فإنه يسعى إلى الخبير بحسب تخصصه، ومجال التخصص محكوم بقاعدة طبيعية وهي قاعدة العلم المؤسس على التحصيل الدوري الدراسي، كما هو الشأن في دراسة الطب أو الهندسة أو العلوم الفنية في مجال الجريمة كدراسة علم البصمات وعلوم الصيدلة[3].

ومن هذا المنطلق سيتم التطرق لكيفية اعتماد الخبير التقني وأنواع الخبرة التقنية وجميع المسائل المتعلقة بها، وذلك على النحو التالي:

الفرع الأول: كيفية إعتماد الخبير التقني.

طبقا للقانون الجزائري، حتى يصبح الخبير خبيرا قضائيا يجب أن يكون معتمدا من طرف القضاء، واعتماد الخبراء من طرف القضاء تنفيذا لنص المادة (144) من قانون الإجراءات الجزائية ينظمه المرسوم التنفيذي رقم (95-310) الذي يحدد شروط التسجيل في قوائم الخبراء القضائيين وكيفياته، كما يحدد حقوقهم وواجباتهم[4]، وهو المرسوم الذي يبين أنّ اختيار الخبراء القضائيين يكون على أساس القوائم التي يوافق عليها وزير العدل في دائرة اختصاص المجلس القضائي، ويمكن تعيينهم استثناءا لممارسة مهامهم خارج اختصاص المجلس الذي ينتمون إليه، وأنّه يجوز للجهة القضائية في حالة الضرورة أن تعين خبيرا لا يوجد اسمه في القوائم المنصوص عليها، أمّا القضاء الفرنسي يستلزم ندب خبير من خارج جدول الخبراء ضرورة أن تقوم جهة التحقيق بتسبيب قراره وإلاّ ترتب البطلان على هذا القرار بندب الخبير[5].

---

[1]– د. طارق عبد الرؤوف الخن، المرجع السابق، ص 331.

[2]– د.طارق فوزي الفقي، المرجع السابق، ص 166.

[3]– د.حسين الغافري، المرجع السابق، ص 562.

[4]– المرسوم التنفيذي رقم 95-310 المؤرخ في 15 جمادى الأولى عام 1416 الموافق لـ 10 أكتوبر سنة 1995 الذي يحدد شروط التسجيل في قوائم الخبراء القضائيين وكيفياته.

[5]–أ.بحيمي جمال، المرجع السابق، ص 224.

وقد ترك القانون لقاضي التحقيق حرية ندب خبير واحد أو خبراء متعددين طبقا لنص المادة (147)[1] من قانون الإجراءات الجزائية الجزائري، وهذا هو حال التشريع المقارن، حيث يعترف بتعدد الخبراء في الدعوى الواحدة، بحيث يمكن أن يكون لكل متهم دورا محددا، ومن ناحية أخرى فإنّ المشرع الجنائي لم ينص على ضرورة أن يكون الخبير في الدعوى واحد، وهذا يتجاوب مع الجرائم الالكترونية وما يكتنفها من تعقيد وتطور سريع يصعب اللحاق به لأجل الوصول إلى النتائج المبتغاة من الإستعانة بالخبير، ومن تم يجب أن يكون هناك أكثر من خبير في الدعوى التي يكون موضوعها تكنولوجيا المعلومات[2]،كما لم يحدد المشرع طبيعة شخص الخبير سواء كان شخصا طبيعيا أو معنويا.

وبالرجوع إلى القانون رقم (09-04) الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، فقد تضمن الفصل الخامس منه ضرورة إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، وحدد مهامها في المادة (14)[3] منه، غير أنّ أهم فقرة في هذه المادة هي الفقرة (ب) التي جعلت من هذه الهيئة خبيرا قضائيا في خدمة الشرطة القضائية والسلطات القضائية.

وإلى جانب الشروط المتطلبة في الخبير (شخص طبيعي) من اشتراط الجنسية، حسن السيرة وغيرها من الشروط التي أقرها المرسوم التنفيذي الذي يحدد شروط التسجيل في قوائم الخبراء القضائيين السابق الإشارة إليه[4]، غير أنّ ما يلفت النظر اشتراط أن تكون لدى الخبير شهادة جامعية أو تأهيل مهني معين في

---

[1]– تنص المادة 147 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يجوز لقاضي التحقيق ندب خبير أو خبراء."

[2]– د. طارق فوزي الفقي، المرجع السابق، ص 176.

[3]– تنص المادة 14 على ما يلي: تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام التالية:

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها في شأن الجرائم ذات الصلة بتكنولوجيات الإعلام والإتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

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

[4]– الشروط الواجب توافرها في الخبير (الشخص الطبيعي) حددها المرسوم التنفيذي المذكور كما يلي:

- أن تكون جنسيته جزائرية مع مراعاة الإتفاقية الدولية.
- أن تكون له شهادة جامعية أو تأهيل مهني معين في الاختصاص الذي يطلب التسجيل فيه.
- ألاّ يكون قد تعرض لعقوبة نهائية بسبب ارتكابه وقائع مخلة بالآداب العامة أو الشرف.
- ألاّ يكون قد تعرض للإفلاس والتسوية القضائية.
- ألاّ يكون ضابطا عموميا وقع خلعه أو عزله، أو محاميا شطب إسمه من نقابة المحامين، أو موظف عزل بمقتضى إجراء تأديبي.
- ألاّ يكون قد منع بقرار قضائي من ممارسة المهنة.
- أن يكون قد مارس هذه المهنة أو هذا النشاط في ظروف سمحت له أن يتحصل على تأهيل كاف لمدة لا تقل عن (7) سنوات.

الإختصاص الذي يطلب التسجيل فيه، فهذا الشرط ضروري ومنطقي أن يتوافر في الخبير التقليدي على أساس أن المنهج الذي ينتهجه في عمله يستند إلى حقائق العلم، في حين لا يتطلب ذلك في الخبير في الجرائم الالكترونية نظرا للتطور السريع في تكنولوجيا المعلومات، ومن تم لا مانع من الإستعانة بخبير غير دارس طالما أنّه يملك من الخبرات ما يمكنه من الوصول إلى الحقيقة، فينبغي التقرير بأنّ دراسات الحاسوب والإنترنت لا ترتبط بمنهج دراسي أو بحثي معين أو حتى مدة زمنية يقضيها الشخص في الجامعات والمعاهد المتخصصة، وإنّما ترتبط بمهارات خاصة إذ أنه من الممكن أن يكون أمهر برمجي نظم التشغيل لم يتجاوز تحصيله العلمي المرحلة الثانوية مثل بيل غيتس (Bill Gates)[1]، كما أنّ التزام الخبير هو إلتزام ببذل عناية، فلا يسأل إذا لم يصل إلى النتيجة المطلوبة نتيجة ضعف خبرته أو بسبب العقبات التي واجهته أثناء مباشرته لمهمته، هذا ويمكن أن تثور مسؤوليته الجنائية في حالة ما إذا قام عمدا بإتلاف البيانات المطلوب منه التعامل معها أو حفظها[2].

وفضلا عن هذه الشروط، هناك إجراءات شكلية يتطلبها القانون في الخبير وكلها إجراءات يترتب على مخالفتها البطلان إذا لم يقم الخبير بمراعاتها كحلف اليمين[3]كي يصبح الخبير معتمدا بصفة رسمية، مع ملاحظة أنّ طلب الإعتماد إذا كان مقدما من طرف شخص معنوي فإنّ النص القانوني لم يحدد من يقوم بأداء اليمين هل هو الممثل القانوني للشخص المعنوي أو الخبراء العاملون لديه،ومن باب القياس فإنّ قانون الإجراءات الجزائية الفرنسي ينص على أن تؤدى اليمين من طرف الخبراء التابعين لهذا الشخص[4] طبقا لنص المادة (157-1)[5].

- أن تعتمد السلطة الوصية في اختصاصه أو يسجل في قائمة تعدها هذه السلطة.

أمّا إذا كان الطلب مقدما من شخص معنوي، فإنّ المرسوم التنفيذي المذكور يشترط ما يلي:

- أن تتوفر في المسيرين الإجتماعيين الشروط المنصوص عليها في الفقرات 3و4و5 من المادة الرابعة السابقة.
- أن يكون الشخص المعنوي قد مارس نشاطا ما لا يقل مدة عن خمس (5) سنوات لاكتساب تأهيل كاف في التخصص الذي يطلب التسجيل فيه.
- أن يكون له مقر رئيسي أو مؤسسة تقنية تتماشى مع تخصصه في دائرة اختصاص المجلس القضائي.

[1] – د.حسين بن سعيد الغافري، المرجع السابق، ص564.

[2] – د.سامح بلتاجي موسى، المرجع السابق، ص262.

[3] – تنص المادة 145 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتية بيانها:

–أقسم بالله العظيم بأن أقوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص و أن أبدي رأيي بكل نزاهة واستقلال–... "

[4] – أ. نجيمي جمال، المرجع السابق، ص 226.

[5]- Article 157-1 (C.P.P.FCréé par Loi 75-701 1975-08-06 art. 24 JORF 7 août 1975 en vigueur le 1er janvier 1976) :Si l'expert désigné est une personne morale, son représentant légal soumet à l'agrément de la juridiction le nom de la ou des personnes physiques qui, au sein de celle-ci et en son nom, effectueront l'expertise.

هذا إضافة إلى أنّ مهمة الخبير تحدد دائما في الأمر أو الحكم أو القرار الذي انتدبه، ويجب لزوما أن تقتصر المهام المسندة إليه على فحص مسائل ذات طابع فني وليس تحليل مسائل قانونية لأنّ ذلك من مهام القضاة[1]، كما ينبغي عليهم التقيد بأجل إنجاز الخبرة طبقا لنص المادة(148)[2] من قانون الإجراءات الجزائية الجزائري، ويجوز أن تمد هذه المهلة بناءا على طلب الخبراء وفي حالة عدم إيداعهم لتقاريرهم واحترام المدة المعينة يمكن استبدالهم بخبراء آخرين مع رد جميع الأشياء والأوراق والوثائق التي تكون قد منحت إليهم من أجل إنجاز مهمتهم، وقد تتخذ ضدهم إجراءات تأديبية تصل إلى حد الشطب من جدول الخبراء.

وقد نص المرسوم التنفيذي السابق ذكره على أن يؤدي الخبير القضائي مهمته تحت سلطة القاضي الذي عيّنه وتحت مراقبة النائب العام[3]، وأنّ الخبير القضائي هو المسؤول الوحيد عن الدراسات والأعمال التي ينجزها ويمنع عليه أن يكلف غيره بمهمة أسندت إليه، ويتعين عليه في جميع الحالات أن يحفظ سر ما اطلع عليه[4]، وهو المسؤول عن جميع الوثائق التي تسلم له بمناسبة تأدية مهمته، ويتعين عليه في كل الأحوال أن يلحقها بتقرير الخبرة الذي يقدم إلى الجهة القضائية[5].

الفرع الثاني: أنواع الخبرة التقنية.

الخبرة في المجال التقني تكون خاصة وتكون عن طريق المؤسسات التعليمية، وقد تتم عن طريق جهات الضبط القضائي، وفيما يلي بيان ذلك[6]:

أولا: الخبرة الخاصة:

تعد هذه الخبرة من أقوى أنواع الخبرات على الإطلاق لكونها تنطلق من مفهوم السعي إلى خلق فرص منافسة حقيقية بين المنظمات الخاصة العاملة في مجال التقنية، وكذا الخبرة الخاصة تضم في جنباتها الخبرة الفردية

---

[1]–أ. نجيمي جمال، المرجع السابق، ص 237.

[2] – تنص المادة 148 من قانون الإجراءات الجزائية الجزائري على ما يلي: " كل قرار يصدر بندب خبراء يجب أن تحدد فيه مهلة لإنجاز مهمتهم، ويجوز أن تمد هذه المهلة بناءا على طلب الخبراء إذا اقتضت ذلك أسباب خاصة ويكون ذلك بقرار مسبب يصدره القاضي أو الجهة التي ندبتهم، وإذا لم يودع الخبراء تقاريرهم في الميعاد المحدد لهم جاز في الحال أن يستبدل بهم غيرهم إذ ذاك أن يقدموا نتائج ما قاموا به من أبحاث كما عليهم أيضا أن يردوا في ظرف ثمان وأربعين ساعة جميع الأشياء والأوراق والوثائق التي تكون قد عهد بها إليهم على ذمة إنجاز مهمتهم .

وعلاوة على ذلك فمن الجائز أن تتخذ ضدهم تدابير تأديبية قد تصل إلى شطب أسمائهم من جدول الخبراء المنصوص عليه في المادة 144... ".

[3]– المادة 10 من المرسوم التنفيذي رقم 95–310.

[4]– المادة 12 من المرسوم التنفيذي رقم 95–310.

[5]– المادة 13 من المرسوم التنفيذي رقم 95–310. نقلا عن: أ. نجيمي جمال، المرجع السابق، ص 241.

[6]– د.طارق فوزي الفقي، المرجع السابق، ص 173.

التي تعد أقوى وأهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات والإنترنت، ويكفي هنا أن نذكر أنّ المؤسسات الكبرى المتخصصة في مجال الحاسوب والإنترنت تسعى بكل جهدها إلى الإستعانة بأشخاص أثبتوا كفاءتهم في مجال تكنولوجيا المعلومات حتى الهاكرز، فإنّ اتجاها اقتصاديا يحاول جاهدا إثبات عدم جدوى التخلص من هؤلاء بمعاقبتهم وفقا للقانون، وإنما يلزم اللجوء إلى الحلول الاقتصادية حتى يظلوا عاملين في إطار الأهداف الإقتصادية.

وإلى جانب الأفراد توجد المنظمات الخاصة في كافة المجالات، والتي سوف يكون لها السبق في مجال الخبرة، وتختلف المنظمات الخاصة ما بين منظمات أهلية تتصدى لكل محاولة من المجرمين بقصد التعدي على الحقوق الإلكترونية، وبين نوعية تسعى إلى فك رموز العالم الإفتراضي على أسس تجارية، فقد استطاعت إحدى الشركات الإسكتلندية المتخصصة في برمجيات الحاسوب والإنترنت وهي شركة (Scottich Software) من إعداد مشروع خريطة للعالم الإفتراضي، وكان من أهم نتائج تلك الخريطة أن تمكنت الخبرة الخاصة من رصد حركة الجريمة عبر الإنترنت ومعرفة تطوراتها في كافة مظاهرها وأشكالها، ولقد استفاد أهل الخبرة من رصد هذه الخريطة في التعرف على التهديدات التي تواجه الدول والأفراد[1]، كما يمكن أن يكون كذلك للشركات المتخصصة دور في هذا المجال، حيث أصبح سوق الإنترنت ينمو من8% إلى 10% سنويا، من خلال اعتمادها على مهندسين متخصصين في مجال التقنية[2].

ثانيا: المؤسسات التعليمية:

إنّ أقوى مظاهر الخبرة التي يمكن الإستعانة بها لمواجهة الجريمة في العالم الإفتراضي يمكن أن تكون من خلال المؤسسات التعليمية، فهذه الأخيرة تعد مصدر دعم متكامل لمؤسسات الدولة ككل، وهذه المؤسسات تعتمد منهج علمي غير تجاري هدفها تطوير العلم ليقضي على المشكلات القائمة، كما أن التفكير العلمي لا يمكن تجنبه في رصده للظاهرة الإنسانية، والإتجاه العالمي في رصد تطورات الجريمة عبر الإنترنت يتجه إلى المؤسسات التعليمية، فليس هناك أفضل من التقنيين في المعلوماتية لفك شر الجريمة عبر الإنترنت[3].

---

[1]–د.طارق فوزي الفقي، المرجع السابق، ص 172.

[2]- Veronique Guillermard, la lutte contre la cybercriminalité est un marché d'avenir, le 06/03/2014, disponible à l'adresse suivante : www.lefigaro.fr

[3]– د.طارق فوزي الفقي، المرجع السابق، ص 174.

ثالثا: جهات الضبط القضائي:

شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الإجرام عبر الإنترنت، من بينها الولايات المتحدة الأمريكية التي تجاوز نشاطها في هذا المجال الإطار الدولي الممثل في الإنتربول، وكان آخر نشاط مؤسسي في هذا الإطار هو ذلك الفرع الجديد الذي تأسس في المباحث الفيدرالية الأمريكية FBI أطلِق عليه المعمل الإقليمي الشرعي للحاسوب غرضه مكافحة الجريمة عبر الإنترنت[1].

رابعا: دور المجني عليه:

إذا كانت الإتجاهات الحديثة في القانون الجنائي تبنى على دراسات تتعلق بالبحث في دور المجني عليه في الجريمة ذاتها، فإنّ مثل هذا الإتجاه يجد مغزاه عبر الإنترنت، حيث أنّ المجني عليه في هذه النوعية من الجرائم كثيرا ما يلجأ إلى اتخاذ دور سلبي حماية لمصالحه التي تتعلق بصفة خاصة بسمعته إذا كان له صفة تجارية كما لو كان مصرفا أو محلا تجاريا.

أضف إلى ذلك أنّ المجني عليه إذا كان شخصا طبيعيا في دولة لم تتخذ الخطوات الجادة نحو تقنين الإنترنت والحاسوب، فإنّ سلوك الضبط القضائي فيها قد يجعل من المستحيل إقامة ذلك التوازن بين العدالة الجنائية وبين المجني عليه، لذلك لا يوجد مانع من التقرير بأهمية دور المجني عليه في الدخول ميدان الخبرة هنا، خاصة في النواحي الفنية، حيث أنّ هناك نوعية من المجني عليه (صغار السن) يمثلون المستقبل بالضرورة، وعلماء التقنية متفقون على أن الإنترنت هي تقنية المستقبل، فالمسألة فيها توازن كبير من هذه الزاوية[2].

خامسا: التعاون الدولي:

قد يكون مفيدا في هذا الإطار التعرض لمنطق التعاون الدولي في مجال الخبرة التقنية، ويثور حينها إشكال يتعلق بمدى جواز انتداب الخبير المعلوماتي الأجنبي؟ فقد تواجه سلطات الإستدلال والتحقيق أثناء التحقيق في الجرائم الإلكترونية بعض المشاكل الفنية التقنية التي تستلزم معالجتها الإستعانة بخبير معلوماتي ذو تخصص دقيق وخاص، وقد لا تتوفر مثل هذه النوعية من الخبرة فيمن يحملون جنسية الدولة.

وفي الإجابة على هذا التساؤل، فإنّ الدولة قد اختلفت في معالجتها لهذه المسألة، فبعض الدول تجد في الإستعانة بخبير أجنبي مصدر تهديد وخطر على سيادتها وأمنها، خصوصا بالنسبة للجرائم الإلكترونية الواقعة على أمنها الداخلي أو الخارجي، فيما لا تجدها دول أخرى كذلك[3].

---

[1]– د.حسين بن سعيد الغافري، المرجع السابق، ص 567.

[2]– د.عمر محمد بن يونس، الدليل الرقمي، المرجع السابق، ص 118.

[3]– أ.رشاد خالد عمر، المرجع السابق، ص 166.

فيلاحظ أنّ المشرع الجزائري اشترط صراحة أن يكون الشخص متمتعا بالجنسية الجزائرية لكي يكون بمقدوره تسجيل إسمه في جدول الخبراء ولكي يمكن من تم انتدابه، إلاّ أنّ الفقرة الثالثة من المادة (144)[1] من قانون الإجراءات الجزائية أجازت للجهات القضائية بصفة استثنائية أن تختار بقرار مسبب خبراء غير مقيدين في الجداول ولكن بشرط أدائهم اليمين القانونية طبقا للفقرة الثالثة من المادة (145)[2] من قانون الإجراءات الجزائية، وبناءا على ذلك أرى أنه لا مانع بالنسبة للقانون الجزائري من انتداب خبير أجنبي.

فبالرجوع إلى المرسوم التنفيذي رقم (95-310) نجده يشترط الجنسية الجزائرية مع إضافة عبارة (مع مراعاة الإتفاقيات الدولية)، فيمكن عندها الإستعانة بالخبير الأجنبي الذي قد يكون شخصا طبيعيا، كما وأنّه قد يكون شخصا معنويا كالمراكز والهيئات والمؤسسات الحكومية وغير الحكومية التي يتم انتدابها وفق اتفاقيات تبرم بينها وبين السلطة المختصة في الدولة المنتدبة، إلا أنه ينبغي ضرورة تقييد هذا الجواز بعدم تأثير ذلك على الأمن الداخلي أو الخارجي للدولة، لما في مثل هذا الندب من خطر في كثير من الأحيان على المعلومات والوثائق الوطنية، فإذا تم التحقق من هذا القيد، فيمكن عندها الإستعانة بالخبير الأجنبي[3].

الفرع الثالث: أهم المسائل التي يستعان فيها بالخبير في مجال الحاسوب والإنترنت.

إنّ البحث عن المعلومات داخل جهاز الحاسوب والتنقيب عنها داخل شبكة الإنترنت أمر بالغ التعقيد ويحتاج إلى وجود خبير في هذا المجال، كما أنّ هناك مسألة يكون فيها الإستعانة بالخبرة التقنية غاية في الأهمية، ومن تلك المسائل ما يلي:

أولا: يستعان بالخبرة في مجال الحاسوب والإنترنت لوصف[4]:

1- تركيب الحواسيب وصناعتها وطرازها ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها، بالإضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور ونظام التشفير.

---

[1] – تنص المادة 144 فقرة 3 من قانون الإجراءات الجزائية الجزائري على ما يلي:" ... ويجوز للجهات القضائية بصفة استثنائية أن تختار بقرار مسبب خبراء ليسوا مقيدين في أي من هذه الجداول ."

[2]–تنص المادة 145 فقرة 3 من قانون الإجراءات الجزائية الجزائري على ما يلي:" ... ويؤدي الخبير الذي يختار من خارج الجدول قبل مباشرة مهمته اليمين السابق بيانها أمام قاضي التحقيق أو القاضي المعين من الجهة القضائية ...".

[3]– أ.رشاد خالد عمر، المرجع السابق، ص 167.

[4]–د. أحمد محمود مصطفى، المرجع السابق، ص 153.

2- طبيعة بيئة الحاسوب أو الشبكة، من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائط الإتصالات وتردد موجات البث وأمكنة اختراقها.

3- الموضع المحتمل لأدلة الإثبات والشكل أو الهيئة التي تكون عليها.

4- أثر التحقيق من الوجهة الإقتصادية والمالية على المشاركة في استخدام هذا النظام.

ثانيا: كما يستعان بالخبرة في مجال الحاسوب والإنترنت لبيان[1]:

1- كيف يمكن عند الإقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة المشتركة في هذا النظام.

2- كيف يمكن عند الإقتضاء نقل أدلة الإثبات على أوعية ملائمة من غير أن يلحقها تلف.

3- كيفية تجسيد الأدلة صورة مادية بنقلها إذا أمكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع إثبات أنّ ما هو موجود على الورق مطابق للمسجل على الحاسوب أو الشبكة أو الدعائم الممغنطة.

الفرع الرابع: أساليب عمل الخبير التقني.

يقوم الخبير التقني في سبيل تحري الحقيقة الإستعانة بكل ما يمكنه من التوصل إليها، وهو في إطار القيام بعمله قد يستخدم العديد من الأدوات والبرمجيات التي تمكنه من الحصول على الدليل الإلكتروني، كما يقوم بفحص الأجهزة الرقمية المتعلقة بالجريمة، ولذلك يجب على الخبير المعلوماتي أن يكون قادرا على القيام بالمهام التالية:

أولا: حجز البيانات:

هناك مبدأ شهير في مجال المعلوماتية يعرف باسم "مبدأ لوكارد التبادلي"، ويقصد به أنّ أي شخص يدخل إلى مسرح الجريمة يجب أن يأخذ منه شيئا، وأن يترك خلفه شيئا ما، فمثلا إذا أرسل شخص رسالة إلكترونية تحمل مضمونا احتياليا إلى أحد الأشخاص، فإنّ هذه الرسالة سوف تخزن لدى مزود خدمة الإنترنت مع التاريخ والوقت، إضافة إلى مسار الرسالة وعنوان رقم النفاذ، لذلك يجب على الخبير المعلوماتي أن يقوم في بادئ الأمر بعملية حجز للبيانات المتعلقة بالجريمة الموجودة لدى مزود الخدمة، إضافة إلى حجز الأجهزة التي تحوي هذه البيانات والتي تكون بحيازة المشتبه به وفي مسرح الجريمة.

[1]- د.أحمد محمود مصطفى، المرجع السابق، ص153.

ثانيا: حفظ البيانات:

يقوم الخبير المعلوماتي في هذه المرحلة بنسخ البيانات التي تم حجزها، بحيث يصبح لديه منها نسختين: النسخة الأولى يتم تخزينها في الأجهزة الرقمية التي تم حجزها، بحيث تبقى محفوظة بشكل جيد، والثانية عبارة عن نسخة طبق الأصل يتم إجراء عملية الإختبار أو الفحص عليها[1].

وتتم عملية حفظ الأدلة داخل الحاسب بأساليب متعددة تتشكل في أبسط مظاهرها باستخدام أسلوب الحفظ العادي، وأقوى مظاهرها في عمليات حجز الحاسب على الدليل الموضوع فيه، ذلك أنّ الدليل الإلكتروني هو في العادة ملف يحتوي على بيانات رقمية تعطي مظهرا معلوماتيا محددا غير قابل للتحويل إلى مظهر آخر، فمثلا إذا كانت الجريمة من جرائم النشر عبر الإنترنت فقد يكتفي بمجرد اللجوء إلى ذاكرة الحاسوب المستخدم دون الحاجة إلى تحديد الخادم، ففي مثل هذه الحالات يقوم الخبير باستخدام برمجيات مساعدة للتوصل إلى القيام بالحفظ في العالم الرقمي، مثلما هو الحال في حجز وتشفير مثل هذه المواقع بعد تحديد جدليتها ووقتها ومسارها، وهذا أمر يترتب عليه عدم إمكانية حذفها في العالم الرقمي، وإذا قام أحدهم بذلك فإنه يكون قد ارتكب جريمة[2].

ثالثا: إستعادة البيانات:

يجب على الخبير المعلوماتي أن يستعيد البيانات المحذوفة، وهو أمر ضروري من أجل إعادة بناء القضية، فيمكن للخبير أن يستعيد جميع الوسائل التي قام الجاني بحذفها عن طريق تتبع الأثر الذي تتركه هذه الرسائل على جهاز التخزين.

رابعا: تحليل البيانات:

في هذه المرحلة يقوم الخبير المعلوماتي بعملية تقييم لمحتوى البيانات الرقمية، بحيث يفحصها بدقة من أجل تحديد وسائل الجريمة ودوافعها والغرض منها.

خامسا: إعادة بناء القضية:

ويقصد بإعادة بناء القضية، العملية التي يقوم بها الخبير بعد تجميع وتحليل البيانات والمعلومات التي تم الحصول عليها نتيجة البحث، فالدليل الإلكتروني الذي تم الحصول عليه يحتوي على آثار سلوكية

---

[1]- د.محمد طارق عبد الرؤوف الخن، المرجع السابق، ص178.

[2]- د.محمد عمر بن يونس، الدليل الرقمي، المرجع السابق، ص124.

للمجرم مثل الكلمات التي استخدمها المجرم في تصفح الإنترنت، والمواقع التي قام بتصفحها على الشبكة، فالربط بين هذه السلوكيات تؤدي إلى معرفة مكان ووقت ارتكاب الجريمة والطريقة التي تمت بها[1].

كما يتم تحويل الدليل الإلكتروني إلى هيئة مادية وذلك عن طريق طباعة الملفات أو تصوير محتواها إذا كانت صور أو نصوص أو وضعها في أي وعاء آخر حسب نوع البيانات والمعلومات المكونة للدليل.

سادسا: تحديد مدى الترابط بين الدليل المادي والدليل الإلكتروني:

في هذه المرحلة يتم فحص كل من الدليل المادي المضبوط والدليل الإلكتروني في شكله المادي ومن تم الربط بينهما، مما يكسب الدليل الموثوقية واليقينية اللتان تؤديان إلى قبوله لدى جهات التحقيق والحكم[2].

سابعا: مرحلة تدوين النتائج وإعداد التقرير:

يتضمن تقرير الخبرة النتائج التي توصل إليها الخبير من خلال عملية البحث ويجب أن يتضمن التقرير ما يلي:مواصفات مسرح الجريمة الإفتراضية، ملخص عن عملية الفحص التي تم القيام بها، إعادة أحداث القضية وأن يكون التقرير متسلسلا من حيث الأحداث، وأن يكون مختصرا من الناحية التقنية ومكتوب بأسلوب واضح وبسيط حتى تتمكن المحكمة من فهمه بسهولة[3]،وإذا تعدد الخبراء واختلفوا في الرأي أو كانت لهم تحفظات في شأن النتائج المشتركة، سجل كل واحد منهم رأيه أو تحفظاته مع تعليل وجهة نظره، وذلك احتراما للنزاهة العلمية لكل واحد منهم، ويودع التقرير والأحراز لدى كاتب الجهة القضائية التي أمرت بالخبرة، ويثبت هذا الإيداع بمحضر طبقا للمادة (153)[4] من قانون الإجراءات الجزائية الجزائري.

وفيما يتعلق بمسألة رد الخبير من طرف الخصوم أمام القضاء الجزائي، فلم يتضمن قانون الإجراءات الجزائية ذلك، غير أنه في المقابل من خلال نص المادة (154)[5]من نفس القانون يتبين أن المشرع قد سمح

---

[1]– د.محمد طارق عبد الرؤوف الخن، المرجع السابق، ص334.

[2]– أ.عائشة بن قارة،، المرجع السابق، ص 149.

[3]– د.طارق عبد الرؤوف الخن، المرجع السابق، ص 336.

[4]–تنص المادة 153 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يحرر الخبراء لدى انتهاء أعمال الخبرة تقريرا يجب أن يشتمل على وصف ما قاموا به من أعمال و نتائجها وعلى الخبراء أن يشهدوا بقيامهم شخصيا بمباشرة هذه الأعمال التي عهد إليهم باتخاذها ويوقعوا على تقريرهم .

فإذا اختلفوا في الرأي أو كانت لهم تحفظات في شأن النتائج المشتركة عين كل منهم رأيه أو تحفظاته مع تعليل وجهة نظره.

ويودع التقرير و الأحراز أو ما تبقى منها لدى كاتب الجهة اقضائية التي أمرت بالخبرة ويثبت هذا الإيداع بمحضر ."

[5] –تنص المادة 154(القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري)على ما يلي:" على قاضي التحقيق أن يستدعي من يعنيهم الأمر من أطراف الخصومة ويحيطهم علما بما انتهى إليه الخبراء من نتائج وذلك بالأوضاع المنصوص عليها في المادتين 105 و106، ويتلقى أقوالهم بشأنها ويحدد لهم أجلا لإبداء ملاحظاتهم عنها أو تقديم طلبات خلاله ولا سيما فيما يخص إجراء أعمال خبرة تكميلية أو القيام بخبرة مضادة...".

للأطراف بإبداء ملاحظاتهم وطلباتهم بشأن الخبرة، فيمكن عندئذ للمعني بالأمر أن يلتمس رد الخبير إذا كانت هناك أسباب تدعو لذلك .

أمّا إذا رأت المحكمة نقصا في تقرير الخبرة، أو كانت فيه مسائل معينة تحتاج إلى إيضاح من الخبير، يمكن استدعاء الخبراء لجلسة المحاكمة، ويعرضون نتيجة أعمالهم الفنية بعد أن يحلفوا اليمين، ويسوغ لهم أثناء سماع أقوالهم أن يراجعوا تقريرهم[1] طبقا لنص المادة (155)[2] من قانون الإجراءات الجزائية الجزائري.

غير أنّ الفقه يرى ضرورة حضور الخبير بالنسبة لهذه النوعية من القضايا، نظرا لأنّ الموضوع تقني خصوصا في الجانب التحليلي من التقرير الذي يحتوي على مصطلحات جديدة، لذلك من المفيد جدا عقد دورات تكوينية للقضاة والمحامين من أجل تدارك هذا النقص وتمكين رجال القانون من الفهم الجيد لتقارير الخبراء التقنيين.

الفرع الخامس: القيود التي ترد على عمل الخبير التقني.

يرتبط عمل الخبير في مجال الجرائم الإلكترونية بالمشروعية، فليس له أن يلجأ إلى أساليب غير مشروعة من أجل إنجاز المهمة المكلف بها، وفي هذا المقام يثور تساؤل حول مدى جواز الإستعانة بخبرة المجرم المعلوماتي؟

وفي الإجابة عن هذا التساؤل، ينبغي الإشارة بداية إلى أنّ كبرى الشركات الأمريكية قد دعت في سنة 1999إلى التعاقد مع الهكرة تجنبا لاختراقاتهم، إلاّ أنّ مدى قبول ذلك أو عدم قبوله يظل دوما للقضاء في مدى تقبل دليل مستمد من استعانة الخبير بهكرة، ومن تم فإنه على الرغم من استعانة الخبير بمجرم معلوماتي للتعرف على أسلوب ارتكاب الجريمة الإلكترونية لا يجعل منه خبيرا في الدعوى، إذ أن الأمر مرجعه للخبير ثم لقاضي الموضوع وما ذلك المجرم إلاّ مساعد للخبير، وفي ذلك سابقة للكونجرس الأمريكي من استدعاء أحد كبار الهكرة للإدلاء بشهادته أمامه[3]، فللخبير أن يطلب مساعدة من يشاء في هذا الإطار، وإن كان ذلك يتم في الغالب بشكل سري[4].

---

[1]– أ. نجيمي جمال، المرجع السابق، ص 244.

[2]– تنص المادة 155 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يعرض الخبراء في الجلسة عند طلب مثولهم بها نتيجة أعمالهم الفنية التي باشروها بعد أن يحلفوا اليمين، على أن يقوموا بعرض نتائج أبحاثهم ومعايناتهم بذمة وشرف ويسوغ لهم أثناء سماع أقوالهم أن يراجعوا تقريرهم ومرفقاته ...".

[3]–د.طارق فوزي الفقي، المرجع السابق، ص 180.

[4]–د.حسين الغافري، المرجع السابق، ص 571.

وبالرجوع إلى القانون الجزائري، أجد أنّ المرسوم التنفيذي رقم (95-310) يشترط في مادته الرابعة ألاّ يكون الخبير قد تعرض لعقوبة نهائية بسبب ارتكابه وقائع مخلة بالآداب العامة أو الشرف، والهاكر قد يكون ارتكب جريمة إلكترونية من ضمن الجرائم الماسة بالشرف وقد صدر بحقه حكم قضائي بذلك،فحسب نص المادة لا يجوز الإستعانة بخبرته مادام لا يتوفر فيه شرط حسن السيرة والنزاهة.

وباستقراء نص المادة (25) من قانون العقوبات المصري قد قضت بعدم جواز إناطة مهمة الخبير قطعا للشخص الذي سبق وأن حكم عليه بعقوبة أشغال شاقة عن جناية، كما اشترط وبالنص الصريح ألاّ يكون من يعين في وظائف الخبرة من المحكومين عليهم سابقا سواء من المحاكم أو من مجالس التأديب عن أمر مخل بالشرف، وأن يكون محمود السيرة وحسن السمعة وهذا طبقا للمادة (18) من قانون تنظيم الخبرة أمام جهات القضاء المصري[1].

المطلب السادس: التسرب.

لقد منحت التعديلات الجديدة لقانون الإجراءات الجزائية المتضمنة بالقانون رقم (06-22) السالف الذكر لقاضي التحقيق صلاحيات جديدة لم يكن يتمتع بها من قبل، وذلك لمواجهة أنواع معينة من الجرائم نظرا لخطورتها ولطبيعتها الخاصة، وهذه الصلاحيات تتمثل في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وكذلك الإذن بإجراء عملية التسرب لأجل مراقبة الأشخاص بإيهامهم من طرف الشخص المتسرب بأنه فاعل معهم أو شريك لهم أو خاف لمتحصلات الجريمة، وذلك متى كانت الوقائع المحقق فيها متعلقة بجرائم المخدرات أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو الجريمة المنظمة أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالصرف، وكذا جرائم الفساد.

وسيتم التطرق إلى تعريف عملية التسرب والضمانات القانونية لهذه العملية، وذلك على النحو التالي:

[1]- أ.رشاد خالد عمر، المرجع السابق، ص170.

الفرع الأول: تعريف عملية التسرب.

يعرف التسرب بأنه: قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.[1]

ويمكن تجسيد عملية التسرب في الجرائم الإلكترونية بإشراك ضابط أو عون الشرطة القضائية في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال أو كلام يقوم حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة ويظهر بمظهر طبيعي كما لو كان فاعل معهم، ويحاول الإستفادة من معرفتهم حول كيفية اقتحام الهاكر لموقع ما أو مباشرة الحديث في الموضوع الجنسي حتى يتمكنوا من اكتشاف وضبط الجرائم التي تتم من خلالها كالدعوة للدعارة مثلا[2].

الفرع الثاني: ضمانات عملية التسرب.

وتتمثل هذه الضمانات فيما يلي[3]:

- إنّ التسرب لا يكون إلا بإذن قضائي سواء من وكيل الجمهورية أو قاضي التحقيق وتتم العملية تحت مراقبته، أي هو الذي يقدّر ما إذا كان الأمر يستدعي اللجوء إلى التسرب حتى لا تكون هناك تجاوزات وحتى يتمكن من وضع حد لها في أي وقت إذا تطلبت خطورة الوضع ذلك[4].
- يجب أن يكون الإذن القضائي الصادر عن وكيل الجمهورية أو من قاضي التحقيق مكتوبا ومسببا تحت طائلة البطلان، وينبغي أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته[5].
- ينبغي أن يحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (04) أشهر على أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية، كما يمكن للقاضي

---

[1]– هذا التعريف مأخوذ من نص المادة 65 مكرر12 فقرة 1 من قانون الإجراءات الجزائية الجزائري.

[2]– أ.عائشة بن قارة، المرجع السابق، ص120.

[3]– أ. نجيمي جمال، المرجع السابق، ص452.

[4] – تنص المادة 65 مكرر 11(القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري)على ما يلي: " عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه ".

[5]– تنص المادة 65 مكرر 15 فقرة 2/1(القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري)على ما يلي: "يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11 أعلاه، مكتوبا ومسببا وذلك تحت طائلة البطلان.

تذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته ...".

الذي رخص بإجرائها أن يأمر بوقفها حتى قبل انقضاء المدة، وقد يكون ذلك حماية للضابط أو العون المتسرب، كما تودع الرخصة في ملف الإجراءات وذلك بعد الإنتهاء من عملية التسرب[1].

- يمنع إظهار الهوية الحقيقية لضباط وأعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة وذلك في أي مرحلة من مراحل الإجراءات، وفي حالة المخالفة رتب المشرع الجزائري على ذلك عقوبات جزائية.[2]
- يجوز سماع ضابط الشرطة القضائية التي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهد عن العملية وهذا طبقا لنص المادة (65 مكرر 18)[3]من قانون الإجراءات الجزائية، معنى ذلك أنه لا يجوز سماع الضابط أو العون الذي قام بعملية التسرب فعليا، وإن كان هذا الأمر يناقض القواعد العامة للشهادة التي تقضي بضرورة حضور الشاهد شخصيا للإدلاء بشهادته أمام المحكمة.
- يمتد اختصاص ضابط الشرطة القضائية إلى كامل الإقليم الوطني إذا تعلق الأمر بجرائم معينة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ويعمل هؤلاء تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا، ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات وهذا طبقا لنص المادة (16)[4] من قانون الإجراءات الجزائية.

---

[1] – تنص المادة 65 مكرر 15 فقرة 4/3 من قانون الإجراءات الجزائية الجزائري على ما يلي: " ... ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر.
يمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية...".

[2] – تنص المادة 65 مكرر 16 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري) على ما يلي: " لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات.
يعاقب كل من يكشف هوية ضابط أو أعوان الشرطة القضائية بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 200.000 دج.
وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس (5) إلى عشر(10) سنوات والغرامة من 200.000 دج إلى 500.000 دج.
وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من عشر (10) سنوات إلى عشرين(20) سنة والغرامة من 500.000 دج إلى 1000.000 دج ...".

[3] – تنص المادة 65 مكرر 18 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري) على ما يلي:" يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية."

[4] – تنص المادة 16(القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري)على ما يلي:" ... غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني.
ويعمل هؤلاء تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات."

وإذا كانت القواعد العامة في الإثبات الجنائي تستوجب النزاهة والشرعية في الحصول على الدليل وترفض أي دليل ناجم عن تحريض الضبطية القضائية للمتهم على ارتكاب الجرائم، إلاّ أنّ التسرب يسمح لرجل السلطة بالقيام ببعض الأفعال الإيجابية التي تشكل جريمة في الظروف العادية، دون أن يكون مسؤولا جزائيا، وهذه الأفعال تتمثل فيما يلي: إقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها، استعمال أو وضع تحت تصرف مرتكبي الجرائم وسائل ذات الطابع القانوني أو المالي وكذلك وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الإتصال[1]، وهذا طبقا لنص المادة (65 مكرر 14)، والمشرع الجزائري لم يضع إلاّ قيدا واحدا لضابط أو عون الشرطة القضائية وهو ألا تشكل الأفعال تحريضا على ارتكاب الجرائم طبقا للمادة (65 مكرر 12 ف 2)[2] من قانون الإجراءات الجزائية الجزائري.

غير أنه من الملاحظ أنّ الإجراءات العامة لجمع الدليل الإلكتروني، وإن كان لها دور مهم في تحديد مرتكبي هذه الجرائم وإثباتها، إلاّ أنها لا تتلائم مع طبيعة الجرائم الإلكترونية، لذلك كان لابد من إيجاد طرق أخرى أكثر حداثة، لأن الإجراءات التقليدية قد تصبح عاجزة عن إثبات هذه النوعية من الجرائم ولا تحقق الهدف المنشود من وراء جمع الأدلة، ومن أجل توضيح هذه الإجراءات الخاصة سيتم التطرق إليها بالتفصيل من خلال هذا المبحث.

المبحث الثاني: الإجراءات الخاصة لجمع الدليل الإلكتروني.

في مقابل الإجراءات العامة لجمع الدليل عموما هناك إجراءات أخرى خاصة بجمع الدليل الإلكتروني، وقد تم استخدام مصطلح الإجراءات الخاصة أي أنها خاصة بالجريمة الإلكترونية، فالتقدم العلمي الكبير الذي تحقق في وسائل الإثبات الجنائي وما نتج عنه من وسائل علمية حديثة استطاعت أن تتغلب على كل محاولات المتهم لتضليل العدالة، فالمجرم لا يترك وسيلة إلاّ ويستعين بها من أجل أداء أفضل للمشروع الإجرامي، فهو يستعين بجميع معطيات العلوم الحديثة، لذلك فالأمر يتطلب من رجال الأمن والقانون أن يتصدوا للجريمة بالبحث العلمي والوسائل العلمية الحديثة التي توصل إليها العقل البشري من أجل مقاومة التيار الإجرامي[3]،

---

[1]–أ. نجيمي جمال، المرجع السابق، ص 451.

[2] – تنص المادة 65 مكرر 12 فقرة 2 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري)على ما يلي: "... ولا يجوز، تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على ارتكاب جرائم ."

[3]– د. محمد أمين الخرشة، المرجع السابق، ص 31.

غير أنه ينبغي أن تكون هناك موازنة بين الكشف عن الحقيقة القضائية وحماية الحياة الخاصة للأفراد، وذلك مادام أن الوسائل العلمية الحديثة أصبحت هي الأخرى تنتهك خصوصيات الأفراد، لذلك فإن استخدامها يجب أن يكون وفق ضوابط معينة.

ويمكن تقسيم الإجراءات الخاصة لجمع الأدلة الإلكترونية إلى ثلاثة أقسام : إجراءات جمع البيانات الإلكترونية المخزنة (المطلب الأول)، ومراقبة الإتصالات الإلكترونية في حينها (المطلب الثاني)، واعتراض الإتصالات السلكية واللاسلكية (المطلب الثالث).

المطلب الأول: إجراءات جمع البيانات الإلكترونية المخزنة.

نظرا للطبيعة الخاصة للجرائم الإلكترونية ، أصبحت الإجراءات التقليدية عاجزة و غير كفيلة لجمع الدليل الإلكتروني، و إنما يتعين الإستعانة بأساليب و تقنيات حديثة تتناسب مع هذه الطبيعة الخاصة، وسيتم التطرق لهذه الإجراءات في الفروع التالية :

الفرع الأول: التحفظ السريع على محتوى البيانات المخزنة.

تتمثل إجراءات التحفظ السريع على مضمون البيانات المخزنة في النظام المعلوماتي، عندما تكون هناك أسباب تدعو للإعتقاد بأن هذه البيانات تكون معرضة للإتلاف أو التعديل، وذلك لفترة زمنية محددة حماية لحق الأفراد في الخصوصية[1].

وقد نصت المادة (16) من الإتفاقية على أنّه يجب على كل دولة طرف أن تتبنى الإجراءات التشريعية وأية إجراءات أخرى ترى أنها ضرورية لتخويل سلطاتها المختصة أن تأمر بالتحفظ العاجل على البيانات المخزنة، ولا شك أنّ الغرض من ذلك هو تمكين السلطة المختصة بالتحقيق في جرائم الكمبيوتر والإنترنت من معرفة مضمون البيانات التي أرسلها المشترك أو استقبلها، سواء عن طريق طلبها من مقدمي الخدمة أو خلال القيام بالتفتيش.

وعلى ذلك فإنّ الأمر الذي تصدره السلطة المختصة في الدولة يلتزم بمقتضاه مقدمي الخدمة بالحفاظ على البيانات وحمايتها من الضياع أو التعديل أو المحو، وبالحفاظ على سريتها ومنع الغير من الحصول أو الوصول إليها، وتختلف مدة التحفظ على البيانات من تشريع لآخر، وإن كانت الإتفاقية قد حددتها بمدة لا

[1]-Bertrand Warusfel, Procédure pénale et technologies de l'information (de la convention sur la cyber criminalité – à la loi sur la sécurité quotidienne), Revue droit et défense, N°1, 2002, p 03.

تتجاوز 90 يوما طبقا لنص المادة (16 فقرة 3) من الإتفاقية، ويختص بإصدار أمر التحفظ السلطة التي يحددها التشريع الداخلي لكل دولة[1].

وتجدر الإشارة إلى أنّ اتخاذ مثل هذا الإجراء له أهمية كبيرة في مجال التحقيق في الجرائم الإلكترونية،لأنّ البيانات الإلكترونية المخزنة لدى مزود خدمات الإتصالات الإلكترونية غالبا ما تتم إزالتها ومحوها فوريا، وذلك احتراما لحرمة الحياة الخاصة[2].

الفرع الثاني: التحفظ السريع على البيانات المتعلقة بخط سير البيانات.

يقصد بالتحفظ على البيانات المتعلقة بخط سير البيانات إلزام مقدمي الخدمات من أفراد أو شركات بالحفاظ على البيانات والمعلومات المخزنة في مصدر الإتصالات ووقتها ومقدمي الخدمة الذين ساهموا في نقل البيانات، ويرجع السبب في اتخاذ هذا الإجراء في أنه يسهم في التعرف على مرتكبي الجرائم الإلكترونية والمساهمين معهم، إلاّ أنّ تنفيذ هذا الإجراء يتطلب سعة تخزين كبيرة، وغالبا ما يتم تحديد مراقبة خط سير بيانات معينة للسلطات المتخصصة بالتحري عنها ومتابعة أصحابها.

وقد عرّفت المادة الأولى (01 فقرة د)[3] من إتفاقية بودابست بشأن الجرائم الإلكترونية هذا النوع من البيانات بأنها صنف من بيانات الحاسوب التي تشكل محلا لنظام قانوني محدد، حيث يتم توالد هذه المعطيات من الحواسيب عبر تسلسل حركة الإتصالات لتحديد مسلك الإتصالات من مصدرها إلى الجهة المقصودة، وهي بذلك تشمل طائفة من المعطيات تتمثل في مصدر الإتصال ووجهته المقصودة، وخط السير ووقت أو زمن الإتصال، حجم الإتصال ومدته ونوع الخدمة المؤداة.

ويختلف إجراء التحفظ على البيانات المتعلقة بخط سير البيانات عن التحفظ السريع على مضمون البيانات الذي نصت عليه المادة (01/16)من الإتفاقية، في أنّ التحفظ يقتصر على البيانات المتعلقة بالإتصال من حيث مصدرها ووقتها ومرسلها ومستقبلها ومن ساهم في نقلها، ولا يشمل محتوى البيانات وما تتضمنه من معلومات، وهذا الإجراء كسابقه يحتاج إلى تقنية عالية تساعد مقدم الخدمة في القيام به في وقت سريع بغية إعطاء السلطة المختصة فرصة اتخاذ الإجراء اللازم لكشف مرتكب الجريمة وضبط أدلتها، وقد

---

[1]– د.رامي متولي القاضي، مكافحة الجرائم المعلوماتية، المرجع السابق، ص126.

[2]– د. شيماء عبد الغني، المرجع السابق، ص 228.

[3] -Article 1/D du C.C.C : «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent.

نصت المادة (01/17)[1] من الإتفاقية الأوروبية على ضرورة تبني الدولة تشريعات تكفل قيام مستخدمي الخدمات بالتحفظ السريع على البيانات المتعلقة بخط سير البيانات، وعلى ضرورة أن تتبنى الدول الإجراءات التي تتضمن قيام مقدم الخدمة بالإفشاء السريع لتلك البيانات للسلطة المختصة[2].

وبالرجوع إلى القانون الجزائري رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، فقد عرّف المعطيات المتعلقة بحركة السير في مادته (02 فقرة هـ) بأنها : " أي معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حركة الإتصال، توضح مصدر الإتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة".

وقد خصص الفصل الرابع من هذا القانون تحت عنوان "إلتزامات مقدمي الخدمات"، ونصت المادة (11) منه[3] على التزام حفظ المعطيات المتعلقة بحركة السير،ويلتزم مقدمو خدمات الإنترنت بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال، الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال، المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، وكذلك المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم،الإتصال، وكذا عناوين المواقع المطلع عليها، كما حدد المشرع الجزائري مدة حفظ المعطيات المذكورة بسنة واحدة ابتداء من تاريخ التسجيل.

---

[1]-Article 17/1 du C.C.C :
Afin d'assurer la conservation des données relatives au trafic en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour:
a. veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de service aient participé à la transmission de cette communication; et
b. assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité de données relatives au trafic suffisante pour permettre l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise.

[2]– د.وليد نبيه طه، الجرائم الإلكترونية طبقا لاتفاقية بودابست، بحث مقدم لندوة الواقع الأمني، مركز بحوث الشرطة بأكاديمية الشرطة، القاهرة، مصر، سنة 2011، ص26.نقلا عن: د. رامي متولي قاضي، المرجع السابق، ص 127.

[3] – تنص المادة (11) من القانون رقم (09-04) السالف الذكر على ما يلي:" مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ :

أ– المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ب– المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال .

ج– الخصائص التقنية و كذا تاريخ ووقت ومدة كل إتصال .

د– المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها .

هـ– المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم، الإتصال و كذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الإتصال وتحديد مكانه تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداءا من تاريخ التسجيل".

ورتب المشرع الجزائري ناهيك عن العقوبات الإدارية، مسؤولية جزائية للأشخاص الطبيعيين والمعنويين في حالة ما إذا شكلت أفعالهم عرقلة لحسن سير التحريات القضائية[1]، حيث رتب عقوبات قد تصل إلى خمس (05) سنوات وغرامة قد تصل إلى 500.000دج بالنسبة للشخص الطبيعي، أما الشخص المعنوي فيعاقب وفقا للقواعد المقررة في قانون العقوبات وهذا طبقا لنص المادة (11) من القانون السالف الذكر.

أمّا المشرع الفرنسي فقد نص على ضرورة حماية حرمة الحياة الخاصة في إطار تخزين المعطيات المتعلقة بالأفراد وذلك طبقا لنص المادة (L34-1 فقرة 02)[2] من قانون البريد والإتصالات الإلكترونية، كما قرر عقوبات أخرى في حالة عدم مسح المعطيات المخزنة وذلك بموجب المادة (L39-3 فقرة 02)[3]، إلا أنه يمكن الإحتفاظ بتلك المعطيات لمدة أقصاها سنة إذا استلزم التحقيق ذلك وهذا طبقا لنص المادة (L34-1 فقرة 03)[4].

[1]– تنص الفقرة الأخيرة من المادة 11 من القانون رقم 09-04 السالف الذكر بأنه : " ... دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الإلتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (06) أشهر إلى خمسة (05) سنوات وبغرامة من 50000 دينار جزائري إلى 500000 دينار جزائري.
يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات".

[2]- Article L34-1/2 (C.P.T.E Modifié par LOI n° 2013-1168 du 18 décembre 2013 - art. 24) : II.-Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI.

[3]- Article L39-3/I/1° (C.P.T.E Modifié par Loi n°2004-669 du 9 juillet 2004 - art. 19 JORF 10 juillet 2004) :I. - Est puni d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents :
1° De ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communications dans les cas où ces opérations sont prescrites par la loi;

[4]- Article L34-1/3 (C.P.T.E Modifié par LOI n° 2013-1168 du 18 décembre 2013 - art. 24) :III.-Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques.

هذا إلى جانب عقوبات أخرى على مزود الخدمات في حالة عدم حفظه للمعطيات التي ينبغي عليه تخزينها وذلك بموجب المادة (L39-3)[1].

أمّا فيما يتعلق بالتحفظ العاجل على بيانات الكمبيوتر المخزنة، فيجوز لأطراف هذه الإتفاقية الطلب من الأطراف الأخرى التحفظ العاجل على بيانات كمبيوتر يقع في إقليم الطرف الآخر، وقد بينت المادة (29)[2] من نفس الإتفاقية الإجراءات المتبعة، ويجوز للطرف الآخر اشتراط ازدواجية الجريمة، وله حق الرفض إذا ما تعلق الطلب يتعلق بجريمة سياسية أو أن تنفيذ الطلب يمس السيادة أو الأمن أو النظام العام، وفيما يتعلق بالدخول على بيانات الكمبيوتر في إقليم دولة أخرى، فيجوز الدخول عن طريق الموافقة أو إذا ما كانت متاحة علنا، وعلى الدول الأعضاء تعيين نقطة اتصال لضمان توافر المساعدة الفورية.

وينبغي الإشارة إلى أنّ الإتفاقية العربية لمكافحة جرائم تقنية المعلومات[3] قد تضمنت عدة أحكام إجرائية لتعزيز التعاون بين الدول العربية في مكافحة جرائم تقنية المعلومات، لتسهيل إجراءات جمع الأدلة والتحقيق في الجرائم الإلكترونية، غير أنّ أحكامها كانت مشابهة للإتفاقية الأوروبية[4].

---

[1]- Article L39-3/I/2° (C.P.T.E Modifié par Loi n°2004-669 du 9 juillet 2004 - art. 19 JORF 10 juillet 2004) :I. - Est puni d'un an d'emprisonnement et de 75000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents :
2° De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.

[2]- Article 29 du C.C.C : – Conservation rapide de données informatiques stockées
1. Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.
2. Une demande de conservation faite en application du paragraphe 1 doit préciser :
a. l'autorité qui demande la conservation ;
b. l'infraction faisant l'objet de l'enquête et un bref exposé des faits qui s'y rattachent ;
c. les données informatiques stockées à conserver et la nature de leur lien avec l'infraction ;
d. toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique ;
e. la nécessité de la mesure de conservation ; et
f. le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

[3]-حررت هذه الإتفاقية بمدينة القاهرة في جمهورية مصر العربية في 1432/01/15 هـ الموافق لـ 2010/12/21، حيث وافقا عليه مجلسا وزراء الداخلية و العدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية. أنظر في ذلك الموقع الإلكتروني:.www.arablegalnet .org

[4]- د. رامي متولي قاضي، المرجع السابق، ص 128.

فالملاحظ من خلال الإتفاقية العربية لمكافحة جرائم تقنية المعلومات أنها أفردت نصوصا خاصة متعلقة بإجراءات التحفظ العاجل على البيانات المخزنة المادة(23)[1]، التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين المادة (24)[2].

أما فيما يتعلق بأوامر تسليم المعلومات فقد نصت عليها في المادة (25)[3]، ناهيك عن إجراءات أخرى تلعب دورا في إجراءات جمع الأدلة تتمثل في التفتيش والضبط للمعلومات المخزنة المواد(26)[4] و(27)[5]، الجمع الفوري لمعلومات تتبع المستخدمين المادة (28)[6].

---

[1]– تنص المادة 23 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي : " –تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة، بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد،أن تلك المعلومات عرضة للفقدان أو التعديل .

–تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة و الموجودة بحيازته أو سيطرته،ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد ،من أجل تمكين السلطات المختصة من البحث والتقصي...".

[2]– تنص المادة 24 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي : "تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل:

أ. ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الإتصالات.

ب. ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات".

[3]– تنص المادة 25 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي : " تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى:

أ. أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات.

ب. أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته".

[4]– تنص المادة 26 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي : "– تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:

أ– تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها.

ب– بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه..."

[5]– تنص المادة 27 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي : "– تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة (1) من المادة السادسة والعشرين من هذه الاتفاقية.

هذه الإجراءات تشمل صلاحيات:

أ– ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات.

ب– عمل نسخة معلومات تقنية المعلومات والإحتفاظ بها.

ج– الحفاظ على سلامة معلومات تقنية المعلومات المخزنة.

د– إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها..."

[6]– تنص المادة 28 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي : "– تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من:

أ– جمع أو تسجيل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف.

الفرع الثالث: إصدار أمر بتقديم بيانات محددة.

يقصد بإصدار أمر بتقديم بيانات محددة تخويل السلطة المختصة بإصدار أمر إلى مقدم الخدمة أو أي شخص في حيازته أو تحت سيطرته بيانات معينة بتقديم تلك البيانات، سواء كانت هذه البيانات تتعلق بالمحتوى أو بخط السير، وهذا الإجراء كغيره من الإجراءات السابقة يصدر عن سلطة مختصة وينفذها أشخاص لا يتبعون هذه السلطة، فهم عبارة عن أشخاص في حيازتهم أو تحت سيطرتهم بيانات مخزنة داخل منظومة الكمبيوتر أو في دعامة تخزين المعلومات، بمعنى أنّ الأمر يصدر لصاحب الحيازة المادية للبيانات ولصاحب السيطرة ولو لم يحوزها حيازة مادية[1].

وقد نصت المادة (18)[2] من الإتفاقية الأوروبية على ضرورة أن تتبنى الدول تشريعات تلزم مقدم الخدمة وغيره من الأشخاص بتقديم بيانات معينة تكون في حيازتهم أو تحت سيطرتهم ومخزنة في منظومة الكمبيوتر أو دعامة التخزين، أما القانون الأمريكي المعروف بـ (ECPA) أجاز إطلاع رجال الضبط القضائي على البيانات الموجودة في حوزة مزودي الخدمات، ويشمل المعلومات الشخصية الخاصة بالمشترك مثل إسمه ورقم هاتفه وعنوانه، المعلومات الشخصية الخاصة بالمتعامل مع المشترك أي كل ما يتصل به أو يدخل معه في صفقة، وكذا المعلومات المتعلقة بمحتوى الملفات وتشمل مضمون المحادثات ومضمون الملفات، فالمشترك لا يتمتع بالحق في الخصوصية بالنسبة لهذه الأنواع الثلاثة من المعلومات[3].

وقد حددت الإتفاقية الأوروبية[4] المقصود بتلك البيانات بقولها أنها تتعلق بنوع خدمة الإتصال التي اشترك فيها الشخص والوسائل الفنية لتحقيقها ومدة الخدمة وشخصية المشترك ورقم دخوله للحصول على

ب- إلزام مزود الخدمة ضمن اختصاصه الفني بأن:

-يجمع أو يسجل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف .

-يتعاون ويساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تثبت بواسطة تقنية المعلومات...".

[1]- د.رامي متولي القاضي، مكافحة الجرائم المعلوماتية، المرجع السابق، ص128.

[2]- Article 18 du C.C.C : 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession où sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique; et

b. à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services… »

[3]- د.شيماء عبد الغني، المرجع السابق، ص216.

[4]- Article 18/3 du C.C.C : Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

تلك الخدمة والفواتير التي ترسل إليه وأي معلومات تتعلق بطريقة الدفع، أو أي معلومات أخرى تتعلق بأداء الخدمة أو بالإتفاق بين هذا المشترك ومزود الخدمة، كما عنيت الإتفاقية ذاتها بالقول أنّ تلك البيانات تشمل أي معلومات تختزن في الكمبيوتر أو في أي شكل آخر والتي تتواجد لدى مزود الخدمات وتتعلق بالمشترك في خدماته، فالإتفاقية لا تستلزم سبق الحصول على إذن قضائي للكشف عن هذه البيانات، وبناءا عليه يجوز للدول الأطراف أن تخول رجال الضبط القضائي لديها سلطة الإطلاع على تلك البيانات في إطار قيامهم بواجبهم في جمع الإستدلالات، ولكنها استثنت أية معلومات متعلقة بحركة ومحتوى البيانات[1].

ومادام أنّ مقدمي الخدمات هم الحائزين لهذه البيانات التي تم التطرق إليها، فسيتم تحديد المقصود بمقدمي الخدمات، ومدى التزامهم بالتعاون مع رجال الضبط القضائي، وذلك على النحو التالي:

البند الأول: تعريف مقدمي الخدمات.

عرّف القانون الجزائري رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها مقدمو الخدمات بأنهم : "أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها"[2].

وقد عرفته إتفاقية بودابست بشأن الجرائم الإلكترونية في المادة (1) فقرة (ج)[3] بأنه كل من يقوم بخدمات الإيصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات، وقد يكون جهة عامة أو جهة خاصة، وقد يقدم خدماته للجمهور أو لمجموعة من المستخدمين الذين يشكلون مجموعة مغلقة، كما أن مزود

---

a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;
c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service.

[1]–د. وليد نبيه طه، المرجع السابق، ص 28. نقلا عن : د. رامي متولي قاضي، المرجع السابق، ص 127.

[2] – طبقا لنص المادة 02 فقرة د من القانون رقم 09-04 السالف الذكر .

[3]- Article 1/C du C.C.C : «fournisseur de service» désigne :
i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;
ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs … ».

الخدمات هو من يقدم خدمته إلى الجمهور بوجه عام في مجال الإتصالات الإلكترونية[1]، كما يقسمون إلى أربعة فئات: موردي المعلومات، متعهدي الإيواء، موردي الدخول و القائم بالعمليات[2].

وقد يعرّف مزودو خدمات الإنترنت بأنهم أولئك الأشخاص الذي ينحصر دورهم في تمكين المستخدم للشبكة من الدخول إليها والتجول فيها والإطلاع على ما يريد، وما يسري على المعلومات في عملية وسطاء الإنترنت يسري كذلك على التجارة عبر الشبكة، وذلك لأنّ التجارة الإلكترونية هي الأخرى تعتمد على نظام معلوماتي عبر الإنترنت، وهذا النظام يشارك في إعداده وتشغيله وتنفيذه أشخاص كثيرون[3].

وفي هذا الإطار تمّ في الجزائر إصدار مرسوم تنفيذي رقم (98-257)[4]، وقد حددت المادة (14)[5] من هذا المرسوم إلتزامات مقدم خدمات الإنترنت خلال ممارسة نشاطاته، كما أنّ المرسوم التنفيذي رقم (02-141)[6] نصّ على عدة إلتزامات أخرى تخص مقدمي الخدمات، ومن بين هذه الإلتزامات أن يضمن مقدمو الخدمات عدم التميز في مجال تحديد تعريفة الخدمات المقدمة للجمهور وللمتعاملين ولمقدمي الخدمات الآخرين[7]،كما يلتزمون بنشر بيان مفصل لتعريفات الخدمات المقدمة للجمهور ويعرضونه في

---

[1]– د. شيماء عبد الغني، المرجع السابق، ص 209.

[2]–Régie Buchillet, La responsabilité des prestataires techniques de l'internet, mémoire DEA droit de l'économie, faculté de droit et de sciences politiques, Université de Bourgogne, France, 2002, p 06.

[3]– د. عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الإنترنت دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2006، ص76.

[4]– مرسوم تنفيذي رقم (98-257) مؤرخ في 03 جمادى الأولى عام 1419هـ الموافق ل 25 غشت سنة 1998، يضبط شروط وكيفيات إقامة خدمات الإنترنت واستغلالها.

[5]– تنص المادة 14 من المرسوم السالف الذكر على ما يلي: "يلتزم مقدم خدمات الإنترنت خلال ممارسة نشاطاته بما يلي:

أ. تسهيل النفاذ إلى خدمات الإنترنت، حسب الإمكانيات المتوفرة إلى كل الراغبين في ذلك باستعمال أنجح الوسائل التقنية.

ب. المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه الخاصة وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون.

ج. إعطاء مشتركيه معلومات واضحة ودقيقة حول موضوع النفاذ إلى خدمات الإنترنت ومساعدتهم كلما طلبوا ذلك.

د. عرض أي مشروع خاص باستعمال منظومات الترميز على اللجنة.

هـ. إحترام قواعد حسن السيرة بالإمتناع خاصة عن استعمال أية طريقة مشروعة سواءا تجاه المستعملين أو اتجاه مقدمي خدمات الإنترنت الآخرين.

و. تحمل مسؤولية محتوى الصفحات وموزعات المعطيات التي يستخرجها ويأويها طبقا للأحكام التشريعية المعمول بها.

ز. إعلام مشتركيه بالمسؤولية المترتبة عليهم فيما يتعلق بمحتوى الصفحات التي يستخرجونها وفقا للأحكام التشريعية المعمول بها.

ح. إتخاذ كل الإجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات المفتوحة لمشتركيه، قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الأخلاق".

[6]– مرسوم تنفيذي رقم (02-141) مؤرخ في 03 صفر عام 1423 الموافق لـ 16 أبريل سنة 2002، يحدد القواعد التي يطبقها متعاملو الشبكات العمومية للمواصلات السلكية واللاسلكية من أجل تحديد تعريفة الخدمات المقدمة للجمهور، ج ر رقم 28.

[7]– المادة (01/03) من المرسوم السالف الذكر.

مكاتبهم المفتوحة للجمهور وعلى مواقعهم على الإنترنت، كما يسلمون لكل شخص بيان التعريفات المطبقة فيما يخص الخدمات المقدمة له أو المقترحة عليه إذا طلب ذلك[1].

البند الثاني: إلتزام مزودي الخدمات بالتعاون مع رجال الضبط القضائي.

نصت بعض التشريعات صراحة على إلزام مقدمي الخدمات بالحفاظ على بيانات مستعملي شبكتهم مع إلزامهم بالتعاون مع رجال الضبط القضائي في حدود معينة تتمثل في معرفة هوية المستخدمين وليس الكشف عن محتوى اتصالاتهم، مثل القانون الإنجليزي والقانون الإسباني.

وبالتالي ليس من حق مزودي الخدمات الذين يقدمون خدماتهم إلى الجمهور أن يقوموا بإفشاء ما لديهم من معلومات إلى الغير، والأمر على خلاف ذلك بالنسبة للتعاون مع رجال الضبط القضائي، فقانون حماية الحياة الخاصة في مجال الإتصالات الإلكترونية في الولايات المتحدة الأمريكية يعطي لمزودي الخدمات الحق في الكشف عما بحوزتهم من معلومات طواعية واختيارا وذلك للجهات العامة في بعض الحالات، فإذا قاموا بذلك فإنّ رجال الضبط القضائي ليسوا بحاجة إلى اللجوء إلى الأمر بتقديم المعلومات أو إذن التفتيش[2].

أما بالنسبة للدول الأوروبية فقد أدركت مبكرا ضرورة حماية الحياة الخاصة للأفراد و بناءا على ذلك قامت بإنشاء مركز لمكافحة الجرائم الإلكترونية، و ذلك بعد الإحصائيات التي قامت بها و التي أفضت إلى تزايد في حجم هذه الجرائم [3].

أما المجلس الأوروبي فكان هو الآخر له دور في الحد من هذه الجرائم التي أصبحت تنتهك خصوصيات الأفراد و ضرورة ترتيب مسؤولية على عاتق مزودي الخدمات، لأن هؤلاء من يمتلكون المعلومات المتعلقة بالأفراد[4]، فلا شك أن المسؤولية تعد محور أي نظام قانوني، فهي القادرة على تفعيله حتى يصبح التزاما التزاما قانونيا، ونجاحه مرهون بمدى الإستجابة لأصداء ذلك التطور[5].

---

[1]– المادة (02/03) من المرسوم السالف الذكر.

[2]–د. شيماء عبد الغني، المرجع السابق، ص 213.

[3]- Julien, l'Europe s'arme contre la cybercriminalité, le 30/07/2014, disponible à l'adresse suivante : www.numerama.com. Et voir : Nicolas Aguila, l'Europe durcit des sanctions contre la cybercriminalité, le 05/07/2013, disponible à l'adresse suivante : www.tomsguide.fr.

[4] -Alexandra Greenwood, Le statut de l'hébergeur et le web, mémoire master ,droit de l'internet, université Paris, France, 2009, P 45.

[5]–د. سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الإتصال الحديثة (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، ط1، سنة 2006، ص288.

أمّا المشرع الجزائري من خلال القانون رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها نص في المادة (10)[1] على التزامات مقدمي الخدمات المتمثلة في مساعدة السلطات، إذ يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها.

كما تضيف هذه المادة على أنّه يتعين عليهم أيضا وضع المعطيات التي يجب عليهم حفظها وفقا للمادة (11) من القانون المذكور تحت تصرف السلطات، وقد سبق وأشرنا لهذه المعطيات المنصوص عليها في المادة (11) من نفس القانون.

ومن خلال هذا القانون يلاحظ أنّ المشرع الجزائري نص على التحفظ المتعلق بالمعطيات الخاصة بهوية المرسل إليه وكذا المواقع وكافة مستعملي الخدمة، وأيضا المعطيات المتعلقة بمحتوى الإتصالات، ويترتب على ذلك أنّ مزودو الخدمات لا يتمتعون بسر المهنة، بل على العكس هم ملزمين بالتعاون مع رجال الضبط القضائي،وذلك من أجل المساهمة الفعالة في الكشف عن الجريمة والوصول إلى الحقيقة،وفي المقابل يتعين عليهم كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق طبقا للفقرة الأخيرة من نص المادة (10) من القانون السالف الذكر.

ناهيك عن هذه الإلتزامات، هناك إلتزامات خاصة نص عليها المشرع في المادة (12)[2] من ذات القانون تتمثل في التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها لمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتهم للقوانين أو على الأقل جعل الدخول إليها غير ممكن، كما ألزمهم القانون بوضع

---

[1]- تنص المادة (10) من القانون رقم (09-04) السالف الذكر على ما يلي:" في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه ، تحت تصرف السلطات المذكورة .

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري و التحقيق."

[2] - تنص المادة (12) من القانون رقم (09-04) السالف الذكر على ما يلي:" زيادة على الإلتزامات المنصوص عليها في المادة 11 أعلاه ، يتعين على مقدمي خدمات الإنترنت ما يأتي:

أ- التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها، أو جعل الدخول إليها غير ممكن.

ب- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة، وإخبار المشتركين لديهم بوجودها."

ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة، وإخبار المشتركين لديها بوجودها.

الفرع الرابع: التجميع في الوقت الفعلي لبيانات خط سير البيانات.

نصت المادة (20)[1] من الإتفاقية على التجميع في الوقت الفعلي لخط سير البيانات، وذلك بأن تتبنى الدول الأطراف تشريعات تخول سلطة معينة القيام بجمع أو تسجيل عن طريق وسائل معينة موجودة على أرضها البيانات المتعلقة بخط سير البيانات في الوقت الصحيح، أو إلزام مقدم الخدمة في حدود قدرته الفنية بجمع وتسجيل البيانات المتعلقة بخط سير البيانات في الوقت الصحيح.

ويهدف هذا الإجراء الخاص بالتجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات الذي قد تقوم به السلطة المختصة في الدولة، أو ينفذه مقدمو الخدمة بناءا على أوامر صادرة إليهم من السلطة المختصة بهذا الإجراء إلى تسهيل مهمة الجهات القائمة بجمع الأدلة.

ويختلف إجراء التجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات عن إجراء التحفظ السريع على البيانات المتعلقة بخط سير البيانات،والذي نصت عليه المادة (16) من الإتفاقية بأنّ البيانات في حالة التحفظ موجودة لدى مقدم الخدمة أي مخزنة بالنظام المعلوماتي للكمبيوتر أو في دعامة التخزين، بينما في حالة التجميع أو التسجيل فالبيانات ليست مخزنة، وتهدف هذه الإجراءات إلى جمعها أو تخزينها وقت مباشرة الإتصال، وهذا ما عبرت عنه الإتفاقية بالوقت الفعلي أو الصحيح، ولهذا فهو يحتاج إلى وسائل تقنية حديثة قد لا تتوافر لدى السلطة المختصة أو قد لا يكون بمقدورها القيام به، وعلى هذا أسندت الإتفاقية القيام بإجراء التجميع أو التسجيل للسلطة المختصة في الدول لتقوم به بنفسها أو تنفذه من خلال مقدم الخدمة أو بمساعدته[2].

---

[1]- Article 20 du C.C.C : 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :
a. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;
b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :
i. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, ou
ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique…

[2]– د.رامي متولي القاضي، مكافحة الجرائم المعلوماتية، المرجع السابق، ص131.

المطلب الثاني: مراقبة الإتصالات الإلكترونية في حينها.

إتسمت حضارة هذا العصر بقفزات تكنولوجية مذهلة في شتى المجالات بصفة عامة وفي مجال الإتصالات بصفة خاصة، إذ لم يعد هناك أي شكل من أشكال الإتصال يخرج عن نطاق تكنولوجيا المعلومات الإلكترونية ولعل شبكة الإنترنت أفضل مثال على ذلك، إذ قدمت وسائل فريدة للإتصال، فاستطاع الشخص أن يخاطب مراسله ويراه في ذات الوقت عن طريق استخدام ملحقات الصوت والصورة الخاصة بجهاز الكمبيوتر[1].

ولكن كما هو شأن كل تقدم علمي، أدى التطور التكنولوجي إلى إفراز أجهزة للمراقبة ذات تقنية عالية وإمكانات خارقة تلتقط أحاديث الشخص دون أن يشعر، ولم تقتصر هذه الأجهزة على المحادثات الشخصية السلكية واللاسلكية، بل امتدت إلى التقاط الأحاديث التي يتم بطريق الإنترنت، مما أفقد الإنسان حريته وخصوصيته، وهدد على نحو خطير كرامته وإنسانيته، حيث أنّ الإتصال عبر أجهزة الكمبيوتر باستخدام شبكة الإنترنت يلزم مجرى الإتصال بأن يتصل بالرقم الخاص بإحدى الشبكات التي تقدم خدمة الإنترنت، وفي هذه الحالة تمر المحادثة عبر شبكة الإتصال والمعلومات مما يسمح بالتنصت عليها.

غير أنه ظهر في الآونة الأخيرة تقنية جديدة في علم الإتصال وهي الإنترنت الفضائي عبر الستالايت، وتسمح هذه التقنية بالإتصال المباشر بالأقمار الصناعية وتمرير مكالمات دولية من خلالها دون المرور على شبكة الإتصال والمعلومات، وهذا أمر خطير لأنّ تلقي خدمة الإنترنت عبر شبكة الأقمار الصناعية سيلغي دور الأجهزة الأمنية في السيطرة على الإنترنت وعلى المكالمات والرسائل المتبادلة بواسطة شبكة المعلومات، باعتبار أنّ الإنترنت الفضائي عبر الستالايت لا يخضع لأي رقابة.

إلاّ أنّ حق الإنسان في الخصوصية ليس حق مطلق بل مقيد بالمصلحة العامة، وقد تتعارض خصوصية الإنسان مع مصلحة المجتمع في كشف الحقيقة في شأن الجريمة ومعاقبة الجناة، مما يستلزم وجود توازن وثيق بين الحق في الخصوصية وحق المجتمع في العقاب، وإدراك هذا التوازن من أصعب المشاكل التي تواجهها النظم الإجرائية المعاصرة، إذ يتطلب التوفيق بين اعتبارات تبدو متعارضة، فبينما تتطلب مصلحة المجتمع إنزال العقاب على كافة المجرمين بما يستوجب أن تكون قواعد الإجراءات الجزائية صارمة لن يفلت

[1]– د.مدحت عبد الحليم رمضان، جرائم الإعتداء على الأشخاص والإنترنت، المرجع السابق، ص5.نقلا عن: د. ياسر الأمير فاروق، المرجع السابق، ص07.

منها مجرم، فإن متطلبات حماية الحق في الخصوصية عملا بقرينة البراءة ترفض الإعتماد على الإجراءات الجزائية الصارمة على نحو ينبغي فيه أن تكون قواعد الإجراءات الجزائية سياجا للحرية الشخصية.

إلاّ أنّ التوازن بين حق المجتمع في كشف الحقيقة في شأن الجريمة وبين الحق في الخصوصية يتحقق بتقرير شرعية المراقبة بصورة استثنائية، وبمقتضى قانون يعمل جاهدا على إقامة هذا التوازن من خلال تحديده وعلى نحو واضح الحالات التي يجوز فيها المراقبة مع إخضاعها لضمانات عديدة تحول دون التعسف في استعمالها، فضلا عن تحديد جزاءات في حالة مخالفة القواعد القانونية المنظمة للمراقبة الإلكترونية[1]، وعلى هذا الأساس سأتطرق أولا لمفهوم مراقبة الإتصالات الالكترونية باعتبار أنّ المصطلح في حد ذاته أثار العديد من المشكلات القانونية، وسيتم تفصيل ضمانات مشروعيتها، ثم يتم التطرق بعد ذلك إلى الآثار المترتبة على مراقبة الإتصالات الإلكترونية،وذلك على النحو التالي:

الفرع الأول: مفهوم مراقبة الإتصالات الإلكترونية.

نظرا لحداثة الإجراء محل الدراسة، فإنّ الفقهاء والباحثين لم يتفقوا بعد على تسمية محددة له، ففي القانون المقارن قد يستخدم مصطلح المراقبة الإلكترونية أو استراق السمع الإلكتروني، أمّا في القانون المصري فقد ذهب رأي[2] إلى تسمية هذا الإجراء بمراقبة المحادثات وتسجيلها، وفي ذات الإتجاه ذهب رأي[3] إلى إطلاق مصطلح التنصت على المحادثات الخاصة وتسجيلها، غير أنّ هذه التسميات غير جامعة لأنّ كلمة المحادثات تعني في اللغة تبادل الحديث بين شخصين أو أكثر مما يشعر أنّ التسمية قاصرة على مثل هذا الحديث دون غيره من الحديث الفردي الذي ينطق به صاحبه ليسجله بنفسه.

وقد استخدم بعض الفقه تسمية الإجراء بالتنصت والرقابة الإلكترونية،كما تم استخدام مصطلح التنصت والتسجيل الإلكتروني، وهذه التسمية بشقيها محل نظر لأنها لم توضح محل الإجراء،وقد اتجه المشرع المصري في المادتين (95و206) من قانون الإجراءات الجزائية تسمية الإجراء "بمراقبة المحادثات السلكية واللاسلكية وإجراء تسجيلات لأحاديث في مكان خاص"، وقد يعاب على هذه التسمية أنها لا تعدّ تعبيرا صادقا عن مضمون وجوهر الإجراء محل البحث، فهي توهم بأنّ الأحاديث محل الحماية هي الأحاديث التي

---

[1]– د.ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، مصر، ط1، سنة 2009، ص22.

[2]– د.عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، دار المطبوعات الجامعية، القاهرة، مصر، بدون طبعة، سنة 1999، ص403.

[3]– د.أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 1994، ص311.نقلا عن : د. ياسر الأمير فاروق، المرجع السابق، ص 20.

تجرى في مكان خاص دون الأحاديث التي تجرى في مكان عام وإن اتسمت بالخصوصية، في حين أنّ محل الحماية هي الأحاديث الخاصة مطلقا بغض النظر عن المكان الذي تدور فيه سواء كان عاما أو خاصا، لأنّ موضوع الحماية هو حرمة الحديث لا حرمة المكان.

غير أنّ هذا الكلام ينطبق على الإتجاه الذي يعتد بموضوع المحادثة لإضفاء صفة الخصوصية على الحديث، فيكون الحديث خاصا إذا جرى في مكان خاص لو تناول موضوعا عاما لا علاقة له بالحياة الخاصة لقائله، ويعتبر الحديث عاما إذا جرى في مكان عام ولو تناول أخص شؤون قائله وأسراره[1]، وإن كان البعض يرى أنّ الحديث يكون خاصا إذا تم عبر وسائل الإتصال كالهاتف أو الهاتف المحمول أو في الإنترنت، فمعيار الخصوصية هو جريان المحادثة عبر وسيلة من هذه الوسائل.

وعلى العكس من ذلك يرى البعض أنّ المحادثات الفورية والمعروفة بنظام التشات (Chat)إضافة إلى المحادثات المعروفة بالدردشة أين يمكن الحديث مع أكثر من شخص في الوقت ذاته، لا تنطبق عليها الحماية الجنائية التي تتمتع بها المحادثات الشفوية التي تتم في مكان خاص، لأنّ شبكة الإنترنت لا تعتبر مكانا خاصا ومن تم يجوز مراقبة هذه الأحاديث دون أي قيد أو شرط[2]، غير أنّ هذا الكلام ينطبق على الإتجاه الذي يعتد بطبيعة المكان.

فالمشرع الأمريكي إستعمل عبارة "للإعتراض" للدلالة على عمليات مراقبة الإتصالات الإلكترونية لدى تعريفه لهذا الإجراء بمقتضى المادة (2510/ف4)من قانون الجرائم والإجراءات الجنائية الأمريكي،والأمر نفسه ينطبق أيضا على المجلس الأوروبي الذي يستخدم العبارة نفسها في الإتفاقية الأوروبية لمكافحة الجرائم الإلكترونية طبقا للمادة (21)[3] من نفس الإتفاقية، كما أنها لم تعرّف المقصود بالمعطيات المتعلقة بالمحتوى.

---

[1]– أعلن جانب من الفقه أنه من الخطأ الإعتماد على أحد المعيارين وإهمال الآخر وإنما يجب المزج بينهما، ومن تم فوفقا لهذا الرأي فإنّ الحديث الذي يدور بالأماكن الخاصة متى كان بصوت غير مسموع يعد حديثا خاصا بغض النظر عما إذا كان صاحب الحديث هو مالك أو حائز أو مجرد زائر للمكان ودون البحث عن مضمون الحديث فالمكان الخاص وانخفاض الصوت قرينة قاطعة على كون الحديث خاصا، بينما إذا تم في مكان خاص بصوت مرتفع فإنّ ذلك يعد قرينة على تعلقه بحديث عام ما لم يثبت العكس كأن يكون إرتفاع الصوت نتيجة لاستفزاز معين، أما بالنسبة للحديث الذي يدور بالأماكن العامة فإذا تم بصوت منخفض غير مسموع وعلى انفراد لمن يتواجد بالمكان، فإنه يعد حديثا خاصا ما لم يثبت العكس. أنظر في ذلك: د. ياسر الأمير فاروق، المرجع السابق، ص536.

[2]– أ.عائشة بن قارة، المرجع السابق، ص 164.

[3]- Article 21 du C.C.C : Interception de données relatives au contenu.

فاستعمال هذه التسمية لا يخلو من الخطأ، سواء من الناحية اللغوية أو العملية، فمن الناحية اللغوية تأتي هذه العبارة بمعنى (صار عارضا له أي منعه)، وهذا يعني من الناحية العملية ينبغي أن يتم اعتراض المحادثة وقطع الطريق عنها، غير أنّ أنظمة المراقبة لا تؤثر في محتوى ووجهة الإتصال المراقب وإنما تقوم فقط بالتنصت، لذلك استعمال عبارة "الإلتقاط" يكون أكثر إتفاقا مع الآلية المقدمة للمراقبة[1].

ويعرف الإعتراض بأنه معرفة محتوى إتصال قد يتم داخل نظام حاسب آلي واحد، أو بين نظامين مختلفين، أو بين عدة أنظمة ترتبط فيما بينها من خلال شبكة إتصالات، وذلك بالتقاط المعلومات التي يتضمنها هذا الإتصال.

وتعد الوسيلة الأساسية لاعتراض نظام الحاسب الآلي، هي استخدام الموجات الكهربائية الصادرة عن الحاسب الآلي، ويعرف في الولايات المتحدة الأمريكية باسم إلتقاط الموجات الكهربائية، وهو جمع معلومات يتم إرسالها من خلال نظام الحاسب الآلي داخل مبنى، وذلك باستعمال شاشة عرض يتم توصيلها بجهاز تسجيل خارج المبنى، وتقوم هذه الشاشة بالتقاط الموجات الكهربائية التي تحيط بالحاسب الآلي، والتي تتحول إلى معلومات مقروءة على الشاشة من ناحية، كما يتم تسجيلها من ناحية أخرى[2].

أمّا القانون الجزائري رقم (04/09)المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، فقد عرّف الإتصالات الإلكترونية بأنها أي تراسل أو إرسال واستقبال علامات أو إشارات أو كتابات أو صور وأصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية طبقا لنص المادة الثانية (02) من نفس القانون، وقد جاء هذا القانون خاليا من تعريف مصطلح المراقبة، كما هو الشأن بالنسبة للمشرع الفرنسي من خلال نص المادة (L32/1°)[3].

كما يعرفها بعض الفقه [4] بأنها إجراء تحقيق يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر بها السلطات القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها، ويتضمن من ناحية استراق السمع إلى الحديث، ومن ناحية أخرى حفظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض.

---

[1]– أ.رشاد خالد عمر، المرجع السابق،ص 182.

[2]– د. أحمد محمود مصطفى، المرجع السابق، ص 258.

[3]- Article L32/1°(C.P.T.E Modifié par Ordonnance n°2011-1012 du 24 août 2011 - art. 1, Modifié par Ordonnance n°2011-1012 du 24 août 2011 - art. 2) : Communications électroniques.
On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique.

[4]– د.ياسر الأمير فاروق، المرجع السابق، ص 150.

غير أنّ المراقبة الإلكترونية لا ترد إلاّ على الإتصالات الإلكترونية حال إجرائها، وهذا ما أكد عليه المشرع الجزائري بموجب المادة(03)[1] من القانون رقم (09-04) المتعلق بتكنولوجيا الإعلام والإتصال ومكافحتها، ذلك أنها إجراء خطير واستثنائي مقرر من أجل التعامل مع الطبيعة الحركية لهذه البيانات التي لا يمكن تفتيشها ولا ضبطها إلاّ من خلال هذا الإجراء، بخلاف الإتصالات الإلكترونية المخزنة يمكن تفتيشها وضبطها مباشرة إذا كانت مخزنة في الكمبيوتر الخاص بالمستخدم أو التحفظ المستعجل إذا كانت مخزنة في الخادم المعلوماتي لدى مزود الخدمات من دون الحاجة إلى مراقبتها إلكترونيا.

وهذا ما أكد عليه المجلس الأوروبي من خلال التوصية التي طالب فيها بضرورة إقامة التمييز بين مراقبة البيانات الإلكترونية المتحركة وتفتيش وضبط البيانات الإلكترونية الساكنة، وهذا يدعو للقول أنّ المراقبة الإلكترونية لا تعد نوعا من التفتيش لأن هذا الوضع الأخير لا يرد إلا على البيانات الإلكترونية الساكنة، إلاّ أنها تعد إجراء خاص ولكنها ليست إجراء مستقل،كونها تبدأ من لحظة التقاط الإتصال الإلكتروني من خلال الأجهزة والتقنيات المعدة لهذا الغرض، وتنتهي بمجرد وصول المحادثة أو المراسلة إلى حيازة الجهة المراقبة[2].

وهناك من يرى أن المراقبة الأمنية الإلكترونية هي عمل أمني أساسي له نظام معلومات إلكتروني، يقوم فيه المراقب (بكسر القاف) بمراقبة المراقب (بفتح القاف) بواسطة الأجهزة الإلكترونية وعبر شبكة الإنترنت لتحقيق غرض محدد وتحرير تقارير بالنتيجة[3].

فيما يتعلق بالأحاديث محل الحماية، أميل إلى تأييد المعيار الموضوعي و في ذلك يرى الدكتور ياسر الأمير فاروق أنّ المحادثات الشخصية تصدر عن حرية تعبير من قبل صاحبها، وهي عبارة عن سلوك نفسي، كما أنّ هذا المعيار يساير أحكام الدستور الجزائري في مادته (39) منه والذي يقضي بأنه لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون، سرية المراسلات والإتصالات بكل أشكالها مضمونة، فهو قد نص على ضرورة حماية الأحاديث الخاصة بصفة مطلقة، دون الأخذ بعين الإعتبار طبيعة المكان الذي يتم فيه الحديث.

---

[1] – تنص المادة (03) من القانون رقم (09-04) السالف الذكر على ما يلي : " مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات ، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية ، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها و القيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية."

[2] – أ.رشاد خالد عمر، المرجع السابق،ص184.

[3] – د.مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت (دراسة مقارنة)، سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية، الكتاب الخامس، بدون ناشر، ص 192.

وبالرجوع إلى القانون الجزائري رقم (09-04) الذي يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها،ألاحظ أنّ المشرع الجزائري قد استعمل عبارة "مراقبة الإتصالات الإلكترونية" وأعتقد أنّ هذا المصطلح هو الأكثر إتفاقا، على اعتبار أنّ الفقهاء يرون أنها تتم من خلال تقنيات وبرامج تقوم بالتقاط تلك المحادثات عن بعد، ومن تم يتم التنصت عليها والإطلاع على محتواها أو ضبطها من قبل الجهة المراقبة، وهذا الأمر يفترض أن يتم دون أن يشعر به أطراف الإتصال، كما أنه ينبغي أن يتم دون أن يؤدي إلى قطع الإتصال أو المحادثة وإلا سينتفي الغرض من إجراء المراقبة[1]، ولذلك يرى الفقه أنّ هذه العملية لا تتم من خلال اعتراض المحادثة وإنما من خلال التقاطها عبر تلك التقنيات والأجهزة، وأنه من غير الصائب استعمال عبارة "الإعتراض" للدلالة على مراقبة الإتصالات الإلكترونية والتنصت عليها.

الفرع الثاني: مشروعية مراقبة الإتصالات الإلكترونية.

إنّ الأصل هو التزام مزود الخدمات بعدم مراقبة الإتصالات الإلكترونية للمشتركين ، لأنّ البيانات الشخصية المتعلقة بمستخدمي الشبكة تدخل ضمن إطار الحق في الخصوصية الذي تحميه الإتفاقية الأوروبية لحقوق الإنسان، ولا يجوز لمزود الخدمة أو غيره أن يقوم بزرع برامج التتبع بغرض التجسس على مستخدمي الشبكة، فلا يجوز زرعها إلاّ بموافقة صاحب النظام وبعلم من يتصلون.

غير أنه من حق مزودي الخدمات أن يعلموا بالبيانات المتعلقة بهوية مستخدمي الشبكات، وذلك عند متابعتهم لأداء الشبكة وإصلاح ما بها من عطل في نقل المعلومات وكذلك بغرض إعداد الفواتير المطلوبة من المشتركين فيها، إلا أنه لا يجوز لمزودي الخدمات أن ينشروا بيانات عن مستخدمي الشبكات في دليل يطلع عليه العامة على الشبكة دون موافقة أصحاب هذه البيانات[2]، وسيتم التمييز في هذا المقام بين مراقبة الإتصالات الالكترونية بناءا على إذن ، وكذا سلطة مزودي الخدمات في مراقبة النظام دون إذن.

البند الأول: مراقبة الإتصالات الإلكترونية بناءا على إذن.

لما كانت المراقبة الالكترونية إجراءا إستثنائيا وخطيرا لمساسها بحق الإنسان في الخصوصية، لذلك فقد حرصت التشريعات الإجرائية على إحاطة اللجوء إلى هذا الإجراء بمجموعة من الضمانات والتي منها

---

[1]–أ.رشاد خالد عمر، المرجع السابق، ص 182.

[2]– د.شيماء عبد الغني، المرجع السابق، ص 217.

ما هي ضمانات موضوعية، ومنها ما هي ضمانات شكلية، وهي تشترك في هذه الضمانات مع اعتراض الإتصالات السلكية واللاسلكية، فبالرجوع إلى القانون الجزائري رقم (09-04)، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، فقد نص على هذه الضمانات وذلك على النحو التالي[1]:

أولا: إختصاص السلطة القضائية بمنح الإذن لإجراء عملية مراقبة الإتصالات الإلكترونية:

لا يجوز مراقبة محتوى الإتصالات الإلكترونية إلا بعد الحصول على إذن بذلك من جهة مختصة قانونا بإصداره، وإلا كان إجراءا معيبا بعدم المشروعية، وفي الواقع اختلفت التشريعات في تحديدها للجهة المختصة قانونا بإصدار الإذن بالمراقبة، إلاّ أنّ المشرع الجزائري حددها بالسلطة القضائية والمقصود بالسلطة القضائية قضاة النيابة والتحقيق والحكم[2].

ثانيا: ينبغي أن يكون هذا الإذن مكتوبا:

فيشترط في أمر المراقبة أن يكون ثابتا بالكتابة، ذلك أنّ هذا الأمر من إجراءات التحقيق فيسري عليه ما يسري على هذه الإجراءات من أحكام، وذلك لكي يبقى حجة ويكون أساسا صالحا لما يبنى عليه من النتائج ذلك أن كتابة الأمر هي الدليل الوحيد على حصوله، فلا يصح إثباته بوسيلة أخرى .

ثالثا: الجرائم التي يجوز فيها المراقبة:

تختلف التشريعات المعاصرة في تحديد الجرائم التي تبرر عملية المراقبة تبعا لفلسفة التشريع من ناحية والسياسة الجنائية التي تتبناها من ناحية أخرى، غير أنّ أغلب التشريعات تلتقي في إجازة المراقبة متى كانت الجريمة على قدر كبير من الخطورة، بينما تحظر اتخاذ المراقبة متى كانت الجريمة المرتكبة بسيطة وهو الأمر الذي يستوجب بيان المعيار الذي تعتمده التشريعات في هذا المجال[3]، إلاّ أنّ المشرع الجزائري في القانون رقم (04/09) السالف الذكر قد حدد في المادة الرابعة (04) الجرائم التي تسمح باللجوء إلى المراقبة الإلكترونية ومن بينها: الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، كذلك في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

---

[1]- د.ياسر الأمير فاروق، المرجع السابق، ص 450 و ما بعدها.

[2] - تنص المادة 4 فقرة 2 من القانون رقم 09-04 السالف الذكر على ما يلي: " ... لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة ...".

[3]- د. ياسر الأمير فاروق، المرجع السابق، ص 510.

أمّا الفقرة (ج) و(د) من المادة الرابعة(04) من القانون (04/09) لم تحدد جرائم وإنما حالتين إذا توفرت يمكن اللجوء إلى إجراء مراقبة الإتصالات الإلكترونية، وتتمثل في أنه إذا اقتضت التحريات والتحقيقات القضائية ذلك حين يكون من الصعب الوصول إلى نتيجة دون اللجوء إلى المراقبة، فحين تقرر النصوص القانونية إجراء، فإنها تجعل لهذا الإجراء غرضا من وراء مباشرته، سيما إذا كان هذا الإجراء ينطوي على مساس بالحقوق والحريات،فوجود الهدف الذي يمكن أن ينتج عن إجراء معين هو الذي يبين مشروعية هذا الإجراء، في حين إذا تخلف الهدف يصبح الإجراء باطلا[1]، وكذلك يتم اتخاذ هذا الإجراء في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[2].

رابعا: مدة المراقبة:

حرصت معظم التشريعات المعاصرة على تحديد مدة معينة للمراقبة للحد من التعسف وإساءة استعمال السلطة، غير أنّ هذه التشريعات لم تسر على وتيرة واحدة في شأن هذه المدة، فمنها من حدد المدة بأمد قصير، ومنها من أطال زمن المدة، ومنها من لجأ إلى تقرير نظام تحديد مدة المراقبة ، وطبقا لنص المادة (4) من القانون (04/09) ، فقد حدد المشرع أنه عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة (أ) والمتمثلة في الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، فيختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها إذنا لمدة ستة (06) أشهر قابلة للتجديد[3].

وتضيف المادة، أنه تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة (أ) موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والإعتداءات على أمن الدولة

---

[1]- د. ياسر الأمير فاروق، المرجع السابق، ص 450.

[2] – تنص المادة 4 فقرة 1 من القانون رقم 09-04 السالف الذكر على ما يلي :" يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

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

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

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

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة..."

[3] – تنص المادة 4 فقرة 3 من القانون رقم 09-04 السالف الذكر على ما يلي:" ... يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد ..."

ومكافحتها، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير طبقا للفقرة الأخيرة من المادة (4) من القانون رقم (09-04) السالف الذكر[1].

وبالنظر لأهمية التسجيل الصوتي الناجم عن مراقبة الإتصالات الإلكترونية في إثبات بعض أنواع الجرائم ومن ضمنها الجرائم الإلكترونية، فقد حرصت التشريعات الإجرائية على إحاطته بضمانات أخرى تكفل صحته ومشروعيته من خلال تنظيم كيفية إحرازه وحفظه بما يزيد من طمأنة محكمة الموضوع إليه وثقتها فيه.

كما أن المشرع الفرنسي نص على ضرورة تحرير محضر بها وإحرازها في أحراز مغلقة، ومن تم ختمها بالأختام الرسمية المغلقة، كما وأجاز إمكانية إتلاف تلك التسجيلات بعد انتهاء التحقيق والمحاكمة، على أن يتم ذلك بناء على طلب المدعي العام في المقاطعة أو النيابة العامة[2]، أما المشرع الجزائري فلم يتطرق لهذه المسألة، وعليه يتعين الرجوع للقواعد العامة، غير أن هذه الأخيرة غير كافية لتجاوز الفراغ الشريعي، لذلك يجب تنظيمها بقوانين خاصة.

البند الثاني: مراقبة الإتصالات الإلكترونية بدون إذن.

السؤال الذي يطرح في هذا المقام، هل يجوز لمزودي الخدمات مراقبة النظام دون إذن قضائي مسبق؟ للإجابة عن هذا التساؤل سيتم التطرق لحالة المراقبة المعتادة لعمل الشبكة، وحالة المراقبة بناءا على شكوى المشترك، بالإضافة لحق رب العمل في مراقبة الإتصالات الإلكترونية الخاصة بالعاملين لديه.

أولا: المراقبة المعتادة لعمل الشبكة.

تقرر بعض التشريعات كالقانون الأمريكي استثناء خاصا لمزودي الخدمات يستطيعون بمقتضاه أن يقوموا بمراقبة المشتركين في خدماتهم، وذلك من خلال معرفة ما يقوم هؤلاء المشتركون من نشاط التداخل في أجهزة الآخرين أو تخزين مواد مخالفة للقانون، وقد قرر القانون الأمريكي هذا الإستثناء وذلك مراعاة لحقوق مزودي الخدمات حتى يمكنهم من الدفاع عن تلك الحقوق في مواجهة المشتركين في الخدمات التي يقدمونها

---

[1]- تنص المادة 4 فقرة أخيرة من القانون رقم 09-04 السالف الذكر على ما يلي:" ... تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة أ من هذه المادة موجهة حصريا لتجميع و تسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والإعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير ".

[2]- أ.رشاد خالد عمر، المرجع السابق، ص 198.

بمقابل، أو الذين يستعملون تلك الخدمات حتى يمكنهم من الأداء اليومي لأجهزتهم ومعداتهم، ومن تم فإنّ القانون الأمريكي يسمح لهم بتسجيل هذه التداخلات والتبليغ عنها لرجال الضبط القضائي، ولا يجوز لرجال الضبط القضائي

أن يبادروا إلى تلك المراقبة دون تبليغ من مزودي الخدمات أو سبق حصولهم على إذن بذلك[1].

ثانيا: المراقبة بناء على شكوى المشترك.

لقد اختلفت التشريعات حول مدى إمكانية السماح بمراقبة الإتصالات الإلكترونية بناءا على الطلب الصادر من صاحب الجهاز، وبالتالي فإنّ الإستثناء يسمح لمزود الخدمات بأن يقوم بذلك، مع توافر شروط معينة تتمثل في:

– أن يسمح المالك لرجال الضبط بوضع الجهاز الخاص به تحت المراقبة.

– أن يتم ذلك في إطار تحقيق جنائي قائم.

– أن تتوافر دلائل كافية على أن تسجل الإتصالات القادمة من الجهاز الصادر منه الإعتداء تفيد في كشف الحقيقة.

– أن يقتصر رجال الضبط على اعتراض الإتصالات الصادرة من وإلى الأجهزة محل التحقيق.

ثالثا: حق رب العمل في مراقبة الإتصالات الالكترونية الخاصة بالعاملين لديه.

يتعين التمييز بين كمبيوتر الشخص المتواجد في منزله والكمبيوتر الخاص بالعمل، ففي الحالة الأولى لاشك أن صاحب الجهاز يتمتع بحرمة الحياة الخاصة بالنسبة لما يحتويه هذا الجهاز من معلومات، أما في الحالة الثانية فإن الكمبيوتر يعتبر من أدوات العمل، وبالتالي إذا كان ما يجري عليه العمل في شركة معينة أو في إدارة معينة هو جواز أن يتابع الرئيس الإداري أجهزة الموظفين لمتابعة سير عملهم وكان ذلك معلنا ومعروفا، فإن ذلك يعتبر من قبيل الرضاء الضمني بالمراقبة.

[1]– وهذا ما قضي به في قضية تتلخص وقائعها في أن رجال الضبط القضائي كانوا يتتبعون متهما في جريمة اختطاف وقد عمد هذا المختطف إلى استخدام خط هاتفي مقلد، لذا لجأ رجال الضبط إلى مزود خدمات الاتصالات السلكية لمراقبة هذا الخط استنادا إلى أن القانون يسمح لهم بتلك الرقابة في حالة الاعتداء على حقوق هؤلاء المزودين بتلك الخدمات، وقد لاحظت المحكمة أن المبادرة بالرقابة على الخطوط يجب أن تبدأ من مزودي الخدمات في أثناء قيامهم بأعمالهم، فلهم عندئذ أن يقوموا بتبليغ رجال الضبط، والعكس من ذلك غير جائز قانونا كما هو الحال في هذه الدعوى.أنظر في ذلك: د.شيماء عبد الغني ، المرجع السابق، ص 221.

فرب العمل له الحق في مراقبة الرسائل الإلكترونية الواردة إلى العاملين لديه في شركته، ويرجع ذلك إلى أنّ رب العمل في القطاع الخاص يمتلك أدوات العمل ويخصصها لمصلحة العمل، ويعتبر جهاز الكمبيوتر من الأدوات[1].

وتجدر الإشارة، إلى أنّ المراقبة الإلكترونية قد تستخدم كوسيلة لتنفيذ العقوبة السالبة للحرية ويقصد بذلك إلزام المحكوم عليه بالإقامة في منزله أو محل إقامته خلال ساعات محددة، ويتم متابعة ذلك عن طريق المراقبة الإلكترونية، ويتحقق ذلك من الناحية الفنية بوضع أداة إرسال على يد المحكوم عليه تشبه الساعة، وتسمح لمركز المراقبة من كمبيوتر مركزي لمعرفة ما إذا كان المحكوم عليه موجودا في المكان والزمان المحددين بواسطة الجهة القائمة على التنفيذ أم لا.

ومؤدى ذلك من الناحية الفنية، أنه يتم تنفيذ هذه المراقبة من خلال ثلاثة عناصر، تتمثل في جهاز إرسال يتم وضعه في يد الخاضع للرقابة، جهاز استقبال موضوع في مكان الإقامة ويرتبط بخط هاتفي وجهاز كمبيوتر مركزي يسمح بتعقب المحكوم عليه عن بعد، ويتم حصر تحرك هذا الأخير في مساحة لا تتجاوز خمسين مترا، بحيث إذا تجاوز هذه المساحة أو حاول تعطيل جهاز الإرسال أو العبث به يتم تلقائيا إرسال إشارة إلى الكمبيوتر المركزي لكي تتخذ بعد ذلك الإجراءات اللازمة.

غير أنّ هذه الوسيلة تفترض صدور حكم بعقوبة سالبة للحرية قصيرة المدة لا تتجاوز كقاعدة عامة مدة عام، فهي لا تسري على المحكوم عليهم الذين تتوافر لديهم القابلية على الإندماج في المجتمع، وذلك بواسطة مواصلة دراستهم وأعمالهم،كما لا تعد عقوبة قائمة بذاتها وإنما طريقة لتنفيذ العقوبة السالبة بالحرية خارج المؤسسة العقابية[2].

الفرع الثالث: الآثار المترتبة على مراقبة الإتصالات الإلكترونية.

تترتب على مراقبة الإتصالات الإلكترونية، كأثر رئيسي تسجيل محتوى تلك الإتصالات وتخزينها على وسائط مادية قابلة للنقل بغية استخدامها لإثبات الجريمة الواقعة، ولكن تختلف نوعية التسجيل هنا

[1]– د. شيماء عبد الغني، المرجع السابق، ص 230.

[2]– د. عمار سالم، المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن، دار النهضة العربية، القاهرة، مصر، ط2، بدون سنة، ص9.

بحسب ما إذا كانت المحادثة الإلكترونية المراقبة هي عبارة عن إتصال صوتي فقط، أو أنها إتصال صوتي مرئي[1]، وذلك على النحو التالي:

البند الأول:التسجيل الصوتي.

يعرف التسجيل الصوتي بأنه عملية ترجمة للتغييرات المؤقتة لموجات الصوت الخاصة بالكلام أو الموسيقى إلى نوع آخر من الموجات أو التغييرات الدائمة، أو هو عبارة عن عملية ترجمة للتغييرات المؤقتة لموجات الصوت الخاصة بالكلام أو رنينه بواسطة آلة تنقل موجات الصوت إلى اهتزازات خاصة والتي تتفق مع الأصوات التي تحدثها بالضبط[2]، كما يثير التسجيل الصوتي كأثر مترتب على مراقبة الإتصالات الإلكترونية مسألة مدى مشروعيته .

فقد أثار التسجيل الصوتي خلسة للمحادثات الهاتفية الذي يأخذ التسجيل الصوتي للمحادثات الإلكترونية حكمه جدلا كبيرا بين فقهاء القانون الجنائي حول مدى مشروعيته، فظهرت الإتجاهات التالية:

الإتجاه الأول:

يرى أصحابه عدم جواز اللجوء إلى التسجيل الصوتي خلسة، لأنه يعتبر سلوكا غير أخلاقي يمس حق الإنسان في سرية أحاديثه كما يعتبر انتهاكا لحرمته وأنه يتنافى مع الحرية الشخصية، بالإضافة إلى أنه لا يمس أحاديث المتهم وحده، وإنما يمس أحاديث الطرف الآخر للمحادثة الذي يكون في الغالب طرفا بريئا،ويضاف إلى ذلك أنّ هذا التسجيل قابل للتحريف والتغيير والتزوير مما يحتمل معه ألاّ يكون مطابقا للحقيقة في جميع الأحوال[3].

ويفرق الأستاذ CHAMBON بين حالتين: الحالة الأولى، عند افتتاح التحقيق القضائي فإن الإتجاه إلى استخدام التنصت الهاتفي يكون عملا غير مشروع لأنه تم بغير علم المعني بالأمر، مما يترتب عليه استحالة الإمتثال لأحكام القانون، أمّا الحالة الثانية وهي استعمال هذه الوسائل بدون علم الشاهد أو المتهم، فينبغي إدانة هذه الممارسة لأنها تنطوي على حيل ومخادعات محظورة على القاضي الذي يجب عليه التصرف بكل نزاهة وبوجه مكشوف[4].

---

[1]-أ. رشاد خالد عمر، المرجع السابق، ص 190.

[2]– د. صالح عبد الزهرة الحسون، أحكام التفتيش وآثاره في القانون العراقي، مطبعة الأديب ، العراق، سنة 1979، ص 124.نقلا عن: أ. رشاد خالد عمر، المرجع السابق، ص 192.

[3]– أ. صالح عبد الزهرة الحسون، المرجع السابق، ص126. نقلا عن:نفس المرجع ، ص 193.

[4]– د. محمد مروان، نظام الإثبات في المواد الجزائية في القانون الوضعي الجزائري، ج2، ديوان المطبوعات الجامعية، الجزائر، بدون طبعة، سنة 1999، ص432.

الإتجاه الثاني:

يذهب أنصار هذا الرأي إلى القول بأن تسجيل الصوت خلسة والإستناد إلى الدليل المستند منه يعد إجراءا مشروعا، طالما أن هذه الإقرارات والمحادثات قد صدرت بحرية واختيار دون أي تأثير، فليس هناك ما يمنع قانونا من الإستفادة من ثمرات التطور العلمي والتكنولوجي في الكشف عن الجرائم ومرتكبيها،والتسجيل الصوتي اكتشاف علمي يساعد على ذلك، حيث أن المشرع لم ينص على بطلان هذا الإجراء وبالتالي لم ينص على بطلان الدليل المستمد منه[1].

الإتجاه الثالث:

حاول أنصار هذا الرأي التوفيق بين الرأي القائل بعدم المشروعية، والرأي الذي يقرر بمشروعية هذا الإجراء، فذهبوا إلى أنّ التسجيل الصوتي يكون باطلا متى تم تسجيل الحديث الخاص بالمتهم في مكان خاص يترتب عليه انتهاك لحقه في حياته الخاصة، أما إذا كان التسجيل لا ينطوي على انتهاك هذا الحق،بأن يتم التسجيل في مكان عام فإنه يكون مشروعا، وعلى ذلك فالتسجيل الذي يتم في مكان عام هو تسجيل مشروع، أمّا التسجيل الذي يتم في مكان خاص فهو باطل حتى ولو كان دخوله قد تم بطريق مشروع، لأنّ من يتحدث حديثا عبر الهاتف يمكن أن يتصور وجود مسترق للسمع وعليه أن يحذر في حديثه[2].

الإتجاه الرابع: لابد من التمييز بين حالتين:

الحالة الأولى: أن يكون التسجيل الصوتي مقدما كدليل إدانة، وهنا يلزم التفرقة بين فرضين:

أ- إذا لم يمثل التسجيل الصوتي أي إعتداء على الحياة الخاصة فيكون الدليل المستمد من التسجيل مشروعا، وللمحكمة الإستناد عليه في الإثبات بشرط أن يرضى المتحدث رضاءا صحيحا بتسجيل حديثه.

ب- إذا انطوى هذا التسجيل على انتهاك لحق المتهم في الخصوصية لا يكون هذا الدليل المستمد من هذا التسجيل مشروعا.

---

[1]- د. أحمد محمد خليفة، مشروعية التسجيل الصوتي في التحقيق الجنائي، مجلة الأمن العام، مصر، العدد الأول، سنة 1958، ص 25. نقلا عن : د.محمد أمين الخرشة، المرجع السابق، ص 156.

[2]-د. عادل حافظ غانم، كشف الجريمة بالوسائل العلمية الحديثة، المركز القومي للبحوث الإجتماعية والجنائية، مصر، بدون طبعة، سنة 1971، ص 235.نقلا عن : د. محمد الأمين الخرشة، المرجع السابق، ص 155.

الحالة الثانية: إذا قدم التسجيل الصوتي كدليل على براءة المتهم،وعندئذ يجوز الإستناد إليه بلا قيد أو شرط حتى ولو كان الحصول عليه قد قدم بطريقة غير مشروعة،لأنّ ذلك عودة لأصل البراءة فلا يقبل تقييد حرية المتهم باشتراط مشروعية دليل البراءة،وفقا لما هو مطلوب في دليل الإدانة[1].

لاشك أنّ التسجيل الصوتي خلسة للمحادثات يكون مشروعا في جميع الأحوال التي يكون فيها اللجوء إلى مراقبة تلك المحادثات مشروعا، أي أنّ التسجيل الصوتي يستمد مشروعيته من مشروعية اللجوء للمراقبة، غير أنه لو تم تحريفه أو تزويره أو التلاعب به يكون التسجيل الصوتي باطلا حتى ولو كان اللجوء إلى المراقبة مشروعا.

غير أنه من حيث مصداقية أدوات التسجيل، فلاشك أن التقدم العلمي قد وصل مرحلة من التطور تسمح بالقول بكل ارتياح أن أدوات التسجيل ذات مصداقية تامة إذا سلمت من يد العبث مما يعني أنه لو تم التسجيل في ظروف نزيهة، فإن ما يحتويه يكون مبدئيا صحيح وواقعي، فالسؤال لا يطرح على مصداقية التسجيل بل على الظروف التي أنجز فيها، والإنتقادات القائمة حاليا إنما تنصب على التشكيك في نزاهة إعداد التسجيل أو نسبة ما هو مسجل للمتهم، وهذا هو الإطار الذي يجب أن تكون فيه المناقشة[2].

البند الثاني: التسجيل الصوتي المرئي.

في الحالات التي تتم فيها مراقبة المحادثات الإلكترونية التي تجري بالصوت والصورة، كالتي تجرى عبر الويب كام وكالتي تجرى من خلال كاميرات المحمول عبر (MMS) ، فإنه يتم تسجيل تلك المحادثات بالصوت والصورة وليس بالصوت فقط، ومن هنا يختلف التسجيل الصوتي المرئي عن التسجيل الصوتي لأنّ الصورة في هذه الحالة تكون مرئية متحركة.

وبالرغم من أنّ الإشكالات بخصوص التسجيل الصوتي خلسة تنطبق أيضا على التسجيل الصوتي المرئي خلسة، إلاّ أنّ الأخير يثير مشاكل، ذلك أنه بالإضافة إلى مساسه بحق الإنسان في خصوصية أحاديثه الشخصية، فإنه يمس أيضا حقه في الصورة الذي يعده الفقهاء واحد من أخطر أشكال الإعتداء على الحق في الخصوصية[3].

---

[1]– د.محمد أمين الخرشة، المرجع السابق، ص 157.

[2]–أ.بخيمي جمال، المرجع السابق، ص 102.

[3]– أ. رشاد خالد عمر، المرجع السابق، ص 199.

أما فيما يتعلق بإشكالية اعتراض البريد الإلكتروني، فلا شك أنّ هذه الفكرة تقوم على تبادل الرسائل الإلكترونية والملفات والرسوم والصور والبرامج عن طريق إرسالها من المرسل إلى شخص أو أكثر، وذلك باستعمال عنوان البريد الإلكتروني للمرسل إليه، فلكل مشترك صندوق بريدي في عالم الإنترنت، مع وجود فارق جوهري يتمثل في أنه في صندوق البريد الإلكتروني توجد الرسائل المرسلة إليك وتلك التي سبق إرسالها والرسائل الملغاة ونماذج عامة لصيغ الرسائل، بالإضافة إلى قائمة بالعناوين البريدية، فهو يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تمت معالجتها رقميا من صندوق خاص وشخصي للمستخدم ولا يمكن الدخول إليه إلاّ عن طريق كلمة المرور[1]،ولذلك فمن المهم جدا إتخاذ جميع الإحتياطات الممكنة للحفاظ على أمن البيانات و إيجاد طرق أكثر أمنا[2].

غير أنه في حالة عدم وجود نص يحدد النظام القانوني للرسائل الإلكترونية، يتعين البحث عما يقترب من الرسائل الإلكترونية، ولا نجد سوى النظام القانوني المعروف والخاص بالرسائل البريدية،والحقيقة أنّ الإثنين يقتربان من عدة أوجه، فلكل منهما يشكل إتصالا مكتوبا بين طرفين، كما أنه تمر مدة بين إرسال واستقبال الرسالة في الحالتين، وتتفق الحالتان في أنه عندما يتم إرسال الرسالة لا يمكن للمرسل أن يستردها مرة أخرى، غير أنّ أهم ما يميزها أنّ الرسائل البريدية تتميز بالسرية بشكل أكبر من الرسائل الإلكترونية التي تسببت الوسائل التكنولوجية في إمكانية التقاطها من الغير بالإستعانة ببرامج خاصة[3].

وعليه ومن أجل حماية أكبر وحفاظا على سرية المعلومات ينبغي الإستعانة بوسائل أكثر أمانا كالتشفير ، وذلك بغرض الحفاظ على بيانات الأشخاص بما في ذلك البريد الإلكتروني[4].

وقد قضي في الولايات المتحدة الأمريكية في قضية Maxwell بأنه لا يجوز الإطلاع على المراسلات الالكترونية لدى الجهاز الخادم إلاّ بعد سبق الحصول على إذن بذلك من الجهة المختصة[5]، وعلى النقيض من ذلك ما حدث في الولايات المتحدة في قضية Charbonneauبأنّ اشتراك الشخص في

---

[1]– د.خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، مصر، ط1، سنة 2010،ص 34.

[2]- Camille Adaoust, la cybercriminalité tisse sa toile, le 19/07/2014, disponible à l’adresse suivante : www.lefigaro.fr.

[3]–د. شيماء عبد الغني، المرجع السابق، ص 263.

[4]- Valerie Sédaillan, droit de l’internet, Collection AUI, Paris, France, 1997, P 111.

[5]- United States C.Maxwell 45 M.J 406 (1996), available online:www.lex-electronica.org.

نقلا عن: د. شيماء عبد الغني، المرجع السابق، ص 261.

غرفة للمحادثات الفورية بين عدة أشخاص لا يجعل المحادثة حرمة خاصة، وبالتالي لا يلزم سبق الحصول على إذن الإستماع والتسجيل مادام أن الاشتراك في غرف المحادثات الجماعية مسموحا لغيره من الناس[1].

المطلب الثالث: إعتراض الإتصالات السلكية واللاسلكية.

كما سبق الذكر،فإنّ التعديلات الجديدة لقانون الإجراءات الجزائية الجزائري المتضمنة بالقانون رقم (06-22)السالف ذكره تضمنت بعض الصلاحيات الجديدة والمتمثلة في اعتراض الإتصالات السلكية واللاسلكية ولاشك أنّ هذا الإعتراض يتعلق بالمحادثات التي تتم عن طريق الهاتف أي التنصت الهاتفي دون المحادثات التي تتم عن طريق الكمبيوتر والتي تتخذ شكل البريد الإلكتروني أو شكل المحادثات الفورية.

وتأكيدا لهذا الكلام، فقد أصدر المشرع الجزائري القانون رقم (09-04) السالف الذكر والذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وهو يتعلق بالإتصالات الإلكترونية، كما أنّه يجيز مراقبة الإتصالات الإلكترونية مع احترام مجموعة من الضمانات، لذلك تمت التفرقة بين الإتصالات السلكية واللاسلكية والإتصالات الإلكترونية، وإن كان ثمة أوجه للتقارب بينهما.

فبعدما أعطى المشرع الجزائري للمتهم الحق في الصمت، فإنه وبشكل غير مباشر أورد استثناء عن هذا الحق، أين أصبح من الممكن أخذ اعتراف الشخص ضد نفسه بشكل خفي ودون رضاه عن طريق تسجيل كل ما يتفوه به من كلام[2].

ويتجه الفقه في غياب النصوص الصريحة والأحكام القضائية إلى أعمال قواعد المتعلقة بالاختصاص في مراقبة الإتصالات الهاتفية لكي تسري في مجال الإتصالات الإلكترونية، بحيث يتم اتباع نفس الضمانات المقررة للمحادثات الهاتفية، ولكن مادام أنّ المشرع الجزائري قد ميز بينهما، فيتم السير نحو ذات الإتجاه

---

[1] - United States V.Charbonneau (1997), available online:www.lex-electronica.org.

نقلا عن: د. شيماء عبد الغني،المرجع السابق، ص 261.

[2] – أ. فوزي عمارة، إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائية، مجلة العلوم الإنسانية، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، الجزائر، العدد 33، جوان 2010، ص 237.

وذلك بالتفرقة بين الضمانات القانونية لمراقبة المحادثات الهاتفية، والضمانات القانونية لمراقبة الإتصالات الإلكترونية التي تم التطرق إليها وإن كانت متقاربة وتتمثل هذه الضمانات فيما يلي[1]:

أولا:اللجوء إلى هذا الإجراء يكون بناءا على إذن صادر من جهة قضائية مختصة:

تتنازع التشريعات إتجاهات عديدة في تحديد السلطة المختصة بالمراقبة، فمنها من يعهد هذا الإجراء إلى القضاء ومنها ما يخول هذا الإجراء إلى النيابة العامة، على أنّ البعض الآخر يجعل اتخاذ المراقبة مشاركة بين النيابة العامة والسلطة القضائية، وأخيرا تذهب قلة من التشريعات إلى تخويل ضباط الشرطة سلطة المراقبة.

أمّا بالنسبة للقانون الفرنسي فقد نص صراحة على إجازة المراقبة بناءا على أمر مسبب صادر من قاضي التحقيق طبقا للمادة (100)[2] من قانون الإجراءات الجزائية الفرنسي، وبالتالي لا يجوز للنيابة العامة أو رجل الضبط القضائي اتخاذ إجراء المراقبة في أي ظرف من الظروف إلاّ بعد الحصول على إذن من قاضي التحقيق.

وبالنسبة للقانون المصري، فيتضح من خلال نص المادتين (95و206) من قانون الإجراءات الجنائية أنّ المشرع استلزم صدور الإذن بالإعتراض، وذلك للحد من سلطة هذه الأخيرة منعا لأي تعسف، ولكن في حالة ما إذا كانت النيابة العامة تتولى التحقيق بنفسها، وتبين لها ضرورة اعتراض المحادثات الهاتفية للمتهم كان عليها أن تحصل على إذن من القاضي بمراقبة المحادثات الهاتفية.

أمّا بالنسبة للمشرع الجزائري، فقد أجاز لوكيل الجمهورية المختص في حالة التحري في الجريمة المتلبس بها أو التحريات الأولية أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية بعدما كانت هذه العمليات لا يجوز اتخاذها إلاّ على مستوى التحقيق القضائي بموجب أمر من قاضي التحقيق، كما يسمح الإذن المسلم لأجل القيام بالترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو كان ذلك خارج المواعيد المحددة في المادة (47) من هذا القانون ولو كان ذلك بغير علم أو رضا الأشخاص

---

[1]– د. ياسر الأمير فاروق، المرجع السابق، ص 289 و مابعدها.

[2] -Article 100 (C.P.P.F Abrogé par Loi 85-1407 1985-12-30 art. 9 et art. 94 JORF 31 décembre 1985 en vigueur le 1er février 1986, Modifié par Loi n°91-646 du 10 juillet 1991 - art. 2 JORF 13 juillet 1991 en vigueur le 1er octobre 1991) :En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications. Ces opérations sont effectuées sous son autorité et son contrôle.
La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

الذين لهم الحق على تلك الأماكن[1]، على أن تتم هذه العمليات تحت المراقبة المباشرة لوكيل الجمهورية المختص[2].

أمّا في حالة فتح تحقيق قضائي، فإنّ هذه العمليات المذكورة تكون بناءا على إذن من قاضي التحقيق،كما تكون تحت المراقبة المباشرة له وهذا طبقا لنص المادة (65 مكرر 5)[3]من قانون الإجراءات الجزائية الجزائري.

ثانيا: أن يكون الإذن الصادر بالإعتراض مكتوبا ومسببا ومحددا:

لا يجوز أن يصدر الإذن بصورة شفوية، ويجب أن يكون مبنيا على أسباب معقولة خصوصا فيما يتعلق بعدم توافر وسائل أخرى بديلة يمكن اللجوء إليها لإثبات الجريمة، وأن تذكر تلك الأسباب في الإذن، وأن يكون الإذن مشتملا ومتضمنا لكافة المعلومات الضرورية لتحديد نوعية الإتصالات المراد التقاطها، والأماكن المقصودة سكنية أو غيرها، وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير طبقا لنص المادة (65 مكرر 7)[4]من قانون الإجراءات الجزائية الجزائري.

ثالثا:حصر اللجوء إلى هذا الإجراء ببعض الجرائم الخطيرة:

نص المشرع الجزائري في المادة (65 مكرر 5) على نوع الجرائم التي يجوز فيها اعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية، ومن بين هذه الجرائم جرائم المساس بأنظمة المعالجة الآلية للمعطيات[5]، إلاّ أنّ المشرع المصري قد اعتمد على معيار جسامة العقوبة، حيث أقر من خلال نص المادتين

---

[1] – أ. نجيمي جمال، المرجع السابق، ص 445.

[2] – تنص المادة 65 مكرر 5 فقرة 3/2 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري)على ما يلي:" ... يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.

تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص..."

[3] – تنص المادة 65 مكرر 5 فقرة 4 من قانون الإجراءات الجزائية الجزائري على ما يلي: "... في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناءا على إذن من قاضي التحقيق وتحت مراقبته المباشرة."

[4] – تنص المادة 65 مكرر 7 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري)على ما يلي:" يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5 أعلاه، كل العناصر التي تسمح بالتعرف على الإتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها ..."

[5]– تنص المادة 65 مكرر 5 فقرة 1 من قانون الإجراءات الجزائية الجزائري على ما يلي:" إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ... يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي :

– إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية ..."

(95 و206) السابق الإشارة إليهما الجرائم الجائز فيها الإعتراض وهي الجنايات والجنح المعاقب عليها لمدة لا تقل عن ثلاثة أشهر، كما يشترط في الجريمة محل الإعتراض أن تكون قد وقعت فعلا.

رابعا: أن يتم اللجوء إلى هذا الإجراء لمدة معينة:

حيث حدد المشرع الجزائري اللجوء إلى هذا الإجراء لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق وضمن نفس الشروط الشكلية والزمنية طبقا لنص المادة (65 مكرر 7فقرة 2)[1]من قانون الإجراءات الجزائية الجزائري، وكذلك المشرع الفرنسي فقد حددها هو الآخر بأربعة (4) أشهر قابلة للتجديد طبقا لنص المادة (100-2)[2] من قانون الإجراءات الجزائية الفرنسي، أمّا المشرع المصري فقد حددها بثلاثين (30) يوما قابلة للتجديد لمدة أو مدد أخرى طبقا لنص المادتين (95 و206) من قانون الإجراءات الجنائية المصري.

وإذا كانت هذه التدابير تمس بصفة فاضحة بالحريات الفردية، وذلك بفعل الحالة الإستثنائية الناجمة عن مكافحة هذه النوعية من الجرائم التي تتطلب تدابير استثنائية، إلاّ أنّ المشرع قد حافظ على حماية السر المهني من خلال نص المادة (65 مكرر 6)[3] من القانون نفسه، على أن تتم عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور دون المساس بالسرّ المهني المنصوص عليه في المادة (45) من نفس القانون.

ولإنجاز العملية تقنيا، فقد سمح القانون بالإستعانة بكل شخص مؤهل عامل في القطاع العام أو الخاص يتم تسخيره من طرف وكيل الجمهورية أو قاضي التحقيق أو ضابط الشرطة القضائية للقيام بكل التدابير والعمليات التقنية التي تسمح باعتراض المراسلات أو تسجيل الصوت أو الصورة دون علم أو موافقة المعنيين في الأماكن الخاصة أو العامة على السواء[4]، وهذا طبقا لنص المادة (65 مكرر 8)[5]، على أن يتم تحرير محضر بما تسفر عليه العملية وتجمع الدعائم التي سجلت عليها المراسلات أو الصور والأصوات وفقا

---

[1] – تنص المادة 65 مكرر 7 فقرة 2 من قانون الإجراءات الجزائية الجزائري على ما يلي:" ... يسلم الإذن مكتوبا لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية ."

[2]-Article 100-2 (C.P.P.F Créé par Loi n°91-646 du 10 juillet 1991 - art. 2 JORF 13 juillet 1991 en vigueur le 1er octobre 1991) : Cette décision est prise pour une durée maximum de quatre mois. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée.

[3] – تنص المادة 65 مكرر 6 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري)على ما يلي:" تتم العمليات المحددة في المادة 65 مكرر 5 أعلاه ، دون المساس بالسر المهني المنصوص عليه في المادة 45 من هذا القانون ..."

[4]–أ. نجيمي جمال، المرجع السابق، ص 447.

[5] – تنص المادة 65 مكرر 8 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري)على ما يلي:" يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له ، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر أعلاه ."

للمادة (65 مكرر 9)[1] من ذات القانون، إلاّ أنّ المشرع الجزائري لم يبين مصير التسجيلات بعد انتهاء الغرض المقصود منها.

المبحث الثالث: التعاون الدولي في مجال إجراءات جمع الدليل الإلكتروني.

إذا كان التعاون الدولي هو السبيل الفعال لمكافحة الجرائم الالكترونية، فإنّ هذا التعاون يقتضي التخفيف من غلو الفوارق بين الأنظمة العقابية الداخلية، لأن التباعد بين هذه الأنظمة يجعل المجرم المعلوماتي يبحث في الأنظمة القانونية الأكثر تسامحا، ولذلك أبرمت العديد من الإتفاقيات الدولية في مجال التعاون الدولي، تستهدف التقريب بين القوانين الجنائية الوطنية من أجل مكافحة الجرائم العابرة للحدود، وتظهر معالم هذا التقارب في قبول حالات تفويض الإختصاص في اتخاذ إجراءات التحقيق وجمع الأدلة وتسليم المجرمين والإعتراف بالأحكام الجنائية الأجنبية، وهذا التعاون القانوني الدولي لا ينال من سيادة الدولة، على العكس فإنّ انعدام هذا التعاون يزيد من التباعد بين الأنظمة العقابية مما يساعد على تزايد الجرائم الالكترونية.

ويجد هذا التعاون الدولي تبريره في بعض الإعتبارات ومنها:

– أنه يعتبر خطوة على طريق تدويل القانون الجنائي، ذلك أنه ثمة قواعد موضوعية وإجرائية تهيمن على أذهان العديد من المشرعين، ومن شأن تشابه هذه القواعد أن يخلق نوعا من التقارب بين التشريعات الحالية، يجعل الحديث عن توحيد أو تدويل القانون الجنائي أمرا قابلا للتحقيق.

– أنه يعتبر من قبيل التدابير المانعة من ارتكاب الجريمة، لأنّ المجرم يجد نفسه محاطا بسياج مانع من الإفلات من المسؤولية عن الجريمة التي ارتكبها، أو من العقوبة التي حكم عليه بها، ما يحقق الردع الخاص للمجرم المعلوماتي[2].

ففعالية التحقيق والملاحقة القضائية في الجريمة الإلكترونية غالبا ما تقتضي تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالإنترنت، وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الإتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في

---

[1] – تنص المادة 65 مكرر 9 (القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري) على ما يلي:" يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الإلتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري.

يذكر بالمحضر تاريخ وساعة بداية هذه العمليات والإنتهاء منها ."

[2]– د.طارق إبراهيم الدسوقي عطية،المرجع السابق،ص 592.

بلدان مختلفة، ولتحديد مصدر الجريمة غالبا ما يتعين على أجهزة إنفاذ القانون الإعتماد على السجلات التاريخية التي تبين متى أجريت تلك التوصيلات ومن الذي أجراها.

وفي أحيان أخرى قد تتطلب أجهزة إنفاذ القانون تتبع أثر التوصيل ووقت إجرائه وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالبا، فإنّ أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها،بمعنى الحاجة إلى ما يسمى بالتعاون القضائي، ويتمثل في مجموعة من الوسائل القانونية والتي بواسطتها تقدم إحدى الدول معاونة سلطاتها العامة أو مؤسساتها القضائية إلى سلطة التحقيق أو الحكم أو التنفيذ في دولة أخرى[1].

وسوف تقتصر الدراسة في هذا المقام على المساعدة القضائية المتبادلة في المطلب الأول، أما المطلب الثاني فخصص لتسليم المجرمين، كما تم التطرق لصعوبات التعاون في مطلب ثالث، وذلك على النحو التالي:

المطلب الأول: المساعدة القضائية المتبادلة.

الإنترنت ما هي إلاّ شبكة عالمية تمتاز بأنها دولية وأنها عابرة للحدود ولا تعرف للحدود الجغرافية معنى، وبالتالي فإنّ الجرائم المتصلة بها تعتبر هي الأخرى عالمية وذات طابع دولي وأثرها يمتد لأكثر من دولة، لذلك فإنّ ملاحقة مرتكبي هذه الجرائم وتقديمهم للعدالة من أجل توقيع العقاب يستلزم القيام بإجراءات خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها، ومن هذه الإجراءات معاينة مواقع الإنترنت في الخارج أو ضبط الأقراص الصلبة أو تفتيش نظم الحاسب الآلي، وهذا كله قد يصطدم بمشاكل الحدود ولأنه كان كذلك فلا مناص من تقديم المساعدة القانونية المتبادلة[2].

[1]- د.يوسف حسن المصري، المرجع السابق،ص 98.

[2]- د.حسين الغافري، المرجع السابق،ص 643.

وتعرف المساعدة القضائية الدولية بأنها: "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"[1]، وتتخذ المساعدة القضائية في المجال الجنائي صور عدة سيتم التطرق لها على النحو التالي:

أولا: الإنابة القضائية:

تعد الإنابة القضائية إحدى صور المساعدة القضائية للتعاون الدولي،فهي تؤدي إلى تمكين دولة ما من الإستفادة من السلطات العامة أو الهيئات القضائية لدولة أخرى، إذا ما حالت الحدود الإقليمية دون نفاذ قانونها اتجاه الجاني.

ويعرف الفقه الجنائي[2] الإنابة القضائية بأنها طلب اتخاذ إجرائي قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك، للفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها، فالإنابة القضائية تعد من الإجراءات المسهلة لمباشرة الإجراءات الجنائية في النطاق الدولي، والتي تساعد على التغلب على عقبة السيادة الإقليمية بما يكفل إنهاء إجراءات التحقيق والمحاكمة في الدعوى الجنائية.

ويشترط لتنفيذ الإنابات القضائية بين الدول عدة شروط، تتمثل في ضرورة وجود إتفاقيات دولية ثنائية أو جماعية تجيز اتخاذ السلطات القضائية لإجراءات الإنابة القضائية، فضلا عن قيام السلطات القضائية المختصة بإرسال الملف الخاص بالدعوى الجنائية بمرفقاته من مستندات ووثائق ومحاضر تحقيق، والتي تم إجرائها بمعرفة السلطات القضائية في الدولة المطلوب فيها اتخاذ بعض إجراءات التحقيق[3].

غير أنه نظرا لأنّ عامل السرعة يعتبر من العوامل الرئيسية والعامة في مكافحة الجرائم المتعلقة بالإنترنت، ولكون غالبية هذه الإتفاقيات قد صدرت في وقت لم تكن شبكة الإنترنت قد ظهرت أو كانت موجودة ولكنها محدودة، فإنّ تعديل هذه الإتفاقيات التقليدية للتعاون القضائي الدولي أصبح ضرورة ملحة خاصة مع التطور الكبير في تكنولوجيا المعلومات والإتصالات[4].

---

[1]–د. سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، سنة 1997، ص 425. نقلا عن د. حسين الغافري، ص 644.

[2]– د. جميل عبد الباقي الصغير، المرجع السابق، ص 83.

[3]– د.رامي متولي القاضي، مكافحة الجرائم المعلوماتية، المرجع السابق،ص 133.

[4]– د.حسين بن سعيد الغافري، المرجع السابق، ص 648.

ويلاحظ أنّ المشرع الجزائري قد نظم مسألة إجراءات الإنابة القضائية في الباب الثاني من الكتاب السابع من قانون الإجراءات الجزائية، حيث أقر بأنه في حالة المتابعات الجزائية غير السياسية في بلد أجنبي تسلم الإنابات القضائية التي تكون صادرة من بلد أجنبي عبر القنوات الدبلوماسية ويتم إرسالها إلى وزارة العدل، كما تنفذ الإنابات القضائية إذا كان لها محل وفقا للقانون الجزائري مع مراعاة مبدأ المعاملة بالمثل طبقا لنص المادة (721)[1] من نفس القانون.

غير أنه سيتم التطرق إلى أحكام المساعدة المتبادلة في اتفاقية بودابست بشأن الجرائم الإلكترونية،وكذا المساعدة المتبادلة في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات،كما سيتم التطرق لموقف القانون الجزائري.

1- المساعدة المتبادلة في اتفاقية بودابست بشأن الجرائم الإلكترونية.

تخضع المساعدة المتبادلة لقانون الدولة المطلوب منها المساعدة، أو إتفاقية طلب المساعدة الواجبة التطبيق، ولا يجوز رفض المساعدة على أساس أنّ الجريمة تعد جريمة مالية، ويعتبر هذا الشرط مستوفى في حالة وجود جريمة مزدوجة، كما يجوز لأطراف هذه الإتفاقية إخطار الأطراف الأخرى في حالة وجود أو بسبب تحقيق يجرى أو بمعلومات قد تساعده في البدء بالتحقيق أو اتخاذ إجراءات بصدد جرائم تتعلق بهذه الإتفاقية، وعلى الطرف المتلقي الحفاظ على سرية المعلومات،وفي حالة العكس عليه إخطار الطرف المعطى للمعلومات لكي يقرر ما إذا كان ينبغي تقديم هذه المعلومات من عدمه[2].

وقد أفردت المادة (27)[3] من الإتفاقية الإجراءات المتعلقة بالمساعدة القضائية في حالة عدم وجود إتفاقية دولية واجبة التطبيق بشأن الطلبات المتبادلة، ذكرت فيها بعض أسباب الرفض مثلا إذا ما تعلق الطلب بجريمة سياسية، أو أنّ تنفيذ الطلب يمس السيادة أو الأمن أو النظام العام.

---

[1] – تنص المادة 721 من قانون الإجراءات الجزائية الجزائري على ما يلي:" في حالة المتابعات الجزائية غير السياسية في بلد أجنبي، تسلم الإنابات القضائية الصادرة من السلطة الأجنبية بالطريق الدبلوماسي وترسل إلى وزارة العدل بالأوضاع المنصوص عليها في المادة 703 وتنفذ الإنابات القضائية إذا كان لها محل وفقا للقانون الجزائري وكل ذلك بشرط المعاملة بالمثل."

[2]- د. رامي متولي قاضي، المرجع السابق، ص 136.

[3]- Article 27 du C.C.C :- En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

- Outre les conditions ou motifs de refus prévus à l'Article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise :

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

2- المساعدة المتبادلة في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات:

أشارت نصوص الإتفاقية العربية إلى أحكام المساعدة في نطاق الجرائم الالكترونية، حيث نصت المادة (32)[1] على حث الدول الأطراف على تقديم المساعدة المتبادلة لغايات التحقيق، وجمع الأدلة في الجرائم الالكترونية، وقد اشترطت المادة ضرورة تقديم طلب خطي للمساعدة المتبادلة على أن تخضع شروط المساعدة لقانون الدولة المطلوب منها المساعدة، كما نصت المادة (33)[2] على جواز إعطاء أية معلومات حصلت عليها الدولة أثناء التحقيقات إلى دولة أخرى طرف في الإتفاقية.

بالإضافة إلى اتخاذ الإجراءات الخاصة بتحديد سلطة محددة تختص بإجراءات المساعدة المتبادلة، كما أشارت الإتفاقية إلى حق الدولة في رفض المساعدة في حالة الجرائم ذات الطابع السياسي أو إذا كانت المساعدة تمثل انتهاكا لأمن هذه الدولة طبقا لنص المادة (35)[3] من نفس الإتفاقية[4].

وما ينبغي الإشارة إليه أن الجزائر وقعت على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات ولكن لم تصادق عليها، ومادام أن الأمر كذلك فإذا اتخذت الجريمة الإلكترونية طابع الجريمة المنظمة فيجب الرجوع إلى إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000بما في ذلك التعاون الدولي، فتنص هذه الإتفاقية على المساعدة القانونية المتبادلة في التحقيقات والملاحقات والإجراءات القضائية طبقا لنص المادة (18)، ويتم تعزيز التعاون مع أجهزة إنفاذ القانون من أجل الإدلاء بمعلومات مفيدة بموجب نص المادة (26).

أما إذا كانت الجريمة الإلكترونية جريمة عادية، فينبغي تطبيق أحكام القانون الجزائري في حالة عدم وجود إتفاقيات لهذا الغرض.

---

b. si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels….

[1] - تنص المادة 32 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي:" على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم..."

[2] - تنص المادة 33 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي:" يجوز لأي دولة طرف ضمن حدود قانونها الداخلي وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن يساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الإتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف ..."

[3]- تنص المادة 35 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي:" يجوز للدولة الطرف المطلوب منها المساعدة أن ترفض المساعدة إذا :

-كان الطلب متعلقا بجريمة يعتبرها قانون الدولة الطرف المطلوب منها المساعدة جريمة سياسية .

-إعتبر أن تنفيذ الطلب يمكن أن يشكل إنتهاكا لسيادته أو أمنه أو نظامه أو مصالحه الأساسية ."

[4]- د. رامي متولي قاضي، المرجع السابق،ص 136.

3- المساعدة المتبادلة في القانون الجزائري.

لقد نص القانون رقم (04/09) الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها على ضرورة المساعدة القضائية الدولية المتبادلة، بحيث أنه يمكن للسلطات المختصة تبادل المساعدة القضائية لجمع الأدلة الخاصة بالجريمة الالكترونية، لكن نظرا للطابع الخاص لهذه النوعية من الجرائم،وما تتميز به شبكة الإنترنت من سرعة وخوفا من العبث بالأدلة الالكترونية يمكن تقديم طلبات المساعدة عن طريق وسائل الإتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها، وكل ذلك مع مراعاة الإتفاقيات الدولية ومبدأ المعاملة بالمثل[1].

غير أنّ هذه الطلبات يمكن أن ترفض في حالة ما إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام، كما يجوز للدول التي تقدم المساعدة أن تفرض شروطا تتمثل في المحافظة على سرية المعلومات المبلغة وكذا اشتراط عدم استعمالها في غير ما هو موضوع في الطلب[2].

ثانيا: تبادل المعلومات:

وهو يشمل تقديم المعلومات والبيانات والوثائق التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الإتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم،وقد يشمل التبادل السوابق القضائية للجناة، ولهذه الصورة من صور المساعدة القضائية الدولية صدى كبير في مثل هذه الإتفاقيات مثل معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية[3]،وكذا منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي[4]، وذات الصورة نجدها في المادة الأولى من إتفاقية الرياض العربية للتعاون

---

[1]- تنص المادة 16 من القانون رقم 04/09 السالف الذكر على ما يلي:" ... يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني .

يمكن في حالة الإستعجال ، ومع مراعاة الإتفاقيات الدولية ومبدأ المعاملة بالمثل ، قبول طلبات المساعدة القضائية ...إذا وردت عن طريق وسائل الإتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني ...".

[2]- تنص المادة 18 من القانون رقم 04/09 السالف الذكر على ما يلي:" يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام .

يمكن أن تكون الإستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب"

[3]- صدرت هذه المعاهدة في 1990/12/14 في الجلسة العامة 68 للجمعية العامة للأمم المتحدة، وتقضي باتفاق أطرافها على أن يقدم كل منهم للأخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات، أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخل في اختصاص السلطة القضائية في الدولة الطالبة للمساعدة.نقلا عن: د. حسين الغافري، المرجع السابق، ص 645.

[4]- صدرت هذه المعاهدة واعتمدت سنة 1999 من قبل مؤتمر وزراء خارجية دول المنظمة في اجتماعهم المنعقد في واغادوغو في الفترة من 1999/06/28 إلى 1999/07/01.نقلا عن: د. حسين الغافري، المرجع السابق، ص 645.

القضائي[1]، والمادة الأولى والثانية من النموذج الاسترشادي واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في البنود الثالث والرابع والخامس من المادة الثامنة منها[2].

وبالرجوع إلى القانون الجزائري رقم (09-04)، فقد نص على ضرورة الإستجابة لطلبات المساعدة المتمثلة في تبادل المعلومات أو اتخاذ أي إجراءات تحفظية، وفقا للإتفاقيات الدولية ذات الصلة، وكذا الإتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل[3].

ثالثا: نقل الإجراءات.

ويقصد بها قيام دولة ما بناءا على إتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة، متى توافرت شروط معينة من أهمها التجريم المزدوج ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة أو الدولة مطلوب إليها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة، وكذلك أن تكون الإجراءات المطلوب اتخاذها تؤدي دورا مهما في الوصول إلى الحقيقة.

ولقد أقرت العديد من الإتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية[4]، وإتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في المادة (21) منها وكذا معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي سنة 1999 في المادة (9) منها،وأيضا المادة (16) من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي سنة 2003[5].

---

[1]- صدرت هذه الإتفاقية في 1993/04/06 بمدينة الرياض بالمملكة العربية السعودية.

[2]- د.يوسف حسن المصري، المرجع السابق، ص 103.

[3]- تنص المادة 17 من القانون رقم 04/09 السالف الذكر على ما يلي: "تتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للإتفاقيات الدولية ذات الصلة والإتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل ".

[4]-إعتمدت بموجب قرار الجمعية العامة للأمم المتحدة رقم 45/118 بتاريخ 1990/12/14 . نقلا عن: حسين الغافري، المرجع السابق، ص646.

[5]- د. حسين بن سعيد الغافري، المرجع السابق، ص 646.

المطلب الثاني : تسليم المجرمين.

إستقر فقه القانون الدولي على اعتبار تسليم المجرمين شكلا من أشكال التعاون الدولي في مكافحة الجريمة والمجرمين وحماية المجتمعات من المخلين بأمنها واستقرارها،وهذا النوع من التعاون الدولي هو نتيجة طبيعية للتطورات التي حدثت في كافة المجالات ومنها مجالات الإتصالات وتقنية المعلومات،حيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم وهذا ينطبق بالفعل على الجرائم الإلكترونية.

ويعرف نظام تسليم المجرمين بأنه قيام دولة ما(الدولة المطلوب منها التسليم) بتسليم شخص موجود في إقليمها إلى دولة أخرى (الدولة طالبة التسليم) بناء على طلبها بغرض محاكمته عن جريمة نسب إليه ارتكابها ولتنفيذ حكم صادر ضده من محاكمها، بمعنى آخر تسليم دولة لدولة أخرى شخصا منسوبا إليه إقتراف جريمة ما أو صدر ضده حكما بالعقاب كي تتولى محاكمته أو تنفيذ العقاب عليه[1].

وسيتم التطرق من خلال هذا المطلب إلى مصادر وأنظمة تسليم المجرمين وكيفية تسليمهم في اتفاقية بودابست بشأن الجرائم الإلكترونية والإتفاقية العربية لمكافحة جرائم تقنية المعلومات، وكذا معرفة موقف القانون الجزائري وذلك على النحو التالي:

الفرع الأول: مصادر وأنظمة تسليم المجرمين.

فيما يتعلق بمصادر هذا النظام، فهي ليست واحدة في كافة التشريعات، وإنما تختلف باختلاف الدول، إلاّ أنه وبشكل عام يمكن حصرها في ثلاثة مصادر هي[2]:

1- **المعاهدات والإتفاقيات الدولية:** وهي تنقسم إلى ثلاثة أنواع: إتفاقيات التسليم الثنائية وهي التي تتم بين دولتين وفقا للشروط والضوابط الموضوعة من قبلهما، إتفاقيات التسليم المتعددة الأطراف وهي إتفاقيات يكون أطرافها عدة دول، أمّا الإتفاقيات الدولية فهي إتفاقيات دولية تتضمن أحكاما متصلة بتسليم المجرمين دون أن تكون بحد ذاتها إتفاقيات تسليم[3]، والجدير بالذكر أنّ منظمة الأمم المتحدة وضعت سنة 1990 معاهدة نموذجية لتسليم المجرمين لتكون إطارا يساعد الدول التي بصدد التفاوض على اتـفاقيات

---

[1]–د. حسين بن سعيد الغافري، المرجع السابق، ص 649.

[2]–د. يوسف حسن المصري، المرجع السابق، ص 108 وكذلك: د. حسين الغافري، المرجع السابق، ص 653.

[3]– ومن الأمثلة على هذا النوع من الإتفاقيات : الإتفاقية العربية لمكافحة الإرهاب سنة 1998، إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000، الإتفاقية الأوروبية بشأن الجرائم الإلكترونية سنة 2001 .

التسليم الثنائية، وتتكون من 18 مادة بالإضافة إلى ملحق صدر لها عام 1997 يتضمن بعض الأحكام التكميلية، كما أنّ مجلس وزراء الداخلية العرب أقر قانونا نموذجيا لتسليم المجرمين.

2- **القوانين الداخلية التي تنظم تسليم المجرمين:** إنّ أغلب الدول لديها قوانين تسليم المجرمين.

3- **العرف الدولي**:والذي يطبق في حالة عدم وجود إتفاقيات أو قوانين داخلية.

كما تتنوع أنظمة تسليم المجرمين،وتختلف كل دولة في الطريقة التي تبحث بها طلب التسليم بحسب نوع النظام الذي تأخذ به، وهناك ثلاثة أنظمة متبعة في تسليم المجرمين هي[1]:

1- التسليم القضائي:

يقوم هذا النظام على أساس احترام حقوق الأفراد وصيانة حرياتهم،لذا تعتبر السلطة القضائية هي الجهة الوحيدة المختصة بإصدار قرار التسليم ولا شأن لجهة الإدارة في هذا الخصوص، والدولة التي تأخذ هذا الاتجاه تنتهج في التنفيذ أحد النهجين: الأول أن تكون المحكمة هي الجهة الوحيدة المختصة إصدار قرار التسليم للدولة الطالبة، ولا دخل للنيابة العامة في إصدار هذا القرار وإنما يقتصر عملها على تلقي طلب التسليم من الجهة المختصة، وتعد أوراق الموضوع للعرض على المحكمة المختصة لتتولى الأخيرة عملية إصدار القرار النهائي حول هذا الطلب،والنهج الثاني يتمثل في إعطاء النائب العام في الدول المطلوب منها التسليم سلطة الفصل في إصدار القرار النهائي من عدمه.

2- التسليم الإداري:

إنّ تسليم المجرمين يعد وفقا لهذا النظام عملا من أعمال السيادة أو تدبيرا من تدابير السلطة التنفيذية التي تملك الصلاحية المطلقة لتقرر التسليم من عدمه وفقا لاعتبارات سياسية أو إدارية وغير ذلك من الإعتبارات، ويتطلب ذلك أن توجه أجهزة الإنتربول بالدولة طالبة التسليم طلبها بشأن القبض على المتهم إلى أنتربول الدولة المطلوب منها التسليم، والتي تحيل الطلب إلى السلطة الإدارية المختصة للدراسة والبحث، ومن تم إصدار القرار.

---

[1]- د. سراج الدين محمد الروبي، الإنتربول وملاحقة المجرمين، الدار المصرية اللبنانية، القاهرة، مصر، ط1، سنة 1998، ص15. وكذلك: د. عبد الجابر اسماعيل، محاضرات في قانون تسليم المجرمين، أكاديمية الشرطة الملكية، الأردن، ط1، بدون سنة، ص 26. نقلا عن: د.حسين بن سعيد الغافري، المرجع السابق، ص 654-657.

3- التسليم المختلط:

يجمع بين الجانبين القضائي والإداري، وهو الأكثر رواجا وانتشارا حيث يوازي بين المصلحتين المتعارضتين، مصلحة الدولة طالبة التسليم ومصلحة الشخص المطلوب تسليمه،فيكون للسلطة القضائية حق فحص الطلب، ويمنح الشخص المراد تسليمه كل الضمانات القانونية للدفاع، بشرط ألاّ تقوم الدولة المطلوب منها التسليم نفسها في فحص وقائع الدعوى وتكتفي بما يرد إليها من مستندات ووثائق من الدولة الطالبة[1].

الفرع الثاني: تسليم المجرمين في الإتفاقيات المتعلقة بالجرائم الإلكترونية.

سيتم التطرق من خلال هذا الفرع إلى كيفية تسليم المجرمين في إتفاقية بودابست بشأن الجرائم الإلكترونية وكذلك في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، وذلك على النحو التالي:

أولا:تسليم المجرمين في إتفاقية بودابست بشأن الجرائم الإلكترونية.

نصت الإتفاقية على انطباقها في حالة ما إذا كانت الجرائم المنصوص عليها في هذه الإتفاقية معاقب عليها بموجب قوانين كلا من الطرفين بعقوبة مقيدة للحرية لمدة سنة على الأقل أو بعقوبة أشد،وتطبق العقوبة الأقل في حالة إذا ما كان توجد تشريعات موحدة أو متبادلة بالمثل أو بموجب إتفاقية تسليم، وقد اعتبرت الإتفاقية الجرائم المنصوص عليها في المواد من (2-13)[2]من الجرائم التي يجب تسليم المجرمين فيها، إذا ما وجدت اتفاقية لتسليم المجرمين بين الأطراف، وفي حالة عدم وجود إتفاقية تسليم مجرمين بين الأطراف، يجوز اعتبار هذه الإتفاقية الأساس القانوني لعملية التسليم.

فالدول بانضمامهم لهذه الإتفاقية يعتمدون الجرائم المنصوص عليها في الإتفاقية كجرائم يجوز فيها تسليم المجرمين، ويخضع تسليم المجرمين لقانون الدولة المطلوب منها التسليم أو إتفاقية تسليم المجرمين الواجبة التطبيق، وفي حالة الرفض بسبب الجنسية أو الإختصاص القضائي،فإنّ الدولة المراد التسليم منها تحيل الدعوى لسلطاتها المختصة وإبلاغ النتيجة للدول الطالبة، وعلى الدول عند التوقيع أن تخطر السكرتير العام لمجلس أوروبا باسم السلطة المسؤولة عن طلبات التسليم.

---

[1]- د.حسين بن سعيد الغافري، المرجع السابق، ص 657.

[2]- هذه الجرائم هي الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية (المواد من 2-6)، الجرائم المعلوماتية (الجرائم المتصلة بالحاسب المواد من (7-8)، الجرائم المتصلة بالمحتوى(المادة9)، الجرائم المتصلة بالإعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة (المادة10)، الشروع والإشتراك (المادة11).أنظر إتفاقية بودابست بشأن الجرائم الإلكترونية على الموقع: http://convention.coe.int/treaty/en/treaties/html/185.htm

ثانيا: تسليم المجرمين في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

نصت الإتفاقية العربية على إجراء تسليم المجرمين، وقد أشارت المادة (31 فقرة 1)[1]من الإتفاقية إلى جواز الإعتداد بالإتفاقية كأساس قانوني بين الدول الأطراف في مسألة تسليم المجرمين، وحددت شروط التسليم بألاّ تكون الجريمة المطلوب فيها التسليم لا تقل عقوبتها عن عقوبة سالبة للحرية لمدة سنة أو أكثر.

فضلا عن خضوع التسليم للشروط المنصوص عليها في الدولة التي يقدم إليها طلب التسليم، مع تقرير حق الدول في رفض طلب التسليم مع التعهد بتوجيه الإتهام للجناة الذين يرتكبون جرائم معاقب عليها وفقا لقانون الدولتين بعقوبة لا تقل عن سنة أو بعقوبة أشد لدى أي من الدولتين[2]طبقا لنص المادة (31فقرة 5)[3] من نفس الإتفاقية.

غير أنه إذا اتخذت الجريمة الإلكترونية طابع الجريمة المنظمة، فيتم تطبيق أحكام تسليم المجرمين التي نصت عليها إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية إذ تطبق المادة (16) من هذه الإتفاقية على الجرائم المذكورة فيها، و على وجود الشخص الذي هو موضوع طلب التسليم في إقليم الدولة الطرف متلقية الطلب شريطة أن يكون الجرم الذي يلتمس بشأنه التسليم معاقبا عليه بمقتضى القانون الداخلي لكل من الدولة الطرف الطالبة والدولة الطرف متلقية الطلب.

كما تعمل كل دولة طرف على إنشاء أو تطوير أو تحسين برنامج تدريب خاص للعاملين في أجهزتها المعنية بإنفاذ القانون كإعارة الموظفين وتبادلهم، وتتناول تلك البرامج على وجه الخصوص المعدات والأساليب الحديثة لإنفاذ القانون بما في ذلك المراقبة الإلكترونية والتسليم المراقب[4] طبقا لنص المادة (29) من الإتفاقية المذكورة.

---

[1]– تنص المادة 31 فقرة 1 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي:" هذه المادة تنطبق على تبادل المجرمين بين الدول الأطراف على الجرائم النصوص عليها في الفصل الثاني من هذه الإتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الأطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد ...".

[2] – د. رامي متولي قاضي، المرجع السابق،ص 137.

[3]– تنص المادة 31 فقرة 5 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي:"...يخضع تسليم الجرمين للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة بما في ذلك الأسس التي يمكن للدولة الطرف الإستناد عليها لرفض تسليم المجرمين ...".

[4] – التسليم المراقب هو الأسلوب الذي يسمح لشحنات غير مشروعة أو مشبوهة بالخروج من إقليم دولة أو أكثر أو المرور عبره أو دخوله، بمعرفة سلطاته المختصة و تحت مراقبتها، بغية التحري عن جرم ما وكشف هوية الأشخاص الضالعين في ارتكابه. أنظر المادة 02 من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000.

أما إذا كانت الجريمة الإلكترونية جريمة عادية و ليست منظمة، فيجب حينها الرجوع إلى القانون الجزائري فيما يتعلق بتسليم المجرمين وذلك ما لم تنص الإتفاقيات على خلاف ذلك،وهذا ما سأتطرق إليه في هذا الفرع.

الفرع الثالث: تسليم المجرمين في القانون الجزائري.

يوجد في القانون الجزائري شروط لتسليم المجرمين لابد من وجودها وإجراءات معينة لا يتم التسليم دونها، وذلك على النحو التالي:

البند الأول: شروط التسليم.

إنّ شروط التسليم لها أهمية في كونها تفصل حدود العلاقة بين الدول الأطراف في عملية التسليم، وتضع الأحكام العامة التي على أساسها سيتم التسليم من عدمه، وذلك متى توافرت هذه الشروط حال البث في قرار التسليم وتتمثل فيما يلي:

أولا: التجريم المزدوج.

والمقصود به أن يكون الفعل المطلوب التسليم من أجله مجرما في تشريع الدولة طالبة التسليم،وكذلك في تشريع الدولة المطلوب إليها التسليم[1]، بحيث لا يجوز قبول التسليم في أية حالة إذا كان الفعل غير معاقب عليه طبقا للقانون الجزائري بعقوبة جناية أو جنحة وفقا المادة(2/697)[2] من قانون الإجراءات الجزائية.

ومع ذلك فإنّ شرط ازدواج التحريم قد يكون عقبة في مجال تسليم المجرمين، لأنه بالرجوع إلى التشريعات العقابية الوطنية يلاحظ أنّ الجرائم الإلكترونية غير معاقب عليها في معظم الدول من ناحية، وأنه من الصعب تحديد في تشريعات الدولة المطلوب إليها التسليم ما إذا كانت النصوص التقليدية لديها يمكن أن تطبق على جرائم شبكات الحاسبات الآلية والإنترنت من عدمه من ناحية أخرى، بمعنى أنه من الصعب البحث في تشريعات الدول المطلوب إليها التسليم عما إذا كانت تشريعاتها التقليدية يمكن أن تطبق على

[1]– د. يوسف حسن المصري، المرجع السابق، ص 111.

[2] – تنص المادة 697 فقرة 2 من قانون الإجراءات الجزائية الجزائري على ما يلي:" ...ولا يجوز قبول التسليم في أية حالة إذا كان الفعل غير معاقب عليه طبقا للقانون الجزائري بعقوبة جناية أو جنحة...".

الجرائم الالكترونية، وتوجد بالفعل بعض الإتفاقيات الدولية الثنائية التي تحدد الجرائم التي لا تتطلب فيها ازدواجية التجريم ومنها الجرائم الالكترونية[1]، مثال ذلك الإتفاقية الثنائية المتعلقة بالمساعدة القانونية المتبادلة والتي تم توقيعها بين أمريكا وكندا.

ثانيا: الشروط المتعلقة بالأشخاص المطلوب تسليمهم[2]:

1. عدم جواز تسليم الجزائريين: من المبادئ السائدة والمستقر عليها في المجتمع الدولي والتي نص عليها القانون الجزائري، مبدأ عدم جواز تسليم الرعايا أيا كان نوع الجريمة المرتكبة من قبلهم وفي أي إقليم خارج دولتهم، فإذا كان هذا الشخص المطلوب تسليمه جزائري الجنسية فلا يقبل تسليمه، والعبرة في تقدير هذه الصفة بوقت وقوع الجريمة المطلوب التسليم من أجلها[3].

2. عدم جواز تسليم ممنوحي حق اللجوء السياسي: هذا المبدأ هو الآخر سائد في أغلب التشريعات والإتفاقيات الدولية والإقليمية وقد أكدت عليه الفقرة الثانية من المادة (698)[4] من قانون الإجراءات الجزائية، بحيث إذا تبين من الظروف أن التسليم الذي يكون مطلوبا بالغرض سياسي فلا يقبل.

3. عدم جواز تسليم من تمت محاكمتهم عن ذات الجريمة المطلوب تسليمهم لأجلها: ولو كانت قد ارتكبت خارج الأراضي الجزائرية[5].

ثالثا: الشروط المتعلقة بالجريمة المطلوب التسليم لأجلها: لا يجوز التسليم إلاّ إذا كانت الجريمة قد ارتكبت إمّا في أراضي الدولة الطالبة من أحد رعاياها أو من أحد الأجانب، وإمّا خارج أراضيها من أحد رعايا هذه الدولة وإمّا خارج أراضيها من أحد الأجانب عن هذه الدولة، وهذا إذا كانت الجريمة من عداد الجرائم التي يجيز القانون الجزائري المتابعة فيها في الجزائر حتى ولو ارتكبت من أجنبي في الخارج طبقا لما تقضي به المادة (2/696)[6] من قانون الإجراءات الجزائية الجزائري، وبالرجوع إلى القانون رقم(09-04) تكون المحاكم

---

[1]–د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 414.

[2]– د.حسين الغافري، المرجع السابق، ص 363 و ما بعدها.

[3]– تنص المادة (01/698) من قانون الإجراءات الجزائية الجزائري على ما يلي: " لا يقبل التسليم إذا كان الشخص المطلوب تسليمه جزائري الجنسية والعبرة في تقدير هذه الصفة بوقت وقوع الجريمة المطلوب التسليم من أجلها..."

[4] –تنص المادة 698 فقرة 2 من قانون الإجراءات الجزائية الجزائري على ما يلي: " ...لا يقبل التسليم إذا كانت للجناية أو الجنحة صيغة سياسية أو إذا تبين من الظروف أن التسليم مطلوب لغرض سياسي..."

[5]– تنص المادة 698 فقرة 4 من قانون الإجراءات الجزائية الجزائري على ما يلي: " ...لا يقبل التسليم إذا تمت متابعة الجناية أو الجنحة و الحكم فيها نهائيا في الأراضي الجزائرية ولو كانت قد ارتكبت خارجها ..."

[6] – تنص المادة696 فقرة 2 من قانون الإجراءات الجزائية الجزائري على ما يلي : "... ومع ذلك لا يجوز التسليم إلا إذا كانت الجريمة موضوع الطلب قد ارتكبت:

الجزائرية مختصة بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني طبقا لنص المادة (15) من القانون السالف الذكر.

كما تحدد المادة (1/697)[1] من ذات القانون الأفعال التي تجيز التسليم، ومن بينها جميع الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة الجناية، وكذا الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جنحة إذا كان الحد الأقصى للعقوبة المطبقة وفقا لنصوص ذلك القانون سنتين أو أقل، أو إذا تعلق الأمر بمتهم قضي عليه بالعقوبة إذا كانت العقوبة التي قضي بها من الجهة القضائية للدولة الطالبة أو تتجاوز الحبس لمدة شهرين ، فالمشرع الجزائري في هذه الحالة اعتمد على أسلوب جسامة الجريمة أو الحد الأقصى للعقوبة المقررة للجرائم التي يمكن أن يتم التسليم لأجلها، كما يشترط ألا تكون الجناية أو الجنحة قد ارتكبت في الأراضي الجزائرية، لأنه لو كانت كذلك فلا يقبل التسليم طبقا للمادة (3/698)[2] من قانون الإجراءات الجزائية الجزائري،وكذا عدم انقضاء الدعوى العمومية أو العقوبة بأحد أسباب الانقضاء كالتقادم[3] أو العفو[4].

– إما في أراضي الدولة الطالبة من أحد رعاياها أو من أحد الأجانب .

– وإما خارج أراضيها من أحد رعايا هذه الدولة .

– وإما خارج أراضيها من أحد الأجانب عن هذه الدولة إذا كانت الجريمة من عداد الجرائم التي يجيز القانون الجزائري المتابعة فيها في الجزائر حتى ولو ارتكبت من أجنبي في الخارج ."

[1] –تنص المادة 697 فقرة 1 من قانون الإجراءات الجزائية الجزائري على ما يلي:" الأفعال التي تجيز التسليم سواء كان مطلوبا أو مقبولا هي الآتية :

– جميع الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جناية .

– الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جنحة إذا كان الحد الأقصى للعقوبة المطبقة طبقا لنصوص ذلك القانون سنتين أو أقل، أو إذا تعلق الأمر بمتهم قضي عليه بالعقوبة إذا كانت العقوبة التي قضي بها من الجهة القضائية للدولة الطالبة تساوي أو تجاوز الحبس لمدة شهرين ..."

[2] – تنص المادة 698 فقرة 3 من قانون الإجراءات الجزائية الجزائري على ما يلي: "...لا يقبل التسليم إذا ارتكبت الجناية أو الجنحة في الأراضي الجزائرية..."

[3] – تنص المادة 698 فقرة 5 من قانون الإجراءات الجزائية الجزائري على ما يلي:"...لا يقبل التسليم إذا كانت الدعوى العمومية قد سقطت بالتقادم قبل تقديم الطلب أو كانت العقوبة قد انقضت بالتقادم قبل القبض على الشخص المطلوب تسليمه ...".

[4]–تنص المادة 698 فقرة 6 من قانون الإجراءات الجزائية الجزائري على ما يلي:"...لا يقبل التسليم إذا صدر عفو في الدولة الطالبة أو الدولة المطلوب إليها التسليم ...".

البند الثاني: إجراءات التسليم.

يقصد بمراحل وإجراءات التسليم تلك القواعد ذات الطبيعة الإجرائية التي تتخذها الدول الأطراف في عملية التسليم وفقا لقوانينها الوطنية وتعهداتها لأجل إتمام عملية التسليم، بهدف التوفيق بين المحافظة على حقوق الإنسان وحريته وبين تأمين الصالح العام الناشئ عن ضرورات التعاون الدولي، وتتمثل فيما يلي[1]:

أولا: إجراءات الدولة طالبة التسليم.

يعتبر طلب التسليم الأداة التي من خلاله تعبر الدولة الطالبة صراحة عن رغبتها في استلام الشخص المطلوب، فبدونه لا يمكن أن ينشأ الحق في التسليم،فيوجه الطلب إلى الحكومة الجزائرية بالطريق الدبلوماسي، ويرفق هذا الطلب الحكم الصادر بالعقوبة حتى لو كان غيابيا، وكذا أوراق الإجراءات الجزائية التي صدر بها الأمر رسميا بإحالة المتهم إلى جهة القضاء الجزائي أو التي تؤدي إلى ذلك بقوة القانون، وكذلك يرفق أمر القبض الذي يكون صادرا من سلطة مختصة على أن تتضمن كل هذه الأوراق بيانا دقيقا للفعل وكذا تاريخ هذا الفعل، كذلك يشترط على الدولة الطالبة التسليم أن ترفق الطلب بصورة من النصوص القانونية التي تعاقب على الفعل مع بيان وقائع الدعوى[2].

ثانيا: إجراءات الدولة المطلوب منها التسليم.

تتمثل المرحلة الأولى في تلقي الطلب، بحيث يتولى وزير الخارجية تحويل طلب التسليم بعد فحص المستندات ومعه الملف إلى وزير العدل الذي يتحقق من سلامته ويعطيه خط السير الذي يتطلبه القانون[3]،ليتم بعد ذلك استجواب الأجنبي المقبوض عليه للتحقق من شخصيته ويحرر محضر بهذه الإجراءات[4]،لينقل بعد ذلك الشخص المطلوب تسليمه في أقصر أجل ويحبس في سجن العاصمة[5]،أمّا المرحلة الثالثة فتتمثل في تحويل المستندات إلى النائب العام للمحكمة العليا الذي يقوم باستجواب الأجنبي ويحرر بذلك محضر خلال أربعة

---

[1]–د. حسين بن سعيد الغافري، المرجع السابق، ص 668.

[2]– طبقا لنص المادة702 من قانون الإجراءات الجزائية الجزائري .

[3]– تنص المادة703 من قانون الإجراءات الجزائية الجزائري على ما يلي" يتولى وزير الخارجية تحويل طلب التسليم بعد فحص المستندات ومعه الملف إلى وزير العدل الذي يتحقق من سلامة الطلب ويعطيه خط السير الذي يتطلبه القانون ."

[4]– تنص المادة704 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يقوم النائب العام باستجواب الأجنبي للتحقق ن شخصيته ويبلغه المستند الذي قبض عليه بموجبه وذلك خلال الأربع والعشرين ساعة التالية للقبض عليه، ويحرر محضر بهذه الإجراءات ."

[5]– تنص المادة705 من قانون الإجراءات الجزائية الجزائري على ما يلي:" ينقل الأجنبي في أقصر أجل ويحبس في سجن العاصمة ".

وعشرين (24)ساعة[1]، على أن يتم رفع المحاضر وكافة المستندات إلى الغرفة الجنائية بالمحكمة العليا ليمثل أمامها الأجنبي في ميعاد أقصاه ثمانية (08) أيام، ويجوز الإفراج عنه في أي وقت أثناء الإجراءات[2].

أمّا إذا رأت المحكمة العليا أنّ الشروط القانونية غير متوافرة، أو أنّ الأدلة الواردة في طلب التسليم غير كافية لثبوت الجريمة فلها أن تصدر رأيا مسببا برفض طلب التسليم ويكون نهائيا ولا يجوز قبول التسليم[3].

وتجدر الإشارة هنا أنه في حالة الموافقة على التسليم، فإنّ القانون الجزائري أوجب على الدولة طالبة التسليم أن تتقدم لاستلامه خلال ميعاد شهر من تاريخ تبليغ الموافقة، وإلا يجب إخلاء سبيله، ولا يجوز المطالبة به بعد ذلك لنفس السبب[4].

المطلب الثالث:صعوبات التعاون الدولي في الجرائم الالكترونية.

تثور بعض المشكلات القانونية التي من شأنها أن تحد من التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، وترتبط هذه المشكلات ببعض العقبات العملية والقانونية التي تظهر في مجال الجريمة الالكترونية، ومن بين هذه الصعوبات ما يلي:

أولا: عدم الإتفاق على مفهوم موحد للجريمة الالكترونية.

بالنظر للأنظمة القانونية القائمة في الكثير من الدول،يتضح من خلالها عدم وجود إتفاق موحد بين الدول حول ماهية الجريمة الإلكترونية ونماذج إساءة استخدام نظم المعلومات والإنترنت،فما يكون مباحا في أحد الأنظمة يكون مجرما وغير مباح في نظام آخر نتيجة لاختلاف السياسة التشريعية من مجتمع لآخر[5]،

---

[1]– تنص المادة706 من قانون الإجراءات الجزائية الجزائري على ما يلي:" تحول في الوقت ذاته المستندات المقدمة تأييدا لطلب التسليم إلى النائب العام لدى المحكمة العليا الذي يقوم باستجواب الأجنبي ويحرر بذلك محضرا خلال أربع وعشرين ساعة ".

[2]– تنص المادة 707 من قانون الإجراءات الجزائية الجزائري على ما يلي: " ترفع المحاضر المشار إليها أعلاه وكافة المستندات الأخرى في الحال إلى الغرفة الجنائية بالمحكمة العليا ويمثل الأجنبي أمامها في ميعاد أقصاه ثمانية أيام تبدأ من تاريخ تبليغ المستندات ، ويجوز أن يمنح مدة ثمانية أيام قبل المرافعات وذلك بناءا على طلب النيابة العامة أو الأجنبي ...".

[3]– تنص المادة 710من قانون الإجراءات الجزائية الجزائري على ما يلي:" إذا أصدرت المحكمة العليا رأيا مسببا برفض طلب التسليم فإن هذا الرأي يكون نهائيا ولا يجوز قبول التسليم ."

[4]– تنص المادة 711 من قانون الإجراءات الجزائية الجزائري على ما يلي:" في الحالة العكسية يعرض وزير العدل للتوقيع إذا كان هناك محل لذلك ، مرسوما بالإذن بالتسليم ، وإذا انقضى ميعاد شهر من تاريخ تبليغ هذا المرسوم إلى حكومة الدول الطالبة دون أن يقوم ممثلو تلك الدولة باستلام الشخص المقرر تسليمه فيفرج عنه، ولا يجوز المطالبة به بعد ذلك لنفس السبب".

[5]– أنظر على التوالي: د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص412. و كذلك : Véronique Arène, les pertes liées à la la cybercriminalité, le 10/06/2014, disponible à l'adresse suivante : www.lemondeinformatique.fr.

ومن تلك الأفعال التي تختلف في شأنها النظرة بين الدول عرض الصور الجنسية الفاضحة وانتقاد نظام الحكم الداخلي، فبينما تتساهل بعض الدول في عرض هذه الصور، فإن دولا أخرى تتشدد في حظرها.

ويؤدي غياب الإتفاق على الأفعال التي تعتبر جرائم وتلك التي تفلت من التجريم إلى عدم وجود إجماع على مكافحة تلك الأفعال على مستوى الدول المختلفة، ومن شأن ذلك أن يؤدي إلى عدم التعاون الدولي في مكافحة هذا النوع من الأفعال[1].

ثانيا: صعوبة معرفة الفاعل أحيانا.

كثيرا ما يتخذ الفاعل احتياطات تكفل صعوبة التوصل إلى الكشف عن شخصيته وذلك بالخصوص عبر شبكة الإنترنت، فأحيانا يقوم المتهم بإرسال رسائل تشكل جرائم من جهاز عمومي بحيث يصعب معرفة مرسل تلك الرسائل،وقد يتخذ إجراءات غرضها التمويه على المرسل إليه بقصد إخفاء شخصيته، فيتدخل في موقع شخص آخر أو جهة أخرى ويبث من خلال موقعها أفعالا غير مشروعة، حيث تواجه السلطات صعوبات كبيرة في اقتفاء أثر المجرمين.

وتثير مشكلة تحديد الفاعل مدى مسؤولية مقدم الخدمات، والذي يتفق معه بعض الأشخاص على فتح صفحة لهم على شبكة الإنترنت، وبالتالي فإنّ علمه بما ينشر على الشبكة يتوافر، وقد لا يعلم بذلك مسبقا ولكن يعلم به بعد ذلك ويستمر في السماح بنشر ما ينطبق عليه وصف الجريمة، وبالتالي تقوم مسؤوليته الجنائية.

ثالثا: وقوع الجريمة في خارج الدولة التي يحدث فيها البث.

تقع الجريمة في الوضع العادي للأمور في نفس المكان الذي يقع فيه الفعل، أي تقع النتيجة في نفس المكان الذي يقع فيه النشاط، بيد أنه بالنسبة للجرائم الالكترونية تقع الجريمة في كثير من الأحيان في مكان آخر غير مكان البث، فإذا أرسل المتهم رسالة غير مشروعة بطريق الكمبيوتر من دولة معينة إلى شخص آخر في دولة أخرى، فإن النشاط يظهر في الخارج وليس في دولة الإرسال، ولكنه يؤدي إلى عدم علم السلطات في الدولة التي يرسل منها المتهم تلك الرسائل بما قام به هذا المتهم من أفعال يعاقب عليها القانون، وبالتالي يؤدي ذلك إلى عدم الإسراع في اتخاذ ما يلزم من إجراءات التحقيق مما يؤثر على تجميع الأدلة ضد المتهم[2].

---

[1]–د.غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 224.

[2]–نفس المرجع، ص 221.

وقد أدى ذلك إلى تجريم بعض الدول لبعض صور النشاط التي من شأنها أن توسع من اختصاص قضائها في الجرائم الالكترونية، فقد عمد المشرع في ولاية Tennessee إلى مد اختصاص محاكم الولاية بخصوص جرائم الكمبيوتر، فقد نص قانون جرائم الكمبيوتر في الفصل المتعلق بالإختصاص على وقوع الجريمة في كل مكان يقع فيه فعل من الأفعال المعاقب عليها، كما نص على وقوع الجريمة في كل مكان يسيطر فيه المتهم على مال متحصل من جريمة من جرائم الكمبيوتر أو يتواجد هذا المال في حيازته،كما تقع الجريمة وفقا لهذا القانون في كل مكان يحوز فيه المتهم كتبا أو تسجيلات أو وثائق أو أموال أو أوراق مالية أو برامج كمبيوتر أو أي أشياء مادية استخدمت في ارتكاب جريمة من جرائم الكمبيوتر[1].

رابعا: الصعوبات المتعلقة بالمساعدات القضائية الدولية.

إنّ الأصل بالنسبة لطلبات الإنابة القضائية الدولية، والتي تعد من أهم صور المساعدات القضائية الدولية في المجال الجنائي أن تسلم بالطرق الدبلوماسية وهذا بالطبع يجعلها تتسم بالبطء والتعقيد والذي يتعارض مع طبيعة الجرائم الإلكترونية، وكذلك من الصعوبات في مجال المساعدات القضائية الدولية التباطؤ في الرد،حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو القواعد والإجراءات التي تعقد الإستجابة وغيرها من الأسباب[2].

خامسا:عدم وجود إتفاقيات دولية بخصوص الجرائم الإلكترونية.

لم تجتمع الدول على التوقيع على إتفاقية واحدة لمكافحة جرائم الكمبيوتر والإنترنت، والأمر متروك في غالبية الأحوال إلى الإتفاقيات الثنائية التي تبرم بين الدول والتي تتناول جرائم مختلفة، ينتمي إليها البعض من جرائم الكمبيوتر ولا ينتمي إليها البعض الآخر، ويبرهن ذلك على الحاجة إلى إتفاقيات ثنائية وإتفاقيات جماعية لمكافحة الجرائم التقليدية التي تقع بطريق الكمبيوتر والإنترنت، وكذلك مكافحة الجرائم الخاصة التي لا تقع إلاّ بطريق الكمبيوتر والإنترنت[3].

ما تم التوصل إليه من قبل الفقهاء هو أن التقدم المتواصل في تكنولوجيا الحاسب والإنترنت يفرض على جهات إنفاذ القانون أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات،

---

[1]– د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر و الإنترنت،، المرجع السابق، ص 222.

[2]– د.حسين بن سعيد الغافري، المرجع السابق، ص 694.

[3]– د.غنام محمد غنام،دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، المرجع السابق،ص 223.

والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا، فظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئا ثقيلا على عاتق جميع أجهزة العدالة، لذلك كان لابد أن تكون تلك الأجهزة على اختلاف أنواعها على درجة كبيرة من الكفاءة والمعرفة، وهذا لن يتحقق إلا بالتدريب، فكفاءة رجال العدالة وقدرتهم في التصدي لهذه الجرائم لابد وأن ترتكز على كيفية تطوير العملية التدريبية والإرتقاء بها والنهوض بأساليب تحقيقها لأهدافها، من هذا المنطلق كانت الدعوى إلى وجوب تأهيل القائمين على هذه الأجهزة[1].

[1]– د. حسين بن سعيد الغافري، المرجع السابق، ص 677.

الباب الثاني: نطاق الدليل الإلكتروني والآثار المترتبة على عدم مشروعيته.

تمثل المحاكمة المرحلة الأخيرة للدعوى العمومية، لذا فهي تعرف باسم التحقيق النهائي ويقصد بها مجموعة الإجراءات المتخذة بهدف تمحيص جميع أدلة الدعوى سواء كانت لمصلحة المتهم أو ضده، وذلك بهدف استقصاء الحقيقة الواقعية والقانونية المتعلقة بالدعوى ومن تم الفصل فيها، فإن كانت أدلة قاطعة وجازمة كان الحكم بالإدانة وإن كانت أدلة غير قاطعة أو مؤكدة كان الحكم بالبراءة، لذلك تعتبر هذه المرحلة من أهم وأخطر المراحل، فتقدير الأدلة فيها نهائي وبها يتحدد مصير المتهم، لذلك أحاطها المشرع بالعديد من الضمانات، كما أن الإختصاص فيها يكون للقضاء وحده، والإجراءات التي تتم بها إجراءات قضائية بحتة[1].

فالغاية من جمع الأدلة من طرف الضبطية القضائية وجهات التحقيق هو توجيه الإتهام والإحالة أمام قضاء الحكم، بينما تمحيص تلك الأدلة والبحث عن غيرها عند الإقتضاء يكون من طرف قاضي الحكم الذي هدفه الحكم بالإدانة أو بالبراءة، والفرق دقيق بين الموقفين ويتطلب مهارة خاصة من طرف جهة التحقيق، لأنّ تمييز الأدلة والقرائن الموجودة هل تكفي للإحالة من عدمه لا يكاد يختلف عن تقدير كفايتها للإدانة، وليس هناك معيار واضح يميز بين الموقفين، ولذلك قد يصدر قاضي التحقيق أمرا بألاّ وجه للمتابعة لعدم وجود الأدلة الكافية، بينما ترى غرفة الإتهام أنّ الأدلة كافية للإحالة فتلغي الأمر، ولا يمكن للملاحظ أو الدارس أن يرجح موقف طرف على طرف لأنّ الأمر يعود إلى السلطة التقديرية لكل جهة، وتلك خاصية العلوم الاجتماعية التي تجمع بين الرأي والرأي المعاكس[2].

---

[1]– د.حسين بن سعيد الغافري، المرجع السابق، ص 575.

[2]– وذلك ما لخصه قرار المحكمة العليا الصادر بتاريخ 19-01-1988 فصلا في الطعن رقم 53194 الذي جاء فيه:"حيث أن مهمة غرفة الإتهام التي هي جهة تحقيق بالدرجة الأولى، لما يعرض عليها ملف تنحصر في السهر على وجود أدلة إثبات علاوة على أنها تتأكد من عدم تسرب أي بطلان في الإجراءات حسب ما تقتضيه ترتيبات قانون الإجراءات الجزائية في هذا الميدان، فإن لم تحدد دلائل كافية ضد المتهم أصدرت قرارا بألاّ وجه للمتابعة، وإن وجدت يرغمها القانون أن تحيل القضية إلى جهة الحكم المختصة حسب نوع الجريمة المرتكبة، ولا يسوغ لها تقييم هذه الأدلة.

حيث أنه في قضية الحال يوجد إقرار صريح للمتهم (ز.ع) فالملف إذن يحتوي على أدلة إثبات، بل على ما يعتبر عادة سيد الأدلة وفي هذه الحالة لا يخول القانون لغرفة الإتهام حق تقييم هذا الدليل والقول عنه أنه غير موضوعي وغير منطقي، وبالتالي يستلزم رفضه ورده على المقر به من تلقاء نفسه ثم انقضاء وجه الدعوى إزاءه وإزاء شريكه.

حيث أنّ القانون لا يخول صلاحية مناقشة وتقييم الأدلة إلاّ لجهات البث وفقا لما نصت عليه المواد 212 وما بعدها من قانون الإجراءات الجزائية ضمن الفصل المتعلق بطرق الإثبات.

وحيث أنه في قضية الحال كان على غرفة الإتهام بسعيدة أن تحيلها إلى محكمة الجنايات وتترك لها مهمة تقدير الأعذار بعد أن تتم أمامها مناقشة كل الوقائع حضوريا، وبالتالي فإنّ هذه الغرفة قد تجاوزت سلطتها لما قضت بألاّ وجه للمتابعة مما يستلزم نقض قرارها المطعون فيه".أنظر في ذلك: أ.نجيمي جمال، المرجع السابق، ص 117.

ولما كانت الجريمة الإلكترونية من الجرائم العابرة للحدود فمن المهم تحديد المحكمة المختصة بالفصل في النزاع، لأنه يترتب على ذلك تحديد القانون الواجب التطبيق في حالة تنازع القوانين، وبالتالي يمكن القول أن المحكمة المختصة هي التي تحدد القانون الواجب التطبيق، لذلك فإنّ تحديد المحكمة المختصة بنظر الدعوى له أهمية واضحة تتمثل في أنّ قاضي الدولة سوف يقوم بتحديد قاعدة الإسناد وفقا لقانون دولته[1].

ولقد تم إحداث تسوية شبه منطقية بين الدليل التقليدي والدليل الإلكتروني، وأساس هذه التسوية المنطقية هي النظرة إلى الواقع الجدي للتقنية الرقمية لكونها ذات مدلول مؤثر وحقيقي في عالم الإنسان المعاصر والمستقبلي، فما تنتجه التقنية الرقمية يؤدي دورا لا يمكن تجاهله حتى في المجتمعات التي يعد نموها بطيئا في هذا المجال.

غير أنه من الصعوبة بما كان رصد وجود أسلوب محدد يمكن أن يقدم ولو جزئيا منطقا قانونيا يمكن من خلاله رصد المعيار المفقود للدليل الإلكتروني، ولعل مثار هذه الصعوبة يكمن في عدم الإستقرار القانوني في كيفية التعامل مع الدليل الإلكتروني، حتى مع قبول القانون واعترافه بهذا الدليل فإن عملية إقراره والإعتماد عليه تجعل عملية بحث موضوعه وأنواعه تزداد صعوبة.

وإن كان هناك من يرى أن الإستعانة بالدليل الإلكتروني يجعل موضوع مثل هذه النقطة محلا لكثير من الشك في قيمته كدليل يتواءم مع مفهوم الأدلة التي يعرفها القانون في صيغته التقليدية[2].

وبالنظر إلى هذه الطبيعة الخاصة التي تتميز بها الأدلة المتحصلة من الوسائل الإلكترونية، وما قد يصاحب الحصول عليها من خطوات معقدة، فإنّ قبولها في الإثبات قد يثير العديد من المشكلات، فمستودع هذه الأدلة هو الوسائل الإلكترونية، ولذلك فإنّ من المشكلات التي تثيرها هذه الأدلة ليس بسبب أنها قد تصلح لتكون طرق إثبات أم لا ؟ وإنما المشكلة التي تتعلق بها تتحدد في كيفية ضمان مصداقية هذه الأدلة، وأن تعبر بالفعل عن الحقيقة التي تهدف إليها الدعوى الجنائية[3].

---

[1] -Thomas Gerbeaux, Internet et le contentieux international, disponible à l'adresse suivante : www.canavet.com.

نقلا عن د. شيماء عبد الغني، المرجع السابق، ص 367.

[2]– د.فتحي أنور عزت، المرجع السابق، ص 403.

[3]– د.علي محمود حمودة، المرجع السابق، ص 62.

ومما لا شك فيه أنّ أي عمل لابد أن يخضع لميزان العدالة، فهذا الأخير هو الذي يقدر مدى حجية أساليب التحقيق وسلطة القاضي في الأخذ بها والبطلان المقرر في مواجهتها[1].

غير أنّ الأعمال الإجرائية تخضع لرقابة القضاء من أجل حماية المشروعية الإجرائية، من خلال التأكد من أنّ أجهزة البحث عن الحقيقة قد التزمت عند مباشرتها لعملها بالقواعد القانونية، فالبحث عن الدليل يجب أن يكون في إطار احترام حقوق الأفراد وحرياتهم، ولما كان الإثبات نشاطا إجرائيا موجها مباشرة للوصول إلى اليقين القضائي طبقا لمعيار الحقيقة الواقعية وأنّ وسائله الأدلة، ولهذا فإنّ شرعية الإثبات الجنائي تستلزم عدم قبوله أي دليل كان البحث عنه أو الحصول عليه قد تم بطريق غير مشروع، ومن هنا تنبع أهمية الجزاء الإجرائي المتمثل في البطلان في حماية ضمانات المتهم، فهو يعد الوسيلة العملية اللازمة لتحقيق سلامة العدالة وهيبتها في جميع مراحل الدعوى الجنائية[2].

وعلى هذا الأساس سيقسم هذا الباب إلى فصلين، أتطرق في الفصل الأول لاختصاص القاضي الجزائي و سلطته في قبول الدليل الإلكتروني وتقديره، أمّا الفصل الثاني فخصص للآثار المترتبة على عدم مشروعية الدليل الإلكتروني.

[1] – أ. أمين ودرار، المرجع السابق، ص 213.

[2] – د. محمد أمين الخرشة، المرجع السابق، ص 215.

الفصل الأول: إختصاص القاضي الجزائي وسلطته في قبول الدليل الإلكتروني وتقديره.

سلطة القضاء هي إحدى مظاهر سيادة الدولة، وهي تمارس هذه السلطة على إقليمها وفي مواجهة شعبها، بل وفي مواجهة من يوجدون في هذا الإقليم، والدولة حينما تتبنى ضابطا للاختصاص القضائي، أي حينما تضع قواعد لاختصاص محاكمها بنزاع ذي طابع دولي، فإنها تراعي عدة إعتبارات، فقد تعقد الدولة الإختصاص لمحاكمها نظرا لارتباط أحد أطراف الدعوى بها، وقد تقرر الدولة إختصاصها نظرا لارتباط موضوع النزاع بإقليمها، أو لتحقيق اعتبارات الملاءمة أو حسن أداء العدالة، كما قد تعتد الدولة عند وضع قواعد إختصاص محاكمها بالمنازعات ذات الطابع الدولي بإرادة أطراف الدعوى.

ولقد أثارت مسألة تراخي النتيجة الإجرامية وتحققها في مكان مختلف عن مكان ارتكاب السلوك الإجرامي والذي قد يكون كما هو الحال في الجرائم الإلكترونية، فالمشكلة تتمثل في معرفة ما إذا كان الإختصاص القضائي بنظر الجرائم الإلكترونية ينعقد للمحاكم التي يقع في دائرة اختصاصها المكان الذي حدث فيه فعل الإعتداء ذاته، أو للمحاكم التي تتحقق في دائرة اختصاصها النتيجة المترتبة على فعل الإعتداء[1]، ولا شك أن المنازعات التي تنشأ عبر شبكة الإنترنت تحتاج إلى تطبيق إجراءات خاصة تتناسب مع طبيعتها، ومن هنا برزت أهمية التحكيم الإلكتروني[2].

كما أنّ الإثبات في المواد الجزائية تحكمه مجموعة من المبادئ العامة يسمح تحديدها وفهمها بالتحكم في الموضوع ومعرفة قصد المشرع أثناء تنظيمه لمختلف طرق الإثبات، مما يسهل عمل رجل القانون سواء من الناحية العلمية أو من الناحية العملية عند التطبيق على مستوى جهة الحكم أو المتابعة[3].

فالقاعدة في الدعاوى الجنائية هي جواز الإثبات بكافة الطرق والوسائل القانونية، والقيد على هذه القاعدة أنه يجب أن يكون الدليل من الأدلة المقبولة قانونا، وبالتالي تظهر أهمية اعتراف القانون بالأدلة الإلكترونية خاصة مع احتمال ظهور أنماط جديدة لجميع الجرائم وخاصة في قطاع المعلومات، ومن هنا كان البحث القانوني في العديد من الدول يتجه إلى الإقرار بحجية قانونية للملفات والمستخرجات الحاسوبية

[1]– أ. عبير فؤاد عبد العزيز، المرجع السابق، ص 271.

[2] -Eric Caprioli, L'importance des preuves électroniques pour résoudre les litiges internationaux, séminaire sur La preuve électronique dans l'arbitrage international, le 10.12.2008, organisé par ICC France, p 10.

[3]– أ. نجيمي جمال، المرجع السابق، ص 36.

والرسائل الإلكترونية ذات المحتوى المعلوماتي ليس بصورتها الموضوعة ضمن وعاء مادي ولكن بطبيعتها الإلكترونية المحضة[1].

كما أنّ التطور الحالي الذي انعكس أثره على قانون العقوبات قد انعكس أثره أيضا على قانون الإجراءات الجزائية، بحيث أنّ هذا القانون الأخير قد لا يطبق بسبب عجز القانون الأول عن استيعاب الجرائم المستحدثة التي ترتكب بالوسائل الإلكترونية،كما وأنّ الإثبات الجنائي وهو أحد الموضوعات الهامة لهذا القانون قد تأثر بدوره بالتطور الهائل الذي لحق الأدلة الجنائية بسبب تطور طرق ارتكاب الجريمة، الأمر الذي يتعين معه تغيير النظرة إلى طرق الإثبات الجنائي لكي تقترب الحقيقة العلمية في واقعها الحالي من الحقيقة القضائية.

فإثبات الجرائم التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية تتأثر بطبيعة هذه الجرائم وبالوسائل العلمية التي قد ترتكب بها، مما قد يؤدي إلى عدم اكتشاف العديد من الجرائم في زمن ارتكابها أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم أو تعذر إقامة الدليل اللازم لإثباتها، مما يترتب عليه إلحاق الضرر بالأفراد وبالمجتمع[2]، هذا إضافة إلى ما قد يثيره المحرر الرقمي من خلاف حول قيمته الثبوتية عند عرضه أمام القاضي لتقديره في حالة التعارض مع المحرر الكتابي[3].

وعلى هذا الأساس سيتم تقسيم هذا الفصل إلى ثلاثة مباحث، أتطرق في المبحث الأول للطابع الخاص للإختصاص القضائي في الجرائم الإلكترونية، أمّا المبحث الثاني فسأخصصه لحرية القاضي الجزائي في قبول الدليل الإلكتروني وتقديره، أمّا المبحث الثالث فقد عني بالإستثناءات والقيود الواردة على حرية القاضي الجزائي وضوابط اقتناعه بالدليل الإلكتروني.

[1]– د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص260.

[2]– د.علي محمود حمودة، المرجع السابق، ص 16.

[3] -Isabelle Renard, Preuve informatique (valeur juridique du document numérique), Expertises des systèmes d'information, N°348, Juin 2010, p 216.

المبحث الأول: الطابع الخاص للإختصاص القضائي في الجرائم الإلكترونية.

الإختصاص القضائي هو السلطة التي يقررها القانون للقضاء في أن ينظر في دعاوى من نوع معين حددها المشرع وفق قواعد وإجراءات معينة[1]، وقد عرفه جانب من الفقه بأنه: "ما لكل محكمة من المحاكم من سلطة القضاء تبعا لمقرها أو لنوع القضية، وهو نوعي إذا اختص بالموضوع ومكاني إذا اختص بالمكان".

ولذلك كان من المنطقي إزاء تجاوز الجرائم الإلكترونية للحدود الوطنية، أن ينعكس ذلك على مسألة القانون الواجب التطبيق عليها، فالنشاط الإجرامي في هذه النوعية من الجرائم أصبح يمارس في أكثر من دولة، ولهذا يثور التساؤل عن مدى إمكانية تطبيق قانون العقوبات الوطني على الجرائم التي تقع من أجانب على إقليم الدولة، والتي يرتكبها مواطنو الدولة على أرض دولة أجنبية، وذلك تطبيقا على الجرائم الإلكترونية[2]، والأصل أنّ القضاء في كل دولة يبحث فيما إذا كان مختصا بنظر هذه القضية أو تلك، لذا فإنّ قواعد الإختصاص تشكل فن عمل القاضي أساسا، فالقاضي الوطني يلتزم في البداية بالفصل في الإختصاص الدولي أي بيان عمّا إذا كان هو أصلا كقضاء وطني مختص بنظر الدعوى أم لا، ومن تم البحث في الإختصاص الداخلي، وعلى ذلك فيجب القول بدخول دعوى ما في اختصاص محكمة معينة في دولة ما أن تكون أصلا هذه الدعوى داخلة في اختصاص القضاء الإقليمي لهذه الدولة[3].

لذا فالإختصاص الجنائي نوعان: إختصاص جنائي دولي يقصد به سلطة محاكم كل دولة في نظر دعاوى معينة، واختصاص جنائي داخلي ويقصد به توزيع الدعاوى الجنائية التي تدخل في اختصاص القضاء الوطني على المحاكم الوطنية المتنوعة وفقا للضوابط والمعايير التي حددها المشرع[4]، ولا شك أن هناك العديد من المشكلات المتعلقة بموضوع الإختصاص القضائي، ففي كل جريمة إلكترونية فإن تحديد مكان ارتكابها يؤثر في قدرة هذه الدولة على العقاب[5].

وسأتطرق لمسألة قواعد الإختصاص القضائي في الجرائم الإلكترونية من خلال تقسيم هذا المبحث إلى مطلبين إثنين على النحو التالي:

المطلب الأول: قواعد الإختصاص الجنائي الدولي في الجرائم الإلكترونية.

---

[1] - د. أسامة فرج الله محمود الصباغ، الحماية الجنائية للمصنفات الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، سنة 2011، ص240.

[2]- د.عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، رسالة دكتوراه، كلية الحقوق ، جامعة القاهرة، مصر، سنة 2011، ص 241.

[3] - د. حسين الغافري، المرجع السابق، ص 576.

[4]- د.جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 43. نقلا عن: د. حسين الغافري، المرجع السابق، ص 577.

[5]- د.عمر محمد بن يونس، التحكم في جرائم الحاسوب وردعها، مؤسسة آدم للنشر والتوزيع، مصر، ط1، سنة 2008، ص 127.

شبكة الإنترنت ليس لها مقر في دولة معينة ولا تخص شخصا محددا، بل نجدها موزعة على المعمورة، فهي تجمع عدد كبير من الشبكات مختلفة النوع والمصدر والوظيفة، فبالتالي هي لا تخضع لرقابة أو سيطرة دولة معينة، ولا يوجد قانون جنائي موحد يحكمها، بل على العكس تتعدد القوانين الجنائية التي تطبق عليها بتعدد الدول المرتبطة، وهنا تكمن المشكلة فما يمكن القيام به من أنشطة إجرامية عبر شبكة الإنترنت يرتبط بمفهوم الإباحة والتجريم في كل دولة، فالأمر الذي تطرحه هذه الشبكة يكمن في تدويل الجرائم المرتكبة عليها.

وحيث أنّ الأصل هو الإرتباط بين تطبيق التشريع العقابي الوطني من حيث المكان وبين الإختصاص الدولي للمحاكم الوطنية، بمعنى آخر كل جريمة يسري عليها قانون العقوبات الوطني تختص بنظرها المحاكم الوطنية[1]، فالإختصاص القضائي الدولي يعطي الحق للدول بملاحقة ومحاكمة مرتكبي الجرائم دون أي اعتبار للجنسية التي يحملونها أو المكان الذي ترتكب فيه الجريمة، أي ينعقد الإختصاص القضائي الجنائي لأية دولة ترغب في ملاحقة الجرائم الدولية، وتأسيسا على ذلك فإن اعتبار الجرائم الإلكترونية من الجرائم الدولية يكون حلا ملائما لما تثيره هذه الجرائم من إشكاليات تنازع القوانين والإختصاص، وبما يكون له دورا مجديا في التصدي لهذه الجرائم ومكافحتها[2]، وبالرجوع إلى القواعد العامة التي تنظم مسألة تطبيق القواعد من حيث المكان، فهي محكومة بالمبادئ الأساسية التي سوف يتم التطرق إليها في الفروع التالية:

الفرع الأول: مبدأ الإقليمية في الجرائم الإلكترونية.

مبدأ الإقليمية يعني انطباق النص الجنائي الوطني عن كل جريمة تقع على إقليم الدولة صاحبة السيادة أيا كانت جنسية مرتكبيها، ويعني هذا أيضا أن القانون الجنائي الوطني لا ينطبق على الجرائم المرتكبة والتي تقع خارج إقليم الدولة سواء وقعت من أو على مواطني الدولة، ومن مساوئ هذا المبدأ أنّ هناك جرائم تقع خارج إقليم الدولة ولكنها تمس مصالح وسيادة هذه الدولة[3].

[1]– د.حسين الغافري، المرجع السابق، ص 577.

[2] - د. سامح أحمد بلتاجي موسى، المرجع السابق، ص 397.

[3]– د. أحمد فتحي سرور ، المرجع السابق، ص 89. نقلا عن : د. عمر أبو الفتوح الحمامي، المرجع السابق، ص 241.

ويعتبر هذا المبدأ القاعدة الأساسية المطبقة في غالبية الدول، فهو المبدأ الأرجح في التشريع الفرنسي سواء في ظل قانون العقوبات الفرنسي القديم أو الجديد، حيث تنص المادة (113-2)[1] من قانون العقوبات الفرنسي الجديد على أنه يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية الفرنسية، وتعد الجرائم مرتكبة داخل فرنسا طالما أنّ أحد الأفعال المكونة لها تم ارتكابها داخل فرنسا، وترتيبا على ذلك ينطبق القانون الفرنسي على كثير من الجرائم الإلكترونية، طالما أنّ الإختصاص ينعقد بمجرد وقوع أحد العناصر المكونة للجريمة أو تحقق النتيجة على الإقليم الفرنسي.

فبالنسبة للجرائم المرتكبة بواسطة شبكات المعلوماتية، مثل جريمة الإستخدام غير المشروع لنظم المعلوماتية، كاستخدام نص أو صورة موجودة على تلك الشبكات بطريقة غير مشروعة، لأنّ هذه المصنفات " النص أو الصورة" محمية قانونا بقانون حق المؤلف، فإذا ما تم الفعل المادي أي التصوير أو الإستخدام غير المشروع في فرنسا، فإنّ القانون الفرنسي هو الواجب التطبيق على هذه الواقعة لأنّ أحد الأركان المكونة للجريمة قد تم ارتكابه في فرنسا، ومن تم فإنّ القانون الجنائي الفرنسي يكون واجب التطبيق.

وكذلك الحال في حالة الدخول غير المشروع في نظام معلوماتي وتعديل المعطيات بغرض الحصول على مبلغ غير مشروع، والفرض هنا أنّ مرتكب الجريمة غير متواجد في فرنسا لكن الركن المادي المتمثل في الدخول في النظام وإتلاف البيانات وتعديلها للحصول على النتيجة المبتغاة قد تم في فرنسا ولكن النتيجة تتحقق في مكان خارج فرنسا، فإنّ القانون الفرنسي هو الواجب التطبيق عملا بنص المادة (113-2) من قانون العقوبات الفرنسي الجديد.

فليست هناك مشكلة في اعتبار أن الجريمة قد تم ارتكابها في فرنسا، حينما يكون أحد الأفعال المشكلة لها قد تم في فرنسا بواسطة رسالة إلكترونية طالما أن أحد الفاعلين موجود في فرنسا، لكن الصعوبة تتأتى في شأن تحديد مكان ارتكاب الجريمة في حالة استخدام قائمة محادثات في الفرض الذي يتم فيه إرسال المعلومة المجرمة من الخارج، ويكون أحد المشتركين الذي قام بتلقي المعلومة فرنسي الجنسية[2].

[1] - Article 113-2 (C.P.F): La loi pénale française est applicable aux infractions commises sur le territoire de la République.
L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire.

[2]- د.عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 244.

وكذلك الحال بالنسبة لمجموعات الأخبار News groups حيث أنّ الفاعل الذي يقوم ببث الرسالة لا يعرف على وجه التحديد في أية دولة سيتم تلقي هذه الرسالة ومن سيطلع على رسالته، فمن غير المعقول والمنطقي أن يلتزم الفرد باحترام جميع قوانين دول العالم، بحجة أنّ رسالته يمكن استقبالها في كل أنحاء العالم.

لكن مع ذلك يمكن لنص المادة (113-2) من القانون الفرنسي أن ينطبق، وذلك إذا تم إثبات أن المعلومة المرسلة موجهة بطريقة مباشرة إلى فرنسا، ذلك أن فعل الإستقبال الذي تم في فرنسا أي الفعل المادي لا يعد في هذه الحالة من قبيل الصدفة، ولكنه يعد مطابقا تماما لإرادة صاحب الرسالة[1].

ونفس المبدأ أخذ به المشرع الجزائري وهذا ما نصت عليه المادة الثالثة (03)[2] من قانون العقوبات على أنه يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية، كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجزائية، وتعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر وهذا عملا بنص المادة (586)[3] من قانون الإجراءات الجزائية، وهذا ما أخذ به المشرع المصري، فيطبق قانون العقوبات على أنه جريمة ترتكب داخل القطر دون تفرقة بين جنسية مرتكب الفعل أو المجني عليه أو نوع المصالح التي مستها الجريمة المرتكبة.

وبناء على ما سبق يمكن القول أنّ قانون دولة ما من الممكن أن ينطبق على الكثير من الجرائم المتعلقة بالإنترنت، طالما أنّ الإختصاص ينعقد بمجرد وقوع أحد العناصر المكونة للجريمة أو حتى وقوع النتيجة على هذا الإقليم، وهنا يثار التساؤل حول علاقة الفرع بالأصل في موضوع مزود الإنترنت وأثر ذلك على الإختصاص القضائي ؟ بمعنى آخر ما مدى إمكانية انطباق قانون دولة يكون فيها مزود الإنترنت مجرد فرع أو تابع لمزود آخر مركزه دولة أخرى في حالة ما إذا تم بث بعض المواقع التي قد لا تكون مجرمة في دولة المركز في الوقت الذي يكون فيه هذا النشاط مجرما في دولة الفرع أو المزود التابع ؟

---

[1]- د.عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 243.

[2] - تنص المادة 3 من قانون العقوبات الجزائري على ما يلي: " يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية .
كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجزائية ."

[3]- تنص المادة 586 من قانون الإجراءات الجزائية :" تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر".

ففي ألمانيا نجد أنّ القضاء اتجه إلى التقرير بانطباق القانون الألماني على الواقعة الإجرامية طالما أنها ذات صلة بالأراضي الألمانية، فقد قضت محكمة ميونخ في حكم لها صادر بتاريخ 28-05-1998 بمسؤولية Compuserve Ger وهي فرع كامل للشركة الأم في الولايات المتحدة الأمريكية عن وجود مواقع ذات طابع إباحي، على الرغم من أنّ مزود الإستضافة لهذه المواقع هو المركز الرئيسي في الولايات المتحدة الأمريكية، حيث قررت المحكمة أنه يجب اعتبار الفرع في ألمانيا مزود استضافة لكونه ذو علاقة وطيدة بالمركز الرئيسي في الولايات المتحدة الأمريكية، إذ أنّ المركز الرئيسي يعد طريق البث إلى الخوادم الأخرى التابعة له عبر العالم.

ونفس الإتجاه نجده في القضاء الفرنسي منذ قضية إتحاد الطلبة اليهود ضد yahoo في فرنسا،حيث اتجه القضاء الفرنسي إلى الإقرار باختصاصه بهذه الدعوى حتى وإن كانت المدعى عليها yahoo في فرنسا فرعا لمركز رئيسي في الولايات المتحدة الأمريكية، طالما أنّ البث يصل إلى الجمهورية الفرنسية، وبالتالي فإنّ تحديد مكان الحاسب الخادم الخاص بالإيواء في الخارج لا أثر له على وقوع الجريمة على الإقليم الوطني، حيث أنّ الفعل الإيجابي للمستخدم هو الذي يجسد الركن المادي للجريمة، فطالما يمكن الإطلاع على المعلومات المجرمة على الإقليم الوطني، فإنّ الإختصاص ينعقد لقانون هذا الإقليم[1].

وإن كان مبدأ الإقليمية هو تأكيد سيادة الدولة على إقليمها، وسهولة إجراءات المحاكمة في حالة وجودها في موقع الجريمة، والوصول إلى الأدلة يكون أقرب للعدالة، وكذلك إرضاء للمشاعر الإجتماعية ويكون العقاب أثر الردع العام، غير أنه يؤخذ عليه أنه قد يعطي الفرصة للجاني للإفلات من العقاب إذا ارتكبت الجريمة خارج حدود الوطن ثم عاد إليه دون أن يعاقب في الخارج[2].

الفرع الثاني: مبدأ العينية في الجرائم الإلكترونية.

يعني مبدأ عينية النصوص الجنائية تطبيقها على كل الجرائم التي تمس كيان الدولة أو مصالحها الأساسية أيا كان مكان وجنسية مرتكبيها، وعادة في التشريعات الحديثة لا يتم الإستعانة بمبدأ العينية كمعيار لتحديد نطاق اختصاص النص الجنائي وانطباقه على الوقائع، و لكن هذه التشريعات تستعين بهذا المبدأ لتكملة مبدأ الإقليمية ولتكملة مبدأ الشخصية أو لمنح النص الجنائي مجالا متسعا قد لا يسمح به أحد هذان المبدآن أو كلاهما[3].

---

[1]- نقلا عن : د.حسين بن سعيد الغافري، المرجع السابق، ص 581.

[2]- د. عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 245.

[3]- د.سامح بلتاجي موسى، المرجع السابق، ص 413.

ويستند هذا الإمتداد في الإختصاص إلى ما للدولة من حقوق الدفاع الذاتي ضد كافة صور الإعتداء على مصالحها الأمنية والمالية ولو وقعت خارج إقليمها، خاصة وأنّ السلطات الأجنبية التي وقعت هذه الجرائم فوق إقليمها قد تتقاعس عن العقاب عليها، كما لو وقعت الجريمة في إقليم دولة معادية.

وقد أخذ المشرع الفرنسي بمبدأ عينية النص الجنائي حيث تنص المادة (113-10)[1] من قانون العقوبات الجديد على أنه: "يطبق القانون الفرنسي على الجنايات والجنح التي ترتكب في الخارج والتي تشكل إعتداء على المصالح الأساسية للأمة المنصوص عليها في الباب الأول من الكتاب الرابع، وكذلك على جرائم تقليد وتزوير أختام الدولة وتزييف العملة المعدنية أو الورقية أو السندات والمعاقب عليها بالمواد (442-1، 442-2، 442-5، 442-15، 443-1، 444-1)، وعلى أية جناية أو جنحة ترتكب ضد أعضاء أو أماكن البعثات الدبلوماسية أو القنصلية الفرنسية في الخارج".

وقد أخذ القانون المصري أيضا بمبدأ العينية بالنسبة لجرائم معينة وردت على سبيل الحصر، تحكمها المادة (02/02) من قانون العقوبات التي تنص على أنه تسري أحكام هذا القانون على كل من ارتكب في خارج القطر جريمة من الجرائم التالية:

1- الجنايات المخلة بأمن الدولة التي نص عليها في البابين الأول والثاني من الكتاب الثاني من هذا القانون.

2- جنايات التزوير والتي نص عليها في المادة (206) من هذا القانون.

3- جنايات تقليد أو تزييف أو تزوير العملة الورقية أو المعدنية التي نص عليها في المادة (302) من هذا القانون، أو جناية إدخال تلك العملة الورقية أو المعدنية المقلدة أو المزيفة أو المزورة إلى مصر أو إخراجها منها، أو ترويجها أو حيازتها بقصد الترويج أو التعامل بها التي نص عليها في المادة (203) من نفس القانون، بشرط أن تكون العملة متداولة قانونا في مصر[2].

[1] - Article 113-10(C.P.F Modifié par Loi n°2001-1168 du 11 décembre 2001 - art. 17 (V)): La loi pénale française s'applique aux crimes et délits qualifiés d'atteintes aux intérêts fondamentaux de la nation et réprimés par le titre Ier du livre IV, à la falsification et à la contrefaçon du sceau de l'Etat, de pièces de monnaie, de billets de banque ou d'effets publics réprimées par les articles 442-1, 442-2, 442-5, 442-15, 443-1 et 444-1 et à tout crime ou délit contre les agents ou les locaux diplomatiques ou consulaires français, commis hors du territoire de la République.

[2] - د. أبو الفتوح الحمامي، المرجع السابق، ص 245.

ومن هذه الجرائم ما يتعلق بالجريمة الإلكترونية كما هو الحال في جريمة التجسس المعلوماتي على الأسرار القومية للدولة، ومنها ما يمكن ارتكابه عن طريق الإنترنت، مثل جريمة السعي أو التخابر لدى دولة أجنبية المادة (77) من قانون العقوبات، وجريمة تسليم أو إفشاء أسرار الدفاع عن البلاد المادة (80) من قانون العقوبات) والتي يمكن أن تتعلق بجريمة التجسس المعلوماتي وجريمة إنشاء أو تأسيس أو تنظيم أو إدارة جمعيات أو هيئات أو منظمات تهدف إلى سيطرة طبقة اجتماعية على غيرها من الطبقات المادة (1/98) من قانون العقوبات، وجريمة حيازة أي وسيلة من وسائل الطبع أو التسجيل أو العلانية مخصصة ولو بصفة وقتية لطبع أو تسجيل أو إذاعة نداءات وأناشيد أو دعاية خاصة بمذهب أو جمعية أو هيئة أو منظمة ترمي إلى غرض من الأغراض المنصوص عنها في المادتين (98، 174) من قانون العقوبات[1].

ونفس المعنى أخذ به المشرع الجزائري، فبالرجوع إلى قانون الإجراءات الجزائية الجزائري نجد أنّ المادة (588)[2] من قانون الإجراءات الجزائية قد حددت على سبيل الحصر، الجنايات والجنح التي يطبق عليها قانون العقوبات الجزائري وهذا بغض النظر عن جنسية مرتكبها ومكان ارتكابها، والعلة في ذلك هو حماية كيانها وحقوقها الأساسية كدولة ذات سيادة، وهذه الجرائم هي[3]:

1- الجرائم المتعلقة بأمن الدولة وسلامتها المواد من (62 إلى 64) من قانون العقوبات.

2- التعدي على الدفاع الوطني المواد من (65 إلى 76) من قانون العقوبات.

3- الجرائم المتعلقة بالمؤامرات وغيرها المواد من (77 إلى 83) من قانون العقوبات.

4- المساهمة في حركات التمرد المواد من (88 إلى 90) من قانون العقوبات.

5- جرائم تزوير النقود وترويجها المواد من (197 إلى 204) من قانون العقوبات.

وتشترط المتابعة أن يقبض على الجاني في الجزائر أو يتم تسليمه من طرف الدول الأخرى التي تمت فيها الجريمة وفقا لاتفاقيات تسليم المجرمين الموقعة عليها الدولة الجزائرية، لذلك ذهب اجتهاد المحكمة العليا إلى تكريس القاعدة، "إن ارتكب الجناية في الخارج من قبل جزائري لا يمنع السلطات القضائية الجزائرية من

---

[1]- د.عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 246.

[2] - تنص المادة 588 من قانون الإجراءات الجزائية الجزئري على ما يلي : " كل أجنبي ارتكب خارج الإقليم الجزائري بصفة فاعل أصلي أو شريك جناية أو جنحة ضد سلامة الدولة الجزائرية، أو تزييفا لنقود أو أوراق مصرفية وطنية متداولة قانونا بالجزائر، تجوز متابعته ومحاكمته وفقا لأحكام القانون الجزائري إذا ألقي القبض عليه في الجزائر أو حصلت الحكومة على تسليمه لها ."

[3]- قرار صادر يوم 12 جوان 1984 من الغرفة الجنائية الأولى،طعن رقم 35917. نقلا عن: د. بلعليات إبراهيم، أركان الجريمة وظروف إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، ط1، سنة 2007، ص 109.

متابعة ومحاكمة الجاني متى يثبت أنه لم يحاكم من أجلها وأنه قضى العقوبة المحكوم بها عليه أو أنها تقادمت أو حصل العفو فيها".

وتطبيقا لهذا المبدأ فإنه متى تبين أن هناك جريمة حتى ولو خرجت عن الحالات الخمس المذكورة آنفا فإنه يجوز للقضاء الجزائري أن يختص في متابعة ومعاقبة الجاني إذا كان حاملا للجنسية الجزائرية، وعليه أن يثبت في ذلك إمّا أنه تمت محاكمته أو أنه قضى العقوبة وأنّ الدعوى العمومية تقادمت أو حصل عفو فيها[1].

وبالرجوع إلى القانون الجزائري رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، تنص المادة (15)[2] على اختصاص المحاكم الجزائرية بالنظر في هذه النوعية من الجرائم التي ارتكبت خارج أراضيها بغض النظر عن جنسية مرتكبها عندما تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني.

وكذا الحال بالنسبة للقانون الفرنسي والقانون المصري ينعقد لهما الإختصاص بالنسبة للجرائم الواردة في المادة (113-10) من القانون الفرنسي، والمادة (02/02) من القانون المصري، ومن هذه الجرائم أيضا ما يقع منها بواسطة شبكات الإتصالات الحديثة، كما في حالة استخدام الحاسب الآلي في جرائم الإخفاء كما في حالة إخفاء الإرهابيين لمنشورات تمس أمن الدولة في ذاكرة الحاسب الآلي، فبوقوع هذه الجرائم تسري أحكام المواد السالفة الذكر في القانون الفرنسي، الجزائري والمصري، لأنهم يتناولون النص على جرائم محددة على سبيل الحصر، وهي تمس مصلحة أساسية للدولة ، حتى ولو كان مرتكب هذه الجرائم موجود خارج فرنسا أو الجزائر أو مصر، وبصرف النظر عن جنسية الجاني إعمالا لمبدأ العينية[3].

الفرع الثالث:مبدأ الشخصية في الجرائم الإلكترونية.

يعني مبدأ شخصية النص الجنائي أن يطبق على كل من يحمل جنسية الدولة بصرف النظر عن مكان وقوع الجريمة أو المصالح المحمية التي انتهكت نتيجة وقوع الجريمة، ولمبدأ الشخصية وجهان، أحدهما إيجابي ويعني تطبيق النص الجنائي على كل من يحمل جنسية الدولة ولو ارتكب جريمته خارج حدود إقليمها،

---

[1]- أ. بلعليات إبراهيم، المرجع السابق، ص 109.

[2]- تنص المادة 15 من القانون رقم 09-04 السالف الذكر على ما يلي:"فضلا عن قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني".

[3]- د.عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 246.

والوجه الآخر سلبي ويعني تطبيق النص على كل جريمة يكون المجني عليه فيها منتميا إلى جنسية الدولة، ولو كان مرتكبها أجنبيا وارتكبها خارج إقليم الدولة، وتتمثل أهمية مبدأ شخصية القانون في كونه الوسيلة التي تتجنب بها الدولة فرار أحد رعاياها بعد ارتكابه جرائم في الخارج إلى داخل الإقليم[1].

ومن الدول التي أخذت به فرنسا، فالمشرع الفرنسي أخذ بهذا المبدأ في شقه الإيجابي بحيث ينطبق القانون متى كان الجاني فرنسي الجنسية بحسب المادة (113-6)[2] من قانون العقوبات الفرنسي، وكذلك في شقه السلبي بحيث ينطبق القانون متى ما كان المجني عليه لحظة ارتكاب الجريمة يتمتع بالجنسية الفرنسية حسب المادة (113-7)[3] من قانون العقوبات الفرنسي.

فالعبرة في تطبيق الجانب الايجابي لمبدأ الشخصية في القانون الفرنسي هي كون الجاني مرتكب الجريمة التي وقعت خارج الإقليم الفرنسي فرنسي الجنسية، حتى ولو كان المتهم قد اكتسب الجنسية الفرنسية بعد ارتكاب الواقعة المنسوبة إليه، بشرط أن تكون الوقائع المسندة للمتهم معاقبا عليها في ظل قانون الدولة التي ارتكب فيها، أمّا العبرة في تطبيق الجانب السلبي لمبدأ الشخصية هي كون المجني عليه فرنسي الجنسية لحظة ارتكاب الجريمة الواقعة عليه والمرتكبة خارج الإقليم الفرنسي، بغض النظر عن كون الجاني فرنسي أم أجنبي، وبغض النظر عن كون الفعل الواقع على المجني عليه الفرنسي معاقب عليه في الخارج أم لا[4].

ولا يعرف المشرع الجزائري مبدأ شخصية النص الجنائي في وجهه السلبي، فجنسية المجني عليه ليست معيارا يحدد نطاق تطبيق النص من حيث المكان، ولكنه يعرف مبدأ شخصية النص في وجهه

---

[1]– د.سامح بلتاجي موسى، المرجع السابق، ص 408.

[2] - Article 113-6 (C.P.F Modifié par LOI n°2009-1503 du 8 décembre 2009 - art. 36): La loi pénale française est applicable à tout crime commis par un Français hors du territoire de la République.
Elle est applicable aux délits commis par des Français hors du territoire de la République si les faits sont punis par la législation du pays où ils ont été commis.
Elle est applicable aux infractions aux dispositions du règlement (CE) n° 561/2006 du Parlement européen et du Conseil du 15 mars 2006 relatif à l'harmonisation de certaines dispositions de la législation sociale dans le domaine des transports par route, commises dans un autre Etat membre de l'Union européenne et constatées en France, sous réserve des dispositions de l'article 692 du code de procédure pénale ou de la justification d'une sanction administrative qui a été exécutée ou ne peut plus être mise à exécution.
Il est fait application du présent article lors même que le prévenu aurait acquis la nationalité française postérieurement au fait qui lui est imputé.

[3] - Article 113-7(C.P.F): La loi pénale française est applicable à tout crime, ainsi qu'à tout délit puni d'emprisonnement, commis par un Français ou par un étranger hors du territoire de la République lorsque la victime est de nationalité française au moment de l'infraction.

[4]– د. عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 247.

الإيجابي، حيث تنص المادة (582)[1] من قانون الإجراءات الجزائية على أن كل واقعة موصوفة بأنها جناية معاقب عليها في القانون الجزائري ارتكبها جزائري في خارج إقليم الجمهورية يجوز أن يتابع ويحاكم فيها في الجزائر، غير أنه لا يجوز المتابعة أو المحاكمة إلاّ في حالة عودة الجاني إلى الجزائر وعدم إثباته أنه حكم عليه نهائيا في الخارج، أو ثبت في حالة الحكم بالإدانة أنه قضى العقوبة أو سقطت عليه بالتقادم أو حصل على العفو عنها، أمّا المادة (583)[2] قد نصت على أنّ كل واقعة تكون موصوفة بأنها جنحة سواء في نظر القانون الجزائري أو في نظر المكان الذي تم ارتكاب فيه الجنحة فيجوز حينها المتابعة والمحاكمة في الجزائر، إذا كان من قام بارتكابها جزائريا، فالمادة (582) تتحدث عن الجنايات، أما المادة (583) فإنها تتحدث عن الجنح[3].

أمّا المشرع المصري، هو الآخر لم يعرف مبدأ شخصية النص الجنائي في وجهه السلبي، وإنما اقتصر على الجانب الإيجابي، فنصت المادة الثالثة (03) من قانون العقوبات على أنّ كل مصري ارتكب وهو في خارج القطر فعلا يعتبر جناية أو جنحة في هذا القانون يعاقب بمقتضى أحكامه إذا عاد إلى القطر وكان الفعل معاقب عليه بمقتضى قانون البلد الذي ارتكب فيه.

ويمكن لهذه النصوص أن تنطبق على الجرائم المرتكبة بواسطة شبكات المعلوماتية، فلقد أفرزت تكنولوجيا المعلومات والاتصالات أساليب مستحدثة يمكن من خلالها ارتكاب الجريمة في دولة أجنبية والمجرم في وطنه الأصلي، أو يقوم الجاني بإعداد الجريمة التي يمكن أن يبدأ بتنفيذها بعد أن يغادر القطر الموجود فيه أي مكان ارتكاب الجريمة، وذلك بطريقة البرامج المحددة الوقت التي تعمل حسب الأمر الموضوع لها كما يحدث في إتلاف المعلومات، وكذلك في حالة تحويل الأموال[4].

---

[1] – تنص المادة 582 من قانون الإجراءات الجزائية الجزائري على ما يلي: " كل واقعة موصوفة بأنها جناية معاقب عليها من القانون الجزائري إرتكبها جزائري في خارج إقليم الجمهورية يجوز أن تتابع ويحكم فيها في الجزائر.

غير أنه لا يجوز أن تجري المتابعة أو المحاكمة إلا إذا عاد الجاني إلى الجزائر ولم يثبت أنه حكم عليه نهائيا في الخارج، وأن يثبت في حالة الحكم بالإدانة أنه قضى العقوبة أو سقطت عنه بالتقادم أو حصل على العفو عنها ."

[2] – تنص المادة 583 من قانون الإجراءات الجزائية الجزائري على ما يلي: " كل واقعة موصوفة بأنها جنحة سواء في نظر القانون الجزائري أم في نظر تشريع القطر الذي ارتكبت فيه، يجوز المتابعة من أجلها والحكم فيها في الجزائر إذا كان مرتكبها جزائريا ...".

[3]– د. بلعليات إبراهيم، المرجع السابق ، ص 111.

[4]– تعتبر قضية Thompsown، V.R التي وقعت عام 1984 نموذجا أمام القضاء الإنجليزي في مسألة اللحظة الزمنية التي يرتكب فيها الغش بالكمبيوتر، وتتلخص وقائع هذه القضية في أن المتهم Thompsown كان يعمل في أحد بنوك دولة الكويت مبرمجا، وأثناء خدمته في البنك دبر خطة للإحتيال على البنك بوضع برنامج أمر بموجبه الكمبيوتر بتحويل مبالغ من حسابات بعض العملاء المحفوظة والتي لم يتم السحب منها وساكنة لمدة من الزمن، وذلك لتحويلها لصالح حسابات أخرى قد فتحها بمجرد عودته إلى المملكة المتحدة، وقد علق التحويل على عودته للمملكة المتحدة بإرسال خطاب إلى مدير البنك لتحويل مستحقاته وأرصدته وقد نفذ مدير البنك ذلك وتم التحويل، وبعد ذلك قد اكتشف أمره واستوقفته الشرطة البريطانية، وحكم بأن مخالفته ارتكبت في اللحظة التي قرأ فيها مدير البنك خطابه وبذلك تخضع الوقائع للمحاكم الإنجليزية. أنظر في ذلك : د. عمر أبو الفتوح الحمامي، المرجع السابق، ص248.

الفرع الرابع: مبدأ العالمية في الجرائم الإلكترونية.

عرف المجتمع الدولي مظهرا هاما من مظاهر تضامن الدول وتعاونها في مكافحة الجرائم ذات الطابع الدولي والجرائم متعدية الحدود، وهو الذي يتمثل في نظام تسليم المجرمين، ويهدف هذا النظام إلى توفير آليات عملية تكفل عدم إفلات المجرم من العقاب إذا ما فر من الدولة الذي ارتكب جريمته فوق إقليمها إلى دولة أخرى، كما تكفل الدولة أن تتولى بنفسها عقاب من يرتكبون جرائم تمس مصالحها العليا خارج إقليمها.

غير أنه لم يقدر لهذا النظام أن يبلغ مرحلة مرضية تتحقق معها الفائدة العملية المرجوة منه، فهناك قيود مسلم بها ترد على المبدأ، أهمها أنه لا يجوز تسليم رعايا الدولة المطلوب منها التسليم، ولا يجوز التسليم في صدد أنواع معينة من الجرائم، وهناك احتمال أن يعجز النظام عن تحقيق الغاية منه كلما ساءت العلاقات بين الدول، وأصبحت إجابة طلب التسليم رهنا باعتبارات سياسية، لذلك اهتدى الباحثون إلى فكرة الإختصاص العالمي أو نظام العقاب العالمي[1].

فلا يقصد بهذا المبدأ امتداد سلطان قانون العقوبات الوطني على العالم بأسره، وإنما يعني أنّ القانون الجنائي الوطني واجب التطبيق على كل مجرم يقبض عليه في إقليم الدولة بغض النظر عن جنسية المجرم أو المجني عليه أو مكان ارتكاب الجريمة، ويعبر أحيانا عن هذا المبدأ بعالمية القاعدة الجنائية، ويهدف مبدأ العالمية إلى عدم إفلات الجاني من العقاب، خاصة إزاء ظاهرة العصابات الدولية التي تتميز بامتداد أنشطتها الإجرامية عبر عدة دول وتنوع جنسيات أعضائها، فهذا المبدأ يعني أن لكل دولة أن تخضع لسلطتها الجرائم المنصوص عليها في قانون العقوبات، دون اعتبار إلى أنّ القانون الأجنبي يصفها بأنها جريمة أم لا، وأنّ الجاني قد عوقب عنها بالخارج ونفذ العقوبة أم لا، و هذا تأكيد على عالمية الجزاء الجنائي[2].

وقد قيل في تبرير فكرة عالمية حق العقاب أنها تخفف من حدة إطلاق مبدأ الإقليمية الذي تعتمده القوانين الجنائية، ولذلك فإن مبدأ العالمية لا يستند على حق سيادة تدعيه الدولة التي تحاكم الجاني، وإنما على وجوب منع الضرر الذي يترتب على إفلاته من المسؤولية، ويقتضي إعمال هذا المبدأ من الناحية العملية توافر ثلاثة شروط طبقا للعرف المستقر، أوّلها أن تكون الجريمة المرتكبة من الجرائم ذات الطابع الدولي التي تتجاوز آثارها الحدود الوطنية، وهو الأمر الذي يبرر اعتبار دولة الضبط بمثابة نائب عن المجتمع الدولي في الملاحقة والعقاب، والشرط الثاني أن يتم ضبط الجاني في إقليم الدولة فلا يتصور محاكمته غيابيا، والشرط الثالث ألاّ

[1]– د.أحمد شحاتة بيومي، المرجع السابق، ص 311.

[2]– د.عمر أبو الفتوح الحمامي، المرجع السابق، ص 249.

يوجد طلب بتسليم الجاني من قبل دولة أخرى وفقا لمبدأ الإقليمية أو مبدأ الشخصية، لأنّ مبدأ العالمية لا يرجح في مواجهتهما[1].

فالجرائم الإلكترونية تدرج ضمن الجرائم العالمية بالمفهوم الدقيق، حيث تتجاوز هذه الجرائم حدود الدولة ولا يعوقها أية عائق، وعلى ذلك يمكن القول بأن ظاهرة الجريمة الإلكترونية تتطلب الأخذ بمبدأ العالمية من عدة نواحي:

الأولى: أنّ هذه الجرائم أصبحت لا تقتصر على دولة معينة، وإنما تتخذ من العالم بأسره مسرحا لها، حيث تتجاوز هذه الجرائم الحدود الدولية ولا يعوقها أية حدود.

الثانية: أصبحت هناك علاقة وثيقة بين المعلومات باعتبار أنّ لها قيمة اقتصادية وبين جميع الأنشطة التي تستخدم الحاسب الآلي، سواء كانت شركات أو مؤسسات أو أفراد أو حتى دول، فلا بد من الحفاظ على تلك المعلومات ومنع كافة صور الإعتداء عليها سواء بالإفشاء أو السرقة أو التزوير أو الإتلاف، بالإضافة إلى ما أفرزته تكنولوجيا الإتصالات السلكية واللاسلكية من جرائم استخدام هذه الشبكات وشبكات المعلومات مثل جرائم الإستغلال الجنسي للأطفال عبر الإنترنت، وجرائم تقليد المصنفات عبر الإنترنت وجرائم القذف والسب عبر الإنترنت.

الثالثة: إنّ عدم الأخذ بمبدأ العالمية قد يؤدي إلى نتائج خطيرة، تتمثل في إفلات الجاني من العقاب وخاصة بالنظر إلى العصابات الإجرامية، كما أنه من المصلحة المشتركة للدول الأخذ بهذا المبدأ في سبيل مكافحة الجريمة.

وإذا كان المشرع الجزائري والمصري لم ينص على مبدأ العالمية إلاّ أنّ بعض الفقه[2]، قد ذهب إلى وجود آلية لتطبيق مبدأ العالمية واستند في ذلك إلى النصوص المتعلق بمبدأ العينة، حيث يذهب إلى أنه وإن كان هذا النص يحدد ضوابط مبدأ العينة إلاّ أنه يمكن من خلاله وضع مبدأ العالمية موضع التنفيذ في حالتين:

الأولى: أن تقع جريمة من الجرائم باستخدام نظم المعالجة الآلية للمعطيات.

الثانية: إستحداث بند جديد يضاف إلى هذه النصوص مخصص للجرائم الإلكترونية[3].

---

[1]- د.أحمد شحاتة بيومي، المرجع السابق، ص 313.

[2]- د.عمر الفاروق الحسيني، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيات المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة في الفترة من 25 إلى 28 أكتوبر 1993، المؤتمر منشور بدار النهضة العربية سنة 1999،ص 467، نقلا عن :د. عمر عبد العظيم الحمامي، المرجع السابق، ص 250.

[3]- د. عمر عبد العظيم الحمامي، المرجع السابق، ص 249 – ص 250.

أما على المستوى الدولي فقد ذهب البعض[1] نظرا لعالمية الجرائم الإلكترونية إلى ضرورة وجود قانون جنائي دولي على غرار القانون الدولي الخاص يطبق في مجال المعلوماتية[2].

المطلب الثاني: قواعد الإختصاص الجنائي الداخلي في الجرائم الإلكترونية.

إنّ توزيع الدعاوى الجنائية التي تدخل في اختصاص القضاء الوطني دوليا على المحاكم الوطنية المتنوعة يتم وفق الضوابط والمعايير التي حددها المشرع والتي يمكن ردها إلى ثلاثة أنواع هي : الإختصاص الشخصي والإختصاص المكاني والإختصاص النوعي[3]، وسأتطرق لهذه الأنواع من الإختصاصات في الفروع التالية:

الفرع الأول: الإختصاص الشخصي.

يعني الإختصاص الشخصي إختصاص المحاكم العادية بالنظر والفصل في كافة الدعاوى الجنائية المقامة ضد كافة الأشخاص على أرض الدولة وخارجها، ومهما كانت صفة أو حالة مرتكبيها مادامت معاقب عليها بموجب نصوص قانون العقوبات[4]، إلاّ أنّ المشرع وفي بعض الحالات خرج عن هذا الأصل العام بأن جعل لبعض العناصر الشخصية كالسن والصفة محل نظر واعتبار في مجال الإختصاص، فتكون المحكمة في هذه الحالة مختصة شخصيا إذا كان القانون يقرر اختصاصها بالنسبة لفئة معينة من المتهمين رأى المشرع عدم وضعهم على قدم المساواة مع غيرهم من الأشخاص، وذلك بالنظر إلى حداثة سنهم مثلا أو تمتعهم بصفة خاصة كأن يكونوا عسكريين.

ومن الأمثلة على هذه المحاكم، محكمة الأحداث المختصة بنظر الدعاوى الخاصة بجرائم الأحداث، المحاكم العسكرية الخاصة بنظر جرائم العسكريين[5]، وعلى ذلك فإذا ارتكب أحد الأشخاص المخاطبون بقانون القضاء العسكري[6] لجريمة إلكترونية مثل إفشاء الأسرار العسكرية المسجلة إلكترونيا وكذلك التواجد و الدخول غير المشروع في النظم الآلية لمعالجة المعلومات الخاصة بالقوات المسلحة، وكذلك إتلاف المعلومات أو البرامج المسجلة على الأقراص الصلبة أو المرنة والخاصة بالقوات المسلحة، فإنّ المحاكم العسكرية هي المختصة بنظر الدعوى الجنائية.

---

[1]- د.جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 60.

[2]- د.عمر أبو الفتوح الحمامي، المرجع السابق، ص 249.

[3]- د. حسين الغافري، المرجع السابق، ص 585.

[4]- د. سامح بلتاجي موسى، المرجع السابق، ص417.

[5]- د. حسين الغافري، المرجع السابق، ص 586.

[6]- الأمر رقم 71-28 المؤرخ في صفر عام 1391 الموافق ل 22 أبريل سنة 1971 المعدل والمتمم بالأمر رقم 73-04 المؤرخ في 05 يناير 1973 المتضمن قانون القضاء العسكري الجزائري، ج .ر رقم 05.

ونفس الأمر إذا وقعت الجريمة على معدات خاصة بالقوات المسلحة كأجهزة الكمبيوتر والشبكات المعلوماتية العسكرية أو برامج معلوماتية عسكرية، وكذلك إذا تعلقت الجريمة الإلكترونية بالمعدات العسكرية والذخيرة وأسرار القوات المسلحة، فإنّ المحاكم العسكرية هي المختصة بنظر الدعاوى المتعلقة بالجرائم التي تقع على أشياء خاصة بالقوات المسلحة[1].

الفرع الثاني :الإختصاص النوعي.

يتحدد إختصاص المحاكم الجنائية بالنظر إلى جسامة الجريمة، حيث نصت المادة (328)[2] من قانون الإجراءات الجزائية الجزائري على أن المحكمة تختص بالفصل في الجنح وكذلك في الجنح و المخالفات المرتبطة أو غير القابلة للتجزئة، كما يوجد قسم للمخالفات يختص بالفصل في الوقائع ذات وصف المخالفة، أما إستئناف هذه الأحكام فيكون أمام الغرفة الجزائية بالمجلس القضائي التي تنظر في استئنافات مواد الجنح والمخالفات طبقا لنص المادة (429)[3]، أما المخالفات التي يرتكبها الحدث فاستئنافها تفصل فيه غرفة الأحداث بالمجلس طبقا للمادة (446)[4] من قانون الإجراءات الجزائية.

وتعتبر محكمة الجنايات الجهة القضائية المختصة بالفصل في الأفعال الموصوفة جنايات وكذا الجنح والمخالفات المرتبطة بها والجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار من غرفة الإتهام، ولمحكمة الجنايات كامل الولاية في الحكم جزائيا على الأشخاص البالغين، كما تختص بالحكم أيضا على القصر البالغين من العمر ستة عشر(16) سنة كاملة إذا ما تعلقت الوقائع و التهم المنسوبة إليهم بأفعال إرهابية أو تخريبية، وهي تنظر في القضية بناءا على قرار الإحالة الصادر نهائيا من غرفة الإتهام طبقا لنص المادة (249) [5]من قانون الإجراءات الجزائية، ولا يجوز لمحكمة الجنايات أن تقضي بعدم اختصاصها طبقا لنص المادة (251)[6] من قانون الإجراءات الجزائية الجزائري[7].

---

[1] – د. عمر أبو الفتوح الحمامي، المرجع السابق، ص 262.

[2] – تنص المادة 328 من قانون الإجراءات الجزائية الجزائري على ما يلي: " تختص المحكمة بالنظر في الجنح والمخالفات ...".

[3] – تنص المادة 429 من قانون الإجراءات الجزائية الجزائري على ما يلي: " يفصل المجلس القضائي في استئنافات مواد الجنح والمخالفات...".

[4] – تنص المادة 446 من قانون الإجراءات الجزائية الجزائري على ما يلي: "... وإذا كان الحكم قابلا للإستئناف حسب أوضاع الفقرة الثانية من المادة 416 من قانون الإجراءات الجزائية، رفع هذا الإستئناف أمام غرفة الأحداث بالمجلس القضائي ."

[5]- تنص المادة 249 من قانون الإجراءات الجزائية الجزائري على ما يلي:"... كما تختص بالحكم على القصر البالغين من العمر ستة عشر (16) سنة كاملة الذين ارتكبوا أفعالا إرهابية أو تخريبية والمحالين إليها بقرار نهائي من غرفة الإتهام."

[6] – تنص المادة 251 من قانون الإجراءات الجزائية الجزائري على ما يلي: " ليس لمحكمة الجنايات أن تقرر عدم اختصاصها."

[7]– أ. محمد حزيط، المرجع السابق، ص196 وما بعدها.

أما المحكمة العليا، فهي في الأصل محكمة قانون، يرفع أمامها الطعن بالنقض المبني على أوجه معينة حددها المشرع الجزائري في نص المادة (500) من قانون الإجراءات الجزائية الجزائري.

الفرع الثالث: الإختصاص المكاني.

لقد تجاوز الأشخاص حدود إقليمهم وهذا يرجع إلى رواج التجارة وكذلك الرواج السياحي، وقد أثر تقارب الحدود الجغرافية بالإتصالات من إقليم إلى آخر على أساليب الجريمة، فأصبحت للجريمة صورا جديدة في النطاق الدولي وأصبح المجرمون يمارسون نشاطهم الإجرامي في أكثر من دولة[1].

وهكذا يوجد إلى جانب الإختصاص النوعي الإختصاص المكاني، ويتحدد هذا الإختصاص بثلاثة معايير تتمثل فيما يلي :

أولا: مكان وقوع الجريمة.

تتميز الجرائم الإلكترونية عن غيرها من الجرائم في أنّ لها بعدا مكانيا دوليا، وذلك لوجود الجهاز الذي يتم إدخال المعلومات غير المشروعة في مكان مختلف عن المكان الذي يتواجد فيه الجهاز الخادم (serveur)، ومع ذلك فإنّ تطبيق معيار مكان وقوع الجريمة لا يخلو من بعض الصعوبات القانونية التي تجد تفسيرها في الطبيعة الخاصة للجريمة الإلكترونية، فما هو مكان وقوع الجريمة الإلكترونية؟

يجب ذكر أنّ هناك طائفتين من جرائم تقنية المعلومات، الطائفة الأولى وتضم الجرائم البحتة لتقنية المعلومات، والنوع الثاني ويتضمن الجرائم التي تقع بطريق من طرق تقنية المعلومات، تنتمي إلى النوع الأول من الجرائم جريمة الدخول والبقاء في النظام وجريمة إتلاف المعلومات والإخلال بسير النظام، وتنتمي إلى النوع الثاني جريمة السب والقذف بطريق الإنترنت وجريمة غسيل الأموال بالإستعانة بالإنترنت، ففي النوع الأول من الجرائم تقع الجريمة على جهاز معين يتداخل فيه المتهم أو يبقى فيه بطريقة غير مسموح بها، وبالتالي يمكن القول بأن الجريمة تقع على جهاز معين يتداخل فيه المتهم أو يبقى فيه بطريقة غير مسموح بها.

وبالتالي يمكن القول بأن الجريمة تقع في نفس المكان الذي يقع فيه الجهاز المعتدى عليه ما دام أنّ النشاط (الدخول أو البقاء) قد تم حدوثه في نفس مكان تواجد الجهاز، بيد أنه قد يحدث أن يكون الدخول أو البقاء عن بعد من جهاز متواجد في مكان آخر، عندئذ يمكن القول بأنّ الجريمة الواقعة تحدث في مكان

[1]– د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي) دراسة مقارنة، رسالة دكتوراه، جامعة طنطا، مصر، كلية الحقوق، سنة 2000، ص 136.

وجود الجهاز المعتدى عليه وفي مكان وجود الجهاز الذي استعان به المتهم للقيام بالنشاط وهو الدخول أو البقاء غير المشروع، هذا المكان الثاني قد يقع في نفس دائرة اختصاص المحكمة التي يقع في دائرتها الجهاز المعتدى عليه، عندئذ لا تثار مشكلة قانونية، وقد يقع هذا المكان في دائرة اختصاص محكمة أخرى، بل قد يقع في خارج البلاد، ففي هذه الحالة الأخيرة يؤول الإختصاص وفقا لمبدأ الإقليمية إلى محكمة الجهاز المعتدى عليه ومحكمة الجهاز الذي تم الدخول منه أو البقاء بالخارج.

أمّا بالنسبة للنوع الثاني من الجرائم والتي تنتمي أصلا إلى الجرائم التقليدية ولكنها تقع بطريق من طرق تقنية المعلومات، فإنّ الأمر يثير بعض الصعوبات القانونية فيما يتعلق بتحديد المحكمة المختصة، فإذا ارتكب شخص سبا أو قذفا في حق شخص آخر ، فإن ذلك قد يقع باستعمال جهازين من أجهزة الكمبيوتر، فمكان الجهاز الذي حمّلت منه الرسالة تختص المحاكم فيه بمحاكمة المتهم عن الجريمة التي تضمنتها تلك الرسالة، أمّا مكان الخادم فإنّ القول باختصاص المحكمة الذي يقع في دائرتها هذا الجهاز يؤدي إلى نتيجة يصعب قبولها وهي أن المحكمة التي يقع في دائرتها ذلك الجهاز تختص بمحاكمة المتهمين عن كل الجرائم التي تمت بطريق الإنترنت، وذلك بسبب أن الجهاز الخادم يؤدي دورا في نقل الرسالة إلى المرسل إليه، فمرور الرسالة مادام أنه يشكل جزءا في الجريمة فإن الإختصاص ينعقد لمحكمة ذلك الجهاز[1].

فينبغي عند تحديد مكان وقوع الجريمة أن يتم ذلك وفقا لطبيعة الجريمة، فالجريمة الوقتية كما في حالة إتلاف المعلومات أو البرامج باستخدام القنبلة المنطقية، يتم تحديد مكان وقوعها بالمكان الذي وقع فيه الفعل التنفيذي، وفي حالة اختلاف مكان وقوع الفعل عن مكان حدوث النتيجة اعتبر كل من المكانين محلا لوقوع الجريمة، وفي الجرائم السلبية يتحدد مكان الوقوع بالمكان الذي كان يجب أن ينفذ فيه العمل أو السلوك الذي يفرضه القانون[2].

أمّا بالنسبة للمحاكم الأمريكية، فإنّ هناك إختلافا في تحديد معيار الإختصاص بالجرائم الإلكترونية من ولاية إلى أخرى، فمن الولايات ما يأخذ بمكان البث (دلاور و كنتاكي و فرجينيا) ومن الولايات ما يأخذ بمعيار مكان وجود جهاز الكمبيوتر المستخدم في ارتكاب الجريمة (ولاية بنسلفانيا، نيو جرسي)، ومنها ما يأخذ بمعيار مكان وقوع الضرر، ومنها ما يأخذ بمعيار مكان وجود المتحصلات الناتجة عن الجريمة والوسائل المستخدمة في ارتكابها (ولاية فرجينيا)، ومنها ما يأخذ بمعيار حدوث الدخول على الجهاز بدون وجه حق أو على الشبكة إذا وقع على إقليم الدولة أو من خلالها (نيوجرسي و فرجينيا).

[1]– د.غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، المرجع السابق، ص208.

[2]– د.حسين الغافري، المرجع السابق، ص589.

كما تسري القواعد العامة في غياب نص خاص بخصوص المحكمة المختصة، حيث للمدعي أن يلجأ إلى محكمة مكان الجهاز الخادم أو محكمة تحقق النتيجة، ولكن المشكلة أن النتيجة تتحقق في أكثر من مكان بل في أكثر من دولة، غير أن اختصاص محكمة الجهاز الخادم يحقق المزايا التالية:

1. سهولة معرفة مكان تواجد الجهاز بينما يصعب أحيانا معرفة صاحب الرسالة الذي يبثها عبر موقع ربما سجل هذا الموقع باسم وهمي أو بدون إسم محدد، وربما يقيم في الخارج ويستدعي الأمر رفع الدعوى في مكان إقامته في الخارج ومتابعة إجراءات الدعوى في الخارج.
2. رفع الدعوى أمام محكمة الجهاز الخادم يجيز التعويض عن سائر الأضرار التي تحققت في أماكن مختلفة من العالم، على خلاف الحال عند رفع تلك الدعوى أمام إحدى المحاكم التي تصل إليها شبكة الإنترنت ويمكن الدخول إلى الموقع فيها، حيث أن ذلك لا يجيز سوى التعويض عن الضرر الذي تحقق في هذا المكان وحده دون غيره.
3. رفع الدعوى أمام محكمة الجهاز الخادم يسمح للمحكمة بأن تصدر أمرا إلى مزود الخدمة بمنع الدخول إلى الموقع الذي يتضمن رسائل مؤثمة أو ضارة بالآخرين[1].

ثانيا: مكان إقامة المتهم.

يقصد به المكان الذي يوجد فيه محل إقامة المتهم فعليا، وهو المكان الذي يقيم فيه أو يسكنه، وقد يكون حكميا أي الموطن القانوني الذي يوجد فيه الشخص عادة أو تعرف فيه سيرته وشؤونه، والعبرة في تحديد هذا المكان يكون بوقت ارتكاب الجريمة، فهذا الأخير هو من ينشئ للدولة حقها في العقاب وبالتالي حقها في توجيه الإتهام إلى الشخص بسبب الجريمة المنسوبة إليه، وإذا تعددت أمكنة إقامة المتهم كانت جميع المحاكم التي تتبعها هذه الأمكنة مختصة مكانيا بالجريمة.[2]

ولما كان مكان إقامة المتهم غير معلوم في حالات كثيرة وبخاصة في جرائم الكمبيوتر والإنترنت، فإنّ قانون إساءة استعمال الكمبيوتر في إنجلترا لسنة 1990[3] قد تضمن نصا يعطي الإختصاص للمحاكم الإنجليزية إذا كانت الجريمة لها علاقة بإنجلترا، وتتحقق تلك العلاقة لو وقعت الجريمة على كمبيوتر متواجد في إنجلترا أو باستعمال كمبيوتر متواجد فيها أو مرورا بهذا الكمبيوتر[4].

---

[1]– د. شيماء عبد الغني، المرجع السابق، ص 379.

[2]– د.جلال ثروت، نظم الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2003، ص 316. نقلا عن: د. حسين الغافري، المرجع السابق، ص 589.

[3]– نقلا عن: د.غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 227.

[4]– د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 227.

ثالثا: مكان القبض على المتهم.

يقصد به المكان الذي يقبض على المتهم وتصح محاكمته فيه، بحيث تكون المحكمة التي يقع هذا المكان في دائرتها هي المختصة مكانيا بنظر الدعوى، والحكمة المتوخاة هنا تكمن في أنه من الجائز أن يكون قد عثر مع المتهم على بعض الأدلة التي تساعد القاضي على كشف الحقيقة والتي يؤدي نقلها إلى تلفها أو ضياعها، وهذا الشيء متصور جدا في الجرائم الإلكترونية حيث توجد الأدلة الإلكترونية كما قد يكون المتهم من معتادي الإجرام، وبالتالي يكون من الخطورة نقله من مكان القبض عليه أو قد يتعذر معرفة مكان ارتكاب الجريمة[1].

ولذلك فإنه من الضروري إنشاء محاكم خاصة بالجرائم الإلكترونية على اعتبار أنه ظهرت أنماط جديدة من الجرائم، فلا يكفي للقائم بالتحقيق أن يكون ملما بالقوانين الجنائية التي يتشكل منها التحقيق الجنائي، بل عليه أن يستزيد من المعلومات العامة وسائر العلوم والقوانين الأخرى التي تتصل بمهنته الأساسية، سيما القوانين المتعلقة بتكنولوجيا المعلومات والإتصالات وشبكة الإنترنت، وكلما زادت معلوماته العامة وثقافته كلما أدى ذلك إلى زيادة خبرته ودرايته بشؤون الحياة العامة، وأدى ذلك لنجاحه وتحقيق هدفه، وإلمام المحقق بهذه العلوم لا يقتضي إلمام المتخصص فيها، بل يكفي أن يكون ملما بأساسيات تلك العلوم لأنه يوجد من الوقائع ما تحتاج إلى معلومات فنية حتى يستظهر عناصر الجريمة[2].

كما ينبغي أيضا ضرورة وضع تنظيم دولي تتبناه الدول المختلفة في قوانينها لتحديد المحكمة المختصة في الجرائم الإلكترونية، وأن يؤول الإختصاص في الدعاوى الجنائية إلى محكمة تواجد الكمبيوتر الذي صدر منه الفعل المعاقب عليها، كما لو أمر المتهم جهازا متواجدا خارج إقليم الدولة التي يقيم فيها بتحويل مبالغ مالية بدون وجه حق، كما يجب أن يؤول الإختصاص إلى محاكم الدولة التي يتواجد فيها مكان وجود هذا الجهاز الأخير الذي صدر إليه الأمر بالإضافة إلى مكان وجود الجهاز الخادم الذي توسط بين جهاز المتهم وجهاز المجني عليه[3].

---

[1]– د.جلال ثروت، المرجع السابق، ص 316. نقلا عن: د. حسين الغافري، المرجع السابق، ص 590.

[2]– د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 118.

[3]– د. شيماء عبد الغني، المرجع السابق، ص 377.

المبحث الثاني: حرية القاضي الجزائي في قبول الدليل الإلكتروني وتقديره.

يثير مبدأ حرية الإثبات في المواد الجزائية مسألة غاية في الأهمية، حيث يتحدد بها ذلك الفهم الحقيقي المنشود للمبدأ، ويتضح من خلالها نطاقه ومداه، وتتعلق تلك المسألة بحقيقة الحرية المسيطرة على قواعد الإثبات الجزائي، ولذلك فإن تحديد حقيقة هذا المبدأ يستلزم ضرورة التعرض لمسألة مدى الحرية الموجودة في نطاق العملية الإثباتية[1].

ولاشك أن مبدأ حرية الإثبات يختلف عن مبدأ حرية القاضي في الإقتناع، هذا الأخير الذي يسيطر على الإثبات الجنائي، فالقاضي الجزائي يستطيع أن يستمد عقيدته من أي دليل يرتاح إليه وجدانه، وهذه الحرية التي يتمتع بها القاضي الجزائي ليست مقررة لكي تتسع سلطته من حيث الإدانة أو البراءة، وإنما هي مقررة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجزائية، فاستنباط الحقيقة من هذا الدليل إنما يتم بمعرفة القاضي ومدى قدرته على الوصول إلى الحقيقة وما لديه من علم ومدى توافر حاسة القضاء لديه.

ولذلك فالقاضي الجزائي يتمتع دائما بدور إيجابي في الدعوى الجزائية، غير أن القاضي وعلى الرغم من أنه يتمتع بالحرية في تكوين عقيدته إلاّ أنه يلتزم ببيان الأدلة التي استمد منها اقتناعه، فليست الحرية أن نطلق له العنان لكي يقتنع بما يريد، وإنما هو حر فقط في استخلاص الحقيقة من أي مصدر مشروع، فهناك طرق للإثبات نص عليها قانون الإجراءات الجزائية وهي التي تعتبر مشروعة وهي التي يجوز له استخلاص الحقيقة منها[2].

فلا تقف الصعوبات التي تواجه الدليل الإلكتروني عند كيفية الحصول عليه وإجراءات حفظه كما تبين سابقا، بل تمتد إلى مدى القوة الثبوتية التي يتمتع بها هذا الدليل، ومدى حرية قاضي الموضوع بالإقتناع به لبناء الحكم على أساسه، لذلك حاول الفقه والقانون والقضاء التصدي لهذه المسألة وذلك بتحديد الشروط التي يجب توفرها في الدليل الإلكتروني حتى يمكن قبوله من قبل القاضي الجزائي[3]، على اعتبار أن الأدلة المتحصلة عن الوسائل الإلكترونية قد توجس منها كل من القضاء والفقه مخافة من عدم تعبيرها عن الحقيقة نظرا لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتزييف والتحريف والأخطاء المتعددة[4].

فينبغي ألاّ يؤسس القاضي اقتناعه على دليل لحقه سبب يبطله أو يعدم أثره، فلا يصح أن يبنى حكم صحيح بالإدانة أو البراءة على دليل باطل في القانون،كما أن المحاكم مثلا قبلت بالدليل المستمد من الآلة

---

[1] – د. أحمد ضياء الدين محمد خليل، المرجع السابق، ص 244.

[2] – د.علي محمود حمودة، المرجع السابق، ص61.

[3] – د.محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 354.

[4] – د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 187.

بشكل عام كما هو الشأن في كاميرات المراقبة في المصارف والطرق السريعة، وتم ترتيب أحكام القانون في ضوء ما تسفر عنه من نتائج، وهذا ما يجعل منطق قبول الدليل المستمد من الحاسب الآلي واردا لاتحاد كل من الدليلين في الأساس وهو الآلة أو المنطق الرقمي أو التكنولوجي ككل[1].

وعلى هذا الأساس قسم هذا المبحث إلى أربعة مطالب، سيتم التطرق في المطلب الأول إلى موقف القوانين اللاتينية من الدليل الإلكتروني، أما المطلب الثاني فأتناول فيه موقف القوانين الأنجلوساكسونية من الدليل الإلكتروني، أمّا المطلب الثالث فخصص لموقف القوانين ذات الصياغة المختلطة من الدليل الإلكتروني، كما تم التطرق للنتائج المترتبة على تطبيق مبدأ الإقتناع الشخصي بالدليل الإلكتروني.

المطلب الأول: موقف القوانين اللاتينية من الدليل الإلكتروني.

القوانين ذات الصياغة اللاتينية تشمل القانون الفرنسي والقوانين الأخرى التي تأثرت به كالقانون الإيطالي والإسباني، وقوانين أمريكا اللاتينية، وتشمل أيضا القانون الألماني والقوانين المشتقة منه، ذلك أنّ القانون الألماني وإن لم يكن لاتيني النزعة إلاّ أنّ صياغته تتشابه مع القانون الفرنسي، بالإضافة إلى القانون المصري وكذا الجزائري، وهذه القوانين تتشابه في الصياغة، فمصادر القانون فيها واحدة وأصولها العامة متحدة وتقسيماتها متماثلة والإصطلاحات القانونية فيها متشابهة، كما أن نظام الإثبات الحر هو السائد في هذه النوعية من القوانين[2]، فطبيعة النظام هو المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الإلكتروني[3]، وسأتطرق في هذا المطلب للطبيعة القانونية للإثبات بالدليل الإلكتروني في الفرع الأول، أمّا الفرع الثاني فخصص لحجية الدليل الإلكتروني.

الفرع الأول: الطبيعة القانونية للإثبات بالدليل الإلكتروني.

في نظام الإثبات الحر لا يحدد القانون أدلة الإثبات ووسائله، بل يترك للقاضي الحرية في أن يؤسس حكمه على أي دليل وفقا لاقتناعه الشخصي دون أن يفرض عليه أي دليل بعينه والإعتراف له بسلطة تقدير قيمة الدليل أو قيمة الأدلة مجتمعة، فهو يقوم على أساس أنّ القوة الإثباتية المقنعة لكل دليل ليست مفروضة على القاضي مقدما من المشرع، وإنما هي مرتبطة بما ترتبه من إقناع القاضي بحقيقة واقعة معينة، وبما يمليه عليه وجدانه وضميره، وكل الأدلة في هذا سواء ولحرية القاضي الجزائي في الإثبات وفقا لهذا النظام وجهان هما:

---

[1]– أنظر في ذلك: د. طارق فوزي الفقي، المرجع السابق، ص209، و كذلك : د. طارق عبد الرؤوف الخن، المرجع السابق، ص 364.

[2]– د.هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية ، المرجع السابق، ص29.

[3] –أ. رشيدة بوكر، الدليل الإلكتروني ومدى حجيته في الإثبات الجزائي في القانون الجزائري، مجلة جامعة دمشق للعلوم الإقتصادية و القانونية، سوريا، المجلد 27، العدد 02، سنة 2011، ص 314.

الأول: أنّ للقاضي الجزائي سلطة قبول أي دليل يمكن أن يتولد معه اقتناعه، فجميع طرق الإثبات أمام القاضي الجزائي سواء.

الثاني: أن القاضي الجزائي نفسه هو الذي يقرر حسب اقتناعه الذاتي الداخلي قبول الدليل من عدمه بشرط أن يكون استنتاجه لحقيقة الواقعة وما كشف عنها من أدلة لا تخرج عن مقتضيات العقل والمنطق، فالحرية التي يتمتع بها القاضي الجزائي في هذا المجال ليست مقررة لكي تتسع سلطته من حيث الإدانة أو البراءة، وإنما هي مقررة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجنائية[1].

هذا وقد أقرت نظام الإثبات الحر المادة (302)[2] من قانون الإجراءات الجزائية المصري، كما أقرته أيضا المادة (427)[3] من نفس القانون، وأيضا نصت المادة (212)[4] من قانون الإجراءات الجزائية الجزائري على جواز إثبات الجرائم بأي طريق من طرق الإثبات.

وهناك أسباب عديدة تبرر الأخذ بمبدأ حرية الإثبات والإقتناع، منها ظهور الأدلة العلمية وتقدمها، مثل تلك الأدلة المستمدة من الطب الشرعي والتحاليل ومضاهاة الخطوط وغيرها، وهي لا تقبل بطبيعتها إخضاع القاضي لأي قيود بشأنها، بل ينبغي أن يترك الأمر في تقديرها لمحض اقتناعه خصوصا وأنها كثيرا ما تتضارب مع باقي أدلة الدعوى، وذلك فضلا عن احتمال تضارب آراء المختصين في شأنها[5].

وهكذا يتميز نظام الإثبات الحر بالدور الفعال للقاضي حيال الدليل، وعلى هذا الأساس سيتم التطرق لمفهوم دور القاضي في البحث عن الأدلة في الجرائم الإلكترونية ومظاهر هذا الدور حيال الدليل الإلكتروني.

أولا: مفهوم الدور الفعال للقاضي الجزائي حيال الدليل الإلكتروني.

إن التطبيق الصارم لقاعدة البراءة الأصلية يؤدي إلى إعفاء الشخص المتابع جنائيا إعفاءا كليا من تحمل كل عبء في ميدان الإثبات، هذا الإثبات الذي يمتد إلى العناصر الثلاثة المكونة للجريمة : الركن

---

[1]- د.حسين الغافري، المرجع السابق، ص 598.

[2]- تنص المادة 302 من قانون الإجراءات الجزائية المصري على ما يلي: " يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته".

[3]- تنص المادة 427 من قانون الإجراءات الجزائية المصري على ما يلي: " تثبت الجرائم بجميع طرق الإثبات ويحكم القاضي تبعا لاقتناعه الخاص".

[4]- تنص المادة 212 من قانون الإجراءات الجزائية الجزائري على ما يلي: " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص.

ولا يسوغ لقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه ".

[5]- د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق،ص 39.

الشرعي، الركن المادي والركن المعنوي، غير أن الشخص قد يجد نفسه مرغما بالرغم من تمتعه بالبراءة الأصلية على الدفاع عن مصلحته حتى يتمكن من إبعاد التهمة الموجهة ضده.

ولا شك أن مهمة جمع أدلة الإثبات هي مهمة ثقيلة وصعبة، لذلك أطلقت عليها تسمية عبء الإثبات، فهذا العبء تتحمله الأطراف في الدعوى الجنائية ممثلة في النيابة العامة، المجني عليه والجاني، إلا أنه لا يمكن إغفال الدور الذي يلعبه القاضي الجزائي في الإثبات إذ يقوم بمساعدة هذه الأطراف لما يتمتع به من وسائل قوية تسمح له بالبحث عن الأدلة[1].

فالدعوى الجزائية هي نشاط القاضي فهو القائم على إدارتها، من هنا كان لزاما عليه أن يصل إلى معرفة الحقيقة المادية كما حدثت في الواقع، أي أن يصل إلى الحقيقة الصحيحة المضبوطة التي تشكل اقتناعه، وعلى ذلك فهو ملزم بالبحث عنها وإقامة الدليل عليها وهذا الدور يبدو من ناحيتين، فمن ناحية فإنّ القاضي حر في أن يستعين بكافة طرق الإثبات للبحث عن الحقيقة والكشف عنها، وهو في ذلك يختلف عن القاضي المدني الذي يكون دوره في الدعوى المدنية المنظورة أمامه سلبيا يقتصر على الموازنة بين أدلة الخصوم الذين يلعبون دورا إيجابيا ويقدمون للمحكمة الأدلة التي يرون أنها مفيدة في تدعيم مراكزهم القانونية، وهكذا فإنّ القاضي المدني لا يملك أن يبحث بنفسه فيما يعتقد أنه مفيد في إظهار الحقيقة بل يجب أن يكتفي بعناصر الإثبات التي قدمها الأطراف، وهذا يرجع في الواقع إلى أنّ الإثبات الجنائي يعالج وقائع مادية ونفسية وليس مجرد تصرفات قانونية والتي هي موضوع الإثبات المدني.

وهكذا فإنّ للقاضي الجزائي سواء بناءا على طلبات الأطراف أو بموجب مقتضيات وظيفته، أن يأمر باتخاذ الإجراء الذي يراه مناسبا وضروريا للفصل في الدعوى، فله أن ينتقل إلى محل الواقعة وأن يأخذ أقوال المتهم بل وأن يقوم باستجوابه، كما خوله القانون حق استدعاء الشهود، وندب الخبراء، كذلك أن يأمر باستكمال التحقيق إذا ما كانت عناصر الإثبات التي بين يديه غير كافية أو غير مقنعة، أيضا فإنّ القاضي يتعين عليه أن يتحقق بنفسه من عدم وجود أدلة براءة ظاهرة حتى ولو لم يدفع المتهم بها[2].

وعلاوة على ذلك، فإنه أمام محكمة الجنايات الفرنسية، فإنّ سلطة القاضي تبدو أكثر اتساعا وشمولا، ذلك أنّ المشرع الفرنسي قد خول رئيس محكمة الجنايات سلطة تفويضية بمقتضاها يمكنه أن يتخذ كافة

[1]- د. محمد مروان، المرجع السابق، ج 2، ص 138 و ما بعدها.

[2]- د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص 30.

الإجراءات التي يعتقد أنها مفيدة في الكشف عن الحقيقة حيث لا قيد عليه سوى شرفه وضميره[1] المادة (310)[2] من قانون الإجراءات الجزائية الفرنسي.

ثانيا: مظاهر الدور الفعال للقاضي الجزائي حيال الدليل الإلكتروني.

تطبيقا على الجرائم الإلكترونية فإن القاضي الجزائي يستطيع من أجل الوصول إلى الحقيقة أن يطلع على جميع الأفعال التي قام بها مستخدم الإنترنت وهو متصل بها كعناوين المواقع التي زارها، ووقت الزيارة والصفحات التي اطلع عليها والملفات التي جلبها والكلمات والمعلومات التي بحث عنها والحوارات التي شارك فيها والرسائل الإلكترونية التي أرسلها ونماذج الشراء التي قام بتعبئتها والتوقيع عليها وغيرها من الأفعال، وذلك عن طريق مزود خدمات الإنترنت الذي عادة ما يحتفظ بسجلات تحوي كل أفعال مستخدم الإنترنت عندما يتصل بالشبكة.

كذلك من الممكن للقاضي الجزائي الإستماع لأقوال الشهود في الجرائم الإلكترونية والتي تعد من أكثر الأدلة حرجا سواء لصالح الإتهام أو الدفاع، لذا كان لابد من تقديم الشهود وفق ضوابط محدّدة وحتى يتحقق ذلك لابد من مراعاة ما يلي:

- تحديد النقاط التي ينبغي إثباتها أمام المحكمة تحديدا دقيقا.
- وضع أسئلة نموذجية مرتبة وفقا للوقائع ترتيبا منطقيا ولها إجابات مؤكدة لإثبات تلك النقاط.
- تحديد الشهود الذين توجه لهم الأسئلة.
- وضع بدائل للأسئلة لمزيد من الشرح في حالة فشل الشاهد في إعطاء إجابات مقنعة.

والشاهد المعلوماتي كما تبين سابقا، هو الفني صاحب الخبرة و التخصص في تقنية المعلومات وعلوم الحاسب الآلي والإنترنت والذي تكون لديه معلومات جوهرية لازمة للولوج إلى نظام المعالجة الآلية للبيانات، فالقاضي يستطيع أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة، وإذا وجدت بيانات مشفرة داخل ذاكرة الحاسب الآلي وكانت المصلحة تستلزم الحصول عليها، يتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات، كذلك فإنّ القاضي الجزائي من أجل البحث عن الأدلة

[1]– د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص 32.

[2] - Article 310 (C.P.P.F Modifié par Loi 72-1226 1972-12-29 art. 6-I, 6-II JORF 30 décembre 1972 en vigueur le 1er janvier 1973) : Le président est investi d'un pouvoir discrétionnaire en vertu duquel il peut, en son honneur et en sa conscience, prendre toutes mesures qu'il croit utiles pour découvrir la vérité. Il peut, s'il l'estime opportun, saisir la cour qui statue dans les conditions prévues à l'article 316…

للوصول إلى الحقيقة له أن يأمر بتفتيش نظم الحاسب الآلي بمكوناته المادية والمعنوية وشبكات الإتصال مثلما تبين سابقا.

وفي مجال الحاسب الآلي والإنترنت تعد الخبرة التقنية من أقوى مظاهر التعامل والتفاعل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات، فهي تؤدي دورا لا يستهان به خاصة مع نقص المعرفة القضائية الشخصية لظاهرة الإنترنت، ومن أهم المسائل التي عادة ما يلجأ القاضي الجزائي فيها إلى الخبرة، تلك المتعلقة بأمور فنية كتركيب أجهزة الحاسب الآلي أو صناعتها أو أنواعها المختلفة، بالإضافة إلى معرفة أنظمة التشغيل التي تعمل عليه، وأهم الأنظمة الفرعية التي يستخدمها بالإضافة إلى الأجهزة الطرفية الملحقة بها وكلمات المرور ونظام التشفير وغيرها من المسائل المعلوماتية.

فخلاصة القول أنّ للقاضي الجزائي دورا فعالا في البحث عن الأدلة وفحصها وتمحيصها وبالتالي الوصول إلى الحقيقة الواقعية ليصدر الحكم بعد ذلك حسب القناعة التي تكونت لديه بكامل حريته[1]، وعليه يكون للقاضي السلطة التقديرية في رفض الأدلة إذا لم يقتنع بها، والخبير يقوم بدور مساعد باعتبار أن الأدلة الإلكترونية أصبحت جزء لا يتجزأ من أدلة الإثبات، فهي ليست سوى شكل خاص منها[2].

الفرع الثاني: حجية الدليل الإلكتروني في القوانين ذات الصياغة اللاتينية.

إذا تم الحديث عن مناقشة حجية الدليل الإلكتروني في القوانين ذات الصياغة اللاتينية حيث يسود مبدأ حرية الإثبات والإقتناع، فإنّ حجية هذا الدليل لا تثير صعوبات سواء بالنسبة لمدى حرية تقديم الدليل الإلكتروني لإثبات الجرائم الإلكترونية، أم بالنسبة لمدى حرية القاضي الجزائي في تقدير الدليل الإلكتروني[3]، وسيتم التطرق لموقف القوانين الغربية والعربية ثم موقف القانون الجزائري، وذلك كما يلي:

البند الأول:حجية الدليل الإلكتروني في القوانين الغربية.

سيتم التطرق من خلال هذا البند لحجية الدليل الإلكتروني في فرنسا وألمانيا واليونان وذلك على النحو التالي:

---

[1]- د. حسين الغافري، المرجع السابق، ص 594.

[2] - Margot Stephan, Le régime de la preuve électronique, le 31/03/2014, disponible à l'adresse suivante : www.faq-adullact.org et voir : Stéphanie Lacour et Marion Videau, Légistique de la preuve électronique, Mars 2007, disponible à l'adresse suivante : www.demotis.org.

[3]- د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 42.

أولا: فرنسا.

الواقع أنّ الفقه الفرنسي يدرس حجية الدليل الإلكتروني في المواد الجنائية ضمن مسألة أوسع وأعم هي مسألة قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل الرادارات والأجهزة السينمائية وأجهزة التصوير وأشرطة التسجيل وأجهزة التنصت.

أما القضاء فقد قبل بهذه الأدلة إذا توفرت فيها مجموعة من الشروط، من أهمها أن يتم الحصول عليها بطريقة شرعية ونزيهة، وأن يتم مناقشتها حضوريا من قبل الأطراف، وقد قضت محكمة النقض الفرنسية بأنّ أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجزائي[1].

أما بالنسبة إلى قناعة القاضي الجزائي، فإنّ الأدلة الإلكترونية تخضع لحرية القاضي في الإقتناع الذاتي، بحيث يمكن أن يطرح مثل هذه الأدلة رغم قطعيتها من الناحية العلمية عندما يجد أنّ الدليل الإلكتروني لا يتسق منطقيا مع ظروف الواقعة وملابساتها[2].

وقد أثيرت في فرنسا مشكلة الإثبات لمحاضر المخالفات التي تتم عن طريق جهاز السينمومتر[3]، وانتهى الخلاف إلى عدم اعتبار محاضر المخالفات المحررة بإثبات المخالفة حجة بذاتها في الإثبات، كما أنّ أي محضر لا تكون له قوة إثباتية إلاّ إذا أثبت فيه محرره وقائع تدخل في اختصاصه، وأن يكون قد شاهدها أو سمعها أو تحقق منها بنفسه.

وبناءا على ذلك يمكن القول بأنّ المحضر الذي يحرره القائم بالتحقيق وذلك عقب عملية المراقبة الإلكترونية للسيارات لا يصلح دليلا على ارتكاب الجريمة، حيث أنّ محرري المحضر لم يتحققوا بأنفسهم من ارتكاب المخالفة.

---

[1] - Cass.Crim.28avr.1987, BULL.Crim.no 173.

نقلا عن :د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 43.

[2]– د.محمد طارق عبد الرؤوف الخن، المرجع السابق،ص 360.

[3]– لقد أصبح بالإمكان قياس سرعة السيارة باستخدام جهاز يطلق عليه السينمومتر، ويوجد حاليا أنواع مختلفة من أجهزة السينمومتر، النوع الأول يطلق عليه إسم مستا Mesta، وهو جهاز يتم تشغيله يدويا، فعندما تمر السيارة المطلوب قياس سرعتها يقوم العامل الفني الضغط على زر معين فيظهر رقم سرعة السيارة على شاشة جهاز السينمومتر وتظل مقروءة طالما أنه لم يضغط على الزر مرة ثانية.

والنوع الثاني من السينمومتر يطلق عليه اسم أسبيك Aspic، فهو جهاز أوتوماتيكي يوضع على حافة الجهة اليمنى من الطريق، ويقوم بعمليتين الأولى التصوير من الخلف والعملية الثانية تتمثل في أنه يسجل في نفس الوقت سرعتها في هذه اللحظة.

أما النوع الثالث من السينمومتر يطلق عيله اسم ترافيباكس traffibax، وهو جهاز يتم تركيبه على سيارة متحركة والتي تقوم بتتبع السيارة المراقبة ويترتب على ذلك أنّ عملية المراقبة باستخدام جهاز السينمومتر قد تتم شكل يدوي أو نصف أوتوماتيكي.أنظر في ذلك: د.جميل عبد الباقي الصغير، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، المرجع السابق، ص01.

وإذا كان الضابط الذي يحرر المخالفة للقيادة بسرعة تزيد عن السرعة المقررة والتي يتم ضبطها عن طريق جهاز الرادار طبقا لقانون المرور المصري، لا يكون قد شاهد بنفسه المخالفة وإنما قام بتسجيلها فقط عن طريق الإشارة اللاسلكية التي تكون قد وصلت إليه، ولذلك فإنّ تقرير مخالفة المرور عن هذه المخالفة لا يمكن أن يحل محل محضر جمع الإستدلالات ولا يصلح لأن يكون دليلا قائما بذاته لإثبات المخالفة[1].

ثانيا: ألمانيا.

طرحت كذلك مسألة مدى قبول الدليل الإلكتروني في إجراءات المحاكمة، حيث أنّ الفقرة الثانية من المادة (224) من قانون الإجراءات الجزائية تلقى على المحكمة التزاما في الوصول إلى الحقيقة والأخذ بالأدلة لكل الوقائع والبنود التي تكون هامة في اتخاذ الحكم، وهذا يعني أن تكون مخرجات الحاسب بأنواعها المختلفة من مطبوعات أو بيانات أحد المصادر التي تقبلها المحكمة وأن تستقي منها اقتناعها طبقا لنص المادة (26) من قانون الإجراءات الجزائية[2].

ثالثا: اليونان.

يسود مبدأ حرية قبول الأدلة وحرية تقييمها، وتبعا لذلك لا يثير اللجوء في الإثبات في المواد الجنائية إلى الأدلة المستمدة أو الناشئة عن الحاسب أية مشكلات، ومع ذلك فإنّ شكا يمكن أن يثور في هذه الحالة نتيجة تطلب المادة (362) من التقنين الإجرائي اليوناني قراءة المستندات والوثائق التي استخدمت كأدلة أثناء التحقيقات، لأنه إذا ما تمثلت هذه المستندات في ذاكرات داخلية أو خارجية لنظام الحاسب، فإنّ القراءة المباشرة لها تكون ممكنة وبسبب ذلك يكون على المحكمة أن تقرر إما اللجوء إلى القراءة غير المباشرة من خلال عرض محتوى الذاكرة على شاشة الحاسب أو اللجوء إلى طباعة البيانات المخزنة[3].

البند الثاني: حجية الدليل الإلكتروني في القوانين العربية.

سيتم التطرق لحجية الدليل الإلكتروني في القانون المصري والقانون العماني وذلك على النحو التالي:

[1]- د.أحمد محمود مصطفى، المرجع السابق، ص 363.

[2]- نقلا عن :د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص44.

[3]- نقلا عن :د.هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية ، المرجع السابق، ص 157.

أولا: القانون المصري.

بالنسبة لحجية الدليل الإلكتروني في مصر، فقد خلا التشريع من التعرض لذلك غير أنه وبالرغم من خلو التشريع الإجرائي المصري من التعرض لهذه المسألة، فإنه يمكن الإستناد إلى المخرجات الكمبيوترية في إثبات أو نفي الجريمة وتكون لها قوة القرائن في الإثبات، حيث أنّ المشرع المصري أخذ بمبدأ الإثبات الحر، فقد نص في المادة (291) من قانون الإجراءات الجزائية المصري على أنه: "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة"، وعلى ذلك يكون للمحكمة أن تستند إلى الدليل الإلكتروني لإثبات وقوع الجريمة أو نفيها[1].

ثانيا: القانون العماني.

مع تزايد الإعتماد على مسائل تقنية المعلومات في إدارة وإنفاذ الأعمال المختلفة في السلطنة إزداد الإهتمام بمبدأ حجية وقوة وسائل التخزين التقني للمعلومات في الإثبات، ومدى حجية الدليل الإلكتروني، ومدى إمكان النظام القانوني للإثبات استيعاب هذه الأنماط المستجدة من وسائل الإثبات.

فالقاعدة في الدعاوى الجزائية جواز الإثبات بكافة طرق الإثبات القانونية، والقيد على هذه القاعدة أنّ الدليل يتعين أن يكون من الأدلة التي يقبلها القانون، وبالتالي تظهر أهمية اعتراف القانون بالأدلة ذات الطبيعة الإلكترونية.

فالمشرع في سلطنة عمان لم يختلف عن المشرع المصري فيما يتعلق بحجية الدليل الإلكتروني، إلاّ أنّ المشرع العماني نص في المادة (186) من قانون الإجراءات الجزائية على أنه: "ليس لمحاضر التحقيقات السابقة على المحاكمة حجية في الإثبات أمام المحكمة، وإنما يجوز لها الإستفادة منها في استخلاص القرائن واستخدام عناصرها في مناقشة المحقق كشاهد بعد حلفه اليمين فيما أثبته في محاضره، " وكذلك المادة (215) من قانون الإجراءات الجزائية التي نصت على أنه: "يحكم القاضي في الدعوى حسب القناعة التي تكونت لديه بكامل حريته، ومع ذلك لا يجوز أن يبنى حكمه على أي دليل لم يطرح على الخصوم أمامه في الجلسة أو على معلوماته الشخصية".

[1]– د.سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2007، ص 366.

وبالتالي فالمحكمة لها أن تستعين بالخبرة في سبيل التيقن من الدليل الإلكتروني المقدم وأن تناقش الخبير عن الجوانب الفنية في الحاسب الآلي المتعلقة بالجريمة، لكي يصل القاضي من خلالها إلى قناعة معينة يترتب عليها صدور حكم في الدعوى [1].

البند الثالث : حجية الدليل الإلكتروني في القانون الجزائري.

لقد أخذ المشرع الجزائري بمبدأ حرية الإثبات طبقا لنص المادة (212) من قانون الإجراءات الجزائية الجزائري، بحيث يجوز إثبات الجرائم بكل طرق الإثبات دون تمييز بين دليل وآخر مادام أنّ المشرع لم ينص على ما يخالف ذلك صراحة، ويترتب على ذلك تكافؤ قيمة الأدلة كقاعدة عامة مادام جمعها وتقديمها قد تم وفقا لأحكام قانون الإجراءات، فلا فرق بين قوة الدليل سواء كان كتابيا أو شفويا، مباشرا أو غير مباشر، فالعبرة فقط بمدى تأثيره وإقناعه للقاضي، فالغاية النهائية من جمع الأدلة وتقديمها ليس الوصول إلى الدليل القاطع بحد ذاته وإنما الوصول إلى إقناع القاضي[2]، كما نص المشرع الجزائري على مبدأ الإقتناع الشخصي بموجب نص المادة (307)[3] من قانون الإجراءات الجزائية.

غير أن التشريع الجزائري لم يتطرق لمسألة حجية الدليل الإلكتروني، إلاّ أنه ما دام يعتنق نظام الإثبات الحر، فيكون الدليل الإلكتروني مقبولا في الإثبات.

وهذا يعني أنّ للقاضي الجزائي مطلق الحرية في أن يصل إلى الحقيقة من أي دليل قانوني مهما كان نوعه بما في ذلك الدليل الإلكتروني، فيستمد القاضي قناعته من أي دليل يطمئن إليه من الأدلة التي تقدم في الدعوى دون التقيد بدليل معين ما لم ينص القانون على غير ذلك، فلا يوجد أدلة يحظر القانون عليه قبولها، فالقانون أمد القاضي الجزائي سلطة واسعة وحرية كاملة في مجال الإثبات، ويمكن الأخذ بالدليل الإلكتروني سواء في إطار الإدانة أو البراءة إذا توافرت في هذا الدليل الشروط التالية:

أ- **المشروعية:** أي أن يتم الحصول على الدليل الإلكتروني بصورة قانونية.

---

[1]- د.هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص 260.

[2]- د.رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، سوريا، ط1، بدون سنة، ص303.

[3]- تنص المادة 307 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يتلو الرئيس قبل مغادرة المحكمة قاعة الجلسة التعليمات الآتية التي تعلق فضلا عن ذلك بحروف كبيرة في أظهر مكان من غرفة المداولة.

(إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم و أوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم :

هل لديكم اقتناع شخصي؟)".

ب- **الصحة و المطابقة:** أي أن يكون الدليل الإلكتروني المقدم إلى المحكمة هو نفس الدليل الذي تم جمعه، وأن لا يطرأ على هذا الدليل أي تغيير خلال فترة حفظه.

ج- **الدقة:** أي أنّ نظام الحاسوب الذي استخرج منه الدليل يعمل على نحو دقيق وسليم، بحيث لا يتطرق الشك في دقته[1].

في حين يرى البعض أنّ المحاكم لم تواجه مشكلة في تعاملها مع الأدلة الجنائية الإلكترونية وذلك للأسباب التالية:

أ- الثقة التي اكتسبها الحاسوب والكفاءة التي حققتها النظم الحديثة للمعلوماتية في مختلف المجالات.

ب- إرتباط الأدلة الجنائية الإلكترونية وآثارها بالجريمة موضوع المحاكمة.

ج- وضوح الأدلة الإلكترونية ودقتها في إثبات العلاقة بين الجاني والمجني عليه، أو بين الجاني والسلوك الإجرامي.

د- إمكانية تعقب آثار الأدلة الإلكترونية والوصول إلى مصادرها بدقة.

هـ- قيام الأدلة الإلكترونية على نظريات حسابية مؤكدة لا يتطرق إليها الشك، مما يقوي يقينية الأدلة الإلكترونية التي تبنى على الدراسات والبحوث والتقنية العلمية.

و- إنتهاء العلم برأي قاطع إلى صحة النتائج التي توصلت إليها علوم الحاسوب.

ز- الأدلة الإلكترونية يدعمها عادة رأي خبير، وللخبرة في المواد الجنائية دورها في الكشف عن الأدلة وفحصها وتقسيمها، وعرضها أمام المحاكم وفق شروط وقواعد نظمها القانون وأقرها القضاء وبهذه الخبرة تأتي النتائج بصورة موضوعية.

ح- إنتشار الجريمة الإلكترونية وجرائم التقنية العالية كظاهرة مستحدثة لم يترك مجالا للبحث عن وسائل لتحقيق العدالة في سياق تلك الأنماط إلاّ من خلال ذات التقنية المعلوماتية[2]، وذلك حتى في الولايات المتحدة الأمريكية التي تعرف انتشارا لهذه الظاهرة بالرغم من الرقابة المفروضة عليها[3].

ط- الأدلة الإلكترونية تقوم على حقائق وأسس علمية ذات نتائج محددة ودقيقة وواضحة، لها أثرها على اقتناع القاضي يتجاوز في تأثيره كل أنواع الأدلة الأخرى[4].

---

[1]- د. محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 363.

[2]- د. ناصر بن محمد البقمي، المرجع السابق، ص 42.

[3] - Bruno Cormier, Cybercriminalité aux USA, disponible à l'adresse suivante : www.pointpact.com.

[4]- د. ناصر بن محمد البقمي، المرجع السابق، ص 43.

ي–أن تطور الجريمة واستفادتها من التطور العلمي يفرض مواجهتها بالأسلوب نفسه سواء في مجال الضبط أو التحقيق أو المحاكمة[1].

فنظام الإثبات الحر لا يلزم القاضي بقبول أو رفض أي دليل، و إنما يكون لهذا الأخير الحرية التامة في الإستعانة بأي دليل يراه كاشفا للحقيقة، كما أن باقي أطراف الدعوى هم كذلك أحرارا في تقديم أي دليل يرونه مناسبا.

وبالرجوع إلى القانون (09-04) الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، فلم يتطرق للدليل الإلكتروني، ولا شك أن هذا الموقف يدعو إلى ضرورة الأخذ بمبدأ حرية الإثبات.

ومن التطبيقات القضائية في هذا الشأن، ما ذهب إليه مجلس قضاء سيدي بلعباس بإدانة المتهم بعقوبة الحبس والغرامة[2] في قضية تتلخص وقائعها أنه بتاريخ 07-11-2007، تقدمت أمام مصالح الشرطة المسماة (ب،ز)، الممثلة القانونية لشركة إتصالات الجزائر للهاتف النقال فرع (موبيليس)، للإبلاغ عن وضع جهاز قرصنة على مستوى نظام الإعلام الآلي لشركة (موبيليس) بوكالة سيدي بلعباس، والذي تم اكتشافه من خلال عملية مراقبة تقنية بالوكالة، موضوع داخل خزانة توصيل كوابل نظام الإعلام الآلي للمعطيات الخاصة بالوكالة، واضعة تحت تصرفهم محضر معاينة ميدانية منجز من طرف المحضر القضائي.

وعلى إثر إبلاغ رجال الشرطة إنتقلوا إلى عين المكان، وتبين من المعاينة الميدانية وجود قاعة مخصصة لتبديل الملابس والإستراحة بداخلها خزانة ذات باب زجاجي مقفل، تحتوي على تجهيزات إلكترونية وتوصيلات وكوابل، مع وجود جهاز إلكتروني دخيل تم تثبيته بإحكام من طرف شخص له معرفة جيدة في مجال الإعلام الآلي مزود بجهاز للشحن من نوع(LINK SYS) MAC 001A70EF1152 ADRESS متصل بكابل يؤدي إلى جهاز آخر مركب بنفس الخزانة إسمه تقنيا Router Wifi متصل بالشبكة الوطنية للهاتف النقال (موبيليس)، أين تم أخذ صور فوتوغرافية لمسرح الجريمة، وكذا وضعية الجهاز الذي تم حجزه و وضعه في حرز مختوم كدليل إثبات مادي في قضية الحال.

[1]– د. ناصر بن محمد البقمي، المرجع السابق، ص 43.

[2]- قرار رقم 10/07841 صادر بتاريخ 2010/07/11 عن الغرفة الجزائية بمجلس قضاء سيدي بلعباس.

وقد تم إرسال الجهاز الإلكتروني المحجوز إلى المديرية الجهوية للوسائل والإتصالات بوهران لإجراء خبرة تقنية لتحديد نطاق استعماله ووظائفه، وبعد التحقيقات تمت متابعة المتهم(ب.ع) لارتكابه جنحة إدخال وتعديل بطريق الغش لمعطيات في نظام المعالجة الآلية، حيث أن المتهم قام بالدخول وتعديل معطيات في الأنظمة المعالجة آليا، فجهاز Router Wifi هو جهاز يستعمل للدخول إلى الشبكة المعلوماتية عن بعد، وهذا ما أكده تقرير المديرية الجهوية لشركة إتصالات الجزائر، وذلك من أجل تزويد شرائح بأرصدة بدون وجه حق، وكذا مسح الديون لبعض الزبائن، كما استعمل شرائح مزودة من طرفه عن طريق دخوله بطريق الغش في نظام Minsat وبيعها وطرحها في السوق وتوزيعها على الأكشاك.

المطلب الثاني: موقف القوانين الأنجلوساكسونية من الدليل الإلكتروني.

يقصد بالقوانين ذات الصياغة الأنجلوساكسونية تلك النظم القانونية التي تعتنق النظام الإنجليزي، ويعد نظام الإثبات القانوني أو المقيد هو السائد في هذه القوانين[1]، وفي هذا النظام تكون الأدلة محصورة ومحددة سلفا من قبل المشرع، بل إنّ قوتها التدليلية محددة ولا يجوز للقاضي أن يخرج عليها أو يبني حكمه على خلافها، ويعني نظام الأدلة القانونية أنّ الشارع هو الذي يحدد للقاضي الأدلة التي يجوز له أن يقبلها في حالة معينة، فيحظر عليه أن يقبل أدلة سواها، وإن كان يجوز له قبول هذه الأخيرة في حالة مختلفة.

وبالإضافة إلى ذلك يحدد الشارع القيمة القانونية للدليل إذا توافرت شروط معينة، وعندها يلتزم القاضي الجزائي بالأخذ به وليس له رفضه، فإذا ما توافرت عناصر الدليل بالشكل المتطلب قانونا يكون القاضي ملزما بأن يبني اقتناعه ويؤسس حكمه على أساس هذا الدليل حتى وإن لم يكن مقتنعا به شخصيا، وإذا لم تتوافر تلك العناصر فالقاضي يكون على العكس ملزما ببناء اقتناعه وتأسيس حكمه على أساس عدم قيام الدليل على الإدعاء حتى وإن كان بداخله مقتنعا تماما بثبوت الإدعاء، فالدليل القانوني وفقا لهذا النظام هو الدليل الذي حدد القانون نوعه وقيمته مسبقا[2].

فدور القاضي في ظل هذا النظام هو دور آلي لا يتعدى مراعاة توفر الأدلة وشروطها القانونية، فهو لا يستطيع أن يتحرى عن الحقيقة بطرق أخرى لم ينص عليها المشرع ولا أن يطلب إكمال أدلة ناقصة، بل عليه أن يلتزم بما حدده المشرع، فهذا النظام يخرج القاضي عن وظيفته الطبيعية بينما هو يسمح للمشرع أن يتدخل في نطاق لا يملكه فهو من ناحية قد قام بتقنين اليقين في قواعد عامة محددة، رغم أن اليقين مسألة

[1]–د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص 49.

[2]– د. حسين الغافري، المرجع السابق، ص 596.

واقع ترتبط بظروف كل قضية وتترك لتقدير قاضي الموضوع، ومن ناحية أخرى فإنّ وضع القاضي في قالب جامد للإثبات قد ترتب عليه إفلات حالات كثيرة من العقاب رغم أن من واجبه أن يقيم موازنة معتدلة من حق الإنسان في البراءة، وحق المجتمع في العقاب.

غير أنه يمكن القول أنه قد طرأت بعض التغييرات على حدة هذا النظام فالقانون العام في إنجلترا لم يعد يأخذ بنظرية الأدلة القانونية على إطلاقها، بل بدأ يتقبل مبدأ حرية تقدير الأدلة، وهكذا إذا كانت قاعدة حرية القاضي في تقدير الدليل قائمة في كل الدول على اختلاف الصياغة فيها، فإنه يمكن أن يخلص إلى نتيجة مؤداها أنّ نظام الإثبات السائد في القوانين ذات الصياغة الأنجلوساكسونية أبعد من أن يكون إثباتا قانونيا أو مقيدا، وأدنى إلى أن يكون إثباتا مختلطا[1].

فالمبدأ العام في كل دول الشريعة العامة أنه يلزم في وسيلة الإثبات كي يكون جائزا قبولها، أن تتعلق بالواقعة التي تنشئ دليلا عليها، وأن يكون تعلقها بها متجاوزا أو يفوق بوضوح تأثيرها الضار على الدعوى، ومع ذلك تستبعد وسائل الإثبات التالية[2]:

1. الشهادة السماعية أو النقلية (غير المباشرة):

ويقصد بها إدلاء الشاهد وتقريره أمام القاضي بأحداث لم يعاينها شخصيا، وإنما استمد علمه بها من شخص آخر ليس موجود أمام القاضي، ونظرا لحدة قاعدة حظر الشهادة النقلية وحيلولتها في بعض الحالات دون ظهور الحقيقة لما يؤدي إليه من حرمان العدالة الجنائية من وسائل هامة للإثبات تفيد في اكتشافها، فقد وردت عليها استثناءات عديدة وفي ظلها قبلت تشريعات بعض الدول مخرجات الحاسب كأدلة إثبات في المواد الجزائية.

[1]– د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص 50.

[2]– د.هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية ، المرجع السابق ، ص 167.

2. الشهادة المفشية للسر المهني:

إنّ هذه الشهادة محظورة من حيث المبدأ وإن كان هناك فروقا بين الدول الأنجلوساكسونية تتعلق بمدى الحظر أو نطاقه، ففي الولايات المتحدة الأمريكية تحظر الشهادة المتعلقة بالأسرار بين الطبيب والمريض أو بين المحاسب وعميله[1].

أمّا فيما يتعلق بحجية الدليل الإلكتروني في القوانين الأنجلوساكسونية، سأتطرق إليها في الفروع التالية:

الفرع الأول: حجية الدليل الإلكتروني في القانون الأمريكي.

تبنى قانون الإثبات الفيدرالي في المادة (1002) منه قاعدة الدليل الأفضل، ويقصد بهذه القاعدة أنه عند إثبات مضمون كتابات أو سجلات أو صور، فإن أصل هذه الكتابات أو الصور أو السجلات يجب أن يكون متوفرا، أي يجب تقديمه للمحكمة.

وقاعدة الدليل الأفضل التي تعبر عن أصالة الدليل تقف حائلا أمام الدليل الإلكتروني، لأنّ ما يتم تقديمه إلى المحكمة ليس الملفات الإلكترونية المخزنة في الحاسوب، وإنما نسخ عن هذه الملفات، ولذلك فقد حسم المشرع الأمريكي هذه المسألة لصالح الدليل الإلكتروني في المادة (3/1001) من قانون الإثبات الأمريكي التي نصت:"إذا كانت البيانات مخزنة في حاسوب أو آلة مشابهة، فإنّ أي مخرجات مطبوعة منها أو مخرجات يمكن قراءتها بالنظر إليها وتعكس دقة البيانات تعد بيانات أصلية"[2].

ووفقا لهذه المادة، فإنّ البيانات أو المعلومات التي تم الحصول عليها من الإنترنت والتي تم استخراجها بواسطة الطابعة تعد دليلا أصليا كاملا ولا حاجة لجلب الحاسوب إلى قاعة المحكمة، أمّا فيما يخص القوة الإثباتية للسجلات الإلكترونية، فإنّ المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب الصادر في عام 2002 يميز بين نوعين من السجلات وهما:

[1]– د. هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 170.

[2]– نقلا عن: د.طارق عبد الرؤوف الخن، المرجع السابق، ص 355.

1- السجلات المخزنة في الحاسوب:

وهي الوثائق الإلكترونية التي تحتوي على كتابات عائدة لشخص ما، ومن أمثلتها: رسائل البريد الإلكتروني وملفات الوارد (WORD) ورسائل غرف الدردشة على الإنترنت، وهذه الوثائق تتضمن إفادات بشرية، وتعد كالشهادة على السماع في مجال الإثبات.

2- السجلات المأخوذة من الحاسوب:

وهي عبارة عن نتائج برامج الحاسوب التي لا تمسها الأيدي البشرية، ومن أمثلتها سجلات الدخول إلى الإنترنت وسجلات الهاتف وإيصالات الصراف الآلي وغيرها، فهذه السجلات لا تتضمن إفادات بشرية، وإنما هي عبارة عن نتائج البرامج الحاسوبية كأرقام وساعة ومدة المكالمات الهاتفية، وهذا النوع من السجلات يمكن للمحاكم أن تأخذ به، إذا كان برنامج الكمبيوتر يؤدي عمله على نحو جيد وسليم[1].

فالأصل إذن أنّ مخرجات الكمبيوتر تشكل شهادة سماعية ما دامت تتكون من جمل وكلمات أدخلها شخص إلى جهاز الكمبيوتر، سواء تم معالجة تلك البيانات أم لا، في هذه الحالة يتعين على سلطة الإدعاء أن تثبت أن مخرجات الكمبيوتر في هذه الحالة تشكل استثناءا على قاعدة الشهادة السماعية، وذلك حتى يتم الإعتداد بها كحجة في الإثبات.

غير أنه يجب التمييز بين المعلومات التي يضعها الإنسان والمعلومات التي تسجلها الآلة من تلقاء نفسها، فالأولى كما سبق الإشارة هي شهادة سماعية مثلها في ذلك مثل الكلمات أو التقريرات التي يسجلها الإنسان على الأجهزة المختلفة، ويرجع السبب في هذا التمييز إلى أنه في الحالة الأولى يقوم الشخص بدور إيجابي في تدوين البيانات أو الملفات، فيتعين عليه أن يحضر كشاهد إلى المحكمة لكي يحلف اليمين وتتم مناقشته في أقواله حتى تكون لها مصداقيتها، أمّا في الحالة الثانية فإن الجهاز هو الذي يقوم بتدوين البيانات التي تصلح أن تقدم مباشرة إلى المحكمة فهي ليست من قبيل الشهادة السماعية[2].

وهناك نوع ثالث من المستندات يجمع بين التدخل الإنساني ومعالجة الكمبيوتر، كما لو أدخل المتهم بيانات معينة وطلب من الكمبيوتر أن يقوم بمعالجتها توصلا إلى نتائج يسمح بها البرنامج المستخدم، كمن يتهرب من الضرائب فيقوم بتسجيل بيانات غير صحيحة عن دخله وربحه طالبا من الكمبيوتر حساب الضريبة المستحقة، في هذه الحالة يجب توافر شرطين لصحة المستند الإلكتروني الصادر عن الكمبيوتر، فمن

[1] – د. طارق عبد الرؤوف الحن، المرجع السابق، ص 356.

[2] - د. شيماء عبد الغني، المرجع السابق، ص 42 و ما بعدها.

جهة يجب توافر الشرط اللازم لصحة الشهادة السماعية، كما أنه يجب التأكد من عمل الجهاز نفسه على نحو صحيح.

وقد أكد القضاء الأمريكي هذا المعنى في قضية تخلص وقائعها، في أنّ متهما بتجارة المخدرات كان يقوم بتسجيل الصفقات الممنوعة في ثلاثة ملفات في الكمبيوتر الخاص به تحت أسماء مستعارة، وقد حصل رجال الضبط القضائي على هذه الملفات بمساعدة المتهم صاحب الكمبيوتر وذلك عند تفتيش الجهاز بناء على إذن بذلك، وقد تم ضبط ملفات تحتوي على أسماء المتعاملين مع المتهم الأول ما دفع أحد هؤلاء المتعاملين بعدم صحة إجراءات الضبط، وذلك لسهولة العبث بالبيانات وتغييرها وسهولة إدخال إسمه من المتهم الأول، ومع ذلك رفضت المحكمة هذا الدفع مستندة إلى أنه لا يشترط لصحة إجراءات ضبط بيانات الكمبيوتر أن يتم من جانب خبير[1].

ومن الواضح أنّ صحة الأدلة الإلكترونية تتوقف على صحة برامج التشغيل الذي يعمل الكمبيوتر بحسب تعليماته، ومن حق المتهم أن تتاح له الفرصة لإثبات أنّ برنامج التشغيل لا يعمل بطريقة صحيحة أو منتظمة، ويعتبر برنامج التشغيل صحيحا إذا كان صاحب الجهاز يعتمد عليه في تشغيله اليومي لسير أعماله وذلك بشكل منتظم، وإذا توافر شرط صحة الدليل من مخرجات الكمبيوتر فإنه يصبح دليلا مقبولا في الإثبات[2].

فالمشرع الأمريكي قد حسم حجية الدليل الإلكتروني وذلك بالنص عليه صراحة في القوانين الخاصة بالولايات المتحدة الأمريكية، حيث نص قانون الحاسب الآلي لسنة 1984 في ولاية أيوا (IOWA) من أنّ مخرجات الحاسب الآلي تكون مقبولة بوصفها أدلة إثبات بالنسبة لبرامج وبيانات الحاسب الآلي والمخزنة بداخله، كذلك نص قانون الإثبات الصادر سنة 1983 في ولاية كاليفورنيا من أن النسخ المستخرجة من المعلومات التي يحتويها الحاسب الآلي تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه المعلومات[3].

وبناءا على هذه القواعد، فإنه حتى يكون الدليل المقدم إلى المحكمة مقبولا، يجب أن تتوفر فيه الشروط التالية:

---

[1] - United States V.Whitaker, 127F3d595, 602 (7th.cir.1997), available online : www.cybercrime.gov/s&smannual2002.htm.

نقلا عن : د. شيماء عبد الغني، المرجع السابق، ص 410.

[2]- نفس المرجع، ص 409.

[3]– نقلا عن:د.هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص262.

1. أن لا يطرأ على محتويات السجل الإلكتروني أي تغيير، أي أن يكون الدليل المقدم إلى المحكمة هو نفس الدليل الذي تم جمعه، ويمكن للشخص الذي قام بجمع الدليل أن يشهد بذلك أمام المحكمة، كما يجب أن يكون الدليل الإلكتروني منذ لحظة جمعه وحتى لحظة تقديمه إلى المحكمة لم يطرأ عليه أي تغيير، ولا يوجد أي احتمال للعبث به، وأنه تمت مراعاة سلامته حتى يبقى بنفس الحالة التي وجد عليها.

2. أن تكون المعلومات الموجودة في السجل قد صدرت فعلا عن المصدر المزعوم، سواء كان المصدر الشخص أم الآلة.

3. أن تكون المعلومات الموجودة في السجل والمتعلقة بالوقت والتاريخ معلومات دقيقة[1].

الفرع الثاني: حجية الدليل الإلكتروني في القانون الإنجليزي.

قبل القانون الإنجليزي المستندات الإلكترونية في الإثبات في بعض الحالات بنص صريح، وإن كان ذلك مسبوقا بشروط معينة، حيث حدد المشرع الإنجليزي في المادة (69) من قانون الشرطة والإثبات الجنائي الشروط الواجب توافرها في المستند الناتج عن الحاسوب حتى يقبل كدليل في الإثبات، وهذه الشروط هي[2]:

1- عدم وجود أسباب معقولة للإعتقاد بأن البيان يفتقر إلى الدقة بسبب الإستخدام غير المناسب أو الخاطئ للحاسب.

2- أنّ الحاسب كان يعمل في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك فإنه لم يثبت أنّ هناك جزء منه لم يكن يعمل فيه بصورة سليمة أو كان عدم انتظامه ناتجا عن عيب لم يكن مؤثرا في استخراج المستند أو دقة محتوياته.

3- الوفاء بأية شروط متعلقة بالمستند محددة طبقا لقواعد المحاكمة المتعلقة بالطريقة أو بالكيفية التي يجب أن تقدم بها المعلومات الخاصة بالبيان المستخرج عن طريق الحاسب.

وقد علق مجلس اللوردات على المادة (69) المشار إليها بأنه:" يمكن للشهادة الشخصية الصادرة عن شخص على علم بطريقة تشغيل الحاسوب الآلي أن تعطي الثقة بالدليل وليس بالضروري أن يكون هذا

[1]- د.طارق عبد الرؤوف الخن، المرجع السابق، ص 358.

[2]- د.شيماء عبد الغني، المرجع السابق، ص 389.

الشخص خبيرا بالحاسوب"، وبناءا على ذلك قبلت المحاكم الإنجليزية فيما يتعلق بسلامة نظام الحاسوب شهادة أشخاص لديهم علم بطريقة عمل نظام الحاسوب.

ولم يكتف قانون الشرطة والإثبات الجنائي لسنة 1984 بتحديد الشروط الواجب توافرها في مخرجات الحاسب كي تكون أدلة مقبولة أمام القضاء، بل تضمن كذلك توجيهات لكيفية تقدير قيمة أو وزن البيان المستخرج عن طريق الحاسب، فأوصت المادة (11) من الجزء الثاني من الملحق الثالث من القانون المذكور بمراعاة كل الظروف عند تقييم البيانات الصادرة عن الحاسب المقبولة في الإثبات طبقا للمادة (69) من القانون، و بوجه خاص مراعاة ما إذا كانت المعلومات المتعلقة بأمر قد تم تزويد الحاسب بها في وقت معاصر لهذا الأمر أم لا، وكذلك مسألة ما إذا كان أي شخص من المتصلين على أي نحو بإخراج البيان من الحاسب، لديه دافع لإخفاء الوقائع أو تشويهها[1].

وقد تم اقتراح أنه في حالة ما إذا كان الحاسب موضوعا للإستخدام غير المصرح به، فإن أي أدلة مستندية ناتجة عن الحاسب بخصوص أصل و مدة هذا الاستعمال، لن تكون مقبولة، لأنّ سوء استخدام الحاسب في حد ذاته أدى إلى أنّ الجهاز لا يعمل كما ينبغي[2].

ويثار التساؤل حول موقف القضاء بخصوص اعتبار الدليل الناتج عن الكمبيوتر مقبولا في الإثبات أم أنه من قبيل الشهادة السماعية ؟

وللإجابة عن هذا التساؤل تبين من خلال قضية R.V.Wood [3] في إنجلترا والتي عثر في حيازة المتهم على بعض المعادن التي قد سرقت وكانت تركيبة المادة الكيميائية لهذه المعادن مسجلة في كمبيوتر المجني عليه، وقد قدمت ورقة مخرجة من الكمبيوتر كدليل، والسؤال الذي طرح في هذه القضية هل تعتبر هذه الورقة الناتجة عن الكمبيوتر دليلا سماعيا وبالتالي لا يتم الأخذ به؟ أجابت عن ذلك المحكمة معتبرة أنّ الورقة الناتجة عن الكمبيوتر مقبولة وفقا للشريعة العامة وتصلح للإثبات، فهي ليست من قبيل الشهادة السماعية.

وفي نفس الإتجاه أيضا قضت محكمة الإستئناف في إنجلترا بقبول الدليل المستمد من الكمبيوتر في قضية R.V. Pettigren بوصفه شهادة مباشرة وليست سماعية والتي تخلص وقائعها في أنه وجد في حيازة

---

[1]– نقلا عن :د.هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 178.

[2]– د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 54.

[3] - R.V.Wood, 1983, 76cr.app.r.23, available online : www.cybercrime.gov/s&smannual2002.htm.
نقلا عن : د. شيماء عبد الغني، المرجع السابق، ص 391.

المتهم الذي قام بالسطو على البنك أرقام النقود المسروقة والتي كانت مسجلة في كمبيوتر البنك في إنجلترا، وقد قبلت المحكمة في هذه القضية مخرجات الكمبيوتر الورقية باعتبارها دليلا مباشرا وليس من الأدلة السماعية[1].

المطلب الثالث: موقف القوانين ذات الصياغة المختلطة من الدليل الإلكتروني.

إنّ القوانين ذات الصياغة المختلطة هي تلك التي تجمع ما بين النظامين اللاتيني والأنجلوساكسوني، وبالتالي تتبع نظاما وسطا بين الإثبات الحر والإثبات المقيد، ففي هذا النظام المختلط يحدد المشرع أدلة الإثبات، بيد أنه يفسح المجال أمام القضاء في تقدير قيمتها الإقناعية.

فهو عملية مزاوجة أو محاولة توفيقية بين المذهبين، وذلك لتلافي ما وجه إلى الإثبات الحر من خشية تعسف القاضي، وما وجه إلى الإثبات القانوني من أنه يجعل دور القاضي سلبيا في عملية الإثبات، وذلك بأن يترك له حرية تقدير ما يعرض عليه من عناصر الإثبات.

وقد أخذ على هذا النظام أنه وإن قصد به الجمع بين مزايا النظامين السابقين والتخفيف من سلبياتهما، إلاّ أنه في الواقع لا يراعي التوازن بين مصلحة المتهم في البراءة ومصلحة المجتمع في العقاب، إذ أنه يهدف إلى مصلحة المتهم فقط، بمعنى أنه إذا لم يوجد الدليل القانوني فلا يجوز الحكم بالإدانة ولو كان هناك دليل آخر اقتنع به[2].

وسأقتصر على بيان موقف هذا النظام من حجية الدليل الإلكتروني على نموذجين: القانون الشيلي والقانون الياباني، وذلك من خلال الفروع التالية:

الفرع الأول: حجية الدليل الإلكتروني في القانون الشيلي.

طرق الإثبات في قانون الإجراءات الجنائية الشيلي تحصرها المادة (475) منه في طرق ستة، هي: شهادة الشهود، تقارير الخبراء، المعاينة، المستندات الرسمية أو العرفية، الإعتراف، والقرائن، وطبقا للمادة (456) مكرر من نفس القانون، لا يجوز إدانة أي شخص بجريمة ما لم تصل المحكمة المختصة من خلال

[1]– نقلا عن : د.شيماء عبد الغني، المرجع السابق، ص 391.

[2]– د. هلالي عبد اللاه،حجية المخرجات الكمبيوترية، المرجع السابق، ص 59.

الوسائل القانونية للإثبات إلى الإقتناع بأنّ الفعل المستوجب العقاب قد ارتكب وأنّ الشخص المدان كانت له مساهمة في هذا الفعل يعاقب عليها القانون.

ويتبين من ذلك تمسك القانون الإجرائي الشيلي بنظام التحديد الحصري لوسائل الإثبات في المواد الجنائية على نحو تكون فيه الوسائل المحددة والمنظمة قانونا هي وحدها التي تعتبر مشروعة وجائز استخلاص الحقيقة عن طريقها، وفي ظل هذا التحديد يمكن أن يكون الدليل الناشئ عن الحاسب مقبولا في مجال الإثبات الجنائي استنادا إلى تقرير يقدمه خبير بشأن البيانات المعنية المعالجة آليا، فللقاضي وفقا للمادة (221) من قانون الإجراءات أن يطلب تقريرا من خبير عند حدوث أي من الحالات التي يحددها القانون، وكذلك عندما تكون هناك معرفة معينة أو خاصة في مجالات العلم أو الفن أو التجارة لازمة أو ضرورية لتقييم واقعة أو ظرف مؤثر في الدعوى، وفي حالة البيانات والعناصر الأخرى التي يقدمها أو يوفرها جهاز الحاسب، وتبعا لطبيعة الدعوى يكون الرأي الفني المتخصص مطلوبا بوجه عام لمساعدة القاضي.

كما يمكن من جهة أخرى النظر إلى المعاينة التي تجريها المحكمة بمساعدة الخبراء على أنها وسيلة إثبات لموضوعات أو عناصر في نظام المعالجة الآلية للمعطيات يمكن أن تقوم على أساسها المسؤولية الجنائية.

وفي بعض القوانين الخاصة تتحدد وسائل الإثبات على نحو يجعلها أعم وأشمل من تحديدها الحصري الوارد بقانون الإجراءات، ومن قبيل ذلك نصت بعض المواد التي تعاقب على الإتجار غير المشروع في المواد والعقاقير المخدرة على أنه يجوز للمحاكم أن تقبل كوسائل للإثبات أفلام السينما والصور الفوتوغرافية ونظم إعادة عرض الصورة والصوت وبوجه عام أية وسيلة مناسبة وذات صلة بالموضوع ومنتجة أو مؤثرة.

وفي هذا الإطار يمكن أن يكون الدليل الناشئ عن الحاسب مقبولا أمام القضاء الجزائي باعتباره دليلا مستنديا، أي إثباتا بمحرر ومثله أيضا النظم الأخرى الحديثة لجمع وتسجيل وإعادة عرض الوقائع، ويمكن أن يجد ذلك أساسه أيضا في أنّ الصور الفوتوغرافية، والصور الضوئية وصور الأشعة والتسجيلات الهاتفية وتسجيلات الصوت تعتبر جميعا مستندا بالمفهوم الواسع للمصطلح، خاصة وقد تخطى التقدم التكنولوجي المفهوم التقليدي للمستند كورقة مكتوبة وسمح بإتاحة وسائل أخرى لتسجيل أو عرض فكرة أو واقعة على نحو أكثر سلامة ودقته[1].

ومع تمسك المشرع الشيلي بمبدأ التحديد الحصري لوسائل الإثبات، وإدراكه لصعوبة إثبات الجرائم الواقعة في بيئة المعالجة الآلية للمعطيات، فقد سعى في مشروع قانون الإجراءات الجزائية مقترح حاليا إلى توسيع دائرة طرق الإثبات المنصوص عليها في القانون في المادة (113) منه بعد إقراره طرق الإثبات القائمة،

[1]– نقلا عن: د. هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 162-164.

على أنّ أفلام السينما والوسائل الأخرى لإعادة عرض الصورة والصوت والنسخ المختزلة وبوجه عام أية وسائل أخرى ملائمة ومؤثرة ومفضية إلى إقامة الدليل المبني على المصداقية يمكن أن تكون مقبولة في الإثبات[1].

الفرع الثاني: حجية الدليل الإلكتروني في القانون الياباني.

لقد حصر المشرع الياباني طرق الإثبات المقبولة بما يأتي: أقوال المتهم، أقوال الشهود، القرائن والخبرة، أمّا بالنسبة لأدلة الحاسوب والإنترنت، فيقرر المشرع الياباني أن السجلات الإلكترومغناطيسية تكون غير مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة إلاّ إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات، وفي مثل هذه الحالة يتم قبول هذه الأدلة الناتجة عن الحاسوب سواء كانت هي الأصل أم كانت نسخة من هذا الأصل.

لكن ما هو السند القانوني لقبول هذه المخرجات الكمبيوترية ؟ للإجابة عن هذا السؤال ينبغي الإشارة إلى أنه إذا كان قانون الإجراءات الجزائية الياباني يستبعد الشهادة السماعية ، إلاّ أنه يرد على هذه القاعدة بعض الإستثناءات المنصوص عليها في المواد (321-328) من نفس القانون، ويدخل ضمن هذه الإستثناءات الأدلة المتولدة عن الحاسب الآلي، إذ يمكن طباعة هذه المخرجات الكمبيوترية وقبولها أثناء فترة المحاكمة من خلال شهادات الخبراء[2].

[1]– د. هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 164.

[2] – د. هلالي عبد اللاه، حجية المخرجات الكمبيوترية، المرجع السابق، ص 62.

المطلب الرابع:النتائج المترتبة على تطبيق مبدأ الإقتناع الشخصي بالدليل الإلكتروني.

إن مبدأ الإقتناع الشخصي ينطبق أمام كل الجهات القضائية الجنائية وفي كل مراحل الدعوى الجنائية، فهو يتعلق بوجود الأدلة الكافية من عدم وجودها أثناء التحقيق الإبتدائي، كما ينطبق على تقييم وسائل الإثبات من طرف قضاء الحكم .

وإذا كانت النصوص القانونية قد كرست مبدأ الإقتناع الشخصي ليطبق أمام جهات قضاء الحكم، فإنه يجري العمل به حتى أمام قضاء التحقيق، وهذا ما يستخلص ضمنيا من أحكام المواد (2/162)[1]، (1/163)[2] من قانون الإجراءات الجزائية الجزائري، كما يستخلص من نصوص المواد (284)[3]، (399)[4] أن قاعدة الإقتناع الشخصي هي قاعدة شاملة تسري أمام كل جهات قضاء الحكم.

فإعمال قاعدة الإقتناع الشخصي يجعل القاضي الجزائي يتمتع بكل حرية في تقدير وسائل الإثبات المطروحة أمامه، كما يستطيع أن يبني اقتناعه على أية وسيلة، فلا وجود لتسلسل أو تدرج بين وسائل الإثبات في المواد الجنائية [5].

غير أن السؤال الذي يطرح في هذا المقام هو القيمة العلمية للدليل الإلكتروني ومدى تأثيرها على اقتناع القاضي الجزائي؟

ينبغي الإشارة إلى أنّ الآراء الفقهية قد تباينت إزاء الأخذ بالدليل العلمي في الإثبات الجنائي، بين مؤيد للأخذ به ورافض له وبين منكر لوجوده أصلا ، ومن أجل توضيح هذه المسألة سيتم استعراض الإتجاهات الفقهية وكذا محاولة الرد عليها.

---

[1]- تنص المادة 2/162 من قانون الإجراءات الجزائية الجزائري على ما يلي:" ...يمحص قاضي التحقيق الأدلة وما إذا كان يوجد ضد المتهم دلائل مكونة لجريمة من جرائم قانون العقوبات".

[2]- تنص المادة 1/163 من قانون الإجراءات الجزائية الجزائري على ما يلي:" إذا رأى قاضي التحقيق أن الوقائع لا تكون جناية أو جنحة أو مخالفة أو أنه لا توجد دلائل كافية ضد المتهم أو كان مقترف الجريمة ما يزال مجهولا ، أصدر أمرا بأن لا وجه لمتابعة المتهم ...".

[3]- تنص المادة 284 من قانون الإجراءات الجزائية الجزائري على ما يلي:"...تقسمون وتتعهدون أمام الله وأمام الناس بأن تمحصوا بالإهتمام البالغ غاية الدقة ما يقع من دلائل اتهام على عاتق فلان ...".

[4]- تنص المادة 399 من قانون الإجراءات الجزائية الجزائري على ما يلي:" تطبق أيضا القواعد المقررة في المواد من 239 إلى 247 المتعلقة بالإدعاء المدني وفي المواد 212 إلى 237 المتعلقة بإقامة الدليل مع التحفظات الواردة بالمادة 400 والمواد من 238 إلى 352 المتعلقة بطلبات النيابة العامة ومذكرات الخصوم الختامية والمادة 355 المتعلقة بالحكم ."

[5]- د.محمد مروان، المرجع السابق ، ج2، ص 469.

أولا: الإتجاه الرافض للدليل العلمي.

يرفض هذا الجانب من الفقه[1] فكرة الدليل العلمي بدعوى أنها تجعل دور الخبير في الدعوى له مكان الصدارة، وأن هذا الدليل يجعل الخبير مسيطرا على العملية الإثباتية، حيث ستصبح مهمة القاضي آلية، وليس له إلا الرضوخ للنتيجة التي توصل إليها الخبير.

ثانيا : الإتجاه المؤيد للدليل العلمي.

يؤيد هذا الفريق من الفقه[2] قبول الدليل العلمي والتسليم بمشروعيته مهما كانت درجة خطورته، على أساس أنّ قبول الدليل العلمي يرجع في الدرجة الأولى إلى حق المجتمع في الدفاع عن نفسه بذات الوسائل التي يستخدمها المجرم وتفرض مشروعية الدليل العلمي في عدم مخالفته للحقوق الأساسية للإنسان مع كفالة حق الشخص في اللجوء إلى القضاء إذا ما ترتب على ذلك إعتداء على حقوقه الأساسية.

ثالثا: الإتجاه المنكر لوجود الدليل العلمي من الأساس.

يذهب هذا الرأي في الفقه[3] إلى أنّ مرحلة الدليل العلمي لا وجود لها إلاّ في مخيلة أصحابها، ومن قبيل المغالطة القول بأنه أصبح هناك نطاق نظام جديد إذا ما وجدت أدلة ذات دقة أكثر ، فالطرق العلمية لا يمكن أن تقدم وسائل جديدة للإثبات بل يمكن أن تقدم وسائل بحث أفضل عن الحقيقة بطرق تفوق قدرتها الوسائل التقليدية.

وفي إطار تقييم الإعتراضات الفقهية بشأن الأدلة العلمية، أنه حال الحديث عن الأدلة العلمية ينبغي التمييز بين فرضين: القيمة العلمية القاطعة للدليل والظروف والملابسات التي وجد فيها الدليل، فتقدير القاضي لا يتناول قيمة الدليل لأنها تقوم على أسس علمية دقيقة، ولا حرية للقاضي في مناقشة الحقائق العلمية الثابتة، أما الظروف والملابسات التي وجد فيها هذا الدليل فهي تدخل في نطاق تقديره الذاتي وصميم وظيفته القضائية بحيث يكون في مقدوره أن يطرح هذا الدليل رغم قطعيته من الناحية العلمية، وذلك عندما يجد أن وجوده لا يتسق منطقيا مع ظروف الواقعة وملابساتها[4].

---

[1]– د. محمود نجيب حسني، المرجع السابق، ص 422. و د. أحمد فتحي سرور، المرجع السابق، ص 408. نقلا عن: د. عبد الناصر محمد محمود فرغلي، المرجع السابق، ص 120.

[2]- ومن بين الفقهاء المؤيدين Bouzat و Vidal. نقلا عن: د. عبد الناصر محمد محمود فرغلي، المرجع السابق، ص 125.

[3]– د. مفيدة سعد سويدان، نظرية الإقتناع الذاتي للقاضي الجنائي(دراسة مقارنة)، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، سنة 1985، ص 167. نقلا عن : نفس المرجع، ص 125.

[4]– د. السيد محمد سعيد عتيق، النظرية العامة للدليل العلمي في الإثبات الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، سنة 1993، ص106. نقلا عن: نفس المرجع، ص 127.

وبالتالي يمكن القول أن الثورة العلمية قد أثرت تأثيرا كبيرا على الإثبات الجنائي وعلى طرق الإثبات، بحيث يمكن القول أن طرق الإثبات التقليدية أصبحت عقيمة بالنسبة لإثبات الجرائم الإلكترونية، وإذا كانت الغلبة لإثبات هذه الجرائم ستكون للإثبات بالقرائن والخبرة، فإن ذلك سيزيد من أهمية الدليل العلمي في الإثبات الجنائي[1].

ولاشك أن الخبرة التقنية تعتبر عنصرا رئيسيا للتحقيق في الجرائم الإلكترونية، بحيث يتطلب الأمر ليس مجرد التعرف على الجزئيات التي تسمح بالإدانة، وبالتالي تحديد كيفية ارتكاب الجريمة من زاوية تقنية، وإنما يكون قصد الخبير التقني أيضا التعرف على ما يمكن أن يكون فكرة تقنية جديدة تفيد القضاء للتوصل إلى الحقيقة كاملة، سيما إزاء عدم وجود قواعد تشكل مقياس عام يعتمد عليه في تقنية الإنترنت يمكن إدراكها بالعلم العام الذي يملكه كل شخص، فلابد من الإستعانة بالخبير الذي يستخدم الأساليب التقنية التي تساعد على ضبط الدليل والتحفظ عليه داخل الحاسب الآلي[2].

- **فيما يتعلق بمسألة تقدير الخبرة :**

إنّ التقرير الذي ينتهي إليه الخبير ليس ملزما من الناحية القانونية بالنسبة للقاضي الذي يمكنه الإعتماد عليه كما يمكنه استبعاده، وليس عليه سوى تسبيب ما انتهى إليه، وأكثر من ذلك إذا تعددت الخبرات في القضية الواحدة فإن الترجيح بينها يعود للسلطة التقديرية للقاضي[3].

ولكن من الناحية الواقعية فإنّ للنتيجة التي يتوصل إليها الخبير حجية كبيرة يصعب على القاضي كما يصعب على الأطراف استبعادها إلا بحجج قوية وهو أمر نادر الوقوع، وفي غالب الأحيان يكتفي الأطراف بطلب خبرة مضادة أو خبرة تكميلية لعل أن يتمكن خبير آخر من دحض ما توصل إليه الخبير الأول.

وهناك رأي آخر للأستاذ إلياس أبو عيد الذي يرى أن القاضي يكون ملزما بما توصل إليه الخبير على أساس أنّه يتناول مسائل فنية ليس بإمكان القاضي أن يستبعدها[4]، غير أنّ رأيه فيه جانب من الصواب لأنّ المسائل الفنية لا يجوز تفنيدها إلاّ بأسانيد فنية، فهي مسائل يتعذر على القاضي فهمها دون الإستعانة

---

[1]- د. علي محمود حمودة، المرجع السابق، ص 69.

[2]- د. محمد فتحي، المرجع السابق، ص 438.

[3]- وهو ما ورد في قرار غرفة الجنح والمخالفات بالمحكمة العليا الصادر بتاريخ 08-10-2008 فصلا في الطعن رقم 412384 (غير منشور) الذي فيه:" حيث أنه بالرجوع إلى الحكم الإبتدائي وإلى القرار المطعون فيه الذي أيده يتبين أنّ قضاة الموضوع قد صرحوا ببراءة المتهم على أساس أن السيارة قد عرضت على ثلاثة خبراء وأنّ اثنين منهما قد أكدا أنها سليمة ورقمها التسلسلي أصلي وغير مزور. أنظر في ذلك: أ.نجيمي جمال ، المرجع السابق، ص 247.

[4]- نفس المرجع، ص 248.

برأي الخبراء، فالدور الجوهري للخبير في تحديد الأدلة الإلكترونية لا يترك مجالا واسعا للقاضي لتحديد مسار الدعوى[1].

ويرى الدكتور طارق عبد الرؤوف الخن أنّ اعتماد المحكمة على تقرير الخبير المعلوماتي لا يعد مساسا بمبدأ قناعة القاضي الشخصية ولا يجعل من الخبير القاضي الحقيقي للدعوى، فدور الخبير التقني لا يمثل سوى أحد الأدوار التي تساعد القاضي على فهم القضية، ومحكمة الموضوع هي صاحبة الفصل في تقرير الخبرة الذي قد تقتنع به أو لا تقتنع[2].

وتستدعي عملية حفظ الأدلة في العالم الرقمي لزوم قيام الخبير بعرض الأدلة في المحكمة أو على جهات التحقيق ، و مثل هذا الأمر يجعل عمل الخبير يستمر لمرحلة المحاكمة، وتفاديا للمشاكل التي يمكن أن تنجم عن حفظ الأدلة في العالم الرقمي، فإن العديد من المحاكم لجأت إلى ميكنة إدارتها رقميا، بحيث يتم تسليم الأدلة إلى إدارة متخصصة تتولى بدورها حفظ الأدلة وذلك لعرضها على القضاء كلما تطلب الأمر ذلك[3].

- **فيما يتعلق بمسألة تقدير الإعتراف :**

إنّ القاضي يقدر بكل حرية مسألة الإعتراف طبقا لنص المادة (213)[4] من قانون الإجراءات الجزائية الجزائري، ذلك أنه قد يحدث أنّ الإعتراف بارتكاب جريمة لا يطابق الحقيقة، كأن ينتزع منه بطرق غير مشروعة، فباستطاعة القاضي الجزائي أن يحتفظ بالإعتراف كأساس لتثبيت الإتهام، كما أنه باستطاعته أن يستبعده ويصدر حكما ببراءة المتهم إذا ما تبين له أن هذا الإعتراف مشتبه فيه أو متناقض مع وسائل إثبات أخرى أو مشكوك في حريته[5].

---

[1] – يستشهد أصحاب هذا الرأي بقضية شهيرة تتلخص وقائعها بأنّه في عام 2000 قام اتحاد الطلبة اليهود في فرنسا رفع دعوى ضد شركة Yahoo الفرنسية والأمريكية، بسبب وجود مزاد علني يتعلق بالنازية على إحدى الصفحات المجانية التي تبث من خلال Yahoo على الإنترنت، وقد تضمن المزاد عرض مجموعة من صور الزعيم النازي (أدولف هيتلر) ومجموعة شعارات وصور وأعلام تتعلق بالحزب النازي.

وقد رفعت دعوى أمام محكمة باريس الإبتدائية بناءا على أنّ شركة (Yahoo) قامت بالتقليل من كارثة "الهولوكوست" عندما سمحت بإجراء مثل هذا المزاد على الإنترنت، وهو الأمر الذي يشكل جريمة وفقا للقانون الفرنسي الذي يكافح النازية.

وقد أصدر القاضي حكمه على شركة Yahoo الفرنسية بإلزامها بمنع المستخدمين من الدخول إلى هذه المزادات، واعتمد القاضي في حكمه على تقرير الخبرة التقنية الذي أكد قدرة شركة Yahoo على منع مستخدمي الإنترنت من الدخول إلى هذه المزادات رغم إصرار شركة Yahoo على عدم قدرتها على ذلك.

ويرى الفقه في هذه القضية أن المحكمة اعتمدت على تقرير الخبرة التقنية دون أن تقوم بمناقشته بشكل جيد فقرار المحكمة صدر بعد أيام قليلة من إيداع لجنة الخبراء لتقريرها. نقلا عن: د.محمد طارق عبد الرؤوف الخن، المرجع السابق، ص338.

[2] – د. طارق عبد الرؤوف الخن، المرجع السابق، ص 338.

[3] – د. محمد فتحي، المرجع السابق، ص 434.

[4] - تنص المادة 213 من قانون الإجراءات الجزائية الجزائري على ما يلي:" الإعتراف شأنه كشأن جميع عناصر الإثبات يترك لحرية تقدير القاضي ."

[5] – د.محمد مروان، المرجع السابق، ج 2، ص 473.

فالإعتراف ليس سيد الأدلة كما هو الحال في القانون المدني، بل إنه مجرد عنصر من عناصر الإثبات يمكن استبعاده أو تجزئته والأخذ ببعضه دون البعض الآخر، ذلك لأن المعترف قد يكون متحايلا وله أغراض محددة من خلال اعترافه، غير أن تفسير اعتراف المتهم مسألة واقع يتولاها القاضي ما دام في إطار المعاني المتعارف عليها في اللغة المستعملة من طرف المقر الذي لا يمكنه أن يتذرع بأنه كان يقصد شيئا آخر ما دام كلامه واضح المعنى والدلالة، نظرا للسلطة التقديرية التي منحها المشرع لقاضي الحكم في تكوين اقتناعه من مجمل الأدلة والقرائن المعروضة عليه.

إلا أنه في الواقع قد تتوصل الضبطية القضائية إلى اعتراف المتهم، وبناءا على ذلك تتوقف عن مواصلة البحث، إلا أن هذا المسلك ينطوي على خطأ جسيم لأن هذه الأقوال لا تشكل اعترافا قضائيا، بل هي مجرد تصريحات تصلح للإستدلال فقط، لأن المتهم بمجرد إنكاره لها أمام الجهات القضائية فلا يؤخذ هذا الإعتراف بعين الإعتبار، وبالتالي تفوت الضبطية القضائية فرصة جمع أدلة أخرى[1]، خصوصا في الجرائم الإلكترونية التي تعتبر الأدلة فيها سريعة الإتلاف.

- **فيما يتعلق بتقدير الشهادة:**

إنّ الإثبات بالشهادة يخضع هو الآخر لحرية تقدير القاضي، وهذا ما تؤكده المحكمة العليا: "... أنّ تقدير الدليل بما فيه شهادة الشهود، المناقش أمام المجلس في معرض المرافعات حضوريا، يدخل في إطار الإقتناع الخاص لقضاة الموضوع"[2].

ومن أجل ذلك ترك المشرع للقاضي سلطة واسعة في تقدير شهادة الشهود، بحيث أنه يجوز ترجيح شهادة البعض على البعض الآخر ، كما يجوز استبعاد الشهادة مباشرة إذا أدرك القاضي أنها مخالفة لما هو ثابت بطرق أقوى كالكتابة أو الدليل العلمي، كما يجوز له تقدير كفايتها في الإثبات من عدمه.

وعلى القاضي بعد سماع شهادة الشهود بالجلسة وفقا للضوابط القانونية التي تم التطرق إليها سابقا، أن يراجع ويمحص تصريحات الشهود سواء لتأسيس الحكم عليها أو لبيان أسباب استبعادها باعتبارها أدلة إثبات مقدمة في الدعوى، ويذكر ذلك في صلب حكمه حتى يتحاشى عيب قصور التسبيب .

كما أن وسائل الإثبات متروكة للسلطة التقديرية لقاضي الحكم، لا فرق في ذلك بين الأدلة التي تقدمها الضبطية القضائية، أو التي يقدمها قاضي التحقيق، أو التي يقدمها الأطراف في الجلسة، بشرط واحد

---

[1]- أ. نجيمي جمال، المرجع السابق، ص 65.

[2] – المحكمة العليا غ ج : 13 ماي 1986، رقم 304، غير منشور، نقلا عن : د. محمد مروان، المرجع السابق، ج2 ، ص 476.

وهو أن تقدم في معرض المرافعات وتتم مناقشتها وجاهيا أمامه ثم ينتقي منها ما يطمئن إليه، ودليله في ذلك المنطق السليم والضمير الحي والشعور بالعدالة، وعلى هذا الأساس يمكن للقاضي بعد إطاحته بكل جوانب القضية أن يأخذ بأقوال الشاهد كلها أو بعضها أو يستبعدها تماما، ولا يطلب منه القانون إلا أن يسبب ما ذهب إليه[1].

المبحث الثالث: الإستثناءات والقيود الواردة على حرية القاضي الجزائي وضوابط اقتناعه بالدليل الإلكتروني.

سبقت الإشارة إلى أنّه للقاضي الجزائي الحرية في تكوين اقتناعه الذاتي دون أن يتقيد بدليل معين، إلاّ إذا نص القانون على غير ذلك، فالقاعدة في الإثبات الجنائي أنه يجوز إثبات الجرائم بكافة الطرق، إلاّ أنّ مبدأ الإقتناع القضائي لا يعني تحكم القاضي، فلا يجوز لهذا الأخير أن يحكم وفقا لهواه أو يحتكم في قضائه لمحض عاطفته، وإنما هو ملتزم بأن يتحرى المنطق في تفكيره الذي قاده إلى اقتناعه، فالقاضي وإن كان غير مكلف ببيان أسباب اقتناعه الشخصي إلاّ أنه مكلف ببيان أسباب الحكم الذي انتهى إليه، وهو في مقام هذه الأسباب لابد أن يذكر الأدلة التي اعتمد عليها وكانت مصدرا لاقتناعه ولكنه غير مكلف بتحديد علة اقتناعه بهذه الأدلة بالذات، فهو مكلف بإثبات ما اقتنع ولكنه غير مطالب لماذا اقتنع[2].

كما يتبين من العرض السابق للنظم التي أخذت بحجية الدليل الإلكتروني، فإنه بالرغم من اختلافها في هذا الشأن، إلاّ أنّ هناك ضوابط معينة تحكم الأدلة الإلكترونية يلتزم بها القاضي لحماية حقوق الأطراف وغيرها من الحقوق، وهذه الضوابط تدور حول أصل البراءة وما يتفرع عنه من نتائج وآثار وما يستتبع ذلك من وجوب توافر شروط معينة في الدليل الإلكتروني حتى يمكن الحكم بالإدانة، ذلك أنه لا محل لافتراض عكس قرينة البراءة إلا عندما يصل القاضي إلى الجزم واليقين[3].

فإذا لم يصل القاضي إلى الجزم بنسبة الفعل أو الجريمة الإلكترونية إلى المتهم المعلوماتي يتعين عليه أن يقضي بالبراءة، كما يجب أن تكون عقيدة القاضي واقتناعه بالإدانة قد استمد من أدلة إلكترونية طرحت

---

[1]- أ. نجيمي جمال، المرجع السابق، ص 360.

[2]– د.منى فتحي أحمد عبد الكريم، المرجع السابق، ص 124.

[3] - ذلك أنّ التصرفات المشبوهة التي تتضمن ردود فعل فورية وانفعالية أثناء التحريات تبقى قرينة غير مؤكدة إذا لم تكن مدعمة بعناصر أكثر واقعية، فإذا كان المجرم المعلوماتي قد سبق له أن ارتكب جرائم مماثلة، فهذا لا يعني أنه هو من قام بهذه الأفعال. أنظر في ذلك :

Mari-Cécile Nagouas-Guérin, le doute en matière pénale, Thèse Doctorat, Université Montesquieu-Bordeaux IV, France, 2002, P 230.

نقلا عن : أ. نجيمي جمال، المرجع السابق، ص 361.

بالجلسة، لأنّ القاعدة هي ألا يحكم القاضي إلاّ بناءا على التحقيقات التي تحصل بالطرق والشروط القانونية لا بناءا على معلومات شخصية أو على ما قد يكون قد رآه بنفسه أو حققه في غير مجلس القضاء، كما ينبغي ألاّ يؤسس القاضي الجزائي حكمه على دليل ناتج عن حاسب آلي لحقه سبب يبطله ويعدم أثره[1].

وإذا كان مبدأ حرية الإثبات يجيز للقاضي حرية الإستعانة بكافة وسائل الإثبات إلاّ أنّ هذا الإطلاق ليس بلا قيد وبلا حدود، لأنّ ذلك سيؤدي إلى التساهل في ارتكاب الجرائم تحت غطاء البحث عن الأدلة والتحقيق فيها[2].

والإستثناء كذلك عن قاعدة حرية الإثبات هو ما يتعلق ببعض الجرائم التي يحدد لها المشرع أدلة الإثبات التي يمكن الإستناد إليها، وهو ما يعرف بنظرية الإثبات المقيد، والقيد كذلك على قاعدة حرية الإثبات هو أن يكون قد تم الحصول على الدليل الإلكتروني بطرق مشروعة، وسيأتي الحديث على هذا تفصيلا في المطالب التالية:

المطلب الأول: الإستثناءات و القيود الواردة على حرية القاضي الجزائي في قبول الدليل الإلكتروني.

تنحصر هذه الإستثناءات في التقيد بأدلة معينة في جريمة الزنا، أما الثاني فيتعلق بطرق الإثبات الخاصة بالمواد غير الجنائية، وبناءا على ذلك سيتم معرفة موقف الدليل الإلكتروني من هذه الإستثناءات، هذا بالإضافة لقيد المشروعية وذلك من خلال الفروع التالية:

الفرع الأول: الإستثناءات المستمدة من نصوص قانونية خاصة.

سيتم التطرق لقيد تحديد الأدلة بالنسبة لجريمة الزنا، وإستثناء آخر على حرية الإثبات أمام القضاء الجزائي هو أنه إذا كانت هناك مسائل تتعلق بقوانين أخرى، كالقانون المدني أو القانون التجاري مثلا تخللت إثبات قيام الجرم، فيتعين إثباتها وفقا لأحكام ذلك القانون مثل: إثبات عقود الأمانة في جريمة خيانة الأمانة أو إثبات تسديد مبالغ معينة وفقا للتحديد الوارد في القانون المدني[3]، وذلك على النحو التالي:

---

[1]- د.طارق فوزي الفقي، المرجع السابق، ص 208.

[2] - أ. رشيدة بوكر، المرجع السابق، ص488.

[3]- أ. نجيمي جمال، المرجع السابق، ص 46.

البند الأول: تحديد الأدلة في جريمة الزنا.

نص المشرع الجزائري في المادة (341) من قانون العقوبات على أنّ" الدليل الذي يقبل عند ارتكاب الجريمة المعاقب عليها بالمادة (339) يقوم إمّا على محضر قضائي يحرره احد رجال الضبط القضائي عن حالة تلبس وإمّا بإقرار وارد في رسائل ومستندات صادرة عن المتهم وإما بإقرار قضائي".

فلا يجوز الإعتماد على شهادة الشهود أو غيرها من الأدلة والقرائن خارج حالة التلبس والإعتراف القضائي وغير القضائي إن كان في رسائل ومستندات، وفي هذا الإطار قضت غرفة الجنح والمخالفات بالمحكمة العليا في قرارها المنشور الصادر بتاريخ 24 جوان 2009 فصلا في الطعن رقم 443709 بما يلي:

"فعلا حيث أنه بالرجوع للقرار المطعون فيه يتضح أن قضاة الموضوع لإدانة الطاعنة بتهمة المشاركة في الزنا طبقا للمادتين (339) و(42) من قانون العقوبات، اعتبروا شريط الفيديو كأنه وسيلة إثبات كاملة، بينما شريط الفيديو ليس من الدلائل المنصوص عليها على سبيل الحصر في المادة (341) من قانون العقوبات التي تشترط أن يكون الدليل الذي يقبل عن ارتكاب هذه الجريمة المعاقب بالمادة (339) من نفس القانون إمّا محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة تلبس، وإمّا بإقرار وارد في رسائل أو مستندات صادرة عن المتهمة وإما بإقرار قضائي.

حيث أن الوسائل التي تأسس عليها الحكم والقرار لا تدخل ضمن الدلائل التي عددتها المادة (341) من قانون العقوبات، خاصة وأنّ المتهمين ينكران التهمة المنسوبة إليهما، وهذا يعد مخالفة للقانون، وبالتالي الوجه المثار مؤسس ويؤدي إلى نقض القرار المطعون فيه، وذلك دون التطرق للأوجه الأخرى المقدمة من قبل الطاعنة"[1].

أمّا المشرع المصري فقد نص في المادة (276) من قانون العقوبات على أن الأدلة التي تقبل وتكون حجة على المتهم بالزنا هي القبض عليه حين تلبسه بالفعل أو اعترافه أو وجود مكاتيب أو أوراق أخرى صادرة منه أو وجوده في منزل مسلم في المحل المخصص للحريم[2]، والواضح من النص أنّ المشرع حدد الأدلة

[1]– مجلة المحكمة العليا، سنة 2009، العدد 02، ص 382.نقلا عن : أ. نجيمي جمال، المرجع السابق، ص 45.

[2]– هذا النص منقول عن المادة 338 من قانون العقوبات الفرنسي، وقد ألغيت هذه المادة سنة 1975 حيث كانت تنص على أنّ الأدلة التي تقبل وتكون حجة على شريك الزوجة الزانية هي التلبس بالجريمة أو وجود خطابات ومكاتيب صادرة عن المتهم، وقد أضاف إليها المشرع المصري إعتراف المتهم ووجوده في المحل المخصص للحريم، وقد اختلف الفقه المصري حول تقدير السياسة التشريعية لنص المادة 276 في حين ذهب رأي إلى انتقاد النص تأسيسا على أنه يقرر نظام شاذ يصعب تبريره إلاّ لأسباب تاريخية صرف، ترجع إلى التقاليد الرومانية والقبلية بوجه عام.أنظر في ذلك:د. رؤوف عبيد، جرائم الإعتداء على الأشخاص و الأموال، بدون ناشر، ط 7، سنة 1987، ص 472.نقلا عن : د. عائشة بن قارة ، المرجع السابق، ص 228.

التي تقبل في شأن إثبات الزنا وحصرها في التلبس بالزنا والاعتراف ووجود أوراق صادرة من المتهم بالزنا، ووجوده في منزل مسلم في المحل المخصص للحريم، ومن المفهوم أنه يكفي توافر أحد هذه الأدلة لإمكان الحكم على المتهم بالزنا.

و يذهب الرأي الغالب في الفقه والقضاء إلى أنّ الأدلة سالفة البيان لازمة فقط لإثبات زنا شريك الزوجة الزانية، أمّا بالنسبة للزوجة أو الزوج أو شريكته فإثبات الزنا على أي منهم يخضع لمبدأ حرية الإثبات الجنائي، ولهذا لا يجوز للقاضي الجزائي أن يقبل لإثبات الزنا في حق شريك الزوجة أدلة أخرى غير ما قرره نص المادة (276) من قانون العقوبات ولو كانت تسجيلات صوتية، وهو أمر محل نظر لأن التسجيل الصوتي يمكن أن يثبت وقوع الزنا أكثر مما يثبته مجرد خطاب صادر من الشريك، لذا فإنه كان من الأجدر بالمشرع أن ينص على التسجيل الصوتي ضمن أدلة الزنا.

ومع ذلك يرى الدكتور"ياسر الأمير فاروق"أنه يجوز قبول التسجيل الصوتي ضمن أدلة الزنا في حالة إذا ما تضمن التسجيل إقرار من شريك الزوجة الزانية على نفسه ارتكاب الزنا، إذ يعد التسجيل الصوتي في هذه الحالة بمثابة إعتراف.

وقد قضت محكمة النقض المصرية بأنّه:"لما كان البين من الإطلاع على محاضر تفريغ التسجيلات الصوتية التي جرت بين الزوجة المطعون ضدها الأولى وبين المطعون ضده الثاني أنها خلت مما يفيد وقوع الوطء فعلا بينهما وإن تضمنت عبارات غير لائقة، ومن تم يكون استخلاص محكمة الموضوع في استبعاد ما أسفرت عنه تلك التسجيلات وعدم اعتبارها دليلا من بين الأدلة التي أوردتها المادة (276) من قانون العقوبات بالنسبة للشريك في جريمة الزنا هو استخلاص سائغ، ومن تم يكون طعن المدعي بالحق المدني قبل المطعون ضده الثاني على غير أساس"[1].

فمن خلال استعراض موقف المشرعين الجزائري والمصري، يستخلص أنه لا يجوز للقاضي الجزائي أن يقبل لإثبات جريمة الزنا أدلة أخرى غير ما قررته النصوص المذكورة،و لو كان دليلا إلكترونيا سواء كان عبارة عن صور فيديو أو رسالة مرسلة من الشريك إلى الزوجة أو إلى غيرها عن طرق الهاتف المحمول (SMS) أو عن طريق الإنترنت (Email) سواء تضمنت هذه الرسالة اعترافا صريحا أو ضمنيا من الشريك بوقوع الزنا، أو فيها نوع من الكلام الذي يوحي بممارسة علاقة غير شرعية مع الزوجة، وإن كان من الأجدر بالمشرعين

[1]- نقض رقم 24-10-2001 الطعن رقم 21392 لسنة 63 ق .نقلا عن د: ياسر الأمير فاروق، المرجع السابق، ص 644.

الجزائري والمصري أن ينصا على الدليل الإلكتروني ضمن أدلة إثبات الزنا، وذلك سدا للفراغ التشريعي الذي أصبح جليا في أغلب التشريعات خصوصا العربية منها[1].

البند الثاني: إثبات المسائل غير الجنائية.

تنص المادة (225) من قانون الإجراءات الجنائية المصري على أن تتبع المحاكم الجنائية في المسائل غير الجنائية التي تفصل فيها تبعا للدعوى الجنائية طرق الإثبات المقررة في القانون الخاص بتلك المسائل، ومفاد هذا النص أنّ إثبات المسائل غير الجنائية التي تطرح على المحكمة ويكون الفصل فيها مقدمة ضرورية للفصل في الدعوى الجنائية وتنتهي بالمسائل الأولية تخضع للقانون الخاص بتلك المسائل، ومن تم فإذا كانت الجريمة خيانة أمانة وصار نزاع بشأن العقد وكانت قيمته تزيد عن خمسمائة ألف(500.000) جنيه، فلا يجوز إثبات هذا العقد بالتسجيلات الصوتية إذ يلزم إثباته بالكتابة، وذلك ما لم يجز القانون المدني إثباته بالبنية لتوافر مبدأ ثبوت بالكتابة أو لوجود مانع أدبي أو مادي يحول دون الحصول على الدليل الكتابي أو لكون العقد ذو صبغة تجارية المواد (60)،(63) من قانون الإثبات.

ولهذا قضي بأن التسجيل الصوتي الذي قامت به الطاعنة يعد ولا ريب إقرار غير قضائي، ولما كانت الطاعنة تسلم في أسباب طعنها أنّ المطعون ضده قد أنكر أن هذا التسجيل خاص به، فإنه يجب على الطاعنة أن تثبت صدوره منه طبقا للقواعد العامة في الإثبات في القانون المدني، وإذا كانت هذه القواعد توجب الحصول على دليل كتابي في هذا الصدد، فإنّ قضاء الحكم المطعون فيه بعدم جواز الإثبات بالبينة ينسحب على هذا التسجيل، ويتضمن الرد عليه مادام لا يعد عنصرا مستقلا عن العناصر التي أبدى الحكم رأيه فيها[2].

غير أنّ تقييد القاضي الجزائي بوسائل الإثبات المقررة في القوانين غير الجنائية بالنسبة للمسائل الأولية مشروط بأن تكون هذه المسألة عنصر مفترض في الجريمة سابق في وجوده على ارتكاب الفعل الإجرامي.

فالإشكالية تبرز كذلك عند اللجوء للدليل الإلكتروني من أجل إثبات العقد الخاص بالأمانة في حالة ما إذا قام طرفا عقد الأمانة بإبرام هذا العقد عن طريق الإنترنت، وكان العقد يتجسد في شكل سند أو محرر إلكتروني، وعلى ذلك إذا كان يتعين على القاضي الجزائي حسب الأصل أن يستبعد الدليل الجنائي بما في ذلك الدليل الإلكتروني عند إثبات المسائل الأولية والتقيد بما هو وارد في النصوص الخاصة بتلك المسائل، إلاّ أنه في هذه الحالة يستثنى منها الدليل الإلكتروني الذي أصبح له دور خاصة في المعاملات المدنية والتجارية، حيث

[1]- أ. عائشة بن قارة، المرجع السابق، ص 230.

[2]- نقض 22-02-1970 مجموعة أحكام النقض س 21 رقم 27 ص 272. نقلا عن د: ياسر الأمير فاروق، المرجع السابق، ص 640.

أدى ذلك إلى تغيير مفهوم الإثبات تبعا لإمكانية إنشاء الحقوق والإلتزامات بطرق إلكترونية، والإستغناء في غالب الأحيان عن الكتابة الورقية.

غير أنه وحتى تواكب مختلف الدول هذه التطورات في مجال تكنولوجيا الإتصالات عن بعد وبالتالي تنمية وتشجيع التجارة الإلكترونية قامت بتوسيع تعريف الكتابة لتشمل المحررات الإلكترونية وذلك كالتشريع الفرنسي الجزائري والمصري، كما تم الإعتراف بالمحرر الإلكتروني كدليل لإثبات المعاملات الإلكترونية[1].

غير أنّ الدليل الكتابي يتألف من عنصرين جوهريين، الكتابة والتوقيع سيتم التطرق لهما على النحو التالي:

أولا: الكتابة الإلكترونية.

بالنسبة للتشريع الفرنسي تنص المادة (1316)[2] من القانون المدني الفرنسي على أن: "الإثبات بالكتابة أو الدليل الكتابي ينتج من تتابع حروف أو خصائص مطبوعة أو أرقام أو كل إشارة أو رموز لها معنى مفهوم أيا كانت الدعامة المدون عليها وطريقة نقله".

كما تنص المادة (1316-01)[3] من القانون المدني الفرنسي على أنه: "تقبل الكتابة في شكل إلكتروني كدليل في الإثبات مثلها في ذلك مثل الكتابة على دعامة ورقية، ما دام أنّ الشخص المنسوب إليه هذه الكتابة قد تم تحديده على وجه صحيح، وقد تم إثبات هذه الكتابة والإحتفاظ بها في ظروف من شأنها أن تضمن سلامتها".

[1]– أ. عائشة بن قارة، المرجع السابق، ص 235.

[2] - Article 1316 (C.C.F Modifié par Loi n°2000-230 du 13 mars 2000 - art. 1 JORF 14 mars 2000) : La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.

[3] - Article 1316-1 (C.C.F Créé par Loi n°2000-230 du 13 mars 2000 - art. 1 JORF 14 mars 2000) : L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

وقد أخذ المشرع الجزائري حرفيا بالنص السابق ذكره، وذلك بموجب القانون رقم (05-10)[1] ، حيث تنص المادة (323 مكرر 1) على أنه يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها.

وفي هذا الصدد فالخصائص المادية للوسيط الإلكتروني تمثل عقبة أمام تحقق هذا الشرط، ذلك أن التكوين المادي للشرائح الممغنطة والأقراص المغناطيسية تتميز بقدر من الحساسية بما يعرضها للتلف السريع، إلا أن هذه الصعوبة تم التغلب عليها باستخدام أجهزة ووسائط أكثر قدرة وجودة[2].

أما بالنسبة للوسائل الإلكترونية الأخرى كالفاكس مثلا، فاتفاقية الأمم المتحدة لنقل البضائع لسنة 1978 أعطت السندات المرسلة بالفاكس حجية في الإثبات وذلك بمنحها حجية السندات العرفية[3].

وقد أعطى الفقه الفرنسي السندات المرسلة عبر جهاز الفاكس الحجية في الإثبات عندما لا يتطلب القانون شكلا معينا للتصرف المراد إبرامه والحرية في الإثبات ما لم يرد عليه قيد، وكذلك عندما نكون بصدد إلتزامات يسمح بإثباتها بطريق غير الكتابة[4]،أما السند المستخرج من التلكس يحتاج ليكون دليلا كتابيا كاملا في الإثبات، أن يتضمن شرطين وهما: الكتابة والتوقيع عليه من قبل المنسوب إليه السند[5]، وفيما يتعلق بالميكروفيلم يمكن القول بأنه يأخذ حكم الكتابة التقليدية، فالفرق الوحيد بينهما أن الكتابة العادية تكون على الورق، والبلاستيك بالنسبة للميكروفيلم،وهناك من الدول اشترطت أن تتطابق الصورة مع الأصل، وأن يحتفظ بالصور الميكروفيلمية المدة المنصوص عليها للأصل الورقي، وأن تبقى الصورة الميكروفيلمية متاحة للقراءة بشكل واضح طوال مدة الحفظ، وظهرت الحاجة إلى ضرورة الإعتراف بالقيمة الإثباتية للأشرطة والفاكس والميكروفيلم، وعموما كل ما يتعلق بالتكنولوجيات الحديثة، ولاشك أن الصور الميكروفيلمية تكون مقبولة إذا كانت في شروط مناسبة وفقا لما نص عليه القانون[6].

---

[1]- قانون رقم 05-10 مؤرخ في 20 يونيو سنة 2005، يعدل ويتمم الأمر رقم 75-58 المؤرخ في 26 سبتمبر سنة 1975 المتضمن القانون المدني، ج.ر العدد 44.

[2]- أ. غنية باطلي، الكتابة الإلكترونية كدليل إثبات، مجلة التواصل في العلوم الإنسانية والإجتماعية، كلية الحقوق، جامعة باجي مختار،عنابة، الجزائر، العدد30، جوان2012، ص 135.

[3]- أنظر نص المادة 3/14 من إتفاقية الأمم المتحدة لنقل البضائع لسنة 1978.

[4]- أنظر على التوالي: أ. أحمد عزمي الحروب، السندات الرسمية الإلكترونية، دار الثقافة، عمان ،الأردن، ط1، سنة2010، ص112. و في نفس المعنى :
Etienne Wery, Droit de la preuve : vers une preuve électronique ?, le 25/01/1999, disponible à l'adresse suivante : www.droit-technologie.org.

[5]-أ. غنية باطلي، المرجع السابق، ص131.

[6]-أنظر على التوالي : أ. أحمد عزمي الحروب، المرجع السابق، ص123. و في نفس المعنى :

أمّا بالنسبة للمشرع المصري، فقد أكد هو أيضا على هذه المساواة، حيث نصّ في المادة (15) من القانون رقم 15 لسنة 2004 الخاص بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعية تكنولوجيا المعلومات، بأنّ للكتابة الإلكترونية والمحررات الإلكترونية في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية، متى استوفت الشروط المنصوص عليها في هذا القانون وفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون، كما نص في المادة (16) منه على أن الصورة المنسوخة على الورق من المحرر الإلكتروني الرسمي حجة على الكافة بالقدر الذي تكون فيه مطابقة لأصل هذا المحرر الإلكتروني الرسمي والتوقيع الإلكتروني الموجودين على الدعامة الإلكترونية[1].

وعلى المستوى الأوروبي فقد اتجه الإتحاد الأوربي إلى توجيه مشرعي دول أوروبا بإقرار حجية الوثائق الإلكترونية ومساواتها بالوثائق الكتابية من حيث الحكم، والأهم من ذلك التوجيه بعدم اشتراط أن تبرز الأدلة من قبل منظميها والإستعاضة عن ذلك بشهادات خطية صادرة عن الجهات مالكة النظم أو جهات وسيطة، لما ظهر عمليا من مشكلات أبرزها أن جانبا من المعلومات لا يدخلها أو ينظمها الأشخاص وإنما يخلقها جهاز الحاسب الآلي نفسه ضمن عمليات المعالجة وفي إطار تقنيات البرمجيات القائمة على الذكاء الصناعي[2].

أما بالنسبة لمسألة الإختيار بين الدليل الكتابي والدليل الإلكتروني، فقد يختلف الدليل الكتابي مع الدليل الإلكتروني، في هذه الحالة أورد القانون المدني الفرنسي حكما خاصا بهذه الحالة يتمثل في السلطة التقديرية للقاضي[3] ، فتنص المادة (1316-2)[4] على أنه عند غياب اتفاق بين طرفي النزاع، فإن القاضي هو الذي يحدد أيا من المستندات المقدمة إليه أقرب إلى الحقيقة بغض النظر عن الدعامة المكتوب عليها الدليل أي سواء كانت دعامة تقليدية أو إلكترونية.

ومن الجدير بالملاحظة أن المادة (15) من القانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني في مصر يضع على قدم المساواة المحرر الإلكتروني والمحرر التقليدي، وبالتالي في حالة التعارض

Claude Fabien, La preuve par document technologique, R.J.T , Faculté de droit de l'Université de Montréal , N° 38, 2004,p538.

[1]– د. شيماء عبد الغني، المرجع السابق، ص 415.

[2]– د. هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص 262.

[3] – د. شيماء عبد الغني، المرجع السابق، ص 420. وفي نفس المعنى :

Marylou Garcias et Max Chouzier, La preuve informatique — Quelles nouveautés techniques pour quelles évolutions juridiques ?, Lexbase Hebdo édition affaires n˚280 du 18 janvier 2012, p02.

[4] - Article 1316-2 (C.C.F Créé par Loi n°2000-230 du 13 mars 2000 - art. 1 JORF 14 mars 2000) : Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support.

بين محررين أحدهما إلكتروني وآخر عادي يعود الأمر للسلطة التقديرية للقاضي للترجيح بينهما مستعينا بالخبرة إذا لزم الأمر[1].

أمّا بالنسبة للقانون الجزائري، فلا يوجد نص يفضل بين المحرر الإلكتروني والمحرر التقليدي في الإثبات، إذ ترك المشرع تقدير ذلك لسلطة القاضي.

وفي هذا الخصوص يتعين ذكر أن قواعد الإثبات ليست من النظام العام، وبالتالي يمكن للأطراف أن يتفقوا على ما يخالف قواعد معينة للإثبات يكون القانون قد أوردها، وبالتالي فإن طريقة التعامل بالإنترنت تدل على أنّ هناك إتفاقا ضمنيا بين الأطراف على إثبات تعاملاتهم بطرق أخرى غير تقليدية وهي طريق المحررات الإلكترونية.

غير أنه ينبغي الإشارة إلى أنّ هناك صعوبات أخرى تقف عائقا أمام الأخذ بالدليل الإلكتروني فيثار التساؤل عن مدى جواز الإستناد إلى البيانات الصادرة من جهاز الكمبيوتر الخاص بالتاجر كدليل في الإثبات؟

فالمحرر إذا كان خارجا من جهاز الكمبيوتر الخاص بالمجني عليه، فإنه ضعيف في قوته الثبوتية، فمن المقرر أنه في المواد الجنائية يجوز الإستناد إلى شهادة المجني عليه،أما المواد المدنية فلا يجوز التعويل على شهادة خصم في الدعوى، بدليل أنه لا يجوز للمتهم أن يصطنع دليلا لنفسه لكي يتمسك به في مواجهة الطرف الآخر. ومع ذلك هناك إستثناءات تجيز الخروج على هذا المبدأ استنادا إلى الدفاتر التجارية، فهل مخرجات الكمبيوتر تعد دفاتر تجارية؟

فبالنسبة لمخرجات الكمبيوتر يجوز التحشير فيها والإضافة إليها، فلا يمكن القول أنها منتظمة سيما الدفتر الورقي المكتوب بحيث تمتنع أي إضافة مما يتيح للمحكمة الأخذ به، مما يترتب عليه أنه لا يجوز الإستناد إلى مخرجات الكمبيوتر كدليل إثبات لهذه الإلتزامات، غير أنّ القانون المدني لمقاطعة الكيبك في كندا في المادة (2837) قد خرج على ذلك وسمح بالاعتداد بالبيانات الصادرة من كمبيوتر التاجر إذا توافرت الشروط التالية[2]:

- أن تكون البيانات مفهومة وبالتالي لا يسمح بالبيانات المشفرة.
- أن يقدم جهاز الكمبيوتر ضمانات جادة وكافية لكي يكون محلا للثقة.
- المحكمة هي التي تحدد وجود ضمانات كافية وذلك إبتداءا من الظروف التي دونت فيها البيانات.

[1]- د. شيماء عبد الغني، المرجع السابق، ص 420.

[2]- نقلا عن :نفس المرجع، ص 399.

فقانون مقاطعة الكيبك يعتد بالمستندات الإلكترونية كدليل في الإثبات، و إن كان يشترط إضافة ما يدعم هذه المستندات حتى تتأكد مصداقيتها و بالتالي يتم الإعتماد عليها كدليل في الإثبات[1].

ثانيا: التوقيع الإلكتروني.

مع ظهور التجارة الإلكترونية، أصبحت الوثائق الرقمية متداولة بكثرة، و أصبح من الصعب إثبات وجود المعاملات عبر الإنترنت، ولذلك كان لابد من الإعتراف بالتوقيع الإلكتروني الذي أصبح ضرورة ملحة، حيث لا يمكن استبعاده لمجرد أنه في بيئة إلكترونية[2].

ففي مجتمع المعلومات أصبح سوق البيانات رهان إقتصادي كبير، خاصة مع انتشار استخدام الوثائق الإلكترونية، إلا أن هذه الأخيرة ما يدعمها هو الإعتراف بالتوقيع الإلكتروني،الذي أصبح يضمن نسبة هذه الوثيقة إلى صاحبها من أجل تفادي أي غموض أو لبس حولها[3].

ويعرف بأنه: "مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية الفرد وقبوله بمضمون التصرف الذي يصدر التوقيع الإلكتروني بمناسبته"[4].

كما يعرف بأنه: "بيانات في شكل إلكتروني موجودة في رسالة بيانات أو مضافة إليها ومرتبطة بها منطقيا، تنسب لشخص معين"[5].

فالمادة (1316-04)[6] تتعلق بالتوقيع، ونصت على شكلين أساسيين للتوقيع يتمثلان في التوقيع العادي اليدوي الذي يتم نسبته إلى شخص معين والتوقيع الإلكتروني ونصت بأنه يتمثل في استعمال طريقة معينة تبرز العلاقة بين التوقيع و صاحبه.

---

[1] - Michel Gagné, La preuve dans un contexte électronique, Ce texte est publié dans Développements récents en droit de l'Internet, Service de la formation permanente, Barreau du Québec, Éditions Yvon Blais Inc., 2001, p 02.

[2] - Mascré Heguy, la signature électronique et le bouleversement du droit de la preuve, disponible à l'adresse suivante : www.mascre-heguy.com/htm/fr/publications/avocatsignaturedroitpreuve.htm.

[3] - David Forest et Gautier Kaufman, Droit de l'informatique, Gualino, lextenso éditions, Paris, France, 2010, p84.

[4] – د. خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2007، ص 38.

[5] - Signature électronique, Document édité par le Bureau conseil de la direction centrale de la sécurité des systèmes d'information (DCSSI),25.08.2004, Paris, France ,p 04.

[6] - Article 1316-4 (C.C.F Créé par Loi n°2000-230 du 13 mars 2000 - art. 4 JORF 14 mars 2000) : La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.
Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.

هذا بالإضافة إلى شروط أخرى يمكن أن نجملها فيما يلي: أن يكون متعلقا بالموقع، أن يتم وفقا لطرق موثوق بها يستطيع الموقع تحمل مسؤوليته من خلالها، أن تكون هناك علاقة بين التوقيع والمحرر الإلكتروني[1].

وللإشارة فإن التوقيع الإلكتروني يستفاد منه رضاء الموقع وقبوله الإلتزام بمجرد وضع توقيعه بالشكل الإلكتروني على البيانات التي تحتويها المحررات الإلكترونية، لأن مجرد التوقيع يحمل دلالة الرضا والإلتزام على ما تم التوقيع عليه[2].

وبالرجوع إلى القانون الجزائري، فالمشرع من خلال تعديل القانون المدني المشار إليه سابقا نص في المادة (327) على أنه يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة (323 مكرر 1) أعلاه".

كما أنّ المشرع الجزائري من خلال المرسوم التنفيذي رقم (07-162) [3] عرف التوقيع الإلكتروني بأنه معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين (323 مكرر و323 مكرر 1)، أمّا التوقيع الإلكتروني المؤمن فهو توقيع إلكتروني يكون خاصا بالموقع، كما يتم إنشاؤه بوسائل يمكن أن يحتفظ بها هذا الأخير وتكون تحت مراقبته الحصرية، كما يضمن مع الفعل المرتبط به صلة بحيث يكون كل تعديل لاحق للفعل قابلا للكشف عنه[4].

ولم يتعرض القانون الجزائري لكيفية التأكد من صحة التوقيع الإلكتروني عكس ما فعله المشرع الفرنسي الذي أصدر مرسوما يتناول المسألة بالتفصيل، ومن المؤكد أنه من الناحية العملية لا يمكن الخروج عن الطريقة التي وضعها القانون الفرنسي.

فيتمثل التوقيع الإلكتروني في وجود سلطة مختصة مهمتها أنها تتولى حفظ التوقيع الذي يضعه صاحبه على شكل حروف أو أرقام أو رموز تكون كلها مشفرة بحيث يستحيل استعمالها من طرف الغير، ويتم التوقيع على الوثيقة باستعمال مفتاحين أحدهما عام والثاني خاص مكونان تحت حفظ سلطة المصادقة، ويستعمل المفتاح الأول لتشفير الوثيقة والسند الذي يشمله، بحيث لا يمكن تغييره بصفة رسمية ولا يمكن إنكار إمضاء ممن نسب إليه[5].

---

[1] - Aboudramane Quattara, La preuve électronique (étude de droit comparé Afrique, Europe, Canada), Press universitaires d'Aix Marseille-PUAM-France, 2011, P 188-189.

[2]- د. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، بدون سنة، ص 243.

[3]- المرسوم التنفيذي رقم (07-162) المؤرخ في 13 جمادى الأولى عام 1428 هـ الموافق ل 30 مايو سنة 2007 يعدل ويتمم المرسوم التنفيذي رقم (01-123) المؤرخ في 15 صفر عام 1422 هـ الموافق ل 9 مايو سنة 2001 والمتعلق بنظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيه اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية. ج.ر. عدد 37 .

[4]- المادة 3 مكرر ف 2 من المرسوم التنفيذي السالف الذكر.

[5]- أ. نجيمي جمال، المرجع السابق، ص 260.

وبالنتيجة نجد أنّ التوقيع الإلكتروني يتمتع بكثير من الثقة في إجراءات توثيقه واستخدامه في تحديد هوية الموقع، فهو يتفوق على التوقيع التقليدي بالنظر لقدرته على التأكد من شخصية صاحب التوقيع، لذلك كان لابد من إدراك أهمية التوقيع الإلكتروني من أجل أمن المعاملات[1].

كما اعتد المشرع المصري بالقوة الثبوتية للتوقيع الإلكتروني بنصه في المادة (14) من القانون السابق الذكر، على أنه:" للتوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للتوقيعات في أحكام قانون الإثبات في المواد المدنية والتجارية إذا روعي في إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون.

أمّا عن الشروط التي يتطلبها المشرع المصري في القانون السابق لحجية التوقيع والكتابة والمحررات الإلكترونية، فإنه قد عددها في المادة (18) من القانون السابق بقوله:يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توافرت فيها الشروط التالية:

- ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.
- سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.
- إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني وتحدد اللائحة التنفيذية لهذا القانون الضوابط الفنية والتقنية اللازمة لذلك[2].

وبالتالي يمكن القول أنه مع ظهور الوثائق الرقمية تطور الإثبات وتم الإعتراف بالتوقيع الإلكتروني، إلا أننا بحاجة إلى وجود رابط موثوق بين التوقيع والوثيقة [3].

وبما أنّ التشفير يعتبر طريقة من طرق التوقيع الإلكتروني، فيطرح سؤال حول القيمة الثبوتية للمحرر المشفر، فبالنسبة للمحرر المشفر، يقصد به المحرر المكتوب بطريقة رمزية وليس بكتابة عادية بحيث لا يفهمه إلا طرفا التعامل، وما دام أن القانون في بعض التشريعات كالتشريع الفرنسي الذي أصبح يعترف بهذا النوع من

التشفير بمقتضى القرار رقم 2001/272 الصادر في 3-3-2001 الذي أجاز التشفير باعتباره طريقة من طرق التوقيع الإلكتروني.

[1]– د. لورانس محمد عبيدات، إثبات المحرر الإلكتروني ، دار الثقافة، عمان ،الأردن، ط1، سنة 2009، ص 155.و في نفس المعنى:
Lionel Revello , La Preuve électronique, disponible à l'adresse suivante : www.sam-mg.com.

[2]- د. شيماء عبد الغني ، المرجع السابق، ص 416.

[3] - Didier Frochot, Preuve et signature électronique, le 16/09/2005, disponible à l'adresse suivante : www.les-infostrategies.com.

ومؤدى ذلك أنّ تلك الرسائل لها قوة في الإثبات أمام المحاكم بل أكثر من ذلك يمكن القول بأن الرسالة المشفرة لها حجية في الإثبات تفوق الرسالة غير المشفرة، وذلك لأن التشفير يكفل لها حماية من العبث بها تفوق ما للرسالة غير المشفرة، وقد أدرك المشرع المصري أهمية تشفير الرسائل الإلكترونية وإن لم يستخدم هذا التعبير صراحة بمقتضى القانون رقم 15 لسنة 2004 عندما تضمن نصوصا تنظم عملية التصديق الإلكتروني[1].

وحتى المشرع الجزائري من خلال المرسوم التنفيذي رقم (07-162) السالف الذكر، تطرق للتشفير بطريقة غير مباشرة عند حديثه عن الشهادة الإلكترونية التي عرفها بأنها: "وثيقة في شكل إلكتروني تبث الصلة بين معطيات فحص التوقيع الإلكتروني والموقع"[2]، كما عرف مؤدي خدمات التصديق الإلكتروني بأنه: "شخص يسلم شهادات إلكترونية أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني"[3].

الفرع الثاني: مبدأ مشروعية الدليل الإلكتروني.

تخضع قواعد الإثبات الجنائي لمبدأ المشروعية، ومقتضاه أنّ الدليل الجنائي لا يكون مشروعا ومن تم مقبولا في الإثبات إلاّ إذا جرت عملية البحث عنه والحصول عليه وإقامته أمام القضاء في إطار أحكام القانون واحترام قيم العدالة وأخلاقياتها التي يحرص على حمايتها.

فإذا كان المشرع يلقي على كاهل المحقق مهمة كشف الحقيقة في شأن الجريمة وجمع أدلتها، فإن عمله مشروط بأن يتم في إطار الشرعية وذلك باحترام حقوق الأفراد وعدم المساس بها إلا في الحدود التي يقررها القانون[4].

كما وأنه وإن أجاز القانون المساس بالحرية الشخصية في حدود معينة من أجل الوصول إلى الحقيقة إلا أنه في ذات الوقت أحاط ذلك بضمانات معينة يتعين احترامها حتى لا يتم تغليب سلطة العقاب على احترام الحريات الشخصية[5].

---

[1]- د. شيماء عبد الغني، المرجع السابق، ص 417.

[2]- المادة 3 مكرر فقرة 8 من المرسوم السابق.

[3]- المادة 3 مكرر فقرة 10 من المرسوم السابق.

[4]- أ. عائشة بن قارة، المرجع السابق، ص 213.

[5]- د. طارق فوزي الفقي، المرجع السابق، ص 209.

وترتيبا على ما تقدم فإنه يتعين على القاضي الجزائي ألا يثبت توافر سلطة الدولة في عقاب المتهم بصفة عامة والمتهم المعلوماتي على وجه الخصوص وذلك من خلال إجراءات مشروعة تحترم فيها الحريات، وتؤمن فيها الضمانات التي رسمها القانون، ولا يحول دون ذلك أن تكون الأدلة تقليدية أم كانت أدلة إلكترونية صارخة على إدانة المتهم طالما كانت هذه الأدلة مشبوهة ولا يتسم مصدرها بالنزاهة واحترام القانون.

وفي الدول ذات النزعة اللاتينية، فإنه وإن كان الإثبات الجنائي حر، إلا أن احترام حقوق الدفاع ونزاهة القضاء تستوجب أن تكون الحصول على الدليل الجنائي قد تم وفقا لطرق قانونية مشروعة، كما أنّ النزاهة هي مسألة تطفو فوق الشرعية وترتبط بالقيم الأخلاقية وبدرجة التمدن وترتكز على اعتبارات العدالة والإنصاف وكرامة القضاء وهيبته[1].

وفي كل الأحوال فإنّ قاعدة المشروعية تستلزم ضرورة إتفاق الدليل الإلكتروني مع النظام القانوني في جملته،و ليس فقط مجرد موافقته للقاعدة المكتوبة أو المنصوص عليها من قبل المشرع، فعلى سبيل المثال فإن قانون الإجراءات الجزائية الفرنسي رغم أنه لا يتضمن أية نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة القضائية حتى بعد تعديلاته الأخيرة، إلاّ أنّ الفقه والقضاء كان بجانب هذا المبدأ سواء في مجال الجرائم التقليدية أم في مجال الجرائم الإلكترونية.

وقد حرص المشرع المصري على إيضاح معنى قاعدة المشروعية وفقا للتعريف السابق، والتي أفصح من خلالها المشرع على وجوب مراعاة أحكام القانون بصفة عامة عند تنظيم الحرية الشخصية للمواطن، وعند القبض عليه أو تقييد لحريته أو إنتهاك حرمة مسكنه أو مراسلاته أو اتصالاته[2].

ونفس الموقف بالنسبة للمشرع الجزائري الذي نص على مبدأ المشروعية من خلال نصوص المواد (32[3]-34[4]-35[5] -46[6]) من الدستور الجزائري.

وبما أنه قد تم التطرق لمشروعية إجراءات جمع الأدلة في الباب الأول، فسنقصر الدراسة على المشروعية في اختيار وسائل الإثبات الجنائي، فمن الأمثلة للطرق غير المشروعة في الحصول على الدليل الإلكتروني استخدام التعذيب أو الإكراه المادي أو المعنوي في مواجهة المتهم المعلوماتي لفك شفرة نظام من

---

[1] – د. محمد مروان، المرجع السابق، ج2، ص 419.

[2]- د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص 121.

[3]– تنص المادة 32 من الدستور الجزائري على ما يلي:" الحريات الأساسية وحقوق الإنسان والمواطن مضمونة ...".

[4]– تنص المادة 34 من الدستور الجزائري على ما يلي:" تضمن الدولة عدم انتهاك حرمة الإنسان، ويحظر أي عنف بدني أو معنوي أو أي مساس بالكرامة".

[5]- تنص المادة 35 من الدستور الجزائري على ما يلي:"يعاقب القانون على المخالفات المرتكبة ضد الحقوق والحريات، وعلى كل ما يمس سلامة الإنسان البدنية البدنية والمعنوية ".

[6]- تنص المادة 46 من الدستور الجزائري على ما يلي:" لا إدانة إلا بمقتضى قانون صادر قبل ارتكاب الفعل المجرم".

النظم المعلوماتية أو الوصول إلى ملفات البيانات المخزنة وأعمال التحريض على ارتكاب الجريمة الإلكترونية من قبل رجال الضبطية القضائية.

ولا شك أن الحق في حرمة الجسم من أهم الحقوق التي يتمتع بها الإنسان في المجتمع بعد حقه في الحياة، ويقصد بهذا الحق عدم المساس بسلامة الجسد و بالعمل الطبيعي لوظائف الأعضاء، فضلا عن تحرره من الآلام البدنية والنفسية[1]، كما أن الحصول على الدليل عن طريق إعتراض المراسلات السلكية و اللاسلكية وكذا تسجيل الفيديوهات يعد عملا باطلا، وعلى القاضي أن يسهر على تطبيق تدابير الحماية من أجل ضمان إحترام الحياة الخاصة للأفراد[2].

فإذا كان هدف الإثبات في الدعوى الجنائية هو إظهار الحقيقة، فإن هذه الغاية لا تبرر استعمال أي وسيلة، وبالتالي فإن حرية مبدأ الإثبات الجنائي ترد عليه قيود تتمثل في ضرورة مراعاة الشرعية في اختيار هذه الوسائل.

ويرى فقهاء القانون الجنائي أنّ الإكراه بصفة عامة والتعذيب بصفة خاصة هما من الطرق اللاإنسانية التي يجب نبذها كلية، لأنه من غير الممكن الوصول إلى الحقيقة مادام المتهم واقعا تحت تأثير التعذيب، فكل الأساليب التي تؤثر على الإرادة الحرة للإنسان سواء كانت عن طريق التعذيب أو الإكراه يجب أن تستبعد[3].

ولا يختلف أيضا ضرورة تطلب مشروعية الدليل الإلكتروني في الأنظمة القانونية التي أخذت بمبدأ الإثبات المقيد وفقا لما يسمى بقاعدة الإستبعاد، ففي إنجلترا مثلا يوجد اتساع العمل بقاعدة استبعاد الدليل الذي تم الحصول عليه بطريقة غير مشروعة.

وهكذا فإن كل دليل قد تم التوصل إليه مباشرة أو بطريقة غير مباشرة وكان متضمنا إعتداءا على الحقوق الأساسية للمواطن يتعين استبعاده حتى ولو كانت دليلا ملائما أو موضوعيا أي يتصل بموضوع النزاع مباشرة فيثبته أو يساهم في إثباته.

وفي كندا ينبغي استبعاد الدليل الذي يتم الحصول عليه بطريقة غير مشروعة فالمادة (2/24) من الدستور الكندي للحقوق والحريات تقرر أنّ المحكمة إذا رأت أثناء نظرها لعناصر الإثبات أنه قد تم الحصول

---

[1] – د. آدم عبد البديع حسين، الحق في الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، رسالة دكتوراه، جامعة القاهرة، مصر، سنة 2000، ص 338.

[2] - Pierre Bolze, Le droit à la preuve contraire en procédure pénale, Thèse Doctorat, Faculté de Droit, Sciences économiques et Gestion, Université Nancy 2, France, 2010, p 395.

[3] - د. محمد مروان، المرجع السابق، ج2، ص 407.

عليها في حالات تحمل اعتداء على الحقوق والحريات التي يحميها الدستور فإنه يجب استبعادها بالنظر إلى هذه الظروف لأنّ استخدامها يفقد العدالة إعتبارها[1].

كما لا تختلف الأنظمة القانونية التي تعتنق مبدأ الإثبات المختلط عن سابقتها في وجوب استناد الحكم بالإدانة على أدلة إلكترونية التي تم الحصول عليها من خلال اعترافات غير مشروعة هذا وإذا كان الفقه الياباني يرى أنّ الأدلة التي يتم الحصول عليها بطريقة غير مشروعة يجب استبعادها سواء كانت تقليدية أم مخرجات كمبيوتر، إلاّ أنّ المحكمة العليا اليابانية ضيقت من نطاق تطبيق قاعدة الإستبعاد وذلك باشتراطها صفة الخطورة إلى جانب عدم المشروعية لاستبعاد الدليل، إذ قررت في أحد أحكامها أن البحث عن الحقيقة يجب أن يتم مع ضمان حقوق الإنسان وعدالة الإجراءات، إلاّ أنه على الرغم من تبني المحكمة العليا في اليابان قاعدة استبعاد الدليل الذي تم الحصول عليه بطريقة غير مشروعة، شريطة اتصاف عدم المشروعية بالخطيرة، إلا أنه من الناحية العملية فإن التطبيقات القضائية لحالات إستبعاد الأدلة الجنائية بما في ذلك الدليل الإلكتروني قليلة الوقوع بل أنها نادرة[2].

أمّا المشرع الجزائري فلم يتدخل بصفة حاسمة للفصل في مختلف جوانب هذه المسألة الشائكة، بل جاءت النصوص بمعالجة جزئية للموضوع مما ترك المجال واسعا أمام الاجتهاد القضائي الذي يجب عليه إعطاء الأجوبة حسب معطيات كل قضية تطرح عليه، ومن خلال الأحكام القضائية يمكن أن تبرز بعض المبادئ التي يستنتجها الفقه وأهمها :

- إحترام كرامة الإنسان واحترام حياته الخاصة.
- التقيد باحترام القواعد الإجرائية من طرف المصالح العمومية.
- منع كل تصرف يشكل تشجيعا أو تحريضا على ارتكاب الجرم ثم استغلال الأدلة المحصلة من خلاله.
- السماح لمن يكون ضحية جرم أن يحضر ما يراه من أدلة في إطار حقه في الدفاع.
- قانون الإجراءات الجزائية يشترط فقط طرح الأدلة على بساط البحث ومناقشتها بصفة وجاهية، ولم يشترط نزاهتها أو مشروعيتها، لأنه من حق القائمين بالمتابعة والبحث أن يسعوا للحصول على أدلة الإثبات شريطة

[1]– أجابت المحكمة العليا في كندا على أنه متى يكون استخدام الدليل يفقد العدالة اعتبارها في قضية زس كولان، فقالت أن القاضي ينبغي له أن يأخذ في الإعتبار ثلاث مجموعات من العوامل التالية: أولها يرتبط بعدالة الدعوى، وثانيها العوامل المرتبطة بجسامة الإعتداء، وآخرها العوامل والتي تتعلق بأثر استبعاد الدليل إذا انعدمت الأدلة الأخرى وكانت الجريمة المرتكبة متناهية الخطورة، وعلى ضوء هذه العوامل مجتمعة يقرر القاضي ما إذا كان استخدام الدليل يفقد العدالة اعتبارها أم لا.نقلا عن د.هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 131.

[2]– نقلا عن: د.طارق فوزي الفقي، المرجع السابق، ص 213.

ألا تتضمن تلك المساعي أي تحريض أو تشجيع للمتهم على ارتكاب الفعل المجرم، وهو ما يعرف بنزاهة الحصول على أدلة إثبات، فإن كان دور المحقق يقتصر على الترصد مثلا للمتهم لضبطه متلبسا بفعل معين دون أن يصدر من المحقق أي توجيه أو تحريض فهذا ليس مخالفا للقانون، والمثل البسيط على ذلك هو وضع رادارات مراقبة سرعة السيارات وأخذ صورة للمخالف دون علمه، أو وضع كاميرات تسجيل في المؤسسات والفنادق[1].

غير أنه إذا تجسد الدليل الناجم عن المراقبة في صورة تسجيلات، فإنّ قبوله يتوقف على توافر عدة ضوابط تتمثل في أن يتأكد القاضي من أنّ الصوت المسجل يخص المتهم وعدم حصول تعديل بالتسجيل أو إجراء مونتاج على الشريط وأن يكون التسجيل واضحا، وكلها تعد ضمانات فنية لمشروعية التسجيل الصوتي المترتب على المراقبة الإلكترونية وتتمثل فيما يلي:

أولا: التأكد من أن الصوت المسجل يخص المتهم:

لعل من أهم الموضوعات التي تثار في حالة تجسد الدليل الناجم عن المراقبة في التسجيلات الصوتية هو هل الصوت المسجل على شريط التسجيل الخاص بالمتهم من عدمه ؟ ولاشك أنّ القاضي يحتاج في حسم هذا الأمر إلى الإستعانة بخبير في الأصوات يكون رأيه استشاريا عملا بالقواعد العامة في الإجراءات الجزائية.

والمقصود ببصمة الصوت أنها عينة من صوت المتهم يأخذها خبير الأصوات بأن يجعل المتهم ينطق الحروف العالية والمنخفضة من الألفاظ، ثم يقوم بإجراء المضاهاة بين هذه العينة والتسجيلات للحكم على الصوت الموجود بالتسجيلات ببيان عما اذا كان بصوت المتهم من عدمه.

ففي الولايات المتحدة الأمريكية اعترفت العديد من ولاياتها ببصمة الصوت كدليل يمكن تقديمه أمام القضاء بصدد قضايا القتل والشروع فيه و الإغتصاب و الإختطاف و الرشوة و المخدرات، إلاّ أنّ هناك مشكلة واجهت القضاء الأمريكي والتي تقرر فيها مبدأ قضائي حول قبول الأدلة الفنية إذ اشترط أن تكون مقبولة من الوسط العلمي المتخصص[2].

وفي الواقع توجد ثلاثة طرق للحصول عل البصمة الصوتية :

أ. الطريقة السمعية (الأسلوب التقليدي): وتتلخص في قيام الخبراء المتخصصين بالإستماع إلى تسجيلات حديثة لبعض الأشخاص وملاحظة سماتها والربط بينها وبين المادة الصوتية للمشبه فيه.

[1] – أ. نجيمي جمال، المرجع السابق، ص82.

[2] – د.ياسر الأمير فاروق، المرجع السابق، ص658.

ب. الطريقة الآلية : وتتضمن إستخدام أجهزة التحليل الصوتي لتحليل المادة الصوتية المتوافرة بعد ربطها بالحاسب الآلي وتحليل النتائج ومقارنتها بنتائج أخرى يتم إدخالها عند الحاجة.

ج. الطريقة المرئية : وتتم باستخدام جهاز المخطط الصوتي المرئي والذي يعتمد على ترجمة الصوت البشري إلى صور أو رسوم دقيقة تمثل ذبذبات النبرة الصوتية المكونة للعناصر الفيزيائية للصوت (مقدار الذبذبة، وحدة الصوت، نبرته و تردده)[1].

و لابد من أن تتضمن مراكز أبحاث الصوت في المجال الجنائي وحدتين هما :

أ. وحدة الفحص الفيزيائي : وذلك باستخدام جهاز التخطيط التحليلي للصوت والأجهزة المساعدة والخبير المختص بهذا الفحص وهو مهندس صوت.

ب. وحدة فحص النطق والتخاطب: والخبير المختص بهذا الفرع من الفحص السماعي هو أخصائي النطق والتخاطب[2].

ثانيا: التأكد من عدم حدوث تعديل بالتسجيل أو إجراء مونتاج على الشريط.

لا يكفي أن يتأكد القاضي من أنّ التسجيل المقدم كدليل إدانة في الدعوى بصوت المتهم، وإنما يلزم فوق ذلك أن يتحقق القاضي من عدم حصول تعديل بالتسجيل أو إجراء مونتاج على الشريط، فمن المعروف علميا أنه يمكن الغش في التسجيل بنقل أجزاء معينة من الأحاديث المسجلة على شريط آخر حتى أنه يبدو حديثا متكاملا.

غير أنه لا ينبغي أن يكون احتمال الغش في التسجيلات مدعاة للتشكيك في قيمة الدليل، ذلك أنه يمكن تلافي حدوث تعديل بالتسجيلات أو إجراء مونتاج على الشريط، وذلك بأن ينص المشرع صراحة على إلزام المحقق بأنه يوقع بصوته على بداية الشريط للتأكيد من أنّ التسجيلات التي أجريت على الشريط معتمدة، وكذلك إلزام المحقق بالتأكد من أنّ الشريط نظيف تماما وفارغا وليست عليه أية تسجيلات فارغة[3].

ثالثا: أن يكون التسجيل واضحا.

لكي يستند القاضي إلى الدليل المستمد من المراقبة لابد أن يكون هذا الدليل واضحا، وهو لا يكون كذلك إلاّ إذا كان التسجيل قد رسم صورة الواقعة الإجرامية كاملة، إذ يستطيع القاضي في هذه الحالة يجب أن يستخلص الحقيقة من التسجيل، وعليه يتعين استبعاد التسجيلات وطرحها جانبا متى كانت

[1] – د.طه أحمد طه متولي ،الدليل العلمي وأثره في الإثبات الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة طنطا، مصر، سنة 2007 ،ص199.

[2] – د.حسين المحمدي بوادي ،المرجع السابق، ص73.

[3]- د. ياسر الأمير فاروق، المرجع السابق، ص 666.

مجهولة لأشخاص المتحدثين أو جاء بها تشويش أو احتوت في معظمها على جمل غير واضحة أو عبارات غير مسموعة أو متداخلة أو أصوات غير عادية إذ أنّ ذلك يدفع المحكمة إلى عدم الإطمئنان إلى التسجيل والثقة فيه[1].

والخلاصة هي أنه إذا كان مبدأ حرية الإثبات الجنائي ينطوي على حرية اختيار وسائل الإثبات وذلك بقبول اللجوء إلى أي طريقة من طرق الإثبات، فإن هذه الحرية لا تتعلق بإدارة وتقديم الوسائل المختارة، فهذه الأخيرة تخضع لتنظيم قانوني محكم لأجل ضمان جديتها في إظهار الحقيقة مع ضرورة احترام حقوق الشخص الذي يعتبر بريئا إلى أن تثبت إدانته من طرف جهة قضائية مختصة[2].

المطلب الثاني: الضوابط التي تحكم مبدأ الإقتناع الشخصي بالدليل الإلكتروني.

إنّ الرباط الموجود بين مبدأ حرية الإثبات ومبدأ الإقتناع الشخصي رباط لا يمكن تصور انفصامه، فكلاهما يكمل الآخر، بل إنّ المبدأ الثاني هو نتيجة طبيعية للأول، لذلك فليس من باب الصدفة أن يذكر المشرع في نفس النص القانوني هذين المبدأين[3].

فالقاضي الجزائي وإن كان يتمتع بسلطة واسعة في تقديره للأدلة بما في ذلك الدليل الإلكتروني، إلاّ أنّ هذه السلطة ليست مطلقة، بل وضع المشرع ضوابط وهي بمثابة صمام أمان إزاء انحراف القاضي عند ممارسته لها[4]، وتتمثل هذه الضوابط فيما يلي:

الفرع الأول: مبدأ يقينية الدليل الإلكتروني.

اليقين القضائي ليس هو اليقين بالمعنى الفلسفي كحالة نفسية وذهنية تلتصق فيها حقيقة الشيء في الذهن على نحو لا يثير شكا ولا يحتمل غلطا، بل هو يقين قائم على تسبيب وأدلة وضعية، ولذلك فهو يقين تقريبي يوصف في العلم بأنه اقتناع وهو حالة ذهنية يتوفر فيها لدى القاضي من الأدلة الوضعية ما يكفي لاقتناعه بالتسليم بثبوت الواقعة كما أثبتها في حكمه، ويكفي فقط أن يشك القاضي في ثبوت التهمة بالبراءة مادامت المحكمة قد ألمت بواقعة الدعوى وأدلتها وخلا حكمها من عيوب التسبيب ومن الخطأ في القانون[1].

---

[1] - د.ياسر الأمير فاروق، المرجع السابق، ص 667.

[2] - Décision de la cour de cassation.

نقلا عن: د. محمد مروان، المرجع السابق، ج2، ص 418.

[3] - د. محمد مروان، المرجع السابق، ج2، ص 478.

[4] – أ. عائشة بن قارة، المرجع السابق، ص 267.

ويمكن القول أنّ اليقين والإقتناع والحقيقة عبارة عن حلقات ثلاث في سلسلة واحدة بدايتها اليقين وهذا اليقين يتدرج من الضعف إلى القوة مع تدرج السير في إجراءات الدعوى الجزائية، ويواكب هذا التدرج تدرج آخر في الاقتناع ، وعندما يتكامل اليقين ينشأ منه ما يسمى بالاقتناع اليقيني، وهو أساس الحقيقة القضائية التي ينشدها القاضي في حكمه.

وإذا كان مصطلح اليقين يغاير مصطلح الإقتناع فإنه يغاير مصطلح الحقيقة، إذ أنّ حقيقة الواقعة الإجرامية تمثل النموذج الواقعي لكيفية حدوثها أو طريقة ارتكابها ومن اشترك أو ساهم فيها وغير ذلك من التفصيلات كما حدثت بالفعل على مسرح الجريمة، وتكون وظيفة الأدلة هو نقل وتصوير هذا الواقع أمام المحكمة، في حين أن اليقين يمثل حالة ذهنية أو عقلانية تتولد لدى القاضي محدثة انطباعا مؤكدا عن كيفية حدوث الواقعة الإجرامية، ويتوقف تكامل هذا اليقين في ضمير القاضي على قدرة الأدلة المطروحة بما فيها الدليل الإلكتروني على توصيل القاضي إلى هذه المرحلة، بحيث أنه إذا استطاع القاضي إدراكها فإنه في هذا الفرض تتطابق حالة الذهن والعقل مع حالة الواقع والحقيقة، وعلى العكس من ذلك يتباعد مصطلح اليقين في حالة تشكك القاضي وعدم قدرة أدلة الدعوى ومن بينها الأدلة الناتجة عن الحاسبات الآلية بطبيعة الحال على توصيله إلى تلك المرحلة من اليقين[2].

ويرى البعض أن النشاط الذهني والوجداني للقاضي يمر بأربعة مراحل حتى يصل إلى اليقين وهي:

1- مرحلة خلو ذهن القاضي من الواقعة:

ويعني ذلك ألاّ يكون لدى القاضي معلومات مسبقة عن الدعوى المطلوب منه الفصل فيها، وهذا المبدأ مقرر لضمان حياد القاضي، فالقاضي لا يحكم بناء على معلوماته الشخصية أو ما قد يكون شاهده بنفسه في غير مجلس القضاء.

2- مرحلة الشك:

في هذه المرحلة يقوم القاضي بالتأمل والتفكير العميق فيما اطلع عليه ويضع نفسه موضع الشخص الماثل أمامه، سواء أكان المتهم أو المجني عليه، يرى بعينه ويدرك بعقله محاولا الوصول إلى الشخصية الماثلة أمامه مستعينا في ذلك بخبرته السابقة وفهم الطبيعة البشرية فهما صادقا، وتتداخل في عقله العناصر الإيجابية والسلبية ويحاول أن يعبر مرحلة الشك، فإن استحال عليه في ذلك فعليه أن يقضي بالبراءة[3].

---

[1]- د.طارق فوزي الفقي، المرجع السابق، ص 217.

[2]- د.هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 83.

[3]- د.طارق فوزي الفقي، المرجع السابق، ص 217.

فقاعدة الشك يفسر لصالح المتهم تعتمد على مبدأ ضروري لإسنادها وهو أن الأدلة التي تقدم أمام القاضي الجزائي لإثبات وقوع الجريمة متروكة للسلطة التقديرية لقاضي الموضوع، بحيث أن الأدلة نفسها قد تكون مقنعة للبعض دون البعض، فالشك هو عكس اليقين، فما يراه أحدهم أمرا واضحا يقينيا، يراه الآخر موضع شك، وبالتالي تختلف النتيجة التي يصل إليها كل منهما، ولكن يتعين أن يكون هناك ضابط أو دليل للتمييز بين الشك المقبول كنشاط ذهني طبيعي وبين الشك الذي قد يكون أقرب إلى الظاهرة المرضية[1].

3- مرحلة الترجيح والإحتمال:

في هذه المرحلة يقوم القاضي بوضع الافتراضات الإحتمالية للصورة التي ارتسمت في ذهنه عن الواقعة ليكتشف ما إذا كانت إحداها يمكن أن تؤدي عقلا ومنطقا إلى نتيجة معينة مستعينا بذلك عن طريق الافتراضات العكسية التي يطرحها من واقع أدلة الدعوى، فيضع أدلة الإثبات في ناحية، وفي الأخرى أدلة النفي طارحا كل ما لا يرتاح إليه ضميره ويطمئن إليه وجدانه.

4- مرحلة بلوغ اليقين:

إذا استطاع القاضي ترجيح فرض من الفروض التي وضعها وتأكد أنه الصورة الحقيقية للواقعة محل الدعوى كما رسمها في وجدانه، فقد وصل بذلك إلى أعلى نقطة من الإحتمالات، ويتولد لديه اليقين وحقيقة الواقعة التي تتفق مع المنطق والعقل.

ويصل القاضي إلى يقينية الدليل الإلكتروني عن طريق نوعين من المعرفة أولهما المعرفة الحسية التي تدركها الحواس من خلال معاينة هذه الأدلة الإلكترونية وتفحصها، وثانيها المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والإستنتاج من خلال الربط بين هذه الأدلة والملابسات التي أحاطت بها، فإذا لم ينته القاضي إلى الجزم بنسبة الفعل أو الجريمة الإلكترونية إلى المتهم المعلوماتي كان من المتعين عليه أن يقضي بالبراءة، فالشك يجب أن يستفيد منه المتهم المعلوماتي[2].

[1]- أ. نجيمي جمال، المرجع السابق، ص 65.

[2]- د.طارق فوزي الفقي، المرجع السابق، ص 217.

الفرع الثاني: مبدأ وجوب مناقشة الدليل الإلكتروني.

يعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة أنّ القاضي لا يمكن أن يؤسس اقتناعه إلاّ على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى.

ولا يختلف الأمر بالنسبة للأدلة الإلكترونية بوصفها أدلة إثبات، إذ ينبغي أن تطرح في الجلسة وأن يتم مناقشتها في مواجهة الأطراف، فظهور المعلوماتية بكل خصائصها لا يغير شيئا من مبدأ الإقتناع الذاتي، فالإقتناع يجب أن يكون بناءا على أثر الدليل المتولد في نفس القاضي، والذي لا يترك أي مجال للشك، وحيث أن القانون لم يقم في المجال الجنائي نموذجا خاصا للإثبات، فإنّ قاضي الموضوع تكون له حرية التقدير، وله الهيمنة في الواقع على القيمة الدامغة للعناصر الإثباتية التي يؤسس عليها إقتناعه، والتي يكون للأطراف حرية الإعتراض عليها ومناقشتها في كافة مراحل الدعوى.

وهذا يعني أنّ الأدلة الإلكترونية سواء كانت مطبوعات أم بيانات معروضة على شاشة الحاسب، أم كانت بيانات مدرجة في حاملات البيانات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية، كل ذلك سيكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة.

وعلى ذلك فإنّ كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات، يجب أن يعرض في الجلسة، ليس من خلال ملف الدعوى في التحقيق الإبتدائي، لكن بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الوسائل الإلكترونية.

وأيضا بالنسبة لشهود الجرائم الإلكترونية الذين يكون قد سبق أن سمعت أقوالهم في التحقيق الابتدائي، فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة، كذلك فإنّ خبراء المعلوماتية على اختلاف تخصصاتهم ينبغي أن يمثلوا أمام المحاكم لمناقشتهم أو مناقشة تقاريرهم التي خلصوا إليها إظهارا للحقيقة، وأخيرا فإنّ متحصلات الجريمة الإلكترونية يجب أن تعرض على القاضي شخصيا، وذلك لأن حياد القاضي توجب عليه أن لا يقيم قضاءه إلاّ على ما يطرح أمامه وكان موضوع الفحص والتحقيق والمناقشة[1].

[1]- د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص 104.

وقد حرصت التشريعات الإجرائية في الدول ذات الصياغة اللاتينية على أن تنص صراحة على هذه القاعدة وفقا للمادة (427)[1] من قانون الإجراءات الجزائية الفرنسي التي تنص على أنه:"لا يجوز للقاضي أن يؤسس حكمه إلاّ على أدلة طرحت عليه أثناء المحكمة ونوقشت أمامه في مواجهة الأطراف"، كذلك المادة (32)[2] من قانون الإجراءات الجنائية المصري، كما أرست هذا الضابط المادة (2/212)[3] من قانون الإجراءات الجزائية الجزائري.

وقد عبرت محكمة النقض المصرية عن هذه القاعدة بقولها:"من المقرر أن لمحكمة الموضوع أن تستخلص من جماع الأدلة والعناصر المطروحة أمامها على بساط البحث الصورة الصحيحة لواقعة الدعوى حسبما يؤدي إليه اقتناعها، وأن تطرح ما يخالفها من صور أخرى لتقتنع بصحتها، ما دام استخلاصها سائغا مستندا إلى أدلة مقبولة في العقل والمنطق ولها أصل في الأوراق"[4].

ويقوم ضابط وجوب مناقشة الدليل الإلكتروني على عنصرين أساسيين هما:

1. إتاحة الفرصة للخصوم للإطلاع على الدليل الإلكتروني والرد عليه.
2. أن يكون للدليل الإلكتروني أصل في أوراق الدعوى.

بالنسبة للعنصر الأول، يجب على القاضي مبدئيا أن يطرح كل دليل مقدم في الدعوى للمناقشة أمام الخصوم، وذلك احتراما لحقوق الدفاع الذي يعد أحد المظاهر الأساسية لدولة القانون، ويتطلب مبدأ المواجهة نوعين من الضمانات: الأول منها سابق على عملية المواجهة ذاتها بين الأطراف في الجلسة، وهو يتضمن ضرورة إحاطة المتهم علما بالتهمة المنسوبة إليه، أما النوع الآخر من الضمانات، فيتم أثناء عملية المواجهة ذاتها وهي الأكثر تأثيرا في الدعوى الجنائية، إذ يلزم أن يسمح لكل طرف بتقديم ما لديه من مستندات وسؤال الشهود والخبراء وأن يطلب اتخاذ أي إجراء يقدر فائدته، ثم حق كل طرف في مناقشة أدلة الطرف الآخر وتفنيدها كسؤال الشهود ومناقشتهم، ومناقشة تقرير الخبير ودحض ما ورد به.

---

[1] - Article 427 du (C.P.P.F Modifié par Loi 93-1013 1993-08-24 art. 28 JORF 25 août 1993 en vigueur le 2 septembre 1993) : … Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui.

[2] - تنص المادة 32 من قانون الإجراءات الجنائية المصري على ما يلي: "لا تجوز للقاضي أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة".

[3] - تنص المادة 212 فقرة 02 من قانون الإجراءات الجزائية الجزائري على ما يلي: "ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".

[4] – نقض 1976/6/6، سنة 46، رقم 360، ص27، كذلك نقض 1982/10/13، السنة 53 رقم 929 نقلا عن: أ.عائشة بن قارة، المرجع السابق، ص270.

أمّا بالنسبة للعنصر الثاني والمتمثل في ضرورة أن يكون للدليل الإلكتروني أصل في أوراق الدعوى، وذلك حتى يكون اقتناع القاضي مبنيا على أساس، وفي ذلك قالت محكمة النقض المصرية في حكم حديث لها:"على المحكمة أن تبني حكمها على الوقائع الثابتة بالدعوى، وليس إقامة قضائها على أمور لا سند لها من التحقيقات"[1] وأن القاضي حر في استمداد اقتناعه من أي دليل يطمئن إليه، طالما أن له مأخذه الصحيح من الأوراق[2].

ومن أجل ذلك أوجب المشرع تحرير محضر الجلسة لإثبات وقائع الدعوى الجزائية وأدلتها لكي يتمكن قاضي الموضوع أو أي من الخصوم من الرجوع إلى هذا المحضر إذا ما رغبوا في استيضاح أي من الوقائع الثابتة به، وذلك منعا للتحكم وتحقيقا للعدالة.

وفي ذلك تشترط محكمة النقض المصرية أن يكون الدليل الثابت في أوراق الدعوى عماد الحكم، أي استندت إليه المحكمة في تكوين عقيدتها[3]، وبخلاف ذلك يكون حكمها معيبا، يستوي في ذلك دليل الإدانة أو البراءة، وذلك لمخالفته لحقوق الدفاع، وهو ما أكدت عليه محكمة النقض المصرية في قولها:"إنه محظور على القاضي أن يبني حكمه على دليل لم يطرح أمامه في الجلسة، يستوي في ذلك أن يكون دليلا على الإدانة أو البراءة، وذلك لكي يتسنى للخصوم الإطلاع عليه والإدلاء برأيهم فيه"[4].

كما يمنع على القاضي أن يؤسس اقتناعه على وسائل إثبات تضمنتها أعمال باطلة من الناحية الإجرائية، فقد يخضع المتهم عند استجوابه للتعذيب أو لأي أسلوب من أساليب الإكراه مما يجعله يعترف بالتهمة، وهنا لا يجوز للقاضي الجزائي أن يبني على هذا الإعتراف اقتناعه الشخصي لأنه عمل إجرائي باطل، كما ينبغي استبعاد تصريحات سجلت على إثر تنصت هاتفي غير شرعي[5].

ولابد من الإشارة أنه حتى يكون للقاضي الجزائي السيادة والهيمنة على الدعوى الجزائية، فلابد أن يكون مدربا تدريبا فنيا خاصا على كيفية التعامل مع تقنية المعلومات وأنظمة معالجة البيانات المعقدة، ومع الأدلة الناتجة عن الحاسب بشكل وافي ودقيق، فلا شك أنّ هذا التأهيل العلمي يضمن نجاح المهمة التي تناط بالقضاة، وهم بصدد مناقشة الأدلة الإلكترونية على اختلاف عناصرها ومفرداتها.

---

[1] – نقض 22 أكتوبر سنة 1990، مجموعة أحكام النقض، س41، رقم 162. ص 929. نقلا عن: أ. عائشة بن قارة، نفس المرجع، ص 273.

[2] – نقض 24 فبراير سنة 1975، مجموعة أحكام النقض، س26، رقم 12، ص188. نقلا عن: نفس المرجع، ص 273.

[3] – نقض 14 أبريل سنة 1952، مجموعة أحكام النقض، س3، رقم 309، ص850. نقلا عن: نفس المرجع، ص 273.

[4] – نقض 25 ماي سنة 1982، مجموعة أحكام النقض، س33، رقم 131، ص 644. نقلا عن: نفس المرجع، ص 273.

[5] - Ch Crim : 27 déc.1935 DP 1936 I 20.
Ch Crim : 11 Juin 1949. JCP 1949 IV 113.
Ch Crim : 28 Juin 1964. JCP 1964 IV 39 Rapport Mimin.
نقلا عن : د. محمد مروان، المرجع السابق، ج2، ص 497.

وإذا كان من المأمول اتخاذ عدد من الإجراءات حتى يمكن الإرتقاء بقضاة الحكم إلى المستوى اللائق للتطور الفني في مجال تكنولوجيا المعلومات التي تسير بخطوات واسعة، لذلك من المهم عقد دورات تدريبية لهؤلاء القضاة على كافة مستوياتهم ودرجاتهم في تقنية وعلوم الحاسب الآلي، فمن الضروري أن يكون هناك تأهيل تقني وفني للقضاة لمواكبة المناقشة العلمية للأدلة الإلكترونية[1].

ويترتب على إعمال مبدأ الشفوية أنه ينبغي على الشهود أن يدلوا بشهاداتهم شفويا، كما يمكن لرئيس الجلسة أن يبلغ لمساعديه أو للمحلفين وثائق مصورة أو تقرير خبير قبل سماع الشهود والخبراء أو تقديم وثائق أخرى من غير قراءتها شفويا أو قبل الإطلاع عليها من طرف المتهم[2].

كما يرى الدكتور محمد مروان أنّ علنية الجلسات تشكل إحدى أهم الضمانات الممنوحة للمتهم، من جهة فإن حضور الجمهور يضمن عدم إهدار حقوق الدفاع، ومن جهة أخرى فإن القاعدة تعتبر ذات أهمية كبيرة بالنسبة للقضاء نفسه إذ أنها تصون هيبته وسمعته، فبإمكان الجمهور حضور الجلسة إلى غاية النطق بالحكم طبقا لنصوص المواد (285[3]، 342[4]، 355[5])من قانون الإجراءات الجزائية الجزائري.

الفرع الثالث: تسبيب الأحكام القضائية.

من الضمانات القانونية التي أقرها المشرع لتقييد حرية القاضي في الإقتناع هي تسبيب الأحكام طبقا لنص المادة(379)[6] من قانون الإجراءات الجزائية الجزائري، فتسبيب الأحكام هو شرط موضوعية اقتناع القاضي، ويقصد بالأسباب الحجج الواقعية والقانونية التي ينبني عليها الحكم.

فالمتهم لابد أن يعرف بدقة لأي سبب أدين وصدر في حقه حكم قضائي، كما أنّ استيعاب الأسباب من طرف المتهم المدان قد يسهل بعد تنفيذ العقوبة وأثناء تنفيذها إعادة إدماجه، كما أنّ تسبيب

---

[1]– د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص 115.

[2] - Ch Crim : 09 Avril Bull N° 120-D1986 I.R.305 obs.Pradel.

نقلا عن : د. محمد مروان، المرجع السابق ، ص 492.

[3]– تنص المادة 285 من قانون الإجراءات الجزائية الجزائري على ما يلي:" المرافعات علنية ما لم يكن في علانيتها خطر على النظام العام أو الآداب ...".

[4] – تنص المادة 342 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يطبق فيما يتعلق بعلانية وضبط الجلسة المادتان 285 و 286 فقرة أولى ."

[5]– تنص المادة 355 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يجب أن يصدر الحكم في جلسة علنية ...".

[6]- تنص المادة 379 من قانون الإجراءات الجزائية الجزائري على ما يلي:" كل حكم يجب أن ينص على هوية الأطراف وحضورهم أو غيابهم في يوم النطق بالحكم، ويجب أن يشتمل على أسباب ومنطوق، وتكون الأسباب أساس الحكم ".

الحكم هو عمل عقلاني يسمح للقاضي بتفحص وسائل الإثبات بكل تمعن، وهو العملية الأساسية التي تسمح في إطار التدرج القضائي ممارسة الرقابة وكذا الطعون[1].

فلا يمكن بأي حال من الأحوال إنكار حجية الأدلة الإلكترونية، فهي أصبحت جزءا لا يتجزأ من طرق الإثبات باعتبارها أدلة تتناسب مع طبيعة الجريمة الإلكترونية التي ترتكب في بيئة تقنية خاصة، فالمبدأ السائد في التشريعات الحالية هو حرية القاضي في الإستناد إلى أي دليل من الأدلة التي يقتنع بحقيقتها وليس هناك مانع في استخدام الوسائل العلمية لمعرفة هذه الحقيقة، وإن كانت حجية الأدلة الإلكترونية تعتمد على العلم الذي بموجبه يتم الوصول إليها واستنتاجها وتقدير مدى صحتها وارتباطها بالقضية موضوع الدعوى، وللتأكد من صفة القائم على ذلك وإلمامه بعلوم الحاسب الآلي والإنترنت، كما تعتمد على الإطار القانوني الذي تتم من خلاله، والمتمثل في التقيد بالقواعد الإجرائية التي تنظم آلية التعامل مع الدليل ومشروعية إجراءات جمع الأدلة التي قد تم التطرق إليها في جميع مراحل هذا البحث.

ويبقى القاضي حر في وزن وتقدير كل دليل طرح أمامه، ولكن حريته في الإقتناع وتكوين عقيدته مقيدة بقيود خاصة أهمها:

1. أن تكون عقيدة القاضي واقتناعه قد استمدت من أدلة طرحت في الجلسة.

2. أن يكون اقتناع القاضي مبنيا على دليل مستمد من إجراء صحيح.

3. أن يكون اقتناع القاضي مبنيا على أدلة مستساغة عقلا، فينبغي أن يكون ما انتهى إليه القاضي في تكوين عقيدته هو أمر يكون الوصول إليه من الثابت في الأوراق، وما طرح من أدلة بالجلسة، وذلك وفقا لمقتضيات العقل والمنطق.

4. يجب أن يكون اقتناع القاضي مبنيا على اليقين[2].

وإن كان قد تم التطرق للإستثناءات التي ترد على حرية القاضي الجزائي، فهناك أيضا استثناءات ترد على مبدأ الإقتناع الشخصي، وهي تتمثل في أن القانون زود بعض المحاضر بقوة إثبات خاصة بحيث يعتبر المحضر حجة لما جاء فيه إلى أن يثبت ما ينفيه طبقا لنص المادة (216)[3] من قانون الإجراءات الجزائية الجزائري، كما أن هناك محاضر التي تحوز حجية إلى حين إثبات عدم صحتها بطريق الطعن بالتزوير،

---

[1] - د. محمد مروان، المرجع السابق، ج2، ص 498.

[2] – د.ناصر بن حمد البقمي، المرجع السابق، ص 41.

[3]- تنص المادة 216 من قانون الإجراءات الجزائية الجزائري على ما يلي:" في الأحوال التي يخول القانون فيها بنص خاص لضباط الشرطة القضائية وأعوانهم ... سلطة إثبات جنح في محاضر أو تقارير، تكون لهذه المحاضر أو التقارير حجيتها ما لم يدحضها دليل عكسي بالكتابة أو شهادة شهود ...".

ويترتب على ذلك أنها تقيد أكثر حرية القاضي الجزائي في الإقتناع، وتدخل المشرع بموجب قوانين خاصة لتنظيم هذا النوع من المحاضر[1]، وهذا ما نصت عليه المادة (218)[2] من قانون الإجراءات الجزائية الجزائري.

[1]– د. محمد مروان ، المرجع السابق، ص 485.

[2]- تنص المادة 218 من قانون الإجراءات الجزائية الجزائري على ما يلي:" إن المواد التي تحرر عنها محاضر لها حجيتها إلى أن يطعن فيها بالتزوير تنظمها قوانين خاصة ...".

الفصل الثاني : الآثار المترتبة على عدم مشروعية الدليل الالكتروني.

سبق وأن تبين طيلة مراحل البحث أنه يشترط في الدليل الجنائي بصفة عامة توافر شروط معينة تتمثل أساسا في المشروعية وضرورة أن تتسم عملية الحصول على الدليل بعدم وقوع أي إعتداءات على إرادة المتهم أو إرادة الغير، بحيث تكون طريقة الحصول عليه أو تقديمه أو تقديره خالية من أي عيب قد يشوب تلك الإرادة.

على أنّ الأمر لا يقف عند هذا الحد وذلك لضمان صحة الدليل وسلامته، بل قد يتعدى ذلك إلى درجة أنه بالرغم من خلو إرادة مصدر الدليل من أي عيب فإن ذلك لا يحتم بالقطع صحة الدليل وسلامته، وذلك بسبب ممارسة سلطة البحث عن الدليل أو تقديره لقدر من التعسف يخرجها عن نطاق الإطار السليم الواجب عليها مراعاة قواعده، مما يباعد بينها وبين إمكانية الوصول إلى درجة اليقين القضائي المطلوب أساسا للأحكام الجزائية[1].

ويعد الحق في حرمة الحياة الخاصة العمود الفقري للحرية الشخصية، و ركيزة أساسية لحقوق الإنسان و الحريات العامة، و تبعا لذلك يقتضي هذا الحق الإحترام من قبل السلطة و الأفراد، كما يقتضي في الوقت نفسه أن تكفل له السلطات الحماية الدستورية و القانونية ضد الإنتهاك غير المشروع، لكن الحق في حرمة الحياة الخاصة ليس حقا مطلقا بطبيعة الحال، بل تقيده اعتبارات المصلحة العامة، و بالتالي فإن المصلحة العامة هي التي ترسم حدود هذا الحق و تحدد نطاقه وفقا لمبدأ المشروعية[2].

وقد كانت حماية حقوق الإنسان وحياته الخاصة في مواجهة الوسائل العلمية موضع إهتمام المؤتمرات والإتفاقيات الدولية والإعلانات العالمية التي أكدت ضرورة احترام محل هذه الحقوق، ووضع القيود التشريعية الواضحة لمساندتها في مواجهة السلطة المطلقة للدولة، وكذلك اتجهت غالبية الدساتير الحديثة إلى تبني العديد من المبادئ التي من شأنها تحقيق هذه الحماية من خلال الحد من استخدام هذه الوسائل في مجال البحث عن الأدلة بوضع شروط على استخدامها حفاظا على حقوق وحريات الأفراد .

ولم يقف الأمر في النظم القانونية المختلفة عند حد الإعتراف الدستوري بحقوق الإنسان وضماناته الأساسية بل امتدت رعاية المشرع لتحيط تلك الحقوق بالحماية القانونية التي تكفل احترامها، فبدون هذه الحماية تبقى الضمانات المختلفة التي تقررها الدساتير لصيانة تلك الحقوق عديمة الجدوى غير محققة لغايتها،

[1] – د.أحمد ضياء الدين محمد، المرجع السابق ، ص509 .

[2]- د. يوسف الشيخ يوسف، حماية الحق في حرمة الأحاديث الخاصة، دار النهضة العربية، القاهرة، مصر، ط1، 1999، ص 192.

فالضمانات التي تحاط بها إجراءات البحث عن الأدلة يترتب على مخالفتها جزاءات تضمن لها الفعالية والجدية، ولاشك أن هذه القواعد أو الضمانات لا تحمي حريات الأفراد فحسب، وإنما هي ضرورية كذلك لتحقيق العدالة التي ينشدها المشرع.

وتختلف الجزاءات المترتبة على المساس بهذه الضمانات باختلاف مصدرها، فقد يكون مصدرها قانون الإجراءات الجزائية، فالقواعد الإجرائية تهدف إلى مراعاة تنظيم مباشرة الدعوى الجزائية وبيان الحدود التي تلتزم بها سلطة التحقيق ورسم السبل التي من خلالها يتمكن المتهم من الدفاع عن نفسه، لذلك يرتب المشرع على مخالفة هذه الإجراءات جزاء يتمثل في حرمان من باشر الإجراء المعيب من ترتيب الأثر القانوني للإجراء الذي باشره بالمخالفة لما تنص عليه القاعدة الإجرائية، فهو جزاء موضوعي الأثر لا ينال من شخص من باشر الإجراء وإنما يرد على العمل الإجرائي المخالف ذاته.

وقد يكون مصدرها قانون العقوبات في صورة جزاءات عقابية نتيجة التصرفات غير القانونية التي تتجاوز حدود صلاحيات سلطة التحقيق أثناء أدائها لواجبها، إذا نتج عنها جريمة ما سواء كان التصرف فعلا أم امتناعا، فهي جزاءات تنال من شخص من باشر الإجراء المخالف.

فالمشرع عندما يضع قواعد وينص على ضرورة مراعاتها لا يضع ذلك إعتباطا، وإنما يهدف من هذه القواعد حماية مصلحة المجتمع في معرفة الحقيقة، ويوازن بين ذلك ومصلحة المتهم في أن يعامل وفق أصل البراءة الكامن في نفسه، فإذا مارست الدولة حقها في العقاب بأدنى قدر من المساس بحريات الأفراد وبأكبر قدر ممكن الضمانات كان هذا دليلا على ديمقراطيتها الحقيقية[1].

وعلى هذا الأساس سيتم تقسيم هذا الفصل إلى مبحثين، أتطرق في المبحث الأول للجزاء الإجرائي المترتب على عدم مشروعية الدليل الإلكتروني، أمّا المبحث الثاني فخصص للجزاء الجنائي المترتب على عدم مشروعية الدليل الإلكتروني.

[1]- محمد أمين الخرشة، المرجع السابق، ص 212.

المبحث الأول : الجزاء الإجرائي المترتب على عدم مشروعية الدليل الإلكتروني.

الدعوى الجزائية هي مجموعة الأعمال الإجرائية التي تهدف إلى التحقق من وقوع الجريمة ونسبتها إلى فاعلها، وهي تشمل جميع الإجراءات التي تباشر منذ أول عمل من أعمال التحقيق حتى صدور حكم بات، وقد اشترط المشرع في كل عمل إجرائي ضرورة توافر شروط معينة لا يصح إلاّ بها، وهذا يعني أنّ الإجراء يجب أن يتم بالطريقة التي حددها القانون ومن قبل السلطة التي أناط بها هذا القانون اتخاذ الإجراء[1].

ووسيلة القضاء في الرقابة على الإجراءات الجزائية تكون من خلال حرمان من باشر الإجراء المعيب من ترتيب الأثر القانوني للإجراء الذي باشره بالمخالفة لما تنص عليه القاعدة الإجرائية، وهذه الأخيرة لا تحترم إلا بمقدار الجزاء المترتب على مخالفتها، والإعتداء على القاعدة الإجرائية غالبا ما يكون بإغفال القواعد التي تحقق مصلحة للمتهم وتغليب أهداف التحقيق على حقوق المتهم، ومن هنا تنبع أهمية الجزاء الإجرائي المتمثل في البطلان في حماية ضمانات المتهم[2].

فتعد نظرية البطلان من أهم موضوعات الإجراءات الجزائية لأنه موضوع عام يثار البحث فيه عند الكلام في كل قاعدة إجرائية ، وترجع أهمية البطلان كجزاء إجرائي إلى عدة أسباب أهمها ما يلي :

1. أنّ القاعدة الإجرائية شأنها في ذلك شأن أية قاعدة قانونية تحتوي على شقين، شق التكليف وشق الجزاء، فالأول يرسم الطريق الواجب على الأجهزة القضائية أن تسلكه للوصول إلى الحقيقة في الجرائم التي تقع ويجري تحقيقها، أما الشق الثاني فيتمثل في حرمان من باشر الإجراء المخالف للقانون من بلوغ الغاية التي يستهدفها الإجراء، فعنصر الجزاء هو الذي يكفل احترام قواعد الإجراءات الجزائية وكفالة حقوق المتهمين وحرياتهم وخاصة حق الدفاع.

إنّ تقرير البطلان يضمن الإلتزام بالقيود التي تحدد أسلوب التنقيب عن الدليل وأسلوب تقديمه باعتبار هذه القيود تمثل الإطار الذي يحكم اقتناع القاضي ويحول دون تحكمه، فإن تم مخالفتها كان محظورا عليه أن يستمد اقتناعه منها، فمشروعية الإجراء الكاشف عن الحقيقة المبتغاة هي التي كانت وراء استبعاد استخدام

[1]- د. محمد أمين الخرشة، المرجع السابق، ص 214.

[2]- د. سامي الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، دار النهضة العربية، مصر، بدون طبعة، سنة 1975، ص 397. نقلا عن : د. محمد أمين الخرشة، المرجع السابق، ص 214.

الوسائل التي تنطوي على مساس بحرية الشخص، فالشرعية الإجرائية هي قيد على حرية القاضي في تكوين عقيدته[1].

وسيتم التطرق لتعريف البطلان وطبيعة بطلان إجراءات جمع الدليل الإلكتروني وكذا الآثار المترتبة على ذلك، وهذا من خلال المطالب التالية:

المطلب الأول : تعريف البطلان والتمييز بينه وبين غيره من الجزاءات الإجرائية الجنائية.

إنّ الحديث عن البطلان يقتضي تحديد المقصود به والتمييز بينه وبين غيره من الجزاءات الإجرائية الجنائية وكذا أنواعه، وهذا ما سيأتي بيانه من خلال ما يلي :

الفرع الأول : تعريف البطلان.

هناك عدة تعاريف تتعلق بالبطلان، فيمكن تعريفه بأنّه جزاء إجرائي يلحق كل إجراء معيب وقع مخالفا للإجراءات المرسومة قانونا فيمنعه من أداء وظيفته، ويجرده من آثاره القانونية التي لا يمكن ترتيبها فيما لو وقع صحيحا[2].

وقد يعرف كذلك بأنه :"جزاء لتخلف كل أو بعض شروط صحة الإجراء ويترتب على ذلك عدم ترتيب الإجراء لآثاره"[3]، و قد قيل بأنه[4]: "جزاء إجرائي يرد على العمل الإجرائي فيمحو آثاره القانونية" .

فالبطلان جزاء يلحق إجراء نتيجة مخالفته أو إغفاله لقاعدة جوهرية في الإجراءات، يترتب عنه عدم إنتاجه لأي أثر قانوني، ولهذا فالإجراء يكون باطلا إمّا بسبب عدم توفره على العناصر اللازمة لصحته، أو لأنّ من قام به لا يملك الصفة والسلطة القانونية لمباشرته، أو أنّ إجراءا جوهريا تم إغفاله أو لم يتم القيام به حسب الشروط التي فرضها القانون أو أقرّها القضاء[5].

---

[1] – د.عبد الحفيظ نقادي، أحكام الإذن بالتفتيش في القانون الجنائي الجزائري، رسالة دكتوراه، كلية الحقوق، جامعة الجيلالي ليابس، سيدي بلعباس، الجزائر، سنة 2006، ص127.

[2] – د. سليمان عبد المنعم، بطلان الإجراء الجنائي (تأصيل أسباب البطلان في ظل قضاء النقض في مصر ولبنان وفرنسا)، الجامعة الجديدة للنشر، القاهرة، مصر، سنة 1999، ص 70.

[3] – د.محمود نجيب حسني ، المرجع السابق، ص330.

[4] – د.أحمد فتحي سرور، المرجع السابق ، ص107.

[5] – أ.أحمد الشافعي ، البطلان في قانون الإجراءات الجزائية (دراسة مقارنة)، دار هومة ، الجزائر، ط5 ، سنة 2007 ص 12.

ومن المقرر في التشريعات الحديثة أنّ البطلان هو الوسيلة العملية اللازمة لتحقيق سلامة العدالة وهيبتها في جميع مراحل الدعوى، فالجزاء في البطلان إجرائي يختلف عن غيره من الجزاءات، فهو أولا جزاء موضوعي لا ينال من شخص من باشر الإجراء وإنما يرد على العمل ذاته[1].

ولقد اتجهت التشريعات في تقريرها لبطلان العمل الإجرائي إلى الأخذ بإحدى النظريتين، هما نظرية البطلان القانوني ونظرية البطلان الذاتي، وإن كان لم يمنع بعض هذه التشريعات من الأخذ بالنظريتين السابقتين في تقرير بطلان العمل الإجرائي.

ويعني مذهب البطلان القانوني أنه "لا بطلان بغير نص" ، ومؤداه أن يقوم المشرع بتحديد حالات البطلان دون أن يترك للقاضي سلطة تقدير في هذا الشأن، وقد نص المشرع الجزائري على هذا النوع من البطلان صراحة في المادتين (100)[2] و(105)[3] من قانون الإجراءات الجزائية والمتعلقتين باستجواب المتهم وسماع الطرف المدني فقرر البطلان القانوني في المادة (157)[4] من قانون الإجراءات الجزائية.

وتبدو أهمية هذا النوع من البطلان أنه يحصر جميع حالات البطلان مما يؤدي إلى استقرار القضاء على حالات البطلان، إلاّ أنّ البطلان القانوني قد يؤخذ عليه أنه يحتوي على مساوئ، فالمشرع لا يمكنه أن يحصر على نحو جامع ودقيق كل الإجراءات والحالات التي يقضي فيها بالبطلان، بينما لا يستطيع المشرع أن يحيط سلفا بكل الأحوال التي تعتبر إخلالا باحترام الشرعية الإجرائية، ويترتب على ذلك إهدار هذه الضمانات[5].

---

[1] – د.عبد الحفيظ نقادي، المرجع السابق، ص 289.

[2]– تنص المادة 100 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يتحقق قاضي التحقيق حين مثول المتهم لديه لأول مرة من هويته، ويحيطه علما صراحة بكل واقعة من الوقائع المنسوبة إليه، وينبهه بأنه حر في عدم الإدلاء بأي إقرار ... كما ينبغي للقاضي أن يوجه المتهم بأن له الحق في اختيار محام عنه ... كما ينبغي للقاضي علاوة على ذلك أن ينبه المتهم إلى وجوب إخطاره بكل تغيير يطرأ على عنوانه ويجوز للمتهم اختيار موطن له في دائرة اختصاص المحكمة".

[3]– تنص المادة 105 من قانون الإجراءات الجزائية الجزائري على ما يلي:" لا يجوز سماع المتهم أو المدعي المدني أو إجراء مواجهة بينهما إلا بحضور محاميه، أو بعد دعوته قانونا ما لم يتنازل صراحة عن ذلك ... ".

[4]- تنص المادة 157 من قانون الإجراءات الجزائية الجزائري على ما يلي:" تراعى الأحكام المقررة في المادة 100 المتعلقة باستجواب المتهمين والمادة 105 المتعلقة بسماع المدعى المدني وإلا ترتب على مخالفتها بطلان الإجراء نفسه وما يتلوه من إجراءات .

ويجوز للخصم الذي لم تراع في حقه أحكام هذه المواد أن يتنازل عن التمسك بالبطلان ويصحح بذلك الإجراء، ويتعين أن يكون التنازل صريحا ولا يجوز أن يبدى إلا في حضور المحامي أو بعد استدعائه قانونا".

[5] – د.عبد الحفيظ نقادي، المرجع السابق، ص295.

أمّا مذهب البطلان الذاتي فمناطه هو طبيعة الإجراء، فإن كان جوهريا كانت مخالفته موجبة للبطلان، وإن كان غير ذلك لم تورث مخالفته البطلان، وفي ظل هذا المذهب يدع المشرع للقاضي سلطة تحديد ما يعد وما لا يعد جوهريا من الإجراءات.

فالمشرع الفرنسي قد هجر تقريبا نظرية البطلان القانوني، وكرس بصدور قانون 24 أوت سنة 1993 نظرية البطلان الذاتي، فوفقا للمادة (171)[1] من قانون الإجراءات الجزائية يتحقق البطلان عندما يترتب على إغفال إجراء جوهري منصوص عليه في قانون الإجراءات الجزائية أو أي نص إجرائي آخر مساس بحقوق الطرف الذي يتعلق به الإجراء، ولكن المشرع الفرنسي آثر الأخذ بمذهب البطلان القانوني في بعض حالات البطلان يهمنا منها في هذا الصدد، ما نصت عليه المادة (100-07) من قانون الإجراءات إذ قررت البطلان على مخالفة إجراءات التنصت وتسجيل المحادثات الهاتفية، ويلاحظ أنّ المشرع الفرنسي قد اشترط للحكم ببطلان إجراء ما بمقتضى نظرية البطلان أن يكون ثمة ضرر بمصالح الطرف الذي يتعلق به الإجراء وهكذا أصبح مفهوم الإضرار بمصالح الخصم ضابطا للبطلان.

ولقد أخذ المشرع المصري بمذهب البطلان الذاتي كأصل عام المواد (331-337) من ق.إ.ج فلم ينص على البطلان إلاّ في حالة واحدة هي عدم التوقيع على الحكم خلال ثلاثين يوما وذلك بمقتضى المادة (2/312)، أما فيما عدا ذلك فإنّ البطلان يترتب على عدم مراعاة أحكام القانون المتعلقة بأي إجراء جوهري المادة (331) من ق.إ.ج ويعني ذلك أنّ المشرع المصري يميز بين القواعد الإجرائية الجوهرية ويقرر البطلان جزاءا لمخالفة الأولى دون الأخرى[2].

أمّا بخصوص المشرع الجزائري فقد نصت المادة (159)[3] من قانون الإجراءات الجزائية على القواعد الجوهرية التي يترتب على مخالفتها البطلان، والمقصود بالإجراءات الجوهرية هي تلك الإجراءات التي يترتب على مخالفتها إلحاق الضرر بمركز أي خصم في الدعوى، مثل الإجراءات المتعلقة بالإنتقال للمعاينة والتفتيش المادة(79) من ق.إ.ج وسماع الشهود المادة (88) من ق.إ.ج والإستجواب والمواجهة المادة (100) من ق.إ.ج وتقابلها الإجراءات غير الجوهرية التي لا يترتب على مخالفتها أي ضرر للأطراف

---

[1] - Article 171 (C.P.P.F Modifié par Loi 93-1013 1993-08-24 art. 21 JORF 25 août 1993 en vigueur le 2 septembre 1993) : Il y a nullité lorsque la méconnaissance d'une formalité substantielle prévue par une disposition du présent code ou toute autre disposition de procédure pénale a porté atteinte aux intérêts de la partie qu'elle concerne.

[2] – د.عمر السعيد رمضان، شرح قانون العقوبات (القسم العام)، دار النهضة العربية ، القاهرة، مصر، بدون طبعة ، سنة 1991 ، ص40 وكذلك: د. محمود نجيب حسني، المرجع السابق، ص 340. نقلا عن: د. ياسر الأمير فاروق ، المرجع السابق، ص 703.

[3]– تنص المادة 159 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يترتب البطلان أيضا على مخالفة الأحكام الجوهرية المقررة في هذا الباب خلاف الأحكام المقررة في المادتين 100 و 105 إذا ترتب على مخالفتها إخلال بحقوق الدفاع أو حقوق أي خصم في الدعوى ...".

مثل :عدم ترقيم وجرد أوراق الملف بمعرفة كاتب التحقيق أولا بأول حسب تاريخ تحريرها أو ورودها لقاضي التحقيق مادة (68) من ق.إ.ج، إختيار شاهدين من غير أقارب المتهم عند تفتيش مسكنه المادة (83) من ق.إ.ج، عدم ذكر مهنة الشاهد[1].

فيثير الأخذ بمذهب البطلان الذاتي مشكلة تحديد القواعد الجوهرية والقواعد غير الجوهرية، فضابط التفرقة بين القواعد الجوهرية والقواعد غير الجوهرية يكمن في فكرة المصلحة، وهذا ما ألمحت إليه المذكرة التفسيرية لمشروع قانون الإجراءات الجنائية المصري، وذلك بقولها أنه لتعرف الأحكام الجوهرية يجب دائما الرجوع إلى علة التشريع، فإذا كان الغرض من الإجراء المحافظة على مصلحة عامة أو مصلحة تخص المتهم أو غيره من الخصوم فإنه يكون جوهريا، ويترتب على عدم مراعاة أحكامه البطلان، أمّا إذا كان الغرض من الإجراء مجرد الإرشاد والتوجيه فإنه لا يعتبر من الإجراءات الجوهرية[2].

وقد اعتبرت المحكمة العليا في الجزائر في إحدى قراراتها الصادرة في نوفمبر 1989 أن القواعد الشكلية تعد جوهرية عندما تمس بحقوق من يتمسك بها[3]، وعلى هذا الأساس يكون الإجراء جوهريا إذا كان يهدف إلى حماية حقوق الدفاع أو حقوق أطراف الدعوى الجزائية أو يرمي إلى حسن سير العدالة.[4]

الفرع الثاني : تمييز البطلان عن الجزاءات الإجرائية المشابهة له.

يعتبر البطلان أهم جزاء إجرائي يمكن أن يلحق إجراءا معينا، لذا أولاه كل من الفقه والقانون والقضاء عناية متميزة وخصه بنصوص تنظمه وأحكام تحدد وتعين مجال تطبيقه وحالات ترتيبه، غير أنّ هذا لا يعني وجود جزاءات أخرى تتشابه مع البطلان في ناحية وتختلف عنه من نواح أخرى كالسقوط وعدم القبول والإنعدام[5]، وذلك على النحو التالي:

البند الأول : التمييز بين البطلان والإنعدام.

إنّ أي إجراء أو تصرف قانوني يجب أن تتوافر فيه مجموعة من المقومات أو الأركان، فإذا انتفى ركن من أركان هذا الإجراء فجزاؤه الإنعدام، إذ أنّ العيب الذي لحق هذا الإجراء لا يقتصر على نفي أحد شروط صحته، بل قد تجاوز ذلك إلى نفي أحد عناصره أو أحد مقومات وجوده، مما يعتبر معه منعدما أي

---

[1]- أ. نجيمي جمال، المرجع السابق، ص 144.

[2] – د.ياسر الأمير فاروق، المرجع السابق، ص 704.

[3] – المجلة القضائية للمحكمة العليا، العدد الثاني ، سنة 1994 ، ص262، نقلا عن : د. عبد الحفيظ نقادي، المرجع السابق، ص 296.

[4] – نفس المرجع، ص 296.

[5]- أ. أحمد الشافعي، المرجع السابق، ص 13.

ليس له وجود قانوني، ويختلف عن الإجراء الباطل الذي يكون معيبا لاختلال شروط صحته، فهو موجود من الناحية القانونية ولكنه غير منتج للآثار القانونية[1].

ولذلك فإنّ الإجراء المنعدم والإجراء الباطل يوصف كل منهما بأنه إجراءا معيبا، إلاّ أنّ الإنعدام يفترض عيبا أشد جسامة مما يفترضه البطلان، لأنه يتعلق بنفي أحد أركان هذا الإجراء، أمّا العيب الذي ينتج عنه البطلان فإنّ الإجراء الذي لحقه مثل هذا العيب تكون أركانه وعناصره كاملة، إلاّ أنّ أحد شروط صحته قد اختل دون أن يصل هذا الإختلال إلى درجة تفقد الإجراء أحد أركان وجوده، هذا وبالإضافة إلى الفروق السابقة بين الإنعدام والبطلان فإنّ هناك فروقا تميز بين الإنعدام والبطلان بشكل أكثر وضوحا وهي :

- البطلان هو عدم صحة الإجراء فقط، بينما الإنعدام هو عدم الوجود.
- يترتب الإنعدام بقوة القانون بعكس البطلان الذي يحتاج إلى حكم من القضاء لتقريره.
- الإنعدام لا يقبل التصحيح لأنه لا وجود له أصلا، بينما الإجراء الباطل يجوز تصحيحه .
- الحكم المنعدم يظل منعدما حتى ولو فات ميعاد الطعن فيه، أمّا البطلان الذي شاب الحكم فإنه يلزم الطعن فيه في مواعيد الطعن المعتادة وإلاّ أصبح نهائيا[2].

ولذلك يلاحظ أنّ الراجح في الفكر القانوني الجنائي هو استبعاد الإنعدام والأخذ بنظرية البطلان جزاءا لمخالفة عناصر التفتيش ويبرر هذا ما يلي :

أولا: طبيعة التفتيش أنه إجراء تحقيق يخضع في نهاية الأمر إلى تقدير المحكمة، فلها أن تستمد منه الدليل متى كان صحيحا أو تستبعده متى كان باطلا أيا كان نوع البطلان، ومعنى ذلك أنه إذا كان التفتيش غير قانوني سواء لتخلف أحد شروطه فإنه يجب التقرير القضائي به دائما، وبذلك تصبح النتيجة التي يرتبها أنصار نظرية الإنعدام محل شك، ومن تم لا مبرر للتمسك في هذا المجال بنظرية الإنعدام لترتيب نتائج يمكن أن ترتبها نظرية البطلان.

ثانيا :إنّ نظرية الإنعدام تبرر في مجال الأحكام الجنائية، بل تعد أهم تطبيقاتها في هذا المجال، وعلى ذلك إذا استند الحكم الصادر بالإدانة على اعتراف ناتج عن تفتيش باطل، فمثل هذا الحكم يعتبر منعدما، فإذا لم يتمسك المتهم بهذا البطلان ولم تستظهره المحكمة من تلقاء نفسها، فإنّ هذا الحكم وإن حاز قوة الشيء

[1] – د. أحمد فتحي سرور ، المرجع السابق، ص 555، و كذلك : د. محمود نجيب حسني ، المرجع السابق، ص 356. نقلا عن : د.محمد أمين الخرشة، المرجع السابق، ص218.

[2] – نفس المرجع، ص 219.

المقضي فيه فلا يكون له وجود في الحقيقة، إذ لا يصح أن تكون الجريمة أساسا له ويكفي لانعدامه فقدان أساسه[1].

البند الثاني :التمييز بين البطلان والسقوط.

السقوط هو جزاء يترتب على عدم ممارسة الحق في مباشرة عمل إجرائي معين خلال المهلة التي حددها القانون، وتتحدد هذه المهلة إمّا بميعاد معين أو بواقعة معينة[2].

أمّا البطلان فهو عيب في الإجراء وبالتحديد في شروط صحته خلافا للسقوط الذي يفترض إجراءا صحيحا ولكنه لم يتخذ خلال الوقت الذي يتعين قانونا اتخاذه، وإنما بعد فوات الميعاد،كما أنّ البطلان يرد على الإجراء في ذاته في حين لا يرد السقوط عليه لأنه يفترض إجراء صحيحا وإنما يرد على الحق في مباشرته، ويرتبط بذلك أنّ الإجراء الباطل يجوز تجديده طالما أنّ الحق في مباشرته مازال باقيا، خلافا للسقوط الذي يفترض سقوط الحق في مباشرة الإجراء الأمر الذي لا يتصور معه تجديده[3].

ولنظرية السقوط مجالا للتطبيق أثناء التحقيق عندما ينص المشرع على فترة يكون للمتهم أو غيره من الخصوم خلالها تقديم بعض الطلبات، ومثال ذلك مواعيد إستئناف قرارات قاضي التحقيق، فإذا لم يتم الإستئناف خلال المدة المنصوص عليها في القانون يردّ الإستئناف لسقوط الحق في مباشرته، فانقضاء الفترة المحددة يسلب الفرد حقه أو سلطته في تنفيذ العمل المطلوب.

كما أنّ البطلان يقبل التصحيح في أحوال معينة ولو كان متعلقا بالنظام العام فيما إذا اكتسب الحكم قوة الشيء المقضي فيه، أمّا السقوط فلا يجوز تصحيحه في كافة الأحوال، والبطلان يتقرر أساسا بحكم أو بأمر بينما السقوط بقوة القانون[4].

وبهذا يتميز السقوط عن البطلان، فمن حيث موضوع الجزاء الإجرائي فإنّ السقوط ينصب إلى الحق في مباشرة الإجراء، في حين أنّ البطلان ينصب على الإجراء ذاته ويؤثر على فعاليته في إنتاج الآثار القانونية المعدة أصلا لإحداثها، ومن حيث القاعدة محل المخالفة فإنّ السقوط لا يكون إلاّ حيث تكون المخالفة المتعلقة بقاعدة تقرر ميعاد مباشرة الإجراء، في حين أنّ البطلان يكون عند مخالفة الإجراء لأية قاعدة جوهرية.

---

[1] – د.عبد الحفيظ نقادي ، المرجع السابق ،ص292.

[2] – د. عبد الفتاح الصيفي، النظرية العامة للقاعدة الإجرائية، منشأة المعارف، الإسكندرية، مصر، بدون طبعة، سنة 1986، ص 156. نقلا عن: د.محمد أمين الخرشة، المرجع السابق، ص219.

[3] – د. أحمد فتحي سرور، المرجع السابق، ص 584. نقلا عن: نفس المرجع، ص219.

[4] – أ.نبيل صقر ، البطلان في المواد الجزائية ، دار الهلال للخدمات الإعلامية ، الجزائر، بدون طبعة، سنة 2003 ، ص26. نقلا عن :د. عبد الحفيظ نقادي، المرجع السابق، ص 293.

ويتحقق البطلان والسقوط معا إذا بوشر العمل الإجرائي على الرغم من سقوط الحق أو السلطة في مباشرته، ويتحقق السقوط وحده إذا لم يباشر العمل الإجرائي بعد أن سقط ما لصاحبه من حق أو سلطة في مباشرته[1].

البند الثالث : التمييز بين البطلان وعدم القبول.

عدم القبول لا يعني أنّ العمل الإجرائي نفسه معيب بل قد يكون صحيحا، إنما هو جزاء إجرائي يرد على الدعوى الجنائية أو غيرها من طلبات الخصوم إذا لم تستوف أحد شروط تحريكها واستعمالها في بداية كل مرحلة من مراحل الخصومة، ومثال ذلك رفع الدعوى الجنائية دون تقديم الشكوى أو الطلب أو صدور الإذن في الحالات التي يتطلبها القانون.

وقد يتعلق عدم القبول بصفة المتهم، فلابد أن تتوافر صفة معينة فيه كصفة الزوج في جريمة الزنا وهي من الشروط الشكلية الواجب اتباعها قانونا، وقد يكون بسبب تخلف أحد الشروط الموضوعية كعدم جواز تحريك الدعوى نتيجة لسقوطها بالتقادم، لذلك فإن المحكمة تقضي بعدم قبول الدعوى إذا افتقدت إلى توافر شرط من الشروط الشكلية أو الموضوعية التي يستلزمها القانون.

ويبدو الشبه بين البطلان وعدم القبول في سبب كل منهما وهو عدم توافر شرط من شروط صحة العمل الإجرائي، أمّا الإختلاف فإنه يكمن في أنّ البطلان أوسع نطاقا من عدم القبول، لأنّ البطلان قد يصيب كل عمل إجرائي معيب وفي جميع مراحله سواء كان في مرحلة التحري أو في مرحلة التحقيق الإبتدائي أو في مرحلة المحاكمة.

بينما عدم القبول جزاء يقتصر على الدعاوى والطلبات وينحصر في رفض الطلب والدعوى، بالإضافة إلى أنّ البطلان يأتي أولا ثم يليه عدم القبول، فعدم القبول يفترض توافر عيب البطلان في الإجراء ولكن يظل هذا العيب كامنا ولا يكتشف إلاّ عند مباشرة الدعوى أو الطلب، لذا فإنّ البطلان جزاء يكون مع بداية العيب الإجرائي بينما عدم القبول جزاء لاحق ينبني على العيب السابق الذي أصاب الإجراء[2].

[1] – د.عبد الحفيظ نقادي، المرجع السابق، ص293.

[2] – أنظر في ذلك : د. أحمد فتحي سرور، المرجع السابق، ص 587. و د. محمود نجيب حسني، المرجع السابق، ص 358. نقلا عن: د.محمد أمين الخرشة، المرجع السابق، ص220.

ويجوز تجديد الإجراء الذي قضي بعدم قبوله إذا توافر الشرط الإجرائي الذي كان منتفيا وكان الحق في اتخاذه ما يزال قائما، فإذا قضي بعدم قبول الدعوى لعدم تقديم شكوى ثم قدمت الشكوى في خلال المهلة التي يقررها القانون كانت الدعوى بعد ذلك مقبولة[1].

الفرع الثالث : أنواع البطلان.

يفترض البطلان في كل أحواله إجراءا جوهريا خولفت أحكام القانون المتعلقة به، فإن لم يكن الإجراء جوهريا فلا بطلان ولو خولفت الأحكام التي وضعت لتنظيمه، على أنّ الفقه درج على تقسيم البطلان إلى أنواع عدة فهناك تقسيم البطلان إلى شكلي وموضوع[2]، وهناك تقسيم البطلان إلى عام وخاص [3]، على أنّ أهم تقسيمات البطلان هو البطلان المطلق والبطلان النسبي لما يترتب على هذا التقسيم من أهمية كبيرة من حيث الآثار العلمية المترتبة عليه، وقد جرى العمل على إطلاق وصف المطلق على البطلان المتعلق بالنظام العام ووصف النسبي على البطلان المتعلق بمصلحة الخصوم، ويرى بعض الفقهاء[4] أنّ ما يجري عليه العمل في هذا الشأن لا ضرر منه، لأنّ معيار النظام العام هو السائد في تمييز البطلان المطلق عن النسبي، كما أنّ البطلان المطلق يلتقي مع البطلان المتعلق بالنظام العام في خصائصه الرئيسية[5].

البند الأول : البطلان المطلق.

يعرف الفقه البطلان المطلق بأنه البطلان المترتب على مخالفة القواعد الخاصة بالإجراءات الجوهرية المتعلقة بالنظام العام،كما اختلف الفقهاء في بيان الضابط الذي يتحدد على أساسه مدى تعلق القاعدة بالنظام العام، فذهب رأي[6] إلى أنّ هذا الضابط يتمثل في نوع المصلحة التي تحميها القاعدة الإجرائية فإذا كانت مصلحة عامة كان البطلان المترتب على مخالفتها متعلقا بالنظام العام، وإن كانت خاصة بالخصوم

---

[1] – د.محمد أمين الخرشة، المرجع السابق ، ص221.

[2] – ويكون البطلان شكليا إذا كان راجعا إلى مخالفة الشروط الشكلية لصحة العمل الإجرائي، ويكون موضوعيا إذا كان راجعا إلى مخالفة الشروط الموضوعية في هذا العمل. أنظر في ذلك: د. أحمد فتحي سرور، المرجع السابق، ص139.نقلا عن: د. ياسر الأمير فاروق، المرجع السابق، ص 705.

[3] – يكون البطلان عاما إذا كان المشرع قد جعله جزاءا لمخالفة طائفة معينة من القواعد أضفى عليها صفة معينة دون أن ينص على البطلان بصدد كل قاعدة، أما البطلان الخاص فهوا لبطلان الذي ينص عليه المشرع بصدد إجراءات معينة. أنظر في ذلك: د.مأمون سلامة ، المرجع السابق ، ص345. نقلا عن: نفس المرجع ، ص 705.

[4] – د.رؤوف عبيد، المرجع السابق ،ص122.نقلا عن: نفس المرجع، ص 706.

[5] – نقلا عن :نفس المرجع ،ص706.

[6] – د.عمر السعيد رمضان ، المرجع السابق ، ص43. نقلا عن: نفس المرجع، ص 706.

كان البطلان غير متعلق بالنظام العام، وذهب رأي ثان[1] إلى أنّ الضابط الصحيح هو أهمية المصلحة المحمية بغض النظر عما إذا كانت عامة أو خاصة بخصوم الدعوى وقاضي الموضوع هو الذي يقدر أهمية المصلحة في كل حالة على حدى، وذهب رأي ثالث[2] إلى أنّ الضابط المعول عليه هو مدى قابلية الحق الذي تحميه القاعدة الإجرائية للتصرف فيه، فإذا كان الحق لا يقبل التصرف فيه فإنّ البطلان يكون متعلقا بالنظام العام[3].

غير أنّ قانون الإجراءات الجزائية الجزائري لم يشر في نصوصه لا إلى البطلان المطلق ولا إلى البطلان المتعلق بالنظام العام، في حين أنّ قضاء المحكمة العليا يستعمل في قراراته مصطلح البطلان المتعلق بالنظام العام بدلا من البطلان المطلق[4].

البند الثاني : البطلان النسبي.

إذا كان البطلان المتعلق بالنظام العام يرمي إلى حماية المصلحة العامة للمجتمع، فإنّ البطلان المتعلق بمصلحة الأطراف قد وضع لحماية مصلحة أطراف الدعوى والمحافظة عليها وتقرير ضمانات لها، وعليه فهو كل بطلان ليس متعلقا بالنظام العام .

فيبقى المعيار أو الضابط الذي يعتمد عليه لتقرير البطلان المتعلق بمصلحة الأطراف هو معيار المصلحة، فالمصلحة المحمية هي التي تحدد حالات البطلان المتعلقة بمصلحة الأطراف وأنّ القضاء هو الذي يقدر أنّ الإجراء الجوهري المخالف يمس بالمصلحة الخاصة لأطراف الدعوى الجزائية، ويترتب على الضرر اللاحق بها البطلان المتعلق بمصلحة الأطراف أو البطلان النسبي[5].

وتختلف الآثار المترتبة على البطلان النسبي عن تلك التي تترتب على البطلان المطلق، ففي حالة كون البطلان نسبيا لا يجوز لغير ذي الشأن التمسك به، بينما في البطلان المطلق لكل ذي مصلحة أن يتمسك به، ومن حيث التمسك بالبطلان يحق لصاحب الشأن التنازل عنه صراحة إذا كان البطلان نسبيا بينما لا يجوز له ذلك إذا كان البطلان مطلقا.

---

[1] – د.فوزية عبد الستار، شرح قانون العقوبات ، دار النهضة العربية القاهرة، مصر، بدون طبعة ، سنة 1990،ص35. نقلا عن: د.ياسر الأمير فاروق، المرجع السابق ، ص707.

[2] – د.عوض محمد عوض، المرجع السابق، ص47. نقلا عن: نفس المرجع ، ص707.

[3] – نقلا عن: د.ياسر الأمير فاروق، المرجع السابق ، ص707.

[4] – أنظر قرار صادر يوم 07 ديسمبر 1982 تحت طعن رقم 29815 نقلا عن: د.عبد الحفيظ نقادي، المرجع السابق، ص299.

[5] – د.أحمد الشافعي، المرجع السابق ،ص61.

وفي حالة البطلان النسبي لا يجوز للمحكمة أن تقضي به من تلقاء نفسها، بل لابد من أن يتمسك به أحد الخصوم وأن يكون هذا الخصم هو ممن قررت القاعدة لمصلحته، بينما في البطلان المطلق يجوز لها القضاء بالبطلان من تلقاء نفسها ولو بغير طلب مع تعلق ذلك البطلان بالنظام العام، كما أنه لا يجوز التمسك بالبطلان النسبي أمام المحكمة العليا لأول مرة بل يجب أن يتمسك به أمام محكمة الموضوع، أمّا بالنسبة للبطلان المطلق فيجوز التمسك به في جميع مراحل الدعوى ولو أمام المحكمة العليا لأول مرة[1].

إلاّ أنّ أهم ما يميز البطلان النسبي عن البطلان المطلق هو أن الأول قابل للتصحيح وتصحيح البطلان النسبي يكون بطريقتين[2] :

الأولى : هو القبول الصريح أو الضمني للإجراء الباطل من قبل من تقرر البطلان لمصلحته، فمثلا يسقط الحق في الدفع ببطلان الإجراءات الخاصة بجمع الاستدلالات أو تحقيق الابتدائي إذا تم الإجراء بوجود المتهم بدون اعتراض منه.

الثانية :هو تحقيق الغرض من الإجراء الباطل وهو يتم عن طريق التصرف أو القيام بإجراء لاحق من شأنه أن يعدم أثر البطلان في الإجراء، مثلا بطلان التكليف بالحضور له أن يطلب تصحيح التكليف أو استيفاء أي نقص فيه وإعطائه ميعادا لتحضير دفاعه قبل البدء في سماع الدعوى وعلى المحكمة إجابته على طلبه.

المطلب الثاني :طبيعة بطلان إجراءات جمع الدليل الإلكتروني.

إنّ البطلان كجزاء إجرائي يلحق الإجراءات التي تتم خلال مراحل الدعوى الجزائية فيعيبها لأنها لم تتم حسب النموذج القانوني للإجراء أو أنها خالفت قاعدة جوهرية، مما يجعل الإجراء لا يؤدي وظيفته ولا يرتب الأثر المبتغى منه[3]، وسأتطرق من خلال هذا المطلب لطبيعة بطلان الإجراءات العامة لجمع الدليل الإلكتروني وذلك في الفرع الأول، أمّا الفرع الثاني فسيخصص لطبيعة بطلان الإجراءات الخاصة لجمع الدليل الإلكتروني.

[1]- د. عبد الحفيظ نقادي، المرجع السابق، ص 299.

[2] – أ.نبيل صقر، البطلان في المواد الجزائية، المرجع السابق ،ص72. نقلا عن : د. عبد الحفيظ نقادي، المرجع السابق، ص 299.

[3] – أ. أحمد الشافعي ،المرجع السابق ،ص65.

الفرع الأول : طبيعة بطلان الإجراءات العامة لجمع الدليل الإلكتروني.

من باب المقارنة يلاحظ أنّ قانون الإجراءات الجزائية الفرنسي في المادة (170)[1] منه قد سمح لغرفة الإتهام بإبطال كل إجراء أو وثيقة دون تمييز بين أعمال الضبطية القضائية وأعمال التحقيق، كما أنّ قانون الإجراءات الجنائية المصري ينص في المادة (333) منه على أنه:" في غير الأحوال المشار إليها في المادة السابقة (البطلان المتعلق بالنظام العام) يسقط الحق في الدفع ببطلان الإجراءات الخاصة بجمع الإستدلالات أو التحقيق الإبتدائي أو التحقيق بالجلسة في الجنح والجنايات إذا كان للمتهم محام وحصل الإجراء بحضوره بدون اعتراض منه.

أمّا في مواد المخالفات فيعتبر الإجراء صحيحا إذا لم يعترض عليه المتهم ولو لم يحضر معه محام في الجلسة وكذلك يسقط حق الدفع بالبطلان بالنسبة للنيابة العامة إذا لم يتمسك به في حينه".

وبذلك يبقى أمام المعني بالأمر في ظل أحكام قانون الإجراءات الجزائية أن يبرز العيوب التي شابت أعمال الضبطية القضائية أمام غرفة الإتهام أو أمام جهة الحكم بهدف كشف بطلانها لمخالفتها للقانون والتشكيك في مصداقيتها وطلب استبعادها، دون أن تستطيع هذه الجهات أن تصرح ببطلانها لانعدام السند القانوني، وإنما تبرز العيب الذي يشوبها وتقرر استبعادها، ماعدا إذا نص القانون صراحة على بطلان إجراء محدد إذا خالف القانون كحالة بطلان الإذن بالتفتيش وكحالة بطلان إجراءات التفتيش إذا كانت هناك مخالفة لأحكام المادتين (45) المتعلقة بكيفية التفتيش و(47) المتعلقة بوقت التفتيش بصريح نص المادة (48) من قانون الإجراءات الجزائية، وما نصت عليه أحكام الفقرة الثانية من المادة (65 مكرر 12) الخاصة بأحكام التسرب من أنه: "يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة أو أن يرتكب عند الضرورة الأفعال المذكورة في المادة (65 مكرر 14) أدناه، ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضا على ارتكاب الجرم"، ووجوب تسبيب الإذن بالتسرب حسب نص المادة (65 مكرر 15) وهذه هي الحالات الوحيدة التي نص فيها المشرع على بطلان أعمال الضبطية القضائية[2].

أمّا مرحلة التحقيق القضائي فهي مرحلة أساسية في الدعوى الجزائية، فهي تمتاز بتنوع وتعدد الإجراءات التي تتم خلالها، وقد أحاط المشرع الكثير من هذه الإجراءات بضمانات وشكليات معينة قد تم التطرق إليها بالتفصيل في الباب الأول .

---

[1] - Article 170 (C.P.P.F Modifié par Loi n°2004-204 du 9 mars 2004 - art. 95 JORF 10 mars 2004 en vigueur le 1er octobre 2004) :En toute matière, la chambre de l'instruction peut, au cours de l'information, être saisie aux fins d'annulation d'un acte ou d'une pièce de la procédure par le juge d'instruction, par le procureur de la République, par les parties ou par le témoin assisté.

[2] - أ. نجيمي جمال، المرجع السابق، ص 142.

وعلى هذا الأساس فالتحقيق القضائي هو عبارة عن إجراءات طويلة ومتشعبة، ومن هذا المنطلق يقوم قاضي التحقيق عند مباشرته لمهمته من أجل البحث والوصول إلى الحقيقة بعدة إجراءات قانونية كاستجواب الأشخاص الذين يمكنهم تقديم معلومات ذات فائدة للتحقيق، مثل المتهمين والضحايا والأطراف المدنية في حالة تأسيسهم كذلك والشهود أو تفتيش المنازل وحجز الأشياء وإصدار أوامر القضاء وتعيين خبراء للقيام بإنجاز خبرات وإعطاء إنابات قضائية[1].

وسيتم التطرق إلى بطلان الإجراءات على النحو التالي:

أولا :بطلان التفتيش في البيئة الإلكترونية.

لقد نظم المشرع الجزائري قواعد وإجراءات التفتيش والحجز والجزاءات المترتبة عن مخالفتها في المواد (44 إلى 49) والمادة (64) ومن المواد (79 إلى 85) من قانون الإجراءات الجزائية وقد نصت المادة (48)[2] على أنّ عدم مراعاة الإجراءات التي استوجبتها المادتان (45 و47) من هذا القانون يترتب عنها البطلان، وبالتالي فإنّ أي تفتيش يقوم به ضابط الشرطة القضائية بالمخالفة لأحكام المواد (44، 45 و47)يقع باطلا، أي أنّ مخالفة القيود المتعلقة بالحضور ووقت التفتيش والإذن من السلطة القضائية المختصة يترتب عليها البطلان ، وإن كان قيد إحترام الوقت والقيد المتعلق بالحضور لا يطبق في حالة التحري حول الجرائم المنصوص عليها في المادة (47) من قانون الإجراءات الجزائية ومن بينها الجرائم الإلكترونية.

وتجدر الإشارة إلى أنّ هذا البطلان هو بطلان نسبي متعلق بمصلحة الأطراف تطبق عليه جميع القواعد التي تطبق على البطلان النسبي وهو في نفس الوقت بطلان قانوني إذ نص عليه المشرع صراحة، ويترتب على كون مخالفة أو عدم مراعاة قواعد وإجراءات التفتيش والحجز المنصوص عليها في المادتين (45) و(47) البطلان النسبي المتعلق بمصلحة الأطراف، أي أنه لا يجوز التمسك ببطلان التفتيش أو الحجز أو التنازل عنه إلاّ لمن قررت الأحكام لمصلحته، فهو بالتالي ليس بطلانا مطلقا لعدم تعلقه بالنظام العام وأنّ المصلحة التي يحميها هي مصلحة شخصية[3].

---

[1] – أ. أحمد الشافعي، المرجع السابق، ص67. وفي نفس المعنى:

Gaston stefani, Georges levasseur, Bernard Bouloc, Procédure pénale,16éme édition, Dalloz, France ,1996, p20.

[2]– تنص المادة 48 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يجب مراعاة الإجراءات التي استوجبتها المادتان 45 و 47 ويترتب على مخالفتها البطلان ".

[3]- د. فتحي والي، نظرية البطلان في قانون المرافعات، رسالة دكتوراه، جامعة القاهرة، مصر، سنة 1988، ص 498.نقلا عن : أحمد الشافعي ، المرجع السابق، ص130.

وهو نفس الموقف الذي أخذت به المحكمة العليا في قرارها بتاريخ 27 جانفي 1987 الغرفة الجنائية الأولى طعن رقم 22147، حيث قضت بأنّ الدفع ببطلان التفتيش هو من المسائل الموضوعية التي يجب عرضها على قضاة الموضوع وإلاّ سقط الحق في إثارتها لأول مرة أمام المحكمة العليا، ولا يجوز الدفع ببطلان التفتيش إلاّ من شخص المتهم الذي قررت القاعدة المخالفة لمصلحته، فليس لغيره ولا النيابة العامة التمسك بهذا الحق[1].

وبناءا على ذلك يجب التمسك به أمام قضاة الموضوع ولا يجوز لقضاة الحكم القضاء به من تلقاء أنفسهم، كما يجوز لمن قررت القاعدة المخالفة لمصلحته التنازل عنه صراحة أو ضمنا مما يؤدي إلى تصحيح التفتيش المشوب بهذا العيب، كما أنّ عدم الدفع به يصحح ما وقع من إجراءات باطلة وأنّ الحكم ببطلان التفتيش يترتب عنه بطلان الأدلة المستقاة منه، ولا يلحق هذا البطلان الإجراءات الصحيحة التي تمت قبل التفتيش الباطل[2].

أمّا القانون المصري فقد اعتبر أنّ البطلان الذي يلحق مخالفة الأحكام التي تنظم التفتيش والحجز هو بطلان نسبي فقد نصت المادة (333) من قانون الإجراءات الجنائية المصري على سقوط الحق في الدفع ببطلان الإجراءات الخاصة بالتحقيق الإبتدائي، ومنها بطبيعة الحال التفتيش والحجز إذا كان للمتهم محام وحصل الإجراء بحضوره دون إعتراض منه[3].

---

[1] – أ.أحمد الشافعي، المرجع السابق، ص104.

[2]– د. عبد الحميد الشواربي، ضمانات المتهم في مرحلة التحقيق الجنائي، منشأة المعارف، الإسكندرية، مصر، بدون طبعة، سنة 1993، ص 212 . وكذلك: د. مأمون محمد سلامة، المرجع السابق، ص 436. نقلا عن: أ. أحمد الشافعي، المرجع السابق، ص 104.

[3] – هذا وإن كانت النصوص المتعلقة بالبطلان قد أثارت خلافا في الفقه المصري حول طبيعته، فذهب بعض الفقهاء ومنهم الدكتور "رؤوف عبيد" أنّ قانون الإجراءات الجنائية قد اعتبر القواعد الجوهرية في التفتيش مما يتعلق بمصلحته المتهم أو غيره من الخصوم في الدعوى وأنّ مخالفة هذه القواعد ترتب البطلان النسبي في جميع الأحوال.

في حين هناك رأي آخر يرى أنّ نوع بطلان التفتيش هو بطلان مطلق يتعلق بالنظام العام إلاّ في حالة واحدة هي عدم حضور شاهدين في التفتيش الذي يجريه ضابط الشرطة القضائية إذا لم يكن المتهم حاضرا أو من ينيبه عنه، وإزاء النقد الموجه لهم لجأ أصحاب هذا الرأي إلى العدول عنه ولجأوا إلى تحديد حالات بطلان التفتيش الذي يتعلق بالنظام العام، وذلك في الحالات التالية :

- إذا صدر التفتيش في دعوى جنائية لم تحرك تحريكا صحيحا، كما لو اشترط فيها القانون تقديم شكوى ولم يحترم هذا القيد.
- إذا صدر التفتيش مخالفا لقواعد الإختصاص.
- عدم حضور المتهم أو من ينيبه عنه متى أمكن ذلك .

وإن كان هناك رأي آخر يفرق بين القواعد الموضوعية والشكلية فيترتب على بطلان القواعد الموضوعية بطلان مطلق وعلى القواعد الشكلية بطلان نسبي، فالقواعد الموضوعية تعتبر من مقومات وجود الحق في مباشرته وعدم وجودها يعني عدم شرعية الإجراء ووجودها ينفي على الإجراء شرعية قانونية، أمّا بالنسبة للقواعد الشكلية فيكون الإجراء صحيحا إذا أقره الصادر لصالحه الحق في حماية نفسه أو مسكنه أو تنازل عن التمسك بالبطلان صراحة أو ضمنا أمام محكمة أول درجة .أنظر في ذلك: د.عبد الحفيظ نقادي، المرجع السابق، ص309.

أمّا بالنسبة للقانون الفرنسي فقد اعتبر البطلان المترتب عن مخالفة إجراءات التفتيش والحجز بطلانا نسبيا متعلقا بمصلحة الأطراف[1]، فقد نصت المادة (2/59)[2] من قانون الإجراءات الجزائية الفرنسي على مراعاة الإجراءات المشار إليها في المواد (56) ،(57) وفي المادة (59) تحت طائلة البطلان، ويتعلق الأمر بالبطلان النسبي وهو في نفس الوقت بطلان قانوني بصريح نص المادة (02/59) ،كما ترى محكمة النقض الفرنسية أنه يصعب تحديد حالات بطلان التفتيش المتعلقة بالنظام العام وتلك المتعلقة بمصلحة الأطراف مسبقا، وإن كانت محكمة النقض الفرنسية إعتبرت في حكمين لها صادرين عن الغرفة الجنائية بتاريخ 1961/04/14 و1961/12/14 أنّ الحجز الذي يتم إثر تفتيش باطل لا يتضمن مساسا بحقوق الدفاع طالما أنّ الأشياء المحجوزة قد نوقشت بحرية أمام المحكمة[3].

أمّا محكمة النقض المصرية فقد أخذت بموقف يخالف ما ذهبت إليه محكمة النقض الفرنسية، إذ رفضت الدليل المستمد من تفتيش باطل وذلك في حكمين لها مؤرخين في 1934/12/27 ، هذا وإن كانت قد أجازت لقضاة الموضوع الأخذ بهذا الدليل في حالة الحكم بالبراءة[4].

و يقول الفقه بشأن طبيعة التفتيش في نظم الحاسب الآلي أنّ هذه الطبيعة لا تختلف عن سابقتها في البيئة التقليدية نظرا لأوجه التماثل التي تم ملاحظتها على مدار هذا البحث، بالإضافة إلى التداخل بين أحكامها وخاصة بالنسبة لتفتيش المساكن أو العقار التي تتواجد فيها الحاسبات الآلية، وكذا تحديد الإذن .

ثانيا : بطلان الشهادة.

أداء اليمين هو من أهم الضمانات التي تضفي الثقة على الشهادة، و لكي تكون دليلا يعتد به وتجعل الشاهد يخضع لضميره في قول الحق، و يتجنب الكذب أو تحريف الشهادة، فالشاهد الذي يدلي بشهادته دون أداء اليمين تعتبر هذه الشهادة باطلة، فأداء اليمين هو إجراء من النظام العام و بدونه يبطل كل أثر يترتب عن الشهادة[5].

---

[1] - Bernard Bouloc, Gaston Stefani et George Levasseur, OP.cit, P 320. نقلا عن: أحمد الشافعي، المرجع السابق، ص102

[2] - Article 59/02 (C.P.P.F Modifié par Loi 93-1013 1993-08-24 art. 20 JORF 25 août 1993 en vigueur le 2 septembre 1993) :…Les formalités mentionnées aux articles 56, 56-1, 57 et au présent article sont prescrites à peine de nullité.

[3] - Crim 14 Avril 1961, Bull 299 : 14 dec 1961. Bull. 528.

نقلا عن: أ. أحمد الشافعي، المرجع السابق ، ص 104.

[4] - نفس المرجع، ص 104.

[5] – د. بلعليات ابراهيم، المرجع السابق، ص 203.

كما يمكن الدفع ببطلان الشهادة في الحالات التالية :

- سماع القصر وأدائهم اليمين القانونية.
- سماع أحد أقارب المتهم وأصهاره.
- عدم أداء الشاهد لليمين القانونية وعدم إمضائه لمحضر الشهادة.
- أداء الشهادة تحت تأثير الإكراه المادي والمعنوي[1].

ومن الحالات التي لا يجوز فيها سماع الشخص كشاهد، حالة وجود شخص تقوم ضده دلائل قوية ومتماسكة على قيام إتهام في حقه، كأن يتبين أنه يشارك في الوقائع الملاحق بها الأشخاص المتهمين في نفس القضية، وهو ما نصت عليه الفقرة الأخيرة من المادة 89 من قانون الإجراءات الجزائية الجزائري، وكذلك إذا كان الشخص المراد السماع لشهادته قد وجهت ضده شكوى مصحوبة بإدعاء، وقد رفض سماعه كشاهد عند تبليغ الشكوى إليه طبقا لأحكام المادة 73 من قانون الإجراءات الجزائية الجزائري، و الحالة الأخيرة إذا كان ادعى الشخص مدنيا، فلا يجوز عندئذ سماعه كشاهد طبقا لنص المادة 243 من نفس القانون[2].

ومن الأسباب التي تؤدي إلى النقض والبطلان عدم ذكر مضمون شهادة الشاهد بالحكم القاضي بالإدانة، لأنه لا يفسح المجال لمحكمة النقض مراقبة تطبيق القانون تطبيقا صحيحا[3].

واستنادا إلى رأي غالبية الفقهاء، و فيما يخص النقطة المتعلقة بأداء الشهادة تحت تأثير الإكراه المادي والمعنوي، فتم في الباب الأول استخلاص أنه وفقا للقواعد العامة في الشهادة لا يستلزم الشاهد إلاّ بذكر ما يعلمه، ولا يجوز إجباره على القيام بسلوك معين.

ولهذا يلاحظ أنّ كثير من التشريعات تلزم الشاهد بتقديم ما يعرفه عن الجريمة وليس القيام بعمل معين، أي أن الشاهد يلتزم فقط بالإجابة عن الأسئلة التي توجهها له المحكمة وليس لها أن تلزمه بالقيام بعمل معين، معنى ذلك ليس للشاهد أن يقوم بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة لأن ذلك يخرج عن نطاق الوقائع محل الشهادة، فليس من التزامات الشهادة بمفهومها التقليدي أن يتعاون الشاهد مع سلطات التحقيق تعاونا فعالا.

---

[1] – أ.بلعليات إبراهيم ،المرجع السابق، ص206.

[2] – د. محمد حزيط، المرجع السابق، ص 114.

[3] – أ. بلعليات إبراهيم، المرجع السابق، ص 206.

إلاّ أنّه في الواقع، تبقى القواعد العامة التقليدية للشهادة عاجزة عن فرض مثل هذا الإلتزام على الشاهد المعلوماتي، وهذا ما يؤكد أهمية وجود قواعد خاصة في مجال الجريمة الإلكترونية تتعلق بضرورة فرض واجب التعاون مع الجهات القضائية أثناء التحقيق والمحاكمة على الشاهد المعلوماتي، وذلك بإيجاد آليات تعاون فعالة ما بين الشهود وسلطات التحقيق على وجه الخصوص فيما يتعلق بإتاحة المعلومات في صورة يمكن استخدامها كدليل إثبات أمام القضاء، وفي هذا الصدد يرى الدكتور "هلالي عبد اللاه أحمد" أنّه نتيجة لقصور أحكام الشهادة في الحصول على الدليل الإلكتروني كان لابد من البحث عن وسيلة قانونية جديدة تحقق ما لم تستطع فكرة الإلتزام بأداء الشهادة أن تؤديه وهذه الوسيلة هي:"الإلتزام بالإعلام في الجريمة المعلوماتية".

ثالثا : بطلان الخبرة التقنية.

تعد جميع الإجراءات التي نصت عليها المادة (144) وما بعدها من قانون الإجراءات الجزائية الجزائري وتقابلها المادة (157) وما بعد ها من قانون الإجراءات الجزائية الفرنسي إجراءات جوهرية، حيث أنها تضمن قيمة الخيرة وأنّ القواعد التي نصت عليها هذه المواد الخاصة بتعيين الخبراء تعتبر من النظام العام.

وقد اعتبر القضاء أنّ تعيين خبير غير مسجل في قائمة الخبراء بأمر غير مسبب يترتب عنه البطلان[1]، كما أنّ عدم مراعاة أحكام المادة (151 فقرة 3)[2] من قانون الإجراءات الجزائية المتعلقة باستجواب المتهم يترتب عنه بطلان من نوع البطلان الذي يلحق مخالفة أحكام المادة (105) من قانون الإجراءات الجزائية، حيث يمتد هذا البطلان إلى إجراءات التحقيق اللاحقة لهذا الإستجواب، ويتعرض القرار الذي أشار واستند إلى خبرة مشوبة بالبطلان إلى البطلان ويجب نقضه سواء تعلق الأمر بقرار إحالة أمام جهة قضائية للحكم صادر عن غرفة الإتهام أو قرار إدانة، غير أنه يجب إثارة الوجه المتعلق ببطلان الخبرة والتمسك به في الوقت المناسب، ذلك أنّ طابع النظام العام للبطلان الذي يلحق الخبرة المرتبطة بإدارة العدالة ليس بالدرجة التي تسمح بإمكانية إثارة هذا البطلان لأول مرة أمام المحكمة العليا حتى ولو كان العيب الذي يلحق الخبرة هو إغفال أداء الخبير لليمين[3].

---

[1] - Crim 20 déc 1983, Bull.Crim N° 350-6 mars 1984. Bull. Crim N° 90.

نقلا عن : أ. أحمد الشافعي، المرجع السابق، ص 114.

[2]- تنص المادة 151 فقرة 3 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يجوز للخبراء على سبيل المعلومات وفي الحدود اللازمة لأداء مهمتهم أن يتلقوا أقوال أشخاص غير المتهم... وإذا رأوا محلا لاستجواب المتهم، فإن هذا الإجراء يقوم به بحضورهم قاضي التحقيق أو القاضي المعين من المحكمة على أن تراعى في جميع الأحوال الأوضاع والشروط المنصوص عليها في المادتين 105 و 106 ...".

[3]- أ. أحمد الشافعي، المرجع السابق، ص 144.

وقد اعتبرت محكمة النقض الفرنسية أنّ للمبادئ العامة للخبرة طابع النظام العام وبناءا عليه قضت ببطلان الخبرة لعدم مراعاة القاعدة التي تفرض تأدية الخبراء لليمين أمام قاضي التحقيق[1]، دون إثبات أنّ طرفا ما قد لحقه ضرر من جراء ذلك وهي تعطي نفس القيمة للقاعدة التي تفرض تأدية المترجمين لليمين[2].

كما ترى محكمة النقض الفرنسية أنه في مادة الجنح فإنّ بطلان الخبرة يجب إثارته أمام قاضي الموضوع وعلى أبعد تقدير خلال مرحلة الإستئناف وليس في بداية التقاضي[3]، أمّا في مادة الجنايات فإنّ قرار الإحالة يغطي ويصحح عيوب الإجراءات السابقة، وعليه يجب إثارة الوجه المتعلق ببطلان الخبرة والتمسك به أمام غرفة الإتهام[4]، وإغفال قاضي التحقيق إخطار الأطراف بخلاصات ونتائج الخبير كما قررت المادة (154) من قانون الإجراءات الجزائية لا يعتبر سببا لبطلان الخبرة إلاّ إذا ترتب عن ذلك إنتهاك حقوق الدفاع[5].

رابعا : بطلان التسرب.

لقد سبقت الإشارة إلى أنه ضمانا من المشرع تحت طائلة البطلان أن يكون الأمر محدد المدة وأن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته، كما يحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (04) أشهر ويمكن أن تجدد هذه العملية حسب مقتضيات التحقيق وضمن نفس الشروط الشكلية والزمنية[6].

ولاشك أنّ هذه الضمانات تتعلق بالنظام العام، ومن تم تجوز التمسك بها في أي وقت من الإجراءات الأمر الذي يرتب على عدم مراعاة تلك الضمانات إهدار الأدلة المستمدة منها، ناهيك عن التحريض البوليسي على ارتكاب الجريمة الذي يعد في حد ذاته قيدا على عون أو ضابط الشرطة القضائية، وإن كان الدكتور "محمد مروان" له رأي في هذه المسألة، حيث يرى أنّ الإغراء الذي تعرض له الشخص يلعب دورا في السلوك، لكن الشخص يحتفظ مع ذلك بحرية الإختيار، فبإمكانه أن يجيب بالنفي أو يستبعد هذا التحريض، وفيما يتعلق بضابط الشرطة القضائية فقصده شرعي، ومن جانب المتهم هناك ضغط يمارس عليه لكنه لا يعيب حرية الإختيار[7].

---

[1] - Crim 17 Juillet 1976, B. N° 256 – 25 Juillet 1979, B. N° 253.
[2] - Crim 28 Février 1974, B. N° 89.
[3] - Crim 22 Mai 1959 , Bull. Crim N° 266.
[4] - Crim 28 déc 1959. Bull. Crim N° 590 – 05 Avril 1965 : Bull. Crim N° 110.
نقلا عن: أ . أحمد الشافعي ، المرجع السابق، ص 141.
[5]- نفس المرجع، ص 115.
[6] – المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري.
[7] - د. محمد مروان، المرجع السابق، ج 2، ص 426.

خامسا : بطلان الإنابة القضائية.

تذكر في الإنابة القضائية صفة القاضي الذي أصدرها والمحكمة التي يعمل بها والجهة الموجهة إليها سواء كان قاضيا أو ضابط شرطة قضائية، ويجب أن تكون الإنابة القضائية مؤرخة وموقعة عليها من طرف القاضي الذي أصدرها وتمهر بختمه الذي يمنح الرسمية للتوقيع المادة (2/138)[1] من قانون الإجراءات الجزائية.

ويعتبر التوقيع إجراءا جوهريا كما يعتبر التاريخ بدوره إجراءا جوهريا يترتب عن إغفاله بطلان الإنابة القضائية ويتعرض قرار الإحالة أمام محكمة الجنايات الذي لم يصرح ببطلان الإنابة القضائية غير المؤرخة للإبطال والنقض[2]، كما تعتبر مسألة التاريخ من النظام العام يمكن إثارتها أمام قضاة الموضوع، غير أنّ تنفيذ الإنابة القضائية بعد اختتام التحقيق القضائي يعتبر غير سليم[3].

سادسا : بطلان الدليل أثناء المحاكمة.

تم التطرق فيما سبق إلى الدفع ببطلان إجراءات جمع وتقديم أدلة الإثبات أثناء مرحلتي التحريات الأولية والتحقيق القضائي، أما بالنسبة للإجراءات المتعلقة بأدلة الإثبات أثناء المحاكمة سواء أمام الدرجة الأولى أو الثانية من درجات التقاضي، فإنّ المفهوم العام لفكرة الدفع بالبطلان لا يتغير، ولكن طرح المسألة هو الذي يعرف بعض الإختلافات.

والبطلان الذي يبرز على هذا المستوى هو أساسا بطلان لمخالفة القواعد الجوهرية للإجراءات أو مخالفة القانون أو الخطأ في تطبيقه، ويمكن ذكر الصور التالية للإحاطة بأكبر عدد من الحالات :

- قبول أدلة خارج معرض المرافعات ودون أن تتم مناقشتها وجاهيا لمخالفته لأحكام المادة (212) من ق.إ.ج التي توجب تقديم الأدلة وطرحها للمناقشة الوجاهية.
- إدانة المتهم لأنه لم يستطع إثبات براءته فهذا الإستدلال باطل لمخالفته للمبادئ العامة للإثبات.
- الإعتماد على أدلة محصل عليها بطرق غير شرعية كالمحجوزات الناجمة عن تفتيش غير شرعي للمسكن أو تسجيلات صوتية وذلك من خلال التنصت الغير مسموح به،وكذا الأدلة المحصل عليها من خلال تصرفات

---

[1]- تنص المادة 2/138 من قانون الإجراءات الجزائية الجزائري على ما يلي:"...ويذكر في الإنابة القضائية نوع الجريمة موضوع المتابعة وتؤرخ وتوقع من القاضي الذي أصدرها وتمهر بختمه ...".

[2] - Crim 10 Novembre 1970. Bull. Crim N° 294.

نقلا عن: أحمد الشافعي، المرجع السابق، ص138.

[3]- أ . أحمد الشافعي ، المرجع السابق، ص 112.

غير نزيهة للضبطية القضائية من خلال قيامها بأعمال تحريضية على ارتكاب الجرم مثلما تم توضيح ذلك بالتفصيل سابقا.

- الإعتماد على غياب المتهم على جلسة المحاكمة كدليل ضده والحكم بإدانته على هذا الأساس.

- إعتبار أنّ إعتراف المتهم دليل قاطع ولا تجوز مناقشته أو تجزئته قياسا على أحكام الإعتراف في القانون المدني وفي ذلك مخالفة لصريح نص المادة (213) من قانون الإجراءات الجزائية الجزائري التي تقضي بأنّ الإعتراف شأنه كشأن جميع عناصر الإثبات يترك لحرية تقدير القاضي.

- عدم تقيد القاضي الجزائي بإثبات المسائل المدنية وفقا للقانون المدني كتصريحه بقيام جنحة خيانة الأمانة دون إثبات عقد الأمانة وفقا لأحكام القانون المدني[1].

فالملاحظ أنّ البطلان خلال مرحلة المحاكمة قد يكون بطلانا متعلقا بالقواعد العامة لانعقاد المحكمة، وقد يكون بطلانا يلحق التكليف بالحضور ،كما قد يكون بطلانا يلحق قواعد المرافعات، وفيما يتعلق بالبطلان المتعلق بالقواعد العامة لانعقاد المحكمة سوف تقتصر الدراسة على مسألة الإختصاص مادام قد تم التطرق في الفصل الأول من هذا الباب للإختصاص القضائي للجرائم الإلكترونية .

فقد تم اعتبار قوانين التنظيم القضائي والإختصاص من النظام العام لأهميتها في حسن سير العدالة، كما أنّ قواعد إختصاص الجهات القضائية تدخل ضمن قواعد التنظيم القضائي وتعتبر جزءا منها.

ويترتب على اعتبار قواعد الإختصاص من النظام العام أنه لا يمكن التنازل عنها ضمنا أو صراحة كما أنه لا يمكن تصحيحها بالسكوت عنها أو الرضا بها، كما يجوز إثارتها خلال جميع مراحل الدعوى الجزائية ومن أي طرف كان في الدعوى الجزائية، كما يتعين على القاضي أن يصرح بعدم اختصاصه ولو تلقائيا إذا كانت القضية والوقائع التي ينظرها والمطروحة عليه ليست من اختصاصه سواء كان الإختصاص نوعيا أو شخصيا أو محليا.

أمّا بالنسبة للمشرع المصري كان قد نص على أنّ مخالفة قواعد الإختصاص النوعي تعتبر من النظام العام ويترتب عنها البطلان المطلق الذي لا يجوز التنازل عنه، فقد ذكر في المادة (332) من ق.إ.ج أنه إذا كان البطلان راجعا لعدم مراعاة أحكام القانون المتعلقة بتشكيل المحكمة أو بولايتها بالحكم في الدعوى

[1] - أ.نجيمي جمال، المرجع السابق، ص 151.

أو باختصاصها من حيث نوع الجريمة المعروضة عليها أو بغير ذلك مما هو متعلق بالنظام العام جاز التمسك به في أية مرحلة كانت عليها الدعوى وتقضي به المحكمة من تلقاء نفسها[1].

أمّا المشرع الجزائري، فلم ينص صراحة على ترتيب البطلان على عدم مراعاة قواعد الإختصاص بأنواعها الثلاثة، وإنما ترك ذلك للقضاء يتولى هذه المهمة، وقد حدد المشرع الجزائري الإختصاص النوعي والشخصي والمحلي العائد لكل جهة قضائية جزائية وذكر في المادة (329)[2] من ق.إ.ج أنّ المحكمة المختصة محليا بنظر الجنح هي محكمة محل الجريمة أو محل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم، غير أنه يجوز تمديد الإختصاص المحلي للمحكمة إلى دائرة إختصاص محاكم أخرى في جرائم معينة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

وقد أكدت المحكمة العليا أنّ المشرع الجزائري قد راعى في تحديد قواعد الإختصاص إعتبارات تتعلق بالسيادة وسهولة التحقيق وفكرة الردع والأثر الفعال في نفوس الأفراد، وعليه تعتبر قواعد الإختصاص في المواد الجزائية من النظام العام يترتب على مخالفتها البطلان المطلق، فعلى الجهة القضائية الفاصلة في الدعوى الجزائية التأكد من إختصاصها مسبقا وقبل الشروع في الموضوع[3].

الفرع الثاني :طبيعة بطلان الإجراءات الخاصة لجمع الدليل الالكتروني.

اختلف الفقه والقضاء حول نوع البطلان المترتب على مخالفة ضمانات وضوابط المراقبة، فثمة رأي يرى أنّ هذا البطلان نسبي وثمة رأي يرى أنه بطلان مطلق وثمة رأي متوسط فيعتبره متعلقا بالنظام العام في أحوال دون أخرى، وسوف يتم عرض موقف الفقه ثم موقف القضاء على النحو التالي :

أولا : الفقه.

ظهر إختلاف في الفقه حول تحديد طبيعة البطلان المترتب على مخالفة ضمانات وضوابط المراقبة، حيث ذهب جانب من الفقه إلى أنه بطلان مطلق[4]، وحجته في ذلك أنّ المصلحة التي تحميها ضمانات وضوابط المراقبة تهدف إلى تحقيق مصلحة عامة ومن تم فإنّ مخالفتها يترتب عليها بطلان مطلق.

---

[1] – أ. أحمد الشافعي، المرجع السابق ،ص138.

[2]- تنص المادة 329 من قانون الإجراءات الجزائية الجزائري على ما يلي:" تختص محليا بالنظر في الجنحة محكمة محل الجريمة أو محل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر ... يجوز تمديد الإختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ...".

[3]- أ. أحمد الشافعي، المرجع السابق، ص 145.

[4] – د. محمود محمود مصطفى، المرجع السابق، ص 106. نقلا عن: د. ياسر الأمير فاروق، المرجع السابق، ص709.

وقد إتجه أغلب الفقهاء[1] إلى القول أنّ البطلان المترتب على مخالفة ضوابط وضمانات المراقبة هو بطلان نسبي، وحجتهم في ذلك أنّ الغرض من هذه الضمانات والضوابط هو تحقيق مصلحة المتهم والخصوم.

وذهب جانب آخر من الفقه[2] إلى القول بأنّ الأصل في بطلان المراقبة أن يكون نسبيا ومع ذلك فإنّ هذا البطلان من الممكن أن يكون مطلقا في حالتين: الأولى إذا كان دليل المراقبة مستمدا من جريمة، والحالة الثانية إذا تم مخالفة الإختصاص بالمراقبة، ومن تم يترتب البطلان المطلق في حالة إجراء المراقبة دون الحصول على إذن من القاضي في الأحول التي يستوجب فيها القانون الحصول على هذا الإذن.

ثانيا : القضاء.

لم تستقر محكمة النقض المصرية في أحكامها على وصف بطلان المراقبة ولم تجر أحكامها في هذا الشأن على وتيرة واحدة، ففي بعض الأحكام تأخذ بالبطلان النسبي وفي أحكام أخرى تتجه إلى الأخذ بفكرة البطلان المطلق، و ذلك على النحو التالي:

الإتجاه الأول: البطلان النسبي.

إتجهت محكمة النقض المصرية في بعض أحكامها إلى فكرة البطلان النسبي فاشترطت توافر الصفة فيمن يدفع ببطلان المراقبة، فقضت بأنّ:" لما كان الحكم المطعون فيه قد عرض للدفع ببطلان إذن النيابة العامة بالتسجيل لإجرائه على هاتف لا يخص الطاعن ورد عليه بقوله على فرض أنّ الهاتف غير خاص بالمتهم وخاص بغيره، فإنّ الدفع في هذا الشأن لا يقبل من غير حائزه باعتبار أنّ الحائز هو صاحب الصفة في ذلك وأنّ الصفة تسبق المصلحة، فإن لم يثره الحائز أو المالك فليس لغيره أن يبديه ولو كان يستفيد منه، لأنّ هذه الفائدة لا تتحقق إلاّ بالتبعية وحدها وإذا كان ما خلص إليه الحكم في طرح ما دفع به الطاعن متفقا وصحيح القانون، فإنّ ما ينعاه على الحكم في هذا الصدد يكون غير مقبول"[3].

ويظهر من خلال هذا الحكم أنه لا يستقيم مع فكرة البطلان المطلق لما هو مقرر من أنّ لكل ذي مصلحة أن يتمسك بهذا البطلان سواء وقع الإجراء الباطل عليه أم على غيره، وقد اشترطت محكمة النقض

[1] – د. نبيل مدحت سالم، شرح قانون الإجراءات الجنائية، دار الثقافة الجامعية، القاهرة، مصر، ط6، سنة 1992، ص 354. نقلا عن: د.محمد أمين الخرشة، المرجع السابق، ص234.

[2] – د.محمود نجيب حسني، المرجع السابق، ص670. نقلا عن: د. ياسر الأمير فاروق، المرجع السابق، ص 709.

[3] – نقض 1998/4/13، مجموعة أحكام النقض، س49، رقم 73، ص563.

للدفع ببطلان المراقبة سبق إثارته أمام محكمة الموضوع وعللت ذلك بأن الإجراءات السابقة على المحاكمة لا تجوز إثارتها أمام محكمة النقض[1].

الإتجاه الثاني :البطلان المطلق.

ظهر هذا الإتجاه في بعض أحكام محكمة النقض المصرية إذ لم تحظر بصفة مطلقة إبداء الدفع ببطلان المراقبة لأول مرة أمامها، وعللت ذلك بأنّ لا شأن لها بطبيعة البطلان وأنّ هذا الدفع من الدفوع الموضوعية المختلفة بالواقع، وتقتضي تحقيقا موضوعيا تنحسر عنه وظيفة محكمة النقض، وعليه فإنه إذا كان الفصل في البطلان يقتضي تحقيقا في الوقائع التي يقوم عليها ولم تجز إثارته أمام محكمة النقض لأول مرة ولو كان متعلقا بالنظام العام لخروجه في ذلك عن اختصاصها.

فقضت محكمة النقض بأنّ: "من المقرر أنّ الدفع ببطلان وتسجيل المحادثات إنما هو من الدفوع القانونية المختلطة بالواقع التي لا يجوز إثارتها لأول مرة أمام محكمة النقض ما لم يكن قد دفع به أمام محكمة الموضوع أو كانت مدونات الحكم تحمل مقوماته، نظرا لأنه يقتضي تحقيقا تنأى عنه وظيفة هذه المحكمة، ولما كان الثابت من محضر جلسة المحاكمة أنّ أيا من الطاعن أو المدافع عنه لم يدفع ببطلان إذن رئيس المحكمة وتسجيل المحادثات لعدم اختصاص مصدره ولخلوه من تاريخ إصداره، وكانت مدونات الحكم قد خلت مما يرشح لقيام ذلك البطلان فلا يقبل إثارته لأول مرة أمام محكمة النقض"[2].

ويستخلص الدكتور ياسر الأمير فاروق أنّ محكمة النقض في أحكامها السابقة تجيز إثارة بطلان المراقبة لأول مرة أمامها إذا كانت الوقائع الثابتة بالحكم دالة على هذا البطلان، أي أنها تعتبر بطلان المراقبة من النظام العام.

المطلب الثالث :آثار بطلان إجراءات جمع الدليل الإلكتروني.

يترتب على الحكم ببطلان إجراء ما تجريد الإجراء من آثاره القانونية أي تعطيله عن أداء وظيفته في الخصومة الجنائية، ولا يقتصر هذا الأثر على الإجراء الباطل فقط، بل يمتد إلى الإجراءات اللاحقة على الإجراء الباطل.

[1] – نقض 1970/4/19، مجموعة أحكام النقض، س21،رقم 147 ،ص617. نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص 235.

[2] – نقض 1996/9/26، مجموعة أحكام النقض، س47، رقم 128 ،ص892 ، نقلا عن :د. ياسر الأمير فاروق، المرجع السابق، ص 712.

وبطلان الإجراء لا يتقرر بقوة القانون بل لابد من حكم أو قرار يصدر من المحكمة سواء كان بطلان مطلقا أي متعلقا بمصلحة عامة أم كان البطلان نسبيا أي متعلقا بمصلحة خاصة، وعلى ذلك فإنّ العمل الإجرائي يكون فعالا ومنتجا لآثاره القانونية إلى أن يحكم ببطلانه[1].

ويترتب على التقرير بالبطلان آثار هامة منها ما يتعلق بالإجراء الباطل ذاته ومنها ما يتعلق بالإجراءات المتصلة به سواء كانت سابقة أو لاحقة، فمتى تقرر بطلان إجراء معين وجب استبعاد الدليل المستمد منه وإلا أضحت الضمانات التي يقررها القانون للحفاظ على الحريات عديمة الجدوى[2]، وسيتم التطرق لهذه الآثار على النحو التالي:

الفرع الأول : أثر البطلان على الإجراء المعيب ذاته.

بمجرد أن يصدر حكم ببطلان إجراء من الإجراءات يترتب عنه زوال آثاره القانونية وفقدان قيمته في الدعوى الجزائية ويتوقف عن أداء وظيفته الأساسية المنوطة به، ويصبح الإجراء المعيب منعدما كأنه لم يكن أبدا،كما أنّ بطلان الإجراء يترتب عنه زوال أثره القانوني المؤدي لقطع تقادم الدعوى الجزائية، وعليه فإنّ الأحكام والقرارات النهائية أو الصادرة قبل الفصل في الموضوع لا تقطع التقادم إذا صدرت إثر تكليف مباشر صرح ببطلانه، كما أنّ تبليغ حكم مشوب بالبطلان لا يمكن اعتباره إجراء من إجراءات المتابعة القاطع للتقادم[3].

كما يترتب البطلان على التفتيش وما نتج عنه إذا لم يتم احترام أحكام المواد (45-47-47 مكرر) من قانون الإجراءات الجزائية الجزائري الخاصة بعمليات التفتيش وكيفية القيام به طبقا للمادة (48) من نفس القانون، إلاّ أنّ المشرع الجزائري واعترافا منه بخصوصية الجرائم الإلكترونية وخوفا من ضياع الدليل وإتلافه واختلاف إجراءات جمع الدليل الإلكتروني بالنسبة لهذه النوعية من الجرائم بالمقارنة مع الجرائم التقليدية، نص في الفقرة الأخيرة من المادة (45) من قانون الإجراءات الجزائية على أنه يستثنى من تطبيق أحكام المادة السابقة فيما يخص حضور الأشخاص المحددين في الفقرة الأولى من هذه المادة عدة جرائم ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

---

[1] – د.محمد أمين الخرشة ، المرجع السابق، ص239.

[2] – د.عبد الحفيظ نقادي ، المرجع السابق ،ص320.

[3] – أ. أحمد الشافعي ، المرجع السابق ،ص269.

الفرع الثاني :أثر البطلان على الإجراءات الأخرى.

إذا تم الحكم على إجراء بأنه باطل فإنّ هذا البطلان لا يمتد تأثيره على الإجراء في حد ذاته، بل قد يمتد إلى الإجراءات اللاحقة عليه، أمّا بالنسبة للإجراءات السابقة فهي محل خلاف بين الفقهاء .

أولا :أثر البطلان على الإجراءات السابقة .

إذا كان الحكم بالبطلان يترتب عنه تجريد الإجراء المعيب نفسه من إنتاج آثاره القانونية في الدعوى الجزائية، كما يمكن أن يمتد أثر الإجراء الباطل لجميع الإجراءات اللاحقة له وهي القاعدة التي أكدتها الأحكام التي وردت في قانون الإجراءات الجزائية الجزائري الخاصة بالبطلان المواد (1/157)، (2/159)[1] و (191) [2] من قانون الإجراءات الجزائية وقرارات المحكمة العليا في هذا الشأن[3]، فإنّ الأمر يختلف جذريا بالنسبة للإجراءات السابقة على الإجراء المعيب، فالقاعدة العامة أنّ الحكم ببطلان الإجراء المعيب لا يمتد أساسا للإجراءات السابقة عليه بل تبقى هذه الإجراءات صحيحة وسليمة تنتج الآثار القانونية المترتبة عليها أصلا ولا يلحقها أو يشوبها أي عيب كان.

فقانون الإجراءات الجزائية لم يتضمن أي حكم يتعلق بامتداد أثر البطلان الذي يلحق إجراءا معينا إلى الإجراءات السابقة على الإجراء المعيب، كما أنّ القضاء الجزائري قد سار في الإتجاه الذي أخذ به التشريع وهو نفس المنحنى الذي اتبعه التشريع والقضاء الفرنسي، غير أنّ بعض الفقهاء[4] يرون أنه يمكن أن يمتد أثر بطلان إجراء إلى الإجراءات السابقة عليه إذا كان هناك ارتباط بينها وبين الإجراء الباطل ،غير أن القضاء لم يتبعه في مسعاه ولم يجد هذا الإتجاه إجماعا بين الفقهاء.

---

[1]- تنص المادة 2/159 من قانون الإجراءات الجزائية الجزائري على ما يلي: " ... وتقرر غرفة الإتهام مإذا كان البطلان يتعين قصره على الإجراء المطعون فيه أو امتداده جزئيا أو كليا على الإجراءات اللاحقة له ...".

[2]- تنص المادة 191 من قانون الإجراءات الجزائية الجزائري على ما يلي:" تنظر غرفة الإتهام في صحة الإجراءات المرفوعة إليها وإذا تكشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به...".

[3] – قرار صادر في 1981/04/21، طعن رقم 24905 عن القسم الأول للغرفة الجنائية الثانية للمحكمة العليا.

– قرار صادر في 1988/11/08، طعن رقم 57557 عن الغرفة الجنائية الأولى للمحكمة العليا.

– قرار صادر في 1988/01/13، طعن رقم 55298 عن الغرفة الجنائية الأولى للمحكمة العليا. نقلا عن: أ. أحمد الشافعي، المرجع السابق، ص272.

[4] – د. أحمد أبو الوفا، أصول المحاكمات المدنية، الدار الجامعية، القاهرة، مصر، بدون طبعة، سنة 1983، ص484. نقلا عن: أ. أحمد الشافعي، المرجع السابق،ص 272.

ثانيا : أثر البطلان على الإجراءات اللاحقة .

القاعدة هي أنّ الإجراء الباطل يمتد بطلانه إلى الإجراءات اللاحقة عليه إذا كانت هذه الإجراءات تترتب عليه مباشرة، وتثير هذه القاعدة مسألة تتعلق بأهمية المعيار الذي يبين مدى العلاقة التي تربط بين العمل الإجرائي الباطل والأعمال التالية له حتى يمتد إليها البطلان، أو بعبارة أخرى بيان متى يكون الإجراء مترتبا على ما سبق وقد اختلف الفقه[1] في تحديد معايير الإجراءات المترتبة على الإجراء الباطل، إلاّ أنّ المعيار السائد هو أنه ينبغي توافر علاقة تبعية بين الإجراء السابق والإجراءات اللاحقة عليه، بحيث يعتبر الإجراء السابق المقدمة الضرورية والشرعية لصحة العمل اللاحق، فالقانون وحده هو الذي يتولى بيان أهمية الإجراء الباطل بالنسبة لما تلاه من الإجراءات، فإذا أوجب مباشرة إجراء معين قبل آخر فيصبح الإجراء الأول بمثابة السبب الوحيد للإجراء الذي تلاه، أي لا يمكن مباشرة الإجراء الأخير دون الإجراء الأول فكان هذا الإجراء الأول شرطا لصحة الإجراء التالي له، فإذا بطل ترتب عليه بطلان الإجراء الذي يبنى عليه.

وفرقت محكمة النقض المصرية في هذا الشأن بين أمرين:

– أنّ الإجراء المعيب سببا أو مقدمة شرعية مفترضة لاتخاذ الإجراء اللاحق، وفي هذه الحالة لا مناص لمحكمة الموضوع من القضاء بالبطلان في شأن الإجراء اللاحق وإلاّ كان حكمها مخالفا للقانون.

– في حالة ما إذا كان الإجراء اللاحق قد تأثر بالإجراء السابق عليه فجاءت نتيجته على وجه معين ويرجع تقدير ذلك لمحكمة الموضوع وتبت فيه على ضوء ظروف كل من الإجراءين.

يتبين مما سبق أنّ بطلان الإجراء المعيب لا يؤثر على صحة الإجراءات اللاحقة عليه متى كانت هذه الإجراءات مستقلة عن الإجراء المعيب، فاستقلال الإجراء اللاحق يعصمه من البطلان الذي شاب ما سبقه من إجراءات، وبالتالي فإنّ الحكم ببطلان التفتيش المعيب لا يؤثر على صحة الإجراءات التالية إذا كانت مستقلة عن هذا التفتيش وغير مرتبطة به[2].

[1] – د. فتحي والي، المرجع السابق، ص 676. نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص 243.

[2] - د. محمد أمين الخرشة، المرجع السابق، ص 244.

و قد أكدت المحكمة العليا في عدة قرارات لها[1] أن أثر بطلان الإجراء يمتد إلى الإجراءات اللاحقة له إذا كان العيب يتصل بها وتوجد بينهما علاقة سببية[2].

الفرع الثالث : أثر بطلان المراقبة على الأدلة الناتجة عنها.

يترتب على بطلان إجراء المراقبة بطلان جميع الإجراءات اللاحقة والمبنية عليه مباشرة واستبعاد الأدلة الناجمة عن المراقبة الباطلة، ومن هنا ترتبط آثار البطلان أشد الإرتباط بقاعدة استبعاد الأدلة وهو ما حدا بغالبية التشريعات إلى دراسة قاعدة الإستبعاد في ضوء نظرية البطلان.

ولاشك في أنّ استبعاد الدليل الناجم عن المراقبة الباطلة من الأمور البالغة الخطر، إذ يترتب عليه إفلات المجرم من العقاب إذا كانت الإدانة متوقفة على الدليل الناجم عن المراقبة الباطلة، ولهذا اتجهت بعض التشريعات في البداية إلى الإلتفات عن قاعدة الإستبعاد، كما حاول البعض الآخر من التشريعات الحد من هذه القاعدة، غير أنّ تطورا ملحوظا طرأ على مسلك هذه التشريعات جعلها تتبنى قاعدة الإستبعاد[3].

وعليه سيتم التطرق لقاعدة استبعاد الأدلة الناجمة عن المراقبة الباطلة في القوانين الغربية ثم في القوانين العربية و كذا القانون الجزائري، وذلك على النحو التالي:

البند الأول :قاعدة استبعاد الأدلة الناجمة عن المراقبة الباطلة في القوانين الغربية.

سيتم التطرق لقاعدة الإستبعاد الناجمة عن المراقبة الباطلة في القانون الأمريكي والقانون الإنجليزي وكذا القانون الفرنسي، وذلك على النحو التالي:

أولا :القانون الأمريكي.

درج القانون الأمريكي في بداية عهده على تطبيق قواعد القانون العام التي لا تشترط لقبول الدليل سوى تعلقه بموضوع الدعوى دون النظر إلى الوسيلة التي تم الحصول عليه من خلالها، أي حتى لو تم بطرق غير مشروعة.

---

[1] – قرار صادر في 1986/12/16، طعن رقم 45442 عن الغرفة الجنائية الأولى للمحكمة العليا.

– قرار صادر في 1988/01/03، طعن رقم 53358 عن الغرفة الجنائية الأولى للمحكمة العليا. نقلا عن: د. عبد الحفيظ نقادي، المرجع السابق، ص323.

[2] – د. عبد الحفيظ نقادي، المرجع السابق، ص 323.

[3] – د.ياسر الأمير فاروق، المرجع السابق، ص 721.

وفي عام 1914 وبالتحديد في قضية weeks تبنت المحكمة الفيدرالية العليا قاعدة استبعاد الدليل متى تم الحصول عليه بطريقة مخالفة للتعديل الدستوري الرابع[1]، ثم سارت المحكمة في ذات الإتجاه بعد ذلك وقضت باستبعاد الدليل المستمد من تنصت رجال الشرطة على المتهم بواسطة أحد مكبرات الصوت وكانت الشرطة قد قدمت ذلك الدليل ضد المتهم كدليل في قضية قمار[2].

وإذا كانت المحكمة الفيدرالية العليا قد صرحت بأنّ قاعدة الإستبعاد لا تلزم محاكم الولايات، إلاّ أنها عادت وغيرت موقفها وألزمت محاكم الولايات بتطبيق قاعدة الإستبعاد، حيث اتجهت المحكمة الفيدرالية العليا إلى القضاء بعدم دستورية قانون ولاية نيويورك الذي يجيز لرجال الأمن مراقبة المحادثات الهاتفية وتسجيلها بعد الحصول على إذن قضائي، وأصبحت القاعدة مطبقة في كافة أرجاء الولايات المتحدة الأمريكية فلا يجوز قبول دليل مستمد من تنصت أو تسجيل باطل والاستناد إليه في إدانة المتهم[3].

ثانيا :القانون الإنجليزي .

السائد في الفقه والقضاء الإنجليزي أنّ عدم تطبيق قاعدة الاستبعاد يستند إلى اعتبارات عملية ومهنية، ذلك أنّ الإجراء غير المشروع له جزاء تأديبي مستقل ولا ينبغي أن يكون أثره على الدليل الناجم منه حتى لا تضار العدالة نتيجة تسرع ورعونة الفرد.

ومن تطبيقات القضاء الإنجليزي حول الإعتداد بالأدلة الناجمة عن المراقبة الباطلة قضية Stewart R.V. إذ قبلت المحكمة في تلك القضية الدليل المستمد من تنصت غير مشروع قام به ضابط شرطة[4]، وأيضا في قضية R.V.keeton أين تقرر قبول دليل قدمه رجل شرطة تحصل عليه من خلال التنصت على محادثة هاتفية أجراها المتهم مع زوجته أثناء احتجازه بقسم الشرطة[5].

غير أنه بصدور قانون الشرطة والإثبات الجنائي لعام 1984 تم التخفيف من حدة هذه القواعد، إذ نصت المادة 1/78 منه على تخويل المحكمة سلطة استبعاد أدلة الإثبات متى تبين لها أنّ قبول تلك الأدلة من شأنه أن يحدث تأثيرا مضادا على نزاهة الإجراءات[6].

---

[1] - Weeks V. United States 232 U.S 383 (1914).

[2] -Silverman V. United States 365. U.S 505 (1961).

نقلا عن : د. ياسر الأمير فاروق، المرجع السابق، ص 722.

[3]- نفس المرجع، ص 723.

[4] -R.V Stewart 54 Cr.APP.R.210, Ca.

[5] -R.V Keeton(1970) 54 Cr.APP.R 267.CA.

[6] – نقلا عن :د.ياسر الأمير فاروق، المرجع السابق ،ص725.

ثالثا :القانون الفرنسي.

نص قانون الإجراءات الجزائية الفرنسي في المادة (170) على أنّ البطلان يلحق بالإجراء المعيب والإجراءات اللاحقة عليه بصرف النظر عن توافر رابطة معينة بينهما، إلاّ أنه قصر هذه القاعدة على إجرائي الإستجواب والمواجهة المنصوص عليهما في المادتين (118،144) من قانون الإجراءات الجزائية.

أمّا بالنسبة للإجراءات الأخرى فإنّ غرفة الإتهام مخولة بمقتضى المادتين (2/172، 206) من قانون الإجراءات تقدير ما إذا كان البطلان يقتصر على الإجراء الباطل ذاته أم يمتد إلى الإجراءات اللاحقة عليه والمتأثرة به[1]، كما نص المشرع الفرنسي صراحة في المادة (100-7)[2] من قانون الإجراءات الجزائية على بطلان مخالفة الضمانات والضوابط التي نظمت إجراء التنصت والتسجيل .

وقد درج القضاء الفرنسي على عدم الإعتداد بالدليل الناجم عن الإجراءات الباطلة مع احتفاظه بسلطة تقديرية في تحديد المخالفة الإجرائية التي من شأنها أن تفضي إلى هذا الأثر، وقد أدان ذات القضاء التنصت أثناء التحقيق الذي تجريه الشرطة سواء كان أوليا أو في جريمة متلبس بها[3]، كما رفض الدليل المستمد من قيام أحد رؤساء المنشأة بالتنصت على محادثات مرؤوسيه محاولا استخدام مضمون المحادثة التي سجلت كدليل إدانة تأسيسا على أنّ التسجيل تم بطريقة غير مشروعة[4].

إلا أنّ القرار الصادر من محكمة استئناف "بواتيي Cour de Poitiers" بتاريخ 07 جانفي 1961 يعتبر أكثر دلالة حول الموضوع، إذ اعتبر أنّ حقوق الدفاع لا تنتهك إلا إذا نظم التنصت الهاتفي بعد توجيه التهمة رسميا لأجل ضبط محادثات بين المتهم ومحاميه أو لأجل الحصول على أدلة إثبات خارجا عن كل استجواب شرعي، وأضاف القرار المذكور أنّ الأمر ليس كذلك على أساس أنّ التنصت وقع في مرحلة لم يكن المشتبه فيه قد وجهت إليه التهمة وأنّ هذا التنصت نفسه وقع من غير تحريض أو نصب[5]، ويستخلص ويستخلص

---

[1] - د. ياسر الأمير فاروق، المرجع السابق، ص 762.

[2] - Article 100-7 (C.P.P.F Modifié par Loi n°2004-204 du 9 mars 2004 - art. 5 JORF 10 mars 2004) : Aucune interception ne peut avoir lieu sur la ligne d'un député ou d'un sénateur sans que le président de l'assemblée à laquelle il appartient en soit informé par le juge d'instruction.
Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé par le juge d'instruction.
Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un magistrat ou de son domicile sans que le premier président ou le procureur général de la juridiction où il réside en soit informé.
Les formalités prévues par le présent article sont prescrites à peine de nullité.

[3] - Cass crim 13 juin 1989, Bull, P254.
- Cass crim 24 Novembre 1989, Bull, P34.

[4] - Cass crim 28 Juin 1983, Bull, P201. نقلا عن :د. محمد أمين الخرشة، المرجع السابق،ص 251.

[5] - Cour de poitiers : 07 Janvier 1960 JCP 1960 – 11- 11599 Note Chambon.

من هذا القرار أنّ التنصت الهاتفي يعتبر مشروعا إذا تم مراعاة الضمانات التي نص عليها القانون، وذلك دون الخروج عن الحالات التي حددها.

أمّا عن التسجيل بواسطة آلة مسجلة (Magnétophone) فإن محكمة النقض الفرنسية أكدت في قرار لها[1] بأن للقاضي الحق في أن يأخذ بعين الإعتبار أقوال أدلى بها أحد الشهود مسجلة على شريط مغناطيسي بدون علمه في فترة لم يكن فيها إجراءات التحقيق قد انطلقت بعد، وعندما يقترن التسجيل على الشريط المغناطيسي باعتراف المتهم، فإنّ محكمة النقض قررت أنّ الأقوال هذه تعتبر قرينة تضاف إلى وسائل الإثبات الأخرى، ويستطيع القاضي أن يسند عليها يقينه الشخصي[2].

و يوجد قرار لمحكمة النقض الفرنسية صادر بتاريخ 17-07-1984 تحت رقم 83-92332 قضى بأن: "تسجيل المكالمات الهاتفية المجهولة والمتكررة من طرف من يستقبلها لا تشكل مساسا بالحياة الخاصة لمن قام بالمكالمة ولا خرقا لحقوق الدفاع"[3].

وفي قرار آخر أيدت محكمة النقض الفرنسية حق الطرف المدني في تسجيل مكالمة هاتفية خاصة (بينه وبين زوجته) من أجل الدفاع عن نفسه والرد على اتهام موجه له من طرف زوجته التي اتهمته بأنه اعتدى عليها وهو سكران واستظهرت بشهادة مزورة من صديقتها، وقد اعترفت الزوجة خلال المكالمة بتزييف وتزوير تلك الشهادة الطبية، وحيث أنّ تسجيل المكالمة الهاتفية الخاصة التي قام بها (أ.ي) كانت مبررة وذلك بضرورة تقديم الدليل على الوقائع التي كانت ضحية لها، وأن يجيب في إطار الدفاع عن نفسه عن الإتهامات بالعنف المنسوبة إليه[4].

نقلا عن : د. محمد مروان، المرجع السابق، ج2 ، ص 429.

[1] - Ch Crim : 18 Février 1958. Bull N° 163.

نقلا عن : نفس المرجع ، ص 430.

[2] - Ch Crim : 16 Mars 1961 JCP.

نقلا عن : نفس المرجع، ص 430.

[3] -La cour , « Attendu qu'en l'état de leurs constatations et énonciations, desquelles il résulte que les prévenus se sont bornés à enregistrer des communications téléphoniques qui étaient destinées à l'un d'eux et qui perturbaient leur vie familiale, les juges, en décidant qu'il n'avait pas été porté atteinte à l'intimité de la vie privée, n'ont pas encouru les griefs portés au moyen ;
D'où il suit que le moyen doit être écarté ».
Disponible à l'adresse suivante :
www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007062981.

[4] - Décision de la cour de cassation, chambre criminelle rendue le 31/01/2007, rejet – Numéro de pourvoi : 06-82383
Attendu qu'il résulte de l'arrêt attaqué et des pièces de procédure que Germaine X... a produit, dans une procédure de divorce, une attestation établie par une amie, relatant de graves violences commises sur elle-même par son époux, Alain Y..., en état d'ébriété ; que celui-ci a porté plainte et s'est constitué partie civile des chefs d'établissement d'attestation faisant état de faits matériellement inexacts et usage et a produit un

وأيضا أكدت محكمة النقض الفرنسية أنّ التسجيلات الصوتية يمكن أن تشكل قرائن تضاف إلى قرائن أخرى يمكن للمحاكم الجزائية أن تؤسس قناعتها بناء عليها، وباعتبارها وسائل إثبات وليست تصرفات إجرائية فإن القضاة لا يمكنهم إبطالها[1]، كما اعتبرت شريط تسجيل صوتي يتضمن عبارات السب والشتم قام به الضحية لتدعيم شكايته أمر مشروع، بينما قيام الشرطي أثناء عمله بعملية التسجيل لمكالمة موجهة له من طرف مشتبه فيه يخالف قواعد الإجراءات ويخل بحقوق الدفاع[2].

البند الثاني :قاعدة استبعاد الأدلة الناجمة عن المراقبة الباطلة في القوانين العربية.

سيتم التطرق من خلال هذا البند لموقف القانون السوري والقانون المصري من قاعدة استبعاد الأدلة الناجمة عن المراقبة الباطلة وذلك على النحو التالي:

أولا : القانون السوري.

إنّ القانون السوري على الرغم من أنه يأخذ بمبدأ البطلان بوجه عام، إلاّ أنّ محكمة النقض السورية قد اتجهت إلى عدم سريان قواعد البطلان على أعمال الضبط القضائي المخالفة للقانون ونتائجها

---

procès-verbal d'huissier retranscrivant intégralement l'enregistrement d'une conversation téléphonique entre lui-même et son épouse, dans laquelle celle-ci reconnaissait le caractère mensonger de l'attestation ;
Attendu que, pour écarter l'argumentation de la prévenue qui invoquait le caractère déloyal de ce moyen de preuve au regard du procès équitable et la condamner du chef d'usage d'attestation inexacte, l'arrêt prononce par les motifs repris au moyen ;
Attendu qu'en statuant ainsi, et dès lors que l'enregistrement de la conversation téléphonique privée, réalisé par Alain Y..., était justifié par la nécessité de rapporter la preuve des faits dont il était victime et de répondre, pour les besoins de sa défense, aux accusations de violences qui lui étaient imputées, la cour d'appel, devant qui la valeur de ce moyen de preuve a été contradictoirement débattue, n'a pas méconnu les textes et les dispositions conventionnelles visés au moyen ;
D'où il suit que le moyen doit être écarté ;
Disponible à l'adresse suivante :
www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000017627847.

[1] - l'enregistrement par magnétophone peut constituer un indice de preuve, susceptible de s'ajouter à d'autres indices, sur lesquels les tribunaux répressifs peuvent fonder leur intime conviction.
Crim. 16 mars 1961: JCP 1961. II. 12157, note Larguier.

[2] - Enregistrement de conversation : constitue un moyen de preuve licite l'exploitation par des enquêteurs de l'enregistrement d'une cassette contenant des propos injurieux proférés par téléphone et enregistrés par la victime qui a déposé plainte. Crim. 13 juin 2001 Procédures 2001. Obs. Buisson.
Mais l'enregistrement effectué de manière clandestine, par un policier agissant dans l'exercice de ses fonctions, des propos qui lui sont tenus, fut-ce spontanément, par une personne suspecte, élude les règles de procédure et compromet les droits de la défense. La validité d'un tel procédé ne peut être admise. Crim. 16 déc. 1997 : Bull. crim No 427 ; D 1998. ترجمة هذه القرارات باللغة العربية مأخوذة عن :أ. نجيمي جمال، المرجع السابق، ص 87-94.

إكتفاء بالمسؤولية التأديبية التي يقررها القانون على المخالف، حيث قضت بأنه: "لما كان عمل الشرطة وإن كان مخالفا للقانون إلاّ أنّ ما نشأ عنه من الأمر الواقع لا يمكن إنكاره والتغاضي عنه واعتباره كأنه لم يكن، فإذا تجاوز رجال الشرطة حدود وظيفتهم فإنهم يعرضون أنفسهم للعقوبة ولكن ذلك لا يحول دون رؤية الأمر الواقع والمشاهد المحسوسة"[1]، كما قضت ذات المحكمة في حكم آخر بأنّ إجراءات التحري التي تمت من قبل رجال الشرطة بدون إذن من المرجع المختص لا تؤثر على نتائجها ولا تمحو آثار الجريمة التي أظهرتها وإن كان مساءلتهم عما أجروه واردة[2].

ثانيا : القانون المصري.

قرر المشرع المصري قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة بصريح نص المادة (336) من قانون الإجراءات الجنائية بقولها: "إذا تقرر بطلان أي إجراء فإنه يتناول جميع الآثار التي تترتب عليه مباشرة ولزوم إعادته متى أمكن ذلك، ومن تم فإنّ بطلان إجراء المراقبة يترتب عليه بطلان جميع الإجراءات اللاحقة والمبنية عليه مباشرة، أمّا الإجراء اللاحق والمستقل عن المراقبة الباطلة لا يمتد تأثير البطلان إليه"، وهذا ما استقر عليه الفقه[3] والقضاء[4].

ومن تطبيقات محكمة النقض المصرية حول عدم الأخذ بالأدلة الناجمة عن المراقبة الباطلة وعدم امتداد أثر البطلان إلى الإجراء اللاحق المستقل عن المراقبة الباطلة قضت بأنه :

"متى كان الحكم المطعون فيه قد استند من بين ما استند إليه في إدانة المتهم إلى التسجيلات الصوتية وكان الدفاع قد نازع في أنّ ما سجل ليس بصوت المتهم، فإنه كان بتعين على المحكمة أن تحقق هذا الدفع الجوهري عن طريق المختص فنيا، أمّا وهي لم تفعل فإن حكمها يكون معيبا لإخلاله بحق الدفاع، ولا يدفع هذا العيب أن يكون الحكم قد استند في إدانة المتهم إلى أدلة أخرى ذلك بأنّ الأدلة في المواد الجنائية متساندة يكمل بعضها البعض الآخر، فتكون عقيدة القاضي منها مجتمعه بحيث إذا سقط أحدها أو استبعد تعذر التعرف على مبلغ الأثر الذي كان للدليل الباطل في الرأي الذي انتهت إليه المحكمة، أو الوقوف على ما كانت تنتهي إليه من نتيجة لو أنها فطنت إلى أنّ هذا الدليل غير قائم [5].

---

[1]- نقض سوري رقم 235 بتاريخ 1965/04/20، مجلة نقابة المحامين، دمشق 224 لسنة 1965.

[2] – نقض سوري رقم 405 بتاريخ 1969/01/17، مجلة نقابة المحامين، دمشق 134 لسنة 1969، نقلا عن : د. ياسر الأمير فاروق، المرجع السابق، ص 728.

[3]- د. أحمد فتحي سرور، المرجع السابق، ص 371 و د. جلال ثروت، المرجع السابق، ص 566.نقلا عن د. ياسر الأمير فاروق، المرجع السابق، ص 733.

[4]- نقض 1956/03/15، مجموعة أحكام النقض س 6، رقم 107،ص 361، نقض 1986/01/13 ، س 14، رقم 12 ،ص 51.

[5] – نقض 1991/6/6، مجموعة أحكام النقض، س42، رقم 135، ص913. نقلا عن : د. محمد أمين الخرشة، المرجع السابق، ص 252.

وبطلان التسجيلات الصوتية ينسحب على الدليل المستمد منها[1]، كما ينبني عليه بطلان كل إجراء تال له يكون مبنيا عليه أو متفرعا منه[2]، ولا تقبل شهادة من قام بإجراء المراقبة الباطلة لأنّ من يقوم بإجراء باطل لا تقبل منه الشهادة عليه[3]، وفي المقابل إذا ثبت أنّ الإجراء اللاحق لم يكن مترتبا على المراقبة الباطلة بل أنه مستقل عنها فإنّ البطلان الذي شاب المراقبة لا يمتد إليه بل يبقى صحيحا ويجوز الأخذ به، وفي هذا الصدد قضت محكمة النقض بأنّ بطلان التسجيلات لا يحول دون أخذ القاضي بجميع عناصر الإثبات الأخرى المستقلة عنه والمؤدية إلى النتيجة التي أسفرت عنها التسجيلات[4].

البند الثالث: قاعدة استبعاد الأدلة الناجمة عن المراقبة الباطلة في القانون الجزائري.

بعد أن تعاين الجهة القضائية المختصة بأنّ إجراءا معينا مشوب بالبطلان تصدر حكما بإلغاء الإجراء المعيب وحده، كما يمكنها أن تحكم أيضا بإلغاء الإجراءات اللاحقة له والمرتبطة به إرتباطا مباشرا والتي لها علاقة به، غير أنّ السؤال الذي يطرح في هذا المقام يتعلق بمصير الإجراءات الملغاة.

فقد نصت المادة (160 فقرة 1)[5] من قانون الإجراءات الجزائية التي وردت في القسم الخاص ببطلان إجراءات التحقيق على أن تسحب من ملف التحقيق أوراق الإجراءات التي أبطلت وتودع لدى كتابة ضبط المجلس القضائي، وعليه لا يمكن للجهة القضائية أن تأمر بسحب الإجراءات الملغاة من الملف إلاّ بكيفية غير قابلة للتجزئة اتجاه جميع الأطراف، إذ لا يسمح للجهة القضائية من استعمال الإجراءات الملغاة لصالح أطراف ضد أطراف أخرى، كما أنّ شرعية الإجراءات القضائية وقانونيتها وحماية حقوق المواطن وتكريس مبدأ البراءة تستدعي أن تكون الأدلة المعتمد عليها في الإدانة قد استخرجت بطريقة قانونية خالية من العيوب التي تشوب شرعيتها وسلامتها.

كما نصت المادة (160 فقرة 2)[6] من قانون الإجراءات الجزائية على منع القضاة والمحامين من الرجوع لأوراق الإجراءات التي أبطلت لاستنباط عناصر أو إتهامات ضد الخصوم في المرافعات وإلاّ تعرضوا

---

[1] – نقض 1989/6/1، مجموعة أحكام النقض، س44، رقم 100، ص594.

[2] – نقض 1996/1/14، مجموعة أحكام النقض، س47، رقم 9، ص72.

[3] – نقض 1994/5/20 مجموعة أحكام النقض، س45، رقم 121، ص776.

[4] – نقض 1976/1/5 مجموعة أحكام النقض س27، رقم 3 ص36. نقلا عن: د.محمد أمين الخرشة، المرجع السابق ،ص252.

[5]– تنص المادة 160 فقرة 1 من قانون الإجراءات الجزائية الجزائري على ما يلي :" تسحب من ملف التحقيق أوراق الإجراءات التي أبطلت وتودع لدى قلم كتاب المجلس القضائي ...".

[6]- تنص المادة 160 فقرة 2 من قانون الإجراءات الجزائية الجزائري على ما يلي :" ...و يخطر الرجوع إليها لاستنباط عناصر أو اتهامات ضد الخصوم في المرافعات و إلا تعرضوا لجزاء تأديبي بالنسبة للقضاة و محاكمة تأديبية للمحامين المدافعين أمام مجلسهم التأديبي."

لعقوبات تأديبية، فإذا كان القانون قد نص على معاقبة القضاة والمحامين المدافعين الذين يلجأون للإجراءات الباطلة الملغاة ليستمدوا منها دلائل اتهام ضد الأطراف الأخرى، فإنه بالعكس من ذلك لم ينص على أي جزاء بالنسبة للإجراءات القضائية المؤسسة على ما تضمنته الإجراءات الباطلة الملغاة[1].

فبالرجوع لمراقبة الإتصالات الإلكترونية على وجه الخصوص حيث أنّ قانون رقم (09-04) الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، قد أجاز مراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها مع مراعاة الضمانات والضوابط التي نص عليها المشرع الجزائري من خلال هذا القانون، وبالتالي عدم احترامها يؤدي حتما إلى استبعادها كدليل يعتمد عليه القاضي في حكمه.

فحسب اعتقادي و بالإستناد إلى رأي غالبية الفقهاء ومن بينهم الدكتور "ياسر الأمير فاروق" أنّ البطلان المترتب على مخالفة ضمانات وضوابط المراقبة هو بطلان مطلق وليس نسبي، وعليه فإنه يجوز إثارته في أي حالة كانت عليها الدعوى وعلى المحكمة أن تقضي به من تلقاء نفسها وهذا راجع إلى ما يلي :

- أنّ المراقبة تعتبر انتهاكا للخصوصية التي يتمتع بها الفرد وهي مصونة بنص الدستور كما أنّ المادة الرابعة(04) من القانون (09-04) السابق ذكره والمتضمن المواد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها حددت الجرائم والحالات التي تسمح باللجوء إلى المراقبة الإلكترونية، كما تتطلب هذه العملية إذنا مكتوبا من السلطة القضائية المختصة ولمدة محددة متمثلة في ستة (06) أشهر قابلة للتجديد واستنادا لذلك فإنّ مخالفة ما نص عليه القانون يترتب عليه بطلان مطلق.

- أمّا السبب الآخر فيرجع إلى أنّ المراقبة تعتبر إجراء منتج للدليل، غير أنه سبق وأن تم توضيح ضرورة أن يكون هذا الدليل مشروعا، فلا ينبغي أن يكون مستمدا من جريمة لأنه حينها يكون هذا الدليل باطلا بطلانا مطلقا، كما يقضي قانون العقوبات الجزائري بحرمة الرسائل البريدية والبرقيات ويعاقب على فضها أو تسهيل ذلك، كما يجرم ويعاقب على المساس بحرمة الحياة الخاصة للمواطن فيما يتعلق بالمكالمات والصور.

وإن كان المشرع الجزائري بموجب القانون رقم 06-22 المؤرخ في 20-12-2006 المتضمن قانون العقوبات قد أجاز في مرحلة التحريات الأولية إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية وكذا وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وتسجيل الكلام المتفوه به في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص، غير أنه أجاز ذلك في جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات،كما يجب أن تنفذ هذه

[1]-أ. أحمد الشافعي، المرجع السابق، ص 297-299.

العمليات بناء على إذن وتحت المراقبة المباشرة لوكيل الجمهورية المختص، وفي حالة فتح تحقيق قضائي تكون بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة المادة (65 مكرر 5) من ق.إ.ج.

ويؤدي عدم الأخذ بهذه الضمانات إلى استبعاد هذا الدليل، غير أنّ بطلان الإجراء المعيب واستبعاده في مجال المراقبة وضبط المراسلات لا يمس صحة الإجراءات السابقة مادامت هذه الإجراءات صحيحة قانونا دون أن تتأثر في وجودها بالإجراء الذي تقرر بطلانه، فبطلان المراقبة واعتراض المراسلات لا يؤثر على صحة إجراءات التحقيق السابقة عليه مثل التفتيش.

فالقاضي لا ينبغي له أن يبني حكمه على دليل متحصل من انتهاك الحقوق والحريات، ومادام أنّ الأمر كذلك يمكن القول بأنّ البطلان المترتب على مخالفة ضمانات المراقبة هو بطلان مطلق متعلق بالنظام العام ويترتب على ذلك أنه يجوز لمحكمة الموضوع أن تقضي به من تلقاء نفسها ولو لم يطلبه أحد الخصوم ويجوز الدفع به لأول مرة أمام المحكمة[1].

وهناك حكم صدر في سنة 1959 عن المحكمة العسكرية بالجزائر في ظروف سياسية متردية صرحت بمقتضاه المحكمة بأن التسجيل بآلة مسجلة يمكن أن يعتبر قرينة إثبات تضاف إلى غيرها من وسائل الإثبات[2].

وعليه يمكن القول أن موقف التشريعات قد اختلف من دولة لأخرى، إلا أنه لا يمكن بأي حال من الأحوال أن نفرط في حقوق و حريات الأفراد، و من أجل إقامة موازنة بين حقوق الأفراد و حق المجتمع ينبغي مراعاة الضمانات المنصوص عليها قانونا.

[1]-د.ياسر الأمير فاروق، المرجع السابق، ص714.

[2] - Trib Militaire d'Alger, 08/01/1958, JCP 1958 2 II 10564.

نقلا عن: د.محمد مروان، المرجع السابق، ج2، ص431.

المبحث الثاني : الجزاء الجنائي المترتب على عدم مشروعية الدليل الإلكتروني.

بعد أن تم التطرق للجزاء الإجرائي الذي أقرته التشريعات المختلفة لحماية حقوق وحريات الأفراد في مواجهة عدم مشروعية الدليل الإلكتروني، فإنّ هناك نوعا آخر من الجزاءات كان موضع إهتمام معظم التشريعات كالجزاء التأديبي والتعويض المدني الذي يلتزم مرتكب الفعل بدفعه نتيجة الضرر الذي نتج عن تصرفه والذي يخرج عن نطاق البحث ويدخل في نطاق الدراسات المتعمقة في القانون الإداري والمدني.

كما قد يكون جزاءا جنائيا إذا توافرت في هذا الإخلال عناصر جريمة معينة، وإن كنت سأخص بالذكر في هذه الدراسة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وكذا الإستخدام غير المشروع لوسائل المراقبة الإلكترونية مادام أن الموضوع يتعلق بالجريمة الإلكترونية .

ويعد الجزاء الجنائي وسيلة فعالة لإسباغ الحماية التامة على حرمة الحياة الخاصة للأفراد، فهو يختلف عن الجزاء الإجرائي إذ ينال ممن باشر الإجراء المخالف مع إنطوائه على عنصر الألم، فهو بالإضافة إلى ردعه للمعتدي ينذر غيره أيضا، ويتمثل ذلك في فرض العقوبة الجنائية على الأفعال التي تقع من الأشخاص الذين يباشرون عملا إجرائيا يشكل إعتداء على حقوق الإنسان وضماناته الأساسية المقررة له خلال إجراءات الدعوى الجزائية.

وتتم مساءلة ممثلي السلطة العامة المكلفين بمهام إدارية أو قضائية وعلى وجه الخصوص الذين يمارسون مهام الضبط القضائي نتيجة قيامهم بمخالفة شروط صحة العمل الإجرائي، فهي ناشئة عن ثبوت اقتراف الشخص فعلا غير مشروع يدخل دائرة النموذج التجريمي المعاقب عليه، فإذا استخدم ممثل السلطة العامة وسائل غير مشروعة للحصول على أدلة، فإنه يتعرض للمسؤولية الجنائية مهما كانت تبريرات السلطة العامة[1].

ويمكن القول أنّ معظم دول العالم أقرت بشكل أو بآخر الحق في الحياة الشخصية في واحد أو أكثر من مظاهره، وهذا لا يعني توفر حماية كافية لدى كافة الدول، كما أنه وفي الوقت الذي قد يوجد فيه حماية الخصوصية بمفهومها المادي أكثر شيوعا، غير أنّ فكرة الخصوصية وارتباطها بتقنية المعلومات هي أول مسائل الكمبيوتر من الوجهة التاريخية، وهي أول مناطق التساؤل عن مدى تأثير التقنية على النظام القانوني

[1] – د.محمد أمين الخرشة، المرجع السابق، ص 254.

ومسائله، وقد تزايدت في إطار التطور التكنولوجي الواسع والإستخدامات المتزايدة للحوسبة وإنشاء بنوك المعلومات وعمليات المعالجة الآلية للمعطيات، فتمس على نحو مباشر خصوصياتهم وأسرارهم.

وفي موازاة هذا التحول سرعان ما نمت الحاجة إلى إيجاد الوسائل القانونية والتقنية التي تضمن الحماية الفعالة للحياة الشخصية في العصر المعلوماتي عموما وشبكة الإنترنت على وجه الخصوص، كما تقي من الإعتداءات المحتملة على الحق في السرية والخصوصية .

وانسجاما مع حركة التشريع فالحماية الجزائية للحياة الشخصية قد شهدت مراحل ثلاثة، فالمرحلة الأولى تناولت الحماية الجنائية للشخص وأملاكه من أنشطة التفتيش وحماية المسكن وجسد الشخص وكل ما يتعلق به من الناحية المادية، أمّا المرحلة الثانية فتناولت حماية البيانات الشخصية من الإعتداءات في عصر الكمبيوتر ومن تم عصر الإنترنت والشبكات الرقمية إنطلاقا من عمليات المعالجة الآلية للمعطيات، أمّا المرحلة الثالثة فتناولت حماية الفرد من أنشطة الرقابة الإلكترونية[1].

ومادام أنّ الطبيعة الخاصة للجريمة الإلكترونية يترتب عنها مشكلات عديدة تختلف كل الإختلاف عن الجرائم التقليدية العادية، فهذه الجرائم كما سبق ذكره لا تترك أثرا ماديا في مسرح الجريمة كغيرها من الجرائم التي تقع في العالم المادي ، كما أنّ مرتكبيها يتميزون بذكاء خارق للعادة يجعل بإمكانهم التخلص من الدليل وإتلافه من أجل الإفلات من العقاب .

ولذلك ارتأيت في مرحلة أولى أن أتطرق للإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، وفي مرحلة ثانية يتم التطرق للإستخدامات غير المشروعة لوسائل المراقبة الإلكترونية، مع تفصيل كل هذه الجرائم والجزاءات المقررة لها من قبل المشرع الجزائري مع إجراء مقاربة مع التشريع الفرنسي والتشريع المصري.

المطلب الأول : المساس بأنظمة المعالجة الآلية للمعطيات.

إنّ أول حقيقة تاريخية تكرس في هذا المجال هي أنّ فكرة الخصوصية وارتباطها بتقنية المعلومات هي أول المسائل القانونية التي أثيرت عموما من الوجهة التاريخية، وهي أول مناطق التساؤل عن أثر التقنية على النظام القانوني ومسائله، وذلك نتيجة للتطور التكنولوجي الواسع وأجواء الإستخدامات المتزايدة لنظم المعلومات وإنشاء بنوك المعلومات وعمليات المعالجة الآلية للمعطيات، ولهذا فقد ارتبط مفهوم خصوصية

[1] – د.بولين أنطونيوس أيوب ، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، لبنان، ط 1، سنة 2009 ، ص18.

المعلومات بالخشية من مخاطر التقنية ذاتها، حيث تصبح المخاطر أوسع عندما لا تقيد عمليات المعالجة بأي قيد، وهذا ما دفع إلى ضرورة إبرام إتفاقيات في مجال حماية البيانات الشخصية عبر الحدود[1].

وعلى هذا الأساس، سيقسم هذا المطلب إلى فرعين، أتطرق في الفرع الأول لأثر المعالجة الآلية للمعطيات على الخصوصية المعلوماتية، أما الفرع الثاني فخصص لجرائم المعالجة الآلية للمعطيات.

الفرع الأول: أثر المعالجة الآلية للمعطيات على الخصوصية المعلوماتية.

تعمل تقنية المعلومات على تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها، كما أنّ استخدام الحاسب الآلي في مجال جمع ومعالجة البيانات المتمثلة بالحياة الخاصة قد خلف آثار إيجابية عريضة لا يستطيع أحد إنكارها خاصة في مجال تنظيم الدولة لشؤون الأفراد، وهذا ما أوجد ما يعرف ببنوك المعلومات.

ويقصد ببنك المعلومات تكوين قاعدة بيانات تفيد موضوعا معينا ويهدف لخدمة غرض معين، ومعالجتها بواسطة أجهزة الحاسبات الآلية لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة، ومن تم يمكن القول بأنّ هناك بنكا للمعلومات المالية أو القانونية أو الطبية أو الأمنية أو العسكرية، والحقيقة المؤكدة هو أنه لا يوجد تحديد قانوني لمصطلح بنوك المعلومات، أمّا من الوجهة الفنية فيقصد بها العمليات المختلفة للكمبيوتر من تسجيل وتصنيف البيانات[2]، و مما لا شك فيه أن بنوك المعلومات تعد أحد أهم مظاهر التقدم التكنولوجي في هذا العصر، إذ تعتبر الركيزة الأساسية في تطور المجتمع و تفعيل التنمية الإجتماعية و الإقتصادية[3].

كما تعرف أيضا بأنها: "مجموعة المعلومات التي يتم معالجتها إلكترونيا، وذلك من أجل بثها عبر شبكة الإنترنت، بحيث يمكن للمشترك الوصول إليها من خلال ربط الكمبيوتر الخاص به بشبكة الإنترنت"[4].

وبفعل الكفاءة العالية لوسائل التقنية والإمكانات غير المحدودة في مجال تحليل واسترجاع المعلومات، إتجهت مختلف دول العالم متمثلة في هيئاتها ومؤسساتها إلى إنشاء قواعد البيانات لتنظيم عملها، غير أنّ التوسع الهائل لاستخدام الكمبيوتر أثار مخاوف من إمكانات انتهاك الحياة الشخصية.

---

[1] -Valérie Sedaillan, Droit de l'internet, OP.cit, P 30..55 نقلا عن: د. بولين أنطونيوس، المرجع السابق، ص

[2]– د. أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، مصر، ط3، سنة 1982، ص 90.نقلا عن : د. بولين أنطونيوس، المرجع السابق، ص 86.

[3]– د. كاظم عطية، الحماية الجنائية لحرمة الحياة الخاصة في مواجهة مخاطر بنوك المعلومات، مجلة كلية الدراسات العليا، القاهرة، مصر، العدد 19، يوليو 2008، ص 04.

[4]– د. فاروق محمد أحمد الأباصيري، عقد الإشتراك في قواعد المعلومات عبر شبكة الإنترنت(دراسة تطبيقية لعقود التجارة الإلكترونية الدولية)، دار الجامعة الجديدة، القاهرة، مصر، بدون طبعة، سنة 2006، ص 51.

والواقع أنّ هناك كثير من الأشكال التي تهدد بها أجهزة بنوك المعلومات حرمة الحياة الخاصة للفرد، بحيث يمكن تجميع كل المعلومات المسجلة التي تكون غالبا شخصية وخاصة، ومن أهم الأخطار التي يمكن أن تهدد حرمة الحياة الخاصة للأفراد وبالتالي قد تسبب مشاكل تتمثل في السماح بجمع البيانات أو المعلومات عن الأشخاص مع عدم معرفة أوجه استخدامها في المستقبل[1]، وفيما يلي سيتم بيان مفهوم نظام المعالجة الآلية للمعطيات، و تأثير بنوك المعلومات على الحق في حرمة الحياة الخاصة.

البند الأول: مفهوم نظام المعالجة الآلية للمعطيات.

كان مجلس الشيوخ قد اقترح تعريفا لنظام المعالجة الآلية للمعطيات بأنه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات، على أن يكون هذا المركب خاضع لحماية فنية"[2].

وبالرجوع إلى هذا التعريف فهو يتضمن عنصرين ، أولهما يشتمل على العناصر المختلفة التي يتكون منها المركب، والثاني يتضمن العلاقات التي تربط بين هذه العناصر وتوحدها نحو تحقيق هدف واحد وهو المعالجة الآلية للمعطيات، كما أنّ العناصر المادية والمعنوية التي يتكون منها المركب مثال ذلك الذاكرة والبرامج، المعطيات، أجهزة الربط جاءت على سبيل المثال لا الحصر، فلا يتوافر نظام المعالجة الآلية للمعطيات، ولا تقع أي جريمة من جرائم الإعتداء المنصوص عليها إذا وقع الإعتداء على جهاز حاسب لم يدخل الخدمة بعد، أو على الأجهزة التي مازالت في مرحلة التجربة، أو حتى على الأنظمة التي خرجت من الخدمة تماما[3].

أمّا مصطلح الحماية الفنية للنظام، فهو ذلك الإجراء الوقائي الذي يتخذه صاحب النظام أو صانع البرنامج أثناء وضعه له للحد من الإعتداءات الخارجية التي قد تقع عليه[4].

غير أن السؤال المطروح يتعلق حول ضرورة وجود أو عدم وجود الحماية الفنية للنظام كشرط للتمتع بالحماية الجنائية؟

تنقسم الأنظمة من هذه الزاوية إلى ثلاثة أنظمة : أنظمة مفتوحة للجمهور ، أنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية وأنظمة قاصرة على أصحاب الحق فيها وتتمتع بحماية فنية، فالنوع الثالث من تلك الأنظمة هو الذي يتمتع بالحماية الجنائية، أما النوع الأول والثاني فلا يتمتعان بتلك

---

[1]- د. بولين أنطونيوس، المرجع السابق، ص87.

[2]– د. علي عبد القادر قهوجي، المرجع السابق، ص120.

[3]– أنظر في ذلك: أ.أمال قارة، المرجع السابق،ص 103.وكذلك :د.عبد الفتاح بيومي حجازي،التجارة الإلكترونية وحمايتها القانونية،المرجع السابق،ص 121.

[4]– أ. خثير مسعود، المرجع السابق، ص110.

الحماية، لأن الحماية الجنائية في نظرهم يجب أن تقتصر على الأنظمة المحمية فنيا، لأنه من الطبيعي أن القانون الجنائي لا يحمي إلا الأشخاص الذين لهم حرص على أموالهم.

وبالرجوع إلى النصوص المتعلقة بجرائم الإعتداء على أنظمة المعالجة للمعطيات فلا يوجد ما يتضمن شرط الحماية الفنية، ومن المبادئ العامة المستقرة في تفسير القانون الجنائي أنه لا يجوز تقييد النص المطلق أو تخصيص النص العام إلا إذا وجد نص يجيز ذلك، ولذلك فإن عدم ذكر المشرع لشرط الحماية الفنية يعني أن المشرع أراد استبعاده[1].

البند الثاني:تأثير بنوك المعلومات على الحق في حرمة الحياة الخاصة .

ظهرت عدة مخاطر مست حريات الأفراد بسبب جمع معلومات شخصية عنهم قبل ظهور و انتشار أجهزة الكمبيوتر و الإستعانة بها في تخزين هذه المعلومات، و ازدادت هذه المخاطر مع انتشار استعمال الكمبيوتر، و هذا التهديد للحياة الخاصة يتحقق سواء كانت هذه المعلومات كاذبة أو صحيحة مادام صاحب الشأن يعترض على من يقوم بجمعها و تخزينها بدون مبرر قانوني[2].

فالحاسب الآلي أصبح يمثل خطرا أوسع مدى بكثير من الوسائل التقليدية التي سبق وأن عرفتها البشرية كوسيلة لحفظ ومراجعة البيانات الخاصة بالأفراد وذلك راجع إلى ما يلي[3]:

أولا: السعة غير المحدودة لذاكرة الحاسب الآلي من الناحية العملية مع تضاؤل حجم وسائط أوعية البيانات، كما أنّ هناك أنظمة كمبيوترية في بلجيكا حيث المقر العام لحلف شمال الأطلسي المعروف باسم "الناتو" تختزن فيها المعلومات حول كل شخص على الكرة الأرضية.

ثانيا: إمكانية اختراق ذاكرة الحاسب الآلي عن بعد، حيث يمكن ألاّ يقتصر هذا الإختراق على مجرد الإطلاع على ما تحتويه هذه الذاكرة من بيانات أو معلومات، بل يتعدى الأمر ذلك ليصل إلى حد استنساخ هذه البيانات الأمر الذي يعد تمهيدا لإساءة استعمالها فيما بعد.

ثالثا: تتجلى مخاطر الحاسب الآلي على الحياة الشخصية حينما يتم ربط أجهزة الكمبيوتر المختلفة ببعضها أو بكمبيوتر مركزي أو بنوع من الشبكات العامة المخصصة للإتصال، على نحو يسمح بأن تتبادل هذه الأجهزة على تعدد الغرض منها وتبادل البيانات التي يحتويها فيما بينها.

---

[1] – أ. أمال قارة، المرجع السابق،ص 105.

[2] – د. غنام محمد غنام، الحماية الإدارية والجنائية للأفراد عند تجميع بياناتهم الشخصية في أجهزة الكمبيوتر، المرجع السابق، ص 87.

[3] - د. بولين أنطونيوس، المرجع السابق، ص 99.

فتقنية الوسائط المتعددة (Multimédia) التي هي عبارة عن ناقل معلوماتي جديد يجمع في الوقت ذاته الصوت والصورة الثابتة والمتحركة والنص والبيانات الوافدة بدورها من وسائط أو وسائل مختلفة، ويتميز بالتفاعلية فيما بين مختلف المعطيات التي يتكون منها هذا العمل، حيث يكون من شأن ذلك أن يتم ربط هذه البيانات بعضها ببعض من أجل استكمالها والقيام بتحليلها ومعالجتها التي قد تؤدي إلى معلومات أو بيانات جديدة.

رابعا: يلاحظ تمكن العديد من مقتحمي الكمبيوتر من الدخول إلى العديد من شبكات الكمبيوتر خاصة شبكة الإنترنت عن طريق استغلالهم مواطن الضعف في منظومة الأمن.

خامسا: إنّ الأمر يبلغ أشده فيما لو قامت الحكومات بذاتها بالتجسس على مراسلات الأفراد عن طريق التنصت والمراقبة الإلكترونية، ولا أدل على ذلك من الشبكة المعروفة "كارنيفور" والتي استخدمت كمشروع تتنصت فيه الحكومة الأمريكية على مزودي خدمات الإنترنت لمراقبة رسائل البريد الإلكتروني.

كذلك قد يثور التساؤل حول مدى صلاحية تطبيق أحكام قانون الأرشيف الجزائري على حالة إفشاء المعلومات الشخصية التي يتم معالجتها إلكترونيا ؟

إنّ قانون الأرشيف الجزائري[1] في مادته الثانية (02) قد عرف الوثائق الأرشيفية بالوثائق التي تتضمن معلومات مهما كان تاريخها أو شكلها وسندها المادي ، ناتجة أو متحصلة من كل شخص طبيعي أو معنوي، ومن كل مصلحة أو جهاز عمومي أو خاص أثناء ممارستهما نشاطهما، فيلاحظ أنّ المشرع كان حريصا على عدم إفشاء الأسرار المتضمنة في الوثائق الأرشيفية المتعلقة بحرمة الحياة الخاصة للأشخاص، وكذلك الوثائق الكاملة للمعلومات الفردية الصحية والملفات المرتبطة بحرمة الحياة الخاصة لهم طبقا لنص المادة (12) من نفس القانون، وأوجب القانون حق الإطلاع بترخيص من المالك أو الحائز بحيث يعتبر الوثائق ملكية خاصة طبقا لنص المادة (24) إلى نص المادة (28) من ذات القانون.

وبالتالي لا يوجد مجال لتطبيق أحكام نصوص هذا القانون على حالة إفشاء المعلومات المختزنة في بنوك المعلومات لخلوه من أي لفظ يدل على ذلك من جهة، ومن جهة أخرى فإنّ القياس ممنوع في تفسير نصوص القانون الجنائي[2].

---

[1]- قانون رقم 09/88 المؤرخ في26 جانفي1988 المتضمن قانون الأرشيف الجزائري.

[2]- د.عاقلي فضيلة، الحماية القانونية للحق في حرمة الحياة الخاصة(دراسة مقارنة)، رسالة دكتوراه، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، سنة2012، ص172.

الفرع الثاني : جرائم المعالجة الآلية للمعطيات.

مع الإنتشار الكبير في استخدام الحاسب الآلي وشبكة الإنترنت ظهرت هذه النوعية من الجرائم، وفي الواقع تختلف أهداف الإختراقات، فقد تكون البيانات والمعلومات هي الهدف المباشر، وقد يقصد المخترق بفعلته إظهار قدرته ومهارته على اختراق الحاسب الآلي، أو لإظهار وجود ثغرات في الجهاز المخترق[1].

وسأتطرق من خلال هذا الفرع لجرائم المساس بأنظمة المعالجة الآلية للمعطيات في القانون الجزائري مع إجراء مقاربة مع القانون المصري والقانون الفرنسي.

البند الأول: جرائم المعالجة الآلية للمعطيات في القانون الجزائري.

أولا: الركن المادي: يتمثل في أشكال الإعتداء على نظم المعالجة الآلية للمعطيات ويتمثل فيما يلي:

1. الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

نصت عليه المادة (02)[2] من إتفاقية بودابست بشأن الجرائم الإلكترونية، والمادة (06)[3] من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، أما المشرع الجزائري فقد نص عليه في المادة (394 مكرر)[4] المضافة بالقانون (04-15)[5]، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء عن طريق الغش في كل أوجزء من منظومة المعالجة الآلية للمعطيات، بينما الصورة المشددة تتحقق في الحالة التي يترتب فيها عن الدخول أو البقاء عن طريق الغش إمّا حذف أو تغيير لمعطيات المنظومة أو إذا نتج عن ذلك تخريب لنظام إشتغال المنظومة.

---

[1]- د. أسامة بن غانم العبيدي، جريمة الدخول غير المشروع إلى النظام المعلوماتي (دراسة قانونية في ضوء القوانين المقارنة)، مجلة دراسات المعلومات، الرياض، السعودية، العدد الرابع عشر، ماي 2012، ص 11.

[2] - Article 2 du (C.C.C) : Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

[3]- تنص المادة 06 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي :" جريمة الدخول غير المشروع : أ- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الإستمرار به .

ب- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الإتصال أو الإستمرار بهذا الإتصال : محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الإتصال وإلحاق الضرر بالمستخدمين والمستفيدين، الحصول على معلومات حكومية سرية."

[4] – تنص المادة 394 مكرر من قانون العقوبات على ما يلي: " "يعاقب بالحبس من ثلاثة (03) أشهر إلى سنة (01) وبغرامة من 50.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة (06) أشهر إلى سنتين (02) والغرامة من 50000 دج إلى 300.000 دج."لقد تم الرفع من قيمة الغرامة طبقا للمادة 467 مكرر من القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المتضمن قانون العقوبات .

[5] – الأمر رقم 156/66 المؤرخ في 8 يونيو 1966 المعدل والمتمم بالقانون رقم 15/04 المؤرخ في 2004/11/10 والمتضمن قانون العقوبات الجزائري.

1.1- الصورة البسيطة: تتمثل في فعل الدخول وفعل البقاء.

أ. فعل الدخول:

لا يقصد بالدخول هنا الدخول بالمعنى المادي أي الدخول إلى مكان أو مسكن وفي نفس الإتجاه إلى جهاز الحاسب الآلي، وإنما يجب أن ينظر إليه كظاهرة معنوية تتمثل في الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات، ولم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم بها الدخول إلى النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر.

وقد يتم هذا الإختراق عن طريق برامج متطورة يستخدمها كل من يملك خبرة في استعمالها، وتقع هذه الجريمة من كل إنسان أيا كانت صفته سواء كان يعمل في مجال الأنظمة أم لا يعمل، وسواء كان يستطيع أن يستفيد من الدخول أم لا، فيكفي أن يكون الجاني ليس ممن يكون لهم الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، فتتوافر الجريمة في كل حالة يكون فيها الدخول مخالفا لشروط الدخول التي نص عليها القانون أو الإتفاق أو مخالفا لإدارة من له حق السيطرة على النظام.

وذلك كما هو الحال إذا كان القانون يفرض سرية معينة بالنسبة لبعض الأنظمة مثل أسرار الدولة أو السرية المتعلقة بالمعلومات الذاتية أو الإسمية أو سر المهنة أو أسرار الأشخاص مثل أسرار الحياة الخاصة المهنية أو أي معلومات يجمعها الإنسان في نظام ولا يترك الإطلاع عليها لأي إنسان[1]، كالمواقع التي تزاول التجارة الإلكترونية مباشرة على الشبكة تحتفظ بالبيانات المتعلقة بالصفقات التي يجريها المتسوقون معها وبمعلومات شخصية حول هؤلاء وينسحب ذلك على الوسطاء ومختلف الهيئات التي تؤدي دور الوساطة بين التاجر وزبائنه، وفي الواقع أنّ غالبية هذه المواقع تحمل زوارها من مستخدمي الشبكة على ملء استمارات إلكترونية تحوي معلومات شخصية عنهم وذلك قبل أن تسمح لهم بالنفاذ إلى الخدمة المقصودة.

فالحق في الحياة الخاصة من الحقوق اللازمة للإنسان والتي تعتبر إحدى وسائل حمايتها وتخزينها لمدة محددة، وهذا يعتبر إحدى الضمانات الوقائية لحماية الحياة الخاصة لأنّ الإحتفاظ ولمدة طويلة ببيانات ومعلومات قابلة للتغيير والتطور يؤدي استرجاعها بعد مدة طويلة من الزمن إلى الإضرار بصاحبها[2].

[1] – أ.أمال قارة، المرجع السابق ، ص107.

[2] - د. بولين أنطونيوس، المرجع السابق، ص 134.

ويرتكب الجريمة من يعمل على الآلة ولكن بنظام معين فيدخل في نظام آخر عليها، كما تقع الجريمة سواء تم الدخول إلى النظام كله أم إلى جزء منه فقط، أي يكفي لتوافر الجريمة أن يتم الدخول على بعض عناصر النظام أو على عنصر واحد منه بشرط أن يكون العنصر الذي يتم الدخول إليه يدخل في برنامج متكامل قابل للتشغيل، فالجريمة تقوم بفعل الدخول إلى النظام مجرد عن أي نتيجة أخرى، فلا يشترط لقيامها إلتقاط المتدخل للمعلومات التي يحتويها النظام أو بعضها أو استعمال تلك المعلومات، بل أنّ الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام[1]، كما لا تتوافر الجريمة إذا اقتصر دور الجاني على مجرد قراءة الشاشة دون الولوج إلى داخل النظام، إذ وبهذه الأفعال لا تقوم جريمة الدخول غير المشروع للنظام المعلوماتي[2].

ب. **فعل البقاء:**

يقصد بفعل البقاء التواجد داخل النظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام وقد يجتمعان، ويكون البقاء معاقبا عليه مستقلا حين يكون الدخول إلى النظام مشروعا كالحالة التي يتحقق الدخول على النظام بالصدفة أو عن طريق الخطأ، فيجب على المتدخل أن يقطع وجوده وينسحب فورا فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي.

كما يكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح له البقاء بداخل النظام أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الرؤية والإطلاع فقط، وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الفرض الذي لا يكون فيه للجاني الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه ثم يبقى داخل النظام بعد ذلك.

فجريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام أو يستمر في التجول بداخله بعد انتهاء الوقت المحدد، لأنّ الغرض يتعلق بدخول غير مشروع أي مع علم الجاني أنه ليس له حق الدخول فإذا دخل وظل ساكنا تظل الجريمة جريمة دخول إلى النظام، أما إذا بدأ في التجول فإنّ جريمة البقاء داخل النظام تبدأ منذ تلك اللحظة لأنّ دخوله غير مشروع واستمراره فيه كذلك غير مشروع ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام[3].

---

[1] – أ. أمال قارة، المرجع السابق، ص 113.

[2] – د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 30.

[3] – أ. أمال قارة، المرجع السابق، ص 110-112.

2.1- الصورة المشددة :

نصت المادة (394 مكرر فقرة 3/2) من قانون العقوبات على ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام، ويتحقق هذان الظرفان عند ما ينتج عن الدخول أو البقاء إمّا محو أو تعديل المعطيات التي يحتويها النظام وإمّا عدم صلاحية النظام لأداء وظائفه، ويكفي لتوافر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع والنتيجة الضارة، ولا يشترط أن تكون تلك النتيجة الضارة مقصودة لأنّ المشرع نص على تجريم الإعتداء المقصود على النظام عن طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة[1].

2. الإعتداءات العمدية على المعطيات.

نصت عليه المواد (03[2]، 04[3]) من إتفاقية بودابست بشأن الجرائم الإلكترونية، والمادة (08)[4] من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، كما نص المشرع الجزائري على هذه الجريمة في المادة (394 مكرر1)[5] من قانون العقوبات، فالإعتداء على البيانات والبرامج داخل النظام المعلوماتي يتخذ إحدى الصورتين :

الصورة الأولى: أن يتم محو البيانات والمعلومات كلية وتدميرها إلكترونيا.

الصورة الثانية: أن يتم تشويه المعلومة أو البرنامج عن طريق تعديل البيانات أو تعديل طرق معالجتها أو وسائل إنتقالها.

---

[1] - أ. أمال قارة، المرجع السابق، ص 114.

[2] - Article 3 du (C.C.C) : Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

[3] - Article 4 du (C.C.C) : - Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.
- Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

[4]- تنص المادة 08 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على ما يلي :" الإعتداء على سلامة البيانات : – تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.
– للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، أن تتسبب بضرر جسيم."

[5]- تنص المادة 394 مكرر 1 من قانون العقوبات: "يعاقب بالحبس من ستة (06) أشهر إلى ثلاثة (03) سنوات وبغرامة من 500000 دج إلى 4000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي تتضمنها". لقد تم الرفع من قيمة الغرامة طبقا للمادة 467 مكرر من القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المتضمن قانون العقوبات .

وتتنوع أساليب الإتلاف التي قد تكون نتيجة فعل الدخول غير المشروع إلى النظام المعلوماتي أوالبقاء فيه بدون إذن، أو قد تكون نتيجة إستخدام الطرق التقنية والفنية كاستخدام فيروسات الحاسب الآلي[1].

كما يرى الفقهاء أنّ النشاط الإجرامي في هذه الجريمة ينحصر في أفعال الإدخال والمحو والتعديل ويكفي توافر أحدها لقيام الجريمة، فلا يشترط اجتماعها معا حتى يتوافر النشاط الإجرامي فيها ومن تم قيام الركن المادي في الجريمة.

1.2- فعل الإدخال :

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية أم كان عليها معطيات من قبل، ويتحقق هذا الفعل في الفرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة، وذلك حين يستخدم رقمه الخاص والسري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب يضيف معطيات جديدة، أو استعمال البطاقة من غير صاحبها وذلك في حالة سرقتها أو فقدانها أو تزويرها[2].

ويشمل الإدخال إدخال معلومات وهمية ويقصد بذلك إدخال بيانات في نظم المعالجة الآلية لم تكن موجودة من قبل، وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة[3]، كما يشمل كل فعل يؤدي إلى إزالة معلومات أو معطيات بصورة غير مشروعة، أو إلى تعديل مضمونها.

ويشترط لتجريم هذه الأفعال أن تكون المعطيات و المعلومات موضوع الجريمة داخل النظام، كما أن موضوع الجريمة هو المعلومات التي يجري عليها معالجات معينة و ترتيبها و تنظيمها و تحليلها بغرض الإستفادة منها و الحصول على نتائج معينة من خلال استخدامها[4].

---

[1] – أ. نبيل صقر، جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 138.

[2] – أنظر على التوالي : أ. أمال قارة، المرجع السابق، ص 121. وكذلك: د.عبد الفتاح بيومي حجازي، الأحداث والإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2004، ص46.

[3]– د.هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، ط1، سنة 1992، ص 569.نقلا عن: د. بولين أنطونيوس، المرجع السابق، ص 431.

[4]– د. بولين أنطونيوس، المرجع السابق، ص 431.

2.2- فعل المحو:

يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[1]، وبما أن عملية المحو تأتي بعد عملية الدخول، يثار التساؤل عما إذا كان هذا الدخول مشروع وكذا عملية المحو إذا تمت عن حسن أو سوء نية[2] .

فإتلاف البيانات سواء بمحوها أو تدميرها إلكترونيا يثير تكييفها جنائيا إختلافا ملموسا بحسب الغاية التي يهدف إليها المجرم المعلوماتي من واقعة الإتلاف، ففي الحالة الأولى تشكل الواقعة إتلافا بالمعنى القانوني إذا كانت هذه المعلومات هي هدف الجاني بقصد الإضرار بالغير أي دون أن تتجه إرادته إلى ارتكاب جريمة أخرى[3].

3.2- فعل التعديل :

يقصد بفعل التعديل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو تعديلها، وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة أو برامج الفيروسات بصفة عامة، وهذه الأفعال المتمثلة في الإدخال والمحو والتعديل وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى ولو تضمن إعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات، فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينها لأنّ كل تلك الأفعال لا تنطوي لا على إدخال ولا على تعديل بالمعنى السابق[4].

فالتغيير أو التبديل الذي يقع على المعطيات أو الأوامر المخزنة والمنقولة عبر شبكة الإنترنت لا تنطبق نصوص التزوير عليها، إذ أنّ الإعتداء على البيانات بتغيير الحقيقة لا يعد تزويرا إلاّ إذا خرجت في صورة محرر مكتوب، ولكن قد تقع جريمة أخرى ولذلك ظهر إتجاه ينادي بالمساواة بين المستند الورقي ومستخرجات الحاسب الآلي من أسطوانات ممغنطة وشرائط ممغنطة وما يسجل في ذاكرة الحاسب الآلي.

---

[1] - أ. أمال قارة، المرجع السابق، ص 122.

[2] - Raymond Gassin, Fraude informatique, Dalloz, France, 1997, P 27.

[3] - أ. نبيل صقر، جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 138.

[4] - Jean Pierre Chamoux, La loi sur la fraude informatique, de nouvelles incrimination, J.C.P, 1989, p223.

نقلا عن: أ. أمال قارة،، المرجع السابق، ص 126.

ويكون تغيير الحقيقة في نطاق المعالجة الآلية للمعطيات عن طريق الحذف بإزالة كلمة أو رمز معين أو عن طريق الإضافة بزيادة عبارات أو بيانات غير صحيحة أو بتغيير محتوى الرسائل المنقولة[1]، وعليه فإن جريمة التلاعب بالبيانات داخل النظام المعلوماتي وكذا جريمة الدخول غير المشروع تتمان عن طريق برامج معينة وذلك من أجل الإخلال بالعمل داخل النظام[2].

فالتلاعب بالبيانات يمكن أن يحصل تبعا للجهة التي يصدر عنها بإحدى صورتين:

الصورة الأولى : التلاعب في بيانات شخصية من طرف أشخاص لا يملكون هذا الحق، وذلك من أجل تحقيق غايات دنيئة كاستغلالها من أجل انتهاك السرية[3].

أما **الصورة الثانية** : إستعمال بيانات شخصية غير حقيقية والمتمثلة بجمع أو معالجة أو نشر بيانات شخصية غير صحيحة من قبل المرخص لهم بذلك قانونا[4].

كما وفر المشرع الجزائري الحماية الجزائية للمعطيات في حد ذاته من خلال تجريمه السلوكات التالية :

– نص المادة (394 مكرر 2) يستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام معالجة آلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة على أشرطة أو أقراص أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية، مادامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

– نص المادة (394 مكرر2/2) يجرم أفعال الحيازة، الإفشاء، النشر، الإستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات[5].

---

[1] – د. بولين أنطونيوس ، المرجع السابق، ص 444.

[2] - Alain Hollande et Xavier Linant de Bellefonds, Pratique du droit de l'informatique et de l'internet, Delmas, France, 2008, p 220.

[3] -Philippe Boure, Internet et la lutte contre la cybercriminalité , la gazette du palais,N°23, Janvier 2003, P11.

[4] – د. بولين أنطونيوس، المرجع السابق، ص 446.

[5] – أ. أمال قارة، المرجع السابق، ص 123.

ثانيا :الركن المعنوي:

إنّ الركن المعنوي في مختلف الإعتداءات الماسة بالأنظمة المعلوماتية يتخذ صورة القصد الجنائي إضافة إلى نية الغش.

فبالنسبة لجريمة الدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات هي جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة، فيلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء وأن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو نفاذه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان مشروع كما لا يتوفر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، فإذا توافر القصد الجنائي بعنصرية العلم والإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى ولو كان الباعث هو الفضول[1].

أمّا بالنسبة لنية الغش تبدو من خلال الغش الذي يتم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام بالنسبة للبقاء، فيستنتج من العمليات التي تمت داخل النظام[2].

أمّا بالنسبة لجريمة الإتلاف تعد من الجرائم العمدية التي لا يكتفي القول بتوافرها في حق الجاني مجرد توافر ركنها المادي وإنما يتطلب الأمر أن يتوافر بجانب هذا الركن ركنا معنويا يتمثل في القصد الجنائي، كما أنها لا تتطلب قصدا خاصا وإنما يكتفي بشأنها القصد العام بعنصريه العلم والإرادة، فيتوافر العلم في حالة إذا كان الجاني عالما بأنّ من شأن سلوكه إتلاف مال الغير بصورة تذهب بقيمته كلها أو بعضها بدون سند مشروع مع علمه لملكية هذا الغير للمال[3].

كما أنّ الإعتداءات العمدية على المعطيات تعد جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصرية العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بأنّ نشاطه الجرمي يترتب عليه التلاعب في المعطيات، ويعلم أيضا أنّ ليس له الحق في القيام بذلك وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته[4].

---

[1] – د. علي عبد القادر قهوجي، المرجع السابق، ص 137. نقلا عن: أ.أمال قارة، المرجع السابق، ص124.

[2] – أ.أمال قارة، المرجع السابق، ص124.

[3] – د.أحمد خليفة الملط، المرجع السابق، ص548.

[4] – د. علي عبد القادر قهوجي، المرجع السابق، ص 145. نقلا عن: أ.أمال قارة، المرجع السابق، ص125.

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير، وإن كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي إلاّ أنه ليس عنصرا في الجريمة.

أمّا استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وذلك إمّا بالتصميم أو البحث أو التجميع أو النشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، هذا الإستخدام يجب أن يكون عمدا وبطريق الغش أي توافر القصد الجنائي العام إضافة إلى القصد الخاص المتمثل في نية الغش[1].

ثالثا : العقوبات المترتبة على المساس بأنظمة المعالجة الآلية للمعطيات.

سأتطرق فيما يلي للجزاءات التي قررها المشرع الجزائري فيما يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات سواء تعلق الأمر بالعقوبات المتعلقة الشخص الطبيعي أو الشخص المعنوي أو عقوبة الإتفاق الجنائي أو الشروع في الجريمة .

1. العقوبات المتعلقة بالشخص الطبيعي.

بالنسبة لدخول منظومة معلوماتية والبقاء فيها عن طريق الغش، فإذا كانت هذه الجريمة بسيطة فالعقوبة المقررة هي ثلاثة (03) أشهر إلى سنة (01) حبس و50000 دج إلى 100.000دج غرامة طبقا للمادة (394 مكرر فقرة 1)، إلا أنه عند الرفع من قيمة الغرامة طبقا للمادة 467 مكرر تصبح الغرامة من 100.000دج إلى 200.000دج، أمّا في حالة ما إذا كانت الجريمة مشددة أي ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة أو تخريب لنظام أشغال المنظومة فتكون العقوبة الحبس من ستة أشهر (06) إلى سنتين (02) وغرامة من 50000 دج إلى 150000 دج طبقا لنص المادة (394 مكرر فقرة 3)، إلا أنه عند الرفع من قيمة الغرامة طبقا للمادة 467 مكرر تصبح الغرامة من 150.000دج إلى 300.000دج.

وطبقا لنص المادة (394 مكرر 1) فالعقوبة المقررة للإعتداء العمدي على المعطيات الموجودة داخل النظام هي الحبس من ستة أشهر (06) إلى ثلاثة سنوات (03) وغرامة من 500000 دج إلى 2000.000 دج، إلا أنه عند الرفع من قيمة الغرامة المالية طبقا للمادة 467 مكرر تصبح الغرامة من

[1] – أ.أمال قارة، المرجع السابق، ص126.

500.000دج إلى 4000.000دج، أمّا العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية فالعقوبة المقررة هي الحبس من شهرين (02) إلى ثلاثة سنوات (03) وغرامة من 1000.000 دج إلى 5000.000دج طبقا لنص المادة(394 مكرر2) من قانون العقوبات، إلا أنه عند الرفع من قيمة الغرامة طبقا للمادة 467 مكرر تصبح الغرامة من 1000.000دج إلى 10.000.000دج.

وتجدر الإشارة إلى أنّ العقوبات التي تم التطرق إليها تتعلق بالعقوبات الأصلية، أمّا العقوبات التكميلية فقد نصت عليها المادة (394 مكرر 6) من قانون العقوبات والمتمثلة فيما يلي :

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

- **إغلاق المواقع** : أي المواقع التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية .

- **إغلاق المحل** :كإغلاق المقهى الإلكتروني الذي ترتكب فيه مثل هذه الجرائم بشرط توافر عنصر العلم لدى مالكها.

أمّا بالنسبة للظروف المشددة فقد نصت المادة (394 مكرر فقرة 3،2) على ظرف تشدد به عقوبة الدخول أو البقاء غير المشروع داخل النظام، وذلك عندما ينتج عن الدخول أو البقاء غير المشروع حذف أو تغيير المعطيات وكذا تخريب نظام إشتغال المنظومة، ففي الحالة الأولى تضاعف العقوبات المقررة في المادة (1/394 مكرر)، وفي الحالة الثانية تكون العقوبة الحبس من ستة أشهر (06) إلى سنتين (02) والغرامة من 50.000 دج إلى 300.000 دج، كما نصت المادة (394 مكرر 3) على أن تضاعف العقوبات المقررة وذلك إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام[1].

2. العقوبات المتعلقة بالشخص المعنوي.

إنّ المسؤولية الجزائية للشخص المعنوي لا تغني عن معاقبة الأشخاص الطبيعيين إذا كانوا فاعلين أو شركاء في الجريمة ، فالعقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح بمقتضى نص المادة (18 مكرر) من القانون (15/04) السالف الذكر تتمثل فيما يلي :

[1]-أ. أمال قارة، المرجع السابق، ص 128.

- الغرامة التي تساوي من مرة (01) إلى خمس 5 مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة، هذا بالإضافة إلى واحدة أو أكثر من العقوبات التكميلية الآتية (القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006):

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات .

أمّا بالنسبة لعقوبة الغرامة المطبقة على الشخص المعنوي عند ارتكابه إحدى الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة (394 مكرر4)[1] من قانون العقوبات خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

3. عقوبة المشاركة في الإعداد للجرائم الماسة بالأنظمة المعلوماتية.

بالنسبة للمجموعة أو الإتفاق يستوي أن يكون أعضاء الإتفاق في صورة شركة أو مؤسسة أو شخص معنوي أو جماعة، فالجنح التي يشكل تحضيرها هدف الإتفاق المنصوص عليه بالمادة (394 مكرر 5)[2] من قانون العقوبات هي الجنح الماسة بالأنظمة المعلوماتية، غير أنّ التحضير لا يكفي بل يجب أن يتم تجسيده بفعل مادي، وكذا توافر القصد الجنائي لدى أعضاء الجماعة والمتمثل في توافر العلم لدى كل منهم بأنه عضو في الجماعة الإجرامية[3]، كما لا يتطلب أن يكون هناك إجتماع حقيقي، وإنما يتصور الإتفاق الجنائي بمجرد إنتقال كلمة السر من شخص إلى آخر وإن لم يكن بينهما معرفة سابقة[4].

---

[1]- تنص المادة 394 مكرر 4 من قانون العقوبات الجزائري على ما يلي :" يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي ."

[2]- تنص المادة 394 مكرر 5 من قانون العقوبات الجزائري على ما يلي :" كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها ."

[3]- أ. أمال قارة، المرجع السابق، ص 131.

[4] - أ. مسعود خثير، المرجع السابق، ص 129.

4. عقوبة الشروع في الجريمة.

يعاقب المشرع على الشروع في ارتكاب الجنح المنصوص عليها بالعقوبات المقررة للجنحة ذاتها، أي أنّ المشرع جعل الشروع في إحدى لجرائم الماسة بالأنظمة المعلوماتية معاقب عليه بنفس عقوبة الجريمة التامة طبقا لنص المادة (394 مكرر7)[1].

ومن التطبيقات القضائية عن جرائم المساس بأنظمة المعالجة الآلية، ما ذهبت إليه محكمة سيدي بلعباس، في قضية تتلخص وقائعها، أنه بتاريخ 2013/01/06 تقدم المدعو(ب.ب) بشكوى أمام مصالح أمن دائرة سيدي بلعباس، مفادها أنه اتفق مع(ص.م) من أجل إعداد موقع إلكتروني خاص بالفندق باعتباره مختص في الإعلام الآلي من أجل القيام بعمليات الحجز من طرف الزبائن مقابل تلقيه مستحقاته المالية، إلا أنه قام بغلق الموقع مما سبب خسائر للفندق وذلك لمدة 12 ساعة، وعليه أدين المتهم (ص.م) عن جرم المساس بأنظمة المعالجة الآلية بعقوبة الحبس والغرامة [2].

إلا أنه بناءا على الإستئناف المرفوع من طرف المتهم والضحية، وعند سماع المشتكى منه صرح بأنه بالفعل قام بإعداد موقع إلكتروني لفندق الشاكي، وأنه صرف أمولا طائلة بلغت 350 دولار أمريكي دون تلقيه كامل مستحقاته المالية لذلك قام بغلقه ثم أعاد تشغيله.

حيث أن المتهم (ص.م) لم يدخل منظومة المعالجة الآلية لفندق الضحية عن طريق الغش، ولم يقم بحذف أو تغيير ما جاء فيها مادام أنه هو من أنشأها وهو من دفع مستحقات فتح هذا الموقع مثلما تبينه الوثائق، فنظرا لعدم توافر الركن المادي للجريمة، يكون الجرم غير ثابت في حق المتهم ويكون قاضي أول درجة قد جانب الصواب عندما قضى بإدانته، فتقرر إلغاء الحكم المستأنف فيه وبراءة المتهم[3].

وفي قضية أخرى تم كذلك إدانة المتهم (ب.ح) بعقوبة الحبس والغرامة[4]، حيث أنه بتاريخ 27-09-2008 تقدم إلى مصالح الأمن المدعو(ب.ع) الممثل القانوني للمديرية الجهوية للصندوق الوطني للتوفير والإحتياط (تلمسان) من أجل رفع شكوى ضد (ب.ح) رئيس قسم التحصيل بالصندوق الوطني للتوفير والإحتياط بسيدي بلعباس، حيث أن هذا الأخير كان يتسلم مبالغ دين الزبائن وكان في بعض الأحيان يدفع جزء من الدين ويحتفظ بالباقي، وفي أحيان أخرى يأخذ كل المبلغ ويسلم لهم وصولات تسديد مزورة ووهمية

[1]- تنص المادة 394 مكرر 7 من قانون العقوبات الجزائري على ما يلي :" يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها."

[2]- حكم رقم 13/03609 بتاريخ 2013/04/17 صادر عن قسم الجنح بمحكمة سيدي بلعباس .

[3]- قرار رقم 14/01051 بتاريخ 2014/02/03 صادر عن الغرفة الجزائية بمجلس قضاء سيدي بلعباس.

[4]- قرار رقم 09/07983 بتاريخ 2009/08/09 صادر عن الغرفة الجزائية بمجلس قضاء سيدي بلعباس.

ولا يوجد عليها ختم أمين الصندوق، وباعتباره مكلف بتحيين حسابات الزبائن بالحاسوب فقد كان يقوم بذلك عن طريق إدخال هؤلاء بهوية ناقصة كي تسهل عليه مهمة تغيير إسم الزبون صاحب الحساب بإسم زبون آخر يعرفه ليسهل عليه مهمة الإستحواذ على المال المختلس، وهو ما أكدته نتيجة الخبرة والتقرير الإداري المتعلق بالتفتيش الداخلي.

البند الثاني :جرائم المعالجة الآلية للمعطيات في القانون الفرنسي.

إنّ اللبنة الأولى لتنظيم وحماية نظام المعلوماتية في فرنسا والذي ينعكس إيجابا فيما بعد على التجارة الإلكترونية كان بصدور القانون رقم (1787) الصادر في 6 يناير عام 1978 في شأن الحريات والمعلوماتية، وقد عالج فيه المشرع مسألة تخزين البيانات في الحاسب الآلي وأنواع هذه البيانات ومدتها وتلك التي تخزن وتلك التي لا يجوز تخزينها، وكذلك الجهة المختصة بالرقابة والإشراف على إعمال ذلك القانون، حيث أنشأت بمقتضاه "اللجنة القومية للمعلوماتية والحريات" وهي تختص بإجراء رقابة سابقة ورقابة لاحقة للتأكد من الحماية الكاملة للحريات في مواجهة نظم المعلومات[1].

وبعد صدور قانون 1978 فقد تلاه مجموعة من القوانين أهمها قانون 03 يوليو 1985 في شأن حماية البرامج في ضوء الحماية المقررة للملكية الفكرية ، ولم يأخذ مشروع قانون العقوبات الفرنسي المعدل في 1988 في الإعتبار بعض التعديلات التي أجريت اعتبارا من عام 1986 على المشروع وخصوصا تلك المتعلقة بالجرائم المعلوماتية والتي نص عليها قانون الخامس من يناير 1988 والذي أراد به المشرع الفرنسي في حينه حماية أنظمة المعلومات نظرا لكثرة استخدام الفيروسات وما أطلق عليه في حينه بالإرهاب المعلوماتي[2]، والمقصود به العدوان أو التخويف أو التهديد ماديا أو معنويا باستعمال الوسائل الإلكترونية[3]، غير أنه حين صدور قانون العقوبات الفرنسي الجديد عام 1992 إستحدث المشرع الفرنسي نصوصا تتعلق بحماية المعلومات المعالجة آليا.

وبالرجوع إلى قانون العقوبات الفرنسي، فقد نصت المادة (323-1)[4] على أنه يعاقب على الدخول أو الإستمرار في البقاء في نظام المعلومات أو جزء منه بقصد الغش، بالحبس لمدة سنتين (2)

---

[1] – د.عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص348.

[2] – د. مدحت رمضان، المرجع السابق، ص45.

[3] – د.عبد الرحمن بن عبد الله السند، وسائل الإرهاب الالكتروني وطرق مكافحتها، بدون تاريخ، ص 02، بحث منشور على الموقع : www.alminbaralislam.com.

[4] - Article 323-1 du (C.P.F Modifié par LOI n°2012-410 du 27 mars 2012 - art. 9): Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

والغرامة 30.000 أورو، وإن كان المشرع الفرنسي قد اعتبر تحقيق النتيجة الإجرامية لهذا النشاط ظرفا مشددا وذلك إذا ترتب على هذا الدخول محو أو تعديل في البيانات أو الإضرار بوظيفة النظام، فعندئذ تشدد العقوبة وتصبح الحبس لمدة ثلاث (3) سنوات والغرامة 45.000 أورو.

والدخول على النظام من الجرائم الوقتية، وتقع الجريمة من أي شخص حيث يستوي أن يكون من الخبراء أو حتى الأفراد العاديين، وسواء كان الدخول للقيام بعمل غير مشروع أو لمجرد الفضول وحب الإستطلاع.

ويرى جانب من الفقه أن الدخول قد يكون مشروعا إذا كان عن طريق الصدفة أو الخطأ أو السهو وكان من الواجب عندئذ أن يقطع تواجده و ينسحب فورا ، فإذا بقي رغم ذلك يعاقب، و إن كان الدكتور "عبد الحليم رمضان" يرى أن الدخول بطريق الصدفة أو الخطأ أو السهو يتسم بعدم المشروعية وإن كان القانون الجنائي لا يعاقب سوى على الدخول العمدي، و عندئذ يعاقب الجاني إذا بقي عمدا داخل النظام.

ويتضح أنّ المشرع قد استخدم بنص المادة (323-1) مصطلحات تسمح بتجريم استعمال أي وسيلة تقنية للدخول على نظام لمعالجة البيانات، كالدخول عن طريق كلمة السر الحقيقية إذا لم يكن للجاني الحق في استخدامها أو باستخدام برنامج أو شفرة خاصة[1].

وتتعلق المادة (323-2)[2] بتجريم أساليب سير العمل في النظام المعلوماتي أو تحريف هذه الأساليب من خلال تعطيل أو إفساد التشغيل وذلك بالنص على أنّ تعطيل أو إفساد تشغيل نظام المعالجة الآلية يعاقب عليه بالحبس لمدة خمس (05) سنوات وغرامة مالية مقدارها 75.000 أورو .

ويتضح من خلال المصطلحات المستخدمة بنص المادة(323-2) أنها تشمل كل فعل من شأنه إرباك عمل نظام المعالجة الآلية، ويستوي أن يكون من شأن نشاط الجاني إعاقة أو إفساد نظام التشغيل أو الإرسال، ويستوي أن يـؤدي نشاط الجاني إلى توقف نظام العمل بصورة دائمة أو مؤقتة، أو أن يستخدم

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende.

[1]– د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص 51.

[2] - Article 323-2 du (C.P.F Modifié par LOI n°2012-410 du 27 mars 2012 - art. 9) : Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende.

الجاني في ارتكاب الجريمة أية وسيلة من شأنها أن تعوق سير النظام كالإعتداء المادي على النظام أو نشر فيروسات بالنظام المعلوماتي[1].

ونصت على هذا الفعل المادتين (05)[2] و (08)[3] من إتفاقية بودابست بشأن الجرائم الإلكترونية، ولقد وضع الفقه معيارا للتفرقة بين الإعتداء على المعطيات والإعتداء على النظام على أساس ما إذا كان الإعتداء وسيلة أم غاية، فإذا كان الإعتداء الذي وقع على المعطيات مجرد وسيلة فإنّ الفعل يشكل جريمة الإعتداء العمدي على النظام، أمّا إذا كان الإعتداء الذي وقع على المعطيات غاية فإنّ الفعل يشكل جريمة الإعتداء العمدي على المعطيات.

ويتمثل هذا السلوك المادي في فعل توقيف نظام المعالجة الآلية للمعطيات عن أداء نشاطه العادي والمنتظر منه القيام به وإما في فعل إفساد نشاط أو وظائف هذا النظام، ولا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام جملة، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية جهاز الحاسب الآلي نفسه وشبكات الإتصال أو المعنوية مثل البرامج والمعطيات[4].

وتتمثل هذه الصور فيما يلي :

1- التعطيل:

يطال التعطيل أجهزة الكمبيوتر عبر تعطيل برامجها، كما قد يؤدي تعطيل البرامج إلى أعطال فنية تطال قطع الأجهزة الإلكترونية، فالهدف من التعطيل هو منع الحواسيب والشبكات من تأدية عملها بدون أن تتم عملية إختراق فعلية لتلك الأجهزة.

وتتم عملية تعطيل الأجهزة عن طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها الأمر الذي يعيقها عن تأدية عملها، فقد وقعت بعض المواقع الكبرى المستضيفة للمواقع على الشبكة ضحية هذا التعطيل.[5]

---

[1]- د .عبد العال الديربي، الحماية الجنائية من الإتلاف المعلوماتي في القانون الفرنسي الحديث، 1 مارس 2013، على الموقع: http://accronline.com

[2] - Article 5 du (C.C.C) : Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques.

[3] - Article 8 du (C.C.C) : Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui par:

a. l'introduction, l'altération, l'effacement ou la suppression de données informatiques,

b. toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

[4] – أ.أمال قارة، المرجع السابق ،114.

[5] – أ. نبيل صقر، جرائم الكمبيوتر والإنترنت، المرجع السابق ،ص 137.

ويستوي أن يكون التعطيل دائما أو مؤقتا فقد يؤدي إلى التوقف الدائم للنظام كما في حالة الإدخال، وقد يكون التوقف مؤقتا أو منقطعا على فترات فيروس معلوماتي تدميري، كما إذا تم إدخال قنبلة معلوماتية زمنية مبرمجة ينجم عنها شل النظام عند البدء في تشغيله مثلا أو عند استخدام أحد برامج التطبيق، كما يستوي أن يكون التوقيف بالنسبة لجميع مستعملي النظام أو بالنسبة لأحدهم فقط، ولكن يشترط في التعطيل أن يكون ايجابيا أي أن يصدر عن الجاني نشاطا إيجابيا يؤدي إلى توقيف النظام، ويمكن أن يتحقق فعل التعطيل بالإمتناع إذا اقترن بنشاط إيجابي كأن يتعسف الجاني ويرفض القيام بما يفرضه عليه القانون[1].

فالتعطيل أو التوقيف الذي يندرج ضمن إعاقة النظام يقع بأي وسيلة، فالمشرع لم يشترط وسيلة معينة لحصول الإعاقة، فقد تكون بطريقة مادية أو معنوية ومن أمثلة إعاقة النظام بطريق مادي أعمال العنف المادي على أجهزة الحاسب وشبكات الإتصال، أمّا الإعاقة والتعطيل بوسيلة معنوية فقد يكون بإدخال فيروس على البرنامج أو تعديل كلمة السر أو كيفية أداء النظام لوظيفته بوسيلة مثلا تؤدي إلى أن يتباطأ في أدائه لوظيفته المعلوماتية داخل النظام المعلوماتي[2].

2- الإفساد:

يقصد بالإفساد كل فعل وإن كان لا يؤدي إلى التعطيل، فقد يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للإستعمال السليم، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.

والإفساد من هذه الزاوية يقترب من التعييب والفارق بينهما يكمن في أنّ الإفساد في حالة الظرف المشدد لا يشترط فيه أن يكون عمديا، بينما يتطلب هذا الشرط بالنسبة لجريمة الإعتداء العمدي على نظام المعالجة الآلية للمعطيات، ومن وسائل التعييب أو الإفساد إستخدام القنبلة المعلوماتية أو إستخدام البرنامج الذي يحمل فيروس يطلق عليه "حصان طروادة" وغير ذلك من الفيروسات التي تجعل مخرجات النظام غير تلك التي كان يجب عليه أن يخرجها، بل أنّ الإفساد يمكن أن يتحقق عن طريق إتلاف أو تخريب العناصر المادية في النظام[3].

---

[1] – أ.أمال قارة ،المرجع السابق ،ص118.

[2] – د.عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص40.

[3] – د.عبد القادر قهوجي، المرجع السابق، ص143. نقلا عن: أ.أمال قارة ،المرجع السابق ،ص119.

أمّا بالنسبة للركن المعنوي فهي تعتبر جريمة عمدية، لأنّ الفقهاء يرون أن الشخص الذي يقوم بالإخلال بالعمل داخل النظام المعلوماتي عن طريق العرقلة والتعطيل، فلاشك أنه يقوم بذلك بصفة عمدية.

وكذلك فإنّ المادة (323-3)[1] من القانون السابق ذكره تشير إلى تحريف سير العمل عمدا مما يؤدي إلى إتلاف المعلومات المخزنة بالنظام المعلوماتي، وذلك بالنص على أنّ إدخال البيانات بطريق الغش في نظام المعالجة الآلية أو محوها أو التعديل بطريق الغش للمعطيات التي يحتويها يعاقب عليه الحبس لمدة خمس (05) سنوات وبغرامة مقدارها 75.000 أورو، وعلى ذلك فإنّ هذا النص يعاقب على إتلاف المعلومات الموجودة في الذاكرة أو على الأسطوانة، حيث يؤدي إدخال البيانات إلى شغلها بالكامل، مما يؤدي إلى عجزها عن التعامل مع هذه المعطيات بمعالجتها أو استخراجها مطبوعة على أوراق والشيء نفسه بالنسبة لمحو المعلومات أو تعديلها حيث يؤدي إلى إتلاف المعلومات الموجودة [2].

غير أنه ينبغي التمييز بين جريمة الإتلاف المعلوماتي و جريمة التزوير المعلوماتي، لأن هذه الأخيرة يتضمن ركنها المادي تغيير الحقيقة في المحرر بإحدى الطرق التي حددها القانون، تغييرا من شأنه إحداث ضرر للغير، و يكون ذلك في حالة حذفه أو إضافته أو التلاعب فيه بأي صورة سواء كانت هذه البيانات مخزنة في ذاكرة الآلة أم كانت تمثل جزءا من برنامج التشغيل أو برامج التطبيق، على أن تكون هذه البيانات محلا للتجريم .

فالضرر عنصر جوهري في جريمة التزوير، و لا يشترط القانون وقوع ضرر بالفعل بل يكفي احتمال وقوعه، و نظرا لعدم كفاية النصوص المتعلقة بالتزوير في المحررات لمواجهة التزوير الذي يقع في مجال المعالجة الآلية للمعطيات، فقد عاقب المشرع الفرنسي على التزوير الذي يقع في المستندات المعالجة آليا، سواء كانت داخل الجهاز أو خارجه[3].

ويرى الفقهاء أن هذه الجريمة يتخذ ركنها المعنوي صورة القصد الجنائي العام بعنصريه العلم والإرادة، وذلك متى تعمد الجاني ارتكاب الفعل واتجهت إرادته إلى إحداث الإتلاف.

---

[1] - Article 323-3 du (C.P.F Modifié par LOI n°2012-410 du 27 mars 2012 - art. 9): Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende.

[2] – أ.محمد أمين أحمد الشوابكة، المرجع السابق، ص224.

[3] – أ.مسعود خثير ، المرجع السابق، ص 137.

وبالرجوع إلى نص المادة(323-4)[1] من قانون العقوبات الفرنسي، فقد نص المشرع على أن المشاركة في مجموعة لإعداد جريمة أو أكثر من الجرائم المنصوص عليها في المواد (323-1) إلى (323-3-1)، وكان الإعداد عن طريق أفعال مادية، فيعاقب الجاني بالعقوبات المقررة للجريمة ذاتها.

كما أن المشرع الفرنسي أقر عقوبة الشروع في هذه الجرائم مثل عقوبة الجريمة التامة وذلك بموجب المادة (323-7)[2] من قانون العقوبات الفرنسي التي نصت على أنه يعاقب على الشروع في الجرائم المنصوص عليها في المواد (323-1) إلى (323-3-1) بالعقوبات المقررة للجريمة نفسها.

فبالنسبة للعقوبات التي تم ذكرها تتعلق بالعقوبات الأصلية، لأن المشرع الفرنسي بالإضافة إلى ذلك نص على عقوبات تكميلية للشخص الطبيعي بموجب نص المادة (323-5)[3] من بينها: الحظر لمدة خمس(5) سنوات من ممارسة الحقوق الوطنية المدنية والعائلية، الحظر لمدة خمس(5) سنوات من ممارسة الوظائف والمناصب العمومية التي لها علاقة بالجريمة، مصادرة الشيء الذي استعمل في ارتكاب الجريمة، ناهيك عن عقوبات أخرى متعلقة بالشخص المعنوي وفقا للأوضاع المنصوص عليها بموجب نص المادة (323-6)[4] .

---

[1] - Article 323-4 du (C.P.F Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004) : La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

[2] - Article 323-7 du (C.P.F Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004) : La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

[3] - Article 323-5 du (C.P.F) : Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

[4] - Article 323-6 du (C.P.F Modifié par LOI n°2009-526 du 12 mai 2009 - art. 124) : Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.
L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

ونظرا لخطورة ما يترتب على معالجة البيانات الإسمية من تهديد لخصوصيات الأفراد فقد قرر المشرع الفرنسي حماية لخمسة أنواع من الجرائم بشأن المعالجة الإلكترونية للبيانات الإسمية، وللإشارة فإن فرنسا كانت من أوائل الدول الغربية التي سارعت بإصدار تشريعات تهتم بحماية المعلوماتية و التصدي لبعض صور الجرائم التي قد تقع بسبب التقدم في استعمال الحاسب الآلي، وكذلك شبكة المعلومات الدولية كالإنترنت أو بعض الشبكات المحلية[1]، والتي تتمثل فيما يلي :

أولا : جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص.

تنشأ هذه الجريمة بمجرد مباشرة القائمين على معالجة البيانات الشخصية أنشطة المعالجة في الأحوال التي لم يمنحوا فيها ترخيصا بذلك من قبل الجهات المختصة المحددة قانونا، كما تنشأ كذلك في الأحوال التي يلغى فيها الترخيص أو تنتهي مدته وتستمر جهة المعالجة بنشاطها.

والواقع أنّ عدم الحصول على الترخيص يمثل في الحقيقة إعتداء على حق الدولة في الرقابة على تداول ونقل البيانات، كما أنه يفقد جهات الرقابة عملها المؤسس على كفالة عدم الإعتداء على الخصوصية.

والفقه الفرنسي على خلاف حول طبيعة هذه الجريمة[2]، فيتجه البعض صوب تصنيفها ضمن طائفة الجرائم العمدية ويرى البعض الآخر أنّ مجرد ارتكاب السلوك المادي المكون لها بإنشاء ملفات البيانات خفية يؤدي إلى توقيع العقوبة معتبرين أنّ النص القانوني لا يتضمن أي اصطلاح يدل على أنّ الجريمة الواردة فيه تتطلب قصدا[3].

وفيما يتعلق بالعقوبة فقد نصت المادة (226-16)[4] من قانون العقوبات الفرنسي الجديد على معاقبة كل من يقوم ولو بإهمال بمعالجة إلكترونية للبيانات الشخصية دون مراعاة الإجراءات الأولية والمحددة في القانون بعقوبة تتمثل بالحبس لمدة خمس (05) سنوات وبغرامة مقدارها 300.000 أورو.

---

[1]– أ. مصطفى لعروم، غياب القوانين التي تعاقب إساءة استخدام الكمبيوتر، مجلة الموثق،الجزائر، من **26** ماي، جوان **2001**، العدد**1**، ص**1**.

[2]- Alain Bensoussan et Pascal Arigo, La cybercriminalité : vers une régulation internationale de l'internet ?, La gazette du palais, 16 Octobre 2001 , N287 , p35.

نقلا عن: د. بولين أنطونيوس، المرجع السابق، ص 418.

[3]– نفس المرجع، ص 418.

[4] - Article 226-16 du (C.P.F Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004) : Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

ثانيا: جريمة الجمع والتخزين غير المشروع للبيانات الشخصية.

فيما يتعلق بصفة عدم المشروعية التي تلحق أفعال الجمع والتخزين قد يكون مصدرها أساليب الحصول على البيانات أو مضمون وطبيعة هذه البيانات، كما أنّ قانون العقوبات الفرنسي من خلال المواد (226-17)[1] إلى (226-19) قد أسبغ صفة عدم المشروعية على جمع البيانات دون سبب مشروع أو جمع البيانات دون موافقة صاحب الشأن رغم اعتراضه أو حفظ البيانات بعد المدة المحددة [2].

فقد اعتبر المشرع الفرنسي جريمة يعاقب عليها بالحبس لمدة خمس (05) سنوات وبغرامة 300.000 أورو عملية وضع أو حفظ بذاكرة إلكترونية، دون موافقة صريحة من صاحب الشأن بيانات إسمية تظهر بصورة مباشرة أو غير مباشرة أصوله العرقية أو معتقداته السياسية أو الفلسفية أو الدينية أو انتماءاته النقابية أو تتعلق بأخلاقه،كما يعاقب بذات العقوبات من يقوم في غير الحالات التي يقررها القانون بوضع أو حفظ بيانات إسمية في ذاكرة إلكترونية تتعلق بالجرائم أو أحكام الإدانة أو التدابير[3].

أما بالنسبة للركن المعنوي في هذه الجريمة، فإنه يتعين على الجاني أن يكون عالما بطبيعة هذه البيانات و يقوم بحفظها و تخزينها دون موافقة المعنيين بالأمر وفقا للمادتين (226-18)[4]، (226-19)[5] من قانون العقوبات الفرنسي الجديد .

ومن التطبيقات القضائية ، إدانة محكمة Privas في فرنسا بتاريخ 03 سبتمبر1997 شخصا على نشر صور لإحدى الفتيات على صفحته الشخصية وذلك بغرض ابتزازها والتشهير بها، وكانت تلك الصور فاضحة، كما قام المتهم بوضع عبارات مستفزة وجارحة تمس بسمعة وشخصية هذه الفتاة، وعاقبته المحكمة

---

[1] - Article 226-17 du (C.P.F Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004): Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

[2] – د. بولين أنطونيوس، المرجع السابق، ص 393.

[3] – د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص 100.

[4] - Article 226-18 du (C.P.F Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004) : Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

[5] - Article 226-19 du (C.P.F Modifié par LOI n°2012-954 du 6 août 2012 - art. 4) : Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation ou identité sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

بناء على نص المادة (226-19) من قانون العقوبات والتي تعاقب كل من يستخدم هذه التقنيات الحديثة لنشر معلومات دون موافقة صاحبها تدل عن أصله أو تعبر عن آرائه السياسية أو الدينية أو انتمائه النقابي[1].

ثالثا: جريمة الحفظ غير المشروع للبيانات الإسمية.

يتحقق الركن المادي لجريمة الحفظ غير المشروع للبيانات الإسمية إذا كانت عملية المعالجة و الحفظ قد تمت وفقا لأحكام القانون، و لكن تم حفظ هذه البيانات لمدة تتجاوز المدة المطلوبة للحفظ، وذلك دون موافقة اللجنة القومية للمعلوماتية و الحريات، أو أن مدة الحفظ تجاوزت الوقت المحدد في طلب الموافقة أو الإخطار السابق على عملية المعالجة .

وبناء على ذلك، فإن المشرع بذلك يريد أن يؤكد أن البيانات الإسمية لا يمكن أن تحفظ لمدة غير محددة إلا في حالات إستثنائية يفترض أنها محددة قانونا و صراحة، و الهدف من وراء ذلك هو حماية الحياة الخاصة للأفراد، لأن حفظ البيانات إلكترونيا في ذاكرة النظام للأبد قد تمس الشخص في سمعته[2].

وتجدر الإشارة أن من شأن استخدام أنظمة الحاسب الآلي في المجال الأمني الإحتفاظ بكم هائل من المعلومات الخاصة بالأفراد، و بالتالي يكون هناك خطر إفشائها أو إساءة استعمالها من قبل أشخاص من المفترض أنهم أمناء عليها[3]، و تعد هذه الجريمة من الجرائم العمدية .

أمّا بالنسبة للعقوبة فيعاقب المشرع الفرنسي على جريمة الحفظ غير المشروع بعقوبة حددها في نص المادة (226-20)[4] من قانون العقوبات الفرنسي وهي الحبس لمدة خمس (05) سنوات وغرامة 300.000 أورو.

رابعا :جريمة الإنحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الإسمية.

يتحقق النشاط المادي لهذه الجريمة بمجرد الإنحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات، والغرض هو موضوع المعالجة الإلكترونية وهي المبرر الوحيد لمعالجة البيانات الإسمية الإلكترونية.

---

[1] - TGI de Privas, Jugement correctionnel du 03/09/1997, disponible à l'adresse suivante :www.legalis.net.

[2]– د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص 102.

[3]– د. فتوح الشاذلي و د. عفيفي كامل عفيفي، المرجع السابق، ص 278.

[4] - Article 226-20 du (C.P.F Modifié par Loi n°2000-321 du 12 avril 2000 - art. 6 - Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004) : Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.

وتفترض جريمة الإنحراف عن الغرض أو الغاية من المعالجة الإلكترونية الحصول إبتداءا على هذه البيانات بصورة مشروعة أي بإذن من اللجنة الوطنية للمعلومات والحريات، ولكن الجاني ينحرف عن الغرض المقصود منها، وعلى سبيل المثال لا الحصر نجد أنّ الجاني يعد مرتكبا للنشاط المادي لهذه الجريمة فيما لو استغل البيانات الخاصة بآخر في الكشف عن مصادر ثروته أو لمعرفة مركزه المالي أو في الإستدلال عليه لخدمة مصلحة الضرائب.

أمّا الركن المعنوي في جريمة الإنحراف عن الغرض والغاية من المعالجة الإلكترونية للبيانات الشخصية صورة القصد الجنائي العام والتي تقوم بتوافر العلم والإرادة، فيتعين أن يعلم الجاني بأنّ من شأن فعله أن يشكل إنحرافا عن الغاية أو الغرض من المعالجة الإلكترونية للبيانات الشخصية وأن تتجه إرادته نحو ذلك[1]، أي غيّر من الوجهة النهائية المقررة لهذه البيانات وفقا للقانون[2].

وفيما يتعلق بالعقوبة يعاقب المشرع الفرنسي في المادة (21/226)[3] من قانون العقوبات الفرنسي الجديد كل من يرتكب جريمة الإنحراف عن الغرض أو الغاية من المعالجة الإلكترونية البيانات الشخصية بالحبس خمس (05) سنوات وبغرامة 300.000 أورو.

خامسا : جريمة الإفشاء غير المشروع للبيانات الإسمية.

يتحقق النشاط المادي لهذه الجريمة بتوافر صورتين :

الصورة الأولى: تلقي أو حيازة البيانات الشخصية، سواء بقصد تصنيفها أو نقلها أو معالجتها تحت أي شكل .

الصورة الثانية : فعل إفشاء البيانات إلى شخص غير مختص أي ليس من حقه الإعتداء عليها، لشخص غير ذي صفة قانونا في تلقي البيانات، فإذا كان للشخص المتلقي صفة حسب القانون فإن الفعل لا يتحقق .

ويتطلب المشرع الفرنسي لقيام الركن المادي توافر ثلاثة شروط :

---

[1] – د. بولين أنطونيوس، المرجع السابق، ص 421.

[2] – أ. سوزان عدنان و أ.صفاء أوتاني، إنتهاك حرمة الحياة الخاصة عبر الإنترنت، مجلة جامعة دمشق للعلوم الإقتصادية و القانونية، سوريا، المجلد 29، العدد 03، سنة 2011، ص437.

[3] - Article 226-21 du (C.P.F Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004) : Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

– أن يكون من شأن فعل الإفشاء أن يضر بالمجني عليه وذلك باقتران فعل الإفشاء بالإعتداء على الشرف أو الإعتبار أو الحياة الخاصة للفرد.

– أن يكون إفشاء البيانات بدون رضاء المجني عليه صاحب العلاقة، وبالتالي لا تتحقق هذه الجريمة إذا كان الإفشاء قد تم بناءا على موافقة صاحب الشأن الصريحة.

– أن يكون الإفشاء إلى شخص ليس له حق الإطلاع على هذه البيانات.

ويأخذ الركن المعنوي لجريمة الإفشاء غير المشروع للبيانات الإسمية صورة العمد أو الخطأ، وتتحقق صورة العمد بتوافر القصد الجنائي العام والذي يقوم بتوافر العلم والإرادة، فيتعين أن يكون الجاني عالما بأنه يقوم بإفشاء بيانات إسمية تشكل إعتداءا على الشرف أو الإعتبار أو الحياة الخاصة للأفراد، وتتحقق صورة الخطأ إذا كان فعل الإفشاء للغير قد وقع نتيجة إهمال أو رعونة أو ترك للبيانات الإسمية[1] .

أمّا بالنسبة للعقوبة فقد شدد المشرع الفرنسي العقاب، حيث نص في المادة (226–22)[2] على عقاب الجاني بالحبس خمس (05) سنوات والغرامة 300.000 أورو، أمّا إذا ارتكب الجريمة بصورة الخطأ فيعاقب المشرع بالحبس ثلاث (03) سنوات والغرامة 100.000 أورو.

البند الثالث : جرائم المعالجة الآلية للمعطيات في القانون المصري.

إستشعر المشرع المصري بضرورة إدخال تشريعات جديدة تحمي المعلومات داخل نظام الكمبيوتر، نظرا لقصور القواعد التقليدية في قانون العقوبات عن حماية هذا النظام، كما أن المشرع يعلق أهمية واضحة على حماية نظام المعلومات، الأمر الذي لم يوفره قانون العقوبات للملفات الورقية التقليدية التي تحتوي على معلومات ذات أهمية مماثلة[3].

[1] - د. بولين أنطونيوس، المرجع السابق، ص 411.

[2] - Article 226-22 du (C.P.F Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004) : Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence.
Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

[3]- د. شيماء عبد الغني، المرجع السابق، ص 94.

أولا: جرائم الإعتداء على النظام المعلوماتي:

يستدل على ذلك بما ورد في المادة (26) من مشروع قانون التجارة الإلكترونية المصري على أنه: "مع عدم الإخلال بأية عقوبة أشد وردت في قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن ثلاثة آلاف (3000) جنيه، أو بإحدى هاتين العقوبتين، كل من دخل بطريق الغش أو التدليس على نظام معلومات أو قاعدة بيانات تتعلق بالتوقيعات الإلكترونية، ويعاقب بنفس العقوبة من اتصل أو أبقى الإتصال بنظام المعلومات أو قاعدة البيانات بصورة غير مشروعة.

كما عاقب المشرع كل من يقوم بكشف مفاتيح التشفير المودع بمكتب التشفير، أو بفض معلومات مشفرة في غير الأحوال المصرح بها قانونا، وذلك بالحبس الذي لا تقل مدته عن سنة(01) والغرامة التي لا تقل عن ثلاثة آلاف (3000) جنيه، ولا تزيد عن عشرة آلاف (10.000) جنيه أو بإحدى هاتين العقوبتين[1].

وتنص المادة (31) من نفس القانون على أنه يعاقب بالحبس مع الشغل كل من أدخل بعمد أو إهمال فيروس إلى نظام معلوماتي بدون موافقة مالك النظام أو حائزه الشرعي .

كما أصدر المشرع المصري تشريع خاص بشأن تنظيم التوقيع الإلكتروني رقم 15 لسنة 2004، حيث نصت المادة (23) منه على أنه يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف (10.000) جنيه ولا تتجاوز مائة ألف (100.000) جنيه أو بإحدى هاتين العقوبتين كل من أصدر شهادة تصديق إلكتروني دون الحصول على ترخيص، أو أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا، أو زور شيئا من ذلك بطريق الإصطناع أو التعديل أو التحوير، أو استعمل توقيعا أو وسيطا أو محررا إلكترونيا معيبا أو مزورا مع علمه بذلك.

ثانيا : حماية البيانات الشخصية.

إنّ المشرع المصري بمقتضى المواد (309 مكرر) و(309 مكرر1) والتي سيتم التطرق إليهما بالتفصيل لاحقا وفر الحماية لبعض صور الحياة الخاصة ومباشرتها وذلك من خلال أفعال معينة كالتسجيل والنشر والتصوير والتعرض لها، ولكن لا توفر الحماية لقواعد البيانات من النسخ والإستخدام والإستغلال، كما أضاف المشرع جريمة جديدة ضمن المادة (21) والمادة (22) من القانون رقم 96 لسنة 1996 بشأن تنظيم سلطة الصحافة حيث لا يجوز للصحفي أو غيره أن يتعرض للحياة الخاصة للمواطنين.

[1]– د.شيماء عبد الغني، المرجع السابق، ص94.

ومن ناحية أخرى يوفر القانون رقم 35 لسنة 1960 المعدل بالقانون رقم 28 لسنة 1982 حماية لقواعد البيانات الخاصة بالتعداد والإحصاء من استخدامها لغير أغراض الإحصاء أو نشرها واتخاذها كأساس للضرائب أو ترتيب الأعباء المالية، ورتب عقوبات على إفشاء هذه البيانات أو استخدام الوسائل غير المشروعة للحصول عليها، إلا أن هذه الحماية لا توازي الحماية التي تكفلها بعض التشريعات الغربية لحرمة الحياة الخاصة[1].

ثالثا : حماية البيانات الإسمية والأسرار.

يرى جانب من الفقه أنّ المادة (310)[2] من قانون العقوبات الخاصة بإفشاء الأسرار لا تنطبق على إفشاء المعلومات الإسمية المخزنة بقواعد البيانات، نظرا لأنّ العبارات المستخدمة لا تحمل إمكانية تطبيقها على حالة إفشاء المعلومات المخزنة في قواعد البيانات، ولم يكن من الممكن تطبيقها لتشمل هذا الأمر نظرا لعدم جواز القياس في المواد الجنائية، كما أنّ البيانات الإسمية تشتمل على بيانات تتعلق بأسرار الناس فقد تتناول بيانات ذات طبيعة سرية، ومثال ذلك الحالات التي يقوم فيها الطبيب بحفظ المعلومات الخاصة بمرضاه الذي يقوم بمعالجتهم على قاعدة بيانات على الحاسب، وكذلك المحامي الذي يحفظ معلومات تتعلق بموكليه وقضاياهم على قاعدة البيانات، ولذلك إذا أفشى الطبيب أو المحامي المعلومات المثبتة على قواعد البيانات الموجودة لديهما إرتكبا الجريمة المنصوص عليها بالمادة (310) من قانون العقوبات المصري[3].

المطلب الثاني: الإستخدام غير المشروع لوسائل المراقبة الإلكترونية.

إنّ خصوصية المعلومات هي حماية البيانات، لكن الخصوصية ليست هي حماية البيانات، فهذه الأخيرة شيء من الخصوصية وتتعلق بمواجهة الإعتداءات على البيانات الشخصية وسيطرة صاحبها عليها، في حين أنّ الخصوصية على إطلاقها تنطوي على خصوصية البيانات وخصوصية الإتصالات في مواجهة أنشطة الرقابة والتجسس وخصوصية المكان وحرمته في مواجهة أنشطة الإعتداءات المادية، والتي سبق وأن

[1] - د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص 112.

[2] – تنص المادة 310 من قانون العقوبات المصري رقم 1982/37 المؤرخ في 1982/09/28 المعدل والمتمم للقانون رقم 1996/95 المؤرخ في 1996/06/30 على ما يلي: "كل من كان من الأطباء أو الجراحين أو الصيادلة أو القوابل أو غيرهم مودعا إليه بمقتضى صناعته أو وظيفته سر خصوصي أو ائتمن عليه فأفشاه في غير الأحوال التي يلزمه القانون فيها بتبليغ ذلك، يعاقب بالحبس مدة لا تزيد على ستة (06) شهور أو بغرامة لا تتجاوز خمسمائة (500) جنيه".

[3] – د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص 113.

تم التفصيل فيها في الباب الأول، وأيضا خصوصية المراسلات ومن ضمنها المادية وأخرى إلكترونية، وغير ذلك من أوجه الحماية ذات الطبيعة المادية أو المعنوية.

فالخصوصية بالعموم تنطوي على حماية مظاهر مادية ومعنوية ومعلوماتية ولا تقف عند حماية البيانات الشخصية، وقد حرص المشرع على توفير الحماية للحق في حرمة الحياة الخاصة، إنطلاقا من مبدأ أساسي مقرر في السياسة الجنائية مضمونه أنّ الحقوق والمصالح الهامة إجتماعيا يجب أن نحميها بأقوى صور الحماية القانونية وأكثرها فاعلية وهي الحماية الجنائية[1]، وسأحاول أن أتطرق من خلال هذا المطلب للإستخدام غير المشروع لوسائل المراقبة الإلكترونية في التشريع الجزائري مع إجراء مقاربة مع التشريع المصري والفرنسي.

الفرع الأول: إنتهاك حرمة الأحاديث الخاصة.

تعتبر المحادثات الخاصة من بين عناصر حرمة الحياة الخاصة التي لا خلاف عليها، ذلك أنّ المتحدث يفصح للمتحدث إليه، سواء كان الحديث مباشرا أو عبر وسيلة من وسائل الإتصال الحديثة السلكية واللاسلكية عن دقائق أسراره وما يختلج في نفسه من خبايا أو عواطف أو أشجان، ثقة منه في شخص هذا الأخير ودون حرج أو خوف من سماع الغير، معتقدا أنه في مأمن من استراق السمع.

ويستوي أن يتحدث الشخص باللغة العربية أو أية لغة أخرى، فجميع اللغات تصلح أن تكون محلا للحماية، ومما لا شك فيه أنّ الأحاديث الشخصية تشمل المكالمات الهاتفية وتعد من ضمن وسائل حرمة الحياة الخاصة للأفراد، ومن هنا أضفى المشرع الحماية على هذه الأحاديث الشخصية حفاظا على حقوق الأشخاص هذا من جهة، ومن جهة أخرى أصبح التطور التكنولوجي المتلاحق في وسائل التنصت على الإتصالات السلكية واللاسلكية والأحاديث الشفوية الخاصة خطرا مستمرا على حرمة الحياة الخاصة[2].

ومن أجل توضيح هذه المسألة سيتم التطرق لموقف المشرع الجزائري مع إجراء مقاربة مع التشريع المصري والتشريع الفرنسي.

---

[1]- د. بولين أنطونيوس، المرجع السابق، ص66.

[2]- د. أحمد فتحي سرور، المرجع السابق، ص 447و د. محمد الدسوقي الشهاوي، المرجع السابق، ص 176. نقلا عن: د. عاقلي فضيلة، المرجع السابق، ص220.

البند الأول: جريمة إلتقاط أو تسجيل أو نقل أحاديث خاصة في القانون الجزائري.

يتضح من خلال نص المادة (303 مكرر)[1] من قانون العقوبات أنّ المشرع الجزائري إشترط لقيام جريمة إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة توافر ركنين: الركن المادي والركن المعنوي وذلك على النحو التالي:

أولا: الركن المادي.

يقوم الركن المادي في هذه الجريمة بتحقق إحدى صور النشاط، وهي إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة، واستنادا لنص المادة (303 مكرر) من قانون العقوبات لابد أن تتوافر شروط في النشاط الإجرامي وهي[2]:

1. نشاط إجرامي يتمثل في إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة.
2. إستخدام تقنية أيا كان نوعها في إلتقاط أو تسجيل الأحاديث أو نقلها.
3. أن تكون الأحاديث التي تم الحصول عليها ذات طابع سري وخصوصي.
4. عدم رضاء المجني عليه.

وسأتطرق لهذه العناصر على النحو التالي:

1.النشاط الإجرامي :

المحادثة في اللغة تعني تبادل الحديث بين شخصين أو أكثر، و من تم فإن المحادثات المعاقب على استراق السمع إليها أو تسجيلها أو نقلها هي الأحاديث المتبادلة بين شخصين أو أكثر، كما أن الحديث يقصد به كل صوت له دلالة التعبير عن مجموعة من المعاني و الأفكار المترابطة، فإذا كان هذا الصوت فاقد الدلالة على أي تعبير فلا يعد حديثا، كما لا يعد حديثا الصوت الذي و إن أعطى دلالة فإنه يعطي دلالة التعبير عن مجموعة من المعاني كاللحن الموسيقي [3].

بينما يقصد بالتقاط المكالمات أو الأحاديث الحصول على ما جرى بين الأشخاص من كلام إمّا تفوه به الفرد سرا ودون علم صاحب الشأن وبأية وسيلة كانت.

---

[1] - تنص المادة 303 مكرر من القانون رقم 06-23 المؤرخ في20-12-2006 المتضمن قانون العقوبات على أنه:"يعاقب بالحبس من ستة (6) أشهر إلى ثلاثة (3) سنوات وبغرامة من 50.000دج إلى 300.000دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

أ- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها ورضاه.

ب- .....

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة".

[2]- د. عاقلي فضيلة، المرجع السابق، ص 239.

[3]- مقال بعنوان : جرائم الإعتداء على حرمة الحياة الخاصة، على الموقع: http://www.permalink.com

أمّا النقل فيقصد به نقل الحديث أو المكالمة اللذين تم الإستماع إليهما أو تسجيلهما من المكان الذي تم فيه هذا الإستماع أو التسجيل إلى مكان آخر غيره.

أمّا التسجيل فيعني حفظ الحديث على جهاز أو أي وسيلة أخرى معدة لذلك بقصد الإستماع إليه فيما بعد، أو نقله إلى مكان آخر غير الذي تم تسجيله فيه[1].

2.وسيلة إرتكاب الجريمة:

لم يحدد المشرع الجزائري نوع التقنية المستعملة في ارتكاب جريمة التقاط أو تسجيل أو نقل أحاديث خاصة، فيمكن أن يستعين الجاني في ارتكابه لهذه الجريمة بأي جهاز تقني، وبالرغم من ذلك المشرع الجزائري قد ضيق من نطاق الحماية باستعماله عبارة (بأية تقنية كانت) وذلك مقارنة مع التشريع الفرنسي كما سيتبين لاحقا.

3.الصفة الخاصة للأحاديث:

إشترط المشرع الجزائري في المادة(303 مكرر/01) من قانون العقوبات أن يكون الحديث الذي تم التقاطه أو تسجيله أو نقله ذو طابع خصوصي، وعليه فمهما كانت طبيعة المكان عاما أو خاصا يعتبر هذا الفعل جريمة يعاقب عليها القانون.

4.عدم رضاء المجني عليه:

إن نطاق الرضا يتحدد بالمدى الذي يخول القانون لإرادة فاعليتها، فحق الإنسان في التقاط حديث خاص وتسجيله ونقله من الحقوق اللصيقة بالشخصية والغير قابلة للتصرف، إلا أن القانون في هذه الحالة إعتد بإرادة المجني عليه وجعل لها دورا تعمل فيه دون الإلتفات إلى صفة الحق فيما إذا كان قابلا للتصرف أم لا، فيرى الدكتور أحمد فتحي سرور أن الرضا بانتهاك الحياة الخاصة لا يعد تنازلا عن حرمتها ، إنما هو إزالة لسريتها و خصوصيتها .

غير أنه يجب أن يكون الرضاء في هذه الجريمة محددا تحديدا دقيقا، فلو رضي إنسان أن ينقل له حديثا عن موضوع معين ثم نقل عنه موضوع آخر، فإن الرضاء في هذه الحالة لا يكون متوافرا ولا أثر له عن قيام هذه الجريمة، وعليه فإذا صدر الرضاء مستوفيا لشروط صحته أي أن يكون سليما وبإرادة حرة خالية من عيوب الإرادة كالغلط والإكراه والتدليس، سابقا أو معاصرا لوقوع هذه الجريمة، فإن الرضاء يبيح الجريمة وبالتالي

[1] – د. آدم عبد البديع حسين، المرجع السابق، ص 538.نقلا عن: د. عاقلي فضيلة، المرجع السابق، ص 242.

يكون سببا من أسباب الإباحة. و ذلك كما أشارت إليه الفقرة الأخيرة من المادة 303 مكرر من قانون العقوبات، حيث أن صفح الضحية يضع حدا للمتابعة الجزائية .

ويتبين من خلال ما تم التطرق إليه، أن المشرع قد جعل من رضاء صاحب المصلحة التي يصونها القانون في غير الأحوال المصرح بها قانونا عنصرا في الركن المادي للجريمة ، فمادام للفرد النصيب الأوفى في المصلحة المصانة ، كما له التنازل عنها ، فمن تم تتوافر بذلك في الرضا الصحيح شروط اعتباره سببا لإباحة الإعتداء على حرمة الحياة الخاصة [1].

ثانيا: الركن المعنوي.

يتخذ الركن المعنوي لجريمة إلتقاط أو تسجيل أو نقل أحاديث خاصة صورة القصد الجنائي، فالقصد يستخلص من طبيعة الأفعال التي يقوم بها النشاط المادي لهذه الجريمة بأنها اعتداء على حرمة الحياة الخاصة، فالإعتداء يفترض القصد.

و ليس في الفقه خلاف حول لزوم القصد الجنائي، و إنما الخلاف على نوعه، و السائد أنه يكفي توافر القصد العام ، و مع ذلك ذهب الفقهاء إلى لزوم أن يقوم بجانبه قصد خاص ، و إن كانوا قد اختلفوا بعد ذلك في تحديده.

والقصد الجنائي في الرأي الراجح هو اتجاه الإرادة إلى ارتكاب الفعل المكون للجريمة مع العلم بسائر عناصرها، و يتحقق هذا القصد إذا اتجهت إرادة الجاني إلى ارتكاب أفعال الإلتقاط و التسجيل والنقل للأحاديث، بينما يتحقق العلم إذا كان الجاني مدركا للطبيعة الخاصة للأحاديث وقت قيامه بهذه الأفعال.

وهذا معناه أن الجريمة المذكورة لا تقوم في حق من يلتقط الحديث أو يسجله أو ينقله بطريق الإهمال أو عدم التبصر أو التقصير، و ذلك مهما كان جسيما، فالتلامس في الخطوط يجعل الحديث غير مقصود ، و بالتالي تنتفي الجريمة لانتفاء القصد الجنائي[2].

[1]- مقال بعنوان : الرضا كسبب لإباحة جرائم الإعتداء على حرمة الحياة الخاصة ، بتاريخ 2011/02/09، على الموقع : www.startimes.com

[2]-مقال بعنوان: جرائم الإعتداء على حرمة الحياة الخاصة ، المرجع السابق ، ص 05.

غير أنّ الرأي الغالب في الفقه يرى أن هذه الجريمة من جرائم القصد الخاص بالإضافة إلى القصد العام، على اعتبار أنّ نية الفاعل هي نية خاصة في قصد المساس بحرمة الحياة الخاصة.

ثالثا: العقوبة.

نص المشرع الجزائري على أنّ جريمة الإلتقاط أو التسجيل أو النقل لأحاديث خاصة هي جنحة تكون عقوبتها الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000دج.

كما نص المشرع الجزائري على عقوبات تكميلية بموجب نص المادة(303 مكرر2)[1] وتعتبر هذه العقوبات جوازية، إلا أنه يتعين دائما مصادرة الأشياء و الأدوات التي استعملت في ارتكاب هذه الجريمة، وتعد هذه الأخيرة وجوبية.

هذا بالإضافة إلى أنّ الشروع في ارتكاب هذه الجنحة يعاقب عليه بنفس العقوبة المقررة في حالة ارتكاب الجريمة التامة وذلك طبقا لنص المادة(303 مكرر) من قانون العقوبات.

أما المادة (09 مكرر) من قانون العقوبات تنص على عقوبة أخرى للجاني تتمثل في الحجر القانوني عن طريق حرمانه من ممارسة حقوقه المالية أثناء تنفيذ العقوبة الأصلية، كما تتم إدارة أمواله طبقا للإجراءات التي نص عليها القانون.

البند الثاني: جريمة إلتقاط أو تسجيل أو نقل أحاديث خاصة في القانون الفرنسي.

لم يكن التشريع الفرنسي الجنائي يتضمن نصوصا تحظر التنصت على الأحاديث الخاصة إلى أن صدر قانون 17 يوليو سنة 1970، ولذلك اضطلع القضاء الفرنسي بحماية الحق في حرمة الأحاديث الخاصة بوصفه حقا دستوريا.

واستنادا إلى إعلان حقوق الإنسان الوارد في مقدمة الدستور الفرنسي وتطبيقا لسلطة القضاء في إرساء قواعد مبدأ المشروعية من جهة، ومن جهة أخرى ما حدث من تقدم علمي وتقني وما نتج عنه من ظهور أشكال وصور جديدة من أفعال الإعتداء على حرمة الحياة الخاصة للغير، تدخل المشرع الفرنسي

[1]- تنص المادة 303 مكرر 2 من قانون العقوبات الجزائري على ما يلي:" يجوز للمحكمة أن تحظر على المحكوم من أجل الجرائم المنصوص عليها في المادتين 303 مكرر و 303 مكرر1، ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 9 مكرر 1 لمدة لا تتجاوز خمس(5) سنوات، كما يجوز لها أن تأمر بنشر حكم الإدانة طبقا للكيفيات المبينة في المادة 18 من هذا القانون.
ويتعين دائما الحكم بمصادرة الأشياء التي استعملت لارتكاب الجريمة".

وأصدر أول قانون وهو القانون السابق الذكر الذي يقتضي حماية جنائية خاصة على الحق في حرمة الحياة الخاصة، والذي أضاف خمسة مواد جديدة إلى قانون العقوبات وهي المواد (368-372)، والتي تعاقب على الإعتداء على حرمة الحياة الخاصة.

وبناء على الملاحظات التي أبداها بعض الفقهاء على نصوص قانون 1970 ألغى المشرع الفرنسي هذا القانون بمقتضى قانون العقوبات الجديد لسنة 1992 والذي كررت المواد (226-1، 226-2، 226-3) منه ذات أحكام التي كانت واردة في القانون القديم مع إجراء بعض التعديلات[1].

فقد نصت المادة (226-1)[2] من قانون العقوبات الفرنسي على أنه: "يعاقب بالحبس سنة (1) وغرامة 45000 أورو كل من اعتدى عمدا بوسيلة أيا كان نوعها على ألفة الحياة الخاصة للآخرين:

-بالتقاط أو تسجيل أو بنقل الأحاديث التي تصدر عن شخص بصفة سرية أو خاصة دون رضاه".

من خلال هذا التعديل المشرع الفرنسي لم يشترط أن يقع الإعتداء بواسطة جهاز من الأجهزة ، كما أنه لا يلزم في حالة التنصت أو تسجيل الحديث أن يتم في مكان خاص، كما اشترط المشرع لقيام هذه الجريمة توافر ركنين وهما : الركن المادي والركن المعنوي[3]، وسوف أتطرق إليهما على النحو التالي مع بيان العقوبة.

أولا : الركن المادي.

إستنادا لنص المادة (226-1) من قانون العقوبات الجديد لابد أن تتوافر شروط في النشاط الإجرامي وهي[4]:

1.أن يكون موضوع الجريمة حديثا.

2.أن يصدر هذا الحديث بصفة خاصة أو سرية.

3.وسيلة ارتكاب الفعل الإجرامي.

4.إرتكاب الجريمة دون رضاء المجني عليه.

وسأتطرق لهذه الشروط على النحو التالي:

---

[1]- د. عاقلي فضيلة، المرجع السابق، ص223.

[2] - Article 226-1 du (C.P.F Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002): Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

[3]- د. محمد أمين الخرشة، المرجع السابق، ص 258.

[4]- نفس المرجع، ص 258.

1. أن يكون موضوع الجريمة حديثا:

لقد اختلف الفقه حول مدى تطبيق نص المادة (226-1) على قيام أي من المتحدثين بالتقاط المحادثة التي جرت بينهما وتسجيلها دون علم الطرف الآخر، حيث ذهب جانب من الفقه[1] إلى مد نطاق تطبيق نص المادة (226-1) على هذه المسألة، وبالتالي فإنّ قيام أحد المتحدثين بالتقاط المحادثة أو تسجيلها دون علم الطرف الأخر يترتب عليه مساءلته جنائيا، بينما ذهب جانب آخر من الفقه[2] إلى اعتبار أنّ قيام أحد المتحدثين بتسجيل المحادثة دون علم الطرف الأخر تنحصر عنه نطاق تطبيق المادة (226-1).

كما يجب أن ينصب فعل الإلتقاط أو التسجيل أو النقل على أحاديث إستنادا لما ورد بنص المادة 368 تقابلها المادة (226-1).

2. أن يصدر هذا الحديث بصفة خاصة أو سرية:

من خلال نص المادة (226-1) من قانون العقوبات الجديد ، يلاحظ أنها ألغت شرط المكان الخاص واستبدلت به شرط أن يصدر الحديث بصفة سرية أو خاصة، وتطبيقا لذلك فإنّ الحديث من الممكن أن يكون محلا للحماية حتى ولو كان قد جرى في مكان عام ، فمن الممكن أن يتسم الحديث بالخصوصية أو السرية حتى ولو تم في مكان عام[3].

هذا و إن كان بعض الفقهاء يرون أن المشرع الفرنسي من خلال نص المادة السالفة الذكر لم يقصر الحماية على الأحاديث التي تتم بين شخصين أو أكثر فقط، و إنما التجريم يشمل أيضا الحديث الفردي، كما لو كان صاحبه ينطق به ليسجل لنفسه فالتقطه آخر في غير الأحوال المصرح بها أو بغير رضاء المجني عليه .

غير أنه في المقابل تعرض هذا الرأي لانتقاد شديد لأنه إذا قلنا أن الحديث الفردي تشمله الحماية، فهذا تفسير واسع للنص لا يتفق و قواعد التفسير في القانون الجنائي [4].

3. وسيلة ارتكاب الفعل الإجرامي:

لقد استعمل المشرع الفرنسي بموجب نص المادة (226-1) عبارة (وسيلة أيا كان نوعها)، وبالتالي فقد جاءت العبارة واسعة تتضمن كل التقنيات الحديثة، إضافة إلى إنتهاك حرمة الحديث الخاص عن طريق الأذن حسب رأي العديد من الفقهاء.

---

[1] -Pierre Kayser, op.cit, p115.

[2]- Isabelle Lolies, La protection de la vie privée, Thése, université de droit d'économie et des sciences, d'Aix Marseille, France, 1999, p73.

نقلا عن :د. محمد أمين الخرشة، المرجع السابق، ص 258.

[3]- نفس المرجع، ص 260.

[4]- مقال بعنوان: جرائم الإعتداء على حرمة الحياة الخاصة، المرجع السابق، ص 03.

4. إرتكاب الجريمة دون علم المجني عليه:

يشترط المشرع الفرنسي لقيام جريمة الحصول على الأحاديث الخاصة أن يكون فعل الإلتقاط على الحديث الخاص أو تسجيله أو التنصت عليه أو نقله قد ارتكب دون رضاء المجني عليه طبقا لنص المادة(226-1 فقرة 1) من قانون العقوبات الفرنسي.

هذا وإن كانت هناك قاعدة يستشف من خلالها رضاء الأفراد مفادها أنّ الأفراد يقررون بأنفسهم أي الجوانب يرغبون في الإحتفاظ بها وأي الجوانب يرغبون في الكشف عنها للغير.

وقد أورد المشرع الفرنسي في الفقرة الأخيرة من المادة (226-1) حالة الإلتقاط على مرأى ومسمع من المجني عليه، ويستفاد من ذلك أنّ المشرع قد افترض رضاء المجني عليه طالما أنّ الفعل قد تم على مرأى ومسمع منه ولم يعترض صاحب الشأن وكان في وسعه ذلك[1].

ثانيا: الركن المعنوي.

إن جريمة الحصول على أحاديث خاصة هي جريمة عمدية ، فلا تقع مطلقا بالإهمال و لو بلغ حد الجسامة ، فيلزم لاكتمال النموذج القانوني للجريمة توافر القصد الجنائي بعنصريه : العلم و الإرادة ، فعلم الجاني يجب أن يمتد إلى جميع عناصر الجريمة و هي متعددة ، منها ما يتعلق بالوقائع التي تقوم عليها الجريمة ، و منها ما يتعلق بالتكييف الذي يخلعه القانون على هذه الوقائع[2] .

ثالثا: العقوبة.

نص قانون العقوبات الفرنسي على أنّ جريمة إلتقاط أو تسجيل أو نقل الأحاديث الخاصة هي جنحة عقوبتها الحبس مدة سنة (1) والغرامة 45 ألف يورو، بالإضافة إلى العقوبات التكميلية منها مصادرة الأشياء التي استعملت في ارتكاب الجريمة طبقا لنص المادة (226-31) من قانون العقوبات، كما قرر المشرع الفرنسي ذات العقوبة في حالة الشروع في ارتكاب الجريمة طبقا للمادة (226-5)[3] من قانون العقوبات.

---

[1]- د. عاقلي فضيلة ،المرجع السابق، ص 244.

[2]- د. فوزية عبد الستار، المرجع السابق، ص 433. نقلا عن مقال بعنوان : جنحة الإعتداء على حرمة الحياة الخاصة على الموقع:
http//aladalacenter.com

[3] - Article 226-5 du (C.P.F) : La tentative des infractions prévues par la présente section est punie des mêmes peines.

البند الثالث: جريمة إستراق السمع أو تسجيل أو نقل أحاديث خاصة في القانون المصري.

تولت الدساتير المصرية حماية الحق في حرمة الأحاديث الخاصة في وقت مبكر نسبيا بالمقارنة مع كثير من الدساتير الحديثة في البلدان العربية، ويلاحظ أنّ الحماية الدستورية لحرمة الأحاديث الخاصة لم تنتقل إلى القانون الجنائي إلاّ بعد صدور دستور سنة 1971 الذي نص في المادة(2/45) منه على أنّ:"...والمحادثات التيلفونية وغيرها من وسائل الإتصال، وسريتها مكفولة لا تجوز مصادرتها أو الإطلاع عليها أو مراقبتها إلاّ بأمر قضائي مسبب ولمدة محددة ووفقا لأحكام القانون".

وقد أضاف القانون الصادر بشأن تنظيم الحريات العامة المواد(309 مكرر) و (309 مكرر أ) إلى قانون العقوبات لتجريم الإعتداء على الحقوق المتعلقة بحرمة الحياة الخاصة، وأضاف المواد (95) و(206) إلى قانون الإجراءات الجنائية لتنظيم كيفية وشروط المساس بالحقوق والحريات[1].

ويلزم لقيام هذه الجريمة توافر ركنين، الركن المادي والركن المعنوي، كما سيتم بيان العقوبة المقررة لهذه الجريمة، وذلك على النحو التالي:

أولا: الركن المادي.

حددت المادة (309 مكرر) من قانون العقوبات المصري صور الفعل الإجرامي وتتمثل فيما يلي:

1- إستراق السمع:

يقصد باستراق السمع التنصت على الحديث أو الإستماع إليه خلسة ، و بمجرد التنصت يتحقق الركن المادي و بالتالي الجريمة.

كما أن المشرع المصري لم ينص على أجهزة بعينها ، و بالتالي يمكن أن تقوم الجريمة بأي جهاز من الأجهزة المعروفة في العصر الحالي لاستراق السمع أو التسجيل أو النقل، كما يمكن أن يشمل التجريم أية وسيلة تقنية حديثة تم اكتشافها بعد النص على هذه الجريمة أو أجهزة لم تكتشف بعد ، و هذا راجع إلى مسايرة التشريع للتطور العلمي الرهيب في مجال إختراع و إنتاج الأجهزة الحديثة .

و يرى جانب من الفقه أن علة اشتراط أن تتم الأفعال المذكورة عن طريق جهاز من الأجهزة يرجع إلى أن هذا الفعل لا تكون له الخطورة التي تقتضي تجريمه إلا إذا استغل العلم الحديث في ارتكابه[2].

---

[1]- د. عاقلي فضيلة، المرجع السابق، ص228.

[2]- مقال بعنوان : جرائم الإعتداء على حرمة الحياة الخاصة، المرجع السابق ، ص 04.

2- تسجيل الحديث:

يقصد به حفظ الحديث على شريط معد لذلك بهدف سماعه فيما بعد [1]، كما يعرف التسجيل بأنه حفظ الرسالة بأية طريقة أو وسيلة وذلك باستعمال خاصية التسجيل الموجودة في تلك الأجهزة، أو باستخدام أجهزة تسجيل مستقلة ملحقة بالوسيلة المستعملة في الإتصال [2].

3- نقل الحديث:

يقصد به إلتقاط الحديث و إرساله من المكان الذي تم فيه إلى مكان آخر [3].

وبالرجوع إلى نص المادة (309 مكرر فقرة أ) السالفة الذكر، يتبين أنّ المشرع اشترط لقيام الإعتداء أن يقع في مكان خاص، ويقصد به المكان الذي لا يمكن أن تنفذ إليه نظرات الناس من الخارج، ولا يدخل إليه إلاّ بإذن من صاحبه.

غير أنه ينبغي عدم الخلط بين المكان الخاص والمسكن، فالمشرع إذ يحمي المكان الخاص فهو يحمي كل من تواجد فيه، سواء كان مالكا له أم مستأجرا، كما يستفيد من الحماية الزائر لذلك المكان، فالمالك يحق له أن يأذن بتسجيل محادثاته هو فقط، ولا ينسحب هذا الإذن على محادثات غيره ممن يتواجدون في المكان الخاص[4].

كما يشترط المشرع المصري أن يتم الإعتداء بغير رضاء المجني عليه، أي دون موافقته الصريحة أو الضمنية،كما في حالة ما إذا صدرت الأفعال المشار إليها على مسمع ومرآى من الحاضرين فهذا يفترض رضاء المتحدث[5].

ثانيا: الركن المعنوي.

تتخذ هذه الجريمة صورة القصد الجنائي العام بعنصريه العلم والإرادة، وأن يكون الجاني على علم بأنه يتنصت على محادثات خاصة مع توافر شرط عدم رضاء المجني عليه، أما إذا جهل الجاني بأنه يقوم بعمل غير مشروع فعندها لا يتشكل النشاط الإجرامي[6].

---

[1]- مقال بعنوان : حرمة الحياة الخاصة، بتاريخ 2013/11/19 ، على الموقع :http//anhri.net

[2]- مقال بعنوان: جنحة الإعتداء على حرمة الحياة الخاصة، المرجع السابق، ص 03.

[3]- مقال بعنوان : حرمة الحياة الخاصة، المرجع السابق، ص 03.

[4]- د. حسام الدين كامل الأهواني، الحماية القانونية لحرمة الحياة الخاصة، مجلة العلوم القانونية و الإقتصادية، جامعة القاهرة، مصر ، العدد الأول ، سنة 1999، ص 117. نقلا عن: د. محمد أمين الخرشة ، المرجع السابق، ص276.

[5]- د. محمد أمين الخرشة، المرجع السابق، ص 279.

[6]- د. آدم عبد البديع، المرجع السابق، ص 530.

كما يجب أن تتجه الإرادة إلى ارتكاب الفعل وتحقيق النتيجة المتمثلة في الحصول على الحديث أو المكالمة، كما لا تقوم الجريمة إذا كان الإستماع للمكالمة الهاتفية نتيجة تداخل الخطوط ووجود عيوب في شبكة الإتصالات[1].

ثالثا: العقوبة.

حدد المشرع المصري لهذه الجريمة الحبس مدته لا تزيد عن سنة، وتكون الجريمة مشددة إذا ارتكبها موظفا عاما إعتمادا على سلطة وظيفته في ارتكابه الجريمة، فتكون العقوبة الحبس الذي يصل حده الأقصى ثلاث(3) سنوات، وهناك عقوبة تكميلية وجوبية تتمثل في مصادرة الأجهزة وغيرها مما يكون قد استخدم في ارتكاب الجريمة ومحو التسجيلات المتحصلة عن الجريمة[2].

الفرع الثاني: إنتهاك حرمة الصورة.

تعد الصورة من أهم المظاهر التي يرد عليها الحق في الخصوصية، حيث أن الصورة تعد سمة مميزة للشخص وبصمة خارجية له، على أنها تعتبر إنعكاسا لشخصية الإنسان ليس فقط في مظهرها المادي الجسماني وإنما أيضا في مظهرها المعنوي، فهي تعكس مشاعر الإنسان وأحاسيسه ورغباته، كما أنّ الأحداث التي يمر بها الإنسان سرعان ما تظهر بصماتها على وجهه، فالصورة ترتبط بشخص الإنسان إرتباطا وثيقا، ومن تم تأتي قيمتها وأيضا ضرورة حمايتها[3].

فالحق في الصورة يعتبر عنصرا من عناصر الحق في حرمة الحياة الخاصة، وهو مظهر من مظاهر خصوصية الفرد[4]، وعليه سأتطرق للإنتهاكات التي تمس هذا الحق في القانون الجزائري مع إجراء مقاربة مع القانون المصري والفرنسي.

---

[1]- د.فوزية عبد الستار، المرجع السابق، ص 642. نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص280.

[2]- نفس المرجع، ص 280.

[3]- د.عاقلي فضيلة، المرجع السابق، ص249.

[4]-Charpontier Elise, Entre droits de la personnalité et droit de propriété, disponible à l'adresse suivante : https://ssl.editionsthemis.com.

البند الأول:جريمة إلتقاط أو تسجيل أو نقل الصورة في القانون الجزائري.

من خلال نص المادة (303 مكرر فقرة ب)[1]، يتضح أنه من أجل تحقق جريمة التقاط أو تسجيل أو نقل الصورة لابد من توافر ركنين وهما: الركن المادي والركن المعنوي، سأتطرق لهما مع بيان العقوبة.

أولا: الركن المادي.

يتحقق هذا الركن طبقا لنص المادة(303 مكرر) بالتقاط أو تسجيل أو نقل صورة شخص قائم في مكان خاص بغير رضاه باستخدام أية تقنية كانت، ويجب أن تتوافر العناصر التالية في الركن المادي وهي[2]:

1- السلوك الإجرامي.

2- وسيلة إرتكاب الجريمة.

3- المكان الخاص.

4- عدم رضاء المجني عليه.

وسيتم التطرق لهذه العناصر على النحو التالي:

1- السلوك الإجرامي:

يتحقق السلوك الإجرامي بالتقاط أو تسجيل أو نقل الصورة، والجدير بالذكر أنّ الصورة هي الشكل الذي يظهر بواسطة آلة التصوير، وهي مرآة الشخص التي تكشف عن ذاته، والصورة لغة تعرف بالشكل ، وتستعمل بمعنى النوع والصفة التي يتميز بها كل واحد عن الآخر، وتأتي بمعنى المشابهة والمقارنة، وهي تعد عنصرا مكونا لشخصية الإنسان بحيث تميزه عن غيره، وقد شهد الحق في الصورة تطورا ملحوظا في الآونة الأخيرة تحت تأثير التطور التقني.

ويتمثل حق الإنسان في الصورة في هذا المجال بحقه في عدم التقاط الصورة له دون موافقته، كما يتضمن هذا الحق إمكانية رفض بث أو نشر هذه الصورة أو استغلالها دون إذنه، بالإضافة إلى إمكانية اعتراض الشخص على المساس بصورته أو تحريفها أو تغيير ملامحها عن طريق وسائل المونتاج، فالحق في

---

[1] - تنص المادة (303 مكرر) من قانون العقوبات الجزائري على ما يلي: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000دج إلى 300.000دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

أ- .....

ب- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه".

[2]- د. عاقلي فضيلة، المرجع السابق، ص 261.

الصورة يعطي لصاحبه سلطة منع غيره من رسمه أو تصويره إذا لم يكن راغبا في ذلك، ومنع الغير من نشر صورته[1].

فالتقاط الصورة يعني تثبيتها على مادة خاصة يمكن عن طريقها الإطلاع على هذه الصورة مثل : الكاميرا و الهاتف المحمول المزود بالكاميرا[2]، مّا إظهار الصورة في هيئة إيجابية على الدعامة المادية المخصصة لذلك لا يعتبر عنصرا في هذا الركن، لهذا تقع الجريمة تامة في ركنها المادي حتى ولو لم يكن باستطاعة الجاني فنيا معالجة (نيجاتيف) كيميائيا، ولا يؤثر كذلك في قيام الجريمة أن يجري بعد التقاطها تشويهها أو تغييرها ليضفي على الصورة مظهرا هزليا أو مغايرا[3].

أمّا تسجيل الصورة فمعناه حفظ صورة الشخص على مادة معدة لذلك بوسيلة أيا كان نوعها لمشاهدتها فيما بعد أو إذاعتها[4]، و يعني النقل إرسال الصورة إلى مكان أخر غير المكان الذي يوجد فيه صاحبها [5]، مما يتيح للأفراد غير المتواجدين في المكان الذي يوجد فيه المجني عليه الإطلاع على صورته[6].

فنظرا لما للصورة من أهمية خطيرة في التأثير على شخص الإنسان الذي تمثله أو الجمهور الذي يراها، فإنه قد انتشر استغلال الصورة في أغراض مختلفة في الدعاية التجارية وغير التجارية، فقد يترتب على نشر الصورة في حالات معينة تشويه لشخصية الإنسان وإظهارها بشكل مختلف عما يريد أن يظهر به أمام أعين الناس، ومع التطور العلمي الهائل في مجال اختراع التصوير والتقاط الصور، أصبح بالإمكان تصوير الشخص دون حتى الإقتراب منه ودون أن يدري، وأصبح من الممكن نشر صورته الثابتة أو المتحركة حتى حدا بالبعض إلى القول بأنّ المدينة الحديثة هي مدينة الصورة[7].

2- وسيلة إرتكاب الجريمة:

إشترط المشرع الجزائري لقيام الجريمة أن يستخدم الجاني أية تقنية كانت، وبالتالي يمكنه ارتكاب أفعال الإلتقاط أو التسجيل أو النقل من أجل الحصول على الصورة بأية تقنية كانت.

---

[1]- د. علاء الدين عبد الله فواز الخصاونة و د. بشار طلال المومني، النظام القانوني للصورة الفوتوغرافية (الحقوق الواردة عليها ووسائل الحماية القانونية)، مجلة الشريعة والقانون، كلية القانون، جامعة الإمارات العربية المتحدة، العدد53، يناير2013،ص223.

[2]- مقال بعنوان : حرمة الحياة الخاصة، المرجع السابق، ص04.

[3]- د. هشام فريد رستم، الحماية الجنائية لحق الإنسان في صورته، دار النهضة العربية، القاهرة، ط1، 2001، ص89. نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص 264.

[4]- د. إبراهيم عيد نايل، الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الفرنسي، دار النهضة العربية، القاهرة، مصر، ط1، سنة 2000، ص 159. نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص 264.

[5]- د. هشام فريد رستم، الحماية الجنائية لحق الإنسان في صورته، المرجع السابق، ص 89. نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص264.

[6]- مقال بعنوان : حرمة الحياة الخاصة، المرجع السابق، ص04.

[7]- د. عاقلي فضيلة، المرجع السابق، ص255.

إلا أن المشرع الجزائري بموجب التعديل الأخير لقانون العقوبات رقم (14-01)[1] أضاف مادة جديدة هي المادة (333 مكرر 1)[2]، حيث أقر عقوبة الحبس و الغرامة لكل من صور قاصرا لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية، كما تشمل العقوبة كل من قام بإنتاج أو توزيع أو ترويج أية مواد إباحية متعلقة بالقصر، والملاحظ في هذه المادة أن المشرع استعمل عبارة " أية وسيلة كانت" بدل عبارة " أية تقنية كانت"، ولا شك أن عبارة أية وسيلة أوسع من عبارة أية تقنية .

3- المكان الخاص:

إشترط المشرع الجزائري بمقتضى نص المادة(303 مكرر) من قانون العقوبات أن يقوم المتهم بالتقاط صورة المجني عليه، أو تسجيلها أو نقلها حال وجود الغير في مكان خاص.

وقد اختلف الفقه حول تحديد المقصود بالمكان الخاص، فاتجه جانب من الفقه إلى الأخذ بالمفهوم الموضوعي للمكان الخاص، وذهب جانب آخر من الفقه إلى الأخذ بالمفهوم الشخصي لمدلول المكان الخاص.

أ- المفهوم الموضوعي للمكان الخاص:

يرى أصحاب هذا الإتجاه[3] أنّ المكان الخاص يتعين تحديده بصورة موضوعية، فيكون الفعل منوطا بالحماية بالنظر إلى المكان ذاته دون الإلتفات إلى حالة الخصوصية التي يكون عليها الأفراد، فقد قدر أنصار هذا الرأي أنّ التحدث في مكان خاص يعني أنّ كلا من أطراف الحديث إئتمن التحدث معه دون سواه على أسرار حياته الخاصة، بخلاف الحديث في مكان عام حيث تتوافر قرينة قانونية على رضاء المتحدثين بعلم الغير بأسرار هذه الحياة، كذلك الحال بالنسبة لوجود الشخص في مكان عام حيث يكون عرضة لأنظار الآخرين، فلا يكون له أن يعترض على التقاط صورته.[4]

---

[1]- قانون رقم 04-01 مؤرخ في 04 فبراير سنة 2014 المتضمن قانون العقوبات، ج ر رقم 07.

[2]- تنص المادة 333 مكرر 1 من قانون العقوبات الجزائري على ما يلي:" يعاقب .... ، كل من صور قاصرا لم يكمل 18 سنة بأية وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة، حقيقية أو غير حقيقية ، أو صور الأعضاء الجنسية للقاصر لأغراض جنسية أساسا، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر ....".

[3]-Chavanne, La protection de la vie pivée dans la loi du 17 Juillet 1970, Rev, SC, crim 1971, p515.
نقلا عن :د. عاقلي فضيلة، المرجع السابق، ص 156.

[4]- نفس المرجع، ص156.

ب– المفهوم الشخصي للمكان الخاص:

يأخذ أنصار هذا الرأي[1] بمعيار شخصي لتحديد مدلول المكان الخاص، ومؤدى هذا الإتجاه أنه حينما تتوافر حالة الخصوصية فإنّ المكان يعد خاصا، معنى ذلك أنّ العبرة بحالة الخصوصية لا بطبيعة المكان، بحيث أنّ الحالة التي يكون عليها الأشخاص هي التي تصبغ المكان بصفتها وتخلع عليه صفة الخصوصية.

فوجود الشخص في مكان عام لا يعني تنازله عن حرمة حياته الخاصة، وبالتالي من حقه أن يعترض على التقاط صورته هذا من جهة، ومن جهة أخرى يميز هذا الإتجاه بين فرضين : الأول أن يكون المكان عاما في حد ذاته وبغض النظر عمن تواجد فيه صدفة، في هذه الحالة لا يلزم الحصول على إذن الموجودين بالمكان مادام كان وقوعهم في مجال التصوير عرضيا، والثاني أن تكون سمات الوجه الإنساني هي الموضوع الأساسي للصورة، في هذه الحالة لا يكون التقاط الصور أو نشرها مشروعا إلاّ بإذن[2].

ج– المفهوم الوسطي بين الموضوعي والشخصي:

ذهب جانب من الفقه[3] إلى ضرورة التمييز بين إلتقاط الصورة وتسجيل الأحاديث، وذلك في نطاق تحديد مفهوم المكان الخاص، فيرى هؤلاء الفقهاء أنّ الحديث يتمتع بالحماية الجنائية مادام له طابع خاص بغض النظر عن المكان الذي يتم فيه، فحالة الخصوصية التي يكون عليها الأفراد هي التي تصبغ المكان بصبغها وتعطيه صفة الخصوصية[4].

أمّا فيما يتعلق بالتقاط صورة الشخص، فينبغي أن يكون هذا الشخص في مكان خاص، وهذا شرط لتجريم فعل الإلتقاط، في حين لو التقطت الصورة في مكان عام فلا تقوم الجريمة عندئذ، على أساس أنه يفترض موافقة ضمنية من الشخص في أن يكون مرئيا من الجميع ، ولا يختلف عن الأشياء الموجودة في المكان العام.[5]

وقد أخذ المشرع الجزائري بالإتجاه الذي يميز بين تسجيل الأحاديث والتقاط الصورة، وذلك في نص المادة (303 مكرر) من قانون العقوبات الجزائري، فقد فرق بين الأحاديث والصورة، حيث جرم

---

[1] - Ravanas, La protection des personnes contre la réalisation et la publication de leur image, LGDJ, 1978, p516.

نقلا عن : عاقلي فضيلة، المرجع السابق، ص 160.

[2]– د. يوسف الشيخ يوسف، المرجع السابق، ص 119. نقلا عن: نفس المرجع، ص 160.

[3] -Becourt, Reflexion sur le projet de la loi relative à la protection de la vie privée, GP, 1er sem, doct, p202.
نقلا عن: نفس المرجع، ص 161.

[4]– د. حسام الدين كامل الأهواني، المرجع السابق، ص 126. نقلا عن: نفس المرجع، ص 161.

[5]– د. يوسف الشيخ يوسف، المرجع السابق، ص474. نقلا عن: نفس المرجع، ص 161.

الإعتداء على الأحاديث متى كانت لها طبيعة خاصة أوسرية وبأية تقنية كانت دون الإلتفات إلى طبيعة المكان مثلما تبين سابقا، في حين اشترط لتجريم الإعتداء على الصورة أن يكون الشخص موجودا في مكان خاص.

فمادام أن المشرع الجزائري قد جرم إلتقاط صورة الشخص الموجود في مكان خاص، فهنا يطرح الإشكال حول مدى جواز أخذ صورة لشخص في مكان عام دون رضاه ؟

فطبقا لنص المادة (303 مكرر) أكدت على أنّ الإلتقاط أو التسجيل أو نقل الصورة يكون في مكان خاص، فإذا كانت صورة الإنسان قد التقطت له بمناسبة حادث وقع في مكان عام، فإنه لا يجوز له الإعتراض على أساس أنّ الحادث ظرف طارئ يغير المجرى العادي للأمور مثل المظاهرات والمباريات الرياضية.

وقد انقسم الفقه في الإجابة عن هذا الإشكال إلى رأيين، **الرأي الأول** ذهب إلى أنّ الشخص الذي يخرج إلى الأماكن العامة يصير حكمه حكم كل ما يوجد في هذه الأماكن من مباني وحدائق، أمّا **الرأي الثاني** فيرى وجوب التمييز بين حالتين، الحالة الأولى عندما يكون وضع الشخص في الصورة ثانويا غير بارزا، أي أنه يظهر بصفة غير مقصودة، فليس له الحق في الإعتراض، أمّا الحالة الثانية فإنّ الشخص يكون هو الموضوع الرئيسي للصورة فهنا لا يجوز إلتقاط صورته إلاّ برضاء صادر منه.

فلما كان الحق في الصورة من الحقوق الملازمة للشخصية طبقا لنص المادة(47)[1] من القانون المدني الجزائري، وأخذا بالرأي الراجح الذي يرى فيه مظهرا من مظاهر الحق في الخصوصية إذا تعلقت الصورة بحرمة الحياة الخاصة، وحقا مستقلا إذا تعلقت الصورة بالحياة العامة.

فالحق في الصورة يعتبر في كلتا الحالتين حقا من حقوق الشخصية، فالإعتداء على هذا الحق يخول المعتدي عليه اللجوء إلى القضاء دون حاجة لإثبات توافر عناصر المسؤولية المدنية[2].

4- عدم رضاء المجني عليه:

يكتمل الركن المادي لهذه الجريمة بأن يتم إلتقاط أو تسجيل أو نقل صورة المجني عليه دون موافقته حال وجوده في مكان خاص[3]، ولكي يكون الرضاء منتجا لآثاره القانونية لابد أن يصدر عن صاحب الحق

---

[1]- تنص المادة47 من القانون المدني الجزائري على ما يلي:"لكل من وقع عليه إعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الإعتداء والتعويض عما يكون قد لحقه من ضرر".

[2]- حسام الدين كامل الأهواني، المرجع السابق، ص 145. نقلا عن: د. عاقلي فضيلة، المرجع السابق، ص257.

[3]- د. عاقلي فضيلة، المرجع السابق، ص 263.

في الصورة أو من يمثله قانونا بإرادة حرة ومدركة لمدى آثار ذلك الرضاء، ويستوي أن يكون الرضاء صريحا أو ضمنيا، ويجب أن يكون رضاء المجني عليه أو من يمثله قانونا معاصرا لفعل الإلتقاط أو التسجيل أو النقل، فإذا كان سابقا يتعين أن يظل قائما حتى لحظة وقوع الفعل[1].

ثانيا: الركن المعنوي.

تعتبر جريمة إلتقاط أو تسجيل أو نقل الصورة من الجرائم العمدية يتحقق ركنها المعنوي بتوافر القصد الجنائي بعنصريه العلم والإرادة، أي أن يعلم المتهم بأنّ الأفعال التي يأتيها وهي الإلتقاط أو التسجيل أو النقل تشكل جريمة، وإذا انتفى العلم فلا قيام للركن المعنوي ولهذا لا تقوم الجريمة، ومن الأمثلة من يقوم بالتقاط صورة لمنزل أثري في الطريق العام، وتظهر صورة مالكه بالداخل دون موافقته لا يكون مرتكبا لجريمة إلتقاط الصورة.

كما يشترط أن تتجه إرادة الجاني إلى التقاط أو تسجيل أو نقل صورة شخص في مكان خاص دون الحصول على موافقته[2].

ثالثا: العقوبة.

طبقا لنص المادة (303 مكرر) من قانون العقوبات الجزائري، فقد أقر المشرع عقوبة الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة تتراوح من 50.000دج إلى 300.000دج، أمّا في حالة الشروع في ارتكاب هذه الجريمة فيعاقب الجاني بعقوبة الجريمة التامة، كما تتم مصادرة الأشياء التي تستخدم في الجريمة، ناهيك عن العقوبة المقررة بنص المادة (9 مكرر) من قانون العقوبات المتمثلة في الحجر القضائي.

أما فيما يتعلق بعقوبة تصوير قاصر فقد أقر المشرع الحبس من خمس (05) سنوات إلى عشر (10) سنوات وبغرامة من 500.000دج إلى 1000.000 دج، إضافة بمصادرة الوسائل المستعملة لارتكاب الجريمة و الأموال المتحصل عليها بطريقة غير مشروعة[3].

ومن التطبيقات القضائية في هذا الشأن ما عالجته محكمة سيدي بلعباس في قضية تتلخص وقائعها أنه بتاريخ 06-07-2012 تقدمت المدعوة (ت.م.س) بشكوى أمام مصالح أمن دائرة سيدي بلعباس مفادها أنها كانت مخطوبة من طرف شخص يدعى (ق.س)، إلاّ أنه وبعد مرور فترة من الزمن، وقعت

---

[1]- د. إبراهيم عيد نايل، المرجع السابق، ص 132. نقلا عن: د. محمد أمين الخرشة ، المرجع السابق، ص268.

[2]- د. محمد أمين الخرشة ، المرجع السابق، ص269.

[3]- تنص المادة 333 مكرر1 من قانون العقوبات الجزائري على ما يلي :" يعاقب بالحبس من خمس (05) سنوات إلى عشر(10) سنوات وبغرامة من 500.000دج إلى 1000.000 دج ، كل من صور قاصرا لم يكمل 18 سنة .... في حالة الإدانة تأمر الجهة القضائية بمصادرة الوسائل المستعملة لارتكاب الجريمة والأموال المتحصل عليها بصفة غير مشروعة مع مراعاة حقوق الغير حسن النية".

بينهما مشاكل فتم فسخ الخطبة وطالبت منه الإبتعاد عنها إلاّ أنه قام بتهديدها، وفي أحد الأيام ذهب بها إلى منزل مهجور أين قام بنزع ثيابها بالقوة وأخذ صور لها بهاتفه النقال وأصبح يهددها بنشر صورها على شبكة الإنترنت وقام بعرض صورتين لها عن طريق الإنترنت، حيث أنّ المتهم حضر إلى جلسة المحاكمة واعترف أنه فعلا قام بأخذ صور للضحية لكن من أجل تخويفها وليس بقصد نشرها.

غير أنّ الضحية أكدت للمحكمة أنها تصفح عن الضحية وتسامحه، وعليه وطبقا لنص المادة(303 مكرر فقرة أخيرة) من قانون العقوبات فإنّ الصفح يضع حدا للمتابعة الجزائية[1].

البند الثاني: جريمة إلتقاط أو تسجيل أو نقل الصورة في القانون الفرنسي.

جرم المشرع الفرنسي فعل الإلتقاط أو التسجيل أو النقل بموجب نص المادة(226-1)[2] من قانون العقوبات الجديد والتي نص فيها على ما يلي:

"يعاقب بالحبس سنة (01) وغرامة 45000 أورو، كل من اعتدى عمدا بوسيلة أيا كان نوعها على ألفة الحياة الخاصة للآخرين:

1-.....

2- بالتقاط أو تسجيل أو نقل صورة شخص في مكان خاص دون موافقة صاحب الشأن".

ويتضح من هذا النص أنّ هذه الجريمة تتطلب لقيامها توافر ركنين، ركن مادي وركن معنوي، أتطرق إليهما مع بيان العقوبة.

أولا :الركن المادي.

تطبيقا لنص المادة(226-1) من قانون العقوبات، فإنّ الركن المادي لهذه الجريمة يتحقق من خلال قيام المتهم بالنشاط الإجرامي والذي يتمثل في فعل الإلتقاط أو التسجيل أو النقل لصورة شخص موجود في مكان خاص دون رضاه، فيجب أن تتوافر العناصر التالية:

[1]- حكم رقم 13/08503 صادر بتاريخ 2013/10/30 عن قسم الجنح بمحكمة سيدي بلعباس.

[2] - Article 226-1 du (C.P.F Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002): Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1°……..

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

1. السلوك الإجرامي.

2. وسيلة ارتكاب الجريمة.

3. المكان الخاص.

4. عدم رضاء المجني عليه.

وسأتطرق لهذه الشروط على النحو التالي:

1- السلوك الإجرامي:

يتحقق السلوك الإجرامي بالتقاط أو تسجيل أو نقل الصورة، وصورة الشخص هي إمتداد ضوئي لجسمه، وهي على خلاف الحديث لا تعبر عن فكرة ولا دلالة غير إشارتها إلى شخصية صاحبها.

بينما يقصد بالصورة المعاقب على التقاطها أو تسجيلها أو نقلها بمقتضى نص المادة (226-1) من قانون العقوبات الفرنسي، تثبيت أو رسم قسمات شكل الإنسان على دعامة مادية أيا كانت، ومن تم فإنّ الحماية المقررة بهذا النص تخص الإنسان، أما الأشياء أيا كانت أهميتها أو الضرر الناجم عن تصويرها فلا تشملها نطاق هذه الحماية[1].

فالعبرة أن يكون موضوع إلتقاط الصورة أو تسجيلها أو نقلها شخصا، ولا يشترط أن يكون هذا الشخص على قيد الحياة، إنما تمتد الحماية لتشمل الشخص المتوفى حسبما قضت به محكمة النقض المصرية[2].

2- وسيلة إرتكاب الجريمة:

إشترط المشرع الفرنسي في ظل القانون القديم لقيام الجريمة أن يستخدم الجاني في ارتكاب الجريمة"جهازا من الأجهزة أيا كان نوعه"، إلا أنه خرج عن هذا التقييد في ظل قانون العقوبات الجديد واشترط لقيام الجريمة أن يستخدم الجاني"وسيلة أيا كان نوعها"، وبالتالي يمتد نطاق التجريم ليشمل أفعال الإعتداء على الصورة التي ارتكبت بوسائل تقليدية، مثل الرسام الذي يستخدم الريشة في رسم صورة إنسان في مكان خاص[3].

---

[1]- د. عاقلي فضيلة، المرجع السابق، ص261.

[2]- د. محمد أمين الخرشة ، المرجع السابق، ص265.

[3]- نفس المرجع، ص266.

3- المكان الخاص:

إشترط المشرع الفرنسي بمقتضى نص المادة(226-1) من قانون العقوبات، أنه ليتحقق إعتداء عن طريق التصوير يجب أن يكون المجني عليه في مكان خاص، بغض النظر عن الوضع الذي كان عليه الشخص أثناء التقاط أو تسجيل صورته.

وقد سبق بيان المقصود بالمكان الخاص وذلك بالتطرق لمفهومه الموضوعي والشخصي، فبالنسبة للمفهوم الموضوعي للمكان الخاص، فقد سايرت بعض أحكام القضاء الفرنسي هذا الإتجاه في قضية تتلخص وقائعها: "أنّ فتاة أقامت دعوى أمام القضاء على إحدى الصحف الفرنسية لنشر صورتها عارية الصدر برفقة أصدقائها على الشاطئ ، فأصدرت المحكمة حكمها في الدعوى بالرفض تأسيسا على أنّ الشاطئ لا يعد مكانا خاصا في مفهوم المادة (368) من قانون العقوبات[1].

أمّا بالنسبة للمفهوم الشخصي للمكان الخاص، فقد ذهب جانب من القضاء إلى الأخذ به، فقضت محكمة إستئناف Besancon في حكمها الصادر في 5 يناير 1978 بأنّ صالة الفندق تعد مكانا عاما إذا كانت مفتوحة للجميع دون إذن خاص من أي شخص[2].

إلاّ أنّ المشرع الفرنسي من خلال قانون العقوبات الفرنسي الجديد أخذ بالإتجاه الذي يميز بين تسجيل الأحاديث والتقاط الصور، وذلك في نص المادة(226-1)، على أساس تجريمه الإعتداء على الأحاديث متى كانت لها طبيعة خاصة دون الأخذ بطبيعة المكان الذي صدرت فيه، في حين اشترط لتجريم الإعتداء على الصورة أن يكون الشخص موجودا في مكان خاص[3].

4- عدم رضاء المجني عليه:

الرضاء هو عنصر مادي يجب أن يتوافر في الركن المادي للجريمة، إلاّ أنّ المشرع الفرنسي في الفقرة الأخيرة من المادة (226-1) من قانون العقوبات الفرنسي إفترض رضاء الشخص إذا وقع فعل الإلتقاط أو التسجيل أو النقل للصورة على مرآى ومسمع منه دون أن يعترض وكان بوسعه الإعتراض[4].

ثانيا: الركن المعنوي: إنّ جريمة إلتقاط أو تسجيل أو نقل الصورة المنصوص عليها في المادة (226-1) جريمة عمدية، يتخذ ركنها المعنوي صورة القصد العام ويتحقق بتوافر عنصري العلم والإرادة، كما ينبغي

---

[1]-TGI Paris, 18 Mars 1971.

نقلا عن : د.عاقلي فضيلة، المرجع السابق، ص263.

[2]- نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص267.

[3]- د. عاقلي فضيلة، المرجع السابق، ص 162.

[4]- د. محمد أمين الخرشة، المرجع السابق، ص 268.

أن تتجه إرادة الجاني إلى التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص دون الحصول على موافقته أو رضاه[1].

ثالثا: العقوبة.

عاقب المشرع الفرنسي على جريمة إلتقاط أو تسجيل أو نقل الصورة بعقوبة الحبس مدة سنة والغرامة 45000 أورو، أمّا في حالة الشروع في ارتكاب هذه الجريمة فيعاقب عليها المشرع بنفس عقوبة الجريمة التامة، إضافة إلى مصادرة جميع الأشياء والأدوات التي استخدمت في ارتكاب الجريمة وهذه الأخيرة تعد من العقوبات التكميلية.

البند الثالث: جريمة إلتقاط أو نقل الصورة في القانون المصري.

نصت المادة (309 مكرر فقرة ب) من قانون العقوبات المصري على أنه :"يعاقب بالحبس مدة لا تزيد على سنة (01) من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن إرتكب أحد الأفعال التالية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه.

أ- .....

ب- إلتقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص".

ويتبين من خلال نص المادة(309 مكرر) أنه يشترط لقيام هذه الجريمة توافر ركنين : ركن مادي وركن معنوي سأتطرق لهما مع بيان العقوبة.

أولا :الركن المادي.

حدد المشرع فعلين تقوم بهما الجريمة وهما: الإلتقاط والنقل، فالإلتقاط يعني تثبيت الصورة على مادة حساسة، وبمجرد إلتقاط الصورة يتحقق الركن المادي للجريمة، لهذا تقع الجريمة تامة في ركنها المادي حتى ولو لم يكن باستطاعة الجاني فنيا المعالجة كيميائيا لإظهار الصورة[2].

أمّا النقل فيعني إرسال الصورة مباشرة إلى مكان آخر بحيث يتمكن الغير من الإطلاع عليها، ويستوي أن يكون هذا المكان خاصا أو عاما، كما يشترط المشرع المصري لقيام جريمة الحصول على الصورة أن يستخدم

[1]- د. عاقلي فضيلة، المرجع السابق، ص264.

[2]- د. محمد زكي أبو عامر، الحماية الجنائية للمحادثات والأوضاع الخاصة، المرجع السابق، ص 93. نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص283.

الجاني في ارتكاب هذه الأفعال جهازا أيا كان نوعه، فلا يمكن أن تقوم الجريمة من خلال رسم صورة لشخص مهما بلغت دقتها أو قام بعمل تمثال له، لأنّ الأداة المستعملة لا تعد من قبيل الأجهزة.

فيستوي أن يرتكب فعل الإلتقاط أو النقل بجهاز أيا كان نوعه، سواء كان الجهاز كاميرا بعيدة المدى، أو دائرة تليفزيونية مغلقة تنقل الصورة عن طريق أجهزة توضع في مكان خاص وتمكن المتهم من رؤية ما يدور فيها على شاشة تلفزيونية، لذا تحوط المشرع المصري من خلال تعبير "بجهاز من الأجهزة، أيا كان نوعه"، ليشمل جميع الأجهزة التي سيسفر عنها العلم الحديث[1].

كما يشترط أن يكون إلتقاط الصورة أو نقلها قد تم بغير رضاء المجني عليه، أي دون موافقته الصريحة أو الضمنية.

ثانيا : الركن المعنوي.

يتحقق الركن المعنوي في هذه الجريمة بتوافر القصد الجنائي بعنصريه العلم والإرادة باعتبارها جريمة عمدية، فلا يكفي لقيامها توافر الخطأ غير العمدي، و إذا انتفى علم الجاني ينتفي قيام القصد الجنائي، فضلا عن أنه يتعين أن تتجه إرادة الجاني إلى التقاط أو نقل صورة في مكان خاص[2].

ثالثا: العقوبة.

إن جريمة إلتقاط أو نقل الصورة يعاقب عليها بالحبس مدته لا تزيد عن سنة (01)، أمّا إذا إرتكب الجريمة موظف عام مستغلا بذلك وظيفته ، تكون العقوبة الحبس الذي يصل حده الأقصى لمدة لا تتجاوز ثلاث (03) سنوات، إضافة إلى عقوبات تكميلية تتمثل في مصادرة الأجهزة و الوسائل المستعملة لارتكاب الجريمة ومحو الصور، وذلك للحفاظ على حرمة الحياة الخاصة[3].

الفرع الثالث: جريمة الإحتفاظ بالتسجيل أو المستند أو إستعماله أو إعلانه.

إنّ انتهاك حرمة حياة الشخص الخاصة بالتنصت أو تسجيل أو نقل أحاديثه الخاصة أو بإلتقاط أو تسجيل أو نقل صورته أثناء وجوده في مكان خاص لا يحدث في الغالب لمجرد الفضول وحب الإستطلاع، وإنما قد يكون الهدف من ورائه الإستفادة بطريقة أو بأخرى كنشر صورته أو إعلان أحاديثه الخاصة للغير لقاء مبلغ من المال أو تهديد المجني عليه بالنشر[4].

---

[1]- د. محمد أمين الخرشة، المرجع السابق، ص 284.

[2]- نفس المرجع، ص 285.

[3]- د. عاقلي فضيلة، المرجع السابق، ص266.

[4]- نفس المرجع، ص268.

ومن أجل توضيح هذه المسألة سيتم التطرق لجريمة الإحتفاظ بالتسجيل أو المستند أو إستعماله أو إعلانه في القانونين الفرنسي والجزائري في البند الأول ثم لجريمة إذاعة أو استعمال التسجيل أو المستند أو التهديد بالإفشاء في القانون المصري في البند الثاني.

البند الأول: جريمة الإحتفاظ بالتسجيل أو المستند أو إستعماله أو إعلانه في القانون الفرنسي والجزائري.

لقد وسع المشرع الفرنسي والجزائري نطاق الحماية الجنائية لحرمة الحياة الخاصة للأفراد، فلم يقف عند حد تجريم إنتهاك الأحاديث الخاصة والصور ، بل جرم الأفعال اللاحقة لارتكاب هذه الجرائم.

وتأسيسا على ذلك نصت المادة (226-2)[1] من قانون العقوبات الفرنسي على أنه: يعاقب بنفس العقوبات المنصوص عليها في المادة (226-1) كل من احتفظ أو أعلن أو سهل إعلان الجمهور أو الغير أو استعمل علنا أو في غير علانية أي تسجيل أو مستند تحصل عليه بإحدى الطرق المبينة في المادة (226-1) ".

كما نصت المادة (303 مكرر1) من قانون العقوبات الجزائري على أنه:"يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير أو استخدم بأية وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة(303 مكرر) من هذا القانون".

ويتضح من هذين النصين أنّ لهذه الجريمة ركنين، أولهما مادي وثانيهما معنوي[2].

أولا : الركن المادي.

لقد حدد كلا المشرعين حالات أو صور السلوك الإجرامي تتمثل في الإحتفاظ ، الإعلان، تسهيل الإعلان والإستعمال.

---

[1] - Article 226-2 : Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1.
Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

[2]- د. عاقلي فضيلة، المرجع السابق، ص 268.

1-الإحتفاظ:

يقصد به إبقاء الشخص في حوزته تسجيل أو مستند خاص للغير عن قصد ومع علمه بمضمون التسجيل أو المستند، مع ضرورة أن يكون قد تم الحصول عليه بإحدى الطرق المبينة في المادة(226-1) من قانون العقوبات الفرنسي ، والمادة(303مكرر) من قانون العقوبات الجزائري[1].

2-الإعلان:

تمكين الجمهور أي عدد من الناس بغير تمييز، من العلم بمضمون التسجيل و المستند، و ذلك بأية طريقة من طرق العلانية كالمجلات و الصحف .

3-تسهيل الإعلان:

يعني تقديم المساعدة للشخص الذي يقوم بنشر مضمون التسجيل أو المستند، و قد اعتبر الفقهاء أن من يقدم المساعدة يعتبر فاعلا أصليا .

4-إستعمال التسجيل أو المستند:

يراد به استخدام التسجيل أو المستند في تحقيق غرض ما[2] ، إلاّ أنّ المشرع الجزائري لم يفصح عن مسألة استعمال التسجيل أو المستند علنا أو في غير علانية.

ومن تم فإنه يتطلب لقيام الجريمة المنصوص عليها في القانون الفرنسي والجزائري أن ترد أفعال الإحتفاظ أو الإعلان أو تسهيل الإعلان أو الإستخدام على تسجيل حديث أو صورة أو مستند أو وثائق تم الحصول عليها بإحدى الطرق المبنية بالمواد السالفة الذكر[3].

ثانيا: الركن المعنوي.

تعتبر جريمة الإحتفاظ بالتسجيل أو المستند أو استعماله أو إعلانه جريمة عمدية يتخذ ركنها المعنوي صورة القصد، والقصد المتطلب فيها هو القصد الجنائي العام بعنصريه العلم والإرادة.

فيتعين أن يعلم الجاني بمصدر الحصول على التسجيل أو المستند، وأنه يقوم بالإعلان أو الإستعمال للتسجيل أو المستند، أما إذا علم المتهم به بعد إرتكابه للجريمة فلا جريمة آنذاك لتخلف عنصر العلم المكون للقصد العام، وإذا علم الجاني بأنه يرتكب جريمة ورغم ذلك استمر في إتيان الأفعال المادية المكونة للجريمة، فهنا يعد مرتكبا لها.

---

[1]- د. عاقلي فضيلة، المرجع السابق، ص 269.

[2]- مقال بعنوان : حرمة الحياة الخاصة، المرجع السابق، ص07.

[3]- د. عاقلي فضيلة، المرجع السابق، ص 270.

كما يجب أن تتجه إرادة الجاني إلى القيام بالنشاط الإجرامي في أي صورة من صوره التي سبق وأن تم التطرق إليها، فلا تقوم الجريمة في حق من حصل على التسجيل أو الصورة ثم فقد منه، فاحتفظ به أو أعلمه للجمهور أو للغير أو إستعمله من عثر عليه أو من سرقه[1].

ثالثا : العقوبة.

إن جريمة إعلان أو إستعمال التسجيل أو المستند المنصوص عليها في المادة (226-2) من قانون العقوبات الفرنسي جنحة عقوبتها الحبس مدته سنة (01) وغرامة 45000 أورو، بالإضافة إلى مصادرة جميع الأشياء التي تكون قد استعملت في ارتكاب الجريمة، كما أنّ الشروع فيها يعاقب عليه بنفس عقوبة الجريمة التامة.

أمّا بالنسبة للقانون الجزائري فقد نص المشرع في نص المادة (303 مكرر) على العقوبة المقررة لهذه الجريمة وهي الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة تتراوح قيمتها من 50000 دج إلى 300.000دج، بالإضافة إلى مصادرة الأشياء التي استخدمت في ارتكاب الجريمة ويجوز للمحكمة أن تطبق واحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة (303 مكرر2)، كما يعاقب على الشروع في ارتكاب هذه الجنحة بنفس العقوبة المقررة للجريمة التامة.

البند الثاني: جريمة إذاعة أو استعمال التسجيل أو المستند أو التهديد بالإفشاء في القانون المصري.

تنص المادة (309 مكرر أ) من قانون العقوبات المصري على هذه الجريمة ، فنص المادة السالفة الذكر يشتمل على جريمتين، جريمة إذاعة أو استعمال التسجيل أو المستند وجريمة التهديد بالإفشاء، وسأتطرق لكلا الجريمتين على النحو التالي:

أولا: جريمة إذاعة أو استعمال التسجيل أو المستند.

إنّ موضوع الجريمة هو التسجيل أو المستند الذي تم الحصول عليه عن طريق ارتكاب أحد الأفعال المنصوص عليها في المادة (309 مكرر).

وسيتم التطرق للركن المادي والركن المعنوي مع بيان العقوبة المقررة لهذه الجريمة.

[1] - د.إبراهيم عيد نايل، المرجع السابق، ص 200. نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص273.

1.الركن المادي.

يتكون الركن المادي لهذه الجريمة من الصور التالية: الإذاعة أو تسهيل الإذاعة أو الإستعمال، فيقصد بالإذاعة تمكين عدد محدود من الناس من العلم أو الإطلاع على فحوى المستند أو التسجيل، سواء تعلق بحديث أو صورة[1]، أمّا تسهيل الإذاعة فهي تقديم العون إلى من يقوم بعملية الإذاعة أو النشر، ويعني الإستعمال إستخدام التسجيل أو المستند لتحقيق غرض ما، ويستوي أن يحصل الإستعمال علنا أو في غير علانية[2].

2.الركن المعنوي.

تعد جريمة إذاعة أو استعمال التسجيل أو المستند جريمة عمدية، يتكون ركنها المعنوي من القصد الجنائي العام بعنصريه العلم والإرادة، فيجب أن يكون الجاني عالما بأنّ التسجيل أو المستند تم الحصول عليه بطريق غير مشروع، كما يتعين أن يعلم الجاني أنّ فعله سيترتب عليه إذاعة أو تسهيل إذاعة أو استعمال التسجيل أو المستند مع علمه بانعدام رضاء المجني عليه وأن تتجه إرادة الجاني إلى ذلك[3].

3- العقوبة.

حدد المشرع المصري عقوبة الحبس كعقوبة أصلية دون أن يحدد حدا أدنى أو أقصى لها، مع وجوب مصادرة الأجهزة التي ارتكبت بها الجريمة، وكذلك الحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها، وشدد المشرع العقوبة إذا كان الجاني موظفا عاما إعتمد على وظيفته في ارتكابه الجريمة، إذ تصبح العقوبة السجن بين حديه الأدنى والأقصى[4].

ثانيا: جريمة التهديد بالإفشاء.

تشتمل على ركنين، ركن مادي وركن معنوي، سنتطرق لهما مع بيان العقوبة المقررة لهذه الجريمة.

1- الركن المادي.

التهديد بالإفشاء هو الضغط على إرادة المجني عليه عن طريق الوعد بشر معين هو عملية الإفشاء التي غالبا ما تكون منطوية على أمر فيه ما يشين إلى شخص المعتدى عليه، ويستوي أن يكون التهديد شفويا أو كتابيا أو حتى بالإشارة أو بإذاعته علنا في جريدة، ولو كان النشر لغرض علمي[5]، فالجريمة لا تقوم

---

[1]- د. فوزية عبد الستار، المرجع السابق، ص 648. نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص287.

[2]- د. محمد أمين الخرشة، المرجع السابق، ص287.

[3]- د. يوسف الشيخ يوسف، المرجع السابق، ص302. نقلا عن: د. محمد أمين الخرشة، المرجع السابق، ص288.

[4]- نفس المرجع، ص 288.

[5]- د. رؤوف عبيد، المرجع السابق، ص 437. نقلا عن: د. عاقلي فضيلة، المرجع السابق، ص248.

بمجرد التهديد إذ يجب أن يكون الغرض من التهديد هو الإفشاء بحسب رأي الفقه.

2- الركن المعنوي.

تتخذ هذه الجريمة صورة القصد الجنائي العام والخاص أي علم الجاني وإرادته، أمّا القصد الخاص يتمثل في نية حمل الشخص على القيام بعمل أو الإمتناع عنه، ويستوي أن يكون العمل المستهدف بالتهديد مشروعا أو غير مشروع، وسواء كان الشخص الذي يريد المتهم حمله على العمل أو الإمتناع هو المجني عليه نفسه أم شخص آخر له عليه سلطان[1].

3- العقوبة.

عقوبة هذه الجريمة هي السجن لمدة لا تزيد عن خمس (05) سنوات، أما إذا ارتكب هذه الجريمة موظفا عاما مستغلا بذلك وظيفته تشدد العقوبة، بالإضافة إلى مصادرة الوسائل و الأدوات التي ارتكبت بها الجريمة و محو التسجيلات.

الفرع الرابع: جريمة نشر المونتاج.

بالإضافة إلى الجرائم السابقة، جرم المشرع الفرنسي نشر المونتاج في المادة (226-8)[2] من قانون العقوبات الفرنسي، وإن كان المشرع الجزائري قد خص هذه الجريمة بشخص رئيس الجمهورية[3]، واستنادا للمادة المذكورة فإنّ جريمة نشر المونتاج تتكون من ركنين: ركن مادي وركن معنوي.

---

[1]- د. محمود نجيب حسني، المرجع السابق، ص 248. نقلا عن: د.عاقلي فضيلة، المرجع السابق، ص248.

[2] - Article 226-8 du (C.P.F Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002): Est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention.
Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

[3]- تنص المادة 144 مكرر(عدلت بالقانون رقم 11-14 المؤرخ في 02 غشت 2011 المتضمن قانون العقوبات): "يعاقب بغرامة من مائة ألف (100.000) دج إلى خمسمائة ألف 500.000دج كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.
تباشر النيابة العامة إجراءات المتابعة الجزائية تلقائيا.
وفي حالة العود، تضاعف الغرامة".

أولا: الركن المادي.

يتضمن الركن المادي عنصرين: نشر الصورة أو الحديث بواسطة المونتاج، ويرتبط المونتاج بالحديث والصورة، لذلك فالمجلات تقوم بنشر صور لأشخاص لا علاقة بينهم، كما قد يكون موضوع المونتاج كلمات صدرت من أشخاص لا يعرفون بعضهم، ويتم تسجيلها على أشرطة مع تغيير صورة المتحدث، أي تركيب صورة على صورة شخص آخر، واشترط المشرع أن يكون المونتاج دون رضاء المجني عليه[1].

ثانيا: الركن المعنوي.

يتخذ الركن المعنوي صورة القصد الجنائي العام بعنصريه العلم والإرادة[2].

ثالثا :العقوبة.

تتمثل العقوبة في الحبس لمدة سنة (01)، والغرامة 15000 أورو، بالإضافة إلى عقوبة تكميلية تتمثل في مصادرة الأشياء التي استخدمت في المونتاج.

ما ينبغي الإشارة إليه أن الجزاءات الجنائية التي تم التطرق إليها تتعلق فقط بالإستخدام غير المشروع لوسائل المراقبة الإلكترونية، وذلك ما دام أن الأمر يتعلق بالدليل الإلكتروني، لأن هناك جزاءات أخرى نص عليها المشرع الجزائري من أجل حماية الحياة الخاصة للأفراد وتتعلق بتجاوزات موظفي وأعوان السلطة العامة[3]

---

[1]– د. عاقلي فضيلة، المرجع السابق، ص267.

[2]– نفس المرجع، ص 267.

[3]– من نصوص قانون العقوبات التي تجرم تجاوزات موظفي وأعوان السلطة العامة ما يلي:

– المادة 107 :" يعاقب الموظف بالسجن المؤقت من خمس(5) إلى عشر(10) سنوات إذا أمر بعمل تحكمي أو ماس سواء بالحرية الشخصية للفرد أو بالحقوق الوطنية لمواطن أو أكثر ."

– المادة 135(القانون رقم 82-04 المؤرخ في 1982/02/13):" كل موظف في السلك الإداري أو القضائي وكل ضابط شرطة وكل قائد أو أحد رجال القوة العمومية دخل بصفته المذكورة منزل أحد المواطنين بغير رضاه، وفي غير الحالات المقررة في القانون وبغير الإجراءات المنصوص عليها فيه، يعاقب بالحبس من شهرين (2) إلى سنة (1) وبغرامة من 20.001 دج إلى 100.000 دج دون الإخلال بتطبيق المادة 107." (تم الرفع من قيمة الغرامة طبقا لما ورد في المادة 467 مكرر التي جاء بها القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006) .

– المادة137(القانون رقم 06-23 المؤرخ في 2006/12/20):" كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة للبريد يقوم بفض أو اختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اختلاسها أو إتلافها، يعاقب بالحبس من ثلاثة (3) أشهر إلى خمس(5) سنوات وغرامة من 30.000 دج إلى 500.000 دج.

ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق يختلس أو يتلف برقية أو يذيع محتواها ."

– المادة 263 مكرر 2 (القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004):" يعاقب بالسجن المؤقت من عشر(10) سنوات إلى عشرين(20) سنة وبغرامة من 150.000 دج إلى 800.0000 دج ، كل موظف يمارس أو يحرض أو يأمر بممارسة التعذيب من أجل الحصول على اعترافات أو معلومات أو لأي سبب أخر .

وتكون العقوبة السجن المؤبد، إذا سبق التعذيب أو صاحب أو تلى جناية غير القتل العمدي.

يعاقب بالسجن المؤقت من خمس(5) سنوات إلى عشر (10) سنوات و بغرامة من 100.000 دج إلى 500.000 دج، كل موظف يوافق أو يسكت عن الأفعال المذكورة في المادة 263 مكرر من هذا القانون."

وكذا تجاوزات الأفراد[1]، ولذلك فالنتيجة التي يمكن التوصل إليها من أجل الحصول على دليل مشروع يمكن الإعتماد عليه في إثبات الجريمة هي ضرورة إلتزام جهات التحقيق وباقي أطراف الدعوى بألا يعتمدوا أو يقدموا دليلا تم الحصول عليه بطرق غير مشروعة .

[1]– من نصوص قانون العقوبات التي تجرم تجاوزات الأفراد ما يلي:

– المادة 263 مكرر 1 (القانون رقم 04–15 المؤرخ في 2004/11/10): " يعاقب بالسجن المؤقت من خمس(5) سنوات إلى عشر(10) سنوات وبغرامة من 100.000دج إلى 500.000 دج كل من يمارس أو يحرض أو يأمر بممارسة التعذيب على شخص .

يعاقب على التعذيب بالسجن المؤقت من عشر(10) سنوات إلى عشرين(20) سنة وبغرامة من 150.000 دج إلى 800.000 دج، إذا سبق أو صاحب أو تلى جناية غير القتل العمد ."

–المادة 291 (معدلة بالقانون رقم 14–01 المؤرخ في 2014/02/04): "يعاقب بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة كل من اختطف أو قبض أو حبس أو حجز أي شخص بدون أمر من السلطات المختصة وخارج الحالات التي يجيز أو يأمر فيها القانون بالقبض على الأفراد.

و تطبق ذات العقوبة على من أعار مكانا لحبس أو لحجز هذا الشخص.

إذا استمر الحبس أو الحجز لمدة أكثر من شهر فتكون العقوبة السجن المؤبد ."

–المادة292 :" إذا وقع القبض أو الإختطاف مع ارتداء بزة رسمية أو شارة نظامية أو يبدو عليها ذلك على النحو المبين في المادة 246 أو بانتحال إسم كاذب أو بموجب أمر مزور على السلطة العمومية فتكون العقوبة السجن المؤبد.

وتطبق العقوبة ذاتها إذا وقع القبض أو الإختطاف بواسطة إحدى وسائل النقل الآلية أو بتهديد المجني عليه بالقتل.

– المادة 293 (القانون رقم 06–23 المؤرخ في 2006/12/20) : "إذا وقع تعذيب بدني على الشخص المختطف أو المقبوض عليه أو المحبوس أو المحجوز يعاقب الجناة بالسجن المؤبد ."

–المادة 301(القانون رقم 82–04 المؤرخ في 1982/02/13):" يعاقب بالحبس من شهر(1) إلى ستة (6) أشهر وبغرامة من 20.001 دج إلى 100.000 دج الأطباء والجراحون والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلي بها إليهم وأفشوها في غير الحالات التي يوجب عليهم فيها القانون إفشاءها ويصرح لهم بذلك ...". (تم الرفع من قيمة الغرامة طبقا لما ورد في المادة 467 مكرر التي جاء بها القانون رقم 06–23 المؤرخ في 20 ديسمبر 2006) .

–المادة303 (القانون رقم 06–23 المؤرخ في 2006/12/20) :" كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137، يعاقب بالحبس من شهر(1) إلى سنة(1) وبغرامة من 25.000 دج إلى 100.000 دج أو بإحدى هاتين العقوبتين فقط ."

خاتمة:

بعد الإنتهاء من دراسة موضوع مشروعية الدليل الإلكتروني في مجال الإثبات الجنائي، سيتم إبراز النتائج التي أسفرت عنها هذه الرسالة، حيث حاولت بحث كافة الجوانب المتعلقة بها والتوصل إلى الحلول المناسبة، خاصة وأنّ قواعد الإثبات الخاصة بالجرائم الإلكترونية تميزها عوائق كثيرة تتمثل في عدم وجود أثر مادي ملموس يدل على ارتكاب هذه الجرائم، وسهولة محو وإتلاف الدليل الإلكتروني، كما أنها تحتاج إلى آليات ووسائل خاصة لكشفها والوصول إلى الحقيقة والوقوف على ماهية الأدلة الإلكترونية، وهنا يبرز دور الدليل العلمي في الإثبات الجنائي.

غير أنّ إكتشاف هذه الجرائم ومعاقبة مرتكبيها يكون عن طريق إجراءات مشروعة، تعتمد على جمع الأدلة الإلكترونية بشكل يساعد على إثبات الجريمة وفق ما ينص عليه القانون، سواء كانت هذه الإجراءات تقليدية أو حديثة، خاصة وأن الإثبات في هذه النوعية من الجرائم يستلزم ضرورة استخدام تقنيات حديثة، لأنه يتم في بيئة إفتراضية متغيرة ومتجددة عكس البيئة التقليدية.

وبالرغم من إصدار القوانين وإجراء التعديلات اللازمة، إلاّ أنّ تطبيق هذه القوانين تقابله تحديات إجرائية ترجع إلى الطبيعة الخاصة لهذه الجرائم، إضافة إلى صعوبة تطبيق بعض الإجراءات التقليدية مثل المعاينة والتفتيش والضبط وغيرها، لأن الأمر يحتاج إلى ضرورة مواكبة التطور، إذ أصبحت هذه الإجراءات عاجزة عن إثبات مثل هذه الجرائم، هذا إضافة إلى عوائق أخرى ناتجة عن عدم وجود إتفاقيات بين الدول بخصوص الجرائم الإلكترونية التي تتعدى حدود الدولة الواحدة، حيث أصبحت هذه الإتفاقيات ضرورية من أجل التعاون في مجال الإجراءات الجزائية.

وتجدر الإشارة إلى أنّ فعالية إجراءات التحقيق في هذه النوعية من الجرائم مرهونة بمدى توافر التأهيل العلمي والتقني لدى جهات التحقيق، كما أنّ هذا التحقيق محكوم بعدم المساس بالخصوصية الفردية والتي يترتب على انتهاكها وعدم مشروعية الدليل جزاءات قد يكون مصدرها قانون الإجراءات الجزائية عن طريق إبطال الإجراء المخالف للقانون وعدم ترتيبه أي أثر قانوني، كما قد تترتب جزاءات عقابية نتيجة التصرفات غير القانونية.

ولقد توصل البحث من خلال هذه الدراسة إلى النتائج التالية:

1.تتميز الجرائم الإلكترونية عن الجرائم التقليدية بمجموعة من الخصائص جعلتها تتميز بطبيعة فنية وتقنية معقدة، ناهيك عن أنّ مجرمي المعلوماتية يتميزون عن غيرهم بصفات تسهل من ارتكابهم لهذه الجرائم، وفي المقابل تجعل مهمة الكشف عنها صعبة للغاية.

2.إنّ الطبيعة الخاصة للجرائم الإلكترونية جعلت من إجراءات التحقيق تتميز بخصوصية فرضتها البيئة الرقمية، والتي حولت الدليل الجنائي التقليدي إلى دليل من نوع آخر، ويصطلح على تسميته بالدليل الإلكتروني والذي هو عبارة عن معلومات مخزنة في الحاسب الآلي أو وسائل إلكترونية أخرى يتم الحصول عليها من خلال إجراءات فنية وقانونية لتقديمها للقضاء بعد ترجمتها من أشخاص متخصصين في هذا المجال، وذلك لإثبات وقوع الجريمة الإلكترونية.

3.من خلال خصائص الجريمة الإلكترونية يتضح أن هناك صعوبة في جمع الأدلة والتصرف فيها لكونها عبارة عن معلومات ذات طبيعة معنوية غير محسوسة، كما أنّ البيانات الموجودة على الكمبيوتر يمكن العبث بها أو محوها بالكامل في ثوان معدودة.

4.في ظل الجرائم التقليدية تقوم جهات التحقيق بجمع الأدلة بطرق تقليدية عن طريق المعاينة والضبط والتفتيش، غير أنّ هذه الإجراءات التقليدية يصعب القيام بها في الجرائم الإلكترونية، كالمعاينة التي يكون لها دور أقل من دورها بالنسبة للجرائم التقليدية.

5.أمّا فيما يتعلق بالتفتيش، فإنه يتم في هذه النوعية من الجرائم على النظم المعلوماتية كنظم الحاسوب وشبكات المعلومات، وقد يتجاوز النظام المشتبه فيه إلى أنظمة أخرى مرتبطة به، إلاّ أنّ امتداد التفتيش يطرح تساؤلات حول مدى مشروعية هذا الإجراء، وإن كان المشرع الجزائري من خلال القانون رقم (09-04) المؤرخ في 14 شعبان سنة 1430هـ الموافق لـ 5 غشت سنة 2009، والذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، قد أجاز التفتيش ولو عن بعد في منظومة معلوماتية أخرى أو جزء منها وذلك بعد إعلام السلطة القضائية المختصة بذلك، كما يمكن تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة ويكون ذلك بمساعدة السلطات الأجنبية وفقا للإتفاقيات الدولية وكذا مبدأ المعاملة بالمثل.

6.يجب أن يمتد التفتيش ليشمل كل البيانات الملموسة والغير الملموسة، وفي حالة البيانات التي تتميز بطبيعتها المعنوية، فإنه ينبغي تحويلها إلى شكل مادي عن طريق طباعتها بواسطة مخرجات الطباعة حتى يمكن ضبطها وبالتالي إعتمادها كدليل لإثبات هذه الجرائم.

7.يجب أن يراعى أثناء التفتيش مجموعة من الضمانات التي تحدد نطاقه المكاني والزمني ، وهذا نظرا لخطورته ومساسه بالحريات الشخصية للأشخاص وكذا حرمة مساكنهم، فهو من أشد إجراءات التحقيق أثرا على الحرية الشخصية المكفولة بموجب الدساتير والقوانين، وإن كان قد تم التطرق لهذه الضمانات في مواضع متفرقة خلال البحث.

8.قد يجد القائم بالتفتيش وهو يقوم بهذا الإجراء أنه سوف يطلع على كافة محتويات الحاسب الآلي، مما قد يشكل إعتداءا على الخصوصية، وبالتالي من حق هذا الشخص أن يرفض هذا الدليل غير المشروع، لأن الحق في الحياة الخاصة هو من الحقوق الأساسية للإنسان والتي تمس ذاته وكرامته الشخصية ، خاصة إذا كشف هذا التحقيق عن تفاصيل كثيرة لا يرغب في كشفها وليس من حق القائم بالتفتيش الإطلاع عليها، لذلك أوليت أهمية خاصة لدراسة شروط صحة الإذن بالتفتيش نظرا لمساسها بالحريات الشخصية للفرد.

9.يترتب على التفتيش الذي يتم وفقا للإجراءات المنصوص عليها قانونا أثر يتمثل في ضبط الأشياء التي تفيد في كشف الحقيقة عن الجريمة المرتكبة ، وهذه الأشياء قد تكون مادية تنصب على جميع الأجهزة والأدوات التي تم تخزين المعلومات فيها، كما قد تكون معنوية تتمثل في المعطيات المعالجة إلكترونيا.

10.إنّ القواعد التقليدية للشهادة ليس بإمكانها فرض الإلتزام بالإعلام على الشاهد المعلوماتي في الجرائم الإلكترونية، وذلك من أجل إجباره على الإدلاء بالمعلومات التي من شأنها تذليل الصعوبات أثناء إجراء التحقيق، مع أنه ينبغي فرض مثل هذا الإلتزام في مجال التحقيق في هذه الجرائم يتمثل في واجب التعاون مع الجهات القضائية وإن كانت هناك شروط سبق التطرق إليها تتعلق بإلزام الشاهد بالإعلام في الجريمة الإلكترونية.

أمّا فيما يخص الشهادة الإلكترونية عبر الإنترنت، فإنه لا مانع من اللجوء إليها لإثبات الجرائم الإلكترونية، وهذا راجع للطبيعة الخاصة لهذه الجرائم خاصة مع افتراض وجود هذا الشاهد خارج الدولة التي وقع فيها الفعل مع عدم إمكانية مجيئه، كما يرى الفقهاء أنّ حضور الشاهد عبر الإنترنت وهو يتحدث وملاحظة ردود أفعاله يساعد المحكمة على تقدير قيمة الشهادة بصورة أفضل، وكل ذلك يصب في مصلحة التحقيق في حالة وجود أسباب تمنعه من الحضور.

11. إن الإستعانة بالخبراء في مجال الجريمة الإلكترونية مسألة محتمة وضرورية أثناء التحقيق في هذه الجرائم ذات الطبيعة الفنية والتقنية ، خاصة عندما تواجه جهات التحقيق مسألة فنية لا تملك تلك السلطات الخبرة الفنية اللازمة لإجرائها، وبالتالي فإنّ اعتماد المحكمة على تقرير الخبير المعلوماتي لا يعد مساسا بمبدأ قناعة القاضي الشخصية، ولا يجعل من الخبير المسيطر والمهيمن على الدعوى، كما توصلت إلى نتيجة مفادها أنه يمكن الإستعانة بالخبير الأجنبي إذا كانت هناك إتفاقيات دولية تجيز ذلك.

12.من بين التعديلات الجديدة التي جاء بها قانون الإجراءات الجزائية والمتضمنة بالقانون رقم (06-22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية أنه منح لقاضي التحقيق صلاحيات جديدة من بينها التسرب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وذلك لمواجهة جرائم معينة نظرا لطبيعتها الخاصة وخطورتها ومن بين هذه الجرائم التي خصها بالذكر الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

13.إنّ الكشف عن هذا النوع من الجرائم وإثباتها ليس بالأمر الهين، ولذلك فإنّ الأمر يتطلب من جهات التحقيق أن تتصدى لها بالبحث العلمي واستخدام تقنيات حديثة في عمليات التحري والكشف عن الأدلة والتحقيق، كإجراءات التحفظ السريع على مضمون البيانات المخزنة وإجراءات التحفظ على البيانات المتعلقة بخط سير البيانات، إصدار أوامر بتقديم بيانات محددة ومراقبة الإتصالات الإلكترونية، فهذه الإجراءات الحديثة تتفق مع طبيعة الدليل الإلكتروني وهذا نظرا لكون الإجراءات التقليدية لجمع الدليل لم تعد كافية.

14.إنّ القانون رقم (09-04) والذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، قد أجاز المراقبة الإلكترونية غير أنّ ذلك يكون عن طريق توافر ضمانات حتى يكون الدليل المستمد منها هو دليل مشروع، فالمراقبة الإلكترونية حسب ما توصل إليه الفقهاء ليست لا تفتيشا ولا ضبطا وإنما هي إجراء خاص ترد فقط على الإتصالات الإلكترونية حال أو أثناء إجرائها.

15.يجوز اللجوء إلى التسجيل الصوتي كأثر من الآثار المترتبة على المراقبة الإلكترونية مع مراعاة مجموعة من الضمانات الفنية و القانونية للتأكد من صحته.

16.وبالنسبة لمسألة الاختصاص، ففي هذه الحالة ينبغي اللجوء إلى القواعد العامة المتعلقة بالجرائم التقليدية، وهذه المبادئ هي مبدأ الإقليمية، العينية، الشخصية والعالمية، وعليه يمكن تطبيق هذه المبادئ على الجرائم الإلكترونية، وإن كانت بعض التشريعات تأخذ بمبدأ العالمية نظرا لوقوع الجريمة الإلكترونية في أكثر من إقليم أي عابرة للحدود.

17.أمّا بالنسبة لمسألة قبول الدليل الإلكتروني، فيمكن للقاضي الجزائي الأخذ به على اعتبار أنّ نظام الإثبات الحر السائد في قضائنا يسمح له بذلك، مع ضرورة توافر شروط معينة سبق التفصيل فيها تتمثل في شرط المشروعية الذي يقتضي أن يتم الحصول على الدليل الإلكتروني بصورة قانونية مع توافر شرط الصحة والمطابقة، أي أن يكون الدليل الإلكتروني المقدم إلى المحكمة هو نفس الدليل الذي تم جمعه، وأن لا يطرأ على هذا الدليل أي تغيير خلال فترة حفظه، وأن يكون نظام الحاسوب الذي استخرج منه الدليل يعمل على نحو دقيق وسليم.

18.وفيما يتعلق بكيفية تقدير قيمة الدليل الإلكتروني، فلابد من التمييز بين أمرين: القيمة العلمية القاطعة للدليل والظروف والملابسات التي وجد فيها الدليل، وعليه فالقاضي لا يمكنه مناقشة ما هو ثابت من الناحية العلمية لأنه من الصعب استبعاده، وإن كان ينبغي ضرورة حسن استخدام الدليل العلمي حتى لا يكون هناك إنتهاك لحقوق وحريات الأشخاص، أما فيما يتعلق بالظروف والملابسات التي أحاطت بالدليل فله أن يقدرها، لأن هذا الأمر يدخل ضمن صلاحياته، فله مثلا أن يستغني عن هذا الدليل إذا كان غير متوافقا مع معطيات الواقعة.

19.لقد أثبتت الدراسة أنّ البطلان المترتب على مخالفة ضمانات وضوابط المراقبة الإلكترونية هو بطلان متعلق بالنظام العام وليس نسبي، وبالتالي يجوز إثارته في أي مرحلة كانت عليها الدعوى، وعلى المحكمة أن تقتضي به من تلقاء نفسها، نظرا لأنّ مخالفة ما نص عليه القانون يعد انتهاكا للخصوصية التي يتمتع بها الفرد، كما حرصت التشريعات على النص على جزاءات عقابية لكل مساس بحق الإنسان في حرمة حياته الخاصة عن طريق تجريم كل فعل من شأنه التعدي على ذلك الحق.

20.لقد كان لظهور هذه النوعية من الجرائم دورا أساسي في قيام الكثير من الدول بسن تشريعات جديدة أو تعديل تشريعاتها القائمة، وذلك من أجل مواجهتها وتفادي مشكلاتها القانونية، وذلك مثل الجزائر التي قامت بتعديل قانون العقوبات بموجب القانون رقم (04-15) المؤرخ في 10 من نوفمبر سنة 2004، وذلك بإضافة قسم خاص تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، كما أنّ هناك تعديلا آخر في قانون الإجراءات الجزائية الجزائري بموجب القانون رقم (06-22) المؤرخ في 20 ديسمبر 2006، ناهيك عن القانون رقم (09-04) المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وهذا على عكس بعض التشريعات العربية التي بقيت عاجزة عن إصدار تشريع خاص بمكافحة الإجرام الإلكتروني.

21.إنّ النصوص التقليدية التي تحمي الحق في الخصوصية لا تكفي وحدها لمواجهة الإعتداء على الحياة الخاصة للأفراد، وحتما ستكون عاجزة خاصة مع التطور الكبير في أجهزة التنصت مثلا، أين يكون الشخص

عرضة للمساس بسرية محادثاته الشخصية والهاتفية خاصة مع التمسك بمبدأ الشرعية، مما يجعل التفسير الضيق الذي يجب أن يراعيه القاضي عائقا أمام مواجهة الظروف المستجدة والتي قد تشمل أفعالا لم يشملها النص التقليدي.

22.إنّ الحقيقة العلمية تضلل الحقيقة القضائية، ولذلك يجب تدريب وتأهيل رجال العدالة بما في ذلك جهات التحقيق والقضاة لمعالجة هذه النوعية من الجرائم، والتي تحتاج إلى خبرات وتقنيات عالية، وهنا تظهر أهمية التخصص، خاصة عندما يكون هؤلاء أمام مناقشة الأدلة الإلكترونية وتقديرها حتى يمكن الحصول على دليل صحيح يمكن الإعتماد عليه.

23.لا يمكن لدولة مواجهة هذه الأنماط المستحدثة من الجرائم بمفردها دون تعاون وتنسيق مع غيرها من الدول، إذ لابد من إيجاد استراتيجيات وآليات محكمة سواء في مجال المساعدات القضائية المتبادلة أو في مجال تسليم المجرمين.

24.أقرت معظم التشريعات المقارنة نصوصا خاصة لتنظيم مسؤولية مزودي الخدمات، كما يقع على عاتقهم الإلتزام بالمراقبة والسهر على تطبيق القوانين واللوائح، مع إلزامهم بالتعاون مع رجال الضبط القضائي وإقرار مسؤوليتهم القانونية عن محتوى المواقع الإلكترونية في حالة نشر ما يخالف القانون.

وبعد التطرق للنتائج التي توصل إليها البحث، يمكن عرض التوصيات التي رأيتها مناسبة، وسوف يتم إجمالها في النقاط التالية:

1. يجب أن يتناسب تعريف الجريمة الإلكترونية مع التطور اللامتناهي لتكنولوجيا المعلومات والإتصالات، وذلك بهدف الإلمام بكل صور هذه الجريمة مهما وصلت درجة التقدم في هذا المجال، كما يجب أن يراعى في هذا التعريف مبدأ الشرعية وذلك بالتطرق إلى خصائص الجريمة الإلكترونية، وينبغي أن تصاغ النصوص القانونية بأسلوب لا يقف عائقا أمام التطور العلمي في مجال تكنولوجيا المعلومات والإتصالات.

2. ضرورة تقنين قواعد جديدة ومناسبة في مجال الإجراءات الجزائية تأخذ بعين الإعتبار الطبيعة الخاصة لهذه الجرائم، تعتمد على أساليب وتقنيات حديثة في مجال التحقيق وجمع الأدلة في الجرائم الإلكترونية حتى تكون مسألة الإثبات سهلة ويسيرة.

3. يجب على الدول أن تتخذ التدابير التشريعية التي تخولها سلطة التفتيش لأحد أنظمة الحاسب الآلي والإطلاع على البيانات المخزنة به والتي تكون متصلة بحاسوب المشتبه به حتى ولو كان خارج إقليم دولة أخرى، وذلك بهدف تسهيل إجراءات التفتيش حتى لا يفلت المجرمون من العقاب.

4. من أجل ضمان حفظ الحياة الخاصة للمتهم وضمان عدم انتهاكها، نوصي بضرورة أن يلتزم الشخص الذي يقوم بالتفتيش بما جاء في إذن التفتيش، إذ أن مشروعية هذا الإجراء تتوقف على ضرورة احترام نطاقه المكاني، إذ ينبغي عدم الإطلاع إلا على البيانات والأماكن المذكورة في الإذن والتي تكون لها علاقة بالجريمة محل التحقيق.

5. من أجل الحفاظ على حقوق المتهم، ينبغي حضور هذا الأخير عند تفتيش حاسبه الآلي، وكذلك الحال عند تفتيش حاسب غيره، وهذا في حالة ضبط دليل ضده، مع ضرورة الإبقاء على الأدلة والمحافظة عليها حتى لا تكون عرضة للإتلاف بسبب وجوده، الأمر الذي يؤثر على سيرورة التحقيق.

6. من أجل تحقيق حماية فعالة في البيئة الإلكترونية ينبغي ضرورة سن تشريعات واتخاذ تدابير تمكّن السلطات المختصة من القيام بالتحفظ على البيانات المخزنة في نظم الحاسوب، وتوسيع صلاحيات جهات التحقيق من أجل إصدار الأوامر لأي شخص يشتبه بحيازته معلومات، وإلى أي مقدم خدمات داخل الدولة من أجل إحضار المعلومات المتعلقة بالمشتركين لديه مما يفيد في إثبات الجريمة والكشف عن الحقيقة.

7. إدخال تعديلات على نصوص قانون الإجراءات الجزائية فيما يتعلق بواجبات الشاهد المعلوماتي ودوره في الإثبات.

8. ضرورة وضع نظام قانوني لحماية الحياة الشخصية في بيئة الإنترنت، وذلك لحمايتها من العبث وتأمين الحماية الفعالة للحياة الشخصية، غير أن هذه الحماية لن تتحقق عن طريق إقرار نصوص قانونية فقط، وإنما ينبغي في نفس الوقت أن تكون هناك توعية لمستعملي النظم المعلوماتية وإدراكهم بمدى خطورة إستعمال شبكة الإنترنت .

9. وجوب الأخذ بالدليل الإلكتروني كدليل أصلي دون أن يوجد دليل يدعمه، مع ضرورة توافر شروط معينة تؤكد مصداقيته.

10. إتخاذ التدابير اللازمة لحل مشكلات الإختصاص القانوني والقضائي التي تثيرها الجرائم الإلكترونية، خاصة مع عالمية هذه الجرائم.

11. ضرورة عقد دورات تدريبية لرجال القانون لدراسة قانون المعلوماتية في المعاهد المتخصصة، خاصة وأن هذا القانون قد يتضمن مصطلحات تقنية لا يعلم مضمونها، لأنه من المفيد جدا ضبط المصطلحات أولا، هذه الأخيرة التي تعتبر جديدة في حقل القانون، كما يتم تدريبهم على كيفية التعامل مع أجهزة الحاسب الآلي

والإنترنت، لأن سوء استخدام هذه الأجهزة والتقنيات الحديثة من شأنه أن يضيع الدليل الإلكتروني دون قصد ومن المهم جدا الإستعانة بالخبراء.

12. تعزيز التعاون الدولي والتنسيق مع المؤسسات الدولية المعنية لمكافحة الجريمة الإلكترونية، وفي هذا الصدد من الضروري أن تنضم الدول العربية إلى الإتفاقيات الدولية الخاصة بمكافحة الجرائم الإلكترونية، وذلك لمواجهة الصعوبات التي تقف عائقا أمام جمع الأدلة.

13. ضرورة تفعيل دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، بحيث تصبح هي المرجعية عند دراسة ظاهرة الجريمة الإلكترونية، كما ينبغي الرجوع إليها في حالة وجود تعديلات وذلك من أجل الأخذ باقتراحاتها، وأيضا عند إصدار نصوص تشريعية جديدة، كما يكون لها دور توعوي يتمثل في التحسيس بمخاطر الإنترنت وضرورة أخذ الحيطة والحذر عند استعمال هذه التقنيات الحديثة.

14. ضرورة إتباع وسائل التأمين الحديثة من أجل حماية أجهزة الحاسب الآلي من خلال استخدام الخصائص البيولوجية، والتي من شأنها أن توفر حماية أكثر وضمان أكبر.

15. إنشاء أقسام متخصصة لمكافحة الجرائم الإلكترونية، كما يمكن الحصول على دورات متخصصة من الدول المتقدمة التي ظهرت فيها هذه الجرائم مبكرا باعتبار أنها كانت السباقة في استخدام هذه التقنيات، ومحاولة الإستفادة من خبراتها وذلك من أجل مسايرة التقدم العلمي الكبير الذي وصلت إليه في مختلف المجالات، مما يساعد في تقديم الحلول لمكافحة هذه النوعية من الجرائم.

16. إنشاء أقسام متخصصة داخل المحاكم للفصل في القضايا المتعلقة بالجرائم الإلكترونية، ودعوة الدول العربية لذلك من أجل التوفيق بين الأحكام الخاصة بهذه الجرائم.

17. ضرورة إنشاء قسم خاص لدراسة قانون تقنية المعلومات بكليات الحقوق وذلك بتكثيف دراسة الحاسب الآلي وشبكة الإنترنت.

18. إنشاء شرطة متخصصة لمكافحة الجرائم الإلكترونية في الدول العربية، وزيادة الجهود فيما بينها كتشجيع بناء منظمات عربية لتبادل المعلومات، وكذا إنشاء موقع إلكتروني للشرطة متخصص في جرائم الكمبيوتر والإنترنت يقدم المعلومات اللازمة عن كافة أنواع هذه الجرائم، كما يتخصص هذا الموقع في تلقي البلاغات المتعلقة بها.

19. ضرورة إصدار دليل إرشادي خاص بالجرائم الإلكترونية بشقيها الموضوعي والإجرائي، إذ يتناول تعريف الجرائم الإلكترونية وبيان صورها وكيفية التحقيق فيها، والأهم من ذلك أن يوضح هذا الدليل كيفية المحافظة

على الأدلة الإلكترونية وطريقة التعامل معها، ومن أجل مواكبة التطور الحاصل في مجال تكنولوجيا الإعلام والإتصال، ينبغي تحديث هذا الدليل بشكل دوري يتماشى بصورة طردية مع التقدم في أساليب ارتكاب الجرائم الإلكترونية.

وفي ختام هذه الدراسة، يستخلص أنّ الأدلة الإلكترونية أصبحت جزءا لا يتجزأ من طرق الإثبات باعتبارها أدلة تتوافق مع طبيعة الجريمة الإلكترونية التي تتم في بيئة إفتراضية غير تقليدية، وهو ما زاد من الحاجة إلى الإستعانة بالوسائل العلمية الحديثة لاكتشاف هذه الجرائم مع مراعاة الضمانات القانونية التي تهدف إلى احترام الحرية الشخصية للأفراد وعدم التعدي عليها في ظل احترام مبدأ الشرعية، وعليه يمكن القول أن الدليل الإلكتروني ما هو إلا تطبيق من تطبيقات الدليل العلمي، إذ يتم الإستعانة بالخبراء الذين يستخدمون الوسائل العلمية الحديثة لاستنباط الدليل والتأكد من صحته.

تم بحمد الله تعالى .

قائمة المصادر والمراجع.

أولا: المراجع باللغة العربية.

1. المراجع العامة:

- إبراهيم بلعليات، أركان الجريمة وظروف إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، ط1،سنة 2007.

- أحمد الشافعي، البطلان في قانون الإجراءات الجزائية (دراسة مقارنة)، دار هومه، الجزائر، ط5، سنة 2005.

- أحمد ضياء الدين، مشروعية الدليل في المواد الجنائية، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2010.

- أحمد عبد الخالق، حقوق الملكية الفكرية، دار المريخ للنشر، المملكة العربية السعودية، بدون طبعة، سنة 2002.

- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 1981.

- أنس العلبي، النظام القانوني لبطاقات الإعتماد، منشورات الحلبي الحقوقية ، بيروت ، لبنان، ط1، سنة 2005.

- إلياس أبو العيد، نظرية الإثبات في أصول المحاكمات المدنية والجزائية، منشورات زين الحقوقية، لبنان، بدون طبعة، سنة 2005.

- جلال وفاء محمدين، الحماية القانونية للملكية الصناعية وفقا لإتفاقية الجوانب المتحصلة بالتجارة من حقوق الملكية الفكرية (تريبس)، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2000.

- جمال نجيمي، إثبات الجريمة على ضوء الإجتهاد القضائي، دار هومة، الجزائر، بدون طبعة، سنة 2012.

- رمسيس بهنام، الإجراءات الجنائية (تأصيلا وتحليلا)، منشأة المعارف، الإسكندرية، مصر، بدون طبعة، سنة 1984.

- سليمان عبد المنعم، بطلان الإجراء الجنائي (تأصيل أسباب البطلان في ظل قضاء النقض في مصر ولبنان وفرنسا)، الجامعة الجديدة، القاهرة، مصر، بدون طبعة، سنة 1999.

- سمير جميل حسين الفتلاوي، الملكية الصناعية وفق القوانين الجزائرية، ديوان المطبوعات الجامعية، الجزائر، بدون طبعة، سنة 2002.

- صلاح الدين جمال الدين، حماية حق المؤلف في ضوء استخدام البث الفضائي للبرامج بالأقمار الصناعية، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2004.
- فاضلي إدريس، المدخل إلى الملكية الفكرية (الملكية الأدبية والفنية والصناعية)، دار هومه، الجزائر، بدون طبعة، سنة 2004.
- مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2003.
- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومه، الجزائر، ط3، سنة 2008.
- محمد عبد اللطيف فرج، شرح قانون الإجراءات الجنائية في مرحلة جمع الإستدلالات والتحقيق الإبتدائي، دار النهضة العربية، القاهرة، مصر، ط2، سنة 2010.
- محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ج 1، ديوان المطبوعات الجامعية، الجزائر، بدون طبعة، سنة 1999.
- نظام الإثبات في المواد الجزائية في القانون الوضعي الجزائري، ج 2 ، ديوان المطبوعات الجامعية، الجزائر، بدون طبعة، سنة 1999.
- محمود صالح العادلي، الجريمة الدولية (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2003 .
- محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، مطبعة جامعة القاهرة، مصر، ط2، سنة 1977.
- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، ط2، سنة 1988.

2. المراجع المتخصصة.

- أحمد خالد العجلوني، التعاقد عن طريق الإنترنت (دراسة مقارنة)، دار الثقافة، عمان، الأردن، بدون طبعة، سنة 2002.
- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2006.
- أحمد عزمي الحروب، السندات الرسمية الإلكترونية، دار الثقافة، عمان، الأردن، ط1، سنة 2010.

- أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، ط1، سنة 2010.

- أسامة أحمد بدر، تداول المصنفات عبر الإنترنت، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2004.

- المطالقة محمد فواز، النظام القانوني لعقود إعداد برامج الحاسب الآلي، دار الثقافة، عمان، الأردن، سنة 2004.

- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه، الجزائر، ط1، سنة 2006.

- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، بدون طبعة، سنة 2005.

- أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني،دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2012.

- أيمن عبد الحفيظ، إستراتيجية مكافحة جرائم الحاسب الآلي، أكاديمية الشرطة، مصر، ط1، سنة 2003.

- بشير عباس العلاق، سعد غالب التكريتي، الأعمال الإلكترونية، دار المناهج للنشر والتوزيع، عمان، الأردن، ط1، سنة 2002.

- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، مصر، ط1، سنة 2011.

- بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، لبنان، ط1، سنة 2009.

- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، مصر، ط1، سنة 1992.

- الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2012.

- حسن المحمدي البوادي، الوسائل العلمية الحديثة في الإثبات الجنائي، منشأة المعارف، الإسكندرية، مصر، بدون طبعة، سنة 2005.

- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2009.

- حسين بن سعيد الغافري، محمد الألفي، جرائم الإنترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة، بدون طبعة، بدون سنة .

- خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2007.

- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2006.

- فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، ط1، سنة 2010.

- حجية البريد الإلكتروني في الإثبات (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، مصر، ط1، سنة 2010.

- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر (أساليب وثغرات)، دار الهدى، الجزائر، ط1، سنة 2010.

- رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة و في ضوء الإتفاقيات والمواثيق الدولية، دار النهضة العربية، القاهرة، مصر، ط1، سنة 2011.

- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة مقارنة)، المكتب الجامعي الحديث، الإسكندرية، مصر، بدون طبعة، سنة 2013.

- رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، سوريا، بدون طبعة، بدون سنة .

- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر و الجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، مصر، ط 1، سنة 1999.

- سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2007.

- سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الإتصال الحديثة (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، ط1، سنة 2006.

- شافع بلعيد عاشور، العولمة التجارية و القانونية للتجارة الإلكترونية، دار هومه، الجزائر، بدون طبعة، سنة 2006.

- شيماء عبد الغني، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر، بدون طبعة، سنة 2007.
- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2009.
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر، بدون طبعة،سنة 2010.
- عبد الحليم مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2001.
- جرائم الإعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2001.
- عبد الفتاح بيومي حجازي، الأحداث والإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2004.
- التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2004.
- مقدمة في حقوق الملكية الفكرية وحماية المستهلك في عقود التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر ، ط1، سنة 2005.
- التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، ط1، سنة 2006.
- مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، ط1، سنة 2006.
- الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار بهجت، الزقازيق، مصر، بدون طبعة، سنة 2009.
- نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار بهجت للطباعة والنشر، نصر، مصر، ط1، سنة 2009.
- التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، بدون سنة.

- عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، شركة البهاء للبرمجيات والكمبيوتر والنشر الإلكتروني، الإسكندرية، مصر، بدون طبعة، بدون سنة.

- عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، مصر، ط2، سنة 2002.

- عزة حمد الحاج سليمان، النظام القانوني للمصارف الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، سنة 2005.

- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الأدبية، منشأة المعارف، الإسكندرية، مصر، بدون طبعة، سنة 2000.

- عفيفي كامل عفيفي وفتوح الشاذلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشورات الحلبي الحقوقية، لبنان، ط2، سنة 2007.

- علي عبد القادر قهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، مصر، بدون طبعة، سنة 1990.

- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة)، المكتب الجامعي الحديث، القاهرة، مصر، بدون طبعة، سنة 2012.

- عمار سالم، المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن، دار النهضة العربية، القاهرة، مصر، ط2، بدون سنة.

- عمر الفاروق حسيني، المشكلات العامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دار النهضة العربية، القاهرة، مصر، ط2، سنة 1995.

- عمر محمد أبو بكر بن يونس، الدليل الرقمي، الجمعية العربية لقانون الإنترنت، مصر، بدون طبعة، سنة2007.

- الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، مؤسسة آدم للنشر والتوزيع، مصر، بدون طبعة، سنة 2008.

- التحكم في جرائم الحاسوب وردعها (المراقبة الدولية للسياسة الجنائية)، مؤسسة آدم للنشر والتوزيع، مصر، بدون طبعة، سنة 2008.

- عمرو عيسى الفقي، وسائل الإتصال الحديثة وحجيتها في الإثبات، المكتب الجامعي الحديث، الإسكندرية، مصر، بدون طبعة، سنة 2006.

- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر والقانون، المنصورة، مصر، بدون طبعة، سنة 2013.

- فاروق محمد أحمد الأباصيري، عقد الإشتراك في قواعد المعلومات عبر شبكة الإنترنت(دراسة تطبيقية لعقود التجارة الإلكترونية الدولية)، دار الجامعة الجديدة، القاهرة، مصر، بدون طبعة، سنة 2006.

- فتحي أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، المركز القومي للإصدارات القانونية، القاهرة، مصر، ط2، سنة 2012.

- كمال السيد غراب، نظم المعلومات الإدارية، دار المعارف، القاهرة، مصر، بدون طبعة، سنة 1997.

- لورنس محمد عبيدات، إثبات المحرر الإلكتروني، دار الثقافة، عمان، الأردن، ط1، سنة 2001.

- محمد إبراهيم أبو الهيجاء، التعاقد بالبيع بواسطة الإنترنت (دراسة مقارنة)، دار الثقافة، عمان، الأردن، بدون طبعة، سنة 2002.

- محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، دار الثقافة، عمان، الأردن، بدون طبعة، سنة 2004.

- محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي (دراسة مقارنة)، دار الثقافة، عمان، الأردن، بدون طبعة، سنة 2011.

- محمد حسن قاسم، مراحل التفاوض في عقد المكينة المعلوماتية (دراسة مقارنة)، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، بدون سنة.

- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2007.

- محمد سامي عبد الصادق، خدمة المعلومات الصوتية والإلتزامات الناشئة عنها، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2005.

- محمد طارق عبد الرؤوف الخن، جريمة الإحتيال عبر الإنترنت (الأحكام الموضوعية والأحكام الإجرائية)، منشورات الحلبي الحقوقية، سوريا، ط2، سنة 2011.

- محمد فتحي، تفتيش شبكة الإنترنت لضبط جرائم الإعتداء على الآداب العامة، المركز القومي للإصدارات القانونية، القاهرة، مصر، ط1،سنة 2012.

- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، مصر، ط1، سنة 2009.

- مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت (دراسة مقارنة)، سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية، الكتاب الخامس، بدون ناشر.
- مصطفى معوان، الإثبات في المعاملات الإلكترونية في التشريعات الدولية (التوقيعات والبصمات الإلكترونية)، دار الكتاب الحديث، القاهرة، مصر، ط1، سنة 2008.
- التجارة الإلكترونية ومكافحة الجريمة المعلوماتية، دار الكتاب الحديث، القاهرة، مصر، ط1، سنة 2008.

- معتز سيد محمد أحمد عفيفي، قواعد الإختصاص القضائي بالمسؤولية الإلكترونية عبر شبكة الإنترنت، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر، ط 1، سنة 2013.
- ممدوح محمد الجنبيهي و منير محمد الجنبيهي، الشركات الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2005.
- بروتوكولات وقوانين الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2006.
- تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، بدون طبعة، سنة 2006.

- ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، بدون طبعة، سنة 2002.
- نبيل صقر، جرائم الكمبيوتر والإنترنت في التشريع الجزائري، دار الهلال للخدمات الإعلامية، الجزائر، بدون طبعة، سنة 2005.
- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، مصر، ط1، سنة 2007.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، الأردن، ط1، سنة 2008.
- هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، مصر، ط1، سنة 1994.
- هلال بن محمد بن حارب البوسعيدي، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2009.

- هلالي عبد اللاه أحمد، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر، ط1، سنة 1997.
- الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2006.
- تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، مصر، ط2، سنة 2008.
- حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، ط2، سنة 2008.

- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، مصر، ط1، سنة 2009.

- يوسف الشيخ يوسف، حماية الحق في حرمة الأحاديث الخاصة في تشريعات التنصت وحرمة الحياة الخاصة، دار الفكر العربي، القاهرة، مصر، ط1، سنة 1997.

- يوسف حسن المصري، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، دار العدالة، القاهرة، مصر، ط1، سنة 2011.

3. الرسائل والمذكرات.

- أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي) دراسة مقارنة، رسالة دكتوراه، جامعة طنطا، مصر، كلية الحقوق، سنة 2000.

- أحمد شحاتة بيومي، الجرائم الماسة بالحياء عبر وسائل الإتصال المستحدثة، رسالة دكتوراه، كلية الدراسات العليا بأكاديمية الشرطة، مصر، سنة 2009.

- أسامة فرج الله محمود الصباغ، الحماية الجنائية للمصنفات الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، سنة 2011.

- سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية، مصر، سنة 2008.

- طارق فوزي الفقي، الجوانب الإجرائية في الجرائم المعلوماتية (دراسة مقارنة)، رسالة دكتوراه، كلية الحقوق، جامعة المنوفية، مصر، سنة 2011.

- طه أحمد طه متولي، الدليل العلمي وأثره في الإثبات الجنائي، رسالة دكتوراه، جامعة طنطا، مصر، سنة 2007.

- عاقلي فضيلة، الحماية القانونية للحق في حرمة الحياة الخاصة (دراسة مقارنة)، رسالة دكتوراه، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، الجزائر، سنة 2012.

- عبد البديع آدم حسين، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، سنة 2000.

- عبد الحفيظ نقادي، أحكام الإذن بالتفتيش في القانون الجنائي الجزائري، رسالة دكتوراه، كلية الحقوق، جامعة الجيلالي ليابس، سيدي بلعباس، الجزائر، سنة 2006.

- عبد الناصر محمد محمود فرغلي، الإثبات العلمي لجرائم تزييف وتزوير المحررات التقليدية والإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، سنة 2010.

- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، سنة 2011.

- محمد محمد الدسوقي الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، سنة 2005.

- منى فتحي عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات (صورها ومشاكل إثباتها)، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، سنة 2009.

- أمين ودرار، مدى شرعية أساليب البحث والتحري الخاصة وحجيتها في الإثبات الجزائي، مذكرة ماجستير، كلية الحقوق، جامعة الجيلالي ليابس، سيدي بلعباس، الجزائر، سنة 2009.

- سمير بردال، جرائم نظام الحاسب الآلي، مذكرة ماجستير، معهد الحقوق، المركز الجامعي مصطفى اسطمبولي، معسكر، الجزائر، سنة 2008.

- عبد القادر درقاوي، جريمة السرقة في عصر المعلوماتية، مذكرة ماجستير، كلية العلوم القانونية والإدارية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، سنة 2005.

- عبير فؤاد عبد العزيز، الحماية الجنائية لبرامج الحاسب الآلي، مذكرة ماجستير، كلية الحقوق، جامعة القاهرة، مصر، سنة 2007.

- محمد حسين علي محمود، التزوير باستخدام الوسائل الإلكترونية، مذكرة ماجستير، كلية الحقوق، جامعة القاهرة، مصر، سنة 2011.

- محمد علي محمد عبيد المحواث الحمودي، دور مأمور الضبط القضائي في مواجهة جرائم المعلومات، مذكرة ماجستير، كلية الحقوق، جامعة القاهرة، مصر، سنة 2009.

4. الإتفاقيات و الدساتير و النصوص التشريعية.

– باللغة العربية:

أ– الإتفاقيات:

- إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية بتاريخ 15-11-2000.

- إتفاقية بودابست الموقعة في 23-11-2001 ببودابست و المتعلقة بالجرائم الإلكترونية.

- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ 21-12-2010 بمدينة القاهرة في جمهورية مصر العربية.

ب– النصوص التشريعية الوطنية.

- الدستور الجزائري لسنة 1996الصادر بتاريخ 08 نوفمبر1996 المعدل بالقانون رقم 08-19 المؤرخ في 15 نوفمبر 2008، الجريدة الرسمية رقم 63.

- قانون رقم 07/79 المؤرخ في 21 يوليو1979 المتضمن قانون الجمارك المعدل والمتمم.

- قانون رقم 88 المؤرخ في 26 جانفي 1988 المتضمن قانون الأرشيف الجزائري.

- قانون رقم 13- 07 المؤرخ في 29 أكتوبر 2013 ينظم مهنة المحاماة، الجريدة الرسمية رقم 55.

- قانون رقم 03/2000 المؤرخ في 05 غشت 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية رقم 48.

- قانون رقم 04/05 المؤرخ في06 فبراير2005 المتضمن قانون تنظيم السجون وإعادة الإدماج الإجتماعي للمحبوسين، الجريدة الرسمية رقم 12.

- قانون رقم 02/06 المؤرخ في 21 محرم 1427 هـ الموافق لـ20 فبراير2006 المتضمن قانون تنظيم مهنة الموثق، الجريدة الرسمية رقم 14.

- قانون رقم 03/06 المؤرخ في21 محرم 1427 هـ الموافق لـ20فبراير 2006 المتضمن قانون تنظيم مهنة المحضر القضائي، الجريدة الرسمية رقم 14.
- قانون رقم 09-04 المؤرخ في 14 شعبان1430 هـ الموافق لـ5غشت2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية رقم 06.
- الأمر رقم 156/66 المؤرخ في08 يونيو1966 المتمم بالأمر رقم 11-02 المؤرخ في 23 فبراير 2011 المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية رقم 12.
- الأمر رقم 156/66 المؤرخ في08 يونيو1966 المعدل و المتمم بالقانون رقم 14-01 المؤرخ في 04 فيفري 2014 المتضمن قانون العقوبات، الجريدة الرسمية رقم 07.
- الأمر رقم 28/71 المؤرخ في .22 أبريل سنة 1971 المعدل و المتمم بالأمر رقم 73-04 المؤرخ في 05 يناير 1973 المتضمن قانون القضاء العسكري، الجريدة الرسمية رقم 05.
- الأمر رقم 58/75 المؤرخ في 26 سبتمبر 1975 المعدل و المتمم بالقانون رقم 05-10 المؤرخ في 20 يونيو 2005 المتضمن القانون المدني، الجريدة الرسمية رقم 44.
- المرسوم التنفيذي رقم 98-257 المؤرخ في25 غشت سنة 1998، المتضمن شروط وكيفيات إقامة خدمات الإنترنت واستغلالها، الجريدة الرسمية رقم 63.
- المرسوم التنفيذي رقم 01-124 المؤرخ في 09 مايو 2001 المتضمن تحديد الإجراء المطبق على المزايدة بإعلان المنافسة من أجل منح رخص في مجال المواصلات السلكية واللاسلكية، الجريدة الرسمية رقم 27.
- المرسوم التنفيذي رقم 141/02 المؤرخ في 16 أبريل سنة 2002 يحدد القواعد التي يطبقها متعاملو الشبكات العمومية للمواصلات السلكية واللاسلكية من أجل تحديد تعريفة الخدمات المقدمة للجمهور، الجريدة الرسمية رقم 28.
- المرسوم التنفيذي رقم162/07 المؤرخ في30 مايو2007، يعدل ويتمم المرسوم التنفيذي رقم123/01 المؤرخ في09 مايو 2001 والمتعلق بنظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، الجريدة الرسمية رقم37.

ج– النصوص التشريعية العربية.

– القانون رقم 1982/37 المؤرخ في 28 سبتمبر 1982 المعدل والمتمم بالقانون رقم 96/95 المؤرخ في 30 جوان 1996 والمتضمن قانون العقوبات المصري.

– القانون رقم 2001/8 المؤرخ في31 ديسمبر2001 بشأن المعاملات الإلكترونية الأردنية.

– القانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات في جمهورية مصر العربية.

– المرسوم الملكي رقم 17 المؤرخ في 1428/03/07 هجري المتضمن نظام مكافحة الجرائم المعلوماتية السعودي.

- **باللغة الأجنبية:**

-Code pénal français (Dernière modification le 06.08.2014).
-Code de procédure pénale français (Dernière modification le 06.08.2014).
-Code des postes et des communications électroniques français (Dernière modification le 04.08.2014).
-Code de la sécurité intérieure français (Dernière modification le 21.08.2014).
-Code civil français (Dernière modification le 06.08.2014).
- Disponible à l'adresse suivante : www.legifrance.gouv.fr

5. المقالات:

– أحمد وهدان، المؤتمر العالمي الأول في الإتجاهات الحديثة في التحقيق الجنائي والإثبات، المجلة الجنائية القومية، المركز القومي للبحوث الإجتماعية والجنائية، القاهرة، مصر، العدد الثاني، يوليو سنة 1996.

– تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت، مجلة الفكر الشرطي، مركز بحوث الشرطة، الشارقة، الإمارات العربية المتحدة، العدد 1، أبريل 2004.

– أسامة بن غانم العبيدي، جريمة الدخول غير المشروع إلى النظام المعلوماتي (دراسة قانونية في ضوء القوانين المقارنة)، مجلة دراسات المعلومات، الرياض، السعودية، العدد الرابع عشر، ماي 2012.

– بشار طلال المومني وعلاء الدين عبد الله الخصاونة، النظام القانوني للصورة الفوتوغرافية (الحقوق الواردة عليها ووسائل الحماية القانونية)، مجلة الشريعة والقانون، كلية الحقوق، جامعة الإمارات العربية المتحدة، العدد 03، يناير 2013.

- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مجلة العلوم القانونية و الإقتصادية، كلية الحقوق، جامعة عين شمس، مصر، العدد الأول، يناير سنة 2007.

- حسن مظفر الرزو، الأمن المعلوماتي (معالجة قانونية أولية)، مجلة الأمن والقانون، أكاديمية شرطة دبي، الإمارات العربية المتحدة، العدد الأول، سنة 1996.

- رشيدة بوكر، الدليل الإلكتروني ومدى حجيته في الإثبات الجزائي في القانون الجزائري، مجلة جامعة دمشق للعلوم الإقتصادية و القانونية، سوريا، المجلد 27، العدد 02، سنة 2011.

- سوزان عدنان وصفاء أوتاني، إنتهاك حرمة الحياة الخاصة عبر الإنترنت، مجلة جامعة دمشق للعلوم الإقتصادية و القانونية، سوريا، المجلد 29، العدد 03، سنة 2013.

- عادل عبد الجواد محمد، إجرام الإنترنت، مجلة الأمن والحياة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، العدد221، ديسمبر سنة 2000.

- غنام محمد غنام، الحماية الإدارية والجنائية للأفراد عند تجميع بياناتهم الشخصية في أجهزة الكمبيوتر، مجلة الأمن والقانون، أكاديمية شرطة دبي، الإمارات العربية المتحدة، العدد الثاني، سنة 2011.

- غنية باطلي، الكتابة الإلكترونية كدليل إثبات، مجلة التواصل في العلوم الإنسانية والإجتماعية، جامعة باجي مختار، عنابة، الجزائر، العدد 30، جوان 2012.

- فوزي عمارة، إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائية، مجلة العلوم الإنسانية، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، الجزائر، العدد 33، جوان 2010.

- كاظم عطية، الحماية الجنائية لحرمة الحياة الخاصة في مواجهة مخاطر بنوك المعلومات، مجلة كلية الدراسات العليا، القاهرة، مصر، العدد19، يوليو2008.

- مصطفى لعروم، غياب القوانين التي تعاقب إساءة استخدام الكمبيوتر، مجلة الموثق،الجزائر، العدد،1 من 26 ماي، جوان 2001.

- ناصر بن محمد البقمي، أهمية الأدلة الرقمية في الإثبات الجنائي، مجلة الفكر الشرطي، الإمارات العربية المتحدة، العدد الأول، يناير2012.

6. الأبحاث والندوات:

- حسين طاهر داوود، جرائم نظم المعلومات، بحث مقدم لأكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، سنة 2000.

- رامي متولي القاضي، الجرائم المعلوماتية وطرق مواجهتها، بحث مقدم لمؤتمر الجرائم المستحدثة (كيفية إثباتها ومواجهتها)، المركز القومي للبحوث الإجتماعية والجنائية، مصر، سنة 2010.

- علي بن عبد الله العسيري، الآثار الأمنية لاستخدام الشباب للإنترنت، بحث مقدم لجامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، سنة 2004.

- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات العربية المتحدة، سنة 2003.

- عمر بن محمد بن يونس، الدليل الرقمي، بحث مقدم إلى الجمعية العربية لقانون الإنترنت، مصر، سنة 2007.

- محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، من 26-2003/04/28، دبي، الإمارات العربية المتحدة.

- محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، بحث مقدم لجامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، سنة 2004.

- موسى مسعود، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية و القانون من 28-10/29 /2009، أكاديمية الدراسات العليا، طرابلس.

7. المجلات القضائية:

- المجلة القضائية للمحكمة العليا، العدد الثاني، سنة 1994.

- الإجتهاد القضائي للغرفة الجنائية بالمحكمة العليا، عدد خاص صادر عن قسم الوثائق بالمحكمة العليا سنة 2003.

8. المواقع الإلكترونية:

- الرضاء سبب لإباحة جرائم الإعتداء على حرمة الحياة الخاصة، بتاريخ: 2011/02/09، على الموقع: www.startimes.com
- تركي محمد العطيان، جرائم الحاسب الآلي، بدون تاريخ، على الموقع: www.aljareh.com
- جرائم الإعتداء على حرمة الحياة الخاصة، على الموقع: www.permalink.com
- جنحة الإعتداء على حرمة الحياة الخاصة، على الموقع: www.aladalacenter.com
-حرمة الحياة الخاصة، بتاريخ :2013/11/19، على الموقع: www.anhri.net
- سعود وصل الله سعد الثبيتي، الجريمة المعاصرة والإستخدامات السلبية للتقنية (جرائم الكمبيوتر والإنترنت)، بدون تاريخ، على الموقع: www.aljareh.com
- عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني وطرق مكافحتها، بدون تاريخ، على الموقع: www.alminbar.alislam.com
- عبد العال الديربي، الحماية الجنائية من الإتلاف المعلوماتي في القانون الفرنسي الحديث، 1 مارس 2013، على الموقع: http://accronline.com
- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، بدون تاريخ، على الموقع: www.aljazeera.talk.net
- محمد أبو العلا عقيدة، التحقيق و جمع الأدلة في مجال الجرائم الإلكترونية، بدون تاريخ، على الموقع: www.flaw.net
- محمد عبد الله المنشاوي، جرائم الإنترنت في المجتمع السعودي، بدون تاريخ، على الموقع: www.minchaoui.com
- محمد عبد الله المنشاوي، جرائم الإنترنت من منظور شرعي وقانوني، بدون تاريخ، على الموقع: www.minchaoui.com
- محمود صالح العادلي، الفراغ التشريعي في مجال مكافحة الجرائم الإلكترونية، بدون تاريخ، على الموقع: www.echoroukonline.com
- يونس عرب، جرائم الكمبيوتر و الإنترنت، بتاريخ **2002/02/01** على الموقع: www.arablaw.net

-www.ioci.org.
-www.swedge.org.

ثانيا: المراجع باللغة الأجنبية.

1- Ouvrages :

-Ouvrages généraux :

-Bernard Bouloc, Gaston Stefani et Georges Levasseur, procedure pénale, 16éme édition, Dalloz, Paris, France, 1996.
-Bernard Bouloc, Georges Levasseur et Gaston Stefani, procédure pénale, Dalloz, Paris, France, 2001.

- Ouvrages spéciaux :

- Aboudramane Quattara, La preuve éléctronique (étude de droit comparé Afrique, Europe, Canada,press universitaires d'Aix marseille-PUAM- France, 2011.
-David Forest et Gautier Kaufman, Droit de l'informatique, Gualino, lextenso éditions, Paris, France, 2010.
-Alain Hollande et Xavier Linant de Bellefonds, Pratique du droit de l'informatique et de l'internet, Delmas, France, 2008.
-Daniel Ventre, Cyberguerre et guerre de l'information, Lavoisier, Paris, France, 2010.
-Jacques Larrieu, Droit de l'internet, Ellipses Edition Marketing, Paris, France, 2010.
-Jean Boyer, L'internet et la protection des données personnelles et de la vie privée, cahiers français, édition de la documentation française, France, 2004.
-Mohamed Chawki, Essai sur la notion de cybercriminalité, IEHEI, France, 2006.
-Raymond Gassin, Fraude informatique, Dalloz, France, 1997.
-Santiago Cavanillas, Vincent Gautrais et autres, Commerce électronique, Delta, Bruxelles, 2001.
-Valérie Sedaillan, Droit de l'internet, collection AUI, Paris, France, 1997.
-Vincent Fauchoux et Pierre Deprez, Le droit de l'internet : Lois, contrats et usages, Litec, Paris, France, 2009.

2- Thèses et mémoires.

-Pierre Bolze**,** Le droit à la preuve contraire en procédure pénale, Thèse Doctorat, Faculté de Droit, Sciences économiques et Gestion, Université Nancy 2, France, 2010.

-Alexandra Greenwood, Le statut de l'hebergueur et le web, mémoire master, droit de l'internet, Université Paris, France, 2009.

-Nathalie Moreau, La formation du contrat électronique : Dispositif de protection du cyberconsommateur et modes alternatifs de règlement des conflits(M.A.R.C), mémoire DEA Droit des contrats, Faculté des Sciences Juridiques, Politiques et Sociales, Université de Lille 2,France, Année universitaire 2002/2003.

-Régie Buchillet, La responsabilité des prestataires techniques de l'internet, mémoire DEA droit de l'économie, faculté de droit et de sciences politiques, Université de Bourgogne, France, 2002.

3- Articles :

-Bertrand Warusfel, Procédure pénale et technologies de l'information (de la convention sur la cyber criminalité – à la loi sur la sécurité quotidienne), Revue droit et défense, N°1, 2002.

-Claude Fabien, La preuve par document technologique, R.J.T , Faculté de droit de l'Université de Montréal , N° 38, 2004.

-Eric Caprioli, L'importance des preuves électroniques pour résoudre les litiges internationaux, séminaire sur La preuve électronique dans l'arbitrage international, le 10.12.2008, organisé par ICC France.

-Isabelle Renard, Preuve informatique(valeur juridique du document numérique), Expertises des systèmes d'information,N°348, Juin 2010.

-Marylou Garcias et Max Chouzier, La preuve informatique — Quelles nouveautés techniques pour quelles évolutions juridiques ?, Lexbase Hebdo édition affaires n˚280 du 18 janvier 2012.

-Michel Gagné, La preuve dans un contexte électronique, Ce texte est publié dans Développements récents en droit de l'Internet, Service de la formation permanente, Barreau du Québec, Éditions Yvon Blais Inc., 2001.

-Philippe Boure, Internet et la lutte contre la cybercriminalité, Gaz.Pal, janvier 2003.

-Signature électronique, Document édité par le Bureau conseil de la direction centrale de la sécurité des systèmes d'information (DCSSI), 25.08.2004, Paris, France.

4- Articles sur internet :

-Algerie vulnérable face à la cybercriminalité, disponible à l'adresse suivante : www.bladi-dz.com.

-Bruno Cormier, cybercriminalité aux USA, disponible à l'adresse suivante : www.pointpact.com.

-Camille Adaoust, La cybercriminalité tisse sa toile, le 19.07.2014, disponible à l'adresse suivante : www.lefigaro.fr.

-Camille Studer, Les géants du web et la cybercriminalité, le 30.06.2014, disponible à l'adresse suivante : www.infoguerre.fr.

-Charpentier Elise, Entre droits de la personnalité et droit de propriété, disponible à l'adresse suivante :https ://ssl.editionsthemis.com.

-Christine Lejoux, La cybercriminalité, un business à 1.000 milliards, le 01.07.2014, disponible à l'adresse suivante : www.latribune.fr.

-Clément Bohic, Le poids économique de la cybercriminalité, le 10.06.2014, disponible à l'adresse suivante : www.itespresso.fr.

- Cybercriminalité: Service national de coordination de la lutte contre la criminalité sur internet(SCOCI),le 07.05.2012,disponible à l'adresse suivante: www.fedpol.admin.ch/fedpol/fr/home/themen/kriminalitaet/cybercrime.html.

-Daguet Julie et Foubert Charlotte, Qu'est-ce que la cybercriminalité ? le 18.03.2014, disponible à l'adresse suivante : http://causes-cybercriminalité.over-blog.com/

-Damien Licata Caruso, Cybercriminalité :72% des sites français mal protégés contre le piratage, le 07.07.2014, disponible à l'adresse suivante : www.leparisien.fr.

-Didier Frochot, preuve et signature électroniques, le 16.09.2005, disponible à l'adresse suivante : www.les-infostrateges.com.

-Eric Caprioli, Traçabilité et droit de la preuve électronique, Mai 2001, disponible à l'adresse suivante : www.caprioli-avocats.com.

-Eric Freyssinet, 160 personnes luttent quotidiennement contre la cybercriminalité, disponible à l'adresse suivante : www.journaldunet.com.

-Eric Freyssinet, La cybercriminalité en mouvement, Novembre 2010, disponible à l'adresse suivante : www.cairn.info/revue-realites-industrielles-2010-4-page-28.htm.

-Erwan Coatnoan De Kerdu, La cybercriminalité pour les entreprises, le 07.03.2014, disponible à l'adresse suivante :www.dynamique-mag.com.

-Etienne Wery, Droit de la preuve : vers une preuve électronique ?, le 25.01.1999, disponible à l'adresse suivante :www.droit-technologie.org.

-Frédérick Gaudreau, Comité technique : Cybercriminalité, disponible à l'adresse suivante : www.francopol.org.

-Gilbert Kallenborn, La cybercriminalité, main dans la main avec le crime organisé, le 16.01.2014, disponible à l'adresse suivante :www.01net.com.

-Internet : comment prévenir et réprimer la cybercriminalité ? le 10.07.2014, disponible à l'adresse suivante : www.vie-publique.fr.
-Jean-Pierre Stroobants, Cybercriminalité : la commission européenne multiplie les actions, le 10.02.2014, disponible à l'adresse suivante : www.lemonde.fr.
-Julien, L'Europe s'arme contre la cybercriminalité, le 30.05.2014, disponible à l'adresse suivante : www.numerama.com.
-La cybercriminalité plus répandue en France qu'ailleurs, le 19.02.2014, disponible à l'adresse suivante : www.challenges.fr.
-La cybercriminalité, disponible à l'adresse suivante :
http://www.interieur.gouv.fr.
-Le droit d'internet, le 03.11.2011, disponible à l'adresse suivante :
www.ladocumentationfrançaise.fr.
-Lionel Revello, La preuve électronique, disponible à l'adresse suivante :
www.sam-mag.com.
-Lova Emmanuel, Loi contre la cybercriminalité – Retouche et amendement possibles, le 31.07.2014, disponible à l'adresse suivante : www.lexpressmada.com.
-Marc Rees, Les principales mesures du plan anti – cybercriminalité, disponible à l'adresse suivante : www.pointpact.com.
-Margaret Beare, Les femmes et le crime organisé, disponible à l'adresse suivante : http://publication.gc.ca.
-Margot Stephan, Le régime de la preuve électronique, le 31.03.2014, disponible à l'adresse suivante : http://faq.adullact.org.
-Marie, Combien coûte la cybercriminalité, le 16.06.2014, disponible à l'adresse suivante :www.lemondenumerique.com.
-Mascré Heguy, La signature électronique et le bouleversement du droit de la preuve, disponible à l'adresse suivante : www.mascre-heguy.com.
-Mathieu Olivier, Cybercriminalité : pourquoi l'Afrique doit faire face ? le 21.02.2014, disponible à l'adresse suivante : www.jeuneafrique.com.
-Nathalie Bismuth, Les perspectives pénals de la loppsi 2 en matiére de cybercriminalité, le 10.02.2010, disponible à l'adresse suivante :
www.e-juristes.org.
-Nicolas Aguila, L'Europe durcit les sanctions contre la cybercriminalité, le 05.05.2013, disponible à l'adresse suivante : www.tomsguide.fr/actualite/europe-cybercriminalité,21819.html.
-Peihao Yuan, L'admission de la preuve électronique dans le droit français et le droit chinois, le 30.03.2011, disponible à l'adresse suivante :
http ://m2bde.u-paris10.fr.
-Peter vakof, Administration de la preuve électronique, disponible à l'adresse suivante : www.pwc.com/ca/fr/risk/forensik-technology/e-discovery.jhtml.
-Services d'administration de la preuve électronique, disponible à l'adresse suivante : www.kpmg.com.

-Solange Ghernaouti-Hélie, comment lutter contre la cybercriminalité ?, Mai 2010, disponible à l'adresse suivante : www.pourlascience.fr.
-Stephanie Lacour et Marion Videau, L'egistique de la preuve électronique, disponible à l'adresse suivante : www.demotis.org.
-Véronique Aréne, Les pertes liées à la cybercriminalité évaluées à 400 Md$, le 10.06.2014, disponible à l'adresse suivante : www.lemondeinformatique.fr.
-Veronique Guillermard, la lutte contre la cybercriminalité est un marché d'avenir, le 06.08.2014, disponible à l'adresse suivante : www.le figaro.fr.
-Yannis Delmas, Histoire de l'informatique, d'Internet et du Web , disponible à l'adresse suivante : www.delmas-rigoutsos.nom.fr.

5-Jugements et décisions des tribunaux étrangères :

-TGI de Privas, Jugement correctionnel du 03 Septembre1997,disponible à l'adresse suivante :www.legalis.net.
-TGI de Clermont-Ferrand, Chambre correctionnelle, jugement du 26 Septembre 2011, disponible à l'adresse suivante : www.legalis.net.
- Décision de la cour de cassation, chambre criminelle rendue le 31/01/2007, rejet – Numéro de pourvoi : 06-82383, Disponible à l'adresse suivante : www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000017627847.

الفهرس